Partial Key Exposure Attacks on RSA with Multiple Exponent Pairs

Atsushi Takayasu(✉) and Noboru Kunihiro

The University of Tokyo, Tokyo, Japan
a-takayasu@it.k.u-tokyo.ac.jp, kunihiro@k.u-tokyo.ac.jp

Abstract. So far, several papers have analyzed attacks on RSA when attackers know the least significant bits of a secret exponent d as well as a public modulus N and a public exponent e, the so-called partial key exposure attacks. Aono (ACISP 2013), and Takayasu and Kunihiro (ACISP 2014) generalized the attacks when there are multiple pairs of a public/secret exponent $(e_1, d_1), \ldots, (e_n, d_n)$ for the same public modulus N. The standard RSA is a special case of the generalization, i.e., $n = 1$. They revealed that RSA becomes more vulnerable when there are more exponent pairs. However, their results have *two obvious drawbacks*. First, partial key exposure situations which they considered are restrictive. They have proposed the attacks only for small secret exponents, although attacks for large secret exponents have also been analyzed for the standard RSA. Second, they could not generalize the attacks perfectly. More concretely, their attacks for $n = 1$ do not correspond to the currently known best attacks on the standard RSA.

In this paper, we propose improved partial key exposure attacks on RSA with multiple exponent pairs. Our results completely solve the above drawbacks. Our attacks are the first results for large exponents, and our attacks for $n = 1$ correspond to the currently known best attacks on the standard RSA. Our results for small secret exponents are superior to previous results when $n = 1$ and 2, and when $n \geq 3$ and $d_1, \ldots, d_n > N^{3(n-1)/(3n+1)}$.

1 Introduction

1.1 Background

Partial Key Exposure Attacks on RSA. RSA is one of the most widely used cryptosystems. For a public modulus $N = pq$ where p and q are distinct primes with the same bit size, there are an encryption/verifying exponent e and a decryption/signing exponent d that satisfy $ed = 1 \mod \phi(N)$ where $\phi(N) = (p-1)(q-1)$. To encrypt a plaintext m (resp. verify a signature σ), $m^e \mod N$ (resp. $\sigma^e \mod N$) should be computed. Similarly, to decrypt a ciphertext c (resp. sign a message m), $c^d \mod N$ (resp. $m^d \mod N$) should be computed. To reduce the complexity of the heavy modular exponentiation, we can use a small public exponent $e \approx N^\alpha$ or a small decryption exponent $d \approx N^\beta$. However, Wiener [28] showed that too small d makes RSA insecure. Their attack factors

J.K. Liu and R. Steinfeld (Eds.): ACISP 2016, Part II, LNCS 9723, pp. 243–257, 2016.
DOI: 10.1007/978-3-319-40367-0_15

public modulus N in polynomial time when $\alpha = 1$ and $\beta < 1/4$. Later, Boneh and Durfee [4] further improved the bound to $\beta < 1 - 1/\sqrt{2} = 0.292\cdots$.

Boneh, Durfee, and Frankel [5] analyzed the security of RSA when attackers know some portions of d, that is, the so-called *partial key exposure attacks*. In this paper, we focus on the situation when attackers know $\tilde{d} > N^{\beta-\delta}$ which is the least significant bits of d. In this situation, the attack of Boneh et al. works only for extremely small $e = \text{poly}(\log N)$.

Thus far, several generalizations and improvements of partial key exposure attacks have been proposed. In this paper, we focus on three situations[1];

(a) $\alpha \leq 1$ and $\beta = 1$,
(b) $\alpha \leq 1$ and $\beta > 1$,
(c) $\alpha = 1$ and $\beta \leq 1$.

Blömer and May [3] analyzed the situation (a), and their attack works when $\alpha < 7/8 = 0.875$. Joye and Lepoint [15] analyzed the situation (b), and their attack works when $\beta < 15/8$ for extremely small α. Ernst et al. [11] analyzed the situation (c), and their attack works when $\beta < 7/8$. In the last situation, Aono [1] proposed an improved attack. When $1 - 1/\sqrt{2} < \beta < (9 - \sqrt{21})/12 = 0.368\cdots$, Aono's attack works with less partial information than that of Ernst et al. Later, in the same range of β, Takayasu and Kunihiro [27] further improved the attack.

RSA with Multiple Exponent Pairs. As opposed to the standard RSA setting, the security of RSA with multiple exponent pairs has also been studied in several papers [2,14,21,23,24,26]. In this setting, there are multiple public/secret exponent pairs $(e_1, d_1), \ldots, (e_n, d_n)$ for the same public modulus N such that $e_j d_j = 1 \mod \phi(N)$ for all $j = 1, 2, \ldots, n$. In this context, the standard RSA can be regarded as the special case, i.e., $n = 1$. We denote sizes of public exponents as $e_1, \ldots, e_n \approx N^{\alpha}$ and sizes of secret exponents as $d_1, \ldots, d_n \approx N^{\beta}$. These works showed that RSA becomes more vulnerable when there are more exponent pairs. Takayasu and Kunihiro [26] proposed a generalization of Boneh and Durfee's attack [4] that works when $\beta < 1 - \sqrt{2/(3n+1)}$ only with public information N and $e_1, \ldots, e_n$. When there are more exponent pairs, i.e., larger n, larger secret exponents can be recovered. Especially, full size secret exponents, i.e., $\beta = 1$, can be recovered with infinitely many exponent pairs.

Partial key exposure attacks on RSA with multiple exponent pairs have also been analyzed. For the attacks, attackers know $\tilde{d}_1, \ldots, \tilde{d}_n > N^{\beta-\delta}$ which are the least significant bits of $d_1, \ldots, d_n$. Aono [2] analyzed a partial key exposure attack[2] in the situation (c). Although the attack on the standard

[1] At a glance, a situation (b) seems useless, since d is defined as $d \in \mathbb{Z}^*_{\phi(N)}$ in many cases, and $\beta \leq 1$ always holds. However, some implementations use an exponent which is larger than N. To decrypt/sign, one may use $d + k\phi(N)$ in turn for some integer $k > 0$. This implementation offers better resistance against side-channel attacks [9] or faster calculation by setting the exponent as low Hamming weight.

[2] In [2,26], they use δ, not $\beta-\delta$ as ours, to represent portions of exposed bits. However, we follow the notation from [11,27].

RSA [2,11,26], i.e., $n = 1$, cannot be applied to full size secret exponent[3] , i.e., $\beta = 1$, Aono's attack can be applied to the case when $n \geq 3$. Takayasu and Kunihiro [26] further improved the attack when $n \geq 3$ and $\beta < 3(n-1)/(3n+1)$. These results are theoretically interesting to ensure the security of RSA.

In this paper, we focus on partial key exposure attacks on RSA with multiple exponent pairs since previous results [2,26] have *two obvious drawbacks*. First, the results focus only on the situation (c). Therefore, there have been no results which analyzed the situations (a) and (b) with multiple exponent pairs. Second, the previous attacks [2,26] cannot be the best even in the situation (c), since the attacks for $n = 1$ do not correspond to the currently known best attacks with a single exponent pair [11,27]. As a result, although the generalization of Boneh and Durfee's small secret exponent attack suggests that partial key exposure attacks should always work when $\beta < 1 - \sqrt{2/(3n+1)}$ in the situation (c) even with no partial information, when $n = 1$ and 2, previous attacks [2,26] does not work in the range with small amounts of partial information.

1.2 Our Contributions

In this paper, we propose improved partial key exposure attacks on RSA with multiple exponent pairs and completely solve the above drawbacks of previous works [2,26]. Unlike previous works, we analyze not only the situation (c), but also the situations (a) and (b). Therefore, we offer the first result for the attack with multiple exponent pairs in (a) and (b). Moreover, our attack in the situation (c) is superior to previous attacks [2,26] when $n = 1$ and 2, and when $n \geq 3$ and $\beta > 3(n-1)/(3n+1)$. Our attack always works when $\beta < 1 - \sqrt{2/(3n+1)}$ for $n = 1$ and 2. When $\beta = 1$, although previous attacks work when $n \geq 3$, our attack works when $n \geq 2$. For all the situations (a), (b), and (c), our proposed attacks for $n = 1$ correspond to the currently known best attacks with a single exponent pair.

1.3 Technical Overview

Almost all the above attacks [2,3,26,27] used the Coppersmith method to solve modular equations that have small solutions [6,13]. In the method, we construct a lattice whose basis vectors are coefficients of polynomials that have the same solutions as the original modular equations. To improve partial key exposure attacks, we should construct algorithms which can find larger solutions. For the improvement, we should select appropriate lattice bases for the resulting lattice to have shorter vectors. We call polynomials which shorten lattice vectors *helpful polynomials*. The exact criteria that decide if polynomials are helpful or not have already been analyzed in [18,25]. To maximize solvable bounds of

[3] From May [17] and Coron and May's [10] results, given whole bits of d then the factorization of N is a trivial. However, it does not immediately suggest that partial key exposure attacks always work when whole bits of d are given. Indeed, Ernst et al. [11] claimed to find such improved attacks is an interesting open problem.

solutions, we should select as many helpful polynomials as possible and as few unhelpful polynomials as possible in lattice bases. For example, first, Boneh and Durfee [4] constructed lattices to obtain Wiener's bound $\beta < 1/4$ [28]. Afterward, they added extra polynomials, which are helpful, in lattice basis and improved the bound to $\beta < 1 - 1/\sqrt{2}$.

As noted in [26], Aono's lattice can be viewed as a generalization of the lattice to obtain Wiener's bound for the small secret exponent attack. The selection of lattice bases is too simple, since it does not depend on any values of n, β and δ. Therefore, the lattice can be applied to attacks in situations (a) and (b), although Aono did not analyze them. However, that means the lattice cannot provide the best bounds when the values of n, α, β, and δ change. In [26], Takayasu and Kunihiro work out new lattice constructions that depend on the values of n, α, β, and δ. They revealed that Aono's lattice contains unhelpful polynomials when n is large and β is small, and they constructed lattices by eliminating as many unhelpful polynomials as possible. The lattice provides an improved results when $n \geq 3$ and $\beta < 3(n-1)/(3n+1)$.

Conversely, the above observation suggests that Aono's lattice does not contain all helpful polynomials when $n = 1$ and 2, and $n \geq 3$ and $\beta > 3(n-1)/(3n+1)$. Therefore, all we have to do is to add as many helpful polynomials as possible. However, Takayasu and Kunihiro [26] could not do the task since adding helpful polynomials is rather difficult compared with eliminating unhelpful polynomials. We work out the analyses required to understand the essence of the lattice constructions for the standard RSA [3,11,15,27]. Although we analyze the three situations, i.e., (a), (b), and (c), there are only two types of lattices in these previous works. We call them the Blömer-May lattice and the Takayasu-Kunihiro lattice. Ernst et al.'s result [11], and Joye and Lepoint's result [15] can be obtained via the Blömer-May lattice. The classification offers better understanding for the lattice constructions and we generalize the two types of lattices in subsequent sections. As a result, this paper completes the analysis of partial key exposure attacks on RSA with multiple exponent pairs.

1.4 Organization

In Sect. 2, we define a scenario of partial key exposure attacks and formulate them as simultaneous modular equations. Afterward, we briefly summarize previous results [2,3,11,26,27]. In Sect. 3, we introduce the Coppersmith method to solve modular equations [6,13]. In Sect. 4, we propose generalized lattice constructions of the Blömer-May. In Sect. 5, we propose generalized lattice constructions of the Takayasu-Kunihiro.

2 Definitions of the Attack and Previous Results

For multiple exponent pairs setting, RSA key generations can be written as $e_j d_j = 1 + \ell_j (N - (p+q) + 1)$ for $j = 1, 2, \ldots, n$ with some integers $\ell_j \approx N^{\alpha+\beta-1}$. We assume that all public exponents $e_1, \ldots, e_n$ are pairwise co-prime as previous works [2,26]. Let $\tilde{d}_j \approx N^{\beta-\delta}$ (resp. $d'_j \approx N^{\delta}$) denote the least (resp. the most) significant bits of d_j. We can rewrite $d_j = d'_j M + \tilde{d}_j$ with some integers $M \approx N^{\beta-\delta}$. We consider partial key exposure attacks when attackers know $\tilde{d}_1, \ldots, \tilde{d}_n$. Rewrite RSA key generations

$$e_j\left(d'_j M + \tilde{d}_j\right) = 1 + \ell_j(N - (p+q) + 1),$$

and consider the following modular polynomials

$$\begin{aligned} f_j(x_j, y) &= 1 - e_j\tilde{d}_j + x_j(N + y) \pmod{e_j M} \text{ and} \\ g_j(x_j, y) &= 1 + x_j(N + y) \pmod{e_j} \end{aligned}$$

for $j = 1, 2, \ldots, n$. The polynomials have the roots

$$(x_1, \ldots, x_n, y) = (\ell_1, \ldots, \ell_n, -(p+q) + 1).$$

The absolute values of the roots are bounded above by $X_j := N^{\alpha+\beta-1}$ for $j = 1, 2, \ldots, n$ and $Y := 3N^{1/2}$. If we can find the roots, we can easily factor RSA modulus N.

In the rest of this section, we summarize previous attacks. First, we show the previous results for the standard RSA. All conditions when Blömer and May's attack [3], Ernst et al.'s attack [11], and Joye and Lepoint's attack [15] work can be written as

$$\delta < \frac{5}{6} - \frac{\sqrt{-5 + 6(\alpha+\beta)}}{3}. \tag{1}$$

All the attacks are based on the Blömer-May lattice and the lattices are constructed to solve a modular equation $f_1(x_1, y) = 0$. Takayasu and Kunihiro's attack [27] works when

$$\delta < \frac{1 + \beta - \sqrt{2 - 3(1-\beta)^2}}{2} \text{ and } \beta < \frac{9 - \sqrt{21}}{12}. \tag{2}$$

The Takayasu-Kunihiro lattices are constructed to solve simultaneous modular equations $f_1(x_1, y) = 0$ and $g_1(x_1, y) = 0$.

Next, we show the previous results with multiple exponent pairs. The following attacks work in time polynomial in $\log N$ and exponential in n. Although Aono [2] only considered the situation (c), their lattice can also be applied to the situations (a) and (b). The attack works when

$$\delta < \frac{3}{2} - \frac{4}{3n+1}\alpha - \beta. \tag{3}$$

Aono's lattice is constructed to solve simultaneous modular equations $f_1(x_1, y) = 0, \ldots, f_n(x_n, y) = 0$. In the situation (c) for $n \geq 3$, Takayasu and Kunihiro [26] solved the same modular equations as Aono and improved the bound to

$$\delta < -\frac{1}{2} + \beta + \frac{(3n+1)(1-\beta)^2}{4} \text{ and } \beta < \frac{3(n-1)}{3n+1}. \tag{4}$$

3 Preliminaries

Consider the modular equations $h(x_1, \ldots, x_n) = 0 \pmod{W}$. All absolute values of the solutions $(\tilde{x}_1, \ldots, \tilde{x}_n)$ are bounded above by $X_1, \ldots, X_n$. When $\prod_{j=1}^{n} X_j$ is reasonably smaller than W, the Coppersmith method can find all the solutions in polynomial time. We write the norm of a polynomial as $\|h(x_1, \ldots, x_n)\|$, which represents the Euclidean norm of the coefficient vector. The following Howgrave-Graham's Lemma reduces the modular equations into integer equations.

Lemma 1 (Howgrave-Graham's Lemma [13]**).** *Let* $\tilde{h}(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ *be a polynomial with at most* w *monomials. Let* $m, W, X_1, \ldots, X_n$ *be positive integers. Suppose that:*

1. $\tilde{h}(\tilde{x}_1, \ldots, \tilde{x}_n) = 0 \pmod{W^m}$*, where* $|\tilde{x}_1| < X_1, \ldots, |\tilde{x}_n| < X_n$*,*
2. $\|\tilde{h}(x_1X_1, \ldots, x_nX_n)\| < W^m/\sqrt{w}$*.*

Then $\tilde{h}(\tilde{x}_1, \ldots, \tilde{x}_n) = 0$ *holds over the integers.*

To solve n-variate modular equations $h(x_1, \ldots, x_n) = 0 \pmod{W}$, it suffices to find n new polynomials $\tilde{h}_1(x_1, \ldots, x_n), \ldots, \tilde{h}_n(x_1, \ldots, x_n)$ whose roots are the same as the original solutions $(\tilde{x}_1, \ldots, \tilde{x}_n)$ and whose norms are small enough to satisfy Howgrave-Graham's Lemma.

To find such polynomials from the original polynomial $h(x_1, \ldots, x_n)$, lattices and the LLL algorithm are often used. Lattices represent the integer linear combinations of the basis vectors. All vectors are row representation. For the basis vectors $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_w$, which are all k dimensional linearly independent vectors in $\mathbb{Z}^k$, the lattice spanned by these vectors is defined as $L(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_w) := \{\sum_{j=1}^{w} c_j\boldsymbol{b}_j : c_j \in \mathbb{Z} \text{ for all } j = 1, 2, \ldots, w\}$. We also use the matrix representation for the basis. We define the basis matrix $\boldsymbol{B}$ as $w \times k$ matrix which has the basis vectors $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_w$ in each row. In the same way, the lattice can be rewritten as $L(\boldsymbol{B})$. We call the lattice full-rank when $w = k$. The volume of the lattice $\mathrm{vol}(L(\boldsymbol{B}))$ is defined as the w-dimensional volume of the parallelepiped $\mathcal{P}(\boldsymbol{B}) := \{\mathbf{c}B : \mathbf{c} \in \mathbb{R}^w, 0 \leq c_j < 1, \text{for all } j = 1, 2, \ldots, w\}$. The volume can be computed as $\mathrm{vol}(L(\boldsymbol{B})) = \sqrt{\det(\boldsymbol{B}\boldsymbol{B}^T)}$ in general, and the volume of a full-rank lattice can be computed as $\mathrm{vol}(L(\boldsymbol{B})) = |\det(\boldsymbol{B})|$.

Lattice has been used in many places in cryptographic research. See [7,8,19,20] for detailed information. In cryptanalysis, to find non-zero short lattice vectors is essential. In this paper, we introduce the LLL algorithm [16] which outputs short lattice vectors in polynomial time.

Proposition 1 (LLL algorithm [16]**).** *Given basis vectors* $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_w$ *in* $\mathbb{Z}^k$*, the LLL algorithm finds LLL-reduced bases* $\tilde{\boldsymbol{b}}_1, \ldots, \tilde{\boldsymbol{b}}_w$ *that satisfy*

$$\|\tilde{\boldsymbol{b}}_j\| \leq 2^{w(w-1)/4(w-j+1)}(\mathrm{vol}(L(\boldsymbol{B})))^{1/(w-j+1)} \quad \text{for } 1 \leq j \leq w,$$

in time polynomial in w, k*, and the maximum input length.*

Again, we consider how to solve the modular equation $h(x_1,\dots,x_n) = 0 \pmod{W}$. First, we construct w polynomials $h_1(x_1,\dots,x_n),\dots,h_w(x_1,\dots,x_n)$ that have the roots $(\tilde{x}_1,\dots,\tilde{x}_n)$ modulo W^m with some positive integer m. We construct w basis vectors $\boldsymbol{b}_1,\dots,\boldsymbol{b}_w$ each whose elements are coefficients of $h_j(x_1X_1,\dots,x_nX_n)$ for $j = 1,2,\dots,w$, and construct a basis matrix $\boldsymbol{B}$. We span a lattice $L(\boldsymbol{B})$. Since all lattice vectors are integer linear combinations of the basis vectors, all polynomials whose coefficients are derived from lattice vectors have the roots $(\tilde{x}_1,\dots,\tilde{x}_n)$ modulo W^m. We apply the LLL algorithm to the lattice bases, and obtain n LLL-reduced vectors $\tilde{\boldsymbol{b}}_1,\dots,\tilde{\boldsymbol{b}}_n$. The new polynomials $\tilde{h}_1(x_1,\dots,x_n),\dots,\tilde{h}_n(x_1,\dots,x_n)$ which are derived from the above n LLL-reduced vectors satisfy Howgrave-Graham's Lemma provided that $(\mathrm{vol}(L(\boldsymbol{B})))^{1/w} < W^m$. Here, we omit small terms. When we obtain the polynomials $\tilde{h}_1(x_1,\dots,x_n),\dots,\tilde{h}_n(x_1,\dots,x_n)$, it is easy to solve the modular equation $h(x_1,\dots,x_n) = 0 \pmod{W}$. What we should do is to find the roots of the polynomials over the integers by computing resultant or Gröbner bases. We should note that the method needs heuristic argument if we consider multivariate problems, since the polynomials $\tilde{h}_1(x_1,\dots,x_n),\dots,\tilde{h}_n(x_1,\dots,x_n)$ have no assurance of algebraic independency. In this paper, we assume that the polynomials derived from outputs of the LLL algorithm are algebraic independent as previous works [2–4,15,26,27]. Indeed, there are few papers that contradict the assumption.

Although we introduce a lattice construction to solve a single multivariate modular equation, the method can be easily applied to simultaneous modular equations in the same way. To attack RSA with multiple exponent pairs, we use *Minkowski sum based lattices* introduced by Aono [2]. To solve n simultaneous modular equations, the technique combine n lattices each of which is a lattice to solve a single equation.

4 Generalizations of the Blömer-May Lattice

4.1 Our Algorithm

In this section, we solve simultaneous modular equations

$$f_j(x_j,y) = 1 - e_j\tilde{d}_j + x_j(N+y) \pmod{e_jM}$$

for $j = 1,2,\dots,n$ by generalizing the Blömer-May lattice [3], and obtain the following result.

Theorem 1. *Let $N = pq$ be an RSA modulus. Let (e_j,d_j) be pubic/secret exponents where $e_j \approx N^\alpha, d_j \approx N^\beta$, and $e_jd_j = 1 \pmod{(p-1)(q-1)}$ for $j = 1,2,\dots,n$. Given public elements $N, e_1,\dots,e_n$, and $\tilde{d}_1,\dots,\tilde{d}_n > N^{\beta-\delta}$ that are the least significant bits of $d_1,\dots,d_n$, respectively. Assume $e_1,\dots,e_n$ are pairwise co-prime and the LLL algorithm outputs algebraically independent polynomials. If*

$$\delta < \frac{9n+1-\sqrt{(3n+1)^2+96n\alpha-24n(3n+1)(1-\beta)}}{12n},$$

then public modulus N can be factored in time polynomial in $\log N$ *and exponential in n.*

Proof. At first, we show the Blömer-May lattice to solve each single modular equation $f_j(x_j, y) = 0$ for $j = 1, 2, \ldots, n$ that yields the bound (1). To solve the single equation, we use shift-polynomials

$$x_j^{i_j} \cdot f_j(x_j, y)^{u_j} \cdot (e_j M)^{m-u_j} \text{ with } i_j = 0, 1, \ldots, m; u_j = 0, 1, \ldots, m - i_j,$$
$$y^{k_j} \cdot f_j(x_j, y)^{i_j} \cdot (e_j M)^{m-i_j} \text{ with } i_j = 0, 1, \ldots, m; k_j = 1, 2, \ldots, \lfloor \tau m \rfloor,$$

in lattice bases with some positive integer m. The parameter $\tau \geq 0$ should be optimized later. All these shift-polynomials modulo $(e_j M)^m$ have the same roots as the original solutions, e.g., $(x_j, y) = (\ell_j, -(p+q)+1)$ for $j = 1, 2, \ldots, n$. These polynomials generate a triangular basis matrix with diagonals

$$X_j^{i'_j} Y^{u'_j} (e_j M)^{m-\min\{i'_j, u'_j\}} \quad \text{with } i'_j = 0, 1, \ldots, m; u'_j = 0, 1, \ldots, i'_j,$$
$$X_j^{i'_j} Y^{i'_j + k'_j} (e_j M)^{m-i'_j} \qquad \text{with } i'_j = 0, 1, \ldots, m; k'_j = 1, 2, \ldots, \lfloor \tau m \rfloor.$$

We set the parameter $\tau = (1 - 2\delta)/2$, and the lattice yields the bound (1).

Next, we combine these n lattices based on Minkowski sum. Since we combine triangular basis matrices, the combined basis matrix also becomes triangular with diagonals

$$X_j^{i'_j} Y^{u'_j} (e_j M)^{m-\min\{i'_j, u'_j\}} \text{ with } i'_j = 0, 1, \ldots, m; u'_j = 0, 1, \ldots, i'_j,$$
$$X_1^{i'_1} \cdots X_n^{i'_n} Y^{\sum_{j=1}^n i'_j + k'} e_1^{m-i'_1} \cdots e_n^{m-i'_n} M^{nm - \sum_{j=1}^n i'_j}$$
$$\text{with } i'_j = 0, 1, \ldots, m \text{ for } j = 1, 2, \ldots, n; k' = 1, 2, \ldots, \lfloor \tau m \rfloor.$$

All polynomials which are derived from resulting lattice vectors modulo $(e_1 \cdots e_n)^m M^{nm}$ have the same roots as the original solutions.

We show that the above lattice offers the bound of Theorem 1. Ignoring low order terms of m, we can compute the dimension

$$w = \sum_{i'_1=0}^{m} \cdots \sum_{i'_n=0}^{m} \sum_{u'=0}^{\sum_{j=1}^n i'_j} 1 + \sum_{i'_1=0}^{m} \cdots \sum_{i'_n=0}^{m} \sum_{k'=1}^{\lfloor \tau m \rfloor} 1 = \left(\frac{n}{2} + \tau\right) m^{n+1},$$

and the volume of the lattice $\mathrm{vol}(L(\boldsymbol{B})) = X_1^{s_{X_1}} \cdots X_n^{s_{X_n}} Y^{s_Y} e_1^{s_{e_1}} \cdots e_n^{s_{e_n}} M^{s_M}$, where

$$s_{X_j} = \sum_{i'_1=0}^{m} \cdots \sum_{i'_n=0}^{m} \sum_{u'=0}^{\sum_{j=1}^n i'_j} i'_j + \sum_{i'_1=0}^{m} \cdots \sum_{i'_n=0}^{m} \sum_{k'=1}^{\lfloor \tau m \rfloor} i'_j = \left(\frac{3n+1}{12} + \frac{\tau}{2}\right) m^{n+2},$$

$$s_{e_j} = \sum_{i'_1=0}^{m} \cdots \sum_{i'_n=0}^{m} \sum_{u'=0}^{\sum_{j=1}^n i'_j} \left(m - \min\{i'_j, u'\}\right) + \sum_{i'_1=0}^{m} \cdots \sum_{i'_n=0}^{m} \sum_{k'=1}^{\lfloor \tau m \rfloor} \left(m - i'_j\right)$$
$$= \left(\frac{3n+1}{12} + \frac{\tau}{2}\right) m^{n+2}$$

for $j = 1, 2, \ldots, n$,

$$
\begin{aligned}
s_Y &= \sum_{i'_1=0}^{m} \cdots \sum_{i'_n=0}^{m} \sum_{u'=0}^{\sum_{j=1}^{n} i'_j} u' + \sum_{i'_1=0}^{m} \cdots \sum_{i'_n=0}^{m} \sum_{k'=1}^{\lfloor \tau m \rfloor} \left(\sum_{j=1}^{n} i'_j + k' \right) \\
&= \left(\frac{n(3n+1)}{24} + \frac{n\tau}{2} + \frac{\tau^2}{2} \right) m^{n+2}, \\
s_M &= \sum_{i'_1=0}^{m} \cdots \sum_{i'_n=0}^{m} \sum_{u'=0}^{\sum_{j=1}^{n} i'_j} (nm - u') + \sum_{i'_1=0}^{m} \cdots \sum_{i'_n=0}^{m} \sum_{k'=1}^{\lfloor \tau m \rfloor} \left(nm - \sum_{j=1}^{n} i'_j \right) \\
&= \left(\frac{n(9n-1)}{24} + \frac{n}{2}\tau \right) m^{n+2}.
\end{aligned}
$$

We can solve the simultaneous modular equations $f_j(x_j, y) = 0$ for $j = 1, 2, \ldots, n$, when $(\mathrm{vol}(L(\boldsymbol{B})))^{1/w} < (e_1 \cdots e_n)^m M^{nm}$, that is,

$$
-12\tau^2 + 24n(1-\delta)\tau + 3n(3n+1) - 8n\alpha - 2n(3n+1)(\beta+\delta) > 0.
$$

To maximize the left-hand side of the above inequality, we set the parameter $\tau = n(1-2\delta)/2$, and the condition becomes

$$
12n\delta^2 - 2(9n+1)\delta + 12n + 3 - 8\alpha - 2(3n+1)\beta > 0.
$$

The inequality results in the bound of Theorem 1,

$$
\delta < \frac{9n + 1 - \sqrt{(3n+1)^2 + 96n\alpha - 24n(3n+1)(1-\beta)}}{12n}
$$

as required. □

4.2 Observation

Compared with Aono's lattice, we select extra shift-polynomials, e.g., $y^{k_j} \cdot f_j(x_j, y)^{i_j} \cdot (e_j M)^{m-i_j}$. As the case of the standard RSA, these extra shift-polynomials reduce the output length of the LLL algorithm and improve partial key exposure attacks.

The bound of Theorem 1 becomes the same as the bound (1) of the Blömer-May lattice when $n = 1$. In situation (a) and (b), the bound is always superior to the bound (3) which is derived from Aono's lattices. In the situation (c), the bound is superior to the bound (3) when $n = 1, 2$, and when $n \geq 3$ and $\beta > 3(n-1)/(3n+1)$. When there are infinitely many exponent pairs n for extremely small α, Aono's attack (3), and Takayasu and Kunihiro's attack (4) work when $\beta < 3/2$ and $\beta < 1$, respectively, although Joye and Lepoint's attack (1), which uses only one exponent pair, works when $\beta < 15/8$. Our attack works when $\beta < 2$ with infinitely many exponent pairs.

5 Generalizations of the Takayasu-Kunihiro Lattice

5.1 Our Algorithm

In this section, we solve simultaneous modular equations

$$\begin{aligned} f_j(x_j, y) &= 1 - e_j\tilde{d}_j + x_j(N+y) \pmod{e_jM} \text{ and} \\ g_j(x_j, y) &= 1 + x_j(N+y) \pmod{e_j}, \end{aligned}$$

for $j = 1, 2, \ldots, n$ by generalizing the Takayasu-Kunihiro lattice [27], and obtain the following result.

Theorem 2. *Let $N = pq$ be an RSA modulus. Let (e_j, d_j) be pubic/secret exponents where $e_j \approx N, d_j \approx N^\beta$, and $e_jd_j = 1 \pmod{(p-1)(q-1)}$ for $j = 1, 2, \ldots, n$. Given public elements $N, e_1, \ldots, e_n$, and $\tilde{d}_1, \ldots, \tilde{d}_n > N^{\beta-\delta}$ that are the least significant bits of $d_1, \ldots, d_n$, respectively. Assume $e_1, \ldots, e_n$ are pairwise co-prime and the LLL algorithm outputs algebraically independent polynomials. If*

$$\delta < \frac{3n+1+(9n-5)\beta - \sqrt{16(3n-1) - 3(3n+1)(7n-3)(1-\beta)^2}}{4(3n-1)} \quad \textit{and}$$
$$\beta < \frac{3(11n+1) - \sqrt{-3(21n^2-130n-3)}}{48n}$$

for $n = 1$ and 2, then public modulus N can be factored in time polynomial in $\log N$ and exponential in n.

Proof. At first, we show the Takayasu-Kunihiro lattice to solve each single modular equation $f_j(x_j, y) = 0$ and $g_j(x_j, y) = 0$ for $j = 1, 2, \ldots, n$ that yields the bound (2). To solve the single equation, when $1 + 2\delta - 4\beta > 0$, we define a function

$$l_1(k) = \max\left\{0, \frac{k - 2(\beta-\delta)m}{1+2\delta-4\beta}\right\},$$

and use shift-polynomials

$$\begin{aligned} &x_j^{i_j} \cdot f_j(x_j, y)^{u_j} \cdot (e_jM)^{m-u_j} \text{ with } i_j = 0, 1, \ldots, m; u_j = 0, 1, \ldots, m - i_j, \\ &y^{k_j} \cdot f(x, y)^{i_j - \lceil l_1(k_j) \rceil} \cdot g(x, y)^{\lceil l_1(k_j) \rceil} \cdot e^{m-i_j} M^{m-(i_j - \lceil l_1(k_j) \rceil)} \\ &\text{with } i_j = 0, 1, \ldots, m; k_j = 1, 2, \ldots, \lfloor 2(\beta-\delta)m + (1+2\delta-4\beta)i_j \rfloor \end{aligned}$$

in lattice bases with some positive integer m. All these shift-polynomials modulo $(e_jM)^m$ have the same roots as the original solutions, $(x_j, y) = (\ell_j, -(p+q)+1)$ for $j = 1, 2, \ldots, n$. Although these polynomials do not directly generate a triangular basis matrix, we can transform it into triangular by using unravelled linearization [12]. See [27] for the detailed analysis of the proof. After the transformation, sizes of diagonals are

$$\begin{aligned}&X_j^{i'_j}Y^{u'_j}(e_jM)^{m-\min\{i'_j,u'_j\}} &&\text{with } i'_j=0,1,\ldots,m;u'_j=0,1,\ldots,i'_j,\\ &X_j^{i'_j}Y^{i'_j+k'_j}e_1^{m-i'_j}M^{m-\left(i'_j-l_1(k'_j)\right)} &&\text{with } i'_j=0,1,\ldots,m;\\ & && k'_j=1,2,\ldots,\lfloor 2(\beta-\delta)m+(1+2\delta-4\beta)i'_j\rfloor.\end{aligned}$$

When $1+2\delta-4\beta>0$, the lattice yields the bound (2).

Next, we combine these n lattices based on Minkowski sum. When $1+2\delta-4\beta>0$, we define a function

$$l_n(k)=\max\left\{0,\frac{k-2(\beta-\delta)nm}{1+2\delta-4\beta}\right\}$$

where the validities of the definition will be discussed later. Since we combine triangular basis matrices, the combined basis matrix becomes triangular with diagonals

$$\begin{aligned}&X_j^{i'_j}Y^{u'_j}(e_jM)^{m-\min\{i'_j,u'_j\}} \text{ with } i'_j=0,1,\ldots,m;u'_j=0,1,\ldots,i'_j,\\ &X_1^{i'_1}\cdots X_n^{i'_n}Y^{\sum_{j=1}^n i'_j+k'}e_1^{m-i'_1}\cdots e_n^{m-i'_n}M^{nm-\left(\sum_{j=1}^n i'_j-l_n(k')\right)}\\ &\text{with } i'_j=0,1,\ldots,m \text{ for } j=1,2,\ldots,n;\\ &\qquad k'=1,2,\ldots,\lfloor 2(\beta-\delta)nm+(1+2\delta-4\beta)\sum_{j=1}^n i'_j\rfloor.\end{aligned}$$

All polynomials which are derived from resulting lattice vectors modulo $(e_1\cdots e_n)^mM^{nm}$ have the same roots as the original solutions.

We show that the above lattice offers the bound of Theorem 2. Ignoring low order terms of m, we can compute the dimension

$$\begin{aligned}w&=\sum_{i'_1=0}^m\cdots\sum_{i'_n=0}^m\sum_{u'=0}^{\sum_{j=1}^n i'_j}1+\sum_{i'_1=0}^m\cdots\sum_{i'_n=0}^m\sum_{k'=1}^{\lfloor 2(\beta-\delta)nm+(1+2\delta-4\beta)\sum_{j=1}^n i'_j\rfloor}1\\ &=n(1-\delta)m^{n+1},\end{aligned}$$

and the volume of the lattice $\mathrm{vol}(L(\boldsymbol{B}))=X_1^{s_{X_1}}\cdots X_n^{s_{X_n}}Y^{s_Y}e_1^{s_{e_1}}\cdots e_n^{s_{e_n}}M^{s_M}$, where

$$\begin{aligned}s_{X_j}&=\sum_{i'_1=0}^m\cdots\sum_{i'_n=0}^m\sum_{u'=0}^{\sum_{j=1}^n i'_j}i'_j+\sum_{i'_1=0}^m\cdots\sum_{i'_n=0}^m\sum_{k'=1}^{\lfloor 2(\beta-\delta)nm+(1+2\delta-4\beta)\sum_{j=1}^n i'_j\rfloor}i'_j\\ &=\left(\frac{3n+1}{12}+(\beta-\delta)n+\frac{3n+1}{12}(1+2\delta-4\beta)\right)m^{n+2},\end{aligned}$$

$$\begin{aligned}
s_{e_j} &= \sum_{i_1'=0}^{m} \cdots \sum_{i_n'=0}^{m} \sum_{u'=0}^{\sum_{j=1}^{n} i_j'} (m - \min\{i_j', u'\}) \\
&\quad + \sum_{i_1'=0}^{m} \cdots \sum_{i_n'=0}^{m} \sum_{k'=1}^{\lfloor 2(\beta-\delta)nm + (1+2\delta-4\beta)\sum_{j=1}^{n} i_j' \rfloor} (m - i_j') \\
&= \left(\frac{3n+1}{12} + n(\beta-\delta) + \frac{3n-1}{12}(1+2\delta-4\beta) \right) m^{n+2}
\end{aligned}$$

for $j = 1, 2, \ldots, n$,

$$\begin{aligned}
s_Y &= \sum_{i_1=0}^{m} \cdots \sum_{i_n=0}^{m} \sum_{u=0}^{\sum_{j=1}^{n} i_j} u \\
&\quad + \sum_{i_1'=0}^{m} \cdots \sum_{i_n'=0}^{m} \sum_{k'=1}^{\lfloor 2(\beta-\delta)nm + (1+2\delta-4\beta)\sum_{j=1}^{n} i_j' \rfloor} \left(\sum_{j=1}^{n} i_j' + k' \right) \\
&= \left(\frac{n(3n+1)}{24} + n^2(\beta-\delta) + 2n^2(\beta-\delta)^2 + n^2(\beta-\delta)(1+2\delta-4\beta) \right) m^{n+2} \\
&\quad + \left(\frac{n(3n+1)}{12}(1+2\delta-4\beta) + \frac{n(3n+1)}{24}(1+2\delta-4\beta)^2 \right) m^{n+2},
\end{aligned}$$

$$\begin{aligned}
s_M &= \sum_{i_1'=0}^{m} \cdots \sum_{i_n'=0}^{m} \sum_{u'=0}^{\sum_{j=1}^{n} i_j'} (nm - u') \\
&\quad + \sum_{i_1'=0}^{m} \cdots \sum_{i_n'=0}^{m} \sum_{k'=1}^{\lfloor 2(\beta-\delta)nm + (1+2\delta-4\beta)\sum_{j=1}^{n} i_j' \rfloor} \left(nm - \left(\sum_{j=1}^{n} i_j' - l_n(k') \right) \right) \\
&= \left(\frac{n(9n-1)}{24} + n^2(\beta-\delta) + \frac{n(9n-1)}{24}(1+2\delta-4\beta) \right) m^{n+2}.
\end{aligned}$$

We can solve the simultaneous modular equations $f_j(x_j, y) = 0$ and $g_j(x_j, y) = 0$ for $j = 1, 2, \ldots, n$, when $(\mathrm{vol}(L(\boldsymbol{B})))^{1/w} < (e_1 \cdots e_n)^m M^{nm}$, that is,

$$\begin{aligned}
&4(3n-1)(\beta-\delta)^2 + 2(3n+1)(1-\beta)(\beta-\delta) \\
&+6n - 2 - (12n+4)\beta + (6n+2)\beta^2 > 0.
\end{aligned}$$

The inequality results in the bound of Theorem 2,

$$\delta < \frac{3n+1+(9n-5)\beta - \sqrt{16(3n-1) - 3(3n+1)(7n-3)(1-\beta)^2}}{4(3n-1)}$$

as required. The bound is valid only when $1 + 2\delta - 4\beta > 0$ that is equivalent to

$$24n\beta^2 - 3(11n+1)\beta + 2(6n-1) > 0,$$

that is,

$$\beta < \frac{3(11n+1) - \sqrt{-3(21n^2 - 130n - 3)}}{48n}.$$

□

5.2 Observation

As with the lattice in the previous section, compared with Aono's lattice, we select extra shift-polynomials, e.g., $y^{k_j} \cdot f_j(x_j, y)^{i_j} \cdot (e_j M)^{m-i_j}$. As the case of the standard RSA, these extra shift-polynomials reduce the output length of the LLL algorithm and improve partial key exposure attacks. Moreover, we eliminate some shift-polynomials from lattices in the previous section. This appropriate elimination enables us to obtain better bounds with some parameters. In particular, to generalize the attack [27], we define a function $l_n(k)$ to satisfy the following property.

Proposition 2. *When* $1 + 2\delta - 4\beta > 0$*, polynomials whose diagonals are* $X_1^{i'_1} \cdots X_n^{i'_n} Y^{\sum_{j=1}^n i'_j + k'}$ *are helpful when* $k' \leq 2(\beta - \delta)nm + (1+2\delta-4\beta)\sum_{j=1}^n i'_j$*. In addition, the polynomials are unhelpful when* $k' > 2(\beta - \delta)nm + (1 + 2\delta - 4\beta)\sum_{j=1}^n i'_j$*.*

The bound of Theorem 2 becomes the same as the bound (2) when $n = 1$. The bound of Theorem 2 is superior to that of Theorem 1 when

$$\beta < \frac{3(11n+1) - \sqrt{-3(21n^2 - 130n - 3)}}{48n}$$

for $n = 1$ and 2, $\beta < \left(9 - \sqrt{21}\right)/12 = 0.368\cdots$ for $n = 1$ and $\beta < \left(69 - \sqrt{537}\right)/96 = 0.477\cdots$ for $n = 2$. Using the attack, partial key exposure attack always works when $\beta < 1 - \sqrt{2/(3n+1)}$.

6 Concluding Remarks

In this paper, we study partial key exposure attacks on RSA with multiple exponent pairs when attackers know the least significant bits of secret exponents. The attacks have been analyzed for a single exponent pair case and we propose generalizations of the attacks. Our proposed attacks cover every situation that is worth studying and provide significant improvements.

Although we think our work completes the attack in this direction, there still remains an open problem. In this paper, we only analyze the case when attackers know the least significant bits of secret exponents. However, for a single exponent pair, partial key exposure attacks on RSA when attackers know the most significant bits of secret exponents have also been analyzed [11,22,27]. To generalize the attack with multiple exponent pairs remains as future work.

Acknowledgements. The author is supported by a JSPS Fellowship for Young Scientists. This research was supported by CREST, JST, and supported by JSPS Grant-in-Aid for JSPS Fellows 14J08237 and KAKENHI Grant Number 25280001.

References

1. Aono, Y.: A new lattice construction for partial key exposure attack for RSA. In: Jarecki, S., Tsudik, G. (eds.) PKC 2009. LNCS, vol. 5443, pp. 34–53. Springer, Heidelberg (2009)
2. Aono, Y.: Minkowski sum based lattice construction for multivariate simultaneous coppersmith's technique and applications to RSA. In: Boyd, C., Simpson, L. (eds.) ACISP. LNCS, vol. 7959, pp. 88–103. Springer, Heidelberg (2013)
3. Blömer, J., May, A.: New partial key exposure attacks on RSA. In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol. 2729, pp. 27–43. Springer, Heidelberg (2003)
4. Boneh, D., Durfee, G.: Cryptanalysis of RSA with private key d less than $N^{0.292}$. IEEE Trans. Inf. Theory **46**(4), 1339–1349 (2000)
5. Boneh, D., Durfee, G., Frankel, Y.: An attack on RSA given a small fraction of the private key bits. In: Ohta, K., Pei, D. (eds.) ASIACRYPT 1998. LNCS, vol. 1514, pp. 25–34. Springer, Heidelberg (1998)
6. Coppersmith, D.: Finding a small root of a univariate modular equation. In: Maurer, U.M. (ed.) EUROCRYPT 1996. LNCS, vol. 1070, pp. 155–165. Springer, Heidelberg (1996)
7. Coppersmith, D.: Small solutions to polynomial equations, and low exponent RSA vulnerabilities. J. Cryptol. **10**(4), 233–260 (1997)
8. Coppersmith, D.: Finding small solutions to small degree polynomials. In: Silverman, J.H. (ed.) CaLC 2001. LNCS, vol. 2146, pp. 20–31. Springer, Heidelberg (2001)
9. Coron, J.-S.: Resistance against differential power analysis for elliptic curve cryptosystems. In: Koç, Ç.K., Paar, C. (eds.) CHES 1999. LNCS, vol. 1717, pp. 292–302. Springer, Heidelberg (1999)
10. Coron, J.-S., May, A.: Deterministic polynomial-time equivalence of computing the RSA secret key and factoring. J. Cryptol. **20**(1), 39–50 (2007)
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.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 371–386. Springer, Heidelberg (2005)
12. Herrmann, M., May, A.: Attacking power generators using unravelled linearization: when do we output too much? In: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, vol. 5912, pp. 487–504. Springer, Heidelberg (2009)
13. Howgrave-Graham, N.: Finding small roots of univariate modular equations revisited. In: Darnell, M.J. (ed.) Cryptography and Coding 1997. LNCS, vol. 1355, pp. 131–142. Springer, Heidelberg (1997)
14. Howgrave-Graham, N., Seifert, J.-P.: Extending wiener's attack in the presence of many decrypting exponents. In: Baumgart, R. (ed.) CQRE 1999. LNCS, vol. 1740, pp. 153–166. Springer, Heidelberg (1999)
15. Joye, M., Lepoint, T.: Partial key exposure on RSA with private exponents larger than N. In: Ryan, M.D., Smyth, B., Wang, G. (eds.) ISPEC 2012. LNCS, vol. 7232, pp. 369–380. Springer, Heidelberg (2012)
16. Lenstra, A.K., Lenstra Jr., H.W., Lovász, L.: Factoring polynomials with rational coefficients. Math. Ann. **261**, 515–534 (1982)
17. May, A.: Computing the RSA secret key is deterministic polynomial time equivalent to factoring. In: Franklin, M. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 213–219. Springer, Heidelberg (2004)
18. May, A.: Using LLL-reduction for solving RSA and factorization problems: A survey. In: [21] (2010). http://www.cits.rub.de/permonen/may.html

19. Nguyên, P.Q., Stern, J.: The two faces of lattices in cryptology. In: Silverman, J.H. (ed.) CaLC 2001. LNCS, vol. 2146, pp. 146–180. Springer, Heidelberg (2001)
20. Nguyen, P.Q., Valláe, B. (eds.): The LLL Algorithm: Survey and Applications. Information Security and Cryptography. Springer, Heidelberg (2010)
21. Peng, L., Hu, L., Lu, Y., Sarkar, S., Xu, J., Huang, Z.: Cryptanalysis of Variants of RSA with Multiple Small Secret Exponents. In: Biryukov, A., Goyal, V. (eds.) INDOCRYPT 2015. LNCS, vol. 9462, pp. 105–123. Springer, Heidelberg (2015)
22. Sarkar, S., Sen Gupta, S., Maitra, S.: Partial key exposure attack on RSA – improvements for limited lattice dimensions. In: Gong, G., Gupta, K.C. (eds.) INDOCRYPT 2010. LNCS, vol. 6498, pp. 2–16. Springer, Heidelberg (2010)
23. Sarkar, S., Maitra, S.: Cryptanalysis of RSA with two decryption exponents. Inf. Process. Lett. **110**, 178–181 (2010)
24. Sarkar, S., Maitra, S.: Cryptanalysis of RSA with more than one decryption exponents. Inf. Process. Lett. **110**, 336–340 (2010)
25. Takayasu, A., Kunihiro, N.: Better lattice constructions for solving multivariate linear equations modulo unknown divisors. In: Boyd, C., Simpson, L. (eds.) ACISP. LNCS, vol. 7959, pp. 118–135. Springer, Heidelberg (2013)
26. Takayasu, A., Kunihiro, N.: Cryptanalysis of RSA with multiple small secret exponents. In: Susilo, W., Mu, Y. (eds.) ACISP 2014. LNCS, vol. 8544, pp. 176–191. Springer, Heidelberg (2014)
27. Takayasu, A., Kunihiro, N.: Partial key exposure attacks on RSA: achieving the boneh-durfee bound. In: Joux, A., Youssef, A. (eds.) SAC 2014. LNCS, vol. 8781, pp. 345–362. Springer, Heidelberg (2014)
28. Wiener, M.J.: Cryptanalysis of short RSA secret exponents. IEEE Trans. Inf. Theory **36**(3), 553–558 (1990)