A Review of Lattice Attacks Applied to Two Types of RSA Variants

Ramona Corbeanu[1] and George Teşeleanu[2]

[1] Faculty of Mathematics, Bucharest University
14 Strada Academiei, Bucharest, Romania
ramona.corbeanu@s.unibuc.ro
[2] Simion Stoilow Institute of Mathematics of the Romanian Academy
21 Calea Grivitei, Bucharest, Romania
george.teseleanu@yahoo.com

Abstract. In recent years, various RSA variants based on diverse algebraic structures have been proposed with the aim of enhancing its security. In this paper, we focus on type-A and type-B variants, which generalize RSA-type constructions over the ring of Gaussian integers modulo $N = pq$ and constructions based on the cubic Pell equation, respectively. First, we present a lattice-based method for finding, in polynomial time, solutions to the equation $xH(y) + cz \equiv 0 \bmod \beta$, where $H(y)$ is a monic polynomial, thereby generalizing previously established bounds. We then apply this method to factor the modulus in both type-A and type-B cryptosystems under multiple attack scenarios, such as partial key information attacks. Therefore, we provide certain bounds for the secret exponent under which these cryptosystems can be compromised.

Keywords: lattice attacks, small private key attack, RSA

1 Introduction

Background. The RSA cryptosystem, introduced by Rivest, Shamir, and Adleman in [31], remains a cornerstone of modern public-key cryptography and one of the most ubiquitously deployed encryption schemes. In its standard formulation, RSA operates in the multiplicative group $\mathbb{Z}_N$, where $N = pq$ is the product of two large primes. Encryption of a message $m \in \mathbb{Z}_N$ is defined by $c \equiv m^e \bmod N$, where the public exponent e satisfies $\gcd(e, \varphi(N)) = 1$ and $\varphi(N) = (p-1)(q-1)$. Decryption is given by $m \equiv c^d \bmod N$, with $d \equiv e^{-1} \bmod \varphi(N)$. The public key is (N, e), whereas the factorization (p, q) and the secret exponent d remain confidential. Throughout this work, we restrict attention to balanced primes, i.e., $q < p < 2q$, ensuring that p and q have equal bit-length.

One of the fundamental problems of cryptanalytic research is the recovery of the secret exponent d from the public key (N, e). Wiener's seminal attack [37] demonstrates that if $d < N^{0.25}/3$, then d can be efficiently recovered from the continued fraction expansion of e/N, thereby yielding a factorization of N. Boneh and Durfee [3] substantially strengthened this result, showing that $d <$

$N^{0.292}$ suffices for efficient recovery via Coppersmith's method [7] and lattice reduction techniques [19]. Herrmann and May [15] later matched this bound using significantly simpler methods. Overviews of these and related attacks can be found in [2, 21, 32].

RSA over Gaussian Integers. Elkamchouchi, Elshenawy, and Shaban introduced in [12] an RSA analogue defined over the ring of Gaussian integers modulo N. Instead of working with integers, their proposal uses elements of the form $a + bi$, with $a, b \in \mathbb{Z}_N$ and $i^2 = -1$. The corresponding multiplicative group $\mathbb{Z}_N[i]$ has order $\phi(N) = (p^2 - 1)(q^2 - 1)$, and the public and secret exponents satisfy $\gcd(e, \phi(N)) = 1$ and $d \equiv e^{-1} \bmod \phi(N)$, respectively. Encryption and decryption are defined exactly as in classical RSA, with all arithmetic performed in $\mathbb{Z}_N[i]$.

Despite initial claims of enhanced security, Bunder *et al.* [4] demonstrated a Wiener-type attack based on continued fractions. Subsequent refinements using lattice-based techniques [26, 38] extended this attack regime to $d < N^{0.585}$. Further cryptanalytic developments and refinements are discussed in [10, 32].

RSA based on the Cubic Pell Equation. Murru and Saettone introduced an RSA-like cryptosystem in [23] based on a structured group formed by equivalence classes of polynomials over $GF(p^3) \times GF(q^3)$, where GF denotes a Galois field. In contrast to classical RSA, the public exponent e is chosen to satisfy $\gcd(e, \psi(N)) = 1$, where $\psi(N) = (p^2 + p + 1)(q^2 + q + 1)$. The corresponding secret exponent is defined by $d \equiv e^{-1} \bmod \psi(N)$. Encryption and decryption are carried out analogously to standard RSA, with all operations performed in this specialized group rather than in $\mathbb{Z}_N$.

As in the case of RSA over Gaussian integers, the authors initially claimed that their construction was immune to classical RSA-like cryptanalytic attacks. This claim was subsequently refuted in [24, 34], where it was shown that a Wiener-type attack remains effective in this setting. Building on the Boneh–Durfee methodology, Nitaj *et al.* [24] strengthened this attack, establishing the bound $d < N^{0.5694}$. Further refinements by Zheng, Kunihiro, and Yao [39] yielded the sharper bound $d < N^{0.585}$. Additional analysis and related developments are discussed in [10, 32].

Generalizing via Galois Fields. The rings $\mathbb{Z}_p$ and $\mathbb{Z}_p[i]$ can be naturally identified with $GF(p)$ and $GF(p^2)$, respectively, where GF denotes a Galois field. Consequently, classical RSA may be viewed as operating over $GF(p) \times GF(q)$, while the Gaussian variant corresponds to $GF(p^2) \times GF(q^2)$. This algebraic viewpoint led Cotan and Teşeleanu [10] to introduce a unified family of RSA-like cryptosystems defined over $GF(p^n) \times GF(q^n)$ for $n \geq 1$, with group order $\varphi_n(N) = (p^n - 1)(q^n - 1)$. Encryption and decryption are direct generalizations of the cases $n = 1$ and $n = 2$. A similar endeavor was taken in [9] where the authors extend the Murru-Saettone construction to equivalence classes of polynomials over $GF(p^n) \times GF(q^n)$ for $n > 1$.

The introduction of these two generic families—hereafter referred to as type-A (RSA and its Gaussian variant) and type-B (Murru–Saettone)—was motivated by the question of whether Wiener-type cryptanalysis extends to these settings. Since then, a substantial body of cryptanalytic attacks has been developed against both families (*e.g.* [1,11,27,35,36]).

Our Contributions. Our first contribution is a lattice-based method for solving equations of the form $xH(y)+cz \equiv 0 \bmod \beta$, where $H(y)$ is a monic polynomial. This result generalizes several existing methods [1,18,28,29].

This method is subsequently applied to the factorization of the modulus for both cryptographic families (type-A and type-B) under multiple attack scenarios. Specifically, we first consider the standard setting in which the adversary has access only to the public key. We then analyze scenarios in which the adversary additionally possesses either an approximation of p, knowledge that the prime difference $|p-q|$ is small, or partial information on the least significant bits of d. All resulting bounds are compared with previously published cryptanalytic results.

Structure of the Paper. We provide preliminary results in Section 2. In Section 3, we show how to solve equations of the form $xH(y) + cz \equiv 0 \bmod \beta$, where $H(y)$ is a monic polynomial. We apply our result to different attack scenarios in Section 4. Final remarks are given in Section 5.

2 Preliminaries

Notations. Throughout the paper, λ denotes a security parameter. Also, the notation $|S|$ denotes the cardinality of a set S. The action of selecting a random element x from a sample space X is denoted by $x \xleftarrow{\$} X$.

2.1 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 [6–8] 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 [16]. We further provide Howgrave-Graham result.

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

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

be its norm. Suppose that

– $f(y_1, \ldots, y_n) \equiv 0 \bmod \alpha$ *for some* $|y_1| \leq X_1, \ldots, |y_n| \leq X_n$,
– $||f(y_1X_1, \ldots, y_nX_n)|| < \alpha/\sqrt{\omega}$,

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

Lenstra, Lenstra and Lovász [19] 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 [17, 20].

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

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

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 3 *The LLL reduced basis polynomials are algebraically independent*[3]*, and the resultant computations for* b_i *yield the common roots of these polynomials.*

Once an attack is obtained for a given upper bound on small private exponents, the result of [22] implies the existence of a corresponding attack for a given lower bound on large private exponents.

Theorem 4. *Let* $N = pq$ *be the product of two unknown primes with* $q < p < 2q$*. Let* $\psi : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$*. Suppose we are given an algorithm* $\mathcal{A}$ *that is able to factor* N *in polynomial time given* N *and a public exponent* $0 < e < \psi(p, q)$ *such that there exists positive integers* x *and* y *satisfying*

$$ex - y\phi(p, q) = z, \text{ with } xy < \mathcal{B}_1 \text{ and } |z| < \mathcal{B}_2,$$

for $\mathcal{B}_1 > 0$ *and* $\mathcal{B}_2 \geq 1$*. Then, using algorithm* $\mathcal{A}$*,* N *can be factored in polynomial time given* N *and a public exponent* $0 < e' < \psi(p, q)$ *such that the corresponding private exponent is* $d' = \psi(p, q) - d$ *for some* $d < \sqrt{\mathcal{B}_1}$*.*

[3] They do not share a non-trivial gcd.

2.2 Quotient Groups

In this section we provide the group theory needed to introduce the RSA-like variants. 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 $a(t), b(t) \in \mathbb{A}_n$. Remark that the quotient field induces a natural product

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

We further introduce another usefull quotient group $\mathbb{B}_n = \mathbb{A}_n^*/\mathbb{F}^*$. The elements from $\mathbb{B}_n$ are equivalence classes of elements from $\mathbb{A}_n^*$. More precisely, we have

$$[a_0 + \ldots + a_{n-1}t^{n-1}] = \{\gamma a_0 + \ldots + \gamma a_{n-1}t^{n-1} \mid \gamma \in \mathbb{F}^*, a_0, \ldots, a_{n-1} \in \mathbb{F}\},$$

where $[a_0 + \ldots + a_{n-1}t^{n-1}] \in \mathbb{B}_n$.

Using Lagrange's theorem [14], we obtain the following result about the cardinality of $\mathbb{B}_n$.

Lemma 1. *The cardinality of* $\mathbb{B}_n$ *is* $\psi_n(\mathbb{F}) = (|\mathbb{F}|^n - 1)/(|\mathbb{F}| - 1)$.

For completeness, we further provide the equivalence classes from $\mathbb{B}_n$. Let $1_{\mathbb{F}^*}$ be the unity of $\mathbb{F}^*$. When $a_0 \neq 0$ and $a_1 = \ldots = a_{n-1} = 0$, we obtain that

$$[a_0 + \ldots + a_{n-1}t^{n-1}] = [a_0] = [a_0 a_0^{-1}] = [1_{\mathbb{F}^*}].$$

If $a_1 \neq 0$ and $a_2 = \ldots = a_{n-1} = 0$, then

$$[a_0 + \ldots + a_{n-1}t^{n-1}] = [a_0 + a_1 t] = [a_0 a_1^{-1} + t].$$

From the previous two examples, we can deduce the general formula. For any $k \in [0, n-1]$, if $a_k \neq 0$ and $a_{k+1} = \ldots = a_{n-1} = 0$, then

$$\begin{aligned} [a_0 + \ldots + a_{n-1}t^{n-1}] &= [a_0 + \ldots + a_k t^k] \\ &= [a_0 a_k^{-1} + a_1 a_k^{-1} t + \ldots + a_{k-1} a_k^{-1} t^{k-1} + t^k]. \end{aligned}$$

From the equivalence classes we can infer the product induced by $\mathbb{B}_n$, namely

$$[a(t)] \odot [b(t)] = [a(t) \circ b(t)] = [c(t)] = [\alpha^{-1} c(t)],$$

where α is the leading coefficient of $c(t)$.

2.3 RSA-like Cryptosystems

Let p be a prime number. We further instantiate $\mathbb{F} = \mathbb{Z}_p$. Therefore, we have that $\mathbb{A}_n = GF(p^n)$ is the Galois field of order p^n.

2.3.1 Type-A Variants (Elkamchouchi *et al.* Based)

Note that $\mathbb{A}_n^*$ is a cyclic group of order $\varphi_n(\mathbb{Z}_p) = p^n - 1$. Furthermore, we have an analogue of Fermat's little theorem

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

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 [10] built an encryption scheme that is similar to 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, 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 $m = (m_0, \ldots, m_{n-1}) \in \mathbb{Z}_N^n$ we first construct the polynomial $m(t) = m_0 + \ldots + m_{n-1}t^{n-1} \in \mathbb{A}_n^*$ and then we 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 get the RSA scheme [31]. Also, when $n = 2$, we obtain the Elkamchouchi *et al.* cryptosystem [12].

2.3.2 Type-B Variants (Murru-Saettone Based)

In this case we work with the cyclic group $\mathbb{B}_n$ which has order $\psi_n(\mathbb{Z}_p) = (p^n - 1)/(p - 1)$. For $\mathbb{B}_n$ the analogous of Fermat's little theorem is

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

where $[a(t)] \in \mathbb{B}_n$ and the power is evaluated by $\odot$-multiplying $[a(t)]$ by itself $\psi_n(\mathbb{Z}_p) - 1$ times. Based on these observations, the authors of [9] build an encryption scheme that is similar to RSA using the $\odot$ as the product.

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

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

Choose an integer e such that $\gcd(e, \psi_n(N)) = 1$ and compute d such that $ed \equiv 1 \bmod \psi_n(N)$. 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 $m = (m_0, \ldots, m_{n-2}) \in \mathbb{Z}_N^{n-1}$ we first construct the polynomial $m(t) = m_0 + \ldots + m_{n-2}t^{n-2} + t^{n-1} \in \mathbb{B}_n$ and then we 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 $m = (m_0, \ldots, m_{n-2})$.

Remark 2. When $n = 3$, we obtain the Murru and Saettone cryptosystem [23].

3 Solving the Equation $xH(y) + cz \equiv 0 \bmod \beta$

In this section we propose a new lattice based heuristics to solve the equation $xH(y) + cz \equiv 0 \bmod \beta$. We further present our result.

Theorem 5. *Let $H(y) \in \mathbb{Z}[y]$ be a monic polynomial with degree $r \geq 1$ and β be an integer. Suppose that*

- *$x_0H(y_0) + cz_0 \equiv 0 \bmod \beta$ for some $|x_0| \leq X = \beta^\delta, |y_0| \leq Y = \beta^\gamma$, $|z_0| \leq Z = \beta^\lambda$, $|c| \leq C = \beta^\varepsilon$,*

then one can solve the equation $xH(y) + cz \equiv 0 \bmod \beta$ if

$$\begin{cases} \delta \leq 1 - 0.5\lambda - \sqrt{r\gamma}, & \text{when } CZ \leq XY^r \text{ and } 0.5\lambda + \sqrt{r\gamma} < 1, \\ \delta \leq 1 - 2\lambda - \varepsilon + \frac{(1-1.5\lambda-\varepsilon)^2}{r\gamma}, & \text{when } CZ > XY^r \text{ and } 2\lambda + \varepsilon < 1. \end{cases}$$

Proof. Let $H(y) = y^r + a_{r-1}y^{r-1} + \ldots + a_1y + a_0 \in \mathbb{Z}[y]$ and consider the polynomial $R_{r+1}(x, y, z) \in \mathbb{Z}[x, y, z]$ defined by

$$R_{r+1}(x, y, z) = x \cdot H(y) + cz = xy^r + a_{r-1}xy^{r-1} + \ldots + a_1xy + a_0x + cz.$$

We denote $w = xy^r + cz$ and define the polynomial:

$$T_r(x, y, w) = w + a_{r-1}xy^{r-1} + \ldots + a_1xy + a_0x.$$

Since there exists a tuple (x_0, y_0, z_0) such that $R_{r+1}(x_0, y_0, z_0) \equiv 0 \bmod \beta$, we can define $w_0 = x_0 \cdot y_0^r + cz_0$ such that we also have

$$T_r(x_0, y_0, w_0) \equiv 0 \bmod \beta, \tag{2}$$

with $|x_0| \leq X = \beta^{\delta}, |y_0| \leq Y = \beta^{\gamma}$ and $|w_0| \leq |x_0 \cdot y_0^r| + |cz_0| \leq XY^r + CZ$.

We consider a parameter ϵ that will be optimized later, and a positive integer ν. We also define the following family of polynomials in four variables:

$$T^r_{j,k,i}(x, y, z, w) = x^i y^j z^{\nu-i-k} T_r(x, y, w)^k \cdot \beta^{\nu-k}, \ \forall \ (j, k, i) \in \mathcal{A} \cup \mathcal{B},$$

where each monomial of type xy^r is replaced by $w - cz$ and the sets $\mathcal{A}$ and $\mathcal{B}$ are given by

$$\mathcal{A} = \{(j, k, i) \mid 0 \leq j \leq r-1, 0 \leq k \leq \nu, 1 \leq i \leq \nu - k\},$$
$$\mathcal{B} = \left\{(j, k, i) \mid 0 \leq j \leq \lfloor \epsilon \rfloor, \left\lfloor \frac{\nu}{\epsilon} \right\rfloor j \leq k \leq \nu, i = 0\right\}.$$

From Equation (2) it follows that

$$T^r_{j,k,i}(x_0, y_0, z_0, w_0) \equiv 0 \mod \beta^{\nu}, \ \forall \ (j, k, i) \in \mathcal{A} \cup \mathcal{B}.$$

Let M be the matrix whose rows are the coefficient vectors corresponding to the polynomials $T^r_{j,k,i}(xX, yY, zZ, wW)$ and let L be the lattice generated by the rows of M. Using the techniques presented in [21], arranging the rows and columns of M according to the lexicographical order of (j, k, i) yields a lower triangular matrix whose determinant is equal to

$$\det(L) = X^{\theta_X} Y^{\theta_Y} Z^{\theta_Z} W^{\theta_W} \beta^{\theta_\beta},$$

where $\theta_X = f(i), \theta_Y = f(j), \theta_Z = f(\nu - i - k), \theta_W = f(k), \theta_\beta = f(\nu - k)$ and the function f is defined as

$$f(z) = \sum_{(j,k,i) \in \mathcal{A}} z + \sum_{(j,k,i) \in \mathcal{B}} z.$$

Let $\tau \geq 0$ be such that $\epsilon = \nu\tau$. To simplify the analysis, we consider the approximations $\lfloor \epsilon \rfloor \simeq \epsilon$ and $\lfloor \nu/\epsilon \rfloor \simeq \nu/\epsilon$. Thus, it follows that

$$\begin{aligned}
\theta_X &= \frac{1}{6} r\nu^3 + \mathcal{O}(\nu^3), \\
\theta_Y &= \frac{1}{6} \tau^2 \nu^3 + \mathcal{O}(\nu^3), \\
\theta_Z &= \frac{1}{6} (\tau + r)\nu^3 + \mathcal{O}(\nu^3), \\
\theta_W &= \frac{1}{6} (2\tau + r)\nu^3 + \mathcal{O}(\nu^3), \\
\theta_\beta &= \frac{1}{6} (\tau + 2r)\nu^3 + \mathcal{O}(\nu^3), \\
\omega &= f(1) = \frac{1}{2} (\tau + r)\nu^2 + \mathcal{O}(\nu^2),
\end{aligned}$$

where ω is the lattice dimension.

Applying the LLL reduction algorithm to M produces a reduced basis with the same determinant, yielding ω polynomials that satisfy

$$F_t(x, y, z, w) \equiv 0 \bmod \beta^\nu, 1 \leq t \leq \omega.$$

Using Equation (1) (resulted from Theorems 1 and 2) we get

$$X^{\theta_X} Y^{\theta_Y} Z^{\theta_Z} W^{\theta_W} \beta^{\theta_\beta} < \beta^{\nu(\omega-3)}. \tag{3}$$

Case 1 ($CZ \leq XY^r$) In this case we have $|w_0| \leq 2 \cdot XY^r = 2 \cdot \beta^{\delta+r\gamma}$. Therefore, Equation (3) is equivalent to

$$\beta^{\frac{\delta}{6}r\nu^3} \cdot \beta^{\frac{\gamma}{6}\tau^2\nu^3} \cdot \beta^{\frac{\lambda}{6}(\tau+r)\nu^3} \cdot \beta^{\frac{\delta+r\gamma}{6}(2\tau+r)\nu^3} \cdot \beta^{\frac{1}{6}(\tau+2r)\nu^3} < \beta^{\frac{1}{2}(\tau+r)\nu^3}.$$

It follows

$$\begin{aligned} \delta r + \gamma\tau^2 + \lambda(\tau + r) + (\delta + r\gamma)(2\tau + r) + (\tau + 2r) - 3(\tau + r) < 0 \Leftrightarrow \\ \delta r + \gamma\tau^2 + \lambda\tau + \lambda r + 2\delta\tau + 2r\gamma\tau + \delta r + \gamma r^2 + \tau + 2r - 3\tau - 3r < 0 \Leftrightarrow \\ \gamma\tau^2 + (\lambda + 2\delta + 2r\gamma - 2)\tau + 2\delta r + \lambda r + \gamma r^2 - r < 0. \end{aligned} \tag{4}$$

The optimal point is $\tau_0 = -\frac{\lambda+2\delta+2r\gamma-2}{2\gamma}$, which has to be positive. Hence, it follows that

$$\gamma \leq \frac{1 - \delta - 0.5\lambda}{r}.$$

Subcase 1.a ($r\gamma = 1 - \delta - 0.5\lambda$): In this case we obtain that $\tau_0 = 0$. Therefore, Equation (4) becomes

$$2\delta + \lambda + \gamma r - 1 < 0 \Leftrightarrow 2\delta + \lambda + 1 - \delta - 0.5\lambda - 1 = \delta + 0.5\lambda < 0,$$

which is a contradiction.

Subcase 1.b ($r\gamma < 1 - \delta - 0.5\lambda$): We introduce the value τ_0 in Equation (4) and we obtain

$$\begin{aligned} -\frac{(\lambda + 2\delta + 2r\gamma - 2)^2}{4\gamma} + 2\delta r + \lambda r + \gamma r^2 - r < 0 \Leftrightarrow \\ -\lambda^2 - 4\delta^2 - 4\gamma^2 r^2 - 4 - 4\lambda\delta - 4r\lambda\gamma + 4\lambda - 8r\delta\gamma + 8\delta + 8r\gamma \\ +8r\delta\gamma + 4r\lambda\gamma + 4\gamma^2 r^2 - 4r\gamma < 0 \Leftrightarrow \\ -\lambda^2 - 4\delta^2 - 4 - 4\lambda\delta + 4\lambda + 8\delta + 4r\gamma < 0 \Leftrightarrow \\ -(1 - \delta - 0.5\lambda)^2 + r\gamma < 0 \Leftrightarrow \\ 1 - 0.5\lambda - \sqrt{r\gamma} > \delta, \end{aligned}$$

since from the hypothesis of this subcase we have $0 < 1 - \delta - 0.5\lambda$. Therefore, it follows that

$$\delta < \min(1 - 0.5\lambda - \sqrt{r\gamma}, 1 - 0.5\lambda - r\gamma) = 1 - 0.5\lambda - \sqrt{r\gamma},$$

if $1 > r\gamma$. The last thing that we need to ensure is that $\delta > 0$. Hence, we have

$$1 - 0.5\lambda - \sqrt{r\gamma} > 0 \Leftrightarrow 1 > 0.5\lambda + \sqrt{r\gamma},$$

just as desired.

Case 2 ($CZ > XY^r$) In this case we have $|w_0| < 2 \cdot CZ = 2 \cdot \beta^{\lambda+\varepsilon}$. Therefore, Equation (3) is equivalent to

$$\beta^{\frac{\delta}{6}r\nu^3} \cdot \beta^{\frac{\gamma}{6}\tau^2\nu^3} \cdot \beta^{\frac{\lambda}{6}(\tau+r)\nu^3} \cdot \beta^{\frac{\lambda+\varepsilon}{6}(2\tau+r)\nu^3} \cdot \beta^{\frac{1}{6}(\tau+2r)\nu^3} < \beta^{\frac{1}{2}(\tau+r)\nu^3}.$$

It follows

$$\begin{aligned} \delta r + \gamma\tau^2 + \lambda(\tau + r) + (\lambda + \varepsilon)(2\tau + r) + (\tau + 2r) - 3(\tau + r) < 0 \Leftrightarrow \\ \delta r + \gamma\tau^2 + \lambda\tau + \lambda r + 2\lambda\tau + 2\varepsilon\tau + \lambda r + \varepsilon r + \tau + 2r - 3\tau - 3r < 0 \Leftrightarrow \\ \gamma\tau^2 + (3\lambda + 2\epsilon - 2)\tau + \delta r + 2\lambda r + \varepsilon r - r < 0. \end{aligned} \quad (5)$$

The optimal point is $\tau_0 = -\frac{3\lambda+2\varepsilon-2}{2\gamma}$, which has to be positive. Hence, it follows that $1.5\lambda + \varepsilon \leq 1$.

Subcase 2.a ($1.5\lambda + \varepsilon = 1$): In this case we obtain that $\tau_0 = 0$. Therefore, Equation (5) becomes

$$\delta + 2\lambda + \varepsilon - 1 < 0 \Leftrightarrow \delta + 2\lambda + 1 - 1.5\lambda - 1 = \delta + 0.5\lambda < 0,$$

which is a contradiction.

Subcase 2.b ($1.5\lambda + \varepsilon < 1$): We introduce the value τ_0 in Equation (5) and we obtain

$$\begin{aligned} -\frac{(3\lambda + 2\varepsilon - 2)^2}{4\gamma} + \delta r + 2\lambda r + \varepsilon r - r < 0 \Leftrightarrow \\ \frac{(3\lambda + 2\varepsilon - 2)^2}{4\gamma r} + 1 - \varepsilon - 2\lambda > \delta. \end{aligned}$$

The last thing that we need to ensure is that $\delta > 0$. Since $2\lambda + \varepsilon < 1$, we obtain our result. □

3.1 Related Work

3.1.1 Solving the Equation $xH(y) + c \equiv 0 \bmod \beta$

When $\lambda = 0$ we obtain the following result from [1] as a corollary of our main theorem.

Corollary 1. *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 $|x_0| < X = \beta^\delta, |y_0| < Y = \beta^\gamma, |c| \leq C$,*

– $C < XY^r$,

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

$$\delta \leq 1 - \sqrt{r\gamma}, \quad \textit{when } r\gamma \leq 1.$$

Remark 3. In [18], the author proves a similar bound, namely

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

Using a different lattice construction, the authors of [1] simplify this bound (see Corollary 1).

We could not find a direct comparison between the bounds presented in [1,18], and therefore we provide such an analysis. The only difference occurs in the case $0 < \gamma < r/(r+1)^2$. In this range, we compare

$$\frac{r+2}{2(r+1)} - \frac{r+1}{2}\gamma < 1 - \sqrt{r\gamma}.$$

Hence, we have

$$\begin{aligned} & r + 2 - (r+1)^2\gamma < 2r + 2 - 2(r+1)\sqrt{r\gamma} \Leftrightarrow \\ & 0 < (r+1)^2\gamma - 2(r+1)\sqrt{\gamma} \cdot \sqrt{r} + r \Leftrightarrow \\ & 0 < (\sqrt{r} - (r+1)\sqrt{\gamma})^2. \end{aligned}$$

Therefore, Corollary 1 improves on Kunihiro's result.

We further provide a corollary for the case $C > XY^r$.

Corollary 2. *Let* $H(y) \in \mathbb{Z}[y]$ *be a monic polynomial of degree* $r \geq 1$ *and* β *be an integer. Suppose that*

– $x_0 H(y_0) + c \equiv 0 \bmod \beta$ *for some* $|x_0| < X = \beta^\delta, |y_0| < Y = \beta^\gamma$, $|c| \leq C = \beta^\varepsilon$,
– $C > XY^r$,

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

$$\delta \leq 1 - \varepsilon + \frac{(1-\varepsilon)^2}{r\gamma} \textit{ when } \varepsilon < 1.$$

Remark 4. The case $C > XY^r$ was previously considered in [18]. Compared to our result, the author directly approximates $|c|$ by β and derives a contradiction.

Using a different method, the authors of [27,30] resolve the equation without imposing any restriction on c as in Corollaries 1 and 2. We further present a rewritten version of the result from [27,30].[4]

[4] Note that the proof in [30] is a more detailed version of the proof in [27].

Theorem 6. *Let $H(y) \in \mathbb{Z}[y]$ be a monic polynomial of degree $r \geq 1$ and β be an integer. Suppose that*

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

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

$$\delta \leq \frac{1}{3} r\gamma + 1 - \frac{2}{3}\sqrt{r^2\gamma^2 + 3r\gamma}, \quad \text{when } \gamma \leq \frac{1-\delta}{r}.$$

Comparison between Corollary 1 and Theorem 6. To compare the two theorems, we have to check if

$$1 - \sqrt{r\gamma} > \frac{1}{3} r\gamma + 1 - \frac{2}{3}\sqrt{r^2\gamma^2 + 3r\gamma}.$$

Therefore, we have

$$\begin{aligned} &2\sqrt{r^2\gamma^2 + 3r\gamma} > r\gamma + 3\sqrt{r\gamma} \Leftrightarrow \\ &4r^2\gamma^2 + 12r\gamma > r^2\gamma^2 + 9r\gamma + 6r\gamma\sqrt{r\gamma} \Leftrightarrow \\ &(r\gamma - \sqrt{r\gamma})^2 > 0. \end{aligned}$$

To conclude, when $C < XY^r$ we obtain a better bound by using Corollary 1, otherwise we should use Theorem 6.

Comparison between Corollary 2 and Theorem 6. We assume that $\gamma \geq 3\varepsilon/r$ and we would like to prove that

$$1 - \varepsilon + \frac{(1-\varepsilon)^2}{r\gamma} > \frac{1}{3} r\gamma + 1 - \frac{2}{3}\sqrt{r^2\gamma^2 + 3r\gamma}.$$

Using our assumption we have

$$r^2\gamma^2 \geq 3\varepsilon r\gamma > 3\varepsilon r\gamma - 3(1-\varepsilon)^2,$$

which leads to

$$2r\gamma\sqrt{r^2\gamma^2 + 3r\gamma} > 2r^2\gamma^2 > r^2\gamma^2 + 3\varepsilon r\gamma - 3(1-\varepsilon)^2,$$

just as desired.

As a conclusion, we further provide a theorem that incorporates Corollaries 1 and 2 and Theorem 6. Note that in practice, when $C > XY^r$, one first tries to apply Corollary 2 and if that fails it applies Theorem 6.

Theorem 7. *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* $|x_0| < X = \beta^\delta, |y_0| < Y = \beta^\gamma$, $|c| \leq C = \beta^\varepsilon$

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

$$\begin{cases} \delta \leq 1 - \sqrt{r\gamma}, & \text{when } C < XY^r, \gamma \leq \frac{1}{r}, \\ \delta \leq 1 - \varepsilon + \frac{(1-\varepsilon)^2}{r\gamma}, & \text{when } C > XY^r, \frac{3\varepsilon}{r} \leq \gamma, \varepsilon < 1 \\ \delta \leq \frac{1}{3} r\gamma + 1 - \frac{2}{3}\sqrt{r^2\gamma^2 + 3r\gamma}, & \text{when } C > XY^r, \gamma < \min\left(\frac{3\varepsilon}{r}, \frac{1-\delta}{r}\right). \end{cases}$$

3.1.2 Solving the Equation $xH(y) + z \equiv 0 \bmod \beta$

A method for solving the generalization of equation $xH(y) + c \equiv 0 \bmod \beta$ is provided in [28]. We also present this result in rewritten form as a corollary of our main result (*i.e.* $\varepsilon = 0$).

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

- $x_0 H(y_0) + z_0 \equiv 0 \bmod \beta$ *for some* $|x_0| < X = \beta^{\delta}, |y_0| < Y = \beta^{\gamma}$, $|z_0| < Z = \beta^{\lambda}$,
- $Z < XY^r$,

then one can solve the equation $xH(y) + z \equiv 0 \bmod \beta$ if

$$\delta \leq 1 - 0.5\lambda - \sqrt{r\gamma}, \quad \textit{when } 0.5\lambda + \sqrt{r\gamma} < 1.$$

3.1.3 Solving the Equation $xy + bx \equiv cz \bmod \beta$

A method for solving the equation $xy + bx \equiv cz \bmod \beta$ is provided in [29]. Considering $r = 1$ and $H(y) = y + b$ in Theorem 5 we obtain their exact result.

Corollary 4. *Let β be an integer. Suppose that*

- $x_0 y_0 + b x_0 \equiv c z_0 \bmod \beta$ *for some* $|x_0| < X = \beta^{\delta}, |y_0| < Y = \beta^{\gamma}$, $|z_0| < Z = \beta^{\lambda}, |c| \leq C$,
- $CZ < XY$,

then one can solve the equation $xy + bx \equiv cz \bmod \beta$ if

$$\delta \leq 1 - 0.5\lambda - \sqrt{\gamma}, \quad \textit{when } 0.5\lambda + \gamma < 1.$$

4 Applying Lattices to RSA Variants

In this section, we apply our main result to different attack scenarios and connect previous results to those introduced in this work. Note that we only prove our results for type-A variants, since the proofs for type-B ones are similar.

4.1 No Partial Information

We further assume that the attacker has access only to the public key and no additional partial information.

Theorem 8. *Let $N = pq$ be the product of two unknown primes with $q < p < 2q$. Also, let $e = N^{\delta}$. Assuming that $e \equiv z_0 u_0^{-1} \bmod \varphi_n(N)$, then for type-A variants, we can factor N in polynomial time if*

$$\begin{cases} \gamma_1 \leq n - 0.5\gamma_2 - \sqrt{0.5n\delta}, & \textit{when } \gamma_2 < \min(\delta + \gamma_1 - 0.5n, 2\delta - \sqrt{2n\delta}) \\ \gamma_1 \leq 0.5(n - \delta), & \textit{when } \delta + \gamma_1 - 0.5n < \gamma_2 < 0.5\delta \end{cases}$$

where $|u_0| \leq N^{\gamma_1}$ *and* $|z_0| \leq N^{\gamma_2}$ *with* $\gamma_2 < \delta + \gamma_1$. *For type-B variants we assume that* $e \equiv z_0 u_0^{-1} \bmod \psi_n(N)$ *and we obtain the bounds*

$$\begin{cases} \gamma_1 \leq n - 1 - 0.5\gamma_2 - \sqrt{0.5(n-1)\delta}, \\ \qquad\qquad when\ \gamma_2 < \min(\delta + \gamma_1 - 0.5(n-1), 2\delta - \sqrt{2(n-1)\delta}) \\ \gamma_1 \leq 0.5(n - 1 - \delta), \\ \qquad\qquad when\ \delta + \gamma_1 - 0.5(n-1) < \gamma_2 < 0.5\delta. \end{cases}$$

Proof. According to our hypothesis, there exist an integer x_0 such that

$$eu_0 + x_0\varphi_n(N) = z_0. \tag{6}$$

According to Proposition 1 with $M = 0$ we have that

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

where $a_k \in \mathbb{Z}$. We define the monic polynomials

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

and $H(y) = -h(y)$.

By rewriting Equation (6), we obtain the congruence $x_0\varphi_n(N) - z_0 \equiv 0 \bmod e$, that is equivalent to $x_0(-\varphi_n(N)) + z_0 \equiv 0 \bmod e$. Consequently, we deduce the equation $xH(y) + z \equiv 0 \bmod e$, which has x_0, $y_0 = p + q$ and z_0 as solutions.

In order to be able to apply Theorem 5 we first need to bound the solutions. Note that $|z_0| \leq e^{\gamma_2/\delta}$. Using Lemma 2 we have that $p + q < 3\sqrt{N}$. Therefore, $y_0 = p + q < Y \simeq e^{1/2\delta}$.

From Equation (6) and Corollary 5 it follows that

$$|x_0| = \frac{|z_0 - eu_0|}{\varphi_n(N)} \leq \frac{|z_0| + |eu_0|}{\varphi_n(N)} \leq N^{-n}(|z_0| + |eu_0|). \tag{7}$$

We further consider two cases.

Case 1 ($\gamma_2 < \delta + \gamma_1$) In this case, from Equation (7) we obtain that $|x_0| \leq 2N^{\delta+\gamma_1-n} = 2e^{(\delta+\gamma_1-n)/\delta}$. We further apply Theorem 5 by taking the monic polynomial $H(y)$ of degree n and $X = e^{(\delta+\gamma_1-n)/\delta}, Y = e^{1/2\delta}, Z = e^{\gamma_2/\delta}, c = 1, \varepsilon = 0$. Therefore, we can find (x_0, y_0, z_0) in polynomial time in the following two situations.

Subcase 1.a ($\gamma_2 \leq \delta + \gamma_1 - 0.5n$) In this case, we have that $Z \leq XY^n$ and we can find the solutions if

$$\frac{\delta + \gamma_1 - n}{\delta} \leq 1 - \frac{\gamma_2}{2\delta} - \frac{\sqrt{n}}{\sqrt{2\delta}} \Leftrightarrow \delta + \gamma_1 - n \leq \delta - 0.5\gamma_2 - \sqrt{0.5n\delta}$$
$$\Leftrightarrow \gamma_1 \leq n - 0.5\gamma_2 - \sqrt{0.5n\delta}$$

and $0.5\gamma_2 + \sqrt{0.5n\delta} < \delta$. Therefore, we obtain

$$\gamma_2 < \min(\delta + \gamma_1 - 0.5n, 2\delta - \sqrt{2n\delta}).$$

Subcase 1.b ($\gamma_2 > \delta + \gamma_1 - 0.5n$) In this case we have $Z > XY^n$ and we can find the solutions if

$$\frac{\delta + \gamma_1 - n}{\delta} \leq 1 - \frac{2\gamma_2}{\delta} + \frac{(2\delta - 3\gamma_2)^2}{2n\delta} \Leftrightarrow \delta + \gamma_1 - n \leq \delta - 2\gamma_2 + \frac{(2\delta - 3\gamma_2)^2}{2n}$$
$$\Leftrightarrow \gamma_1 \leq n - 2\gamma_2 + \frac{(2\delta - 3\gamma_2)^2}{2n}$$

and $\gamma_2 < \delta/2$. Since the following condition must be satisfied

$$\delta + \gamma_1 - 0.5n < \gamma_2 < 0.5\delta \Leftrightarrow \gamma_1 < 0.5(n - \delta),$$

we obtain

$$\gamma_1 \leq \min\left(n - 2\gamma_2 + \frac{(2\delta - 3\gamma_2)^2}{2n}, \frac{n-\delta}{2}\right) = \frac{n-\delta}{2},$$

which is true since $n > \delta > 2\gamma_2$.

Case 2 ($\gamma_2 > \delta + \gamma_1$) From Equation (7) it follows $|x_0| < 2N^{\gamma_2 - n}$. Hence, we have that $x_0 < X = e^{(\gamma_2 - n)/\delta}$. Note that the case $\gamma_2 \leq \gamma_2 - 0.5n$ (*i.e.* $Z \leq XY^n$) leads to a contradiction. Therefore, we only consider the case $\gamma_2 > \gamma_2 - 0.5n$ (*i.e.* $Z > XY^n$). In this case, one condition we must satisfy is $\gamma_2 < \delta/2$. Thus, we have

$$\delta + \gamma_1 < \gamma_2 < 0.5\delta \Leftrightarrow 0.5\delta + \gamma_1 < 0,$$

which is a contradiction.

Note that, 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. □

We further provide a result that works directly with the secret exponent d. The proof is given in Appendix B.

Theorem 9. *Let $N = pq$ be the product of two unknown primes with $q < p < 2q$. Also, let $e = N^\delta$. Assuming that $e \equiv d^{-1} \bmod \varphi_n(N)$, then for type-A variants, we can factor N in polynomial time if*

$$\begin{cases} \gamma \leq n - \sqrt{0.5n\delta}, & \text{when } 0.5n < \delta \\ \gamma \leq 0.5n - \delta, & \text{when } 0.5n > \delta \end{cases}$$

where $|d| \leq N^\gamma$. For type-B variants we assume that $e \equiv d^{-1} \bmod \psi_n(N)$ and we obtain the bounds

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

4.1.1 Related Work

In [28], the authors assume that $e \equiv z_0 u_0^{-1} \bmod \psi_n(N)$ and use Corollary 3 to derive their bound, *i.e.*

$$\gamma_1 \leq n - 1 - 0.5\gamma_2 - \sqrt{0.5(n-1)\delta}.$$

In the case of φ_n, the authors of [29] use Corollary 4 to derive the bound

$$\gamma_1 \leq n - 0.5\gamma_2 - \sqrt{0.5n\delta}.$$

Note that both bounds are a special case of Theorem 8.

We further consider that $u_0 = d$, $\gamma_1 = \gamma$ and $\gamma_2 = 0$. Applying Corollary 1 to type-A and type-B key equations we obtain the bounds from [30,35] and [1], respectively. Namely,

$$\gamma \leq n - \sqrt{0.5n\delta}, \quad \text{when } \frac{n}{2} \leq \delta \leq 2n,$$

for type-A variants, while for type-B variants we have

$$\gamma \leq n - 1 - \sqrt{0.5(n-1)\delta}, \quad \text{when } \frac{n-1}{2} \leq \delta \leq 2(n-1).$$

For $n = 3$, the type-B bound of [39] for Murru-Saettone's scheme is recovered. For type-A variants with $e \simeq N^n$ and $n = 1, 2$, the optimal bounds of [3,15] for RSA and [26,38] for Elkamchouchi *et al.*'s scheme are obtained.

4.2 Known Approximation of p

We further provide a method for finding the factorization of N when the attacker knows an approximation $\tilde{p}$ of p.

Theorem 10. *Let $N = pq$ be the product of two unknown primes with $q < p < 2q$ and $\tilde{p}$ be an approximation of p with $|p - \tilde{p}| \leq N^\lambda$. Also, let $e = N^\delta$. Assuming that $e \equiv z_0 u_0^{-1} \bmod \varphi_n(N)$, then for type-A variants, we can factor N in polynomial time if*

$$\begin{cases} \gamma_1 \leq n - 0.5\gamma_2 - \sqrt{n\lambda\delta}, & \text{when } \gamma_2 < \min(\delta + \gamma_1 - n(1-\lambda), 2\delta - 2\sqrt{n\lambda\delta}) \\ \gamma_1 \leq n(1-\lambda) - 0.5\delta, & \text{when } \delta + \gamma_1 - n(1-\lambda) < \gamma_2 < \lambda\delta, \end{cases}$$

where $|u_0| \leq N^{\gamma_1}, |z_0| \leq N^{\gamma_2}$ with $\gamma_2 \leq \delta + \gamma_1$. For type-B variants, we assume that $e \equiv z_0 u_0^{-1} \bmod \psi_n(N)$ and we obtain the bounds

$$\begin{cases} \gamma_1 \leq n - 1 - 0.5\gamma_2 - \sqrt{(n-1)\lambda\delta}, \\ \qquad \text{when } \gamma_2 < \min(\delta + \gamma_1 - (n-1)(1-\lambda), 2\delta - 2\sqrt{(n-1)\lambda\delta}) \\ \gamma_1 \leq (n-1)(1-\lambda) - 0.5\delta, \\ \qquad \text{when } \delta + \gamma_1 - (n-1)(1-\lambda) < \gamma_2 < \lambda\delta. \end{cases}$$

Proof. From the hypothesis, it follows that there exists an integer x_0 such that

$$eu_0 + x_0\varphi_n(N) = z_0. \tag{8}$$

Since $\tilde{p}$ approximates p, it follows from Lemma 3 that $\tilde{q} = \lfloor N/\tilde{p} \rfloor$ approximates q and we have

$$|q - \tilde{q}| < N^{\lambda} \text{ and } |p + q - \tilde{p} - \tilde{q}| < |p - \tilde{p}| + |q - \tilde{q}| < 2N^{\lambda}.$$

Using Proposition 1 with $M = \tilde{p} + \tilde{q}$, we obtain integers a_k such that

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

Thus, we define the polynomial $H(y) = y^n - \sum_{k=0}^{n-1} a_k y^k \in \mathbb{Z}[y]$. From Equation (8) it follows that $x_0 H(y_0) + z_0 = eu_0$, where $y_0 = p + q - \tilde{p} - \tilde{q}$ and $|y_0| \leq 2N^{\lambda}$.

From Equation (8) and Corollary 5 it follows

$$|x_0| = \frac{|z_0 - eu_0|}{\varphi_n(N)} \leq \frac{|z_0| + |eu_0|}{\varphi_n(N)} \leq N^{-n}(|z_0| + |eu_0|). \tag{9}$$

We further consider two cases.

Case 1 ($\gamma_2 < \delta + \gamma_1$) From Equation (9) we obtain that $|x_0| \leq 2N^{\delta+\gamma_1-n} = e^{(\delta+\gamma_1-n)/\delta}$. We further apply Theorem 5 by taking the monic polynomial $H(y)$ of degree n and $X = e^{(\delta+\gamma_1-n)/\delta}, Y = e^{\lambda/\delta}, Z = e^{\gamma_2/\delta}, c = 1, \varepsilon = 0$. Therefore, we can find (x_0, y_0, z_0) in polynomial time in the following two situations.

Subcase 1.a ($\gamma_2 \leq \delta + \gamma_1 - n + \lambda n$) In this case, we have $Z \leq XY^n$ and we can find the solutions if

$$\begin{aligned} \frac{\delta + \gamma_1 - n}{\delta} \leq 1 - \frac{\gamma_2}{2\delta} - \sqrt{\frac{\lambda n}{\delta}} &\Leftrightarrow \delta + \gamma_1 - n \leq \delta - 0.5\gamma_2 - \sqrt{n\lambda\delta} \\ &\Leftrightarrow \gamma_1 \leq n - 0.5\gamma_2 - \sqrt{n\lambda\delta} \end{aligned}$$

and $0.5\gamma_2 + \sqrt{n\lambda\delta} < \delta$. Therefore, we obtain

$$\gamma_2 < \min(\delta + \gamma_1 - n + \lambda n, 2\delta - 2\sqrt{n\lambda\delta}).$$

Subcase 1.b ($\gamma_2 > \delta + \gamma_1 - n + \lambda n$) In this case, we have $Z > XY^n$ and we can find the solutions if

$$\begin{aligned} \frac{\delta + \gamma_1 - n}{\delta} \leq 1 - \frac{2\gamma_2}{\delta} + \frac{(\delta - 1.5\gamma_2)^2}{n\lambda\delta} &\Leftrightarrow \delta + \gamma_1 - n \leq \delta - 2\gamma_2 + \frac{(\delta - 1.5\gamma_2)^2}{n\lambda} \\ &\Leftrightarrow \gamma_1 \leq n - 2\gamma_2 + \frac{(\delta - 1.5\gamma_2)^2}{n\lambda} \end{aligned}$$

and $\gamma_2 < 0.5\delta$. Since the following condition must be satisfied

$$\delta + \gamma_1 - n + \lambda n < \gamma_2 < 0.5\delta \Leftrightarrow \gamma_1 < n(1-\lambda) - 0.5\delta,$$

we obtain

$$\begin{aligned}\gamma_1 &\leq \min\left(n - 2\gamma_2 + \frac{(\delta - 1.5\gamma_2)^2}{n\lambda}, n(1-\lambda) - 0.5\delta\right)\\ &= n(1-\lambda) - 0.5\delta,\end{aligned}$$

which is true since we imposed the condition $\lambda n > \lambda\delta > \gamma_2$.

Case 2 ($\gamma_2 > \delta + \gamma_1$) From Equation (9) it follows $|x_0| < 2N^{\gamma_2 - n}$. We use again Theorem 5 for $H(y)$ and $X = e^{\frac{\gamma_2 - n}{\delta}}, Y = e^{\frac{\lambda}{\delta}}, Z = e^{\frac{\gamma_2}{\delta}}, c = 1, \varepsilon = 0$. Note that the case $\gamma_2 \leq \gamma_2 - n(1-\lambda)$ (*i.e* $Z \leq XY^n$) leads to a contradiction since $0 \leq \lambda \leq 0.5$. Now we consider the subcase $\gamma_2 > \gamma_2 - n(1-\lambda)$. In this situation, it follows

$$\delta + \gamma_1 < \gamma_2 < 0.5\delta \Leftrightarrow 0.5\delta + \gamma_1 < 0,$$

which is a contradiction.

We obtain $y_0 = p + q - \tilde{p} - \tilde{q}$, and therefore $p + q$. Since we know $N = pq$, we can find the values p and q. □

We further provide a result that works directly with the secret exponent d. The proof is given in Appendix C.

Theorem 11. *Let $N = pq$ be the product of two unknown primes with $q < p < 2q$ and $\tilde{p}$ be an approximation of p with $|p - \tilde{p}| \leq N^{\lambda}$. Also, let $e = N^{\delta}$. Assuming that $e \equiv d^{-1} \bmod \varphi_n(N)$, then for type-A variants, we can factor N in polynomial time if*

$$\begin{cases}\gamma \leq n - \sqrt{n\delta\lambda}, & \text{when } \max(n\lambda, n(1-\lambda)) < \delta\\ \gamma \leq n(1-\lambda) - \delta, & \text{when } n(1-\lambda) > \delta,\end{cases}$$

where $|d| \leq N^{\gamma}$. For type-B variants, we assume that $e \equiv d^{-1} \bmod \psi_n(N)$ and we obtain the bounds

$$\begin{cases}\gamma \leq n - 1 - \sqrt{(n-1)\delta\lambda}, & \text{when } \max((n-1)\lambda, (n-1)(1-\lambda)) < \delta\\ \gamma \leq (n-1)(1-\lambda) - \delta, & \text{when } (n-1)(1-\lambda) > \delta,\end{cases}$$

4.2.1 Related Work

In [36], the author uses Kunihiro's result [18] to derive a bound for φ_n when a known approximation for p is known. Using Theorem 11, the bound from [36] can be simplified to

$$\gamma \leq n - \sqrt{n\lambda\delta}.$$

In the case of ψ_n, using Theorem 10 we recover a result from [28], namely

$$\gamma_1 \leq n - 1 - 0.5\gamma_2 - \sqrt{(n-1)\lambda\delta}.$$

If we use Theorem 11, we obtain the bound

$$\gamma \leq (n-1)(1-\lambda) - \delta, \tag{10}$$

derived from the case $Z > XY^n$ of Theorem 7. The authors of [27], use Theorem 6 to derive the bound

$$\gamma \leq \left(1 + \frac{\lambda}{3}\right)(n-1) - \frac{2}{3}\sqrt{(n-1)^2\lambda^2 + 3(n-1)\lambda\delta}. \tag{11}$$

Looking at Theorem 7 we can see that Equation (11) is better than Equation (10) when $\gamma < 0$. Therefore, the bound Equation (10) is better.

4.3 Primes Sharing the Least Significant Bits

We further provide a factorization method for N when the two primes share an amount of the least significant bits.

Theorem 12. *Let $N = pq$ be the product of two unknown primes with $q < p < 2q$ such that p and q share their s least significant bits. Also, let $e = N^\delta$ and $2^s = N^\alpha$, where $\alpha \in [0, 1/4)$. Assuming that $e \equiv z_0 u_0^{-1} \bmod \varphi_n(N)$, for type-A variants, we can factor N in polynomial time if*

$$\begin{cases} \gamma_1 \leq n - 0.5\gamma_2 - \sqrt{\delta n(0.5 - 2\alpha)}, \\ \qquad\qquad \text{when } \gamma_2 < \min\left(\delta + \gamma_1 - 0.5n, 2\delta - \sqrt{2n\delta(1-4\alpha)}\right), \\ \gamma_1 < n(0.5+\alpha) - 0.5\delta, \\ \qquad\qquad \text{when } \delta + \gamma_1 - 0.5n < \gamma_2 < 0.5\delta + n\alpha \text{ and } \delta < n(1-2\alpha), \end{cases}$$

where $|u_0| \leq N^{\gamma_1}, |z_0| \leq N^{\gamma_2}$. Also, when $\gamma_2 < n\alpha + 0.5\delta$ and $\gamma_1 < n\alpha - 0.5\delta$ we can factor N if

$$0 \leq \delta + n(1+2\alpha) - 3\gamma_2 + \frac{(\delta - 1.5\gamma_2 - 2n\alpha)^2}{n(0.5-2\alpha)}.$$

For type-B variants we assume that $e \equiv z_0 u_0^{-1} \bmod \psi_n(N)$ and we obtain the bounds

$$\begin{cases} \gamma_1 \leq n - 1 - 0.5\gamma_2 - \sqrt{\delta(n-1)(0.5 - 2\alpha)}, \\ \quad \text{when } \gamma_2 < \min\left(\delta + \gamma_1 - 0.5(n-1), 2\delta - \sqrt{2(n-1)\delta(1-4\alpha)}\right), \\ \gamma_1 < (n-1)(0.5+\alpha) - 0.5\delta, \\ \quad \text{when } \delta + \gamma_1 - 0.5(n-1) < \gamma_2 < 0.5\delta + (n-1)\alpha \text{ and } \delta < (n-1)(1-2\alpha), \end{cases}$$

and

$$0 \leq \delta + (n-1)(1+2\alpha) - 3\gamma_2 + \frac{(\delta - 1.5\gamma_2 - 2(n-1)\alpha)^2}{(n-1)(0.5-2\alpha)},$$

where $\gamma_2 < (n-1)\alpha + 0.5\delta$ and $\gamma_1 < (n-1)\alpha - 0.5\delta$.

Proof. Since p and q share their s least significant bits, there exists an integer t such that $p - q = 2^s t$. From Lemma 4 it follows that we can write $p = p_1 \cdot 2^s + w_0, q = q_1 \cdot 2^s + w_0$ and $p + q = v_1 \cdot 2^{2s} + v_0$, where w_0 is a solution of the equation $x^2 \equiv N \bmod 2^s$, $v_0 \equiv 2w_0 + (N - w_0^2)w_0^{-1} \bmod 2^{2s}$ and p_1, q_1, v_1 are some integers. From Proposition 1 with $M = v_0$ it follows

$$\varphi_n(N) = -2^{2sn} v_1^n + \sum_{j=0}^{n-1} a_j v_1^j, \tag{12}$$

where $a_j \in \mathbb{Z}$ depends only on N, n, s and v_0, for all $j \in \{0, 1, \ldots, n-1\}$. We observe that

$$|v_1| = \frac{|p + q - v_0|}{2^{2s}} < \frac{|p + q|}{2^{2s}} \leq 3 \cdot N^{1/2 - 2\alpha},$$

where we used Lemma 2. Since $1/2 - 2\alpha$ has to be positive, it follows the condition $\alpha \in [0, 1/4)$. From our hypothesis there exists an integer x_0 such that $eu_0 + x_0\varphi_n(N) = z_0$ and using Equation (12) we obtain

$$x_0 \cdot \left(-2^{2sn} v_1^n + \sum_{j=0}^{n-1} a_j v_1^j \right) \equiv z_0 \bmod e \Leftrightarrow$$

$$x_0 \cdot \left(v_1^n - \sum_{j=0}^{n-1} b_j v_1^j \right) + z_0 2^{-2sn} \equiv 0 \bmod e, \tag{13}$$

where $b_j = a_j \cdot 2^{-2sn}$. Observe that the last identity is valid because $\gcd(e, 2) = 1$. We define the polynomial $H(y) = y^n - \sum_{j=0}^{n-1} b_j y^j$ and denote the integer $c = 2^{-2sn} = e^{-2n\alpha/\delta}$. Then from Equation (13) it follows that (x_0, v_1, z_0) is a solution of the equation $xH(y) + cz \equiv 0 \bmod e$.

From the equality $eu_0 + x_0\varphi_n(N) = z_0$ it follows

$$|x_0| = \frac{|eu_0 - z_0|}{\varphi_n(N)} < N^{-n}(e|u_0| + |z_0|) \tag{14}$$

We further consider two cases.

Case 1 ($\gamma_2 < \delta + \gamma_1$) In this case, Equation (14) becomes $|x_0| < 2N^{\delta + \gamma_1 - n}$. Thus, we can apply Theorem 5 for $X = e^{(\delta + \gamma_1 - n)/\delta}, Y = e^{(0.5 - 2\alpha)/\delta}, Z = e^{\gamma_2/\delta}, |c| = C = e^{-2n\alpha/\delta}$ to find the values of x_0, $y_0 = v_1$ and z_0 in polynomial time if the following situations hold.

Subcase 1.a ($\gamma_2 \leq \delta + \gamma_1 - 0.5n$) In this case, we have $CZ \leq XY^n$ and it follows that

$$\frac{\delta + \gamma_1 - n}{\delta} \leq 1 - \frac{\gamma_2}{2\delta} - \sqrt{\frac{n(0.5 - 2\alpha)}{\delta}} \Leftrightarrow$$

$$\delta + \gamma_1 - n \leq \delta - 0.5\gamma_2 - \sqrt{\delta n(0.5 - 2\alpha)} \Leftrightarrow$$

$$\gamma_1 \leq n - 0.5\gamma_2 - \sqrt{\delta n(0.5 - 2\alpha)},$$

if $\gamma_2 < 2\delta - \sqrt{2n\delta(1-4\alpha)}$. So, it follows

$$\gamma_2 < \min\left(\delta + \gamma_1 - 0.5n, 2\delta - \sqrt{2n\delta(1-4\alpha)}\right)$$

Subcase 1.b ($\gamma_2 > \delta + \gamma_1 - 0.5n$) In this case, we have $CZ > XY^n$ and it follows

$$\begin{aligned}\frac{\delta+\gamma_1-n}{\delta} &\leq 1 - \frac{2\gamma_2}{\delta} + \frac{2n\alpha}{\delta} + \frac{(\delta - 1.5\gamma_2 + 2n\alpha)^2}{\delta n(0.5-2\alpha)} \Leftrightarrow \\ \delta+\gamma_1-n &\leq \delta - 2\gamma_2 + 2n\alpha + \frac{(\delta - 1.5\gamma_2 + 2n\alpha)^2}{n(0.5-2\alpha)} \Leftrightarrow \\ \gamma_1 &< n(1+2\alpha) - 2\gamma_2 + \frac{2(\delta - 1.5\gamma_2 + 2n\alpha)^2}{n(1-4\alpha)},\end{aligned}$$

if $\gamma_2 < 0.5\delta + n\alpha$. Since the following condition must be satisfied

$$\delta + \gamma_1 - 0.5n < \gamma_2 < 0.5\delta + n\alpha \Leftrightarrow \gamma_1 < n(0.5+\alpha) - 0.5\delta,$$

we obtain

$$\begin{aligned}\gamma_1 &< \min\left(n(1+2\alpha) - 2\gamma_2 + \frac{2(\delta - 1.5\gamma_2 + 2n\alpha)^2}{n(1-4\alpha)}, n(0.5+\alpha) - 0.5\delta\right) \\ &= n(0.5+\alpha) - 0.5\delta,\end{aligned}$$

since $n > \delta + 2n\alpha > 2\gamma_2$.

Case 2 ($\gamma_2 > \delta + \gamma_1$) In this case, Equation (14) becomes $|x_0| < 2N^{\gamma_2 - n}$. Thus, we can apply Theorem 5 for $X = e^{(\gamma_2-n)/\delta}, Y = e^{(0.5-2\alpha)/\delta}, Z = e^{\gamma_2/\delta}, |c| = C = e^{-2n\alpha/\delta}$ to find in polynomial time the values of x_0, $y_0 = v_1$, z_0 if some conditions hold. The subcase $CZ \leq XY^n$ yields

$$\frac{-2n\alpha}{\delta} + \frac{\gamma_2}{\delta} \leq \frac{\gamma_2 - n}{\delta} + \frac{0.5n - 2n\alpha}{\delta} \Leftrightarrow 0 \leq -0.5n,$$

which is a contradiction. In the complementary subcase ($C > XY^n$) we must have $\gamma_2 < \delta/2 + n\alpha$. Therefore, it follows

$$\delta + \gamma_1 < \gamma_2 < \delta/2 + n\alpha \Leftrightarrow 0.5\delta + \gamma_1 < n\alpha.$$

Also, we have

$$\begin{aligned}\frac{\gamma_2 - n}{\delta} &\leq 1 - \frac{2\gamma_2}{\delta} + \frac{2n\alpha}{\delta} + \frac{(\delta - 1.5\gamma_2 + 2n\alpha)^2}{\delta n(0.5-2\alpha)} \Leftrightarrow \\ \gamma_2 - n &\leq \delta - 2\gamma_2 + 2n\alpha + \frac{(\delta - 1.5\gamma_2 + 2n\alpha)^2}{n(0.5-2\alpha)} \Leftrightarrow \\ 0 &\leq \delta + n(1+2\alpha) - 3\gamma_2 + \frac{(\delta - 1.5\gamma_2 - 2n\alpha)^2}{n(0.5-2\alpha)}.\end{aligned}$$

Since we know s, v_0 and v_1, we can find the value of $p+q = v_1 \cdot 2^{2s} + v_0$, and thus the integers p and q. □

We further provide a result that works directly with the secret exponent d. The proof is given in Appendix D.

Theorem 13. *Let $N = pq$ be the product of two unknown primes with $q < p < 2q$ such that p and q share their s least significant bits. Also, let $e = N^\delta$ and $2^s = N^\alpha$, where $\alpha \in [0, 1/4)$. Assuming that $e \equiv d^{-1} \bmod \varphi_n(N)$, for type-A variants, we can factor N in polynomial time if*

$$\begin{cases} \gamma \leq n - \sqrt{n\delta(0.5 - 2\alpha)}, & \text{when } \max(0.5n, n(0.5-2\alpha)) < \delta, \\ \gamma \leq 0.5n - \delta, & \text{when } 0.5n > \delta, \end{cases}$$

where $|d| \leq N^\gamma$. For type-B variants we assume that $e \equiv d^{-1} \bmod \psi_n(N)$ and we obtain the bounds

$$\begin{cases} \gamma \leq n - 1 - \sqrt{(n-1)\delta(0.5 - 2\alpha)}, & \text{when } \max(0.5(n-1), (n-1)(0.5-2\alpha)) < \delta, \\ \gamma \leq 0.5(n-1) - \delta, & \text{when } 0.5n > \delta + 0.5. \end{cases}$$

4.3.1 Related Work

In [36], the author uses Kunihiro's result [18] to derive a bound for φ_n when p and q share their least significant bits and $e \equiv d^{-1} \bmod \varphi_n(N)$. The bound provided in Theorem 13 is a simplification of that bound.

Similarly to the known-approximation case for p the bounds derived in [27] and [30] for $\psi_n(N)$ and $\varphi_n(N)$, respectively, using Theorem 6 are improved by our result.

4.4 Known Least Significant Bits of d

Finally, we provide a method for factoring N when the attacker knows the least significant bits of d.

Theorem 14. *Let $N = pq$ be the product of two unknown primes with $q < p < 2q$. Also, let $e = N^\delta$. We also assume that $e \equiv d^{-1} \bmod \varphi_n(N)$ and $d = d_1 \cdot 2^s + d_0$, where the values of s and $d_0 \geq 1$ are known. Then for type-A variants, we factor N in polynomial time if*

$$\gamma \leq \frac{7n}{6} + \alpha - \frac{1}{3}\sqrt{n^2 + 6n(\delta + \alpha)}, \tag{15}$$

where $|d| < N^\gamma$ and $2^s = N^\alpha$. For type-B variants we assume that $e \equiv d^{-1} \bmod \psi_n(N)$ and we obtain the bound

$$\gamma \leq \frac{7(n-1)}{6} + \alpha - \frac{1}{3}\sqrt{(n-1)^2 + 6(n-1)(\delta + \alpha)}.$$

Proof. We assume that $|d| < N^\gamma$ and $2^s = N^\alpha$. From hypothesis we have $ed - k\varphi_n(N) = 1$ and denoting by $E = e \cdot 2^s = N^{\delta+\alpha}$, it follows

$$ed_1 \cdot 2^s + ed_0 - k\varphi_n(N) = 1 \Leftrightarrow -k\varphi_n(N) + ed_0 - 1 \equiv 0 \bmod E.$$

From Proposition 1 with $M = 0$ we have the equality

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

where $a_j \in \mathbb{Z}$ depends only on N and n, for all $j \in \{0, \ldots, n-1\}$. We denote $c = ed_0 - 1$ and define the polynomial $H(y) = y^n - \sum_{j=0}^{n-1} a_j y^j$. Hence, $(k, p+q)$ is a solution of the equation

$$xH(y) + c \equiv 0 \bmod E.$$

From Lemma 2 we know that $p+q < 3N^{1/2}$ and from $ed - k\varphi_n(N) = 1$ it follows

$$k = \frac{ed-1}{\varphi_n(N)} < \frac{ed}{\varphi_n(N)} < N^{\delta+\gamma-n},$$

where we used Corollary 5. We also observe that

$$|c| = |ed_0 - 1| < ed_0 < e \cdot 2^s = E = N^{\delta+\alpha}.$$

Now we can apply Theorem 7 for $X = E^{(\delta+\gamma-n)/(\delta+\alpha)}$, $Y = E^{1/2(\delta+\alpha)}$ and $|c| \leq E$ and obtain the following two situations.

Case 1 $(\gamma \geq \alpha + 0.5n)$ In this case, we have $|c| \leq XY^n$ and it follows

$$\frac{\delta+\gamma-n}{\delta+\alpha} \leq 1 - \sqrt{\frac{n}{2(\delta+\alpha)}} \Leftrightarrow \delta+\gamma-n \leq \delta+\alpha - \sqrt{\frac{n(\delta+\alpha)}{2}}$$
$$\Leftrightarrow \gamma \leq n+\alpha - \sqrt{0.5n(\delta+\alpha)},$$

if $\delta + \alpha > 0.5n$. Since we must have

$$0.5n + \alpha \leq \gamma \leq n + \alpha - \sqrt{0.5n(\delta+\alpha)},$$

we obtain that $\delta + \alpha < 0.5n$, which leads to a contradiction.

Case 2 $(\gamma < \alpha + 0.5n)$ In this case, we have $|c| > XY^n$. Since $\varepsilon = 1$, we can only apply the third branch. Hence, we obtain

$$\frac{\delta+\gamma-n}{\delta+\alpha} \leq \frac{n}{6(\delta+\alpha)} + 1 - \frac{2}{3}\sqrt{\frac{n^2}{4(\delta+\alpha)^2} + \frac{3n}{2(\delta+\alpha)}} \Leftrightarrow$$
$$\delta+\gamma-n \leq \frac{n}{6} + \delta + \alpha - \frac{2}{3}\sqrt{\frac{n^2}{4} + \frac{3n(\delta+\alpha)}{2}} \Leftrightarrow$$
$$\gamma \leq \frac{7n}{6} + \alpha - \frac{1}{3}\sqrt{n^2 + 6n(\delta+\alpha)},$$

when

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

Therefore, we have

$$\gamma \leq \min(\frac{7n}{6} + \alpha - \frac{1}{3}\sqrt{n^2+6n(\delta+\alpha)}, 0.5n+\alpha)$$
$$= \frac{7n}{6} + \alpha - \frac{1}{3}\sqrt{n^2+6n(\delta+\alpha)},$$

just as desired. □

4.4.1 Related Work

In [36], the author uses Kunihiro's result [18] to derive a bound for φ_n when $d_0 \geq 1$ is known. Unfortunately the conclusion from [36] is misleading since the author concludes that we can factor N if

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

and $0.5n+\alpha < \gamma$ when $d_0 \geq 1$. The first case leads to

$$0.5n+\alpha < n+\alpha-\sqrt{0.5n(\delta+\alpha)} \Leftrightarrow \delta+\alpha < 0.5n,$$

which is a contradiction with $0.5n \leq \delta+\alpha$. In the second case we have

$$\frac{n}{2}+\alpha < \frac{3n-1}{4} + \frac{(n+2)\alpha-n\delta}{2(n+1)} \Leftrightarrow 0 < \frac{n-1}{4} - \frac{n(\alpha+\delta)}{2(n+1)}$$
$$\Leftrightarrow \delta+\alpha < \frac{n^2-1}{2n},$$

which is a contradiction with $(n+1)^2/2n < \delta+\alpha$. Therefore, although the statement is correct, the conditions to factor N are never fullfilled.

When considering ψ_n, the bound derived in [27,30] using Theorem 7 is identical to our result.

5 Conclusions

In this paper, we presented a lattice-based technique for solving, in polynomial time, modular equations of the form $xH(y)+cz \equiv 0 \pmod{\beta}$ under certain conditions. We then applied this approach to factor the module $N=pq$ of type-A and type-B cryptosystems. The resulting bounds were compared with previously known results, demonstrating a significant improvement.

References

1. Abderrahmane Nitaj, N.N.H.A., Ariffin, M.R.B.K.: Cryptanalysis of a New Variant of the RSA Cryptosystem. In: AFRICACRYPT 2024. Springer (2024)
2. Boneh, D.: Twenty Years of Attacks on the RSA Cryptosystem. Notices of the AMS **46**(2), 203–213 (1999)
3. Boneh, D., Durfee, G.: Cryptanalysis of RSA with Private Key d Less than $N^{0.292}$. In: EUROCRYPT 1999. Lecture Notes in Computer Science, vol. 1592, pp. 1–11. Springer (1999)
4. Bunder, M., Nitaj, A., Susilo, W., Tonien, J.: A New Attack on Three Variants of the RSA Cryptosystem. In: ACISP 2016. Lecture Notes in Computer Science, vol. 9723, pp. 258–268. Springer (2016)
5. Bunder, M., Nitaj, A., Susilo, W., Tonien, J.: A Generalized Attack on RSA Type Cryptosystems. Theoretical Computer Science **704**, 74–81 (2017)
6. Coppersmith, D.: Finding a Small Root of a Bivariate Integer Equation; Factoring with High Bits Known. In: EUROCRYPT 1996. Lecture Notes in Computer Science, vol. 1070, pp. 178–189. Springer (1996)
7. Coppersmith, D.: Finding a Small Root of a Univariate Modular Equation. In: EUROCRYPT 1996. Lecture Notes in Computer Science, vol. 1070, pp. 155–165. Springer (1996)
8. Coppersmith, D.: Small Solutions to Polynomial Equations, and Low Exponent RSA Vulnerabilities. Journal of Cryptology **10**(4), 233–260 (1997)
9. Cotan, P., Teşeleanu, G.: Continued Fractions Applied to a Family of RSA-like Cryptosystems. In: ISPEC 2022. pp. 589–605. Springer (2022)
10. Cotan, P., Teşeleanu, G.: Small Private Key Attack Against a Family of RSA-Like Cryptosystems. In: NordSEC 2023. Lecture Notes in Computer Science, vol. 14324, pp. 57–72. Springer (2023)
11. Cotan, P., Teşeleanu, G.: A Security Analysis of Two Classes of RSA-Like Cryptosystems. Journal of Mathematical Cryptology **18**(1), 20240013 (2024)
12. Elkamchouchi, H., Elshenawy, K., Shaban, H.: Extended RSA Cryptosystem and Digital Signature Schemes in the Domain of Gaussian Integers. In: ICCS 2002. vol. 1, pp. 91–95. IEEE Computer Society (2002)
13. Feng, Y., Nitaj, A., Pan, Y.: Partial Prime Factor Exposure Attacks on Some RSA Variants. Theoretical Computer Science **999**, 114549 (2024)
14. Gallian, J.: Contemporary Abstract Algebra. Chapman and Hall/CRC, 10 edn. (2020)
15. Herrmann, M., May, A.: Maximizing Small Root Bounds by Linearization and Applications to Small Secret Exponent RSA. In: PKC 2010. Lecture Notes in Computer Science, vol. 6056, pp. 53–69. Springer (2010)
16. Howgrave-Graham, N.: Finding small roots of univariate modular equations revisited. In: IMA 1997. Lecture Notes in Computer Science, vol. 1355, pp. 131–142. Springer (1997)
17. Jochemsz, E., May, A.: A Strategy for Finding Roots of Multivariate Polynomials with New Applications in Attacking RSA Variants. In: ASIACRYPT 2006. Lecture Notes in Computer Science, vol. 4284, pp. 267–282. Springer (2006)
18. Kunihiro, N.: On Optimal Bounds of Small Inverse Problems and Approximate GCD Problems with Higher Degree. In: ISC 2012. Lecture Notes in Computer Science, vol. 7483, pp. 55–69. Springer (2012)
19. Lenstra, A.K., Lenstra, H.W., Lovász, L.: Factoring Polynomials with Rational Coefficients. Mathematische Annalen **261**, 515–534 (1982)

20. May, A.: New RSA Vulnerabilities Using Lattice Reduction Methods. Ph.D. thesis, University of Paderborn (2003)
21. May, A.: Using LLL-Reduction for Solving RSA and Factorization Problems. In: The LLL Algorithm: Survey and Applications, pp. 315–348. Information Security and Cryptography, Springer (2010)
22. Michel, S., Niang, O., Sow, D.: A new generalized attack on rsa-like cryptosystems. IACR Cryptology ePrint Archive **2025/380** (2025)
23. Murru, N., Saettone, F.M.: A Novel RSA-Like Cryptosystem Based on a Generalization of the Rédei Rational Functions. In: NuTMiC 2017. Lecture Notes in Computer Science, vol. 10737, pp. 91–103. Springer (2017)
24. Nitaj, A., Ariffin, M.R.B.K., Adenan, N.N.H., Abu, N.A.: Classical Attacks on a Variant of the RSA Cryptosystem. In: LATINCRYPT 2021. Lecture Notes in Computer Science, vol. 12912, pp. 151–167. Springer (2021)
25. Nitaj, A., Ariffin, M.R.K., Nassr, D.I., Bahig, H.M.: New Attacks on the RSA Cryptosystem. In: AFRICACRYPT 2014. Lecture Notes in Computer Science, vol. 8469, pp. 178–198. Springer (2014)
26. Peng, L., Hu, L., Lu, Y., Wei, H.: An Improved Analysis on Three Variants of the RSA Cryptosystem. In: Inscrypt 2016. Lecture Notes in Computer Science, vol. 10143, pp. 140–149. Springer (2016)
27. Rahmani, M., Nitaj, A., Ziane, M.: Partial Exposure Attacks on a New RSA Variant. Cryptography **8**(4) (2024)
28. Rahmani, M., Nitaj, A., Ziane, M.: A Generalized Attack on a New Variant of the RSA Cryptosystem. Computational and Applied Mathematics **45**(1), 11 (2026)
29. Rahmani, M., Nitaj, A., Ziane, M.: A Novel Cryptanalytic Attack on a Family of RSA-Like Cryptosystems. Discrete Mathematics **349**(1), 114660 (2026)
30. Rahmani, M., Nitaj, A., Ziane, M.: Cryptanalysis of Some Algebraic Variants of the RSA Cryptosystem. Finite Fields and Their Applications **110**, 102757 (2026)
31. Rivest, R.L., Shamir, A., Adleman, L.: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM **21**(2), 120–126 (1978)
32. Shi, G., Wang, G., Gu, D.: Further Cryptanalysis of a Type of RSA Variants. In: ISC 2022. Lecture Notes in Computer Science, vol. 13640, pp. 133–152. Springer (2022)
33. Steinfeld, R., Zheng, Y.: On the Security of RSA with Primes Sharing Least-Significant Bits. Applicable Algebra in Engineering, Communication and Computing **15**, 179–200 (2004)
34. Susilo, W., Tonien, J.: A Wiener-type Attack on an RSA-like Cryptosystem Constructed from Cubic Pell Equations. Theor. Comput. Sci. **885**, 125–130 (2021)
35. Teşeleanu, G.: A Lattice Attack Against a Family of RSA-Like Cryptosystems. In: CSCML 2024. Lecture Notes in Computer Science, vol. 15349, pp. 343–355. Springer (2024)
36. Teşeleanu, G.: Partial Exposure Attacks Against a Family of RSA-like Cryptosystems. Cryptography **9**(1) (2025)
37. Wiener, M.J.: Cryptanalysis of Short RSA Secret Exponents. IEEE Trans. Inf. Theory **36**(3), 553–558 (1990)
38. Zheng, M., Kunihiro, N., Hu, H.: Cryptanalysis of RSA Variants with Modified Euler Quotient. In: AFRICACRYPT 2018. Lecture Notes in Computer Science, vol. 10831, pp. 266–281. Springer (2018)
39. Zheng, M., Kunihiro, N., Yao, Y.: Cryptanalysis of the RSA Variant Based on Cubic Pell Equation. Theoretical Computer Science **889**, 135–144 (2021)

A Useful Lemmas

In this appendix, we provide the results needed to prove some of the results presented in this paper. We start by providing lower and upper bounds for $p+q$ (see [5, Lemma 3]).

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

$$2\sqrt{N} < p + q < \frac{3\sqrt{2}}{2}\sqrt{N}.$$

If an approximation of p is known, an approximation of q can be derived using the following result from [13].

Lemma 3. *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 [25, 33] 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 4. *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, $p = p_1 \cdot 2^s + u_0$, $q = q_1 \cdot 2^s + u_0$ and $p+q = v_1 \cdot 2^{2s} + v_0$ for some integers p_1, q_1 and v_1.

The bounds for $\varphi_n(N)$ and $\psi_n(N)$ are provided in [10, Corollary 1] and [9, Corollary 1]. This results imply that $\varphi_n(N) \simeq N^n$ and $\psi_n(N) \simeq N^{n-1}$.

Corollary 5. *Let $N = pq$ be the product of two unknown primes with $q < p < 2q$. Then the following properties hold*

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

and

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

In order to apply the presented lattice attacks, we first need to show that φ_n and ψ_n can be written as polynomials with integer coefficients. Therefore, we present the following results from [27,36].

Proposition 1. *Let N be a positive integer and $M \in \mathbb{Z}$. Then for any integer $n \geq 1$ the following properties hold*

$$\varphi_n(N) = -(p+q-M)^n + \sum_{k=0}^{n-1} a_k (p+q-M)^k,$$
$$\psi_n(N) = (p+q-M)^{n-1} + \sum_{j=0}^{n-2} b_j (p+q-M)^j,$$

where $a_j, b_j \in \mathbb{Z}$ depend only on N, M and n, for all $0 \leq i \leq n-1$ and $0 \leq j \leq n-2$.

B Proof of Theorem 9

According to our hypothesis, there exists an integer x_0 such that

$$ed + x_0 \varphi_n(N) = 1.$$

Similarly to Theorem 8's proof we deduce the equation $xH(y) + 1 \equiv 0 \bmod e$, which has x_0 and $y_0 = p + q$ as solutions.

In order to be able to apply Theorem 7 we first need to bound the solutions. Hence, we have $y_0 = p + q < Y \simeq e^{1/2\delta}$ and

$$|x_0| = \frac{|1 - ed|}{\varphi_n(N)} \leq \frac{|ed|}{\varphi_n(N)} \leq N^{\delta+\gamma-n}. \tag{16}$$

We further apply Theorem 7 by taking the monic polynomial $H(y)$ of degree n and $X = e^{(\delta+\gamma-n)/\delta}$, $Y = e^{1/2\delta}$, $c = 1$. We further consider two cases.

Case 1 $(0.5n < \gamma + \delta)$ In this case we have that $1 \leq XY^n$ and we can find the solutions if

$$\frac{\delta + \gamma - n}{\delta} \leq 1 - \frac{\sqrt{n}}{\sqrt{2\delta}} \Leftrightarrow \gamma \leq n - \sqrt{0.5n\delta}$$

and $0.5n < \delta$.

Case 2 $(0.5n > \gamma + \delta)$ In this case we have $1 > XY^n$. Note that we can only apply the second brach, since for the last one we obtain $\gamma < 0$. Therefore, we can find the solutions if

$$\frac{\delta + \gamma - n}{\delta} \leq 1 + \frac{2\delta}{n} \Leftrightarrow \gamma \leq n + \frac{2\delta^2}{n}.$$

Therefore, we obtain

$$\gamma \leq \min\left(n + \frac{2\delta^2}{n}, 0.5n - \delta\right) = 0.5n - \delta,$$

and $\delta < 0.5n$,

Note that, once y_0 is found, we can factorize the modulus N. □

C Proof of Theorem 11

According to our hypothesis, there exists an integer x_0 such that

$$ed + x_0\varphi_n(N) = 1 \tag{17}$$

Similarly to Theorem 10's proof, we deduce that $(x_0, y_0 = p + q - \tilde{p} - \tilde{q})$ is a solution of the equation $xH(y) + 1 \equiv 0 \bmod \varphi_n(N)$, where $H(y) \in \mathbb{Z}[y]$ is a monic polynomial of degree n and $\tilde{q} = \lfloor N/\tilde{p} \rfloor$ is an approximation of q with $|q - \tilde{q}| < N^{\lambda}$. Thus, we obtain $|p + q - \tilde{p} - \tilde{q}| < 2N^{\lambda}$. Also, from Equation (17) it follows that

$$|x_0| = \frac{|1 - ed|}{\varphi_n(N)} < \frac{ed}{\varphi_n(N)} \leq N^{\delta+\gamma-n}.$$

We further apply Theorem 7 with $X = e^{(\delta+\gamma-n)/\delta}, Y = e^{\lambda/\delta}$ and $c = 1$ and it follows that we can find (x_0, y_0) in polynomial time if the following situations hold.

Case 1 $(n(1-\lambda) < \delta + \gamma)$ In this case, we have $1 < XY^n$ and we can find the solutions if

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

and $n\lambda \leq \delta$.

Case 2 $(n(1-\lambda) > \delta+\gamma)$ In this case, we have $1 > XY^n$. Note that we can only apply the second branch, since for the last one we obtain $\gamma < 0$. Therefore, we can find the solutions if

$$\frac{\delta + \gamma - n}{\delta} \leq 1 + \frac{\delta}{n\lambda} \Leftrightarrow \gamma \leq n + \frac{\delta^2}{n\lambda}$$

Therefore, we obtain

$$\gamma \leq \min\left(n + \frac{\delta^2}{n\lambda}, n(1-\lambda) - \delta\right) = n(1-\lambda) - \delta$$

and $n(1-\lambda) > \delta$. □

D Proof of Theorem 13

According to our hypothesis, there exists an integer x_0 such that

$$ed + x_0\varphi_n(N) = 1.$$

Similarly to Theorem 12's proof, we obtain the equation $xH(y) + c \equiv 0 \bmod e$, where $H(y) \in \mathbb{Z}[y]$ is a monic polynomial of degree n and $c = 2^{-2sn} = e^{-2n\alpha/\delta}$.

We also obtain that $(x_0, y_0 = v_1)$ is a solution of this equation with $|v_1| \leq 3 \cdot N^{1/2-2\alpha}$ and

$$|x_0| \leq \frac{|1 - ed|}{\varphi_n(N)} < \frac{ed}{\varphi_n(N)} \leq N^{\delta+\gamma-n}.$$

We further apply Theorem 7 with $X = e^{(\delta+\gamma-n)/\delta}, Y = e^{(0.5-2\alpha)/\delta}$ and $C = e^{-2n\alpha/\delta}$ and it follows that we can find x_0 and v_1 in polynomial time if the following situations hold.

Case 1 $(\delta + \gamma > 0.5n)$ In this case, we have $C < XY^n$ and it follows that

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

if $n(0.5 - 2\alpha) \leq 2\delta$.

Case 2 $(\delta + \gamma < 0.5n)$ In this case, we have $C > XY^n$. Note that the third branch yields the condition

$$\frac{0.5 - 2\alpha}{\delta} < \min\left(\frac{3\varepsilon}{n}, \frac{1 - \delta}{n}\right) \leq \frac{3\varepsilon}{n} = \frac{-6n\alpha}{\delta n} \Leftrightarrow 0.5 + 4\alpha < 0,$$

which is a contradiction. Thus, we focus only on the second branch, where we have

$$\frac{\delta + \gamma - n}{\delta} \leq 1 + \frac{2n\alpha}{\delta} + \frac{(\delta + 2n\alpha)^2}{n\delta(0.5 - 2\alpha)} \Leftrightarrow \gamma \leq n(1 + 2\alpha) + \frac{(\delta + 2n\alpha)^2}{n(0.5 - 2\alpha)},$$

if $0.5 + 4\alpha \geq 0$ and $-2n\alpha < \delta$, which are always true. Therefore, we obtain

$$\begin{aligned}\gamma &\leq \min\left(n(1 + 2\alpha) + \frac{(\delta + 2n\alpha)^2}{n(0.5 - 2\alpha)}, 0.5n - \delta\right) \\ &= 0.5n - \delta,\end{aligned}$$

and $0.5n > \delta$. □