A Lattice Attack Against a Family of RSA-like Cryptosystems

George Teşeleanu[1,2]

[1] Advanced Technologies Institute
10 Dinu Vintilă, Bucharest, Romania
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 interesting RSA-like cryptosystem that, unlike the classical RSA key equation $ed - k(p-1)(q-1) = 1$, uses the key equation $ed - k(p^2 - 1)(q^2 - 1) = 1$. The scheme was further extended by Cotan and Teşeleanu to a variant that uses the key equation $ed - k(p^n - 1)(q^n - 1) = 1$, where $n \geq 1$. Furthermore, they provide a continued fractions attack that recovers the secret key d if $d < N^{0.25n}$. In this paper we improve this bound using a lattice based method. Moreover, our method also leads to the factorisation of the modulus N, while the continued fractions one does not (except for $n = 1, 2, 3, 4$).

Keywords: lattice attack, small private key attack, RSA

1 Introduction

RSA is one of the most widely adopted cryptosystems and was designed by Rivest, Shamir and Adleman [22] in 1978. The standard version of RSA has as an underlying group $\mathbb{Z}_N$, where N is the product of two large prime numbers p and q. To encrypt a message m such that $m < N$, the process involves computing $c \equiv m^e \bmod N$, where e satisfies $\gcd(e, \varphi(N)) = 1$ and $\varphi(N) = (p-1)(q-1)$ is Euler's totient function. The inverse operation requires computing $m \equiv c^d \bmod N$, where $d \equiv e^{-1} \bmod \varphi(N)$. Note that (N, e) are public, while (p, q, d) are kept secret. The standard RSA, termed balanced RSA, employs primes p and q that have the same bit-size (*i.e.* $q < p < 2q$). This paper exclusively focuses on balanced RSA and its variations.

In parallel with the development of modulus factoring methods, several specific attacks have been developed in order to extract as much information as possible from the public key (N, e). Therefore, Wiener showed in [24] that if $d < N^{0.25}/3$, then one can retrieve d from the continued fraction expansion of e/N, and thus factor N. This bound was improved by Boneh and Durfee [4] to $N^{0.292}$. The main tools that they used are Coppersmith's method [7] and lattice reduction techniques [16]. Later on, Herrmann and May [12] obtain the same bound, but using simpler techniques. For more details about RSA attacks we refer the reader to [3, 18, 23].

A variant of RSA was proposed by Elkamchouchi, Elshenawy and Shaban [11] in 2002. The authors extended the traditional RSA scheme to the ring of Gaussian integers modulo N. A Gaussian integer modulo N assumes the form $a + bi$, where a and b belong to $\mathbb{Z}_N$ and $i^2 = -1$. We further denote the set of all Gaussian integers modulo N by $\mathbb{Z}_N[i]$. The equivalent of Euler's totient function for $\mathbb{Z}_N[i]$ is $\phi(N) = (p^2 - 1)(q^2 - 1)$. In this case, the encryption exponent is chosen such that $\gcd(e, \phi(N)) = 1$, and the corresponding decryption exponent is computed as $d \equiv e^{-1} \bmod \phi(N)$. The encryption and decryption processes are similar to RSA. More precisely, 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 all exponentiations are conducted within the ring $\mathbb{Z}_N[i]$.

The authors of [11] argue that this extension offers enhanced security compared to the traditional RSA approach. Unfortunately, a continued fraction attack similar to Wiener's was developed in [5]. As in the case of RSA, using lattice reduction techniques, the bound was latter improved to $d < N^{0.585}$ in [21, 26]. For more details about attacks against Elkamchouchi *et al.*'s scheme we refer the reader to [10, 23].

We note that the rings Z_p and $Z_p[i]$ can be interpreted as $Z_p = \mathbb{Z}_p[t]/(t+1) = GF(p)$ and $Z_p[i] = \mathbb{Z}_p[t]/(t^2 + 1) = GF(p^2)$, where GF stands for Galois field. Therefore, for RSA, we have that $\mathbb{Z}_N = GF(p) \times GF(q)$, while for Elkamchouchi *et al.*, $\mathbb{Z}_N[i] = GF(p^2) \times GF(q^2)$. Building upon this observation, the authors of [10], provide a cryptosystem that extends both the RSA and Elkamchouchi *et al.*' schemes to the $GF(p^n) \times GF(q^n)$ group, where $n \geq 1$. In this case, the group order is $\varphi_n(N) = (p^n - 1)(q^n - 1)$ and the encryption/decryption process is a direct extension of RSA and Elkamchouchi *et al.* ones.

The purpose of extending both schemes to $GF(p^n) \times GF(q^n)$ was to see if Wiener-type attacks work in the generic setting. The authors of [10] manage to prove that when $d < N^{0.25n}$, we can always mount a continued fractions attack, and thus recover the secret exponent regardless the value of n. The development of a lattice reduction attack was left as an open problem, as well as a factoring method for N when $\varphi_n(N)$ is known[3].

Related work. It is worth noting that our current undertaking shares similarities with the work of [1], where the authors explored a cryptographic system closely related to our own. Specifically, they studied the effect of using latices against the generalized Murru-Saettone cryptosystem [9]. Their attack implicitly leads to factoring N.

Our Contributions. In this paper we develop a lattice type of attack against Cotan and Teşeleanu's scheme, thus filling a gap in the literature. More precisely,

[3] The only known cases are for $n = 1, 2, 3, 4$.

we prove that when $d < N^\gamma$, where

$$\begin{cases} \gamma \leq n(1-\sqrt{0.5}), & \text{when } n = 1 \text{ or } n = 2, \\ \gamma \leq \frac{3n-1}{4} - \frac{n^2}{2(n+1)}, & \text{otherwise,} \end{cases}$$

we can always factor N. To establish these bounds, we first had to prove that $\varphi_n(N)$ can be written as a polynomial in $p+q$. Then, we showed how to reduce the problem of finding $p+q$ to solving an equation of the form $xH(y)+1 \equiv 0 \bmod e$, where $H(y)$ is a monic univariate polynomial. A method for solving such equations is described in [15]. Finally, we prove that the new bounds are always better than the ones presented in [10].

Structure of the Paper. Preliminary notions are provided in Section 2. In Section 3 we take a new look at the group's order, while in Section 4 we describe our attack. An example is given in Section 5 and we conclude our paper in Section 6.

2 Preliminaries

Notations. Throughout the paper, λ denotes a security parameter. Also, the notation $|S|$ denotes the cardinality of a set S. We use $\simeq$ to indicate that two values are approximately equal.

2.1 Quotient Groups

In this section we provide the group theory needed to introduce the RSA-like family. 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

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

2.2 RSA-like Cryptosystems

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

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

where $a(t) \in \mathbb{A}_n^*$ and the power is evaluated by $\circ$-multiplying $a(t)$ by itself $\varphi_n(\mathbb{Z}_p) - 1$ times. Based on these observations, the authors of [10] built an encryption scheme that is similar to RSA by using the $\circ$ operation 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 [22]. Also, when $n = 2$, we obtain the Elkamchouchi *et al.* cryptosystem [11].

2.3 Useful Lemmas

The results provided in this section will be used in Section 4 to bound the solutions of the equation $xH(y) - 1 \equiv 0 \bmod e$, which is derived from the key equation $ed - k\varphi_n(N) = 1$. We start by providing lower and upper bounds for p and q (see [19, Lemma 1]).

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

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

The bounds for $\varphi_n(N)$ are provided in [10, Corollary 1]. This result implies that $\varphi_n(N)$ can be approximated by N^n.

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

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

2.4 Finding Small Roots

In this section, we outline some tools used for solving the problem of finding small roots, both in the modular and integer cases.

Coppersmith [6–8] provided rigorous techniques for computing small integer roots of single-variable polynomials modulo an integer, as well as bivariate polynomials over the integers. In the case of modular roots, Coppersmith's ideas were reinterpreted by Howgrave-Graham [13]. We further provide Howgrave-Graham result.

Theorem 1. *Let $f(x_1, \ldots, x_n) = \sum a_{i_1 \ldots i_n} x_1^{i_1} \ldots x_n^{i_n} \in \mathbb{Z}[x_1, \ldots, x_n]$ be a polynomial with at most ω monomials, α be an integer and let*

$$||f(x_1, \ldots, x_n)|| = \sqrt{\sum |a_{i_1 \ldots i_n}|^2}$$

be its norm. Suppose that

- *$f(y_1, \ldots, y_n) \equiv 0 \bmod \alpha$ for some $|y_1| < X_1, \ldots, |y_n| < X_n$,*
- *$||f(y_1 X_1, \ldots, y_n X_n)|| < \alpha/\sqrt{\omega}$,*

then $f(y_1, \ldots, y_n) = 0$ holds over integers.

Lenstra, Lenstra and Lovász [16] proposed a lattice reduction algorithm (LLL) that is widely used in cryptanalysis and is typically combined with Howgrave-Graham's lemma. We further provide the version presented in [14, 17].

Theorem 2. *Let L be a lattice of dimension ω. In polynomial time, the LLL algorithm outputs a reduced basis $(b_1, \ldots, b_\omega)$ that satisfies*

$$||b_1|| \leq \ldots \leq ||b_i|| \leq 2^{\frac{\omega(\omega-1)}{4(\omega+1-i)}} det(L)^{\frac{1}{\omega+1-i}},$$

where $det(L)$ is the determinant of lattice L.

Note that the condition

$$2^{\frac{\omega(\omega-1)}{4(\omega+1-i)}} det(L)^{\frac{1}{\omega+1-i}} < \alpha/\sqrt{\omega}$$

implies that the polynomials corresponding to b_i match Howgrave-Graham's bound. This leads to

$$det(L) \leq \varepsilon \alpha^{\omega+1-i},$$

where ε is an error term that is usually ignored.

In order to find a solution $(y_1, \ldots, y_n)$ we need the following assumption to be true.

Assumption 3 *The LLL reduced basis polynomials are algebraically independent[4], and the resultant computations for b_i yields the common roots of these polynomials.*

[4] they do not share a non-trivial gcd

In [15], a lattice based method for finding small solutions of the equation $xH(y) + c \equiv 0 \bmod \beta$ is provided. This result extensions the Boneh and Durfee method [4] and uses the LLL algorithm [16] and Howgrave-Graham's lemma [13] to derive the solutions. The author shows that the bounds provided in [15] are optimal under reasonable assumptions.

Theorem 4. *Let $H(y) \in \mathbb{Z}[y]$ be a monic polynomial with degree $r \geq 1$ and β be an integer. Suppose that*

- $x_0 H(y_0) + c \equiv 0 \bmod \beta$ *for some* $|x_0| < X = \beta^\delta, |y_0| < Y = \beta^\gamma$,
- $|c| < XY^r$,

then one can solve the equation $xH(y) + c \equiv 0 \bmod \beta$ if

$$\begin{cases} \delta \leq \frac{r+2}{2(r+1)} - \frac{r+1}{2}\gamma & \textit{when } 0 < \gamma < r/(r+1)^2, \\ \delta \leq 1 - \sqrt{r\gamma}, & \textit{when } r/(r+1)^2 \leq \gamma \leq 1/r. \end{cases}$$

3 A New Look at φ_n

In this section we analyze the group's order and show that it can be expressed as a polynomial in $p + q$ with integer coefficients. This polynomial is later used to derive $H(y)$, and thus we are able to apply Kunihiro's result. We also provide a recurrence relation for φ_n.

Proposition 1. *Let N be a positive integer. Then for any integers $n \geq 1$ the following property holds*

$$\varphi_n(N) = -(p+q)^n + \sum_{k=0}^{n-1} a_k (p+q)^k,$$

where $a_k \in \mathbb{Z}$.

Proof. Using the roots of unity we can express $x^n - 1$ as a product of linear factors

$$x^n - 1 = \prod_{k=0}^{n-1} (x - e^{2i\pi k/n}),$$

where e is Euler's constant and $i^2 = -1$. Using the fact that

$$e^{2(n-i)\pi k/n} = e^{2\pi k} e^{-2i\pi k/n} = e^{-2i\pi k/n}$$

we obtain that

$$x^n - 1 = \begin{cases} (x-1)\prod_{k=1}^{j}(x - e^{2i\pi k/n})(x - e^{-2i\pi k/n}), & \text{when } n = 2j+1, \\ (x^2-1)\prod_{k=1}^{j-1}(x - e^{2i\pi k/n})(x - e^{-2i\pi k/n}), & \text{when } n = 2j. \end{cases}$$

Let α be an integer. We have the following relation

$$\begin{aligned}
e^{\alpha i\pi k/n} + e^{-\alpha i\pi k/n} &= \cos\left(\frac{\alpha\pi k}{n}\right) + i\sin\left(\frac{\alpha\pi k}{n}\right) + \cos\left(\frac{-\alpha\pi k}{n}\right) + i\sin\left(\frac{-\alpha\pi k}{n}\right)\\
&= \cos\left(\frac{\alpha\pi k}{n}\right) + i\sin\left(\frac{\alpha\pi k}{n}\right) + \cos\left(\frac{\alpha\pi k}{n}\right) - i\sin\left(\frac{\alpha\pi k}{n}\right)\\
&= 2\cos\left(\frac{\alpha\pi k}{n}\right). \qquad (1)
\end{aligned}$$

Let $S = p + q$. For $n = 2j + 1$ we have

$$\begin{aligned}
\varphi_n(N) &= (p^n - 1)(q^n - 1)\\
&= (p-1)(q-1)\prod_{k=1}^{j}(p - e^{2i\pi k/n})(p - e^{-2i\pi k/n})(q - e^{2i\pi k/n})(q - e^{-2i\pi k/n})\\
&= (N - S + 1)\prod_{k=1}^{j}(N - Se^{2i\pi k/n} + e^{4i\pi k/n})(N - Se^{-2i\pi k/n} + e^{-4i\pi k/n})\\
&= (N - S + 1)\prod_{k=1}^{j}\left(N^2 - 2S(N+1)\cos\left(\frac{2\pi k}{n}\right) + 2N\cos\left(\frac{4\pi k}{n}\right) + S^2 + 1\right)\\
&= -S^{2j+1} + \sum_{k=0}^{2j} a_k S^k,
\end{aligned}$$

where for the fourth equality we used Equation (1). Since $\varphi_n(N) \in \mathbb{Z}$, we obtain that $a_k \in \mathbb{Z}$ for all k.

When $n = 2j$, using Equation (1) we obtain

$$\begin{aligned}
\varphi_n(N) &= (p^2 - 1)(q^2 - 1)\prod_{k=1}^{j-1}(p - e^{2i\pi k/n})(p - e^{-2i\pi k/n})(q - e^{2i\pi k/n})(q - e^{-2i\pi k/n})\\
&= (N^2 - S^2 + 2N + 1)\prod_{k=1}^{j-1}\left(N^2 - 2S(N+1)\cos\left(\frac{2\pi k}{n}\right) + 2N\cos\left(\frac{4\pi k}{n}\right) + S^2 + 1\right)\\
&= -S^{2j} + \sum_{k=0}^{2j-1} a_k S^k.
\end{aligned}$$

Again, since $\varphi_n(N) \in \mathbb{Z}$, we obtain that $a_k \in \mathbb{Z}$ for all k. This concludes our proof. □

Our attack relies on expressing φ_n as a polynomial in N and S. To ease the computation of the a_k values, we further provide a recurrence relation for φ_n.

Lemma 2. *Let $N = pq$ and $S = p + q$ be two positive integers. Then for any integers $n \geq 2$ the following property holds*

$$\varphi_n(N) = (N^{n-1} + 1)(N - S + 1) + S\varphi_{n-1}(N) + N\varphi_{n-2}(N),$$

where $\varphi_0(N) = 0$ and $\varphi_1(N) = N - S + 1$.

Proof. For $n \geq 2$ we have the following

$$\begin{aligned}
p^n + q^n &= (p+q)(p^{n-1} + q^{n-1}) - pq(p^{n-2} + q^{n-2})\\
&= S(p^{n-1} + q^{n-1}) - N(p^{n-2} + q^{n-2})\\
&= S(N^{n-1} + 1 - \varphi_{n-1}(N)) - N(N^{n-2} + 1 - \varphi_{n-2}(N))\\
&= (S-1)N^{n-1} + S - N - S\varphi_{n-1}(N) + N\varphi_{n-2}(N).
\end{aligned}$$

which leads to

$$\begin{aligned}\varphi_n(N) &= N^n + 1 - (p^n + q^n)\\ &= N^n + 1 - (S-1)N^{n-1} - S + N + S\varphi_{n-1}(N) - N\varphi_{n-2}(N)\\ &= (N^{n-1}+1)(N - S + 1) + S\varphi_{n-1}(N) - N\varphi_{n-2}(N),\end{aligned}$$

just as desired. □

Using Lemma 2, we can compute the first few values for φ_n as a polynomial in $p+q$

$$\begin{aligned}\varphi_2 &= N^2 + 2N - S^2 + 1,\\ \varphi_3 &= N^3 + 3NS - S^3 + 1,\\ \varphi_4 &= N^4 - 2N^2 + 4NS^2 - S^4 + 1,\\ \varphi_5 &= N^5 - 5N^2S + 5NS^3 - S^5 + 1,\\ \varphi_6 &= N^6 + 2N^3 - 9N^2S^2 + 6NS^4 - S^6 + 1,\\ \varphi_7 &= N^7 + 7N^3S - 14N^2S^3 + 7NS^5 - S^7 + 1,\\ \varphi_8 &= N^8 - 2N^4 + 16N^3S^2 - 20N^2S^4 + 8NS^6 - S^8 + 1,\\ \varphi_9 &= N^9 - 9N^4S + 30N^3S^3 - 27N^2S^5 + 9NS^7 - S^9 + 1.\end{aligned}$$

4 Application of Lattices

We further provide a method for finding the factorisation of N when d is small enough.

Theorem 5. *Let $N = pq$ be the product of two unknown primes with $q < p < 2q$. Also, let $e = N^\delta$ and $d < N^\gamma$. We can factor N in polynomial time if*

$$\begin{cases}\gamma \le n - \sqrt{0.5n\delta}, & \text{when } \frac{n}{2} \le \delta \le \frac{(n+1)^2}{2n},\\ \gamma \le \frac{3n-1}{4} - \frac{n\delta}{2(n+1)}, & \text{when } \frac{(n+1)^2}{2n} < \delta \le \frac{(n+1)(3n-1)}{2n}.\end{cases}$$

Proof. According to Proposition 1 we have that

$$\varphi_n(N) = -(p+q)^n + \sum_{k=0}^{n-1} a_k (p+q)^k,$$

where $a_k \in \mathbb{Z}$. Finding $p+q$ is equivalent to solving the equation

$$h(y) = -y^n + \sum_{k=0}^{n-1} a_k y^k,$$

or analogously the monic polynomial $H(y) = -h(y)$.

By rewriting the key equation $ed - k\varphi_n(N) = 1$, we obtain the congruence $k\varphi_n(N) + 1 \equiv 0 \bmod e$, that is equivalent to $k(-\varphi_n(N)) - 1 \equiv 0 \bmod e$. Consequently, we deduce the equation $xH(y) - 1 \equiv 0 \bmod e$, which has k and $p+q$ as solutions.

In order to be able to apply Theorem 4 we first need to bound k and $p+q$. Since $k\varphi_n(N) = ed - 1 < ed$ and $N^n < \varphi(N)$ (see Corollary 1), we obtain that

$$k < \frac{ed}{\varphi_n(N)} < N^{\delta+\gamma-n}.$$

Using Lemma 1 we have that $p + q < 3\sqrt{N}$. Therefore, we have that $k < X = e^{(\delta+\gamma-n)/\delta}$ and $p + q < Y \simeq e^{0.5/\delta}$.

According to Theorem 4, we can find the solutions $x_0 = k$ and $y_0 = p+q$ to equation $xH(y) - 1 \equiv 0 \bmod e$ if certain conditions are met.

Let consider the first case of Theorem 4. We have

$$0 \leq \frac{1}{2\delta} < \frac{n}{(n+1)^2} \Leftrightarrow \frac{(n+1)^2}{2n} < \delta$$

and

$$\begin{aligned}\frac{\delta+\gamma-n}{\delta} \leq \frac{n+2}{2(n+1)} - \frac{n+1}{2}\cdot\frac{1}{2\delta} &\Leftrightarrow \delta+\gamma-n \leq \frac{(n+2)\delta}{2(n+1)} - \frac{n+1}{4}\\ &\Leftrightarrow \gamma \leq n - \frac{n+1}{4} + \left(\frac{n+2}{2(n+1)} - 1\right)\delta\\ &\Leftrightarrow \gamma \leq \frac{3n-1}{4} - \frac{n\delta}{2(n+1)}.\end{aligned}$$

Since we also want $\gamma \geq 0$ we must have

$$0 \leq -\frac{n\delta}{2(n+1)} + \frac{3n-1}{4} \Leftrightarrow \delta \leq \frac{(n+1)(3n-1)}{2n}.$$

In the second case of Theorem 4 we have

$$\frac{n}{(n+1)^2} \leq \frac{1}{2\delta} \leq \frac{1}{n} \Leftrightarrow \frac{n}{2} \leq \delta \leq \frac{(n+1)^2}{2n}$$

and

$$\begin{aligned}\frac{\delta+\gamma-n}{\delta} \leq 1 - \frac{\sqrt{n}}{\sqrt{2\delta}} &\Leftrightarrow \delta+\gamma-n \leq \delta - \sqrt{0.5n\delta}\\ &\Leftrightarrow \gamma \leq n - \sqrt{0.5n\delta}.\end{aligned}$$

Since we also want $\gamma \geq 0$ we must have

$$0 \leq n - \sqrt{0.5n\delta} \Leftrightarrow \delta \leq 2n.$$

Once y_0 is found, solving the following system of equations

$$\begin{cases} p + q = y_0 \\ pq = N \end{cases}$$

enables us to factorise the modulus N. □

The following corollary tells us what happens when e is large enough.

Corollary 2. *Let $N = pq$ be the product of two unknown primes with $q < p < 2q$. Also, let $e \simeq N^n$ and $d < N^\gamma$. We can factor N in polynomial time if*

$$\begin{cases} \gamma \leq n(1 - \sqrt{0.5}), & \textit{when } n = 1 \textit{ or } n = 2, \\ \gamma \leq \frac{3n-1}{4} - \frac{n^2}{2(n+1)}, & \textit{otherwise.} \end{cases}$$

Proof. In the first case we must have $n/2 \leq n \leq (n+1)^2/2n$. The first inequality is always true. Lets check the conditions for the second one

$$n \leq \frac{(n+1)^2}{2n} \Leftrightarrow 2n^2 \leq n^2 + 2n + 1 \Leftrightarrow (n-1)^2 \leq 2 \Leftrightarrow n \leq \sqrt{2} + 1 \simeq 2.41.$$

Thus, the second inequality is true only for $n = 1$ or $n = 2$.

In the second case, according to the previous statements, we automatically have $(n+1)^2/2n < n$ for $n \geq 3$. Therefore, we only need to check if

$$n \leq \frac{(n+1)(3n-1)}{2n} \Leftrightarrow 2n^2 \leq 3n^2 + 2n - 1 \Leftrightarrow 2 \leq (n+1)^2.$$

This inequality is always true for $n \geq 3$. This concludes our proof. □

When cases $n = 1$ and $n = 2$ are considered, the optimal bounds presented in [4, 12] for RSA and [21, 26] for Elkamchouchi *et al.*'s scheme become special cases of Corollary 2.

Corollary 3. *Let $N = pq$ be the product of two unknown primes with $q < p < 2q$. Also, let $n = 1$, $e \simeq N$ and $d < N^\gamma$. We can factor N in polynomial time if $\gamma \leq (2 - \sqrt{2})/2 \simeq 0.292$.*

Corollary 4. *Let $N = pq$ be the product of two unknown primes with $q < p < 2q$. Also, let $n = 2$, $e \simeq N^2$ and $d < N^\gamma$. We can factor N in polynomial time if $\gamma \leq 2 - \sqrt{2} \simeq 0.585$.*

Remark 2. In [20], 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 [20].

4.1 Lattices versus Continued Fractions

According [10], we can recover the secret exponent d using an attack based on continued fractions if the following bound holds

$$\log_2(d) < 0.5(1.5n - \delta)\log_2(N).$$

The previous bound is equivalent to

$$\gamma < 0.75n - 0.5\delta,$$

when $e = N^\delta$ and $d < N^\gamma$.

To compare the continued fractions bound with the lattice based ones, we need to consider two cases. In the first case, $n/2 \leq \delta \leq (n+1)^2/2n$, we have that the difference is

$$D_0 = n - \frac{\sqrt{2n\delta}}{2} - \frac{3n}{4} + \frac{\delta}{2} = \frac{n + 2\delta - 2\sqrt{2n\delta}}{4}.$$

To see that $D_0 > 0$ we rewrite it as

$$n + 2\delta > 2\sqrt{2n\delta} \Leftrightarrow n^2 + 4\delta^2 + 4n\delta > 8n\delta \Leftrightarrow (n - 2\delta)^2 > 0,$$

which is always true. Therefore, in this case the lattice attack is always better than the continued fraction attack of [10].

In the second case, $(n+1)^2/2n < \delta \leq (n+1)(3n-1)/2n$, we have that the difference is

$$D_1 = \frac{3n-1}{4} - \frac{n\delta}{2(n+1)} - \frac{3n}{4} + \frac{\delta}{2} = \frac{\delta}{2(n+1)} - \frac{1}{4}.$$

The difference D_1 is positive once $\delta > (n+1)/2$. Since $(n+1)^2/2n > (n+1)/2$, the condition $D_1 > 0$ is met. Hence, we obtain the same result as in the first case.

5 Experimental Results

To check the validity of our result, we ran the code for our attack [2] on a workstation using Ubuntu 20.04.1, with the following specifications: Intel(R) Core(TM) i7-1165G7 CPU 2.80GHz with 8 cores and 16 Gigabytes of RAM. The programming language we used for implementing our attack was SageMath 10.3. We based our code on the Boneh-Durfee attack implementation found in [25].

For $n = 3$ we used the following parameters

$$\begin{aligned} N &= 30149726335030403365902265083163510227689133 23933,\\ e &= 6533219229319375155841652794855616437173116 9655155\\ &\ 0689661966133765127824043894656155756279180 0951772\\ &\ 99327928182942709277283882982169138979615253. \end{aligned}$$

Remark that $e \simeq N^{2.966}$ and the equation is $xH(y) - 1 \equiv 0 \bmod e$, where

$$H(y) = y^3 - 3Ny - N^3 - 1.$$

Using the notations from [15], we set the bounds

$$\begin{aligned}
X &= 1223404362148854061445173739 52 \simeq N^{0.6},\\
Y &= 173636765504977093263360 0 \simeq N^{0.5},\\
Z &= XY^3 + |-1|\\
&= 6404645352802741504214236211001940001519012\\
&\quad\ 9395671373426965878351755901829539946543645\\
&\quad\ 5016333311999999 \simeq N^{2.099}
\end{aligned}$$

and the lattice parameters $m = 5$ and $\tau = 1$. The size of the lattice is $\omega = 77$.

Let $\bar{f}(x, y, z) = xH(y) - 1$. We define the shift polynomials

$$\bar{g}_{[i,j,k]} = x^i y^j \bar{f}(x, y, z)^k e^{m-k}.$$

We construct the lattice $\mathcal{L}$ using the coefficients of the polynomials defined by

$$\begin{cases}
\bar{g}_{[u-i,j,i]} & \text{, for } u = 0, \ldots, m; i = 0, \ldots u; j = 0, \ldots, n-1;\\
\bar{g}_{[0,j,u]} & \text{, for } u = 0, \ldots, m; j = n, \ldots, n + \tau u - 1.
\end{cases}$$

Then we reduce the lattice using LLL, look for independent vectors in $\mathcal{L}$, compute the resultant and derive the solutions

$$\begin{aligned}
x_0 &= 29164002913657120804207335 03,\\
y_0 &= 354208390765907302551462 6.
\end{aligned}$$

We know that $p + q = y_0$. Therefore, we can combine y_0 with N to find the prime factors

$$\begin{aligned}
p &= 211977819903685906870781 9,\\
q &= 142230570862221395680680 7.
\end{aligned}$$

Note that our attack takes around 6 seconds to find p and q.

6 Conclusions

In this paper, we presented a lattice based small private key attack against a family of RSA-like cryptosystems. To mount our attack we first reduce the problem to solving the equation $xH(y) - 1 \equiv 0 \bmod e$, after which we apply a result proven by Kunihiro [15]. The resulting bound improves the previous one, which was based on continued fractions and presented in [10]. In the cases of RSA and Elkamchouchi *et al.*'s scheme, our derived bounds reduce to the optimal bounds found in [4, 12] and [21, 26], respectively. Additionally, our attack works by factorising the modulus, and thus addressing an open problem left in [10].

Future Work. An interesting research direction, is to find out whether the attacks presented in [3,10,18,23,23] for the RSA and Elkamchouchi *et al.*'s schemes are applicable in the general case.

References

1. Abderrahmane Nitaj, N.N.H.A., Ariffin, M.R.B.K.: Cryptanalysis of a New Variant of the RSA Cryptosystem. In: AFRICACRYPT 2024. Springer (2024)
2. Author, N.: No Title. For anonimity the Github repositry will be published after acceptance.
3. Boneh, D.: Twenty Years of Attacks on the RSA Cryptosystem. Notices of the AMS **46**(2), 203–213 (1999)
4. 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)
5. 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)
6. Coppersmith, D.: Finding a Small Root of a Bivariate Integer Equation; Factoring with High Bits Known. In: EUROCRYPT 1996. Lecture Notes in Computer Science, vol. 1070, pp. 178–189. Springer (1996)
7. Coppersmith, D.: Finding a Small Root of a Univariate Modular Equation. In: EUROCRYPT 1996. Lecture Notes in Computer Science, vol. 1070, pp. 155–165. Springer (1996)
8. Coppersmith, D.: Small Solutions to Polynomial Equations, and Low Exponent RSA Vulnerabilities. Journal of Cryptology **10**(4), 233–260 (1997)
9. Cotan, P., Teşeleanu, G.: Continued Fractions Applied to a Family of RSA-like Cryptosystems. In: ISPEC 2022. pp. 589–605. Springer (2022)
10. 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)
11. 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)
12. 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)
13. Howgrave-Graham, N.: Finding small roots of univariate modular equations revisited. In: IMA 1997. Lecture Notes in Computer Science, vol. 1355, pp. 131–142. Springer (1997)
14. Jochemsz, E., May, A.: A Strategy for Finding Roots of Multivariate Polynomials with New Applications in Attacking RSA Variants. In: ASIACRYPT 2006. Lecture Notes in Computer Science, vol. 4284, pp. 267–282. Springer (2006)
15. Kunihiro, N.: On Optimal Bounds of Small Inverse Problems and Approximate GCD Problems with Higher Degree. In: ISC 2012. Lecture Notes in Computer Science, vol. 7483, pp. 55–69. Springer (2012)
16. Lenstra, A.K., Lenstra, H.W., Lovász, L.: Factoring Polynomials with Rational Coefficients. Mathematische Annalen **261**, 515–534 (1982)

17. May, A.: New RSA Vulnerabilities Using Lattice Reduction Methods. Ph.D. thesis, University of Paderborn (2003)
18. May, A.: Using LLL-Reduction for Solving RSA and Factorization Problems. In: The LLL Algorithm: Survey and Applications, pp. 315–348. Information Security and Cryptography, Springer (2010)
19. 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)
20. Padhye, S.: A Public Key Cryptosystem Based on Pell Equation. IACR Cryptology ePrint Archive **2006/191** (2006)
21. 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)
22. 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)
23. 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)
24. Wiener, M.J.: Cryptanalysis of Short RSA Secret Exponents. IEEE Trans. Inf. Theory **36**(3), 553–558 (1990)
25. Wong, D.: Lattice Based Attacks on RSA. https://github.com/mimoo/RSA-and-LLL-attacks
26. 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)