Exponential Increment of RSA Attack Range via Lattice Based Cryptanalysis

Abderahmanne Nitaj, Muhammad Rezal Kamel, Nurul Nur Hanisah Adenan, Domenica Stefania Merenda, Ali Ahmadian

▶ **To cite this version:**

Abderahmanne Nitaj, Muhammad Rezal Kamel, Nurul Nur Hanisah Adenan, Domenica Stefania Merenda, Ali Ahmadian. Exponential Increment of RSA Attack Range via Lattice Based Cryptanalysis. Multimedia Tools and Applications, 2021, 10.1007/s11042-021-11335-8 . hal-03441724

HAL Id: hal-03441724
https://hal.science/hal-03441724v1

Submitted on 22 Nov 2021

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Exponential Increment of RSA Attack Range via Lattice Based Cryptanalysis

Abderahmanne Nitaj[1], Muhammad Rezal Kamel Ariffin[2,3,*] Nurul Nur Hanisah Adenan[2], Domenica Stefania Merenda[4], and Ali Ahmadian[4,5]

[1] Normandie Univ, UNICAEN, CNRS, LMNO, 14000 Caen, France
[2] Institute for Mathematical Research, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor Darul Ehsan, Malaysia
[3] Department of Mathematics, Faculty of Science, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor Darul Ehsan, Malaysia
[4] DiGiS & Decisions Lab, Mediterranea University of Reggio Calabria, Reggio Calabria, 89125, Italy
[5] Institute of IR 4.0, The National University of Malaysia, Bangi, 43600 UKM, Selangor, Malaysia
*rezal@upm.edu.my

Abstract. The RSA cryptosystem comprises of two important features that are needed for encryption process known as the public parameter e and the modulus N. In 1999, a cryptanalysis on RSA which was described by Boneh and Durfee focused on the key equation $ed - k\phi(N) = 1$ and e of the same magnitude to N. Their method was applicable for the case of $d < N^{0.292}$ via Coppersmith's technique. In 2012, Kumar et al. presented an improved Boneh-Durfee attack using the same equation which is valid for any e with arbitrary size. In this paper, we present an exponential increment of the two former attacks using the variant equation $ea - \phi(N)b = c$. The new attack breaks the RSA system when a and $|c|$ are suitably small integers. Moreover, the new attack shows that the Boneh-Durfee attack and the attack of Kumar et al. can be derived using a single attack. We also showed that our bound manage to improve the bounds of Ariffin et al. and Bunder and Tonien.

Keywords: encryption, RSA, cryptanalysis, Coppersmith's technique, integer factorization

1 Introduction

The initial idea of cryptography started from a symmetric idea which implies that users were utilizing the same key in order to encrypt and decrypt the data. However, the problem on how to distribute key efficiently eventually arose as the number of the users increased. Two cryptographers namely Diffie and Hellman [6] contributed towards solving this problem by introducing public key cryptography (PKC) or also known as asymmetric cryptography which lead to a successful mass utilization of cryptography [15]. An important feature of PKC is that, it uses a one-way function together with its trapdoor information. A one way

function is a function that is easy to compute but computationally infeasible to invert unless if one has the trapdoor information that allows the inverse computation in polynomial time [10]. In 1978, Rivest, Shamir, and Adleman used the idea of [6] and invented an astounding cryptosystem namely RSA [19] and it has been deployed globally to provide security in communication as well as protect information. The main characters in the RSA are the modulus N where it is a product of two distinct large and balance primes called p and q, a parameter e which is set as public key and relatively prime to Euler's totient function $\phi(N)$, and a private exponent d connected via the relation $ed \equiv 1 \pmod{\phi(N)}$. The following algorithms describe the initial schemes of the RSA cryptosystem in details.

Algorithm 1: RSA Key Generation

Input: The bit-size n of the modulus N.
Output: A public key (N, e) and a private key (N, d).

1. Generate two large random and distinct primes p and q with $(n/2)$-bit primes size.
2. Compute the modulus $N = pq$ and $\phi(N) = (p-1)(q-1)$.
3. Choose a random integer e satisfying $\gcd(e, \phi(N)) = 1$.
4. Compute an integer d such that $d \equiv e^{-1} \pmod{\phi(N)}$.
5. Return the public key (N, e) and the private key $(p, q, \phi(N), d)$.

Algorithm 2: RSA Encryption

Input: The public key (N, e) and the original message M.
Output: The ciphertext C.

1. Choose a message $M \in \mathbb{Z}_N^*$
2. Compute $C \equiv M^e \pmod{N}$.
3. Return the ciphertext C.

Algorithm 3: RSA Decryption

Input: The private key (N, d) and the ciphertext C.
Output: The original message M.

1. Compute $M \equiv C^d \pmod{N}$.
2. Return the message M.

From Algorithm 2 and 3, it can be seen that both parameters e and d will be used respectively, as public and private exponents modulo the large RSA modulus, which is, in general, deemed as computationally costly. Over the years,

variants of RSA have been designed in order to increase efficiency and to reduce cost of implementation. Works by [17], [18], [21] are the instances of variants of RSA. An interested reader may refer to [9] for further explanation. Another popular method to reduce the cost of the decryption and the signature generation is to use a short private exponent d. It is related to the public exponent e by the above congruence relations vis- à-vis the equation $ed - k\phi(N) = 1$. Unfortunately, this might render RSA insecure.

Indeed, in 1990, Wiener's work [24] indicated that the RSA modulus N can be factored if $d < \frac{1}{3}N^{0.25}$ by the continued fraction attack. Using Coppersmith's technique and lattice reduction, [3] enhanced the attack range up to $d < N^{0.292}$. Later on, [2] improved [24] and presented a generalized equation in the form $ex + y = k\phi(N)$. They utilized the continued fraction method and Coppersmith's technique [5] and exposed that the solution for $ex + y = k\phi(N)$ can be obtained if $x < \frac{1}{3}N^{0.25}$ and $|y| < N^{-0.75}ex$. Note that the bound of [3] is valid essentially when e is of the same magnitude than N. [13] extended the attack of [3] with the equation $ed - k\phi(N) = 1$ for arbitrary $e < N^{\beta}$ and $d < N^{\delta}$. They showed that RSA is vulnerable if $\delta < 1 - \frac{1}{2}\sqrt{2\beta}$. In 2018, Bunder and Tonien proposed an attack on the RSA utilising continued fraction expansion over $\frac{e}{N'}$ where N' is a value that depends on the modulus N. They proved that the RSA is susceptible when $e \approx N^t$ for $0 < t < 1$ and $d < 2\sqrt{2}N^{\frac{3}{4}-\frac{t}{2}}$.

Another attack on the small decryption exponent was proposed by Weger [23] using the primes difference method. He proved that the RSA is insecure when $d < \frac{N^{\frac{3}{4}}}{|p-q|}$. In 2012, Nitaj [16] also proposed an attack on the RSA using the same method and he managed to improved Wiener's bound up to $\frac{\sqrt{6\sqrt{2}}}{6}N^{\frac{1}{4}}$. Later in 2018, Ariffin et al. generalized [16] and described an attack on the RSA using a combination of the small prime and continued fractions expansion methods and showed that when $d < \frac{\sqrt{3}}{\sqrt{2}}N^{\frac{3}{4}-\gamma}$, one can find d and k which then can lead to the factorization of the modulus N.

Note that if d satisfies the equation $ed - k\phi(N) = 1$ then the continued fraction expansion of $\frac{e}{\phi(N)}$ would yield the candidates for $\frac{k}{d}$ in the list of the convergents. Exploiting this fact, from the relation $ea - \phi(N)b = c$ with $0 < a < d$, $0 < b < k$ and is suitably small, if one obtains the convergent of $\frac{a}{b}$ which corresponds to $\frac{e}{\phi(N)}$, the factorization of RSA modulus $N = pq$ is feasible. In this paper, we study the RSA's public parameter associated with the equation of the form $ea - \phi(N)b = c$ with

$$e = N^{\beta}, \quad 0 < a < N^{\delta}, \quad 0 < |c| < N^{\gamma}.$$

Using Coppersmith's method and lattice reduction techniques, we show that if

$$\delta < 1 - \frac{1}{2}\gamma - \frac{1}{2}\sqrt{2\beta}, \quad \beta > \frac{1}{2},$$

then the modulus N can be factored.

If $\gamma = 0$, we get $\delta < 1 - \frac{1}{2}\sqrt{2\beta}$ which retrieves the bounds of [1], [13], [22] for the equation $ed - k\phi(N) = 1$. Moreover, if $\beta = 1$, we get $\delta < 1 - \frac{1}{2}\sqrt{2} \approx 0.292$, which in turn retrieves the bound of [3]. As a consequence, our new attack fully covers both attacks of [3] and [13] on RSA. The method presented in this paper shows that the set of the weak public exponents e in the attacks of [3] and [13] can be expanded to more exponents.

The initiation for the new attack is the equation $ea - \phi(N)b = c$. In all cases, we transform it to two a modular polynomial equations,

$$\begin{aligned} f(y_1, y_2, y_3) &\equiv 0 \pmod{e} \text{ with } f(y_1, y_2, y_3) = y_1y_2 + a_1y_2 + y_3, \\ F(y_1, u) &\equiv 0 \pmod{e} \text{ with } F(y_1, u) = u + a_1y_3 \text{ and } u = y_1y_2 + y_3. \end{aligned}$$

To find the small solutions of the modular equation $f(y_1, y_2, y_3) \equiv 0 \pmod{e}$, we use Coppersmith's technique [5] and lattice reduction, combined with the strategies presented in [8] as well as in [12]. Under the condition that the parameters a and c are suitably small, the solutions of the modular equation lead to the factorization of the RSA modulus.

This paper has been divided into the following sections. Section 2 reviews on lattice reduction and Coppersmith's technique. Section 3 describes the new attack on RSA while Section 4 presents a comparison of the new attack with the existing attacks. Lastly, Section 5 provides the conclusion for this study.

2 Preliminaries

This section briefly present basics yet important materials on lattice reduction and Coppersmith's technique.

2.1 Lattice Reduction

Let $u_1, \ldots, u_\omega$ be ω linearly independent vectors of $\mathbb{R}^n$ with $\omega \leq n$. The lattice $\mathcal{L}$ spanned by $(u_1, \ldots, u_\omega)$ is the set of all integer linear combinations of the u_i. Namely,

$$\mathcal{L} = \left\{ \sum_{i=1}^{\omega} u_i x_i, \ x_i \in \mathbb{Z} \right\}.$$

Let U be the basis matrix, that is the matrix of the set $(u_1, \ldots, u_\omega)$ in the canonical basis of $\mathbb{R}^n$. The determinant of $\mathcal{L}$ is defined as $\det(\mathcal{L}) = \sqrt{\det(U^tU)}$. The determinant reduces to $\det(\mathcal{L}) = |\det(U)|$ when $\omega = n$. The set $(u_1, \ldots, u_\omega)$ is called a basis of $\mathcal{L}$ with dimension ω. Denote by $||v||$ the Euclidean norm of a vector $v \in \mathcal{L}$. The main problem in lattice reduction is to find short non-zero vectors in $\mathcal{L}$. It is known that vectors with enough short norms can be found with the aid of using LLL algorithm [14].

Theorem 1. *[14] Suppose that lattice $\mathcal{L}$ is spanned by a basis $u_1, \ldots, u_\omega$ denoted by $\mathcal{L}$. Then a new basis $(b_1, \ldots, b_\omega)$ of $\mathcal{L}$ will be produced by the LLL algorithm such that*

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

for $i = 1, 2, \ldots, \omega$.

The complexity of the LLL algorithm depends on the dimension ω and on the maximum bitsize of the entries of the lattice matrix.

2.2 Coppersmith's method

In [5], new techniques to find small modular roots of polynomials in one variable, and solutions of polynomial equations in two variables over the integers was presented. For better understanding, one may refer to [7]. Since its invention, the ideas of Coppersmith have been heuristically extended to more than two variables. This was possible by applying a theorem in [11]. For example, for a polynomial $h(y_1, y_2, y_3, u) = \sum_{i_1,i_2,i_3,i_4} a_{i,j,k} y_1^{i_1} y_2^{i_2} y_3^{i_3} u^{i_4}$ with the Euclidean norm $\|h(y_1, y_2, y_3, u)\| = \sqrt{\sum_{i_1,i_2,i_3,i_4} a_{i,j,k}^2}$, Howgrave-Graham's theorem reduces to the following result.

Theorem 2. *([11]) Let $h(y_1, y_2, y_3, u) \in \mathbb{Z}[y_1, y_2, y_3, u]$ be a polynomial with at most ω monomials. Suppose $h(y_1^{(0)}, y_2^{(0)}, y_3^{(0)}, u^{(0)}) \equiv 0 \pmod{e^m}$, provided that $h(y_1, y_2, y_3, u) < e^{\frac{m}{\sqrt{\omega}}}$, where $|y_1^{(0)}| < Y_1$, $|y_2^{(0)}| < Y_2$, $|y_3^{(0)}| < Y_3$ and $|u^{(0)}| < U$. Then, $h(y_1^{(0)}, y_2^{(0)}, y_3^{(0)}, u^{(0)}) = 0$ holds over integers.*

To find the roots of a system of polynomials, we use the Gröbner basis technique. As required by most multivariate applications of Coppersmith's technique, finding the roots relies on the subsequent assumption.

Assumption 1 *Let $h(y_1, y_2, y_3, u) \in \mathbb{Z}[y_1, y_2, y_3, u]$ be the polynomial that are found by LLL algorithm. Then the ideal generated by the polynomial equations $h_1(y_1, y_2, y_3, u) = 0$, $h_2(y_1, y_2, y_3, u) = 0$, $h_3(y_1, y_2, y_3, u) = 0$, $h_4(y_1, y_2, y_3, u) = 0$ has dimension zero.*

Note that in our attack, the strategy of Jochemsz-May [12] that we utilised implemented the Coppersmith's method in order to find the roots of a polynomial. They reformulated the idea from [4], and came out with a strategy to find the roots of either modular or integer multivariate polynomial.

3 The Proposed Attack on RSA

A new attack on RSA will be described throughout this section. We examine the case where the RSA public parameters (N, e) satisfies an equation $ea - \phi(N) = c$ where $\phi(N) = (p-1)(q-1)$ and a and $|c|$ are suitably small unknown integers.

Theorem 3. *Let the modulus and the public exponent of the RSA be $N = pq$ and $e = N^\beta$ respectively with $\beta > \frac{1}{2}$. Suppose that e satisfies the equation $ea - (p-1)(q-1)b = c$ with $a < N^\delta$ and $|c| < N^\gamma$. If $\delta < 1 - \frac{1}{2}\gamma - \frac{1}{2}\sqrt{2\beta} - \varepsilon$, then under Assumption 1, the modulus can be factored in polynomial time.*

Proof. Let $N = pq$ be an RSA modulus, e be its public exponent and e is required to satisfy $ea - (p-1)(q-1)b = c$. Then $-b(N+1-p-q) - c \equiv 0 \pmod e$. Expanding this equation, we have $b(p+q) - (N+1)b - c \equiv 0 \pmod e$. Consider the polynomial

$$f(y_1, y_2, y_3) = y_1 y_2 + a_1 y_1 + y_3; \qquad a_1 = -(N+1).$$

Then the polynomial modular equation $f(y_1, y_2, y_3) \equiv 0 \pmod e$ would yield $(y_1^{(0)}, y_2^{(0)}, y_3^{(0)}) = (b, p+q, -c)$ as its solution. To obtain the intended roots of this modular equation, we apply Coppersmith's method combined with Jochemsz and May's strategy [12] for choosing the extra shifts.

Let $s, t \in \mathbb{Z}^+$ that will be determined next. For $0 \le r \le s$, assign the set

$$M_r = \bigcup_{0 \le j \le t} \Big\{ y_1^{i_1} y_2^{i_2+j} y_3^{i_3} \quad | y_1^{i_1} y_2^{i_2} y_3^{i_3} \text{is a monomial of } f^s(y_1, y_2, y_3) \text{ and} \frac{y_1^{i_1} y_2^{i_2} y_3^{i_3}}{(y_1 y_2)^r} \text{is a monomial of} f^{s-r} \Big\}.$$

A direct computation shows that $f^s(y_1, y_2, y_3)$ is

$$f^s(y_1, y_2, y_3) = \sum_{i_1=0}^{s} \sum_{i_2=0}^{i_1} \binom{s}{i_1} \binom{i_1}{i_2} a_1^{i_1 - i_2} y_1^{i_1} y_2^{i_2} y_3^{s-i_1}.$$

Hence, $y_1^{i_1} y_2^{i_2} y_3^{i_3}$ is a monomial of $f^s(y_1, y_2, y_3)$ if

$$i_1 = 0, \ldots, s, i_2 = 0, \ldots, i_1, i_3 = s - i_1.$$

Similarly, $y_1^{i_1} y_2^{i_2} y_3^{i_3}$ is a monomial of $f^{s-r}(y_1, y_2, y_3)$ if

$$i_1 = 0, \ldots, s-r, i_2 = 0, \ldots, i_1, i_3 = s - r - i_1.$$

Hence, for $0 \le r \le s$, if $y_1^{i_1} y_2^{i_2} y_3^{i_3}$ is a monomial of $f^s(y_1, y_2, y_3)$ then $\frac{y_1^{i_1} y_2^{i_2} y_3^{i_3}}{(y_1 y_2)^r}$ is a monomial of $f^{s-r}(y_1, y_2, y_3)$ if

$$i_1 = r, \ldots, s, i_2 = r, \ldots, i_1, i_3 = s - i_1.$$

which directs to classification of the set M_r. For $0 \le r \le s$, we have

$$y_1^{i_1} y_2^{i_2} y_3^{i_3} \in M_r \text{ if } i_1 = r, \cdots, s, i_2 = r, \cdots, i_1 + t, i_3 = s - i_1.$$

Substitute r by $r+1$, we obtain

$$\begin{aligned}&y_1^{i_1}y_2^{i_2}y_3^{i_3} \in M_{r+1} \text{ if}\\ &i_1 = r+1, \cdots, s, i_2 = r+1, \cdots, i_1+t, i_3 = s-i_1.\end{aligned}$$

For $0 \le r \le s$, define the following polynomials

$$g_{r,i_1,i_2,i_3}(y_1,y_2,y_3) = \frac{y_1^{i_1}y_2^{i_2}y_3^{i_3}}{(y_1y_2)^r} f(y_1,y_2,y_3)^r e^{s-r} \quad \text{with} \quad y_1^{i_1}y_2^{i_2}y_3^{i_3} \in M_r \backslash M_{(r+1)}.$$

Since

$$\begin{aligned}&y_1^{i_1}y_2^{i_2}y_3^{i_3} \in M_r \backslash M_{r+1}\\ &\text{if } i_1 = r, \cdots, s, i_2 = r, i_3 = s-i_1\\ &\text{or } i_1 = r, i_2 = r+1, \cdots, i_1+t, i_3 = s-i_1\end{aligned}$$

then, the polynomials $g_{r,i_1,i_2,i_3}(y_1,y_2,y_3)$ are reduced into two polynomials denoted by $A_{r,i_1,i_2,i_3}(y_1,y_2,y_3)$ and $B_{r,i_1,i_2,i_3}(y_1,y_2,y_3)$ where

$$\begin{aligned}A_{r,i_1,i_2,i_3}(y_1,y_2,y_3) &= y_1^{i_1-r}y_2^{i_2-r}y_3^{i_3} f(y_1,y_2,y_3)^r e^{s-r},\\ &\text{for } r = 0, \cdots, s, i_1 = r, \cdots, s, i_2 = r, i_3 = s-i_1\\ B_{r,i_1,i_2,i_3}(y_1,y_2,y_3) &= y_1^{i_1-r}y_2^{i_2-r}y_3^{i_3} f(y_1,y_2,y_3)^r e^{s-r},\\ &\text{for } r = 0, \cdots, s, i_1 = r, i_2 = r+1, \cdots, i_1+t, i_3 = s-i_1.\end{aligned}$$

The former polynomials can be slightly transformed as follows

$$\begin{aligned}A_{r,i_1,i_2,i_3}(y_1,y_2,y_3) &= y_1^{i_1}y_3^{i_3} f(y_1,y_2,y_3)^r e^{s-r},\\ &\text{for } r = 0, \cdots, s, i_1 = 0, \cdots, s-r, i_2 = 0, i_3 = s-r-i_1,\\ B_{r,i_1,i_2,i_3}(y_1,y_2,y_3) &= y_2^{i_2}y_3^{i_3} f(y_1,y_2,y_3)^r e^{s-r},\\ &\text{for } r = 0, \cdots, s, i_1 = 0, i_2 = 1, \cdots, t, i_3 = s-r.\end{aligned}$$

Next, we use the linearization technique that has been introduced by Herrmann and May in [8]. We transform the polynomial $f(y_1,y_2,y_3) = y_1y_2 + a_1y_1 + y_3$ to the reduced polynomial

$$F(y_1,u) = u + a_1y_1, \qquad u = y_1y_2 + y_3.$$

Using the polynomials $A_{r,i_1,i_2,i_3}(y_1,y_2,y_3)$ and $B_{r,i_1,i_2,i_3}(y_1,y_2,y_3)$, we construct two new families of polynomials where each term y_1y_2 is replaced by $y_3 - u$, namely

$$\begin{aligned}G_{r,i_1,i_2,i_3}(y_1,y_2,y_3,u) &= y_1^{i_1}y_3^{i_3} F(y_1,u)^r e^{s-r},\\ &\text{for } r = 0, \cdots, s, i_1 = 0, \cdots, s-r, i_2 = 0, i_3 = s-r-i_1, i_4 = r,\\ H_{r,i_1,i_2,i_3}(y_1,y_2,y_3,u) &= y_2^{i_2}y_3^{i_3} F(y_1,u)^r e^{s-r},\\ &\text{for } i_1 = 0, i_2 = 1, \cdots t, r = \lfloor \frac{s}{t} \rfloor i_2, \cdots, s, i_3 = s-r, i_4 = r.\end{aligned}$$

It follows that the monomials in $G_{r,i_1,i_2,i_3}(y_1, y_2, y_3, u)$ are in the form $y_1^{i_1} y_2^{i_2} y_3^{i_3} u^{i_4}$ with

$$r = 0, \cdots, s, i_1 = 0, \cdots, s - r, i_2 = 0, i_3 = s - r - i_1, i_4 = r \tag{1}$$

Similarly, the monomials in $H_{r,i_1,i_2,i_3}(y_1, y_2, y_3, u)$ are in the form $y_1^{i_1} y_2^{i_2} y_3^{i_3} u^{i_4}$ with

$$i_1 = 0, i_2 = 1, \cdots t, r = \lfloor \frac{s}{t} \rfloor i_2, \cdots, s, i_3 = s - r, i_4 = r. \tag{2}$$

The lattice denoted as $\mathcal{L}$ is built by the coefficient vectors of the two families of polynomials $G_{r,i_1,i_2,i_3}(y_1Y_1, y_2Y_2, y_3Y_3, uU)$ and $H_{r,i_1,i_2,i_3}(y_1Y_1, y_2Y_2, y_3Y_3, uU)$ where Y_1, Y_2, Y_3, U are integers. These values will be defined later with the condition $Y_1Y_2y_1y_2 = Uu - Y_3y_3$. The ordering of the rows is such that any polynomial $G_{r,i_1,i_2,i_3}(y_1Y_1, y_2Y_2, y_3Y_3, uU)$ is prior to any polynomial $H_{r,i_1,i_2,i_3}(y_1Y_1, y_2Y_2, y_3Y_3, uU)$, and in $G_{r,i_1,i_2,i_3}(y_1Y_1, y_2Y_2, y_3Y_3, uU)$ or in $H_{r,i_1,i_2,i_3}(y_1Y_1, y_2Y_2, y_3Y_3, uU)$, G_{r,i_1,i_2,i_3} is prior to G_{r',i'_1,i'_2,i'_3} and H_{r,i_1,i_2,i_3} is prior to G_{r',i'_1,i'_2,i'_3} if one of the following conditions is satisfied

$$\begin{aligned}
&r < r',\\
&r = r', i_1 < i'_1,\\
&r = r', i_1 = i'_1, i_2 < i'_2,\\
&r = r', i_1 = i'_1, i_2 = i'_2, i_3 < i'_3,\\
&r = r', i_1 = i'_1, i_2 = i'_2, i_3 = i'_3, i_4 < i'_4.
\end{aligned}$$

A similar rule is applied to order the monomials and the columns. Thus a lower triangular matrix is formed as in the following matrix where $s = 3$ and $t = 2$.

$\{G,H\}(r,i_1,i_2,i_3,i_4)$	y_3^3	$y_1y_3^2$	$y_1^2y_3$	y_1^3	y_3^2u	y_1y_3u	y_1^2u	y_3u^2	y_1u^2	u^3	$y_2y_3^2u$	$y_2y_3u^2$	y_2u^3	$y_2^2y_3u^2$	$y_2^2u^3$
$G(0,0,0,3,0)$	$Y_3^3e^3$	0	0	0	0	0	0	0	0	0	0	0	0	0	0
$G(0,1,0,2,0)$	0	$Y_1Y_3^2e^3$	0	0	0	0	0	0	0	0	0	0	0	0	0
$G(0,2,0,1,0)$	0	0	$Y_1^2Y_3e^3$	0	0	0	0	0	0	0	0	0	0	0	0
$G(0,3,0,0,0)$	0	0	0	$Y_1^3e^3$	0	0	0	0	0	0	0	0	0	0	0
$G(1,0,0,2,1)$	0	$Y_3^2Y_1a_1e^2$	0	0	$Y_3^2Ue^2$	0	0	0	0	0	0	0	0	0	0
$G(1,1,0,1,1)$	0	0	$Y_1^2Y_3a_1e^2$	0	0	$Y_1y_3Ue^2$	0	0	0	0	0	0	0	0	0
$G(1,2,0,0,1)$	0	0	0	$Y_1^3a_1e^2$	0	0	$Y_1^2Ue^2$	0	0	0	0	0	0	0	0
$G(2,0,0,1,2)$	0	0	$Y_3Y_1^2a_1^2e$	0	0	$2Y_3UY_1a_1e$	0	Y_3U^2e	0	0	0	0	0	0	0
$G(2,1,0,0,2)$	0	0	0	$Y_1^3a_1^2e$	0	0	$2Y_1^2Ua_1e$	0	Y_1U^2e	0	0	0	0	0	0
$G(3,0,0,0,3)$	0	0	0	$Y_1^3a_1^3$	0	0	$3UY_1^2a_1^2$	0	$3U^2Y_1a_1$	U^3	0	0	0	0	0
$H(1,0,1,2,1)$	$-Y_3^3a_1e^2$	0	0	0	$Y_3^2a_1e^2U$	0	0	0	0	0	$UY_2Y_3^2e^2$	0	0	0	0
$H(2,0,1,1,2)$	0	$-Y_3^2a_1^2eY_1$	0	0	$-2UY_3^2a_1e$	$Y_3a_1^2eUY_1$	0	$2U^2Y_3a_1e$	0	0	0	$U^2Y_2Y_3e$	0	0	0
$H(3,0,1,0,3)$	0	0	$-a_1^3Y_3Y_1^2$	0	0	$-3Ua_1^2Y_3Y_1$	$a_1^3UY_1^2$	$-3U^2a_1Y_3$	$3U^2a_1^2Y_1$	$3U^3a_1$	0	0	U^3Y_2	0	0
$H(2,0,2,1,2)$	$Y_3^3a_1^2e$	0	0	0	$-2Y_3^2a_1^2eU$	0	0	$Y_3a_1^2eU^2$	0	0	$-2UY_3^2a_1eY_2$	$2U^2Y_3a_1eY$	0	$U^2Y_2^2Y_3e$	0
$H(3,0,2,0,3)$	0	$a_1^3Y_3^2Y_1$	0	0	$3Ua_1^2Y_3^2$	$-2a_1^3UY_3Y_1$	0	$-6U^2a_1^2Y_3$	$a_1^3U^2Y_1$	$3U^3a_1^2$	0	$-3U^2a_1Y_3Y_2$	$3U^3a_1Y_2$	0	$U^3Y_2^2$

Table 1. The coefficient matrix for $s = 3$ and $t = 2$.

Since the lattice of $\mathcal{L}$ is a lower triangular matrix, thus the determinant is obtained by multiplying the diagonal terms. Since only Y_1, Y_2, Y_3, U and e are involved, then determinant is of the form

$$\det(\mathcal{L}) = Y_1^{n_{Y_1}} Y_2^{n_{Y_2}} Y_3^{n_{Y_3}} U^{n_U} e^{n_e} \tag{3}$$

Using the construction of the monomials of the polynomials $G_{r,i_1,i_2,i_3,i_4}(y_1, y_2, y_3, u)$ and $H_{r,i_1,i_2,i_3,i_4}(y_1, y_2, y_3, u)$ where r, i_1, i_2, i_3, i_4 satisfy the conditions (1) and (2), the dominant terms of the exponents $n_{Y_1}, n_{Y_2}, n_{Y_3}, n_U, n_e$ as well as the dimension ω of the lattice satisfy

$$\begin{aligned}
n_{Y_1} &= \sum_{r=0}^{s} \sum_{i_1=0}^{s-r} i_1 = \frac{1}{6}s^3 + o(s^3) \\
n_{Y_2} &= \sum_{i_2=1}^{t} \sum_{r=\lfloor \frac{s}{t} \rfloor}^{s} i_2 = \frac{1}{2}st^2 - \frac{1}{3}\lfloor \frac{s}{t} \rfloor t^3 + o(s^3) \\
n_{Y_3} &= \sum_{r=0}^{s} \sum_{i_1=0}^{s-r} (s - r - i_1) + \sum_{i_2=1}^{t} \sum_{r=\lfloor \frac{s}{t} \rfloor}^{s} (s - r) \\
&= \frac{1}{6}s^3 + \frac{1}{2}st^2 - \frac{1}{2}\lfloor \frac{s}{t} \rfloor s^2 t + \frac{1}{6}\lfloor \frac{s}{t} \rfloor^2 t^3 \\
n_U &= \sum_{r=0}^{s} \sum_{i_1=0}^{s-r} r + \sum_{i_2=1}^{t} \sum_{r=\lfloor \frac{s}{t} \rfloor}^{s} r \\
&= \frac{1}{6}s^3 + \frac{1}{2}st^2 + \frac{1}{6}\lfloor \frac{s}{t} \rfloor^2 t^3 \\
n_e &= \sum_{r=0}^{s} \sum_{i_1=0}^{s-r} (s - r) + \sum_{i_2=1}^{t} \sum_{r=\lfloor \frac{s}{t} \rfloor}^{s} (s - r) \\
&= \frac{1}{3}s^3 + \frac{1}{2}s^2 t + \frac{1}{6}\lfloor \frac{s}{t} \rfloor^2 t^3 - \frac{1}{2}\lfloor \frac{s}{t} \rfloor st^2 \\
\omega &= \sum_{r=0}^{s} \sum_{i_1=0}^{s-r} 1 + \sum_{i_2=1}^{t} \sum_{r=\lfloor \frac{s}{t} \rfloor}^{s} 1 = \frac{1}{2}s^2 + st - \frac{1}{2}\lfloor \frac{s}{t} \rfloor t^2.
\end{aligned}$$

In the following asymptotic analysis, we set $t = \tau s$ with $0 < \tau \leq 1$ and use $\lfloor \frac{s}{t} \rfloor \approx 1/\tau$. Then, for sufficiently large s, the exponents $n_{Y_1}, n_{Y_2}, n_{Y_3}, n_U, n_e$ and

the dimension ω reduce to

$$\begin{aligned} n_{Y_1} &= \frac{1}{6}s^3 + o(s^3), \\ n_{Y_2} &= \frac{1}{6}\tau^2 s^3 + o(s^3), \\ n_{Y_3} &= \frac{1}{6}(\tau+1)s^3 + o(s^3), \\ n_U &= \frac{1}{6}(2\tau+1)s^3 + o(s^3), \\ n_e &= \frac{1}{6}(\tau+2)s^3 + o(s^3), \\ \omega &= \frac{1}{2}(\tau+1)s^2 + o(s^2). \end{aligned} \tag{4}$$

To apply Theorem 1 with $i = 4$ to the four shortest vectors in the LLL-reduced basis of $\mathcal{L}$, we set

$$2^{\frac{\omega(\omega-1)}{4(\omega-3)}} \det(\mathcal{L})^{\frac{1}{\omega-3}} < \frac{e^s}{\sqrt{\omega}}.$$

This transform to

$$\det(\mathcal{L}) < \frac{2^{-\frac{\omega(\omega-1)}{4}}}{(\sqrt{\omega})^{\omega-3}} e^{s(\omega-3)}.$$

Then, using (3), we get

$$e^{n_e - s\omega} Y_1^{n_{Y_1}} Y_2^{n_{Y_2}} Y_3^{n_{Y_3}} U^{n_U} < \frac{2^{-\frac{\omega(\omega-1)}{4}}}{(\sqrt{\omega})^{\omega-3}} e^{s(\omega-3)}. \tag{5}$$

Suppose that from $ea-(p-1)(q-1)b = c$ we have $e = N^\beta$, $a < N^\delta$ and $|c| < N^\gamma$. We set

$$Y_1 = 2N^{\beta+\delta-1}, Y_2 = 3N^{\frac{1}{2}}, Y_3 = N^\gamma, U = 12N^{\beta+\delta-\frac{1}{2}}. \tag{6}$$

Then the target solution $\left(y_1^{(0)}, y_2^{(0)}, y_3^{(0)}, u^{(0)}\right) = (b, p+q, -c, b(p+q)-c)$ satisfies $|y_2^{(0)}| < p+q < Y_2$, $|y_3^{(0)}| = |c| < Y_3$, and

$$|y_1^{(0)}| = b = \frac{(ea-c)}{\phi(N)} < \frac{ea+|c|}{\phi(N)} < 2N^{\beta+\delta-1}, \tag{7}$$

where we used $\phi(N) \approx N$ and $|c| < ea$. Hence, $|y_1^{(0)}| < Y_1$. It follows that

$$\begin{aligned} |u^{(0)}| = |y_1^{(0)} y_2^{(0)} + y_3^{(0)}| &< 2\max(Y_1 Y_2, Y_3) \\ &= 2\max\left(2N^{\beta+\delta-1} \cdot 3N^{\frac{1}{2}}, N^\gamma\right) \\ &= 12N^{\beta+\delta-\frac{1}{2}} \end{aligned}$$

and consequently $|u^{(0)}| < U$. Using the values $n_{Y_1}, n_{Y_2}, n_{Y_3}, n_U, n_e$ and ω from (4) as well as the values of Y_1, Y_2, Y_3, and U from (6), we get

$$e^{n_e - s_\omega} = N^{\left(-\frac{1}{3}\tau - \frac{1}{6}\right)\beta s^3 + o(s^3)}$$
$$Y_1^{n_{Y_1}} = 2^{\frac{1}{6}s^3 + o(s^3)} N^{\frac{1}{6}(\beta+\delta-1)s^3 + o(s^3)} = N^{\frac{1}{6}(\beta+\delta-1)s^3 + o(s^3) + \varepsilon_1},$$
$$Y_2^{n_{Y_2}} = 3^{\frac{1}{6}\tau^2 s^3 + o(s^3)} N^{\frac{1}{2}\tau^2 s^3 + o(s^3)} = N^{\frac{1}{2}\tau^2 s^3 + o(s^3) + \varepsilon_2}$$
$$Y_3^{n_{Y_3}} = N^{\left(\frac{1}{6}\tau + \frac{1}{6}\right)\gamma s^3 + o(s^3)}$$
$$U^{n_U} = 12^{\left(\frac{1}{3}\tau + \frac{1}{6}\right)s^3 + o(s^3)} N^{\left(\frac{1}{3}\tau + \frac{1}{6}\right)\left(\beta+\delta-\frac{1}{2}\right)s^3 + o(s^3)} = N^{\left(\frac{1}{3}\tau + \frac{1}{6}\right)\left(\beta+\delta-\frac{1}{2}\right)s^3 + o(s^3) + \varepsilon_3}$$
$$\frac{2^{-\frac{\omega(\omega-1)}{4}}}{(\sqrt{\omega})^{\omega-3}} e^{-3s} = N^{-2\beta s - \varepsilon_4}.$$

where $\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4 \in \mathbb{Z}^+$ and their values are small depending on s and N. Then, taking logarithms, dividing by $s^3 \log(N)$ and letting $\varepsilon_5 > 0$ for the contributions of the small terms, the inequality (5) leads to

$$\left(-\frac{1}{3}\tau - \frac{1}{6}\right)\beta + \frac{1}{6}(\beta+\delta-1) + \frac{1}{12}\tau^2 + \left(\frac{1}{6}\tau + \frac{1}{6}\right)\gamma + \left(\frac{1}{3}\tau + \frac{1}{6}\right)\left(\beta + \delta - \frac{1}{2}\right) < -\varepsilon_5,$$

where $\varepsilon_5 \in \mathbb{Z}^+$ is a small value and depends on s and N. Then, rearranging, we get

$$\tau^2 + (4\delta + 2\gamma - 2)\tau + 2\beta + 4\delta + 2\gamma - 3 < -12\varepsilon_5. \tag{8}$$

From the left side of (8), the value for τ is optimum when

$$\tau_0 = 1 - 2\delta - \gamma.$$

Here we need $\tau_0 > 0$. This is achieved if

$$\delta < \frac{1}{2} - \frac{1}{2}\gamma. \tag{9}$$

Replacing τ_0 in (8), we get

$$-4\delta^2 + (8 - 4\gamma)\delta + 4\gamma + 2\beta - \gamma^2 - 4 < -12\varepsilon_4,$$

which will be true if

$$\delta < 1 - \frac{1}{2}\gamma - \frac{1}{2}\sqrt{2\beta} - \varepsilon, \tag{10}$$

where $\varepsilon \in \mathbb{Z}^+$ is a small value and depends on s and N. Since δ satisfies (9) and (10) and $\beta > \frac{1}{2}$ then

$$\delta < \min\left(1 - \frac{1}{2}\gamma - \frac{1}{2}\sqrt{2\beta} - \varepsilon, \frac{1}{2} - \frac{1}{2}\gamma\right) = 1 - \frac{1}{2}\gamma - \frac{1}{2}\sqrt{2\beta} - \varepsilon.$$

Using the first four vectors u_1, u_2, u_3 and u_4 in the LLL reduced basis, we get four vectors $g_1(y_1, y_2, y_3, u), g_2(y_1, y_2, y_3, u), g_3(y_1, y_2, y_3, u)$ and $g_4(y_1, y_2, y_3, u)$ such that

$$g_1(y_1^{(0)}, y_2^{(0)}, y_3^{(0)}, u^{(0)}) = g_2(y_1^{(0)}, y_2^{(0)}, y_3^{(0)}, u^{(0)}) = g_3(y_1^{(0)}, y_2^{(0)}, y_3^{(0)}, u^{(0)})$$
$$= g_4(y_1^{(0)}, y_2^{(0)}, y_3^{(0)}, u^{(0)}) = 0.$$

Assume that $g_1(y_1, y_2, y_3, u), g_2(y_1, y_2, y_3, u), g_3(y_1, y_2, y_3, u)$ and $g_4(y_1, y_2, y_3, u)$ are algebraically independent, we apply resultant techniques or Gröbner basis method to find the solution $(y_1^{(0)}, y_2^{(0)}, y_3^{(0)}, u^{(0)}) = (b, p+q, -c, b(p+q)-c)$. From $y_2^{(0)} = p+q$ and $N = pq$, we get p and q. Thus, this gives the factorization of N. □

4 Comparison with Existing Results

4.1 Comparison with the result in [3]

For the balanced primes p and q and in the presence of an encryption exponent e of the same magnitude to N, [3] showed that the RSA modulus $N = pq$ is factorable satisfying its original key equation $ed - k\phi(N) = 1$ with

$$\delta = 1 - \frac{\sqrt{2}}{2} \approx 0.292. \quad \text{for} \quad d < N^{\delta}.$$

In the equation $ea - \phi(N)b = c$ with $e = N^{\beta}$, $a < N^{\delta}$, and $|c| < N^{\gamma}$, this corresponds to $\beta = 1$ and $\gamma = 0$. Plugging these values in $\delta < \frac{1}{2} - \frac{1}{2}\gamma$, we get

$$\delta = 1 - \frac{\sqrt{2}}{2} \approx 0.292,$$

which recovers the same bound as in [3]. Observe that when $a = d$, $b = k$, $c = 1$, then the original RSA key equation is a particular case of the equation $ea - \phi(N)b = c$. This implies that the class of the weak exponents in [3] is a subclass of the weak exponents of the new attack.

4.2 Comparison with the result in [13]

The result presented in [13] extended the attack of [3] to all exponents $e = N^{\beta}$ and demonstrate that N can be factored with

$$\delta < 1 - \frac{1}{2}\sqrt{2\beta} \quad \text{where} \quad d < N^{\delta}.$$

Remark that $ed - k\phi(N) = 1$ is a particular equation of $ea - \phi(N)b = c$ whenever $c = N^{\gamma} = 1$ that is $\gamma = 0$. When we substitute this value in the new bound $\delta < 1 - \frac{1}{2}\gamma - \frac{1}{2}\sqrt{2\beta} - \varepsilon$, we get

$$\delta < 1 - \frac{1}{2}\sqrt{2\beta} - \varepsilon,$$

which retrieves the bound of [13]. Moreover, as in the previous comparison, the class of the weak exponents in [13] is a subclass of the weak exponents of the new attack.

4.3 Comparison with the result in [2]

A cryptanalysis result on RSA presented in [2] showed that for encryption exponent satisfies an equation $ex - y\phi(N) = z$ provided $0 < |x| \leq \frac{1}{3}\sqrt{\frac{\phi(N)}{e}}\frac{N^{\frac{3}{4}}}{p-q}$ and $|z| \leq \frac{p-q}{\phi(N)N^{\frac{1}{4}}}ex$, then the RSA modulus can be factored. Suppose that $|x| < N^{\delta}$, $e = N^{\beta}$, and $p - q = cN^{\frac{1}{2}}$ for some constant $c < 1$. Then, the attack in [2] can be applied only if

$$\delta < \frac{3}{4} - \frac{1}{2}\beta, \quad \text{and} \quad \gamma < \beta + \delta - \frac{3}{4}.$$

Hence, in the situation $e \approx N^{\beta}$, that is $\beta = 1$, therefore such attack is applicable only for $\delta < \frac{1}{4}$ and $\gamma < \frac{1}{2}$ while our attack is applicable whenever the conditions of Theorem 3 are satisfied with $\beta = 1$, that is whenever

$$\delta < 1 - \frac{1}{2}\gamma - \frac{1}{2}\sqrt{2} - \varepsilon \approx 0.292 - \frac{1}{2}\gamma.$$

This is better than the bound in [2] when $0.292 - \frac{1}{2}\gamma > \frac{1}{4}$, that is for $\gamma < 0.048$.

4.4 Comparison with the result in [22]

Bunder and Tonien described an attack on the RSA by using the continued fraction expansion. However, instead of finding the convergents of $\frac{e}{N}$, they find the convergents of $\frac{e}{N'}$ where N' is given by $N' = \left[N - \left(a + \frac{3}{2\sqrt{2}}\right)N^{\frac{1}{2}} + 1\right]$. In their attack, they showed that for $e \approx N^{\beta}$, they can recover the private exponent when

$$d < 2\sqrt{2}N^{\frac{3}{4}-\frac{\beta}{2}}.$$

Note that [22] also used the original key equation, $ed - k\phi(N) = 1$. Thus, in comparison, we let $c = N^{\gamma} = 1$ which indicates that $\gamma = 0$. Thus we have

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

Here is a direct way to show that our bound is better. We have

$$1 - \frac{1}{2}\sqrt{2\beta} - \frac{3}{4} + \frac{\beta}{2} = \frac{\beta}{2} - \frac{1}{2}\sqrt{2\beta} + \frac{1}{4} = \frac{1}{4}\left(2\beta - 2\sqrt{2\beta} + 1\right) = \frac{1}{4}\left(\sqrt{2\beta} - 1\right)^2 \geq 0.$$

This shows that our bound is better than the bound of[22].

4.5 Comparison with the result in [1]

Ariffin et al. [1] proposed a short decryption exponent attack on the RSA. Using the small prime difference method of the form $|b^2p - a^2q| < N^{\gamma}$ where the

ratio of $\frac{b^2}{a^2}$ is approximately close to $\frac{q}{p}$, they show that one can find $\frac{k}{d}$ from the convergents of the continued fraction expansion of $\frac{e}{N-\lceil \frac{a^2+b^2}{ab}\sqrt{N}\rceil+1}$ whenever

$$d < \frac{\sqrt{3}}{\sqrt{2}} N^{\frac{3}{4}-\gamma} \quad \text{for} \quad |b^2 p - a^2 q| < N^{\gamma}. \tag{11}$$

Since [1] used the key equation $ed - k\phi(N) = 1$, thus for our bound, we let $\gamma = 0$. Thus we have

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

From (11), it can be seen that their bound only depends on γ and they have stated that $0.25 \leq \gamma < 0.5$. Meanwhile, our bound depends on the size of β such that $\beta = \log_N e$. We present the comparison of bound in the following tables.

Bound of δ \ **$\beta = \log_N(e)$**	$\beta = 1$	$\beta = 0.8$	$\beta = 0.6$	$\beta = 0.4$	$\beta = 0.2$
Ariffin et al.[1]	0.50	0.50	0.50	0.50	0.50
Our bound	0.29	0.36	0.45	0.55	0.68

Table 2. Comparison with methods from [1] for $\gamma = 0.25$.

Bound of δ \ **$\beta = \log_N(e)$**	$\beta = 1$	$\beta = 0.8$	$\beta = 0.6$	$\beta = 0.4$	$\beta = 0.2$
Ariffin et al.[1]	0.30	0.30	0.30	0.30	0.30
Our bound	0.29	0.36	0.45	0.55	0.68

Table 3. Comparison with methods from [1] for $\gamma = 0.45$.

The tables above show that our bound is increasing as the value of β is decreasing. From Table 2, we manage to improve [1] when $\beta = 0.4$ and from Table 3, we improve [1] when $\beta = 0.8$. This indicates that our bound is better [1] for smaller values of β.

4.6 A numerical example

As a numerical example, let us consider the RSA public key (N, e) with

$$N = 5339583385665627056733057342119365266735235221280290598464283$$
$$e = 3873527233077759931835049102329492476182864153016922288436 81$$

Observe that e and N satisfy an equation $ea - (p-1)(q-1)b = c$. Define the polynomial $f(y_1, y_2, y_3) = y_1 y_2 + a_1 y_1 + y_3$ where $a_1 = -(N+1)$, $y_1 = b$,

$y_2 = p + q$ and $y_3 = -c$. Then, applying the method of Theorem 3 with the parameters

$$s = 5,\ t = 3,\ Y_1 = 2\lfloor N^{\frac{1}{4}} \rfloor,\ Y_2 = 3\lfloor N^{\frac{1}{2}} \rfloor,\ Y_3 = \lfloor N^{0.06} \rfloor,\ U = 12N^{0.74},$$

we get a lattice of dimension 27 by executing the LLL algorithm. After which, when followed by the resultant technique, we obtain small solutions from systems of polynomial equations as follows;

$$\begin{aligned} y_1 &= 660305687366885, \\ y_2 &= 462232197246100674972501649396, \\ y_3 &= -4183, \\ u &= 30521454872569207394551705385272228316517182 77. \end{aligned}$$

Hence, $p + q = y_2 = 462232197246100674972501649396$, which is sufficient to compute its corresponding prime factors

$$\begin{aligned} p &= 23545397668533603706015305949 37 \\ q &= 22677822056076463791234858990 59. \end{aligned}$$

We notice that, using $\phi(N) = (p-1)(q-1)$, we get

$$\begin{aligned} d &\equiv e^{-1} \pmod{\phi(N)} \\ &\equiv 592294212514666735434888502687363310152982843784672392529585. \end{aligned}$$

Hence, $d \approx N^{0.981} >> N^{0.292}$. This is clearly an exponential increment of the RSA attack range. This shows that the attacks of Boneh-Durfee [3], Kumar et al. [13], Ariffin et al. [1], and Bunder-Tonien [22] can not be applied for the key (e, N). We also are able to retrieve the values

$$\begin{aligned} b &= y_1 = 660305687366885, \\ c &= -y_3 = 4183, \\ a &= \frac{c + (N + 1 - p - q)b}{e} = 9102187917040423, \end{aligned}$$

so that $ea - \phi(N)b = c$ with $a \approx N^{0.262}$. Also, we observe that $\frac{a}{b}$ is not a convergent of $\frac{e}{N}$. Moreover, all the convergents $\frac{a'}{b'}$ of $\frac{e}{N}$ with $a' < \frac{1}{3}N^{\frac{1}{4}}$ satisfy $|ea' - \phi(N)b'| > N^{-\frac{3}{4}}ea'$. This shows that the attack [2] will not give the factorization of N.

5 Conclusion

In this study, the case that we have taken into consideration is when the RSA public parameter N with its corresponding exponent e which associated to the equation $ea - \phi(N)b = c$. Using Coppersmith's method, we have proved that

RSA is unsecure if the parameters a,b, and c are suitably small. Moreover, we have shown that the famous bound $d < N^{0.292}$ of [2] is a particular case of our attack. Thus, one needs to be cautious in choosing the public and private exponent in order to ensure that the cryptosystem is invunerable from attacks. Alternatively, [20] suggested that one could use unbalanced primes as an attempt to avoid small decryption exponent attack.

6 Acknowledgement

1. The research was supported by Mediterranea Universiti of Reggio Calabria (UNIRC) Research Grant (UPM/INSPEM/700-3/1/GERAN ANTARABA NGSA/6380071-10065).
2. The present research was partially supported by the Putra Grant with Project Number GP-IPS/2018/9657300.

References

1. Ariffin, M. R. K., Abubakar, S. I., Yunos, F., & Asbullah, M. A.: New cryptanalytic attack on RSA modulus $N = pq$ using small prime difference method. Cryptography, 3(1), (2019) https://doi.org/10.3390/cryptography3010002
2. Blömer J., May, A.: A generalized Wiener attack on RSA. In: LNCS of PKC, vol. 12, pp. 1–13. (2004) https://doi.org/10.1007/978-3-540-24632-9_1
3. Boneh, D., Durfee, G. :Cryptanalysis of RSA with private key d less than $N^{0.292}$. In: LNCS of Advances in Cryptology-EUROCRYPT'99, vol. 12, pp. 1–13. (1999) https://doi.org/doi:10.1007/3-540-48910-X_1
4. Coron, J. S.: Finding small roots of bivariate integer polynomial equations revisited. In International Conference on the Theory and Applications of Cryptographic Techniques Springer, Berlin, Heidelberg. pp. 492-505, (2004, May)
5. Coppersmith, D.: Small solutions to polynomial equations, and low exponent RSA vulnerabilities. In: LNCS of Advances in Cryptology-EUROCRYPT'99, vol. 10, pp.233–260. (1997) https://doi.org/10.1007/s001459900030
6. Diffie, W., & Hellman, M.: New directions in cryptography. IEEE transactions on Information Theory, 22(6), 644-654. (1976) https://doi.org/10.1109/TIT.1976.1055638
7. Galbraith, S. D.: Mathematics of public key cryptography. Cambridge University Press. (2012)
8. Herrmann, M., May, A.: Maximizing small root bounds by linearization and applications to small secret exponent RSA. In: LNCS of PKC pp. 53–69. (2010) https://doi.org/10.1007/978-3-642-13013-7_4
9. Hinek, M. J.: Cryptanalysis of RSA and its variants. CRC press. (2009)
10. Hoffstein, J., Pipher, J., Silverman, J. H., Silverman, J. H.: An Introduction to Mathematical Cryptography (Vol. 1). New York: Springer. (2008).
11. Howgrave-Graham, N.: Finding small roots of univariate modular equations revisited. In: LNCS of Cryptography and Coding, pp. 131–142. (1997) https://doi.org/10.1007/BFb0024458
12. Jochemsz, E., May, A.: A strategy for finding roots of multivariate polynomials with new applications in attacking RSA variants. In: LNCS of Advances in Cryptology-ASIACRYPT 2006, pp. 267–282. (2006) https://doi.org/10.1007/11935230_18

13. Kumar, S., Narasimam, C., Pallam Setty, S.: Generalization of Boneh- Durfee's attack for arbitrary public exponent RSA. International Journal of Computer Applications, vol. 49, pp. 39–42. (2012) https://doi.org/10.5120/7880-1190
14. Lenstra, A.K., Lenstra,H.W., Lovász, L.: Factoring polynomials with rational coeffficients . Mathematische Annalen, vol. 261, pp. 513–534. (1982) https://doi.org/10.1007/BF01457454
15. May, A.: New RSA vulnerabilities using lattice reduction methods (Doctoral dissertation, University of Paderborn). (2003)
16. Nitaj, A.: Cryptanalysis of RSA using the ratio of the primes. In AFRICACRYPT 2009 (pp. 98-115). Springer, Berlin, Heidelberg. (2009) https://doi.org/10.1007/978-3-642-02384-2_7
17. Quisquater, J.-J., Couvreur, C.: Fast decipherment algorithm for RSA public key cryptosystem. Electronics Letters, vol. 18(21), pp. 905–907. (1982)
18. Rabin, M. O.: Digitalized signatures and public-key functions as intractable as factorization. Massachusetts Inst of Tech Cambridge Lab for Computer Science. (1979)
19. Rivest, R., Shamir, A., Adleman, L.: A Method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, vol. 21, pp. 120–126. (1978) https://doi.org/10.1145/357980.358017
20. Sun, H. M., Yang, W. C., Laih, C. S.: On the design of RSA with short secret exponent. In International Conference on the Theory and Application of Cryptology and Information Security (pp. 150-164). Springer, Berlin, Heidelberg. (1999)
21. Takagi, T.: A fast RSA-type public-key primitive modulo $p^k q$ using Hensel lifting. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 87(1), 94-101. (2004)
22. Bunder, M. W., & Tonien, J.: A new attack on the RSA cryptosystem based on continued fractions. Malaysian Journal of Mathematical Sciences, vol. 11(S), pp. 45–57. (2017)
23. Weger, B. D.: Cryptanalysis of RSA with small prime difference. Applicable Algebra in Engineering, Communication and Computing, 13(1), 17–28. (2002)
24. Wiener, M.: Cryptanalysis of short RSA secret exponents. IEEE Transactions on Information Theory, vol.36, pp. 553–558. (1990) https:doi.org/10.1109/18.54902