A New Generalized Attack on RSA-like Cryptosystems

Michel SECK[1], Oumar Niang[1], and Djiby Sow[2]

[1] LTISI, CRISIN'2D, Ecole Polytechnique de Thies, Senegal
{mseck,oniang}@ept.edu.sn
[2] Dept. Mathematics and Computer Science, FST, UCAD, Senegal
djiby.sow@ucad.edu.sn

Abstract. Rivest, Shamir, and Adleman published the RSA cryptosystem in 1978, which has been widely used over the last four decades. The security of RSA is based on the difficulty of factoring large integers $N = pq$, where p and q are prime numbers. The public exponent e and the private exponent d are related by the equation $ed-k(p-1)(q-1) = 1$. Recently, Cotan and Teşeleanu (NordSec 2023) introduced a variant of RSA, where the public exponent e and the private exponent d satisfy the equation $ed - k(p^n - 1)(q^n - 1) = 1$ for some positive integer n. In this paper, we study the general equation $eu - (p^n - 1)(q^n - 1)v = w$ with positive integers u and v, and $w \in \mathbb{Z}$. We show that, given the public parameters N and e, one can recover u and v and factor the modulus N in polynomial time by combining continued fractions with Coppersmith's algorithm which relies on lattice reduction techniques, under specific conditions on u, v, and w. Furthermore, we show that if the private exponent d in an RSA-like cryptosystem is either small or too large, then N can be factored in polynomial time. This attack applies to the standard RSA cryptosystem.

Keywords: RSA · Continued fractions · Crypanalysis · Coppersmith's method · Generalized Wiener attack

1 Introduction

The RSA cryptosystem [RSA78], published in 1978 by Ron Rivest, Adi Shamir, and Leonard Adleman, is a widely used cryptographic primitive over the past four decades that enables secure data transmission over insecure channels. Its security relies on the computational difficulty of factoring an integer $N = pq$ which is a product of two large prime numbers, a problem believed to be intractable for classical computers when N is big. The public key $pk = (N, e)$ and the private key $sk = (N, d)$ are related by the equation $ed - k(p - 1)(q - 1) = 1$ for some positive integer k. To obtain a safe private key, the public exponent e, the private exponent d and the parameter k should be chosen carefully. It is well known that if these parameters are too small, then RSA cryptosystem is vulnerable. For instance, Håstad [Hås86] has showed that when the same message m is encrypted

with multiple public keys $(e, N_1), (e, N_2), \ldots, (e, N_s)$ sharing a same small public exponent e (e.g. $e = 3$) and broadcast to multiple recipients, then m can be recovered in polynomial time given only the public information. Wiener [Wie90] show in 1990 that if the private exponent $d < \frac{1}{3}N^{\frac{1}{4}}$, then the modulus N can be factored in polynomial time by using continued fractions[Moo64] by exploiting the equation

$$ed - k(p-1)(q-1) = 1 \tag{1}$$

This bound was later improved by Boneh and Durfee [BD99] who have proved that the primes p and q can be recovered in polynomial time if $d < N^{0.292}$. Their attack is based on Coppersmith's method [May03,HG97] which is based on lattice reduction techniques, especially the LLL algorithm [LLL82]. Recently, Cotan and Teşeleanu [CT23] (NordSec 2023) have proposed a variant of RSA cryptosystem where the public exponent e and the private exponent d are related by the equation

$$ex - (p^n - 1)(q^n - 1)y = 1 \tag{2}$$

where n is a positive intger. Notice that the RSA equation is a spacial case of this generalized equation ($n = 1$).

In this paper, we are mainly interested to the crypanalysis of this Cotan and Teşeleanu cryptosystem. More specifically, we study the generalized equation

$$eu - (p^n - 1)(q^n - 1)v = w \tag{3}$$

where u and v are positive integers and $w \in \mathbb{Z}$. The key ingredients of our attack is combining continued fractions and Coppersmith's method to successfully recover u, v, and the factors p and q in polynomial time under specific conditions on u, v and w.

1.1 Related works

We summarize the generalized Wiener attack on some RSA-like cryptosystems combining the continued fractions and Coppersmith's method.

Blömer and May attack [BM04]. In 2004, Blömer and May proposed, to our knowledge, the first generalized Wiener attack combining continued fractions and Coppersmith's method. They proved that, for an RSA modulus $N = pq$, if the pubblic exponent e satisfies the equation

$$ex + y = (p-1)(q-1)k \tag{4}$$

with $0 < x < \frac{1}{3}\sqrt{\frac{(p-1)(q-1)}{e}}\frac{N^{3/4}}{p-q}$ and $|y| < \frac{p-q}{(p-1)(q-1)\cdot N^{3/4}} \cdot ex$. Then one can factor N in polynomial time in $\log(N)$.

Nitaj attack [Nit08]. In 2008, Nitaj [Nit08] proposed another generalized attack on RSA cryptosystem. He showed that if the public exponent e is related to the equation

$$eX - (p-u)(q-v)Y = 1 \tag{5}$$

with integers X, Y, u, v such that

$$1 \leq X < Y < 2^{-1/4}N^{1/4}, |u| < N^{1/4}, v = \left[-\frac{qu}{p-u}\right]$$

with the extra condition on $p-u$ and $(q-v)$ yields the factorization of $N = pq$.

Another Nitaj attack [Nit14]. In 1991, Koyama, Maurer, Okamoto and Vanstone [KMOV92] introduced a new public key cryptosystem on elliptic curves over the ring $\mathbb{Z}/N\mathbb{Z}$, with $N = pq$, called KMOV, where e and d are related to the equation $ed-(p+1)(q+1)k = 1$. Nitaj have proposed a generalized Wiener attack on their scheme. He have showed that if the public exponent e satisfies an equation

$$ex - (p+1)(q+1)y = z \tag{6}$$

where x and y are positive integers with $\gcd(x, y) = 1$ and

$$|z| < \frac{(p-q)N^{1/4}y}{3(p+q)} \text{ and } xy < \frac{\sqrt{2N}}{12}$$

Then one can recover p and q in polynomial time.

Bunder et al. attack [BNST17]. In 2002, Elkamchouchi, Elshenawy and Shaban [EES02] adapted RSA to the Gaussian domain by using a modulus of the form $N = PQ$ where P and Q are two Gaussian primes. their exponents e and d are related to the equation $ed - (p^2-1)(q^2-1)k = 1$. In 2017, Bunder et al. [BNST17] proposed an attack that factors the modulus $N = pq$ in their schemes by using the generalized equation

$$ex - (p^2-1)(q^2-1)y = z \tag{7}$$

by combining the continued fraction algorithm and Coppersmith's method.

1.2 Our contributions

In this paper, we study a generalized Wiener attack for RSA-like cryptosystems whose their public exponent e and the private exponent d satisfy the generalized equation

$$eu - (p^4-1)(q^4-1)v = w \tag{8}$$

We get the following result:

- Combining continued fractions and Coppersmith's method, we show that one can recover u, v and the primes p and q in polynomial time in $\log(N)$ if $uv < (2N^4 - 49N^2 + 2)/(4N + 170N^2)$ and $|w| < vN$.

- We have also proposed a generic attack for some RSA-like cryptosystems when e is related to the equation

$$ex - y\psi(p,q) = z \text{ with } |z| < \mathcal{B}_2,\ \mathcal{B}_2 \geq 1 \tag{9}$$

  We show that if there is 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 exist positive integers x and y with $xy < \mathcal{B}_1 \in \mathbb{R}^+$ (resp. $x < \mathcal{B}_1 \in \mathbb{R}^+$) satisfying Equation 9, then using $\mathcal{A}$, one can factor N in polynomial time given N and a public exponent $0 < e' < \psi(p,q)$ such that the corresponding private exponent $d' = \psi(p,q) - d$ for some $d < \sqrt{\mathcal{B}_1}$ (resp. $d < \mathcal{B}_1$).

- A consequence of the previous result is that for many RSA-like cryptosystems, including standard RSA and the Cotan-Teşeleanu cryptosystem [CT23], if the private key d, $0 < d < \psi(p,q)$ is too large, then one can factor N in polynomial time. To the best of our knowledge, this result is novel. In general, for RSA-like cryptosystems, it is well known that if d is small, i.e. $d < N^\delta$ for some positive real δ, then N can be factored in polynomial time [MP19,May03,Bon99].

- We give an algorithm that is able to generate weak RSA public key instances (N, e) in polynomial time such that (N, e) is vulnerable to our attack but safe for classical Wiener-like attacks. We provide a proof-of-concept implementation [3] in SageMath [Dev24] for this algorithm and for our generalized attack.

Organization of this paper. The rest of this paper is organized as follows. Section 2 is devoted to the preliminaries on continued fractions, Coppersmith's method and the Cotan and Teşeleanu cryptosystem [CT23]. In Section 3, we detail our generalized Wiener attack on Cotan and Teşeleanu cryptosystem [CT23]. In Section 4, we show how to recover p and q in polynomial time if the private exponents d of RSA-like cryptosystems are large. We conclude our work in the final Section 5

2 Preliminaries

In this section, we recall useful properties on continued fractions expansion and Legendre's Theorem. We also summarize the Coppersmith's method for factoring integers $N = pq$ given an approximation $\widehat{p}$ of p such that $|p - \widehat{p}| < N^{1/4}$. We terminate by presenting the algorithms of Cotan and Teşeleanu cryptosystem [CT23].

[3] https://github.com/mseckept/generalized-wiener-attack

2.1 Continued Fractions

Definition 1 (continued fraction[HW79,Moo64]). *A continued fraction is an expression of the form:*

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots}}}$$

where a_0 is an integer and $a_1, a_2, a_3, \ldots$ are positive integers. This representation is often denoted as $[a_0; a_1, a_2, a_3, \ldots]$.

Notice that every real number α can be expressed as a continued fraction; and α is a rational number if and only if it has a finite continued fraction representation i.e

$$\alpha = \frac{a}{b} = [a_0; a_1, a_2, \ldots, a_k]$$

Definition 2 (Compution of a_i). *Let $\lfloor \alpha \rfloor$ denote the greatest integer less than or equal to α. Let $\alpha_0 = \alpha$ and $a_0 = \lfloor \alpha_0 \rfloor$. Then the other a_i, $i \geq 1$ are computed as follows.*

$$a_{i+1} = \lfloor \alpha_{i+1} \rfloor \text{ where } \alpha_{i+1} = \frac{1}{\alpha_i - a_i}$$

Notice that this procedure terminates only if $a_i = \alpha_i$ for some $i \geq 0$.

Definition 3 (convergent,[HW79,Moo64]).
The convergents of a continued fraction $[a_0; a_1, a_2, \ldots]$ are the rational numbers obtained by truncating the continued fraction at each step. The n-th convergent is given by:

$$C_n = [a_0; a_1, a_2, \ldots, a_n] = \frac{p_n}{q_n}$$

where p_n and q_n are the numerator and denominator of the n-th convergent, respectively. These can be computed recursively using the relations:

$$p_n = a_n p_{n-1} + p_{n-2}, \quad q_n = a_n q_{n-1} + q_{n-2}$$

with initial conditions $p_{-2} = 0$, $p_{-1} = 1$, $q_{-2} = 1$, and $q_{-1} = 0$.

We denote the set of the convergents of a rational number $r := [a_0; a_1, a_2, \ldots, a_m]$ by

$$\text{Convergents}(r) := \left\{ (u, v) \in \mathbb{N}^2 : \frac{v}{u} = C_n, \gcd(u, v) = 1, n = 1, 2, \ldots, m \right\} \quad (10)$$

In the following, we recall the Legendre's theorem which provides a criterion for a rational number to be a convergent of a real number's continued fraction.

Theorem 1 (Legendre). *Let α be a real number, and let $\frac{a}{b}$ be a rational number where a and b are positive integers such that* $\gcd(a, b) = 1$. *If*

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{2b^2},$$

then $\frac{a}{b}$ is a convergent of the continued fraction expansion of α.

It is well known that if α is a rational number, then the sequence of convergents of its continued fraction expansion can be computed in polynomial time in $\log(\max(a, b))$.

2.2 Coppersmith's method

Coppersmith [Cop96] presented, in 1996, an algorithm to find small integer roots of univariate modular polynomials. His method is based on lattice reduction techniques such as the well known LLL algorithm [LLL82]. A lattice is a discrete additive subgroup of $\mathbb{R}^n$ and is generated by a basis of linearly independent vectors $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_m$, forming integer linear combinations:

$$\mathcal{L} = \left\{ \sum_{i=1}^{m} a_i \mathbf{b}_i \mid a_i \in \mathbb{Z} \right\}$$

The rank of a lattice is the number of basis vectors. If the rank is equal to the ambient space dimension n, the lattice is full-rank. The determinant (or covolume) of a lattice is $\det(\mathcal{L}) = \sqrt{\det(B^T B)}$ where B is the $n \times m$ matrix whose columns are the basis vectors. If the lattice is full-rank ($m = n$), the determinant simplifies to $\det(\mathcal{L}) = |\det(B)|$. In a lattice, short vectors refer to nonzero lattice points with relatively small Euclidean norm. Finding such vectors is crucial in many computational problems, including cryptanalysis and integer factorization. Efficient approximation of short vectors is achieved using lattice reduction techniques like LLL [LLL82] and BKZ [Sch91], which are widely used in cryptographic attacks (e.g. Coppersmith-like algorithms [Cop96]) and post-quantum cryptography.

Theorem 2 (Coppersmith [May03,HG97]). *Let $N = pq$ be an RSA modulus, where p and q have the same bit size. Suppose we are given an approximation of p with additive error at most $N^{1/4}$. Then N can be factored in time polynomial in* $\log(N)$.

For the sake of completeness, we summarize in the following, the Coppersmith's algorithm (see [May03] for more details) to find a factor p of N given N and an approximation $\widehat{p}$ of p.

Algorithm 1 Coppersmith's algorithm for finding a factor p of N

Input: $N = pq$ (unknown factorization), an approximation $\widehat{p}$ of p and a lower bound $p > N^{\beta}$.

Output: A factor p of N or $\perp$

1: Define the polynomial $f_p(x) = (x - \widehat{p})$.
2: Choose the smallest integer m such that $m \geq \max\left\{\frac{\beta^2}{\epsilon}, 7\beta\right\}$. ▷ ϵ is a positive parameter such that $|p - \widehat{p}| < N^{\frac{1}{2}-\epsilon}$
3: Compute $t = \lfloor m\left(\frac{1}{\beta} - 1\right)\rfloor$.
4: Compute the shift polynomials

$$g_i(x) = N^i f_p^{m-i}(x), \quad \text{for } i = 0, 1, \ldots, m,$$
$$h_i(x) = x^i f_p^m(x), \quad \text{for } i = 0, 1, \ldots, t-1.$$

5: Compute the bound $X = \lceil N^{\beta^2-\epsilon}\rceil$.
6: Construct the lattice basis B, where the basis vectors of B are the coefficient vectors of $g_i(xX)$ and $h_i(xX)$.
7: Apply the LLL-algorithm to B. Let v be the shortest vector in the LLL-reduced bases.
8: Construct $f(x)$ from v.
9: Find the set $\mathcal{R}$ of all roots of $f(x)$ over the integers. For every root $x_0 \in \mathcal{R}$, check whether $\gcd(N, f_p(x_0)) \geq N^{\beta}$. If this condition is not satisfied then remove x_0 from $\mathcal{R}$.
10: **If** $\widehat{p} + x_0$ divides N; $p := \widehat{p} + x_0$ **else** $p :=\perp$.
11: **Return** p

2.3 Cotan and Teşeleanu Scheme

In NordSec 2023, Cotan and Teşeleanu [CT23] introduced a new RSA-like cryptosystem using the key equation

$$ex - k(p^n - 1)(q^n - 1) = 1 \text{ for some positive integer } n$$

Notice that for $n = 1$, we have the standard RSA [RSA78] equation and for $n = 2$, the Elkamchouchi, Elshenawy and Shaban scheme proposed in 2002 [EES02].

In the Cotan and Teşeleanu public key encryption scheme, the computations are done in the set $\dfrac{\mathbb{Z}/N\mathbb{Z}[t]}{t^n - r}$ instead of $\mathbb{Z}/N\mathbb{Z}$.

Let p be a prime number, n a positive integer and $r \in \dfrac{\mathbb{Z}}{p\mathbb{Z}}$ such that $t^n - r$ is an irreducible polynomial over $\dfrac{\mathbb{Z}}{p\mathbb{Z}}[t]$. Define the set

$$\mathbb{A}_n(p) = \frac{\mathbb{Z}/p\mathbb{Z}[t]}{t^n - r}$$

Notice that $\mathbb{A}_n(p)$ is a finite field of order p^n and can be represented as follows:

$$\mathbb{A}_n(p) = \left\{ a(t) = a_0 + a_1 t + \ldots + a_{n-1} t^{n-r} : a_0, a_1, \ldots, a_{n-1} \in \frac{\mathbb{Z}}{p\mathbb{Z}} \right\}$$

Let $a(t)$ and $b(t)$ be two elements in $\mathbb{A}_n(p)$, then the quotient field induces a natural product $\circ$

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

$\mathbb{A}_n^\star(p)$ is a cyclic group of order $\phi_n(p) = p^n - 1$. Let $a(t) \in \mathbb{A}_n^\star(p)$ and e an integer, we define

$$[a(t)]^e = a(t) \circ a(t) \circ \ldots \circ a(t) \ (e \ \text{ times })$$

The key generation, encryption and decryption algorithms are given as follows.

Key Generation : Let λ be a security parameter and $n \geq 1$ an integer.

- Randomly generate two distinct large prime numbers p, q such that $p, q \geq 2^\lambda$ and compute the modulus $N = pq$.
- Choose an integer $r \in \mathbb{Z}/N\mathbb{Z}$ such that $t^n - r$ is an irreducible polynomial over $\frac{\mathbb{Z}}{p\mathbb{Z}}[t]$ and $\frac{\mathbb{Z}}{q\mathbb{Z}}[t]$. Let $\phi_n = (p^n - 1)(q^n - 1)$.
- Select a positive integer $e < \phi_n$ such that $\gcd(e, \phi_n) = 1$.
- Compute $d = e^{-1} \pmod{\phi_n}$. The public key is $pk = (N, e, n, r)$ and the secret key is $sk = (N, d, n, r)$.

Encryption process : To encrypt a message $m = (m_0, m_1, \ldots, m_{n-1}) \in (\mathbb{Z}/N\mathbb{Z})^n$ with the public key $pk = (N, e, n, r)$,

- Represent the message m as $m(t) = m_0 + m_1 t + \ldots + m_{n-1} t^{n-1} \in \mathbb{A}_n^\star(N)$.
- The ciphertext is $c(t) = [m(t)]^e \pmod{N}$.

Decryption process : To decrypt a ciphertext $c(t) \in \mathbb{A}_n^\star(N)$ with the secret key $sk = (N, d, n, r)$, Compute

$$m(t) = [c(t)]^d \pmod{N}$$

Lemma 1. *[BNST17] Let $N = pq$ be an RSA modulus with $q < p < 2q$. The following holds:*

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

Wlog, we can assume, in the rest of this paper that $p - q > N^{\frac{1}{4}}$; otherwise N can be factored in polynomial time [May03].

3 Our New Attack

In this section, we present our new attack to factor N by combining two techniques : the continued fractions and Coppersmith's algorithm. More precisely, we show how to obtain p and q by solving the general equation

$$eu - (p^4 - 1)(q^4 - 1)v = w$$

3.1 The New Attack

Lemma 2. *Let $N = pq$ be a balanced RSA modulus ($q < p < 2q$). Let u and v be two coprime positive integers. Let e a public exponent satisfying $eu - (p^4 - 1)(q^4 - 1)v = w$ such that $|w| < vN$. Given e, N, u and v, one can find p and q in polynomial time.*

Proof. Suppose that we know e, N, u and v such that $eu-(p^4-1)(q^4-1)v = w$ with $|w| < vN$. To show that one can factor N in polynomial time, we will first find an approximation $\widehat{p}$ of the prime p such that $|p-\widehat{p}| < N^{1/4}$. Afterwards, we apply the Coppersmith's algorithm as stated in Theorem 2 to find p; and finally get $q = N/p$.

First, let us find an approximation of $p + q$ and $p - q$.

i) **Approximation of** $p+q$: In the one hand, $\phi_4 = \dfrac{eu}{v} - \dfrac{w}{v}$ since $eu-\phi_4 v = w$. In the other hand, $\phi_4 = (p+q)^4-4N(p+q)^2-(N^2-1)^2$. Then $p+q$ satisfies the following equation:

$$\left((p+q)^2\right)^2 - 4N(p+q)^2 - \left((N^2-1)^2 - \frac{eu}{v} + \frac{w}{v}\right) = 0$$

By computing the discriminant, we get

$$\Delta = 16N^2 + 4\left((N^2-1)^2 - \frac{eu}{v} + \frac{w}{v}\right) \geq 0$$

This implies that

$$(p+q)^2 = \frac{4N + 2\sqrt{\left((N^2+1)^2 - \dfrac{eu}{v} + \dfrac{w}{v}\right)}}{2}$$

Thus

$$p + q = \sqrt{2N + \sqrt{(N^2+1)^2 - \frac{eu}{v} + \frac{w}{v}}}$$

We then approximate $p + q$ as follows.

$$\widehat{p+q} = \sqrt{2N + \sqrt{(N^2+1)^2 - \frac{eu}{v}}}$$

Using the fact that $\sqrt{a} - \sqrt{b} < \sqrt{a \pm b} < \sqrt{a} + \sqrt{b}$ for positive integers $a > b > 0$, then the following holds.

$$\left|(p+q) - \widehat{p+q}\right| < \sqrt{\sqrt{\frac{|w|}{v}}} = N^{1/4}$$

ii) **Approximation of** $p - q$: We have

$$\phi_4 = N^4 - (p^4 + q^4) + 1 = (N^2-1)^2 - (p-q)^4 - 4N(p-q)^2$$

Then $p - q$ satisfies the following equation.

$$\left((p-q)^2\right)^2 + 4N(p-q)^2 - \left((N^2-1)^2 - \frac{eu}{v} + \frac{w}{v}\right) = 0$$

The discriminant of the previous equation is

$$\Delta' = 16N^2 + 4\left((N^2-1)^2 - \frac{eu}{v} + \frac{w}{v}\right) \geq 0$$

Thus

$$p - q = \sqrt{-2N + \sqrt{(N^2+1)^2 - \frac{eu}{v} + \frac{w}{v}}}$$

And we approximate $p - q$ as follows.

$$\widehat{p-q} = \sqrt{-2N + \sqrt{(N^2+1)^2 - \frac{eu}{v}}}$$

Notice that $\widehat{p-q}$ is well defined since we have supposed that $p - q > N^{1/4}$.

One can check that $\left|(p-q) - \widehat{p-q}\right| < \sqrt{\sqrt{\frac{|w|}{v}}} = N^{1/4}$.

Combining the approximation of $p+q$ and $p-q$, we have

$$\begin{aligned}\left|p - \frac{1}{2}\left(\widehat{p+q} + \widehat{p-q}\right)\right| &\leq \frac{1}{2}\left|(p+q) - \widehat{p+q}\right| + \frac{1}{2}\left|(p-q) - \widehat{p-q}\right| \\ &< \frac{1}{2}N^{1/4} + \frac{1}{2}N^{1/4} = N^{1/4}\end{aligned}$$

Now applying the Coppersmith's algorithm for input N and the approximation $\widehat{p} = \frac{1}{2}\left(\widehat{p+q} + \widehat{p-q}\right)$, we get p, and then we compute $q = N/p$. □

Theorem 3. *Let $N = pq$ be an RSA modulus where p and q have the same bit size ($q < p < 2q$). Let e be a public exponent satisfying*

$$eu - (p^4-1)(q^4-1)v = w$$

with coprime positive integers u and v. If $uv < (2N^4 - 49N^2 + 2)/(4N + 170N^2)$ and $|w| < vN$, then one can find p and q in polynomial time in $\log(N)$.

Proof. Suppose that $N = pq$ and $q < p < 2q$ and the public exponent e satisfies the general equation $eu - (p^4-1)(q^4-1)v = w$ with $u, v > 0$ and $\gcd(u, v) = 1$.

$$\begin{aligned}\phi_4 &= (p^4-1)(q^4-1)\\ &= N^4 - (p^4+q^4) + 1\\ &= N^4 - (p+q)^4 + 4N(p+q)^2 - 2N^2 + 1\\ &= N^4 - 2N^2 + 1 - (p+q)^4 + 4N(p+q)^2\end{aligned}$$

This implies that

$$\begin{aligned}eu - \phi_4 v = w &\iff eu - \left[N^4 - 2N^2 + 1 - (p+q)^4 + 4N(p+q)^2\right] v = w\\ &\iff eu - \left(N^4 - \frac{49}{2}N^2 + 1\right) v - \left[-(p+q)^4 + 4N(p+q)^2 + \frac{45}{2}N^2\right] v = w\\ &\iff eu - \left(N^4 - \frac{49}{2}N^2 + 1\right) v = w + \left[-(p+q)^4 + 4N(p+q)^2 + \frac{45}{2}N^2\right] v.\end{aligned}$$

Then we divide both side by $(N^4 - \frac{49}{2}N^2 + 1)u$ and we obtain

$$\frac{2e}{2N^4 - 49N^2 + 2} - \frac{v}{u} = \frac{w + \left[-(p+q)^4 + 4N(p+q)^2 + \frac{45}{2}N^2\right] v}{(N^4 - \frac{49}{2}N^2 + 1)u}$$

The absolute value of the left hand side is bounded as follows

$$\begin{aligned}\left|\frac{2e}{2N^4 - 49N^2 + 2} - \frac{v}{u}\right| &\leq \frac{|w| + \left|-(p+q)^4 + 4N(p+q)^2 + \frac{45}{2}N^2\right| v}{(N^4 - \frac{49}{2}N^2 + 1)u}\\ &< \frac{2N + 2\left|-(p+q)^4 + 4N(p+q)^2 + \frac{45}{2}N^2\right|}{2N^4 - 49N^2 + 2} \times \left(\frac{v}{u}\right)\\ &= \frac{2N + 2\,|A|}{2N^4 - 49N^2 + 2} \times \left(\frac{v}{u}\right)\end{aligned}$$

with $A = -(p+q)^4 + 4N(p+q)^2 + \frac{45}{2}N^2$. Let us now find an upper bound of $|A|$. By Lemma 1, we have $2\sqrt{N} < p + q < 3\sqrt{N}$. This implies that $4N < (p+q)^2 < 9N$ and $16N^2 < (p+q)^4 < 81N^2$. Then we have the following bound

$$16N^2 - 36N^2 - \frac{45}{2}N^2 < (p+q)^4 - 4N(p+q)^2 - \frac{45}{2}N^2 < 81N^2 - 16N^2 - \frac{45}{2}N^2$$

Therefore $|A| = |(p+q)^4 - 4N(p+q)^2 - \frac{45}{2}N^2| < \frac{85}{2}N^2$.

Then we get

$$\left|\frac{2e}{2N^4 - 49N^2 + 2} - \frac{v}{u}\right| < \frac{2N + 85N^2}{2N^4 - 49N^2 + 2} \times \left(\frac{v}{u}\right)$$

Since $uv < \dfrac{2N^4 - 49N^2 + 2}{4N + 170N^2}$ then $\dfrac{2N + 85N^2}{2N^4 - 49N^2 + 2} < \dfrac{1}{2uv}$.

Thus

$$\left| \frac{2e}{2N^4 - 49N^2 + 2} - \frac{v}{u} \right| < \frac{1}{2uv} \times \left(\frac{v}{u} \right) = \frac{1}{2u^2}$$

Hence, by Lemma 2, the fraction $\dfrac{v}{u}$ appears among the convergents of the continued fraction expansion of $\dfrac{2e}{2N^4 - 49N^2 + 2}$ which can be computed in polynomial time in $\log(N)$. Thus once we obtain u and v, one can compute p and q in polynomial time by Lemma 2.

□

Corollary 1. *Let $N = pq$ be an RSA modulus with $q < p < 2q$. Let $e < (p^4 - 1)(q^4 - 1)$ be a public exponent. If the private exponent d satisfies the following bound*

$$d < \sqrt{(2N^4 - 49N^2 + 2)/(4N + 170N^2)}$$

then one can find p and q in polynomial time in $\log(N)$.

Proof. Suppose that $q < p < 2q$ and $e < (p^4 - 1)(q^4 - 1)$. Suppose that the private exponent $d < \sqrt{(2N^4 - 49N^2 + 2)/(4N + 170N^2)}$. We know that the private exponent d satisfies the equation

$$ed - (p^4 - 1)(q^4 - 1)k = 1$$

for some positive integer k. Then to show that one can factor N in polynomial time in $\log(N)$, it is enough to show that $kd < (2N^4 - 49N^2 + 2)/(4N + 170N^2)$ by Theorem 3. We have

$$k = \frac{ed - 1}{(p^4 - 1)(q^4 - 1)} < \left(\frac{e}{(p^4 - 1)(q^4 - 1)} \right) d < d$$

Therefore $kd < d^2 < (2N^4 - 49N^2 + 2)/(4N + 170N^2)$. This ends the proof.

□

We summarize in the following algorithm our attack to factor N.

Algorithm 2 Our Attack to factor a modulus N

Input: The modulus N and the public exponent e.
Output: The factors (p, q) of N or $\perp$.

1: $r := (2e)/(2N^4 - 49N + 2)$.
2: convs := Convergents(r) ▷ Defined in Eq. 10
3: **For** (u, v) in convs **do**
4: $\quad \widehat{p+q} := \left\lfloor \sqrt{\left| 2N + \sqrt{\left| (N^2+1)^2 - \frac{eu}{v} \right|} \right|} \right\rfloor$.
5: $\quad \widehat{p-q} := \left\lfloor \sqrt{\left| -2N + \sqrt{\left| (N^2+1)^2 - \frac{eu}{v} \right|} \right|} \right\rfloor$.
6: $\quad \widehat{p} := \left\lfloor \frac{1}{2} \left(\widehat{p+q} + \widehat{p-q} \right) \right\rfloor$.
7: $\quad p := \text{Coppersmith}(\text{N}, \widehat{\text{p}})$ ▷ See Algo. 2.2
8: $\quad$ **If** $p \neq \perp$ **then**
9: $\quad\quad q := N/p$.
10: $\quad\quad$ Return (p, q) and stop the loop.
11: $\quad$ **end If**
12: **end For**
13: Return $\perp$.

3.2 A Numerical Example

In this section, we give a detailed numerical example to explain the different steps of our attack as presented in Algorithm 3.1. Let us consider the following public parameters where N is a 192 bit integer:

$$N = 348965558859919659799872778156428368196003826103849376373 1$$

$$e = 121264571400523650213000320784539221955091428942157954287 6\backslash$$
$$2747588869937066452764958707247235073835137336084401036312 3\backslash$$
$$2696543804656879163494807215473923870631948211710169000322 4\backslash$$
$$8592826620643450055808148570038313973227958484483674761$$

We get

$$2N^4 - 49N^2 + 2 = 296592565925128224985260928573727752634933194356 31\backslash$$
$$228113422881048895189176448539116661868758369415 74\backslash$$
$$772595490809626658037224782060803377911228330289331\backslash$$
$$027312229395683785037068498150661534674700219693407\backslash$$
$$915803297056579985444010429 55$$

The continued fraction expansion of $\dfrac{2e}{2N^4 - 49N^2 + 2}$ is given as follows.

$$\frac{2e}{2N^4 - 49N^2 + 2} = [0; 1, 4, 2, 17, 2, 1, 2, 4, 1, 2, 1, 2, 1, 1, 3, 2, 11, 3, 2, 13, 10, \backslash$$
$$1, 1, 1, 1, 9, 6, 3, 1, 2, 2, 15, 4, 2, 2, 29, 20, 1, 1, 2, 13, 3, 14, \backslash$$
$$1, 2, 2, 1, 1, 7, 1, 4, 1, 2, 44, 3, 1, 8, 5, 1, 232, 1, 3, 1, 6, 2, 1, 5, \ldots]$$

For the 101^{st} convergent C_{101} (note that $C_1 = 1$, $C_2 = \frac{4}{5}$, and $C_3 = \frac{9}{11}$) of the continued fraction expansion of $\dfrac{2e}{2N^4 - 49N^2 + 2}$, we obtain

$$u = 109164662112272346444555233788248142952377469519040396359$$
$$v = 892659323529332038082395493395165371330497220591579657 12$$

One can check that $uv < (2N^4 - 49N^2 + 2)/(4N + 170N^2) \approx 1.43 \times 10^{113}$. We obtain the approximation of $p + q$ and $p - q$ (see Alg. 3.1) as follows.

$$\widehat{p+q} = 158666848432062407414462565131$$
$$\widehat{p-q} = 105908198157490520315381810349$$

From the approximation of $p + q$ and $p - q$, we compute the approximation of p and obtain

$$\widehat{p} = \left\lfloor \frac{\widehat{p+q} + \widehat{p-q}}{2} \right\rfloor = 132287523294776463864922187740$$

By applying Coppersmith's algorithm, we find

$$p = 1322875232947764638649221877 41$$

which is a divisor of N. Finally, we compute the other factor as $q = N/p = 263793251372859435495403773 91$.

One can verify that:

$$w = eu - (p^4 - 1)(q^4 - 1)v = -1.$$

The private exponent is

$$d = 148296282962564112492630464286863876317466597178156140567 1144\backslash$$
$$0524447594588224269558330934379184707873862977454048132452157\backslash$$
$$4290751123131376788278676855736667385482052185665565195204905\backslash$$
$$5799517494405727330239363916651940505959660932 41$$

which is large but

$$\phi_4 - d = 109164662112272346444555233788248142952377469519040396359$$

Notice that the parameter k such that $ed - k(p^4 - 1)(q^4 - 1) = 1$ is also too large.

$$k = 148296282962564112492630464286863876317466597178156140567 11\backslash$$
$$4405244475945882242695583309343791847078738629774540481324 5\backslash$$
$$2157429075112313137678827867685573666738548205218566556519 5\backslash$$
$$2049055799517494405727330239363916651940505959660932 41$$

4 A Generalized Wiener Attack for RSA-like Cryptosystems

In the following Theorem, we prove that if the private exponent of an RSA-like cryptosystem is too large, then one can factor N in polynomial time given the public parameters (N, e).

Theorem 4. *Let $N = pq$ an RSA modulus. Let $\psi : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$. Suppose $\mathcal{A}$ is an algorithm that is able to factor N in polynomial time given N and a public exponent $0 < e < \psi(p,q)$ such that there exist positive integers x and y with $xy < \mathcal{B}_1 \in \mathbb{R}^+$ satisfying*

$$ex - y\psi(p,q) = z \text{ with } |z| < \mathcal{B}_2,\ \mathcal{B}_2 \geq 1$$

Then, using $\mathcal{A}$, one can factor N in polynomial time given N and a public exponent $0 < e' < \psi(p,q)$ such that the corresponding private exponent $d' = \psi(p,q) - d$ for some $d < \sqrt{\mathcal{B}_1}$.

Proof. Suppose $\mathcal{A}$ is able to factor N in polynomial time given N and a public exponent $0 < e < \psi(p,q)$ such that there exist positive integers x and y with $xy < \mathcal{B}_1$, $ex - y\psi(p,q) = z$ with $|z| < \mathcal{B}_2$, $\mathcal{B}_2 \geq 1$. Let e', $0 < e' < \psi(p,q)$ a public exponent such that $(e')^{-1} \mod \psi(p,q) = d' = \psi(p,q) - d$ for some $d < \sqrt{\mathcal{B}_1}$. To show that one can factor N in polynomial time, we will show that there exist positive integers x_0 and y_0 such that $e'x_0 - y_0\psi(p,q) = -1$ with $x_0y_0 < \mathcal{B}_1$ and afterwards use the algorithm $\mathcal{A}$ to factor N. We have $(e')^{-1} \mod \psi(p,q) = \psi(p,q) - d$, then there exists a positive integer k such that

$$\begin{aligned} e'(\psi(p,q) - d) - k\psi(p,q) = 1 &\iff e'(-d) + (\psi(p,q) - k)\psi(p,q) = 1 \\ &\iff e'd - (\psi(p,q) - k)\psi(p,q) = -1 \end{aligned}$$

We have $\psi(p,q) - k = \dfrac{e'd + 1}{\psi(p,q)} > 0$. This implies that

$$(\psi(p,q) - k) - \frac{1}{\psi(p,q)} = \frac{e'd}{\psi(p,q)} < d \text{ since } 0 < e' < \psi(p,q)$$

Therefore $\psi(p,q) - k < d + \dfrac{1}{\psi(p,q)}$. Since $\psi(p,q) - k \in \mathbb{N}$, then $\psi(p,q) - k \leq d \Rightarrow d(\psi(p,q) - k) < d^2 < \mathcal{B}_1$. We have showed that $e'd - (\psi(p,q) - k)\psi(p,q) = -1$ with $d(\psi(p,q) - k) < \mathcal{B}_1$, then using algorithm $\mathcal{A}$, one can factor N in polynomial time. □

Notice that if the private exponent d' is big then so is the positive integer k such that

$$e'd' - k\psi(p,q) = 1$$

since $\psi(p,q) - k \leq d$.

Corollary 2. *Let $N = pq$ be an RSA modulus with $q < p < 2q$. Let $e < (p^4 - 1)(q^4 - 1)$ be a public exponent. If the private exponent d satisfies the following bound*

$$d > (p^4 - 1)(q^4 - 1) - \sqrt{\frac{2N^4 - 49N^2 + 2}{4N + 170N^2}}$$

then one can find p and q in polynomial time in $\log(N)$.

Proof. It follows from Theorem 3 and Theorem 4. □

This corollary tell us if the private exponent d is too large, i.e

$$|\phi_4 - d| < \sqrt{\frac{2N^4 - 49N^2 + 2}{4N + 170N^2}}$$

then we can factor the modulus N in polynomial time. To our knowledge, this result is completely new. Generally, Wiener-like attacks a dealing with small private exponent i.e $d < N^\delta$ for some positive reel number δ.

Using the result of Bunder et al. [BNST17] (Theorem 3) and Theorem 4, we get the following result.

Corollary 3. *Let $N = pq$ be an RSA modulus with $q < p < 2q$. Let $e < (p^2 - 1)(q^2 - 1)$ be a public exponent. If the private exponent d satisfies the following bound*

$$d > (p^2 - 1)(q^2 - 1) - \sqrt{2N - 4\sqrt{2}N^{\frac{3}{4}}}$$

then one can find p and q in polynomial time in $\log(N)$.

The following Theorem is a variant of Theorem 4.

Theorem 5. *Let $N = pq$ an RSA modulus. Let $\psi : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$. Suppose $\mathcal{A}$ is an algorithm that is able to factor N in polynomial time given N and a public exponent $0 < e < \psi(p, q)$ such that there exist positive integers x and y with $x < \mathcal{B}_1 \in \mathbb{R}^+$ satisfying*

$$ex - y\psi(p, q) = z \text{ with } |z| < \mathcal{B}_2,\ \mathcal{B}_2 \geq 1$$

Then, using $\mathcal{A}$, one can factor N in polynomial time given N and a public exponent $0 < e' < \psi(p, q)$ such that the corresponding private exponent $d' = \psi(p, q) - d$ for some $d < \mathcal{B}_1$.

Proof. Similarly to the proof of Theorem 4, we have

$$e'(\psi(p, q) - d) - k\psi(p, q) = 1 \iff e'd - (\psi(p, q) - k)\psi(p, q) = -1$$

This shows that if $d < \mathcal{B}_1$, one can factor N in polynomial time using the algorithm $\mathcal{A}$. □

Combining the result of Blömer and May [BM04] (Theorem 2) and previous theorem, we get the following result.

Corollary 4. *Let $c \leq 1$ and let (N, e) be an RSA public key tuple with $N = pq$ and $p - q \geq c\sqrt{N}$. If the private exponent d verify*

$$d > (p-1)(q-1) - \frac{1}{3}N^{\frac{1}{4}}$$

Then N can be factored in polynomial time.

We summarize in the following figure, the vulnerable areas for the private exponent d.

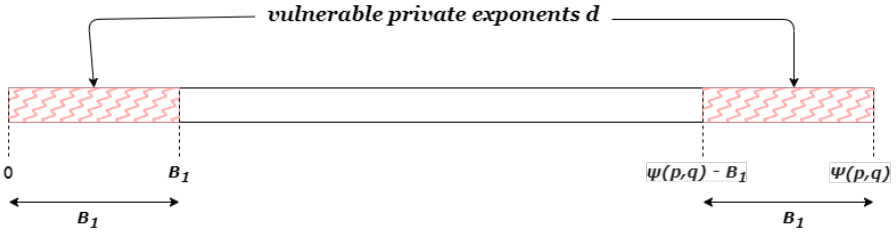

Fig. 1. Vulnerable areas for the private exponent d

Notice that in our generalized attack,

$$\psi(p,q) = (p^4-1)(q^4-1) \text{ and } \mathcal{B}_1 \geq \sqrt{\frac{2N^4 - 49N^2 + 2}{4N + 170N^2}}$$

From Theorem 4, we build an algorithm that takes as input a security parameter λ and outputs a weak RSA public key (N, e).

Algorithm 3 GenWeakRSAInstance : An algorithm which generates weak RSA public key instances.

Input: A security parameter λ.
Output: a weak RSA public key (N, e).

1: Generate randomly a prime p of size $\lambda/2$ bits.
2: Generate randomly a prime q of size $\lambda/2$ bits with $q < p < 2q$.
3: Compute $N = pq$ and $\psi(p,q) = (p^4-1)(q^4-1)$.
4: Generate randomly an integer d with $0 < d < \sqrt{\frac{2N^4 - 49N^2 + 2}{4N + 170N^2}}$ such that

$$\gcd(\psi(p,q) - d, \psi(p,q)) = 1$$

5: Compute $e = (\psi(p,q) - d)^{-1} \pmod{\psi(p,q)}$.
6: Return (N, e).

Notice that this algorithm runs in polynomial time and can be easily adapted for other RSA-like cryptosystems. The weak instances (N, e) outputted by the previous Algorithm 4 are

- vulnerable for the generalized Wiener attack presented in Algorithm 3.1;
- safe for classical Wiener-like attacks because the corresponding private exponents d' are very large.

We have provided a proof-of-concept implementation [4] in SageMath [Dev24] of our attack presented in Algorithm 3.1 as well as an implementation of the previous Algorithm 4 that generates weak instances in polynomial time.

5 Conclusion

In this paper, we have investigated a special case of the general equation $w = eu - (p^n - 1)(q^n - 1)v = w$. We have showed that for $n = 4$, by combining the continued fractions techniques and the Coppersmith's method, one can find (u, v) and factor the modulus N in polynomial time when $uv < (2N^4 - 49N^2 + 2)/(4N + 170N^2)$ and $|w| < vN$. We have also demonstrated that a private exponent which is small or very large can be recovered in polynomial time.

References

BD99. Dan Boneh and Glenn Durfee. Cryptanalysis of rsa with private key d less than n 0.292. In *Advances in Cryptology—EUROCRYPT'99: International Conference on the Theory and Application of Cryptographic Techniques Prague, Czech Republic, May 2–6, 1999 Proceedings 18*, pages 1–11. Springer, 1999. 1

BM04. Johannes Blömer and Alexander May. A generalized wiener attack on rsa. In *International Workshop on Public Key Cryptography*, pages 1–13. Springer, 2004. 1.1, 4

BNST17. Martin Bunder, Abderrahmane Nitaj, Willy Susilo, and Joseph Tonien. A generalized attack on rsa type cryptosystems. *Theoretical Computer Science*, 704:74–81, 2017. 1.1, 1, 4

Bon99. Dan Boneh. Twenty years of attacks on the rsa cryptosystem. *Notices of the AMS*, 46(2):203–213, 1999. 1.2

Cop96. Don Coppersmith. Finding a small root of a univariate modular equation. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 155–165. Springer, 1996. 2.2

CT23. Paul Cotan and George Teşeleanu. Small private key attack against a family of rsa-like cryptosystems. In *Nordic Conference on Secure IT Systems*, pages 57–72. Springer, 2023. 1, 1.2, 2, 2.3

Dev24. The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 10.4)*. SageMath, https://www.sagemath.org, 2024. 1.2, 4

[4] https://github.com/mseckept/generalized-wiener-attack

EES02. H Elkamchouchi, K Elshenawy, and H Shaban. Extended rsa cryptosystem and digital signature schemes in the domain of gaussian integers. In *The 8th International Conference on Communication Systems, 2002. ICCS 2002.*, volume 1, pages 91–95. IEEE, 2002. 1.1, 2.3

Hås86. Johan Håstad. On using rsa with low exponent in a public key network. In *Advances in Cryptology – CRYPTO '85*, volume 218 of *Lecture Notes in Computer Science*, pages 403–408. Springer, 1986. 1

HG97. Nicholas Howgrave-Graham. Finding small roots of univariate modular equations revisited. In *IMA International Conference on Cryptography and Coding*, pages 131–142. Springer, 1997. 1, 2

HW79. GH Hardy and Edward Maitland Wright. An introduction to the theory of numbers. oxford university press. 1979. 1, 3

KMOV92. K. Koyama, U. Maurer, T. Okamoto, and S. A. Vanstone. New public-key schemes based on elliptic curves over the ring $\mathbb{Z}_n$. In *Advances in Cryptology – CRYPTO '91*, volume 576 of *Lecture Notes in Computer Science*, pages 252–266. Springer, 1992. 1.1

LLL82. Arjen K Lenstra, Hendrik Willem Lenstra, and László Lovász. Factoring polynomials with rational coefficients. *Mathematische annalen*, 261:515–534, 1982. 1, 2.2

May03. Alexander May. *New RSA vulnerabilities using lattice reduction methods. Ph.D. Thesis, University of Paderborn, Paderborn, Germany.* PhD thesis, Citeseer, 2003. 1, 1.2, 2, 2.2, 2.3

Moo64. Charles G. Moore. *An Introduction to Continued Fractions.* National Council of Teachers of Mathematics, Washington, D.C., 1964. 1, 1, 3

MP19. Majid Mumtaz and Luo Ping. Forty years of attacks on the rsa cryptosystem: A brief survey. *Journal of Discrete Mathematical Sciences and Cryptography*, 22(1):9–29, 2019. 1.2

Nit08. Abderrahmane Nitaj. Another generalization of wiener's attack on rsa. In *International Conference on Cryptology in Africa*, pages 174–190. Springer, 2008. 1.1

Nit14. Abderrahmane Nitaj. A new attack on the KMOV cryptosystem. *Bulletin of the Korean Mathematical Society*, 51(5):1347–1356, 2014. 1.1

RSA78. R Rivest, A Shamir, and L Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 1978. 1, 2.3

Sch91. Claus-Peter Schnorr. A hierarchy of polynomial time lattice basis reduction algorithms. In *Proceedings of the 30th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 179–185. IEEE Computer Society, 1991. 2.2

Wie90. Michael J Wiener. Cryptanalysis of short rsa secret exponents. *IEEE Transactions on Information theory*, 36(3):553–558, 1990. 1