Small Private Key Attack Against a Family of RSA-Like Cryptosystems

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

[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. Elkamchouchi, Elshenawy and Shaban presented in 2002 an interesting RSA-like cryptosystem that uses the key equation $ed - k(p^2 - 1)(q^2 - 1) = 1$, instead of the classical RSA key equation $ed - k(p - 1)(q - 1) = 1$. The authors claimed that their scheme is more secure than RSA. Unfortunately, the common attacks developed against RSA can be adapted for Elkamchouchi *et al.*'s scheme. In this paper, we introduce a family of RSA-like encryption schemes that uses the key equation $ed - k(p^n - 1)(q^n - 1) = 1$, where $n > 0$ 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 [29] proposed one of the most popular and widely used cryptosystems, 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's 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 2002, Elkamchouchi, Elshenawy and Shaban [15] extend the classical RSA scheme to the ring of Gaussian integers modulo N. A Gaussian integer modulo N is a number of the form $a+bi$, where $a, b \in \mathbb{Z}_N$ and $i^2 = -1$. Let $\mathbb{Z}_N[i]$ denote the set of all Gaussian integers modulo N and let $\phi(N) = |\mathbb{Z}_N^*[i]| = (p^2-1)(q^2-1)$. To set up the public exponent, in this case we must have $\gcd(e, \phi(N)) = 1$. The corresponding private exponent is $d \equiv e^{-1} \bmod \phi(N)$. In order to encrypt a message $m \in \mathbb{Z}_N[i]$, we simply compute $c \equiv m^e \bmod N$ and to decrypt it $m \equiv c^d \bmod N$. Note that the exponentiations are computed in the ring $\mathbb{Z}_N[i]$.

L. Fritsch et al. (Eds.): NordSec 2023, LNCS 14324, pp. 57–72, 2024.
https://doi.org/10.1007/978-3-031-47748-5_4

The authors of [15] claim that this extension provides more security than that of the classical RSA. In the following paragraphs we present a series of common attacks that work for both types of cryptosystems.

Small Private Key Attacks. In order to decrease decryption time, one may prefer to use a smaller d. Wiener showed in [33] 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 [12], Boneh and Durfee [5] improved Wiener's bound to $N^{0.292}$. Later on, Herrmann and May [19] 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 [25] present a method based on continued fractions for recovering d when $d < N^{(1-\delta)/2}$.

In the case of Elkamchouchi *et al.*, a small private key attack based on continued fractions was presented in [7]. Using lattice reduction, the attack was improved in [28,34]. The authors obtained a bound of $d < N^{0.585}$. A generalization of the attack presented in [7] to unbalanced prime numbers was presented in [9]. Considering the generic equation $ex - y\phi(N) = z$, the authors of [8] describe a method for factoring N when $xy < 2N - 4\sqrt{2}N^{0.75}$ and $|z| < (p - q)N^{0.25}y$. An extension of the previous attack was proposed in [27].

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 [20] describe an attack against RSA that recovers the corresponding small private exponents $d_i \simeq N^{\beta}$. This attack was later improved by Sarkar and Maitra [30], Aono [1] and Takayasu and Kunihiro [31]. The best known bound [31] 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 Elkamchouchi *et al.* cryptosystem was studied by Zheng, Kunihiro and Hu [34]. The bound obtained by the authors is $\beta < 2 - 2\sqrt{2/(3\ell + 1)}$ and it is twice the bound obtained by Takayasu and Kunihiro [31]. Note that when $\ell = 1$ the bound is equal to 0.585.

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.* [16] and Takayasu and Kunihiro [32]. The best known bound [32] is $\beta < (\gamma + 2 - \sqrt{2 - 3\gamma^2})/2$, where the attacker knows N^{γ} leaked bits.

Zheng, Kunihiro and Hu [34] describe a partial exposure attack that works in the case of the Elkamchouchi *et al.* 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 prime difference $|p - q|$ is small and certain conditions hold, de Weger [14] 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 [22,23] 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.* [21].

The small prime difference attack against the Elkamchouchi *et al.* public key encryption scheme was studied in [11]. Note that when the common condition $|p-q| < N^{0.5}$ holds, their bound leads to the small private key bound $d < N^{0.585}$.

Related Work. It is worth noting that our current undertaking shares similarities with a prior work of ours [13], where we explored a cryptographic system closely related to our own. Specifically, we studied the implications of generalizing the Murru-Saettone cryptosystem [24], and the effect of using continued fractions to recover the private key.

1.1 Our Contributions

We first remark that the rings $Z_p = \mathbb{Z}_p[t]/(t+1) = GF(p)$ and $Z_p[i] = \mathbb{Z}_p[t]/(t^2+1) = GF(p^2)$, where GF stands for Galois field. Therefore, we can rethink the RSA scheme as working in the $GF(p) \times GF(q)$ group instead of $\mathbb{Z}_N$. Also, that the Elkamchouchi *et al.* scheme is an extension to $GF(p^2) \times GF(q^2)$ instead of $Z_N[i]$. This leads to a natural generalization of RSA to $GF(p^n) \times GF(q^n)$, where $n > 1$. In this paper we introduce exactly this extension. We wanted to see if only for $n = 1$ and $n = 2$ the common attacks presented in the introduction 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 $d < N^{0.25n}$, 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 Sect. 2 notations and definitions used throughout the paper. Inspired by Rivest *et al.* and Elkamchouchi *et al.*'s work [15,29], in Sect. 3 we construct a family of RSA-like cryptosystems. After proving several useful lemmas in Sect. 4, we extend Wiener's small private key attack in Sect. 5. Two concrete instantiations are provided in Sect. 6. We conclude our paper in Sect. 7.

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 $[0, a]$. We use $\simeq$ to indicate that two values are approximately equal.

2.1 Continued Fraction

For any real number ζ there exists a 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 [18], 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 $[a_0, a_1, a_2, \ldots]$.

2.2 Quotient Groups

In this section we will provide the mathematical theory needed to generalize the Rivest, Shamir and Adleman, and the Elkamchouchi, Elshenawy and Shaban encryption schemes. Therefore, let $(\mathbb{F}, +, \cdot)$ be a field and $t^n - r$ an irreducible polynomial in $\mathbb{F}[t]$. Then

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

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

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

3 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, $\mathbb{A}_n^*$ is a cyclic group of order $\varphi_n(\mathbb{Z}_p) = p^n - 1$. Remark that an analogous of Fermat's little theorem holds

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

where $a(x) \in \mathbb{A}_n^*$ and the power is evaluated by $\circ$-multiplying $a(x)$ by itself $\varphi_n(\mathbb{Z}_p) - 1$ times. Therefore, we can build an encryption scheme that is similar to RSA using the $\circ$ as the product.

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

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

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

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

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

Remark 1. When $n = 1$ we get the RSA scheme [29]. Also, when $n = 2$, we obtain the Elkamchouchi *et al.* cryptosystem [15].

4 Useful Lemmas

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

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

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

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

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

is strictly decreasing with x.

Proof. Computing the derivative of f we have that

$$f'(x) = -n\left(x^{n-1} - \frac{1}{x^{n+1}} \cdot N^n\right).$$

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

$$x^{2n} > N^n \Leftrightarrow x^{n-1} > \frac{1}{x^{n+1}} \cdot N^n \Leftrightarrow f'(x) < 0,$$

and therefore we have f is strictly decreasing function. □

Using the following result from [26, Lemma 1], we will compute a lower and upper bound for $\varphi_n(N)$.

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

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

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

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

Proof. By Lemma 1 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

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

as desired. □

When $n = 1$ and $n = 2$, the following results proven in [10] and [7] respectively become 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*

$$(\sqrt{N} - 1)^2 > \varphi_1(N) > N + 1 - \frac{3}{\sqrt{2}}\sqrt{N}.$$

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

$$(N - 1)^2 > \varphi_2(N) > N^2 + 1 - \frac{5}{2}N.$$

We can use Corollary 1 to find a useful approximation of φ_n. This result will be useful when devising the attack against the generalized RSA scheme.

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

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

Then the following holds

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

where

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

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

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

as desired. □

When $n = 1$ and $n = 2$, the following property presented in [10] and [7] respectively become a special case of Proposition 2.

Corollary 4. *Let $N = pq$ be the product of two unknown primes with $q < p < 2q$. Then the following holds*

$$|\varphi_1(N) - \varphi_{1,0}(N)| < \frac{3 - 2\sqrt{2}}{2\sqrt{2}}\sqrt{N}.$$

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

$$|\varphi_2(N) - \varphi_{2,0}(N)| < \frac{1}{4}N.$$

5 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 $e < \varphi_n(N)$ satisfies $ed - k\varphi_n(N) = 1$ with*

$$d < \sqrt{\frac{\sqrt{2}^n N^n (\sqrt{N}^n - \delta_n)}{e(\sqrt{2}^n - 1)^2}}, \tag{1}$$

where

$$\delta_n = \frac{2\sqrt{2}^n}{(\sqrt{2}^n - 1)^2} + \frac{2(2^n + 1)}{\sqrt{2}^n},$$

then we can recover d in polynomial time.

Proof. Since $ed - k\varphi_n(N) = 1$, we have that

$$\begin{aligned}\left|\frac{k}{d} - \frac{e}{\varphi_{n,0}(N)}\right| &\le e\left|\frac{1}{\varphi_{n,0}(N)} - \frac{1}{\varphi_n(N)}\right| + \left|\frac{e}{\varphi_n(N)} - \frac{k}{d}\right| \\ &= e\frac{|\varphi_n(N) - \varphi_{n,0}(N)|}{\varphi_{n,0}(N)\varphi_n(N)} + \frac{1}{\varphi_n(N)d}.\end{aligned}$$

Let $\varepsilon_n = N^n - \sqrt{N}^n(2^n+1)/\sqrt{2}^n + 1$. Using $d = (k\varphi_n(N) - 1)/e = 1$ and Proposition 2 we obtain

$$\begin{aligned}
\left|\frac{k}{d} - \frac{e}{\varphi_{n,0}(N)}\right| &\leq \frac{\frac{\Delta_n}{2} e\sqrt{N}^n}{\varphi_{n,0}(N)\varphi_n(N)} + \frac{e}{\varphi_n(N)(k\varphi_n(N)-1)} \\
&\leq \frac{e\sqrt{N}^n(\sqrt{2}^n-1)^2}{2\sqrt{2}^n\varepsilon_n^2} + \frac{e}{\varepsilon_n(k\varepsilon_n - 1)} \\
&\leq \frac{e\sqrt{N}^n(\sqrt{2}^n-1)^2}{2\sqrt{2}^n\varepsilon_n^2} + \frac{e}{\varepsilon_n^2} \\
&= \frac{e[\sqrt{N}^n(\sqrt{2}^n-1)^2 + 2\sqrt{2}^n]}{2\sqrt{2}^n\varepsilon_n^2} \\
&\leq \frac{e[\sqrt{N}^n(\sqrt{2}^n-1)^2 + 2\sqrt{2}^n]}{2\sqrt{2}^n(N^n - \frac{2^n+1}{\sqrt{2}^n}\sqrt{N}^n)^2}.
\end{aligned}$$

Note that

$$\begin{aligned}
\frac{[\sqrt{N}^n(\sqrt{2}^n-1)^2 + 2\sqrt{2}^n]}{2\sqrt{2}^n(N^n - \frac{2^n+1}{\sqrt{2}^n}\sqrt{N}^n)^2} &= \frac{(\sqrt{2}^n-1)^2[\sqrt{N}^n + \frac{2\sqrt{2}^n}{(\sqrt{2}^n-1)^2}]}{2\sqrt{2}^n N^n(\sqrt{N}^n - \frac{2^n+1}{\sqrt{2}^n})^2} \\
&\leq \frac{(\sqrt{2}^n-1)^2}{2\sqrt{2}^n N^n(\sqrt{N}^n - \delta_n)},
\end{aligned}$$

which leads to

$$\left|\frac{k}{d} - \frac{e}{\varphi_{n,0}(N)}\right| \leq \frac{e(\sqrt{2}^n-1)^2}{2\sqrt{2}^n N^n(\sqrt{N}^n - \delta_n)} \leq \frac{1}{2d^2}.$$

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

Corollary 6. *Let $\alpha < 1.5n$ 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 Eq. 1 becomes*

$$d < \frac{2^{(n-\alpha)\lambda + \frac{n}{4}}\sqrt{2^{n\lambda} - \delta_n}}{\sqrt{2}^n - 1} < \frac{2^{(1.5n-\alpha)\lambda+\frac{n}{4}}}{\sqrt{2}^n - 1}$$

or equivalently

$$\log_2(d) < (1.5n-\alpha)\lambda + \frac{n}{4} - \log_2(\sqrt{2}^n - 1) \simeq (1.5n - \alpha)\lambda$$

When cases $n = 1$ and $n = 2$ are considered the following properties presented in [10] and [7] respectively become a special case of Corollary 6. Note that when $n = \alpha = 1$ we obtain roughly the same margin as Wiener [4,33] obtained for the classical RSA.

Corollary 7. *Let $\alpha < 1.5$ 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 Eq. 1 is equivalent to*

$$\log_2(d) < (1.5-\alpha)\lambda - 0.25 + 1.27 \simeq (1.5-\alpha)\lambda.$$

Corollary 8. *Let $\alpha < 3$ 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 Eq. 1 is equivalent to*

$$\log_2(d) < (3-\alpha)\lambda - 0.5 \simeq (3-\alpha)\lambda.$$

The last corollary tells us what happens when e is large enough. We can see that n is directly proportional to the secret exponent's upper bound.

Corollary 9. *Let $N = pq$ be the product of two unknown primes with $q < p < 2q$. If we approximate $e \simeq N^n$ and $N \simeq 2^{2\lambda}$ then Eq. 1 is equivalent to*

$$\log_2(d) < 0.5n\lambda + \frac{n}{4} - \log_2(\sqrt{2}^n - 1) \simeq 0.5n\lambda.$$

6 Experimental Results

We further present an example for the $n = 3$ and $n = 4$ cases. Examples for $n = 1$ and $n = 2$ cases are provided in [10] and [7] respectively, and thus we omit them.

6.1 Case $n = 3$

Before providing our example, we first show how to recover p and q once $\varphi_3(N) = (ed-1)/k$ is recovered using our attack.

Lemma 2. *Let $N = pq$ be the product of two unknown primes with $q < p < 2q$. If $\varphi_3(N) = N^3 - p^3 - q^3 + 1$ is known, then p and q can be recovered in polynomial time.*

Proof. We will rewrite $\varphi_3(N)$ as

$$\begin{aligned}\varphi_3(N) &= N^3 - p^3 - 3p^2q - 3pq^2 - q^3 + 1 + 3p^2q + 3pq^2\\ &= N^3 - (p+q)^3 + 3N(p+q) + 1,\end{aligned}$$

which is equivalent to

$$(p+q)^3 - 3N(p+q) + \varphi_3(N) - N^3 - 1 = 0.$$

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

$$x^3 - 3Nx + (\varphi_3(N) - N^3 - 1) = 0. \tag{2}$$

which can be done in polynomial time as it is presented in [17]. In order to find p and q, we compute $D = p - q$ using the following remark

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

Taking into account that $p > q$, D is the positive square root of the previous quantity, and thus we derive the following

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

□

The following lemma shows that in order to factor N we only need to find one solution to Eq. 2, namely its unique integer solution.

Lemma 3. *Eq. 2 always has exactly two non-real roots and an integer one.*

Proof. Let x_1, x_2 and x_3 be Eq. 2's roots. Using Vieta's formulas we have

$$\begin{aligned} x_1 + x_2 + x_3 &= 0, \\ x_1x_2 + x_2x_3 + x_3x_1 &= -3N, \\ x_1x_2x_3 &= -(\varphi_3(N) - N^3 - 1). \end{aligned}$$

From the first two relations we obtain

$$\begin{aligned} x_1^2 + x_2^2 + x_3^2 &= (x_1 + x_2 + x_3)^2 - 2(x_1x_2 + x_2x_3 + x_3x_1) \\ &= 6N. \end{aligned}$$

If we assume that $x_1 = p + q$ and x_2, x_3 are both real, we get the following system

$$\begin{cases} x_2 + x_3 = -(p+q) \\ x_2^2 + x_3^2 = 6N - (p+q)^2 \end{cases} \Rightarrow \begin{cases} (x_2 + x_3)^2 = (p+q)^2 \\ 2(x_2^2 + x_3^2) = 12N - 2(p+q)^2 \end{cases} \Rightarrow$$

$$\begin{aligned} (x_2 - x_3)^2 &= 12N - 3(p+q)^2 \\ &= 6pq - 3p^2 - 3q^2 \\ &= -3(p-q)^2 < 0. \end{aligned}$$

Therefore, we obtain a contradiction, and hence we conclude that Eq. 2 has one real root, which is $p + q \in \mathbb{Z}$, and two non-real roots. □

Now, we will exemplify our attack for $n = 3$ using the following small public key

$$\begin{aligned} N &= 301497263350304033659022650831635102276891332393 3, \\ e &= 820565649379899255763245233292622281976243530699 9 \\ &\quad 012462603561251756300599889565468852664300271543 4 \\ &\quad 25112020628278119623817044320522328087505650969. \end{aligned}$$

Remark that $e \approx N^{2.989}$. We use the Euclidean algorithm to compute the continued fraction expansion of $e/\varphi_{3,0}(N)$ and obtain that the first 25 partial quotients are

$$[0, 3, 2, 1, 16, 5, 3, 5, 1, 5, 1, 11, 2, 6, 1, 3, 1, 4, 1, 1, 1, 267, 1, 1, 4, \ldots].$$

According to Theorem 2, the set of convergents of $e/\varphi_{3,0}(N)$ contains all the possible candidates for k/d. From these convergents we select only those for which $\varphi_3 = (ed - 1)/k$ is an integer and the following system of equations

$$\begin{cases} \varphi_3 = (p^3 - 1)(q^3 - 1) \\ N = pq \end{cases}$$

has a solution as given in Lemma 2. The $2nd$, $3rd$ and $21st$ convergents satisfy the first condition, however only the last one leads to a valid solution for p and q. More precisely, the $21st$ convergent leads to

$$\begin{aligned} \varphi_3 &= 274062820789295320701870217407748380756326440877 3\\ &\quad 705796398775750937428051715725970822299448776344 6\\ &\quad 946621855565600927215471565545807198298953933036,\\ \frac{k}{d} &= \frac{514812488}{1719435401},\\ p &= 211977819903685906870781 9,\\ q &= 142230570862221395680680 7. \end{aligned}$$

6.2 Case $n = 4$

As in the previous case, we first show how to factorize N once φ_4 is known.

Lemma 4. *Let $N = pq$ be the product of two unknown primes with $q < p < 2q$. If $\varphi_4(N) = N^4 - p^4 - q^4 + 1$ is known, then*

$$p = \frac{1}{2}(S + D) \quad \text{and} \quad q = \frac{1}{2}(S - D),$$

where $S = \sqrt{2N + \sqrt{(N^2+1)^2 - \varphi_4(N)}}$ and $D = \sqrt{S^2 - 4N}$.

Proof. We will rewrite $\varphi_4(N)$ as

$$\begin{aligned} \varphi_4(N) &= N^4 - p^4 - 4p^3q - 6p^2q^2 - 4pq^3 - q^4 + 1 + 4p^3q + 6p^2q^2 + 4pq^3 \\ &= N^4 - (p+q)^4 + 4N(p^2 + 2pq + q^2) - 2p^2q^2 + 1 \\ &= N^4 - (p+q)^4 + 4N(p+q)^2 - 2N^2 + 1 \end{aligned}$$

which is equivalent to

$$(p+q)^4 - 4N(p+q)^2 + \varphi_4(N) - (N^2-1)^2 = 0.$$

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

$$x^4 - 4Nx^2 + \varphi_4(N) - (N^2 - 1)^2 = 0 \Leftrightarrow$$
$$(x^2)^2 - 4N(x^2) + \varphi_4(N) - (N^2 - 1)^2 = 0.$$

The previous equation can be solved as a normal quadratic equation. Computing the discriminant Δ, we have that

$$\Delta = 4(N^2 + 1)^2 - 4\varphi_4(N) > 0.$$

Thus, the roots of the quadratic equation, $x'_{1,2}$, are

$$x'_{1,2} = 2N \pm \sqrt{(N^2 + 1)^2 - \varphi_4(N)}.$$

The roots of the biquadratic equation are the square roots of the previous quantities.

$$x_{1,2} = \pm\sqrt{2N + \sqrt{(N^2 + 1)^2 - \varphi_4(N)}}$$
$$x_{3,4} = \pm\sqrt{2N - \sqrt{(N^2 + 1)^2 - \varphi_4(N)}}$$

The roots $x_{3,4}$ are pure imaginary since

$$\begin{aligned} \sqrt{(N^2 + 1)^2 - \varphi_4(N)} &> 2N \Leftrightarrow \\ (N^2 + 1)^2 - \varphi_4(N) &> 4N^2 \Leftrightarrow \\ N^4 + 2N^2 + 1 - N^4 + p^4 + q^4 - 1 - 4N^2 &> 0 \Leftrightarrow \\ (p^2 - q^2)^2 &> 0. \end{aligned}$$

The root $x_2 = -\sqrt{2N + \sqrt{(N^2 + 1)^2 - \varphi_4(N)}} < 0$, thus we get $S' = S = x_1 = \sqrt{2N + \sqrt{(N^2 + 1)^2 - \varphi_4(N)}}$. The values of p and q can be recovered by using the algorithm from Lemma 2. $\square$

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

$$\begin{aligned} N &= 30149726335030403365902265083163510227689133239 33, \\ e &= 388664907815721751254078126828021336031997013314 5 \\ &\quad 6396788273204320283738850302214441484301356047280 \\ &\quad 9980074678226938065582620857819830171139174634897 \\ &\quad 6973105501097738003951257510630159060039123284 7. \end{aligned}$$

Note that $e \approx N^{3.993}$. Applying the continued fraction expansion of $e/\varphi_{4,0}(N)$, we get the first 25 partial quotients

$$[0, 2, 7, 1, 15, 6, 1, 2, 4, 1, 1, 2, 1, 1, 3, 1, 1, 1, 2, 38, 1, 2, 1, 45, 8, \ldots].$$

In this case, we consider the convergents of $e/\varphi_{4,0}(N)$, and we select only those for which $\varphi_4 = (ed-1)/k$ is an integer and the following system of equations

$$\begin{cases}\varphi_4 = (p^4-1)(q^4-1)\\ N = pq\end{cases}$$

has a solution as given in Lemma 4. The $2nd$ and $23rd$ convergents satisfy the first condition, however only the last one leads to a valid solution for p and q. More precisely, the $23rd$ convergent leads to

$$\begin{aligned}\varphi_4 &= 8262919045403735048878111025050137547018067986718\\ &\quad\;\, 6489272861711603139280409749776405912009959512474\\ &\quad\;\, 1225965967573968605037596274853618481302754457480\\ &\quad\;\, 6787891184267004832506535094151626645227104000 0,\\ \frac{k}{d} &= \frac{799532980}{1699787183},\\ p &= 2119778199036859068707819,\\ q &= 1422305708622213956806807.\end{aligned}$$

7 Conclusions

In this paper we introduced a family of RSA-like cryptosystems, which includes the RSA and Elkamchouchi *et al.* public key encryption schemes [15,29] (*i.e.* $n=1$ and $n=2$). 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 and the secret exponent is smaller that $N^{0.25n}$.

Future Work. When $n = 1,2,3,4$, in Sect. 6 and [4,7,10] a method for factoring N once φ_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 Sect. 1 for the RSA and Elkamchouchi *et al.* 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: Boyd, C., Simpson, L. (eds.) ACISP 2013. LNCS, vol. 7959, pp. 88–103. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-39059-3_7
2. Blömer, J., May, A.: New partial key exposure attacks on RSA. In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol. 2729, pp. 27–43. Springer, Heidelberg (2003). https://doi.org/10.1007/978-3-540-45146-4_2

3. Blömer, J., May, A.: A generalized wiener attack on RSA. In: Bao, F., Deng, R., Zhou, J. (eds.) PKC 2004. LNCS, vol. 2947, pp. 1–13. Springer, Heidelberg (2004). https://doi.org/10.1007/978-3-540-24632-9_1
4. Boneh, D.: Twenty years of attacks on the RSA cryptosystem. Notices AMS **46**(2), 203–213 (1999)
5. Boneh, D., Durfee, G.: Cryptanalysis of RSA with private key d less than $N_{0.292}$. In: Stern, J. (ed.) EUROCRYPT 1999. LNCS, vol. 1592, pp. 1–11. Springer, Heidelberg (1999). https://doi.org/10.1007/3-540-48910-X_1
6. Boneh, D., Durfee, G., Frankel, Y.: An attack on RSA given a small fraction of the private key bits. In: Ohta, K., Pei, D. (eds.) ASIACRYPT 1998. LNCS, vol. 1514, pp. 25–34. Springer, Heidelberg (1998). https://doi.org/10.1007/3-540-49649-1_3
7. Bunder, M., Nitaj, A., Susilo, W., Tonien, J.: A new attack on three variants of the RSA cryptosystem. In: Liu, J.K., Steinfeld, R. (eds.) ACISP 2016. LNCS, vol. 9723, pp. 258–268. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-40367-0_16
8. Bunder, M., Nitaj, A., Susilo, W., Tonien, J.: A generalized attack on RSA type cryptosystems. Theor. Comput. Sci. **704**, 74–81 (2017)
9. Bunder, M., Nitaj, A., Susilo, W., Tonien, J.: Cryptanalysis of RSA-type cryptosystems based on Lucas sequences, Gaussian integers and elliptic curves. J. Inf. Secur. Appl. **40**, 193–198 (2018)
10. Bunder, M., Tonien, J.: A new attack on the RSA cryptosystem based on continued fractions. Malays. J. Math. Sci. **11**, 45–57 (2017)
11. Cherkaoui-Semmouni, M., Nitaj, A., Susilo, W., Tonien, J.: Cryptanalysis of RSA variants with primes sharing most significant bits. In: Liu, J.K., Katsikas, S., Meng, W., Susilo, W., Intan, R. (eds.) ISC 2021. LNCS, vol. 13118, pp. 42–53. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-91356-4_3
12. Coppersmith, D.: Small solutions to polynomial equations, and low exponent RSA vulnerabilities. J. Cryptol. **10**(4), 233–260 (1997)
13. Cotan, P., Teşeleanu, G.: Continued fractions applied to a family of RSA-like cryptosystems. In: Su, C., Gritzalis, D., Piuri, V. (eds.) Information Security Practice and Experience. ISPEC 2022. LNCS, vol. 13620, pp. 589–605. Springer, Cham (2022). https://doi.org/10.1007/978-3-031-21280-2_33
14. De Weger, B.: Cryptanalysis of RSA with small prime difference. Appl. Algebra Eng. Commun. Comput. **13**(1), 17–28 (2002)
15. Elkamchouchi, H., Elshenawy, K., Shaban, H.: Extended RSA cryptosystem and digital signature schemes in the domain of Gaussian integers. In: ICCS 2002, vol. 1, pp. 91–95. IEEE Computer Society (2002)
16. Ernst, M., Jochemsz, E., May, A., de Weger, B.: Partial key exposure attacks on RSA up to full size exponents. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 371–386. Springer, Heidelberg (2005). https://doi.org/10.1007/11426639_22
17. Fujii, K.: A Modern Introduction to Cardano and Ferrari Formulas in the Algebraic Equations. arXiv Preprint arXiv:quant-ph/0311102 (2003)
18. Hardy, G.H., Wright, E.M., et al.: An Introduction to the Theory of Numbers. Oxford University Press, Oxford (1979)
19. Herrmann, M., May, A.: Maximizing small root bounds by linearization and applications to small secret exponent RSA. In: Nguyen, P.Q., Pointcheval, D. (eds.) PKC 2010. LNCS, vol. 6056, pp. 53–69. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-13013-7_4

20. Howgrave-Graham, N., Seifert, J.-P.: Extending wiener's attack in the presence of many decrypting exponents. In: CQRE 1999. LNCS, vol. 1740, pp. 153–166. Springer, Heidelberg (1999). https://doi.org/10.1007/3-540-46701-7_14
21. 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)
22. Maitra, S., Sarkar, S.: Revisiting wiener's attack – new weak keys in RSA. In: Wu, T.-C., Lei, C.-L., Rijmen, V., Lee, D.-T. (eds.) ISC 2008. LNCS, vol. 5222, pp. 228–243. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-85886-7_16
23. Maitra, S., Sarkar, S.: Revisiting Wiener's Attack - New Weak Keys in RSA. IACR Cryptology ePrint Archive 2008/228 (2008)
24. Murru, N., Saettone, F.M.: A novel RSA-like cryptosystem based on a generalization of the Rédei rational functions. In: Kaczorowski, J., Pieprzyk, J., Pomykała, J. (eds.) NuTMiC 2017. LNCS, vol. 10737, pp. 91–103. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-76620-1_6
25. 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)
26. Nitaj, A.: Another generalization of wiener's attack on RSA. In: Vaudenay, S. (ed.) AFRICACRYPT 2008. LNCS, vol. 5023, pp. 174–190. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-68164-9_12
27. Nitaj, A., Pan, Y., Tonien, J.: A generalized attack on some variants of the RSA cryptosystem. In: Cid, C., Jacobson Jr., M. (eds.) Selected Areas in Cryptography – SAC 2018. SAC 2018. LNCS, vol. 11349, pp. 421–433. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-10970-7_19
28. Peng, L., Hu, L., Lu, Y., Wei, H.: An improved analysis on three variants of the RSA cryptosystem. In: Chen, K., Lin, D., Yung, M. (eds.) Inscrypt 2016. LNCS, vol. 10143, pp. 140–149. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-54705-3_9
29. Rivest, R.L., Shamir, A., Adleman, L.: A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM **21**(2), 120–126 (1978)
30. Sarkar, S., Maitra, S.: Cryptanalysis of RSA with more than one decryption exponent. Inf. Process. Lett. **110**(8–9), 336–340 (2010)
31. Takayasu, A., Kunihiro, N.: Cryptanalysis of RSA with multiple small secret exponents. In: Susilo, W., Mu, Y. (eds.) ACISP 2014. LNCS, vol. 8544, pp. 176–191. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-08344-5_12
32. Takayasu, A., Kunihiro, N.: Partial key exposure attacks on RSA: achieving the Boneh-Durfee bound. In: Joux, A., Youssef, A. (eds.) SAC 2014. LNCS, vol. 8781, pp. 345–362. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-13051-4_21
33. Wiener, M.J.: Cryptanalysis of short RSA secret exponents. IEEE Trans. Inf. Theory **36**(3), 553–558 (1990)
34. Zheng, M., Kunihiro, N., Hu, H.: Cryptanalysis of RSA variants with modified Euler quotient. In: Joux, A., Nitaj, A., Rachidi, T. (eds.) AFRICACRYPT 2018. LNCS, vol. 10831, pp. 266–281. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-89339-6_15