# New Partial Key Exposure Attacks on CRT-RSA with Large Public Exponents

Yao Lu[1,2,⋆], Rui Zhang[1,⋆], and Dongdai Lin[1]

[1] State Key Laboratory of Information Security (SKLOIS)
Institute of Information Engineering (IIE)
Chinese Academy of Sciences (CAS)
[2] University of Chinese Academy of Sciences (UCAS)
lywhhit@gmail.com, {r-zhang,ddlin}@iie.ac.cn

**Abstract.** In Crypto'03, Blömer and May provided several partial key exposure attacks on CRT-RSA. In their attacks, they suppose that an attacker can either succeed to obtain the most significant bits (MSBs) or the least significant bits (LSBs) of $d_p = d \mod (p-1)$ in consecutive order. For the case of known LSBs of $d_p$, their algorithm is polynomial-time only for small public exponents $e$ (i.e. $e = \text{poly}(\log N)$). However, in some practical applications, we prefer to use large $e$ (Like $e \approx d_p$, to let the public and private operations with the same computational effort). In this paper, we propose some lattice-based attacks for this extended setting. For known LSBs case, we introduce two approaches that work up to $e < N^{\frac{3}{8}}$. Similar results (though not as strong) are obtained for MSBs case. We also provide detailed experimental results to justify our claims.

**Keywords:** lattices, RSA, Coppersmith's method.

## 1 Introduction

Let $N = pq$ be an RSA modulus where $p$, $q$ are of the same bitsize. The public exponent $e$ and private exponent $d$ satisfy $ed - 1 \equiv 0 \mod (p-1)(q-1)$. Since the decryption/signing in RSA require taking heavy exponential multiplication modulus of $N$, low efficiency became a bottleneck of using RSA cryptosystem.

Perhaps the most straightforward solution to speed up RSA decryption/signing process is to choose small $d$. However, in 1991, Wiener [24] showed that if $d < N^{0.25}$ then the factorization of $N$ can be found in polynomial-time. Later, Boneh and Durfee [2] improved Wiener's bound to $d < N^{0.292}$, in their attack, the proof of the final bound is complicated. Recently, a simple and elementary proof is given to achieve Boneh-Durfee's bound [9,14].

Another sophisticated approach, proposed by Quisquater and Couvreur [18], is to use the Chinese Remainder Theorem (CRT) for decryption/signing. In this case, the public exponent $e$ and private CRT-exponents $d_p$ and $d_q$ satisfy

$$\begin{aligned} ed_p &\equiv 1 \mod (p-1) \\ ed_q &\equiv 1 \mod (q-1) \end{aligned}$$

[⋆] Corresponding author.

I. Boureanu, P. Owesarski, and S. Vaudenay (Eds.): ACNS 2014, LNCS 8479, pp. 151–162, 2014.

In [24], Wiener stated that decryption/signing time can be further reduced if we use small private CRT-exponents. However, there are several attacks that can break CRT-RSA if the CRT-exponents are sufficiently small. In Crypto'02, May [16] described two attacks when the smaller prime factor is less than $N^{0.382}$. Later, in PKC'06, Bleichenbacher and May [1] improved May's bound to $N^{0.468}$. These two attacks focus on the special case where $p$ and $q$ are unbalanced. In Crypto'07, Jochemsz and May [12] presented an attack on the case of $p$ and $q$ are balanced and $e$ is full size (i.e. $e \approx N$), they showed that CRT-RSA can be broken when $d_p$ and $d_q$ are smaller than $N^{0.073}$.

**Partial Key Exposure Attacks on RSA.** Even if we choose to use large private exponents, in implementations, it may leaks some bits of the private key, we can still recover the entire private key from this knowledge. This is known as partial key exposure attack. Actually small private key attacks can be seen as partial key exposure attacks where MSBs of the private exponent are known to be equal to zero. In Asiacrypt'98, Boneh, Durfee and Frankel [3] presented several attacks on RSA where the attacker gains knowledge of MSBs or LSBs of $d$. In their attacks, the public exponent $e$ must be relatively small. In Crypto'03, Blömer and May [11] described several attacks for larger values of public exponent $e$. Further in Eurocrypt'05, Ernst et al. [5] extended these attacks to work up to full size $e$. As a follow-up work of [5], recently, Joye and Lepoint [13] provided several attacks on the practical setting of a private exponent $d$ larger than the modulus $N$.

**Partial Key Exposure Attacks on CRT-RSA.** In Crypto'03, Blömer and May [11] provided some partial key exposure attacks on CRT-RSA. Suppose $d_p \approx p$, they showed that for small public exponents $e$ (i.e. $e = \text{poly}(\log N)$), known half of the LSBs of $d_p$ are sufficient to factorize $N$.

Later in PKC'04, May [17] generalized Blömer-May's results [11] to the multi-power RSA [20] (Takagi's scheme: Modulus $N = p^r q$ $(r \geq 2)$). Using Boneh, Durfee and Howgrave-Graham's result [4], May presented polynomial-time attacks that need only a fraction of $\frac{1}{r+1}$ of the MSBs or LSBs of $d_p(d_p \approx p)$ to factor $N$ when the public exponent $e$ is small.

In ACNS'09, Sarkar and Maitra [19] provided another partial key exposure attack on CRT-RSA. In their attack, they assume that certain amounts of MSBs of $d_p$ and $d_q$ are exposed. Actually their attack can be regard as an extension of Jochemsz-May's attack [12].

### 1.1 Our Contribution

In this paper, we present two extended polynomial-time attacks that even works for all $e < N^{\frac{3}{8}}$ when certain amounts of LSBs of $d_p$ are exposed. Moreover, in our attacks, the upper bound of $e$ can be further improved if one uses a small secret CRT-exponent $d_p$. As an immediate application, we can utilize our approach to analyze Tunable Balancing of RSA which was introduced by Galbraith et al. [6] in ACISP'05. Moreover, for known MSBs of $d_p$, we can extend the results of [11] to any small secret exponents $d_p$. We also point out that there are close relations between our technique and the algorithm of Blömer and May [11].

Additionally, our technique can be easily extended to improve May's attack [17] on Takagi's scheme. However, Takagi's scheme requires the public exponent $e$ extremely small to make the decryption efficient (In the Hensel lifting Step in Decryption, $r-1$ modular exponentiations with exponent $e$ need to be done). Therefore, we do not discuss these extensions in this paper.

**Experimental Results.** For all these attacks, we carry out experiments to verify the effectiveness of our algorithms, which are depicted in Sec. 5 in detail. These experimental results demonstrate that our attacks are effective.

## 2 Preliminaries

### 2.1 Lattices

Our attacks are based on the techniques that rely on lattice basis reduction. In this section, we review some basic background information about lattices and lattice basis reduction.

A lattice is a discrete additive subgroup of $\mathbb{R}^n$. For our purpose, given $m \le n$ linearly independent vectors $b_1, \dots, b_m \in \mathbb{R}^n$, the set

$$\mathcal{L} = \mathcal{L}(b_1, \dots, b_m) = \{\sum_{i=1}^{m} \alpha_i b_i | \alpha_i \in \mathbb{Z}\}$$

is a lattice. The $b_i$ are called the basis vectors of $\mathcal{L}$ and $\mathcal{B} = \{b_i, \dots, b_m\}$ is called a lattice basis for $\mathcal{L}$. The determinant of a lattice is defined as $\det(\mathcal{L}) = \det(BB^t)^{\frac{1}{2}}$. When the lattice is full-rank ($m = n$), the formula simplifies to $\det(\mathcal{L}) = |\det B|$.

An important class of reduced basis, are LLL-algorithm, named after Lenstra, Lenstra and Lovász [15]. The following lemma gives bounds on LLL-reduced basis vectors.

**Lemma 1 (LLL [15]).** *Let $\mathcal{L}$ be a lattice of dimension $w$. Within polynomial-time, LLL-algorithm outputs a set of reduced basis vectors $v_i$, $1 \leqslant i \leqslant w$ that satisfies*

$$||v_1|| \leqslant ||v_2|| \leqslant \cdots \leqslant ||v_i|| \leqslant 2^{\frac{w(w-1)}{4(w+1-i)}} \det(\mathcal{L})^{\frac{1}{w+1-i}}$$

We also state a useful lemma from Howgrave-Graham [10]. Let $g(x_1, \cdots, x_k) = \sum_{i_1, \cdots, i_k} a_{i_1, \cdots, i_k} x_1^{i_1} \cdots x_k^{i_k}$. We define the norm of $g$ by the Euclidean norm of its coefficient vector: $||g||^2 = \sum_{i_1, \cdots, i_k} a_{i_1, \cdots, i_k}^2$.

**Lemma 2 (Howgrave-Graham [10]).** *Let $g(x_1, \cdots, x_k) \in \mathbb{Z}[x_1, \cdots, x_k]$ be an integer polynomial that consists of at most $w$ monomials. Suppose that*

1. *$g(y_1, \cdots, y_k) = 0 \bmod p^m$ for $| y_1 | \leqslant X_1, \cdots, | y_k | \leqslant X_k$ and*
2. *$||g(x_1 X_1, \cdots, x_k X_k)|| < \frac{p^m}{\sqrt{w}}$*

*Then $g(y_1, \cdots, y_k) = 0$ holds over integers.*

Our attacks rely on a well-known assumption which was widely used in the literature [5,2,8].

**Assumption 1.** *The lattice-based construction yields algebraically independent polynomials. The common roots of these polynomials can be efficiently computed using the* Gröbner basis technique.

### 2.2 Blömer-May's Partial Key Exposure Attacks on CRT-RSA

In [11], Blömer and May proposed two partial key exposure attacks on CRT-RSA. Following we list their results.

**Theorem 1 (LSBs).** *Let $(N, e)$ be an RSA public key with $N = pq$ and secret key $d$. Let $d_p = d \mod (p-1)$. Given $d_0, M$ with $d_0 = d_p \mod M$ and*

$$M > N^{\frac{1}{4}}$$

*Then the factorization of $N$ can be found in time $e \cdot poly(\log N)$.*

**Theorem 2 (MSBs).** *Let $(N, e)$ be an RSA public key with $N = pq$ and secret key $d$ and $e = N^{\alpha}$ for some $\alpha \in [0, \frac{1}{4}]$. Furthermore, let $d_p = d \mod (p-1)$. Given $\tilde{d}$ with*

$$|d_p - \tilde{d}| \le N^{\frac{1}{4} - \alpha}$$

*Then $N$ can be factored in polynomial-time.*

### 2.3 Finding Small Root of Bivariate Linear Equations

In Asiacrypt'08, Herrmann and May [8] gave an upper bound on the solutions of a bivariate linear equations modulo an unknown divisor of a known composite, which can also be extended to multivariate linear equations. Recently in ACISP'13 [21], Takayasu and Kunihiro improved Herrman-May's results by taking into account the sizes of the root bound. In this paper we used their approach to find small root of our attack polynomial.

**Theorem 3 (Herrmann-May-Takayasu-Kunihiro).** *Let $N$ be a sufficiently large composite integer (of unknown factorization) with a divisor $p \ge N^{\beta}$. Let $f(x_1, x_2) \in \mathbb{Z}[x_1, x_2]$ be a linear polynomial in two variables. Under Assumption 1, we can find all the solutions $(y_1, y_2)$ of the equation $f(x_1, x_2) = 0 \bmod p$ with $|y_1| \le N^{\gamma}$ and $|y_2| \le N^{\delta}$ (Suppose $\delta > \gamma$) if*

$$\begin{cases} \gamma + \delta \le 3\beta - 2 + 2(1-\beta)^{\frac{3}{2}} & \text{if } \delta < \beta(1 - \sqrt{1-\beta}) \\ \delta(3\beta - \gamma - 2\sqrt{\delta - \gamma}) < \beta^3 & \text{if } \beta^2 > \delta > \beta(1 - \sqrt{1-\beta}) \end{cases}$$

*The time and space complexities of the algorithm are polynomial in $\log N$.*

# 3 Key Recovery from Known LSBs

In this section, we assume that the attacker succeeded in getting the least significant bits of $d_p$

$$d_p = d_1 M + d_0$$

where $d_0$ is known to the attacker, together with its higher bound $M$, but $d_1$ is unknown. (In a special case of known LSBs, $M$ is a power of two.)

## 3.1 The Description of Our Attacks

In Crypto'03, Blömer and May [11] showed that if half of the lower bits of $d_p$ ($d_p \approx p$) are known, one can factorize $N$ in time $e \cdot \text{poly}(\log N)$. Obviously their attack is of exponential time when the public exponent $e$ is large. However, in some practical applications we need large $e$ (Like $e \approx \sqrt{d_p}$) to satisfy our specific requirements, e.g., Galbraith et al.'s scheme [6] in ACISP'05. In such a situation, the attack of [11] will not work.

We propose two polynomial-time attacks for the case of large $e$. Our attacks are based on Coppersmith's method for finding small roots of modular equations. The fist step of our attacks is to derive, from an CRT-RSA equation, a multivariate polynomial in some of the unknowns of CRT-RSA parameters, like $p, d_p$.

Since $d_p = d_1 M + d_0$ and $ed - 1 = k_p(p-1)$, we can rewrite CRT-RSA equation as

$$eMd_1 + ed_0 - 1 - k_p(p-1) = 0$$

Suppose that $d_1 \approx N^{\delta_1}$, $d_p \approx N^{\delta}$ and $e \approx N^{\alpha}$, we have

$$k_p = \frac{ed_p - 1}{p-1} \approx \frac{N^{\delta+\alpha}}{N^{\frac{1}{2}}} \approx N^{\delta+\alpha-\frac{1}{2}}$$

For the first attack, we consider a bivariate modular polynomial

$$f_{LSB1}(x, y) = eMx + y + ed_0 - 1$$

with the root $(x_0, y_0) = (d_1, k_p)$ modulo $p$. Let $X = N^{\delta_1}, Y = N^{\delta+\alpha-\frac{1}{2}}$, then $|x_0| < X, |y_0| < Y$.

For the second attack, we use a different bivariate polynomial that modulo $eM$. Specifically, we focus on the polynomial

$$f_{LSB2}(x, y) = x(y-1) + 1 - ed_0$$

with the root $(x_0, y_0) = (k_p, p)$ modulo $eM$. Using $X = N^{\delta+\alpha-\frac{1}{2}}, Y = N^{\frac{1}{2}}$, then $|x_0| < X, |y_0| < Y$.

Next we give the details on how to find the small root of $f_{LSB1}$ and $f_{LSB2}$.

### 3.2 Attack I: An Approach Modulo $p$

**Theorem 4 (Attack I).** *Let $N = pq$, where $p, q$ are primes of the same bit-size. Let the public exponent $e$ ($e \approx N^{\alpha}$) and private CRT-exponent $d_p$ ($d_p \approx N^{\delta}$) satisfy $ed_p \equiv 1 \bmod (p-1)$. Suppose that $d_p = d_1 M + d_0$ where $d_1 \approx N^{\delta_1}$. Given $d_0, M$, and assume that the following conditions are satisfied*

$$\begin{cases} 2-\delta-\alpha-2\sqrt{\delta_1-\delta-\alpha+0.5} < \frac{0.125}{\delta_1} & \textit{if } \ 0.5 > \delta_1 > 0.146 > \delta+\alpha-0.5 \\ 1.5-\delta_1-2\sqrt{\delta+\alpha-\delta_1-0.5} < \frac{0.125}{\delta+\alpha-0.5} & \textit{if } \ 0.5 > \delta+\alpha-0.5 > 0.146 > \delta_1 \\ \delta_1+\delta+\alpha-0.707 < 0 & \textit{if } \ 0.146 > \max\{\delta+\alpha-0.5, \delta_1\} \end{cases}$$

*Then $N$ can be factored in polynomial-time.*

*Proof.* According to the analysis of Sec. 3.1, we try to find the small root $(x_0, y_0) = (d_1, k_p)$ of the polynomial

$$f_{LSB1}(x, y) = eMx + y + ed_0 - 1$$

Applying Theorem 3 and setting $\beta = \frac{1}{2}$, then

$$\beta(1-\sqrt{1-\beta}) = \frac{2-\sqrt{2}}{4} \approx 0.146$$

For the case of $0.146 > \max\{\delta+\alpha-0.5, \delta_1\}$, we can get $\delta_1+\delta+\alpha-0.707 < 0$. For the case of $0.146 < \max\{\delta+\alpha-0.5, \delta_1\}$, we consider two subcases: $\delta+\alpha-0.5 > \delta_1$ and $\delta+\alpha-0.5 < \delta_1$. After some calculations, we obtain the claimed result. □

### 3.3 Attack II: An Approach Modulo $eM$

**Theorem 5 (Attack II).** *Using the notations of Theorem 4, provided that*

$$\delta + \frac{5}{2}\delta_1 - 3\delta_1^2 + \alpha - \frac{7}{8} < 0$$

*Then $N$ can be factored in polynomial-time.*

*Proof.* According to the analysis of Section 3.1, we try to find the small root $(x_0, y_0) = (k_p, p)$ of the polynomial

$$f_{LSB2}(x, y) = x(y-1) + 1 - ed_0$$

Note that the desired small solution contains the prime factor $p$, but $p$ is already determined by modulus $N$. Based on this observation, we apply the technique of Bleichenbacher and May [1]. Define two integers $m$ and $t$. Then we introduce a new variable $z$ for the prime factor $q$, and multiply the polynomial $f_{LSB2}(x, y)$ by a power $z^s$ for some $s$ that has to be optimized. Let us look at the following collection of trivariate polynomials that all have the root $(x_0, y_0)$ modulo $(eM)^m$.

$$g_{i,j}(x, y, z) = (eM)^{m-i} x^j z^s f_{LSB2}^i(x, y) \quad \text{for } \ i = 0, \ldots, m; \ j = 0, \ldots, m-i$$

$$h_{i,j}(x,y,z) = (eM)^{m-i} y^j z^s f_{LSB2}^i(x,y) \quad \text{for } \; i = 0,\ldots,m; \; j = 1,\ldots,t.$$

For $g_{i,j}(x,y,z), h_{i,j}(x,y,z)$, we replace every occurrence of the monomial $yz$ by $N$ because $N = pq$. Therefore, compared to the unchanged collection, every monomial $x^i y^j z^s (j \geq s)$ with coefficient $a_{i,j}$ is transformation into a monomial $x^i y^{j-s}$ with coefficient $a_{i,j}N^s$. And every monomial $x^i y^j z^s (j < s)$ with coefficient $a_{i,j}$ is transformation into a monomial $x^i z^{s-j}$ with coefficient $a_{i,j}N^j$.

To keep the lattice determinant as small as possible, we try to eliminate the factor of $N^j$ in the coefficient of diagonal entry. Since $\text{GCD}(eM,N) = 1$, we only need multiplying the corresponding polynomial with the inverse of $N^j$ modulo $(eM)^m$ [1].

We have to find two short vectors in lattice $\mathcal{L}$. Suppose that these two vectors are the coefficient vectors of two trivariate polynomial $f_1(xX,yY,zZ)$ and $f_2(xX,yY,zZ)$. There two polynomials have the root $(k_p,p,q)$ over the integers. Then we can eliminate the variable $z$ from these polynomials by setting $z = \frac{N}{y}$. Finally, we can extract the desired root $(k_p,p)$ from the new two polynomials if these polynomials are algebraically independent. Therefore, our attack relies on Assumption 1.

Now we give the details of the condition which we can find two sufficiently short vectors in the lattice $\mathcal{L}$. Let $t = \tau m, s = \sigma m$, the determinate of the lattice $\mathcal{L}$ is

$$\det(\mathcal{L}) = (eM)^{s_{eM}} X^{s_X} Y^{s_Y} Z^{s_Z}$$

where

$$s_{eM} = \sum_{i=0}^{m}\sum_{j=0}^{m-i}(m-i) + \sum_{i=0}^{m}\sum_{j=1}^{t}(m-i) = (2+3\tau)\cdot\frac{1}{6}m^3 + o(m^3)$$

$$s_X = \sum_{i=0}^{m}\sum_{j=0}^{m-i}(i+j) + \sum_{i=0}^{m}\sum_{j=1}^{t} i = (2+3\tau)\cdot\frac{1}{6}m^3 + o(m^3)$$

$$\begin{aligned} s_Y &= \sum_{i=s}^{m}\sum_{j=0}^{m-i}(i-s) + \sum_{i=0}^{m}\sum_{j=\max\{1,s-i\}}^{t}(j+i-s) \\ &= (1+3(\tau-\sigma)(1+\tau-\sigma))\cdot\frac{1}{6}m^3 + o(m^3) \end{aligned}$$

$$s_Z = \sum_{i=0}^{s}\sum_{j=0}^{m-i}(s-i) + \sum_{i=0}^{s}\sum_{j=1}^{s-i}(s-i-j) = 3\tau^2\cdot\frac{1}{6}m^3 + o(m^3)$$

And $X,Y,Z$ are the upper bounds of $k_p,p,q$. An easy calculation shows the dimension of the lattice is

$$n = \dim(\mathcal{L}) = \frac{1}{6}(3+6\tau)m^2 + o(m^2)$$

[1] In Sec. 4 of [1], the authors eliminated the factor $N^j$ by multiplying the inverse of $N^j$ modulo $e$, in fact it should be $e^m$ to satisfy the first condition of Lemma 2.

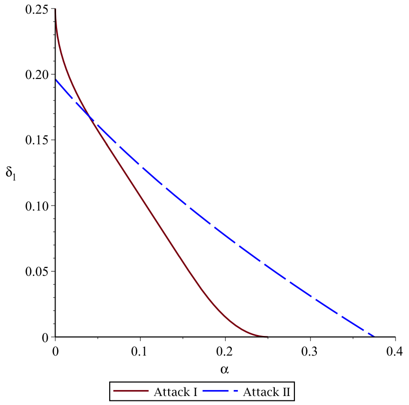

**Fig. 1.** The Case of Known LSBs of $d_p$ ($d_p \approx p$)

To get two polynomials which sharing the root $(k_p, p, q)$, we get the condition $\det(\mathcal{L}) \leq (eM)^{m \dim(\mathcal{L})}$. Substituting the values of the $\dim(\mathcal{L})$ and neglecting low-order term, we obtain the new condition

$$(2+3\tau)(\alpha+\delta-\frac{1}{2})+\frac{1}{2}(1+3(\tau-\sigma)(1+\tau-\sigma))+\frac{3}{2}\tau^2-(1+3\tau)(\alpha+\delta-\delta_1)<0$$

The optimized values of parameters $\tau$ and $\sigma$ were given by

$$\sigma = \frac{1}{2}+\delta_1 \qquad \tau = \frac{1}{2}-2\delta_1$$

Plugging in this values, we finally end up with the condition

$$\delta + \frac{5}{2}\delta_1 - 3\delta_1^2 + \alpha - \frac{7}{8} < 0$$

□

### 3.4 Comparison of the Attacks

We give the comparison of our attacks when the private exponent is full sized i.e. $d_p \approx p$. Fig. 1 illustrates our results on known LSBs of $d_p$ when $\delta = \frac{1}{2}$. The maximal size of unknown $d_1$ ($d_1 \approx N^{\delta_1}$) for an attack is plotted as a function of the size of $e$ ($e \approx N^{\alpha}$). Notice that the bounds for Attack I and Attack II match when $\alpha \approx 0.04$, thus Attack II is stronger than Attack I for $\alpha > 0.04$. Besides our attacks works up to $\alpha = \frac{3}{8} = 0.375$.

## 4 Key Recovery from Known MSBs

In this section we consider the case when some MSBs of $d_p$ are known.

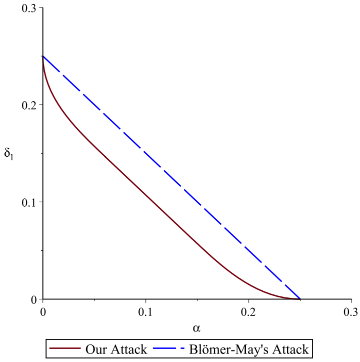

**Fig. 2.** Known MSBs: $\delta = 0.5$

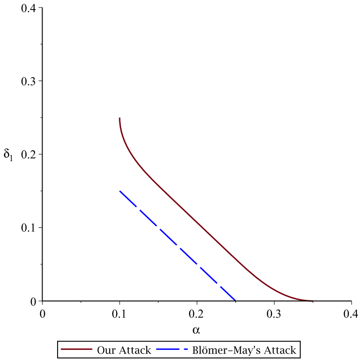

**Fig. 3.** Known MSBs: $\delta = 0.4$

**Theorem 6 (Known MSBs).** *Let $N = pq$, where $p, q$ are primes of the same bit-size. Let the public exponent $e$ ($e \approx N^{\alpha}$) and the private CRT-exponent $d_p$ ($d_p \approx N^{\delta}$) satisfying $ed_p \equiv 1 \bmod (p-1)$. Given $\tilde{d}$ where $|d_p - \tilde{d}| < N^{\delta_1}$, and assume that the following conditions are satisfied*

$$\begin{cases} 2 - \delta - \alpha - 2\sqrt{\delta_1 - \delta - \alpha + 0.5} < \frac{0.125}{\delta_1} & \textit{if} \;\; 0.5 > \delta_1 > 0.146 > \delta + \alpha - 0.5 \\ 1.5 - \delta_1 - 2\sqrt{\delta + \alpha - \delta_1 - 0.5} < \frac{0.125}{\delta + \alpha - 0.5} & \textit{if} \;\; 0.5 > \delta + \alpha - 0.5 > 0.146 > \delta_1 \\ \delta_1 + \delta + \alpha - 0.707 < 0 & \textit{if} \;\; 0.146 > \max\{\delta + \alpha - 0.5, \delta_1\} \end{cases}$$

*Then $N$ can be factored in polynomial-time.*

*Proof.* We have that $ed_p - 1 = k_p(p-1)$ for some $k \in \mathbb{N}$. We can rewrite our equation as

$$e(d_p - \tilde{d}) + k_p + e\tilde{d} - 1 \equiv 0 \mod p$$

Now we try to find the small root $(y_1, y_2) = (d_p - \tilde{d}, k_p)$ of the polynomial

$$f_{MSB}(x_1, x_2) = ex_1 + x_2 + e\tilde{d} - 1$$

Since $d_p - \tilde{d} \approx N^{\delta_1}$, $d_p \approx N^{\delta}$ and $e \approx N^{\alpha}$, we have

$$k_p = \frac{ed_p - 1}{p - 1} \approx \frac{N^{\delta+\alpha}}{N^{0.5}} \approx N^{\delta+\alpha-0.5}$$

Applying Theorem 3 and setting $\beta = 0.5$, we obtain the claimed result. □

### 4.1 Comparison with Blömer-May's [11] Results

Fig. 2 and Fig. 3 compare the results on known MSBs of $d_p$. We focus on two cases: $\delta = 0.5$ and $\delta = 0.4$. In Fig. 2, note that Blömer-May's [11] result is better than ours. However, for the case $\delta = 0.4$, our result is better (Fig. 3). Actually our result is better than Theorem 2 if $\delta < 0.457$.

**Table 1.** Experimental Results for Partial Key Exposure Attacks (LSBs)

(a) LSBs Case: Attack I

| $e$ | $d$ | $d_1$ | $(m, t)$ | dim($\mathcal{L}$) | time(sec) |
|---|---|---|---|---|---|
| 30 | 512 | 150 | $(10, 3)$ | 66 | 172.241 |
| 60 | 512 | 110 | $(10, 3)$ | 66 | 191.304 |
| 100 | 512 | 60 | $(10, 3)$ | 66 | 250.397 |
| 150 | 512 | 20 | $(10, 3)$ | 66 | 272.378 |
| 85 | 512 | 85 | $(13, 4)$ | 105 | 4012.299 |

(b) LSBs Case: Attack II

| $e$ | $d$ | $d_1$ | $(m, t, u)$ | dim($\mathcal{L}$) | time(sec) |
|---|---|---|---|---|---|
| 30 | 512 | 130 | $(7, 4, 2)$ | 68 | 95.176 |
| 60 | 512 | 100 | $(7, 4, 2)$ | 68 | 152.295 |
| 80 | 512 | 100 | $(10, 6, 3)$ | 132 | 5642.342 |
| 100 | 512 | 70 | $(7, 4, 3)$ | 68 | 391.281 |
| 150 | 512 | 35 | $(7, 4, 3)$ | 68 | 605.471 |
| 200 | 512 | 10 | $(8, 4, 4)$ | 81 | 3096.707 |

In fact, we can apply the linearization method on the equation of Theorem 6:

$$\underbrace{e(d_p - \tilde{d}) + k_p}_{x} + e\tilde{d} - 1 \equiv 0 \mod p$$

This can be stated as finding the root of the linear monic polynomial $f(x) = x + e\tilde{d} - 1 \bmod p$ where $p = N^{\frac{1}{2}}$. Using Herrmann-May's method [8], we can get the same bound as [11]. In [8], Herrmann and May observed that their algorithm gives much better bounds for a smaller number of unknown variables (From two to one). That is the reason why [11]'s result is better than ours when $\delta = 0.5$. However, as the size of $e(d_p - \tilde{d})$ and $k_p$ increasingly unbalanced, this linearization method can not exploit the relation between the coefficients of the polynomial $f_{MSB}$. Therefore, our method is more appropriate for this scenario ($\delta$ is small). Actually, in [22,7], the authors used the similar technique to improve the bound for solving the Multi-Prime $\Phi$-Hiding Problem.

## 5 Experimental Results

To verify the effectiveness of our lattice-based approaches, we carry out some experiments[2]. We have implemented our attacks using Magma [23] on a laptop with Intel© Core$^{\text{TM}}$ i5-2430M CPU 2.40 GHz, 2 GB RAM. For all the listed-up parameters, we can recover the factorization of $N$.

In Table 1[3] we illustrate partial known LSBs attacks for 1024-bit RSA modulus $N$ with 512-bit primes $p, q$. From the data of the table, it is clear that for large $e$, Attack II works better than Attack I for recovering the whole key, which was already shown in Sec. 3.4.

[2] Since the attack of Sec. 4 is similar to the attack of Sec. 3.2, we omit experiments for the MSBs case here.

[3] In Table 1(a), we did not exploit Takayasu-Kunihiro's technique [21] that consider the sizes of the root bound. Because we believe that it is enough to show the efficiency comparison of our two attacks.

**Acknowledgments.** We would like to thank the anonymous reviewers for helpful comments. This work is supported by the National 973 Program of China under Grant No. 2011CB302400, the National Natural Science Foundation of China under Grant No. 61303257, No. 61100225 and No. 61379139. IIEs Research Project on Cryptography under Grant No. Y3Z001C102, One Hundred Talents Project of the Chinese Academy of Sciences, the Strategic Priority Research Program of the Chinese Academy of Sciences under Grant No. XDA06010701.

## References

1. Bleichenbacher, D., May, A.: New attacks on RSA with small secret CRT-exponents. In: Yung, M., Dodis, Y., Kiayias, A., Malkin, T. (eds.) PKC 2006. LNCS, vol. 3958, pp. 1–13. Springer, Heidelberg (2006)
2. Boneh, D., Durfee, G.: Cryptanalysis of RSA with private key $d$ less than $N^{0.292}$. IEEE Transactions on Information Theory 46(4), 1339–1349 (2000)
3. Boneh, D., Durfee, G., Frankel, Y.: Exposing an RSA private key given a small fraction of its bits. In: Full Version of the work from Asiacrypt, vol. 98 (1998)
4. Boneh, D., Durfee, G., Howgrave-Graham, N.: Factoring $n = p^r q$ for large $r$. In: Advances in Cryptology–CRYPTO 1999, p. 787. Springer (1999)
5. Ernst, M., Jochemsz, E., May, A., de Weger, B.: Partial key exposure attacks on RSA up to full size exponents. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 371–386. Springer, Heidelberg (2005)
6. Galbraith, S.D., Heneghan, C., McKee, J.F.: Tunable balancing of RSA. In: Boyd, C., González Nieto, J.M. (eds.) ACISP 2005. LNCS, vol. 3574, pp. 280–292. Springer, Heidelberg (2005)
7. Herrmann, M.: Improved cryptanalysis of the multi-prime $\phi$ - hiding assumption. In: Nitaj, A., Pointcheval, D. (eds.) AFRICACRYPT 2011. LNCS, vol. 6737, pp. 92–99. Springer, Heidelberg (2011)
8. Herrmann, M., May, A.: Solving linear equations modulo divisors: On factoring given any bits. In: Pieprzyk, J. (ed.) ASIACRYPT 2008. LNCS, vol. 5350, pp. 406–424. Springer, Heidelberg (2008)
9. Herrmann, M., May, A.: Maximizing small root bounds by linearization and applications to small secret exponent RSA. In: Nguyen, P.Q., Pointcheval, D. (eds.) PKC 2010. LNCS, vol. 6056, pp. 53–69. Springer, Heidelberg (2010)
10. Howgrave-Graham, N.: Finding small roots of univariate modular equations revisited. In: Möhring, R.H. (ed.) WG 1997. LNCS, vol. 1335, pp. 131–142. Springer, Heidelberg (1997)
11. Blömer, J., May, A.: New partial key exposure attacks on RSA. In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol. 2729, pp. 27–43. Springer, Heidelberg (2003)
12. Jochemsz, E., May, A.: A polynomial time attack on RSA with private CRT-exponents smaller than $N^{0.073}$. In: Menezes, A. (ed.) CRYPTO 2007. LNCS, vol. 4622, pp. 395–411. Springer, Heidelberg (2007)
13. Joye, M., Lepoint, T.: Partial key exposure on RSA with private exponents larger than $n$. In: Ryan, M.D., Smyth, B., Wang, G. (eds.) ISPEC 2012. LNCS, vol. 7232, pp. 369–380. Springer, Heidelberg (2012)
14. Kunihiro, N., Shinohara, N., Izu, T.: A unified framework for small secret exponent attack on RSA. In: Miri, A., Vaudenay, S. (eds.) SAC 2011. LNCS, vol. 7118, pp. 260–277. Springer, Heidelberg (2012)

15. Lenstra, A.K., Lenstra, H.W., Lovász, L.: Factoring polynomials with rational coefficients. Mathematische Annalen 261(4), 515–534 (1982)
16. May, A.: Cryptanalysis of unbalanced RSA with small CRT-exponent. In: Yung, M. (ed.) CRYPTO 2002. LNCS, vol. 2442, pp. 242–256. Springer, Heidelberg (2002)
17. May, A.: Secret exponent attacks on RSA-type schemes with moduli $N = p^r q$. In: Bao, F., Deng, R., Zhou, J. (eds.) PKC 2004. LNCS, vol. 2947, pp. 218–230. Springer, Heidelberg (2004)
18. Quisquater, J.-J.: Chantal Couvreur. Fast decipherment algorithm for RSA public-key cryptosystem. Electronics Letters 18(21), 905–907 (1982)
19. Sarkar, S., Maitra, S.: Partial key exposure attack on CRT-RSA. In: Abdalla, M., Pointcheval, D., Fouque, P.-A., Vergnaud, D. (eds.) ACNS 2009. LNCS, vol. 5536, pp. 473–484. Springer, Heidelberg (2009)
20. Takagi, T.: Fast RSA-type cryptosystem modulo $p^k q$. In: Krawczyk, H. (ed.) CRYPTO 1998. LNCS, vol. 1462, pp. 318–326. Springer, Heidelberg (1998)
21. Takayasu, A., Kunihiro, N.: Better lattice constructions for solving multivariate linear equations modulo unknown divisors. In: Boyd, C., Simpson, L. (eds.) ACISP 2013. LNCS, vol. 7959, pp. 118–135. Springer, Heidelberg (2013)
22. Tosu, K., Kunihiro, N.: Optimal bounds for multi-prime $\phi$-hiding assumption. In: Susilo, W., Mu, Y., Seberry, J. (eds.) ACISP 2012. LNCS, vol. 7372, pp. 1–14. Springer, Heidelberg (2012)
23. Cannon, J., Bosma, W., Playoust, C.: The Magma algebra system. I. The user language. J. Symbolic Comput. 24(3-4), 235–265 (1997); Computational algebra and number theory, London (1993)
24. Wiener, M.J.: Cryptanalysis of short RSA secret exponents. IEEE Transactions on Information Theory 36(3), 553–558 (1990)