mathematics

MDPI

Article

Factoring the Modulus of Type $N = p^2q$ by Finding Small Solutions of the Equation $er - (Ns + t) = \alpha p^2 + \beta q^2$

Muhammad Asyraf Asbullah [1,2,*,†], Normahirah Nek Abd Rahman [3,†], Muhammad Rezal Kamel Ariffin [1,4,†] and Nur Raidah Salim [1,†]

[1] Laboratory of Cryptography, Analysis and Structure, Institute for Mathematical Research, University Putra Malaysia, UPM, Serdang 43400, Malaysia; rezal@upm.edu.my (M.R.K.A.); nurraidah@upm.edu.my (N.R.S.)
[2] Centre of Foundation Studies for Agricultural Science, University Putra Malaysia, UPM, Serdang 43400, Malaysia
[3] Pusat GENIUS@Pintar Negara, University Kebangsaan Malaysia, UKM, Bangi 43600, Malaysia; normahirah@ukm.edu.my
[4] Department of Mathematics & Statistics, Faculty of Science, University Putra Malaysia, UPM, Serdang 43400, Malaysia
* Correspondence: ma_asyraf@upm.edu.my
† These authors contributed equally to this work.

Abstract: The modulus of type $N = p^2q$ is often used in many variants of factoring-based cryptosystems due to its ability to fasten the decryption process. Faster decryption is suitable for securing small devices in the Internet of Things (IoT) environment or securing fast-forwarding encryption services used in mobile applications. Taking this into account, the security analysis of such modulus is indeed paramount. This paper presents two cryptanalyses that use new enabling conditions to factor the modulus $N = p^2q$ of the factoring-based cryptosystem. The first cryptanalysis considers a single user with a public key pair (e, N) related via an arbitrary relation to equation $er - (Ns + t) = \alpha p^2 + \beta q^2$, where r, s, t are unknown parameters. The second cryptanalysis considers two distinct cases in the situation of k-users (i.e., multiple users) for $k \geq 2$, given the instances of (N_i, e_i) where $i = 1, \ldots, k$. By using the lattice basis reduction algorithm for solving simultaneous Diophantine approximation, the k-instances of (N_i, e_i) can be successfully factored in polynomial time.

Keywords: cryptography; IoT security; lattice basis reduction; Diophantine approximation; pre-quantum cryptography

check for updates

Citation: Asbullah, M.A.; Rahman, N.N.A.; Ariffin, M.R.K.; Salim, N.R. Factoring the Modulus of Type $N = p^2q$ by Finding Small Solutions of the Equation $er - (Ns + t) = \alpha p^2 + \beta q^2$. *Mathematics* **2021**, *9*, 2931. https://doi.org/10.3390/math9222931

Academic Editors: Luis Hernández Encinas and Víctor Gayoso Martínez

Received: 29 September 2021
Accepted: 12 November 2021
Published: 17 November 2021

1. Introduction

The integration of digital and physical realms has advanced considerably during the previous decade, resulting in the Internet of Things (IoT). The IoT is frequently viewed as a paradigm shift from the standard Internet to environments connected to everything. The advancement of technology incorporated in heterogeneous devices, such as smartphones, tablets, radio-frequency identification (RFID), Wifi, smart cities, and smart homes enables all types of communications, even unlawful ones. These connected gadgets equipped with actuators or sensors can detect their surroundings, comprehend current events, and act appropriately, resulting in increased data transfers, as [1] points out.

Individuals have been adapting to the IoT ecosystem without realizing that all the data stored, transferred, and processed in the network are not primarily designed with security aspects [2]. Henceforth, this causes more security and privacy risks for the users of these devices, which is currently one of the significant challenges of the IoT, also allowing the ecosystem to be susceptible and prone to many threats and security attacks [3]. Additionally, IoT devices are frequently limited in computing power, energy, and memory capacity, and the prototypical Internet protocols and cryptography algorithms lack many of these resources, potentially making them inadmissible for IoT devices [4].

Several security properties and requirements may need to be satisfied in order to secure the IoT. These general security properties have also been classified into four categories: confidentiality, integrity, authentication, and authorization. Likewise, as mentioned in [5], the security properties that should be considered with the security protocols for IoT are described in the Table 1 as follows.

Table 1. Basic security properties for IoT.

Category	Security Properties
Confidentiality	Confidentiality permit information to be transferred securely during all means. Without authentication or encryptions, the transmitted messages between sensor nodes and the network can be tampered with by the adversaries.
Integrity	Integrity pledges that data received has not been manipulated throughout the transmission process. The addressee should detect any changes.
Authentication	Authentication refers to the verification processes of the exchanged messages whereby the receiver can verify the root of the messages.
Authorization	Authorization refers to the particular entities that have the authority to access the measured data. The authorized IoT devices should be able to access the network.

Developing a cryptographic algorithm is the utmost priority to retain a user's privacy in IoT's security issues, explicitly in authentication and data integrity. In order to encrypt the end-to-end messages, either asymmetric cryptography or symmetric cryptography will be implemented. Both techniques can be used to ensure data security in IoT. Recently, the refs. [6,7] independently investigated the symmetric encryption schemes to secure the IoT platform. By contrast, a few studies have been conducted involving asymmetric encryption schemes. The ref. [8] employed a keyword search using public-key encryption in a cloud environment, which focuses on cloud computing popularization, a diversified industry, and personal choices. In the same environment, the ref. [9] proposed a dynamical scheme based on an Efficient and non-shareable Public Key Exponent Secure Scheme (ENPKESS) via a non-linear Diophantine equation on cloud-based security. Besides, the ref. [10] implemented an equality test, which is significantly secure and indistinguishable against the random oracle of the specified model discussed in their studies. To another extent, the ref. [11] designed asymmetric cryptographic functions by employing the generative adversarial neural networks in IoT settings.

The necessity of keeping information private cannot be overstated, particularly in today's competitive environment, where eavesdroppers are ubiquitous in our communication channels. Thus, we are encouraged to utilise sophisticated encryption algorithms to protect our communication system's security. Until the 1970s, symmetrical methods for communication security were used, where the same key was utilised for both encryption and decryption. In 1978, Rivest, Shamir and Adleman (RSA) [12] had introduced the first workable asymmetric cryptosystem. In the RSA cryptosystem, two primes p and q of the same bit-size produces the modulus $N = pq$. At the same time, the public exponent, e is a positive integer relatively prime to a parameter $\phi(N) = (p-1)(q-1)$, and d is a private exponent used for decryption to satisfy the Diophantine equation $ed - \phi(N)k = 1$.

The use of the small private exponent d was an early idea in the RSA cryptosystem to lower the computing costs of decryption. Consequently, the total number of modular multiplications needed in the modular exponentiation and overall decryption costs is reduced. Even though RSA is still relatively secure when used with correct cryptographic techniques, the literature on its cryptanalysis is quite extensive. Since then, this system is undoubtedly the most researched topic in cryptology research. For instance, a classical result in [13] shows that if the decryption exponent d is less than $\frac{1}{3}N^{\frac{1}{4}}$, then using continued fractions, the RSA cryptosystem is insecure. Later, ref. [14] revised the bound to $d < N^{0.292}$ via Coppersmith's method [15] for finding small solutions of modular univariate polynomials. The ref. [16] later discovered that it is feasible to increase the bound of $d < \frac{1}{3}N^{\frac{1}{4}}$ to $d < \frac{1}{\sqrt[4]{18}}N^{\frac{1}{4}}$. The new bound is partially derived from the restriction that both primes p and q have the same bit length.

In recent years, many researchers have extended Wiener's and Boneh-Durfee's results. For instance, the ref. [17] presented the type of attacks zoomed into the RSA Diophantine equation in its original form of $ed - k\phi(N) = 1$, focusing on increasing the bound of d, which combines the continued fraction expansion. Instead of deriving an equation from the RSA key equation in its original, the ref. [18] utilized an arbitrary Diophantine equation in the form of $eX - uY = Z - \phi_b$. Furthermore, their proposed conditions upon parameters have no relation between the parameters X and Y and the parameters d and $\phi(N)$. As a result, their strategy enables factoring modulus $N = pq$ for a set of weak keys with $d \approx N$. The ref. [19] then revisited Wiener's continued fraction technique. Thus, a new attack against RSA is proposed. In contrast to the conclusion of [14] where $e \approx N$, their technique is well-suited to the circumstance when e is substantially less than N. Consequently, when the public key exponent is substantially less than the RSA modulus, the new attack in [19] surpasses the best current attack.

Many RSA variations have been proposed in parallel with these efforts to ensure computational performance while retaining acceptable security levels. There are respective variants of RSA that are established on the moduli, having the form $N = p^2q$. Such a modulus is widely employed in cryptography, as explained in [20], representing one of the most critical instances. One such prominent variant is proposed in [21], which applied the Hensel-lifting technique to verify a faster decryption algorithm compared to the original RSA decryption procedure. Other cryptosystems that also employed the modulus of the form $N = p^2q$ were designed in [22–24]. In comparison to the conventional RSA, their experiments were successful in demonstrating reduced computing costs.

Consequently, the security analysis of $N = p^2q$ becomes essential. For instance, the ref. [25] has proved that the cryptosystem that used $N = p^2q$ is vulnerable if coupled with a decryption exponent d, which is upper-bounded by $N^{0.395}$. Unlike [25], who solved $ex - Ny = 1$, the ref. [26] solved $ex - Ny = z$, which is a more generic equation. Their results increase the number of possible solutions to the problem. Intuitively, the technique in [26] appears to have a better probability of discovering solutions, that is, factoring the modulus N. Successful cryptanalysis for the modulus $N = p^2q$ that is linked to partial key exposure was published very recently in [27,28]. They employed Jochemsz and May's comprehensive approach [29], which is a highly successful methodology for finding small roots of integer polynomials and, as a result, factoring the modulus N. Despite the advantages of using the modulus $N = p^2q$, it is susceptible to attackers if the primes share some of their least significant bits (LSBs), as explained in [27], or if the primes and private keys share some of their most significant bits (MSBs), as described in [28].

To demonstrate that the class of keys is indeed weak, we must establish the existence of a probabilistic polynomial-time algorithm that accepts public parameters as input and returns the factors p and q. Thus, the procedure may be used to determine whether the key belongs to the relevant weak class. This trait may be advantageous when designing a cryptosystem's key generation procedure to avoid mistakenly creating a weak key. The suggested approach may be beneficial in designing a cryptosystem's key generation process to guarantee that no weak key is created accidentally.

Our contribution. In this paper, we introduce two interesting findings of cryptanalysis of moduli in the form $N = p^2q$. Firstly, we consider the solution on the public key pair (e, N) that is related via an arbitrary relation to equation $er - (Ns + t) = \alpha p^2 + \beta q^2$, where r, s, t are unknown parameters. We present a strategy by applying the continued fraction expansion to factor primes p and q, given public key pairs (e, N), which satisfy the following enabling conditions; $\gcd(r, s) = 1, |\alpha p^2 - \beta q^2| < N^{\frac{1}{2}}, r < \frac{N}{3(\alpha p^2 + \beta q^2)}$ and $|t| <$

$\frac{|\alpha p^2-\beta q^2|}{3(\alpha p^2+\beta q^2)}N^{\frac{1}{3}}$. Furthermore, we show that there exists a significant number of factorizable key pairs (e,N) that fall under our first cryptanalysis.

Secondly, we consider the security of k-users (i.e., multiple users) for $k \geq 2$, given the instances of (N_i,e_i) where $i = 1,\dots,k$. There are two distinct cases to be considered in the second cryptanalysis. Case number one is about solving k-instances (N_i,e_i) for fixed integer $r < N^{\delta_1}$, satisfying $e_i r - (N_i s_i + t_i) = \alpha p_i^2 + \beta q_i^2$, where the parameter δ_1 will be defined later. Similarly, on the case number two, the analysis worked on fixed integer $s < N^{\delta_2}$, satisfying $e_i r_i - (N_i s + t_i) = \alpha p_i^2 + \beta q_i^2$, where the parameter δ_2 will be defined later. In the second cryptanalysis, we convert the equations into a simultaneous Diophantine problem and use lattice basis reduction techniques to obtain parameters (r,s_i) or (s,r_i) in both situations. This gives us a good estimate of $\alpha p^2 + \beta q^2$, allowing us to calculate the prime factors p_i and q_i of each modulus N_i. We further show that, in both situations, the suggested approach allows one to factor k-moduli of the form $N_i = p_i^2 q_i$ at the same time.

Organization of the article. We begin with a brief review of the continuous fractions expansion, lattice basis reduction, and simultaneous Diophantine approximation techniques discussed in Section 2. Section 3 shows the results and details the discussion. The first cryptanalysis is presented in Section 3.1, together with the estimation of the number of weak exponents. Following that, Section 3.2 discusses the second cryptanalysis. The examples are presented to illustrate the achieved outcomes. Section 4 compares our findings against relevant and significant previous findings corresponding to their enabling conditions. Section 5 summarises our findings and suggests intriguing future work.

2. Mathematical Foundation

In this section, we give brief reviews on Legendre's theorem of continued fractions expansion and simultaneous Diophantine approximation via lattice reduction that will be used throughout this paper.

2.1. Continued Fraction Expansion

Let $\chi = [a_0, a_1, a_2, \dots]$ be the continued fraction expansion of χ. If χ is a rational number, then the process of listing the continued fractions expansion will finish in some finite index n (i.e., $\chi = [a_0, a_1, \dots, a_n]$). In recent years, there has been an increasing amount of work on using the continued fraction expansion, for instance, [17,30], as a tool for analysing the security of public key cryptosystems. An important result on continued fractions is due to the following theorem, widely known as Legendre's theorem.

Theorem 1 ([31]). *Suppose χ is a rational number. Let r and s be integers where $s \neq 0$ and $\gcd(r,s) = 1$, such that $\left|\chi - \frac{r}{s}\right| < \frac{1}{2s^2}$, then $\frac{r}{s}$ is a convergent of χ.*

2.2. Simultaneous Diophantine Approximations

Let $u_1, \dots, u_d$ be d linearly independent vectors of $\mathbb{R}^n$ with $d \leq n$. The set of all integer linear combinations of the vectors $u_1, \dots, u_d$ is called a lattice, and is in the form

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

The set $(u_1, \dots, u_d)$ is the basis of $\mathcal{L}$, and its dimension is d. The determinant of $\mathcal{L}$ is defined as $\det(\mathcal{L}) = \sqrt{\det(U^T U)}$, where U is the matrix of the u_i's in the canonical basis of $\mathbb{R}^n$. Define the Euclidean norm of a vector $v \in \mathcal{L}$ as $\|v\|$. Define the Euclidean norm of a vector $v \in \mathcal{L}$ as $\|v\|$. Finding a short non-zero vector in $\mathcal{L}$ is a crucial problem in lattice reduction. The LLL algorithm generates a reduced basis vector [32], and the following result fixes the reduced basis vector's sizes (see [20]).

Theorem 2 ([32])**.** *Let $\mathcal{L}$ be a lattice of dimension ω with a basis $\{v_1, \ldots, v_\omega\}$. The LLL algorithm produces a reduced basis $\{b_1, \ldots, b_\omega\}$ satisfying*

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

for all $1 \le i \le \omega$.

The simultaneous Diophantine approximations problem, which is stated as follows, is one of the most significant applications of the LLL algorithm. Let $\chi_1, \ldots, \chi_n$ be n real numbers, and ε a real number such that $0 < \varepsilon < 1$. Dirichlet's classical theorem states that integers exist $p_1, \ldots, p_n$, and a positive integer $q \le \varepsilon^{-n}$, such that $|q\chi_i - p_i| < \varepsilon$ for $1 \le i \le n$. The LLL algorithm described a method for finding simultaneous Diophantine approximations to rational numbers using a lattice with real number elements [32]. In [33] (Appendix A), a comparable solution for a lattice with integer elements is provided.

Theorem 3 ([33])**.** *There is a polynomial time algorithm for given rational numbers $\chi_1, \ldots, \chi_n$ and $0 < \varepsilon < 1$, to compute integers $p_1, \ldots, p_n$ and a positive integer q, such that*

$$\max_i |q\chi_i - p_i| < \varepsilon \text{ and } q \le 2^{\frac{n(n-3)}{4}} \cdot 3^n \cdot \varepsilon^{-n}.$$

3. Results and Discussion

In this section, we present our first cryptanalysis which focuses on a single public key pair (e, N), that is related via an arbitrary relation to equation $er - (Ns + t) = \alpha p^2 + \beta q^2$, where $N = p^2 q$ and r, s, t are unknown parameters.

3.1. The First Cryptanalysis

Suppose that for $N = p^2 q$ with $q < p < 2q$, then $\left(\frac{N}{2}\right)^{\frac{1}{3}} < q < N^{\frac{1}{3}} < p < (2N)^{\frac{1}{3}}$ holds [27], unless stated otherwise, and this relation defines the integer N throughout this work. Let $[x]$ be the integer that is closest to x. Let's start with the lemma below.

Lemma 1. *Let $|\alpha p^2 - \beta q^2| < N^{\frac{1}{2}}$ where α, β are suitable small integers with $\gcd(\alpha, \beta) = 1$. Let Δ be an approximation of $\alpha p^2 + \beta q^2$ such that $|\alpha p^2 + \beta q^2 - \Delta| < \frac{|\alpha p^2 - \beta q^2|}{3(\alpha p^2 + \beta q^2)} N^{\frac{1}{3}}$, then $\alpha\beta q = \left[\frac{\Delta^2}{4N}\right]$.*

Proof. Set $\Delta = \alpha p^2 + \beta q^2 + \nu$ with $|\nu| < \frac{|\alpha p^2 - \beta q^2|}{3(\alpha p^2 + \beta q^2)} N^{\frac{1}{3}}$. Consider the following equation.

$$\begin{aligned} \Delta^2 - 4\alpha\beta q N &= (\alpha p^2 + \beta q^2 + \nu)^2 - 4\alpha\beta q N \\ &= (\alpha p^2 + \beta q^2)^2 - 4\alpha\beta q N + 2\nu(\alpha p^2 + \beta q^2) + \nu^2. \end{aligned}$$

By using the identity $(\alpha p^2 - \beta q^2)^2 = (\alpha p^2 + \beta q^2)^2 - 4\alpha\beta q N$, we can rewrite the equation as

$$\Delta^2 - 4\alpha\beta q N = (\alpha p^2 - \beta q^2)^2 + 2|\nu|(\alpha p^2 + \beta q^2) + \nu^2.$$

Since $|\alpha p^2 - \beta q^2| < N^{\frac{1}{2}}$ and $|\nu| < \frac{|\alpha p^2 - \beta q^2|}{3(\alpha p^2 + \beta q^2)} N^{\frac{1}{3}} < N^{\frac{1}{3}}$, hence

$$\begin{aligned} |\Delta^2 - 4\alpha\beta q N| &< (N^{\frac{1}{2}})^2 + 2(\alpha p^2 + \beta q^2) \frac{|\alpha p^2 - \beta q^2|}{3(\alpha p^2 + \beta q^2)} N^{\frac{1}{3}} + (N^{\frac{1}{3}})^2 \\ &< 2N. \end{aligned}$$

Divide both sides by $4N$, hence $\left|\frac{\Delta^2}{4N} - \alpha\beta q\right| < \frac{1}{2}$. It follows that $\alpha\beta q = \left[\frac{\Delta^2}{4N}\right]$. □

Theorem 4. *Let $N = p^2q$ with $q < p < 2q$. Let α, β be suitably small integers, such that $|\alpha p^2 - \beta q^2| < N^{\frac{1}{2}}$. Let e satisfying the equation $er - (Ns + t) = \alpha p^2 + \beta q^2$ with $\gcd(r, s) = 1$. If $1 \leq s < r < \frac{N}{3(\alpha p^2+\beta q^2)}$ and $|t| < \frac{|\alpha p^2-\beta q^2|}{3(\alpha p^2+\beta q^2)} N^{\frac{1}{3}}$, then N can be factored in polynomial time.*

Proof. Suppose that a public key pair (e, N) satisfies an arbitrary equation

$$er - (Ns + t) = \alpha p^2 + \beta q^2 \tag{1}$$

with $\gcd(r, s) = 1$. Suppose $|t| < \frac{|\alpha p^2-\beta q^2|}{3(\alpha p^2+\beta q^2)} N^{\frac{1}{3}}$, thus, $|t| < N^{\frac{1}{3}}$. Rearrange (1) as $er - Ns = \alpha p^2 + \beta q^2 + t$, and dividing both sides by Nr, we have

$$\begin{aligned} \left| \frac{e}{N} - \frac{s}{r} \right| &= \left| \frac{\alpha p^2 + \beta q^2 + t}{Nr} \right| \\ &\leq \frac{|\alpha p^2 + \beta q^2| + |t|}{Nr} \\ &< \frac{|(\alpha p^2 + \beta q^2) + N^{\frac{1}{3}}|}{Nr}. \end{aligned}$$

If the condition $\frac{|(\alpha p^2+\beta q^2)+N^{\frac{1}{3}}|}{Nr} < \frac{1}{2r^2}$ holds, we can infer that $\frac{s}{r}$ is a convergent of the continuing fraction $\frac{e}{N}$ using Theorem 1. Observe that, this is equivalent to $r < \frac{N}{2(\alpha p^2+\beta q^2)+N^{\frac{1}{3}}}$. From Lemma 1, we have $\Delta = \alpha p^2 + \beta q^2 + \nu$ with $|\nu| < \frac{|\alpha p^2-\beta q^2|}{3(\alpha p^2+\beta q^2)} N^{\frac{1}{3}}$. This implies that

$$\begin{aligned} \alpha p^2 + \beta q^2 + \Delta &< 2(\alpha p^2 + \beta q^2) + \frac{|\alpha p^2 - \beta q^2|}{3(\alpha p^2 + \beta q^2)} N^{\frac{1}{3}} \\ &< 2(\alpha p^2 + \beta q^2) + N^{1/3} \\ &< 3(\alpha p^2 + \beta q^2). \end{aligned} \tag{2}$$

We can see from (2) that this requirement is satisfied for $r < \frac{N}{3(\alpha p^2+\beta q^2)}$. As a result, we may deduce that $\frac{s}{r}$ is a convergent of the continuing fraction $\frac{e}{N}$. Following that, we define $\Delta = er - Ns$. By Lemma 1, Δ is a satisfactory approximation of $\alpha p^2 + \beta q^2$, hence this implies that $\alpha\beta q = \left[\frac{\Delta^2}{4N} \right]$. It follows that $\gcd\left(\left[\frac{\Delta^2}{4N} \right], N \right) = q$, hence $p = \sqrt{\frac{N}{q}}$. □

3.1.1. The Uniqueness of Paramaters r, s, and t for Which the Theorem 4 Applies

Let's start with the following result. It proves that given fixed integers α and β, the public parameter $e < N$ satisfies, at most, one equation $er - (Ns + t) = \alpha p^2 + \beta q^2$, where the unknown parameters r, s and t satisfy the conditions of Theorem 4.

Proposition 1. *Let e satisfying $er_i - (Ns_i + t_i) = \alpha p^2 + \beta q^2$ with $e < N$ and $i = 1, 2$. Let $\gcd(r_i, s_i) = 1$, $r_i < \frac{N}{3(\alpha p^2+\beta q^2)}$ and $|t_i| < \frac{|\alpha p^2-\beta q^2|}{3(\alpha p^2+\beta q^2)} N^{\frac{1}{3}}$. Then $r_1 = r_2, s_1 = s_2$ and $t_1 = t_2$.*

Proof. Suppose that e satisfies two equations

$$\begin{aligned} er_1 - (Ns_1 + t_1) = \alpha p^2 + \beta q^2 \\ er_2 - (Ns_2 + t_2) = \alpha p^2 + \beta q^2 \end{aligned}$$

with $r_1, r_2 < \frac{N}{3(\alpha p^2+\beta q^2)}$ and $|t_1|, |t_2| < \frac{|\alpha p^2-\beta q^2|}{3(\alpha p^2+\beta q^2)} N^{\frac{1}{3}}$. Then, equating the e, we have

$$\frac{\alpha p^2 + \beta q^2 + t_1 + Ns_1}{r_1} = \frac{\alpha p^2 + \beta q^2 + t_2 + Ns_2}{r_2}. \tag{3}$$

We rearranged (3) to become

$$(\alpha p^2 + \beta q^2)(r_2 - r_1) + t_1 r_2 - t_2 r_1 = N(r_1 s_2 - r_2 s_1). \tag{4}$$

Consider the left-hand side of (4). Since $|\alpha p^2 - \beta q^2| < \alpha p^2 + \beta q^2$ and $\alpha p^2 + \beta q^2 > p^2 > N^{\frac{2}{3}}$, thus

$$\begin{aligned} |(\alpha p^2 + \beta q^2)(r_2 - r_1) + t_1 r_2 - t_2 r_1| &\le |\alpha p^2 + \beta q^2|(|r_2| + |r_1|) + |t_1 r_2| + |t_2 r_1| \\ &< \frac{2|\alpha p^2 + \beta q^2|N}{3(\alpha p^2 + \beta q^2)} + \frac{2|\alpha p^2 - \beta q^2|N^{\frac{4}{3}}}{(3(\alpha p^2 + \beta q^2))^2} \\ &< \frac{2N}{3} + \frac{2(\alpha p^2 + \beta q^2)N^{\frac{4}{3}}}{(3(\alpha p^2 + \beta q^2))^2} \\ &< \frac{2N}{3} + \frac{2N^{\frac{2}{3}}}{9} \\ &< N. \end{aligned}$$

We may conclude from the right-hand side of (4) that $r_1 s_2 - r_2 s_1 = 0$. Since $\gcd(r_1, s_1) = \gcd(r_2, s_2) = 1$, it shows that $r_1 = r_2$ and $s_1 = s_2$. As a result, $t_1 = t_2$ is obtained. □

3.1.2. Counting the Number of e's for Which the Theorem 4 Applies

The number of e's that fulfil the arbitrary equation $er - (Ns + t) = \alpha p^2 + \beta q^2$ is estimated in the following result.

Theorem 5. *Let e satisfy an arbitrary equation* $er - (Ns + t) = \alpha p^2 + \beta q^2$*, where* r, s *are integers satisfying* $1 \le s < r < \frac{|\alpha p^2 - \beta q^2|}{3(\alpha p^2 + \beta q^2)} N^{\frac{1}{3}}$ *with* $\gcd(r, s) = 1$*. Then, the number of the parameter e's is at least* $N^{\frac{2}{3} - \epsilon}$*, where* $\epsilon > 0$ *is suitably small for large N.*

Proof. Suppose r and s are two integers satisfying $1 \le s < r < \frac{|\alpha p^2 - \beta q^2|}{3(\alpha p^2 + \beta q^2)} N^{\frac{1}{3}}$ and $\gcd(r, s) = 1$. From $er - (Ns + t) = \alpha p^2 + \beta q^2$, we have $er \equiv Ns + t + \alpha p^2 + \beta q^2 \equiv 0 \pmod r$. Define $t \equiv -(Ns + \alpha p^2 + \beta q^2) \pmod r$ with $0 \le t < r$. Hence, there exists an integer t such that $e = \frac{Ns + t + \alpha p^2 + \beta q^2}{r}$ is also an integer. Let $t_0 = t + \alpha p^2 + \beta q^2$, thus $e = \frac{Ns + t_0}{r}$. The number of the parameter e's, denoted by $\#(e)$, satisfying the conditions given in Theorem 4 is

$$\#(e) = \sum_{r=1}^{\mathcal{T}} \sum_{\substack{s=1 \\ \gcd(r,s)=1}}^{r-1} 1 \tag{5}$$

where $\mathcal{T} = \frac{|\alpha p^2 - \beta q^2|}{3(\alpha p^2 + \beta q^2)} N^{\frac{1}{3}} \approx c_1 N^{\frac{1}{3}}$ for some positive constants c_1. Observe the following.

$$\sum_{\substack{s=1 \\ \gcd(r,s)=1}}^{r-1} 1 = \phi(r) > \frac{c_2 r}{\log\log r} > \frac{c_2 r}{\log\log N} \tag{6}$$

where c_2 is a constant (see [31], Theorem 328). Substitute (6) in (5), we obtain

$$\#(e) > \frac{c_2}{\log\log N} \sum_{r=1}^{\mathcal{T}} r. \tag{7}$$

Next, for $\sum_{r=1}^{\mathcal{T}} r$, we have

$$\sum_{r=1}^{\mathcal{T}} r = \frac{\mathcal{T}(\mathcal{T}+1)}{2} > \frac{\mathcal{T}^2}{2} = \frac{\left(c_1 N^{\frac{1}{3}}\right)^2}{2}. \tag{8}$$

Substitute (8) in (7), we obtain $\#(e) > \left(\frac{c_2}{\log\log N}\right)\frac{\left(c_1 N^{\frac{1}{3}}\right)^2}{2} > \frac{c_1^2 c_2}{2\log\log N} N^{\frac{2}{3}} = N^{\frac{2}{3}-\epsilon}$. Hence, a good approximation for $\#(e)$ is at least $N^{\frac{2}{3}-\epsilon}$, where $\epsilon > 0$ is arbitrarily small for suitably large N with $N^{-\epsilon} = \frac{c_1^2 c_2}{2\log\log N}$. □

3.1.3. Numerical Illustration of the First Cryptanalysis

Suppose we are given a public key pairs $(e, N) = (52{,}043{,}126{,}208{,}617,\ 64{,}533{,}181{,}881{,}083)$ and satisfy all the condition stated in Theorem 4. At first, we compute the continued fraction of $\frac{e}{N}$, and the list of the first convergents of the continued fraction expansion are

$$\left[0, 1, \frac{4}{5}, \frac{21}{26}, \frac{25}{31}, \frac{7046}{8737}, \frac{7071}{8768}, \frac{28{,}259}{35{,}041}, \frac{35{,}330}{43{,}809}, \dots\right].$$

Observe that we may omit the first and second convergents. Furthermore, the convergents $\frac{4}{5}$ and $\frac{21}{26}$ give $\gcd\left(\left[\frac{\Delta^2}{4N}\right], N\right) = 1$, respectively. We proceed with the next convergent $\frac{25}{31}$, then we compute $\Delta = er - Ns = 7{,}365{,}440{,}052$, hence $\left[\frac{\Delta^2}{4N}\right] = 210{,}162$. Finally, we compute $\gcd(210{,}162,\ 64{,}533{,}181{,}881{,}083) = 35{,}027$, which leads to the factorization of N (i.e., $q = 35{,}027$ and $p = \sqrt{\frac{N}{q}} = 42{,}923$).

The above illustration can also be viewed as the following algorithm.

Algorithm 1 Factoring public key pairs which satisfy Theorem 4.

```
Input: A public key pair $(e, N)$.
Output: The prime factors $p, q$.
1: Compute the continued fraction $\frac{e}{N}$.
2: For each convergent $\frac{r}{s}$ of $\frac{e}{N}$, compute $\Delta = er - Ns$.
3: Calculate $\left[\frac{\Delta^2}{4N}\right]$.
4: Compute $\gcd\left(\left[\frac{\Delta^2}{4N}\right], N\right) = x_1$.
5: If $1 < x_1 < N$, then compute $x_2 = \sqrt{\frac{N}{x_1}}$. Otherwise, repeat Step 2.
6: Return: $q = x_1$ and $p = x_2$.
```

3.2. *The Second Cryptanalysis*

In this section, we consider the security of k-users (i.e., multiple users) for $k \geq 2$, given the instances of (N_i, e_i) where $i = 1, \dots, k$. By using the lattice basis reduction algorithm for solving simultaneous Diophantine approximation, the k-instances of public key pairs (N_i, e_i) can be factored in polynomial time.

3.2.1. The Second Cryptanalysis: Case #1

Suppose that we are given k-instances (N_i, e_i) for fixed integer r, satisfying $e_i r - (N_i s_i + t_i) = \alpha p_i^2 + \beta q_i^2$. The following Theorem 6 proves that we are able to factor in such moduli if the unknown parameters r, s_i, and t_i satisfy the given conditions.

Theorem 6. *Let i be integers such that $i = 1, \dots, k$ for $k \geq 2$. Suppose e_i are k-public exponents and $N_i = p_i^2 q_i$ are k-moduli, each with the same bit-size N where $N = \min\{N_i\}$. Let α, β be suitably small integers with $\gcd(\alpha, \beta) = 1$ such that $\alpha p_i^2 + \beta q_i^2 < N^{\frac{2}{3}+\gamma}$ where $0 < \gamma < \frac{1}{3}$.*

Define $\delta_1 = (\frac{1}{3} - \gamma)k$. If there exists a fixed integer $r < N^{\delta_1}$, k-integers $s_i < N^{\delta_1}$ and $|t_i| < \frac{|\alpha p_i^2 - \beta q_i^2|}{3(\alpha p_i^2 + \beta q_i^2)} N^{\frac{1}{3}}$ satisfying the equation $e_i r - (N_i s_i + t_i) = \alpha p_i^2 + \beta q_i^2$, then k-moduli of the form $N_i = p_i^2 q_i$ can be factored in polynomial time.

Proof. Let $N = \min\{N_i\}$, $s_i < N^{\delta_1}$ and $|t_i| < \frac{|\alpha p_i^2 - \beta q_i^2|}{3(\alpha p_i^2 + \beta q_i^2)} N^{\frac{1}{3}}$, where $k \geq 2$ and $i = 1, \ldots, k$. Thus, $|t_i| < N^{\frac{1}{3}}$. Let $\alpha p_i^2 + \beta q_i^2 < N^{\frac{2}{3} + \gamma}$ with $0 < \gamma < \frac{1}{3}$. Consider the equation $e_i r - (N_i s_i + t_i) = \alpha p_i^2 + \beta q_i^2$. We rearranged the equation and divided by N_i for both sides, and obtained the following;

$$\begin{aligned} \left| \frac{e_i}{N_i} r - s_i \right| &= \frac{|\alpha p_i^2 + \beta q_i^2 + t_i|}{N_i} \\ &\leq \frac{|\alpha p_i^2 + \beta q_i^2 + t_i|}{N} \\ &< \frac{(N^{\frac{2}{3}+\gamma}) + N^{\frac{1}{3}}}{N} \\ &< \frac{2N^{\frac{2}{3}+\gamma}}{N} \\ &= 2N^{-\frac{1}{3}+\gamma}. \end{aligned}$$

To show the existence of integer r and s_i, let $\varepsilon = 2N^{-\frac{1}{3}+\gamma}$, $\delta_1 = \frac{k}{3} - \gamma k$. We have

$$N^{\delta_1} \cdot \varepsilon^k = 2^k N^{\delta 1 - \frac{k}{3} + k\gamma} = 2^k.$$

Since $2^k < 2^{\frac{k(k-3)}{4}} \cdot 3^k$ for $k \geq 2$, thus Theorem 3 gives $N^{\delta} \cdot \varepsilon^k < 2^{\frac{k(k-3)}{4}} \cdot 3^k$. It follows that if $r < N^{\delta}$, then $r < 2^{\frac{k(k-3)}{4}} \cdot 3^k \cdot \varepsilon^{-k}$. Hence, for $i = 1, \ldots, k$, we obtain $\left| \frac{e_i}{N_i} r - s_i \right| < \varepsilon$ and $r < 2^{\frac{k(k-3)}{4}} \cdot 3^k \cdot \varepsilon^{-k}$. If the requirements of Theorem 3 are fulfilled, we will be able to calculate r and s_i for $i = 1, \ldots, k$.

Next, observe the equation $e_i r - N_i s_i - (\alpha p_i^2 + \beta q_i^2) = t_i$. If $|t_i| < \frac{|\alpha p_i^2 - \beta q_i^2|}{3(\alpha p_i^2 + \beta q_i^2)} N^{\frac{1}{3}}$, then from Lemma 1 and Theorem 4, $\Delta_i = e_i r - N_i s_i$ is an approximation of $\alpha p_i^2 + \beta q_i^2$. Hence, this implies that $\alpha \beta q_i = \left[\frac{\Delta_i^2}{4N} \right]$ for $\Delta_i = e_i r - N_i s_i$. Finally, we compute $q_i = \gcd\left(\left[\frac{\Delta_i^2}{4N_i} \right], N_i \right)$. Therefore, k-moduli of the form $N_i = p_i^2 q_i$ can be factored in polynomial time. □

3.2.2. Numerical Illustration of the Second Cryptanalysis: Case #1

As an illustration of our second cryptanalysis for Case #1, suppose we consider three pairs of public keys, as follows.

$$\begin{aligned} (e_1, N_1) &= (29{,}255{,}562{,}123{,}506{,}221{,}224{,}250{,}868{,}221,\ 37{,}592{,}434{,}777{,}609{,}854{,}322{,}998{,}042{,}083), \\ (e_2, N_2) &= (31{,}666{,}949{,}665{,}785{,}721{,}076{,}995{,}001{,}363,\ 37{,}159{,}723{,}778{,}525{,}259{,}456{,}378{,}519{,}073), \\ (e_3, N_3) &= (31{,}035{,}716{,}184{,}317{,}012{,}442{,}375{,}761{,}677,\ 33{,}509{,}497{,}293{,}946{,}637{,}275{,}529{,}693{,}389). \end{aligned}$$

Observe that $N = \min(N_1, N_2, N_3) = 33{,}509{,}497{,}293{,}946{,}637{,}275{,}529{,}693{,}389$. Supposing $k = 3$ and $0 < \gamma < \frac{1}{3}$, we obtain $\delta_1 = \frac{k}{3} - \gamma k = \frac{1}{4}$ and $\varepsilon = 2N^{-\frac{1}{3}+\gamma} \approx 0.0083932985$. Suppose that we consider the parameter C as defined in [33], (Appendix A, page 196) using $n = m = 3$, hence we have

$$C = \left[3^{n+1} \cdot 2^{\frac{(n+1)(n-4)}{4}} \cdot \varepsilon^{-n-1} \right] = 8{,}160{,}642{,}349.$$

Suppose that the lattice $\mathcal{L}$ is spanned by the following matrix:

$$M = \begin{bmatrix} 1 & -\left[\frac{Ce_1}{N_1}\right] & -\left[\frac{Ce_2}{N_2}\right] & -\left[\frac{Ce_3}{N_3}\right] \\ 0 & C & 0 & 0 \\ 0 & 0 & C & 0 \\ 0 & 0 & 0 & C \end{bmatrix}.$$

After applying the LLL algorithm to $\mathcal{L}$, the following matrix is obtained as a reduced basis.

$$K = \begin{bmatrix} 13{,}521{,}818 & 140{,}673 & 7{,}755{,}891 & 7{,}168{,}491 \\ -13{,}012{,}033 & -19{,}197{,}443 & -1{,}873{,}112 & 13{,}025{,}663 \\ 3{,}675{,}331 & -9{,}727{,}267 & -34{,}041{,}935 & 13{,}188{,}947 \\ -16{,}634{,}061 & 23{,}434{,}710 & 4{,}721{,}887 & 19{,}989{,}237 \end{bmatrix}.$$

Now, computing $K \cdot M^{-1}$, we have

$$K \cdot M^{-1} = \begin{bmatrix} 3{,}521{,}818 & 10{,}523{,}085 & 11{,}523{,}087 & 12{,}523{,}593 \\ -13{,}012{,}033 & -10{,}126{,}355 & -11{,}088{,}656 & -12{,}051{,}442 \\ 3{,}675{,}331 & 2{,}860{,}253 & 3{,}132{,}061 & 3{,}404{,}006 \\ -16{,}634{,}061 & -12{,}945{,}126 & -14{,}175{,}293 & -15{,}406{,}080 \end{bmatrix}.$$

According to the first row of the above matrix, we obtain $r = 13{,}521{,}818$, $s_1 = 10{,}523{,}085$, $s_2 = 11{,}523{,}087$ and $s_3 = 12{,}523{,}593$. By applying r and s_i for $i = 1, 2, 3$, we define $\Delta_i = e_i r - N_i s_i$ as an approximation of $\alpha p_i^2 + \beta q_i^2$, respectively. Hence, by using Lemma 1 and Theorem 4, this implies that $\alpha\beta q_i = \left[\frac{\Delta_i^2}{4N}\right]$ for $\Delta_i = e_i r - N_i s_i$. Thus, we have the following;

$$\begin{aligned} \Delta_1 &= 51{,}383{,}531{,}574{,}753{,}359{,}723, \\ \Delta_2 &= 50{,}988{,}468{,}015{,}130{,}899{,}583, \\ \Delta_3 &= 47{,}592{,}177{,}797{,}589{,}142{,}109. \end{aligned}$$

Next, for each $i = 1, 2, 3$, we compute the following;

$$\left[\frac{\Delta_1^2}{4N_1}\right] = 17{,}558{,}501{,}682, \left[\frac{\Delta_2^2}{4N_2}\right] = 17{,}490{,}871{,}878, \left[\frac{\Delta_3^2}{4N_3}\right] = 16{,}898{,}309{,}214.$$

This leads us to the factorization of three RSA-Takagi moduli N_1, N_2 and N_3, where

$$p_1 = 3{,}584{,}116{,}567, \;\; p_2 = 3{,}570{,}311{,}711, \;\; p_3 = 3{,}449{,}355{,}491.$$

Hence, by using Lemma 1 and Theorem 4, for each $i = 1, 2, 3$, this implies that $\alpha\beta q_i = \left[\frac{\Delta_i^2}{4N}\right]$. Hence, $q_i = \gcd\left(\left[\frac{\Delta_i^2}{4N_i}\right], N_i\right)$ which we obtain $q_1 = 2{,}926{,}416{,}947, q_2 = 2{,}915{,}145{,}313, q_3 = 2{,}816{,}384{,}869$. This results in the factorization of three moduli N_1, N_2 and N_3 with $p_1 = 3{,}584{,}116{,}567, p_2 = 3{,}570{,}311{,}711, p_3 = 3{,}449{,}355{,}491$, respectively.

3.2.3. The Second Cryptanalysis: Case #2

In this section, we consider the Case #2 that is when k-moduli of the form $N_i = p_i^2 q_i$ satisfy k-equations of the form $e_i r_i - (N_i s + t_i) = \alpha p_i^2 + \beta q_i^2$, where the parameters r_i, s, and t_i are suitably small unknown parameters. This analysis is for the fixed value of s instead of fixed value of r from Case #1. Thus, the following theorem is looking for k-integers of r_i and an integer s.

Theorem 7. *Let i be integers such that $i = 1, \ldots, k$ for $k \geq 2$. Suppose e_i be k-public exponents with $\min\{e_i\} = N^\tau$ and $N_i = p_i^2 q_i$ be k-moduli, each with the same bit-size N, where $N = \max\{N_i\}$. Let α, β be suitably small integers with $\gcd(\alpha, \beta) = 1$ such that $\alpha p_i^2 + \beta q_i^2 < N^{\frac{2}{3}+\gamma}$ where $0 < \gamma < \frac{1}{3}$. Define $\delta_2 = (\tau - \gamma - \frac{2}{3})k$. If there exists a fixed integer $s < N^{\delta_2}$, k-integers*

$r_i < N^{\delta_2}$ and $|t_i| < \frac{|\alpha p_i^2 - \beta q_i^2|}{3(\alpha p_i^2 + \beta q_i^2)} N^{\frac{1}{3}}$ satisfy the equation $e_i r_i - (N_i s + t_i) = \alpha p_i^2 + \beta q_i^2$, then k-moduli of the form $N_i = p_i^2 q_i$ can be factored in polynomial time.

Proof. Let e_i be k-public exponents with $\min\{e_i\} = N^\tau$ and $N = \max\{N_i\}$ where $i = 1, \ldots, k$ for $k \geq 2$. Let $\alpha p_i^2 + \beta q_i^2 < N^{\frac{2}{3}+\gamma}$, where $0 < \gamma < \frac{1}{3}$. Suppose that $s < N^{\delta_2}$, where $\delta_2 = (\tau - \gamma - \frac{2}{3})k$. Observe that $|t_i| < \frac{|\alpha p_i^2 - \beta q_i^2|}{3(\alpha p_i^2 + \beta q_i^2)} N^{\frac{1}{3}} < N^{\frac{1}{3}}$. Consider the equation $e_i r_i - (N_i s + t_i) = \alpha p_i^2 + \beta q_i^2$. Rearranging the equation and dividing by e_i for both sides, we have the following:

$$\begin{aligned} \left| \frac{N_i}{e_i} s - r_i \right| &= \frac{|\alpha p_i^2 + \beta q_i^2 + t_i|}{e_i} \\ &\leq \frac{\alpha p_i^2 + \beta q_i^2 + |t_i|}{N^\tau} \\ &< \frac{N^{\frac{2}{3}+\gamma} + N^{\frac{1}{3}}}{N^\tau} \\ &< \frac{2N^{\frac{2}{3}+\gamma}}{N^\tau} \\ &= 2N^{\frac{2}{3}+\gamma-\tau}. \end{aligned}$$

We now continue to demonstrate the existence of integers r_i and s. Let $\varepsilon = 2N^{\frac{2}{3}+\gamma-\tau}$ and $\delta_2 = (\tau - \gamma - \frac{2}{3})k$. Then, we obtain

$$N^{\delta_2} \cdot \varepsilon^k = N^{\delta_2}(2N^{\frac{2}{3}+\gamma-\tau})^k = 2^k(N^{\delta_2 + (\frac{2}{3}+\gamma-\tau)k}) = 2^k.$$

Since $2^k < 2^{\frac{k(k-3)}{4}} \cdot 3^k$ for $k \geq 2$, therefore, Theorem 3 gives $N^\delta \cdot \varepsilon^k < 2^{\frac{k(k-3)}{4}} \cdot 3^k$. It follows that if $s < N^{\delta_2}$, then $s < 2^{\frac{k(k-3)}{4}} \cdot 3^k \cdot \varepsilon^{-k}$. Next, for $i = 1, \ldots, k$, we have $\left| \frac{N_i}{e_i} s - r_i \right| < \varepsilon$ and $s < 2^{\frac{k(k-3)}{4}} \cdot 3^k \cdot \varepsilon^{-k}$. If the conditions of Theorem 3 are fulfilled, we will find s and r_i. Next, by rearranging the equation $e_i r_i - (N_i s + t_i) = \alpha p_i^2 + \beta q_i^2$, observe the following equation;

$$e_i r_i - N_i s - (\alpha p_i^2 + \beta q_i^2) = t_i.$$

Since $|t_i| < \frac{|\alpha p_i^2 - \beta q_i^2|}{3(\alpha p_i^2 + \beta q_i^2)} N^{\frac{1}{3}}$, hence, using Lemma 1 and Theorem 4 confirms that such $\Delta_i = e_i r_i - N_i s$ is an approximation of $\alpha p_i^2 + \beta q_i^2$, which implies that $\left\lceil \frac{\Delta_i^2}{4N} \right\rceil = \alpha \beta q_i$. Finally, we compute $q_i = \gcd\left(\left\lceil \frac{\Delta_i^2}{4N_i} \right\rceil, N_i \right)$. Therefore, k-moduli of the form $N_i = p_i^2 q_i$ can be factored in. □

3.2.4. Numerical Illustration of the Second Cryptanalysis: Case #2

It should be noted that the numerical illustration can be accomplished in a similar manner and with a slight adjustment with the Case #1. We consider three moduli and three public exponents to show our second cryptanalysis for Case #2 as follows.

$$\begin{aligned} (e_1, N_1) &= (32{,}951{,}266{,}308{,}456{,}173{,}805{,}039{,}470{,}651,\ 41{,}828{,}330{,}615{,}126{,}280{,}338{,}151{,}779{,}539), \\ (e_2, N_2) &= (44{,}947{,}125{,}051{,}796{,}195{,}048{,}817{,}663{,}864,\ 51{,}165{,}390{,}796{,}774{,}300{,}447{,}936{,}871{,}731), \\ (e_3, N_3) &= (28{,}130{,}995{,}660{,}813{,}675{,}001{,}279{,}183{,}769,\ 33{,}865{,}943{,}931{,}730{,}327{,}074{,}467{,}227{,}163). \end{aligned}$$

Observe that $N = \max\{N_1, N_2, N_3\} = 51{,}165{,}390{,}796{,}774{,}300{,}447{,}936{,}871{,}731$. We also obtain $\min\{e_1, e_2, e_3\} = N^\tau$ with $\tau \approx 0.9909508724$. Let $k = 3$ and $0 < \gamma < \frac{1}{3}$, therefore $\delta_2 = (\tau - \gamma - \frac{2}{3})k = 0.222852617$ and $\varepsilon = 2N^{\frac{2}{3}+\gamma-\tau} \approx 0.014736912$. Consider the parameter C as defined in [33] (Appendix A, page 196) using $n = m = 3$; hence, we obtain

$$C = \left[3^{n+1} \cdot 2^{\frac{(n+1)(n-4)}{4}} \cdot \varepsilon^{-n-1}\right] = 858{,}675{,}450.$$

Suppose that the lattice $\mathcal{L}$ is spanned by the following matrix:

$$M = \begin{bmatrix} 1 & -\left[\frac{CN_1}{e_1}\right] & -\left[\frac{CN_2}{e_2}\right] & -\left[\frac{CN_3}{e_3}\right] \\ 0 & C & 0 & 0 \\ 0 & 0 & C & 0 \\ 0 & 0 & 0 & C \end{bmatrix}.$$

After applying the LLL algorithm to $\mathcal{L}$, the following matrix is obtained as a reduced basis.

$$K = \begin{bmatrix} -1{,}526{,}872 & -106{,}014 & -1{,}217{,}082 & -1{,}225{,}226 \\ -1{,}318{,}171 & -5{,}327{,}802 & 140{,}949 & -41{,}543 \\ -2{,}844{,}631 & 822{,}078 & 82{,}689 & 4{,}989{,}427 \\ -2{,}916{,}075 & -233{,}400 & 7{,}550{,}325 & -4{,}455{,}075 \end{bmatrix}.$$

Now, computing $K \cdot M^{-1}$, we have

$$K \cdot M^{-1} = \begin{bmatrix} -1{,}526{,}872 & -1{,}938{,}211 & -1{,}738{,}109 & -1{,}838{,}149 \\ -1{,}318{,}171 & -1{,}673{,}286 & -1{,}500{,}535 & -1{,}586{,}901 \\ -2{,}844{,}631 & -3{,}610{,}974 & -3{,}238{,}175 & -3{,}424{,}554 \\ -2{,}916{,}075 & -3{,}701{,}665 & -3{,}319{,}503 & -3{,}510{,}563 \end{bmatrix}.$$

We derive $s = 1{,}526{,}872$, $r_1 = 1{,}938{,}211$, $r_2 = 1{,}738{,}109$ and $r_3 = 1{,}838{,}149$ from the first row of the aforementioned matrix. By applying s and r_i for $i = 1,2,3$, we look at the relation $\Delta_i = e_i r_i - N_i s$ as an approximation of $\alpha p_i^2 + \beta q_i^2$, respectively. Thus, we have the following;

$$\begin{aligned} \Delta_1 &= 55{,}174{,}364{,}873{,}521{,}673{,}353, \\ \Delta_2 &= 63{,}106{,}563{,}153{,}707{,}337{,}744, \\ \Delta_3 &= 47{,}929{,}080{,}406{,}292{,}979{,}445. \end{aligned}$$

Hence, by using Lemma 1 and Theorem 4, for each $i = 1,2,3$, this implies that $\alpha\beta q_i = \left[\frac{\Delta_i^2}{4N}\right]$. Hence, $q_i = \gcd\left(\left[\frac{\Delta_i^2}{4N_i}\right], N_i\right)$ which we obtain $q_1 = 3{,}032{,}444{,}851, q_2 = 3{,}243{,}108{,}811, q_3 = 2{,}826{,}335{,}843$. This results in the factorization of three moduli N_1, N_2 and N_3 with $p_1 = 3{,}713{,}973{,}583$, $p_2 = 3{,}971{,}983{,}061$, $p_3 = 3{,}461{,}542{,}829$, respectively.

4. Comparative Analysis

In this section, we compare our findings against previous findings of security analysis related to $N = p^2 q$ concerning the form of the modified key equations and their conditions. The comparisons are illustrated in Table 2.

From Table 2, based on the references given (i.e., [25–27,34,35], we can view that all earlier first five findings are a type of cryptanalysis as a zoomed-in generalized Diophantine equation in the form $eX - NY = Z$ for suitable integers X, Y, Z. The first five findings had to dictate conditions upon the key pairs (e, N) and its corresponding generalized parameters. All of the mentioned attacks usually combine the continued fraction method, the lattice reduction technique such as the Coppersmith's method [15] or utilize Jochemsz and May's strategy [29] to formulate a new strategy in factoring N.

Table 2. Comparison of Our Results Against Previous Findings.

Reference	Utilized Key Equations	Enabling Conditions
[25]	$ex-(N-(p^2-pq-p))y=1$	$x=N^{\delta}$, $y^2z=N$
[26]	$ex-(N-(p^2-pq-p))y=z$	$\lvert x\rvert<N^{\delta}$, $z<N^{\gamma}$ $\lvert xz\rvert<N^{\delta+\gamma}\approx N^{0.22}$
[27]	$ed-k(N-(p^2+pq-p))=1$	$p-q=2^b\approx N^{\alpha}$, $e\approx N^{\gamma}$, $d<N^{\delta}$, $\delta<\frac{11}{9}-\frac{2}{9}\sqrt{4+18\gamma}$
[34]	$ex-(N-(ap^2+bq^2))y=z$	$1\leq y\leq x<\frac{1}{2}N^{\frac{1}{6}-\frac{\alpha}{2}}$, $\lvert z\rvert<\frac{1}{3}N^{1/3+\alpha}y$
[35]	$ex-Ny=(ap^2+bq^2)z$	$1\leq y<x<\frac{N}{2\lvert z\rvert(ap^2+bq^2)}$, $\lvert z\rvert<\frac{\sqrt{2}N^{1/2}}{\lvert ap^2-bq^2\rvert}$
Our result: Theorem 4	$er-(Ns+t)=\alpha p^2+\beta q^2$	$1\leq s<r<\frac{N}{3(\alpha p^2+\beta q^2)}$, $\lvert t\rvert<\frac{\lvert\alpha p^2-\beta q^2\rvert}{3(\alpha p^2+\beta q^2)}N^{\frac{1}{3}}$
Our result: Theorem 6	$e_ir-(N_is_i+t_i)=\alpha p_i^2+\beta q_i^2$	$r,s_i<N^{\delta_1}$, $\lvert t_i\rvert<\frac{\lvert\alpha p_i^2-\beta q_i^2\rvert}{3(\alpha p_i^2+\beta q_i^2)}N^{\frac{1}{3}}$, $\alpha p_i^2+\beta q_i^2<N^{\frac{2}{3}+\gamma}$, $0<\gamma<\frac{1}{3}$, $\delta_1=\frac{k}{3}-\gamma k$, $N=\min\{N_i\}$.
Our result: Theorem 7	$e_ir_i-(N_is+t_i)=\alpha p_i^2+\beta q_i^2$	$r_i,s<N^{\delta_2}$, $\lvert t_i\rvert<\frac{\lvert\alpha p_i^2-\beta q_i^2\rvert}{3(\alpha p_i^2+\beta q_i^2)}N^{\frac{1}{3}}$, $\alpha p_i^2+\beta q_i^2<N^{\frac{2}{3}+\gamma}$, $0<\gamma<\frac{1}{3}$, $\min\{e_i\}=N^{\tau}$, $\delta_2=(\tau-\gamma-\frac{2}{3})k$, $N=\max\{N_i\}$.

The above collection depicts the progress of cryptanalysis efforts over some time. To continue the research, there might be more generalization key equations that can be provided to emphasize the technique to factor $N=p^2q$ in polynomial time. Hence, this paper presents two new cryptanalyses that depend on an arbitrary Diophantine key equation, which differ from earlier studies.

There are two different results of cryptanalysis of the modulus in the form $N=p^2q$ presented in this paper, which is briefly summarized in Table 2. As a consequence, our strategy enables us to factor $N=p^2q$ for a collection of weak keys with requirements as specified in Theorems 4, 6 and 7, respectively. Thus, our results are novel and essential. The conditions upon our parameters cannot be compared to conditions upon parameters of earlier results. It is due to the proposed results in another addition to the not-to-do list during the key generation process to guarantee that the crypto-designers or implementors do not unawarely construct a weak key.

5. Conclusions and Future Work

The modulus of type $N = p^2 q$ is often used in many variants of factoring-based public-key encryption due to its ability to fasten the decryption process. Faster decryption is very suitable for securing small devices in the IoT environment or securing fast-forwarding encryption services used in mobile applications. Taking this into account, the security of those devices is paramount. Finally, two new cryptanalyses of the modulus $N = p^2 q$ were presented. This study focused on two cryptanalyses that use new enabling conditions to factor the modulus $N = p^2 q$ of the factoring-based cryptosystem. The first cryptanalysis considered a single user with a public key pair (e, N) related via an arbitrary relation to equation $er - (Ns + t) = \alpha p^2 + \beta q^2$, where r, s, t are unknown parameters. The second cryptanalysis considered two distinct cases in the situation of k-users (i.e., multiple users) for $k \geq 2$, given the instances of (N_i, e_i) where $i = 1, \ldots, k$. By using the lattice basis reduction algorithm for solving simultaneous Diophantine approximation, the k-instances of (N_i, e_i) can be successfully factored in polynomial time.

It was proven that a probabilistic polynomial-time algorithm exists that takes public parameters as an input and returns the factors p and q. Hence, we executed the procedure to see if the key belonged to the weak class. The proposed results may be helpful during key generation to avoid creating a weak key by accident. This study revealed specific flaws in the relaxed model using faulty public variables and limited parameter selection. These flaws do not compromise the factoring-based cryptosystem's security. Nevertheless, our findings can help uncover possible flaws and better understand the underlying mathematics and parameter choices.

Future work. Given the resource constraints associated with various IoT devices, cryptographic solutions in this environment must be resilient while remaining practical, posing a challenge for security analysts and crypto designers. Therefore, other generalization key equations can be presented in the future to demonstrate how to recover the prime factors p and q in polynomial time. It would be splendid if a small private exponent could reduce the encryption and decryption time. Under partial key exposure attacks, future researchers can analyze the RSA variant's security when the prime factor p and q share many LSBs or MSBs. There are other schemes that one might be interested in by using a small private exponent that can be employed to recover the prime factor p and q in polynomial time, such as [27,28].

Author Contributions: Formal analysis, M.A.A., N.N.A.R. and M.R.K.A.; Funding acquisition, M.A.A.; Investigation, M.A.A. and N.N.A.R.; Project administration, M.R.K.A.; Validation, M.A.A., N.N.A.R. and M.R.K.A.; Writing—original draft, M.A.A. and N.N.A.R.; Writing—review and editing, M.A.A., N.N.A.R., M.R.K.A. and N.R.S. All authors have read and agreed to the published version of the manuscript.

Funding: Universiti Putra Malaysia partially supported the present research under PutraGrant—GP/2017/9552200.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations and Mathematical Symbols

The following abbreviations and mathematical symbols are used in this manuscript:

ENPKESS	Efficient and non-shareable Public Key Exponent Secure Scheme
IoT	Internet of Things
LLL	Lenstra-Lenstra-Lovasz
LSBs	least significant bits
MSBs	most significant bits

RFID	Radio-frequency Identification
RSA	Rivest-Shamir-Adleman
p, q	Prime Numbers
$\mathbb{Z}$	Set of Integers
$\mathbb{R}$	Set of Real Numbers
$\mathbb{N}$	Set of Natural Numbers
χ	Set of Rational Numbers
$\approx$	Approximation
$<$	Less than
$>$	Greater than
$\leq$	Less than and equal to
$\geq$	Greater than and equal to
$\sum$	Summation
$\lvert \ldots \rvert$	Absolute value (modulus) of
$\lVert \ldots \rVert$	Norm
min	Minimum
max	Maximum
mod	Modulo
$f(x)$	Polynomials with One-Variable
gcd	Greatest Common Divisor
det	Determinant

References

1. Hossain, M.M.; Fotouhi, M.; Hasan, R. Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things. In Proceedings of the 2015 IEEE World Congress on Services—SERVICES 2015, New York, NY, USA, 27 June–2 July 2015; Zhang, L., Bahsoon, R., Eds.; pp. 21–28. [CrossRef]
2. Chatzigiannakis, I.; Vitaletti, A.; Pyrgelis, A. A Privacy-preserving Smart Parking System using an IoT Elliptic Curve Based Security Platform. *Comput. Commun.* **2016**, *89*, 165–177. [CrossRef]
3. Jing, Q.; Vasilakos, A.V.; Wan, J.; Lu, J.; Qiu, D. Security of the Internet of Things: Perspectives and Challenges. *Wirel. Netw.* **2014**, *20*, 2481–2501. [CrossRef]
4. Samaila, M.; Neto, M.; Fernandes, D.; Freire, M.; Inácio, P. Challenges of Securing Internet of Things Devices: A survey. *Secur. Priv.* **2018**, *1*, e20. [CrossRef]
5. Nguyen, K.T.; Laurent, M.; Oualha, N. Survey on Secure Communication Protocols for The Internet of Things. *Ad Hoc Netw.* **2015**, *32*, 17–31. [CrossRef]
6. Saraiva, D.A.; Leithardt, V.R.Q.; de Paula, D.; Sales Mendes, A.; González, G.V.; Crocker, P. Prisec: Comparison of Symmetric Key Algorithms for IoT Devices. *Sensors* **2019**, *19*, 4312. [CrossRef]
7. Prathiba, A.; Bhaaskaran, V.K. Hardware Footprints of S-box in Lightweight Symmetric Block Ciphers for IoT and CPS Information Security Systems. *Integration* **2019**, *69*, 266–278. [CrossRef]
8. Zhou, Y.; Li, N.; Tian, Y.; An, D.; Wang, L. Public Key Encryption with Keyword Search in Cloud: A Survey. *Entropy* **2020**, *22*, 421. [CrossRef]
9. Thirumalai, C.; Mohan, S.; Srivastava, G. An Efficient Public Key Secure Scheme for Cloud and IoT Security. *Comput. Commun.* **2020**, *150*, 634–643. [CrossRef]
10. Deverajan, G.G.; Muthukumaran, V.; Hsu, C.H.; Karuppiah, M.; Chung, Y.C.; Chen, Y.H. Public key encryption with equality test for Industrial Internet of Things system in cloud computing. *Trans. Emerg. Telecommun. Technol.* **2021**, e4202. [CrossRef]
11. Hao, X.; Ren, W.; Xiong, R.; Zhu, T.; Choo, K.K.R. Asymmetric Cryptographic Functions Based on Generative Adversarial Neural Networks for Internet of Things. *Future Gener. Comput. Syst.* **2021**, *24*, 243–253. [CrossRef]
12. Rivest, R.L.; Shamir, A.; Adleman, L. A Method for Obtaining Digital Signatures and Public-key Cryptosystems. *Commun. ACM* **1978**, *21*, 120–126. [CrossRef]
13. Wiener, M.J. Cryptanalysis of Short RSA Secret Exponents. *IEEE Trans. Inf. Theory* **1990**, *36*, 553–558. [CrossRef]
14. Boneh, D.; Durfee, G. Cryptanalysis of RSA with Private Key d Less Than $N^{0.292}$. *IEEE Trans. Inf. Theory* **2000**, *46*, 1339–1349. [CrossRef]
15. Coppersmith, D. Small Solutions to Polynomial Equations, and Low Exponent RSA Vulnerabilities. *J. Cryptol.* **1997**, *10*, 233–260. [CrossRef]
16. Susilo, W.; Tonien, J.; Yang, G. A Generalised Bound for The Wiener Attack on RSA. *J. Inf. Secur. Appl.* **2020**, *53*, 102531. [CrossRef]
17. Ariffin, M.R.K.; Abubakar, S.I.; Yunos, F.; Asbullah, M.A. New Cryptanalytic Attack on RSA Modulus $N = pq$ using Small Prime Difference Method. *Cryptography* **2019**, *3*, 2. [CrossRef]
18. Ghafar, A.H.A.; Ariffin, M.R.K.; Md Yasin, S.; Sapar, S.H. Partial Key Attack Given MSBs of CRT-RSA Private Keys. *Mathematics* **2020**, *8*, 2188. [CrossRef]

19. Susilo, W.; Tonien, J.; Yang, G. Divide and Capture: An Improved Cryptanalysis of the Encryption Standard Algorithm RSA. *Comput. Stand. Interfaces* **2021**, *74*, 103470. [CrossRef]
20. May, A. Secret Exponent Attacks on RSA-type Schemes with Moduli $N = p^r q$. In *Public Key Cryptography—PKC 2004, Proceedings of the 7th International Workshop on Public Key Cryptography, Singapore, 1–4 March 2004*; Bao, F., Deng, R., Zhou, J. Eds.; Springer: Berlin/Heidelberg, Germany, 2004; pp. 218–230. [CrossRef]
21. Takagi, T. Fast RSA-type Cryptosystem Modulo $p^k q$. In *Advances in Cryptology—CRYPTO '98, Procedings of the 28th Annual International Cryptology Conference—CRYPTO 1998, Santa Barbara, CA, USA, 23–27 August 1998*; Krawczyk, H., Ed.; Springer: Berlin/Heidelberg, Germany, 1998; pp. 318–326. [CrossRef]
22. Batten, L.M.; Williams, H.C. *Unique Rabin-Williams Signature Scheme Decryption*; Cryptology ePrint Archive, Report 2019/915; International Association for Cryptologic Research: Nevada, CA, USA, 2019; p. 915. [CrossRef]
23. Mooney, D.; Batten, L.M.; Zhang, L.Y. A New Rabin-type Cryptosystem with Modulus $p^2 q$. In Proceedings of the 11th International Conference on Applications and Techniques in Information Security—ATIS 2020, Brisbane, QLD, Australia, 12–13 November 2020; Batina, L., Li, G., Eds.; Springer: Singapore, 2020; pp. 61–77. [CrossRef]
24. Nishioka, M.; Satoh, H.; Sakurai, K. Design and Analysis of Fast Provably Secure Public-key Cryptosystems based on A Modular Squaring. In Proceedings of the 4th International Conference on Information Security and Cryptology—ICISC 2001, Seoul, Korea, 6–7 December 2001; Kim, K., Ed.; Springer: Berlin/Heidelberg, Germany, 2001; pp. 81–102. [CrossRef]
25. Sarkar, S. Small Secret Exponent Attack on RSA Variant with Modulus $N = p^r q$. *Des. Codes Cryptogr.* **2014**, *73*, 383–392. [CrossRef]
26. Nitaj, A.; Rachidi, T. New Attacks on RSA with Moduli $N = p^r q$. In Proceedings of the First International Conference on Codes, Cryptology, and Information Security—C2SI 2015, Rabat, Morocco, 26–28 May 2015; El Hajji, S., Nitaj, A., Carlet, C., Souidi, E., Eds.; Springer: Cham, Switzerland, 2015; pp. 352–360. [CrossRef]
27. Adenan, N.N.H.; Ariffin, M.R.K.; Yunos, F.; Sapar, S.H.; Asbullah, M.A. Analytical Cryptanalysis upon $N = p^2 q$ utilizing Jochemsz-May Strategy. *PLoS ONE* **2021**, *16*, e0248888. [CrossRef]
28. Adenan, N.N.H.; Ariffin, M.R.K.; Sapar, S.H.; Ghafar, A.H.A.; Asbullah, M.A. New Jochemsz–May Cryptanalytic Bound for RSA System utilizing Common Modulus $N = p^2 q$. *Mathematics* **2021**, *9*, 340. [CrossRef]
29. Jochemsz, E.; May, A. A strategy for finding roots of multivariate polynomials with new applications in attacking RSA variants. In *Advances in Cryptology—ASIACRYPT 2006, Proceedings of the 12th International Conference on the Theory and Application of Cryptology and Information Security—ASIACRYPT 2006, Shanghai, China, 3–7 December 2006*; Lai, X., Chen, K., Eds.; Springer: Berlin/Heidelberg, Germany, 2006; pp. 267–282. [CrossRef]
30. Wu, M.E.; Tso, R.; Sun, H.M. On the Improvement of Fermat Factorization using a Continued Fraction Technique. *Future Gener. Comput. Syst.* **2014**, *30*, 162–168. [CrossRef]
31. Hardy, G.H.; Wright, E.M. *An Introduction to the Theory Numbers*, 5th ed.; The Clarendon Press; Oxford University Press: New York, NY, USA, 1979; ISBN 978-0-19-853171-5.
32. Lenstra, A.K.; Lenstra, H.W.; Lovász, L. Factoring polynomials with rational coefficients. *Math. Ann.* **1982**, *261*, 515–534. [CrossRef]
33. Nitaj, A.; Ariffin, M.R.K.; Nassr, D.I.; Bahig, H.M. New attacks on the RSA cryptosystem. In Proceedings of the 7th International Conference on Cryptology in Africa—AFRICACRYPT 2014, Marrakesh, Morocco, 28–30 May 2014; Pointcheval, D., Vergnaud, D., Eds.; Springer: Cham, Switzerland, 2014; pp. 178–198. [CrossRef]
34. Asbullah, M.A.; Ariffin, M.R.K. New Attacks on RSA with Modulus $N = p^2 q$ using Continued Fractions. *J. Phys. Conf. Ser.* **2015**, *622*, 012019. [CrossRef]
35. Rahman, N.N.A.; Ariffin, M.R.K.; Asbullah, M.A. Successful Cryptanalysis upon a Generalized RSA Key Equation. *ASM Sci. J.* **2019**, *12*, 191–202.