IEICE TRANSACTIONS

on Fundamentals of Electronics, Communications and Computer Sciences

VOL. E103-A NO. 8
AUGUST 2020

A PUBLICATION OF THE ENGINEERING SCIENCES SOCIETY
The Institute of Electronics, Information and Communication Engineers
Kikai-Shinko-Kaikan Bldg., 5-8, Shibakoen 3 chome, Minato-ku, TOKYO, 105-0011 JAPAN

PAPER

Lattice-Based Cryptanalysis of RSA with Implicitly Related Keys*

Mengce ZHENG[†a)], ***Nonmember***, **Noboru KUNIHIRO**[††], ***Senior Member***, ***and*** **Honggang HU**[†], ***Nonmember***

SUMMARY We address the security issue of RSA with implicitly related keys in this paper. Informally, we investigate under what condition is it possible to efficiently factorize RSA moduli in polynomial time given implicit relation of the related private keys that certain portions of bit pattern are the same. We formulate concrete attack scenarios and propose lattice-based cryptanalysis by using lattice reduction algorithms. A subtle lattice technique is adapted to represent an unknown private key with the help of known implicit relation. We analyze a simple case when given two RSA instances with the known amount of shared most significant bits (MSBs) and least significant bits (LSBs) of the private keys. We further extend to a generic lattice-based attack for given more RSA instances with implicitly related keys. Our theoretical results indicate that RSA with implicitly related keys is more insecure and better asymptotic results can be achieved as the number of RSA instances increases. Furthermore, we conduct numerical experiments to verify the validity of the proposed attacks.

key words: *RSA, implicitly related keys, cryptanalysis, factorization, lattice*

1. Introduction

Background. The RSA cryptosystem [31] plays an important role in the area of public-key cryptography and information security due to its simplicity and popularity. In the standard RSA scheme, the key equation is $ed \equiv 1 \pmod{\varphi(N)}$, where N, e, d and $\varphi(N)$ are defined as follows. N is the product of two large primes p, q of the same bit-size. (N, e) and (p, q, d) denote the public and private keys, respectively. e and d are also called the public (or encryption) and private (or decryption) exponents. $\varphi(N) = (p-1)(q-1)$ is Euler's totient function. To encrypt an integer m, one needs to compute $c = m^e \pmod{N}$. To decrypt the ciphertext c, one needs to compute $c^d \pmod{N}$. The correctness of $c^d = m^{ed} = m \pmod{N}$ is guaranteed by Euler's theorem. Its vulnerability was surveyed in [3] after two decades of research into attacking the RSA cryptosystem.

In 1996, Coppersmith [7]–[9] made a significant breakthrough based on finding small roots of modular and integer polynomial equations. The fundamental works proposed novel and advanced attacks on RSA using lattice reduction algorithms, e.g. the LLL algorithm [23]. The main method is known as lattice-based techniques and has been widely applied in cryptanalyses of RSA and its variants afterwards. Many researchers proposed several nice attacks such as [2], [4], [10], [11], [13], [21], [25], [39] etc. Among them, the *partial key exposure attack* has been intensively studied as an active attack scenario.

In 1998, Boneh et al. [5] proposed several attacks on RSA given a fraction of the private key bits with small public exponent e. Their attacks employed some known most significant bits (MSBs) or some known least significant bits (LSBs) of the private exponent d. In practice, above partial key information can be captured using side channel attacks, e.g. cold boot attacks [16] and others [22], [30]. Therefore, the partial key exposure attack has gradually become an important part when estimating the security of RSA.

In 2003, Blömer and May [2] improved partial key exposure attacks on RSA using Coppersmith's lattice-based techniques. They showed that RSA is also vulnerable for larger public exponent e given some private key exposure. In 2005, Ernst et al. [13] presented several new attacks that work up to full size exponents via three theorems under a heuristic assumption. The best known attack was proposed by Takayasu and Kunihiro [37], [38], which can achieve Boneh-Durfee bound of small private exponent attack on RSA [4]. In our opinion, partial key exposure attack can be refined to the problem of factorizing RSA modulus with an oracle that outputs some *explicit* information of the private key d.

In 2009, May and Ritzenhofen [28] proposed the *implicit factorization problem* to factorize RSA moduli with an oracle that provides *implicit* information about the prime factors. To be specific, for two different RSA moduli $N_1 = p_1 q_1$ and $N_2 = p_2 q_2$ with α-bit q_i's and p_1, p_2 sharing at least t LSBs, they proved that q_1 and q_2 can be recovered if $t > 2(\alpha + 2)$ holds. Thus, N_1 and N_2 can be factorized easily. They later extended the analysis to the case of k moduli and improved the insecure bound to $t > \frac{k}{k-1}\alpha$ by acquiring more oracle queries. This problem is mainly considered in the area of malicious generation of RSA moduli, e.g. the construction of backdoor RSA moduli.

Later, other implicit information like shared MSBs and shared middle bits were studied by Faugére et al. [14]. Sarkar and Maitra [34] proposed a new approach based on the idea of solving approximate common divisor problem to further improve the previous results. The best known attack was proposed by Lu et al. [24], which made use of the following tricky technique. They introduced a new variable to miti-

Manuscript received December 22, 2019.
Manuscript revised April 5, 2020.

[†]The authors are with the Key Laboratory of Electromagnetic Space Information, CAS, University of Science and Technology of China, Hefei, China.

[††]The author is with the Department of Computer Science, University of Tsukuba, Tsukuba-shi, 305-8573 Japan.

*This is a revised and extended version of the paper "Implicit Related-Key Factorization Problem on the RSA Cryptosystem" [41] that has been presented in CANS 2019.

a) E-mail: mczheng@ustc.edu.cn (Corresponding author)

DOI: 10.1587/transfun.2019EAP1170

gate the effect of large prime factors, which correspond to unknown variables in the polynomial equations to be solved. It is the first time that this problem can be experimentally handled for balanced RSA moduli. However, in order to successfully factorize given three RSA moduli, one still needs to know that p_i's share nearly 90% MSBs.

Implicit Related-Key Factorization Problem. Inspired by the partial key exposure attack and the implicit factorization problem, we raise an interesting problem how to efficiently factorize RSA moduli for given some implicit information about the related private keys. We present the description of the *implicit related-key factorization problem* as follows. Consider $(N_1, e_1, d_1), \ldots, (N_n, e_n, d_n)$ are n distinct key pairs, where $N_1, \ldots, N_n$ are of the same bit-size and their prime factors are all of the same bit-size. Given that certain portions of bit pattern in the implicitly related private keys $d_1, \ldots, d_n$ are common,[†] under what condition is it possible to efficiently factorize $N_1, \ldots, N_n$. In this sense, the implicit factorization problem can be refined into the implicit related-prime factorization problem accordingly.

Some researchers have studied and extended previous lattice-based attacks on RSA with more than one key pair for a *common* modulus. Sarkar and Maitra [32], [33] studied the weakness of RSA when given more RSA key pairs for the same modulus. Aono [1] also gave improved bounds by Minkowski sum based lattice construction. Takayasu and Kunihiro [36] proposed better cryptanalytic results for multiple small private exponents. Additionally, Hinek [18, Chapter 4] studied another case when given many RSA moduli along with a *common* private key. Its implicit information is that all the private keys are identical. Our problem can be seen as an extension of above two special cases.

There are several situations of using more distinct RSA instances in practice. For example, Dual RSA scheme proposed in [35] is applied to blind signatures and authentication. Once such RSA instances are generated with imperfect randomness or malicious backdoor keys, one may encounter our implicit related-key factorization problem. Our motivations come from two aspects. On the one hand, side channel attacks may not give explicit information like the exact bits of the private keys as expected. Instead, one may know the amounts of shared MSBs and LSBs of the private keys as some implicit information. On the other hand, malicious attackers may control backdoor keys rather than backdoor RSA moduli. The users' misuses of their private keys with certain repeated bit patterns may lead to this problem as well. Mainly from the theoretical view, our aim is to further disclose the vulnerability of RSA with weaker condition and enrich lattice-based cryptanalyses in the literature.

Our Contributions. Firstly, we provide the formalization of the implicit related-key factorization problem. We identify a hybrid problem based on the partial key exposure attack and the implicit factorization problem. The formal description will be provided shortly afterwards. Secondly, we propose lattice-based cryptanalyses and several specific attacks. Our cryptanalyses are based on Coppersmith's techniques. In addition to the fundamental techniques, we further adapt two subtle lattice techniques, namely the linearization technique and the splitting technique. We present lattice-based attacks for given two RSA instances and extend a heuristic lattice construction for given more RSA instances. Thirdly, we provide verification by computer experiments. We justify the validity of the proposed attacks by various numerical experiments.

We formulate the implicit related-key factorization problem using several RSA instances clearly. For n key pairs of RSA parameters (N_i, e_i, d_i) with $1 \le i \le n$, we consider the full size case of $e_i \approx N$, where N denotes an integer of the same bit-size as N_i. Unless otherwise noted, N denotes an integer of the same bit-size as given RSA moduli in this paper. The moduli $N_1, \ldots, N_n$ are assumed given in descending order without loss of generality. Besides, we assume $d_i \approx N^\delta$ and all the private keys share MSBs of bit-size $(\delta - \beta - \gamma)\log_2 N$ and LSBs of bit-size $\gamma \log_2 N$ leaving middle difference of bit-size $\beta \log_2 N$. To be specific, we assume the implicit relation is $d_j = d_i + d_L d_{ji}$ for $1 \le i < j \le n$ with known value $d_L = 2^{\lfloor \gamma \log_2 N \rfloor}$ and unknown value d_{ji} satisfying $|d_{ji}| \approx N^\beta$. The size relation between δ, β and γ is $0 < \beta,\ \gamma,\ \beta + \gamma < \delta$. The goal of the problem is to factorize the RSA moduli $N_1, \ldots, N_n$ for given public data $(N_1, e_1, \ldots, N_n, e_n)$ and known parameters δ, β and γ.

We follow Coppersmith's techniques [9] to deal with the implicit related-key factorization problem. Our attacks rely on the following *heuristic assumption*, which is always mentioned in the literature. Because our lattice-based attacks are eventually reduced to solving multivariate polynomial equations, we assume that algebraically independent polynomials can be obtained from our attacks throughout the paper. Thus, the small roots can be efficiently extracted by resultant computations or the Gröbner basis computations [6].

Our main results are stated in Proposition 1 and Proposition 2. We want to point out that the theoretical results are asymptotic since we require the corresponding lattice dimension to be preferably large. We first give the results for given two RSA instances and then extend to more RSA instances.

Proposition 1: Let $N_1 = p_1 q_1$ and $N_2 = p_2 q_2$ 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 $e_1 d_1 \equiv 1 \pmod{(p_1 - 1)(q_1 - 1)}$ and $e_2 d_2 \equiv 1 \pmod{(p_2 - 1)(q_2 - 1)}$ such that $e_1 \approx e_2 \approx N$ and $d_1 \approx d_2 \approx N^\delta$. Given that $d_2 = d_1 + d_L d_{21}$ with $|d_{21}| \approx N^\beta$ and $d_L = 2^{\lfloor \gamma \log_2 N \rfloor}$. Then N_1 and N_2 can be factorized in polynomial time if

$$\delta < \max\left(\frac{25 - 16\beta - \sqrt{177 - 96\beta}}{32},\ \frac{2\gamma + 3 - \sqrt{\gamma + 2}}{6} \right).$$

Proposition 2: Let $N_i = p_i q_i$ for $1 \le i \le n$ be given RSA

[†]The private keys are supposed of the same bit-size, otherwise MSBs of the shorter ones can be padded with zero to make it true.

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 $e_i d_i \equiv 1 \pmod{(p_i-1)(q_i-1)}$ such that $e_i \approx N$ and $d_i \approx N^{\delta}$. Given the implicit information that $d_j = d_i + d_L d_{ji}$ for $1 \le i < j \le n$ with $|d_{ji}| \approx N^{\beta}$. Then given RSA moduli can be factorized in polynomial time (but exponential in n) if

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

Actually, the formula presented in Proposition 2 covers that in Proposition 1 for $n = 2$ with respect to β. But it does not indicate the condition with respect to γ as we apply a different approach for given more RSA instances.

Organizations. The rest of the paper is organized as follows. We provide some basic knowledge of Coppersmith's techniques and Gaussian heuristic in Sect. 2. In Sect. 3, we propose three distinct attacks for given two RSA instances. In addition to the proposed attacks, we discuss the differences and exhibit the superior one. In Sect. 4, we further extend a heuristic lattice construction to analyze the case of given n RSA instances. We verify the validity of the proposed attacks by computer experiments in Sect. 5. Finally, we conclude the paper in Sect. 6.

2. Preliminaries

In this section, we briefly introduce lattice, the LLL algorithm [23] and Coppersmith's techniques [9]. Moreover, we provide a rough condition for finding the common small roots of constructed polynomial equations and present the splitting technique that is based on the Gaussian heuristic.

A lattice $\mathcal{L}$ spanned by linearly independent vectors $\vec{b}_1, \ldots, \vec{b}_m \in \mathbb{R}^n$ is the set of their integer linear combinations, which is denoted by $\mathcal{L}(\vec{b}_1,\ldots,\vec{b}_m) = \left\{\sum_{i=1}^m z_i\vec{b}_i : z_i \in \mathbb{Z}\right\}$. These basis vectors derive a basis matrix B by regarding each $\vec{b}_i$ as row (or column) vectors. The determinant of $\mathcal{L}$ is calculated as $\det(\mathcal{L}) = \sqrt{\det(BB^T)}$. m is the rank of $\mathcal{L}$ and we always consider a full-rank lattice when $m = n$. Hence, we have $\det(\mathcal{L}) = |\det(B)|$.

The LLL lattice reduction algorithm proposed by Lenstra, Lenstra and Lovász [23] is practically used for computing approximately short lattice vectors due to its efficient running outputs. We provide the following substratal lemma from [26, Section 2.2 Theorem 4].

Lemma 1: Let lattice $\mathcal{L}$ be spanned by basis vectors $(\vec{b}_1,\ldots,\vec{b}_m)$. The LLL algorithm outputs a reduced basis $(\vec{v}_1,\ldots,\vec{v}_m)$ satisfying the following property in polynomial time for $1 \le i \le m$,

$$\|\vec{v}_1\|, \|\vec{v}_2\|, \ldots, \|\vec{v}_i\| \le 2^{\frac{m(m-1)}{4(m+1-i)}} \det(\mathcal{L})^{\frac{1}{m+1-i}}.$$

Since Howgrave-Graham [20] refined on Coppersmith's techniques to propose a useful lemma, we directly give it for judging whether the desired small roots of a modular equation are also roots over $\mathbb{Z}$ for a given polynomial $g(x_1,\ldots,x_n) = \sum a_{i_1,\ldots,i_n} x_1^{i_1}\cdots x_n^{i_n}$, whose 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 with at most m monomials. Suppose that

1. $g(x_1',\ldots,x_n') \equiv 0 \pmod{R}$, $|x_1'| \le X_1, \ldots, |x_n'| \le X_n$,
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 Lemma 1 and Lemma 2, one can solve modular polynomial equations under a rough condition. One can first construct shift polynomials from a known modular polynomial. Then the shift polynomials' coefficient vectors (with known upper bounds on unknown variables) generate a lattice basis matrix. In the next step, enough integer equations are derived from short reduced vectors through the LLL algorithm.

Consider that one can obtain the first t vectors, then one can extract the solutions if $2^{\frac{m(m-1)}{4(m+1-t)}} \det(\mathcal{L})^{\frac{1}{m+1-t}} < R/\sqrt{m}$, which leads to $\det(\mathcal{L}) < R^{m+1-t}2^{-\frac{m(m-1)}{4}} m^{-\frac{m+1-t}{2}}$. Since we always have $t \ll m \ll R$ in lattice-based cryptanalyses, this condition roughly reduces to

$$\det(\mathcal{L}) < R^m \tag{1}$$

when we ignore the lower terms.

Under above rough condition (1), the first t vectors of the reduced basis can be further transformed into polynomial equations sharing the common roots over the integers. We can apply Gröbner basis computations to extract the common roots since it is efficient for more variables. One can refer to [26], [27] in detail.

Recently, Peng et al. [29] presented improved attacks on the Dual RSA scheme [35] and common private exponent RSA scheme. They used a lattice technique that can discover a linear combination of some lattice reduced basis vectors if the desired result was not directly obtained after running lattice basis reduction algorithms. We call it the splitting technique, which is based on the observation of Gaussian heuristic in certain lattices. We adapt the splitting technique along with the linearization technique [17] to present convenient and lucid lattice constructions. We start from the Gaussian heuristic that is the understructure and then introduce the splitting technique, which aims to split a variable of large norm into several variables of smaller norm by reducing a low-dimensional lattice.

The Gaussian heuristic says that the norm of the shortest non-zero vector $\vec{s}$ of a random m-dimensional lattice $\mathcal{L}$ satisfies $\|\vec{s}\| \approx \sqrt{\frac{m}{2\pi e}} \det(\mathcal{L})^{\frac{1}{m}}$. $\|\vec{s}\|$ is also written as $\lambda_1(\mathcal{L})$, where the successive minimum $\lambda_i(\mathcal{L})$ denotes the i-th minimum of $\mathcal{L}$, which means that it is the radius of the smallest zero-centered ball containing at least i many linearly independent lattice vectors. One may refer to [19, Section 6.5.3] for more details.

A further claim on this property of random lattices can be found in [15]. 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 $\lambda_i(\mathcal{L})/\det(\mathcal{L})^{\frac{1}{m}} \approx \sqrt{\frac{m}{2\pi e}}$ for all $1 \le i \le m$. Though the constructed low-dimensional lattices in our attacks are not random lattices as described in the Gaussian heuristic, the norms of the reduced basis vectors are asymptotically close to $\det(\mathcal{L})^{\frac{1}{m}}$ according to practical experiments. Furthermore, we have $|v_{i1}| \approx \det(\mathcal{L}_0)^{\frac{1}{m}}$ that is useful in our analyses[†], where $\vec{v}_i$ (for $1 \le i \le m$) is a reduced basis vector after running the LLL algorithm on constructed m-dimensional full-rank lattice $\mathcal{L}_0$.

3. Cryptanalysis for Given Two Instances

In this section, we propose our attacks for given two RSA instances (N_1, e_1, d_1) and (N_2, e_2, d_2). Recall that the analytic scenario is $e_1 \approx e_2 \approx N$, where N denotes an integer with the same bit-size as N_1, N_2 and the private keys $d_1 \approx d_2 \approx N^\delta$ share some MSBs and LSBs leaving one different block in the middle. Specifically, we assume the attacker learns that $d_2 = d_1 + d_L d_{21}$ with known values δ, β, γ and $d_L = 2^{\lfloor \gamma \log_2 N \rfloor}$, where unknown d_{21} satisfying $|d_{21}| \approx N^\beta$ denotes the difference between two unknown middle blocks.

3.1 Using Two-Dimensional Lattices

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 $e_1 d_1 \equiv 1 \pmod{\varphi(N_1)}$ and $\varphi(N_1) = (p_1 - 1)(q_1 - 1) = N_1 + 1 - p_1 - q_1$, we have $e_1 d_1 - k_1 N_1 = k_1(1 - p_1 - q_1) + 1$ for a positive integer k_1. Then we know $(d_1, -k_1)B_0 = (a_0 d_1, k_1(1 - p_1 - q_1) + 1)$ is a vector belonging to $\mathcal{L}_0$. We have $k_1 = (e_1 d_1 - 1)/\varphi(N_1) \approx N^\delta$. To let each coordinate of $(a_0 d_1, k_1(1-p_1-q_1)+1)$ be balanced, we set $a_0 \approx N^{\frac{1}{2}}$. Then its norm is $\|(a_0 d_1, k_1(1 - p_1 - q_1) + 1)\| \approx N^{\delta + \frac{1}{2}}$. We know the determinant of $\mathcal{L}_0$ is $\det(\mathcal{L}_0) = |\det(B_0)| = a_0 N_1 \approx N^{\frac{3}{2}}$ 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}) derived from the lattice reduction algorithms. Further by applying the Gaussian heuristic, we have $\|(s_{11}, s_{12})\| = \|(s_{21}, s_{22})\| \approx \det(\mathcal{L}_0)^{\frac{1}{2}} \approx N^{\frac{3}{4}}$ with a high possibility. It means that the sizes of all coordinates s_{11}, s_{12}, s_{21} and s_{22} are roughly $N^{\frac{3}{4}}$. Actually, we have $s_{11} = a_0 a_1$ and $s_{21} = a_0 a_2$ since the reduced basis vectors are generated by B_0 as follows.

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

where known integers a_1 and a_2 are elements appearing in the first column vector of the unimodular transformation matrix.

On the other hand, we have $a_0 d_1 = s_{11} c_1 + s_{21} c_2$ since (s_{11}, s_{12}) and (s_{21}, s_{22}) are also basis vectors of $\mathcal{L}_0$. Thus, we obtain $d_1 = a_1 c_1 + a_2 c_2$ for unknown c_1 and c_2. Combining it with $d_2 = d_1 + d_L d_{21}$, we finally have $d_2 = a_1 c_1 + a_2 c_2 + d_L d_{21}$. Now we figure out the sizes of above parameters. It can be easily deduced that $|a_1| \approx |a_2| \approx N^{\frac{1}{4}}$ and hence $|c_1| \approx |c_2| \approx N^{\delta - \frac{1}{4}}$. We substitute the expression of d_2 in another key equation $e_2 d_2 = k_2(N_2 + 1 - p_2 - q_2) + 1$. That is $e_2(a_1 c_1 + a_2 c_2 + d_L d_{21}) = k_2(N_2 + 1 - p_2 - q_2) + 1$. Therefore, we turn to solving the following modular polynomials for the implicit related-key factorization problem. The first polynomial $f_1(x, y, z, w)$ is

$$x(y - N_2 - 1) + e_2 a_1 z + e_2 d_L w - 1 \pmod{e_2 a_2} \quad (2)$$

with roots $(k_2, p_2 + q_2, c_1, d_{21})$. The second polynomial $f_2(x, y, z, w)$ is

$$x(y - N_2 - 1) + e_2 a_1 z + e_2 a_2 w - 1 \pmod{e_2 d_L} \quad (3)$$

with roots $(k_2, p_2 + q_2, c_1, c_2)$. Notice that we need to deal with the modular polynomials in four variables. To provide elegant lattice constructions, we further apply the linearization technique introduced in [17].

3.1.1 The First Attack

To solve the first polynomial (2), we let $u := xy - 1$ and derive the following linear polynomial

$$\bar{f}_1(x, z, w, u) := u - (N_2 + 1)x + e_2 a_1 z + e_2 d_L w \pmod{e_2 a_2}.$$

The shift polynomials $g_{[i,j,k,l_1,l_2]}(x, y, z, w, u)$ are defined as

$$g_{[i,j,k,l_1,l_2]}(x, y, z, w, u) := x^i y^j z^{l_1} w^{l_2} \bar{f}_1^k(x, z, w, u) E^{s-k}$$

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 shift polynomials by $\mathcal{G}$ that can be written as $\mathcal{G} := \mathcal{G}_1 \cup \mathcal{G}_2$, where

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

for an optimizing parameter $0 \le \tau \le 1$ to be determined later. Thus, all the shift polynomials in $\mathcal{G}$ share the common roots $(k_2, p_2 + q_2, c_1, d_0, k_2(p_2 + q_2) - 1)$ modulo E^s.

By introducing auxiliary parameters $r = i + k + l_1 + l_2$ and

[†]The splitting technique in our proposed attacks only deals with the first column vector, namely $(v_{11}, \ldots, v_{m1})$.

Table 1 A toy example of lattice basis matrix for $s = 1$ and $\tau = 1$ with $E = e_2a_2$ 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_2d_LW		U	
$g_{[0,1,1,0,0]}(xX, yY, zZ, wW, uU)$	C			e_2a_1YZ		e_2d_LYW	CU	YU

$r' = i' + k' + l_1' + l_2'$, 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 the small roots. The rows and columns of B are set according to above polynomial and monomial orders $\prec$. Two parameters s and τ 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.

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.

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

where the exponents s_x, s_y, s_z, s_w, s_u and s_E are the contributions of the diagonal entries to the determinant. 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, omitting the rounding of τl_1 since it is negligible for asymptotic analysis with sufficiently large s, we have $s_x = \frac{1}{120}s^5 + o(s^5)$, $s_y = \frac{\tau^2}{20}s^5 + o(s^5)$, $s_z = s_w = s_u = \frac{1+4\tau}{120}s^5 + o(s^5)$, $s_E = \frac{4+11\tau}{120}s^5 + o(s^5)$. From condition (1) with $R = E^s$ for acquiring enough integer equations sharing the common roots, we have

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

where the lower terms are neglected. Moreover, let s go to infinite and we 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 $\xi_x, \xi_y, \xi_z, \xi_w, \xi_u$ and ξ_E denote the exponents of the upper bounds. We reduce the crucial condition to a simplified one that is

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

Since we know $\xi_x = \delta$, $\xi_y = \frac{1}{2}$, $\xi_z = \delta - \frac{1}{4}$, $\xi_w = \beta$, $\xi_u = \delta + \frac{1}{2}$, $\xi_E = \frac{5}{4}$, we hence have $\delta + 3\tau^2 + (1+4\tau)\left(\delta - \frac{1}{4} + \beta + \delta + \frac{1}{2} - \frac{5}{4}\right) < 0$, which leads to $\delta < \frac{(1-\beta)(1+4\tau)-3\tau^2}{3+8\tau}$. The right side reaches its maximum by taking $\tau = \frac{\sqrt{177-96\beta}-9}{24}$. We put it in the inequality and hence derive the final condition

$$\delta < \frac{25 - 16\beta - \sqrt{177-96\beta}}{32}. \quad (5)$$

Once $(k_2, p_2+q_2, c_1, d_{21}, k_2(p_2+q_2)-1)$ are extracted, we can easily factorize N_2 since knowing the value of $p_2 + q_2$. We further have d_2 from the key equation $d_2 = e_2^{-1} \pmod{\varphi(N_2)}$, which is used to recover d_1 by $d_1 = d_2 - d_L d_{21}$. Thus, we can factorize N_1 since knowing d_1 is equivalent to knowing the factorization of N_1, which has been proven in [12].

3.1.2 The Second Attack

To solve the second polynomial (3), we let $u := xy - 1$ and derive the following linear polynomial

$$\bar{f_2}(x, z, w, u) := u - (N_2+1)x + e_2a_1z + e_2a_2w \pmod{e_2d_L}.$$

The shift polynomials $g_{[i,j,k,l_1,l_2]}(x, y, z, w, u)$ are defined similarly to the foregoing case,

$$g_{[i,j,k,l_1,l_2]}(x, y, z, w, u) := x^i y^j z^{l_1} w^{l_2} \bar{f_2}^k(x, z, w, u) E^{s-k}$$

for $E = e_2d_L$, a positive integer s and $i, j, k, l_1, l_2 \in \mathbb{N}$.

The concrete lattice construction is identical to that of Sect. 3.1.1 along with the construction of the set $\mathcal{G}$ of the shift polynomials. Therefore, we focus on the simplified crucial condition (4). The only differences between two attacks are the upper bounds on unknown variables as well as their exponents based on N. We figure out them in the second attack as follows: $\xi_x = \delta$, $\xi_y = \frac{1}{2}$, $\xi_z = \xi_w = \delta - \frac{1}{4}$, $\xi_u = \delta + \frac{1}{2}$, $\xi_E = 1 + \gamma$. Thus, we have $\delta + 3\tau^2 + (1+4\tau)\left(\delta - \frac{1}{4} + \delta - \frac{1}{4} + \delta + \frac{1}{2} - 1 - \gamma\right) < 0$. We then infer that

$$\delta < \frac{(1+\gamma)(1+4\tau) - 3\tau^2}{4+12\tau}.$$

The right side reaches its maximum by taking $\tau = \frac{\sqrt{\gamma+2}-1}{3}$. We put it in the inequality and obtain the final condition

$$\delta < \frac{2\gamma + 3 - \sqrt{\gamma+2}}{6}. \quad (6)$$

Once we extract the common roots $(k_2, p_2 + q_2, c_1, c_2, k_2(p_2+q_2)-1)$, we can easily factorize N_2. We further have d_2 from the key equation $d_2 = e_2^{-1} \pmod{\varphi(N_2)}$. On the other hand, we know $d_1 = a_1c_1 + a_2c_2$ from Gaussian heuristic. Thus, we can factorize N_1 since knowing d_1 is equivalent to knowing the factorization of N_1.

3.2 Using Three-Dimensional Lattices

In order to avoid a discussion of modulus E of the constructed polynomials like forms (2) and (3) in Sect. 3.1, we propose a heuristic lattice construction and perform the splitting technique on a three-dimensional lattice, which is constructed by the following basis matrix

$$B_0 = \begin{bmatrix} a_0 & 0 & e_2 \\ 0 & b_0 & e_2 d_L \\ 0 & 0 & N_2 \end{bmatrix}$$

for two well-chosen integers a_0 and b_0. Then we have a vector in $\mathcal{L}_0$ that is $(d_1, d_{21}, -k_2)B_0 = (a_0d_1, b_0d_{21}, e_2d_1 + e_2d_Ld_{21} - k_2N_2) = (a_0d_1, b_0d_{21}, e_2d_2 - k_2N_2) = (a_0d_1, b_0d_{21}, k_2(1 - p_2 - q_2) + 1)$. Since $k_2 \approx N^{\delta}$, we set $a_0 \approx N^{\frac{1}{2}}$ and $b_0 \approx N^{\frac{1}{2}+\delta-\beta}$ to balance its coordinate.

Then its norm is roughly $N^{\delta+\frac{1}{2}}$. We calculate the determinant of $\mathcal{L}_0$ as $\det(\mathcal{L}_0) = |\det(B_0)| = a_0b_0N_2 \approx N^{2+\delta-\beta}$ from our construction of the basis matrix B_0. In this case, we split d_1 into a linear combination of three smaller variables as $d_1 = a_1c_1 + a_2c_2 + a_3c_3$ for unknown c_1, c_2 and c_3, where known a_1, a_2 and a_3 come from the first column vector of the unimodular transformation matrix. We have $|a_i| \approx \det(\mathcal{L})^{\frac{1}{3}}/a_0 \approx N^{\frac{2\delta-2\beta+1}{6}}$ and hence $|c_i| \approx N^{\delta-\frac{1+2\delta-2\beta}{6}} = N^{\frac{4\delta+2\beta-1}{6}}$.

We substitute the expression of d_1 in the key equation $e_1d_1 = k_1(N_1 + 1 - p_1 - q_1) + 1$ and obtain

$$e_1(a_1c_1 + a_2c_2 + a_3c_3) = k_1(N_1 + 1 - p_1 - q_1) + 1.$$

So we aim to solve $f_3(x, y, z, w)$ that is

$$x(y - N_1 - 1) + e_1a_1z + e_1a_2w - 1 \pmod{e_1a_3} \quad (7)$$

with roots $(k_1, p_1 + q_1, c_1, c_2)$.

3.2.1 The Third Attack

We reduce the implicit related-key factorization problem to solving polynomial (7). Since it is a modular polynomial in four variables, we follow the foregoing strategy and define

$$\bar{f}_3(x, z, w, u) := u-(N_1+1)x+e_1a_1z+e_1a_2w \pmod{e_1a_3}$$

for $u := xy - 1$. The shift polynomials are defined similarly except for $E = e_1a_3$ and we skip the detailed lattice construction here. Recall that the crucial condition (4) for acquiring the insecure bound on δ is $\xi_x + 6\tau^2\xi_y + (1 + 4\tau)(\xi_z + \xi_w + \xi_u - \xi_E) < 0$.

We know $\xi_x = \delta$, $\xi_y = \frac{1}{2}$, $\xi_z = \xi_w = \frac{4\delta+2\beta-1}{6}$, $\xi_u = \delta + \frac{1}{2}$, $\xi_E = 1 + \frac{2\delta-2\beta+1}{6}$. Thus, we have $\delta + 3\tau^2 + (1 + 4\tau)\left(\frac{4\delta+2\beta-1}{3} + \delta + \frac{1}{2} - 1 - \frac{2\delta-2\beta+1}{6}\right) < 0$, which leads to $\delta < \frac{(1-\beta)(1+4\tau)-3\tau^2}{3+8\tau}$. The right side reaches its maximum by taking $\tau = \frac{\sqrt{177-96\beta}-9}{24}$. We put it in the inequality and obtain the final condition

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

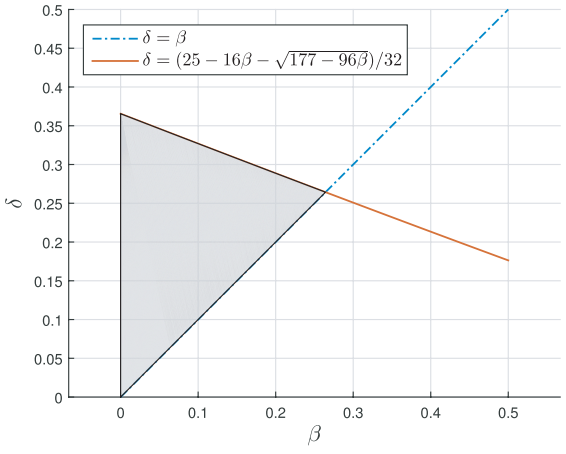
Once $(k_1, p_1 + q_1, c_1, c_2, k_1(p_1 + q_1) - 1)$ are extracted, we can factorize N_1 through $p_1 + q_1$. To factorize N_2, we construct a similar basis matrix and perform the splitting technique on d_2. Interestingly, this insecure bound is identical to (5) in Sect. 3.1.1.

3.3 Illustrations and Discussions

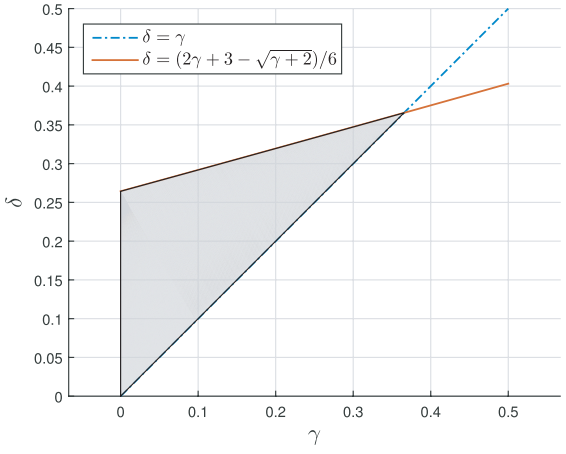
In order to provide a concise solution to the implicit related-key factorization problem, we employ a three-dimensional lattice in Sect. 3.2. However the result is the same as (5) of Sect. 3.1.1 while the latter uses a two-dimensional lattice that is more efficient. We illustrate our main attack results from Sect. 3.1 in Fig. 1. It is obvious that we gain an improvement of the insecure bound on δ with the help of known implicit information about the private keys. For example, we should have $\beta < 0.17$ from our first result (5) if we want to factorize two RSA moduli with $\delta = 0.3$, which means we should already know the implicit information that the private keys share at least $\frac{0.3-0.17}{0.3} \approx 43.3\%$ MSBs and LSBs. Note that there is no restriction on how to distribute two partial amounts of shared MSBs and LSBs.

But if we apply our second result (6) for the same attack scenario with $\delta = 0.3$, we should have $\gamma > 0.13$. It means we should already know the implicit information that the private keys share at least $\frac{0.13}{0.3} \approx 43.3\%$ LSBs. Thus, we observe that the first attack is preferable since the shared bits can locate in both MSBs and LSBs, whereas the shared bits (of the same amount) are forced to locate in LSBs in the second attack.

Furthermore, we show that the first attack is always better than the second one. We consider two attacks for the same δ and discuss the boundary values of β and γ below. We obtain the boundary value of β from (5) that is $\frac{11-16\delta-\sqrt{48\delta+9}}{8}$. On the other hand, we obtain the boundary value of γ from (6) that is $\frac{24\delta-11+\sqrt{48\delta+9}}{8}$. We compare two fractions of shared bits derived from above computations that is $1 - \frac{11-16\delta-\sqrt{48\delta+9}}{8\delta} = \frac{24\delta-11+\sqrt{48\delta+9}}{8\delta}$, which means the implicit information about the amount of shared bits is identical. Since the shared bits of the first attack can be located in both MSBs and LSBs, it is more flexible and



(a) The illustration of (5) of the first attack in Section 3.1.1



(b) The illustration of (6) of the second attack in Section 3.1.2

Fig. 1 The main results of the proposed attacks for given two RSA instances. The solid line denotes the upper bound on δ and the dot-dash line denotes the lower bound. The gray areas indicate the vulnerable scenarios.

suitable for more scenarios.

To summarize, we propose three distinct attacks when given two RSA instances. The first one is the best among them because it offers lower computation complexity and higher flexibility. One may wonder whether our approach can handle the implicit related-key factorization problem for more than two RSA instances. The answer to this question is given in Sect. 4.

4. Cryptanalysis for Given More Instances

We recall the concrete attack scenario for handling n distinct RSA instances. For n key pairs of RSA parameters (N_i, e_i, d_i) with $1 \le i \le n$, we have $e_i \approx N$ and $d_i \approx N^\delta$ with $d_j = d_i + d_L d_{ji}$ for $1 \le i < j \le n$, where $d_L = 2^{\lfloor \gamma \log_2 N \rfloor}$ is known and d_{ji} satisfying $|d_{ji}| \approx N^\beta$ is unknown. Specifically, the attacker aims to factorize the moduli for known δ, β, γ and given public data $(N_1, e_1, \ldots, N_n, e_n)$.

We wish to perform the splitting technique to split d_1 into a linear combination of several smaller unknown variables. However, the low-dimensional lattice construction is not as straightforward as that in Sect. 3.1 when we have more than two RSA instances. This is the reason why we introduce a heuristic construction in Sect. 3.2, which can be easily extended to the case for given more RSA instances.

To do so, we construct a $(2n-1)$-dimensional lattice $\mathcal{L}_0$ that is generated by the following basis matrix

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

for two well-chosen integers a_0 and b_0. We can compute a lattice vector $(d_1, d_{21}, \ldots, d_{n1}, -k_2, \ldots, -k_n)B_0$ in $\mathcal{L}_0$, that is $(a_0 d_1, b_0 d_{21}, \ldots, b_0 d_{n1}, k_2(1 - p_2 - q_2) + 1, \ldots, k_n(1 - p_n - q_n) + 1)$ since we have $e_i d_1 + e_i d_L d_{i1} - k_i N_i = e_i(d_1 + d_L d_{i1}) - k_i N_i = e_i d_i - k_i N_i = k_i(1 - p_i - q_i) + 1$ for $2 \le i \le n$ from the related-key equations $d_j = d_i + d_L d_{ji}$ 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 $a_0 \approx N^{\frac{1}{2}}$ and $b_0 \approx N^{\frac{1}{2}+\delta-\beta}$. 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 basis matrix B_0.

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 write d_1 as an integer linear combination of $(2n-1)$ unknown variables for $d_1 = a_1 c_1 + a_2 c_2 + \cdots + a_{2n-1} c_{2n-1}$, where a_i's are calculated from the first column vector of the unimodular transformation matrix. We have $|a_i| \approx \frac{\det(\mathcal{L}_0)^{\frac{1}{2n-1}}}{a_0} \approx N^{\frac{3n-2+2(n-1)(\delta-\beta)}{2(2n-1)} - \frac{1}{2}} = N^{\frac{(n-1)(2\delta-2\beta+1)}{2(2n-1)}}$ and hence $|c_i| \approx N^{\delta - \frac{(n-1)(2\delta-2\beta+1)}{2(2n-1)}} = N^{\frac{2n\delta+2(n-1)\beta-n+1}{2(2n-1)}}$.

Substituting the expression of d_1 in the key equation $e_1 d_1 = k_1(N_1 + 1 - p_1 - q_1) + 1$, we aim to solve the following modular polynomial in $(\hat{n}+2)$ variables,

$$x(y - N_1 - 1) + e_1 a_1 z_1 + \cdots + e_1 a_{\hat{n}} z_{\hat{n}} - 1 \pmod{e_1 a_{\hat{n}+1}}$$

with roots $(k_1, p_1 + q_1, c_1, \ldots, c_{\hat{n}})$ for $\hat{n} := 2n-2$. Letting $u := xy - 1$, the polynomial $f_{\hat{n}}(x, z_1, \ldots, z_{\hat{n}}, u)$ can be rewritten as

$$u - (N_1 + 1)x + e_1 a_1 z_1 + \cdots + e_1 a_{\hat{n}} z_{\hat{n}} \pmod{e_1 a_{\hat{n}+1}}.$$

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 $i, j, k, l_1, \ldots, l_{\hat{n}} \in \mathbb{N}$. We denote the set of shift polynomials by $\mathcal{G}$ that is the union of $\mathcal{G}_1$ and $\mathcal{G}_2$, where

$$\mathcal{G}_1 := \{g_{[i,0,k,l_1,\ldots,l_{\hat{n}}]} : k = 0,\ldots,s; i = 0,\ldots,s-k;\ldots; l_{\hat{n}} = 0,\ldots,s-k-i-l_1-\cdots-l_{\hat{n}-1}.\},$$
$$\mathcal{G}_2 := \{g_{[0,j,k,l_1-l_2,l_2-l_3,\ldots,l_{\hat{n}}-k]} : l_1 = 0,\ldots,s; j = 1,\ldots,\tau l_1; l_2 = 0,\ldots,l_1; l_3 = 0,\ldots,l_2;\ldots; k = 0,\ldots,l_{\hat{n}}.\}$$

for an optimizing parameter $0 \le \tau \le 1$ to be determined later. Thus, all the shift polynomials in $\mathcal{G}$ share the common roots $(k_1, p_1+q_1, c_1, \ldots, c_{\hat{n}}, k_1(p_1+q_1)-1)$ modulo E^s.

The constructions of the basis matrix B and lattice $\mathcal{L}$ are similar, so we skip them here. The upper bounds on unknown variables are calculated as $X \approx N^{\delta}$, $Y \approx N^{\frac{1}{2}}$, $Z_i \approx N^{\frac{2n\delta+2(n-1)\beta-n+1}{2(2n-1)}}$, $U \approx N^{\delta+\frac{1}{2}}$, $E \approx N^{1+\frac{(n-1)(2\delta-2\beta+1)}{2(2n-1)}}$. Similarly, we can calculate the determinant of $\mathcal{L}$ that is the product of the diagonal entries of the basis matrix B as $\det(\mathcal{L}) = X^{s_X} Y^{s_Y} Z_1^{s_{z_1}} \cdots Z_{\hat{n}}^{s_{z_{\hat{n}}}} U^{s_u} E^{s_E}$, where the exponents s_x, s_y, s_{z_i}, s_u and s_E are the contributions of the diagonal entries to the determinant.

We list s_x, s_y, s_{z_i}, s_u, s_E and the lattice dimension m without the lower terms after tedious computations. $s_x = \frac{1}{(\hat{n}+3)!}s^{\hat{n}+3}$, $s_y = \frac{(\hat{n}+1)(\hat{n}+2)\tau^2}{2(\hat{n}+3)!}s^{\hat{n}+3}$, $s_{z_i} = \frac{1+(\hat{n}+2)\tau}{(\hat{n}+3)!}s^{\hat{n}+3}$, $s_u = \frac{1+(\hat{n}+2)\tau}{(\hat{n}+3)!}s^{\hat{n}+3}$, $s_E = \frac{\hat{n}+2+(\hat{n}^2+3\hat{n}+1)\tau}{(\hat{n}+3)!}s^{\hat{n}+3}$, $m = \frac{1+(\hat{n}+1)\tau}{(\hat{n}+2)!}s^{\hat{n}+2}$.

Using condition (1) with $R = E^s$ for acquiring enough integer equations with the common roots, we have a simplified crucial condition $2\xi_x + (\hat{n}+1)(\hat{n}+2)\tau^2\xi_y + 2(1+(\hat{n}+2)\tau)(\hat{n}\xi_{z_i} + \xi_u - \xi_E) < 0$. We have $\xi_x = \delta$, $\xi_y = \frac{1}{2}$, $\xi_{z_i} = \frac{2n\delta+2(n-1)\beta-n+1}{2(2n-1)}$, $\xi_u = \delta+\frac{1}{2}$, $\xi_E = 1+\frac{(n-1)(2\delta-2\beta+1)}{2(2n-1)}$, which denote the corresponding exponents of the upper bounds.

Since $\hat{n} = 2n-2$, we further have $\xi_x + n(2n-1)\tau^2\xi_y + (1+2n\tau)((2n-2)\xi_{z_i} + \xi_u - \xi_E) < 0$. We substitute ξ_x, ξ_y, ξ_{z_i}, ξ_u and ξ_E in this inequality and obtain $\delta + \frac{n(2n-1)}{2}\tau^2 + (1+2n\tau)\left(n\delta + (n-1)\beta - \frac{n}{2}\right) < 0$, which can be reduced to

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

The right side reaches its maximum by taking $\tau = \frac{\sqrt{(2n-1)(6n^3+3n^2-1-8n^2(n-1)\beta)}-(n+1)(2n-1)}{2n^2(2n-1)}$. We put it back in the inequality and hence obtain the final condition

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

The solvable condition (8) with respect to various β's is illustrated in Fig. 2 and discuss more about it. We can achieve higher insecure bound as the unknown part i.e., β decreases. On the other hand, exposing more RSA instances with implicitly related keys is more vulnerable. Let n go to infinity, the asymptotic bound on δ converges to $\frac{1}{2}-\beta$. Consequently, it means that our attacks are still effective for $\delta < \frac{1}{2}$, which matches a conjecture in previous small private exponent attack [4] unless there exist other more effective attacks.

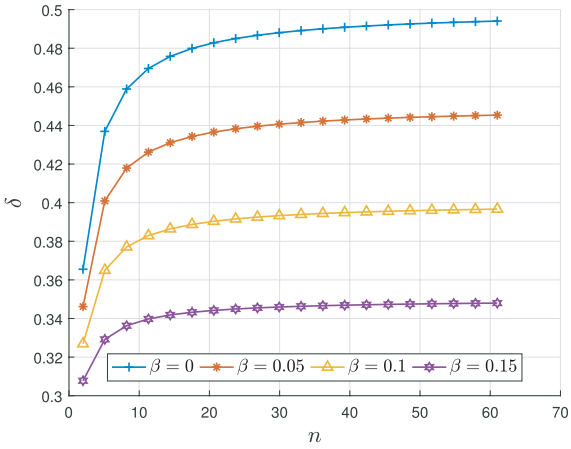


Fig. 2 The comparison of the insecure upper bounds on δ in condition (8) for given n RSA instances with respect to $\beta = 0$, $\beta = 0.05$, $\beta = 0.1$ and $\beta = 0.15$.

5. Experimental Results

In Sect. 3 and Sect. 4, we proposed lattice-based attacks using the splitting technique and the linearization technique. Now, we want to verify the validity of the proposed attacks. The computer experiments are carried out in `SageMath` [40] running on a virtual machine with Intel Xeon CPU E5-2620 v4 @ 2.10 GHz. Because practical attacks always have slight worse performance compared with theoretical asymptotic results, we aim to obtain the average performance for conducting successful attacks. To do so, we first randomly fix the bit-sizes of LSBs and MSBs, which imply γ and $(\delta-\beta-\gamma)$ respectively. Then we gradually increase the bit-size of the different middle block that relates to β in each attack setting. Finally, we randomly generate specified private keys and 1024-bit RSA moduli with corresponding public keys. We carry out the proposed attacks for fixed δ, β and γ with simulated public data several times to conclude the average experimental results. Conversely, an attacker can perform successful lattice-based attacks for given public data with δ_e, β and γ listed in Table 2 in practice.

We mainly implement the proposed attacks for given two RSA instances, which have been analyzed in Sect. 3. During the experiments, we can collect much more polynomial equations satisfying our requirements. In other words, after running the LLL algorithm, we obtain enough sufficiently short reduced vectors, which are later transformed into a system of integer equations. Hence, we can extract their common roots by the Gröbner basis computations and finally derive the factorization of given RSA moduli. We choose a suitable s with an optimal τ for concrete attack settings, which implies we shall first reduce a two-dimensional (or three-dimensional) lattice and then another m-dimensional one. The comparison of the asymptotic and experimental results are given in Table 2.

To be specific, the γ, β columns indicate the known information of the implicitly related keys. The δ_∞ column

Table 2 The asymptotic bounds and experimental results of the proposed attacks for given two RSA instances.

Attack Type	γ	β	δ_∞	LSBs	MSBs	KBs	δ_e	s	τ	m
First Attack	0.117	0.038	0.350	120	160	319	0.312	6	0.167	225
First Attack	0.078	0.092	0.330	80	128	303	0.296	5	0.200	136
First Attack	0.023	0.195	0.290	24	56	280	0.274	7	0.143	351
Second Attack	0.156	0.061	0.307	160	65	288	0.282	5	0.200	136
Second Attack	0.131	0.101	0.300	135	45	284	0.278	6	0.167	225
Second Attack	0.117	0.093	0.296	120	62	278	0.272	6	0.167	225
Third Attack	0.178	0.070	0.338	183	54	309	0.302	5	0.200	136
Third Attack	0.156	0.053	0.345	160	96	311	0.304	6	0.167	225
Third Attack	0.117	0.039	0.350	120	143	303	0.296	6	0.167	225

provides the asymptotic bounds when the lattice dimension goes to infinity. The LSBs and MSBs columns (recorded in bits) provide the numbers of shared bits in implicitly related keys for simulating three proposed distinct attacks. The KBs column (recorded in bits) provides the numbers of the private key bits when successfully conducting the proposed attacks. The δ_e column provides the experimental results for our lattice settings, which are denoted by the s, τ, m columns.

We briefly comment on the root extraction process that completes the proposed attacks. We are able to collect sufficient equations sharing the common roots over the integers after transforming the reduced vectors into polynomials. Then we put them into the Gröbner basis computations and obtain $p_2 + q_2$ that leads to the factorization of N_2. As mentioned in Sect. 3.1, we can obtain the factorization of N_1 as well. In another case, we first calculate the correct value of w if the Gröbner basis computations do not give explicit solutions. Thus, we can recover the values of other variables including $p_2 + q_2$ and finally factorize N_1 and N_2.

6. Conclusions

In this paper, we propose the formulation of a new factorization problem of RSA with respect to implicitly related keys, whose goal is to factorize RSA moduli with the help of implicit hints about related private keys. We propose several lattice-based attacks using Coppersmith's techniques that is applied for solving modular polynomials as a powerful tool. We adapt the splitting technique to split a variable of large norm into some variables of smaller norm. This technique is further used to represent one private key with known implicit relation about other private keys.

We analyze the implicit related-key factorization problem for given two RSA instances in detail. Three distinct attacks are presented and the theoretical results are illustrated and discussed. The validity of the proposed attacks are further verified by numerical computer experiments. We extend a heuristic lattice construction to the attack scenario for given more than two RSA instances. A heuristic attack is proposed and we illustrate the theoretical results according to various implicit hints of the related keys. In conclusion, more RSA instances with implicitly related keys generated by more shared bits make the RSA cryptosystem much more vulnerable.

Acknowledgments

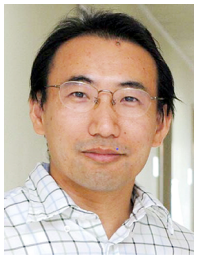
This research was partially supported by the National Natural Science Foundation of China (Grant Nos. 61972370 and 61632013), Anhui Initiative in Quantum Information Technologies under Grant AHY150400, JST CREST Grant Number JPMJCR14D6, Japan and JSPS KAKENHI Grant Number JP16H02780.

References

[1] Y. Aono, "Minkowski sum based lattice construction for multivariate simultaneous Coppersmith's technique and applications to RSA," ACISP 13, C. Boyd and L. Simpson, eds., LNCS, vol.7959, pp.88–103. Springer, Heidelberg July 2013.
[2] J. Blömer and A. May, "New partial key exposure attacks on RSA," CRYPTO 2003, D. Boneh, ed., LNCS, vol.2729, pp.27–43, Springer, Heidelberg Aug. 2003.
[3] D. Boneh, "Twenty years of attacks on the RSA cryptosystem," Notices of the AMS, vol.46, no.2, pp.203–213, Feb. 1999.
[4] D. Boneh and G. Durfee, "Cryptanalysis of RSA with private key d less than $N^{0.292}$, EUROCRYPT'99, J. Stern, ed., LNCS, vol.1592, pp.1–11, Springer, Heidelberg, May 1999.
[5] D. Boneh, G. Durfee, and Y. Frankel, "An attack on RSA given a small fraction of the private key bits," ASIACRYPT'98, K. Ohta and D. Pei, eds., LNCS, vol.1514, pp.25–34, Springer, Heidelberg, Oct. 1998.
[6] B. Buchberger and F. Winkler, Gröbner Bases and Applications, London Mathematical Society Lecture Note Series, vol.251, Cambridge University Press, Cambridge, United Kingdom, 1998.
[7] D. Coppersmith, "Finding a small root of a bivariate integer equation; Factoring with high bits known," EUROCRYPT'96, U.M. Maurer, ed., LNCS, vol.1070, pp.178–189. Springer, Heidelberg, May 1996.
[8] D. Coppersmith, "Finding a small root of a univariate modular equation," EUROCRYPT'96, U.M. Maurer, ed., LNCS, vol.1070, pp.155–165. Springer, Heidelberg, May 1996.
[9] D. Coppersmith, "Small solutions to polynomial equations, and low exponent RSA vulnerabilities," J. Cryptol., vol.10, no.4, pp.233–260, Sept. 1997.
[10] J.S. Coron, "Finding small roots of bivariate integer polynomial equations revisited," EUROCRYPT 2004, C. Cachin and J. Camenisch, eds., LNCS, vol.3027, pp.492–505, Springer, Heidelberg, May 2004.
[11] J.S. Coron, "Finding small roots of bivariate integer polynomial equations: A direct approach," CRYPTO 2007, A. Menezes, ed., LNCS, vol.4622, pp.379–394. Springer, Heidelberg, Aug. 2007.
[12] J.S. Coron and A. May, "Deterministic polynomial-time equivalence of computing the RSA secret key and factoring," J. Cryptol., vol.20, no.1, pp.39–50, Jan. 2007.
[13] M. Ernst, E. Jochemsz, A. May, and B. de Weger, "Partial key exposure attacks on RSA up to full size exponents," EUROCRYPT 2005, R. Cramer, ed., LNCS, vol.3494, pp.371–386, Springer, Heidelberg,

May 2005.
[14] J.C. Faugère, R. Marinier, and G. Renault, "Implicit factoring with shared most significant and middle bits," PKC 2010, P.Q. Nguyen and D. Pointcheval, eds., LNCS, vol.6056, pp.70–87, Springer, Heidelberg, May 2010.
[15] N. Gama and P.Q. Nguyen, "Predicting lattice reduction," EUROCRYPT 2008, N.P. Smart, ed., LNCS, vol.4965, pp.31–51, Springer, Heidelberg, April 2008.
[16] J.A. Halderman, S.D. Schoen, N. Heninger, W. Clarkson, W. Paul, J.A. Calandrino, A.J. Feldman, J. Appelbaum, and E.W. Felten, "Lest we remember: Cold-boot attacks on encryption keys," Commun. ACM, vol.52, no.5, pp.91–98, May 2009.
[17] M. Herrmann and A. May, "Maximizing small root bounds by linearization and applications to small secret exponent RSA," PKC 2010, P.Q. Nguyen and D. Pointcheval, eds., LNCS, vol.6056, pp.53–69, Springer, Heidelberg, May 2010.
[18] M.J. Hinek, On the Security of Some Variants of RSA, Ph.D. thesis, University of Waterloo, Waterloo, Ontario, Canada, 2007.
[19] J. Hoffstein, J.C. Pipher, and J.H. Silverman, An Introduction to Mathematical Cryptography, Springer, New York, NY, USA, 2008.
[20] N. Howgrave-Graham, "Finding small roots of univariate modular equations revisited," 6th IMA International Conference on Cryptography and Coding, M. Darnell, ed., LNCS, vol.1355, pp.131–142, Springer, Heidelberg, Dec. 1997.
[21] E. Jochemsz and A. May, "A polynomial time attack on RSA with private CRT-exponents smaller than $N^{0.073}$," CRYPTO 2007, A. Menezes, ed., LNCS, vol.4622, pp.395–411, Springer, Heidelberg, Aug. 2007.
[22] P.C. Kocher, "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems," CRYPTO'96, N. Koblitz, ed., LNCS, vol.1109, pp.104–113, Springer, Heidelberg, Aug. 1996.
[23] A.K. Lenstra, H.W. Lenstra, and L. Lovász, "Factoring polynomials with rational coefficients," Math. Ann., vol.261, no.4, pp.515–534, Dec. 1982.
[24] Y. Lu, L. Peng, R. Zhang, L. Hu, and D. Lin, "Towards optimal bounds for implicit factorization problem," SAC 2015, O. Dunkelman and L. Keliher, eds., LNCS, vol.9566, pp.462–476, Springer, Heidelberg, Aug. 2016.
[25] A. May, "Cryptanalysis of unbalanced RSA with small CRT-exponent," CRYPTO 2002, M. Yung, ed., LNCS, vol.2442, pp.242–256, Springer, Heidelberg, Aug. 2002.
[26] A. May, New RSA Vulnerabilities Using Lattice Reduction Methods, Ph.D. thesis, University of Paderborn, Paderborn, Germany, 2003.
[27] A. May, "Using LLL-reduction for solving RSA and factorization problems," ISC, pp.315–348, Springer, Heidelberg, 2010.
[28] A. May and M. Ritzenhofen, "Implicit factoring: On polynomial time factoring given only an implicit hint," PKC 2009, S. Jarecki and G. Tsudik, eds., LNCS, vol.5443, pp.1–14, Springer, Heidelberg, March 2009.
[29] L. Peng, L. Hu, Y. Lu, J. Xu, and Z. Huang, "Cryptanalysis of dual RSA," Des. Codes Cryptogr., vol.83, no.1, pp.1–21, April 2017.
[30] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, "Hey, you, get off of my cloud: Exploring information leakage in third-party compute clouds," ACM CCS 2009, E. Al-Shaer, S. Jha, and A.D. Keromytis, eds., pp.199–212, ACM Press, Nov. 2009.
[31] R.L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Commun. ACM, vol.21, no.2, pp.120–126, Feb. 1978.
[32] S. Sarkar and S. Maitra, "Cryptanalysis of RSA with more than one decryption exponent," Inform. Process. Lett., vol.110, no.8, pp.336–340, 2010.
[33] S. Sarkar and S. Maitra, "Cryptanalysis of RSA with two decryption exponents," Inform. Process. Lett., vol.110, no.5, pp.178–181, 2010.
[34] S. Sarkar and S. Maitra, "Approximate integer common divisor problem relates to implicit factorization," IEEE Trans. Inf. Theory, vol.57, no.6, pp.4002–4013, June 2011.
[35] H.M. Sun, M.E. Wu, W.C. Ting, and M.J. Hinek, "Dual RSA and its security analysis," IEEE Trans. Inf. Theory, vol.53, no.8, pp.2922–2933, Aug. 2007.
[36] A. Takayasu and N. Kunihiro, "Cryptanalysis of RSA with multiple small secret exponents," ACISP 14, W. Susilo and Y. Mu, eds., LNCS, vol.8544, pp.176–191, Springer, Heidelberg, July 2014.
[37] A. Takayasu and N. Kunihiro, "Partial key exposure attacks on RSA: Achieving the Boneh-Durfee bound," SAC 2014, A. Joux and A.M. Youssef, eds., LNCS, vol.8781, pp.345–362, Springer, Heidelberg, Aug. 2014.
[38] A. Takayasu and N. Kunihiro, "A tool kit for partial key exposure attacks on RSA," CT-RSA 2017, H. Handschuh, ed., LNCS, vol.10159, pp.58–73, Springer, Heidelberg, Feb. 2017.
[39] A. Takayasu, Y. Lu, and L. Peng, "Small CRT-exponent RSA revisited," EUROCRYPT 2017, Part II, J. Corond and J.B. Nielsen, eds., LNCS, vol.10211, pp.130–159, Springer, Heidelberg, April/May 2017.
[40] The Sage Developers: SageMath, the Sage Mathematics Software System (Version 7.3), 2019, https://www.sagemath.org
[41] M. Zheng and H. Hu, "Implicit related-key factorization problem on the RSA cryptosystem," CANS 2019, Y. Mu, R. Deng, and X. Huang, eds., LNCS, vol.11829, pp.525–537, Springer, Cham, Oct. 2019.

Mengce Zheng received the B.E. degree in information security in 2013, and the Ph.D. degree in information and communication engineering in 2018 from the University of Science and Technology of China, Hefei, China. He is now a postdoctoral researcher with the Key Laboratory of Electromagnetic Space Information, CAS, University of Science and Technology of China, Hefei, China. His research interests include cryptography and information security.



Noboru Kunihiro received his B.E., M.E. and Ph.D. in mathematical engineering and information physics from the University of Tokyo in 1994, 1996 and 2001, respectively. He has been a professor of University of Tsukuba since 2019. He was a researcher of NTT Communication Science Laboratories from 1996 to 2002. He was an associate professor of the University of Electro-Communications from 2002 to 2008. He was an associate professor of the University of Tokyo from 2008 to 2019. His research interest includes cryptography, information security and quantum computations. He was awarded the SCIS'97 paper prize and the Best Paper Award from IEICE.

Honggang Hu received the B.S. degree in mathematics in 2000, and the B.E. degree in electrical engineering in 2001 from the University of Science and Technology of China, Hefei, China, and the Ph.D. degree in electrical engineering from the Graduate School of Chinese Academy of Sciences, Beijing, China, in 2005. He was a postdoctoral fellow and a research associate at the University of Waterloo, Canada from 2007 to 2009 and 2009 to 2011, respectively. He has been a professor with the School of Information Science and Technology, University of Science and Technology of China since 2011. His research interests include cryptography and coding theory.