A Tool Kit for Partial Key Exposure Attacks on RSA*

†Atsushi Takayasu and ‡Noboru Kunihiro

November 10, 2016

Abstract

Thus far, *partial key exposure attacks on RSA* have been intensively studied using lattice based Coppersmith's methods. In the context, attackers are given partial information of a *secret exponent* and *prime factors* of *(Multi-Prime) RSA* where the partial information is exposed in various ways. Although these attack scenarios are worth studying, there are several known attacks whose constructions have similar flavor. In this paper, we try to formulate general attack scenarios to capture several existing ones and propose attacks for the scenarios. Our attacks contain all the state-of-the-art partial key exposure attacks, e.g., due to Ernst et al. (Eurocrypt'05) and Takayasu-Kunihiro (SAC'14, ICISC'14), as special cases. As a result, our attacks offer better results than previous best attacks in some special cases, e.g., Sarkar-Maitra's partial key exposure attacks on RSA with the most significant bits of a prime factor (ICISC'08) and Hinek's partial key exposure attacks on Multi-Prime RSA (J. Math. Cryptology '08). We claim that our contribution is not only generalizations or improvements of the existing results. Since our attacks capture general exposure scenarios, the results can be used as a tool kit; the security of some future variants of RSA can be examined without any knowledge of Coppersmith's methods.

*This research was supported by JSPS Grant-in-Aid for JSPS Fellows 14J08237, CREST, JST, and KAKENHI Grant Number 25280001 and 16H02780.

†The University of Tokyo. The author is supported by a JSPS Fellowship for Young Scientists. e-mail: a-takayasu@it.k.u-tokyo.ac.jp

‡The University of Tokyo.

1 Introduction

Background. Let $N = pq$ be a public RSA modulus where p and q are distinct prime factors with the same bit-size. A public/secret exponent e and d such that $ed = 1 \pmod{\Phi(N)}$ where $\Phi(N)$ is Euler's totient function. There is a variant of RSA called Multi-Prime RSA that have a public modulus $N = \prod_{i=1}^{r} p_i$ where p_i's are all distinct primes with the same bit-size. A public/secret exponent of Multi-Prime RSA satisfies the same equation as the standard RSA. Multi-Prime RSA offers faster decryption/signing by combining with Chinese Remainder Theorem.

From the invention of RSA cryptosystems, hardness of the factorization/RSA problem have been intensively studied. One well known approach in the literature is lattice based Coppersmith's methods [Cop96a, Cop96b]. The method showed an RSA modulus $N = pq$ can be factorized in polynomial time with half the most significant bits of a prime factor. Although Coppersmith's methods requires involved technical analyses, the method has revealed the vulnerability of RSA in many papers. One of the most famous result is Boneh and Durfee's small secret exponent attack on RSA [BD00] that factorizes an RSA modulus N in polynomial time when $d < N^{1-1/\sqrt{2}} = N^{0.292\cdots}$. Ciet et al. [CKLQ02] extended the attack for Multi-Prime RSA and their attack works when $d < N^{1-\sqrt{1-1/r}}$.

Boneh, Durfee, and Frankel [BDF98] proposed several attacks on RSA called *partial key exposure attacks* that make use of the most/least significant bits (MSBs/LSBs) of d. Afterwards, the research becomes a hot topic and numerous papers have been published. Although the original attacks [BDF98] work only for a small e, several improvements [BM03, EJMdW05, SSM10, TK14d] have been proposed using Coppersmith's methods [Cop96a, Cop96b]. In particular, Ernst et al. [EJMdW05] revealed that RSA becomes vulnerable even for a full size e and Takayasu-Kunihiro's attacks [TK14d] contain Boneh-Durfee's small secret exponent attack [BD00] as a special case. Besides these results, numerous papers have studied partial key exposure attacks for various attack scenarios; attacks on Multi-Prime RSA with the MSBs/LSBs of d [Hin08], attacks on RSA with the MSBs of a prime factor [SMS08], attacks on RSA with the MSBs/LSBs of d and the MSBs of a prime factor [SM08], attacks on RSA where the prime factors share the same LSBs [SWS$^+$08], attacks on RSA where the prime factors are almost the same sizes [dW02], attacks on Multi-Prime RSA where all the prime factors are almost the same sizes [TK14c, ZT13, ZT14], and more.

Indeed, there are many papers that study partial key exposure attacks on RSA. However, the situation does not immediately mean that the problem is worth studying in such many papers. Among the above variants of the attack, some papers capture almost the same attack scenarios. Hence, essentially the same algorithms have been proposed in several papers. We do not think the situation is not desirable for the development of the cryptographic research.

Our Contributions. To resolve the situation, we define a general partial key exposure scenario. For the purpose, we classify some existing works with respect to three properties; attackers know partial information of a *secret exponent* and *prime factors* for *Multi-Prime RSA*. Since there are no results that capture the three properties simultaneously, we define a general attack scenario as follows.

Definition 1 ($(\alpha, \beta, \gamma, \delta)$-Partial Key Exposure Attacks on RSA)**.** *Let $N = \prod_{i=1}^{r} p_i$ where all $p_1, \ldots, p_r$ are distinct primes of the same bit-size. Let $e = N^{\alpha}$ and $d = N^{\beta}$ such that $ed = 1$*

mod $\Phi(N)$. *Given* $(N, e, \tilde{d}, \tilde{\Phi}(N))$ *where* $\tilde{d} \geq N^{\beta-\gamma}$ *is the MSBs/LSBs of* d *and* $|\Phi(N) - \tilde{\Phi}(N)| \leq N^{\delta}$*, the goal of the problem is to compute* $\Phi(N)$*.*

We parametrize the problem with respect to $(\alpha, \beta, \gamma, \delta)$. Notice that the number of prime factors r is independent of the hardness of the problem. Although partial information of prime factors in previous works are defined in various ways, the above definition captures several exposure scenarios simultaneously. For example, let us focus on an attack on RSA with the most significant bits prime factors and an attack on Multi-Prime RSA. Given $\tilde{p}$ which is the $\delta' \log N$ MSBs of an RSA prime factor p, then we regard $\tilde{\Phi}(N) = N - \tilde{p}N^{1/2-\delta'} - \lfloor N/\tilde{p}N^{1/2-\delta'} \rfloor$ and an attack on RSA with the most significant bits of prime factors is captured by $\delta = 1/2 - \delta'$ since $|\Phi(N) - \tilde{\Phi}(N)|$ is bounded above by $N^{1/2-\delta'}$ within a constant factor [SM08, SMS08]. Similarly, we regard $\tilde{\Phi}(N) = N$ and an attack on Multi-Prime RSA is captured by $\delta = 1 - 1/r$ since $|\Phi(N) - N|$ is bounded above by $N^{1-1/r}$ within a constant factor [Hin08]. Since we analyze all $0 \leq \gamma \leq \beta$ and $0 \leq \delta \leq 1$, our definition covers several existing works simultaneously. Moreover, the definition will cover other unknown variants that will be studied in the future. Then our results can be viewed as a *tool kit* to study partial key exposure attacks as [BM05]. It means that our results enable even beginners of Coppersmith's methods to examine the security of such future variants without understanding the technical detail of this paper.

We use lattice based Coppersmith's methods to solve integer/modular equations as previous works and obtain the following results.

Theorem 1. *Given the MSBs/LSBs of* d*, there are polynomial time algorithms to solve* $(\alpha, \beta, \gamma, \delta)$*-Partial Key Exposure Attacks on RSA when*

- $\gamma < \frac{3-\delta-2\sqrt{\delta^2+3(\alpha+\beta-1)\delta}}{3}$.

Theorem 2. *Given the MSBs of* d*, there are polynomial time algorithms to solve* $(1, \beta, \gamma, \delta)$*-Partial Key Exposure Attacks on RSA when*

1. $\gamma < 1 - \frac{2}{3}\left(\delta + \sqrt{\delta(4\delta - 3 + 6\beta)}\right)$ *for* $\beta < 1 - \delta - \sqrt{\frac{\delta(1-\delta)}{3}}$,
2. $\gamma < \frac{1+\beta-\sqrt{4\delta-3(1-\beta)^2}}{2}$ *for* $1 - \delta - \sqrt{\frac{\delta(1-\delta)}{3}} \leq \beta < 1 - \delta$ *and* $1/3 \leq \delta$*, and for* $1 - \delta - \sqrt{\frac{\delta(1-\delta)}{3}} \leq \beta < 1 - \sqrt{\frac{\delta}{3}}$ *and* $\delta < 1/3$,
3. $3\lambda\tau - 3(1-\delta)\tau^2 + \tau^3 < \frac{(\delta\tau-\beta+\lambda)^3}{\delta(1+\lambda-2\beta)}$ *where* $\lambda = \max\{\gamma, \beta + \delta - 1\}$ *and* $\tau = 1 - \frac{\beta+\delta-1}{\delta-\sqrt{1+\lambda-2\beta}}$ *for* $1 - \delta \leq \beta < \frac{3(1-\delta)(1+\delta)}{4}$ *and* $1/3 \leq \delta < 2/3$*, and for* $1 - \delta \leq \beta < \delta - \frac{(2\delta-1)^2}{\delta^2}$ *and* $2/3 \leq \delta$,
4. $\gamma \leq \frac{3(1-\delta)^2}{4}$ *for* $\frac{3(1-\delta)(1+\delta)}{4} \leq \beta < \frac{3(1-\delta)^2+4(1-\delta)}{4}$ *and* $1/3 \leq \delta < 2/3$,
5. $\gamma < \frac{2+\beta-2\delta-2\sqrt{(\beta+\delta-1)(\beta+4\delta-1)}}{3}$ *for* $\frac{3(1-\delta)^2+4(1-\delta)}{4} \leq \beta$ *and* $1/3 \leq \delta$,
6. $\gamma \leq 1 - \frac{2\sqrt{3\delta}}{3}$ *for* $1 - \sqrt{\frac{\delta}{3}} \leq \beta$ *and* $\delta < 1/3$.

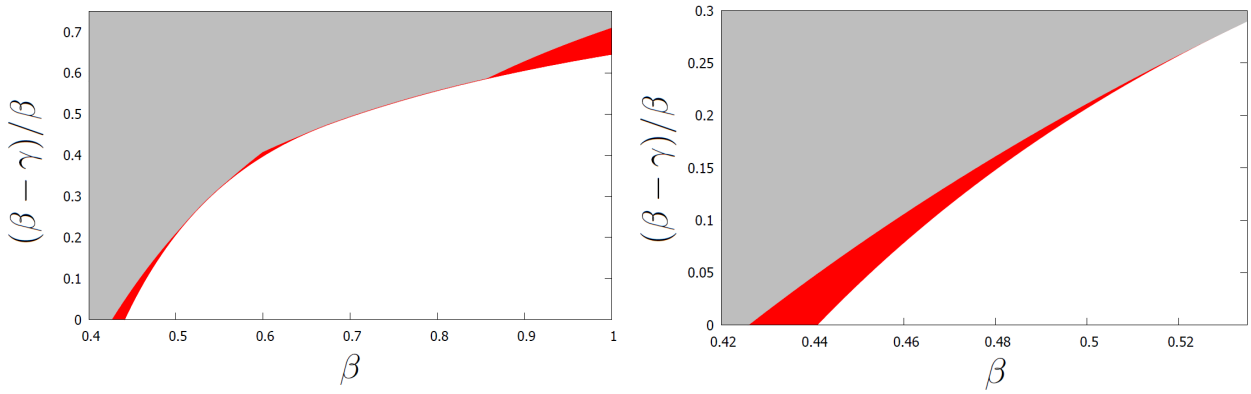

Figure 1: Comparisons of partial key exposure attacks on RSA with the $\approx \frac{3}{16}\log N$ MSBs of p, i.e., $(1,\beta,\gamma,5/16)$-partial key exposure attacks. We compare how much portions of d should be exposed for β between Sarkar and Maitra's attack (gray areas) [SM08] and our Theorem 2 and 3 (red areas). The left (resp. right) figure represents the attack with the MSBs (resp. LSBs).

Theorem 3. *Given the LSBs of d, there are polynomial time algorithms to solve $(1,\beta,\gamma,\delta)$-Partial Key Exposure Attacks on RSA when*

1. $\gamma < 1 - \frac{2}{3}\left(\delta + \sqrt{\delta(4\delta - 3 + 6\beta)}\right)$ *for* $\beta < 1 - \delta - \sqrt{\frac{\delta(1-\delta)}{3}}$,
2. $\gamma < \frac{1+\beta-\sqrt{4\delta-3(1-\beta)^2}}{2}$ *for* $1 - \delta - \sqrt{\frac{\delta(1-\delta)}{3}} \le \beta < 1 - \frac{\delta}{2} - \frac{\sqrt{3\delta(4-\delta)}}{6}$,
3. $\gamma < 1 - \frac{\delta+2\sqrt{\delta(\delta+3\beta)}}{3}$ *for* $1 - \frac{\delta}{2} - \frac{\sqrt{3\delta(4-\delta)}}{6} \le \beta$.

First of all, our results cover all the known best attacks as special cases, e.g., Theorem 1, the conditions 4–6 of Theorem 2, and the condition 3 of Theorem 3 for $\delta = 1/2$ are the same as Ernst et al.'s attack [EJMdW05]. Extensions of previous works are not trivial at all. In the context of the algorithm construction of Coppersmith's methods, to tackle the equations with the more monomials requires the more involved analyses. Hence, to extend some attacks with more partial information and the extended attacks completely cover the original ones as special cases is challenging in some cases. For example, Ernst et al.'s $(1,\beta,\gamma,1/2)$-partial key exposure attack [EJMdW05] for $\gamma = \beta$ do not cover Boneh and Durfee's $(1,\beta,\beta,1/2)$-partial key exposure attack [BD00]. It takes about ten years until the desired attacks [TK14d] were proposed. Indeed, in this paper, we have to analyze eight attacks to obtain the best results for all the cases.

Furthermore, our results offer improved attacks in some special cases. More concretely, we improve Sarkar and Maitra's partial key exposure attacks on RSA with partial information of prime factors [SM08] for small d and Hinek's partial key exposure attacks on Multi-Prime RSA [Hin08]. See Figures 1 and 2 for detailed comparisons. Indeed, our attacks require smaller portions of partial information of d than their attacks.

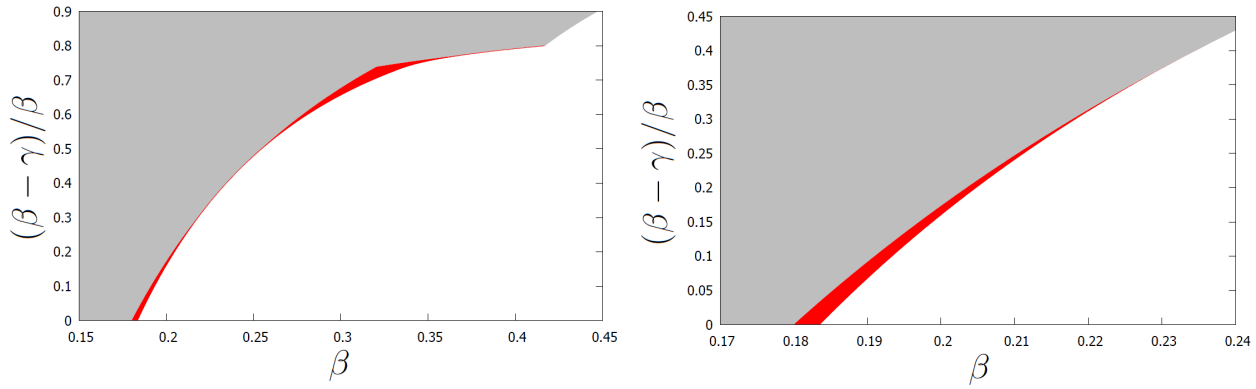

Figure 2: Comparisons of partial key exposure attacks on Multi-Prime RSA for the number of prime factors $r = 3$, i.e., $(1, \beta, \gamma, 2/3)$-partial key exposure attacks. We compare how much portions of d should be exposed for β between Hinek's attack (gray areas) [Hin08] and our Theorem 2 and 3 (red areas). The left (resp. right) figure represents the attack with the MSBs (resp. LSBs).

Technical Overview. To provide better attacks based on Coppersmith's methods is equivalent to provide better lattice constructions to solve the underlying equations. There is a well-known strategy for the construction due to Jochemsz and May [JM06]. The construction may be simple and easy to understand even for beginners of the research area. Ernst et al. [EJMdW05] made use of the strategy for their attacks. Sarkar-Maitra [SM08], Hinek [Hin08], and some other papers extended the attack of Ernst et al. Then, we also follow the strategy and propose extended attacks in Section 3; Theorem 1, the conditions 4–6 of Theorem 2, and the condition 3 of Theorem 3. The results based on the strategy are almost naive extensions of the previous attacks although there are some improved analyses in our results; the condition 6 of Theorem 2 in Section 3.3 improves Sarkar-Maitra's attack.

Notice that the Jochemsz-May strategy does not always offer the best attacks and lattice constructions that outperform the strategy require involved analyses. For example, Boneh and Durfee's small secret exponent attack [BD00]; $(1, \beta, \beta, 1/2)$-partial key exposure attack, does not seem to be captured by the strategy. To construct better attacks, we make use of Takayasu and Kunihiro's attacks [TK14c, TK14d] where the attack in [TK14c] and [TK14d] solved $(1, \beta, \beta, \delta)$-partial key exposure attacks for $0 \leq \delta \leq 1$ and $(1, \beta, \gamma, 1/2)$-partial key exposure attacks for $0 \leq \gamma \leq \beta$, respectively. Technically, the former and the latter attack constructs a better lattice with respect to the value of δ and γ, respectively. Moreover, they are the only existing partial key exposure attacks that outperform the Jochemsz-May strategy [JM06] except the Boneh-Durfee attack and its straightforward extension. As we suggested above, these lattice constructions [TK14c, TK14d] seem to be technically hard to follow. Indeed, there are only a few papers [TK16a, TK16c] that make use of these results to obtain better results. In this paper, we fully exploit the spirit of the lattice constructions [TK14c, TK14d] and propose $(1, \beta, \gamma, \delta)$-partial key exposure attacks for arbitrary $0 \leq \gamma \leq \beta$ and $0 \leq \delta \leq 1$. Our attacks cover Takayasu and Kunihiro's attacks [TK14c, TK14d] for a fixed $\gamma = \beta$ and $\delta = 1/2$, respectively. We study the attacks with the MSBs and LSBs of d in

Section 4 and 5, respectively.

2 Preliminaries

In this section, we briefly introduce some basic notions of Coppersmith's methods. For more detailed information, see [Cop97, Cop01, May10, NS01].

Let $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n \in \mathbb{Z}^{n'}$ be linearly independent n'-dimensional vectors. All vectors are row representations. A lattice $L(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n)$ spanned by the basis vectors $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$ is defined as $L(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n) = \{\sum_{j=1}^{n} c_j \boldsymbol{b}_j : c_j \in \mathbb{Z}\}$. We also use matrix representations $\boldsymbol{B} \in \mathbb{Z}^{n \times n'}$ for the bases where each row corresponds to basis vectors $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$. Then, a lattice spanned by the basis matrix $\boldsymbol{B}$ is defined as $L(\boldsymbol{B}) = \{\boldsymbol{c}\boldsymbol{B} : \boldsymbol{c} \in \mathbb{Z}^n\}$. We call n a rank of the lattice, and n' a dimension of the lattice. We call the lattice full-rank when $n = n'$. We define a determinant of a lattice $\det(L(\boldsymbol{B}))$ as $\det(L(\boldsymbol{B})) = \sqrt{\det(\boldsymbol{B}\boldsymbol{B}^T)}$ where $\boldsymbol{B}^T$ is a traspose of $\boldsymbol{B}$. By definition, a determinant of a full-rank lattice can be computed as $\det(L(\boldsymbol{B})) = |\det(\boldsymbol{B})|$. Moreover, a determinant of a triangular matrix can be easily computed as the product of all diagonals.

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

Propostition 1 (LLL algorithm [LLL82, May03])**.** *Given a matrix $\boldsymbol{B} \in \mathbb{Z}^{n \times n'}$, the LLL algorithm finds vectors $\boldsymbol{b}'_1$ and $\boldsymbol{b}'_2$ in a lattice $L(\boldsymbol{B})$. Euclidean norms of the vectors are bounded by*

$$\|\boldsymbol{b}'_1\| \leq 2^{(n-1)/4}(\det(L(\boldsymbol{B})))^{1/n} \text{ and } \|\boldsymbol{b}'_2\| \leq 2^{n/2}(\det(L(\boldsymbol{B})))^{1/(n-1)}.$$

The running time is polynomial time in n, n', and input length.

Although the outputs of the LLL algorithm are not the shortest lattice vectors in general, the fact is not the matter in the context of Coppersmith's methods.

Instead of original Coppersmith's methods, we introduce Howgrave-Graham's reformulation to solve modular equations [How97] and Coron's reformulation to solve integer equations [Cor04]. Although Coron's method [Cor04] is less efficient than original Coppersmith's method [Cop96a] and Coron's other method [Cor07], it is simpler to analyze than the other methods.

For a k-variate polynomial $h(x_1, \ldots, x_k) = \sum h_{i_1,\ldots,i_k} x_1^{i_1} \cdots x_k^{i_k}$, we define a norm of a polynomial $\|h(x_1, \ldots, x_k)\| = \sqrt{\sum h_{i_1,\ldots,i_k}^2}$ and $\|h(x_1, \ldots, x_k)\|_\infty = \max_{i_1,\ldots,i_k} |h_{i_1,\ldots,i_k}|$. At first, we show a modular method since an integer method makes use of the modular method. Coppersmith's method can find solutions $(\tilde{x}_1, \tilde{x}_2)$ of a bivariate modular equation $h(x_1, x_2) = 0 \pmod{e}$ when $|\tilde{x}_1| < X_1, |\tilde{x}_2| < X_2$, and $X_1 X_2$ is reasonably smaller than e. In general, the simpler the Newton polygon of the polynomial is, the larger solutions can be recovered. Let m be a positive integer. We construct n polynomials $h_1(x_1, x_2), \ldots, h_n(x_1, x_2)$ that have the root $(\tilde{x}_1, \tilde{x}_2)$ modulo e^m. Then, we construct a matrix $\boldsymbol{B}$ whose rows consist of coefficients of $h_1(x_1 X_1, x_2 X_2), \ldots, h_n(x_1 X_1, x_2 X_2)$. Applying the LLL algorithm to $\boldsymbol{B}$ and we obtain two short vectors $\boldsymbol{b}'_1$ and $\boldsymbol{b}'_2$, and their corresponding polynomials $h'(x_1, x_2)$ and $h'_2(x_1, x_2)$. If norms of these polynomials are small, they have the root $(\tilde{x}_1, \tilde{x}_2)$ over the integers. The fact comes from the following lemma due to Howgrave-Graham [How97].

Lemma 1 ([How97]). *Let $h(x_1, \ldots, x_k) \in \mathbb{Z}[x_1, \ldots, x_k]$ be a polynomial over the integers that consists of at most n monomials. Let $X_1, \ldots, X_k$, and R be positive integers. If the polynomial $h(x_1, \ldots, x_k)$ satisfies the following two conditions:*

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.

Therefore, if $h'(x_1, x_2)$ and $h'_2(x_1, x_2)$ satisfy Lemma 1, we can compute Gröbner bases or a resultant of them and easily recover $(\tilde{x}_1, \tilde{x}_2)$. By making use of the unravelled linearization, we only analyze triangular matrices in this paper. Better lattice constructions for triangular matrices are well analyzed [May10, TK14a] by introducing helpful polynomials. Intuitively, polynomials in lattice bases are called helpful when their diagonals in the triangular basis matrices are smaller than the modulus of the equations e^m. To solve modular equations for larger roots, as many (resp. less) helpful (resp. unhelpful) polynomials as possible should be selected as long as the basis matrices are triangular. We follow the definition from [TK14d] as follows.

Definition 2 (Helpful Polynomials). *To solve equations modulo e, consider a basis matrix $\boldsymbol{B}$. We add a new shift-polynomial $h_{[i',j']}(x, y)$ and construct a new basis matrix $\boldsymbol{B}^+$. We call $h_{[i',j']}(x, y)$ a helpful polynomial, provided that $\det(\boldsymbol{B}^+)/\det(\boldsymbol{B}) \leq e^m$. Conversely, if the inequality does not hold, we call $h_{[i',j']}(x, y)$ an unhelpful polynomial.*

Next, we show an integer method. Coppersmith's method can find solutions $(\tilde{x}_1, \tilde{x}_2, \tilde{x}_3)$ of a trivariate integer equation $h(x_1, x_2, x_3) = 0$ when $|\tilde{x}_1| < X_1, |\tilde{x}_2| < X_2, |\tilde{x}_3| < X_3$, and $X_1X_2X_3$ is reasonably smaller than $\|h(x_1X_1, x_2X_2, x_3X_3)\|_\infty$. Although we omit details of the method, we set a reasonable integer R and remaining procedures are almost the same as modular case by solving a modular equation $h(x_1, x_2, x_3) = 0 \mod R$. New polynomials $h'(x_1, x_2, x_3)$ and $h'_2(x_1, x_2, x_3)$ obtained by outputs of the LLL algorithm are provably algebraically independent of $h(x_1, x_2, x_3)$. See [Cor04] for the detail. To the best of our knowledge, there are no algorithms to solve integer equations known that outperform the algorithm based on the Jochemsz-May strategy [JM06]. Hence, we follow the strategy. Let l_j denote the largest exponent of x_j in the polynomial $h(x_1, \ldots, x_k) = \sum h_{i_1,\ldots,i_k} x_1^{i_1} \cdots x_k^{i_k}$. We set an (possibly large) integer W such that $W \leq \|h(x_1, \ldots, x_k)\|_\infty$ and an integer $R := WX_1^{l_1(m-1)+t} \prod_{u=2}^{k} X_j^{l_u(m-1)}$ with some positive integers m and $t = O(m)$ such that $\gcd(R, h_{0,\ldots,0}) = 1$. We compute $c = h_{0,\ldots,0}^{-1} \pmod R$ and $h'(x_1, \ldots, x_k) := c \cdot h(x_1, \ldots, x_k) \pmod R$. We define shift-polynomials g and g' as

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

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

for sets of monomials

$$S := \bigcup_{0 \leq j \leq t} \{x_1^{i_1+j} \cdots x_k^{i_k} | x_1^{i_1} \cdots x_k^{i_k} \text{ is a monomial of } h(x_1, \ldots, x_k)^{m-1}\},$$

$$M := \{\text{monomials of } x_1^{i_1} \cdots x_k^{i_k} \cdot h(x_1, \ldots, x_k) \text{ for } x_1^{i_1} \cdots x_k^{i_k} \in S\}.$$

All these shift-polynomials g and g' modulo R have the root $(\tilde{x}_1, \ldots, \tilde{x}_k)$ that is the same as $h(x_1, \ldots, x_k)$. We construct a lattice with coefficients of $g(x_1X_1, \ldots, x_kX_k)$ and $g'(x_1X_1, \ldots, x_kX_k)$ as the bases. The shift-polynomials generate a triangular basis matrix. Ignoring low order terms of m, LLL outputs short vectors that satisfy Lemma 1 when $\prod_{j=1}^{k} X_j^{s_j} < W^{|S|}$ for $s_j = \sum_{x_1^{i_1} \cdots x_k^{i_k} \in M \setminus S} i_j$. When the condition holds, we can find all the small root. See [JM06] for the detail.

We should note that these methods require heuristic argument. There are no assurance if new polynomials obtained by outputs of the LLL algorithm are algebraically independent. In this paper, we assume that these polynomials are always algebraically independent and resultants of polynomials will not vanish as previous works.

3 Attacks by Solving Integer Equations

In this section, we solve integer equations and propose three attacks, i.e., Attacks 1–3. The Attack 1, 2, and 3 in Section 3.1, 3.2, and 3.3 corresponds to Theorem 1 and the condition 3 of Theorem 3, the conditions 4 and 5 of Theorem 2, and the condition 6 of Theorem 2, respectively. Algorithm constructions in this section are similar to Ernst et al. [EJMdW05].

3.1 The Attack 1

In this section, we consider $(\alpha, \beta, \gamma, \delta)$-partial key exposure attacks with the MSBs/LSBs of d. When $\tilde{d}$ which is the MSBs/LSBs of d is given, RSA key generation can be written as $e(\tilde{d}\tilde{M} + d'M') = 1 + k\Phi(N)$ with some integer k such that $|k| \leq N^{\alpha+\beta-1}$. When $\tilde{d}$ is the MSBs (resp. LSBs), d' denotes the LSBs (resp. MSBs) of d, and $\tilde{M} = 2^{\lfloor \gamma \log N \rfloor}$ and $M' = 1$ (resp. $\tilde{M} = 1$ and $M' = 2^{\lfloor (\beta-\gamma) \log N \rfloor}$). Then, we find the root of the following polynomial over the integers:

$$f_{i1}(x, y, z) = c + eM'x + y(\tilde{\Phi} + z)$$

where $c = 1 - e\tilde{d}\tilde{M}$. If we can recover the root $(x, y, z) = (-d', k, \Phi(N) - \tilde{\Phi}(N))$, whole secret information can be computed. By definition, the absolute values of the root are bounded above by $X := N^{\gamma}, Y := N^{\alpha+\beta-1}, Z := N^{\delta}$. By solving the integer equation based on the Jochemsz-May strategy [JM06], Theorem 1 and the condition 3 of Theorem 3 can be obtained.

We set an (possibly large) integer W such that $W < N^{\alpha+\beta}$ since $\|f_{i1}(xX, yY, zZ)\|_{\infty} \geq \max\{|c|, |eM'X|\} \approx N^{\alpha+\beta}$. Next, we set an integer $R := W(XY)^{m-1} \cdot Z^{m+r-1+t}$ with some integers $m = \omega(r)$ and $t = \tau m$ where $\tau \geq 0$ such that $\gcd(R, c) = 1$. We compute $c' = c^{-1} \mod R$ and $f'_{i1}(x, y, z) := c \cdot f_{i1}(x, y, z) \mod R$. We define shift-polynomials g_{i1} and g'_{i1} as

$$g_{i1} : x^{i_X} y^{i_Y} z^{i_Z} \cdot f'^{1}_{i1} \cdot X^{m-1-i_X} Y^{m-1-i_Y} Z^{m+r-1+t-i_Z} \text{ for } x^{i_X} y^{i_Y} z_1^{i_Z} \in S,$$
$$g'_{i1} : x^{i_X} y^{i_Y} z^{i_Z} \cdot R \quad \text{for } x^{i_X} y^{i_Y} z_1^{i_Z} \in M \setminus S,$$

for sets of monomials

$$S := \bigcup_{0 \le j \le t} \left\{ x^{i_X} y^{i_Y} z^{i_Z+j} \middle| x^{i_X} y^{i_Y} z^{i_Z} \text{ is a monomial of } f_i(x,y,z_1)^{m-1} \right\},$$
$$M := \left\{ x^{i_X} y^{i_Y} z^{i_Z} \middle| \text{ monomials of } x^{i'_X} y^{i'_Y} z^{i'_Z} \cdot f_i(x,y,z) \text{ for } x^{i'_X} y^{i'_Y} z^{i'_Z} \in S \right\}.$$

By definition of sets of monomials S and M, it follows that

$$x^{i_X} y^{i_y} z^{i_Z} \in S \Leftrightarrow \ i_X = 0,1,\ldots,m-1; i_Y = 0,1,\ldots,m-1-i_X; i_Z = 0,1,\ldots,i_Y+t,$$
$$x^{i_X} y^{i_y} z^{i_Z} \in M \Leftrightarrow \ i_X = 0,1,\ldots,m; i_Y = 0,1,\ldots,m-i_X; i_Z = 0,1,\ldots,i_Y+t.$$

All these shift-polynomials g_{i1} and g'_{i1} modulo R have the root $(x,y,z) = (-d', k, \Phi(N) - \tilde{\Phi}(N))$ that is the same as $f_{i1}(x,y,z)$. We build a lattice with these polynomials.

Based on the Jochemsz-May strategy, the integer equation $f_{i1}(x,y,z) = 0$ can be solved when

$$X^{\left(\frac{1}{6}+\frac{\tau}{2}\right)m^3} Y^{\left(\frac{1}{3}+\frac{\tau}{2}\right)m^3} Z^{\left(\frac{1}{6}+\frac{\tau}{2}+\frac{\tau^2}{2}\right)m^3} < W^{\left(\frac{1}{6}+\frac{\tau}{2}\right)m^3}$$
$$\Leftrightarrow \gamma\left(\frac{1}{6}+\frac{\tau}{2}\right) + (\alpha+\beta-1)\left(\frac{1}{3}+\frac{\tau}{2}\right) + \delta\left(\frac{1}{6}+\frac{\tau}{2}+\frac{\tau^2}{2}\right) < (\alpha+\beta)\left(\frac{1}{6}+\frac{\tau}{2}\right).$$

By substituting $\tau = \frac{1-\gamma-\delta}{2\delta}$, the claimed inequality of Theorem 1 can be obtained:

$$\gamma < \frac{3-\delta-2\sqrt{\delta^2+3(\alpha+\beta-1)\delta}}{3}.$$

The condition 3 of Theorem 3 can be obtained by substituting $\alpha = 1$.

3.2 The Attack 2

In this section, we consider $(1,\beta,\gamma,\delta)$-partial key exposure attacks with the MSBs of d. As in Section 3.1, when $\tilde{d}$ which is the MSBs of d is given, RSA key generation can be written as $e(\tilde{d}M + d') = 1 + k\Phi(N)$ with some integer k such that $|k| \le N^\beta$ and $M = 2^{\lfloor \gamma \log N \rfloor}$. In this section, we use an additional information $\tilde{k} = \lfloor (e\tilde{d}-1)/\tilde{\Phi}(N) \rfloor$ which is an approximation to k. From the simple calculation,

$$\begin{aligned}
|\tilde{k}-k| &= \left| \frac{e\tilde{d}M-1}{\tilde{\Phi}(N)} - \frac{ed-1}{\Phi(N)} \right| = \left| \frac{\Phi(N)(e\tilde{d}M-1) - \tilde{\Phi}(N)(ed-1)}{\tilde{\Phi}(N)\Phi(N)} \right| \\
&= \left| \frac{e(\Phi(N)\tilde{d}M - \tilde{\Phi}(N)d) + (\tilde{\Phi}(N)-\Phi(N))}{\tilde{\Phi}(N)\Phi(N)} \right| \\
&= \left| \frac{e\tilde{\Phi}(N)(\tilde{d}M-d) - (\tilde{\Phi}(N)-\Phi(N))(e\tilde{d}M-1)}{\tilde{\Phi}(N)\Phi(N)} \right|
\end{aligned}$$

$$\leq \left|\frac{e(\tilde{d}M-d)}{\Phi(N)}\right| + \left|\frac{(\tilde{\Phi}(N)-\Phi(N))(e\tilde{d}M-1)}{\tilde{\Phi}(N)\Phi(N)}\right|.$$

By definition,

$$\left|\frac{e(\tilde{d}M-d)}{\Phi(N)}\right| \leq N^{\gamma} \quad \text{and} \quad \left|\frac{(\tilde{\Phi}(N)-\Phi(N))(e\tilde{d}M-1)}{\tilde{\Phi}(N)\Phi(N)}\right| \leq N^{\beta+\delta-1}.$$

Therefore, $\tilde{k}$ satisfies the following condition:

$$|\tilde{k}-k| < 2N^{\lambda} \quad \text{where} \quad \lambda = \max\{\gamma, \beta+\delta-1\}.$$

The approximate value enables us to obtain better results for large β. Since Sarkar and Maitra [SM08] used $\lambda = \max\{\gamma, \beta-1/2\}$ for $\delta \leq 1/2$, we improve the bound although the following lattice construction is completely the same. We find the root of the following polynomial over the integers:

$$f_{i2}(x,y,z) = c + ex + (\tilde{k}+y)(\tilde{\Phi}+z),$$

where $c = 1-e\tilde{d}\tilde{M}$ as in Section 3.1. If we can recover the root $(x,y,z) = (-d', k-\tilde{k}, \Phi(N)-\tilde{\Phi}(N))$, whole secret information can be computed. The absolute values of the root are bounded above by $X := N^{\gamma}, Y := N^{\lambda}, Z := N^{\delta}$ where $\lambda = \max\{\gamma, \beta+\delta-1\}$. Although the absolute values of solutions become smaller than those in Section 3.1, the result in this section is not always better since the Newton polygon of the polynomial becomes more complex.

We set an (possibly large) integer W such that $W < N^{1+\lambda}$ since $\|f_{i2}(xX, yY, zZ)\|_{\infty} \geq |\tilde{\Phi}(N)Y| \approx N^{1+\lambda}$. Next, we set an integer $R := WX^{m-1} \cdot Y^{m+r-1+t}Z^{m-1}$ with some integers $m = \omega(r)$ and $t = \tau m$ where $\tau \geq 0$ such that $\gcd(R, c) = 1$. We compute $c' = c^{-1} \mod R$ and $f'_{i2}(x,y,z) := c \cdot f_{i2}(x,y,z) \mod R$. We define shift-polynomials g_{i1} and g'_{i1} as

$$g_{i2} : x^{i_X}y^{i_Y}z^{i_Z} \cdot f'^{2}_{i} \cdot X^{m-1-i_X}Y^{m-1+t-i_Y}Z^{m+r-1-i_Z} \text{ for } x^{i_X}y^{i_Y}z_1^{i_Z} \in S,$$
$$g'_{i2} : x^{i_X}y^{i_Y}z^{i_Z} \cdot R \quad \text{for } x^{i_X}y^{i_Y}z_1^{i_Z} \in M \backslash S,$$

for sets of monomials

$$S := \bigcup_{0 \leq j \leq t} \left\{ x^{i_X}y^{i_Y+j}z^{i_Z} \middle| x^{i_X}y^{i_Y}z^{i_Z} \text{ is a monomial of } f_i(x,y,z_1)^{m-1} \right\},$$
$$M := \left\{ x^{i_X}y^{i_Y}z^{i_Z} \middle| \text{ monomials of } x^{i'_X}y^{i'_Y}z^{i'_Z} \cdot f_i(x,y,z) \text{ for } x^{i'_X}y^{i'_Y}z^{i'_Z} \in S \right\}.$$

By definition of sets of monomials S and M, it follows that

$$x^{i_X}y^{i_y}z^{i_Z} \in S \Leftrightarrow \ i_X = 0,1,\ldots,m-1; i_Y = 0,1,\ldots,m-1+t-i_X; i_Z = 0,1,\ldots,m-1-i_X,$$
$$x^{i_X}y^{i_y}z^{i_Z} \in M \Leftrightarrow \ i_X = 0,1,\ldots,m; i_Y = 0,1,\ldots,m+t-i_X; i_Z = 0,1,\ldots,m-i_X.$$

All these shift-polynomials g_{i2} and g'_{i2} modulo R have the root $(x,y,z) = (-d', k-\tilde{k}, \Phi(N)-\tilde{\Phi}(N))$ that is the same as $f_{i2}(x,y,z)$. We build a lattice with these polynomials.

Based on the Jochemsz-May strategy [JM06], the integer equation $f_{i1}(x,y,z)=0$ can be solved when $X^{(\frac{1}{3}+\frac{\tau}{2})m^3}Y^{\left(\frac{1}{2}+\tau+\frac{\tau^2}{2}\right)m^3}Z^{(\frac{1}{2}+\frac{\tau}{2})m^3} < W^{(\frac{1}{3}+\frac{\tau}{2})m^3}$. By substituting $\tau=\frac{1-\gamma-\delta-\lambda}{2\lambda}$, the conditions 4 and 5 of Theorem 2 can be obtained. To follow the definition $\lambda=\max\{\gamma,\beta+\delta-1\}$, $\lambda=\gamma$ when $\beta<\frac{3(1-\delta)^2+4(1-\delta)}{4}$ and $\lambda=\beta+\delta-1$ otherwise.

3.3 Attack 3

In this section, we propose a better lattice construction than that in Section 3.2. Notice that the Newton polygon of $f_{i2}(x,y,z)$ is symmetric with respect to y and z. Hence, we should add extra shifts for the smaller variable. From the bound of the Attack 2, $Y=N^{\lambda}=N^{3(1-\delta)^2/4}\geq Z=N^{\delta}$ when $\delta<1/3$. Therefore, we add extra shifts for z for such small δ. We construct a lattice that is symmetric with respect to y and z from that in Section 3.2 and the integer equation $f_{i2}(x,y,z)=0$ can be solved when $X^{(\frac{1}{3}+\frac{\tau}{2})m^3}Y^{(\frac{1}{2}+\frac{\tau}{2})m^3}Z^{\left(\frac{1}{2}+\tau+\frac{\tau^2}{2}\right)m^3} < W^{(\frac{1}{3}+\frac{\tau}{2})m^3}$. By substituting $\tau=\frac{1-\lambda-2\delta}{2\delta}$, the condition 6 of Theorem 2 can be obtained. Notice that when $\delta<1/3$, $\beta+\delta-1<\gamma\leq 1-\frac{2\sqrt{3\delta}}{3}$ always hold for $\beta<1$.

4 Attacks with the MSBs of d by Solving Modular Equations

In this section, we solve modular equations and propose three attacks, i.e., Attacks 4–6, for $(1,\beta,\gamma,\delta)$-partial key exposure attacks with the MSBs of d. The Attack 4, 5, and 6 in Section 4.1, 4.2, and 4.3 correspond to the conditions 2, 3, and 1 of Theorem 2, respectively. Algorithm constructions in Section 4.1 and 4.2, that in Section 4.3 are similar to Takayasu-Kunihiro's [TK14d] and [TK14c], respectively.

4.1 The Attack 4

As in Section 3.2, when $\tilde{d}$ which is the MSBs of d is given, RSA key generation can be written as $e(\tilde{d}M+d')=1+k\Phi(N)$ with some integer k such that $|k|\leq N^{\beta}$ and $M=2^{\lfloor\gamma\log N\rfloor}$. Then, we find the root of the following modular polynomial:

$$f_{MSBs,m}(x,y)=1+(\tilde{k}+x)(\tilde{\Phi}(N)+y) \pmod e$$

where $\tilde{k}=\lfloor(e\tilde{d}-1)/\tilde{\Phi}(N)\rfloor$ which is an approximation to k as in Section 3.2. If we can recover the root $(x,y)=(k-\tilde{k},\Phi(N)-\tilde{\Phi}(N))$, whole secret information can be computed. To obtain better results than integer equations based method in Section 3, we use a linearized variable $z=(\tilde{k}+x)y+1$. The absolute values of the root are bounded above by $X:=N^{\lambda},Y:=N^{\delta},Z:=N^{\beta+\delta}$ where $\lambda=\max\{\gamma,\beta+\delta-1\}$.

To solve the modular equation $f_{MSBs,m}(x,y)=0$, we use the following shift-polynomials $g_{[u,i]}^{MSBs.m1}(x,y)$ and $g_{[u,i]}^{MSBs.m2}(x,y)$:

$$g_{[u,i]}^{MSBs.m1}(x,y):=x^{u-i}f_{MSBs,m}(x,y)^i e^{m-i} \text{ and}$$
$$g_{[u,j]}^{MSBs.m2}(x,y):=y^j f_{MSBs,m}(x,y)^u e^{m-u}.$$

All these shift-polynomials $g_{[u,i]}^{MSBs.m1}$ and $g_{[u,j]}^{MSBs.m2}$ modulo e^m have the root $(x,y) = (k-\tilde{k}, \Phi(N)-\tilde{\Phi}(N))$ that is the same as $f_{MSBs,m}(x,y)$. We build a lattice with these polynomials. In this section, we show a basic lattice construction to solve the modular equation and the resulting algorithm works when $1-\delta-\sqrt{\frac{\delta(1-\delta)}{3}} \leq \beta < 1-\delta$ and $1/3 \leq \delta$, and when $1-\delta-\sqrt{\frac{\delta(1-\delta)}{3}} \leq \beta < 1-\sqrt{\frac{\delta}{3}}$ and $\delta < 1/3$. In the lattice construction, we use shift-polynomials $g_{[u,i]}^{MSBs.m1}(x,y)$ and $g_{[u,i]}^{MSBs.m2}(x,y)$ with indices in $\mathcal{I}_x$ and $\mathcal{I}_y$ where

$$\begin{aligned}\mathcal{I}_x \Leftrightarrow\ & u = 0,1,\ldots,m; i = 0,1,\ldots,u \ \text{ and}\\ \mathcal{I}_y \Leftrightarrow\ & u = 0,1,\ldots,m; j = 1,2,\ldots,\left\lfloor \frac{\beta-\lambda}{\delta}m + \frac{1+\lambda-\delta-2\beta}{\delta}u \right\rfloor,\end{aligned}$$

respectively. Although the selections of shift-polynomials generate non-triangular basis matrices, we partially apply the linearization $z = (\tilde{k}+x)y + 1$ and the basis matrices can be transformed into triangular as in [TK14c]. We follow the result and the basis matrices have diagonals

- $X^{u-\lceil l^{MSBs}(i)\rceil} Y^{i-\lceil l^{MSBs}(i)\rceil} Z^{\lceil l^{MSBs}(i)\rceil} e^{m-i}$ for $g_{[u,i]}^{MSBs.m1}(x,y)$ and
- $X^{u-\lceil l^{MSBs}(u+j)\rceil} Y^{u+j-\lceil l^{MSBs}(u+j)\rceil} Z^{\lceil l^{MSBs}(u+j)\rceil} e^{m-u}$ for $g_{[u,j]}^{MSBs.m2}(x,y)$ where

$$l^{MSBs}(j) := \max\left\{0, \frac{\delta j - (\beta-\lambda)m}{1+\lambda-2\beta}\right\}.$$

Notice that the result is valid only when $\frac{1+\lambda-\delta-2\beta}{\delta} \leq 1$, i.e., $\beta \geq \frac{1+\lambda-2\delta}{2}$, since unravelled linearization does not work well otherwise in the sense that the diagonals of triangular basis matrices become larger. We define the above polynomial selections for all the $g_{[u,j]}^{MSBs.m2}(x,y)$ to be helpful.

Lemma 2. *Assume there are shift-polynomials $g_{[u,u'+j']}^{MSBs.m1}(x,y)$ for $u = u'+j', \ldots, m$ and $g_{[u,u'+j'-u]}^{MSBs.m2}(x,y)$ for $u = u'+1, \ldots, u'+j'-1$ in lattice bases. Then, shift-polynomials $g_{[u',j']}^{MSBs.m2}(x,y)$ are helpful polynomials when $u' = 0,1,\ldots,m; j' = 1,\ldots,\lfloor \frac{\beta-\lambda}{\delta}m + \frac{1+\lambda-\delta-2\beta}{\delta}u \rfloor$, whereas shift-polynomials $g_{[u',j']}^{MSBs.m2}(x,y)$ are unhelpful polynomials when $u' = 0,1,\ldots,m; j' > \frac{\beta-\lambda}{\delta}m + \frac{1+\lambda-\delta-2\beta}{\delta}u$.*

Proof. Consider the basis matrix $\boldsymbol{B}$. We add a new shift-polynomial $g_{[u',j']}^{MSBs2}(x,y)$ and construct the basis matrix $\boldsymbol{B}^+$. The value $\det(\boldsymbol{B}^+)/\det(\boldsymbol{B})$ can be computed as

$$\frac{\det(\boldsymbol{B}^+)}{\det(\boldsymbol{B})} = Y^{j'} Z^{u'} e^{m-u'} \cdot \left(\frac{XY}{Z}\right)^{m-u'}$$

where the size is bounded above by $N^{\delta j' + (\beta+\delta)u' + m - u' + (\lambda-\beta)(m-u')}$ within a constant factor. This value is smaller than the size of the modulus e^m, if and only if

$$\begin{aligned}&\delta j' + (\beta+\delta)\,u' + m - u' + (\lambda-\beta)(m-u') \leq m\\ \Leftrightarrow\ & j' \leq \frac{\beta-\lambda}{\delta}m + \frac{1+\lambda-\delta-2\beta}{\delta}u'\end{aligned}$$

as required. □

When $m+\frac{\beta-\lambda}{\delta}m+\frac{1+\lambda-\delta-2\beta}{\delta}m=\frac{1-\beta}{\delta}m\leq 1$, i.e., $\beta\geq 1-\delta$, shift-polynomials $g^{MSBs.m1}_{[u,j]}(x,y)$ for $u\geq\frac{\beta-\lambda}{2\beta+\delta-\lambda-1}; i\geq\frac{\beta-\lambda}{2\beta+\delta-\lambda-1}$ are unhelpful polynomials and do not contribute for the basis matrices to be triangular. In addition, when $\frac{1+\lambda-\delta-2\beta}{\delta}\leq 0$, i.e., $\beta\geq\frac{1+\lambda-\delta}{2}$, not all the $g^{MSBs.m2}_{[u,j]}(x,y)$ become helpful polynomials. Hence, we use the above collection of shift-polynomials only when $\beta<\min\{1-\delta,\frac{1+\lambda-\delta}{2}\}$.

We show that the above lattice yields the condition 2 of Theorem 2. For the purpose, we compute the dimension

$$n=|\mathcal{I}_x\cup\mathcal{I}_y|=\frac{1-\lambda}{2\delta}m^2+o(m^2),$$

and the determinant of the lattices $\det(\boldsymbol{B})=X^{s_X}Y^{s_Y}Z^{s_Z}e^{s_e}$ where

$$\begin{aligned}
s_X&=\sum_{(u,i)\in\mathcal{I}_x}(u-\lceil l_{MSBs}(i)\rceil)+\sum_{(u,j)\in\mathcal{I}_y}(u-\lceil l_{MSBs}(u+j)\rceil)=\frac{1+\beta-2\lambda}{6\delta}m^3+o(m^3),\\
s_Y+s_Z&=\sum_{(u,i)\in\mathcal{I}_x}i+\sum_{(u,j)\in\mathcal{I}_y}(u+j)=\frac{1-\beta-\lambda+\beta^2-\beta\lambda+\lambda^2}{6\delta^2}m^3+o(m^3),\\
s_Z&=\sum_{(u,i)\in\mathcal{I}_x}\lceil l_{MSBs}(i)\rceil+\sum_{(u,j)\in\mathcal{I}_y}\lceil l_{MSBs}(u+j)\rceil=\frac{1+\lambda-2\beta}{6\delta}m^3+o(m^3),\\
s_e&=\sum_{(u,i)\in\mathcal{I}_x}(m-i)+\sum_{(u,j)\in\mathcal{I}_y}(m-u)=\frac{1+\beta-2\lambda+\delta}{6\delta}m^3+o(m^3)
\end{aligned}$$

as required. We can find solutions of $f_{MSBs}(x,y)=0$ provided that $(\det(\boldsymbol{B}))^{1/n}<e^m$. Ignoring low order terms of m, the inequality becomes

$$\lambda^2-(1+\beta)\lambda+\beta^2-\beta+1-\delta>0$$

that yields the bound

$$\lambda<\frac{1+\beta-\sqrt{-3+4\delta+6\beta-3\beta^2}}{2}.$$

To satisfy the restriction $\frac{1+\lambda-2\delta}{2}\leq\beta<\min\{1-\delta,\frac{1+\lambda-\delta}{2}\}$ discussed above, the condition is valid only when $1-\delta-\sqrt{\frac{\delta(1-\delta)}{3}}\leq\beta<1-\delta$ and $1/3\leq\delta$, and when $1-\delta-\sqrt{\frac{\delta(1-\delta)}{3}}\leq\beta<1-\sqrt{\frac{\delta}{3}}$ and $\delta<1/3$. Notice that the bound is always larger than $\beta+\delta-1$. When $\beta\geq 1-\sqrt{\frac{\delta}{3}}$ and $\delta<1/3$, the Attack 3 becomes the best.

4.2 The Attack 5

In this section, we propose an attack for larger β, i.e., $\beta\geq 1-\delta$ for $1/3\leq\delta$. As discussed above, the polynomial selections in Section 4.1 have unhelpful polynomials in this case and we should

eliminate them to obtain better results. For the purpose, in this section, we use shift-polynomials $g_{[u,i]}^{MSBs.m1}(x,y)$ and $g_{[u,j]}^{MSBs.m2}(x,y)$ with indices in $\mathcal{I}_x$ and $\mathcal{I}_y$ where

$$\mathcal{I}_x \Leftrightarrow u = 0,1,\ldots,m; i = 0,1,\ldots,\min\{u,t\} \text{ and}$$
$$\mathcal{I}_y \Leftrightarrow u = 0,1,\ldots,m; j = 1,2,\ldots,\min\left\{\left\lfloor \frac{\beta-\lambda}{\delta}m + \frac{1+\lambda-\delta-2\beta}{\delta}u \right\rfloor, t-u\right\},$$

for some integer t, respectively. The parameter $\tau = t/m$ should be optimized later. The selections of shift-polynomials generate basis matrices that are not triangular. However, we partially apply the linearization $z = (\tilde{k}+x)y+1$ and the basis matrices can be transformed into triangular as in Section 3.3. Moreover, the diagonals of the basis matrices are the same as those in Section 3.3. Hence, Lemma 2 also holds. We use the above polynomial selections when $\frac{\beta-\lambda}{\delta}m < t$ and $\frac{1+\lambda-\delta-2\beta}{\delta} > 0$ hold, i.e., $\beta < \min\{\delta\tau+\lambda, \frac{1+\lambda-\delta}{2}\}$, since all the $g_{[u,j]}^{MSBs.m2}(x,y)$ do not become helpful polynomials otherwise.

We show that the above lattice yields the condition 3 of Theorem 2. For the purpose, we compute the dimension

$$n = |\mathcal{I}_x \cup \mathcal{I}_y| = \left(\tau - \frac{(\delta\tau-\beta+\lambda)^2}{2\delta(1+\lambda-2\beta)}\right)m^2 + o(m^2),$$

and the determinant of the lattices $\det(\boldsymbol{B}) = X^{s_X}Y^{s_Y}Z^{s_Z}e^{s_e}$ where

$$\begin{aligned}
s_X &= \sum_{(u,i)\in\mathcal{I}_x}(u - \lceil l_{MSBs}(i)\rceil) + \sum_{(u,j)\in\mathcal{I}_y}(u - \lceil l_{MSBs}(u+j)\rceil)\\
&= \left(\frac{\tau}{2} - \frac{(\delta\tau-\beta+\lambda)^3}{6\delta(1+\lambda-2\beta)^2}\right)m^3 - s_Z + o(m^3),\\
s_Y + s_Z &= \sum_{(u,i)\in\mathcal{I}_x} i + \sum_{(u,j)\in\mathcal{I}_y}(u+j)\\
&= \left(\frac{\tau^2}{2} - \frac{(\delta\tau-\beta+\lambda)^3}{3\delta^2(1+\lambda-2\beta)} - \frac{(\beta-\lambda)(\delta\tau-\beta+\lambda)^2}{2\delta^2(1+\lambda-2\beta)}\right)m^3 + o(m^3),\\
s_Z &= \sum_{(u,i)\in\mathcal{I}_x}\lceil l_{MSBs}(i)\rceil + \sum_{(u,j)\in\mathcal{I}_y}\lceil l_{MSBs}(u+j)\rceil\\
&= \left(\frac{(\delta\tau-\beta+\lambda)^2}{2\delta(1+\lambda-2\beta)} - \frac{(\delta\tau-\beta+\lambda)^3}{3\delta(1+\lambda-2\beta)^2}\right)m^3 + o(m^3),\\
s_e &= \sum_{(u,i)\in\mathcal{I}_x}(m-i) + \sum_{(u,j)\in\mathcal{I}_y}(m-u)\\
&= \tau m^3 - \frac{\tau^2}{2}m^3 + \frac{\tau^3}{6}m^3 - \frac{(\delta\tau-\beta+\lambda)^2}{2\delta(1+\lambda-2\beta)}m^3 + \frac{(\delta\tau-\beta+\lambda)^3}{6\delta(1+\lambda-2\beta)^2}m^3 + o(m^3).
\end{aligned}$$

We can find solutions $f_{MSBs}(x,y) = 0$ provided that $(\det(\boldsymbol{B}))^{1/n} < e^m$. Ignoring low order terms of m, the inequality becomes

$$\lambda\frac{\tau}{2} - (1-\delta)\frac{\tau^2}{2} + \frac{\tau^3}{6} < \frac{(\delta\tau-\beta+\lambda)^3}{6\delta(1+\lambda-2\beta)}.$$

To maximize the solvable root bounds, we set $\tau = 1 - \frac{\beta+\delta-1}{\delta-\sqrt{1+\lambda-2\beta}}$. To satisfy the restriction $\beta < \min\{\delta\tau + \lambda, \frac{1+\lambda-\delta}{2}\}$ discussed above, the attack works when $1-\delta \le \beta < \frac{3(1-\delta)(1+\delta)}{4}$ and $1/3 \le \delta < 2/3$, and when $1-\delta \le \beta < \delta - \frac{(2\delta-1)^2}{\delta^2}$ and $2/3 \le \delta$. The attack 2 becomes the best for larger β.

4.3 The Attack 6

In this section, we propose an attack for smaller β, i.e., $\beta < 1-\delta-\sqrt{\frac{\delta(1-\delta)}{3}}$. As discussed above, the polynomial selections in Section 4.1 collect $g_{[u,j]}^{MSBs.m2}(x,y)$ where all the shifts are not helpful. The defect follows from the fact that when $\frac{1+\lambda-\delta-2\beta}{\delta} > 1$, the unravelled linearization does not work well and the diagonals of the resulting triangular basis matrices become larger. Hence, in this section, we use shift-polynomials $g_{[u,i]}^{MSBs.m1}(x,y)$ and $g_{[u,j]}^{MSBs.m2}(x,y)$ with indices in $\mathcal{I}_x$ and $\mathcal{I}_y$ where

$$\begin{aligned}\mathcal{I}_x &\Leftrightarrow\ u = 0,1,\ldots,m; i = 0,1,\ldots,u \ \text{ and}\\ \mathcal{I}_y &\Leftrightarrow\ u = 0,1,\ldots,m; j = 1,2,\ldots,t+u,\end{aligned}$$

for some integer t, respectively. The parameter $\tau = t/m$ should be optimized later. The selections of shift-polynomials generate basis matrices that are not triangular. However, we partially apply the linearization $z = (\tilde{k}+x)y+1$ and the basis matrices can be transformed into triangular as in Section 4.1. Moreover, the diagonals of the basis matrices are the same as those in Section 3.3 by modifying

$$l^{MSBs}(k) := \max\left\{0, \frac{k-\tau m}{2}\right\}.$$

Hence, Lemma 2 also holds.

We show that the above lattice yields the condition 1 of Theorem 2. For the purpose, we compute the dimension

$$n = |\mathcal{I}_x \cup \mathcal{I}_y| = (1+\tau)m^2 + o(m^2),$$

and the determinant of the lattices $\det(\boldsymbol{B}) = X^{s_X} Y^{s_Y} Z^{s_Z} e^{s_e}$ where

$$\begin{aligned}s_X &= \sum_{(u,i)\in\mathcal{I}_x} (u - \lceil l_{MSBs}(i)\rceil) + \sum_{(u,j)\in\mathcal{I}_y} (u - \lceil l_{MSBs}(u+j)\rceil) = \left(\frac{1}{3}+\frac{\tau}{2}\right)m^3 + o(m^3),\\ s_Y + s_Z &= \sum_{(u,i)\in\mathcal{I}_x} i + \sum_{(u,j)\in\mathcal{I}_y} (u+j) = \left(\frac{2}{3}+\tau+\frac{\tau^2}{2}\right)m^3 + o(m^3),\\ s_Z &= \sum_{(u,i)\in\mathcal{I}_x} \lceil l_{MSBs}(i)\rceil + \sum_{(u,j)\in\mathcal{I}_y} \lceil l_{MSBs}(u+j)\rceil = \frac{1}{3}m^3 + o(m^3),\\ s_e &= \sum_{(u,i)\in\mathcal{I}_x} (m-i) + \sum_{(u,j)\in\mathcal{I}_y} (m-u) = \frac{1+\tau}{2}m^3 + o(m^3).\end{aligned}$$

We can find solutions of $f_{MSBs}(x,y)=0$ provided that $(\det(\boldsymbol{B}))^{1/n} < e^m$. Ignoring low order terms of m, the inequality becomes

$$\lambda\left(\frac{1}{3}+\frac{\tau}{2}\right)+\delta\left(\frac{2}{3}+\tau+\frac{\tau^2}{2}\right)+\beta\frac{1}{3}+\frac{1+\tau}{2}<1+\tau.$$

To maximize the right hand side of the inequality, we set the parameter $\tau = \frac{1-2\delta-\lambda}{2\delta}$ and the condition becomes

$$\lambda < \frac{3-2\delta-2\sqrt{4\delta^2-3\delta+6\beta\delta}}{3}$$

as required.

5 Attacks with the LSBs of d by Solving Modular Equations

In this section, we solve modular equations and propose two attacks, i.e., Attacks 6 and 7, for $(1,\beta,\gamma,\delta)$-partial key exposure attacks with the LSBs of d. The Attack 7 and 8 in Section 5.1 and 5.2 corresponds to the conditions 2 and 1 of Theorem 3, respectively. Algorithm constructions in Section 5.1 and that in Section 5.2 is similar to Takayasu-Kunihiro's [TK14d] and [TK14c], respectively.

5.1 The Attack 7

As in Section 3.1, when $\tilde{d}$ which is the LSBs of d is given, RSA key generation can be written as $e(\tilde{d}+d'M)=1+k\Phi(N)$ with some integer k such that $|k|\le N^\beta$ and $M=2^{\lfloor(\beta-\gamma)\log N\rfloor}$. Then, we find the root of the following modular polynomials:

$$\begin{aligned}
f_{LSBs.m1}(x,y) &:= 1-e\tilde{d}+x(\tilde{\Phi}(N)+y) \pmod{eM},\\
f_{LSBs.m2}(x,y) &:= 1+x(\tilde{\Phi}(N)+y) \pmod{e}.
\end{aligned}$$

If we can recover the root $(x,y)=(k,\Phi(N)-\tilde{\Phi}(N))$, whole secret information can be computed. To obtain better results than integer equations based method in Section 3, we use a linearized variable $z=xy+1$. The absolute values of the root are bounded above by $X:=N^\beta, Y:=N^\delta, Z:=N^{\beta+\delta}$.

To solve the modular equations $f_{LSBs.m1}(x,y)=0$ and $f_{LSBs.m2}(x,y)=0$, we use the following shift-polynomials $g^{LSBs.m1}_{[u,i]}(x,y)$ and $g^{LSBs.m2}_{[u,j]}(x,y)$:

$$\begin{aligned}
&g^{LSBs.m1}_{[u,i]}(x,y) := x^{u-i}f_{LSBs.m1}(x,y)^i(eM)^{m-i} \text{ and}\\
&g^{LSBs.m2}_{[u,j]}(x,y) := y^j f_{LSBs.m1}(x,y)^{u-\lceil l^{LSBs}(j)\rceil} f_{LSBs.m2}(x,y)^{\lceil l^{LSBs}(j)\rceil} e^{m-u}M^{m-(u-\lceil l^{LSBs}(j)\rceil)},
\end{aligned}$$

where

$$l^{LSBs}(j)=\max\left\{0,\frac{\delta j-(\beta-\gamma)m}{1-2\beta+\gamma-\delta}\right\}.$$

All these shift-polynomials $g_{[u,i]}^{LSBs.m1}$ and $g_{[u,j]}^{LSBs.m2}$ modulo $(eM)^m$ have the root $(x,y) = (k, \Phi(N) - \tilde{\Phi}(N))$ that is the same as $f_{LSBs,m1}(x,y)$ and $f_{LSBs,m2}(x,y)$. We build a lattice with these polynomials. In this section, we show a basic lattice construction to solve the modular equations and the resulting algorithm works when $1-\delta-\sqrt{\frac{\delta(1-\delta)}{3}} \leq \beta < 1-\frac{\delta}{2}-\frac{\sqrt{3\delta(4-\delta)}}{6}$. In the lattice construction, we use shift-polynomials $g_{[u,i]}^{LSBs.m1}(x,y)$ and $g_{[u,j]}^{LSBs.m2}(x,y)$ with indices in $\mathcal{I}_x$ and $\mathcal{I}_y$ where

$$\begin{aligned}
\mathcal{I}_x &\Leftrightarrow\ u = 0,1,\ldots,m; i = 0,1,\ldots,u \ \text{ and} \\
\mathcal{I}_y &\Leftrightarrow\ u = 0,1,\ldots,m; j = 1,2,\ldots, \left\lfloor \frac{\beta-\lambda}{\delta} m + \frac{1+\lambda-\delta-2\beta}{\delta} u \right\rfloor,
\end{aligned}$$

respectively. Although the selections of shift-polynomials generate non-triangular basis matrices, we partially apply the linearization $z = xy + 1$ and the basis matrices can be transformed into triangular as in [TK14c]. We follow the result and the basis matrices have diagonals

- $X^u Y^i (eM)^{m-i}$ for $g_{[u,i]}^{LSBs.m1}(x,y)$ and
- $X^{u-\lceil l^{LSBs}(u+j)\rceil} Y^{u+j-\lceil l^{LSBs}(u+j)\rceil} Z^{\lceil l^{LSBs}(u+j)\rceil} e^{m-u} M^{m-(u-\lceil l^{LSBs}(u+j)\rceil)}$ for $g_{[u,j]}^{LSBs.m2}(x,y)$.

Notice that the result is valid only when $\frac{1+\gamma-\delta-2\beta}{\delta} \leq 1$, i.e., $\beta \geq \frac{1+\gamma-2\delta}{2}$, since unravelled linearization does not work well otherwise. We define the above polynomial selections for all the $g_{[u,j]}^{MSBs.m2}(x,y)$ to be helpful.

Lemma 3. *Assume there are shift-polynomials $g_{[u'+i,j'+i]}^{LSBs.m2}(x,y)$ for $i = 1,2,\ldots,m-u'$ in lattice bases. Then, shift-polynomials $g_{[u',j']}^{LSBs.m2}(x,y)$ are helpful polynomials when $u' = 0,1,\ldots,m; j' = 1,\ldots,\lfloor \frac{\beta-\gamma}{\delta} m + \frac{1+\gamma-\delta-2\beta}{\delta} u' \rfloor$, whereas shift-polynomials $g_{[u',j']}^{LSBs.m2}(x,y)$ are unhelpful polynomials when $u' = 0,1,\ldots,m; j' > \frac{\beta-\gamma}{\delta} m + \frac{1+\gamma-\delta-2\beta}{\delta} u'$.*

Proof. Consider the basis matrix $\boldsymbol{B}$. We add a new shift-polynomial $g_{[u',k']}^{LSBs.m2}(x,y)$ and construct the basis matrix $\boldsymbol{B}^+$. The value $\det(\boldsymbol{B}^+)/\det(\boldsymbol{B})$ can be computed as

$$\frac{\det(\boldsymbol{B}^+)}{\det(\boldsymbol{B})} = Y^{j'} Z^{u'} e^{m-u'} M^{u'}.$$

where the size is bounded above by $N^{\delta j' + (\delta+\beta)u' + m - u' + (\beta-\gamma)u'}$ within a constant factor. This value is smaller than the size of the modulus $(eM)^m$, if and only if

$$\begin{aligned}
&\delta j' + (\delta+\beta)\, u' + m - u' + (\beta-\gamma)u' \leq (1+\beta-\gamma)m \\
\Leftrightarrow\ & j' \leq \frac{\beta-\gamma}{\delta} m + \frac{1-2\beta+\gamma-\delta}{\delta} u'
\end{aligned}$$

as required. □

When $\frac{1+\gamma-\delta-2\beta}{\delta} \leq 0$, i.e., $\beta \geq \frac{1+\gamma-\delta}{2}$, all the shift-polynomials $g_{[u,j]}^{LSBs.m2}(x,y)$ in the above selection do not become a helpful polynomial since the assumption in Lemma 3 fails. Hence, we use the above collection of shift-polynomials only when $\beta < \frac{1+\gamma-\delta}{2}$.

We show that the above lattice yields the condition 2 of Theorem 3. For the purpose, we compute the dimension

$$n = |\mathcal{I}_x \cup \mathcal{I}_y| = \frac{1-\gamma}{2\delta}m^2 + o(m^2),$$

and the determinant of the lattices $\det(\boldsymbol{B}) = X^{s_X} Y^{s_Y} Z^{s_Z} e^{s_e} M^{s_M}$ where

$$\begin{aligned}
s_X + s_Z &= \sum_{(u,i)\in\mathcal{I}_x} u + \sum_{(u,j)\in\mathcal{I}_y} u = \frac{1-\beta-\gamma}{6\delta}m^3 + o(m^3),\\
s_Y + s_Z &= \sum_{(u,i)\in\mathcal{I}_x} i + \sum_{(u,j)\in\mathcal{I}_y} (u+j) = \frac{1-\beta-\gamma+\beta^2-\beta\gamma+\gamma^2}{6\delta^2}m^3 + o(m^3),\\
s_Z &= \sum_{(u,i)\in\mathcal{I}_x} \lceil l_{MSBs}(i)\rceil + \sum_{(u,j)\in\mathcal{I}_y} \lceil l_{MSBs}(u+j)\rceil = \frac{1-2\beta+\gamma}{6\delta}m^3 + o(m^3),\\
s_e &= \sum_{(u,i)\in\mathcal{I}_x} (m-i) + \sum_{(u,j)\in\mathcal{I}_y} (m-u) = \frac{1+\beta-2\gamma+\delta}{6\delta}m^3 + o(m^3),\\
s_M &= \sum_{(u,i)\in\mathcal{I}_x} (m-i) + \sum_{(u,j)\in\mathcal{I}_y} (m-(u-\lceil l^{LSBs}(j)\rceil)) = \frac{2-\beta-\gamma}{6\delta}m^3 + o(m^3).
\end{aligned}$$

We can find solutions of $f_{LSBs.m1}(x,y) = 0$ and $f_{LSBs.m2}(x,y) = 0$ provided that $(\det(\boldsymbol{B}))^{1/n} < (eM)^m$. Ignoring low order terms of m, the inequality becomes

$$\gamma^2 - (1+\beta)\gamma + \beta^2 - \beta + 1 - \delta > 0$$

that yields the bound

$$\gamma < \frac{1+\beta-\sqrt{-3+4\delta+6\beta-3\beta^2}}{2}$$

as required. To satisfy the restriction $\frac{1+\gamma-2\delta}{2} \leq \beta < \frac{1+\gamma-\delta}{2}$ discussed above, the condition is valid only when $1-\delta-\sqrt{\frac{\delta(1-\delta)}{3}} \leq \beta < 1-\frac{\delta}{2}-\frac{\sqrt{3\delta(4-\delta)}}{6}$. When $1-\frac{\delta}{2}-\frac{\sqrt{3\delta(4-\delta)}}{6} \leq \beta$, Theorem 1 becomes the best.

5.2 The Attack 8

In this section we propose an attack that works when $\beta < 1-\delta-\sqrt{\frac{\delta(1-\delta)}{3}}$. In the lattice construction, we use the same shift-polynomials $g_{[u,i]}^{LSBs.m1}(x,y)$ and $g_{[u,j]}^{LSBs.m2}(x,y)$ where

$$l^{LSBs}(j) = \max\{0, j-\tau m\}$$

with indices in $\mathcal{I}_x$ and $\mathcal{I}_y$ where

$$\mathcal{I}_x \Leftrightarrow u = 0, 1, \ldots, m; i = 0, 1, \ldots, u \text{ and}$$
$$\mathcal{I}_y \Leftrightarrow u = 0, 1, \ldots, m; j = 1, 2, \ldots, t + u,$$

respectively. The parameter $\tau = t/m$ should be optimized later. Although the selections of shift-polynomials generate non-triangular basis matrices, we partially apply the linearization $z = xy + 1$ and the basis matrices can be transformed into triangular as in Section 5.1. The basis matrices have the same diagonals as those in Section 5.1 although the function $l^{LSBs}(j)$ is modified.

We show that the above lattice yields the condition 1 of Theorem 2. For the purpose, we compute the dimension

$$n = |\mathcal{I}_x \cup \mathcal{I}_y| = (1 + \tau)m^2 + o(m^2),$$

and the determinant of the lattices $\det(\boldsymbol{B}) = X^{s_X} Y^{s_Y} Z^{s_Z} e^{s_e} M^{s_M}$ where

$$\begin{aligned}
s_X &= \sum_{(u,i)\in\mathcal{I}_x} u + \sum_{(u,j)\in\mathcal{I}_y} u = \left(\frac{2}{3} + \frac{\tau}{2}\right) m^3 + o(m^3), \\
s_Y + s_Z &= \sum_{(u,i)\in\mathcal{I}_x} i + \sum_{(u,j)\in\mathcal{I}_y} (u + j) = \left(\frac{2}{3} + \tau + \frac{\tau^2}{2}\right) m^3 + o(m^3), \\
s_e &= \sum_{(u,i)\in\mathcal{I}_x} (m - i) + \sum_{(u,j)\in\mathcal{I}_y} (m - u) = \frac{1 + \tau}{2} m^3 + o(m^3), \\
s_M &= \sum_{(u,i)\in\mathcal{I}_x} (m - i) + \sum_{(u,j)\in\mathcal{I}_y} (m - (u - \lceil l^{LSBs}(j) \rceil)) = \left(\frac{2}{3} m^3 + \frac{\tau}{2}\right) m^3 + o(m^3).
\end{aligned}$$

We can find solutions of $f_{LSBs.m1}(x, y) = 0$ and $f_{LSBs.m2}(x, y) = 0$ provided that $(\det(\boldsymbol{B}))^{1/n} < (eM)^m$. Ignoring low order terms of m, the inequality becomes

$$\beta \left(\frac{2}{3} + \frac{\tau}{2}\right) + \delta \left(\frac{2}{3} + \tau + \frac{\tau^2}{2}\right) + \frac{1 + \tau}{2} + (\beta - \gamma) \left(\frac{2}{3} + \frac{\tau}{2}\right) < (1 + \beta - \gamma)(1 + \tau).$$

To maximize the right hand side of the inequality, we set the parameter $\tau = \frac{1 - 2\delta - \gamma}{2\delta}$ and the condition becomes

$$\gamma < \frac{3 - 2\delta - 2\sqrt{4\delta^2 - 3\delta + 6\beta\delta}}{3}$$

as required.

6 Concluding Remarks

In this paper, we defined partial key exposure attacks on RSA to capture general scenarios. Indeed, several existing works can be viewed as special cases of our general definition. Then we constructed

eight attacks for the scenario. These attacks contain all the state-of-the-art partial key exposure attacks as special cases. Furthermore, our attacks improve several existing attacks in some cases. Due to our generalized definition of partial key exposure scenarios, we believe that our attacks can be used as a tool kit. The results enable even beginners of Coppersmith's methods to examine the security of several future variants of RSA and upcoming partial key exposure scenarios.

Although we tried to capture as wide class of partial key exposure scenarios as possible in this paper, we could only capture Multi-Prime RSA with partial information. There are other papers that studied partial key exposure attacks on other variants of RSA; RSA with moduli $N = p^r q$ [LZPL15, Sar16, TK16a], CRT-RSA [BM03, TK15, TK16b], RSA with multiple exponent pairs [PHL$^+$15, TK14b, TK16c], and more. It should be interesting open problems to study generalized partial key exposure scenarios for these variants as our work.

References

[BD00] Dan Boneh and Glenn Durfee. Cryptanalysis of RSA with private key d less than $N^{0.292}$. *IEEE Trans. Information Theory*, 46(4):1339–1349, 2000.

[BDF98] Dan Boneh, Glenn Durfee, and Yair Frankel. An attack on RSA given a small fraction of the private key bits. In Kazuo Ohta and Dingyi Pei, editors, *Advances in Cryptology - ASIACRYPT '98, International Conference on the Theory and Applications of Cryptology and Information Security*, volume 1514 of *Lecture Notes in Computer Science*, pages 25–34. Springer, 1998.

[BM03] Johannes Blömer and Alexander May. New partial key exposure attacks on RSA. In Dan Boneh, editor, *Advances in Cryptology - CRYPTO 2003, 23rd Annual International Cryptology Conference*, volume 2729 of *Lecture Notes in Computer Science*, pages 27–43. Springer, 2003.

[BM05] Johannes Blömer and Alexander May. A tool kit for finding small roots of bivariate polynomials over the integers. In Ronald Cramer, editor, *Advances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, volume 3494 of *Lecture Notes in Computer Science*, pages 251–267. Springer, 2005.

[CKLQ02] Mathieu Ciet, Francois Koeune, Fabien Laguillaumie, and Jean-Jacques Quisquater. Short private exponent attacks on fast variants of rsa. *UCL Crypto Group Technical Report Series CG-2002/4, University Catholique de Louvain*, 2002.

[Cop96a] Don Coppersmith. Finding a small root of a bivariate integer equation; factoring with high bits known. In Ueli M. Maurer, editor, *Advances in Cryptology - EUROCRYPT '96, International Conference on the Theory and Application of Cryptographic Techniques*, volume 1070 of *Lecture Notes in Computer Science*, pages 178–189. Springer, 1996.

[Cop96b] Don Coppersmith. Finding a small root of a univariate modular equation. In Ueli M. Maurer, editor, *Advances in Cryptology - EUROCRYPT '96, International Conference on the Theory and Application of Cryptographic Techniques*, volume 1070 of *Lecture Notes in Computer Science*, pages 155–165. Springer, 1996.

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

[Cop01] Don Coppersmith. Finding small solutions to small degree polynomials. In Joseph H. Silverman, editor, *Cryptography and Lattices, International Conference, CaLC 2001*, volume 2146 of *Lecture Notes in Computer Science*, pages 20–31. Springer, 2001.

[Cor04] Jean-Sébastien Coron. Finding small roots of bivariate integer polynomial equations revisited. In Christian Cachin and Jan Camenisch, editors, *Advances in Cryptology - EUROCRYPT 2004, International Conference on the Theory and Applications of Cryptographic Techniques*, volume 3027 of *Lecture Notes in Computer Science*, pages 492–505. Springer, 2004.

[Cor07] Jean-Sébastien Coron. Finding small roots of bivariate integer polynomial equations: A direct approach. In Alfred Menezes, editor, *Advances in Cryptology - CRYPTO 2007, 27th Annual International Cryptology Conference*, volume 4622 of *Lecture Notes in Computer Science*, pages 379–394. Springer, 2007.

[dW02] Benne de Weger. Cryptanalysis of rsa with small prime difference. *Applicable Algebra in Engineering, Communication and Computing*, 13(1):17–28, 2002.

[EJMdW05] Matthias Ernst, Ellen Jochemsz, Alexander May, and Benne de Weger. Partial key exposure attacks on RSA up to full size exponents. In Ronald Cramer, editor, *Advances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, volume 3494 of *Lecture Notes in Computer Science*, pages 371–386. Springer, 2005.

[Hin08] M. Jason Hinek. On the security of multi-prime RSA. *J. Mathematical Cryptology*, 2(2):117–147, 2008.

[How97] Nick Howgrave-Graham. Finding small roots of univariate modular equations revisited. In Michael Darnell, editor, *Cryptography and Coding, 6th IMA International Conference*, volume 1355 of *Lecture Notes in Computer Science*, pages 131–142. Springer, 1997.

[JM06] Ellen Jochemsz and Alexander May. A strategy for finding roots of multivariate polynomials with new applications in attacking RSA variants. In Xuejia Lai and Kefei Chen, editors, *Advances in Cryptology - ASIACRYPT 2006, 12th International Conference on the Theory and Application of Cryptology and Information Security*, volume 4284 of *Lecture Notes in Computer Science*, pages 267–282. Springer, 2006.

[LLL82] A.K. Lenstra, H.W.jun. Lenstra, and László Lovász. Factoring polynomials with rational coefficients. *Math. Ann.*, 261:515–534, 1982.

[LZPL15] Yao Lu, Rui Zhang, Liqiang Peng, and Dongdai Lin. Solving linear equations modulo unknown divisors: Revisited. In Tetsu Iwata and Jung Hee Cheon, editors, *Advances in Cryptology - ASIACRYPT 2015 - 21st International Conference on the Theory and Application of Cryptology and Information Security*, volume 9452 of *Lecture Notes in Computer Science*, pages 189–213. Springer, 2015.

[May03] Alexander May. *New RSA vulnerabilities using lattice reduction methods*. PhD thesis, University of Paderborn, 2003.

[May10] Alexander May. Using LLL-reduction for solving RSA and factorization problems. In Phong Q. Nguyen and Brigitte Vallée, editors, *The LLL Algorithm - Survey and Applications*, Information Security and Cryptography, pages 315–348. Springer, 2010.

[NS01] Phong Q. Nguyen and Jacques Stern. The two faces of lattices in cryptology. In Joseph H. Silverman, editor, *Cryptography and Lattices, International Conference, CaLC 2001*, volume 2146 of *Lecture Notes in Computer Science*, pages 146–180. Springer, 2001.

[PHL+15] Liqiang Peng, Lei Hu, Yao Lu, Santanu Sarkar, Jun Xu, and Zhangjie Huang. Cryptanalysis of variants of RSA with multiple small secret exponents. In Alex Biryukov and Vipul Goyal, editors, *Progress in Cryptology - INDOCRYPT 2015 - 16th International Conference on Cryptology in India*, volume 9462 of *Lecture Notes in Computer Science*, pages 105–123. Springer, 2015.

[Sar16] Santanu Sarkar. Revisiting prime power RSA. *Discrete Applied Mathematics*, 203:127–133, 2016.

[SM08] Santanu Sarkar and Subhamoy Maitra. Improved partial key exposure attacks on RSA by guessing a few bits of one of the prime factors. In Pil Joong Lee and Jung Hee Cheon, editors, *Information Security and Cryptology - ICISC 2008*, volume 5461 of *Lecture Notes in Computer Science*, pages 37–51. Springer, 2008.

[SMS08] Santanu Sarkar, Subhamoy Maitra, and Sumanta Sarkar. RSA cryptanalysis with increased bounds on the secret exponent using less lattice dimension. *IACR Cryptology ePrint Archive*, 2008:315, 2008.

[SSM10] Santanu Sarkar, Sourav Sengupta, and Subhamoy Maitra. Partial key exposure attack on RSA - improvements for limited lattice dimensions. In Guang Gong and Kishan Chand Gupta, editors, *Progress in Cryptology - INDOCRYPT 2010 - 11th International Conference on Cryptology in India*, volume 6498 of *Lecture Notes in Computer Science*, pages 2–16. Springer, 2010.

[SWS+08] Hung-Min Sun, Mu-En Wu, Ron Steinfeld, Jian Guo, and Huaxiong Wang. Cryptanalysis of short exponent RSA with primes sharing least significant bits. In Matthew K. Franklin, Lucas Chi Kwong Hui, and Duncan S. Wong, editors, *Cryptology and Network Security, 7th International Conference, CANS 2008*, volume 5339 of *Lecture Notes in Computer Science*, pages 49–63. Springer, 2008.

[TK14a] Atsushi Takayasu and Noboru Kunihiro. Better lattice constructions for solving multivariate linear equations modulo unknown divisors. *IEICE Transactions*, 97-A(6):1259–1272, 2014.

[TK14b] Atsushi Takayasu and Noboru Kunihiro. Cryptanalysis of RSA with multiple small secret exponents. In Willy Susilo and Yi Mu, editors, *Information Security and Privacy - 19th Australasian Conference, ACISP 2014*, volume 8544 of *Lecture Notes in Computer Science*, pages 176–191. Springer, 2014.

[TK14c] Atsushi Takayasu and Noboru Kunihiro. General bounds for small inverse problems and its applications to multi-prime RSA. In Jooyoung Lee and Jongsung Kim, editors, *Information Security and Cryptology - ICISC 2014 - 17th International Conference*, volume 8949 of *Lecture Notes in Computer Science*, pages 3–17. Springer, 2014.

[TK14d] Atsushi Takayasu and Noboru Kunihiro. Partial key exposure attacks on RSA: achieving the boneh-durfee bound. In Antoine Joux and Amr M. Youssef, editors, *Selected Areas in Cryptography - SAC 2014 - 21st International Conference*, volume 8781 of *Lecture Notes in Computer Science*, pages 345–362. Springer, 2014.

[TK15] Atsushi Takayasu and Noboru Kunihiro. Partial key exposure attacks on CRT-RSA: better cryptanalysis to full size encryption exponents. In Tal Malkin, Vladimir Kolesnikov, Allison Bishop Lewko, and Michalis Polychronakis, editors, *Applied Cryptography and Network Security - 13th International Conference, ACNS 2015*, volume 9092 of *Lecture Notes in Computer Science*, pages 518–537. Springer, 2015.

[TK16a] Atsushi Takayasu and Noboru Kunihiro. How to generalize RSA cryptanalyses. In Chen-Mou Cheng, Kai-Min Chung, Giuseppe Persiano, and Bo-Yin Yang, editors, *Public-Key Cryptography - PKC 2016 - 19th IACR International Conference on Practice and Theory in Public-Key Cryptography*, volume 9615 of *Lecture Notes in Computer Science*, pages 67–97. Springer, 2016.

[TK16b] Atsushi Takayasu and Noboru Kunihiro. Partial key exposure attacks on CRT-RSA: general improvement for the exposed least significant bits. In Matt Bishop and Anderson C. A. Nascimento, editors, *Information Security - 19th International Conference, ISC 2016*, volume 9866 of *Lecture Notes in Computer Science*, pages 35–47. Springer, 2016.

[TK16c] Atsushi Takayasu and Noboru Kunihiro. Partial key exposure attacks on RSA with multiple exponent pairs. In Joseph K. Liu and Ron Steinfeld, editors, *Information*

Security and Privacy - 21st Australasian Conference, ACISP 2016, volume 9723 of *Lecture Notes in Computer Science*, pages 243–257. Springer, 2016.

[ZT13] Hui Zhang and Tsuyoshi Takagi. Attacks on multi-prime RSA with small prime difference. In Colin Boyd and Leonie Simpson, editors, *Information Security and Privacy - 18th Australasian Conference, ACISP 2013*, volume 7959 of *Lecture Notes in Computer Science*, pages 41–56. Springer, 2013.

[ZT14] Hui Zhang and Tsuyoshi Takagi. Improved attacks on multi-prime RSA with small prime difference. *IEICE Transactions*, 97-A(7):1533–1541, 2014.