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

†Atsushi Takayasu and ‡Noboru Kunihiro

May 25, 2018

Abstract

Thus far, several lattice-based algorithms for *partial key exposure attacks* on RSA, i.e., given the most/least significant bits (MSBs/LSBs) of a secret exponent d and factoring an RSA modulus N, have been proposed such as Blömer and May (Crypto'03), Ernst et al. (Eurocrypt'05), and Aono (PKC'09). Due to Boneh and Durfee's small secret exponent attack, partial key exposure attacks should always work for $d < N^{0.292}$ even without any partial information. However, it was difficult task to make use of the given partial information without losing the quality of Boneh-Durfee's attack. In particular, known partial key exposure attacks fail to work for $d < N^{0.292}$ with only few partial information. Such unnatural situation stems from the fact that the additional information makes underlying modular equations involved. In this paper, we propose improved attacks when a secret exponents d is small. Our attacks are better than all known previous attacks in the sense that our attacks require less partial information. Specifically, our attack is better than all known ones for $d < N^{0.5625}$ and $d < N^{0.368}$ with the MSBs and the LSBs, respectively. Furthermore, our attacks fully cover the Boneh-Durfee bound, i.e., they always work for $d < N^{0.292}$. At a high level, we obtain the improved attacks by fully utilizing *unravelled linearization technique* proposed by Herrmann and May (Asiacrypt'09). Although Herrmann and May (PKC'10) already applied the technique to Boneh-Durfee's attack, we show elegant and impressive extensions to capture partial key exposure attacks. More concretely, we construct structured triangular matrices that enable us to recover more useful algebraic structures of underlying modular polynomials. We embed the given MSBs/LSBs to the recovered algebraic structures and construct our partial key exposure attacks. In this full version, we provide overviews and explicit proofs of the triangular matrix constructions. We believe that the additional explanations help readers to understand our techniques.

*This is the full version of [TK14c].

†The University of Tokyo, National Institute of Advanced Industrial Science and Technology (AIST). e-mail: takayasu@mist.i.u-tokyo.ac.jp

‡The University of Tokyo

Contents

1 Introduction

1.1 Background

RSA is one of the most famous public key cryptosystems and numerous papers have studied the security. Let $N = pq$ be a public modulus, where p and q are distinct primes with the same bit-size. The bit-size of N should be sufficiently large so that the factorization is computationally hard. There are a public exponent e and a secret exponent d that satisfy $ed = 1 \mod \phi(N)$, where $\phi(N) = (p-1)(q-1)$ is Euler's totient function. During decryption/signing, heavy modular exponentiations $c^d \mod N$ should be computed. The most trivial way to reduce the computational cost is using small d. However, Wiener [Wie90] first reported that too small d makes RSA insecure. He claimed that there is a polynomial time algorithm for factoring N when $d < N^{1/4}$. Boneh and Durfee [BD00] revisited the attack by using lattice-based Coppersmith's method [Cop96b]. At first, they proposed an improved attack that works for $d < N^{(7-2\sqrt{7})/6} = N^{0.284\cdots}$. In the same work, they further improved the bound to $d < N^{1-1/\sqrt{2}} = N^{0.292\cdots}$. Throughout the paper, we call these bounds the Boneh-Durfee weaker and the stronger bound, respectively.

Boneh, Durfee, and Frankel [BDF98] introduced *partial key exposure attacks* on RSA, where the attackers are given the most/least significant bits (MSBs/LSBs) of full size d. The attack is theoretically interesting to study how many portions of secret information enable attackers to break the security of RSA. Although Boneh et al.'s partial key exposure attacks work only for small e, several improvements have been proposed by using Coppersmith's methods [Cop96a, Cop96b]. Blömer and May [BM03] improved the bound to $e < N^{7/8}$ with the LSBs of d. Ernst et al. [EJMdW05] proposed the first attack for full size e with the MSBs of d.

In the same work [EJMdW05], Ernst et al. also studied the attacks with the MSBs/LSBs of small d. By definition, the attack scenario is an extension of Boneh-Durfee's work [BD00]. Specifically, Boneh-Durfee's small secret exponent attack is a special case of the partial key exposure attack when the given partial information is exactly zero. Hence, Boneh and Durfee's result suggests that partial key exposure attacks should always work for $d < N^{0.292\cdots}$ even without any partial information. However, Ernst et al.'s attacks only cover the Boneh-Durfee weaker bound $d < N^{0.284\cdots}$ when the given partial information is exactly zero. Aono [Aon09] proposed the first attack to cover the Boneh-Durfee stronger bound with the LSBs of d. Aono's attack requires less partial information than Ernst et al.'s attack for $d < N^{(9-\sqrt{21})/12} = N^{0.368\cdots}$ to factor a modulus N. Unfortunately, a trick of Aono's algorithm is not applicable to the MSBs case. Hence, extending the Boneh-Durfee stronger attack with MSBs of d is still an interesting open problem.

1.2 Our Results

In this paper, we propose improved partial key exposure attacks on RSA with the MSBs/LSBs of d. Our attacks work with less partial information than the previous attacks [Aon09, BM03, EJMdW05, SSM10] for $d < N^{9/16} = N^{0.5625}$ and $d < N^{(9-\sqrt{21})/12} = N^{0.368\cdots}$ with the MSBs and the LSBs, respectively. Furthermore, the most impressive feature of our proposed attacks is that they always work for $d < N^{0.292\cdots}$ even when the given partial information is exactly zero. Therefore, our attack with the MSBs is the first one that cover the Boneh-Durfee stronger bound.

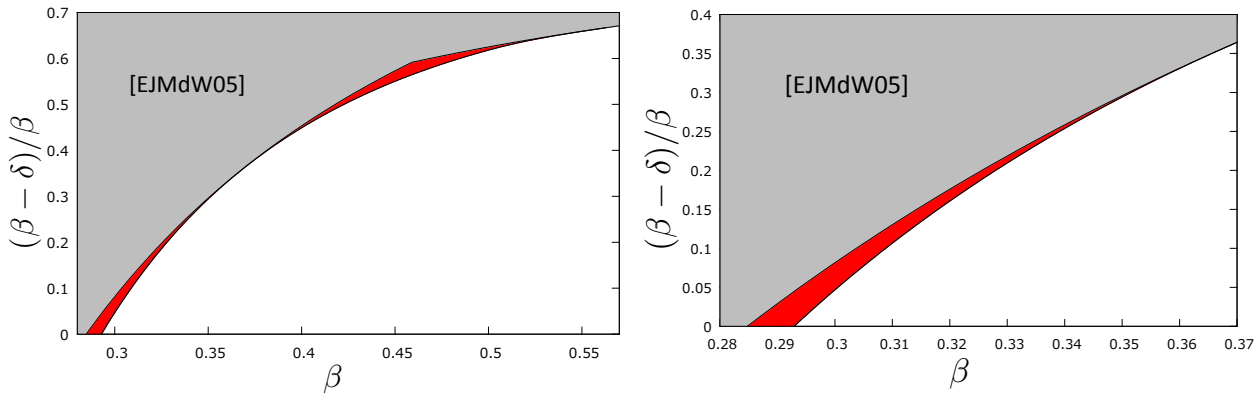

Figure 1: Comparison of attack conditions

Figure 1 compares attack conditions with Ernst et al's and ours. Since a condition of Aono's attack is close to ours, we do not compare it in the figure. The left and the right figure is for the MSBs and the LSBs, respectively. Horizontal axes and vertical axes represent sizes of secret exponents $\beta := \log_N d$ and ratios of exposed bits $(\beta - \delta)/\beta$, where δ represents sizes of d_1 which are unknown parts of d, respectively. Ernst et al.'s attacks work in the gray areas while our attack improve the red areas when β is small.

We also show numerical comparisons for attack conditions. Table 1 provides a comparison between Ernst et al.'s attack and our attack with the MSBs for $1 - 1/\sqrt{2} = 0.292\cdots \leq \beta \leq 9/16 = 0.5625$. Table 2 provides a comparison between Ernst et al.'s attack, Aono's attack, and our attack for $1 - 1/\sqrt{2} = 0.292\cdots \leq \beta \leq (9 - \sqrt{21})/12 = 0.368\cdots$. In such small β, our proposed attacks are better than other ones.

1.3 Technical Overview

Here, we summarize technical background of the work. Then, we explain a technical overview of our improvements.

Coppersmith's Methods. In 1996, Coppersmith [Cop96a, Cop96b] introduced lattice-based methods for solving integer/modular equations with small solutions in polynomial time. The methods first construct a matrix whose rows consist of coefficient vectors of polynomials that have the same roots as the original polynomials. Then, we apply the LLL reduction algorithm [LLL82] to the matrix. If the LLL outputs sufficiently short vectors, one can obtain the desired solutions. The methods are actively utilized to study the security of RSA including Boneh and Durfee's small secret exponent attack [BD00], and partial key exposure attacks [Aon09, BM03, EJMdW05, SSM10].

Some researchers believe that if there is an attack based on Coppersmith's integer equation solving method, there should be an analogous attack based on the modular equation solving method, and vice versa. For example, Blömer-May's [BM03] and Ernst et al.'s [EJMdW05] partial key exposure attacks with the LSBs work for the same condition, where the former/latter attack utilized the modular/integer equation solving method, respectively. However, to the best of our knowledge,

Table 1: Comparison of the recoverable bounds for partial key exposure attacks with the MSBs

β	Ernst et al.'s δ	Our δ
0.292893219	0.27982339	0.292893219
0.3	0.275559982	0.285994506
0.32	0.263733084	0.268592284
0.34	0.252146808	0.253706834
0.36	0.240787039	0.240910032
0.368118692	0.236237384	0.236237384
0.38	0.229640991	0.229891317
0.4	0.218697036	0.220416848
0.42	0.207944565	0.212305314
0.44	0.197373866	0.205412787
0.46	0.1875	0.199622776
0.48	0.1875	0.194839473
0.5	0.1875	0.190983006
0.52	0.1875	0.188518542
0.54	0.1875	0.187647679
0.5625	0.1875	0.1875

there are several counterexamples. The most basic example is Boneh-Durfee's attack [BD00]. Boneh and Durfee utilized Coppersmith's modular equation solving method to construct their attack. After the proposal, numerous papers have studied several variants of the attack. Then, integer equation solving analogue has been reported for the Boneh-Durfee weaker bound $d < N^{0.284\cdots}$. However, such analogue has not been reported for the stronger bound $d < N^{0.292\cdots}$.

Due to the situation, solving modular equations seems an appropriate approach to construct partial key exposure attacks that cover the Boneh-Durfee stronger bound. Indeed, Aono [Aon09] took the approach and obtained the desired attack with the LSBs. Hence, Sarkar et al. [SSM10] tried to improve partial key exposure attacks with the MSBs by solving modular equations. However, what they obtained is the same attack condition as Ernst et al. for $N^{235/512} = N^{0.458\cdots} \leq d \leq N^{11/16} = N^{0.6875}$.

Unraveled Linearization. As we claimed above, Coppersmith's methods can solve modular equations whose solutions are small in polynomial time. Constructing partial key exposure attacks with less partial information is equivalent to constructing modular equation solving algorithms that can find larger solutions. Technically, it is further equivalent to constructing basis matrices such that lattices spanned by the matrices have shorter vectors. How to construct such matrices is the most technical part in this research area. To resolve the technical issue, Jochemsz and May [JM06] introduced a strategy for the matrix construction. Since the strategy is easy to understand, most works follow it including partial key exposure attacks of Blömer-May [BM03], Ernst et al. [EJMdW05], and Sarkar et al. [SSM10]. However, the fact does not mean that the Jochemsz-May strategy

Table 2: Comparison of the recoverable bounds for partial key exposure attacks with the LSBs

β	Ernst et al.'s δ	Aono's δ	Our δ
0.292893219	0.27982339	0.292893219	0.292893219
0.3	0.275559982	0.283716	0.285994506
0.31	0.269615516	0.274073	0.276945771
0.32	0.263733084	0.266059	0.268592284
0.33	0.257910783	0.259	0.260865122
0.34	0.252146808	0.252565	0.253706834
0.35	0.246439438	0.246548	0.247068931
0.36	0.240787039	0.240796	0.240910032
0.368118692	0.236237384	0.236237384	0.236237384

always enables ones to construct optimal algorithms. For example, by following the strategy, we obtain the Boneh-Durfee weaker attack. Constructing the stronger one requires a more technical matrix construction. Matrices obtained by the Jochemsz-May strategy are always triangular. Since computing determinants of large matrices is essential task to obtain attack conditions of modular equation solving algorithms, triangular ones simplify the analyses. However, Boneh and Durfee constructed non-triangular matrices to obtain the stronger bound with highly technical analyses. Due to the fact, there were several attacks [Aon13, DN00, Sar14, Sar16] that are extensions of Boneh-Durfee's attack, however, cover only the weaker attack.

In 2009, Herrmann and May [HM09] introduced a novel technique which they called *unraveled linearization*. They aimed at introducing the technique to solve nonlinear modular equations. For the purpose, the technique first applies *linearization* and obtain new *linearized variables*; the linearization combines several monomials into one monomial. Although the linearization has been already taken by numerous papers, the unraveled linearization technique has an additional trick. Reducing the number of monomials has benefit in general, however, the linearization may lose some algebraic information. Hence, during the matrix construction, the technique also applies *unraveling* that cancels the linearization and separates the combined monomials as they were. The unraveling enables ones to recover the lost algebraic structures. In other words, the unraveled linearization transforms non-triangular basis matrices to triangular ones. Furthermore, if we can apply appropriate unraveling, the matrices preserve useful algebraic structures. Indeed, Herrmann and May [HM10] provided a simpler proof of the Boneh-Durfee stronger attack. After the proposal, the unraveled linearization technique has been intensively utilized to improve several lattice-based attacks on RSA [BVZ12, Her11, HM10, HHX14, Kun12, KSI14, TK14b, TK14c, TK16a, TK16c, TK17a, TK17b].

Our Approach. In this paper, we fully utilize the unraveled linearization technique and improve partial key exposure attacks with the MSBs/LSBs of d by solving modular equations. In this full version, to help readers to understand our techniques easily, we first provide an alternative proof of the Boneh-Durfee stronger attack. Although the proof does not have any advantages for the attack,

it enables readers to easily understand our subsequent matrix constructions of partial key exposure attacks. In the proof, we apply additional unraveling to Herrmann-May's triangular matrix while the matrix is still triangular. It means that our triangular matrix recovers lost algebraic structures from Herrmann-May's one. Although the recovered algebraic structures do not affect the attack condition of the Boneh-Durfee, they are useful for partial key exposure attacks. Specifically, the recovered structures will enable us to embed the partial information of d.

We provide an improved partial key exposure attack with the MSBs of d by solving modular equations. As we claimed above, Sarkar et al.'s attack [SSM10] is a modular equation solving analogue of Ernst et al.'s attack [EJMdW05] for $N^{0.458\cdots} \leq d \leq N^{0.6875}$. In this full version, before providing our improved attack, we first construct modular equation solving analogue of Ernst et al.'s attack for $N^{0.284\cdots} \leq d \leq N^{0.458\cdots}$. The analogous attack can be viewed as an extension of the Boneh-Durfee weaker attack that utilize the given MSBs of d. We believe that the attack helps readers to understand how to embed the partial information in Boneh-Durfee's matrix. Then, we provide our main attack that can be viewed as an extension of the Boneh-Durfee stronger attack with the partial information. We construct the attack by embedding the partial information in Boneh-Durfee's stronger matrix with additional unraveling. To this end, our additional unraveling becomes effective. Herrmann-May's matrix does not preserve enough algebraic structures to embed the given partial information. On the other hand, by applying additional unraveling, we recovered lost algebraic structures that are useful to embed the partial information. As a result, we can successfully construct the partial key exposure attack that is an extension of the Boneh-Durfee stronger attack.

Next, we provide an improved partial key exposure attack with the LSBs of d by solving modular equations. As we suggested above, Blömer-May's attack [BM03] works for the same condition as Ernst et al.'s attack [EJMdW05] and it can be viewed as an extension of the Boneh-Durfee weaker attack that utilized the given LSBs of d. Hence, the result tells us how to embed the given partial information in Boneh-Durfee's weaker matrix. To improve the attack, Aono [Aon09] constructed a matrix that has two layers. The first layer is the same as Blömer-May's matrix while the second layer is the same as Boneh-Durfee's stronger matrix. The second layer did not utilize the partial information at all, however, it was effective to improve Blömer-May's attack. Although Aono analyzed non-triangular basis matrices, we can obtain the same attack condition by using Herrmann-May's matrix, which does not have much algebraic structures to embed the given partial information, in the second layer. In our attack, we construct a matrix, where the second layer is replaced by Boneh-Durfee's stronger matrix with additional unraveling. Since the matrix has more algebraic structures to embed partial information than Aono's one, we can successfully improve the attack.

1.4 Related Works

Boneh-Dufee's small secret exponent attack [BD00] is one of the most famous application of Coppersmith's methods [Cop96a, Cop96b]. Thus far, several variants of the attack has been proposed. They include attacks on RSA variants, e.g., unbalanced RSA [DN00, TK16d], prime power RSA [LZPL15, Sar14, Sar16, TK16a], Takagi's RSA [IKK08, IKK09, TK16a], multi-prime RSA [Hin08], and RSA with multiple exponent pairs [TK14b], and its mathematical exten-

sions [Kun11, Kun12, KSI14, TK17a]. Recently, Aono et al. [AASW18] found an optimality of the Boneh-Durfee stronger attack under heuristic assumptions. As similar settings, there are small CRT exponent attacks [TLP17]. Similarly, there are several partial key exposure on RSA variants, e.g., prime power RSA [LZPL15, TK16a], Takagi's RSA [TK16a], multi-prime RSA [Hin08, TK17b], and RSA with multiple exponent pairs [TK14b, TK16c]. As similar settings, several papers study partial key exposure attacks on CRT-RSA [SM09, LZL14, TK15, TK16b].

1.5 Roadmap

The organization of this paper is as follows. In Section 2, we recall basic tools and an overview of Coppersmith's methods to solve modular equations. In Section 3, we provide an alternative proof of the Boneh-Durfee stronger attack. In Sections 4 and 5, we study partial key exposure attacks with the MSBs and the LSBs, respectively.

2 Preliminaries

In this section, we recall Coppersmith's method to solve modular equations with small solutions [Cop96b]. Coppersmith's method has been utilized to reveal several vulnerabilities of RSA. See [Cop97, Cop01, May03, May10, NS01] for more information. In this paper, we use Howgrave-Graham's simpler reformulation of the method [How97]. At the end of the section, we summarize a basic approach to maximize solvable root bounds by utilizing a notion of helpful polynomials [May10, TK14a].

For bivariate polynomials $h(x,y) = \sum h_{i_X,i_Y} x^{i_X} y^{i_Y}$, let $\|h(x,y)\| := \sqrt{\sum h_{i_X,i_Y}^2}$ denote a norm of the polynomial. The following Howgrave-Graham's lemma [How97] enables us to solve modular equations by solving integer equations.

Lemma 1 (Howgrave-Graham's lemma [How97])**.** *Let $h(x,y) \in \mathbb{Z}[x,y]$ be a bivariate integer polynomial that consists of at most n monomials. Let W, X, Y be positive integers. If the polynomial $h(x,y)$ satisfies*
1. $h(\tilde{x},\tilde{y}) = 0 \pmod{W}$, where $|\tilde{x}| < X, |\tilde{y}| < Y$,
2. $\|h(xX, yY)\| < W/\sqrt{n}$.
Then $h(\tilde{x},\tilde{y}) = 0$ holds over the integers.

Based on the lemma, solving bivariate modular equations is reduced to finding two low norm polynomials that has the same small solutions. To find the polynomials, we utilize the LLL lattice reduction algorithm [LLL82]. Let $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$ be linearly independent k-dimensional vectors. The lattice $L(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n)$ spanned by the basis vectors $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$ is defined as $L(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n) = \{\sum_{j=1}^{n} c_j \boldsymbol{b}_j : c_j \in \mathbb{Z}\}$. When $n = k$, lattices are described as full rank. The basis matrix of the lattice $\boldsymbol{B}$ is defined as the $n \times k$ matrix that has a basis vector $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$ in each row. In this paper, we use only full rank lattices, i.e., $k = n$. The determinant of a full rank lattice is computed by $\mathrm{vol}(L(\boldsymbol{B})) = |\det(\boldsymbol{B})|$. A lattice has infinitely many bases. Finding a basis that contains low norm vectors is a fundamental lattice problem. The LLL algorithm proposed by Lenstra, Lenstra and Lovász [LLL82] finds short lattice vectors in polynomial time.

Proposition 1 (LLL algorithm [LLL82, May03]). *Given k-dimensional basis vectors $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$, the LLL algorithm finds linearly independent lattice vectors $\boldsymbol{v}_1$ and $\boldsymbol{v}_2$ in $L(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n)$ such that*

$$\|\boldsymbol{v}_1\| \leq 2^{(n-1)/4}(\mathrm{vol}(L(\boldsymbol{B})))^{1/n} \quad \textit{and} \quad \|\boldsymbol{v}_2\| \leq 2^{n/2}(\mathrm{vol}(L(\boldsymbol{B})))^{1/(n-1)}.$$

These norms are Euclidean norms. The running time is polynomial in k, n, and the maximum input length of $\boldsymbol{B}$.

We summarize how Coppersmith's method finds a solution $(\tilde{x}, \tilde{y})$ of a bivariate modular equation $h(x, y) = 0 \pmod{W}$ if $|\tilde{x}| < X, |\tilde{y}| < Y$. At first, we create n polynomials $h_1(x, y), \ldots, h_n(x, y)$ that have the root $(\tilde{x}, \tilde{y})$ modulo W^m for a positive integer m, and so do any integer linear combinations of $h_1(x, y), \ldots, h_n(x, y)$. Then, we generate basis vectors $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$ that are coefficient vectors of $h_1(xX, yY), \ldots, h_n(xX, yY)$, respectively. All lattice points correspond to polynomials that are integer linear combinations of $h_1(x, y), \ldots, h_n(x, y)$. Hence, applying the LLL algorithm to $\boldsymbol{B}$, we obtain two short vectors $\boldsymbol{v}_1$ and $\boldsymbol{v}_2$ along with their corresponding low norm polynomials $\tilde{h}_1(x, y)$ and $\tilde{h}_2(x, y)$. If norms of the polynomials are enough small to satisfy Howgrave-Graham's lemma, they have the root $(\tilde{x}, \tilde{y})$ over the integers. The root can efficiently be recovered by computing the Gröbner bases or resultants of the polynomials. The method is heuristic for the bivariate case since the polynomials $\tilde{h}_1(x, y)$ and $\tilde{h}_2(x, y)$ have no assurance of algebraic independency. In this paper, we assume that these polynomials are algebraic independent and the resultant will not vanish. This assumption should be reasonable since few negative cases have been reported.

To conclude this section, we briefly explain how to construct a better matrix to find larger solutions. By using Coppersmith's method, we can recover the root when $|\det(\boldsymbol{B})|^{1/n} < W^m$ by omitting small terms. Hence, we can recover larger solutions if we can construct a matrix $\boldsymbol{B}$ with smaller $|\det(\boldsymbol{B})|^{1/n}$ for a fixed m. Since matrices $\boldsymbol{B}$ usually tend to be triangular, $|\det(\boldsymbol{B})|^{1/n}$ is an absolute value of a geometric mean of all diagonals. Thus, May [May10] defined a notion of *helpful polynomials* whose diagonals in $\boldsymbol{B}$ has smaller absolute values than the modulus W^m since such polynomials reduce the quantity of $|\det(\boldsymbol{B})|^{1/n}$ and contribute to recovering larger solutions. Indeed, Takayasu and Kunihiro [TK14a] constructed matrices by collecting as many helpful polynomials as possible and as few unhelpful polynomials as possible, then improve several algorithms for solving multivariate modular equations.

In this paper, we follow the approach to improve partial key exposure attacks. Furthermore, we extend the definition of helpful to capture special matrices which we will use. Specifically, to recover algebraic structures of modular polynomials, several diagonals of our matrices will change by adding a new polynomial. Hence, to minimize $|\det(\boldsymbol{B})|^{1/n}$ for fixed m, we use the following notion.

Definition 1 (Helpful Polynomials). *Let $\boldsymbol{B}$ be a matrix to solve a modular equation $h(x, y) = 0 \pmod{W}$. Let $\boldsymbol{B}'$ be a matrix that has the same polynomials as $\boldsymbol{B}$ except $h'(x, y)$ and does not have further polynomials. We call $h'(x, y)$ a helpful polynomial if and only if*

$$\frac{\det(\boldsymbol{B}')}{\det(\boldsymbol{B})} \leq W^m$$

holds. Otherwise, we call $h'(x, y)$ an unhelpful polynomial.

3 Revisiting Herrmann-May's Matrix

In this section, we recall Herrmann-May's triangular matrix that provides a simpler proof for the Boneh-Durfee stronger attack. Then, we provide an alternative triangular matrix with additional unraveling. Although our matrix does not improve Boneh-Durfee's attack at all, it will recover useful algebraic structures that will be essential to improve partial key exposure attacks in the subsequent sections.

3.1 Boneh-Durfee's Attack

We first review the Boneh-Durfee weaker attack. Then, we explain how Boneh-Durfee improves it to the stronger attack.

Recall an RSA key generation

$$ed = 1 + \ell(p-1)(q-1) = 1 + \ell(N - p - q + 1),$$

where ℓ is an unknown integer. Boneh and Durfee [BD00] solved the following modular equation

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

whose solution is $(x, y) = (\ell, -p - q + 1)$. Let e be full size and $d = N^{\beta}$. Then, an absolute value of the solution is bounded above by $X := N^{\beta}$ and $Y := N^{1/2}$ within a constant factor, respectively. To recover the solution, Boneh and Durfee utilized the following shift-polynomials

$$g^{BD.x}_{[u,i]}(x, y) := x^{u-i} f_{BD}(x, y)^i e^{m-i} \quad \text{and} \quad g^{BD.y}_{[u,j]}(x, y) := y^j f_{BD}(x, y)^u e^{m-u}. \tag{1}$$

They first defined sets of indices

$$\begin{aligned} \mathcal{I}_{BD,x} &:= \{u = 0, 1, \ldots, m; i = 0, 1, \ldots, u\}, \\ \mathcal{I}_{BD,y1} &:= \{u = 0, 1, \ldots, m; j = 1, 2, \ldots, k\}, \end{aligned} \tag{2}$$

where $\kappa = k/m \geq 0$ is a parameter to be optimized. They constructed a matrix $\boldsymbol{B}$ that has a coefficient vector of $g^{BD.x}_{[u,i]}(xX, yY)$ for $(u, i) \in \mathcal{I}_{BD,x}$ and $g^{BD.y}_{[u,j]}(xX, yY)$ for $(u, j) \in \mathcal{I}_{BD,y1}$ in each row. Based on the construction, the matrix $\boldsymbol{B}$ becomes triangular as follows.

Lemma 2 (Boneh-Durfee Weaker Matrix [BD00])**.** *Let shift-polynomials $g^{BD.x}_{[u,i]}(x, y)$ and $g^{BD.y}_{[u,j]}(x, y)$, sets of indices $\mathcal{I}_{BD,x}$ and $\mathcal{I}_{BD,y1}$, be defined as in (1), (2), respectively. Let $\boldsymbol{B}$ be a matrix whose rows consist of coefficients of $g^{BD.x}_{[u,i]}(xX, yY)$ for $(u, i) \in \mathcal{I}_{BD,x}$ and $g^{BD.y}_{[u,j]}(xX, yY)$ for $(u, j) \in \mathcal{I}_{BD,y1}$. If the shift-polynomials are ordered as*

- $g^{BD.x}_{[u,i]}(xX, yY) \prec g^{BD.y}_{[u,j]}(xX, yY)$,
- $g^{BD.x}_{[u',i']}(xX, yY) \prec g^{BD.x}_{[u,i]}(xX, yY)$ *for*
  - $u' < u$,

Table 3: Example of a matrix $\boldsymbol{B}$ of Boneh-Durfee's weaker lattices for $m = 2$ and $\kappa = 1$.

	1	y	y^2	x	xy	xy^2	xy^3	x^2	x^2y	x^2y^2	x^2y^3	x^2y^4
$g^{BD.x}_{[0,0]}$	e^2											
$g^{BD.y}_{[0,1]}$		Ye^2										
$g^{BD.y}_{[0,2]}$			Y^2e^2									
$g^{BD.x}_{[1,0]}$				Xe^2								
$g^{BD.x}_{[0,1]}$	–			–	XYe							
$g^{BD.y}_{[1,1]}$		–			–	XY^2e						
$g^{BD.y}_{[1,2]}$			–			–	XY^3e					
$g^{BD.x}_{[2,0]}$								X^2e^2				
$g^{BD.x}_{[1,1]}$				–				–	X^2Ye			
$g^{BD.x}_{[0,2]}$	–			–	–			–	–	X^2Y^2		
$g^{BD.y}_{[2,1]}$		–			–	–			–	–	X^2Y^3	
$g^{BD.y}_{[2,2]}$			–			–	–			–	–	X^2Y^4

  - $u' = u, i' < i$,
- $g^{BD.y}_{[u',j']}(xX, yY) \prec g^{BD.y}_{[u,j]}(xX, yY)$ *for*
  - $u' < u$,
  - $u' = u, j' < j$,

then the matrix $\boldsymbol{B}$ *becomes triangular with diagonals*

- $X^uY^ie^{m-i}$ *for* $g^{BD.x}_{[u,i]}(xX, yY)$,
- $X^uY^{u+j}e^{m-u}$ *for* $g^{BD.y}_{[u,j]}(xX, yY)$.

Table 3 shows[1] an example of the triangular matrix. By optimizing $\kappa = (1 - 2\beta)/2$, the matrix provides the Boneh-Durfee weaker attack that works when $\beta < (7 - 2\sqrt{7})/6 = 0.284\cdots$.

To improve the weaker attack, Boneh and Durfee exploited sublattices. To be precise, they used a submatrix of the previous one as a lattice basis. For the purpose, they replaced a set of index $\mathcal{I}_{BD,y1}$ by[2]

$$\mathcal{I}_{BD,y2} := \{u = 0, 1, \ldots, m; j = 1, 2, \ldots, k + \lfloor \tau u \rfloor\}, \tag{3}$$

[1] "–" in matrices denote non-zero elements throughout the paper.

[2] To be precise, the upper bound of j in $\mathcal{I}_{BD,y2}$ was $\lfloor \tau u \rfloor$ in the original paper [BD00]. Indeed, the additional k is optimized to $k = 0$. We modify the upper bound since it will be convenient to explain our partial key exposure attacks later.

where τ is a parameter to be optimized such that $0 \leq \tau \leq 1$. By optimizing $k = 0$ and $\tau = 1 - 2\beta$, the matrix $\boldsymbol{B}$ that has a coefficient vector of $g_{[u,i]}^{BD.x}(xX, yY)$ for $(u, i) \in \mathcal{I}_{BD,x}$ and $g_{[u,j]}^{BD.y}(xX, yY)$ for $(u, j) \in \mathcal{I}_{BD,y2}$ in each row provides the Boneh-Durfee stronger attack that works when $\beta < 1 - 1/\sqrt{2} = 0.292\cdots$. Since the matrix does not become triangular, the analysis is involved.

3.2 Herrmann-May's Matrix

Herrmann and May [HM10] revisited Boneh-Durfee's work and provided a simpler proof. Specifically, they applied unraveled linearization [HM09] to the Boneh-Durfee's stronger matrix and transformed it to be triangular. For the purpose, a new variable

$$z := 1 + xy$$

plays an essential role, where an absolute value of the solution is bounded above by $Z := XY = N^{\beta+1/2}$ within a constant factor. In the following lemma, we summarize Herrmann-May's triangular matrix.[3]

Lemma 3 (Herrmann-May's Triangular Matrix [HM10, TK17a])**.** *Let shift-polynomials $g_{[u,i]}^{BD.x}(x, y)$ and $g_{[u,j]}^{BD.y}(x, y)$, sets of indices $\mathcal{I}_{BD,x}$ and $\mathcal{I}_{BD,y2}$, be defined as in (1), (3), respectively. Let $\boldsymbol{B}$ be a matrix whose rows consist of coefficients of $g_{[u,i]}^{BD.x}(xX, yY)$ for $(u, i) \in \mathcal{I}_{BD,x}$ and $g_{[u,j]}^{BD.y}(xX, yY)$ for $(u, j) \in \mathcal{I}_{BD,y2}$. If the shift-polynomials are ordered as the same way in Lemma 2, then the matrix $\boldsymbol{B}$ becomes triangular with diagonals*

- $X^{u-i}Z^i e^{m-i}$ *for* $g_{[u,i]}^{BD.x}(xX, yY)$,
- $Y^j Z^u e^{m-u}$ *for* $g_{[u,j]}^{BD.y}(xX, yY)$.

As the last statement suggests, all monomials do not have two variables x and y, simultaneously. Although the linearization $z = 1 + xy$ loses the information of x and y, it can be recovered by unraveling. Table 4 shows an example of the triangular matrix. The triangular matrix enables us to analyze the structure easily. Indeed, the following lemma shows one evidence of the optimality of the Boneh-Durfee stronger attack.

Lemma 4. *In the matrix $\boldsymbol{B}$ of the Boneh-Durfee stronger attack, polynomials $g_{[u,j]}^{BD.y}(x, y)$ are helpful if and only if $j \leq (1 - 2\beta)u$ for all u.*

Proof of Lemma 4. Let $g_{[u',j']}^{BD.y}(x, y)$ be a polynomial with fixed indices (u', j'), and $\boldsymbol{B}'$ be a matrix that is a matrix $\boldsymbol{B}$ without the polynomial $g_{[u',j']}^{BD.y}(x, y)$. As stated in Lemma 3, a diagonal of the polynomial $g_{[u',j']}^{BD.y}(x, y)$ in $\boldsymbol{B}$ is $Y^{j'}Z^{u'}e^{m-u'}$. Hence,

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

[3] As we mentioned, the set of indices $\mathcal{I}_{BD,y2}$ is not the same as the the original one in [BD00]. Hence, it is not the same as the one which Herrmann and May studied in [HM10]. However, Herrmann-May's approach is also useful for the modified $\mathcal{I}_{BD,y2}$, where the fact was utilized in [TK17a].

Table 4: Herrmann-May's matrix $\boldsymbol{B}$ for $m = 2$ and $\kappa = 1/2, \tau = 1$

	1	y	x	z	yz	y^2z	x^2	xz	z^2	yz^2	y^2z^2	y^3z^2
$g_{[0,0]}^{BD.x}$	e^2											
$g_{[0,1]}^{BD.y}$		Ye^2										
$g_{[1,0]}^{BD.x}$			Xe^2									
$g_{[0,1]}^{BD.x}$			–	Ze								
$g_{[1,1]}^{BD.y}$	–			–	YZe							
$g_{[1,2]}^{BD.y}$		–			–	Y^2Ze						
$g_{[2,0]}^{BD.x}$							X^2e^2					
$g_{[1,1]}^{BD.x}$							–	XZe				
$g_{[0,2]}^{BD.x}$							–	–	Z^2			
$g_{[2,1]}^{BD.y}$			–	–				–	–	YZ^2		
$g_{[2,2]}^{BD.y}$	–			–	–				–	–	Y^2Z^2	
$g_{[2,3]}^{BD.y}$		–			–	–				–	–	Y^3Z^2

that is smaller than or equal to the modulus e^m if and only if

$$\begin{aligned} Y^{j'}Z^{u'}e^{m-u'} \leq e^m &\Leftrightarrow Y^{j'}Z^{u'} \leq e^{u'} \\ &\Leftrightarrow \frac{1}{2}j' + \left(\beta + \frac{1}{2}\right)u' \leq u' \\ &\Leftrightarrow j' \leq (1-2\beta)u'. \end{aligned}$$

Hence, we conclude the proof. □

The lemma suggests that the Boneh-Durfee stronger attack used only helpful $g_{[u,j]}^{BD.y}(x,y)$ and no unhelpful $g_{[u,j]}^{BD.y}(x,y)$. That is why they could successfully improve their own weaker attack. However, we should note that the lemma does not prove a rigorous optimality of the attack.

3.3 Herrmann-May's Matrix with Additional Unraveling

In this subsection, we show a new triangular matrix for the Boneh-Durfee stronger attack. In short, we apply additional unraveling to Herrmann-May's triangular matrix. Then, there are several monomials which have two variables x and y, simultaneously, in our matrix. Before providing the matrix, we introduce some functions that will be used to control the power of unraveling throughout the paper.

Definition 2. *Let m and k be non-negative integers, τ be a real number such that $0 \leq \tau \leq 1$. Define the following functions $l_{k,\tau}^{MSBs}(\cdot)$ and $l_{k,\tau}^{LSBs}(\cdot)$ whose domains and ranges are non-negative*

Table 5: Herrmann-May's matrix $\boldsymbol{B}$ with additional unraveling by the function $l_{k,\tau}^{LSBs}(j)$ for $m = 2$ and $\kappa = 1/2, \tau = 1$

	1	y	x	xy	xy^2	y^2z	x^2	x^2y	x^2y^2	x^2y^3	y^2z^2	y^3z^2
$g_{[0,0]}^{BD.x}$	e^2											
$g_{[0,1]}^{BD.y}$		Ye^2										
$g_{[1,0]}^{BD.x}$			Xe^2									
$g_{[0,1]}^{BD.x}$	–		–	XYe								
$g_{[1,1]}^{BD.y}$		–		–	XY^2e							
$g_{[1,2]}^{BD.y}$					–	Y^2Ze						
$g_{[2,0]}^{BD.x}$							X^2e^2					
$g_{[1,1]}^{BD.x}$			–				–	X^2Ye				
$g_{[0,2]}^{BD.x}$	–		–	–			–	–	X^2Y^2			
$g_{[2,1]}^{BD.y}$		–		–	–			–	–	X^2Y^3		
$g_{[2,2]}^{BD.y}$					–				–	–	Y^2Z^2	
$g_{[2,3]}^{BD.y}$						–				–	–	Y^3Z^2

integers:

$$l_{k,\tau}^{MSBs}(x) := \max\left\{0, \left\lceil \frac{x-k}{\tau+1} \right\rceil \right\} \qquad \textit{and} \qquad l_{k,\tau}^{LSBs}(x) := \max\left\{0, \left\lceil \frac{x-k}{\tau} \right\rceil \right\}.$$

Then, we provide our matrix.

Lemma 5. *Let shift-polynomials $g_{[u,i]}^{BD.x}(x,y)$ and $g_{[u,j]}^{BD.y}(x,y)$, sets of indices $\mathcal{I}_{BD,x}$ and $\mathcal{I}_{BD,y2}$, a function $l_{k,\tau}^{LSBs}(x)$, a matrix $\boldsymbol{B}$ be defined as in (1), (3), Definition 2, and Lemma 3, respectively. If the shift-polynomials are ordered as the same way in Lemma 2, then the matrix $\boldsymbol{B}$ becomes triangular with diagonals*

- $X^uY^ie^{m-i}$ *for* $g_{[u,i]}^{BD.x}(xX, yY)$,
- $X^{u-l_{k,\tau}^{LSBs}(j)}Y^{u+j-l_{k,\tau}^{LSBs}(j)}Z^{l_{k,\tau}^{LSBs}(j)}e^{m-u}$ *for* $g_{[u,j]}^{BD.y}(xX, yY)$.

In Herrmann-May's matrix, two variables x and y does not appear in the same monomials. Specifically, X does not appear in diagonals of $g_{[u,j]}^{BD.y}(x,y)$. However, X appears in our matrix. It means that we apply less linearization $z = 1+xy$ or more unraveling than Herrmann-May's matrix. How much we apply linearization/unraveling is controlled by a function $l_{k,\tau}^{LSBs}(j)$.

Table 5 shows an example of the matrix that has the same polynomials as Herrmann-May's matrix in Table 4. To illustrate our idea, we use the examples. Herrmann-May's matrix has diagonals y, yz, and yz^2 for $g_{[0,1]}^{BD.y}, g_{[1,1]}^{BD.y}$, and $g_{[2,1]}^{BD.y}$ whereas our matrix has diagonals y, xy^2, and

x^2y^3 for the same polynomials. We apply additional unravelings $z \Rightarrow 1 + xy$ and transform the former diagonals to the latter ones by using the following simple relations:

$$yz = y(1 + xy) = y + xy^2 \qquad \text{and} \qquad yz^2 = y(1 + xy)^2 = y + 2xy^2 + x^2y^3.$$

The relation suggests that all integer linear combinations of (y, yz) and (y, yz, yz^2) can be replaced by those of (y, xy^2) and (y, xy^2, x^2y^3), respectively. Hence, the matrix is still triangular even if we apply the additional unravelings. Here, we want to claim that integer linear combinations of (yz) and (yz, yz^2) cannot be rewritten as those of (xy^2) and (xy^2, x^2y^3), respectively. To apply the additional unraveling, the existence of y was essential. Without the variable y, we cannot replace yz by xy^2. However, since yz exists, we can replace yz^2 by xy^2z by using a relation

$$yz^2 = yz(1 + xy) = yz + xy^2z.$$

Therefore, we define the function $l^{LSBs}_{k,\tau}(j)$ so that $y^j z^{l^{LSBs}_{k,\tau}(j)}$ exists, however, $y^j z^{l^{LSBs}_{k,\tau}(j)-1}, y^j z^{l^{LSBs}_{k,\tau}(j)-2}, \cdots$ do not exist in Herrmann-May's matrix $\boldsymbol{B}$. In other words, in the a set of indices $\mathcal{I}_{BD,y2}$, there are indices $(u, j) = (l^{LSBs}_{k,\tau}(j'), j'), (l^{LSBs}_{k,\tau}(j') + 1, j'), \ldots, (m, j')$ whereas no indices $(u, j) = (0, j'), (1, j'), \ldots, (l^{LSBs}_{k,\tau}(j') - 1, j')$ for a fixed $j' \geq k$. The fact follows from that

- $k + \lfloor \tau u \rfloor < j'$ for $u < l^{LSBs}_{k,\tau}(j')$ since $k + \lfloor \tau(l^{LSBs}_{k,\tau}(j') - 1) \rfloor < j'$ holds,
- $k + \lfloor \tau u \rfloor \geq j'$ for $u \geq l^{LSBs}_{k,\tau}(j')$ since $k + \lfloor \tau l^{LSBs}_{k,\tau}(j') \rfloor \geq j'$ holds.

Therefore, the function $l^{LSBs}_{k,\tau}(j)$ tells us the maximum unraveling which we can apply.

The matrix with additional unraveling does not provide any benefits in the context of Boneh-Durfee's attack. We use the matrix to explain an overview of an unraveled linearization for our partial key exposure attacks with the LSBs in Section 5.3.

Proof of Lemma 5. We apply unraveling $z \Rightarrow 1 + xy$ to each variable of Herrmann-May's matrix $\boldsymbol{B}$ in Lemma 3 and obtain a claimed matrix in Lemma 5. Since the diagonals $X^{u-i}Z^i e^{m-i}$ of $g^{BD.x}_{[u,i]}(xX, yY)$ and those $Y^j Z^u e^{m-u}$ of $g^{BD.y}_{[u,j]}(xX, yY)$ for $(u, j) = (l^{LSBs}_{k,\tau}(j), j)$ are the same between Lemmas 3 and 5, we focus on the other variables

- $x^{u-l^{LSBs}_{k,\tau}(j)} y^{u+j-l^{LSBs}_{k,\tau}(j)} z^{l^{LSBs}_{k,\tau}(j)}$ for $j = 1, 2, \ldots, k + \lfloor \tau m \rfloor; l^{LSBs}_{k,\tau}(j) + 1, , l^{LSBs}_{k,\tau}(j) + 2, \ldots, m$.

We want to claim that a matrix $\boldsymbol{B}$ is still triangular when all variables $y^j z^u$ are replaced by $x^{u-l^{LSBs}_{k,\tau}(j)} y^{u+j-l^{LSBs}_{k,\tau}(j)} z^{l^{LSBs}_{k,\tau}(j)}$ by applying unraveling $z^{u-l^{LSBs}_{k,\tau}(j)} \Rightarrow (1 + xy)^{u-l^{LSBs}_{k,\tau}(j)}$.

Here, we show an inductive proof that

$$y^j z^u = \sum_{t=0}^{u-l^{LSBs}_{k,\tau}(j)} c_t x^t y^{j+t} z^{l^{LSBs}_{k,\tau}(j)}$$

holds, where $c_0, c_1, \ldots, c_{u-l_{k,\tau}^{LSBs}(j)}$ are integers and $c_{u-l_{k,\tau}^{LSBs}(j)} = 1$. The statement holds for $u = l_{k,\tau}^{LSBs}(j)$. We assume that the statement holds for fixed (u', j') and prove that the statement also holds for $(u'+1, j')$. It follows that

$$\begin{aligned}
y^{j'}z^{u'+1} &= y^{j'}z^{u'}(1+xy) \\
&= \left(\sum_{t=0}^{u'-l_{k,\tau}^{LSBs}(j')} c_t x^t y^{j'+t} z^{l_{k,\tau}^{LSBs}(j')}\right)(1+xy) \\
&= \sum_{t=0}^{u'-l_{k,\tau}^{LSBs}(j')} c_t x^t y^{j'+t} z^{l_{k,\tau}^{LSBs}(j')} \\
&\quad + \left(\sum_{t=0}^{u'-l_{k,\tau}^{LSBs}(j')-1} c_t x^t y^{j'+t} z^{l_{k,\tau}^{LSBs}(j')} + x^{u'-l_{k,\tau}^{LSBs}(j')} y^{u'+j'-l_{k,\tau}^{LSBs}(j')} z^{l_{k,\tau}^{LSBs}(j')}\right) xy \\
&= \sum_{t=0}^{u'-l_{k,\tau}^{LSBs}(j')} c'_t x^t y^{j'+t} z^{l_{k,\tau}^{LSBs}(j')} + x^{u'-l_{k,\tau}^{LSBs}(j')+1} y^{u'+j'-l_{k,\tau}^{LSBs}(j')+1} z^{l_{k,\tau}^{LSBs}(j')},
\end{aligned}$$

where $c'_0, c'_1, \ldots, c'_{u'-l_{k,\tau}^{LSBs}(j)}$ are integers. Hence, the statement holds for all (u, j). By using the relation, we can replace all integer linear combinations of $\sum_{u=l_{k,\tau}^{LSBs}(j)}^{u'} d_u y^j z^u$ by $\sum_{u=l_{k,\tau}^{LSBs}(j)}^{u'} d'_u x^{u-l_{k,\tau}^{LSBs}(j)} y^{u+j-l_{k,\tau}^{LSBs}(j)} z^{l_{k,\tau}^{LSBs}(j)}$, where $d_{l_{k,\tau}^{LSBs}(j)}, d_{l_{k,\tau}^{LSBs}(j)+1}, \ldots, d_{u'}$ and $d'_{l_{k,\tau}^{LSBs}(j)}, d'_{l_{k,\tau}^{LSBs}(j)+1}, \ldots, d'_{u'}$ are integers such that $d_{u'} = d'_{u'}$. Thus, we can replace all variables $y^j z^u$ in diagonals of $g_{[u,j]}^{BD.y}(x, y)$ by $x^{u-l_{k,\tau}^{LSBs}(j)} y^{u+j-l_{k,\tau}^{LSBs}(j)} z^{l_{k,\tau}^{LSBs}(j)}$. Hence, we complete the proof. □

As we claimed, the function $l_{k,\tau}^{LSBs}(j)$ tells us the maximum unraveling which we can apply to Herrmann-May's matrix $\boldsymbol{B}$. On the other hand, Herrmann-May's matrix $\boldsymbol{B}$ is still triangular when we apply less additional unraveling than the above one. For example, Herrmann-May's matrix $\boldsymbol{B}$ can be modified as a triangular matrix with diagonals

- $X^{u-l_{k,\tau}^{MSBs}(i)} Y^{i-l_{k,\tau}^{MSBs}(i)} Z^{l_{k,\tau}^{MSBs}(i)} e^{m-i}$ for $g_{[u,i]}^{BD.x}(xX, yY)$,
- $X^{u-l_{k,\tau}^{MSBs}(u+j)} Y^{u+j-l_{k,\tau}^{MSBs}(u+j)} Z^{l_{k,\tau}^{MSBs}(u+j)} e^{m-u}$ for $g_{[u,j]}^{BD.y}(xX, yY)$.

Here, observe that

$$l_{k,\tau}^{MSBs}(u+j) = \max\left\{0, \left\lceil \frac{u+j-k}{\tau+1} \right\rceil\right\} \geq \max\left\{0, \left\lceil \frac{j-k}{\tau} \right\rceil\right\} = l_{k,\tau}^{LSBs}(j)$$

holds for $(u, j) \in \mathcal{I}_{BD.y2}$ since $j \leq k + \tau u$. Hence, when we apply an unraveling by the function $l_{k,\tau}^{MSBs}(u+j)$, there are less and more Z's in diagonals for $g_{[u,j]}^{BD.y}(xX, yY)$ than Herrmann-May's

Table 6: Herrmann-May's matrix $\boldsymbol{B}$ with additional unraveling by the function $l_{k,\tau}^{MSBs}(u+j)$ for $m=2$ and $\kappa=1/2, \tau=1$

	1	y	x	xy	yz	y^2z	x^2	x^2y	xyz	xy^2z	y^2z^2	y^3z^2
$g_{[0,0]}^{BD.x}$	e^2											
$g_{[0,1]}^{BD.y}$		Ye^2										
$g_{[1,0]}^{BD.x}$			Xe^2									
$g_{[0,1]}^{BD.x}$	–		–	XYe								
$g_{[1,1]}^{BD.y}$				–	YZe							
$g_{[1,2]}^{BD.y}$		–			–	Y^2Ze						
$g_{[2,0]}^{BD.x}$							X^2e^2					
$g_{[1,1]}^{BD.x}$			–	–			–	X^2Ye				
$g_{[0,2]}^{BD.x}$	–	–	–	–	–		–	–	XYZ			
$g_{[2,1]}^{BD.y}$		–		–	–	–		–	–	XY^2Z		
$g_{[2,2]}^{BD.y}$		–		–	–	–			–	–	Y^2Z^2	
$g_{[2,3]}^{BD.y}$		–			–	–				–	–	Y^3Z^2

original matrix and a matrix with an additional unraveling by the function $l_{k,\tau}^{LSBs}(j)$. We omit a proof that a matrix with an unraveling by the function $l_{k,\tau}^{MSBs}(u+j)$ is triangular with the above diagonals since the proof is almost the same as the that of Lemma 5. We use the matrix to explain an overview of an unraveled linearization for our partial key exposure attacks with the MSBs in Section 4.4.

Table 6 shows an example of the matrix with an additional unraveling by the function $l_{k,\tau}^{MSBs}(u+j)$, where the matrix has the same polynomials as Tables 4 and 5. Herrmann-May's matrix in Table 4 has diagonals z, xz, z^2, and yz^2 for $g_{[0,1]}^{BD.x}, g_{[1,1]}^{BD.x}, g_{[0,2]}^{BD.x}$, and $g_{[2,1]}^{BD.y}$ whereas our matrix has diagonals xy, x^2y, xyz, and xy^2z for the same polynomials. Our matrix in Table 5 has diagonals xy^2, x^2y^2, and x^2y^3 for $g_{[1,1]}^{BD.y}, g_{[0,2]}^{BD.x}$, and $g_{[2,1]}^{BD.y}$ whereas our matrix in Table 6 has diagonals yz, xyz, and xy^2z for the same polynomials.

4 Partial Key Exposure Attacks with the MSBs

In this section, we propose our improved partial key exposure attack on RSA with the MSBs of d. In Section 4.1, we formulate the attack scenario as a modular equation. In Section 4.2, we recall previous attacks [EJMdW05, SSM10]. In Section 4.3, we propose an attack that works in the same condition as Ernst et al.'s attack [EJMdW05] by solving modular equations. In Section 4.4, we propose our main attack.

4.1 Formulation

In this subsection, we formulate the attack scenario with the MSBs as modular equations. We write a secret exponent $d = N^\beta$ as $d = d_0 M + d_1$, where $d_0 > N^{\beta-\delta}$ and $d_1 < N^\delta$ denote the known MSBs and the unknown LSBs of d, respectively, with an integer $M := 2^{\lfloor \delta \log N \rfloor}$. Recall an RSA key generation

$$e(d_0 M + d_1) = 1 + \ell(p-1)(q-1) = 1 + \ell(N - p - q + 1) \tag{4}$$

with an unknown integer ℓ as in Section 3.1. Let publicly computable $\ell_0 = \lfloor (ed_0 M - 1)/N \rfloor$ be an approximation to ℓ since

$$\begin{aligned}
|\ell - \ell_0| &= \left| \frac{e(d_0 M + d_1) - 1}{N - p - q + 1} - \left\lfloor \frac{ed_0 M - 1}{N} \right\rfloor \right| \\
&\le \left| \frac{e(d_0 M + d_1)N - N - (ed_0 M - 1)(N - p - q + 1)}{(N - p - q + 1)N} - 1 \right| \\
&= \left| \frac{ed_1 N - (ed_0 M - 1)(-p - q + 1)}{(N - p - q + 1)N} - 1 \right| \\
&\le \left| \frac{ed_1}{N - p - q + 1} \right| + \left| \frac{(ed_0 M - 1)(p + q - 1)}{(N - p - q + 1)N} \right| + 1 \\
&\le N^\delta + N^{\beta - 1/2} + 1.
\end{aligned}$$

Hence, we can bound unknown $|\ell - \ell_0| < N^\gamma$ such that $\gamma = \max\{\delta, \beta - 1/2\}$ within a constant factor. By taking modulo e of the equation (4), we obtain a modular polynomial

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

whose root is $(x, y) = (\ell - \ell_0, -p - q + 1)$. Absolute values of the root are bounded above by $X := N^\gamma$ and $Y := N^{1/2}$ within constant factors.

4.2 Previous Works

In this subsection, we briefly recall previous attacks proposed by Ernst et al. [EJMdW05] and Sarkar et al. [SSM10]. Ernst et al.'s attack, which solves integer equations, works when

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

(2) $\delta < \frac{3}{16}$ and $\beta \le \frac{11}{16}$,

(3) $\delta < \frac{1}{3} + \frac{1}{3}\beta - \frac{1}{3}\sqrt{4\beta^2 + 2\beta - 2}$ and $\beta > \frac{11}{16}$.

The condition (1) is the best for $\beta < 235/512$. Ernst et al.'s attack can be viewed as an extension of the Boneh-Durfee weaker attack since the condition (1) is the same as $\beta < (7 - 2\sqrt{7})/6 = 0.284\cdots$ for $\delta = \beta$.

Sarkar et al.'s attack, which solves the modular equation $f_{MSBs}(x,y)=0$, works in the above condition (2). To solve the modular equation, they used shift-polynomials

$$\begin{aligned} g_{[u,i]}^{MSBs.x}(x,y) &:= x^{u-i} f_{MSBs}(x,y)^i e^{m-i}, \\ g_{[u,j]}^{MSBs.y}(x,y) &:= y^j f_{MSBs}(x,y)^u e^{m-u}. \end{aligned} \tag{5}$$

Both shift-polynomials modulo e^m have the same root as the original solutions, i.e., $g_{[u,i]}^{MSBs.x}(\ell-\ell_0,-p-q+1)=0 \pmod{e^m}$ and $g_{[u,j]}^{MSBs.y}(\ell-\ell_0,-p-q+1)=0 \pmod{e^m}$. They defined sets of indices

$$\begin{aligned} \mathcal{I}_{SSM,x} &:= \{u=0,1,\ldots,m; i=0,1,\ldots,\min\{u,s\}\}, \\ \mathcal{I}_{SSM,y} &:= \{u=0,1,\ldots,s-1; j=1,2,\ldots,s-u\}, \end{aligned}$$

and used shift-polynomials $g_{[u,i]}^{MSBs.x}(xX,yY)$ for $(u,i)\in\mathcal{I}_{SSM,x}$ and $g_{[u,j]}^{MSBs.y}(xX,yY)$ for $(u,j)\in\mathcal{I}_{SSM,y}$ to construct a triangular matrix $\boldsymbol{B}$. The definitions of $\mathcal{I}_{SSM,x}$ and $\mathcal{I}_{SSM,y}$ quite differs from Boneh-Durfee's one although Sarkar et al. solved the similar equation. Indeed, Sarkar et al.'s attack is not an extension of the Boneh-Durfee attack since it does not work for small d.

4.3 Revisiting Ernst et al.'s Attack by Solving Modular Equations

In this subsection, we show that by solving modular equation $f_{MSBs}(x,y)=0$ as Sarkar et al., we can obtain an attack that works in Ernst et al.'s condition (1). We believe that a content in this subsection will be useful to understand our improved attacks in Section 4.4.

Technically, we use the same shift-polynomials as Sarkar et al., however, we use sets of indices $\mathcal{I}_{BD,x}$ and $\mathcal{I}_{BD,y1}$ as the Boneh-Durfee weaker attack to construct a basis matrix $\boldsymbol{B}$. Furthermore, we employ the unraveled linearization to construct triangular matrices. Observe that the modular polynomial

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

becomes the same as Boneh-Durfee's one

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

by introducing a linearized variable

$$w := \ell_0 + x,$$

where the absolute value of the solution $w=\ell$ is bounded above by $W := N^\beta$ within a constant factor. Hence, our matrix construction starts from that of the Boneh-Durfee weaker attack in Section 3.1. Then, we partially apply unraveling $w=\ell_0+x$ to utilize the given MSBs.

Proof of the Condition (1) of Ernst et al. As Sarkar et al., we solve the modular equation $f_{MSBs}(x,y)=0$ and use the shift-polynomials $g_{[u,i]}^{MSBs.x}(w,x,y)$ and $g_{[u,j]}^{MSBs.y}(w,x,y)$ defined in (5). As a lattice construction of the Boneh-Durfee weaker attack, we use shift-polynomials $g_{[u,i]}^{MSBs.x}(wW,xX,yY)$ for $(u,i)\in\mathcal{I}_{BD,x}$ and $g_{[u,j]}^{MSBs.y}(wW,xX,yY)$ for $(u,j)\in\mathcal{I}_{BD,y1}$, where sets

of indices $\mathcal{I}_{BD,x}$ and $\mathcal{I}_{BD,y1}$ were defined in Section 3.1, then construct a basis matrix $\boldsymbol{B}$. As in Lemma 2, we can construct a triangular matrix if we only use a linearized variable w and do not use x. To utilize the given partial information and equivalently a variable x, we construct a triangular matrix as follows.

Lemma 6. *Let shift-polynomials $g^{MSBs.x}_{[u,i]}(w,x,y)$ and $g^{MSBs.y}_{[u,j]}(w,x,y)$, sets of indices $\mathcal{I}_{BD,x}$ and $\mathcal{I}_{BD,y1}$, a function $l^{MSBs}_{k,0}(\cdot)$ be defined as in (5), (2), and Definition 2, respectively. Let $\boldsymbol{B}$ be a matrix whose rows consist of coefficients of $g^{MSBs.x}_{[u,i]}(wW,xX,yY)$ for $(u,i) \in \mathcal{I}_{BD,x}$ and $g^{MSBs.y}_{[u,j]}(wW,xX,yY)$ for $(u,j) \in \mathcal{I}_{BD,y1}$. If the shift-polynomials are ordered as*

- $g^{MSBs.x}_{[u',i']}(wW,xX,yY) \prec g^{MSBs.x}_{[u,i]}(wW,xX,yY)$ *for*
  - $u' < u$,
  - $u' = u, i' < i$,
- $g^{MSBs.x}_{[u',i']}(wW,xX,yY) \prec g^{MSBs.y}_{[u,j]}(wW,xX,yY)$ *for* $u' \leq u$,
- $g^{MSBs.y}_{[u',j']}(wW,xX,yY) \prec g^{MSBs.x}_{[u,i]}(wW,xX,yY)$ *for* $u' < u$,
- $g^{MSBs.y}_{[u',j']}(wW,xX,yY) \prec g^{MSBs.y}_{[u,j]}(wW,xX,yY)$ *for*
  - $u' < u$,
  - $u' = u, j' < j'$,

then the matrix $\boldsymbol{B}$ becomes triangular with diagonals

- $W^{l^{MSBs}_{k,0}(i)} X^{u-l^{MSBs}_{k,0}(i)} Y^i e^{m-i}$ *for* $g^{MSBs.x}_{[u,i]}(wW,xX,yY)$,
- $W^{l^{MSBs}_{k,0}(u+j)} X^{u-l^{MSBs}_{k,0}(u+j)} Y^{u+j} e^{m-u}$ *for* $g^{MSBs.y}_{[u,j]}(wW,xX,yY)$.

If we apply linearization $\ell_0 + x \Rightarrow w$ to all terms, $f_{MSBs}(x,y) = f_{BD}(w,y)$ holds. Hence, a basis matrix $\boldsymbol{B}$ is the same as that of the Boneh-Durfee weaker attack in Lemma 2. To utilize partial information ℓ_0, we apply unraveling $w \Rightarrow \ell_0 + x$ and obtain a matrix as stated in Lemma 6. How much we apply linearization/unraveling is controlled by a function $l^{MSBs}_{k,0}(\cdot)$.

Table 7 shows an example of the matrix that has the same polynomials as Boneh-Durfee's weaker matrix in Table 3. To illustrate our idea, we use the examples. Here, please replace a variable x, a polynomial $g^{BD.x}_{[u,i]}$ and $g^{BD.y}_{[u,j]}$ in Table 3 by w, $g^{MSBs.x}_{[u,i]}$, and $g^{MSBs.y}_{[u,j]}$, respectively, in mind. Boneh-Durfee's weaker matrix has diagonals y, wy, and w^2y for $g^{MSBs.y}_{[0,1]}, g^{MSBs.x}_{[0,1]}$, and $g^{MSBs.x}_{[1,1]}$ whereas our matrix has diagonals y, xy, and x^2y for the same polynomials. We apply unravelings $w \Rightarrow \ell_0 + x$ and transform the former diagonals to the latter diagonals by using the following simple relations:

$$wy = (\ell_0 + x)y = \ell_0 y + xy \qquad \text{and} \qquad w^2y = (\ell_0 + x)^2 y = \ell_0^2 y + 2\ell_0 xy + x^2 y.$$

Table 7: Matrix $\boldsymbol{B}$ for Ernst et al.'s partial key exposure attack with the MSBs for $m = 2$ and $\kappa = 1$.

	1	y	y^2	x	xy	xy^2	wy^3	x^2	x^2y	x^2y^2	wxy^3	w^2y^4
$g_{[0,0]}^{MSBs.x}$	e^2											
$g_{[0,1]}^{MSBs.y}$		Ye^2										
$g_{[0,2]}^{MSBs.y}$			Y^2e^2									
$g_{[1,0]}^{MSBs.x}$				Xe^2								
$g_{[0,1]}^{MSBs.x}$	–	–		–	XYe							
$g_{[1,1]}^{MSBs.y}$		–	–		–	XY^2e						
$g_{[1,2]}^{MSBs.y}$			–			–	WY^3e					
$g_{[2,0]}^{MSBs.x}$								X^2e^2				
$g_{[1,1]}^{MSBs.x}$				–	–			–	X^2Ye			
$g_{[0,2]}^{MSBs.x}$	–	–	–	–	–	–		–	–	X^2Y^2		
$g_{[2,1]}^{MSBs.y}$		–	–		–	–	–		–	–	WXY^3	
$g_{[2,2]}^{MSBs.y}$			–			–	–			–	–	W^2Y^4

The relation suggests that all integer linear combinations of (y, wy) and (y, wy, w^2y) can be rewritten as those of (y, xy) and (y, xy, x^2y), respectively. Hence, the matrix is still triangular even if we apply the unravelings. Here, we want to claim that integer linear combinations of (wy) and (wy, w^2y) cannot be rewritten as those of (xy) and (xy, x^2y), respectively. To apply the above unraveling, the existence of y is essential. Without the variable y, we cannot replace wy and w^2y by xy and x^2y, respectively. However, if wy exists, we can replace w^2y by wxy since

$$w^2y = w(\ell_0 + x)y = \ell_0 wy + wxy.$$

Therefore, we define the function $l_{k,0}^{MSBs}(\cdot)$ so that $w^{l_{k,0}^{MSBs}(i_y)}y^{i_y}$ exists, however, $w^{l_{k,0}^{MSBs}(i_y)-1}y^{i_y}, w^{l_{k,0}^{MSBs}(i_y)-2}y^{i_y}, \cdots$ do not exist in Boneh-Durfee's weaker matrix $\boldsymbol{B}$. In other words, in the set of indices $\mathcal{I}_{BD.y1}$, there are indices $(u, u+j) = (l_{k,0}^{MSBs}(u'+j'), u'+j'), (l_{k,0}^{MSBs}(u'+j')+1, u'+j'), \ldots, (m, u'+j')$ whereas no $(u, u+j) = (0, u'+j'), (1, u'+j'), \ldots, (l_{k,0}^{MSBs}(u'+j')-1, u'+j')$ for a fixed $u'+j'$. The fact follows from that

- $k < j'$ for $u < l_{k,0}^{MSBs}(u+j')$ since $u < u + j' - k$ holds,
- $k \geq j'$ for $u \geq l_{k,0}^{MSBs}(u+j')$ since $u \geq u + j' - k$ holds.

Therefore, the function $l_{k,0}^{MSBs}(\cdot)$ tells us the maximum unraveling which we can apply.

Proof of Lemma 6. From Lemma 2, it is straightforward that we can prove the shift-polynomials in Lemma 6 derive a triangular basis matrix with diagonals

- $W^u Y^i e^{m-i}$ for $g^{MSBs.x}_{[u,i]}(wW, xX, yY)$,
- $W^u Y^{u+j} e^{m-u}$ for $g^{MSBs.y}_{[u,j]}(wW, xX, yY)$.

We apply unraveling $w = \ell_0 + x$ to each variable of the above matrix. Since the diagonals of $g^{MSBs.x}_{[u,i]}(wW, xX, yY)$ for[4] $(u, i) = (l^{MSBs}_{k,0}(i), i)$ and those of $g^{MSBs.y}_{[u,j]}(wW, xX, yY)$ for $(u, u+j) = (l^{MSBs}_{k,0}(u+j), u+j)$ are the same between Lemmas 2 and 6, we focus on the other variables[5]

- $w^{l^{MSBs}_{k,0}(i_y)} x^{u - l^{MSBs}_{k,0}(i_y)} y^{i_y}$ for $i_y = 0, 1, \ldots, m+k; u = l^{MSBs}_{k,0}(i_y) + 1, l^{MSBs}_{k,0}(i_y) + 2, \ldots, m$.

We want to claim that a matrix $\boldsymbol{B}$ is still triangular when all variables $w^u y^{i_y}$ are replaced by $w^{l^{MSBs}_{k,0}(i_y)} x^{u - l^{MSBs}_{k,0}(i_y)} y^{i_y}$.

Here, we show an inductive proof that

$$w^u = \sum_{t=0}^{u - l^{MSBs}_{k,0}(i_y)} c_t w^{l^{MSBs}_{k,0}(i_y)} x^t$$

holds, where $c_0, c_1, \ldots, c_{u - l^{MSBs}_{k,0}(i_y)}$ are integers and $c_{u - l^{MSBs}_{k,0}(i_y)} = 1$. The statement holds for $u = l^{MSBs}_{k,0}(i_y)$. We assume that the statement holds for fixed $u = u'$ and prove that the statement also holds for $u = u' + 1$. It follows that

$$\begin{aligned}
w^{u'+1} &= w^{u'}(\ell_0 + x) \\
&= \left(\sum_{t=0}^{u' - l^{MSBs}_{k,0}(i'_y)} c_t w^{l^{MSBs}_{k,0}(i'_y)} x^t \right) (\ell_0 + x) \\
&= \sum_{t=0}^{u' - l^{MSBs}_{k,0}(i'_y)} c_t \ell_0 w^{l^{MSBs}_{k,0}(i'_y)} x^t + \left(\sum_{t=0}^{u' - l^{MSBs}_{k,0}(i'_y) - 1} c_t w^{l^{MSBs}_{k,0}(i'_y)} x^t + w^{l^{MSBs}_{k,0}(i'_y)} x^{u' - l^{MSBs}_{k,0}(i'_y)} \right) x \\
&= \sum_{t=0}^{u' - l^{MSBs}_{k,0}(i'_y)} c'_t w^{l^{MSBs}_{k,0}(i'_y)} x^t + w^{l^{MSBs}_{k,0}(i'_y)} x^{u' - l^{MSBs}_{k,0}(i'_y) + 1},
\end{aligned}$$

where $c'_0, c'_1, \ldots, c'_{u' - l^{MSBs}_{k,0}(i'_y)}$ are integers. Hence, the statement holds for all (u, i_y). By using the relation, we can replace all integer linear combinations of $\sum_{u = l^{MSBs}_{k,0}(i_y)}^{u'} d_u w^u y^{i_y}$ by $\sum_{u = l^{MSBs}_{k,0}(i_y)}^{u'} d'_u w^{l^{MSBs}_{k,0}(i_y)} x^{u - l^{MSBs}_{k,0}(i_y)} y^{i_y}$, where $d_{l^{MSBs}_{k,0}(i_y)}, d_{l^{MSBs}_{k,0}(i_y)+1}, \ldots, d_{u'}$ and $d'_{l^{MSBs}_{k,0}(i_y)}, d'_{l^{MSBs}_{k,0}(i_y)+1}, \ldots, d'_{u'}$ are integers such that $d_{u'} = d'_{u'}$. Thus, we can replace all variables $w^u y^{i_y}$ by $w^{l^{MSBs}_{k,0}(i_y)} x^{u - l^{MSBs}_{k,0}(i_y)} y^{i_y}$. Hence, we complete the proof. □

[4] When $k > 0$, there is an index $(u, i) \in \mathcal{I}_{BD.x}$ such that $u = l^{MSBs}_{k,0}(i)$ only for $(u, i) = (0, 0)$.

[5] These variables are diagonals for both $g^{MSBs.x}_{[u,i]}(wW, xX, yY)$ and $g^{MSBs.y}_{[u,j]}(wW, xX, yY)$.

To obtain the bound (i), we compute a dimension

$$n = \sum_{(u,i)\in\mathcal{I}_{BD,x}} 1 + \sum_{(u,j)\in\mathcal{I}_{BD,y1}} 1 = \left(\frac{1}{2}+\kappa\right)m^2 + o(m^2),$$

and a determinant $\det(\boldsymbol{B}) = W^{s_W}X^{s_X}Y^{s_Y}e^{s_e}$, where

$$\begin{aligned}
s_W &= \sum_{(u,i)\in\mathcal{I}_{BD,x}} l_{k,0}^{MSBs}(i) + \sum_{(u,j)\in\mathcal{I}_{BD,y1}} l_{k,0}^{MSBs}(u+j) = \frac{1}{6}m^3 + o(m^3),\\
s_X &= \sum_{(u,i)\in\mathcal{I}_{BD,x}} \left(u - l_{k,0}^{MSBs}(i)\right) + \sum_{(u,j)\in\mathcal{I}_{BD,y1}} \left(u - l_{k,0}^{MSBs}(u+j)\right) = \left(\frac{1}{6}+\frac{\kappa}{2}\right)m^3 + o(m^3),\\
s_Y &= \sum_{(u,i)\in\mathcal{I}_{BD,x}} i + \sum_{(u,j)\in\mathcal{I}_{BD,y1}} (u+j) = \frac{(1+\kappa)^3-\kappa^3}{6}m^3 + o(m^3),\\
s_e &= \sum_{(u,i)\in\mathcal{I}_{BD,x}} (m-i) + \sum_{(u,j)\in\mathcal{I}_{BD,y1}} (m-u) = \left(\frac{1}{3}+\frac{\kappa}{2}\right)m^3 + o(m^3).
\end{aligned}$$

New polynomials which are derived from outputs of the LLL algorithm satisfy Howgrave-Graham's lemma when $(\det(\boldsymbol{B}))^{1/n} < e^m$, i.e.,

$$\beta\frac{1}{6} + \gamma\left(\frac{1}{6}+\frac{\kappa}{2}\right) + \frac{1}{2}\left(\frac{(1+\kappa)^3-\kappa^3}{6}\right) + \frac{1}{3} + \frac{\kappa}{2} < \frac{1}{2} + \kappa,$$

by omitting small terms. To maximize the right hand side of the inequality, we set

$$\kappa = \frac{1-2\gamma}{2}$$

and obtain an inequality

$$12\gamma^2 - 20\gamma + 7 - 8\beta > 0.$$

By solving the inequality, we obtain the condition (1) of Ernst et al.'s attack

$$\delta < \frac{5 - 2\sqrt{1+6\beta}}{6}$$

since $\gamma = \delta$ holds. Hence, we conclude the proof. □

4.4 Our Attack

In this subsection, we propose our improved partial key exposure attacks with the MSBs of d.

Theorem 1. *Given a public key (N, e) of RSA such that e is full size and $d = N^{\beta}$ along with $d_0 > N^{\beta-\delta}$ which is the MSBs of d, if N is sufficiently large and polynomials output by the LLL will not vanish, then there is a polynomial time factorization algorithm for N when*

$$(i)\ \delta < \frac{1+\beta-\sqrt{-1+6\beta-3\beta^2}}{2} \quad \text{and} \quad \beta \le \frac{1}{2},$$
$$(ii)\ 6\gamma\sigma - 3\sigma^2 + 2\sigma^3 < \frac{(\sigma - 2(\beta-\gamma))^3}{2+2\gamma-4\beta},\ \sigma = 1 - \frac{2\beta-1}{1-2\sqrt{1+\gamma-2\beta}}, \quad \text{and} \quad \frac{1}{2} < \beta \le \frac{9}{16}.$$

The attack is an appropriate extension of the Boneh-Durfee stronger attack in the sense that the first bound (i) of Theorem 1 is $\beta < 1 - 1/\sqrt{2}$ for $\delta = \beta$. We obtain the improved attack by modifying a polynomial selection for the same shift-polynomials as Sarkar et al. [SSM10].

At first, we focus on the first condition (i) for $\beta \le 1/2$.

Proof of the Condition (i) of Theorem 1. As Sarkar et al., we solve the modular equation $f_{MSBs}(x, y) = 0$ and use the shift-polynomials $g_{[u,i]}^{MSBs.x}(w, x, y)$ and $g_{[u,j]}^{MSBs.y}(w, x, y)$ defined in (5). As a lattice construction of the Boneh-Durfee stronger attack, we use shift-polynomials $g_{[u,i]}^{MSBs.x}(wW, xX, yY)$ for $(u, i) \in \mathcal{I}_{BD,x}$ and $g_{[u,j]}^{MSBs.y}(wW, xX, yY)$ for $(u, j) \in \mathcal{I}_{BD,y2}$, where sets of indices $\mathcal{I}_{BD,x}$ and $\mathcal{I}_{BD,y2}$ were defined in Section 3.1, then construct a basis matrix $\boldsymbol{B}$. As in Lemma 5, we can construct a triangular matrix if we only use w along with a linearized variable

$$z := 1 + wy = 1 + (\ell_0 + x)y,$$

where the absolute value of the root is bounded above by $Z := N^{\beta+1/2}$ within a constant factor, and do not use x. To utilize the given partial information and equivalently a variable x, we construct a triangular matrix as follows.

Lemma 7. *Let shift-polynomials $g_{[u,i]}^{MSBs.x}(w, x, y)$ and $g_{[u,j]}^{MSBs.y}(w, x, y)$, sets of indices $\mathcal{I}_{BD,x}$ and $\mathcal{I}_{BD,y2}$, a function $l_{k,\tau}^{MSBs}(x)$ be defined as in (5), (3), and Definition 2, respectively. Let $\boldsymbol{B}$ be a matrix whose rows consist of coefficients of $g_{[u,i]}^{MSBs.x}(wW, xX, yY)$ for $(u, i) \in \mathcal{I}_{BD,x}$ and $g_{[u,j]}^{MSBs.y}(wW, xX, yY)$ for $(u, j) \in \mathcal{I}_{BD,y2}$. If the shift-polynomials are ordered as the same way in Lemma 6, then the matrix $\boldsymbol{B}$ becomes triangular with diagonals*

- $X^{u-l_{k,\tau}^{MSBs}(i)} Y^{i-l_{k,\tau}^{MSBs}(i)} Z^{l_{k,\tau}^{MSBs}(i)} e^{m-i}$ *for* $g_{[u,i]}^{MSBs.x}(wW, xX, yY)$,
- $X^{u-l_{k,\tau}^{MSBs}(u+j)} Y^{u+j-l_{k,\tau}^{MSBs}(u+j)} Z^{l_{k,\tau}^{MSBs}(u+j)} e^{m-u}$ *for* $g_{[u,j]}^{MSBs.y}(wW, xX, yY)$.

If we apply linearization $\ell_0 + x \Rightarrow w$ to all terms, $f_{MSBs}(x, y) = f_{BD}(w, y)$ holds. Hence, a basis matrix $\boldsymbol{B}$ is the same as that of the Boneh-Durfee stronger attack. To utilize partial information ℓ_0, we apply unraveling $w \Rightarrow \ell_0 + x$ and obtain a matrix as stated in Section 3.3. How much we apply linearization/unraveling is controlled by a function $l_{k,\tau}^{MSBs}(\cdot)$.

Table 8 shows an example of the matrix that has the same polynomials as Boneh-Durfee's stronger matrix with additional unravelings in Table 6. To illustrate our idea, we use the examples. Here, please replace a variable x, a polynomial $g_{[u,i]}^{BD.x}$ and $g_{[u,j]}^{BD.y}$ in Table 6 by w, $g_{[u,i]}^{MSBs.x}$, and

Table 8: Our matrix $\boldsymbol{B}$ of a partial key exposure attack with the MSBs for $m = 2$ and $\kappa = 1/2, \tau = 1$.

	1	y	x	xy	yz	y^2z	x^2	x^2y	xyz	xy^2z	y^2z^2	y^3z^2
$g_{[0,0]}^{MSBs.x}$	e^2											
$g_{[0,1]}^{MSBs.y}$		Ye^2										
$g_{[1,0]}^{MSBs.x}$			Xe^2									
$g_{[0,1]}^{MSBs.x}$	–	–	–	XYe								
$g_{[1,1]}^{MSBs.y}$		–		–	YZe							
$g_{[1,2]}^{MSBs.y}$		–			–	Y^2Ze						
$g_{[2,0]}^{MSBs.x}$							X^2e^2					
$g_{[1,1]}^{MSBs.x}$			–	–			–	X^2Ye				
$g_{[0,2]}^{MSBs.x}$	–	–	–	–	–		–	–	XYZ			
$g_{[2,1]}^{MSBs.y}$		–		–	–	–		–	–	XY^2Z		
$g_{[2,2]}^{MSBs.y}$		–		–	–	–			–	–	Y^2Z^2	
$g_{[2,3]}^{MSBs.y}$		–			–	–				–	–	Y^3Z^2

$g_{[u,j]}^{MSBs.y}$, respectively, in mind. The matrix in Table 6 has diagonals w, wy, w^2, w^2y, w^2y^2, and w^2y^3 for $g_{[1,0]}^{MSBs.x}, g_{[0,1]}^{MSBs.x}, g_{[2,0]}^{MSBs.x}, g_{[1,1]}^{MSBs.x}, g_{[0,2]}^{MSBs.x}$, and $g_{[2,1]}^{MSBs.y}$ whereas our matrix has diagonals x, xy, x^2y, xyz, and xy^2z for the same polynomials. We apply unravelings $w \Rightarrow \ell_0 + x$ and transform the former diagonals to the latter diagonals. Here, we use the same relation which was used in Lemma 6. Hence, the core of a proof of Lemma 7 is the similar to that of Lemma 6.

Proof of Lemma 7. From the discussion at the end of Section 3.3, it is straightforward that we can prove the shift-polynomials in Lemma 7 derive a triangular basis matrix with diagonals

- $W^{u-l_{k,\tau}^{MSBs}(i)} Y^{i-l_{k,\tau}^{MSBs}(i)} Z^{l_{k,\tau}^{MSBs}(i)} e^{m-i}$ for $g_{[u,i]}^{MSBs.x}(wW, xX, yY)$,
- $W^{u-l_{k,\tau}^{MSBs}(u+j)} Y^{u+j-l_{k,\tau}^{MSBs}(u+j)} Z^{l_{k,\tau}^{MSBs}(u+j)} e^{m-u}$ for $g_{[u,j]}^{MSBs.y}(wW, xX, yY)$.

We apply unraveling $w \Rightarrow \ell_0 + x$ to each variable of the above matrix. Since

$$w^{i_w} = (\ell_0 + x)^{i_w} = \sum_{t=0}^{i_w} c_t w^{i_w - t} x^t \tag{6}$$

holds, where $c_0, c_1, \ldots, c_{i_w}$ are integers and $c_{i_w} = 1$, we can replace all integer linear combinations of $\sum_{i_w=0}^{u-l_{k,\tau}^{MSBs}(i_y+i_z)} d_{i_w} w^{i_w} y^{i_y} z^{i_z}$ by $\sum_{i_x=0}^{u-l_{k,\tau}^{MSBs}(i_y+i_z)} d'_{i_x} x^{i_x} y^{i_y} z^{i_z}$, where $d_0, d_1, \ldots, d_{u-l_{k,\tau}^{MSBs}(i_y+i_z)}$ and $d'_0, d'_1, \ldots, d'_{u-l_{k,\tau}^{MSBs}(i_y+i_z)}$ are integers such that $d_{u-l_{k,\tau}^{MSBs}(i_y+i_z)} = d'_{u-l_{k,\tau}^{MSBs}(i_y+i_z)}$. Thus, we can replace all the above variables by those of Lemma 7. Hence, we complete the proof. □

To make use of the given MSBs d_0, we set

$$\kappa = 2(\beta - \gamma) \qquad \text{and} \qquad \tau = 1 + 2\gamma - 4\beta$$

and use the set of indices $\mathcal{I}_{BD.y2}$ by following the lemma.

Lemma 8. *In the matrix $\boldsymbol{B}$ of Lemma 7, polynomials $g^{MSBs.y}_{[u,j]}(x,y)$ are helpful if and only if $j \leq 2(\beta-\gamma)m + (1+2\gamma-4\beta)u$ for all u.*

Proof of Lemma 8. Let $g^{MSBs.y}_{[u',j']}(x,y)$ be a polynomial with fixed indices (u',j') such that

$$u' = l^{MSBs}_{k,\tau}(u'+j'),$$

and $\boldsymbol{B'}$ be a matrix that is a matrix $\boldsymbol{B}$ without the polynomial $g^{MSBs.y}_{[u',j']}(x,y)$. As stated in Lemma 7, diagonals of the polynomial $g^{MSBs.y}_{[u',j']}(x,y)$ in $\boldsymbol{B}$ is

$$Y^{j'}Z^{u'}e^{m-u'}.$$

Furthermore, diagonals of polynomials

$$g^{MSBs.y}_{[u'+1,j'-1]}(x,y), g^{MSBs.y}_{[u'+2,j'-2]}(x,y), \ldots, g^{MSBs.y}_{[u'+j'-1,1]}(x,y)$$

and

$$g^{MSBs.x}_{[u'+j',u'+j']}(x,y), g^{MSBs.x}_{[u'+j'+1,u'+j']}(x,y), \ldots, g^{MSBs.x}_{[m,u'+j']}(x,y)$$

in $\boldsymbol{B}$ are

$$XY^{j'}Z^{u'}e^{m-u'-1}, X^2Y^{j'}Z^{u'}e^{m-u'-2}, \ldots, X^{j'-1}Y^{j'}Z^{u'}e^{m-u'-j'+1}$$

and

$$X^{j'}Y^{j'}Z^{u'}e^{m-u'-j'}, X^{j'+1}Y^{j'}Z^{u'}e^{m-u'-j'}, \ldots, X^{m-u'}Y^{j'}Z^{u'}e^{m-u'-j'}.$$

On the other hand, by following the proof of Lemma 7, diagonals of the same polynomials in $\boldsymbol{B'}$ are

$$Y^{j'-1}Z^{u'+1}e^{m-u'-1}, XY^{j'-1}Z^{u'+1}e^{m-u'-2}, \ldots, X^{j'-2}Y^{j'-1}Z^{u'+1}e^{m-u'-j'+1}$$

and

$$X^{j'-1}Y^{j'-1}Z^{u'+1}e^{m-u'-j'}, X^{j'}Y^{j'-1}Z^{u'+1}e^{m-u'-j'}, \ldots, X^{m-u'-1}Y^{j'-1}Z^{u'+1}e^{m-u'-j'}.$$

Hence,

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

that is smaller than or equal to the modulus e^m if and only if

$$Y^{j'}Z^{u'}e^{m-u'} \cdot \left(\frac{XY}{Z}\right)^{m-u'} \leq e^m \Leftrightarrow Y^{j'}Z^{u'} \cdot \left(\frac{XY}{Z}\right)^{m-u'} \leq e^{u'}$$

$$\begin{aligned}
&\Leftrightarrow X^{m-u'}Y^{j'+m-u'}Z^{2u'-m} \leq e^{u'} \\
&\Leftrightarrow \gamma(m-u') + \frac{1}{2}\left(j'+m-u'\right) + \left(\beta+\frac{1}{2}\right)(2u'-m) \leq u' \\
&\Leftrightarrow j' \leq 2(\beta-\gamma)m + (1+2\gamma-4\beta)u'.
\end{aligned}$$

Hence, we conclude the proof. □

To obtain the bound (i) of Theorem 1, we compute a dimension

$$n = \sum_{(u,i)\in\mathcal{I}_{BD,x}} 1 + \sum_{(u,j)\in\mathcal{I}_{BD,y2}} 1 = \left(\frac{1}{2} + 2(\beta-\gamma) + \frac{1+2\gamma-4\beta}{2}\right)m^2 + o(m^2),$$

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

$$\begin{aligned}
s_X &= \sum_{(u,i)\in\mathcal{I}_{BD,x}} \left(u - l_{k,\tau}^{MSBs}(i)\right) + \sum_{(u,j)\in\mathcal{I}_{BD,y2}} \left(u - l_{k,\tau}^{MSBs}(u+j)\right) \\
&= \left(\frac{1}{6} + (\beta-\gamma) + \frac{1+2\gamma-4\beta}{6}\right)m^3 + o(m^3), \\
s_Y &= \sum_{(u,i)\in\mathcal{I}_{BD,x}} \left(i - l_{k,\tau}^{MSBs}(i)\right) + \sum_{(u,j)\in\mathcal{I}_{BD,y2}} \left(u+j - l_{k,\tau}^{MSBs}(u+j)\right) \\
&= \left((\beta-\gamma) + 2(\beta-\gamma)^2 + (\beta-\gamma)(1+2\gamma-4\beta) + \frac{1+2\gamma-4\beta}{6} + \frac{(1+2\gamma-4\beta)^2}{6}\right)m^3 + o(m^3), \\
s_Z &= \sum_{(u,i)\in\mathcal{I}_{BD,x}} l_{k,\tau}^{MSBs}(i) + \sum_{(u,j)\in\mathcal{I}_{BD,y2}} l_{k,\tau}^{MSBs}(u+j) = \left(\frac{1}{6} + \frac{1+2\gamma-4\beta}{6}\right)m^3 + o(m^3), \\
s_e &= \sum_{(u,i)\in\mathcal{I}_{BD,x}} (m-i) + \sum_{(u,j)\in\mathcal{I}_{BD,y2}} (m-u) = \left(\frac{1}{3} + (\beta-\gamma) + \frac{1+2\gamma-4\beta}{6}\right)m^3 + o(m^3).
\end{aligned}$$

New polynomials which are derived from outputs of the LLL algorithm satisfy Howgrave-Graham's lemma when $(\det(\boldsymbol{B}))^{1/n} < e^m$. By omitting small terms, we obtain an inequality

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

By solving the inequality, we obtain the first bound (i) of Theorem 1

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

since $\gamma = \delta$ holds. Hence, we conclude the proof. □

Before providing a proof of the second condition (ii) of Theorem 1, we explain that the set of indices

$$\mathcal{I}_{BD.y2} = \{u = 0, 1, \ldots, m; j = 1, 2, \ldots, 2(\beta-\gamma)m + \lfloor(1+2\gamma-4\beta)u\rfloor\}$$

which was used for the condition (i) to select shift-polynomials $g_{[u,j]}^{MSBs.y}(x,y)$ is not useful for $\beta > 1/2$. Observe that an upper bound of j is negative for large u since $2(\beta-\gamma)m+\lfloor(1+2\gamma-4\beta)m\rfloor < (1-2\beta)m < 0$ for $\beta > 1/2$. A naive modification is replacing the upper bound by $\max\{0, 2(\beta-\gamma)m+\lfloor(1+2\gamma-4\beta)u\rfloor\}$. However, in this case, there are useless polynomials $g_{[u,i]}^{MSBs.x}(x,y)$ for $(u,i) \in \mathcal{I}_{BD.x}$. In particular, shift-polynomials $g_{[u',i']}^{MSBs.x}(x,y)$ for large u' contributed to the matrix $\boldsymbol{B}$ to be triangular. However, if there are no $g_{[u,j]}^{MSBs.y}(x,y)$ for the same u', the matrix $\boldsymbol{B}$ becomes triangular without the polynomials $g_{[u',i']}^{MSBs.x}(x,y)$ and the polynomials degrade the quality of $\boldsymbol{B}$. Hence, some polynomials $g_{[u,i]}^{MSBs.x}(x,y)$ for large u should be omitted from the above matrix $\boldsymbol{B}$. On the other hand, we cannot omit all such polynomials $g_{[u,i]}^{MSBs.x}(x,y)$ since the polynomials $g_{[u',i']}^{MSBs.x}(x,y)$ for small i' contributed for polynomials $g_{[u,j]}^{MSBs.y}(x,y)$ for $i' = u+j$ to be helpful by following the proof of Lemma 8.

Thus, we modify definition of sets of indices such as

$$\begin{aligned}\mathcal{I}_{MSBs.x} &:= \{u = 0,1,\ldots,m; i = 0,1,\ldots,\min\{u,s\}\},\\ \mathcal{I}_{MSBs.y} &:= \{u = 0,1,\ldots,s-1; j = 1,2,\ldots,\min\{k+\lfloor\tau u\rfloor, s-u\}\}\end{aligned} \tag{7}$$

with an additional parameter $\sigma := s/m$. As the case for $\beta \le 1/2$, all shift-polynomials $g_{[u,j]}^{MSBs.y}(x,y)$ for $(u,j) \in \mathcal{I}_{MSBs.y}$ are helpful. The core trick of the modification is that although the polynomials

$$g_{[u,s-u+1]}^{MSBs.y}(x,y), g_{[u,s-u+2]}^{MSBs.y}(x,y), \ldots, g_{[u,k+\lfloor\tau u\rfloor]}^{MSBs.y}(x,y)$$

are helpful, we do not use them. To be precise, let $j' = k+\lfloor\tau u'\rfloor$. Then, for the polynomial $g_{[u',j']}^{MSBs.y}(x,y)$ whose corresponding diagonal is $W^{u'}Y^{u'+j'}e^{m-u'}$ to be helpful, we should also use polynomials

$$g_{[u'+1,j'-1]}^{MSBs.y}(x,y), g_{[u'+2,j'-2]}^{MSBs.y}(x,y), \ldots, g_{[u'+j'-1,1]}^{MSBs.y}(x,y)$$

and

$$g_{[u'+j',u'+j']}^{MSBs.x}(x,y), g_{[u'+j'+1,u'+j']}^{MSBs.x}(x,y), \ldots, g_{[m,u'+j']}^{MSBs.x}(x,y)$$

whose corresponding diagonals in a matrix $\boldsymbol{B}$ are

$$W^{u'}XY^{u'+j'}e^{m-u'-1}, W^{u'}X^2Y^{u'+j'}e^{m-u'-2}, \ldots, W^{u'}X^{j'-1}Y^{u'+j'}e^{m-u'-j'+1},$$

and

$$W^{u'}X^{j'}Y^{u'+j'}e^{m-u'-j'}, W^{u'}X^{j'+1}Y^{u'+j'}e^{m-u'-j'}, \ldots, W^{u'}X^{m-u'}Y^{u'+j'}e^{m-u'-j'}.$$

When the diagonal $W^{u'}Y^{u'+j'}e^{m-u'}$ of helpful $g_{[u',j']}^{MSBs.y}(x,y)$ is close to e^m, a set of the polynomials may degrade the quality of the matrix $\boldsymbol{B}$ since other diagonals are large. Hence, we introduce a parameter $\sigma = s/m$ to verify whether the set of polynomials is helpful or not.

Proof of the Condition (ii) of Theorem 1. As Sarkar et al. and the condition (i) of Theorem 1, we solve the modular equation $f_{MSBs}(x,y)=0$ and use the shift-polynomials $g_{[u,i]}^{MSBs.x}(w,x,y)$ and $g_{[u,j]}^{MSBs.y}(w,x,y)$ defined in (5). We use shift-polynomials $g_{[u,i]}^{MSBs.x}(wW,xX,yY)$ for $(u,i)\in\mathcal{I}_{MSBs,x}$ and $g_{[u,j]}^{MSBs.y}(wW,xX,yY)$ for $(u,j)\in\mathcal{I}_{MSBs,y}$, where sets of indices $\mathcal{I}_{MSBs,x}$ and $\mathcal{I}_{MSBs,y}$ were defined in (7), then construct a basis matrix $\boldsymbol{B}$. As in Section 4.3, we construct a triangular matrix with a linearized variable

$$w := \ell_0 + x,$$

where the absolute value of the root is bounded above by $W := N^{\beta}$ within a constant factor. To utilize the given partial information and equivalently a variable x, we construct a triangular matrix as follows.

Lemma 9. *Let shift-polynomials $g_{[u,i]}^{MSBs.x}(w,x,y)$ and $g_{[u,j]}^{MSBs.y}(w,x,y)$, sets of indices $\mathcal{I}_{MSBs,x}$ and $\mathcal{I}_{MSBs,y}$, a function $l_{k,\tau}^{MSBs}(x)$ be defined as in (5), (7), and Definition 2, respectively. Let $\boldsymbol{B}$ be a matrix whose rows consist of coefficients of $g_{[u,i]}^{MSBs.x}(wW,xX,yY)$ for $(u,i)\in\mathcal{I}_{MSBs,x}$ and $g_{[u,j]}^{MSBs.y}(wW,xX,yY)$ for $(u,j)\in\mathcal{I}_{MSBs,y}$. If the shift-polynomials are ordered as the same way in Lemmas 6 and 7, then the matrix $\boldsymbol{B}$ becomes triangular with diagonals*

- $W^{l_{k,\tau}^{MSBs}(i)}X^{u-l_{k,\tau}^{MSBs}(i)}Y^{i}e^{m-i}$ *for* $g_{[u,i]}^{MSBs.x}(wW,xX,yY)$,
- $W^{l_{k,\tau}^{MSBs}(u+j)}X^{u-l_{k,\tau}^{MSBs}(u+j)}Y^{u+j}e^{m-u}$ *for* $g_{[u,j]}^{MSBs.y}(wW,xX,yY)$.

We omit a detailed proof of Lemma 9. It is almost trivial that the matrix becomes triangular with diagonals

- $W^{u}Y^{i}e^{m-i}$ for $g_{[u,i]}^{MSBs.x}(wW,xX,yY)$,
- $W^{u}Y^{u+j}e^{m-u}$ for $g_{[u,j]}^{MSBs.y}(wW,xX,yY)$.

Then, by using the same relation (6) as the proof of Lemma 7, we obtain the matrix as stated in Lemma 9.

Due to Lemma 8, we set

$$\kappa = 2(\beta-\gamma) \qquad \text{and} \qquad \tau = 1+2\gamma-4\beta$$

for all shift-polynomials $g_{[u,j]}^{MSBs.y}$ to be helpful.

To obtain the bound (ii) of Theorem 1, we compute a dimension

$$n = \sum_{(u,i)\in\mathcal{I}_{MSBs,x}} 1 + \sum_{(u,j)\in\mathcal{I}_{MSBs,y}} 1 = \left(\sigma - \frac{(\sigma-2(\beta-\gamma))^2}{2(2+2\gamma-4\beta)}\right)m^2 + o(m^2),$$

and a determinant $\det(\boldsymbol{B}) = W^{s_W}X^{s_X}Y^{s_Y}e^{s_e}$, where

$$s_W = \sum_{(u,i)\in\mathcal{I}_{MSBs,x}} l_{k,\tau}^{MSBs}(i) + \sum_{(u,j)\in\mathcal{I}_{MSBs,y}} l_{k,\tau}^{MSBs}(u+j)$$

$$
\begin{aligned}
&= \left(\frac{(\sigma - 2(\beta-\gamma))^2}{2(2+2\gamma-4\beta)} - \frac{(\sigma-2(\beta-\gamma))^3}{3(2+2\gamma-4\beta)^2} \right) m^3 + o(m^3), \\
s_X &= \sum_{(u,i)\in\mathcal{I}_{MSBs,x}} \left(u - l_{k,\tau}^{MSBs}(i)\right) + \sum_{(u,j)\in\mathcal{I}_{MSBs,y}} \left(u - l_{k,\tau}^{MSBs}(u+j)\right) \\
&= \left(\frac{\sigma}{2} - \frac{(\sigma-2(\beta-\gamma))^3}{6(2+2\gamma-4\beta)^2} \right) m^3 - s_W + o(m^3), \\
s_Y &= \sum_{(u,i)\in\mathcal{I}_{MSBs,x}} i + \sum_{(u,j)\in\mathcal{I}_{MSBs,y}} (u+j) \\
&= \left(\frac{\sigma^3 - 8(\beta-\gamma)^3}{6(2+2\gamma-4\beta)} + \frac{\sigma^2}{2}\left(1 - \frac{\sigma-2(\beta-\gamma)}{2+2\gamma-4\beta}\right)\right) m^3 + o(m^3), \\
s_e &= \sum_{(u,i)\in\mathcal{I}_{MSBs,x}} (m-i) + \sum_{(u,j)\in\mathcal{I}_{MSBs,y}} (m-u) \\
&= \left(\sigma - \frac{\sigma^2}{2} + \frac{\sigma^3}{6} - \frac{(\sigma-2(\beta-\gamma))^2}{2(2+2\gamma-4\beta)} + \frac{(\sigma-2(\beta-\gamma))^3}{6(2+2\gamma-4\beta)^2} \right) m^3 + o(m^3).
\end{aligned}
$$

New polynomials which are derived from outputs of the LLL algorithm satisfy Howgrave-Graham's lemma when $(\det(\boldsymbol{B}))^{1/n} < e^m$. By omitting small terms, we obtain an inequality

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

To maximize the right hand side of the inequality, we set

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

and obtain the condition (ii) of Theorem 1. Hence, we conclude the proof. □

5 Partial Key Exposure Attacks with the LSBs

In this section, we propose our improved partial key exposure attack on RSA with the LSBs of d. In Section 5.1, we formulate the attack scenario as a modular equation. In Section 5.2, we recall previous attacks [BM03, EJMdW05, Aon09]. In Section 5.3, we propose our main attack.

5.1 Formulation

In this subsection, we formulate the attack scenario with the LSBs as modular equations. We write a secret exponent $d = N^\beta$ as $d = d_1 M + d_0$, where $d_0 > N^{\beta-\delta}$ and $d_1 < N^\delta$ denote the known LSBs and the unknown MSBs of d, respectively, with an integer $M := 2^{\lfloor(\beta-\delta)\log N\rfloor}$. Recall an RSA key generation

$$
e(d_1 M + d_0) = 1 + \ell(p-1)(q-1) = 1 + \ell(N - p - q + 1) \tag{8}
$$

with an unknown integer ℓ as in Sections 3.1 and 5.1. By taking modulo eM of the equation (8), we obtain a modular polynomial

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

whose root is $(x,y) = (\ell, -p-q+1)$. Absolute values of the root are bounded above by $X := N^{\beta}$ and $Y := N^{1/2}$ within constant factors.

5.2 Previous Works

In this subsection, we briefly recall previous attacks proposed by Ernst et al. [EJMdW05], Blömer and May [BM03], and Aono [Aon09]. Ernst et al.'s attack, which solves integer equations, works when

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

Ernst et al.'s attack can be viewed as an extension of the Boneh-Durfee weaker attack since the condition is the same as $\beta < (7-2\sqrt{7})/6 = 0.284\cdots$ for $\delta = \beta$.

We can obtain the same condition by solving a modular equation $f_{LSBs}(x,y) = 0$, where the construction is similar to Blömer and May's attack [BM03] which focused on partial key exposure attacks with large d and small e. To solve the modular equation, Blömer and May used shift-polynomials

$$\begin{aligned} g_{[u,i]}^{LSBs.x}(x,y) &:= x^{u-i} f_{LSBs}(x,y)^i (eM)^{m-i}, \\ g_{[u,j]}^{LSBs.BM}(x,y) &:= y^j f_{LSBs}(x,y)^u (eM)^{m-u}. \end{aligned} \tag{9}$$

Both shift-polynomials modulo $(eM)^m$ have the same root as the original solutions, i.e., $g_{[u,i]}^{LSBs.x}(\ell, -p-q+1) = 0 \pmod{(eM)^m}$ and $g_{[u,j]}^{LSBs.BM}(\ell, -p-q+1) = 0 \pmod{(eM)^m}$. They used shift-polynomials $g_{[u,i]}^{LSBs.x}(xX, yY)$ for $(u,i) \in \mathcal{I}_{BD,x}$ and $g_{[u,j]}^{LSBs.BM}(xX, yY)$ for $(u,j) \in \mathcal{I}_{BD,y1}$ to construct a triangular matrix $\boldsymbol{B}$ as the Boneh-Durfee weaker attack. We can obtain Ernst et al's condition by using the matrix.

To improve Ernst et al.'s attack by solving the same modular equation $f_{LSBs}(x,y) = 0$ as Blömer and May, Aono [Aon09] used the other modular polynomial

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

which we can obtain by taking modulo e of the equation (8) along with a shift-polynomial

$$g_{[u,j]}^{LSBs.Aon}(x,y) := g_{[u,j]}^{BD.y}(x,y) \cdot M^m = y^j f_{BD}(x,y)^u e^{m-u} M^m. \tag{10}$$

The shift-polynomial modulo $(eM)^m$ have the same root as the original solutions, i.e., $g_{[u,j]}^{LSBs.Aon}(\ell, -p-q+1) = 0 \pmod{(eM)^m}$. Aono defined a set of indices

$$\mathcal{I}_{Aon} := \{u = 0, 1, \ldots, m; j = 1, 2, \ldots, \lfloor \tau u \rfloor\} \setminus \mathcal{I}_{BD.y1} \tag{11}$$

Table 9: Aono's matrix $\boldsymbol{B}$ of a partial key exposure attack with the LSBs for $m = 2$ and $\kappa = 1/2, \tau = 1$.

	1	y	x	xy	xy^2	y^2z	x^2	x^2y	x^2y^2	x^2y^3	y^2z^2	y^3z^2
$g_{[0,0]}^{LSBs.x}$	$(eM)^2$											
$g_{[0,1]}^{LSBs.y}$		$Y(eM)^2$										
$g_{[1,0]}^{LSBs.x}$			$X(eM)^2$									
$g_{[0,1]}^{LSBs.x}$	–		–	$XYeM$								
$g_{[1,1]}^{LSBs.y}$		–		–	XY^2eM							
$g_{[1,2]}^{LSBs.y}$					–	Y^2ZeM^2						
$g_{[2,0]}^{LSBs.x}$							$X^2(eM)^2$					
$g_{[1,1]}^{LSBs.x}$			–				–	X^2YeM				
$g_{[0,2]}^{LSBs.x}$	–		–	–			–	–	X^2Y^2			
$g_{[2,1]}^{LSBs.y}$		–		–	–			–	–	X^2Y^3		
$g_{[2,2]}^{LSBs.y}$					–				–	–	$Y^2Z^2M^2$	
$g_{[2,3]}^{LSBs.y}$						–				–	–	$Y^3Z^2M^2$

and used shift-polynomials $g_{[u,i]}^{LSBs.x}(xX, yY)$ for $(u, i) \in \mathcal{I}_{BD,x}$, $g_{[u,j]}^{LSBs.BM}(xX, yY)$ for $(u, j) \in \mathcal{I}_{BD,y1}$, and $g_{[u,j]}^{LSBs.Aon}(xX, yY)$ for $(u, j) \in \mathcal{I}_{Aon}$ to construct a non-triangular matrix $\boldsymbol{B}$.

Aono claimed that the matrix $\boldsymbol{B}$ is not triangular. However, we find that by utilizing an unraveled linearization with a linearized variable

$$z := 1 + xy$$

and the matrix becomes triangular. Table 9 shows an example of the triangular matrix.

Lemma 10. *Let shift-polynomials $g_{[u,i]}^{LSBs.x}(x, y)$ and $g_{[u,j]}^{LSBs.BM}(x, y)$, and $g_{[u,j]}^{LSBs.Aon}(x, y)$, sets of indices $\mathcal{I}_{BD,x}$ and $\mathcal{I}_{BD,y1}$, $\mathcal{I}_{Aon}$ and be defined as in (9), (10), (2), and (11), respectively. Let $\boldsymbol{B}$ be a matrix whose rows consist of coefficients of $g_{[u,i]}^{LSBs.x}(xX, yY)$ for $(u, i) \in \mathcal{I}_{BD,x}$, $g_{[u,j]}^{LSBs.BM}(xX, yY)$ for $(u, j) \in \mathcal{I}_{BD,y1}$, and $g_{[u,j]}^{LSBs.Aon}(xX, yY)$ for $(u, j) \in \mathcal{I}_{Aon}$. If the shift-polynomials are ordered as*

- $g_{[u,i]}^{LSBs.x}(xX, yY) \prec g_{[u,j]}^{LSBs.BM}(xX, yY) \prec g_{[u,j]}^{LSBs.Aon}(xX, yY, zZ)$,
- $g_{[u',i']}^{LSBs.x}(xX, yY) \prec g_{[u,i]}^{LSBs.x}(xX, yY)$ *for*
  - $u' < u$,
  - $u' = u, i' < i$,
- $g_{[u',i']}^{LSBs.y1}(xX, yY) \prec g_{[u,j]}^{LSBs.BM}(xX, yY)$ *for*
  - $u' < u$,

  - $u' = u, j' < j$,
- $g^{LSBs.y2}_{[u',i']}(xX, yY, zZ) \prec g^{LSBs.Aon}_{[u,j]}(xX, yY, zZ)$ *for*
  - $u' < u$,
  - $u' = u, j' < j$,

then the matrix $\boldsymbol{B}$ *becomes triangular with diagonals*

- $X^u Y^i (eM)^{m-i}$ *for* $g^{LSBs.x}_{[u,i]}(xX, yY)$,
- $X^u Y^{u+j} (eM)^{m-u}$ *for* $g^{LSBs.BM}_{[u,j]}(xX, yY)$,
- $Y^j Z^u e^{m-u} M^m$ *for* $g^{LSBs.Aon}_{[u,j]}(xX, yY, zZ)$.

We omit a proof of Lemma 10 since it is almost straightforward from Herrmann-May's matrix [HM10].

Aono improved Ernst et al.'s attack for $\beta < (9 - \sqrt{21})/12$. In other words, Aono interpolated the Boneh-Durfee stronger attack and Blömer-May's attack. The set $\mathcal{I}_{BD.x}$ is common among the three attacks. Recall the definition $\mathcal{I}_{BD,y1} := \{u = 0, 1, \ldots, m; j = 1, 2, \ldots, k\}$ in (2). Aono's matrix for $k = 0$ is the same as that of the Boneh-Durfee stronger attack since $\mathcal{I}_{BD.y2} = \emptyset$ and[6] $\mathcal{I}_{Aon} = \mathcal{I}_{BD.y2}$. Aono's matrix for $\tau < \kappa = k/m$ is the same as that of Blömer-May's attack since $\mathcal{I}_{Aon} = \emptyset$.

5.3 Our Attack

In this subsection, we propose our improved partial key exposure attacks with the LSBs of d.

Theorem 2. *Given a public key* (N, e) *of RSA such that* e *is full size and* $d = N^\beta$ *along with* $d_0 > N^{\beta-\delta}$ *which is the LSBs of* d*, if* N *is sufficiently large and polynomials output by the LLL will not vanish, then there is a polynomial time factorization algorithm for* N *when*

$$\delta < \frac{1 + \beta - \sqrt{-1 + 6\beta - 3\beta^2}}{2} \quad \textit{and} \quad \beta \leq \frac{9 - \sqrt{21}}{12}.$$

The attack is an appropriate extension of the Boneh-Durfee stronger attack in the sense that the bound of Theorem 2 is $\beta < 1 - 1/\sqrt{2} = 0.292\cdots$ for $\delta = \beta$. We obtain the improved attack by introducing a new shift-polynomial

$$\begin{aligned} g^{LSBs.y}_{[u,j]}(x, y) &:= g^{LSBs.BM}_{[u - l^{LSBs}_{k,\tau}(j), j]}(x, y) \cdot (f_{BD}(x, y)/e)^{l^{LSBs}_{k,\tau}(j)} \\ &= g^{LSBs.Aon}_{[l^{LSBs}_{k,\tau}(j), j]}(x, y) \cdot (f_{LSBs}(x, y)/(eM))^{u - l^{LSBs}_{k,\tau}(j)} \\ &= y^j f_{LSBs}(x, y)^{u - l^{LSBs}_{k,\tau}(j)} f_{BD}(x, y)^{l^{LSBs}_{k,\tau}(j)} e^{m-u} M^{m - (u - l^{LSBs}_{k,\tau}(j))}, \end{aligned} \tag{12}$$

[6] Here, we use the fact that $k = 0$ in $\mathcal{I}_{BD.y2}$ when we optimize $\kappa = k/m$.

where the function $l_{k,\tau}^{LSBs}(\cdot)$ was defined in Definition 2. The shift-polynomial modulo $(eM)^m$ have the same root as the original solutions, i.e., $g_{[u,j]}^{LSBs.y}(\ell, -p-q+1) = 0 \pmod{(eM)^m}$. The shift-polynomial $g_{[u-l_{k,\tau}^{LSBs}(j),j]}^{LSBs.BM}$ and $g_{[l_{k,\tau}^{LSBs}(j),j]}^{LSBs.Aon}(x,y)$ is a special case of $g_{[u,j]}^{LSBs.y}(x,y)$ for $l_{k,\tau}^{LSBs}(j) = 0$ and $l_{k,\tau}^{LSBs}(j) = u$, respectively. As opposed to Blömer-May's matrix, we can exploit the structure of Boneh-Durfee's stronger matrix by using the polynomial $f_{BD}(x,y)$, where the same trick was already used by Aono. Furthermore, as opposed to Aono, we can reduce powers of M by using the polynomial $f_{LSBs}(x,y)$. The function $l_{k,\tau}^{LSBs}(\cdot)$ is used to construct a triangular matrix with minimum powers of M.

Proof of Theorem 2. As a lattice construction of the Boneh-Durfee stronger attack, we use shift-polynomials $g_{[u,i]}^{LSBs.x}(xX, yY)$ for $(u,i) \in \mathcal{I}_{BD,x}$ and $g_{[u,j]}^{LSBs.y}(xX, yY, zZ)$ for $(u,j) \in \mathcal{I}_{BD,y2}$, where sets of indices $\mathcal{I}_{BD,x}$ and $\mathcal{I}_{BD,y2}$ were defined in Section 3.1, then construct a basis matrix $\boldsymbol{B}$. As in Lemma 5, to construct a triangular matrix, we use a linearized variable

$$z := 1 + xy,$$

where the absolute value of the root is bounded above by $Z := N^{\beta+1/2}$ within a constant factor. To utilize as many given partial information as possible, we construct a triangular matrix as follows.

Lemma 11. *Let shift-polynomials $g_{[u,i]}^{LSBs.x}(x,y)$, $g_{[u,j]}^{LSBs.y}(x,y)$, sets of indices $\mathcal{I}_{BD,x}$ and $\mathcal{I}_{BD,y2}$, a function $l_{k,\tau}^{LSBs}(x)$ be defined as in (9), (12), (3), and Definition 2, respectively. Let $\boldsymbol{B}$ be a matrix whose rows consist of coefficients of $g_{[u,i]}^{LSBs.x}(xX, yY)$ for $(u,i) \in \mathcal{I}_{BD,x}$, $g_{[u,j]}^{LSBs.y}(xX, yY, zZ)$ for $(u,j) \in \mathcal{I}_{BD,y2}$, and If the shift-polynomials are ordered as*

- $g_{[u,i]}^{LSBs.x}(xX, yY) \prec g_{[u,j]}^{LSBs.y}(xX, yY, zZ)$
- $g_{[u',i']}^{LSBs.x}(xX, yY) \prec g_{[u,i]}^{LSBs.x}(xX, yY)$ *for*
  - $u' < u$,
  - $u' = u, i' < i$,
- $g_{[u',i']}^{LSBs.y}(xX, yY, zZ) \prec g_{[u,j]}^{LSBs.y}(xX, yY, zZ)$ *for*
  - $u' < u$,
  - $u' = u, j' < j$,

then the matrix $\boldsymbol{B}$ becomes triangular with diagonals

- $X^u Y^i (eM)^{m-i}$ *for* $g_{[u,i]}^{LSBs.x}(xX, yY)$,
- $X^{u-l_{k,\tau}^{LSBs}(j)} Y^{u+j-l_{k,\tau}^{LSBs}(j)} Z^{l_{k,\tau}^{LSBs}(j)} e^{m-u} M^{m-(u-l_{k,\tau}^{LSBs}(j))}$ *for* $g_{[u,j]}^{LSBs.y}(xX, yY, zZ)$.

Table 10: Our matrix $\boldsymbol{B}$ of a partial key exposure attack with the LSBs for $m = 2$ and $\kappa = 1/2, \tau = 1$.

	1	y	x	xy	xy^2	y^2z	x^2	x^2y	x^2y^2	x^2y^3	xy^3z	y^3z^2
$g^{LSBs.x}_{[0,0]}$	$(eM)^2$											
$g^{LSBs.y}_{[0,1]}$		$Y(eM)^2$										
$g^{LSBs.x}_{[1,0]}$			$X(eM)^2$									
$g^{LSBs.x}_{[0,1]}$	–		–	$XYeM$								
$g^{LSBs.y}_{[1,1]}$		–		–	XY^2eM							
$g^{LSBs.y}_{[1,2]}$					–	Y^2ZeM^2						
$g^{LSBs.x}_{[2,0]}$							$X^2(eM)^2$					
$g^{LSBs.x}_{[1,1]}$			–				–	X^2YeM				
$g^{LSBs.x}_{[0,2]}$	–		–	–			–	–	X^2Y^2			
$g^{LSBs.y}_{[2,1]}$		–		–	–			–	–	X^2Y^3		
$g^{LSBs.y}_{[2,2]}$					–	–			–	–	XY^3ZM	
$g^{LSBs.y}_{[2,3]}$						–				–	–	$Y^3Z^2M^2$

The diagonals of $g^{LSBs.y}_{[u,j]}(x,y)$ are the same as those of $g^{LSBs.BM}_{[u,j]}(x,y)$ of Blömer-May's matrix and $g^{LSBs.Aon}_{[u,j]}(x,y)$ of Aono's matrix for $l^{LSBs}_{k,\tau}(j) = 0$ and $l^{LSBs}_{k,\tau}(j) = u$, respectively. By utilizing as many given partial information as possible, diagonals of $g^{LSBs.y}_{[u,j]}(x,y)$ for $l^{LSBs}_{k,\tau}(j) \neq 0$ and $l^{LSBs}_{k,\tau}(j) < u$ are smaller than $g^{LSBs.Aon}_{[u,j]}(x,y)$ of Aono's matrix.

Table 10 shows an example of the matrix that has the same polynomials as Aono's matrix in Table 9. To illustrate our idea, we use the examples. The matrix in Table 9 has a diagonal $Y^2Z^2M^2$ for $g^{LSBs.Aon}_{[2,2]}$ whereas our matrix has diagonals XY^3ZM for the analogous polynomial $g^{LSBs.y}_{[2,2]}$. Since $Y^2Z^2 = XY^3Z$, the diagonal in Table 10 is smaller by a factor M. We reduce the factor by using the polynomial $f_{LSBs}(x,y)$ which was not used in $g^{LSBs.Aon}_{[2,2]}$.

Proof of Lemma 11. It is straightforward that the shift-polynomials $g^{LSBs.x}_{[u,i]}(x,y)$ and $g^{LSBs.y}_{[u,j]}(x,y)$ for $l^{LSBs}_{k,\tau}(j) = 0$ and $l^{LSBs}_{k,\tau}(j) = u$ derive a triangular basis matrix $\boldsymbol{B}$ with diagonals as stated in Lemma 11. We show that so do $g^{LSBs.y}_{[u,j]}(x,y)$ for $l^{LSBs}_{k,\tau}(j) \neq 0$ and $l^{LSBs}_{k,\tau}(j) < u$. For the purpose, we define sets of indices

$$\mathcal{I}^{(u,j)}_{LSBs} := \{i_y = j, j+1, \ldots, u+j; i_x = l^{LSBs}_{k,\tau}(i_y), l^{LSBs}_{k,\tau}(i_y)+1, \ldots, u\}$$

parametrized by $(u,j) \in \mathcal{I}_{BD.y2}$ and provide an inductive proof that

$$y^j f_{LSBs}(x,y)^{u-l^{LSBs}_{k,\tau}(j)} f_{BD}(x,y)^{l^{LSBs}_{k,\tau}(j)} = \sum_{(i_x,i_y)\in\mathcal{I}^{(u,j)}_{LSBs}} c^{(u,j)}_{i_x,i_y} x^{i_x - l^{LSBs}_{k,\tau}(i_y)} y^{i_y - l^{LSBs}_{k,\tau}(i_y)} z^{l^{LSBs}_{k,\tau}(i_y)}$$

holds, where $c_{i_x,i_y}^{(u,j)}$ for $(i_x,i_y) \in \mathcal{I}_{LSBs}^{(u,j)}$ are integers and $c_{u,u+j}^{(u,j)} = 1$. Recall that

$$g_{[u,j]}^{LSBs.y}(x,y) := y^j f_{LSBs}(x,y)^{u-l_{k,\tau}^{LSBs}(j)} f_{BD}(x,y)^{l_{k,\tau}^{LSBs}(j)}.$$

We assume that the claim holds for $(u'-1,j')$ and $(u',j'-1)$, then show that it holds for (u',j'). Observe that

$$\begin{aligned}
& y^j f_{LSBs}(x,y)^{u-l_{k,\tau}^{LSBs}(j)} f_{BD}(x,y)^{l_{k,\tau}^{LSBs}(j)} \\
&= y^j f_{LSBs}(x,y)^{u-l_{k,\tau}^{LSBs}(j)-1} f_{BD}(x,y)^{l_{k,\tau}^{LSBs}(j)} \cdot (1 - ed_0 + x(N+y)) \\
&= \sum_{(i_x,i_y)\in\mathcal{I}_{LSBs}^{(u-1,j)}} c_{i_x,i_y}^{(u-1,j)} x^{i_x - l_{k,\tau}^{LSBs}(i_y)} y^{i_y - l_{k,\tau}^{LSBs}(i_y)} z^{l_{k,\tau}^{LSBs}(i_y)} \cdot (1 - ed_0 + x(N+y)) \\
&= \sum_{(i_x,i_y)\in\mathcal{I}_{LSBs}^{(u,j)}\setminus(u,u+j)} d_{i_x,i_y}^{(u,j)} x^{i_x - l_{k,\tau}^{LSBs}(i_y)} y^{i_y - l_{k,\tau}^{LSBs}(i_y)} z^{l_{k,\tau}^{LSBs}(i_y)} + x^{u - l_{k,\tau}^{LSBs}(u+j)} y^{u+j-l_{k,\tau}^{LSBs}(u+j)} z^{l_{k,\tau}^{LSBs}(u+j)}
\end{aligned}$$

holds, where $d_{i_x,i_y}^{(u,j)} \in \mathcal{I}_{LSBs}^{(u,j)} \setminus (u,u+j)$ are integers. Since $\mathcal{I}_{LSBs}^{(u,j)} \setminus (u,u+j) \subset \mathcal{I}_{LSBs}^{(u-1,j)} \cup \mathcal{I}_{LSBs}^{(u,j-1)}$ holds, we proved the above claim. Hence, we conclude the proof. □

To make use of the given LSBs d_0, we set

$$\kappa = 2(\beta - \delta) \qquad \text{and} \qquad \tau = 1 + 2\delta - 4\beta$$

and use the set of indices $\mathcal{I}_{BD.y2}$ by following the lemma.

Lemma 12. *In the matrix $\boldsymbol{B}$ of Lemma 11, polynomials $g_{[u,j]}^{LSBs.y}(x,y)$ are helpful if and only if $j \le 2(\beta-\delta)m + (1+2\delta-4\beta)u$ for all u.*

Proof of Lemma 12. Let $g_{[u',j']}^{LSBs.y}(x,y)$ be a polynomial with fixed indices (u',j') such that

$$u' = l_{k,\tau}^{MSBs}(j'),$$

and $\boldsymbol{B'}$ be a matrix that is a matrix $\boldsymbol{B}$ without the polynomial $g_{[u',j']}^{LSBs.y}(x,y)$. As stated in Lemma 11, diagonals of the polynomial $g_{[u',j']}^{MSBs.y}(x,y)$ in $\boldsymbol{B}$ is

$$Y^{j'} Z^{u'} e^{m-u'} M^m.$$

Furthermore, diagonals of polynomials

$$g_{[u'+1,j']}^{LSBs.y}(x,y), g_{[u'+2,j']}^{LSBs.y}(x,y), \ldots, g_{[m,j']}^{LSBs.y}(x,y)$$

in $\boldsymbol{B}$ are

$$XY^{j'+1}Z^{u'}e^{m-u'-1}M^{m-1}, X^2Y^{j'+2}Z^{u'}e^{m-u'-2}M^{m-2}, \ldots, X^{m-u'}Y^{j'+m-u'}Z^{u'}M^{u'}.$$

On the other hand, by following the proof of Lemma 11, diagonals of the same polynomials in $\boldsymbol{B}'$ are

$$Y^{j'}Z^{u'+1}e^{m-u'-1}M^m, XY^{j'+1}Z^{u'+1}e^{m-u'-2}M^{m-1}, \ldots, X^{m-u'-1}Y^{j'+m-u'-1}Z^{u'+1}M^{u'+1}.$$

Hence,

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

that is smaller than or equal to the modulus $(eM)^m$ if and only if

$$\begin{aligned} Y^{j'}Z^{u'}e^{m-u'}M^m \cdot \left(\frac{XY}{ZM}\right)^{m-u'} \leq (eM)^m &\Leftrightarrow Y^{j'}Z^{u'} \leq e^{u'}M^{m-u'} \\ &\Leftrightarrow \frac{1}{2}j' + \left(\beta + \frac{1}{2}\right)u' \leq u' + (\beta-\delta)(m-u') \\ &\Leftrightarrow j' \leq 2(\beta-\delta)m + (1+2\delta-4\beta)u'. \end{aligned}$$

Hence, we conclude the proof. □

To obtain the bound of Theorem 2, we compute a dimension

$$n = \sum_{(u,i)\in\mathcal{I}_{BD,x}} 1 + \sum_{(u,j)\in\mathcal{I}_{BD,y2}} 1 = \left(\frac{1}{2} + 2(\beta-\delta) + \frac{1+2\delta-4\beta}{2}\right)m^2 + o(m^2),$$

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

$$\begin{aligned} s_X &= \sum_{(u,i)\in\mathcal{I}_{BD,x}} u + \sum_{(u,j)\in\mathcal{I}_{BD,y2}} \left(u - l_{k,\tau}^{LSBs}(j)\right) = \left(\frac{1}{3} + (\beta-\delta) + \frac{1+2\delta-4\beta}{6}\right)m^3 + o(m^3), \\ s_Y &= \sum_{(u,i)\in\mathcal{I}_{BD,x}} i + \sum_{(u,j)\in\mathcal{I}_{BD,y2}} \left(u + j - l_{k,\tau}^{LSBs}(j)\right) \\ &= \left(\frac{1}{6} + (\beta-\delta) + 2(\beta-\delta)^2 + (\beta-\delta)(1+2\delta-4\beta) + \frac{1+2\delta-4\beta}{6} + \frac{(1+2\delta-4\beta)^2}{6}\right)m^3 + o(m^3), \\ s_Z &= \sum_{(u,j)\in\mathcal{I}_{BD,y2}} l_{k,\tau}^{LSBs}(j) = \frac{1+2\delta-4\beta}{6}m^3 + o(m^3), \\ s_e &= \sum_{(u,i)\in\mathcal{I}_{BD,x}} (m-i) + \sum_{(u,j)\in\mathcal{I}_{BD,y2}} (m-u) = \left(\frac{1}{3} + (\beta-\delta) + \frac{1+2\delta-4\beta}{6}\right)m^3 + o(m^3), \\ s_M &= \sum_{(u,i)\in\mathcal{I}_{BD,x}} (m-i) + \sum_{(u,i)\in\mathcal{I}_{BD,y2}} \left(m - \left(u - l_{k,\tau}^{LSBs}(j)\right)\right) = \left(\frac{1}{3} + (\beta-\delta) + \frac{1+2\delta-4\beta}{3}\right)m^3 + o(m^3). \end{aligned}$$

New polynomials which are derived from outputs of the LLL algorithm satisfy Howgrave-Graham's lemma when $(\det(\boldsymbol{B}))^{1/n} < (eM)^m$. By omitting small terms, we obtain an inequality

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

By solving the inequality, we obtain the bound of Theorem 2

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

Hence, we conclude the proof. □

6 Concluding Remarks

In this paper, we proposed improved partial key exposure attacks on RSA with the MSBs and the LSBs of d. In particular, our attack with the MSBs and the LSBs is better than all known attacks when d is small such that $d < N^{9/16}$ and $d < N^{(9-\sqrt{21})/12}$, respectively. Furthermore, our attack with the MSBs is the first result that is an extension of the Boneh-Durfee stronger attack and always works for $d < N^{1-1/\sqrt{2}}$. We obtained these improved attacks by utilizing the unraveled linearization technique and fully exploit the structure of the lattice for the Boneh-Durfee stronger attack.

References

[AASW18] Yoshinori Aono, Manindra Agrawal, Takakazu Satoh, and Osamu Watanabe. On the optimality of lattices for the coppersmith technique. *Appl. Algebra Eng. Commun. Comput.*, 29(2):169–195, 2018.

[Aon09] Yoshinori Aono. A new lattice construction for partial key exposure attack for RSA. In Stanislaw Jarecki and Gene Tsudik, editors, *Public Key Cryptography - PKC 2009, 12th International Conference on Practice and Theory in Public Key Cryptography*, volume 5443 of *Lecture Notes in Computer Science*, pages 34–53. Springer, 2009.

[Aon13] Yoshinori Aono. Minkowski sum based lattice construction for multivariate simultaneous Coppersmith's technique and applications to RSA. 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 88–103. Springer, 2013.

[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.

[BVZ12] Aurélie Bauer, Damien Vergnaud, and Jean-Christophe Zapalowicz. Inferring sequences produced by nonlinear pseudorandom number generators using Coppersmith's methods. In Marc Fischlin, Johannes A. Buchmann, and Mark Manulis, editors, *Public Key Cryptography - PKC 2012 - 15th International Conference on Practice and Theory in Public Key Cryptography*, volume 7293 of *Lecture Notes in Computer Science*, pages 609–626. Springer, 2012.

[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.

[DN00] Glenn Durfee and Phong Q. Nguyen. Cryptanalysis of the RSA schemes with short secret exponent from asiacrypt '99. In Tatsuaki Okamoto, editor, *Advances in Cryptology - ASIACRYPT 2000, 6th International Conference on the Theory and Application of Cryptology and Information Security*, volume 1976 of *Lecture Notes in Computer Science*, pages 14–29. Springer, 2000.

[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.

[Her11] Mathias Herrmann. *Lattice-based Cryptanalysis Using Unravelled Linearization.* PhD thesis, der Ruhr-University Bochum, 2011.

[HHX14] Zhangjie Huang, Lei Hu, and Jun Xu. Attacking RSA with a composed decryption exponent using unravelled linearization. In Dongdai Lin, Moti Yung, and Jianying Zhou, editors, *Information Security and Cryptology - 10th International Conference, Inscrypt 2014*, volume 8957 of *Lecture Notes in Computer Science*, pages 207–219. Springer, 2014.

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

[HM09] Mathias Herrmann and Alexander May. Attacking power generators using unravelled linearization: When do we output too much? In Mitsuru Matsui, editor, *Advances in Cryptology - ASIACRYPT 2009, 15th International Conference on the Theory and Application of Cryptology and Information Security*, volume 5912 of *Lecture Notes in Computer Science*, pages 487–504. Springer, 2009.

[HM10] Mathias Herrmann and Alexander May. Maximizing small root bounds by linearization and applications to small secret exponent RSA. In Phong Q. Nguyen and David Pointcheval, editors, *Public Key Cryptography - PKC 2010, 13th International Conference on Practice and Theory in Public Key Cryptography*, volume 6056 of *Lecture Notes in Computer Science*, pages 53–69. Springer, 2010.

[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.

[IKK08] Kouichi Itoh, Noboru Kunihiro, and Kaoru Kurosawa. Small secret key attack on a variant of RSA (due to takagi). In Tal Malkin, editor, *Topics in Cryptology - CT-RSA 2008, The Cryptographers' Track at the RSA Conference 2008*, volume 4964 of *Lecture Notes in Computer Science*, pages 387–406. Springer, 2008.

[IKK09] Kouichi Itoh, Noboru Kunihiro, and Kaoru Kurosawa. Small secret key attack on a takagi's variant of RSA. *IEICE Transactions*, 92-A(1):33–41, 2009.

[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.

[KSI14] Noboru Kunihiro, Naoyuki Shinohara, and Tetsuya Izu. A unified framework for small secret exponent attack on RSA. *IEICE Transactions*, 97-A(6):1285–1295, 2014.

[Kun11] Noboru Kunihiro. Solving generalized small inverse problems. *IEICE Transactions*, 94-A(6):1274–1284, 2011.

[Kun12] Noboru Kunihiro. On optimal bounds of small inverse problems and approximate GCD problems with higher degree. In Dieter Gollmann and Felix C. Freiling, editors, *Information Security - 15th International Conference, ISC 2012*, volume 7483 of *Lecture Notes in Computer Science*, pages 55–69. Springer, 2012.

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

[LZL14] Yao Lu, Rui Zhang, and Dongdai Lin. New partial key exposure attacks on CRT-RSA with large public exponents. In Ioana Boureanu, Philippe Owesarski, and Serge Vaudenay, editors, *Applied Cryptography and Network Security - 12th International Conference, ACNS 2014*, volume 8479 of *Lecture Notes in Computer Science*, pages 151–162. Springer, 2014.

[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.

[Sar14] Santanu Sarkar. Small secret exponent attack on RSA variant with modulus $N = p^r q$. *Des. Codes Cryptography*, 73(2):383–392, 2014.

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

[SM09] Santanu Sarkar and Subhamoy Maitra. Partial key exposure attack on CRT-RSA. In Michel Abdalla, David Pointcheval, Pierre-Alain Fouque, and Damien Vergnaud, editors, *Applied Cryptography and Network Security, 7th International Conference, ACNS 2009*, volume 5536 of *Lecture Notes in Computer Science*, pages 473–484, 2009.

[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.

[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. 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.

[TK16d] Atsushi Takayasu and Noboru Kunihiro. Small secret exponent attacks on RSA with unbalanced prime factors. In *2016 International Symposium on Information Theory and Its Applications, ISITA 2016*, pages 236–240. IEEE, 2016.

[TK17a] Atsushi Takayasu and Noboru Kunihiro. General bounds for small inverse problems and its applications to multi-prime RSA. *IEICE Transactions*, 100-A(1):50–61, 2017.

[TK17b] Atsushi Takayasu and Noboru Kunihiro. A tool kit for partial key exposure attacks on RSA. In Helena Handschuh, editor, *Topics in Cryptology - CT-RSA 2017 - The Cryptographers' Track at the RSA Conference 2017*, volume 10159 of *Lecture Notes in Computer Science*, pages 58–73. Springer, 2017.

[TLP17] Atsushi Takayasu, Yao Lu, and Liqiang Peng. Small crt-exponent RSA revisited. In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *Advances in Cryptology - EUROCRYPT 2017 - 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, volume 10211 of *Lecture Notes in Computer Science*, pages 130–159, 2017.

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