Partial Key Exposure Attacks on RSA: Achieving the Boneh-Durfee Bound

Atsushi Takayasu(✉) and Noboru Kunihiro

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

Abstract. Several algorithms have been proposed for factoring RSA modulus N when attackers know the most or the least significant $(\beta - \delta)\log N$ bits of secret exponents $d < N^{\beta}$. The attacks are expected to work when $\beta < 1 - 1/\sqrt{2}$ with full size public exponent e considering Boneh and Durfee's result for small secret exponent attacks on RSA. However, previous attacks do not always work in this condition when attackers know only a small amount of information on secret exponent, that is, δ is close to β. In this paper, we propose the improved algorithms for partial key exposure attacks which cover Boneh and Durfee's bound when $\delta = \beta$. Our algorithms are the best among all known results when attackers know the most significant bits of $d \leq N^{9/16}$ or the least significant bits of $d \leq N^{(9-\sqrt{21})/12}$. In our algorithm constructions, we construct basis matrices for lattices which are not triangular and analyze the determinant by using unravelled linearization. The analysis enables us to make better use of the algebraic structures of modular polynomials, that is, we can select appropriate lattice bases or construct appropriate lattice bases.

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

1 Introduction

1.1 Background

Small Secret Exponent RSA. When small secret exponent $d < N^{\beta}$ is used, RSA cryptosystem becomes efficient for the decryption cost or the signature generation cost. However, Wiener [32] revealed the vulnerability. They claimed that public modulus N can be factored in polynomial time when $\beta < 1/4$.

Boneh and Durfee [5] revisited the attack and further improved the result. They used lattice-based Coppersmith's method to solve modular equations [8, 20]. At first, they constructed lattices which provide Wiener's bound $\beta < 1/4$. Next, they added some extra polynomials in the lattice bases and improved the bound to $\beta < (7-2\sqrt{7})/6 = 0.28474\cdots$. Finally, they achieved a stronger bound $\beta < 1 - 1/\sqrt{2} = 0.29289\cdots$ by extracting sublattices. To achieve the stronger bound, they used lattices which are not full-rank. Since the determinant of such lattices are difficult to compute, the analysis of the bound is involved.

A. Joux and A. Youssef (Eds.): SAC 2014, LNCS 8781, pp. 345–362, 2014.
DOI: 10.1007/978-3-319-13051-4_21

Partial Key Exposure Attacks on RSA. Boneh, Durfee and Frankel [6] introduced several attacks on RSA with small public exponent e. Their attacks make good use of the knowledge of the most significant bits (MSBs) or the least significant bits (LSBs) of secret exponent d. After that, such partial key exposure situations have been practically reported using side channel attacks, cold boot attacks [14]. Therefore, estimating the security of RSA with partial knowledge of the secret key has become increasingly important problem. See also [15,16,22,23,28].

Blömer and May [4] improved the attacks using Coppersmith's method to solve modular equations [8,20]. Blömer and May's work revealed that partial key exposure RSA is vulnerable for larger public exponent e. Ernst et al. [13] improved the attack to full size encryption exponent e using Coppersmith's method to find small roots of polynomials over the integers [9,12]. In addition, they proposed analogous attacks with full size public exponent e and small secret exponent d. In this paper, we study the situation:

- the prime factors p, q are the same bit size, $q < p < 2q$,
- the public exponent e is full size, the bit length of e is $\log N$,
- the secret exponent $d < N^{\beta}$ is small, $0 < \beta \leq 1$,
- in addition to public keys (N, e), attackers know d_0 which is $(\beta - \delta) \log N$ the most or the least significant bits of the secret exponent d with $0 \leq \delta \leq \beta$.

Partial key exposure situation with $\delta = \beta$, when attackers know no information of secret exponent d, is the same situation as Boneh and Durfee's work [5]. Therefore, the attack should always work when $\beta < 1 - 1/\sqrt{2}$. However, Ernst et al.'s results [13] only achieved the Boneh and Durfee's weaker bound $\beta < (7 - 2\sqrt{7})/6$ when $\delta = \beta$.

At PKC 2009, Aono [1] improved the algorithm for the LSBs partial key exposure attacks using Coppersmith's method to solve modular equations [8,20]. Aono used lattices which are not full rank and the basis matrices are not triangular. The result covers Boneh and Durfee's stronger bound $\beta < 1 - 1/\sqrt{2}$ when $\delta = \beta$. However, the attack is not applicable to the MSBs partial key exposure case. Sarkar, Gupta and Maitra [29] analyzed the MSBs partial key exposure attacks using Coppersmith's method to solve modular equations [8,20]. Though their attack partially covers Ernst et al.'s bound, they cannot improve it. To construct algorithms for the MSBs partial key exposure attacks that cover Boneh and Durfee's stronger bound remains an open problem.

Unravelled Linearization. Herrmann and May [18] introduced a new technique for lattice constructions, *unravelled linearization*. To solve nonlinear modular equations, consider the linear modular polynomials using *linearization*. In addition, unravelled linearization makes use of the lost algebraic structure using *unravelling*, which partially unravel the linearized variables in basis matrices. This operation transform basis matrices which are not triangular to be triangular and enables us to analyze the lattices which are not full rank easily. At PKC 2010, Herrmann and May [19] gave an elementary proof for Boneh and

Durfee's attack to achieve the stronger bound $\beta < 1 - 1/\sqrt{2}$. They used unravelled linearization and transformed Boneh and Durfee's lattices to be full rank with triangular basis matrices. Compared with original Boneh and Durfee's proof [5], the elegant technique enables us to extract appropriate sublattices easily. In addition, several results [2,18,21,31] have been reported to improve the previous results with the technique.

Collecting Helpful Polynomials. To maximize solvable root bounds, it is crucial to select appropriate polynomials in lattice bases. To examine which polynomials to be selected, May introduced the notion of *helpful* in his survey [26]. They called the polynomials whose sizes of diagonals in the basis matrices are smaller than the size of the modulus helpful polynomials. Helpful polynomials reduce the determinant of the lattices and enable us to obtain better bounds.

At a glance, the notion is completely trivial. However, Takayasu and Kunihiro [30] made use of the notion and provided the improved lattice constructions. They claimed that as many helpful polynomials as possible should be selected in lattice bases as long as the basis matrices are triangular. Based on the strategy, they improved the algorithms to solve two forms of modular multivariate linear equations [7,17]. The two algorithms were improved with full rank lattices with triangular basis matrices. That means though the analyses of triangular basis matrices are easy, that do not mean selections of appropriate lattice bases are trivial. Takayasu and Kunihiro's results [30] imply that the notion of helpful enables us to determine the appropriate polynomial selections.

1.2 Our Contributions

In this paper, we use Coppersmith's method to solve modular equations [8,20] and propose a improved algorithms for partial key exposure attacks on RSA for both the MSBs and the LSBs cases. Both our algorithms achieve Boneh and Durfee's stronger bound $\beta < 1 - 1/\sqrt{2}$ when $\delta = \beta$. Since we consider bivariate equations, our algorithms work under the assumption that polynomials obtained by the LLL reduced bases are algebraically independent as in previous works [1,4,5,13,29]. The assumption may be valid since few negative cases have been reported.

For the MSBs partial key exposure attacks, this is the first result to cover Boneh and Durfee's stronger bound when $\delta = \beta$.

Theorem 1. *When we know the most significant $(\beta - \delta)\log N$ bits of secret exponent d, public moduli N can be factored in polynomial time in $\log N$ and $1/\epsilon$ provided that*

$$\text{(i) } \delta \le \frac{1 + \beta - \sqrt{-1 + 6\beta - 3\beta^2}}{2} - \epsilon, \beta \le \frac{1}{2},$$

$$\text{(ii) } \delta \le \frac{\tau}{2} - \frac{\tau^2}{3} + \frac{1}{6\tau} \cdot \frac{(\tau - 2(\beta - \delta))^3}{2 + 2\delta - 4\beta} - \epsilon, \tau = 1 - \frac{2\beta - 1}{1 - 2\sqrt{1 + \delta - 2\beta}},$$

$$\frac{1}{2} < \beta \le \frac{9}{16}.$$

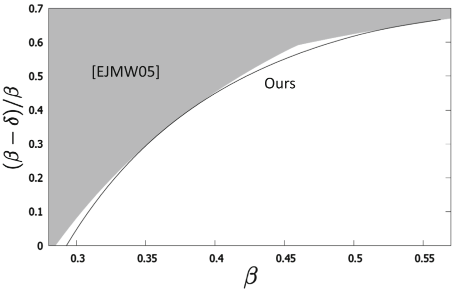

Fig. 1. Recoverable conditions for the MSBs partial key exposure attacks. Grey area represents the condition established by Ernst et al. Our algorithm works in the area left above of the solid line.

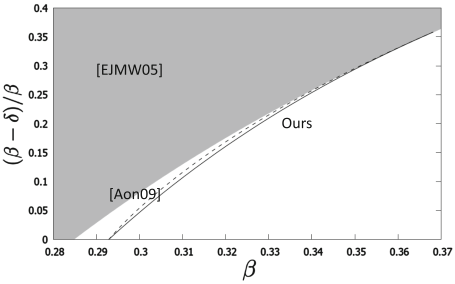

Fig. 2. Recoverable condition for the LSBs partial key exposure attacks. Grey area represents the condition established by Ernst et al. Aono's algorithm works in the area left above of the broken line. Our algorithm works in the area left above of the solid line.

We solve the same modular equations as Sarkar et al. [29], though Sarkar et al.'s algorithm does not even cover Boneh and Durfee's weaker bound. To the best of our knowledge, this is the first result to analyze the basis matrices which are not triangular for the MSBs partial key exposure attacks. Unravelled linearization enables us to analyze algebraic structures of modular polynomials in detail. Though we use the same polynomials as Sarkar et al. in lattice bases, we change the selections. Figure 1 compares the solvable root bounds of our algorithm and Ernst et al.'s algorithms [13]. When $\beta \leq 9/16 = 0.5625$, our algorithm is superior to the previous ones.

For the LSBs partial key exposure attacks, our algorithms cover Boneh and Durfee's stronger bound when $\delta = \beta$ and are superior to Aono's algorithm [1].

Theorem 2. *When we know the least significant $(\beta - \delta)\log N$ bits of secret exponent d, public moduli N can be factored in polynomial time in $\log N$ and $1/\epsilon$ provided that*

$$\delta \leq \frac{1+\beta-\sqrt{-1+6\beta-3\beta^2}}{2} - \epsilon, \beta \leq \frac{9-\sqrt{21}}{12}.$$

We solve the same modular equations as Aono. First, we use unravelled linearization and transform Aono's basis matrices to be triangular. This transformation reveals a bottleneck of Aono's lattice constructions. We change polynomials in lattice bases in order to make full use of algebraic structures of modular polynomials. Figure 2 compares the solvable root bounds of our algorithm, Ernst et al.'s algorithm [13], and Aono's algorithm [1]. When $\beta < (9-\sqrt{21})/12 = 0.36811\cdots$, our algorithms are superior to the previous ones.

1.3 Roadmap

The organization of this paper is as follows. In Sect. 2, we recall the RSA key generation and formulate the MSBs and the LSBs partial key exposure attacks. In Sect. 3, we introduce Coppersmith's method to solve modular equations, the technique and the strategy for the lattice constructions. In Sect. 4, we analyze the MSBs partial key exposure attack and prove Theorem 1. In Sect. 5, we analyze the LSBs partial key exposure attack and prove Theorem 2.

2 Formulations of Partial Key Exposure Attacks

We recall that the RSA key generation is described as

$$ed = 1 + \ell\phi(N), \text{where } \phi(N) = (p-1)(q-1) = N - (p+q-1).$$

In the MSBs partial key exposure case, we know d_0 which is the most significant bits of secret exponent d. We rewrite $d = d_0M + d_1$ with an integer $M := 2^{\lfloor \delta \log N \rfloor}$, d_1 is the unknown part of d. In this case, we can easily calculate an approximation to ℓ, $\ell_0 = \lfloor (ed_0 - 1)/N \rfloor$. We rewrite $\ell = \ell_0 + \ell_1$. The size of the unknown ℓ_1 is bounded by N^γ with $\gamma = \max\{\delta, \beta - 1/2\}$. This analysis is written in [4] in detail. Again, looking at the RSA key generation,

$$e(d_0M + d_1) = 1 + (\ell_0 + \ell_1)(N - (p+q-1)).$$

We consider the modular polynomial

$$f_{MSBs}(x,y) = 1 + (\ell_0 + x)(N + y) \pmod{e}.$$

This polynomial has the roots $(x,y) = (\ell_1, -(p+q-1))$. Sizes of the roots are bounded by X, Y where $X := N^\gamma, Y := 3N^{1/2}$. We can factor the RSA modulus N, if we can find the roots of $f_{MSBs}(x,y)$.

In the LSBs partial key exposure case, we know d_0 which is the least significant bits of secret exponent d. We rewrite $d = d_1M + d_0$ with an integer $M := 2^{\lfloor (\beta-\delta) \log N \rfloor}$, d_1 is the unknown part of d. In this case, we cannot calculate an approximation to ℓ. Again, look at the RSA key generation,

$$e(d_1M + d_0) = 1 + \ell(N - (p+q-1)).$$

We consider the modular polynomial

$$f_{LSBs}(x,y) = 1 - ed_0 + x(N + y) \pmod{eM}.$$

This polynomial has the roots $(x,y) = (\ell, -(p+q-1))$. Sizes of the roots are bounded by X, Y where $X := N^\beta, Y := 3N^{1/2}$. We can factor the RSA modulus N, if we can find the roots of $f_{LSBs}(x,y)$.

3 Coppersmith's Method to Solve Modular Equations

The Overview of the Method. At EUROCRYPT 1996, Coppersmith introduced the lattice based method to solve modular univariate equations in polynomial time. The method reveals several vulnerabilities of RSA cryptosystems. See [10,11,25–27] for more information. This method can be heuristically extended to bivariate cases with reasonable assumption. In this paper, we explain the reformulation by Howgrave-Graham [20]. For bivariate polynomials $h(x,y) = \sum h_{i_X,i_Y} x^{i_X} y^{i_Y}$, define a norm of the polynomials as $\|h(x,y)\| := \sqrt{\sum h_{i_X,i_Y}^2}$. The following Howgrave-Graham's lemma enables us to solve modular equations by finding roots of polynomials over the integers.

Lemma 1 (Howgrave-Graham's lemma [20]). *Let $h(x,y)$ be a bivariate integer polynomial which consists of at most n monomials. Let W, m, X, Y be positive integers. When the polynomial $h(x,y)$ satisfies*

1. $h(\bar{x},\bar{y}) = 0 \pmod{W^m}$, *where* $|\bar{x}| < X, |\bar{y}| < Y$,
2. $\|h(xX,yY)\| < W^m/\sqrt{n}$.

Then $h(\bar{x},\bar{y}) = 0$ holds over the integers.

To solve bivariate equations, we should find two polynomials that satisfy Howgrave-Graham's lemma. We use lattices and the LLL algorithm to find such low norm polynomials. Let $\mathbf{b}_1, \ldots, \mathbf{b}_n$ be linearly independent k-dimensional vectors. 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 call n the rank of the lattice, and k the dimension of the lattice. When $n = k$, lattices are described as full rank. The basis matrix of the lattice B is defined as the $n \times k$ matrix that has basis vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n$ in each row. In this paper, we use only full rank lattices. The determinant of a full rank lattice is computed by $\mathrm{vol}(L(B)) = |\det(B)|$.

In 1982, Lenstra, Lenstra and Lovász proposed the LLL algorithm [24], which find short lattice vectors in polynomial time.

Proposition 1 (LLL algorithm [24]). *Given k-dimensional basis vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n$, the LLL algorithm finds short lattice vectors $\mathbf{v}_1, \mathbf{v}_2$ that satisfy*

$$\|\mathbf{v}_1\| \leq 2^{(n-1)/4}(\mathrm{vol}(L))^{1/n}, \|\mathbf{v}_2\| \leq 2^{n/2}(\mathrm{vol}(L))^{1/(n-1)}.$$

These norms are all Euclidean norms. The running time of the LLL algorithm is $O(n^5 k (\log B)^3)$ where $\log B$ represents the maximum input length.

To solve the modular equations $h(x,y) = 0 \pmod{W}$, we create n polynomials $h_1(x,y), \ldots, h_n(x,y)$ that have the same roots as the original solutions modulo W^m with a positive integer m. We generate basis vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n$ whose elements are the coefficients of the polynomials $h_1(xX,yY), \ldots, h_n(xX,yY)$, respectively. The polynomials modulo W^m whose coefficients correspond to any lattice vectors spanned by $\mathbf{b}_1, \ldots, \mathbf{b}_n$ have the same roots as the original solutions. If two polynomials $p_1(x,y)$ and $p_2(x,y)$ whose coefficients correspond to short lattice vectors $\mathbf{v}_1, \mathbf{v}_2$ satisfy Howgrave-Graham's lemma, we can find the roots over the integers. This operation can easily be done by computing the Gröbner bases or resultant of $p_1(x,y), p_2(x,y)$.

We should note that the polynomials $p_1(x,y)$ and $p_2(x,y)$ have no assurance of algebraic independency. We assume that these polynomials are algebraic independent, and the resultant will not vanish. This assumption might be valid, since few negative cases have been reported.[1]

Unravelled Linearization. Boneh and Durfee [5] solved modular equations

$$f_{BD}(x,y) := 1 + N(x+y) = 0 \pmod{e}$$

for small secret exponent attacks on RSA. They selected shift-polynomials

$$g^{BD1}_{[u,i]}(x,y) := x^{u-i} f_{BD}(x,y)^i e^{m-i}, \text{ for } u = 0,1,\ldots,m, i = 0,1,\ldots,u,$$
$$g^{BD2}_{[u,j]}(x,y) := y^j f_{BD}(x,y)^u e^{m-u}, \text{ for } u = 0,1,\ldots,m, j = 0,1,\ldots,\lfloor(1-2\beta)u\rfloor,$$

in the lattice bases. The selection generates the basis matrix which is not triangular. That means there are some shift-polynomials which have several new monomials when added in the basis matrix. To avoid the situation, Herrmann and May [19] use the linearization $z := 1 + xy$. The linearization reduces the number of monomials of $f_{BD}(x,y)$. We partially apply the linearization to some monomials and the basis matrix becomes triangular. This operation enables us to compute the determinant of the lattice easily. See [19] for detailed analysis.

Collecting Helpful Polynomials. May [26] defined the notion of helpful compared with sizes of diagonals and a size of a modulus. Helpful polynomials contribute to the conditions for modular equations to be solved. Since each polynomial may affect not only the diagonal but also several other diagonals in our analyses, we cannot examine which polynomials to be selected with the previous definition of helpful polynomials. Therefore, we redefine the notion which covers the previous definition.

Definition 1 (Helpful Polynomials). *To solve equations with a modulus W, consider a basis matrix B. We add a new shift-polynomial $h_{[i',j']}(x,y)$ and construct a new basis matrix B^+. We call $h_{[i',j']}(x,y)$ a helpful polynomial, provided that*

$$\frac{\det(B^+)}{\det(B)} \le W^m.$$

Conversely, if the inequality does not hold, we call $h_{[i',j']}(x,y)$ an unhelpful polynomial.

[1] We should note that in Bernstein et al.'s [3] millions of experiments with very small lattice dimension, the heuristic assumption fails in many cases. However, they propose the method to recover small solutions in such cases. See the paper for detailed information.

4 Partial Key Exposure Attack: The Most Significant Bits Case

4.1 Previous Works

In the MSBs partial key exposure case, Ernst et al. [13] found the small roots of polynomials over the integers

$$g^{EJMW1}(x,y,z) = 1 - ed_0M + ex + y(N+z),$$
$$\text{or } g^{EJMW2}(x,y,z) = 1 - ed_0M + ex + (\ell_0 + y)(N+z),$$

to factor N. The polynomial $g^{EJMW1}(x,y,z)$ has the roots $(x,y) = (-d_1, \ell, -(p+q-1))$, and the polynomial $g^{EJMW2}(x,y,z)$ has the roots $(x,y) = (-d_1, \ell_1, -(p+q-1))$. Their algorithms work provided that

(1) $\gamma \le \frac{5}{6} - \frac{1}{3}\sqrt{1+6\beta} - \epsilon$,
(2) $\gamma \le \frac{3}{16} - \epsilon$ and $\beta \le \frac{11}{16}$,
(3) $\gamma \le \frac{1}{3} + \frac{1}{3}\beta - \frac{1}{3}\sqrt{4\beta^2 + 2\beta - 2} - \epsilon$ and $\beta \ge \frac{11}{16}$.

The condition (1) can be obtained by finding the roots of the polynomial g^{EJMW1} (x,y,z). The conditions (2), (3) can be obtained by finding the roots of the polynomial $g^{EJMW2}(x,y,z)$ with $\gamma = \delta$ and $\gamma = \beta - 1/2$, respectively. The condition yields Boneh and Durfee's weaker bound $\beta < (7 - 2\sqrt{7})/6$ when $\delta = \beta$.

Sarkar et al. [29] solved the modular equation $f_{MSBs}(x,y) = 0$ to factor N. To solve the modular equation, they used shift-polynomials

$$g^{MSBs1}_{[u,i]}(x,y) := x^{u-i} f_{MSBs}(x,y)^i e^{m-i},$$
$$g^{MSBs2}_{[u,j]}(x,y) := y^j f_{MSBs}(x,y)^u e^{m-u}.$$

Both shift-polynomials modulo e^m have the same roots as the original solutions, that is, $g^{MSBs1}_{[u,i]}(\ell_1, -(p+q-1)) = 0 \pmod{e^m}$ and $g^{MSBs2}_{[u,j]}(\ell_1, -(p+q-1)) = 0$ $\pmod{e^m}$. They selected shift-polynomials

$$g^{MSBs1}_{[u,i]}(x,y) \quad \text{for } u = 0,1,\ldots,\lfloor m/4\gamma \rfloor, i = 0,1,\ldots,\max\{m,u\},$$
$$g^{MSBs2}_{[u,j]}(x,y) \quad \text{for } u = 0,1,\ldots,m, i = 1,2,\ldots,u,$$

in the lattice bases. This selection generates triangular basis matrices with diagonals $X^uY^ie^{m-i}$ for $g^{MSBs1}_{[u,i]}(x,y)$, and $X^uY^{u+j}e^{m-u}$ for $g^{MSBs2}_{[u,j]}(x,y)$. The condition for the algorithm to work is the same as (2) of Ernst et al.'s condition.

4.2 Our Lattice Constructions

In this section, we explain our improved lattice constructions. At first, we consider the case for $\beta \le 1/2$.

For Smaller *d*. To solve the modular equation $f_{MSBs}(x,y)=0$, we use the same shift-polynomials $g_{[u,i]}^{MSBs1}(x,y), g_{[u,j]}^{MSBs2}(x,y)$ as Sarkar et al. However, we change the selections. To construct the basis matrix, we use shift-polynomials

$$g_{[u,i]}^{MSBs1}(x,y) \text{ for } u=0,1,\ldots,m, i=0,1,\ldots,u,$$
$$g_{[u,j]}^{MSBs2}(x,y) \text{ for } u=0,1,\ldots,m, j=1,2,\ldots,\lfloor 2(\beta-\gamma)m+(1+2\gamma-4\beta)u\rfloor,$$

in the lattice bases. The selections of shift-polynomials generate basis matrices which are not triangular. However, we partially apply the linearization $z = 1+(\ell_0+x)y$ and the basis matrices can be transformed into triangular. The size of the root for the linearized variable z is bounded by $Z := 3N^{1/2+\beta}$. In general, we reveal the following property.

Lemma 2. *We define the polynomial order $\prec$ as*

$$g_{[u,i]}^{MSBs1}(x,y), g_{[u,j]}^{MSBs2}(x,y) \prec g_{[u',i']}^{MSBs1}(x,y), g_{[u',j']}^{MSBs2}(x,y), \text{ if } u<u',$$
$$g_{[u,i]}^{MSBs1}(x,y) \prec g_{[u',j']}^{MSBs2}(x,y), \text{ if } u=u'$$
$$g_{[u,i]}^{MSBs1}(x,y) \prec g_{[u',i']}^{MSBs1}(x,y), \text{ if } u=u', i<i',$$
$$g_{[u,j]}^{MSBs2}(x,y) \prec g_{[u',j']}^{MSBs2}(x,y), \text{ if } u=u', j<j'.$$

Ordered in this way, the basis matrices become triangular with 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* $g_{[u,i]}^{MSBs1}(x,y)$*, 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* $g_{[u,j]}^{MSBs2}(x,y)$*, where*

$$l^{MSBs}(k) := \max\left\{0, \frac{k-2(\beta-\gamma)m}{2+2\gamma-4\beta}\right\}.$$

The proof is written in the full version.

The linearization technique enables us to select shift-polynomials more flexibly with the constraint for basis matrices to be triangular. Therefore, we can eliminate some unhelpful polynomials and add helpful polynomials compared with Sarkar et al.'s basis matrices. To maximize the solvable root bounds, our collections of shift-polynomials are determined by the following lemma.

Lemma 3. *When $\beta \le 1/2$, assume there are shift-polynomials $g_{[u,i]}^{MSBs1}(x,y)$ for $u=u'+j',\ldots,m, i=u'+j'$ and $g_{[u,j]}^{MSBs2}(x,y)$ for $u=u'+1,\ldots,u'+j'-1, j=u'+j'-u$ in lattice bases. In this case, shift-polynomials $g_{[u',j']}^{MSBs2}(x,y)$ are helpful polynomials when $u'=0,1,\ldots,m, j'=1,\ldots,\lfloor 2(\beta-\gamma)+(1+2\gamma-4\beta)u\rfloor$. Shift-polynomials $g_{[u',j']}^{MSBs2}(x,y)$ are unhelpful polynomials when $u'=0,1,\ldots,m, j'>2(\beta-\gamma)+(1+2\gamma-4\beta)u'$.*

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

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

$$\approx N^{\frac{1}{2}j'+\left(\frac{1}{2}+\beta\right)u'+m-u'-(\beta-\gamma)(m-u')}.$$

This value is smaller than the size of the modulus $e^m \approx N^m$, when

$$j' \leq 2(\beta-\delta)m + (1+2\delta-4\beta)u'.$$

That is, Lemma 3 is proved. □

We prove the bound (i) of Theorem 1. We can rewrite the diagonals as $X^{u'-\lceil l^{MSBs}(j')\rceil}Y^{j'-\lceil l^{MSBs}(j')\rceil}Z^{\lceil l^{MSBs}(j')\rceil}e^{m-\min\{u',j'\}}$ for $j'=0,1,\ldots,2(1-\beta)m, u'=\lceil l^{MSBs}(j')\rceil,\ldots,m$. Ignoring low order terms of m, we compute the dimension

$$n = \sum_{j'=0}^{\lfloor 2(1-\beta)m\rfloor} \sum_{u'=\lceil l^{MSBs}(j)\rceil}^{m} 1 = \left(\frac{1}{2}+2(\beta-\gamma)+\frac{1+2\gamma-4\beta}{2}\right)m^2,$$

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

$$\begin{aligned}
s_X &= \sum_{j'=0}^{\lfloor 2(1-\beta)m\rfloor} \sum_{u'=\lceil l^{MSBs}(j)\rceil}^{m} (u'-\lceil l^{MSBs}(j')\rceil) \\
&= \left(\frac{1}{6}+(\beta-\gamma)+\frac{1+2\gamma-4\beta}{6}\right)m^3, \\
s_Y &= \sum_{j'=0}^{\lfloor 2(1-\beta)m\rfloor} \sum_{u'=\lceil l^{MSBs}(j)\rceil}^{m} (j'-\lceil l^{MSBs}(j')\rceil) \\
&= ((\beta-\gamma)+2(\beta-\gamma)^2+(\beta-\gamma)(1+2\gamma-4\beta)+\frac{1+2\gamma-4\beta}{6} \\
&+\frac{(1+2\gamma-4\beta)^2}{6})m^3, \\
s_Z &= \sum_{j'=0}^{\lfloor 2(1-\beta)m\rfloor} \sum_{u'=\lceil l^{MSBs}(j')\rceil}^{m} \lceil l^{MSBs}(j')\rceil = \left(\frac{1}{6}+\frac{1+2\gamma-4\beta}{6}\right)m^3, \\
s_e &= \sum_{j'=0}^{\lfloor 2(1-\beta)m\rfloor} \sum_{u'=\lceil l^{MSBs}(j)\rceil}^{m} (m-\min\{u',j'\}) \\
&= \left(\frac{1}{3}+(\beta-\gamma)+\frac{1+2\gamma-4\beta}{6}\right)m^3,
\end{aligned}$$

We can find solutions of $f_{MSBs}(x,y)=0$ provided that $(\det(B))^{1/n} < e^m$, that is,

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

This condition yields the bound

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

It is clear that $\gamma = \max\{\delta, \beta - 1/2\} = \delta$ when $\beta \leq 1/2$. Therefore, the bound (i) of Theorem 1 is proved.

For Larger *d*. In the following, we briefly summarize the case for $1/2 < \beta \leq 9/16$. The detailed analysis is written in the full version.

When $\beta > 1/2$, $2(\beta-\gamma)m+(1+2\gamma-4\beta)u < 0$ for larger $u > -2(\beta-\gamma)m/(1+2\gamma-4\beta)$. Since we select shift-polynomials $g^{MSBs1}_{[u,i]}(x,y)$ for $-2(\beta-\gamma)m/(1+2\gamma-4\beta) < u \leq m$ which are unhelpful polynomials and do not contribute for basis matrices to be triangular, we should redefine collections of shift-polynomials. We use shift-polynomials

$$\begin{aligned}
&g^{MSBs1}_{[u,i]}(x,y) \text{ with } u = 0,1,\ldots,m, i = 0,1,\ldots,\min\{u,t\},\\
&g^{MSBs2}_{[u,j]}(x,y) \text{ with } u = 0,1,\ldots,m,\\
&\qquad\qquad j = 1,2,\ldots,\min\{\lfloor 2(\beta-\gamma)m+(1+2\gamma-4\beta)u\rfloor, t-u\},
\end{aligned}$$

in the lattice bases. The parameter $\tau = t/m$ should be optimized later[2]. The selections of shift-polynomials generate basis matrices which are not triangular. However, we partially apply the linearization $z = 1 + (l_0 + x)y$ and the basis matrices can be transformed into triangular. That means Lemma 2 holds.

We prove the bound (ii) of Theorem 1. We can rewrite the diagonals as $X^{u'-\lceil l^{MSBs}(j')\rceil}Y^{j'-\lceil l^{MSBs}(j')\rceil}Z^{\lceil l^{MSBs}(j')\rceil}e^{m-\min\{u',j'\}}$ for $j' = 0,1,\ldots,t, u' = \lceil l^{MSBs}(j)\rceil, \lceil l^{MSBs}(j)\rceil + 1, \ldots, m$. Ignoring low order term of m, we compute the dimension

$$n = \sum_{j'=0}^{t} \sum_{u'=\lceil l^{MSBs}(j)\rceil}^{m} 1 = mt - \frac{1}{2}\cdot\frac{(t-2(\beta-\gamma)m)^2}{2+2\gamma-4\beta},$$

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

$$\begin{aligned}
s_X &= \sum_{j'=0}^{t} \sum_{u'=\lceil l^{MSBs}(j')\rceil}^{m} (u' - \lceil l^{MSBs}(j')\rceil)\\
&= \frac{m^2t}{2} - \frac{1}{6}\cdot\frac{(t-2(\beta-\gamma)m)^3}{(2+2\gamma-4\beta)^2} - s_Z,\\
s_Y + s_Z &= \sum_{j'=0}^{t} \sum_{u'=\lceil l^{MSBs}(j')\rceil}^{m} j'
\end{aligned}$$

[2] These collections and optimization of the parameter τ are based on the notion of *consecutive helpful polynomials* defined in [30]. See the paper in detail.

$$= \frac{1}{6} \cdot \frac{t^3 - 8(\beta-\gamma)^3 m^3}{2+2\gamma-4\beta} + \frac{t^2}{2}\left(m - \frac{t-2(\beta-\gamma)m}{2+2\gamma-4\beta}\right)$$

$$s_Z = \sum_{j'=0}^{t} \sum_{u'=\lceil l^{MSBs}(j')\rceil}^{m} \lceil l^{MSBs}(j')\rceil$$

$$= \frac{m}{2} \cdot \frac{(t-2(\beta-\gamma)m)^2}{2+2\gamma-4\beta} - \frac{1}{3} \cdot \frac{(t-2(\beta-\gamma)m)^3}{(2+2\gamma-4\beta)^2}$$

$$s_e = \sum_{j'=0}^{t} \sum_{u'=\lceil l^{MSBs}(j')\rceil}^{m} (m - \min\{u', j'\})$$

$$= -\frac{m}{2} \cdot \frac{(t-2(\beta-\gamma)m)^2}{2+2\gamma-4\beta} + \frac{1}{6} \cdot \frac{(t-2(\beta-\gamma)m)^3}{(2+2\gamma-4\beta)^2} + m^2 t - \frac{mt^2}{2} + \frac{1}{6}t^3$$

We can find solutions $f_{MSBs}(x, y) = 0$ provided that $(\det(B))^{1/n} < e^m$, that is,

$$\gamma\tau - \frac{\tau^2}{2} + \frac{\tau^3}{3} < \frac{1}{6} \cdot \frac{(\tau - 2(\beta-\gamma))^3}{2+2\gamma-4\beta}.$$

Note that Sarkar et al.'s condition can be written as $\gamma\tau - \tau^2/2 + \tau^3/3 < 0$ with $\tau = (1/4-\gamma)/\gamma$. We can improve the result since $\tau - 2(\beta-\gamma) > 0, 2+2\gamma-4\beta > 0$ and the right hand side of the inequality is positive. To maximize the solvable root bound, we set the parameter

$$\tau = 1 - \frac{2\beta - 1}{1 - 2\sqrt{1+\gamma-2\beta}}$$

and obtain the bound (ii) of Theorem 1.

5 Partial Key Exposure Attack: The Least Significant Bits Case

5.1 Previous Works

In the LSBs partial key exposure case, Ernst et al. [13] found the small roots of polynomials over the integers

$$g^{EMJW3}(x, y, z) = 1 - ed_0 + eMx + y(N+z),$$

to factor N. The polynomial $g^{EJMW3}(x, y, z)$ has the roots $(x, y) = (-d_1, \ell, -(p+q-1))$. Their algorithm works provided that

$$\delta \le \frac{5}{6} - \frac{1}{3}\sqrt{1+6\beta} - \epsilon.$$

When $\delta = \beta$, the condition yields Boneh and Durfee's weaker bound [5] $\beta < (7-2\sqrt{7})/6$.

Blömer and May [4] consider LSBs key exposure attacks with small public exponents e and full size secret exponents d. Though the situation is slightly different from the one considered in this paper, their lattice construction provides the same bound as Ernst et al.'s algorithm. Blömer and May solve the modular equation $f_{LSBs}(x,y)=0$ to factor N. To solve the modular equation, they used shift-polynomials

$$g_{[u,i]}^{LSBs1}(x,y) := x^{u-i} f_{LSBs}(x,y)^i (eM)^{m-i},$$
$$g_{[u,j]}^{LSBs2}(x,y) := y^j f_{LSBs}(x,y)^u (eM)^{m-u}.$$

Both shift-polynomials modulo $(eM)^m$ have the same roots as the original solutions, that is, $g_{[u,i]}^{LSBs1}(\ell, -(p+q-1)) = 0 \pmod{(eM)^m}$, $g_{[u,j]}^{LSBs2}(\ell, -(p+q-1)) = 0 \pmod{(eM)^m}$. They selected shift-polynomials

$$g_{[u,i]}^{LSBs1}(x,y) \text{ with } u=0,1,\ldots,m, i=0,1,\ldots,u,$$
$$g_{[u,j]}^{LSBs2}(x,y) \text{ with } u=0,1,\ldots,m, j=1,2,\ldots,\lfloor(1-2\delta)m/2\rfloor,$$

in the lattice bases. This selections generate triangular basis matrices with diagonals $X^uY^ie^{m-i}$ for $g_{[u,i]}^{LSBs1}(x,y)$, and $X^uY^{u+j}e^{m-u}$ for $g_{[u,j]}^{LSBs2}(x,y)$. Their algorithm works provided that $\delta \leq \frac{5}{6} - \frac{1}{3}\sqrt{1+6\beta} - \epsilon$. The bound corresponds to Ernst et al.'s bound.

Aono [1] improved the attack and firstly achieved Boneh and Durfee's stronger bound [5]. To improve the bound, Aono considered the other modular polynomial,

$$f_{LSBs1}(x,y) = 1 + x(N+y) \pmod{e}.$$

The roots of the polynomials are $(x,y) = (\ell, -(p+q-1))$ which are the same as $f_{LSBs}(x,y)$. To construct the basis matrix, Aono used shift-polynomials $g_{[u,i]}^{LSBs1}, g_{[u,j]}^{LSBs2}(x,y)$, and

$$g_{[u,k]}^{LSBs3}(x,y) := y^k f_{LSBs1}(x,y)^u e^{m-u} M^m.$$

Shift-polynomials $g_{[u,k]}^{LSBs3}(x,y)$ modulo $(eM)^m$ have the same roots as the original solutions, that is, $g_{[u,k]}^{LSBs3}(\ell, -(p+q-1)) = 0 \pmod{(eM)^m}$. Aono selected shift-polynomials

$$g_{[u,i]}^{LSBs1}(x,y) \text{ with } u=0,1,\ldots,m, i=0,1,\ldots,u,$$
$$g_{[u,j]}^{LSBs2}(x,y) \text{ with } u=0,1,\ldots,m, j=1,2,\ldots,t,$$
$$g_{[u,k]}^{LSBs3}(x,y) \text{ with } u=\lceil t/(1-2\beta)\rceil, \lceil t/(1-2\beta)\rceil+1,\ldots,m,$$
$$k=t+1,t+2,\ldots,\lfloor(1-2\beta)u\rfloor,$$

with $t = \sqrt{2(1-2\beta)(\beta-\delta)}m$ in the lattice bases. This selections of shift-polynomials generate basis matrices which are not triangular. Aono bounded the determinant of the lattice by computing Gram-Schmidt orthogonal bases. The algorithm works provided that

$$2\beta^2 - 3\beta + 2\tau(\beta-\delta) - \delta + 1 > 0,$$

when $1+2\delta-4\beta>0$. When $\delta=\beta$, this yields Boneh and Durfee's stronger bound $\beta<1-1/\sqrt{2}$. When $1+2\delta-4\beta\leq 0$, Aono's lattice construction becomes the same as Blömer and May [4].

5.2 Our Observation of Aono's Lattice Using Unravelled Linearization

As we showed, the basis matrix constructed by Aono [1] is not triangular. However, we reveal that the basis matrix can be transformed into triangular with linearization $z=1+xy$. The size of the root for the linearized variable z is bounded by $Z:=3N^{1/2+\beta}$.

Lemma 4. *We define the polynomial order $\prec$ as*

$$\begin{aligned}
&g^{LSBs1}_{[u,i]}(x,y)\prec g^{LSBs2}_{[u,j]}(x,y)\prec g^{LSBs3}_{[u,k]}(x,y),\\
&g^{LSBs1}_{[u,i]}(x,y)\prec g^{LSBs1}_{[u',i']}(x,y),\ \textit{if}\ u<u'\ \textit{or}\ u=u',i<i',\\
&g^{LSBs2}_{[u,j]}(x,y)\prec g^{LSBs2}_{[u',j']}(x,y),\ \textit{if}\ u<u'\ \textit{or}\ u=u',j<j',\\
&g^{LSBs3}_{[u,k]}(x,y)\prec g^{LSBs3}_{[u',k']}(x,y),\ \textit{if}\ u<u'\ \textit{or}\ u=u',k<k'.
\end{aligned}$$

Ordered in this way, the basis matrix becomes triangular with diagonals $X^uY^i\times(eM)^{m-i}$ for $g^{LSBs1}_{[u,i]}(x,y)$, $X^uY^{u+j}(eM)^{m-u}$ for $g^{LSBs2}_{[u,j]}(x,y)$, and $Y^kZ^u\times e^{m-u}M^m$ for $g^{LSBs3}_{[u,k]}(x,y)$.

The proof is written in the full version.

5.3 Our Lattice Constructions

In this section, we propose the improved algorithm for LSBs partial key exposure attacks when $1+2\delta-4\beta>0$. We change the shift-polynomials used in the lattice bases. We use the shift-polynomial $g^{LSBs1}_{[u,i]}(x,y)$, and

$$\begin{aligned}
g^{LSBs4}_{[u,k]}(x,y):=y^kf_{LSBs}(x,y)^{u-\lceil l^{LSBs}(k)\rceil}f_{LSBs1}(x,y)^{\lceil l^{LSBs}(k)\rceil}\\
\times e^{m-u}M^{m-(u-\lceil l^{LSBs}(k)\rceil)},
\end{aligned}$$

where

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

Shift-polynomials $g^{LSBs4}_{[u,k]}(x,y)$ modulo $(eM)^m$ have the same roots as the original solutions, that is, $g^{LSBs4}_{[u,k]}(\ell,-(p+q-1))=0\pmod{(eM)^m}$. We selected shift-polynomials

$g^{LSBs1}_{[u,i]}(x,y)$ with $u=0,1,\ldots,m,i=0,1,\ldots,u$,
$g^{LSBs4}_{[u,k]}(x,y)$ with $u=0,1,\ldots,m,k=1,2,\ldots,\lfloor 2(\beta-\delta)m+(1+2\delta-4\beta)u\rfloor$,

in the lattice bases. Though the selections generate basis matrices which are not triangular, we partially apply the linearization $z = 1 + xy$ and the basis matrix can be transformed into triangular. In general, we reveal the following property.

Lemma 5. *We define the polynomial order* $\prec$ *as*

$$\begin{aligned}
&g^{LSBs1}_{[u,i]}(x,y) \prec g^{LSBs4}_{[u,k]}(x,y),\\
&g^{LSBs1}_{[u,i]}(x,y) \prec g^{LSBs1}_{[u',i']}(x,y), \ \textit{if } u < u' \ \textit{or } u = u', i < i',\\
&g^{LSBs4}_{[u,k]}(x,y) \prec g^{LSBs4}_{[u',k']}(x,y), \ \textit{if } u < u' \ \textit{or } u = u', k < k'.
\end{aligned}$$

Ordered in this way, the basis matrix becomes triangular with diagonals $X^uY^i \times (eM)^{m-i}$ *for* $g^{LSBs1}_{[u,i]}(x,y)$*, and* $X^{u-\lceil l^{LSBs}(k)\rceil}Y^{u-\lceil l^{LSBs}(k)\rceil+k}Z^{\lceil l^{LSBs}(k)\rceil} \times e^{m-u} M^{m-(u-\lceil l^{LSBs}(k)\rceil)}$ *for* $g^{LSBs4}_{[u,k]}(x,y)$*.*

The proof is written in the full version.

Lemmas 4, 5 clarify the point of our improvements. When $l^{LSBs}(k) = 0$, $g^{LSBs4}_{[u,k]}(x,y) = g^{LSBs2}_{[u,k]}(x,y)$. When $l^{LSBs}(k) > 0$, the diagonals of $g^{LSBs4}_{[u,k]}(x,y)$ in our basis matrices are smaller than that of $g^{LSBs3}_{[u,k]}(x,y)$ in Aono's basis matrices with respect to powers of M. Therefore, we can improve the bound when shift-polynomials $g^{LSBs4}_{[u,k]}(x,y)$ with $l^{LSBs}(k) > 0$ are used.

To maximize the solvable root bounds, our collection of shift-polynomials is determined by the following lemma.

Lemma 6. *Assume that there are shift-polynomials* $g^{LSBs4}_{[u,k]}(x,y)$ *for* $(u,k) = (u'+1, k'+1), (u'+2, k'+2), \ldots, (m, m-u'+k')$ *in* B*. Shift-polynomials* $g^{LSBs4}_{[u',k']}(x,y)$ *are helpful polynomials when* $u' = 0, 1, \ldots, m, k' = 1, 2, \ldots, \lfloor 2(\beta-\delta)m + (1+2\delta-4\beta)u\rfloor$*. Shift-polynomials* $g^{LSBs4}_{[u',k']}(x,y)$ *are unhelpful polynomials when* $u' = 0, 1, \ldots, m, k' > 2(\beta-\delta)m + (1+2\delta-4\beta)u'$*.*

Proof. Consider the basis matrix B. We add a new shift-polynomial $g^{LSBs4}_{[u',k']}(x,y)$ and construct the basis matrix B^+. The value $\det(B^+)/\det(B)$ can be computed as

$$\begin{aligned}
\frac{\det(B^+)}{\det(B)} &= Y^{k'}Z^{u'}e^{m-u'}M^m \times \left(\frac{1}{M}\right)^{u'}\\
&\approx N^{\frac{1}{2}k' + \left(\frac{1}{2}+\beta\right)u' + m - u' + (\beta-\delta)u'}.
\end{aligned}$$

This value is smaller than the size of the modulus $(eM)^m \approx N^{(1+\beta-\delta)m}$, when

$$j' \leq 2(\beta-\delta)m + (1+2\delta-4\beta)u'.$$

That is, Lemma 6 is proved. □

Note that Lemma 6 does not hold when $1 + 2\delta - 4\beta < 0$. Since our assumption that there are shift-polynomials $g^{LSBs4}_{[u,k]}(x,y)$ for $(u,k) = (u'+1, k'+1), (u'+2, k'+2), \ldots, (m, m-u'+k')$ in B does not hold.

We prove the bound of Theorem 2. Ignoring low order terms of m, we compute the dimension

$$n=\sum_{u=0}^{m}\sum_{i=0}^{u}1+\sum_{u=0}^{m}\sum_{k=1}^{\lfloor 2(\beta-\delta)m+(1+2\delta-4\beta)u\rfloor}1=\left(\frac{1}{2}+2(\beta-\delta)+\frac{1+2\delta-4\beta}{2}\right)m^2,$$

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

$$\begin{aligned}
s_X&=\sum_{u=0}^{m}\sum_{i=0}^{u}(u-i)=\frac{1}{3}m^3,\\
s_Y&=\sum_{u=0}^{m}\sum_{i=0}^{u}i+\sum_{u=0}^{m}\sum_{k=1}^{\lfloor 2(\beta-\delta)m+(1+2\delta-4\beta)u\rfloor}k\\
&=\left(\frac{1}{6}+2(\beta-\delta)^2+(\beta-\delta)(1+2\delta-4\beta)+\frac{(1+2\delta-4\beta)^2}{6}\right)m^3,\\
s_Z&=\sum_{u=0}^{m}\sum_{k=1}^{\lfloor 2(\beta-\delta)m+(1+2\delta-4\beta)u\rfloor}u=\left((\beta-\delta)+\frac{1+2\delta-4\beta}{3}\right)m^3,\\
s_e&=\sum_{u=0}^{m}\sum_{i=0}^{u}(m-i)+\sum_{u=0}^{m}\sum_{k=1}^{\lfloor 2(\beta-\delta)m+(1+2\delta-4\beta)u\rfloor}(m-u)\\
&=\left(\frac{1}{3}+(\beta-\delta)+\frac{1+2\delta-4\beta}{6}\right)m^3,\\
s_M&=\sum_{u=0}^{m}\sum_{i=0}^{u}(m-i)+\sum_{u=0}^{m}\sum_{k=1}^{\lfloor 2(\beta-\delta)m+(1+2\delta-4\beta)u\rfloor}(m-(u-\lceil l^{LSBs}(k)\rceil))\\
&=\left(\frac{1}{3}+(\beta-\delta)+\frac{1+2\delta-4\beta}{3}\right)m^3.
\end{aligned}$$

We can find solutions of $f_{LSBs}(x,y)=0, f_{LSBs1}(x,y)=0$ provided that $(\det(B))^{1/n}<(eM)^m$, that is,

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

This condition yields the bound

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

Therefore, the bound of Theorem 2 is proved.

References

1. Aono, Y.: A new lattice construction for partial key exposure attack for RSA. In: Jarecki, S., Tsudik, G. (eds.) PKC 2009. LNCS, vol. 5443, pp. 34–53. Springer, Heidelberg (2009)

2. Bauer, A., Vergnaud, D., Zapalowicz, J.-C.: Inferring sequences produced by nonlinear pseudorandom number generators using Coppersmith's methods. In: Fischlin, M., Buchmann, J., Manulis, M. (eds.) PKC 2012. LNCS, vol. 7293, pp. 609–626. Springer, Heidelberg (2012)
3. Bernstein, D.J., Chang, Y.-A., Cheng, C.-M., Chou, L.-P., Heninger, N., Lange, T., van Someren, N.: Factoring RSA keys from certified smart cards: Coppersmith in the wild. In: Sako, K., Sarkar, P. (eds.) ASIACRYPT 2013, Part II. LNCS, vol. 8270, pp. 341–360. Springer, Heidelberg (2013)
4. 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)
5. 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)
6. 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)
7. Cohn, H., Heninger, N.: Approximate common divisors via lattices. In: ANTS-X, 2012. IACR Cryptology ePrint Archive, Report 2011/437 (2011). http://eprint.iacr.org/2011/437
8. 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)
9. 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)
10. Coppersmith, D.: Small solutions to polynomial equations, and low exponent RSA vulnerabilities. J. Cryptol. **10**(4), 233–260 (1997)
11. 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)
12. 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)
13. 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)
14. Halderman, J.A., Schoen, S.D., Heninger, N., Clarkson, W., Paul, W., Calandrino, J.A., Feldman, A.J., Appelbaum, J., Felten, E.W.: Lest we remember: cold boot attacks on encryption keys. In: Proceedings of the USENIX Security Symposium 2008, pp. 45–60 (2008)
15. Henecka, W., May, A., Meurer, A.: Correcting errors in RSA private keys. In: Rabin, T. (ed.) CRYPTO 2010. LNCS, vol. 6223, pp. 351–369. Springer, Heidelberg (2010)
16. Heninger, N., Shacham, H.: Reconstructing RSA private keys from random key bits. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 1–17. Springer, Heidelberg (2009)
17. Herrmann, M., May, A.: Solving linear equations modulo divisors: on factoring given any bits. In: Pieprzyk, J. (ed.) ASIACRYPT 2008. LNCS, vol. 5350, pp. 406–424. Springer, Heidelberg (2008)
18. Herrmann, M., May, A.: Attacking power generators using unravelled linearization: when do we output too much? In: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, vol. 5912, pp. 487–504. Springer, Heidelberg (2009)

19. 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)
20. Howgrave-Graham, N.: Finding small roots of univariate modular equations revisited. In: Darnell, Michael J. (ed.) Cryptography and Coding 1997. LNCS, vol. 1355, pp. 131–142. Springer, Heidelberg (1997)
21. Kunihiro, N.: On optimal bounds of small inverse problems and approximate GCD problems with higher degree. In: Gollmann, D., Freiling, F.C. (eds.) ISC 2012. LNCS, vol. 7483, pp. 55–69. Springer, Heidelberg (2012)
22. Kunihiro, N., Honda, J.: RSA meets DPA: recovering RSA secret keys from noisy analog data. IACR Cryptology ePrint Archive, Report 2014/513 (2014). http://eprint.iacr.org/2014/513
23. Kunihiro, N., Shinohara, N., Izu, T.: Recovering RSA secret keys from noisy key bits with erasures and errors. In: Kurosawa, K., Hanaoka, G. (eds.) PKC 2013. LNCS, vol. 7778, pp. 180–197. Springer, Heidelberg (2013)
24. Lenstra, A.K., Lenstra Jr., H.W., Lovász, L.: Factoring polynomials with rational coefficients. Math. Ann. **261**, 515–534 (1982)
25. May, A.: New RSA vulnerabilities using lattice reduction methods. Ph.D. thesis, University of Paderborn (2003)
26. May, A.: Using LLL-reduction for solving RSA and factorization problems: a survey (2010). http://www.cits.rub.de/permonen/may.html
27. 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)
28. Paterson, K.G., Polychroniadou, A., Sibborn, D.L.: A coding-theoretic approach to recovering noisy RSA keys. In: Wang, X., Sako, K. (eds.) ASIACRYPT 2012. LNCS, vol. 7658, pp. 386–403. Springer, Heidelberg (2012)
29. 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)
30. Takayasu, A., Kunihiro, N.: Better lattice constructions for solving multivariate linear equations modulo unknown divisors. In: Boyd, C., Simpson, L. (eds.) ACISP. LNCS, vol. 7959, pp. 118–135. Springer, Heidelberg (2013)
31. Takayasu, A., Kunihiro, N.: Cryptanalysis of RSA with multiple small secret exponents. In: Susilo, W., Mu, Y. (eds.) ACISP 2014. LNCS, vol. 8544, pp. 176–191. Springer, Heidelberg (2014)
32. Wiener, M.J.: Cryptanalysis of short RSA secret exponents. IEEE Trans. Inf. theory **36**(3), 553–558 (1990)