Malaysian Journal of Mathematical Sciences 13(S) August: 141–189 (2019)
Special Issue: The 6th International Cryptology and Information Security Conference (CRYPTOLOGY2018)

MALAYSIAN JOURNAL OF MATHEMATICAL SCIENCES

Journal homepage: http://einspem.upm.edu.my/journal

Successful Cryptanalytic Attacks Upon RSA Moduli $N = pq$

Abubakar, S.I. *[1], Ariffin, M.R.K.[1,2], and Asbullah, M.A.[1,3]

[1]*Laboratory of Cryptography, Analysis and Structure, Institute for Mathematical Research, Universiti Putra Malaysia, Malaysia*
[2]*Department of Mathematics, Faculty of Science, Universiti Putra Malaysia, Malaysia*
[3]*Centre of Foundation Studies for Agricultural Science, Universiti Putra Malaysia, Malaysia*

E-mail: siabubakar82@gmail.com
* *Corresponding author*

ABSTRACT

This paper reports four new cryptanalytic attacks which show that t instances of RSA moduli $N_s = p_s q_s$ for $s = 1, \dots, t$ where $t \geq 2$ can be simultaneously factored in polynomial time using simultaneous Diophantine approximations and lattice basis reduction techniques. We construct four system of equations of the form $e_s d - k_s \phi(N_s) = 1$, $e_s d_s - k\phi(N_s) = 1$, $e_s d - k\phi(N_s) = z_s$ and $e_s d_s - k\phi(N_s) = z_s$ using $N - \left\lceil \left(\frac{a^{\frac{i+1}{i}} + b^{\frac{i+1}{i}}}{2(ab)^{\frac{i+1}{2i}}} + \frac{a^{\frac{1}{j}} + b^{\frac{1}{j}}}{2(ab)^{\frac{1}{2j}}} \right) \sqrt{N} \right\rceil + 1$ as a good approximations of $\phi(N_s)$ for unknown positive integers d, d_s, k_s, k, and z_s . In our attacks, we found an improved short decryption exponent bound of some reported attacks.

Keywords: RSA Moduli, Simultaneous, Diophantine, Approximations, Lattice, Basis, Reduction, LLL algorithm, etc.

1. Introduction

The increased day to day applications of shared telecommunications channels, particularly wireless and local area networks(LAN's), results to larger connectivity, but also to a much greater opportunity to intercept data and forge messages. The only practical way to maintain privacy and integrity of information is by using public-key cryptography, Yan (2008).

The most widely used public-key cryptosystem is RSA. It was developed in Rivest. et al. (1978). The RSA cryptosystem setup involves randomly selecting two large prime numbers p, q whose product $N = pq$ known as the RSA modulus and a public key pair (N, e) used in encrypting message where e is randomly generated and a private key pair (N, d) used in decrypting the ciphertext. The two parameters e, d are connected by $ed \equiv 1 \pmod{\phi(N)}$ where $\phi(N) = (p-1)(q-1)$ is called the Euler totient function of N. The applications of RSA cryptosystem can be found in areas such as secure telephone, e-commerce, e-banking, smart cards, digital communication in different types of networks Dubey et al. (2014).

The security of RSA cryptosystem as one of the public-key cryptosystems relies on three major problems which include: integer factorization problem, that is the difficulty of factoring the RSA modulus $N = pq$ into two non-trivial prime factors p and q, finding integer solution of the equation $ed = 1 + k\phi(N)$ where only e is known and k, d and $\phi(N)$ are unknown positive integers and finally finding the $e-th$ root of the expression $C = M^e \pmod{N}$. It is therefore recommended for RSA users to generates primes p and q in such a way that the problem of factoring $N = pq$ is computationally infeasible for an adversary. Choosing p and q as strong primes has been recommended as a way of maximizing the difficulty of factoring RSA modulus N.

The use of short decryption exponent is to reduce the decryption time or the signature generation time. Wiener, (1990) proved that RSA is insecure if the decryption exponent is $d < \frac{1}{3}N^{\frac{1}{4}}$ using continued fraction. He showed that d can be found from the convergent of the continued fraction expansion of $\frac{e}{N}$ Wiener (1990). In 2004, Blömer and May reported an improved version of Wiener's attack using generalized key equation of the form $ex - y\phi(N) = z$ for unknown parameters $x < \frac{1}{3}N^{\frac{1}{4}}$ and $|z| < exN^{\frac{-3}{4}}$ by using a combinations of continued fraction method and lattice basis reduction methods. We emphasize that the continued fraction technique is still widely used for current algebraic cryptanalysis, for instance, Asbullah and Ariffin (2016a) and Asbullah and Ariffin (2016b).

Also, Hinek (2007), proved that k RSA moduli N_i can be factored if $d < N^\gamma$ for $\gamma = \frac{k}{2(k+1)} - \varepsilon$ where ε is a small constant to be determined by considering the size of $\max N_i$. Another instances of factoring generalized key equations was reported by Nitaj et al. (2014). Nitaj et al. (2014), presented two scenarios which showed that k RSA moduli $N_i = p_i q_i$ can be factored simultaneously in polynomial-time. In the first scenario, they proved that if the given equation $e_i x - y_i \phi(N_i)$ is satisfied where $x < N^\delta$, $y_i < N^\delta$, and $|z_i| < \frac{p_i - q_i}{3(p_i+q_i)} y_i N^{\frac{1}{4}}$ for $\delta = \frac{k}{2(k+1)}$, $N = \min\{N_i\}$ then RSA moduli N_i can be factored simultaneously and the second scenario showed that k instances of RSA public key pairs (N_i, e_i) satisfying generalized key equation $e_i d_i - y\phi(N_i) = z_i$ for unknown integers x_i, y, and z_i where $x < N^\delta$, $y_i < N^\delta$ and $|z_i| < \frac{p_i - q_i}{3(p_i+q_i)} y_i N^{\frac{1}{4}}$ for all $\delta = \frac{k(2\alpha-1)}{2(k+1)}$, $N = \min\{N_i\}$ and $\min\{e_i\} = N^\alpha$. They applied simultaneous Diophantine approximations and lattice basis reduction techniques and finally use the Coppersmith's method to compute prime factors p_i and q_i of RSA moduli N_i in polynomial time.

Similarly, Isah et al. (2018) presented some results where we established that if the short decryption exponent $d < \sqrt{\frac{a^j+b^i}{2}} \left(\frac{N}{e}\right)^{\frac{1}{2}} N^{0.375}$ then $\frac{k}{d}$ can be found from the convergent of the continued fraction expansion of $\frac{e}{N_1}$, where $N - \left\lceil \left(\frac{a^{\frac{i+1}{i}} + b^{\frac{i+1}{i}}}{2(ab)^{\frac{i+1}{2i}}} + \frac{a^{\frac{1}{j}} + b^{\frac{1}{j}}}{2(ab)^{\frac{1}{2j}}} \right) \sqrt{N} \right\rceil + 1$ where a, b, i, j are small positive integers which led to the factorization of N in polynomial time, Abubakar et al. (2018). This paper presents four attacks on t instances of RSA public key pair (N_s, e_s) for $s = 1, \ldots, t$ satisfying the following equations $e_s d - k_s \phi(N_s) = 1$, $e_s d_s - k\phi(N_s) = 1$, $e_s d - k_s \phi(N_s) = z_s$ and $e_s d_s - k\phi(N_s) = z_s$ where d, d_s, k, k_s, and z_s are unknown positive integers. In the first attack, we show that t RSA moduli $N_s = p_s q_s$ can be efficiently factored if there exists an integer d and t integers k_s such that $e_s d - k_s \phi(N_s) = 1$ is satisfied. We show that the prime factors p_s and q_s of t moduli N_s for $s = 1, \ldots, t$ can be found efficiently if $N = \max\{N_s\}$ and $d < N^\gamma,\ k_s < N^\gamma,\ for\ all\ \gamma = \frac{t(1+\beta)}{3t+1}$ for $\beta < \gamma \leq \frac{1}{2}$. In the second attack, we also show that the t instances of RSA moduli can be simultaneously factored if the equation $e_s d_s - k\phi(N_s) = 1$ is satisfied for integers $d_s < N^\gamma,\ k < N^\gamma,\ for\ \gamma = \frac{t(\alpha+\beta)}{3t+1}$, $N = \max\{N_s\}$ and $e_s = \min e_s$. In the third attack, we also show that a generalized key equation $e_s d - k_s \phi(N_s) = z_s$ can be factored using simultaneous Diophantine approximations and lattice basis reduction methods if $d < N^\gamma,\ k_s < N^\gamma,\ z_s < N^\gamma$ for all $\gamma = \frac{t(1+\beta)}{3t+1}$ and $N = \max N_s$. In the final attack, the paper presents an attack on t RSA moduli $N_s = p_s q_s$ satisfying an equation $e_s d_s - k\phi(N_s) = z_s$ in which we show that the attack can simultaneously factor t RSA moduli if $d_s < N^\gamma,\ k < N^\gamma, z_s < N^\gamma$ for all $\gamma = \frac{t(\alpha+\beta)}{3t+1}$ where $e_s = \min\{e_s\} = N^\alpha$ and $N = \max\{N_s\}$.

The rest of the paper is organize as follows. In Section 2, we present review of some preliminaries results, some previous theorems on t instances of RSA public key pair (N_i, e_i) which simultaneously factored t RSA moduli $N_i = p_i q_i$ using simultaneous Diophantine approximations and lattice basis reduction techniques . In Section 3 , we present the proofs of our main results with lemmas and theorems and their respective numerical examples and finally in Section 4, we conclude the paper.

2. Preliminaries

In this section, we state some definitions and theorems related to t instances of RSA public key pair (N_i, e_i) that simultaneous factored RSA moduli $N_i = p_i q_i$ using simultaneous Diophantine approximations and lattice basis reduction techniques.

Definition 2.1. *Let $\vec{b_1}, \ldots, \vec{b_m} \in \mathcal{R}^n$. The vectors $\mathbf{b_i'}$s are said to be linearly dependent if there exist $x_1, \ldots, x_m \in R$, which are not all zero such that*

$$\sum_{i}^{m}(x_i \mathbf{b_i} = \mathbf{0}).$$

Otherwise, they are said to be linearly independent.

Definition 2.2. *(Lenstra et al., 1982): Let n be a positive integer. A subset $\mathcal{L}$ of an n-dimensional real vector space $\mathcal{R}^n$ is called a lattice if there exists a basis $b_1, \ldots, b_n$ on $\mathcal{R}^n$ such that $\mathcal{L} = \sum_{i=1}^{n} \mathcal{Z} b_i = \sum_{i=1}^{n} r_i b_i : r_i \in \mathcal{Z}, 1 \leq i \leq n$. In this situation, we say that $b_1, \ldots, b_n$ are basis for $\mathcal{L}$ or that they span $\mathcal{L}$.*

Definition 2.3. *(LLL Reduction) Nitaj (2012) Let $\mathcal{B} = \langle b_1, \ldots, b_n \rangle$ be a basis for a lattice $\mathcal{L}$ and let $B^* = \langle b_1^*, \ldots, b_n^* \rangle$ be the associated Gram- Schmidt orthogonal basis. Let*

$$\mu_{i,j} = \frac{\langle b_i, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle} for 1 \leq j < i$$

The basis $\mathcal{B}$ is said to be LLL reduce if it satisfies the following two conditions:

1. $\mu_{i,j} \leq \frac{1}{2}$, *for* $1 \leq j < i \leq n$
2. $\frac{3}{4}||b_{i-1}^*||^2 \leq ||b_i^* + \mu_{i,i-1} b_{i-1}^*||^2$ *for* $1 \leq i \leq n$. *Equivalently, it can be written as*

$$||b_i^*||^2 \geq (\frac{3}{4} - \mu_{i,i-1}^2)||b_{i-1}^*||^2$$

Theorem 2.1. *(Blömer,2004) Let (N, e) be RSA public key pair with modulus $N = pq$ and the prime difference $p - q \geq cN^{\frac{1}{2}}$. Suppose that the public exponent $e \in \mathcal{Z}_{\phi(N)}$ satisfies an equation $ex + y = k\phi(N)$ with*

$$0 < x < \frac{1}{3}N^{\frac{1}{4}} \quad and \quad |y| \leq N^{\frac{-3}{4}}ex$$

for $c \leq 1$. Then N can be factored in polynomial time.

Theorem 2.2. *(Lenstra, 1982) Let $\mathcal{L}$ be a lattice basis of dimension n having a basis $v_1, \ldots, v_n$. The LLL algorithm produces a reduced basis $b_1, \ldots, b_n$ satisfying the following condition*

$$||b_1|| \leq ||b_2|| \leq \cdots \leq ||b_j|| \leq 2^{\frac{n(n-1)}{4(n+1-j)}} det(\mathcal{L})^{\frac{1}{n+1-j}}$$

for all $1 \leq j \leq n$, Lenstra et al. (1982).

Theorem 2.3. *(Nitaj et al. 2014) (Simultaneous Diophantine Approximations) Given any rational numbers of the form $\alpha_1, \ldots, \alpha_n$ and $0 < \varepsilon < 1$,there is a polynomial time algorithm to compute integers $p_1, ..., p_n$ and a positive integer q such that*

$$max_i\, |q\alpha_i - p_i| < \varepsilon \quad and \quad q \leq 2^{\frac{n(n-3)}{4}}.3^n.\varepsilon^{-n}.$$

Theorem 2.4. *Nitaj et al. (2014) Let $N_i = p_i q_i$ be k RSA moduli for $i = 1, \ldots, k$ for $k \geq 2$ and $N = \min\{N_i\}$. Let e_i, $i = 1, \ldots, k$, be k public exponents. Define $\delta = \frac{k}{2(k+1)}$. If there exist an integer $x < N^\delta$ and k integers $y_i < N^\delta$ and $|z_i| < \frac{p_i - q_i}{3(p_i + q_i)} y_i N^{1/4}$ such that $e_i x - y_i \phi(N_i) = z_i$ for $i = 1, \cdots, k$, then one can factor the k RSA moduli $N_1, \ldots, N_k$ in polynomial time.*

Theorem 2.5. *Nitaj et al. (2014) Let $N_i = p_i q_i$ be k RSA moduli for $i1, \ldots, k$ for $k \geq 2$ where $q < p < 2q$. Let e_i, $i = 1, \cdots, k$, be k public exponents with $\min\{e_i\} = N^\alpha$. Let $\delta = \frac{(2\alpha - 1)k}{2(k+1)}$. If there exist an integer $y < N^\delta$ and k integers $x_i < N^\delta$ and $|z_i| < \frac{p_i - q_i}{3(p_i + q_i)} y N^{1/4}$ such that $e_i x_i - y\phi(N_i) = z_i$ for $i = 1, \ldots, k$, then one can factor the k RSA moduli $N_1, \ldots, N_k$ in polynomial time.*

3. Results

In this section, we present some theorems and their proofs with numerical examples to show how the attacks are carried out to simultaneously factor t RSA moduli.

Lemma 3.1. *If a and b are positive integers less than* $\log\ N$ *and p and q are prime numbers such that $a > b$ and $ap^j - bq^j \neq 0$ and $N = pq$, then* $\phi(N) < N - \left\lceil \frac{(a+b)^{\frac{1}{j}}}{(ab)^{\frac{1}{2j}}}\sqrt{N} \right\rceil + 1$.

Proof. Let $(ap^j - bq^j)(bp^j - aq^j) > 0$, then we get

$$abp^{2j} - a^2p^jq^j - b^2p^jq^j + abq^{2j} > 0$$
$$ab(p^{2j} + q^{2j}) > (a^2 + b^2)p^jq^j.$$

Adding $2abp^jq^j$ to both sides we have:

$$ab(p^{2j} + 2p^jq^j + q^{2j}) > (a^2 + 2ab + b^2)p^jq^j$$
$$(p^j + q^j)^2 > \frac{(a+b)^2p^jq^j}{ab}$$
$$p^j + q^j > \frac{(a+b)(p^jq^j)^{\frac{1}{2}}}{\sqrt{ab}}.$$

Since $(p+q)^j > p^j + q^j$, then

$$p + q > \frac{(a+b)^{\frac{1}{j}}}{(ab)^{\frac{1}{2j}}}\sqrt{N}.$$

Then $\phi(N) < N - \left\lceil \frac{(a+b)^{\frac{1}{j}}}{(ab)^{\frac{1}{2j}}}\sqrt{N} \right\rceil + 1.$ □

Lemma 3.2. *If a and b are small positive integers and p and q are prime numbers such that $a^jp^i - b^jq^i \neq 0$ and $N = pq$ is RSA modulus satisfying the condition $e < \phi(N)$, then $\phi(N) > N - \left\lceil \frac{(a+b)^{\frac{j}{i}}}{(ab)^{\frac{j}{2i}}}\sqrt{N} \right\rceil + 1$, for $2 < i < j$ and $a > b$.*

Proof. Let $(a^jp^i - b^jq^i)(b^jp^i - a^jq^i) < 0$, then we get

$$a^jb^jp^{2i} - a^{2j}p^iq^i - b^{2j}p^iq^i + a^jb^jq^{2i} < 0$$
$$a^jb^j(p^{2i} + q^{2i}) < (a^{2j} + b^{2j})p^iq^i.$$

Adding $2a^jb^jp^iq^i$ to both sides we have

$$a^jb^j(p^i+q^i)^2 < (a^j+b^j)^2p^iq^i$$
$$(p^i+q^i)^2 < \frac{(a^j+b^j)^2}{a^jb^j}N^i$$
$$p^i+q^i < \frac{a^j+b^j}{(ab)^{\frac{j}{2}}}N^{\frac{i}{2}}.$$

Since $p^i+q^i < (p+q)^i$, then

$$p+q < \frac{(a+b)^{\frac{j}{i}}}{(ab)^{\frac{j}{2i}}}\sqrt{N}.$$

Taking $j = i+1$, we have $\phi(N) > N - \left\lceil \frac{(a+b)^{\frac{i+1}{i}}}{(ab)^{\frac{i+1}{2i}}}\sqrt{N} \right\rceil + 1.$ □

Theorem 3.1. *Let p and q be distinct prime numbers and let $N = pq$ be RSA modulus where (N, e) are public key pair with condition $e < \phi(N)$. If $d < \sqrt{\frac{a^{i+1}+b^i}{2}(\frac{N}{e})^{\frac{1}{2}}N^{0.375}}$ and $N_1 = N - \left\lceil \left(\frac{a^{\frac{i+1}{i}}+b^{\frac{i+1}{i}}}{2(ab)^{\frac{i+1}{2i}}} + \frac{a^{\frac{1}{j}}+b^{\frac{1}{j}}}{2(ab)^{\frac{1}{2j}}} \right)\sqrt{N} \right\rceil + 1$, for $i > 2$ then one of the convergent $\frac{k}{d}$ can be found from the continued fraction expansion of $\frac{e}{N_1}$ which leads to the factorization of RSA modulus N in polynomial time.*

Proof. See Abubakar et al. (2018) □

3.1 System of Equation Using $N - \left\lceil \left(\frac{a^{\frac{i+1}{i}}+b^{\frac{i+1}{i}}}{2(ab)^{\frac{i+1}{2i}}} + \frac{a^{\frac{1}{j}}+b^{\frac{1}{j}}}{2(ab)^{\frac{1}{2j}}} \right)\sqrt{N} \right\rceil + 1$ as Approximation of $\phi(N)$

In this section, we present four attacks on t RSA moduli $N_s = p_sq_s$ using system of equations of the form $e_sd - k_s\phi(N_s) = 1$, $e_sd_s - k\phi(N_s) = 1$, $e_sd - k_s\phi(N_s) = z_1$ and $e_sd_s - k\phi(N_s) = z_1$ for $s = 1, \ldots, t$, for $3 \geq j < i$ in which we successfully factor t RSA moduli in polynomial time.

3.1.1 The Attack on t RSA Moduli $N_s = p_sq_s$ Satisfying $e_sd - k_s\phi(N_s) = 1$

Taking $t \geq 2$, let $N_s = p_sq_s$ be t RSA moduli, for $s = 1, \ldots, t$. The attack works for t instances (N_s, e_s) when there exists integer d and t integers k_s satisfying $e_sd - k_s\phi(N_s) = 1$. We show that prime factors p_s and q_s of t RSA moduli N_s for $s = 1, \ldots, t$, $3 \geq i < j$ can be found efficiently for $N = \max\{N_s\}$ and $d < N^{\sigma}$, $k_s < N^{\sigma}$, for all $\sigma = \frac{t(1+\beta)}{3t+1}$ for $\beta < \sigma \leq \frac{1}{2}$.

Theorem 3.2. *Let $N_s = p_s q_s$ be RSA moduli for $i = 3, \ldots, j$, $s = 1, \ldots, t$ and $t \geq 2$. Let (e_s, N_s) be public key pair and (d, N_s) be private key pair with condition $e_s < \phi(N_s)$ and a relation $e_s d \equiv 1 \pmod{\phi(N_s)}$ is satisfied. Let $N = \max\{N_s\}$, if there exists positive integers $d < N^{\gamma}$, $k_s < N^{\gamma}$ for all $\gamma = \frac{t(1+\beta)}{3t+1}$ such that equation $e_s d - k_s \phi(N_s) = 1$ holds, for $\beta < \gamma \leq \frac{1}{2}$, then t RSA moduli N_s can be successfully recovered in polynomial time.*

Proof. Given $t \geq 2$, $i = 3, \ldots, j$ and suppose $N_s = p_s q_s$ be t RSA moduli for $s = 1, \ldots, t$. Suppose that $N = \max\{N_s\}$ and $k_s < N^{\gamma}$. Then the equation $e_s d - k_s \phi(N_s) = 1$ can be rewritten as follows

$$e_s d - k_s(N_s - (p_s + q_s) + 1) = 1$$

$$e_s d - k_s(N_s - (N_s - \phi(N_s) + 1) + 1) = 1.$$

Let $\varPhi = \left\lceil \left(\frac{a^{\frac{i+1}{i}} + b^{\frac{i+1}{i}}}{2(ab)^{\frac{i+1}{2i}}} + \frac{a^{\frac{1}{j}} + b^{\frac{1}{j}}}{2(ab)^{\frac{1}{2j}}} \right) \sqrt{N_s} \right\rceil$

$$e_s d - k_s \left(N_s - \varPhi + \varPhi - (N_s - \phi(N_s) + 1) + 1\right) = 1$$

$$\left| \frac{e_s}{N_s - \varPhi + 1} d - k_s \right| = \frac{\left|1 - k_s \left(N_s - \phi(N_s) + 1 - \varPhi\right)\right|}{N_s - \varPhi + 1}. \tag{1}$$

Setting $N = \max\{N_s\}$, $k_s < N^{\gamma}$, $d < N^{\gamma}$ be positive integers and suppose that

$$\begin{aligned} |\varPhi + \phi(N_s) - N_s - 1| &< N^{2\gamma - \beta} \\ N_s - \varphi + 1 &> \frac{a}{b^2} N. \end{aligned}$$

Plugging the conditions into equation (1) gives the following

$$\begin{aligned} \frac{\left|1 - k_s \left(N_s - \phi(N_s) + 1 - \varPhi\right)\right|}{N_s - \varPhi + 1} &< \frac{\left|1 + k_s \left(\varPhi - N_s + \phi(N_s) - 1\right)\right|}{N_s - \varphi + 1} \\ &< \frac{1 + N^{\gamma}(N^{2\gamma - \beta})}{\frac{a}{b^2} N} \\ &= \frac{b^2(1 + N^{3\gamma - \beta})}{aN} \\ &< \left(\frac{a}{b}\right)^{\frac{i}{j}} N^{3\gamma - \beta - 1}. \end{aligned}$$

Then, it follows that

$$\left|\frac{e_s}{N_s - \Phi + 1}d - k_s\right| < \left(\frac{a}{b}\right)^{\frac{i}{j}} N^{3\gamma-\beta-1}.$$

We next proceed to show the existence of integer d and t integers k_s. We let $\varepsilon = \left(\frac{a}{b}\right)^{\frac{i}{j}} N^{3\gamma-\beta-1}$, with $\gamma = \frac{t(1+\beta)}{3t+1}$. Then we have

$$N^{\gamma}\varepsilon^{t} = N^{\gamma}\left(\left(\frac{a}{b}\right)^{\frac{i}{j}} N^{3\gamma-\beta-1}\right)^{t} = (\frac{a}{b})^{\frac{it}{j}} N^{\gamma+3\gamma t-\beta t-t} = (\frac{a}{b})^{\frac{t}{2}}.$$

Since $(\frac{a^i}{b^j})^{\frac{it}{j}} < 2^{\frac{t(t-3)}{4}} \cdot 3^t$ for $t \geq 2$, then we get $N^{\gamma}\varepsilon^{t} < 2^{\frac{t(t-3)}{4}} \cdot 3^t$. It follows that if $d < N^{\gamma}$ then $d < 2^{\frac{t(t-3)}{4}} \cdot 3^t \cdot \varepsilon^{-t}$, we have

$$\left|\frac{e_s}{N_s - \Phi + 1}d - k_s\right| < \varepsilon, \qquad d < 2^{\frac{t(t-3)}{4}} \cdot 3^t \cdot \varepsilon^{-t}.$$

This satisfies the conditions of Theorem 2.3 and we proceed to find integer d and t integers k_s for $s = 1, \ldots, t$. Next, from equation $e_s d - k_s\phi(N_s) = 1$ we compute the following:

$$\phi(N_s) = \frac{e_s d - 1}{k_s}$$

$$p_s + q_s = N_s - \phi(N_s) + 1$$
$$x^2 - (N_s - \phi(N_s) + 1)x + N_s = 0.$$

Finally, by finding the roots of the quadratic equation, the prime factors p_s and q_s can be revealed which lead to the factorization of t RSA moduli N_s for $s = 1, \ldots, t$. □

Let

$$X_1 = \frac{e_1}{N_1 - \left\lceil\left(\frac{a^{\frac{i+1}{i}} + b^{\frac{i+1}{i}}}{2(ab)^{\frac{i+1}{2i}}} + \frac{a^{\frac{1}{j}} + b^{\frac{1}{j}}}{2(ab)^{\frac{1}{2j}}}\right)\sqrt{N_1}\right\rceil + 1}$$
$$X_2 = \frac{e_2}{N_2 - \left\lceil\left(\frac{a^{\frac{i+1}{i}} + b^{\frac{i+1}{i}}}{2(ab)^{\frac{i+1}{2i}}} + \frac{a^{\frac{1}{j}} + b^{\frac{1}{j}}}{2(ab)^{\frac{1}{2j}}}\right)\sqrt{N_2}\right\rceil + 1}$$
$$X_3 = \frac{e_3}{N_3 - \left\lceil\left(\frac{a^{\frac{i+1}{i}} + b^{\frac{i+1}{i}}}{2(ab)^{\frac{i+1}{2i}}} + \frac{a^{\frac{1}{j}} + b^{\frac{1}{j}}}{2(ab)^{\frac{1}{2j}}}\right)\sqrt{N_3}\right\rceil + 1}$$

Consider the lattice $\mathcal{L}$ spanned by the matrix

$$M = \begin{bmatrix} 1 & -[C(X_1)] & -[C(X_2)] & -[C(X_3)] \\ 0 & C & 0 & 0 \\ 0 & 0 & C & 0 \\ 0 & 0 & 0 & C \end{bmatrix}$$

Also input $a = 3,\ b = 2,\ j = 4,\ t = 3$ and $i = 3$ as small positive integers. The above matrix M will be used for computing required reduced basis which leads to successful factoring of moduli N_s for $s = 1, \ldots, t$.

Table 1: Algorithm for factoring RSA moduli $N_s = p_s q_s$ for $e_s d - k_s \phi(N_s) = 1$ of Theorem 3.2

INPUT: The public key tuple (N_s, e_s, σ) satisfying Theorem 3.2.

OUTPUT: The prime factors p_s and q_s.

1. Compute $\varepsilon = \left(\frac{a}{b}\right)^{\frac{i}{j}} N^{3\sigma-\beta-1}$, where $N = \max\{N_s\}$ for $s = 1, \ldots, t$, $\beta < \sigma \leq \frac{1}{2}$ and $a > b$.
2. Compute $C = [3^{t+1} \cdot 2^{\frac{(t+1)(t-4)}{4}} \cdot \varepsilon^{-t-1}]$ for $t \geq 2$.
3. Consider the lattice $\mathcal{L}$ spanned by the matrix M as stated above.
4. Applying the LLL algorithm to $\mathcal{L}$, we obtain the reduced basis matrix K.
5. Compute $J = M^{-1}$.
6. Compute $Q = JK$ to produce integer d and t integers k_s for $s = 1 \ldots, t$.
7. Compute $\phi(N_s) = \frac{e_s d - 1}{k_s}$ for $s = 1, \ldots, t$.
8. Compute $N_s - \phi(N_s)+1$.
9. Solve the quadratic equation $x^2 - (N_s - \phi(N_s) + 1)x + N_s = 0$.
10. Then output the roots of the equation as p_s and q_s for $s = 1, \ldots, t$.

Example 3.1. *In what follows, we give an illustration to show how Theorem*

3.2 works on 3 RSA moduli and their corresponding public exponents: Let

$$\begin{aligned}
N_1 \quad = \quad & 6873759006499876318806143993197356564591388266671764381824926\\
& 3846051525412519477341947854641345828302449064555046022658532\\
& 2294757161953899804299046773862357772238793538346038690333358\\
& 4005355615949819852825099249580914306069158122568478713851337\\
& 9297105644771277087971272536948011093049702148354789189194680\\
& 7378961261693885067649290531129757984797441797978880421889884\\
& 4938375945264466689615792890611317250548197417336207014476483\\
& 4099357391502750121741231747591044796068015398327404507739611\\
& 2140179292264918180345351177923138063579852385919236227751980\\
& 4955061306507800411759709768988763372228548308239065587556264\\
& 454521
\end{aligned}$$

$$\begin{aligned}
N_2 \quad = \quad & 6873759006499876318806143993197356564591388266671764381824926\\
& 7844181203918265072709146693385362771399837104508302530605547\\
& 7578563691758443580670089792237291021205227470484658605927963\\
& 0183716564607314293229098374753748839266068589770120701997873\\
& 0607996611048310203178053273608613824614890848421930274235576\\
& 1728874810851036160417484819782253601577312336352969195141625\\
& 3277146634354443879199361296961781013613991043578887980883412\\
& 6302224046543243911354519858608423657878981907425836256862367\\
& 5631721550745656583734569695446525649246881269398127476965115\\
& 3001286334451806875770579694109475342828781134506112848187247\\
& 5811456149592808848044135907640086362341746144237314114206092\\
& 4475533
\end{aligned}$$

$$
\begin{aligned}
N_3 = {} & 8978139558472362675873367508731483070511520914060463888155026\\
& 1388928088778065844511827653848185447102581197560657340302537\\
& 8111410341951027371148973259338530549228638186507249798434636\\
& 2980876969880857643563960910844555358165030055640958729707728\\
& 0554263508473112207932398227170321064490121048310237056891329\\
& 5830669060755842391713804406388292714270464770346737668464215\\
& 5354233976928129457338829423595874460595457212461912834775228\\
& 2247082540729123802116973627850647882737066228541102586794719\\
& 3127513376185237230986463004307926102019124994508881206205365\\
& 5308947554364568356384242213969998323148216121283612455796817\\
& 545379
\end{aligned}
$$

$$
\begin{aligned}
e_1 = {} & 2655596774191944112368935733634869417398335543575728971240447\\
& 8501596577009193302839124857406930246492853575725109088184349\\
& 9006927411709255255922739531924336011072672986262282732654731\\
& 9709585298825633727012585324352521162977634816903358929973590\\
& 6726569408454092611085327817025242382554638889567210806243119\\
& 5530302853178637011285349145211416103389461701990856119478336\\
& 2682180561374505114559411405728656644490977959211960989049384\\
& 6189057792305777375878001634296635879452858499104866220270414\\
& 4969178976900294459165402153720145113449807943118999248613601\\
& 5673571155128036701732252704602271698931905924083705251619145\\
& 944309
\end{aligned}
$$

$$
\begin{aligned}
e_2 = {} & 2137745452908426791531742811783474397659260072423118418529723\\
& 1372064771035649088448013128296348832537804035825327721170489\\
& 1255984069379198925155608924379540042740361215100326292175421\\
& 0173002638767016670991056518566884505098318855462539320915538\\
& 8868593919903505503692350147451275178922089935514586090984763\\
& 6238068913104272975193992317380535596708790612428893128610184\\
& 3138182503063563344841084528340368084427577651608221100811177\\
& 7867853094388593898728031601497941742777391724040370716152221\\
& 9128194178458922078879557955267787939397480551344365322841503\\
& 9061482163394965150561205571395599983210195227888058502310633\\
& 024525
\end{aligned}
$$

$$
\begin{aligned}
e_3 \;=\;& 3376302598271191870188405364071713065607100240181184699662570 \\
& 2255086258436583211335843258793030936072336392983215856540479 \\
& 9953125779525511439128291020834389613374068416205032628729198 \\
& 1614581551642757897767829436911032605178624200673043346061001 \\
& 2142248700441721659939208924087950529260916887929812535473932 \\
& 1817090001202244567834249200232976426215389468855576323277726 \\
& 1862370550936835074376899622865460438674567718027330038509377 \\
& 5099874246378735790918793792747677982857557119205283807903203 \\
& 9392650709827067367352258205096098914166051373859769018576614 \\
& 8835065491259971934045455754080194274389976593356624639028151 \\
& 554549
\end{aligned}
$$

Observe $N = \max\{N_1, N_2, N_3\}$,

$$
\begin{aligned}
N \;=\;& 8978139558472362675873367508731483070511520914060463888155026 \\
& 1388928088778065844511827653848185447102581197560657340302537 \\
& 8111410341951027371148973259338530549228638186507249798434636 \\
& 2980876969880857643563960910844555358165030055640958729707728 \\
& 0554263508473112207932398227170321064490121048310237056891329 \\
& 5830669060755842391713804406388292714270464770346737668464215 \\
& 5354233976928129457338829423595874460595457212461912834775228 \\
& 2247082540729123802116973627850647882737066228541102586794719 \\
& 3127513376185237230986463004307926102019124994508881206205365 \\
& 5308947554364568356384242213969998323148216121283612455796817 \\
& 545379
\end{aligned}
$$

Taking $t = 3$, *we have* $\sigma = \frac{t(1+\beta)}{3t+1} = 0.360$ *and* $\varepsilon = \left(\frac{a}{b}\right)^{\frac{i}{j}} N^{3\sigma-\beta-1} = 1.650768155 \times 10^{-74}$. *Applying Theorem 2.3 for* $n = t = 3$ *we compute*

$$C = [3^{t+1} \cdot 2^{\frac{(t+1)(t-4)}{4}} \cdot \varepsilon^{-t-1}]$$

$$
\begin{aligned}
C \;=\;& 5453944245000000000000000000000000000000000000000000000000000 \\
& 0000000000000000000000000000000000000000000000000000000000000 \\
& 0000000000000000000000000000000000000000000000000000000000000 \\
& 0000000000000000000000000000000000000000000000000000000000000 \\
& 00000000000000000000000000000000000000000000000000000
\end{aligned}
$$

Consider the lattice $\mathcal{L}$ *spanned by the matrix*

$$M = \begin{bmatrix} 1 & -[C(X_1)] & -[C(X_2)] & -[C(X_3)] \\ 0 & C & 0 & 0 \\ 0 & 0 & C & 0 \\ 0 & 0 & 0 & C \end{bmatrix}$$

Therefore, by applying the LLL algorithm to $\mathcal{L}$, we obtain reduced basis with following matrix

$$K = \begin{bmatrix} A_{11} & A_{12} & A_{13} & A_{14} \\ B_{11} & B_{12} & B_{13} & B_{14} \\ C_{11} & C_{12} & C_{13} & C_{14} \\ D_{11} & D_{12} & D_{13} & D_{14} \end{bmatrix}$$

where

$$\begin{aligned} A_{11} &= 6059171132112429370227828012581845104164008148990042013797541 \\ &\quad 9140872732217516309085619258940600739427834221565424466839826 \\ &\quad 9578297613560979072176306252357569225734821095555675380913166 \\ &\quad 832634661106754662488616099056785385589 \\ A_{12} &= 6800583981171717241577599736578815180114240756874229033882279 \\ &\quad 5998283251793363259789070846584989247833233640877551305300099 \\ &\quad 1536327844175667981009967877404370215470311589181379531856784 \\ &\quad 65119824864286858214207512779514173 54 \\ A_{13} &= 5856340701315242563153348516943422939173792145408460319569249 \\ &\quad 0139823375558125147734468127787499591851124594365096123870162 \\ &\quad 8196744465226306783146956887212216292158721596169098004285729 \\ &\quad 698912298496206489699850615301577 90174 \\ A_{14} &= 3528786261647555852229497420785428604674128437766283217131054 \\ &\quad 1894672299649975694881953525933282557858125704672982122851973 \\ &\quad 0169754693217292921174539810256414344000362227371359620271077 \\ &\quad 342924451105759962622852547199201 57942 \end{aligned}$$

$$
\begin{aligned}
B_{11} &= 6485305148842603073254473445733872192861516473847813363352444\\
&\quad 6748784751837606998144127764756312526278989428939457673635997\\
&\quad 1934513893737128853530585970252343214334105471630794307655801\\
&\quad 498923861020470398031560982125764725084\\
B_{12} &= -70696472602177265331143656712619611810496372012502761162314 2\\
&\quad 7539191630039889136160588696462882491400181951760642256218762\\
&\quad 9788428188047930793461066437952642437958848437023797397659666\\
&\quad 7491995717955371053027179022480232508 5576\\
B_{13} &= 2538424016210092518054803535189846526159866714582452429451 11\\
&\quad 1659831369896498691216063860335401571860587093213225162367 84\\
&\quad 1543471984160542359450880271274747825071544674609853047934 19\\
&\quad 508538349313094840307234531213644261825 0344\\
B_{14} &= -20273926105471824014697978269645704341858222667856911273321 0\\
&\quad 1657016914411582988568155521091280475459703089461549444068241\\
&\quad 4076020056995897251101978011131825849071656921991061809225804\\
&\quad 341641084906142354998197734729945795 5448
\end{aligned}
$$

$$
\begin{aligned}
C_{11} &= 2059664963139457188110847531253351499121304309331725416349 42\\
&\quad 0970032434465486369971170456495961279859556791403102953265 40\\
&\quad 9444419641531614988135854465414838138903904372139099224221 06\\
&\quad 680331300199866174943809864451304130402 7107\\
C_{12} &= -3637455195068763770466417320548596097683973526297894244423\\
&\quad 8138258551008077343133798437292031870242581291067184854536 26\\
&\quad 0438494497738581211779811283724335041939503487389286091133 68\\
&\quad 758609333834110829515358177495290215799650698\\
C_{13} &= -5205119373155228047055224271360717839670487507036561829528\\
&\quad 4751605611267790530799354244330673473781227581224104571542 99\\
&\quad 1746188160866749306698761043825903559723765747467664196587 43\\
&\quad 254928922300310475104237609195533827705683038\\
C_{14} &= 6881783648364273724288594487141594092826468761202093979393 24\\
&\quad 1954250606821320210940397303559751164269941046589821345169 26\\
&\quad 1446167232323205589624133853385392142778330247481952801070 67\\
&\quad 873826268006990706231150822761014261743 8346
\end{aligned}
$$

$$
\begin{aligned}
D_{11} &= -15670375536279242003650070460157850805583635125144181927002919988646065507701448977752602127271548995662657187839789724777165741419806069656319133286453863860652767025409928905038839527684351916756595398901544180525700058764 \\
D_{12} &= -53094119671157515905032669329339882944938073812923326342622435204203162015943265202709969354972608883644658989836746287605412020994073479671386538727929738276222890847296624378709430741387140753764179312836287287584703549 04 \\
D_{13} &= 884593889254469694171682084467432055158786994908589932468481971207114687276718726540544246089169503338322282424783597039497240506218972401749022448264533913547313456293280513835858929024053946752077457582465323225881143077 6 \\
D_{14} &= 14790890704130541472981948756413109810917792203668397764961753120853606538362107927161171606633869483364680302364142156761466158645761475688841534967932040929992797487082026668739891393521529573149775001244116508461608168408
\end{aligned}
$$

Next we compute $Q = JK$

$$
Q = \begin{bmatrix} E_{11} & E_{12} & E_{13} & E_{14} \\ F_{21} & F_{22} & F_{23} & F_{24} \\ G_{31} & G_{32} & G_{33} & G_{34} \\ H_{41} & H_{24} & H_{43} & H_{44} \end{bmatrix}
$$

where

$$
\begin{aligned}
E_{11} &= 6059171132112429370227828012581845104164008148990042013797541914087273221751630908561925894060073942783422156542446683982695782976135609790721763062523575692257348210955556753809131668326346611067546624886160990567853858 9 \\
E_{12} &= 23408902316038750389994782010468410260059436995698834749355090835125224729071955974224764306374733528010091783138112213698303490239106604655439840642913356584989261582290643215102266582940788728772531288756359513996465200
\end{aligned}
$$

$$
\begin{aligned}
E_{13} &= 16512833142606630115004811481072026078654429925799521433747 2\\
&\ 4901823523195960836746199756576604478736296000681902893884 07\\
&\ 4948164536227523645471136341491612339913298064134436488531 93\\
&\ 92344899326752280314601162291124318656418\\
E_{14} &= 22786007171625955393614063951034915441330944433889707086843 5\\
&\ 7208455567429345463769941156113186831185846979334631237513 56\\
&\ 8775884942429616542457407818232983928024044918700773839897 56\\
&\ 84026195741550966450944037664572599581072
\end{aligned}
$$

$$
\begin{aligned}
F_{21} &= 648530514884260307325447344573387219286151647384781336335244\\
&\ 467487847518376069981441277647563125262789894289394576736359\\
&\ 971934513893737128853530585970252343214334105471630794307655\\
&\ 80149892386102047039803156098212576472 5084\\
F_{22} &= 250552214830796928104434306191780365179349132440120620737425\\
&\ 524620887935780204423052538741060989066425015223804405995034\\
&\ 548142752051132451694406773407133041074819274216889364117715\\
&\ 48598263491747008537632269774860950091 9501\\
F_{23} &= 176741602880574434429720975166023459325114137265491206396832\\
&\ 496367373777294629657840551399770810570918016472588021703193\\
&\ 933162037447414144211894248753329236420312160372552183832594\\
&\ 67187024646887162715376409808988828557 1469\\
F_{24} &= 243885188930439177261877251441269206441242023021553965921986\\
&\ 425723389982598346882757762903998817422665601939906627393842\\
&\ 126713461991372794412512501020114727727423768470589968639220\\
&\ 43897499560987797306320164105151131171 5772
\end{aligned}
$$

$$
\begin{aligned}
G_{31} &= 2059664963139457188110847531253351499121304309331725416349420970032434465486369971170456495961279859556791403102953265409444419641531614988135854465414838138903904372139099224221066803313001998661749438098644513041304027107 \\
G_{32} &= 7957275817870805652201006189252212921241192386830697536101965523334262012722231422394863672708298626738633149254813703874452122031874914829432404590770844663296671696910402021686497338976244416559160264970459857323000443 64 \\
G_{33} &= 5613128120073009906471095280509323939324256304081559521029880539093090087638610097137175850989803073322838250438482715959132515243372489138037172796358442113608324427426860458025095890309747121590489207194147535934570542 03 \\
G_{34} &= 7745538060893236145652145035533792493353879609630295285694878043540200184325862105651174386835947399799141074931843359240966491120330692693480012731456469167325669057025560282942352585029143456809003460426217757907057176 19
\end{aligned}
$$

$$
\begin{aligned}
H_{41} &= -1567037553627924200365007046015785080558363512514418192700\\
&\quad 2919988646065507701448977752602127271548995662657187839789 72\\
&\quad 4777165741419806069656319133286453863860652767025409928905 03\\
&\quad 883952768435191675659539890154418152570005876 4\\
H_{42} &= -6054067168367238876243034290723471619641612044251184828220\\
&\quad 8469413640396633365118804075201765960353169379048521216342 17\\
&\quad 6852583602726130158038830269265711654848697525598583229988 50\\
&\quad 700642466835137450075339773544873687733039195\\
H_{43} &= -4270589010783572899231495551136012574246458580594951657801\\
&\quad 6930152871398230484549596853828216974284173492383122690758 67\\
&\quad 3594266059677920962211470382142963483417899462855013563168 87\\
&\quad 395178099792870263526865739320122399532970701\\
H_{44} &= -5892972513341867815659798977789247910589781024397651168186\\
&\quad 5403765688866770801891297591770243820574809372779496320861 22\\
&\quad 5375643983759341399496878016669466131261002159346157532105 42\\
&\quad 124817884144476374946057920486834741895620193
\end{aligned}
$$

From first row of Q we obtain $d, k_1,\ k_2$ and k_3 as follows:

$$
\begin{aligned}
d &= 6059171132112429370227828012581845104164008148990042013797 54\\
&\quad 1914087273221751630908561925894060073942783422156542446683 98\\
&\quad 2695782976135609790721763062523575692257348210955556753809 13\\
&\quad 166832634661106754662488616099056785385 89\\
k_1 &= 2340890231603875038999478201046841026005943699569883474935 50\\
&\quad 9083512522472907195597422476430637473352801009178313811221 36\\
&\quad 9830349023910660465543984064291335658498926158229064321510 22\\
&\quad 665829407887287725312887563595139964652 00\\
k_2 &= 1651283314260663011500481148107202607865442992579952143374 72\\
&\quad 4901823523195960836746199756576604478736296000681902893884 07\\
&\quad 4948164536227523645471136341491612339913298064134436488531 93\\
&\quad 923448993267522803146011622911243186564 18\\
k_3 &= 2278600717162595539361406395103491544133094443388970708684 35\\
&\quad 7208455567429345463769941156113186831185846979334631237513 56\\
&\quad 8775884942429616542457407818232983928024044918700773839897 56\\
&\quad 840261957415509664509440376645725995810 72
\end{aligned}
$$

We now compute $\phi(N_s) = \frac{e_s d-1}{k_s}$ for $s = 1, 2, 3$. That is:

$$\begin{aligned}
\phi(N_1) \;=\; & 68737590064998763188061439931973565645913882666717643818249 2\\
& 638460515254125194773419478546413458283024490645550460226585\\
& 322294757161953899804299046773862357772238793538346038690333\\
& 358400535561594981985282509924958091430606915812256847871385\\
& 133792971056447712770879712725369480110930497021483547891891\\
& 946807360906095280083909717496446505531479472986033753897760\\
& 367942687288162446822134767302902029299493785165241282825225\\
& 623920362223822049345924474082392120601335215889420685144595\\
& 811139251091531776514757224777370239239633300076336913146576\\
& 473999369370158589950521059851901110403500812176893937099504\\
& 8630070755267200\\
\phi(N_2) \;=\; & 784418120391826507270914669338536277139983710450830253060554\\
& 775785636917584435806700897922372910212052274704846586059279\\
& 630183716564607314293290983747537488392660685897701207019978\\
& 730607996611048310203178053273608613824614890848421930274235\\
& 576172887481085103616041748481978225360157731233635296919514\\
& 162532751562028316287381173037950565587458832439953591139026\\
& 725888203856656197264793082012577143329208120771702368982033\\
& 383214897511242425889202320641960830128452923366191813805353\\
& 442534742799770934799524311337770261069154984217409112166315\\
& 947748907777012844876275123925721944130295749953302496334351\\
& 0419369343056668\\
\phi(N_3) \;=\; & 897813955847236267587336750873148307051152091406046388815502\\
& 613889280887780658445118276538481854471025811975606573403025\\
& 378111410341951027371148973259338530549228638186507249798434\\
& 636298087696988085764356396091084455535816503005564095872970\\
& 772805542635084731122079323982271703210644901210483102370568\\
& 913295810309804959337412093232358779040936236019252541559327\\
& 275375936498645195769915756459950707462479935501936405367606\\
& 940071196318547735104326128510755921219197493948748668265595\\
& 331363085552946018482605313925873605856652404785009531194603\\
& 667223820325515453692232867711762366885551219766212423600874\\
& 2966722938884880
\end{aligned}$$

Also, we proceed to compute $N_s - \phi(N_s) + 1$ for $s = 1, 2, 3$.

$$
\begin{aligned}
N_1 - \phi(N_1) + 1 &= 1805516641380115793179408462422650532445576422498\\
&\quad 2661521941806549432079624534194276387031832231269\\
&\quad 654500450795475823727978769751865681576743329925\\
&\quad 3553091127447907332981294492662568610486475157157\\
&\quad 501609555679809386835047635035154727726597537526\\
&\quad 1112534754070025898132406986649537552504596089372\\
&\quad 44016957485509187322
\end{aligned}
$$

$N_1 - \phi(N_1) + 1 = 18055166413801157931794084624226505324455764224982$
$66152194180654943207962453419427638703183223126965$
$45004507954758237279787697518656815767433299253553$
$09112744790733298129449266256861048647515715750160$
$95556798093868350476350351547277265975375261112534$
$75407002589813240698664953755250459608937244016957$
485509187322

$N_2 - \phi(N_2) + 1 = 19904315228151410820575019052222677307470482197740$
$78210823809836739034597911827250728146509444975821$
$02050568542234791526656609126486764560528150087145$
$24112001321935126007394253976787213092409718544446$
$36802668002559844407040223289481253412356803444330$
$47165337241184139635097906123884436479029630722691$
581418866

$N_3 - \phi(N_3) + 1 = 20359255796504979620572047609251778034445517805178$
$34118883959892475249704302997742299165212496612404$
$37848408236765374516261522776721869118926589803572$
$87281333421913617145430536584107574567357702631917$
$06058939845127369723411546331427753898154520537930$
$17442239679266618545114486125486091885274869489073$
878660500

Finally, solving quadratic equation $x^2 - (N_s - \phi(N_s) + 1)x + N_s$ for $s = 1, 2, 3$ gives us p_1, p_2, p_3 and q_1, q_2, q_1 which lead to the factorization of 3 RSA moduli N_1, N_2, N_3. That is:

$p_1 = 12599651024357937703657870962507050914996560728919746238032 3$
$56805059108860680530849822611044428218420431997713654025222 8$
$40482404177017498078753206348972699234085742876073049033608 8$
$29378475777745190869293996615711540810037123028987315836659 7$
$87484713061020407428758836995509170992965069443605838644675 9$
856020881

$$
\begin{aligned}
p_2 &= 144912796807558235227224448071847089726991649207347724182024\\
&\quad 222904224424246307807314892132273304147585475369132446627841\\
&\quad 072419525104684923701516949551889868917461979250212886412199\\
&\quad 798432583631043448100999635346072672806149552170468670640315\\
&\quad 413279511112706033529388400459627682480890373049785944192653\\
&\quad 667580799\\
p_3 &= 139003037188738962566074612642830443452225212660273650472251\\
&\quad 568209599310351634537275215878176674386285311684308958328894\\
&\quad 785970321757979050842136830517175022646286898260911409072158\\
&\quad 014503113747448580372331966193565931585504803326953181330325\\
&\quad 462356074101577929451389018253165508365397034276878394464475\\
&\quad 925478761\\
q_1 &= 545551538944322022813621366171945440945920349606291528390944\\
&\quad 974437297076385366342656442078780305123406845308182179850513\\
&\quad 828734768866407866457671900633641351070499042205640023264803\\
&\quad 167017173800497008627398432297196395346639244378534391709282\\
&\quad 364063447967985155256523287098620453208089145011856305107256\\
&\quad 53166441\\
q_2 &= 541303554739558729785257424503796833477131727700600969003567\\
&\quad 607696790355448749177579225186711934345165751994097881636855\\
&\quad 841896013820796368266331375933512510957573720098610561275680\\
&\quad 736983404661419963626806314541833116345544701584794547009202\\
&\quad 670649219344593037117957391754702236429940634292436865300379\\
&\quad 13838067\\
q_3 &= 645895207763108336396458634496873368922299653915097614161444\\
&\quad 210379256600786652369547006430729868541525367239278070456214\\
&\quad 755524549638900680844529730556977906879322379105428962936830\\
&\quad 612425598295777387982739277909468053868363513061895940594899\\
&\quad 896977189158643102278776002919489777600890576083964750245979\\
&\quad 53181739
\end{aligned}
$$

From our result, one can observe that we get $d \approx N^{0.3584}$ which is larger than the Blömer-May's bound of $x < \frac{1}{3}N^{0.25}$, Blömer and May (2004). This shows that the Blömer-May's attack can not yield the factorization of t RSA moduli in our case. Our bound $d \approx N^{0.3584}$ is also greater than bound $x =$

$N^{0.344}$ of Nitaj et al. (2014).

3.1.2 The Attack on t RSA Moduli $N_s = p_s q_s$ Satisfying $e_s d_s - k\phi(N_s) = 1$

In this section, we consider second case in which t RSA moduli satisfy t equations of the form $e_s d_s - k\phi(N_s) = 1$ for unknown parameters d_s and k for $s = 1, \ldots, t$.

Theorem 3.3. *Let $N_s = p_s q_s$ be t RSA moduli for $s = 1, \ldots, t$, $i = 3, \ldots, j$ and $t \geq 2$. Let (e_s, N_s) be public key pair and (d_s, N_s) be private key pair with $e_s < \phi(N_s)$ and given relation $e_s d_s \equiv 1 \pmod{\phi(N_s)}$ is satisfied. Let $e = \min\{e_s\} = N^{\alpha}$ be t public exponents. If there exists positive integers $d_s < N^{\sigma}$, $k < N^{\sigma}$*, for all $\sigma = \frac{t(\alpha+\beta)}{3t+1}$ *such that equation $e_s d_s - k\phi(N_s) = 1$ holds, then prime factors p_s and q_s of t RSA moduli N_s can successfully be recovered in polynomial time.*

Proof. For $t \geq 2$ and $i = 3, \ldots, j$. Let $N_s = p_s q_s$ be t RSA moduli for $s = 1, \ldots, t$ and suppose $e = \min\{e_s\} = N^{\alpha}$ be t public exponents for $s = 1, \ldots, t$ and suppose that $d_s < N^{\gamma}$. Then equation $e_s d_s - k\phi(N_s) = 1$ can be rewritten as

$$\begin{aligned} e_s d_s - k(N_s - (p_s + q_s) + 1) &= 1 \\ e_s d_s - k(N_s - (N_s - \phi(N_s) + 1)) &= 1. \end{aligned}$$

Let $\Delta = \left\lceil \left(\frac{a^{\frac{i+1}{i}} + b^{\frac{i+1}{i}}}{2(ab)^{\frac{i+1}{2i}}} + \frac{a^{\frac{1}{j}} + b^{\frac{1}{j}}}{2(ab)^{\frac{1}{2j}}} \right) \sqrt{N_s} \right\rceil$.

$$e_s d_s - k\left(N_s - \Delta + \Delta - (N_s - \phi(N_s) + 1) + 1\right) = 1.$$

Then we can have:

$$\left| k \frac{(N_s - \Delta + 1)}{e_s} - d_s \right| = \frac{\left|1 - k\left(N_s - \phi(N_s) + 1 - \Delta\right)\right|}{e_s}.$$

Taking $N = \max\{N_s\}$ and suppose that $d_s < N^{\gamma}$, $k < N^{\gamma}$ be positive integers and

$$|\Delta + \phi(N_s) - N_s - 1| \quad < \quad N^{2\gamma - \beta}.$$

Suppose also $e = \min\{e_s\} = N^{\alpha}$ for $s = 1, \ldots, t$ then we have

$$\begin{aligned}\frac{|1 - k\left(N_s - \phi(N_s) + 1 - \Delta\right)|}{e_s} &\leq \frac{|1 + k\left(\Delta - N_s + \phi(N_s) - 1\right)|}{e_s} \\ &< \frac{1 + N^{\gamma}(N^{2\gamma-\beta})}{N^{\alpha}} \\ &= \frac{1 + N^{3}\gamma - \beta}{N^{\alpha}} \\ &< \left(\frac{a}{b}\right)^{\frac{i}{2j}} N^{3\gamma-\alpha-\beta}.\end{aligned}$$

Hence, we get:

$$\left|k\frac{(N_s - \Delta + 1)}{e_s} - d_s\right| \quad < \quad \left(\frac{a}{b}\right)^{\frac{i}{2j}} N^{3\gamma-\alpha-\beta}.$$

We now proceed to show the existence of integer k and t integers d_s. Taking $\varepsilon = \left(\frac{a}{b}\right)^{\frac{i}{2j}} N^{3\gamma-\alpha-\beta}$ and $\gamma = \frac{t(\alpha+\beta)}{3t+1}$. Then we get

$$N^{\gamma}\varepsilon^{t} = N^{\gamma}\left(\left(\frac{a}{b}\right)^{\frac{i}{2j}} N^{3\gamma-\alpha-\beta}\right)^{t} = \left(\frac{a}{b}\right)^{\frac{it}{2j}} N^{\gamma+3\gamma t-\alpha t-\beta t} = \left(\frac{a}{b}\right)^{\frac{it}{2j}}.$$

Since $\left(\frac{a}{b}\right)^{\frac{it}{2j}} < 2^{\frac{t(t-3)}{4}} \cdot 3^{t}$ for $t \geq 2$, then $N^{\gamma}\varepsilon^{t} < 2^{\frac{t(t-3)}{4}} \cdot 3^{t}$. It follows that if $k < N^{\gamma}$ then $k < 2^{\frac{t(t-3)}{4}} \cdot 3^{t} \cdot \varepsilon^{-t}$ for $s = 1, \ldots, t$, we have

$$\left|k\frac{(N_s - \Delta + 1)}{e_s} - d_s\right| < \varepsilon, \qquad k < 2^{\frac{t(t-3)}{4}} \cdot 3^{t} \cdot \varepsilon^{-t}.$$

This also satisfies the conditions of Theorem 2.3 and we now proceed to reveal the private key d_s and k for $s = 1, \ldots, t$. Next, from equation $e_s d_s - k\phi(N_s) = 1$ we compute the following:

$$\phi(N_s) = \frac{e_s d_s - 1}{k},\ p_s + q_s = N_s - \phi(N - s) + 1,\ x^2 - (N_s - \phi(N_s) + 1)x + N_s = 0.$$

Finally, by finding the rots of the quadratic equation, the prime factors p_s and q_s can be found which lead to the factorization of t RSA moduli N_s for $s = 1, \ldots, t$. □

Let

$$X_1 = \frac{N_1 - \left\lceil \left(\frac{a^{\frac{i+1}{i}} + b^{\frac{i+1}{i}}}{2(ab)^{\frac{i+1}{2i}}} + \frac{a^{\frac{1}{j}} + b^{\frac{1}{j}}}{2(ab)^{\frac{1}{2j}}} \right) \sqrt{N_1} \right\rceil + 1}{e_1}$$

$$X_2 = \frac{N_2 - \left\lceil \left(\frac{a^{\frac{i+1}{i}} + b^{\frac{i+1}{i}}}{2(ab)^{\frac{i+1}{2i}}} + \frac{a^{\frac{1}{j}} + b^{\frac{1}{j}}}{2(ab)^{\frac{1}{2j}}} \right) \sqrt{N_2} \right\rceil + 1}{e_2}$$

$$X_3 = \frac{N_3 - \left\lceil \left(\frac{a^{\frac{i+1}{i}} + b^{\frac{i+1}{i}}}{2(ab)^{\frac{i+1}{2i}}} + \frac{a^{\frac{1}{j}} + b^{\frac{1}{j}}}{2(ab)^{\frac{1}{2j}}} \right) \sqrt{N_3} \right\rceil + 1}{e_3}.$$

Consider the lattice $\mathcal{L}$ spanned by the matrix

$$M = \begin{bmatrix} 1 & -[C(X_1)] & -[C(X_2)] & -[C(X3)] \\ 0 & C & 0 & 0 \\ 0 & 0 & C & 0 \\ 0 & 0 & 0 & C \end{bmatrix}$$

Also input $a = 3,\ b = 2,\ j = 4,\ i = 3$ and $t = 3$ as small positive integers. The above matrix M will be used for computing required reduced basis which leads to successful factoring of moduli N_s for $s = 1, \ldots, t$.

Example 3.2. *In what follows, we give an illustration of how Theorem 3.3 works on 3 RSA moduli and their corresponding public exponents*

$$\begin{aligned} N_1 &= 330887927826729358131406751905555113358427 \\ N_2 &= 909455241479718015703976451522306293699987 \\ N_3 &= 896255999831476423504365353752613393410129 \\ e_1 &= 260093505791357595269019761161559922357089 \\ e_2 &= 830211428275988442317142948578507842037903 \\ e_3 &= 260639236216424239075202140155225066663301 \end{aligned}$$

Observe

$$\begin{aligned} N &= \max\{N_1, N_2, N_3\} = 909455241479718015703976451522306293699987 \\ e &= \min\{e_1, e_2, e_3\} = 260093505791357595269019761161559922357089 \end{aligned}$$

Table 2: Algorithm for factoring RSA moduli $N_s = p_s q_s$ for $e_s d_s - k\phi(N_s) = 1$ of Theorem 3.3

INPUT: The public key tuple $(N_s, e_s, \alpha, \sigma$ satisfying the above Theorem 3.3.

OUTPUT: The prime factors p_s and q_s.

1. Compute $\varepsilon = \left(\frac{a}{b}\right)^{\frac{i}{2j}} N^{3\sigma-\alpha-\beta}$ for $\beta < \alpha \leq \frac{1}{2}$ and $N = \max\{N_s\}$ for $s = 1, \ldots, t$, $t \geq 2$ and $a > b$. Also compute $e = \min\{e_s\} = N^{\alpha}$.
2. Compute $C = [3^{t+1} \cdot 2^{\frac{(t+1)(t-4)}{4}} \cdot \varepsilon^{-t-1}]$.
3. Consider the lattice $\mathcal{L}$ spanned by the matrix M as stated above.
4. Applying the LLL algorithm to $\mathcal{L}$, we obtain the reduced basis matrix K.
5. Compute $J = M^{-1}$.
6. Compute $Q = JK$ to produce d and k_s.
7. Compute $\phi(N_s) = \frac{e_s d_s - 1}{k}$.
8. Compute $N_s - \phi(N_s)+1$.
9. Solve the quadratic equation $x^2 - (N_s - \phi(N_s) + 1)x + N_s = 0$.
10. Then output the roots of the equation as p_s and q_s for $s = 1, \ldots, t$.

with $e = \min\{e_1, e_2, e_3\} = N^{\alpha}$ *with* $\alpha = 0.9870431932$. *Taking* $t = 3$, $\beta = 0.25$ *we have* $\sigma = \frac{t(\alpha+\beta)}{3t+1} = 0.3711129579$ *and* $\varepsilon = 0.000007508475067$.
Applying Theorem 2.3, we compute

$$C = [3^{t+1} \cdot 2^{\frac{(t+1)(t-4)}{4}} \cdot \varepsilon^{-t-1}] = 127423066200000000000000.$$

Consider the lattice $\mathcal{L}$ *spanned by the matrix*

$$M = \begin{bmatrix} 1 & -[C(X_1)] & -[C(X_2)] & -[C(X3)] \\ 0 & C & 0 & 0 \\ 0 & 0 & C & 0 \\ 0 & 0 & 0 & C \end{bmatrix}$$

Therefore, by applying the LLL algorithm to $\mathcal{L}$, we obtain reduced basis with following matrix

$$K = \begin{bmatrix} -175146409612035 & -823228839795 & 174148519192170 & -114206584622820 \\ -84039951771888287 & 80666065160018481 & -87963455766549006 & -5966375445846324 \\ 76917823720099937 & 113434318528267569 & 264927030686706 & -118170963300717876 \\ 21604480682726699 & 152229348988955163 & 151359706383740262 & 196696397901374148 \end{bmatrix}$$

Next we compute $Q = JK$

$$Q = \begin{bmatrix} -175146409612035 & -222819221750609 & -191864162336087 & -602273175529801 \\ -84039951771888287 & -106914647529743848 & -92061578568439781 & -288986846702386117 \\ 76917823720099937 & 97853959199204323 & 84259642258505725 & 264496098146466542 \\ 21604480682726699 & 27484968619764657 & 23666631808664282 & 74290984412871231 \end{bmatrix}$$

From first row of Q we obtain $k,\ d_1,\ d_2$ and d_3 as follows:

$k = 175146409612035,\ d_1 = 222819221750609,\ d_2 = 191864162336087,$
$d_3 = 602273175529801$

We now compute $\phi(N_s) = \frac{e_s d_s - 1}{k}$ for $s = 1, 2, 3$. That is:

$$\phi(N_1) = 330887927826729358130254895146939245547920$$
$$\phi(N_2) = 909455241479718015702034073311041714951816$$
$$\phi(N_3) = 896255999831476423502471935613753586474660$$

Also, we proceed to compute $N_s - \phi(N_s) + 1$ for $s = 1, 2, 3$.

$$N_1 - \phi(N_1) + 1 = 115185675861586781050\,8$$
$$N_2 - \phi(N_2) + 1 = 1942378211264578748172$$
$$N_3 - \phi(N_3) + 1 = 1893418138859806935470$$

Finally, solving quadratic equation $x^2 - (N_s - \phi(N_s) + 1)x + N_s = 0$ for $s = 1, 2, 3$ gives us p_1, p_2, p_3 and q_1, q_2, q_1 which lead to the factorization of 3 RSA moduli N_1, N_2, N_3. That is:

$$p_1 = 604310949056531947721, p_2 = 1154909102962814371933,$$
$$p_3 = 948145143716756720671,\ q_1 = 547545809559335862787,$$
$$q_2 = 787469108301764376239,\ q_3 = 945272995143050214799$$

From our result, one can observe that we get $\min\{d_1, d_2, d_3\} \approx N^{0.3404}$ which is larger than the Blömer-May's bound of $x < \frac{1}{3}N^{0.25}$, Blömer and May (2004). This shows that the Blömer-May's attack can not yield the factorization of t RSA moduli in our case. Our $\min\{d_1, d_2, d_3\} \approx N^{0.3404}$ is also greater than the $\min\{x_1, x_2, x_3\} \approx N^{0.337}$ of Nitaj et al. (2014).

3.1.3 The Attack on t RSA Moduli $N_s = p_s q_s$ Satisfying $e_s d - k_s \phi(N_s) = z_s$

In this section, we consider another case in which t RSA moduli satisfies t equations of the form $e_s d_s - k\phi(N_s) = z_s$ for unknown parameters $d,\ k_s$ and z_s

for $s = 1, \ldots, t$.
Taking $s \geq 2$, let $N_s = p_s q_s$, $s = 1, \ldots, t$. The attack works for t instances (N_s, e_s) when there exists an integer d and t integers k_s satisfying equation $e_s d - k_s \phi(N_s) = z_s$. We show that t prime factors p_s and q_s of t RSA moduli N_s can be found efficiently for $N = \max\{N_s\}$ and $d < N^{\sigma}$, $k_s < N^{\sigma}$, $z_s < N^{\sigma}$, for all $\sigma = \frac{t(1+\beta)}{3t+1}$.

Theorem 3.4. *Let $N_s = p_s q_s$ be t RSA moduli for $s = 1 \ldots, t$, $i = 3, \ldots, j$ and $t \geq 2$. Let (e_s, N_s) be public key pair and (d, N_s) be private key pair with $e_s < \phi(N_s)$ and the relation $e_s d \equiv 1 \pmod{\phi(N_s)}$ is satisfied. Let $N = \max\{N_s\}$. If there exists positive integers $d < N^{\sigma}$, $k_s < N^{\sigma}$, $z_s < N^{\sigma}$, for all $\sigma = \frac{t(1+\beta)}{3t+1}$ such that $e_s d - k_s \phi(N_s) = z_s$ holds, then prime factors p_s and q_s of t RSA moduli N_s can successfully be found in polynomial time.*

Proof. Given $t \geq 2$, $i = 3, \ldots, j$ and let $N_s = p_s q_s$, be t moduli. Also Suppose $N = \max\{N_s\}$ and $k_s < N^{\gamma}$. Then equation $e_s d - k_s \phi(N_s) = z_s$ can be rewritten as

$$e_s d - k_s(N_s - (p_s + q_s) + 1) = z_s$$
$$e_s d - k_s(N_s - (N_s - \phi(N_s) + 1)) = z_s.$$

Let $\Psi = \left\lceil \left(\frac{a^{\frac{i+1}{i}} + b^{\frac{i+1}{i}}}{2(ab)^{\frac{i+1}{2i}}} + \frac{a^{\frac{1}{j}} + b^{\frac{1}{j}}}{2(ab)^{\frac{1}{2j}}} \right) \sqrt{N_s} \right\rceil$, then we have

$$e_s d - k_s \left(N_s - \Psi + \Psi - (N_s - \phi(N_s) + 1) + 1\right) = z_s.$$

$$\left| \frac{e_s}{N_s - \Psi + 1} d - k_s \right| = \frac{|z_s - k_s \left(N_s - \phi(N_s) + 1 - \Psi\right)|}{N_s - \Psi + 1}. \tag{2}$$

Let $N = \max N_s$ and $k_s < N^{\gamma}$, $z_s < N^{\gamma}$ be positive integers and also suppose

$$\begin{aligned} |\Psi + \phi(N_s) - N_s - 1| &< N^{2\gamma - \beta} \\ N_s - \Psi + 1 &> \frac{a}{b^2} N. \end{aligned} \tag{3}$$

Then plugging into equation (2) yields

$$\begin{aligned}\frac{|z_s - k_s\left(N_s - \phi(N_s) + 1 - \Psi\right)|}{N_s - \Psi + 1} &< \frac{|z_s + k_s\left(\Psi - N_s + \phi(N_s) - 1\right)|}{N_s - \Psi + 1} \\ &< \frac{N^{\gamma} + N^{\gamma}(N^{2\gamma-\beta})}{\frac{a}{a^2}N} \\ &= \frac{b^2(N^{\gamma} + N^{3\gamma-\beta})}{aN}. \\ &< \left(\frac{a}{b}\right)^{\frac{j}{i}} N^{3\gamma-\beta-1} \\ \left|\frac{e_s}{N_s - \Psi + 1}d - k_s\right| &< \left(\frac{a}{b}\right)^{\frac{j}{i}} N^{3\gamma-\beta-1}.\end{aligned}$$

We now proceed to show the existence of an integer d and t integers k_s. Taking $\varepsilon = \left(\frac{a}{b}\right)^{\frac{j}{i}} N^{3\gamma-\beta-1}$, with $\gamma = \frac{t(1+\beta)}{3t+1}$. Then we have

$$N^{\gamma}\varepsilon^{t} = N^{\gamma}\left(\left(\frac{a}{b}\right)^{\frac{jt}{i}} N^{3\gamma-\beta-1}\right)^{t} = \left(\frac{a}{b}\right)^{\frac{j}{i}} N^{\gamma+3\gamma t-\beta t-t} = \left(\frac{a}{b}\right)^{\frac{jt}{i}}.$$

Since $\left(\frac{a}{b}\right)^{\frac{jt}{i}} < 2^{\frac{t(t-3)}{4}} \cdot 3^{t}$ for $t \geq 3$,then, we get $N^{\gamma}\varepsilon^{t} < 2^{\frac{t(t-3)}{4}} \cdot 3^{t}$. It follows that if $d < N^{\gamma}$ then $d < 2^{\frac{t(t-3)}{4}} \cdot 3^{t} \cdot \varepsilon^{-t}$ $s = 1, \ldots, t$ we have

$$\left|\frac{e_s}{N_s - \Psi + 1}d - k_s\right| < \varepsilon, \qquad d < 2^{\frac{t(t-3)}{4}} \cdot 3^{t} \cdot \varepsilon^{-t}. \tag{4}$$

This also satisfies the conditions of Theorem 2.3. We next proceed to reveal the integer d and t integers k_s for $s = 1, \ldots, t$. Next, from equation $e_s d - k_s\phi(N_s) = z_s$ we compute the following:

$$\phi(N_s) = \frac{e_s d - z_s}{k_s},\ p_s + q_s = N_s - \phi(N_s) + 1,\ \textit{and}\ x^2 - (N_s - \phi(N_s) + 1)x + N_s = 0.$$

Finally, by finding the roots of the quadratic equation, the prime factors p_s and q_s can be revealed which lead to the factorization of t RSA moduli N_s for $s = 1, \ldots, t$. □

Let

$$X_1 = \frac{e_1}{N_1 - \left\lceil \left(\frac{a^{\frac{i+1}{i}} + b^{\frac{i+1}{i}}}{2(ab)^{\frac{i+1}{2i}}} + \frac{a^{\frac{1}{j}} + b^{\frac{1}{j}}}{2(ab)^{\frac{1}{2j}}} \right) \sqrt{N_1} \right\rceil + 1}$$

$$X_2 = \frac{e_2}{N_2 - \left\lceil \left(\frac{a^{\frac{i+1}{i}} + b^{\frac{i+1}{i}}}{2(ab)^{\frac{i+1}{2i}}} + \frac{a^{\frac{1}{j}} + b^{\frac{1}{j}}}{2(ab)^{\frac{1}{2j}}} \right) \sqrt{N_2} \right\rceil + 1}$$

$$X_3 = \frac{e_3}{N_3 - \left\lceil \left(\frac{a^{\frac{i+1}{i}} + b^{\frac{i+1}{i}}}{2(ab)^{\frac{i+1}{2i}}} + \frac{a^{\frac{1}{j}} + b^{\frac{1}{j}}}{2(ab)^{\frac{1}{2j}}} \right) \sqrt{N_3} \right\rceil + 1}.$$

Consider the lattice $\mathcal{L}$ spanned by the matrix

$$M = \begin{bmatrix} 1 & -[C(X_1)] & -[C(X_2)] & -[C(X_3)] \\ 0 & C & 0 & 0 \\ 0 & 0 & C & 0 \\ 0 & 0 & 0 & C \end{bmatrix}$$

Also input $a = 3,\ b = 2,\ t = 3,\ i = 3$ and $j = 4$ as small positive integers. The above matrix M will be used for computing required reduced basis which leads to successful factoring of moduli N_s for $s = 1, \dots, t$.

Table 3: Algorithm for factoring RSA moduli $N_s = p_s q_s$ for $e_s d - k_s \phi(N_s) = z_s$ of Theorem 3.4

INPUT: The public key tuple (N_s, e_s, σ) satisfying Theorem 3.4.

OUTPUT: The prime factors p_s and q_s.

1. Compute $\varepsilon = \left(\frac{a}{b}\right)^{\frac{j}{i}} N^{3\sigma-\beta-1}$, where $N = \max\{N_s\}$ for $s = 1, \dots, t$, $t \geq 2$ and $a > b$.
2. Compute $C = [3^{t+1} \cdot 2^{\frac{(t+1)(t-4)}{4}} \cdot \varepsilon^{-t-1}]$.
3. Consider the lattice $\mathcal{L}$ spanned by the matrix M as stated above.
4. Applying the LLL algorithm to $\mathcal{L}$, we obtain the reduced basis matrix K.
5. Compute $J = M^{-1}$.
6. Compute $Q = JK$ to produce d and k_s.
7. Compute $\phi(N_s) = \frac{e_s d - z_s}{k_s}$.
8. Compute $N_s - \phi(N_s) + 1$.
9. Solve the quadratic equation $x^2 - (N_s - \phi(N_s) + 1)x + N_s = 0$.
10. Then output the roots of the equation as p_s and q_s for $s = 1, \dots, t$.

Example 3.3. *In what follows, we give an illustration of how Theorem 3.4 works on 3 RSA moduli and their corresponding public exponents: Let*

$$
\begin{aligned}
N_1 = {} & 37527028838815595255917926673341020013014971163375784863807 2\\
& 2273041568912045244659295163793565326525944300991931444130 53\\
& 0346848160866908955039488375413453331726530746504330399771 09\\
& 9859485224424383277444300277732009078494311763616050721625 98\\
& 3991232827201399331174635649076897585957206775300140052737 66\\
& 1334910240100265527841902543150106879212052886386192096561 03\\
& 0171743670986414636270642717745717534880103731653138370546 37\\
& 1868308374421776832377999187326326939384176002146138276428 09\\
& 7673248094536541669031520182903142314212438994669751397311 99\\
& 3558179472850508064821020259986634221461389256296540557395 96\\
& 7868252883230089\\
N_2 = {} & 4257840089267745419233875938262076642141139469439616809226 20\\
& 3946673541695192526050595813913325313453434881153953819503 28\\
& 2977282460750908859903441533555796983314565375303493701215 32\\
& 2950909532542949679595392947796419813401223472999054834813 10\\
& 4496684588268025763918381605311605447901653440424156299336 93\\
& 5216307028632117389235152565274025245577016639874659426056 60\\
& 1504419749727137316375411080571906384073150128758719722036 15\\
& 2746184307628707852003333956939016552280052367816436998439 78\\
& 8565472393429943478177205298246885453884662430203582920683 04\\
& 1450649381174527191842473767023385293276620178155990785991 08\\
& 3101909875503667
\end{aligned}
$$

N_3 = 40565882786130754871728524678066471472077897829524278600448541732968506028430835583520123764365979911830247650097055172240734178782055395263159113970779344075728444048481090921924291322306879973039541315265990377120590564560588215866344408359081784886244566432309003037674371180924550371383029698730102115500797986627083568576833618106432183182341230541128523337715053529885338516984934015900007176042744519346274032671028179705382040942218740107570597277230019377816042239520485935873586450472448223347763511006309073180469288531595989020980798968722283212203319294101275285310405146548961722338861137767994095226396

e_1 = 31593632293898605395344151939069609240628253192715144269834097893833846460621110821785930231580422788914185534274385081967473253629745328529558593294037245469657837473210729207272105483421698992318134992460879216376584499123639576955099928951228220949109217372996476279212872688475037567457240568101551086055521126222403999748195895103880210851844106707540648319056780851665243389942979689233956182384175533849656330574754271296823441972137960934751739772607492893952612578152314685317596174555227228226009731386247626723303069531689678900171129677473013698918872518768479492814932147412489863274843803123636801195

e_2 = 16282903099274440299694388751758944933561010276258482392478157846602991183825301269471069861103659989633037505921423882571968126199772133117160613801035470776578149576507637935593893585615002519153380131299894916919670339023788289281416536680558500242553055049776613298551332282815525009866756356721410523749264782461987741265126627492355630970829352060055821359742528910181807891168816877626949227506366691841846815798000767508036236132086960795835698837128036500432187907763544767064589303038617623323069889310205858933054002834305814461483309267613572921942016626590062404864053700392286741675343724087506296701366

$$
\begin{aligned}
e_3 \quad = \quad & 374533755671870516734222609878629757277492925305117434141619\\
& 048431905951544749617870567510409397156516937221760227207149\\
& 984287184026078276716270619111472566029919700204422364826748 4\\
& 984792787464149907985737355428217766562790113478199959147600\\
& 419022398347604333936947680116684621807606356895121005876932\\
& 446015594306063035154855849039407809183142326918996682127443\\
& 847103267978592727526480380870702442941305892609280488501587\\
& 963163562235185528467716165043295902500328463809470299736439\\
& 721319876835570785315643106962502149044187965580563421283123\\
& 173154801659289187264751506032471121352621581049648365894461\\
& 3670174221911309
\end{aligned}
$$

Observe $N = \max\{N_1, N_2, N_3\}$

$$
\begin{aligned}
N \quad = \quad & 425784008926774541923387593826207664214113946943961680922620\\
& 394667354169519252605059581391332531345343488115395381950328\\
& 297728246075090885990344153355579698331456537530349370121532\\
& 295090953254294967959539294779641981340122347299905483481310\\
& 449668458826802576391838160531160544790165344042415629933693\\
& 521630702863211738923515256527402524557701663987465942605660\\
& 150441974972713731637541108057190638407315012875871972203615\\
& 274618430762870785200333395693901655228005236781643699843978\\
& 856547239342994347817720529824688545388466243020358292068304\\
& 145064938117452719184247376702338529327662017815599078599108\\
& 3101909875503667
\end{aligned}
$$

Taking $t = 3$, $\beta = 0.2$, *then we have* $\sigma = \frac{t(1+\beta)}{3t+1} = 0.36$ *and*
$\varepsilon = \left(\frac{a}{b}\right)^{\frac{j}{i}} N^{3\sigma-\beta-1} = 2.287102475 \times 10^{-74}$. *Applying Theorem 2.3, for* $n = t = 3$ *we compute*

$$
C = [3^{t+1} \cdot 2^{\frac{(t+1)(t-4)}{4}} \cdot \varepsilon^{-t-1}]
$$

$$
\begin{aligned}
C \quad = \quad & 148017317000000000000000000000000000000000000000000000000000\\
& 000000000000000000000000000000000000000000000000000000000000\\
& 000000000000000000000000000000000000000000000000000000000000\\
& 000000000000000000000000000000000000000000000000000000000000\\
& 000000000000000000000000000000000000000000000000000000000
\end{aligned}
$$

Consider the lattice $\mathcal{L}$ *spanned by the matrix*

$$M = \begin{bmatrix} 1 & -[C(X_1)] & -[C(X_2)] & -[C(X_3)] \\ 0 & C & 0 & 0 \\ 0 & 0 & C & 0 \\ 0 & 0 & 0 & C \end{bmatrix}$$

Therefore, by applying the LLL algorithm to $\mathcal{L}$, we obtain reduced basis with following matrix

$$K = \begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ b_{11} & b_{12} & b_{13} & b_{14} \\ c_{11} & c_{12} & c_{13} & c_{14} \\ d_{11} & d_{12} & d_{13} & d_{14} \end{bmatrix}$$

where

$$\begin{aligned} a_{11} &= 13764109169144680060901580870681534619170310496083843503546 \\ &\quad 51346136536532065426353753447144420359794583065283628799813 \\ &\quad 51762199642971142694746397186704960941040360841201206616533 \\ &\quad 8088091698047207156772202365608501207998259 21 \\ a_{12} &= 90544431818271366650544993838206745402107549787860221393961 \\ &\quad 55886914921275774580715467460102780858221478486305452993305 \\ &\quad 15801905196977221355910545045736648835429108720656938385070 \\ &\quad 3706163508396607200747191584682994183207271 7 \\ a_{13} &= 12409071826642183984226409880744674434150298040976327871402 \\ &\quad 60423043250364219446724089697299805117837451977723236427059 \\ &\quad 97702475924918835477610663956941145673060616092165129427759 \\ &\quad 9715801639465957152771689225256122165790511 21 \\ a_{14} &= 59732348790424814599936340116480003460415709176580583901462 \\ &\quad 72518243422072713285452315038744773369330528302501440582322 \\ &\quad 86058454282076663844255737950410695538967576582591725597514 \\ &\quad 411483167200409786509511158858414312306312 4 \end{aligned}$$

$$
\begin{aligned}
b_{11} &= 2096872423248418693131478074337349342131772063716581091411 0\\
&\quad 27412328698477773042950621794776094516949522135460925298081\\
&\quad 02874469975981081109038258518435448770962495557354655536239\\
&\quad 565856389509558528737371211152950350120172842\\
b_{12} &= -5116229348259363951525639020430493827054702967373919091 17\\
&\quad 18881334787736675374150844859264902217170198452946596164554\\
&\quad 86916309855549625278842563956862349507810301451096370262633\\
&\quad 4310686254068068455427964938432867223509893756 6\\
b_{13} &= 22741758683451874283652846271436440028158711747699383670475\\
&\quad 35221492107466309221077786949524256980700095247232739455629\\
&\quad 84544211317357476046802209566307091781595710935107634367521\\
&\quad 694618887879506559295808014103945866423823242\\
b_{14} &= -1822083129276065168578690667462771977444609056782085868 64\\
&\quad 84032694725285582282850953842741240029631082473622499229983\\
&\quad 24108773733960920592322553078704727992530657738707909277959\\
&\quad 6098208485528505329635524347804875213493683497 52
\end{aligned}
$$

$$
\begin{aligned}
c_{11} &= 10190561812860238985232930483137397052006077279889821060374\\
&\quad 44617823788614923287006777432084215379933653255526620917454\\
&\quad 54546717697311606108901615936861675588885815246096274485 41\\
&\quad 327621781136401007270581830534080333662484582\\
c_{12} &= 21483687164200957468716905211736490301316107663114169773285\\
&\quad 87750118839105848548335895935608811951468663803974429048003\\
&\quad 61724737818147563565440865025446386261952908418682329878593\\
&\quad 7604482417697977351481295421690199776404058414\\
c_{13} &= -1634700076223096471572567225356065881995722363687341483 84\\
&\quad 95303311697313864567558293217767111858275112897040805899282\\
&\quad 03882599594335521526911929382449920195588322055901600263190\\
&\quad 9626757228308654135243050373624358133393069770 18\\
c_{14} &= -8119416089378864543845729463056385877408665028040197102 08\\
&\quad 51623435615808854626941263763776466618417849842298201930500\\
&\quad 30883535163966164315073162196587661840842031006921813573420\\
&\quad 876988647923758803794315510314099052406397891 92
\end{aligned}
$$

$$
\begin{aligned}
d_{11} &= -2204922496476637656518456942487891498824667288301029214700621584253280153653060453019928319756922220434280616955657442244013302742115535369358906003443609850353143881135545695018993880348493894726640724112517387848080358489\\
d_{12} &= 4960213629494718111287033475427898268482363682140251990114198896899746343738375350457884321006531048513868589474250305735513777256639565941785351335372875466452953777386033797914717843453687924154164192420103214175749451 47\\
d_{13} &= 21717149370209085094208259533302246359057175002517911924260792020798149264490171703628320210673216205688293762528087155514181741828800187389313321728799533166506140902693180634526254187892007176472555317902442351554523747 11\\
d_{14} &= 58923837435646816496506610388711379471240719311492431389753135460819219485097467446736466108102749230156091135949030993898249826176644055882395312952778251939660979470506089191487034338130340768550268728863791521032860308 4
\end{aligned}
$$

Next we compute $Q = JK$

$$
Q = \begin{bmatrix} e_{11} & e_{12} & e_{13} & e_{14} \\ f_{21} & f_{22} & f_{23} & f_{24} \\ g_{31} & g_{32} & g_{33} & g_{34} \\ h_{41} & h_{24} & h_{43} & h_{44} \end{bmatrix}
$$

where

$$
\begin{aligned}
e_{11} &= 137641091691446800609015808706815346191703104960838435035 46\\
&\ 5134613653653206542635375344714442035979458306528362879981 3\\
&\ 5176219964297114269474639718670496094104036084120120661653 3\\
&\ 808809169804720715677220236560850120799825921\\
e_{12} &= 1158786659638892931053866906384283760501278140588755079698 9\\
&\ 7753066174271351966930325326036587988230995253773480574985 5\\
&\ 9498107673504149389320778585539464038249280179128247602772 6\\
&\ 37920010417664257109466302145478671696693740\\
e_{13} &= 5263693589947885755810769451355048410570178852715156596163 4\\
&\ 9910197925657220739509237850422247143041636063337112133780 6\\
&\ 2015100211357337271480687091022043264481249202868616046972 9\\
&\ 63010936775458141913852745928074110596728068\\
e_{14} &= 1270802740267221245530765405406026989230868194235991554744 1\\
&\ 5253372513926014566968375221339033749062157494086129998836 9\\
&\ 1614393114860765430419282078483608839024681930734879716115 9\\
&\ 856425729061648261648042890595862176168936738
\end{aligned}
$$

$$
\begin{aligned}
f_{21} &= 2096872423248418693131478074337349342131772063716581091411 0\\
&\ 2741232869847777304295062179477609451694952213546092529808 1\\
&\ 0287446997598108110903825851843544877096249555735465553623 9\\
&\ 565856389509558528737371211152950350120172842\\
f_{22} &= 1765336035311276671604056378185377533496379662936974455176 1\\
&\ 7621832414171130428919108140396052824108170238498098790602 5\\
&\ 7766386995264634922346239029008867703825800742922158943950 7\\
&\ 13513610333690970685764085527740064716818008\\
f_{23} &= 8018894501311967991912829715960561216693205283742348749871 5\\
&\ 9184503716699833347724568670013992153481542431638564066180 3\\
&\ 1516005017244465621565385512815379924149582488842000267145 0\\
&\ 80007081339524633521949201753036471643301050\\
f_{24} &= 1935985241550105864532361687103700242532090930544857026361 5\\
&\ 8728397069225117189372818095447927712134680836978813575597 2\\
&\ 9732867422695329391782099235100690764910387148525026989447 5\\
&\ 302423966553119415015867124748654465601987139
\end{aligned}
$$

$$
\begin{aligned}
g_{31} &= 10190561812860238985232930483137397052006077279889821060374\\
&\quad 44617823788614923287006777432084215379933653255526620917454\\
&\quad 54546717697311606108901615936861675588888581524609627448541\\
&\quad 327621781136401007270581830534080333662484582\\
g_{32} &= 85793326236032643288429002735351776758842061322544084622305\\
&\quad 90254414116973405550866339834474119854609111520802751732684\\
&\quad 72190023299851600300329202957706151440374100459211646150498\\
&\quad 5139164412039876919548746114431465168627656\\
g_{33} &= 38970916485148312927226294089754917464310616507795093058515\\
&\quad 94824991200623365939636619441929113970025103712497418498704\\
&\quad 23340880575791486596723742729093916455220287649477307278012\\
&\quad 27483614500669723640765211813766133056267431\\
g_{34} &= 94086683834766734320044951580133722765379998324918157401495\\
&\quad 27457818812549450706886303953133286529574605764932015534978\\
&\quad 21496040785553274738982782735038003990066344949820768262395\\
&\quad 19201327652227368984959598805242908362174753
\end{aligned}
$$

$$
\begin{aligned}
h_{41} &= -220492249647663765651845694248789149882466728830102921470\\
&\quad 06215842532801536530604530199283197569222204342806169556574\\
&\quad 42244013302742115535369358906003443609850353143881135545695\\
&\quad 018993880348493894726640724112517387848080358489\\
h_{42} &= -185630231717610305510146773184653381708763646679052793881\\
&\quad 21352957917587684167925309837404873921477856601682870648703\\
&\quad 46345190977572508810792455253838773694645531713502442907039\\
&\quad 18644912015609978145835895070038786227547548885\\
h_{43} &= -843210139385808271167305136371322428922999519211220352650\\
&\quad 82624687685130234110110265317875594037118424792797497736414\\
&\quad 13900120168434355151597796516343278844729088938247065609543\\
&\quad 71550662798999847138487046066008034994157570619\\
h_{44} &= -203574493355567808167639049697066773410850056050899250784\\
&\quad 75597543303207716879388510130345847706800427899745333513841\\
&\quad 45498859376755868228086491996070719438870961482009775280763\\
&\quad 138243859278604016577961402508535522479482598359
\end{aligned}
$$

From first row of Q we obtain $d,\ k_1,\ k_2$ and k_3 as follows:

$$
\begin{aligned}
d &= 137641091691446800609015808706815346191703104960838435035465\,1\\
&\quad 346136536532065426353753447144420359794583065283628799813517\,6\\
&\quad 219964297114269474639718670496094104036084120120661653380880\,9\\
&\quad 16980472071567722023656085012079982592\,1\\
k_1 &= 115878665963889293105386690638428376050127814058875507969897\\
&\quad 753066174271351966930325326036587988230995253773480574985594\\
&\quad 981076735041493893207785855394640382492801791282476027726379\\
&\quad 2001041766425710946630214547867169669374\,0\\
k_2 &= 526369358994788575581076945135504841057017885271515659616349\\
&\quad 910197925657220739509237850422247143041636063337112133780620\\
&\quad 151002113573372714806870910220432644812492028686160469729630\\
&\quad 1093677545814191385274592807411059672806\,8\\
k_3 &= 127080274026722212455307654054060269892308681942359915547441\,5\\
&\quad 253372513926014566968375221339033749062157494086129998836916\\
&\quad 143931148607654304192820784836088390246819307348797161159856\\
&\quad 4257290616482616480428905958621761689367\,38
\end{aligned}
$$

We next compute $\phi(N_s) = \frac{e_s d - z_s}{k_s}$ for $s = 1, 2, 3$ where z_1, z_2, z_3 are :

$$
\begin{aligned}
z_1 &= 305275083049103130204432261599597271283929787990806869804242\\
&\quad 738943678699349447449517970019048175311322812618197269590308\\
&\quad 048135406770206408852804441649032819252518609182707587065745\\
&\quad 9365072154247354641706834115178085017288\,39\\
z_2 &= 180872351698788201821103431504798876851625557857784396929326\\
&\quad 302728400947153023238062338566181756927152509363417997023999\\
&\quad 274734787344845273288270990000261654426220646299049668139206\\
&\quad 1838638069336534283058849402559363201930\,48\\
z_3 &= 187976824174617411275658492727608034753152272175419260812887\\
&\quad 823819864021035965072399171413779616629629429327078502026383\\
&\quad 174803613079415952341627800975362562615214821149720393612897\\
&\quad 9021230252918686036689147428504826145756\,61
\end{aligned}
$$

$$
\begin{aligned}
\phi(N_1) \quad = \quad & 3752702883881559525591792667334102001301497116337578486638\\
& 0722273041568912045244659295163793565326525944300991931144\\
& 4130530346848160866908955039488375413453331726530746504433\\
& v03997710998594852244243832774443002777320090784943117636 1\\
& 6050721625983991232827201399331174635649076897585957206 77\\
& 5300140052737661334910073434592004617280589311900334818 70\\
& 6827495605415965273828730167785082445005140393942994464 25\\
& 9201697629641183924391453037840871616767601940056142584 94\\
& 4507814035304014787232149584252054635561681375045029782 71\\
& 3641812124244137350389761637111945078121470838515484127 74\\
& 47550821324601307983500545057123447202753414 60
\end{aligned}
$$

$$
\begin{aligned}
\phi(N_2) \quad = \quad & 4257840089267745419233875938262076642141139469439616809 22\\
& 6203946673541695192526050595813913325313453434881153953 81\\
& 9503282977282460750908859903441533555796983314565375303 49\\
& 3701215322950909532542949679595392947796419813401223472 99\\
& 9054834813104496684588268025763918381605311605447901653 44\\
& 0424156299336935216306877457564519779360184657532900122 20\\
& 3037259875620011703110364903609881412258986580056015083 70\\
& 4120251735272514854115800847279817010374815172669685376 56\\
& 4341278978046073159247843047336583071559510562225121329 82\\
& 0148730450029843515797010848925023543607816214358883280 56\\
& 39160434723229454082105998457587938838711328 56
\end{aligned}
$$

$$
\begin{aligned}
\phi(N_3) \quad = \quad & 4056588278613075487172852467806647147207789782952427860 04\\
& 4854173296850602843083558352012376436597991183024765009 70\\
& 5517224073417878205539526315911397077934407572844404848 10\\
& 9092192429132230687997303954131526599037712059056456058 82\\
& 1586634440835908178488624456643230900303767437118092455 03\\
& 7138302969873010211549941006344691199946767847745282396 42\\
& 2607982130350661161578492424836936417517430694710658749 24\\
& 2013559182511273241563640999769627941755158821357486504 11\\
& 5238107447916182615546662631223321553947626769358893921 27\\
& 4536438817290462505262221020779055166807743556873300537 42\\
& 99682631575425901273483904275157316362944702 56
\end{aligned}
$$

Also, we proceed to compute $N_s - \phi(N_s) + 1$ for $s = 1, 2, 3$.

$$
\begin{aligned}
N_1 - \phi(N_1) + 1 &= 16666567352322462195383820654439334605889058668 05\\
&\quad 9575634301350320133219126550232380272307062090203\\
&\quad 4023497186621980415270533550160064776059131183741\\
&\quad 9948763619668421234891959480889960399009799876564\\
&\quad 7515312042867240031475053240100755035644623439472\\
&\quad 9037226305536132241879139328929125498190502890255\\
&\quad 523532607888630\\
N_2 - \phi(N_2) + 1 &= 1511745528694557923806164923454548136026147838060\\
&\quad 4489839405484611725590411642450051589130036902987\\
&\quad 7023447207182036945337027811697477188161287253639\\
&\quad 9879387733897703638391919455181358103583839676149\\
&\quad 8017691706530515421240036006712367219252562583756\\
&\quad 6710977483590486459469249804297232747780186145324\\
&\quad 308026004370812\\
N_3 - \phi(N_3) + 1 &= 1387923180171569109155140653608218956261409237621\\
&\quad 9117219301292815159743418106270687934196836226089\\
&\quad 2752116130025539176970768576152466715189399573223\\
&\quad 6077638303336880413365019309561353234932971955654\\
&\quad 1745717935637087922963839065433668107730084170542\\
&\quad 0577663458628872697560267882972064768823843458598\\
&\quad 045163115052384
\end{aligned}
$$

Finally, solving quadratic equation $x^2 - (N_s - \phi(N_s) + 1)x + N_s = 0$ for $s = 1, 2, 3$ gives us p_1, p_2, p_3 and q_1, q_2, q_1 which lead to the factorization of 3 RSA moduli

N_1, N_2, N_3. That is:

$$
\begin{aligned}
p_1 \quad = \quad & 1398276046508245355021068800067597877059240554624910849848824 \\
& 4118902091550501203982563020295350942490801485172074998144458 \\
& 0994271881536035961017180352611218776729314349077042736900514 \\
& 4257657254957479317330859698227233874889969090224669571668382 \\
& 2563454862278195530112545424932607306782392870130587352706881 \\
& 183878759 \\
p_2 \quad = \quad & 1137395538182894929346824436519918772915025520783537169152686 \\
& 6295421113498707278873078360864316929425807323410492979473774 \\
& 4856296323248104035572604353014099052267878567122995476190043 \\
& 3979364258174257078681927636279756270905369389364512931333002 \\
& 2764180763059403512810235868056177273759127043064481078968644 \\
& 419447669 \\
p_3 \quad = \quad & 9695044373039312336431871781964612707096358329084059299747166 \\
& 6740538523458732464136088131895767035471787426330620469710621 \\
& 1445280523666574490761565029456177766174521443711212665756982 \\
& 2919612952978406442704786652506660255464512346519892619005124 \\
& 4678547961541158747673729270182232103354097268424892972803618 \\
& 81770807 \\
q_1 \quad = \quad & 2683806887240008645173132653763355835296653121810467135813109 \\
& 9131112303621538192554642104108580778494334866941448060081243 \\
& 3412297191117246302946570673375448429391068858149167439894461 \\
& 1413525449190854342003445884967692726153549198508339927939613 \\
& 3838355099848598312098733664606819844725890348983152025284442 \\
& 24009871 \\
q_2 \quad = \quad & 3743499905116629944593404869342936311112231727691181478786216 \\
& 6575144554245696613208055213937336934442714866132738997959542 \\
& 2182065152377757729993204686528868162982507126892397899131412 \\
& 2421958150189272308724301677178585309823128187220899392325561 \\
& 1148634671543239205435882444186569856835075879697216411161584 \\
& 4923143
\end{aligned}
$$

$$
\begin{aligned}
q_3 \quad = \quad & 418418742867637875511953475411757685551773404713505791955412 \\
& 607462121995937380655184606494045905380342418667193344798645 \\
& 541233472300494444919575733132020526719428268993898042985654 \\
& 942971676657813530301314898458126270837455308714821511107904 \\
& 586350980480470413959602675660606510312278511592096683171269 \\
& 33281577.
\end{aligned}
$$

From our result, one can observe that we get $d \approx N^{0.3592}$ which is larger than the Blömer-May's bound of $x < \frac{1}{3}N^{0.25}$, Blömer and May (2004). This shows that the Blömer-May's attack can not yield the factorization of t RSA moduli in our case. Also our bound $d \approx N^{0.3599}$ is greater than $x = N^{0.344}$ of Nitaj et al. (2014).

3.1.4 The Attack on t RSA Moduli $N_s = p_s q_s$ Satisfying $e_s d_s - k\phi(N_s) = z_s$

In this section, we present another case in which t RSA moduli satisfying equations of the form $e_s d_s - k\phi(N_s) = z_s$ for unknown parameters d_s, k and z_s for $s = 1, \ldots, t$ can be simultaneously factored in polynomial time.

Theorem 3.5. *Let $N_s = p_s q_s$ be t RSA moduli for $s = 1, \cdots, t$, $i = 3, \ldots, j$ and $t \geq 2$. Let (e_s, N_s) be public key pair and (d_s, N_s) be private key pair with condition $e_s < \phi(N_s)$ such that the relation $e_s d \equiv z_s \pmod{\phi(N_s)}$ is satisfied. Also, let $e = \min\{e_s\} = N^{\alpha}$ be t public exponents. If there exists positive integers $d_s < N^{\gamma}$, $k < N^{\gamma}, z_s < N^{\gamma}$, for all $\gamma = \frac{t(\alpha+\beta)}{3t+1}$ such that equation $e_s d_s - k\phi(N_s) = z_s$ holds, then prime factors p_s and q_s of t RSA moduli N_s can be successfully recovered in polynomial time for $s = 1, \ldots, t$.*

Proof. Given $t \geq 2$, for $i = 3, \ldots, j$ and suppose $N_s = p_s q_s$, $1 \leq s \leq t$ be t RSA moduli. Setting $e = \min\{e_s\} = N^{\alpha}$ be t public exponents for $s = 1, \ldots, t$ and suppose that $d_s < N^{\gamma}$. Then equation $e_s d_s - k\phi(N_s) = z_s$ can be rewritten as

$$
\begin{aligned}
e_s d_s - k(N_s - (p_s + q_s) + 1) &= z_s \\
e_s d_s - k(N_s - (N_s - \phi(N_s) + 1)) &= z_s.
\end{aligned}
$$

Suppose $\Upsilon = \left\lceil \left(\frac{a^{\frac{i+1}{i}} + b^{\frac{i+1}{i}}}{2(ab)^{\frac{i+1}{2i}}} + \frac{a^{\frac{1}{j}} + b^{\frac{1}{j}}}{2(ab)^{\frac{1}{2j}}} \right) \sqrt{N_s} \right\rceil$, then we have

$$
e_s d_s - k\left(N_s - \Upsilon + \Upsilon - (N_s - \phi(N_s) + 1) + 1\right) = z_s.
$$

$$
\left| k\frac{(N_s - \Upsilon + 1)}{e_s} - d_s \right| = \frac{|z_s - k\left(N_s - \phi(N_s) + 1 - \Upsilon\right)|}{e_s}. \tag{5}
$$

Suppose $N = \max\{N_s\}$, $d_s < N^\gamma$, $k < N^\gamma$, $z_s < N^\gamma$ are positive integers and

$$|\Upsilon + \phi(N_s) - N_s - 1| \quad < \quad N^{2\gamma-\beta}$$

and taking $e = \min\{e_s\} = N^\alpha$. Plugging the above conditions into inequality (5), then we have:

$$\begin{aligned}\frac{|z_s - k\left(N_s - \phi(N_s) + 1 - \Upsilon\right)|}{e_s} &\leq \frac{|z_s + k\left(\Upsilon + \phi(N_s) - N_s - 1\right)|}{e_s} \\ &< \frac{N^\gamma + N^\gamma(N^{2\gamma-\beta})}{N^\alpha} \\ &= \frac{N^\gamma + N^{3\gamma-\beta}}{N^\alpha} \\ &< \left(\frac{a}{b}\right)^{\frac{j}{2i}} N^{3\gamma-\alpha-\beta}.\end{aligned}$$

Hence we get:

$$\left|k\frac{(N_s - \Upsilon + 1)}{e_s} - d_s\right| < \left(\frac{a}{b}\right)^{\frac{j}{2i}} N^{3\gamma-\alpha-\beta}.$$

We now proceed to show the existence of integer k and the t integers d_s. Let $\varepsilon = \left(\frac{a}{b}\right)^{\frac{j}{2i}} N^{3\gamma-\alpha-\beta}$ and $\gamma = \frac{t(\alpha+\beta)}{3t+1}$. Then we get

$$N^\gamma \varepsilon^t = N^\gamma \left(\left(\frac{a}{b}\right)^{\frac{j}{2i}} N^{3\gamma-\alpha-\beta}\right)^t = \left(\frac{a}{b}\right)^{\frac{jt}{2i}} tN^{3\gamma t - t\alpha - \beta t} = \left(\frac{a}{b}\right)^{\frac{jt}{2i}}.$$

Since $\left(\frac{a}{b}\right)^{\frac{jt}{2i}} < 2^{\frac{t(t-3)}{4}} \cdot 3^t$ for $t \geq 2$, then, it implies that $N^\gamma \varepsilon^t < 2^{\frac{t(t-3)}{4}} \cdot 3^t$. It follows that if $k < N^\gamma$ then $k < 2^{\frac{t(t-3)}{4}} \cdot 3^t \cdot \varepsilon^{-t}$ for $s = 1, \ldots, t$, we have

$$\left|k\frac{(N_s - \Upsilon + 1)}{e_s} - d_s\right| < \varepsilon, \qquad k < 2^{\frac{t(t-3)}{4}} \cdot 3^t \cdot \varepsilon^{-t}.$$

This fulfilled the conditions of Theorem 2.3. We next proceed to reveal the private key d_s and k for $s = 1, \ldots, t$. Next, from equation $e_s d_s - k\phi(N_s) = z_s$ we compute the following:

$$\phi(N_s) = \frac{e_s d_s - z_s}{k},\ p_s + q_s = N_s - \phi(N-s) + 1,\ and\ x^2 - (N_s - \phi(N_s) + 1)x + N_s = 0.$$

Finally, by finding the roots of the quadratic equation, the prime factors p_s and q_s can be found which lead to the factorization of t RSA moduli N_s for $s = 1, \ldots, t$ in polynomial time. □

Let

$$X_1 = \frac{N_1 - \left\lceil \left(\frac{a^{\frac{i+1}{i}} + b^{\frac{i+1}{i}}}{2(ab)^{\frac{i+1}{2i}}} + \frac{a^{\frac{1}{j}} + b^{\frac{1}{j}}}{2(ab)^{\frac{1}{2j}}} \right) \sqrt{N_1} \right\rceil + 1}{e_1}$$

$$X_2 = \frac{N_2 - \left\lceil \left(\frac{a^{\frac{i+1}{i}} + b^{\frac{i+1}{i}}}{2(ab)^{\frac{i+1}{2i}}} + \frac{a^{\frac{1}{j}} + b^{\frac{1}{j}}}{2(ab)^{\frac{1}{2j}}} \right) \sqrt{N_2} \right\rceil + 1}{e_2}$$

$$X_3 = \frac{N_3 - \left\lceil \left(\frac{a^{\frac{i+1}{i}} + b^{\frac{i+1}{i}}}{2(ab)^{\frac{i+1}{2i}}} + \frac{a^{\frac{1}{j}} + b^{\frac{1}{j}}}{2(ab)^{\frac{1}{2j}}} \right) \sqrt{N_3} \right\rceil + 1}{e_3}.$$

Consider the lattice $\mathcal{L}$ spanned by the matrix

$$M = \begin{bmatrix} 1 & -[C(X_1)] & -[C(X_2)] & -[C(X_3)] \\ 0 & C & 0 & 0 \\ 0 & 0 & C & 0 \\ 0 & 0 & 0 & C \end{bmatrix}$$

Also input $a = 3,\ b = 2,\ t = 3,\ i = 3$ and $j = 4$ as small positive integers. The above M matrix will be used for computing required reduced basis which leads to successful factoring of moduli N_s for $s = 1, \ldots, t$.

Table 4: Algorithm for factoring RSA moduli $N_s = p_s q_s$ for $e_s d_s - k\phi(N_s) = z_s$ of Theorem 3.5

INPUT: The public key tuple $(N_s, e_s, \alpha, \sigma$ satisfying the above Theorem 3.5.

OUTPUT: The prime factors p_s and q_s.

1. Compute $\varepsilon = \left(\frac{a}{b}\right)^{\frac{j}{2i}} N^{3\sigma-\alpha-\beta}$, where $N = \max\{N_s\}$ for $s = 1, \ldots, t$, $t \geq 2$, $\beta < \sigma \leq \frac{1}{2}$ and $a > b$. Also compute $e_s = \min\{e_1, \ldots, e_t\} = N^{\alpha}$.
2. Compute $C = [3^{t+1} \cdot 2^{\frac{(t+1)(t-4)}{4}} \cdot \varepsilon^{-t-1}]$.
3. Consider the lattice $\mathcal{L}$ spanned by the matrix M as stated above.
4. Applying the LLL algorithm to $\mathcal{L}$, we obtain the reduced basis matrix K.
5. Compute $J = M^{-1}$.
6. Compute $Q = JK$ to produce d and k_s.
7. Compute $\phi(N_s) = \frac{e_s d_s - z_s}{k}$.
8. Compute $N_s - \phi(N_s)+1$.
9. Solve the quadratic equation $x^2 - (N_s - \phi(N_s) + 1)x + N_s = 0$.
10. Then output prime factors p_s and q_s for $s = 1, \ldots, t$.

Example 3.4. *In what follows, we give an illustration of how Theorem 3.5 works on 3 RSA moduli and their corresponding public exponents:*

$$
\begin{aligned}
N_1 &= 3295148183979075111945350675197442 87 \\
N_2 &= 853577457696022637279536861717261139 \\
N_3 &= 689835688169708146675664504365049467 \\
e_1 &= 167369348344774632991700349806069653 \\
e_2 &= 737687793704945765120221919495997383 \\
e_3 &= 156091109112298242178765923428663298
\end{aligned}
$$

Observe

$$
\begin{aligned}
N &= \max\{N_1, N_2, N_3\} = 853577457696022637279536861717261139 \\
e &= \min\{e_1, e_2, e_3\} = 156091109112298242178765923428663298
\end{aligned}
$$

with $e = \min\{e_1, e_2, e_3\} = N^{\alpha}$ *for* $\alpha = 0.9794645353$. *Since* $t = 3$, *we have* $\gamma = \frac{t(\alpha+\beta)}{3t+1} = 0.3688393605$ *and* $\varepsilon = 0.00005009279807$.
Applying Theorem 2.3, we compute

$$C = [3^{t+1} \cdot 2^{\frac{(t+1)(t-4)}{4}} \cdot \varepsilon^{-t-1}] = 0.00005009279807.$$

Consider the lattice $\mathcal{L}$ *spanned by the matrix*

$$M = \begin{bmatrix} 1 & -[C(X_1)] & -[C(X_2)] & -[C(X_3)] \\ 0 & C & 0 & 0 \\ 0 & 0 & C & 0 \\ 0 & 0 & 0 & C \end{bmatrix}$$

Therefore, by applying the LLL algorithm to $\mathcal{L}$, we obtain reduced basis with following matrix

$$K = \begin{bmatrix} -1424579461243 & -60125738090 & 266732672439 & 2957665316792 \\ 258395480634514 & 21185514433820 & -129818740616122 & 137993452225584 \\ 196899106295135 & 291427529910050 & 274154359898645 & 74704790779560 \\ -162814655725785 & 366161498530450 & -421680171226195 & -33871422775960 \end{bmatrix}$$

Next we compute $Q = JK$

$$Q = \begin{bmatrix} -1424579461243 & -2804695406341 & -1648378792750 & -6295847076671 \\ 258395480634514 & 508726004601070 & 298989029400110 & 1141963979993325 \\ 196899106295135 & 387652660987237 & 227831665385049 & 870184287007563 \\ -162814655725785 & -320547592761628 & -188392597920164 & -719550016112108 \end{bmatrix}$$

From the first row of Q we obtain $k,\ d_1,\ d_2$, and d_3 as follows:

$$k = 1424579461243, d_1 = 2804695406341,$$
$$d_2 = 1648378792750,\ d_3 = 6295847076671$$

We now compute $\phi(N_s) = \frac{e_s d_s - z_s}{k}$ for $s = 1, 2, 3$ where z_1, z_2, z_3 are :

$$z_1 = 579057474385,\ z_2 = 1556015073242,\ z_3 = 38593801470$$
$$\phi(N_1) = 329514818397907510033962670013247816$$
$$\phi(N_2) = 853577457696022635407743651209932856$$
$$\phi(N_3) = 689835688169708144943019327714137216$$

Also, we proceed to compute $N_s - \phi(N_s) + 1$ for $s = 1, 2, 3$.

$$N_1 - \phi(N_1) + 1 = 1160572397506496472$$
$$N_2 - \phi(N_2) + 1 = 1871793210507328284$$
$$N_3 - \phi(N_3) + 1 = 1732645176650912252$$

Finally, solving quadratic equation $x^2 - (N_i - \phi(N_i) + 1)x + N_i = 0$ for $i = 1, 2, 3$ gives us p_1, p_2, p_3 and q_1, q_2, q_1 which lead to the factorization of 3 RSA moduli N_1, N_2, N_3. That is:

$$p_1 = 665240622214224083,\ p_2 = 1085312126633841397,$$
$$p_3 = 1112653948231598779,\ q_1 = 495331775292272389,$$
$$q_2 = 786481083873486887,\ q_3 = 619991228419313473$$

From our result, one can observe that we get $\min\{d_1, d_2, d_3\} \approx N^{0.3400}$ which is larger than the Blöomer-May's, bound of $x < \frac{1}{3}N^{0.25}$, Blömer and May (2004) . This shows that the Blöomer-May's attack can not yield the factorization of t RSA moduli in our case. Also our $\min\{d_1, d_2, d_3\} \approx N^{0.340}$ is greater than $\min\{x_1, x_2, x_3\} \approx N^{0.337}$ of Nitaj et al. (2014) .

4. Conclusion

The paper reported some improvement of bounds over some former attacks on t instances of factoring RSA moduli $N_s = p_s q_s$. It has been shown that t instances of RSA moduli $N_s = p_s q_s$ satisfying equations of the form $e_s d - k_s \phi(N_s) = 1$, $e_s d_s - k\phi(N_s) = 1$, $e_s d - k_s \phi(N_s) = z_1$ and $e_s d_s - k\phi(N_s) = z_1$ for $s = 1, \ldots, t$ using $N - \left\lceil \left(\frac{a^{\frac{i+1}{i}} + b^{\frac{i+1}{i}}}{2(ab)^{\frac{i+1}{2i}}} + \frac{a^{\frac{1}{j}} + b^{\frac{1}{j}}}{2(ab)^{\frac{1}{2j}}} \right) \sqrt{N} \right\rceil + 1$ as a good approximations of $\phi(N_s)$ for unknown positive integers d, d_s, k, k_s and z_s can be simultaneously factored in polynomial time using simultaneous Diophantine approximations and lattice basis reductions methods.

Acknowledgements

The present research was partially supported by the Universiti Putra Malaysia Grant with Project Number GP-IPS/2018/9657300.

References

Abubakar, S. I., Ariffin, M. R. K., and Asbullah, M. A. (2018). A New Improved Bound for Short Decryption Exponent on RSA Modulus $N = pq$ Using Wiener's Method. In *3rd International Conference on Mathematical Sciences and Statistics (ICMSS'2018)*, page 122.

Asbullah, M. A. and Ariffin, M. R. K. (2016a). Analysis on the AA_β Cryptosystem. In *The 5th International Cryptology and Information Security Conference 2016 (Cryptology2016)*, pages 41–48.

Asbullah, M. A. and Ariffin, M. R. K. (2016b). Analysis on the Rabin-p Cryptosystem. In *The 4th International Conference on Fundamental and Applied Sciences (ICFAS2016)*, pages 080012–1–080012–8. AIP Conf. Proc. 1787.

Blömer, J. and May, A. (2004). A generalized Wiener Attack on RSA. In *International Workshop on Public Key Cryptography*, pages 1–13. Springer.

Dubey, M. K., Ratan, R., Verma, N., and Saxena, P. K. (2014). Cryptanalytic Attacks and Countermeasures on RSA. In *Proceedings of the Third International Conference on Soft Computing for Problem Solving*, pages 805–819. Springer.

Hinek, J. (2007). *On the Security of Some Variants of RSA*. PhD thesis, University of Waterloo, Ontario, Canada.

Lenstra, A. K., Lenstra, H. W., and Lovász, L. (1982). Factoring Polynomials with Rational Coefficients. *Mathematische Annalen*, 261(4):515–534.

Nitaj, A. (2012). Diophantine and Lattice Cryptanalysis of RSA Cryptosystem. *Artificial Intelligence Evolutionary Computation and Metaheuristics (AIECM)*, 2(11):139–168.

Nitaj, A., Ariffin, M. R. K., Nassr, D. I., and Bahig, H. M. (2014). New Attacks on the RSA Cryptosystem. In *International Conference on Cryptology in Africa*, pages 178–198. Springer.

Rivest., R., Shamir, A., and Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-key Cryptosystems. *Communications of the ACM*, 21(2):120–126.

Wiener, M. (1990). Cryptanalysis of Short RSA Secret Exponents. *IEEE Trans. Inform. Theory*, 36(3):553–558.

Yan, S. Y. Y. (2008). *Cryptanalytic Attacks on RSA*. Springer, 1st edition.