Partial Key Exposure Attack on Common Prime RSA[*]

Mengce Zheng

Zhejiang Wanli University
mengce.zheng@gmail.com

Abstract. In this paper, we focus on the common prime RSA variant and introduces a novel investigation into the partial key exposure attack targeting it. We explore the vulnerability of this RSA variant, which employs two common primes p and q defined as $p = 2ga + 1$ and $q = 2gb + 1$ for a large prime g. Previous cryptanalysis of common prime RSA has primarily focused on the small private key attack. In our work, we delve deeper into the realm of 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. To validate the effectiveness and soundness of our proposed attacks, we conduct experimental evaluations. Through these examinations, we demonstrate the validity and practicality of the proposed partial key exposure attacks on common prime RSA.

Keywords: Cryptanalysis · Common Prime RSA · Weak Key · Partial Key Exposure Attack · Lattice

1 Introduction

1.1 Background

The RSA cryptosystem, invented by Rivest, Shamir, and Adleman [RSA78], is a well-known public key encryption algorithm. Over the years, various generalizations of RSA have been proposed in the literature. These generalizations include modifications to the modulus [CHLS98, Tak98], Euler quotient [KKT95], and encryption or decryption processes [Fia97, QC82] to cater to different requirements and constraints. To address the high processing demands of RSA, several RSA variants have been introduced, such as CRT-RSA [QC82], multi-prime RSA [CHLS98], prime-power RSA [Tak98], and common prime RSA [Hin06]. 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.

[*] This work was supported by the National Natural Science Foundation of China, grant number 62002335, Ningbo Natural Science Foundation, grant number 2021J174, and Ningbo Young Science and Technology Talent Cultivation Program, grant number 2023QL007.

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 [RSA78], 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 now common to define these exponents modulo Carmichael's lambda function [EPS91], denoted as $\lambda(N) = \mathrm{lcm}(p-1, q-1)$, which is the least common multiple of $p-1$ and $q-1$. In the case of common prime RSA, a more secure variant of RSA first mentioned by Wiener [Wie90] and refined by Hinek [Hin06], the balanced primes p and q exhibit a special structure that provides resistance against small private key attacks.

Let us delve into the mathematical background of common prime RSA as proposed by Hinek [Hin06]. 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 prime and a, b are positive integers. These primes are referred to as common primes. Two 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 RSA modulus N. We provide a modified version of the common primes generation algorithm from [Hin06, Appendix A] in Algorithm 1.

Algorithm 1: Common Primes Generation

```
Input: Modulus bit-length $n$ and $\gamma$
Output: Common 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
    $p \leftarrow 2ga + 1$;
    $q \leftarrow 2gb + 1$;
    $h \leftarrow 2gab + a + b$;
end
return $p$ and $q$
```

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

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

According to Hinek's design, we have the equation

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

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. 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 security of common prime RSA has been intensively studied by several researchers [Hin06, JM06, LZPL15, ML20, SM13, Zhe24]. To achieve a tradeoff between security and efficiency, it is recommended to set $1/4 \leq \gamma < 1/2$ due to previous attacks. 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 [ML20]. These attacks exploit side channel information that may be obtained through various means, including cold boot attacks [HSH$^+$09] and other side channel analysis techniques [Koc96, RTSS09, SM12]. 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. [BDF98]. 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. Subsequently, Blömer and May [BM03] improved upon these attacks using Coppersmith's lattice-based technique [Cop97], demonstrating that RSA is vulnerable to larger public exponents e when some private key bits are exposed. Ernst et al. [EJMdW05] 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 [TK19], achieves Boneh-Durfee's bound [BD99] for small private key attacks.

Partial key exposure attacks have also been extended to other RSA variants [MNS21, YYWL22, ZvdPYS22]. 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 of the private key are leaked. We categorize these scenarios into three cases: MSB case, LSB case, and MSB-LSB 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 [Cop97].

Additionally, we employ an additional modular univariate linear equation to 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 deal with the simultaneous solution of two modular univariate linear equations. This work presents the first demonstration of partial key exposure attacks on common prime RSA.

Proposition 1. *Let $N = pq$ be a common prime RSA modulus with two balanced common 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 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*

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

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

1.3 Organization

The remainder of this paper is structured as follows. In Section 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 Section 4, we present the results of our experiments conducted to validate the effectiveness of the proposed attacks. Finally, Section 5 concludes the paper.

2 Preliminaries

We introduce the application of Coppersmith's technique [Cop96, Cop97], which is based on the LLL algorithm [LLL82]. 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 method.

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

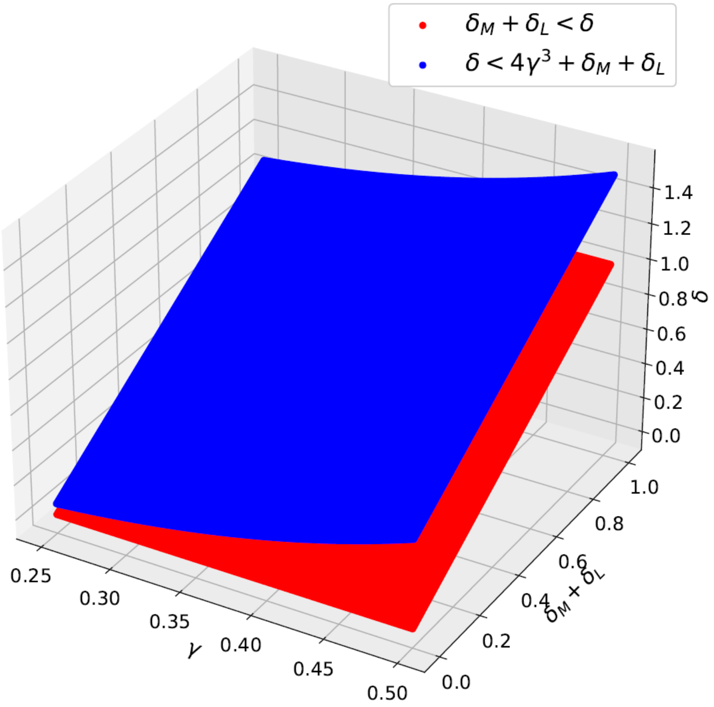

Figure 1: The illustration of partial key exposure attack on common prime RSA considering both MSBs and LSBs exposure. The vulnerable δ is located between the red surface $\delta_{\mathrm{M}} + \delta_{\mathrm{L}}$ and the blue surface $4\gamma^3 + \delta_{\mathrm{M}} + \delta_{\mathrm{L}}$ for $1/4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

on the roots. The problem is to recover roots $(x_1', \ldots, x_n')$ satisfying the above modular equation through a polynomial-time algorithm. One may refer to [JM06, May03, May10] using the lattice-based method for more details.

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

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

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 $\det(\mathcal{L}) = |\det(B)|$ 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 [LLL82] is commonly used to output approximately shortest 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 $\mathcal{L}$. The LLL algorithm outputs a reduced basis $(\vec{v}_1, \ldots, \vec{v}_w)$ satisfying*

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

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

Howgrave-Graham [How97] refined the original lattice construction and proposed a subtle lemma. Consider a 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 of $h(x_1, \ldots, x_n) = \sum a_{i_1,\ldots,i_n} x_1^{i_1} \cdots x_n^{i_n}$ 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 $\|h(x_1 X_1, \ldots, x_n X_n)\| < R/\sqrt{w}$ and $h(x_1', \ldots, x_n') \equiv 0 \pmod{R}$ 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 creation of a 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 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.

When the first ℓ reduced vectors are obtained through the LLL algorithm, the solutions can be extracted if If we obtain the first ℓ reduced vectors using the LLL algorithm, it is required that

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

to extract the solution. This condition can be simplified to $\det(\mathcal{L}) < R^w$ by disregarding the lower order terms. The common root of the resulting integer equations can be extracted by employing resultant computation or Gröbner basis computation [BWK93].

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 $f_i(x_1 X_1, \ldots, x_n X_n)$. This lattice, denoted as $\mathcal{L}$, is defined as the set of all possible integer linear combinations of these vectors. To simplify the lattice, we apply the LLL reduction 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 [Cop97, How97], there are other improved and simplified constructions available, such as those presented in [JM06, LZPL15, TK13]. In this paper, we have chosen to utilize the lattice construction proposed in [LZPL15] for our attack scenarios. This particular construction allows for the easier creation 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 extended 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 given parameters are positive integers $r_1, \ldots, r_n, r, a_1, \ldots, a_n, U$, 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 $|x'_1| \le U^{\gamma_1}, \ldots, |x'_n| \le U^{\gamma_n}$.

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 $\mathcal{F}$ for a predetermined positive integer t.

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

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

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

The modulus R involved in the above lattice-based construction is u^t. With the parameters mentioned above, we present the following lemma. For a detailed explanation, please refer to [LZPL15, Theorem 10] and its accompanying proof.

Lemma 3. *The extended simultaneous modular univariate linear equations can be solved 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* $\gamma_i \le r_i \eta$ *for* $1 \le i \le n$. *The running time is polynomial in* $\log U$ *but exponential in* n.

3 Partial Key Exposure Attack

In this section, we analyze and propose partial key exposure attacks on common prime RSA. We consider three distinct situations for the given leakage of the private key, which we refer to as the MSB case, LSB case, and MSB-LSB case. Let N be the product of two common 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 $\lambda(N) = \operatorname{lcm}(p-1, q-1) = 2gab$ is described in Section 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.

MSB-LSB Case. Given N, e and 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 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 δ_{M}, δ_{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

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

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

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 $\eta = \gamma$. Therefore, all the shift polynomials in our attack scenario are specified as

$$f_{[i_1,i_2]}(x_1,x_2) = (x_1+a_1)^{i_1}(x_2+a_2)^{i_2}\, U^{\max\{t-i_1-2i_2,0\}}$$

induced from definition 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 $\mathcal{F} = \left\{ f_{[i_1,i_2]}(x_1,x_2) : 0 \le \gamma_1 i_1 + \gamma_2 i_2 \le \gamma t \right\}$. A lattice matrix example is shown in Table 1, where other non-zero off-diagonal entries are denoted by '–'.

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

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

Following the solving strategy for extended 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 $\det(\mathcal{L}) = X_1^{s_1} X_2^{s_2} U^{s_U}$, 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 $\det(\mathcal{L}) < R^w$ 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 for simplicity to 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 can 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

$$\sqrt[n]{\frac{\gamma_1\cdots\gamma_n}{rr_1\cdots r_n}} < \eta^{\frac{n+1}{n}} \Rightarrow \gamma_1\gamma_2 < 2\gamma^3.$$

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

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

Since we deal with two simultaneous modular univariate linear equations, the running time is polynomial in $\log_2 N$. For completeness, we conclude partial key exposure attack on common prime RSA under the MSB case with the following proposition.

Proposition 2. *Let $N = pq$ be a common prime RSA modulus with two balanced common 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 $|\bar{d}| \le N^{\delta-\delta_\mathrm{M}}$. Then N can be efficiently factored in time polynomial in $\log_2 N$ if*

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

3.2 LSB Case

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 $n=2$, $r_1=1$, $r_2=2$, $r=1$, $U=N-1\simeq N$, $\eta=\gamma$. Therefore, we directly apply Lemma 3 and obtain

$$\sqrt[n]{\frac{\gamma_1\cdots\gamma_n}{rr_1\cdots r_n}}<\eta^{\frac{n+1}{n}}\Rightarrow \gamma_1\gamma_2<2\gamma^3.$$

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

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

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

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

The detailed analysis and lattice construction is similar to that of MSB case and we omit it here. For completeness, we conclude partial key exposure attack on common prime RSA under the LSB case with the following proposition.

Proposition 3. *Let $N = pq$ be a common prime RSA modulus with two balanced common 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 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*

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

3.3 MSB-LSB Case

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 $n=2$, $r_1 = 1$, $r_2 = 2$, $r=1$, $U = N-1 \simeq N$, $\eta = \gamma$. Therefore, we directly apply Lemma 3 and obtain

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

Substituting $\gamma_1 = \delta - \delta_{\mathrm{M}} - \delta_{\mathrm{L}}$ and $\gamma_2 = 1/2$, we finally 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. For completeness, we conclude partial key exposure attack on common prime RSA under the MSB-LSB case with the following proposition.

Proposition 4. *Let $N = pq$ be a common prime RSA modulus with two balanced common 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*

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

As observed, the MSB-LSB case described in Proposition 4 covers both MSB case and LSB case as two specific scenarios. More precisely, when $\delta_{\mathrm{L}} = 0$, Proposition 4 is identical to Proposition 2, and when $\delta_{\mathrm{M}} = 0$, it is identical to Proposition 3.

4 Experimental Results

To validate the validity and effectiveness of our proposed partial key exposure attacks on common prime RSA, which exploits Proposition 2, Proposition 3, and Proposition 4, 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 [The23], and the parameters for generating the common prime RSA instances were randomly chosen.

We generated a common prime RSA modulus N with $\log_2 N = 1024$ 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 $ed \equiv 1 \pmod{\operatorname{lcm}(p-1, q-1)}$. 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 Type 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 lattice settings are controlled by t, and the lattice dimension is provided in the w column. The time consumption of the LLL algorithm and the Gröbner basis computation is recorded in the Time column (measured in seconds).

Table 2: Experimental partial key exposure attacks on common prime RSA

$\log_2 N$	Type	γ	δ_{M}	δ_{L}	δ_t	δ_e	t	w	Time
1024	MSB	0.36	0.117	0	0.304	0.252	4	22	0.52 s
1024	MSB	0.40	0.127	0	0.383	0.314	4	20	0.35 s
1024	MSB	0.44	0.132	0	0.473	0.388	5	25	0.82 s
1024	MSB	0.48	0.068	0	0.511	0.422	6	31	1.53 s
1024	LSB	0.36	0	0.146	0.333	0.290	5	32	3.20 s
1024	LSB	0.40	0	0.156	0.412	0.350	5	29	0.86 s
1024	LSB	0.44	0	0.144	0.484	0.412	6	34	3.15 s
1024	LSB	0.48	0	0.125	0.567	0.479	7	41	5.57 s
1024	MSB-LSB	0.36	0.098	0.137	0.421	0.337	3	18	0.13 s
1024	MSB-LSB	0.40	0.132	0.127	0.515	0.450	5	29	1.56 s
1024	MSB-LSB	0.44	0.102	0.144	0.586	0.518	7	44	10.53 s
1024	MSB-LSB	0.48	0.144	0.165	0.751	0.691	10	72	101.46 s

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. We obtained the integer polynomial equations having a shared root by transforming the derived vectors into polynomials.

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 a partial key exposure attack on common prime RSA, utilizing Proposition 4. In this example, we consider a toy scenario where we have set $\gamma = 0.4$, and we are working with two 256-bit common primes, denoted as p and q, resulting in a composite modulus N with a bit-length of $\log_2 N = 512$.

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

$$\begin{aligned}
N &= 96612085779573789844190032734611214944237738080822481722482 6\backslash \\
&\quad 80097966648686276683063935153983163269887563643166482174781 8\backslash \\
&\quad 3954539327105043455767039958608711, \\
e &= 1154330863728081604554444040360339939327123281300782466520 48\backslash \\
&\quad 3411196573351008764265709995321 31, \\
d_M &= 700237, \\
d_L &= 856799747.
\end{aligned}$$

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

$$\begin{aligned}
a_1 &= 339435056389007461382995828393378087822726708759137592568410\backslash \\
&\quad 311579754228258366362973498272326193741451030909579746435335\backslash \\
&\quad 3007008342224368098868455268561086, \\
a_2 &= 966120857795737898441900327346112149442377380808224817224826\backslash \\
&\quad 800979666486862766830639351539831632698875636431664821747818\backslash \\
&\quad 3954539327105043455767039958608712.
\end{aligned}$$

We 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.

$$\begin{aligned}
x_1' &= 52773049414374368388105933715755 7, \\
x_2' &= -1967782802395917871498351671411072466617287473504814039126 0\backslash \\
&\quad 0015507712845340600.
\end{aligned}$$

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

$$\begin{aligned}
p &= 94005726432331417142970636651483950933949271009000242214848 2\backslash \\
&\quad 07760523437055033, \\
q &= 10277255380726037000686453048962329572777947634148116169775 1\backslash \\
&\quad 807747189408285567.
\end{aligned}$$

It can be easily verified that $N = pq$ does hold, confirming the success of applying Proposition 4 to the partial key exposure attack on common prime RSA.

5 Concluding Remarks

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 attack on common prime RSA. We present three attack propositions, each based on a distinct attack scenario: the most significant bit (MSB) case, the least significant bit (LSB) case, and the MSB-LSB case. 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, 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.

References

[BD99] Dan Boneh and Glenn Durfee. Cryptanalysis of RSA with private key d less than $N^{0.292}$. In Jacques Stern, editor, *Advances in Cryptology - EUROCRYPT '99, International Conference on the Theory and Application of Cryptographic Techniques, Prague, Czech Republic, May 2-6, 1999, Proceeding*, volume 1592 of *Lecture Notes in Computer Science*, pages 1–11. Springer, 1999.

[BDF98] Dan Boneh, Glenn Durfee, and Yair Frankel. An attack on RSA given a small fraction of the private key bits. In Kazuo Ohta and Dingyi Pei, editors, *Advances in Cryptology - ASIACRYPT '98, International Conference on the Theory and Applications of Cryptology and Information Security, Beijing, China, October 18-22, 1998, Proceedings*, volume 1514 of *Lecture Notes in Computer Science*, pages 25–34. Springer, 1998.

[BM03] Johannes Blömer and Alexander May. New partial key exposure attacks on RSA. In Dan Boneh, editor, *Advances in Cryptology - CRYPTO 2003, 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings*, volume 2729 of *Lecture Notes in Computer Science*, pages 27–43. Springer, 2003.

[BWK93] Thomas Becker, Volker Weispfenning, and Heinz Kredel. *Gröbner bases - a computational approach to commutative algebra*, volume 141 of *Graduate texts in mathematics.* Springer, 1993.

[CHLS98] Thomas Collins, Dale Hopkins, Susan Langford, and Michael Sabin. Public key cryptographic apparatus and method, dec 1998. U.S. Patent 5848159.

[Cop96] Don Coppersmith. Finding a small root of a univariate modular equation. In Ueli M. Maurer, editor, *Advances in Cryptology - EUROCRYPT '96, International Conference on the Theory and Application of Cryptographic Techniques, Saragossa, Spain, May 12-16, 1996, Proceeding*, volume 1070 of *Lecture Notes in Computer Science*, pages 155–165. Springer, 1996.

[Cop97] Don Coppersmith. Small solutions to polynomial equations, and low exponent RSA vulnerabilities. *J. Cryptol.*, 10(4):233–260, 1997.

[EJMdW05] Matthias Ernst, Ellen Jochemsz, Alexander May, and Benne de Weger. Partial key exposure attacks on RSA up to full size exponents. In Ronald Cramer, editor, *Advances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005, Proceedings*, volume 3494 of *Lecture Notes in Computer Science*, pages 371–386. Springer, 2005.

[EPS91] Paul Erdos, Carl Pomerance, and Eric Schmutz. Carmichael's lambda function. *Acta Arith*, 58(4):363–385, 1991.

[Fia97] Amos Fiat. Batch RSA. *J. Cryptol.*, 10(2):75–88, 1997.

[Hin06] M. Jason Hinek. Another look at small RSA exponents. In David Pointcheval, editor, *Topics in Cryptology - CT-RSA 2006, The Cryptographers' Track at the RSA Conference 2006, San Jose, CA, USA, February 13-17, 2006, Proceedings*, volume 3860 of *Lecture Notes in Computer Science*, pages 82–98. Springer, 2006.

[How97] Nick Howgrave-Graham. Finding small roots of univariate modular equations revisited. In Michael Darnell, editor, *Cryptography and Coding, 6th IMA International Conference, Cirencester, UK, December 17-19, 1997, Proceedings*, volume 1355 of *Lecture Notes in Computer Science*, pages 131–142. Springer, 1997.

[HSH$^+$09] J. Alex Halderman, Seth D. Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A. Calandrino, Ariel J. Feldman, Jacob Appelbaum, and Edward W. Felten. Lest we remember: cold-boot attacks on encryption keys. *Commun. ACM*, 52(5):91–98, 2009.

[JM06] Ellen Jochemsz and Alexander May. A strategy for finding roots of multivariate polynomials with new applications in attacking RSA variants. In Xuejia Lai and Kefei Chen, editors, *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*, volume 4284 of *Lecture Notes in Computer Science*, pages 267–282. Springer, 2006.

[KKT95] Hidenori Kuwakado, Kenji Koyama, and Yukio Tsuruoka. New RSA-type scheme based on singular cubic curves $y^2 \equiv x^3 + bx^2 \pmod{n}$.

IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, E78-A(1):27–33, 1995.

[Koc96] Paul C. Kocher. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In Neal Koblitz, editor, *Advances in Cryptology - CRYPTO '96, 16th Annual International Cryptology Conference, Santa Barbara, California, USA, August 18-22, 1996, Proceedings*, volume 1109 of *Lecture Notes in Computer Science*, pages 104–113. Springer, 1996.

[LLL82] Arjen Klaas Lenstra, Hendrik Willem Lenstra, and László Lovász. Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261(4):515–534, 1982.

[LZPL15] Yao Lu, Rui Zhang, Liqiang Peng, and Dongdai Lin. Solving linear equations modulo unknown divisors: Revisited. In Tetsu Iwata and Jung Hee Cheon, editors, *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*, volume 9452 of *Lecture Notes in Computer Science*, pages 189–213. Springer, 2015.

[May03] Alexander May. *New RSA vulnerabilities using lattice reduction methods.* PhD thesis, University of Paderborn, 2003.

[May10] Alexander May. Using LLL-reduction for solving RSA and factorization problems. In Phong Q. Nguyen and Brigitte Vallée, editors, *The LLL Algorithm - Survey and Applications*, Information Security and Cryptography, pages 315–348. Springer, 2010.

[ML20] Majid Mumtaz and Ping Luo. Remarks on the cryptanalysis of common prime RSA for IoT constrained low power devices. *Inf. Sci.*, 538:54–68, 2020.

[MNS21] Alexander May, Julian Nowakowski, and Santanu Sarkar. Partial key exposure attack on short secret exponent CRT-RSA. In Mehdi Tibouchi and Huaxiong Wang, editors, *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*, volume 13090 of *Lecture Notes in Computer Science*, pages 99–129. Springer, 2021.

[QC82] J.-J. Quisquater and C. Couvreur. Fast decipherment algorithm for RSA public-key cryptosystem. *Electronics Letters*, 18(21):905–907, 1982.

[RSA78] Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21(2):120–126, 1978.

[RTSS09] Thomas Ristenpart, Eran Tromer, Hovav Shacham, and Stefan Savage. Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. In Ehab Al-Shaer, Somesh Jha, and Angelos D. Keromytis, editors, *Proceedings of the 2009 ACM Conference on Computer and Communications Security, CCS 2009, Chicago, Illinois, USA, November 9-13, 2009*, pages 199–212. ACM, 2009.

[SM12] Santanu Sarkar and Subhamoy Maitra. Side channel attack to actual cryptanalysis: Breaking CRT-RSA with low weight decryption exponents. In Emmanuel Prouff and Patrick Schaumont, editors, *Cryptographic Hardware and Embedded Systems - CHES 2012 - 14th International Workshop, Leuven, Belgium, September 9-12, 2012. Proceedings*, volume 7428 of *Lecture Notes in Computer Science*, pages 476–493. Springer, 2012.

[SM13] Santanu Sarkar and Subhamoy Maitra. Cryptanalytic results on 'dual CRT' and 'common prime' RSA. *Des. Codes Cryptogr.*, 66(1-3):157–174, 2013.

[Tak98] Tsuyoshi Takagi. Fast RSA-type cryptosystem modulo $p^k q$. In Hugo Krawczyk, editor, *Advances in Cryptology - CRYPTO '98, 18th Annual International Cryptology Conference, Santa Barbara, California, USA, August 23-27, 1998, Proceedings*, volume 1462 of *Lecture Notes in Computer Science*, pages 318–326. Springer, 1998.

[The23] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.5)*, 2023. https://www.sagemath.org.

[TK13] Atsushi Takayasu and Noboru Kunihiro. Better lattice constructions for solving multivariate linear equations modulo unknown divisors. In Colin Boyd and Leonie Simpson, editors, *Information Security and Privacy - 18th Australasian Conference, ACISP 2013, Brisbane, Australia, July 1-3, 2013. Proceedings*, volume 7959 of *Lecture Notes in Computer Science*, pages 118–135. Springer, 2013.

[TK19] Atsushi Takayasu and Noboru Kunihiro. Partial key exposure attacks on RSA: achieving the Boneh-Durfee bound. *Theor. Comput. Sci.*, 761:51–77, 2019.

[Wie90] Michael J. Wiener. Cryptanalysis of short RSA secret exponents. *IEEE Trans. Inf. Theory*, 36(3):553–558, 1990.

[YYWL22] Simeng Yuan, Wei Yu, Kunpeng Wang, and Xiuxiu Li. 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*, pages 1436–1440. IEEE, 2022.

[Zhe24] Mengce Zheng. Revisiting small private key attacks on common prime rsa. *IEEE Access*, 12:5203–5211, 2024.

[ZvdPYS22] Yuanyuan Zhou, Joop van de Pol, Yu Yu, and François-Xavier Standaert. A third is all you need: Extended partial key exposure attack on CRT-RSA with additive exponent blinding. In Shweta Agrawal and Dongdai Lin, editors, *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*, volume 13794 of *Lecture Notes in Computer Science*, pages 508–536. Springer, 2022.