Implicit Related-Key Factorization Problem on the RSA Cryptosystem

Mengce Zheng(✉) and Honggang Hu

Key Laboratory of Electromagnetic Space Information, CAS,
University of Science and Technology of China, Hefei, China
{mczheng,hghu2005}@ustc.edu.cn

Abstract. In this paper, we address the implicit related-key factorization problem on the RSA cryptosystem. Informally, we investigate under what condition it is possible to efficiently factor RSA moduli in polynomial time given the implicit information of related private keys. We propose lattice-based attacks using Coppersmith's techniques. We first analyze the special case given two RSA instances with known amounts of shared most significant bits (MSBs) and least significant bits (LSBs) of unknown related private keys. Subsequently a generic attack is proposed using a heuristic lattice construction when given more RSA instances. Furthermore, we conduct numerical experiments to verify the validity of the proposed attacks.

Keywords: RSA · Factorization · Implicit related-key · Lattice-based attack · Coppersmith's techniques

1 Introduction

The RSA public-key cryptosystem [18] plays an important role in the area of information security due to its simplicity and popularity. Its key equation is $ed \equiv 1 \bmod \varphi(N)$, where N, e, d and $\varphi(N)$ are defined as follows. $N = pq$ is the product of two large primes of the same bit-size. e, d denote the public and private keys, which are also called the public/encryption and private/decryption exponents. $\varphi(N) = (p-1)(q-1)$ is Euler's totient function. One computes $c = m^e \bmod N$ and $c^d \bmod N$ for encryption and decryption operations, respectively.

In 1996, Coppersmith [4,5] made a significant breakthrough based on finding small roots of modular and integer polynomial equations. The fundamental works proposed novel and advanced lattice-based attacks on RSA. The main method is known as Coppersmith's techniques [6] and has been widely applied in the cryptanalytic field of RSA. Many researchers have proposed several effective attacks such as [1,7–10,15,21] etc. Among them, the *partial key exposure attack* has been extensively studied as an active attack scenario.

In 1998, Boneh et al. [2] proposed several attacks on RSA given a fraction of the private key bits with small public exponent e. The attacks employed some known most significant bits (MSBs) or least significant bits (LSBs) of d. In 2005,

Y. Mu et al. (Eds.): CANS 2019, LNCS 11829, pp. 525–537, 2019.
https://doi.org/10.1007/978-3-030-31578-8_29

Ernst et al. [10] presented improved lattice-based attacks that work up to full size exponents under a heuristic assumption. In our opinion, partial key exposure attack can be reduced to the problem of factoring RSA modulus with an oracle outputting some *explicit* information of d.

In 2009, May and Ritzenhofen [16] proposed the *implicit factorization problem*, which aims to factor RSA moduli with an oracle providing implicit information about the amount of shared LSBs of the primes. It is mainly considered for the malicious generation of RSA moduli like the construction of backdoor RSA moduli. Later, Sarkar and Maitra [19] proposed a better approach based on solving the approximate common divisor problem.

Inspired by the above attacks, we raise an interesting hybrid problem that aims to efficiently factor RSA moduli given some implicit information about the related private keys. We herein present the description of the *implicit related-key factorization problem* as follows. Let $(N_1, e_1, d_1), \ldots, (N_n, e_n, d_n)$ be n distinct key pairs, where $N_1, \ldots, N_n$ are of the same bit-size and the prime factors are also all of the same bit-size. Given the implicit information that certain portions of the bit pattern in private keys $d_1, \ldots, d_n$ are common, under what condition is it possible to efficiently factor $N_1, \ldots, N_n$. In this sense, the implicit factorization problem [16] can be refined into the implicit related-prime factorization problem accordingly.

There are several situations to use many RSA instances in practice like [20]. Once such RSA instances are generated with imperfect randomness or malicious backdoor keys, one may encounter the implicit related-key factorization problem. Our motivations come from two aspects. Mainly from the theoretical view, we study a new problem combing two existing attacks, which may further disclose the vulnerability of RSA with implicit information and enrich lattice-based cryptanalyses in the literature. Practically, side channel attacks may not give explicit information as expected. Instead, one may know the amounts of shared MSBs and LSBs of the private keys as some implicit information. The users' misuses with certain repeated bit patterns in the private keys may also lead to this problem.

We formulate the implicit related-key factorization problem with several RSA instances clearly. Given n key pairs of RSA parameters (N_i, e_i, d_i) for $1 \leq i \leq n$. We consider the full size case when $e_i \approx N$ for N denoting an integer of the same bit-size as N_i for simplicity. Besides, we assume $d_i \approx N^{\delta}$ share certain MSBs and LSBs like $d_j = d_i + d_{ji}D$ for $1 \leq i < j \leq n$, where D denotes the bit-length of shared LSBs-block and d_{ji} denotes the difference between every two unknown middle blocks with $|D| \approx N^{\gamma}$ and $|d_{ji}| \approx N^{\beta}$.

We follow Coppersmith's techniques [6] to handle the implicit related-key factorization problem. In addition, we adapt two subtle lattice techniques, namely the splitting technique and the linearization technique. Our attacks rely on a *heuristic assumption*, which works well in the literature. The assumption says that algebraically independent polynomials can be obtained by the lattice-based attacks and the common root can be efficiently extracted by the Gröbner basis computation [3].

Our main result is stated in Proposition 1, which will be proven in Sect. 3. We want to point out that the theoretical result is asymptotic since the corresponding lattice dimension is required preferably large.

Proposition 1. *Let $N_1 = p_1q_1$ and $N_2 = p_2q_2$ be given two RSA moduli of the same bit-size, where p_1, q_1, p_2, q_2 are large primes of the same bit-size. Let e_1, d_1, e_2, d_2 be some integers satisfying $e_1d_1 \equiv 1 \bmod (p_1-1)(q_1-1)$ and $e_2d_2 \equiv 1 \bmod (p_2-1)(q_2-1)$ such that $e_1 \approx e_2 \approx N$ and $d_1 \approx d_2 \approx N^{\delta}$. Given the implicit information that $d_2 = d_1 + d_{21}D$ for $|d_{21}| \approx N^{\beta}$. Then N_1 and N_2 can be factored in polynomial time if*

$$\delta < \frac{25 - 16\beta - \sqrt{177 - 96\beta}}{32}.$$

The rest of the paper is organized as follows. We provide basic knowledge of Coppersmith's techniques and Gaussian heuristic in Sect. 2. In Sect. 3, we propose a lattice-based attack for given two instances and further develop a notable lattice construction to analyze the case of n instances. We verify the validity of the proposed attacks by computer experiments in Sect. 4. Finally, concluding remarks are given in Sect. 5.

2 Preliminaries

In this section, we first briefly introduce lattice, the LLL reduction algorithm [14] and Coppersmith's techniques [6]. Then we give a rough condition for finding the small roots of modular polynomial equations. We also briefly describe the splitting technique [17] based on the Gaussian heuristic.

A lattice $\mathcal{L}$ spanned by linearly independent vectors $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m \in \mathbb{R}^n$ is the set of their integer linear combinations, which can be denoted by

$$\mathcal{L}(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m) = \left\{ \sum_{i=1}^{m} z_i \boldsymbol{b}_i : z_i \in \mathbb{Z} \right\}.$$

The basis vectors derive a basis matrix B by regarding each $\boldsymbol{b}_i$ as row (or column) vectors. The determinant of $\mathcal{L}$ is calculated as $\det(\mathcal{L}) = \sqrt{\det(BB^{\mathsf{T}})}$. The rank of $\mathcal{L}$ is m and we always consider a full-rank lattice for $m = n$. Thus, we have $\det(\mathcal{L}) = |\det(B)|$.

The LLL algorithm [14] is practically used for computing approximately short lattice vectors due to its efficient running outputs. We provide the following substratal lemma, whose proof refers to [15].

Lemma 1. *Let $\mathcal{L}$ be a lattice spanned by basis vectors $(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m)$. The LLL algorithm outputs a reduced basis $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m)$ satisfying*

$$\|\boldsymbol{v}_1\|, \|\boldsymbol{v}_2\|, \ldots, \|\boldsymbol{v}_i\| \leq 2^{\frac{m(m-1)}{4(m+1-i)}} \det(\mathcal{L})^{\frac{1}{m+1-i}} \text{ for } 1 \leq i \leq m$$

in time polynomial in m and in the bit-size of the entries of the basis matrix.

Howgrave-Graham [13] refined on Coppersmith's techniques to propose a succinct lemma for judging whether the small roots of a modular equation are roots over $\mathbb{Z}$. For a given polynomial $g(x_1, \ldots, x_n) = \sum a_{i_1,\ldots,i_n} x_1^{i_1} \cdots x_n^{i_n}$, its norm is defined as $\|g(x_1, \ldots, x_n)\| := \sqrt{\sum |a_{i_1,\ldots,i_n}|^2}$.

Lemma 2. *Let $g(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ be an integer polynomial of at most m monomials. Suppose that*

1. $g(x'_1, \ldots, x'_n) \equiv 0 \bmod R$, *where* $|x'_1| \leq X_1, \ldots, |x'_n| \leq X_n$,
2. $\|g(x_1X_1, \ldots, x_nX_n)\| < R/\sqrt{m}$.

Then $g(x'_1, \ldots, x'_n) = 0$ holds over the integers.

Combining Lemmas 1 and 2, one can solve modular/integer equations under a particular condition. One first constructs shift polynomials from a given equation and then generate a lattice basis matrix using the coefficient vectors. Once integer equations are derived from the first ℓ reduced vectors through the LLL algorithm, one can extract the root for $2^{\frac{m(m-1)}{4(m+1-\ell)}} \det(\mathcal{L})^{\frac{1}{m+1-\ell}} < R/\sqrt{m}$. It further leads to a rough condition $\det(\mathcal{L}) < R^m$ if ignoring the negligible lower terms. The first ℓ vectors are transformed into simultaneous equations sharing the common root over the integers. Hence, one can apply the Gröbner basis computation to extract the common root.

Recently, Peng et al. [17] proposed an improved lattice-attack on the Dual RSA scheme [20] using the splitting technique. It can split a variable of large norm into several variables of smaller norm by reducing a low-dimensional lattice. Concretely, it is based on the observation of Gaussian heuristic in random lattices, which says that the norm of the shortest non-zero vector $\boldsymbol{s}$ of a random m-dimensional lattice $\mathcal{L}$ satisfies $\|\boldsymbol{s}\| \approx \sqrt{m/(2\pi \mathrm{e})} \det(\mathcal{L})^{\frac{1}{m}}$. Let the successive minimum $\lambda_i(\mathcal{L})$ denote the i-th minimum of $\mathcal{L}$, which is the radius of the smallest zero-centered ball containing at least i linearly independent lattice vectors. In this sense, $\|\boldsymbol{s}\|$ can be written as $\lambda_1(\mathcal{L})$.

A further claim on this property can be found in [11]. The successive minima of a random m-dimensional lattice $\mathcal{L}$ are all asymptotically close to the Gaussian heuristic with an overwhelming probability. That is $\lambda_i(\mathcal{L}) \approx \sqrt{m/(2\pi \mathrm{e})} \det(\mathcal{L})^{\frac{1}{m}}$ for all $1 \leq i \leq m$. We adapt the splitting technique along with the linearization technique [12] to present convenient lattice construction in our lattice-based attacks. In this paper, we use the fact $|s_{i1}| \approx \det(\mathcal{L}_0)^{\frac{1}{m}}$, where $\boldsymbol{s}_i$ for $1 \leq i \leq m$ is a reduced basis vector after running the LLL algorithm on the constructed m-dimensional full-rank lattice $\mathcal{L}_0$.

3 Implicit Related-Key Factorization Attacks

We first propose a lattice-based attack for given two RSA instances, namely (N_1, e_1, d_1) and (N_2, e_2, d_2). Recall that we know $e_1 \approx e_2 \approx N$, where N denotes an integer with the same bit-size as N_1, N_2 and the private keys d_1, d_2 share some MSBs and LSBs leaving one different block in the middle. Moreover, we

have $d_1 \approx d_2 \approx N^{\delta}$ and $d_2 = d_1 + d_{21}D$ for $|d_{21}| \approx N^{\beta}$ and $|D| \approx N^{\gamma}$ (assuming γ and β are given in advance).

We first perform the splitting technique to split one unknown private key into a linear combination of two smaller unknown variables. To do so, we construct a two-dimensional lattice $\mathcal{L}_0$ that is generated by the following basis matrix

$$B_0 = \begin{bmatrix} a_0 & e_1 \\ 0 & N_1 \end{bmatrix}$$

for a well-chosen integer a_0.

From the key equation $e_1d_1 \equiv 1 \bmod \varphi(N_1)$ and $\varphi(N_1) = N_1 + 1 - p_1 - q_1$, we have $e_1d_1 - k_1N_1 = k_1(1 - p_1 - q_1) + 1$ for a positive integer k_1. Hence, we know $(d_1, -k_1)B_0 = (a_0d_1, k_1(1 - p_1 - q_1) + 1)$ is a vector belonging to $\mathcal{L}_0$. We have $k_1 = (e_1d_1 - 1)/\varphi(N_1) \approx N^{\delta}$. We set $a_0 = [N^{\frac{1}{2}}]$ to balance each coordinate of $(a_0d_1, k_1(1-p_1-q_1)+1)$, whose norm is $\|(a_0d_1, k_1(1-p_1-q_1)+1)\| \approx N^{\delta+\frac{1}{2}}$. The determinant of $\mathcal{L}_0$ is $\det(\mathcal{L}_0) = |\det(B_0)| = a_0N_1 \approx N^{\frac{3}{2}}$ from our construction of the basis matrix B_0.

We can obtain two reduced basis vectors (s_{11}, s_{12}) and (s_{21}, s_{22}) through the lattice reduction algorithm. Further by applying the Gaussian heuristic, we have $\|(s_{11}, s_{12})\| = \|(s_{21}, s_{22})\| \approx \det(\mathcal{L}_0)^{\frac{1}{2}} \approx N^{\frac{3}{4}}$, which indicates the norms of s_{11}, s_{12}, s_{21} and s_{22} are roughly $N^{\frac{3}{4}}$. Actually, we have $s_{11} = a_0a_1$ and $s_{21} = a_0a_2$ as the reduced basis vectors are generated by

$$\begin{bmatrix} s_{11} & s_{12} \\ s_{21} & s_{22} \end{bmatrix} = \begin{bmatrix} a_1 & - \\ a_2 & - \end{bmatrix} \begin{bmatrix} a_0 & e_1 \\ 0 & N_1 \end{bmatrix} = \begin{bmatrix} a_0a_1 & * \\ a_0a_2 & * \end{bmatrix},$$

where known integers a_1 and a_2 are elements appearing in the first column vector of the unimodular transformation matrix. It can easily deduced that $|a_1| \approx |a_2| \approx |s_{21}/a_0| \approx N^{\frac{1}{4}}$.

On the other hand, we have $a_0d_1 = s_{11}c_1 + s_{21}c_2$ since (s_{11}, s_{12}) and (s_{21}, s_{22}) are also basis vectors. Hence, we obtain $d_1 = a_1c_1 + a_2c_2$ for unknown c_1 and c_2. Combining it with $d_2 = d_1 + d_{21}D$, we finally have $d_2 = a_1c_1 + a_2c_2 + d_{21}D$. We want to figure out the norms of c_1 and c_2. As $|a_1| \approx |a_2| \approx N^{\frac{1}{4}}$, we have $|c_1| \approx |c_2| \approx |d_2/a_2| \approx N^{\delta-\frac{1}{4}}$. We substitute $d_2 = a_1c_1 + a_2c_2 + d_{21}D$ in another key equation $e_2d_2 = k_2(N_2 + 1 - p_2 - q_2) + 1$ and have $e_2(a_1c_1 + a_2c_2 + d_{21}D) = k_2(N_2 + 1 - p_2 - q_2) + 1$. Therefore, we turn to solving $f(x, y, z, w) := x(y - N_2 - 1) + e_2a_1z + e_2Dw - 1 \bmod e_2a_2$ with the root $(k_2, p_2 + q_2, c_1, d_{21})$ for the implicit related-key factorization problem.

To provide an elegant lattice construction, we further apply the linearization technique introduced in [12]. Letting $u := xy - 1$, we have the linear polynomial $\bar{f}(x, z, w, u) := u - (N_2 + 1)x + e_2a_1z + e_2Dw \bmod e_2a_2$. The shift polynomials are defined as

$$g_{[i,j,k,l_1,l_2]}(x, y, z, w, u) := x^i y^j z^{l_1} w^{l_2} \bar{f}^k(x, z, w, u) E^{s-k}$$

for $E = e_2 a_2$, a positive integer s and $i, j, k, l_1, l_2 \in \mathbb{N}$. We denote the set of the shift polynomials by $\mathcal{G} := \mathcal{G}_1 \cup \mathcal{G}_2$, where

$$\begin{aligned}\mathcal{G}_1 :=& \{g_{[i,0,k,l_1,l_2]}(x,y,z,w,u) : k = 0,\ldots,s; i = 0,\ldots,s-k;\\ & l_1 = 0,\ldots,s-k-i; l_2 = 0,\ldots,s-k-i-l_1.\},\\ \mathcal{G}_2 :=& \{g_{[0,j,k,l_1-l_2,l_2-k]}(x,y,z,w,u) : l_1 = 0,\ldots,s; j = 1,\ldots,\tau l_1;\\ & l_2 = 0,\ldots,l_1; k = 0,\ldots,l_2.\}\end{aligned}$$

for an optimizing parameter $0 \leq \tau \leq 1$ to be determined later. It is obvious that all the shift polynomials share the common root $(k_2, p_2+q_2, c_1, d_0, k_2(p_2+q_2)-1)$ modulo E^s.

By defining auxiliary parameters $r = i+k+l_1+l_2$ and $r' = i'+k'+l_1'+l_2'$, the polynomial and monomial orders $\prec$ are defined as $g_{[i,j,k,l_1,l_2]} \prec g_{[i',j',k',l_1',l_2']}$ and $x^i y^j u^k z^{l_1} w^{l_2} \prec x^{i'} y^{j'} u^{k'} z^{l_1'} w^{l_2'}$, respectively if $r < r'$ or $r = r',\ i \geq i'$ or $r = r',\ i = i',\ l_1 \geq l_1'$ or $r = r',\ i = i',\ l_1 = l_1',\ l_2 \geq l_2'$ or $r = r',\ i = i',\ l_1 = l_1',\ l_2 = l_2',\ j < j'$.

We can substitute each occurrence of xy by $u+1$. The lattice basis matrix B is constructed by taking the coefficient vectors of $g_{[i,j,k,l_1,l_2]}(xX, yY, zZ, wW, uU)$ in $\mathcal{G}$ as row vectors, where X, Y, Z, W and U denote the upper bounds on unknown variables. Additionally, the rows and columns of B are arranged according to the above polynomial and monomial orders. Two parameters s and τ can guarantee that B is square and triangular.

Table 1 shows a toy example of the lattice basis matrix B for $s = 1$ and $\tau = 1$, where each row can be viewed as the coefficient vector transformation from a shift polynomial. We are able to obtain the basis matrix B that generates the main lattice $\mathcal{L}$ directly from our construction.

Table 1. A toy example of the constructed lattice basis matrix B for $s = 1$ and $\tau = 1$ with $E = e_2 a_2$ and $C = -(N_2 + 1)$.

	1	x	z	yz	w	yw	u	yu
$g_{[0,0,0,0,0]}(xX, yY, zZ, wW, uU)$	E							
$g_{[1,0,0,0,0]}(xX, yY, zZ, wW, uU)$		EX						
$g_{[0,0,0,1,0]}(xX, yY, zZ, wW, uU)$			EZ					
$g_{[0,1,0,1,0]}(xX, yY, zZ, wW, uU)$				EYZ				
$g_{[0,0,0,0,1]}(xX, yY, zZ, wW, uU)$					EW			
$g_{[0,1,0,0,1]}(xX, yY, zZ, wW, uU)$						EYW		
$g_{[0,0,1,0,0]}(xX, yY, zZ, wW, uU)$		CX	e_2a_1Z		e_2DW		U	
$g_{[0,1,1,0,0]}(xX, yY, zZ, wW, uU)$	C			e_2a_1YZ		e_2DYW	CU	YU

Since we already know $X \approx N^{\delta}$, $Y \approx N^{\frac{1}{2}}$, $Z \approx N^{\delta-\frac{1}{4}}$, $W \approx N^{\beta}$, $U \approx N^{\delta+\frac{1}{2}}$ and $E \approx N^{\frac{5}{4}}$, we can calculate the determinant of $\mathcal{L}$ that is the product of the diagonal entries of the basis matrix B.

$$\begin{aligned}\det(\mathcal{L}) &= \left(\prod_{k=0}^{s}\prod_{i=0}^{s-k}\prod_{l_1=0}^{s-k-i}\prod_{l_2=0}^{s-k-i-l_1} X^i Z^{l_1} W^{l_2} U^k E^{s-k}\right) \\ &\times \left(\prod_{l_1=0}^{s}\prod_{j=1}^{\tau l_1}\prod_{l_2=0}^{l_1}\prod_{k=0}^{l_2} Y^j Z^{l_1-l_2} W^{l_2-k} U^k E^{s-k}\right) \\ &= X^{s_x} Y^{s_y} Z^{s_z} W^{s_w} U^{s_u} E^{s_E},\end{aligned}$$

where s_x, s_y, s_z, s_w, s_u and s_E are the respective exponent sums of the diagonal entries of the basis matrix B. The lattice dimension is

$$m = \sum_{k=0}^{s}\sum_{i=0}^{s-k}\sum_{l_1=0}^{s-k-i}\sum_{l_2=0}^{s-k-i-l_1} 1 + \sum_{l_1=0}^{s}\sum_{j=1}^{\tau l_1}\sum_{l_2=0}^{l_1}\sum_{k=0}^{l_2} 1 = \frac{1+3\tau}{24}s^4 + o(s^4).$$

Similarly, we calculate $s_x = \frac{1}{120}s^5$, $s_y = \frac{\tau^2}{20}s^5$, $s_z = s_w = s_u = \frac{1+4\tau}{120}s^5$ and $s_E = \frac{4+11\tau}{120}s^5$ when omitting $o(s^5)$ as it is negligible for sufficiently large s. From the rough condition $\det(\mathcal{L}) < R^m$ with $R = E^s$ for acquiring enough integer equations sharing the common root, we have

$$X^{s_x} Y^{s_y} Z^{s_z} W^{s_w} U^{s_u} E^{s_E} < E^{\frac{1+3\tau}{24}s^5}.$$

Moreover, we let s go to infinite and obtain the crucial condition

$$\frac{1}{120}\cdot\xi_x + \frac{\tau^2}{20}\cdot\xi_y + \frac{1+4\tau}{120}\cdot(\xi_z+\xi_w+\xi_u) + \frac{4+11\tau}{120}\cdot\xi_E < \frac{1+3\tau}{24}\cdot\xi_E,$$

where ξ_x, ξ_y, ξ_z, ξ_w, ξ_u and ξ_E denote the exponents of the respective upper bounds. We further reduce the crucial condition to a simplified one

$$\xi_x + 6\tau^2\xi_y + (1+4\tau)(\xi_z+\xi_w+\xi_u-\xi_E) < 0.$$

We know $\xi_x = \delta$, $\xi_y = \frac{1}{2}$, $\xi_z = \delta - \frac{1}{4}$, $\xi_w = \beta$, $\xi_u = \delta + \frac{1}{2}$ and $\xi_E = \frac{5}{4}$. Thus, we obtain

$$\delta + 3\tau^2 + (1+4\tau)\left(\delta - \frac{1}{4} + \beta + \delta + \frac{1}{2} - \frac{5}{4}\right) < 0,$$

which leads to

$$\delta < \frac{(1-\beta)(1+4\tau) - 3\tau^2}{3+8\tau}.$$

The right side reaches its maximum by taking $\tau = (\sqrt{177-96\beta}-9)/24$. We put it into the above inequality and hence derive the final condition

$$\delta < \frac{25 - 16\beta - \sqrt{177-96\beta}}{32}.$$

Once we extract the common root $(k_2, p_2+q_2, c_1, d_{21}, k_2(p_2+q_2)-1)$, we can easily factorize N_2 using the value of p_2+q_2. Then we have d_2 from $d_2 = e_2^{-1} \bmod \varphi(N_2)$, which can be used to recover d_1 by $d_1 = d_2 - d_{21}D$. Thus, we

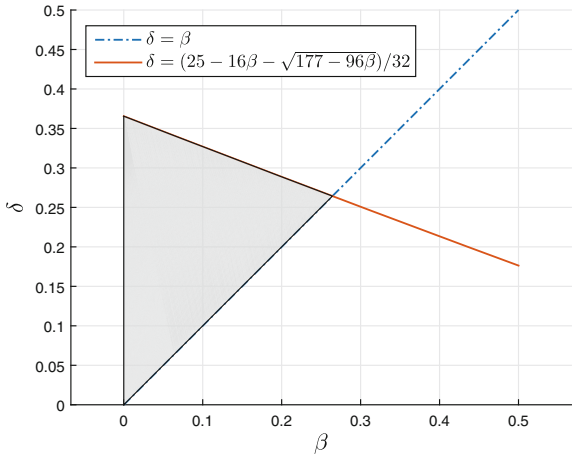

Fig. 1. The solid curve denotes the upper bound on δ and the dot-dash line denotes the lower bound on δ. The gray area indicates the vulnerable scenarios of the proposed implicit related-key factorization attack for given two RSA instances.

can factorize N_1 as knowing d_1 is equivalent to the factorization of N_1, which has been proved in [9].

The above result is illustrated in Fig. 1. We gain a significant improvement of the insecure bound on δ with the help of known implicit information about the related private keys. One may wonder whether our approach can handle the implicit related-key factorization problem for more than two RSA instances. We give an answer to this question below.

Recall the attack scenario for handling the implicit related-key factorization problem with n distinct RSA instances. Given n key pairs of RSA parameters (N_i, e_i, d_i) for $1 \leq i \leq n$. We assume $e_i \approx N$ and $d_i \approx N^{\delta}$ with $d_j = d_i + d_{ji}D$, where $|d_{ji}| \approx N^{\beta}$ and $|D| \approx N^{\gamma}$ for $1 \leq i < j \leq n$.

We first perform the splitting technique to split d_1 into a linear combination of several smaller unknown variables. We introduce a concise heuristic construction of a $(2n-1)$-dimensional lattice $\mathcal{L}_0$ that is generated by the basis matrix

$$B_0 = \begin{bmatrix} a_0 & 0 & \cdots & 0 & e_2 & \cdots & e_n \\ 0 & b_0 & \cdots & 0 & e_2 D & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & b_0 & 0 & \cdots & e_n D \\ 0 & 0 & \cdots & 0 & N_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & N_n \end{bmatrix}$$

for two well-chosen integers a_0 and b_0. Hence, $(d_1, d_{21}, \ldots, d_{n1}, -k_2, \ldots, -k_n)B_0$ belongs to $\mathcal{L}_0$. That is $(a_0 d_1, b_0 d_{21}, \ldots, b_0 d_{n1}, k_2(1-p_2-q_2)+1, \ldots, k_n(1-p_n-q_n)+1)$ as we know $e_i d_1 + e_i d_{i1} D - k_i N_i = e_i d_i - k_i N_i = k_i(1-p_i-q_i)+1$ for $2 \le i \le n$ from the related-key equations of d_i, d_j and the RSA key equations.

We know that $k_i = (e_i d_i - 1)/\varphi(N_i) \approx N^{\delta}$ for $1 \le i \le n$. To balance each coordinate of above vector, we set $a_0 = [N^{\frac{1}{2}}]$ and $b_0 = [N^{\frac{1}{2}+\delta-\beta}]$. The norm of the constructed vector is roughly estimated as $N^{\delta+\frac{1}{2}}$. The determinant of $\mathcal{L}_0$ is $\det(\mathcal{L}_0) = |\det(B_0)| = a_0 b_0^{n-1} \prod_{i=2}^{n} N_i \approx N^{\frac{3}{2}n-1+(n-1)(\delta-\beta)}$ from our construction of the basis matrix B_0.

When applying the Gaussian heuristic, the norm of the reduced basis vectors is roughly $\det(\mathcal{L}_0)^{\frac{1}{2n-1}} \approx N^{\frac{3n-2+2(n-1)(\delta-\beta)}{2(2n-1)}}$. Similarly, we have $d_1 = a_1 c_1 + a_2 c_2 + \cdots + a_{2n-1} c_{2n-1}$ as an integer linear combination of $(2n-1)$ unknown variables, where a_i's come from the first column vector of the unimodular transformation matrix. We have $|a_i| \approx \det(\mathcal{L}_0)^{\frac{1}{2n-1}}/a_0 \approx N^{\frac{3n-2+2(n-1)(\delta-\beta)}{2(2n-1)} - \frac{1}{2}} = N^{\frac{(n-1)(2\delta-2\beta+1)}{2(2n-1)}}$ and hence $|c_i| \approx |d_1/a_1| \approx N^{\delta - \frac{(n-1)(2\delta-2\beta+1)}{2(2n-1)}} = N^{\frac{2n\delta+2(n-1)\beta-n+1}{2(2n-1)}}$.

Substituting the alternative expression of d_1 in $e_1 d_1 = k_1(N_1+1-p_1-q_1)+1$, we try to solve $x(y-N_1-1) + e_1 a_1 z_1 + \cdots + e_1 a_{\hat{n}} z_{\hat{n}} - 1 \bmod e_1 a_{\hat{n}+1}$ in $(\hat{n}+2)$ variables with the root $(k_1, p_1+q_1, c_1, \ldots, c_{\hat{n}})$ for $\hat{n} = 2n-2$. Letting $u := xy-1$, it can be rewritten in the linear form as $f_{\hat{n}}(x, z_1, \ldots, z_{\hat{n}}, u) := u - (N_1+1)x + e_1 a_1 z_1 + \cdots + e_1 a_{\hat{n}} z_{\hat{n}} \bmod e_1 a_{\hat{n}+1}$. The shift polynomials are defined as $g_{[i,j,k,l_1,\ldots,l_{\hat{n}}]}(x, z_1, \ldots, z_{\hat{n}}, u) := x^i y^j z_1^{l_1} \cdots z_{\hat{n}}^{l_{\hat{n}}} f_{\hat{n}}^k E^{s-k}$ for $E = e_1 a_{\hat{n}+1}$, a positive integer s and $i, j, k, l_1, \ldots, l_{\hat{n}} \in \mathbb{N}$.

Analogous to the lattice-based solution applied to the case of two instances, we finally obtain the following proposition for the case of n instances.

Proposition 2. *Let $N_i = p_i q_i$ for $1 \le i \le n$ be given RSA moduli of the same bit-size, where p_i and q_i are large primes of the same bit-size. Let e_i and d_i be some integers satisfying $e_i d_i \equiv 1 \bmod (p_i-1)(q_i-1)$ such that $e_i \approx N$ and $d_i \approx N^{\delta}$. Given the implicit information that $d_j = d_i + d_{ji} D$ for $1 \le i < j \le n$ with $|d_{ji}| \approx N^{\beta}$. Then given RSA moduli can be factored in polynomial time (but exponential in n) if*

$$\delta < \frac{1}{2} - \beta + \frac{2n^2 + n - 1 + 4n^2\beta - \sqrt{(2n-1)(6n^3+3n^2-1-8n^2(n-1)\beta)}}{4n^3}.$$

We illustrate the above result with respect to various β's in Fig. 2 and discuss more about it. On the one hand, we can achieve higher insecure bound as β decreases. On the other hand, exposing more RSA instances with implicit related-keys is more vulnerable. Let n go to infinity, the asymptotic upper bound converges to $\frac{1}{2} - \beta$. Consequently, it indicates that the proposed attack is effective for $\delta < \frac{1}{2}$ at best for $\beta = 0$, which is the same as the conjecture of the previous small exponent attack [1] unless there exist more effective attacks.

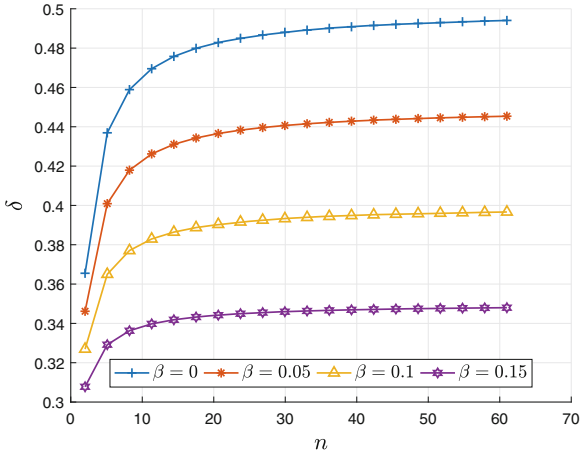

Fig. 2. The comparison of the upper bounds on δ of the proposed implicit related-key factorization attack for given n RSA instances with respect to $\beta = 0$, $\beta = 0.05$, $\beta = 0.1$ and $\beta = 0.15$.

4 Experimental Results

We verify the validity of the proposed attacks analyzed in Sect. 3 on the implicit related-key factorization problem for two instances. The experiments are carried out in `SageMath` under Windows 10 running on a laptop with Intel Core i7-8550U CPU 1.80 GHz. The numbers for generating the parameters of two RSA instances are chosen at random.

To be specific, we first generate two 1024-bit RSA moduli N_1 and N_2. Then we generate the implicit related-keys d_1 and d_2 with certain shared MSBs and LSBs according to the preset values of β and γ. Finally, we compute the corresponding public keys e_1 and e_2 from N_1, d_1 and N_2, d_2, respectively.

In each numerical experiment, we choose a suitable s with an optimal τ for constructing the lattice, which implies we shall first reduce a two-dimensional lattice and then another m-dimensional one. The comparison of the asymptotic and experimental results are given in Table 2. The γ and β-columns provide the concrete attack scenarios, by which we randomly generate two related private keys. The amounts (recorded in bits) of shared MSBs and LSBs are given in the MSBs and LSBs-columns. The δ_∞-column provides the asymptotic bounds on δ when s goes to infinity. The δ_e-column provides the experimental bounds for our lattice settings indicated by the s, τ and m-columns. The respective time consumption (recorded in seconds) of the LLL algorithm and the Gröbner basis computation are given in the TL and TG-columns.

During the experiments, we can collect sufficient polynomials satisfying our requirements. In other words, after running the LLL algorithm, we obtain enough short reduced basis vectors. The polynomial equations sharing the common root

Table 2. The comparison of asymptotic bounds and experimental results on δ of the proposed implicit related-key factorization attack for given two RSA instances.

γ	β	MSBs	LSBs	δ_∞	δ_e	s	τ	m	TL	TG
0.117	0.048	130	120	0.346	0.292	5	0.200	136	112.834	0.121
0.117	0.039	163	120	0.350	0.315	6	0.166	225	1933.569	0.151
0.043	0.058	199	44	0.342	0.295	5	0.200	136	140.853	0.122
0.034	0.063	204	35	0.340	0.296	6	0.166	225	1647.016	0.176
0.078	0.092	123	80	0.329	0.290	5	0.200	136	174.732	0.146
0.078	0.097	121	80	0.327	0.293	6	0.166	225	2336.019	0.162

over the integers are derived from the vector-to-equation transformation of the outputted lattice vectors. Based on the observation from Table 2, we briefly comment on the root-extraction procedure of the proposed attack. We put the derived polynomials into the Gröbner basis computation and obtain $p_2 + q_2$ that leads to the factorization of N_2. As mentioned before, we can also obtain the factorization of N_1. The time consumption of the Gröbner basis computation is much lower than that for running the LLL algorithm.

5 Concluding Remarks

In this paper, we propose the formulation of a new problem with respect to implicit related-key factorization, whose goal is to factor RSA moduli with the help of implicit information about related private keys. We then propose lattice-based attacks using Coppersmith's techniques, which are applied for solving modular polynomials as a powerful tool. Another technique we adapt is the splitting technique, which can split a variable of the large norm into some variables of the smaller norm.

We analyze the implicit related-key factorization problem for a special case when given two RSA instances. A lattice-based attack for such case is proposed and illustrated. We further verify the validity of the proposed attack by numerical experiments. For the case of more than two RSA instances, a similar attack is proposed based on a heuristic lattice construction. The concrete matrix construction with respect to the splitting technique may be improved (i.e. a_0 and b_0 can be further optimized).

Acknowledgments. The authors would like to thank the anonymous reviewers for their valuable comments and suggestions. This work was partially supported by the National Natural Science Foundation of China (Grant No. 61632013) and Anhui Initiative in Quantum Information Technologies under Grant AHY150400.

References

1. Boneh, D., Durfee, G.: Cryptanalysis of RSA with private key d less than $N^{0.292}$. In: Stern, J. (ed.) EUROCRYPT 1999. LNCS, vol. 1592, pp. 1–11. Springer, Heidelberg (1999). https://doi.org/10.1007/3-540-48910-X_1
2. Boneh, D., Durfee, G., Frankel, Y.: An attack on RSA given a small fraction of the private key bits. In: Ohta, K., Pei, D. (eds.) ASIACRYPT 1998. LNCS, vol. 1514, pp. 25–34. Springer, Heidelberg (1998). https://doi.org/10.1007/3-540-49649-1_3
3. Buchberger, B., Winkler, F.: Gröbner Bases and Applications. London Mathematical Society Lecture Note Series, vol. 251. Cambridge University Press, Cambridge (1998)
4. Coppersmith, D.: Finding a small root of a bivariate integer equation; factoring with high bits known. In: Maurer, U. (ed.) EUROCRYPT 1996. LNCS, vol. 1070, pp. 178–189. Springer, Heidelberg (1996). https://doi.org/10.1007/3-540-68339-9_16
5. Coppersmith, D.: Finding a small root of a univariate modular equation. In: Maurer, U. (ed.) EUROCRYPT 1996. LNCS, vol. 1070, pp. 155–165. Springer, Heidelberg (1996). https://doi.org/10.1007/3-540-68339-9_14
6. Coppersmith, D.: Small solutions to polynomial equations, and low exponent RSA vulnerabilities. J. Cryptol. **10**(4), 233–260 (1997)
7. Coron, J.-S.: Finding small roots of bivariate integer polynomial equations revisited. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 492–505. Springer, Heidelberg (2004). https://doi.org/10.1007/978-3-540-24676-3_29
8. Coron, J.-S.: Finding small roots of bivariate integer polynomial equations: a direct approach. In: Menezes, A. (ed.) CRYPTO 2007. LNCS, vol. 4622, pp. 379–394. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-74143-5_21
9. Coron, J.S., May, A.: Deterministic polynomial-time equivalence of computing the RSA secret key and factoring. J. Cryptol. **20**(1), 39–50 (2007)
10. 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). https://doi.org/10.1007/11426639_22
11. Gama, N., Nguyen, P.Q.: Predicting lattice reduction. In: Smart, N. (ed.) EUROCRYPT 2008. LNCS, vol. 4965, pp. 31–51. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-78967-3_3
12. 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). https://doi.org/10.1007/978-3-642-13013-7_4
13. Howgrave-Graham, N.: Finding small roots of univariate modular equations revisited. In: Darnell, M. (ed.) Cryptography and Coding 1997. LNCS, vol. 1355, pp. 131–142. Springer, Heidelberg (1997). https://doi.org/10.1007/BFb0024458
14. Lenstra, A.K., Lenstra, H.W., Lovász, L.: Factoring polynomials with rational coefficients. Math. Ann. **261**(4), 515–534 (1982)
15. May, A.: New RSA vulnerabilities using lattice reduction methods. Ph.D. thesis, University of Paderborn (2003)
16. May, A., Ritzenhofen, M.: Implicit factoring: on polynomial time factoring given only an implicit hint. In: Jarecki, S., Tsudik, G. (eds.) PKC 2009. LNCS, vol. 5443, pp. 1–14. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-00468-1_1

17. Peng, L., Hu, L., Lu, Y., Xu, J., Huang, Z.: Cryptanalysis of dual RSA. Des. Codes Cryp. **83**(1), 1–21 (2017)
18. Rivest, R.L., Shamir, A., Adleman, L.: A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM **21**(2), 120–126 (1978)
19. Sarkar, S., Maitra, S.: Approximate integer common divisor problem relates to implicit factorization. IEEE Trans. Inf. Theory **57**(6), 4002–4013 (2011)
20. Sun, H.M., Wu, M.E., Ting, W.C., Hinek, M.J.: Dual RSA and its security analysis. IEEE Trans. Inf. Theory **53**(8), 2922–2933 (2007)
21. Takayasu, A., Lu, Y., Peng, L.: Small CRT-exponent RSA revisited. In: Coron, J.-S., Nielsen, J.B. (eds.) EUROCRYPT 2017. LNCS, vol. 10211, pp. 130–159. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-56614-6_5