South East Asian J. of Mathematics and Mathematical Sciences
Vol. 17, No. 3 (2021), pp. 01-16

ISSN (Online): 2582-0850

ISSN (Print): 0972-7752

CRYPTANALYSIS OF RSA-LIKE CRYPTOSYSTEM WITH MODULUS $N = pq$ AND $ed \equiv 1(\text{mod } (p^2+p+1)(q^2+q+1))$

L. Jyotsna and L. Praveen Kumar

Department of Mathematical and Computational Sciences,
Sri Sathya Sai University for Human Excellence,
Kalaburagi - 585313, Karnataka, INDIA

E-mail : jyotsna.l@sssuhe.ac.in, praveen.l@sssuhe.ac.in

(**Received:** *Apr. 12, 2021* **Accepted:** *Oct. 28, 2021* **Published:** *Dec. 30, 2021)*

Abstract: In 2018, N. Murru and F. M. Saettone proposed a novel RSA-like cryptosystem with modulus $N = pq$ and $ed \equiv 1(\text{ mod } (p^2+p+1)(q^2+q+1))$ based on a generalization of the Rédei Rational functions. In this paper, we give some bounds on the deciphering exponent $d = N^\delta$, in which this RSA-like cryptosystem is insecure. For the enciphering exponent $e = N^\alpha$ and $p + q + 1 = N^\beta$, the attack bound on d is $\delta < \frac{2-(\alpha+\beta)}{3}$ in the case of $\alpha < 1$ and $\delta < \frac{\alpha-2\beta}{2}$ when $\alpha > 1$. Furthermore, we describe the magnitude of the bounds in all cases of α and β.

Keywords and Phrases: RSA-like cryptosystem, Cryptanalysis, LLL algorithm, Coppersmith's method.

2020 Mathematics Subject Classification: 11T71.

1. Introduction

RSA Cryptosystem [8] is the first public-key cryptosystem invented by Ronald Rivest, Adi Shamir, and Leonard Adleman in 1977 and is widely used for secure data transmission. RSA involves a public key and a private key. The public key (enciphering exponent) can be shared with everyone, whereas the private key (deciphering exponent) must be kept secret. The keys for the RSA algorithm are generated in the following way:

- Choose two distinct prime numbers p, q, and compute $N = pq$, the RSA modulus.

- Choose an integer e such that $1 < e < \varphi(N)$ and $\gcd(e, \varphi(N)) = 1$ where $\varphi(N)$ is Euler's totient function. The exponent e is released as the public key exponent.

- The private key exponent d is the multiplicative inverse of e modulo $\varphi(N)$, i.e., $ed \equiv 1 (\text{mod } \varphi(N))$.

The security of RSA based on the practical difficulty of factoring the product of two large prime numbers, the "factoring problem".

In 1990, M.J. Wiener [15] was the first one to describe a cryptanalytic attack on the use of short RSA decryption exponent d. The Wiener attack exploits the properties of continued fractions. Indeed, this attack utilized the estimate of $\varphi(N)$, i.e., $N - 3\sqrt{N} < \varphi(N) < N$, and is used to create inequality $\left|\frac{k}{d} - \frac{e}{N}\right| < \frac{1}{2d^2}$, where $k = \frac{ed-1}{\varphi(N)}$. This inequality discovered a sufficiently short secrete exponent, i.e., $d < N^{0.25}$. Wiener's bound was later subsequently improved to $d < N^{0.292}$ by Boneh and Durfee [1] [2]. Their method is based on Coppersmith's technique [4] for finding small solutions of modular polynomial equations, which in turn is based on the LLL lattice reduction algorithm [11]. In particular, they applied this technique for the modular equations $k(A + s) \equiv 1 (\text{mod } e)$, where $k = \frac{ed-1}{\varphi(N)}$, $s = \frac{-(p+q)}{2}$ and $A = \frac{N+1}{2}$.

In 2018, N. Murru and F. M. Saettone presented a novel RSA-like cryptosystem based on a generalization of the Rédei Rational functions [12]. In this cryptosystem they considered modulo $N = pq$ and the enciphering exponent e and the deciphering exponent d are such that $ed \equiv 1 (\text{mod } (p^2+p+1)(q^2+q+1))$. In this scheme, the role of $\varphi(N)$ in RSA is substituted by $(p^2+p+1)(q^2+q+1))$. So Wiener's and Boneh-Durfee's attacks are not affected as the inequalities $\left|\frac{k}{d} - \frac{e}{N}\right| < \frac{1}{2d^2}$ and the modular equation $k(A + s) \equiv 1 (\text{mod } e)$ not hold in this case. Using the proposed scheme, the deciphering exponent d could be less than the attack bounds on d, given by Wiener and Boneh-Durfee without being affected by their attacks.

In this paper, we show that if $d < N^{\frac{2-(\alpha+\beta)}{3}}$ for $e < N$ and $d < N^{\frac{\alpha-2\beta}{2}}$ for $e > N$, where $e = N^\alpha$ and $p + q + 1 = N^\beta$ then this RSA-like cryptosystem is insecure. This method makes use of Coppersmith's technique for finding small solutions of modular polynomial equations [4]. Applying this technique to the modular equation $ed \equiv 1 + t(p + q + 1)(N - 1) + t(2N - 1) (\text{mod } N^2)$ in the case of $e < N$ and $1 + t((p + q + 1)^2 + (p + q + 1)(N - 1) + (N - 1)^2 \equiv 0 (\text{mod } e)$ when $e > N$, we get the first and second attack bounds for d respectively, where $t = \frac{ed-1}{(p^2+p+1)(q^2+q+1)}$. Later, we notice that for some values of α and β, our bounds may reach or overcome the Wiener and Boneh-Durfee's attack bounds on d.

2. Preliminaries

In this section, we state basic results on lattice, lattice basis reduction, Coppersmith's method, and Howgrave-Graham theorem that are based on lattice reduction techniques.

Definition 1. *Let $\boldsymbol{b}_1, \boldsymbol{b}_2, ..., \boldsymbol{b}_n \in \mathbb{R}^m$ be a set of linearly independent vectors. The lattice L generated by $\boldsymbol{b}_1, \boldsymbol{b}_2, ..., \boldsymbol{b}_n$ is the set of linear combinations of $\boldsymbol{b}_1, \boldsymbol{b}_2, ..., \boldsymbol{b}_n$ 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 [6].

Let $b_1, b_2, ..., b_n \in \mathbb{Z}^m$and $\{b_1, b_2, ..., b_n\}$ be a basis for L with $n \leq m$. 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 $b_1, b_2, ..., b_n$. If $b = \sum_{i=1}^{n} \lambda_i b_i$ is a vector of L, the Euclidean norm of b is $||b|| = \left(\sum_{i=1}^{n} \lambda_i^2\right)^{\frac{1}{2}}$.

A lattice has infinitely many bases with the same determinant and it is useful to find a basis of small vectors. However, finding the shortest nonzero vector in a lattice is very hard in general.

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. (LLL) *Let L be a lattice of dimension ω. In polynomial time, the LLL-algorithm outputs a reduced basis $b_1, b_2, \cdots, b_\omega$ that satisfy*

$$||b_1|| \leq ||b_2|| \leq \cdots ||b_i|| \leq 2^{\frac{\omega(\omega-1)}{4(\omega+1-i)}} \det(L)^{\frac{1}{\omega+1-i}},$$

for all $i = 1, \cdots, \omega$. [11]

An important application of lattice reduction found by Coppersmith in 1996 [4] is finding small roots of low-degree polynomial equations. This includes modular univariate polynomial equations and bivariate integer equations. In 1997 Howgrave-Graham [5] reformulated Coppersmith's techniques and proposed the following result and it shows that if the coefficients of $h(x_1, x_2, ..., x_n)$ 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 $h(x_1, x_2, ..., x_n) = \sum a_{i_1 ... i_n} x_1^{i_1} ... x_n^{i_n}$ is defined by the Euclidean norm of its coefficient vector i.e., $||h(x_1, x_2, ..., x_n)|| = \sqrt{\sum a_{i_1 ... i_n}^2}$ given

as follows:

Theorem 2. (Howgrave-Graham's Theorem): *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.*

Definition 2. *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* $1 \leq i \leq n$, *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* $1 \leq i \leq n$.

Remark 1. *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* $m \geq n$, *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. An Attack on RSA-like Cryptosystem with Modulus $N = pq$ and $ed \equiv 1 (\bmod\ ((p^2 + p + 1)(q^2 + q + 1))$

In this section, we propose the given scheme is insecure for specific bounds on d, which depends on the range of e. In paper [12], N. Murru and F. M. Saettone presented an RSA-like cryptosystem, in which the enciphering e and deciphering d exponents satisfying the modular equation $ed \equiv 1 (\bmod\ (p^2 + p + 1)(q^2 + q + 1))$, where the modulus $N = pq$. If the deciphering exponent d is sufficiently small, then it can be effectively recovered by using attacks like Wiener [15], Boneh-Durfee [2], Wegar [14] and Sarkar-Maitra [10] on RSA and these attacks depending on $\varphi(N)$. However, those kinds of attacks fail in this strategy, as they replaced $(p^2 + p + 1)(q^2 + q + 1)$ instead of $\varphi(N)$. In that context, this section describes an attack on the system by giving bounds on d using Coppersmith's techniques.

3.1. An Attack Bound on d when $e > N$

In this section, for the case of $e > N$ we present the procedure for finding the bound on d where this cryptosystem is insecure.

As $ed \equiv 1(\text{mod } (p^2+p+1)(q^2+q+1))$, there exists $t, t = \frac{ed-1}{(p^2+p+1)(q^2+q+1)}$ such that $ed = 1 + t((p^2+p+1)(q^2+q+1))$. This can be rewrite as $\frac{ed-1}{t} = N^2 + N(p+q+1) + (p+q+1) + p^2 + q^2$. Now add and subtract with $(p+q+1)^2$ to the R.H.S of the above equation. After that, we obtain an equation $ed = 1 + t((p+q+1)^2 + (p+q+1)(N-1) + (N-1)^2)$. This leads a modular equation

$$1 + t((p+q+1)^2 + (p+q+1)(N-1) + (N-1)^2) \equiv 0(\text{mod } e). \tag{1}$$

Take $t = x, p+q+1 = y$, then (1) becomes

$$1 + (N-1)^2 x + (N-1)xy + xy^2 \equiv 0(\text{mod } e). \tag{2}$$

Consider the polynomial $f(x,y) = 1+(N-1)^2x+(N-1)xy+xy^2$. Then $(x_0, y_0) = (t, p+q+1)$ is a root modulo e. Define

$$e = N^\alpha,\ p+q+1 = N^\beta \text{ and } d = N^\delta.$$

We have $t = \frac{ed-1}{(p^2+p+1)(q^2+q+1)} \approx \frac{ed}{(p^2+p+1)(q^2+q+1)}$. Since $e < (p^2+p+1)(q^2+q+1)$, $\frac{ed}{(p^2+p+1)(q^2+q+1)} < d$.
So $t < N^\delta$.
Let $X = N^\delta$ and $Y = N^\beta$, then the bounds for x_0 and y_0 are X and Y, respectively.

To apply Coppersmith's method [4] to find the small modular roots of the equation $f(x,y) \equiv 0\ (\text{mod } e)$, we first use the basic strategy of Jochemsz and May [7]. For $k \in \{0, \cdots, m\}$, define the set

$$M_k = \{x^i y^j; x^i y^j \text{ is a monomial of } f^m \text{ and } \frac{x^i y^j}{(xy^2)^k} \text{ is a monomial of } f^{m-k}\},$$

where xy^2 is a leading monomial of f , with coefficient 1. Observe that

$$x^i y^j \in f^m \text{ if } i = 0, \cdots, m, j = 0, \cdots, 2i \text{ and } \frac{x^i y^j}{(xy^2)^k} \in f^{m-k} \text{ if } x^{i-k} y^{j-2k} \in f^{m-k.}$$

That is

$$x^i y^i \in M_k \text{ if } i = 0, \cdots, m, j = 0, \cdots, 2i \text{ and } i = k, \cdots, m, j = 2k, \cdots, 2i.$$

For $k = 0, \cdots, m$, we obtain $x^i y^j \in M_k$ if $i = k, \cdots, m, j = 2k, \cdots, 2i$ and $x^i y^j \in M_{k+1}$ if $i = k+1, \cdots, m, j = 2k+2, \cdots, 2i$.
From this, we deduce

$$x^i y^j \in M_k \setminus M_{k+1} \text{ if } i = k, j = 2k \text{ and } i = k+1, \cdots, m, j = 2k, 2k+1.$$

Next, we define the following shift polynomials:

$$g_{k,i,j}(x,y) = \frac{x^i y^j}{(xy^2)^k}(f(x,y))^k e^{m-k}, \text{ for } k = 0, \cdots m \text{ and } x^i, y^j \in M_k \setminus M_{k+1}.$$

These polynomials can be altered as the following two different forms, i.e.,

$$\begin{aligned} G_{k,i,j}(x,y) =& \frac{x^i y^j}{(xy^2)^k}(f(x,y))^k e^{m-k}, \text{ for } k = 0, \cdots m \text{ and } i = k, j = 2k. \\ H_{k,i,j}(x,y) =& \frac{x^i y^j}{(xy^2)^k}(f(x,y))^k e^{m-k}, \text{ for } k = 0, \cdots m \\ & \text{and } i = k+1, \cdots, m, j = 2k, 2k+1. \end{aligned}$$

Define the lattice $\mathcal{L}$ spanned by the coefficients of the vectors $G_{k,i,j}(xX, yY)$ and $H_{k,i,j}(xX, yY)$. Notice that the matrix M of $(\mathcal{L})$ is lower triangular. For $k = 0, \cdots, m$, the coefficient of the leading monomial in $G_{k,i,j}(xX, yY)$ is $X^i Y^j$, $i = k$, $j = 2k$ and in $H_{k,i,j}(xX, yY)$ is $X^i Y^j$, $i = k+1, \cdots, m$, $j = 2k, 2k+1$ and these coefficients are the diagonal elements of the matrix M , so the determinant is

$$\det(\mathcal{L}) = e^{n(e)} X^{n(X)} Y^{n(Y)}, \tag{3}$$

where $n(e), n(X), n(Y)$ are the number of e's, X's, Y's in all diagonal elements respectively, and

$$\begin{aligned} n(e) &= \sum_{k=0}^{m} \sum_{i=k} \sum_{j=2k} (m-k) + \sum_{k=0}^{m} \sum_{i=k+1}^{m} \sum_{j=2k}^{2k+1} (m-k) \\ &= \frac{m}{6}(4m+5)(m+1), \\ n(X) &= \sum_{k=0}^{m} \sum_{i=k} \sum_{j=2k} i + \sum_{k=0}^{m} \sum_{i=k+1}^{m} \sum_{j=2k}^{2k+1} i \\ &= \frac{m}{6}(4m+5)(m+1), \\ n(Y) &= \sum_{k=0}^{m} \sum_{i=k} \sum_{j=2k} j + \sum_{k=0}^{m} \sum_{i=k+1}^{m} \sum_{j=2k}^{2k+1} j \\ &= \frac{m}{6}(4m+5)(m+1), \text{ and the dimension } \omega \text{ of } (\mathcal{L}) \text{ is} \\ \omega &= \sum_{k=0}^{m} \sum_{i=k} \sum_{j=2k} 1 + \sum_{k=0}^{m} \sum_{i=k+1}^{m} \sum_{j=2k}^{2k+1} 1 \\ &= (m+1)^2. \end{aligned}$$

For sufficiently large m, the exponents $n(e), n(X), n(Y)$ and the dimension ω reduce to

$$\begin{aligned} n(e) &= \frac{2}{3}m^3 + o(m^2), \\ n(X) &= \frac{2}{3}m^3 + o(m^2), \\ n(Y) &= \frac{2}{3}m^3 + o(m^2), \text{ and} \\ \omega &= m^2 + o(m) \end{aligned}$$

Apply the LLL algorithm to the basis vectors of the lattice $\mathcal{L}$, i.e., coefficient vectors of the shift polynomials. Then from the Theorem 1, we get a LLL-reduced basis say $b_1, b_2, ..., b_\omega$ and we have

$$||b_1|| \leq ||b_2|| \leq 2^{\frac{\omega(\omega-1)}{4(\omega-1)}} \det(\mathcal{L})^{\frac{1}{\omega-1}},$$

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

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

This implies

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

As the dimension ω is not depending on the public encryption exponent e, $\frac{1}{\left(2^{\frac{\omega(\omega-1)}{4(\omega-1)}}\sqrt{\omega}\right)^{\omega-1}}$ is a fixed constant.

So we need the inequality $\det(\mathcal{L}) < e^{m\omega}$. Using (3), we get the inequality

$$e^{n(e)} X^{n(X)} Y^{n(Y)} < e^{m\omega}.$$

Substitute all values and taking logarithms, neglecting the lower order terms and after simplifying by m^3 we get

$$\frac{2}{3}\alpha + \frac{2}{3}\delta + \frac{2}{3}\beta < \alpha.$$

From this inequality, the bound for δ is

$$\delta < \frac{\alpha}{2} - \beta. \tag{4}$$

Now, we analyze the outcome of the attack on the size of the deciphering exponent d that going through the extended strategy [7].

Define the set

$$M'_k = \bigcup_{0 \le j' \le t'} \{x^i y^{j+j'}; x^i y^j \text{ is a monomial of } f^m \text{ and } \frac{x^i y^j}{(xy^2)^k} \text{ is a monomial of } f^{m-k}\},$$

where xy^2 is the leading monomial of f and define the shift polynomials as

$$g'_{k,i,j}(x,y) = \frac{x^i y^j}{(xy^2)^k}(f(x,y))^k e^{m-k}, \text{ for } k = 0, \cdots, m \text{ and } x^i, y^j \in M'_k \setminus M'_{k+1}.$$

and $x^i, y^j \in M'_k \setminus M'_{k+1}$ if

$$\begin{cases} k = 0, \cdots, m-1 \\ i = k, \\ i = 2k \end{cases} \text{(or)} \begin{cases} k = 0, \cdots, m-1, \\ i = k+1, \cdots, m, \cdots, m+t', \\ i = 2k, 2k+1 \end{cases} \text{(or)} \begin{cases} k = m, \\ i = m, \cdots, m+t' \\ i = 2m. \end{cases}$$

Consequently, these polynomials $g'_{k,i,j}(x,y)$ are in one of the following forms

$$\begin{aligned} G'_{k,i,j}(x,y) &= x^{i-k} y^{j-2k} f^k e^{m-k}, \text{ for } k = 0, \cdots, m-1, i = k, j = 2k, \\ H'_{k,i,j}(x,y) &= x^{i-k} y^{j-2k} f^k e^{m-k}, \text{ for } k = 0, \cdots, m-1, i = k+1, \cdots, m+t', j = 2k, 2k+1, \\ I'_{k,i,j}(x,y) &= x^{i-k} y^{j-2k} f^k e^{m-k}, \text{ for } k = m, i = m, \cdots, m+t', j = 2m. \end{aligned}$$

Let $\mathcal{L}'$ be the lattice spanned by the three vectors $G'_{k,i,j}(x,y), H'_{k,i,j}(x,y)$, and $I'_{k,i,j}(x,y)$ and M' be the matrix of $\mathcal{L}'$.

Then note that M is lower triangular and the coefficient of the leading monomial of three vectors are $X^i y^j$, for $k = 0, \cdots, m-1, i = k, j = 2k,$, $X^i y^j$, for $k = 0, \cdots, m-1, i = k+1, \cdots, m+t', j = 2k, 2k+1$, and $X^i y^j$ for $k = m, i = m, \cdots, m+t', j = 2m$ respectively. Accordingly, the determinant is

$$\det(\mathcal{L}') = e^{n(e)} X^{n(X)} Y^{n(y)}, \tag{5}$$

where

$$\begin{aligned}
n(e) &= \sum_{k=0}^{m-1}\sum_{i=k}\sum_{j=2k}(m-k) + \sum_{k=0}^{m-1}\sum_{i=k+1}^{m+t}\sum_{j=2k}^{2k+1}(m-k) + \sum_{k=m}\sum_{i=m}^{m+t}\sum_{j=2m}(m-k) \\
&= \frac{2}{3}m^3 + \frac{3}{2}m^2 + (m^2+m)t + \frac{5}{6}m \\
n(X) &= \sum_{k=0}^{m-1}\sum_{i=k}\sum_{j=2k} i + \sum_{k=0}^{m-1}\sum_{i=k+1}^{m+t'}\sum_{j=2k}^{2k+1} i + \sum_{k=m}\sum_{i=m}^{m+t'}\sum_{j=2m} i \\
&= \frac{2}{3}m^3 + mt^2 + \frac{3}{2}m^2 + (2m^2+m)t + \frac{1}{2}(2m+1)t' + \frac{1}{2}t'^2 + \frac{5}{6}m \\
n(Y) &= \sum_{k=0}^{m-1}\sum_{i=k}\sum_{j=2k} j + \sum_{k=0}^{m-1}\sum_{i=k+1}^{m+t'}\sum_{j=2k}^{2k+1} j + \sum_{k=m}\sum_{i=m}^{m+t'}\sum_{j=2m} j \\
&= \frac{2}{3}m^3 + \frac{3}{2}m^2 + (2m^2-m)t' + 2mt' + \frac{5}{6}m \\
\text{dimension } \omega' &= \sum_{k=0}^{m-1}\sum_{i=k}\sum_{j=2k} 1 + \sum_{k=0}^{m-1}\sum_{i=k+1}^{m+t'}\sum_{j=2k}^{2k+1} 1 + \sum_{k=m}\sum_{i=m}^{m+t'}\sum_{j=2m} 1 \\
&= m^2 + 2mt' + 2m + t' + 1
\end{aligned}$$

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

$$\begin{aligned}
n(e) &= \left(\frac{2}{3} + \tau\right) m^3 + o(m^3) \\
n(X) &= \left(\frac{2}{3} + \tau^2 + 2\tau\right) m^3 + o(m^3) \\
n(Y) &= \left(\frac{2}{3} + 2\tau\right) m^3 + o(m^3) \\
\omega &= (1+2\tau)m^2 + o(m^2)
\end{aligned} \tag{6}$$

By employing the preceding argument to the lattice $\mathcal{L}'$, the generalization of Howgrave-Graham result holds if $\det(\mathcal{L}') < e^{m\omega}$.
Using (5) as well as the values (6) and neglecting the lower order terms, we get the inequality

$$N^{\left(\alpha\left(\left(\frac{2}{3}+\tau\right)m^3\right)\right)+\delta\left(\left(\frac{2}{3}+\tau^2+2\tau\right)m^3\right)+\beta\left(\left(\frac{2}{3}+2\tau\right)m^3\right)\right)} < N^{\left(\alpha((1+2\tau)m^2)\right)m}.$$

From this, we deduce

$$\alpha\left(-\frac{1}{3}-\tau\right)+\delta\left(\frac{2}{3}+\tau^2+2\tau\right)+\beta\left(\frac{2}{3}+2\tau\right)<0$$

and the left hand side is minimized with the value $\tau_0=\frac{\alpha-2\delta-2\beta}{2\delta}$.

Substitute $\tau=\tau_0$ in the inequality, we get the bound for δ, i.e.,

$$\delta<\frac{\alpha}{2}-\beta \tag{7}$$

Observe that the value $\tau_0>0$ as $t'=\tau m>0$ and $\tau_0>0$ if $\alpha>1$.
Thus, in this approach, the Howgrave-Graham result applicable if

$$\delta<\frac{\alpha}{2}-\beta \text{ and } \alpha>1. \tag{8}$$

Proposition 1. *Let $d=N^\delta$, the deciphering exponent. The attack bounds for δ obtained via implementing both basic and extended strategy are the same, nevertheless the basic approach requires a smaller dimension than the extended technique.*
Proof. From (4) and (7), we can conclude that the two approaches have the same bounds on δ. We have $\omega=(m+1)^2$ and $\omega'=m^2+2mt'+2m+t'+1$, the dimensions obtained in the basic and extended strategies, respectively. As $t'\geq 1$, $\omega<\omega'$.

Note 1. *In terms of dimension, it is advisable to choose the primary method for this outcome.*

Lemma 1. *Let $N=pq$ be the modulus of a given RSA-like cryptosystem. Then the prime factors p and q satisfy the following properties*

$$p+q+1>N^{0.5} \text{ (or) } p+q+1\approx N^{0.5}$$

Proof. As $N=pq$, either $p<N^{0.5}$ and $q>N^{0.5}$ or vice versa. So, the inequality $p+q+1>N^{0.5}$ contains in both cases.
If balanced primes are chosen like in RSA, that is, $q<p<2q$ with $p>N^{0.5}$ and $q<N^{0.5}$, then the inequality $p+q+1\leq 3N^{0.5}$ holds. Therefore, $p+q+1\approx N^{0.5}$ for large prime factors p and q.

Note 2. *From the preceding Lemma and (8), it follows that the bound for δ valid only if $\alpha>1$ in both strategies.*

Theorem 3. *Let $N=pq$ be the modulus of an RSA-like cryptosystem with $ed\equiv 1(\mod((p^2+p+1)(q^2+q+1)))$ where e, d are enciphering and deciphering*

exponents respectively. If $d = N^{\delta}$, $e = N^{\alpha}$, and $p + q + 1 = N^{\beta}$, then N can be factorized in polynomial time if

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

and this bound is efficient only if $\alpha > 1$.

Proof. Take any of the previous methods to get

$$||b_1|| \leq ||b_2|| < \frac{e^m}{\sqrt{\omega}} \text{ when } \delta < \frac{\alpha}{2} - \beta.$$

Suppose $\delta < \frac{\alpha}{2} - \beta$. Then from the two vectors $b_1(xX, yY)$ and $b_2(xX, yY)$, we obtain two polynomials $h_1(x, y)$ and $h_2(x, y)$ with the common root (x_0, y_0). Let $g(y)$ be the resultant polynomial of $h_1(x, y)$ and $h_2(x, y)$ with respect of x. From the Remark 1, $g(y)$ is not identically zero. If $x_0 < N^{\delta}$ and $y_0 < N^{\beta}$ are small such that $\delta < \frac{\alpha}{2} - \beta$, then $g(y) = 0$ holds over the integers. Find the root $y_0 = p + q + 1$ using the polynomial $g(y)$. With the knowledge of $p + q$ and pq, one can obtain the values of p and q, factors of N.

The condition regarding the efficiency of the bound for δ is coming from Note 2.

3.2. An Attack Bound on d when $e < N$

In this section, we find an attack bound on d for small e, that is, $e < N$, by changing the above modular equation.

In the previous section, consider the equation $ed = 1 + t(N(p^2 + p + 1) + (p + q + 1) + p^2 + q^2 + N)$. After adding and subtracting with $(p + q + 1)^2$ to this equation, we get

$$ed = 1 + t\left((p + q + 1)(N + 1 - 2) + 1 - 2N + N^2\right).$$

This can be written as the modular equation

$$ed \equiv 1 + t(p + q + 1)(N - 1) + t(2N - 1) (\text{mod } N^2).$$

Subsequently, the tuple $(x, y, z, w) = (t, p + q + 1, d, e)$ is a solution to the modular equation

$$1 + xy(N - 1) + x(2N - 1)) - zw \equiv 0 \ (\text{mod } N^2).$$

Define $e = N^{\alpha}, p + q + 1 = N^{\beta}, d = N^{\delta}$, and $t = N^{\gamma}$.

Let $X = N^{\delta}, Y = N^{\beta}$, and $W = N^{\alpha}$, then X, Y, X, and W are the bounds of x, y, z and w, respectively.

Directly implement the basic scheme presented in Section 3.1 to the above modular

equation with the leading monomial zw. Consequently, we get the attack bound on δ is

$$\delta < \frac{2-(\alpha+\beta)}{3} \tag{9}$$

and the dimension ω of the corresponding lattice is $\frac{1}{6}m^3 + m^2 + \frac{11}{6}m + 1$.

Now, define the set $M'_k = \bigcup_{0 \le j' \le t'} \{x^{i_1}y^{i_2}z^{i_3+j'}w^{i_4}; x^{i_1}y^{i_2}z^{i_3}w^{i_4}$ is a monomial of f^m and $\frac{x^{i_1}y^{i_2}z^{i_3}w^{i_4}}{(zw)^k}$ is a monomial of $f^{m-k}\}$,

where $f(x,y,z,w) = 1 + xy(N-1) + x(2N-1) - zw$ with the leading monomial zw

Employ an extended procedure similar to that in Section 3.1. After performing, we obtain the attack bound on δ is

$$\delta < \frac{2-(\alpha+\beta)}{3}, \tag{10}$$

and the corresponding lattice dimension ω' is $\frac{1}{6}m^3 + m^2 + \frac{1}{6}(m^3+3m^2+2m)t' + \frac{1}{2}(m^2+3m+2)t' + \frac{11}{6}m + 1$.

Remark 2. *The bounds in (9) and (10) obtained using the two schemes are identical and effective if $\alpha < 1$ as $N^\beta = p + q + 1 < N$.*

Remark 3. *As $t' \ge 1$, $\omega < \omega'$. So regarding the dimension, it is preferable to implement the basic method for this result.*

Theorem 4. *Let $N = pq$ be the modulus of an RSA-like cryptosystem with $ed \equiv 1(\mod((p^2+p+1)(q^2+q+1)))$ where e, d are enciphering and deciphering exponents respectively. If $d = N^\delta$, $e = N^\alpha$, and $p + q + 1 = N^\beta$, then N can be factorized in polynomial time if*

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

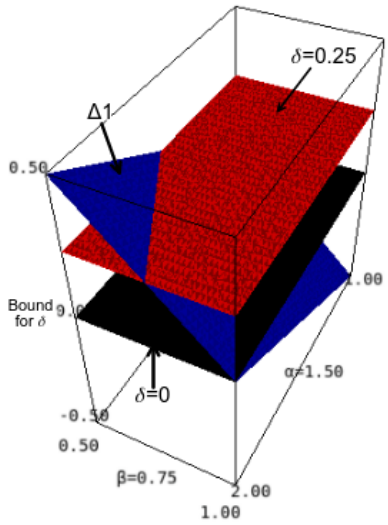
and this bound is efficient if $\alpha < 1$.

Proof. From (9) and using the process in the proof of Theorem 4, we get this result.

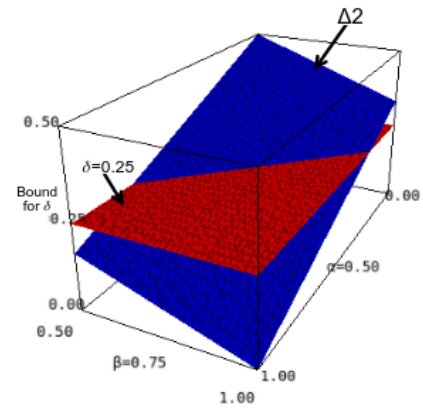
4. Analysis of Attack Bounds on d

In the image above, we have depicted the x-axis, y-axis, and z-axis as α, β, and 'Bound for δ' respectively. Take $\Delta_1 = \frac{\alpha}{2} - \beta$, then Δ_1 is an attack bound to the δ when $\alpha > 1$, as shown in Figure (a). In Figure (a), we can see that the bound Δ_1 at some points of the α and β is above the graph of $\delta = 0.25$ (Weiner's bound).

Note that at some values of α and β, the fraction of the bound Δ_1 is below the graph of $\delta = 0$, and for those values i.e., $2\beta > \alpha$, we can not find an attack bound because here $\Delta_1 < 0$.



(a) Bound for δ when $\alpha > 1$



(b) Bound for δ when $\alpha < 1$

In Figure (b), we represented $\Delta_2 = \frac{2-(\alpha+\beta)}{3}$, which is an attack bound to the δ when $\alpha < 1$. At each value of α and β, this bound is always greater than zero. It can be viewed in Figure (b) that some portion of Δ_2 is above the graph of $\delta = 0.25$ in a few cases of α and β.

Note 4. *If $2\beta > \alpha$ and $\alpha > 1$, then the bound Δ_2 can be used when $\beta < \frac{2}{3}$. In that context, the size of Δ_2 is between 0 and $\frac{1}{6}$.*

5. Conclusion

In this paper, we attack a novel RSA-like cryptosystem with modulus $N = pq$ and $ed \equiv 1 \pmod{(p^2+p+1)(q^2+q+1)}$ by giving bounds on deciphering exponent $d = N^\delta$ in both cases of enciphering exponent $e = N^\alpha$ less than and greater than N. The method is based on transforming the key equation $ed = 1 + t((p^2 + p + 1))(q^2 + q + 1)$ into the two modular equations $f(x, y) = 1 + (N - 1)^2x + (N - 1)xy + xy^2 \equiv 0 \pmod{e}$ for $\alpha > 1$ and $f(x, y, z, w) = 1 + xy(N - 1) + x(2N - 1) - zw \equiv 0 \pmod{N^2}$ for $\alpha < 1$ where $(x_0, y_0) = (t, p + q + 1)$ and $(x_0, y_0, z_0, w_0) = (t, p+q+1, d, e)$ are the solution of the first and second equations, respectively. Using Coppersmith's technique and the LLL algorithm, we obtain the attack bounds on δ, and within those bounds, we can find $p + q + 1 = N^\beta$, which

leads to the factorization of N. At some values of α and β, we later observe that our attack bounds on δ could reach or overcome the Weiner and Bone-Durfee's bound in the RSA. In future, this method can be extended to implement lattice-based attacks on the RSA given in [3] [10] [13] [14] for our polynomial congruences.

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 Eurocrypt-99, Lecture Notes in Computer Science Vol. 1592, Springer-Verlag, (1999), 1-11.

[3] Blömer J., May A., Low Secret Exponent RSA Revisited, Cryptography and Lattice Conference (CaLC 2001), Lecture Notes in Computer Science Volume 2146, Springer-Verlag, (2001), 4-19.

[4] Coppersmith, D., Small solutions to polynomial equations, and low exponent RSA vulnerabilities, Journal of Cryptology, 10(4) (1997), 233-260.

[5] Howgrave-Graham, N., Finding small roots of univariate modular equations revisited, In Cryptography and Coding, LNCS 1355, Springer-Verlag, (1997), 131-142.

[6] Hoftstein, J., Pipher, J., Silverman, J. H., An Introduction to Mathematical Cryptography, Springer: Berlin, Germany, (2008).

[7] Jochemsz, E., May, A., A strategy for finding roots of multivariate polynomials with new applications in attacking RSA variants, in: ASIACRYPT 2006, LNCS, Springer-Verlag, Vol. 4284, (2006), 267–282.

[8] Neal Kobliz, A Course in Number Theory and Cryprography, SPIN 10893308.

[9] Lenstra, A. K., Lenstra, H. W., Lov´asz, L. Factoring polynomials with rational coefficients, Mathematische Annalen, Vol. 261 (1982), 513-534.

[10] Maitra Subhamoy and Sarkar Santanu, 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.

[11] May A., New RSA Vulnerabilities Using Lattice Reduction Methods, PhD thesis, University of Paderborn (2003).
http://wwwcs.upb.de/cs/ag-bloemer/personen/alex/publikationen/

[12] Murru Nadir and Francesco M. Saettone, A Novel RSA-Like Cryptosystem Based on a Generalization of the Rédei Rational Functions, In: Kaczorowski J., Pieprzyk J., Pomykała J. (eds) Number-Theoretic Methods in Cryptology. NuTMiC 2017. Lecture Notes in Computer Science, Vol. 10737 (2018), 91-103. Springer, Cham.

[13] Nitaj A., Douh M. O., A new attack on RSA with a composed decryption exponent, Int. J. Crypt. Inf. Secur. (IJCIS), 3(4) (2013), 1121.

[14] Weger B. de, Cryptanalysis of RSA with Small Prime Difference, Applicable Algebra in Engineering, Communication and Computing, 13(1) (2002), 17-28.

[15] Wiener M., Cryptanalysis of Short RSA Secret Exponents, IEEE Transactions on Information Theory, 36(3) (1990), 553-558.