Classical Attacks on a Variant of the RSA Cryptosystem

Abderrahmane Nitaj[1(✉)], Muhammad Rezal Bin Kamel Ariffin[2], Nurul Nur Hanisah Adenan[2], and Nur Azman Abu[3]

[1] *Normandie Univ, UNICAEN, CNRS, LMNO, 14000 Caen, France
abderrahmane.nitaj@unicaen.fr
[2] Institute for Mathematical Research, Universiti Putra Malaysia, 43400 Serdang
Selangor, Malaysia
[3] Faculty of Information Technology and Communication Technology, Universiti
Teknikal Malaysia, Melaka, Malaysia

Abstract. Let $N = pq$ be an RSA modulus with balanced prime factors. In 2018, Murru and Saettone presented a variant of the RSA cryptosystem based on a cubic Pell equation in which the public key (N, e) and the private key (N, d) satisfy $ed \equiv 1 \pmod{(p^2+p+1)(q^2+q+1)}$. They claimed that the classical small private attacks on RSA such as Wiener's continued fraction attack do not apply to their scheme. In this paper, we show that, on the contrary, Wiener's method as well as the small inverse problem technique of Boneh and Durfee can be applied to attack their scheme. More precisely, we show that the proposed variant of RSA can be broken if $d < N^{0.5694}$. This shows that their scheme is in reality more vulnerable than RSA, where the bound of vulnerability is $d < N^{0.292}$.

相反

Keywords: RSA, Factorization, Continued fractions, Small inverse problem, Coppersmith's method

1 Introduction

Data transaction during early 70's was conducted using symmetric cryptosystems which means the same key were used for encryption and decryption processes. However, problems on distributing keys arose as the number of users increased. In 1976, this problem was solved mathematically by Diffie and Hellman [10], and improved in 1978 by Rivest, Shamir and Adleman [23]. Rivest, Shamir and Adleman invented an elegant cryptosytem named RSA which utilized different keys for encryption and decryption algorithms. The construction of RSA begins with key generation process. Let $N = pq$ be the modulus of RSA where p and q are large primes. To resist the factorization attacks, it is recommended that p and q should be of the same bitsize, that is $q < p < 2q$. Let e be an integer such that $\gcd(e, \phi(N)) = 1$ where $\phi(N) = (p-1)(q-1)$ is Euler-totient function. Let $d \equiv e^{-1} \pmod{\phi(N)}$. The key (N, e) is public while $p, q, d, \phi(N)$ are kept secret. For encryption and decryption processes, both involve modulo operations. To encrypt a message m, one needs to compute $c \equiv m^e \pmod N$

while to decrypt and retrieve back the message, one needs to compute $m \equiv c^d \pmod{N}$.

It can be seen that the private exponent d is needed to decrypt the ciphertext c. Note that the cost incurred to decrypt increases directly proportional with the size of d. Thus, one would prefer to use small value of d. Unfortunately, Wiener [27] showed that the cryptosystem that employ a small value of d is vulnerable. Wiener showed that for $d < \frac{1}{3}N^{\frac{1}{4}}$, one could retrieve d via the continued fraction expansion of $\frac{e}{N}$ and thus factor the modulus N. This bound was then improved by Boneh and Durfee [6] up to $d < N^{0.292}$. Later in 2004, Blömer and May [2] described a generalized Wiener's attack. Utilizing the combination of lattice reduction and continued fraction, Blömer and May showed that if there exists three integers x, y, z such that $ex - y\phi(N) = z$ with $x < \frac{1}{3}N^{\frac{1}{4}}$ and $|z| < exN^{-3/4}$, then N can be factored.

Since then, researchers studied thoroughly on this cryptosystem in order to find any other weakness that could lead to the vulnerabilities of RSA. They found that, any leakage on either of the primes could lead to the factorization of N. In 1996, Coppersmith [8] showed that RSA is susceptible given only half of the most significant bits of one of the primes. Later, Boneh et al. [4] showed that if one knew half of the least significant bit of either prime p or q, then RSA can be factored. Ernest et al. [11] and Boneh et al. [4] also worked upon this matter and they showed that indeed RSA is susceptible if one knows some information on bits of either most significant bits (MSBs) or least significant bits (LSBs) of private exponents.

Meanwhile, some researchers began to design variants of the RSA cryptosystem purposely to enhance its security. Takagi [25] was the first that designed a variant of RSA using the modulus $N = p^{r-1}q$ for $r \geq 3$ and showed that this scheme is more efficient in both its key generation and decryption algorithms. However, the studies from [5], [24], [1] showed that this variant of RSA is also insecure from attacks if certain conditions are satisfied.

In 2018, another scheme was invented by Murru and Saettone [21]. They introduced a new variant of the RSA cryptosystem based on the cubic Pell equation $x^3 + ry^3 + r^2z^3 - 3rxyz = 1$. In their cryptosystem, they utilized the standard modulus $N = pq$, a public exponent e, a private exponent d, and the key equation $ed - k\psi(N) = 1$ with $\psi(N) = (p^2 + p + 1)(q^2 + q + 1)$. The authors investigated the proposed cryptosystem for efficiency and security, and claimed that the attack of Wiener is not usable against their scheme.

In this paper, we show that the attack of Wiener, as well as the method of Boneh and Durfee, can be applied to factor $N = pq$ with $q < p < 2q$ when the decryption exponent d is sufficiently small. More precisely, we set $e = N^\alpha$, and $d = N^\delta$, and we show that Wiener's attack can solve the equation $ed - k\psi(N) = 1$ and factor N if $\delta < \frac{5}{4} - \frac{1}{2}\alpha$. In the normal case where $e \approx N^2$, the bound becomes $d < N^{\frac{1}{4}}$. Astonishingly, this is roughly the same bound than the classical bound obtained by Wiener's method for standard RSA. Similarly, we show that the method of Boneh and Durfee can be applied if $\delta < \frac{7}{3} - \frac{2}{3}\sqrt{3\alpha + 1}$. When $e \approx N^2$, the bound reduces to $d < N^{0.5694}$. Here, we observe that 0.5694 is twice the weaker bound 0.2847 obtained by Boneh and Durfee [6] with the small inverse problem attack on RSA.

The framework of this paper is as follows. In Section 2 and Section 3, we describe some important tools and useful lemmas respectively. In Section 4, we present our first results while Section 5 presents our second results. We conclude the paper in Section 6.

2 Preliminaries

In this section, we summarize the scheme of Murru and Saettone [21], and describe briefly on some important tools that are needed in our attacks.

2.1 The scheme of Murru and Saettone

Let $(\mathbb{F}, +, \cdot)$ be a field, and $r \in \mathbb{F}$ be a non-cubic integer. Then the polynomial $t^3 - r$ is irreducible in $\mathbb{F}[t]$, and the quotient field $\mathbb{A} = \mathbb{F}[t]/\left(t^3 - r\right)$ is the set of elements of the form $x + ty + t^2 z$ with $(x, y, z) \in \mathbb{F}^3$. A product $\bullet$ between the elements of $\mathbb{A}$ can be conducted by the rule

$$\begin{aligned}(x_1, y_1, z_1) &\bullet (x_2, y_2, z_2)\\ &= ((x_1x_2 + (y_2z_1 + y_1z_2)r, x_2y_1 + x_1y_2 + rz_1z_2, y_1y_2 + x_2z_1 + x_1z_2).\end{aligned}$$

The norm of an element $x + ty + t^2 z \in \mathbb{A}$ is defined by

标注

$$N(x, y, z) = x^3 + ry^3 + r^2z^3 - 3rxyz.$$

The cubic Pell equation is defined by the solutions $(x, y, z) \in \mathbb{F}^3$ of the equation $N(x, y, z) = 1$. The solutions form the commutative group $(\mathcal{C}, \bullet)$ where

$$\mathcal{C} = \left\{(x, y, z) \in \mathbb{F}^3,\ x^3 + ry^3 + r^2z^3 - 3rxyz = 1\right\}.$$

In $(\mathcal{C}, \bullet)$, the identity is $(1, 0, 0)$ and the inverse of $(x, y, z) \in \mathcal{C}$ is $(x, y, z)^{-1} = \left(x^2 - ryz, rz^2 - xy, y^2 - xz\right)$. Next, let $B = \mathbb{A}^*/\mathbb{F}^*$ be the quotient group. Let $\alpha \notin \mathbb{F}$ be fixed. The elements of B are of one of the forms $m + nt + t^2$, or $m + t$, or 1. As a consequence, B reduces to

$$B = (\mathbb{F} \times \mathbb{F}) \cup (\mathbb{F} \times \{\alpha\}) \cup \{(\alpha, \alpha)\},$$

where (α, α) will play the point at infinity for the addition operation $\odot$ defined by the following cases

- $(m, \alpha) \odot (p, \alpha) = (mp, m + p)$,
- if $n + p \neq 0$, then $(m, n) \odot (p, \alpha) = \left(\frac{mp+r}{n+p}, \frac{m+np}{n+p}\right)$,
- if $n + p = 0$ and $m - n^2 \neq 0$, then $(m, n) \odot (p, \alpha) = \left(\frac{mp+r}{m-n^2}, \alpha\right)$,
- if $n + p = 0$ and $m - n^2 = 0$, then $(m, n) \odot (p, \alpha) = (\alpha, \alpha)$,

ADDITION

RULE

$\alpha^{p^2+p+1} \equiv 1 \ (\mathrm{mod}\ p)$

$a^{p-1} \equiv 1 \ \mathrm{mod}\ (p)$ 正常

- if $m+p+nq \neq 0$, then $(m,n) \odot (p,q) = \left(\frac{mp+(n+q)r}{m+p+nq}, \frac{np+mq+r}{m+p+nq}\right)$,
- if $m+p+nq = 0$ and $np+mq+r \neq 0$, then $(m,n) \odot (p,q) = \left(\frac{mp+(n+q)r}{np+mq+r}, \alpha\right)$,
- if $m+p+nq = 0$ and $np+mq+r = 0$, then $(m,n) \odot (p,q) = (\alpha, \alpha)$,

Then $(B, \odot)$ is a 交换群 commutative group, and the scheme of Murru and Saettone [21] is based on the cubic Pell equation $x^3 + ry^3 + r^2z^3 - 3rxyz = 1$ where r is a 非三次整数 non-cubic integer. When $\mathbb{F} = \mathbb{Z}/p\mathbb{Z}$ where p is a prime number, one can take $\alpha = \infty$, and $\mathbb{A} = \mathbb{F}_{p^3}$ is the Galois field with p^3 elements. Hence, $B = B_p$ is a cyclic group of order p^2+p+1, and for every $(m,n) \in B_p$, one has $(m,n)^{\odot(p^2+p+1)} = (\alpha, \alpha) \pmod p$ where $x^{\odot k} = x \odot x \odot \cdots x$ (k times). Using these facts, a variant of the RSA cryptosystem can be built by choosing an RSA modulus $N = pq$, an integer r which is non-cubic modulo p, q, and N, and by combing the cyclic groups B_p and B_q. In this scheme, the public exponent is an [illegible] integer e satisfying $\gcd\left(e, \left(p^2+p+1\right)\left(q^2+q+1\right)\right) = 1$. To encrypt a message $M \in B$, the operation is $C = M^{\odot e} \pmod N$, and to decrypt C, the operation is $M = C^{\odot d} \pmod N$ where $d \equiv e^{-1} \pmod{\left(p^2+p+1\right)\left(q^2+q+1\right)}$. We notice that the idea of constructing a variant of RSA based on a cubic curve has already been used in [17,18,16,7]. We also notice that the XTR cryptosystem [20] uses the arithmetic that consists of representing the elements of $\mathbb{F}^*_{p^6}$ with order dividing $p^2 - p + 1$ by their trace over $\mathbb{F}^2_p$.

$\varphi_{\odot}(n)$?

In [21], the efficiency and the security of the RSA variant are studied. The authors claim that classical small exponent attacks such as Wiener's continued fraction attack can not be applied since the trapdoor function is not a simple monomial power as in RSA. In this paper, we show that Wiener's attack as well as Boneh and Durfee lattice reduction based attack can be applied to this variant of RSA. Moreover, we show that it is more vulnerable in general than RSA.

2.2 Continued fraction

The continued fraction expansion of a real number ξ can be written in the form

$$\xi = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \cdots}}}} \tag{1}$$

where $a_0 \in \mathbb{Z}$ and $a_i \in \mathbb{Z}^+$ are the partial quotients. The form in (1) is often expressed as $\xi = [a_0, a_1, \ldots, a_n]$. Thus, for $i \geq 0$, every rational number $\frac{r}{s}$, such that

$$\frac{r}{s} = [a_0, a_1, \ldots, a_n]$$

is a convergent of the continued fraction expansion of ξ. The continued fraction expansion is finite if ξ is a rational number. Moreover, r and s are coprime. The following theorem is a tool to test if a rational number $\frac{r}{s}$ is a convergent of ξ (see [12], Theorem 184).

Theorem 1. *Let ξ be a positive number. Suppose that* $\gcd(r,s)=1$ *and*

$$\left|\xi-\frac{r}{s}\right|<\frac{1}{2s^2}.$$

Then $\frac{r}{s}$ is a convergent of the continued fraction expansion of ξ.

2.3 Lattices and Coppersmith's method

Let ω and n be two positive integers. Let $u_1,\cdots,u_\omega\in\mathbb{R}^n$ be a set of ω linearly independent vectors. A lattice $\mathcal{L}$ is constructed based on the linear combinations of $u_1,\ldots,u_\omega$ such that $\mathcal{L}=\{\sum_{i=1}^{\omega}\lambda_i u_i|\ \lambda_i\in\mathbb{Z}\}$. For full ranked lattice which means $\omega=n$, the determinant is defined as $\det(\mathcal{L})=(\det(UU^T))^{\frac{1}{2}}=|\det(U)|$. In 1982, Lenstra, Lenstra, and Lovász [19] introduced an important algorithm called LLL that is used to produce a reduced basis with optimal properties. Their result is described as follows.

Theorem 2 (LLL). *Let $\mathcal{L}$ be a lattice that is constructed by a basis $(u_1,\ldots,u_\omega)$. The LLL algorithm yields a new basis $(b_1,\ldots,b_\omega)$ of L satisfying*

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

for $i=1,2,\ldots,\omega$.

One of the numerous applications of the LLL algorithm is Coppersmith's method [8]. The method is suited to find the small solutions of an univariate polynomial modular equation $f(x)=0 \pmod N$, or a bivariate polynomial equation $f(x,y)=0$. Coppersmith's method has various applications, especially in cryptanalysis, and has been extended to more variables. Two of the key ingredients in Coppersmith's method are lattice reduction and the following result, as reformulated by Howgrave-Graham [14].

Theorem 3 (Howgrave-Graham). *Let $h(x,y)=\sum a_{ij}x^iy^j\in\mathbb{Z}[x,y]\in\mathbb{Z}[x,y]$ be a polynomial with at most ω monomials and norm $\|h(x,y)\|=\sqrt{\sum a_{ij}^2}$. If $|x_0|<X$, $|y_0|<Y$, and*

$$h\left(x_0,y_0\right)\equiv 0 \pmod{e^m},\quad \|h(xX,yY)\|<\frac{e^m}{\sqrt{\omega}},$$

then $h\left(x_0,y_0\right)=0$ holds over the integers.

In this paper, we will consider the bivariate modular polynomial equation $f(x,y)=x(y^2+ay+b)+1\equiv 0 \pmod e$, where a, b, and e are fixed integers. To find the small solutions of this equation, we build a lattice $\mathcal{L}$ of dimension ω with a basis formed by the coefficients of a class of polynomials $G(x,y)$ derived from $f(x,y)$. Each polynomial $G(x,y)$ is such that $G(x,y)\equiv 0 \pmod{e^m}$ for a fixed integer m. Then, applying the LLL algorithm, we reduce the basis and construct new polynomials $h(x,y)$ such that $h(x,y)\equiv 0 \pmod{e^m}$. Under certain conditions, we have also $h(x,y)=0$ over the integers for some polynomials. Then, assuming that such polynomials are algebraically independent, we use Gröbner basis technique to find the common roots. The assumption can be formulated as follows.

Assumption 1 *The lattice reduced basis yields algebraically independent polynomials, and the common roots of these polynomials can be efficiently computed using the Gröbner basis technique.*

3 Useful Lemmas

Let $N = pq$ be an RSA modulus with $q < p < 2q$. The following result gives the bounds for p, and q in terms of N (See [22]).

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

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

The former lemma can be used to find an upper and a lower bound for $\psi(N)$.

Proposition 1. *Let $N = pq$ be the product of two unknown prime integers with $q < p < 2q$, and $\psi(N) = \left(p^2+p+1\right)\left(q^2+q+1\right)$. Then*

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

Proof. Plugging $q = \frac{N}{p}$ in $\psi(N) = \left(p^2+p+1\right)\left(q^2+q+1\right)$, we get a function f with p as a variable, namely

$$f(p) = \left(p^2+p+1\right)\left(\frac{N^2}{p^2}+\frac{N}{p}+1\right).$$

The derivative of f at p is

$$f'(p) = \frac{\left(p^2-N\right)\left(2p^2+(N+1)p+2N\right)}{p^3}.$$

By Lemma 1, we have $p^2 > N$, which implies $f'(p) > 0$. It follows that f is increasing with p. Also, by Lemma 1, we have $\sqrt{N} < p < \sqrt{2}\sqrt{N}$. Hence $f\left(\sqrt{N}\right) < f(p) < f\left(\sqrt{2}\sqrt{N}\right)$, which leads to

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

This terminates the proof. □

The former proposition can be used to find a good approximation for $\psi(N)$.

Proposition 2. *Let $N = pq$ be the product of two unknown prime integers with $q < p < 2q$, and*

$$\psi_0(N) = \frac{1}{2}\left(N+\sqrt{N}+1\right)^2 + \frac{1}{2}\left(N+\frac{3}{4}\sqrt{2}\sqrt{N}+1\right)^2 + \frac{3}{16}N.$$

Then

$$|\psi(N)-\psi_0(N)| < \frac{1}{2}N^{\frac{3}{2}}.$$

Proof. By Proposition 1, $\psi_0(N)$ is the mean value of the two bounds $\left(N+\sqrt{N}+1\right)^2$ and $\left(N+\frac{3}{4}\sqrt{2}\sqrt{N}+1\right)^2+\frac{3}{8}N$. Then

$$\begin{aligned}|\psi(N)-\psi_0(N)| &\leq \frac{1}{2}\left(\left(N+\frac{3}{4}\sqrt{2}\sqrt{N}+1\right)^2 - \left(N+\sqrt{N}+1\right)^2 + \frac{3}{8}N\right)\\ &= \frac{1}{2}\left(\frac{3}{4}\sqrt{2}-1\right)\sqrt{N}\left(2N+\left(\frac{3}{4}\sqrt{2}+1\right)\sqrt{N}+2\right)+\frac{3}{16}N\\ &= \left(\frac{3}{4}\sqrt{2}-1\right)N^{\frac{3}{2}}\left(1+\left(\frac{3}{8}\sqrt{2}+\frac{1}{2}\right)N^{-\frac{1}{2}}+N^{-2}\right)+\frac{3}{16}N\\ &< \frac{1}{2}N^{\frac{3}{2}},\end{aligned}$$

which is valid for all $N > 2$. This terminates the proof. □

The following result shows that one can factor the modulus $N = pq$ if $\psi(N)$ is known.

Proposition 3. *Let $N = pq$ be the product of two unknown integers with $q < p$. Suppose that $\psi(N) = \left(p^2+p+1\right)\left(q^2+q+1\right)$ is known. Then*

$$p = \frac{1}{2}\left(S+\sqrt{S^2-4N}\right), \quad q = \frac{1}{2}\left(S-\sqrt{S^2-4N}\right),$$

where

$$S = \frac{1}{2}\left(\sqrt{(N+1)^2+4\left(\psi(N)-(N^2-N+1)\right)}-(N+1)\right).$$

Proof. Expanding $\psi(N) = \left(p^2+p+1\right)\left(q^2+q+1\right)$ and rearranging, we get

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

Solving for $p+q$, we get

$$p+q = \frac{1}{2}\left(\sqrt{(N+1)^2+4\left(\psi(N)-(N^2-N+1)\right)}-(N+1)\right).$$

Let $S = \frac{1}{2}\left(\sqrt{(N+1)^2+4\left(\psi(N)-(N^2-N+1)\right)}-(N+1)\right)$. Using $q = \frac{N}{p}$, we get $p^2 - Sp + N = 0$. Then solving this equation for p, we get

$$p = \frac{1}{2}\left(S+\sqrt{S^2-4N}\right), \text{ and } q = \frac{1}{2}\left(S-\sqrt{S^2-4N}\right).$$

This gives the result. □

4 Application of Continued Fractions

In this section, we give an upper bound for d for which the continued fractions algorithm will succeed to find d and factor the modulus $N = pq$.

4.1 The attack

Theorem 4. *Let $N = pq$ be the product of two unknown prime numbers with $q < p < 2q$. Suppose that $ed - k\psi(N) = 1$ with $\psi(N) = \left(p^2+p+1\right)\left(q^2+q+1\right)$, $e = N^\alpha$, and $d = N^\delta$. Then, for $\frac{3}{2} < \alpha < \frac{5}{2}$, one can find d and factor N in polynomial time if*

$$\delta < \frac{5}{4} - \frac{1}{2}\alpha.$$

Proof. Suppose that $ed - k\psi(N) = 1$ with $\psi(N) = \left(p^2+p+1\right)\left(q^2+q+1\right)$. Let

$$\psi_0(N) = \frac{1}{2}\left(N + \sqrt{N} + 1\right)^2 + \frac{1}{2}\left(N + \frac{3}{4}\sqrt{2}\sqrt{N} + 1\right)^2 + \frac{3}{16}N.$$

Then

$$\left|\frac{k}{d} - \frac{e}{\psi_0(N)}\right| = \frac{|ed - k\psi_0(N)|}{d\psi_0(N)} \le \frac{|ed - k\psi(N)| + k|\psi(N) - \psi_0(N)|}{d\psi_0(N)}.$$

We have $|ed - k\psi(N)| = 1$, and, by Proposition 2, we have $|\psi(N) - \psi_0(N)| < \frac{1}{2}N^{\frac{3}{2}}$. Also, by Proposition 1, we have

$$\psi(N) > \left(N + \sqrt{N} + 1\right)^2 > N^2.$$

Using this, we get

$$\left|\frac{k}{d} - \frac{e}{\psi_0(N)}\right| < \frac{1 + \frac{1}{2}kN^{\frac{3}{2}}}{d\psi_0(N)} < \frac{k}{2d} \cdot \frac{2 + N^{\frac{3}{2}}}{\psi_0(N)}$$

By Proposition 1, we have

$$\psi_0(N) > \left(N + \sqrt{N} + 1\right)^2 > N^2 + 2\sqrt{N}.$$

Then

$$\left|\frac{k}{d} - \frac{e}{\psi_0(N)}\right| < \frac{k}{2d} \cdot \frac{2 + N^{\frac{3}{2}}}{N^2 + 2\sqrt{N}} = \frac{k}{2d\sqrt{N}}$$

Now, we have $k\psi(N) = ed - 1 < ed$, which leads to

$$\frac{k}{d} < \frac{e}{\psi(N)} < \frac{N^\alpha}{N^2} = N^{\alpha-2}.$$

We then obtain

$$\left|\frac{k}{d} - \frac{e}{\psi_0(N)}\right| < \frac{1}{2}\frac{N^{\alpha-2}}{\sqrt{N}} = \frac{1}{2}N^{\alpha-\frac{5}{2}}.$$

Now, if $\alpha - \frac{5}{2} < -2\delta$, that is $\delta < \frac{5}{4} - \frac{1}{2}\alpha$, then

$$\left|\frac{k}{d} - \frac{e}{\psi_0(N)}\right| < \frac{1}{2d^2}.$$

Consequently, by Theorem 1, $\frac{k}{d}$ is a convergent of $\frac{e}{\psi_0(N)}$ that can be computed by the continued fraction algorithm. Using $\frac{k}{d}$ in $ed - k\psi(N) = 1$, we get $\psi(N) = \frac{ed-1}{k}$. By Proposition 3, this leads to the values of the prime factors p and q. Observe that we must have $\delta > 0$, which implies that $\frac{5}{4} - \frac{1}{2}\alpha > 0$, and consequently $\alpha < \frac{5}{2}$. Also, we must have $\delta + \alpha > 2$. This implies that $\alpha > \frac{3}{2}$. □

If e is a full size exponent, that is $e \approx N^2$, then the bound on δ becomes $\delta < \frac{1}{4}$, which is the bound that can be attained by applying Wiener's method to the standard RSA.

4.2 A numerical example

As an example for the continued fraction attack, let us consider the small public key

$$\begin{aligned} N =&232133791034339655955539211937770616372332996733998207,\\ e =&380450490442297682094223716703548547490913325181786182\backslash\\ &142476527346417353000910073416245032502125803359 18003.\end{aligned}$$

We have $e \approx N^\alpha$ with $\alpha \approx 1.997$. We apply the continued fraction algorithm to $\frac{e}{\psi_0(N)}$ and get the first 30 partial quotients

$$[0, 1, 2, 2, 2, 23, 2, 12, 5, 2, 2, 8, 8, 1, 10, 1, 1, 1, 17, 6, 1, 1, 29, 1, 2, 1, 34, 22, 2, 1, 10, \ldots]$$

All the corresponding convergents are candidates for $\frac{k}{d}$. We consider only the convergents such that $\psi = \frac{ed-1}{k}$ is an integer. This happens for the 2th, 3th, 4th and 26th convergents. Among them, we consider only the convergents such that the system of equations

$$\begin{cases} \left(p^2+p+1\right)\left(q^2+q+1\right) & = \psi,\\ pq & = N, \end{cases}$$

has a solution as given in Proposition 3. This happens only for the 26th convergent, that is for $\frac{k}{d} = \frac{14646831653369}{20745421813476}$. It leads to

$$\begin{aligned} \psi(N) =&538860969399744700383693016290517492832014314220182 06\backslash\\ &725952642886800244273357202657271138657794039600145283,\end{aligned}$$

and, by Proposition 3, we get

$$\begin{aligned} p =&544726659808151712460129079,\\ q =&426147292141154398781533433.\end{aligned}$$

We observe that $d \approx N^\delta$ with $\delta \approx 0.249$, which satisfies the condition of Theorem 4, that is $\delta < \frac{5}{4} - \frac{1}{2}\alpha \approx 0.251$.

5 Application of Coppersmith's method

Let e and d be the public and the private exponent such that $ed - k\psi(N) = 1$ with $\psi(N) = \left(p^2+p+1\right)\left(q^2+q+1\right)$. In this section, we focus on solving the small inverse problem $x(y^2+ay+b)+1 \pmod{e}$, where $a = N+1$ and $b = N^2-N+1$. We then apply the method to show that one can factor N if k or d is sufficiently small.

5.1 The small inverse problem

Theorem 5. *Let $N = pq$ be the product of two unknown prime factors with $q < p < 2q$. Let $a = N+1$ and $b = N^2-N+1$. Suppose that $x(y^2+ay+b)+1 \equiv 0 \pmod{e}$ with $e = N^\alpha$, $y < 2\sqrt{2}N^{\frac{1}{2}}$, and $x = N^\gamma$. Then, for $1 < \alpha < \frac{15}{4}$, one can find x and y in polynomial time if*

$$\gamma < \alpha + \frac{1}{3} - \frac{2}{3}\sqrt{3\alpha+1}.$$

$$\begin{cases} \alpha = N+1 \\ b = N^2-N+1 \\ x(y^2+ay+b)+1 \equiv 0 \ (\mathrm{mod}\, e) \end{cases} \qquad \begin{cases} e = N^\alpha \\ y < 2\sqrt{2}N^{\frac{1}{2}} \end{cases}$$

Proof. Let $N = pq$ be an RSA modulus. Let e be a public exponent satisfying $x\left(y^2+ay+b\right)+1 \equiv 0 \pmod{e}$ where $a = N+1$ and $b = N^2-N+1$. Consider the polynomial $f(x,y) = x\left(y^2+ay+b\right)+1$. The small solutions of the former equation could be found by Coppersmith's method [8] combined with the extended strategy of Jochemsz and May [15]. Let m and t be positive integers. For $0 \le k \le m$, define the set

$x = N^\gamma$

对于 $1<\alpha<\frac{15}{4}$

当 $\gamma<\alpha+\frac{1}{3}-\frac{2}{3}\sqrt{3\alpha+1}$ 时

存 x, y

$$M_k = \bigcup_{0 \le h \le t} \left\{ x^i y^{j+h} \;\middle|\; x^i y^j \quad \text{is a monomial of} \quad f^m(x,y) \right.$$
$$\left. \text{and} \quad \frac{x^i y^j}{(xy^2)^k} \quad \text{is a monomial of} \quad f^{m-k}(x,y) \right\}.$$

We have

$$f^m(x,y) = \sum_{i_1=0}^{m} \sum_{j_1=0}^{i_1} \sum_{j_2=0}^{i_1-j_1} \binom{m}{i_1}\binom{i_1}{j_1}\binom{i_1-j_1}{j_2} a^{j_2} b^{i_1-j_1-j_2} x^{i_1} y^{2j_1+j_2}.$$

It follows that $x^i y^j$ is a monomial of $f^m(x,y,z)$ if

$$i = 0,\ldots,m, \quad j = 0,\ldots,2i.$$

Then, we deduce that $x^i y^j$ is a monomial of $f^{m-k}(x,y)$ if

$$i = 0,\ldots,m-k, \quad j = 0,\ldots,2i.$$

It follows that, if $x^i y^j$ is a monomial of $f^m(x,y)$, then $\frac{x^i y^j}{(xy^2)^k}$ is a monomial of $f^{m-k}(x,y)$ if $i = k,\ldots,m$, $j = 2k,\ldots,2i$. Hence, the set M_k is as follows

$$x^i y^j \in M_k \text{ if } i = k,\ldots,m,\; j = 2k,\ldots,2i+t.$$

Similarly, we have

$$x^i y^j \in M_{k+1} \text{ if } i = k+1, \ldots, m,\ \ j = 2k+2, \ldots, 2i+t.$$

Then $x^i y^j \in M_k \backslash M_{k+1}$ if

$$i = k, \ldots, m,\ \ j = 2k, 2k+1 \text{ or } i = k,\ \ j = 2k+2, \ldots, 2i+t.$$

For $0 \leq k \leq m$, we define the polynomials

$$g_{k,i,j}(x,y) = \frac{x^i y^j}{(xy^2)^k} f(x,y)^k e^{m-k} \quad \text{with} \quad x^i y^j \in M_k \backslash M_{k+1}.$$

They reduce to one of the following polynomials

$$g_{k,i,j}(x,y) = x^{i-k} y^{j-2k} f(x,y)^k e^{m-k},$$

$$\text{for} \quad k = 0, \ldots m,\ i = k, \ldots, m,\ j = 2k, 2k+1,$$

$$\text{or} \quad k = 0, \ldots m,\ i = k,\ j = 2k+2, \ldots, 2i+t.$$

$\begin{cases} a = \overline{N+1} \\ b = N^2 - N + 1 \\ x(y^2+ay+b)+1 \equiv 0 \ (\bmod e) \end{cases}$ $\begin{cases} e = N \\ y < 2\sqrt{2} N^{\frac{1}{2}} \end{cases}$

$x = N^\gamma$

对于 $1 < \alpha < \frac{15}{4}$

当 $1 < \alpha + \frac{1}{3} - \frac{2}{3}\sqrt{3\alpha+1}$ 时

有 x, y

Next, define the lattice $\mathcal{L}$ spanned by the coefficient vectors of the polynomials $g_{k,i,j}(xX, yY)$ where X and Y are positive integers satisfying

$$X = N^\gamma, Y = 2\sqrt{2}N^{\frac{1}{2}}.$$

The rows of the matrix of the lattice are denoted $g_{k,i,j}$ and ordered following the natural order of (i,j), completed by k. Similarly, the monomials $x^i y^j$ are ordered as in the natural order of (i,j). In Table 1, we present an example of the matrix of the lattice for $m = 2$, $t = 2$, where every symbol ⊛ is a non zero entry. We obtain a left triangular matrix and its determinant is the product of

	1	y	y^2	x	xy	xy^2	xy^3	xy^4	x^2	x^2y	x^2y^2	x^2y^3	x^2y^4	x^2y^5	x^2y^6
$g_{0,0,0}$	e^2	0	0	0	0	0	0	0	0	0	0	0	0	0	0
$g_{0,0,1}$	0	Ye^2	0	0	0	0	0	0	0	0	0	0	0	0	0
$g_{0,0,2}$	0	0	Y^2e^2	0	0	0	0	0	0	0	0	0	0	0	0
$g_{0,1,0}$	0	0	0	Xe^2	0	0	0	0	0	0	0	0	0	0	0
$g_{0,1,1}$	0	0	0	0	XYe^2	0	0	0	0	0	0	0	0	0	0
$g_{1,1,2}$	⊛	0	0	⊛	⊛	XY^2e	0	0	0	0	0	0	0	0	0
$g_{1,1,3}$	0	⊛	0	0	⊛	⊛	XY^3e	0	0	0	0	0	0	0	0
$g_{1,1,4}$	0	0	⊛	0	0	⊛	⊛	XY^4e	0	0	0	0	0	0	0
$g_{0,2,0}$	0	0	0	0	0	0	0	0	X^2e^2	0	0	0	0	0	0
$g_{0,2,1}$	0	0	0	0	0	0	0	0	0	X^2Ye^2	0	0	0	0	0
$g_{1,2,2}$	0	0	0	⊛	0	0	0	0	⊛	⊛	X^2Y^2e	0	0	0	0
$g_{1,2,3}$	0	0	0	0	⊛	0	0	0	0	⊛	⊛	X^2Y^3e	0	0	0
$g_{2,2,4}$	⊛	0	0	⊛	⊛	⊛	0	0	⊛	⊛	⊛	⊛	X^2Y^4	0	0
$g_{2,2,5}$	0	⊛	0	0	⊛	⊛	⊛	0	0	⊛	⊛	⊛	⊛	X^2Y^5	0
$g_{2,2,6}$	0	0	⊛	0	0	⊛	⊛	⊛	0	0	⊛	⊛	⊛	⊛	X^2Y^6

Table 1. The matrix of the lattice for $m = 2$, $t = 2$.

对角线上只有X，Y，e，使用到了

the diagonal terms, where only X, Y, and e are used. Hence, the determinant is of the form

故 det(L)=

$$\det(\mathcal{L}) = X^{n_X} Y^{n_Y} e^{n_e}. \tag{2}$$

Define

$$S(z) = \sum_{k=0}^{m} \sum_{i=k}^{m} \sum_{j=2k}^{2k+1} z + \sum_{k=0}^{m} \sum_{i=k}^{k} \sum_{j=2k+2}^{t} z$$

We set $t = m\tau$, where $\tau \geq 0$ will be optimised later. The exact values of n_X, n_Y, and n_e, as well as the dimension ω of the lattice, and their approximations are

$$\begin{aligned} n_X &= S(i) = \frac{1}{6} m(m+1)(4m+3\tau+5) \\ &= \frac{1}{6}(3\tau+4)m^3 + o(m^3) \\ n_Y &= S(j) = \frac{1}{6}(m+1)\left(4m^2+6m\tau+3\tau^2+5m+3\tau\right) \\ &= \frac{1}{6}\left(3\tau^2+6\tau+4\right)m^3 + o(m^3) \\ n_e &= S(m-k) = \frac{1}{6} m(m+1)(4m+3\tau+5) \\ &= \frac{1}{6}(3\tau+4)m^3 + o(m^3) \\ \omega &= S(1) = (m+1)(m+1+\tau) \\ &= (\tau+1)m^2 + o(m^2). \end{aligned} \tag{3}$$

In order to combine Theorem 3 and Theorem 2 for $i = 2$, we need

$$2^{\frac{\omega}{4}} \det(\mathcal{L})^{\frac{1}{\omega-1}} < \frac{e^m}{\sqrt{\omega}},$$

which gives

$$\det(\mathcal{L}) < \frac{2^{-\frac{\omega(\omega-1)}{4}}}{(\sqrt{\omega})^{\omega-1}} e^{m(\omega-1)}.$$

Combining with (2), we get

$$e^{n_e - m\omega} X^{n_X} Y^{n_Y} < \frac{2^{-\frac{\omega(\omega-1)}{4}}}{(\sqrt{\omega})^{\omega-1}} e^{-m}. \tag{4}$$

Substituting the values of n_X, n_Y, n_e, and ω from (3) as well as $X = N^\gamma$ and $Y = 2\sqrt{2}N^{\frac{1}{2}}$ in (4), taking logarithms, and dividing by $\log(N)$, we get

$$3\tau^2 + 6(\gamma - \alpha + 1)\tau + 4(2\gamma - \alpha + 1) < -\varepsilon_1,$$

where ε_1 is a small positive constant, that depends on m and N. The optimal value for τ in the left side is $\tau_0 = \alpha - \gamma - 1$. It gives

$$-3\gamma^2 + 2(1+3\alpha)\gamma - 3\alpha^2 + 2\alpha + 1 < -\varepsilon_1,$$

which is true if

$$\gamma < \alpha + \frac{1}{3} - \frac{2}{3}\sqrt{3\alpha+1}.$$

We need $\gamma \geq 0$. This is satisfied if

$$\alpha + \frac{1}{3} - \frac{2}{3}\sqrt{3\alpha+1} \geq 0,$$

that is $\alpha \geq 1$. On the other hand, we need $\tau_0 = \alpha - \gamma - 1 \geq 0$, that is $\gamma \leq \alpha - 1$. Hence, for $\alpha \geq 1$, we have

$$\gamma < \min\left(\alpha - 1, \alpha + \frac{1}{3} - \frac{2}{3}\sqrt{3\alpha+1}\right) = \alpha + \frac{1}{3} - \frac{2}{3}\sqrt{3\alpha+1}.$$

Using two vectors in the LLL reduced basis, we form two polynomials $G_1(x,y)$, $G_2(x,y)$ satisfying

$$G_1(x,y) = G_2(x,y) = 0.$$

Assuming that the polynomials are algebraically independent, we apply resultant techniques or Gröbner basis method to find the solution (x,y). This terminates the proof. □

5.2 The attack with small k

As an application of the method of Theorem 1, we have the following result.

Corollary 1. *Let $N = pq$ be the product of two unknown prime factors with $q < p < 2q$. Suppose that $ed - k\psi(N) = 1$ with $\psi(N) = \left(p^2+p+1\right)\left(q^2+q+1\right)$, $e = N^\alpha$, and $k = N^\gamma$. Then, for $1 < \alpha$, one can factor N in polynomial time if*

$$\gamma < \alpha + \frac{1}{3} - \frac{2}{3}\sqrt{3\alpha+1}.$$

Proof. Let $N = pq$ be an RSA modulus. Let e be a public exponent satisfying $ed - k\psi(N) = 1$, with $\psi(N) = \left(p^2+p+1\right)\left(q^2+q+1\right)$, $e = N^\alpha$, and $k = N^\gamma$. Since

$$\left(p^2+p+1\right)\left(q^2+q+1\right) = (p+q)^2 + a(p+q) + b$$

where $a = N+1$ and $b = N^2 - N + 1$, then the equation $ed - k\psi(N) = 1$ can be rewritten as

$$k\left((p+q)^2 + a(p+q) + b\right) + 1 \equiv 0 \pmod{e}.$$

$(k, p+q)$是其中一个解

Consider the polynomial $f(x,y) = x\left(y^2 + ay + b\right) + 1$. Then $(x_0, y_0) = (k, p+q)$ is a solution of the polynomial modular equation $f(x,y) \equiv 0 \pmod{e}$. The equation can be solved by the method of Theorem 5 if $\gamma < \alpha + \frac{1}{3} - \frac{2}{3}\sqrt{3\alpha+1}$. Using $p+q = y_0$, and $pq = N$, this leads to the factorization of N. □

$$\begin{cases} y_0 = p+q \\ N = pq \\ ed - k\varphi(n) = 1 \\ \varphi(N) = (p^2+p+1)(q^2+q+1) \\ e = N^\alpha \quad k = N^\gamma \end{cases}$$

$f(x,y) = x(y^2+ay+b)+1$

$e=N$, $k<N$

Let us present a small numerical example for Corollary 1. Consider

$$N = 437444022784453, e = 370036391765209395740444739800.$$

Since $e \approx N^{1.951}$, then the bound is $\gamma < \alpha + \frac{1}{3} - \frac{2}{3}\sqrt{3\alpha+1} \approx 0.539$. So we take $X_1 = \lfloor N^{0.6} \rfloor$, $Y_2 = 3\left\lfloor \sqrt{N} \right\rfloor$, $m = 4$, and $t = 3$. We build a lattice with a dimension $\omega = 40$. Then applying our method, we get the solution

$$x = k = 164427, y = p + q = 42593626.$$

Combining with $pq = N$, we finally get $p = 25310567$, and $q = 17283059$, which factors the modulus.

5.3 The attack with small d

Now, we focus on the attack on the scheme when d is small.

Theorem 6. *Let $N = pq$ be the product of two unknown prime factors with $q < p < 2q$. Suppose that $ed - k\psi(N) = 1$ with $\psi(N) = \left(p^2+p+1\right)\left(q^2+q+1\right)$, $e = N^\alpha$, and $d = N^\delta$. Then, for $1 < \alpha < \frac{15}{4}$, one can find d, and factor N in polynomial time if*

$$\delta < \frac{7}{3} - \frac{2}{3}\sqrt{3\alpha+1}.$$

Proof. Let $N = pq$ be an RSA modulus. Let e be a public exponent satisfying $ed - k\psi(N) = 1$, where $\psi(N) = \left(p^2+p+1\right)\left(q^2+q+1\right)$. We use the bounds $e = N^\alpha$, $d = N^\delta$. By Proposition 1, we have $(p+q)^2 + a(p+q) + b = \psi(N) > N^2$. Then

$$k = \frac{ed-1}{(p+q)^2 + a(p+q) + b} < N^{\alpha+\delta-2}.$$

We apply Corollary 1 with $\gamma = \alpha + \delta - 2$. The condition is

$$\gamma = \alpha + \delta - 2 < \alpha + \frac{1}{3} - \frac{2}{3}\sqrt{3\alpha+1},$$

which is true if

$$\delta < \frac{7}{3} - \frac{2}{3}\sqrt{3\alpha+1}.$$

Since $ed = k\psi(N) + 1 > \psi(N) > N^2$, then we need $\alpha + \delta > 2$. The condition is satisfied if

$$\alpha + \frac{7}{3} - \frac{2}{3}\sqrt{3\alpha+1} > 2,$$

and is valid if $\alpha > 1$. On the other hand, we need $\delta > 0$. This is satisfied if

$$\alpha + \frac{7}{3} - \frac{2}{3}\sqrt{3\alpha+1} > 0,$$

leading to $\alpha < \frac{15}{4}$. This terminates the proof. □

$\alpha=2$, $\delta=0.569$

example

~~If e is a full size exponent, that is~~ $e \approx N^2$, then the bound on δ becomes $\delta < \frac{7}{3} - \frac{2}{3}\sqrt{7} \approx 0.569$. This is twice the bound obtained by Boneh and Durfee [6] with the small inverse problem attack on RSA.

$e=N^\alpha$

$d=N^\delta$

$k<N^{\alpha+\delta-2}$

5.4 Experimental results

We implemented the method described in Theorem 6, and conducted intensive experiments in Windows 10 environment on a computer with Intel(R) Core(TM) i5-8250U CPU 1.60 GHZ, 8.0 GO. We experimented the method with the following process

– We generate two random prime numbers p, q of various sizes up to 1024 bits.
– We compute $N = pq$, and $\psi(N) = \left(p^2+p+1\right)\left(q^2+q+1\right)$.
– We generate a random integer $d = N^\delta$ with $\delta < 0.56$ and $\gcd(d, \psi(N)) = 1$.
– We compute $e \equiv d^{-1} \pmod{\psi(N)}$.
– We apply the method described in Theorem 6 to find the small solutions of the equation $x\left(y^2+ay+b\right)+1 \equiv 0 \pmod{e}$.
– Using $p+q = y$ and $pq = N$, we retrieve p and q.

The longest phase in the method is the computation of the reduced basis when applying the LLL algorithm. It depends mainly on the dimension ω and the size of N.

So far, we succeeded to factor the very small RSA modulus $N = 601396198489$ for $e = 1569479955769308430$. Since $e \approx N^{1.544}$, then the bound on δ is $\delta < \frac{7}{3} - \frac{2}{3}\sqrt{3\alpha+1} \approx 0.750$. So we applied our method method with $X = \left\lfloor N^{0.75}\right\rfloor$, $Y = 3\left\lfloor\sqrt{N}\right\rfloor$, $m = 6$, and $t = 3$. We get a lattice with a dimension $\omega = 70$. We solved the equation $x\left(y^2+ay+b\right)+1 \equiv 0 \pmod{e}$, and get the solution $x = 13$, $y = 1559590$. Then, using $p+q = y$ and $pq = N$, we get $p = 861551$, and $q = 698039$. We notice here that $d = N^\delta$ with $\delta \approx 0.55$. The whole process took less than 240 seconds.

When N is a 1024 bit modulus, we were able to factor N with $d = N^\delta$ for $\delta < 0.43$, with $m = 4$, $t = 2$, $\omega = 35$, $X = \left\lfloor N^{0.5}\right\rfloor$, and $Y = 3\left\lfloor\sqrt{N}\right\rfloor$. The computation took approximately 8372 seconds.

6 Conclusion

In this paper, we presented two distinct attacks on a cubic Pell equation variant of the RSA cryptosystem presented by Murru and Saettone in 2018. The variant is based on an RSA modulus $N = pq$, with a public exponent $e = N^\alpha$, a private exponent d and a key equation of the form $ed - k\psi(N) = 1$ where $\psi(N) = \left(p^2+p+1\right)\left(q^2+q+1\right)$. For the first attack, we extended Wiener's attack and showed that one can factor the modulus N via the continued fraction expansion provided $d = N^\delta$ for $\delta < \frac{5}{4} - \frac{1}{2}\alpha$. Moreover, we showed that this variant of RSA is more vulnerable by our second attack which is based on Coppersmith's method. We extended the method of Boneh and Durfee and showed that the RSA variant is insecure whenever $\delta < \frac{7}{3} - \frac{2}{3}\sqrt{3\alpha+1}$. When $\alpha \approx 2$, the bound resumes to $d < N^{0.5694}$, which is much larger than the classical bound $d < N^{0.292}$ for RSA. As a conclusion, the variant RSA scheme is more vulnerable than the RSA cryptosystem.

References

1. Adenan, N. N. H., Ariffin, M. R. K., Sapar, S. H., Ghafar, A. H. A., Asbullah, M. A.: New Jochemsz-May Cryptanalytic Bound For RSA System Utilizing Common Modulus $N = p^2q$. Mathematics 2021, 9, 4, 340.https://www.mdpi.com/2227-7390/9/4/340
2. Blömer, J., May, A.: A generalized Wiener attack on RSA. In Public Key Cryptography - PKC 2004, volume 2947 of Lecture Notes in Computer Science, 1–13. Springer-Verlag (2004)
3. Boneh, D.: Twenty years of attacks on the RSA cryptosystem, Notices Amer. Math. Soc. 46 (2), 203–213, (1999)
4. Boneh, D., Durfee, G., and Frankel, Y.: An attack on RSA given a small fraction of the private key bits. inASIACRYPT 1998, 25–34.
5. Boneh, D., Durfee, G., and Howgrave-Graham, N.: Factoring $N = p^rq$ for large r. in CRYPTO 1999, 326–337.
6. Boneh, D., Durfee, G.: Cryptanalysis of RSA with private key d less than $N^{0.292}$, Advances in Cryptology-Eurocrypt'99, Lecture Notes in Computer Science Vol. 1592, Springer-Verlag, pp. 1–11 (1999)
7. Bpudabra, M., Nitaj, A.: A new generalization of the KMOV cryptosystem, Journal of Applied Mathematics and Computing, June 2018, Volume 57, Issue 12, pp 229245 (2018)
8. Coppersmith, D.: Small solutions to polynomial equations, and low exponent RSA vulnerabilities. Journal of Cryptology, 10(4), pp. 233–260 (1997)
9. Demytko, N.: A new elliptic curve based analogue of RSA, in T. Helleseth (ed.), EUROCRYPT 1993, Lecture Notes in Computer Science **765**, Springer-Verlag, 40–49 (1994)
10. Diffie, W., Hellman, M.: New directions in cryptography, Institute of Electri-cal and Electronics Engineers., vol. IT-22, Transactions on Information Theory, no. 6, 1976, pp. 644654 (1976)
11. Ernst, M., Jochemsz, E., May, A., de Weger, B.: Partial key exposure attacks on RSA up to full size exponents. In: Cramer, R. (ed.) Advances in Cryptology Eurocrypt 2005. Lecture Notes in Computer Science, vol. 3494, pp. 371–386. Springer-Verlag (2005)
12. Hardy, G.H., Wright, E.M.: An Introduction to Theory of Numbers, 5th Edition, The Clarendon Press Oxford University Press, New York (1979)
13. Hinek, M.: Cryptanalysis of RSA and Its Variants, Chapman & Hall/CRC, Cryptography and Network Security Series, Boca Raton, (2009)
14. Howgrave-Graham, N.: Finding small roots of univariate modular equations revisited, In Cryptography and Coding, LNCS 1355, pp. 131–142, Springer-Verlag (1997)
15. Jochemsz, E., May, A.: A strategy for finding roots of multivariate polynomials with new applications in attacking RSA variants, in: ASIACRYPT 2006, LNCS 4284, 2006, pp. 267–282, Springer-Verlag (2006)
16. Koyama, K.: Fast RSA type scheme based on singular cubic curve $y^2 + axy = x^3 \pmod{n}$. Proc. Eurocrypt'95, Lecture Notes in Computer Science, **921**, Springer-Verlag, 329–339 (1995)
17. Koyama, K., Maurer, U. M., Okamoto, T., Vanstone, S. A.: New public-key schemes based on elliptic curves over the ring $\mathbb{Z}_n$, in: Proceedings of CRYPTO 1991, Lecture Notes in Computer Science 576, 1991, pp. 252–266.

18. Kuwakado H., Koyama K., Tsuruoka, Y.: A new RSA-type scheme based on singular cubic curves $y^2 \equiv x^3 + bx^2 \pmod{n}$, IEICE Transactions on Fundamentals, E78-A, 27–33 (1995)
19. Lenstra, A.K., Lenstra, H.W., Lovász, L.: Factoring polynomials with rational coefficients, Mathematische Annalen, Vol. 261, pp. 513–534, (1982)
20. Lenstra, A.K., Verheul, E.R.: The XTR public key system. In M. Bellare, Ed., Advances in Cryptology CRYPTO 2000, vol. 1880 of Lecture Notes in Computer Science, pp. 1–19. Springer-Verlag, 2000.
21. Murru N., Saettone F.M.: A Novel RSA-Like Cryptosystem Based on a Generalization of the Rédei Rational Functions. In: Kaczorowski J., Pieprzyk J., Pomykala J. (eds) Number-Theoretic Methods in Cryptology. NuTMiC 2017. Lecture Notes in Computer Science, vol 10737. Springer, Cham (2018)
22. Nitaj, A.: Another generalization of Wiener's attack on RSA, In: Vaudenay, S. (Ed.) Africacrypt 2008. LNCS, vol. 5023, 174190. Springer, Heidelberg (2008)
23. Rivest, R., Shamir, A., Adleman, L.: A Method for Obtaining digital signatures and public-key cryptosystems, Communications of the ACM, Vol. 21 (2), pp. 120–126 (1978)
24. Sarkar, S.: Small secret exponent attack on RSA varian with modulus $N = p^r q$. Des. Codes Cryptogr. 2014 73, 2, 383–392.
25. Takagi, T.: A fast RSA-type public-key primitive modulo $p^k q$ using Hensel lifting, IEICE Transactions 2004, 87-A, 94–101.
26. B. de Weger: Cryptanalysis of RSA with small prime difference. Applicable Algebra in Engineering, Communication and Computing, 13(1), pp. 1728, 2002.
27. Wiener, M.: Cryptanalysis of short RSA secret exponents, IEEE Transactions on Information Theory, Vol. 36, 553–558 (1990)