Punjab University Journal of Mathematics (2024), 56(5), 123-134
https://doi.org/10.52280/pujm.2024.56(5)01

Another Look at the Security Analysis of the Modulus $N = p^2q$ by Utilizing an Approximation Approach for $\phi(N)$

Wan Nur Aqlili Ruzai
School of Distance Education, Universiti Sains Malaysia, Malaysia,
Email: aqliliruzai@usm.my
Normahirah Nek Abd Rahman
Pusat GENIUS@Pintar Negara, Universiti Kebangsaan Malaysia, Malaysia,
Email: normahirah@ukm.edu.my
Muhammad Asyraf Asbullah*
Centre for Foundation Studies in Science of Universiti Putra Malaysia, Universiti Putra Malaysia, Malaysia,
Email: ma asyraf@upm.edu.my

Received: 06 July, 2023 / Accepted: 18 September, 2024 / Published online: 31 October, 2024

Abstract. Newly developed techniques have been recently documented, which capitalize on the security provided by prime power modulus denoted as $N = p^r q^s$ where $2 \leq s < r$. Previous research primarily concentrated on the factorization of the modulus of type at minimum $N = p^3q^2$. In contrast, within the context of $2 \leq s < r$, we address scenarios in the modulus $N = p^2q$ (i.e. $r = 2$ and $s = 1$) still need to be covered, showing a significant result to the field of study. This work presents two factorization approaches for the multiple moduli $N_i = p_i^2 q_i$, relying on a good approximation of the Euler's totient function $\phi(N_i)$. The initial method for factorization deals with the multiple moduli $N_i = p_i^2 q_i$ derived from m public keys (N_i, e_i) and is interconnected through the equation $e_i d - k_i \phi(N_i) = 1$. In contrast, the second factorization method is associated with the $e_i d_i - k\phi(N_i) = 1$. By reorganizing the equations as a simultaneous Diophantine approximation problem and implementing the LLL algorithm, it becomes possible to factorize the list of moduli $N_i = p_i^2 q_i$ concurrently, given that the unknowns d, d_i, k, and k_i are sufficiently small. The key difference between our results and the referenced work is that we cover a real-world cryptosystem that uses the modulus $N = p^2q$. In contrast, the previous work covers a hypothetical situation of modulus in the form of $N = p^r q^s$.

AMS (MOS) Subject Classification Codes: 94A60, 11T71, 68P25
Keywords: Diophantine approximations, Lattice reduction, RSA cryptanalysis, Continued fractions, Cryptography.

1. INTRODUCTION

In the modern digital era, the need for data security has surged due to the widespread use of digital communication in business and everyday life. Safeguarding confidential information from hackers is now more critical than ever. As noted by [7], cryptographic methods remain the most reliable tools for securing sensitive data. A breakthrough in this field came from the seminal work of Turing Award recipients Rivest, Shamir, and Adleman [11], who introduced the RSA cryptosystem. This cryptographic system pioneered using distinct keys for encryption and decryption, represented by e and d, where $e \neq d$. Since its introduction in 1978, RSA has become widely recognized as a public-key encryption system that ensures the confidentiality of digital data. Its security is based on the computational difficulty of factoring large integers. While multiplying two prime numbers, p and q, to form the modulus N is straightforward, the reverse process of determining p and q from a given N remains computationally challenging, even for modern computers [4].

The security of RSA is maintained through three essential mathematical components. The first component involves selecting two large prime numbers from their product $N = pq$. The second component revolves around solving the eth root problem, specifically finding solutions to the equation $C \equiv M^e (\mathrm{mod}\ N)$. Lastly, the third component involves solving the Diophantine key equation $ed - k\phi(N) = 1$, which involves three unknowns: d, $\phi(N)$, and k.

Several factors must be considered when implementing the RSA cryptosystem to optimize the encryption and decryption processes. Decryption can be significantly accelerated if the parameter d is relatively small. However, if this small value of d is compromised, the modulus N can be efficiently factored in polynomial time. For instance, as indicated by Wiener's classical result [17], the RSA cryptosystem is particularly vulnerable when the decryption exponent is selected such that $d < \frac{1}{3} N^{\frac{1}{4}}$. This vulnerability arises from mathematical manipulations of the key equation and the continued fraction expansion of $\frac{e}{N}$. In a subsequent study, [16] presented an analysis that weakens the RSA cryptosystem when the modulus is generated by multiplying two prime numbers that are relatively close in value. These attacks rely on the same tools, specifically the Legendre theorem on continued fractions expansion, briefly detailed in [3].

In a separate study, [4] introduced an alternative attack strategy applicable when a singular entity generates k instances of RSA encryption (N_i, e_i), where each instance satisfies k equations of the form $e_i d - k_i \phi(N_i) = 1$, involving a small private exponent d. More recently, [12] discovered another vulnerability when RSA key pairs possess parameters satisfying the system of equations $e_i x_i^2 - y^2 \phi(N_i) = z_i$, allowing for simultaneous factorization if appropriately small, unknown integers x_i, y, and z_i exist. The study in [13] reaffirmed the hypothesis. Considering the equation $ex - (N - p - q + u)y = z$, where all variables except e and N are private, they demonstrated that it is feasible to compromise the RSA modulus even if only one private parameter, either x or y, remains constant, given that certain conditions are met. Their results hold for both scenarios: $e_i x - (N_i - p_i - q_i + u_i) y_i = z_i$ and $e_i x_i - (N_i - p_i - q_i + u_i) y = z_i$.

In a different scenario, [8] introduced a novel technique for factoring multiple instances of RSA moduli $N_1, ..., N_k$, involving a system of k equations in the form of $e_i x - y_i \phi(N_i) =$

z_i or $e_i x_i - y\phi(N_i) = z_i$, where $\phi(N_i) = (p_i - 1)(q_i - 1)$. The unknown parameters (x, y_i) or (y, x_i) were concurrently solved using the LLL algorithm [5], with suitable values assigned to the parameters x, x_i, y, y_i, and z_i, which made significant advancements by further expanding the field. Their research explores four innovative cryptanalytic attacks that demonstrate the feasibility of concurrently factoring multiple RSA moduli $N = pq$ by applying lattice basis reduction techniques.

In [15], an alternative approach known as prime power RSA was introduced, which employs a different form of RSA modulus. This approach enhances decryption by having the modulus as $N = p^r q$, where $r \geq 2$. Following that, numerous adjustments have been put forward to evaluate the security of the $N = p^r q$ modulus while upholding adequate levels of protection. As an illustration, two attacks are presented in [6] that specifically target small secret exponents and exploit techniques for solving modular univariate polynomial equations. The discoveries of [6] emphasize the heightened susceptibility of RSA-type schemes utilizing moduli in the form of $N = p^r q$ compared to the original RSA scheme employing $N = pq$. As a result, it is imperative to conduct a thorough security assessment of the $N = p^r q$ scenario.

Additionally, research by [14] demonstrates that a cryptosystem utilizing $N = p^r q$ becomes vulnerable when combined with a decryption exponent d limited by an upper bound of $N^{0.395}$. In contrast to the method employed by [14] to solve the equation $ex - Ny = 1$, [9] tackled the broader equation $ex - Ny = z$. As a result, their findings revealed many potential solutions to the problem. From an intuitive standpoint, the technique utilized by [9] enhances the likelihood of identifying solutions, especially in the factorization of the modulus N.

Our Contributions. Considering the effectiveness of cryptographic attacks, it is essential to consider various factors, including parameter choices, modulus size, and implemented security measures within the cryptosystem. Recent research by [1] introduces new techniques that exploit the security of prime power moduli of the form $N = p^r q^s$, where $2 \leq s < r$. Please observe that the primary distinction between our findings and the referenced study lies in the fact that we address a real-world cryptosystem employing the modulus $N = p^2 q$. In contrast, the prior work examines a theoretical case with a modulus of the form $N = p^r q^s$. Specifically, in the context of $2 \leq s < r$, at minimum, the modulus is of type $N = p^3 q^2$, while in this work, we focus on cases where $r = 2$ and $s = 1$ still need to be explored, thereby contributing a significant result to the field. Consequently, our research complements the findings presented by [1].

Motivated by the developments in [1], [10], and [8], we propose two factorization methods that address the case where all RSA moduli $N_1, ..., N_m$ satisfy a set of m equations. The first method is designed for m instances of (N_i, e_i), where $N_i = p_i^2 q_i$ for $i = 1, ..., m$ and $m \geq 2$. Note that this approach is applicable whenever the integers d, m, k_i and δ_1 met certain conditions such that $e_i d - k_i \phi(N_i) = 1$ and satisfying

$$d < N^{\delta_1},\ k_i < N^{\delta_1} \text{ where } \delta_1 = \frac{m(1-\gamma)}{m+1},\ N = \min\{N_i\}.$$

Note that the parameter γ is defined as the upper bound inequality from Lemma 2.2 (See Section 2.1 for more details). The second method of factorization is centered around a set of m instances (N_i, e_i) that satisfy the equation $e_i d_i - k\phi(N_i) = 1$, where k is an

integer and d_i are multiple integers. Additionally, this research proposes a polynomial-time factorization algorithm for m RSA moduli N_i under certain conditions. Specifically, if the values satisfy the inequalities:

$$d_i < N^{\delta_2},\ k < N^{\delta_2},\ \ \delta_2 = \frac{m(\alpha-\gamma)}{m+1},\ N = \max\{N_i\},\ \min\{e_i\} = N^{\alpha}.$$

We employ a technique that involves restructuring the equations into a problem of simultaneous Diophantine approximations. By applying the LLL algorithm [5], we can solve for the unknown parameters (d, k_i) and (k, d_i). This approach allows us to factorize m moduli $N_i = p_i^2 q_i$ simultaneously, thereby obtaining the prime factors p_i and q_i for each modulus N_i.

This research paper consists of five sections. In Section 2, we review the actual results that serve as the basis for our work. The first and second factorization methods are presented in Sections 3 and 4, respectively, along with numerical examples. Finally, the overall work is concluded in Section 5.

2. Mathematical Groundwork

In the following section, we will introduce a set of definitions and theorems that pertain to the good approximation of $\phi(N)$ and the approach for solving simultaneous Diophantine approximations by employing lattice basis reduction methods. We will present the following lemmas and theorems, which will play a significant role in this research's subsequent discussions and analyses.

2.1. A Good Approximation of $\phi(N)$.

Suppose $N = p^2q$ with $q < p < 2q$, then $2^{-1/3}N^{1/3} < q < N^{1/3} < p < 2^{1/3}N^{1/3}$. Let $\phi(N) = p(p-1)(q-1)$, hence $N - \phi(N) = p^2 + pq - p$, therefore [10] show that $2N^{2/3} - N^{1/3} < N - \phi(N) < (2^{2/3} + 2^{-1/3})N^{2/3} - 2^{1/3}N^{1/3}$, which are the upper and lower bounds in terms of N. It proves that both $N - (2N^{2/3} - N^{1/3})$ and $N - \left((2^{2/3} + 2^{-1/3})N^{2/3} - 2^{1/3}N^{1/3}\right)$ is a good approximation of $\phi(N)$, respectively for the case of $p \approx q$ or $p \approx 2q$.

Lemma 2.2 ([10]). *Let $N = p^2q$ with $q < p < 2q$. Then*

$$|N - \left((2^{2/3} + 2^{-1/3})N^{2/3} - 2^{1/3}N^{1/3}\right) - \phi(N)| < 2p^{5/3}|2^{1/3}q^{1/3} - p^{1/3}|$$

To facilitate our analysis, let $\left((2^{2/3} + 2^{-1/3})N^{2/3} - 2^{1/3}N^{1/3}\right)$ be defined as Θ. Hence, the expression $N - \Theta$ is considered a good approximation of $\phi(N)$, satisfying $1 < e < \phi(N) < N - \Theta$. Furthermore, [10] introduced a parameter γ and established an upper bound inequality from Lemma 2.2 as $2p^{5/3}\left|2^{1/3}q^{1/3} - p^{1/3}\right| < \frac{1}{6}N^{\gamma}$. Next, [10] presented the following theorem, which we will use as the foundational theorem for our work.

Theorem 2.3 ([10]). *Let $N = p^2q$ with $q < p < 2q$. Let $\Theta = (2^{2/3} + 2^{-1/3})N^{2/3} - 2^{1/3}N^{1/3}$ satisfying $1 < e < \phi(N) < N - \Theta$ and $ed - k\phi(N) = 1$ where the values $\phi(N)$, d and k are unknowns. Let $\phi(N) > \frac{2}{3}N$ and $N > 6d$. Suppose $2p^{5/3}|2^{1/3}q^{1/3} - p^{1/3}| < \frac{1}{6}N^{\gamma}$ and $d < N^{\delta}$. If $\delta < \frac{1-\gamma}{2}$, then $\left|\frac{e}{N-\Theta} - \frac{k}{d}\right| < \frac{1}{2d^2}$.*

2.4. **Simultaneous Diophantine Approximations.** A collection of d linearly independent vectors $u_1, \ldots, u_\omega$ in $\mathbb{R}^n$ establishes a lattice when $\omega \leq n$. This lattice is constructed by considering all conceivable integer linear combinations of the vectors $u_1, \ldots, u_\omega$.

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

For a given lattice $\mathcal{L}$ with a basis consisting of the set $(u_1, \ldots, u_\omega)$ in $\mathbb{R}^n$, where each u_i is an integer vector in the canonical basis of $\mathbb{R}^n$, the determinant of the lattice, represented as $\det(\mathcal{L})$, can be computed as $\sqrt{\det(U^T U)}$. Here, U denotes the matrix composed of the vectors u_i.

Within the realm of lattice reduction, a significant and complex task involves locating a short nonzero vector within $\mathcal{L}$. The LLL algorithm (refer to [5] for citation) offers a reduced basis for the lattice, and this concept is outlined by the following theorem, as mentioned in [6].

Theorem 2.5 ([5])**.** *Suppose a basis $\{v_1, ..., v_\tau\}$ formed a lattice $\mathcal{L}$ with dimension τ. Then a reduced basis $\{b_1, ..., b_\tau\}$ satisfies*

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

for all $1 \leq i \leq \tau$ is produced by the LLL algorithm.

The LLL algorithm, introduced in the work by Lenstra, Lenstra, and Lovász [5], plays a crucial role in solving the problem of simultaneous Diophantine approximations. This algorithm is particularly valuable in scenarios where the lattice contains real-valued entries, as evidenced by the following statement. Employing the LLL method allows for the computation of simultaneous Diophantine approximations for rational numbers.

Later, Nitaj et al. ([8]) presented a result that is analogous to Dirichlet's Theorem ([2]), but for a lattice with integer entries, as opposed to rational entries. The following theorem demonstrates this equivalence.

Theorem 2.6 (Simultaneous Diophantine Approximations, [8])**.** *For a given collection of rational numbers $\alpha_1, \cdots, \alpha_n$, with $0 < \varepsilon < 1$, there exists an algorithm that operates in polynomial time and can determine values $p_1, \cdots, p_n \in \mathbb{Z}$ and $q \in \mathbb{Z}^+$ such that*

$$\max_i |q\alpha_i - p_i| < \varepsilon \ \text{ and } \ q \leq 2^{n(n-3)/4} \cdot 3^n \cdot \varepsilon^{-n}$$

3. Factoring m Moduli $N_i = p_i^2 q_i$ satisfy $e_i d - k_i \phi(N_i) = 1$

This section will examine our initial approach to factoring, which involves considering m moduli $N_i = p_i^2 q_i$. Suppose we have a system with a key equation given by $e_i d - k_i \phi(N_i) = 1$. Then, we demonstrate a method for factoring each modulus $N_i = p_i^2 q_i$ if the unknown values of d and k_i are sufficiently small. Let $N_i = p_i^2 q_i$ for $1 \leq i \leq m$. Assuming $m \geq 2$, this mathematical statement means that we are given $N_1, N_2, N_3, ..., N_m$ moduli instances or similarly can be viewed as a set of m moduli N.

Recall that in Section 2.1, we defined $\Theta = (2^{2/3} + 2^{-1/3})N^{2/3} - 2^{1/3}N^{1/3}$. Similarly, in this section, we define $\Theta_i = \left((2^{2/3} + 2^{-1/3})N_i^{2/3} - 2^{1/3}N_i^{1/3}\right)$. For the remainder of this section, we approximate $\phi(N_i)$ as $N_i - \Theta_i$ and satisfy $1 < e_i < \phi(N_i) < N_i - \Theta_i$.

Moreover, from Lemma 2.2 the parameter γ provides an upper bound inequality given by $2p^{5/3}\left|2^{1/3}q^{1/3}-p^{1/3}\right| < \frac{1}{6}N^{\gamma}$. To achieve our objectives, we apply a combination of the LLL algorithm technique and the integration of the problem.

Theorem 3.1. *Suppose $m \geq 2$. Let $N_i = p_i^2 q_i$ with $1 \leq i \leq m$ be a set of m moduli N_i. Consider a set of m public exponents e_i such that $e_i d - \phi(N_i)k_i = 1$ with $1 < e_i < \phi(N_i) < N_i - \Theta_i$. Define δ_1 as $\delta_1 = \frac{m(1-\gamma)}{m+1}$. Let $N = \min\{N_i\}$. Suppose there exists an integer d such that $d < N^{\delta_1}$ and a set of m integers k_i such that $k_i < N^{\delta_1}$, then it becomes feasible to simultaneously factor a set of m moduli $N_i = p_i^2 q_i$.*

Proof. Let rewrite the equation $e_i d - \phi(N_i)k_i = 1$ with $i = 1, ..., m$ as $e_i d - k_i(N_i - \Theta_i) = 1 - k_i(N_i - \Theta_i - \phi(N_i))$ by assuming $m \geq 2$. Dividing both sides by $(N_i - \Theta_i)$,

$$\left|\frac{e_i d}{N_i - \Theta_i} - k_i\right| = \frac{|1 - k_i(N_i - \Theta_i - \phi(N_i))|}{N_i - \Theta_i}. \tag{3. 1}$$

Let $N = \min\{N_i\}$ and suppose that $k_i < N^{\delta_1}$. By applying Lemma 2.2 and Theorem 2.3 to equation (3. 1), we have

$$\begin{aligned}
\frac{|1 - k_i(N_i - \Theta_i - \phi(N_i))|}{N_i - \Theta_i} &\leq \frac{|1 + k_i(N_i - \Theta_i - \phi(N_i))|}{N - \Theta} \\
&< \frac{1 + N^{\delta_1}(2p^{5/3}|2^{1/3}q^{1/3} - p^{1/3}|)}{\phi(N)} \\
&< \frac{N^{\delta_1}\left(\frac{N^{\gamma}}{6}\right)}{\frac{2}{3}N} \\
&= \frac{1}{4}N^{\gamma - 1 + \delta_1}.
\end{aligned} \tag{3. 2}$$

Substituting (3. 2) into (3. 1) yields $\left|\frac{e_i d}{N_i - \Theta_i} - k_i\right| < \frac{1}{4}N^{\gamma - 1 + \delta_1}$. This inequality is connected to the relation of $|q\alpha_i - p_i| < \varepsilon$ in Theorem 2.6.

Next, suppose $\varepsilon = \frac{1}{4}N^{\gamma - 1 + \delta_1}$ with $\delta_1 = \frac{m(1-\gamma)}{m+1}$. Thus, we can show that the integers k_i and an integer d exist as follows.

$$\begin{aligned}
N^{\delta_1} \cdot \varepsilon^m &= N^{\delta_1} \cdot \left(\frac{1}{4}N^{\gamma - 1 + \delta_1}\right)^m \\
&= \left(\frac{1}{4}\right)^m \cdot N^{m\gamma - m + \delta_1(m+1)} \\
&= \left(\frac{1}{4}\right)^m.
\end{aligned}$$

By utilizing Theorem 2.6, we can establish that $\left(\frac{1}{4}\right)^m < 2^{\frac{m(m-3)}{4}} \cdot 3^m$ holds true for $m \geq 2$. As a result, we derive the inequality $N^{\delta_1} \cdot \varepsilon^m < 2^{\frac{m(m-3)}{4}} \cdot 3^m$. This implies that if $d < N^{\delta_1}$, then $d < 2^{\frac{m(m-3)}{4}} \cdot 3^m \cdot \varepsilon^{-m}$.

In summary, for $i = 1, ..., m$, we have the following expressions

$$\left|\frac{e_i d}{N_i - \Theta_i} - k_i\right| < \varepsilon, \;\; d < 2^{\frac{m(m-3)}{4}} \cdot 3^m \cdot \varepsilon^{-m}.$$

The LLL method may be used to determine appropriate values for d and k_i if the requirements of Theorem 2.6 are satisfied.

Next, we can observe that from the relation $\frac{e_i d-1}{k_i} = \phi(N_i) = p_i(p_i-1)(q_i-1)$ obtained from the key equation $e_i d - k_i\phi(N_i) = 1$. By computing $\gcd\left(\frac{e_i d-1}{k_i}, N_i\right)$, we can determine the prime factors p_i and q_i. This step concludes the proof. □

Example 3.2. *Now we consider the following set of moduli N_i and public exponents e_i of $i = 1, 2, 3$ to illustrate the result given by Theorem 3.1;*

$$\begin{aligned}
N_1 &= 112867123376470408653263199054463502693791,\\
N_2 &= 136789857845500469532399383417508044710603,\\
N_3 &= 208365783654051108310301332834225969741073,\\
e_1 &= 175383882354917454124520905611608095924 97,\\
e_2 &= 103007543093641616857371139631264721817913,\\
e_3 &= 637948016052436305353322362030672574746 17.
\end{aligned}$$

Then,

$$\begin{aligned}
N &= \min\{N_1, N_2, N_3\}\\
&= 112867123376470408653263199054463502693791.
\end{aligned}$$

For $m = 3$ and $\gamma < \frac{2}{3}$, we have $\delta_1 = \frac{m(1-\gamma)}{m+1} = \frac{3}{8}$ and $\varepsilon = \frac{1}{4}N^{\gamma-1+\delta_1} \approx 0.00000184658403$. Suppose that we consider the parameter C as defined in [8]*(Appendix A), hence*

$$C = 3^{n+1} \cdot 2^{\frac{(n+1)(n-4)}{4}} \cdot \varepsilon^{-n-1} = 34832024464334231759555 54.$$

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

$$M = \begin{bmatrix} 1 & -\left(\frac{Ce_1}{N_1-\Theta_1}\right) & -\left(\frac{Ce_2}{N_2-\Theta_2}\right) & -\left(\frac{Ce_3}{N_3-\Theta_3}\right)\\ 0 & C & 0 & 0\\ 0 & 0 & C & 0\\ 0 & 0 & 0 & C \end{bmatrix}.$$

The LLL algorithm is applied to the lattice $\mathcal{L}$, resulting in a reduced basis and a corresponding matrix $K =$

$$K = \begin{bmatrix} 41576213882633 & 24678480219062 & 22966785794519 & 11271983811383\\ -19110663333309233790 & -11608797265014257382 & 18330462969482397926 & 58556327000651781146\\ 53696242185316569007 & -16156024869951421484 & -86545885487631096783 & 13653334934646825167\\ 40394375403892696664 & -10408336725530587911 2 & 39647605397062117470 & -18987960312013678 44 \end{bmatrix}.$$

Multiplying K with M^{-1}, we have

$$K\cdot M^{-1} = \begin{bmatrix} 41576213882633 & 6460515326534 & 31308341938794 & 12729279585287\\ -19110663333309233790 & -29696002073110532 13 & -14390997314124042296 & -58510613139692698 76\\ 53696242185316569007 & 8343842866375736503 & 40435146786379784230 & 16440036636950507088\\ 40394375403892696664 & 6276869802029453220 & 30418376264832485819 & 12367439219952058594 \end{bmatrix}.$$

Observe that from the first row of the matrix, we deduce $d = 41576213882633$, $k_1 = 6460515326534$, $k_2 = 31308341938794$, and $k_3 = 12729279585287$. We can proceed further by applying these values for d and k_i (where $i = 1, 2, 3$). Next, we observe that from the equation $\frac{e_i d-1}{k_i} = \phi(N_i) = p_i(p_i-1)(q_i-1)$, we can determine the values of p_i and q_i.

$$\frac{e_1d-1}{k_1} = 1128671233764654870170389451108994394869 00,$$
$$\frac{e_2d-1}{k_2} = 1367898578454949684268812245174131816901 12,$$
$$\frac{e_3d-1}{k_3} = 2083657836540438627943427200491454070028 80.$$

By computing $\gcd\left(\frac{e_id-1}{k_i}, N_i\right)$ *for each* $i = 1, 2, 3$*, we obtain*

$$\begin{aligned} p_1 &= 52740952448491, \\ p_2 &= 54829642997377, \\ p_3 &= 62575397893241. \end{aligned}$$

We can compute $q_i = \frac{N_i}{p_i}$ *for* $i = 1, 2, 3$ *to complete the factorisation. This will give us the following values of* q_i*.*

$$\begin{aligned} q_1 &= 40576213733911, \\ q_2 &= 45501222159307, \\ q_3 &= 53213174014433. \end{aligned}$$

4. Factoring m Moduli $N_i = p_i^2q_i$ Satisfying $e_id_i - k\phi(N_i) = 1$

We examine m moduli $N_i = p_i^2q_i$ with a distinct framework in the second scenario. Specifically, we focus on the key equation system denoted by $e_id_i - k\phi(N_i) = 1$, where k remains constant. This section presents an alternative method for factoring multiple moduli $N_i = p_i^2q_i$ using a similar approach to that described in Section 3. Let Θ_i be the parameter as defined in Section 3 such that $1 < e_i < \phi(N_i) < N_i - \Theta_i$ and γ as defined in Lemma 2.2. In essence, our objective in this section is to determine suitable values for the integer k and m integers d_i, allowing us to simultaneously compute the prime factors p_i and q_i for each $N_i = p_i^2q_i$.

Theorem 4.1. *Suppose* $m \geq 2$*. Let* $N_i = p_i^2q_i$ *with* $1 \leq i \leq m$ *be a set of* m *moduli* N_i*. Consider a set of* m *public exponents* e_i *with* $\min\{e_i\} = N^\alpha$ *such that* $e_id_i - \phi(N_i)k = 1$ *with* $1 < e_i < \phi(N_i) < N_i - \Theta_i$*. Let* $N = \max\{N_i\}$*. Define* δ_2 *as* $\delta_2 = \frac{m(\alpha-\gamma)}{m+1}$*. Suppose there exists a set of* m *integers* d_i *such that* $d_i < N^{\delta_2}$ *and an integer* k *such that* $k < N^{\delta_2}$*, then it becomes feasible to simultaneously factor a set of* m *moduli* $N_i = p_i^2q_i$*.*

Proof. Let's assume that $m \geq 2$ and $i = 1, ..., m$. The key equation of the form $e_id_i - \phi(N_i)k = 1$ can also be expressed as $e_id_i - k(N_i - \Theta_i) = 1 - k(N_i - \Theta_i - \phi(N_i))$. By dividing both sides of the equation by e_i, we obtain

$$\left|\frac{(N_i - \Theta_i)k}{e_i} - d_i\right| = \frac{|1 - k(N_i - \Theta_i - \phi(N_i))|}{e_i}. \tag{4. 3}$$

Let $N = \max\{N_i\}$ and suppose that $k < N^{\delta_2}$. By applying Lemma 2.2 and Theorem 2.3 to equation (4. 3), we have

$$\begin{aligned}\frac{|1-k(N_i-\Theta_i-\phi(N_i))|}{e_i} &\leq \frac{|1+k(N_i-\Theta_i-\phi(N_i))|}{e_i}\\ &< \frac{N^{\delta_2}(\frac{1}{6}N^{\gamma})}{N^{\alpha}}\\ &= \frac{1}{6}N^{\gamma+\delta_2-\alpha}. \qquad (4.\ 4)\end{aligned}$$

Next, we can substitute (4. 4) into (4. 3), resulting in

$$\left|\frac{(N_i-\Theta_i)k}{e_i}-d_i\right| < \frac{1}{6}N^{\gamma+\delta_2-\alpha}.$$

By examining the relationship $\left|\frac{N_i-\Theta_i k}{e_i}-d_i\right| < \frac{1}{6}N^{\gamma+\delta_2-\alpha}$ and $|q\alpha_i - p_i| < \varepsilon$, it verifies that an integer k and a set of m integers d_i exist and satisfy the requirement stated in Theorem 2.6. Therefore, we can confirm the existence of an integer k and m integers d_i. Let $\varepsilon = \frac{1}{6}N^{\gamma+\delta_2-\alpha}$, where $\delta_2 = \frac{m(\alpha-\gamma)}{m+1}$. Thus, we obtain:

$$N^{\delta_2}\cdot\varepsilon^m = \left(\frac{1}{6}\right)^m \cdot N^{m\gamma+m\delta_2-m\alpha+\delta_2} = \left(\frac{1}{6}\right)^m.$$

We can observe that since $\left(\frac{1}{6}\right)^m < 2^{\frac{m(m-3)}{4}}\cdot 3^m$ holds true for $m \geq 2$, then from Theorem 2.6 we deduce that $N^{\delta_2}\cdot\varepsilon^m < 2^{\frac{m(m-3)}{4}}\cdot 3^m$. Consequently, if $k < N^{\delta_2}$, then $k < 2^{\frac{m(m-3)}{4}}\cdot 3^m\cdot\varepsilon^{-m}$. Summarizing for $i = 1,\ldots,m$, thus

$$\left|\frac{(N_i-\Theta_i)k}{e_i}-d_i\right| < \varepsilon,\ \ k < 2^{\frac{m(m-3)}{4}}\cdot 3^m\cdot\varepsilon^{-m}.$$

The fulfillment of the conditions outlined in Theorem 2.6 enables us to find suitable values for k and d_i, where $i = 1,\ldots,m$. Subsequently, utilizing the equation $\frac{e_i d_i-1}{k} = \phi(N_i)$ derived from $e_i d_i - k\phi(N_i) = 1$, hence from the $\gcd\left(\frac{e_i d_i-1}{k}, N_i\right)$, we have the primes p_i and q_i. □

Example 4.2. *Now we consider the following set of moduli N_i and public exponents e_i of $i = 1,2,3$ to illustrate our second attack;*

$$\begin{aligned}N_1 &= 6363691928758772595649269221177397975336 1,\\ N_2 &= 2537256059018434446852821228666856830358954 1,\\ N_3 &= 1456890342745477337643604259935152780295 01,\\ e_1 &= 7911921927156091123970669618740459681 9,\\ e_2 &= 3024902410247848931985857610521212 3,\\ e_3 &= 5170221537914384465237028435595908969 95.\end{aligned}$$

Then, $N = \max\{N_1,N_2,N_3\} = 25372560590184344468528212286656830358954 1$. It is observed that the values of $\min(e_1,e_2,e_3)$ are equal to N^{α}, where $\alpha \approx 0.8327796345$. Given that $m = 3$ and $\gamma < \frac{2}{3}$, we can calculate δ_2 as $\frac{m(\alpha-\gamma)}{m+1} = 0.2495847259$. Furthermore, ε can be computed as $\frac{1}{6}N^{\gamma+\delta_2-\alpha} \approx 0.00005987099092$.

Let us consider the same parameter C as defined in Section 3, which is given by $C = 3152021988753206625$. We define the lattice $\mathcal{L}$ as the lattice formed by the vectors generated by the rows of the matrix.

$$M = \begin{bmatrix} 1 & -\left(\frac{C(N_1-\Theta_1)}{e_1}\right) & -\left(\frac{C(N_2-\Theta_2)}{e_2}\right) & -\left(\frac{C(N_3-\Theta_3)}{e_3}\right) \\ 0 & C & 0 & 0 \\ 0 & 0 & C & 0 \\ 0 & 0 & 0 & C \end{bmatrix}.$$

Applying the LLL algorithm to the lattice $\mathcal{L}$ results in the reduced basis along with the corresponding matrix as follows.

$$K = \begin{bmatrix} 199550684 & 31567911 & 20616855 & 184883415 \\ -1518078889982202 & 1431558690461667 & 508689221635560 & 1337355126515130 \\ -1408066824069149 & -4162944694575771 & 1293928905936345 & 2086284551976435 \\ -1516501615446218 & -1680556031238597 & -8235463408567710 & 2842114932882045 \end{bmatrix}.$$

Now, we multiply K with M^{-1}, we have

$$K \cdot M^{-1} = \begin{bmatrix} 199550684 & 160501972699 & 1673809972662131 & 56230368907 \\ -1518078889982202 & -1221016393784205771 & -12733484718799899997442 & -427771703421614356 \\ -1408066824069149 & -1132531838152527650 & -11810715178012799535388 & -396771964776207508 \\ -1516501615446218 & -1219747765336340707 & -12720254707280841238424 & -427327251279190241 \end{bmatrix}.$$

From the first row of the matrix provided above, we can deduce the following values: $k = 199550684$, $d_1 = 160501972699$, $d_2 = 1673809972662131$, and $d_3 = 1673809972662131$. By utilizing these values of d_i (where $i = 1, 2, 3$) and k, we can observe that applying $\frac{e_i d_i - 1}{k} = \phi(N_i)$ from the key equation, we obtain:

$$\frac{e_1 d_1 - 1}{k} = 6363691928758442162448797417421180067872 0$$

$$\frac{e_2 d_2 - 1}{k} = 2537256059018352546317153537117028950289 68$$

$$\frac{e_3 d_3 - 1}{k} = 1456890342745418631900595370196812012732 96.$$

Therefore, by computing $\gcd\left(\frac{e_i d_i - 1}{k}, N_i\right)$ for each i=1,2,3, we obtain

$$\begin{aligned} p_1 &= 42514915472999, \\ p_2 &= 65860199881523, \\ p_3 &= 57926883793637. \end{aligned}$$

For completion of the factorization, we compute $q_i = \frac{N_i}{p_i}$ for $i = 1, 2, 3$ which gives

$$\begin{aligned} q_1 &= 35206796259361, \\ q_2 &= 58494927820829, \\ q_3 &= 43417671901829. \end{aligned}$$

5. CONCLUSION

This work introduces novel cryptanalysis techniques specifically designed for moduli of the form $N_i = p_i^2 q_i$. Our approach involves utilizing the expression $N_i - ((2^{2/3} + 2^{-1/3})N_i^{2/3} - 2^{1/3}N_i^{1/3})$ as an approximation for Euler's totient function ($\phi(N_i)$). We explore two key equations: $e_i d - k_i \phi(N_i) = 1$ for the first cryptanalysis technique, and $e_i d_i - k\phi(N_i) = 1$ for the second cryptanalysis technique. Our findings demonstrate that both attacks successfully factorize moduli $N_i = p_i^2 q_i$ when certain parameters, specifically d, d_i, k, and k_i, are sufficiently small. Importantly, we highlight that each cryptanalysis technique achieves factorization by transforming the problem into a set of simultaneous Diophantine approximation equations and applying the LLL algorithm. This work sheds light on the effectiveness of these approaches in successfully breaking the security of the considered moduli.

Our work complements the findings in [1], providing additional insights and contributions to the field. While [1] primarily concentrated on the factorization of the $N = p^r q^s$ where $2 \leq s < r$, which we observed at minimum $N = p^3 q^2$, our work focuses on a scenario not covered in [1], where $r = 2$ and $s = 1$. Hence, our work extends the scope by considering a specific case not previously explored. Acknowledging that various factors influence the effectiveness of cryptographic attacks is crucial. These factors include the specific choices of parameters, the size of the moduli involved, and the security measures implemented within the cryptosystem. Considering these factors is essential for a comprehensive evaluation of cryptographic security.

Acknowledgments The authors sincerely thank the anonymous reviewers for their insightful comments and constructive suggestions.

Author contributions Wan Nur Aqlili Ruzai: Writing-original draft, Writing – review & editing, Formal analysis; Normahirah Nik Abd Rahman: Writing – review & editing, Methodology, Formal analysis, Validation; Muhammad Asyraf Asbullah: Writing-original draft, Conceptualization, Funding acquisition, Validation, Writing – review & editing.

Funding This research received no external funding.

Conflict of Interest The authors have declared no conflict of interest.

REFERENCES

[1] S. I. Abubakar, S. Shehu. *Exploiting the Security of $N = p^r q^s$ Through Approximation of $\phi(N)$*. Discrete Mathematics, Algorithms and Applications **14**, no. 4 (2022): 2150144.

[2] J. W. S. Cassels, *An Introduction to the Geometry of Numbers*, Springer Science & Business Media, 2012.

[3] A. Gaber. *Intersections of Pell, Pell-Lucas Numbers and Sums of Two Jacobsthal Numbers*. Punjab Univ. J. Math. **55**, no. 5-6, (2023): 241-252.

[4] M. J. Hinek, *On the Security of Some Variants of RSA*, PhD Thesis, Waterloo, Ontario, Canada, 2007.

[5] A. K. Lenstra, H. W. Lenstra, and L. Lovász. *Factoring Polynomials With Rational Coefficients*. Mathematische Annalen **261**, no. 4 (1982): 515-534.

[6] A. May. *Secret Exponent Attacks on RSA-Type Schemes With Moduli $N = p^r q$*. In Proceedings of the Public Key Cryptography—PKC 2004, Springer: Berlin/Heidelberg, Germany, (2004), 218-230.

[7] R. Navalakhe, and A. Harsha. *Implementation of Cryptographic Algorithms Using Moore Machine and Recurrence Matrix*. Punjab Univ. J. Math. **55**, no. 3 (2023).

[8] A. Nitaj, M. R. K. Ariffin, D. I. Nassr, and H. M. Bahig. *New attacks on the RSA cryptosystem*. In Pointcheval, D., Vergnaud, D. (eds) Progress in Cryptology – AFRICACRYPT 2014. AFRICACRYPT 2014. Lecture Notes in Computer Science, vol. **8469**, Springer: Cham, (2014), 178-198.

[9] A. Nitaj, T. Rachidi. *New attacks on RSA with moduli $N = p^r q$*. In Proceedings of the Codes, Cryptology, and Information Security, Springer: Cham, (2015), 352-360.

[10] N. N. A. Rahman, M. A. Asbullah, M. R. K. Ariffin, S. H. Sapar, and F. Yunos. *Cryptanalysis of RSA Key Equation of $N = p^2 q$ for Small $|2q - p|$ Using Continued Fraction*. Malaysian Journal of Science **39**, no. 1 (2020): 72-80.

[11] R. Rivest, A. Shamir, and L. Adleman. *A Method for Obtaining Digital Signatures and Public Key Cryptosystems*. Communication of the ACM **21**, no. 2 (1978): 120-126.

[12] W. N. A. Ruzai, M. R. K. Ariffin, M.A. Asbullah, and A. H. A. Ghafar. *New Simultaneous Diophantine Attacks on Generalized RSA Key Equations*. Journal of King Saud University-Computer and Information Sciences **36**, no. 5 (2024):102074.

[13] W. N. A. Ruzai, Y. Ying, K. N. Muhammad, M. A. Asbullah, and M. R. K. Ariffin, *Concurrent Factorization of RSA Moduli Via Weak Key Equations*. AIMS Mathematics **9**, no. 10 (2024): 28211-28231.

[14] S. Sarkar. *Small Secret Exponent Attack on RSA Variant with Modulus $N = p^r q$*. Designs, Codes and Cryptography **73**, no. 2 (2014): 383-392.

[15] T. Takagi. *Fast RSA-Type Cryptosystem Modulo $p^k q$*. In Proceedings of the Advances in Cryptology—CRYPTO' 98, Springer: Berlin Heidelberg, (1998), 318-326.

[16] B. De Weger. *Cryptanalysis of RSA with Small Prime Difference*. Applicable Algebra in Engineering, Communication and Computing **13**, no. 1, (2002): 17-28.

[17] M. Wiener. *Cryptanalysis of Short RSA Secret Exponents*. IEEE Transaction on Information Theory **36**, no. 3 (1990): 553-558.