Cryptanalysis of RSA with Moduli N=p^rq Based on Coppersmith Method: A survey

Simeng Yuan, Wei Yu, Kunpeng Wang, Xiuxiu Li
State Key Laboratory of Information Security, Institute of Information Engineering, CAS
School of Cyber Security, University of Chinese Academy of Sciences
Beijing, China
emails: yuansimeng@iie.ac.cn, yuwei_1_yw@163.com, wangkunpeng@iie.ac.cn, lixiuxiu@iie.ac.cn

***Abstract*—This paper briefly summarizes the Coppersmith method, its extension strategy and lattice construction techniques. Then we describe several attacks on Rivest-Shamir-Adleman cryptosystem with moduli $N = p^r q$ based on Coppersmith method, including small exponent attacks, partial key exposure attacks, and factoring RSA moduli with partial known. A survey of recent progress for these three kinds of attacks, and general methods on how these attacks work are given.**

***Keywords*—Coppersmith method; Takagi RSA; prime power RSA.**

I. INTRODUCTION

RSA is one of the most widely used public key cryptosystems today. In the environment with limited resources, it may be slow for encryption and decryption, due to the modular operation of large integers. In order to speed up the operation, many RSA fast variants have been produced. One of the most important variants is the scheme proposed by Takagi [30] with moduli $N = p^r q$. Compared with the standard RSA scheme, Takagi RSA is more efficient in key generation and decryption. Another fast variant with moduli $N = p^r q$ is the prime power RSA. For Takagi RSA, the public exponent e and the secret exponent d satisfy

$$ed \equiv 1 \bmod (p-1)(q-1),$$

and for the prime power RSA, e and d satisfy

$$ed \equiv 1 \bmod p^{r-1}(p-1)(q-1).$$

These fast variants are usually used in smart cards and programs with higher speed.

With the development of lattice theory, the famous algorithm proposed by Lenstra, Lenstra and Lovász (LLL algorithm), and lattice basis reduction technique has become an important tool for cryptanalysis of RSA and its variants. In 1996, Coppersmith proposed so called Coppersmith algorithm to find small roots of single variable modular equation [7] or the double variable integer equation [6]. The core idea of this algorithm is to convert the modular equation or integer equation with large norm into integer equations with small norm by lattice basis reduction algorithm such as LLL algorithm, and the roots of the original equation can be found over integers. In the above process, the construction of the lattice basis is the most critical part. Howgrave-Graham [16] simplified the work of [7], and put forward a more straightforward lattice basis construction method, which can be generalized to the case of multivariable modular equation. Since then, a large number of scholars have used this lattice analysis method to analyze the security of RSA. The method has also continued to be extended, and gradually form the current Coppersmith method. In 2006, Jochemsz and May [19] proposed a general strategy for multivariate modular equations and integer equations. They gave a method to obtain a triangular matrix when one constructs lattice basis. In the case of multivariable equations, the methods mentioned above are based on a heuristic assumption that the reduced basis output by LLL algorithm is algebraically independent.

In order to get a better lattice, there are many lattice basis construction techniques, of which the two most widely used techniques are substitution technique and unraveled linearization technique. Substitution technique was first used by Durfee and Nguyen [10]. According to the RSA equation $ed = 1 + k(p-1)(q-1)$, they constructed a three variable modular equation $f(x, y, z) = x(N + 1 + y + z) + 2 \pmod e$ with roots $(x_0, y_0, z_0) = (k, -p, -q)$. Knowing $N = pq$, they replaced all occurrences of the monomial yz with N, when constructing the lattice. By this substitution technique, they reduced the number of variables and optimized the result of lattice analysis. Unraveled linearization technique was first proposed by Herrmann and May [14]. By exploiting the implicit algebraic relationships in equations, the construction of lattice can be simplified and the result of lattice analysis can be improved.

In this paper, we focus on RSA with moduli $N = p^r q$, and survey the applications of Coppersmith method in the cryptanalysis of it.

The remainder of this paper is organized as follows. In Section II, we describe the theory and steps of Coppersmith method, and summarize Jochemsz-May strategy and unraveled linearization. The general methods of small exponent attacks on RSA with moduli $N = p^r q$ are given in Section III. We conclude the partial key exposure attacks in Section IV, and the methods of factoring RSA moduli with partial known in Section V. Section VI gives the development suggestions.

II. COPPERSMITH METHOD

Before describing the Coppersmith method, we first revise the concept of lattices and LLL algorithm. Let $\boldsymbol{b_1}, \ldots, \boldsymbol{b_n} \in$

 ISBN: 978-1-61208-919-5

$\mathbb{Z}^{\omega}$ be linearly independent row vectors. The set of all integer linear combinations of $\boldsymbol{b_1}, \ldots, \boldsymbol{b_n}$ compose lattice, which is written as

$$L(\boldsymbol{b_1}, \ldots, \boldsymbol{b_n}) = \left\{ \sum_{j=1}^{n} x_j \boldsymbol{b_j} : x_j \in \mathbb{Z} \right\}.$$

We write n the rank of the lattice and ω the dimension of the lattice. The matrix $B \in \mathbb{Z}^{n \times \omega}$ consisting of $\boldsymbol{b_1}, \ldots, \boldsymbol{b_n}$ is a basis matrix of lattice L. We call these lattices full-rank when $n = \omega$. The determinant of L is denoted as $\det(L) = \sqrt{\det(BB^T)}$. In order to find short vectors on lattices, Lenstra, Lenstra and Lovász proposed the LLL algorithm [20].

Lemma 1 (LLL). L is a ω-dimensional lattice, and the LLL algorithm can output a reduced basis vectors $\boldsymbol{v_1}, \ldots, \boldsymbol{v_\omega}$ satisfying

$$\|\boldsymbol{v_i}\| \leq 2^{\frac{\omega(\omega-1)}{4(\omega-i+1)}} \det(L)^{\frac{1}{\omega-i+1}}, \text{ for } 1 \leq i \leq \omega.$$

The time complexity of LLL algorithm is polynomial in ω and the bitsize of input.

A. Coppersmith Method

Coppersmith [7] described the method to get small root of modular equations based on LLL algorithm. Then, the sufficient condition for Coppersmith method was given by Howgrave-Graham [16].

Lemma 2 (Howgrave-Graham). Let $g(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ be a polynomial, which has at most δ monomials. Let p, m be positive integers. Suppose that

1.$g(\widetilde{x}_1, \ldots, \widetilde{x}_n) \equiv 0 \pmod{p^m}$, where $|\widetilde{x}_1| < X_1, \ldots, |\widetilde{x}_n| < X_n$,

2.$\|g(x_1X_1, \ldots, x_nX_n)\| < \frac{p^m}{\sqrt{\delta}}$.

Then, $g(\widetilde{x}_1, \ldots, \widetilde{x}_n) = 0$ holds over integers.

Therefore, the modular equation can be converted into n integer equations, if these n short vectors output by LLL algorithm satisfy Lemma 2, that is

$$\|\boldsymbol{v_i}\| \leq 2^{\frac{\omega(\omega-1)}{4(\omega-i+1)}} \det(L)^{\frac{1}{\omega-i+1}} < \frac{p^m}{\sqrt{\delta}}, \text{ for } 1 \leq i \leq \omega.$$

Ignoring the small items, the condition becomes $\det(L) < p^{m\omega}$. One can use Gröbner base or a resultant of these n integer equations to find all roots.

Next, we will illustrate the general steps of Coppersmith method. Take the solution of univariate modular equation for example. Let $f(x)$ be a univariate modular polynomial of degree δ

$$f(x) = x^{\delta} + a_{\delta-1}x^{\delta-1} + \ldots + a_1x + a_0 \pmod{p}.$$

The root of $f(x_0) \equiv 0 \pmod{p}$, is bound by X. And the steps of Coppersmith method are as follows.

- Construct ω shift polynomials $g_1(x), \ldots, g_\omega(x)$, which have the same small roots x_0 modulo p^m, and m, t is positive integers (which can be optimized). Shift polynomials can be constructed in the following way
  $g_i(x) = x^i p^{m-j} f^j(x)$ for $i = 0, \ldots, \delta-1, j = 0, \ldots, m-1$,
  $g_{\delta+i}(x) = x^i f^m(x)$ for $i = 0, \ldots, t-1$.
- Use the coefficient vectors of $g_i(xX)$ and $g_{\delta+i}(xX)$ to construct a lattice basis.
- Apply LLL algorithm to the lattice basis, and we get a short vector $\boldsymbol{v}$, corresponding a polynomial $v(x)$. Since the vectors on the lattice are integer linear combination of the lattice basis vectors, the polynomials $v(x)$ is integer linear combination of $g_i(x)$ and $g_{\delta+i}(x)$, with the same small roots x_0 modulo p^m.
- If $\boldsymbol{v}$ is short enough to satisfy Lemma 2, the modular equation can be converted to an integer equation. And we can solve it over integers

For the case of multivariate modular equation $f(x_1, \ldots, x_n) \equiv 0 \bmod p$, the steps are similar. Notice that the dimension of the lattice should be larger than the number of variables, which means $\omega > n$. And the shift polynomials can be defined as

$$g_{i_1,\ldots,i_n}(x_1, \ldots, x_n) := x_1^{i_1}, \ldots, x_n^{i_n} p^{m-j} f^j$$

The parameters $i_1, \ldots, i_n$ and j are selected based on different cases.

The most time-consuming part of Coppersmith method is LLL algorithm, and it works in polynomial time. Therefore, Coppersmith method also works in polynomial time.

B. Jochemsz-May Strategy

In order to optimize the bound of desired roots, Jochemsz and May [19] proposed a general strategy for constructing full rank lattices and gave the methods to solve modular equations and integer equations with arbitrary variables. Jochemsz-May strategy is the best method for finding small roots of integer equations at present. Next, we will describe Jochemsz-May strategy to solve small roots of multivariate integer equations.

Let $f(x_1, \ldots, x_n) = \sum f_{i_1,\ldots,i_n} x_1^{i_1} \cdots x_n^{i_n}$ be a monic polynomial with roots $(\widetilde{x}_1, \ldots, \widetilde{x}_n)$ which are bound by $(X_1, \ldots X_n)$. First, we give some notations. Denote l_j as the maximum exponent of x_j in $f(x_1, \ldots, x_n)$. Take an integer W as large as possible satisfying that $W \leq \|f(x_1, \ldots, x_n)\|_{\infty}$. Define an integer $R := W X_1^{l_1(m-1)+t} \prod_{j=2}^{k} X_j^{l_j(m-1)}$ (m and $t = O(m)$ are positive integers, which will be optimized later). Then, we define two sets

$$S := \bigcup_{0 \leq j \leq t} \{x_1^{i_1+j} x_2^{i_2} \cdots x_k^{i_k} \mid x_1^{i_1} x_2^{i_2} \cdots x_k^{i_k} \text{ is a monomial of } f^{m-1}\}$$

$$M := \{\text{monomial of } x_1^{i_1} \cdots x_k^{i_k} \cdot f \mid x_1^{i_1} \cdots x_k^{i_k} \in S\}$$

The next steps are similar to the original Coppersmith method. 1) Construct a set of shift polynomials with the same roots $(\widetilde{x}_1, \ldots, \widetilde{x}_n)$ modulo R. 2) Construct lattice by the coefficient vectors of the shift polynomials. 3) Apply LLL algorithm to get n short vectors. 4) Obtain n integer equations corresponding these n short vectors, and solve these integer

equations. The selection of shift polynomials is different from the original Coppersmith method.

$$g : x_1^{i_1} \cdots x_k^{i_k} \cdot f \cdot X_1^{l_1(m-1)+t-i_1} \prod_{j=2}^{k} X_j^{l_j(m-1)-i_j}, \quad \text{for } x_1^{i_1} \cdots x_k^{i_k} \in S$$

$$g' : x_1^{i_1} \cdots x_k^{i_k} \cdot R, \text{ for } x_1^{i_1} \cdots x_k^{i_k} \in M \backslash S$$

And the condition to get all small roots becomes

$$\prod_{j=1}^{k} X_j^{s_j} < W^{|S|} \text{ for } s_j = \sum_{x_1^{i_1} \ldots x_k^{i_k} \in M \backslash S} i_j$$

C. Unraveled linearization

Herrmann and May [14], combining the method of linearization and Coppersmith method, introduced a new technique called unraveled linearization.

Recall the work of Boneh and Durfee [3]. They transformed the RSA moduli factorization problem into solving the small inverse problem. Specifically, they obtained an equation $ed + k(N + 1 - p - q) = 1$ from RSA equation $ed \equiv 1 \bmod \varphi(N)$. Let $A = (N + 1)$ and $s = (-p - q)$. Then, they got $k(A + s) = 1 \bmod e$, where k, s are unknown. The RSA system can be completely broken by solving small roots of the modular equation

$$f(x, y) = 1 + x(A + y) = 0 \bmod e.$$

Let $e = N^{\alpha}, d = N^{\beta}$. The small roots $(x_0, y_0) = (-k, s)$ satisfy

$$|x_0| = |k| = \frac{ed - 1}{\varphi(N)} < \frac{ed}{\frac{1}{2}N} = 2N^{\alpha+\beta-1} = X,$$
$$|y_0| = |-s| = p + q < 2N^{\frac{1}{2}} = Y.$$

For a fixed integer m, Boneh and Durfee constructed two sets of shift polynomials, such that the roots are the same as (x_0, y_0) modulo e^m.

$$g_{i,j}(x, y) = x^i e^{m-j} f^j \text{ for } i = 0, \ldots, m - j, \ j = 0, \ldots, m$$
$$h_{i,j}(x, y) = y^i e^{m-j} f^j \text{ for } i = 1, \ldots, t, \ j = 0, \ldots, m$$

Next, we use a example to illustrate the construction of lattice basis in [3]. Let $m = 2, t = 1$, and the lattice basis matrix consisting of the coefficient vectors of $g_{i,j}(xX, yY)$ and $h_{i,j}(xX, yY)$ is as Figure 1.

According to Coppersmith method, the equation can be solved under the condition $\det(L) < e^{m\omega}$ (ω is dimension of the lattice). The elements on the diagonal should be as small as possible to make this condition easier to meet. On average, the diagonal elements less than e^m are helpful. We call the shift polynomials helpful if the diagonal elements introduced by them are less than e^m. For the sake of better lattice and superior result, Boneh and Durfee [3] excluded the unhelpful polynomials ye^2 and yef. Consequently, the lattice basis matrix was no longer triangular, and it is difficult to derive the determinant formula for general m and t. They

	1	x	x^2	xy	x^2y	x^2y^2	y	xy^2	x^2y^3
$g_{0,0} = e^2$	e^2								
$g_{1,0} = xe^2$		e^2X							
$g_{2,0} = x^2e^2$			e^2X^2						
$g_{0,1} = ef$	e	eAX		eXY					
$g_{1,1} = xef$		eX	eAX^2		eX^2Y				
$g_{0,2} = f^2$	1	$2AX$	A^2X^2	$2XY$	$2AX^2Y$	X^2Y^2			
$\boldsymbol{h_{1,0} = ye^2}$							e^2Y		
$\boldsymbol{h_{1,1} = yef}$				$eAXY$			eY	eXY^2	
$h_{1,2} = yf^2$				$2AXY$	A^2X^2Y	$2AX^2Y^2$	Y	$2XY^2$	X^2Y^3

Figure 1. Lattice basis for $m = 2, t = 1$.

introduced a technique called geometric progressive matrix to solve this problem.Their result shows that one can factor the modulus N in polynomial time, when $d < N^{0.292}$. So far, no other attack improve this bound.

Herrmann and May applied the unraveled linearization technique [15], and got the same result as [3]. They replaced $xy + 1$ by u, and changed the original polynomial $f(x, y) = 1 + x(A + y) = 0 \pmod e$ into a linear polynomial $\hat{f}(x, u) = u + Ax = 0 \pmod e$. They used the new polynomial $\hat{f}(x, u)$ to construct shift polynomials in the similar way. They replaced xy by $u - 1$, x^2y by $ux - x$, and uxy by $u^2 - u$. Then, for $m = 2, t = 1$, the lattice basis matrix is as Figure 2.

	1	x	x^2	u	ux	u^2	y	uy	u^2y
$g_{0,0} = e^2$	e^2								
$g_{1,0} = xe^2$		e^2X							
$g_{2,0} = x^2e^2$			e^2X^2						
$g_{0,1} = ef$		eAX		eU					
$g_{1,1} = xef$			eAX^2		eUX				
$g_{0,2} = f^2$			A^2X^2		$2AUX$	U^2			
$\boldsymbol{h_{1,0} = ye^2}$							e^2Y		
$\boldsymbol{h_{1,1} = yef}$	$-eA$			eAU				eUY	
$h_{1,2} = yf^2$		$-A^2X$		$-2AU$	A^2UX	$2AU^2$			U^2Y

Figure 2. Lattice basis for $m = 2, t = 1$.

It is also a triangular matrix after removing the unhelpful polynomials ye^2 and $ye\hat{f}$, because $y\hat{f}^2$ only introduces one monomial u^2y.

Although Herrmann and May [15] did not improve the bound $d < N^{0.292}$, they simplified the calculation of determinant by unraveled linearization technique.

D. Factor RSA Moduli by Coppersmith Method

Coppersmith method is a kind of method to solve the small roots of modular equations or integer equations, which can be construted from RSA equations. Due to special parameter selection (small private key exponent d) or partial information (partial private key d or partial p) exposured, the roots have upper bound and we just need to find all the roots in a relatively small range. Therefore, RSA is broken by Coppersmith method.

Next, we will discuss how to construct the equations and use Coppersmith method to solve them in three specific cases

including private key exponent d small, partial private key d known and partial information of p known. Suppose that the size of p and q are the same. Let $e = N^{\alpha}, d = N^{\beta}$. For partial key exposure attacks, we write known partial of d as $\widetilde{d}$. When most significant bits (MSBs) are known, write unknown bits as $d_0 = d - \widetilde{d}$ such that $|d_0| < N^{\delta}$. For known least significant bits (LSBs) of the private exponent, denote d_1 as unknown bits, and $d = d_1 M + \widetilde{d}$, where $M = 2^{\lfloor (\beta-\delta)\log N \rfloor}$.

III. Small Exponent Attacks

Wiener [33] proposed an attack on RSA with small decryption exponent. Their algorithm was based on continued fraction, and they proved that d can be recovered in polynomial time under the condition $d < N^{0.25}$. Boneh and Durfee [3] improved Wiener's bound to $d < N^{0.292}$ based on Coppersmith method. Next, we mainly discuss the small decryption exponent attack on RSA with moduli $N = p^r q$.

A. Attack on Takagi RSA

Recall the equation of Takagi RSA

$$ed \equiv 1 \bmod (p-1)(q-1).$$

There is an integer k satisfying

$$ed - k\,(p-1)\,(q-1) = 1$$

where k, p, q and d are unknown. Then, we construct a three-variable modular polynomial

$$f\,(x,y,z) = x\,(y-1)\,(z-1) + 1 = 0 \pmod{e}.$$

The roots $(x_0, y_0, z_0) = (k, p, q)$ of the equation have upper bounds

$$|x_0| = |k| = \frac{ed-1}{(p-1)(q-1)} < \frac{2ed}{pq} < N^{\alpha+\beta-\frac{2}{(r+1)}} = X,$$
$$|y_0| = |p| < 2N^{1/(r+1)} = Y,$$
$$|z_0| = |q| < 2N^{1/(r+1)} = Z.$$

Then, we use the Coppersmith method to find the small roots. Due to the additional algebraic relations $N = p^r q$, we use substitution technique (replace each occurrence of $y^r z$ by N to construct the lattice) to optimize the lattice basis. Unraveled linearization technique can also be used to remove unhelpful polynomials and construct triangular matrices which are easier to analyze.

Itoh et al. [18] proved that d can be recovered in polynomial time when $d \leq N^{\frac{2-\sqrt{2}}{r+1}}$. Their result is based on geometric progressive matrix. The attack on standard RSA described by Boneh and Durfee [3] is a special case of $r = 1$. Takayasu and Kunihiro [32] obtained the same results based on unraveled linearization technique. They use linearization $u_1 = 1 + xy$ and $u_2 = 1 + xz$ to remove the unhelpful polynomials and construct a triangular matrix which simplify the calculation.

B. Attack on Prime Power RSA

Recall the equation of prime power RSA

$$ed \equiv 1 \bmod p^{r-1}(p-1)(q-1).$$

There is an integer k satisfying

$$ed - kp^{r-1}\,(p-1)\,(q-1) = 1$$

where $k,\ p,\ q$ and d are unknown. A three-variable modular polynomial is obtained

$$f\,(x,y,z) = 1 + xy^{r-1}(y-1)(z-1) = 0 \pmod{e}.$$

The roots $(x_0, y_0, z_0) = (k, p, q)$ are bound by $X = N^{\alpha+\beta-1}, Y = Z = 2N^{1/(r+1)}$.

In the similar way, we use Coppersmith method to find the roots of the modular equation and factor N.

Takagi [30] applied Wiener's attack on prime power RSA and proved that one can recover d in polynomial time under the condition $d \leq N^{\frac{1}{2(r+1)}}$. Later, May [25] gave two small exponent attacks using Coppersmith method. The first attack works when $d \leq N^{\frac{r}{(r+1)^2}}$ for $r \geq 2$, based on the result of [5]. The second attack works when $d \leq N^{1-\frac{4r}{(r+1)^2}}$ for $r \geq 2$, based on solving univariate modular equation. Sarkar [27] studied the case of $r = 2$, and showed that N can be factored in polynomial time when $d < N^{0.395}$. It improves the bound $d < N^{0.22}$ in [25]. Lu et al. [24] put forward three algorithms for solving three types of linear equations. The first one is multivariate linear equation modulo an unknown divisor p^v for a known composite integer N ($N \equiv 0 \bmod p^u, u \geq 1$). As an application of the algorithm, they proved that one can factor N when $d < N^{\frac{r(r-1)}{(r+1)^2}}$, which improves the work of [25]. Sarkar [28] further extended the result of [27]. They studied the case of $2 < r < 8$, and improved previous works when $r = 3, 4$.

Similar to modular equation, one can obtain integer equations

$$f\,(x_1,x_2,x_3,x_4) = 1 - ex_1 + x_2(x_3-1)(x_4-1).$$

from Takagi RSA, and

$$f\,(x_1,x_2,x_3,x_4) = 1 - ex_1 + x_2x_3^{r-1}(x_3-1)(x_4-1).$$

from prime power RSA.

Then, we can follow the steps of Jochemsz-May strategy to solve small roots of the integer equations. Takayasu and Kunihiro analyzed the case of solving integer equation base on Jochemsz-May strategy. Their results [32] show that using modular equation and unraveled linearization technique can analyze a wider range than using integer equation and Jochemsz-May strategy. Therefore, the modular equation combined with unraveled linearization can usually obtain better results.

 ISBN: 978-1-61208-919-5

C. Attack on RSA with Modulus $N = p^r q^s$

Lim et al. [21] proposed a RSA scheme with modulus $N = p^r q^s$. They showed that the scheme is even more efficient. Lu et al. [22] extended small exponent attack to RSA with moduli $N = p^r q^s$. They analyzed both variants satisfying $ed \equiv 1 \bmod (p-1)(q-1)$ and $ed \equiv 1 \bmod p^{r-1}(p-1)(q-1)$. For the first variant, they used the same modular equation as the attack on Takagi RSA. Note that they replaced $y^r z^s$ with N instead of $y^r z$. Finally, they proved that N can be factored in polynomial time when $d \leq N^{\frac{7-2\sqrt{7}}{3(r+s)}}$. For the second variant, they used an univariable modulus equation. They took d as the variable and obtained a modular equation

$$f(x) = (E - x) \bmod p^{r-1} q^{s-1}$$

where E is the inverse of e modulo N. Finally, they proved that N can be factored in polynomial time when $d < N^{1-(3r+s)(r+s)^{-2}}$.

IV. Partial Key Exposure Attacks

In 1998, Boneh, Durfee and Frankel [4] studied partial private key exposure attack on RSA with moduli $N = pq$. They pointed out that if one knows a quarter bit of the private, it is enough to recover the whole private key, when the encryption exponent is small. More private key bits are required for recovering private key with a larger encryption exponent. However, their attacks only work when $e < N^{0.5}$. Subsequently, Blömer and May [2] improved the result of [4], expanding the range of e from $N^{0.5}$ to $N^{0.725}$. When the LSBs are known, they proposed an algorithm with better result $e < N^{0.875}$. Soon afterwards, Ernst et al. [11] proposed some attacks for known MSBs or LSBs of the private exponent. Their work first considers the case of full size e. Aono [1] proposed an optimized method for lattice construction, and use it to attack RSA with small d and known LSBs of d. The method is theoretically more effective than the previous partial private key exposure attack. Later, Takayasu and Kunihiro [31] combined unraveled linearization technique and improved previous works. They gave the attacks with known MSBs of $d < N^{0.5625}$ or LSBs of $d < N^{0.368}$. Recently, Suzuki, Takayasu and Kunihiro [29] extended the work of [31] and proposed an attack when both MSBs and LSBs of d are known. At the same time, some scholars have also studied private key exposure attacks of other RSA variants. Next, we mainly discuss private key exposure attacks on RSA with modulus $N = p^r q$.

A. Attack on Takagi RSA

If we know the MSBs of d, and the equation of Takagi RSA is

$$e\left(\widetilde{d} + d_0\right) = 1 + k(p-1)(q-1)$$

where d_0, k, p, q are unknown. A four variable modular polynomial is obtained

$$f(x_1, x_2, x_3, x_4) = ex_1 + x_2(x_3 - 1)(x_4 - 1) + 1$$

The roots $(\widetilde{x}_1, \widetilde{x}_2, \widetilde{x}_3, \widetilde{x}_4) = (-d_0, k, p, q)$ of $f(\widetilde{x}_1, \widetilde{x}_2, \widetilde{x}_3, \widetilde{x}_4) = 0 \pmod{e\widetilde{d}}$ are bound by $X_1 = N^{\delta}, X_2 = 2N^{\alpha+\beta-2/(r+1)}, X_3 = X_4 = 2N^{1/(r+1)}$.

Suppose the LSBs of d are exposured, and the equation of Takagi RSA can be rewritten as

$$e\left(d_1 M + \widetilde{d}\right) = 1 + k(p-1)(q-1).$$

We can construct a three variable modular polynomial

$$f(x, y, z) = x(y-1)(z-1) + \left(1 - e\widetilde{d}\right).$$

The roots $(x_0, y_0, z_0) = (k, p, q)$ of $f(x_0, y_0, z_0) = 0 \pmod{eM}$ are bound by $X = 2N^{\alpha+\beta-2/(r+1)}, Y = Z = 2N^{1/(r+1)}$.

Thus, the problem of recovering d is converted to solving modular equation.

We can also use the integer equation. Assuming we know some bits of d regardless of the MSBs or LSBs. Write known bits as $\widetilde{d}$, and the equation of Takagi RSA is

$$e\left(\widetilde{d} + \left(d - \widetilde{d}\right)\right) = 1 + k(p-1)(q-1).$$

Construct a four variable integer equation

$$f(x_1, x_2, x_3, x_4) = 1 - e\widetilde{d} + eMx_1 + x_2(x_3 - 1)(x_4 - 1) + 1$$

where $M = 1$ for known MSBs, and $M = 2^{\lfloor(\beta-\delta)\log N\rfloor}$ for known LSBs. And the roots $(\widetilde{x}_1, \widetilde{x}_2, \widetilde{x}_3, \widetilde{x}_4) = (-d_0, k, p, q)$ are bound by $X_1 = N^{\delta}, X_2 = 2N^{\alpha+\beta-2/(r+1)}, X_3 = X_4 = 2N^{1/(r+1)}$. Thus, the problem of recovering d is converted to solving integer equation. Then, we can use Jochemsz-May Strategy to find the roots.

In 2014, Huang et al. [17] studied partial key exposure attacks on Takagi RSA. They used the lattice basis structure similar to [18] and gave the attacks with known MSBs, known LSBs and known some bits in the middle of the private exponent known. Their results show that one can factor N in polynomial time giving about $(1 - \frac{\delta}{\beta})$-fraction of MSBs or continuous bits in middle of d when

$$\delta \leq \frac{7}{4(r+1)} - \frac{1}{4}\sqrt{\frac{24(\alpha+\beta)}{r+1} - \frac{39}{(r+1)^2}} - \epsilon.$$

For known LSBs, they proved that one can factor N in polynomial time giving about $(1 - \frac{\delta}{\beta})$-fraction of LSBs of d when

$$\delta \leq \frac{5}{3(r+1)} - \frac{2}{3}\sqrt{\frac{3(\alpha+\beta)}{r+1} - \frac{5}{(r+1)^2}} - \epsilon.$$

Later, Takayasu and Kuniriho [32] used integer equation and modular equation respectively to improve the results in [17] for known MSBs and LSBs.

 ISBN: 978-1-61208-919-5

B. Attack on Prime Power RSA

For prime power RSA, the method to recover d is analogous to Takagi RSA. In addition, because p^{r-1} is in prime power RSA equation, we get a polynomial modulo p^{r-1}. Suppose we know some bits of d regardless of the MSBs or LSBs. Write known bits as $\widetilde{d}$ such that $\left|d-\widetilde{d}\right| < N^{\delta}$, and the equation of prime power RSA can be rewritten as

$$f(x) = eMx + e\widetilde{d} - 1 \pmod{p^{r-1}}$$

where $M = 1$ for known MSBs, and $M = 2^{\lfloor(\beta-\delta)\log N\rfloor}$ for known LSBs. The root x_0 is bound by $X = N^{\delta}$. Thus, the problem of recovering d is converted to solving univariate modular equation. We use Coppersmith method to find the root.

May [25] studied partial private key exposure attack on prime power RSA. They extended two small decryption exponent attacks on prime power RSA to partial private key exposure attack, and proved that one can factor N in polynomial time giving about $\min\{1-\frac{r}{(r+1)^2}, \frac{4r}{(r+1)^2}\}$-fraction of MSBs or LSBs. Later, Esgin et al. [12] extended the small decryption exponent attack on prime power RSA in [27] to partial private key exposure attack. Sarkar [28] gave the partial private key exposure attack when $r < 8$ and $d < N^{\frac{1}{r+1}+\frac{3r-2\sqrt{3r+3}+3}{3(r+1)}}$.

V. Factoring RSA Moduli with partial Known

In this section, we will describe attacks on RSA when partial bits of moduli N are known by side channel analysis or other ways. As early as 1985, Rivest and Shamir [26] have analyzed this problem. They used the method of integer programming to factor $N = pq$ in the case of two thirds of the consecutive bits of p known. Then, Coppersmith [6] factored N based on the lattice analysis method when half of the consecutive bits of p are known. Herrmann and May [13] first considered the situation that known bits are inconsecutive, and extended the problem to factor N with n blocks bits known. They proved that one could factor N when know 70% of random bits of p.

For the RSA scheme with modulus $N = p^r q$, Boneh, Durfee and Howgrave-Graham [5] showed that one can factor N when know $\frac{1}{r+1}$-fraction of the MSBs bits of p. Their basic idea is to guess the high bits of p, and calculate the entire p. Let the high bits of p as known P and the low bits as a variable x. Then, we get a univariate modular equation

$$f(x) = (P+x)^r \bmod p^r.$$

The small root can be found by Coppersmith method. Lu et al. [23] extend the problem to the case of n unknown bit blocks rather than a consecutive block. Their results show that the modulus N can be factored when $\frac{\ln(r+1)}{r}$-fraction of random bits of p are known.

Subsequently, Coron et al. [8] extended the attack of [5] to RSA with modulus $N = p^r q^s$. They used

$$\begin{cases} r = u\cdot\alpha + a \\ s = u\cdot\beta + b \end{cases}$$

And skillfully converted $N = p^r q^s$ into $N = P^u Q$, where $P := p^{\alpha}q^{\beta}, Q := p^a q^b$. Next, N can be factored based on [5]. Their results show that when r or s is greater than $(\log p)^3$, N can be factored in polynomial time.

Lu et al. [22] also discussed the security of RSA with modulus $N = p^r q^s$. They studied the case of known LSBs of p, and proposed two attacks, modulo p and modulo pq. They showed that when know $\min\{\frac{s}{r+s}, \frac{2(r-s)}{r+s}\}$ of the bits of p, one can factor N in polynomial time. When $2r > 3s$, the attack modulo p is better than modulo pq.

Later, Coron and Zeitoun [9] took advantage of Bézout identity and got a new relationship

$$\alpha\cdot s - \beta\cdot r = 1.$$

They converted $N = p^r q^s$ to $N = P^r q$, where $P := p^{\alpha}q^{\beta}$. Then, the results of [5] was used to factor N, which improved the result of [8]. That is, when $r \geq \log p$, N can be factored in polynomial time.

VI. Conclusion

Coppersmith method is a very important tool in RSA cryptanalysis. We survey the application of Coppersmith method in RSA with modulus $N = p^r q$ from three aspects, including small exponent attack, partial key exposure attack and factoring RSA moduli with partial known. These three types of attacks usually rely on special parameter selection. Therefore, the selection of parameters needs to be more careful to avoid the above attacks.

For the three attacks discussed in this paper, adding more helpful polynomials and eliminate unhelpful polynomials to construct lattice basis are the key to improve the attacks, which means to factor N with less information known. In addition, there are other attacks on RSA with moduli $N = p^r q$, which are mentioned in [34] and [35].

The crux of Coppersmith method is how to transform the problem of solving modular equation or integer equation into a short vector problem on lattices. In other words, the construction of the lattice basis is the most critical step. For now, Jochemsz-May strategy is the best general strategy for solving multivariate integer equation. A triangular matrix can be constructed easily by Jochemsz-May strategy. However, for some special algebraic structures, Jochemsz-May strategy does not always get the best results. We need to exploit the implicit algebraic relationships to construct a better lattice basis. The work of [32] shows that modular equations combined with unraveled technique usually obtain better results than integer equation based on Jochemsz-May Strategy. The construction of a better lattice basis and optimization of the results still have room for improvement.

References

[1] Y. Aono, "A new lattice construction for partial key exposure attack for RSA," In Public Key Cryptography - PKC 2009, volume 5443 of Lecture Notes in Computer Science, pp. 34–53, Springer, 2009.

[2] J. Blömer and A. May, "New partial key exposure attacks on RSA," In Advances in Cryptology - CRYPTO 2003, 23rd Annual International Cryptology Conference, volume 2729 of Lecture Notes in Computer Science, pp. 27–43, Springer, 2003.

[3] D. Boneh and G. Durfee, "Cryptanalysis of RSA with private key d less than $N^{0.292}$," In Advances in Cryptology - EUROCRYPT 1999, volume 1592 of Lecture Notes in Computer Science, pp. 1–11, Springer, 1999.

[4] D. Boneh, G. Durfee, and Y. Frankel, "An attack on RSA given a small fraction of the private key bits," In Advances in Cryptology - ASIACRYPT 1998, volume 1514 of Lecture Notes in Computer Science, pp. 25–34, Springer, 1998.

[5] D. Boneh, G. Durfee, and N. Howgrave-Graham, "Factoring $N = p^r q$ for large r," In Advances in Cryptology - CRYPTO 1999, volume 1666 of Lecture Notes in Computer Science, pp. 326–337, Springer, 1999.

[6] D. Coppersmith, "Finding a small root of a bivariate integer equation; factoring with high bits known," In Advances in Cryptology - EUROCRYPT 1996, volume 1070 of Lecture Notes in Computer Science, pp. 178–189, Springer, 1996.

[7] D. Coppersmith, "Finding a small root of a univariate modular equation," In Advances in Cryptology - EUROCRYPT 1996, volume 1070 of Lecture Notes in Computer Science, pp. 155–165, Springer, 1996.

[8] J. Coron, J. Faugère, G. Renault, and R. Zeitoun, "Factoring $n = p^r q^s$ for large r and s," In Topics in Cryptology - CT-RSA 2016, volume 9610 of Lecture Notes in Computer Science, pp. 448–464, Springer, 2016.

[9] J. Coron and R. Zeitoun, "Improved factorization of $n = p^r q^s$," In Topics in Cryptology - CT-RSA 2018, volume 10808 of Lecture Notes in Computer Science, pp. 65–79, Springer, 2018.

[10] G. Durfee and P. Q. Nguyen, "Cryptanalysis of the RSA schemes with short secret exponent from asiacrypt'99," In Advances in Cryptology - ASIACRYPT 2000, volume 1976 of Lecture Notes in Computer Science, pp. 14–29, Springer, 2000.

[11] M. Ernst, E. Jochemsz, A. May, and B. de Weger, "Partial key exposure attacks on RSA up to full size exponents," In Advances in Cryptology - EUROCRYPT 2005, volume 3494 of Lecture Notes in Computer Science, pp. 371–386, Springer, 2005.

[12] M. F. Esgin, M. S. Kiraz, and O. Uzunkol, "A new partial key exposure attack on multi-power RSA," In Algebraic Informatics - CAI 2015, volume 9270 of Lecture Notes in Computer Science, pp. 103–114, Springer, 2015.

[13] M. Herrmann and A. May, "Solving linear equations modulo divisors: On factoring given any bits," In Advances in Cryptology - ASIACRYPT 2008, volume 5350 of Lecture Notes in Computer Science, pp. 406– 424, Springer, 2008.

[14] M. Herrmann and A. May, "Attacking power generators using unravelled linearization: When do we output too much?" In Advances in Cryptology - ASIACRYPT 2009, volume 5912 of Lecture Notes in Computer Science, pp. 487–504, Springer, 2009.

[15] M. Herrmann and A. May, "Maximizing small root bounds by linearization and applications to small secret exponent RSA," In Public Key Cryptography - PKC 2010, volume 6056 of Lecture Notes in Computer Science, pp. 53–69, Springer, 2010.

[16] N. Howgrave-Graham, "Finding small roots of univariate modular equations revisited," In Cryptography and Coding 1997, volume 1355 of Lecture Notes in Computer Science, pp. 131–142, Springer, 1997.

[17] Z. Huang, L. Hu, J. Xu, L. Peng, and Y. Xie, "Partial key exposure attacks on takagi's variant of RSA," In Applied Cryptography and Network Security - ACNS 2014, volume 8479 of Lecture Notes in Computer Science, pp. 134–150, Springer, 2014.

[18] K. Itoh, N. Kunihiro, and K. Kurosawa, "Small secret key attack on a variant of RSA (due to takagi)," In Topics in Cryptology - CT-RSA 2008, volume 4964 of Lecture Notes in Computer Science, pp. 387–406, Springer, 2008.

[19] E. Jochemsz and A. May, "A strategy for finding roots of multivariate polynomials with new applications in attacking RSA variants," In Advances in Cryptology - ASIACRYPT 2006, volume 4284 of Lecture Notes in Computer Science, pp. 267–282, Springer, 2006.

[20] A. K. Lenstra, H. W. Lenstra, and L. Lovász, "Factoring polynomials with rational coefficients," Mathematische Annalen, vol. 261(4), pp.515–534, 1982.

[21] S. Lim, S. Kim, I. Yie, and H. Lee, "A generalized takagi-cryptosystem with a modulus of the form $p^r q^s$," In Progress in Cryptology - INDOCRYPT 2000, volume 1977 of Lecture Notes in Computer Science, pp. 283–294, Springer, 2000.

[22] Y. Lu, L. Peng, and S. Sarkar, "Cryptanalysis of an RSA variant with moduli $n = p^r q^l$," J. Math. Cryptol., vol. 11(2), pp. 117-130, 2017.

[23] Y. Lu, R. Zhang, and D, "Lin. Factoring multi-power RSA modulus $N = p^r q$ with partial known bits," In Information Security and Privacy - ACISP 2013, volume 7959 of Lecture Notes in Computer Science, pp. 57–71, Springer, 2013.

[24] Y. Lu, R. Zhang, L. Peng, and D. Lin, "Solving linear equations modulo unknown divisors: Revisited," In Advances in Cryptology - ASIACRYPT 2015, volume 9452 of Lecture Notes in Computer Science, pp. 189– 213, Springer, 2015.

[25] A. May, "Secret exponent attacks on rsa-type schemes with moduli $n = p^r q$," In Public Key Cryptography - PKC 2004, volume 2947 of Lecture Notes in Computer Science, pp. 218–230, Springer, 2004.

[26] R. L. Rivest and A. Shamir, "Efficient factoring based on partial information," In Advances in Cryptology - EUROCRYPT 1985, volume 219 of Lecture Notes in Computer Science, pp. 31–34, Springer, 1985.

[27] S. Sarkar, "Small secret exponent attack on RSA variant with modulus $n = p^r q$," Des. Codes Cryptogr., vol. 73(2), pp. 383–392, 2014.

[28] S. Sarkar, "Revisiting prime power RSA," Discret. Appl. Math., vol. 203, pp. 127– 133, 2016.

[29] K. Suzuki, A. Takayasu, and N. Kunihiro, "Extended partial key exposure attacks on RSA: improvement up to full size decryption exponents," Theor. Comput. Sci., vol. 841, pp. 62–83, 2020.

[30] T. Takagi, "Fast rsa-type cryptosystem modulo $p^k q$," In Advances in Cryptology - CRYPTO 1998, volume 1462 of Lecture Notes in Computer Science, pp. 318–326. Springer, 1998.

[31] A. Takayasu and N. Kunihiro, "Partial key exposure attacks on RSA: achieving the Boneh-Durfee bound," In Selected Areas in Cryptography - SAC 2014, volume 8781 of Lecture Notes in Computer Science, pp. 345–362. Springer, 2014.

[32] A. Takayasu and N. Kunihiro, "How to generalize RSA cryptanalyses," In Public-Key Cryptography - PKC 2016, volume 9615 of Lecture Notes in Computer Science, pp. 67–97. Springer, 2016.

[33] M. J. Wiener, "Cryptanalysis of short RSA secret exponents," IEEE Trans. Inf. Theory, vol. 36(3), pp. 553–558, 1990.

[34] L. Peng, L. Hu, Y. Lu, S. Sarkar, J. Xu, Z. Huang, " Cryptanalysis of Variants of RSA with Multiple Small Secret Exponents," In: Biryukov A., Goyal V. (eds) Progress in Cryptology - INDOCRYPT 2015, volume 9462 of Lecture Notes in Computer Science, pp. 105-123, Springer, 2015.

[35] A. Nitaj and T. Rachidi, "New Attacks on RSA with Moduli $N = p^r q$," In: El Hajji S., Nitaj A., Carlet C., Souidi E. (eds) Codes, Cryptology, and Information Security. C2SI 2015. volume 9084 of Lecture Notes in Computer Science, pp. 352-360 Springer, 2015.

 ISBN: 978-1-61208-919-5