Theoretical Computer Science 889 (2021) 135–144

Contents lists available at ScienceDirect

Theoretical Computer Science

www.elsevier.com/locate/tcs

Cryptanalysis of the RSA variant based on cubic Pell equation

Mengce Zheng [a,c,*], Noboru Kunihiro [b], Yuanzhi Yao [c]

[a] College of Information and Intelligence Engineering, Zhejiang Wanli University, Ningbo, China
[b] Department of Computer Science, University of Tsukuba, Tsukuba, Japan
[c] Department of Electronic Engineering and Information Science, University of Science and Technology of China, Hefei, China

ARTICLE INFO

Article history:
Received 11 March 2021
Received in revised form 25 June 2021
Accepted 1 August 2021
Available online 5 August 2021
Communicated by G. Yang

Keywords:
Cryptanalysis
RSA variant
Cubic Pell equation
Lattice-based method
Small private exponent attack

ABSTRACT

RSA (Rivest-Shamir-Adleman) cryptosystem is the most popular asymmetric key cryptographic algorithm used in computer science and information security. Recently, an RSA-like cryptosystem was proposed using a novel product that arises from a cubic field connected to the cubic Pell equation. The relevant *key equation* is $ed \equiv 1 \bmod (p^2+p+1)(q^2+q+1)$ with $N = pq$. This RSA variant is claimed to be robust against the Wiener's attack and hence the bit-size of the private key could be shorter, namely $d < N^{1/4}$. In this paper, we explore the further security analysis and investigate the potential small private exponent attack. We show that such RSA variant is particularly vulnerable to the *lattice-based* method. To be specific, we can carry out the lattice-based small private exponent attack if $d < N^{2-\sqrt{2}}$, which is less secure than the standard RSA. Furthermore, we conduct numerical experiments to verify the validity of the proposed attack.

1. Introduction

RSA [1] is currently the most widely used public key cryptosystem in the world. In the standard RSA cryptosystem, a public modulus N is the product of two large primes p and q of the same bit-size, namely $N = pq$. The key equation is $ed \equiv 1 \bmod \varphi(N)$, where $\varphi(N) = (p-1)(q-1)$ is Euler's totient function. (N, e) and (p, q, d) are called the public and private keys, respectively. In the encryption process, a message string is transformed into an integer m and then encrypted as $c = m^e \bmod N$. The decryption process computes $c^d \bmod N$. As e and d are calculated as exponents in the encryption and decryption phases, they are called public and private exponents as well. In this paper, we assume $e = N^\alpha$, $d = N^\delta$ and further use two parameters α and δ in the cryptanalysis for simplicity.

The standard RSA scheme has been generalized by various approaches such as modifying the modulus [2] and modifying the decryption process [3] to gain a significant speed-up in the practical implementation. Besides, several RSA variants like [4,5] have been proposed to be more secure against the broadcast attack [6]. In this paper, we focus on the RSA variant based on cubic Pell equation that was proposed in [5]. It defines a novel product that is applied in the encryption and decryption processes. We conclude the *modified key equation* arisen from such RSA variant, which can be written as

$$ed \equiv 1 \bmod (p^2+p+1)(q^2+q+1). \tag{1}$$

* Corresponding author at: College of Information and Intelligence Engineering, Zhejiang Wanli University, Ningbo, China.
E-mail address: mengce.zheng@gmail.com (M. Zheng).

https://doi.org/10.1016/j.tcs.2021.08.001
0304-3975/

Generally, we have $0 < \alpha, \delta < 2$ as $0 < e, d < (p^2+p+1)(q^2+q+1) \approx N^2$. Moreover, α and δ can be set to exceed the above range for particular security considerations in practice. We introduce the relevant RSA variant and its mathematical background below. One may refer to [5] for more details.

This RSA variant was recently proposed by Murru and Saettone. It is related to an interesting definition of *product* that arises from a cubic field connected to the cubic Pell equation. Let $\mathbb{F}$ be a field and $(t^3 - r)$ be an irreducible polynomial in $\mathbb{F}[t]$. We consider the quotient field

$$\mathbb{A} = \mathbb{F}[t]/(t^3 - r) = \{x + yt + zt^2 : x, y, z \in \mathbb{F}\}.$$

$\mathbb{A}$ induces a product $\bullet$ between two triples like (x_1, y_1, z_1), $(x_2, y_2, z_2) \in \mathbb{F}^3$. The product $(x_1, y_1, z_1) \bullet (x_2, y_2, z_2)$ is calculated as

$$(x_1x_2 + (y_2z_1 + y_1z_2)r, x_2y_1 + x_1y_2 + rz_1z_2, y_1y_2 + x_2z_1 + x_1z_2).$$

The norm of an element (x, y, z) is given by $N(x, y, z) = x^3 + ry^3 + r^2z^3 - 3rxyz$. Considering the unitary elements, we obtain the cubic Pell curve

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

where $x^3 + ry^3 + r^2z^3 - 3rxyz = 1$ is the more natural cubic Pell equation for a non-cubic integer r. Starting from $\mathbb{A}$, we consider the quotient group $B = \mathbb{A}^*/\mathbb{F}^*$ with a non-standard product $\odot$. The group B can be rewritten as

$$B = \{[m + nt + t^2] : m, n \in \mathbb{F}\} \cup \{[m + t] : m \in \mathbb{F}\} \cup \{[1_{\mathbb{F}^*}]\},$$

where $[\cdot]$ stands for the equivalent set. Fixing an element $\theta \notin \mathbb{F}$, the elements of B can be seen as (m, n) with $m, n \in \mathbb{F}$, or (m, θ) with $m \in \mathbb{F}$, or (θ, θ). Now the group B is

$$B = (\mathbb{F} \times \mathbb{F}) \cup (\mathbb{F} \times \{\theta\}) \cup (\{\theta\} \times \{\theta\}).$$

The rules for computing the commutative product $\odot$ in B are defined as follows, where (θ, θ) is the identity.

- $(m, \theta) \odot (k, \theta) = (mk, m + k)$;
- $(m, n) \odot (k, \theta) =$
  - $\left(\frac{mk+r}{n+k}, \frac{m+nk}{n+k}\right)$, $n + k \neq 0$;
  - $\left(\frac{mk+r}{m-n^2}, \theta\right)$, $n + k = 0$, $m - n^2 \neq 0$;
  - (θ, θ), otherwise;
- $(m, n) \odot (k, l) =$
  - $\left(\frac{mk+(n+l)r}{m+k+nl}, \frac{nk+ml+r}{m+k+nl}\right)$, $m + k + nl \neq 0$;
  - $\left(\frac{mk+(n+l)r}{nk+ml+r}, \theta\right)$, $m + k + nl = 0$, $nk + ml + r \neq 0$;
  - (θ, θ), otherwise.

The RSA variant scheme is based on the following useful facts. Letting $\mathbb{F} = \mathbb{Z}_p$ and fixing $\theta = \infty$, we have $\mathbb{A} = GF(p^3)$ in this case. Thus, B is a cyclic group of order $\frac{p^3-1}{p-1} = p^2 + p + 1$, with respect to a well-defined product $\odot$. An analog of the little Fermat's theorem holds.

$$(m, n)^{\odot p^2+p+1} \equiv (\infty, \infty) \bmod p,$$

for any $m \in \mathbb{Z}_p$ and $n \in \mathbb{Z}_p \cup \{\infty\}$. Moreover, the power using the product $\odot$ can be evaluated through a generalization of the Rédei rational functions. When $N = pq$, for two prime numbers p and q of the same bit-size, it follows from the above power computation that

$$(m, n)^{\odot (p^2+p+1)(q^2+q+1)} \equiv (\infty, \infty) \bmod N,$$

which can be seen as an analog of the Euler's theorem. The proposed public-key cryptosystem in [5] using the product $\odot$ is described as follows.

Key Generation. Randomly choose two prime numbers of the same bit-size p, q and compute the modulus $N = pq$. Randomly choose an integer e such that $\gcd(e, (p^2+p+1)(q^2+q+1)) = 1$ along with a non-cubic integer r in $\mathbb{Z}_p, \mathbb{Z}_q$ and $\mathbb{Z}_N$. Compute d such that $ed \equiv 1 \bmod (p^2 + p + 1)(q^2 + q + 1)$. The public encryption key is (N, e, r) and the corresponding secret decryption key is (p, q, d).

Encryption. Given a pair of plaintexts m_1 and m_2 in $\mathbb{Z}_N$, they are encrypted by

$$(c_1, c_2) \equiv (m_1, m_2)^{\odot e} \bmod N.$$

Decryption. Given a pair of ciphertexts c_1 and c_2 in $\mathbb{Z}_N$, the receiver can decrypt them by evaluating

$$(c_1, c_2)^{\odot d} \bmod N.$$

In summary, this RSA variant scheme uses a new group equipped with a non-standard product whose powers can be evaluated means of some generalized Rédei functions. The authors claim that the proposed scheme is more secure than the standard RSA in broadcast scenarios since the corresponding trapdoor function is not a simple monomial power as in the standard RSA. Furthermore, the authors claim that Wiener's attack [7] is not usable against the proposed RSA variant scheme. For the same reason, further attacks exploiting continued fractions also fail in such case. Hence, the private key of bit-size less than $N^{1/4}$ can be used without being affected by Wiener's attack.

It is interesting to investigate whether the proposed scheme in [5] can be used with a much shorter private exponent in theory and in practice as claimed. Surprisingly, we conclude that the RSA variant based on cubic Pell equation is particularly vulnerable to the *lattice-based* small private exponent attack.

We first review several small private exponent attacks below. In 1990, Wiener [7] showed that one can break the standard RSA scheme when the private key d is less than $\frac{1}{3}N^{1/4}$. This bound was further improved to $\frac{1}{\sqrt[4]{18}}N^{1/4}$ in [8]. Wiener's attack utilizes the continued fraction approach to deal with the key equation $ed = k(p-1)(q-1)+1$. If d is small enough, k/d will be one of the convergents of the continued fraction expansion of the public rational fraction e/N. Thus, k and d can be recovered by computing the continued fraction expansion of e/N.

Later in 1999, Boneh and Durfee [9] introduced the small inverse problem and further improved the insecure bound to $d < N^{1-\sqrt{2}/2}$ using Coppersmith's lattice-based techniques [10]. The aim of the lattice-based method is to find the small roots of the modular equation $x(y+A)+1 \equiv 0 \bmod e$ with known A and e. Moreover, Herrmann and May [11] presented an elementary method to solve the same equation using the linearization technique that is applied to construct smaller dimensional lattices. Though it does not improve the insecure bound, it simplifies the lattice construction and reduces the practical consumption. More small private exponent attacks [12–18] and other types of cryptanalyses [19–23] on RSA and its variants have been proposed using the lattice-based method.

The small inverse problem is a natural extension of the small private exponent attack on the standard RSA and has been studied in [9,24–26]. In 2012, Kunihiro [25] presented a lattice-based method to solve small inverse problems with a higher degree. To be specific, for a monic polynomial $h(y)$ of degree $\kappa \geq 1$, integers C and e, a lattice-based algorithm was proposed to find all small roots of a bivariate modular equation $xh(y)+C \equiv 0 \bmod e$. A similar approach as the linearization technique is employed for especially evaluating the lattice determinant. We adapt the lattice-based method in [25] to conduct the small private exponent attack on the RSA variant based on cubic Pell equation.

In this paper, we first derive the critical modular equation to be solved from the modified key equation (1). It can be rewritten as

$$ed = k\left((p+q)^2 + (N+1)(p+q) + N^2 - N + 1\right) + 1.$$

Thus, we are required to solve a small inverse problem with degree two. The critical modular equation is

$$x(y^2 + ay + b) + 1 \equiv 0 \bmod e \tag{2}$$

for $a := N+1$ and $b := N^2 - N + 1$ with small roots $x := k$ and $y := p+q$. We propose the small private exponent attack for a general case when using full-size public key $e \approx N^2$, which is stated below.

Proposition 1. *Let $N = pq$ be a modulus of the RSA variant based on cubic Pell equation. Two prime factors p and q are of the same bit-size. Let $e \approx N^2$ be a valid public key and $d = N^\delta$ be its corresponding private key such that $ed \equiv 1 \bmod (p^2+p+1)(q^2+q+1)$. Then N can be efficiently factored in polynomial time if*

$$\delta < 2 - \sqrt{2}.$$

It is oblivious that the RSA variant based on cubic Pell equation can be broken in polynomial time for small private key $d < N^{2-\sqrt{2}}$. Moreover, it indicates that such RSA variant is even more vulnerable than the standard RSA since $2-\sqrt{2} \approx 0.585$ is much greater than $1-\sqrt{2}/2 \approx 0.292$ reported in [9]. Concretely, $2-\sqrt{2}$ is twice of $1-\sqrt{2}/2$.

The rest of the paper is organized as follows. We review some mathematical facts and useful lemmas of the lattice-based method in Section 2. In Section 3, we present the small private exponent attack on the RSA variant based on cubic Pell equation in detail. In Section 4, we verify the validity of the proposed attack by computer experiments. Finally, we conclude the paper in Section 5.

2. Preliminaries

In this section, we introduce Coppersmith's techniques [10,27] based on the LLL lattice reduction algorithm [28] and summarize a crucial condition for finding the small roots of modular/integer polynomial equations. We briefly explain how to solve multivariate modular polynomial equations using the idea of Coppersmith's techniques. One may refer to [29–31] for more details.

Problem 1. Let $f(x_1, \ldots, x_n)$ be an irreducible multivariate polynomial defined over $\mathbb{Z}$, which has a small root $(x'_1, \ldots, x'_n)$ modulo a known positive integer such that $|x'_1| \leq X_1, \ldots, |x'_n| \leq X_n$. The question is to recover the desired root $(x'_1, \ldots, x'_n)$ in polynomial time under the established upper bounds $X_1, \ldots, X_n$.

We start with the lattice theory and the lattice reduction algorithm. A lattice $\mathcal{L}$ spanned by linearly independent vectors $\vec{b}_1, \ldots, \vec{b}_w \in \mathbb{R}^n$ is the set of their integer linear combinations, which is denoted by

$$\mathcal{L}(\vec{b}_1, \ldots, \vec{b}_w) = \left\{ \sum_{i=1}^{w} z_i \vec{b}_i : z_i \in \mathbb{Z} \right\}.$$

By regarding each $\vec{b}_i$ as a row/column vector, they generate a lattice basis matrix B. The determinant of $\mathcal{L}$ is defined as $\det(\mathcal{L}) = \sqrt{\det(BB^{\mathsf{T}})}$, where B^{T} is a transpose of B. The rank of $\mathcal{L}$ is w and we always consider a full-rank lattice for $w = n$. We have $\det(\mathcal{L}) = |\det(B)|$ for a full-rank lattice since B is a square matrix. Moreover, the determinant of a triangular basis matrix can be easily estimated as the product of its diagonal entries.

The LLL algorithm proposed by Lenstra, Lenstra and Lovász [28] is practically used for computing approximately short reduced vectors due to its efficient running outputs. We provide the following substratal lemma that has been proven in [29].

Lemma 1. *Let $\mathcal{L}$ be a lattice spanned by basis vectors $(\vec{b}_1, \ldots, \vec{b}_w)$. The LLL algorithm outputs a reduced basis $(\vec{v}_1, \ldots, \vec{v}_w)$ satisfying*

$$\|\vec{v}_1\|, \|\vec{v}_2\|, \ldots, \|\vec{v}_i\| \leq 2^{\frac{w(w-1)}{4(w+1-i)}} \det(\mathcal{L})^{\frac{1}{w+1-i}} \text{ for } 1 \leq i \leq w$$

in time polynomial in w and in the bit-size of the entries of the basis matrix.

Howgrave-Graham [32] later refined on Coppersmith's techniques to propose a succinct lemma, which is used for judging if the roots of a modular equation are roots over $\mathbb{Z}$. For a given polynomial $h(x_1, \ldots, x_n) = \sum a_{i_1,\ldots,i_n} x_1^{i_1} \cdots x_n^{i_n}$, its norm is defined as $\|h(x_1, \ldots, x_n)\| := \sqrt{\sum |a_{i_1,\ldots,i_n}|^2}$.

Lemma 2. *Let $h(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ be an integer polynomial, which is a sum of at most w monomials. Let $X_1, \ldots, X_n$ and R be some positive integers. Suppose that*

1. *$h(x'_1, \ldots, x'_n) \equiv 0 \bmod R$, where $|x'_1| \leq X_1, \ldots, |x'_n| \leq X_n$,*
2. *$\|h(x_1X_1, \ldots, x_nX_n)\| < R/\sqrt{w}$.*

Then $h(x'_1, \ldots, x'_n) = 0$ holds over the integers.

Hence, the root-finding problem in modular polynomial equations can be reduced to the case of that in equation over the integers by using Lemma 2. Further combining with Lemma 1, one can solve a given modular equation under a certain condition. The main idea of the lattice-based method is to construct a set of shift polynomials modulo R with the common root and then reduce them to several integer equations. The basis matrix generating by the shift polynomials' coefficient vectors spans a w-dimensional lattice. One can use the LLL algorithm to obtain short lattice vectors and transform them into polynomial equations. If the norms of the polynomials are sufficiently small, the equations hold over the integers.

When one obtains the first ℓ reduced vectors through the LLL algorithm, he/she can extract the solutions if

$$2^{\frac{w(w-1)}{4(w+1-\ell)}} \det(\mathcal{L})^{\frac{1}{w+1-\ell}} < R/\sqrt{w},$$

which can be roughly reduced to $\det(\mathcal{L}) < R^w$ when ignoring the lower terms. Eventually, one can efficiently extract the common root of the derived integer equations by the Gröbner basis computation [33] or resultant computation.

In summary, we have four steps to solve a multivariate modular polynomial equation using the lattice-based method.

Shift Polynomials. Using $f(x_1, \ldots, x_n)$ and given modulus to generate a collection $\mathcal{F}$ of shift polynomials $g_1(x_1, \ldots, x_n)$, $\ldots, g_w(x_1, \ldots, x_n)$ such that $(x'_1, \ldots, x'_n)$ is a common root modulo R.

Lattice Generation. Let $\vec{b}_i$ be a row vector derived from the coefficient vector of $g_i(x_1X_1, \ldots, x_nX_n)$ for all $1 \le i \le w$. Hence, one can generate the lattice $\mathcal{L} = \left\{ \sum_{i=1}^{w} z_i \vec{b}_i : z_i \in \mathbb{Z} \right\}$.

Lattice Reducion. Applying the LLL reduction algorithm on $\mathcal{L}$, one can get the first n many reduced basis vectors $\vec{v}_1, \ldots, \vec{v}_n$. One can transform the vectors to polynomials $h_1(x_1, \ldots, x_n), \ldots, h_n(x_1, \ldots, x_n)$ sharing the common root $(x'_1, \ldots, x'_n)$ over $\mathbb{Z}$.

Root Extraction. If derived integer polynomials $h_i(x_1, \ldots, x_n)$ for $1 \le i \le n$ are algebraically independent, the equation system $h_i(x_1, \ldots, x_n) = 0$ can be solved using the Gröbner basis computation. Hence, one extracts the desired root $(x'_1, \ldots, x'_n)$.

We do not mention how to solve integer polynomial equations since it makes use of the essential idea of solving modular equations by adding an auxiliary parameter. We further apply the lattice technique introduced in [25], which can make it easier to construct a triangular lattice matrix in our attack scenario.

Notice that solving multivariate equations is heuristic because the newly derived polynomials are not guaranteed to be algebraically independent. In this paper, we assume that the polynomials derived from the reduced vectors of the LLL algorithm are algebraically independent as discussed in the literature of the lattice-based attacks on RSA and its variants. In fact, there are barely existing works that contradict this assumption.

Assumption 1. The integer polynomials finally obtained from the lattice-based method are algebraically independent. Thus, the common root of the derived polynomial equations can be efficiently recovered by the Gröbner basis computation.

3. Small private exponent attack

We aim to produce the lattice-based attack on the RSA variant based on cubic Pell equation for sufficient small private key d, i.e. small private exponent δ. Applying the subtle technique introduced in [25], we solve the crucial modular equation (2) and present the small private exponent attack.

We address how to find all small roots of the bivariate modular equation

$$f(x, y) := x(y^2 + ay + b) + 1 \equiv 0 \bmod e.$$

Let $h(y) := y^2 + ay + b = y^2 + \bar{h}(y)$ for $\bar{h}(y) := ay + b$ with $a = N + 1$ and $b = N^2 - N + 1$. We transform the original polynomial $f(x, y)$ into

$$f(x, y) = xh(y) + 1 = x(y^2 + \bar{h}(y)) + 1 = (xy^2 + 1) + x\bar{h}(y).$$

Letting $z := xy^2 + 1$, we have $\bar{f}(x, y, z) := z + x\bar{h}(y)$. The shift polynomials $g_{[i,j,k]}(x, y, z)$ are defined as

$$g_{[i,j,k]}(x, y, z) := x^i y^j \bar{f}^k(x, y, z) e^{s-k} = x^i y^j (z + x\bar{h}(y))^k e^{s-k}$$

for a fixed positive integer s and non-negative integers i, j, k. We denote the set of shift polynomials by $\mathcal{F} := \mathcal{G} \cup \mathcal{H}$ for

$$\mathcal{G} := \{g_{[i,j,k]}(x, y, z) : (i, j, k) \in \mathcal{I}_{\mathcal{G}}\},$$
$$\mathcal{H} := \{g_{[i,j,k]}(x, y, z) : (i, j, k) \in \mathcal{I}_{\mathcal{H}}\},$$

where the corresponding index set $\mathcal{I} := \mathcal{I}_{\mathcal{G}} \cup \mathcal{I}_{\mathcal{H}}$ is defined by

$$\mathcal{I}_{\mathcal{G}} := \{(i, j, k) : i = 0, \ldots, s;\ j = 0, 1;\ k = 0, \ldots, s - i\},$$
$$\mathcal{I}_{\mathcal{H}} := \{(i, j, k) : i = 0;\ j = 2, \ldots, \lfloor \tau k \rfloor + 1;\ k = 0, \ldots, s\},$$

for a parameter $0 \le \tau \le 1$ to be optimized later. The definitions of $\mathcal{I}_{\mathcal{G}}$ and $\mathcal{I}_{\mathcal{H}}$ are modified from the original ones in [25].

Let $(x, y) = (x_0, y_0)$ be a solution of $f(x, y) \equiv 0 \bmod e$ and $z_0 := x_0 y_0^2 + 1$, it is easy to see that all the shift polynomials $g_{[i,j,k]}(x, y, z)$ in $\mathcal{F}$ share the common small root (x_0, y_0, z_0) modulo e^s.

The polynomial order $\prec_{\mathrm{p}}$ is defined as $g_{[i,j,k]} \prec_{\mathrm{p}} g_{[i',j',k']}$ if

- $i + k < i' + k'$; or
- $i + k = i' + k'$ and $i < i'$; or
- $i = i'$, $k = k'$ and $j < j'$.

The monomial order $\prec_{\mathrm{m}}$ is defined as $x^i y^j z^k \prec_{\mathrm{m}} x^{i'} y^{j'} z^{k'}$ if

- $i + k < i' + k'$; or
- $i + k = i' + k'$ and $i < i'$; or

Table 1
A toy example of the lattice basis matrix for $s=2$ and $\tau=1$.

	1	y	x	xy	z	yz	y^2z	x^2	x^2y	xz	xyz	z^2	yz^2	y^2z^2	y^3z^2
$g_{[0,0,0]}$	e^2														
$g_{[0,1,0]}$		e^2Y													
$g_{[1,0,0]}$			e^2X												
$g_{[1,1,0]}$				e^2XY											
$g_{[0,0,1]}$			–	–	eZ										
$g_{[0,1,1]}$	–			–	–	eYZ									
$g_{[0,2,1]}$	–	–			–	–	eY^2Z								
$g_{[2,0,0]}$								e^2X^2							
$g_{[2,1,0]}$									e^2X^2Y						
$g_{[1,0,1]}$								–	–	eXZ					
$g_{[1,1,1]}$			–						–	–	$eXYZ$				
$g_{[0,0,2]}$			–					–	–	–	–	Z^2			
$g_{[0,1,2]}$			–	–	–				–	–	–	–	YZ^2		
$g_{[0,2,2]}$	–		–	–	–	–				–	–	–	–	Y^2Z^2	
$g_{[0,3,2]}$	–	–		–	–	–	–				–	–	–	–	Y^3Z^2

- $i=i'$, $k=k'$ and $j<j'$.

We can substitute each occurrence of xy^2 by the term $z-1$. The lattice basis matrix is generated by taking the coefficient vectors of $g_{[i,j,k]}(xX, yY, zZ)$ as row vectors, where X, Y and Z denote the upper bounds on the root (x_0, y_0, z_0). Additionally, the rows and columns are arranged according to the above orders $\prec_{\mathrm{p}}$ and $\prec_{\mathrm{m}}$, which guarantees that the lattice basis matrix is triangular (this property has been proven in [25]). Table 1 shows a toy example for two parameters $s=2$ and $\tau=1$, where symbols "–" denote the non-zero off-diagonal entries and other off-diagonal entries are 0.

Since $e=N^{\alpha}$, $d=N^{\delta}$ and $\sqrt{N/2}<p,q<\sqrt{2N}$, we can figure out $X=N^{\alpha+\delta-2}$, $Y\approx N^{1/2}$ and $Z\approx XY^2=N^{\alpha+\delta-1}$ when omitting small terms compared to N. We are able to compute the lattice determinant, which can be calculated as

$$\begin{aligned}\det(\mathcal{L}) &= \prod_{(i,j,k)\in\mathcal{I}} X^iY^jZ^ke^{s-k} = \prod_{(i,j,k)\in\mathcal{I}_{\mathcal{G}}} X^iY^jZ^ke^{s-k} \prod_{(i,j,k)\in\mathcal{I}_{\mathcal{H}}} X^iY^jZ^ke^{s-k} \\ &= \prod_{i=0}^{s}\prod_{k=0}^{s-i}\prod_{j=0}^{1} X^iY^jZ^ke^{s-k} \prod_{k=0}^{s}\prod_{j=2}^{\lfloor\tau k\rfloor+1} Y^jZ^ke^{s-k}.\end{aligned}$$

By counting the numbers of X, Y, Z and e appearing in the diagonal entries, we know the contributions of the shift polynomials to $\det(\mathcal{L})$. We omit the rounding of τk as $\lfloor\tau k\rfloor$ is negligible in the asymptotic analysis for sufficiently large s.

We compute the dimension w of the full-rank lattice $\mathcal{L}$ and the contributions of the shift polynomials denoted by n_X, n_Y, n_Z and n_e, respectively.

$$\begin{aligned}w &= \sum_{(i,j,k)\in\mathcal{I}} 1 = \sum_{(i,j,k)\in\mathcal{I}_{\mathcal{G}}} 1 + \sum_{(i,j,k)\in\mathcal{I}_{\mathcal{H}}} 1 = \sum_{i=0}^{s}\sum_{k=0}^{s-i}\sum_{j=0}^{1} 1 + \sum_{k=0}^{s}\sum_{j=2}^{\lfloor\tau k\rfloor+1} 1 \\ &\approx (s+1)(s+2) + \frac{\tau}{2}s(s+1) = \frac{2+\tau}{2}s^2 + o(s^2),\end{aligned}$$

$$\begin{aligned}n_X &= \sum_{(i,j,k)\in\mathcal{I}} i = \sum_{(i,j,k)\in\mathcal{I}_{\mathcal{G}}} i + \sum_{(i,j,k)\in\mathcal{I}_{\mathcal{H}}} i = \sum_{i=0}^{s}\sum_{k=0}^{s-i}\sum_{j=0}^{1} i \\ &\approx \frac{1}{3}s(s+1)(s+2) = \frac{1}{3}s^3 + o(s^3),\end{aligned}$$

$$\begin{aligned}n_Y &= \sum_{(i,j,k)\in\mathcal{I}} j = \sum_{(i,j,k)\in\mathcal{I}_{\mathcal{G}}} j + \sum_{(i,j,k)\in\mathcal{I}_{\mathcal{H}}} j = \sum_{i=0}^{s}\sum_{k=0}^{s-i}\sum_{j=0}^{1} j + \sum_{k=0}^{s}\sum_{j=2}^{\lfloor\tau k\rfloor+1} j \\ &\approx \frac{1}{2}(s+1)(s+2) + \frac{\tau^2}{12}s(s+1)(2s+1) + \frac{3\tau}{4}s(s+1) = \frac{\tau^2}{6}s^3 + o(s^3),\end{aligned}$$

$$n_Z = \sum_{(i,j,k)\in\mathcal{I}} k = \sum_{(i,j,k)\in\mathcal{I}_\mathcal{G}} k + \sum_{(i,j,k)\in\mathcal{I}_\mathcal{H}} k = \sum_{i=0}^{s}\sum_{k=0}^{s-i}\sum_{j=0}^{1} k + \sum_{k=0}^{s}\sum_{j=2}^{\lfloor \tau k\rfloor+1} k$$
$$\approx \frac{1}{3}s(s+1)(s+2) + \frac{\tau}{6}s(s+1)(2s+1) = \frac{1+\tau}{3}s^3 + o(s^3),$$
$$n_e = \sum_{(i,j,k)\in\mathcal{I}} (s-k) = \sum_{(i,j,k)\in\mathcal{I}_\mathcal{G}} (s-k) + \sum_{(i,j,k)\in\mathcal{I}_\mathcal{H}} (s-k) = \sum_{i=0}^{s}\sum_{k=0}^{s-i}\sum_{j=0}^{1}(s-k) + \sum_{k=0}^{s}\sum_{j=2}^{\lfloor \tau k\rfloor+1} (s-k)$$
$$\approx \frac{2}{3}s(s+1)(s+2) + \frac{\tau}{6}s(s-1)(s+1) = \frac{4+\tau}{6}s^3 + o(s^3).$$

Hence, we have $\det(\mathcal{L}) = X^{n_X} Y^{n_Y} Z^{n_Z} e^{n_e}$ for the above values. Substituting the values of X, Y, Z and e, the lattice determinant $\det(\mathcal{L})$ is approximately equal to

$$N^{(\alpha+\delta-2)\left(\frac{1}{3}s^3+o(s^3)\right)} N^{\frac{1}{2}\left(\frac{\tau^2}{6}s^3+o(s^3)\right)} N^{(\alpha+\delta-1)\left(\frac{1+\tau}{3}s^3+o(s^3)\right)} N^{\alpha\left(\frac{4+\tau}{6}s^3+o(s^3)\right)},$$

which can be simplified into

$$\det(\mathcal{L}) = N^{\left(\frac{1}{3}(\alpha+\delta-2)+\frac{\tau^2}{12}+\frac{1+\tau}{3}(\alpha+\delta-1)+\frac{4+\tau}{6}\alpha\right)s^3}$$

when omitting the lower order term $o(s^3)$. Consider the condition $\det(\mathcal{L}) < R^w$ for $R = e^s$, we substitute the values of e and deduce

$$R^w = e^{ws} = N^{\frac{2+\tau}{2}\alpha s^3}.$$

Hence, we deal with the exponents in $\det(\mathcal{L}) < R^w$ and obtain

$$4(\alpha+\delta-2) + \tau^2 + 4(1+\tau)(\alpha+\delta-1) + 2(4+\tau)\alpha < 6(2+\tau)\alpha.$$

It can be simplified into

$$\tau^2 + (4\delta-4)\tau + 4\alpha + 8\delta - 12 < 0.$$

The value of the left side reaches its minimum by setting $\tau = 2-2\delta$ and then the inequality becomes

$$\delta^2 - 4\delta - \alpha + 4 > 0.$$

Hence, we obtain the final condition

$$\delta < 2 - \sqrt{\alpha}.$$

Note that we must have $0 \le \tau = 2-2\delta \le 1$ and hence $1/2 \le \delta \le 1$. Combining it with $\alpha + \delta \ge 2$ and $\delta < 2-\sqrt{\alpha}$, we have $1 \le \alpha < 9/4$. We discuss more about how to solve the modular equation (2) for other cases like $0 < \alpha < 1$ and $\alpha \ge 9/4$. The optimizing parameter τ is no longer $\tau = 2-2\delta$ when considering other values of α.

For $0 < \alpha < 1$, we can infer that $\delta > 1$ and hence τ should be less than 0. In this case, we take $\tau = 0$ and obtain $\delta < (3-\alpha)/2$. Combining it with $\alpha + \delta \ge 2$, we have $2-\alpha \le \delta < (3-\alpha)/2$ leading to $\alpha > 1$, which contradicts the prerequisite $0 < \alpha < 1$. Therefore, we cannot solve the modular equation (2) for $0 < \alpha < 1$.

For $\alpha \ge 9/4$, we can infer that $\delta < 1/2$ and hence τ should be greater than 1. In this case, we take $\tau = 1$ and obtain $\delta < 5/4 - \alpha/3$. Combining it with $\alpha + \delta \ge 2$, we have $2-\alpha \le \delta < 5/4 - \alpha/3$ leading to $\alpha > 9/8$, which satisfies the prerequisite $\alpha \ge 9/4$. Besides, we should ensure $0 < \delta < 5/4 - \alpha/3$, which can be reduced to $\alpha < 15/4$. Therefore, we can solve the modular equation (2) for $9/4 \le \alpha < 15/4$ using $\tau = 1$.

Once we extract the common root $(x_0,\ y_0) = (k,\ p+q)$, we can easily factorize N using the value of $p+q$. The above results of our attacks are illustrated in Fig. 1. It is oblivious that we gain a significant finding of the insecure bound on δ through the lattice-based method. The RSA variant based on cubic Pell equation is not so secure as claimed.

To summarize, we propose the small private exponent attack on the RSA variant based on cubic Pell equation for the public key e of an arbitrary bit-size (i.e. an arbitrary value of α) as follows.

Proposition 2. *Let $N = pq$ be a modulus of the RSA variant based on cubic Pell equation. Two prime factors p and q are of the same bit-size. Let $e = N^\alpha$ be a valid public key and $d = N^\delta$ be its corresponding private key such that $ed \equiv 1 \bmod (p^2+p+1)(q^2+q+1)$. Then N can be efficiently factored in polynomial time if*

$$\delta < 2 - \sqrt{\alpha} \text{ for } 1 \le \alpha < \frac{9}{4}, \quad \text{or} \quad \delta < \frac{5}{4} - \frac{\alpha}{3} \text{ for } \frac{9}{4} \le \alpha < \frac{15}{4}.$$

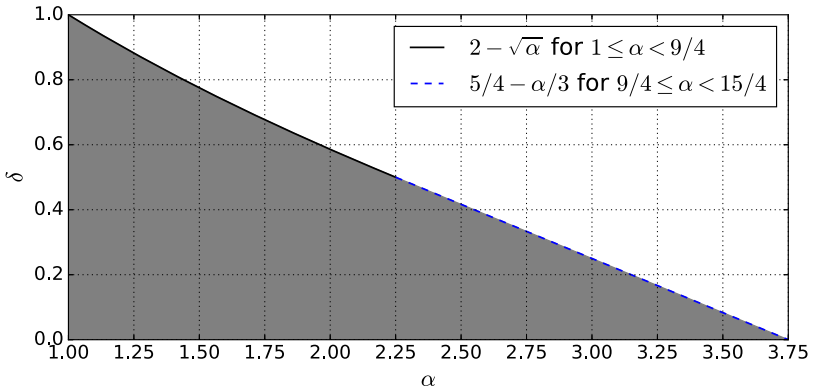

Fig. 1. The curves denote the asymptotic insecure bound on δ with respect to various α's. The gray region indicates the vulnerable attack scenarios of the proposed small private exponent attack on the RSA variant based on cubic Pell equation.

Table 2
The experimental results on the proposed small private key attack.

$\log_2 N$	$\alpha \log_2 N$	$\delta_e \log_2 N$	δ_e	s	τ	w	T_{LLL}	T_{GB}
1024	2044	439	0.428	3	1	26	0.419	0.100
1024	2047	467	0.456	4	1	40	6.807	0.137
1024	2048	485	0.473	5	1	57	126.737	0.115
1024	2047	496	0.484	6	1	77	3430.796	0.162
1024	2045	504	0.492	7	0.857	93	6149.896	0.146
1024	2045	514	0.501	8	1	126	23610.149	0.093
1024	2047	524	0.511	9	1	155	78149.222	10.715

For the general case when $e \approx (p^2+p+1)(q^2+q+1) \approx N^2$, we obtain the solvable condition $\delta < 2-\sqrt{2}$ as stated in Proposition 1 directly from Proposition 2. Note this insecure bound is much higher than that derived in the small private exponent attack on the standard RSA. Thus, the RSA variant based on cubic Pell equation is much more vulnerable to attacks using the lattice-based method.

4. Experimental results

In this section, we verify the validity of the proposed small private exponent attack on the RSA variant based on cubic Pell equation. The experiments are carried out in `SageMath`[1] under Windows 10 running on a laptop with Intel Core i7-8550U CPU 1.80 GHz. The numbers for generating the concrete parameters of RSA variant instances are chosen at random.

For each numerical experiment, we first generate a 1024-bit RSA modulus N (i.e. $\log_2 N = 1024$) with the private key d of predetermined bit-size. Then we generate the corresponding public key e according to the modified key equation $ed \equiv 1 \bmod (p^2+p+1)(q^2+q+1)$. Moreover, we gradually increase the bit-size of the public key e to achieve greater α when performing the small private exponent attack.

For conducting the proposed attack, we choose a suitable s with an optimal τ to construct the lattice. The experimental results are given in Table 2. The $\alpha \log_2 N$-column provides the bit-size of the public key of the generated RSA variant instance. The $\delta_e \log_2 N$-column provides the bit-size of the private key used in the experiments for our lattice settings, which are indicated by the s, τ and w-columns. The δ_e-column provides the experimental results of the insecure small private exponent in our attacks. The respective time consumption (recorded in seconds) of the LLL algorithm and the Gröbner basis computation are given in the T_{LLL} and T_{GB}-columns.

During each experiment, we could collect abundant polynomials satisfying the solvable requirements. In other words, we could obtain sufficient reduced basis vectors after running the lattice reduction algorithm. The running time of the LLL algorithm heavily depends on the lattice dimension and the entries of the lattice basis matrix. As showed in Table 2, the running time gets longer as the above parameters get larger. The polynomial equations sharing the common root over the integers are derived from the vector-to-polynomial transformation of the outputted lattice basis vectors.

We concisely comment on the root-extraction procedure of the proposed attack. We put the derived polynomials into the Gröbner basis computation and obtain $p+q$ that leads to the factorization of N. We successfully recover the common root in all the experiments, where we generate the RSA variant instances using the parameters showed in Table 2. The time consumption of the Gröbner basis computation is much lower than that for running the LLL algorithm. Unfortunately, the experimental results are still a few bits away from the asymptotic insecure bound due to the restricted computing resource.

[1] We use the Sage Mathematics Software System (Version 8.0) that is available at https://www.sagemath.org.

If we apply the lattice-based method with much higher-dimensional lattices, the practical attack results can be further improved.

5. Conclusions

We propose an effective lattice-based attack on the RSA variant based on cubic Pell equation using Coppersmith's techniques in this paper. Though such RSA variant is designed using complicated product and power computations, the key equation $ed \equiv 1 \bmod (p^2+p+1)(q^2+q+1)$ is quite simple. We focus on how to solve the bivariate modular equation $x(y^2+ay+b)+1 \equiv 0 \bmod e$ and present the small private exponent attack on this RSA variant. Further attack results for the public key e of arbitrary bit-size are also presented and illustrated. We justify the validity of the proposed small private exponent attack by numerical computer experiments.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

This work was partially supported by the National Natural Science Foundation of China under Grant Number 62002335 and 61802357, the National Key Research and Development Program of China under Grant Number 2018YFB0804102, JST CREST Grant Number JPMJCR14D6, Japan and JSPS KAKENHI Grant Number JP16H02780.

References

[1] R.L. Rivest, A. Shamir, L.M. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Commun. ACM 21 (2) (1978) 120–126, https://doi.org/10.1145/359340.359342.
[2] T. Takagi, Fast RSA-type cryptosystem modulo $p^k q$, in: H. Krawczyk (Ed.), Advances in Cryptology - CRYPTO '98, 18th Annual International Cryptology Conference, Santa Barbara, California, USA, August 23-27, 1998, Proceedings, in: Lecture Notes in Computer Science, vol. 1462, Springer, 1998, pp. 318–326.
[3] J.-J. Quisquater, C. Couvreur, Fast decipherment algorithm for RSA public-key cryptosystem, Electron. Lett. 18 (21) (1982) 905–907, https://doi.org/10.1145/359340.359342.
[4] K. Koyama, Fast rsa-type schemes based on singular cubic curves $y^2+axy \equiv x^3 \pmod n$, in: L.C. Guillou, J. Quisquater (Eds.), Advances in Cryptology - EUROCRYPT '95, International Conference on the Theory and Application of Cryptographic Techniques, Saint-Malo, France, May 21-25, 1995, Proceeding, in: Lecture Notes in Computer Science, vol. 921, Springer, 1995, pp. 329–340.
[5] N. Murru, F.M. Saettone, A novel RSA-like cryptosystem based on a generalization of the Rédei rational functions, in: J. Kaczorowski, J. Pieprzyk, J. Pomykała (Eds.), Number-Theoretic Methods in Cryptology, NuTMiC 2017, in: Lecture Notes in Computer Science, vol. 10737, Springer, Cham, 2018, pp. 91–103.
[6] J. Håstad, On using RSA with low exponent in a public key network, in: H.C. Williams (Ed.), Advances in Cryptology - CRYPTO '85, Santa Barbara, California, USA, August 18-22, 1985, Proceedings, in: Lecture Notes in Computer Science, vol. 218, Springer, 1985, pp. 403–408.
[7] M.J. Wiener, Cryptanalysis of short RSA secret exponents, IEEE Trans. Inf. Theory 36 (3) (1990) 553–558, https://doi.org/10.1109/18.54902.
[8] W. Susilo, J. Tonien, G. Yang, The Wiener attack on RSA revisited: a quest for the exact bound, in: J. Jang-Jaccard, F. Guo (Eds.), Information Security and Privacy - 24th Australasian Conference, ACISP 2019, Christchurch, New Zealand, July 3-5, 2019, Proceedings, in: Lecture Notes in Computer Science, vol. 11547, Springer, 2019, pp. 381–398.
[9] D. Boneh, G. Durfee, Cryptanalysis of RSA with private key d less than $N^{0.292}$, in: J. Stern (Ed.), Advances in Cryptology - EUROCRYPT '99, International Conference on the Theory and Application of Cryptographic Techniques, Prague, Czech Republic, May 2-6, 1999, Proceeding, in: Lecture Notes in Computer Science, vol. 1592, Springer, 1999, pp. 1–11.
[10] D. Coppersmith, Small solutions to polynomial equations, and low exponent RSA vulnerabilities, J. Cryptol. 10 (4) (1997) 233–260, https://doi.org/10.1007/s001459900030.
[11] M. Herrmann, A. May, Maximizing small root bounds by linearization and applications to small secret exponent RSA, in: P.Q. Nguyen, D. Pointcheval (Eds.), Public Key Cryptography - PKC 2010, 13th International Conference on Practice and Theory in Public Key Cryptography, Paris, France, May 26-28, 2010, Proceedings, in: Lecture Notes in Computer Science, vol. 6056, Springer, 2010, pp. 53–69.
[12] A. Takayasu, Y. Lu, L. Peng, Small CRT-exponent RSA revisited, J. Cryptol. 32 (4) (2019) 1337–1382, https://doi.org/10.1007/s00145-018-9282-3.
[13] Y. Lu, R. Zhang, L. Peng, D. Lin, Solving linear equations modulo unknown divisors: revisited, in: T. Iwata, J.H. Cheon (Eds.), Advances in Cryptology - ASIACRYPT 2015 - 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, November 29 - December 3, 2015, Proceedings, Part I, in: Lecture Notes in Computer Science, vol. 9452, Springer, 2015, pp. 189–213.
[14] A. Takayasu, N. Kunihiro, How to generalize RSA cryptanalyses, in: C. Cheng, K. Chung, G. Persiano, B. Yang (Eds.), Public-Key Cryptography - PKC 2016 - 19th IACR International Conference on Practice and Theory in Public-Key Cryptography, Taipei, Taiwan, March 6-9, 2016, Proceedings, Part II, in: Lecture Notes in Computer Science, vol. 9615, Springer, 2016, pp. 67–97.
[15] A. Takayasu, N. Kunihiro, Cryptanalysis of RSA with multiple small secret exponents, in: W. Susilo, Y. Mu (Eds.), Information Security and Privacy - 19th Australasian Conference, ACISP 2014, Wollongong, NSW, Australia, July 7-9, 2014, Proceedings, in: Lecture Notes in Computer Science, vol. 8544, Springer, 2014, pp. 176–191.
[16] M. Zheng, H. Hu, Cryptanalysis of prime power RSA with two private exponents, Sci. China Inf. Sci. 58 (11) (2015) 1–8, https://doi.org/10.1007/s11432-015-5409-4.
[17] M. Zheng, N. Kunihiro, H. Hu, Cryptanalysis of RSA variants with modified Euler quotient, in: A. Joux, A. Nitaj, T. Rachidi (Eds.), Progress in Cryptology - AFRICACRYPT 2018 - 10th International Conference on Cryptology in Africa, Marrakesh, Morocco, May 7-9, 2018, Proceedings, in: Lecture Notes in Computer Science, vol. 10831, Springer, 2018, pp. 266–281.
[18] L. Peng, A. Takayasu, Generalized cryptanalysis of small CRT-exponent RSA, Theor. Comput. Sci. 795 (2019) 432–458, https://doi.org/10.1016/j.tcs.2019.07.031.

[19] M. Zheng, H. Hu, Z. Wang, Generalized cryptanalysis of RSA with small public exponent, Sci. China Inf. Sci. 59 (3) (2016) 32108, https://doi.org/10.1007/s11432-015-5325-7.
[20] M.W. Bunder, A. Nitaj, W. Susilo, J. Tonien, A generalized attack on RSA type cryptosystems, Theor. Comput. Sci. 704 (2017) 74–81, https://doi.org/10.1016/j.tcs.2017.09.009.
[21] M. Ernst, E. Jochemsz, A. May, B. de Weger, Partial key exposure attacks on RSA up to full size exponents, in: R. Cramer (Ed.), Advances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005, Proceedings, in: Lecture Notes in Computer Science, vol. 3494, Springer, 2005, pp. 371–386.
[22] A. Takayasu, N. Kunihiro, Partial key exposure attacks on RSA: achieving the Boneh-Durfee bound, Theor. Comput. Sci. 761 (2019) 51–77, https://doi.org/10.1016/j.tcs.2018.08.021.
[23] K. Suzuki, A. Takayasu, N. Kunihiro, Extended partial key exposure attacks on RSA: improvement up to full size decryption exponents, Theor. Comput. Sci. 841 (2020) 62–83, https://doi.org/10.1016/j.tcs.2020.07.004.
[24] N. Kunihiro, Solving generalized small inverse problems, IEICE Trans. Fundam. Electron. Commun. Comput. Sci. 94-A (6) (2011) 1274–1284, https://doi.org/10.1587/transfun.E94.A.1274.
[25] N. Kunihiro, On optimal bounds of small inverse problems and approximate GCD problems with higher degree, in: D. Gollmann, F.C. Freiling (Eds.), Information Security - 15th International Conference, ISC 2012, Passau, Germany, September 19-21, 2012, Proceedings, in: Lecture Notes in Computer Science, vol. 7483, Springer, 2012, pp. 55–69.
[26] A. Takayasu, N. Kunihiro, General bounds for small inverse problems and its applications to multi-prime RSA, IEICE Trans. Fundam. Electron. Commun. Comput. Sci. 100-A (1) (2017) 50–61, https://doi.org/10.1587/transfun.E100.A.50.
[27] D. Coppersmith, Finding a small root of a univariate modular equation, in: U.M. Maurer (Ed.), Advances in Cryptology - EUROCRYPT '96, International Conference on the Theory and Application of Cryptographic Techniques, Saragossa, Spain, May 12-16, 1996, Proceeding, in: Lecture Notes in Computer Science, vol. 1070, Springer, 1996, pp. 155–165.
[28] A.K. Lenstra, H.W. Lenstra, L. Lovász, Factoring polynomials with rational coefficients, Math. Ann. 261 (4) (1982) 515–534.
[29] A. May, New RSA vulnerabilities using lattice reduction methods, Ph.D. thesis, University of Paderborn, 2003, http://ubdata.uni-paderborn.de/ediss/17/2003/may/disserta.pdf.
[30] E. Jochemsz, A. May, A strategy for finding roots of multivariate polynomials with new applications in attacking RSA variants, in: X. Lai, K. Chen (Eds.), Advances in Cryptology - ASIACRYPT 2006, 12th International Conference on the Theory and Application of Cryptology and Information, Security, Shanghai, China, December 3-7, 2006, Proceedings, in: Lecture Notes in Computer Science, vol. 4284, Springer, 2006, pp. 267–282.
[31] A. May, Using LLL-reduction for solving RSA and factorization problems, in: P.Q. Nguyen, B. Vallée (Eds.), The LLL Algorithm - Survey and Applications, Information Security and Cryptography, Springer, 2010, pp. 315–348.
[32] N. Howgrave-Graham, Finding small roots of univariate modular equations revisited, in: M. Darnell (Ed.), Cryptography and Coding, 6th IMA International Conference, Cirencester, UK, December 17-19, 1997, Proceedings, in: Lecture Notes in Computer Science, vol. 1355, Springer, 1997, pp. 131–142.
[33] T. Becker, V. Weispfenning, H. Kredel, Gröbner Bases - a Computational Approach to Commutative Algebra, Graduate Texts in Mathematics, vol. 141, Springer, 1993.