cryptography

MDPI

Article

Partial Exposure Attacks Against a Family of RSA-like Cryptosystems

George Teşeleanu [1,2]

[1] Advanced Technologies Institute, 10 Dinu Vintilă, 021101 Bucharest, Romania; george.teseleanu@yahoo.com
[2] Simion Stoilow Institute of Mathematics of the Romanian Academy, 21 Calea Grivitei, 010702 Bucharest, Romania

Abstract: An RSA generalization using complex integers was introduced by Elkamchouchi, Elshenawy and Shaban in 2002. This scheme was further extended by Cotan and Teșeleanu to Galois fields of order $n \geq 1$. In this generalized framework, the key equation is $ed - k(p^n - 1)(q^n - 1) = 1$, where p and q are prime numbers. Note that the classical RSA and Elkamchouchi et al.'s key equations are special cases, namely, when $n = 1$ and $n = 2$. In addition to introducing this generic family, Cotan and Teșeleanu described a continued fractions attack capable of recovering the secret key d if $d < N^{0.25n}$. This bound was later improved by Teșeleanu using a lattice-based method. In this paper, we explore other lattice attacks that could lead to factoring the modulus $N = pq$, namely, we propose a series of partial exposure attacks that can aid an adversary in breaking this family of cryptosystems if certain conditions hold.

Keywords: lattice attack; partial exposure attacks; RSA

1. Introduction

The RSA, one of the most widely used cryptosystems, was introduced by Rivest, Shamir and Adleman in their 1978 paper [1]. The classical RSA scheme works using elements from the group $\mathbb{Z}_N^*$, where N is the product of two large prime numbers p and q. More precisely, to encrypt an element $m \in \mathbb{Z}_N^*$, we have to compute the ciphertext $c \equiv m^e \bmod N$, where e satisfies $\gcd(e, \varphi(N)) = 1$ and $\varphi(N) = (p-1)(q-1)$. To recover the original element, we simply compute $m \equiv c^d \bmod N$, where $d \equiv e^{-1} \bmod \varphi(N)$. The user's public key is (N, e), while (p, q, d) constitutes its secret key. In this paper, we focus only on primes that satisfy $q < p < 2q$ (i.e., have the same bit size), further referred to as balanced primes.

Over time, various attacks were developed to extract the secret key d from the public key (N, e) under certain conditions. Wiener proved in [2] that if $d < N^{0.25}/3$, the secret key d can be recovered from the continued fraction expansion of e/N, hence enabling the factorization of N. Boneh and Durfee [3] improved this bound to $d < N^{0.292}$ using Coppersmith's method [4] and lattice-reduction techniques [5]. Herrmann and May [6] later achieved the same bound with simpler methods. For an overview of RSA attacks, see [7–9].

Elkamchouchi, Elshenawy and Shaban [10] extended the RSA scheme to the ring of Gaussian integers modulo N. Such an integer modulo N has the form $a + bi$, where $a, b \in \mathbb{Z}_N$ and $i^2 = -1$. The set of all Gaussian integers modulo N is denoted by $\mathbb{Z}_N[i]$, and its group order is $\phi(N) = (p^2 - 1)(q^2 - 1)$. In this case, the encryption exponent e satisfies $\gcd(e, \phi(N)) = 1$, and the decryption exponent d is computed using $d \equiv e^{-1} \bmod \phi(N)$.

Academic Editor: Josef Pieprzyk

Received: 22 November 2024
Revised: 23 December 2024
Accepted: 26 December 2024
Published: 28 December 2024

Citation: Teşeleanu, G. Partial Exposure Attacks Against a Family of RSA-like Cryptosystems. *Cryptography* **2025**, *9*, 2. https://doi.org/10.3390/cryptography9010002

The encryption and decryption processes mirror those of the RSA: for $m \in \mathbb{Z}_N[i]$, the ciphertext is $c \equiv m^e \bmod N$, and to recover m, we compute $m \equiv c^d \bmod N$. Note that all operations are performed in the ring $\mathbb{Z}_N[i]$.

Elkamchouchi et al. [10] argued that their extension has better security compared with the traditional RSA. However, Bunder [11] developed a Wiener-type continued fraction attack against this scheme. Using lattice-reduction techniques, the authors of [12,13] improved the bound to $d < N^{0.585}$. For more details on attacks against Elkamchouchi et al.'s scheme, see [9,14].

The rings Z_p and $Z_p[i]$ can be rewritten as $Z_p = \mathbb{Z}_p[t]/(t+1) = GF(p)$ and $Z_p[i] = \mathbb{Z}_p[t]/(t^2+1) = GF(p^2)$, where GF stands for a Galois field. Consequently, the underlying RSA group is $\mathbb{Z}_N = GF(p) \times GF(q)$, while in Elkamchouchi et al.'s case, it is $\mathbb{Z}_N[i] = GF(p^2) \times GF(q^2)$. Using these observations, Cotan and Teşeleanu [14] generalized both schemes to $GF(p^n) \times GF(q^n)$ for $n \geq 1$. In this case, the group order is $\varphi_n(N) = (p^n - 1)(q^n - 1)$, while the encryption and decryption algorithms are direct extensions of the RSA and Elkamchouchi et al.'s algorithm.

The motivation for this extension was to evaluate whether Wiener-type attacks apply to the generic setting. The authors of [14] proved that when $d < N^{0.25n}$, a continued fractions attack can always recover the secret exponent, regardless of n. This result was extended to unbalanced primes in [15]. The development of a lattice-based attack was left open in [14,15], but it was subsequently resolved in [16], thus leading to a better attack bound.

1.1. Related Work

It is worth noting that our current undertaking shares similarities with the work of [17], where the authors explored a cryptographic system closely related to our own. Specifically, they studied the effect of using latices against the generalized Murru–Saettone cryptosystem [18].

1.2. Our Contributions

In this paper, we develop several lattice-based attacks against Cotan and Teșeleanu's scheme, thus providing deeper insights into the inner workings of this family. More precisely, we prove that it is possible to factor N if d is smaller than a given threshold and the attacker has knowledge of one of the following:

- The least significant bits of d;
- An approximation of p;
- That the prime difference $|p - q|$ is small;
- That the primes share an amount of least significant bits.

To establish these results, we first prove that $\varphi_n(N)$ can be expressed as a polynomial in $p + q - M$ for a given integer M. Next, we show how to reduce each problem to solving an equation of the form $xH(y) + 1 \equiv 0 \bmod e$, where $H(y)$ is a monic univariate polynomial. Therefore, this allows us to apply Kunihiro's method for solving such equations [19].

1.3. Structure of the Paper

Preliminary notions are provided in Section 2. In Section 3, we reevaluate the previous result about the group's order, while in Section 4, we describe a series of attacks. We conclude our paper in Section 5.

2. Preliminaries

2.1. Notations

Throughout this paper, λ denotes a security parameter. Also, the notation $|S|$ denotes the cardinality of a set S. We use $\simeq$ to indicate that two values are approximately equal.

2.2. Quotient Groups

In this section, we provide the group theory needed to introduce the RSA-like family. Therefore, let $(\mathbb{F}, +, \cdot)$ be a field and $t^n - r$ an irreducible polynomial in $\mathbb{F}[t]$. Then,

$$\mathbb{A}_n = \mathbb{F}[t]/(t^n - r) = \{a_0 + a_1 t + \ldots + a_{n-1} t^{n-1} \mid a_0, a_1, \ldots, a_{n-1} \in \mathbb{F}\}$$

is the corresponding quotient field. Let $a(t), b(t) \in \mathbb{A}_n$. We remark that the quotient field induces a natural product:

$$a(t) \circ b(t) = \sum_{i=0}^{n-2} \left(\sum_{j=0}^{i} a_j b_{i-j} + r \sum_{j=0}^{i+n} a_j b_{i-j+n} \right) t^i + \sum_{j=0}^{n-1} a_j b_{n-1-j} t^{n-1}.$$

2.3. RSA-like Cryptosystems

Let p be a prime number. When we instantiate $\mathbb{F} = \mathbb{Z}_p$, we have that $\mathbb{A}_n = GF(p^n)$ is the Galois field of order p^n. Moreover, $\mathbb{A}_n^*$ is a cyclic group of order $\varphi_n(\mathbb{Z}_p) = p^n - 1$. We remark that a theorem analogous to Fermat's little theorem holds:

$$a(t)^{\varphi_n(\mathbb{Z}_p)} \equiv 1 \bmod p,$$

where $a(t) \in \mathbb{A}_n^*$ and the power is evaluated by $\circ$-multiplying $a(t)$ by itself $\varphi_n(\mathbb{Z}_p) - 1$ times. Based on these observations, the authors of [14] built an encryption scheme that is similar to the RSA by using the $\circ$ operation as the product.

Setup(λ): Let $n \geq 1$ be an integer. Randomly generate two distinct large prime numbers p and q such that $p, q \geq 2^\lambda$ and compute their product $N = pq$. Select $r \in \mathbb{Z}_N$ such that the polynomial $t^n - r$ is irreducible in $\mathbb{Z}_p[t]$ and $\mathbb{Z}_q[t]$. Let

$$\varphi_n(\mathbb{Z}_N) = \varphi_n(N) = (p^n - 1) \cdot (q^n - 1).$$

Choose an integer e such that $\gcd(e, \varphi_n(N)) = 1$ and compute d such that $ed \equiv 1 \bmod \varphi_n(N)$. Output the public key $pk = (n, N, r, e)$. The corresponding secret key is $sk = (p, q, d)$.

Encrypt(pk, m): To encrypt a message $m = (m_0, \ldots, m_{n-1}) \in \mathbb{Z}_N^n$, first construct the polynomial $m(t) = m_0 + \ldots + m_{n-1} t^{n-1} \in \mathbb{A}_n^*$, and then compute $c(t) \equiv [m(t)]^e \bmod N$. Output the ciphertext $c(t)$.

Decrypt($sk, c(t)$): to recover the message, simply compute $m(t) \equiv [c(t)]^d \bmod N$ and reassemble $m = (m_0, \ldots, m_{n-1})$.

Remark 1. *When $n = 1$, we obtain the RSA scheme [1]. Also, when $n = 2$, we obtain the Elkamchouchi et al. cryptosystem [10].*

2.4. Useful Lemmas

The results presented in this section serve as a foundation for devising our novel attacks on the RSA-like family from Section 4. Hence, we first provide some results about p and q. The first one contains lower and upper bounds for p and q (see [20], Lemma 1).

Lemma 1. *Let $N = pq$ be the product of two unknown primes with $q < p < 2q$. Then, the following property holds:*

$$\frac{\sqrt{2}}{2}\sqrt{N} < q < \sqrt{N} < p < \sqrt{2}\sqrt{N}.$$

If an approximation of p is known, an approximation of q can be derived using the following result from [21].

Lemma 2. *Let $N = pq$ be the product of two unknown primes with $q < p < 2q$. Let p_0 be an approximation of p such that $|p - p_0| < N^\varepsilon$. Then, $q_0 = \lfloor N/p_0 \rfloor$ is an approximation of q such that*

$$|q - q_0| < N^\varepsilon \text{ and } |p + q - p_0 - q_0| < 2N^\varepsilon.$$

When $p - q = 2^s u$, with s known and u unknown, the following result from [22,23] allows us to determine the s least significant bits of both p and q. Additionally, it enables the recovery of the $2s$ least significant bits of $p + q$.

Lemma 3. *Let $N = pq$ be the product of two unknown primes with $q < p < 2q$. Let $p - q = 2^s u$ with a known s and an unknown u. We define u_0 as a solution of $x^2 \equiv N \bmod 2^s$ and*

$$v_0 \equiv 2u_0 + (N - u_0^2)u_0^{-1} \bmod 2^{2s}.$$

Then, $p = p_1 \cdot 2^s + u_0$, $p = q_1 \cdot 2^s + u_0$ and $p + q = v_1 \cdot 2^{2s} + v_0$ for some integers p_1, q_1 and v_1.

We further provide a series of results concerning φ_n. The following bounds for $\varphi_n(N)$, provided in [14], (Corollary 1), imply that $\varphi_n(N)$ can be approximated by N^n.

Corollary 1. *Let $N = pq$ be the product of two unknown primes with $q < p < 2q$. Then, the following property holds:*

$$\left(\sqrt{N}^n - 1\right)^2 > \varphi_n(N) > N^n\left(1 - \frac{2^n + 1}{\sqrt{2N}^n}\right) + 1.$$

The next two results are proved in [16] and show that φ_n can be written as a polynomial in $p + q$ and that its coefficients can be computed using only N and n.

Proposition 1. *Let N be a positive integer. Then, for any integer $n \geq 1$, the following property holds:*

$$\varphi_n(N) = -(p + q)^n + \sum_{k=0}^{n-1} a_k (p + q)^k,$$

where $a_k \in \mathbb{Z}$.

Lemma 4. *Let $N = pq$ and $S = p + q$ be two positive integers. Then, for any integer $n \geq 2$, the following property holds:*

$$\varphi_n(N) = (N^{n-1} + 1)(N - S + 1) + S\varphi_{n-1}(N) - N\varphi_{n-2}(N),$$

where $\varphi_0(N) = 0$ and $\varphi_1(N) = N - S + 1$.

2.5. Finding Small Roots

In this section, we outline some tools used for solving the problem of finding small roots, both in the modular and integer cases.

Coppersmith [4,24,25] provided rigorous techniques for computing small integer roots of single-variable polynomials modulo an integer, as well as bivariate polynomials over the integers. In the case of modular roots, Coppersmith's ideas were reinterpreted by Howgrave–Graham [26]. We further provide the Howgrave–Graham result.

Theorem 1. *Let* $f(x_1, \ldots, x_n) = \sum a_{i_1 \ldots i_n} x_1^{i_1} \ldots x_n^{i_n} \in \mathbb{Z}[x_1, \ldots, x_n]$ *be a polynomial with at most* ω *monomials,* α *be an integer, and*

$$||f(x_1, \ldots, x_n)|| = \sqrt{\sum |a_{i_1 \ldots i_n}|^2}$$

be the norm of f*. Suppose that*

- $f(y_1, \ldots, y_n) \equiv 0 \bmod \alpha$ *for some* $|y_1| < X_1, \ldots, |y_n| < X_n$*;*
- $||f(y_1 X_1, \ldots, y_n X_n)|| < \alpha/\sqrt{\omega}$*.*

Then, $f(y_1, \ldots, y_n) = 0$ *holds over the integers.*

Lenstra, Lenstra and Lovász [5] proposed a lattice-reduction algorithm (LLL) that is widely used in cryptanalysis and is typically combined with Howgrave–Graham's lemma. We further provide the version presented in [27,28].

Theorem 2. *Let* L *be a lattice of dimension* ω*. In polynomial time, the LLL algorithm outputs a reduced basis* $(b_1, \ldots, b_\omega)$ *that satisfies*

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

where $det(L)$ *is the determinant of lattice* L*.*

Note that the condition

$$2^{\frac{\omega(\omega-1)}{4(\omega+1-i)}} det(L)^{\frac{1}{\omega+1-i}} < \alpha/\sqrt{\omega}$$

implies that the polynomials corresponding to b_i match Howgrave–Graham's bound. This leads to

$$det(L) \leq \varepsilon \alpha^{\omega+1-i},$$

where ε is an error term that is usually ignored.

In order to find a solution $(y_1, \ldots, y_n)$, we need the following assumption to be true.

Assumption 1. *The LLL reduced-basis polynomials are algebraically independent (they do not share a non-trivial gcd), and the resultant computations for* b_i *yield the common roots of these polynomials.*

In [19], a lattice-based method for finding small solutions of the equation $xH(y) + c \equiv 0 \bmod \beta$ is provided. This result extends the Boneh and Durfee method [3] and uses the LLL algorithm [5] and Howgrave–Graham's lemma [26] to derive the solutions. The author shows that the bounds provided in [19] are optimal under reasonable assumptions.

Theorem 3. *Let* $H(y) \in \mathbb{Z}[y]$ *be a monic polynomial with degree* $r \geq 1$ *and* β *be an integer. Suppose that*

- $x_0 H(y_0) + c \equiv 0 \bmod \beta$ *for some* $|x_0| < X = \beta^\delta$ *and* $|y_0| < Y = \beta^\gamma$*;*
- $|c| < XY^r$*.*

Then, one can solve the equation $xH(y) + c \equiv 0 \bmod \beta$ *if*

$$\begin{cases} \delta \leq \frac{r+2}{2(r+1)} - \frac{r+1}{2}\gamma & \text{when } 0 < \gamma < r/(r+1)^2, \\ \delta \leq 1 - \sqrt{r\gamma}, & \text{when } r/(r+1)^2 \leq \gamma \leq 1/r. \end{cases}$$

3. A New Look at φ_n

In this section, we further generalize the result from Proposition 1. This result is later used as building blocks for some of the partial exposure attacks presented in Section 4.

Proposition 2. *Let N be a positive integer and $M \in \mathbb{Z}$. Then, for any integer $n \geq 1$, the following property holds:*

$$\varphi_n(N) = -(p+q-M)^n + \sum_{k=0}^{n-1} a_k (p+q-M)^k,$$

where $a_k \in \mathbb{Z}$ and a_k depend only on N, M and n.

Proof. We use Lemma 4 to see that this result always holds. In order to be able to apply it, we first need to check that the first two values φ_1 and φ_2 satisfy this property.

It is easy to see that

$$\begin{aligned}\varphi_1(N) &= (p-1)(q-1) = -(p+q) + N + 1 \\ &= -(p+q-M) - M + N + 1\end{aligned}$$

and

$$\begin{aligned}\varphi_2(N) &= (p^2-1)(q^2-1) = -(p^2+q^2) + N^2 + 1 \\ &= -(p+q-M)^2 - 2M(p+q-M) - M^2 + N^2 + 2N + 1.\end{aligned}$$

Let $S = p + q$. Now, we assume that the property holds for

$$\begin{aligned}\varphi_{n-1} &= -(S-M)^{n-1} + \sum_{k=0}^{n-2} b_k (S-M)^k, \\ \varphi_{n-2} &= -(S-M)^{n-2} + \sum_{k=0}^{n-3} c_k (S-M)^k,\end{aligned}$$

and using Lemma 4, we obtain

$$\begin{aligned}\varphi_n &= S\varphi_{n-1}(N) - N\varphi_{n-2}(N) + (N^{n-1}+1)(N-S+1) \\ &= (S-M)\varphi_{n-1}(N) + M\varphi_{n-1}(N) - N\varphi_{n-2}(N) + (N^{n-1}+1)(N-S+1) \\ &= -(S-M)^n + \sum_{k=0}^{n-2} b_k (S-M)^{k+1} - M(S-M)^{n-1} + \sum_{k=0}^{n-2} b_k M (S-M)^k \\ &+ N(S-M)^{n-2} - \sum_{k=0}^{n-3} c_k N (S-M)^k + (N^{n-1}+1)(N-S+1) \\ &= -(S-M)^n + (b_{n-2} - M)(S-M)^{n-1} + (b_{n-3} + b_{n-2}M + N)(S-M)^{n-2} \\ &+ \sum_{k=1}^{n-3} (b_{k-1} + b_k M - c_k N)(S-M)^k + b_0 M - c_0 N + (N^{n-1}+1)(N-S+1).\end{aligned}$$

Therefore, if we set

$$\begin{aligned}a_{n-1} &= b_{n-2} - M \\ a_{n-2} &= b_{n-3} + b_{n-2}M + N \\ a_k &= b_{k-1} + b_k M - c_k N, \text{ for } k = 1, \ldots, n-3 \\ a_0 &= b_0 M - c_0 N + (N^{n-1}+1)(N-S+1),\end{aligned}$$

we obtain our desired result. □

Using Lemma 4, we can compute the first few values for φ_n as a polynomial in $T = p + q - M$:

$$\begin{aligned}
\varphi_1 &= -M + N - T + 1 \\
\varphi_2 &= -M^2 - 2MT + N^2 + 2N - T^2 + 1, \\
\varphi_3 &= -M^3 - 3M^2T + 3MN - 3MT^2 + N^3 + 3NT - T^3 + 1, \\
\varphi_4 &= -M^4 - 4M^3T + 4M^2N - 6M^2T^2 + 8MNT - 4MT^3 + N^4 - 2N^2 \\
&\quad + 4NT^2 - T^4 + 1, \\
\varphi_5 &= -M^5 - 5M^4T + 5M^3N - 10M^3T^2 + 15M^2NT - 10M^2T^3 - 5MN^2 \\
&\quad + 15MNT^2 - 5MT^4 + N^5 - 5N^2T + 5NT^3 - T^5 + 1, \\
\varphi_6 &= -M^6 - 6M^5T + 6M^4N - 15M^4T^2 + 24M^3NT - 20M^3T^3 - 9M^2N^2 \\
&\quad + 36M^2NT^2 - 15M^2T^4 - 18MN^2T + 24MNT^3 - 6MT^5 + N^6 + 2N^3 \\
&\quad - 9N^2T^2 + 6NT^4 - T^6 + 1.
\end{aligned}$$

The following corollary is useful in devising our attack when the two primes share a portion of their least significant bits.

Corollary 2. *Let N be a positive integer and $p + q = v_1 \cdot 2^{2s} + v_0$. Then, for any integer $n \geq 1$, the following property holds:*

$$\varphi_n(N) = -v_1^n \cdot 2^{2sn} + \sum_{k=0}^{n-1} b_k v_1^k,$$

where $b_k \in \mathbb{Z}$ and b_k depend only on N, v_0, n and s.

Proof. Rewriting $p + q = v_1 \cdot 2^{2s} + v_0$, we have $p + q - v_0 = v_1 \cdot 2^{2s}$. Replacing M with v_0 in Proposition 2, we obtain

$$\begin{aligned}
\varphi_n(N) &= -(p + q - v_0)^n + \sum_{k=0}^{n-1} a_k (p + q - v_0)^k \\
&= -(v_1 \cdot 2^{2s})^n + \sum_{k=0}^{n-1} a_k (v_1 \cdot 2^{2s})^k \\
&= -v_1^n \cdot 2^{2sn} + \sum_{k=0}^{n-1} (a_k \cdot 2^{2sk}) v_1^k \\
&= -v_1^n \cdot 2^{2sn} + \sum_{k=0}^{n-1} b_k v_1^k,
\end{aligned}$$

where $b_k = a_k \cdot 2^{2sk}$. □

4. Application of Lattices

In this section, we present our lattice-based partial exposure attacks and connect previous results to those introduced in this work.

4.1. Known Least Significant Bits of d

We further provide a method for finding the factorization of N when the attacker knows the least significant bits of d.

Theorem 4. *Let $N = pq$ be the product of two unknown primes with $q < p < 2q$. Also, let $d = d_1 \cdot 2^s + d_0$, where d_0 and s are known integers. When $e = N^\delta$, $d < N^\gamma$ and $2^s = N^\varepsilon$, we can factor N in polynomial time if*

$$\begin{cases} \gamma \leq n + \varepsilon - \sqrt{0.5n(\delta+\varepsilon)}, & \text{when } \frac{n}{2} - \varepsilon \leq \delta \leq \frac{(n+1)^2}{2n} - \varepsilon, \\ \gamma \leq \frac{3n-1}{4} + \frac{(n+2)\varepsilon - n\delta}{2(n+1)}, & \text{when } \frac{(n+1)^2}{2n} - \varepsilon < \delta \leq \frac{(n+1)(3n-1)}{2n} + \frac{(n+2)\varepsilon}{n}, \end{cases}$$

and $0.5n + \varepsilon < \gamma$ when $d_0 \geq 1$.

Proof. According to Proposition 1, we have that

$$\varphi_n(N) = -(p+q)^n + \sum_{k=0}^{n-1} a_k (p+q)^k,$$

where $a_k \in \mathbb{Z}$. Finding $p+q$ is equivalent to solving the equation

$$h(y) = -y^n + \sum_{k=0}^{n-1} a_k y^k,$$

or analogously, the monic polynomial $H(y) = -h(y)$.

By rewriting the key equation $ed - k\varphi_n(N) = 1$, we obtain $1 + k\varphi_n(N) - ed_0 = ed_1 \cdot 2^s$. Let $E = e \cdot 2^s$; then, we have the congruence $k\varphi_n(N) + 1 - ed_0 \equiv 0 \bmod E$, which is equivalent to $k(-\varphi_n(N)) - 1 + ed_0 \equiv 0 \bmod E$. Consequently, we deduce the equation $xH(y) - 1 + ed_0 \equiv 0 \bmod E$, which has k and $p+q$ as solutions.

In order to be able to apply Theorem 3, we first need to bound k and $p+q$. Since $k\varphi_n(N) = ed - 1 < ed$ and $N^n < \varphi(N)$ (see Corollary 1), we obtain that

$$k < \frac{ed}{\varphi_n(N)} < N^{\delta+\gamma-n}.$$

Using Lemma 1, we have that $p+q < 3\sqrt{N}$. Therefore, we have that $k < X = E^{(\delta+\gamma-n)/(\delta+\varepsilon)}$ and $p+q < Y \simeq E^{0.5/(\delta+\varepsilon)}$.

According to Theorem 3, we can find the solutions $x_0 = k$ and $y_0 = p+q$ to the equation $xH(y) - 1 + ed_0 \equiv 0 \bmod E$ if certain conditions are met.

We start with bounding the constant $|ed_0 - 1|$. We obtain the following inequalities:

$$|ed_0 - 1| < ed_0 < e \cdot 2^s < XY^n = E^{\frac{\delta+\gamma-n}{\delta+\varepsilon}} \cdot E^{\frac{0.5n}{\delta+\varepsilon}},$$

and the last one is equivalent to

$$1 < E^{\frac{\gamma-0.5n-\varepsilon}{\delta+\varepsilon}} \Leftrightarrow 0.5n + \varepsilon < \gamma.$$

The last inequality has to hold when $d_0 \geq 1$, and no restrictions are necessary otherwise.

Now, let us consider the first case of Theorem 3. We have

$$0 \leq \frac{1}{2(\delta+\varepsilon)} < \frac{n}{(n+1)^2} \Leftrightarrow \frac{(n+1)^2}{2n} - \varepsilon < \delta$$

and

$$\begin{aligned}\frac{\delta+\gamma-n}{\delta+\varepsilon} &\leq \frac{n+2}{2(n+1)} - \frac{n+1}{2}\cdot\frac{1}{2(\delta+\varepsilon)}\\ &\Leftrightarrow \delta+\gamma-n \leq \frac{(n+2)(\delta+\varepsilon)}{2(n+1)} - \frac{n+1}{4}\\ &\Leftrightarrow \gamma \leq n - \frac{n+1}{4} + \left(\frac{n+2}{2(n+1)} - 1\right)\delta + \frac{(n+2)\varepsilon}{2(n+1)}\\ &\Leftrightarrow \gamma \leq \frac{3n-1}{4} - \frac{n\delta}{2(n+1)} + \frac{(n+2)\varepsilon}{2(n+1)}.\end{aligned}$$

Since we also want $\gamma \geq 0$, we must have

$$0 \leq -\frac{n\delta}{2(n+1)} + \frac{(n+2)\varepsilon}{2(n+1)} + \frac{3n-1}{4} \Leftrightarrow \delta \leq \frac{(n+1)(3n-1)}{2n} + \frac{(n+2)\varepsilon}{n}.$$

In the second case of Theorem 3, we have

$$\frac{n}{(n+1)^2} \leq \frac{1}{2(\delta+\varepsilon)} \leq \frac{1}{n} \Leftrightarrow \frac{n}{2} - \varepsilon \leq \delta \leq \frac{(n+1)^2}{2n} - \varepsilon$$

and

$$\begin{aligned}\frac{\delta+\gamma-n}{\delta+\varepsilon} \leq 1 - \frac{\sqrt{n}}{\sqrt{2(\delta+\varepsilon)}} &\Leftrightarrow \delta+\gamma-n \leq \delta+\varepsilon-\sqrt{0.5n(\delta-\varepsilon)}\\ &\Leftrightarrow \gamma \leq n+\varepsilon-\sqrt{0.5n(\delta+\varepsilon)}.\end{aligned}$$

Since we also want $\gamma \geq 0$, we must have

$$0 \leq n+\varepsilon-\sqrt{0.5n(\delta+\varepsilon)} \Leftrightarrow \delta \leq 2n+3\varepsilon+\frac{2\varepsilon^2}{n}.$$

Note that $(n+1)^2/2n \leq 2n$ for $n \geq 1$, and thus, $(n+1)^2/2n - \varepsilon \leq 2n+3\varepsilon+2\varepsilon^2/n$.

Once y_0 is found, solving the following system of equations:

$$\begin{cases} p+q = y_0 \\ pq = N \end{cases}$$

enables us to factorize the modulus N. □

When the case $s = 0$ is considered, the lattice attack presented in [16] for the RSA-like family becomes a special case of Theorem 4.

Corollary 3. *Let $N = pq$ be the product of two unknown primes with $q < p < 2q$. Also, let $e = N^\delta$ and $d < N^\gamma$. We can factor N in polynomial time if*

$$\begin{cases} \gamma \leq n - \sqrt{0.5n\delta}, & \text{when } \frac{n}{2} \leq \delta \leq \frac{(n+1)^2}{2n}, \\ \gamma \leq \frac{3n-1}{4} - \frac{n\delta}{2(n+1)}, & \text{when } \frac{(n+1)^2}{2n} < \delta \leq \frac{(n+1)(3n-1)}{2n}. \end{cases}$$

The following corollary tells us what happens when e is large enough.

Corollary 4. *Let $N = pq$ be the product of two unknown primes with $q < p < 2q$. Also, let $d = d_1 \cdot 2^s + d_0$, where d_0 and s are known integers. When $e \simeq N^n$, $d < N^\gamma$ and $2^s = N^\varepsilon$, we can factor N in polynomial time if*

$$\begin{cases} \gamma \leq n + \varepsilon - \sqrt{0.5n(n+\varepsilon)}, & \text{when } n = 1 \text{ or } n = 2, \\ \gamma \leq \frac{3n-1}{4} + \frac{(n+2)\varepsilon - n^2}{2(n+1)}, & \text{otherwise.} \end{cases}$$

Proof. In the first case, we must have $n/2 - \varepsilon \leq n \leq (n+1)^2/2n - \varepsilon$. The first inequality is always true. Let us check the conditions for the second one:

$$\begin{aligned} n \leq \frac{(n+1)^2}{2n} - \varepsilon &\Leftrightarrow 2n^2 \leq n^2 + 2n + 1 - \varepsilon \\ &\Leftrightarrow (n-1)^2 \leq 2 - \varepsilon \\ &\Leftrightarrow n \leq \sqrt{2-\varepsilon} + 1 \leq 2.42. \end{aligned}$$

Thus, the second inequality is true only for $n = 1$ or $n = 2$.

In the second case, according to the previous statements, we automatically have $(n+1)^2/2n - \varepsilon < n$ for $n \geq 3$. Therefore, we only need to check whether

$$\begin{aligned} n \leq \frac{(n+1)(3n-1)}{2n} + \frac{(n+2)\varepsilon}{n} &\Leftrightarrow 2n^2 \leq 3n^2 + 2n - 1 + 2(n+2)\varepsilon \\ &\Leftrightarrow 2 \leq (n+1)^2 + 2(n+2)\varepsilon. \end{aligned}$$

This inequality is always true for $n \geq 3$. This concludes our proof. □

When cases $(s, n) = (0, 1)$ and $(s, n) = (0, 2)$ are considered, the optimal bounds presented in [3,6] for the RSA and [12,13] for Elkamchouchi et al.'s scheme become special cases of Corollary 4.

Corollary 5. *Let $N = pq$ be the product of two unknown primes with $q < p < 2q$. Also, let $n = 1$, $e \simeq N$ and $d < N^\gamma$. We can factor N in polynomial time if $\gamma \leq (2 - \sqrt{2})/2 \simeq 0.292$.*

Corollary 6. *Let $N = pq$ be the product of two unknown primes with $q < p < 2q$. Also, let $n = 2$, $e \simeq N^2$ and $d < N^\gamma$. We can factor N in polynomial time if $\gamma \leq 2 - \sqrt{2} \simeq 0.585$.*

4.2. Known Approximation of p

We further provide a method for finding the factorization of N when the attacker knows an approximation p_0 of p. Note that when $n = 2$, we obtain the same bound as the one presented in [21].

Theorem 5. *Let $N = pq$ be the product of two unknown primes with $q < p < 2q$. Also, let p_0 be a known approximation of p. When $e = N^\delta$, $d < N^\gamma$ and $|p - p_0| < N^\varepsilon$, we can factor N in polynomial time if*

$$\begin{cases} \gamma \leq n - \sqrt{\varepsilon n \delta}, & \text{when } \varepsilon n \leq \delta \leq \frac{\varepsilon(n+1)^2}{n}, \\ \gamma \leq \frac{n(2-\varepsilon)-1}{2} - \frac{n\delta}{2(n+1)}, & \text{when } \frac{\varepsilon(n+1)^2}{n} < \delta \leq \frac{(n+1)[n(2-\varepsilon)-1]}{n}, \end{cases}$$

and $\varepsilon < (2n-1)/(2n+1)$.

Proof. Using Lemma 2, we have that $q_0 = \lfloor N/p_0 \rfloor$ is an approximation of q such that

$$|q - q_0| < N^\varepsilon \text{ and } |p + q - p_0 - q_0| < 2N^\varepsilon.$$

Setting $M = p_0 + q_0$ in Proposition 2, we obtain that

$$\varphi_n(N) = -(p+q-p_0-q_0)^n + \sum_{k=0}^{n-1} a_k (p+q-p_0-q_0)^k,$$

where $a_k \in \mathbb{Z}$. Finding $p+q-p_0-q_0$ is equivalent to solving the equation

$$h(y) = -y^n + \sum_{k=0}^{n-1} a_k y^k,$$

or analogously, the monic polynomial $H(y) = -h(y)$.

By rewriting the key equation $ed - k\varphi_n(N) = 1$, we obtain the congruence $k\varphi_n(N) + 1 \equiv 0 \bmod e$, which is equivalent to $k(-\varphi_n(N)) - 1 \equiv 0 \bmod e$. Consequently, we deduce the equation $xH(y) - 1 \equiv 0 \bmod e$, which has k and $p+q-p_0-q_0$ as solutions.

In order to be able to apply Theorem 3, we first need to bound k and $p+q-p_0-q_0$. Since $k\varphi_n(N) = ed - 1 < ed$ and $N^n < \varphi(N)$ (see Corollary 1), we obtain that

$$k < \frac{ed}{\varphi_n(N)} < N^{\delta+\gamma-n}.$$

Using Lemma 2, we have that $|p+q-p_0-q_0| < 2N^{\varepsilon}$. Therefore, we have that $k < X = e^{(\delta+\gamma-n)/\delta}$ and $|p+q-p_0-q_0| < Y \simeq e^{\varepsilon/\delta}$.

According to Theorem 3, we can find the solutions $x_0 = k$ and $y_0 = p+q-p_0-q_0$ to the equation $xH(y) - 1 \equiv 0 \bmod e$ if certain conditions are met.

Let us consider the first case of Theorem 3. We have

$$0 \le \frac{\varepsilon}{\delta} < \frac{n}{(n+1)^2} \Leftrightarrow \frac{\varepsilon(n+1)^2}{n} < \delta$$

and

$$\begin{aligned}\frac{\delta+\gamma-n}{\delta} \le \frac{n+2}{2(n+1)} - \frac{n+1}{2}\cdot\frac{\varepsilon}{\delta} &\Leftrightarrow \delta+\gamma-n \le \frac{(n+2)\delta}{2(n+1)} - \frac{\varepsilon(n+1)}{2} \\ &\Leftrightarrow \gamma \le n - \frac{\varepsilon(n+1)}{2} + \left(\frac{n+2}{2(n+1)} - 1\right)\delta \\ &\Leftrightarrow \gamma \le \frac{n(2-\varepsilon)-1}{2} - \frac{n\delta}{2(n+1)}.\end{aligned}$$

Since we also want $\gamma \ge 0$, we must have

$$0 \le -\frac{n\delta}{2(n+1)} + \frac{n(2-\varepsilon)-1}{2} \Leftrightarrow \delta \le \frac{(n+1)[n(2-\varepsilon)-1]}{n}.$$

This leads to

$$\begin{aligned}\frac{\varepsilon(n+1)^2}{n} < \frac{(n+1)[n(2-\varepsilon)-1]}{n} &\Leftrightarrow \varepsilon(n+1) < n(2-\varepsilon) - 1 \\ &\Leftrightarrow \varepsilon < \frac{2n-1}{2n+1}.\end{aligned} \tag{1}$$

In the second case of Theorem 3, we have

$$\frac{n}{(n+1)^2} \le \frac{\varepsilon}{\delta} \le \frac{1}{n} \Leftrightarrow \varepsilon n \le \delta \le \frac{\varepsilon(n+1)^2}{n}$$

and

$$\frac{\delta+\gamma-n}{\delta} \leq 1-\frac{\sqrt{\varepsilon n}}{\sqrt{\delta}} \Leftrightarrow \delta+\gamma-n \leq \delta-\sqrt{\varepsilon n \delta}$$
$$\Leftrightarrow \gamma \leq n-\sqrt{\varepsilon n \delta}.$$

Since we also want $\gamma \geq 0$, we must have

$$0 \leq n-\sqrt{\varepsilon n \delta} \Leftrightarrow \delta \leq \frac{n}{\varepsilon}.$$

Therefore, we need to check that

$$\frac{\varepsilon(n+1)^2}{n} < \frac{n}{\varepsilon} \Leftrightarrow \varepsilon < \frac{n}{n+1}.$$

Note that Equation (1) implies that

$$\varepsilon < \frac{2n-1}{2n+1} < \frac{n}{n+1}.$$

Once y_0 is found, solving the following system of equations

$$\begin{cases} p+q = y_0+p_0+q_0 \\ pq = N \end{cases}$$

enables us to factorize the modulus N. □

The following corollary tells us what happens when e is large enough.

Corollary 7. *Let $N = pq$ be the product of two unknown primes with $q < p < 2q$. Also, let p_0 be a known approximation of p. When $e \simeq N^n$, $d < N^\gamma$ and $|p-p_0| < N^\varepsilon$, we can factor N in polynomial time if*

$$\begin{cases} \gamma \leq n(1-\sqrt{\varepsilon}), & \text{when } \frac{n^2}{(n+1)^2} \leq \varepsilon \leq \frac{2n-1}{2n+1}, \\ \gamma \leq \frac{n(2-\varepsilon)-1}{2} - \frac{n^2}{2(n+1)}, & \text{when } 0 < \varepsilon \leq \frac{n^2}{(n+1)^2}, \end{cases}$$

and $\varepsilon < (2n-1)/(2n+1)$.

Proof. The only thing that we need to prove are the bounds provided in the statement. The first bound from Theorem 5 becomes

$$\varepsilon n \leq n \leq \frac{\varepsilon(n+1)^2}{n} \Leftrightarrow \frac{n^2}{(n+1)^2} \leq \varepsilon \leq 1,$$

but we also have that $\varepsilon < (2n-1)/(2n+1) < 1$. Thus, we obtain the first bound.

The second bound from Theorem 5 becomes

$$\frac{\varepsilon(n+1)^2}{n} < n \leq \frac{(n+1)[n(2-\varepsilon)-1]}{n} \Leftrightarrow \varepsilon < \frac{n^2}{(n+1)^2} \text{ and } \varepsilon \leq \frac{n^2+n-1}{n^2+n}.$$

Since we also want $\varepsilon > 0$, we obtain our desired result. □

For the cases $n = 1$ and $n = 2$, we derive the following bounds. Notice that for $n = 1$, our result is similar to the one presented in [29], which states that if $|p-p_0| < N^\varepsilon/8$ and $\varepsilon < 0.5$, then d can be recovered if $\gamma < (1-\varepsilon)/2$. The key difference is that Nassr, Anwar

and Bahig's attack relies on continued fractions, whereas ours is lattice-based. Note that for the RSA, a lattice approach that leads to a similar bound can be found in [30]. When $n = 2$, the optimal bounds presented in [31] for Elkamchouchi et al.'s scheme are identical with ours.

Corollary 8. *Let $N = pq$ be the product of two unknown primes with $q < p < 2q$. Also, let p_0 be a known approximation of p. When $n = 1$, $e = N$, $d < N^\gamma$ and $|p - p_0| < N^\varepsilon$, we can factor N in polynomial time if*

$$\begin{cases} \gamma \leq 1 - \sqrt{\varepsilon}, & \text{when } 0.25 \leq \varepsilon < 0.(3), \\ \gamma \leq \frac{1-\varepsilon}{2}, & \text{when } \varepsilon < 0.25. \end{cases}$$

Corollary 9. *Let $N = pq$ be the product of two unknown primes with $q < p < 2q$. Also, let p_0 be a known approximation of p. When $n = 2$, $e = N^2$, $d < N^\gamma$ and $|p - p_0| < N^\varepsilon$, we can factor N in polynomial time if*

$$\begin{cases} \gamma \leq 2(1 - \sqrt{\varepsilon}), & \text{when } 0.(4) \leq \varepsilon < 0.6, \\ \gamma \leq \frac{3-2\varepsilon}{2}, & \text{when } \delta < 0.(4). \end{cases}$$

The following corollary tells us what happens if the prime difference $|p - q|$ is small (or stated alternatively, the primes share the most significant bits). Note that when $n = 2$ and $e = N^2$, the bound presented in [32] for Elkamchouchi et al.'s scheme is a special case of Corollary 10. For RSA, similar bounds to ours are provided in [30,33].

Corollary 10. *Let $N = pq$ be the product of two unknown primes with $q < p < 2q$. When $e = N^\delta$, $d < N^\gamma$ and $|p - q| < N^\varepsilon$, we can factor N in polynomial time if*

$$\begin{cases} \gamma \leq n - \sqrt{\varepsilon n \delta}, & \text{when } \varepsilon n \leq \delta \leq \frac{\varepsilon(n+1)^2}{n}, \\ \gamma \leq \frac{n(2-\varepsilon)-1}{2} - \frac{n\delta}{2(n+1)}, & \text{when } \frac{\varepsilon(n+1)^2}{n} < \delta \leq \frac{(n+1)[n(2-\varepsilon)-1]}{n}, \end{cases}$$

and $\varepsilon < (2n-1)/(2n+1)$.

Proof. Using Lemma 1, we have that $q < \sqrt{N} < p$, which leads to

$$0 < p - \sqrt{N} < p - q < N^\varepsilon.$$

Therefore, $\sqrt{N}$ is a good approximation for p. Using Theorem 5, we obtain our desired bound. □

4.3. Primes Sharing the Least Significant Bits

Finally, we provide a factorization method for N when the two primes share an amount of the least significant bits.

Theorem 6. *Let $N = pq$ be the product of two unknown primes with $q < p < 2q$. Also, let $p - q = v_1 \cdot 2^s + v_0$, where s is a known integer. When $e = N^\delta$, $d < N^\gamma$ and $2^s = N^\varepsilon$, we can factor N in polynomial time if*

$$\begin{cases} \gamma \leq n - \sqrt{0.5n\delta(1-4\varepsilon)}, & \text{when } \frac{n(1-4\varepsilon)}{2} \leq \delta \leq \frac{(1-4\varepsilon)(n+1)^2}{2n}, \\ \gamma \leq \frac{3n-1}{4} + \varepsilon(n+1) - \frac{n\delta}{2(n+1)}, & \text{when } \frac{(1-4\varepsilon)(n+1)^2}{2n} < \delta \leq \frac{4\varepsilon(n+1)^2+(n+1)(3n-1)}{2n}, \end{cases}$$

and $0.5n < \delta + \gamma$.

Proof. According to Corollary 2, we have that

$$\varphi_n(N) = -v_1^n \cdot 2^{2sn} + \sum_{k=0}^{n-1} b_k v_1^k,$$

where $b_k \in \mathbb{Z}$. Finding v_1 is equivalent to solving the equation

$$h(y) = -2^{2sn} \cdot \left(y^n - \sum_{k=0}^{n-1} \frac{b_k y^k}{2^{2sn}} \right),$$

or analogously, the monic polynomial $H(y) = -h(y)/2^{2sn}$.

By rewriting the key equation $ed - k\varphi_n(N) = 1$, we obtain the congruence $k(-2^{-2sn} \cdot \varphi_n(N)) - 2^{-2sn} \equiv 0 \bmod e$. Note that 2^{-2sn} makes sense since $\gcd(2, e) = 1$. Consequently, we deduce the equation $xH(y) - 2^{-2sn} \equiv 0 \bmod e$, which has k and v_1 as solutions.

In order to be able to apply Theorem 3, we first need to bound k and v_1. Since $k\varphi_n(N) = ed - 1 < ed$ and $N^n < \varphi(N)$ (see Corollary 1), we obtain that

$$k < \frac{ed}{\varphi_n(N)} < N^{\delta+\gamma-n}.$$

Using Lemma 1, we have that $p + q = v_1 \cdot 2^{2s} + v_0 < 3\sqrt{N}$, and thus,

$$v_1 = \frac{p + q - v_0}{2^{2s}} < 3N^{0.5-2\varepsilon}.$$

Note that if $v_1 = 1$ or $v_1 = 2$, we can easily factor N. Hence, we can safely assume that $0.5 - 2\varepsilon > 0$. Therefore, we have that $k < X = e^{(\delta+\gamma-n)/\delta}$ and $v_1 < Y \simeq e^{(0.5-2\varepsilon)/\delta}$.

According to Theorem 3, we can find the solutions $x_0 = k$ and $y_0 = v_1$ to equation $xH(y) - 2^{-2sn} \equiv 0 \bmod E$ if certain conditions are met.

We start with bounding the constant $|-2^{-2sn}|$. We obtain the following inequality:

$$|-2^{-2sn}| = 2^{-2sn} = N^{-2n\varepsilon} = e^{\frac{-2n\varepsilon}{\delta}} < e^{\frac{\delta+\gamma-n}{\delta}} \cdot e^{\frac{(0.5-2\varepsilon)n}{\delta}} = e^{\frac{\delta+\gamma-(0.5+2\varepsilon)n}{\delta}},$$

which is equivalent to

$$-2n\varepsilon < \delta + \gamma - (0.5 + 2\varepsilon)n \Leftrightarrow 0.5n < \delta + \gamma.$$

Now, let us consider the first case of Theorem 3. We have

$$0 \leq \frac{1 - 4\varepsilon}{2\delta} < \frac{n}{(n+1)^2} \Leftrightarrow \frac{(1 - 4\varepsilon)(n+1)^2}{2n} < \delta$$

and

$$\begin{aligned}
\frac{\delta + \gamma - n}{\delta} &\leq \frac{n+2}{2(n+1)} - \frac{n+1}{2} \cdot \frac{1 - 4\varepsilon}{2\delta} \\
&\Leftrightarrow \delta + \gamma - n \leq \frac{(n+2)\delta}{2(n+1)} - \frac{(1 - 4\varepsilon)(n+1)}{4} \\
&\Leftrightarrow \gamma \leq n - \frac{(1 - 4\varepsilon)(n+1)}{4} + \left(\frac{n+2}{2(n+1)} - 1 \right) \delta \\
&\Leftrightarrow \gamma \leq \frac{3n - 1}{4} + \varepsilon(n+1) - \frac{n\delta}{2(n+1)}.
\end{aligned}$$

Since we also want $\gamma \geq 0$, we must have

$$0 \leq -\frac{n\delta}{2(n+1)} + \varepsilon(n+1) + \frac{3n-1}{4}$$
$$\Leftrightarrow \delta \leq \frac{4\varepsilon(n+1)^2 + (n+1)(3n-1)}{2n}.$$

In the second case of Theorem 3, we have

$$\frac{n}{(n+1)^2} \leq \frac{1-4\varepsilon}{2\delta} \leq \frac{1}{n} \Leftrightarrow \frac{n(1-4\varepsilon)}{2} \leq \delta \leq \frac{(1-4\varepsilon)(n+1)^2}{2n}$$

and

$$\frac{\delta+\gamma-n}{\delta} \leq 1 - \frac{\sqrt{n(1-4\varepsilon)}}{\sqrt{2\delta}} \Leftrightarrow \delta+\gamma-n \leq \delta - \sqrt{0.5n\delta(1-4\varepsilon)}$$
$$\Leftrightarrow \gamma \leq n - \sqrt{0.5n\delta(1-4\varepsilon)}.$$

Since we also want $\gamma \geq 0$, we must have

$$0 \leq n - \sqrt{0.5n\delta(1-4\varepsilon)} \Leftrightarrow \delta \leq \frac{2n}{1-4\varepsilon}.$$

Once y_0 is found, solving the following system of equations

$$\begin{cases} p+q = y_0 \cdot 2^{2s} + v_0 \\ pq = N \end{cases}$$

enables us to factorize the modulus N. □

The following corollary tells us what happens when e is large enough.

Theorem 7. *Let $N = pq$ be the product of two unknown primes with $q < p < 2q$. Also, let $p - q = v_1 \cdot 2^s + v_0$, where s is a known integer. When $n > 2$, $e \simeq N^n$, $d < N^\gamma$ and $2^s = N^\varepsilon$, we can factor N in polynomial time if*

$$\gamma \leq \frac{3n-1}{4} + \varepsilon(n+1) - \frac{n^2}{2(n+1)}.$$

Proof. The only thing that we need to prove are the bounds provided in the statement. The first bound from Theorem 6 becomes

$$\frac{n(1-4\varepsilon)}{2} \leq n \leq \frac{(1-4\varepsilon)(n+1)^2}{2n} \Leftrightarrow \varepsilon \leq \frac{1}{4} - \frac{n^2}{2(n+1)^2}.$$

The second bound from Theorem 6 becomes

$$\frac{(1-4\varepsilon)(n+1)^2}{2n} < n \leq \frac{4\varepsilon(n+1)^2 + (n+1)(3n-1)}{2n}$$
$$\Leftrightarrow \frac{1}{4} - \frac{n^2}{2(n+1)^2} < \varepsilon \text{ and } \frac{-n^2-2n+1}{4(n+1)^2} \leq \varepsilon.$$

Therefore, we obtain the following result

$$\begin{cases} \gamma \leq n[1-\sqrt{0.5(1-4\varepsilon)}], & \text{when } \varepsilon \leq \frac{1}{4} - \frac{n^2}{2(n+1)^2}, \\ \gamma \leq \frac{3n-1}{4} + \varepsilon(n+1) - \frac{n^2}{2(n+1)}, & \text{when } \frac{1}{4} - \frac{n^2}{2(n+1)^2} < \varepsilon. \end{cases} \tag{2}$$

Note that we also want $\varepsilon > 0$. When $n > 2$, we obtain just this only in the second case, and thus, we obtain our desired result. □

When $n = 1$ and $n = 2$, we obtain the following bounds. Note that these results are a direct consequence of Equation (2).

Corollary 11. *Let $N = pq$ be the product of two unknown primes with $q < p < 2q$. Also, let $p - q = v_1 \cdot 2^s + v_0$, where s is a known integer. When $n = 1$, $e = N$, $d < N^\gamma$ and $2^s = N^\varepsilon$, we can factor N in polynomial time if*

$$\begin{cases} \gamma \leq 1 - \sqrt{0.5(1-4\varepsilon)}, & \textit{when } \varepsilon \leq 0.125, \\ \gamma \leq \frac{1+4\varepsilon}{2}, & \textit{when } 0.125 < \varepsilon. \end{cases}$$

Corollary 12. *Let $N = pq$ be the product of two unknown primes with $q < p < 2q$. Also, let $p - q = v_1 \cdot 2^s + v_0$, where s is a known integer. When $n = 2$, $e = N^2$, $d < N^\gamma$ and $2^s = N^\varepsilon$, we can factor N in polynomial time if*

$$\begin{cases} \gamma \leq n - \sqrt{0.5n\delta(1-4\varepsilon)}, & \textit{when } \varepsilon \leq 0.02(7), \\ \gamma \leq \frac{5+12\varepsilon}{4}, & \textit{when } 0.02(7) < \varepsilon. \end{cases}$$

5. Conclusions

In this paper, we present several lattice-based attacks on a family of RSA-like cryptosystems. To execute our attacks, we first reduce the problem to solving an equation of type $xH(y) - 1 \equiv 0 \bmod e$, after which we apply a result proven by Kunihiro [19]. The resulting bounds extend prior results for the RSA and the scheme by Elkamchouchi et al. while providing deeper insights into selecting optimal parameters for the broader RSA-like family.

Future Work

An interesting research direction is whether more of the attacks presented in [7–9,14] can be adapted to the general case.

Funding: This research received no external funding.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: The author declares no conflicts of interest.

References

1. Rivest, R.L.; Shamir, A.; Adleman, L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Commun. ACM* **1978**, *21*, 120–126. [CrossRef]
2. Wiener, M.J. Cryptanalysis of Short RSA Secret Exponents. *IEEE Trans. Inf. Theory* **1990**, *36*, 553–558. [CrossRef]
3. Boneh, D.; Durfee, G. Cryptanalysis of RSA with Private Key d Less than $N^{0.292}$. In Proceedings of the EUROCRYPT 1999, Prague, Czech Republic, 2–6 May 1999; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 1999; Volume 1592, pp. 1–11.

4. Coppersmith, D. Finding a Small Root of a Univariate Modular Equation. In Proceedings of the EUROCRYPT 1996, Saragossa, Spain, 12–16 May 1996; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany 1996; Volume 1070, pp. 155–165.
5. Lenstra, A.K.; Lenstra, H.W.; Lovász, L. Factoring Polynomials with Rational Coefficients. *Math. Ann.* **1982**, *261*, 515–534. [CrossRef]
6. Herrmann, M.; May, A. Maximizing Small Root Bounds by Linearization and Applications to Small Secret Exponent RSA. In Proceedings of the PKC 2010, Paris, France, 26–28 May 2010; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2010; Volume 6056, pp. 53–69.
7. Boneh, D. Twenty Years of Attacks on the RSA Cryptosystem. *Not. AMS* **1999**, *46*, 203–213.
8. May, A. Using LLL-Reduction for Solving RSA and Factorization Problems. In *The LLL Algorithm: Survey and Applications*; Information Security and Cryptography; Springer: Berlin/Heidelberg, Germany, 2010; pp. 315–348.
9. Shi, G.; Wang, G.; Gu, D. Further Cryptanalysis of a Type of RSA Variants. In Proceedings of the ISC 2022, Bali, Indonesia, 18–22 December 2022; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2022; Volume 13640, pp. 133–152.
10. Elkamchouchi, H.; Elshenawy, K.; Shaban, H. Extended RSA Cryptosystem and Digital Signature Schemes in the Domain of Gaussian Integers. In Proceedings of the ICCS 2002, Amsterdam, The Netherlands, 21–24 April 2002; IEEE Computer Society: Washington, DC, USA, 2002; Volume 1, pp. 91–95.
11. Bunder, M.; Nitaj, A.; Susilo, W.; Tonien, J. A New Attack on Three Variants of the RSA Cryptosystem. In Proceedings of the ACISP 2016, Melbourne, Australia, 4–6 July 2016; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2016; Volume 9723, pp. 258–268.
12. Peng, L.; Hu, L.; Lu, Y.; Wei, H. An Improved Analysis on Three Variants of the RSA Cryptosystem. In Proceedings of the Inscrypt 2016, Beijing, China, 4–6 November 2016; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2016; Volume 10143, pp. 140–149.
13. Zheng, M.; Kunihiro, N.; Hu, H. Cryptanalysis of RSA Variants with Modified Euler Quotient. In Proceedings of the AFRICACRYPT 2018, Marrakesh, Morocco, 7–9 May 2018; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2018; Volume 10831, pp. 266–281.
14. Cotan, P.; Teşeleanu, G. Small Private Key Attack Against a Family of RSA-Like Cryptosystems. In Proceedings of the NordSEC 2023, Oslo, Norway, 16–17 November 2023; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2023; Volume 14324, pp. 57–72.
15. Cotan, P.; Teşeleanu, G. A Security Analysis of Two Classes of RSA-Like Cryptosystems. *J. Math. Cryptol.* **2024**, *18*, 20240013. [CrossRef]
16. Teşeleanu, G. A Lattice Attack Against a Family of RSA-like Cryptosystems. In Proceedings of the CSCML 2024, Be'er Sheva, Israel, 19–20 December 2024; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2024.
17. Rahmani, M.; Nitaj, A.; Ziane, M. Partial Exposure Attacks on a New RSA Variant. *Cryptography* **2024**, *8*, 44. [CrossRef]
18. Cotan, P.; Teşeleanu, G. Continued Fractions Applied to a Family of RSA-like Cryptosystems. In Proceedings of the ISPEC 2022, Taipei, Taiwan, 23–25 November 2022; Springer: Berlin/Heidelberg, Germany, 2022; pp. 589–605.
19. Kunihiro, N. On Optimal Bounds of Small Inverse Problems and Approximate GCD Problems with Higher Degree. In Proceedings of the ISC 2012, Passau, Germany, 19–21 September 2012; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2012; Volume 7483, pp. 55–69.
20. Nitaj, A. Another Generalization of Wiener's Attack on RSA. In Proceedings of the AFRICACRYPT 2008, Casablanca, Morocco, 11–14 June 2008; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2008; Volume 5023, pp. 174–190.
21. Feng, Y.; Nitaj, A.; Pan, Y. Partial Prime Factor Exposure Attacks on Some RSA Variants. *Theor. Comput. Sci.* **2024**, *999*, 114549. [CrossRef]
22. Steinfeld, R.; Zheng, Y. On the Security of RSA with Primes Sharing Least-Significant Bits. *Appl. Algebra Eng. Commun. Comput.* **2004**, *15*, 179–200. [CrossRef]
23. Nitaj, A.; Ariffin, M.R.K.; Nassr, D.I.; Bahig, H.M. New Attacks on the RSA Cryptosystem. In Proceedings of the AFRICACRYPT 2014, Marrakesh, Morocco, 28–30 May 2014; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2014; Volume 8469, pp. 178–198.
24. Coppersmith, D. Finding a Small Root of a Bivariate Integer Equation; Factoring with High Bits Known. In Proceedings of the EUROCRYPT 1996, Saragossa, Spain, 12–16 May 1996; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 1996; Volume 1070, pp. 178–189.
25. Coppersmith, D. Small Solutions to Polynomial Equations, and Low Exponent RSA Vulnerabilities. *J. Cryptol.* **1997**, *10*, 233–260. [CrossRef]
26. Howgrave-Graham, N. Finding Small Roots of Univariate Modular Equations Revisited. In Proceedings of the IMA 1997, Cirencester, UK, 17–19 December 1997; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 1997; Volume 1355, pp. 131–142.

27. May, A. New RSA Vulnerabilities Using Lattice Reduction Methods. Ph.D. Thesis, University of Paderborn, Paderborn, Germany, 2003.
28. Jochemsz, E.; May, A. A Strategy for Finding Roots of Multivariate Polynomials with New Applications in Attacking RSA Variants. In Proceedings of the ASIACRYPT 2006, Shanghai, China, 3–7 December 2006; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2006; Volume 4284, pp. 267–282.
29. Nassr, D.I.; Bahig, H.M.; Bhery, A.; Daoud, S.S. A New RSA Vulnerability Using Continued Fractions. In Proceedings of the AICCSA 2008, Doha, Qatar, 1–4 April 2008; IEEE Computer Society: Washington, DC, USA, 2008; pp. 694–701.
30. Feng, Y.; Liu, Z.; Nitaj, A.; Pan, Y. Practical Small Private Exponent Attacks against RSA. *IACR Cryptol. ePrint Arch.* **2024**. Available online: https://eprint.iacr.org/2024/1331 (accessed on 23 December 2024). [CrossRef]
31. Abderrahmane Nitaj, N.N.H.A.; Ariffin, M.R.B.K. Cryptanalysis of a New Variant of the RSA Cryptosystem. In Proceedings of the AFRICACRYPT 2024, Douala, Cameroon, 10–12 July 2024; Springer: Berlin/Heidelberg, Germany, 2024.
32. Cherkaoui-Semmouni, M.; Nitaj, A.; Susilo, W.; Tonien, J. Cryptanalysis of RSA Variants with Primes Sharing Most Significant Bits. In Proceedings of the ISC 2021, Virtual Event, 10–12 November 2021; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2021; Volume 13118, pp. 42–53.
33. De Weger, B. Cryptanalysis of RSA with Small Prime Difference. *Appl. Algebra Eng. Commun. Comput.* **2002**, *13*, 17–28. [CrossRef]