How to Generalize RSA Cryptanalyses

†‡Atsushi Takayasu and †Noboru Kunihiro

†The University of Tokyo, Chiba, Japan
‡AIST, Tokyo, Japan
{a-takayasu@it., kunihiro@}k.u-tokyo.ac.jp

Abstract. Recently, the security of RSA variants with moduli $N = p^r q$, e.g., the Takagi RSA and the prime power RSA, have been actively studied in several papers. Due to the unusual composite moduli and rather complex key generations, the analyses are more involved than the standard RSA. Furthermore, the method used in some of these works are specialized to the form of composite integers $N = p^r q$.
In this paper, we generalize the techniques used in the current best attacks on the standard RSA to the RSA variants. We show that the lattices used to attack the standard RSA can be transformed into lattices to attack the variants where the dimensions are larger by a factor of $(r + 1)$ of the original lattices. We believe the steps we took present to be more natural than previous researches, and to illustrate this point we obtained the following results:

- Simpler proof for small secret exponent attacks on the Takagi RSA proposed by Itoh et al. (CT-RSA 2008). Our proof generalizes the work of Herrmann and May (PKC 2010).
- Partial key exposure attacks on the Takagi RSA; generalizations of the works of Ernst et al. (Eurocrypt 2005) and Takayasu and Kunihiro (SAC 2014). Our attacks improve the result of Huang et al. (ACNS 2014).
- Small secret exponent attacks on the prime power RSA; generalizations of the work of Boneh and Durfee (Eurocrypt 1999). Our attacks improve the results of Sarkar (DCC 2014, ePrint 2015) and Lu et al. (Asiacrypt 2015).
- Partial key exposure attacks on the prime power RSA; generalizations of the works of Ernst et al. and Takayasu and Kunihiro. Our attacks improve the results of Sarkar and Lu et al.

The construction techniques and the strategies we used are conceptually easier to understand than previous works, owing to the fact that we exploit the exact connections with those of the standard RSA.

Keywords: RSA, Takagi RSA, prime power RSA, cryptanalysis, small secret exponent, partial key exposure, lattices, Coppersmith's method

1 Introduction

Background. RSA [RSA78] is one of the most well-known cryptosystems. Let N be the public RSA modulus, a product of two distinct primes p and q with

the same bit sizes. The public and secret exponents are positive integers such that $ed = 1 \mod (p-1)(q-1)$. The RSA cryptosystem has been extensively studied in numerous papers including lattice based cryptanalysis. In this paper, we introduce two well-analyzed attacks; *small secret exponent attacks* and *partial key exposure attacks*. Boneh and Durfee [BD00] showed that a public RSA modulus N can be factorized when a secret exponent d is small, e.g., they proposed a weaker result $d < N^{0.284}$ and a stronger result $d < N^{0.292}$. Several papers [BM03,EJMW05,SGM10,TK14] have studied the security of RSA when some portions of the most significant bits (MSBs) or the least significant bits (LSBs) of d are exposed to attackers. The attack of Ernst et al. [EJMW05] are the best results for general cases, e.g., the MSBs or the LSBs are exposed for general sizes of e and d. Although Blömer and May [BM03] and Sarkar et al. [SGM10] achieved the same result, they are only special cases of Ernst et al., e.g., Blömer and May's attack works only with the LSBs and the attack of Sarkar et al. works only with the MSBs and large e. Takayasu and Kunihiro [TK14] proposed an improved attack of Ernst et al. for specific parameters, e.g., small d.

There are some variants of RSA. In this paper, we study two of them that we call the *Takagi RSA* [Tak98] and the *prime power RSA*. Both have a public RSA modulus $N = p^r q$ for $r \geq 2$ with distinct primes p and q with the same bit sizes. A public and a secret exponent $e \approx N^\alpha$ and $d \approx N^\beta$ satisfy

$$ed = 1 \mod (p-1)(q-1)$$

for the Takagi RSA and

$$ed = 1 \mod p^{r-1}(p-1)(q-1)$$

for the prime power RSA, respectively. The security of the variants have been analyzed; May [May04] proposed small secret exponent attacks and partial key exposure attacks on the prime power RSA, and Itoh et al. [IKK08] proposed small secret exponent attacks on the Takagi RSA. Recently, the research area becomes a hot topic and several papers have been published. Huang et al. [HHX+14] proposed partial key exposure attacks on the Takagi RSA. Sarkar [Sar14] proposed small secret exponent attacks on the prime power RSA, and further improved the result in [Sar15] with a result for partial key exposure attacks. The result is better than May for small r. Lu et al. [LZPL15] proposed small secret exponent attacks and partial key exposure attacks on the prime power RSA that fully improve May's attack and are better than Sarkar's attack for $r \geq 5$.

Attacks of May [May04], and Lu et al. [LZPL15] make use of the special structure of a public modulus $N = p^r q$ and a key generation equality of the prime power RSA. Then, their attacks do not work for the standard RSA. However, a naive approach for the analysis of RSA variants should be generalizations of the attacks on the standard RSA. By definition, the Takagi RSA and the prime power RSA become the same as the standard RSA for $r = 1$. Hence, the attacks on the variants for $r = 1$ should completely cover the currently known best attacks on the standard RSA; the stronger Boneh-Durfee small secret exponent attack, partial key exposure attacks of Ernst et al., and Takayasu and Kunihiro.

Since a public modulus N and key generations for the variants are more involved than the standard RSA, the analyses also become involved. Indeed, almost all the algorithm constructions and their strategies are too complicated to understand since the connections with those for the standard RSA are unclear. Moreover, existing attacks on the variants for $r = 1$ do not fully cover the currently known best attacks on the standard RSA.

Our Results. In this paper, we study the security of the Takagi RSA and the prime power RSA. The main focus of this paper is to generalize the currently known best attacks on the standard RSA, e.g., small secret exponent attacks and partial key exposure attacks, to the variants and to exploit the connections between their algorithm constructions. We show that the lattices used to attack the standard RSA can be transformed into lattices to attack the variants with simple operations. More concretely, the lattices used to attack the standard RSA can be transformed into lattices to attack the Takagi RSA (resp. the prime power RSA) by multiplying $\{1, q, pq, p^2q, \ldots, p^{r-1}q\}$ (resp. $\{q^a, pq^a, p^2q^a, \ldots, p^{r-1}q^a, p^{r-1}q^{a+1}\}$ with some integer a) to all the polynomials in the bases. Hence, dimensions of the lattices that we use to attack the variants are larger by a factor of $(r + 1)$ of the original lattices to attack the standard RSA. We believe that the connections offer better understanding for our algorithm constructions and enable us to easily generalize other attacks for their variants. As applications of our generalizations, we obtain the following results:

- In Section 3, we propose a partial key exposure attack on the Takagi RSA that fully generalizes the attack of Ernst et al. [EJMW05]. Our attack becomes the same as Huang et al. [HHX+14] with the exposed LSBs and better than the attack with the exposed MSBs for all α, β, and r.
- In Section 4, we give a simpler proof for the Itoh et al. small secret exponent attack on the Takagi RSA that fully generalizes the stronger Boneh-Durfee attack [BD00]. Our alternative proof fully generalizes that of Herrmann and May [HM10] for the stronger Boneh-Durfee attack and enables us to understand the Itoh et al. attack in detail. Based on the understanding, we propose a partial key exposure attack on the Takagi RSA with the exposed LSBs that fully generalizes Takayasu and Kunihiro's attack [TK14]. The attack is better than our attack in Section 3 and that of Huang et al. [HHX+14] for all α and r when β is small.
- In Section 5, we propose a small secret exponent attack on the prime power RSA that fully generalizes the weaker Boneh-Durfee attack [BD00]. To obtain the attack is technically easy since it is an extension of Sarkar's attack [Sar15] for arbitrary α. However, the extension reveals an important fact. Although Sarkar's attack, which captures only for $\alpha = 1$, is weaker than Lu et al. [LZPL15] for $r \geq 5$, our attack is better than Lu et al. for all r when α is small. In addition, we propose a partial key exposure attack that fully generalizes the Ernst et al. [EJMW05]. Our attack is better than Sarkar's result for small α and β, and is better than Lu et al. [LZPL15] for small r.

– In Section 6, we propose a small secret exponent attack on the prime power RSA that (almost) fully generalizes the stronger Boneh-Durfee [BD00]. The attack is better than our attack in Section 5. In addition, we propose a partial key exposure attack that (almost) fully generalizes Takayasu and Kunihiro [TK14]. The attack is better than all known attacks for small r and β.

Since the elliptic curve method factorization [Len87] becomes efficient for large r and Boneh et al. [BDH99] revealed that only a $1/(r+1)$ fraction of the most significant bits of p suffices to factorize the modulus, they are the more important for small r. Then, we mainly compare our results and previous works for $r = 2$ and 3 throughout the paper, although we analyze the security for arbitrary r.

Technical Overview. In 1996, Coppersmith introduced lattice based methods to solve univariate modular equations [Cop96a] and bivariate integer equations [Cop96b], and they can be extended to more variables with a reasonable assumption (that we discuss later). The method is useful to evaluate the security of RSA. See [Cop97,Cop01,NS01,May03,May10]. Indeed, small secret exponent attack was firstly mentioned by Wiener [Wie90]. The attack is based on a continued fraction approach and works when $d < N^{0.25}$. Later, Boneh and Durfee revisited the attack and improved the bound to $d < N^{0.292}$ using the Coppersmith method. Although the original Coppersmith method is conceptually involved, simpler reformulations have been proposed; for modular equations by Howgrave-Graham [How97] and for integer equations by Coron [Cor04,Cor07]. In short, the methods construct a lattice whose bases consist of coefficients of polynomials that have the same roots as the original equations. By finding short lattice vectors using the LLL reduction, the original equations can be solved. The methods can solve modular (resp. integer) equations when sizes of roots are to some extent smaller than the modulus (resp. the norm of polynomial).

To maximize solvable root bounds, appropriate selections of lattice bases are essential. Jochemsz and May [JM06] proposed a conceptually simple strategy for the lattice constructions. Although the strategy does not always offer the best results, usually offers the best or similar bounds. For example, the Boneh-Durfee weaker result $d < N^{0.284}$ can be obtained based on the strategy. Especially, the strategy is the more compatible with integer equations based analysis. To the best of our knowledge, there are no algorithms solving integer equations outperforming the Jochemsz-May strategy; currently known best algorithms solving any integer equations can be captured by the Jochemsz-May strategy. Furthermore, most algorithms by solving modular equations based on the Jochemsz-May strategy can also be obtained by solving integer equations based on the strategy although reverse does not always hold. For example, in the context of partial key exposure attacks on the standard RSA, Ernst et al. [EJMW05] solved integer equations, whereas Blömer and May [BM03], and Sarkar et al. [SGM10] solved modular equations, and all these results are captured by the Jochemsz-May strategy. As we noted, attacks of Blömer and May, and Sarkar et al. are only the special cases of Ernst et al. However, in the context of security analyses of the Takagi RSA and the prime power RSA, there are no results known that

solved integer equations. Therefore, we solve integer equations for the Takagi RSA (Section 3) and the prime power RSA (Section 5), and fully generalize the weaker Boneh-Durfee and Ernst et al.

Although the differences are small, there are some results beyond the Jochemsz-May strategy that solve modular equations, e.g., the stronger Boneh-Durfee attack $d < N^{0.292}$ [BD00]. In general, analyses to obtain attacks outperforming the Jochemsz-May strategy are difficult. Indeed, there are no results known that attack the Takagi RSA or the prime power RSA outperforming the Jochemsz-May strategy except the Itoh et al. small secret exponent attack on the Takagi RSA [IKK08]. In the context of the stronger Boneh-Durfee attack, the proof is involved since determinants of lattices, whose basis matrices are non-triangular, should be calculated. For the purpose, Boneh and Durfee introduced geometrically progressive matrix although the notion is unfamiliar. Since Itoh et al. followed the proof, the analysis is also involved. The fact makes it difficult to obtain partial key exposure attacks on the Takagi RSA outperforming the Jochemsz-May strategy. As the hope of such situations, Herrmann and May [HM10] gave a simpler proof for the stronger Boneh-Durfee attack. They used unravelled linearization [HM09] and transformed Boneh and Durfee's non-triangular basis matrices to be triangular. The simpler proof offers better understanding of the attack. Based on the understanding, Takayasu and Kunihiro extended the stronger Boneh-Durfee attack to partial key exposure attacks outperforming the Jochemsz-May strategy. As the same way, we give a simpler proof of the Itoh et al. and propose a partial key exposure attack on the Takagi RSA outperforming the Jochemsz-May strategy (Section 4). Moreover, we analyze better lattice constructions and propose small secret exponent attacks and partial key exposure attacks on the prime power RSA outperforming the Jochemsz-May strategy (Section 6).

2 Preliminaries

In the beginning of this section, we formulate the exposed bits that will be used to analyze partial key exposure attacks. In the remaining of this section, we introduce tools to solve modular equations and integer equations; lattices and the LLL algorithm, the overview of the Coppersmith method, and the Jochemsz-May strategy. The experts of the research area can skip this part.

Exposed Bits. In this paper, we analyze partial key exposure attacks when some portions of the MSBs or the LSBs are exposed. In this section, we formulated the exposed bits. When the MSBs (resp. LSBs) are exposed, let $d_0 > N^{\beta-\delta}$ denote the exposed MSBs (resp. LSBs) and $d_1 < N^{\delta}$ denote the unknown LSBs (resp. MSBs). The secret exponent can be written as $d = d_0M + d_1$ (resp. $d = d_1M + d_0$) with an integer $M = 2^{\lfloor \delta \log N \rfloor}$ (resp. $M = 2^{\lfloor (\beta-\delta) \log N \rfloor}$). We also use $\tilde{d}$ to denote d_0M (resp. d_0).

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

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

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

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

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

Although the outputs of the LLL algorithm are not the shortest lattice vectors in general, the fact is not the matter when we use the Coppersmith method.

The Coppersmith Methods. Instead of the original Coppersmith method, we introduce Howgrave-Graham's reformulation to solve modular equations [How97] and Coron's reformulation to solve integer equations [Cor04]. Although Coron's method [Cor04] is less efficient than the original Coppersmith method [Cop96b] and Coron's method [Cor07], it is simpler to analyze than the other methods.

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

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

positive integers. If the polynomial $h(x_1, \ldots, x_k)$ satisfies the following two conditions:
1. $h(\tilde{x}_1, \ldots, \tilde{x}_k) = 0 \pmod{R}$*, where* $|\tilde{x}_1| < X_1, \ldots, |\tilde{x}_k| < X_k$*,*
2. $\|h(x_1X_1, \ldots, x_kX_k)\| < R/\sqrt{n}$*.*
Then, $h(\tilde{x}_1, \ldots, \tilde{x}_k) = 0$ *holds over the integers.*

Therefore, if $h'(x_1, x_2)$ and $h'_2(x_1, x_2)$ satisfy Lemma 1, we can compute Gröbner bases or a resultant of them and easily recover $(\tilde{x}_1, \tilde{x}_2)$.

Next, we show an integer case. The Coppersmith method can find solutions $(\tilde{x}_1, \tilde{x}_2, \tilde{x}_3)$ of a trivariate equation $h(x_1, x_2, x_3) = 0$ over the integers when $|\tilde{x}_1| < X_1, |\tilde{x}_2| < X_2, |\tilde{x}_3| < X_3$, and $X_1X_2X_3$ is reasonably smaller than $\|h(x_1X_1, x_2X_2, x_3X_3)\|_\infty$. Although we omit details of the method, we set a reasonable integer R and remaining procedures are almost the same as modular case by solving a modular equation $h(x_1, x_2, x_3) = 0 \mod R$. New polynomials $h'(x_1, x_2, x_3)$ and $h'_2(x_1, x_2, x_3)$ obtained by outputs of the LLL algorithm are provably algebraically independent of $h(x_1, x_2, x_3)$. See [Cor04] for the detail.

We should note that the methods need heuristic argument. There are no assurance if new polynomials obtained by outputs of the LLL algorithm are algebraically independent. In this paper, we assume that these polynomials are always algebraically independent and resultants of polynomials will not vanish since there have been few negative reports that contradict the assumption. Moreover, most our attacks use sublattices of lattices that are used in previous works. Hence, validities of previous attacks justify validities of our results.

The Jochemsz-May Strategy. We summarize lattice constructions to solve integer equations based on the Jochemsz-May strategy [JM06]. Let l_j denote the largest exponent of x_j in the polynomial $h(x_1, \ldots, x_k) = \sum h_{i_1,\ldots,i_k} x_1^{i_1} \cdots x_k^{i_k}$. We set an (possibly large) integer W such that $W \leq \|h(x_1, \ldots, x_k)\|_\infty$. Next, we set an integer $R := WX_1^{l_1(m-1)+t} \prod_{u=2}^{k} X_j^{l_u(m-1)}$ with some positive integers m and $t = O(m)$ such that $\gcd(R, h_{0,\ldots,0}) = 1$. We compute $c = h_{0,\ldots,0}^{-1} \mod R$ and $h'(x_1, \ldots, x_k) := c \cdot h(x_1, \ldots, x_k) \mod R$. We define shift-polynomials g and g' as

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

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

for sets of monomials

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

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

All these shift-polynomials g and g' modulo R have the roots $(\tilde{x}_1, \ldots, \tilde{x}_k)$ that are the same as $h(x_1, \ldots, x_k)$. We construct a lattice with coefficients of

$g(x_1X_1, \ldots, x_kX_k)$ and $g'(x_1X_1, \ldots, x_kX_k)$ as the bases. The shift-polynomials generate a triangular basis matrix. Ignoring low order terms of m, LLL outputs short vectors that satisfy Lemma 1 when

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

When the condition holds, we can find all small roots. See [JM06] for the detail.

3 Attacks on the Takagi RSA by Solving Integer Equations

In this section, we analyze the security of the Takagi RSA by solving integer equations. In Section 3.1, we give an alternative proof of the Itoh et al. small secret exponent attack [IKK08] that was proposed by solving modular equations. In Section 3.2, we propose a partial key exposure attack that fully generalizes the attack of Ernst et al. [EJMW05].

3.1 Small Secret Exponent Attack

In this section, we revisit the Itoh et al. small secret exponent attacks [IKK08]. The result fully generalizes the weaker Boneh-Durfee [BD00] in the sense that it completely covers their attack, i.e., $\beta < (7 - 2\sqrt{7})/6$ for $r = 1$ and $\alpha = 1$.

Theorem 1 ([IKK08]) *Let $N = p^r q$ be a public modulus and let $e \approx N^\alpha$ and $d \approx N^\beta$ be public exponent and secret exponent of the Takagi RSA, respectively. If*

$$\beta < \frac{7 - 2\sqrt{1 + 3(r+1)\alpha}}{3(r+1)} \text{ for } \alpha \leq \frac{1}{r+1}$$

holds, then the Takagi RSA modulus N can be factorized in polynomial time.

Although the original paper [IKK08] solved modular equations for the attack, we solve integer equations and give an alternative proof. The proof is convenient to analyze partial key exposure attacks in Section 3.2. Moreover, we exploit the exact connection between the algorithm constructions of Itoh et al. and the weaker Boneh-Durfee.

Alternative Proof of Theorem 1. Looking at a key generation for the Takagi RSA; $ed = 1 + \ell(p-1)(q-1)$ with some integer $|\ell| \approx N^{\alpha+\beta-2/(r+1)}$. To recover the secret exponent d, we use the following polynomial

$$f_{T.SSE.i}(x, y, z_1, z_2) = 1 + ex + y(z_1 + 1)(z_2 + 1)$$

whose roots over the integers are $(x, y, z_1, z_2) = (-d, \ell, -p, -q)$. The absolute values are bounded by $X := N^\beta, Y := N^{\alpha+\beta-2/(r+1)}, Z_1 := 2N^{1/(r+1)}, Z_2 :=$

$2N^{1/(r+1)}$. We also use a notation $Z = Z_1 = Z_2$ for simplicity. We set an (possibly large) integer W such that $W < N^{\alpha+\beta}$ since $\|f_{T.SSE.i}(xX, yY, z_1Z_1, z_2Z_2)\|_\infty \geq |eX| \approx N^{\alpha+\beta}$. Next, we set an integer $R := W(XY)^{m-1}Z^{m+r-1+t}$ with some integers $m = \omega(r)$ and $t = \tau m$ where $\tau \geq 0$. We define shift-polynomials $g_{T.SSE.i}$ and $g'_{T.SSE.i}$ as

$$\begin{aligned} g_{T.SSE.i} &: x^{i_X} y^{i_Y} z_1^{i_{Z_1}} z_2^{i_{Z_2}} \cdot f_{T.SSE.i} \cdot X^{m-1-i_X} Y^{m-1-i_Y} Z^{m+r-1+t-i_{Z_1}-i_{Z_2}} \\ &\qquad \text{for } x^{i_X} y^{i_Y} z_1^{i_{Z_1}} z_2^{i_{Z_2}} \in S_1 \cup S_2, \\ g'_{T.SSE.i} &: x^{i_X} y^{i_Y} z_1^{i_{Z_1}} z_2^{i_{Z_2}} \cdot R \quad \text{for } x^{i_X} y^{i_Y} z_1^{i_{Z_1}} z_2^{i_{Z_2}} \in (M_1 \cup M_2) \backslash (S_1 \cup S_2), \end{aligned}$$

for sets of monomials

$$\begin{aligned} S_1 &:= \bigcup_{0 \leq j \leq t} \left\{ x^{i_X} y^{i_Y} z_1^{i_{Z_1}+j} \middle| \begin{array}{c} x^{i_X} y^{i_Y} z_1^{i_{Z_1}} \text{ is a monomial of} \\ f_{T.SSE.i}(x, y, z_1, z_2)^{m-1} \end{array} \right\}, \\ S_2 &:= \bigcup_{0 \leq j \leq t} \left\{ x^{i_X} y^{i_Y} z_1^{i_{Z_1}} z_2^{i_{Z_2}+j} \middle| \begin{array}{c} x^{i_X} y^{i_Y} z_1^{i_{Z_1}} z_2^{i_{Z_2}} \text{ is a monomial of} \\ \tilde{s} \cdot f_{T.SSE.i}(x, y, z_1, z_2)^{m-1} \text{ for } i_{Z_2} \geq 1 \\ \text{where } \tilde{s} = \{z_1^{r-1} z_2, z_1^{r-2} z_2, \ldots, z_1 z_2\} \end{array} \right\}, \\ M_1 &:= \left\{ x^{i_X} y^{i_Y} z_1^{i_{Z_1}} \middle| \begin{array}{c} \text{monomials of } x^{i'_X} y^{i'_Y} z_1^{i'_{Z_1}} \cdot f_{T.SSE.i}(x, y, z_1, z_2) \\ \text{for } x^{i'_X} y^{i'_Y} z_1^{i'_{Z_1}} \in S_1 \end{array} \right\}, \\ M_2 &:= \left\{ x^{i_X} y^{i_Y} z_1^{i_{Z_1}} z_2^{i_{Z_2}} \middle| \begin{array}{c} \text{monomials of } x^{i'_X} y^{i'_Y} z_1^{i'_{Z_1}} z_2^{i'_{Z_2}} \cdot f_{T.SSE.i}(x, y, z_1, z_2) \\ \text{for } i_{Z_2} \geq 1 \text{ where } x^{i'_X} y^{i'_Y} z_1^{i'_{Z_1}} z_2^{i'_{Z_2}} \in S_2 \end{array} \right\}. \end{aligned}$$

By definition of sets of monomial S_1, S_2, M_1, and M_2, it follows that

$$\begin{aligned} x^{i_X} y^{i_y} z_1^{i_{Z_1}} \in S_1 \Leftrightarrow\ & i_X = 0, 1, \ldots, m-1; i_Y = 0, 1, \ldots, m-1-i_X; \\ & i_{Z_1} = 0, 1, \ldots, i_Y + t, \\ x^{i_X} y^{i_y} z_1^{i_{Z_1}} z_2^{i_{Z_2}} \in S_2 \Leftrightarrow\ & i_X = 0, 1, \ldots, m-1; i_Y = 0, 1, \ldots, m-1-i_X; \\ & i_{Z_1} = 0, 1, \ldots, r-1; i_{Z_2} = 1, 2, \ldots, i_Y + t + 1, \\ x^{i_X} y^{i_y} z_1^{i_{Z_1}} \in M_1 \Leftrightarrow\ & i_X = 0, 1, \ldots, m; i_Y = 0, 1, \ldots, m-i_X; \\ & i_{Z_1} = 0, 1, \ldots, i_Y + t, \\ x^{i_X} y^{i_y} z_1^{i_{Z_1}} z_2^{i_{Z_2}} \in M_2 \Leftrightarrow\ & i_X = 0, 1, \ldots, m; i_Y = 0, 1, \ldots, m-i_X; \\ & i_{Z_1} = 0, 1, \ldots, r-1; i_{Z_2} = 1, 2, \ldots, i_Y + t + 1. \end{aligned}$$

All these shift-polynomials $g_{T.SSE.i}$ and $g'_{T.SSE.i}$ modulo R have the roots $(x, y, z_1, z_2) = (-d, \ell, -p, -q)$ that are the same as $f_{T.SSE.i}(x, y, z_1, z_2)$. We replace each occurrence of $z_1^r z_2$ by N and construct a lattice with coefficients of $g_{T.SSE.i}(xX, yY, z_1Z_1, z_2Z_2)$ and $g'_{T.SSE.i}(xX, yY, z_1Z_1, z_2Z_2)$ as the bases. The shift-polynomials generate a triangular basis matrix. Ignoring low order terms of m, based on the Jochemsz-May strategy [JM06], LLL outputs short vectors that satisfy Lemma 1 when

$$X^{(r+1)\left(\frac{1}{6}+\frac{\tau}{2}\right)m^3} Y^{(r+1)\left(\frac{1}{3}+\frac{\tau}{2}\right)m^3} Z^{(r+1)\left(\frac{1}{6}+\frac{\tau}{2}+\frac{\tau^2}{2}\right)m^3} < W^{(r+1)\left(\frac{1}{6}+\frac{\tau}{2}\right)m^3} \qquad (1)$$

that leads to

$$0 < -(r+1)\alpha - (r+1)(2+3\tau)\beta + 3 + 3\tau - 3\tau^2.$$

To maximize the right hand side of the inequality, we set the parameter $\tau = (1-(r+1)\beta)/2$ and the condition becomes

$$\beta < \frac{7 - 2\sqrt{1+3(r+1)\alpha}}{3(r+1)}$$

as required. To satisfy the restriction $\tau \geq 0$, the condition $\beta \leq \frac{1}{r+1}$ should hold. The condition results in $\alpha \geq \frac{1}{r+1}$. □

The algorithm construction fully generalizes that of Ernst et al. that is a partial key exposure extension of the weaker Boneh-Durfee by solving integer equations, although the connection is hard to follow from the original proof in [IKK08]. In [EJMW05], Ernst et al. used a similar polynomial as $f_{T.SSE.i}$ and the condition becomes $X^{\left(\frac{1}{6}+\frac{\tau}{2}\right)m^3} Y^{\left(\frac{1}{3}+\frac{\tau}{2}\right)m^3} Z^{\left(\frac{1}{6}+\frac{\tau}{2}+\frac{\tau^2}{2}\right)m^3} < W^{\left(\frac{1}{6}+\frac{\tau}{2}\right)m^3}$. Clearly, the condition relates to that of (1). The connection comes from our definition of sets of monomials S_1, S_2, M_1, and M_2 that are generalizations of those of Ernst et al. by a factor of $(r+1)$. More concretely, each of our S_1 and S_2 for $i_{Z_1} = 0, 1, \ldots, r-1$ play the same role as that for Ernst et al. and so do M_1 and M_2 for $i_{Z_1} = 0, 1, \ldots, r-1$. Hence, our n, s_X, s_Y, and s_Z are larger by a factor of $(r+1)$ of Ernst et al. As a result, we successfully proposed a generalization the weaker Boneh-Durfee. In Section 3.2, we use the same sets of monomials S_1, S_2, M_1, and M_2 and construct a generalization of the partial key exposure attack of Ernst et al.

3.2 Partial Key Exposure Attack

In this section, we propose partial key exposure attacks on the Takagi RSA that satisfy the following property.

Theorem 2 *Let $N = p^r q$ be a public modulus and let $e \approx N^\alpha$ and $d \approx N^\beta$ be public exponent and secret exponent of the Takagi RSA, respectively. When $(\beta - \delta)\log N$ bits of the most significant bits or the least significant bits are exposed, if*

$$\delta < \frac{5 - 2\sqrt{-5+3(r+1)(\alpha+\beta)}}{3(r+1)} \text{ for } \frac{2}{r+1} \leq \alpha + \beta$$

holds, then the Takagi RSA modulus N can be factorized in polynomial time.

The result fully generalizes Ernst et al. [EJMW05] in the sense that it completely covers their attack, i.e., $\beta < \left(5 - 2\sqrt{-5+6(\alpha+\beta)}\right)/6$ for $r = 1$. When the LSBs are exposed, our attack becomes the same as Huang et al. [HHX+14].

Although the attack of Huang et al. with the MSBs is weaker than that with the LSBs, our attacks work in the same conditions. We can obtain the advantage by solving integer equations.

Proof of Theorem 2. Looking at a key generation for the Takagi RSA with the exposed bits (regardless of the MSBs or the LSBs); $e\left(\tilde{d}+(d-\tilde{d})\right)=1+\ell(p-1)(q-1)$ with some integer $|\ell|\approx N^{\alpha+\beta-2/(r+1)}$. To recover unknown parts $d-\tilde{d}$, we use the following polynomial

$$f_{T.PKE.i}(x,y,z_1,z_2)=1-e\tilde{d}+eMx+y(z_1+1)(z_2+1)$$

where $M=1$ (resp. $M=2^{\lfloor(\beta-\delta)\log N\rfloor}$) with the exposed MSBs (resp. LSBs) whose roots over the integers are $(x,y,z_1,z_2)=(-(d-\tilde{d}),\ell,-p,-q)$. The absolute values are bounded by $X:=N^{\delta}, Y:=N^{\alpha+\beta-2/(r+1)}, Z_1:=2N^{1/(r+1)}, Z_2:=2N^{1/(r+1)}$. We also use a notation $Z=Z_1=Z_2$ for simplicity.

These formulations and those for small secret exponent attacks in Section 3.1 are essentially the same when we use the Jochemsz-May strategy. That means the Newton polygons of polynomials $f_{T.SSE.i}(x,y,z_1,z_2)$ and $f_{T.PKE.i}(x,y,z_1,z_2)$ are the same, e.g., there are six monomials for variables $1,x,y,yz_1,yz_2$, and yz_1z_2. Hence, we use almost the same algorithm construction. We set an (possibly large) integer W such that $W<N^{\alpha+\beta}$ since $\|f_{T.SSE.i}(xX,yY,z_1Z_1,z_2Z_2)\|_\infty\geq\max\{|1-e\tilde{d}|,|eMX|\}\approx N^{\alpha+\beta}$. Next, we set an integer $R:=W(XY)^{m-1}\cdot Z^{m+r-1+t}$ with some integers $m=\omega(r)$ and $t=\tau m$ where $\tau\geq 0$ such that $\gcd(R,1-e\tilde{d})=1$. We compute $c=(1-e\tilde{d})^{-1} \mod R$ and $f'_{T.PKE.i}(x,y,z_1,z_2) := c\cdot f_{T.PKE.i}(x,y,z_1,z_2) \mod R$. We define shift-polynomials $g_{T.PKE.i}$ and $g'_{T.PKE.i}$ as

$$g_{T.PKE.i}: x^{i_X}y^{i_Y}z_1^{i_{Z_1}}z_2^{i_{Z_2}}\cdot f'_{T.PKE.i}\cdot X^{m-1-i_X}Y^{m-1-i_Y}Z^{m+r-1+t-i_{Z_1}-i_{Z_2}}$$
$$\text{for } x^{i_X}y^{i_Y}z_1^{i_{Z_1}}z_2^{i_{Z_2}}\in S_1\cup S_2,$$
$$g'_{T.PKE.i}: x^{i_X}y^{i_Y}z_1^{i_{Z_1}}z_2^{i_{Z_2}}\cdot R \quad \text{for } x^{i_X}y^{i_Y}z_1^{i_{Z_1}}z_2^{i_{Z_2}}\in(M_1\cup M_2)\backslash(S_1\cup S_2),$$

for sets of monomials S_1,S_2,M_1, and M_2 that are the same as in Section 3.1 where $f_{T.SSE.i}$ is replaced by $f'_{T.PKE.i}$. All these shift-polynomials $g_{T.PKE.i}$ and $g'_{T.PKE.i}$ modulo R have the roots $(x,y,z_1,z_2)=(-(d-\tilde{d}),\ell,-p,-q)$ that are the same as $f_{T.PKE.i}(x,y,z_1,z_2)$. We replace each occurrence of $z_1^rz_2$ by N and construct a lattice with coefficients of $g_{T.PKE.i}(xX,yY,z_1Z_1,z_2Z_2)$ and $g'_{T.PKE.i}(xX,yY,z_1Z_1,z_2Z_2)$ as the bases. Hence, ignoring low order terms of m, based on the Jochemsz-May strategy [JM06], LLL outputs short lattice vectors that satisfy Lemma 1 when the inequality (1) holds. For partial key exposure attacks (regardless of the MSBs or the LSBs are exposed), the inequality becomes

$$0<-(r+1)(\alpha+\beta)-(r+1)\delta(1+3\tau)+3+3\tau-3\tau^2.$$

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

$$\delta<\frac{5-2\sqrt{-5+3(r+1)(\alpha+\beta)}}{3(r+1)}$$

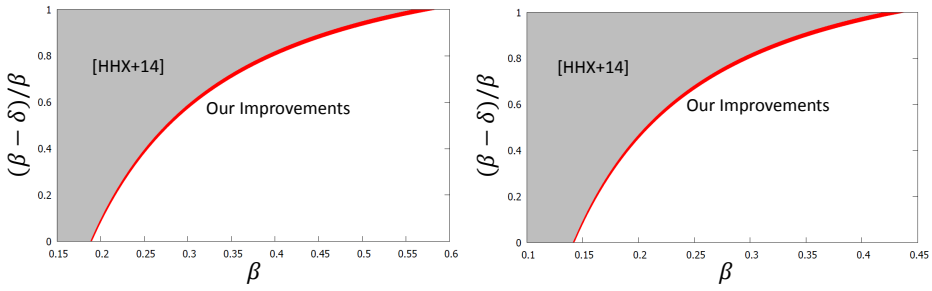

Fig. 1. Comparisons of partial key exposure attacks on the Takagi RSA when the MSBs are exposed for $\alpha = 1/(r+1)$. We compare how much portions of d should be exposed for β between the attack of Huang et al. [HHX+14] and our Theorem 2. The left figure is for $r = 2$ and the right figure is for $r = 3$.

as required. To satisfy the restriction $\eta \geq 0$, the condition $\delta \leq \frac{1}{r+1}$ should hold. The condition results in $\frac{2}{r+1} \leq \alpha + \beta$. □

As we claimed in Section 3.1, the algorithm construction fully generalizes Ernst et al.

When the MSBs are exposed, our attack is always better than Huang et al. [HHX+14] that works when $\delta < \frac{7-\sqrt{-39+24(r+1)(\alpha+\beta)}}{4(r+1)}$. Figure 1 compare Theorem 2 and Huang et al. for $r = 2$ and 3. Our attack is the better for all β, e.g., our attack works with less partial information.

In Section 4.2, we propose an improved attack when the LSBs are exposed. It seems that our Theorem 2 with the exposed MSBs is hard to be improved. Although there exist attacks that are better than Ernst et al. (the other attack of Ernst et al. [EJMW05] and Takayasu and Kunihiro's attack [TK14]), by definition, it seems difficult to generalize the attacks for the Takagi RSA since both attacks make use of the MSBs of ℓ. To compute the MSBs of ℓ, we have to know the MSBs of $(p-1)(q-1)$. It is possible for the standard RSA since $pq = N$. However, it seems difficult for the Takagi RSA. Hence, to improve Theorem 2, we have to exploit the special structure of the Takagi RSA or improve the attacks on the standard RSA without the knowledge of the MSBs of ℓ.

4 Attacks on the Takagi RSA by Solving Modular Equations

In this section, we analyze the security of the Takagi RSA by solving modular equations. In Section 4.1, we give an alternative proof of the Itoh et al. small secret exponent attack [IKK08] that is analogous to Herrmann and May [HM10]. In Section 4.2, we propose a partial key exposure attack that fully generalizes Takayasu and Kunihiro's result [TK14].

4.1 Small Secret Exponent Attack

In this section, we prove the following Itoh et al. small secret exponent attack. The result fully generalizes the stronger Boneh-Durfee [BD00] in the sense that it completely covers their attack, i.e., $\beta < 1 - 1/\sqrt{2}$ for $r = 1$ and $\alpha = 1$.

Theorem 3 ([IKK08]) *Let $N = p^r q$ be a public modulus and let $e \approx N^\alpha$ and $d \approx N^\beta$ be public exponent and secret exponent of the Takagi RSA, respectively. If*

$$\beta < \frac{2 - \sqrt{(r+1)\alpha}}{r+1} \text{ for } \frac{1}{r+1} \leq \alpha$$

holds, then the Takagi RSA modulus N can be factorized in polynomial time.

The original proof in [IKK08] is involved since they used geometrically progressive matrix. We use unravelled linearization [HM09] and offer simpler proof. Moreover, we exploit the exact connection between the algorithm constructions of Itoh et al. and the stronger Boneh-Durfee.

Alternative Proof of Theorem 3. Looking at a key generation for the Takagi RSA modulo $N = p^r q$, $ed = 1 + \ell(p-1)(q-1)$ with some integer $|\ell| \approx N^{\alpha+\beta-2/(r+1)}$. Itoh et al. [IKK08] considered a polynomial

$$f_{T.SSE.m}(x, y_1, y_2) = 1 + x(y_1 + 1)(y_2 + 1).$$

The polynomial modulo e has roots $(x, y_1, y_2) = (\ell, -p, -q)$. The absolute values are bounded by $X := N^{\alpha+\beta-2/(r+1)}, Y_1 = Y_2 := 2N^{1/(r+1)}$. Let $m = \omega(r)$ be an integer and $\tau \geq 0$. To solve a modular equation $f_{T.SSE.m}(x, y_1, y_2) = 0 \mod e$, we use shift-polynomials

$$g_{T.SSE.m}(x, y_1, y_2) = x^{i_X} y_1^{i_{Y_1}} y_2^{i_{Y_2}} f_{T.SSE.m}^u(x, y_1, y_2) e^{m-u}$$

with indices in

$$\begin{aligned}
\mathcal{I}_{x1} \Leftrightarrow\ & u = 0, 1, \ldots, m; i_X = 0, 1, \ldots, m-u; i_{Y_1} = 0; i_{Y_2} = 0, \text{or} \\
\mathcal{I}_{x2} \Leftrightarrow\ & u = 0, 1, \ldots, m; i_X = 0, 1, \ldots, m-u; i_{Y_1} = 0, 1, \ldots, r-1; i_{Y_2} = 1, \\
\mathcal{I}_{y1} \Leftrightarrow\ & u = 0, 1, \ldots, m; i_X = 0; i_{Y_1} = 1, 2, \ldots, \lceil \tau u \rceil; i_{Y_2} = 0, \text{or} \\
\mathcal{I}_{y2} \Leftrightarrow\ & u = 0, 1, \ldots, m; i_X = 0; i_{Y_1} = 0, 1, \ldots, r-1; i_{Y_2} = 2, 3, \ldots, \lceil \tau u \rceil.
\end{aligned}$$

All these shift-polynomials $g_{T.SSE.m}$ modulo e^m have the roots $(x, y_1, y_2) = (\ell, -p, -q)$ that are the same as $f_{T.SSE.m}$. We replace each occurrence of $y_1^r y_2$ by N and construct a lattice with coefficients of $g_{T.SSE.m}(xX, y_1 Y_1, y_2 Y_2)$ as the bases.

Here, we observe why the construction offers a bound outperforming the Jochemsz-May strategy. In the above $\mathcal{I}_{y1}$ and $\mathcal{I}_{y2}$, i_{Y_1} and i_{Y_2} are upper bounded by $\lceil \tau u \rceil$ that depend on u. In the Jochemsz-May strategy, the corresponding indices ($i_{Z_1} - i_Y$ and $i_{Z_2} - i_Y$ in S_1, S_2, M_1, and M_2 in Section 3.1) are bounded

by $t = \tau m$ that only depends m. Since the former covers the latter, we can analyze broader classes of lattice constructions. The restriction of the Jochemsz-May strategy offers simpler analysis with a triangular basis matrix although that does not always offer the best bound. Moreover, the parameter is eventually set to $\tau = 1 - (r+1)\beta$. The optimization follows from the fact that shift-polynomials $g_{T.SSE.m}$ with indices in $\mathcal{I}_{y1}$ and $\mathcal{I}_{y2}$ reduce the norm of outputs of the LLL algorithm, e.g., the diagonals for the shift-polynomials are smaller than the modulus e^m. This observation enables readers to understand our improvements in Section 6 easily.

However, the former selection requires involved analysis since the shift-polynomials generate non-triangular basis matrices. The dependence of the Jochemsz-May strategy always generates triangular basis matrices and the analysis is easy. To construct partial key exposure attacks outperforming the Jochemsz-May strategy, we require better understanding for small secret exponent attacks. For the purpose, we show an analogous elementary proof to Herrmann and May [HM10]. Although the above shift-polynomials generate non-triangular basis matrices, we can transform it to be triangular by using unravelled linearization.

Lemma 2 *Using a linearization $z_1 = 1 + xy_1$ and $z_2 = 1 + xy_2$, the above shift-polynomials generate a triangular basis matrix. The diagonals of the basis matrix for $g_{T.SSE.m}$ are*

- $X^{u+i_X} Y_1^u e^{m-u}$ *for indices in $\mathcal{I}_{x1}$,*
- $X^{u+i_X} Y_1^{i_{Y_1}} Y_2^{u+1} e^{m-u}$ *for indices in $\mathcal{I}_{x2}$,*
- $Y_1^{i_{Y_1}} Z_1^u e^{m-u}$ *for indices in $\mathcal{I}_{y1}$,*
- $Y_1^{i_{Y_1}} Y_2 Z_2^u e^{m-u}$ *for indices in $\mathcal{I}_{y2}$.*

Indeed, the transformation is analogous to Herrmann and May [HM10], and show the exact connection with the stronger Boneh-Durfee and the Itoh et al. attack although the connection is hard to follow from the original proof [IKK08]. The shift-polynomials for indices in $\mathcal{I}_{x1}$ and $\mathcal{I}_{x2}$ for $i_{Y_1} = 0, 1, \ldots, r-1$ (resp. $\mathcal{I}_{y1}$ and $\mathcal{I}_{y2}$ for $i_{Y_1} = 0, 1, \ldots, r-1$) play the same role as x-shifts (resp. y-shifts) of the stronger Boneh-Durfee. Ignoring low order terms of m, the dimension of the lattice is $(r+1)\left(\frac{1}{2} + \frac{\tau}{2}\right) m^2$, and the determinant of the basis matrix is $X^{(r+1)\left(\frac{1}{3}+\frac{\tau}{3}\right)m^3} Y^{(r+1)\left(\frac{1}{6}+\frac{\tau}{3}+\frac{\tau^2}{6}\right)m^3} e^{(r+1)\left(\frac{1}{3}+\frac{\tau}{6}\right)m^3}$. Notice that $Z_1 = Z_2 \approx XY$. Again, we stress the connection with the stronger Boneh-Durfee. In the proof, a dimension of a lattice is $\left(\frac{1}{2} + \frac{\tau}{2}\right) m^2$ and its determinant is $X^{\left(\frac{1}{3}+\frac{\tau}{3}\right)m^3} Y^{\left(\frac{1}{6}+\frac{\tau}{3}+\frac{\tau^2}{6}\right)m^3} e^{\left(\frac{1}{3}+\frac{\tau}{6}\right)m^3}$. Hence, it is clear that the algorithm construction of Itoh et al. is a generalization of that for the stronger Boneh-Durfee. We set the parameter $\tau = 1 - (r+1)\beta$, and obtain Theorem 3. Here, we omit overall calculations since they are completely the same as those in [IKK08]. □

4.2 Partial Key Exposure Attack

In this section, we propose a partial key exposure attack on the Takagi RSA that satisfies the following property.

Theorem 4 *Let $N = p^r q$ be a public modulus and let $e \approx N^\alpha$ and $d \approx N^\beta$ be public exponent and secret exponent of the Takagi RSA, respectively. When $(\beta - \delta)\log N$ bits of the least significant bits are exposed, if*

$$\delta < \frac{2 + (r+1)\beta - \sqrt{-12 + 4(r+1)\alpha + 12(r+1)\beta - 3(r+1)^2\beta^2}}{2(r+1)} \text{ and}$$
$$\beta \leq \frac{9 - \sqrt{-3 + 12(r+1)\alpha}}{6(r+1)}$$

hold, then the Takagi RSA modulus N can be factorized in polynomial time.

The result fully generalizes Takayasu and Kunihiro's result [TK14] in the sense that it completely covers their attack, i.e., $\delta < \left(1 + \beta - \sqrt{-1 + 6\beta - 3\beta^2}\right)/2$ and $\beta < (9 - \sqrt{21})/12$ for $r = 1$ and $\alpha = 1$.

Proof of Theorem 4. Looking at a key generation for the Takagi RSA with the exposed LSBs; $e(d_1 M + d_0) = 1 + \ell(p-1)(q-1)$ with some integer $|\ell| \approx N^{\alpha+\beta-2/(r+1)}$. To recover the unknown MSBs of the secret exponent d_1, we use the following polynomials

$$f_{T.PKE.m1}(x, y_1, y_2) = 1 - ed_0 + x(y_1 + 1)(y_2 + 1) \text{ and}$$
$$f_{T.PKE.m2}(x, y_1, y_2) = 1 + x(y_1 + 1)(y_2 + 1)$$

whose roots with appropriate moduli are $(x, y_1, y_2) = (\ell, -p, -q)$, e.g., $f_{T.PKE.m1}(\ell, -p, -q) = 0 \mod eM$ and $f_{T.PKE.m2}(\ell, -p, -q) = 0 \mod e$. The absolute values are bounded by $X := N^{\alpha+\beta-2/(r+1)}, Y_1 = Y_2 := 2N^{1/(r+1)}$. Let $m = \omega(r)$ be an integer and define a function

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

To solve modular equations $f_{T.PKE.m1}(x, y_1, y_2) = 0 \mod eM$ and $f_{T.PKE.m2}(x, y_1, y_2) = 0 \mod e$ simultaneously, we use following shift-polynomials

$$g_{T.PKE.m1}(x, y_1, y_2) = x^{i_X} y_1^{i_{Y_1}} y_2^{i_{Y_2}} f_{T.PKE.m1}^u(x, y_1, y_2)(eM)^{m-u},$$
$$g_{T.PKE.m2}(x, y_1, y_2) = y_1^{i_{Y_1}+k_1} y_2^{i_{Y_2}+k_2} f_{T.PKE.m1}^{u-\lceil l_r(k_1+k_2)\rceil}(x, y_1, y_2) \cdot f_{T.PKE.m2}^{\lceil l_r(k_1+k_2)\rceil}(x, y_1, y_2) e^{m-u} M^{m-(u-\lceil l_r(k_1+k_2)\rceil)}.$$

To construct a lattice we use $g_{T.PKE.m1}$ with indices in $\mathcal{I}_{x1}, \mathcal{I}_{x2}$ and $g_{T.PKE.m2}$ with indices in $\mathcal{I}_{y1}, \mathcal{I}_{y2}$ where

$$\mathcal{I}_{x1} \Leftrightarrow\ u = 0, 1, \ldots, m; i_X = 0, 1, \ldots, m - u; i_{Y_1} = 0; i_{Y_2} = 0,$$
$$\mathcal{I}_{x2} \Leftrightarrow\ u = 0, 1, \ldots, m; i_X = 0, 1, \ldots, m - u; i_{Y_1} = 0, 1, \ldots, r - 1; i_{Y_2} = 1,$$
$$\mathcal{I}_{y1} \Leftrightarrow\ u = 0, 1, \ldots, m; i_{Y_1} = 0; i_{Y_2} = 0;$$
$$k_1 = 1, 2, \ldots, \lfloor (r+1)(\beta - \delta)m + (1 + (r+1)(\delta - 2\beta))u \rfloor; k_2 = 0,$$

$$\mathcal{I}_{y2} \Leftrightarrow\ u = 0, 1, \ldots, m; i_{Y_1} = 0, 1, \ldots, r-1; i_{Y_2} = 1; k_1 = 0;$$
$$k_2 = 1, 2, \ldots, \lfloor (r+1)(\beta-\delta)m + (1+(r+1)(\delta-2\beta))u \rfloor.$$

All these shift-polynomials $g_{T.PKE.m1}$ and $g_{T.PKE.m2}$ modulo $(eM)^m$ have the roots $(x, y_1, y_2) = (\ell, -p, -q)$ that are the same as $f_{T.PKE.m}$. We replace each occurrence of $y_1^r y_2$ by N and construct a lattice with coefficients of $g_{T.PKE.m1}(xX, y_1Y_1, y_2Y_2)$ and $g_{T.PKE.m2}(xX, y_1Y_1, y_2Y_2)$ as the bases.

As in the proof of Theorem 3, the shift-polynomials $g_{T.PKE.m1}$ with indices in $\mathcal{I}_{x1}$ and $\mathcal{I}_{x2}$ for $i_{Y_1} = 0, 1, \ldots, r-1$ (resp. $g_{T.PKE.m2}$ with indices in $\mathcal{I}_{y1}$ and $\mathcal{I}_{y2}$ for $i_{Y_1} = 0, 1, \ldots, r-1$) play the same role as x-shifts (resp. y-shifts) of Takayasu and Kunihiro. The shift-polynomials generate a triangular basis matrix using a linearization $z_1 = 1 + xy_1$ and $z_2 = 1 + xy_2$. Assume $1 + (r+1)(\delta - 2\beta) \geq 0$ and the diagonals of the basis matrix are

- $X^{u+i_X} Y_1^u e^{m-u}$ for $g_{T.PKE.m1}$ with indices in $\mathcal{I}_{x1}$,
- $X^{u+i_X} Y_1^{i_{Y_1}} Y_2^{u+1} e^{m-u}$ for $g_{T.PKE.m1}$ with indices in $\mathcal{I}_{x2}$,
- $X^{u-\lceil l_r(k_1) \rceil} Y_1^{u-\lceil l_r(k_1) \rceil + k_1} Z_1^{\lceil l_r(k_1) \rceil} e^{m-u} M^{m-(u-\lceil l_r(k_1) \rceil)}$ for $g_{T.PKE.m2}$ with indices in $\mathcal{I}_{y1}$,
- $X^{u-\lceil l_r(k_2) \rceil} Y_1^{i_{Y_1}} Y_2^{u-\lceil l_r(k_2) \rceil + k_1 + 1} Z_2^{\lceil l_r(k_2) \rceil} e^{m-u} M^{m-(u-\lceil l_r(k_2) \rceil)}$ for $g_{T.PKE.m2}$ with indices in $\mathcal{I}_{y2}$.

In $\mathcal{I}_{y1}$ and $\mathcal{I}_{y2}$, k_1 and k_2 are upper bounded by $\lfloor (r+1)(\beta-\delta)m + (1+(r+1)(\delta - 2\beta))u \rfloor$. As Takayasu and Kunihiro, the definition follows from the fact that the shift-polynomials reduce norms of output vectors by the LLL algorithm.

As the proof of Theorem 3, all these values are larger by a factor of $(r+1)$ of Takayasu and Kunihiro's. Ignoring low order term of m, the LLL algorithm outputs short vectors that satisfy Lemma 1 when

$$(r+1)^2\delta^2 - (r+1)(2+(r+1)\beta)\delta + 4 - (r+1)\alpha - 2(r+1)\beta + (r+1)^2\beta^2 > 0.$$

Hence, we obtain the bound of Theorem 4

$$\delta < \frac{2 + (r+1)\beta - \sqrt{-12 + 4(r+1)\alpha + 12(r+1)\beta - 3(r+1)^2\beta^2}}{2(r+1)}$$

as required. To satisfy the restriction $1 + (r+1)(\delta - 2\beta) \geq 0$, the condition $\beta \leq \frac{9 - \sqrt{-3 + 12(r+1)\alpha}}{6(r+1)}$ should hold. □

When the LSBs are exposed and $\beta \leq \frac{9 - \sqrt{-3 + 12(r+1)\alpha}}{6(r+1)}$, our attack is better than Huang et al. [HHX+14] that works when $\delta < \frac{5 - 2\sqrt{-5 + 3(r+1)(\alpha+\beta)}}{3(r+1)}$. Figure 2 compare our results and Huang et al. for $r = 2$ and 3. Our attack is the better for small β, e.g., our attack works with less partial information.

5 Attacks on the Prime Power RSA by Solving Integer Equations

In this section, we analyze the security of the prime power RSA by solving integer equations. In Section 5.1, we propose a small secret exponent attack that fully

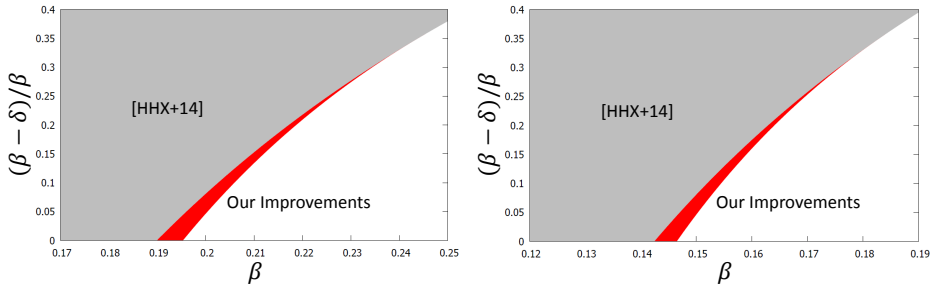

Fig. 2. Comparisons of partial key exposure attacks on the Takagi RSA when the LSBs are exposed and $\alpha = 1/(r+1)$. We compare how much portions of d should be exposed for β between the attack of Huang et al. [HHX+14] and our Theorem 4. The left figure is for $r = 2$ and the right figure is for $r = 3$.

generalizes the weaker Boneh-Durfee result [BD00]. In Section 5.2, we propose a partial key exposure attack that fully generalizes Ernst et al. [EJMW05].

5.1 Small Secret Exponent Attack

In this section, we propose small secret exponent attacks on the prime power RSA that satisfy the following property.

Theorem 5 *Let $N = p^r q$ be a public modulus for $r \geq 2$ and let $e \approx N^\alpha$ and $d \approx N^\beta$ be public exponent and secret exponent of the prime power RSA, respectively. If*

$$0 < -r(r+1)^2\alpha + r(r+1)(1-\beta)(2(r+1)+3r\tau) - 1 - 3r\eta(1+r\eta) - r^3(1-\eta+\tau)^3 + r^2(\eta-\tau)^3 \text{ where}$$

$$\eta = \frac{r(r+1)(1-\beta)-1}{2r} \text{ and } \tau = \eta - \frac{r - \sqrt{-r+(r+1)^2(1-\beta)}}{r+1}$$

$$\text{for } \frac{3r^3+r^2+r-1}{4(r+1)} \leq \alpha, \text{ or}$$

$$\beta < \frac{r+(\sqrt{r}-1)^2}{2r(r+1)} - \frac{\alpha}{2} \text{ for } \frac{r+(\sqrt{r}-1)^2}{r(r+1)} < \alpha \leq \frac{3r^3+r^2+r-1}{4(r+1)}$$

holds, then prime power RSA modulus N can be factorized in polynomial time.

The result extends Sarkar's attack [Sar15] for arbitrary α although they solved modular equations. The result for $r = 1$ does not cover the weaker Boneh-Durfee [BD00]. Moreover, the second condition becomes $\beta < 1/4$ for $r = 1$ and $\alpha = 1$ that is the same as Wiener's result [Wie90]. Indeed, Sarkar did not claim the connection with their attack and the weaker Boneh-Durfee at all. However, we think that the result fully generalizes the weaker Boneh-Durfee. Although we

should use parameters (η and τ such that $\eta \geq \tau$ in the following proof) that do not exactly cover lattices for the weaker Boneh-Durfee to make use of the special structure of the prime power RSA, the construction is conceptually the same. Moreover, we will show in Section 5.2 that our construction covers Ernst et al. [EJMW05] that is a partial key exposure extension of the weaker Boneh-Durfee. The proof is convenient to analyze partial key exposure attacks in Section 3.2.

Proof of Theorem 5. Looking at a key generation for the prime power RSA; $ed = 1 + \ell p^{r-1}(p-1)(q-1)$ with some integer $|\ell| \approx N^{\alpha+\beta-1}$. To recover the secret exponent d, we use the following polynomial

$$f_{PP.SSE.i}(x, y, z_1, z_2) = 1 + ex + yz_1^{r-1}(z_1 - 1)(z_2 - 1)$$

whose roots over the integers are $(x, y, z_1, z_2) = (-d, \ell, p, q)$. The absolute values are bounded by $X := N^{\beta}, Y := N^{\alpha+\beta-1}, Z_1 := 2N^{1/(r+1)}, Z_2 := 2N^{1/(r+1)}$. We also use a notation $Z = Z_1 = Z_2$ for simplicity. We set an (possibly large) integer W such that $W < N^{\alpha+\beta}$ since $\|f_{PP.SSE}(xX, yY, z_1Z_1, z_2Z_2)\|_{\infty} \geq |eX| \approx N^{\alpha+\beta}$. Next, we set an integer $R := W(XY)^{m-1}Z^{r(m-1-a+t)}$ with some integers $m = \omega(r), t = \tau m$, and $a = \eta m$ where $\tau \geq 0$ and $\eta \geq \tau$. We define shift-polynomials $g_{PP.SSE.i}$ and $g'_{PP.SSE.i}$ as

$$\begin{aligned}
g_{PP.SSE.i} &: x^{i_X} y^{i_Y} z_1^{i_{Z_1}} z_2^{i_{Z_2}} \cdot f_{PP.SSE.i} \cdot X^{m-1-i_X} Y^{m-1-i_Y} Z^{r(m-1-a+t)-i_{Z_1}-i_{Z_2}} \\
&\qquad \text{for } x^{i_X} y^{i_Y} z_1^{i_{Z_1}} z_2^{i_{Z_2}} \in S, \\
g'_{PP.SSE.i} &: x^{i_X} y^{i_Y} z_1^{i_{Z_1}} z_2^{i_{Z_2}} \cdot R \quad \text{for } x^{i_X} y^{i_Y} z_1^{i_{Z_1}} z_2^{i_{Z_2}} \in M \backslash S,
\end{aligned}$$

for sets of monomials

$$\begin{aligned}
S &:= \bigcup_{0 \leq j \leq rt} \left\{ x^{i_X} y^{i_Y} z_1^{i_{Z_1}+j} z_2^{i_{Z_2}} \middle| \begin{array}{c} x^{i_X} y^{i_Y} z_1^{i_{Z_1}} z_2^{i_{Z_2}} \text{ is a monomial of} \\ \tilde{s} \cdot f_{PP.SSE.i}(x, y, z_1, z_2)^{m-1} \text{ where} \\ \tilde{s} = \left\{ z_2^a, z_1 z_2^a, z_1^2 z_2^a, \ldots, z_1^r z_2^a, z_1^{r-1} z_2^{a+1} \right\} \end{array} \right\}, \\
M &:= \left\{ x^{i_X} y^{i_Y} z_1^{i_{Z_1}} z_2^{i_{Z_2}} \middle| \begin{array}{c} \text{monomials of } x^{i'_X} y^{i'_Y} z_1^{i'_{Z_1}} z_2^{i'_{Z_2}} \cdot f_{PP.SSE.i}(x, y, z_1, z_2) \\ \text{where } x^{i'_X} y^{i'_Y} z_1^{i'_{Z_1}} z_2^{i'_{Z_2}} \in S \end{array} \right\},
\end{aligned}$$

with an integer $a = \eta m$ for $\eta \geq \tau$. By definition, it follows that

$$\begin{aligned}
x^{i_X} y^{i_y} z_1^{i_{Z_1}} z_2^{i_{Z_2}} \in S \Leftrightarrow\ & i_X = 0, 1, \ldots, m - a + t - 1; \\
& i_Y = a - t, a - t + 1, \ldots, m - 1 - i_X; \\
& i_{Z_1} = 0, 1, \ldots, r(i_Y - a + t); i_{Z_2} = 0, \text{ and} \\
& i_X = 0, 1, \ldots, m - 1; i_Y = 0, 1, \ldots, m - 1 - i_X; \\
& i_{Z_1} = \max\{0, r - i_Y + r(i_{Z_2} - 1 - a)\}, \ldots, r - 1; \\
& i_{Z_2} = a + 1, a + 2, \ldots, a + \lceil (i_Y + 1)/r \rceil, \text{ and} \\
& i_X = 0, 1, \ldots, m - 1; i_Y = 0, 1, \ldots, m - 1 - i_X; \\
& i_{Z_1} = 0, 1, \ldots, r - 1; \\
& i_{Z_2} = \max\{0, -i_Y + a - t\}, \ldots, a,
\end{aligned}$$

$$
\begin{aligned}
x^{i_X} y^{i_y} z_1^{i_{Z_1}} z_2^{i_{Z_2}} \in M \Leftrightarrow\ & i_X = 0, 1, \ldots, m - a + t; \\
& i_Y = a - t, a - t + 1, \ldots, m - i_X; \\
& i_{Z_1} = 0, 1, \ldots, r(i_Y - a + t); i_{Z_2} = 0, \text{ and} \\
& i_X = 0, 1, \ldots, m; i_Y = 0, 1, \ldots, m - i_X; \\
& i_{Z_1} = \max\{0, r - i_Y + r(i_{Z_2} - 1 - a)\}, \ldots, r - 1; \\
& i_{Z_2} = a + 1, a + 2, \ldots, a + \lceil (i_Y + 1)/r \rceil, \text{ and} \\
& i_X = 0, 1, \ldots, m; i_Y = 0, 1, \ldots, m - i_X; \\
& i_{Z_1} = 0, 1, \ldots, r - 1; \\
& i_{Z_2} = \max\{0, -i_Y + a - t\}, \ldots, a.
\end{aligned}
$$

All these shift-polynomials $g_{PP.SSE.i}$ and $g'_{PP.SSE.i}$ modulo R have the roots $(x, y, z_1, z_2) = (-d, \ell, -p, -q)$ that are the same as $f_{PP.SSE.i}(x, y, z_1, z_2)$. We replace each occurrence of $z_1^r z_2$ by N and construct a lattice with coefficients of $g_{PP.SSE.i}(xX, yY, z_1 Z_1, z_2 Z_2)$ and $g'_{PP.SSE.i}(xX, yY, z_1 Z_1, z_2 Z_2)$ as the bases. The shift-polynomials generate a triangular basis matrix.

Ignoring low order terms of m, based on the Jochemsz-May strategy [JM06], LLL outputs short vectors that satisfy Lemma 1 when

$$
X^{\left(\frac{r+1}{6}+\frac{r}{2}\tau\right)m^3} Y^{\left(\frac{r+1}{3}+\frac{r}{2}\tau\right)m^3} Z_1^{\left(\frac{r^2(1-\eta+\tau)^3}{6}\right)m^3} Z_2^{\left(\frac{1}{6r}+\frac{1}{2}\eta+\frac{r}{2}\eta^2-\frac{r}{6}(\eta-\tau)^3\right)m^3} < W^{\left(\frac{r+1}{6}+\frac{r}{2}\tau\right)m^3} \tag{2}
$$

that leads to

$$
\begin{aligned}
0 < & -r(r+1)^2\alpha + r(r+1)(1-\beta)(2(r+1)+3r\tau) \\
& - 1 - 3r\eta(1+r\eta) - r^3(1-\eta+\tau)^3 + r^2(\eta-\tau)^3.
\end{aligned} \tag{3}
$$

To maximize the right hand side of the inequality, we set parameters $\eta = \frac{r(r+1)(1-\beta)-1}{2r}$ and $\tau = \eta - \frac{r-\sqrt{-r+(r+1)^2(1-\beta)}}{r+1}$ that results in the first condition of Theorem 5.

To satisfy the restriction $\tau \geq 0$, the condition $\beta \leq \frac{r^2-r-1+2\sqrt{r}}{r(r+1)}$ should hold. The condition results in $\alpha \geq \frac{3r^3+r^2+r-1}{4(r+1)}$. Other restrictions $\eta \geq \tau$ and $\eta \geq 0$ always hold.

In the other cases, e.g. $\alpha \leq \frac{3r^3+r^2+r-1}{4(r+1)}$, we fix the parameter $\tau = 0$. To maximize the right hand side of the inequality (3), we set the other parameter $\eta = 1 - 1/\sqrt{r}$ and the condition becomes

$$
\beta < \frac{r + (\sqrt{r}-1)^2}{2r(r+1)} - \frac{\alpha}{2}
$$

as required. Since the prime power RSA satisfies $\alpha + \beta > 1$ by definition, $\alpha > \frac{r+(\sqrt{r}-1)^2}{r(r+1)}$ should hold. □

This attack is an extension of Sarkar's attack [Sar15] for arbitrary α. However, the extension offers an advantage of the approach although Sarkar did not claim.

Lu et al. [LZPL15] claimed that their attack, which works when $\beta < \frac{r(r-1)}{(r+1)^2}$, is better than Sarkar's attack for $r \geq 5$. Indeed, the attack of Lu et al. is better than Theorem 5 for $\alpha = 1$ (that is equivalent to Sarkar's attack). However, our attack becomes better than the attack of Lu et al. for small α. Considering the restriction $\alpha + \beta > 1$, although the attack of Lu et al. works when $\alpha > \frac{3r+1}{(r+1)^2}$, our attack works when $\alpha > \frac{r+(\sqrt{r}-1)^2}{r(r+1)}$. Hence, our attack works for smaller α than Lu et al. In Section 6.1, we propose further (although slight) improvements and compare our results and Lu et al.

We note that the restriction $\eta \geq \tau$ comes from the fact that we can obtain better results than $\eta < \tau$ for small secret exponent attacks on the prime power RSA for $r \geq 2$. As we claimed, the algorithm construction fully generalizes the weaker Boneh-Durfee. That means the weaker Boneh-Durfee result can be obtained by setting $\eta < \tau$. The connection is hard to follow from Sarkar's proof [Sar15] and they did not claim it. As our previous proofs, the construction comes from our definition of sets of monomials S and M that play the same roles as those for Ernst et al. that is a partial key exposure extension of the weaker Boneh-Durfee. More concretely, each of our S for $\tilde{s} = \left\{z_2^a, z_1 z_2^a, z_1^2 z_2^a, \ldots, z_1^{r-1} z_2^a, z_1^{r-1} z_2^{a+1}\right\}$ play the same role as that for Ernst et al. and so do M. However, our n, s_X, s_Y, and s_Z do not become larger by a factor of $(r+1)$ of those of Ernst et al for the asymmetry of p and q for the prime power RSA key generation. So far, the asymmetry made it difficult to exploit the connection between the standard RSA and the prime power RSA, and to generalize attacks on the standard RSA to the prime power RSA.

5.2 Partial Key Exposure Attack.

In this section, we propose partial key exposure attacks on the prime power RSA that satisfy the following property.

Theorem 6 *Let $N = p^r q$ be a public modulus and let $e \approx N^\alpha$ and $d \approx N^\beta$ be public exponent and secret exponent of prime power RSA, respectively. When $(\beta - \delta)\log N$ bits of the most significant bits or the least significant bits are exposed, if*

$$
\begin{aligned}
&0 < -r(r+1)^2(\alpha+\beta) + r(r+1)(1-\delta)((r+1)+3r\tau) + r(r+1)^2 - 1 \\
&\quad - 3r\eta(1+r\eta) - r^3(1-\eta+\tau)^3 + r^2(\eta-\tau)^3 \ \textit{where} \\
&\eta = \frac{r(r+1)(1-\delta)-1}{2r} \ \textit{and} \ \tau = \eta - \frac{r - \sqrt{-r + (r+1)^2(1-\delta)}}{r+1} \\
&\textit{for } 1 < \alpha+\beta \leq \frac{3r^3+r^2+5r-1}{4r(r+1)}, \textit{or} \\
&\delta < 1 - \frac{r + \sqrt{12r^2(r+1)(\alpha+\beta) - r(9r^2+14r-3)}}{3r(r+1)} \\
&\textit{for } \frac{3r^3+r^2+5r-1}{4r(r+1)} \leq \alpha+\beta
\end{aligned}
$$

holds, then prime power RSA modulus N can be factorized in polynomial time.

The result fully generalizes Ernst et al. [EJMW05] in the sense that it completely covers their attack, i.e., $\beta < \left(5 - 2\sqrt{-5 + 6(\alpha + \beta)}\right)/6$ for $r = 1$. Moreover, we exploit the exact connection between the algorithm constructions of Theorem 6 and the Ernst et al.

Proof of Theorem 6. Looking at a key generation for prime power RSA with the exposed bits (regardless of the MSBs or the LSBs); $e(\tilde{d} + (d - \tilde{d})) = 1 + \ell p^{r-1}(p - 1)(q - 1)$ with some integer $|\ell| \approx N^{\alpha+\beta-1}$. To recover unknown parts $d - \tilde{d}$, we use the following polynomial

$$f_{PP.PKE.i}(x, y, z_1, z_2) = 1 - e\tilde{d} + eMx + yz_1^{r-1}(z_1 - 1)(z_2 - 1)$$

where $M = 1$ (resp. $M|2^{\lfloor(\beta-\delta)\log N\rfloor}$) with the exposed MSBs (resp. LSBs) whose roots over the integers are $(x, y, z_1, z_2) = (-(d - \tilde{d}), \ell, p, q)$. The absolute values are bounded by $X := N^{\delta}, Y := N^{\alpha+\beta-1}, Z_1 := 2N^{1/(r+1)}, Z_2 := 2N^{1/(r+1)}$. We also use a notation $Z = Z_1 = Z_2$ for simplicity.

These formulations and that for small secret exponent attacks in Section 5.1 are essentially the same when we use the Jochemsz-May strategy. That means the Newton polygons of polynomials $f_{PP.PKE.i}(x, y, z_1, z_2)$ and $f_{PP.PKE.i}(x, y, z_1, z_2)$ are the same, e.g., there are six monomials for variables $1, x, yz_1^{r-1}, yz_1^r, yz_1^{r-1}z_2$, and y. Hence, we use almost the same algorithm construction. We set an (possibly large) integer W such that $W < N^{\alpha+\beta}$ since $\|f_{PP.PKE.i}(xX, yY, z_1Z_1, z_2Z_2)\|_\infty \geq \max\{|1 - e\tilde{d}|, |eMX|\} \approx N^{\alpha+\beta}$. Next, we set an integer $R := W(XY)^{m-1} \cdot Z^{r(m-1-a+t)}$ with some integers $m = \omega(r)$ and $t = \tau m$ where $\tau \geq 0$ such that $\gcd(R, 1 - e\tilde{d}) = 1$. We compute $c = (1 - e\tilde{d})^{-1} \mod R$ and $f'_{PP.PKE.i}(x, y, z_1, z_2) := c \cdot f_{PP.PKE.i}(x, y, z_1, z_2) \mod R$. We define shift-polynomials $g_{PP.PKE.i}$ and $g'_{PP.PKE.i}$ as

$$g_{PP.PKE.i} : x^{i_X} y^{i_Y} z_1^{i_{Z_1}} z_2^{i_{Z_2}} \cdot f'_{PP.PKE.i} \cdot X^{m-1-i_X} Y^{m-1-i_Y} Z^{r(m-1-a+t)-i_{Z_1}-i_{Z_2}}$$
$$\text{for } x^{i_X} y^{i_Y} z_1^{i_{Z_1}} z_2^{i_{Z_2}} \in S,$$
$$g'_{PP.PKE.i} : x^{i_X} y^{i_Y} z_1^{i_{Z_1}} z_2^{i_{Z_2}} \cdot R \quad \text{for } x^{i_X} y^{i_Y} z_1^{i_{Z_1}} z_2^{i_{Z_2}} \in M \backslash S,$$

for sets of monomials S and M that are the same as in Section 5.1 where $f_{PP.SSE.i}$ is replaced by $f'_{PP.PKE.i}$. All these shift-polynomials $g_{PP.PKE.i}$ and $g'_{PP.PKE.i}$ modulo R have the roots $(x, y, z_1, z_2) = (-(d - \tilde{d}), \ell, -p, -q)$ that are the same as $f_{PP.PKE.i}(x, y, z_1, z_2)$. Hence, based on the Jochemsz-May strategy [JM06], LLL outputs short lattice vectors that satisfy Lemma 1 when the inequality (2) holds. For partial key exposure attacks (regardless of the MSBs or the LSBs are exposed), the inequality leads to

$$\begin{aligned} 0 < & -r(r+1)^2(\alpha+\beta) + r(r+1)(1-\delta)((r+1)+3r\tau) + r(r+1)^2 \\ & - 1 - 3r\eta(1+r\eta) - r^3(1-\eta+\tau)^3 + r^2(\eta-\tau)^3. \end{aligned}$$

To maximize the right hand side of the inequality, we set parameters $\eta = \frac{r(r+1)(1-\delta)-1}{2r}$ and $\tau = \eta - \frac{r-\sqrt{-r+(r+1)^2(1-\delta)}}{r+1}$ that results in the first condition

of Theorem 6. To satisfy the restriction $\eta \geq \tau$, the condition $\delta \geq \frac{1}{r+1}$ should hold. The condition results in $\alpha+\beta \leq \frac{3r^3+r^2+5r-1}{4r(r+1)}$. Notice that other restrictions $\tau \geq 0$ and $\eta \geq 0$ always hold.

For smaller $\alpha+\beta$, we use the other lattice construction that fully generalizes Ernst et al. However, the construction is essentially the same as previous one as we noted in the proof of Theorem 5. Indeed, we use the same shift-polynomials $g_{PP.PKE.i}$ and $g'_{PP.PKE.i}$ with the same sets of monomials S and M. The only difference is a restriction of parameters $\eta \leq \tau$. Hence, by definition, it follows that

$$
\begin{aligned}
x^{i_X} y^{i_y} z_1^{i_{Z_1}} z_2^{i_{Z_2}} \in S \Leftrightarrow\ & i_X = 0, 1, \ldots, m-a+t-1; \\
& i_Y = a-t, a-t+1, \ldots, m-1-i_X; \\
& i_{Z_1} = 0, 1, \ldots, r(i_Y - a + t); i_{Z_2} = 0, \text{ and} \\
& i_X = 0, 1, \ldots, m-1; i_Y = 0, 1, \ldots, m-1-i_X; \\
& i_{Z_1} = \max\{0, r - i_Y + r(i_{Z_2} - 1 - a)\}, \ldots, r-1; \\
& i_{Z_2} = a+1, a+2, \ldots, a + \lceil (i_Y+1)/r \rceil, \text{ and} \\
& i_X = 0, 1, \ldots, m-1; i_Y = 0, 1, \ldots, m-1-i_X; \\
& i_{Z_1} = 0, 1, \ldots, r-1; \\
& i_{Z_2} = \max\{0, -i_Y + a - t\}, \ldots, a, \\
x^{i_X} y^{i_y} z_1^{i_{Z_1}} z_2^{i_{Z_2}} \in M \Leftrightarrow\ & i_X = 0, 1, \ldots, m-a+t; \\
& i_Y = a-t, a-t+1, \ldots, m-i_X; \\
& i_{Z_1} = 0, 1, \ldots, r(i_Y - a + t); i_{Z_2} = 0, \\
& i_X = 0, 1, \ldots, m; i_Y = 0, 1, \ldots, m-i_X; \\
& i_{Z_1} = \max\{0, r - i_Y + r(i_{Z_2} - 1 - a)\}, \ldots, r-1; \\
& i_{Z_2} = a+1, a+2, \ldots, a + \lceil (i_Y+1)/r \rceil, \text{ and} \\
& i_X = 0, 1, \ldots, m; i_Y = 0, 1, \ldots, m-i_X; \\
& i_{Z_1} = 0, 1, \ldots, r-1; \\
& i_{Z_2} = \max\{0, -i_Y + a - t\}, \ldots, a.
\end{aligned}
$$

All these shift-polynomials $g_{PP.PKE.i}$ and $g'_{PP.PKE.i}$ modulo R have the roots $(x, y, z_1, z_2) = (-d, \ell, -p, -q)$ that are the same as $f_{PP.PKE.i}(x, y, z_1, z_2)$. We replace each occurrence of $z_1^r z_2$ by N and construct a lattice with coefficients of $g_{PP.PKE.i}(xX, yY, z_1 Z_1, z_2 Z_2)$ and $g'_{PP.SSE.i}(xX, yY, z_1 Z_1, z_2 Z_2)$ as the bases. The shift-polynomials generate a triangular basis matrix.

Ignoring low order terms of m, based on the Jochemsz-May strategy [JM06], LLL outputs short vectors that satisfy Lemma 1 when

$$
X^{\left(\frac{r+1}{6}+\frac{r}{2}\tau\right)m^3} Y^{\left(\frac{r+1}{3}+\frac{r}{2}\tau\right)m^3} Z_1^{\left(\frac{r^2(1+\tau-\eta)^3}{6} - \frac{r^2(\tau-\eta)^3}{6}\right)m^3} Z_2^{\left(\frac{1}{6r}+\frac{1}{2}\eta+\frac{r}{2}\eta^2\right)m^3} < W^{\left(\frac{r+1}{6}+\frac{r}{2}\tau\right)m^3}
$$

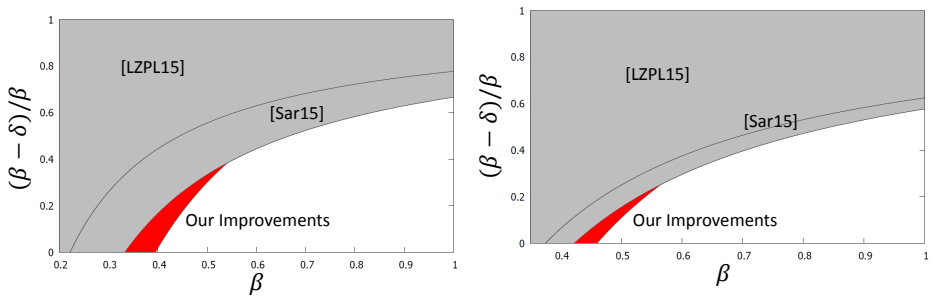

Fig. 3. Comparisons of partial key exposure attacks on the prime power RSA when the MSBs are exposed for $\alpha = 1$. We compare how much portions of d should be exposed for β between the attack of Lu et al. [LZPL15], Sarkar [Sar15], and our Theorem 6. The left figure is for $r = 2$ and the right figure is for $r = 3$.

that leads to

$$0 < -(r+1)^2(\alpha+\beta) + (2(r+1)^2 + 3r(r+1)\tau) - \delta((r+1)^2 + 3r(r+1)\tau) \\ - r^2(1+\tau-\eta)^3 + r^2(\tau-\eta)^3 - \frac{1}{r} - 3\eta - 3r\eta^2.$$

To maximize the right hand side of the inequality, we set parameters $\eta = \frac{r(r+1)(1-\delta)-1}{2r}$ and $\tau = \eta + \frac{(r+1)(1-\delta)-r}{2r}$ and the condition becomes

$$\delta < 1 - \frac{r + \sqrt{12r^2(r+1)(\alpha+\beta) - r(9r^2+14r-3)}}{3r(r+1)}$$

as required. To satisfy the restriction $\eta \leq \tau$, the condition $\delta \leq \frac{1}{r+1}$ should hold. The condition results in $\frac{3r^3+r^2+5r-1}{4r(r+1)} \leq \alpha + \beta$. Notice that other restrictions $\tau \geq 0$ and $\eta \geq 0$ always hold. □

When the MSBs are exposed, our attack is better than that of Sarkar when $\alpha+\beta$ is small and is better than that of Lu et al. when r is small. Figure 3 compare Theorem 6 and those of Lu et al. and Sarkar for $r = 2$ and 3. Our attack is the better for small β, e.g., our attack works with less partial information.

In Section 6.2, we propose an improved attack with the LSBs. However, it seems that our Theorem 6 with the exposed MSBs also has room for improvements. As opposed to the Takagi RSA, and as the standard RSA, we can compute the MSBs of ℓ since we know the MSBs of $p^{r-1}(p-1)(q-1)$. Indeed, the result of Sarkar makes use of the fact and generalize the other attack of Ernst et al. In addition, there exists better attacks by Takayasu and Kunihiro for small β. To generalize the attack to the prime power RSA remains as a future work.

6 Attacks on the Prime Power RSA by Solving Modular Equations

In this section, we analyze the security of prime power RSA by solving modular equations. In Section 6.1, we propose a small secret exponent attack that (almost) fully generalizes the stronger Boneh-Durfee result [BD00]. In Section 6.2, we propose a partial key exposure attack that (almost) fully generalizes Takayasu and Kunihiro's result [TK14].

6.1 Small Secret Exponent Attack

In this section, we propose small secret exponent attacks on the prime power RSA that satisfy the following property.

Theorem 7 *Let $N = p^r q$ be a public modulus and let $e \approx N^\alpha$ and $d \approx N^\beta$ be public exponent and secret exponent of prime power RSA, respectively. If*

$$\beta < 1 - \frac{-r + \sqrt{4r(r+1) + 4r^2(3r+4)(r+1)^2\alpha}}{r(3r+4)(r+1)} \text{ for}$$
$$\alpha \geq \frac{9(r+1)^2}{(r+2)^2(3r+4)} - \frac{1}{r(r+1)(3r+4)}, \text{ or}$$
$$\beta < \frac{7r^2 + 17r + 9 - \sqrt{36r^4 + 204r^3 + 376r^2 + 292r + 84 + 4r(r+1)^2(r+3)\alpha}}{r(r+1)}$$
$$\text{for } \alpha > \frac{-4r^2 - 8r - 3 + 2\sqrt{(r+1)(4r^3 + 15r^2 + 10r + 3)}}{r(r+1)}$$

holds, then prime power RSA modulus N can be factorized in polynomial time.

The result (almost) fully generalizes the stronger Boneh-Durfee [BD00] in the sense that it is better than the weaker Boneh-Durfee and weaker than the stronger Boneh-Durfee for $r = 1$, i.e., $\beta < (15 - 2\sqrt{30})/14 = 0.28896\cdots$. Since the results of Theorem 7 are better than those of Theorem 5, they are outperforming the Jochemsz-May.

Proof of Theorem 7. Looking at a key generation for the prime power RSA; $ed = 1 + \ell p^{r-1}(p-1)(q-1)$ with some integer $|\ell| \approx N^{\alpha+\beta-1}$. To recover the secret exponent d, we use the following polynomial

$$f_{PP.SSE.m}(x, y_1, y_2) = 1 + xy_1^{r-1}(y_1 - 1)(y_2 - 1).$$

The polynomial modulo e has roots $(x, y_1, y_2) = (\ell, p, q)$. The absolute values are bounded by $X := N^{\alpha+\beta-1}, Y_1 = Y_2 := 2N^{1/(r+1)}$. Let $m = \omega(r)$ and $a = \eta m$ be integers. To solve a modular equation $f_{PP.SSE.m}(x, y_1, y_2) = 0 \mod e$, we use shift-polynomials

$$g_{PP.SSE.m}(x, y_1, y_2) = x^{i_X} y_1^{i_{Y_1}} y_2^{a+i_{Y_2}} f_{PP.SSE.m}^u(x, y_1, y_2) e^{m-u}$$

with indices in

$$\begin{aligned}
\mathcal{I}_{x1} &\Leftrightarrow\ u = 0, 1, \ldots, m; i_X = 0, 1, \ldots, m-u; i_{Y_1} = 0, 1, \ldots, r-1; i_{Y_2} = 0,\\
\mathcal{I}_{x2} &\Leftrightarrow\ u = 0, 1, \ldots, m; i_X = 0, 1, \ldots, m-u; i_{Y_1} = r-1; i_{Y_2} = 1,\\
\mathcal{I}_{y} &\Leftrightarrow\ u = 0, 1, \ldots, m; i_X = 0; i_{Y_1} = 1, 2, \ldots, \lfloor (1-(r+1)\beta)u \rfloor + ra; i_{Y_2} = 0.
\end{aligned}$$

All these shift-polynomials $g_{PP.SSE.m}$ modulo e^m have the roots $(x, y_1, y_2) = (\ell, -p, -q)$ that are the same as $f_{PP.sse.m}(x, y_1, y_2)$. We replace each occurrence of $y_1^r y_2$ by N and construct a lattice with coefficients of $g_{PP.SSE.m}(xX, y_1Y_1, y_2Y_2)$ as the bases.

As in the proof of Theorem 5, the shift-polynomials $g_{PP.SSE.m}$ with indices in $\mathcal{I}_{x1}$ for $i_{Y_1} = 0, 1, \ldots, r-1$ and $\mathcal{I}_{x2}$ play the same role as x-shifts of the stronger Boneh-Durfee by a factor of $(r+1)$. Although $g_{PP.SSE.m}$ with indices in $\mathcal{I}_y$ plays the same role as y-shifts of the stronger Boneh-Durfee by a factor of r since i_{Y_1} is upper bounded by $\lfloor (1-(r+1)\beta)u \rfloor + ra$ that depends on u. However, there are no additional y-shifts which play the same role as the stronger Boneh-Durfee. Notice that all polynomials are multiplied by y_2^a and the operation plays the same role as the y-shifts of the weaker Boneh-Durfee. Hence, our Theorem 7 (almost) fully generalizes the stronger Boneh-Durfee and is always better than Theorem 5. We do not know how to fully generalize the stronger Boneh-Durfee and we think there may be room for improvements.

Assume that $\lfloor (1-(r+1)\beta)u \rfloor + ra \geq 0$, e.g., $\eta \geq ((r+1)\beta - 1)/r$, and the shift-polynomials generate triangular basis matrix with diagonals

- $X^{u+i_X} Y_1^{\max\{0, r(u-a)+i_{Y_1}\}} Y_2^{\max\{a-\lfloor u+i_{Y_1}/r \rfloor, 0\}} e^{m-u}$ for indices in $\mathcal{I}_{x1}$,
- $X^{u+i_X} Y_2^{a+\lceil (u+1)/r \rceil} e^{m-u}$ for indices in $\mathcal{I}_{x2}$,
- $X^u Y_1^{ru+i_{Y_1}} e^{m-u}$ for indices in $\mathcal{I}_y$.

In $\mathcal{I}_y$, i_{Y_1} is upper bounded by $\lfloor (1-(r+1)\beta)u \rfloor + ra$. The definition follows from the fact that the shift-polynomials reduce norms of outputs by the LLL algorithm, e.g., the diagonals for the shift-polynomials are smaller than e^m.

Ignoring low order terms of m, the LLL algorithm outputs short lattice vectors that satisfy Lemma 1 when $(\det(L))^{1/n} < e^m$ that leads to

$$\begin{aligned}
0 < &- r(r+1)^2\alpha - 1 - 3r\eta(1+r\eta)\\
&+ r(r+1)(2+3r\eta)(1-\delta) + r(r+1)^2(1-\delta)^2.
\end{aligned}$$

To maximize the right hand side of the inequality, we set the parameter $\eta = \frac{r(r+1)(1-\beta)-1}{2r}$ and the condition becomes

$$\beta < 1 - \frac{-r + \sqrt{4r(r+1) + 4r^2(3r+4)(r+1)^2\alpha}}{r(3r+4)(r+1)}$$

as required. To satisfy the restriction $\eta \geq ((r+1)\beta - 1)/r$, the condition $\beta < \frac{r(r+1)+1}{(r+2)(r+1)}$ should hold. The condition results in $\frac{9(r+1)^2}{(r+2)^2(3r+4)} - \frac{1}{r(r+1)(3r+4)} \leq \alpha$.

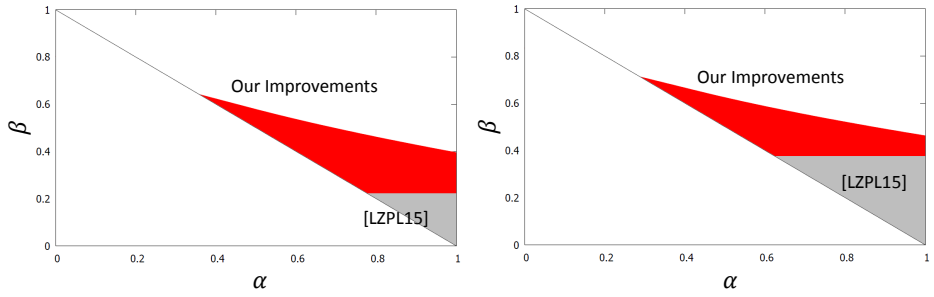

Fig. 4. Comparisons of small secret exponent attacks on the prime power RSA. We compare recoverable values β for α between the attack of Lu et al. [LZPL15] and our Theorem 7. The left figure is for $r = 2$ and the right figure is for $r = 3$.

For smaller α, we propose an alternative lattice construction. We use the same shift-polynomials $g_{PP.SSE.m}(x, y_1, y_2)$ with indices in

$$\begin{aligned}
\mathcal{I}_{x1} &\Leftrightarrow\ u = 0, 1, \ldots, m; i_X = 0, 1, \ldots, m - u; i_{Y_1} = 0, 1, \ldots, r - 1; i_{Y_2} = 0, \\
\mathcal{I}_{x2} &\Leftrightarrow\ u = 0, 1, \ldots, m; i_X = 0, 1, \ldots, m - u; i_{Y_1} = r - 1; i_{Y_2} = 1, \\
\mathcal{I}'_y &\Leftrightarrow\ u = 0, 1, \ldots, m; i_X = 0; i_{Y_1} = 1, 2, \ldots, \lfloor r(a - \eta u) \rfloor; i_{Y_2} = 0.
\end{aligned}$$

We replace each occurrence of $y_1^r y_2$ by N and construct a lattice with coefficients of $g_{PP.SSE.m}(xX, y_1Y_1, y_2Y_2)$ as the bases. Assume $0 \leq \eta$ and the shift-polynomials generate a triangular basis matrix with the same diagonals as previous ones.

As previous cases, we should define $\mathcal{I}'_y$ such that the shift-polynomials reduce norms of outputs by the LLL algorithm, e.g., the diagonals for the shift-polynomials are smaller than e^m. However, that is not the case and the definition is a suboptimal. Therefore, we think there may be room for improvements.

Ignoring low order terms of m, the LLL algorithm outputs short vectors that satisfy Lemma 1 when $(\det(L))^{1/n} < e^m$ that leads to

$$0 < -r(r+1)^2\alpha + r(1-\beta)\left(2(r+1)^2 + r(r+1)\eta\right) - r^3(1-\eta)^2 - 1 - 3r\eta(1 + r\eta).$$

To maximize the right hand side of the inequality, we set the parameter $\eta = \frac{r(r+1)(1-\beta)+2r^2-3}{2r^2+6r}$ and the condition becomes

$$\beta < \frac{7r^2 + 17r + 9 - \sqrt{36r^4 + 204r^3 + 376r^2 + 292r + 84 + 4r(r+1)^2(r+3)\alpha}}{r(r+1)}$$

as required. To satisfy $\alpha + \beta > 1$, the condition $\alpha > \frac{-4r^2-8r-3+2\sqrt{(r+1)(4r^3+15r^2+10r+3)}}{r(r+1)}$ should hold. The restriction $\eta \geq 0$ always holds. □

Table 1. Comparisons of small secret exponent attacks on the prime power RSA. We compare recoverable values β for α between the attack of Lu et al. [LZPL15], our Theorem 5, and Theorem 7. The left table is for $r = 5$ and the right table is for $r = 6$.

α	[LZPL15]	Theorem 5	Theorem 7
1	0.5555	0.5442	0.5495
0.9	0.5555	0.5670	0.5730
0.8	0.5555	0.5911	0.5979
0.7	0.5555	0.6167	0.6244
0.6	0.5555	0.6442	0.6528
0.5	0.5555	0.6741	0.6837
0.4	–	0.7073	0.7179
0.3	–	0.7452	0.7561

α	[LZPL15]	Theorem 5	Theorem 7
1	0.6122	0.5738	0.5798
0.9	0.6122	0.5950	0.6017
0.8	0.6122	0.6174	0.6248
0.7	0.6122	0.6412	0.6494
0.6	0.6122	0.6668	0.6759
0.5	0.6122	0.6946	0.7046
0.4	0.6122	0.7254	0.7364
0.3	–	0.7607	0.7724
0.2	–	0.8036	0.8106

Since Theorem 7 works when $\alpha > \frac{-4r^2-8r-3+2\sqrt{(r+1)(4r^3+15r^2+10r+3)}}{r(r+1)}$, it works for smaller α than Theorem 5. Indeed, Theorem 7 is (although slightly) always better than Theorem 5. Figure 4 compare Theorem 7 and Lu et al. for $r = 2$ and 3. Theorem 7 is the better for all α and the differences become larger for smaller α. Moreover, Table 1 compare Lu et al., Theorem 5, and Theorem 7 for $r = 5$ and 6. When $\alpha = 1$, Lu et al. is the best. However, our attack becomes the better for smaller α.

6.2 Partial Key Exposure Attack

In this section, we propose small secret exponent attacks on the prime power RSA that satisfy the following property.

Theorem 8 *Let $N = p^r q$ be a public modulus and let $e \approx N^\alpha$ and $d \approx N^\beta$ be public exponent and secret exponent of prime power RSA, respectively. When $(\beta - \delta)\log N$ bits of the least significant bits are exposed, if*

$$\delta < 1 - \frac{r(2r+1) + 2\sqrt{r(r+1)(r(r+1)(3r+4)(\alpha+\beta) - 3r^3 - 6r^2 - 4r + 1)}}{r(r+1)(3r+4)}$$
$$\text{for } \frac{30r^3 + 51r^2 + 25r - 4}{4r(r+1)(3r+4)} \leq \alpha + \beta$$

holds, then prime power RSA modulus N can be factorized in polynomial time.

As Theorem 7, the result (only almost) fully generalizes Takayasu and Kunihiro's attack. However, the result is better than Theorem 6 with the exposed LSBs.

Proof of Theorem 8. Looking at a key generation for prime power RSA with the exposed LSBs; $e(d_1M + d_0) = 1 + \ell p^{r-1}(p-1)(q-1)$ with some integer $|\ell| \approx N^{\alpha+\beta-1}$. To recover the unknown MSBs of the secret exponent d_1, we use the following polynomials

$$f_{PP.PKE.m}(x, y_1, y_2) = 1 - ed_0 + xy_1^{r-1}(y_1 - 1)(y_2 - 1)$$

whose roots modulo e are $(x, y_1, y_2) = (\ell, p, q)$.

To solve a modular equation $f_{PP.PKE.m}(x, y_1, y_2) = 0 \mod e$, we use the following shift-polynomials

$$g_{PP.PKE.m}(x, y_1, y_2) = x^{i_X} y_1^{i_{Y_1}} y_2^{a+i_{Y_2}} f^u_{PP.SSE.m}(x, y_1, y_2)(eM)^{m-u}$$

with indices in

$$\begin{aligned}
\mathcal{I}_{x1} &\Leftrightarrow\ u = 0, 1, \ldots, m; i_X = 0, 1, \ldots, m-u; i_{Y_1} = 0, 1, \ldots, r-1; i_{Y_2} = 0,\\
\mathcal{I}_{x2} &\Leftrightarrow\ u = 0, 1, \ldots, m; i_X = 0, 1, \ldots, m-u; i_{Y_1} = r-1; i_{Y_2} = 1,\\
\mathcal{I}_{y} &\Leftrightarrow\ u = 0, 1, \ldots, m; i_X = 0; i_{Y_1} = 1, 2, \ldots, \lfloor ((r+1)(1-\delta) - 1)u \rfloor + ra; i_{Y_2} = 0.
\end{aligned}$$

All these shift-polynomials modulo $(eM)^m$ have roots $(x, y_1, y_2) = (\ell, p, q)$ that are the same as $g_{PP.PKE.m}$. We replace each occurrence of $y_1^r y_2$ by N and construct a lattice with coefficients of $g_{PP.PKE.m}(xX, y_1Y_1, y_2Y_2)$ as the bases. The shift-polynomials generate a triangular basis matrix with diagonals

- $X^{u+i_X} Y_1^{\max\{0, r(u-a)+i_{Y_1}\}} Y_2^{\max\{a-\lfloor u+i_{Y_1}/r \rfloor, 0\}} (eM)^{m-u}$ with indices in $\mathcal{I}_{x1}$,
- $X^{u+i_X} Y_2^{a+\lceil (u+1)/r \rceil} (eM)^{m-u}$ with indices in $\mathcal{I}_{x2}$,
- $X^u Y_1^{ru+i_{Y_1}} (eM)^{m-u}$ with indices in $\mathcal{I}_y$.

In $\mathcal{I}_y$, i_{Y_1} is upper bounded by $\lfloor ((r+1)(1-\delta) - 1)u \rfloor + ra$. The definition follows from the fact that the shift-polynomials reduce norms of outputs by the LLL algorithm, e.g., the diagonals for the shift-polynomials are smaller than the modulus $(eM)^m$.

Ignoring low order terms of m, the LLL algorithm outputs short vectors that satisfy Lemma 1 when $(\det(L))^{1/n} < (eM)^m$ that leads to

$$\begin{aligned}
0 <& -r(r+1)^2(\alpha+\beta-1) - 1 - 3r\eta(1+r\eta)\\
&- r(r+1)(r-1-3r\eta)(1-\delta) + r(r+1)^2(1-\delta)^2.
\end{aligned}$$

To maximize the right hand side of the inequality, we set the parameter $\eta = \frac{r(r+1)(1-\delta)-1}{2r}$ and the condition becomes

$$\delta < 1 - \frac{r(2r+1) + 2\sqrt{r(r+1)(r(r+1)(3r+4)(\alpha+\beta) - 3r^3 - 6r^2 - 4r + 1)}}{r(r+1)(3r+4)}$$

as required. To satisfy the restriction $\eta \geq 0$, $\delta \leq 1 - \frac{1}{r(r+1)}$ should hold. The condition results in $\frac{30r^3+51r^2+25r-4}{4r(r+1)(3r+4)} \leq \alpha + \beta$. □

When the LSBs are exposed, our attack is better than that of Lu et al. when r is small. Figure 5 compare Theorem 8 and Lu et al. for $r = 2$ and 3. Our attack is the better for all β, e.g., our attack works with less partial information.

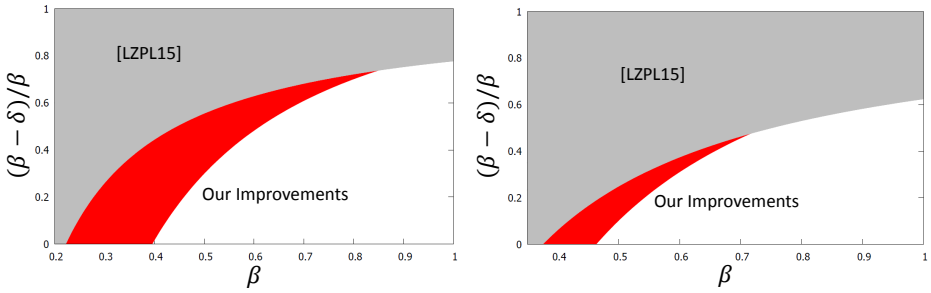

Fig. 5. Comparisons of partial key exposure attacks on the prime power RSA for $\alpha = 1$ when the least significant bits are exposed. We compare how much portions of d should be exposed for β between the attack of Lu et al. [LZPL15] and our Theorem 8. The left figure is for $r = 2$ and the right figure is for $r = 3$.

Acknowledgement. We would like to thank Shuichi Katsumata for their helpful comments. The first author is supported by a JSPS Fellowship for Young Scientists. This research was supported by CREST, JST and supported by JSPS KAKENHI Grant Number 25280001 and 26·8237.

References

[BD00] D. Boneh, G. Durfee, "Cryptanalysis of RSA with private key d less than $N^{0.292}$," IEEE Trans. Inf. Theory, vol. 46, no. 4, pp. 1339–1349, 2000. Proc. Eurocrypt 1999, LNCS 1592, pp. 1–11, Springer, 1999,

[BDH99] D. Boneh, G. Durfee, and N. Howgrave-Graham, "Factoring $N = p^r q$ for large r," Proc. Crypto 1999, LNCS 1666, pp. 326–337, Springer, 1999.

[BM03] J. Blömer, A. May, "New partial key exposure attacks on RSA," Proc. Crypto 2003, LNCS 2729, pp. 27–43, Springer, 2003.

[Cop96a] D. Coppersmith, "Finding a small root of a univariate modular equation," Proc. Eurocrypt 1996, LNCS 1070, pp. 155–165, Springer, 1996.

[Cop96b] D. Coppersmith, "Finding a small root of a bivariate integer equation: Factoring with high bits known," Proc. Eurocrypt 1996, LNCS 1070, pp. 178–189, Springer, 1996.

[Cop97] D. Coppersmith, "Small solutions to polynomial equations, and low exponent RSA vulnerabilities," J. Cryptology, vol. 10, no. 4, pages 233–260, 1997.

[Cop01] D. Coppersmith, "Finding small solutions to small degree polynomials," Proc. CaLC2001, LNCS 2146, pp. 20–31, Springer, 2001.

[Cor04] J. -S. Coron, "Finding small roots of bivariate integer equations revisited," Proc. Eurocrypt 2004, LNCS 3027, pp. 492–505, Springer, 2004.

[Cor07] J. -S. Coron, "Finding small roots of bivariate integer equations: A direct approach," Proc. Crypto 2007, LNCS 4622, pp. 379–394, Springer, 2007.

[EJMW05] M. Ernst, E. Jochemsz, A. May, B. Weger, "Partial key exposure attacks on RSA up to full size exponents," Proc. Eurocrypt 2005, LNCS 3494, pp. 371–386, Springer, 2005.

[HM09] M. Herrmann, A. May, "Attacking power generators using unravelled linearization: When do we output too much?," Proc. Asiacrypt 2009, LNCS 5912, pp. 487–504, Springer, 2009.

[HM10] M. Herrmann and A. May, "Maximizing small root bounds by linearization and applications to small secret exponent RSA," Proc. PKC 2010, LNCS 6056, pp. 53–69, Spriner, 2010.

[How97] N. Howgrave-Graham, "Finding small roots of univariate modular equations revisited," Proc. Cryptography and Coding, LNCS 1355, pp. 1331–142, Springer, 1997.

[HHX+14] Z. Huang, L. Hu, J. Xu, L. Peng, and Y. Xie, "Partial key exposure attacks on Takagi's variant of RSA," Proc. ACNS 2014, LNCS 8479, pp. 134–150, Springer, 2014.

[IKK08] K. Itoh, N. Kunihiro, K. Kurosawa, "Small secret exponent attack on a variant of RSA (due to Takagi)," Proc. CT-RSA 2008, LNCS 4964, pp. 387–406, Springer, 2008.

[JM06] E. Jochemsz and A. May, "A strategy for finding roots of multivariate polynomials with new applications in attacking RSA variants," Proc. Asiacrypt 2006, LNCS 4284, pp. 267–282, Springer, 2006.

[Len87] H. W. Lenstra, "Factoring integers with elliptic curves," Annals of Mathematics, 126:649–673, 1987

[LLL82] A. K. Lenstra, H. W. Lenstra, L. Lovasz. "Factoring polynomials with rational coefficients," Mathematische Annalen 261, pp.515–534, 1982.

[LZPL15] Y. Lu, R. Zhang, L. Peng, and D. Lin, "Solving linear equations modulo unknown divisors: Revisited," Proc. Asiacrypt 2015, LNCS 9452, pp. 189–213, Springer, 2015.

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

[May04] A. May, "Secret exponent attacks on RSA-type schemes with moduli $N = p^r q$," Proc. PKC 2004, LNCS 2947, pp. 218–230, Springer, 2004.

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

[NS01] P. Q. Nguyen and J. Stern, "The two faces of lattices in cryptology," Proc. CaLC 2001, LNCS 2146, pp. 146–180, Springer, 2001.

[RSA78] R. L. Rivest, A. Shamir, L. M. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Communications of the ACM, 21 (2), pp. 120–126, 1978.

[Sar14] S. Sarkar, "Small secret exponent attack on RSA variant with modulus $N = p^r q$," Designs, Codes and Cryptography, pp. 1–10, 2014.

[Sar15] S. Sarkar, "Revisiting prime power RSA," Available from IACR Cryptology ePrint Archive, Report 2015/774, 2015.

[SGM10] S. Sarkar, S. Sen Gupta and S. Maitra, "Partial key exposure attack on RSA - Improvements for limited lattice dimensions," Proc. Indocrypt 2010, LNCS , pp. 2–16, Springer, 2010.

[Tak98] T. Takagi, "Fast RSA-type cryptosystem modulo $p^k q$," Proc. Crypto 1998, LNCS 1462, pp. 318–326, Springer, 1998.

[TK14] A. Takayasu and N. Kunihiro, "Partial key exposure attacks on RSA: Achieving the Boneh-Durfee bound," Proc. SAC 2014, LNCS, pp. 345–362, Springer, 2014.

[Wie90] M. J. Wiener, "Cryptanalysis of short RSA secret exponents," IEEE Trans. inf. theory, vol. 36, (3), pp. 553–558, 1990.