Journal of Cryptographic Engineering (2025) 15:19
https://doi.org/10.1007/s13389-025-00383-7

RESEARCH ARTICLE

New lattice-based partial key exposure attacks on common prime RSA

Mengce Zheng[1]

Received: 10 March 2025 / Accepted: 11 September 2025

Abstract
In this paper, we focus on the common prime RSA variant and introduce a novel investigation into the partial key exposure attack targeting it for the first time. We explore the vulnerability of this RSA variant, which employs two primes p and q defined as $p = 2ga + 1$ and $q = 2gb + 1$ for a large common prime g. Previous cryptanalysis of common prime RSA has primarily concentrated on the small private key attack. In contrast, we delve deeper into the partial key exposure attacks by categorizing them into three distinct cases. We are able to identify weak private keys that are susceptible to partial key exposure by using the lattice-based method for solving simultaneous modular univariate linear equations. Moreover, we conduct numerical experimental evaluations and demonstrate the validity of the proposed partial key exposure attacks on common prime RSA.

Keywords Common prime RSA · Partial key exposure attack · Weak key · Lattice

Mathematics Subject Classification 94A60

1 Introduction

The RSA cryptosystem, invented by Rivest, Shamir, and Adleman [25], is a well-known public key algorithm. Over the years, various generalizations of RSA scheme have been proposed in the literature. These generalizations include modifications to the modulus [5, 28], its Euler quotient [16], and encryption or decryption processes [10, 23] for adaptation to different requirements and constraints. To address the high processing demands or security assurance of RSA, several variants have been introduced, such as CRT-RSA [23], multi-prime RSA [5], prime-power RSA [28], and common prime RSA [12]. We investigate partial key exposure attacks on common prime RSA using lattice-based solving strategy in this paper. The lattice-based method serves as an effective tool for assessing potential vulnerabilities in cryptanalysis of RSA and its variants.

Let us consider an instance of RSA with a public key (N, e) and a private key (p, q, d), where the modulus $N = pq$ is the product of two balanced primes. In the original RSA scheme [25], the public and private exponents e and d are chosen to be inverses of each other modulo $\varphi(N) = (p-1)(q-1)$. However, it is common to define these exponents modulo Carmichael's lambda function [8], denoted as $\lambda(N) = \text{lcm}(p-1, q-1)$, which is the least common multiple of $(p-1)$ and $(q-1)$. In the case of common prime RSA, a more secure variant first mentioned by Wiener [32] and later refined by Hinek [12], the balanced primes p and q exhibit a special structure that provides resistance against small private key attacks.

1.1 Common prime RSA

Let us delve into the mathematical background of common prime RSA as proposed by Hinek [12]. In Hinek's design, the balanced primes p and q are defined as $p = 2ga + 1$ and $q = 2gb + 1$, where g is a large common prime and a, b are positive integers. Two additional constraints are imposed: $\gcd(a, b) = 1$ and $h = 2gab + a + b$ is a prime integer. The first constraint ensures that $\gcd(p-1, q-1)$ is computed as $2g$, while the second constraint ensures that $(pq-1)/2 = gh$ is a semiprime of approximately the same bit-length as the

A preliminary version [34] appeared in Proceedings of the 19th International Conference on Information Security and Cryptology (Inscrypt 2023), LNCS 14527, pp. 407–410.

✉ Mengce Zheng
mengce.zheng@gmail.com

[1] College of Information and Intelligence Engineering, Zhejiang Wanli University, Ningbo, China

Published online: 29 September 2025

modulus N. We provide a modified version of the primes generation algorithm from [12, Appendix A] in Algorithm 1.

Algorithm 1: Primes Generation

Input: Modulus bit-length n and predetermined parameter γ
Output: Balanced primes p and q

$g \leftarrow$ a random $[\gamma n]$-bit prime;
while p, q, h *are not primes* **do**
  while $\gcd(a, b) \neq 1$ **do**
    $a, b \leftarrow$ two random $[(1/2 - \gamma)n - 1]$-bit positive integers;
  end while
  $p \leftarrow 2ga + 1$;
  $q \leftarrow 2gb + 1$;
  $h \leftarrow 2gab + a + b$;
end while
return p and q

In the common prime RSA scheme, the public and private exponents e, d are defined modulo

$$\begin{aligned}\lambda(N) &= \lambda(pq) = \mathrm{lcm}(p-1, q-1)\\ &= \mathrm{lcm}(2ga, 2gb) = 2gab.\end{aligned}$$

According to Hinek's design, we have the equation

$$\begin{aligned}N &= pq = (2ga+1)(2gb+1)\\ &= 2g(2gab + a + b) + 1 = 2gh + 1.\end{aligned} \tag{1}$$

The key equation $ed \equiv 1 \pmod{\mathrm{lcm}(p-1, q-1)}$ can be rewritten as

$$ed \equiv 1 \pmod{2gab}, \tag{2}$$

which further leads to

$$ed = 2gabk + 1,$$

where k is an unknown positive integer relatively prime to $2g$. In this paper, we use γ and δ to represent the greatest common divisor $g \simeq N^{\gamma}$ and the private exponent $d \simeq N^{\delta}$, respectively. Here, the symbol $\simeq$ is used to denote parameters with respect to certain powers of N. Since $2g = \gcd(p-1, q-1)$ for balanced p and q, we have $0 < \gamma < 1/2$. Additionally, the bit-length of e is assumed to be roughly the same as N/g, which implies $e \simeq N^{1-\gamma}$.

The broader theoretical recommendation for common prime RSA, aiming to balance security and efficiency, suggests $1/4 \leq \gamma < 1/2$ while the established practices for deployment suggests moderate $0.15 < \gamma < 0.35$. Instances with $\gamma > 0.35$ may appear largely limited to academic proofs of concept rather than real-world application.

The security of common prime RSA has been intensively studied by several works [12, 14, 18, 22, 27, 35]. However, it is worth noting that partial key exposure attacks, which involve the leakage of certain bits of the private key, are particularly relevant in scenarios where common prime RSA is used in constrained environments like the Internet of Things [22]. These attacks exploit side channel information that may be obtained through various means, including cold boot attack [11] and other side channel analysis techniques [15, 24, 26]. Thus, investigating partial key exposure attacks on common prime RSA is of great importance.

Partial key exposure attacks on RSA, where a fraction of the private key bits are known, were first proposed by Boneh et al. [4]. These attacks exploit the knowledge of the most significant bits (MSBs) or least significant bits (LSBs) of the private exponent d. In practice, these partial key bits can be obtained through side channel attacks as mentioned above. Subsequently, Blömer and May [2] improved upon these attacks and demonstrated that RSA is vulnerable to larger public exponent e when some private key bits are exposed. Ernst et al. [9] presented several new attacks that work with full-size exponents, i.e., $e \simeq N$ or $d \simeq N$, based on three theorems under a common heuristic assumption. The most powerful attack to date, proposed by Takayasu and Kunihiro [30], achieves Boneh-Durfee's bound [3] for small private key attacks.

Furthermore, partial key exposure attacks have also been applied to other RSA variants [21, 33, 37, 38]. However, no research has been conducted on partial key exposure attacks specifically targeting the common prime RSA scheme.

1.2 Our contribution

In this paper, we present the first investigation of partial key exposure attacks on common prime RSA. We begin by exploring the relationship between the values e, d, and $\lambda(N)$, where $ed \equiv 1 \pmod{\lambda(N)}$ can be rewritten as $ed \equiv 1 \pmod{2gab}$, with $\lambda(N) = 2gab$. To address the scenario of small private key attack on common prime RSA, it is aimed to solve the equation

$$ex - 1 \equiv 0 \pmod{g}, \tag{3}$$

where $x = d$ is the small root.

To extend the above analysis to partial key exposure attacks, we first define and formalize specific attack scenarios. These scenarios include situations where the most significant bits (MSBs) of the private key, the least significant bits (LSBs) of the private key, or both the MSBs and LSBs are leaked. We categorize these scenarios into three cases: MSB case, LSB case, and Mix case.

In each of the three cases, the private key d takes on different forms based on the known information. By substituting

such d into the equation $ex - 1 \equiv 0 \pmod{g}$ and multiplying by a modular inverse, we obtain a new modular univariate linear equation that applies to our attack scenarios. To solve these modular equations, we utilize the lattice-based method introduced by Coppersmith [7].

Additionally, we employ an additional modular univariate linear equation to further improve our analysis results. This equation is derived from $(p-1)(q-1) = 2ga \cdot 2gb = 4g^2ab$, which implies $pq - p - q + 1 \equiv 0 \pmod{g^2}$. Consequently, we aim to solve the equation

$$x + N + 1 \equiv 0 \pmod{g^2}, \tag{4}$$

where $x = -(p+q)$ is the small root.

Thus, we need to deal with the simultaneous solution of two modular univariate linear equations. In designing our attacks, we aim to (1) exploit as many congruences modulo powers of g as possible, (2) choose the unknown so that it is directly related to the prime factors or the private key, and (3) use the highest feasible power of g to gain better performance. While one might use simpler relations such as

$$p - 1 \equiv 0 \pmod{g} \quad \text{or} \quad q - 1 \equiv 0 \pmod{g},$$

these involve only g^1. By contrast, using $x + N + 1 \equiv 0 \pmod{g^2}$ with $x = p + q$ has the advantage that we use a congruence modulo g^2 and maximize the power of g in a single linear equation. This choice yields a better theoretical and practical performance.

The first demonstration of partial key exposure attacks on common prime RSA is stated as follows. Let $N = pq$, whose bit-length is denoted $\log_2 N$, be a common prime RSA modulus with two balanced primes p and q of the same bit-length. Let $e \simeq N^{1-\gamma}$ and $d \simeq N^{\delta}$ be its public and private exponents such that $ed \equiv 1 \pmod{\operatorname{lcm}(p-1, q-1)}$, where $\gcd(p-1, q-1) = 2g$ for a large prime $g \simeq N^{\gamma}$. Given an approximation of d with known MSBs d_{M} in a $(\delta_{\mathrm{M}} \log_2 N)$-bit block along with LSBs d_{L} in a $(\delta_{\mathrm{L}} \log_2 N)$-bit block satisfying $d = d_{\mathrm{M}}M + \bar{d}L + d_{\mathrm{L}}$, where $M = 2^{(\delta - \delta_{\mathrm{M}}) \log_2 N}$, $L = 2^{\delta_{\mathrm{L}} \log_2 N}$ for known $\delta_{\mathrm{M}}, \delta_{\mathrm{L}}$ and unknown $\bar{d}$ is bounded by $|\bar{d}| \leq N^{\delta - \delta_{\mathrm{M}} - \delta_{\mathrm{L}}}$. Then N can be efficiently factored in time polynomial in $\log_2 N$ if

$$\delta_{\mathrm{M}} + \delta_{\mathrm{L}} < \delta < 4\gamma^3 + \delta_{\mathrm{M}} + \delta_{\mathrm{L}}, \quad \frac{1}{4} \leq \gamma < \frac{1}{2}.$$

To provide a better understanding of our main result regarding the partial key exposure attack on common prime RSA, it is illustrated in Fig. 1.

While the preliminary version [34] introduced a basic attack scenario on common prime RSA, this full version extends the analysis to MSB, LSB and mixed MSB+LSB cases. Moreover, we develop a framework for solving simultaneous modular univariate linear equations via lattice reduction, and presents expanded experimental validation (including larger key sizes and boundary-region tests) to fully characterize both theoretical and practical performance.

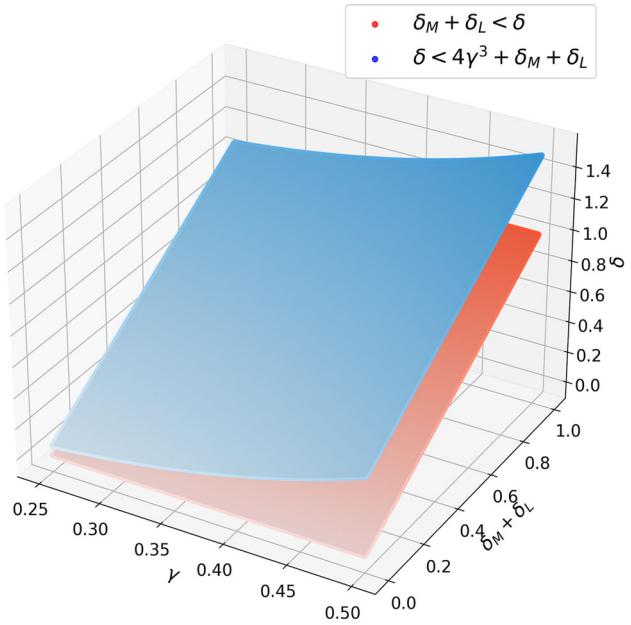

Fig. 1 The illustration of partial key exposure attack on common prime RSA considering both MSBs and LSBs exposure. The vulnerable δ is located between the red surface $\delta_{\mathrm{M}} + \delta_{\mathrm{L}}$ and the blue surface $4\gamma^3 + \delta_{\mathrm{M}} + \delta_{\mathrm{L}}$ for $1/4 \leq \gamma < 1/2$

1.3 Organization

The rest of this paper is structured as follows. In Sect. 2, we present a review of important mathematical lemmas and facts related to the lattice-based method. Section 3 provides a detailed explanation of our proposed partial key exposure attacks on common prime RSA. In Sect. 4, we present the results of numerical experiments conducted to validate the effectiveness of the proposed attacks. Finally, Sect. 5 concludes the paper.

2 Preliminaries

We introduce the application of Coppersmith's technique [6, 7], which is based on the LLL lattice reduction algorithm [17]. This technique proves to be instrumental in cryptanalysis, as it allows one to identify small roots of modular polynomial equations under a critical condition using the lattice-based solving strategy.

Consider given an irreducible multivariate polynomial $f(x_1, \ldots, x_n)$ having an integer root $(x'_1, \ldots, x'_n)$ modulo a known/unknown integer with upper bounds $X_1, \ldots, X_n$

on the root. The problem is to recover the desired root $(x'_1, \ldots, x'_n)$ satisfying the above modular equation through a polynomial-time algorithm. One may refer to [19, 20, 36] using the lattice-based method for more details.

We then describe the LLL lattice reduction algorithm [17]. A lattice $\mathscr{L}$ is the set of integer linear combinations of linearly independent basis vectors $\vec{b}_1, \ldots, \vec{b}_w \in \mathbb{R}^n$, denoted as

$$\mathscr{L}(\vec{b}_1, \ldots, \vec{b}_w) = \left\{ \sum_{i=1}^{w} z_i \vec{b}_i : z_i \in \mathbb{Z} \right\}.$$

The lattice is generated by the lattice basis matrix B, where each $\vec{b}_i$ is regarded as a row/column vector. Its determinant is $\det(\mathscr{L}) = |\det(B)|$ for a full-rank lattice with $w = n$, which is calculated as the product of the diagonal entries if B is a triangular matrix.

The LLL algorithm is commonly used to output approximately shortest basis vectors in a given lattice. We present the following lemma.

Lemma 1 *Let given basis vectors $(\vec{b}_1, \ldots, \vec{b}_w)$ span a lattice $\mathscr{L}$. The LLL algorithm outputs a reduced basis $(\vec{v}_1, \ldots, \vec{v}_w)$ satisfying*

$$\|\vec{v}_1\|, \ \|\vec{v}_2\|, \ \ldots, \ \|\vec{v}_i\| \leq 2^{\frac{w(w-1)}{4(w+1-i)}} \det(\mathscr{L})^{\frac{1}{w+1-i}}$$

for $1 \leq i \leq w$. The running time is a polynomial regarding w and the maximal bit-length of $\vec{b}_i$.

Howgrave-Graham [13] refined the original lattice construction in [7] and proposed a subtle lemma. Consider given a multivariate polynomial $h(x_1, \ldots, x_n) = \sum a_{i_1,\ldots,i_n} x_1^{i_1} \cdots x_n^{i_n}$. The norm is defined as $\|h(x_1, \ldots, x_n)\| = \sqrt{\sum |a_{i_1,\ldots,i_n}|^2}$.

Lemma 2 *Let $h(x_1, \ldots, x_n)$ be an integer polynomial having at most w monomials, and let $R, X_1, \ldots, X_n$ be some positive integers. If $\|h(x_1X_1, \ldots, x_nX_n)\| < R/\sqrt{w}$ and $h(x'_1, \ldots, x'_n) \equiv 0 \pmod{R}$ hold for $|x'_1| \leq X_1, \ldots, |x'_n| \leq X_n$, then $h(x'_1, \ldots, x'_n) = 0$ holds over the integers.*

By connecting Lemma 2 with Lemma 1, a given modular equation can be solved through solving several relevant integer equations. The fundamental concept of the lattice-based method involves the collection of shift polynomials modulo R, all sharing a common root, and subsequently reducing them to a set of integer equations. The basis matrix, derived from the coefficient vectors of these shift polynomials, forms a lattice of dimension w. By employing the LLL algorithm, it becomes possible to extract short reduced lattice vectors, which can subsequently be converted into polynomial equations. The equations hold over the integers if the norms of these polynomials are sufficiently small.

If we obtain the first ℓ reduced vectors using the LLL algorithm, it is required the following condition

$$2^{\frac{w(w-1)}{4(w+1-\ell)}} \det(\mathscr{L})^{\frac{1}{w+1-\ell}} < \frac{R}{\sqrt{w}}$$

holds to extract the solution. This condition can be reduced to

$$\det(\mathscr{L}) < R^{w-\epsilon},$$

where ϵ denotes a negligible real compared to R. It is further simplified to $\det(\mathscr{L}) < R^w$ by disregarding the lower order terms. Eventually, the common root of the derived integer equations can be extracted by employing the resultant computation or Gröbner basis computation [1].

In summary, the lattice-based method for solving a given multivariate modular equation consists of four steps. First, we generate a collection of shift polynomials using the given polynomial $f(x_1, \ldots, x_n)$ and given modulus. These shift polynomials are designed to have a common root modulo R with the form $(x'_1, \ldots, x'_n)$. Next, we generate a lattice by deriving row vectors $\vec{b}_i$ from the coefficient vector of each shift polynomial $g_i(x_1X_1, \ldots, x_nX_n)$. This lattice, denoted as $\mathscr{L}$, is defined as the set of all possible integer linear combinations of these vectors. To simplify the lattice, we apply the LLL algorithm to obtain the first n reduced basis vectors $\vec{v}_1, \ldots, \vec{v}_n$. These vectors are then transformed into polynomials $h_1(x_1, \ldots, x_n), \ldots, h_n(x_1, \ldots, x_n)$ that share the common root $(x'_1, \ldots, x'_n)$ over the integers. Finally, if the derived integer polynomials $h_i(x_1, \ldots, x_n)$ are algebraically independent, we can solve the equation system $h_i(x_1, \ldots, x_n) = 0$ using Gröbner basis computation. This allows us to extract the desired root $(x'_1, \ldots, x'_n)$.

It is important to note that the process of solving multivariate equations using the lattice-based method is heuristic because there is no guarantee that the derived polynomials will be algebraically independent. However, in the literature of lattice-based attacks, it is commonly assumed that the polynomials obtained from the LLL algorithm are algebraically independent. While there is limited research contradicting this assumption, it is generally accepted. Therefore, we make the following assumption.

Assumption 1 The obtained integer polynomials are algebraically independent, allowing for the efficient recovery of their common root using Gröbner basis computation.

In addition to the lattice construction originally introduced in [7, 13], there are other improved and simplified constructions available, such as those presented in [14, 18, 29]. In this paper, we choose to utilize the lattice construction proposed in [18] for our attack scenarios. This particular construction allows for the easier generation of a triangular lattice matrix,

while also yielding superior analysis results. The method is specifically designed to solve the problem of finding small roots of simultaneous modular univariate linear equations,

$$\begin{cases} f_1(x_1) := x_1 + a_1 \equiv 0 \pmod{u^{r_1}} \\ \vdots \\ f_n(x_n) := x_n + a_n \equiv 0 \pmod{u^{r_n}} \end{cases}$$

The known parameters are some positive integers $a_1, \ldots, a_n$, $r_1, \ldots, r_n, r, U$, and bounding reals $\eta, \gamma_1, \ldots, \gamma_n \in (0, 1)$, where $U \equiv 0 \pmod{u^r}$ for unknown $u \simeq U^\eta$. The goal is to extract all roots $(x_1', \ldots, x_n')$ such that $|x_1'| \leq U^{\gamma_1}, \ldots, |x_n'| \leq U^{\gamma_n}$.

We briefly mention the relevant shift polynomials step, as it plays a crucial role in the lattice-based method. In this step, we define a suitable polynomial collection $\mathcal{G}$ for a predetermined positive integer t:

$$\mathcal{G} = \left\{ g_{[i_1,\ldots,i_n]}(x_1, \ldots, x_n) : 0 \leq \sum_{j=1}^{n} \gamma_j i_j \leq \eta t \right\},$$

where each shift polynomial $g_{[i_1,\ldots,i_n]}(x_1, \ldots, x_n)$ for $i_1, \ldots, i_n \in \mathbb{N}$ is

$$g_{[i_1,\ldots,i_n]}(x_1, \ldots, x_n) := (x_1 + a_1)^{i_1} \cdots (x_n + a_n)^{i_n} \cdot U^{\max\left\{ \left\lceil \frac{t - \sum_{j=1}^{n} r_j i_j}{r} \right\rceil, 0 \right\}}. \tag{5}$$

The modulus R involved in this lattice-based construction is u^t. With the parameters mentioned above, we present the following lemma. For a detailed explanation and calculation, one may refer to [18, Theorem 10] and its accompanying proof.

Lemma 3 *The root of the above simultaneous modular univariate linear equations can be recovered if*

$$\sqrt[n]{\frac{\gamma_1 \cdots \gamma_n}{r r_1 \cdots r_n}} < \eta^{\frac{n+1}{n}}$$

provided that $\eta \gg 1/\sqrt{\log U}$ *and* $\gamma_i \leq r_i \eta$ *for* $1 \leq i \leq n$. *The running time is polynomial in* $\log U$ *but exponential in* n.

3 Partial key exposure attack

We analyze and propose partial key exposure attacks on common prime RSA in this section. We consider three distinct situations for the given leakage of the private key, which we refer to as the MSB case, LSB case, and Mix case. Let N be the product of two balanced primes p and q, both having the same bit-length. Let $e \simeq N^{1-\eta}$ and $d \simeq N^\delta$ satisfy $ed \equiv 1 \pmod{\lambda(N)}$, where $\lambda(N) = \mathrm{lcm}(p-1, q-1) = 2gab$ is described in Sect. 1.

MSB Case. Given N, e and MSBs d_{M} in a $(\delta_{\mathrm{M}} \log_2 N)$-bit block of d satisfying $d = d_{\mathrm{M}} M + \bar{d}$, where $M = 2^{(\delta - \delta_{\mathrm{M}}) \log_2 N}$ for known δ_{M}, and unknown $\bar{d}$ is bounded by $|\bar{d}| \simeq N^{\delta - \delta_{\mathrm{M}}}$, the target is to efficiently factor N in polynomial.

LSB Case. Given N, e and LSBs d_{L} in a $(\delta_{\mathrm{L}} \log_2 N)$-bit block of d satisfying $d = \bar{d} L + d_{\mathrm{L}}$, where $L = 2^{\delta_{\mathrm{L}} \log_2 N}$ for known δ_{L}, and unknown $\bar{d}$ is bounded by $|\bar{d}| \simeq N^{\delta - \delta_{\mathrm{L}}}$, the target is to efficiently factor N in polynomial.

Mix Case. Given N, e and MSBs d_{M} in a $(\delta_{\mathrm{M}} \log_2 N)$-bit block, LSBs d_{L} in a $(\delta_{\mathrm{L}} \log_2 N)$-bit block of d satisfying $d = d_{\mathrm{M}} M + \bar{d} L + d_{\mathrm{L}}$, where $M = 2^{(\delta - \delta_{\mathrm{M}}) \log_2 N}$, $L = 2^{\delta_{\mathrm{L}} \log_2 N}$ for known $\delta_{\mathrm{M}}, \delta_{\mathrm{L}}$, and unknown $\bar{d}$ is bounded by $|\bar{d}| \simeq N^{\delta - \delta_{\mathrm{M}} - \delta_{\mathrm{L}}}$, the target is to efficiently factor N in polynomial.

3.1 MSB Case

We present the partial key exposure attack on common prime RSA under the MSB case with the following proposition.

Proposition 1 *Let* $N = pq$ *be a common prime RSA modulus with two balanced primes* p *and* q *of the same bit-length. Let* $e \simeq N^{1-\gamma}$ *and* $d \simeq N^\delta$ *be its public and private exponents such that* $ed \equiv 1 \pmod{\mathrm{lcm}(p-1, q-1)}$, *where* $\gcd(p-1, q-1) = 2g$ *for a large prime* $g \simeq N^\gamma$. *Given an approximation of* d *with known MSBs* d_{M} *in a* $(\delta_{\mathrm{M}} \log_2 N)$*-bit block satisfying* $d = d_{\mathrm{M}} M + \bar{d}$, *where* $M = 2^{(\delta - \delta_{\mathrm{M}}) \log_2 N}$ *for known* δ_{M} *and unknown* $\bar{d}$ *is bounded by* $|\bar{d}| \leq N^{\delta - \delta_{\mathrm{M}}}$. *Then* N *can be efficiently factored in time polynomial in* $\log_2 N$ *if*

$$\delta_{\mathrm{M}} < \delta < 4\gamma^3 + \delta_{\mathrm{M}}, \quad \frac{1}{4} \leq \gamma < \frac{1}{2}.$$

Proof According to the property of common prime RSA, we have $N - 1 = 2gh$ for two primes g, h from relation (1), which implies $N - 1 \equiv 0 \pmod{g}$ and further

$$\frac{N-1}{2} \equiv 0 \pmod{g}.$$

Besides, we have $ed - 1 \equiv 0 \pmod{g}$ from equation (2). Since $d = d_{\mathrm{M}} M + \bar{d}$ for $M = 2^{(\delta - \delta_{\mathrm{M}}) \log_2 N}$ with known δ_{M} and unknown $\bar{d}$, we substitute d into $ed - 1 \equiv 0 \pmod{g}$ and obtain

$$e d_{\mathrm{M}} M + e\bar{d} - 1 \equiv 0 \pmod{g}.$$

Because $(N-1)/2 = gh$ is a product of two primes, the inverse of e modulo $(N-1)/2$ must exist, which is denoted

by $e^{-1} \bmod (N-1)/2$. Multiplying the above equation by $e^{-1} \bmod (N-1)/2$, we have a modular univariate linear equation,

$$x_1 + a_1 \equiv 0 \pmod{g}, \tag{6}$$

where x_1 represents the unknown $\bar{d}$ and

$$a_1 = (ed_{\mathrm{M}}M - 1)\left(e^{-1} \bmod \frac{N-1}{2}\right) \bmod (N-1).$$

Moreover, since $(p-1)(q-1) = 2ga \cdot 2gb = 4g^2ab$ and $(p-1)(q-1) = pq - p - q + 1 = N + 1 - (p+q)$, we have another modular univariate linear equation,

$$x_2 + a_2 \equiv 0 \pmod{g^2}, \tag{7}$$

where x_2 represents the unknown $-(p+q)$ and $a_2 = N+1$. Thus, combining two simultaneous modular univariate linear equations (6) and (7), we have the following equation system,

$$\begin{cases} x_1 + a_1 \equiv 0 \pmod{g} \\ x_2 + a_2 \equiv 0 \pmod{g^2} \end{cases} \tag{8}$$

We focus on the above equation system with roots $x_1' = \bar{d}$ and $x_2' = -(p+q)$. Once we discover an integer pair (x_1', x_2') satisfying (8), we can factor the RSA modulus N via $p+q$. From (8) and $U \equiv 0 \pmod{g}$ with $g \simeq N^{\gamma}$, we have $n = 2$, $r_1 = 1, r_2 = 2, r = 1, u = g, U = N-1$, and $\gamma_1 = \delta - \delta_{\mathrm{M}}$, $\gamma_2 = 1/2, \eta = \gamma$. Therefore, all the shift polynomials in our attack scenario are specified as

$$g_{[i_1,i_2]}(x_1, x_2) = (x_1 + a_1)^{i_1} (x_2 + a_2)^{i_2} U^{\max\{t - i_1 - 2i_2, 0\}}, \quad 0 \le \gamma_1 i_1 + \gamma_2 i_2 \le \gamma t$$

for a positive integer t induced from (5) (here we use U instead of $N-1$ for simplicity).

These shift polynomials share a common root $(\bar{d}, -(p+q))$ modulo g^t for a predetermined integer t. By a straightforward polynomial arrangement, we can construct a triangular basis matrix with diagonal entries

$$X_1^{i_1} X_2^{i_2} U^{\max\{t - i_1 - 2i_2, 0\}}$$

for each polynomial in $\mathcal{G} = \{g_{[i_1,i_2]}(x_1, x_2) : 0 \le \gamma_1 i_1 + \gamma_2 i_2 \le \gamma t\}$. A lattice matrix example is shown in Table 1, where other non-zero off-diagonal entries are denoted by '–'.

Following the solving strategy for simultaneous modular univariate linear equations, we compute the lattice dimension,

$$w = \sum_{0 \le \gamma_1 i_1 + \gamma_2 i_2 \le \gamma t} 1 = \frac{\gamma^2 t^2}{2\gamma_1\gamma_2} + o\left(t^2\right).$$

The lattice determinant is $\det(\mathscr{L}) = X_1^{s_1} X_2^{s_2} U^{s_U}$, where

$$s_1 = \sum_{0 \le \gamma_1 i_1 + \gamma_2 i_2 \le \gamma t} i_1 = \frac{\gamma^3 t^3}{6\gamma_1^2\gamma_2} + o\left(t^3\right),$$

$$s_2 = \sum_{0 \le \gamma_1 i_1 + \gamma_2 i_2 \le \gamma t} i_2 = \frac{\gamma^3 t^3}{6\gamma_1\gamma_2^2} + o\left(t^3\right),$$

$$s_U = \sum_{0 \le i_1 + 2i_2 \le t} (t - i_1 - 2i_2) = \frac{t^3}{12} + o\left(t^3\right).$$

Ignoring low order terms of t, the crucial condition $\det(\mathscr{L}) < R^w$ with $R = g^t \simeq U^{\gamma t}$ leads to

$$X_1^{\frac{\gamma^3 t^3}{6\gamma_1^2\gamma_2}} X_2^{\frac{\gamma^3 t^3}{6\gamma_1\gamma_2^2}} U^{\frac{t^3}{12}} < U^{\gamma t \cdot \frac{\gamma^2 t^2}{2\gamma_1\gamma_2}}.$$

The unknown variables x_1, x_2 are bounded by $X_1 = U^{\gamma_1}, X_2 = U^{\gamma_2}$, respectively. Therefore, we deal with the exponents over U and obtain

$$\frac{\gamma^3 t^3}{6\gamma_1^2\gamma_2} \cdot \gamma_1 + \frac{\gamma^3 t^3}{6\gamma_1\gamma_2^2} \cdot \gamma_2 + \frac{t^3}{12} < \frac{\gamma^3 t^3}{2\gamma_1\gamma_2},$$

which reduces to $\gamma_1\gamma_2 < 2\gamma^3$.

Because $X_1 = N^{\delta - \delta_{\mathrm{M}}} \simeq U^{\delta - \delta_{\mathrm{M}}}$ and $X_2 = N^{1/2} \simeq U^{1/2}$, we have $\gamma_1 = \delta - \delta_{\mathrm{M}}$, $\gamma_2 = 1/2$ and hence

$$(\delta - \delta_{\mathrm{M}}) \cdot \frac{1}{2} < 2\gamma^3,$$

which leads to

$$\delta < 4\gamma^3 + \delta_{\mathrm{M}}.$$

Actually, we may directly apply Lemma 3 with $n = 2$, $r_1 = 1, r_2 = 2, r = 1, U = N - 1 \simeq N, \eta = \gamma$. Thus, we have

$$\sqrt[n]{\frac{\gamma_1 \cdots \gamma_n}{r r_1 \cdots r_n}} < \eta^{\frac{n+1}{n}} \quad \Rightarrow \quad \gamma_1 \cdots \gamma_n < r r_1 \cdots r_n \eta^{n+1} \quad \Rightarrow \quad \gamma_1\gamma_2 < 2\gamma^3.$$

Substituting $\gamma_1 = \delta - \delta_{\mathrm{M}}$ and $\gamma_2 = 1/2$, we then have

$$\delta < 4\gamma^3 + \delta_{\mathrm{M}}.$$

Moreover, we must ensure that $0 < \delta - \delta_{\mathrm{M}} \le \gamma$ and $1/2 \le 2\gamma$, which imply that $\gamma \ge 1/4$ and $\delta_{\mathrm{M}} < \delta < \gamma + \delta_{\mathrm{M}}$. Gathering them together with $0 < \gamma < 1/2$, we derive the final condition,

$$\delta_{\mathrm{M}} < \delta < 4\gamma^3 + \delta_{\mathrm{M}}, \quad \frac{1}{4} \le \gamma < \frac{1}{2}.$$

Table 1 A lattice matrix example with $\gamma_1 = 0.35$, $\gamma_2 = 0.5$, $\gamma = 0.45$, and $t = 3$

$g_{[i_1,i_2]}$	1	x_1	x_2	x_1^2	x_1x_2	x_2^2	x_1^3	$x_1^2x_2$	$x_1x_2^2$
$g_{[0,0]}$	U^3								
$g_{[1,0]}$	–	X_1U^2							
$g_{[0,1]}$	–		X_2U						
$g_{[2,0]}$	–	–		X_1^2U					
$g_{[1,1]}$	–	–	–		X_1X_2				
$g_{[0,2]}$	–		–			X_2^2			
$g_{[3,0]}$	–	–		–			X_1^3		
$g_{[2,1]}$	–	–	–	–	–			$X_1^2X_2$	
$g_{[1,2]}$	–	–	–		–	–			$X_1X_2^2$

Since we deal with two simultaneous modular univariate linear equations, the running time is still polynomial in $\log_2 N$. □

3.2 LSB Case

We present the partial key exposure attack on common prime RSA under the LSB case with the following proposition.

Proposition 2 *Let $N = pq$ be a common prime RSA modulus with two balanced primes p and q of the same bit-length. Let $e \simeq N^{1-\gamma}$ and $d \simeq N^{\delta}$ be its public and private exponents such that $ed \equiv 1 \pmod{\mathrm{lcm}(p-1, q-1)}$, where $\gcd(p-1, q-1) = 2g$ for a large prime $g \simeq N^{\gamma}$. Given an approximation of d with known LSBs d_{L} in a $(\delta_{\mathrm{L}} \log_2 N)$-bit block satisfying $d = \bar{d}L + d_{\mathrm{L}}$, where $L = 2^{\delta_{\mathrm{L}} \log_2 N}$ for known δ_{L} and unknown $\bar{d}$ is bounded by $|\bar{d}| \leq N^{\delta - \delta_{\mathrm{L}}}$. Then N can be efficiently factored in time polynomial in $\log_2 N$ if*

$$\delta_{\mathrm{L}} < \delta < 4\gamma^3 + \delta_{\mathrm{L}}, \quad \frac{1}{4} \leq \gamma < \frac{1}{2}.$$

Proof According to the property of common prime RSA, we have $N - 1 = 2gh$ for two primes g, h from relation (1), which implies $N - 1 \equiv 0 \pmod{g}$ and further

$$\frac{N-1}{2} \equiv 0 \pmod{g}.$$

Besides, we have $ed - 1 \equiv 0 \pmod{g}$ from equation (2). Since $d = \bar{d}L + d_{\mathrm{L}}$ for $L = 2^{\delta_{\mathrm{L}} \log_2 N}$ with known δ_{L} and unknown $\bar{d}$, we substitute d into $ed - 1 \equiv 0 \pmod{g}$ and obtain

$$e\bar{d}L + ed_{\mathrm{L}} - 1 \equiv 0 \pmod{g}.$$

Because $(N-1)/2 = gh$ is a product of two primes, the inverse of eL modulo $(N-1)/2$ must exist, which is denoted by $(eL)^{-1} \bmod (N-1)/2$. Multiplying the above equation by $(eL)^{-1} \bmod (N-1)/2$, we have a modular univariate linear equation,

$$x_1 + a_1 \equiv 0 \pmod{g}, \tag{9}$$

where x_1 represents the unknown $\bar{d}$ and

$$a_1 = (ed_{\mathrm{L}} - 1)\left((eL)^{-1} \bmod \frac{N-1}{2}\right) \bmod (N-1).$$

Moreover, since $(p-1)(q-1) = 2ga \cdot 2gb = 4g^2ab$ and $(p-1)(q-1) = pq - p - q + 1 = N + 1 - (p+q)$, we have another modular univariate linear equation,

$$x_2 + a_2 \equiv 0 \pmod{g^2}, \tag{10}$$

where x_2 represents the unknown $-(p+q)$ and $a_2 = N + 1$. Thus, combining two simultaneous modular univariate linear equations (9) and (10), we have the following equation system,

$$\begin{cases} x_1 + a_1 \equiv 0 \pmod{g} \\ x_2 + a_2 \equiv 0 \pmod{g^2} \end{cases} \tag{11}$$

We focus on the above equation system with roots $x_1' = \bar{d}$ and $x_2' = -(p+q)$. Once we discover an integer pair (x_1', x_2') satisfying (11), we can factor the RSA modulus N via $p + q$. Similarly, since $U \equiv 0 \pmod{g}$ with $g \simeq N^{\gamma}$, and $X_1 = N^{\delta - \delta_{\mathrm{L}}}$, $X_2 = N^{1/2}$, we have $n = 2$, $r_1 = 1$, $r_2 = 2$, $r = 1$, $U = N - 1 \simeq N$, $\gamma_1 = \delta - \delta_{\mathrm{L}}$, $\gamma_2 = 1/2$ and $\eta = \gamma$. Therefore, we directly apply Lemma 3 and obtain

$$\sqrt[n]{\frac{\gamma_1 \cdots \gamma_n}{r r_1 \cdots r_n}} < \eta^{\frac{n+1}{n}}$$
$$\Rightarrow \quad \gamma_1 \cdots \gamma_n < r r_1 \cdots r_n \eta^{n+1} \quad \Rightarrow \quad \gamma_1\gamma_2 < 2\gamma^3.$$

Substituting $\gamma_1 = \delta - \delta_{\mathrm{L}}$ and $\gamma_2 = 1/2$, we have

$$\delta < 4\gamma^3 + \delta_{\mathrm{L}}.$$

Moreover, we must ensure that $0 < \delta - \delta_{\mathrm{L}} \leq \gamma$ and $1/2 \leq 2\gamma$, which imply that $\gamma \geq 1/4$ and $\delta_{\mathrm{L}} < \delta < \gamma + \delta_{\mathrm{L}}$. Gathering them together with $0 < \gamma < 1/2$, we derive the final condition,

$$\delta_{\mathrm{L}} < \delta < 4\gamma^3 + \delta_{\mathrm{L}}, \quad \frac{1}{4} \leq \gamma < \frac{1}{2}.$$

The detailed analysis and lattice construction is similar to that of MSB case and we omit it here. □

3.3 Mix case

We present the partial key exposure attack on common prime RSA under the Mix case with the following proposition.

Proposition 3 *Let $N = pq$ be a common prime RSA modulus with two balanced primes p and q of the same bit-length. Let $e \simeq N^{1-\gamma}$ and $d \simeq N^{\delta}$ be its public and private exponents such that $ed \equiv 1 \pmod{\mathrm{lcm}(p-1, q-1)}$, where $\gcd(p-1, q-1) = 2g$ for a large prime $g \simeq N^{\gamma}$. Given an approximation of d with known MSBs d_{M} in a $(\delta_{\mathrm{M}} \log_2 N)$-bit block along with LSBs d_{L} in a $(\delta_{\mathrm{L}} \log_2 N)$-bit block satisfying $d = d_{\mathrm{M}}M + \bar{d}L + d_{\mathrm{L}}$, where $M = 2^{(\delta-\delta_{\mathrm{M}})\log_2 N}$, $L = 2^{\delta_{\mathrm{L}} \log_2 N}$ for known δ_{M}, δ_{L} and unknown $\bar{d}$ is bounded by $|\bar{d}| \leq N^{\delta-\delta_{\mathrm{M}}-\delta_{\mathrm{L}}}$. Then N can be efficiently factored in time polynomial in $\log_2 N$ if*

$$\delta_{\mathrm{M}} + \delta_{\mathrm{L}} < \delta < 4\gamma^3 + \delta_{\mathrm{M}} + \delta_{\mathrm{L}}, \quad \frac{1}{4} \leq \gamma < \frac{1}{2}.$$

Proof According to the property of common prime RSA, we have $N - 1 = 2gh$ for two primes g, h from relation (1), which implies $N - 1 \equiv 0 \pmod{g}$ and further

$$\frac{N-1}{2} \equiv 0 \pmod{g}.$$

Besides, we have $ed - 1 \equiv 0 \pmod{g}$ from equation (2). Since $d = d_{\mathrm{M}}M + \bar{d}L + d_{\mathrm{L}}$ for $M = 2^{(\delta-\delta_{\mathrm{M}})\log_2 N}$, $L = 2^{\delta_{\mathrm{L}} \log_2 N}$ with known δ_{M}, δ_{L} and unknown $\bar{d}$, we substitute d into $ed - 1 \equiv 0 \pmod{g}$ and obtain

$$ed_{\mathrm{M}}M + e\bar{d}L + ed_{\mathrm{L}} - 1 \equiv 0 \pmod{g}.$$

Because $(N-1)/2 = gh$ is a product of two primes, the inverse of eL modulo $(N-1)/2$ must exist, which is denoted by $(eL)^{-1} \bmod (N-1)/2$. Multiplying the above equation by $(eL)^{-1} \bmod (N-1)/2$, we have a modular univariate linear equation,

$$x_1 + a_1 \equiv 0 \pmod{g}, \tag{12}$$

where x_1 represents the unknown $\bar{d}$ and

$$a_1 = (ed_{\mathrm{M}}M + ed_{\mathrm{L}} - 1)\left((eL)^{-1} \bmod \frac{N-1}{2}\right) \bmod (N-1).$$

Moreover, since $(p-1)(q-1) = 2ga \cdot 2gb = 4g^2ab$ and $(p-1)(q-1) = pq - p - q + 1 = N + 1 - (p+q)$, we have another modular univariate linear equation,

$$x_2 + a_2 \equiv 0 \pmod{g^2}, \tag{13}$$

where x_2 represents the unknown $-(p+q)$ and $a_2 = N+1$. Thus, combining two simultaneous modular univariate linear equations (12) and (13), we have the following equation system,

$$\begin{cases} x_1 + a_1 \equiv 0 \pmod{g} \\ x_2 + a_2 \equiv 0 \pmod{g^2} \end{cases} \tag{14}$$

We focus on the above equation system with roots $x_1' = \bar{d}$ and $x_2' = -(p+q)$. Once we discover an integer pair (x_1', x_2') satisfying (14), we can factor the RSA modulus N via $p+q$. Similarly, since $U \equiv 0 \pmod{g}$ with $g \simeq N^{\gamma}$, and $X_1 = N^{\delta-\delta_{\mathrm{M}}-\delta_{\mathrm{L}}}$, $X_2 = N^{1/2}$, we have $n = 2$, $r_1 = 1$, $r_2 = 2$, $r = 1$, $U = N - 1 \simeq N$, $\gamma_1 = \delta - \delta_{\mathrm{M}} - \delta_{\mathrm{L}}$, $\gamma_2 = 1/2$, and $\eta = \gamma$. Therefore, we directly apply Lemma 3 and obtain

$$\begin{aligned} \sqrt[n]{\frac{\gamma_1 \cdots \gamma_n}{r r_1 \cdots r_n}} < \eta^{\frac{n+1}{n}} \quad &\Rightarrow \quad \gamma_1 \\ \cdots \gamma_n < r r_1 \cdots r_n \eta^{n+1} \quad &\Rightarrow \quad \gamma_1\gamma_2 < 2\gamma^3. \end{aligned}$$

Substituting $\gamma_1 = \delta - \delta_{\mathrm{M}} - \delta_{\mathrm{L}}$ and $\gamma_2 = 1/2$, we have

$$\delta < 4\gamma^3 + \delta_{\mathrm{M}} + \delta_{\mathrm{L}}.$$

Moreover, we must ensure that $0 < \delta - \delta_{\mathrm{M}} - \delta_{\mathrm{L}} \leq \gamma$ and $1/2 \leq 2\gamma$, which imply that $\gamma \geq 1/4$ and $\delta_{\mathrm{M}} + \delta_{\mathrm{L}} < \delta < \gamma + \delta_{\mathrm{M}} + \delta_{\mathrm{L}}$. Gathering them together with $0 < \gamma < 1/2$, we derive the final condition,

$$\delta_{\mathrm{M}} + \delta_{\mathrm{L}} < \delta < 4\gamma^3 + \delta_{\mathrm{M}} + \delta_{\mathrm{L}}, \quad \frac{1}{4} \leq \gamma < \frac{1}{2}.$$

The detailed analysis and lattice construction is similar to that of MSB case and we omit it here. □

As observed, the Mix case described in Proposition 3 covers both MSB case and LSB case as two specific scenarios. More precisely, when $\delta_{\mathrm{L}} = 0$, Proposition 3 is identical to Proposition 1, and when $\delta_{\mathrm{M}} = 0$, it is identical to Proposition 2.

4 Experimental results

To validate the validity and effectiveness of our proposed partial key exposure attacks on common prime RSA, which

exploits Proposition 1, Proposition 2, and Proposition 3, we conducted a series of numerical experiments. These experiments were performed on a computer running a 64-bit Windows 10 operating system with Ubuntu 22.04 installed on WSL 2. The system had a CPU operating at 2.80 GHz and 16 GB of RAM. The experiments were conducted using `SageMath` [31], and the parameters for generating the common prime RSA instances were randomly chosen.

We generated a common prime RSA modulus N of bit-length $\log_2 N$ and a private exponent d with a predetermined bit-length and known most significant bits (MSBs) and/or least significant bits (LSBs) in each experiment. We then derived the corresponding public exponent e using its key equation $ed \equiv 1 \pmod{\text{lcm}(p-1, q-1)}$. Furthermore, we gradually increased the bit-length of d to achieve a larger δ for performing a successful partial key exposure attack.

To execute the proposed attacks, we selected a suitable parameter t to construct a lattice. The experimental results are presented in Table 2. The Case column indicates the specific exposure case discussed earlier. The γ column indicates the size of g in the generated common prime RSA instance. The δ_{M} and δ_{L} columns indicate the size of the known MSBs and LSBs exposures used in the experiments, respectively. The δ_t column provides the theoretical upper bound of d, while the δ_e column presents the corresponding experimental results. The Leak column shows the percentage of partial key exposure in private key. The lattice settings are controlled by t, and the lattice dimension is denoted by w. The time consumption of the LLL algorithm and the Gröbner basis computation is recorded in the Time column (measured in seconds).

During each experiment, we collected sufficient polynomials that satisfied the solvable requirements after running the LLL algorithm. As indicated in Table 2, the running time increases as the dimension of the lattice becomes larger. The reason is that it is mainly influenced by the lattice dimension and the lattice basis matrix entries. Finally, we obtained the integer polynomial equations having a shared root by transforming the derived vectors into polynomials and extracted this shared root.

To demonstrate scalability beyond 1024-bit RSA moduli, we extended our experiments to 2048- and 3072-bit moduli (see Table 2). Under the same lattice parameter settings, the running time increases by roughly 2.5× for 2048-bit moduli and 4.5× for 3072-bit moduli, while all three attack variants (MSB, LSB, Mix) still succeed at the same relative leakage rates. These results confirm that our proposed attacks remain practical and effective at larger, real-world key sizes.

Furthermore, we discuss additional findings based on several observations from Table 2. First, we noticed that the proportion of required partial key exposure (indicated by the green mark) decreases as γ increases. This suggests that our proposed attack becomes more effective when larger values of g are used in common prime RSA. We observed that the proportion of required partial key exposure (indicated by the blue mark) increases as the number of exposed bits grows. This implies that our attack remains feasible even when only a small number of bits in the private key are exposed. Moreover, an interesting phenomenon (indicated by the red mark) was observed during the experiments, showing that partial key exposure attack targeting the MSB case tends to be slightly better.

We provide a concise explanation of the root extraction procedure used in our attacks. We recovered $x_2' = -(p+q)$, which allows us to factorize N by putting obtained integer polynomials into Gröbner basis computation. The common root was successfully recovered in all generated common prime RSA instances. However, the experimental results fell slightly short of reaching the theoretical insecure bound due to limited computing resources. We believe that the practical attack results can be further improved by constructing lattices with higher dimension. Additionally, we provide the following toy example to aid in numerical understanding.

Example 1 We provide a numerical example to illustrate the partial key exposure attack on common prime RSA, utilizing Proposition 3. In this example, we consider a toy scenario where we have set $\gamma = 0.4$, and work with two 256-bit primes, denoted as p and q, resulting in a composite modulus N with a bit-length of $\log_2 N = 512$.

Besides, we have a private exponent d consisting of 159 bits, of which the most significant bits (MSBs) and least significant bits (LSBs) are leaked, revealing 20 and 30 bits, respectively. The specific values for this example instance are as follows.

$$
\begin{aligned}
N &= 96612085779573789844190032734611214944237738080822481722482680097966648686276683063935153983163269887563643166482174781839545393271050434557670399586087113541543308637280816045544440403603399393271232813007824665204834119657335100876426570999532131,\\
e &= 700237 \text{ (i.e., } \texttt{10101010111101001101}\text{)},\\
d_{\text{M}} &= 856799747 \text{ (i.e., } \texttt{11001100010001101110100000011}\text{)}.
\end{aligned}
$$

We now show how the parameters in Lemma 3 are instantiated in this concrete setting. First, we have

$$
n = 2,\ r_1 = 1,\ r_2 = 2,\ r = 1,\ U = N - 1,\ \gamma_1 = 0.213,\ \gamma_2 = 0.5,\ \eta = 0.4.
$$

Table 2 Experimental results of partial key exposure attacks on common prime RSA

$\log_2 N$	Case	γ	δ_{M}	δ_{L}	δ_t	δ_e	Leak	t	w	Time
1024	MSB	0.36	0.146	0	0.332	0.282	51.7%	4	22	0.55 s
1024	MSB	0.40	0.127	0	0.383	0.314	40.4%	4	20	0.35 s
1024	MSB	0.40	0.146	0	0.402	0.329	44.3%	4	20	0.35 s
1024	MSB	0.44	0.146	0	0.486	0.401	36.4%	5	25	0.85 s
1024	MSB	0.48	0.146	0	0.588	0.497	29.3%	6	31	1.58 s
1024	MSB	0.49	0.146	0	0.616	0.511	28.5%	6	31	1.65 s
2048	MSB	0.29	0.014	0	0.111	0.088	15.9%	4	29	1.98 s
2048	MSB	0.36	0.146	0	0.332	0.282	51.7%	4	22	1.52 s
2048	MSB	0.40	0.127	0	0.383	0.314	40.4%	4	20	0.97 s
3072	MSB	0.36	0.146	0	0.332	0.282	51.7%	4	22	2.56 s
3072	MSB	0.40	0.127	0	0.383	0.314	40.4%	4	20	1.42 s
1024	LSB	0.40	0	0.127	0.383	0.306	41.5%	4	21	0.21 s
1024	LSB	0.45	0	0.003	0.367	0.290	1.03%	6	33	2.71 s
1024	LSB	0.45	0	0.039	0.404	0.327	11.9%	6	33	2.72 s
1024	LSB	0.45	0	0.073	0.438	0.350	20.8%	6	34	2.91 s
1024	LSB	0.45	0	0.161	0.526	0.442	36.4%	6	34	2.99 s
1024	LSB	0.45	0	0.423	0.787	0.693	61.0%	6	35	3.14 s
2048	LSB	0.29	0	0.015	0.111	0.088	17.0%	4	29	1.86 s
2048	LSB	0.40	0	0.127	0.383	0.306	41.5%	4	21	0.53 s
2048	LSB	0.45	0	0.003	0.367	0.290	1.03%	6	33	7.58 s
3072	LSB	0.40	0	0.127	0.383	0.306	41.5%	4	21	0.95 s
3072	LSB	0.45	0	0.003	0.367	0.290	1.03%	6	33	12.51 s
1024	Mix	0.32	0.004	0.004	0.139	0.090	8.88%	2	10	0.04 s
1024	Mix	0.36	0.098	0.137	0.421	0.337	69.7%	3	18	0.13 s
1024	Mix	0.40	0.059	0.068	0.383	0.304	41.7%	4	22	0.42 s
1024	Mix	0.40	0.132	0.127	0.515	0.450	57.5%	5	29	1.56 s
1024	Mix	0.44	0.102	0.144	0.586	0.518	47.4%	7	44	10.53 s
1024	Mix	0.48	0.144	0.165	0.751	0.691	44.7%	10	72	101.46 s
2048	Mix	0.29	0.007	0.007	0.111	0.088	15.9%	5	40	4.59 s
2048	Mix	0.32	0.004	0.004	0.139	0.090	8.88%	2	10	0.09 s
2048	Mix	0.36	0.098	0.137	0.421	0.337	69.7%	3	18	0.35 s
3072	Mix	0.32	0.004	0.004	0.139	0.090	8.88%	2	10	0.19 s
3072	Mix	0.36	0.098	0.137	0.421	0.337	69.7%	3	18	0.62 s

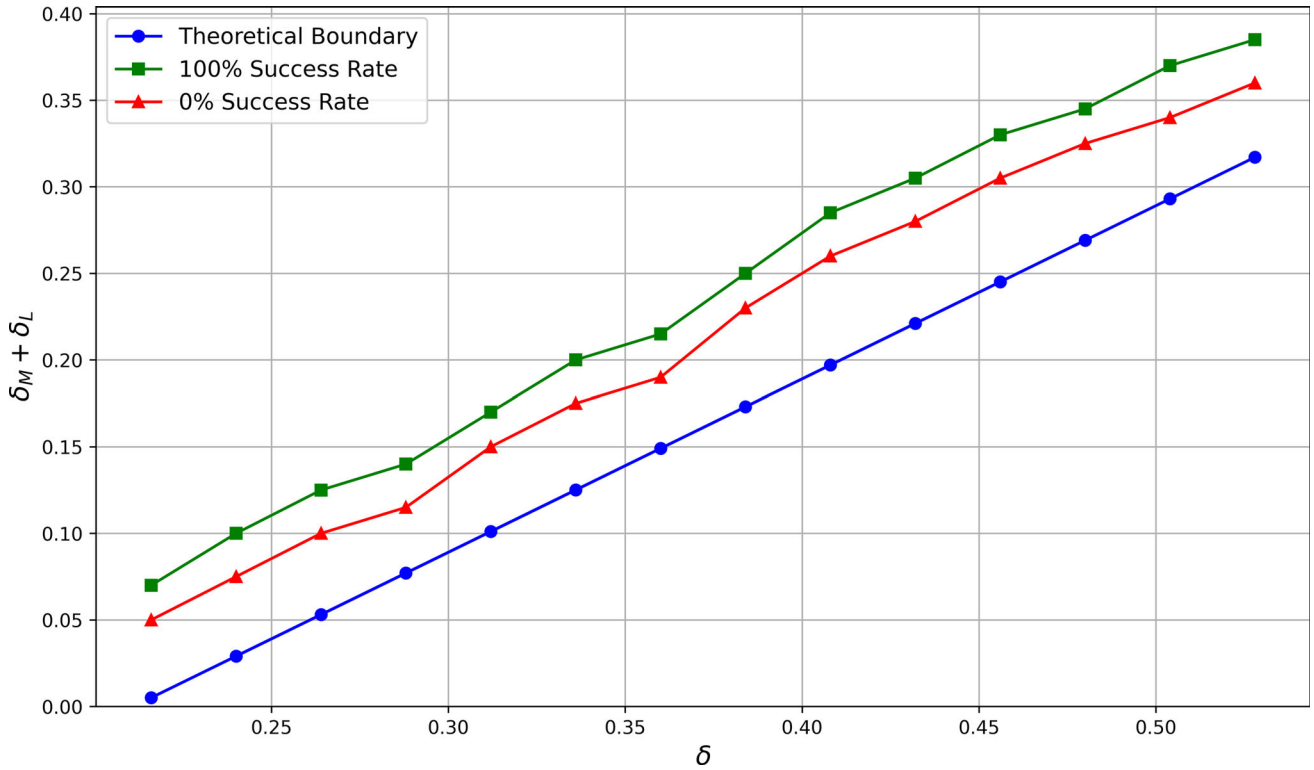

Fig. 2 Boundary region tests on known-bit fraction $\delta_{\mathrm{M}} + \delta_{\mathrm{L}}$ for various δ's and $\gamma = 0.375$, illustrating the transition at 100% success rate boundary, 0% success rate boundary, and theoretical boundary

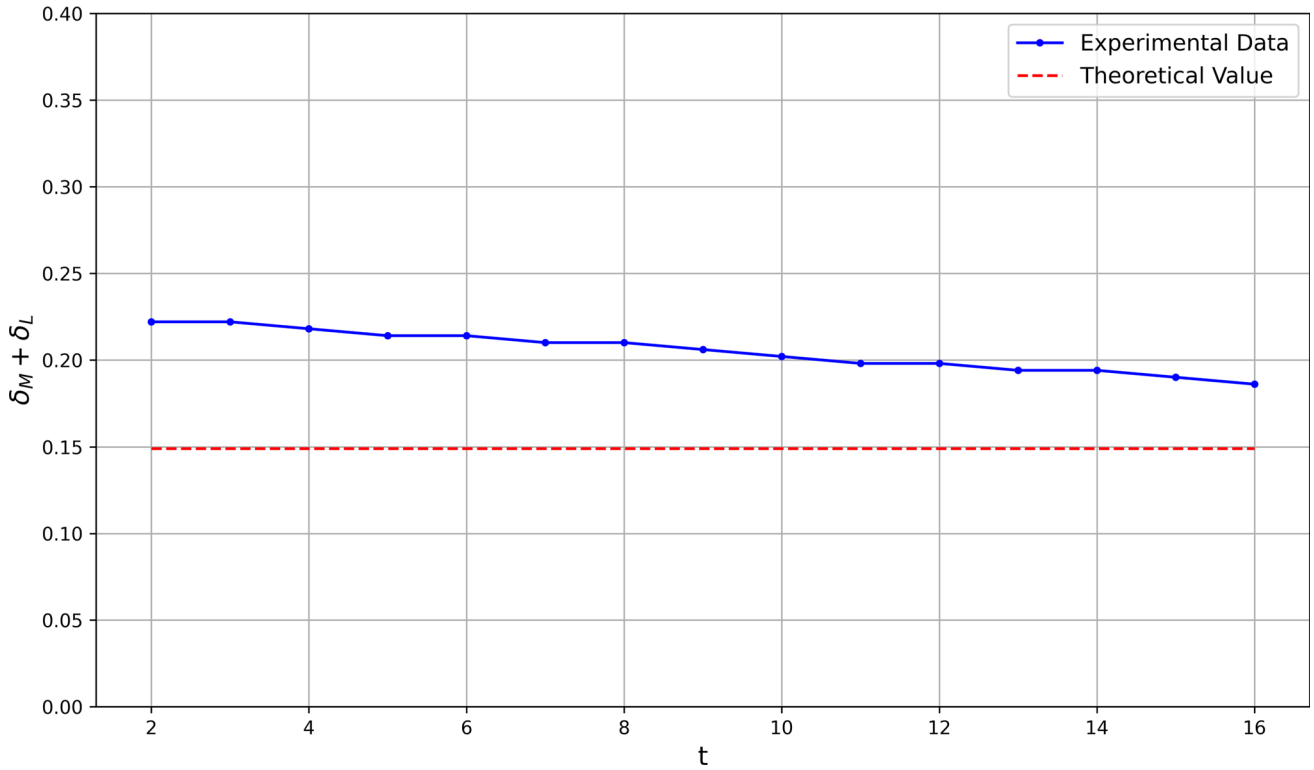

Fig. 3 Discrepancy tests on known-bit fraction $\delta_{\mathrm{M}} + \delta_{\mathrm{L}}$ for various t's and $\delta = 0.36$, $\gamma = 0.375$, illustrating its downward trend using higher-dimensional lattices

Then, we know $\log U = \log(N-1) \approx \log N \approx 154$ and hence $1/\sqrt{\log U} \approx 0.08$. Therefore, the condition $\eta \gg 1/\sqrt{\log U}$ is satisfied. Finally, we verify by direct substitution that the remaining inequalities, i.e., $\gamma_1 \leq r_1\eta$ and $\gamma_2 \leq r_2\eta$ hold for this concrete setting.

$$\gamma_1 \leq r_1\eta : \ 0.213 < 1 \times 0.4, \qquad \gamma_2 \leq r_2\eta : \ 0.5 < 2 \times 0.4.$$

To conduct the partial key exposure attack, we utilize the computed parameters a_1, a_2 as follows.

$$\begin{aligned} a_1 = {} & 339435056389007461382995828393378087822726708759137592568410 \\ & 311579754228258366362973498272326193741451030909579746435335 \\ & 300700834222436809886845526856108 6, \\ a_2 = {} & 966120857795737898441900327346112149442377380808224817224826 \\ & 800979666486862766830639351539831632698875636431664821747818 \\ & 395453932710504345576703995860871 2. \end{aligned}$$

We then set $t = 10$ to construct a 90-dimensional lattice. After approximately 397 seconds, we successfully extract the desired root (x_1', x_2'). The obtained root values are as follows.

$$\begin{aligned} x_1' = {} & 527730494143743683881059337157557, \\ x_2' = {} & -196778280239591787149835167141107246661728747350481403912600 \\ & 01550771284534060 0. \end{aligned}$$

Using x_2', we compute $p + q = -x_2'$, which allows us to factorize $N = pq$ as follows.

$$\begin{aligned} p = {} & 940057264323314171429706366514839509339492710090002422148482 \\ & 07760523437055033, \\ q = {} & 102772553807260370006864530489623295727779476341481161697751 \\ & 807747189408285567. \end{aligned}$$

It can be easily verified that $N = pq$ does hold, confirming the success of applying Proposition 3 to the partial key exposure attack on common prime RSA.

4.1 Boundary region Tests

To investigate the behavior of our lattice-based attacks as the total fraction of exposed key bits, i.e. $\delta_M + \delta_L$, approaches the theoretical limits, we conducted a fine-grained sweep of $\delta_M + \delta_L$ in steps of 0.005 down to the theoretical value $\delta - 4\gamma^3$ for a moderate $\gamma = 0.375$. For each δ we performed 10 independent trials, constructing lattices of the appropriate dimension and measuring the practical success probability. As shown in Figure 2, the attack maintains 100% success until within approximately 0.07 above the predicted boundary, and the success rate falls off sharply to near 0% if $\delta_M + \delta_L$ is a bit lower. We also observe a small gap between the theoretical and experimental curves, which we attribute to the limited computing resources used in practice and the resulting deviation from asymptotic lattice reduction performance.

To provide a more thorough explanation of the gap between the theoretical and experimental bounds in Table 2 and Figure 2, we conducted a set of additional experiments using increased computational resources. In the test, we fix a representative attack instance and incrementally increase the lattice dimension parameter t, thereby enlarging the lattice. As shown in Figure 3, the minimum leakage fraction required for success decreases smoothly as t grows, drawing closer to the theoretical threshold. Although the practical cutoff never exactly attains the ideal bound, the downward trend demonstrates that higher-dimensional lattices consistently improve attack performance. Therefore, the observed discrepancy simply reflects our initial focus on smaller, faster validation and does not affect the practical applicability of the proposed attacks.

5 Conclusion

The literature extensively examines the vulnerability of common prime RSA to small private key attacks. However, an unexplored area is the partial key exposure attack, which assumes knowledge of some significant bits of the private key due to side channel leakage. In this paper, we conduct the first study on partial key exposure attacks on common prime RSA. We present three attack propositions, each based on a distinct attack scenario. Our results demonstrate further advancements in security assessment on common prime RSA compared to previous small private key attacks.

It is worth mentioning that there are several approaches that can be employed to enhance our primary results (especially exploring attacks that falls outside our proposed region, namely $\gamma < 1/4$), such as using more efficient lattice-based strategy, considering multiple private keys or leaking the middle bits of the private key. These possibilities remain to be

explored in future work to generalize partial key exposure attacks on common prime RSA.

Author Contributions M.Z. wrote the main manuscript text and prepared figures. All authors reviewed the manuscript.

Funding This work was supported by the National Natural Science Foundation of China, grant number 62002335 Ningbo Young Science and Technology Talent Cultivation Program, grant number 2023QL007 and the Open Fund of Advanced Cryptography and System Security Key Laboratory of Sichuan Province, grant number SKLACSS-202315.

Data Availability The datasets generated during and/or analyzed during the current study are available from the corresponding author on reasonable request.

Declarations

Competing interests The authors declare no competing interests.

References

1. Becker, T., Weispfenning, V., Kredel, H.: Gröbner bases - a computational approach to commutative algebra, Graduate texts in mathematics, vol. 141. Springer (1993)
2. Blömer, J., May, A.: New partial key exposure attacks on RSA. In: Boneh D (ed) Advances in Cryptology - CRYPTO 2003, 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings, Lecture Notes in Computer Science, vol 2729. Springer, pp 27–43, (2003) https://doi.org/10.1007/978-3-540-45146-4_2
3. Boneh, D., Durfee, G.: Cryptanalysis of RSA with private key d less than $N^{0.292}$. In: Stern J (ed) Advances in Cryptology - EUROCRYPT '99, International Conference on the Theory and Application of Cryptographic Techniques, Prague, Czech Republic, May 2-6, 1999, Proceeding, Lecture Notes in Computer Science, vol 1592. Springer, pp 1–11, (1999) https://doi.org/10.1007/3-540-48910-X_1
4. 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) Advances in Cryptology - ASIACRYPT '98, International Conference on the Theory and Applications of Cryptology and Information Security, Beijing, China, October 18-22, 1998, Proceedings, Lecture Notes in Computer Science, vol 1514. Springer, pp 25–34, (1998) https://doi.org/10.1007/3-540-49649-1_3
5. Collins, T., Hopkins, D., Langford, S., et al: Public key cryptographic apparatus and method. U.S. Patent 5848159 (1998)
6. Coppersmith, D.: Finding a small root of a univariate modular equation. In: Maurer UM (ed) Advances in Cryptology - EUROCRYPT '96, International Conference on the Theory and Application of Cryptographic Techniques, Saragossa, Spain, May 12-16, 1996, Proceeding, Lecture Notes in Computer Science, vol 1070. Springer, pp 155–165, (1996) https://doi.org/10.1007/3-540-68339-9_14
7. Coppersmith, D.: Small solutions to polynomial equations, and low exponent rsa vulnerabilities. J. Cryptol. **10**(4), 233–260 (1997). https://doi.org/10.1007/s001459900030
8. Erdos, P., Pomerance, C., Schmutz, E.: Carmichael's lambda function. Acta Arith **58**(4), 363–385 (1991)
9. Ernst, M., Jochemsz, E., May, A., et al: Partial key exposure attacks on RSA up to full size exponents. In: Cramer R (ed) Advances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005, Proceedings, Lecture Notes in Computer Science, vol 3494. Springer, pp 371–386, (2005). https://doi.org/10.1007/11426639_22
10. Fiat, A.: Batch RSA. J Cryptol **10**(2), 75–88 (1997). https://doi.org/10.1007/s001459900021
11. Halderman, J.A., Schoen, S.D., Heninger, N., et al.: Lest we remember: cold-boot attacks on encryption keys. Commun. ACM **52**(5), 91–98 (2009). https://doi.org/10.1145/1506409.1506429
12. Hinek, M.J.: Another look at small RSA exponents. In: Pointcheval D (ed) Topics in Cryptology - CT-RSA 2006, The Cryptographers' Track at the RSA Conference 2006, San Jose, CA, USA, February 13-17, 2006, Proceedings, Lecture Notes in Computer Science, vol 3860. Springer, pp 82–98, (2006). https://doi.org/10.1007/11605805_6
13. Howgrave-Graham, N.: Finding small roots of univariate modular equations revisited. In: Darnell M (ed) Cryptography and Coding, 6th IMA International Conference, Cirencester, UK, December 17-19, 1997, Proceedings, Lecture Notes in Computer Science, vol 1355. Springer, pp 131–142, (1997). https://doi.org/10.1007/BFb0024458
14. Jochemsz, E., May, A.: A strategy for finding roots of multivariate polynomials with new applications in attacking RSA variants. In: Lai X, Chen K (eds) Advances in Cryptology - ASIACRYPT 2006, 12th International Conference on the Theory and Application of Cryptology and Information Security, Shanghai, China, December 3-7, 2006, Proceedings, Lecture Notes in Computer Science, vol 4284. Springer, pp 267–282, (2006). https://doi.org/10.1007/11935230_18
15. Kocher, P.C.: Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In: Koblitz N (ed) Advances in Cryptology - CRYPTO '96, 16th Annual International Cryptology Conference, Santa Barbara, California, USA, August 18-22, 1996, Proceedings, Lecture Notes in Computer Science, vol 1109. Springer, pp 104–113, (1996). https://doi.org/10.1007/3-540-68697-5_9
16. Kuwakado, H., Koyama, K., Tsuruoka, Y.: New RSA-type scheme based on singular cubic curves $y^2 \equiv x^3 + bx^2 \ (modn)$. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences E78-A(1):27–33 (1995)
17. Lenstra, A.K., Lenstra, H.W., Lovász, L.: Factoring polynomials with rational coefficients. Math. Ann. **261**(4), 515–534 (1982)
18. Lu, Y., Zhang, R., Peng, L., et al: Solving linear equations modulo unknown divisors: Revisited. In: Iwata T, Cheon JH (eds) Advances in Cryptology - ASIACRYPT 2015 - 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, November 29 - December 3, 2015, Proceedings, Part I, Lecture Notes in Computer Science, vol 9452. Springer, pp 189–213, (2015)https://doi.org/10.1007/978-3-662-48797-6_9
19. May, A.: New RSA vulnerabilities using lattice reduction methods. PhD thesis, University of Paderborn, (2003) http://ubdata.uni-paderborn.de/ediss/17/2003/may/disserta.pdf
20. May, A.: Using LLL-reduction for solving RSA and factorization problems. In: Nguyen PQ, Vallée B (eds) The LLL Algorithm - Survey and Applications. Information Security and Cryptography, Springer, p 315–348, (2010) https://doi.org/10.1007/978-3-642-02295-1_10
21. May, A., Nowakowski, J., Sarkar, S.: Partial key exposure attack on short secret exponent CRT-RSA. In: Tibouchi M, Wang H (eds) Advances in Cryptology - ASIACRYPT 2021 - 27th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 6-10, 2021, Proceedings, Part I, Lecture Notes in Computer Science, vol 13090. Springer, pp 99–129, (2021) https://doi.org/10.1007/978-3-030-92062-3_4

22. Mumtaz, M., Luo, P.: Remarks on the cryptanalysis of common prime rsa for iot constrained low power devices. Inf. Sci. **538**, 54–68 (2020). https://doi.org/10.1016/j.ins.2020.05.075
23. Quisquater, J.J., Couvreur, C.: Fast decipherment algorithm for RSA public-key cryptosystem. Electronics Letters **18**(21), 905–907 (1982). https://doi.org/10.1145/359340.359342
24. Ristenpart, T., Tromer, E., Shacham, H., et al: Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. In: Al-Shaer E, Jha S, Keromytis AD (eds) Proceedings of the 2009 ACM Conference on Computer and Communications Security, CCS 2009, Chicago, Illinois, USA, November 9-13, 2009. ACM, pp 199–212, (2009) https://doi.org/10.1145/1653662.1653687
25. Rivest, R.L., Shamir, A., Adleman, L.M.: A method for obtaining digital signatures and public-key cryptosystems. Commun ACM **21**(2), 120–126 (1978). https://doi.org/10.1145/359340.359342
26. Sarkar, S., Maitra, S.: Side channel attack to actual cryptanalysis: Breaking CRT-RSA with low weight decryption exponents. In: Prouff E, Schaumont P (eds) Cryptographic Hardware and Embedded Systems - CHES 2012 - 14th International Workshop, Leuven, Belgium, September 9-12, 2012. Proceedings, Lecture Notes in Computer Science, vol 7428. Springer, pp 476–493, (2012) https://doi.org/10.1007/978-3-642-33027-8_28
27. Sarkar, S., Maitra, S.: Cryptanalytic results on dual crt and common prime rsa. Des. Codes Cryptogr. **66**(1–3), 157–174 (2013). https://doi.org/10.1007/s10623-012-9675-5
28. Takagi, T.: Fast RSA-type cryptosystem modulo $p^k q$. In: Krawczyk H (ed) Advances in Cryptology - CRYPTO '98, 18th Annual International Cryptology Conference, Santa Barbara, California, USA, August 23-27, 1998, Proceedings, Lecture Notes in Computer Science, vol 1462. Springer, pp 318–326, (1998) https://doi.org/10.1007/BFb0055738
29. Takayasu, A., Kunihiro, N.: Better lattice constructions for solving multivariate linear equations modulo unknown divisors. In: Boyd C, Simpson L (eds) Information Security and Privacy - 18th Australasian Conference, ACISP 2013, Brisbane, Australia, July 1-3, 2013. Proceedings, Lecture Notes in Computer Science, vol 7959. Springer, pp 118–135, (2013) https://doi.org/10.1007/978-3-642-39059-3_9
30. Takayasu, A., Kunihiro, N.: Partial key exposure attacks on rsa: achieving the boneh-durfee bound. Theor. Comput. Sci. **761**, 51–77 (2019). https://doi.org/10.1016/j.tcs.2018.08.021
31. The Sage Developers (2023) SageMath, the Sage Mathematics Software System (Version 9.5). https://www.sagemath.org
32. Wiener, M.J.: Cryptanalysis of short rsa secret exponents. IEEE Trans. Inf. Theory **36**(3), 553–558 (1990). https://doi.org/10.1109/18.54902
33. Yuan, S., Yu, W., Wang, K., et al: Partial key exposure attacks on RSA with moduli $n = p^r q^s$. In: IEEE International Symposium on Information Theory, ISIT 2022, Espoo, Finland, June 26 - July 1, 2022. IEEE, pp 1436–1440, (2022) https://doi.org/10.1109/ISIT50566.2022.9834542
34. Zheng, M.: Partial key exposure attack on common prime RSA. In: Ge C, Yung M (eds) Information Security and Cryptology - 19th International Conference, Inscrypt 2023, Hangzhou, China, December 9-10, 2023, Revised Selected Papers, Part II, Lecture Notes in Computer Science, vol 14527. Springer, pp 407–410, (2023) https://doi.org/10.1007/978-981-97-0945-8_27
35. Zheng, M.: Revisiting small private key attacks on common prime rsa. IEEE Access **12**, 5203–5211 (2024). https://doi.org/10.1109/ACCESS.2024.3349633
36. Zheng, M., Kang, H.: Lattice-based cryptanalysis of rsa-type cryptosystems: a bibliometric analysis. Cybersecur **7**(1), 74 (2024). https://doi.org/10.1186/s42400-024-00289-7
37. Zheng, M., Kunihiro, N., Hu, H.: Cryptanalysis of RSA variants with modified Euler quotient. In: Joux A, Nitaj A, Rachidi T (eds) Progress in Cryptology - AFRICACRYPT 2018 - 10th International Conference on Cryptology in Africa, Marrakesh, Morocco, May 7-9, 2018, Proceedings, Lecture Notes in Computer Science, vol 10831. Springer, pp 266–281, (2018) https://doi.org/10.1007/978-3-319-89339-6_15
38. Zhou, Y., van de Pol, J., Yu, Y., et al.: A third is all you need: Extended partial key exposure attack on CRT-RSA with additive exponent blinding. In: Agrawal S, Lin D (eds) Advances in Cryptology - ASIACRYPT 2022 - 28th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, December 5-9, 2022, Proceedings, Part IV, Lecture Notes in Computer Science, vol 13794. Springer, pp 508–536, (2022) https://doi.org/10.1007/978-3-031-22972-5_18