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 $s = 1, \ldots, t$ 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. $\mu_{i,j} \leq \frac{1}{2}, \quad for \quad 1 \leq j < i \leq n$
2. $\frac{3}{4}||b_{i-1}^*||^2 \leq ||b_i^* + \mu_{i,i-1} b_{i-1}^*||^2 \quad for \quad 1 \leq i \leq n$. *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 $N_i = p_iq_i$ 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 $N_i = p_iq_i$ 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 $2a^j b^j p^i q^i$ to both sides we have

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

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 $N_s = p_s q_s$ using system of equations of the form $e_s d - k_s \phi(N_s) = 1$, $e_s d_s - k\phi(N_s) = 1$, $e_s d - k_s \phi(N_s) = z_1$ and $e_s d_s - k\phi(N_s) = z_1$ 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 $N_s = p_s q_s$ Satisfying $e_s d - k_s \phi(N_s) = 1$

Taking $t \geq 2$, let $N_s = p_s q_s$ 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 $e_s d - k_s \phi(N_s) = 1$. 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 $\Phi = \left\lceil \left(\frac{a^{\frac{i+1}{i}} + b^{\frac{i+1}{i}}}{2(ab)^{\frac{i+1}{2i}}} + \frac{a^{\frac{1}{j}} + b^{\frac{1}{j}}}{2(ab)^{\frac{1}{2j}}} \right) \sqrt{N_s} \right\rceil$

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

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

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

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

Plugging the conditions into equation (1) gives the following

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

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

$$N_1 = 687375900649987631880614399319735656459138826667176438182492638460515254125194773419478546413458283024490645550460226585322294757161953899804299046773862357772238793538346038690333584005355615949819852825099249580914306069158122568478713851337929710564477127708797127253694801109304970214835478918919468073789612616938850676492905311297579847974417979788804218898844938375945264466689615792890611317250548197417336207014476483409935739150275012174123174759104479606801539832740450773961121401792922649181803453511779231380635798523859192362277519804955061306507800411759709768988763372228548308239065587556264454521$$

$$N_2 = 687375900649987631880614399319735656459138826667176438182492678441812039182650727091466933853627713998371045083025306055477578563691758443580670089792237291021205227470484658605927963018371656460731429322909837475374883926606858977012070199787306079966110483102031780532736086138246148908484219302742355761728874810851036160417484819782253601577312336352969195141625327714663435444387919936129696178101361399104357888798088341263022404654324391135451985860842365787898190742583625686236756317215507456565837345696954465256492468812693981274769651153001286334451806875770579694109475342828781134506112848187247581145614959280884804413590764008636234174614423731411420609244755333 $$

$$N_3 = 897813955847236267587336750873148307051152091406046388815502613889280887780658445118276538481854471025811975606573403025378111410341951027371148973259338530549228638186507249798434636298087696988085764356396091084455535816503005564095872970772805542635084731122079323982271703210644901210483102370568913295830669060755842391713804406388292714270464770346737668464215535423397692812945733882942359587446059545721246191283477522822470825407291238021169736278506478827370662285411025867947193127513376185237230986463004307926102019124994508881206205365530894755436456835638424221396999832314821612128361245579681754537$$

$$e_1 = 265559677419194411236893573363486941739833554357572897124044785015965770091933028391248574069302464928535757251090881843499006927411709255255922739531924336011072672986262282732654731970958529882563372701258532435252116297763481690335892997359067265694084540926110853278170252423825546388895672108062431195530302853178637011285349145211416103389461701990856119478336268218056137450511455941140572865664449097795921196098904938461890577923057773758780016342966358794528584991048662202704144969178976900294459165402153720145113449807943118999248613601567357115512803670173225270460227169893190592408370525161914594430 9$$

$$e_2 = 213774545290842679153174281178347439765926007242311841852972313720647710356490884480131282963488325378040358253277211704891255984069379198925155608924379540042740361215100326292175421017300263876701667099105651856688450509831885546253932091553888685939199035055036923501474512751789220899355145860909847636238068913104272975193992317380535596708790612428893128610184313818250306356334484108452834036808442757765160822110081117778678530943885938987280316014979417427773917240403707161522219128194178458922078879557955267787939397480551344365322841503906148216339496515056120557139559998321019522788805850231063302452 5$$

$$e_3 = 3376302598271191870188405364071713065607100240181184699662570
2255086258436583211335843258793030936072336392983215856540479
9953125779525511439128291020834389613374068416205032628729198
1614581551642757897767829436911032605178624200673043346061001
2142248700441721659939208924087950529260916887929812535473932
1817090001202244567834249200232976426215389468855576323277726
1862370550936835074376899622865460438674567718027330038509377
5099874246378735790918793792747677982857557119205283807903203
9392650709827067367352258205096098914166051373859769018576614
8835065491259971934045455754080194274389976593356624639028151
554549$$

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

$$N = 8978139558472362675873367508731483070511520914060463888155026
1388928088778065844511827653848185447102581197560657340302537
8111410341951027371148973259338530549228638186507249798434636
2980876969880857643563960910844555358165030055640958729707728
0554263508473112207932398227170321064490121048310237056891329
5830669060755842391713804406388292714270464770346737668464215
5354233976928129457338829423595874460595457212461912834775228
2247082540729123802116973627850647882737066228541102586794719
3127513376185237230986463004307926102019124994508881206205365
5308947554364568356384242213969998323148216121283612455796817
545379$$

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*

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

$$C = 5453944245000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000$$

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

$A_{11} = 605917113211242937022782801258184510416400814899004201379754191408727322175163090856192589406007394278342215654244668398269578297613560979072176306252357569225734821095555675380913166832634661106754662488616099056785385 89$

$A_{12} = 680058398117171724157759973657881518011424075687422903388227959982832517933632597890708465849892478332336408775513053000991536327844175667981009967877404370215470311589181379531856784651198248642868582142075127795141735 4$

$A_{13} = 585634070131524256315334851694342293917379214540846031956924901398233755581251477344681277874995918511245943650961238701628196744465226306783146956887212216292158721596169098004285729698912298496206489699850615301577901 74$

$A_{14} = 352878626164755585222949742078542860467412843776628321713105418946722996499756948819535259332825578581257046729821228519730169754693217292921174539810256414344000362227371359620271077342924451105759962622852547199201579 42$

$$B_{11} = 648530514884260307325447344573387219286151647384781336335244467487847518376069981441277647563125262789894289394576736359971934513893737128853530585970252343214334105471630794307655801498923861020470398031560982125764725084$$

$$B_{12} = -706964726021772653311436567126196118104963720125027611623142753919163003988913616058869646288249140018195176064225621876297884281880479307934610664379526424379588484370237973976596667491995717955371053027179022480232508557 6$$

$$B_{13} = 253842401621009251805480353518984652615986671458245242945111165983136989649869121606386033540157186058709321322516236784154347198416054235945088027127474782507154467460985304793419508538349313094840307234531213644261825034 4$$

$$B_{14} = -202739261054718240146979782696457043418582226678569112733210165701691441158298856815552109128047545970308946154944406824140760200569958972511019780111318258490716569219910618092258043416410849061423549981977347299457955448$$

$$C_{11} = 205966496313945718811084753125335149912130430933172541634942097003243446548636997117045649596127985955679140310295326540944419641531614988135854465414838138903904372139099224221066803313001998661749438098644513041304027107$$

$$C_{12} = -363745519506876377046641732054859609768397352629789424442381382585510080773431337984372920318702425812910671848545362604384944977385812117798112837243350419395034873892860911336875860933383411082951535817749529021579965069 8$$

$$C_{13} = -520511937315522804705522427136071783967048750703656182952847516056112677905307993542443306734737812275812241045715429917461881608667493066987610438259035597237657474676641965874325492892230031047510423760919553382770568303 8$$

$$C_{14} = 688178364836427372428859448714159409282646876120209397939324195425060682132021094039730355975116426994104658982134516926144616723232320558962413385338539214277833024748195280107067873826268006990706231150822761014261743834 6$$

$$
\begin{aligned}
D_{11} &= -15670375536279242003650070460157850805583635125144181927002919988646065507701448977752602127271548995662657187839789724777165741419806069656319133286453863860652767025409928905038839527684351916756595398901544180525700058764\\
D_{12} &= -53094119671157515905032669329339882944938073812923326342622435204203162015943265202709969354972608883644658989836746287605412020994073479671386538727929738276222890847296624378709430741387140753764179312836287287584703549044\\
D_{13} &= 88459388925446969417168208446743205515878699490858993246848197120711468727671872654054424608916950333832228242478359703949724050621897240174902244826453391354731345629328051383585892902405394675207745758246532322588114307764\\
D_{14} &= 14790890704130541472981948756413109810917792203668397764961753120853606538362107927161171606633869483364680302364142156761466158645761475688841534967932040929992797487082026668739891393521529573149775001244116508461608168408
\end{aligned}
$$

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

$$
\begin{aligned}
E_{11} &= 60591711321124293702278280125818451041640081489900420137975419140872732217516309085619258940600739427834221565424466839826957829761356097907217630625235756922573482109555567538091316683263466110675466248861609905678538589\\
E_{12} &= 23408902316038750389994782010468410260059436995698834749355090835125224729071955974224764306374733528010091783138112213698303490239106604655439840642913356584989261582290643215102266582940788728772531288756359513996465200
\end{aligned}
$$

$$E_{13} = 16512833142606630115004811481072026078654429925799521433747249018235231959608367461997565766044787362960006819028938840749481645362275236454711363414916123399132980641344364885319392344899326752280314601162291124318656418$$

$$E_{14} = 22786007171625955393614063951034915441330944433889707086843572084555674293454637699411561131868311858469793346312375135687758849424296165424574078182329839280240449187007738398975684026195741550966450944037664572599581072$$

$$F_{21} = 64853051488426030732544734457338721928615164738478133633524446748784751837606998144127764756312526278989428939457673635997193451389373712885353058597025234321433410547163079430765580149892386102047039803156098212576472508 4$$

$$F_{22} = 25055221483079692810443430619178036517934913244012062073742552462088793578020442305253874106098906642501522380440599503454814275205113245169440677340713304107481927421688936411771548598263491747008537632269774860950091950 1$$

$$F_{23} = 17674160288057443442972097516602345932511413726549120639683249636737377294629657840551399770810570918016472588021703193933162037447414144211894248753329236420312160372552183832594671870246468871627153764098089888285571469$$

$$F_{24} = 24388518893043917726187725144126920644124202302155396592198642572338998259834688275776290399881742266560193990662739384212671346199137279441251250102011472772742376847058996863922043897499560987797306320164105151131171577 2$$

$$
\begin{aligned}
G_{31} &= 20596649631394571881108475312533514991213043093317254163494 2\\
&\ 0970032434465486369971170456495961279859556791403102953265 40\\
&\ 9444419641531614988135854465414838138903904372139099224221 06\\
&\ 680331300199866174943809864451304130402710 7\\
G_{32} &= 7957275817870805652201006189252212921241192386830697536101 96\\
&\ 5523334262012722231422394863672708298626738633149254813703 87\\
&\ 4452122031874914829432404590770844663296671696910402021686 49\\
&\ 733897624441655916026497045985732300044364\\
G_{33} &= 5613128120073009906471095280509323939324256304081559521029 88\\
&\ 0539093090087638610097137175850989803073322838250438482715 95\\
&\ 9132515243372489138037172796358442113608324427426860458025 09\\
&\ 589030974712159048920719414753593457054203\\
G_{34} &= 7745538060893236145652145035533792493353879609630295285694 87\\
&\ 8043540200184325862105651174386835947399799141074931843359 24\\
&\ 0966491120330692693480012731456469167325669057025560282942 35\\
&\ 258502914345680900346042621775790705717619
\end{aligned}
$$

$$H_{41} = -15670375536279242003650070460157850805583635125144181927002919988646065507701448977752602127271548995662657187839789724777165741419806069656319133286453863860652767025409928905038839527684351916756595398901544181525700058764$$

$$H_{42} = -60540671683672388762430342907234716196416120442511848282208469413640396633365118804075201765960353169379048521216342176852583602726130158038830269265711654848697525595858322998850700642466835137450075339773544873687733039195$$

$$H_{43} = -42705890107835728992314955511360125742464585805949516578016930152871398230484549596853828216974284173492383122690758673594266059677920962211470382142963483417899462855013563168873951780997928702635268657393201223995329707014$$

$$H_{44} = -58929725133418678156597989777892479105897810243976511681865403765688866770801891297591770243820574809372779496320861225375643983759341399496878016669466131261002159346157532105421248178841444763749460579204868347418956201933$$

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

$$d = 6059171132112429370227828012581845104164008148990042013797541914087273221751630908561925894060073942783422156542446683982695782976135609790721763062523575692257348210955556753809131668326346611067546624886160990567853858 9$$

$$k_1 = 2340890231603875038999478201046841026005943699569883474935509083512522472907195597422476430637473352801009178313811221369830349023910660465543984064291335658498926158229064321510226658294078872872531288756359513996465200$$

$$k_2 = 1651283314260663011500481148107202607865442992579952143374724901823523195960836746199756576604478736296000681902893884074948164536227523645471136341491612339913298064134436488531939234489932675228031460116229112431865641 8$$

$$k_3 = 2278600717162595539361406395103491544133094443388970708684357208455567429345463769941156113186831185846979334631237513568775884942429616542457407818232983928024044918700773839897568402619574155096645094403766457259958107 2$$

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) &= 687375900649987631880614399319735656459138826667176438182492\\
&\quad 638460515254125194773419478546413458283024490645550460226585\\
&\quad 322294757161953899804299046773862357772238793538346038690333\\
&\quad 358400535561594981985282509924958091430606915812256847871385\\
&\quad 133792971056447712770879712725369480110930497021483547891891\\
&\quad 946807360906095280083909717496446505531479472986033753897760\\
&\quad 367942687288162446822134767302902029299493785165241282825225\\
&\quad 623920362223822049345924474082392120601335215889420685144595\\
&\quad 811139251091531776514757224777370239239633300076336913146576\\
&\quad 473999369370158589950521059851901110403500812176893937099504\\
&\quad 8630070755267200\\
\phi(N_2) &= 784418120391826507270914669338536277139983710450830253060554\\
&\quad 775785636917584435806700897922372910212052274704846586059279\\
&\quad 630183716564607314293290983747537488392660685897701207019978\\
&\quad 730607996611048310203178053273608613824614890848421930274235\\
&\quad 576172887481085103616041748481978225360157731233635296919514\\
&\quad 162532751562028316287381173037950565587458832439953591139026\\
&\quad 725888203856656197264793082012577143329208120771702368982033\\
&\quad 383214897511242425889202320641960830128452923366191813805353\\
&\quad 442534742799770934799524311337770261069154984217409112166315\\
&\quad 947748907777012844876275123925721944130295749953302496334351\\
&\quad 0419369343056668\\
\phi(N_3) &= 897813955847236267587336750873148307051152091406046388815502\\
&\quad 613889280887780658445118276538481854471025811975606573403025\\
&\quad 378111410341951027371148973259338530549228638186507249798434\\
&\quad 636298087696988085764356396091084455535816503005564095872970\\
&\quad 772805542635084731122079323982271703210644901210483102370568\\
&\quad 913295810309804959337412093232358779040936236019252541559327\\
&\quad 275375936498645195769915756459950707462479935501936405367606\\
&\quad 940071196318547735104326128510755921219197493948748668265595\\
&\quad 331363085552946018482605313925873605856652404785009531194603\\
&\quad 667223820325515453692232867711762366885551219766212423600874\\
&\quad 2966722938884880
\end{aligned}$$

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

$$
\begin{aligned}
N_1 - \phi(N_1) + 1 &= 1805516641380115793179408462422650532445576422498266152194180654943207962453419427638703183223126965450045079547582372797876975186568157674332992535530911274479073329812944926625686104864751571575016095556798093868350476350351547277265975375261112534754070025898132406986649537552504596089372440169574855091873 22\\
N_2 - \phi(N_2) + 1 &= 1990431522815141082057501905222267730747048219774078210823809836739034597911827250728146509444975821020505685422347915266566091264867645605281500871452411200132193512600739425397678721309240971854444636802668002559844407040223289481253412356803444330471653372411841396350979061238844364790296307226915814188 66\\
N_3 - \phi(N_3) + 1 &= 2035925579650497962057204760925177803444551780517834118883959892475249704302997742299165212496612404378484082367653745162615227767218691189265898035728728133342191361714543053658410757456735770263191706058939845127369723411546331427753898154520537930174422396792666185451144861254860918852748694890738786605 00
\end{aligned}
$$

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:

$$
\begin{aligned}
p_1 &= 1259965102435793770365787096250705091499656072891974623803235680505910886068053084982261104442821842043199771365402522284048240417701749807875320634897269923408574287607304903360882937847577774519086929399661571154081003712302898731583665978748471306102040742875883699550917099296506944360583864467598560208 81
\end{aligned}
$$

$$p_2 = 144912796807558235227224448071847089726991649207347724182024$$
$$222904224424246307807314892132273304147585475369132446627841$$
$$072419525104684923701516949551889868917461979250212886412199$$
$$798432583631043448100999635346072672806149552170468670640315$$
$$413279511112706033529388400459627682480890373049785944192653$$
$$667580799$$

$$p_3 = 139003037188738962566074612642830443452225212660273650472251$$
$$568209599310351634537275215878176674386285311684308958328894$$
$$785970321757979050842136830517175022646286898260911409072158$$
$$014503113747448580372331966193565931585504803326953181330325$$
$$462356074101577929451389018253165508365397034276878394464475$$
$$925478761$$

$$q_1 = 545551538944322022813621366171945440945920349606291528390944$$
$$974437297076385366342656442078780305123406845308182179850513$$
$$828734768866407866457671900633641351070499042205640023264803$$
$$167017173800497008627398432297196395346639244378534391709282$$
$$364063447967985155256523287098620453208089145011856305107256$$
$$53166441$$

$$q_2 = 541303554739558729785257424503796833477131727700600969003567$$
$$607696790355448749177579225186711934345165751994097881636855$$
$$841896013820796368266331375933512510957573720098610561275680$$
$$736983404661419963626806314541833116345544701584794547009202$$
$$670649219344593037117957391754702236429940634292436865300379$$
$$13838067$$

$$q_3 = 645895207763108336396458634496873368922299653915097614161444$$
$$210379256600786652369547006430729868541525367239278070456214$$
$$755524549638900680844529730556977906879322379105428962936830$$
$$612425598295777387982739277909468053868363513061895940594899$$
$$896977189158643102278776002919489777600890576083964750245979$$
$$53181739$$

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:

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

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

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

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*

$$N_1 = 330887927826729358131406751905555113358427$$
$$N_2 = 909455241479718015703976451522306293699987$$
$$N_3 = 896255999831476423504365353752613393410129$$
$$e_1 = 260093505791357595269019761161559922357089$$
$$e_2 = 830211428275988442317142948578507842037903$$
$$e_3 = 260639236216424239075202140155225066663301$$

Observe

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

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

$$C = [3^{t+1} \cdot 2^{\frac{(t+1)(t-4)}{4}} \cdot \varepsilon^{-t-1}] = 12742306620000000000000.$$

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 $s = 1, 2, 3$.

$$N_1 - \phi(N_1) + 1 = 1151856758615867810508$$
$$N_2 - \phi(N_2) + 1 = 1942378211264578748172$$
$$N_3 - \phi(N_3) + 1 = 1893418138859806935470$$

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

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

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

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

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 $s = 1, \ldots, t$.

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 $s = 1, \ldots, t$, $t \geq 2$ 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 $s = 1, \ldots, t$.

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*

$N_1 = 375270288388155952559179266733410200130149711633757848638072$
$227304156891204524465929516379356532652594430099193144413053$
$034684816086690895503948837541345333172653074650433039977109$
$985948522442438327744430027773200907849431176361605072162598$
$399123282720139933117463564907689758595720677530014005273766$
$133491024010026552784190254315010687921205288638619209656103$
$017174367098641463627064271774571753488010373165313837054637$
$186830837442177683237799918732632693938417600214613827642809$
$767324809453654166903152018290314231421243899466975139731199$
$355817947285050806482102025998663422146138925629654055739596$
7868252883230089

$N_2 = 425784008926774541923387593826207664214113946943961680922620$
$394667354169519252605059581391332531345343488115395381950328$
$297728246075090885990344153355579698331456537530349370121532$
$295090953254294967959539294779641981340122347299905483481310$
$449668458826802576391838160531160544790165344042415629933693$
$521630702863211738923515256527402524557701663987465942605660$
$150441974972713731637541108057190638407315012875871972203615$
$274618430762870785200333395693901655228005236781643699843978$
$856547239342994347817720529824688545388466243020358292068304$
$145064938117452719184247376702338529327662017815599078599108$
3101909875503667

$$N_3 = 405658827861307548717285246780664714720778978295242786004485$$
$$417329685060284308355835201237643659799118302476500970551722$$
$$407341787820553952631591139707793440757284440484810909219242$$
$$913223068799730395413152659903771205905645605882158663444083$$
$$590817848862445664323090030376743711809245503713830296987301$$
$$021155007979866270835685768336181064321831823412305411285233$$
$$377150535298853385169849340159000071760427445193462740326710$$
$$281797053820409422187401075705972772300193778160422395204859$$
$$358735864504724482233477635110063090731804692885315959890209$$
$$807989687222832122033192941012752853104051465489617223388611$$
$$3776799409522639$$

$$e_1 = 315936322938986053953441519390696092406282531927151442698340$$
$$978938338464606211108217859302315804227889141855342743850819$$
$$674732536297453285295585932940372454696578374732107292072721$$
$$054834216989923181349924608792163765844991236395769550999289$$
$$512282209491092173729964762792128726884750375674572405681015$$
$$510860555211262224039997481958951038802108518441067075406483$$
$$190567808516652433899429796892339561823841755338496563305747$$
$$542712968234419721379609347517397726074928939526125781523146$$
$$853175961745552272282260097313862476262733030695316896789001$$
$$711296774730136989188725187684794928149321474124898632748438$$
$$031236368011959$$

$$e_2 = 162829030992744402996943887517589449335610102762584823924781$$
$$578466029911838253012694710698611036599896330375059214238825$$
$$719681261997721331171606138010354707765781495765076379355938$$
$$935856150025191533801312998949169196703390237882892814165366$$
$$805585002425530550497766132985513322828155250098667563567214$$
$$105237492647824619877412651266274923556309708293520600558213$$
$$597425289101818078911688168776269492275063666918418468157980$$
$$007675080362361320869607958356988371280365004321879077635447$$
$$670645893030386176233230698893102058589330540028343058144614$$
$$833092676135729219420166265900624048640537003922867416753437$$
$$2408750629670136$$

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

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

$$\begin{aligned}
a_{11} &= 13764109169144680060901580870681534619170310496083843503546 \\
&\quad 51346136536532065426353753447144420359794583065283628799813 \\
&\quad 51762199642971142694746397186704960941040360841201206616533 \\
&\quad 80880916980472071567722023656085012079982592 1 \\
a_{12} &= 90544431818271366650544993838206745402107549787860221393961 \\
&\quad 55886914921275774580715467460102780858221478486305452993305 \\
&\quad 15801905196977221355910545045736648835429108720656938385070 \\
&\quad 37061635083966072007471915846829941832072717 \\
a_{13} &= 12409071826642183984226409880744674434150298040976327871402 \\
&\quad 60423043250364219446724089697299805117837451977723236427059 \\
&\quad 97702475924918835477610663956941145673060616092165129427759 \\
&\quad 97158016394659571527716892252561221657905 1121 \\
a_{14} &= 59732348790424814599936340116480003460415709176580583901462 \\
&\quad 72518243422072713285452315038744773369330528302501440582322 \\
&\quad 86058454282076663844255737950410695538967576582591725597514 \\
&\quad 41148316720040978650951115885841431230631 24
\end{aligned}$$

$$b_{11} = 209687242324841869313147807433734934213177206371658109141102741232869847777304295062179477609451694952213546092529808102874469975981081109038258518435448770962495557354655536239565856389509558528737371211152950350120172842$$

$$b_{12} = -511622934825936395152563902043049382705470296737391909117188813347877366753741508448592649022171701984529465961645548691630985554962527884256395686234950781030145109637026263343106862540680684554279649384328672235098937566$$

$$b_{13} = 227417586834518742836528462714364400281587117476993836704753522149210746630922107778694952425698070009524723273945562984544211317357476046802209566307091781595710935107634367521694618887879506559295808014103945866423823242$$

$$b_{14} = -182208312927606516857869066746277197744460905678208586864840326947252855822828509538427412400296310824736224992299832410877373396092059232255307870472799253065773870790927795960982084855285053296355243478048752134936834975 2$$

$$c_{11} = 101905618128602389852329304831373970520060772798898210603744461782378861492328700677743208421537993365325552662091745454546717697311606108901615936861675588888581524609627448541327621781136401007270581830534080333662484582$$

$$c_{12} = 214836871642009574687169052117364903013161076631141697732858775011883910584854833589593560881195146866380397442904800361724737818147563565440865025446386261952908418682329878593760448241769797735148129542169019977640405841 4$$

$$c_{13} = -163470007622309647157256722535606588199572236368734148384953033116973138645675582932177671118582751128970408058992820388259959433552152691192938244992019558832205590160026319096267572283086541352430503736243581333930697701 8$$

$$c_{14} = -811941608937886454384572946305638587740866502804019710208516234356158088546269412637637764666184178498422982019305003088353516396616431507316219658766184084203100692181357342087698864792375880379431551031409905240639789192$$

$$
\begin{aligned}
d_{11} &= -220492249647663765651845694248789149882466728830102921470 \\
&\quad 062158425328015365306045301992831975692222043428061695565 74 \\
&\quad 422440133027421155353693589060034436098503531438811355456 95 \\
&\quad 01899388034849389472664072411251738784808035848 9 \\
d_{12} &= 496021362949471811128703347542789826848236368214025199011 41 \\
&\quad 988968997463437383753504578843210065310485138685894742503 05 \\
&\quad 735513777256639565941785351335372875466452953777386033797 91 \\
&\quad 47178434536879241541641924201032141757494514 7 \\
d_{13} &= 217171493702090850942082595333022463590571750025179119242 60 \\
&\quad 792020798149264490171703628320210673216205688293762528087 15 \\
&\quad 551418174182880018738931332172879953316650614090269318063 45 \\
&\quad 262541878920071764725553179024423515545237471 1 \\
d_{14} &= 589238374356468164965066103887113794712407193114924313897 53 \\
&\quad 135460819219485097467446736466108102749230156091135949030 99 \\
&\quad 389824982617664405588239531295277825193966097947050608919 14 \\
&\quad 870343381303407685502687288637915210328603084
\end{aligned}
$$

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

$$e_{11} = 137641091691446800609015808706815346191703104960838435035465134613653653206542635375344714442035979458306528362879981351762199642971142694746397186704960941040360841201206616533808809169804720715677220236560850120799825921$$

$$e_{12} = 115878665963889293105386690638428376050127814058875507969897753066174271351966930325326036587988230995253773480574985594981076735041493893207785855394640382492801791282476027726379200104176642571094663021454786716966937400$$

$$e_{13} = 526369358994788575581076945135504841057017885271515659616349910197925657220739509237850422247143041636063337112133780620151002113573372714806870910220432644812492028686160469729630109367754581419138527459280741105967280680$$

$$e_{14} = 127080274026722124553076540540602698923086819423599155474415253372513926014566968375221339033749062157494086129998836916143931148607654304192820784836088390246819307348797161159856425729061648261648042890595862176168936738$$

$$f_{21} = 209687242324841869313147807433734934213177206371658109141102741232869847777304295062179477609451694952213546092529808102874469975981081109038258518435448770962495557354655536239565856389509558528737371211152950350120172842$$

$$f_{22} = 176533603531127667160405637818537753349637966293697445517617621832414171130428919108140396052824108170238498098790602577663869952646349223462390290088677038258007429221589439507135136103336909706857640855277400647168180080$$

$$f_{23} = 801889450131196799191282971596056121669320528374234874987159184503716699833347724568670013992153481542431638564066180315160050172444656215653855128153799241495824888420002671450800070813395246335219492017530364716433010500$$

$$f_{24} = 193598524155010586453236168710370024253209093054485702636158728397069225117189372818095447927712134680836978813575597297328674226953293917820992351006907649103871485250269894475302423966553119415015867124748654465601987139$$

$$g_{31} = 10190561812860238985232930483137397052006077279889821060374$$
$$4461782378861492328700677743208421537993365325552662091745 4$$
$$5454671769731160610890161593686167558888858152460962744854 1$$
$$3276217811364010072705818305340803336624845 82$$

$$g_{32} = 85793326236032643288429002735351776758842061322544084622305$$
$$9025441411697340555086633983447411985460911152080275173268 4$$
$$7219002329985160030032920295770615144037410045921164615049 8$$
$$5139164412039876919548746114431465168627656$$

$$g_{33} = 38970916485148312927226294089754917464310616507795093058515$$
$$9482499120062336593963661944192911397002510371249741849870 4$$
$$2334088057579148659672374272909391645522028764947730727801 2$$
$$2748361450066972364076521181376613305626743 1$$

$$g_{34} = 94086683834766734320044951580133722765379998324918157401495$$
$$2745781881254945070688630395313328652957460576493201553497 8$$
$$2149604078555327473898278273503800399006634494982076826239 5$$
$$1920132765222736898495959880524290836217475 3$$

$$h_{41} = -22049224964766376565184569424878914988246672883010292147 0$$
$$0621584253280153653060453019928319756922220434280616955657 4$$
$$4224401330274211553536935890600344360985035314388113554569 5$$
$$0189938803484938947266407241125173878480803584 89$$

$$h_{42} = -18563023171761030551014677318465338170876364667905279388 1$$
$$2135295791758768416792530983740487392147785660168287064870 3$$
$$4634519097757250881079245525383877369464553171350244290703 9$$
$$1864491201560997814583589507003878622754754888 5$$

$$h_{43} = -84321013938580827116730513637132242892299951921122035265 0$$
$$8262468768513023411011026531787559403711842479279749773641 4$$
$$1390012016843435515159779651634327884472908893824706560954 3$$
$$7155066279899984713848704606600803499415757061 9$$

$$h_{44} = -20357449335556780816763904969706677341085005605089925078 4$$
$$7559754330320771687938851013034584770680042789974533351384 1$$
$$4549885937675586822808649199607071943887096148200977528076 3$$
$$1382438592786040165779614025085355224794825983 59$$

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

$$\begin{aligned}
d &= 137641091691446800609015808706815346191703104960838435035465134613653653206542635375344714442035979458306528362879981351762199642971142694746397186704960941040360841201206616533808809169804720715677220236560850120799825921\\
k_1 &= 115878665963889293105386690638428376050127814058875507969897753066174271351966930325326036587988230995253773480574985594981076735041493893207785855394640382492801791282476027726379200104176642571094663021454786716966937 40\\
k_2 &= 526369358994788575581076945135504841057017885271515659616349910197925657220739509237850422247143041636063337112133780620151002113573372714806870910220432644812492028686160469729630109367754581419138527459280741105967280 68\\
k_3 &= 127080274026722124553076540540602698923086819423599155474415253372513926014566968375221339033749062157494086129998836916143931148607654304192820784836088390246819307348797161159856425729061648261648042890595862176168936738
\end{aligned}$$

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 :

$$\begin{aligned}
z_1 &= 305275083049103130204432261599597271283929787990806869804242738943678699349447449517970019048175311322812618197269590308048135406770206408852804441649032819252518609182707587065745936507215424735464170683411517808501728839\\
z_2 &= 180872351698788201821103431504798876851625557857784396929326302728400947153023238062338566181756927152509363417997023999274734787344845273288270990000261654426220646299049668139206183863806933653428305884940255936320193048\\
z_3 &= 187976824174617411275658492727608034753152272175419260812887823819864021035965072399171413779616629629429327078502026383174803613079415952341627800975362562615214821149720393612897902123025291868603668914742850482614575661
\end{aligned}$$

$$\begin{aligned}
\phi(N_1) &= 37527028838815595255917926673341020013014971163375784863807222730415689120452446592951637935653265259443009919314441305303468481608669089550394883754134533317265307465043339977109985948522442438327744430027773200907849431176361605072162598399123282720139933117463564907689758595720677530014005273766133491007343459200461728058931190033481870682749560541596527382873016778508244500514039394299446425920169762964118392439145303784087161676760194005614258494450781403530401478723214958425205463556168137504502978271364181212424413735038976163711194507812147083851548412774475508213246013079835005450571234472027534146\\
\phi(N_2) &= 42578400892677454192338759382620766421411394694396168092262039466735416951925260505958139133253134534348811539538195032829772824607509088599034415335557969833145653753034937012153229509095325429496795953929477964198134012234729990548348131044966845882680257639183816053116054479016534404241562993369352163068774575645197793601846575329001222030372598756200117031103649036098814122589865800560150837041202517352725148541158008472798170103748151726696853765643412789780460731592478430473365830715595105622251213298201487304500298435157970108489250235436078162143588832805639160434723229454082105998457587938838711328563956588278613075487172852467806647147207789782952427860044854173296850602843083558352012376436597991183024765009705517224073417878205539526315911397077934407572844404848109092192429132230687997303954131526599037712059056456058821586634440835908178488624456643230900303767437118092455037138302969873010211549941006344691199946767847745282396422607982130350661161578492424836936417517430694710658749242013559182511273241563640999769627941755158821357486504115238107447916182615546662631223321553947626769358893921274536438817290462505262221020779055166807743556873300537429968263157542590127348390427515731636294470256
\end{aligned}$$

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

$$
\begin{aligned}
N_1 - \phi(N_1) + 1 &= 166665673523224621953838206544393346058890586680595756343013503201332191265502323802723070620902034023497186621980415270533550160064776059131183741994876361966842123489195948088996039900979987656475153120428672400314750532401007550356446234394729037226305536132241879139328929125498190502890255523532607888630 \\
N_2 - \phi(N_2) + 1 &= 151174552869455792380616492345454813602614783806044898394054846117255904116424500515891300369029877023447207182036945337027811697477188161287253639987938773389770363839191945518135810358383967614980176917065305154212400360067123672192525625837566710977483590486459469249804297232747780186145324308026004370812 \\
N_3 - \phi(N_3) + 1 &= 138792318017156910915514065360821895626140923762191172193012928151597434181062706879341968362260892752116130025539176970768576152466715189399573223607763830333688041336501930956135323493297195565417457179356370879229638390654336681077300841705420577663458628872697560267882972064768823843458598045163115052384
\end{aligned}
$$

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:

$$
\begin{aligned}
p_1 &= 139827604650824535502106880006759787705924055462491084984882\\
&\quad 411890209155050120398256302029535094249080148517207499814458\\
&\quad 099427188153603596101718035261121877672931434907704273690051\\
&\quad 425765725495747931733085969822723387488996909022466957166838\\
&\quad 256345486227819553011254542493260730678239287013058735270688\\
&\quad 183878759\\
p_2 &= 113739553818289492934682443651991877291502552078353716915268\\
&\quad 629542111349870727887307836086431692942580732341049297947377\\
&\quad 485629632324810403557260435301409905226787856712299547619004\\
&\quad 397936425817425707868192763627975627090536938936451293133300\\
&\quad 276418076305940351281023586805617727375912704306448107896864\\
&\quad 419447669\\
p_3 &= 969504437303931233643187178196461270709635832908405929974716\\
&\quad 674053852345873246413608813189576703547178742633062046971062\\
&\quad 144528052366657449076156502945617776617452144371121266575698\\
&\quad 291961295297840644270478665250666025546451234651989261900512\\
&\quad 467854796154115874767372927018223210335409726842489297280361\\
&\quad 81770807\\
q_1 &= 268380688724000864517313265376335583529665312181046713581310\\
&\quad 913111230362153819255464210410858077849433486694144806008124\\
&\quad 341229719111724630294657067337544842939106885814916743989446\\
&\quad 141352544919085434200344588496769272615354919850833992793961\\
&\quad 383835509984859831209873366460681984472589034898315202528444\\
&\quad 24009871\\
q_2 &= 374349990511662994459340486934293631111223172769118147878621\\
&\quad 657514455424569661320805521393733693444271486613273899795954\\
&\quad 218206515237775772999320468652886816298250712689239789913141\\
&\quad 242195815018927230872430167717858530982312818722089939232556\\
&\quad 114863467154323920543588244418656985683507587969721641116158\\
&\quad 4923143
\end{aligned}
$$

$$q_3 = 418418742867637875511953475411757685551773404713505791955412$$
$$607462121995937380655184606494045905380342418667193344798645$$
$$541233472300494444919575733132020526719428268993898042985654$$
$$942971676657813530301314898458126270837455308714821511107904$$
$$586350980480470413959602675660606510312278511592096683171269$$
$$33281577.$$

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

$$e_s d_s - k(N_s - (p_s + q_s) + 1) = z_s$$
$$e_s d_s - k(N_s - (N_s - \phi(N_s) + 1)) = z_s.$$

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:

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

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:

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

Finally, by finding the roots of the quadratic equation, the prime factors p_s and q_s can be 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:*

$$\begin{aligned}
N_1 &= 32951481839790751119453506751974428 7\\
N_2 &= 85357745769602263727953686171726113 9\\
N_3 &= 68983568816970814667566450436504946 7\\
e_1 &= 16736934834477463299170034980606965 3\\
e_2 &= 73768779370494576512022191949599738 3\\
e_3 &= 15609110911229824217876592342866329 8
\end{aligned}$$

Observe

$$\begin{aligned}
N &= \max\{N_1, N_2, N_3\} = 85357745769602263727953686171726113 9\\
e &= \min\{e_1, e_2, e_3\} = 15609110911229824217876592342866329 8
\end{aligned}$$

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.