

Refining the RSA Attack Bounds

Final Report of UGC MRP (2015)

MRP ID: MRP-MAJOR-MATH-2013-22283

(UGC F. No. 43-427/2014(SR)/Dt.20-08-2015)



Dr. P. Anuradha Kameswari
Principle Investigator

DEPARTMENT OF MATHEMATICS
ANDHRA UNIVERSITY
VISA KHAPATNAM
2018

S. No.	CONTENTS	Page No./ Enclosures
1.	Statement of expenditure	Annexure-III
2.	Project Fellow appointment	Annexure-VI
3.	Final Report of the work done on MRP	Annexure-VIII
4.	Proforma for submission of information with the Final Report	Annexure-IX
5.	Assessment Certificate	Annexure-X
6.	Report of work done	Enclosure-1
	Acknowledgements	Page-i
	Abstract of the Project	Page-ii
	Chapter-0: Introduction	Page 1
	Chapter-1: Preliminaries	Page 7
	Chapter-2: Cryptanalysis Based on Continued Fractions, for RSA with Small Deciphering Exponent	Page 31
	Chapter-3: Cryptanalysis Based on Lattice-Based Techniques, for RSA with Small Deciphering Exponent	Page 53
	Chapter-4: Cryptanalysis Based on Lattice-Based Techniques, for RSA with Small Multiplicative Inverse of $(p-1)$ or $(q-1)$ Modulo e	Page 75
	Chapter-5: Cryptanalysis Based on Lattice-Based Techniques, for RSA with Small Multiplicative Inverse of $\varphi(N)$ Modulo e and with a Composed Prime Sum $p+q$	Page 97
	Chapter-6: Conclusion	Page 131
	Appendices	Page 133
	References	Page 141
7.	Research Publications	Enclosure-2
8.	Achievements of the project study	Enclosure-3
9.	Summary of the findings	Enclosure-4
10.	Contribution to the Society	Enclosure-5

**UNIVERSITY GRANTS COMMISSION
BAHADUR SHAH ZAFAR MARG
NEW DELHI – 110 002**

STATEMENT OF EXPENDITURE IN RESPECT OF MAJOR RESEARCH PROJECT

1. Name of Principal Investigator: **Dr. P. Anuradha Kameswari**
2. Dept. of Principal Investigator: **Department of Mathematics**
University/College: Andhra University
3. UGC approval Letter No. and Date: **F.No:43-427/2014(SR), dt:20-08-2015**
4. Title of the Research Project: **Refining the RSA Attack Bounds**
5. Effective date of starting the project: **01-07-2015**
6. a. Period of Expenditure: **From 01-07-2015 to 30-06-2018**
b. Details of Expenditure _____

S.No.	Item Head	Amount Approved	Grant Released During the period		Expenditure Incurred
			Grant Released 1 st Instalment	Grant Released 2 nd Instalment	
1	Books & Journals	Rs.75,000/-	Rs.75,000/-	---	Rs.75,000/-
2	Equipment	Rs.1,00,000/-	Rs.1,00,000/-	---	Rs.99,900/-
3	Contingency	Rs. 1,50,000/-	Rs.75,000/-	Rs.60,000/-	Rs. 1,50,000/-
4	Field work/ Travel(Give details in Proforma at Annexure VI)	Rs. 1,50,000/-	Rs.75,000/-	Rs. 0/-	Rs.36,736.75/-
5	Hiring Services	---	----	----	----
6	Chemicals & Glassware	----	----	----	----
7	Overhead	Rs.75,000/-	Rs.75,000/-	---	Rs.75,000/-
8	Any other items (Please specify)	---	----	----	----

c . Staff

Date of Appointment: **01-01-2016(Project fellow)**

S.No	Items	From	To	Amount Approved (Rs.)	Expenditure incurred (Rs.)
1.	Honorarium to PI (Retired Teachers) @ Rs. 18,000/-p.m.				
2.	Project fellow: i) NET/GATE qualified -Rs. 16,000/- p.m. for initial 2 years and Rs. 18,000/- p.m. for the third year. ii) Non-GATE/Non-NET - Rs. 14,000/- p.m. for initial 2 years and Rs. 16,000/- p.m. for the third year.	01-01-2016 01-01-2018	31-12-2017 31-03-2018	3,00,000/- 88000/-	336000/- 48000/-

1. It is certified that the appointment(s) have been made in accordance with the terms and conditions laid down by the Commission.
2. If as a result of check or audit objection some irregularly is noticed at later date, action will be taken to refund, adjust or regularize the objected amounts.
3. Payment @ revised rates shall be made with arrears on the availability of additional funds.
4. Certified that an amount of Rs.8,68,636/- (Rupees eight lakhs sixty eight thousand six hundred thirty six only) out of the total sanctioned grant of Rs.9,82,000/- (Rupees nine lakhs eighty two thousand only) vide Lr.No.F-43-427/2014 (SR), dt.04-11-2017, released grant of Rs.8,48,800/- vide UGC Letter No.F-43-427/2014 (SR), dt.04-11-2017, received from the University Grants Commission under the scheme of support for Major Research Project entitled: "Refining the RSA Attack Bounds", has been utilized for the purpose for which it was sanctioned and in accordance with the terms and conditions laid down by the University Grants Commission. An amount of Rs.38,364/- (Rupees thirty eight thousand three hundred sixty four only) is lying with university as unspent balance.

SIGNATURE OF THE
PRINCIPAL INVESTIGATOR

REGISTRAR/PRINCIPAL

(Seal)

STATUTORY AUDITOR

(Seal)



**INFORMATION OF THE PROJECT FELLOW (STAFF)
APPOINTED UNDER THE SCHEME OF MAJOR RESEARCH PROJECT**

UGC FILE NO. : F. No-43-427/2014(SR)

YEAR OF COMMENCEMENT: 01-07-2015

TITLE OF THE PROJECT: REFINING THE RSA ATTACK BOUNDS

1.	Name of the Principal Investigator	Dr. P. Anuradha Kameswari			
2.	Name of the University	Andhra University			
3.	Name of the Project fellow appointed	L. Jyotsna			
4.	Academic qualifications	S.No	Qualifications	Year	Grades
		1.	M.Sc.	2009	9.6
		2.	M.Phil.	2012	9.3
5.	Date of Joining	01-01- 2016			
6.	Date of Birth of Project fellow	05-06-1988			
7.	Amount of HRA, if drawn	-----			
8.	Number of Candidates applied for the post	08			

CERTIFICATE

This is to certify that all the rules and regulations of UGC Major Research Project outlined in the guidelines have been followed. Any lapse on the part of the university will liable to terminate of said UGC project

Principal Investigator**Head of the Department****Registrar/Principal**

**UNIVERSITY GRANTS COMMISSION
BAHADUR SHAH ZAFAR MARG
NEW DELHI 110 002**

FINAL REPORT OF THE WORK DONE ON THE MAJOR RESEARCH PROJECT
(Report to be submitted within 6 weeks after completion of each year)

1.	Project Report No.	:	FINAL
2.	UGC Reference No.	:	F.No:43-427/2014(SR), dt:20-08-2015
3.	Period of Report	:	01-07-2015 to 30-06-2018
4.	Title of the Project	:	Refining the RSA Attack Bounds
5.	(a) Name of the Principal Investigator (b) Department (c) University/College where work has progressed	:	Dr. P. Anuradha Kameswari Department of Mathematics Andhra University Visakhapatnam 530 003
6.	Effective date of starting of the project	:	01-07-2015
7.	Grant approved and expenditure incurred during the period of the report a. Total amount approved b. Total expenditure c. Report of the work done(Please attach the separate sheet)	:	Rs. 9,82,000/- Rs. 8,68,636/- Enclosure-1
	(i) Brief Objective of the Project	:	The objective of the project is to refine RSA attack bound by extending the techniques of Coppersmith, the lattice based approach and sub lattice based approach initiated by Boneh and Durfee and Blomer-May for appropriate univariate, bivariate or multivariate polynomials and extend the existing algorithms for the computation
	(ii) Work done so far and results achieved and publications, if any, resulting from the work (Give details of the papers and names of the journals in which it has been published or accepted for publication	:	Enclosure-2
	(iii) Has the progress been according to original plan of work and towards	:	Yes (completed the project as per the original plan of work)

	achieving the objective? if not, state reasons		
	(iv) Please indicate the difficulties, if any, experienced in implementing the project		None
	(v) If project has not been completed, please indicate the approximate time by which it is likely to be completed. A summary of the work done for the period (Annual basis) may please be sent to the Commission on a separate sheet		Not applicable
	(vi) If the project has been completed, please enclose a summary of the findings of the study. One bound copy of the final report of work done may also be sent to University Grants Commission		Enclosure-1
	(vii) Any other information which would help in evaluation of work done on the project. At the completion of the project, the first report should indicate the output, such as (a) Manpower trained (b) Ph. D. awarded (c) Publication of results (d) other impact, if any		(b) Project fellow enrolled for Ph.D. (c) Enclosure-2

Signature of the Principal
Investigator

Signature of the
Registrar/Principal

**UNIVERSITY GRANTS COMMISSION
BAHADUR SHAH ZAFAR MARG
NEW DELHI 110 002**

**PROFORMA FOR SUBMISSION OF INFORMATION AT THE TIME OF SENDING THE
FINAL REPORT OF THE WORK DONE ON THE PROJECT**

1.	Title of the Project		Refining the RSA Attack Bounds
2.	Name and address of the Principal Investigator	:	Dr. P. Anuradha Kameswari
3.	Name and address of the Institution		Department of Mathematics Andhra University Visakhapatnam 530 003 Email: panuradhakameswari@yahoo.in
4.	UGC Approval No. and Date	:	F.No:43-427/2014(SR), dt:20-08-2015
5.	Date of implementation	:	01-07-2015
6.	Tenure of the Project	:	Three years
7.	Total grant allocated	:	9,82,000/-
8.	Total grant received	:	8,48,800/-
9.	Final expenditure	:	8,68,636/-
10.	Title of the Project		Refining the RSA Attack Bounds
11.	Objectives of the Project:		<p>(i) Proposed to study the scope for choice of polynomials called shift polynomials that monitor the applications of coppersmith methods of finding small modular univariate polynomials.</p> <p>(ii) To study the scope for choice of shift polynomials by lattice reduction and sub lattice reduction by using the techniques of Boneh-Durfee for bivariate polynomials. Finally used in RSA attack and then refine the attack with these ideas by choosing another appropriate bivariate polynomials.</p> <p>(iii) To study the scope for choice of shift polynomials by lattice reduction and sub lattice reduction by using the techniques of Blomer-May for bivariate polynomials. Finally used in RSA attack and then refine the attack with these ideas by choosing another appropriate bivariate</p>

			<p>polynomials.</p> <p>(iv) To study the scope for choice of shift polynomials by lattice reduction and sub lattice reduction by using the techniques of Boneh-Durfee for bivariate polynomials. Finally used in RSA attack and then refine the attack with these ideas by choosing another appropriate multivariate polynomials.</p>
12.	Whether objectives were achieved	:	Yes
13.	Achievements of the project	:	Enclosure-3
14.	Summary of the Findings		Enclosure-4
15.	Contribution to Society		Enclosure-5
16.	Whether any Ph.D. enrolled/produced out of the project:	:	Project fellow enrolled for Ph.D.
17.	No. of Publications out of the Project:	:	Enclosure-2

Signature of the Principal
Investigator

Signature of the
Registrar/Principal

FINAL REPORT ASSESSMENT/EVALUATION CERTIFICATE

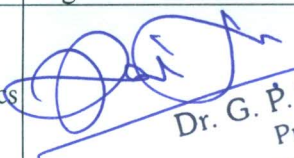
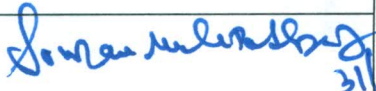

(Two Member Expert Committee not belonging to the institute of Principal Investigator)
(to be submitted with the Final Report)

It is certified that the final report of Major Research Project entitled “**Refining the RSA attack bounds**” by Dr. P. Anuradha Kameswari, Department of Mathematics, Andhra University, Visakhapatnam has been assessed by the committee consisting the following members of the final submission of the report to the UGC, New Delhi under the scheme of Major Research Project.

Comments/ Suggestions of the Expert Committee

The project balances both theory and application. The outcome is very good.

Name & Signatures of Experts

Name of Expert	University/College Name	Signature with Date
G P Raja Sekhar	Professor Department of Mathematics IIT Kharagpur Kharagpur 721302	 Dr. G. P. Raja Sekhar Professor Department of Mathematics Indian Institute of Technology Kharagpur Kharagpur-721302, India
Sourav Mukhopadhyay	Associate Professor Department of Mathematics IIT Kharagpur Kharagpur 721302	 31/10/18  Dr. Sourav Mukhopadhyay Associate Professor Department of Mathematics I.I.T. Kharagpur-721302

It is certified that the final report has been uploaded on UGC-MRP portal _____

It is also certified that final report, Executive summary of the report, Research documents, academic papers provided under Major research Project have been posted on the website of University.

Principal Investigator

Registrar

Enclosure-2

REPORT OF WORK DONE

Acknowledgments

I duly acknowledge the University Grants Commission (UGC), New Delhi for granting financial assistance to UGC Major Research Project (MRP) titled “**Refining the RSA attack bounds**”.

I sincerely extend my thanks to the administration and secretarial staff of UGC section Andhra University, Visakhapatnam for their constant support and help in the execution of project study successfully.

I duly acknowledge the Head, Department of Mathematics, J.V.D. College of Science & Technology, Andhra University for the facilities extended during the project study.

I am grateful to Mrs. Suguna, in charge CSA Department of Library, Department of Computer Science & Automation, IISc, Bangalore for granting the permission to avail the Library facility.

I am grateful to Dr. Ramakrishna Nanduri, from Department of Mathematics, IIT Kharagpur for granting the permission to avail the Library facility of the IIT Kharagpur Central Library.

I am grateful to Prof. K. Srinivas, IMSc for helping with the related discussions on the topic that enhance the ideas and permitting me to use the Library facilities.

Abstract of the Project

The studies of Wiener's attack on RSA with small decryption exponents initiated the study of continued fraction based attacks on RSA and led to the study of refinement of attack bounds on the decryption exponent, by B de Weger, Subhamoy Maitra and Santanu Sarkar. Further R.G.E. Pinch proved that Wiener's attack on RSA cryptosystem with small decryption exponent may be extended to RSA-like cryptosystems on elliptic curves and Lucas sequences. Coppersmith methods of finding small roots of univariate modular equations initiated the study of lattice based attacks on RSA with low decryption exponent and led to the study of refinement of these attack bounds by Boneh-Durfee, Blömer-May, B de Weger and Maitra-Sarkar. In this project we proposed an attack using lattice reduction techniques on RSA when $p - 1$ or $q - 1$ have small multiplicative inverse less than or equal to N^δ modulo the public encryption exponent e and further refined the attack bounds for δ . We also proposed an attack using lattice reduction techniques on RSA when $\varphi(N)$ has small multiplicative inverse k modulo the public encryption exponent e and for $k \leq N^\delta$, the attack bounds for δ are described. Later proved that if the prime sum $p + q$ is of the form $p + q = 2^n k_0 + k_1$ where n is a given positive integer and k_0 and k_1 are two suitably small unknown integers then the maximum bound for δ can be refined. Employing the previous tools, we provide an attack bound for the deciphering exponent d when the prime sum $p + q = 2^n k_0 + k_1$ for appropriately small k_0 and k_1 . We proved that all the continued fraction based attacks and lattice reduction based attacks can be extended to RSA-like cryptosystem over elliptic curves $E(\mathbb{Z}_{pq})$ due to KMOV.

Chapter 0

Introduction

Cryptography is a tool used in the protection of information regarding national and private sector by means of cryptosystems. There are different cryptosystems like classical and public key. In 1978 Rivest, Shamir and Adleman discovered first practical public key cryptosystem named after them as RSA. RSA is used in applications such as e-mail, e-banking etc. The study of security analysis of cryptosystem called cryptanalysis. Much research is done on the security analysis of RSA. The secret information of the RSA parameters (p, q, d) is obtained from the public information (N, e) in the cryptanalysis of RSA. This may be attained by factorizing N . In the past three decades lots of weaknesses of RSA with respect to its variants are identified and the study of cryptanalysis of RSA has gained importance.

In RSA cryptosystem, the encryption and decryption are based on the fact that for $N = pq$, the modulus for RSA, for p, q distinct primes and if $1 \leq e \leq \varphi(N)$ with $(e, \varphi(N)) = 1$ and d , the multiplicative inverse of e modulo $\varphi(N)$, then $(m^e)^d = m \pmod{N}$, for any message m in \mathbb{Z}_N . The security of this system depends on the difficulty of finding factors of a composite positive integer, that is product of two large primes.

In 1990, M.J. Wiener [48] was the first one to describe a cryptanalytic attack on the

use of short RSA decryption exponent d . This attack is based on continued fraction algorithm which finds the fraction $\frac{t}{d}$ that is a convergent of $\frac{e}{N}$, where $t = \frac{ed-1}{\varphi(N)}$, in a polynomial time when $d < N^{0.25}$ for $N = pq$ and $q < p < 2q$.

The studies on Wiener's attack on RSA with small decryption exponents led to the refinement of attack bounds on the decryption exponent.

In 2000, D. Boneh and G. Durfee [5] improved the Wiener bound on d from $N^{0.25}$ to $N^{0.292}$, for $q < p < 2q$ using lattice reduction theory.

In 2001, a lattice attack on RSA with short secret exponent d , for d less than $N^{0.29}$ was given by J. Blömer and A. May [3], this is slightly less than that of Boneh and Durfee but this method requires lattices of dimension smaller than the approach by Boneh and Durfee.

In 2002, B de Weger [47], for $d = N^\delta$, $p - q = N^\beta$ and $q < p < 2q$ extended the Wiener's attack in the range $N^{0.25} \leq d \leq N^{0.75-\beta}$, using continued fractions and the bound improved to $\delta < \frac{1}{6}(4\beta + 5) - \frac{1}{3}\sqrt{(4\beta + 5)(4\beta - 1)}$ using lattice based techniques in [5] and the bound improved to $\delta < 1 - \sqrt{2\beta - \frac{1}{2}}$ using sub-lattice based techniques in [5] under the condition $\delta > 2 - 4\beta$.

In 2008, Subhamoy Maitra and Santanu Sarkar [30] instead of considering $p-q = N^\beta$, considered $|p - \rho q| \leq \frac{N^\gamma}{16}$ where $1 \leq \rho \leq 2$ to get the bound when $d = N^\delta$ and $\delta < \frac{1}{2} - \frac{\gamma}{2}$, for $|p - \rho q| \leq \frac{N^\gamma}{16}$ and $\gamma \leq \frac{1}{2}$ using continued fractions and also showed that this bound on δ can be extended using the lattice based techniques [31].

In 2006, E. Jochemsz and A. May [18] gave a new attack on an RSA variant called common prime RSA. In 1995, R.G.E. Pinch in [37], proved that Wiener's attack on RSA Cryptosystem with small decryption exponent may be extended to RSA-like cryptosystems on elliptic curves and Lucas sequences.

In this project we described the refinement of all these attacks on RSA by cate-

gorizing the attacks as attacks based on continued fractions and attacks based on lattice reduction and proposed extensions of these attacks on RSA with respect to other variants of RSA and RSA-like cryptosystem over elliptic curves $E(\mathbb{Z}_{pq})$ due to KMOV.

We first described the **continued fraction** based attacks of M.J. Wiener and its extensions by B de Weger and Subhamoy Maitra and Santanu Sarkar [21] and then proposed that the Wiener's extensions can also be extended to RSA-like Cryptosystem over elliptic curves $E(\mathbb{Z}_{pq})$ due to KMOV. Next we described the **lattice reduction** based attacks on RSA by Boneh-Durfee, Blömer-May, B de Weger and Maitra-Sarkar. All these existing lattice reduction based attacks are with respect to low decryption exponent d of RSA.

We proposed the extensions of lattice reduction attacks on RSA with respect to small multiplicative inverse of $p - 1$ or $q - 1$ modulo e and with respect to small multiplicative inverse of $\varphi(N)$ modulo e , the public encryption exponent.

If $e = N^\alpha > p - 1$, r and s the multiplicative inverses of $p - 1$ and $q - 1$ modulo e respectively, then for (x_0, y_0) solution of the polynomial congruence $f(x, y) \equiv 0 \pmod{e}$, for $f(x, y) = x(y + A) - 1$ with $A = \lceil \sqrt{N} \rceil - 1$ and N^δ, N^γ upper bounds for x_0, y_0 respectively, we implemented the idea of Boneh and Durfee as in [5] based on lattice reduction techniques to our polynomial congruence and proved that the attack works for $\delta < \frac{3\alpha + \gamma - 2\sqrt{\gamma(3\alpha + \gamma)}}{3}$ when both x and y shifts are used and $\delta < \frac{\alpha - \gamma}{2}$ when only x -shifts are used. Further we improved the bound for δ as $\alpha - \gamma(1 + \alpha) < \delta < \alpha - \sqrt{\alpha\gamma}$ and $\delta < \frac{2\alpha - 6\gamma + 2\sqrt{\alpha^2 - \alpha\gamma + 4\gamma^2}}{5}$ by implementing the sublattice based techniques of Boneh-Durfee and Blömer-May respectively.

We also extended the lattice attacks on RSA if the multiplicative inverse k of $\varphi(N)$ modulo e is small for $q < p < 2q$ and $e = N^\alpha > p + q$, the prime sum. This case can

be considered even when both $(p - 1) \bmod e$ and $(q - 1) \bmod e$ do not have small inverses but $\varphi(N) \bmod e$ has small inverse. For $k \leq N^\delta$, the attack bounds for δ are described by repeating the above lattice based techniques. Further noted that for $\beta \approx 0.5$, the maximum bound for δ can be improved when the prime sum $p + q$ is in the composed form $p + q = 2^n k_0 + k_1$ for known positive integer n and for unknown suitably small integers k_0, k_1 . By using lattice based techniques to the polynomial congruence $f(x, y, z) \equiv 0 \pmod{e}$ for

$$f(x, y, z) = \begin{cases} (N + 1)x + xy + (2^n)xz - 1 & \text{if } |k_0| \leq |k_1| \\ 2^{n'}x(N + 1) + xy + 2^{n'}xz - 2^{n'} & \text{if } |k_1| \leq |k_0| \end{cases}$$

where $2^{n'}$ is an inverse of $2^n \bmod e$, the attack bound for δ is such that $\delta < \frac{1}{2}\alpha - \frac{1}{2}\gamma_1 + \frac{1}{16}\gamma_2 - \frac{1}{16}\sqrt{48(\alpha - \gamma_1)\gamma_2 + 33\gamma_2^2}$ where $N^{\gamma_1}, N^{\gamma_2}$ are the upper bounds for $\max\{|k_0|, |k_1|\}$, $\min\{|k_0|, |k_1|\}$ respectively. Later we slightly improved the previous bound by using the sub-lattice based techniques given by J. Blömer, A. May in [3] to the above polynomial congruence and this method requires lattice of smaller dimension than the above method. The new bound on δ is $\frac{1}{2}\alpha - \frac{1}{2}\gamma_1 - \frac{1}{6}\sqrt{6(\alpha - \gamma_1)\gamma_2 + 3\gamma_2^2}$ and showed that this is a little bit greater than the former bound graphically. Note that this new attack bound is also an attack bound for the deciphering exponent d . The corresponding refinement of attack bounds in each case is depicted explicitly in tabular forms.

The project is organized as follows:

In **Chapter 1** of Preliminaries, basic concepts of Cryptography, Continued fractions and Lattice reduction theory that are employed throughout the book are described

[6][26][2][14][29][8][12].

In **Chapter 2** the attacks on RSA and RSA-like cryptosystem over elliptic curves $E(\mathbb{Z}_{pq})$ due to KMOV based on continued fractions are described. The Wiener's attack on RSA cryptosystem and its extension given by B de Weger, Maitra - Sarkar are described in **section 2.1** and **2.2** respectively. In **section 2.3** analysis on extending Wiener's attack to RSA-like cryptosystem over elliptic curves $E(\mathbb{Z}_{pq})$ due to KMOV is given. In **section 2.4** we proposed that the Wieners extensions on RSA that refine the attack bound may be extended to RSA-like cryptosystem over elliptic curves $E(\mathbb{Z}_{pq})$ due to KMOV.

In **Chapter 3** we review some of the existing lattice based attacks on RSA with respect to low decryption exponent, based on modified Coppersmith methods for finding small roots of bivariatate integer polynomial equations due to Howgrave-Graham. In **section 3.1**, we described the method of finding small roots of univariate integer modular equations given by Howgrave-Graham. In **section 3.2, 3.3, 3.4, 3.5** and **3.6**, we described the Boneh and Durfee's attack, Blömer and May's attack, B de Weger attack, Subbhamoy Maitra and Santanu Sarkar's attack and A. Nitaj and M.O. Douh's attack on RSA respectively and noted that these attacks can be extended to RSA-like cryptosystem over elliptic curves $E(\mathbb{Z}_{pq})$ due to KMOV in **section 3.7**.

In **Chapter 4** we mount an attack on RSA when the multiplicative inveres of $p - 1$ or $q - 1$ modulo the public encryption exponent e is small, that is less than or equal to N^δ , for some small δ . In **section 4.1** considering a bivariate polynomial congruence with one of the small inverses as a root and we gave attack bounds for δ , using lattice based techniques in the direction of Boneh- Durfee and Blömer-May for the proposed polynomial congruence. We analyze these bounds with respect to the

prime difference $p - q$ in **section 4.1.1** and with respect to $p - \rho q$, for ρ such that ρq is a better approximation for p in **section 4.1.2** and further in **section 4.2** it is noted that repeating the above arguments the attack may be extended to RSA-like cryptosystem over elliptic curves $E(\mathbb{Z}_{pq})$ due to KMOV.

In **Chapter 5** we mount an attack on RSA when $\varphi(N)$ has small multiplicative inverse k modulo e , the public encryption exponent and with a composed prime sum $p + q$, i.e., $p + q = 2^n k_0 + k_1$ for a known positive integer n for some small suitable unknown integers k_0 and k_1 . In **section 5.1** for $k \leq N^\delta$, we gave attack bounds for δ using lattice based techniques by considering a bivariate polynomial congruence with one of the inverse as a root. In **section 5.2**, we further refined attack bounds for δ for $\beta \approx 0.5$ by taking the prime sum $p + q$ as a composed prime sum i.e., $p + q = 2^n k_0 + k_1$ for a known positive integer n and small suitable unknown integers k_0 and k_1 and applying the lattice based arguments for trivariate polynomials with the multiplicative inverse $\varphi(N)$ modulo e as one root. Also we provide a new attack bound for the deciphering exponent d when the prime sum $p + q = 2^n k_0 + k_1$ and analyzed with Boneh and Durfee's deciphering exponent bound for appropriately small k_0 and k_1 . In **section 5.3** it is noted that these lattice-based attacks on RSA can be extended to RSA-like cryptosystem over elliptic curves $E(\mathbb{Z}_{pq})$ due to KMOV.

All the computations regarding, LLL-algorithm for lattice reduction, resultant of polynomials, prime number generations, plotting of graphs are done using the SAGE-7.0.ova software.

Chapter 1

Preliminaries

This chapter contains basic concepts of cryptography, RSA, security of RSA, continued fractions, lattices, lattice basis reduction and theorems based on lattice reduction techniques that are employed throughout the book [2][6][8][12][14][26][29]. Some basic concepts of modular arithmetic and KMOV-Public key cryptosystem over elliptic curves are included in Appendix A and B respectively.

1.1 Cryptography

Cryptography is a study of methods of sending messages in disguised form. The message that is to be sent is called **plaintext message** and the message received in disguised form is called **ciphertext message**. The process of converting a plaintext to a ciphertext is **enciphering**. The process of converting a ciphertext to a plaintext is **deciphering** [26].

Enciphering and Deciphering Transformations:

Let \mathcal{P} be the set of all possible plaintext message units and \mathcal{C} be the set of all possible ciphertext message units. Let k be a parameter, then the function $E_k : \mathcal{P} \rightarrow \mathcal{C}$ which is 1-1 and onto, is called enciphering transformation and the function

$D_k : \mathcal{C} \rightarrow \mathcal{P}$ is called deciphering transformation [6][26].

The enciphering transformation may be constructed by labeling the message units with mathematical objects like integers, vectors, points on curve etc.

Definition 1.1.1. A **cryptosystem** is a tuple $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ where

1. \mathcal{P} is a finite set of possible plaintexts.
2. \mathcal{C} is a finite set of possible ciphertexts.
3. \mathcal{K} , the key space is a finite set of possible keys.
4. $\mathcal{E} = \{E_k/k \in \mathcal{K}\}$ is a family of functions $E_k : \mathcal{P} \rightarrow \mathcal{C}$. Its elements are called enciphering transformations.
5. $\mathcal{D} = \{D_k/k \in \mathcal{K}\}$ is a family of functions $D_k : \mathcal{C} \rightarrow \mathcal{P}$. Its elements are called deciphering transformations.
6. For each $e \in \mathcal{K}$, there is $d \in \mathcal{K}$ such that $D_d(E_e(p)) = p$, for all $p \in \mathcal{P}$ [2].

1.1.1 Classical and Public Key Cryptosystems

Classical Cryptosystem:

The sender communicates the secret key to the intended recipient over a secured channel before the message being interchanged. When the sender and recipient agree upon the secret key, they communicate with each other. This type of cryptosystem is called **classical cryptosystem** [2][41][45].

In this classical cryptosystem the enciphering key is always equal to the deciphering key or computing deciphering key is feasible.

Public Key Cryptosystem:

Maintaining the secrecy of enciphering key in the classical cryptosystem for a long time seemed to be difficult, hence the search for cryptosystems where the enciphering key may be made public, but computing the deciphering key is infeasible has gained importance.

With the advent of existence of one-way functions, cryptosystems whose transformations are one way functions were first introduced by W. Diffie and M. Hellman in 1976 and are called as public key cryptosystems [2][11][26].

1.1.2 Cryptanalysis

Definition 1.1.2. The science of breaking a cryptosystem is called **cryptanalysis**.

Cryptanalysis is a means to assure that a cryptosystem is secure. The philosophy of modern cryptanalysis is based on the **Kerchoff's principle** [2], "The security of cryptosystem must not depend on keeping the cryptoalgorithm secret rather it should depend only on keeping the key secret".

1.1.3 RSA Cryptosystem

The RSA cryptosystem [26] [41] is the first public key cryptosystem invented by Ronald **R**ivest, Adi **S**hamir and Leonard **A**dleman in 1977 and is named after them as RSA cryptosystem. The security of this system is based on the difficulty of finding factors of a composite positive integer, that is the product of two large primes.

Key generation in RSA cryptosystem:

Let **A** and **B** be two parties wishing to communicate each other. **B** generates the public and private keys as follows:

- **B** generates randomly two large primes p and q .
- Computes the product $N = pq$.
- Choose a random integer $e \in \mathbb{Z}_{\varphi(N)}^*$ with $1 < e < \varphi(N)$ such that $\gcd(e, \varphi(N)) = 1$, where $\varphi(N)$ is the Euler function [1][7] of N ,
i.e., $\varphi(N) = \varphi(pq) = (p - 1)(q - 1)$.
- **B** computes the integer $d \in \mathbb{Z}_{\varphi(N)}^*$ with $1 < d < \varphi(N)$ such that $de \equiv 1 \pmod{\varphi(N)}$, i.e., d is the multiplicative inverse of e in $\mathbb{Z}_{\varphi(N)}^*$.
- N is called the RSA modulus, e is called the encryption exponent, and d is called the decryption exponent.
- The pair (N, e) is the public key and d is the private key for **B**.

RSA encryption:

- **A** considers the public key (N, e) of **B**.
- The message m to be encrypted is taken modulo N , i.e., $m \in \mathbb{Z}_N$.
- The plaintext m is encrypted by **A** into the ciphertext c as $c = m^e \pmod{N}$.

RSA decryption:

- **B** considers the ciphertext c received from **A**.
- **B** decrypts c and obtains plaintext m by computing $c^d = m \pmod{N}$.

The decryption is based on the following theorem:

Theorem 1.1.3. Let $N = pq$, p and q are distinct primes and $1 \leq e \leq \varphi(N)$ with $(e, \varphi(N)) = 1$. If d is a multiplicative inverse of e modulo $\varphi(N)$, then $m^{ed} \equiv m \pmod{N}$, for any integer $m \in \mathbb{Z}_N$ [21].

1.1.4 Security of the Secret Key and Factoring Algorithms

The security of RSA cryptosystem based on the secret key d . Computing the secret key d is feasible with the knowledge of $\varphi(N) = (p-1)(q-1)$, for p, q are the prime factors of N and d is the multiplicative inverse of e modulo $\varphi(N)$ which is possible when the factors p, q of N are known.

Hence forth, to break the RSA cryptosystem, there are several factorization techniques developed. Some of the factoring algorithms are given below [2][6][41].

Factoring Algorithms:

Trial Division:

This factorization method based on the fact that composite number N have at least one prime factor $\leq \sqrt{N}$. For finding a factor N , compute $N = aq + r$ for each $a = 2, 3, 5, 7, 9 \dots$, an odd number which is less than or equal to \sqrt{N} . This takes approximately $\frac{1}{2}\sqrt{N}$ divisions with remainders. Thus, the time required to compute this algorithm is $O(N^{\frac{1}{2}})$.

Fermat Factorization:

For $N = pq$, this is a sequential method in which factorization of N is determined by the solution (x, y) of the diophantine equation $x^2 - y^2 = 4N$.

Algorithm of Fermat Factorization Attack:

Step 1: Find positive integers (x, y) a nontrivial solution of a diophantine equation

$$4N = x^2 - y^2.$$

Step 2: Compute for $x = [2N^{\frac{1}{2}}], [2N^{\frac{1}{2}}] + 1, [2N^{\frac{1}{2}}] + 2, \dots$, the value $x^2 - 4N$ until

$x^2 - 4N$ is a square.

Step 3: For x and y in step 2, compute $p = \frac{1}{2}(x + y)$ and $q = \frac{1}{2}(x - y)$, which gives the factors of N as $N = pq$.

It can be proved that when $|p - q| < cN^{\frac{1}{4}}$, the number of values of x that have to be tried is at most $\frac{c^2}{4}$. Therefore, when c is small constant, factoring N is trivial.

The Polard $(p - 1)$ Algorithm:

The $(p - 1)$ method works best for composite integer N with a prime factor p such that $p - 1$ has only small prime divisors.

The algorithm proceeds as follows:

Step 1: Choose an integer k which is a multiple of all or most integers up to some bound B , i.e., $k = B!$ or $k = \text{lcm}[1, 2, \dots, [B]]$.

Step 2: Choose a random integer ‘ a ’ such that $2 < a < n - 2$.

Step 3: Compute $a^k \pmod N$ by the repeated squaring method.

Step 4: Compute $\text{gcd}(a^k - 1, N) = d$.

Step 5: If d is not a trivial division of N , start over with a new choice of ‘ a ’ and/or a new choice of k .

Since k is divisible by all positive integers $\leq B$ and if p is a prime divisor of N such that $p - 1$ has divisors of all small prime powers $\leq B$, then k is a multiple of $p - 1$. Therefore by using Fermat’s little theorem, $a^k \equiv 1 \pmod p$, for all integers ‘ a ’ that are not divisible by p , i.e., $p \mid a^k - 1$.

If $a^k - 1$ is not divisible by N , then $\gcd(a^k - 1, N)$, is a proper divisor of N .

Pollard's rho Method of Factoring:

The smallest algorithm for factoring N , that is substantially faster than trial division is Pollard's rho method. Then algorithm proceeds as follows:

Step 1: Choose an easily evaluated map $f : \mathbb{Z}_N \rightarrow \mathbb{Z}_N$ such that $f(x) = x^2 + 1 \pmod N$, a fairly simple polynomial with integer coefficients.

Step 2: Choose some partial value of x , say $x = x_0$ and compute $f(x_0)$. Define $x_1 = f(x_0), x_2 = f(f(x_0)), \dots$, i.e., $x_{j+1} = f(x_j)$ for $j = 0, 1, \dots$

step 3: Make comparisons between the different x_j 's, until to find some x_k such that $x_j \equiv x_k \pmod r$ for some proper divisor of N . Then we have $\gcd(x_j - x_k, N)$ equal to a proper divisor of N .

As k becomes large, it is very time consuming, as it needs to compute $\gcd(x_j - x_k, N)$ for each $j < k$. It is observed that there we may carry out the algorithm by making out one gcd computation for each $k, k = 0, 1, 2, \dots$

If k is an $(h + 1)$ bit integer, i.e., $2^h \leq k < 2^{h+1}$, take j be the largest h bit-integer given as $j = 2^h - 1$ then compute $\gcd(x_j - x_k, n) \forall k = 0, 1, 2, \dots$

The Quadratic Sieve Method:

The Quadratic sieve was invented by Carl Pomerance in 1981, extending earlier ideas of Kraitchik and Dixon. The Quadratic Sieve was the fastest known factoring algorithm until the number field sieve was discovered in 1993. Still the Quadratic Sieve is used for numbers up to 110 digits long.

This method works as follows:

If N is the number to be factored, the Quadratic Sieve attempts to find two numbers x and y such that $x \not\equiv \pm y \pmod{N}$ and $x^2 \equiv y^2 \pmod{N}$, then using $(x - y)(x + y) \equiv 0 \pmod{N}$ and compute $\gcd(x - y, N)$ by Euclidean algorithm.

If $\gcd(x - y, N) = d$ and $1 < d < N$, we get a non-trivial factor of N .

Now to find such x and y , consider the polynomial $f(x) = (x + [\sqrt{N}])^2 - N$, then $f(x) \in \mathbb{Z}[x]$ and of degree 2.

If x is an integer, then $(x + [\sqrt{N}])^2 \equiv f(x) \pmod{N}$, where the congruence is not trivial.

Now we proceed to find a set of distinct integers x_1, x_2, \dots, x_k such that $f(x_1) \cdot f(x_2) \cdot \dots \cdot f(x_k)$ is a square, i.e, $f(x_1) \cdot f(x_2) \cdot \dots \cdot f(x_k) = y^2$.

Now taking $x = (x_1 + [\sqrt{N}])(x_2 + [\sqrt{N}]) \dots (x_k + [\sqrt{N}])$, we have

$$\begin{aligned} x^2 &= (x_1 + [\sqrt{N}])^2(x_2 + [\sqrt{N}])^2 \dots (x_k + [\sqrt{N}])^2 \\ &\equiv f(x_1) \cdot f(x_2) \cdot \dots \cdot f(x_k) \\ &\equiv y^2 \pmod{N} \end{aligned}$$

It is infeasible to compute the secret key d from the public key (N, e) whenever that $N = pq$ is large enough that factoring is computationally infeasible by the existing factorization algorithms. But there are other attacks like Wiener's attack which uses an alternate method in computing the secret key d . In the next section we discuss the topic of continued fraction on which the wiener's attack and its extensions are based on.

1.2 Continued Fractions

This section introduces the basic concepts of continued fractions [7][10] and also describes the use of theory of continued fractions to give the best rational approximation to real numbers.

1.2.1 Finite Continued Fractions

Definition 1.2.1. A rational number $q \in \mathbb{Q}$ is said to have a **finite continued fraction** [24] if q can be expressed as

$$q = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\ddots + \frac{1}{a_n}}}}$$

for $a_0 \in \mathbb{Z}$, $a_i \in \mathbb{N} \forall i > 0$ called partial quotients and the continued fraction for q is denoted as $q = [a_0; a_1, \dots, a_n]$.

Theorem 1.2.2. Every rational number has a finite continued fraction and conversely every finite continued fraction is a rational number.

1.2.2 Convergents of Finite Continued Fractions

Definition 1.2.3. Let q be a rational number with the continued fraction $q = [a_0; a_1, \dots, a_n]$, then the continued fraction $[a_0; a_1, \dots, a_i]$ is called the i^{th} **convergent of q** for all $0 \leq i \leq n$.

Remark 1.2.4. Let q be a rational number and q_i be the partial quotients, then we have the following recurrence relations [36]

$$h_i = a_i h_{i-1} + h_{i-2},$$

$$k_i = a_i k_{i-1} + k_{i-2}, \text{ for } h_{-1} = 1, k_{-1} = 0, h_{-2} = 0 \text{ and } k_{-2} = 1.$$

Lemma 1.2.5. Given that $[a_0; a_1, \dots, a_i]$ is the i^{th} convergent of q , then $[a_0; a_1, \dots, a_i + \frac{1}{a_{i+1}}]$ is the $(i+1)^{\text{st}}$ convergent of q .

Theorem 1.2.6. Suppose $q \in \mathbb{Q}$ has the continued fraction $[a_0; a_1, \dots, a_n]$. Then $C_i = \frac{h_i}{k_i}$ is the i^{th} convergent of q for all $0 \leq i \leq n$, where

$$h_i = a_i h_{i-1} + h_{i-2},$$

$$k_i = a_i k_{i-1} + k_{i-2}, \text{ with } h_{-1} = 1, k_{-1} = 0, h_{-2} = 0 \text{ and } k_{-2} = 1.$$

Notation:

Suppose $q = [a_0; a_1, \dots, a_n]$, we define q_i as $q_i = [a_i; a_{i+1}, \dots, a_n]$ for $0 \leq i \leq n$.

Lemma 1.2.7. For any continued fraction $q = [a_0; a_1, \dots, a_n]$, $q = \frac{q_i h_{i-1} + h_{i-2}}{q_i k_{i-1} + k_{i-2}}$, $0 \leq i \leq n$.

Since Convergents of a continued fractions play a fundamental role in approximations to real numbers, so we now state some lemmas concerning the central properties of convergents.

Lemma 1.2.8. The sequence $\{k_1, k_2, \dots, k_n\}$ is strictly increasing.

Lemma 1.2.9. Let $C_i = \frac{h_i}{k_i}$ be the i^{th} convergent of a continued fraction $[a_0; a_1, \dots, a_n]$. Then $h_i k_{i-1} - h_{i-1} k_i = (-1)^{i-1}$ for $i \geq 1$.

Corollary 1.2.10. Let $C_i = \frac{h_i}{k_i}$ be the i^{th} convergent of a continued fraction $[a_0; a_1, \dots, a_n]$, then for $i \geq 0$, $\gcd(h_i, k_i) = 1$.

Lemma 1.2.11. The sequence of convergents $\{C_0, C_1, \dots, C_n\}$ of a continued fraction $[a_0; a_1 \dots a_n]$ satisfy the following infinite chain of inequalities

$$C_0 < C_2 < \dots < C_n < C_{n-1} < C_{n-3} < \dots < C_3 < C_1 \text{ if } n \text{ is even.}$$

$$C_0 < C_2 < \dots < C_{n-1} < C_n < C_{n-2} < \dots < C_3 < C_1 \text{ if } n \text{ is odd.}$$

Further, $r = \lim_{n \rightarrow \infty} C_n$ exists and for every $j \geq 0$, $C_{2j} < \lim_{n \rightarrow \infty} C_n < C_{2j+1}$.

1.2.3 Infinite Continued Fractions

Definition 1.2.12. An irrational number S is said to have an **infinite continued fraction** [13] if $S = \lim_{n \rightarrow \infty} [a_0; a_1, \dots, a_n]$, for $a_0 \in \mathbb{Z}, a_i \in \mathbb{N} \forall i > 0$ and it can be expressed as

$$q = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\ddots + \frac{1}{a_n + \dots}}}} = [a_0; a_1, \dots, a_n, \dots]$$

Theorem 1.2.13. Every irrational number has an infinite continued fraction and conversely every infinite continued fraction is an irrational number.

Now in the following, we proceed to give the theorem on best rational approximation to a real number using the continued fraction.

Lemma 1.2.14. Let $C_n = \frac{h_n}{k_n}$ be the n^{th} convergent of a real number r . If a and b are integers with $1 \leq b < k_{n+1}$, then $|rk_n - h_n| \leq |rb - a|$.

Theorem 1.2.15. Let $C_n = \frac{h_n}{k_n}$ be the n^{th} convergent of a real number r . Then for any $a, b \in \mathbb{Z}$, $1 \leq b \leq k_n$,

$$\left| r - \frac{h_n}{k_n} \right| \leq \left| r - \frac{a}{b} \right|.$$

The main theory of rational approximations to real number is contained in the following theorem, which plays a vital role in attacking RSA cryptosystem.

Theorem 1.2.16. Let r be a real number. For any integers a and b with $\gcd(a, b) = 1$ such that $\left| r - \frac{a}{b} \right| < \frac{1}{2b^2}$, $b \geq 1$, then $\frac{a}{b}$ is a convergent of r .

1.3 Lattice Reduction

In this section we state few basic results on lattices, describe briefly lattice basis reduction [14][29]. Also describe Coppersmith's theorems and Howgrave-Graham Lemma that are based on lattice reduction techniques [8][12].

Definition 1.3.1. Let $b_1, b_2, \dots, b_n \in \mathbb{R}^m$ be a set of linearly independent vectors. The **lattice L generated** by b_1, b_2, \dots, b_n is the set of linear combinations of b_1, b_2, \dots, b_n with coefficients in \mathbb{Z} .

A **basis** for L is any set of independent vectors that generates L . The **dimension** of L is the number of vectors in a basis for L .

Remark 1.3.2. If L is a full rank lattice, means $n = m$ then the determinant of L is equal to the determinant of the $n \times n$ matrix whose rows are the basis vectors b_1, b_2, \dots, b_n .

Theorem 1.3.3. Any two bases for a lattice L are related by a matrix having integer coefficients and determinant equal to ± 1 .

Definition 1.3.4. Any **integral** (or **integer**) **lattice** is a lattice all of whose vectors have integer coordinates. Equivalently, an integral lattice is an additive subgroup of \mathbb{Z}^m for some $m \geq 1$.

Definition 1.3.5. A subset L of \mathbb{R}^m is an **additive subgroup** if it is closed under addition and subtraction. It is called a **discrete additive subgroup** if there is a positive constant $\epsilon > 0$ with the following property: for every $b' \in L$,

$$L \cap \{b \in \mathbb{R}^m : \|b' - b\| < \epsilon\} = \{b'\}$$

where $\| \cdot \|$ denotes the Euclidean norm on vectors.

Theorem 1.3.6. A subset of \mathbb{R}^m is a lattice if and only if it is a discrete additive subgroup.

Definition 1.3.7. Let L be a lattice of dimension n and let b_1, b_2, \dots, b_n be a basis for L . The **fundamental domain** (or **fundamental parallelepiped**) for L corresponding to this basis is the set

$$\mathcal{F}(b_1, b_2, \dots, b_n) = \{t_1 b_1 + t_2 b_2 + \dots + t_n b_n : 0 \leq t_i < 1\}.$$

Theorem 1.3.8. Let $L \subset \mathbb{R}^n$ be a lattice of dimension n and let \mathcal{F} be a fundamental domain for L . Then every vector $b \in \mathbb{R}^n$ can be written in the form $b = t + b'$ for a unique $t \in \mathcal{F}$ and a unique $b' \in L$.

Equivalently, the union of the translated fundamental domains

$$\mathcal{F} + b' = \{t + b' : t \in \mathcal{F}\}.$$

as b' ranges over the vectors in the lattice L exactly covers \mathbb{R}^n .

Definition 1.3.9. Let L be a lattice of dimension n and let \mathcal{F} be a fundamental domain for L . Then the n -dimensional volume of \mathcal{F} is called the **determinant of L** . It is denoted by $\det(L)$.

Definition 1.3.10. An **orthogonal basis** for a vector space V is a basis $\{b_1, b_2, \dots, b_n\}$ with the property that

$$b_i \cdot b_j = 0 \text{ for all } i \neq j.$$

The basis is **orthonormal** if in addition, $\|b_i\| = 1$ for all i .

If $V \subset \mathbb{R}^m$ is a vector space of dimension n , then for any basis b_1, b_2, \dots, b_n of V , the standard method by Gram-Schmidt is used to obtain an orthogonal basis $b_1^*, b_2^*, \dots, b_n^*$ for V is given in the following algorithm:

Set $b_1^* = b_1$.

Loop $i = 2, 3, \dots, n$.

Compute $\mu_{ij} = b_i \cdot b_j^* / \|b_j^*\|^2$ for $1 \leq j < i$.

Set $b_i^* = b_i - \sum_{j=1}^{i-1} \mu_{ij} b_j^*$.

End Loop

Figure 1.1: Gram-Schmidt Algorithm.

Theorem 1.3.11. Let $\mathcal{B} = \{b_1, b_2, \dots, b_n\}$ be a basis for a lattice L and let $\mathcal{B}^* = \{b_1^*, b_2^*, \dots, b_n^*\}$ be the associated Gram-Schmidt orthogonal basis. Then

$$\det(L) := \prod_{i=1}^n \|b_i^*\|.$$

Remark 1.3.12. The basic vectors b_1, \dots, b_n as being vectors of a given length that describe the sides of the parallelepiped \mathcal{F} , then for basis vectors of given lengths, the largest volume is obtained when the vectors are pairwise orthogonal to one another.

Theorem 1.3.13. (Hadamard's Inequality). Let L be a lattice, take any basis b_1, \dots, b_n for L , and let \mathcal{F} be a fundamental domain for L . Then

$$\det L = \text{Vol}(\mathcal{F}) \leq \|b_1\| \|b_2\| \cdots \|b_n\|.$$

1.3.1 Short Vectors in Lattices

The Shortest Vector Problem(SVP): Find a shortest nonzero vector in a lattice L , i.e., find a nonzero vector $b \in L$ that minimizes the Euclidean norm $\|b\|$.

Shortest Basis Problem(SBP): Find a basis b_1, \dots, b_n for a lattice that is shortest in some sense. For example, we might require that

$$\max_{1 \leq i \leq n} \|b_i\| \text{ or } \sum_{i=1}^n \|b_i\|^2$$

be minimized. There are thus many different versions of SBP, depending on how one decides to measure the "size" of a basis.

Theorem 1.3.14. (Hermite's Theorem). Every lattice L of dimension n contains

a nonzero vector $b \in L$ satisfying

$$\|b\| \leq \sqrt{n} \det(L)^{\frac{1}{n}}.$$

Remark 1.3.15. For a given dimension n , Hermite's constant γ_n is the smallest value such that every lattice L of dimension n contains a nonzero vector $b \in L$ satisfying

$$\|b\|^2 \leq \gamma_n \det(L)^{\frac{2}{n}}.$$

Remark 1.3.16. There are versions of Hermite's theorem that deal with more than one vector. For example, one can prove that an n -dimensional lattice L always has a basis b_1, \dots, b_n satisfying

$$\|b_1\| \|b_2\| \cdots \|b_n\| \leq n^{\frac{n}{2}} (\det L).$$

Definition 1.3.17. The **Hadamard ratio** of the basis $\mathcal{B} = \{b_1, \dots, b_n\}$ is defined to be the quantity

$$\mathcal{H}(\mathcal{B}) = \left(\frac{\det L}{\|b_1\| \cdots \|b_n\|} \right)^{\frac{1}{n}}.$$

Remark 1.3.18. The Hadamard ratio $\mathcal{H}(\mathcal{B})$ satisfies $0 < \mathcal{H}(\mathcal{B}) \leq 1$, and the closer that the value is to 1, the more orthogonal are the vectors in the basis.

Definition 1.3.19. For any $a \in \mathbb{R}^n$ and any $R > 0$, the **(closed) ball of radius R** centered at a is the set

$$\mathbb{B}_R(a) = \{x \in \mathbb{R}^n : \|x - a\| \leq R\}.$$

Definition 1.3.20. Let S be a subset of \mathbb{R}^n .

- (a) S is **bounded** if the lengths of the vectors in S are bounded. Equivalently, S is bounded if there is a radius R such that S is contained within the ball $\mathbb{B}_R(0)$.
- (b) S is **symmetric** if for every point a in S , the negation $-a$ is also in S .
- (c) S is **convex** if whenever two points a and b are in S , then the entire line segment connecting a and b lies completely in S .
- (d) S is **closed** if it has the following property: If $a \in \mathbb{R}^n$ is a point such that every ball $\mathbb{B}_R(a)$ contains a point of S , then a is in S .

Theorem 1.3.21. (Minkowski's Theorem). Let $L \subset \mathbb{R}^n$ be a lattice of dimension n and let $S \subset \mathbb{R}^n$ be a symmetric convex set whose volume satisfies

$$\text{Vol}(S) > 2^n \det(L).$$

Then S contains a nonzero lattice vector.

If S is also closed, then it suffices to take $\text{Vol}(S) \geq 2^n \det(L)$.

1.3.2 LLL Algorithm

The Lenstra-Lenstra-Lovász (LLL) algorithm is an iterative algorithm that transforms a given lattice basis into an LLL-reduced one and also solves SVP (Shortest Vector Problem) up to a factor of C^n , where C is a small constant and n is the dimension of the lattice. Thus, the LLL algorithm comes close to solve SVP in small dimensions but is not guaranteed to output a shortest vector in large dimensions.

Using the set $\{b_1^*, b_2^*, \dots, b_n^*\}$ of associated Gram-Schmidt vectors, LLL reduced basis is defined as follows:

Definition 1.3.22. Let $\mathcal{B} = \{b_1, b_2, \dots, b_n\}$ be a basis for a lattice L and let $\mathcal{B}^* = \{b_1^*, b_2^*, \dots, b_n^*\}$ be the associated Gram - Schmidt orthogonal basis. The basis \mathcal{B} is said to be **LLL reduced** if the following conditions hold:

- (Size Condition) $|\mu_{i,j}| = \frac{|b_i \cdot b_j^*|}{\|b_j^*\|^2} \leq \frac{1}{2}$ for all $1 \leq j < i \leq n$.
- (Lovász Condition) $\|b_i^*\|^2 \geq \left(\frac{3}{4} - \mu_{i,i-1}^2\right) \|b_{i-1}^*\|^2$ for all $1 < i \leq n$.

The LLL reduction algorithm is given as follows:

INPUT: A basis $\{b_1, b_2, \dots, b_n\}$ for a lattice L .

OUTPUT: LLL reduced basis $\{b_1, b_2, \dots, b_n\}$

1. Compute the Gram-Schmidt basis $\{b_1^*, b_2^*, \dots, b_n^*\}$ and coefficients $\mu_{i,j}$ for $1 \leq j < i \leq n$
2. Set $k = 2$
3. while $k \leq n$ do
4. for $j = (k - 1)$ down to 1 do
5. Set $b_k = b_k - \lfloor \mu_{k,j} \rfloor b_j^*$ [Size reduction]
6. Update the values $\mu_{k,j}$ for $1 \leq j < k$
7. end for
8. if $\|b_k^*\|^2 \geq \left(\frac{3}{4} - \mu_{k,k-1}^2\right) \|b_{k-1}^*\|^2$ then [Lovász Condition]
9. $k = k + 1$
10. else
11. Swap b_k with b_{k-1}
12. Update the values $b_k^*, b_{k-1}^*, \|b_k^*\|^2, \|b_{k-1}^*\|^2, \mu_{k-1,j}$ and $\mu_{k,j}$ for $1 \leq j < k$,
 and $\mu_{i,k}, \mu_{i,k-1}$ for $k < i \leq n$
13. end if
14. end while

Figure 1.2: The LLL lattice reduction algorithm.

Properties of LLL Algorithm:

Let L be a lattice spanned by $\langle u_1, u_2, \dots, u_n \rangle$. Then the LLL (Lenstra-Lenstra-Lovász) algorithm, given $\langle u_1, u_2, \dots, u_n \rangle$, runs in polynomial time and produces a new basis $\langle b_1, b_2, \dots, b_n \rangle$ of L satisfying:

1. $\|b_i^*\|^2 \leq 2 \|b_{i+1}^*\|^2$, for all $1 \leq i < n$.
2. For all i , if $b_i = b_i^* + \sum_{j=1}^{i-1} \mu_j b_j^*$ then $|\mu_j| \leq \frac{1}{2}$ for all j .

Theorem 1.3.23. Let L be a lattice and b_1, b_2, \dots, b_n be an LLL-reduction basis of L . Then $\|b_1\| \leq 2^{n/2} \det(L)^{1/n}$.

Theorem 1.3.24. Let L be a lattice spanned by $\langle u_1, u_2, \dots, u_n \rangle$ and let $\langle b_1, b_2, \dots, b_n \rangle$ be the result of applying LLL to the given basis. Suppose $u_{min}^* \geq 1$ where u_{min}^* is a lower bound on the length of the shortest vector in L . Then $\|b_2\| \leq 2^{n/2} \det(L)^{\frac{1}{n-1}}$.

In the following theorem, we state a general result on the size of the individual reduced basis vectors.

Theorem 1.3.25. Let L be a lattice and b_1, b_2, \dots, b_n be an LLL-reduction basis of L . Then $\|b_1\| \leq \|b_2\| \leq \dots \leq \|b_i\| \leq 2^{\frac{n(n-1)}{4(n+1-i)}} \det(L)^{\frac{1}{n+1-i}}$ for all $1 \leq i \leq n$.

Complexity of LLL Algorithm:

In paper [29], Lenstra, Lenstra and Lovász proves that the LLL algorithm terminates and runs in polynomial-time for any lattice in \mathbb{R}^n but only gives a precise complexity for lattices in \mathbb{Z}^n and is given in the following theorem.

Theorem 1.3.26. Let $\{b_1, b_2, \dots, b_n\}$ be a basis for a lattice L . The algorithm described in Figure 1.1 terminates in a finite number of steps and returns an LLL

reduced basis for L .

More precisely, let $\mathbf{B} = \max \|b_i\|$. Then the algorithm executes the main k loop (Steps 3-14) no more than $\mathcal{O}(n^2 \log n + n^2 \log B)$ times. In particular, the LLL algorithm is a polynomial-time algorithm.

1.3.3 Howgrave-Graham Results

An important application of lattice reduction found by Coppersmith in 1996 [8] is finding small roots of low-degree polynomial equations. This includes modular univariate polynomial equations and bivariate integer equations. Coppersmith methods initiated the study of RSA attacks with lattice basis reduction techniques. Howgrave-Graham modified the Coppersmith methods by using this theory on modular solutions to integer solutions. In this section we state the theorems on Coppersmith methods and state the theorems of Howgrave-Graham on modular solutions to integer solutions.

In the following theorem Coppersmith states that the problem of finding small roots is easy by using the LLL lattice reduction algorithm.

Theorem 1.3.27. Given a monic polynomial $P(x)$ of degree δ , modulo an integer N of unknown factorization, one can find in time polynomial in $(\log N, 2^\delta)$ all integers x_0 such that $P(x_0) = 0 \pmod{N}$ and $|x_0| \leq N^{1/\delta}$ [8].

Similarly, the problem of solving bivariate integer polynomial equations seems to be hard. Letting $p(x, y)$ be a polynomial in two variables with integer coefficients, $p(x, y) = \sum_{i,j} p_{i,j} x^i y^j$ it consists in finding all integer pairs (x_0, y_0) such that $p(x_0, y_0) = 0$. We see that integer factorization is a special case as one can take $p(x, y) = N - xy$. In the following theorem Coppersmith [8] shows that using LLL,

the problem of finding small roots of bivariate polynomial equations is easy:

Theorem 1.3.28. Let $p(x, y)$ be an irreducible polynomial in two variables over \mathbb{Z} , of maximum degree δ in each variable separately. Let X and Y be upper bounds on the desired integer solution (x_0, y_0) , and let $W = \max_{i,j} |p_{ij}| X^i Y^j$. If $XY < W^{2/(3\delta)}$, then in time polynomial in $(\log W, 2^\delta)$, one can find all integer pairs (x_0, y_0) such that $p(x_0, y_0) = 0$, $|x_0| \leq X$, and $|y_0| \leq Y$.

An alternative techniques for finding small roots of univariate modular equations given by Howgrave-Graham in [12]. The following lemma, due to Howgrave-Graham, shows that if the roots of a univariate modular equation $h(x) = 0 \pmod{N}$ are sufficiently small, then the equality $h(x_0) = 0$ holds not only modulo N , but also over \mathbb{Z} for any such small root $x = x_0$.

Lemma 1.3.29. Let $h(x) \in \mathbb{Z}[x]$ which is a sum of at most ω monomials. Suppose that $h(x_0) = 0 \pmod{N}$ where $|x_0| \leq X$ and $\|h(xX)\| < N/\sqrt{\omega}$. Then $h(x_0) = 0$ holds over the integers [17].

Lemma 1.3.30. (Generalized Howgrave-Graham's Lemma). Let $h(x_1, \dots, x_n) \in \mathbb{Z}[x_1, \dots, x_n]$ be an integer polynomial that consists of at most ω monomials. Suppose that

1. $h(x_1^{(0)}, \dots, x_n^{(0)}) = 0 \pmod{N}$ for some $|x_1^{(0)}| < X_1, \dots, |x_n^{(0)}| < X_n$, and
2. $\|h(x_1 X_1, \dots, x_n X_n)\| < \frac{N}{\sqrt{\omega}}$.

Then $h(x_1^{(0)}, \dots, x_n^{(0)}) = 0$ holds over the integers [17].

Howgrave-Graham modified the Coppersmith methods by using the above two results and this modification is reviewed in chapter 3. The generalization of Coppersmith and Howgrave-Graham methods to multivariate polynomials depends on

the concept of resultant of two polynomials, in the following we define resultant and some remarks on resultant.

1.3.4 Resultant

Definition 1.3.31. Given polynomials f and g of positive degree, write them in the form

$$\begin{aligned} f &= a_0x^l + \dots + a_l, a_0 \neq 0 \\ g &= b_0x^m + \dots + b_m, b_0 \neq 0 \end{aligned}$$

Then the **Sylvester matrix** of f and g with respect to x , denoted by $\text{Syl}(f, g, x)$, is the coefficient matrix of the system of equations given above. Thus $\text{Syl}(f, g, x)$ is the following $(l+m)(l+m)$ matrix:

$$\text{Syl}(f, g, x) = \begin{pmatrix} a_0 & 0 & \dots & 0 & b_0 & 0 & \dots & 0 \\ a_1 & a_0 & \ddots & \vdots & b_1 & b_0 & \ddots & \vdots \\ a_2 & a_1 & \ddots & 0 & b_2 & b_1 & \ddots & 0 \\ \vdots & & \ddots & a_0 & \vdots & & \ddots & b_0 \\ & \vdots & & a_1 & & \dots & & b_1 \\ a_{l-1} & & & & b_{m-1} & & & \\ a_l & a_{l-1} & & \vdots & b_m & b_{m-1} & & \vdots \\ 0 & a_l & \ddots & & 0 & b_m & \ddots & \\ \vdots & \ddots & \ddots & a_{l-1} & \vdots & \ddots & \ddots & b_{m-1} \\ 0 & \dots & 0 & a_l & 0 & \dots & 0 & b_m \end{pmatrix}$$

Definition 1.3.32. The **resultant** of two polynomials $f(x_1, x_2, \dots, x_n)$ and $g(x_1, x_2, \dots, x_n)$ with respect to the variable x_i for some $1 \leq i \leq n$, is defined as

the determinant of Sylvester matrix of $f(x_1, x_2, \dots, x_n)$ and $g(x_1, x_2, \dots, x_n)$ when considered as polynomials in the single indeterminate x_i , for some $1 \leq i \leq n$.

Remark 1.3.33. The resultant of two polynomials is non-zero if and only if the polynomials are algebraically independent .

Remark 1.3.34. If $(x_1^{(0)}, x_2^{(0)}, \dots, x_n^{(0)})$ is a common solution of algebraically independent polynomials f_1, f_2, \dots, f_m for $m \geq n$, then these polynomials yield g_1, g_2, \dots, g_{n-1} resultants in $n - 1$ variables and continuing so on the resultants yield a polynomial $t(x_i)$ in one variable with $x_i = x_i^{(0)}$ for some i is a solution of $t(x_i)$. Note the polynomials considered to compute resultants are always assumed to be algebraically independent.

Geometrically progressive matrices is used in the improvement of attack bounds, we define the geometrically progressive matrices and state a theorem on geometrically progressive matrices in the following.

1.3.5 Geometrically Progressive Matrices

Now we describe the definition of geometrically progressive matrices in the following.

Definition 1.3.35. Let M be an $(a+1)b \times (a+1)b$ matrix. The pair (i, j) corresponds to $(bi + j)^{th}$ column of M . Similarly a pair (k, l) can be used to index $(bk + l)^{th}$ row of M . Let $C, D, c_0, c_1, c_2, c_3, c_4, \beta$ be real numbers with $C, D, \beta \geq 1$. A matrix M is said to be geometrically progressive with parameters $(C, D, c_0, c_1, c_2, c_3, c_4, \beta)$ if the following conditions hold for all i, k in $[0, \dots, a]$ and for all j, l in $[1, \dots, b]$:

- i*) $|M(i, j, k, l)| \leq CD^{c_0+c_1i+c_2j+c_3k+c_4l}$,
- ii*) $M(k, l, k, l) = D^{c_0+c_1k+c_2l+c_3k+c_4l}$,

iii) $M(i, j, k, l) = 0$ whenever $i > k$ or $j > l$,

iv) $\beta c_1 + c_3 \geq 0$ and $\beta c_2 + c_4 \geq 0$.

Theorem 1.3.36. Let M be an $(a+1)b \times (a+1)b$ geometrically progressive matrix with parameters $(C, D, c_0, c_1, c_2, c_3, c_4, \beta)$, and let B be a real number. Define

$$S_B = \{(k, l) \in 0, \dots, a \times 1, \dots, b \mid M(k, l, k, l) = B\}$$

and set $w = |S_B|$. If L is the lattice defined by rows $(k, l) \in S_B$ of M , then

$$\det(L) \leq ((a+1)b)^{w/2} (1+C)^{w^2} \prod_{(k,l) \in S_B} M(k, l, k, l).$$

This theorem on geometrically progressive matrices is used in the improvement of attack bounds for RSA with low decryption exponent by Boneh-Durfee.

Chapter 2

Cryptanalysis Based on Continued Fractions, for RSA with Small Deciphering Exponent

In this chapter we first describe Wiener's attack on RSA and describe some of the extensions of Wiener's attack that refine the attack bounds. All the attacks described in this chapter are based on the theory of continued fractions. R.G.E. Pinch in his paper [37] extended the Wiener's attack to RSA-like cryptosystems over elliptic curves and LUC cryptosystem, in this chapter we extended Wiener's attack and Wiener extensions to RSA-like cryptosystem over elliptic curves due to KMOV, by developing certain estimates on $\psi(N) = (p+1)(q+1)$, which is an analogue to $\varphi(N)$ for RSA-like cryptosystem with elliptic curves $E(\mathbb{Z}_{pq})$ due to KMOV.

2.1 Wiener's Attack on RSA Cryptosystem

In this section we describe an attack on RSA due to M.J. Wiener. The main idea of Wiener's attack [48] is that certain restrictions of the decryption exponent d

allow the fraction $\frac{t}{d}$ to be a convergent of $\frac{e}{N}$, where $t = \frac{ed-1}{\varphi(N)}$, which follows by the approximation theorem.

Theorem 2.1.1. (Approximation Theorem): Let r be a real number, for any integer a and b with $\gcd(a, b) = 1$ such that $|r - \frac{a}{b}| < \frac{1}{2b^2}$, $b \geq 1$ then $\frac{a}{b}$ is convergent of r [7][10].

Estimation of $\varphi(N)$ when $q < p < aq$ for some $a \in \mathbb{N}$ given in the following lemma, plays a key role in Wiener's attack.

Lemma 2.1.2. Let $N = pq$, where p and q are odd primes such that $q < p < aq$ for some $a \in \mathbb{N}$. Then

$$N - (a + 1)\sqrt{N} < \varphi(N) < N \text{ [21][24].}$$

Theorem 2.1.3. (Wiener's attack): Let $N = pq$, for $q < p < aq$ be the modulus for RSA, e be the public encryption exponent and d be the decryption exponent. If $d \leq \frac{N^{\frac{1}{4}}}{\sqrt{2(a+1)}}$, then $\frac{t}{d}$ is a convergent of $\frac{e}{N}$, for $t = \frac{ed-1}{\varphi(N)}$ [21][24].

Theorem 2.1.4. (Implementation of Wiener's attack): Let $d \leq \frac{N^{\frac{1}{4}}}{\sqrt{2(a+1)}}$ and for any convergent $\frac{t'}{d'}$ of $\frac{e}{N}$, take $\varphi'(N) = \frac{ed'-1}{t'}$, $x' = \frac{N-\varphi'(N)+1}{2}$ and $y' = \sqrt{x'^2 - N}$. If $x', y' \in \mathbb{N}$, then the private key $(q, p, d) = (x' - y', x' + y', d')$ [21][24].

Remark 2.1.5. Let the bound $\frac{N^{\frac{1}{4}}}{\sqrt{2(a+1)}}$ of d be denoted by $B_d(a)$, for $a \geq 2$ and note $B_d(a)$ decreases as 'a' increases. This is graphically represented in the following figure for a fixed N .

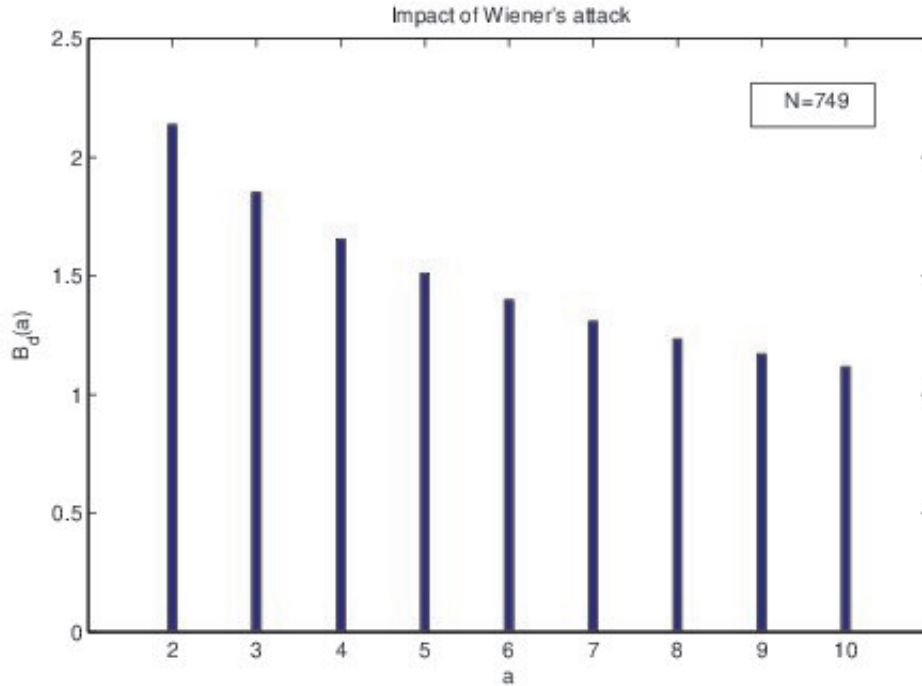


Figure 2.1: Impact of Wiener's attack

Note 2.1.6. As the impact of Wiener's attack is maximum for $a = 2$, in all of the extensions of Wiener's attack in the later sections a is taken to be 2.

Example 2.1.7. Let $(N, e) = (2016991, 1084453)$ be the public key.

The continued fraction of $\frac{e}{N} = [0; 1, 1, 6, 7, 4, 1, 1, 2, 11, 2, 38]$.

The i^{th} convergent of $\frac{e}{N}$ is $\frac{h_i}{k_i} = \frac{a_i h_{i-1} + h_{i-2}}{a_i k_{i-1} + k_{i-2}}$, for $i = 0, 1, 2, \dots, 11$, where $h_{-1} = 1$, $h_{-2} = 0$, $k_{-1} = 0$, $k_{-2} = 1$ and a_i 's are the quotients of $\frac{e}{N}$.

We have $\varphi'(N) = \frac{ed'-1}{t'}$, for each convergent $\frac{t'}{d'}$ of $\frac{e}{N}$. For each convergent $\frac{h_i}{k_i}$, $\varphi'(N) = \frac{ek_i-1}{h_i}$, $x' = \frac{N-\varphi'(N)+1}{2}$ and $y' = \sqrt{(x')^2 - N}$. The first three convergents $\frac{0}{1}$, $\frac{1}{1}$ and $\frac{1}{2}$ fail the Wiener test, since each of $x', y' \notin \mathbb{N}$.

For the next convergent $\frac{7}{13}$, we have

$$\begin{aligned}\varphi'(N) &= \frac{13 \cdot 1084453 - 1}{7} \\ &= 2013984 \text{ and which gives } x' = 1504 \text{ and } y' = 495.\end{aligned}$$

As $x', y' \in \mathbb{N}$, by Wiener's test $\frac{7}{13}$ is the required convergent of $\frac{e}{N}$ with

$$\begin{aligned}(q, p, d) &= (x' - y', x' + y', d') \\ &= (1009, 1999, 13).\end{aligned}$$

As the Wiener's attack fails for the decryption exponent d above the bound $B_d(a)$ of Wiener's attack, the study of weakness of RSA in this direction of the bound $B_d(a)$ and its further extensions gained importance. In the next section we describe the extensions of Wiener's attack for $q < p < 2q$.

2.2 Wieners Extensions on RSA

2.2.1 Wieners Extension on RSA with Small Prime

Difference $p - q$ by B de Weger

In this section we describe the extension of the Wiener's result by B de Weger to the case of small prime difference based on continued fraction algorithm [47].

The following theorem yields an estimate of $\varphi(N)$ that is used for this attack.

Theorem 2.2.1. Estimation of $\varphi(N)$ when $q < p < 2q$ is given by

$$N + 1 - \frac{3}{\sqrt{2}}N^{\frac{1}{2}} < \varphi(N) < N + 1 - 2N^{\frac{1}{2}} \quad [21][24].$$

Wiener result is applicable when the secret exponent $d < N^{\frac{1}{4}}$, and B de Weger extended this result from $N^{\frac{1}{4}}$ to $N^{\frac{3}{4}-\beta}$, where $p - q = N^\beta$, the prime difference by the following theorem.

Theorem 2.2.2. Let $N = pq$ for $q < p < 2q$ be the modulus of RSA with the encryption exponent e and the decryption exponent d . For $\Delta = p - q = N^\beta$, if $d < N^{\frac{3}{4}-\beta}$, then $\frac{t}{d}$ is a convergent of $\frac{e}{N+1-2N^{\frac{1}{2}}}$.

Example 2.2.3. Let $(N, e) = (2691281, 571607)$ be a public key.

The continued fraction expression of $\frac{571607}{2691281}$ is $[0; 4, 1, 2, 2, 2, 1, 27, 2, 2, 3, 3, 1, 1, 7]$.

The sequence of convergents of above continued fraction is

$\left\{ \frac{0}{1}, \frac{1}{4}, \frac{1}{5}, \frac{3}{14}, \frac{7}{33}, \frac{17}{80}, \frac{24}{113}, \frac{665}{3131}, \dots \right\}$. The first five convergents fail the Wiener's test and the next convergents are not useful, since the fifth convergent already has a denominator that is much larger than $N^{\frac{1}{4}} \approx 40.5$. Therefore as the decryption exponent is not less than the bound $B_d(2)$, Wiener's attack does not yield the result. Now we apply B de Weger method in this case and obtain the result (p, q, d) as follows:

We consider the infinite continued fraction of $\frac{e}{N+1-2N^{\frac{1}{2}}} = \frac{571607}{2688000.975} \approx 0.212651336$ given as $[0; 4, 1, 2, 2, 1, 3, 4, 23, \dots]$. The sequence of convergents of the above continued fraction is $\left\{ \frac{0}{1}, \frac{1}{4}, \frac{1}{5}, \frac{3}{14}, \frac{7}{33}, \frac{10}{47}, \frac{37}{174}, \frac{158}{743}, \dots \right\}$. The first seven convergents are not good approximations of $\frac{e}{N+1-2N^{\frac{1}{2}}}$, as $\varphi'(N)$, x' and y' defined in Wiener's attack, are not integers. The next convergent $\frac{158}{743}$ is a good approximation to $\frac{e}{N+1-2N^{\frac{1}{2}}}$, since $\varphi'(N)=2688000$, $x' = 1641$ and $y' = 40$ are positive integers. Therefore, the public key

$$\begin{aligned}
(p, q, d) &= (x' + y', x' - y', d) \\
&= (1681, 1601, 743).
\end{aligned}$$

Note 2.2.4. In the above example $\delta \approx 0.446 > \frac{1}{4}$, so Wiener's attack fails to give a required convergent of $\frac{e}{N}$. But the above extension of Wiener attack succeeds through a convergent of $\frac{e}{N+1-2N^{\frac{1}{2}}}$ for δ just a little less than $\frac{3}{4} - \beta$. Therefore B de Weger method is a refinement of the attack bound for d , over Wiener's method.

2.2.2 Wieners Extension on RSA for Small Difference

$p - \rho q$ with ρq , a Better Approximation of p by Maitra-Sarkar

In this section we describe an extension of Wiener's result given by Subhamoy Maitra and Santanu Sarkar in the paper [30] based on the theory of continued fractions [48]. B de Weger has shown that for $d = N^\delta$, $\delta < \frac{3}{4} - \beta$ RSA is insecure as in this case $\frac{t}{d}$ is a convergent of $\frac{e}{N+1-2N^{\frac{1}{2}}}$. B de Weger method is a refinement of the attack bound for d over Wiener's method and note this refinement is depending on the prime difference $p - q = N^\beta$ but note that this refinement is not significant when $p - q \approx N^{0.5}$. Thus the refinement increases when β decreases i.e., for smaller prime differences. In [30] instead of considering the prime difference $p - q$, Subhamoy Maitra and Santanu Sarkar considered $|p - \rho q|$ for ρ such that $1 \leq \rho \leq 2$ and ρq is a better approximation for p . They proved that for a given ρ (known to the attacker), $|p - \rho q| \leq \frac{N^\gamma}{16}$ and for $d < N^{\frac{1-\gamma}{2}}$, $\frac{t}{d}$ is a convergent of $\frac{e}{N - (\sqrt{\rho} + \frac{1}{\sqrt{\rho}})\sqrt{N+1}}$ and is based on the following proposition.

Proposition 2.2.5. Let $|p - \rho q| \leq \frac{N^\gamma}{16}$, where $\gamma \leq \frac{1}{2}$ and $1 \leq \rho \leq 2$. Then

$$\left| p + q - \left(\sqrt{\rho} + \frac{1}{\sqrt{\rho}} \right) \sqrt{N} \right| < \frac{N^\gamma}{8}.$$

The attack bound for δ when $|p - \rho q| \leq \frac{N^\gamma}{16}$ for $1 \leq \rho \leq 2, \gamma \leq \frac{1}{2}$ is given in the following theorem.

Theorem 2.2.6. Let $|p - \rho q| \leq \frac{N^\gamma}{16}$ with $1 \leq \rho \leq 2, \gamma \leq \frac{1}{2}$ and $d = N^\delta$, then N can be factored in $O(\text{poly}(\log N))$ time when $\delta < \frac{1-\gamma}{2}$.

The above theorem states that this RSA attack runs in a polynomial time. So the RSA attack exists if $|p - \rho q| \leq \frac{N^\gamma}{16}$ for $1 \leq \rho \leq 2, \gamma \leq \frac{1}{2}$ and if $d < N^{\frac{1-\gamma}{2}}$.

Example 2.2.7. Let $p = 2017$ and $q = 1009$, which gives $N = 2035153$.

Then $\varphi(N) = (p - 1)(q - 1) = 20321281$. Note for $d = N^\delta$, δ is such that $\delta > \frac{3}{4} - \beta \approx 0.28$, therefore B de Weger method does not yield the result but by Maitra-Sarkar's method, in this example for $\rho = 2$ we get $\frac{1-\gamma}{2} = 0.375$ for $\gamma = 0.25$ as $|p - 2q| = 1 < \frac{N^{0.25}}{16} = 2.3606374$. Thus, in this case for any $d < N^{0.375}$, RSA will be insecure. Therefore we take d such that $N^{0.374} < d < N^{0.375}$.

In particular for $d = 229$, then the corresponding e , the multiplicative inverse of d modulo $\varphi(N)$ is 1242349, that is $e = 1242349$ and the value for t satisfying $e = 1 + t\varphi(N)$, is 140. The continued fraction expression of $\frac{e}{N - \frac{3}{\sqrt{2}}\sqrt{N} + 1}$ is $[0; 1, 1, 1, 1, 2, 1, 11, 1, 245, \dots]$. More partial quotients are not useful, as $d = 229 < 245$.

The corresponding convergents of the above continued fraction expression are

$\frac{0}{1}, \frac{1}{1}, \frac{1}{2}, \frac{2}{3}, \frac{3}{5}, \frac{8}{13}, \frac{11}{18}, \frac{129}{211}, \frac{140}{229}, \dots$, and the required convergent is $\frac{140}{229}$. From this, we get the public key $(p, q, d) = (2017, 1009, 229)$.

The refinement process of RSA attack bounds on decryption exponent d using theory of continued fractions is given in the following table.

Attack	Refining the RSA attack bounds
Wiener's attack	$d < N^{0.25}$.
Wieners extension on RSA by B de Weger	$N^{0.25} < d < N^{0.75-\beta}$, for $N^\beta = p - q $.
Wieners extension on RSA by Maitra-Sarkar	$N^{0.25} < d < N^{\frac{1-\gamma}{2}}$, for $ p - \rho q = \frac{N^\gamma}{16}$, where $\gamma \leq \frac{1}{2}$, $1 \leq \rho \leq 2$.

Table 2.1: Refinement process of RSA attack bounds on decryption exponent d .

2.3 Extending Wiener's Attack to an RSA-Like Cryptosystem over Elliptic Curves

In this section we describe an extension of Wiener's attack to an RSA-like cryptosystem over elliptic curves. RSA-like cryptosystem over elliptic curves considered by Koyama-Maurer-Okamoto-Vanstone[46][50] for the elliptic curves in the form

$$E_b(N) : y^2 = x^3 + b \pmod{N} \text{ for } N = pq, p, q \text{ primes with } p \equiv q \equiv 2 \pmod{3}.$$

The curves $E_b(p) : y^2 = x^3 + b \pmod{p}$ and $E_b(q) : y^2 = x^3 + b \pmod{q}$ are super singular with orders $\#E_b(p) = p + 1$ & $\#E_b(q) = q + 1$. Further as the group $E(\mathbb{Z}_{pq})$ is such that $E(\mathbb{Z}_{pq}) \simeq E(\mathbb{Z}_p) \oplus E(\mathbb{Z}_q)$, the order of the group $E(\mathbb{Z}_{pq})$ is given as $\#E(\mathbb{Z}_N) = \#E(\mathbb{Z}_p) \cdot \#E(\mathbb{Z}_q) = (p+1)(q+1)$. This system is also known as KMOV. In the KMOV system the receiver chooses primes p, q with $p \equiv q \equiv 2 \pmod{3}$ takes $N = pq$ and chooses e such that $1 \leq e \leq (p+1)(q+1)$ with $\gcd(e, (p+1)(q+1)) = 1$

and makes (N, e) public. The sender represents the message $M = (m_1, m_2)$ as a point on elliptic curve $E_b : y^2 = x^3 + b$, for $b = m_2^2 - m_1^3 \pmod{N}$. The message is encrypted as $C = eM$ and the cipher text C is sent to the receiver. The receiver for decryption uses the decryption exponent d such that $1 \leq d \leq (p+1)(q+1)$ with $ed \equiv 1 \pmod{(p+1)(q+1)}$ and obtains the message as $dC = deM = M \pmod{N}$. The computations are carried using the Group laws on elliptic curves [46][14].

In [37] R.G.E. Pinch shows that Wiener's attack extends to RSA-like cryptosystems on elliptic curves and Lucas sequences. In this section we show that Wiener's attack can be extended to KMOV by developing an estimation for $\psi(N) = \#E(\mathbb{Z}_N) = (p+1)(q+1)$. This estimation on $\psi(N)$ when $q < p < aq$ for some $a \in \mathbb{N}$ plays a key role in extending Wiener's attack to KMOV is given in the following lemma.

Lemma 2.3.1. Let $N = pq$, where p and q are odd primes such that $q < p < aq$ for some $a \in \mathbb{N}$. Then

$$N + 1 < \psi(N) < N + (a + 1)\sqrt{N} - 1.$$

Proof. By defining of $\psi(N)$, $\psi(N) = (p+1)(q+1)$ we have

$$\psi(N) > N + 1.$$

As $a \geq 2$ and $q < \sqrt{N}$, we have $q + \frac{2}{a+1} < q + 1 \leq \sqrt{N}$. Then from the inequality $p < 2q$ we get

$$\psi(N) < N + (a + 1)\sqrt{N} - 1.$$



Theorem 2.3.2. (Wiener's attack on RSA-like over $E(\mathbb{Z}_N)$ due to KMOV)

Let $N = pq$, for $q < p < aq$ be the modulus for RSA, e be the public encryption exponent and d be the decryption exponent. If $d \leq \frac{N^{\frac{1}{4}}}{\sqrt{2(a+1)}}$, then $\frac{t}{d}$ is a convergent of $\frac{e}{N}$, for $t = \frac{ed-1}{\psi(N)}$.

Proof. First note for $d \leq \frac{N^{\frac{1}{4}}}{\sqrt{2(a+1)}}$, we have

$$\frac{a+1}{\sqrt{N}} \leq \frac{1}{2d^2}. \quad (2.3.1)$$

As $\frac{ed-1}{t} = \psi(N)$ and by the right inequality $\psi(N) < N + (a+1)\sqrt{N} - 1$ in the above lemma, we get

$$\frac{ed-1}{dN} < \frac{(a+1)t\sqrt{N}}{dN} + \frac{Nt}{dN} - \frac{t}{dN}.$$

Then from this and as $t \geq 1$, we obtain

$$\frac{e}{N} - \frac{t}{d} < \frac{(a+1)t\sqrt{N}}{dN}. \quad (2.3.2)$$

Now by using the left inequality $N+1 < \psi(N)$ of the above lemma and as $(a+1)t\sqrt{N} > 0$, we have

$$\frac{e}{N} - \frac{t}{d} > -\frac{(a+1)t\sqrt{N}}{dN}. \quad (2.3.3)$$

Also we have

$$t < d, \text{ for } e < \psi(N). \quad (2.3.4)$$

From (2.3.2), (2.3.3) and (2.3.4),

$$\left| \frac{e}{N} - \frac{t}{d} \right| < \frac{(a+1)}{\sqrt{N}}. \quad (2.3.5)$$

By (2.3.1) and (2.3.5), we get

$$\left| \frac{e}{N} - \frac{t}{d} \right| < \frac{1}{2d^2}.$$

Therefore, $\frac{t}{d}$ is convergent of $\frac{e}{N}$ by Approximation Theorem ■

Theorem 2.3.3. (Implementation of Wiener's attack): Let $d \leq \frac{N^{\frac{1}{4}}}{\sqrt{2(a+1)}}$ and for any convergent $\frac{t'}{d'}$ of $\frac{e}{N}$, take $\psi'(N) = \frac{ed'-1}{t'}$, $x' = \frac{\psi'(N)-N-1}{2}$ and $y' = \sqrt{(x')^2 - N}$. If $x', y' \in \mathbb{N}$, then $\psi'(N) = \psi(N)$ and the private key is $(p, q, d) = (x' + y', x' - y', d')$.

Proof. For $y' = \sqrt{(x')^2 - N}$, $N = (x' + y')(x' - y')$.

If $x', y' \in \mathbb{N}$, then the possible cases are

(i) $(x' - y') = 1$ and $(x' + y') = N$

(ii) $(x' - y') = q$ and $(x' + y') = p$, as $N = pq$ and $q < p$.

For $(x' - y') = 1$ and $(x' + y') = N$, we have $\frac{N+1}{2} = x'$.

Then $\psi'(N) - N - 1 = 2x' = N + 1$.

Thus $2(N + 1) = \psi'(N)$

$$= \frac{ed' - 1}{t'}$$

$$< N + (a + 1)\sqrt{N} - 1, \text{ as } \frac{e}{N + (a + 1)\sqrt{N} - 1} < \frac{t'}{d'}, \text{ for some } t', d'$$

$$\text{and } \psi(N) < N + (a + 1)\sqrt{N} - 1.$$

Therefore $N^{\frac{1}{2}} < a + 1$.

Which is a contradiction, as we are choosing a large N .

Hence case(i) is not possible.

Therefore, the only possible case is $q = x' - y', p = x' + y'$.

By defining of x' , we have $x' = \frac{\psi'(N) - N - 1}{2}$.

$$\begin{aligned} \text{Then } \psi'(N) &= 2x' + N + 1 \\ &= p + q + N + 1 \\ &= \psi(N). \end{aligned}$$

Now as $ed' = 1 \pmod{\psi'(N)}$ and $\psi'(N) = \psi(N), d = d'$.

Therefore, for $\psi'(N), x', y' \in \mathbb{N}$, the private key $(p, q, d) = (x' + y', x' - y', d')$. ■

Example 2.3.4. (Implementation of Wiener's attack)

Let $(N, e) = (59729269, 36366887)$ be the public key.

The continued fraction of $\frac{e}{N} = \frac{36366887}{59729269}$ is $[0; 1, 1, 1, 1, 3, 1, 10, 1, 1, 2, 1, 3, 1, 44, 4, 1, 30]$ and the first six convergents of the above continued fractions $\frac{0}{1}, \frac{1}{1}, \frac{1}{2}, \frac{2}{3}, \frac{3}{5}$ and $\frac{11}{18}$ are not good approximations of $\frac{e}{N}$ as $\psi'(N), x', y' \notin \mathbb{N}$.

The next convergent $\frac{14}{23}$ is a good approximation to $\frac{e}{N}$ as $\psi'(N) = 59745600, x' = 8165, y' = 2634$ are such that $\psi'(N), x', y' \in \mathbb{N}$.

Therefore the private key $(p, q, d) = (x' + y', x' - y', d') = (10799, 5531, 23)$.

2.4 Extending Wiener's Extension to an RSA-Like Cryptosystem over Elliptic Curves

R.G.E. Pinch in his paper [37] showed that Wiener's attack applies to KMOV as well. In [47] B de Weger and in [30] Subhamoy Maitra - Santanu Sarkar are proposed Wiener extension on RSA cryptosystem refining the attack bound for the decryption exponent d . In this section we show that these Wiener's extensions also apply to the RSA-like cryptosystems over elliptic curves due to KMOV. This is done by looking at $\psi(N) := (p+1)(q+1)$ as an analogue of Euler's function $\varphi(N)$ in the RSA-like cryptosystems over the specific elliptic curves $E_b : y^2 = x^3 + b \pmod{N}$. In this section we proposed that the above Wiener extensions can be extended to RSA-like cryptosystem over elliptic curves due to KMOV by developing certain estimates on $\psi(N)$, we prove the results regarding the estimates for $\psi(N)$ in the following lemma.

Lemma 2.4.1. If $q < p < 2q$ and $\psi(N) = (p+1)(q+1)$ then $N + 1 + 2N^{\frac{1}{2}} < \psi(N) < N + 1 + \frac{3}{\sqrt{2}}N^{\frac{1}{2}}$.

Proof. We have $\psi(N) = (p+1)(q+1) = N + 1 + p + q$.

Therefore as $p + q > 2N^{\frac{1}{2}}$ note $\psi(N) > N + 1 + 2N^{\frac{1}{2}} \dots (1)$.

Now as $\left(p + q + \frac{3}{\sqrt{2}}N^{\frac{1}{2}}\right) \left(p + q - \frac{3}{\sqrt{2}}N^{\frac{1}{2}}\right) < 0$ for $q < p < 2q$, note

$\left(p + q - \frac{3}{\sqrt{2}}N^{\frac{1}{2}}\right) < 0 \dots (2)$

This implies $\psi(N) = N + 1 + p + q < \left(N + 1 + \frac{3}{\sqrt{2}}N^{\frac{1}{2}}\right)$.

From (1) and (2) $N + 1 + 2N^{\frac{1}{2}} < \psi(N) < N + 1 + \frac{3}{\sqrt{2}}N^{\frac{1}{2}}$. ■

The estimation of $\psi(N)$ given in the above lemma leads to an approximate convergent for $\frac{t}{d}$ is described in the following theorem.

Theorem 2.4.2. (Wieners extension on RSA-like over $E(\mathbb{Z}_N)$ due to KMOV)

Let $N = pq$ for $q < p < 2q$ with the encryption exponent e and decryption exponents d such that $\frac{ed-1}{t} = \psi(N)$. If $\Delta = p - q = N^\beta$, $d < N^{\frac{3}{4}-\beta}$, then $\frac{t}{d}$ is a convergent of $\frac{e}{N+1+2N^{\frac{1}{2}}}$.

Proof. We have

$$\begin{aligned} \left| \frac{e}{N+1+2N^{\frac{1}{2}}} - \frac{t}{d} \right| &= \left| \frac{e}{N+1+2N^{\frac{1}{2}}} + \frac{e}{\psi(N)} - \frac{e}{\psi(N)} - \frac{t}{d} \right| \\ &\leq \left| \frac{e}{N+1+2N^{\frac{1}{2}}} - \frac{e}{\psi(N)} \right| + \left| \frac{e}{\psi(N)} - \frac{t}{d} \right| \\ &= e \left| \frac{1}{N+1+2N^{\frac{1}{2}}} - \frac{1}{\psi(N)} \right| + \frac{1}{\psi(N)d}, \end{aligned}$$

as $e > 0$ and $ed - 1 = \psi(N)t$.

$$< \psi(N) \left| \frac{\psi(N) - (N+1+2N^{\frac{1}{2}})}{(N+1+2N^{\frac{1}{2}})\psi(N)} \right| + \frac{1}{\psi(N)d},$$

as $e < \psi(N)$.

$$= \psi(N) \left| \frac{N+1+p+q-N-1-2N^{\frac{1}{2}}}{\psi(N)(N+1+2N^{\frac{1}{2}})} \right| + \frac{1}{\psi(N)d}$$

$$= \frac{p+q-2N^{\frac{1}{2}}}{N+1+2N^{\frac{1}{2}}} + \frac{1}{\psi(N)d} \text{ as } p+q-2N^{\frac{1}{2}} > 0.$$

$$< \frac{\Delta^2}{4N^{\frac{1}{2}}} \left(\frac{1}{N+1+2N^{\frac{1}{2}}} \right) + \frac{1}{\psi(N)d},$$

as $p+q-2N^{\frac{1}{2}} = \frac{\Delta^2}{p+q+2N^{\frac{1}{2}}}$.

$$< \frac{\Delta^2}{4N^{\frac{1}{2}}} \left(\frac{1}{\varphi(N)} \right) + \frac{1}{\varphi(N)d},$$

as $N+1+2N^{\frac{1}{2}} > \varphi(N)$ and $\psi(N) > \varphi(N)$.

$$\text{Therefore } \left| \frac{e}{N+1+2N^{\frac{1}{2}}} - \frac{t}{d} \right| < \frac{1}{\varphi(N)} \left(\frac{\Delta^2}{4N^{\frac{1}{2}}} + \frac{1}{d} \right) \dots (1)$$

Now note $\psi(N) > \frac{3}{4}N$, since $p + q < \frac{1}{4} + 1$ for all $N^{\frac{1}{2}} > 9$ by assuming N is large.

Also note $8d < N$ for all $N^{\frac{1}{4}} > 8$, since $d < N^{\frac{3}{4}}$.

Therefore, for $\Delta = N^\beta$ and $d = N^\delta$ and substitute $\varphi(N) > \frac{3}{4}N$ and $N > 8d$ in (1), we get

$$\begin{aligned} \left| \frac{e}{N+1+2N^{\frac{1}{2}}} - \frac{t}{d} \right| &< \frac{1}{3}N^{2\beta-\frac{3}{2}} + \frac{4}{3Nd} \\ &< \frac{1}{3}N^{2\beta-\frac{3}{2}} + \frac{1}{6N^{2\delta}} \end{aligned}$$

and as $2\beta - \frac{3}{2} < -2\beta$ for all $\delta < \frac{3}{4} - \beta$, we have

$$\left| \frac{e}{N+1+2N^{\frac{1}{2}}} - \frac{t}{d} \right| < \frac{1}{2d^2}.$$

Therefore $\frac{t}{d}$ is a convergent of $\frac{e}{N+1+2N^{\frac{1}{2}}}$ for $d < N^{\frac{3}{4}-\beta}$. ■

Now using the above estimates for $\psi(N)$ we prove the following theorem of implementation on Wiener's extension.

Theorem 2.4.3. (Implementation of Wiener's extension): Let $d < N^{\frac{3}{4}-\beta}$ for $p - q = N^\beta$ and for any convergent $\frac{t'}{d'}$ of $\frac{e}{N+1+2N^{\frac{1}{2}}}$, take $\psi'(N) = \frac{ed'-1}{t'}$, $x' = \frac{\psi'(N)-N-1}{2}$ and $y' = \sqrt{(x')^2 - N}$. If $x', y' \in \mathbb{N}$, then $\psi'(N) = \psi(N)$ and the private key is $(p, q, d) = (x' + y', x' - y', d')$.

Proof. For $y' = \sqrt{(x')^2 - N}$, $N = (x' + y')(x' - y')$.

If $x', y' \in \mathbb{N}$, then the possible cases are

(i) $(x' - y') = 1$ and $(x' + y') = N$

(ii) $(x' - y') = q$ and $(x' + y') = p$, as $N = pq$ and $q < p$.

For $(x' - y') = 1$ and $(x' + y') = N$, we have $\frac{N+1}{2} = x'$.

Then $\psi'(N) - N - 1 = 2x' = N + 1$.

Thus $2(N + 1) = \psi'(N)$.

$$\begin{aligned} &= \frac{ed' - 1}{t'} \\ &< N + 2 + \frac{3}{\sqrt{2}}N^{\frac{1}{2}}, \text{ as } \frac{e}{N + 2 + \frac{3}{\sqrt{2}}N^{\frac{1}{2}}} < \frac{t'}{d'}, \text{ for some } t', d' \\ &\text{and } \psi(N) < N + 1 + \frac{3}{\sqrt{2}}N^{\frac{1}{2}}. \end{aligned}$$

Therefore $N^{\frac{1}{2}} < \frac{3}{\sqrt{2}}$.

Which is a contradiction, as we are choosing a large N .

Hence case(i) is not possible.

Therefore, the only possible case is $q = x' - y', p = x' + y'$.

By defining of x' , we have $x' = \frac{\psi'(N) - N - 1}{2}$.

$$\begin{aligned} \text{Then } \psi'(N) &= 2x' + N + 1 \\ &= p + q + N + 1 \\ &= \psi(N). \end{aligned}$$

Now as $ed' = 1 \pmod{\psi'(N)}$ and $\psi'(N) = \psi(N), d = d'$.

Therefore, for $\psi'(N), x', y' \in \mathbb{N}$, the private key $(p, q, d) = (x' + y', x' - y', d')$. ■

The following example demonstrates the working of KMOV cryptosystem.

Example 2.4.4. The receiver chooses primes $p = 5, q = 11$ takes $N = pq = 55$.

Then he chooses $e = 5$ and makes (N, e) public.

The sender chooses a message $M = (2, 3)$, a point on the elliptic curve $E_b : y^2 =$

$x^3 + 1 \pmod{55}$ and enciphers the message as $C = eM \pmod{N}$ and sends the cipher text C to the receiver. The computations are done by using the group laws on elliptic curves and the algorithms like doubling and adding algorithm [9] may be used for computations

$$\begin{aligned} C &= 5M = 5(2, 3) = (1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0)(2, 3) \\ &= (2(2(2, 3)) + (2, 3)) \\ &= (2, 52) \pmod{55}. \end{aligned}$$

For decryption the receiver computes $29C \pmod{55}$ as follows

$$\begin{aligned} 29C &= (1 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0)C \\ &= 2(2(2(2(2(2, 52)))) + 2(2(2(2, 52))) + 2(2(2, 52)) + (2, 52) \pmod{55} \\ &= (2, 3) \pmod{55} \\ &= M \pmod{55}, \text{ the required message.} \end{aligned}$$

Example 2.4.5. (Implementation of Wiener's extension)

Let $(N, e) = (10610503, 8916809)$ be the public key.

The continued fraction of

$$\begin{aligned} \frac{e}{N + 1 + 2N^{\frac{1}{2}}} &= \frac{8916809}{10610503 + 1 + 2 \cdot (10610503)^{\frac{1}{2}}} \\ &\sim 0.83985 \\ &= [0; 1, 5, 4, 11, 5, 2, 1, 1, 1 \dots] \end{aligned}$$

The first five convergents of the above continued fractions are

$$\frac{0}{1}, \frac{1}{1}, \frac{5}{6}, \frac{21}{25}, \frac{236}{281}, \dots$$

The required convergent is $\frac{236}{281}$ as $\psi'(N) = 10617048, x' = 3272, y' = 309$ are such that $\psi'(N), x', y' \in \mathbb{N}$.

Therefore the private key $(p, q, d) = (x' + y', x' - y', d') = (3581, 2963, 281)$.

Similarly we can extend the generalized version by Subhamoy Maitra and Santanu Sarkar's result to RSA-like cryptosystem over elliptic curves due to KMOV to get the bound for d , as $d < N^{\frac{1-\gamma}{2}}$ for $|p - \rho q| \leq \frac{N^\gamma}{16}$ and $1 \leq \rho \leq 2, \gamma \leq \frac{1}{2}$. By the inequality $\left| p + q - \left(\sqrt{\rho} + \frac{1}{\sqrt{\rho}} \right) \sqrt{N} \right| < \frac{N^\gamma}{8}$ in Proposition 2.2.5 note we have the estimation $N + 1 + \left(\sqrt{\rho} + \frac{1}{\sqrt{\rho}} \right) \sqrt{N} - \frac{N^\gamma}{8} < \psi(N) < N + 1 + \left(\sqrt{\rho} + \frac{1}{\sqrt{\rho}} \right) \sqrt{N} + \frac{N^\gamma}{8}$ and this leads to an approximate convergent for $\frac{t}{d}$ is described in the following theorem.

Theorem 2.4.6. Let $N = pq$ for $q < p < 2q$ with the encryption exponent e and decryption exponents d such that $\frac{ed-1}{t} = \psi(N)$. If $|p - \rho q| \leq \frac{N^\gamma}{16}, 1 \leq \rho \leq 2, \gamma \leq \frac{1}{2}$ and if $d = N^\delta, \delta < \frac{1-\gamma}{2}$, then $\frac{t}{d}$ is a convergent of $\frac{e}{N+1+\left(\sqrt{\rho}+\frac{1}{\sqrt{\rho}}\right)\sqrt{N}}$.

Proof. Since $|p - \rho q| \leq \frac{N^\gamma}{16}$, we have

$$\left| p + q - \left(\sqrt{\rho} + \frac{1}{\sqrt{\rho}} \right) \sqrt{N} \right| < \frac{N^\gamma}{8} \quad (2.4.1)$$

by Proposition 2.2.5. Also we have $2 \left(\sqrt{\rho} + \frac{1}{\sqrt{\rho}} \right) \sqrt{N} \leq 3\sqrt{2}\sqrt{N} + 2$, as $\rho \leq 2$ and $3\sqrt{2}\sqrt{N} + 2 < N$, as N is such large integer. Therefore

$$N + \left(\sqrt{\rho} + \frac{1}{\sqrt{\rho}} \right) \sqrt{N} + 1 > \frac{N}{2}. \quad (2.4.2)$$

Now we have,

$$\begin{aligned}
\left| \frac{e}{N + \left(\sqrt{\rho} + \frac{1}{\sqrt{\rho}}\right) \sqrt{N} + 1} - \frac{t}{d} \right| &\leq \left| \frac{e}{N + \left(\sqrt{\rho} + \frac{1}{\sqrt{\rho}}\right) \sqrt{N} + 1} - \frac{e}{\psi(N)} \right| + \left| \frac{e}{\psi(N)} - \frac{t}{d} \right| \\
&< \frac{\left| \psi(N) - \left(N + \left(\sqrt{\rho} + \frac{1}{\sqrt{\rho}}\right) \sqrt{N} + 1\right) \right|}{N + \left(\sqrt{\rho} + \frac{1}{\sqrt{\rho}}\right) \sqrt{N} + 1} + \frac{1}{d\psi(N)}, \\
&\hspace{15em} \text{as } e < \psi(N) \\
&< \frac{N^\gamma}{8\frac{N}{2}} + \frac{1}{4d^2},
\end{aligned}$$

by (2.4.1), (2.4.2) and by assuming $\psi(N) > 4d$.

Thus,

$$\left| \frac{e}{N + \left(\sqrt{\rho} + \frac{1}{\sqrt{\rho}}\right) \sqrt{N} + 1} - \frac{t}{d} \right| < \frac{N^{\gamma-1}}{4} + \frac{1}{4d^2}.$$

Therefore, when $\frac{N^{\gamma-1}}{4} < \frac{1}{4d^2}$ we get

$$\left| \frac{e}{N + \left(\sqrt{\rho} + \frac{1}{\sqrt{\rho}}\right) \sqrt{N} + 1} - \frac{t}{d} \right| < \frac{1}{2d^2}.$$

Putting $d = N^\delta$ in the inequality $\frac{N^{\gamma-1}}{4} < \frac{1}{4d^2}$, we get $\delta < \frac{1-\gamma}{2}$.

Therefore, for $\delta < \frac{1-\gamma}{2}$, $\frac{t}{d}$ is a convergent of the continued fraction of $\frac{e}{N+1+\left(\sqrt{\rho}+\frac{1}{\sqrt{\rho}}\right)\sqrt{N}}$. ■

Now using the above estimates for $\psi(N)$ we prove the following theorem of implementation on Wiener's extension.

Theorem 2.4.7. (Implementation of Wiener's extension): Let $d < N^{\frac{1-\gamma}{2}}$ for $|p - \rho q| \leq \frac{N^\gamma}{16}$, $1 \leq \rho \leq 2$, $\gamma \leq \frac{1}{2}$ and for any convergent $\frac{t'}{d'}$ of $\frac{e}{N+1+(\sqrt{\rho}+\frac{1}{\sqrt{\rho}})\sqrt{N}}$, take $\psi'(N) = \frac{ed'-1}{t'}$, $x' = \frac{\psi'(N)-N-1}{2}$ and $y' = \sqrt{(x')^2 - N}$. If $x', y' \in \mathbb{N}$, then $\psi'(N) = \psi(N)$ and the private key is $(p, q, d) = (x' + y', x' - y', d')$.

Proof. For $y' = \sqrt{(x')^2 - N}$, $N = (x' + y') \cdot (x' - y')$.

If $x', y' \in \mathbb{N}$, then the possible cases are

$$(i) (x' - y') = 1 \text{ and } (x' + y') = N$$

$$(ii) (x' - y') = q \text{ and } (x' + y') = p, \text{ as } N = pq \text{ and } q < p.$$

For $(x' - y') = 1$ and $(x' + y') = N$, we have $\frac{N+1}{2} = x'$.

Then $\psi'(N) - N - 1 = 2x' = N + 1$. Thus $2(N + 1) = \psi'(N)$.

From the inequality $\psi(N) < N + 1 + \left(\sqrt{\rho} + \frac{1}{\sqrt{\rho}}\right)\sqrt{N} + \frac{N^\gamma}{8}$ and for some t' and d' , we have

$$2(N + 1) < N + 1 + \left(\sqrt{\rho} + \frac{1}{\sqrt{\rho}}\right)\sqrt{N} + \frac{N^\gamma}{8}.$$

This gives the inequality

$$N^{\frac{1}{2}} < \left(\sqrt{\rho} + \frac{1}{\sqrt{\rho}}\right) + \frac{N^{\gamma-\frac{1}{2}}}{8} - \frac{1}{N^{\frac{1}{2}}}.$$

For $1 \leq \rho \leq 2$ and $\gamma \leq \frac{1}{2}$, we have

$$N^{\frac{1}{2}} < \sqrt{2} + 1.$$

Which is a contradiction, as we are choosing a large N .

Hence case(i) is not possible.

Therefore, the only possible case is $q = x' - y', p = x' + y'$.

By defining of x' , we have $x' = \frac{\psi'(N) - N - 1}{2}$.

$$\begin{aligned} \text{Then } \psi'(N) &= 2x' + N + 1 \\ &= p + q + N + 1 \\ &= \psi(N). \end{aligned}$$

Now as $ed' = 1 \pmod{\psi'(N)}$ and $\psi'(N) = \psi(N), d = d'$.

Therefore, for $\psi'(N), x', y' \in \mathbb{N}$, the private key $(p, q, d) = (x' + y', x' - y', d')$. ■

Example 2.4.8. (Implementation of Wiener's extension)

Let $(N, e) = (8162729, 578321)$ be the public key.

For $\rho = 2$, the infinite continued fraction of $\frac{e}{N + (\sqrt{\rho + \frac{1}{\rho}})\sqrt{N+1}} = \frac{578321}{8162729 + (\sqrt{2 + \frac{1}{2}})\sqrt{8162729+1}}$ is $[0; 14, 7, 1, 1370, 11, 12, \dots]$ and the sequence of convergents is $\{\frac{0}{1}, \frac{1}{14}, \frac{7}{99}, \frac{8}{113}, \frac{10967}{154909}, \dots\}$.

The required convergent is $\frac{8}{113}$ as $\psi'(N) = 8168784, x' = 3027, y' = 1000$ are such that $\psi'(N), x', y' \in \mathbb{N}$.

Therefore the private key $(p, q, d) = (x' + y', x' - y', d') = (4027, 2027, 113)$.

2.5 Summary

The idea of Wiener is that certain restrictions of d allow to obtain a convergent of $\frac{e}{N}$ that is useful in finding the factors p, q of N and the decryption exponent d . Further Wiener's extension given by B de Weger and Subhamoy Maitra - Santanu Sarkar is the idea of obtaining a convergent of $\frac{e}{N+1-2N^{\frac{1}{2}}}$ and $\frac{e}{N - (\sqrt{\rho + \frac{1}{\rho}})\sqrt{N+1}}$ respectively rather than that of $\frac{e}{N}$, which increases the bound of d , from $N^{\frac{1}{4}}$ to N^δ , for $\delta < \frac{3}{4} - \beta$ and for $\delta < \frac{1-\gamma}{2}$ respectively. These ideas are based on developing certain estimates

for $\varphi(N)$. Looking at $\psi(N) = (p + 1)(q + 1)$ as the analogue of Euler's function $\varphi(N)$ in the RSA-like cryptosystem over the elliptic curves $E(\mathbb{Z}_{pq})$ due to KMOV developing certain estimates on $\psi(N)$, we proposed that the Wiener's attack and its extensions can be extended to RSA-like cryptosystem over elliptic curves $E(\mathbb{Z}_{pq})$ due to KMOV.

Chapter 3

Cryptanalysis Based on Lattice-Based Techniques, for RSA with Small Deciphering Exponent

In this chapter we review some of the lattice attacks on RSA with low private decryption exponent, based on modified Coppersmith method due to Howgrave-Graham for finding small roots of bivariate integer polynomial equations and extended strategy of Jochemsz and May for finding roots of multivariate polynomials. Also we noted that all these Lattice-based attacks on RSA can be extended to the RSA-like cryptosystem over $E(\mathbb{Z}_{pq})$ due to KMOV.

3.1 Finding small roots of univariate integer modular equations

If the relation between the parameters N, p, q, e , and d of RSA can be converted into a polynomial with a small root and if the root can be found, then one can

find the secret information (d, p, q) , thereby breaking RSA. RSA attacks using lattice based techniques were initiated with the method developed by Coppersmith to find small integer solutions for univariate modular equations. Coppersmith methods later were modified and generalized to integer solutions of multivariate polynomials. Howgrave-Graham modified Coppersmith method, Boneh-Durfee generalized the method to bivariate and Jochemsz-May [18] generalized to multivariate polynomial modular equations. Using the lemma by Howgrave-Graham, he modified Coppersmith method, to find the small roots of univariate modular equations. In the following we describe Howgrave-Graham method.

Theorem 3.1.1. Given a monic polynomial $P(x)$ of degree δ , modulo an integer N of unknown factorization, one can find in polynomial time for all integers x_0 such that $P(x_0) = 0 \pmod{N}$ and $|x_0| \leq \frac{1}{2}N^{1/k}$.

Proof. Let $p(x)$ be a univariate modular polynomial of degree k

$$p(x) = x^k + a_{k-1}x^{k-1} + \dots + a_1x + a_0 \pmod{N}.$$

To find the small roots of a monic univariate modular equation $p(x) = 0 \pmod{N}$: Let h be an integer $h \geq 2$, and natural number X define a lower triangular $(hk) \times (hk)$ matrix $M = (m_{i,j})$. The entry $m_{i,j}$ is given by $e_{i,j}X^{j-1}$, where $e_{i,j}$ is the coefficient of x^{j-1} in the expression,

$$q_{u,v}(x) = N^{(h-1-v)}x^u(p(x))^v$$

with $v = \lfloor (i-1)/k \rfloor$, and $u = (i-1) - kv$. Notice that $q_{u,v}(x_0) = 0 \pmod{N^{h-1}}$ for all $u, v \geq 0$. All other entries of the matrix are zero, so it has determinant

$$X^{hk(hk-1)/2} N^{hk(h-1)}/2.$$

Let B be an LLL-reduced basis of the rows of M , and denote the first (small) row vector of B by b_1 . By the conditions on reduced basis

$$\|b_1\| \leq 2^{(hk-1)/4} X^{(hk-1)/2} N^{(h-1)/2}. \quad (3.1.1)$$

Letting $b_1 = cM$ for some $c \in Z^n$ also gives

$$\begin{aligned} \|b_1\| &\geq \frac{1}{\sqrt{hk}} \left(\left| \sum_{i=1}^{hk} c_i m_{i,1} \right| + \dots + \left| \sum_{i=1}^{hk} c_{hk} m_{i,hk} \right| \right) \\ &= \frac{1}{\sqrt{hk}} \left(\left| \sum_{i=1}^{hk} c_i e_{i,1} \right| + \dots + \left| \sum_{i=1}^{hk} c_{hk} e_{i,hk} \right| X^{hk-1} \right) \\ &\geq \frac{1}{\sqrt{hk}} |r(x)| \text{ for all } |x| \leq X, \end{aligned}$$

where

$$r(x) = c_1 \sum_{j=1}^{hk} e_{1,j} x^{j-1} + \dots + c_{hk} \sum_{j=1}^{hk} e_{hk,j} x^{j-1}. \quad (3.1.2)$$

So $\|b_1\|$ is “almost” an upper bound for the polynomial $r(x)$ in the entire range $|x| \leq X$. Notice also that $r(x_0) = 0 \pmod{N^{h-1}}$ since each sum in equation 3.0.2 is zero modulo N^{h-1} .

By 3.0.1 and 3.0.2 implies that, from the matrix M with a natural number X , we have a polynomial $r(x)$ that satisfies $r(x_0) = 0 \pmod{N^{h-1}}$ and

$$|r(x)| \leq \left(2^{(hk-1)/4} \sqrt{hk} \right) X^{(hk-1)/2} N^{(h-1)/2} \text{ for all } |x| \leq X.$$

Thus choosing

$$X = \lceil 2^{-1/2}(hk)^{-1/(hk-1)}N^{(h-1)/(hk-1)} \rceil - 1$$

shows that one can form a polynomial $r(x)$ such that $r(x_0) = 0 \pmod{N^{h-1}}$ and $|r(x)| < N^{h-1}$ for all $|x| \leq X$, therefore by Howgrave-Graham lemma, $r(x_0) = 0$ over the integers as well, for any x_0 such that $|x_0| \leq X$, and $p(x_0) = 0 \pmod{N}$. Solving this univariate equation $r(x)$ over the integers can be done in polynomial time and then one can test each solution to see if it satisfies $p(x_0) = 0 \pmod{N}$ as well.

Notice that the bound $X \rightarrow \frac{1}{2}N^{1/k}$ as $h \rightarrow \infty$. The polynomial $r(x)$ can be formed from equation 3.0.2 or the coefficient may be obtained by dividing the entries of the vector b_1 by appropriate powers of X . ■

Example of Howgrave-Graham method for finding small roots of univariate integer modular equations is given as follows

Example 3.1.2. Consider the polynomial congruence $x^2 + 22x + 19 \equiv 0 \pmod{21}$ with $x = 1$ is a solution. For $h = 2, k = 2$, take $X \approx \frac{1}{2}(21)^{\frac{1}{2}} \approx 2.29$ such that X is a positive integer, in particular, we take $X = 2$, then the matrix defined in the Howgrave-Graham method is given as

$$M = \begin{pmatrix} 21 & 0 \times 2 & 0 \times 2^2 & 0 \times 2^3 \\ 0 & 21 \times 2 & 0 \times 2^2 & 0 \times 2^3 \\ 19 & 22 \times 2 & 1 \times 2^2 & 0 \times 2^3 \\ 0 & 19 \times 2 & 22 \times 2^2 & 1 \times 2^3 \end{pmatrix}$$

Now applying LLL-algorithm to the above matrix we get

$$M^{LLL} = \begin{pmatrix} -2 & 2 & 4 & 0 \\ 0 & -4 & 4 & 8 \\ 17 & 4 & 8 & 0 \\ 8 & 26 & -8 & 16 \end{pmatrix}$$

Then the polynomial $r(x)$ given in the above method is $r(x) = \frac{-2}{1} + \frac{2}{2} \cdot x + \frac{4}{2^2} \cdot x^2 + 0 \cdot x^3$, i.e., $r(x) = x^2 + x - 2$ and its integer roots are 1 and -2 . But note that -2 is not a solution for the polynomial congruence $x^2 + 22x + 19 \equiv 0 \pmod{21}$.

Therefore $x = 1$ is a root of a univariate modular equation $x^2 + 22x + 19 \equiv 0 \pmod{21}$ with $|x| \leq X$.

This method due to Howgrave-Graham is adapted by Boneh-Durfee to bivariate polynomials and an attack on RSA is developed. In the following we describe this attack on RSA due to Boneh-Durfee.

3.2 An Attack on RSA, Based on Lattice Basis Reduction by Boneh-Durfee

The first improvement of Wiener's bound for the decryption exponent d unconditionally is given by Boneh-Durfee in [5] employing lattice-based techniques. In their first and second results, they executed an attack bound for d , $d < N^{0.284}$ using lattice-based techniques and improved the bound for d , $d < N^{0.292}$ using sub-lattice based techniques and a strategy of geometrically progressive matrices. Boneh-Durfee approach is as follows:

Consider the normal RSA scheme where p, q are balanced, i.e., $q < p < 2q$ and defining equation of the RSA: $ed - k(N + 1 - (p + q)) = 1$. Taking $s = -(p + q)$, note $|s| \leq 3N^{\frac{1}{2}}$ and for $A = N + 1$, above equation can be simplified to $-k(A + s) \equiv 1 \pmod{e}$. Also as $k = \frac{ed-1}{\varphi(N)}$, if $e = N^\alpha$ (note that α is approximately equal to 1) and $d = N^\delta$ for some α, δ , the idea is to find the solution for the **Small Inverse Problem (SVP)** as follows:

Given a polynomial $f(x, y) = x(A + y) - 1$ to find the root $(x_0, y_0) = (-k, s)$ for the congruence $f(x, y) \equiv 0 \pmod{e}$ with $|x_0| < e^\delta$ and $|y_0| < e^{0.5}$. As note SIP is solved, from $s = -(p + q)$ the factorization N is obtained. So the goal is to identify the values of δ for which the roots (x_0, y_0) with $|x_0| < e^\delta, |y_0| < e^{0.50}$ can be recovered in polynomial time. The main idea of Boneh-Durfee is first to transform the modular equation into an equation over the integers using Howgrave-Graham's lemma for the bivariate case. In order to apply Howgrave-Graham lemma Boneh-Durfee defined for a positive integer m , the shift polynomials $g_{i,k}(x, y)$ and $h_{j,k}(x, y)$ as follows:

$$g_{i,k}(x, y) = x^i f^k(x, y) e^{m-k} \text{ and } h_{j,k}(x, y) = y^j f^k(x, y) e^{m-k},$$

the polynomials $g_{i,k}$ are referred to as x -shifts and analogously the polynomials $h_{j,k}$ are referred to as y -shifts.

Then, considered the lattice spanned by the coefficient vectors of the polynomials $g_{i,k}(x, y), h_{j,k}(x, y)$ for certain parameters i, j and k . For each $k = 0, 1, \dots, m$ use $g_{i,k}(xX, yY)$ for $i = 0, \dots, m - k$, and $h_{j,k}(xX, yY)$ for $j = 1, \dots, t$, for some parameter t to be optimized later. For $m = 2$ and $t = 1$, the shift polynomials and the matrix spanned by x and y shifts are depicted in the following tables.

Shift Polynomials for $m = 2$ and $t = 1$:

k	i	$g_{i,k}(xX, yY)(x - \text{shifts})$
0	0	$g_{0,0}(xX, yY) = e^2$
	1	$g_{1,0}(xX, yY) = xXe^2$
	2	$g_{2,0}(xX, yY) = x^2X^2e^2$
1	0	$g_{0,1}(xX, yY) = xX Ae + xX yYe - e$
	1	$g_{1,1}(xX, yY) = x^2X^2 Ae + x^2X^2 yYe - xXe$
2	0	$g_{0,2}(xX, yY) = x^2X^2 A^2 + x^2X^2 y^2 Y^2 + 2xX AyY - 2xY A - 2xX yY + 1$

k	j	$h_{j,k}(xX, yY)(y - \text{shifts})$
0	1	$h_{0,1}(xX, yY) = e^2 yY$
1	1	$h_{1,1}(xX, yY) = xX yYe A - yYe + xxy^2 Y^2 e$
2	1	$h_{1,2}(xX, yY) = -2xX yY A + 2x^2 X^2 y^2 Y^2 A + yY - 2xX y^2 Y^2 + x^2 X^2 y^3 Y^3$

When $m = 2$ and $t = 1$ the lattice is spanned by the rows of the matrix in the following Table.

		1	x	xy	x^2	x^2y	x^2y^2	y	xy^2	x^2y^3
$i + k = 0$	$g_{0,0}$	e^2	0	0	0	0	0	0	0	0
$i + k = 1$	$g_{1,0}$	0	$e^2 X$	0	0	0	0	0	0	0
	$g_{0,1}$	$-e$	eAX	eXY	0	0	0	0	0	0
$i + k = 2$	$g_{2,0}$	0	0	0	$e^2 X^2$	0	0	0	0	0
	$g_{1,1}$	0	$-eX$	0	eAX^2	eX^2Y	0	0	0	0
	$g_{0,2}$	1	$-2AX$	$-2XY$	$A^2 X^2$	$2AX^2Y$	$X^2 Y^2$	0	0	0
$k + j = 1$	$h_{1,0}$	0	0	0	0	0	0	$e^2 Y$	0	0
$k + j = 2$	$h_{1,1}$	0	0	$eAXY$	0	0	0	$-eY$	eXY^2	0
$k + j = 3$	$h_{1,2}$	0	0	$-2AXY$	0	$A^2 X^2 Y$	$2AX^2 Y^2$	Y	$-2XY^2$	$X^2 Y^3$

Table 3.1: The matrix spanned by x and y shifts for $m = 2$ and $t = 1$.

Let \mathcal{L}_{BD} denote the lattice and \mathcal{B}_{BD} be the corresponding basis. Running LLL algorithm there are two short vectors b_1, b_2 that satisfy $\|b_1\|, \|b_2\| \leq 2^{\frac{n}{2}} \det(\mathcal{L}_{BD})^{\frac{1}{n-1}}$ where n is the dimension of the lattice. For the hypothesis of Howgrave-Graham's lemma, $\det(\mathcal{L}_{BD})$ is such that

$$2^{\frac{n}{2}} \det(\mathcal{L}_{BD})^{\frac{1}{n-1}} \leq \frac{e^m}{\sqrt{(n)}}.$$

Now as the determinant and the dimension of the lattice \mathcal{L}_{BD} satisfy the following respectively

$$\begin{aligned} \det(\mathcal{L}_{BD}) &= e^{\frac{5+4\delta}{m} + \frac{3+2\delta}{4}tm^2} + \frac{mt^2}{4} + o(m^3) \text{ and} \\ n &= \frac{m^2}{2} + tm + o(m^2). \end{aligned}$$

Substituting these values in the above inequality and optimizing with respect to t and ignoring low degree terms, the condition is on δ given as $12 - 12\delta^2 + 28\delta - 7 < 0$, i.e., $\delta < \frac{7}{6} - \frac{1}{3}\sqrt{7} \approx 0.284$. This means that if $\delta < 0.284$ or, equivalently if $d < N^{0.284}$ by repeating the Howgrave-Graham argument as in Theorem 3.1.1 to bivariate polynomial $f(x, y)$ there are two polynomials $g_1(x, y)$ and $g_2(x, y)$ constructed using the vectors b_1 and b_2 respectively. Note as the common integer solution of $g_1(x, y)$ and $g_2(x, y)$ are all modular solutions of $f(x, y) \equiv (0 \pmod{e})$ and the common solutions of $g_1(x, y)$ and $g_2(x, y)$ are obtained by finding the resultant $r(x)$ or $r(y)$ of $g_1(x, y)$ and $g_2(x, y)$. Then for any solution x_0 of $r(x)$ substituting in $g_1(x, y)$ and $g_2(x, y)$ a common solution (x_0, y_0) of $g_1(x, y)$ and $g_2(x, y)$ gives rise to $f(x_0, y_0) \equiv 0 \pmod{e}$ and this solution leads to the factorization of N .

Improved bounds:

The results in the above show that the small inverse problem can be solved when

$\delta < 0.284$. The bound is derived from the determinant of the lattice L , which gives an upper bound on the lengths of the shortest vectors of the lattice. In the above, we compute the determinant of a lattice L generated by shifts and powers of f . Since L is full rank and corresponding matrix is triangular, the determinant is just the product of the entries on the diagonal-carefully balanced so that this product is less than 1. Once $\delta > 0.284$ the approach no longer works, as the product exceeds 1 for every choice of m . But if the some of the larger terms of this product were removed, we might be able to find greater values of δ . This suggests that one can ignore some rows which have large diagonal values. But unfortunately the resulting lattice is not of full rank, and computing its determinant is not easy, Boneh-Durfee used the theorem on “Geometric progressive matrices” to obtain the determinant of the lattice and improve the bound to 0.292.

Boneh and Durfee also note that using $t = 0$, that is only x -shifts are used to construct a lattice basis, one obtains an attack working for $d < N^{0.25}$. This reproduces Wiener’s result.

3.3 An Attack on RSA, Based on Lattice Basis Reduction with Lower Dimension by Blömer and May

Blömer and May revisited the above attack [3]. They come up with the bound 0.290. Even though it is slightly less than Boneh and Durfee’s bound, analysis is much simpler than Boneh and Durfee. They begin their analysis by choosing pa-

rameters m, t and then construct exactly the same lattice as Boneh and Durfee, before removal the rows with corresponding basis of \mathcal{B}_{BD} . Next they remove certain rows of \mathcal{B}_{BD} to take an intermediate matrix \bar{B} . Let $\bar{\mathcal{L}}$ be the lattice spanned by \bar{B} . Unlike Boneh-Durfee, they go on removing an equal number of columns in order to obtain a square matrix. We denote the final matrix constructed by Blömer and May as \mathcal{B}_{BM} and the corresponding lattice \mathcal{L}_{BM} . The row vectors of the matrix \mathcal{B}_{BM} are no longer the coefficient vectors of the polynomials $g_{i,k}(x, y)$ and $h_{j,k}(x, y)$ since they have removed some columns from the initial basis matrix \mathcal{B}_{BD} . Notice that the basis constructed by Boneh and Durfee does not suffer from the same drawback since they have only removed rows but not columns. In order to apply Howgrave's theorem, it is necessary to ensure that the linear combination of bivariate polynomials evaluates to zero modulo e^m . Blömer and May show how to associate the rows of matrix with the polynomials $g_{i,k}$ and $h_{j,k}$. This means that they show how to reconstruct a vector $\bar{u} \in \bar{\mathcal{L}}$ by a vector $u \in \mathcal{L}_{BM}$. More significantly, they prove that short vectors $u \in \mathcal{L}_{BM}$ lead to short reconstruction vector $\bar{u} \in \bar{\mathcal{L}}$ i.e., the size of small vectors found in the eliminated lattice \mathcal{L}_{BM} by LLL is the same size as those found in the original lattice $\bar{\mathcal{L}}$ up to a small correction term.

Steps in construction of the new lattice \mathcal{L}_{BM} with basis \mathcal{B}_{BM} by Blömer-May is described in the following:

1. Choose lattice parameters m and t and build the Boneh-Durfee lattice basis \mathcal{B}_{BD}
2. Label the coefficient vectors of the polynomials $g_{i,k}(xX, yY)$ as the X - block, the block X_l consist of the $l + 1$ coefficient vectors of $g_{i,k}$ with $i + k = l$ and

$X_{l,k}$, that is the k -th vectors in the X_l block is the coefficient vector of $g_{l-k,k}$.

Similarly, define the blocks Y, Y_j and $Y_{j,k}$.

3. In the Y_t block of the basis \mathcal{B}_{BD} remove every vector except for the last vector $Y_{t,m}$, in the Y_{t-1} block remove every vector except for the last two vectors $Y_{t,m-1}$ and $Y_{t,m}$, and so on. Finally, in the Y_1 block remove every vector except for the last t vectors Y_{m-t+1}, \dots, Y_m .
4. Remove every vector in the X -block except for the vectors in the $t+1$ blocks $X_{m-t}, X_{m-t+1}, \dots, X_m$.
5. All column vectors with label $x^l y^j, l \geq j$, form the $X^{(l)}$ column block. Analogously, define the $Y^{(l)}$ column block to consist of all column vectors labeled with $x^i y^{i+l}$.
6. Delete columns in such a way that the resulting basis is again triangular. That is, remove all column blocks $X^{(0)}, X^{(1)}, \dots, X^{(m-t-1)}$. Furthermore in the column block $Y^{(l)}, l = 1, \dots, t$, remove the columns labeled with $x^i y^{i+l}$ for $0 \leq i < m - t + l$.

This construction leads to a triangular basis \mathcal{B}_{BM} of a new lattice \mathcal{L}_{BM} , which will be used in this approach. As opposed to Boneh and Durfee, this attack do not remove y -shifts alone to improve the bound $\delta < 0.284$, instead remove some x -shifts and corresponding columns as well, which retains a square lower triangular matrix and helps in the computation of the determinant of the lattice.

Example of Blömer and May lattice for $m = 2$ and $t = 1$:

Blocks		$X^{(0)}$	$X^{(1)}$	$X^{(1)}$	$X^{(2)}$	$X^{(2)}$	$X^{(2)}$	$Y^{(1)}$	$Y^{(1)}$	$Y^{(1)}$
		1	x	xy	x^2	x^2y	x^2y^2	y	xy^2	x^2y^3
X_0	$g_{0,0}$	e^2	0	0	0	0	0	0	0	0
X_1	$g_{1,0}$	0	e^2X	0	0	0	0	0	0	0
	$g_{0,1}$	$-e$	eAX	eXY	0	0	0	0	0	0
X_2	$g_{2,0}$	0	0	0	e^2X^2	0	0	0	0	0
	$g_{1,1}$	0	$-eX$	0	eAX^2	eX^2Y	0	0	0	0
	$g_{0,2}$	1	$-2AX$	$-2XY$	A^2X^2	$2AX^2Y$	X^2Y^2	0	0	0
Y_1	$h_{1,0}$	0	0	0	0	0	0	e^2Y	0	0
Y_2	$h_{1,1}$	0	0	$eAXY$	0	0	0	$-eY$	eXY^2	0
Y_3	$h_{1,2}$	0	0	$-2AXY$	0	A^2X^2Y	$2AX^2Y^2$	Y	$-2XY^2$	X^2Y^3

Table 3.2: Blömer-May matrix for $m = 2$ and $t = 1$.

Remove the shaded rows and columns of the matrix, whose rows spans the lattice \mathcal{L}_{BD} in the above figure to get a new matrix and its rows spans the new lattice \mathcal{L}_{BM} , for $m = 2$ and $t = 1$.

This attack does not improve the bound $d < N^{0.292}$ of Boneh and Durfee's result but it has several advantages. First, the lattice dimension is reduced. Therefore, in practice we are able to get closer to the theoretical bounds. Second, the new lattice basis is triangular. This leads to rather simple proofs.

3.4 An Attack on RSA with Small Prime Difference $p - q$, Based on Lattice Basis Reduction by B de Weger

Based on lattice based techniques Boneh and Durfee improved the Wiener's bound for $d = N^\delta$ from 0.25 to 0.284 and improved their bounds up to 0.292 using the strategy of Geometrically progressive matrices. In this section we describe the extension of Boneh and Durfee's result by B de Weger to the case of small prime difference based on Lattice-based techniques. In the paper [47], B de Weger shown that the first result of Boneh and Durfee can be improved to $\delta < \frac{1}{6}(4\beta + 5) - \frac{1}{3}\sqrt{(4\beta + 5)(4\beta - 1)}$ and the second result of Boneh and Durfee can be improved to $\delta < 1 - \sqrt{2\beta - \frac{1}{2}}$ under the condition $\delta > 2 - 4\beta$, for the prime difference $p - q = N^\beta$ in the direction of Boneh and Durfee.

Boneh-Durfee considered the polynomial congruence $-k(A - s) \equiv 1 \pmod{e}$ for $A = N + 1$, $s = p + q$ and e^δ and $e^{\frac{1}{2}}$ are the upper bounds for the solution of this congruence $p + q$ and k respectively ($e \approx N$). Instead of taking $A = N + 1$ and $s = p + q$, B de Weger considered $A = N + 1 - \lceil 2\sqrt{N} \rceil$ and $s = p + q - \lceil 2\sqrt{N} \rceil$ and in this case $-k(A - s) \equiv 1 \pmod{e}$. The upper bound for s is such that $e^{2\beta - \frac{1}{2}}$ and is follows from the below given theorem.

Theorem 3.4.1. If $N = pq$ and $\Delta = p - q$ then

$$0 < p + q - 2\sqrt{N} < \frac{\Delta^2}{4\sqrt{N}}.$$

Apply the same analysis given in the Boneh-Durfee's first result to solve the small inverse problem for the polynomial congruence $-k(A - s) \equiv 1 \pmod{e}$ for $A = N + 1 - \lceil 2\sqrt{N} \rceil$, $s = p + q - \lceil 2\sqrt{N} \rceil$ and $|s| < e^{2\beta - \frac{1}{2}}$, $|k| < e^\delta$ to get the attack bounds for δ is such that

$$\delta < \frac{1}{6}(4\beta + 5) - \frac{1}{3}\sqrt{(4\beta + 5)(4\beta - 1)}.$$

The second result of Boneh-Durfee's improved version using the sublattice technique can be extended under the condition $\delta > 2 - 4\beta$ as the (iv) condition of geometrically progressive matrices satisfied for the matrix of sublattice of L (given in Boneh-Durfee's second result [5]) only if $\delta > 2 - 4\beta$ and the attack bound is

$$2 - 4\beta < \delta < 1 - \sqrt{2\beta - \frac{1}{2}}.$$

Note that in this extension the Boneh and Durfee's attack bounds on RSA improved only if the prime difference $p - q$ is essentially smaller than $N^{\frac{1}{2}}$.

3.5 An Attack on RSA with Small Difference

$p - \rho q$, for ρq a Better Approximation of p ,

Based on Lattice Basis Reduction by

Maitra-Sarkar

B de Weger gave an attack bounds for RSA using lattice based techniques in the direction of Boneh-Durfee's first and second results when the prime difference $p - q$

is bounded. Subhamoy Maitra-Santanu Sarkar gave an attack bounds not only using the idea of Boneh-Durfee(both results) and also used sub lattice based techniques given by Blömer - May when $\rho q - p$ is bounded for ρ is such that $1 \leq \rho \leq 2$ and ρq is a better approximation for p .

Consider the polynomial congruence $1 + x(A + y) \equiv 0 \pmod{e}$ for $A = N + 1 - \left(\sqrt{\rho} + \frac{1}{\sqrt{\rho}}\right) \sqrt{N}$ with the solutions $x = x_0 = k$ and $y = y_0 = -(p + q - \left(\sqrt{\rho} + \frac{1}{\sqrt{\rho}}\right))$. For $e = N$ and $d = N^\delta$, e^δ is an upper bound for the solution x_0 and from the Proposition 2.2.5 e^γ is an upper bound for y_0 for $|p - \rho q| \leq \frac{N^\gamma}{16}$, where $\gamma \leq \frac{1}{2}$. The attack bounds for δ are given by implementing the analysis of Boneh-Durfee in their first and second results and Blömer - May to the above polynomial congruence in the following respectively [31]

$$\begin{aligned} \delta &< \frac{\gamma + 3 - 2\sqrt{\gamma(\gamma + 3)}}{3}; \\ 1 - 2\gamma &< \delta < 1 - \sqrt{\gamma}; \\ \delta &< \frac{\sqrt{16\gamma^2 - 4\gamma + 4} - (6\gamma - 2)}{5}. \end{aligned}$$

3.6 An Attack on RSA with a Composed Decryption Exponent, Based on Lattice Basis Reduction by Nitaj-Douh

In this section, we describe a new attack on RSA proposed by A. Nitaj and M.O. Douh [35], when the private exponent is in the form $d = Md_1 + d_0$ with a known

integer M and suitably small unknown integers d_1 and d_2 by using the extended strategy of Jochemsz and May for finding roots of multivariate polynomials [3]. In 2000, Boneh and Durfee presented an attack on RSA when $d < N^{0.292}$. When $d = Md_1 + d_0$, this attack enables one to overcome Boneh and Durfees bound and to factor the RSA modulus.

Suppose d is composed as $d = Md_1 + d_0$ where M is known and d_1 and d_0 are unknown, then this result shows that one can find the factorization of N if d_1 and d_0 are suitably small and the result as follows.

Let $e = N^\alpha$, $M = N^\beta$, $d_1 < N^\delta$, $d_0 < N^\gamma$. If

$$\delta < \frac{1}{4}(5 - 4\gamma - \sqrt{12\alpha + 12\beta - 12\gamma + 3}),$$

then there is a polynomial time algorithm to factor the modulus N , which breaks the RSA cryptosystem and is given in the Theorem 3.6.1. The starting point of the attack is the key equation

$ed - k\varphi(N) = 1$, which can be rewritten as

$$ed_0 - kN + k(p + q - 1) - 1 = 0 \pmod{Me}.$$

From the left side, a polynomial $f(x, y, z) = ex - Ny + yz - 1$ is derived and note $(x_0, y_0, z_0) = (d_0, k, p + q - 1)$ is a solution of the modular equation $f(x, y, z) = 0 \pmod{Me}$ and N^γ , $2N^{\alpha+\beta+\delta-1}$ and $\frac{3\sqrt{2}}{2}N^{\frac{1}{2}}$ are the upper bounds for x_0 , y_0 and z_0 respectively. When the LLL algorithm is applied, three polynomials $h_i(x, y, z)$ for $1 \leq i \leq 3$ are obtained and since $(d_0, k, p + q - 1)$ is a small solution of the equation $f(x, y, z) = 0 \pmod{Me}$, then using the resultant process there is z_0 such that $z_0 = p + q - 1$. Hence using $p + q - 1 = z_0$ and $pq = N$, one can find p and q . Therefore this is the argument for lattice attack due to Nitaj-Douh as given in the following theorem.

Theorem 3.6.1. Let $N = pq$ be an RSA modulus with $q < p < 2q$. Let $M = N^\beta$ be a positive integer and $e = N^\alpha$ a public exponent satisfying $ed - k\varphi(N) = 1$ with $d = Md_1 + d_0$. Suppose that $d_1 \leq N^\delta$ and $d_0 < N^\gamma$. Then one can factor N in polynomial time if $\delta < \frac{1}{4}(5 - 4\gamma - \sqrt{12\alpha + 12\beta - 12\gamma + 3})$.

This review on lattice attacks of RSA with low decryption exponent d is depicted in a tabular form describing the refinement process of RSA attack bounds in the following.

Attack	Based on theory	Refining the RSA attack bounds
Boneh and Durfee's attack	Lattice based techniques	$d < N^{0.284}$, for $e \approx N$.
Boneh and Durfee's attack	Sublattice based techniques	$d < N^{0.292}$, for $e \approx N$.
Blömer and May's attack	Sublattice based techniques with lower dimension	$d < N^{0.290}$, for $e \approx N$.
Weger's attack	Lattice based techniques	$d < N^{\frac{1}{6}(4\beta+5) - \frac{1}{3}\sqrt{(4\beta+5)(4\beta-1)}}$, for $e \approx N$ and $N^\beta = p - q $.
Weger's attack	Sublattice based techniques	$N^{2-4\beta} < d < N^{1-\sqrt{2\beta-\frac{1}{2}}}$, for $e \approx N$ and $N^\beta = p - q $.
Maitra- Sarkar's attack	Lattice based techniques	$d < N^{\frac{\gamma+3-2\sqrt{\gamma+3}}{3}}$, for $e \approx N$ and $ p - \rho q \leq \frac{N^\gamma}{16}$, where $\gamma \leq \frac{1}{2}$ and $1 \leq \rho \leq 2$.
Maitra- Sarkar's attack	Sublattice based techniques	$N^{1-2\gamma} < d < N^{1-\sqrt{\gamma}}$, for $e \approx N$ and $ p - \rho q \leq \frac{N^\gamma}{16}$, where $\gamma \leq \frac{1}{2}$ and $1 \leq \rho \leq 2$.
Maitra- Sarkar's attack	Sublattice based techniques with lower dimension	$d < N^{\frac{\sqrt{16\gamma^2-4\gamma+4-(6\gamma-2)}}{5}}$, for $e \approx N$ and $ p - \rho q \leq \frac{N^\gamma}{16}$, where $\gamma \leq \frac{1}{2}$ and $1 \leq \rho \leq 2$.
Nitaj and Douh's attack	Lattice based techniques	$d = Md_1 + d_0$, $\delta < \frac{1}{4}(5 - 4\gamma - \sqrt{12\alpha + 12\beta - 12\gamma + 3})$, for $e = N^\alpha$, $d_1 < N^\delta$ and $d_0 < N^\beta$.

Table 3.3: Refinement process of RSA attack bounds on decryption exponent d .

In the next section it is noted that these lattice attacks can be extended to RSA-like cryptosystem on elliptic curves due to KMOV.

3.7 Extending Lattice-Based Attacks to an RSA-Like Cryptosystem over $E(\mathbb{Z}_{pq})$

All the lattice-based attacks on RSA for small decryption exponent may be extended to RSA-like cryptosystem over elliptic curves $E(\mathbb{Z}_{pq})$ due to KMOV by repeating the argument for $\varphi(N)$ replaced by $\psi(N)$ for $\psi(N) = (p + 1)(q + 1)$.

Lattice-based attack given by Boneh-Durfee and Blömer-May on RSA can be extended to RSA-like cryptosystem over elliptic curves $E(\mathbb{Z}_{pq})$ due to KMOV, according to the polynomial congruence as in the following

Boneh-Durfee and Blömer-May	RSA	RSA-like over $E(\mathbb{Z}_{pq})$ due to KMOV
Polynomial Congruence	$x(A + y) - 1 \equiv 0 \pmod{e}$ where $A = N + 1$.	$x(A + y) - 1 \equiv 0 \pmod{e}$ where $A = N + 1$.
Solution	$\left(-\frac{ed-1}{\varphi(N)}, -(p+q)\right)$.	$\left(-\frac{ed-1}{\psi(N)}, (p+q)\right)$.

note as the monomials and upper bounds for solutions are same for both the polynomials with respect to $\varphi(N)$ and $\psi(N)$, the arguments of Boneh-Durfee and Blömer-May can be repeated for $\varphi(N)$ replaced by $\psi(N)$ then it is observed that RSA and RSA-like have same attack bound for δ , given as $\delta < 0.292$ and $\delta < 0.29$ respectively

for $d = N^\delta$ and $e \approx N$.

Lattice-based attack given by B de Weger on RSA can be extended to RSA-like cryptosystem over elliptic curves $E(\mathbb{Z}_{pq})$, according to the polynomial congruence as in the following

Weger	RSA	RSA-like over $E(\mathbb{Z}_{pq})$ due to KMOV
Polynomial Congruence	$x(A + y) - 1 \equiv 0 \pmod{e}$ where $A = N + 1 - \lceil 2\sqrt{N} \rceil$.	$x(A + y) - 1 \equiv 0 \pmod{e}$ where $A = N + 1 + \lceil 2\sqrt{N} \rceil$.
Solution	$\left(-\frac{ed-1}{\varphi(N)}, -(p+q - \lceil 2\sqrt{N} \rceil)\right)$.	$\left(-\frac{ed-1}{\psi(N)}, (p+q - \lceil 2\sqrt{N} \rceil)\right)$.

note as the monomials and upper bounds for solutions are same for both the polynomials with respect to $\varphi(N)$ and $\psi(N)$, the argument of B de Weger can be repeated for $\varphi(N)$ replaced by $\psi(N)$ then it is observed that RSA and RSA-like have same attack bounds for δ , given as $\delta < \frac{1}{6}(4\beta + 5) - \frac{1}{3}\sqrt{(4\beta + 5)(4\beta - 1)}$ and $2 - 4\beta < \delta < 1 - \sqrt{2\beta - \frac{1}{2}}$ for $p - q = N^\beta$ and $d = N^\delta$.

Lattice-based attack given by Maitra-Sarkar on RSA can be extended to RSA-like cryptosystem over elliptic curves $E(\mathbb{Z}_{pq})$ due to KMOV, according to the polynomial congruence as in the following

Maitra-Sarkar	RSA	RSA-like over $E(\mathbb{Z}_{pq})$ due to KMOV
Polynomial Congruence	$x(A + y) + 1 \equiv 0 \pmod{e}$ where $A = N + 1 - \left(\sqrt{\rho} + \frac{1}{\sqrt{\rho}}\sqrt{N}\right)$.	$x(A + y) + 1 \equiv 0 \pmod{e}$ where $A = N + 1 + \left(\sqrt{\rho} + \frac{1}{\sqrt{\rho}}\sqrt{N}\right)$.
Solution	$\left(\frac{ed-1}{\varphi(N)}, -\left(p + q - \left(\sqrt{\rho} + \frac{1}{\sqrt{\rho}}\sqrt{N}\right)\right)\right)$.	$\left(\frac{ed-1}{\psi(N)}, \left(p + q - \left(\sqrt{\rho} + \frac{1}{\sqrt{\rho}}\sqrt{N}\right)\right)\right)$.

note as the monomials and upper bounds for solutions are same for both the polynomials with respect to $\varphi(N)$ and $\psi(N)$, the argument of Maitra-Sarkar can be repeated for $\varphi(N)$ replaced by $\psi(N)$ then it is observed that RSA and RSA-like have same attack bounds for δ , given as $\delta < \frac{\gamma+3-2\sqrt{\gamma(\gamma+3)}}{3}$, $1 - 2\gamma < \delta < 1 - \sqrt{\gamma}$ and $\delta < \frac{\sqrt{16\gamma^2-4\gamma+4-(6\gamma-2)}}{5}$ for $|p - \rho q| \leq \frac{N\gamma}{16}$, where $1 \leq \rho \leq 2$ and $\gamma \leq \frac{1}{2}$.

Lattice-based attack given by Nitaj-Douh on RSA can be extended to RSA-like cryptosystem over elliptic curves $E(\mathbb{Z}_{pq})$ due to KMOV, according to the polynomial congruence as in the following

Nitaj-Douh	RSA	RSA-like over $E(\mathbb{Z}_{pq})$ due to KMOV
Polynomial Congruence	$ex - Ny + yz - 1 \equiv 0 \pmod{Me}$ where $d = Md_1 + d_0$.	$ex - Ny + yz - 1 \equiv 0 \pmod{Me}$ where $d = Md_1 + d_0$.
Solution	$(d_0, k, p + q - 1)$.	$(d_0, k, -(p + q + 1))$.

note as the monomials and upper bounds for solutions are same for both the polynomials with respect to $\varphi(N)$ and $\psi(N)$, the argument of Nitaj-Douh using the strategy given by Jochemsz-May for finding roots of multivariate polynomials can be repeated for $\varphi(N)$ replaced by $\psi(N)$, then it is observed that RSA and RSA-like

have same attack bound for δ , given as $\delta < \frac{1}{4}(5 - 4\gamma - \sqrt{12\alpha + 12\beta - 12\gamma + 3})$ for $d = N^\delta$ and for the decryption exponent is of the form $d = Md_1 + d_0$ with known integer M and suitably small unknown integers d_1 and d_0 .

3.8 Summary

In this chapter, attacks based on lattice-based techniques for RSA with small decryption exponent are analyzed. M.J. Wiener used continued fraction algorithm to find sufficiently short RSA secret exponents in polynomial time for $d < N^{0.25}$ and when $e > N^{1.5}$ as continued fraction algorithm is not guaranteed to work. Boneh-Durfee attack is analyzed and noted that Boneh-Durfee proposed their work, as an application of Coppersmith's techniques to bivariate modular polynomial and their approach is efficient as long as $e < N^{1.875}$ and $d < N^{0.292}$. Attack by J. Blömer and A. May is analyzed and noted that J. Blömer and A. May proposed an algorithm to find an attack on RSA for $d < N^{0.29}$ and this bound for d is slightly worse than Boneh-Durfee's bound for d but this algorithm was several times faster due to the reduced lattice dimension. After that attack by Benne de Weger is analyzed and noted that B de Weger shown that choosing an RSA modulus with a small difference $p - q$ of its prime factors yields improvements on the small private exponent attacks of Wiener and Boneh-Durfee. Next refinement by Subhamoy Maitra and Santanu Sarkar is analyzed and noted that Maitra-Sarkar considered the difference $p - \rho q$, for ρq a better approximation for p instead of considering the prime difference $p - q$ and gave an attack bound for d . Further analyzed the attack by A.Nitaj and M.O.Douh. It is observed that the method given by A.Nitaj and M.O.Douh, enables us to find the private exponent d even when $d > N^{0.292}$ depending on the possibility that d

has the composed form $d = Md_1 + d_0$ for a suitable known integer M and suitable unknown parameters d_1 and d_0 . These results show that one should be more careful when using RSA with small and special private exponent. It is observed that all the lattice based attacks on RSA discussed here can be extended to an RSA-like cryptosystem over elliptic curves $E(\mathbb{Z}_{pq})$ due to KMOV and the corresponding analysis is given.

Chapter 4

Cryptanalysis Based on Lattice-Based Techniques, for RSA with Small Multiplicative Inverse of $(p - 1)$ or $(q - 1)$ Modulo e

In this chapter, we mount an attack on RSA by using lattice based techniques implemented in the case when $p - 1$ or $q - 1$ have small multiplicative inverse less than or equal to N^δ modulo the public encryption exponent e , for some small δ and described the attack bounds for δ . Also we noted that all these Lattice-based attacks on RSA can be extended to the RSA-like cryptosystem over $E(\mathbb{Z}_{pq})$ due to KMOV.

4.1 Cryptanalysis of RSA and an Attack Bound Using Lattice Based Techniques

In this section we describe how a small multiplicative inverse of $(p - 1)$ or $(q - 1)$ modulo e results a new weakness for RSA by using the lattice reduction techniques

as in [5] by Boneh-Durfee and in [3] by Blömer-May.

Let $N = pq$, $q < p < 2q$, e be the public encryption exponent and d be the private decryption exponent. The public encryption exponent e and $\varphi(N)$ are relatively prime so for $e > p - 1$ there exist unique r, s such that

$$(p - 1)r \equiv 1 \pmod{e} \text{ and } (q - 1)s \equiv 1 \pmod{e} \quad (4.1.1)$$

and note r, s are the multiplicative inverses of $p - 1, q - 1$ respectively. Now let $f(x, y) = x(y + A) - 1$ for $A = \lceil \sqrt{N} \rceil - 1$. If $x_0 = r$ then for $y_0 = p - \lceil \sqrt{N} \rceil$ we have $f(x_0, y_0) \equiv 0 \pmod{e}$ and if $x_0 = s$ then for $y_0 = q - \lceil \sqrt{N} \rceil$ we have $f(x_0, y_0) \equiv 0 \pmod{e}$ by using (4.1.1). Now for $|x_0| \leq N^\delta, |y_0| \leq N^\gamma$ for some δ and γ note $N^\gamma = |\rho - 1|\sqrt{N}, 1 < \rho < \sqrt{2}$ if $y_0 = p - \lceil \sqrt{N} \rceil$ and $N^\gamma = |\rho - 1|\sqrt{N}, \frac{1}{\sqrt{2}} < \rho < 1$ if $y_0 = q - \lceil \sqrt{N} \rceil$ by using the inequality $\frac{\sqrt{2}\sqrt{N}}{2} < q < \sqrt{N} < p < \sqrt{2}\sqrt{N}$ in [34] (observe that $p - \lceil \sqrt{N} \rceil \pmod{e} \leq p - \lceil \sqrt{N} \rceil, \lceil \sqrt{N} \rceil - q \pmod{e} \leq \lceil \sqrt{N} \rceil - q$ and $(r, p - \lceil \sqrt{N} \rceil \pmod{e})$ and $(s, -(\lceil \sqrt{N} \rceil - q) \pmod{e})$ are also solutions but in this case $p - \lceil \sqrt{N} \rceil \pmod{e} = p - \lceil \sqrt{N} \rceil$ and $\lceil \sqrt{N} \rceil - q \pmod{e} = \lceil \sqrt{N} \rceil - q$ as $e > p - 1$).

Now we consider the polynomial $f(x, y) = x(y + A) - 1$ and find (x_0, y_0) satisfying: $f(x_0, y_0) \equiv 0 \pmod{e}$, for $e = N^\alpha, |x_0| \leq N^\delta$ and $|y_0| \leq N^\gamma$, with

$N^\gamma = |\rho - 1|\sqrt{N}$ such that ρ is in the range

$$\begin{cases} \frac{1}{\sqrt{2}} < \rho < 1, & \text{if } x_0 = s, y_0 = q - \lceil \sqrt{N} \rceil \\ 1 < \rho < \sqrt{2}, & \text{if } x_0 = r, y_0 = p - \lceil \sqrt{N} \rceil. \end{cases}$$

To solve for the above (x_0, y_0) we use lattice based techniques to our polynomial and the upper bounds $X = N^\delta, Y = N^\gamma$ as in [5]:

For given a positive integer m , define the polynomials

$$g_{i,k} = x^i f^k(x, y) e^{m-k} \text{ and}$$

$$h_{j,k} = y^j f^k(x, y) e^{m-k},$$

referred as the x -shifts and y -shifts respectively. Now define the lattice \mathcal{L} spanned by the coefficients of the vectors $g_{i,k}(xX, yY)$ and $h_{j,k}(xX, yY)$ for $k = 0, \dots, m$, $i = 0, \dots, m - k$ and $j = 0, \dots, t$. Note that the matrix M of \mathcal{L} is lower triangular and the coefficient of the leading monomial of $g_{i,k}(xX, yY)$ is $X^{i+k} Y^k e^{m-k}$ and also the coefficient of the leading monomial of $h_{i,k}(xX, yY)$ is $X^k Y^{j+k} e^{m-k}$, so the determinant is

$$\det(\mathcal{L}) = e^{n_e} X^{n_X} Y^{n_Y}$$

where

$$n_e = \sum_{k=0}^m \sum_{i=0}^{m-k} (m-k) + \sum_{k=0}^m \sum_{j=1}^t (m-k)$$

$$= \frac{m(m+1)(m+2)}{3} + \frac{tm(m+1)}{2},$$

$$n_X = \sum_{k=0}^m \sum_{i=0}^{m-k} (i+k) + \sum_{k=0}^m \sum_{j=1}^t k$$

$$= \frac{m(m+1)(m+2)}{3} + \frac{tm(m+1)}{2},$$

$$n_Y = \sum_{k=0}^m \sum_{i=0}^{m-k} k + \sum_{k=0}^m \sum_{j=1}^t (j+k)$$

$$= \frac{m(m+1)(m+2)}{6} + \frac{t(m+1)(m+t+1)}{2}$$

and the dimension of \mathcal{L} is

$$\begin{aligned} w &= \sum_{k=0}^m \sum_{i=0}^{m-k} 1 + \sum_{k=0}^m \sum_{j=1}^t 1 \\ &= \frac{(m+1)(m+2)}{2} + t(m+1). \end{aligned}$$

Applying the LLL algorithm we can obtain two short vectors b_1, b_2 and by using Theorem 1.7.23 & 1.7.24 this vectors satisfies

$$\|b_1\|, \|b_2\| \leq 2^{w/2} \det(\mathcal{L})^{\frac{1}{w-1}}.$$

Now in order to apply Howgrave-Graham's theorem, we should have

$$2^{\frac{w}{2}} \det(\mathcal{L})^{\frac{1}{w-1}} < \frac{e^m}{\sqrt{w}}.$$

From this, we deduce

$$\det(\mathcal{L}) < \frac{1}{(2^{\frac{w}{2}})^{w-1}} e^{m(w-1)} < e^{mw}$$

To satisfy the above inequality we need the following inequality

$$e^{n_e} X^{n_X} Y^{n_Y} < e^{mw}.$$

Substitute all values and taking logarithms, neglecting the low order terms and after simplifying we get

$$m^3 \left(\frac{2\alpha + 2\delta + \gamma}{6} \right) + tm^2 \left(\frac{\alpha + \delta + \gamma}{2} \right) + mt^2 \left(\frac{\gamma}{2} \right) < \alpha \left(\frac{1}{2}m^3 + tm^2 \right)$$

This leads to

$$m^2 \left(\frac{-\alpha + 2\delta + \gamma}{6} \right) + tm \left(\frac{\gamma + \delta - \alpha}{2} \right) + t^2 \left(\frac{\gamma}{2} \right) < 0.$$

After fixing an m , the left hand side is minimized at $t = \frac{\alpha - \delta - \gamma}{2\gamma}m$. Putting this value we get the inequality

$$\delta < \frac{3\alpha + \gamma - 2\sqrt{\gamma(3\alpha + \gamma)}}{3}.$$

From the vectors b_1 and b_2 we obtain two polynomials $g_1(x, y)$ and $g_2(x, y)$ over \mathbb{Z} such that $g_1(x_0, y_0) = g_2(x_0, y_0) = 0$. Let $h(x)$ be the resultant polynomial of $g_1(x, y)$ and $g_2(x, y)$ with respect to y . By Remark 1.3.34, $h(x)$ is not identically zero. Now note if r or s are small such that $|s|$ or $|r| \leq N^\delta$ for $\delta < \frac{3\alpha + \gamma - 2\sqrt{\gamma(3\alpha + \gamma)}}{3}$ then $(r, p - \lceil \sqrt{N} \rceil)$ or $(s, q - \lceil \sqrt{N} \rceil)$ are also common solutions of $g_1(x, y)$ and $g_2(x, y)$, therefore either $y_0 = p - \lceil \sqrt{N} \rceil$ or $y_0 = q - \lceil \sqrt{N} \rceil$ is a root of $g_1(x_0, y)$ for $x_0 = r$ or s , a solution for $h(x)$ and with this knowledge of y_0 the factorization of N is known.

Theorem 4.1.1. Let $N = pq$ be an RSA modulus with $q < p < 2q$. Let $e = N^\alpha$, $X = N^\delta$ and $Y = N^\gamma$, $N^\gamma = |\rho - 1|\sqrt{N}$ where ρ in the range

$$\begin{cases} 1 < \rho < \sqrt{2}, & \text{if } x_0 = r, y_0 = p - \lceil \sqrt{N} \rceil \\ \frac{1}{\sqrt{2}} < \rho < 1, & \text{if } x_0 = s, y_0 = q - \lceil \sqrt{N} \rceil, \end{cases} \quad \text{and } r, s \text{ are the multiplicative inverses}$$

of $p - 1, q - 1$ modulo e respectively. Suppose that $|x_0| \leq X$ and $|y_0| \leq Y$ then one can factor N in polynomial time if

$$\delta < \frac{3\alpha + \gamma - 2\sqrt{\gamma(3\alpha + \gamma)}}{3}.$$

Proof. Follows from the above argument and the LLL lattice basis reduction algo-

rithm operates in polynomial time [29]. ■

Corollary 4.1.2. If the lattice basis reduction algorithm is implemented only using x -shifts and repeating the above argument then we can factorize N whenever

$$\delta < \frac{\alpha - \gamma}{2}.$$

Note that this RSA attack does not depend on the private decryption exponent d . Sometimes our attack may work if d is exceeding the bound given by Boneh and Durfee. For a given $e = N^\alpha$ and for $d = N^{\delta'}$, $p - q = N^\beta$, the prime difference, the Boneh-Durfee's bound for δ' (in the first result) is given by $\delta' < \frac{5}{6} + \frac{2}{3}\beta - \frac{1}{3}\sqrt{8(3\alpha - 1)\beta + 16\beta^2 - 6\alpha + 1}$. Therefore the Boneh-Durfee's bound for $d = N^{\delta'}$ for a given α, β in example 4.1.3 is such that $\delta' < 0.5029$ but note that in this example $d = N^{\delta'} \approx N^{0.996307}$ exceeding the bound given by Boneh and Durfee.

4.1.1 Refined Attack Bound Using Sub-Lattice Based Techniques

Boneh and Durfee [5] improved their result by using sub-lattice techniques. Now we implement their idea to our polynomial for improving the result.

Let M_y be the portion of the matrix M with rows corresponding to the y -shifts $h_{l,k}$ and columns corresponding to variable of the form $x^u y^v$, $v > u$ and take the parameter t as twice the value of t in the above lattice based technique i.e., $t = \frac{\alpha - \delta - \gamma}{\gamma} m$.

Define the matrix M_1 as follows: Take every row $g_{i,k}$ of M corresponding to the

x -shifts and take only those rows $h_{l,k}$ of M corresponding to the y -shifts whose diagonal entry is less than or equal to e^m . Let \mathcal{L}_1 be a lattice described by M_1 . Then \mathcal{L}_1 is a sublattice of \mathcal{L} , so short vector of \mathcal{L}_1 will be in \mathcal{L} . Now perform the Gaussian elimination to the first $(m+1)(m+2)/2$ rows of M that is the those rows corresponding to the x -shifts to set the off-diagonal entries of every row to zero, then there is a unitary matrix A over \mathbb{R} such that $M_2 = AM_1$ is a matrix whose upper left block Δ is a diagonal matrix of order $(m+1)(m+2)/2$, lower right block M'_y consists selected rows of M_y and remaining upper right block and lower left block of M_2 are zero blocks. Since A is unitary, the determinant of the lattice L_2 described by M_2 is equal to $\det(\mathcal{L}_1)$ and the $\det(\mathcal{L}_2) = \det(\Delta) \cdot \det(\mathcal{L}'_y)$ where \mathcal{L}'_y be the lattice induced by M'_y .

Let w' be the dimension of \mathcal{L}'_y . First we compute w' by setting $S = \{(k, l) \in \{0, \dots, m\} \times \{1, \dots, t\} | M(k, l, k, l) \leq e^m\}$ and then $w' = |S|$. The matrix M_y is a geometrically progressive matrix with parameter choice $(m^{2m}, N, \alpha m, \delta + \gamma, \gamma - 1, -\alpha, 1, b)$ for some b . Note that the first three conditions of Definition 1 hold. To satisfy the fourth condition, the parameter b should satisfy $b(\delta + \gamma) - \alpha \geq 0$ and $b(\gamma - 1) + 1 \geq 0$ together and thus we get the constraint $\delta > \alpha - \gamma(1 + \alpha)$, which in turn gives a possible value of b as $b = \frac{1}{1-\gamma}$. We have $M_y(k, l, k, l) = N^{\alpha m + (\delta - \alpha + \gamma)k + \gamma l}$ for $k = 0, \dots, m$ and $l = 1, \dots, t$. Since $(k, l) \in S$ only if $N^{\alpha m + (\delta - \alpha + \gamma)k + \gamma l} < N^{\alpha m}$, so for $l \leq \frac{\alpha - \delta - \gamma}{\gamma} k$ we get this inequality. Thus

$$w' = |S| = \sum_{k=0}^m \left\lfloor \frac{\alpha - \delta - \gamma}{\gamma} k \right\rfloor = \frac{\alpha - \delta - \gamma}{2\gamma} m^2 + o(m^2)$$

and the dimension of the lattice \mathcal{L}_2 is

$$w = \frac{(m+1)(m+2)}{2} + w' = \left(\frac{1}{2} + \frac{\alpha - \delta - \gamma}{2\gamma} \right) m^2 + o(m^2).$$

Since the lattice \mathcal{L}'_y defined by the rows $(k, l) \in S$ of M_y and by Theorem 1.3.36 we have

$$\det \mathcal{L}'_y \leq \left((m+1) \left\lfloor \frac{\alpha - \delta - \gamma}{\gamma} \right\rfloor m \right)^{\frac{w'}{2}} (1 + m^{2m})^{(w')^2} \prod_{(k,l) \in S} M_y(k, l, k, l).$$

As $\left((m+1) \left\lfloor \frac{\alpha - \delta - \gamma}{\gamma} \right\rfloor m \right)^{\frac{w'}{2}} (1 + m^{2m})^{(w')^2}$ is a function of only δ (but not of N) and

$$\prod_{(k,l) \in S} M_y(k, l, k, l) = \prod_{k=0}^m \prod_{l=0}^{\left\lfloor \frac{\alpha - \delta - \gamma}{\gamma} k \right\rfloor} N^{\alpha m + (\delta - \alpha + \gamma)k + \gamma l}, \text{ we have}$$

$$\det \mathcal{L}'_y = N^{\left(\frac{2\alpha^2 - \alpha\gamma - \gamma^2 - (\alpha + 2\gamma)\delta - \delta^2}{6\gamma} \right) m^3 + o(m^3)}.$$

Now as $\det(\Delta) = e^{n_e} X^{n_x} Y^{n_y}$ pertaining to just x -shifts, repeating the argument as in the above lattice based strategy we have $\det(\Delta) = N^{\left(\frac{2\alpha + 2\delta + \gamma}{6} \right) m^3 + o(m^2)}$, so then the condition $\det(\mathcal{L}_1) = \det(\Delta) \cdot \det(\mathcal{L}'_y) < e^{mw}$ gives the bound

$$\delta < \alpha - \sqrt{\alpha\gamma}.$$

Theorem 4.1.3. Let $N, p, q, e, X, Y, x_0, y_0, \delta, \gamma$ and ρ be defined in Theorem 4.1.1 Suppose that $|x_0| \leq X$ and $|y_0| \leq Y$, then RSA is insecure if

$$\alpha - \gamma(1 + \alpha) < \delta < \alpha - \sqrt{\alpha\gamma}.$$

Proof. Follows from the above argument and the LLL lattice basis reduction algorithm operates in polynomial time [29]. ■

Now we follow the idea of Blömer-May in [3] using sub-lattice techniques and this approach does not improve the above bound for δ and also slightly less than to this bound but this method requires lattice of smaller dimension than the above approach.

Theorem 4.1.4. Let $N, p, q, e, X, Y, x_0, y_0, \delta, \gamma$ and ρ be defined in Theorem 4.1.1 Suppose that $|x_0| \leq X$ and $|y_0| \leq Y$, then RSA is insecure if

$$\delta < \frac{2\alpha - 6\gamma + 2\sqrt{\alpha^2 - \alpha\gamma + 4\gamma^2}}{5}.$$

Proof. This proof is similar to the above argument but determinant of lattice will be different here.

Unlike the above remove the some rows corresponding to the both x -shifts and y -shifts of M in order to obtain a square matrix and to apply Howgrave's theorem by following the same idea of Blömer-May in [3] and denote the final constructed matrix by M_B and corresponding lattice \mathcal{L}_B .

So the new lattice M_B formed by removing the row vectors corresponding to the x -shift polynomials $g_{i,k}(xX, yY)$ if $i+k = 0, 1, \dots, m-t-1$, the y -shift polynomials

$h_{j,k}(xX, yY)$ if $k = \begin{cases} 0, \dots, m-t & \text{if } j = 1 \\ 0, \dots, m-t+1 & \text{if } j = 2 \\ \vdots \\ 0, \dots, m-2 & \text{if } j = t-1 \\ 0, \dots, m-1 & \text{if } j = t \end{cases}$ and remove columns in order to form a lower triangular square matrix.

Then the dimension of the lattice $\mathcal{L}_B = (m+1)(t+1)$ and the diagonal elements of the matrix M_B will be

$$\begin{aligned}
 & X^m e^m, X^m Y e^{m-1}, \dots, X^m Y^m, \\
 & X^{m-1} e^m, X^{m-1} Y e^{m-1}, \dots, X^{m-1} Y^{m-1} e, \\
 & \dots, \\
 & X^{m-t} e^m, X^{m-t} Y e^{m-1}, \dots, X^{m-t} Y^{m-t} e^t \text{ (for } x\text{-shifts) and} \\
 & X^m Y^{m+t}, \\
 & X^m Y^{m+t-1}, X^{m-1} Y^{m+t-2} e, \\
 & \dots, \\
 & X^m Y^{m+1}, X^{m-1} Y^m e, \dots, X^{m-t+1} Y^{m-t+2} e^{t-1} \text{ (for } y\text{-shifts)}.
 \end{aligned}$$

Multiplying the diagonal elements and neglecting the lower order terms, we need the condition

$$X^{tm^2 - \frac{mt^2}{2} + \frac{t^3}{6}} Y^{\frac{tm^2}{2} + \frac{t^3}{6}} < e^{\frac{tm^2}{2}}.$$

Putting the values of $e = N^\alpha$, $X = N^\delta$, $Y = N^\gamma$ and $t = \tau m$, we have the required condition

$$\left(\frac{\delta}{6} + \frac{\gamma}{6}\right) \tau^2 - \frac{1}{2} \delta \tau + \left(\delta + \frac{\gamma}{2} - \frac{\alpha}{2}\right) < 0.$$

The left hand side is minimized at the value $\tau = \frac{\delta}{\frac{2}{3}(\delta+\gamma)}$. Putting this value of τ in the previous inequality we get the bound for δ is

$$\delta < \frac{2\alpha - 6\gamma + 2\sqrt{\alpha^2 - \alpha\gamma + 4\gamma^2}}{5}.$$

■

4.1.2 Analysis of Attack Bounds

As it is known that, for $p - q < N^{\frac{1}{4}}$, then RSA is insecure by Fermat's Factorization technique, in this section we first analyze all the above attack bounds on δ in the range $N^{\frac{1}{4}} < p - q < \frac{N^{\frac{1}{2}}}{\sqrt{2}}$. We proposed by denoting the δ obtained using both x and y shifts as in Theorem(4.1.1) by $\delta_{x,y}$, the δ obtained using only x -shifts as in Corollary(4.1.2) by δ_x , the δ obtained using sublattice based techniques as in Theorem(4.1.4) by δ_s and the δ obtained using sublattice based techniques with lower dimension as in Theorem(4.1.5) by δ_{s_d} . Let $p - q = N^\beta$ for $\frac{1}{4} < \beta < \frac{1}{2}$, then we have $p - \lceil \sqrt{N} \rceil, \lceil \sqrt{N} \rceil - q < N^\beta$ as $q < \lceil \sqrt{N} \rceil < p$. As $y_0 = q - \lceil \sqrt{N} \rceil$ or $p - \lceil \sqrt{N} \rceil$, we may take $Y = N^\beta, \frac{1}{4} < \beta < \frac{1}{2}$ and for $Y = N^\beta$ the attack bound for δ in the above results are given as:

$$\delta_x < \frac{\alpha - \beta}{2} \text{ for any } m \geq 1. \quad (4.1.2)$$

$$\delta_{x,y} < \frac{3\alpha + \beta - 2\sqrt{\beta(3\alpha + \beta)}}{3} \text{ for } t = \frac{\alpha - \delta - \beta}{2\beta}m. \quad (4.1.3)$$

$$\alpha - \beta(1 + \alpha) < \delta_s < \alpha - \sqrt{\alpha\beta} \text{ for } t = \frac{\alpha - \delta - \beta}{\beta}m. \quad (4.1.4)$$

$$\delta_{sd} < \frac{2\alpha - 6\beta + 2\sqrt{\alpha^2 - \alpha\beta + 4\beta^2}}{5} \text{ for } t = \frac{\delta}{\frac{2}{3}(\delta + \beta)}m. \quad (4.1.5)$$

In Table 4.1, we represent how the bound for δ increase when the prime difference N^β is decreasing from $N^{\frac{1}{2}}$ to $N^{\frac{1}{4}}$ for a given public key exponent $e = N^\alpha$ in the all above cases (4.1.2),(4.1.3),(4.1.4) and (4.1.5).

α	β	δ			
		$\delta_x <$	$\delta_{x,y} <$	$\delta_s <$	$\delta_{sd} <$
0.501	≈ 0.50	0.0005	0.0005001873	(0, 0.0005002497)	0.0005001874
	0.45	0.0255	0.0260200003	(0, 0.0261842462)	0.0260339152
	0.40	0.0505	0.0526881570	(0, 0.0533394142)	0.0528096268
	0.35	0.0755	0.0807826527	(0, 0.0822518656)	0.0812390932
	0.30	0.1005	0.1106939731	(0.0570000001, 0.1133145605)	0.1118998342
	0.26	0.1205	0.1363082232	(0.1174, 0.1400844974)	0.1385650655
0.55	≈ 0.50	0.025	0.0254519548	(0, 0.0255955759)	0.0254626986
	0.45	0.05	0.0519259301	(0, 0.0525062814)	0.0520215047
	0.40	0.075	0.0796409907	(0, 0.0809584240)	0.0800000000
	0.35	0.1	0.1088933156	(0.0075000001, 0.1112517806)	0.1098386676
	0.30	0.125	0.1400980486	(0.0850000001, 0.1437980797)	0.1421347195
	0.26	0.145	0.1668676552	(0.147, 0.1718465919)	0.1702670394
0.75	≈ 0.50	0.125	0.1349307066	(0, 0.1376275643)	0.1358898943
	0.45	0.15	0.1651530771	(0, 0.1690524980)	0.1669397989
	0.40	0.175	0.1969579906	(0.0499999999, 0.2022774424)	0.2
	0.35	0.2	0.2307071990	(0.1375, 0.2376524617)	0.2355277766
	0.30	0.225	0.2669048105	(0.225, 0.2756583509)	0.2740658617
	0.26	0.245	0.2981089219	(0.295, 0.3084119566)	0.3074745686
1	≈ 0.50	0.25	0.2847495629	(0, 0.2928932188)	0.2898979485
	0.45	0.275	0.3193376137	(0.1, 0.3291796067)	0.3264761515
	0.40	0.3	0.3558730806	(0.2, 0.3675444679)	0.3654211490
	0.35	0.325	0.3947864057	(0.3, 0.4083920216)	0.4070831300
	0.30	0.35	0.4366750419	(0.4, 0.4522774424)	0.4518252056
	0.26	0.37	0.4728987047	(0.48, 0.4900980486)	0.4900746199

Table 4.1: Bound for δ corresponding to the values of α and β in all cases.

In Figure 4.1 we plot the bounds for δ_s , δ_{s_d} , $\delta_{x,y}$ and δ_x for a given e in different values of β i.e., $\beta = 0.5, 0.45, 0.35$ and 0.26 . Within that bounds the RSA cryptosystem is insecure and note that the region for which RSA is insecure increases when the value of β decreases.

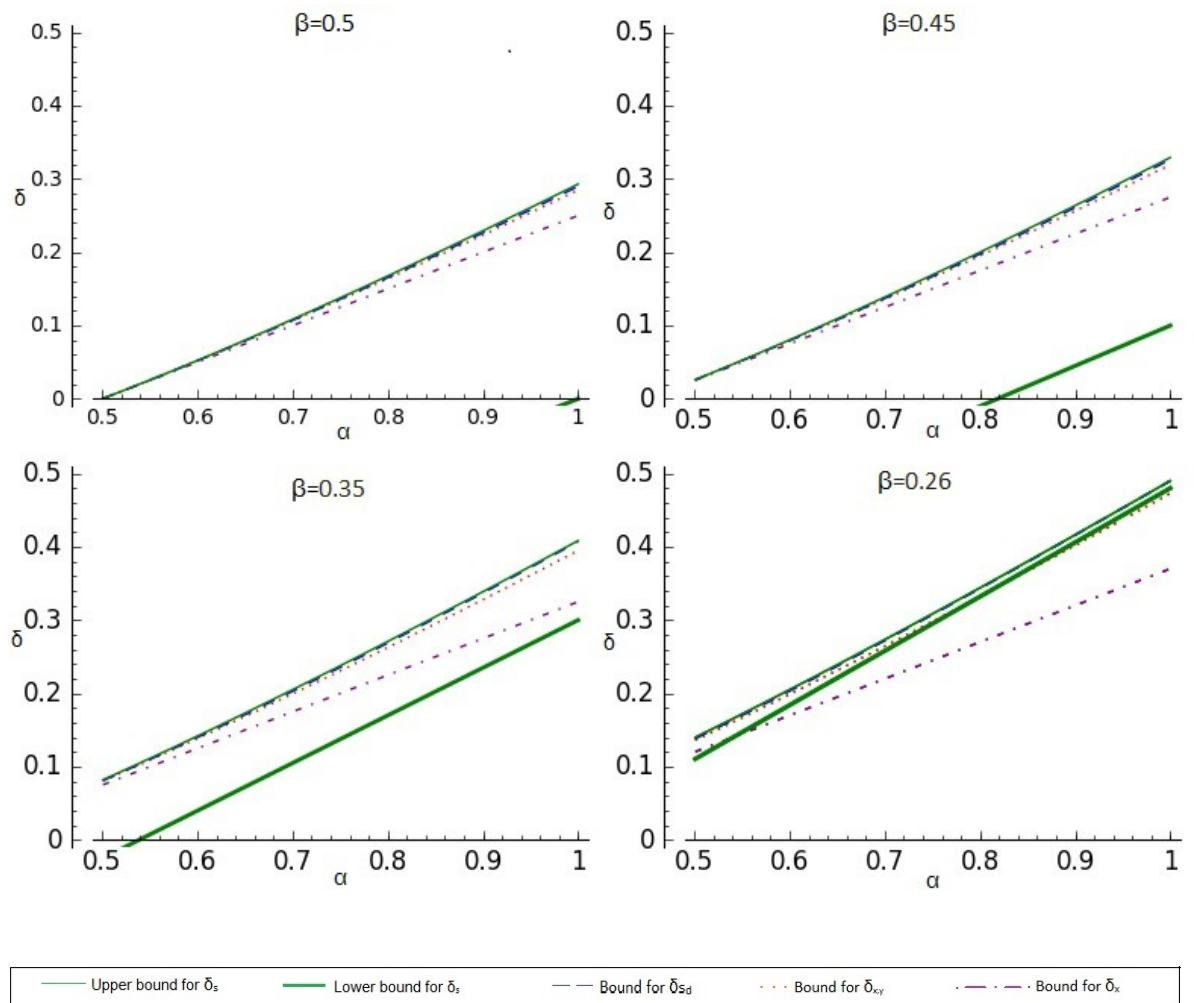


Figure 4.1: The region for δ and α values for which RSA is insecure for different values of β

From the above observations it is noted for a given α if δ is beyond the upper bound δ_s then the RSA is secure with respect to all the above attacks and if δ is within the bound for δ_x and beyond the lower bound for δ_s then RSA is insecure with respect to all the the above attacks and for any δ within any of the four attack bounds corresponding attack may be implemented. Further it is also observed that δ always lies beyond the attack bounds for certain values of the public encryption exponent e and such inefficient lower bound of e for each attack related to the prime difference are listed in Table 4.2 for $e = N^\alpha$ and $L(\alpha)$, denoting the lower bound for inefficient e for the above attacks using lattice based techniques.

N	β (\approx)	$L(\alpha)$			
		Attack with x -shifts	Attack with x and y shifts	Attack with sublattice based techniques	Attack with sublattice based techniques with lower dimension
1000 bits	0.50	0.5025	0.5025	0.5025	0.5025
	0.45	0.5520	0.5560	0.5600	0.5570
	0.35	0.66	0.71	0.72	0.7130
	0.26	0.75	0.9120	0.9675	0.9670
2000 bits	0.50	0.5013	0.5013	0.5013	0.5013
	0.45	0.5510	0.5550	0.5590	0.5560
	0.35	0.6520	0.70	0.72	0.71
	0.26	0.7450	0.91	0.9645	0.9640
4000 bits	0.50	0.5010	0.5010	0.5010	0.5010
	0.45	0.5505	0.5545	0.5570	0.5550
	0.35	0.6510	0.6990	0.7160	0.7095
	0.26	0.7410	0.9090	0.9640	0.9435

Table 4.2: List of $L(\alpha)$ corresponding to β and no.of bits in N .

In such cases we proceed to improve the attack bounds for δ so that the inefficient e may turn efficient for the attacks with lattice based techniques by considering the same polynomial congruence with N replaced by ρN or $\frac{N}{\rho}$ for some appropriate ρ , $1 \leq \rho \leq 2$ such that $\rho q \approx p$ and is based on the following Theorem.

Theorem 4.1.5. Let $|p - \rho q| \leq N^{\gamma'}$ where $\gamma' < \frac{1}{2}$ and $1 \leq \rho \leq 2$. Then we have $|p - \sqrt{\rho N}|, |q - \sqrt{\frac{N}{\rho}}| < N^{\gamma'}$ [30].

To improve the bound for δ , we consider the polynomial congruence $f(x, y) \equiv 0 \pmod{e}$ in which the upper bound $N^{\gamma'}$ for the solution $y = y_0$ is depending on the value $|p - \rho q|$, rather than the prime difference $p - q$ for $f(x, y) = x(y + A) - 1$, with $A = \begin{cases} \lceil \sqrt{\rho N} \rceil - 1, & \text{if } \min\{r, s\} = r \\ \lceil \sqrt{\frac{N}{\rho}} \rceil - 1, & \text{if } \min\{r, s\} = s. \end{cases}$

Then the solutions $x = x_0$ and $y = y_0$ for the polynomial congruence $f(x, y) \equiv x(y + A) - 1 \pmod{e}$ are given as $x_0 = \min\{r, s\}$ and $y_0 = \begin{cases} p - \lceil \sqrt{\rho N} \rceil, & \text{if } \min\{r, s\} = r \\ q - \lceil \sqrt{\frac{N}{\rho}} \rceil, & \text{if } \min\{r, s\} = s. \end{cases}$

In [42], it has been studied how a few MSBs of p or q can be found from the knowledge of N only, where $N = pq$, p and q are primes of same size and this knowledge of most significant bits(MSBs) of p or q can provide approximation of ρ . Otherwise one may try to guess ρ for different values (that are computationally feasible) to mount the attack. To mount the attack we establish the attack bounds for δ by repeating the argument for $|x_0| \leq N^\delta$ and $|y_0| \leq N^{\gamma'}$, $\gamma' \leq \frac{1}{2}$ in Corollary 4.1.2, Theorem 4.1.1, Theorem 4.1.4 and Theorem 4.1.5. Note for the above attack bounds thus obtained depending on appropriate ρ .

Example 4.1.6. Let $p=202578011750906281247094079898482654152352800202967795174672010161491336804628653$

58574779284875457806030124268550700030014115264772567435253175260469958709084217 and

$$q = 106620006184687516445838989420254028501238315896298839565616847453416493055067712$$

$$41355146992039714634752696983447736857902165928827667136006663483150507256156183$$

be two 533 and 532 bit integer primes respectively with $q < p < 2q$.

$$\text{Then } N = 215988688657633280888137261514522896004197165983041322871302383040220579435985189458249347389135513014$$

$$66581746670813928474835987795 78805377405134605780218613554771847080564776236921530596976503056680174210821867015751$$

$$8254139618999751340345127999866829966392864624231228730005 5328685941416182541762052991358334639452263711.$$

For the public encryption exponent $e = 203570487608519177130387858346335949982681274302465056311222282$

$$65727831120341504227605379168525 574184831255713809622106188803980126100142376033417564441502906816081028618399597927$$

$$513832190649042334179538898854354716330533894180986228498033 07996837184668882334422884965338353654061812322328244014$$

873765, the multiplicative inverses of $p-1$ and $q-1$ modulo e are $r = 158632059222900190064040197$

$$82584099034358123662465732469953170767501769225883755689521518192482725595496589763798408382380531132272292363326 287$$

$$32137867246713845703554488416968391320841470705716962245803211633386377136888877661949911543059259693132107562595887$$

$$0066127685434042170604888 47920706636452261,$$

$$S = 745823645745560047400757447700005723876746573657571523716437596174571647385613746587436756732657136495761847356$$

$$71436756173564375674365716349 705193 \text{ respectively and } e \approx N^{0.937484971166478}.$$

Taking $\rho = 1.9$, we get $|p - \rho q| = N^{0.0814475914542542436619469358}$. For $\gamma' \approx 0.082$, the bound for δ corresponds to the results given in Corollary 4.1.2 and Theorems 5 & 7 are 0.428018689856112, 0.640973585517601 and 0.641467151800484 respectively and note the solution $x = x_0 = s \approx N^{0.455376075838353}$ is exceeding the bound given in Corollary 4.1.2 (The method given in the Theorem 4.1.4 is not applicable in this case as we have $\alpha - \gamma(1 + \alpha) < \alpha - \sqrt{\alpha\gamma}$ only if $\sqrt{\gamma} \frac{1+\sqrt{\alpha}}{\sqrt{\alpha}} > 1$, but in this case $\sqrt{\gamma} \frac{1+\sqrt{\alpha}}{\sqrt{\alpha}} < 1$). By using the lattice parameters $m = 3$ and $t = 1$ we can factor the RSA modulus N in both cases corresponding to the Theorems 4.1.1 & 4.1.5. If $|y_0| = |q - \lceil \sqrt{\frac{N}{\rho}} \rceil|$, then for the polynomial congruence $x(y + A) - 1 \equiv 1 \pmod{e}$,

where $A = \lceil \sqrt{\frac{N}{\rho}} \rceil - 1$ and for $\beta \approx 0.49942206$, the solution $x = x_0$ is exceeding the bound given in (4.1.2),(4.1.3),(4.1.4) and (4.1.5).

The refinement process of RSA attack bounds on δ for N^δ , an upper bound for $\min\{(p-1)^{-1} \bmod e, (q-1)^{-1} \bmod e\}$ using lattice-based techniques is given in the following table.

Lattice based attack	Attack bound when $p - q$ is bounded	Attack bound when $p - \rho q$ is bounded
Attack with x -shifts	$(\alpha - \beta)/2$	$(\alpha - \gamma')/2$
Attack with x and y shifts	$(3\alpha + \beta - 2\sqrt{\beta(3\alpha + \beta)})/3$	$(3\alpha + \gamma' - 2\sqrt{\gamma'(3\alpha + \gamma')})/3$
Attack with sublattice based techniques	$\alpha - \beta(1 + \alpha) < \delta < \alpha - \sqrt{\alpha\beta}$	$\alpha - \gamma'(1 + \alpha) < \delta < \alpha - \sqrt{\alpha\gamma'}$
Attack with sublattice based techniques with lower dimension	$(2\alpha - 6\beta + 2\sqrt{\alpha^2 - \alpha\beta + 4\beta^2})/5$	$(2\alpha - 6\gamma' + 2\sqrt{\alpha^2 - \alpha\gamma' + 4\gamma'^2})/5$

Table 4.3: Refinement process of RSA attack bounds on δ for N^δ , an upper bound for $\min\{(p-1)^{-1} \bmod e, (q-1)^{-1} \bmod e\}$.

4.2 Extending Lattice-Based Attacks to an RSA-Like Cryptosystem over $E(\mathbb{Z}_{pq})$

All the lattice-based attacks on RSA for small multiplicative inverse of $p-1$ or $q-1$ modulo e may be extended to RSA-like cryptosystem over elliptic curves $E(\mathbb{Z}_{pq})$ due to KMOV by repeating the argument for $\varphi(N)$ replaced by $\psi(N) = (p+1)(q+1)$.

The above lattice-based attacks on RSA for $p - q$ bounded can be extended to RSA-like cryptosystem over elliptic curves $E(\mathbb{Z}_{pq})$ due to KMOV, according to the polynomial congruence as in the following

When $p - q$ is bounded	RSA	RSA-like over $E(\mathbb{Z}_{pq})$ due to KMOV
Polynomial Congruence	$x(A + y) - 1 \equiv 0 \pmod{e}$ where $A = \lceil N \rceil - 1$.	$x(A + y) - 1 \equiv 0 \pmod{e}$ where $A = \lceil N \rceil + 1$.
Solutions	$(r, p - \lceil \sqrt{N} \rceil)$ and $(s, q - \lceil \sqrt{N} \rceil)$ where $r = (p - 1)^{-1} \pmod{e}$ and $s = (q - 1)^{-1} \pmod{e}$.	$(r, p - \lceil \sqrt{N} \rceil)$ and $(s, q - \lceil \sqrt{N} \rceil)$ where $r = (p + 1)^{-1} \pmod{e}$ and $s = (q + 1)^{-1} \pmod{e}$.

note as the monomials are same for both the polynomials with respect to $\varphi(N)$ and $\psi(N)$, the arguments of our results when $p - q$ is bounded can be repeated for $\varphi(N)$ replaced by $\psi(N)$ then it is observed that RSA and RSA-like have same attack bounds for δ , given as:

$$\delta < \frac{\alpha - \beta}{2},$$

$$\delta < \frac{3\alpha + \beta - 2\sqrt{\beta(3\alpha + \beta)}}{3},$$

$$\alpha - \beta(1 + \alpha) < \delta < \alpha - \sqrt{\alpha\beta} \text{ and}$$

$$\delta < \frac{2\alpha - 6\beta + 2\sqrt{\alpha^2 - \alpha\beta + 4\beta^2}}{5}$$

for $p - q = N^\beta$ and N^δ is an upper bound for $\min\{(p - 1)^{-1} \pmod{e}, (q - 1)^{-1} \pmod{e}\}$ and $\min\{(p + 1)^{-1} \pmod{e}, (q + 1)^{-1} \pmod{e}\}$ in RSA and RSA-like cryptosystem over elliptic curves $E(\mathbb{Z}_{pq})$ due to KMOV respectively.

The lattice-based attacks on RSA for $p - \rho q$ bounded, ρq a better approximation for p can be extended to RSA-like cryptosystem over elliptic curves $E(\mathbb{Z}_{\rho q})$ due to KMOV, according to the polynomial congruence as in the following

When $p - \rho q$ is bounded	RSA	RSA-like over $E(\mathbb{Z}_{\rho q})$ due to KMOV
Polynomial Congruence	$x(A + y) - 1 \equiv 0 \pmod{e}$ where $A = \lceil \sqrt{\rho N} \rceil - 1$ if $\min\{r, s\} = r$ and $A = \lceil \sqrt{\frac{N}{\rho}} \rceil - 1$ if $\min\{r, s\} = s$.	$x(A + y) - 1 \equiv 0 \pmod{e}$ where $A = \lceil \sqrt{\rho N} \rceil + 1$ if $\min\{r, s\} = r$ and $\lceil \sqrt{\frac{N}{\rho}} \rceil + 1$ if $\min\{r, s\} = s$.
Solutions	$(r, p - \lceil \sqrt{\rho N} \rceil)$ if $A = \lceil \sqrt{\rho N} \rceil - 1$ and $(s, q - \lceil \sqrt{\frac{N}{\rho}} \rceil)$ if $A = \lceil \sqrt{\frac{N}{\rho}} \rceil - 1$.	$(r, p - \lceil \sqrt{\rho N} \rceil)$ if $A = \lceil \sqrt{\rho N} \rceil + 1$ and $(s, q - \lceil \sqrt{\frac{N}{\rho}} \rceil)$ if $A = \lceil \sqrt{\frac{N}{\rho}} \rceil + 1$.

note as the monomials are same for both the polynomials with respect to $\varphi(N)$ and $\psi(N)$, the arguments of our results when $p - \rho q$ is bounded can be repeated for $\varphi(N)$ replaced by $\psi(N)$ then it is observed that RSA and RSA-like have same attack bounds for δ , given as:

$$\delta < \frac{\alpha - \gamma'}{2},$$

$$\delta < \frac{3\alpha + \gamma' - 2\sqrt{\gamma'(3\alpha + \gamma')}}{3},$$

$$\alpha - \gamma'(1 + \alpha) < \delta < \alpha - \sqrt{\alpha\gamma'} \text{ and}$$

$$\delta < \frac{2\alpha - 6\gamma' + 2\sqrt{\alpha^2 - \alpha\gamma' + 4\gamma'^2}}{5}$$

for $|p - \rho q| \leq N^{\gamma'}, \gamma' < \frac{1}{2}$, $1 \leq \rho \leq 2$ and N^δ is an upper bound for $\min\{r, s\}$.

4.3 Summary

In this chapter it is shown that RSA is insecure if the multiplicative inverse of $p-1$ or $q-1$ modulo the public encryption exponent e is small, that is less than or equal to N^δ , for some small δ . This is established by using the lattice based techniques implemented by the polynomial congruence $f(x, y) \equiv 0 \pmod{e}$ for $f(x, y) = x(y + A) - 1$ with $A = \lceil \sqrt{N} \rceil - 1$. Lattice based techniques were implemented first using both x and y shifts then implemented using only x -shifts. These were also implemented using sublattice based techniques and sublattice based techniques with lower dimension and in each of the above implementation for δ denoted as $\delta_{x,y}$, δ_x , δ_s and δ_{s_d} respectively, the attack bounds were described. An analysis of these bounds with respect to the prime difference $p - q$, for $p - q = N^\beta$ and with respect to $p - \rho q$, for ρ such that ρq is a better approximation for p are also described. It is observed that these lattice-based attacks on RSA for small multiplicative inverse of $(p-1)^{-1} \pmod{e}$ or $(q-1)^{-1} \pmod{e}$ can be extended to the RSA-like cryptosystem over $E(\mathbb{Z}_{pq})$ due to KMOV and the corresponding analysis is given.

Chapter 5

Cryptanalysis Based on Lattice-Based Techniques, for RSA with Small Multiplicative Inverse of $\varphi(N)$ Modulo e and with a Composed Prime Sum $p + q$

In this chapter, we mount an attack on RSA when $\varphi(N)$ has small multiplicative inverse k modulo e , the public encryption exponent. For $k \leq N^\delta$, the attack bounds for δ are described by using lattice based techniques. The bound for δ depends on the prime difference $p - q = N^\beta$ and the maximum bound for δ is $\alpha - \sqrt{\frac{\alpha}{2}}$ for $e = N^\alpha$ and for $\beta \approx 0.5$. If the prime sum $p + q$ is of the form $p + q = 2^n k_0 + k_1$ where n is a given positive integer and k_0 and k_1 are two suitably small unknown integers then the maximum bound for δ is improved for $\beta \approx 0.5$. Also we gave a new attack bound for the deciphering exponent d with above composed prime sum and compare it to Boneh and Durfee's bound. Further noted that all these Lattice-based attacks on RSA can be extended to the RSA-like cryptosystem over $E(\mathbb{Z}_{pq})$ due to KMOV.

5.1 Attack Bounds for RSA Using Lattice Based Techniques Based on Finding Small Modular Roots of Bivariate Polynomials

In our paper [19] and in chapter 4, we described an attack on RSA by using lattice based techniques implemented in the case when $p-1$ or $q-1$ have small multiplicative inverse less than or equal to N^δ modulo the public encryption exponent e , for some small δ and for $q < p < 2q$, $e = N^\alpha > p-1$.

Let $f(x, y) = x(y + A) - 1$ where $A = \lceil \sqrt{N} \rceil - 1$ and r, s be the multiplicative inverses of $p-1, q-1$ modulo the private encryption exponent e respectively. For $x_0 = \min\{r, s\}$ and $y_0 = \begin{cases} p - \lceil \sqrt{N} \rceil & \text{if } \min\{r, s\} = r \\ q - \lceil \sqrt{N} \rceil & \text{if } \min\{r, s\} = s, \end{cases}$ the pair (x_0, y_0) is a solution for the modular polynomial equation $f(x, y) \equiv 0 \pmod{e}$. For $|x_0| \leq N^\delta, |y_0| \leq N^\gamma$, the attack bounds for δ are described in [19] by using lattice reduction techniques in the direction of Boneh-Durfee [5] and Blömer-May [3] for $q < p < 2q$ and $e = N^\alpha > p-1$.

Applying the analysis described by Boneh-Durfee in [5] using x, y shifts and using only x shifts to the above modular polynomial equation, we get the attack bounds for δ as given in the following Theorem and Corollary [19] respectively.

Theorem 5.1.1. Let $N = pq$ be an RSA modulus with $q < p < 2q$. Let $e = N^\alpha$, $X = N^\delta$, $Y = N^\gamma$ and r, s are the multiplicative inverses of $p-1, q-1$ modulo e respectively. Suppose that $|x_0| \leq X$ and $|y_0| \leq Y$ then one can factor N in

polynomial time if

$$\delta < \frac{3\alpha + \gamma - 2\sqrt{\gamma(3\alpha + \gamma)}}{3}.$$

Corollary 5.1.2. If the lattice basis reduction algorithm is implemented only using x -shifts and repeating the above argument then we can factorize N whenever

$$\delta < \frac{\alpha - \gamma}{2}.$$

In [19] further, the bound given in the above theorem is improved by implementing the ideas given by Boneh-Durfee[5] and Blömer-May[3] to the above modular equation using sublattice based techniques as given in the following Theorems.

Theorem 5.1.3. Let $N, p, q, e, X, Y, x_0, y_0, \delta$ and γ be defined in Theorem 5.1.1. Suppose that $|x_0| \leq X$ and $|y_0| \leq Y$, then RSA is insecure if

$$\alpha - \gamma(1 + \alpha) < \delta < \alpha - \sqrt{\alpha\gamma}.$$

Theorem 5.1.4. Let $N, p, q, e, X, Y, x_0, y_0, \delta$ and γ be defined in Theorem 5.1.1. Suppose that $|x_0| \leq X$ and $|y_0| \leq Y$, then RSA is insecure if

$$\delta < \frac{2\alpha - 6\gamma + 2\sqrt{\alpha^2 - \alpha\gamma + 4\gamma^2}}{5}.$$

The bound given in the Theorem 5.1.4 is slightly less than the bound(upper) given in the Theorem 5.1.3 but the method used to obtain this bound requires lattice of smaller dimension than the above.

Now in this section we first describe the attack bounds for RSA cryptosystem in this section using the lattice based techniques based on the Coppersmith techniques

[8] for finding small solutions of modular bivariate integer polynomial equations following the idea of Boneh-Durfee[5] and Blömer-May[3], when $\varphi(N)$ have some small multiplicative inverse modulo e . Let $N = pq, q < p < 2q, p - q = N^\beta$ and $e = N^\alpha > p + q$. As $(e, \varphi(N)) = 1$, there exist unique r, s such that

$$(p - 1)r \equiv 1 \pmod{e} \text{ and } (q - 1)s \equiv 1 \pmod{e}.$$

Let $k = rs \pmod{e}$, then $k\varphi(N) \equiv 1 \pmod{e}$, i.e., k is a multiplicative inverse of $\varphi(N)$ modulo e . For $g(x, y) = x(y + B) - 1$ where $B = N + 1 - \lceil 2\sqrt{N} \rceil$, the pair $(x_0, y_0) = (k, -((p + q) - \lceil 2\sqrt{N} \rceil))$ is a solution for the modular polynomial equation $g(x, y) \equiv 0 \pmod{e}$ (in general $(p + q) - \lceil 2\sqrt{N} \rceil \pmod{e} \leq (p + q) - \lceil 2\sqrt{N} \rceil$ and $(k, -((p + q) - \lceil 2\sqrt{N} \rceil \pmod{e}))$ is also a solution but in this case $(p + q) - \lceil 2\sqrt{N} \rceil \pmod{e} = (p + q) - \lceil 2\sqrt{N} \rceil$ as $e > p + q$). Note as $q < \sqrt{N}$, $p + q - \lceil 2\sqrt{N} \rceil < N^\beta$, hence N^β is an upper bound for y_0 . Now note as the monomials for the polynomial g^m where $g(x, y) = x(y + N + 1 - \lceil 2\sqrt{N} \rceil) - 1$ and for the polynomial f^m where $f(x, y) = x(y + \lceil \sqrt{N} \rceil - 1) - 1$ described as in [19] are same for any positive integer m , we have the same analysis as in [19] for the above given modular equation with the multiplicative inverse k of $\varphi(N) \pmod{e}$ bounded by N^δ , we have $|k| \leq N^\delta$ and for $x_0 = k$, RSA is insecure under the following conditions:

$$\delta < \frac{3\alpha + \beta - 2\sqrt{\beta(3\alpha + \beta)}}{3}; \quad (5.1.1)$$

$$\delta < \frac{\alpha - \beta}{2}; \quad (5.1.2)$$

$$\alpha - \beta(1 + \alpha) < \delta < \alpha - \sqrt{\alpha\beta}; \quad (5.1.3)$$

$$\delta < \frac{2\alpha - 6\beta + 2\sqrt{\alpha^2 - \alpha\beta + 4\beta^2}}{5}. \quad (5.1.4)$$

Denoting the upper bounds for δ as in (5.1.1),(5.1.2),(5.1.3) and (5.1.4) by $\delta_1, \delta_2, \delta_3$ and δ_4 respectively, we have the bound for δ corresponding to α and β as given in Table 5.1, depicting the refinement of the attack bounds in the following.

α	β (\approx)	δ			
		δ_1	δ_2	δ_3	δ_4
0.501	0.50	0.0005	0.0005001873	0.0005002497	0.0005001874
0.55	0.50	0.025	0.0254519548	0.0255955759	0.0254626986
0.75	0.50	0.125	0.1349307066	0.1376275643	0.1358898943
1	0.50	0.25	0.2847495629	0.2928932188	0.2898979485

Table 5.1: Bounds for δ corresponding to certain values of α and $\beta \approx 0.5$ depicting the refinement.

By the analysis as in [19] note in all the above cases the maximum upper bound for δ is the bound as in (5.1.3), it is $\alpha - \sqrt{\frac{\alpha}{2}}$ for $\beta \approx 0.5$ and for $\alpha = 0.501, 0.55, 0.75, 1$, the value $\delta_3 = \alpha - \sqrt{\frac{\alpha}{2}} \approx 0.000501, 0.0254627, 0.135890, 0.289898$ respectively are the bounds for δ . Note the arguments above are considered for small multiplicative inverse of $\varphi(N) \bmod e$.

Note when either $(p-1) \bmod e$ or $(q-1) \bmod e$ has small inverse we may adapt the attack as in [19] but when both $(p-1) \bmod e$ and $(q-1) \bmod e$ do not have small inverses the $\varphi(N) \bmod e$ may have small inverse as in Table 5.2 then this modified attack proposed in the following may be used.

e	$\varphi(N)^{-1} \bmod e$	$(p-1)^{-1} \bmod e$	$(q-1)^{-1} \bmod e$	e	$\varphi(N)^{-1} \bmod e$	$(p-1)^{-1} \bmod e$	$(q-1)^{-1} \bmod e$
1	0	0	0	97	48	91	89
5	3	1	3	101	10	19	59
7	5	4	3	103	22	58	43
11	9	9	1	107	34	87	9
13	4	9	12	109	88	75	100
17	7	16	10	113	103	106	66
19	10	6	8	115	3*	36	48
23	3	13	2	119	75	67	10
25	3*	11	23	121	75	53	111
29	21	20	17	125	28	86	73
31	26	2	13	127	43	8	53
35	33	11	3	131	58	41	11
37	16	7	34	133	124	25	122
41	22	18	24	137	5*	21	60
43	28	35	18	139	113	80	58
47	12	3	4	143	108	9	12
49	12	46	45	145	108	136	133
53	45	10	31	149	52	28	87
55	53	31	23	151	70	85	63
59	4*	48	5	155	88	126	13
61	34	42	56	157	9*	108	144
65	43	61	38	161	26	151	94
67	52	21	28	163	45	51	68
71	27	40	6	167	147	94	14
73	27	32	67	169	147	74	155
77	75	53	45	173	82	119	101
79	7	5	33	175	103	11	73
83	16	26	7	179	124	56	15
85	58	16	78	181	33	34	166
89	70	39	52	185	53	81	108
91	82	74	38	187	75	152	78
95	48	6	8	191	1*	12	16

Table 5.2: Multiplicative inverses of $\varphi(N)$, $p-1$ and $q-1$ modulo e for fixed $N = pq = 13 \cdot 17$.

* For all such $\varphi(N)^{-1} \bmod e$ in the table, note $\varphi(N)^{-1} \bmod e$ is small but $(p-1)^{-1} \bmod e$ and $(q-1)^{-1} \bmod e$ are not small.

Now in the next section the attack bound for δ is further refined for $\beta \approx 0.5$ by taking the prime sum $p + q$ as a composed prime sum i.e., $p + q = 2^n k_0 + k_1$ where n is a known positive integer, k_0 and k_1 are suitably small unknown integers and applying the lattice based arguments for trivariate polynomials.

5.2 An Attack Bound for RSA Using Lattice Based Techniques Based on Finding Small Modular Roots of Trivariate Polynomials

In this section, the attack bound for RSA is described when the prime sum $p + q$ is of the form $p + q = 2^n k_0 + k_1$ with a known positive integer n and unknown integers k_0 and k_1 using the lattice based techniques based on the E. Jochemsz and A. May's extended strategy [18] for finding small solutions of modular multivariate integer polynomial equations. In this method the bound for δ can be improved for a suitable known integer n and suitable unknown parameters k_0, k_1 and for $\beta \approx 0.5$.

Let $p + q = 2^n k_0 + k_1$ where n is a given positive integer and k_0 and k_1 are unknown integers. First assume that $|k_0| \leq |k_1|$. As $k(N + 1 - (p + q)) \equiv 1 \pmod{e}$ for $k = rs \pmod{e}$, the triple $(x_0, y_0, z_0) = (k, -k_1, -k_0)$ is a solution for the modular polynomial equation $f(x, y, z) \equiv 0 \pmod{e}$ for $f(x, y, z) = (N + 1)x + xy + (2^n)xz - 1$ (observe that $|k_0| \pmod{e} = |k_0|$ and $|k_1| \pmod{e} = |k_1|$ as $e > p + q$).

To apply the generalization of Howgrave-Graham result to find the small modular roots of the above equation $f(x, y, z) \equiv 0 \pmod{e}$, we use the extended strategy of Jochemsz and May [18].

Now define the set

$$M_k = \bigcup_{0 \leq j \leq t} \{x^{i_1} y^{i_2} z^{i_3+t} | x^{i_1} y^{i_2} z^{i_3} \text{ is a monomial of } f^m \text{ and } \frac{x^{i_1} y^{i_2} z^{i_3}}{l^k} \text{ is a monomial of } f^{m-k}\},$$

where l is a leading monomial of f and define the shift polynomials as

$$g_{k,i_1,i_2,i_3}(x,y,z) = \frac{x^{i_1} y^{i_2} z^{i_3}}{l^k} (f'(x,y,z))^k e^{m-k}, \text{ for } k = 0, \dots, m, x^{i_1} y^{i_2} z^{i_3} \in M_k \setminus M_{k+1}$$

and $f' = a_l^{-1} f \bmod e$ for the coefficient a_l of l . For $f(x,y,z) = (N+1)x + xy + (2^n)xz - 1$, $x^{i_1} y^{i_2} z^{i_3}$ is a monomial of f^m if $i_1 = 0, \dots, m$, $i_2 = 0, \dots, i_1$, $i_3 = 0, \dots, (i_1 - i_2)$ and xy the leading monomial of f as $|k_0| \leq |k_1|$ with coefficient $a_l = 1$. Then for $0 \leq k \leq m$, $x^{i_1-k} y^{i_2-k} z^{i_3}$ is a monomial of f^{m-k} if $i_1 = k, \dots, m$, $i_2 = k, \dots, i_1$, $i_3 = 0, \dots, (i_1 - i_2)$.

Therefore

$$x^{i_1} y^{i_2} z^{i_3} \in M_k \text{ if } i_1 = k, \dots, m, i_2 = k, \dots, i_1, i_3 = 0, \dots, (i_1 - i_2) + t$$

$$\text{and } x^{i_1} y^{i_2} z^{i_3} \in M_{k+1} \text{ if } i_1 = k+1, \dots, m, i_2 = k+1, \dots, i_1, i_3 = 0, \dots, (i_1 - i_2) + t.$$

From this, we obtain for $0 \leq k \leq m$,

$$x^{i_1} y^{i_2} z^{i_3} \in M_k \setminus M_{k+1} \text{ if } i_1 = k, i_2 = k, i_3 = 0, \dots, t \text{ and}$$

$$\text{if } i_1 = k+1, \dots, m, i_2 = k, i_3 = 0, \dots, (i_1 - i_2) + t.$$

Then for $0 \leq k \leq m$, the shift polynomials are

$$g_{k,i_1,i_2,i_3}(x,y,z) = z^{i_3} (f(x,y,z))^k e^{m-k}, \text{ for } i_1 = i_2 = k, i_3 = 0, \dots, t \text{ and}$$

$$g_{k,i_1,i_2,i_3}(x,y,z) = x^{i_1-k} z^{i_3} (f(x,y,z))^k e^{m-k}, \text{ for } i_1 = k+1, \dots, m, i_2 = k,$$

$$i_3 = 0, \dots, (i_1 - i_2) + t.$$

Suppose $X = N^\delta, Y = N^{\gamma_1}$ and $Z = N^{\gamma_2}$ are the upper bound for k, k_1 and k_0 respectively, then define the lattice \mathcal{L} spanned by the coefficient of the vectors $g_{k,i_1,i_2,i_3}(xX, yY, zZ)$.

For example, the matrix M of \mathcal{L} when $m = 2$ and $t = 1$ is as given in the Table 5.3.

	$\mathbf{1}$	x	xz	x^2	x^2z	x^2z^2	xy	x^2y	x^2yz	x^2y^2	z	xz^2	x^2z^3	xyz	x^2yz^2	x^2y^2z
e^2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
xe^2	0	Xe^2	0	0	0	0	0	0	0	0	0	0	0	0	0	0
xze^2	0	0	XZe^2	0	0	0	0	0	0	0	0	0	0	0	0	0
x^2e^2	0	0	0	X^2e^2	0	0	0	0	0	0	0	0	0	0	0	0
x^2ze^2	0	0	0	0	X^2Ze^2	0	0	0	0	0	0	0	0	0	0	0
$x^2z^2e^2$	0	0	0	0	0	$X^2Z^2e^2$	0	0	0	0	0	0	0	0	0	0
fe	$-e$	$(N+1)Xe$	2^mXZe	0	0	0	XYe	0	0	0	0	0	0	0	0	0
xfe	0	$-Xe$	0	$(N+1)X^2e$	2^mX^2Ze	0	0	X^2Ye	0	0	0	0	0	0	0	0
$xzfe$	0	0	$-XZe$	0	$(N+1)X^2Ze$	$2^mX^2Z^2e$	0	0	X^2YZe	0	0	0	0	0	0	0
f^2	1	$-2(N+1)X$	$-2^{m+1}XZ$	$(N+1)^2X^2$	$2^{m+1}(N+1)X^2Z$	$2^{2m}X^2Z^2$	$-2XY$	$2(N+1)X^2Y$	$2^{m+1}X^2YZ$	X^2Y^2	0	0	0	0	0	0
ze^2	0	0	0	0	0	0	0	0	0	0	Ze^2	0	0	0	0	0
xz^2e^2	0	0	0	0	0	0	0	0	0	0	0	XZ^2e^2	0	0	0	0
$x^2z^3e^2$	0	0	0	0	0	0	0	0	0	0	0	0	$X^2Z^3e^2$	0	0	0
zfe	0	0	$(N+1)XZe$	0	0	0	0	0	0	0	$-Ze$	0	0	$XYZe$	0	0
xz^2fe	0	0	0	0	$(N+1)X^2Z^2e$	0	0	0	0	0	0	$-XZ^2e$	$2^mX^2Z^3e$	0	X^2YZ^2e	0
zf^2	0	0	$-2(N+1)XZ$	0	$(N+1)^2X^2Z$	$2^{m+1}(N+1)X^2Z^2$	0	0	$2(N+1)X^2YZ$	0	Z	$-2^{m+1}XZ^2$	$2^{2m}X^2Z^3$	$-2XYZ$	$2^{m+1}X^2YZ^2$	X^2Y^2Z

Table 5.3: The matrix spanned by the coefficient vectors of the shift polynomials $g_{k,i_1,i_2,i_3}(xX, yY, zZ)$ for $m = 2$ and $t = 1$.

Note that the matrix M of \mathcal{L} is lower triangular matrix and the coefficient of the leading monomial of $g_{k,i_1,i_2,i_3}(x,y,z) = z^{i_3}(f(x,y,z))^k e^{m-k}$, for $i_1 = i_2 = k$, $i_3 = 0, \dots, t$ is $X^k Y^k e^{m-k} Z^{i_3}$ and $g_{k,i_1,i_2,i_3}(x,y,z) = x^{i_1-k} z^{i_3} (f(x,y,z))^k e^{m-k}$, for $i_1 = k+1, \dots, m, i_2 = k, i_3 = 0, \dots, (i_1 - i_2) + t$ is $X^{i_1} Y^k e^{m-k} Z^{i_3}$.

Also note that these coefficients are the diagonal elements of the matrix M , so the determinant is

$$\det(\mathcal{L}) = e^{n_e} X^{n_X} Y^{n_Y} Z^{n_Z} \quad (5.2.1)$$

where

$$\begin{aligned} n_e &= \sum_{k=0}^m \sum_{i_1=k}^k \sum_{i_2=k}^k \sum_{i_3=0}^t (m-k) + \sum_{k=0}^m \sum_{i_1=k+1}^m \sum_{i_2=k}^k \sum_{i_3=0}^{(i_1-i_2)+t} (m-k) \\ &= \frac{1}{8}m^4 + \frac{1}{12}(4t+9)m^3 + \frac{1}{8}(8t+11)m^2 + \frac{1}{12}(8t+9)m, \\ n_X &= \sum_{k=0}^m \sum_{i_1=k}^k \sum_{i_2=k}^k \sum_{i_3=0}^t k + \sum_{k=0}^m \sum_{i_1=k+1}^m \sum_{i_2=k}^k \sum_{i_3=0}^{(i_1-i_2)+t} i_1 \\ &= \frac{1}{8}m^4 + \frac{1}{12}(4t+9)m^3 + \frac{1}{8}(8t+11)m^2 + \frac{1}{12}(8t+9)m, \\ n_Y &= \sum_{k=0}^m \sum_{i_1=k}^k \sum_{i_2=k}^k \sum_{i_3=0}^t k + \sum_{k=0}^m \sum_{i_1=k+1}^m \sum_{i_2=k}^k \sum_{i_3=0}^{(i_1-i_2)+t} k \\ &= \frac{1}{24}m^4 + \frac{1}{12}(2t+3)m^3 + \frac{1}{24}(12t+11)m^2 + \frac{1}{12}(4t+3)m, \\ n_Z &= \sum_{k=0}^m \sum_{i_1=k}^k \sum_{i_2=k}^k \sum_{i_3=0}^t i_3 + \sum_{k=0}^m \sum_{i_1=k+1}^m \sum_{i_2=k}^k \sum_{i_3=0}^{(i_1-i_2)+t} i_3 \\ &= \frac{1}{24}m^4 + \frac{1}{12}m^3(2t+3) + \frac{1}{24}(6t^2+18t+11)m^2 + \frac{1}{12}(9t^2+13t+3)m + \frac{1}{2}(t^2+t) \end{aligned}$$

and the dimension of \mathcal{L} is

$$\begin{aligned} \omega &= \sum_{k=0}^m \sum_{i_1=k}^k \sum_{i_2=k}^k \sum_{i_3=0}^t 1 + \sum_{k=0}^m \sum_{i_1=k+1}^m \sum_{i_2=k}^k \sum_{i_3=0}^{(i_1-i_2)+t} 1 \\ &= \frac{1}{6}m^3 + \frac{1}{2}m^2(t+2) + \frac{1}{6}m(9t+11) + (t+1). \end{aligned}$$

Take $t = \tau m$, then for sufficiently large m , the exponents n_e, n_X, n_Y, n_Z and the dimension ω reduce to

$$\begin{aligned} n_e &= \frac{1}{24}(3 + 8\tau)m^4 + o(m^3), \\ n_X &= \frac{1}{24}(3 + 8\tau)m^4 + o(m^3), \\ n_Y &= \frac{1}{24}(1 + 4\tau)m^4 + o(m^3), \\ n_Z &= \frac{1}{24}(1 + 4\tau + 6\tau^2)m^4 + o(m^3), \\ \omega &= \frac{1}{6}(1 + 3\tau)m^3 + o(m^2). \end{aligned}$$

Applying the LLL algorithm to the basis vectors of the lattice \mathcal{L} , i.e., coefficient vectors of the shift polynomials, we get a LLL-reduced basis say $\{v_1, v_2, \dots, v_\omega\}$ and from the Theorem 1.3.25 we have

$$\|v_1\| \leq \|v_2\| \leq \|v_3\| \leq 2^{\frac{\omega(\omega-1)}{4(\omega-2)}} \det(\mathcal{L})^{\frac{1}{\omega-2}}.$$

In order to apply the generalization of Howgrave-Graham result in Theorem 1.3.25, we need the following inequality

$$2^{\frac{\omega(\omega-1)}{4(\omega-2)}} \det(\mathcal{L})^{\frac{1}{\omega-2}} < \frac{e^m}{\sqrt{\omega}}.$$

from this, we deduce

$$\det(\mathcal{L}) < \frac{1}{\left(2^{\frac{\omega(\omega-1)}{4(\omega-2)}} \sqrt{\omega}\right)^{\omega-2}} e^{m(\omega-2)} < \frac{1}{\left(2^{\frac{\omega(\omega-1)}{4(\omega-2)}} \sqrt{\omega}\right)^{\omega-2}} e^{m\omega}.$$

As the dimension ω is not depending on the public encryption exponent e , $\frac{1}{\left(2^{\frac{\omega(\omega-1)}{4(\omega-2)}}\sqrt{\omega}\right)^{\omega-2}}$ is a fixed constant, so we need the inequality $\det(\mathcal{L}) < e^{m\omega}$.

Using (5.2.1), we get the inequality

$$e^{ne} X^{nX} Y^{nY} Z^{nZ} < e^{m\omega}.$$

Substitute all values and taking logarithms, neglecting the lower order terms and after simplifying by m^4 we get

$$(3 + 8\tau)\alpha + (3 + 8\tau)\delta + (1 + 4\tau)\gamma_1 + (1 + 4\tau + 6\tau^2)\gamma_2 - 4\alpha(1 + 3\tau) < 0.$$

The left hand side inequality is minimized at $\tau = \frac{\alpha - (2\delta + \gamma_1 + \gamma_2)}{3\gamma_2}$ and putting this value in the above inequality we get

$$\delta < \frac{1}{2}\alpha - \frac{1}{2}\gamma_1 + \frac{1}{16}\gamma_2 - \frac{1}{16}\sqrt{48(\alpha - \gamma_1)\gamma_2 + 33\gamma_2^2}.$$

From the first three vectors v_1, v_2 and v_3 in LLL reduced basis we consider three polynomials $g_1(x, y, z), g_2(x, y, z)$ and $g_3(x, y, z)$ over \mathbb{Z} such that $g_1(x_0, y_0, z_0) = g_2(x_0, y_0, z_0) = g_3(x_0, y_0, z_0) = 0$. Suppose g_1, g_2 and g_3 are algebraically independent and let $h_1(x, y)$ be the resultant polynomial of $g_1(x, y, z)$ and $g_2(x, y, z)$ with respect to z and $h_2(x, y)$ be the resultant polynomial of $g_1(x, y, z)$ and $g_3(x, y, z)$ with respect to z and if h_1, h_2 are algebraically independent and let $h(x)$ be the resultant polynomial of $h_1(x, y)$ and $h_2(x, y)$ with respect to y , then we have $h(x)$ is not identically zero and with a solution $x = x_0$ from Remark 1.3.33 & 1.3.34. Note that if k is small such that $k \leq N^\delta$ for $\delta < \frac{1}{2}\alpha - \frac{1}{2}\gamma_1 + \frac{1}{16}\gamma_2 - \frac{1}{16}\sqrt{48(\alpha - \gamma_1)\gamma_2 + 33\gamma_2^2}$, then $x_0 = k$ is a solution for the polynomial $h(x)$ over \mathbb{Z} . With the knowledge of k , we can find the $\varphi(N)$ and the value $p + q$ can be obtained from $\varphi(N)$. Then we can factor the RSA modulus N as $(p+q)^2 - 4N = (p-q)^2$.

Theorem 5.2.1. Let $N = pq$ be an RSA modulus with $q < p < 2q$. Let $e = N^\alpha$, $X = N^\delta$, $Y = N^{\gamma_1}$, $Z = N^{\gamma_2}$ and k be the multiplicative inverse of $\varphi(N)$ modulo e . Suppose the prime sum $p + q$ is of the form $p + q = 2^n k_0 + k_1$, for a known positive integer n and assume that $|k_0| \leq |k_1|$ then for $|k| \leq X$, $|k_1| \leq Y$ and $|k_0| \leq Z$ one can factor N in polynomial time if

$$\delta < \frac{1}{2}\alpha - \frac{1}{2}\gamma_1 + \frac{1}{16}\gamma_2 - \frac{1}{16}\sqrt{48(\alpha - \gamma_1)\gamma_2 + 33\gamma_2^2}. \quad (5.2.2)$$

Proof. Follows from the above argument and the LLL lattice basis reduction algorithm operates in polynomial time [29].

■

Suppose $|k_1| \leq |k_0|$. As $2|\varphi(N)$, $\gcd(e, 2^n) = 1$ for any n . If $2^{n'} = (2^n)^{-1} \pmod{e}$ then the triple $(k, -k_0, -k_1)$ is a solutions for the modular polynomial equation $f(x, y, z) \equiv 0 \pmod{e}$ where $f(x, y, z) = 2^{n'}x(N+1) + xy + 2^{n'}xz - 2^{n'}$ with the leading monomial xy with coefficient 1. Applying the above analysis to the above modular equation for the upper bounds $X = N^\delta$, $Y = N^{\gamma_1}$ and $Z = N^{\gamma_2}$ of k , k_0 and k_1 respectively, we get the bound for δ same as in (5.2.2).

Note that for any given primes p and q with $q < p < 2q$, we can always find a positive integer n such that $p + q = 2^n k_0 + k_1$ where $0 \leq |k_0|, |k_1| \leq \approx 0.25$. A typical example is $2^n \approx \frac{3}{\sqrt{2}}N^{0.25}$ as $p + q < \frac{3}{\sqrt{2}}N^{0.5}$ [34]. Denoting the bound for δ as in (5.2.2) by δ_5 and as $\gamma_2 \leq \gamma_1$ for $|k_0| \leq |k_1|$ or $|k_1| \leq |k_0|$, in the Table 5.4 we represent the values of γ_1 and γ_2 for given α and the bound δ_5 which is grater than $\alpha - \sqrt{\frac{\alpha}{2}}$, δ_3 for $\beta \approx 0.5$.

α	γ_1	γ_2	δ_5
0.501	0.25	0.249 - 0	0.00067 - 0.1255
	0.15	0.149 - 0	0.07227 - 0.1755
	0.01	0.009 - 0	0.21710 - 0.2455
0.55	0.25	0.225 - 0	0.02557 - 0.15
	0.15	0.149 - 0	0.09084 - 0.2
	0.01	0.009 - 0	0.24021 - 0.27
0.75	0.25	0.133 - 0	0.13687 - 0.25
	0.15	0.149 - 0	0.16923 - 0.3
	0.01	0.009 - 0	0.33508 - 0.37
1	0.25	0.052 - 0	0.29073 - 0.375
	0.15	0.116 - 0	0.29005 - 0.425
	0.01	0.009 - 0	0.45457 - 0.495

Table 5.4: The improved bounds for δ for $\beta \approx 0.5$ and for a given e with suitable values of γ_1 and γ_2 .

In the following Table 5.5 we give the attack bounds for δ for the small multiplicative inverse of $\varphi(N) \bmod e$ obtained using methods based on lattice based techniques with respect to bivariate and trivariate polynomial congruences for certain values of α and $\beta \approx 0.5$ thereby depicting the refinement of attack bounds for δ .

α	δ_1	δ_2	δ_3	δ_4	δ_5	
0.501	0.0005	0.0005001873	0.0005002497	0.0005001874	$\gamma_1 = 0.25$	0.00067 - 0.1255
					$\gamma_2 = 0.249 - 0$	
					$\gamma_1 = 0.15$	0.07227 - 0.1755
					$\gamma_2 = 0.149 - 0$	
					$\gamma_1 = 0.01$	0.21710 - 0.2455
					$\gamma_2 = 0.009 - 0$	
0.55	0.025	0.0254519548	0.0255955759	0.0254626986	$\gamma_1 = 0.25$	0.02557 - 0.15
					$\gamma_2 = 0.225 - 0$	
					$\gamma_1 = 0.15$	0.09084 - 0.2
					$\gamma_2 = 0.149 - 0$	
					$\gamma_1 = 0.01$	0.24021 - 0.27
					$\gamma_2 = 0.009 - 0$	
0.75	0.125	0.1349307066	0.1376275643	0.1358898943	$\gamma_1 = 0.25$	0.13687 - 0.25
					$\gamma_2 = 0.133 - 0$	
					$\gamma_1 = 0.15$	0.16923 - 0.3
					$\gamma_2 = 0.149 - 0$	
					$\gamma_1 = 0.01$	0.33508 - 0.37
					$\gamma_2 = 0.009 - 0$	
1	0.25	0.2847495629	0.2928932188	0.2898979485	$\gamma_1 = 0.25$	0.29073 - 0.375
					$\gamma_2 = 0.052 - 0$	
					$\gamma_1 = 0.15$	0.29005 - 0.425
					$\gamma_2 = 0.116 - 0$	
					$\gamma_1 = 0.01$	0.45457 - 0.495
					$\gamma_2 = 0.009 - 0$	

Table 5.5: Refinement of attack bounds for δ using lattice based techniques with respect to bivariate and trivariate polynomials.

To improve the bound for δ as in (5.2.2), i.e., δ_5 in a lower dimension than the above dimension, first we construct a sublattice S_L of L and after that we apply the sublattice based techniques to the lattice S_L given by J. Blömer, A. May in [3], and are described in the following section.

5.2.1 An Attack Bound Using Sublattice Reduction Techniques

In this section, an attack bound for a small multiplicative inverse k of $\varphi(N)$ modulo e when the prime sum $p + q$ is of the form $p + q = 2^n k_0 + k_1$, where n is a given positive integer and k_0 and k_1 are two suitably small unknown integers using sublattice reduction techniques is described.

For $0 \leq k \leq m$, divide the shift polynomials, in the above method according to $t = 0$ and $t \geq 1$. Then for $t = 0$, the shift polynomials $g(x, y, z)$ are

$$g(x, y, z) = \begin{cases} z^{i_3} (f(x, y, z))^k e^{m-k}, & \text{for } i_1 = i_2 = k, i_3 = 0 \\ x^{i_1-k} z^{i_3} (f(x, y, z))^k e^{m-k}, & \text{for } k \leq m-1, i_1 = k+1, \dots, m, i_2 = k, i_3 = 0, \dots, (i_1 - i_2). \end{cases}$$

and for $t \geq 1$, the shift polynomials $h(x, y, z)$ are

$$h(x, y, z) = \begin{cases} z^{i_3} (f(x, y, z))^k e^{m-k}, & \text{for } i_1 = i_2 = k, i_3 = 1, \dots, t \\ x^{i_1-k} z^{i_3} (f(x, y, z))^k e^{m-k}, & \text{for } k \leq m-1, i_1 = k+1, \dots, m, i_2 = k, \\ & i_3 = (i_1 - i_2) + 1, \dots, (i_1 - i_2) + t. \end{cases}$$

Now M be the matrix of L with each row is the coefficients of the shift polynomial

$$\begin{array}{l}
\left. \begin{array}{l}
e^m, xe^m, xze^m, x^2e^m, x^2ze^m, x^2z^2e^m, \dots, x^m e^m, x^m ze^m, \dots, x^m z^m e^m, \\
fe^{m-1}, xfe^{m-1}, xzfe^{m-1}, \dots, x^{m-1}fe^{m-1}, x^{m-1}zfe^{m-1}, \dots, x^{m-1}z^{m-1}fe^{m-1}, \\
\vdots \\
f^{m-1}e, xf^{m-1}e, xzf^{m-1}e, \\
f^m,
\end{array} \right\} \begin{array}{l}
g\text{-shifts} \\
\vdots
\end{array} \\
\left. \begin{array}{l}
ze^m, \dots, z^t e^m, xz^2e^m, \dots, xz^{1+t}e^m, \dots, x^m z^{m+1}e^m, \dots, x^m z^{m+t}e^m, \\
zfe^{m-1}, \dots, z^t fe^{m-1}, xz^2fe^{m-1}, \dots, xz^{1+t}fe^{m-1}, \dots, x^{m-1}z^m fe^{m-1}, \dots, x^{m-1}z^{(m-1)+t} fe^{m-1}, \\
\vdots \\
zf^{m-1}e, \dots, z^t f^{m-1}e, xz^2f^{m-1}e, \dots, xz^{1+t}f^{m-1}e, \\
zf^m, \dots, z^t f^m
\end{array} \right\} \begin{array}{l}
h\text{-shifts} \\
\vdots
\end{array}
\end{array}$$

and each column is the coefficients of each variable (in shift polynomials)

$$\begin{array}{l}
\left. \begin{array}{l}
1, x, xz, x^2, x^2z, x^2z^2, \dots, x^m, x^m z, \dots, x^m z^m, \\
xy, x^2y, x^2yz, x^3y, x^3yz, x^3yz^2, \dots, x^m y, x^m yz, \dots, x^m yz^{m-1}, \\
\text{(first } (\frac{1}{6}m^3 + m^2 + \frac{11}{6}m + 1) \text{ columns)} \vdots \\
x^{m-1}y^{m-1}, x^m y^{m-1}, x^m y^{m-1}z, \\
x^m y^m,
\end{array} \right\} \\
\left. \begin{array}{l}
z, \dots, z^t, xz^2, \dots, xz^{1+t}, \dots, x^m z^{m+1}, \dots, x^m z^{m+t}, \\
xyz, \dots, xyz^t, x^2yz^2, \dots, x^2yz^{1+t}, \dots, x^m yz^m, \dots, x^m yz^{(m-1)+t}, \\
\text{(remaining columns)} \vdots \\
x^{m-1}y^{m-1}z, \dots, x^{m-1}y^{m-1}z^t, x^m y^{m-1}z^2, \dots, x^m y^{m-1}z^{1+t}, \\
x^m y^m z, \dots, x^m y^m z^t.
\end{array} \right\}
\end{array}$$

As xy is the leading monomial in $f(x, y, z)$ with coefficient 1, the diagonal elements in the matrix M are

$$\begin{array}{l}
g\text{-shifts} \left\{ \begin{array}{l}
e^m, Xe^m, XZe^m, X^2e^m, X^2Ze^m, X^2Z^2e^m, \dots, X^me^m, X^mZe^m, \dots, X^mZ^me^m, \\
XYe^{m-1}, X^2Ye^{m-1}, X^2YZe^{m-1}, \dots, X^mYe^{m-1}, X^mYZe^{m-1}, \dots, X^mYZ^{m-1}e^{m-1}, \\
\vdots \\
X^{m-1}Y^{m-1}e, X^mY^{m-1}e, X^mY^{m-1}Ze, \\
X^mY^m,
\end{array} \right. \\
h\text{-shifts} \left\{ \begin{array}{l}
Ze^m, \dots, Z^te^m, XZ^2e^m, \dots, XZ^{1+t}e^m, \dots, X^mZ^{m+1}e^m, \dots, X^mZ^{m+t}e^m, \\
XYZe^{m-1}, \dots, XYZ^te^{m-1}, \dots, X^mYZ^me^{m-1}, \dots, X^mYZ^{(m-1)+t}e^{m-1}, \\
\vdots \\
X^{m-1}Y^{m-1}Ze, \dots, X^{m-1}Y^{m-1}Z^te, X^mY^{m-1}Z^2e, \dots, X^mY^{m-1}Z^{1+t}e, \\
X^mY^mZ, \dots, X^mY^mZ^t.
\end{array} \right.
\end{array}$$

Construction of a sublattice \mathbf{S}_L of L :

The construction of a sublattice S_L of L in order to improve the bound for δ is given in the following.

- First remove following rows in M corresponding to g -shifts

$$\begin{array}{l}
e^m, xe^m, xze^m, \dots, x^{m-1}e^m, \dots, x^{m-1}z^{m-1}e^m, \\
fe^{m-1}, xfe^{m-1}, xzfe^{m-1}, \dots, x^{m-2}fe^{m-1}, \dots, x^{m-2}z^{m-2}fe^{m-1}, \\
\vdots \\
f^{m-2}e^2, xf^{m-2}e^2, xzf^{m-2}e^2, \\
f^{m-1}e.
\end{array}$$

Therefore the remaining rows in M corresponding to g -shifts are

$$x^me^m, x^mze^m, \dots, x^mz^me^m,$$

$$\begin{aligned}
& x^{m-1} f e^{m-1}, \dots, x^{m-1} z^{m-1} f e^{m-1}, \\
& \vdots \\
& x f^{m-1} e, x z f^{m-1} e, \\
& f^m,
\end{aligned}$$

and its corresponding g -shifts can be written as

$$g_s(x, y, z) = x^{l_1} z^{l_2} (f(x, y, z))^k e^{m-k} \text{ for } k = 0, \dots, m, l_1 = m - k, l_2 = 0, \dots, l_1.$$

- Now remove some rows in M corresponding to h -shifts are

$$\begin{aligned}
& z e^m, \dots, z^t e^m, \dots, x^{m-1} z^m e^m, \dots, x^{m-1} z^{(m-1)+t} e^m, \\
& z f e^{m-1}, \dots, z^t f e^{m-1}, \dots, x^{m-2} z^{m-1} f e^{m-1}, \dots, x^{m-2} z^{(m-2)+t} f e^{m-1}, \\
& \vdots \\
& z f^{m-2} e^2, \dots, z^t f^{m-2} e^2, x z^2 f^{m-2} e^2, \dots, x z^{1+t} f^{m-2} e^2, \\
& z f^{m-1} e, \dots, z^t f^{m-1} e.
\end{aligned}$$

Therefore the remaining rows in M corresponding to h -shifts are

$$\begin{aligned}
& x^m z^{m+1} e^m, \dots, x^m z^{m+t} e^m, \\
& x^{m-1} z^m f e^{m-1}, \dots, x^{m-1} z^{(m-1)+t} f e^{m-1}, \\
& \vdots \\
& x z^2 f^{m-1} e, \dots, x z^{t+1} f^{m-1} e, \\
& z f^m, \dots, z^t f^m, \text{ and its corresponding } h\text{-shifts can be written as}
\end{aligned}$$

$$h_s(x, y, z) = x^{l_1} z^{l_2} (f(x, y, z))^k e^{m-k} \text{ for } k = 0, \dots, m, l_1 = m - k, l_2 = l_1 + 1, \dots, l_1 + t.$$

Now let S_L be the sub-lattice of L spanned by the coefficients of the vectors $g_s(xX, yY, zZ)$ and $h_s(xX, yY, zZ)$ shifts and M_s be the matrix of the lattice S_L .

Note that the matrix M_s is not square. So apply the sublattice based techniques to the basis of S_L or the rows of M_s to get a square matrix. Using that square matrix, the attack

bound can be found and is given in the following.

Applying sub-lattice based techniques to get an attack bound:

In [3], J. Blomer, A. May proposed a method to find an attack bound for low deciphering exponent in a smaller dimension than the approach by Boneh and Durfee's attack in [5]. Apply their method based on sublattice reduction techniques to our lattice S_L to get an attack bound and is described in the following.

In order to apply the Howgrave-Graham's theorem [12] by using Theorem 1.3.25, we need three short vectors in S_L as our polynomial consists of three variables. But note that M_s is not a square matrix. So, first construct a square matrix M_{sl} by removing some columns in M_s , which are small linear combination of non-removing columns in M_s . Then the short vector in M_{sl} lead to short reconstruction vector in S_L .

Construction of a square sub-matrix M_{sl} of M_s .

Columns in M and M_s are same and each column in M is nothing but the coefficients of a variable, which is a leading monomial of the polynomial g or h -shifts. The first $(\frac{1}{6}m^3 + m^2 + \frac{11}{6}m + 1)$ and remaining $(\frac{1}{2}(m^2 + m)t + (m + 1)t)$ columns are corresponding to the leading monomial of the polynomials g and h -shifts respectively. Therefore,

1. the first $(\frac{1}{6}m^3 + m^2 + \frac{11}{6}m + 1)$ columns are the coefficients of the each variable $x^{i_1}y^{i_2}z^{i_3}$ for $i_1 = i_2 = k, i_3 = 0$ and $i_1 = k + 1, \dots, m, i_2 = k, i_3 = 0, \dots, (i_1 - i_2)$ and remaining $(\frac{1}{2}(m^2 + m)t + (m + 1)t)$ columns are the coefficients of the each variable $x^{i_1}y^{i_2}z^{i_3}$ for $i_1 = i_2 = k, i_3 = 1, \dots, t$ and $i_1 = k + 1, \dots, m, i_2 = k, i_3 = (i_1 - i_2) + 1, \dots, (i_1 - i_2) + t$. So the variable $x^{i_1}y^{i_2}z^{i_3}$ corresponds a column in first $(\frac{1}{6}m^3 + m^2 + \frac{11}{6}m + 1)$ columns if $i_1 \geq i_2 + i_3$ and corresponds a column in remaining $(\frac{1}{2}(m^2 + m)t + (m + 1)t)$ columns if $i_1 < i_2 + i_3$.

2. As $1, x, xy, xz$ are the monomials of f , the set of all monomials of f^m for $m \geq 0$ is $\{x^{i_1}y^{i_2}z^{i_3}; i_1 = 0, \dots, m, i_2 = 0, \dots, i_1, i_3 = 0, \dots, i_1 - i_2\}$. Therefore, the coefficient of the variable $x^{i_1}y^{i_2}z^{i_3}$ in f^m is non-zero if and only if $i_3 \leq i_1 - i_2$, i.e., $i_1 \geq i_2 + i_3$.

Remove columns in M_s corresponding to the coefficients of the variable $x^a y^b z^c$ for all $0 \leq a \leq m - 1$ and note that every such column is $\left(\frac{m-(a-b)}{(m-a)!b!}\right) \cdot \frac{1}{X^{m-a}Y^{m-a}}$ multiple of a non-removed column, corresponding to the coefficients of $x^m y^{m-(a-b)} z^c$ and is proved in the following theorem.

Theorem 5.2.2. Each column in M_s corresponding to the coefficients of the variable $x^a y^b z^c$, a leading monomial of the polynomial g or h -shifts, for all $0 \leq a \leq m - 1$ is $\left(\frac{m-(a-b)}{(m-a)!b!}\right) \cdot \frac{1}{X^{m-a}Y^{m-a}}$ multiple of a non-removed column, represents the coefficients of the variable $x^m y^{m-(a-b)} z^c$.

Proof. First assume that $|k_0| \leq |k_1|$, then $f(x, y, z) = (N + 1)x + xy + 2^n xz - 1$.

For $n = 0, \dots, m, k_1 = m - n, k_2 = 0, \dots, k_1$, the g_s -shifts $x^{k_1} z^{k_2} f^n e^{k_1}$ corresponds first $(\frac{1}{6}m^3 + m^2 + \frac{11}{6}m + 1)$ rows in M_s and for $n = 0, \dots, m, k_1 = m - n, k_2 = k_1 + 1, \dots, k_1 + t$, the h_s -shifts $x^{k_1} z^{k_2} f^n e^{k_1}$ corresponds remaining rows in M_s . We prove this theorem in two cases.

Case(i): Any column in first $(\frac{1}{6}m^3 + m^2 + \frac{11}{6}m + 1)$ columns of M_s . i.e., a column corresponding coefficients of a variable $x^a y^b z^c$ with $a \geq b + c$, from the above analysis in (1).

Given that $0 \leq a \leq m - 1$. From the above analysis in (1) and (2), the coefficient of $x^a y^b z^c$ is non-zero in g_s -shifts $x^{k_1} z^{k_2} f^n e^{k_1}$ if and only if $a \geq k_1, b \leq m - k_1, c \geq k_2$ and $a - k_1 \geq b + (c - k_2)$. As $k_1 \geq k_2, k_2 \geq 0$ and $a - k_1 \geq b + (c - k_2)$, $\max\{0, k_1 - (a - (b + c))\} \leq k_2 \leq \min\{k_1, c\}$ and also as $a - k_1 < b + (c - k_2)$ for $k_1 > a - b, k_1$ is such that $0 \leq k_1 \leq a - b$.

Therefore, the coefficient of $x^a y^b z^c$ is non-zero in g_s -shifts $x^{k_1} z^{k_2} f^n e^{k_1}$ if and only if $a \geq k_1, b \leq m - k_1, c \geq k_2$ and $k_1 = 0, \dots, a - b, k_2 = \max\{0, k_1 - (a - (b + c))\}, \dots, \min\{k_1, c\}$.

Similarly we can prove that, the coefficient of $x^a y^b z^c$ is non-zero in h_s -shifts $x^{k_1} z^{k_2} f^n e^{k_1}$ if and only if $a \geq k_1, b \leq m - k_1, c \geq k_2$ and $k_1 = 0, \dots, c, k_2 = k_1 + 1, \dots, \min\{c, k_1 + t\}$ using the inequalities $k_1 + 1 \leq k_2 \leq k_1 + t, a \geq b + c$ and analysis in (1) and (2), and say $\min\{c, k_1 + t\} = l_t$

The formula for finding a coefficient of a variable $x^{l_1} y^{l_2} z^{l_3} = (1)^{n-l_1} x^{l_1-(l_2+l_3)} (xz)^{l_3} (xy)^{l_2}$ for $l_1 \leq n - 1$ in f^n is

$$\frac{n!}{(n-l_1)!(l_1-(l_2+l_3))!l_2!l_3!} (-1)^{n-l_1} (N+1)^{l_1-(l_2+l_3)} (2^n)^{l_3}$$

and coefficient of $x^a y^b z^c$ in $x^{k_1} y^{k_2} f^n e^{k_1}$ is nothing but a coefficient of $x^{a-k_1} y^b z^{c-k_2}$ in f^n .

Note that a column corresponding to a variable $x^m y^{m-a} z^c$ is in the non-removing columns in M_s and coefficient of $x^m y^{m-a} z^c$ is zero for $k_1 > a - b$ in g_s -shifts, $k_1 > c$ in h_s -shifts. The columns corresponding to a variable $x^a y^b z^c$ and a variable $x^m y^{m-a} z^c$ only with non-zero terms is depicted in Table 5.6.

Therefore, from Table 5.6 the result holds in this case.

Case(ii): Any column in remaining $(\frac{1}{2}(m^2 + m)t + (m + 1)t)$ columns of M_s , i.e., a column corresponding coefficients of a variable $x^a y^b z^c$ with $a < b + c$, from the above analysis in (1).

The coefficient of $x^a y^b z^c$ is non-zero in g_s -shifts $x^{k_1} z^{k_2} f^n e^{k_1}$ if and only if $a \geq k_1, b \leq m - k_1, c \geq k_2, a - k_1 \geq b + (c - k_2)$ and note for $a < b + c, a - k_1 < b + (c - k_2)$ as $k_1 \geq k_2$ in g_s -shifts. So the coefficient of $x^a y^b z^c$ is zero in all rows corresponding to g_s -shifts.

The coefficient of $x^a y^b z^c$ is non-zero in h_s -shifts $x^{k_1} z^{k_2} f^n e^{k_1}$ if and only if $a \geq k_1, b \leq m - k_1, c \geq k_2$ and $a - k_1 \geq b + (c - k_2)$. For $k_1 > a - b, a - k_1 < b + (c - k_2)$ and from the inequalities $k_1 + 1 \leq k_2 \leq k_1 + t, a - k_1 \geq b + (c - k_2)$, we have the coefficient of $x^a y^b z^c$ is non-zero in h_s -shifts $x^{k_1} z^{k_2} f^n e^{k_1}$ if and only if $a \geq k_1, b \leq m - k_1, c \geq k_2$ and $k_1 = 0, \dots, a - b, k_2 = \max\{k_1 + 1, k_1 + (b + c) - a\}, \dots, \min\{c, k_1 + t\}$. Take $l_t = \min\{c, k_1 + t\}$.

Note that coefficient of $x^m y^{m-a} z^c$ is zero in all g_s -shifts as $a > c$ and for $k_1 > a - b$ in h_s -shifts. The columns corresponding to a variable $x^a y^b z^c$ and a variable $x^m y^{m-a} z^c$ only with non-zero terms is depicted in Table 5.7. Therefore, from Table 5.7 the result holds in this case.

Now apply the above analysis to the polynomial $f(x, y, z) = 2^{n'} x(N + 1) + xy + 2^{n'} xz - 2^{n'}$ for $|k_1| \leq |k_0|$, then this result is obtained. ■

Rows corresponding to g and h shifts	Column corresponding to $x^a y^b z^c$	Column corresponding to $x^m y^{m-a} z^c$
$x^{\alpha-b} z^c f^{m-(a-b)} e^{a-b}$	$\frac{(m-a)!}{(m-a)!b!} (-1)^{m-a} X^a Y^b Z^c e^{a-b}$	$X^m Y^{m-(a-b)} Z^c e^{a-b}$
$x^{\alpha-b-1} z^{c-1} f^{m-(a-b-1)} e^{a-b-1}$	$\frac{(m-a-1)!}{(m-a)!b!} (-1)^{m-a} X^a Y^b Z^c e^{a-b-1}$	$\frac{(m-a-1)!}{(m-a)!b!} (2^n)^m X^m Y^{m-(a-b)} Z^c e^{a-b-1}$
$x^{\alpha-b-1} z^c f^{m-(a-b-1)} e^{a-b-1}$	$\frac{(m-a-1)!}{(m-a)!b!} (-1)^{m-a} (N+1) X^a Y^b Z^c e^{a-b-1}$	$\frac{(m-a-1)!}{(m-a)!b!} (N+1) X^m Y^{m-(a-b)} Z^c e^{a-b-1}$
\vdots	\vdots	\vdots
$x^{\alpha-b-(c-1)} z^c f^{m-(a-b)-(c-1)} e^{a-b-(c-1)}$	$\frac{(m-a-b+c-1)!}{(m-a)!b!c!} (-1)^{m-a} (2^n)^{c-1} X^a Y^b Z^c e^{a-b-(c-1)}$	$\frac{(m-a-b+c-1)!}{(m-a)!b!c!} (2^n)^{c-1} X^m Y^{m-(a-b)} Z^c e^{a-b-(c-1)}$
\vdots	\vdots	\vdots
$x^{\alpha-b-(c-1)} z^c f^{m-(a-b)-(c-1)} e^{a-b-(c-1)}$	$\frac{(m-a-b+c-1)!}{(m-a)!b!c!} (-1)^{m-a} (N+1)^{c-1} X^a Y^b Z^c e^{a-b-(c-1)}$	$\frac{(m-a-b+c-1)!}{(m-a)!b!c!} (N+1)^{c-1} X^m Y^{m-(a-b)} Z^c e^{a-b-(c-1)}$
$x^{\alpha-b-c} f^{m-(a-b)+c} e^{a-(b+c)}$	$\frac{(m-a-b+c)!}{(m-a)!b!c!} (-1)^{m-a} (2^n)^c X^a Y^b Z^c e^{a-b-c}$	$\frac{(m-a-b+c)!}{(m-a)!b!c!} (2^n)^c X^m Y^{m-(a-b)} Z^c e^{a-b-c}$
\vdots	\vdots	\vdots
$x^{\alpha-b-c} z^c f^{m-(a-b)+c} e^{a-(b+c)}$	$\frac{(m-a-b+c)!}{(m-a)!b!c!} (-1)^{m-a} (N+1)^c X^a Y^b Z^c e^{a-b-c}$	$\frac{(m-a-b+c)!}{(m-a)!b!c!} (N+1)^c X^m Y^{m-(a-b)} Z^c e^{a-b-c}$
\vdots	\vdots	\vdots
f^m	$\frac{m!}{(m-a)!b!c!(a-(b+c))!} (-1)^{m-a} (N+1)^{a-(b+c)} (2^n)^c X^a Y^b Z^c$	$\frac{m!}{(m-a)!b!c!(a-(b+c))!} (N+1)^{a-(b+c)} (2^n)^c X^m Y^{m-(a-b)} Z^c$
$x^{\alpha-1} z^c f^{m-(c-1)} e^{c-1}$	$\frac{(m-c-1)!}{(m-a)!b!(a-(b+c)+1)!} (-1)^{m-a} (N+1)^{a-(b+c)+1} X^a Y^b Z^c e^{c-1}$	$\frac{(m-c-1)!}{(m-a)!b!(a-(b+c)+1)!} (N+1)^{a-(b+c)+1} X^m Y^{m-(a-b)} Z^c e^{c-1}$
\vdots	\vdots	\vdots
$x^{\alpha} z^2 f^{m-1} e$	$\frac{(m-1)!}{(m-a)!b!(c-2)!(a-(b+c)+1)!} (-1)^{m-a} (N+1)^{a-(b+c)+1} (2^n)^{c-2} X^a Y^b Z^c e$	$\frac{(m-1)!}{(m-a)!b!(c-2)!(a-(b+c)+1)!} (N+1)^{a-(b+c)+1} (2^n)^{c-2} X^m Y^{m-(a-b)} Z^c e$
\vdots	\vdots	\vdots
$x^{\alpha} z^t f^{m-1} e$	$\frac{(m-1)!}{(m-a)!b!(c-t)!(a-(b+c)+t-1)!} (-1)^{m-a} (N+1)^{a-(b+c)+t-1} (2^n)^{c-t} X^a Y^b Z^c e$	$\frac{(m-1)!}{(m-a)!b!(c-t)!(a-(b+c)+t-1)!} (N+1)^{a-(b+c)+t-1} (2^n)^{c-t} X^m Y^{m-(a-b)} Z^c e$
$z^m f^m$	$\frac{m!}{(m-a)!b!(c-1)!(a-(b+c)+1)!} (-1)^{m-a} (N+1)^{a-(b+c)+1} (2^n)^{c-1} X^a Y^b Z^c$	$\frac{m!}{(m-a)!b!(c-1)!(a-(b+c)+1)!} (N+1)^{a-(b+c)+1} (2^n)^{c-1} X^m Y^{m-(a-b)} Z^c$
\vdots	\vdots	\vdots
$z^t f^m$	$\frac{m!}{(m-a)!b!(c-t)!(a-(b+c)+t)!} (-1)^{m-a} (N+1)^{a-(b+c)+t} (2^n)^{c-t} X^a Y^b Z^c$	$\frac{m!}{(m-a)!b!(c-t)!(a-(b+c)+t)!} (-1)^{m-a} (N+1)^{a-(b+c)+t} (2^n)^{c-t} X^m Y^{m-(a-b)} Z^c$

Table 5.6: A column in first $(\frac{1}{6}m^3 + m^2 + \frac{11}{6}m + 1)$ columns of M_s and a column corresponding to coefficients of a variable $x^m y^{m-a} z^c$ only with non-zero terms.

Rows corresponding to g and h shifts	Column corresponding to $x^a y^b z^c$	Column corresponding to $x^m y^{m-a} z^c$
$x^{a-b} z^c f^{m-(a-b)} e^{a-b}$	$\frac{(m-(a-b))!}{(m-a)!b!} (-1)^{m-a} X^a Y^b Z^c e^{a-b}$	$X^m Y^{m-(a-b)} Z^c e^{a-b}$
\vdots	\vdots	\vdots
$x^2 z^{(b+c)-a+2} f^{m-2} e^2$	$\frac{(m-2)!}{(m-a)!b!(a-b-2)!} (-1)^{m-a} (2^n)^{(a-b)-2} X^a Y^b Z^c e^2$	$\frac{(m-2)!}{(m-(a-b))!(a-b-2)!} (2^n)^{(a-b)-2} X^m Y^{m-(a-b)} Z^c e^2$
\vdots	\vdots	\vdots
$x z^{(b+c)-a+1} f^{m-1} e$	$\frac{(m-2)!}{(m-a)!b!(c-t)!(t-(b+c)-a+2)!} (-1)^{m-a} (N+1)^{t-(b+c)-a+2} (2^n)^{c-t} X^a Y^b Z^c e^2$	$\frac{(m-2)!}{(m-(a-b))!(c-t)!(t-(b+c)-a+2)!} (N+1)^{t-(b+c)-a+2} (2^n)^{c-t} X^m Y^{m-(a-b)} Z^c e^2$
\vdots	\vdots	\vdots
$x z^{(b+c)-a+1} f^{m-1} e$	$\frac{(m-1)!}{(m-a)!b!(a-b-1)!} (-1)^{m-a} (2^n)^{(a-b)-1} X^a Y^b Z^c e$	$\frac{(m-1)!}{(m-(a-b))!(a-b-1)!} (2^n)^{(a-b)-1} X^m Y^{m-(a-b)} Z^c e$
\vdots	\vdots	\vdots
$x z^t f^{m-1} e$	$\frac{(m-1)!}{(m-a)!b!(c-t)!(t-(b+c)-a+1)!} (-1)^{m-a} (N+1)^{t-(b+c)-a+1} (2^n)^{c-t} X^a Y^b Z^c e$	$\frac{(m-1)!}{(m-(a-b))!(c-t)!(t-(b+c)-a+1)!} (N+1)^{t-(b+c)-a+1} (2^n)^{c-t} X^m Y^{m-(a-b)} Z^c e$
$z^{b+c-a} f^m$	$\frac{m!}{(m-a)!b!(a-b)!} (-1)^{m-a} (2^n)^{a-b} X^a Y^b Z^c$	$\frac{m!}{(m-(a-b))!(a-b)!} (2^n)^{a-b} X^m Y^{m-(a-b)} Z^c$
\vdots	\vdots	\vdots
$z^t f^m$	$\frac{m!}{(m-a)!b!(c-t)!(t-(b+c)-a)!} (-1)^{m-a} (N+1)^{t-(b+c)-a} (2^n)^{c-t} X^a Y^b Z^c$	$\frac{m!}{(m-(a-b))!(c-t)!(t-(b+c)-a)!} (-1)^{m-a} (N+1)^{t-(b+c)-a} (2^n)^{c-t} X^m Y^{m-(a-b)} Z^c$

Table 5.7: A column in the last $(\frac{1}{2}(m^2 + m)t + (m + 1)t)$ columns of M_s and a column corresponding to coefficients of a variable $x^m y^{m-a} z^c$ only with non-zero terms.

From the above theorem, all columns corresponding to a variable $x^a y^b z^c$ for all $0 \leq a \leq m-1$ are depending on a non-removed column, corresponding to a variable $x^m y^{m-(a-b)} z^c$ in M_s . Let M_{sl} be a matrix formed by removing all above columns from the matrix M_s and S_l be a lattice spanned by rows of M_{sl} . Then the short vector in S_l lead to short reconstruction vector in S_L , i.e., if $u = \sum_{b \in B} c_b b$ is a short vector in S_l then this lead to a short vector $\bar{u} = \sum_{b \in \bar{B}} c_b b$ (same coefficients c_b) in S_L where B and \bar{B} are the basis for S_l and S_L respectively.

As we removed all depending columns in M_s to form a matrix M_{sl} , apply the lattice based techniques to S_l instead of S_L to get an attack bound and this lattice reduction techniques gives a required short vectors in S_L for a given bound.

The matrix M_{sl} is lower triangular with rows same as in M_s and each column corresponding to coefficients of one of the variables (leading monomials of g_s and h_s -shifts)

$$\begin{array}{l}
 g_s\text{-shift} \left\{ \begin{array}{l} x^m, x^m z, \dots, x^m z^m, \\ x^m y, \dots, x^m y z^{m-1}, \\ \vdots \\ x^m y^{m-1}, x^m y^{m-1} z, \\ x^m y^m, \end{array} \right. \\
 \\
 h_s\text{-shift} \left\{ \begin{array}{l} x^m z^{m+1}, \dots, x^m z^{m+t}, \\ x^m y z^m, \dots, x^m y z^{(m-1)+t}, \\ \vdots \\ x^m y^{m-1} z^2, \dots, x^m y^{m-1} z^{1+t}, \\ x^m y^m z, \dots, x^m y^m z^t. \end{array} \right.
 \end{array}$$

Therefore S_l is a lattice spanned by coefficient vectors of the shift polynomials $g_{sl}(xX, yY, zZ)$ and $h_{sl}(xX, yY, zZ)$ where

$$g_{sl}(x, y, z) = x^{l_1} z^{l_2} (f(x, y, z) - \text{constant term of } f)^n e^{l_1} \text{ for } n = 0, \dots, m, l_1 = m - n, l_2 = 0, \dots, l_1 \text{ and}$$

$$h_{sl}(x, y, z) = x^{l_1} z^{l_2} (f(x, y, z) - \text{constant term of } f)^n e^{l_1} \text{ for } n = 0, \dots, m, l_1 = m - n, l_2 = l_1 + 1, \dots, l_1 + t.$$

$$\text{Since } S_l \text{ is full-rank lattice, } \det S_l = \det M_{sl} = e^{n(e)} X^{n(X)} Y^{n(Y)} Z^{n(Z)}$$

where $n(e), n(X), n(Y), n(Z)$ are denotes the number of $e's, X's, Y's, Z's$ in all the diagonal elements of M_{sl} respectively. As $x^n y^n$ is a leading monomial of f^n with coefficient 1, we have

$$\begin{aligned} n(e) &= \sum_{n=0}^m \sum_{l_1=m-n} \sum_{l_2=0}^{l_1} l_1 + \sum_{n=0}^m \sum_{l_1=m-n} \sum_{l_2=l_1+1}^{l_1+t} l_1 \\ &= (1/3)m^3 + m^2 + (1/2)(m^2 + m)t + (2/3)m, \end{aligned}$$

$$\begin{aligned} n(X) &= \sum_{n=0}^m \sum_{l_1=m-n} \sum_{l_2=0}^{l_1} n + l_1 + \sum_{n=0}^m \sum_{l_1=m-n} \sum_{l_2=l_1+1}^{l_1+t} n + l_1 \\ &= (1/2)m^3 + (3/2)m^2 + (m^2 + m)t + m, \end{aligned}$$

$$\begin{aligned} n(Y) &= \sum_{n=0}^m \sum_{l_1=m-n} \sum_{l_2=0}^{l_1} n + \sum_{n=0}^m \sum_{l_1=m-n} \sum_{l_2=l_1+1}^{l_1+t} n \\ &= (1/6)m^3 + (1/2)m^2 + (1/2)(m^2 + m)t + (1/3)m, \end{aligned}$$

$$\begin{aligned} n(Z) &= \sum_{n=0}^m \sum_{l_1=m-n} \sum_{l_2=0}^{l_1} l_2 + \sum_{n=0}^m \sum_{l_1=m-n} \sum_{l_2=l_1+1}^{l_1+t} l_2 \\ &= (1/6)m^3 + (1/2)(m+1)t^2 + (1/2)m^2 + (1/2)(m^2 + 2m + 1)t + (1/3)m \end{aligned}$$

$$\begin{aligned} \text{and } \dim(S_l) = \omega &= \sum_{n=0}^m \sum_{l_1=m-n} \sum_{l_2=0}^{l_1} 1 + \sum_{n=0}^m \sum_{l_1=m-n} \sum_{l_2=l_1+1}^{l_1+t} 1 \\ &= (1/2)m^2 + (m+1)t + (3/2)m + 1. \end{aligned}$$

Take $t = \tau m$, then for sufficiently large m , the exponents $n(e), n(X), n(Y), n(Z)$ and the dimension ω reduce to

$$\begin{aligned}\omega &= \left(\frac{1}{2} + \tau\right) m^2 + o(m^2), \\ n(e) &= \left(\frac{1}{3} + \frac{1}{2}\tau\right) m^3 + o(m^3), \\ n(X) &= \left(\frac{1}{2} + \tau\right) m^3 + o(m^3), \\ n(Y) &= \left(\frac{1}{6} + \frac{1}{2}\tau\right) m^3 + o(m^3), \\ n(Z) &= \left(\frac{1}{6} + \frac{1}{2}\tau + \frac{1}{2}\tau^2\right) m^3 + o(m^3).\end{aligned}$$

Applying the LLL algorithm to the basis vectors of the lattice S_l , i.e., coefficient vectors of the shift polynomials, we get a LLL-reduced basis say $\{v_1, v_2, \dots, v_\omega\}$ and from the Theorem 1.3.25 we have

$$\|v_1\| \leq \|v_2\| \leq \|v_3\| \leq 2^{\frac{\omega(\omega-1)}{4(\omega-2)}} \det(S_l)^{\frac{1}{\omega-2}}.$$

In order to apply the generalization of Howgrave-Graham result in Theorem 1.3.25, we need the following inequality

$$2^{\frac{\omega(\omega-1)}{4(\omega-2)}} \det(S_l)^{\frac{1}{\omega-2}} < \frac{e^m}{\sqrt{\omega}}.$$

from this, we deduce

$$\det(S_l) < \frac{1}{\left(2^{\frac{\omega(\omega-1)}{4(\omega-2)}} \sqrt{\omega}\right)^{\omega-2}} e^{m(\omega-2)} < \frac{1}{\left(2^{\frac{\omega(\omega-1)}{4(\omega-2)}} \sqrt{\omega}\right)^{\omega-2}} e^{m\omega}.$$

As the dimension ω is not depending on the public encryption exponent e , $\frac{1}{\left(2^{\frac{\omega(\omega-1)}{4(\omega-2)}} \sqrt{\omega}\right)^{\omega-2}}$

is a fixed constant, so we need the inequality $\det(S_l) < e^{m\omega}$,

i.e., $e^{n(e)} X^{n(X)} Y^{n(Y)} Z^{n(Z)} < e^{m\omega}$.

Substitute all values and taking logarithms, neglecting the lower order terms and after simplifying by m^3 we get

$$(-1 - 3\tau)\alpha + (3 + 6\tau)\delta + (1 + 3\tau)\gamma_1 + (1 + 3\tau + 3\tau^2)\gamma_2 < 0.$$

The left hand side inequality is minimized at $\tau = \frac{\alpha - (2\delta + \gamma_1 + \gamma_2)}{2\gamma_2}$ and putting this value in the above inequality we get

$$\delta < \frac{1}{2}\alpha - \frac{1}{2}\gamma_1 - \frac{1}{6}\sqrt{6(\alpha - \gamma_1)\gamma_2 + 3\gamma_2^2}.$$

From the first three short vectors v_1, v_2 and v_3 in LLL reduced basis of a basis B in S_l we consider three polynomials $g_1(x, y, z), g_2(x, y, z)$ and $g_3(x, y, z)$ over \mathbb{Z} such that $g_1(x_0, y_0, z_0) = g_2(x_0, y_0, z_0) = g_3(x_0, y_0, z_0) = 0$. These short vectors v_1, v_2 and v_3 lead to a short vector \bar{v}_1, \bar{v}_2 and \bar{v}_3 respectively and $\bar{g}_1(x, y, z), \bar{g}_2(x, y, z)$ and $\bar{g}_3(x, y, z)$ its corresponding polynomials. Apply the same analysis in the previous section to the above polynomials to get the factors p and q of RSA modulus N .

Theorem 5.2.3. Let $N = pq$ be an RSA modulus with $q < p < 2q$. Let $e = N^\alpha, X = N^\delta, Y = N^{\gamma_1}, Z = N^{\gamma_2}$ and k be the multiplicative inverse of $\varphi(N)$ modulo e . Suppose the prime sum $p + q$ is of the form $p + q = 2^n k_0 + k_1$, for a known positive integer n and for $|k| \leq X, \max\{|k_0|, |k_1|\} \leq Y$ and $\min\{|k_0|, |k_1|\} \leq Z$ one can factor N in polynomial time if

$$\delta < \frac{1}{2}\alpha - \frac{1}{2}\gamma_1 - \frac{1}{6}\sqrt{6(\alpha - \gamma_1)\gamma_2 + 3\gamma_2^2}. \quad (5.2.3)$$

Proof. Follows from the above argument and the LLL lattice basis reduction algorithm operates in polynomial time [29]. ■

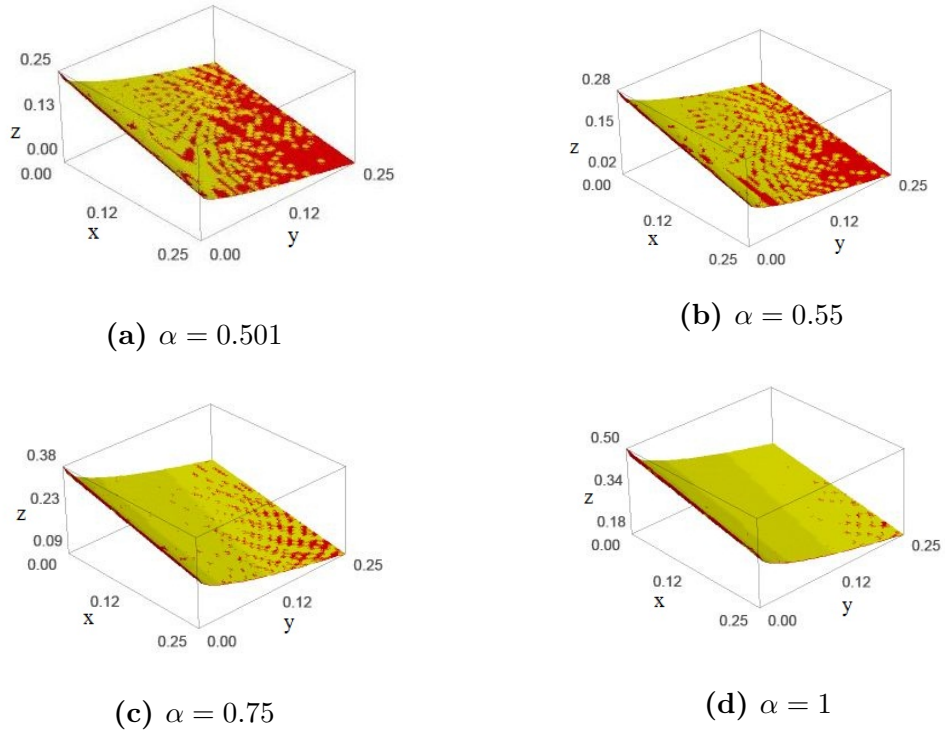


Figure 5.1: The region of δ_{sl} and δ_L for $\alpha = 0.501, 0.55, 0.75, 1$.

Note that for any given primes p and q with $q < p < 2q$, we can always find a positive integer n such that $p + q = 2^n k_0 + k_1$ where $0 \leq |k_0|, |k_1| \leq \approx 0.25$. A typical example is $2^n \approx \frac{3}{\sqrt{2}} N^{0.25}$ as $p + q < \frac{3}{\sqrt{2}} N^{0.5}$ [34]. So take γ_1 and γ_2 in the range $(0, 0.25)$. Let δ_L and δ_{sl} be the bounds for δ in inequalities (5.2.2) and (5.2.3) respectively. Then note that δ_{sl} is slightly larger than δ_L and is depicted in Figure 5.1 for $\alpha = 0.51, 0.55, 0.750$ and 1.

In the Figure 5.1, x, y, z -axis represents γ_1, γ_2 , bound for δ respectively and yellow, red regions represents δ_{sl}, δ_L respectively. From this figure, it is noted that the yellow region is slightly above the red region, i.e., δ_{sl} is slightly greater than δ_L and this improvement increases when the values of α increases.

As the dimension of L is $(1/6)m^3 + (1/2)m^2(t + 2) + (1/6)m(9t + 11) + (t + 1)$ for $t = \left(\frac{\alpha - (2\delta + \gamma_1 + \gamma_2)}{3\gamma_2}\right)m$ [19] and S_l is $(1/2)m^2 + (m + 1)t + (3/2)m + 1$ for $t = \left(\frac{\alpha - (2\delta + \gamma_1 + \gamma_2)}{2\gamma_2}\right)m$, note the dimension of S_l is $(1/6)m^3 + (1/3)t(m^2 - 1) + (1/2)m^2 + (1/3)m$, for $t = \left(\frac{\alpha - (2\delta + \gamma_1 + \gamma_2)}{2\gamma_2}\right)$ smaller than the dimension of L .

A new attack bound for deciphering exponent d with a composed prime sum:

In this section, we apply the same analysis for getting bound for d which we have earlier obtained resultant bound for k .

From the relation $ed \equiv 1 \pmod{\varphi(N)}$, we get

$$t(N + 1 - (2^n k_0 + k_1)) + 1 \equiv 0 \pmod{e} \quad (5.2.4)$$

for $t = \frac{ed-1}{\varphi(N)}$ and the prime sum $p + q = 2^n k_0 + k_1$.

Now define

$$f'(x, y, z) = \begin{cases} (N + 1)x + xy + (2^n)xz + 1 & \text{if } |k_0| \leq |k_1| \\ 2^{n'}x(N + 1) + xy + 2^{n'}xz + 2^{n'} & \text{if } |k_1| \leq |k_0|. \end{cases}$$

From equation (5.2.4), note that if $|k_0| \leq |k_1|$ then $(t, -k_1, -k_0)$ is a solution and if $|k_1| \leq |k_0|$ then $(t, -k_0, -k_1)$ is a solution for the modular polynomial equation $f'(x, y, z) \equiv 0 \pmod{e}$.

As the polynomials $f(x, y, z)$, $f'(x, y, z)$ differ by signs only, we can implement the above argument for $f(x, y, z)$ to $f'(x, y, z)$ and obtained new bound on d for $t < d = N^{\delta'}$, $\max |k_0|, |k_1| \leq N^{\gamma_1}$, $\min |k_0|, |k_1| \leq N^{\gamma_2}$ and for $e = N^\alpha$ is

$$\delta' < \frac{1}{2}\alpha - \frac{1}{2}\gamma_1 - \frac{1}{6}\sqrt{6(\alpha - \gamma_1)\gamma_2 + 3\gamma_2^2}. \quad (5.2.5)$$

For $\alpha = 1$, the Boneh and Durfee's bound for $d = N^{\delta'}$ is $N^{0.292}$. The new bound on d may overcome this bound for $\alpha = 1$ and for some values of γ_1 and γ_2 and that values are depicted in the following table.

γ_1	γ_2	δ' new bound
0.40	0.005-0	0.2929-0.3
0.35	0.0094-0	0.2929-0.325
0.25	0.052-0	0.2929-0.375
0.15	0.1152-0	0.2929-0.425
0.01	0.009-0	0.4563-0.495

Table 5.8: For $\alpha = 1$, the values of bound on $d = N^{\delta'}$ in terms of γ_1 and γ_2 .

For $e = N^\alpha$, $|p - q| = N^\beta$, $\max\{|k_0|, |k_1|\} \leq N^{\gamma_1}$ and $\min\{|k_0|, |k_1|\} \leq N^{\gamma_2}$ and for N^δ , an upper bound for $\varphi(N)^{-1} \bmod e$, the refinement process of RSA attack bounds on δ is depicted in the following table.

Lattice based attack	Attack bound
Attacks with x -shifts	$\delta < (\alpha - \beta)/2$
Attack with x and y shifts	$\delta < (3\alpha + \beta - 2\sqrt{\beta(3\alpha + \beta)})/3$
Attack with sublattice based techniques	$\alpha - \beta(1 + \alpha) < \delta < \alpha - \sqrt{\alpha\beta}$
Attack with sublattice based techniques with lower dimension	$\delta < (2\alpha - 6\beta + 2\sqrt{\alpha^2 - \alpha\beta + 4\beta^2})/5$
Attack with for $p + q$ as a composed form	$\delta < \frac{1}{2}\alpha - \frac{1}{2}\gamma_1 + \frac{1}{16}\gamma_2 - \frac{1}{16}\sqrt{48(\alpha - \gamma_1)\gamma_2 + 33\gamma_2^2}$
Attack with for $p + q$ as a composed form and with sublattice based techniques	$\delta < \frac{1}{2}\alpha - \frac{1}{2}\gamma_1 - \frac{1}{6}\sqrt{6(\alpha - \gamma_1)\gamma_2 + 3\gamma_2^2}$

Table 5.9: Refinement process of RSA attack bounds on δ for $(\varphi(N)^{-1} \bmod e) \leq N^\delta$.

5.3 Extending Lattice-Based Attacks to an RSA-Like Cryptosystem over $E(\mathbb{Z}_{pq})$

All the lattice-based attacks on RSA for small multiplicative inverse of $\varphi(N)$ modulo e may be extended to RSA-like cryptosystem over elliptic curves $E(\mathbb{Z}_{pq})$ due to KMOV by repeating the argument for $\varphi(N)$ replaced by $\psi(N) = (p+1)(q+1)$.

The above lattice-based attacks on RSA for $p - q$ bounded can be extended to RSA-like cryptosystem over elliptic curves $E(\mathbb{Z}_{pq})$ due to KMOV, according to the polynomial congruence as in the following

When $p - q$ is bounded	RSA	RSA-like over $E(\mathbb{Z}_{pq})$ due to KMOV
Polynomial Congruence	$x(A + y) - 1 \equiv 0 \pmod{e}$ where $A = N + 1 - \lceil 2\sqrt{N} \rceil$.	$x(A + y) - 1 \equiv 0 \pmod{e}$ where $A = N + 1 + \lceil 2\sqrt{N} \rceil$.
Solution	$(k, -(p + q - \lceil 2\sqrt{N} \rceil))$ where $k = \varphi(N)^{-1} \pmod{e}$.	$(k, p + q - \lceil 2\sqrt{N} \rceil)$ $k = \psi(N)^{-1} \pmod{e}$.

note as the monomials are same for both the polynomials with respect to $\varphi(N)$ and $\psi(N)$, the arguments of our results when $p - q$ is bounded can be repeated for $\varphi(N)$ replaced by $\psi(N)$ then it is observed that RSA and RSA-like have same attack bounds for δ , given as:

$$\delta < \frac{\alpha - \beta}{2},$$

$$\delta < \frac{3\alpha + \beta - 2\sqrt{\beta(3\alpha + \beta)}}{3},$$

$$\alpha - \beta(1 + \alpha) < \delta < \alpha - \sqrt{\alpha\beta} \text{ and}$$

$$\delta < \frac{2\alpha - 6\beta + 2\sqrt{\alpha^2 - \alpha\beta + 4\beta^2}}{5}$$

for $p - q = N^\beta$ and N^δ is an upper bound for $\varphi(N)^{-1} \bmod e$ and $\psi(N)^{-1} \bmod e$ in RSA and RSA-like cryptosystem over elliptic curves $E(\mathbb{Z}_{pq})$ due to KMOV respectively.

The lattice-based attack on RSA with a composed prime sum $p + q = 2^n k_0 + k_1$, for known positive integer n , suitable small integers k_0, k_1 can be extended to RSA-like cryptosystem over elliptic curves $E(\mathbb{Z}_{pq})$ due to KMOV, according to the polynomial congruence as in the following

RSA attack with a composed prime sum	RSA	RSA-like over $E(\mathbb{Z}_{pq})$ due to KMOV
Polynomial Congruence for $ k_0 \leq k_1 $	$(N + 1)x + xy + 2^n xz - 1 \equiv 0 \pmod{e}$	$(N + 1)x + xy + 2^n xz - 1 \equiv 0 \pmod{e}$
Solution	$(k, -k_1, -k_0)$ where $k = \varphi(N)^{-1} \bmod e$.	(k, k_1, k_0) $k = \psi(N)^{-1} \bmod e$.
Polynomial Congruence for $ k_1 \leq k_0 $	$2^{n'}x(N + 1) + xy + 2^{n'}xz - 2^{n'} \equiv 0 \pmod{e}$	$2^{n'}x(N + 1) + xy + 2^{n'}xz - 2^{n'} \equiv 0 \pmod{e}$
Solution	$(k, -k_0, -k_1)$ where $k = \varphi(N)^{-1} \bmod e$.	(k, k_0, k_1) $k = \psi(N)^{-1} \bmod e$.

note as the monomials are same for both the polynomials with respect to $\varphi(N)$ and $\psi(N)$, the arguments of our result when the prime sum is of the form $p + q = 2^n k_0 + k_1$ can be repeated for $\varphi(N)$ replaced by $\psi(N)$ then it is observed that RSA and RSA-like have same attack bounds for δ , given as:

$$\delta < \frac{1}{2}\alpha - \frac{1}{2}\gamma_1 + \frac{1}{16}\gamma_2 - \frac{1}{16}\sqrt{48(\alpha - \gamma_1)\gamma_2 + 33\gamma_2^2}$$

$$\text{and } \delta < \frac{1}{2}\alpha - \frac{1}{2}\gamma_1 - \frac{1}{6}\sqrt{6(\alpha - \gamma_1)\gamma_2 + 3\gamma_2^2}.$$

for a composed prime sum $p + q = 2^n k_0 + k_1$ and N^δ, N^{γ_1} and N^{γ_2} are the upper bounds for $k, \max\{|k_0|, |k_1|\}$ and $\min\{|k_0|, |k_1|\}$ respectively.

5.4 Summary

In this chapter it is shown that RSA is insecure if $\varphi(N)$ has small multiplicative inverse k modulo e , the public encryption exponent. For $k \leq N^\delta$, the attack bounds for δ are described by using lattice based techniques with respect to bivariate polynomial congruence and this attack bound for δ is further refined for $\beta \approx 0.5$ by taking the prime sum $p + q$ as a composed prime sum i.e., $p + q = 2^n k_0 + k_1$ where n is a known positive integer, k_0 and k_1 are suitably small unknown integers and applying the lattice based arguments for trivariate polynomials. This refinement of attack bound for δ is depicted for certain values of α and $\beta \approx 0.5$. This refined attack bound is slightly improved by using the sub-lattice based techniques and this method requires lattice of smaller dimension than the above method. Also a new attack bound for the deciphering exponent d with above composed prime sum is given and compare it to Boneh and Durfee's bound. It is observed that these lattice-based attacks on RSA for small multiplicative inverse of $\varphi(N)$ modulo e can be extended to the RSA-like cryptosystem over $E(\mathbb{Z}_{pq})$ due to KMOV and the corresponding analysis is given.

Chapter 6

Conclusion

The idea of Wiener to obtain a convergent $\frac{e}{N}$ for certain bounds on the private exponent d by using certain estimations of $\varphi(N)$ was extended for refinement of the bounds by Weger, Maitra-Sarkar by developing certain estimates for $\varphi(N)$. The bounds on private exponent d were refined further by using the lattice reduction techniques. The lattice based attacks by Boneh-Durfee, Blömer-May, Weger and Maitra-Sarkar, gave bounds and refined the bounds for the private exponent d . In this project the existing continued fraction based and lattice based attacks that are given for RSA with low decryption exponent are extended to other variants of RSA. The advantage of lattice based attacks proposed by us is that we considered the other invariant of RSA like $p, q, \varphi(N)$ and noted that these attacks can also be mounted for the private key exponent d not in the range of existing attack bounds. It is also noted that looking at $\psi(N) = (p + 1)(q + 1)$ as the analogue of Euler's function $\varphi(N)$ in the RSA-like cryptosystem over elliptic curve $E(\mathbb{Z}_{pq})$ due to KMOV, all the lattice attacks can be extended to RSA-like cryptosystem over elliptic curve $E(\mathbb{Z}_{pq})$ due to KMOV. This may be adapted for other RSA-like cryptosystems with Dickson polynomials, Lucas sequences etc. by identifying the corresponding analogue to $\varphi(N)$.

All these attacks teach us to avoid the major difficulties while implementing RSA and sustain against all existing attacks. We conclude here and note that this study of refinement of attack bounds of RSA is useful in taking some precautionary measures in the adaptation of RSA according to the following Table 6.1 on refinement of attack bounds.

Attack	Based on theory	Refining the RSA attack bounds
Wiener's attack	continued fraction algorithm	$d < N^{0.25}$.
Weger's attack	continued fraction algorithm	$N^{0.25} < d < N^{0.75-\beta}$, for $e \approx N$ and $N^\beta = p - q $.
Maitra-Sarkar's attack	continued fraction algorithm	$N^{0.25} < d < N^{\frac{1-\gamma}{2}}$, for $e \approx N$ and $ p - \rho q \leq \frac{N^\gamma}{16}$, where $\gamma \leq \frac{1}{2}$ and $1 \leq \rho \leq 2$.
Boneh and Durfee's attack	Lattice based techniques	$d < N^{0.284}$ for $e \approx N$.
Boneh and Durfee's attack	sublattice based techniques	$d < N^{0.292}$ for $e \approx N$.
Blömer and May's attack	Sublattice based techniques with lower dimension	$d < N^{0.290}$ for $e \approx N$.
Weger's attack	Lattice based techniques	$d < N^{\frac{1}{6}(4\beta+5) - \frac{1}{3}\sqrt{(4\beta+5)(4\beta-1)}}$, for $e \approx N$ and $N^\beta = p - q $.
Weger's attack	sublattice based techniques	$N^{2-4\beta} < d < N^{1-\sqrt{2\beta-\frac{1}{3}}}$, for $e \approx N$ and $N^\beta = p - q $.
Maitra-Sarkar's attack	Lattice based techniques	$d < N^{\frac{7+13-2\sqrt{7(7+3)}}{3}}$, for $e \approx N$ and $ p - \rho q \leq \frac{N^\gamma}{16}$, where $\gamma \leq \frac{1}{2}$ and $1 \leq \rho \leq 2$.
Maitra-Sarkar's attack	sublattice based techniques	$N^{1-2\gamma} < d < N^{1-\sqrt{\gamma}}$, for $e \approx N$ and $ p - \rho q \leq \frac{N^\gamma}{16}$, where $\gamma \leq \frac{1}{2}$ and $1 \leq \rho \leq 2$.
Maitra-Sarkar's attack	sublattice based techniques with lower dimension	$d < N^{\frac{\sqrt{16\gamma^2-4\gamma+4-(6\gamma-2)}}{6}}$, for $e \approx N$ and $ p - \rho q \leq \frac{N^\gamma}{16}$, where $\gamma \leq \frac{1}{2}$ and $1 \leq \rho \leq 2$.
Nitaj and Douh's attack	Lattice based techniques	$d = Md_1 + d_0$, $\delta < \frac{1}{4}(5 - 4\gamma - \sqrt{12\alpha + 12\beta - 12\gamma + 3})$, for $e = N^\alpha$, $d_1 < N^\delta$ and $d_0 < N^\beta$.
Proposed attack when $(p-1)$ or $(q-1)$ have small multiplicative inverse	Lattice based techniques with x shifts	$\min\{(p-1)^{-1} \bmod e, (q-1)^{-1} \bmod e\} < N^{\frac{\alpha-\beta}{2}}$, for $e = N^\alpha$ and $p - q = N^\beta$.
Proposed attack when $(p-1)$ or $(q-1)$ have small multiplicative inverse	Lattice based techniques with x and y shifts	$\min\{(p-1)^{-1} \bmod e, (q-1)^{-1} \bmod e\} < N^{\frac{(3\alpha+\beta-2\sqrt{\beta(3\alpha+\beta)})}{3}}$, for $e = N^\alpha$ and $p - q = N^\beta$.
Proposed attack when $(p-1)$ or $(q-1)$ have small multiplicative inverse	Sublattice based techniques	$N^{\alpha-\beta(1+\alpha)} < \min\{(p-1)^{-1} \bmod e, (q-1)^{-1} \bmod e\} < N^{\alpha-\sqrt{\alpha\beta}}$, for $e = N^\alpha$ and $p - q = N^\beta$.
Proposed attack when $(p-1)$ or $(q-1)$ have small multiplicative inverse	Sublattice based techniques with lower dimension	$\min\{(p-1)^{-1} \bmod e, (q-1)^{-1} \bmod e\} < N^{\frac{2\alpha-6\beta+2\sqrt{\alpha^2-\alpha\beta+4\beta^2}}{6}}$, for $e = N^\alpha$ and $p - q = N^\beta$.
Proposed attack when $(p-1)$ or $(q-1)$ have small multiplicative inverse	Lattice based techniques with x shifts	$\min\{(p-1)^{-1} \bmod e, (q-1)^{-1} \bmod e\} < N^{\frac{\alpha-\gamma}{2}}$, for $e = N^\alpha$ and $ p - \rho q \leq N^\gamma$, $\gamma' \leq \frac{1}{2}$.
Proposed attack when $(p-1)$ or $(q-1)$ have small multiplicative inverse	Lattice based techniques with x and y shifts	$\min\{(p-1)^{-1} \bmod e, (q-1)^{-1} \bmod e\} < N^{\frac{(3\alpha+\gamma)-2\sqrt{\gamma(3\alpha+\gamma)}}{3}}$, for $e = N^\alpha$ and $ p - \rho q \leq N^\gamma$, $\gamma' \leq \frac{1}{2}$.
Proposed attack when $(p-1)$ or $(q-1)$ have small multiplicative inverse	Sublattice based techniques	$N^{\alpha-\gamma'(1+\alpha)} < \min\{(p-1)^{-1} \bmod e, (q-1)^{-1} \bmod e\} < N^{\alpha-\sqrt{\alpha\gamma'}}$, for $e = N^\alpha$ and $ p - \rho q \leq N^\gamma$, $\gamma' \leq \frac{1}{2}$.
Proposed attack when $(p-1)$ or $(q-1)$ have small multiplicative inverse	Sublattice based techniques with lower dimension	$\min\{(p-1)^{-1} \bmod e, (q-1)^{-1} \bmod e\} < N^{\frac{2\alpha-6\gamma'+2\sqrt{\alpha^2-\alpha\gamma'+4\gamma'^2}}{6}}$, for $e = N^\alpha$ and $ p - \rho q \leq N^\gamma$, $\gamma' \leq \frac{1}{2}$.
Proposed attack when $\varphi(N)^{-1}$ have small multiplicative inverse	Lattice based techniques with x shifts	$(\varphi(N)^{-1} \bmod e) < N^{\frac{\alpha+\beta}{2}}$, for $e = N^\alpha$ and $p - q = N^\beta$.
Proposed attack when $\varphi(N)^{-1}$ have small multiplicative inverse	Lattice based techniques with x and y shifts	$(\varphi(N)^{-1} \bmod e) < N^{\frac{(3\alpha+\beta-2\sqrt{\beta(3\alpha+\beta)})}{3}}$, for $e = N^\alpha$ and $p - q = N^\beta$.
Proposed attack when $\varphi(N)^{-1}$ have small multiplicative inverse	Sublattice based techniques	$N^{\alpha-\beta(1+\alpha)} < (\varphi(N)^{-1} \bmod e) < N^{\alpha-\sqrt{\alpha\beta}}$, for $e = N^\alpha$ and $p - q = N^\beta$.
Proposed attack when $\varphi(N)^{-1}$ have small multiplicative inverse	Sublattice based techniques with lower dimension	$(\varphi(N)^{-1} \bmod e) < N^{\frac{2\alpha-6\beta+2\sqrt{\alpha^2-\alpha\beta+4\beta^2}}{6}}$, for $e = N^\alpha$ and $p - q = N^\beta$.
Proposed attack when $\varphi(N)^{-1}$ have small multiplicative inverse and an attack bound on d	Lattice based techniques	$(\varphi(N)^{-1} \bmod e) < N^{\frac{1}{2}\alpha - \frac{1}{2}\gamma + \frac{1}{16}\gamma^2 - \frac{1}{16}\sqrt{48(\alpha-\gamma)\gamma^2 + 35\gamma^2}}$, for $e = N^\alpha$, $\max\{ k_0 , k_1 \} \leq N^{\gamma_0}$ and $\min\{ k_0 , k_1 \} \leq N^{\gamma_2}$.
with composed prime sum $p + q = 2^n k_0 + k_1$	Sublattice based techniques	$(\varphi(N)^{-1} \bmod e), d < N^{\frac{1}{2}\alpha - \frac{1}{2}\gamma_1 - \frac{1}{6}\sqrt{6(\alpha-\gamma_1)\gamma_2 + 5\gamma_2^2}}$, $\max\{ k_0 , k_1 \} \leq N^{\gamma_0}$ and $\min\{ k_0 , k_1 \} \leq N^{\gamma_2}$.

Table 6.1: Attack bounds for all described attacks on RSA.

Appendix A

Modular Arithmetic

A.1 Modular Arithmetic

Definition A.1.1. Let m be a positive integer we say a is congruent to b modulo m and write $a \equiv b \pmod{m}$ if $m|b - a$.

Theorem A.1.2. \equiv is an equivalence relation on \mathbb{Z} , the set of all integers and the equivalence classes are called residue classes denoted as \bar{a} and are given as

$$\forall a \in \mathbb{Z}, \bar{a} = \{a + mt : t \in \mathbb{Z}\}.$$

Remark A.1.3. The set of all residue classes is denoted as $\mathbb{Z}/m\mathbb{Z}$ is a finite set and $\{0,1,2,\dots,m-1\}$ are called least positive residues modulo m .

Theorem A.1.4. $\mathbb{Z}/m\mathbb{Z}$ forms a Ring with respect to addition '+' and multiplication '.' given as follows:

For any $\bar{a}, \bar{b} \in \mathbb{Z}/m\mathbb{Z}$, $\bar{a} = a + m\mathbb{Z}$, $\bar{b} = b + m\mathbb{Z}$ and

$$\bar{a} + \bar{b} = a + b + m\mathbb{Z}$$

$$\bar{a} \cdot \bar{b} = ab + m\mathbb{Z}.$$

Theorem A.1.5. The residue class $a + m\mathbb{Z}$ is invertible in $\mathbb{Z}/m\mathbb{Z}$ (i.e., the congruence $ax \equiv 1 \pmod{m}$ is solvable) if and only if $\gcd(a, m) = 1$. If $\gcd(a, m) = 1$, then the

inverse of $a + m\mathbb{Z}$ is uniquely determined (i.e, the solution x of $ax \equiv 1 \pmod{m}$ is uniquely determined mod m).

Theorem A.1.6. The residue class ring $\mathbb{Z}/m\mathbb{Z}$ is a field if and only if m is a prime number.

Definition A.1.7. The **Euler function** $\varphi : \mathbf{N} \rightarrow \mathbf{N}$ is defined as

$$\varphi(n) = \#\{m : 1 \leq m \leq n, (m, n) = 1\}.$$

Theorem A.1.8. If p is a prime then $\varphi(p) = p - 1$.

Theorem A.1.9. (Euler-Fermat:) If $\gcd(a, m) = 1$ then $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Theorem A.1.10. The set of all invertible residue classes modulo m is a finite abelian group with respect to multiplication denoted as $(\mathbb{Z}/m\mathbb{Z})^*$ is of order $\varphi(m)$.

Theorem A.1.11. (Chinese Remainder:)[1] Let m_1, m_2, \dots, m_r be positive integers that are pairwise co-prime and a_1, a_2, \dots, a_r . Then the system of congruences

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r}. \end{aligned}$$

has a unique solution modulo the product $m_1.m_2\dots m_r$.

Theorem A.1.12. Let m_1, m_2, \dots, m_n be pairwise co prime integers and let $m = m_1 m_2 \dots m_n$.

Then the map

$$\mathbb{Z}/m\mathbb{Z} \rightarrow \prod_{i=1}^n \mathbb{Z}/m_i\mathbb{Z}, a + m\mathbb{Z} \mapsto (a + m_1\mathbb{Z}, \dots, a + m_n\mathbb{Z})$$

is an isomorphism of rings.

Theorem A.1.13. Let m_1, \dots, m_r be pair wise integers and $m = \prod_{i=1}^r (m_i)$, then

$$\varphi(m) = \varphi(m_1) \dots \varphi(m_r).$$

A.1.1 Time estimates in Arithmetic

The security of a cryptosystem depends on time taken in investigating the cryptoalgorithm or the secret key parameter. Hence, studying the running time of an algorithm plays a vital role in cryptography.

In cryptographic applications multi precision integer must be added, multiplied and divided with remainder. To estimate the running time of such applications we must study how long such operations take.

Definition A.1.14. Let b be an integer greater than 1 for each positive integer there is a uniquely determined positive integer k and uniquely determined sequence $\{a_i\}_{i=1}^k$, $a_i \in \{0, \dots, b-1\}$ with $a_1 \neq 0$ and

$$\begin{aligned} a &= a_1b^{k-1} + a_2b^{k-2} + \dots + a_{k-2}b + a_k \\ &= \sum_{i=1}^k a_i b^{k-i} \end{aligned}$$

and the sequence $\{a_1, a_2, \dots, a_k\}$ is called **b -adic expansion** of ' a ' or ' a ' is a k -digit number to the base b [6].

The number of digits in the 2-adic expansion of a positive integer ' a ' is denoted as **size**(a) [6] and is given by

$$\begin{aligned} \mathbf{size}(a) &= \left\lceil \frac{\log a}{\log 2} \right\rceil + 1 \\ &= O(\log a) \end{aligned}$$

Definition A.1.15. Time taken to perform an arithmetic operations $+$ or $-$ on binary digits 1, 0, i.e., $1 \pm 1, 1 \pm 0, 0 \pm 0$, each with the carry or without a carry is called a **bit operation**.

Remark A.1.16. The amount of time taken by a computer to perform a task is propor-

tional to the number of bit operations involved in the task.

Definition A.1.17. The **time estimate of task** is defined to be the estimation of number of bit operations.

Example A.1.18. Addition of a 7-bit integer $(1110010)_2$ with a 6-bit integer $(100110)_2$ is given as,

$$\begin{array}{r} 1110010 \\ 100110 \\ \hline 10011000 \end{array}$$

The above addition we requires 8 bit operations and the time estimate taken to perform such operation is taken as 8 units.

For any $a, b \in \mathbb{Z}$, the following table represents the time for the given operation.

operation	Time
$a + b$	$O(\max\{\log a, \log b\})$
$a \cdot b$	$O(\log a \cdot \log b)$
$a = bq + r$	$O(\log b \cdot \log q)$
$\gcd(a, b)$	$O(\log a \cdot \log b)$
$(a + b) \bmod N$	$O(\log N)$
$(ab) \bmod N$	$O(\log N)^2$
$a \mid b \bmod N$	$O(\log N)^2$
$a^e \bmod N$	$O(\log e)(\log N)^2$

A.1.2 Polynomial running time algorithm

An algorithm with input integers z_1, z_2, \dots, z_N of k_1, k_2, \dots, k_N is said to have polynomial running time [17]. If there are non-negative integers e_1, e_2, \dots, e_N such that the time

estimate of algorithm denoted as T_A given as

$$T_A = O((\log Z_1)^{e_1} \cdot (\log Z_2)^{e_2} \cdot \dots \cdot (\log Z_n)^{e_n}) = O(k_1^{e_1} \cdot \dots \cdot k_N^{e_n}) \text{ [6].}$$

Definition A.1.19. An algorithm is said to be efficient if it has polynomial running time with the e_i and the O -constant are small.

Theorem A.1.20. Suppose the residue classes modulo m are represented by their least non negative representatives. Then two residue classes mod m can be added and subtracted using time and space $O(\text{size } m)$. They can be multiplied and divided using time $O((\text{size } m)^2)$ and space $O(\text{size } m)$.

Proposition A.1.21. Suppose that n known to be product of two distinct primes. Then knowledge of two primes p, q is equivalent to knowledge of $\varphi(n)$. More precisely, one can compute $\varphi(n)$ from p, q in $O(\log n)$ bit operations and one can compute p and q from n and $\varphi(n)$ in $(\log^3 n)$ bit operations.

A.1.3 Modular Exponentiation

It is a method for computing modulo n .

To compute $g^e \pmod n$,

Step 1: Express binary expression of e .

$$e = \sum_{i=0}^k x_i 2^i, x_i = 0 \text{ or } 1$$

Step 2: Succussive square g^{2^i} , $0 \leq i \leq k$

Step 3:

$$\begin{aligned} g^e &= g^{\sum_{i=0}^k x_i 2^i} \\ &= \prod_{i=0}^k (g^{2^i})^{x_i} \\ &= \prod_{i=0, x_i=1}^k g^{2^i} \end{aligned}$$

Remark A.1.22. Computation of $g^e \pmod n$ based on the computation of g^{2^i} , for $0 \leq i \leq k$ and this reduces the total number of multiplication than by usual multiplication.

Theorem A.1.23. The computation of $g^e \pmod m$ requires time $O((\mathbf{size})(\mathbf{size}^2))$.

Remark A.1.24. Modular exponentiation is in polynomial time.

Appendix B

KMOV public key cryptosystem

B.1 KMOV public key cryptosystem

$E : y^2 = x^3 + Ax + B$ is the Weierstrass form of an Elliptic curve. For any finite field \mathbb{F}_q of characteristic p , $E(\mathbb{F}_q) = \{(x, y) \in \mathbb{F}_q \times \mathbb{F}_q; y^2 = x^3 + Ax + B\} \cup \{\infty\}$ is the elliptic curve over \mathbb{F}_q . In 1985 Koblitz[27] and Miller[33] independently proposed using the group of points on an elliptic curves over finite fields in discrete log cryptosystems, as there are no sub exponential time algorithms to find the discrete log on elliptic curves.

The elliptic curves considered by Koyama-Maurer-Okamoto-Vanstone[46][50] for KMOV system are the elliptic curves in the form

$$E_b(N) : y^2 = x^3 + b \pmod{N} \text{ for } N = pq, p, q \text{ primes with } p \equiv q \equiv 2 \pmod{3}.$$

The curves $E_b(p) : y^2 = x^3 + b \pmod{p}$ and $E_b(q) : y^2 = x^3 + b \pmod{q}$ are super singular with orders $\#E_b(p) = p + 1$ & $\#E_b(q) = q + 1$. Further as the group $E(\mathbb{Z}_{pq})$ is such that $E(\mathbb{Z}_{pq}) \simeq E(\mathbb{Z}_p) \oplus E(\mathbb{Z}_q)$, the order of the group $E(\mathbb{Z}_{pq})$ is given as $\#E(\mathbb{Z}_N) = \#E(\mathbb{Z}_p) \cdot \#E(\mathbb{Z}_q) = (p + 1)(q + 1)$.

In the KMOV system the receiver chooses primes p, q with $p \equiv q \equiv 2 \pmod{3}$ takes $N = pq$ and chooses e such that $1 \leq e \leq (p + 1)(q + 1)$ with $\gcd(e, (p + 1)(q + 1)) = 1$ and makes (N, e) public. The sender represents the message $M = (m_1, m_2)$ as a point on elliptic curve $E_b : y^2 = x^3 + b$, for $b = m_2^2 - m_1^3 \pmod{N}$. The message is encrypted as $C = eM$ and

the cipher text C is sent to the receiver. The receiver for decryption uses the decryption exponent d such that $1 \leq d \leq (p+1)(q+1)$ with $ed \equiv 1 \pmod{(p+1)(q+1)}$ and obtains the message as $dC = deM = M \pmod{N}$. The computations are carried using the Group laws on elliptic curves[\[46\]](#)[\[14\]](#).

Bibliography

- [1] Tom M. Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag, New York Inc.
- [2] A. K. Bhandari, D. S. Naraj, B. Ramakrishnan and T. N. Venkataramana, *Elliptic Curves, Modular Forms and Cryptography*, New Delhi, 2003, Hindustan Book Agency, India, 2003.
- [3] J. Blömer, A. May, “*Low Secret Exponent RSA Revisited*”, Cryptography and Lattice Conference (CaLC 2001), Lecture Notes in Computer Science Volume 2146, Springer-Verlag, pp. 4-19, 2001.
- [4] D. Boneh, “*Twenty Years of Attacks on the RSA Cryptosystem*”, Notices Amer. Math. Soc., 46:203-213, 1999.
- [5] D. Boneh, G. Durfee, “*Cryptanalysis of RSA with private key d less than $N^{0.292}$* ”, IEEE Transactions on Information Theory, IT-46:1339-1349, 2000.
- [6] J. Buchmann, “*Introduction to cryptography*”, Springer-Verlag, 2001.
- [7] D. Burton, *Elementary Number Theory*, Sixth ed, Mc Graw Hill, New York, 2007.
- [8] D. Coppersmith, “*Small solutions to polynomial equations, and low exponent RSA vulnerabilities*”, Journal of Cryptology, 10(4), pp. 233-260, 1997.

- [9] Abhijit Das, “*Computational Number Theory*”, CRC Press, ISBN 9781439866153, Series: Discrete Mathematics and Its Applications, Editor : Kenneth H. Rosen.
- [10] H. Davenport, “*The Higher Arithmetic. An Introduction to the Theory of Numbers*”, Eighth edition, Cambridge University Press, 1952, ISBN-13978-1-107-68854-4.
- [11] W. Diffie and M. E. Hellman, “*New directions in cryptography*”, IEEE Transactions on Information Theory, 22(6), 644-654, 1976.
- [12] N. Howgrave-Graham, “*Finding small roots of univariate modular equations revisited*”, In Cryptography and Coding, LNCS 1355, pp. 131-142, Springer-Verlag (1997).
- [13] G. H. Hardy, E. M. Wright, D. R. Heath-Brown and J. H. Silverman, “*An Introduction to the Theory of Numbers*”, Oxford University Press, 1965.
- [14] Jeffery Hoftstein, Jill Pipher, Joseph H. Silverman, “*An Introduction to Mathematical Cryptography*”, Springer Science & Business Media, (2008):, Germany.
- [15] L. k. Hua, “*Introduction to Number Theory*”, Springer-Verlag, New York, 1982.
- [16] Kenneth Ireland and Michael Rosen, *A Classical Introduction to Modern Number Theory*, 1972, Spring Science+Business Media LLC, ISBN 978-1-4757-17815.
- [17] E. Jochemsz, *Cryptanalysis of RSA variants using small roots of polynomials*. Ph.D. Thesis, Technische Universiteit Eindhoven (2007).
- [18] E. Jochemsz, A. May, “*A strategy for finding roots of multivariate polynomials with new applications in attacking RSA variants*”, in: ASIACRYPT 2006, LNCS, vol. 4284, 2006, pp. 267-282, Springer-Verlag.
- [19] P. Anuradha Kameswari and L. Jyotsna, “*Cryptanalysis of RSA with small multiplicative inverse of $p - 1$ or $q - 1$ modulo e* ”.

- [20] P A Kameswari, L Jyotsna, “*Extending Wiener’s Extension to RSA-Like Cryptosystems over Elliptic Curves*”, British Journal of Mathematics & Computer Science 14 (1), 1-8, Jan 2016, SCIENCEDOMAIN International.
- [21] P. Anuradha Kameswari, L. Jyotsna, *Wiener’s Attack and its Extensions on RSA Cryptosystem*, M.Phil dissertation, Department of Mathematics, Andhra University 2012.
- [22] P. Anuradha Kameswari, L. Praveen Kumar, *Implementation of GCD attack with Projective Coordinates on Demytko’s Cryptosystem*, International Journal Of Computer Applications, ISSN : 0975-8887 volume 124 - No.6, pp.33-40, August 2015.
- [23] P. Anuradha Kameswari, L. Praveen Kumar, *Implementation Of Signature Scheme With Projective Coordinates On Elliptic Curve Cryptosystem*, International Research Journal Of Mathematics, Engineering and IT, ISSN : 2349-0322 volume 2, Issue - 7, (July 2015), pp.1-15.
- [24] Aaron H. Kaufer, “*Applications of Continued Fractions in Cryptography and Diophantine Equations*”, M.Sc. thesis, School of Mathematical Sciences, Rochester Institute of Technology, 2009.
- [25] Donald E. Knuth, *The Art of Computer Programming*, Volume 2: Seminumerical Algorithms (3rd Edition), 1997, Addison-Wesley Professional, ISBN 0-201-89684-2.
- [26] Neal Koblitz, “*A course in number theory and cryptography*”, Springer-Verlag, New York, 1994, ISBN 3-578071-8, SPIN 10893308.
- [27] Neal Koblitz, “*Elliptic curves Cryptosystems*”. Mathematics of Computation , 48: 203-209,1987.
- [28] Thomas Koshy, *Elementary Number Theory with Applications*, 2nd Edition, Elsevier Inc ,USA, 2007.

- [29] A.K. Lenstra, H.W. Lenstra, L. Lovász, “*Factoring polynomials with rational coefficients*”, *Mathematische Annalen*, Vol. 261, pp. 513-534, 1982.
- [30] Subhamoy Maitra and Santanu Sarkar, “*Reviving Wiener’s Attack - New Weak Keys in RSA*”, ISC 2008, pp.228-243.
- [31] Subhamoy Maitra and Santanu Sarkar, “*RSA Cryptanalysis with Increased Bounds on the Secret Exponent using Less Lattice Dimension*”, *Cryptology ePrint Archive: Report 2008/315*.
- [32] A. May, : “*New RSA Vulnerabilities Using Lattice Reduction Methods*”, PhD thesis, University of Paderborn (2003).
- [33] V.S. Miller, “*Use of Elliptic Curves in Cryptography*”. In H.C. Williams, editor *Advances in Cryptology-CRYPTO 85*, Volume 218 of *Lecture notes in Computer Science*, 417-426, Springer-Verlag, 1986.
- [34] A. Nitaj, : *Another generalization of Wiener’s attack on RSA*, In: Vaudenay, S. (ed.) *Africacrypt 2008*, LNCS, vol. 5023, pp. 174-190. Springer, Heidelberg (2008).
- [35] A. Nitaj, M.O. Douh, *A new attack on RSA with a composed decryption exponent*, *Int. J. Crypt. Inf. Secur. (IJCIS)* 3(4), 1121 (2013).
- [36] I. Niven, H. S. Zuckerman, and H.L. Montgomery, “*An Introduction to the Theory of Numbers*”, Fifth edition, John Wiley & Sons, New York, 1991.
- [37] R. G. E. Pinch. “*Extending The Wiener’s Attack to RSA-Type Cryptosystem*”. *Electronics Letters* 31 (1995), 1736-1738.
- [38] K. H. Rosen, “*Elementary Number Theory and Its Applications*”, Addison-Wesley, Reading Mass, 1984.

- [39] Victor Shoup, *A computational Introduction to Number Theory and Algebra*, 2005, cambridge university press, ISBN-13 978-0-521-85154-1.
- [40] William Stein, *Elementary Number Theory: Primes, Congruences and Secrets*, A Computational Approach, Undergraduate Texts in Mathematics, Springer, 2009.
- [41] Douglas R. Stinson, *Cryptography: Theory and Practice*, CRC Press, 1995.
- [42] H. -M. Sun, M. -E. Wu and Y. -H. Chen. “*Estimating the prime-factors of an RSA modulus and an extension of the Wiener attack*”. ACNS 2007, LNCS 4521, pp. 116128, 2007.
- [43] Jhon Talbot and Dominic Welsh, *Complexity and Cryptography: An Introduction*, Cambridge University Press, New York, 2006.
- [44] James. J.Tattersall, *Elementary Number Theory in Nine Chapters*, second Edition, cambridge university press, ISBN 978-1-107-67000-6.
- [45] R. Thangadurai, *Classical Cryptosystems*, Proceedings of the advanced instructional workshop on Algebraic number theory, HBA (2003) 287-301.
- [46] Lawrence C. Washington “*Elliptic Curves: Number Theory and Cryptography*” Chapman & Hall/CRC, 2003.
- [47] B. de Weger, “*Cryptanalysis of RSA with Small Prime Difference*”, Applicable Algebra in Engineering, Communication and Computing, 13(1);17-28,2002.
- [48] M. Wiener, “*Cryptanalysis of Short RSA Secret Exponents*”, IEEE Transactions on Information Theory, 36(3)-553-558, 1990.
- [49] Song Y. Yan, *Computational Number Theory and Modern Cryptography*, 1st edition, Wiley, 2013, ISBN:978-1-118-18858-3.

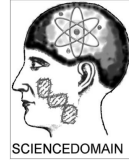
- [50] Song Y. Yan, *Number Theory for computing*, Springer Science & Business Media, 2002.

Enclosure-2

RESEARCH PUBLICATIONS

Research Papers Published/Accepted/Communicated

1. Dr. P. Anuradha Kameswari, L. Jyotsna “Extending Wiener’s Extension to RSA-Like Cryptosystems over Elliptic curves”, **British Journal of Mathematics & Computer Science** 14(1): 1-8, Jan 2016, Article no.BJMCS.23036 ISSN: 2231-0851, SCIENCEDOMAIN International.
2. P. Anuradha Kameswari, L. Jyotsna, “Cryptanalysis of RSA with small multiplicative Inverse of $(p - 1)$ or $(q - 1)$ modulo e ”, **Journal of Global Research in Mathematical Achieves (JGRMA)**, ISSN: 2320-5822, Volume 5, No. 5(May-2018), pp. 72-81.
3. P. Anuradha Kameswari, L. Jyotsna, “Cryptanalysis of RSA with Small Multiplicative Inverse of $\phi(N)$ Modulo e and with a Composed Prime Sum $p + q$ ”, **International Journal of Mathematics and its Applications**, ISSN: 2347-1557, Volume 6, No. 1(2018), Impact factor: 0.421, pp 515-526.
4. P. Anuradha Kameswari, L. Jyotsna, “An Attack Bound for Small Multiplicative Inverse of $\phi(N)$ modulo e with a Composed Prime Sum $p + q$ using Sub lattice Based Techniques”, accepted for publication in the Journal of **Cryptography**, ISSN 2410-387X



Extending Wiener's Extension to RSA-Like Cryptosystems over Elliptic Curves

P. Anuradha Kameswari^{1*} and L. Jyotsna¹

¹Department of Mathematics, Andhra University, Visakhapatnam - 530003, Andhra Pradesh, India.

Authors' contributions

This work was carried out in collaboration between both authors. Author PAK designed the study, wrote the protocol and wrote the first draft of the manuscript and managed literature searches. Author LJ managed the analyses of the study and literature searches. Both authors read and approved the final manuscript.

Article Information

DOI: 10.9734/BJMCS/2016/23036

Editor(s):

(1) Dariusz Jacek Jakbczak, Chair of Computer Science and Management in this Department, Technical University of Koszalin, Poland.

Reviewers:

(1) Anand Nayyar, KCL Institute of Management and Technology, India.

(2) S. K. Rososhek, Tomsk State University, Tomsk, Russia.

(3) Vipin Saxena, Babasaheb Bhimrao Ambedkar University, Lucknow, India.

(4) Anonymous, China University of Mining and Technology, China.

Complete Peer review History: <http://sciencedomain.org/review-history/13055>

Received: 11th November 2015

Accepted: 5th January 2016

Published: 23rd January 2016

Short Research Article

Abstract

The studies on Wiener's attack on RSA with small deciphering exponents led to the refinement of attack bounds on the deciphering exponent in the paper "Revisiting Wiener's Attack - New Weak Keys in RSA" by Subhamoy Maitra and Santanu Sarkar. Further in the paper "Extending The Wiener's Attack to RSA-Type Cryptosystem" by R. G. E. Pinch, it is proved that Wiener's attack on RSA Cryptosystem with small deciphering exponent may be extended to RSA-like Cryptosystems on elliptic curves. Now in this paper we show that the Wiener's extension on RSA that refines the attack bound on deciphering exponent can also be extended to RSA-like Cryptosystems on elliptic curves.

Keywords: RSA cryptosystem; elliptic curve.

2010 Mathematics Subject Classification: 94A60.

*Corresponding author: E-mail: panuradhakameswari@yahoo.in;

1 Introduction

RSA Cryptosystem [1] is the first public key Cryptosystem invented by Ronald Rivest, Adi Shamir and Leonard Adleman in 1977 where the encryption and decryption are based on the fact that if $N = pq$ is the modulus for RSA, p, q distinct primes, if $1 \leq e \leq \varphi(N)$ with $(e, \varphi(N)) = 1$ and d , the multiplicative inverse of e modulo $\varphi(N)$, then $m^{ed} = m \pmod N$, for any message m , an integer in Z_N . The security [2] of this system depends on the difficulty of finding factors of a composite positive integer, that is product of two large primes.

Wiener [3] showed that RSA Cryptosystem has a weakness if the private deciphering exponent $d < \frac{N^{\frac{1}{4}}}{\sqrt{2}}$. In [4], Boneh and Durfee showed that RSA is weak for $d < N^{0.292}$. In [5] Subhamoy Maitra and Santanu Sarkar shown that RSA is weak when $d = N^\delta$, $\delta < \frac{1}{2} - \frac{\gamma}{2}$, where $|\rho q - p| \leq \frac{N^\gamma}{16}$, $\gamma \leq \frac{1}{2}$ for $1 \leq \rho \leq 2$ and also for $d < \frac{1}{2}N^\delta$ along with a condition on exponent $e = O(N^{\frac{3}{2}-2\delta})$, $\delta \leq \frac{1}{2}$ and some extensions considering the difference $p - q$ are also given. In [6] R.G.E Pinch has shown that the Wiener's attack extends to RSA-like Cryptosystems over elliptic curves. In this paper we show that the Wiener's extension on RSA that refines the attack bound on deciphering exponent can also be extended to RSA-like Cryptosystems on elliptic curves. The study is based on developing certain estimates of Euler function $\varphi(N)$ and $\psi(N)$ an analogue to $\varphi(N)$.

2 Wiener's Attack on RSA Cryptosystem

The main idea of Wiener's attack [3] is that certain restrictions of d allow the fraction $\frac{t}{d}$ to be a convergent of $\frac{e}{N}$, where $t = \frac{ed-1}{\varphi(N)}$, this follows by using the approximation theorem.

Theorem 2.1. (Approximation Theorem): Let r be a real number, for any integer a and b with $\gcd(a, b) = 1$ such that $|r - \frac{a}{b}| < \frac{1}{2b^2}$, $b \geq 1$ then $\frac{a}{b}$ is convergent of r . [7]

Theorem 2.2. (Wiener's attack): Let $N = pq$, for $q < p < 2q$ be the modulus for RSA, e be the public enciphering exponent and d be the deciphering exponent. If $d \leq \frac{N^{\frac{1}{4}}}{\sqrt{6}}$, then $\frac{t}{d}$ is a convergent of $\frac{e}{N}$, for $t = \frac{ed-1}{\varphi(N)}$.

Theorem 2.3. (Implementation of Wiener's attack): Let $d \leq \frac{N^{\frac{1}{4}}}{\sqrt{6}}$ and for any convergent $\frac{t'}{d'}$ of $\frac{e}{N}$, take $\varphi'(N) = \frac{ed'-1}{t'}$, $x' = \frac{N-\varphi'(N)+1}{2}$ and $y' = \sqrt{x'^2 - N}$. If $x', y' \in \mathbb{N}$, then the private key $(q, p, d) = (x' - y', x' + y', d')$.

The idea of Wiener is that certain restrictions of d allow to obtain a convergent of $\frac{e}{N}$ that is useful in finding the factors p, q of N and the deciphering exponent d . In [5] Subhamoy Maitra and Santanu Sarkar proposed Wiener's extension on RSA cryptosystem improving the attack bound for the decryption exponent d . In the following section we recall the corresponding results for Wiener's extension [8].

3 Wiener's Extension on RSA

Wiener's extension on a RSA Cryptosystem, refining the attack bound is based on following theorem [9]. Wiener's extension is the idea of obtaining a convergent of $\frac{e}{N+1-2N^{\frac{1}{2}}}$ rather than that of $\frac{e}{N}$, which increases the bound of d , from $N^{\frac{1}{4}}$ to N^δ , for $\frac{1}{4} < \delta < \frac{3}{4} - \beta$. These ideas are based on developing certain estimates for $\varphi(N)$.

Theorem 3.1. Let $N = pq$ for $q < p < 2q$ be the modulus of RSA with the enciphering exponent e and the deciphering exponent d . For $\Delta = p - q = N^\beta$, if $d < N^{\frac{3}{4}-\beta}$, then $\frac{t}{d}$ is a convergent of $\frac{e}{N+1-2N^{\frac{1}{2}}}$.

Theorem 3.2. (Implementation of Wiener's Extension) Let $d < N^{\frac{3}{4}-\beta}$ for $p - q = N^\beta$ and for any convergent $\frac{t'}{d'}$ of $\frac{e}{N+1-2N^{\frac{1}{2}}}$, take $\varphi'(N) = \frac{ed'-1}{t'}$, $x' = \frac{N-\varphi'(N)+1}{2}$ and $y' = \sqrt{x'^2 - N}$. If $x', y' \in \mathbb{N}$, then the private key $(q, p, d) = (x' - y', x' + y', d')$.

Implementation of extension of Wiener's attack is the same as implementation of Wiener's attack on RSA Cryptosystem.

4 Extending Wiener's Extension to RSA-like Cryptosystems over Elliptic Curves

$E : y^2 = x^3 + Ax + B$ is the Weierstrass form of an Elliptic curve. For any finite field \mathbb{F}_q of characteristic p , $E(\mathbb{F}_q) = \{(x, y) \in \mathbb{F}_q \times \mathbb{F}_q; y^2 = x^3 + Ax + B\} \cup \{\infty\}$ is the elliptic curve over \mathbb{F}_q . In 1985 Koblitz [10] and Miller [11] independently proposed using the group of points on an elliptic curves over finite fields in discrete log cryptosystems, as there are no sub exponential time algorithms to find the discrete log on elliptic curves.

The elliptic curves considered by Koyama-Maurer-Okamoto-Vanstone [12][13] for KMOV system are the elliptic curves in the form

$$E_b(N) : y^2 = x^3 + b \pmod N \text{ for } N = pq, p, q \text{ primes with } p \equiv q \equiv 2 \pmod 3.$$

The curves $E_b(p) : y^2 = x^3 + b \pmod p$ and $E_b(q) : y^2 = x^3 + b \pmod q$ are super singular with orders $\#E_b(p) = p+1$ & $\#E_b(q) = q+1$. Further as the group $E(\mathbb{Z}_{pq})$ is such that $E(\mathbb{Z}_{pq}) \simeq E(\mathbb{Z}_p) \oplus E(\mathbb{Z}_q)$, the order of the group $E(\mathbb{Z}_{pq})$ is given as $\#E(\mathbb{Z}_N) = \#E(\mathbb{Z}_p) \cdot \#E(\mathbb{Z}_q) = (p+1)(q+1)$ [14].

In the KMOV system the receiver chooses primes p, q with $p \equiv q \equiv 2 \pmod 3$ takes $N = pq$ and chooses e such that $1 \leq e \leq (p+1)(q+1)$ with $\gcd(e, (p+1)(q+1)) = 1$ and makes (N, e) public. The sender represents the message $M = (m_1, m_2)$ as a point on elliptic curve $E_b : y^2 = x^3 + b$, for $b = m_2^2 - m_1^3 \pmod N$. The message is encrypted as $C = eM$ and the cipher text C is sent to the receiver. The receiver for decryption uses the decryption exponent d such that $1 \leq d \leq (p+1)(q+1)$ with $ed \equiv 1 \pmod (p+1)(q+1)$ and obtains the message as $dC = deM = M \pmod N$. The computations are carried using the Group laws on elliptic curves [12][15][16][17].

Pinch in his paper [6] showed that Wiener's attack applies to KMOV as well. In [5] Subhamoy Maitra and Santanu Sarkar proposed Wiener's extension on RSA cryptosystem improving the attack bound for the decryption exponent d . In this paper we show that Wiener's extension also applies to the above RSA like cryptosystems over elliptic curves(KMOV). This is done by looking at $\psi(N) := (p+1)(q+1)$ as an analogue of Euler's function $\varphi(N)$. In the above RSA like cryptosystems over the specific elliptic curves $E_b : y^2 = x^3 + b \pmod N$, Wiener's extension is extended by developing certain estimates on $\psi(N)$, we prove the results regarding the estimates for $\psi(N)$ in the following.

Lemma 4.1. If $q < p < 2q$ and $\psi(N) = (p+1)(q+1)$ then $N+1+2N^{\frac{1}{2}} < \psi(N) < N+1+\frac{3}{\sqrt{2}}N^{\frac{1}{2}}$.

Proof.

$$\begin{aligned} \text{We have } \psi(N) &= (p+1)(q+1) \\ &= N+1+pq \\ &> N+1+2N^{\frac{1}{2}} \text{ as } p+q > 2N^{\frac{1}{2}} \dots (1) \end{aligned}$$

Also We have $\left(p + q + \frac{3}{\sqrt{2}}N^{\frac{1}{2}}\right) \left(p + q - \frac{3}{\sqrt{2}}N^{\frac{1}{2}}\right) < 0$ for $q < p < 2q$.

Then $\left(p + q - \frac{3}{\sqrt{2}}N^{\frac{1}{2}}\right)$ should be less than 0.

Therefore $\psi(N) = N + 1 + p + q < \left(N + 1 + \frac{3}{\sqrt{2}}N^{\frac{1}{2}}\right)$ as $\left(p + q - \frac{3}{\sqrt{2}}N^{\frac{1}{2}}\right) < 0 \dots (2)$.

From (1) and (2) $N + 1 + 2N^{\frac{1}{2}} < \psi(N) < N + 1 + \frac{3}{\sqrt{2}}N^{\frac{1}{2}}$. □

Theorem 4.2. (Wiener's Extension on RSA over $E(\mathbb{Z}_N)$) Let $N = pq$ for $q < p < 2q$ with the enciphering exponent e and deciphering exponents d such that $\frac{ed-1}{t} = \psi(N)$. If $\Delta = p - q = N^\beta, d < N^{\frac{3}{4}-\beta}$, then $\frac{t}{d}$ is a convergent of $\frac{e}{N+1+2N^{\frac{1}{2}}}$.

Proof. We have

$$\begin{aligned} \left| \frac{e}{N+1+2N^{\frac{1}{2}}} - \frac{t}{d} \right| &= \left| \frac{e}{N+1+2N^{\frac{1}{2}}} + \frac{e}{\psi(N)} - \frac{e}{\psi(N)} - \frac{t}{d} \right| \\ &\leq \left| \frac{e}{N+1+2N^{\frac{1}{2}}} - \frac{e}{\psi(N)} \right| + \left| \frac{e}{\psi(N)} - \frac{t}{d} \right| \\ &= e \left| \frac{1}{N+1+2N^{\frac{1}{2}}} - \frac{1}{\psi(N)} \right| + \frac{1}{\psi(N)d}, \text{ as } e > 0 \text{ and } ed - 1 = \psi(N)t. \\ &< \psi(N) \left| \frac{\psi(N) - (N+1+2N^{\frac{1}{2}})}{(N+1+2N^{\frac{1}{2}})\psi(N)} \right| + \frac{1}{\psi(N)d}, \text{ as } e < \psi(N). \\ &= \psi(N) \left| \frac{N+1+p+q-N-1-2N^{\frac{1}{2}}}{\psi(N)(N+1+2N^{\frac{1}{2}})} \right| + \frac{1}{\psi(N)d} \\ &= \frac{p+q-2N^{\frac{1}{2}}}{N+1+2N^{\frac{1}{2}}} + \frac{1}{\psi(N)d} \text{ as } p+q-2N^{\frac{1}{2}} > 0. \\ &< \frac{\Delta^2}{4N^{\frac{1}{2}}} \left(\frac{1}{N+1+2N^{\frac{1}{2}}} \right) + \frac{1}{\psi(N)d}, \\ &\qquad \text{as } p+q-2N^{\frac{1}{2}} = \frac{\Delta^2}{p+q+2N^{\frac{1}{2}}}. \\ &< \frac{\Delta^2}{4N^{\frac{1}{2}}} \left(\frac{1}{\varphi(N)} \right) + \frac{1}{\varphi(N)d}, \\ &\qquad \text{as } N+1+2N^{\frac{1}{2}} > \varphi(N) \text{ and } \psi(N) > \varphi(N). \end{aligned}$$

Therefore $\left| \frac{e}{N+1+2N^{\frac{1}{2}}} - \frac{t}{d} \right| < \frac{1}{\varphi(N)} \left(\frac{\Delta^2}{4N^{\frac{1}{2}}} + \frac{1}{d} \right) \dots (1)$

Now note $\psi(N) > \frac{3}{4}N$, since $p+q < \frac{1}{4} + 1$ for all $N^{\frac{1}{2}} > 9$ by assuming N is large.

Also note $8d < N$ for all $N^{\frac{1}{4}} > 8$, since $d < N^{\frac{3}{4}}$.

Therefore, for $\Delta = N^\beta$ and $d = N^\delta$ and substitute $\varphi(N) > \frac{3}{4}N$ and $N > 8d$ in (1), we get

$$\begin{aligned} \left| \frac{e}{N+1+2N^{\frac{1}{2}}} - \frac{t}{d} \right| &< \frac{1}{3}N^{2\beta-\frac{3}{2}} + \frac{4}{3Nd} \\ &< \frac{1}{3}N^{2\beta-\frac{3}{2}} + \frac{1}{6N^{2\delta}} \end{aligned}$$

and as $2\beta - \frac{3}{2} < -2\beta$ for all $\delta < \frac{3}{4} - \beta$, we have

$$\left| \frac{e}{N+1+2N^{\frac{1}{2}}} - \frac{t}{d} \right| < \frac{1}{2d^2}.$$

Therefore $\frac{t}{d}$ is a convergent of $\frac{e}{N+1+2N^{\frac{1}{2}}}$ for $d < N^{\frac{3}{4}-\beta}$. □

Now using the above estimates for $\psi(N)$ we prove the following theorem of implementation of Wiener's extension.

Theorem 4.3. (Implementation of Wiener's extension): Let $d < N^{\frac{3}{4}-\beta}$ for $p - q = N^\beta$ and for any convergent $\frac{t'}{d'}$ of $\frac{e}{N+1+2N^{\frac{1}{2}}}$, take $\psi'(N) = \frac{ed'-1}{t'}$, $x' = \frac{\psi'(N)-N-1}{2}$ and $y' = \sqrt{(x')^2 - N}$. If $x', y' \in \mathbb{N}$, then $\psi'(N) = \psi(N)$ and the private key is $(p, q, d) = (x' + y', x' - y', d')$.

Proof. For $y' = \sqrt{(x')^2 - N}$, $N = (x' + y') \cdot (x' - y')$.

If $x', y' \in \mathbb{N}$, then the possible cases are

- (i) $(x' - y') = 1$ and $(x' + y') = N$
- (ii) $(x' - y') = q$ and $(x' + y') = p$, as $N = pq$ and $q < p$.

For $(x' - y') = 1$ and $(x' + y') = N$, we have $\frac{N+1}{2} = x'$.

Then $\psi'(N) - N - 1 = 2x' = N + 1$.

Thus $2(N+1) = \psi'(N)$.

$$= \frac{ed' - 1}{t'}$$

$$< N + 2 + \frac{3}{\sqrt{2}}N^{\frac{1}{2}}, \text{ as } \frac{e}{N+2+\frac{3}{\sqrt{2}}N^{\frac{1}{2}}} < \frac{t'}{d'}, \text{ for some } t', d'$$

$$\text{and } \psi(N) < N + 1 + \frac{3}{\sqrt{2}}N^{\frac{1}{2}}.$$

$$\text{Therefore } N^{\frac{1}{2}} < \frac{3}{\sqrt{2}}.$$

Which is a contradiction, as we are choosing a large 'N.'

Hence case(i) is not possible.

Therefore, the only possible case is $q = x' - y', p = x' + y'$.

$$\text{By defining of } x', \text{ we have } x' = \frac{\psi'(N) - N - 1}{2}$$

$$\begin{aligned} \text{Then } \psi'(N) &= 2x' + N + 1 \\ &= p + q + N + 1 \\ &= \psi(N) \end{aligned}$$

Now as $ed' = 1 \pmod{\psi'(N)}$ and $\psi'(N) = \psi(N)$, $d = d'$.

Therefore, for $\psi'(N)$, $x', y' \in \mathbb{N}$, the private key $(p, q, d) = (x' + y', x' - y', d')$. □

The following example demonstrates the working of KMOV cryptosystem.

Example 4.4. The receiver chooses primes $p = 5, q = 11$ takes $N = pq = 55$. Then he chooses $e = 5$ and makes (N, e) public.

The sender chooses a message $M = (2, 3)$, a point on the elliptic curve $E_b : y^2 = x^3 + 1 \pmod{55}$ and enciphers the message as $C = eM \pmod{N}$ and sends the cipher text C to the receiver. The computations are done by using the group laws on elliptic curves and the algorithms like doubling and adding algorithm [15] may be used for computations

$$\begin{aligned} C &= 5M = 5(2, 3) = (1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0)(2, 3) \\ &= (2(2(2, 3)) + (2, 3)) \\ &= (2, 52) \pmod{55}. \end{aligned}$$

For decryption the receiver computes $29C \pmod{55}$ as follows

$$\begin{aligned} 29C &= (1 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0)C \\ &= 2(2(2(2(2, 52)))) + 2(2(2(2, 52))) + 2(2(2, 52)) + (2, 52) \pmod{55} \\ &= (2, 3) \pmod{55} \\ &= M \pmod{55}, \text{ the required message.} \end{aligned}$$

Example 4.5. (Implementation of Wiener's extension)

Let $(N, e) = (10610503, 8916809)$ be the public key.

The continued fraction of

$$\begin{aligned} \frac{e}{N + 1 + 2N^{\frac{1}{2}}} &= \frac{8916809}{10610503 + 1 + 2 \cdot (10610503)^{\frac{1}{2}}} \\ &\sim 0.83985 \\ &= [0; 1, 5, 4, 11, 5, 2, 1, 1, 1 \dots] \end{aligned}$$

The first five convergents of the above continued fractions are

$$\frac{0}{1}, \frac{1}{1}, \frac{5}{6}, \frac{21}{25}, \frac{236}{281}, \dots [18][19].$$

The required convergent is $\frac{236}{281}$ as $\psi'(N) = 10617048, x' = 3272, y' = 309$ are such that $\psi'(N), x', y' \in \mathbb{N}$.

Therefore the private key $(p, q, d) = (x' + y', x' - y', d') = (3581, 2963, 281)$.

5 Conclusion

The idea of Wiener is that certain restrictions of d allow to obtain a convergent of $\frac{e}{N}$ that is useful in finding the factors p, q of N and the deciphering exponent d . Further Wiener's extension is the idea of obtaining a convergent of $\frac{e}{N+1-2N^{\frac{1}{2}}}$ rather than that of $\frac{e}{N}$, which increases the bound of d , from $N^{\frac{1}{4}}$ to N^δ , for $\frac{1}{4} < \delta < \frac{3}{4} - \beta$. These ideas are based on developing certain estimates for $\varphi(N)$; Looking at $\psi(N) = (p+1)(q+1)$ as the analogue of Euler's function $\varphi(N)$ in the RSA like cryptosystems over the specific elliptic curves $E_b : y^2 = x^3 + b \pmod{N}$, Wiener's extension is extended by developing certain estimates on $\psi(N)$.

Competing Interests

The authors declare that no competing interests exist.

References

- [1] Neal Koblitz. A course in number theory and cryptography. ISBN 3-578071-8, SPIN 10893308.
- [2] Boneh D. Twenty years of attacks on the RSA cryptosystem. Available: <http://www.ams.org/notices/199902/boneh.pdf>
- [3] Wiener M. Cryptanalysis of short RSA secret exponents. *IEEE Transactions on Information Theory*. 1990;36(3):553-558.
- [4] Boneh D, Durfee G. Cryptanalysis of RSA with private key d less than $N^{0.292}$. *IEEE Trans. on Information Theory*. 2000;46(4):1339-1349.
- [5] Subhamoy Maitra, Santanu Sarkar. Revisiting Wiener's attack - New Weak Keys in RSA. Available: <http://eprint.iacr.org/2005/228.pdf>
- [6] Pinch RGE. Extending the Wiener's attack to RSA-Type cryptosystem. *Electronics Letters*. 1995;31:1736-1738.
- [7] Rosen KH. Elementary number theory and its applications. Addison-Wesley, Reading Mass; 1984.
- [8] Anuradha Kameswari P, Jyotsna L. Wiener's attack and its extensions on RSA cryptosystem. M.Phil dissertation, Department of Mathematics, Andhra University; 2012.
- [9] de Weger B. Cryptanalysis of RSA with small prime difference. *Applicable Algebra in Engineering, Communication and Computing*. 2002;13(1):17-28.
- [10] Neal Koblitz. Elliptic curves cryptosystems. *Mathematics of Computation*. 1987;48:203-209.
- [11] Miller VS. Use of elliptic curves in cryptography. In H.C. Williams, editor *Advances in Cryptology-CRYPTO 85*, Volume 218 of *Lecture notes in Computer Science*. Springer-Verlag. 1986;417-426.
- [12] Lawrence C Washington. *Elliptic curves number theory and cryptography*. Second edition, Chapman & Hall/CRC; 2008.
- [13] Song Y. Yan. *Number theory for computing*, 2nd edition. Springer, ISBN:3-540-43072-5.
- [14] Anuradha Kameswari P, Praveen Kumar L. Encryption on elliptic curves over Z_{pq} with arithmetic on $E(Z_{pq})$ via $E(Z_p)$ and $E(Z_q)$. (*International Organization of Scientific Research*) *IOSR Journal of Mathematics*, e- ISSN: 2278-5728. 2014;10(6).
- [15] Jeffery Hoftstein, Jill Pipher, Joseph H. Silverman. *An Introduction to Mathematical Cryptography*. Springer, ISBN:978-0-387-77993-5.
- [16] Anuradha Kameswari P, Praveen Kumar L. Implementation of GCD attack with Projective Coordinates on Demytko's Cryptosystem. *International Journal of Computer Applications*. 2015;124(6):33-40. ISSN: 0975-8887.
- [17] Anuradha Kameswari P, Praveen Kumar L. Implementation of signature scheme with projective coordinates on elliptic curve cryptosystem. *International Research Journal of Mathematics, Engineering and IT*. 2015;2(7):1-15. ISSN: 2349-0322.
- [18] Burton D. *Elementary number theory*, Sixth edition. Mc Graw Hill, New York; 2007.

- [19] Devenport H. The higher arithmetic, Eight edition. Cambridge University Press, ISBN-13 978-1-107-68854-4.

©2016 Kameswari and Jyotsna; This is an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Peer-review history:

The peer review history for this paper can be accessed here (Please copy paste the total link in your browser address bar)

<http://sciencedomain.org/review-history/13055>

Cryptanalysis of RSA with Small Multiplicative Inverse of $\varphi(N)$ Modulo e and with a Composed Prime Sum $p + q$ ^{*}

P. Anuradha Kameswari^{1,*} and L. Jyotsna¹

¹ Department of Mathematics, Andhra University, Visakhapatnam, Andhra Pradesh, India.

Abstract: In this paper, we mount an attack on RSA when $\varphi(N)$ has small multiplicative inverse k modulo e , the public encryption exponent. For $k \leq N^\delta$, the attack bounds for δ are described by using lattice based techniques. The bound for δ depends on the prime difference $p - q = N^\beta$ and the maximum bound for δ is $\alpha - \sqrt{\frac{\alpha}{2}}$ for $e = N^\alpha$ and for $\beta \approx 0.5$. If the prime sum $p + q$ is of the form $p + q = 2^n k_0 + k_1$ where n is a given positive integer and k_0 and k_1 are two suitably small unknown integers then the maximum bound for δ can be improved for $\beta \approx 0.5$.

MSC: 11T71, 94A60.

Keywords: RSA, Cryptanalysis, Lattices, LLL algorithm, Coppersmith's method.

© JS Publication.

1. Introduction

RSA Cryptosystem is the first public key cryptosystem invented by Ronald Rivest, Adi Shamir and Leonard Adelman in 1977 where the encryption and decryption are based on the fact that if $N = pq$, is the modulus for RSA, p, q distinct primes, if $1 \leq e \leq \varphi(N)$ with $(e, \varphi(N)) = 1$ and d , the multiplicative inverse of e modulo $\varphi(N)$, then $m^{ed} = m \pmod{N}$, for any message m , an integer in Z_N . The security of this system depends on the difficulty of finding factors of a composite positive integer, that is product of two large primes. In 1990, M.J.Wiener [20] was the first one to describe a cryptanalytic attack on the use of short RSA deciphering exponent d . This attack is based on continued fraction algorithm which finds the fraction $\frac{t}{d}$, where $t = \frac{ed-1}{\varphi(n)}$ in a polynomial time when d is less than $N^{0.25}$ for $N = pq$ and $q < p < 2q$. Using lattice reduction approach based on the Coppersmith techniques [6] for finding small solutions of modular bivariate integer polynomial equations, D. Boneh and G. Durfee [3] improved the wiener result from $N^{0.25}$ to $N^{0.292}$ in 2000 and J. Blömer and A. May [4] has given an RSA attack for d less than $N^{0.29}$ in 2001, that requires lattices of dimension smaller than the approach by Boneh and Durfee. In 2006, E. Jochemsz and A. May [10], described a strategy for finding small modular and integer roots of multivariate polynomial using lattice-based Coppersmith techniques and by implementing this strategy they gave a new attack on an RSA variant called common prime RSA.

In our paper [8], we described an attack on RSA by using lattice based techniques implemented in the case when $p - 1$ or $q - 1$ have small multiplicative inverse less than or equal to N^δ modulo the public encryption exponent e , for some small δ and for $q < p < 2q$, $e = N^\alpha > p - 1$. For r and s are the multiplicative inverses of $p - 1$ and $q - 1$ modulo e respectively,

* E-mail: panuradhakameswari@yahoo.in

* Both authors thank the University Grants Commission(UGC) for the support of the UGC grant under UGC-MRP scheme.

and for N^δ is an upper bound of $\min\{r, s\}$ and N^γ is an upper bound of $\begin{cases} p - \lceil\sqrt{N}\rceil & \text{if } \min\{r, s\} = r \\ q - \lceil\sqrt{N}\rceil & \text{if } \min\{r, s\} = s, \end{cases}$, we shown that

RSA will be insecure for $\delta < \frac{3\alpha + \gamma - 2\sqrt{\gamma(3\alpha + \gamma)}}{3}$ when both x and y shifts are used and for $\delta < \frac{\alpha - \gamma}{2}$ when only x -shifts are used. Later we improved the bound for δ up to $\alpha - \sqrt{\alpha\gamma}$ by implementing the sublattice based techniques given by Boneh and Durfee in [3] under the condition $\delta > \alpha - \gamma(1 + \alpha)$ and improved the bound for δ up to $\delta < \frac{2\alpha - 6\gamma + 2\sqrt{\alpha^2 - \alpha\gamma + 4\gamma^2}}{5}$ by implementing the sublattice based techniques with lower dimension given by J. Blömer and A. May in [4], this bound is slightly less then the above bound but this method requires lattices of smaller dimension than the above method.

For r and s the multiplicative inverses of $p - 1$ and $q - 1$ modulo e respectively, we have $k = rs \pmod e$, the multiplicative inverse of $\varphi(N)$ modulo e . In this paper it is shown that if k is small, that is the multiplicative inverse of $\varphi(N)$ modulo e is small, then RSA will be insecure for $q < p < 2q$ and $e = N^\alpha > p + q$, the prime sum. This case may be considered when both $(p - 1) \pmod e$ and $(q - 1) \pmod e$ do not have small inverses but $\varphi(N) \pmod e$ has small inverse as in Table 1. Let $f(x, y) = x(y + A) - 1$ where $A = N + 1 - \lceil 2\sqrt{N} \rceil$, then $(k, \lceil 2\sqrt{N} \rceil - (p + q))$ is a solution for the modular bivariate integer polynomial equation $f(x, y) \equiv 0 \pmod e$ and note $N^\beta = p - q$, the prime difference is an upper bound for $\lceil 2\sqrt{N} \rceil - (p + q)$. For $k \leq N^\delta$, the attack bounds for δ are described by implementing all lattice based techniques as given in [8], based on the theory of finding small bivariate modular integer polynomial equations to the above modular polynomial equation. For $\beta \approx 0.5$, the maximum bound for δ in which RSA will be insecure is such that $\alpha - \sqrt{\frac{\alpha}{2}}$ and this bound can be improved when the prime sum $p + q$ is of the form $p + q = 2^n k_0 + k_1$ for known positive integer n and for unknown suitably small integers k_0, k_1 by using the strategy given by E. Jochemsz and A. May as in [10] for finding small modular roots of multivariate polynomials.

2. Preliminaries

In this section we state basic results on lattices, described briefly lattice basis reduction, Coppersmith’s method and Howgrave-Graham theorem that are based on lattice reduction techniques are described.

Let $u_1, u_2, \dots, u_n \in \mathbb{Z}^m$ be linearly independent vectors with $n \leq m$. Let $\det(\mathcal{L})$ be a lattice spanned by $\langle u_1, u_2, \dots, u_n \rangle$. Let $b_1^*, b_2^*, \dots, b_n^*$ be the vectors obtained by applying the Gram-Schmidt process to the vectors u_1, u_2, \dots, u_n . The determinant of the lattice L is defined as $\det(L) := \prod_{i=1}^n \|b_i^*\|$, where $\|\cdot\|$ denotes the Euclidean norm on vectors. The lattice L is called full rank if $n = m$ and when $n = m$, the determinant of L is equal to the determinant of the $n \times n$ matrix whose rows are the basis vectors u_1, u_2, \dots, u_n .

In 1982, A. K. Lenstra, H. W. Lenstra, Jr. and L. Lovasz [11] invented the LLL lattice based reduction algorithm to reduce a basis and to solve the shortest vector problem in polynomial time. The general result on the size of individual LLL-reduced basis vectors is given in the following and a proof of that result can be found in [12].

Theorem 2.1. *Let L be a lattice of dimension ω . In polynomial time, the LLL-algorithm outputs reduced basis vectors v_i , $1 \leq i \leq \omega$ that satisfy*

$$\|v_1\| \leq \|v_2\| \leq \dots \leq \|v_i\| \leq 2^{\frac{\omega(\omega-1)}{4(\omega+1-i)}} \det(\mathcal{L})^{\frac{1}{\omega+1-i}}.$$

An important application of lattice reduction found by Coppersmith in 1996 [6] is finding small roots of low-degree polynomial equations. This includes modular univariate polynomial equations and bivariate integer equations. In 1997 Howgrave-Graham [7] reformulated Coppersmith’s techniques and proposed a result which shows that if the coefficients of $h(x, y)$ are sufficiently small, then the equality $h(x_0, y_0) = 0$ holds not only modulo N , but also over integers. The generalization of Howgrave-Graham result in terms of the Euclidean norm of a polynomial $h(x_1, x_2, \dots, x_n) = \sum a_{i_1 \dots i_n} x_1^{i_1} \dots x_n^{i_n}$ is defined by

the Euclidean norm of its coefficient vector i.e., $\|h(x_1, x_2, \dots, x_n)\| = \sqrt{\sum a_{i_1 \dots i_n}^2}$ given as follows:

Theorem 2.2 (Howgrave-Graham). *Let $h(x_1, x_2, \dots, x_n) \in \mathbb{Z}[x_1, x_2, \dots, x_n]$ be an integer polynomial that consists of at most ω monomials. Suppose that*

- (1). $h(x_1^{(0)}, x_2^{(0)}, \dots, x_n^{(0)}) \equiv 0 \pmod{e^m}$ for some m where $|x_1^{(0)}| < X_1, |x_2^{(0)}| < X_2 \dots |x_n^{(0)}| < X_n$, and
- (2). $\|h(x_1 X_1, x_2 X_2, \dots, x_n X_n)\| < \frac{e^m}{\sqrt{\omega}}$.

Then $h(x_1, x_2, \dots, x_n) = 0$ holds over the integers.

Resultant of two polynomials: The resultant of two polynomials $f(x_1, x_2, \dots, x_n)$ and $g(x_1, x_2, \dots, x_n)$ with respect to the variable x_i for some $1 \leq i \leq n$, is defined as the determinant of Sylvester matrix of $f(x_1, x_2, \dots, x_n)$ and $g(x_1, x_2, \dots, x_n)$ when considered as polynomials in the single indeterminate x_i , for some $1 \leq i \leq n$.

Remark 2.3. *The resultant of two polynomials is non-zero if and only if the polynomials are algebraically independent .*

Remark 2.4. *If $(x_1^{(0)}, x_2^{(0)}, \dots, x_n^{(0)})$ is a common solution of algebraically independent polynomials f_1, f_2, \dots, f_m for $m \geq n$, then these polynomials yield g_1, g_2, \dots, g_{n-1} resultants in $n-1$ variables and continuing so on the resultants yield a polynomial $t(x_i)$ in one variable with $x_i = x_i^{(0)}$ for some i is a solution of $t(x_i)$. Note the polynomials considered to compute resultants are always assumed to be algebraically independent.*

3. Attack Bounds for RSA using Lattice Based Techniques based on finding Small Modular Roots of Bivariate Polynomials

In our paper [8], we described an attack on RSA by using lattice based techniques implemented in the case when $p-1$ or $q-1$ have small multiplicative inverse less than or equal to N^δ modulo the public encryption exponent e , for some small δ and for $q < p < 2q$, $e = N^\alpha > p-1$.

Let $f(x, y) = x(y + A) - 1$ where $A = \lceil \sqrt{N} \rceil - 1$ and r, s be the multiplicative inverses of $p-1, q-1$ modulo the private encryption exponent e respectively. For $x_0 = \min\{r, s\}$ and $y_0 = \begin{cases} p - \lceil \sqrt{N} \rceil & \text{if } \min\{r, s\} = r \\ q - \lceil \sqrt{N} \rceil & \text{if } \min\{r, s\} = s, \end{cases}$ the pair (x_0, y_0) is a solution for the modular polynomial equation $f(x, y) \equiv 0 \pmod{e}$. For $|x_0| \leq N^\delta, |y_0| \leq N^\gamma$, the attack bounds for δ are described in [8] by using lattice reduction techniques in the direction of Boneh-Durfee [3] and Blömer-May [4] for $q < p < 2q$ and $e = N^\alpha > p-1$.

Applying the analysis described by Boneh-Durfee in [3] using x, y shifts and using only x shifts to the above modular polynomial equation, we get the attack bounds for δ as given in the following Theorem and Corollary [8] respectively.

Theorem 3.1. *Let $N = pq$ be an RSA modulus with $q < p < 2q$. Let $e = N^\alpha, X = N^\delta, Y = N^\gamma$ and r, s are the multiplicative inverses of $p-1, q-1$ modulo e respectively. Suppose that $|x_0| \leq X$ and $|y_0| \leq Y$ then one can factor N in polynomial time if*

$$\delta < \frac{3\alpha + \gamma - 2\sqrt{\gamma(3\alpha + \gamma)}}{3}.$$

Corollary 3.2. *If the lattice basis reduction algorithm is implemented only using x -shifts and repeating the above argument then we can factorize N whenever*

$$\delta < \frac{\alpha - \gamma}{2}.$$

In [8] further, the bound given in the above theorem is improved by implementing the ideas given by Boneh-Durfee [3] and Blömer-May [4] to the above modular equation using sublattice based techniques as given in the following Theorems.

Theorem 3.3. *Let $N, p, q, e, X, Y, x_0, y_0, \delta$ and γ be defined in Theorem 3. Suppose that $|x_0| \leq X$ and $|y_0| \leq Y$, then RSA is insecure if*

$$\alpha - \gamma(1 + \alpha) < \delta < \alpha - \sqrt{\alpha\gamma}.$$

Theorem 3.4. *Let $N, p, q, e, X, Y, x_0, y_0, \delta$ and γ be defined in Theorem 3. Suppose that $|x_0| \leq X$ and $|y_0| \leq Y$, then RSA is insecure if*

$$\delta < \frac{2\alpha - 6\gamma + 2\sqrt{\alpha^2 - \alpha\gamma + 4\gamma^2}}{5}.$$

The bound given in the Theorem 5 is slightly less than the bound(upper) given in the Theorem 4 but the method used to obtain this bound requires lattice of smaller dimension than the above.

Now in this paper we first describe the attack bounds for RSA cryptosystem in this section using the lattice based techniques based on the Coppersmith techniques [6] for finding small solutions of modular bivariate integer polynomial equations following the idea of Boneh-Durfee [3] and Blömer-May [4], when $\varphi(N)$ have some small multiplicative inverse modulo e , note when either $(p - 1) \bmod e$ or $(q - 1) \bmod e$ has small inverse we may adapt the attack as in [8] but when both $(p - 1) \bmod e$ and $(q - 1) \bmod e$ do not have small inverses the $\varphi(N) \bmod e$ may have small inverse as in Table 1 then this modified attack proposed in the following may be used.

e	$\varphi(N)^{-1} \bmod e$	$(p - 1)^{-1} \bmod e$	$(q - 1)^{-1} \bmod e$
1	0	0	0
5	3	1	3
7	5	4	3
11	9	9	1
13	4	9	12
17	7	16	10
19	10	6	8
23	3	13	2
25	3*	11	23
29	21	20	17
31	26	2	13
35	33	11	3
37	16	7	34
41	22	18	24
43	28	35	18
47	12	3	4
49	12	46	45
53	45	10	31
55	53	31	23
59	4*	48	5
61	34	42	56
65	43	61	38
67	52	21	28
71	27	40	6
73	27	32	67
77	75	53	45
79	7	5	33
83	16	26	7
85	58	16	78
89	70	39	52
91	82	74	38

e	$\varphi(N)^{-1} \bmod e$	$(p-1)^{-1} \bmod e$	$(q-1)^{-1} \bmod e$
95	48	6	8
97	48	91	89
101	10	19	59
103	22	58	43
107	34	87	9
109	88	75	100
113	103	106	66
115	3*	36	48
119	75	67	10
121	75	53	111
125	28	86	73
127	43	8	53
131	58	41	11
133	124	25	122
137	5*	21	60
139	113	80	58
143	108	9	12
145	108	136	133
149	52	28	87
151	70	85	63
155	88	126	13
157	9*	108	144
161	26	151	94
163	45	51	68
167	147	94	14
169	147	74	155
173	82	119	101
175	103	11	73
179	124	56	15
181	33	34	166
185	53	81	108
187	75	152	78
191	1*	12	16

Table 1: Multiplicative inverse of $\varphi(N), p-1$ and $q-1$ modulo e for fixed $N = pq = 13 \cdot 17$.

*For all such $\varphi(N)^{-1} \bmod e$ in the table, note $\varphi(N)^{-1} \bmod e$ is small but $(p-1)^{-1} \bmod e$ and $(q-1)^{-1} \bmod e$ are not small.

Let $N = pq, q < p < 2q, p - q = N^\beta$ and $e = N^\alpha > p + q$. As $(e, \varphi(N)) = 1$, there exist unique r, s such that

$$(p-1)r \equiv 1 \pmod e \text{ and } (q-1)s \equiv 1 \pmod e.$$

Let $k = rs \bmod e$, then $k\varphi(N) \equiv 1 \pmod e$, i.e., k is a multiplicative inverse of $\varphi(N)$ modulo e . For $g(x, y) = x(y + B) - 1$ where $B = N + 1 - \lceil 2\sqrt{N} \rceil$, the pair $(x_0, y_0) = (k, -((p+q) - \lceil 2\sqrt{N} \rceil))$ is a solution for the modular polynomial equation $g(x, y) \equiv 0 \pmod e$ (in general $(p+q) - \lceil 2\sqrt{N} \rceil \bmod e \leq (p+q) - \lceil 2\sqrt{N} \rceil$ and $(k, -((p+q) - \lceil 2\sqrt{N} \rceil) \bmod e)$ is also a solution but in this case $(p+q) - \lceil 2\sqrt{N} \rceil \bmod e = (p+q) - \lceil 2\sqrt{N} \rceil$ as $e > p+q$). Note as $q < \sqrt{N}, p+q - \lceil 2\sqrt{N} \rceil < N^\beta$, hence N^β is an upper bound for y_0 . Now note as the monomials for the polynomial g^m where $g(x, y) = x(y + N + 1 - \lceil 2\sqrt{N} \rceil) - 1$ and for the polynomial f^m where $f(x, y) = x(y + \lceil \sqrt{N} \rceil - 1) - 1$ described as in [8] are same for any positive integer m , we have the same analysis as in [8] for the above given modular equation with the multiplicative inverse k of $\varphi(N) \bmod e$ bounded by N^δ , we have $|k| \leq N^\delta$ and for $x_0 = k$, RSA is insecure under the following conditions:

$$\delta < \frac{3\alpha + \beta - 2\sqrt{\beta(3\alpha + \beta)}}{3}; \tag{1}$$

$$\delta < \frac{\alpha - \beta}{2}; \tag{2}$$

$$\alpha - \beta(1 + \alpha) < \delta < \alpha - \sqrt{\alpha\beta}; \tag{3}$$

$$\delta < \frac{2\alpha - 6\beta + 2\sqrt{\alpha^2 - \alpha\beta + 4\beta^2}}{5}. \tag{4}$$

Denoting the upper bounds for δ as in (1),(2),(3) and (4) by $\delta_1, \delta_2, \delta_3$ and δ_4 respectively, we have the bound for δ corresponding to α and β as given in Table 2, depicting the refinement of the attack bounds in the following.

α	β (\approx)	δ			
		δ_1	δ_2	δ_3	δ_4
0.501	0.50	0.0005	0.0005001873	0.0005002497	0.0005001874
0.55	0.50	0.025	0.0254519548	0.0255955759	0.0254626986
0.75	0.50	0.125	0.1349307066	0.1376275643	0.1358898943
1	0.50	0.25	0.2847495629	0.2928932188	0.2898979485

Table 2: Bounds for δ corresponding to certain values of α and $\beta \approx 0.5$ depicting the refinement.

By the analysis as in [8] note in all the above cases the maximum upper bound for δ is the bound as in (3), it is $\alpha - \sqrt{\frac{\alpha}{2}}$ for $\beta \approx 0.5$ and for $\alpha = 0.501, 0.55, 0.75, 1$, the value $\delta_3 = \alpha - \sqrt{\frac{\alpha}{2}} \approx 0.000501, 0.0254627, 0.135890, 0.289898$ respectively are the bounds for δ . Note the arguments above are considered for small multiplicative inverse of $\varphi(N) \bmod e$. Now in the next section the attack bound for δ is further refined for $\beta \approx 0.5$ by taking the prime sum $p + q$ as a composed prime sum i.e., $p + q = 2^n k_0 + k_1$ where n is a known positive integer, k_0 and k_1 are suitably small unknown integers and applying the lattice based arguments for trivariate polynomials.

4. An Attack Bound for RSA Using Lattice Based Techniques Based on Finding Small Modular Roots of Trivariate Polynomials

In this section, the attack bound for RSA is described when the prime sum $p + q$ is of the form $p + q = 2^n k_0 + k_1$ with a known positive integer n and unknown integers k_0 and k_1 using the lattice based techniques based on the E. Jochemsz and A. May’s extended strategy [10] for finding small solutions of modular multivariate integer polynomial equations. In this method the bound for δ can be improved for a suitable known integer n and suitable unknown parameters k_0, k_1 and for $\beta \approx 0.5$.

Let $p + q = 2^n k_0 + k_1$ where n is a given positive integer and k_0 and k_1 are unknown integers. First assume that $|k_0| \leq |k_1|$. As $k(N + 1 - (p + q)) \equiv 1 \pmod e$ for $k = rs \pmod e$, the triple $(x_0, y_0, z_0) = (k, -k_1, -k_0)$ is a solution for the modular polynomial equation $f(x, y, z) \equiv 0 \pmod e$ for $f(x, y, z) = (N + 1)x + xy + (2^n)xz - 1$ (observe that $|k_0| \pmod e = |k_0|$ and $|k_1| \pmod e = |k_1|$ as $e > p + q$). To apply the generalization of Howgrave-Graham result to find the small modular roots of the above equation $f(x, y, z) \equiv 0 \pmod e$, we use the extended strategy of Jochemsz and May [10]. Now define the set $M_k = \bigcup_{0 \leq j \leq t} \{x^{i_1}y^{i_2}z^{i_3+t} | x^{i_1}y^{i_2}z^{i_3}$ is a monomial of f^m and $\frac{x^{i_1}y^{i_2}z^{i_3}}{l^k}$ is a monomial of $f^{m-k}\}$, where l is a leading monomial of f and define the shift polynomials as $g_{k,i_1,i_2,i_3}(x, y, z) = \frac{x^{i_1}y^{i_2}z^{i_3}}{l^k} (f'(x, y, z))^k e^{m-k}$, for $k = 0, \dots, m, x^{i_1}y^{i_2}z^{i_3} \in M_k \setminus M_{k+1}$ and $f' = a_l^{-1}f \pmod e$ for the coefficient a_l of l . For $f(x, y, z) = (N + 1)x + xy + (2^n)xz - 1$, $x^{i_1}y^{i_2}z^{i_3}$ is a monomial of f^m if $i_1 = 0, \dots, m, i_2 = 0, \dots, i_1, i_3 = 0, \dots, (i_1 - i_2)$ and xy the leading monomial of f as $|k_0| \leq |k_1|$ with coefficient $a_l = 1$. Then for $0 \leq k \leq m, x^{i_1-k}y^{i_2-k}z^{i_3}$ is a monomial of f^{m-k} if $i_1 = k, \dots, m, i_2 = k, \dots, i_1, i_3 = 0, \dots, (i_1 - i_2)$. Therefore $x^{i_1}y^{i_2}z^{i_3} \in M_k$ if $i_1 = k, \dots, m, i_2 = k, \dots, i_1, i_3 = 0, \dots, (i_1 - i_2) + t$ and $x^{i_1}y^{i_2}z^{i_3} \in M_{k+1}$ if $i_1 = k + 1, \dots, m, i_2 = k + 1, \dots, i_1, i_3 = 0, \dots, (i_1 - i_2) + t$. From this, we obtain for $0 \leq k \leq m$,

$$x^{i_1}y^{i_2}z^{i_3} \in M_k \setminus M_{k+1} \text{ if } i_1 = k, i_2 = k, i_3 = 0, \dots, t \text{ and if } i_1 = k + 1, \dots, m, i_2 = k, i_3 = 0, \dots, (i_1 - i_2) + t.$$

Then for $0 \leq k \leq m$, the shift polynomials are $g_{k,i_1,i_2,i_3}(x,y,z) = z^{i_3}(f(x,y,z))^k e^{m-k}$, for $i_1 = i_2 = k, i_3 = 0, \dots, t$ and $g_{k,i_1,i_2,i_3}(x,y,z) = x^{i_1-k} z^{i_3}(f(x,y,z))^k e^{m-k}$, for $i_1 = k+1, \dots, m, i_2 = k, i_3 = 0, \dots, (i_1 - i_2) + t$. Suppose $X = N^\delta, Y = N^{\gamma_1}$ and $Z = N^{\gamma_2}$ are the upper bound for k, k_1 and k_0 respectively, then define the lattice \mathcal{L} spanned by the coefficient of the vectors $g_{k,i_1,i_2,i_3}(xX, yY, zZ)$. For example, the matrix M of \mathcal{L} when $m = 2$ and $t = 1$ is as given in the Table 3. Note that the matrix M of \mathcal{L} is lower triangular matrix and the coefficient of the leading monomial of

$$g_{k,i_1,i_2,i_3}(x,y,z) = z^{i_3}(f(x,y,z))^k e^{m-k}, \text{ for } i_1 = i_2 = k, i_3 = 0, \dots, t \text{ is } X^k Y^k e^{m-k} Z^{i_3} \text{ and}$$

$$g_{k,i_1,i_2,i_3}(x,y,z) = x^{i_1-k} z^{i_3}(f(x,y,z))^k e^{m-k}, \text{ for } i_1 = k+1, \dots, m, i_2 = k, i_3 = 0, \dots, (i_1 - i_2) + t \text{ is}$$

$X^{i_1} Y^k e^{m-k} Z^{i_3}$. Also note that these coefficients are the diagonal elements of the matrix M , so the determinant is

$$\det(\mathcal{L}) = e^{n_e} X^{n_X} Y^{n_Y} Z^{n_Z} \tag{5}$$

where

$$\begin{aligned} n_e &= \sum_{k=0}^m \sum_{i_1=k}^k \sum_{i_2=k}^k \sum_{i_3=0}^t (m-k) + \sum_{k=0}^m \sum_{i_1=k+1}^m \sum_{i_2=k}^k \sum_{i_3=0}^{(i_1-i_2)+t} (m-k) \\ &= \frac{1}{8}m^4 + \frac{1}{12}(4t+9)m^3 + \frac{1}{8}(8t+11)m^2 + \frac{1}{12}(8t+9)m, \\ n_X &= \sum_{k=0}^m \sum_{i_1=k}^k \sum_{i_2=k}^k \sum_{i_3=0}^t k + \sum_{k=0}^m \sum_{i_1=k+1}^m \sum_{i_2=k}^k \sum_{i_3=0}^{(i_1-i_2)+t} i_1 \\ &= \frac{1}{8}m^4 + \frac{1}{12}(4t+9)m^3 + \frac{1}{8}(8t+11)m^2 + \frac{1}{12}(8t+9)m, \\ n_Y &= \sum_{k=0}^m \sum_{i_1=k}^k \sum_{i_2=k}^k \sum_{i_3=0}^t k + \sum_{k=0}^m \sum_{i_1=k+1}^m \sum_{i_2=k}^k \sum_{i_3=0}^{(i_1-i_2)+t} k \\ &= \frac{1}{24}m^4 + \frac{1}{12}(2t+3)m^3 + \frac{1}{24}(12t+11)m^2 + \frac{1}{12}(4t+3)m, \\ n_Z &= \sum_{k=0}^m \sum_{i_1=k}^k \sum_{i_2=k}^k \sum_{i_3=0}^t i_3 + \sum_{k=0}^m \sum_{i_1=k+1}^m \sum_{i_2=k}^k \sum_{i_3=0}^{(i_1-i_2)+t} i_3 \\ &= \frac{1}{24}m^4 + \frac{1}{12}m^3(2t+3) + \frac{1}{24}(6t^2+18t+11)m^2 + \frac{1}{12}(9t^2+13t+3)m + \frac{1}{2}(t^2+t) \end{aligned}$$

and the dimension of \mathcal{L} is

$$\begin{aligned} \omega &= \sum_{k=0}^m \sum_{i_1=k}^k \sum_{i_2=k}^k \sum_{i_3=0}^t 1 + \sum_{k=0}^m \sum_{i_1=k+1}^m \sum_{i_2=k}^k \sum_{i_3=0}^{(i_1-i_2)+t} 1 \\ &= \frac{1}{6}m^3 + \frac{1}{2}m^2(t+2) + \frac{1}{6}m(9t+11) + (t+1). \end{aligned}$$

Take $t = \tau m$, then for sufficiently large m , the exponents n_e, n_X, n_Y, n_Z and the dimension ω reduce to

$$\begin{aligned} n_e &= \frac{1}{24}(3+8\tau)m^4 + o(m^3), \\ n_X &= \frac{1}{24}(3+8\tau)m^4 + o(m^3), \\ n_Y &= \frac{1}{24}(1+4\tau)m^4 + o(m^3), \\ n_Z &= \frac{1}{24}(1+4\tau+6\tau^2)m^4 + o(m^3), \\ \omega &= \frac{1}{6}(1+3\tau)m^3 + o(m^2). \end{aligned}$$

Applying the LLL algorithm to the basis vectors of the lattice \mathcal{L} , i.e., coefficient vectors of the shift polynomials, we get a LLL-reduced basis say $\{v_1, v_2, \dots, v_\omega\}$ and from the Theorem 1 we have

$$\|v_1\| \leq \|v_2\| \leq \|v_3\| \leq 2^{\frac{\omega(\omega-1)}{4(\omega-2)}} \det(\mathcal{L})^{\frac{1}{\omega-2}}.$$

In order to apply the generalization of Howgrave-Graham result in Theorem 2, we need the following inequality

$$2^{\frac{\omega(\omega-1)}{4(\omega-2)}} \det(\mathcal{L})^{\frac{1}{\omega-2}} < \frac{e^m}{\sqrt{\omega}}.$$

from this, we deduce

$$\det(\mathcal{L}) < \frac{1}{\left(2^{\frac{\omega(\omega-1)}{4(\omega-2)}} \sqrt{\omega}\right)^{\omega-2}} e^{m(\omega-2)} < \frac{1}{\left(2^{\frac{\omega(\omega-1)}{4(\omega-2)}} \sqrt{\omega}\right)^{\omega-2}} e^{m\omega}.$$

As the dimension ω is not depending on the public encryption exponent e , $\frac{1}{\left(2^{\frac{\omega(\omega-1)}{4(\omega-2)}} \sqrt{\omega}\right)^{\omega-2}}$ is a fixed constant, so we need the inequality $\det(\mathcal{L}) < e^{m\omega}$.

Using (5), we get the inequality

$$e^{ne} X^{nX} Y^{nY} Z^{nZ} < e^{m\omega}.$$

Substitute all values and taking logarithms, neglecting the lower order terms and after simplifying by m^4 we get

$$(3 + 8\tau)\alpha + (3 + 8\tau)\delta + (1 + 4\tau)\gamma_1 + (1 + 4\tau + 6\tau^2)\gamma_2 - 4\alpha(1 + 3\tau) < 0.$$

The left hand side inequality is minimized at $\tau = \frac{1-(2\delta+\gamma_1+\gamma_2)}{3\gamma_2}$ and putting this value in the above inequality we get

$$\delta < \frac{1}{2}\alpha - \frac{1}{2}\gamma_1 + \frac{1}{6}\gamma_2 - \frac{1}{6}\sqrt{48(1-\gamma_1)\gamma_2 + 33\gamma_2^2}.$$

From the first three vectors v_1, v_2 and v_3 in LLL reduced basis we consider three polynomials $g_1(x, y, z), g_2(x, y, z)$ and $g_3(x, y, z)$ over \mathbb{Z} such that $g_1(x_0, y_0, z_0) = g_2(x_0, y_0, z_0) = g_3(x_0, y_0, z_0) = 0$. Suppose g_1, g_2 and g_3 are algebraically independent and let $h_1(x, y)$ be the resultant polynomial of $g_1(x, y, z)$ and $g_2(x, y, z)$ with respect to z and $h_2(x, y)$ be the resultant polynomial of $g_1(x, y, z)$ and $g_3(x, y, z)$ with respect to z and if h_1, h_2 are algebraically independent and let $h(x)$ be the resultant polynomial of $h_1(x, y)$ and $h_2(x, y)$ with respect to y , then we have $h(x)$ is not identically zero and with a solution $x = x_0$ from Remark 1 & 2. Note that if k is small such that $k \leq N^\delta$ for $\delta < \frac{1}{2}\alpha - \frac{1}{2}\gamma_1 + \frac{1}{6}\gamma_2 - \frac{1}{6}\sqrt{48(1-\gamma_1)\gamma_2 + 33\gamma_2^2}$, then $x_0 = k$ is a solution for the polynomial $h(x)$ over \mathbb{Z} . With the knowledge of k , we can find the $\varphi(N)$ and the value $p + q$ can be obtained from $\varphi(N)$. Then we can factor the RSA modulus N as $(p + q)^2 - 4N = (p - q)^2$.

Theorem 4.1. *Let $N = pq$ be an RSA modulus with $q < p < 2q$. Let $e = N^\alpha, X = N^\delta, Y = N^{\gamma_1}, Z = N^{\gamma_2}$ and k be the multiplicative inverse of $\varphi(N)$ modulo e . Suppose the prime sum $p + q$ is of the form $p + q = 2^n k_0 + k_1$, for a known positive integer n and assume that $|k_0| \leq |k_1|$ then for $|k| \leq X, |k_1| \leq Y$ and $|k_0| \leq Z$ one can factor N in polynomial time if*

$$\delta < \frac{1}{2}\alpha - \frac{1}{2}\gamma_1 + \frac{1}{6}\gamma_2 - \frac{1}{6}\sqrt{48(1-\gamma_1)\gamma_2 + 33\gamma_2^2}. \quad (6)$$

Proof. Follows from the above argument and the LLL lattice basis reduction algorithm operates in polynomial time [11]. □

	1	x	xz	x^2	x^2z	x^2z^2	xy	x^2y	x^2yz	x^2y^2	z	xz^2	x^2z^3	xyz	x^2yz^2	x^2y^2z
e^2	e^2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
xe^2	0	Xe^2	0	0	0	0	0	0	0	0	0	0	0	0	0	0
xze^2	0	0	XZe^2	0	0	0	0	0	0	0	0	0	0	0	0	0
x^2e^2	0	0	0	X^2e^2	0	0	0	0	0	0	0	0	0	0	0	0
x^2ze^2	0	0	0	0	X^2Ze^2	0	0	0	0	0	0	0	0	0	0	0
$x^2z^2e^2$	0	0	0	0	0	$X^2Z^2e^2$	0	0	0	0	0	0	0	0	0	0
fe	$-e$	$(N+1)Xe$	2^nXZe	0	0	0	XYe	0	0	0	0	0	0	0	0	0
xfe	0	$-Xe$	0	$(N+1)X^2e$	2^nX^2Ze	0	0	X^2Ye	0	0	0	0	0	0	0	0
$xzfe$	0	0	$-XZe$	0	$(N+1)X^2Ze$	$2^nX^2Z^2e$	0	0	X^2YZe	0	0	0	0	0	0	0
f^2	1	$-2(N+1)X$	$-2^{n+1}XZ$	$(N+1)^2X^2$	$2^{n+1}(N+1)X^2Z$	$2^{2n}X^2Z^2$	$-2XY$	$2(N+1)X^2Y$	$2^{n+1}X^2YZ$	X^2Y^2	0	0	0	0	0	0
ze^2	0	0	0	0	0	0	0	0	0	0	Ze^2	0	0	0	0	0
xz^2e^2	0	0	0	0	0	0	0	0	0	0	0	XZ^2e^2	0	0	0	0
$x^2z^3e^2$	0	0	0	0	0	0	0	0	0	0	0	0	$X^2Z^3e^2$	0	0	0
zfe	0	0	$(N+1)XZe$	0	0	0	0	0	0	0	$-Ze$	2^nXZ^2e	0	$XYZe$	0	0
xz^2fe	0	0	0	0	$(N+1)X^2Z^2e$	0	0	0	0	0	0	$-XZ^2e$	$2^nX^2Z^3e$	0	X^2YZ^2e	0
zf^2	0	0	$-2(N+1)XZ$	0	$(N+1)^2X^2Z$	$2^{n+1}(N+1)X^2Z^2$	0	0	$2(N+1)X^2YZ$	0	Z	$-2^{n+1}XZ^2$	$2^{2n}X^2Z^3$	$-2XYZ$	$2^{n+1}X^2YZ^2$	X^2Y^2Z

Table 3: The matrix spanned by the coefficient vectors of the shift polynomials $g_{n,i_1,i_2,i_3}(xX, yY, zZ)$ for $m = 2$ and $t = 1$.

Suppose $|k_1| \leq |k_0|$. As $2|\varphi(N)$, $\gcd(e, 2^n) = 1$ for any n . If $2^{n'} = (2^n)^{-1} \pmod e$ then the triple $(k, -k_0, -k_1)$ is a solutions for the modular polynomial equation $f(x, y, z) \equiv 0 \pmod e$ where $f(x, y, z) = 2^{n'}x(N + 1) + xy + 2^{n'}xz - 2^{n'}$ with the leading monomial xy with coefficient 1. Applying the above analysis to the above modular equation for the upper bounds $X = N^\delta, Y = N^{\gamma_1}$ and $Z = N^{\gamma_2}$ of k, k_0 and k_1 respectively, we get the bound for δ same as in (6).

Note that for any given primes p and q with $q < p < 2q$, we can always find a positive integer n such that $p + q = 2^n k_0 + k_1$ where $0 \leq |k_0|, |k_1| \leq \approx 0.25$. A typical example is $2^n \approx \frac{3}{\sqrt{2}}N^{0.25}$ as $p + q < \frac{3}{\sqrt{2}}N^{0.5}$ [14]. Denoting the bound for δ as in (6) by δ_5 and as $\gamma_2 \leq \gamma_1$ for $|k_0| \leq |k_1|$ or $|k_1| \leq |k_0|$, in the Table 4 we represent the values of γ_1 and γ_2 for given α and the bound δ_5 which is grater than $\alpha - \sqrt{\frac{\alpha}{2}}, \delta_3$ for $\beta \approx 0.5$.

α	γ_1	γ_2	δ_5
0.501	0.25	0.249 - 0	0.00067 - 0.1255
	0.15	0.149 - 0	0.07227 - 0.1755
	0.01	0.009 - 0	0.21710 - 0.2455
0.55	0.25	0.225 - 0	0.02557 - 0.15
	0.15	0.149 - 0	0.09084 - 0.2
	0.01	0.009 - 0	0.24021 - 0.27
0.75	0.25	0.133 - 0	0.13687 - 0.25
	0.15	0.149 - 0	0.16923 - 0.3
	0.01	0.009 - 0	0.33508 - 0.37
1	0.25	0.052 - 0	0.29073 - 0.375
	0.15	0.116 - 0	0.29005 - 0.425
	0.01	0.009 - 0	0.45457 - 0.495

Table 4: The improved bounds for δ for $\beta \approx 0.5$ and for a given e with suitable values of γ_1 and γ_2 .

In the following Table 5 we give the attack bounds for δ for the small multiplicative inverse of $\varphi(N) \pmod e$ obtained using methods based on lattice based techniques with respect to bivariate and trivariate polynomial congruences for certain values of α and $\beta \approx 0.5$ thereby depicting the refinement of attack bounds for δ .

α	δ_1	δ_2	δ_3	δ_4	δ_5	
0.501	0.0005	0.0005001873	0.0005002497	0.0005001874	$\gamma_1 = 0.25$ $\gamma_2 = 0.249 - 0$	0.00067 - 0.1255
					$\gamma_1 = 0.15$ $\gamma_2 = 0.149 - 0$	0.07227 - 0.1755
					$\gamma_1 = 0.01$ $\gamma_2 = 0.009 - 0$	0.21710 - 0.2455
0.55	0.025	0.0254519548	0.0255955759	0.0254626986	$\gamma_1 = 0.25$ $\gamma_2 = 0.225 - 0$	0.02557 - 0.15
					$\gamma_1 = 0.15$ $\gamma_2 = 0.149 - 0$	0.09084 - 0.2
					$\gamma_1 = 0.01$ $\gamma_2 = 0.009 - 0$	0.24021 - 0.27
0.75	0.125	0.1349307066	0.1376275643	0.1358898943	$\gamma_1 = 0.25$ $\gamma_2 = 0.133 - 0$	0.13687 - 0.25
					$\gamma_1 = 0.15$ $\gamma_2 = 0.149 - 0$	0.16923 - 0.3
					$\gamma_1 = 0.01$ $\gamma_2 = 0.009 - 0$	0.33508 - 0.37

α	δ_1	δ_2	δ_3	δ_4	δ_5	
1	0.25	0.2847495629	0.2928932188	0.2898979485	$\gamma_1 = 0.25$	0.29073 - 0.375
					$\gamma_2 = 0.052 - 0$	
					$\gamma_1 = 0.15$	0.29005 - 0.425
					$\gamma_2 = 0.116 - 0$	
$\gamma_1 = 0.01$	0.45457 - 0.495					
$\gamma_2 = 0.009 - 0$						

Table 5: Refinement of attack bounds for δ using lattice based techniques with respect to bivariate and trivariate polynomials.

5. Conclusion

In this paper it is shown that RSA is insecure if $\varphi(N)$ has small multiplicative inverse k modulo e , the public encryption exponent. For $k \leq N^\delta$, the attack bounds for δ are described by using lattice based techniques with respect to bivariate polynomial congruence and this attack bound for δ is further refined for $\beta \approx 0.5$ by taking the prime sum $p+q$ as a composed prime sum i.e., $p+q = 2^n k_0 + k_1$ where n is a known positive integer, k_0 and k_1 are suitably small unknown integers and applying the lattice based arguments for trivariate polynomials. This refinement of attack bound for δ is depicted for certain values of α and $\beta \approx 0.5$.

References

- [1] Tom M.Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag, New York Inc.
- [2] D.Boneh, *Twenty Years of Attacks on the RSA Cryptosystem*, Notices Amer. Math. Soc., 46(2)(1999), 203-213.
- [3] D.Boneh and G.Durfee, *Cryptanalysis of RSA with private key d less than $N^{0.292}$* , Advances in Cryptology Eurocrypt, Lecture Notes in Computer Science Vol. 1592, Springer-Verlag, (1999), 1-11).
- [4] J.Blömer and A.May, *Low Secret Exponent RSA Revisited*, Cryptography and Lattice Conference (CaLC 2001), Lecture Notes in Computer Science Volume 2146, Springer Verlag, (2001), 4-19.
- [5] D.Burton, *Elementary Number Theory*, Sixth edition, Mc Graw Hill, New York, (2007).
- [6] D.Coppersmith, *Small solutions to polynomial equations, and low exponent RSA vulnerabilities*, Journal of Cryptology, 10(4)(1997), 233-260 .
- [7] N.Howgrave-Graham, *Finding small roots of univariate modular equations revisited*, In Cryptography and Coding, LNCS 1355, Springer-Verlag, (1997), 131-142.
- [8] P.Anuradha Kameswari and L.Jyotsna, *Cryptanalysis of RSA with small multiplicative inverse of $p-1$ or $q-1$ modulo e* , (Communicated).
- [9] P.A.Kameswari and L.Jyotsna, *Extending Wiener’s Extension to RSA-Like Cryptosystems over Elliptic Curves*, British Journal of Mathematics & Computer Science 14(1)(2016), 1-8.
- [10] E.Jochemsz and A.May, *A strategy for finding roots of multivariate polynomials with new applications in attacking RSA variants*, ASIACRYPT 2006, LNCS, Springer-Verlag, 4284(2006), 267-282.
- [11] A.K.Lenstra, H.W.Lenstra and L.Lovasz, *Factoring polynomials with rational coefficients*, Mathematische Annalen, 261(1982), 513-534.
- [12] A.May, *New RSA Vulnerabilities Using Lattice Reduction Methods*, Ph.D thesis, University of Paderborn, (2003).
- [13] Neal Koblitz, *A Course in Number Theory and Cryptography*, ISBN 3-578071-8, SPIN 10893308.

- [14] A.Nitaj, *Another generalization of Wiener's attack on RSA*, In: Vaudenay, S. (ed.) Africacrypt 2008. LNCS, 5023(2008), 174-190.
- [15] K.H.Rosen, *Elementary Number Theory and Its Applications*, Addison-Wesley, Reading Mass, (1984).
- [16] Subhamoy Maitra and Santanu Sarkar, *Revisiting Wiener's Attack - New Weak Keys in RSA*, Available: <http://eprint.iacr.org/2005/228.pdf>.
- [17] Subhamoy Maitra and Santanu Sarkar, *RSA Cryptanalysis with Increased Bounds on the Secret Exponent using Less Lattice Dimension*, Cryptology ePrint Archive: Report 2008/315, Available at <http://eprint.iacr.org/2008/315>.
- [18] H.-M.Sun, M.-E.Wu and Y.-H.Chen, *Estimating the prime-factors of an RSA modulus and an extension of the Wiener attack*, ACNS 2007, LNCS 4521(2007), 116-128.
- [19] B.de Weger, *Cryptanalysis of RSA with Small Prime Difference*", *Applicable Algebra in Engineering, Communication and Computing*, 13(1)(2002), 17-28.
- [20] M.Wiener, *Cryptanalysis of Short RSA Secret Exponents*, *IEEE Transactions on Information Theory*, 36(3)(1990), 553-558.

Cryptanalysis of RSA with Small Multiplicative Inverse of $(p - 1)$ or $(q - 1)$ Modulo e

P. Anuradha Kameswari, L. Jyotsna

Department of Mathematics, Andhra University,
Visakhapatnam - 530003, Andhra Pradesh, India.
panuradhakameswari@yahoo.in, jyotsna.jahnavi@gmail.com

Abstract

In this paper, we mount an attack on RSA by using lattice based techniques implemented in the case when $p - 1$ or $q - 1$ have small multiplicative inverse less than or equal to N^δ modulo the public encryption exponent e , for some small δ and described the attack bounds for δ .

Key words : RSA, Cryptanalysis, LLL algorithm, Coppersmith's method.

2010 Mathematics Subject Classification: 11T71, 94A60.

1 Introduction

RSA Cryptosystem is the first public key cryptosystem invented by Ronald Rivest, Adi Shamir and Leonard Adelman in 1977 where the encryption and decryption are based on the fact that if $N = pq$, is the modulus for RSA, p, q distinct primes, if $1 \leq e \leq \varphi(N)$ with $(e, \varphi(N)) = 1$ and d , the multiplicative inverse of e modulo $\varphi(N)$, then $m^{ed} = m \pmod{N}$, for any message m , an integer in Z_N . The security of this system depends on the difficulty of finding factors of a composite positive integer, that is product of two large primes. In 1990, M.J. Wiener [15] was the first one to describe a cryptanalytic attack on the use of short RSA deciphering exponent d . This attack is based on continued fraction algorithm which finds the fraction $\frac{t}{d}$, where $t = \frac{ed-1}{\varphi(N)}$ in a polynomial time when d is less than $N^{0.25}$ for $N = pq$ and $q < p < 2q$. In 2000, D. Boneh and G. Durfee [2] improved the Wiener result from $N^{0.25}$ to $N^{0.292}$, for $q < p < 2q$ using lattice reduction approach based on the theory of finding small roots of polynomials by methods due to Coppersmith. A lattice attack on RSA with short secret exponent d , for d less than $N^{0.29}$ was given by J. Blömer and A. May [3] in 2001, this is slightly less than that of Boneh and Durfee but this method requires lattices of dimension smaller than the approach by Boneh and Durfee. In 2002, de Weger [14], extended the Wiener's attack in the range $N^{0.25} \leq d \leq N^{0.75-\beta}$, for $p - q = N^\beta$ and $q < p < 2q$ by method of continued fraction and the bound improved to $\delta < \frac{1}{6}(4\beta + 5) - \frac{1}{3}\sqrt{(4\beta + 5)(4\beta - 1)}$ using the first result of Boneh and Durfee(lattice based techniques) in [2] and the bound improved to $\delta < 1 - \sqrt{2\beta - \frac{1}{2}}$ using the second result of Boneh and Durfee(sub-lattice based techniques)in [2] under the condition $\delta > 1 - 4\beta$. Instead of considering $p - q = N^\beta$, Subhamoy Maitra and Santanu Sarkar [12] considered $|p - \rho q| \leq \frac{N^\gamma}{16}$ where $1 \leq \rho \leq 2$ to get some additional results. That is, given ρ with $1 \leq \rho \leq 2$ known to the attacker, RSA is insecure when $d = N^\delta$ and $\delta < \frac{1}{2} - \frac{\gamma}{2}$, for $|p - \rho q| \leq \frac{N^\gamma}{16}$ and $\gamma \leq \frac{1}{2}$ and also showed that this bound on δ can be extended using the lattice based techniques. In this attack the value of ρ should be known to the attacker and is possible by the fact that, the knowledge of most significant bits(MSBs) [13] of p or q can provide approximation of ρ or one may try to guess ρ for different values (that are computationally feasible) to mount the attack.

In this paper it is shown that RSA will be insecure if one of the multiplicative inverse of $p - 1$ and $q - 1$ modulo the public encryption exponent e is small. Let $e = N^\alpha > p - 1$, s and r be the multiplicative inverses of $q - 1$ and $p - 1$ modulo e respectively, then note the pairs $(s, q - \lceil \sqrt{N} \rceil)$ and $(r, p - \lceil \sqrt{N} \rceil)$ are the solutions of the polynomial congruence $f(x, y) \equiv 0 \pmod{e}$, for $f(x, y) = x(y + A) - 1$ with $A = \lceil \sqrt{N} \rceil - 1$. Let (x_0, y_0) be the solutions of the polynomial congruence $f(x, y) \equiv 0 \pmod{e}$, with $x_0 = \min\{r, s\}$ and N^δ, N^γ be an upper bounds for x_0, y_0 respectively then by implementing the idea of Boneh and Durfee as in [2] based on lattice reduction techniques to our polynomial congruence we show that the attack works for $\delta < \frac{3\alpha + \gamma - 2\sqrt{\gamma(3\alpha + \gamma)}}{3}$ when both x and y shifts are used and $\delta < \frac{\alpha - \gamma}{2}$ when only x -shifts are used. Later to improve the bound for

* Both authors thank the University Grants Commission(UGC) for the support of the UGC grant under UGC-MRP scheme.

δ up to $\alpha - \sqrt{\alpha\gamma}$ we implemented the sublattice based techniques by Boneh and Durfee under the condition $\delta > \alpha - \gamma(1 + \alpha)$ and to improve the bound as $\delta < \frac{2\alpha - 6\gamma + 2\sqrt{\alpha^2 - \alpha\gamma + 4\gamma^2}}{5}$ we implemented the sublattice based techniques of J. Blömer and A. May as in [3], in this result the bound for δ is only slightly less than the bound for δ as in the above method with sublattice based techniques by Boneh and Durfee but the advantage of this method is that it requires lattices of smaller dimension than the above method. Further note that as N^γ is depending on the prime difference $p - q = N^\beta$, i.e., the value of N^γ decreases when the prime difference is decreasing, the bound for δ increases when the prime difference is decreasing. Also it is observed that in a practical implementation of our results, the above RSA attacks are ineffective if e is exceeding a particular bound that is based on prime difference. In the above four implementations for δ denoted as $\delta_{x,y}$, δ_x , δ_s and δ_{sd} respectively, the attack bounds are described with an analysis of these bounds with respect to the prime difference $p - q$, for $p - q = N^\beta$ and with respect to $p - \rho q$, for ρ such that ρq is a better approximation for p .

2 Preliminaries

In this section we state a few basic results about lattices, lattice basis reduction and also Coppersmith’s method and Howgrave-Graham theorems based on lattice reduction techniques.

Let $u_1, u_2, \dots, u_n \in \mathbb{Z}^m$ be linearly independent vectors with $n \leq m$. Let L be a lattice spanned by $\langle u_1, u_2, \dots, u_n \rangle$ and $b_1^*, b_2^*, \dots, b_n^*$ be the vectors obtained by applying the Gram-Schmidt process to the vectors u_1, u_2, \dots, u_n . The determinant of the lattice L is defined as $det(L) := \prod_{i=1}^n \|b_i^*\|$, where $\| \cdot \|$ denotes the Euclidean norm on vectors. If L is a full rank lattice, means $n = m$ then the determinant of L is equal to the determinant of the $n \times n$ matrix whose rows are the basis vectors u_1, u_2, \dots, u_n .

Properties of LLL Algorithm:

Let L be a lattice spanned by $\langle u_1, u_2, \dots, u_n \rangle$. Then the LLL (Lenstra-Lenstra-Lovász) algorithm for a given $\langle u_1, u_2, \dots, u_n \rangle$, runs in polynomial time and produces a new basis $\langle b_1, b_2, \dots, b_n \rangle$ of L satisfying:

1. $\|b_i^*\|^2 \leq 2 \|b_{i+1}^*\|^2$, for all $1 \leq i < n$.
2. For all i , if $b_i = b_i^* + \sum_{j=1}^{i-1} \mu_j b_j^*$ then $|\mu_j| \leq \frac{1}{2}$ for all j .

Theorem 1. Let L be a lattice and b_1, b_2, \dots, b_n be an LLL-reduction basis of L . Then $\|b_1\| \leq 2^{n/2} det(L)^{1/n}$ [2].

Theorem 2. Let L be a lattice spanned by $\langle u_1, u_2, \dots, u_n \rangle$ and let $\langle b_1, b_2, \dots, b_n \rangle$ be the result of applying LLL to the given basis. Suppose $u_{min}^* \geq 1$ where u_{min}^* is a lower bound on the length of the shortest vector in L . Then $\|b_2\| \leq 2^{n/2} det(L)^{\frac{1}{n-1}}$ [2].

An important application of lattice reduction found by Coppersmith in 1996 [5] is finding small roots of low-degree polynomial equations. This includes modular univariate polynomial equations and bivariate integer equations. In 1997 Howgrave-Graham [6] reformulated Coppersmith’s techniques and proposed the following result and it shows that if the coefficients of $h(x, y)$ are sufficiently small, then the equality $h(x_0, y_0) = 0$ holds not only modulo N , but also over integers.

Theorem 3. (Howgrave-Graham): Let $h(x, y) \in \mathbb{Z}[x, y]$ be an integer polynomial that consists of at most w monomials. Suppose that

1. $h(x_0, y_0) = 0 \pmod{e^m}$ for some m where $|x_0| < X$ and $|y_0| < Y$, and
2. $\|h(xX, yY)\| < \frac{e^m}{\sqrt{w}}$.

Then $h(x_0, y_0) = 0$ holds over integers.

Now we present the definition of geometrically progressive matrices in the following.

Definition 1. Let M be an $(a + 1)b \times (a + 1)b$ matrix. The pair (i, j) corresponds to $(bi + j) - th$ column of M . Similarly a pair (k, l) can be used to index $(bk + l) - th$ row of M . Let $C, D, c_0, c_1, c_2, c_3, c_4, \beta$ be real numbers with $C, D, \beta \geq 1$. A matrix M is said to be geometrically progressive with parameters $(C, D, c_0, c_1, c_2, c_3, c_4, \beta)$ if the following conditions hold for all i, k in $[0, \dots, a]$ and for all j, l in $[1, \dots, b]$:

- i) $|M(i, j, k, l)| \leq CD^{c_0 + c_1 i + c_2 j + c_3 k + c_4 l}$,
- ii) $M(k, l, k, l) = D^{c_0 + c_1 k + c_2 l + c_3 k + c_4 l}$,
- iii) $M(i, j, k, l) = 0$ whenever $i > k$ or $j > l$,
- iv) $\beta c_1 + c_3 \geq 0$ and $\beta c_2 + c_4 \geq 0$.

Theorem 4. Let M be an $(a+1)b \times (a+1)b$ geometrically progressive matrix with parameters $(C, D, c_0, c_1, c_2, c_3, c_4, \beta)$, and let B be a real number. Define

$$S_B = \{(k, l) \in 0, \dots, a \times 1, \dots, b \mid M(k, l, k, l) = B\}$$

and set $w = |S_B|$. If L is the lattice defined by rows $(k, l) \in S_B$ of M , then

$$\det(L) \leq ((a+1)b)^{w/2} (1+C)^{w^2} \prod_{(k,l) \in S_B} M(k, l, k, l) \quad [2].$$

Resultant of two bivariate polynomials:

The resultant of two polynomials $f(x, y)$ and $g(x, y)$ with respect to the variable y , is defined as the determinant of Sylvester matrix of $f(x, y)$ and $g(x, y)$ when considered as polynomials in the single indeterminate y . The resultant is non-zero if and only if the two polynomials are algebraically independent. When the polynomials are algebraically independent, the resultant yields a new polynomial $h(x)$ such that if (x_0, y_0) is a root of both $f(x, y)$ and $g(x, y)$ then $h(x_0) = 0$.

Assumption 1. The two polynomials return by LLL algorithm are algebraically independent.

There is no theoretical proof for this one, but in practice most of the times achieved.

Result 1. Let $N = pq$ be an RSA modulus with $q < p < 2q$. Then the prime factors p and q satisfy the following property [9]

$$\frac{\sqrt{2}\sqrt{N}}{2} < q < \sqrt{N} < p < \sqrt{2}\sqrt{N}. \tag{1}$$

3 Cryptanalysis of RSA and an Attack Bound Using Lattice-Based Techniques

In this section we describe how small multiplicative inverse of $(p-1)$ or $(q-1)$ modulo e results a new weakness for RSA by using the lattice reduction techniques as in [2] by Boneh-Durfee and in [3] by Blömer-May.

Let $N = pq, q < p < 2q, e$ be the public encryption exponent and d be the private decryption exponent. The public encryption exponent e and $\varphi(N)$ are relatively prime so for $e > p-1$ there exist unique r, s such that

$$(p-1)r \equiv 1 \pmod{e} \text{ and } (q-1)s \equiv 1 \pmod{e} \tag{2}$$

and note r, s are the multiplicative inverses of $p-1, q-1$ respectively. Now let $f(x, y) = x(y+A) - 1$ for $A = \lceil \sqrt{N} \rceil - 1$. If $x_0 = r$ then for $y_0 = p - \lceil \sqrt{N} \rceil$ we have $f(x_0, y_0) \equiv 0 \pmod{e}$ and if $x_0 = s$ then for $y_0 = q - \lceil \sqrt{N} \rceil$ we have $f(x_0, y_0) \equiv 0 \pmod{e}$ by using (2). Now for $|x_0| \leq N^\delta, |y_0| \leq N^\gamma$ for some δ and γ note $N^\gamma = |\rho - 1|\sqrt{N}, 1 < \rho < \sqrt{2}$ if $y_0 = p - \lceil \sqrt{N} \rceil$ and $N^\gamma = |\rho - 1|\sqrt{N}, \frac{1}{\sqrt{2}} < \rho < 1$ if $y_0 = q - \lceil \sqrt{N} \rceil$ by using (1) (observe that $p - \lceil \sqrt{N} \rceil \pmod{e} \leq p - \lceil \sqrt{N} \rceil, \lceil \sqrt{N} \rceil - q \pmod{e} \leq \lceil \sqrt{N} \rceil - q$ and $(r, p - \lceil \sqrt{N} \rceil \pmod{e})$ and $(s, -(\lceil \sqrt{N} \rceil - q) \pmod{e})$ are also solutions but in this case $p - \lceil \sqrt{N} \rceil \pmod{e} = p - \lceil \sqrt{N} \rceil$ and $\lceil \sqrt{N} \rceil - q \pmod{e} = \lceil \sqrt{N} \rceil - q$ as $e > p - 1$).

Now we consider the polynomial $f(x, y) = x(y+A) - 1$ and find (x_0, y_0) satisfying:

$$f(x_0, y_0) \equiv 0 \pmod{e}, \text{ for } e = N^\alpha, |x_0| \leq N^\delta \text{ and } |y_0| \leq N^\gamma, \text{ with } N^\gamma = |\rho - 1|\sqrt{N} \text{ such that } \rho \text{ is in the range } \begin{cases} \frac{1}{\sqrt{2}} < \rho < 1, & \text{if } x_0 = s, y_0 = q - \lceil \sqrt{N} \rceil \\ 1 < \rho < \sqrt{2}, & \text{if } x_0 = r, y_0 = p - \lceil \sqrt{N} \rceil. \end{cases}$$

To solve for the above (x_0, y_0) we use lattice based techniques to our polynomial and the upper bounds $X = N^\delta, Y = N^\gamma$ as in [2]:

For given a positive integer m , define the polynomials

$$g_{i,k} = x^i f^k(x, y) e^{m-k} \text{ and } h_{j,k} = y^j f^k(x, y) e^{m-k},$$

referred as the x -shifts and y -shifts respectively. Now define the lattice \mathcal{L} spanned by the coefficients of the vectors $g_{i,k}(xX, yY)$ and $h_{j,k}(xX, yY)$ for $k = 0, \dots, m, i = 0, \dots, m-k$ and $j = 0, \dots, t$. Note that the matrix M of \mathcal{L} is lower triangular and the coefficient of the leading monomial of $g_{i,k}(xX, yY)$ is $X^{i+k} Y^k e^{m-k}$ and also the coefficient of the leading monomial of $h_{i,k}(xX, yY)$ is $X^k Y^{j+k} e^{m-k}$, so the determinant is

$$\det(\mathcal{L}) = e^{n_e} X^{n_x} Y^{n_y}$$

where

$$\begin{aligned}
 n_e &= \sum_{k=0}^m \sum_{i=0}^{m-k} (m-k) + \sum_{k=0}^m \sum_{j=1}^t (m-k) \\
 &= \frac{m(m+1)(m+2)}{3} + \frac{tm(m+1)}{2}, \\
 n_X &= \sum_{k=0}^m \sum_{i=0}^{m-k} (i+k) + \sum_{k=0}^m \sum_{j=1}^t k \\
 &= \frac{m(m+1)(m+2)}{3} + \frac{tm(m+1)}{2}, \\
 n_Y &= \sum_{k=0}^m \sum_{i=0}^{m-k} k + \sum_{k=0}^m \sum_{j=1}^t (j+k) \\
 &= \frac{m(m+1)(m+2)}{6} + \frac{t(m+1)(m+t+1)}{2}
 \end{aligned}$$

and the dimension of \mathcal{L} is

$$\begin{aligned}
 w &= \sum_{k=0}^m \sum_{i=0}^{m-k} 1 + \sum_{k=0}^m \sum_{j=1}^t 1 \\
 &= \frac{(m+1)(m+2)}{2} + t(m+1).
 \end{aligned}$$

Applying the LLL algorithm we can obtain two short vectors b_1, b_2 and by using Theorem 1 & 2 this vectors satisfies

$$\|b_1\|, \|b_2\| \leq 2^{w/2} \det(\mathcal{L})^{\frac{1}{w-1}}.$$

Now in order to apply Howgrave-Graham's theorem, we should have

$$2^{\frac{w}{2}} \det(\mathcal{L})^{\frac{1}{w-1}} < \frac{e^m}{\sqrt{w}}.$$

From this, we deduce

$$\det(\mathcal{L}) < \frac{1}{(2^{\frac{w}{2}})^{w-1}} e^{m(w-1)} < e^{mw}$$

To satisfy the above inequality we need the following inequality

$$e^{n_e} X^{n_X} Y^{n_Y} < e^{mw}.$$

Substitute all values and taking logarithms, neglecting the low order terms and after simplifying we get

$$m^3 \left(\frac{2\alpha + 2\delta + \gamma}{6} \right) + tm^2 \left(\frac{\alpha + \delta + \gamma}{2} \right) + mt^2 \left(\frac{\gamma}{2} \right) < \alpha \left(\frac{1}{2}m^3 + tm^2 \right)$$

This leads to

$$m^2 \left(\frac{-\alpha + 2\delta + \gamma}{6} \right) + tm \left(\frac{\gamma + \delta - \alpha}{2} \right) + t^2 \left(\frac{\gamma}{2} \right) < 0.$$

After fixing an m , the left hand side is minimized at $t = \frac{\alpha - \delta - \gamma}{2\gamma} m$. Putting this value we get the inequality

$$\delta < \frac{3\alpha + \gamma - 2\sqrt{\gamma(3\alpha + \gamma)}}{3}.$$

From the vectors b_1 and b_2 we obtain two polynomials $g_1(x, y)$ and $g_2(x, y)$ over \mathbb{Z} such that $g_1(x_0, y_0) = g_2(x_0, y_0) = 0$. Let $h(x)$ be the resultant polynomial of $g_1(x, y)$ and $g_2(x, y)$ with respect to y . By Assumption 1, $h(x)$ is not identically zero. Now note if r or s are small such that $|s|$ or $|r| \leq N^\delta$ for $\delta < \frac{3\alpha + \gamma - 2\sqrt{\gamma(3\alpha + \gamma)}}{3}$ then $(r, p - \lceil \sqrt{N} \rceil)$ or $(s, q - \lceil \sqrt{N} \rceil)$ are also common solutions of $g_1(x, y)$ and $g_2(x, y)$, therefore either $y_0 = p - \lceil \sqrt{N} \rceil$ or $y_0 = q - \lceil \sqrt{N} \rceil$ is a root of $g_1(x_0, y)$ for $x_0 = r$ or s , a solution for $h(x)$ and with this knowledge of y_0 the factorization of N is known.

Theorem 5. Let $N = pq$ be an RSA modulus with $q < p < 2q$. Let $e = N^\alpha$, $X = N^\delta$ and $Y = N^\gamma$, $N^\gamma = |\rho - 1|\sqrt{N}$ where ρ in the range $\begin{cases} 1 < \rho < \sqrt{2}, & \text{if } x_0 = r, y_0 = p - \lceil \sqrt{N} \rceil \\ \frac{1}{\sqrt{2}} < \rho < 1, & \text{if } x_0 = s, y_0 = q - \lceil \sqrt{N} \rceil, \end{cases}$ and r, s are the multiplicative inverses of $p - 1, q - 1$ modulo e respectively. Suppose that $|x_0| \leq X$ and $|y_0| \leq Y$ then one can factor N in polynomial time if

$$\delta < \frac{3\alpha + \gamma - 2\sqrt{\gamma(3\alpha + \gamma)}}{3}.$$

Proof. Follows from the above argument and the LLL lattice basis reduction algorithm operates in polynomial time [7]. □

Corollary 1. If the lattice basis reduction algorithm is implemented only using x -shifts and repeating the above argument then we can factorize N whenever

$$\delta < \frac{\alpha - \gamma}{2}.$$

Example 1. Consider the 500-bit integer primes p, q with $q < p < 2q$,

$p = 170012412412228374002637939365519830443328409208612957896658273619226759280$

9349109766540184651808314301773368255120142018434513091770786106657055179759 and

$q = 163669530394807093500659484841379957610832102302153239474164568404806689820$

2337277441635046162952078575443342063780035504608628272942696526664263794849.

Then $N = 2782585170079769062918329910316787739378614130731076762352269011625498885922423284650282977151279067225907184247826345726495657669$
 $9945593549454620693622688394500288852011908015225770521720915088650416587150349934694039019945761261530500516111094464262815422498738078576927$
 $5110281016352359905193261391$ and $\beta \approx 0.4952739$ where $N^\beta = p - q$, the prime difference.

For the public encryption exponent $e = 22101613613589688620342932117517577957632693197119684526565575704994787065215384269650224004$
 $7350805923053787316561846239648670193020219386541717336853,$

we have the private decryption exponent $d = 216201370580541988693840426730298193325865077817631810740453077605631407659496761063845$
 $8434785818513310159374909618692760679322173549277293291619261105938581620978897815237996653745248363714823777142661558419180059837734262872817$
 $60891038992603481181995446154263957587057164886397572862071123797744253.$

The multiplicative inverses of $p - 1$ and $q - 1$ modulo e are $r = 13$ and $s = 4968276086601860948375689811877277322092297400304711$
 $022160255819913121429929859233226176582706704776055610600183947453151776198378126007566405809480544$ respectively.

Now the solutions $x_0 = \min\{r, s\} = 13$ and $y_0 = p - \lceil \sqrt{N} \rceil = 3201586322319897015959134510540798302375082313137026615967102648045625402299655001412198712844034932966724165924$
 $456254022996550014121987128440349329667241659248764234628857989720083312382248332471.$

For $\gamma \approx 0.49429$, the RSA will be insecure if $\delta < 0.00473936615773426$ when we use both x -shifts and y -shifts and $\delta < 0.00472256612547278$ if we use only x -shifts. The solution $x_0 = 13 = N^{0.00370765164073960} < N^\delta$ for the both the cases. So for this x_0 we can find the factors p, q of N by using LLL algorithm in both the cases but note that for sufficiently large primes p and q , the Corollary 1 holds for any positive integer m .

For $m = 2$, $X = 15, Y = 3201586322319897015959134510540798302375082313137026615967102648045625402299655001412198712844034932966724165924$
 $8764234628857989720083312382248332471,$ the upper bounds for x_0 and y_0 respectively and

$A = 166810826089908476986678804854979032140953326895475931280691170971181133878635255975241819752336796497210612659587137778380565510205070279$
 $4274806847287,$ apply LLL algorithm to the matrix M formed by the row vectors $[e^2, 0, 0, 0, 0, 0], [0, Xe^2, 0, 0, 0, 0],$
 $[-e, XAe, XYe, 0, 0, 0], [0, 0, 0, X^2e^2, 0, 0], [0, -Xe, 0, X^2ae, X^2Ye, 0], [1, -2AX, -2XY, A^2X^2, 2AX^2Y, X^2Y^2].$

Let $b_1 = [i_0, i_1, i_2, i_3, i_4, i_5]$ and $b_2 = [j_0, j_1, j_2, j_3, j_4, j_5]$ be the first two short vectors and $g_1(x, y) = c_0 + c_1x + c_2xy + c_3x^2 + c_4x^2y + c_5x^2y^2$ and $g_2(x, y) = d_0 + d_1x + d_2xy + d_3x^2 + d_4x^2y + d_5x^2y^2$ be two polynomials where $c_0 = \frac{i_0}{1}, c_1 = \frac{i_1}{X}, c_2 = \frac{i_2}{XY}, c_3 = \frac{i_3}{X^2}, c_4 = \frac{i_4}{X^2Y}, c_5 = \frac{i_5}{X^2Y^2}$ and $d_0 = \frac{j_0}{1}, d_1 = \frac{j_1}{X}, d_2 = \frac{j_2}{XY}, d_3 = \frac{j_3}{X^2}, d_4 = \frac{j_4}{X^2Y}, d_5 = \frac{j_5}{X^2Y^2}$. If $h(x) = \text{res}(g_1(x, y), g_2(x, y))$, then for the solution $x = x_0 = 13$ of $h(x)$ we have $y = y_0 = p - \lceil \sqrt{N} \rceil$ is a solution for $g_1(13, y)$ and with the knowledge of y_0 we can find the prime factors p and q .

Note that this RSA attack does not depend on the private decryption exponent d . Sometimes our attack may work if d is exceeding the bound given by Boneh and Durfee. For a given $e = N^\alpha$ and for $d = N^{\delta'}, p - q = N^\beta$, the prime difference, the Boneh-Durfee's bound for δ' (in the first result) is given by $\delta' < \frac{5}{6} + \frac{2}{3}\beta - \frac{1}{3}\sqrt{8(3\alpha - 1)\beta + 16\beta^2 - 6\alpha + 1}$. Therefore the Boneh-Durfee's bound for $d = N^{\delta'}$ for a given α, β in example 1 is such that $\delta' < 0.5029$ but note that in this example $d = N^{\delta'} \approx N^{0.996307}$ exceeding the bound given by Boneh and Durfee.

3.1 Refined Attack Bound Using Sub-Lattice Based Techniques

Boneh and Durfee [2] improved their result by using sub-lattice techniques. Now we implement their idea to our polynomial for improving the result.

Let M_y be the portion of the matrix M with rows corresponding to the y -shifts $h_{l,k}$ and columns corresponding to variable of the form $x^u y^v, v > u$ and take the parameter t as twice the value of t in the above lattice based technique i.e., $t = \frac{\alpha - \delta - \gamma}{\gamma} m$.

Define the matrix M_1 as follows: Take every row $g_{i,k}$ of M corresponding to the x -shifts and take only those rows $h_{l,k}$ of M corresponding to the y -shifts whose diagonal entry is less than or equal to e^m . Let \mathcal{L}_1 be a lattice described by M_1 . Then \mathcal{L}_1 is a sublattice of \mathcal{L} , so short vector of \mathcal{L}_1 will be in \mathcal{L} . Now perform the Gaussian elimination to the first $(m+1)(m+2)/2$ rows of M that is the those rows corresponding to the x shifts to set the off-diagonal entries of every row to zero, then there is a unitary matrix A over \mathbb{R} such that $M_2 = AM_1$ is a matrix whose upper left block Δ is a diagonal matrix of order $(m+1)(m+2)/2$, lower right block M'_y consists selected rows of M_y and remaining upper right block and lower left block of M_2 are zero blocks. Since A is unitary, the determinant of the lattice \mathcal{L}_2 described by M_2 is equal to $\det(\mathcal{L}_1)$ and the $\det(\mathcal{L}_2) = \det(\Delta) \cdot \det(\mathcal{L}'_y)$ where \mathcal{L}'_y be the lattice induced by M'_y .

Let w' be the dimension of \mathcal{L}'_y . First we compute w' by setting $S = \{(k, l) \in \{0, \dots, m\} \times \{1, \dots, t\} | M(k, l, k, l) \leq e^m\}$ and then $w' = |S|$. The matrix M_y is a geometrically progressive matrix with parameter choice $(m^{2m}, N, \alpha m, \delta + \gamma, \gamma - 1, -\alpha, 1, b)$ for some b . Note that the first three conditions of Definition 1 hold. To satisfy the fourth condition, the parameter b should satisfy $b(\delta + \gamma) - \alpha \geq 0$ and $b(\gamma - 1) + 1 \geq 0$ together and thus we get the constraint $\delta > \alpha - \gamma(1 + \alpha)$, which in turn gives a possible value of b as $b = \frac{1}{1 - \gamma}$. We have $M_y(k, l, k, l) = N^{\alpha m + (\delta - \alpha + \gamma)k + \gamma l}$ for $k = 0, \dots, m$ and $l = 1, \dots, t$. Since $(k, l) \in S$ only if $N^{\alpha m + (\delta - \alpha + \gamma)k + \gamma l} < N^{\alpha m}$, so for $l \leq \frac{\alpha - \delta - \gamma}{\gamma} k$ we get this inequality. Thus

$$w' = |S| = \sum_{k=0}^m \lfloor \frac{\alpha - \delta - \gamma}{\gamma} k \rfloor = \frac{\alpha - \delta - \gamma}{2\gamma} m^2 + o(m^2)$$

and the dimension of the lattice \mathcal{L}_2 is

$$w = \frac{(m+1)(m+2)}{2} + w' = \left(\frac{1}{2} + \frac{\alpha - \delta - \gamma}{2\gamma} \right) m^2 + o(m^2).$$

Since the lattice \mathcal{L}'_y defined by the rows $(k, l) \in S$ of M_y and by theorem 4 we have

$$\det \mathcal{L}'_y \leq \left((m+1) \lfloor \frac{\alpha - \delta - \gamma}{\gamma} m \rfloor \right)^{\frac{w'}{2}} (1 + m^{2m})^{(w')^2} \prod_{(k,l) \in S} M_y(k, l, k, l).$$

As $\left((m+1) \lfloor \frac{\alpha - \delta - \gamma}{\gamma} m \rfloor \right)^{\frac{w'}{2}} (1 + m^{2m})^{(w')^2}$ is a function of only δ (but not of N) and $\prod_{(k,l) \in S} M_y(k, l, k, l) =$

$$\prod_{k=0}^m \prod_{l=0}^{\lfloor \frac{\alpha - \delta - \gamma}{\gamma} k \rfloor} N^{\alpha m + (\delta - \alpha + \gamma)k + \gamma l}, \text{ we have}$$

$$\det \mathcal{L}'_y = N^{\left(\frac{2\alpha^2 - \alpha\gamma - \gamma^2 - (\alpha + 2\gamma)\delta - \delta^2}{6\gamma} \right) m^3 + o(m^3)}.$$

Now as $\det(\Delta) = e^{n_e X^{n_x} Y^{n_y}}$ pertaining to just x -shifts, repeating the argument as in the above lattice based strategy we have $\det(\Delta) = N^{\left(\frac{2\alpha + 2\delta + \gamma}{6} \right) m^3 + o(m^2)}$, so then the condition $\det(\mathcal{L}_1) = \det(\Delta) \cdot \det(\mathcal{L}'_y) < e^{mw}$ gives the bound

$$\delta < \alpha - \sqrt{\alpha\gamma}.$$

Theorem 6. Let $N, p, q, e, X, Y, x_0, y_0, \delta, \gamma$ and ρ be defined in Theorem 5. Suppose that $|x_0| \leq X$ and $|y_0| \leq Y$, then RSA is insecure if

$$\alpha - \gamma(1 + \alpha) < \delta < \alpha - \sqrt{\alpha\gamma}.$$

Proof. Follows from the above argument and the LLL lattice basis reduction algorithm operates in polynomial time [7]. □

Now we follow the idea of Blömer-May in [3] using sub-lattice techniques and this approach does not improve the above bound for δ and also slightly less than to this bound but this method requires lattice of smaller dimension than the above approach.

Theorem 7. Let $N, p, q, e, X, Y, x_0, y_0, \delta, \gamma$ and ρ be defined in Theorem 5. Suppose that $|x_0| \leq X$ and $|y_0| \leq Y$, then RSA is insecure if

$$\delta < \frac{2\alpha - 6\gamma + 2\sqrt{\alpha^2 - \alpha\gamma + 4\gamma^2}}{5}.$$

Proof. This proof is similar to the above argument but determinant of lattice will be different here.

Unlike the above remove the some rows corresponding to the both x -shifts and y -shifts of M in order to obtain a square matrix and to apply Howgrave’s theorem by following the same idea of Blömer-May in [3] and denote the final constructed matrix by M_B and corresponding lattice \mathcal{L}_B .

So the new lattice M_B formed by removing the row vectors corresponding to the x -shift polynomials $g_{i,k}(xX, yY)$

$$\text{if } i + k = 0, 1, \dots, m - t - 1, \text{ the } y\text{-shift polynomials } h_{j,k}(xX, yY) \text{ if } k = \begin{cases} 0, \dots, m - t & \text{if } j = 1 \\ 0, \dots, m - t + 1 & \text{if } j = 2 \\ \vdots \\ 0, \dots, m - 2 & \text{if } j = t - 1 \\ 0, \dots, m - 1 & \text{if } j = t \end{cases} \text{ and}$$

remove columns in order to form a lower triangular square matrix .

Then the dimension of the lattice $\mathcal{L}_B = (m + 1)(t + 1)$ and the diagonal elements of the matrix M_B will be

$$\begin{aligned} & X^m e^m, X^m Y e^{m-1}, \dots, X^m Y^m, \\ & X^{m-1} e^m, X^{m-1} Y e^{m-1}, \dots, X^{m-1} Y^{m-1} e, \\ & \dots, \\ & X^{m-t} e^m, X^{m-t} Y e^{m-1}, \dots, X^{m-t} Y^{m-t} e^t \text{ (for } x\text{-shifts) and} \\ & X^m Y^{m+t}, \\ & X^m Y^{m+t-1}, X^{m-1} Y^{m+t-2} e, \\ & \dots, \\ & X^m Y^{m+1}, X^{m-1} Y^m e, \dots, X^{m-t+1} Y^{m-t+2} e^{t-1} \text{ (for } y\text{-shifts).} \end{aligned}$$

Multiplying the diagonal elements and neglecting the lower order terms, we need the condition

$$X^{tm^2 - \frac{mt^2}{2} + \frac{t^3}{6}} Y^{\frac{tm^2}{2} + \frac{t^3}{6}} < e^{\frac{tm^2}{2}}.$$

Putting the values of $e = N^\alpha$, $X = N^\delta$, $Y = N^\gamma$ and $t = \tau m$, we have the required condition

$$\left(\frac{\delta}{6} + \frac{\gamma}{6}\right) \tau^2 - \frac{1}{2} \delta \tau + \left(\delta + \frac{\gamma}{2} - \frac{\alpha}{2}\right) < 0.$$

The left hand side is minimized at the value $\tau = \frac{\delta}{\frac{2}{3}(\delta + \gamma)}$. Putting this value of τ in the previous inequality we get the bound for δ is

$$\delta < \frac{2\alpha - 6\gamma + 2\sqrt{\alpha^2 - \alpha\gamma + 4\gamma^2}}{5}.$$

□

3.2 Analysis of Attack Bounds

As it is known that, for $p - q < N^{\frac{1}{4}}$, then RSA is insecure by Fermat’s Factorization technique, in this section we first analyze all the above attack bounds on δ in the range $N^{\frac{1}{4}} < p - q < \frac{N^{\frac{1}{2}}}{\sqrt{2}}$. We proceed by denoting the δ obtaining using both x and y shifts as in Theorem(5) by $\delta_{x,y}$, the δ obtaining using only x -shifts as in Corollary(1) by δ_x , the δ obtaining using sublattice based techniques as in Theorem(6) by δ_s and the δ obtaining using sublattice based techniques with lower dimension as in Theorem(7) by δ_{s_d} . Let $p - q = N^\beta$ for $\frac{1}{4} < \beta < \frac{1}{2}$, then we have $p - \lceil \sqrt{N} \rceil, \lceil \sqrt{N} \rceil - q < N^\beta$ as $q < \lceil \sqrt{N} \rceil < p$. As $y_0 = q - \lceil \sqrt{N} \rceil$ or $p - \lceil \sqrt{N} \rceil$, we may take $Y = N^\beta$, $\frac{1}{4} < \beta < \frac{1}{2}$ and for $Y = N^\beta$ the attack bound for δ in the above results are given as:

$$\delta_x < \frac{\alpha - \beta}{2} \text{ for any } m \geq 1. \tag{3}$$

$$\delta_{x,y} < \frac{3\alpha + \beta - 2\sqrt{\beta(3\alpha + \beta)}}{3} \text{ for } t = \frac{\alpha - \delta - \beta}{2\beta} m. \tag{4}$$

$$\alpha - \beta(1 + \alpha) < \delta_s < \alpha - \sqrt{\alpha\beta} \text{ for } t = \frac{\alpha - \delta - \beta}{\beta} m. \tag{5}$$

$$\delta_{s_d} < \frac{2\alpha - 6\beta + 2\sqrt{\alpha^2 - \alpha\beta + 4\beta^2}}{5} \text{ for } t = \frac{\delta}{\frac{2}{3}(\delta + \beta)} m. \tag{6}$$

In Table 1, we represent how the bound for δ increase when the prime difference N^β is decreasing from $N^{\frac{1}{2}}$ to $N^{\frac{1}{4}}$ for a given public key exponent $e = N^\alpha$ in the all above cases (3),(4),(5) and (6).

α	β	δ			
		δ_x	$\delta_{x,y}$	δ_s	δ_{s_d}
0.501	≈ 0.50	0.0005	0.0005001873	(0, 0.0005002497)	0.0005001874
	0.45	0.0255	0.0260200003	(0, 0.0261842462)	0.0260339152
	0.40	0.0505	0.0526881570	(0, 0.0533394142)	0.0528096268
	0.35	0.0755	0.0807826527	(0, 0.0822518656)	0.0812390932
	0.30	0.1005	0.1106939731	(0.0570000001, 0.1133145605)	0.1118998342
	0.26	0.1205	0.1363082232	(0.1174, 0.1400844974)	0.1385650655
0.55	≈ 0.50	0.025	0.0254519548	(0, 0.0255955759)	0.0254626986
	0.45	0.05	0.0519259301	(0, 0.0525062814)	0.0520215047
	0.40	0.075	0.0796409907	(0, 0.0809584240)	0.0800000000
	0.35	0.1	0.1088933156	(0.0075000001, 0.1112517806)	0.1098386676
	0.30	0.125	0.1400980486	(0.0850000001, 0.1437980797)	0.1421347195
	0.26	0.145	0.1668676552	(0.147, 0.1718465919)	0.1702670394
0.75	≈ 0.50	0.125	0.1349307066	(0, 0.1376275643)	0.1358898943
	0.45	0.15	0.1651530771	(0, 0.1690524980)	0.1669397989
	0.40	0.175	0.1969579906	(0.0499999999, 0.2022774424)	0.2
	0.35	0.2	0.2307071990	(0.1375, 0.2376524617)	0.2355277766
	0.30	0.225	0.2669048105	(0.225, 0.2756583509)	0.2740658617
	0.26	0.245	0.2981089219	(0.295, 0.3084119566)	0.3074745686
1	≈ 0.50	0.25	0.2847495629	(0, 0.2928932188)	0.2898979485
	0.45	0.275	0.3193376137	(0.1, 0.3291796067)	0.3264761515
	0.40	0.3	0.3558730806	(0.2, 0.3675444679)	0.3654211490
	0.35	0.325	0.3947864057	(0.3, 0.4083920216)	0.4070831300
	0.30	0.35	0.4366750419	(0.4, 0.4522774424)	0.4518252056
	0.26	0.37	0.4728987047	(0.48, 0.4900980486)	0.4900746199

Table 1: Bound for δ corresponding to the values of α and β in all cases.

In Figure 1 we plot the bounds for δ_s , δ_{s_d} , $\delta_{x,y}$ and δ_x for a given e in different values of β i.e., $\beta = 0.5, 0.45, 0.35$ and 0.26 . Within that bounds the RSA cryptosystem is insecure and note that the region for which RSA is insecure increases when the value of β decreases.

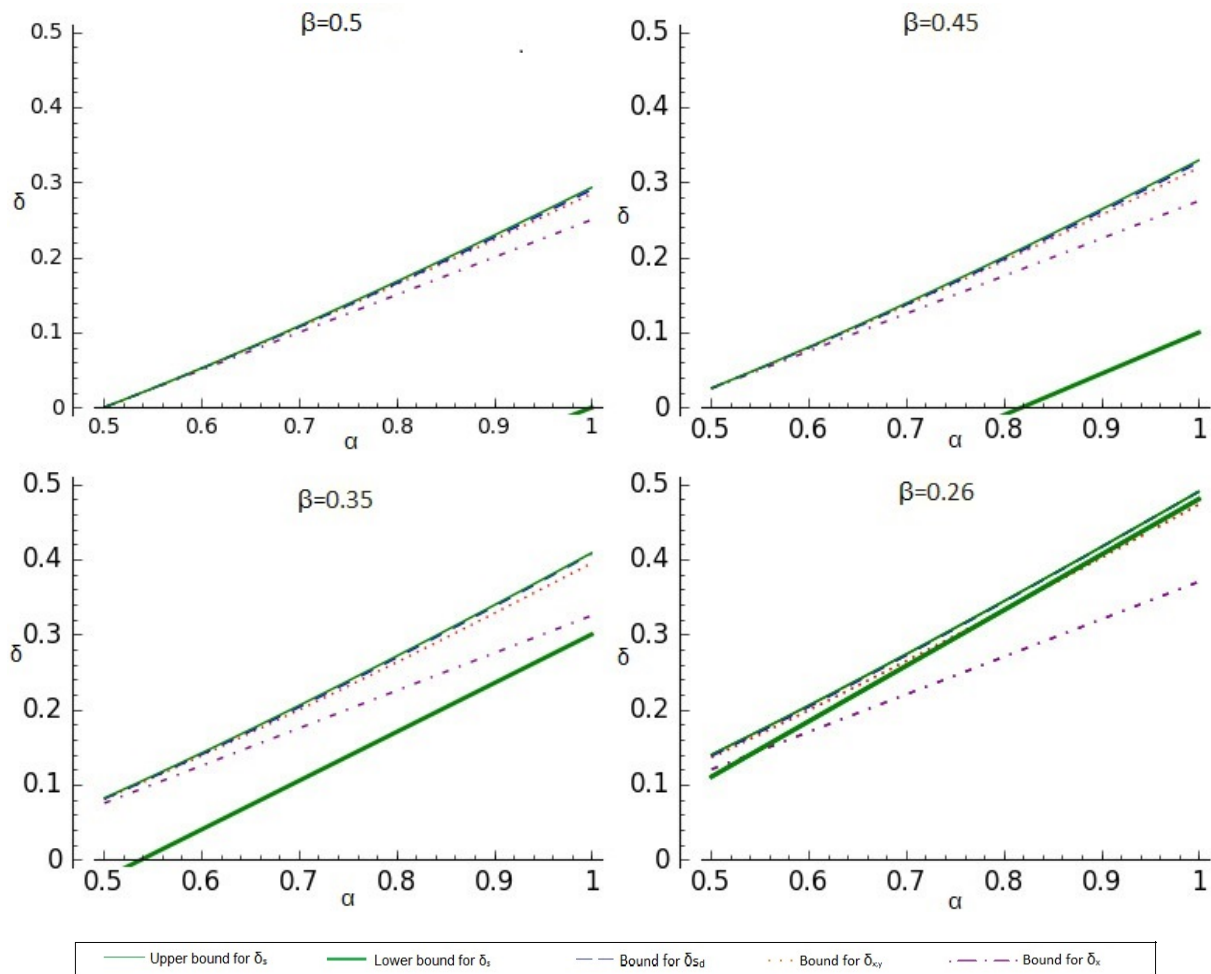


Fig.1. The region for δ and α values for which RSA is insecure for different values of β .

From the above observations it is noted for a given α if δ is beyond the upper bound δ_s then the RSA is secure with respect to all the above attacks and if δ is within the bound for δ_x and beyond the lower bound for δ_s then RSA is insecure with respect to all the the above attacks and for any δ within any of the four attack bounds corresponding attack may be implemented. Further it is also observed that δ always lies beyond the attack bounds for certain values of the public encryption exponent e and such inefficient lower bound of e for each attack related to the prime difference are listed in Table 2 for $e = N^\alpha$ and $L(\alpha)$, denoting the lower bound for inefficient e for the above attacks using lattice based techniques.

N	β (\approx)	$L(\alpha)$			
		Attack with x -shifts	Attack with x and y shifts	Attack with sublattice based techniques	Attack with sublattice based techniques with lower dimension
1000 bits	0.50	0.5025	0.5025	0.5025	0.5025
	0.45	0.5520	0.5560	0.5600	0.5570
	0.35	0.66	0.71	0.72	0.7130
	0.26	0.75	0.9120	0.9675	0.9670
2000 bits	0.50	0.5013	0.5013	0.5013	0.5013
	0.45	0.5510	0.5550	0.5590	0.5560
	0.35	0.6520	0.70	0.72	0.71
	0.26	0.7450	0.91	0.9645	0.9640
4000 bits	0.50	0.5010	0.5010	0.5010	0.5010
	0.45	0.5505	0.5545	0.5570	0.5550
	0.35	0.6510	0.6990	0.7160	0.7095
	0.26	0.7410	0.9090	0.9640	0.9435

Table 2: List of $L(\alpha)$ corresponding to β and no.of bits in N .

In such cases we proceed to improve the attack bounds for δ so that the inefficient e may turn efficient for the attacks with lattice based techniques by considering the same polynomial congruence with N replaced by ρN or $\frac{N}{\rho}$ for some appropriate ρ , $1 \leq \rho \leq 2$ such that $\rho q \approx p$ and is based on the following Theorem.

Theorem 8. Let $|p - \rho q| \leq N^{\gamma'}$ where $\gamma' < \frac{1}{2}$ and $1 \leq \rho \leq 2$. Then we have $|p - \sqrt{\rho N}|, |q - \sqrt{\frac{N}{\rho}}| < N^{\gamma'}$ [12].

To improve the bound for δ , we consider the polynomial congruence $f(x, y) \equiv 0 \pmod e$ in which the upper bound $N^{\gamma'}$ for the solution $y = y_0$ is depending on the value $|p - \rho q|$, rather than the prime difference $p - q$ for $f(x, y) = x(y + A) - 1$, with $A = \begin{cases} \lceil \sqrt{\rho N} \rceil - 1, & \text{if } \min\{r, s\} = r \\ \lceil \sqrt{\frac{N}{\rho}} \rceil - 1, & \text{if } \min\{r, s\} = s. \end{cases}$

Then the solutions $x = x_0$ and $y = y_0$ for the polynomial congruence $f(x, y) \equiv x(y + A) - 1 \pmod e$ are given as $x_0 = \min\{r, s\}$ and $y_0 = \begin{cases} p - \lceil \sqrt{\rho N} \rceil, & \text{if } \min\{r, s\} = r \\ q - \lceil \sqrt{\frac{N}{\rho}} \rceil, & \text{if } \min\{r, s\} = s. \end{cases}$

In [13], it has been studied how a few MSBs of p or q can be found from the knowledge of N only, where $N = pq$, p and q are primes of same size and this knowledge of most significant bits(MSBs) of p or q can provide approximation of ρ . Otherwise one may try to guess ρ for different values (that are computationally feasible) to mount the attack. To mount the attack we establish the attack bounds for δ by repeating the argument for $|x_0| \leq N^\delta$ and $|y_0| \leq N^{\gamma'}$, $\gamma' \leq \frac{1}{2}$ in Corollary 1, Theorem 5, Theorem 6 and Theorem 7. Note for the above attack bounds thus obtained depending on appropriate ρ .

Example 2. Let $p=202578011750906281247094079898482654152352800202967795174672010161491336804628653$
 $58574779284875457806030124268550700030014115264772567435253175260469958709084217$ and
 $q=106620006184687516445838989420254028501238315896298839565616847453416493055067712$
 $41355146992039714634752696983447736857902165928827667136006663483150507256156183$

be two 533 and 532 bit integer primes respectively with $q < p < 2q$.

Then $N=2159886886576332808881372615452289600419716598304132287130238304022057943598518945824934738913551301466581746670813928474835987795$
 $788053774051346057802186135547718470805647762369215305969765030566801742108218670157518254139618999751340345127999866829966392864624231228730005$
 $5328685941416182541762052991358334639452263711.$

For the public encryption exponent $e=20357048760851917713038785834633594998268127430246505631122228265727831120341504227605379168525$
 $574184831255713809622106188803980126100142376033417564441502906816081028618399597927513832190649042334179538898854354716330533894180986228498033$
 $0799683718466882334422884965338353654061812322328244014873765,$ the multiplicative inverses of $p - 1$ and $q - 1$ modulo e are
 $r=15863205922290019006404019782584099034358123662465732469953170767501769225883755689521518192482725595496589763798408382380531132272292363326$
 $28732137867246713845703554488416968391320841470705716962245803211633386377136888776619499115430592596931321075625958870066127685434042170604888$
 $47920706636452261,$

$S=74582364574556004740075744770000572387674657365757152371643759617457164738561374658743675673265713649576184735671436756173564375674365716349$
 705193 respectively and $e \approx N^{0.937484971166478}$.

Taking $\rho = 1.9$, we get $|p - \rho q| = N^{0.0814475914542542436619469358}$. For $\gamma' \approx 0.082$, the bound for δ corresponds to the results given in Corollary 1 and Theorems 5 & 7 are 0.428018689856112, 0.640973585517601

and 0.641467151800484 respectively and note the solution $x = x_0 = s \approx N^{0.455376075838353}$ is exceeding the bound given in Corollary 1 (The method given in the Theorem 6 is not applicable in this case as we have $\alpha - \gamma(1 + \alpha) < \alpha - \sqrt{\alpha\gamma}$ only if $\sqrt{\gamma} \frac{1+\sqrt{\alpha}}{\sqrt{\alpha}} > 1$, but in this case $\sqrt{\gamma} \frac{1+\sqrt{\alpha}}{\sqrt{\alpha}} < 1$). By using the lattice parameters $m = 3$ and $t = 1$ we can factor the RSA modulus N in both cases corresponding to the Theorems 5 & 7. If $|y_0| = |q - \lceil \sqrt{\frac{N}{\rho}} \rceil|$, then for the polynomial congruence $x(y + A) - 1 \equiv 1 \pmod{e}$, where $A = \lceil \sqrt{\frac{N}{\rho}} \rceil - 1$ and for $\beta \approx 0.49942206$, the solution $x = x_0$ is exceeding the bound given in (3),(4),(5) and (6).

4 Conclusion

In this paper it is shown that RSA is insecure if the multiplicative inverse of $p - 1$ or $q - 1$ modulo the public encryption exponent e is small, that is less than or equal to N^δ , for some small δ . This is established by using the lattice based techniques implemented by the polynomial congruence $f(x, y) \equiv 0 \pmod{e}$ for $f(x, y) = x(y + A) - 1$ with $A = \lceil \sqrt{N} \rceil - 1$. Lattice based techniques were implemented first using both x and y shifts then implemented using only x -shifts. These were also implemented using sublattice based techniques and sublattice based techniques with lower dimension and in each of the above four implementation for δ denoted as $\delta_{x,y}$, δ_x , δ_s and δ_{s_d} respectively, the attack bounds were described. An analysis of these bounds with respect to the prime difference $p - q$, for $p - q = N^\beta$ and with respect to $p - \rho q$, for ρ such that ρq is a better approximation for p are also described.

References

- [1] Boneh, D. "Twenty Years of Attacks on the RSA Cryptosystem", <http://www.ams.org/notices/199902/boneh.pdf>.
- [2] Boneh, D., Durfee, G. "Cryptanalysis of RSA with private key d less than $N^{0.292}$ ", Advances in Cryptology Eurocrypt99, Lecture Notes in Computer Science Vol.1592, Springer-Verlag, pp. 111 (1999).
- [3] J. Blomer, A. May, "Low Secret Exponent RSA Revisited", Cryptography and Lattice Conference (CaLC 2001), Lecture Notes in Computer Science Volume 2146, Springer-Verlag, pp. 419, 2001.
- [4] D. Burton, "Elementary Number Theory", Sixth edition, Mc Graw Hill, New York, 2007.
- [5] Coppersmith, D. "Small solutions to polynomial equations, and low exponent RSA vulnerabilities". Journal of Cryptology, 10(4), pp. 233260 (1997).
- [6] Howgrave-Graham, N. "Finding small roots of univariate modular equations revisited", In Cryptography and Coding, LNCS 1355, pp. 131142, Springer-Verlag (1997).
- [7] Lenstra, A.K., Lenstra, H.W., Lovasz, L. "Factoring polynomials with rational coefficients, Mathematische Annalen", Vol. 261, pp. 513534, 1982.
- [8] Neal Koblitz, "A Course in Number Theory and Cryptography" ISBN 3-578071-8, SPIN 10893308.
- [9] Nitaj, A.: Another generalization of Wiener's attack on RSA, In: Vaudenay, S. (ed.) Africacrypt 2008. LNCS, vol. 5023, pp. 174190. Springer, Heidelberg (2008).
- [10] K. H. Rosen, "Elementary Number Theory and Its Applications", Addison-Wesley, Reading Mass, 1984.
- [11] Subhamoy Maitra and Santanu Sarkar, "RSA Cryptanalysis with Increased Bounds on the Secret Exponent using Less Lattice Dimension", Cryptology ePrint Archive: Report 2008/315, Available at <http://eprint.iacr.org/2008/315>.
- [12] Subhamoy Maitra and Santanu Sarkar, "Reviving Wiener's Attack - New Weak Keys in RSA", <http://eprint.iacr.org/2005/228.pdf>.
- [13] H. -M. Sun, M. -E. Wu and Y. -H. Chen. "Estimating the prime-factors of an RSA modulus and an extension of the Wiener attack". ACNS 2007, LNCS 4521, pp. 116128, 2007.
- [14] B. de Weger, "Cryptanalysis of RSA with Small Prime Difference", Applicable Algebra in Engineering, Communication and Computing, 13(1);17-28,2002.
- [15] M. Wiener, "Cryptanalysis of Short RSA Secret Exponents", IEEE Transactions on Information Theory, 36(3)-553-558, 1990.



Article

An Attack Bound for Small Multiplicative Inverse of $\varphi(N) \bmod e$ with a Composed Prime Sum $p + q$ Using Sublattice Based Techniques

P. Anuradha Kameswari * and L. Jyotsna

Department of Mathematics, Andhra University, Visakhapatnam, Andhra Pradesh 530003, India; jyotsna.jahnavi@gmail.com

* Correspondence: panuradhakameswari@yahoo.in; Tel.: +91-986-681-5530

Received: 18 July 2018; Accepted: 11 November 2018; Published: date



Abstract: In this paper, we gave an attack on RSA Cryptosystem when $\varphi(N)$ has small multiplicative inverse modulo e and the prime sum $p + q$ is of the form $p + q = 2^n k_0 + k_1$, where n is a given positive integer and k_0 and k_1 are two suitably small unknown integers using sublattice reduction techniques and Coppersmith's methods for finding small roots of modular polynomial equations. When we compare this method with an approach using lattice based techniques, this procedure slightly improves the bound and reduces the lattice dimension. Employing the previous tools, we provide a new attack bound for the deciphering exponent when the prime sum $p + q = 2^n k_0 + k_1$ and performed an analysis with Boneh and Durfee's deciphering exponent bound for appropriately small k_0 and k_1 .

Keywords: RSA; Cryptanalysis; lattices; LLL algorithm; Coppersmith's method

JEL Classification: 11T71; 94A60

1. Introduction

RSA Cryptosystem [1] is the first public key cryptosystem invented by Ronald Rivest, Adi Shamir and Leonard Adleman in 1977. The primary parameters in RSA are the modulus $N = pq$, which is the product of two large distinct primes, a public exponent e such that $\gcd(e, \varphi(N)) = 1$ and a private exponent d , the multiplicative inverse of e modulo $\varphi(N)$. In this system the encryption and decryption are based on the fact that for any message m in Z_N , $m^{ed} = m \bmod N$. The security of this system depends on the difficulty of finding factors of a composite positive integer, which is a product of two large primes. In 1990, M.J.Wiener [2] was the first one to describe a cryptanalytic attack on the use of short RSA deciphering exponent d . This attack is based on continued fraction algorithm which finds the fraction $\frac{t}{d}$, where $t = \frac{ed-1}{\varphi(n)}$ in a polynomial time when d is less than $N^{0.25}$ for $N = pq$ and $q < p < 2q$. Using lattice reduction approach based on the Coppersmith techniques [3] for finding small solutions of modular bivariate integer polynomial equations, D. Boneh and G. Durfee [4] improved the wiener result from $N^{0.25}$ to $N^{0.292}$ in 2000 and J. Blömer and A. May [5] has given an RSA attack for d less than $N^{0.29}$ in 2001, which requires lattices of dimension smaller than the approach by Boneh and Durfee. In 2006, E. Jochemsz and A. May [6], described a strategy for finding small modular and integer roots of multivariate polynomial using lattice-based Coppersmith techniques and by implementing this strategy they gave a new attack on an RSA variant called common prime RSA.

In the paper [7], first we described an attack on RSA when $\varphi(N)$ has small multiplicative inverse k of modulo e , the public encryption exponent by using lattice and sublattice based techniques. Let $N = pq$, $q < p < 2q$, $p - q = N^\beta$ and $e = N^\alpha > p + q$. As $(e, \varphi(N)) = 1$, there exist unique r, s such that

$(p - 1)r \equiv 1 \pmod{e}$ and $(q - 1)s \equiv 1 \pmod{e}$. For $k = rs \pmod{e}$, $k\varphi(N) \equiv 1 \pmod{e}$ and define $g(x, y) = x(y + B) - 1$ where $B = N + 1 - \lfloor 2\sqrt{N} \rfloor$. Then the pair $(x_0, y_0) = (k, -((p + q) - \lfloor 2\sqrt{N} \rfloor))$ is a solution for the modular polynomial equation $g(x, y) \equiv 0 \pmod{e}$. Now applying the lattice based techniques given by Boneh-Durfee in [4] using x, y shifts and using only x shifts to the above modular polynomial equation, we get the attack bounds for δ , $|k| \leq N^\delta$ are $\delta < \frac{3\alpha + \beta - 2\sqrt{\beta(3\alpha + \beta)}}{3}$ and $\delta < \frac{\alpha - \beta}{2}$, respectively. Also, we improved the bound for δ up to $\alpha - \sqrt{\alpha\beta}$ by implementing the sublattice based techniques given by Boneh and Durfee in [4] under the condition $\delta > \alpha - \beta(1 + \alpha)$ and improved the bound for δ up to $\delta < \frac{2\alpha - 6\beta + 2\sqrt{\alpha^2 - \alpha\beta + 4\beta^2}}{5}$ by implementing the sublattice based techniques with lower dimension given by J. Blömer and A. May in [5]; this bound is slightly less than the above bound but this method requires lattices of smaller dimension than the above method. All these attack bounds are depending on the prime difference $p - q = N^\beta$ and $\alpha - \sqrt{\alpha\beta}$ is the maximum upper bound for δ .

Later in paper [7], we described that, for $\beta \approx 0.5$, the maximum bound for δ may be improved if the prime sum $p + q$ is in the form of the composed sum $p + q = 2^n k_0 + k_1$ where n is a given positive integer and k_0 and k_1 are two suitably small unknown integers. Define the polynomial congruence $f(x, y, z) \equiv 0 \pmod{e}$ for

$$f(x, y, z) = \begin{cases} (N + 1)x + xy + (2^n)xz - 1 & \text{if } |k_0| \leq |k_1| \\ 2^{n'}x(N + 1) + xy + 2^{n'}xz - 2^{n'} & \text{if } |k_1| \leq |k_0| \end{cases}$$

where $2^{n'}$ is an inverse of $2^n \pmod{e}$. By using lattice based techniques to the above polynomial congruence, the attack bound for δ is such that $\delta < \frac{1}{2}\alpha - \frac{1}{2}\gamma_1 + \frac{1}{16}\gamma_2 - \frac{1}{16}\sqrt{48(\alpha - \gamma_1)\gamma_2 + 33\gamma_2^2}$ where $N^{\gamma_1}, N^{\gamma_2}$ are the upper bounds for $\max\{|k_0|, |k_1|\}$, $\min\{|k_0|, |k_1|\}$ respectively.

Now, in this paper, we slightly improved the above bound by using the sub-lattice based techniques given by J. Blömer, A. May in [5] to the above polynomial congruence and this method requires lattice of smaller dimension than the above method. The new bound on δ is $\frac{1}{2}\alpha - \frac{1}{2}\gamma_1 - \frac{1}{6}\sqrt{6(\alpha - \gamma_1)\gamma_2 + 3\gamma_2^2}$ and showed that this is a little bit greater than the former bound graphically. Note that this new attack bound is also an attack bound for the deciphering exponent d .

2. Preliminaries

In this section we state basic results on lattices, lattice basis reduction, Coppersmith’s method and Howgrave-Graham theorem that are based on lattice reduction techniques.

Definition 1. Let $\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_n \in \mathbb{R}^m$ be a set of linearly independent vectors. The lattice L generated by $\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_n$ is the set of linear combinations of $\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_n$ with coefficients in \mathbb{Z} .

A basis for L is any set of independent vectors that generates L . The dimension of L is the number of vectors in a basis for L .

Definition 2. Let L be a lattice of dimension n and let $\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_n$ be a basis for L . The fundamental domain for L corresponding to this basis is the set

$$\mathcal{F}(\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_n) = \{t_1\mathbf{b}_1 + t_2\mathbf{b}_2 + \dots + t_n\mathbf{b}_n : 0 \leq t_i < 1\} \quad [8].$$

Definition 3. Let L be a lattice of dimension n and let \mathcal{F} be a fundamental domain for L . Then the n -dimensional volume of \mathcal{F} is called the determinant of L . It is denoted by $\det(L)$ [8].

Remark 1. If L is a full rank lattice, which means $n = m$ then the determinant of L is equal to the absolute value of the determinant of the $n \times n$ matrix whose rows are the basis vectors $\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_n$.

In 1982, A. K. Lenstra, H. W. Lenstra, Jr. and L. Lovasz [9] invented the LLL lattice based reduction algorithm to reduce a basis and to solve the shortest vector problem. The general result on the size of individual LLL-reduced basis vectors is given in the following Theorem.

Theorem 1. *Let L be a lattice and $\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_n$ be an LLL-reduction basis of L . Then*

$$\|\mathbf{b}_1\| \leq \|\mathbf{b}_2\| \leq \dots \leq \|\mathbf{b}_i\| \leq 2^{\frac{n(n-1)}{4(n+1-i)}} \det(L)^{\frac{1}{n+1-i}}$$

for all $1 \leq i \leq n$ [10].

An important application of lattice reduction found by Coppersmith in 1996 [3] is finding small roots of low-degree polynomial equations. This includes modular univariate polynomial equations and bivariate integer equations. In 1997 Howgrave-Graham [11] reformulated Coppersmith’s techniques and proposed a result which shows that if the coefficients of $h(x, y)$ are sufficiently small, then the equality $h(x_0, y_0) = 0$ holds not only modulo N , but also over integers. The generalization of Howgrave-Graham result in terms of the Euclidean norm of a polynomial $h(x_1, x_2, \dots, x_n) = \sum a_{i_1 \dots i_n} x_1^{i_1} \dots x_n^{i_n}$ is defined by the Euclidean norm of its coefficient vector i.e., $\|h(x_1, x_2, \dots, x_n)\| = \sqrt{\sum a_{i_1 \dots i_n}^2}$ given as follows:

Theorem 2. (Howgrave-Graham): *Let $h(x_1, x_2, \dots, x_n) \in \mathbb{Z}[x_1, x_2, \dots, x_n]$ be an integer polynomial that consists of at most ω monomials. Suppose that*

1. $h(x_1^{(0)}, x_2^{(0)}, \dots, x_n^{(0)}) \equiv 0 \pmod{e^m}$ for some m where $|x_1^{(0)}| < X_1, |x_2^{(0)}| < X_2 \dots |x_n^{(0)}| < X_n$, and
2. $\|h(x_1 X_1, x_2 X_2, \dots, x_n X_n)\| < \frac{e^m}{\sqrt{\omega}}$.

Then $h(x_1, x_2, \dots, x_n) = 0$ holds over the integers.

Definition 4. *The resultant of two polynomials $f(x_1, x_2, \dots, x_n)$ and $g(x_1, x_2, \dots, x_n)$ with respect to the variable x_i for some $1 \leq i \leq n$, is defined as the determinant of Sylvester matrix of $f(x_1, x_2, \dots, x_n)$ and $g(x_1, x_2, \dots, x_n)$ when considered as polynomials in the single indeterminate x_i , for some $1 \leq i \leq n$.*

Remark 2. *The resultant of two polynomials is non-zero if and only if the polynomials are algebraically independent.*

Remark 3. *If $(x_1^{(0)}, x_2^{(0)}, \dots, x_n^{(0)})$ is a common solution of algebraically independent polynomials f_1, f_2, \dots, f_m for $m \geq n$, then these polynomials yield g_1, g_2, \dots, g_{n-1} resultants in $n - 1$ variables and continuing so on the resultants yield a polynomial $t(x_i)$ in one variable with $x_i = x_i^{(0)}$ for some i is a solution of $t(x_i)$. Note the polynomials considered to compute resultants are always assumed to be algebraically independent.*

3. An Attack Bound Using Sublattice Reduction Techniques

In this section, an attack bound for a small multiplicative inverse k of $\varphi(N)$ modulo e when the prime sum $p + q$ is of the form $p + q = 2^n k_0 + k_1$, where n is a given positive integer and k_0 and k_1 are two suitably small unknown integers using sublattice reduction techniques is described.

In a previous paper [7], we proposed an attack on RSA when $\varphi(N)$ has small multiplicative inverse modulo e and the prime sum $p + q$ is of the form $p + q = 2^n k_0 + k_1$, where n is a given positive integer and k_0 and k_1 are two suitably small unknown integers using lattice reduction techniques.

For $2^{n'}$ is an inverse of $2^n \pmod{e}$, define $f(x, y, z) = \begin{cases} (N + 1)x + xy + (2^n)xz - 1 & \text{if } |k_0| \leq |k_1| \\ 2^{n'}x(N + 1) + xy + 2^{n'}xz - 2^{n'} & \text{if } |k_1| \leq |k_0|. \end{cases}$

If $|k_0| \leq |k_1|$, then $(k, -k_1, -k_0)$ is a solution and if $|k_1| \leq |k_0|$ then $(k, -k_0, -k_1)$ is a solution for the modular polynomial equation $f(x, y, z) \equiv 0 \pmod{e}$.

Now define the set $M_k = \bigcup_{0 \leq j \leq t} \{x^{i_1}y^{i_2}z^{i_3+j} \mid x^{i_1}y^{i_2}z^{i_3} \text{ is a monomial of } f^m \text{ and } \frac{x^{i_1}y^{i_2}z^{i_3}}{l^k} \text{ is a monomial of } f^{m-k}\}$, where l is a leading monomial of f and define the shift polynomials as

$$g_{k,i_1,i_2,i_3}(x,y,z) = \frac{x^{i_1}y^{i_2}z^{i_3}}{l^k} (f'(x,y,z))^k e^{m-k}, \text{ for } k = 0, \dots, m, x^{i_1}y^{i_2}z^{i_3} \in M_k \setminus M_{k+1}$$

and $f' = a_l^{-1}f \pmod e$ for the coefficient a_l of l . For $0 \leq k \leq m$, divide the above shift polynomials according to $t = 0$ and $t \geq 1$. Then for $t = 0$, the shift polynomials $g(x,y,z)$ are

$$g(x,y,z) = \begin{cases} z^{i_3} (f(x,y,z))^k e^{m-k}, & \text{for } i_1 = i_2 = k, i_3 = 0 \\ x^{i_1-k} z^{i_3} (f(x,y,z))^k e^{m-k}, & \text{for } k \leq m-1, i_1 = k+1, \dots, m, i_2 = k, i_3 = 0, \dots, (i_1 - i_2). \end{cases}$$

and for $t \geq 1$, the shift polynomials $h(x,y,z)$ are

$$h(x,y,z) = \begin{cases} z^{i_3} (f(x,y,z))^k e^{m-k}, & \text{for } i_1 = i_2 = k, i_3 = 1, \dots, t \\ x^{i_1-k} z^{i_3} (f(x,y,z))^k e^{m-k}, & \text{for } k \leq m-1, i_1 = k+1, \dots, m, i_2 = k, i_3 = (i_1 - i_2) + 1, \dots, (i_1 - i_2) + t. \end{cases}$$

Let L be the lattice spanned by the coefficient vectors $g(xX, yY, zZ)$ and $h(xX, yY, zZ)$ shifts with dimension $(\frac{1}{6}m^3 + m^2 + \frac{11}{6}m + 1) + (\frac{1}{2}(m^2 + m)t + (m + 1)t)$ [7]. Let M be the matrix of L with each row is the coefficients of the shift polynomial

$$\begin{aligned} g - \text{shifts} & \begin{cases} e^m, xe^m, xze^m, x^2e^m, x^2ze^m, x^2z^2e^m, \dots, x^m e^m, x^m ze^m, \dots, x^m z^m e^m, \\ fe^{m-1}, xfe^{m-1}, xzfe^{m-1}, \dots, x^{m-1} fe^{m-1}, x^{m-1} zfe^{m-1}, \dots, x^{m-1} z^{m-1} fe^{m-1}, \\ \vdots \\ f^{m-1}e, x f^{m-1}e, xz f^{m-1}e, \\ f^m, \end{cases} \\ h - \text{shifts} & \begin{cases} ze^m, \dots, z^t e^m, xz^2e^m, \dots, xz^{1+t} e^m, \dots, x^m z^{m+1} e^m, \dots, x^m z^{m+t} e^m, \\ zfe^{m-1}, \dots, z^t fe^{m-1}, xz^2 fe^{m-1}, \dots, xz^{1+t} fe^{m-1}, \dots, x^{m-1} z^m fe^{m-1}, \dots, x^{m-1} z^{(m-1)+t} fe^{m-1}, \\ \vdots \\ z f^{m-1}e, \dots, z^t f^{m-1}e, xz^2 f^{m-1}e, \dots, xz^{1+t} f^{m-1}e, \\ z f^m, \dots, z^t f^m \end{cases} \end{aligned}$$

and each column is the coefficients of each variable (in shift polynomials)

$$\begin{aligned} (\text{first } (\frac{1}{6}m^3 + m^2 + \frac{11}{6}m + 1) \text{ columns}) & \begin{cases} 1, x, xz, x^2, x^2z, x^2z^2, \dots, x^m, x^m z, \dots, x^m z^m, \\ xy, x^2y, x^2yz, x^3y, x^3yz, x^3yz^2, \dots, x^m y, x^m yz, \dots, x^m yz^{m-1}, \\ \vdots \\ x^{m-1} y^{m-1}, x^m y^{m-1}, x^m y^{m-1} z, \\ x^m y^m, \end{cases} \\ (\text{remaining } (\frac{1}{2}(m^2 + m)t + (m + 1)t) \text{ columns}) & \begin{cases} z, \dots, z^t, xz^2, \dots, xz^{1+t}, \dots, x^m z^{m+1}, \dots, x^m z^{m+t}, \\ xyz, \dots, xyz^t, x^2yz^2, \dots, x^2yz^{1+t}, \dots, x^m yz^m, \dots, x^m yz^{(m-1)+t}, \\ \vdots \\ x^{m-1} y^{m-1} z, \dots, x^{m-1} y^{m-1} z^t, x^m y^{m-1} z^2, \dots, x^m y^{m-1} z^{1+t}, \\ x^m y^m z, \dots, x^m y^m z^t. \end{cases} \end{aligned}$$

As xy is the leading monomial in $f(x, y, z)$ with coefficient 1, the diagonal elements in the matrix M are

$$\begin{aligned}
 & \left. \begin{array}{l} g - \text{shifts} \\ \\ \\ \\ \end{array} \right\} \begin{array}{l} e^m, Xe^m, XZe^m, X^2e^m, X^2Ze^m, X^2Z^2e^m, \dots, X^m e^m, X^m Ze^m, \dots, X^m Z^m e^m, \\ XYe^{m-1}, X^2Ye^{m-1}, X^2YZe^{m-1}, \dots, X^mYe^{m-1}, X^mYZe^{m-1}, \dots, X^mYZ^{m-1}e^{m-1}, \\ \vdots \\ X^{m-1}Y^{m-1}e, X^mY^{m-1}e, X^mY^{m-1}Ze, \\ X^mY^m, \end{array} \\
 & \left. \begin{array}{l} h - \text{shifts} \\ \\ \\ \\ \end{array} \right\} \begin{array}{l} Ze^m, \dots, Z^t e^m, XZ^2e^m, \dots, XZ^{1+t}e^m, \dots, X^m Z^{m+1}e^m, \dots, X^m Z^{m+t}e^m, \\ XYZe^{m-1}, \dots, XYZ^t e^{m-1}, X^2YZ^2e^{m-1}, \dots, X^2YZ^{1+t}e^{m-1}, \dots, X^mYZ^m e^{m-1}, \dots, X^mYZ^{(m-1)+t}e^{m-1}, \\ \vdots \\ X^{m-1}Y^{m-1}Ze, \dots, X^{m-1}Y^{m-1}Z^t e, X^mY^{m-1}Z^2e, \dots, X^mY^{m-1}Z^{1+t}e, \\ X^mY^mZ, \dots, X^mY^mZ^t. \end{array}
 \end{aligned}$$

Note that the matrix M is lower triangular matrix. Therefore, the determinant is

$$\det(L) = e^{n(e)} X^{n(X)} Y^{n(Y)} Z^{n(Z)}$$

where $n(e)$, $n(X)$, $n(Y)$ and $n(Z)$ are the number of e 's, X 's, Y 's and Z 's in all diagonal elements respectively, and

$$\begin{aligned}
 n(e) &= (((1/8)m^4 + (3/4)m^3 + (11/8)m^2 + (3/4)m) + ((1/6)(2m^3 + 3m^2 + m)t + (1/2)(m^2 + m)t)) \\
 n(X) &= (((1/8)m^4 + (3/4)m^3 + (11/8)m^2 + (3/4)m) + ((1/6)(2m^3 + 3m^2 + m)t + (1/2)(m^2 + m)t)) \\
 n(Y) &= (((1/24)m^4 + (1/4)m^3 + (11/24)m^2 + (1/4)m) + ((1/6)(m^3 - m)t + (1/2)(m^2 + m)t)) \\
 n(Z) &= (((1/24)m^4 + (1/4)m^3 + (11/24)m^2 + (1/4)m) + \\
 & \quad ((1/4)(m^2 + m)t^2 + (1/2)(m + 1)t^2 + (1/12)(2m^3 + 9m^2 + 7m)t + (1/2)(m + 1)t))
 \end{aligned}$$

Let N^δ , N^{γ_1} and N^{γ_2} be the upper bounds for X , $\max\{k_0, k_1\}$ and $\min\{k_0, k_1\}$ respectively, then the bound for δ in which the generalized Howgrave-Graham result holds given in the following theorem.

Theorem 3. [7] Let $N = pq$ be an RSA modulus with $q < p < 2q$. Let $e = N^\alpha$, $X = N^\delta$, $Y = N^{\gamma_1}$, $Z = N^{\gamma_2}$ and k be the multiplicative inverse of $\varphi(N)$ modulo e . Suppose the prime sum $p + q$ is of the form $p + q = 2^n k_0 + k_1$, for a known positive integer n and for $|k| \leq X$, $\max\{|k_0|, |k_1|\} \leq Y$ and $\min\{|k_0|, |k_1|\} \leq Z$ one can factor N in polynomial time if

$$\delta < \frac{1}{2}\alpha - \frac{1}{2}\gamma_1 + \frac{1}{16}\gamma_2 - \frac{1}{16}\sqrt{48(\alpha - \gamma_1)\gamma_2 + 33\gamma_2^2}. \tag{1}$$

To improve this bound in a lower dimension than the above dimension, first we construct a sublattice S_L of L and after that we apply the sublattice based techniques to the lattice S_L given by J. Blömer, A. May in [5], and are described in the following sections.

3.1. Construction of a Sublattice S_L of L

The construction of a sublattice S_L of L in order to improve the bound for δ is given in the following.

- First remove following rows in M corresponding to g -shifts
 $e^m, xe^m, xze^m, \dots, x^{m-1}e^m, \dots, x^{m-1}z^{m-1}e^m,$
 $fe^{m-1}, xfe^{m-1}, xzfe^{m-1}, \dots, x^{m-2}fe^{m-1}, \dots, x^{m-2}z^{m-2}fe^{m-1},$

$$\begin{aligned} & \vdots \\ & f^{m-2}e^2, x f^{m-2}e^2, xz f^{m-2}e^2, \\ & f^{m-1}e. \end{aligned}$$

Therefore the remaining rows in M corresponding to g -shifts are

$$\begin{aligned} & x^m e^m, x^m z e^m, \dots, x^m z^m e^m, \\ & x^{m-1} f e^{m-1}, \dots, x^{m-1} z^{m-1} f e^{m-1}, \\ & \vdots \\ & x f^{m-1} e, xz f^{m-1} e, \\ & f^m, \end{aligned}$$

and its corresponding g -shifts can be written as

$$g_s(x, y, z) = x^{l_1} z^{l_2} (f(x, y, z))^k e^{m-k} \text{ for } k = 0, \dots, m, l_1 = m - k, l_2 = 0, \dots, l_1.$$

- Now remove some rows in M corresponding to h -shifts are

$$\begin{aligned} & z e^m, \dots, z^t e^m, \dots, x^{m-1} z^m e^m, \dots, x^{m-1} z^{(m-1)+t} e^m, \\ & z f e^{m-1}, \dots, z^t f e^{m-1}, \dots, x^{m-2} z^{m-1} f e^{m-1}, \dots, x^{m-2} z^{(m-2)+t} f e^{m-1}, \\ & \vdots \\ & z f^{m-2} e^2, \dots, z^t f^{m-2} e^2, xz^2 f^{m-2} e^2, \dots, xz^{1+t} f^{m-2} e^2, \\ & z f^{m-1} e, \dots, z^t f^{m-1} e. \end{aligned}$$

Therefore the remaining rows in M corresponding to h -shifts are

$$\begin{aligned} & x^m z^{m+1} e^m, \dots, x^m z^{m+t} e^m, \\ & x^{m-1} z^m f e^{m-1}, \dots, x^{m-1} z^{(m-1)+t} f e^{m-1}, \\ & \vdots \\ & xz^2 f^{m-1} e, \dots, xz^{t+1} f^{m-1} e, \\ & z f^m, \dots, z^t f^m, \end{aligned}$$

and its corresponding h -shifts can be written as

$$h_s(x, y, z) = x^{l_1} z^{l_2} (f(x, y, z))^k e^{m-k} \text{ for } k = 0, \dots, m, l_1 = m - k, l_2 = l_1 + 1, \dots, l_1 + t.$$

Now, let S_L be the sub-lattice of L spanned by the coefficients of the vectors $g_s(xX, yY, zZ)$ and $h_s(xX, yY, zZ)$ shifts and M_s be the matrix of the lattice S_L .

Note that the matrix M_s is not square. So apply the sublattice based techniques to the basis of S_L or the rows of M_s to get a square matrix. Using that square matrix, the attack bound can be found and is given in the following section.

3.2. Applying Sub-Lattice Based Techniques to Get an Attack Bound

In [5], J. Blomer, A. May proposed a method to find an attack bound for low deciphering exponent in a smaller dimension than the approach by Boneh and Durfee’s attack in [4]. Apply their method based on sublattice reduction techniques to our lattice S_L to get an attack bound and is described in the following.

In order to apply the Howgrave-Graham’s theorem [11] by using Theorem 1, we need three short vectors in S_L as our polynomial consists of three variables. However, note that M_s is not a square matrix. So, first construct a square matrix M_{sl} by removing some columns in M_s , which are small linear combination of non-removing columns in M_s . Then the short vector in M_{sl} lead to short reconstruction vector in S_L .

Construction of a square sub-matrix M_{sl} of M_s .

Columns in M and M_s are same and each column in M is nothing but the coefficients of a variable, which is a leading monomial of the polynomial g or h -shifts. The first $(\frac{1}{6}m^3 + m^2 + \frac{11}{6}m + 1)$ and

remaining $\left(\frac{1}{2}(m^2 + m)t + (m + 1)t\right)$ columns are corresponding to the leading monomial of the polynomials g and h -shifts respectively. Therefore,

1. the first $\left(\frac{1}{6}m^3 + m^2 + \frac{11}{6}m + 1\right)$ columns are the coefficients of the each variable $x^{i_1}y^{i_2}z^{i_3}$ for $i_1 = i_2 = k, i_3 = 0$ and $i_1 = k + 1, \dots, m, i_2 = k, i_3 = 0, \dots, (i_1 - i_2)$ and remaining $\left(\frac{1}{2}(m^2 + m)t + (m + 1)t\right)$ columns are the coefficients of the each variable $x^{i_1}y^{i_2}z^{i_3}$ for $i_1 = i_2 = k, i_3 = 1, \dots, t$ and $i_1 = k + 1, \dots, m, i_2 = k, i_3 = (i_1 - i_2) + 1, \dots, (i_1 - i_2) + t$. So the variable $x^{i_1}y^{i_2}z^{i_3}$ corresponds a column in first $\left(\frac{1}{6}m^3 + m^2 + \frac{11}{6}m + 1\right)$ columns if $i_1 \geq i_2 + i_3$ and corresponds a column in remaining $\left(\frac{1}{2}(m^2 + m)t + (m + 1)t\right)$ columns if $i_1 < i_2 + i_3$.
2. As $1, x, xy, xz$ are the monomials of f , the set of all monomials of f^m for $m \geq 0$ is $\{x^{i_1}y^{i_2}z^{i_3}; i_1 = 0, \dots, m, i_2 = 0, \dots, i_1, i_3 = 0, \dots, i_1 - i_2\}$. Therefore, the coefficient of the variable $x^{i_1}y^{i_2}z^{i_3}$ in f^m is non-zero if and only if $i_3 \leq i_1 - i_2$, i.e., $i_1 \geq i_2 + i_3$.

Remove columns in M_s corresponding to the coefficients of the variable $x^a y^b z^c$ for all $0 \leq a \leq m - 1$ and note that every such column is $\left(\frac{m-(a-b)}{(m-a)!b!}\right) \cdot \frac{1}{X^{m-a}Y^{m-a}}$ multiple of a non-removed column, corresponding to the coefficients of $x^m y^{m-(a-b)} z^c$ and is proved in the following theorem.

Theorem 4. Each column in M_s corresponding to the coefficients of the variable $x^a y^b z^c$, a leading monomial of the polynomial g or h -shifts, for all $0 \leq a \leq m - 1$ is $\left(\frac{m-(a-b)}{(m-a)!b!}\right) \cdot \frac{1}{X^{m-a}Y^{m-a}}$ multiple of a non-removed column, represents the coefficients of the variable $x^m y^{m-(a-b)} z^c$.

Proof. First assume that $|k_0| \leq |k_1|$, then $f(x, y, z) = (N + 1)x + xy + 2^n xz - 1$.

For $n = 0, \dots, m, k_1 = m - n, k_2 = 0, \dots, k_1$, the g_s -shifts $x^{k_1} z^{k_2} f^n e^{k_1}$ corresponds first $\left(\frac{1}{6}m^3 + m^2 + \frac{11}{6}m + 1\right)$ rows in M_s and for $n = 0, \dots, m, k_1 = m - n, k_2 = k_1 + 1, \dots, k_1 + t$, the h_s -shifts $x^{k_1} z^{k_2} f^n e^{k_1}$ corresponds remaining rows in M_s . We prove this theorem in two cases.

Case(i): Any column in first $\left(\frac{1}{6}m^3 + m^2 + \frac{11}{6}m + 1\right)$ columns of M_s . i.e., a column corresponding coefficients of a variable $x^a y^b z^c$ with $a \geq b + c$, from the above analysis in (1).

Given that $0 \leq a \leq m - 1$. From the above analysis in (1) and (2), the coefficient of $x^a y^b z^c$ is non-zero in g_s -shifts $x^{k_1} z^{k_2} f^n e^{k_1}$ if and only if $a \geq k_1, b \leq m - k_1, c \geq k_2$ and $a - k_1 \geq b + (c - k_2)$. As $k_1 \geq k_2, k_2 \geq 0$ and $a - k_1 \geq b + (c - k_2)$, $\max\{0, k_1 - (a - (b + c))\} \leq k_2 \leq \min\{k_1, c\}$ and also as $a - k_1 < b + (c - k_2)$ for $k_1 > a - b, k_1$ is such that $0 \leq k_1 \leq a - b$.

Therefore, the coefficient of $x^a y^b z^c$ is non-zero in g_s -shifts $x^{k_1} z^{k_2} f^n e^{k_1}$ if and only if $a \geq k_1, b \leq m - k_1, c \geq k_2$ and $k_1 = 0, \dots, a - b, k_2 = \max\{0, k_1 - (a - (b + c))\}, \dots, \min\{k_1, c\}$.

Similarly we can prove that, the coefficient of $x^a y^b z^c$ is non-zero in h_s -shifts $x^{k_1} z^{k_2} f^n e^{k_1}$ if and only if $a \geq k_1, b \leq m - k_1, c \geq k_2$ and $k_1 = 0, \dots, c, k_2 = k_1 + 1, \dots, \min\{c, k_1 + t\}$ using the inequalities $k_1 + 1 \leq k_2 \leq k_1 + t, a \geq b + c$ and analysis in (1) and (2), and say $\min\{c, k_1 + t\} = l_t$

The formula for finding a coefficient of a variable $x^{l_1} y^{l_2} z^{l_3} = (1)^{n-l_1} x^{l_1-(l_2+l_3)} (xz)^{l_3} (xy)^{l_2}$ for $l_1 \leq n - 1$ in f^n is

$$\frac{n!}{(n - l_1)!(l_1 - (l_2 + l_3))!l_2!l_3!} (-1)^{n-l_1} (N + 1)^{l_1-(l_2+l_3)} (2^n)^{l_3}$$

and coefficient of $x^a y^b z^c$ in $x^{k_1} y^{k_2} f^n e^{k_1}$ is nothing but a coefficient of $x^{a-k_1} y^b z^{c-k_2}$ in f^n .

Note that a column corresponding to a variable $x^m y^{m-a} z^c$ is in the non-removing columns in M_s and coefficient of $x^m y^{m-a} z^c$ is zero for $k_1 > a - b$ in g_s -shifts, $k_1 > c$ in h_s -shifts. The columns corresponding to a variable $x^a y^b z^c$ and a variable $x^m y^{m-a} z^c$ only with non-zero terms is depicted in Table 1.

Therefore, from Table 1 the result holds in this case.

Case(ii): Any column in remaining $\left(\frac{1}{2}(m^2 + m)t + (m + 1)t\right)$ columns of M_s , i.e., a column corresponding coefficients of a variable $x^a y^b z^c$ with $a < b + c$, from the above analysis in (1).

The coefficient of $x^a y^b z^c$ is non-zero in g_s -shifts $x^{k_1} z^{k_2} f^n e^{k_1}$ if and only if $a \geq k_1, b \leq m - k_1, c \geq k_2, a - k_1 \geq b + (c - k_2)$ and note for $a < b + c, a - k_1 < b + (c - k_2)$ as $k_1 \geq k_2$ in g_s -shifts. So the coefficient of $x^a y^b z^c$ is zero in all rows corresponding to g_s -shifts.

The coefficient of $x^a y^b z^c$ is non-zero in h_s -shifts $x^{k_1} z^{k_2} f^n e^{k_1}$ if and only if $a \geq k_1, b \leq m - k_1, c \geq k_2$ and $a - k_1 \geq b + (c - k_2)$. For $k_1 > a - b, a - k_1 < b + (c - k_2)$ and from the inequalities $k_1 + 1 \leq k_2 \leq k_1 + t, a - k_1 \geq b + (c - k_2)$, we have the coefficient of $x^a y^b z^c$ is non-zero in h_s -shifts $x^{k_1} z^{k_2} f^n e^{k_1}$ if and only if $a \geq k_1, b \leq m - k_1, c \geq k_2$ and $k_1 = 0, \dots, a - b, k_2 = \max\{k_1 + 1, k_1 + (b + c) - a\}, \dots, \min\{c, k_1 + t\}$. Take $l_t = \min\{c, k_1 + t\}$.

Note that coefficient of $x^m y^{m-a} z^c$ is zero in all g_s -shifts as $a > c$ and for $k_1 > a - b$ in h_s -shifts. The columns corresponding to a variable $x^a y^b z^c$ and a variable $x^m y^{m-a} z^c$ only with non-zero terms is depicted in Table 2. Therefore, from Table 2 the result holds in this case.

Now apply the above analysis to the polynomial $f(x, y, z) = 2^{n'} x(N + 1) + xy + 2^{n'} xz - 2^{n'}$ for $|k_1| \leq |k_0|$, then this result is obtained. \square

From the above theorem, all columns corresponding to a variable $x^a y^b z^c$ for all $0 \leq a \leq m - 1$ are depending on a non-removed column, corresponding to a variable $x^m y^{m-(a-b)} z^c$ in M_s . Let M_{sl} be a matrix formed by removing all above columns from the matrix M_s and S_l be a lattice spanned by rows of M_{sl} . Then the short vector in S_l lead to short reconstruction vector in S_L , i.e., if $u = \sum_{b \in B} c_b b$ is a short vector in S_l then this lead to a short vector $\bar{u} = \sum_{b \in \bar{B}} c_b b$ (same coefficients c_b) in S_L where B and \bar{B} are the basis for S_l and S_L respectively.

As we removed all depending columns in M_s to form a matrix M_{sl} , apply the lattice based techniques to S_l instead of S_L to get an attack bound and this lattice reduction techniques gives a required short vectors in S_L for a given bound. The matrix M_{sl} is lower triangular with rows same as in M_s and each column corresponding to coefficients of one of the variables (leading monomials of g_s and h_s -shifts)

$$\begin{aligned}
 g_s - \text{shift} & \left\{ \begin{array}{l} x^m, x^m z, \dots, x^m z^m, \\ x^m y, \dots, x^m y z^{m-1}, \\ \vdots \\ x^m y^{m-1}, x^m y^{m-1} z, \\ x^m y^m, \end{array} \right. \\
 h_s - \text{shift} & \left\{ \begin{array}{l} x^m z^{m+1}, \dots, x^m z^{m+t}, \\ x^m y z^m, \dots, x^m y z^{(m-1)+t}, \\ \vdots \\ x^m y^{m-1} z^2, \dots, x^m y^{m-1} z^{1+t}, \\ x^m y^m z, \dots, x^m y^m z^t. \end{array} \right.
 \end{aligned}$$

Table 1. A column in first $(\frac{1}{6}m^3 + m^2 + \frac{11}{6}m + 1)$ columns of M_s and a column corresponding to coefficients of a variable $x^m y^{m-a} z^c$ only with non-zero terms.

Rows Corresponding to g and h Shifts	Column Corresponding to $x^a y^b z^c$	Column Corresponding to $x^m y^{m-a} z^c$
$x^{a-b} z^c f^{m-(a-b)} e^{a-b}$	$\frac{(m-(a-b))!}{(m-a)!b!} (-1)^{m-a} X^a Y^b Z^c e^{a-b}$	$X^m Y^{m-(a-b)} Z^c e^{a-b}$
$x^{a-b-1} z^{c-1} f^{m-(a-b-1)} e^{a-b-1}$	$\frac{(m-(a-b)+1)!}{(m-a)!b!} (-1)^{m-a} 2^n X^a Y^b Z^c e^{a-b-1}$	$\frac{(m-(a-b)+1)!}{(m-(a-b))!} 2^n X^m Y^{m-(a-b)} Z^c e^{a-b-1}$
$x^{a-b-1} z^c f^{m-(a-b-1)} e^{a-b-1}$	$\frac{(m-(a-b)+1)!}{(m-a)!b!} (-1)^{m-a} (N+1) X^a Y^b Z^c e^{a-b-1}$	$\frac{(m-(a-b)+1)!}{(m-(a-b))!} (N+1) X^m Y^{m-(a-b)} Z^c e^{a-b-1}$
⋮	⋮	⋮
$x^{a-b-(c-1)} z f^{m-((a-b)-(c-1))} e^{a-b-(c-1)}$	$\frac{(m-(a-b)+(c-1))!}{(m-a)!b!(c-1)!} (-1)^{m-a} (2^n)^{c-1} X^a Y^b Z^c e^{a-b-(c-1)}$	$\frac{(m-(a-b)+(c-1))!}{(m-(a-b))!(c-1)!} (2^n)^{c-1} X^m Y^{m-(a-b)} Z^c e^{a-b-(c-1)}$
⋮	⋮	⋮
$x^{a-b-(c-1)} z^c f^{m-((a-b)-(c-1))} e^{a-b-(c-1)}$	$\frac{(m-(a-b)+(c-1))!}{(m-a)!b!(c-1)!} (-1)^{m-a} (N+1)^{c-1} X^a Y^b Z^c e^{a-b-(c-1)}$	$\frac{(m-(a-b)+(c-1))!}{(m-(a-b))!(c-1)!} (N+1)^{c-1} X^m Y^{m-(a-b)} Z^c e^{a-b-(c-1)}$
$x^{a-b-c} f^{m-(a-b)+c} e^{a-(b+c)}$	$\frac{(m-(a-b)+c)!}{(m-a)!b!c!} (-1)^{m-a} (2^n)^c X^a Y^b Z^c e^{a-b-c}$	$\frac{(m-(a-b)+c)!}{(m-(a-b))!c!} (2^n)^c X^m Y^{m-(a-b)} Z^c e^{a-b-c}$
⋮	⋮	⋮
$x^{a-b-c} z^c f^{m-(a-b)+c} e^{a-(b+c)}$	$\frac{(m-(a-b)+c)!}{(m-a)!b!c!} (-1)^{m-a} (N+1)^c X^a Y^b Z^c e^{a-b-c}$	$\frac{(m-(a-b)+c)!}{(m-(a-b))!c!} (N+1)^c X^m Y^{m-(a-b)} Z^c e^{a-b-c}$
⋮	⋮	⋮
f^m	$\frac{m!}{(m-a)!b!c!(a-(b+c))!} (-1)^{m-a} (N+1)^{a-(b+c)} (2^n)^c X^a Y^b Z^c$	$\frac{m!}{(m-(a-b))!c!(a-(b+c))!} (N+1)^{a-(b+c)} (2^n)^c X^m Y^{m-(a-b)} Z^c$
$x^{c-1} z^c f^{m-(c-1)} e^{c-1}$	$\frac{(m-(c-1))!}{(m-a)!b!(a-(b+c)+1)!} (-1)^{m-a} (N+1)^{a-(b+c)+1} X^a Y^b Z^c e^{c-1}$	$\frac{(m-(c-1))!}{(m-(a-b))!(a-(b+c)+1)!} (N+1)^{a-(b+c)+1} X^m Y^{m-(a-b)} Z^c e^{c-1}$
⋮	⋮	⋮
$xz^2 f^{m-1} e$	$\frac{(m-1)!}{(m-a)!b!(c-2)!(a-(b+c)+1)!} (-1)^{m-a} (N+1)^{a-(b+c)+1} (2^n)^{c-2} X^a Y^b Z^c e$	$\frac{(m-1)!}{(m-(a-b))!(c-2)!(a-(b+c)+1)!} (N+1)^{a-(b+c)+1} (2^n)^{c-2} X^m Y^{m-(a-b)} Z^c e$
⋮	⋮	⋮
$xz^{l_i} f^{m-1} e$	$\frac{(m-1)!}{(m-a)!b!(c-l_i)!(a-(b+c)+l_i-1)!} (-1)^{m-a} (N+1)^{a-(b+c)+l_i-1} (2^n)^{c-l_i} X^a Y^b Z^c e$	$\frac{(m-1)!}{(m-(a-b))!(c-l_i)!(a-(b+c)+l_i-1)!} (N+1)^{a-(b+c)+l_i-1} (2^n)^{c-l_i} X^m Y^{m-(a-b)} Z^c e$
$z f^m$	$\frac{m!}{(m-a)!b!(c-1)!(a-(b+c)+1)!} (-1)^{m-a} (N+1)^{a-(b+c)+1} (2^n)^{c-1} X^a Y^b Z^c$	$\frac{m!}{(m-(a-b))!(c-1)!(a-(b+c)+1)!} (N+1)^{a-(b+c)+1} (2^n)^{c-1} X^m Y^{m-(a-b)} Z^c$
⋮	⋮	⋮
$z^{l_i} f^m$	$\frac{m!}{(m-a)!b!(c-l_i)!(a-(b+c)+l_i)!} (-1)^{m-a} (N+1)^{a-(b+c)+l_i} (2^n)^{c-l_i} X^a Y^b Z^c$	$\frac{m!}{(m-(a-b))!(c-l_i)!(a-(b+c)+l_i)!} (-1)^{m-a} (N+1)^{a-(b+c)+l_i} (2^n)^{c-l_i} X^m Y^{m-(a-b)} Z^c$

Table 2. A column in the last $\left(\frac{1}{2}(m^2 + m)t + (m + 1)t\right)$ columns of M_s and a column corresponding to coefficients of a variable $x^m y^{m-a} z^c$ only with non-zero terms.

Rows Corresponding to g and h Shifts	Column Corresponding to $x^a y^b z^c$	Column Corresponding to $x^m y^{m-a} z^c$
$x^{a-b} z^c f^{m-(a-b)} e^{a-b}$	$\frac{(m-(a-b))!}{(m-a)!b!} (-1)^{m-a} X^a Y^b Z^c e^{a-b}$	$X^m Y^{m-(a-b)} Z^c e^{a-b}$
⋮	⋮	⋮
$x^2 z^{(b+c)-a+2} f^{m-2} e^2$	$\frac{(m-2)!}{(m-a)!b!((a-b)-2)!} (-1)^{m-a} (2^n)^{(a-b)-2} X^a Y^b Z^c e^2$	$\frac{(m-2)!}{(m-(a-b))!((a-b)-2)!} (2^n)^{(a-b)-2} X^m Y^{m-(a-b)} Z^c e^2$
⋮	⋮	⋮
$x^2 z^{l_i} f^{m-2} e^2$	$\frac{(m-2)!}{(m-a)!b!(c-l_i)!(l_i-((b+c)-a+2))!} (-1)^{m-a} (N+1)^{l_i-((b+c)-a+2)} (2^n)^{c-l_i} X^a Y^b Z^c e^2$	$\frac{(m-2)!}{(m-(a-b))!(c-l_i)!(l_i-((b+c)-a+2))!} (N+1)^{l_i-((b+c)-a+2)} (2^n)^{c-l_i} X^m Y^{m-(a-b)} Z^c e^2$
$x z^{b+c-a+1} f^{m-1} e$	$\frac{(m-1)!}{(m-a)!b!((a-b)-1)!} (-1)^{m-a} (2^n)^{(a-b)-1} X^a Y^b Z^c e$	$\frac{(m-1)!}{(m-(a-b))!((a-b)-1)!} (2^n)^{(a-b)-1} X^m Y^{m-(a-b)} Z^c e$
⋮	⋮	⋮
$x z^{l_i} f^{m-1} e$	$\frac{(m-1)!}{(m-a)!b!(c-l_i)!(l_i-(b+c-a+1))!} (-1)^{m-a} (N+1)^{(l_i-(b+c-a+1))} (2^n)^{c-l_i} X^a Y^b Z^c e$	$\frac{(m-1)!}{(m-(a-b))!(c-l_i)!(l_i-(b+c-a+1))!} (N+1)^{(l_i-(b+c-a+1))} (2^n)^{c-l_i} X^m Y^{m-(a-b)} Z^c e$
$z^{b+c-a} f^m$	$\frac{m!}{(m-a)!b!(a-b)!} (-1)^{m-a} (2^n)^{a-b} X^a Y^b Z^c$	$\frac{m!}{(m-(a-b))!(a-b)!} (2^n)^{a-b} X^m Y^{m-(a-b)} Z^c$
⋮	⋮	⋮
$z^{l_i} f^m$	$\frac{m!}{(m-a)!b!(c-l_i)!(l_i-((b+c)-a))!} (-1)^{m-a} (N+1)^{l_i-((b+c)-a)} (2^n)^{c-l_i} X^a Y^b Z^c$	$\frac{m!}{(m-(a-b))!(c-l_i)!(l_i-((b+c)-a))!} (-1)^{m-a} (N+1)^{l_i-((b+c)-a)} (2^n)^{c-l_i} X^m Y^{m-(a-b)} Z^c$

Therefore S_l is a lattice spanned by coefficient vectors of the shift polynomials $g_{sl}(xX, yY, zZ)$ and $h_{sl}(xX, yY, zZ)$ where

$$g_{sl}(x, y, z) = x^{l_1} z^{l_2} (f(x, y, z) - \text{constant term of } f)^n e^{l_1} \text{ for } n = 0, \dots, m, l_1 = m - n, l_2 = 0, \dots, l_1 \text{ and}$$

$$h_{sl}(x, y, z) = x^{l_1} z^{l_2} (f(x, y, z) - \text{constant term of } f)^n e^{l_1} \text{ for } n = 0, \dots, m, l_1 = m - n, l_2 = l_1 + 1, \dots, l_1 + t.$$

Since S_l is full-rank lattice, $\det S_l = \det M_{sl} = e^{n(e)} X^{n(X)} Y^{n(Y)} Z^{n(Z)}$ where $n(e), n(X), n(Y), n(Z)$ are denotes the number of e 's, X 's, Y 's, Z 's in all the diagonal elements of M_{sl} respectively. As $x^n y^n$ is a leading monomial of f^n with coefficient 1, we have

$$\begin{aligned} n(e) &= \sum_{n=0}^m \sum_{l_1=m-n} \sum_{l_2=0}^{l_1} l_1 + \sum_{n=0}^m \sum_{l_1=m-n} \sum_{l_2=l_1+1}^{l_1+t} l_1 \\ &= (1/3)m^3 + m^2 + (1/2)(m^2 + m)t + (2/3)m, \end{aligned}$$

$$\begin{aligned} n(X) &= \sum_{n=0}^m \sum_{l_1=m-n} \sum_{l_2=0}^{l_1} n + l_1 + \sum_{n=0}^m \sum_{l_1=m-n} \sum_{l_2=l_1+1}^{l_1+t} n + l_1 \\ &= (1/2)m^3 + (3/2)m^2 + (m^2 + m)t + m, \end{aligned}$$

$$\begin{aligned} n(Y) &= \sum_{n=0}^m \sum_{l_1=m-n} \sum_{l_2=0}^{l_1} n + \sum_{n=0}^m \sum_{l_1=m-n} \sum_{l_2=l_1+1}^{l_1+t} n \\ &= (1/6)m^3 + (1/2)m^2 + (1/2)(m^2 + m)t + (1/3)m, \end{aligned}$$

$$\begin{aligned} n(Z) &= \sum_{n=0}^m \sum_{l_1=m-n} \sum_{l_2=0}^{l_1} l_2 + \sum_{n=0}^m \sum_{l_1=m-n} \sum_{l_2=l_1+1}^{l_1+t} l_2 \\ &= (1/6)m^3 + (1/2)(m + 1)t^2 + (1/2)m^2 + (1/2)(m^2 + 2m + 1)t + (1/3)m \end{aligned}$$

$$\begin{aligned} \text{and } \dim(S_l) = \omega &= \sum_{n=0}^m \sum_{l_1=m-n} \sum_{l_2=0}^{l_1} 1 + \sum_{n=0}^m \sum_{l_1=m-n} \sum_{l_2=l_1+1}^{l_1+t} 1 \\ &= (1/2)m^2 + (m + 1)t + (3/2)m + 1. \end{aligned}$$

Take $t = \tau m$, then for sufficiently large m , the exponents $n(e), n(X), n(Y), n(Z)$ and the dimension ω reduce to

$$\begin{aligned} \omega &= \left(\frac{1}{2} + \tau\right) m^2 + o(m^2), \\ n(e) &= \left(\frac{1}{3} + \frac{1}{2}\tau\right) m^3 + o(m^3), \\ n(X) &= \left(\frac{1}{2} + \tau\right) m^3 + o(m^3), \\ n(Y) &= \left(\frac{1}{6} + \frac{1}{2}\tau\right) m^3 + o(m^3), \\ n(Z) &= \left(\frac{1}{6} + \frac{1}{2}\tau + \frac{1}{2}\tau^2\right) m^3 + o(m^3). \end{aligned}$$

Applying the LLL algorithm to the basis vectors of the lattice S_l , i.e., coefficient vectors of the shift polynomials, we get a LLL-reduced basis say $\{v_1, v_2, \dots, v_\omega\}$ and from the Theorem 1 we have

$$\|v_1\| \leq \|v_2\| \leq \|v_3\| \leq 2^{\frac{\omega(\omega-1)}{4(\omega-2)}} \det(S_l)^{\frac{1}{\omega-2}}.$$

In order to apply the generalization of Howgrave-Graham result in Theorem 2, we need the following inequality

$$2^{\frac{\omega(\omega-1)}{4(\omega-2)}} \det(S_l)^{\frac{1}{\omega-2}} < \frac{e^m}{\sqrt{\omega}}.$$

from this, we deduce

$$\det(S_l) < \frac{1}{\left(2^{\frac{\omega(\omega-1)}{4(\omega-2)}} \sqrt{\omega}\right)^{\omega-2}} e^{m(\omega-2)} < \frac{1}{\left(2^{\frac{\omega(\omega-1)}{4(\omega-2)}} \sqrt{\omega}\right)^{\omega-2}} e^{m\omega}.$$

As the dimension ω is not depending on the public encryption exponent e , $\frac{1}{\left(2^{\frac{\omega(\omega-1)}{4(\omega-2)}} \sqrt{\omega}\right)^{\omega-2}}$ is a fixed constant, so we need the inequality $\det(S_l) < e^{m\omega}$, i.e., $e^{n(e)} X^{n(X)} Y^{n(Y)} Z^{n(Z)} < e^{m\omega}$.

Substitute all values and taking logarithms, neglecting the lower order terms and after simplifying by m^3 we get

$$(-1 - 3\tau)\alpha + (3 + 6\tau)\delta + (1 + 3\tau)\gamma_1 + (1 + 3\tau + 3\tau^2)\gamma_2 < 0.$$

The left hand side inequality is minimized at $\tau = \frac{\alpha - (2\delta + \gamma_1 + \gamma_2)}{2\gamma_2}$ and putting this value in the above inequality we get

$$\delta < \frac{1}{2}\alpha - \frac{1}{2}\gamma_1 - \frac{1}{6}\sqrt{6(\alpha - \gamma_1)\gamma_2 + 3\gamma_2^2}.$$

From the first three short vectors v_1, v_2 and v_3 in LLL reduced basis of a basis B in S_l we consider three polynomials $g_1(x, y, z), g_2(x, y, z)$ and $g_3(x, y, z)$ over \mathbb{Z} such that $g_1(x_0, y_0, z_0) = g_2(x_0, y_0, z_0) = g_3(x_0, y_0, z_0) = 0$. These short vectors v_1, v_2 and v_3 lead to a short vector \bar{v}_1, \bar{v}_2 and \bar{v}_3 respectively and $\bar{g}_1(x, y, z), \bar{g}_2(x, y, z)$ and $\bar{g}_3(x, y, z)$ its corresponding polynomials. Apply the same analysis in paper [7] to the above polynomials to get the factors p and q of RSA modulus N .

Theorem 5. Let $N = pq$ be an RSA modulus with $q < p < 2q$. Let $e = N^\alpha, X = N^\delta, Y = N^{\gamma_1}, Z = N^{\gamma_2}$ and k be the multiplicative inverse of $\varphi(N)$ modulo e . Suppose the prime sum $p + q$ is of the form $p + q = 2^n k_0 + k_1$, for a known positive integer n and for $|k| \leq X, \max\{|k_0|, |k_1|\} \leq Y$ and $\min\{|k_0|, |k_1|\} \leq Z$ one can factor N in polynomial time if

$$\delta < \frac{1}{2}\alpha - \frac{1}{2}\gamma_1 - \frac{1}{6}\sqrt{6(\alpha - \gamma_1)\gamma_2 + 3\gamma_2^2}. \tag{2}$$

Proof. Follows from the above argument and the LLL lattice basis reduction algorithm operates in polynomial time [9]. \square

Note that for any given primes p and q with $q < p < 2q$, we can always find a positive integer n such that $p + q = 2^n k_0 + k_1$ where $0 \leq |k_0|, |k_1| \leq \approx 0.25$. A typical example is $2^n \approx \frac{3}{\sqrt{2}} N^{0.25}$ as $p + q < \frac{3}{\sqrt{2}} N^{0.5}$ [12]. So take γ_1 and γ_2 in the range $(0, 0.25)$.

Let δ_L and δ_{sl} be the bounds for δ in inequalities (1) and (2) respectively. Then note that δ_{sl} is slightly larger than δ_L and is depicted in Figure 1 for $\alpha = 0.51, 0.55, 0.750$ and 1.

In the Figure 1, x, y, z -axis represents γ_1, γ_2 , bound for δ respectively and yellow, red regions represents δ_{sl}, δ_L receptively. From this figure, it is noted that the yellow region is slightly above the red region, i.e., δ_{sl} is slightly grater than δ_L and this improvement increases when the values of α increases.

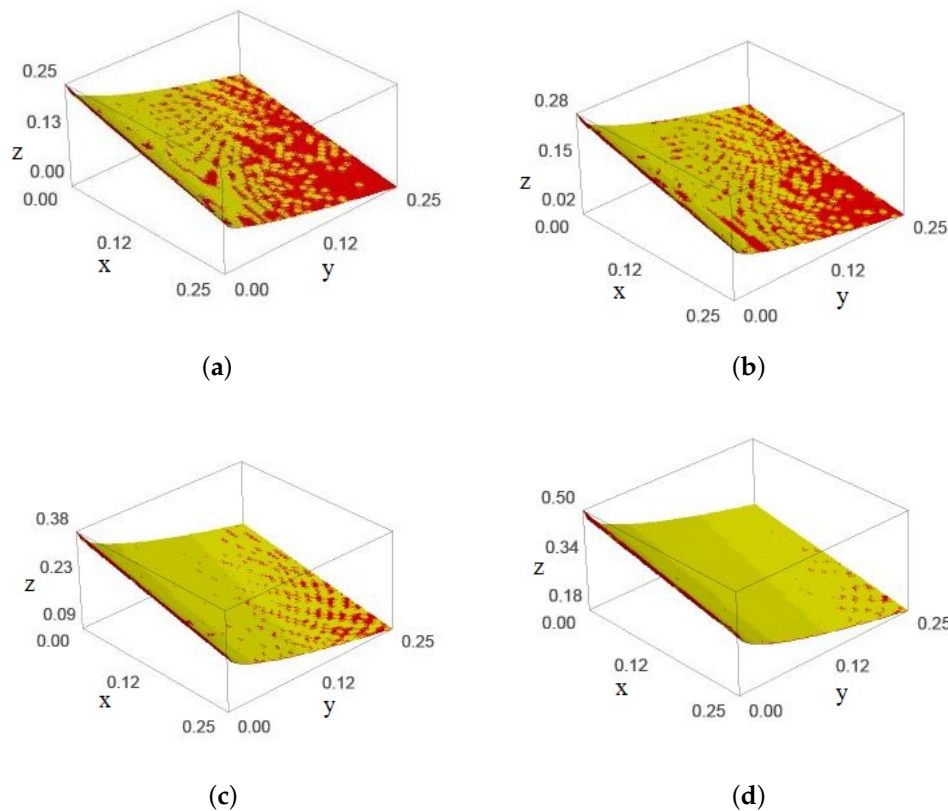


Figure 1. The region of δ_{sl} and δ_L for $\alpha = 0.501, 0.55, 0.75, 1$; (a) $\alpha = 0.501$; (b) $\alpha = 0.55$; (c) $\alpha = 0.75$; (d) $\alpha = 0.1$.

As the dimension of L is $(1/6)m^3 + (1/2)m^2(t + 2) + (1/6)m(9t + 11) + (t + 1)$ for $t = \left(\frac{\alpha - (2\delta + \gamma_1 + \gamma_2)}{3\gamma_2}\right) m$ [7] and S_l is $(1/2)m^2 + (m + 1)t + (3/2)m + 1$ for $t = \left(\frac{\alpha - (2\delta + \gamma_1 + \gamma_2)}{2\gamma_2}\right) m$, note the dimension of S_l is $(1/6)m^3 + (1/3)t(m^2 - 1) + (1/2)m^2 + (1/3)m$, for $t = \left(\frac{\alpha - (2\delta + \gamma_1 + \gamma_2)}{2\gamma_2}\right)$ smaller than the dimension of L .

3.3. A New Attack Bound for Deciphering Exponent d with a Composed Prime Sum

In this section, we apply the same analysis for getting bound for d which we have earlier obtained resultant bound for k .

From the relation $ed \equiv 1 \pmod{\varphi(N)}$, we get

$$t(N + 1 - (2^n k_0 + k_1)) + 1 \equiv 0 \pmod{e} \tag{3}$$

for $t = \frac{ed-1}{\varphi(N)}$ and the prime sum $p + q = 2^n k_0 + k_1$.

Now define

$$f'(x, y, z) = \begin{cases} (N + 1)x + xy + (2^n)xz + 1 & \text{if } |k_0| \leq |k_1| \\ 2^{n'}x(N + 1) + xy + 2^{n'}xz + 2^{n'} & \text{if } |k_1| \leq |k_0|. \end{cases}$$

From Equation (3), note that if $|k_0| \leq |k_1|$ then $(t, -k_1, -k_0)$ is a solution and if $|k_1| \leq |k_0|$ then $(t, -k_0, -k_1)$ is a solution for the modular polynomial equation $f'(x, y, z) \equiv 0 \pmod{e}$.

As the polynomials $f(x, y, z)$, $f'(x, y, z)$ differ by signs only, we can implement the above argument for $f(x, y, z)$ to $f'(x, y, z)$ and obtained new bound on d for $t < d = N^{\delta'}$, $\max |k_0|, |k_1| \leq N^{\gamma_1}$, $\min |k_0|, |k_1| \leq N^{\gamma_2}$ and for $e = N^\alpha$ is

$$\delta' < \frac{1}{2}\alpha - \frac{1}{2}\gamma_1 - \frac{1}{6}\sqrt{6(\alpha - \gamma_1)\gamma_2 + 3\gamma_2^2}. \tag{4}$$

For $\alpha = 1$, the Boneh and Durfee’s bound for $d = N^\delta$ is $N^{0.292}$. The new bound on d may overcome this bound for $\alpha = 1$ and for some values of γ_1 and γ_2 and that values are depicted in Table 3.

Table 3. For $\alpha = 1$, the values of bound on δ' in terms of γ_1 and γ_2 .

γ_1	γ_2	δ' New Bound
0.40	0.005–0	0.2929–0.3
0.35	0.0094–0	0.2929–0.325
0.25	0.052–0	0.2929–0.375
0.15	0.1152–0	0.2929–0.425
0.01	0.009–0	0.4563–0.495

4. Conclusions

In this paper, another attack bound for k , a small multiplicative inverse of $\varphi(N)$ modulo e is given when the prime sum $p + q$ is of the form $p + q = 2^n k_0 + k_1$ where n is a given positive integer and k_0 and k_1 are two suitably small unknown integers using sublattice reduction techniques and Coppersmith’s methods for finding small roots of modular polynomial equations. This attack bound is slightly larger than the bound, in the approach using lattice based techniques and requires lattice of smaller dimension than the approach given by using lattice based techniques. Also, we gave a new attack bound for the deciphering exponent d with above composed prime sum and compare it to Boneh and Durfee’s bound.

Author Contributions: Conceptualization P.A.K. and L.J.; Methodology P.A.K; Software L.J.; Formal Analysis P.A.K. and L.J.; Investigation L.J.; Writing—Original Draft Preparation P.A.K. and L.J.; Writing—Review & Editing P.A.K. and L.J.; Supervision P.A.K.

Funding: This research is part of research project funded by the University Grants Commission (UGC) under Major Research Project (MRP) with P. Anuradha Kameswari as Principal Investigator and L. Jyotsna as the Project Fellow.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Koblitz, N. *A Course in Number Theory and Cryptography*; Springer: Berlin, Germany, 1994; ISBN 3-578071-8.
2. Wiener, M. Cryptanalysis of Short RSA Secret Exponents. *IEEE Trans. Inf. Theory* **1990**, *36*, 553–558.
3. Coppersmith, D. Small solutions to polynomial equations, and low exponent RSA vulnerabilities. *J. Cryptol.* **1997**, *10*, 233–260.
4. Boneh, D.; Durfee, G. *Cryptanalysis of RSA with Private Key D Less than $N^{0.292}$* ; Advances in Cryptology Eurocrypt99, Lecture Notes in Computer Science; Springer: Berlin, Germany, 1999; Volume 1592, p. 111.
5. Blomer, J.; May, A. *Low Secret Exponent RSA Revisited*; Cryptography and Lattice Conference (CaLC 2001), Lecture Notes in Computer Science; Springer: Berlin, Germany, 2001; Volume 2146, p. 419.
6. Jochemsz, E.; May, A. *A Strategy for Finding Roots of Multivariate Polynomials with New Applications in Attacking RSA Variant*; ASIACRYPT 2006, LNCS; Springer: Berlin, Germany, 2006; Volume 4284, pp. 267–282.
7. Anuradha Kameswari, P.; Jyotsna, L. Cryptanalysis of RSA with Small Multiplicative Inverse of $\varphi(N)$ Modulo e and with a Composed Prime Sum $p + q$. *Int. J. Math. Appl.* **2018**, *6*, 515–526.
8. Hoftstein, J.; Pipher, J.; Silverman, J.H. *An Introduction to Mathematical Cryptography*; Springer: Berlin, Germany, 2008.
9. Lenstra, A.K.; Lenstra, H.W.; Lovasz, L. Factoring polynomials with rational coefficients. *Math. Annalen* **1982**, *261*, 515–534.

10. May, A. New RSA Vulnerabilities Using Lattice Reduction Methods. Ph.D. Thesis, University of Paderborn, Paderborn, Germany, 2003. Available online: <http://wwwcs.upb.de/cs/agbloemer/personen/alex/publikationen/> (accessed on 19 October, 2003)
11. Howgrave-Graham, N. Finding small roots of univariate modular equations revisited. In *Cryptography and Coding*; LNCS 1355; Springer: Berlin, Germany, 1997; pp. 131–142.
12. Nitaj, A. *Another Generalization of Wiens Attack on RSA*; Vaudenay, S., Ed.; Africacrypt 2008. LNCS; Springer: Berlin, Germany, 2008; Volume 5023, pp. 174–190.



© 2018 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).

Enclosure-3

ACHIEVEMENTS FROM PROJECT

Achievements from the project

First the continued fraction based attacks of M.J. Wiener and its extensions are extended to RSA-like Cryptosystem over elliptic curves $E(\mathbb{Z}_{pq})$ due to KMOV. Published these results under the title "Extending Wiener's Extension to RSA-Like Cryptosystems over Elliptic curves" in the British Journal of Mathematics & Computer Science 14(1): 1-8, Jan 2016, Article no.BJMCS.23036 ISSN: 2231-0851, SCIENCEDOMAIN International.

Lattice reduction attacks on RSA with respect to small multiplicative inverse of $p - 1$ or $q - 1$ modulo e and with respect to small multiplicative inverse of $\varphi(N)$ modulo e are proposed for e the public encryption exponent. If $e = N^\alpha > p - 1$, r and s the multiplicative inverses of $p - 1$ and $q - 1$ modulo e respectively, then for (x_0, y_0) solution of the polynomial congruence $f(x, y) \equiv 0 \pmod{e}$, for $f(x, y) = x(y + A) - 1$ with $A = \lceil \sqrt{N} \rceil - 1$ and N^δ, N^γ upper bounds for x_0, y_0 respectively, we implemented lattice reduction techniques to our polynomial congruence and proved that the attack works for $\delta < \frac{3\alpha + \gamma - 2\sqrt{\gamma(3\alpha + \gamma)}}{3}$ when both x and y shifts are used and $\delta < \frac{\alpha - \gamma}{2}$ when only x -shifts are used. Further we improved the bound for δ as $\alpha - \gamma(1 + \alpha) < \delta < \alpha - \sqrt{\alpha\gamma}$ and $\delta < \frac{2\alpha - 6\gamma + 2\sqrt{\alpha^2 - \alpha\gamma + 4\gamma^2}}{5}$ by implementing the sublattice based techniques.

Published these results under the title "Cryptanalysis of RSA with small multiplicative Inverse of $(p - 1)$ or $(q - 1)$ modulo e ", in the journal of Journal of Global Research in Mathematical Achieves (JGRMA), ISSN: 2320-5822, Volume 5, No. 5(May-2018), pp. 72-81.

Further considered the lattice attacks on RSA if the multiplicative inverse k of $\varphi(N)$ modulo e is small for $q < p < 2q$ and $e = N^\alpha > p + q$, the prime sum. The polynomial congruence $f(x, y, z) \equiv 0 \pmod{e}$ for

$$f(x, y, z) = \begin{cases} (N + 1)x + xy + (2^n)xz - 1 & \text{if } |k_0| \leq |k_1| \\ 2^{n'}x(N + 1) + xy + 2^{n'}xz - 2^{n'} & \text{if } |k_1| \leq |k_0| \end{cases}$$

where $2^{n'}$ is an inverse of $2^n \pmod{e}$, the attack bound for δ is such that $\delta < \frac{1}{2}\alpha - \frac{1}{2}\gamma_1 + \frac{1}{16}\gamma_2 - \frac{1}{16}\sqrt{48(\alpha - \gamma_1)\gamma_2 + 33\gamma_2^2}$ where $N^{\gamma_1}, N^{\gamma_2}$ are the upper bounds for $\max\{|k_0|, |k_1|\}$, $\min\{|k_0|, |k_1|\}$ respectively.

Published these results under the title "Cryptanalysis of RSA with Small Multiplicative Inverse of $\varphi(N)$ Modulo e and with a Composed Prime Sum $p + q$ ", in the journal of International Journal of Mathematics and its Applications (IJMAA), ISSN: 2347-1557, Volume 6, No. 1(2018), Impact factor: 0.421 pp 515-526.

Further improved the previous bound by using the sub-lattice based techniques. The new bound on δ is $\frac{1}{2}\alpha - \frac{1}{2}\gamma_1 - \frac{1}{6}\sqrt{6(\alpha - \gamma_1)\gamma_2 + 3\gamma_2^2}$ is showed to be greater than the former bound graphically.

Communicated these results under the title "An Attack Bound for Small Multiplicative Inverse of $\varphi(N)$ modulo e with a Composed Prime Sum $p + q$ using Sub lattice Based Techniques", in Journal of Cryptography, ISSN 2410-387X. The corresponding refinement of attack bounds in each case is depicted explicitly in tabular forms.

This study is helpful in the other RSA-like cryptosystems with Dickson polynomials, Lucas sequences etc. by identifying the corresponding analogue to $\phi(N)$. This study of refinement of attack bounds of RSA has refined some attack bounds and is also useful in taking some precautionary measures in the implementation of RSA. All the attacks and refinement of attack bounds proposed in the study are presented in a tabular form that is useful in the adaption of RSA and the selections of parameters of RSA may be carried out according to the table on refinement of attack bounds as given in table 6.1, thereby avoiding the choices of parameters that lead to an attack.

Attack	Based on theory	Refining the RSA attack bounds
Wiener's attack	continued fraction algorithm	$d < N^{0.25}$.
Weger's attack	continued fraction algorithm	$N^{0.25} < d < N^{0.75-\beta}$, for $e \approx N$ and $N^\beta = p - q $.
Maitra-Sarkar' attack	continued fraction algorithm	$N^{0.25} < d < N^{\frac{1-\gamma}{2}}$, for $e \approx N$ and $ p - \rho q \leq \frac{N^\gamma}{16}$, where $\gamma \leq \frac{1}{2}$ and $1 \leq \rho \leq 2$.
Boneh and Durfee's attack	Lattice based techniques	$d < N^{0.284}$ for $e \approx N$.
Boneh and Durfee's attack	sublattice based techniques	$d < N^{0.292}$ for $e \approx N$.
Blömer and May's attack	Sublattice based techniques with lower dimension	$d < N^{0.290}$ for $e \approx N$.
Weger's attack	Lattice based techniques	$d < N^{\frac{1}{6}(4\beta+5) - \frac{1}{3}\sqrt{(4\beta+5)(4\beta-1)}}$, for $e \approx N$ and $N^\beta = p - q $.
Weger's attack	sublattice based techniques	$N^{2-4\beta} < d < N^{1-\sqrt{2\beta-\frac{1}{3}}}$, for $e \approx N$ and $N^\beta = p - q $.
Maitra-Sarkar's attack	Lattice based techniques	$d < N^{\frac{7+13-2\sqrt{7(7+3)}}{3}}$, for $e \approx N$ and $ p - \rho q \leq \frac{N^\gamma}{16}$, where $\gamma \leq \frac{1}{2}$ and $1 \leq \rho \leq 2$.
Maitra-Sarkar's attack	sublattice based techniques	$N^{1-2\gamma} < d < N^{1-\sqrt{\gamma}}$, for $e \approx N$ and $ p - \rho q \leq \frac{N^\gamma}{16}$, where $\gamma \leq \frac{1}{2}$ and $1 \leq \rho \leq 2$.
Maitra-Sarkar's attack	sublattice based techniques with lower dimension	$d < N^{\frac{\sqrt{16\gamma^2-4\gamma+4-(6\gamma-2)}}{6}}$, for $e \approx N$ and $ p - \rho q \leq \frac{N^\gamma}{16}$, where $\gamma \leq \frac{1}{2}$ and $1 \leq \rho \leq 2$.
Nitaj and Douh's attack	Lattice based techniques	$d = Md_1 + d_0$, $\delta < \frac{1}{4}(5 - 4\gamma - \sqrt{12\alpha + 12\beta - 12\gamma + 3})$, for $e = N^\alpha$, $d_1 < N^\delta$ and $d_0 < N^\beta$.
Proposed attack when $(p-1)$ or $(q-1)$ have small multiplicative inverse	Lattice based techniques with x shifts	$\min\{(p-1)^{-1} \bmod e, (q-1)^{-1} \bmod e\} < N^{\frac{\alpha-\beta}{2}}$, for $e = N^\alpha$ and $p - q = N^\beta$.
Proposed attack when $(p-1)$ or $(q-1)$ have small multiplicative inverse	Lattice based techniques with x and y shifts	$\min\{(p-1)^{-1} \bmod e, (q-1)^{-1} \bmod e\} < N^{\frac{(3\alpha+\beta-2\sqrt{\beta(3\alpha+\beta)})}{3}}$, for $e = N^\alpha$ and $p - q = N^\beta$.
Proposed attack when $(p-1)$ or $(q-1)$ have small multiplicative inverse	Sublattice based techniques	$N^{\alpha-\beta(1+\alpha)} < \min\{(p-1)^{-1} \bmod e, (q-1)^{-1} \bmod e\} < N^{\alpha-\sqrt{\alpha\beta}}$, for $e = N^\alpha$ and $p - q = N^\beta$.
Proposed attack when $(p-1)$ or $(q-1)$ have small multiplicative inverse	Sublattice based techniques with lower dimension	$\min\{(p-1)^{-1} \bmod e, (q-1)^{-1} \bmod e\} < N^{\frac{2\alpha-6\beta+2\sqrt{\alpha^2-\alpha\beta+4\beta^2}}{6}}$, for $e = N^\alpha$ and $p - q = N^\beta$.
Proposed attack when $(p-1)$ or $(q-1)$ have small multiplicative inverse	Lattice based techniques with x shifts	$\min\{(p-1)^{-1} \bmod e, (q-1)^{-1} \bmod e\} < N^{\frac{\alpha-\gamma}{2}}$, for $e = N^\alpha$ and $ p - \rho q \leq N^\gamma$, $\gamma \leq \frac{1}{2}$.
Proposed attack when $(p-1)$ or $(q-1)$ have small multiplicative inverse	Lattice based techniques with x and y shifts	$\min\{(p-1)^{-1} \bmod e, (q-1)^{-1} \bmod e\} < N^{\frac{(3\alpha+\gamma-2\sqrt{\gamma(3\alpha+\gamma)})}{3}}$, for $e = N^\alpha$ and $ p - \rho q \leq N^\gamma$, $\gamma \leq \frac{1}{2}$.
Proposed attack when $(p-1)$ or $(q-1)$ have small multiplicative inverse	Sublattice based techniques	$N^{\alpha-\gamma(1+\alpha)} < \min\{(p-1)^{-1} \bmod e, (q-1)^{-1} \bmod e\} < N^{\alpha-\sqrt{\alpha\gamma}}$, for $e = N^\alpha$ and $ p - \rho q \leq N^\gamma$, $\gamma \leq \frac{1}{2}$.
Proposed attack when $(p-1)$ or $(q-1)$ have small multiplicative inverse	Sublattice based techniques with lower dimension	$\min\{(p-1)^{-1} \bmod e, (q-1)^{-1} \bmod e\} < N^{\frac{2\alpha-6\gamma+2\sqrt{\alpha^2-\alpha\gamma+4\gamma^2}}{6}}$, for $e = N^\alpha$ and $ p - \rho q \leq N^\gamma$, $\gamma \leq \frac{1}{2}$.
Proposed attack when $\varphi(N)^{-1}$ have small multiplicative inverse	Lattice based techniques with x shifts	$(\varphi(N)^{-1} \bmod e) < N^{\frac{\alpha-\beta}{2}}$, for $e = N^\alpha$ and $p - q = N^\beta$.
Proposed attack when $\varphi(N)^{-1}$ have small multiplicative inverse	Lattice based techniques with x and y shifts	$(\varphi(N)^{-1} \bmod e) < N^{\frac{(3\alpha+\beta-2\sqrt{\beta(3\alpha+\beta)})}{3}}$, for $e = N^\alpha$ and $p - q = N^\beta$.
Proposed attack when $\varphi(N)^{-1}$ have small multiplicative inverse	Sublattice based techniques	$N^{\alpha-\beta(1+\alpha)} < (\varphi(N)^{-1} \bmod e) < N^{\alpha-\sqrt{\alpha\beta}}$, for $e = N^\alpha$ and $p - q = N^\beta$.
Proposed attack when $\varphi(N)^{-1}$ have small multiplicative inverse	Sublattice based techniques with lower dimension	$(\varphi(N)^{-1} \bmod e) < N^{\frac{2\alpha-6\beta+2\sqrt{\alpha^2-\alpha\beta+4\beta^2}}{6}}$, for $e = N^\alpha$ and $p - q = N^\beta$.
Proposed attack when $\varphi(N)^{-1}$ have small multiplicative inverse and an attack bound on d	Lattice based techniques	$(\varphi(N)^{-1} \bmod e) < N^{\frac{1}{2}\alpha - \frac{1}{2}\gamma + \frac{1}{16}\gamma^2 - \frac{1}{16}\sqrt{48(\alpha-\gamma)\gamma^2 + 35\gamma^2}}$, for $e = N^\alpha$, $\max\{ k_0 , k_1 \} \leq N^{\gamma\alpha}$ and $\min\{ k_0 , k_1 \} \leq N^{7\alpha}$.
with composed prime sum $p + q = 2^n k_0 + k_1$	Sublattice based techniques	$(\varphi(N)^{-1} \bmod e), d < N^{\frac{1}{2}\alpha - \frac{1}{2}\gamma - \frac{1}{6}\sqrt{6(\alpha-\gamma)\gamma^2 + 5\gamma^2}}$, $\max\{ k_0 , k_1 \} \leq N^{\gamma\alpha}$ and $\min\{ k_0 , k_1 \} \leq N^{7\alpha}$.

Table 6.1: Attack bounds for all described attacks on RSA.

Enclosure-4

SUMMARY OF THE FINDINGS

Summary of the Findings

In 1990, M.J. Wiener was the first one to describe a cryptanalytic attack on the use of short RSA decryption exponent d . This attack is based on continued fraction algorithm which finds the fraction $\frac{t}{d}$ that is a convergent of $\frac{e}{N}$, where $t = \frac{ed-1}{\varphi(N)}$, in a polynomial time when $d < N^{0.25}$ for $N = pq$ and $q < p < 2q$.

The studies on Wiener's attack on RSA with small decryption exponents led to the refinement of attack bounds on the decryption exponent.

In 2000, D. Boneh and G. Durfee improved the Wiener bound on d from $N^{0.25}$ to $N^{0.292}$, for $q < p < 2q$ using lattice reduction theory.

In 2001, a lattice attack on RSA with short secret exponent d , for d less than $N^{0.29}$ was given by J. Blömer and A. May, this is slightly less than that of Boneh and Durfee but this method requires lattices of dimension smaller than the approach by Boneh and Durfee.

In 2002, B de Weger, for $d = N^\delta$, $p - q = N^\beta$ and $q < p < 2q$ extended the Wiener's attack in the range $N^{0.25} \leq d \leq N^{0.75-\beta}$, using continued fractions and the bound improved to $\delta < \frac{1}{6}(4\beta + 5) - \frac{1}{3}\sqrt{(4\beta + 5)(4\beta - 1)}$ using lattice based techniques in and the bound improved to $\delta < 1 - \sqrt{2\beta - \frac{1}{2}}$ using sub-lattice based techniques in under the condition $\delta > 2 - 4\beta$.

In 2008, Subhamoy Maitra and Santanu Sarkar instead of considering $p - q = N^\beta$, considered $|p - \rho q| \leq \frac{N^\gamma}{16}$ where $1 \leq \rho \leq 2$ to get the bound when $d = N^\delta$ and $\delta < \frac{1}{2} - \frac{\gamma}{2}$, for $|p - \rho q| \leq \frac{N^\gamma}{16}$ and $\gamma \leq \frac{1}{2}$ using continued fractions and also showed that this bound on δ can be extended using the lattice based techniques.

In 2006, E. Jochemsz and A. May gave a new attack on an RSA variant called common prime RSA. In 1995, R.G.E. Pinch in, proved that Wiener's attack on RSA Cryptosystem with small decryption exponent may be extended to RSA-like cryptosystems on elliptic curves and Lucas sequences.

In this project we described the refinement of all these attacks on RSA by categorizing the attacks as attacks based on continued fractions and attacks based on lattice reduction and proposed extensions of these attacks on RSA with respect to other variants of RSA and RSA-like cryptosystem over elliptic curves $E(\mathbb{Z}_{pq})$ due to KMOV.

We first described the **continued fraction** based attacks of M.J. Wiener and its extensions by B de Weger and Subhamoy Maitra and Santanu Sarkar and then proposed that the Wiener's extensions can also be extended to RSA-like Cryptosystem over elliptic curves $E(\mathbb{Z}_{pq})$ due to KMOV. Next we described the **lattice reduction** based attacks on RSA by Boneh-Durfee, Blömer-May, B de Weger and Maitra-Sarkar. All these existing lattice reduction based attacks are with respect to low

decryption exponent d of RSA.

We proposed the extensions of lattice reduction attacks on RSA with respect to small multiplicative inverse of $p - 1$ or $q - 1$ modulo e and with respect to small multiplicative inverse of $\varphi(N)$ modulo e , the public encryption exponent.

If $e = N^\alpha > p - 1$, r and s the multiplicative inverses of $p - 1$ and $q - 1$ modulo e respectively, then for (x_0, y_0) solution of the polynomial congruence $f(x, y) \equiv 0 \pmod{e}$, for $f(x, y) = x(y + A) - 1$ with $A = \lceil \sqrt{N} \rceil - 1$ and N^δ, N^γ upper bounds for x_0, y_0 respectively, we implemented the idea of Boneh and Durfee as in based on lattice reduction techniques to our polynomial congruence and proved that the attack works for $\delta < \frac{3\alpha + \gamma - 2\sqrt{\gamma(3\alpha + \gamma)}}{3}$ when both x and y shifts are used and $\delta < \frac{\alpha - \gamma}{2}$ when only x -shifts are used. Further we improved the bound for δ as $\alpha - \gamma(1 + \alpha) < \delta < \alpha - \sqrt{\alpha\gamma}$ and $\delta < \frac{2\alpha - 6\gamma + 2\sqrt{\alpha^2 - \alpha\gamma + 4\gamma^2}}{5}$ by implementing the sublattice based techniques of Boneh-Durfee and Blömer-May respectively.

We also extended the lattice attacks on RSA if the multiplicative inverse k of $\varphi(N)$ modulo e is small for $q < p < 2q$ and $e = N^\alpha > p + q$, the prime sum. This case can be considered even when both $(p - 1) \pmod{e}$ and $(q - 1) \pmod{e}$ do not have small inverses but $\varphi(N) \pmod{e}$ has small inverse. For $k \leq N^\delta$, the attack bounds for δ are described by repeating the above lattice based techniques. Further noted that for $\beta \approx 0.5$, the maximum bound for δ can be improved when the prime sum $p + q$ is in the composed form $p + q = 2^n k_0 + k_1$ for known positive integer n and for unknown suitably small integers k_0, k_1 . By using lattice based techniques to the polynomial congruence $f(x, y, z) \equiv 0 \pmod{e}$ for

$$f(x, y, z) = \begin{cases} (N + 1)x + xy + (2^n)xz - 1 & \text{if } |k_0| \leq |k_1| \\ 2^{n'}x(N + 1) + xy + 2^{n'}xz - 2^{n'} & \text{if } |k_1| \leq |k_0| \end{cases}$$

where $2^{n'}$ is an inverse of $2^n \pmod{e}$, the attack bound for δ is such that $\delta < \frac{1}{2}\alpha - \frac{1}{2}\gamma_1 + \frac{1}{16}\gamma_2 - \frac{1}{16}\sqrt{48(\alpha - \gamma_1)\gamma_2 + 33\gamma_2^2}$ where $N^{\gamma_1}, N^{\gamma_2}$ are the upper bounds for $\max\{|k_0|, |k_1|\}$, $\min\{|k_0|, |k_1|\}$ respectively. Later we slightly improved the previous bound by using the sub-lattice based techniques given by J. Blömer, A. May in to the above polynomial congruence and this method requires lattice of smaller dimension than the above method. The new bound on δ is $\frac{1}{2}\alpha - \frac{1}{2}\gamma_1 - \frac{1}{6}\sqrt{6(\alpha - \gamma_1)\gamma_2 + 3\gamma_2^2}$ and showed that this is a little bit greater than the former bound graphically. Note that this new attack bound is also an attack bound for the deciphering exponent d . The corresponding refinement of attack bounds in each case is depicted explicitly in tabular forms.

Enclosure-5

CONTRIBUTION TO THE SOCIETY

Contribution to the society

Many practical advantages of RSA in online banking email and many more, are primarily based on the security of RSA. Any study on the security analysis of RSA hence is a contribution to society. The security of RSA is based on factorization of composite number $N = pq$ for p, q prime numbers.

RSA can be attacked by factorization methods and also there are attacking methods based on the choices of parameters of RSA. This idea was initiated by M.J. Wiener using continued fractions.

This project contributes to society by analyzing the existing continued fraction based attacks and lattice based attacks and then further refine the attack bounds by proposing some more latticed based attacks.

The advantage of lattice based attacks proposed by us is that we considered the other invariant of RSA like $p, q, \varphi(N)$ and noted that these attacks can also be mounted for the private key exponent d not in the range of existing attack bounds.

It is also noted that looking at $\psi(N) = (p + 1)(q + 1)$ as the analogue of Euler's function $\varphi(N)$ in the RSA-like cryptosystem over elliptic curve $E(\mathbb{Z}_{pq})$ due to KMOV, all the lattice attacks can be extended to RSA-like cryptosystem over elliptic curve $E(\mathbb{Z}_{pq})$ due to KMOV. This may be adapted for other RSA-like cryptosystems with Dickson polynomials, Lucas sequences etc. by identifying the corresponding analogue to $\varphi(N)$.

All these attacks teach us to avoid the major difficulties while implementing RSA and sustain against all existing attacks. This study of refinement of attack bounds of RSA is useful in taking some precautionary measures in the adaptation of RSA according to the refinement of attack bounds.