cryptography

MDPI

Article

Partial Exposure Attacks on a New RSA Variant

Mohammed Rahmani [1], Abderrahmane Nitaj [2,*] and Mhammed Ziane [1]

[1] ACSA Laboratory, Department of Mathematics and Computer Science, Sciences Faculty, Mohammed First University, Oujda 60000, Morocco; mohammed.rahmani@ump.ac.ma (M.R.); m.ziane@ump.ac.ma (M.Z.)
[2] LMNO, CNRS, UNICAEN, Caen Normandie University, 14000 Caen, France
* Correspondence: abderrahmane.nitaj@unicaen.fr

Abstract: In 2022, Cotan and Teşeleanu presented a variant of the RSA cryptosystem where the modulus is of the form $N = pq$, and the private and the public exponents satisfy $ed \equiv 1 \pmod{\psi_n(N)}$ with $n \geq 2$, and $\psi_n(N) = \frac{(p^n-1)(q^n-1)}{(p-1)(q-1)}$. This variant of RSA was recently cryptanalyzed by Nitaj, Adenan, and Ariffin at Africacrypt 2024. In this paper, we push further the cryptanalysis of the scheme of Cotan and Teşeleanu by presenting a method to solve the equation $xH(y) + c \equiv 0 \pmod{e}$ where c is a constant that is independent of x and y. This enables us to propose more attacks on the scheme, including a partial key exposure attack, an attack when the most significant bits of one of the prime factors are known, and an attack when the least significant bits of one of the prime factors are known.

Keywords: RSA; factorization; Coppersmith's method; lattice basis reduction; RSA variants

1. Introduction

Invented in 1978 by Rivest, Shamir, and Adleman [1], the RSA cryptosystem is one of the most used public key cryptosytems regarding its practical applications. Its security is related to the hardness of factoring composite large integers. To use the RSA scheme, one starts by generating two large prime numbers p and q of the same bit size, and it computes $N = pq$ as the RSA modulus. Then, one selects an integer e, called the public exponent, satisfying $\gcd(e, p-1)(q-1)) = 1$. This enables us to compute the private exponent d as the inverse of e modulo $(p-1)(q-1)$, that is $ed \equiv 1 \pmod{(p-1)(q-1)}$. The encryption process allows transforming a plaintext $m < N$ to a ciphertext $c \equiv m^e \pmod{N}$. To recover the plaintext m, one applies the decryption process $m \equiv c^d \pmod{N}$. The efficiency of both encryption and decryption is based on the run time of the modular exponentiation. To reduce the run time, specifically in the decryption, it is tempting to use small private exponents. Unfortunately, in 1990, Wiener [2] showed that such a choice is vulnerable when $d \leq \frac{1}{3}N^{\frac{1}{4}}$. The former bound was improved later by Boneh and Durfee [3] up to $N^{0.292}$.

Based on these obstacles, several variants have been proposed to improve the efficiency as well as the security of RSA. Some of these variants employ a modulus of the form $N = pq$ as in CRT-RSA [4], rebalanced RSA [2], and KMOV [5]. In contrast, other variants utilize different types of moduli, such as Multi-Prime RSA [6] and Prime-Power RSA [7].

In 2018, Murru and Saettone [8] introduced a new variant of the RSA scheme based on the cubic Pell equation $x^3 + ay^3 + a^2z^3 - 3axyz = 1$, where a is a cubic non-residue modulo $N = pq$. They used $N = pq$ as a modulus, with the public key being (N, e) and the private key (N, d), where e and d satisfy $ed \equiv 1 \left(\mod \frac{(p^3-1)(q^3-1)}{(p-1)(q-1)}\right)$. This variant of RSA has been intensively cryptanalyzed in [9–12].

In 2022, Cotan and Teşeleanu [13] proposed a generalization of the scheme of Murru and Saettone. They used a modulus $N = pq$, a public exponent e, and a private exponent d such that $ed \equiv 1 \left(\mod \frac{(p^n-1)(q^n-1)}{(p-1)(q-1)}\right)$ for $n \geq 2$. The special case $n = 3$ is the scheme of

check for updates

Citation: Rahmani, M.; Nitaj, A.; Ziane, M. Partial Exposure Attacks on a New RSA Variant. *Cryptography* **2024**, *8*, 44. https://doi.org/10.3390/cryptography8040044

Academic Editor: Josef Pieprzyk

Received: 26 August 2024
Revised: 19 September 2024
Accepted: 2 October 2024
Published: 6 October 2024

Murru and Saettone. The authors also presented an attack based on the continued fraction algorithm whenever $n \leq 4$, $d = N^{\delta}$, $e = N^{\alpha}$, $\alpha \leq n - \frac{1}{2}$, and $\delta < \frac{1}{4}(2n - 2\alpha - 1)$.

In 2024, Nitaj et al. [14] developed a novel attack on the Cotan and Teşeleanu scheme using Coppersmith's method and lattice basis reduction. They demonstrated that one can efficiently factor the modulus $N = pq$ if $e = N^{\alpha}$, $d \leq N^{\delta}$, $\frac{n-1}{2} \leq \alpha \leq 2(n-1)$, and $\delta < n - 1 - \frac{\sqrt{2}}{2}\sqrt{(n-1)\alpha}$.

In the work of Nitaj et al. [14], the authors started by solving the modular equation $xH(y) + c \equiv 0 \pmod{e}$ where $H(y)$ is a monic polynomial of degree r, under certain conditions, namely, $e = N^{\alpha}$, $|x| < N^{\beta}$, $|y| < N^{\gamma}$, $c < |x||y|^r < e$, and $\beta < \alpha - \sqrt{r\alpha\gamma}$. As a by-product, they presented an attack on the scheme of Cotan and Teşeleanu and showed that $N = pq$ can be factored for any $n \geq 2$ if e and d satisfy $ed \equiv 1 \left(\mod \frac{(p^n-1)(q^n-1)}{(p-1)(q-1)}\right)$ and $\delta < n - 1 - \frac{\sqrt{2}}{2}\sqrt{(n-1)\alpha}$. This significantly improved the bound $\delta < \frac{1}{4}(2n - 2\alpha - 1)$ of Cotan and Teşeleanu.

In this paper, for a monic univariate polynomial $H(y) \in \mathbb{Z}[y]$ of degree r, we propose a new lattice-based method to solve the equation $xH(y) + c \equiv 0 \pmod{e}$ when $N = pq$, $e = N^{\alpha}$, $|x| \leq N^{\beta}$, $|y| \leq N^{\gamma}$, $|x||y|^r < e$, and $\beta < \alpha + \frac{1}{3}r\gamma - \frac{2}{3}\sqrt{3r\alpha\gamma + r^2\gamma^2}$. This can be achieved for any value of c; in particular, the condition $|c| < |xy^r|$ is no more required. This allows us to perform four attacks on the scheme of Cotan and Teşeleanu. The first attack deals with the situation where the least significant bits (LSBs) of the private exponent d are known. The second attack concerns the situation where an approximation of one of the primes is known. The third attack concerns the situation when the primes share their most significant bits (MSBs). The fourth attack concerns the situation where the primes share their least significant bits.

The paper is organized as follows. In Section 2, we present some preliminaries and provide a new expression for $\psi_n(N)$ that is useful in the sequel. In Section 3, we present the new method to find the small solutions of the equation $xH(y) + c \equiv 0 \pmod{e}$. In Section 4, we apply the proposed method to perform the first attack on the cryptosystem of Cotan and Teşeleanu, namely, an attack with known LSBs. In Section 5, we present the second attack, which is a partial prime exposure attack. In Section 6, we apply the third attack when the prime factors of the modulus share their MSBs. In Section 7, we present another expression for ψ_n which allows performing the fourth attack when the prime factors of the modulus share their LSBs. Finally, we conclude the paper in Section 8.

2. Preliminaries

Let $N = pq$ be an RSA modulus with $q < p < 2q$. Then, p and q can be bounded in terms of N as in the following simple lemma.

Lemma 1. *Let $N = pq$ be an RSA modulus with $q < p < 2q$. Then,*

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

The following lemma shows how to find an approximation of q if an approximation of p is given (see [9]).

Lemma 2. *Let $N = pq$ be an RSA modulus with $q < p < 2q$. Let p_0 be an approximation of p such that $|p - p_0| = N^{\mu}$. Then, $q_0 = \left\lfloor \frac{N}{p_0} \right\rfloor$ is an approximation of q such that*

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

The generalized totient function in the system of Cotan and Teşeleanu [13] is defined for $N = pq$ and $n \geq 2$ by

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

The following result gives simple upper and lower bounds for $\psi_n(N)$.

Lemma 3. *Let $N = pq$, $n \geq 2$, and $\psi_n(N) = \frac{(p^n-1)(q^n-1)}{(p-1)(q-1)}$. Then*

$$N^{n-1} < \psi_n(N) < 4N^{n-1}.$$

Proof. For the lower bound, we have

$$\psi_n(N) = \left(p^{n-1} + p^{n-2} \ldots + 1\right)\left(q^{n-1} + q^{n-2} + \ldots + 1\right) > p^{n-1}q^{n-1} = N^{n-1}.$$

For the upper bound, using $x^{n-1} + x^{n-2} + \ldots + 1 < 2x^{n-1}$ for $x > 2$, we obtain

$$\psi_n(N) = \left(p^{n-1} + p^{n-2} \ldots + 1\right)\left(q^{n-1} + q^{n-2} + \ldots + 1\right) < 4p^{n-1}q^{n-1} = 4N^{n-1}.$$

This terminates the proof. □

The following result shows how to compute $\psi_n(N)$ (see [14]).

Lemma 4. *Let $N = pq$ and $S = p + q$. Then, $\psi_1(N) = 1$, $\psi_2(N) = N + 1 + S$, and for $n \geq 3$,*

$$\psi_n(N) = N^{n-1} + 1 + S\psi_{n-1}(N) - N\psi_{n-2}(N).$$

The following result shows that $\psi_n(N)$ can be expressed as a polynomial of $p + q$ (see [14]).

Lemma 5. *Let $N = pq$ and $n \geq 2$. Then, there exist $n - 1$ integer coefficients $a_{n-2}, \ldots, a_0$ depending only on N and n such that*

$$\psi_n(N) = (p+q)^{n-1} + \sum_{j=0}^{n-2} a_j (p+q)^j.$$

Note that in Lemma 5, the coefficients a_i can be computed only by using N and n. Nevertheless, $\psi_n(N)$ cannot be computed by an adversary who does not know $p + q$.

The former result can be extended in the following form.

Lemma 6. *Let $N = pq$, $n \geq 2$, $\psi_n(N) = \frac{(p^n-1)(q^n-1)}{(p-1)(q-1)}$, and $M \in \mathbb{Z}$. Then, there exist $n - 1$ coefficients $a_j^{(n)} \in \mathbb{Z}$, $j = 0, \ldots, n-2$, depending only on N, n, and M such that*

$$\psi_n(N) = (p+q-M)^{n-1} + \sum_{j=0}^{n-2} a_j^{(n)} (p+q-M)^j.$$

Proof. We proceed by recursion. We have $\psi_1(N) = 1$, and

$$\begin{aligned}
\psi_2(N) &= (p+1)(q+1) \\
&= (p+q-M) + N + M + 1, \\
\psi_3(N) &= (p^2+p+1)(q^2+q+1) \\
&= (p+q-M)^2 + (N+2M+1)(p+q-M) \\
&\quad + M(N+M+1) + N^2 - N + 1.
\end{aligned}$$

Assume that, for $n \geq 4$, we have

$$\psi_{n-2}(N) = (p+q-M)^{n-3} + \sum_{j=0}^{n-4} a_j^{(n-2)}(p+q-M)^j,\ a_j^{(n-2)} \in \mathbb{Z},$$
$$\psi_{n-1}(N) = (p+q-M)^{n-2} + \sum_{j=0}^{n-3} a_j^{(n-1)}(p+q-M)^j,\ a_j^{(n-1)} \in \mathbb{Z}.$$

Using Lemma 4, we obtain

$$\begin{aligned}
\psi_n(N) &= (p+q)\psi_{n-1}(N) - N\psi_{n-2}(N) + N^{n-1} + 1 \\
&= (p+q-M)\psi_{n-1}(N) + M\psi_{n-1}(N) - N\psi_{n-2}(N) + N^{n-1} + 1 \\
&= (p+q-M)^{n-1} + \left(a_{n-3}^{(n-1)} + M\right)(p+q-M)^{n-2} \\
&+ \left(a_{n-4}^{(n-1)} + Ma_{n-3}^{(n-1)} - N\right)(p+q-M)^{n-3} \\
&\quad + \sum_{j=1}^{n-4}\left(a_{j-1}^{(n-1)} + Ma_j^{(n-1)} - Na_j^{(n-2)}\right)(p+q-M)^j \\
&\quad + Ma_0^{(n-1)} - Na_0^{(n-2)} + N^{n-1} + 1 \\
&= (p+q-M)^{n-1} + \sum_{j=0}^{n-2} a_j^{(n)}(p+q-M)^j,
\end{aligned}$$

where

$$\begin{aligned}
a_{n-2}^{(n)} &= a_{n-3}^{(n-1)} + M, \\
a_{n-3}^{(n)} &= a_{n-4}^{(n-1)} + Ma_{n-3}^{(n-1)} - N, \\
a_j^{(n)} &= a_{j-1}^{(n-1)} + Ma_j^{(n-1)} - Na_j^{(n-2)},\ j = 1, \ldots, n-4, \\
a_0^{(n)} &= Ma_0^{(n-1)} - Na_0^{(n-2)} + N^{n-1} + 1.
\end{aligned}$$

This shows that all the coefficients $a_j^{(n)}$, $0 \leq j \leq n-2$ are integers and depend only on N, n, and M. This terminates the proof. □

Using Lemma 4, one can express the first values of $\psi_n(N)$ as a polynomial in $T = p+q-M$. For instance, we have

$$\begin{aligned}
\psi_1(N) &= 1, \\
\psi_2(N) &= T + M + N + 1, \\
\psi_3(N) &= T^2 + (2M+N+1)T + M(M+N+1) + N^2 - N + 1, \\
\psi_4(N) &= T^3 + (3M+N+1)T^2 + \left(M(3M+2N+2) + N^2 - 2N + 1\right)T \\
&\quad + M^2 + M^3 + M + M(N^2 + MN - 2N) + N^3 - N^2 - N + 1, \\
\psi_5(N) &= T^4 + (4M+N+1)T^3 + \left(M(6M+3N+3) + N^2 - 3N + 1\right)T^2 \\
&\quad + \left(4M^3 + 3M^2 + 2M + M(3MN + 2N^2 - 6N) + N^3 - 2N^2 - 2N + 1\right)T \\
&\quad + M^4 + M^3 + M^2 + M + M(M^2N + MN^2 - 3MN + N^3 - 2N^2 - 2N) \\
&\quad + N^4 - N^3 + N^2 - N + 1.
\end{aligned}$$

2.1. Lattice Basis Reduction and Coppersmith's Method

Let ω and n be positive integers with $\omega \leq n$. Let $v_1, v_2, \ldots, v_\omega$ be ω linearly independent vectors of $\mathbb{R}^n$. A lattice $\mathcal{L} \subset \mathbb{R}^n$ is the set of all integer linear combinations of $v_1, v_2, \ldots, v_\omega$, that is,

$$\mathcal{L} = \mathbb{Z}v_1 + \mathbb{Z}v_2 + \ldots + \mathbb{Z}v_\omega.$$

The lattice $\mathcal{L}$ can be represented by a matrix B whose rows are the vectors $v_1, v_2, \ldots, v_\omega$. The parameter n is the dimension of the lattice $\mathcal{L}$, and ω is its rank. Its determinant is defined to be $\det(\mathcal{L}) = \sqrt{\det(B^t B)}$ where B^t is the transpose of B. When $\omega = n$, we say that the lattice $\mathcal{L}$ is full-rank, and then its determinant is simplified to $\det(\mathcal{L}) = |\det(B)|$.

It is known that a lattice $\mathcal{L}$ has infinitely many bases, and finding a basis with short vectors is a hard task especially when the dimension of the lattice is large. In 1982, Lenstra, Lenstra and Lovász [15] proposed LLL, which is a polynomial time algorithm to find a short basis. The following result [16] is widely used to estimate the output of the LLL algorithm.

Theorem 1. *Let $\mathcal{L}$ be a lattice spanned by a basis $(v_1, v_2, \ldots, v_\omega)$. The LLL algorithm produces a reduced basis $(u_1, u_2, \ldots, u_\omega)$ satisfying*

$$\|u_1\| \leq \ldots \leq \|u_i\| \leq 2^{\frac{\omega(\omega-1)}{4(\omega+1-i)}} \det(\mathcal{L})^{\frac{1}{\omega+1-i}}, \text{ for } i = 1, \ldots, \omega.$$

2.2. Coppersmith's Method

In 1996, Coppersmith [17] proposed an efficient way to find small roots of modular polynomial equations of the form $f(x) \equiv 0 \pmod{M}$, mainly when the factorization of the modulus M is unknown. Since then, Coppersmith's method has been generalized to polynomials with more variables, specifically polynomials of the form

$$f(x_1, x_2, \ldots, x_n) = \sum_{i_1, i_2, \ldots, i_n} a_{i_1, i_2, \ldots, i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n},$$

with $a_{i_1, i_2, \ldots, i_n} \in \mathbb{Z}$. For such polynomials, the Euclidean norm is defined by $\|f(x_1, x_2, \ldots, x_n)\| = \sqrt{\sum a_{i_1, i_2, \ldots, i_n}^2}$.

In 1997, Howgrave-Graham [18] clarified Coppersmith's method in the following sense.

Theorem 2 (Howgrave-Graham). *Let $f(x_1, x_2, \ldots, x_n) \in \mathbb{Z}[x_1, x_2, \ldots, x_n]$ be a multivariate polynomial with at most ω monomials. Let e and m be positive integers. Suppose that*

1. $f(y_1, y_2, \ldots, y_n) \equiv 0 \pmod{e^m}$.
2. $\|f(x_1 X_1, x_2 X_2, \ldots, x_n X_n)\| < \frac{e^m}{\sqrt{\omega}}$, $|y_i| < X_i$, *for* $i = 1, \ldots, n$.

Then, $f(y_1, y_2, \ldots, y_n) = 0$ holds over the integers.

When more than two variables are involved, the methods based on Coppersmith's technique are heuristic. In this paper, we use the following assumption [3,12,19,20]. This is a reasonable assumption that holds true when the parameters are sufficiently smaller than the theoretical bounds.

Assumption 1. *The reduced polynomials $h_1, h_2, \ldots, h_\omega$ generated by the LLL algorithm are algebraically independent.*

Under the former assumption, the common root $(y_1, y_2, \ldots, y_n)$ of the polynomial equations $h_i(y_1, y_2, \ldots, y_n) = 0$, $i = 1, \ldots, \omega$ can be extracted by the Gröbner basis method or resultant techniques.

2.3. The Scheme of Cotan and Teşeleanu

Before describing the scheme, we need to define some mathematical objects that are useful in the sequel. Let $(\mathbb{F}, +, \cdot)$ be a field. Let n be an integer and $a \in \mathbb{F}$ such that $x^n - a$ is irreducible in $\mathbb{F}[x]$. Define the quotient field

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

The product of two elements $a(x) = \sum_{i=0}^{n-1} a_i x^i$ and $b(x) = \sum_{i=0}^{n-1} b_i x^i$ of $\mathbb{A}_n$ can be computed by the rule

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

Consider the quotient group $\mathbb{B}_n = \mathbb{A}_n^*/\mathbb{F}^*$; then, elements of $\mathbb{B}_n$ are equivalence classes of the form

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

Note that $\mathbb{B}_n = \bigcup_{k=0}^{n-1} \mathbb{B}_k$, where

$$\mathbb{B}_k = \{a_0 + \ldots + a_{k-1}x^{k-1} + x^k \mid a_0, \ldots, a_{k-1} \in \mathbb{F}\}, \quad k = 0, \ldots, n-1,$$

and $\mathbb{B}_i \cap \mathbb{B}_j = \emptyset$ whenever $i \neq j$.

When p is a prime number and $\mathbb{F} = \mathbb{F}_p$ is the finite field of p elements, $\mathbb{A}_n$ becomes the Galois field of order p^n. Also, $\mathbb{B}_n$ is a cyclic group of order

$$\sum_{k=0}^{n-1} |\mathbb{F}_p|^k = \frac{p^n - 1}{p - 1}.$$

If m is a positive integer and $y \in \mathbb{B}_n$, denote by y^m the product of y in $\mathbb{B}_n$, $m - 1$ times. Hence, an analogous of Fermat's little theorem is given by

$$[a(x)]^{|\mathbb{B}_n|} \equiv 1 \pmod{p}, \quad \forall\, [a(x)] \in \mathbb{B}_n.$$

Observe that if $N = pq$ is the product of two prime numbers, and $\mathbb{F} = \mathbb{Z}/N\mathbb{Z}$, we obtain

$$|\mathbb{B}_n| = \frac{(p^n - 1)(q^n - 1)}{(p - 1)(q - 1)}.$$

Furthermore, for every $[a(x)] \in \mathbb{B}_n$, we also have

$$[a(x)]^{|\mathbb{B}_n|} \equiv 1 \pmod{N}.$$

The scheme of Cotan and Teşeleanu can be summarized as follows.

Key Generation

1. Select a positive integer $n > 1$ and a security size $\lambda > 0$.
2. Generate randomly two distinct large prime numbers of size λ.
3. Calculate $N = pq$ and $\psi_n(N) = \frac{(p^n-1)(q^n-1)}{(p-1)(q-1)}$.
4. Choose an integer a for which $x^n - a$ is irreducible in $\mathbb{Z}/p\mathbb{Z}[x]$, $\mathbb{Z}/q\mathbb{Z}[x]$, and $\mathbb{Z}/N\mathbb{Z}[x]$.
5. Select an integer e such that $\gcd(e, \psi_n(N)) = 1$ and compute d, the inverse of e modulo $\psi_n(N)$.
6. The public key is (N, n, a, e) and the private key is (p, q, d).

Encryption

1. Represent the plaintext as a polynomial

$$m(x) = m_0 + m_1 x + \ldots + m_{n-2}x^{n-2} + x^{n-1} \in \mathbb{B}_n.$$

2. Compute $c(x) \equiv [m(x)]^e \pmod N$.
3. The ciphertext is $c(x)$.

Decryption

To recover the plaintext $m(x)$, one needs to compute

$$m(x) \equiv [c(x)]^d \pmod N.$$

3. Solving the Equation $xH(y) + c \equiv 0 \pmod e$

In this section, we propose a new technique to find the small solutions of the modular equation $xH(y) + c \equiv 0 \pmod e$ where c is a constant, and $H(y) \in \mathbb{Z}[y]$ is a monic polynomial of degree r. The equation $xH(y) + c \equiv 0 \pmod e$ was previously studied by Kunihiro [21] and recently by Nitaj et al. [14]. In both works, the value xy^r is replaced by $z - c$, and the assumption $|c| < |x||y|^r$ is used. In this paper, we present a different method where xy^r is independent of c. This relaxes the condition $|c| < |x||y|^r$ used in [14,21], and it permits more applications in the cryptanalysis of some variants of RSA.

3.1. The New Method

Theorem 3. *Let $N = pq$ be an RSA modulus with $q < p < 2q$. Let $H(y) \in \mathbb{Z}[y]$ be a monic polynomial of degree $r \geq 1$. If $xH(y) + c \equiv 0 \pmod e$ with $e = N^\alpha$, $|x| \leq N^\beta$, $|y| \leq N^\gamma$, $|x||y|^r < e$, and*

$$\beta < \alpha + \frac{1}{3}r\gamma - \frac{2}{3}\sqrt{3r\alpha\gamma + r^2\gamma^2},$$

then one can find x and y in polynomial time.

Proof. Let $f(x,y) = xH(y) + c$ with $H(y) = y^r + a_{r-1}y^{r-1} + \ldots + a_0 \in \mathbb{Z}[y]$. We use Coppersmith's technique [17] and the strategy of Jochemsz and May [19] to find the small solutions of the equation $f(x,y) \equiv 0 \pmod e$. Let m be a positive integer and t be a positive value. For $0 \leq k \leq m$, consider the set

$$M_k = \bigcup_{0 \leq j' \leq \lfloor t \rfloor} \{x^i y^{j+j'} \mid \quad x^i y^j \text{ is a monomial of } f^m(x,y) \text{ and } \frac{x^i y^j}{(xy^r)^k} \text{ is a monomial of } f^{m-k}(x,y)\}.$$

A direct computation shows that the monomials $x^i y^j$ of $f^m(x,y)$ are composed by the couples (i,j) with

$$i = 0, \ldots, m, \quad j = 0, \ldots, ri.$$

Also, the monomials $x^i y^j$ of $f^{m-k}(x,y)$ are composed by (i,j) with

$$i = 0, \ldots, m-k, \quad j = 0, \ldots, ri.$$

This implies that the monomials $x^i y^j$ of M_k are composed by (i,j) with

$$i - k = 0, \ldots, m-k, \quad j - rk = 0, \ldots, r(i-k) + \lfloor t \rfloor,$$

or equivalently

$$i = k, \ldots, m, \quad j = rk, \ldots, ri + \lfloor t \rfloor$$

In the strategy of Jochemsz and May [19], we need to form the set $M_k \backslash M_{k+1}$. Since M_{k+1} is composed by the monomials $x^i y^j$ with

$$i = k+1, \ldots, m, \quad j = rk+r, \ldots, ri + \lfloor t \rfloor,$$

then $M_k \backslash M_{k+1}$ is the set of the monomials $x^i y^j$ composed by

$$\begin{aligned} &i = k+1, \ldots, m, \quad j = rk, rk+1, \ldots, rk+r-1, \\ &i = k, \quad j = rk, \ldots, rk + \lfloor t \rfloor. \end{aligned}$$

As in the strategy of Jochemsz and May, consider the list of polynomials

$$g_{k,i,j}(x,y) = \frac{x^i y^j}{(xy^r)^k} f(x,y)^k e^{m-k}, \; x^i y^j \in M_k \backslash M_{k+1}.$$

These polynomials reduce to

$$\begin{aligned} &g_{k,i,j}(x,y) = x^i y^j f(x,y)^k e^{m-k}, \\ &i = 1, \ldots, m-k, \quad j = 0, \ldots r-1, \\ &i = 0, \quad j = 0, \ldots, \lfloor t \rfloor. \end{aligned}$$

Using $f(x,y) = xH(y) + c = xy^r + x\left(a_{r-1}y^{r-1} + \ldots + a_0\right) + c$, we set $xy^r = z$, and $F(x,y,z) = z + x\left(a_{r-1}y^{r-1} + \ldots + a_0\right) + c$. Then, the polynomials $g_{k,i,j}(x,y)$ can be transformed into the following ones,

$$\begin{aligned} &G_{k,i,j}(x,y,z) = x^i y^j F(x,y,z)^k e^{m-k}, \\ &k = 0, \ldots, m, \quad i = 1, \ldots, m-k, \quad j = 0, \ldots, r-1, \\ &k = 0, \ldots, m, \quad i = 0, \quad j = 0, \ldots, \lfloor t \rfloor, \end{aligned}$$

where each term xy^r is replaced by z.

Let (x_0, y_0) be a solution of the equation $f(x,y) \equiv 0 \pmod{e}$, and $z_0 = x_0 y_0^r$. Then, (x_0, y_0, z_0) is a solution of the equation $F(x,y,z) \equiv 0 \pmod{e}$, and the polynomials $G_{k,i,j}(x,y,z)$ satisfy $G_{k,i,j}(x_0, y_0, z_0) \equiv 0 \pmod{e^m}$.

Define the bounds

$$X = N^{\beta}, \; Y = N^{\gamma}, \; Z = N^{\beta + r\gamma},$$

and assume that the solution (x_0, y_0, z_0) satisfies $|x_0| \leq X$, $|y_0| \leq Y$, $|z_0| \leq Z$. Following Coppersmith's method, we use the coefficient vectors of the polynomials $G_{k,i,j}(Xx, Yy, Zz)$ to form a matrix which is used as the basis matrix of a lattice $\mathcal{L}$. In this matrix, the rows are ordered so that $G_{k,i,j}(Xx, Yy, Zz) \prec G_{k',i',j'}(Xx, Yy, Zz)$ if $k < k'$, or if $k = k'$ and $i < i'$, or if $k = k'$, $i = i'$, and $j < j'$. Similarly, the monomials are ordered so that $z^k x^i y^j \prec z^{k'} x^{i'} y^{j'}$ if $k < k'$, or if $k = k'$ and $i < i'$, or if $k = k'$, $i = i'$, and $j < j'$. In Table 1, we present an example of the matrix of the lattice for $m = 2$, $t = 1$ where the symbols $\star$ are non-zero entries.

Table 1. The matrix of the lattice for $m = 2$, $t = 1$ with the polynomial $H(y) = y^3 + a_2 y^2 + a_1 y + a_0$.

$G_{k,i,j}$	$\mathbf{1}$	y	x	xy	xy^2	x^2	x^2y	x^2y^2	z	yz	xz	xyz	xy^2z	z^2	yz^2
$G_{0,0,0}$	e^2	0	0	0	0	0	0	0	0	0	0	0	0	0	0
$G_{0,0,1}$	0	e^2Y	0	0	0	0	0	0	0	0	0	0	0	0	0
$G_{0,1,0}$	0	0	e^2X	0	0	0	0	0	0	0	0	0	0	0	0
$G_{0,1,1}$	0	0	0	e^2XY	0	0	0	0	0	0	0	0	0	0	0
$G_{0,1,2}$	0	0	0	0	e^2XY^2	0	0	0	0	0	0	0	0	0	0
$G_{0,2,0}$	0	0	0	0	0	e^2X^2	0	0	0	0	0	0	0	0	0
$G_{0,2,1}$	0	0	0	0	0	0	e^2X^2Y	0	0	0	0	0	0	0	0
$G_{0,2,2}$	0	0	0	0	0	0	0	$e^2X^2Y^2$	0	0	0	0	0	0	0

Table 1. *Cont.*

$G_{k,i,j}$	$\mathbf{1}$	y	x	xy	xy^2	x^2	x^2y	x^2y^2	z	yz	xz	xyz	xy^2z	z^2	yz^2
$G_{1,0,0}$	$\star$	0	$\star$	$\star$	$\star$	0	0	0	Ze	0	0	0	0	0	0
$G_{1,0,1}$	0	$\star$	0	$\star$	$\star$	0	0	0	$\star$	YZe	0	0	0	0	0
$G_{1,1,0}$	0	0	$\star$	0	0	$\star$	$\star$	$\star$	0	0	XZe	0	0	0	0
$G_{1,1,1}$	0	0	0	$\star$	0	0	$\star$	$\star$	0	0	$\star$	$XYZe$	0	0	0
$G_{1,1,2}$	0	0	0	0	$\star$	0	0	$\star$	0	0	$\star$	$\star$	XY^2Ze	0	0
$G_{2,0,0}$	$\star$	0	$\star$	$\star$	$\star$	$\star$	$\star$	$\star$	$\star$	0	$\star$	$\star$	$\star$	Z^2	0
$G_{2,0,1}$	0	$\star$	0	$\star$	$\star$	0	$\star$	$\star$	$\star$	$\star$	$\star$	$\star$	$\star$	$\star$	YZ^2

By construction, the matrix of the lattice is triangular, and its determinant is the product of the diagonal terms

$$\det(\mathcal{L}) = X^{n_X} Y^{n_Y} Z^{n_Z} e^{n_e}. \tag{1}$$

To compute the former exponents, consider the function

$$S(v) = \sum_{k=0}^{m} \sum_{i=1}^{m-k} \sum_{j=0}^{r-1} v + \sum_{k=0}^{m} \sum_{i=0}^{0} \sum_{j=0}^{\lfloor t \rfloor} v.$$

Set $t = m\tau$ for $\tau \geq 0$. To ease the computations, we take $\lfloor m\tau \rfloor \approx m\tau$. The dominant parts of the exponents n_X, n_Y, n_Z, n_e as well as of the dimension ω of the lattice satisfy

$$\begin{aligned} n_X &= S(i) = \frac{1}{6} r m^3 + o(m^3) \\ n_Y &= S(j) = \frac{1}{2} \tau^2 m^3 + o(m^3) \\ n_Z &= S(k) = \frac{1}{6}(3\tau + r) m^3 + o(m^3) \\ n_e &= S(m-k) = \frac{1}{6}(3\tau + 2r) m^3 + o(m^3) \\ \omega &= S(1) = \frac{1}{2}(2\tau + r) m^2 + o(m^2). \end{aligned} \tag{2}$$

After applying the LLL algorithm to the matrix of the lattice $\mathcal{L}$, we obtain a reduced matrix from which we can extract ω new polynomials $h_{k,i,j}(x, y, z)$. To combine Theorems 1 and 2 with $i = 3$, we set

$$2^{\frac{\omega(\omega-1)}{4(\omega-2)}} \det(\mathcal{L})^{\frac{1}{\omega-2}} < \frac{e^m}{\sqrt{\omega}}.$$

Using (1), this reduces to

$$e^{n_e - m(\omega-2)} X^{n_X} Y^{n_Y} Z^{n_Z} < \frac{2^{-\frac{\omega(\omega-1)}{4}}}{\left(\sqrt{\omega}\right)^{\omega-2}}. \tag{3}$$

Using the dominant parts (2) with $X = N^\beta$, $Y = N^\gamma$, $Z = N^{\beta + r\gamma}$, and $e = N^\alpha$, we obtain, after neglecting some small terms

$$\left(\frac{1}{6}(3\tau + 2r) - \frac{1}{2}(2\tau + r)\right)\alpha + \frac{1}{6} r\beta + \frac{1}{2}\gamma\tau^2 + \frac{1}{6}(3\tau + r)(\beta + r\gamma) < 0.$$

Rearranging, we obtain

$$3\gamma\tau^2 + 3(r\gamma - \alpha + \beta)\tau + r^2\gamma - r\alpha + 2r\beta < 0, \tag{4}$$

in which the optimal value for τ is $\tau_0 = \frac{\alpha-\beta-r\gamma}{2\gamma}$. Since $e > |x||y|^r$, then $\alpha > \beta + r\gamma$, and $\tau_0 > 0$. Then, plugging τ_0 in (4), we obtain

$$-3\beta^2 + (6\alpha + 2r\gamma)\beta - 3\alpha^2 + 2r\gamma\alpha + r^2\gamma^2 < 0,$$

which leads to

$$\beta < \alpha + \frac{1}{3}r\gamma - \frac{2}{3}\sqrt{3r\alpha\gamma + r^2\gamma^2}.$$

We notice that the former bound is positive since $\alpha > \beta + r\gamma$. Under this bound, using three reduced polynomials $h_1(x,y,z), h_2(x,y,z), h_3(x,y,z)$, we can extract the solution (x_0, y_0, z_0) by the Gröbner basis method or resultant computations. This terminates the proof. □

3.2. A Numerical Example

In this section, we present a small numerical example to show the details of the resolution method of Theorem 3 with $n = 4$, and $r = n - 1 = 3$. Consider the following parameters

$$\begin{aligned} N &= 463028995904606051817018641173, \\ c &= 895087879645377698399589802186741096954354552299285\backslash \\ &\quad 874926542281770464634989776173600270 22, \\ e &= 172459409963116822030248732348419638390904926885797\backslash \\ &\quad 131150907194065829062468518630339169 22. \end{aligned}$$

Then, $e = N^\alpha$ with $\alpha \approx 2.97437$, and $p + q < 3\sqrt{N}$, so that $y < 3N^\gamma$ with $\gamma = \frac{1}{2}$. Set $\beta = \frac{1}{2}$. Then, the conditions of Theorem 3 are satisfied since $\alpha > \beta + r\gamma = 2$, and $\beta < \alpha + \frac{1}{3}r\gamma - \frac{2}{3}\sqrt{3r\alpha\gamma + r^2\gamma^2} \approx 0.838$. The goal is to find a small solution (x_0, y_0) of the equation $xH(y) + c \equiv 0 \pmod{e}$ where $H(y)$ is derived from

$$\psi_4(N) = (p+q)^3 + (N+1)(p+q)^2 + \left(N^2 - 2N + 1\right)(p+q) + N^3 - N^2 - N + 1,$$

with $p + q = y$, that is

$$H(y) = y^3 + (N+1)y^2 + \left(N^2 - 2N + 1\right)y + N^3 - N^2 - N + 1.$$

Consider the bounds $|x_0| \le X$, $|y_0| \le Y$, and $|x_0 y_0^3| \le Z$ with

$$\begin{aligned} X &= \left\lfloor N^{0.5} \right\rfloor = 680462339813605, \\ Y &= \left\lfloor 3N^{0.5} \right\rfloor = 2041387019440815, \\ Z &= XY^3 = 57886879783075473856583677199173978274072553269 8185\backslash \\ &\quad 4011616875. \end{aligned}$$

Let $m = 4$, $t = 2$, and

$$F(x,y,z) = z + x\left((N+1)y^2 + \left(N^2 - 2N + 1\right)y + N^3 - N^2 - N + 1\right) + c.$$

The lattice $\mathcal{L}$ is constructed with the coefficients of the polynomials defined by

$$\begin{aligned} &G_{k,i,j}(x,y,z) = x^i y^j F(x,y,z)^k e^{m-k}, \\ &k = 0, \ldots, m, \quad i = 1, \ldots, m-k, \quad j = 0, \ldots, r-1, \\ &k = 0, \ldots, m, \quad i = 0, \quad j = 0, \ldots, \lfloor t \rfloor, \end{aligned}$$

where each term xy^r is replaced by z. The dimension of the lattice is $\omega = 45$. After reducing the lattice with the LLL algorithm, and solving a system formed by three polynomial equations over the integers with the Gröbner basis method, we find the solution

$$\begin{aligned} x_0 &= 16165734257585, \\ y_0 &= 1360935721901674, \\ z_0 &= 4074818564895003591068030402887264755851830979982675503204 0. \end{aligned}$$

Using $p + q = y_0$ and $pq = N$, we obtain

$$p = 683209007134751, \quad q = 677726714766923,$$

and the factorization of N is complete. Notice that $\frac{c}{x_0 y_0^3} > 10^{30}$, and c is much larger than $|x_0 y_0^3|$. This shows that the methods described in [14,21] cannot be applied to solve the equation $xH(y) + c \equiv 0 \pmod{e}$.

4. Partial Key Attack on the Scheme of Cotan and Teşeleanu with Known LSBs

In this section, we apply Theorem 3 to attack the scheme of Cotan and Teşeleanu when the attacker knows the s least significant bits (LSBs) of d so that $d = d_1 M + d_0$ for $M = 2^s$, with known d_0, and unknown d_1.

Theorem 4. *Let $n \geq 2$, and $N = pq$ be the product of two unknown prime factors with $q < p < 2q$. Let $e = N^\alpha$, and $d \leq N^\delta$ such that $ed \equiv 1 \pmod{\psi_n(N)}$ with $\psi_n(N) = \frac{(p^n-1)(q^n-1)}{(p-1)(q-1)}$. Let M and d_0 be two known integers such that $d = d_1 M + d_0$ with $M = N^\mu$. Then, one can factor N in polynomial time if*

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

Proof. In the equation $ed - k\psi_n(N) = 1$, assume that $d = d_1 M + d_0$ where M and d_0 are known, and d_1 is unknown. We assume the following bounds

$$e = N^\alpha, \ M = N^\mu, \ d \leq N^\delta.$$

We rewrite the equation $ed - k\psi_n(N) = 1$ as

$$k\psi_n(N) - ed_0 + 1 = ed_1 M,$$

where by Lemma 5, $\psi_n(N) = (p+q)^{n-1} + \sum_{j=0}^{n-2} a_j (p+q)^j$ with known coefficients a_j, $j = 0, \ldots, n-2$. Let $H(y) = y^{n-1} + \sum_{j=0}^{n-2} a_j y^j$, and consider the polynomial

$$f(x, y) = xH(y) - ed_0 + 1.$$

Then, $(x_0, y_0) = (k, p+q)$ satisfies $f(x_0, y_0) \equiv 0 \pmod{eM}$. By Lemma 1, we have $y_0 < 3\sqrt{N}$. Also, we have

$$x_0 = k = \frac{ed-1}{\psi_n(N)} < N^{\alpha+\delta-n+1}.$$

We can then apply Theorem 3 where α is replaced by $\alpha + \mu$, β is replaced by $\alpha + \delta - n + 1$, $\gamma = \frac{1}{2}$, and $r = n - 1$. Then, the inequality $\beta < \alpha + \frac{1}{3}r\gamma - \frac{2}{3}\sqrt{3r\alpha\gamma + r^2\gamma^2}$ in Theorem 3 leads to

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

After finding the solutions of the equation $f(x,y) \equiv 0 \pmod{eM}$, only one satisfies $(x_0, y_0) = (k, p+q)$. Then, combining $y_0 = p+q$, and $N = pq$, this leads to the factorization of N and terminates the proof. □

5. Cryptanalysis of the Scheme of Cotan and Teşeleanu with a Known Approximation of One of the Primes

In this section, we consider the scheme of Cotan and Teşeleanu with $N = pq$ when $p < q < 2q$, and an approximation p_0 of p is known.

Theorem 5. *Let $n \geq 2$, and $N = pq$ be the product of two unknown prime factors with $q < p < 2q$. Suppose that $ed - k\psi_n(N) = 1$ with $\psi_n(N) = \frac{(p^n-1)(q^n-1)}{(p-1)(q-1)}$, $e = N^\alpha$, and $d \leq N^\delta$. Let p_0 be an approximation of p with $|p - p_0| < N^\mu$. Then, one can factor N in polynomial time if*

$$\delta < \left(1 + \frac{1}{3}\mu\right)(n-1) - \frac{2}{3}\sqrt{3(n-1)\mu\alpha + (n-1)^2\mu^2}.$$

Proof. Suppose that $ed - k\psi_n(N) = 1$ with $e = N^\alpha$ and $d \leq N^\delta$. This implies that $k\psi_n(N) + 1 \equiv 0 \pmod{e}$. Let p_0 be an approximation of p with $|p - p_0| < N^\gamma$. Then, by Lemma 2, the integer $q_0 = \left\lfloor \frac{N}{p_0} \right\rfloor$ is an approximation of q such that $|q - q_0| < N^\mu$ and $|p+q-p_0-q_0| < 2N^\mu$. Set $M = p_0 + q_0$. By Lemma 6, one has $\psi_n(N) = (p+q-M)^{n-1} + \sum_{j=0}^{n-2} a_j^{(n)}(p+q-M)^j$. Then, the equation $k\psi_n(N) + 1 \equiv 0 \pmod{e}$ can be rewritten as

$$k\left((p+q-M)^{n-1} + \sum_{j=0}^{n-2} a_j^{(n)}(p+q-M)^j\right) + 1 \equiv 0 \pmod{e}.$$

Consider the polynomial $F(x,y) = xH(y) + 1$ with $H(y) = y^{n-1} + \sum_{j=0}^{n-2} a_j^{(n)} y^j$. Then, $(x_0, y_0) = (k, p+q-M)$ is a solution of the modular polynomial equation $F(x,y) \equiv 0 \pmod{e}$. Using $ed - k\psi_n(N) = 1$, $e = N^\alpha$, $d \leq N^\delta$, and since $\psi_n(N) > p^{n-1}q^{n-1} = N^{n-1}$, we obtain

$$k = \frac{ed-1}{\psi_n(N)} < \frac{N^{\alpha+\delta}}{N^{n-1}} = N^{\alpha+\delta-n+1}.$$

Let $X = N^{\alpha+\delta-n+1}$ and $Y = N^\gamma$. Then, using $r = n-1$, $\gamma = \mu$, and $\beta = \alpha + \delta - n + 1$ in Theorem 3, we obtain

$$\delta < \left(1 + \frac{1}{3}\mu\right)(n-1) - \frac{2}{3}\sqrt{3(n-1)\mu\alpha + (n-1)^2\mu^2}.$$

After finding the solutions of the equation $F(x,y) \equiv 0 \pmod{e}$, only one satisfies $(x_0, y_0) = (k, p+q-M)$. Then, combining $y_0 + M = p+q$, and $N = pq$, this leads to the factorization of N and terminates the proof. □

6. Cryptanalysis of the Scheme of Cotan and Teşeleanu with Primes Sharing MSBs

The following result is a direct application of Theorem 5. It concerns the case of a modulus $N = pq$ where the prime difference $|p - q|$ is small.

Corollary 1. *Let $n \geq 2$ and $N = pq$ be the product of two unknown prime factors with $q < p < 2q$ and $p - q < N^\mu$. Suppose that $ed - k\psi_n(N) = 1$ with $\psi_n(N) = \frac{(p^n-1)(q^n-1)}{(p-1)(q-1)}$, $e = N^\alpha$, and $d \leq N^\delta$. Then, one can factor N in polynomial time if*

$$\delta < \left(1 + \frac{1}{3}\mu\right)(n-1) - \frac{2}{3}\sqrt{3(n-1)\mu\alpha + (n-1)^2\mu^2}.$$

Proof. Suppose that $p - q < N^{\mu}$. Since, by Lemma 1, we have $q < \sqrt{N} < p$, one obtains

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

This implies that $p_0 = \sqrt{N}$ is an approximation of p such that $|p - p_0| < N^{\mu}$. Then, using Theorem 5, one can factor $N = pq$ if

$$\delta < \left(1 + \frac{1}{3}\mu\right)(n-1) - \frac{2}{3}\sqrt{3(n-1)\mu\alpha + (n-1)^2\mu^2}.$$

This terminates the proof. □

7. Cryptanalysis of the Scheme of Cotan and Teşeleanu with Primes Sharing LSBs

In this section, we propose an attack on the scheme of Cotan and Teşeleanu when the prime factors share an amount of their least significant bits.

Let $N = pq$ be an RSA modulus with $q < p < 2q$. Suppose that p and q share their least significant bits so that $p - q = 2^s u$ for a known s and an unknown u. Then, the following result shows that one can find the s least significant bits of p and q and the $2s$ least significant bits of $p + q$ (see [22,23]).

Lemma 7. *Let $N = pq$ be an RSA modulus with $q < p < 2q$. Suppose that $p - q = 2^s u$ with a known s and an unknown u. Let u_0 be a solution of the equation $z^2 \equiv N \pmod{2^s}$ and*

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

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

For $p + q = 2^{2s} v + v_0$, the following Lemma shows that $\psi_n(N)$ can be expressed as a polynomial in v with integer coefficients.

Lemma 8. *Let $N = pq$, $n \geq 2$, $\psi_n(N) = \frac{(p^n-1)(q^n-1)}{(p-1)(q-1)}$, with $p + q = 2^{2s} v + v_0$. Then, there exist $n - 1$ coefficients $b_j^{(n)} \in \mathbb{Z}$, $j = 0, \ldots, n-2$, depending only on N, n, s, and v_0 such that*

$$\psi_n(N) = 2^{2s(n-1)} v^{n-1} + \sum_{j=0}^{n-2} b_j^{(n)} v^j.$$

Proof. Since $p + q = 2^{2s} v + v_0$, then $p + q - v_0 = 2^{2s} v$. Then, by Lemma 6, with $M = v_0$, there exist $n - 1$ integers $a_j^{(n)}$, $j = 0, \ldots, n-2$, such that

$$\psi_n(N) = (p + q - v_0)^{n-1} + \sum_{j=0}^{n-2} a_j^{(n)} (p + q - v_0)^j.$$

Then,

$$\begin{aligned}
\psi_n(N) &= \left(2^{2s} v\right)^{n-1} + \sum_{j=0}^{n-2} a_j^{(n)} \left(2^{2s} v\right)^j \\
&= 2^{2s(n-1)} v^{n-1} + \sum_{j=0}^{n-2} 2^{2sj} a_j^{(n)} v^j \\
&= 2^{2s(n-1)} v^{n-1} + \sum_{j=0}^{n-2} b_j^{(n)} v^j,
\end{aligned}$$

where $b_j = 2^{2sj} a_j^{(n)}$, $j = 0, \ldots, n-2$. This terminates the proof. □

The following result concerns the situation where the prime factors p and q share their least significant bits.

Theorem 6. *Let $n \geq 2$ and $N = pq$ be an RSA modulus with $q < p < 2q$. Suppose that $e = N^{\alpha}$ is odd and satisfies the equation $ed - k\psi_n(N) = 1$ with $\psi_n(N) = \frac{(p^n-1)(q^n-1)}{(p-1)(q-1)}$ and $d \leq N^{\delta}$. Suppose that p and q share their s least significant bits with $2^s = N^{\mu}$. If*

$$\delta < \left(\frac{7}{6} - \frac{2}{3}\mu\right)(n-1) - \frac{2}{3}\sqrt{3(n-1)\alpha\left(\frac{1}{2} - 2\mu\right) + (n-1)^2\left(\frac{1}{2} - 2\mu\right)^2}.$$

then one can factor N in polynomial time.

Proof. Assume that p and q share their least significant bits so that $p - q = 2^s v$. Let u_0 be a solution of the equation $z^2 \equiv N \pmod{2^s}$ and,

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

Then, by Lemma 7, we have $p = 2^s p_1 + u_0$, $q = 2^s q_1 + u_0$, and $p + q = 2^{2s} v + v_0$. The equation $ed - k\psi_n(N) = 1$ can be rewritten as $k\psi_n(N) + 1 \equiv 0 \pmod{e}$, and by Lemma 8, we have

$$\psi_n(N) = 2^{2s(n-1)} v^{n-1} + \sum_{j=0}^{n-2} b_j^{(n)} v^j.$$

Suppose that e is odd. Then, $\gcd(2, e) = 1$, and the equation $k\psi_n(N) + 1 \equiv 0 \pmod{e}$ can be rewritten as

$$k\left(v^{n-1} + \sum_{j=0}^{n-2} b_j^{(n)} 2^{-2s(n-1)} v^j\right) + 2^{-2s(n-1)} \equiv 0 \pmod{e},$$

where $2^{-2s(n-1)}$ is the inverse of $2^{2s(n-1)}$ modulo e. Consider the polynomial $F(x, y) = xH(y) + c$ where $H(y) = y^{n-1} + \sum_{j=0}^{n-2} b_j^{(n)} 2^{-2s(n-1)} y^j \pmod{e}$, and $c \equiv 2^{-2s(n-1)} \pmod{e}$. Then, $(x_0, y_0) = (k, v)$ is a solution of the equation $F(x, y) \equiv 0 \pmod{e}$. Theorem 3 can then be applied to find the small solutions. Assume that $e = N^{\alpha}$, $d \leq N^{\delta}$, and $2^s = N^{\mu}$. Then, using $ed - k\psi_n(N) = 1$, we obtain

$$k = \frac{ed - 1}{\psi_n(N)} < N^{\alpha + \delta - n + 1}.$$

Also, using $p + q = 2^{2s} v + v_0 < 3\sqrt{N}$, we obtain

$$v = \frac{p + q - v_0}{2^{2s}} < 3N^{\frac{1}{2} - 2\mu}.$$

Observe that $\frac{1}{2} - 2\mu > 0$. Otherwise, one obtains $v \leq 2$, that is $p + q = 2^{2s} v + v_0$ with $v \in \{1, 2\}$. This leads to the factorization of N.

Let $X = N^{\alpha + \delta - n + 1}$, and $Y = 3N^{\frac{1}{2} - 2\mu}$. Then, applying Theorem 3 with $\beta = \alpha + \delta - n + 1$, $\gamma = \frac{1}{2} - 2\mu$, and $r = n - 1$, we can find the solution $(x_0, y_0) = (k, v)$ if

$$\delta < \left(\frac{7}{6} - \frac{2}{3}\mu\right)(n-1) - \frac{2}{3}\sqrt{3(n-1)\alpha\left(\frac{1}{2} - 2\mu\right) + (n-1)^2\left(\frac{1}{2} - 2\mu\right)^2}.$$

Using $N = pq$ and $v = y_0$, we obtain $p + q = 2^{2s} v + v_0$. This leads to the factorization of N. □

8. Conclusions

In this paper, we proposed a new technique to solve the modular equation $xH(y) + c \equiv 0 \pmod{e}$ for small unknown integers x, y, and for an arbitrary value of c where $H(y) \in \mathbb{Z}[y]$ is a monic polynomial of degree $r \geq 1$. The methodology is based on Coppersmith's method and lattice basis reduction. It finds the solutions in contrast to the former methods which fail when $|c| \geq |xy^r|$. As an application of our method, we present four attacks on the scheme of Cotan and Teşeleanu, namely a partial key exposure attack with known least significant bits, a partial prime exposure attack, and two attacks when the prime factors share their least or most significant bits.

Author Contributions: Conceptualization, M.R. and A.N.; methodology, M.R. and A.N.; software, M.R. and A.N.; validation, M.R., A.N. and M.Z.; formal analysis, M.R. and A.N.; investigation, M.R. and A.N.; resources, M.R. and A.N.; data curation, M.R. and A.N.; writing—original draft preparation, M.R. and A.N.; writing—review and editing, M.R. and A.N.; visualization, M.R. and A.N.; supervision, M.R., A.N. and M.Z.; project administration, M.R., A.N. and M.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding

Data Availability Statement: Data are contained within the article.

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

Abbreviations

The following abbreviations are used in this manuscript:

RSA	Rivest, Shamir, Adleman
KMOV	Koyama, Maurer, Okamoto, Vanstone
CRT	Chinese Remainder Theorem
MSBs	most significant bits
LSBs	least significant bits
LLL	Lenstra, Lenstra, and Lovász

References

1. Rivest, R.; Shamir, A.; Adleman, L. A Method for Obtaining digital signatures and public-key cryptosystems. *Commun. ACM* **1978**, *21*, 120–126. [CrossRef]
2. Wiener, M. 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 *Advances in Cryptology-Eurocrypt'99, Lecture Notes in Computer Science*; Springer: Berlin/Heidelberg, Germany, 1999; Volume 1592, pp. 1–11.
4. Quisquater, J.J.; Couvreur, C. Fast decipherment algorithm for RSA public-key cryptosystem. *Electron. Lett.* **1982**, *18*, 905–907. [CrossRef]
5. Koyama, K.; Maurer, U.M.; Okamoto, T.; Vanstone, S.A. New public-key schemes based on elliptic curves over the ring $\mathbb{Z}_n$. In *Advances in Cryptology—CRYPTO 1991, Lecture Notes in Computer Science*; Springer: Berlin/Heidelberg, Germany, 1991; Volume 576, pp. 252–266.
6. Collins, T.; Hopkins, D.; Langford, S.; Sabin, M. Public Key Cryptographic Apparatus and Method. US Patent 5,848,159, 16 January 1997.
7. Takagi, T. A fast RSA-type public-key primitive modulo $p^k q$ using Hensel lifting. *IEICE Trans.* **2004**, *87*, 94–101.
8. Murru, N.; Saettone, F.M. A Novel RSA-Like Cryptosystem Based on a Generalization of the Rédei Rational Functions. In *Number-Theoretic Methods in Cryptology. NuTMiC 2017. Lecture Notes in Computer Science*; Kaczorowski, J., Pieprzyk, J., Pomykala, J., Eds.; Springer: Cham, Switzerland, 2018; Volume 10737.
9. Feng, Y.; Nitaj, A.; Pan, Y. Partial prime factor exposure attacks on some RSA variants. In *Theoretical Computer Science*; Elsevier: Amsterdam, The Netherlands, 2024; Volume 999, p. 114549.
10. 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*; Springer: Berlin/Heidelberg, Germany, 2021; Volume 12912, pp. 151–167.
11. Shi, G.; Wang, G.; Gu, D. Further Cryptanalysis of a Type of RSA Variants. In *Information Security. ISC 2022. Lecture Notes in Computer Science*; Susilo, W., Chen, X., Guo, F., Zhang, Y., Intan, R., Eds.; Springer: Cham, Switzerland, 2022; Volume 13640.
12. Zheng, M.; Kunihiro, N.; Yao, Y. Cryptanalysis of the RSA variant based on cubic Pell equation. *Theor. Comput. Sci.* **2021**, *889*, 135–144. [CrossRef]

13. Cotan, P.; Teşeleanu, G. Continued fractions applied to a family of RSA-like cryptosystems. In *Information Security Practice and Experience. ISPEC 2022. Lecture Notes in Computer Science*; Su, C., Gritzalis, D., Piuri, V., Eds.; Springer: Cham, Switzerland, 2022; Volume 13620, pp. 589–605.
14. Nitaj, A.; Adenan, N.N.H.; Ariffin, M.R.K. Cryptanalysis of a New Variant of the RSA Cryptosystem. In *Progress in Cryptology—AFRICACRYPT 2024. AFRICACRYPT 2024. Lecture Notes in Computer Science*; Vaudenay, S., Petit, C., Eds.; Springer: Cham, Switzerland, 2024; Volume 14861.
15. Lenstra, A.K.; Lenstra, H.W.; Lovász, L. Factoring polynomials with rational coefficients. *Math. Ann.* **1982**, *261*, 513–534. [CrossRef]
16. May, A. New RSA Vulnerabilities Using Lattice Reduction Methods. Ph.D. Thesis, University of Paderborn, Paderborn, Germany, 2003.
17. Coppersmith, D. Small solutions to polynomial equations, and low exponent RSA vulnerabilities. *J. Cryptol.* **1997**, *10*, 233–260. [CrossRef]
18. Howgrave-Graham, N. Finding small roots of univariate modular equations revisited. In *Cryptography and Coding, LNCS 1355*; Springer: Berlin/Heidelberg, Germany, 1997; pp. 131–142.
19. Jochemsz, E.; May, A. A strategy for finding roots of multivariate polynomials with new applications in attacking RSA variants. In *ASIACRYPT 2006, LNCS 4284*; Springer: Berlin/Heidelberg, Germany, 2006; pp. 267–282.
20. Peng, L.; Hu, L.; Lu, Y.; Wei, H. An improved analysis on three variants of the RSA cryptosystem. In Proceedings of the International Conference on Information Security and Cryptology, Beijing, China, 4–6 November 2016; Springer: Cham, Switzerland, 2016; Volume 10143, pp. 140–149.
21. Kunihiro, N. On Optimal Bounds of Small Inverse Problems and Approximate GCD Problems with Higher Degree. In *Information Security. ISC 2012. Lecture Notes in Computer Science*; Gollmann, D., Freiling, F.C., Eds.; Springer: Berlin/Heidelberg, Germany, 2012; Volume 7483.
22. Nitaj, A.; Ariffin, M.R.K.; Nassr, D.I.; Bahig, H.M. New attacks on the RSA cryptosystem. In *AFRICACRYPT 2014, LNCS 8469*; Pointcheval, D., Vergnaud, D., Eds.; Springer: Berlin/Heidelberg, Germany, 2014; p. 178198.
23. Steinfeld, R.; Zheng, Y. On the Security of RSA with Primes Sharing Least-Significant Bits. *Appl. Algebra Eng. Commun. Comput.* **2004**, *15*, 179200. [CrossRef]