Continued Fractions Applied to a Family of RSA-like Cryptosystems

Paul Cotan[1,2] (iD) and George Teşeleanu[1,2](iD)

[1] Advanced Technologies Institute
10 Dinu Vintilă, Bucharest, Romania
{paul.cotan,tgeorge}@dcti.ro
[2] Simion Stoilow Institute of Mathematics of the Romanian Academy
21 Calea Grivitei, Bucharest, Romania

Abstract. Let $N = pq$ be the product of two balanced prime numbers p and q. Murru and Saettone presented in 2017 an interesting RSA-like cryptosystem that uses the key equation $ed - k(p^2+p+1)(q^2+q+1) = 1$, instead of the classical RSA key equation $ed - k(p-1)(q-1) = 1$. The authors claimed that their scheme is immune to Wiener's continued fraction attack. Unfortunately, Nitaj *et. al.* developed exactly such an attack. In this paper, we introduce a family of RSA-like encryption schemes that uses the key equation $ed - k[(p^n - 1)(q^n - 1)]/[(p-1)(q-1)] = 1$, where $n > 1$ is an integer. Then, we show that regardless of the choice of n, there exists an attack based on continued fractions that recovers the secret exponent.

1 Introduction

In 1978, Rivest, Shamir and Adleman [24] proposed one of the most popular and widely used cryptosystem, namely RSA. In the standard RSA encryption scheme, we work modulo an integer N, where N is the product of two large prime numbers p and q. Let $\varphi(N) = (p-1)(q-1)$ denote the Euler totient function. In order to encrypt a message $m < N$, we simply compute $c \equiv m^e \bmod N$, where e is generated a priori such that $\gcd(e, \varphi(N)) = 1$. To decrypt, one needs to compute $m \equiv c^d \bmod N$, where $d \equiv e^{-1} \bmod \varphi(N)$. Note that (N, e) are public, while (p, q, d) are kept secret. In the standard version of RSA, also called balanced RSA, p and q are of the same bit-size such that $q < p < 2q$. In this paper, we only consider the balanced RSA scheme and its variants.

In 2017, Murru and Saettone introduced an RSA-like cryptosystem [18]. Instead of using $\mathbb{Z}_N^*$, the scheme works with a special type of group that consists of equivalence classes of polynomials from the $GF(p^3) \times GF(q^3)$, where GF stands for Galois field. Furthermore, when developing their cryptosystem, the authors use the same modulus as the RSA scheme, but they choose e such that $\gcd(e, \psi(N)) = 1$, where $\psi(N) = (p^2 + p + 1)(q^2 + q + 1)$. Also, the decryption exponent is $d \equiv e^{-1} \bmod \psi(N)$. In [18], the authors claim that their scheme is more secure than RSA. More precisely, they say that their scheme is secure against Wiener's small private key attack [30] and Hastad's broadcast attack [12]. Unfortunately, this is not true as can be seen in the following paragraphs.

Small Private Key Attacks. In order to decrease decryption time, one may prefer to use a smaller d. Wiener showed in [30] that this is not always a good idea. More exactly, in the case of RSA, if $d < N^{0.25}/3$, then one can retrieve d from the continued fraction expansion of e/N, and thus factor N. Using a result developed by Coppersmith [7], Boneh and Durfee [5] improved Wiener's bound to $N^{0.292}$. Later on, Herrmann and May [13] obtain the same bound, but using simpler techniques. A different approach was taken by Blömer and May [3], whom generalized Wiener's attack. More precisely, they showed that if there exist three integers x, y, z such that $ex - y\varphi(N) = z$, $x < N^{0.25}/3$ and $|z| < |exN^{-0.75}|$, then the factorisation of N can be recovered. When an approximation of p is known such that $|p - p_0| < N^\delta/8$ and $\delta < 0.5$, Nassr, Anwar and Bahig [20] present a method based on continued fractions for recovering d when $d < N^{(1-\delta)/2}$.

In the case of the Murru-Saetonne scheme, it was shown in [22, 27] that a Wiener-type attack still works. Using a technique based on continued fractions they showed that when $d < N^{0.25}$ we can factor N. Applying the method proposed by Boneh-Durfee, Nitaj *et al.* [22] improved the bound to $N^{0.5694}$. A better bound $d < N^{0.585}$ was found by Zheng, Kunihiro and Yao in [31]. When p_0 is known such that $|p - p_0| < N^\delta$ and $\delta < 0.5$, Nassr, Anwar and Bahig [19] show how to recover d when $d < N^{(1-\delta)/2}$.

Multiple Private Keys Attack. Let $\ell > 0$ be an integer and $i \in [1, \ell]$. When multiple large public keys $e_i \simeq N^\alpha$ are used with the same modulus N, Howgrave-Graham and Seifert [14] describe an attack for RSA that recovers the corresponding small private exponents $d_i \simeq N^\beta$. This attack was later improved by Sarkar and Maitra [25], Aono [1] and Takayasu and Kunihiro [28]. The best known bound [28] is $\beta < 1 - \sqrt{2/(3\ell + 1)}$. Remark that when $\ell = 1$ we obtain the Boneh-Durfee bound.

The multiple private keys attack against the Murru-Saetonne cryptosystem was studied by Shi, Wang and Gu [26]. The bound obtained by the authors is $\beta < 3/2 - 4/(3\ell + 1)$ and it is twice the bound obtained by Aono [1]. Note that when $\ell = 1$ the bound is less than 0.585, and thus tighter bounds might exist.

Partial Key Exposure Attack. In this type of attack, the most or least significant bits of the private exponent d are known. Starting from these, an adversary can recover the entire RSA private key using the techniques presented by Boneh, Durfee and Frankel in [6]. The attack was later improved by Blömer and May [2], Ernst *et al.* [9] and Takayasu and Kunihiro [29]. The best known bound [29] is $\beta < (\gamma + 2 - \sqrt{2 - 3\gamma^2})/2$, where the attacker knows N^γ leaked bits.

Shi, Wang and Gu [26] describe a partial exposure attack that works in the case of the Murru-Saetonne scheme. The bound they achieve is $\beta < (3\gamma + 7 - 2\sqrt{3\gamma + 7})/3$. When $\gamma = 0$, the bound is close to 0.569, and thus it remains an open problem how to optimize it.

Small Prime Difference Attack. When the primes difference $|p - q|$ is small and certain conditions hold, de Weger [8] described two methods to recover d, one based on continued fractions and one on lattice reduction. These methods were

further extended by Maitra and Sakar [16, 17] to $|\rho q - p|$, where $1 \leq \rho \leq 2$. Lastly, Chen, Hsueh and Lin generalize them further to $|\rho q - \epsilon p|$, where ρ and ϵ have certain properties. The continued fraction method is additionally improved by Ariffin *et al.* [15].

The de Weger attack was adapted to the Murru-Saetonne public key encryption scheme by Nitaj *et al.* [23], Nassr, Anwar and Bahig [19] and Shi, Wang and Gu [26]. The best bounds for the continued fraction and lattice reduction methods are found in [23]. The Maitra-Sakar extension was studied only in [19].

1.1 Our Contributions

In this paper we generalize the Murru-Saetonne scheme to equivalence classes of polynomials from $GF(p^n) \times GF(q^n)$, where $n > 1$. We wanted to see if only for $n = 3$ the attacks devised for RSA work or this is something that happens in general. In this study we present a Wiener-type attack that works for any $n > 1$. More precisely, we prove that when $d < N^{0.25}$ we can recover the secret exponent regardless the value of n. Therefore, no matter how we instantiate the generalized version, a small private key attack will always succeed.

Structure of the Paper. We introduce in Section 2 notations and definitions used throughout the paper. Inspired by Murru and Saettone's work [18], in Section 3 we introduce a family of groups that is latter used in Section 4 to construct RSA-like cryptosystems. After proving several useful lemmas in Section 5, we extend Wiener's small private key attack in Section 6. Two concrete instantiations are provided in Section 7. We conclude our paper in Section 8.

2 Preliminaries

Notations. Throughout the paper, λ denotes a security parameter. Also, the notation $|S|$ denotes the cardinality of a set S. The set of integers $\{0, \ldots, a\}$ is further denoted by $[0, a]$.

2.1 Continued fraction

For any real number ζ there exist an unique sequence $(a_n)_n$ of integers such that

$$\zeta = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \cdots}}}},$$

where $a_k > 0$ for any $k \geq 1$. This sequence represents the continued fraction expansion of ζ and is denoted by $\zeta = [a_0, a_1, a_2, \ldots]$. Remark that ζ is a rational number if and only if its corresponding representation as a continued fraction is finite.

For any real number $\zeta = [a_0, a_1, a_2, \ldots]$, the sequence of rational numbers $(A_n)_n$, obtained by truncating this continued fraction, $A_k = [a_0, a_1, a_2, \ldots, a_k]$, is called the convergents sequence of ζ.

According to [11], the following bound allows us to check if a rational number u/v is a convergent of ζ.

Theorem 1. *Let $\zeta = [a_0, a_1, a_2, \ldots]$ be a positive real number. If u, v are positive integers such that $\gcd(u, v) = 1$ and*

$$\left| \zeta - \frac{u}{v} \right| < \frac{1}{2v^2},$$

then u/v is a convergent of $[a_0, a_1, a_2, \ldots]$.

3   Useful Quotient Groups

In this section we will provide the mathematical theory needed to generalize the Murru and Saettone encryption scheme. 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

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

In order to describe our family of RSA-like cryptosystems, we need to introduce another 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 $[a_0 + \ldots + a_{n-1} t^{n-1}] \in \mathbb{B}_n$.

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

Proof. 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

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

For any $k \in [0, n-1]$, we define the following sets

$$B_k = \{a_0 + \ldots + a_{k-1}t^{k-1} + t^k \mid a_0, a_1, \ldots, a_{k-1} \in \mathbb{F}\}.$$

Remark that $B_i \cap B_j = \emptyset$ for $i \neq j$. From the previous analysis of the equivalence classes of $\mathbb{A}_n^*$, we can deduce that $\mathbb{B}_n = \cup_{k=0}^{n-1} B_k$. Therefore, we obtain

$$|\mathbb{B}_n| = \sum_{k=0}^{n-1} |B_i| = 1 + |\mathbb{F}| + \ldots + |\mathbb{F}|^{n-1} = \frac{|\mathbb{F}|^n - 1}{|\mathbb{F}| - 1},$$

as desired. $\square$

From the proof of the previous lemma we can deduce 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 $c(t)$.

4 The Scheme

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

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

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. Therefore, we can build an encryption scheme that is similar to RSA using the $\odot$ as the product.

$Setup(\lambda)$: 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 $\mathbb{Z}_p[t]$, $\mathbb{Z}_q[t]$ and $\mathbb{Z}_N[t]$. 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 1. When $n = 3$, we obtain the Murru and Saettone cryptosystem [18].

5 Useful Lemmas

In this section we provide a few useful properties of $\psi_n(N)$. Before starting our analysis, we first note that plugging $q = N/p$ in $\psi_n(N)$ leads to the following function

$$f_n(p) = \frac{p^n - 1}{p - 1} \cdot \frac{\left(\frac{N}{p}\right)^n - 1}{\frac{N}{p} - 1},$$

with p as a variable. The next lemma tells us that, under certain conditions, f_n is a strictly increasing function.

Proposition 1. *Let N a positive integer. Then for any integers $n > 1$ and $\sqrt{N} \leq x < N$, we have that the function*

$$f_n(x) = \frac{x^n - 1}{x - 1} \cdot \frac{\left(\frac{N}{x}\right)^n - 1}{\frac{N}{x} - 1},$$

is strictly increasing with x.

Proof. Before starting our proof, we notice that the function f_n can be expanded into $f_n(x) = g_n(x) \cdot h_n(x)$, where

$$g_n(x) = 1 + x + x^2 + \ldots + x^{n-1}$$

and

$$h_n(x) = 1 + \frac{N}{x} + \left(\frac{N}{x}\right)^2 + \ldots + \left(\frac{N}{x}\right)^{n-1}.$$

We will further prove our statement using induction with respect to n. When $n = 2$, we have that

$$f_2(x) = (1 + x)\left(1 + \frac{N}{x}\right) = 1 + \frac{N}{x} + x + N.$$

Using $x \geq \sqrt{N}$ we obtain that

$$f_2'(x) = 1 - \frac{N}{x^2} \geq 0 \Leftrightarrow 1 \geq \frac{N}{x^2} \Leftrightarrow x^2 \geq N,$$

and therefore we have that f_2 is strictly increasing.

For the induction step we assume that f_k is strictly increasing and we will show that f_{k+1} is also strictly increasing. Hence, we have that

$$f_{k+1}(x) = g_{k+1}(x) \cdot h_{k+1}(x)$$

$$= g_k(x) \cdot h_k(x) + g_k(x) \cdot \left(\frac{N}{x}\right)^k + x^k \cdot h_k(x) + N^k.$$

Considering the induction hypothesis, it is enough to prove that the function

$$s_k(x) = g_k(x) \cdot \left(\frac{N}{x}\right)^k + x^k \cdot h_k(x)$$

is strictly increasing. Therefore, we have that

$$s_k(x) = \left(N^k \cdot \frac{1}{x^k} + x^k\right) + \left(N^k \cdot \frac{1}{x^{k-1}} + N \cdot x^{k-1}\right)$$

$$+ \left(N^k \cdot \frac{1}{x^{k-2}} + N^2 \cdot x^{k-2}\right) + \ldots + \left(N^k \cdot \frac{1}{x} + N^{k-1} \cdot x\right)$$

$$= s_{k,0}(x) + s_{k,1}(x) + s_{k,2}(x) + \ldots + s_{k,k-1}(x),$$

where we considered

$$s_{k,i}(x) = N^k \cdot \frac{1}{x^{k-i}} + N^i \cdot x^{k-i}.$$

Bear in mind that

$$s_{k,i}'(x) = N^k \cdot \frac{-(k-i)}{x^{k-i+1}} + N^i \cdot (k-i) \cdot x^{k-i-1}$$

$$= N^i(k-i)\left(x^{k-i-1} - N^{k-i} \cdot \frac{1}{x^{k-i+1}}\right).$$

For any $i \in [0, k-1]$ we have that $s_{k,i}$ is strictly increasing since

$$s_{k,i}'(x) \geq 0 \Leftrightarrow x^{k-i-1} \geq N^{k-i} \cdot \frac{1}{x^{k-i+1}} \Leftrightarrow x^{2(k-i)} \geq N^{k-i},$$

where for the last inequality we used $x \geq \sqrt{N}$. Therefore, s_k is strictly increasing, which implies that f_{k+1} is strictly increasing.

$\square$

Using the following lemma from [21], we will compute a lower and upper bound for $\psi_n(N)$.

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

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

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

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

Proof. By Lemma 2 we have that

$$\sqrt{N} < p < \sqrt{2}\sqrt{N},$$

which, according to Proposition 1, leads to

$$f_n(\sqrt{N}) < f_n(p) < f_n(\sqrt{2}\sqrt{N}).$$

This is equivalent to

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

as desired.

$\square$

When $n = 3$, the following result proven in [22] becomes a special case of Corollary 1.

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

$$\left(N + \sqrt{N} + 1\right)^2 < \psi_3(N) < \left(N + \frac{3}{4}\sqrt{2N} + 1\right)^2 - \frac{3}{8}N.$$

We can use Corollary 1 to find an useful approximation of ψ_n. This result will be useful when devising the attack against the generalized Murru-Saettone scheme.

Proposition 2. *Let $N = pq$ be the product of two unknown primes with $q < p < 2q$. We define*

$$\psi_{n,0}(N) = \frac{1}{2}\left(\frac{\sqrt{N}^n - 1}{\sqrt{N} - 1}\right)^2 + \frac{1}{2} \cdot \frac{(\sqrt{2N})^n - 1}{\sqrt{2N} - 1} \cdot \frac{\left(\frac{\sqrt{2N}}{2}\right)^n - 1}{\frac{\sqrt{2N}}{2} - 1}.$$

Then the following holds

$$|\psi_n(N) - \psi_{n,0}(N)| < \frac{\Delta_n}{2} N^{n-2}\sqrt{N},$$

where

$$\Delta_n = \left(\frac{\sqrt{2}^n - 1}{\sqrt{2} - 1}\right)\left(\frac{\left(\frac{\sqrt{2}}{2}\right)^n - 1}{\frac{\sqrt{2}}{2} - 1}\right) - n^2.$$

Proof. According to Corollary 1, $\psi_{n,0}(N)$ is the mean value of the lower and upper bound. The following property holds

$$
\begin{aligned}
|\psi_n(N) - \psi_{n,0}(N)| &\leq \frac{1}{2}\left[\frac{(\sqrt{2N})^n - 1}{\sqrt{2N} - 1} \cdot \frac{\left(\frac{\sqrt{2N}}{2}\right)^n - 1}{\frac{\sqrt{2N}}{2} - 1} - \left(\frac{\sqrt{N}^n - 1}{\sqrt{N} - 1}\right)^2\right] \\
&= \frac{1}{2}\left[\sum_{i,j=0}^{n-1}(\sqrt{2N})^i\left(\frac{\sqrt{2N}}{2}\right)^j - \sum_{i,j=0}^{n-1}\sqrt{N}^i\sqrt{N}^j\right] \\
&= \frac{1}{2}\left[\sum_{i,j=0}^{n-1}\sqrt{N}^i\sqrt{N}^j\left(\frac{\sqrt{2}^{i+j}}{2^j} - 1\right)\right] \\
&= \frac{1}{2}\left[\sum_{\substack{i,j=0 \\ i\neq j}}^{n-1}\sqrt{N}^i\sqrt{N}^j\left(\frac{\sqrt{2}^{i+j}}{2^j} - 1\right)\right].
\end{aligned}
$$

Note that in the last expression all the coefficients are non-zero and the leading coefficient is $\sqrt{N}^{n-1+n-2} = N^{n-2}\sqrt{N}$. Therefore, we obtain

$$
\begin{aligned}
|\psi_n(N) - \psi_{n,0}(N)| &< \frac{1}{2}N^{n-2}\sqrt{N}\left[\sum_{\substack{i,j=0 \\ i\neq j}}^{n-1}\left(\frac{\sqrt{2}^{i+j}}{2^j} - 1\right)\right] \\
&= \frac{1}{2}N^{n-2}\sqrt{N}\left[\sum_{i,j=0}^{n-1}\frac{\sqrt{2}^{i+j}}{2^j} - n(n-1) - n\right] \\
&= \frac{1}{2}N^{n-2}\sqrt{N}\left[\left(\frac{\sqrt{2}^n - 1}{\sqrt{2} - 1}\right)\left(\frac{\left(\frac{\sqrt{2}}{2}\right)^n - 1}{\frac{\sqrt{2}}{2} - 1}\right) - n^2\right],
\end{aligned}
$$

as desired.

$\square$

When $n = 3$, the following property presented in [22] becomes a special case of Proposition 2.

Corollary 3. *Let $N = pq$ be the product of two unknown primes with $q < p < 2q$. Then the following holds*

$$|\psi_3(N) - \psi_{3,0}(N)| < 0.372N\sqrt{N} < 0.5N\sqrt{N}.$$

6 Application of Continued Fractions

We further provide an upper bound for selecting d such that we can use the continued fraction algorithm to recover d without knowing the factorisation of the modulus N.

Theorem 2. *Let $N = pq$ be the product of two unknown primes with $q < p < 2q$. If $e < \psi_n(N)$ satisfies $ed - k\psi_n(N) = 1$ with*

$$d < \sqrt{\frac{N^{n-0.5}}{e\Delta_n}}, \tag{1}$$

then we can recover d in polynomial time.

Proof. We have that

$$\left| \frac{k}{d} - \frac{e}{\psi_{n,0}(N)} \right| = \frac{|ed - k\psi_{n,0}(N)|}{d\psi_{n,0}(N)}$$
$$\leq \frac{|ed - k\psi_n(N)| + k|\psi_n(N) - \psi_{n,0}(N)|}{d\psi_{n,0}(N)}.$$

Using $ed - k\psi_n(N) = 1$ and Proposition 2 we obtain

$$\left| \frac{k}{d} - \frac{e}{\psi_{n,0}(N)} \right| \leq \frac{1 + \frac{\Delta_n}{2}kN^{n-2}\sqrt{N}}{d\psi_{n,0}(N)}$$
$$\leq \frac{k}{2d} \cdot \Delta_n \cdot \frac{2 + N^{n-2}\sqrt{N}}{\psi_{n,0}(N)}.$$

Note that

$$\psi_{n,0}(N) > \left(\frac{\sqrt{N}^n - 1}{\sqrt{N} - 1} \right)^2 > \sqrt{N}^{2(n-1)} + 2\sqrt{N},$$

which leads to

$$\left| \frac{k}{d} - \frac{e}{\psi_{n,0}(N)} \right| \leq \frac{k}{2d} \cdot \Delta_n \cdot \frac{2 + \sqrt{N}^{2n-3}}{\sqrt{N}^{2n-2} + 2\sqrt{N}}$$
$$= \frac{k\Delta_n}{2d\sqrt{N}}. \tag{2}$$

According to Corollary 1, we have that $\psi_n(N) > \sqrt{N}^{2(n-1)} = N^{n-1}$. Since $k\psi_n(N) = ed - 1 < ed$, we have

$$\frac{k}{d} < \frac{e}{\psi_n(N)} < \frac{e}{N^{n-1}}.$$

Equation (2) becomes

$$\left| \frac{k}{d} - \frac{e}{\psi_{n,0}(N)} \right| \leq \frac{1}{2} \cdot \frac{e\Delta_n}{N^{n-0.5}} < \frac{1}{2d^2}.$$

Using Theorem 1 we obtain that k/d is a convergent of the continued fraction expansion of $e/\psi_{n,0}(N)$. Therefore, d can be recovered in polynomial time.

□

Corollary 4. *Let $\alpha + 0.5 < n$ and $N = pq$ be the product of two unknown primes with $q < p < 2q$. If we approximate $e \simeq N^\alpha$ and $N \simeq 2^{2\lambda}$, then Equation (1) becomes*

$$d < \frac{2^{(n-\alpha-0.5)\lambda}}{\sqrt{\Delta_n}}$$

or equivalently

$$\log_2(d) < (n - \alpha - 0.5)\lambda - \log_2(\sqrt{\Delta_n}) \simeq (n - \alpha - 0.5)\lambda.$$

When case $n = 3$ is considered, the following property presented in [22] becomes a special case of Corollary 4.

Corollary 5. *Let $\alpha < 2.5$ and $N = pq$ be the product of two unknown primes with $q < p < 2q$. If we approximate $e \simeq N^\alpha$ and $N \simeq 2^{2\lambda}$ then Equation (1) is equivalent with*

$$\log_2(d) < (2.5 - \alpha)\lambda - 0.43 \simeq (2.5 - \alpha)\lambda.$$

The following corollary tells us that when e is large enough we obtain roughly the same margin as Wiener [4, 30] obtained for the classical RSA.

Corollary 6. *Let $N = pq$ be the product of two unknown primes with $q < p < 2q$. If we approximate $e \simeq N^{n-1}$ and $N \simeq 2^{2\lambda}$ then Equation (1) is equivalent with*

$$\log_2(d) < 0.5\lambda - \log_2(\sqrt{\Delta_n}) \simeq 0.5\lambda.$$

7 Experimental results

We further present an example for each of the $n = 2$ and $n = 4$ cases. An example for the $n = 3$ case is provided in [22], and thus we omit it.

7.1 Case $n = 2$

Before providing our example, we first show how to recover p and q once $\psi_2(N) = (1 - ed)/k$ is recovered using our attack.

Lemma 3. *Let $N = pq$ be the product of two unknown primes with $q < p < 2q$. If $\psi_2(N) = (1+p)(1+q)$ is known, then p and q can be recovered in polynomial time.*

Proof. Expanding $\psi_2(N)$ we obtain that

$$\psi_2(N) = 1 + p + q + pq = 1 + p + q + N,$$

which is equivalent to

$$p + q = \psi_2(N) - N - 1.$$

Let $S = \psi_2(N) - N - 1$. We remark that

$$(p - q)^2 = (p + q)^2 - 4pq = S^2 - 4N.$$

Let D be the positive square root of the previous quantity. Taking into account that $p > q$, we derive the following

$$\begin{cases} p = \frac{S+D}{2} \\ q = \frac{S-D}{2} \end{cases}.$$

$\square$

Now, we will exemplify our attack for $n = 2$ using the following small public key

$$N = 1193955469391405546525045411470651045582478 7856591,$$
$$e = 6074574633060181514768858436051302980810169830821.$$

Remark that $e \approx N^{0.994}$. We use the Euclidean algorithm to compute the continue fraction expansion of $e/\psi_{2,0}(N)$ and obtain that the first 20 partial quotients are

$$[0, 1, 1, 27, 1, 56, 7, 23, 3, 2, 9, 2, 20, 1, 3, 1, 1, 1, 2, 7, 17, \ldots].$$

According to Theorem 2, the set of convergents of $e/\psi_{2,0}(N)$ contains all the possible candidates for k/d. From these convergents we select only those for which $\psi_2 = (ed - 1)/k$ is an integer and the following system of equations

$$\begin{cases} \psi_2 = (1 + p)(1 + q) \\ N = pq \end{cases}$$

has a solution as given in Lemma 3. The $2nd$, $3rd$ and $15th$ convergents satisfy the first condition, however only the last one leads to a valid solution for p and q. More precisely, the $15th$ convergent leads to

$$\psi_2 = 1193955469391405546525046128356787695878533749000,$$
$$\frac{k}{d} = \frac{3205471919}{6300343581},$$
$$p = 45376298382661174418120249,$$
$$q = 26312315282368431315131 59.$$

7.2 Case $n = 4$

As in the previous case, we first show how to factorize N once ψ_4 is known.

Lemma 4. *Let $N = pq$ be the product of two unknown primes with $q < p < 2q$. If $\psi_4(N) = (1 + p + p^2 + p^3)(1 + q + q^2 + q^3)$ is known, then p and q can be recovered in polynomial time.*

Proof. Expanding $\psi_4(N)$ we obtain that

$$
\begin{aligned}
\psi_4(N) &= p^3q^3 + p^3q^2 + p^3q + p^3 + p^2q^3 + p^2q^2 + p^2q + p^2 \\
&\quad + pq^3 + pq^2 + pq + p + q^3 + q^2 + q + 1 \\
&= N^3 + (N^2 + 1)(p + q) + (N + 1)(p^2 + pq + q^2) + \\
&\quad + (p^3 + p^2q + pq^2 + q^3) + 1 \\
&= N^3 + (N^2 + 1)(p + q) + (N + 1)(p + q)^2 - (N + 1)N \\
&\quad + (p + q)^3 - 2N(p + q) + 1.
\end{aligned}
$$

We further consider the following form of ψ_4

$$\psi_4(N) = (p + q)^3 + (N + 1)(p + q)^2 + (N - 1)^2(p + q) + N^3 - N^2 - N + 1.$$

Finding $S = p + q$ is equivalent to solving (in $\mathbb{Z}$) the cubic equation

$$x^3 + (N + 1)x^2 + (N - 1)^2 x + (N^3 - N^2 - N + 1 - \psi_4(N)) = 0, \qquad (3)$$

which can be done in polynomial time as it is presented in [10]. In order to find p and q, we compute $D = p - q$ as in Lemma 3. This concludes our proof. $\qquad \square$

The following lemma shows that in order to factor N we only need to find one solution to Equation (3), namely its unique integer solution.

Lemma 5. *Equation (3) always has exactly two non-real roots and an integer one.*

Proof. Let x_1, x_2 and x_3 be Equation (3)'s roots. Using Vieta's formulas we have

$$x_1 + x_2 + x_3 = -(N+1),$$
$$x_1 x_2 + x_2 x_3 + x_3 x_1 = (N-1)^2,$$
$$x_1 x_2 x_3 = -(N^3 - N^2 - N + 1 - \psi_4(N)).$$

From the first two relations we obtain

$$\begin{aligned} x_1^2 + x_2^2 + x_3^2 &= (x_1 + x_2 + x_3)^2 - 2(x_1 x_2 + x_2 x_3 + x_3 x_1) \\ &= (N+1)^2 - 2(N-1)^2 \\ &= -N^2 + 6N - 1. \end{aligned}$$

If we assume that x_1, x_2, x_3 are all real, we get the following inequalities

$$0 < x_1^2 + x_2^2 + x_3^2 = -(N-3)^2 + 8 < 0,$$

for any $N \geq 6$. Therefore, we obtain a contradiction, and hence we conclude that Equation (3) has one real root, which is $p + q \in \mathbb{Z}$, and two non-real roots. $\qquad\square$

We will further present our attack for $n = 4$ using the following small public key

$$N = 1193955469391405546525045411470651045582478856591,$$
$$\begin{aligned} e = {}& 1500665228703975986133780232456521562331094047651 3 \\ & 925426704347225501574482708873182176329621382054 21 \\ & 899647696285870461657741073464172612216312741409. \end{aligned}$$

Note that $e \approx N^{2.998}$. Applying the continue fraction expansion of $e/\psi_{4,0}(N)$, we get the first 20 partial quotients

$$[0, 1, 7, 2, 4, 1, 4, 6, 1, 4, 26, 1, 7, 1, 1, 10, 2, 1, 11, 1, 1, \ldots].$$

In this case, we consider the convergents of $e/\psi_{4,0}(N)$, and we select only those for which $\psi_4 = (ed - 1)/k$ is an integer and the following system of equations

$$\begin{cases} \psi_4 = (1 + p + p^2 + p^3)(1 + q + q^2 + q^3) \\ N = pq \end{cases}$$

has a solution as given in Lemma 4. The $2nd$ and $19th$ convergents satisfy the first condition, however only the last one leads to a valid solution for p and q.

More precisely, the 19th convergent leads to

$$\psi_4 = 170201893778678602470965530944670615912076408355062190775345791193418238762318868318717043063672778999618058600556573209318787267816952014412436000,$$

$$\frac{k}{d} = \frac{2425248603}{2750659489},$$

$$p = 4537629838266117418120249,$$

$$q = 2631231528236843131513159.$$

8   Conclusions

In this paper we introduced a family of RSA-like cryptosystems, which includes the Murru and Saettone public key encryption scheme [18] (*i.e.* $n = 3$). Then, we presented a small private key attack against our family of cryptosystems and provided two instantiations of it. As a conclusion, the whole family of RSA-like schemes allows an attacker to recover the secret exponent via continued fractions when the public exponent is close to N^{n-1} and the secret exponent is smaller that $N^{0.25}$.

Future Work. When $n = 2, 3, 4$, in Section 7 and [22] a method for factoring N once ψ_n is known is provided. Although we found a method for particular cases of n we could not find a generic method for factoring N. Therefore, we leave it as an open problem. Another interesting research direction, is to find out if the attack methods described in Section 1 for the Murru-Saetonne schemes also work in the general case.

References

1. Aono, Y.: Minkowski Sum Based Lattice Construction for Multivariate Simultaneous Coppersmith's Technique and Applications to RSA. In: ACISP 2013. Lecture Notes in Computer Science, vol. 7959, pp. 88–103. Springer (2013)
2. Blömer, J., May, A.: New Partial Key Exposure Attacks on RSA. In: CRYPTO 2003. Lecture Notes in Computer Science, vol. 2729, pp. 27–43. Springer (2003)
3. Blömer, J., May, A.: A Generalized Wiener Attack on RSA. In: PKC 2004. Lecture Notes in Computer Science, vol. 2947, pp. 1–13. Springer (2004)
4. Boneh, D.: Twenty Years of Attacks on the RSA Cryptosystem. Notices of the AMS **46**(2), 203–213 (1999)
5. 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)
6. Boneh, D., Durfee, G., Frankel, Y.: An Attack on RSA Given a Small Fraction of the Private Key Bits. In: ASIACRYPT 1998. Lecture Notes in Computer Science, vol. 1514, pp. 25–34. Springer (1998)

7. Coppersmith, D.: Small Solutions to Polynomial Equations, and Low Exponent RSA Vulnerabilities. Journal of Cryptology **10**(4), 233–260 (1997)
8. De Weger, B.: Cryptanalysis of RSA with Small Prime Difference. Appl. Algebra Eng. Commun. Comput. **13**(1), 17–28 (2002)
9. Ernst, M., Jochemsz, E., May, A., Weger, B.d.: Partial Key Exposure Attacks on RSA up to Full Size Exponents. In: EUROCRYPT 2005. Lecture Notes in Computer Science, vol. 3494, pp. 371–386. Springer (2005)
10. Fujii, K.: A Modern Introduction to Cardano and Ferrari Formulas in the Algebraic Equations. arXiv Preprint **arXiv:quant-ph/0311102** (2003)
11. Hardy, G.H., Wright, E.M., et al.: An Introduction to the Theory of Numbers. Oxford University Press (1979)
12. Hastad, J.: On Using RSA with Low Exponent in a Public Key Network. In: CRYPTO 1985. Lecture Notes in Computer Science, vol. 218, pp. 403–408. Springer (1985)
13. 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)
14. Howgrave-Graham, N., Seifert, J.P.: Extending Wiener's Attack in the Presence of Many Decrypting Exponents. In: CQRE (Secure) 1999. Lecture Notes in Computer Science, vol. 1740, pp. 153–166. Springer (1999)
15. Kamel Ariffin, M.R., Abubakar, S.I., Yunos, F., Asbullah, M.A.: New Cryptanalytic Attack on RSA Modulus $N = pq$ Using Small Prime Difference Method. Cryptography **3**(1), 2 (2018)
16. Maitra, S., Sarkar, S.: Revisiting Wiener's Attack - New Weak Keys in RSA. In: ISC 2008. Lecture Notes in Computer Science, vol. 5222, pp. 228–243. Springer (2008)
17. Maitra, S., Sarkar, S.: Revisiting Wiener's Attack - New Weak Keys in RSA. IACR Cryptology ePrint Archive **2008/228** (2008)
18. 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)
19. Nassr, D.I., Anwar, M., Bahig, H.M.: Improving Small Private Exponent Attack on the Murru-Saettone Cryptosystem. Theor. Comput. Sci. **923**, 222–234 (2022)
20. Nassr, D.I., Bahig, H.M., Bhery, A., Daoud, S.S.: A New RSA Vulnerability Using Continued Fractions. In: AICCSA 2008. pp. 694–701. IEEE Computer Society (2008)
21. Nitaj, A.: Another Generalization of Wiener's Attack on RSA. In: AFRICACRYPT 2008. Lecture Notes in Computer Science, vol. 5023, pp. 174–190. Springer (2008)
22. 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)
23. Nitaj, A., Ariffin, M.R.B.K., Adenan, N.N.H., Lau, T.S.C., Chen, J.: Security Issues of Novel RSA Variant. IEEE Access **10**, 53788–53796 (2022)
24. 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)
25. Sarkar, S., Maitra, S.: Cryptanalysis of RSA with more than one Decryption Exponent. Information Processing Letters **110**(8-9), 336–340 (2010)
26. Shi, G., Wang, G., Gu, D.: Further Cryptanalysis of a Type of RSA Variants. IACR Cryptology ePrint Archive **2022/611** (2022)

27. 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)
28. Takayasu, A., Kunihiro, N.: Cryptanalysis of RSA with Multiple Small Secret Exponents. In: ACISP 2014. Lecture Notes in Computer Science, vol. 8544, pp. 176–191. Springer (2014)
29. Takayasu, A., Kunihiro, N.: Partial Key Exposure Attacks on RSA: Achieving the Boneh-Durfee Bound. In: SAC 2014. Lecture Notes in Computer Science, vol. 8781, pp. 345–362. Springer (2014)
30. Wiener, M.J.: Cryptanalysis of Short RSA Secret Exponents. IEEE Trans. Inf. Theory **36**(3), 553–558 (1990)
31. Zheng, M., Kunihiro, N., Yao, Y.: Cryptanalysis of the RSA Variant Based on Cubic Pell Equation. Theor. Comput. Sci. **889**, 135–144 (2021)