A Security Analysis of Two Classes 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. In 2002, Elkamchouchi, Elshenawy and Shaban introduced an RSA-like cryptosystem that uses the key equation $ed - k(p^2-1)(q^2-1) = 1$, instead of the classical RSA key equation $ed - k(p-1)(q-1) = 1$. Another variant of RSA, presented in 2017 by Murru and Saettone, uses the key equation $ed - k(p^2+p+1)(q^2+q+1) = 1$. Despite the authors' claims of enhanced security, both schemes remain vulnerable to adaptations of common RSA attacks. Let n be an integer. This paper proposes two families of RSA-like encryption schemes: one employs the key equation $ed - k(p^n-1)(q^n-1) = 1$ for $n > 0$, while the other uses $ed - k[(p^n-1)(q^n-1)]/[(p-1)(q-1)] = 1$ for $n > 1$. Note that we remove the conventional assumption of primes having equal bit sizes. In this scenario, we show that regardless of the choice of n, continued fraction-based attacks can still recover the secret exponent. Additionally, this work fills a gap in the literature by establishing an equivalent of Wiener's attack when the primes do not have the same bit size.

1 Introduction

In 1978, Rivest, Shamir and Adleman [45] 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 $q < p < 2q$.

A frequently used method for speeding up decryption is to first compute $m_p \equiv c^{d_p} \bmod p$ and $m_q \equiv c^{d_q} \bmod q$, where $d_p \equiv d \bmod p-1$ and $d_q \equiv d \bmod q-1$. Then using the Chinese Remainder Theorem (CRT), we can recover m from m_p and m_q. In [47], Shamir remarked that if $m < q$ then it suffices to compute m_q, since $m = m_q$. Asymmetric encryption schemes are usually used to encapsulate

keys for symmetric schemes, and thus the restriction holds for most practical cases. To further speed up the process, Shamir proposed a variant of RSA, called the unbalanced RSA, where the bit size of q is much more smaller than that of p. As long as q and N are large enough to prevent factorisation via the Elliptic Curve Method (ECM) and the Number Field Sieve (NFS), the unbalanced RSA is secure.

In 2002, Elkamchouchi, Elshenawy and Shaban [20] 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 $i^2 = -1$. We denote the set of all Gaussian integers modulo N by $\mathbb{Z}_N[i]$ and the totient function of N by $\phi(N) = |\mathbb{Z}_N^*[i]| = (p^2 - 1)(q^2 - 1)$. To set up the public exponent, we require $\gcd(e, \phi(N)) = 1$. The corresponding private exponent computed as $d \equiv e^{-1} \bmod \phi(N)$. Encryption of a message $m \in \mathbb{Z}_N[i]$ is obtained by computing $c \equiv m^e \bmod N$ and decryption by $m \equiv c^d \bmod N$. Note that the exponentiations are computed in the ring $\mathbb{Z}_N[i]$.

In 2017, Murru and Saettone introduced an RSA-like cryptosystem [36] that involves a special type of group composed of equivalence classes of polynomials from the $GF(p^3) \times GF(q^3)$, where GF stands for Galois field. Unlike the classical RSA scheme, they select the public exponent e such that $\gcd(e, \psi(N)) = 1$, where $\psi(N) = (p^2 + p + 1)(q^2 + q + 1)$. The decryption exponent is then computed as $d \equiv e^{-1} \pmod{\psi(N)}$. Encryption and decryption follow a process similar to classical RSA, except that they employ this specific group instead of $\mathbb{Z}_N^*$.

The authors of both papers [20, 36] claim that their extension offer more security compared to the classical RSA. However, as elaborated in the following paragraphs, these assertions prove to be inaccurate. It is important to clarify that throughout the ensuing discussion, RSA refers to the classical RSA scheme.

Small Private Key Attacks. In order to decrease decryption time, one may prefer to use a smaller d. Wiener showed in [54] 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 [15], Boneh and Durfee [7] improved Wiener's bound to $N^{0.292}$. Later on, Herrmann and May [26] obtain the same bound, but using simpler techniques. A different approach was taken by Blömer and May [5], 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 [38] present a method based on continued fractions for recovering d when $d < N^{(1-\delta)/2}$.

In the case of Elkamchouchi *et al.*'s scheme, a series of small private key attacks have been developed. Initially presented in [10], the attack made use of continued fractions. Subsequent improvements utilizing lattice reduction techniques were made in [44, 55], refining the attack's efficiency and leading to a bound of $d < N^{0.585}$. A generalization of the attack presented in [10] to unbalanced prime numbers was presented in [12]. Considering the generic equation $ex - y\phi(N) = z$, the authors of [11] described 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 [42].

As for the Murru-Saettone scheme, it was shown in [40, 50] that a Wiener-type attack remains effective. Utilizing continued fractions, the authors showed that when $d < N^{0.25}$, it is possible to factor N. Building upon the Boneh-Durfee method, Nitaj *et al.* [40] improved the bound to $N^{0.5694}$. Further advancements were made by Zheng, Kunihiro, and Yao in [56], achieving a tighter bound of $d < N^{0.585}$. Moreover, Nassr, Anwar, and Bahig [37] demonstrated a technique to recover d when p_0 satisfies $|p - p_0| < N^{\delta}$ and $d < N^{(1-\delta)/2}$, where $\delta < 0.5$.

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 [27] 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 [46], Aono [2] and Takayasu and Kunihiro [51]. The best known bound [51] 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 [55]. They derived a bound of $\beta < 2 - 2\sqrt{2/(3\ell+1)}$, which is twice the bound obtained by Takayasu and Kunihiro [51]. Note that, when $\ell = 1$, the bound equals 0.585.

Similarly, Shi, Wang and Gu [48] studied the multiple private keys attack against the Murru-Saettone cryptosystem. They obtained a bound of $\beta < 3/2 - 4/(3\ell+1)$, which is twice the bound derived by Aono [2]. It is worth noting that when $\ell = 1$, the bound is less than 0.585, suggesting the possibility of tighter bounds.

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 [8]. The attack was later improved by Blömer and May [4], Ernst *et al.* [21] and Takayasu and Kunihiro [52]. The best known bound [52] is $\beta < (\gamma + 2 - \sqrt{2 - 3\gamma^2})/2$, where the attacker knows N^{γ} leaked bits.

Zheng, Kunihiro and Hu [55] and Shi, Wang and Gu [48] describe a partial exposure attack that works in the case of the Elkamchouchi *et al.* scheme and 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 [18] 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 [34, 35] 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.* [30].

The small prime difference attack against the Elkamchouchi *et al.* public key encryption scheme was studied in [14]. Note that when the common condition $|p-q| < N^{0.5}$ holds, their bound leads to the small private key bound $d < N^{0.585}$.

The de Weger attack was adapted to the Murru-Saetonne public key encryption scheme by Nitaj *et al.* [41], Nassr, Anwar and Bahig [37] and Shi, Wang and Gu [48]. The best bounds for the continued fraction and lattice reduction methods are found in [41]. The Maitra-Sakar extension was studied only in [37].

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 reinterpret the RSA scheme as working in the $GF(p)\times GF(q)$ group instead of $\mathbb{Z}_N$. Additionally, the Elkamchouchi *et al.* scheme is an extension to $GF(p^2) \times GF(q^2)$ instead of $Z_N[i]$. This naturally leads to a generalization of RSA to $GF(p^n) \times GF(q^n)$, where $n \geq 1$. In this paper we introduce exactly this extension. Moreover, 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 $n = 1$ and $n = 2$ (RSA and Elkamchouchi *et al.*) or $n = 3$ (Murru-Saetonne) the common attacks presented in the introduction work or this is something that happens in general. In this study we present several Wiener-type attacks that work for any n. More precisely, we prove that for any $p > q$, when $d < N^{0.25n} \cdot (q/p)^{0.5n} \cdot 2^{-0.5n}$ or $d < N^{0.25} \cdot (q/p)^{0.25(n-1)}$, respectively we can recover the secret exponent. Therefore, no matter how we instantiate the generalized version, a small private key attack will always succeed. In the case of the first family[3], we construct a probabilistic factorization algorithm once the group order is determined. For completeness, we also generalized Wiener's attack to unbalanced prime numbers.

Previous work. The generalizations of Elkamchouchi *et al.* and Murru-Saetonne encryption schemes, along with their corresponding attacks, were initially presented in [17] and [16], respectively. It is important to note that these versions specifically addressed the case of balanced prime numbers and did not consider the unbalanced scenario.

Structure of the Paper. We introduce in Section 2 notations and definitions used throughout the paper. The necessary group theory is developed in Section 3. Inspired by Rivest *et al.*, Elkamchouchi *et al.* and Murru and Saettone's work [20, 36, 45], in Section 4 we construct two families of RSA-like cryptosystems. After proving several useful lemmas in Sections 5.1 and 6.1, we extend Wiener's small private key attack in Sections 5.2 and 6.2. Discussions and conclusions are presented in Sections 7 and 8. Concrete instantiations of our classes of attacks are provided in Appendices A and B. For completeness, in Appendix C we generalize Wiener's attack to the unbalanced RSA case, while in Appendix D we provide a concrete example.

[3] that generalizes the RSA and Elkamchouchi *et al.* schemes

2 Preliminaries

Notations. Throughout the paper, λ denotes a security parameter. The notation $|S|$ denotes the cardinality of a set S. When n is an integer, $|n|$ denotes the size of n in bits. The set of integers $\{0, \ldots, a\}$ is further denoted by $[0, a]$. We use $\simeq$ to indicate that two values are approximately equal.

The Jacobi symbol of an integer a modulo an integer N is represented by $J_N(a)$. J_N^+ and J_N^- denote the sets of integers modulo n with Jacobi symbol 1, respectively -1. Throughout the paper, we let QR_N be the set of quadratic residues modulo N.

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 [25], 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 Parameter Selection

In an unbalanced RSA-type encryption scheme, in order to decrease decryption time we lower the bit size of q (denoted by λ_q) while preserving the bit size of N (denoted by λ_N). Therefore, we have $\lambda_N = \lambda_p + \lambda_q$, where $\lambda_p = |p|$ and $\lambda_q \leq \lambda_p$. Remark that when $\lambda_p = \lambda_q$ we obtain the balanced RSA-type encryption schemes.

The fastest currently known method for factoring composite numbers is the NFS algorithm [33]. The expected running time of the NFS depends on the size

of the modulus N and not on the size of its factors. More precisely, the expected running time is approximately

$$L[N] = e^{1.923(\log N)^{1/3}(\log\log N)^{2/3}}.$$

In [32, 33], the authors use the computational effort needed to factor a 512-bit modulus to extrapolate the running time required to factor a modulus of size λ_N. Therefore, a λ_N-bit modulus offers a security equivalent to a block cipher of d-bit security if

$$L[2^{\lambda_N}] \simeq 50 \cdot 2^{d-56} \cdot L[2^{512}]. \tag{1}$$

Therefore, if we select a modulus size that offers protection against the NFS, decreasing the size of one of the factors does not increase the success probability of factoring N using the NFS. Unfortunately, lowering the bit size of q below a certain threshold can make the resulting encryption scheme vulnerable to the ECM algorithm [29]. Compared to the NFS, the ECM has the running time determined by the size of the smallest factor. More precisely, the running time of the ECM is

$$E[N, q] = (\log_2 N)^2 e^{\sqrt{2\log q \log\log q}}.$$

Similarly to the NFS, Lenstra [31] extrapolates that the equivalent security is

$$E[2^{\lambda_N}, 2^{\lambda_q}] \geq 80 \cdot 2^{d-56} \cdot E[2^{768}, 2^{167}]. \tag{2}$$

Using Equations (1) and (2) we can compute the following relation

$$E[2^{\lambda_N}, 2^{\lambda_q}] \geq 80 \cdot 2^{\log_2(L[2^{\lambda_N}]/(50 \cdot L[2^{512}]))} \cdot E[2^{768}, 2^{167}]. \tag{3}$$

Using known historical factoring records, Brent develops a different model [9] to predict the security against the NFS and the ECM. More specifically, Brent provides an equation[4] that links the number of digits D_N and D_q of the modulus and, respectively, the smallest prime factor to the year Y when is possible to factor the modulus using the NFS or the ECM. We further provide the updated equations [53] for the NFS

$$D_N^{1/3} = \frac{Y - 1926}{13.97} \text{ or equivalently } Y = 13.97 \cdot D_N^{1/3} + 1926 \tag{4}$$

and for the ECM

$$D_q^{1/2} = \frac{Y - 1939}{8.207} \text{ or equivalently } Y = 8.207 \cdot D_q^{1/2} + 1939. \tag{5}$$

Using Equations (4) and (5) we obtain the following relation

$$D_q^{1/2} = \frac{13.97 \cdot D_N^{1/3} - 13}{8.207}. \tag{6}$$

[4] derived using the least-squares fit

According to NIST [3], if we choose $\lambda_N = 3072/7680/15360$ we can guarantee protection against the NFS at least until 2030. We chose to use NIST's key lengths since the ones provided in [32,33] are criticized as being too conservative [49]. Another argument for using the key sizes suggested by NIST is that these are the ones used by the industry. Therefore, using NIST's recommendations, and Equations (3) and (6) we can compute the size of the smallest prime that offers the same level of protection against the ECM. The results are presented in Table 1.

Modulus key size	3072	7680	15360
Lenstra model	800	1617	2761
Regression model	749	1457	2385

Table 1. The equivalent sizes of the smallest prime number

The following lemma provides some useful bounds for the larges prime factor.

Lemma 1. *Let p, q be two primes such that $|p| = \lambda_p$ and $|q| = \lambda_q$. If $\lambda_p = \lambda_q + \lambda$, then*

$$2^{\lambda-1}q < p < 2^{\lambda}q \quad \text{or} \quad 2^{\lambda}q < p < 2^{\lambda+1}q.$$

Proof. According to the statement we have the following inequalities

$$2^{\lambda_p} < p < 2^{\lambda_p+1} \quad \text{and} \quad 2^{\lambda_q} < q < 2^{\lambda_q+1}.$$

From the previous relations, we obtain the following

$$p < 2^{\lambda_p+1} = 2^{\lambda_q} \cdot 2^{\lambda+1} < q \cdot 2^{\lambda+1}$$
$$p > 2^{\lambda_p} = 2^{\lambda_q+1} \cdot 2^{\lambda-1} > q \cdot 2^{\lambda-1},$$

as desired. □

Note that when $\lambda_p = \lambda_q$, according to Lemma 1 we obtain that $q < p < 2q$. To be consistent with the balanced case, we further assume, without loss of generality, that $\mu q < p < 2\mu q$. According to Lemma 1 we have either $\mu = 2^{\lambda-1}$ or $\mu = 2^{\lambda}$.

3 Useful Quotient Groups

In the first part of this section we will provide the mathematical theory needed to generalize 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

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

In order to generalize the Murru and Saettone encryption scheme, 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 $[a_0 + \ldots + a_{n-1}t^{n-1}] \in \mathbb{B}_n$.

Using Lagrange's theorem [23], we obtain the following result about the cardinality of $\mathbb{B}_n$.

Lemma 2. *The cardinality of* $\mathbb{B}_n$ *is* $\psi_n(\mathbb{F}) = (|\mathbb{F}|^n - 1)/(|\mathbb{F}| - 1)$.

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

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

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

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

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

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

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

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

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

4 RSA-like Unbalanced Encryption Schemes

4.1 Generalized Elkamchouchi *et al.* Unbalanced 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 $\varphi_n(\mathbb{Z}_p) = \varphi_n(p) = p^n - 1$. Remark that an analogous of Fermat's little theorem holds

$$a(t)^{\varphi_n(p)} \equiv 1,$$

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

Setup(λ_p, λ_q): Let $n > 1$ be an integer. Randomly generate two distinct large prime numbers p, q such that $|p| = \lambda_p$, $|q| = \lambda_q$ 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 $c(t) \equiv m(t)^e$. Output the ciphertext $c(t)$.

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

Remark 1. When $n = 1$ we get the RSA scheme [45]. Also, when $n = 2$ and $\lambda_p = \lambda_q$, we obtain the Elkamchouchi *et al.* cryptosystem [20].

Remark 2. When $m_1 = m_2 = \ldots = m_{n-1} = 0$, encryption is reduced to $c(t) = m_0^e \bmod N$. Therefore, everything is computed in $\mathbb{Z}_N$, as in the classical RSA scheme, due to all other message components being zero.

4.2 Generalized Murru and Saettone Unbalanced Scheme

In this case, we use the group $\mathbb{B}_n$ instead of $\mathbb{A}_n$. Therefore, when we instantiate $\mathbb{F} = \mathbb{Z}_p$, we obtain that $\mathbb{B}_n$ is a cyclic group of order $\psi_n(\mathbb{Z}_p) = \psi_n(p) = (p^n - 1)/(p - 1)$. Note that an analogue of Fermat's little theorem also exists in this case, namely

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

where $[a(t)] \in \mathbb{B}_n$ and the power is evaluated by $\odot$-multiplying $[a(t)]$ by itself $\psi_n(p) - 1$ times. Hence, we can build an encryption scheme that is similar to

RSA using the $\odot$ as the product. Note that the equivalence class of $[0]$ contains all the polynomials that are either divisible by $t^n - r$ or have all their coefficient divisible by p.

Setup(λ_p, λ_q): Let $n > 1$ be an integer. Randomly generate two distinct large prime numbers p, q such that $|p| = \lambda_p$, $|q| = \lambda_q$ and compute their product $N = pq$. Select r such that the polynomial $t^n - r$ is irreducible in $\mathbb{Z}_N[t]$. 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 $c(t) \equiv [m(t)]^e$. Output the ciphertext $c(t)$.

Decrypt$(sk, c(t))$: To recover the message, simply compute $m(t) \equiv [c(t)]^d$ and reassemble $m = (m_0, \ldots, m_{n-2})$.

Remark 3. When $\lambda_p = \lambda_q$ and $n = 3$, we obtain the Murru and Saettone cryptosystem [36].

Remark 4. The group $\mathbb{B}_n$ has been used to define ElGamal-based cryptosystems as well. For more details, we refer the reader to [1] and [19] for the cases $n = 2$ and $n = 3$, respectively.

4.3 Optimisations

In this section, we present a possible optimisation for the generalized Murru and Saettone scheme. We focus solely on this family, as the underlying group is more intricate. A similar optimisation is also feasible for the generalized Elkamchouchi *et al.* scheme. The main differences lie in changing the equivalence classes, and we work with φ_n instead of ψ_n.

Therefore, to efficiently decrypt the message we first have to compute $m_p(t) \equiv [c(t)]^{d_p} \bmod p$ and $m_q(t) \equiv [c(t)]^{d_q} \bmod q$, where $d_p \equiv d \bmod \psi_n(p)$ and $d_q \equiv d \bmod \psi_n(q)$. Then we can use the CRT to recover m from m_p and m_q. If $m \in \mathbb{Z}_N^{n-1}$, then this procedure makes sense only when $\lambda_p = \lambda_q$. In the practical case of key wrapping, we have that the coefficients of $m(t)$ are strictly smaller than q (*i.e* $m_i \in [0, 2^{\lambda_k}]$, where $\lambda_k < \lambda_q$), and thus is sufficient only to compute $m_q(t) \equiv [c(t)]^{d_q} \bmod q$. Also, in this case, using the equivalent sizes of q provided in Table 1, we obtain a significant speed up for decryption compared to the balanced case.

Note that we must always set parameter λ_k in the *Setup* phase and make it public. Also, in the *Decrypt* phase, after recovering m we must always check that for all i we have $m_i \in [0, 2^{\lambda_k}]$. If this is not true, then we must discard the

message. In the following paragraphs we will provide the technical details for setting these restrictions.

If we do not check whether $m_i \in [0, 2^{\lambda_k}]$, then the following chosen ciphertext attack is possible. The attacker chooses a message m' such that $m'_i > q$ and he encrypts it. Let $c'(t)$ denote the corresponding ciphertext. When the recipient decrypts $c'(t)$ obtains $[m(t)] \equiv [m'(t)] \bmod q$. Once the attacker has access[5] to $m(t)$ then he computes $\gcd(m'_0 - m_0, N)$ and obtains the factorisation of N. To check that he truly obtains q, we observe that $[m(t)] \equiv [m'(t)] \bmod q$ leads to $[m(t) - m'(t)] \equiv 0 \bmod q$. Then either $t^n - r | m(t) - m'(t)$ or $q | m_i - m'_i$ for all i. Since both messages have degree less than n, we have that $q | m_i - m'_i$ for all i. Therefore, we obtain

$$\gcd(m'_0 - m_0, N) = \gcd(aq, pq) = q,$$

as desired.

If we only check internally that $m_i < q$ then the attacker can probe[6] the recipient and reveal q. In order to do that he sets $m_i = 0$ for $i > 0$ and sets m_0 randomly. If the message is discarded then the attacker knows that $q < m_0$, otherwise $m_0 < q$. Once the attacker knows a lower and an upper bound of q he can do a binary search and locate q.

Remark 5. Attacks similar to those presented above are described in [24] for the unbalanced RSA and in [28] for the Okamoto-Uchiyama scheme.

5 Attacking the Generalized Elkamchouchi *et al.* Unbalanced Scheme

5.1 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 $\sqrt{N} \leq x < N$, we have that the function*

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

is strictly decreasing with x.

[5] *e.g.* the attacker has access to the recipient's recycle bin or the message is simply returned to the attacker by the recipient since it is meaningless

[6] *e.g.* if the scheme is used for session key exchange, the attacker simply checks if the session is successful or not

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 $x \geq \sqrt{N}$ 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 lemma, we will compute a lower and upper bound for $\varphi_n(N)$.

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

$$\sqrt{\mu N} < p < \sqrt{2\mu N} \quad \text{and} \quad \frac{\sqrt{2N\mu}}{2\mu} < q < \frac{\sqrt{N\mu}}{\mu}.$$

Proof. Multiplying $\mu q < p < 2\mu q$ with p we obtain $\mu N < p^2 < 2\mu N$. This is equivalent with $\sqrt{\mu N} < p < \sqrt{2\mu N}$. Since $q = N/p$, the previous relation becomes $\sqrt{N}/\sqrt{2\mu} < q < \sqrt{N}/\sqrt{\mu}$, and thus we conclude our proof. □

When $\mu = 1$, the following result proven in [39] becomes a special case of Lemma 3.

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

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

Proof. By Lemma 3 we have that

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

which, according to Proposition 1, leads to

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

This is equivalent to our desired inequality. □

For $\mu = 1$, when $n = 1$ and $n = 2$, the following results proven in [13] and [10], respectively become special cases of Corollary 2.

Corollary 3. *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 4. *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 2 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 $\mu q < p < 2\mu q$. We define*

$$\begin{aligned}\varphi_{n,0}(N) = &\frac{1}{2} \cdot \left(N^n - (\sqrt{\mu N})^n - \left(\frac{\sqrt{\mu N}}{\mu} \right)^n + 1 \right) \\ &+ \frac{1}{2} \cdot \left(N^n - (\sqrt{2\mu N})^n - \left(\frac{\sqrt{2\mu N}}{2\mu} \right)^n + 1 \right).\end{aligned}$$

Then the following holds

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

where

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

Proof. According to Corollary 2, $\varphi_{n,0}(N)$ is the mean value of the lower and upper bound. The following property holds

$$\begin{aligned}|\varphi_n(N) - \varphi_{n,0}(N)| \leq &\frac{1}{2} \left(N^n - (\sqrt{\mu N})^n - \left(\frac{\sqrt{\mu N}}{\mu} \right)^n + 1 \right. \\ &\left. - N^n + (\sqrt{2\mu N})^n + \left(\frac{\sqrt{2\mu N}}{2\mu} \right)^n - 1 \right) \\ = &\frac{1}{2}\sqrt{N}^n \left(-\sqrt{\mu}^n - \frac{1}{\sqrt{\mu}^n} + \sqrt{2\mu}^n + \frac{1}{\sqrt{2\mu}^n} \right) \\ = &\frac{\Delta_n^E}{2}\sqrt{N}^n,\end{aligned}$$

as desired. □

For $\mu = 1$, when $n = 1$ and $n = 2$, the following properties presented in [13] and [10], respectively become special cases of Proposition 2.

Corollary 5. *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 6. *Let $N = pq$ be the product of two unknown primes with $q < p < 2q$. Then the following holds*

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

5.2 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 $\mu q < p < 2\mu q$. If $e < \varphi_n(N)$ satisfies $ed - k\varphi_n(N) = 1$ with*

$$d < \sqrt{\frac{N^n(\sqrt{N}^n - \delta_n^E)}{e\Delta_n^E}}, \tag{7}$$

where

$$\delta_n^E = \frac{4\sqrt{2\mu}^n}{\mu^n(2^n - \sqrt{2}^n) - \sqrt{2}^n + 1} + \frac{2[(2\mu)^n + 1]}{\sqrt{2\mu}^n}$$

then we can recover d in polynomial time.

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

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

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

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

Note that

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

which leads to

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

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.

□

In the case of unbalanced RSA (*i.e.* $n = 1$), when e is large enough, Theorem 2 is simplified into the following corollary. We achieve a tighter bound in Appendix C, where we directly generalized Wiener's attack [6, 54].

Corollary 7. *Let $N = pq$ be the product of two unknown primes with $\mu q < p < 2\mu q$. If we approximate $e \simeq N^n$ then Theorem 2 is equivalent to*

$$d < \frac{(\mu N)^{0.25}}{\sqrt{\mu(\sqrt{2}-1)-1}}.$$

Corollary 8. *Let $\alpha < 1.5n$ and $N = pq$ be the product of two unknown primes with $\mu q < p < 2\mu q$. If we approximate $e \simeq N^{\alpha}$, $N \simeq 2^{\lambda_N}$ and $\mu \simeq 2^{\lambda}$, then Equation (7) becomes*

$$d < \frac{2^{0.5(n-\alpha)\lambda_N}\sqrt{2^{0.5n\lambda_N} - \delta_n^E}}{\sqrt{\Delta_n^E}} < \frac{2^{0.5(1.5n-\alpha)\lambda_N}}{\sqrt{\Delta_n^E}}$$

or equivalently

$$\log_2(d) < 0.5(1.5n - \alpha)\lambda_N - \log_2(\sqrt{\Delta_n^E}) \simeq 0.5(1.5n - \alpha)\lambda_N - 0.5n(\lambda + 1).$$

Proof. From the definition of Δ_n^E we obtain that

$$\Delta_n^E = \frac{\mu^n(2^n - \sqrt{2}^n) - \sqrt{2}^n + 1}{\sqrt{2\mu}^n} \simeq \frac{2^{n\lambda}(2^n - \sqrt{2}^n) - \sqrt{2}^n + 1}{2^{n(\lambda+1)/2}} \simeq 2^{n(\lambda+1)/2},$$

as desired. □

When $\mu = 1$, the following properties presented in [13] ($n = 1$) and those in [10] ($n = 2$) become special cases of Corollary 8. Note that when $n = \alpha = 1$ we obtain roughly the same margin as Wiener [6, 54] obtained for the classical RSA.

Corollary 9. *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 $N \simeq 2^{\lambda_N}$ then Equation (7) is equivalent to*

$$\log_2(d) < 0.5(1.5 - \alpha)\lambda_N - 0.25 + 1.27 \simeq 0.5(1.5 - \alpha)\lambda_N.$$

Corollary 10. *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 $N \simeq 2^{\lambda_N}$ then Equation (7) is equivalent to*

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

Corollary 11. *Let $N = pq$ be the product of two unknown primes with $\mu q < p < 2\mu q$. If we approximate $e \simeq N^{n}$ and $N \simeq 2^{\lambda_N}$ then Equation (7) is equivalent to*

$$\log_2(d) < 0.25n\lambda_N - \log_2(\sqrt{\Delta_n^E}) \simeq 0.25n\lambda_N - 0.5n(\lambda + 1).$$

We further provide a theorem that allows us to devise a probabilistic algorithm for factoring the modulus N once $\varphi_n(N)$ is known.

Theorem 3. *Let $N = pq$ be an RSA-modulus. If $\varphi_n(N) = (p^n - 1)(q^n - 1)$ is known, then one can find primes p and q.*

Proof. Consider $a \in J_N^-$ and $b \in J_N^+ \setminus QR_N$. Without loss of generality we can assume that $J_p(a) = 1$ and $J_q(a) = -1$, which is equivalent to

$$a^{\frac{p-1}{2}} = 1 \bmod p \qquad \text{and} \qquad a^{\frac{q-1}{2}} = -1 \bmod q.$$

Remark that for any odd $t \in \mathbb{Z}$, the properties

$$a^{\frac{t(p-1)}{2}} = 1 \bmod p \qquad \text{and} \qquad a^{\frac{t(q-1)}{2}} = -1 \bmod q$$

hold. Equivalent equations can be obtained for b.

Using Remark 2 and noticing that $(q-1)/2$ divides $(p^n-1)(q^n-1)/4$, we consider $u_1, u_2, t_1, t_2, v \in \mathbb{N}$ such that

$$u_1 \cdot 2^v \cdot \frac{p-1}{2^{t_1}} = u_2 \cdot 2^v \cdot \frac{q-1}{2^{t_2}} = \frac{(p^n-1)(q^n-1)}{4},$$

where $u_1, u_2, (p-1)/2^{t_1}, (q-1)/2^{t_2}$ are odd numbers. Thus, naturally we get

$$\begin{aligned} a^{\frac{u_2(q-1)}{2}} &= -1 \bmod q \Leftrightarrow a^{\frac{u_2(q-1)}{2}} + 1 = 0 \bmod q, \\ b^{\frac{u_1(p-1)}{2}} &= -1 \bmod p \Leftrightarrow b^{\frac{u_1(p-1)}{2}} + 1 = 0 \bmod p, \\ b^{\frac{u_2(q-1)}{2}} &= -1 \bmod q \Leftrightarrow b^{\frac{u_2(q-1)}{2}} + 1 = 0 \bmod q. \end{aligned}$$

We want to prove that either

$$a^{\frac{u_2(q-1)}{2}} + 1 \neq 0 \pmod p \quad \text{or} \quad b^{\frac{u_1(p-1)}{2}} + 1 \neq 0 \pmod q.$$

We further consider the following cases

1. If $t_1 = t_2$, then

   $$a^{\frac{u_2(q-1)}{2}} \equiv a^{\frac{u_1(p-1)}{2}} \equiv 1 \pmod p,$$

   which implies

   $$a^{\frac{v(q-1)}{2}} + 1 \equiv 2 \not\equiv 0 \pmod p.$$

2. Note that

   $$a^{u_2 \cdot (q-1)/2^{t_2}} = a^{u_1 \cdot (p-1)/2^{t_1}}. \tag{8}$$

   If $t_1 < t_2$, then raising both sides of Equation (8) to 2^{t_2-1}, we get

   $$a^{\frac{u_2(q-1)}{2}} \equiv a^{u_1(p-1) \cdot 2^{t_2-t_1-1}} \equiv \left(a^{\frac{u_1(p-1)}{2}}\right)^{2^{t_2-t_1}} \equiv 1 \pmod p.$$

3. Note that

   $$b^{u_1 \cdot \frac{p-1}{2^{t_1}}} = b^{u_2 \cdot \frac{q-1}{2^{t_2}}}. \tag{9}$$

   If $t_1 > t_2$, then raising both sides of Equation (9) to 2^{t_1-1}, we get

   $$b^{\frac{u_1(p-1)}{2}} \equiv b^{u_2(q-1) \cdot 2^{t_1-t_2-1}} \equiv \left(b^{\frac{u_2(q-1)}{2}}\right)^{2^{t_1-t_2}} \equiv 1 \pmod q.$$

Algorithm 1: Factoring the modulus when the order of the group is known

Input: A composite number N and $\varphi_n(N)$.
Output: The prime factors p and q.

while $1 \neq 0$ **do**
  $a \xleftarrow{\$} J_N^-$, $b \xleftarrow{\$} J_N^+$
  while $\varphi \bmod 2 = 0$ **do**
    $\varphi \leftarrow \varphi/2$
    $y_1 \leftarrow a^{\varphi} + 1 \bmod N$, $y_2 \leftarrow b^{\varphi} + 1 \bmod N$
    $d_1 \leftarrow \gcd(y_1, N)$, $d_2 \leftarrow \gcd(y_2, N)$
    if $y_1 \neq 0$ **and** $d_1 \neq 1$ **then**
      return $d_1, N/d_1$
    if $y_2 \neq 0$ **and** $d_2 \neq 1$ **then**
      return $d_2, N/d_2$

Taking into account the previous arguments, we conclude that by computing either

$$y = a^{\frac{u_2(q-1)}{2}} + 1 \pmod{N} \quad \text{or} \quad z = b^{\frac{u_1(p-1)}{2}} + 1 \pmod{N}$$

and evaluating $\gcd(y, N)$ or $\gcd(z, N)$, respectively allows us to determine one of the factors q or p. □

Remark 6. Before stating our proposed factoring algorithm, some remarks are in place

1. In the third case of the previous proof, one could consider an element $x \in \mathbb{Z}_N$ satisfying $J_p(x) = -1$ and $J_q(x) = 1$, and the proof would proceed similarly to the second case.
2. Without knowing the factorisation of N, due to Quadratic Residuosity assumption[7], b must be chosen from J_N^+. Then, with probability of $1/2$ we have that $b \in J_N^+ \setminus QR_N$.
3. An equivalent proof can be obtained by considering numbers of the form $y = a^{\frac{u_2(q-1)}{2}} - 1$.

Using Theorem 2 we can compute the order $\varphi_n(N) = (ed-1)/k$. Based on Theorem 3, in Algorithm 1 we provide a probabilistic algorithm for computing the factorisation of N for any $n \geq 1$. Note that for $n = 3$ and $n = 4$, we provide in Appendix A a deterministic algorithm that solves a cubic or biquadratic equation, respectively. For $n = 1$ and $n = 2$ similar methods are presented in [6, 10, 13]. Therefore, for these cases we avoid doing exponentiations[8].

[7] This assumption stated that we cannot decide if $x \in QR_N$ or $J_N^+ \setminus QR_N$ without knowing the factorisation of N.
[8] that are computationally expensive

It is know that $|J_N^-| = |\mathbb{Z}_N|/2$ and $|J_N^+ \setminus QR_N| = |QR_N| = |\mathbb{Z}_N|/4$. When $b \in J_N^+ \setminus QR_N$, Algorithm 1 always returns the factorisation of N. When $b \in QR_N$, the factorisation of N can surely be found if $t_1 \leq t_2$. Thus, the probability of obtaining the factorisation of N for a single pair (a, b) is greater than $1/2$.

Remark 7. In [43], the author describes a public key encryption scheme based on Pell's equation, choosing key exponents such that $ed \equiv 1 \bmod \operatorname{lcm}(p-1, q-1)$. Using our attack with $n = 1$ we recover the factors of N, thereby we also break the scheme presented in [43].

6 Attacking the Generalized Murru and Saettone Unbalanced Scheme

6.1 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 3. *Let N be 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

$$\begin{aligned} f_{k+1}(x) &= g_{k+1}(x) \cdot h_{k+1}(x) \\ &= g_k(x) \cdot h_k(x) + g_k(x) \cdot \left(\frac{N}{x}\right)^k + x^k \cdot h_k(x) + N^k. \end{aligned}$$

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

$$\begin{aligned} s_k(x) = &\left(N^k \cdot \frac{1}{x^k} + x^k\right) + \left(N^k \cdot \frac{1}{x^{k-1}} + N \cdot x^{k-1}\right) \\ &+ \left(N^k \cdot \frac{1}{x^{k-2}} + N^2 \cdot x^{k-2}\right) + \ldots + \left(N^k \cdot \frac{1}{x} + N^{k-1} \cdot x\right) \\ &= s_{k,0}(x) + s_{k,1}(x) + s_{k,2}(x) + \ldots + s_{k,k-1}(x), \end{aligned}$$

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

$$\begin{aligned} s_{k,i}'(x) &= N^k \cdot \frac{-(k-i)}{x^{k-i+1}} + N^i \cdot (k-i) \cdot x^{k-i-1} \\ &= N^i (k-i) \left(x^{k-i-1} - N^{k-i} \cdot \frac{1}{x^{k-i+1}}\right). \end{aligned}$$

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.

□

Using Lemma 3 from Section 5.1, we further compute a lower and upper bound for $\psi_n(N)$.

Corollary 12. *Let $N = pq$ be the product of two unknown primes with $\mu q < p < 2\mu q$. Then the following property holds*

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

Proof. By Lemma 3 we have that

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

which, according to Proposition 3, leads to

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

This is equivalent to our desired inequality. □

When $n = 3$ and $\mu = 1$, the following result proven in [40] becomes a special case of Corollary 12.

Corollary 13. *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 12 to find an useful approximation of ψ_n. This result will be useful when devising the attack against the generalized Murru-Saettone scheme.

Proposition 4. *Let $N = pq$ be the product of two unknown primes with $\mu q < p < 2\mu q$. We define*

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

Then the following holds

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

where

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

Proof. According to Corollary 12, $\psi_{n,0}(N)$ is the mean value of the lower and upper bound. The following property holds

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

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

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

as desired.

□

When $n = 3$ and $\mu = 1$, the following property presented in [40] becomes a special case of Proposition 4.

Corollary 14. *Let $N = pq$ be the product of two unknown primes with $q < p < 2q$. Then the following holds*

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

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

$$d < \sqrt{\frac{N^{n-0.5}}{e\Delta_n^M}}, \tag{10}$$

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 4 we obtain

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

Note that

$$\begin{aligned}\psi_{n,0}(N) &> \frac{(\sqrt{\mu N})^n-1}{\sqrt{\mu N}-1}\cdot\frac{\left(\frac{\sqrt{\mu N}}{\mu}\right)^n-1}{\frac{\sqrt{\mu N}}{\mu}-1}\\ &> \frac{\sqrt{\mu N}^{2(n-1)}}{\mu^{n-1}}+\sqrt{\mu N}+\frac{\sqrt{\mu N}}{\mu}\\ &= \sqrt{N}^{2(n-1)}+\sqrt{N}\cdot(\sqrt{\mu}+\frac{1}{\sqrt{\mu}})\\ &> \sqrt{N}^{2(n-1)}+2\sqrt{N},\end{aligned}$$

which leads to

$$\left|\frac{k}{d}-\frac{e}{\psi_{n,0}(N)}\right| \leq \frac{k}{2d}\cdot\Delta_n^M\cdot\frac{2+\sqrt{N}^{2n-3}}{\sqrt{N}^{2n-2}+2\sqrt{N}} = \frac{k\Delta_n^M}{2d\sqrt{N}}. \tag{11}$$

According to Corollary 12, we have that $\psi_n(N) > \frac{\sqrt{\mu N}^{2(n-1)}}{\mu^{n-1}} = N^{n-1}$. Since $k\psi_n(N) = ed-1 < ed$, we have

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

Equation (11) becomes

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

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 15. *Let $\alpha + 0.5 < n$, $\lambda = \lambda_p - \lambda_q$ and $N = pq$ be the product of two unknown primes with $\mu q < p < 2\mu q$. If we approximate $e \simeq N^\alpha$, $N \simeq 2^{\lambda_N}$ and $\mu \simeq 2^\lambda$, then Equation (10) becomes*

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

or equivalently

$$\log_2(d) < 0.5(n-\alpha-0.5)\lambda_N - \log_2(\sqrt{\Delta_n^M}) \simeq 0.5(n-\alpha-0.5)\lambda_N - 0.25(n-1)\lambda.$$

Proof. From the definition of Δ_n^M we obtain that

$$\begin{aligned}
\Delta_n^M &= \sum_{\substack{i,j=0 \\ i\neq j}}^{n-1} \sqrt{\mu}^{i-j}(\sqrt{2}^{i-j} - 1) \simeq \sum_{\substack{i,j=0 \\ i\neq j}}^{n-1} 2^{\lambda(i-j)/2}(\sqrt{2}^{i-j} - 1) \\
&\simeq \sum_{\substack{i,j=0 \\ i\neq j}}^{n-1} 2^{\lambda(i-j)/2} \simeq \sum_{\substack{j=0 \\ i>j}}^{n-1} 2^{\lambda(i-j)/2} = \sum_{j=0}^{n-1} 2^{\lambda/2}\frac{2^{\lambda(n-1-j)/2} - 1}{2^{\lambda/2} - 1} \\
&\simeq \sum_{j=0}^{n-1} 2^{\lambda(n-1-j)/2} = \frac{2^{\lambda n/2} - 1}{2^{\lambda/2} - 1} \simeq 2^{\lambda(n-1)/2},
\end{aligned}$$

as desired. □

When case $n = 3$ and $\mu = 1$ is considered, the following property presented in [40] becomes a special case of Corollary 15.

Corollary 16. *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 $N \simeq 2^{\lambda_N}$ then Equation (10) is equivalent with*

$$\log_2(d) < 0.5(2.5-\alpha)\lambda_N - 0.43 \simeq 0.5(2.5-\alpha)\lambda_N.$$

Corollary 17. *Let $N = pq$ be the product of two unknown primes with $\mu q < p < 2\mu q$. If we approximate $e \simeq N^{n-1}$, $N \simeq 2^{\lambda_N}$ and $\mu \simeq 2^\lambda$ then Equation (10) is equivalent with*

$$\log_2(d) < 0.25(\lambda_N - \lambda(n-1)).$$

7 Discussions

In this section we will compare the attack intervals for the two RSA-like families. We start with the balanced primes case (*i.e.* $\lambda = 0$). According to Corollaries 8 and 15 for a given α, $n > 1$ and λ_N, we have

$$\begin{aligned}
0.5(1.5n-\alpha)\lambda_N \geq 0.5(n-\alpha-0.5)\lambda_N &\Leftrightarrow 1.5n - \alpha \geq n - \alpha - 0.5 \\
&\Leftrightarrow 0.5(n+1) \geq 0.
\end{aligned}$$

Therefore, the attack interval for the generalized Elkamchouchi *et al.* scheme is always greater that the one for the generalized Murru and Saettone scheme.

In the unbalanced case, for a given α, $n > 1$, λ_p and λ_q, we obtain that

$$\begin{aligned} 0.5(1.5n-\alpha)\lambda_N - 0.5n(\lambda+1) &\geq 0.5(n-\alpha-0.5)\lambda_N - 0.25(n-1)\lambda \\ &\Leftrightarrow 0.5(0.5n+0.5)\lambda_N \geq 0.25(n+1)\lambda + 0.5n \\ &\Leftrightarrow (n+1)\lambda_N \geq (n+1)\lambda + 2n \\ &\Leftrightarrow (n+1)(\lambda_p+\lambda_q) \geq (n+1)(\lambda_p-\lambda_q) + 2n \\ &\Leftrightarrow (n+1)\lambda_q \geq -(n+1)\lambda_q + 2n \\ &\Leftrightarrow (n+1)\lambda_q \geq n. \end{aligned}$$

Therefore, the attack interval for the generalized Elkamchouchi *et al.* scheme is always greater that the one for the Murru and Saettone scheme.

Taking into account the previous arguments and the fact that for the generalized Elkamchouchi *et al.* scheme we found a probabilistic factoring algorithm[9], we conclude that the security assurances[10] are greater for the generalized Murru and Saettone scheme.

8 Conclusions

In this paper, we introduced two families of RSA-like cryptosystems. The first one includes the RSA and Elkamchouchi *et al.* public key encryption schemes [20, 45] (*i.e.* $n = 1$ and $n = 2$), while the second one includes the Murru and Saettone public key encryption scheme [36] (*i.e.* $n = 3$). Then, we presented a small private key attack against each family of cryptosystems and provided several instantiations of it.

As a conclusion, the both families of RSA-like schemes allow 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 than $N^{0.25n} \cdot (q/p)^{0.5n} \cdot 2^{-0.5n}$ or N^{n-1}, or when the secret exponent is smaller than $N^{0.25} \cdot (q/p)^{0.25(n-1)}$, respectively. Note that in the case of the generalized Elkamchouchi *et al.* scheme, we also provided a probabilistic factorisation algorithm once the order φ_n is known. For completeness, we also provided a generalization of Wiener's attack to the unbalanced RSA. In this case we can recover the secret exponent when it is smaller than $N^{0.25}(q/p)^{0.25}$.

Future Work. We leave the construction of a deterministic factoring algorithm, capable of factoring N given the order of the group φ_n or ψ_n, as an open problem. While we have managed to devise such algorithms for specific cases

- for φ_n when $n = 1, 2, 3, 4$ (see Appendix A and [6, 10, 13]),
- for ψ_n when $n = 2, 3, 4$ (see Appendix B and [40]),

[9] once the order is known

[10] from a continued fraction perspective

the general case remains unsolved. Note that when ψ_n is given, we could not even find a probabilistic algorithm for factoring. Another interesting research direction is to find out whether the attack methods described in Section 1 also work in the general case of the two RSA-like families.

References

1. Alecci, G., Dutto, S., Murru, N.: Pell Hyperbolas in DLP–based Cryptosystems. Finite Fields and Their Applications **84**, 102112 (2022)
2. 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)
3. Barker, E.: NIST SP800-57 Recommendation for Key Management, Part 1: General. Tech. rep., NIST (2016)
4. 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)
5. 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)
6. Boneh, D.: Twenty Years of Attacks on the RSA Cryptosystem. Notices of the AMS **46**(2), 203–213 (1999)
7. 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)
8. 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)
9. Brent, R.P.: Some Parallel Algorithms for Integer Factorisation. In: Euro-Par 1999. Lecture Notes in Computer Science, vol. 1685, pp. 1–22. Springer (1999)
10. Bunder, M., Nitaj, A., Susilo, W., Tonien, J.: A New Attack on Three Variants of the RSA Cryptosystem. In: ACISP 2016. Lecture Notes in Computer Science, vol. 9723, pp. 258–268. Springer (2016)
11. Bunder, M., Nitaj, A., Susilo, W., Tonien, J.: A generalized attack on RSA type cryptosystems. Theoretical Computer Science **704**, 74–81 (2017)
12. 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)
13. Bunder, M., Tonien, J.: A New Attack on the RSA Cryptosystem Based on Continued Fractions. Malaysian Journal of Mathematical Sciences **11**, 45–57 (2017)
14. Cherkaoui-Semmouni, M., Nitaj, A., Susilo, W., Tonien, J.: Cryptanalysis of RSA Variants with Primes Sharing Most Significant Bits. In: ISC 2021. Lecture Notes in Computer Science, vol. 13118, pp. 42–53. Springer (2021)
15. Coppersmith, D.: Small Solutions to Polynomial Equations, and Low Exponent RSA Vulnerabilities. Journal of Cryptology **10**(4), 233–260 (1997)
16. Cotan, P., Teşeleanu, G.: Continued Fractions Applied to a Family of RSA-like Cryptosystems. In: ISPEC 2022. Lecture Notes in Computer Science, vol. 13620, pp. 589–605. Springer (2022)
17. Cotan, P., Teşeleanu, G.: Small Private Key Attack Against a Family of RSA-Like Cryptosystems. In: NordSEC 2023. Lecture Notes in Computer Science, vol. 14324, pp. 57–72. Springer (2023)

18. De Weger, B.: Cryptanalysis of RSA with Small Prime Difference. Appl. Algebra Eng. Commun. Comput. **13**(1), 17–28 (2002)
19. Dutto, S.: DLP-based Cryptosystems with Pell Cubics. Banach Center Publications **126**, 123–136 (2023)
20. 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)
21. 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)
22. Fujii, K.: A Modern Introduction to Cardano and Ferrari Formulas in the Algebraic Equations. arXiv Preprint **arXiv:quant-ph/0311102** (2003)
23. Gallian, J.: Contemporary Abstract Algebra. Chapman and Hall/CRC, 10 edn. (2020)
24. Gilbert, H., Gupta, D., Odlyzko, A., Quisquater, J.J.: Attacks on Shamir's 'RSA for Paranoids'. Information Processing Letters **68**(4), 197–199 (1998)
25. Hardy, G.H., Wright, E.M., et al.: An Introduction to the Theory of Numbers. Oxford University Press (1979)
26. 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)
27. 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)
28. Joye, M., Quisquater, J.J., Yen, S.M.: Two Protocol Attacks on Okamoto and Uchiyama's Cryptosystem. Tech. Rep. TR-98-8B, TamKang University (1998)
29. Jr., H.W.L.: Factoring Integers with Elliptic Curves. Annals of Mathematics pp. 649–673 (1987)
30. 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)
31. Lenstra, A.K.: Unbelievable Security. Matching AES Security Using Public Key Systems. In: ASIACRYPT 2001. Lecture Notes in Computer Science, vol. 2248, pp. 67–86. Springer (2001)
32. Lenstra, A.K., Verheul, E.R.: Selecting Cryptographic Key Sizes. In: PKC 2000. Lecture Notes in Computer Science, vol. 1751, pp. 446–465. Springer (2000)
33. Lenstra, A.K., Verheul, E.R.: Selecting Cryptographic Key Sizes. Journal of Cryptology **14**(4), 255–293 (2001)
34. 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)
35. Maitra, S., Sarkar, S.: Revisiting Wiener's Attack - New Weak Keys in RSA. IACR Cryptology ePrint Archive **2008/228** (2008)
36. 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)
37. 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)
38. 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)

39. 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)
40. 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)
41. 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)
42. Nitaj, A., Pan, Y., Tonien, J.: A Generalized Attack on Some Variants of the RSA Cryptosystem. In: SAC 2018. Lecture Notes in Computer Science, vol. 11349, pp. 421–433. Springer (2018)
43. Padhye, S.: A Public Key Cryptosystem Based on Pell Equation. IACR Cryptology ePrint Archive **2006/191** (2006)
44. Peng, L., Hu, L., Lu, Y., Wei, H.: An Improved Analysis on Three Variants of the RSA Cryptosystem. In: Inscrypt 2016. Lecture Notes in Computer Science, vol. 10143, pp. 140–149. Springer (2016)
45. 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)
46. Sarkar, S., Maitra, S.: Cryptanalysis of RSA with more than one Decryption Exponent. Information Processing Letters **110**(8-9), 336–340 (2010)
47. Shamir, A.: RSA for Paranoids. RSA Laboratories' Cryptobytes **1**(3), 1–4 (1995)
48. Shi, G., Wang, G., Gu, D.: Further Cryptanalysis of a Type of RSA Variants. In: ISC 2022. Lecture Notes in Computer Science, vol. 13640, pp. 133–152. Springer (2022)
49. Silverman, R.D.: A Cost-Based Security Analysis of Symmetric and Asymmetric Key Lengths. RSA Laboratories' Bulletin 13 (2000)
50. 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)
51. 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)
52. 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)
53. Teşeleanu, G.: The Case of Small Prime Numbers Versus the Joye–Libert Cryptosystem. Mathematics **10**(9) (2022)
54. Wiener, M.J.: Cryptanalysis of Short RSA Secret Exponents. IEEE Trans. Inf. Theory **36**(3), 553–558 (1990)
55. Zheng, M., Kunihiro, N., Hu, H.: Cryptanalysis of RSA Variants with Modified Euler Quotient. In: AFRICACRYPT 2018. Lecture Notes in Computer Science, vol. 10831, pp. 266–281. Springer (2018)
56. Zheng, M., Kunihiro, N., Yao, Y.: Cryptanalysis of the RSA Variant Based on Cubic Pell Equation. Theor. Comput. Sci. **889**, 135–144 (2021)

A Experimental Results for the Elkamchouchi *et al.* scheme

We further present some examples for the attack presented in Section 5.2 in the cases $n = 3$ and $n = 4$. When $\lambda_p = \lambda_q$, examples for $n = 1$ and $n = 2$ cases are provided in [13] and [10] respectively, and thus we omit them.

A.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 4. *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

$$x^3 - 3Nx + (\varphi_3(N) - N^3 - 1) = 0. \tag{12}$$

which can be done in polynomial time as it is presented in [22]. 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 Equation (12), namely its unique integer solution.

Lemma 5. *Equation (12) always has exactly two non-real roots and an integer one.*

Proof. Let x_1, x_2 and x_3 be Equation (12)'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 Equation (12) has one real root, which is $p + q \in \mathbb{Z}$, and two non-real roots.

□

A.1.1 Same size primes

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

$$\begin{aligned} N = {} & 30149726335030403365902265083163510227689133239 33, \\ e = {} & 82056564937989925576324523329262228197624353069 99 \\ & 01246260356125175630059988956546885266430027154 34 \\ & 25112020628278119623817044320522328087505650969. \end{aligned}$$

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 4, 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 4. 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

$$\begin{aligned} \varphi_3 &= 27406282078929532070187021740774838075632644087737057963987757509374280517157259708222994487763446\\ &\quad 94662185556560092721547156554580719829895393303 6, \\ \frac{k}{d} &= \frac{514812488}{1719435401}, \\ p &= 2119778199036859068707819, \\ q &= 1422305708622213956806807. \end{aligned}$$

A.1.2 Different size primes

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

$$\begin{aligned} N &= 285581348061409421627439459247261854727823254141939536 1, \\ e &= 463008404666242909733655867067130423327143258410921646 8\\ &\quad 091589499179996970789732007667794789828707573166786708 0\\ &\quad 462283856689108932845889311220553749263154878486739999, \end{aligned}$$

with security parameters $\lambda_p = 100$ and $\lambda_q = 80$.

Remark that $e \approx N^{2.987}$. We use the Euclidean algorithm to compute the continued fraction expansion of $e/\varphi_{3,0}(N)$ and obtain that the first 30 partial quotients are

$$[0, 5, 32, 1, 11, 4, 4, 4, 1, 1, 12, 2, 1, 2, 1, 1, 1, 5, 1, 1, 2, 1, 3, 1, 10, 1, 1, 1, 1, 1, \ldots].$$

According to Theorem 4, 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 4. The $2nd$ and $29th$ convergents satisfy the first condition, however only the last one leads to a valid solution for p and q.

More precisely, the $29th$ convergent leads to

$$\begin{aligned}
\varphi_3 = {} & 232910741459006402295102053105919242653973275049 6 \\
& 029108317719444597784927237235625011288576301878 6 \\
& 831400586896415450819952957332371482427309558790 0 \\
& 67149237117218500, \\
\frac{k}{d} = {} & \frac{293248165996}{1475149199999}, \\
p = {} & 154574243774571078739749638371 1, \\
q = {} & 184753514613920593790515 1.
\end{aligned}$$

A.2 Case $n = 4$

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

Lemma 6. *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*

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

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

$$\begin{gathered}
x^4 - 4Nx^2 + \varphi_4(N) - (N^2-1)^2 = 0 \Leftrightarrow \\
(x^2)^2 - 4N(x^2) + \varphi_4(N) - (N^2-1)^2 = 0.
\end{gathered}$$

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 4.

□

A.2.1 Same size primes

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

$$\begin{aligned} N = {} & 30149726335030403365902265083163510227689133239 33, \\ e = {} & 38866490781572175125407812682802133603199701331 45 \\ & 63967882732043202837388503022144414843013560472 80 \\ & 99800746782269380655826208578198301711391746348 97 \\ & 69731055010977380039512575106301590600391232847. \end{aligned}$$

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 6. 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

$$\begin{aligned}
\varphi_4 = {} & 82629190454037350488781110250501375470180679867186489272861711603139280409749776405912009959512474\\
& 12259659675739686050375962748536184813027544574806787891184267004832506535094151626645227104000,\\
\frac{k}{d} = {} & \frac{799532980}{1699787183},\\
p = {} & 2119778199036859068707819,\\
q = {} & 1422305708622213956806807.
\end{aligned}$$

A.2.2 Different size primes

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

$$\begin{aligned}
N = {} & 285581348061409421627439459247261854727823254141939536 1,\\
e = {} & 256737051097223200677353704721562756910723228181218920 3\\
& 476871582305102261954225735072829560938781181613256217012123246497544282774147846042464386984086249436061680284389852002469708776700405298285081740832540792743333.
\end{aligned}$$

with security parameters $\lambda_p = 100$ and $\lambda_q = 80$.

Note that $e \approx N^{3.974}$. Applying the continued fraction expansion of $e/\varphi_{4,0}(N)$, we get the first 30 partial quotients

$$[0, 25, 1, 9, 1, 5, 1, 1, 2, 1, 5, 2, 6, 6, 1, 1, 1, 1, 1, 1, 7, 1, 92, 3, 1, 1, 1, 1, 2, 1, \ldots].$$

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 6. The $2nd$, $3rd$ and $30th$ convergents satisfy the first condition, however only the last one leads to a valid solution for p and

q. More precisely, the $30th$ convergent leads to

$$\begin{aligned}
\varphi_4 = {} & 665149635238454490318812061977090819661681701620093863096585108343044888192867730092513807651941224968129797199545925318425222504044575756485728476654739258155949912\\
& 41680627125876858676996469366026313423904013451264000,\\
\frac{k}{d} = {} & \frac{184064447974}{4768707901997},\\
p = {} & 154574243774571078739749638371,\\
q = {} & 184753514613920593790515 1.
\end{aligned}$$

B Experimental Results for the Murru and Saettone scheme

In this section we provide examples for the attack discussed in Section 6.2, specifically we examine the cases where $n = 2$ and $n = 4$. An example for the case $\lambda_p = \lambda_q$ and $n = 3$ is provided in [40], and thus we omit it.

B.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 7. *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

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

□

B.1.1 Same size primes

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

$$\begin{aligned} N &= 119395546939140554652504541147065104558247878565 91, \\ e &= 607457463306018151476885843605130298081016983082 1. \end{aligned}$$

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 4, 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 7. 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

$$\begin{aligned} \psi_2 &= 119395546939140554652504612835678769587853374900 00, \\ \frac{k}{d} &= \frac{3205471919}{6300343581}, \\ p &= 453762983826611741812024 9, \\ q &= 263123152823684313151315 9. \end{aligned}$$

B.1.2 Different size primes

In this scenario we will consider the following public key

$$\begin{aligned} N &= 501973603006739414747573670718922806133921978656698 2627, \\ e &= 485434467383574169502440945536575804609769000630574045, \end{aligned}$$

with security parameters $\lambda_p = 100$ and $\lambda_q = 80$.

Observe that $e \approx N^{0.9815}$. Using the Euclidean algorithm to compute the continue fraction expansion of $e/\psi_{2,0}(N)$ we obtain that the first 20 partial quotients are

$$[0, 10, 2, 1, 14, 2, 2, 286, 1, 2, 1, 32, 1, 4, 2, 1, 3, 1, 1, 2, \ldots].$$

As stated in Theorem 4, the set of convergents of $e/\psi_{2,0}$ includes all possible candidates for k/d. From these convergents we choose 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 7. The $2nd$, $3rd$, $4th$ 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

$$\begin{aligned} \psi_2 &= 501973603006739414747573907174692512527542976620121765 6, \\ \frac{k}{d} &= \frac{1167480464}{12072574453}, \\ p &= 2364555574155054332193018723851, \\ q &= 212290888187778661551117 7. \end{aligned}$$

B.2 Case $n = 4$

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

Lemma 8. *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

$$x^3 + (N+1)x^2 + (N-1)^2x + (N^3 - N^2 - N + 1 - \psi_4(N)) = 0, \tag{13}$$

which can be done in polynomial time as it is presented in [22]. In order to find p and q, we compute $D = p - q$ as in Lemma 7. This concludes our proof. □

The following lemma shows that in order to factor N we only need to find one solution to Equation (13), namely its unique integer solution.

Lemma 9. *Equation (13) always has exactly two non-real roots and an integer one.*

Proof. Let x_1, x_2 and x_3 be Equation (13)'s roots. Using Vieta's formulas we have

$$\begin{aligned} x_1 + x_2 + x_3 &= -(N+1), \\ x_1x_2 + x_2x_3 + x_3x_1 &= (N-1)^2, \\ x_1x_2x_3 &= -(N^3 - N^2 - N + 1 - \psi_4(N)). \end{aligned}$$

From the first two relations we obtain

$$\begin{aligned} x_1^2 + x_2^2 + x_3^2 &= (x_1 + x_2 + x_3)^2 - 2(x_1x_2 + x_2x_3 + x_3x_1) \\ &= (N+1)^2 - 2(N-1)^2 \\ &= -N^2 + 6N - 1. \end{aligned}$$

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 (13) has one real root, which is $p+q \in \mathbb{Z}$, and two non-real roots. □

B.2.1 Same size primes

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

$$\begin{aligned} N = {} & 11939554693914055465250454114706510455824787856591, \\ e = {} & 15006652287039759861337802324565215623310940476513 \\ & 92542670434722550157448270887318217632962138205421 \\ & 89964769628587046165774107346417261221631274140 9. \end{aligned}$$

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 8. 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

$$\begin{aligned}
\psi_4 &= 17020189377867860247096553094467061591207640835506 \\
&\quad 21907753457911934182387623188683187170430636727789 \\
&\quad 99618058600556573209318787267816952014412436000, \\
\frac{k}{d} &= \frac{2425248603}{2750659489}, \\
p &= 45376298382661174181202 49, \\
q &= 26312315282368431315131 59.
\end{aligned}$$

B.2.2 Different size primes

In this scenario we will consider the following public key

$$\begin{aligned}
N &= 50197360300673941474757367071892280613392197865669826 27, \\
e &= 21445035131128300767668909857408911291817946304088842 43 \\
&\quad 83517627180999492717723394729154173432144092541548212 28 \\
&\quad 34928451250224578936058306348284684412610415326683657 9,
\end{aligned}$$

with security parameters $\lambda_p = 100$ and $\lambda_q = 80$.

Notice that $e \approx N^{2.986}$. Using the Euclidean algorithm to compute the continue fraction expansion of $e/\psi_{4,0}(N)$ we obtain that the first 20 partial quotients are

$$[0, 5, 1, 8, 1, 4, 1, 1, 30, 1, 22, 1, 1, 4, 24, 1, 50, 2, 2, 3, \ldots].$$

As stated in Theorem 4, the set of convergents of $e/\psi_{4,0}$ includes all possible candidates for k/d. From these convergents we choose 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 8. The $2nd$, $3rd$, $5th$ and $17th$ convergents satisfy the first condition, however only the last one leads to a valid solution for

p and q. More precisely, the $13th$ convergent leads to

$$\begin{aligned}
\psi_4 &= 126486052605695372282429207929730908438877658224124401024242401547851990497837329277957404040229825866202705537312473369988620334246189313082892046200224081054148960,\\
\frac{k}{d} &= \frac{927107051}{5468217259},\\
p &= 2364555574155054332193018723851,\\
q &= 212290888187778661551117 7.
\end{aligned}$$

C Generalized Wiener Attack

In this section we provide an equivalent of Wiener's attack applied to the unbalanced RSA. To the best of our knowledge, there is no such equivalent in the literature.

Theorem 5. *Let $N = pq$ be the product of two unknown primes with $\mu q < p < 2\mu q$. If $e < \varphi(N)$ satisfies $ed - k\varphi(N) = 1$ with*

$$d < \frac{(\mu N)^{0.25}}{\sqrt{2(2\mu+1)}} \tag{14}$$

then we can recover d in polynomial time.

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

$$\begin{aligned}
\left|\frac{k}{d} - \frac{e}{N}\right| &= \frac{|ed - kN|}{dN}\\
&= \frac{|ed - k\varphi(N) + k\varphi(N) - kN|}{dN}\\
&= \frac{|1 - k(N - \varphi(N))|}{dN}.
\end{aligned}$$

Since $\mu q < p < 2\mu q$, we obtain

$$N - \varphi(N) = p + q - 1 < (2\mu+1)q < \frac{(2\mu+1)}{\sqrt{\mu}}\sqrt{N},$$

where for the last inequality we used Lemma 3. Therefore, we have

$$\left|\frac{k}{d} - \frac{e}{N}\right| < \frac{|k(2\mu+1)\sqrt{N}|}{d\sqrt{\mu}N} = \frac{k(2\mu+1)}{d\sqrt{\mu N}}.$$

Since $k\varphi(N) = ed - 1 < ed$ and $e < \varphi(N)$, we obtain $k < d$. This leads to

$$\left|\frac{k}{d} - \frac{e}{N}\right| < \frac{2\mu+1}{\sqrt{\mu N}} < \frac{1}{2d^2}.$$

Using Theorem 1 we obtain that k/d is a convergent of the continued fraction expansion e/N. Therefore, d can be recovered in polynomial time. □

When case $\mu = 1$ is considered, Wiener's attack [6,54] becomes a special case of Theorem 5.

Corollary 18. *Let $N = pq$ be the product of two unknown primes with $q < p < 2q$. If $e < \varphi(N)$ satisfies $ed - k\varphi(N) = 1$ with*

$$d < \frac{N^{0.25}}{\sqrt{6}} < \frac{N^{0.25}}{3}$$

then we can recover d in polynomial time.

Corollary 19. *Let $\lambda = \lambda_p - \lambda_q$ and $N = pq$ be the product of two unknown primes with $\mu q < p < 2\mu q$. If we approximate $N \simeq 2^{\lambda_N}$ and $\mu \simeq 2^{\lambda}$ then Equation (14) becomes*

$$d < 2^{0.25(\lambda_N - \lambda)}$$

or equivalently

$$\log_2(d) < 0.25(\lambda_N - \lambda).$$

D Experimental Results for the Generalized Wiener Attack

For completeness, we additionally present an example for the generalized Wiener attack when $\lambda_p > \lambda_q$. An example for the case $\lambda_p = \lambda_q$ is provided in [54], and thus we omit it.

D.1 Different size primes

We will exemplify the generalized Wiener's attack using the following public key

$$N = 352080370719441442895298810396141575157497456664 1,$$
$$e = 212301849899841499079336298834789918610175943273 3,$$

with security parameters $\lambda_p = 120$ and $\lambda_q = 40$.

Notice that by setting $\mu = 2^{80}$, we obtain that in order to apply Wienner's attack, we need $d < 653176$. Using the Euclidean algorithm to compute the continue fraction expansion of e/N we obtain that the first 20 partial quotients are

$$[0, 1, 1, 1, 1, 12, 1, 3, 3, 1, 1, 3, 1, 2, 1, 2, 1, 3, 14, 2, \ldots].$$

As stated in Theorem 5, the set of convergents of e/N includes all possible candidates for k/d. From these convergents we choose only those for which $\varphi(N) = (ed - 1)/k$ is an integer and the following system of equations

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

has a solution. Note that the system's solutions can be computed similarly as in the case of Lemma 7. The $2nd$, $3rd$, $4th$ and $18th$ convergents satisfy the first condition, however only the $18th$ convergent leads to a valid solution for p and q. More precisely, the last one leads to

$$\begin{aligned}
\varphi(N) &= 352080370719271160376481448771473905416440058123 2, \\
\frac{k}{d} &= \frac{291041}{482661}, \\
p &= 17028251881736162466766953429491160 7, \\
q &= 2067624869333.
\end{aligned}$$