Small CRT-Exponent RSA Revisited

Atsushi Takayasu[1,2], Yao Lu[1], and Liqiang Peng[3]

[1] The University of Tokyo, Japan,
[2] National Institute of Advanced Industrial Science and Technology (AIST), Japan,
[3] State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, China
a-takayasu@it.k.u-tokyo.ac.jp

Abstract. Since May (Crypto'02) revealed the vulnerability of the small CRT-exponent RSA using Coppersmith's lattice-based method, several papers have studied the problem and two major improvements have been made. Bleichenbacher and May (PKC'06) proposed an attack for small d_q when the prime factor p is significantly smaller than the other prime factor q; the attack works for $p < N^{0.468}$. Jochemsz and May (Crypto'07) proposed an attack for small d_p and d_q where the prime factors p and q are balanced; the attack works for $d_p, d_q < N^{0.073}$. Even after a decade has passed since their proposals, the above two attacks are still considered to be the state-of-the-art, and no improvements have been made thus far. A novel technique seems to be required for further improvements since the attacks have been studied with all the applicable techniques for Coppersmith's methods proposed by Durfee-Nguyen (Asiacrypt'00), Jochemsz-May (Asiacrypt'06), and Herrmann-May (Asiacrypt'09, PKC'10). In this paper, we propose two improved attacks on the small CRT-exponent RSA: a small d_q attack for $p < N^{0.5}$ (an improvement of Bleichenbacher-May's) and a small d_p and d_q attack for $d_p, d_q < N^{0.091}$ (an improvement of Jochemsz-May's). We use Coppersmith's lattice-based method to solve modular equations and obtain the improvements from a novel lattice construction by exploiting useful algebraic structures of the CRT-RSA key generation. We explicitly show proofs of our attacks and verify the validities by computer experiments. In addition to the two main attacks, we propose small d_q attacks on several variants of RSA.

Keywords: CRT-RSA, cryptanalysis, Coppersmith's method, lattices, LLL algorithm

1 Introduction

1.1 Background

Let $N = pq$ be a public RSA modulus whose prime factors p and q are usually the same bit-size. A public exponent e and a secret exponent d satisfy $ed = 1 \mod (p-1)(q-1)$. For encryption/verifying (resp. decryption/signing), the heavy

modular exponentiation of e (resp. d) has to be computed. To achieve faster computation, a simple solution is to use a small public or secret exponent. However, Wiener [50] showed that a public RSA modulus is factorized in polynomial time when the secret exponent is too small such that $d < N^{0.25}$. Boneh and Durfee [5] revisited the problem with Coppersmith's lattice-based method [8,18] and improved the bound to $d < N^{0.284}$. Furthermore, in the same work, the bound was improved to $d < N^{0.292}$ by exploiting sublattice structures from the previous one although the proof is involved.

To simultaneously thwart the small secret exponent attack and achieve faster decryption/signing, the Chinese Remainder Theorem (CRT) is often used as described by Quisquater and Couvreur [35]. Instead of the original secret exponent d, there are CRT-exponents d_p and d_q that satisfy

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

Then a natural question to ask is whether there exist analogous attacks of the Boneh-Durfee [5] to the small CRT-exponents. The first answer was given by May (Crypto'02) [29]. May analyzed the unbalanced RSA whose prime factor p is significantly smaller than the other prime factor q, and proposed an attack for a small d_q with an arbitrary large d_p. The paper contains two attacks where the former attack works for $p < N^{0.382}$. The latter attack works only for smaller p, however, is better than the former attack for $p < N^{0.23}$ in the sense that a larger d_q can be recovered. Since May's attack works only in the unbalanced setting, it is an interesting open question if the attacks can be improved to cover the balanced RSA.

Subsequently, several improved attacks on the small CRT-exponent RSA have been proposed. Bleichenbacher and May (PKC'06) [3] revisited May's work [29] in the same attack scenario and proposed an improved attack. The attack works for a larger p such that $p < N^{0.468}$, and recovers a larger d_q than May's attack for any size of p. However, the balanced prime factors still could not be captured. To capture the balanced RSA, Bleichenbacher and May analyzed other attack scenarios where both d_p and d_q are small in the same work. They proposed an attack which works for $e < N$. Although the same situation was already studied by Galbraith et al. [14], Sun and Wu [40], their attacks only work for a smaller e. Jochemsz and May (Crypto'07) [22] proposed the first attack that works for a full size e when $d_p, d_q < N^{0.073}$.

In the past decade, no improved attacks of Bleichenbacher-May [3] and Jochemsz-May [22] have been proposed. Hence, following these attacks seems to be the best way to study the security of the CRT-RSA. Indeed, until recently, several papers followed the attacks and reported the vulnerabilities of the CRT-RSA, e.g., an attack on Takagi's RSA [39], an attack on the RSA with multiple exponent pairs [34], and partial key exposure attacks [4,27,38,45,47].

1.2 Technical Hardness

Coppersmith introduced two lattice-based methods; to solve a modular equation [8] and an integer equation [7]. May's attack and Bleichenbacher-May's

attack used the former method whereas Jochemsz-May's attack used the latter method. Both methods first construct a lattice and then solve equations with a small root in polynomial time. In this research area, constructing better attacks is equivalent to designing better lattices that reflect the more useful algebraic structure of the equation. For the purpose, several useful strategies and techniques for lattice constructions have been introduced thus far. Currently best known small CRT-exponent attacks [3,22,29] are based on the state-of-the-art lattice constructions; the Durfee-Nguyen technique (Asiacrypt'00) [12] and the Jochemsz-May strategy (Asiacrypt'06) [21]. Since the Durfee-Nguyen technique is useful to handle the relation $N = pq$ and the Jochemsz-May construction yields good lattices for arbitrary polynomials, these approaches [3,29] seem appropriate to study the attack. Moreover, to the best of our knowledge, there remained no useful strategies to analyze the attack scenarios at that time. After the proposals of [3,22,29], a new technique called unravelled linearization was introduced by Herrmann and May (Asiacrypt'09) [16]. The technique has been used to study various attack scenarios on RSA, e.g., [2,15,17,19,23,24,42,43,44,46,48,49], and drastically developed the research area. For example, Herrmann and May [17] showed an elementary proof of Boneh-Durfee's attack [5] to exploit the sublattice structures. However, unfortunately, unravelled linearization could not improve small CRT-exponent attacks. Although Herrmann and May (PKC'10) [17] tried to exploit sublattice structures, they could not obtain better asymptotic bounds. Therefore, to obtain better bounds, a novel technique seems to be developed.

1.3 Our Results

In this paper, we develop a novel lattice construction technique for Coppersmith's modular method where the technique enables us to exploit more useful algebraic structures of the CRT-RSA key generation. A basic application of the technique is an improved small d_q attack for unbalanced prime factors (Section 3). As opposed to the previous results by May [29] and Bleichenbacher-May [3], our attack is the first result to reach a meaningful bound, i.e., $p < N^{0.5}$. Hence, we solve one of the major open problems for the security of the small CRT-exponent RSA. Moreover, our attack can recover a larger d_q than [3,29] for any size of p. In addition, our attack requires less lattice dimensions than Bleichenbacher-May's attack [3] since our technique exploits sublattice structures from [3]'s lattice where the approach is similar to Boneh-Durfee [5]. Indeed, our experiments show that Bleichenbacher-May's attack works better than their theoretical analyses.

We claim that our technique is not limited to the small d_q attack. The technique is also applicable to a small d_p and d_q attack (Section 4) that improves Jochemsz-May's attack [22]. As we mentioned, small d_q attacks [3,29] and small d_p and d_q attacks [22] were studied with different approaches in previous works; the former attack used Coppersmith's modular method whereas the latter attack used Coppersmith's integer method. However, our powerful technique enables us to improve these attacks in the same manner. Our attack[4] works for

[4] In the full version, we further improve the bound to $d_p, d_q < N^{0.122}$.

$d_p, d_q < N^{0.091}$ with a full size e where the exponent of N is about 25% larger than Jochemsz-May's attack.

Recently, numerous papers [13,20,26,28,33,34,36,37,39,42,46,48] have been studying the security of RSA variants. We further show that we can extend our small d_q attack to the RSA variants (Section 5), i.e., the Multi-Prime RSA, Takagi's RSA, and the RSA with multiple exponent pairs. Our attacks significantly improve previous attacks on these variants [34,39].

1.4 Key Technique

We show an overview of our technique. The CRT-RSA key generation for d_q is written as

$$ed_q = 1 + k(q-1) \tag{1}$$

with some integer k. By multiplying the equation by p, we obtain

$$ed_q p = p + k(N-p) = N + (k-1)(N-p). \tag{2}$$

Recall in May's and Bleichenbacher-May's attack scenario [3,29], the prime p is significantly smaller than the other prime q. They solved the latter equation (2) modulo e to recover unknown $(k-1, p)$. Since the prime p is significantly smaller than the other prime q, to construct better attacks, solving the equation (2) is more promising approach than solving the equation (1) to recover (k, q). Hence, only the equation (2) was used in previous attacks. However, it means that the constructions of previous attacks significantly rely on the fact that p is much smaller than q. As a result, these attacks do not work when p is close to $N^{0.5}$.

What we focus on is a fact that the equations (1) and (2) are essentially the same; there are two representations for the same CRT-RSA key generation. As opposed to previous works, our improved lattice constructions utilize the algebraic structure of both equations (1) and (2) simultaneously not only the equation (2). The two representations are compatible in the sense that the combination enables us to exploit more useful algebraic structures. More specifically, we use the equations (1) and (2) where the proportion can be adaptively determined by the sizes of p and q. Then, to solve the modulo e equation as previous works, our framework always yields the better lattices than previous approaches. Our attacks are better than Bleichenbacher-May's attack for any size of p.

At a glance, our lattice construction technique is specialized to the improvement of Bleichenbacher-May's attack. As we pointed out, May's attack and Bleichenbacher-May's attack used Coppersmith's method to solve a modular equation [8,18] whereas Jochemsz-May's attack used the method to solve an integer equation [7,11]. The modular equation for the former attack and the integer equation for the latter attack have completely different algebraic structures. However, surprisingly, our powerful technique enables us to construct better lattices and improves Jochemsz-May's attack, too. It suggests that our proposed technique is quite useful to study the security of CRT-RSA over a wide range.

2 Preliminaries

Consider a modular equation $h(x_1, \ldots, x_r) = 0 \pmod{W}$, where all the absolute values of the target solutions $(\tilde{x}_1, \ldots, \tilde{x}_r)$ are bounded above by $X_1, \ldots, X_r$. When $\prod_{j=1}^{r} X_j$ is reasonably smaller than W, Coppersmith's method can find all the solutions in polynomial time. In this section, we recall a simplified reformulation of the method due to Howgrave-Graham [18] and its basis tools, i.e., Howgrave-Graham's lemma and the LLL algorithm.

Let $\|h(x_1, \ldots, x_r)\|$ denote a norm of a polynomial which represents the Euclidean norm of the coefficient vector. The following Howgrave-Graham's lemma reduces the modular equations into integer equations.

Lemma 1 (Howgrave-Graham's Lemma [18]). *Let $\tilde{h}(x_1, \ldots, x_r) \in \mathbb{Z}[x_1, \ldots, x_r]$ be a polynomial with at most n monomials. Let $m, W, X_1, \ldots, X_r$ be positive integers. Suppose that:*

1. $\tilde{h}(\tilde{x}_1, \ldots, \tilde{x}_r) = 0 \pmod{W^m}$, *where* $|\tilde{x}_1| < X_1, \ldots, |\tilde{x}_r| < X_r$,
2. $\|\tilde{h}(x_1 X_1, \ldots, x_r X_r)\| < W^m/\sqrt{n}$.

Then $\tilde{h}(\tilde{x}_1, \ldots, \tilde{x}_r) = 0$ holds over the integers.

To solve r-variate modular equations $h(x_1, \ldots, x_r) = 0 \pmod{W}$, it suffices to find r new polynomials $\tilde{h}_1(x_1, \ldots, x_r), \ldots, \tilde{h}_r(x_1, \ldots, x_r)$ whose root is the same as the original one, i.e., $(x_1, \ldots, x_r) = (\tilde{x}_1, \ldots, \tilde{x}_r)$, and whose norms are small enough to satisfy Howgrave-Graham's lemma.

To find such small norm polynomials from the original modular polynomial $h(x_1, \ldots, x_r)$, lattices and the LLL algorithm are used. An n-dimensional lattice is an additive discrete subgroup of $\mathbb{Z}^n$. In other words, a lattice represents all integer linear combinations of its basis vectors. All vectors are row representation throughout the paper. Let $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m$ be n-dimensional linearly independent vectors in $\mathbb{Z}^n$. A lattice spanned by these vectors as a basis is defined as $L(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m) := \{\sum_{j=1}^{m} c_j \boldsymbol{b}_j : c_j \in \mathbb{Z} \text{ for all } j = 1, 2, \ldots, n\}$. We also use a matrix representation for the basis. We define a basis matrix $\boldsymbol{B}$ as $m \times n$ matrix which has the basis vectors $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m$ in each row. A lattice spanned by a basis matrix $\boldsymbol{B}$ is denoted as $L(\boldsymbol{B})$. We call a lattice full-rank if and only if $n = m$. A determinant of a lattice $\det(L(\boldsymbol{B}))$ is defined as the m-dimensional volume of the fundamental parallelepiped; $\mathcal{P}(\boldsymbol{B}) := \{\mathbf{c}B : \mathbf{c} \in \mathbb{R}^m, 0 \leq c_j < 1, \text{for all } j = 1, 2, \ldots, m\}$. The determinant can be computed as $\det(L(\boldsymbol{B})) = \sqrt{\det(\boldsymbol{B}\boldsymbol{B}^T)}$ in general and that of a full-rank lattice can be computed as $\det(L(\boldsymbol{B})) = |\det(\boldsymbol{B})|$. In this paper, we only use a full-rank lattice. More specifically, we only use a lattice with a triangular basis matrix. Hence, the determinant of the lattice can be computed easily as the absolute value of a product of all diagonals.

Lattice has been used in various ways in cryptographic research. See [9,10,30,31,32] for more information. In cryptanalysis, finding non-zero short lattice vectors is usually an essential operation. In this paper, we recall the LLL algorithm [25] that outputs short lattice vectors in polynomial time.

Proposition 1 (LLL algorithm [25,30]). *Given linearly independent vectors $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$ in $\mathbb{Z}^n$, the LLL algorithm finds new basis vectors $\tilde{\boldsymbol{b}}_1, \ldots, \tilde{\boldsymbol{b}}_n$ for a lattice $L(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n)$ that satisfy*

$$\|\tilde{\boldsymbol{b}}_j\| \leq 2^{n(n-1)/4(n-j+1)} \det(L(\boldsymbol{B}))^{1/(n-j+1)} \quad \text{for } 1 \leq j \leq n,$$

in time polynomial in n and the maximum input length of $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$.

Again, we explain how to solve the modular equation $h(x_1, \ldots, x_r) = 0 \pmod{W}$. At first, we construct n polynomials $h_1(x_1, \ldots, x_r), \ldots, h_n(x_1, \ldots, x_r)$ that have the root $(\tilde{x}_1, \ldots, \tilde{x}_r)$ modulo W^m with some positive integer m. Then we construct n basis vectors $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$ and equivalently its matrix representation $\boldsymbol{B}$. Each elements of a vector $\boldsymbol{b}_j$ for $j = 1, 2, \ldots, n$ consist of coefficients of $h_j(x_1 X_1, \ldots, x_r X_r)$. Since all vectors in a lattice $L(\boldsymbol{B})$ are integer linear combinations of the basis vectors, all polynomials whose coefficients are derived from lattice vectors have the root $(\tilde{x}_1, \ldots, \tilde{x}_r)$ modulo W^m. We apply the LLL algorithm to a lattice basis $\boldsymbol{B}$ and obtain r LLL-reduced vectors $\tilde{\boldsymbol{b}}_1, \ldots, \tilde{\boldsymbol{b}}_r$. Then new polynomials $\tilde{h}_1(x_1, \ldots, x_r), \ldots, \tilde{h}_r(x_1, \ldots, x_r)$ which are derived from the above r LLL-reduced vectors satisfy Howgrave-Graham's lemma provided that $\det(L(\boldsymbol{B}))^{1/n} < W^m$. Here, we omit small terms. When we obtain r polynomials $\tilde{h}_1(x_1, \ldots, x_r), \ldots, \tilde{h}_r(x_1, \ldots, x_r)$, the root $(\tilde{x}_1, \ldots, \tilde{x}_r)$ can easily be recovered by computing resultant or Gröbner bases for the polynomials.

We should note that the method needs heuristic argument for multivariate problems. The polynomials $\tilde{h}_1(x_1, \ldots, x_r), \ldots, \tilde{h}_n(x_1, \ldots, x_r)$ derived from LLL output vectors have no assurance of algebraic independency. In this paper, we assume that the polynomials are algebraic independent as previous works [3,22,29] since there exist few negative reports. Moreover, we justify the validity of our attacks by computer experiments.

3 Small d_q Attack

In this section, we propose an attack for small d_q when p is significantly smaller than q. The attack improves Bleichnbacher-May's attack [3].

3.1 An Overview of the Lattice Construction

At first, we explain our strategy for lattice constructions. Since our lattice construction is highly technical, we show toy examples that compare previous lattices [3,29] and ours. We hope that these examples help readers to understand our technique easily.

Recall the CRT-RSA key generation;

$$ed_q = 1 + k(q-1)$$

with some integer k. If we can solve the following modular equation:

$$f_q(x_q, y_q) = 1 + x_q(y_q - 1) = 0 \pmod{e}$$

whose root is $(x_q, y_q) = (k, q)$, a public modulus N can be factorized. However, since the prime factor q is significantly larger than the other prime factor p, i.e., $p = N^\beta$ and $q = N^{1-\beta}$ for $\beta \leq 1/2$, May [29] multiplied the above equation by p and obtain the following equation:

$$ed_q p = p + k(N - p) = N + (k - 1)(N - p).$$

Hence, if the following modular equation can be solved, the public modulus N can be factorized:

$$f_p(x_p, y_p) = N + x_p(N - y_p) = 0 \pmod{e}$$

whose root is $(x_p, y_p) = (k - 1, p)$. Let $e = N^\alpha$ and $d_q = N^\delta$. Then the absolute values of the root (x_p, x_q, y_p, y_q) is bounded above by $X_p := N^{\alpha+\beta+\delta-1}, X_q := N^{\alpha+\beta+\delta-1}, Y_p := N^\beta, Y_q := N^{1-\beta}$ respectively within constant factors. Later we also use a notation $X := X_p = X_q$. In this setting, the other CRT-exponent d_p can be arbitrary large such that $d_p \approx N^\beta$.

May's Matrix. May [29] solved the modular equation $f_p(x_p, y_p) = 0$ under the standard lattice construction which can be captured by Jochemsz-May's strategy [22]. For example, although we omit the detail, he constructed the basis matrix as the following:

$$\begin{pmatrix}
e & & & & & & \\
0 & eX_p & & & & & \\
N & NX_p & -X_pY_p & & & & \\
0 & 0 & 0 & eY_p & & & \\
0 & 0 & NX_pY_p & NY_p & -X_pY_p^2 & & \\
0 & 0 & 0 & 0 & 0 & eY_p^2 & \\
0 & 0 & 0 & 0 & NX_pY_p^2 & NY_p^2 & -X_pY_p^3
\end{pmatrix}$$

where the rows consist of coefficients of seven polynomials: e, ex_p, $f_p(x_p, y_p)$, ey_p, $y_p f_p(x_p, y_p)$, ey_p^2, $y_p^2 f_p(x_p, y_p)$. All the polynomials share the common root as $f_p(x_p, y_p)$ modulo e. In addition to the base polynomials, i.e., $e, ex_p, f_p(x_p, y_p)$, he added extra y_p-shifts, i.e., $ey_p, y_p f_p(x_p, y_p), ey_p^2, y_p^2 f_p(x_p, y_p)$. Applying the LLL reduction to the above matrix, polynomials derived from the LLL output vectors satisfy Howgrave-Graham's lemma when

$$\begin{aligned}
X_p^4 Y_p^9 e^4 < e^7 &\Leftrightarrow 4(\alpha + \beta + \delta - 1) + 9\beta < 3\alpha \\
&\Leftrightarrow \delta < 1 - \frac{\alpha + 13\beta}{4}.
\end{aligned}$$

The core idea of the approach is solving the equation (2) not (1) since p is significantly smaller than q. Hence, if p becomes close to q such that $\beta \geq 0.382$, May's attack does not work.

Bleichenbacher-May Matrix. To improve May's attack [29] based on the above matrix, Bleichenbacher and May [3] made use of the relation $y_p y_q = N$ as Durfee and Nguyen [12]. Although the exact solution of y_p is unknown, the relation enables us to reduce powers of Y_p in the diagonals by multiplying powers of y_q to all the polynomials. By optimizing the powers of y_q, Bleichenbacher-May's matrix always offers better results than May's matrix.

To explain our improvement later, we modify Bleichenbacher-May's matrix where the modified matrix offer the same bound as the original Bleichenbacher-May matrix. The modification helps readers to understand the spirit of our improvement. Previous May's matrix used only extra y_p-shifts, however, modified Bleichenbacher-May's matrix used both y_p-shifts and y_q-shifts. Hence, we omit $ey_p^2, y_p^2 f_p(x_p, y_p)$ from the above matrix and add $ey_q, N^{-1} \cdot y_q f_p(x_p, y_p)$ in turn where the new polynomials share the common root as $f_p(x_p, y_p)$ modulo e:

$$\begin{pmatrix} e & & & & & & \\ 0 & eX_p & & & & & \\ N & NX_p & -X_pY_p & & & & \\ 0 & 0 & 0 & eY_p & & & \\ 0 & 0 & NX_pY_p & NY_p & -X_pY_p^2 & & \\ 0 & 0 & 0 & 0 & 0 & eY_q & \\ 0 & -X_p & 0 & 0 & 0 & Y_q & X_pY_q \end{pmatrix}.$$

Although the precise definition of the polynomial selection is slightly different from the one in the original paper, they are essentially the same in the sense that the above matrix yields the same bound as the original Bleichenbacher-May attack. Applying the LLL reduction to the above matrix, polynomials derived from the LLL output vectors satisfy Howgrave-Graham's lemma when

$$\begin{aligned} X_p^4 Y_p^4 Y_q^2 e^4 < e^7 &\Leftrightarrow 4(\alpha+\beta+\delta-1) + 4\beta + 2(1-\beta) < 3\alpha \\ &\Leftrightarrow \delta < \frac{1}{2} - \frac{\alpha + 6\beta}{4}. \end{aligned}$$

Compared with May's matrix, the matrix reduces the powers of Y_p by multiplying the powers of Y_q. It means that Bleichenbacher-May's approach tries to control the appearance of Y_p and Y_q. Then the attack works for larger p than May's attack up to $p < N^{0.468}$. By optimizing the selection of y_p-shifts and y_q-shifts, Bleichenbacher-May's attack is always better than May's attack.

Our Matrix. To improve the Bleichenbacher-May attack, what we focus on is the representation of the polynomial. More concretely, previous works used the only one representation, i.e., $f_p(x_p, y_p)$, however, there is the other representation, i.e., $f_q(x_q, y_q)$, for the same polynomial. Indeed, a useful algebraic property can be exploited from the polynomial $f_q(x_q, y_q)$ by making use of the fact that $x_q = x_p + 1$. For the above Bleichenbacher-May matrix to be triangular, the polynomial ey_q is necessary. Since eY_q is larger than the modulus e, the polynomial does not contribute to maximize the solvable root bound as explained

in [31,41]. However, we make use of $f_q(x_q, y_q)$ and show that the matrix becomes triangular without ey_q as follows:

$$\begin{pmatrix} e & & & & & \\ 0 & eX_p & & & & \\ N & NX_p & -X_pY_p & & & \\ 0 & 0 & 0 & eY_p & & \\ 0 & 0 & NX_pY_p & NY_p & -X_pY_p^2 & \\ 0 & -X_p & 0 & 0 & 0 & X_qY_q \end{pmatrix}.$$

Although the above Bleichenbacher-May matrix used $N^{-1} \cdot y_q f_p(x_p, y_p)$ in the bottom row, we use $f_q(x_q, y_q)$ in turn. Notice that $f_q(x_q, y_q) = N^{-1} \cdot y_q f_p(x_p, y_p)$ and we use the same polynomial as the Bleichenbacher-May, however, the algebraic structure of $f_q(x_q, y_q)$, i.e., the relation $x_q = x_p + 1$, enables the matrix to be triangular without ey_q. The operation means that Bleichenbacher-May's matrix contains better sublattices. The representation $f_q(x_q, y_q)$, which was not used by Bleichenbacher and May, enables us to exploit the sublattices. Indeed, by construction, our matrix always outperforms the above Bleichenbacher-May matrix with less lattice dimensions. Applying the LLL reduction to our above matrix, polynomials derived from the LLL output vectors satisfy Howgrave-Graham's lemma when

$$\begin{aligned} X_p^3 X_q Y_p^4 Y_q e^3 < e^6 &\Leftrightarrow 4(\alpha + \beta + \delta - 1) + 4\beta + (1 - \beta) < 3\alpha \\ &\Leftrightarrow \delta < \frac{3}{4} - \frac{\alpha + 7\beta}{4}. \end{aligned}$$

Since $\beta \leq 1/2$, the bound is always better than the above Bleichenbacher-May example.

May's modulo q Attack. We should notice that our lattice construction technique does not always offer the best attack. More concretely, as we discussed above, our lattice offers better results than all the existing lattices to solve $f_p(x_p, y_p) = 0$ and $f_q(x_q, y_q) = 0$. However, there is the other formulations to attack CRT-RSA, i.e., May's modulo q approach [29]. From the CRT-RSA key generation $ed_q = 1 + k(q - 1)$, May solved a modular equation;

$$x + ey = 0 \pmod{q}$$

whose root is $(k - 1, d_q)$. Since the modulo e and the modulo q approach is different, we should check whether which method is the better. Although our modulo e attacks are the better in most cases, we will show in Section 5.2 that the modulo p approach outperforms modulo e approach for small d_p attack with a modulus $N = p^r q$.

3.2 Attack for Large e

Although the above discussion handled only toy examples, our approach improves an asymptotic condition of the small CRT-exponent attack. In this sec-

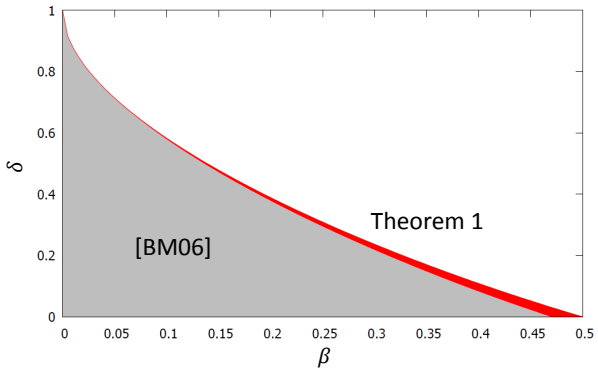

Fig. 1. Comparison between our attack (Theorem 1) and the Bleichenbacher-May for $\alpha = 1$.

tion, we propose an improved attack that works when $\alpha > \beta/(1-\beta)$. The attack is the first result to cover the desired bound, i.e., $\beta < 1/2$ with a full size e.

Theorem 1. *Let $N = pq$ be an RSA modulus where $p = N^{\beta}$ and $q = N^{1-\beta}$ for $\beta \leq 1/2$. Let $e = N^{\alpha}$ and $d_q < N^{\delta}$ be a public/CRT exponent respectively such that $ed_q = 1 \pmod{(q-1)}$. Given public elements N and e, if*

$$\delta < \frac{(1-\beta)(3+2\beta) - 2\sqrt{\beta(1-\beta)(\alpha\beta+3\alpha+\beta)}}{3+\beta} \text{ and } \alpha > \frac{\beta}{1-\beta},$$

then N can be factorized in polynomial time by assuming that polynomials which are derived from LLL reduced bases are algebraically independent.

As opposed to previous results, when $\alpha = 1$, the attack works to $\beta < 1/2$. Figure 1 compares our result and the Bleichenbacher-May for $\alpha = 1$. Our attack covers larger δ than the Bleichenbacher-May attack for all β.

Proof of Theorem 1. To solve the modular equation $f_q(x_q, y_q) = 0$ and equivalently $f_p(x_p, y_p) = 0$, we use the following shift-polynomials:

$$\begin{aligned} g_{[i,j]}(x_p, y_p) &:= x_p^j f_p^i(x_p, y_p) e^{m-i}, \\ g'_{[i,j]}(x_p, y_p) &:= y_p^j f_p^i(x_p, y_p) e^{m-i}, \\ g''_{[i,j]}(x_p, x_q, y_p, y_q) &:= f_p^{i-j}(x_p, y_p) f_q^j(x_q, y_q) e^{m-i}, \end{aligned}$$

with some positive integer m. For non-negative integers i and j, all the shift-polynomials share the same root as $f_p(x_p, y_p)$ and $f_q(x_q, y_q)$ modulo e^m. May [29] used the same shift-polynomials as $g_{[i,j]}(x_p, y_p)$ and $g'_{[i,j]}(x_p, y_p)$. The (modified) Bleichenbacher-May attack used an additional shift-polynomial which used only $f_p(x_p, y_p)$. However, as we showed an example in the previous section, we use the both representations $f_p(x_p, y_p)$ and $f_q(x_q, y_q)$ simultaneously. Then we can construct triangular basis matrices that generalize the toy example as follows.

Lemma 2. *Let all the polynomials be defined as above. Let τ_p and τ_q be constants such that $\tau_p \geq 0$ and $0 \leq \tau_q \leq 1$. Define sets of indices*

$$\begin{aligned}\mathcal{I}_x &:= \{i = 0, 1, \ldots, m; j = 0, 1, \ldots, m - i\},\\ \mathcal{I}_{y,p} &:= \{i = 0, 1, \ldots, m; j = 1, 2, \ldots, \lceil \tau_p m \rceil\},\\ \mathcal{I}_{y,q} &:= \{i = 1, 2, \ldots, m; j = 1, 2, \ldots, \lceil \tau_q i \rceil\}.\end{aligned}$$

Let $\boldsymbol{B}$ be a matrix whose rows consist of coefficients of $g_{[i,j]}(x_pX_p, y_pY_p)$, $g'_{[i,j]}(x_pX_p, y_pY_p)$, and $g''_{[i,j]}(x_pX_p, x_qX_q, y_pY_p, y_qY_q)$ with indices in $\mathcal{I}_x$, $\mathcal{I}_{y,p}$, and $\mathcal{I}_{y,q}$, respectively. If the shift-polynomials are ordered as

$$\begin{aligned}&g_{[i,j]} \prec g'_{[i,j]}, g''_{[i,j]},\\ &g_{[i,j]} \prec g_{[i',j']}, g'_{[i,j]} \prec g'_{[i',j']}, g''_{[i,j]} \prec g''_{[i',j']} \quad \textit{for} \quad i < i',\\ &g_{[i,j]} \prec g_{[i,j']}, g'_{[i,j]} \prec g'_{[i,j']}, g''_{[i,j]} \prec g''_{[i,j']} \quad \textit{for} \quad j < j',\end{aligned}$$

and $N^{-1} \pmod{e^m}$ is multiplied appropriately, then the matrix becomes triangular with diagonals

- $X_p^{i+j}Y_p^i e^{m-i}$ *for* $g_{[i,j]}(x_pX_p, y_pY_p)$,
- $X_p^i Y_p^{i+j} e^{m-i}$ *for* $g'_{[i,j]}(x_pX_p, y_pY_p)$,
- $X_q^i Y_q^j e^{m-i}$ *for* $g''_{[i,j]}(x_pY_p, x_qX_q, y_pY_p, y_qY_q)$.

Here, we do not prove the lemma. Later, we prove a more general form of the statement, i.e., Lemma 3.

We compute the resulting condition of Theorem 1. The dimension n and the determinant of the lattice $\det(\boldsymbol{B}) = X^{s_X} Y_p^{s_{Y_p}} Y_q^{s_{Y_q}} e^{s_e}$ can be computed as:

$$\begin{aligned}n &= \sum_{(i,j)\in\mathcal{I}_x} 1 + \sum_{(i,j)\in\mathcal{I}_{y,p}} 1 + \sum_{(i,j)\in\mathcal{I}_{y,q}} 1 = \frac{1 + 2\tau_p + \tau_q}{2} m^2 + o(m^2),\\ s_X &= \sum_{(i,j)\in\mathcal{I}_x} (i + j) + \sum_{(i,j)\in\mathcal{I}_{y,p}} i + \sum_{(i,j)\in\mathcal{I}_{y,q}} i = \frac{2 + 3\tau_p + 2\tau_q}{6} m^3 + o(m^3),\\ s_{Y_p} &= \sum_{(i,j)\in\mathcal{I}_x} i + \sum_{(i,j)\in\mathcal{I}_{y,p}} (i + j) = \frac{1 + 3\tau_p + 3\tau_p^2}{6} m^3 + o(m^3),\\ s_{Y_q} &= \sum_{(i,j)\in\mathcal{I}_{y,q}} j = \frac{\tau_q^2}{6} m^3 + o(m^3),\\ s_e &= \sum_{(i,j)\in\mathcal{I}_x} (m - i) + \sum_{(i,j)\in\mathcal{I}_{y,p}} (m - i) + \sum_{(i,j)\in\mathcal{I}_{y,q}} (m - i)\\ &= \frac{2 + 3\tau_p + \tau_q}{6} m^3 + o(m^3).\end{aligned}$$

Applying the LLL reduction, the polynomials obtained from the output vectors satisfy Howgrave-Graham's lemma if $X^{s_X} Y_p^{s_{Y_p}} Y_q^{s_{Y_q}} e^{s_e} < e^{nm}$, i.e.,

$$(\alpha + \beta + \delta - 1)\frac{2 + 3\tau_p + 2\tau_q}{6} + \beta\frac{1 + 3\tau_p + 3\tau_p^2}{6}$$

$$+(1-\beta)\frac{\tau_q^2}{6}-\alpha\frac{1+3\tau_p+2\tau_q}{6}<0$$

by omitting low order terms of m. To minimize the left hand side of the inequality, we substitute the parameters $\tau_p=(1-2\beta-\delta)/(2\beta)$ and $\tau_q=(1-\beta-\delta)/(1-\beta)$, then the condition becomes

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

as required. To satisfy the restriction $\tau_p\geq 0$, $\alpha>\beta/(1-\beta)$ should hold. The other parameter τ_q always satisfies $0\leq\tau_q\leq 1$. □

3.3 Attack for Small e

The attack of Theorem 1 works only for $\alpha>\beta/(1-\beta)$. The constraint comes from the fact that the parameter τ_p used in the proof should be non-negative. To capture the other case, i.e., $\alpha\leq\beta/(1-\beta)$, under the same algorithm construction, we set the parameters $\tau_p=0$ and $\tau_q=(1-\beta-\delta)/(1-\beta)$, then the attack works for $\delta<2(1-\beta)-\sqrt{(1+\alpha)(1-\beta)}$.

However, by modifying the lattice construction, a better result can be obtained as follows.

Theorem 2. *Let $N=pq$ be an RSA modulus where $p<N^\beta$ and $q\geq N^{1-\beta}$ for $\beta\leq 1/2$. Let $e=N^\alpha$ and $d_q<N^\delta$ be a public/CRT exponent respectively such that $ed_q=1 \pmod{(q-1)}$. Given public elements N and e, if*

$$\delta<1-\beta-\sqrt{\alpha\beta(1-\beta)} \text{ for } \beta(1-\beta)\leq\alpha\leq\frac{\beta}{1-\beta},$$

then N can be factorized in polynomial time by assuming that polynomials which are derived from LLL reduced bases are algebraically independent.

As we claimed, the bound of Theorem 2 is better than $\delta<2(1-\beta)-\sqrt{(1+\alpha)(1-\beta)}$ which can be obtained from the same algorithm construction as Theorem 1. We show the proof of Theorem 2. The proof is more technical than that of Theorem 1, however, the spirit is almost the same. In the subsequent sections, lattices which are similar to that of Theorem 2 will be used.

Proof of Theorem 2. To solve the modular equation $f_q(x_q,y_q)=0$ and equivalently $f_p(x_p,y_p)=0$, we use the following shift-polynomials:

$$g_{[i,j],\lambda}(x_p,x_q,y_p,y_q):=x_p^j f_p^{\lceil\lambda i\rceil}(x_p,y_p)f_q^{\lfloor(1-\lambda)i\rfloor}(x_q,y_q)e^{m-i},$$
$$g'_{[i,j],\lambda}(x_p,x_q,y_p,y_q):=y_q^j f_p^{\lceil\lambda i\rceil}(x_p,y_p)f_q^{\lfloor(1-\lambda)i\rfloor}(x_q,y_q)e^{m-i},$$

with some positive integer m and a parameter $0<\lambda\leq 1$. For non-negative integers i and j, all the shift-polynomials share the common root as $f_p(x_p,y_p)$ and $f_q(x_q,y_q)$ modulo e^m. Here, notice that $\lceil\lambda i\rceil+\lfloor(1-\lambda)i\rfloor=i$ for all i. The

shift-polynomials $g'_{[i,j]}(x_p, y_p)$ and $g''_{[i,j]}(x_p, y_p)$ used in the proof of Theorem 1 is the special case of $g_{[i,j],\lambda}(x_p, x_q, y_p, y_q)$ and $g'_{[i,j],\lambda}(x_p, x_q, y_p, y_q)$ for $\lambda = 1$. As the attack of Theorem 1, we use both representations $f_p(x_p, y_p)$ and $f_q(x_q, y_q)$ simultaneously for all shift-polynomials. Using these shift-polynomials, we can construct triangular basis matrices as follows.

Lemma 3. *Let all the polynomials be defined as above. Let τ be a constant such that $1 - \lambda < \tau \leq 1$. Let m be a positive integer. Define sets of indices as*

$$\begin{aligned}\mathcal{I}_x &:= \{i = 0, 1, \ldots, m; j = 0, 1, \ldots, m - i\},\\ \mathcal{I}_{y_q} &:= \{i = 1, 2, \ldots, m; j = 1, 2, \ldots, \lceil \tau i \rceil - \lfloor (1 - \lambda) i \rfloor\}.\end{aligned}$$

Let $\boldsymbol{B}$ be a matrix whose rows consist of coefficients of $g_{[i,j],\lambda}(x_p X_p, x_q X_q, y_p Y_p, y_q Y_q)$ and $g'_{[i,j],\lambda}(x_p X_p, x_q X_q, y_p Y_p, y_q Y_q)$ with indices in $\mathcal{I}_x$ and $\mathcal{I}_{y,q}$ respectively. If the shift-polynomials are ordered as

$$\begin{aligned}&g_{[i,j],\lambda} \prec g'_{[i,j],\lambda},\\ &g_{[i,j],\lambda} \prec g_{[i',j'],\lambda}, g'_{[i,j],\lambda} \prec g'_{[i',j'],\lambda} \text{ for } i < i',\\ &g_{[i,j],\lambda} \prec g_{[i,j'],\lambda}, g'_{[i,j],\lambda} \prec g'_{[i,j'],\lambda} \text{ for } j < j',\end{aligned}$$

and $N^{-1} \pmod{e^m}$ is multiplied appropriately, then the matrix becomes triangular with diagonals

- $X_p^{i+j} Y_p^{\lceil \lambda i \rceil} e^{m-i}$ *for* $g_{[i,j],\lambda}(x_p X_p, x_q X_q, y_p Y_p, y_q Y_q)$ *with i such that $i = 0$ and $\lceil \lambda i \rceil - \lceil \lambda (i-1) \rceil = 1$,*
- $X_q^{i+j} Y_q^{\lfloor (1-\lambda) i \rfloor} e^{m-i}$ *for* $g_{[i,j],\lambda}(x_p X_p, x_q X_q, y_p Y_p, y_q Y_q)$ *with i such that $i \neq 0$ and $\lceil \lambda i \rceil - \lceil \lambda (i-1) \rceil = 0$,*
- $X_q^{i} Y_q^{\lfloor (1-\lambda) i \rfloor + j} e^{m-i}$ *for* $g'_{[i,j],\lambda}(x_p X_p, x_q X_q, y_p Y_p, y_q Y_q)$.

A proof of the lemma is the most technical part of this paper. We prove it in Section 3.4.

We compute the resulting condition of Theorem 2. The dimension n and the determinant of the lattice $\det(\boldsymbol{B}) = X^{s_X} Y_p^{s_{Y_p}} Y_q^{s_{Y_q}} e^{s_e}$ can be computed as:

$$\begin{aligned}n &= \sum_{(i,j)\in\mathcal{I}_x} 1 + \sum_{(i,j)\in\mathcal{I}_{y_q}} 1 = \frac{\lambda + \tau}{2} m^2 + o(m^2),\\ s_X &= \sum_{(i,j)\in\mathcal{I}_x} (i + j) + \sum_{(i,j)\in\mathcal{I}_{y_q}} i = \frac{\lambda + \tau}{3} m^3 + o(m^3),\\ s_{Y_p} &= \sum_{(i,j)\in\mathcal{I}_x} \lceil \lambda i \rceil = \frac{\lambda^2}{6} m^3 + o(m^3),\\ s_{Y_q} &= \sum_{(i,j)\in\mathcal{I}_x} \lfloor (1 - \lambda) i \rfloor + \sum_{(i,j)\in\mathcal{I}_{y_q}} (\lfloor (1 - \lambda) i \rfloor + j) = \frac{\tau^2}{6} m^3 + o(m^3),\end{aligned}$$

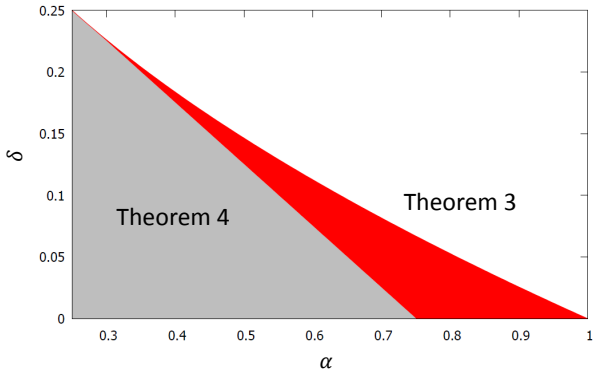

Fig. 2. Comparison between our attack (Theorem 3) and the attack of Lu et al. (Theorem 4) [28].

$$s_e = \sum_{(i,j)\in\mathcal{I}_x} (m-i) + \sum_{(i,j)\in\mathcal{I}_{y_q}} (m-i) = \frac{1+\lambda+\tau}{6} m^3 + o(m^3).$$

Applying the LLL reduction, the polynomials obtained from the output vectors satisfy Howgrave-Graham's lemma if $X^{s_X} Y_p^{s_{Y_p}} Y_q^{s_{Y_q}} e^{s_e} < e^{nm}$, i.e.,

$$(\alpha+\beta+\delta-1)\frac{\lambda+\tau}{3} + \beta\frac{\lambda^2}{6} + (1-\beta)\frac{\tau^2}{6} - \alpha\frac{-1+2\lambda+2\tau}{6} < 0$$

by omitting low order terms of m. To minimize the left hand side of the inequality, we set the parameters $\lambda = (1-\beta-\delta)/\beta$ and $\tau = (1-\beta-\delta)/(1-\beta)$, then the condition becomes

$$\delta < 1 - \beta - \sqrt{\alpha\beta(1-\beta)}$$

as required. To satisfy the restrictions $0 < \lambda \leq 1$ and $1-\lambda < \tau \leq 1$, $\beta(1-\beta) \leq \alpha \leq \beta/(1-\beta)$ should hold. □

As opposed to the attack of Theorem 1, that of Theorem 2 is applicable to a balanced RSA, i.e., $\beta = 1/2$, for $\alpha \leq 1$. For a balanced RSA, we substitute $\beta = 1/2$ and the attack becomes as follows.

Theorem 3. *Let $N = pq$ be an RSA modulus where the prime factors p and q are the same bit-size. Let $e = N^\alpha$ and $d_q < N^\delta$ be a public/CRT exponent respectively such that $ed_q = 1 \pmod{(q-1)}$. Given public elements N and e, if*

$$\delta < \frac{1-\sqrt{\alpha}}{2} \quad \textit{for} \quad \alpha \geq \frac{1}{4},$$

then N can be factorized in polynomial time by assuming that polynomials which are derived from LLL reduced bases are algebraically independent.

By construction, the attack always outperforms that under Bleichenbacher-May's lattice construction. We also compare our attack with that of Lu et al. [29] (Theorem 9 of [28]) which follows May's modulo q approach.

Theorem 4 ([28]). *Let $N = pq$ be an RSA modulus where the prime factors p and q are the same bit-size. Let $e = N^{\alpha}$ and $d_q < N^{\delta}$ be a public/CRT exponent respectively such that $ed_q = 1 \pmod{(q-1)}$. Given public elements N and e, if*

$$\delta < \frac{3 - 4\alpha}{8},$$

then N can be factorized in polynomial time by assuming that polynomials which are derived from LLL reduced bases are algebraically independent.

Figure 2 compares our attack (Theorem 3) and that of Lu et al. (Theorem 4). Our attack is better for all $1/4 < \alpha < 1$.

3.4 Proof of Lemma 3

In this section, we show a proof of Lemma 3 that is the most technical part of this paper. Before the detailed proof, we explain the spirit of our triangular matrix. The polynomials which we use contains four variables x_p, x_q, y_p, y_q. Furthermore, there are two algebraic relations: $x_q = x_p + 1$ and $y_p y_q = N$. By using the latter relation, i.e., $y_p y_q = N$, we transform all monomials as they do not have both y_p and y_q simultaneously where the same operation was also done in previous works [3,12]. Moreover, we use an additional trick. By using the former relation, i.e., $x_q = x_p + 1$, we transform all monomials as they do not have both x_p and x_q simultaneously. More concretely, the variable x_p appears only in monomials where powers of y_p are non-negative whereas the variable x_q appears only in monomials where powers of y_q are positive. The simple operation is the key technique of this paper.

Then we show the proof of Lemma 3.

Proof of Lemma 3. Since all $g_{[i,j],\lambda}(x_p, x_q, y_p, y_q)$ for $i = 0$ have only one monomial $x_p^j e^m$, these polynomials generate triangular basis matrix with diagonals $X_p^j e^m$. Then remaining proof is inductive; we show that the basis matrix is still triangular with other polynomials.

At first, we assume that polynomials $g_{[i',j'],\lambda}(x_p, x_q, y_p, y_q)$ such that $g_{[i',j'],\lambda}(x_p, x_q, y_p, y_q) \prec g_{[i,j],\lambda}(x_p, x_q, y_p, y_q)$ generate a triangular matrix as stated in Lemma 3. Then, we show that a matrix is still triangular with a new polynomial $g_{[i,j],\lambda}(x_p, x_q, y_p, y_q)$ whose diagonal is $x_p^{i+j} y_p^{\lceil \lambda i \rceil} e^{m-i}$. By definition,

$$\begin{aligned} g_{[i,j],\lambda}(x_p, x_q, y_p, y_q) &= x_p^j f_p^{\lceil \lambda i \rceil}(x_p, y_p) f_q^{\lfloor (1-\lambda) i \rfloor}(x_q, y_q) e^{m-i} \\ &= x_p^j (N + N x_p - x_p y_p)^{\lceil \lambda i \rceil} (1 - x_q + x_q y_q)^{\lfloor (1-\lambda) i \rfloor} e^{m-i}. \end{aligned}$$

From the relation $x_q = x_p + 1$ and equivalently $x_p = x_q - 1$, the polynomial becomes

$$= x_p^j (N x_q - x_p y_p)^{\lceil \lambda i \rceil} (x_p + x_q y_q)^{\lfloor (1-\lambda) i \rfloor} e^{m-i}.$$

By expanding $(Nx_q - x_p y_p)^{\lceil \lambda i \rceil}$ and $(x_p + x_q y_q)^{\lfloor (1-\lambda) i \rfloor}$,

$$
\begin{aligned}
&= x_p^j \left(\sum_{i_p=0}^{\lceil \lambda i \rceil} \binom{\lceil \lambda i \rceil}{i_p} (-x_p y_p)^{i_p} \cdot (Nx_q)^{\lceil \lambda i \rceil - i_p} \right) \cdot \\
&\quad \left(\sum_{i_q=0}^{\lfloor (1-\lambda) i \rfloor} \binom{\lfloor (1-\lambda) i \rfloor}{i_q} (x_q y_q)^{i_q} \cdot x_p^{\lfloor (1-\lambda) i \rfloor - i_q} \right) e^{m-i} \\
&= \sum_{i_p=0}^{\lceil \lambda i \rceil} \sum_{i_q=0}^{\lfloor (1-\lambda) i \rfloor} (-1)^{i_p} \binom{\lceil \lambda i \rceil}{i_p} \binom{\lfloor (1-\lambda) i \rfloor}{i_q} N^{\lceil \lambda i \rceil - i_p} \cdot \\
&\quad x_p^{\lfloor (1-\lambda) i \rfloor + i_p - i_q + j} x_q^{\lceil \lambda i \rceil - i_p + i_q} y_q^{i_q} y_p^{i_p} e^{m-i}.
\end{aligned}
$$

From the relation $y_p y_q = N$, the polynomial becomes

$$
\begin{aligned}
&= \sum_{i_q=0}^{\lfloor (1-\lambda) i \rfloor} \sum_{i_p=i_q}^{\lceil \lambda i \rceil} (-1)^{i_p} \binom{\lceil \lambda i \rceil}{i_p} \binom{\lfloor (1-\lambda) i \rfloor}{i_q} N^{\lceil \lambda i \rceil - i_p + i_q} \cdot \\
&\quad x_p^{\lfloor (1-\lambda) i \rfloor + i_p - i_q + j} x_q^{\lceil \lambda i \rceil - i_p + i_q} y_p^{i_p - i_q} e^{m-i} \\
&+ \sum_{i_p=0}^{\lfloor (1-\lambda) i \rfloor - 1} \sum_{i_q=i_p+1}^{\lfloor (1-\lambda) i \rfloor} (-1)^{i_p} \binom{\lceil \lambda i \rceil}{i_p} \binom{\lfloor (1-\lambda) i \rfloor}{i_q} N^{\lceil \lambda i \rceil} \cdot \\
&\quad x_p^{\lfloor (1-\lambda) i \rfloor + i_p - i_q + j} x_q^{\lceil \lambda i \rceil - i_p + i_q} y_q^{i_q - i_p} e^{m-i}.
\end{aligned}
$$

Notice that there are no monomials that have y_p and y_q simultaneously. The exponents of y_p in the first summation are non-negative whereas the exponents of y_q in the second summation are positive. Hence, as we discussed above, we replace all x_q in the first summation by $x_p + 1$ and replace all x_p in the second summation by $x_q - 1$. Then, the polynomial becomes

$$
\begin{aligned}
&= \sum_{i_q=0}^{\lfloor (1-\lambda) i \rfloor} \sum_{i_p=i_q}^{\lceil \lambda i \rceil} (-1)^{i_p} \binom{\lceil \lambda i \rceil}{i_p} \binom{\lfloor (1-\lambda) i \rfloor}{i_q} N^{\lceil \lambda i \rceil - i_p + i_q} \cdot \\
&\quad x_p^{\lfloor (1-\lambda) i \rfloor + i_p - i_q + j} (x_p + 1)^{\lceil \lambda i \rceil - i_p + i_q} y_p^{i_p - i_q} e^{m-i} \\
&+ \sum_{i_p=0}^{\lfloor (1-\lambda) i \rfloor - 1} \sum_{i_q=i_p+1}^{\lfloor (1-\lambda) i \rfloor} (-1)^{i_p} \binom{\lceil \lambda i \rceil}{i_p} \binom{\lfloor (1-\lambda) i \rfloor}{i_q} N^{\lceil \lambda i \rceil} \cdot \\
&\quad (x_q - 1)^{\lfloor (1-\lambda) i \rfloor + i_p - i_q + j} x_q^{\lceil \lambda i \rceil - i_p + i_q} y_q^{i_q - i_p} e^{m-i} \\
&= \sum_{i_q=0}^{\lfloor (1-\lambda) i \rfloor} \sum_{i_p=i_q}^{\lceil \lambda i \rceil} \sum_{i'=0}^{\lceil \lambda i \rceil - i_p + i_q} (-1)^{i_p} \binom{\lceil \lambda i \rceil}{i_p} \binom{\lfloor (1-\lambda) i \rfloor}{i_q} \binom{\lceil \lambda i \rceil - i_p + i_q}{i'} \cdot \\
&\quad N^{\lceil \lambda i \rceil - i_p + i_q} x_p^{i - i' + j} y_p^{i_p - i_q} e^{m-i} \\
&+ \sum_{i_p=0}^{\lfloor (1-\lambda) i \rfloor - 1} \sum_{i_q=i_p+1}^{\lfloor (1-\lambda) i \rfloor} \sum_{i'=0}^{\lfloor (1-\lambda) i \rfloor + i_p - i_q + j} (-1)^{i_p + i'} \binom{\lceil \lambda i \rceil}{i_p} \binom{\lfloor (1-\lambda) i \rfloor}{i_q} \cdot
\end{aligned}
$$

$$\binom{\lfloor(1-\lambda)i\rfloor + i_p - i_q + j}{i'} N^{\lceil\lambda i\rceil} x_q^{i-i'+j} y_q^{i_q - i_p} e^{m-i}.$$

The polynomial has monomials for variables

- $x_p^{i_{px}} y_p^{i_{py}}$ for $i_{py} = 0, 1, \ldots, \lceil\lambda i\rceil; i_{px} = i_{py} + \lfloor(1-\lambda)i\rfloor + j, \ldots, i + j$,
- $x_q^{i_{qx}} y_q^{i_{qy}}$ for $i_{qy} = 1, 2, \ldots, \lfloor(1-\lambda)i\rfloor; i_{qx} = i_{qy} + \lceil\lambda i\rceil, \ldots, i + j$.

Then, we show that these variables except $x_p^{i+j} y_p^{\lceil\lambda i\rceil}$ already appeared in the diagonals of a basis matrix. The above variables appeared for diagonals of $g_{[i',j'],\lambda}(x_pX_p, x_qX_q, y_pY_p, y_qY_q)$ for

$$\begin{aligned}
&i' = 0, 1, \ldots, i-1 \text{ such that } \lceil\lambda i'\rceil - \lceil\lambda(i'-1)\rceil = 1;\\
&j' = \lfloor(1-\lambda)i\rfloor - \lfloor(1-\lambda)i'\rfloor + j, \ldots, i + j - i', \text{ and}\\
&i' = 1, 2, \ldots, i-1 \text{ such that } \lceil\lambda i'\rceil - \lceil\lambda(i'-1)\rceil = 0;\\
&j' = \lceil\lambda i\rceil - \lceil\lambda i'\rceil, \ldots, i + j - i'.
\end{aligned}$$

Since $i' < i$, by our definition of the polynomial order,

$$g_{[i',j'],\lambda}(x_pX_p, x_qX_q, y_pY_p, y_qY_q) \prec g_{[i,j],\lambda}(x_pX_p, x_qX_q, y_pY_p, y_qY_q)$$

holds for all the above i' and j'. All we have to show is that these polynomials are selected in the lattice basis. For the purpose, we show that the indices

$$\begin{aligned}
&i' = 0, 1, \ldots, i-1;\\
&j' = \min\{\lfloor(1-\lambda)i\rfloor - \lfloor(1-\lambda)i'\rfloor + j, \lceil\lambda i\rceil - \lceil\lambda i'\rceil\}, \ldots, i + j - i',
\end{aligned}$$

are contained in

$$i' = 0, 1, \ldots, m; j' = 0, 1, \ldots, m - i'.$$

Since $0 < \lambda \leq 1, 0 \leq i' \leq i$, and $j \geq 0$,

$$\lfloor(1-\lambda)i\rfloor - \lfloor(1-\lambda)i'\rfloor + j \geq 0 \quad \text{and} \quad \lceil\lambda i\rceil - \lceil\lambda i'\rceil \geq 0$$

hold. Since $i + j \leq m$ holds,

$$i + j - i' \leq m - i'$$

holds. Then the statement holds. In the same manner, analogous proof is obtained for the other polynomials $g'_{[i,j],\lambda}(x_p, x_q, y_p, y_q)$. We will show the remaining proof in the full version. □

To end this section, we briefly show how to deduce Lemma 2 from Lemma 3. The collection of shift-polynomials $g_{[i,j]}(x_p, y_p)$ and $g''_{[i,j]}(x_p, x_q, y_p, y_q)$ in Lemma 2 are essentially the same as $g_{[i,j],\lambda}(x_p, x_q, y_p, y_q)$ and $g'_{[i,j],\lambda}(x_p, x_q, y_p, y_q)$ in Lemma 3 for $\lambda = 1$. Hence, by setting the parameters (λ, τ) in Lemma 3 as $(1, \tau_q)$, Lemma 3 show that $g_{[i,j]}(x_p, y_p)$ and $g''_{[i,j]}(x_p, x_q, y_p, y_q)$ in Lemma 2 generate a triangular matrix. To complete the proof of Lemma 2, we also use May's result [29] that showed that polynomials $g_{[i,j]}(x_p, y_p)$ and $g'_{[i,j]}(x_p, y_p)$ generate a triangular matrix. As a result, $g_{[i,j]}(x_p, y_p)$, $g'_{[i,j]}(x_p, y_p)$, and $g''_{[i,j]}(x_p, x_q, y_p, y_q)$ in Lemma 2 generates a triangular matrix.

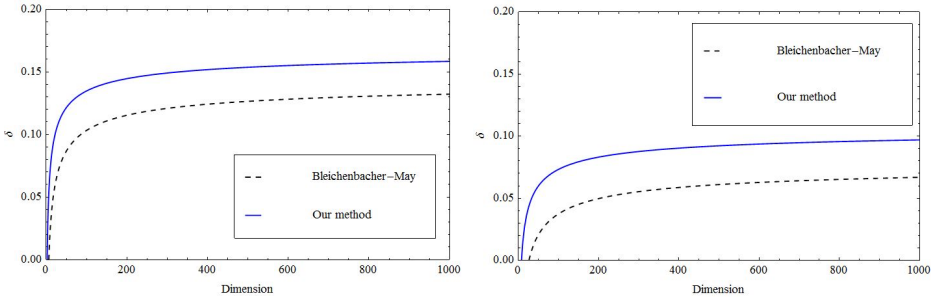

Fig. 3. Comparisons of recoverable bounds depending on lattice dimensions. The left and the right figure is for $\beta = 0.35$ and $\beta = 0.40$, respectively.

3.5 Experimental results

We have implemented the experiment program in Magma 2.10 computer algebra system [6] on a PC with Intel(R) Core(TM) Duo CPU(3.30GHz, 4.0GB RAM Windows 7). Table 1 lists some theoretical and experimental results on factoring two 1000-bit RSA moduli with varying bit-size of q. In all experiments, we successfully find the factorization of these RSA moduli.

In [3], the experimental results are much better than their theoretical analysis. For example, for 440-bit factor q, with a lattice dimension of 63, in theory the attack should not work (we can recover the small private key d_p up to a size of $N^{-0.083}$), however, in practice, we succeed for d_p with bit-size a 0.010-fraction of N. Since our lattice construction captures the underlying sublattice structure of [3]'s desired lattice, we can do better than [3]: with a lattice dimension of 66, experimentally we can reconstruct d_p with a size of $N^{0.012}$.

Note that our result of Theorem 1 is an asymptotic improvement. In Table 2, we present numerical values of δ for different values of β and lattice dimension. Moreover, compared with [3], our method requires smaller lattice dimensions. For $\beta = 0.35$ and $\beta = 0.40$, Figure 3 shows a comparison of these two approaches in the terms of the bit-size of small secret exponent d_p that can be attacked.

Table 1. For 1000-bit RSA moduli, asymptotic and experimental comparisons of small d_q attacks

Bitsize of q	Bleichenbacher-May [3]				Our work			
	Asymptotic	Expt.	dim.	L^3 time	Asymptotic	Expt.	dim.	L^3 time
305	0.210	0.160	63	53 min	0.230	0.170	56	15 min
355	0.140	0.100	63	44 min	0.164	0.100	58	16 min
405	0.075	0.050	63	35 min	0.103	0.055	66	57 min
440	0.033	0.010	63	35 min	0.064	0.012	66	60 min

Table 2. Asymptotic bounds and lattice dimension for small δ with fixed lattice dimensions.

$\beta = 0.45$					
δ	0.010	0.020	0.030	0.040	0.052
dim.	109	154	340	1055	Asymptotic
$\beta = 0.48$					
δ	0.002	0.005	0.010	0.015	0.020
dim.	486	686	1491	5443	Asymptotic

4 Small d_p and d_q Attack

In this section, we propose an attack when both d_p and d_q are small. The attack improves Jochemsz-May's attack [22].

4.1 Our Attack

Recall the CRT-RSA key generation;

$$ed_q = 1 + k_q(q-1) \quad \text{and} \quad ed_p = 1 + k_p(p-1)$$

with some integers k_q and k_p. Hence, if we can solve the following simultaneous modular equations, RSA modulus N can be factorized:

$$\begin{aligned} f_{q,1}(x_{q,1}, y_q) &= 1 + x_{q,1}(y_q - 1) = 0 \mod e, \\ f_{p,2}(x_{p,2}, y_p) &= 1 + x_{p,2}(y_p - 1) = 0 \mod e, \end{aligned}$$

where the root is $(x_{q,1}, x_{p,2}, y_q, y_p) = (k_q, k_p, q, p)$.

In addition, by multiplying p and q to the key generation equations respectively, the following representations can be obtained:

$$\begin{aligned} ed_qp &= p + k_q(N-p) = N + (k_q - 1)(N-p), \\ ed_pq &= q + k_p(N-q) = N + (k_p - 1)(N-q). \end{aligned}$$

Then, we can also use the following modular equations:

$$\begin{aligned} f_{p,1}(x_{p,1}, y_p) &= N + x_{p,1}(N - y_p) = 0 \mod e, \\ f_{q,2}(x_{q,2}, y_q) &= N + x_{q,2}(N - y_q) = 0 \mod e, \end{aligned}$$

where the root is $(x_{p,1}, x_{q,2}, y_p, y_q) = (k_q - 1, k_p - 1, p, q)$.

To summarize the above discussion, we want to solve the following simultaneous modular equations:

$$\begin{aligned} f_{p,1}(x_{p,1}, y_p) &= N + x_{p,1}(N - y_p) = 0 \mod e, \\ f_{q,1}(x_{q,1}, y_q) &= 1 + x_{q,1}(y_q - 1) = 0 \mod e, \\ f_{p,2}(x_{p,2}, y_p) &= 1 + x_{p,2}(y_p - 1) = 0 \mod e, \end{aligned}$$

$$f_{q,2}(x_{q,2}, y_q) = N + x_{q,2}(N - y_q) = 0 \mod e,$$

where the root is $(x_{p,1}, x_{q,1}, x_{p,2}, x_{q,2}, y_p, y_q) = (k_q - 1, k_q, k_p, k_p - 1, p, q)$. Let $e = N^\alpha$, $d_p < N^\delta$, and $d_q < N^\delta$ for a balanced RSA, i.e, $q < p < 2q$. The absolute values of $x_{p,1}, x_{q,1}, x_{p,2}, x_{q,2}$ are bounded above by $X = N^{\alpha+\delta-1/2}$ within constant factors whereas the absolute values of y_p and y_q are bounded above by $Y = N^{1/2}$ within constant factors.

Unfortunately, an approach to solve the above four equations simultaneously does not offer an improvement. The approach gives us only the same bound as Theorem 3. Hence, we use an additional algebraic relation. From the CRT-RSA key generation,

$$\begin{aligned} & ed_q = 1 + k_q(q-1) \ \text{ and } \ ed_p = 1 + k_p(p-1), \\ \Leftrightarrow\ & k_q - 1 = k_q q \pmod e \ \text{ and } \ k_p - 1 = k_p p \pmod e. \end{aligned}$$

By multiplying these two equations, we obtain

$$(k_q - 1)(k_p - 1) = k_q k_p N \pmod e.$$

Then the following new equation can be obtained:

$$\begin{aligned} h(x_{p,1}, x_{q,1}, x_{p,2}, x_{q,2}) &= (N-1)x_{p,1}x_{p,2} + x_{p,1} + Nx_{p,2} = 0 \pmod e \\ &= (N-1)x_{q,1}x_{q,2} + Nx_{q,1} + x_{q,2} = 0 \pmod e. \end{aligned}$$

The polynomial also has two representations as the previous polynomials. Notice that the same equation as $h(x_{p,1}, x_{q,1}, x_{p,2}, x_{q,2})$ was already used by Galbraith et al. [14]. We make use of these equations and obtain the following result.

Theorem 5. *Let $N = pq$ be an RSA modulus where p and q are the same bit-size. Let $e = N^\alpha$ and $d_p, d_q < N^\delta$ be a public/CRT exponent respectively such that $ed_q = 1 \pmod{(q-1)}$ and $ed_p = 1 \pmod{(p-1)}$. Given public elements N and e, if*

$$\delta < \frac{1}{2} - \sqrt{\frac{\alpha}{6}} \ \text{ for } \ \alpha \geq \frac{3}{8},$$

then N can be factorized in polynomial time by assuming that polynomials which are derived from LLL reduced bases are algebraically independent.

For the full size e, the attack works for $\delta < 1/2 - 1/\sqrt{6} = 0.091\cdots$ which is better than Jochemsz-May's bound [22], i.e., $\delta < 0.073$. Our attack is better than all existing attacks.

Proof of Theorem 5. To solve the above modular equations, we use the following shift-polynomials:

$$\begin{aligned} & g_{[i_1,i_2,j_1,j_2,u]}(x_{p,1}, x_{q,1}, x_{p,2}, x_{q,2}, y_p, y_q) \\ :=& x_{p,1}^{j_1} x_{p,2}^{j_2} y_q^{\lfloor (i_1+i_2)/2 \rfloor} f_{p,1}^{i_1}(x_{p,1}, y_p) f_{p,2}^{i_2}(x_{p,2}, y_p) h^u(x_{p,1}, x_{p,2}, x_{q,1}, x_{q,2}). \end{aligned}$$

$$
\begin{aligned}
& e^{m-(i_1+i_2+u)}, \\
& g'_{[i_1,i_2,j_1],p}(x_{p,1},x_{q,1},x_{p,2},x_{q,2},y_p,y_q) \\
:=& y_q^{\lfloor (i_1+i_2)/2 \rfloor - j_1} f_{p,1}^{i_1}(x_{p,1},y_p) f_{p,2}^{i_2}(x_{p,2},y_p) e^{m-(i_1+i_2+u)}, \\
& g'_{[i_1,i_2,j_2],q}(x_{p,1},x_{q,1},x_{p,2},x_{q,2},y_p,y_q) \\
:=& y_q^{\lfloor (i_1+i_2)/2 \rfloor + j_2} f_{p,1}^{i_1}(x_{p,1},y_p) f_{p,2}^{i_2}(x_{p,2},y_p) e^{m-(i_1+i_2+u)},
\end{aligned}
$$

with some positive integer m. For non-negative integers i_1, i_2, j_1, i_2, and u, all the shift-polynomials share the common root as $f_{p,1}(x_{p,1}, y_p)$, $f_{p,2}(x_{p,2}, y_p)$, $f_{q,1}(x_{q,1}, y_q)$, $f_{q,2}(x_{q,2}, y_q)$, and $h(x_{p,1}, x_{q,1}, x_{p,2}, x_{q,2})$ modulo e^m. Then we can construct triangular basis matrices as follows.

Lemma 4. *Let all the polynomials be defined as above. Let τ be a constant such that $1/2 \le \tau \le 1$. Define sets of indices as*

$$
\mathcal{I}_x := \left\{ \begin{array}{c}
i_1 = 0,1,\ldots,m; i_2 = 0,1,\ldots,m-i_1; j_1 = j_2 = 0; \\
u = 0,1,\ldots,\lfloor \frac{m-(i_1+i_2)}{2} \rfloor, \ \textit{and} \\
i_1 = 0,1,\ldots,m-2; i_2 = 1,2,\ldots,m-1-i_1; j_1 = 1; \\
j_2 = 0; u = 0,1,\ldots,\lfloor \frac{m-1-(i_1+i_2)}{2} \rfloor, \ \textit{and} \\
i_1 = 0,1,\ldots,m; i_2 = 0; j_1 = 1,2,\ldots,m-i_1; j_2 = 0; \\
u = 0,1,\ldots,\lfloor \frac{m-(i_1+j_1)}{2} \rfloor, \ \textit{and} \\
i_1 = 0; i_2 = 0,1,\ldots,m; j_1 = 0; j_2 = 1,2,\ldots,m-i_2; \\
u = 0,1,\ldots,\lfloor \frac{m-(i_2+j_2)}{2} \rfloor,
\end{array} \right\},
$$

$$
\mathcal{I}_{y,p} := \left\{ \begin{array}{c}
i_1 = 0,1,\ldots,m; i_2 = 0,1,\ldots,m-i_1; \\
j_1 = 1,2,\ldots,\lceil \tau(i_1+i_2) \rceil - \lceil (i_1+i_2)/2 \rceil
\end{array} \right\},
$$

$$
\mathcal{I}_{y,q} := \left\{ \begin{array}{c}
i_1 = 0,1,\ldots,m; i_2 = 0,1,\ldots,m-i_1; \\
j_2 = 1,2,\ldots,\lceil \tau(i_1+i_2) \rceil - \lfloor (i_1+i_2)/2 \rfloor
\end{array} \right\}.
$$

Let $\boldsymbol{B}$ be a matrix whose rows consist of coefficients of $g_{[i_1,i_2,j_1,j_2,u]}(x_{p,1}X_{p,1}, x_{q,1}X_{q,1}, x_{p,2}X_{p,2}, x_{q,2}X_{q,2}, y_pY_p, y_qY_q)$, $g'_{[i_1,i_2,j_1],p}(x_{p,1}X_{p,1}, x_{q,1}X_{q,1}, x_{p,2}X_{p,2}, x_{q,2}X_{q,2}, y_pY_p, y_qY_q)$, and $g'_{[i_1,i_2,j_2],q}(x_{p,1}X_{p,1}, x_{q,1}X_{q,1}, x_{p,2}X_{p,2}, x_{q,2}X_{q,2}, y_pY_p, y_qY_q)$ with indices in $\mathcal{I}_x$, $\mathcal{I}_{y,p}$, and $\mathcal{I}_{y,q}$, respectively. If the shift-polynomials are ordered as

$$
\begin{aligned}
& g_{[i_1,i_2,j_1,j_2,u]} \prec g'_{[i_1,i_2,j_1],p}, g'_{[i_1,i_2,j_2],q}, \\
& g_{[i'_1,i'_2,j'_1,j'_2,u']} \prec g_{[i_1,i_2,j_1,j_2,u]} \textit{ for } i'_1+i'_2 < i_1+i_2, \\
& g_{[i'_1,i'_2,j'_1,j'_2,u']} \prec g_{[i_1,i_2,j_1,j_2,u]} \textit{ for } i'_1+i'_2 = i_1+i_2, u' < u, \\
& g_{[i'_1,i'_2,j'_1,0,u]} \prec g_{[i_1,i_2,j_1,0,u]} \textit{ for } i'_1+i'_2 = i_1+i_2, j'_1 < j_1, \\
& g_{[i'_1,i'_2,0,j'_2,u]} \prec g_{[i_1,i_2,0,j_2,u]} \textit{ for } i'_1+i'_2 = i_1+i_2, j'_2 < j_2, \\
& g'_{[i'_1,i'_2,j'_1]}, g'_{[i'_1,i'_2,j'_2],q} \prec g'_{[i_1,i_2,j_1],p}, g'_{[i_1,i_2,j_2],q} \textit{ for } i'_1+i'_2 < i_1+i_2, \\
& g'_{[i'_1,i'_2,j'_1]} \prec g'_{[i_1,i_2,j_1],p} \textit{ for } i'_1+i'_2 = i_1+i_2, j'_1 < j_1, \\
& g'_{[i'_1,i'_2,j'_2],q} \prec g'_{[i_1,i_2,j_2],q} \textit{ for } i'_1+i'_2 = i_1+i_2, j'_2 < j_2,
\end{aligned}
$$

and $N^{-1} \pmod{e^m}$ *is multiplied appropriately, then the matrix becomes triangular with diagonals*

- $X_{p,1}^{i_1+j_1+u} X_{p,2}^{i_2+j_2+u} Y_p^{\lceil (i_1+i_2)/2 \rceil} e^{m-(i_1+i_2+u)}$ *for* $g_{[i_1,i_2,j_1,j_2,u]}$ *if* i_1+i_2 *is odd,*
- $X_{q,1}^{i_1+j_1+u} X_{q,2}^{i_2+j_2+u} Y_q^{\lfloor (i_1+i_2)/2 \rfloor} e^{m-(i_1+i_2+u)}$ *for* $g_{[i_1,i_2,j_1,j_2,u]}$ *if* i_1+i_2 *is even,*
- $X_{p,1}^{i_1} X_{p,2}^{i_2} Y_p^{\lceil (i_1+i_2)/2 \rceil + j_1} e^{m-(i_1+i_2)}$ *for* $g'_{[i_1,i_2,j_1],p}$,
- $X_{q,1}^{i_1} X_{q,2}^{i_2} Y_q^{\lfloor (i_1+i_2)/2 \rfloor + j_2} e^{m-(i_1+i_2)}$ *for* $g'_{[i_1,i_2,j_2],q}$.

We do not prove the lemma, however, the proof can be obtained in the same manner as in Section 3.4. The polynomials which we use contain six variables $x_{p,1}, x_{p,2}, x_{q,1}, x_{q,2}, y_p, y_q$. Furthermore, there are three algebraic relations, i.e., $x_{q,1} = x_{p,1} + 1$, $x_{p,2} = x_{q,2} + 1$, and $y_p y_q = N$. By using the last relation, i.e., $y_p y_q = N$, we transform all monomials as they do not have both y_p and y_q simultaneously as the proof of Lemma 3. In addition, by using the other relations, i.e., $x_{q,1} = x_{p,1} + 1$ and $x_{p,2} = x_{q,2} + 1$, we transform all monomials as they do not have both $x_{p,1}$ and $x_{q,1}$ simultaneously or both $x_{p,2}$ and $x_{q,2}$ simultaneously. More concretely, the variables $x_{p,1}$ and $x_{p,2}$ appear only in monomials whose exponents of y_p are positive whereas the variables $x_{q,1}$ and $x_{q,2}$ appear only in monomials whose exponents of y_q are non-negative.

We compute the resulting condition of Theorem 5. The dimension n and the determinant of the lattice $\det(\boldsymbol{B}) = X^{s_X} Y^{s_Y} e^{s_e}$ can be computed as:

$$
\begin{aligned}
n =& \sum_{(i_1,i_2,j_1,j_2,u)\in\mathcal{I}_x} 1 + \sum_{(i_1,i_2,j_1)\in\mathcal{I}_{y,p}} 1 + \sum_{(i_1,i_2,j_2)\in\mathcal{I}_{y,q}} 1 \\
=& \frac{2\tau}{3} m^3 + o(m^3), \\
s_X =& \sum_{(i_1,i_2,j_1,j_2,u)\in\mathcal{I}_x} (i_1+i_2+j_1+j_2+2u) + \sum_{(i_1,i_2,j_1)\in\mathcal{I}_{y,p}} (i_1+i_2) \\
&+ \sum_{(i_1,i_2,j_2)\in\mathcal{I}_{y,q}} (i_1+i_2) \\
=& \frac{\tau}{2} m^4 + o(m^4), \\
s_Y =& \sum_{\substack{(i_1,i_2,j_1,j_2,u)\in \\ \mathcal{I}_x \text{ s.t. } i_1+i_2 \text{ is odd}}} \left\lceil \frac{i_1+i_2}{2} \right\rceil + \sum_{\substack{(i_1,i_2,j_1,j_2,u)\in \\ \mathcal{I}_x \text{ s.t. } i_1+i_2 \text{ is even}}} \left\lfloor \frac{i_1+i_2}{2} \right\rfloor \\
&+ \sum_{(i_1,i_2,j_1)\in\mathcal{I}_{y,p}} \left(\left\lceil \frac{i_1+i_2}{2} \right\rceil + j_1 \right) + \sum_{(i_1,i_2,j_2)\in\mathcal{I}_{y,q}} \left(\left\lfloor \frac{i_1+i_2}{2} \right\rfloor + j_2 \right) \\
=& \frac{\tau^2}{4} m^4 + o(m^4), \\
s_e =& \sum_{(i_1,i_2,j_1,j_2,u)\in\mathcal{I}_x} (m-(i_1+i_2+u)) + \sum_{(i_1,i_2,j_1)\in\mathcal{I}_{y,p}} (m-(i_1+i_2))
\end{aligned}
$$

$$+ \sum_{(i_1,i_2,j_2)\in\mathcal{I}_{y,q}} (m-(i_1+i_2))$$
$$= \frac{2\tau+1}{12} m^4 + o(m^4).$$

Applying the LLL reduction, the polynomials obtained from the output vectors satisfy Howgrave-Graham's lemma if $X^{s_X} Y^{s_Y} e^{s_e} < e^{nm}$, i.e.,

$$\left(\alpha+\delta-\frac{1}{2}\right)\frac{\tau}{2}+\frac{1}{2}\cdot\frac{\tau^2}{4}+\alpha\cdot\frac{2\tau+1}{12} < \alpha\cdot\frac{2\tau}{3}$$

by omitting low order terms of m. To minimize the left hand side of the inequality, we set the parameters $\tau = 1-2\delta$, then the condition becomes

$$\delta < \frac{1}{2} - \sqrt{\frac{\alpha}{6}}$$

as required. To satisfy the restriction $\tau \geq 1/2$, $\delta \leq 1/4$ and equivalently $\alpha \geq 3/8$ should hold. □

4.2 Experimental results

We have implemented the experiment program of Section 4.1 in Magma 2.10 computer algebra system [6] on a PC with Intel(R) Core(TM) Duo CPU(3.30GHz, 4.0GB RAM Windows 7). Table 3 lists the asymptotic and experimental results on factoring 1000-bit RSA moduli with varying dimension of lattice under small decryption exponents. In all experiments, we successfully find the factorization of these RSA moduli.

5 Attacks on the Variants

In this section, we study small CRT-exponent attacks on the RSA variants, i.e., the Multi-Prime RSA, Takagi's RSA, and the RSA with multiple exponent pairs. We extend our attack of Theorem 2 to the variants.

5.1 Multi-Prime RSA

In this section, we extends the small CRT-exponent attack for the Multi-Prime RSA as follows.

Table 3. For 1000-bit RSA moduli, asymptotic and experimental comparisons of small d_p and d_q attacks on balanced CRT-RSA

Bitsize of N	Asymptotic	Expt.	(m,dim.)	L^3 time (in sec.)
1000	0.091	0.034	(4,95)	358.787
		0.053	(6,252)	31390.147

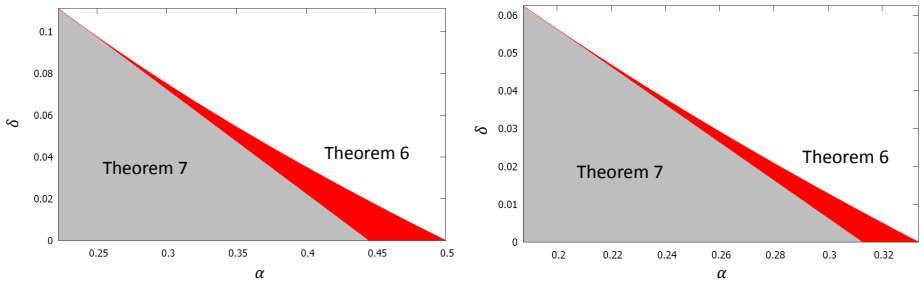

Fig. 4. Comparisons between our attacks of Theorem 6 and 7. The left and the right figure is for $r = 3$ and 4, respectively.

Theorem 6. *Let $N = \prod_{i=1}^{r} p_i$ be an RSA modulus where $r \geq 2$ and all the prime factors $p_1, \ldots, p_r$ are the same bit-size. Let $e = N^{\alpha}$ and $d_{p_i} < N^{\delta_i}$ be a public/CRT exponent respectively such that $ed_{p_i} = 1 \pmod{(p_i - 1)}$ for all $i = 1, \ldots, r$. Given public elements N and e, if*

$$\min_{i \in \{1,\ldots,r\}} \delta_i < \frac{1 - \sqrt{(r-1)\alpha}}{r} \quad \text{for} \quad \alpha > \frac{r-1}{r^2},$$

then N can be factorized in polynomial time by assuming that polynomials which are derived from LLL reduced bases are algebraically independent.

We can successfully extend an attack for the Multi-Prime RSA in the sense that Theorem 6 becomes the same as Theorem 3 for $r = 2$.

We also extend May's modulo p_i attack [29] for the Multi-Prime RSA as follows.

Theorem 7 (Adapted from [28]). *Let $N = \prod_{i=1}^{r} p_i$ be an RSA modulus where $r \geq 2$ and all the prime factors $p_1, \ldots, p_r$ are the same bit-size. Let $e = N^{\alpha}$ and $d_{p_i} < N^{\delta_i}$ be a public/CRT exponent respectively such that $ed_{p_i} = 1 \pmod{(p_i - 1)}$ for all $i = 1, \ldots, r$. Given public elements N and e, if*

$$\min_{i \in \{1,\ldots,r\}} \delta_i < \frac{r + 1 - r^2\alpha}{2r^2},$$

then N can be factorized in polynomial time by assuming that polynomials which are derived from LLL reduced bases are algebraically independent.

We can successfully extend an attack for the Multi-Prime RSA in the sense that Theorem 7 becomes the same as Theorem 4 for $r = 2$. We omit the proof since it is almost the same as Theorem 9 of [28]. The bound of Theorem 6 is always better than or equal to that of Theorem 7. Figure 4 compares the attack condition between Theorem 6 and 7 for $r = 3$ and 4.

5.2 Takagi's RSA

In this section, we extends the small CRT-exponent attack for Takagi's RSA as follows.

Theorem 8. *Let $N = p^r q$ be an RSA modulus where $r \geq 1$ and the prime factors p and q are the same bit-size. Let $e = N^{\alpha}$ and $d_p < N^{\delta_p}, d_q < N^{\delta_q}$ be a public/CRT exponent respectively such that $ed_p = 1 \pmod{(p-1)}$ and $ed_q = 1 \pmod{(q-1)}$. Given public elements N and e, if*

$$\min\{\delta_p, \delta_q\} < \frac{1 - \sqrt{r\alpha}}{r+1} \quad \textit{for} \quad \alpha > \frac{r}{(r+1)^2},$$

then N can be factorized in polynomial time by assuming that polynomials which are derived from LLL reduced bases are algebraically independent.

We can successfully extend an attack for Takagi's RSA in the sense that Theorem 8 becomes the same as Theorem 3 for $r = 1$. Although Shinohara et al. [39] extended Bleichenbacher-May's attack, our attack is always better.

We also extend May's modulo a prime factor attack [29] for Takagi's RSA as follows.

Theorem 9 (Adapted from [29]). *Let $N = p^r q$ be an RSA modulus where $r \geq 1$ and the prime factors p and q are the same bit-size. Let $e = N^{\alpha}$ and $d_p < N^{\delta_p}, d_q < N^{\delta_q}$ be a public/CRT exponent respectively such that $ed_p = 1 \pmod{(p-1)}$ and $ed_q = 1 \pmod{(q-1)}$. Given public elements N and e, if*

$$\delta_p < \frac{2r + 1 - (r+1)^2\alpha}{2(r+1)^2} \text{ or } \delta_q < \frac{r + 2 - (r+1)^2\alpha}{2(r+1)^2},$$

then N can be factorized in polynomial time by assuming that polynomials which are derived from LLL reduced bases are algebraically independent.

We can successfully extend an attack for the Takagi's RSA in the sense that Theorem 9 becomes the same as Theorem 4 for $r = 1$. We omit the proof since it is almost the same as Theorem 9 of [28]. The bound for δ_q of Theorem 8 is always better than or equal to that of Theorem 9, however, the bound for δ_p of Theorem 9 is better than or equal to that of Theorem 8. Figure 5 compares the attack condition for small d_p between Theorem 8 and 9 for $r = 2$ and 3.

5.3 RSA with Multiple Exponent Pairs

In this section, we extends the small CRT-exponent attack for the RSA with multiple exponent pairs as follows.

Theorem 10. *Let $N = pq$ be an RSA modulus where the prime factors p and q are the same bit-size. Let $e_\ell = N^{\alpha}$ and $d_{q,\ell} < N^{\delta}$ for $\ell = 1, \ldots, r$ be a*

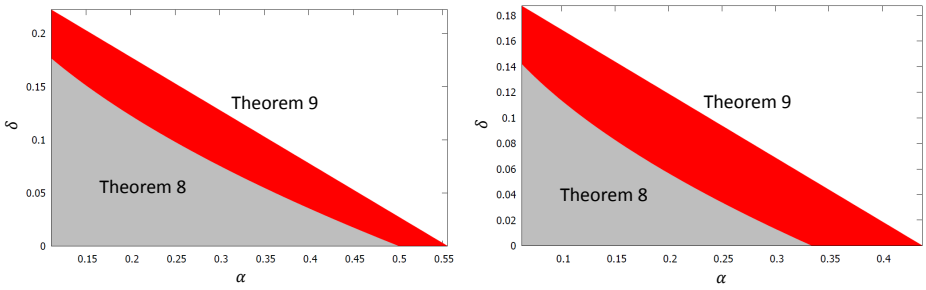

Fig. 5. Comparisons between our attacks of Theorem 8 and 9. The left and the right figure is for $r = 2$ and 3, respectively.

public/CRT exponent respectively such that $e_\ell d_{q,\ell} = 1 \pmod{(q-1)}$. *Given public elements* N *and* $e_1, \ldots, e_r$, *if*

$$\delta < \frac{1}{2} - \sqrt{\frac{\alpha}{3r+1}},$$

then N *can be factorized in time polynomial in input length and exponential in* r *by assuming that polynomials which are derived from LLL reduced bases are algebraically independent.*

We can successfully extend the attack for RSA with multiple exponent pairs in the sense that Theorem 10 becomes the same as Theorem 3 for $r = 1$. We do not think May's modulo q approach is an appropriate way for the attack scenario, hence, we do not extend it. Peng et al. proposed the attack (Theorem 2 of [34]) which extended Bleichenbacher-May's [3] and works when $\delta < (9r-14)/(24r+8)$ for an $\alpha = 1$. Theorem 10 is always better than the attack of Peng et al. Indeed, even if there are infinitely many exponent pairs r, the attack of Peng et al. works for $\delta < 3/8$ whereas our attack works for the same bound of δ with only 21 exponent pairs. Figure 6 compares recoverable sizes of d_q between our attack and that of Peng et al. [34].

6 Concluding Remarks

In this paper, we studied a lattice-based cryptanalysis of the small CRT-exponent RSA. We developed a novel lattice construction technique that is specialized to the CRT-RSA key generation and proposed several improved attacks. When a prime factor p is significantly smaller than the other prime factor q with a small d_q, we solved an open problem which was claimed in [3,29]; we proposed an attack that works for $p < N^{0.5}$. When both d_p and d_q are small, we proposed an attack that works for $d_p, d_q < N^{0.091}$ with a full size e. We also proposed attacks on the RSA variants, i.e., the Multi-Prime RSA, Takagi's RSA, and RSA with multiple exponent pairs.

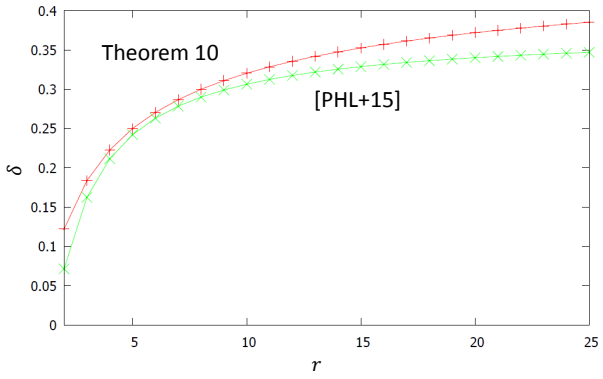

Fig. 6. Comparison between our attack (Theorem 10) and the attack of Peng et al. [34]

Acknowledgement. We would like to thank Shuichi Katsumata for his helpful comments. Atsushi Takayasu is supported by a JSPS Fellowship for Young Scientists. This research was supported by CREST, JST, JSPS KAKENHI Grant Number 14J08237, National Key Basic Research Program of China (2013CB834203) and the National Natural Science Foundation of China (Grants 61472417, 61632020, 61472416).

References

1. Aono, Y.: Minkowski sum based lattice construction for multivariate simultaneous coppersmith's technique and applications to RSA. In: Boyd, C., Simpson, L. (eds.) Information Security and Privacy - 18th Australasian Conference, ACISP 2013. Lecture Notes in Computer Science, vol. 7959, pp. 88–103. Springer (2013)
2. Bauer, A., Vergnaud, D., Zapalowicz, J.: Inferring sequences produced by nonlinear pseudorandom number generators using coppersmith's methods. In: Fischlin, M., Buchmann, J.A., Manulis, M. (eds.) Public Key Cryptography - PKC 2012. Lecture Notes in Computer Science, vol. 7293, pp. 609–626. Springer (2012)
3. Bleichenbacher, D., May, A.: New attacks on RSA with small secret CRT-exponents. In: Yung, M., Dodis, Y., Kiayias, A., Malkin, T. (eds.) Public Key Cryptography - PKC 2006. Lecture Notes in Computer Science, vol. 3958, pp. 1–13. Springer (2006)
4. Blömer, J., May, A.: New partial key exposure attacks on RSA. In: Boneh, D. (ed.) Advances in Cryptology - CRYPTO 2003. Lecture Notes in Computer Science, vol. 2729, pp. 27–43. Springer (2003)
5. Boneh, D., Durfee, G.: Cryptanalysis of RSA with private key d less than $N^{0.292}$. IEEE Trans. Information Theory 46(4), 1339–1349 (2000)
6. Bosma, W., Cannon, J.J., Playoust, C.: The magma algebra system I: the user language. J. Symb. Comput. 24(3/4), 235–265 (1997)
7. Coppersmith, D.: Finding a small root of a bivariate integer equation; factoring with high bits known. In: Maurer, U.M. (ed.) Advances in Cryptology - EURO-

CRYPT '96. Lecture Notes in Computer Science, vol. 1070, pp. 178–189. Springer (1996)
8. Coppersmith, D.: Finding a small root of a univariate modular equation. In: Maurer, U.M. (ed.) Advances in Cryptology - EUROCRYPT '96. Lecture Notes in Computer Science, vol. 1070, pp. 155–165. Springer (1996)
9. Coppersmith, D.: Small solutions to polynomial equations, and low exponent RSA vulnerabilities. J. Cryptology 10(4), 233–260 (1997)
10. Coppersmith, D.: Finding small solutions to small degree polynomials. In: Silverman, J.H. (ed.) Cryptography and Lattices, International Conference, CaLC 2001. Lecture Notes in Computer Science, vol. 2146, pp. 20–31. Springer (2001)
11. Coron, J.: Finding small roots of bivariate integer polynomial equations revisited. In: Cachin, C., Camenisch, J. (eds.) Advances in Cryptology - EUROCRYPT 2004. Lecture Notes in Computer Science, vol. 3027, pp. 492–505. Springer (2004)
12. Durfee, G., Nguyen, P.Q.: Cryptanalysis of the RSA schemes with short secret exponent from asiacrypt '99. In: Okamoto, T. (ed.) Advances in Cryptology - ASIACRYPT 2000. Lecture Notes in Computer Science, vol. 1976, pp. 14–29. Springer (2000)
13. Esgin, M.F., Kiraz, M.S., Uzunkol, O.: A new partial key exposure attack on multi-power RSA. In: Maletti, A. (ed.) Algebraic Informatics - 6th International Conference, CAI 2015. Lecture Notes in Computer Science, vol. 9270, pp. 103–114. Springer (2015)
14. Galbraith, S.D., Heneghan, C., McKee, J.F.: Tunable balancing of RSA. In: Boyd, C., Nieto, J.M.G. (eds.) Information Security and Privacy, 10th Australasian Conference, ACISP 2005. Lecture Notes in Computer Science, vol. 3574, pp. 280–292. Springer (2005)
15. Herrmann, M.: Lattice-based Cryptanalysis Using Unravelled Linearization. Ph.D. thesis, der Ruhr-Universitat Bochum (2011)
16. Herrmann, M., May, A.: Attacking power generators using unravelled linearization: When do we output too much? In: Matsui, M. (ed.) Advances in Cryptology - ASIACRYPT 2009. Lecture Notes in Computer Science, vol. 5912, pp. 487–504. Springer (2009)
17. Herrmann, M., May, A.: Maximizing small root bounds by linearization and applications to small secret exponent RSA. In: Nguyen, P.Q., Pointcheval, D. (eds.) Public Key Cryptography - PKC 2010. Lecture Notes in Computer Science, vol. 6056, pp. 53–69. Springer (2010)
18. Howgrave-Graham, N.: Finding small roots of univariate modular equations revisited. In: Darnell, M. (ed.) Cryptography and Coding, 6th IMA International Conference. Lecture Notes in Computer Science, vol. 1355, pp. 131–142. Springer (1997)
19. Huang, Z., Hu, L., Xu, J.: Attacking RSA with a composed decryption exponent using unravelled linearization. In: Lin, D., Yung, M., Zhou, J. (eds.) Information Security and Cryptology - 10th International Conference, Inscrypt 2014. Lecture Notes in Computer Science, vol. 8957, pp. 207–219. Springer (2014)
20. Huang, Z., Hu, L., Xu, J., Peng, L., Xie, Y.: Partial key exposure attacks on takagi's variant of RSA. In: Boureanu, I., Owesarski, P., Vaudenay, S. (eds.) Applied Cryptography and Network Security - 12th International Conference, ACNS 2014. Lecture Notes in Computer Science, vol. 8479, pp. 134–150. Springer (2014)
21. Jochemsz, E., May, A.: A strategy for finding roots of multivariate polynomials with new applications in attacking RSA variants. In: Lai, X., Chen, K. (eds.) Advances in Cryptology - ASIACRYPT 2006. Lecture Notes in Computer Science, vol. 4284, pp. 267–282. Springer (2006)

22. Jochemsz, E., May, A.: A polynomial time attack on RSA with private CRT-exponents smaller than $N^{0.073}$. In: Menezes, A. (ed.) Advances in Cryptology - CRYPTO 2007. Lecture Notes in Computer Science, vol. 4622, pp. 395–411. Springer (2007)
23. Kunihiro, N.: On optimal bounds of small inverse problems and approximate GCD problems with higher degree. In: Gollmann, D., Freiling, F.C. (eds.) Information Security - 15th International Conference, ISC 2012. Lecture Notes in Computer Science, vol. 7483, pp. 55–69. Springer (2012)
24. Kunihiro, N., Shinohara, N., Izu, T.: A unified framework for small secret exponent attack on RSA. IEICE Transactions 97-A(6), 1285–1295 (2014)
25. Lenstra, A., Lenstra, H., Lovász, L.: Factoring polynomials with rational coefficients. Math. Ann. 261, 515–534 (1982)
26. Lu, Y., Zhang, R., Lin, D.: Factoring multi-power RSA modulus $N = p^r q$ with partial known bits. In: Boyd, C., Simpson, L. (eds.) Information Security and Privacy - 18th Australasian Conference, ACISP 2013. Lecture Notes in Computer Science, vol. 7959, pp. 57–71. Springer (2013)
27. Lu, Y., Zhang, R., Lin, D.: New partial key exposure attacks on CRT-RSA with large public exponents. In: Boureanu, I., Owesarski, P., Vaudenay, S. (eds.) Applied Cryptography and Network Security - 12th International Conference, ACNS 2014. Lecture Notes in Computer Science, vol. 8479, pp. 151–162. Springer (2014)
28. Lu, Y., Zhang, R., Peng, L., Lin, D.: Solving linear equations modulo unknown divisors: Revisited. In: Iwata, T., Cheon, J.H. (eds.) Advances in Cryptology - ASIACRYPT 2015. Lecture Notes in Computer Science, vol. 9452, pp. 189–213. Springer (2015)
29. May, A.: Cryptanalysis of unbalanced RSA with small CRT-exponent. In: Yung, M. (ed.) Advances in Cryptology - CRYPTO 2002. Lecture Notes in Computer Science, vol. 2442, pp. 242–256. Springer (2002)
30. May, A.: New RSA vulnerabilities using lattice reduction methods. Ph.D. thesis, University of Paderborn (2003)
31. May, A.: Using LLL-reduction for solving RSA and factorization problems. In: Nguyen, P.Q., Vallée, B. (eds.) The LLL Algorithm - Survey and Applications, pp. 315–348. Information Security and Cryptography, Springer (2010)
32. Nguyen, P.Q., Stern, J.: The two faces of lattices in cryptology. In: Silverman, J.H. (ed.) Cryptography and Lattices, International Conference, CaLC 2001. Lecture Notes in Computer Science, vol. 2146, pp. 146–180. Springer (2001)
33. Peng, L., Hu, L., Huang, Z., Xu, J.: Partial prime factor exposure attacks on RSA and its takagi's variant. In: Lopez, J., Wu, Y. (eds.) Information Security Practice and Experience - 11th International Conference, ISPEC 2015. Lecture Notes in Computer Science, vol. 9065, pp. 96–108. Springer (2015)
34. Peng, L., Hu, L., Lu, Y., Sarkar, S., Xu, J., Huang, Z.: Cryptanalysis of variants of RSA with multiple small secret exponents. In: Biryukov, A., Goyal, V. (eds.) Progress in Cryptology - INDOCRYPT 2015. Lecture Notes in Computer Science, vol. 9462, pp. 105–123. Springer (2015)
35. Quisquater, J.J., Couvreur, C.: Fast decipherment algorithm for RSA public-key cryptosystem. Electronics Letters 18, 905–907(2) (October 1982)
36. Sarkar, S.: Small secret exponent attack on RSA variant with modulus $N = p^r q$. Des. Codes Cryptography 73(2), 383–392 (2014)
37. Sarkar, S.: Revisiting prime power RSA. Discrete Applied Mathematics 203, 127–133 (2016)

38. Sarkar, S., Maitra, S.: Partial key exposure attack on CRT-RSA. In: Abdalla, M., Pointcheval, D., Fouque, P., Vergnaud, D. (eds.) Applied Cryptography and Network Security, 7th International Conference, ACNS 2009. Lecture Notes in Computer Science, vol. 5536, pp. 473–484 (2009)
39. Shinohara, N., Izu, T., Kunihiro, N.: Small secret CRT-exponent attacks on takagi's RSA. IEICE Transactions 94-A(1), 19–27 (2011)
40. Sun, H., Wu, M.: An approach towards rebalanced RSA-CRT with short public exponent. IACR Cryptology ePrint Archive 2005, 53 (2005)
41. Takayasu, A., Kunihiro, N.: Better lattice constructions for solving multivariate linear equations modulo unknown divisors. IEICE Transactions 97-A(6), 1259–1272 (2014)
42. Takayasu, A., Kunihiro, N.: Cryptanalysis of RSA with multiple small secret exponents. In: Susilo, W., Mu, Y. (eds.) Information Security and Privacy - 19th Australasian Conference, ACISP 2014. Lecture Notes in Computer Science, vol. 8544, pp. 176–191. Springer (2014)
43. Takayasu, A., Kunihiro, N.: General bounds for small inverse problems and its applications to multi-prime RSA. In: Lee, J., Kim, J. (eds.) Information Security and Cryptology - ICISC 2014. Lecture Notes in Computer Science, vol. 8949, pp. 3–17. Springer (2014)
44. Takayasu, A., Kunihiro, N.: Partial key exposure attacks on RSA: achieving the boneh-durfee bound. In: Joux, A., Youssef, A.M. (eds.) Selected Areas in Cryptography - SAC 2014. Lecture Notes in Computer Science, vol. 8781, pp. 345–362. Springer (2014)
45. Takayasu, A., Kunihiro, N.: Partial key exposure attacks on CRT-RSA: better cryptanalysis to full size encryption exponents. In: Malkin, T., Kolesnikov, V., Lewko, A.B., Polychronakis, M. (eds.) Applied Cryptography and Network Security - 13th International Conference, ACNS 2015. Lecture Notes in Computer Science, vol. 9092, pp. 518–537. Springer (2015)
46. Takayasu, A., Kunihiro, N.: How to generalize RSA cryptanalyses. In: Cheng, C., Chung, K., Persiano, G., Yang, B. (eds.) Public-Key Cryptography - PKC 2016. Lecture Notes in Computer Science, vol. 9615, pp. 67–97. Springer (2016)
47. Takayasu, A., Kunihiro, N.: Partial key exposure attacks on CRT-RSA: general improvement for the exposed least significant bits. In: Bishop, M., Nascimento, A.C.A. (eds.) Information Security - 19th International Conference, ISC 2016. Lecture Notes in Computer Science, vol. 9866, pp. 35–47. Springer (2016)
48. Takayasu, A., Kunihiro, N.: Partial key exposure attacks on RSA with multiple exponent pairs. In: Liu, J.K., Steinfeld, R. (eds.) Information Security and Privacy - 21st Australasian Conference, ACISP 2016. Lecture Notes in Computer Science, vol. 9723, pp. 243–257. Springer (2016)
49. Takayasu, A., Kunihiro, N.: A tool kit for partial key exposure attacks on RSA. In: Handschuh, H. (ed.) Topics in Cryptology - CT-RSA 2017, The Cryptographers' Track at the RSA Conference 2017. Lecture Notes in Computer Science, vol. 10159, pp. 58–73. Springer (2017)
50. Wiener, M.J.: Cryptanalysis of short RSA secret exponents. IEEE Trans. Information Theory 36(3), 553–558 (1990)