Partial Key Exposure Attacks on CRT-RSA: Better Cryptanalysis to Full Size Encryption Exponents

Atsushi Takayasu(✉) and Noboru Kunihiro

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

Abstract. There have been several papers which studied the security of CRT-RSA when some bits of CRT-exponents d_p and d_q are known to attackers. At first, Blömer and May (Crypto 2003) proposed attacks which used the most or the least significant bits of either d_p or d_q. Next, Sarkar and Maitra (ACNS 2009) generalized the scenario and proposed an attack which used the most significant bits of both d_p and d_q. Recently, Lu et al. (ACNS 2014) proposed improved attacks for the same scenario as Blömer and May. These works showed that public RSA modulus can be factored when $e < N^{3/8}$, or sizes of unknown bits are less than $N^{1/4}$. In this paper, we propose improved attacks when attackers know the most/least significant bits of d_p or/and d_q. Unlike previous works, our attacks work in the same conditions regardless of positions of known bits; either the most or the least significant bits are not the matter. In addition, using our attacks, public RSA modulus can be factored even when an encryption exponent is full size or sizes of unknown bits are less than $N^{1/3}$.

Keywords: CRT-RSA · Cryptanalysis · Partial key exposure · Coppersmith's method · Lattices

1 Introduction

1.1 Background

CRT-RSA. RSA [RSA78] is one of the most famous cryptosystems and is widely used. Let $N = pq$ be a public RSA modulus where prime factors p and q are the same bit size. An encryption exponent e and a decryption exponent d satisfy $ed = 1 \mod (p-1)(q-1)$. For encryption/verifying (resp. decryption/signing), we should calculate the heavy modular exponentiation. To speed up the calculation, a simple solution is to use a smaller encryption (resp. decryption) exponent. However, public RSA modulus can be factored in polynomial time when too small decryption exponent is used. At first, Wiener [Wie90] proposed a polynomial time attack which works when $d < N^{0.25}$. Boneh and Durfee [BD00] revisited the attack and improved the bound to $d < N^{0.292}$ using the Coppersmith method [Cop96a].

T. Malkin et al. (Eds.): ACNS 2015, LNCS 9092, pp. 518–537, 2015.
DOI: 10.1007/978-3-319-28166-7_25

To thwart the attack and achieve a faster calculation for decryption/signing, Chinese Remainder Theorem (CRT) is often used as described by Quisquater and Couvreur [QC82]. Instead of the original decryption exponent d, we use CRT-exponents d_p and d_q which satisfy

$$ed_p = 1 \mod (p-1) \quad \text{and} \quad ed_q = 1 \mod (q-1).$$

However, when too small CRT-exponents are used, analogous attacks to [BD00] have been proposed [May02, GHM05, BM06, JM07, HM10]. Jochemsz and May [JM07] revealed that public RSA modulus N can be factored in polynomial time when an encryption exponent is full size, and d_p and $d_q < N^{0.073}$. In addition, CRT-RSA is more vulnerable than standard RSA against fault injection attacks [BDL97]. To use RSA efficiently and securely, we should analyze the security in detail.

Partial Key Exposure Attacks on RSA. It is widely known that factorization and RSA problems become easy when certain amount of secret information is known to attackers. When we know the most significant bits of primes factors, we can factor public RSA modulus N [RS86, Cop95, Cop96b]. Coppersmith [Cop96b] showed that the half most significant bits of a prime factor suffices to factor N.

RSA becomes vulnerable also with partial bits of decryption exponent d. Boneh et al. [BDF98] showed that the most or the least significant bits of a decryption exponent d enable us to factor public RSA modulus N. Later, several papers revisited the attack [BM03, EJMW05, Aon09, SGM10, JL12, TK14], and Ernst et al. [EJMW05] revealed that RSA is vulnerable even for a full size encryption/decryption exponent against the attack.

Partial Key Exposure Attacks on CRT-RSA. As with standard RSA, several attacks which use partial information of d_p and d_q have also been considered [BM03, SM09, LZL14]. Blömer and May [BM03] proposed attacks when the most or the least significant bits of either d_p *or* d_q are known to attackers. The attacks work when encryption exponent is small, $e < N^{1/4}$ when the most significant bits are known and $e = poly(\log N)$ when the least significant bits are known. In addition, the attacks can recover unknown bits which are less than $N^{1/4}$. Recently, Lu et al. [LZL14] revisited Blömer and May's attack [BM03]. When the most significant bits are known and d_p and $d_q \approx N^{1/2}$, they cannot improve Blömer and May's attack. However, for smaller d_p and d_q, they improved the previous attack. When the least significant bits are known, they improved Blömer and May's result and their attack works when $e < N^{3/8}$.

Sarkar and Maitra [SM09] generalized partial key exposure attacks on CRT-RSA. Unlike other previous works [BM03, LZL14], they proposed an attack when the most significant bits of both d_p *and* d_q are known to attackers[1]. However, the

[1] In their paper [SM09], they also used the most significant bits of a prime factor p. However, we do not consider the additional information in this paper.

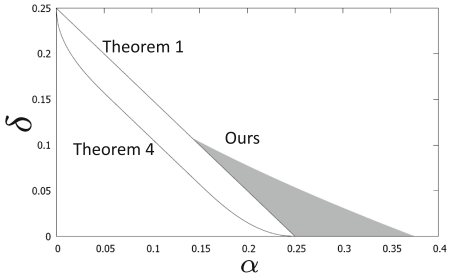

Fig. 1. Recoverable conditions for partial key exposure attacks on CRT-RSA when the most significant bits of either d_p or d_q are known to attackers.

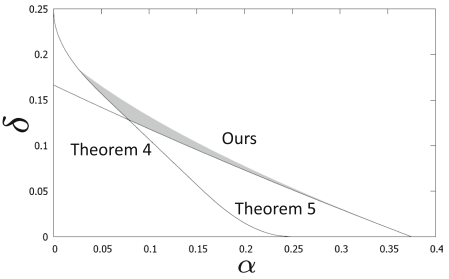

Fig. 2. Recoverable conditions for partial key exposure attacks on CRT-RSA when the least significant bits of either d_p or d_q are known to attackers.

attack is weaker than other attacks [BM03,LZL14] in the sense that the attack does not work when d_p and $d_q \approx N^{1/2}$ though they used more information than [BM03,LZL14]. The attack works only for smaller d_p and d_q.

1.2 Our Contributions

Our Results. In this paper, we study partial key exposure attacks on CRT-RSA. We propose improved attacks when the most/least significant bits of d_p or/and d_q are known. Unlike previous works, the conditions when our attacks work do not depend on the position of known bits, that is, either the most or the least significant bits are not the matter.

When we know the most/least significant bits of d_p *or* d_q, we improve Blömer and May's results [BM03] and Lu et al.'s results [LZL14] for a large encryption exponent e. As we claimed, our attack works in the same condition regardless of positions of known bits. Therefore, this is the first result to attack CRT-RSA when $1/4 \leq e < N^{3/8}$ and the most siginificant bits of either d_p or d_q are known. Figures 1 and 2 compares the recoverable ranges by each algorithm when d_p and $d_q \approx N^{1/2}$. Horizontal axis α represents a size of encryption exponent, $\alpha = \log_N e$. Vertical axis δ represents a size of unknown bits. We obtain improvements in gray areas. Our improved algorithms can recover larger δ for large α. Note that we do not compare the bound of Theorem 2 by Blömer and May [BM03], since the algorithm works only for an extremely small encryption exponent $e = poly(\log N)$.

When we know the most significant bits of both d_p *and* d_q, we improve Sarkar and Maitra's result [SM09]. In addition, we also propose an analogous attack when the least significant bits of d_p and d_q are known. Our algorithm works even when an encryption exponent e is full size and sizes of unknown bits are less than $N^{1/3}$. Figure 3 shows the recoverable ranges by our algorithm when d_p and $d_q \approx N^{1/2}$. We again stress that Sarkar and Maitra's algorithm does not work when d_p and $d_q \approx N^{1/2}$. Their algorithm works only for smaller d_p and d_q.

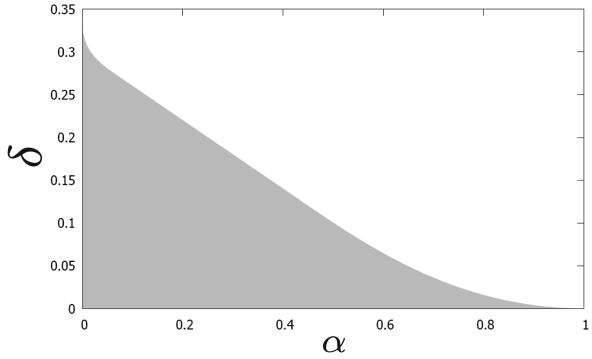

Fig. 3. Recoverable conditions for partial key exposure attacks on CRT-RSA when the most/least significant bits of both d_p and d_q are known to attackers.

Technical Overview. At Eurocrypt 1996, Coppersmith introduced two lattice-based methods, (1) to find small roots of modular univariate polynomials [Cop96a] and (2) to find small roots of bivariate polynomials over the integers [Cop96b]. The methods can be generalized to find small roots with more variables under heuristic argument. So far, several RSA vulnerabilities have been revealed by using the methods. See [Cop97, Cop01, NS01, May03, May10] for more information.

Recoverable sizes of roots using the Coppersmith methods depend on two factors, Newton polygon and a size of a modulus of a polynomial[2]. The simpler Newton polygon of a polynomial is, and the larger the size of the modulus is, we can recover larger roots. To the best of our knowledge, there are no exact criteria to decide which methods (1) or (2) enable us to recover larger roots. Therefore, we should use the appropriate method for each problem.

Blömer and May [BM03] and Lu et al. [LZL14] used the method (1). Though Lu et al.'s first attack (Theorem 4) works under the same condition regardless of positions of known bits, Blömer and May's attack (Theorem 1) and Lu et al.'s second attack (Theorem 5) work for only the case when the most or the least significant bits are known, respectively. Blömer and May's attack makes use of the most significant bits of d_p or d_q and exploits a modular polynomial with a simple Newton polygon. Lu et al.'s attack makes use of the least significant bits of d_p or d_q and exploits a modular polynomial with a large modulus. Therefore, these attacks cannot simply be generalized to the other cases when the least or the most significant bits known, respectively.

In this paper, we use the Coppersmith method (2) for partial key exposure attacks on CRT-RSA. For the attacks, we can consider polynomials with the same Newton polygon regardless of positions of known bits. Note that the Newton polygons of these polynomials are the same as that of the polynomials

[2] Note that when we use the Coppersmith method (2), we set a suitable modulus and solve a modular equation. The size of the modulus depends on a size of the polynomial.

Ernst et al. [EJMW05] used for partial key exposure attacks on RSA. In addition, Ernst et al.'s attacks work under the same condition regardless of positions of known bits, since sizes of polynomials are the same and we can use moduli for the same sizes. Analogous to Ernst et al.'s results, our partial key exposure attacks on CRT-RSA work in the same conditions regardless of positions of known bits.

To achieve better bounds when we use the Coppersmith method, it is crucial to select appropriate lattice bases. Our lattice constructions are based on the Jochemsz-May strategy [JM06]. The Jochemsz-May strategy is very simple to understand. Moreover, to the best of our knowledge, there are no results known which achieve better bounds when we use the Coppersmith method (2). The finer analyses enable us to obtain better bounds than previous results including Sarkar and Maitra's results [SM09] which also use the Coppersmith method (2).

1.3 Organization

In Sect. 2, we introduce tools for the Coppersmith method to find small roots of multivariate polynomials over the integers, Howgrave-Graham's Lemma and the LLL algorithm. Afterward, we explain the Jochemsz-May lattice construction strategy. In Sect. 3, we define the situations of partial key exposure attacks on CRT-RSA and summarize previous results [BM03,SM09,LZL14]. In Sect. 4, we propose our attacks when the most/least significant bits of either d_p or d_q are known. In Sect. 5, we propose our attacks when the most/least significant bits of both d_p and d_q are known.

2 Preliminaries

In this section, we summarize the Coppersmith method to find small roots of polynomials over the integers [Cop96b] and the Jochemsz-May strategy for lattice constructions [JM06]. So far, simpler reformulations of the method have been proposed by Coron [Cor04,Cor07]. In this paper, we introduce Coron's reformulation in [Cor04]. Though the method needs larger dimensional lattice than the other methods [Cop96b,Cor07], is much easier to understand.

For a k-variate polynomial over the integers $h(x_1,\ldots,x_k) = \sum h_{i_1,\ldots,i_k} x_1^{i_1} \cdots x_k^{i_k}$, we define a norm of a polynomial $\|h(x_1,\ldots,x_k)\| = \sqrt{\sum h_{i_1,\ldots,i_k}^2}$ and $\|h(x_1,\ldots,x_k)\|_\infty = \max_{i_1,\ldots,i_k} |h_{i_1,\ldots,i_k}|$. To find roots of a polynomial $h(x_1,\ldots,x_k)$, it suffices to find new $k-1$ polynomials which have the same roots over the integers. We use l_j to denote the largest exponent of x_j in the polynomial $h(x_1,\ldots,x_k)$. We set a integer m and $W \leq \|h(x_1,\ldots,x_k)\|_\infty$. Based on the Jochemsz-May strategy [JM06], we set a integer $R := W \prod_{j=1}^{k} X_j^{l_j(m-1)}$ and consider a modular equation $h(x_1,\ldots,x_k) = 0 \mod R$. To derive new polynomials from the modular equation, we introduce Howgrave-Graham's Lemma [How97].

Lemma 1 (Howgrave-Graham's Lemma [How97]). *Let $h(x_1,\ldots,x_k) \in \mathbb{Z}[x_1,\ldots,x_k]$ be a polynomial over the integers, which consists of at most n*

monomials. Let $R, X_1, \ldots, X_k$ be positive integers. Consider the case that the polynomial $h(x_1, \ldots, x_k)$ satisfies
1. $h(\tilde{x}_1, \ldots, \tilde{x}_k) = 0 \pmod{R}$, where $|\tilde{x}_1| < X_1, \ldots, |\tilde{x}_k| < X_k$,
2. $\|h(x_1X_1, \ldots, x_kX_k)\| < R/\sqrt{n}$.
Then $h(\tilde{x}_1, \ldots, \tilde{x}_k) = 0$ holds over the integers.

To find new polynomials which have the same roots as the original polynomial, we should find $k-1$ new polynomials which have the same roots modulo R and whose norms are small enough to satisfy Howgrave-Graham's Lemma.

To find such small polynomials, we use the LLL Algorithm. Let $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathbb{Z}^d$ be linearly independent d-dimensional vectors. All vectors are row representations. The lattice $L(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ spanned by the basis vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n$ is defined as $L(\mathbf{b}_1, \ldots, \mathbf{b}_n) = \{\sum_{j=1}^{n} c_j\mathbf{b}_j : c_j \in \mathbb{Z}\}$. We also use matrix representations for lattice bases. A basis matrix B is defined as the $n \times d$ matrix that has basis vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n$ in each row. In this representation, a lattice spanned by the basis matrix B is defined as $L(B) = \{\mathbf{c}B : \mathbf{c} \in \mathbb{Z}^n\}$. We call n a rank of the lattice, and d a dimension of the lattice. We call the lattice full-rank when $n = d$. In this paper, we only use full-rank lattices. We define a determinant of a lattice $\det(L(B))$ as $\det(L(B)) = \sqrt{\det(BB^T)}$ where B^T is a transpose of B. A determinant of a full-rank lattice can be computed as $\det(L) = |\det(B)|$.

For a cryptanalysis, to find short lattice vectors is a very important problem. In 1982, Lenstra et al. [LLL82] proposed a polynomial time algorithm to find short lattice vectors.

Proposition 1 (LLL algorithm [May03]). *Given a lattice L spanned by a basis matrix $B \in \mathbb{Z}^{n \times n}$, the LLL algorithm finds new reduced bases $\mathbf{b}'_1, \ldots, \mathbf{b}'_n$ for the same lattice that satisfy*

$$\|\mathbf{b}'_j\| \leq 2^{n(n-1)/4(n-j+1)}(\det(L(B)))^{1/(n-j+1)},$$

for all $j = 1, 2, \ldots, n$. These norms are all Euclidean norms. The running time of the LLL algorithm is polynomial time in n and input length.

Based on the Jochemsz-May strategy [JM06], we define a set of shift-polynomials g and g' as

$$g : x_1^{i_1} \cdots x_k^{i_k} \cdot h(x_1, \ldots, x_k) \prod_{j=1}^{n} X_j^{l_j(m-1)-i_j} \quad \text{for } x_1^{i_1} \cdots x_k^{i_k} \in S,$$
$$g' : x_1^{i_1} \cdots x_k^{i_k} \cdot R \quad \text{for } x_1^{i_1} \cdots x_k^{i_k} \in M \backslash S,$$

for

$$S := \{x_1^{i_1} \cdots x_k^{i_k} | x_1^{i_1} \cdots x_k^{i_k} \text{ is a monomial of } h(x_1, \ldots, x_k)^{m-1}\},$$
$$M := \{\text{monomials of } x_1^{i_1} \cdots x_k^{i_k} \cdot h(x_1, \ldots, x_k) \text{ for } x_1^{i_1} \cdots x_k^{i_k} \in S\}.$$

All these shift-polynomials g and g' modulo R have the same roots as $h(x_1, \ldots, x_k)$. We construct a lattice with coefficient vectors of $g(x_1X_1, \ldots, x_kX_k)$

and $g'(x_1X_1, \ldots, x_kX_k)$ as the bases. Polynomials whose coefficients correspond to any lattice vectors modulo R also have the same roots as the original roots. By omitting a small term and Jochemsz and May showed that new $k-1$ polynomials obtained by vectors output by the LLL algorithm satisfy Howgrave-Graham's Lemma when

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

When the condition holds, we can find all small roots.

The above lattice construction is based on the Jochemsz-May *basic* strategy. In the *extended* strategy, we add extra shifts for some variables. We omit the detail in this section though we use the strategy in the following sections. See [JM06] for more detailed information.

We should note that the method needs heuristic argument. There are no assurance if new polynomials obtained by vectors output by the LLL algorithm are algebraically independent though Coron [Cor04] proved that the original polynomial and each new polynomial is algebraically independent. In this paper, we assume that these polynomials are always algebraically independent and resultants of polynomials will not vanish since there have been few negative reports which contradict the assumption.

3 Previous Works

3.1 Definitions of Partial Key Exposure Attacks on CRT-RSA

We use α, β to represent the sizes of encryption/CRT exponents, that is, $e \approx N^{\alpha}$ and $d_p, d_q \approx N^{\beta}$. When attackers know some bits of either d_p *or* d_q, we call an attack a *single* partial key exposure attack on CRT-RSA. Similarly, when attackers know some bits of both d_p *and* d_q, we call an attack a *double* partial key exposure attack on CRT-RSA. Without loss of generality, we assume that attackers know some bits of d_p for single cases.

Next, we formulate exposed bits. When attackers know the most significant bits (MSBs) of d_p and d_q, we write d_{p_0} and d_{q_0} as partial information. Therefore, we can rewrite

$$d_p = d_{p_0}M + d_{p_1} \quad \text{and} \quad d_q = d_{q_0}M + d_{q_1}$$

with some positive integer $M \approx N^{\delta}$. Attackers do not know the least significant bits d_{p_1} and $d_{q_1} < N^{\delta}$. Similarly, when attackers know the least significant bits (LSBs) of d_p and d_q, we write d_{p_0} and d_{q_0} as partial information. Therefore, we can rewrite

$$d_p = d_{p_1}M + d_{p_0} \quad \text{and} \quad d_q = d_{q_1}M + d_{q_0}$$

with some positive integer $M \approx N^{\beta-\delta}$. Attackers do not know the most significant bits d_{p_1} and $d_{q_1} < N^{\delta}$.

3.2 Previous Results

Next, we summarize the previous results for single/double MSBs/LSBs partial key exposure attacks on CRT-RSA which work in polynomial time in $\log N$.

Theorem 1 (Single MSBs [BM03]). *Let $0 < \alpha \leq 1/4$. For a single MSBs partial key exposure attacks on CRT-RSA, when*

$$\delta < \frac{1}{4} - \alpha,$$

then public RSA modulus N can be factored in polynomial time.

The algorithm is the best when α is small and β is large.

Theorem 2 (Single LSBs [BM03]). *Let $e = poly(\log N)$. For a single LSBs partial key exposure attacks on CRT-RSA, when*

$$\delta < \beta - \frac{1}{4},$$

then public RSA modulus N can be factored in polynomial time.

In this paper, we do not compare our results with the above result, since the algorithm works only for an extremely small encryption exponent.

Theorem 3 (Double MSBs Adapted from [SM09]). *Let $1/2 - \beta < \alpha < 5/4 - 5\beta/2$. For a double MSBs partial key exposure attacks on CRT-RSA, when*

$$\delta < \frac{(18 - 36\beta - 12\alpha)\tau^2 + (20 - 40\beta - 16\alpha)\tau + 5 - 10\beta - 4\alpha}{24\tau^3 + 30\tau^2 + 16\tau + 4}$$

holds for some $\tau \geq 0$, then public RSA modulus N can be factored in polynomial time.

Theorem 4 (Single MSBs/LSBs [LZL14]). *Let $1/2 < \alpha + \beta < 3/4$. For a single MSBs/LSBs partial key exposure attacks on CRT-RSA, when*

$$\left(\alpha + \beta - \frac{1}{2}\right)\left(\frac{3}{2} - \delta - 2\sqrt{\alpha + \beta - \delta - \frac{1}{2}}\right) < \frac{1}{8} \quad \text{for } 1 - \frac{\sqrt{2}}{4} \leq \alpha + \beta < \frac{3}{4},$$

$$\alpha + \beta + \delta < \frac{1}{\sqrt{2}},$$

$$\delta\left(2 - \alpha - \beta - 2\sqrt{\delta - \alpha - \beta + \frac{1}{2}}\right) < \frac{1}{8} \quad \text{for } \frac{1}{2} < \alpha + \beta \leq \frac{3\sqrt{2}}{4} - \frac{1}{2},$$

then public RSA modulus N can be factored in polynomial time.

The algorithm is the best for the single LSBs attack for small α. Note that the second condition is valid when $1/2 < \alpha + \beta \leq 1/\sqrt{2}$ and better than the other conditions when $3\sqrt{2}/4 - 1/2 < \alpha + \beta < 1 - \sqrt{2}/4$.

Theorem 5 (Single LSBs Adapted from [LZL14]). *Let* $1/2 < \alpha + \beta \leq 7/8$. *For a single LSBs partial key exposure attacks on CRT-RSA, when*

$$\delta < \frac{5 - 2\sqrt{1 + 6(\alpha + \beta)}}{6},$$

then public RSA modulus N *can be factored in polynomial time.*

The algorithm is the best for large α and the first algorithm which works when $1/4 < \alpha \leq 3/8$. Note that the condition of Theorem 5 is slightly worse than that was written in [LZL14]. Though we omit the detail, thier condition is not valid, since their analysis implicitly has a restriction for the parameter $\sigma \leq \tau$ in their notation and the result does not satisfy the restriction.

4 Single Partial Key Exposure Attacks on CRT-RSA

For single MSBs/LSBs partial key exposure attacks on CRT-RSA, we obtain the following result.

Theorem 6 (Single MSBs/LSBs). *Let* $1/2 < \alpha + \beta \leq 7/8$. *For single MSBs/LSBs partial key exposure attacks on CRT-RSA, when*

$$-5 + 8(\alpha + \beta) + 8\delta - 12\delta^2 - 2(1 - 4\delta)\sqrt{1 - 4\delta} < 0,$$

then public RSA modulus N *can be factored in polynomial time.*

In this section, we focus on the MSBs case.

Based on the Jochemsz-May Basic Strategy. At first, we start from the Jochemsz-May basic strategy. It is interesting that the lattice construction yields the second condition of Theorem 4.

For a single MSBs partial key exposure attack on CRT-RSA, looking at CRT-RSA key generation,

$$e(d_{p_0}M + d_{p_1}) = 1 + \ell(p - 1),$$

with some integer $\ell \approx N^{\alpha+\beta-1/2}$. We consider a polynomial over the integers

$$f_{sMSBs}(x, y, z_1) := c_{sMSBs} + ex + y(z_1 - 1)$$

where $c_{sMSBs} = 1 - ed_{p_0}M$ whose roots are $(x, y, z_1) = (-d_{p_1}, \ell, p)$. If we can find two polynomials which have the same roots over the integers as f_{sMSBs}, we can recover the roots. We also use an additional variable $z_2 = q$ and the Durfee-Nguyen technique [DN00] $z_1 z_2 = N$ which Bleichenbacher and May [BM06] and Lu et al. [LZL14] used to attack CRT-RSA. Sizes of the solutions are bounded by $X := N^{\delta}, Y := N^{\alpha+\beta-1/2}, Z_1 := N^{1/2}, Z_2 := N^{1/2}$.

We set an integer $W_{sMSBs} := N^{\alpha+\beta}$ since $\|f_{sMSBs}(x, y, z_1)\|_{\infty} \geq |c_{sMSBs}| \approx N^{\alpha+\beta}$. Next, we set an integer $R_{s1} := W_{sMSBs}(XY)^{m-1}Z_1^{m-1-k}Z_2^k$ with

some integer m and $k = \eta m$ with a restriction $0 \leq \eta \leq 1$ such that $\gcd(c_{sMSBs}, R_{s1}) = 1$. We compute $a_{sMSBs1} = c_{sMSBs}^{-1} \bmod R_{s1}$ and $f'_{sMSBs1}(x, y, z_1) := a_{sMSBs1} \cdot f_{sMSBs}(x, y, z_1) \bmod R_{s1}$. We define a set of shift-polynomials g_{sMSBs1}, g_{sMSBs2} and g'_{sMSBs1}, g'_{sMSBs2} as

$$\begin{aligned}
g_{sMSBs1} &: x^{i_x} y^{i_y} z_1^{i_{z_1}-k} \cdot f'^{\,}_{sMSBs1}(x, y, z_1) X^{m-1-i_x} Y^{m-1-i_y} Z_1^{m-1-i_{z_1}} Z_2^{k} \\
&\quad \text{for } x^{i_x} y^{i_y} z_1^{i_{z_1}} \in S_{s1}, \\
g_{sMSBs2} &: x^{i_x} y^{i_y} z_2^{k-i_{z_1}} \cdot f'^{\,}_{sMSBs1}(x, y, z_1) X^{m-1-i_x} Y^{m-1-i_y} Z_1^{m-1-k} Z_2^{i_{z_1}} \\
&\quad \text{for } x^{i_x} y^{i_y} z_1^{i_{z_1}} \in S_{s2}, \\
g'_{sMSBs1} &: x^{i_x} y^{i_y} z_1^{i_{z_1}-k} \cdot R_{s1} \quad \text{for } x^{i_x} y^{i_y} z_1^{i_{z_1}} \in M_{s1} \backslash (S_{s1} \cup S_{s2}), \\
g'_{sMSBs2} &: x^{i_x} y^{i_y} z_2^{k-i_{z_1}} \cdot R_{s1} \quad \text{for } x^{i_x} y^{i_y} z_1^{i_{z_1}} \in M_{s2} \backslash (S_{s1} \cup S_{s2}),
\end{aligned}$$

for

$$\begin{aligned}
S_1 &:= \{x^{i_x} y^{i_y} z_1^{i_{z_1}} | x^{i_x} y^{i_y} z_1^{i_{z_1}} \text{ is a monomial of } f'^{\,}_{sMSBs1}(x, y, z_1)^{m-1} \text{ and } i_{z_1} \geq k\}, \\
S_2 &:= \{x^{i_x} y^{i_y} z_1^{i_{z_1}} | x^{i_x} y^{i_y} z_1^{i_{z_1}} \text{ is a monomial of } f'^{\,}_{sMSBs1}(x, y, z_1)^{m-1} \text{ and } i_{z_1} < k\}, \\
M_1 &:= \{x^{i_x} y^{i_y} z_1^{i_{z_1}} | \text{monomials of } x^{i'_x} y^{i'_y} z_1^{i'_{z_1}} \cdot f'^{\,}_{sMSBs1}(x, y, z_1) \\
&\qquad \text{for } x^{i'_x} y^{i'_y} z_1^{i'_{z_1}} \in S_{s1} \cup S_{s2} \text{ and } i_{z_1} \geq k\}, \\
M_2 &:= \{x^{i_x} y^{i_y} z_1^{i_{z_1}} | \text{monomials of } x^{i'_x} y^{i'_y} z_1^{i'_{z_1}} \cdot f'^{\,}_{sMSBs1}(x, y, z_1) \\
&\qquad \text{for } x^{i'_x} y^{i'_y} z_1^{i'_{z_1}} \in S_{s1} \cup S_{s2} \text{ and } i_{z_1} < k\}.
\end{aligned}$$

For shift-polynomials g_{sMSBs2}, we eliminate the term $z_1 z_2$ by using the Durfee-Nguyen technique $z_1 z_2 = N$. By definition, the index sets become

$$\begin{aligned}
S_{s1} \Leftrightarrow\ & i_x = 0, 1, \ldots, m-1-k; i_y = k, k+1, \ldots, m-1-i_x; \\
& i_{z_1} = k, k+1, \ldots, m-1-i_x, \\
S_{s2} \Leftrightarrow\ & i_x = 0, 1, \ldots, m-1; i_y = 0, 1, \ldots, m-1-i_x; \\
& i_{z_1} = 0, 1, \ldots, \min\{k-1, m-1-i_x\}, \\
M_{s1} \Leftrightarrow\ & i_x = 0, 1, \ldots, m-k; i_y = k, k+1, \ldots, m-i_x; i_{z_1} = k, k+1, \ldots, m-i_x, \\
M_{s2} \Leftrightarrow\ & i_x = 0, 1, \ldots, m; i_y = 0, 1, \ldots, m-i_x; i_{z_1} = 0, 1, \ldots, \min\{k-1, m-i_x\}.
\end{aligned}$$

All these shift-polynomials g_{sMSBs1}, g_{sMSBs2} and g'_{sMSBs1}, g'_{sMSBs2} modulo R_{s1} have the roots $(x, y, z_1, z_2) = (-d_{p_1}, \ell, p, q)$ which are the same as $f_{sMSBs}(x, y, z_1)$ and the definition of z_2. We construct a lattice with coefficient vectors of $g_{sMSBs1}(xX, yY, z_1 Z_1, z_2 Z_2), g_{sMSBs2}(xX, yY, z_1 Z_1, z_2 Z_2)$ and $g'_{sMSBs1}(xX, yY, z_1 Z_1, z_2 Z_2), g'_{sMSBs2}(xX, yY, z_1 Z_1, z_2 Z_2)$ as the bases. Based on the Jochemsz-May strategy [JM06], LLL outputs two short lattice vectors which satisfy Howgrave-Graham's Lemma when

$$X^{\frac{m^3}{6}+o(m^3)} Y^{\frac{m^3}{3}+o(m^3)} Z_1^{\frac{(1-\eta)^3}{6}m^3+o(m^3)} Z_2^{\left(\frac{\eta^2}{2}-\frac{\eta^3}{6}\right)m^3+o(m^3)} < W_{sMSBs}^{\frac{m^3}{6}+o(m^3)}.$$

Ignoring low order terms of m, and the condition becomes

$$\delta \cdot \frac{1}{6} + \left(\alpha + \beta - \frac{1}{2}\right) \cdot \frac{1}{3} + \frac{1}{2} \cdot \left(\frac{(1-\eta)^3}{6} + \frac{\eta^2}{2} - \frac{\eta^3}{6}\right) < (\alpha + \beta) \cdot \frac{1}{6}.$$

The detailed calculation is discussed later. We optimize the parameter $\eta = 1 - 1/\sqrt{2}$ which satisfy $0 \leq \eta \leq 1$ and obtain the condition,

$$\alpha + \beta + \delta < \frac{1}{\sqrt{2}}.$$

The condition corresponds to the second condition of Theorem 4.

Based on the Jochemsz-May Extended Strategy. Next, we show our lattice construction based on the Jochemsz-May extended strategy. The lattice construction enables us to solve the equation $f_{sMSBs}(x, y, z_1) = 0$ for larger $\alpha + \beta$ and yields the condition of Theorem 6.

We set an integer $R_{s2} := W_{sMSBs}(XY)^{m-1} Z_1^{m-1-k+t} Z_2^k$ with some integers $m, k = \eta m$ and $t = \tau m$ with restrictions $0 \leq \tau \leq \eta \leq 1$ such that $\gcd(c_{sMSBs}, R_{s2}) = 1$. We compute a_{sMSBs2} and $f'_{sMSBs2}(x, y, z_1)$ as in the basic strategy and define a set of shift-polynomials g_{sMSBs3}, g_{sMSBs4} and g'_{sMSBs3}, g'_{sMSBs4} as

$$\begin{aligned}
g_{sMSBs3} &: x^{i_x} y^{i_y} z_1^{i_{z_1}-k} \cdot f'_{sMSBs2}(x, y, z_1) X^{m-1-i_x} Y^{m-1-i_y} Z_1^{m-1+t-i_{z_1}} Z_2^k \\
&\quad \text{for } x^{i_x} y^{i_y} z_1^{i_{z_1}} \in S_{s3}, \\
g_{sMSBs4} &: x^{i_x} y^{i_y} z_2^{k-i_{z_1}} \cdot f'_{sMSBs2}(x, y, z_1) X^{m-1-i_x} Y^{m-1-i_y} Z_1^{m-1-k+t} Z_2^{i_{z_1}} \\
&\quad \text{for } x^{i_x} y^{i_y} z_1^{i_{z_1}} \in S_{s4}, \\
g'_{sMSBs3} &: x^{i_x} y^{i_y} z_1^{i_{z_1}-k} \cdot R_{s2} \quad \text{for } x^{i_x} y^{i_y} z_1^{i_{z_1}} \in M_{s3} \backslash (S_{s3} \cup S_{s4}), \\
g'_{sMSBs4} &: x^{i_x} y^{i_y} z_2^{k-i_{z_1}} \cdot R_{s2} \quad \text{for } x^{i_x} y^{i_y} z_1^{i_{z_1}} \in M_{s4} \backslash (S_{s3} \cup S_{s4}),
\end{aligned}$$

for

$$\begin{aligned}
S_{s3} &:= \bigcup_{0 \leq j \leq t} \{x^{i_x} y^{i_y} z_1^{i_{z_1}+j} | x^{i_x} y^{i_y} z_1^{i_{z_1}} \text{ is a monomial of } f'_{sMSBs2}(x, y, z_1)^{m-1} \\
&\qquad \text{and } i_{z_1} \geq k\}, \\
S_{s4} &:= \bigcup_{0 \leq j \leq t} \{x^{i_x} y^{i_y} z_1^{i_{z_1}+j} | x^{i_x} y^{i_y} z_1^{i_{z_1}} \text{ is a monomial of } f'_{sMSBs2}(x, y, z_1)^{m-1} \\
&\qquad \text{and } i_{z_1} < k\}, \\
M_{s3} &:= \{x^{i_x} y^{i_y} z_1^{i_{z_1}} | \text{monomials of } x^{i'_x} y^{i'_y} z_1^{i'_{z_1}} \cdot f'_{sMSBs2}(x, y, z_1) \\
&\qquad \text{for } x^{i'_x} y^{i'_y} z_1^{i'_{z_1}} \in S_{s3} \cup S_{s4} \text{ and } i_{z_1} \geq k\}, \\
M_{s4} &:= \{x^{i_x} y^{i_y} z_1^{i_{z_1}} | \text{monomials of } x^{i'_x} y^{i'_y} z_1^{i'_{z_1}} \cdot f'_{sMSBs2}(x, y, z_1) \\
&\qquad \text{for } x^{i'_x} y^{i'_y} z_1^{i'_{z_1}} \in S_{s3} \cup S_{s4} \text{ and } i_{z_1} < k\}.
\end{aligned}$$

For shift-polynomials g_{sMSBs4}, we eliminate the term $z_1 z_2$ by using the Durfee-Nguyen technique $z_1 z_2 = N$. By definition, the index sets become

$$\begin{aligned}
S_{s3} \Leftrightarrow i_x &= 0, 1, \ldots, m-1-k+t; i_y = k-t, k-t+1, \ldots, m-1-i_x; \\
i_{z_1} &= k, k+1, \ldots, m-1+t-i_x, \\
S_{s4} \Leftrightarrow i_x &= 0, 1, \ldots, m-1; i_y = 0, 1, \ldots, m-1-i_x; \\
i_{z_1} &= 0, 1, \ldots, \min\{k-1, m-1+t-i_x\}, \\
M_{s3} \Leftrightarrow i_x &= 0, 1, \ldots, m-k+t; i_y = k-t, k-t+1, \ldots, m-i_x; \\
i_{z_1} &= k, k+1, \ldots, m+t-i_x, \\
M_{s4} \Leftrightarrow i_x &= 0, 1, \ldots, m; i_y = 0, 1, \ldots, m-i_x; \\
i_{z_1} &= 0, 1, \ldots, \min\{k-1, m+t-i_x\}.
\end{aligned}$$

All these shift-polynomials g_{sMSBs3}, g_{sMSBs4} and g'_{sMSBs3}, g'_{sMSBs4} modulo R_{s2} have the roots $(x, y, z_1, z_2) = (-d_{p_1}, \ell, p, q)$ which are the same as $f_{sMSBs}(x, y, z_1)$ and the definition of z_2. We construct a lattice with coefficient vectors of $g_{sMSBs3}(xX, yY, z_1 Z_1, z_2 Z_2), g_{sMSBs4}(xX, yY, z_1 Z_1, z_2 Z_2)$ and $g'_{sMSBs3}(xX, yY, z_1 Z_1, z_2 Z_2), g'_{sMSBs4}(xX, yY, z_1 Z_1, z_2 Z_2)$ as the bases. Based on the Jochemsz-May strategy [JM06], LLL outputs two short lattice vectors which satisfy Howgrave-Graham's Lemma when $X^{s_X} Y^{s_Y} Z_1^{s_{Z_1}} Z_2^{s_{Z_2}} < W_{sMSBs}^{|S|}$ where

$$s_X = \sum_{i=0}^{m} \sum_{j=0}^{m-i} (m-i-j) + \sum_{i=0}^{m} \sum_{j=1}^{t} (m-i) = \left(\frac{1}{6} + \frac{\tau}{2}\right) m^3 + o(m^3),$$

$$s_Y = \sum_{i=0}^{m} \sum_{j=0}^{m-i} (i+j) + \sum_{i=0}^{m} \sum_{j=1}^{t} i = \left(\frac{1}{3} + \frac{\tau}{2}\right) m^3 + o(m^3),$$

$$s_{Z_1} = \sum_{i=s}^{m} \sum_{j=0}^{m-i} (i-s) + \sum_{i=s-t}^{m} \sum_{j=s-t-i}^{t} (i+j-s) = \frac{(1+\tau-\eta)^3}{6} m^3 + o(m^3),$$

$$s_{Z_2} = \sum_{i=0}^{s} \sum_{j=0}^{m-i} (s-i) + \sum_{i=0}^{s} \sum_{j=1}^{\min\{t, s-i\}} (s-i-j) = \left(\frac{\eta^2}{2} - \frac{(\eta-\tau)^3}{6}\right) m^3 + o(m^3),$$

$$|S| = \sum_{i_x=0}^{m-1} \sum_{i_y=0}^{m-1-i_x} \sum_{i_{z_1}=0}^{m-1+t-i_x} 1 = \left(\frac{1}{6} + \frac{\tau}{2}\right) m^3 + o(m^3).$$

Ignoring low order terms of m, the condition becomes

$$\begin{aligned}
&\delta \cdot \left(\frac{1}{6} + \frac{\tau}{2}\right) + \left(\alpha + \beta - \frac{1}{2}\right) \cdot \left(\frac{1}{3} + \frac{\tau}{2}\right) + \frac{1}{2} \cdot \left(\frac{(1+\tau-\eta)^3}{6} + \frac{\eta^2}{2} - \frac{(\eta-\tau)^3}{6}\right) \\
&< (\alpha + \beta) \cdot \left(\frac{1}{6} + \frac{\tau}{2}\right).
\end{aligned}$$

Let $\tau = 0$ and we can obtain the condition based on the Jochemsz-May basic strategy. We optimize the parameter $\eta = (1 - 2\delta)/2, \tau = \left(\sqrt{1 - 4\delta} - 2\delta\right)/2$ and obtain the condition,

$$-5+8(\alpha+\beta)+8\delta-12\delta^2-2(1-4\delta)\sqrt{1-4\delta}<0.$$

Note that the restriction $\tau \leq \eta \leq 1$ always holds. The restriction $0 \leq \tau$ holds only when $\delta \leq 1/\sqrt{2}-1/2$. However, the condition always holds for $\alpha+\beta > 1/2$, which is the smallest choice of $\alpha+\beta$ for CRT-RSA.

Single LSBs Partial Key Exposure Attack on CRT-RSA. For a single LSBs partial key exposure attack on CRT-RSA, looking at CRT-RSA key generation,

$$e(d_1M+d_0) = 1+\ell(p-1),$$

with some integer $\ell \approx N^{\alpha+\beta-1/2}$. We consider a polynomial over the integers

$$f_{sLSBs}(x,y,z_1) := c_{sLSBs} + eMx + y(z_1-1)$$

where $c_{sLSBs} = 1-ed_0$ whose roots are $(x,y,z_1) = (-d_0, \ell, p)$. We also use an additional variable $z_2 = q$. Sizes of the solutions are bounded by $X := N^{\delta}, Y := N^{\alpha+\beta-1/2}, Z_1 := N^{1/2}, Z_2 := N^{1/2}$.

We set an integer $W_{sLSBs} := N^{\alpha+\beta}$ since $\|f_{sLSBs}(x,y,z_1)\|_{\infty} \geq |eMx| \approx N^{\alpha+\beta}$. The polynomial $f_{sLSBs}(x,y,z_1)$ has the same Newton polygon as $f_{sMSBs}(x,y,z_1)$, and the integers W_{sMSBs} and W_{sLSBs} are the same sizes. Therefore, we use the same lattice construction as above and obtain the condition of Theorem 6.

5 Double Partial Key Exposure Attacks on CRT-RSA

For double MSBs/LSBs partial key exposure attacks on CRT-RSA, we obtain the following result.

Theorem 7 (Double MSBs/LSBs). *Let $1/2 < \alpha+\beta \leq 3/2$. For double MSBs/LSBs partial key exposure attacks on CRT-RSA, when*

$$\delta < \frac{(18-12(\alpha+\beta))\tau^2+(20-16(\alpha+\beta))\tau+5-4(\alpha+\beta)}{24\tau^3+54\tau^2+40\tau+10} \text{ for } \frac{15}{16} < \alpha+\beta < \frac{3}{2},$$

$$\delta < \frac{5-4(\alpha+\beta)}{10},$$

$$\delta < \frac{(12-24(\alpha+\beta))\tau^3+(27-30(\alpha+\beta))\tau^2+(20-16(\alpha+\beta))\tau+5-4(\alpha+\beta)}{36\tau^2+40\tau+10}$$

$$\text{for } \frac{1}{2} < \alpha+\beta < \frac{15}{26},$$

hold for some $\tau > 0$, then public RSA modulus N can be factored in polynomial time.

Note that the second condition is valid when $1/2 \leq \alpha+\beta \leq 5/4$ and better than the other conditions when $15/26 \leq \alpha+\beta \leq 15/16$.

In this section, we focus on the MSBs case.

Based on the Jochemsz-May Basic Strategy. As in a previous section, we start from the Jochemsz-May basic strategy. The lattice construction yields the second condition of Theorem 7.

Looking at CRT-RSA key generation,

$$ed_p = 1 + \ell_p(p-1) \quad \text{and} \quad ed_q = 1 + \ell_q(q-1),$$

with some integers $\ell_p, \ell_q \approx N^{\alpha+\beta-1/2}$. We multiply following two equations

$$ed_p - 1 + \ell_p = \ell_p p \quad \text{and} \quad ed_q - 1 + \ell_q = \ell_q q,$$

and obtain

$$e^2 d_p d_q + ed_p(\ell_q - 1) + ed_q(\ell_p - 1) - (N-1)\ell_p\ell_q - (\ell_p + \ell_q - 1) = 0.$$

For a double MSBs partial key exposure attack on CRT-RSA, we obtain

$$\begin{aligned} &e^2(d_{p_0}M + d_{p_1})(d_{q_0}M + d_{q_1}) + e(d_{p_0}M + d_{p_1})(\ell_q - 1) \\ &+e(d_{q_0}M + d_{q_1})(\ell_p - 1) - (N-1)\ell_p\ell_q - (\ell_p + \ell_q - 1) = 0. \end{aligned}$$

We consider a polynomial over the integers,

$$\begin{aligned} f_{dMSBs}(x_1, x_2, y_1, y_2) = e^2 x_1 x_2 + (e^2 d_{q_0} M - e)x_1 + (e^2 d_{p_0} M - e)x_2 \\ +ex_1 y_2 + ex_2 y_1 + (ed_{q_0} M - 1)y_1 + (ed_{p_0} M - 1)y_2 \\ -(N-1)y_1 y_2 + c_{dMSBs}, \end{aligned}$$

where $c_{dMSBs} = e^2 d_{p_0} d_{q_0} M^2 - ed_{p_0} M - ed_{q_0} M + 1$ whose roots are $(x_1, x_2, y_1, y_2) = (d_{p_1}, d_{q_1}, \ell_p, \ell_q)$. Sizes of the roots are bounded by $X_1 := N^\delta, X_2 := N^\delta, Y_1 := N^{\alpha+\beta-1/2}, Y_2 := N^{\alpha+\beta-1/2}$.

We set an integer $W_{dMSBs} := N^{2(\alpha+\beta)}$ since $\|f_{dMSBs}(x_1, x_2, y_1, y_2)\|_\infty \geq |(N-1)y_1 y_2| \approx N^{2(\alpha+\beta)}$. Note that $f_{dMSBs}(x_1, x_2, y_1, y_2)$ has the same monomials as the polynomial which Jochemsz and May considered in [JM07]. Therefore, we use the same lattice construction as [JM07]. We set an integer $R_{d1} := W_{dMSBs}(X_1 X_2 Y_1 Y_2)^{m-1}$ with some integer m such that $\gcd(c_{dMSBs}, R_{d1}) = 1$. We compute $a_{dMSBs1} = c_{dMSBs}^{-1} \mod R_{d1}$ and $f'_{dMSBs1}(x_1, x_2, y_1, y_2) := a_{dMSBs1} \cdot f_{dMSBs}(x_1, x_2, y_1, y_2) \mod R_{d1}$. We define a set of shift-polynomials g_{dMSBs1} and g'_{dMSBs1} as

$$\begin{aligned} g_{dMSBs1} :\ & x_1^{i_{x_1}} x_2^{i_{x_2}} y_1^{i_{y_1}} y_2^{i_{y_2}} \\ & \cdot f'_{dMSBs1}(x_1, x_2, y_1, y_2) X_1^{m-1-i_{x_1}} X_2^{m-1-i_{x_2}} Y_1^{m-1-i_{y_1}} Y_2^{m-1-i_{y_2}} \\ & \text{for } x_1^{i_{x_1}} x_2^{i_{x_2}} y_1^{i_{y_1}} y_2^{i_{y_2}} \in S_{d1}, \\ g'_{dMSBs1} :\ & x_1^{i_{x_1}} x_2^{i_{x_2}} y_1^{i_{y_1}} y_2^{i_{y_2}} \cdot R_{d1} \quad \text{for } x_1^{i_{x_1}} x_2^{i_{x_2}} y_1^{i_{y_1}} y_2^{i_{y_2}} \in M_{d1} \backslash S_{d1}, \end{aligned}$$

for

$$\begin{aligned} S_{d1} := \{ & x_1^{i_{x_1}} x_2^{i_{x_2}} y_1^{i_{y_1}} y_2^{i_{y_2}} \mid x_1^{i_{x_1}} x_2^{i_{x_2}} y_1^{i_{y_1}} y_2^{i_{y_2}} \text{ is a monomial of} \\ & f'_{dMSBs1}(x_1, x_2, y_1, y_2)^{m-1} \}, \\ M_{d1} := \{ & \text{monomials of } x_1^{i_{x_1}} x_2^{i_{x_2}} y_1^{i_{y_1}} y_2^{i_{y_2}} \cdot f'_{dMSBs1}(x_1, x_2, y_1, y_2) \mid \\ & x_1^{i_{x_1}} x_2^{i_{x_2}} y_1^{i_{y_1}} y_2^{i_{y_2}} \in S_{d1} \}. \end{aligned}$$

By definition, the index sets become

$$\begin{aligned} S_{d1} \Leftrightarrow i_{x_1} &= 0, 1, \ldots, m-1-i_{y_1}; i_{x_2} =; 0, 1, \ldots, m-1-i_{y_2}; \\ i_{y_1} &= 0, 1, \ldots, m-1; i_{y_2} = 0, 1, \ldots, m-1, \\ M_{d1} \Leftrightarrow i_{x_1} &= 0, 1, \ldots, m-i_{y_1}; i_{x_2} =; 0, 1, \ldots, m-i_{y_2}; i_{y_1} = 0, 1, \ldots, m; \\ i_{y_2} &= 0, 1, \ldots, m. \end{aligned}$$

Shift-polynomials g_{dMSBs1} and g'_{dMSBs1} modulo R_{d1} have the roots $(x_1, x_2, y_1, y_2) = (d_{p_1}, d_{q_1}, \ell_p, \ell_q)$ which are the same as $f_{dMSBs}(x_1, x_2, y_1, y_2)$. We construct a lattice with coefficient vectors of $g_{dMSBs1}(x_1X_1, x_2X_2, y_1Y_1, y_2Y_2)$ and $g'_{dMSBs1}(x_1X_1, x_2X_2, y_1Y_1, y_2Y_2)$ as the bases. Based on the Jochemsz-May strategy [JM06], LLL outputs three short lattice vectors which satisfy Howgrave-Graham's Lemma when

$$(X_1X_2)^{\frac{5}{12}m^4+o(m^4)}(Y_1Y_2)^{\frac{5}{12}m^4+o(m^4)} < W_{dMSBs}^{\frac{1}{4}m^4+o(m^4)}.$$

Ignoring low order terms of m, the condition becomes

$$\delta \cdot 2 \cdot \frac{5}{12} + \left(\alpha + \beta - \frac{1}{2}\right) \cdot 2 \cdot \frac{5}{12} < 2(\alpha+\beta) \cdot \frac{1}{4},$$

that is,

$$\delta < \frac{5 - 4(\alpha+\beta)}{10}.$$

The detailed calculation is discussed later.

Based on the Jochemsz-May Extended Strategy. Next, we show our lattice construction based on the Jochemsz-May extended strategy. The lattice construction enables us to solve the equation $f_{dMSBs}(x_1, x_2, y_1, y_2) = 0$ for larger $\alpha+\beta$ and yields the first and the third condition of Theorem 7. At first, we show the lattice construction for the first condition of Theorem 7.

We set an integer $R_{d2} := W_{dMSBs}(X_1X_2)^{m-1+t}(Y_1Y_2)^{m-1}$ with some integers m and $t = \tau m$ such that $\gcd(c_{dMSBs}, R_{d2}) = 1$. We compute $a_{dMSBs2} = c_{dMSBs}^{-1} \mod R_{d2}$ and $f'_{dMSBs2}(x_1, x_2, y_1, y_2)$ as in the basic strategy. We define a set of shift-polynomials g_{dMSBs2} and g'_{dMSBs2} as

$$\begin{aligned} g_{dMSBs2} : \; & x_1^{i_{x_1}} x_2^{i_{x_2}} y_1^{i_{y_1}} y_2^{i_{y_2}} \\ & \cdot f'_{dMSBs2}(x_1, x_2, y_1, y_2) X_1^{m-1+t-i_{x_1}} X_2^{m-1+t-i_{x_2}} Y_1^{m-1-i_{y_1}} Y_2^{m-1-i_{y_2}} \\ & \text{for } x_1^{i_{x_1}} x_2^{i_{x_2}} y_1^{i_{y_1}} y_2^{i_{y_2}} \in S_{d2}, \\ g'_{dMSBs2} : \; & x_1^{i_{x_1}} x_2^{i_{x_2}} y_1^{i_{y_1}} y_2^{i_{y_2}} \cdot R_{d2} \quad \text{for } x_1^{i_{x_1}} x_2^{i_{x_2}} y_1^{i_{y_1}} y_2^{i_{y_2}} \in M_{d2} \backslash S_{d2}, \end{aligned}$$

for

$$S_{d2} := \bigcup_{0 \le j_1, j_2 \le t} \{x_1^{i_{x_1}+j_1} x_2^{i_{x_2}+j_2} y_1^{i_{y_1}} y_2^{i_{y_2}} \mid x_1^{i_{x_1}} x_2^{i_{x_2}} y_1^{i_{y_1}} y_2^{i_{y_2}} \text{ is a monomial of } f'_{dMSBs2}(x_1, x_2, y_1, y_2)^{m-1}\},$$

$$M_{d2} := \{\text{monomials of } x_1^{i_{x_1}} x_2^{i_{x_2}} y_1^{i_{y_1}} y_2^{i_{y_2}} \cdot f'_{dMSBs2}(x_1, x_2, y_1, y_2) \mid x_1^{i_{x_1}} x_2^{i_{x_2}} y_1^{i_{y_1}} y_2^{i_{y_2}} \in S_{d2}\}.$$

By definition, the index sets become

$$\begin{aligned} S_{d2} \Leftrightarrow\ & i_{x_1} = 0, 1, \ldots, m-1+t-i_{y_1}; i_{x_2} =; 0, 1, \ldots, m-1+t-i_{y_2}; \\ & i_{y_1} = 0, 1, \ldots, m-1; i_{y_2} = 0, 1, \ldots, m-1, \\ M_{d2} \Leftrightarrow\ & i_{x_1} = 0, 1, \ldots, m+t-i_{y_1}; i_{x_2} =; 0, 1, \ldots, m+t-i_{y_2}; i_{y_1} = 0, 1, \ldots, m; \\ & i_{y_2} = 0, 1, \ldots, m. \end{aligned}$$

Shift-polynomials g_{dMSBs2} and g'_{dMSBs2} modulo R_{d2} have the roots $(x_1, x_2, y_1, y_2) = (d_{p_1}, d_{q_1}, \ell_p, \ell_q)$ which are the same as $f_{dMSBs}(x_1, x_2, y_1, y_2)$. We construct a lattice with coefficient vectors of $g_{dMSBs2}(x_1X_1, x_2X_2, y_1Y_1, y_2Y_2)$ and $g'_{dMSBs2}(x_1X_1, x_2X_2, y_1Y_1, y_2Y_2)$ as the bases. Based on the Jochemsz-May strategy [JM06], LLL outputs three short lattice vectors which satisfy Howgrave-Graham's Lemma when[3]

$$\begin{aligned} & (X_1X_2)^{(\tau^2+\frac{9}{4}\tau^2+\frac{5}{3}\tau+\frac{5}{12})m^4+o(m^4)} (Y_1Y_2)^{(\frac{3}{2}\tau^2+\frac{5}{3}\tau+\frac{5}{12})m^4+o(m^4)} \\ & < W_{dMSBs}^{(\tau^2+\tau+\frac{1}{4})m^4+o(m^4)}. \end{aligned}$$

Ignoring low order terms of m, the condition becomes

$$\begin{aligned} & \delta \cdot 2 \cdot \left(\tau^2 + \frac{9}{4}\tau^2 + \frac{5}{3}\tau + \frac{5}{12}\right) + \left(\alpha + \beta - \frac{1}{2}\right) \cdot 2 \cdot \left(\frac{3}{2}\tau^2 + \frac{5}{3}\tau + \frac{5}{12}\right) \\ & < 2(\alpha+\beta) \cdot \left(\tau^2 + \tau + \frac{1}{4}\right), \end{aligned}$$

that is,

$$\delta < \frac{(18 - 12(\alpha+\beta))\tau^2 + (20 - 16(\alpha+\beta))\tau + 5 - 4(\alpha+\beta)}{24\tau^3 + 54\tau^2 + 40\tau + 10}.$$

The condition becomes the first condition of Theorem 7.

Next, we briefly summarize the lattice construction to yield the third condition of Theorem 7. This is the almost the same as the lattice construction described above except we add extra-shifts to y_1 and y_2 instead of x_1 and x_2.

To solve the equation $f_{dMSBs}(x_1, x_2, y_1, y_2) = 0$, we set an integer $R_{d3} := W_{dMSBs}(X_1X_2)^{m-1}(Y_1Y_2)^{m-1+t}$ with some integer m and $t = \tau m$ such

[3] In this paper, we omit the calculation since that is the same as [JM07]. See the paper for detailed calculation.

that $\gcd(c_{dMSBs}, R_{d3}) = 1$. We compute $a_{dMSBs3} = c_{dMSBs}^{-1} \bmod R_{d3}$ and $f'_{dMSBs3}(x_1, x_2, y_1, y_2) := a_{dMSBs3} f_{dMSBs}(x_1, x_2, y_1, y_2) \bmod R_{d3}$. We define a set of shift-polynomials g_{dMSBs3} and g'_{dMSBs3} as

$$\begin{aligned} g_{dMSBs3} :\ & x_1^{i_{x_1}} x_2^{i_{x_2}} y_1^{i_{y_1}} y_2^{i_{y_2}} \\ & \cdot f'_{dMSBs3}(x_1, x_2, y_1, y_2) X_1^{m-1-i_{x_1}} X_2^{m-1-i_{x_2}} Y_1^{m-1+t-i_{y_1}} Y_2^{m-1+t-i_{y_2}} \\ & \text{for } x_1^{i_{x_1}} x_2^{i_{x_2}} y_1^{i_{y_1}} y_2^{i_{y_2}} \in S_{d3}, \\ g'_{dMSBs3} :\ & x_1^{i_{x_1}} x_2^{i_{x_2}} y_1^{i_{y_1}} y_2^{i_{y_2}} \cdot R_{d3} \quad \text{for } x_1^{i_{x_1}} x_2^{i_{x_2}} y_1^{i_{y_1}} y_2^{i_{y_2}} \in M_{d3} \backslash S_{d3}, \end{aligned}$$

for

$$\begin{aligned} S_{d3} := & \bigcup_{0 \le j_1, j_2 \le t} \{x_1^{i_{x_1}} x_2^{i_{x_2}} y_1^{i_{y_1}+j_1} y_2^{i_{y_2}+j_2} | \ x_1^{i_{x_1}} x_2^{i_{x_2}} y_1^{i_{y_1}} y_2^{i_{y_2}} \text{ is a monomial of} \\ & f'_{dMSBs3}(x_1, x_2, y_1, y_2)^{m-1}\}, \\ M_{d3} := & \{\text{monomials of } x_1^{i_{x_1}} x_2^{i_{x_2}} y_1^{i_{y_1}} y_2^{i_{y_2}} \cdot f'_{dMSBs3}(x_1, x_2, y_1, y_2) | \\ & x_1^{i_{x_1}} x_2^{i_{x_2}} y_1^{i_{y_1}} y_2^{i_{y_2}} \in S_{d3}\}. \end{aligned}$$

By definition, the index sets become

$$\begin{aligned} S_{d3} \Leftrightarrow & i_{x_1} = 0, 1, \ldots, m-1-i_{y_1}; i_{x_2} =; 0, 1, \ldots, m-1-i_{y_2}; \\ & i_{y_1} = 0, 1, \ldots, m-1+t; i_{y_2} = 0, 1, \ldots, m-1+t, \\ M_{d3} \Leftrightarrow & i_{x_1} = 0, 1, \ldots, m-i_{y_1}; i_{x_2} =; 0, 1, \ldots, m-i_{y_2}; i_{y_1} = 0, 1, \ldots, m+t; \\ & i_{y_2} = 0, 1, \ldots, m+t. \end{aligned}$$

Shift-polynomials g_{dMSBs3} and g'_{dMSBs3} modulo R_{d3} have the roots $(x_1, x_2, y_1, y_2) = (d_{p_1}, d_{q_1}, \ell_p, \ell_q)$ which are the same as $f_{dMSBs}(x_1, x_2, y_1, y_2)$. We construct a lattice with coefficient vectors of $g_{dMSBs3}(x_1 X_1, x_2 X_2, y_1 Y_1, y_2 Y_2)$ and $g'_{dMSBs3}(x_1 X_1, x_2 X_2, y_1 Y_1, y_2 Y_2)$ as the bases. Based on the Jochemsz-May strategy [JM06], LLL outputs three short lattice vectors which satisfy Howgrave-Graham's Lemma when

$$\begin{aligned} & (X_1 X_2)^{\left(\frac{3}{2}\tau^2 + \frac{5}{3}\tau + \frac{5}{12}\right)m^4 + o(m^4)} (Y_1 Y_2)^{\left(\tau^2 + \frac{9}{4}\tau^2 + \frac{5}{3}\tau + \frac{5}{12}\right)m^4 + o(m^4)} \\ & < W_{dMSBs}^{\left(\tau^2 + \tau + \frac{1}{4}\right)m^4 + o(m^4)}. \end{aligned}$$

Ignoring low order terms of m, the condition becomes

$$\begin{aligned} & \delta \cdot 2 \cdot \left(\frac{3}{2}\tau^2 + \frac{5}{3}\tau + \frac{5}{12}\right) + \left(\alpha + \beta - \frac{1}{2}\right) \cdot 2 \cdot \left(\tau^2 + \frac{9}{4}\tau^2 + \frac{5}{3}\tau + \frac{5}{12}\right) \\ & < 2(\alpha + \beta) \cdot \left(\tau^2 + \tau + \frac{1}{4}\right), \end{aligned}$$

that is,

$$\delta < \frac{(12 - 24(\alpha+\beta))\tau^3 + (27 - 30(\alpha+\beta))\tau^2 + (20 - 16(\alpha+\beta))\tau + 5 - 4(\alpha+\beta)}{36\tau^2 + 40\tau + 10}.$$

The condition becomes the third condition of Theorem 7.

Double LSBs Partial Key Exposure Attack on CRT-RSA. As above, we can obtain the following equation

$$e^2 d_p d_q + e d_p(\ell_q - 1) + e d_q(\ell_p - 1) - (N-1)\ell_p\ell_q - (\ell_p + \ell_q - 1) = 0,$$

from CRT-RSA key generations. For a double LSBs partial key exposure attack on CRT-RSA, we obtain

$$\begin{aligned} &e^2(d_{p_1}M + d_{p_0})(d_{q_1}M + d_{q_0}) + e(d_{p_1}M + d_{p_0})(\ell_q - 1) \\ &+e(d_{q_1}M + d_{q_0})(\ell_p - 1) - (N-1)\ell_p\ell_q - (\ell_p + \ell_q - 1) = 0. \end{aligned}$$

We consider a polynomial over the integers,

$$\begin{aligned} f_{dLSBs}(x_1, x_2, y_1, y_2) = e^2M^2x_1x_2 + (e^2d_{q_0} - e)Mx_1 + (e^2d_{p_0} - e)Mx_2 \\ +eMx_1y_2 + eMx_2y_1 + (ed_{q_0} - 1)y_1 + (ed_{p_0} - 1)y_2 \\ -(N-1)y_1y_2 + c_{dLSBs}, \end{aligned}$$

where $c_{dLSBs} = e^2 d_{p_0} d_{q_0} - e d_{p_0} - e d_{q_0} + 1$ whose roots are $(x_1, x_2, y_1, y_2) = (d_{p_1}, d_{q_1}, \ell_p, \ell_q)$. Sizes of the roots are bounded by $X_1 := N^\delta, X_2 := N^\delta, Y_1 := N^{\alpha+\beta-1/2}, Y_2 := N^{\alpha+\beta-1/2}$.

We set an integer $W_{dLSBs} := N^{2(\alpha+\beta)}$ since $\|f_{dLSBs}(x_1, x_2, y_1, y_2)\|_\infty \geq |e^2M^2x_1x_2| \approx N^{2(\alpha+\beta)}$. The polynomial $f_{dLSBs}(x_1, x_2, y_1, y_2)$ has the same Newton polygon as $f_{dMSBs}(x_1, x_2, y_1, y_2)$, and the integers W_{dMSBs} and W_{dLSBs} are the same sizes. Therefore, we use the same lattice construction as above and obtain the condition of Theorem 7.

Acknowledgement. We would like to thank members of the study group "Shin-Akarui-Angou-Benkyou-Kai" for their helpful comments. The first author is supported by a JSPS Fellowship for Young Scientists. This research was supported by CREST, JST and JSPS KAKENHI Grant Number 25280001.

References

[Aon09] 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)

[BM06] Bleichenbacher, D., May, A.: New attacks on RSA with small secret CRT-exponents. In: Yung, M., Dodis, Y., Kiayias, A., Malkin, T. (eds.) PKC 2006. LNCS, vol. 3958, pp. 1–13. Springer, Heidelberg (2006)

[BM03] 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)

[BDL97] Boneh, D., DeMillo, R.A., Lipton, R.J.: On the importance of checking cryptographic protocols for faults. J. Cryptol. **10**(4), 233–260 (1997)

[BD00] 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)

[BDF98] 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)

[Cop95] Coppersmith, D.: Factoring with a hint. IBM Research Report RC 19905 (1995)

[Cop96a] 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)

[Cop96b] Coppersmith, D.: Finding a small root of a bivariate integer equation; factoring with high bits known. In: Maurer, U.M. (ed.) EUROCRYPT 1996. LNCS, vol. 1070, pp. 178–189. Springer, Heidelberg (1996)

[Cop97] Coppersmith, D.: Small solutions to polynomial equations, and low exponent RSA vulnerabilities. J. Cryptol. **10**(4), 233–260 (1997)

[Cop01] 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)

[Cor04] Coron, J.-S.: Finding small roots of bivariate integer polynomial equations revisited. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 492–505. Springer, Heidelberg (2004)

[Cor07] Coron, J.-S.: Finding small roots of bivariate integer polynomial equations: a direct approach. In: Menezes, A. (ed.) CRYPTO 2007. LNCS, vol. 4622, pp. 379–394. Springer, Heidelberg (2007)

[DN00] Durfee, G., Nguyên, P.Q.: Cryptanalysis of the RSA schemes with short secret exponent from Asiacrypt 1999. In: Okamoto, T. (ed.) ASIACRYPT 2000. LNCS, vol. 1976, pp. 14–29. Springer, Heidelberg (2000)

[EJMW05] 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)

[GHM05] Galbraith, S.D., Heneghan, C., McKee, J.F.: Tunable balancing of RSA. In: Boyd, C., González Nieto, J.M. (eds.) ACISP 2005. LNCS, vol. 3574, pp. 280–292. Springer, Heidelberg (2005)

[HM10] Herrmann, M., May, A.: Maximizing small root bounds by linearization and applications to small secret exponent RSA. In: Nguyen, P.Q., Pointcheval, D. (eds.) PKC 2010. LNCS, vol. 6056, pp. 53–69. Springer, Heidelberg (2010)

[How97] 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)

[JM06] Jochemsz, E., May, A.: A strategy for finding roots of multivariate polynomials with new applications in attacking RSA variants. In: Lai, X., Chen, K. (eds.) ASIACRYPT 2006. LNCS, vol. 4284, pp. 267–282. Springer, Heidelberg (2006)

[JM07] Jochemsz, E., May, A.: A polynomial time attack on RSA with private CRT-exponents smaller than $N^{0.073}$. In: Menezes, A. (ed.) CRYPTO 2007. LNCS, vol. 4622, pp. 395–411. Springer, Heidelberg (2007)

[JL12] 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)

[LLL82] Lenstra, A.K. Lenstra Jr., H.W., Lovász, L.: Factoring polynomials with rational coefficients. Math. Ann. **261**, 515–534 (1982)

[LZL14] Lu, Y., Zhang, R., Lin, D.: New partial key exposure attacks on CRT-RSA with large public exponents. In: Boureanu, I., Owesarski, P., Vaudenay, S. (eds.) ACNS 2014. LNCS, vol. 8479, pp. 151–162. Springer, Heidelberg (2014)

[May02] May, A.: Cryptanalysis of unbalanced RSA with small CRT-exponent. In: Yung, M. (ed.) CRYPTO 2002. LNCS, vol. 2442, pp. 242–256. Springer, Heidelberg (2002)

[May03] May, A.: New RSA vulnerabilities using lattice reduction methods. Ph.D. thesis, University of Paderborn (2003)

[May10] May, A.: Using LLL-reduction for solving RSA and factorization problems: a survey. http://www.cits.rub.de/permonen/may.html (2010)

[NS01] 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)

[QC82] Quisquater, J.J., Couvreur, C.: Fast decipherment algorithm for RSA public-key cryptosystems. Electron. Lett. **18**, 905–907 (1982)

[RS86] Rivest, R.L., Shamir, A.: Efficient factoring based on partial information. In: Pichler, F. (ed.) EUROCRYPT 1985. LNCS, vol. 219, pp. 31–34. Springer, Heidelberg (1986)

[RSA78] Rivest, R.L., Shamir, A., Adleman, L.M.: A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM **21**(2), 120–126 (1978)

[SGM10] 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)

[SM09] Sarkar, S., Maitra, S.: Partial key exposure attack on CRT-RSA. In: Abdalla, M., Pointcheval, D., Fouque, P.-A., Vergnaud, D. (eds.) ACNS 2009. LNCS, vol. 5536, pp. 473–484. Springer, Heidelberg (2009)

[TK14] 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)

[Wie90] Wiener, M.J.: Cryptanalysis of short RSA secret exponents. IEEE Trans. Inf. Theory **36**(3), 553–558 (1990)