Int. J. Math. And Appl., 6(1–C)(2018), 515–526

ISSN: 2347-1557

Available Online: http://ijmaa.in/

International Journal of *Mathematics And its Applications*

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. Jyotsna[1]

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.

1. Introduction

RSA Cryptosystem is the first public key cryptosystem invented by Ronald Rivest, Adi Shamir and Leonard Adalman 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 $m^{ed} = m \bmod N$, 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 $k = rs \bmod e$, 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 $(p-1) \bmod e$ and $(q-1) \bmod e$ do not have small inverses but $\varphi(N) \bmod e$ 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 $f(x,y) \equiv 0 \mod e$ 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 $u_1, u_2, ..., u_n \in \mathbb{Z}^m$ be linearly independent vectors with $n \leq m$. Let $\det(\mathscr{L})$ be a lattice spanned by $< u_1, u_2, ..., u_n >$. Let $b_1^*, b_2^*, ..., b_n^*$ be the vectors obtained by applying the Gram-Schmidt process to the vectors $u_1, u_2, ..., u_n$. The determinant of the lattice L is defined as $det(L) := \prod_{i=1}^{n} \parallel b_i^* \parallel$, where $\parallel . \parallel$ 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 $u_1, u_2, ..., u_n$.

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 ba lattice of dimension ω. In polynomial time, the LLL-algorithm outputs reduced basis vectors v_i, $1 \leq i \leq \omega$ that satisfy*

$$||v_1|| \leq ||v_2|| \leq ... \leq ||v_i|| \leq 2^{\frac{\omega(\omega-1)}{4(\omega+1-i)}} \det(\mathscr{L})^{\frac{1}{\omega+1-i}}.$$

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 $h(x_1, x_2, ..., x_n) = \sum a_{i_1 \dots i_n} x_1^{i_1} \dots x_n^{i_n}$ is defined by the Euclidean norm of its coefficient vector i.e., $||h(x_1,x_2,...,x_n)|| = \sqrt{\sum a^2_{i_1\ldots i_n}}$ given as follows:

Theorem 2.2 (Howgrave-Graham)**.** *Let $h(x_1,x_2,...,x_n) \in \mathbb{Z}[x_1,x_2,...,x_n]$ be an integer polynomial that consists of at most ω monomials. Suppose that*

(1). $h\left(x_1^{(0)},x_2^{(0)},...,x_n^{(0)}\right) \equiv 0 \bmod e^m$ for some m where $|x_1^{(0)}| < X_1, |x_2^{(0)}| < X_2 \ldots |x_n^{(0)}| < X_n$, and

(2). $||h(x_1X_1,x_2X_2,...,x_nX_n)|| < \frac{e^m}{\sqrt{\omega}}$.

Then $h((x_1,x_2,...,x_n) = 0$ holds over the integers.

Resultant of two polynomials: The resultant of two polynomials $f(x_1,x_2,\ldots,x_n)$ and $g(x_1,x_2,\ldots,x_n)$ with respect to the variable x_i for some $1 \le i \le n$, is defined as the determinant of Sylvester matrix of $f(x_1,x_2,\ldots,x_n)$ and $g(x_1,x_2,\ldots,x_n)$ when considered as polynomials in the single indeterminate x_i, for some $1 \le i \le n$.

Remark 2.3. *The resultant of two polynomials is non-zero if and only if the polynomials are algebraically independent .*

Remark 2.4. *If $\left(x_1^{(0)},x_2^{(0)},\ldots,x_n^{(0)}\right)$ is a common solution of algebraically independent polynomials $f_1,f_2,\ldots,f_m$ for $m \ge n$, then these polynomials yield $g_1,g_2,\ldots,g_{n-1}$ 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 $f(x,y) \equiv 0 \bmod e$. For $|x_0| \le N^\delta, |y_0| \le N^\gamma$, 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 $|x_0| \le X$ and $|y_0| \le Y$ 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 $(p-1)$ mod e or $(q-1)$ mod e has small inverse we may adapt the attack as in [8] but when both $(p-1)$ mod e and $(q-1)$ mod e do not have small inverses the $\varphi(N)$ mod e may have small inverse as in Table 1 then this modified attack proposed in the following may be used.

e	$\varphi(N)^{-1}$ mod e	$(p-1)^{-1}$ mod e	$(q-1)^{-1}$ mod 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	$\varphi(N)^{-1}$ mod e	$(p-1)^{-1}$ mod e	$(q-1)^{-1}$ mod 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 $\varphi(N)^{-1}$ mod e in the table, note $\varphi(N)^{-1}$ mod e is small but $(p-1)^{-1}$ mod e and $(q-1)^{-1}$ mod 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

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

Let $k = rs \bmod e$, then $k\varphi(N) \equiv 1 \bmod e$, 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 $g(x, y) \equiv 0 \bmod e$ (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 $\varphi(N)$ mod 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	δ			
	$(\approx)$	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 $\varphi(N)$ mod 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 $k(N+1-(p+q)) \equiv 1 \bmod e$ for $k = rs \bmod e$, the triple $(x_0, y_0, z_0) = (k, -k_1, -k_0)$ is a solution for the modular polynomial equation $f(x,y,z) \equiv 0 \bmod e$ for $f(x,y,z) = (N+1)x + xy + (2^n)xz - 1$ (observe that $|k_0| \bmod e = |k_0|$ and $|k_1| \bmod e = |k_1|$ as $e > p+q$). To apply the generalization of Howgrave-Graham result to find the small modular roots of the above equation $f(x,y,z) \equiv 0 \bmod e$, 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 $k = 0, ..., m$, $x^{i_1}y^{i_2}z^{i_3} \in M_k \backslash M_{k+1}$ 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 $i_1 = 0, ..., m,\ i_2 = 0, ..., i_1,\ i_3 = 0, ..., (i_1 - i_2)$ 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 $i_1 = k, ..., m,\ i_2 = k, ..., i_1,\ i_3 = 0, ..., (i_1 - i_2)$. Therefore $x^{i_1}y^{i_2}z^{i_3} \in M_k$ if $i_1 = k, ..., m, i_2 = k, ..., i_1, i_3 = 0, ..., (i_1 - i_2) + t$ and $x^{i_1}y^{i_2}z^{i_3} \in M_{k+1}$ if $i_1 = k+1, ..., m, i_2 = k+1, ..., i_1,$ $i_3 = 0, ..., (i_1 - i_2) + t$. From this, we obtain for $0 \leq k \leq m$,

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

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 $i_1 = i_2 = k$, $i_3 = 0,...,t$ 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 $i_1 = k+1,...,m$, $i_2 = k$, $i_3 = 0,...,(i_1-i_2)+t$. 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 $\mathscr{L}$ spanned by the coefficient of the vectors $g_{k,i_1,i_2,i_3}(xX,yY,zZ)$. For example, the matrix M of $\mathscr{L}$ when $m = 2$ and $t = 1$ is as given in the Table 3. Note that the matrix M of $\mathscr{L}$ is lower triangular matrix and the coefficient of the leading monomial of

$$g_{k,i_1,i_2,i_3}(x,y,z) = z^{i_3}(f(x,y,z))^k e^{m-k}, \text{ for } i_1 = i_2 = k, \ i_3 = 0,...,t \text{ is } X^kY^ke^{m-k}Z^{i_3} \text{ and}$$

$$g_{k,i_1,i_2,i_3}(x,y,z) = x^{i_1-k}z^{i_3}(f(x,y,z))^k e^{m-k}, \text{ for } i_1 = k+1,...,m, \ i_2 = k, \ i_3 = 0,...,(i_1-i_2)+t \text{ is}$$

$X^{i_1}Y^ke^{m-k}Z^{i_3}$. Also note that these coefficients are the diagonal elements of the matrix M, so the determinant is

$$det(\mathscr{L}) = e^{n_e}X^{n_X}Y^{n_Y}Z^{n_Z} \tag{5}$$

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 $\mathscr{L}$ 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 $\mathscr{L}$, i.e., coefficient vectors of the shift polynomials, we get a LLL-reduced basis say $\{v_1, v_2, ..., v_\omega\}$ and from the Theorem 1 we have

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

In order to apply the generalization of Howgrave-Graham result in Theorem 2, we need the following inequality

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

from this, we deduce

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

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 $\det(\mathscr{L}) < e^{m\omega}$.

Using (5), we get the inequality

$$e^{n_e} X^{n_X} Y^{n_Y} Z^{n_Z} < e^{m\omega}.$$

Substitute all values and taking logarithms, neglecting the lower order terms and after simplifying by m^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 $g_1(x_0,y_0,z_0) = g_2(x_0,y_0,z_0) = g_2(x_0,y_0,z_0) = 0$. 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*

$$\delta < \frac{1}{2}\alpha - \frac{1}{2}\gamma_1 + \frac{1}{6}\gamma_2 - \frac{1}{6}\sqrt{48(1-\gamma_1)\gamma_2 + 33\gamma_2^2}. \tag{6}$$

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	0	$(N+1)X^2Z^2e$	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 $g_{k,i_1,i_2,i_3}(xX, yY, zZ)$ 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 $2^{n'}$=$(2^n)^{-1} \bmod e$ then the triple $(k, -k_0, -k_1)$ is a solutions for the modular polynomial equation $f(x, y, z) \equiv 0 \bmod e$ 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 $\alpha - \sqrt{\frac{\alpha}{2}}$, 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 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 $\varphi(N) \bmod e$ 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	γ_1 = 0.25 γ_2 =0.249 - 0	0.00067 - 0.1255
					γ_1 =0.15 γ_2 = 0.149 - 0	0.07227 - 0.1755
					γ_1 =0.01 γ_2 = 0.009 - 0	0.21710 - 0.2455
0.55	0.025	0.0254519548	0.0255955759	0.0254626986	γ_1 = 0.25 γ_2 =0.225 - 0	0.02557 - 0.15
					γ_1 =0.15 γ_2 =0.149 - 0	0.09084 - 0.2
					γ_1 =0.01 γ_2 = 0.009 - 0	0.24021 - 0.27
0.75	0.125	0.1349307066	0.1376275643	0.1358898943	γ_1 = 0.25 γ_2 = 0.133 - 0	0.13687 - 0.25
					γ_1 =0.15 γ_2 =0.149 - 0	0.16923 - 0.3
					γ_1 =0.01 γ_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	$\gamma_1 = 0.25$ $\gamma_2 = 0.052$ - 0	0.29073 - 0.375
					γ_1 =0.15 $\gamma_2 = 0.116$ - 0	0.29005 - 0.425
					$\gamma_1 = 0.01$ γ_2 =0.009 - 0	0.45457 - 0.495

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 Kobliz, *A Course in Number Theory and Cryprography*, ISBN 3-578071-8, SPIN 10893308.

[14] A.Nitaj, *Another generalization of Wieners attack on RSA*, In: Vaudenay, S. (ed.) Africacrypt 2008. LNCS, 5023(2008), 174-190.

[15] K.H.Rosen, *Elemetary 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.