Higher Residuosity Attacks on Small RSA Subgroup Decision Problems

Xiaopeng Zhao$^{1(\boxtimes)[0009-0004-1838-6471]}$, Zhenfu Cao$^{2[0000-0002-5250-5030]}$,
Xiaolei Dong[2], and Zhusen Liu$^{3[0000-0001-7441-2954]}$

[1] School of Computer Science and Technology, Donghua University, 201620,
Shanghai, China
zxp@dhu.edu.cn

[2] Department of Cryptography and Cyber Security, East China Normal University,
200062, Shanghai, China
{zfcao,dongxiaolei}@sei.ecnu.edu.cn

[3] Hangzhou Innovation Institute of Beihang University, Hangzhou, 311121, Zhejiang,
China
zhusen_liu@163.com

Abstract. Secure two-party comparison, known as Yao's millionaires' problem, has been a fundamental challenge in privacy-preserving computation. It enables two parties to compare their inputs without revealing the exact values of those inputs or relying on any trusted third party. One elegant approach to secure computation is based on homomorphic encryption. Recently, building on this approach, Carlton et al. (CT-RSA 2018) and Bourse et al. (CT-RSA 2020) presented novel solutions for the problem of secure integer comparison. These protocols have demonstrated significantly improved performance compared to the well-known and frequently used DGK protocol (ACISP 2007 and Int. J. Appl. Cryptogr. **1**(4),323–324, 2009). In this paper, we introduce a class of higher residuosity attacks, which can be regarded as an extension of the classical quadratic residuosity attack on the decisional Diffie-Hellman problem. We demonstrate that the small RSA subgroup decision problems, upon which both the CEK and BST protocols are based, are not difficult to solve when the prime base p_0 is small (e.g., $p_0 < 100$). Under these conditions, the protocols achieve optimal overall performance. Furthermore, we offer recommendations for precluding such attacks, including one approach that does not adversely affect performance. We hope that these attacks can be applied to analyze other number-theoretic hardness assumptions.

Keywords: Secure two-party comparison · Small RSA subgroup decision problem · Higher residuosity attacks.

1 Introduction

Secure two-party comparison, known as Yao's millionaires' problem [33], has been a fundamental challenge in privacy-preserving computation. The traditional solution to this problem is based on Yao's Garbled Circuit [33]. In Yao's protocol, two parties use their bitwise representations of private inputs to securely evaluate a comparison function, which is represented as a Boolean circuit, in the presence of semi-honest adversaries. However, the memory, energy, and communication costs associated with garbled circuit evaluation protocols are substantial.

Another significant approach to secure computation is based on homomorphic encryption. This method is typically less computationally efficient than protocols utilizing garbled circuits; however, it is more straightforward to implement and incurs a lower overall communication cost. Fischlin [13] first constructed a secure comparison of two numbers using a Boolean circuit based on the XOR-homomorphic Goldwasser-Micali cryptosystem [15]. Other notable examples of secure Boolean evaluation of bitwise encryption of integers include the schemes developed by Blake and Kolesnikov [2], Garay et al. [14] and Lin and Tzeng [25]. Later, Damgård, Geisler, and Krøigaard (DGK) enhanced this approach in [11,12]. Drawing inspiration from the strong RSA subgroup assumption (related to high residuosity assumptions) proposed by Groth in [16] as well as the DGK comparison protocol in [11,12], Carlton et al. [8] employed an *RSA quintuple* (see Definition 1) as a public key in their encryption scheme. Notably, they discovered that the encryption possesses a *threshold* (scalar) homomorphic property. Leveraging this property, they constructed a protocol (termed the CEK protocol) that efficiently compares two encrypted integers through the (nearly) direct application of the homomorphism on a single encrypted value. Following a similar approach, Bourse et al. [4] improved the CEK protocol (termed the BST protocol) by avoiding one round induced by the plaintext equality test. Both the CEK and BST protocols have been proven to be secure under the small RSA subgroup decision problems. Performance results indicate that they are several times faster than the DGK protocol.

However, we will demonstrate that the small RSA subgroup decision problems are not difficult to solve when the public prime base p_0 is small (e.g., $p_0 < 100$), in which case both the CEK and BST protocols achieve optimal overall performance. The small RSA subgroup decision problems involve an RSA quintuple that contains an RSA modulus $N = pq$ such that $p = 2p_0^d p_s p_t + 1$ and $q = 2p_0^d q_s q_t + 1$ where p_s, q_s, p_t, q_t are pairwise distinct primes, d is an integer greater than 1. Our attacks on them mainly utilize the leakage of an element of order p_0 in $\mathbb{Z}_N^*$, in which case a partial decomposition of N in the algebraic integer ring $\mathbb{Z}[\zeta_{p_0}]$ can be easily computed. Consequently, higher residuosity attacks that leverage power residue symbols naturally arise from this leakage, even though the classical quadratic residuosity attack[4] does not work. Since both protocols reveal an RSA quintuple as part of the public key, we can similarly present practical higher residuosity attacks against them (see Section 5). Furthermore, we provide recommendations for precluding such attacks, including one approach that does not adversely affect their performance.

[4] Because of this attack the decisional Diffie-Hellman problem in the group $\mathbb{Z}_p^*$ is not hard.

The rest of this paper is organized as follows. Section 2 introduces the background knowledge on small RSA subgroup decision problems. In Section 3, we provide a detailed quartic residuosity attack on these problems with $p_0 = 2$. Section 4 presents a higher residuosity attack on these problems when p_0 is an odd prime. In Section 5, we discuss practical higher residuosity attacks on the CEK and BST protocols and offer recommendations for precluding such attacks. Finally, conclusions are drawn in Section 6.

2 Preliminaries

2.1 Notations

For the sake of clarity, Table 1 summarizes the frequently used notations in this paper.

Table 1. Frequently Used Notations

$\mathbb{Z}, \mathbb{Q}$	the integers, the rational numbers
$\mathbb{N}^+$	the set of positive integers
$\mathbb{C}$	the complex numbers
K	a number field
$\mathcal{O}_K$	the ring of integers in a number field K
$\mathfrak{a}, \mathfrak{b}, \ldots$	the ideals in $\mathcal{O}_K$
$\mathbb{Z}_n$	$= \{0, 1, \ldots, n-1\}$ integers mod n
$\mathbb{Z}_n^*$	$= \{b \in \mathbb{Z}_n \mid \gcd(b, N) = 1\}$ multiplicative group mod n
$\mathbb{F}_p$	$= \mathbb{Z}/p\mathbb{Z}$ the field of p elements for a prime p
$R^\times$	the unit group of the multiplicative monoid of a ring R
ζ_n	a primitive n^{th} root of unity, i.e., $\zeta_n = e^{2\pi \mathrm{i}/n}$
i	the imaginary unit, i.e., $\mathrm{i} = \zeta_4$
$a \mid b$	a divides b
$\langle X \rangle$	the group generated by a set X
$(a, b, \ldots)$	the ideal generated by $a, b, \ldots$
$\gcd(a, b)$	the greatest commom divisor of a, b
$a \equiv b \pmod{\mathfrak{D}}$	the relation $a - b \in \mathfrak{D}$, where elements $a, b \in \mathcal{O}_K$
$\varphi(n)$	the number of elements in $\mathbb{Z}_n^*$
log	the binary logarithm
$\lvert A \rvert$	the number of elements of a set A
$\mathcal{N}(\alpha)$	the norm of $\alpha \in \mathbb{Z}[\zeta_n]$ given by $\mathcal{N}(\alpha) = \prod_{k \in \mathbb{Z}_n^*} \sigma_k(\alpha)$ where $\sigma_k : \zeta_n \mapsto \zeta_n^k$
$\mathcal{N}(\mathfrak{a})$	$= \lvert \mathcal{O}_K / \mathfrak{a} \rvert$
$(\frac{\cdot}{\cdot})$	the Jacobi symbol
$\mathcal{QR}_n$	$= \{x^2 : x \in \mathbb{Z}_n^*\}$ the set of quadratic residues in the group $\mathbb{Z}_n^*$
PPT	probabilistic polynomial time
O	the big-oh notation
$\mathscr{D}$	a distinguisher, possibly a probabilistic one

2.2 Small RSA Subgroup Decision Problems

In this section, we will first briefly review the small RSA subgroup decision problems as defined in [8, Definition 2] and in [4, Definition 2], respectively, and then we will discuss the close relationship between them. The following definition is drawn from [8, Definition 1] and [4, Section 3.1].

Definition 1. *An* RSA quintuple *is a quintuple* (N, p_0, d, g, u) *where:*

1. *u is an integer such that the Discrete Logarithm Problem is computationally infeasible in a subgroup of $\mathbb{Z}_N^*$ whose order is a prime of bit-length u;*
2. *p_0 is a prime of bit-length less than u;*
3. *d is an integer greater than 1;*
4. *$N = pq$ is a composite integer with computationally infeasible factorization, where the primes p and q are constructed as:*

$$p = 2p_0^d p_s p_t + 1 \quad \textit{and} \quad q = 2p_0^d q_s q_t + 1,$$

   satisfying the following conditions:
   - *p_s and q_s are primes of bit-length u;*
   - *p_t and q_t are primes with bit-length different from u;*
   - *p_s, q_s, p_t, q_t are pairwise distinct;*
5. *g is an element in $\mathbb{Z}_N^*$ which has order p_0^d modulo p and modulo q.*

Remark 1. We slightly modify the condition *5* for security purposes. The original definition only requires g to be of order p_0^d in $\mathbb{Z}_N^*$, whereas this might lead to the leakage of the factorization of N since both g and its order are public: consider the case where g has order p_0^d in $\mathbb{Z}_p^*$ but has order $p_0^{d'}$ for some integer $d' < d$ in $\mathbb{Z}_q^*$, then g would have the correct order p_0^d in $\mathbb{Z}_N^*$, thus $\gcd(g^{p_0^{d-1}} - 1, N)$ would immediately give a factor of N.

The BST and CEK protocols have been proven secure, relying on the hardness of the Small RSA Subgroup Decision Problem SRSDP and $\widetilde{\mathsf{SRSDP}}$, respectively. These two problems are defined as follows.

Definition 2 (Small RSA Subgroup Decision Problem [4] (SRSDP)). *Given an RSA quintuple (N, p_0, d, g, u), distinguish the two uniform distributions over $\mathcal{QR}_N$ and over $\{x^{p_0^d p_t q_t} \mid x \in \mathcal{QR}_N\}$, respectively.*

Definition 3 (Small RSA Subgroup Decision Problem [8] ($\widetilde{\mathsf{SRSDP}}$)). *Given an RSA quintuple (N, p_0, d, g, u), distinguish the two uniform distributions over $\mathcal{QR}_N$ and over $\{x \in \mathcal{QR}_N \mid x$ has order $p_s q_s$ in $\mathbb{Z}_N^*\}$, respectively.*

Definition 4 (Advantage for Solving the SRSDP). *Given an instance $\mathcal{I} = \{(N, p_0, d, g, u), x\}$ of SRSDP, where x is sampled according to one of the two distributions stated in Definition 2, the advantage of a distinguisher $\mathscr{D}$ for solving the SRSDP (being able to correctly guess the target) is defined as*

$$\begin{aligned} \mathsf{Adv}_{\mathscr{D},\mathcal{I}}^{\mathsf{SRSDP}} &= \Pr[\mathscr{D}(\mathcal{I}) \textit{ outputs “yes”} \mid {}_{\substack{x \textit{ is of the form } y^{p_0^d p_t q_t} \\ \textit{with } y \in \mathcal{QR}_N}}] - \frac{1}{2} \\ &\quad + \Pr[\mathscr{D}(\mathcal{I}) \textit{ outputs “no”} \mid x \in \mathcal{QR}_N] - \frac{1}{2} \end{aligned}$$

Remark 2. According to the probabilistic definition of $\mathsf{Adv}^{\mathsf{SRSDP}}_{\mathscr{D},\mathcal{I}}$, a perfect distinguisher would not have an advantage of 1.

The advantage for solving the $\widetilde{\mathsf{SRSDP}}$ can be defined analogously. Theorem 1 is crucial to reveal the close relationship between the SRSDP and the $\widetilde{\mathsf{SRSDP}}$.

Theorem 1. *Given an RSA quintuple (N, p_0, d, g, u) and $x \in \mathcal{QR}_N$, if x has order $p_s q_s$ in $\mathbb{Z}_N^*$, then x can be written in the form $y^{p_0^d p_t q_t}$ for some $y \in \mathcal{QR}_N$.*

Proof. Suppose that x has order $p_s q_s$ in $\mathbb{Z}_N^*$. Then x must have order p_s in $\mathbb{Z}_p^*$ and order q_s in $\mathbb{Z}_q^*$. Let g_p and g_q be primitive roots modulo p and q, respectively. Then x can be written as $x \equiv g_p^{2p_0^d p_t a} \pmod{p}$ and $x \equiv g_q^{2p_0^d q_t b} \pmod{q}$ with $p_s \nmid a$ and $q_s \nmid b$. Let $y \in \mathcal{QR}_N$ be such that $y \equiv g_p^{2\ell} \pmod{p}$ and $y \equiv g_q^{2\ell'} \pmod{q}$ where $q_t \ell \equiv a \pmod{p_s}$ and $p_t \ell' \equiv b \pmod{q_s}$. Thus, x can be written as $x = y^{p_0^d p_t q_t}$ in $\mathbb{Z}_N^*$. □

Remark 3. It follows quite easily that a counterexample to the reverse direction is $y = 1$. Let

$$H = \{x \in \mathcal{QR}_N \mid x \text{ has order } p_s q_s \text{ in } \mathbb{Z}_N^*\},$$
$$G = \{x \in \mathcal{QR}_N \mid x \text{ is of the form } y^{p_0^d p_t q_t} \text{ with } y \in \mathcal{QR}_N\}.$$

By the proof of Theorem 1 we can see that

$$|H| = (p_s - 1)(q_s - 1) \text{ and } |G| = p_s q_s.$$

Remark 4. Let $||n||$ denote the bit-length of the integer n. Since the SRSDP problem operates on the group G whose order is $p_s q_s$ and $u = ||p_s|| = ||q_s||$, u should define a length for which computing the discrete logarithm in a group of prime u-bit order is infeasible. Therefore, working at the 128-bit security level requires $||N|| = 3072$, $u = 256$; The 192-bit security level requires $||N|| = 7680$, $u = 384$ and the 256-bit security level requires $||N|| = 15360$, $u = 512$.

Theorem 2 below shows that if there exists a PPT distinguisher being able to solve the SRSDP with light advantage then one can solve the $\widetilde{\mathsf{SRSDP}}$ in polynomial time with non-negligible advantage. Therefore, we next focus mainly on investigating the hardness of the SRSDP. We remark that all of the attacks described in the following sections have advantages of at least 1/2.

Theorem 2. *Let $\mathscr{D}$ be a PPT distinguisher being able to solve the SRSDP with*

$$\mathsf{Adv}^{\mathit{SRSDP}}_{\mathscr{D},\mathcal{I}} - \frac{(p_s + q_s - 1)}{p_s q_s}$$

non-negligible. Then given an RSA quintuple (N, p_0, d, g, u), there exists a PPT distinguisher $\mathscr{D}'$ being able to solve the $\widetilde{SRSDP}$, i.e., distinguish whether a random element in $\mathcal{QR}_N$ has order $p_s q_s$ in $\mathbb{Z}_N^*$ with non-negligible advantage.

Proof. We construct $\mathscr{D}'$ that takes an RSA quintuple and $x \in \mathcal{QR}_N$ as input, and whose goal is to determine whether x has order $p_s q_s$ in $\mathbb{Z}_N^*$:

```
Distinguisher $\mathscr{D}'$: $\mathscr{D}'$ is given as input an RSA quintuple $(N, p_0, d, g, u)$ and $x \in \mathcal{QR}_N$.
1: Construct an instance $\mathcal{I} = \{(N, p_0, d, g, u), x\}$ and run $\mathscr{D}(\mathcal{I})$ to obtain an output string $w$.
2: Output $w$.
```

$\mathscr{D}'$ clearly runs in polynomial time because $\mathscr{D}$ does. By Theorem 1 and Remark 3, we see that $H \subset G$ and the advantage of $\mathscr{D}'$ is given by

$$\begin{aligned}
\mathsf{Adv}^{\widetilde{\mathsf{SRSDP}}}_{\mathscr{D}',\mathcal{I}} &= \Pr[\mathscr{D}'(\mathcal{I}) \text{ outputs “yes”} \mid x \in H] + \Pr[\mathscr{D}'(\mathcal{I}) \text{ outputs “no”} \mid x \in \mathcal{QR}_N] - 1 \\
&\geq \Pr[\mathscr{D}(\mathcal{I}) \text{ outputs “yes”} \mid x \in G] - \frac{|G| - |H|}{|G|} \\
&\qquad\qquad\qquad + \Pr[\mathscr{D}(\mathcal{I}) \text{ outputs “no”} \mid x \in \mathcal{QR}_N] - 1 \\
&= \mathsf{Adv}^{\mathsf{SRSDP}}_{\mathscr{D},\mathcal{I}} - \frac{p_s + q_s - 1}{p_s q_s},
\end{aligned}$$

which is non-negligible under the assumption in the theorem. □

3 A Quartic Residuosity Attack on the SRSDP when $p_0 = 2$

Carlton et al. [8] suggested to take $p_0 = 2$ in the CEK protocol for efficiently computing a discrete logarithm in the cyclic group generated by g. The BST protocol also achieves the best performance in this case. However, in this section, we shall show that the SRSDP with $p_0 = 2$ can be efficiently solved with advantage $1/2$ by using quartic residuosity.

3.1 The Quartic Jacobi Symbol

We start with the elementary results concerning the ring of *Gaussian integers* $\mathbb{Z}[\mathrm{i}]$. It is a Euclidean Domain and $\mathbb{Z}[\mathrm{i}]^\times = \langle \mathrm{i} \rangle$. For every prime element $\pi = a + b\mathrm{i} \in \mathbb{Z}[\mathrm{i}]$, the norm of π is given by $\mathcal{N}(\pi) = \pi\overline{\pi} = a^2 + b^2$; there is a unique prime $p \in \pi\mathbb{Z}[\mathrm{i}]$ such that $\pi\mathbb{Z}[\mathrm{i}] \cap \mathbb{Z} = p\mathbb{Z}$, and if $p \equiv 1 \bmod 4$ then $p = \pi\overline{\pi}$. The residue class ring $\mathbb{Z}[\mathrm{i}]/\pi\mathbb{Z}[\mathrm{i}]$ is a finite field with $\mathcal{N}(\pi)$ elements. In particular, $(\mathbb{Z}[\mathrm{i}]/\pi\mathbb{Z}[\mathrm{i}])^\times$ is a cyclic group of order $\mathcal{N}(\pi) - 1$. An element $\alpha \in \mathbb{Z}[\mathrm{i}]$ is called *primary* if $\alpha \equiv 1 \bmod (1 + \mathrm{i})^3$. If $\alpha \notin (1 + \mathrm{i})\mathbb{Z}[\mathrm{i}]$, then there exists a unique $u \in \mathbb{Z}[\mathrm{i}]^\times$ such that $u\alpha$ is primary.

Let $\pi \in \mathbb{Z}[\mathrm{i}] \setminus (1 + \mathrm{i})\mathbb{Z}[\mathrm{i}]$ be a prime element. Then there exists a unique character $\chi_\pi : (\mathbb{Z}[\mathrm{i}]/\pi\mathbb{Z}[\mathrm{i}])^\times \mapsto \mathbb{C}^\times$ of order 4 such that

$$\chi_\pi(\xi) + \pi\mathbb{Z}[\mathrm{i}] = \xi^{\frac{\mathcal{N}(\pi)-1}{4}} \quad \text{for all} \quad \xi \in (\mathbb{Z}[\mathrm{i}]/\pi\mathbb{Z}[\mathrm{i}])^\times .$$

For $\alpha \in \mathbb{Z}[\mathrm{i}]$, we define the *quartic residue symbol* of α modulo π by

$$\left(\frac{\alpha}{\pi}\right)_4 = \begin{cases} 0, & \text{if } \pi \mid \alpha; \\ \chi_\pi(\alpha + \pi\mathbb{Z}[\mathrm{i}]) \in \{\pm 1, \pm \mathrm{i}\}, & \text{if } \pi \nmid \alpha. \end{cases}$$

Suppose that $\beta = \epsilon\pi_1 \cdots \pi_r \in \mathbb{Z}[\mathrm{i}] \setminus (1+\mathrm{i})\mathbb{Z}[\mathrm{i}]$, where $r \in \mathbb{N}^+$, $\epsilon \in \mathbb{Z}[\mathrm{i}]^\times$ and $\pi_1, \ldots, \pi_r \in \mathbb{Z}[\mathrm{i}] \setminus (1+\mathrm{i})\mathbb{Z}[\mathrm{i}]$ are prime elements. For $\alpha \in \mathbb{Z}[\mathrm{i}]$, the *quartic Jacobi symbol* $\left(\frac{\alpha}{\beta}\right)_4$ is defined by

$$\left(\frac{\alpha}{\beta}\right)_4 = \prod_{j=1}^{r} \left(\frac{\alpha}{\pi_j}\right)_4.$$

Theorem 3 below is known as the *general quartic reciprocity law* in $\mathbb{Z}[\mathrm{i}]$. Equation (1) was proposed by Gauss and later proved by Jacobi and Eisenstein. This theorem together with its supplement deals with the beautiful relations that exist among quartic Jacobi symbols and gives an efficient method for computation (see Algorithm 1 and Table 3). We refer the reader to [19, Chapter 9] and [17, Chapter 7] for more details.

Theorem 3 (Quartic Reciprocity Law [17, Theorem 7.4.7]). *Let $\alpha, \beta \in \mathbb{Z}[\mathrm{i}] \setminus (1+\mathrm{i})\mathbb{Z}[\mathrm{i}]$ be such that $\gcd(\alpha, \beta) = 1$, $\alpha = a + bi$ and $\beta = c + di$, where $a, b, c, d \in \mathbb{Z}$.*

1. *(Jacobi, Kaplan) If $a \equiv c \equiv 1 \pmod 4$ and $b \equiv d \equiv 0 \pmod 2$, then*

$$\left(\frac{\alpha}{\beta}\right)_4 = \left(\frac{\beta}{\alpha}\right)_4 (-1)^{bd/4}.$$

2. *(Gauss, Eisenstein) If α and β are both primary, then*

$$\begin{aligned} \left(\frac{\alpha}{\beta}\right)_4 &= \left(\frac{\beta}{\alpha}\right)_4 (-1)^{bd/4} = \left(\frac{\beta}{\alpha}\right)_4 (-1)^{\frac{a-1}{2}\frac{c-1}{2}} \\ &= \left(\frac{\beta}{\alpha}\right)_4 (-1)^{\frac{\mathcal{N}(\alpha)-1}{4}\frac{\mathcal{N}(\beta)-1}{4}}. \end{aligned} \tag{1}$$

Theorem 4 (Supplement to the Quartic Reciprocity Law [17, Theorem 7.4.8]). *Suppose that $a, b \in \mathbb{Z}$ and $\beta = a + bi \in \mathbb{Z}[\mathrm{i}]$. Then*

$$\left(\frac{-1}{\beta}\right)_4 = (-1)^{b/2} \quad \textit{if} \quad \beta \equiv 1 \pmod 2,$$

and if β is primary,

$$\left(\frac{\mathrm{i}}{\beta}\right)_4 = \mathrm{i}^{(1-a)/2} \quad \textit{and} \quad \left(\frac{1+\mathrm{i}}{\beta}\right)_4 = \mathrm{i}^{(a-b-b^2-1)/4}.$$

3.2 Computing the GCD and the Quartic Jacobi Symbol in $\mathbb{Z}[\mathrm{i}]$

Since $\mathbb{Z}[\mathrm{i}]$ is Euclidean and, by [19, Proposition 1.4.1], it allows a *Euclidean Algorithm* for computing $\gcd(a,b)$ for every $a, b \in \mathbb{Z}[\mathrm{i}]$, $b \neq 0$: by successive "divisions" (actually in $\mathbb{Q}(\mathrm{i})$) we can write:

$$\begin{aligned}
a &= q_0 b + r_1 & \mathcal{N}(r_1) &\leq \frac{1}{2}\mathcal{N}(b),\\
b &= q_1 r_1 + r_2 & \mathcal{N}(r_2) &\leq \frac{1}{2}\mathcal{N}(r_1),\\
r_1 &= q_2 r_2 + r_3 & \mathcal{N}(r_3) &\leq \frac{1}{2}\mathcal{N}(r_2),\\
&\vdots\\
r_{n-1} &= q_n r_n + r_{n+1} & \mathcal{N}(r_{n+1}) &= 0.
\end{aligned}$$

Then after a finite number of steps there must exist n such that $r_{n+1} = 0$ and hence $r_n = \gcd(a,b)$. This is because $0 = \mathcal{N}(r_{n+1}) < 1 \leq \mathcal{N}(r_n) \leq 1/2\mathcal{N}(r_{n-1}) \leq \ldots \leq 1/2^n\mathcal{N}(b)$ and $\mathcal{N}(b)$ is finite. As $n \leq \lceil \log \mathcal{N}(b) \rceil$, it follows that $\gcd(a,b)$ can be computed in time $O\left((\log \mathcal{N}(ab))^3\right)$ by means of the Euclidean Algorithm in $\mathbb{Z}[\mathrm{i}]$. In [10], Dåmgard et al. presented more efficient algorithms for computing the GCD and cubic (resp. quartic) residuosity in the ring of Eisenstein (resp. Gaussian) integers, which only take time $O\left((\log \mathcal{N}(ab))^2\right)$ and can be seen as generalisations of the binary integer GCD and derived Jacobi symbol algorithms.

Knowing Theorem 3 and Theorem 4, it is easy to obtain Algorithm 1 for computing the quartic Jacobi symbol. Note that β is primary in each iteration. The algorithm terminates since $\mathcal{N}(\beta)$ is strictly decreasing in each iteration of the **while** loop. Upon termination, it is clear that $\beta = 1$, and thus c is the desired result since it is deduced from Theorem 3 and Theorem 4. Using the complexity analysis of the GCD algorithm, it can likewise be shown that Algorithm 1 also takes $O\left((\log \mathcal{N}(\alpha\beta))^3\right)$ time to compute $\left(\frac{\alpha}{\beta}\right)_4$. By virtue of a connection between the quartic residue symbol and the Hilbert symbol, Weilert [31] described a fast algorithm for the computation of the quartic residue symbol, whose running time is $O\left(n(\log n)^2 \log\log n\right)$ for Gaussian integers bounded by 2^n in the norm.

3.3 Attacking the SRSDP via the Quartic Jacobi Symbol

With the preparation for the quartic Jacobi symbol in $\mathbb{Z}[\mathrm{i}]$, attacks on the SRSDP with $p_0 = 2$ are possible. Given an RSA quintuple $(N, p_0 := 2, d, g, u)$ and a sample $x \in \mathcal{QR}_N$, $\mathscr{D}$ first computes $h = g^{p_0^d/4} \bmod N$, whose order is 4 in both $\mathbb{Z}_p^*$ and $\mathbb{Z}_q^*$. Then it computes $\rho = \gcd(N, h - \mathrm{i})$ by the Euclidean Algorithm in $\mathbb{Z}[\mathrm{i}]$. Let $p = \pi\overline{\pi}$, $q = \lambda\overline{\lambda}$ for some prime elements $\pi, \lambda \in \mathbb{Z}[\mathrm{i}]$. We see that $h^2 \equiv -1 \bmod N$ and $\pi\overline{\pi} \mid (h+\mathrm{i})(h-\mathrm{i})$, $\lambda\overline{\lambda} \mid (h+\mathrm{i})(h-\mathrm{i})$. Since $\pi, \overline{\pi}, \lambda, \overline{\lambda}$ are prime elements and $p = \pi\overline{\pi} \nmid h + \mathrm{i}$, it follows that one of π or $\overline{\pi}$ (resp. one of λ

Algorithm 1: Compute the quartic Jacobi symbol in $\mathbb{Z}[\mathrm{i}]$

```
Input: $\alpha \in \mathbb{Z}[\mathrm{i}]$, $\beta \in \mathbb{Z}[\mathrm{i}] \setminus (1+\mathrm{i})\mathbb{Z}[\mathrm{i}]$
Output: $c = \left(\frac{\alpha}{\beta}\right)_4$
$c = 1$
Let primary $\gamma$ be defined by $\beta = \mathrm{i}^{j_1}\gamma$.
$\beta \leftarrow \gamma$
while $\beta \neq 1$ do
    Let $\alpha = \mu\beta + \nu$ with $\mathcal{N}(\nu) = 0$ or $\mathcal{N}(\nu) \leq \frac{1}{2}\mathcal{N}(\beta)$.
    $\alpha \leftarrow \nu$
    if $\alpha$ == 0 then                                        // gcd$(\alpha, \beta) \neq 1$
        return 0
    end
    /* remove factors of $1+\mathrm{i}$ in $\alpha$ and apply Theorem 4          */
    Let $\beta = a + b\mathrm{i}$ and let primary $\delta = e + f\mathrm{i}$ be defined by $\alpha = \mathrm{i}^{j_1}(1+\mathrm{i})^{j_2}\delta$.
    $c \leftarrow c \times \mathrm{i}^{(a-1)j_1/2} \times \mathrm{i}^{(a-b-b^2-1)j_2/4}$.
    $\alpha \leftarrow \delta$
    /* apply Theorem 3                                                        */
    if $a \equiv 3 \bmod 4$ and $e \equiv 3 \bmod 4$ then
        $c \leftarrow -c$
    end
    Interchange $\alpha, \beta$.
end
return $c$
```

or $\overline{\lambda}$) must divide $h - \mathrm{i}$. By renaming π and λ if needed, we may write $\rho = \pi\lambda$. Finally, $\mathscr{D}$ computes $c = \left(\frac{x}{\rho}\right)_4$ by Algorithm 1, it outputs "yes" if $c = 1$ and "no" otherwise. Note that if x is of the form $y^{p_0^d p_t q_t}$ with $y \in \mathcal{QR}_N$ then we must have $c = \left(\frac{y^{2^d p_t q_t}}{\rho}\right)_4 = \left(\frac{y}{\rho}\right)_4^{2^d p_t q_t} = 1$ (since $d > 1$ and $\gcd(y, \rho) = \gcd(y, N) = 1$). This gives us with an efficient distinguisher $\mathscr{D}$:

Distinguisher $\mathscr{D}$: $\mathscr{D}$ is given as input an RSA quintuple $(N, p_0 := 2, d, g, u)$ and a sample $x \in \mathcal{QR}_N$.

```
Compute $h = g^{p_0^d/4} \bmod N$.
Compute $\rho = \gcd(N, h - \mathrm{i})$ by the Euclidean Algorithm in $\mathbb{Z}[\mathrm{i}]$.
Compute $c = \left(\frac{x}{\rho}\right)_4$ by Algorithm 1.
if $c$ == 1 then
    Output "yes".
else
    Output "no".
end if
```

According to the complexity analysis in Section 3.2, the overall time complexity of $\mathscr{D}$ will then be

$$O\left(\log\left(\frac{p_0^d}{4}\right)\cdot(\log N)^2\right)+O\left((\log\mathcal{N}(N(h-\mathrm{i})))^3\right)+O\left((\log\mathcal{N}(x\rho))^3\right)=O\left((\log N)^3\right)$$

bit operations, so that $\mathscr{D}$ runs in polynomial time. To show that $\mathscr{D}$ can solve the SRSDP with non-negligible advantage, we need the following two lemmas. To state them, we define the function $\mathbb{I}_\epsilon$ ($\epsilon\in\mathbb{Z}[\mathrm{i}]^\times$) by $\mathbb{I}_\epsilon[\epsilon]=1$ and $\mathbb{I}_\epsilon[\delta]=0$ for all $\delta\in\mathbb{Z}[\mathrm{i}]^\times\setminus\{\epsilon\}$.

Lemma 1. *Let $p\equiv 1 \bmod 4$ be a prime and let $p=\pi\overline{\pi}$ for some prime element $\pi\in\mathbb{Z}[\mathrm{i}]$. Then for $\epsilon\in\{\pm1\}$ we have*

$$\sum_{\substack{0\le r\le p-1\\ \left(\frac{r}{p}\right)=1}}\mathbb{I}_\epsilon\left[\left(\frac{r}{\pi}\right)_4\right]=\frac{p-1}{4},$$

and for $\delta\in\{\pm\mathrm{i}\}$ we have

$$\sum_{\substack{0\le r\le p-1\\ \left(\frac{r}{p}\right)=-1}}\mathbb{I}_\delta\left[\left(\frac{r}{\pi}\right)_4\right]=\frac{p-1}{4}.$$

Proof. We calculate

$$\begin{aligned}\sum_{\substack{0\le r\le p-1\\ \left(\frac{r}{p}\right)=1}}\mathbb{I}_\epsilon\left[\left(\frac{r}{\pi}\right)_4\right]&=\frac{\epsilon}{4}\sum_{1\le r\le p-1}\left[\left(\frac{r}{p}\right)+1\right]\left[\left(\frac{r}{\pi}\right)_4+\epsilon\right]\\&=\frac{\epsilon}{4}\left[\sum_{1\le r\le p-1}\left(\frac{r}{\pi}\right)_4^3+\sum_{1\le r\le p-1}\epsilon\right]\\&=\frac{\epsilon}{4}\sum_{1\le r\le p-1}\left(\frac{r}{\overline{\pi}}\right)_4+\frac{p-1}{4}\\&=\frac{p-1}{4}\end{aligned}$$

where the last three lines follow from the three facts:

- If χ is a non-trivial multiplicative character, then $\sum_{t\in\mathbb{F}_p}\chi(t)=0$.
- If $\alpha\in\mathbb{Z}[\mathrm{i}]$, $\beta\in\mathbb{Z}[\mathrm{i}]^\times$ and $\gcd(2\alpha,\beta)=1$, then $\gcd(\overline{\alpha},\overline{\beta})=1$ and $\overline{\left(\frac{\alpha}{\beta}\right)_4}=\left(\frac{\alpha}{\beta}\right)_4^3=\left(\frac{\overline{\alpha}}{\overline{\beta}}\right)_4$.
- If $a\in\mathbb{Z},\beta\in\mathbb{Z}[\mathrm{i}]^\times$ and $\gcd(2a,\beta)=1$, then $\left(\frac{a}{\beta}\right)_4^2=\left(\frac{a}{\mathcal{N}(\beta)}\right)$.

The second formula can be proved similarly. □

Lemma 2. *Let $p \equiv q \equiv 1 \bmod 4$ be two distinct primes and let $p = \pi\overline{\pi}$, $q = \lambda\overline{\lambda}$ for some prime elements $\pi, \lambda \in \mathbb{Z}[\mathrm{i}]$. Set $N = pq$ and $\gamma = \pi\lambda$. Then*

$$\sum_{k \in \mathcal{QR}_N} \mathbb{I}_1 \left[\left(\frac{k}{\gamma} \right)_4 \right] = \sum_{k \in \mathcal{QR}_N} \mathbb{I}_{-1} \left[\left(\frac{k}{\gamma} \right)_4 \right] = \frac{(p-1)(q-1)}{8}. \tag{2}$$

Proof. We calculate

$$\begin{aligned} \sum_{k \in \mathcal{QR}_N} \mathbb{I}_1 \left[\left(\frac{k}{\gamma} \right)_4 \right] &= \sum_{\substack{1 \le k \le N \\ \left(\frac{k}{p}\right) = \left(\frac{k}{q}\right) = 1}} \mathbb{I}_1 \left[\left(\frac{k}{\gamma} \right)_4 \right] \\ &= \sum_{\substack{0 \le r \le p-1,\, 0 \le s \le q-1 \\ k \equiv r \bmod p,\, k \equiv s \bmod q \\ \left(\frac{k}{p}\right) = \left(\frac{k}{q}\right) = 1}} \mathbb{I}_1 \left[\left(\frac{k}{\pi\lambda} \right)_4 \right] \\ &= \sum_{\substack{0 \le r \le p-1,\, 0 \le s \le q-1 \\ \left(\frac{r}{p}\right) = \left(\frac{s}{q}\right) = 1}} \mathbb{I}_1 \left[\left(\frac{r}{\pi} \right)_4 \left(\frac{s}{\lambda} \right)_4 \right]. \end{aligned}$$

Since $\left(\frac{r}{p}\right) = \left(\frac{s}{q}\right) = 1$ if and only if both $\left(\frac{r}{\pi}\right)_4$ and $\left(\frac{s}{\lambda}\right)_4$ are equal to ± 1, it follows by Lemma 1 that

$$\begin{aligned} \sum_{\substack{0 \le r \le p-1,\, 0 \le s \le q-1 \\ \left(\frac{r}{p}\right) = \left(\frac{s}{q}\right) = 1}} \mathbb{I}_1 \left[\left(\frac{r}{\pi} \right)_4 \left(\frac{s}{\lambda} \right)_4 \right] &= \sum_{\substack{0 \le r \le p-1 \\ \left(\frac{r}{p}\right) = 1}} \mathbb{I}_1 \left[\left(\frac{r}{\pi} \right)_4 \right] \times \sum_{\substack{0 \le s \le q-1 \\ \left(\frac{s}{q}\right) = 1}} \mathbb{I}_1 \left[\left(\frac{s}{\lambda} \right)_4 \right] \\ &\quad + \sum_{\substack{0 \le r \le p-1 \\ \left(\frac{r}{p}\right) = 1}} \mathbb{I}_{-1} \left[\left(\frac{r}{\pi} \right)_4 \right] \times \sum_{\substack{0 \le s \le q-1 \\ \left(\frac{s}{q}\right) = 1}} \mathbb{I}_{-1} \left[\left(\frac{s}{\lambda} \right)_4 \right] \\ &= \frac{(p-1)(q-1)}{8}. \end{aligned}$$

The second formula can be proved in a similar way. □

Theorem 5. *Given an instance $\mathcal{I} = \{(N, p_0 := 2, d, g, u), x\}$ of SRSDP, the advantage of the above distinguisher $\mathscr{D}$ for solving the SRSDP satisfies*

$$\mathsf{Adv}_{\mathscr{D},\mathcal{I}}^{\mathit{SRSDP}} = \frac{1}{2}.$$

Proof. By Definition 4 and the method explained above, we have

$$\begin{aligned} \mathsf{Adv}_{\mathscr{D},\mathcal{I}}^{\mathsf{SRSDP}} &= \Pr[\mathscr{D}(\mathcal{I}) \text{ outputs ``yes''} \mid {\scriptstyle x \text{ is of the form } y^{p_0^d p_t q_t} \atop \text{with } y \in \mathcal{QR}_N}] - \frac{1}{2} \\ &\quad + \Pr[\mathscr{D}(\mathcal{I}) \text{ outputs ``no''} \mid x \in \mathcal{QR}_N] - \frac{1}{2} \\ &= \Pr[\mathscr{D}(\mathcal{I}) \text{ outputs ``no''} \mid x \in \mathcal{QR}_N]. \end{aligned}$$

Note that $\rho = \pi\lambda$ can be computed by $\mathscr{D}$ where $N = pq$ and $p = \pi\overline{\pi}$, $q = \lambda\overline{\lambda}$, then Lemma 2 implies that

$$\Pr[\mathscr{D}(\mathcal{I}) \text{ outputs ``no''} \mid x \in \mathcal{QR}_N] = \frac{\dfrac{(p-1)(q-1)}{8}}{\dfrac{(p-1)(q-1)}{4}} = \frac{1}{2}. \tag{3}$$

This concludes the proof of the theorem. □

3.4 Examples

To better understand how $\mathscr{D}$ shown in Section 3.3 works, we give a toy example as follows.

Example 1. Assume that the parameters of the SRSDP are set as in Table 2. Note that here g is of order $p_0^d = 8$ in both $\mathbb{Z}_p^*$ and $\mathbb{Z}_q^*$, and x is a sample from the uniform distributions over $\mathcal{QR}_N$.

Table 2. Parameters of the SRSDP in Example 1

Parameter	Value	Parameter	Value
p_0	2	d	3
p_s	5	p	$3761 = (56+25\mathrm{i})(56-25\mathrm{i})$
p_t	47	q	$2129 = (40+23\mathrm{i})(40-23\mathrm{i})$
q_s	7	N	8007169
q_t	19	g	18315
u	3	x	$200003 \equiv 555183^2 \pmod{N}$

$\mathscr{D}$ first calculates

$$g^{p_0^d/4} \equiv 7145296 \pmod{N}$$

and

$$\gcd(N, 7145296 - \mathrm{i}) = 2815 - 288\mathrm{i}.$$

(indeed, $2815 - 288\mathrm{i} = (40 - 23\mathrm{i})(56 + 25\mathrm{i})$). Next, $\mathscr{D}$ calculates $\left(\frac{200003}{2815-288\mathrm{i}}\right)_4$ as in Table 3 and obtains

$$\left(\frac{200003}{2815-288\mathrm{i}}\right)_4 = \mathrm{i} \times -\mathrm{i} \times -1 \times 1 = -1.$$

without knowing the factorization of N or $2815 - 288\mathrm{i}$.

Finally, $\mathscr{D}$ correctly outputs "no" because the above quartic Jacobi symbol is not equal to 1, which means that $x = 200003$ is not a quartic residue and x cannot therefore be written as $y^{p_0^d p_t q_t}$ for any $y \in \mathcal{QR}_N$. Further, its order in $\mathbb{Z}_N^*$ is

$$50008 = 2^3 \times 7 \times 19 \times 47$$

Table 3. Procedures for calculating $\left(\frac{200003}{2815-288i}\right)_4$

Make the modulus of a quartic residue symbol primary	Calculate the remainder of a primary when divided by an element in $\mathbb{Z}[i]$	Remove factors of $1+i$ and apply the general quartic reciprocity law (Theorem 3) and its supplement (Theorem 4)
$\left(\frac{200003}{2815-288i}\right)_4 = \left(\frac{200003}{-2815+288i}\right)_4$	$200003 = (-2815+288i)(-70-7i)$ $+ (937+455i)$	$\left(\frac{200003}{-2815+288i}\right)_4 = \left(\frac{937+455i}{-2815+288i}\right)_4 = \left(\frac{(1+i)(696-241i)}{-2815+288i}\right)_4$ $= 1 \times \left(\frac{696-241i}{-2815+288i}\right)_4$ $= \left(\frac{-i}{-2815+288i}\right)_4 \left(\frac{241+696i}{-2815+288i}\right)_4$ $= 1 \times \left(\frac{241+696i}{-2815+288i}\right)_4 = \left(\frac{-2815+288i}{241+696i}\right)_4$
$\left(\frac{-2815+288i}{241+696i}\right)_4 = \left(\frac{-2815+288i}{241+696i}\right)_4$	$-2815+288i = (241+696i)(-1+4i)$ $+ (210+20i)$	$\left(\frac{-2815+288i}{241+696i}\right)_4 = \left(\frac{210+20i}{241+696i}\right)_4 = \left(\frac{(1+i)^2(10-105i)}{241+696i}\right)_4$ $= 1 \times \left(\frac{10-105i}{241+696i}\right)_4$ $= \left(\frac{i}{241+696i}\right)_4 \left(\frac{-105-10i}{241+696i}\right)_4$ $= 1 \times \left(\frac{-105-10i}{241+696i}\right)_4 = \left(\frac{241+696i}{-105-10i}\right)_4$
$\left(\frac{241+696i}{-105-10i}\right)_4 = \left(\frac{241+696i}{-105-10i}\right)_4$	$241+696i = (-105-10i)(-3-6i)$ $+ (-14+36i)$	$\left(\frac{241+696i}{-105-10i}\right)_4 = \left(\frac{-14+36i}{-105-10i}\right)_4 = \left(\frac{(1+i)^2(18+7i)}{-105-10i}\right)_4$ $= -1 \times \left(\frac{18+7i}{-105-10i}\right)_4$ $= -1 \times \left(\frac{i}{-105-10i}\right)_4 \left(\frac{7-18i}{-105-10i}\right)_4$ $= -i \times \left(\frac{7-18i}{-105-10i}\right)_4 = i \times \left(\frac{-105-10i}{7-18i}\right)_4$
$\left(\frac{-105-10i}{7-18i}\right)_4 = \left(\frac{-105-10i}{7-18i}\right)_4$	$-105-10i = (7-18i)(-1-5i)$ $+ (-8+7i)$	$\left(\frac{-105-10i}{7-18i}\right)_4 = \left(\frac{-8+7i}{7-18i}\right)_4 = \left(\frac{(1+i)^0(-8+7i)}{7-18i}\right)_4$ $= 1 \times \left(\frac{-8+7i}{7-18i}\right)_4 = \left(\frac{-i}{7-18i}\right)_4 \left(\frac{-7-8i}{7-18i}\right)_4$ $= -i \times \left(\frac{-7-8i}{7-18i}\right)_4 = -i \times \left(\frac{7-18i}{-7-8i}\right)_4$
$\left(\frac{7-18i}{-7-8i}\right)_4 = \left(\frac{7-18i}{-7-8i}\right)_4$	$7-18i = (-7-8i)(1+2i)$ $+ (-2+4i)$	$\left(\frac{7-18i}{-7-8i}\right)_4 = \left(\frac{-2+4i}{-7-8i}\right)_4 = \left(\frac{(1+i)^2(2+i)}{-7-8i}\right)_4$ $= 1 \times \left(\frac{2+i}{-7-8i}\right)_4 = \left(\frac{-i}{-7-8i}\right)_4 \left(\frac{-1+2i}{-7-8i}\right)_4$ $= 1 \times \left(\frac{-1+2i}{-7-8i}\right)_4 = \left(\frac{-7-8i}{-1+2i}\right)_4$
$\left(\frac{-7-8i}{-1+2i}\right)_4 = \left(\frac{-7-8i}{-1+2i}\right)_4$	$-7-8i = (-1+2i)(-2+4i)$ $+ (-1)$	$\left(\frac{-7-8i}{-1+2i}\right)_4 = \left(\frac{-1}{-1+2i}\right)_4 = \left(\frac{(1+i)^0(-1)}{-1+2i}\right)_4$ $= 1 \times \left(\frac{-1}{-1+2i}\right)_4 = \left(\frac{-1}{-1+2i}\right)_4 \left(\frac{1}{-1+2i}\right)_4$ $= -1 \times \left(\frac{1}{-1+2i}\right)_4 = -1 \times \left(\frac{-1+2i}{1}\right)_4$
$\left(\frac{-1+2i}{1}\right)_4 = \left(\frac{-1+2i}{1}\right)_4$	$-1+2i = (1)(-1+2i) + (0)$	$\left(\frac{-1+2i}{1}\right)_4 = \left(\frac{0}{1}\right)_4 = 1$

not equal to $p_s q_s = 5 \times 7$.

The C++ codes for the above attack can be found at https://github.com/tcet030840zxp/Quartic-Residuosity-Attack-on-the-SRSDP.

4 A Higher Residuosity Attack on the SRSDP

In this section, we describe a higher residuosity attack on the SRSDP when p_0 is an odd prime. The success probability of this attack is very high, but computing the p_0^{th} power residue symbol for large p_0 turns out to be its efficiency bottleneck in practical implementations.

4.1 The Power Residue Symbol

Let K be a number field. We say a prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$ is prime to an integer $\ell \geq 1$ if $\mathfrak{p} \nmid \ell\mathcal{O}_K$, this is equivalent to the assertion that $\gcd(\mathcal{N}(\mathfrak{p}), \ell) = 1$, where $\mathcal{N}(\mathfrak{p}) = |\mathcal{O}_K/\mathfrak{p}|$. Since the multiplicative group of $\mathcal{O}_K/\mathfrak{p}$ has $\mathcal{N}(\mathfrak{p}) - 1$ elements, we have

$$\alpha^{\mathcal{N}(\mathfrak{p})-1} \equiv 1 \pmod{\mathfrak{p}} \quad \text{for } \alpha \in \mathcal{O}_K,\ \alpha \notin \mathfrak{p}.$$

Furthermore, if we have an additional condition that $\zeta_\ell \in K$, then the order of the group $\langle \zeta_\ell/\mathfrak{p} \rangle$ generated in $(\mathcal{O}_K/\mathfrak{p})^\times$ is ℓ, and hence $\ell \mid \mathcal{N}(\mathfrak{p}) - 1$. Now, we can define the ℓ^{th} *power residue symbol* $\left(\frac{\alpha}{\mathfrak{p}}\right)_\ell$ as follows: if $\alpha \in \mathfrak{p}$, then $\left(\frac{\alpha}{\mathfrak{p}}\right)_\ell = 0$; otherwise, $\left(\frac{\alpha}{\mathfrak{p}}\right)_\ell$ is the unique ℓ^{th} root of unity such that

$$\left(\frac{\alpha}{\mathfrak{p}}\right)_\ell \equiv \alpha^{\frac{\mathcal{N}(\mathfrak{p})-1}{\ell}} \pmod{\mathfrak{p}}.$$

This definition can be naturally extended to the case that $\mathfrak{a} = \prod_i \mathfrak{p}_i$ is prime to ℓ, i.e., $\gcd(\mathcal{N}(\mathfrak{p}_i), \ell) = 1$ for each i. For $\alpha \in \mathcal{O}_K$, define the generalized ℓ^{th} power residue symbol as

$$\left(\frac{\alpha}{\mathfrak{a}}\right)_\ell = \prod_i \left(\frac{\alpha}{\mathfrak{p}_i}\right)_\ell.$$

If $\beta \in \mathcal{O}_K$ and β is prime to ℓ define $\left(\frac{\alpha}{\beta}\right)_\ell = \left(\frac{\alpha}{(\beta)}\right)_\ell$. We suggest interested readers to refer to [19,23,28] for more details about the power residue symbol. In the rest of this paper, we shall simply consider the case of $K = \mathbb{Q}(\zeta_\ell)$ for $\ell > 2$. In this case, it is well known that $\mathcal{O}_K = \mathbb{Z}[\zeta_\ell]$ and that $\mathcal{O}_K^\times$ is a finitely generated abelian group of rank $r = \varphi(\ell)/2 - 1$; there exists a *fundamental system of units* $\{u_1, \ldots, u_r\}$ of K such that every element $x \in \mathcal{O}_K^\times$ can be written in a unique way as $x = \zeta u_1^{n_1} \cdots u_r^{n_r}$ where $n_i \in \mathbb{Z}$ and $\zeta \in \langle \pm\zeta_\ell \rangle$ (e.g., $\ell = 5$, $r = 1$, and $u_1 = 1 + \zeta_5$).

We now turn to the case ℓ is an odd prime. Let $\omega = 1 - \zeta_\ell$, we have $(\ell) = (\omega)^{\ell-1}$ and (ω) is a prime ideal of degree 1. An element $\alpha \in \mathbb{Z}[\zeta_\ell]$ is called *primary* if $\alpha \not\equiv 0 \bmod \omega$, $\alpha \equiv B \bmod \omega^2$ and $\alpha\overline{\alpha} \equiv B^2 \bmod \ell$ for some $B \in \mathbb{Z}$. If $\mathbb{Q}(\zeta_\ell)$

is *regular*[5], then each $\alpha \in \mathbb{Z}[\zeta_\ell]$ prime to ℓ can be transformed into a primary number on multiplication by a suitable unit [18, Theorem 157]. More properties of primary elements can be found in [7, Lemma 2.6]. *Kummer's reciprocity law* is crucial to the computation of power residue symbols, especially when $\mathbb{Z}[\zeta_\ell]$ is *norm-Euclidean* (e.g., $\ell \leq 13$ [24,22,6]). The complementary laws for ω, ℓ and units can be found in [7].

Theorem 6 (Kummer's Reciprocity Law [18, Theorem 161]). *Let ℓ be a regular prime number and let α and β be two primary elements in $\mathbb{Z}[\zeta_\ell]$. Then*

$$\left(\frac{\alpha}{\beta}\right)_\ell = \left(\frac{\beta}{\alpha}\right)_\ell .$$

Theorem 6 was established in 1850. It is restricted to so-called "regular" primes, which include the odd primes $p \leq 13$. It is crucial for designing algorithms to compute residue symbols, akin to the quadratic reciprocity law used for evaluating the Jacobi symbol in $\mathbb{Z}$). For $\ell \leq 11$, these results can be integrated with Lenstra's norm-Euclidean algorithm [24] (see also [7, Section 7]) to develop an effective algorithm for computing $\left(\frac{\alpha}{\beta}\right)_\ell$ in $\mathbb{Q}(\zeta_\ell)$. We present a list of references for the relevant fast algorithms in Table 4.

Table 4. Algorithms for Computing the ℓ^{th} Power Residue Symbol

ℓ	3	5	7	11	13
References	[32,30,10]	Scheidler et al. [30]	Caranay et al. [7]	Joye et al. [21]	Brier et al. [6]

The general case of computing higher power residue symbols was tackled by de Boer [3] and the resulting algorithms are probabilistic. However, it has not yet been proven to be a polynomial-time algorithm. De Boer's computational results [3, Chapter 5] show that for degrees around 100 the computation of one single power residue symbol might last for several weeks.

4.2 Attacking the SRSDP via the Power Residue Symbol

With the preparation for the power residue symbol, attacks on the SRSDP are possible when p_0 is a small odd prime number. Given an RSA quintuple (N, p_0, d, g, u) and a sample $x \in \mathcal{QR}_N$, $\mathscr{D}$ first computes $h = g^{p_0^{d-1}} \bmod N$, whose order is p_0 in $\mathbb{Z}_N^*$. Let $K = \mathbb{Q}(\zeta_{p_0})$. Then the prime decomposition of p in $\mathcal{O}_K$ can be obtained immediately from [9, Theorem 4.8.13] as follows:

$$p\mathcal{O}_K = \prod_{i=1}^{p_0-1} \mathfrak{p}_i$$

[5] If the class number of $\mathbb{Q}(\zeta_\ell)$ is not divisible by ℓ, then $\mathbb{Q}(\zeta_\ell)$ is called a *regular cyclotomic field* and ℓ is called a *regular prime number*. The first few *irregular prime numbers* are 37, 59, 67, 101, 103, 149 and 157.

where $\mathfrak{p}_i = p\mathcal{O}_K + (h^i - \zeta_{p_0})\mathcal{O}_K$ and $\mathcal{N}(\mathfrak{p}_i) = p$. Similarly,

$$q\mathcal{O}_K = \prod_{i=1}^{p_0-1} \mathfrak{q}_i$$

where $\mathfrak{q}_i = q\mathcal{O}_K + (h^i - \zeta_{p_0})\mathcal{O}_K$ and $\mathcal{N}(\mathfrak{q}_i) = q$. Next, $\mathscr{D}$ sets

$$\mathfrak{a} = \mathfrak{p}_1\mathfrak{q}_1 = N\mathcal{O}_K + (h - \zeta_{p_0})\mathcal{O}_K.$$

Finally, $\mathscr{D}$ computes $c = \left(\frac{x}{\mathfrak{a}}\right)_{p_0}$ using the algorithms introduced earlier, it outputs "yes" if $c = 1$ and "no" otherwise. Note that if x is of the form $y^{p_0^d p_t q_t}$ with $y \in \mathcal{QR}_N$ then we must have $c = 1$. This gives us a distinguisher $\mathscr{D}$:

Distinguisher $\mathscr{D}$: $\mathscr{D}$ is given as input an RSA quintuple $(N, p_0(>2), d, g, u)$ and a sample $x \in \mathcal{QR}_N$.

```
Compute $h = g^{p_0^{d-1}} \bmod N$.
if $p_0 \leq 13$ then
    Compute $\beta = \gcd(N, h - \zeta_{p_0})$ by Lenstra's norm-Euclidean algorithm [24] for $p_0 \leq 11$ and by McKenzie's norm-Euclidean algorithm [26] for $p_0 = 13$.
    Compute $c = \left(\frac{x}{\beta}\right)_{p_0}$ by the algorithms in Table 4.
else
    Set $\mathfrak{a} = N\mathcal{O}_K + (h - \zeta_{p_0})\mathcal{O}_K$.
    Compute $c = \left(\frac{x}{\mathfrak{a}}\right)_{p_0}$ by de Boer's Algorithm [3].
end if
if $c == 1$ then
    Output "yes".
else
    Output "no".
end if
```

Notice that when $p_0 \leq 13$, $\mathscr{D}$ runs in polynomial time and is efficient. To show that $\mathscr{D}$ can solve the SRSDP with non-negligible advantage, we need the following lemma.

Lemma 3. *With notations as above, let*

$$S_\epsilon = \left\{ k \in \mathcal{QR}_N : \left(\frac{k}{\mathfrak{a}}\right)_{p_0} = \epsilon \right\}, \quad \epsilon \in \langle \zeta_{p_0} \rangle.$$

Then $|S_\epsilon| = \frac{(p-1)(q-1)}{4p_0}$ *for every* $\epsilon \in \langle \zeta_{p_0} \rangle$.

Proof. It is easy to see that $\sum_{\epsilon \in \langle \zeta_{p_0} \rangle} |S_\epsilon| = |\mathcal{QR}_N| = \frac{(p-1)(q-1)}{4}$, so it suffices to prove that all of the S_ϵ's have identical cardinalities. Let a_p (resp. a_q) be a generator of $\mathcal{QR}_p$ (resp. $\mathcal{QR}_q$). Then the order of $a_p^{\frac{p-1}{p_0}}$ (resp. $a_q^{\frac{q-1}{p_0}}$) is p_0, and therefore $\left(\frac{a_p}{\mathfrak{p}_1}\right)_{p_0} = \zeta_{p_0}^i$ for some $0 < i < p_0$ (resp. $\left(\frac{a_q}{\mathfrak{q}_1}\right)_{p_0} = \zeta_{p_0}^j$ for some $0 < j < p_0$). For every $k \in \mathbb{Z}_{p_0}$, we have $\left(\frac{a}{\mathfrak{a}}\right)_{p_0} = \zeta_{p_0}^k$ if a is chosen so that $a \equiv a_p^{k(i^{-1} \bmod p_0)} \pmod p$ and $a \equiv a_q^{p_0} \pmod q$, so if $|S_\alpha| < |S_\beta|$ for some $\alpha, \beta \in \langle \zeta_{p_0} \rangle$, then there exists $b \in \mathcal{QR}_N$ such that the coset $bS_\beta \subset S_\alpha$, a contradiction. In fact, S_1 is a subgroup of $\mathbb{Z}_N^*$ and all of the remaining sets S_ϵ ($\epsilon \in \langle \zeta_{p_0} \rangle \setminus \{1\}$) are its cosets. □

Theorem 7. *Given an instance $\mathcal{I} = \{(N, p_0(>2), d, g, u), x\}$ of SRSDP, the advantage of the above distinguisher $\mathscr{D}$ for solving the SRSDP satisfies*

$$\mathsf{Adv}_{\mathscr{D},\mathcal{I}}^{\mathit{SRSDP}} = \frac{p_0 - 1}{p_0}.$$

Proof. By Definition 4 and the method explained above, we have

$$\begin{aligned}
\mathsf{Adv}_{\mathscr{D},\mathcal{I}}^{\mathsf{SRSDP}} &= \Pr[\mathscr{D}(\mathcal{I}) \text{ outputs “yes”} \mid {\scriptstyle x \text{ is of the form } y^{p_0^d p_t q_t} \atop \text{with } y \in \mathcal{QR}_N}] - \frac{1}{2} \\
&\quad + \Pr[\mathscr{D}(\mathcal{I}) \text{ outputs “no”} \mid x \in \mathcal{QR}_N] - \frac{1}{2} \\
&= \Pr[\mathscr{D}(\mathcal{I}) \text{ outputs “no”} \mid x \in \mathcal{QR}_N].
\end{aligned}$$

Note that $\mathfrak{a} = N\mathcal{O}_K + (h - \zeta_{p_0})\mathcal{O}_K$ can be computed by $\mathscr{D}$, then Lemma 3 implies that

$$\begin{aligned}
\Pr[\mathscr{D}(\mathcal{I}) \text{ outputs “no”} \mid x \in \mathcal{QR}_N] &= \frac{\frac{(p-1)(q-1)(p_0-1)}{4p_0}}{\frac{(p-1)(q-1)}{4}} \\
&= \frac{p_0 - 1}{p_0}. \qquad (4)
\end{aligned}$$

This concludes the proof of the theorem. □

5 Higher Residuosity Attacks on the CEK and BST Protocols

In this section, we present practical higher residuosity attacks on the CEK and BST protocols. Throughout this section, we assume that the prime base p_0 is small enough so that the p_0^{th} power residue symbol can be efficiently computed, e.g., $p_0 < 100$ according to de Boer's computational results [3, Chapter 5].

We first show that the encryption scheme $\Pi = (\mathsf{KGen}, \mathsf{Enc}, \mathsf{Dec})$ proposed in [8, Section 4], which is the principal ingredient in both protocols, is not semantically secure. Except for replacing b with p_0, we use the notations as in [8, Section 4]. Consider the following experiment between a challenger $\mathscr{C}$ and an adversary $\mathscr{A}$:

1. $\mathscr{C}$ runs $\mathsf{KGen}(\tau)$ to obtain keys $\mathcal{PK} = (N, p_0, d(\geq 3), g, u, h)$ and $\mathcal{SK}$, where (N, p_0, d, g, u) is an RSA quintuple, h has order p_s in $\mathbb{Z}_p^*$ and q_s in $\mathbb{Z}_q^*$.
2. $\mathscr{A}$ is given $\mathcal{PK}$, and outputs a pair of messages $m_0 = 0$, $m_1 = 1$.
3. $\mathscr{C}$ chooses a uniform bit $b \in \{0, 1\}$, and then a challenge ciphertext $C \leftarrow \mathsf{Enc}(\mathcal{PK}, m_b) := g^{p_0^{m_b}} h^r \bmod N$ is computed and given to $\mathscr{A}$, where r is chosen uniformly from $\{1, \ldots, 2^u - 1\}$.
4. $\mathscr{A}$ computes[6]

$$c = \begin{cases} \left(\frac{C}{\gcd\left(N, g^{p_0^{d-3}} - \zeta_8\right)}\right)_8, & \text{if } p_0 = 2; \\ \left(\frac{C}{\left(N, g^{p_0^{d-1}} - \zeta_{p_0}\right)}\right)_{p_0}, & \text{otherwise.} \end{cases}$$

   It outputs a bit $b' = 1$ if $c = 1$ and $b' = 0$ otherwise. If $b' = b$ we say that $\mathscr{A}$ correctly guesses the encrypted message.

We claim that the advantage of correctly guessing the encrypted message in the above experiment is 1 when $2p_0 \nmid p_s p_t + q_s q_t$. From the proof of Theorem 1, h is a p_0^{th} power, hence $c = 1$ if $m_b = 1$; otherwise we have

$$c = \begin{cases} \left(\frac{g}{\gcd\left(N, g^{p_0^{d-3}} - \zeta_8\right)}\right)_8 = \zeta_4^{p_s p_t + q_s q_t}, & \text{if } p_0 = 2; \\ \left(\frac{g}{\left(N, g^{p_0^{d-1}} - \zeta_{p_0}\right)}\right)_{p_0} = \zeta_{p_0}^{2(p_s p_t + q_s q_t)}, & \text{otherwise.} \end{cases}$$

If $2p_0 \nmid p_s p_t + q_s q_t$, then we have $c \neq 1$, thus the claim is established.

From the attack above, we can see that the ciphertext may leak information about whether the corresponding plaintext is 0. Since in the first pass of both the CEK and BST protocols the party P_1 (having private input m_1) sends the encryption of integer multiples of m_1 to the party P_2, then P_2 is able to determine whether m_1 is zero, hence neither of the two protocols protects the privacy of P_1.

Finally, to preclude such attacks, we provide the following suggestions for improvement:

1. use larger p_0, so that it is infeasible to compute the p_0^{th} power residue symbol.
2. choose two distinct large primes p_s and q_s such that $p_s \mid p - 1$ and $q_s \mid q - 1$, and then choose g to be of order $p_0^d p_s q_s$, modify the protocols as in [12].
3. force the RSA quintuple to satisfy $2p_0^d \mid p_s p_t + q_s q_t$ and try to prove the semantic security under some number-theoretic hardness assumptions pertaining to higher residuosity, the protocols' performance is not impacted in this way.

[6] See [20] for an algorithm to evaluate octic residue symbols. Lenstra's norm-Euclidean algorithm [24] can be used for GCD computation.

6 Conclusion

Quadratic and higher residuosity are powerful tools that find applications in various cryptographic constructions. For instance, they are used in encryption schemes [15,32,30,1], authentication schemes [27,5], and digital signatures [29]. In this paper, we present higher residuosity attacks against two efficient two-party comparison protocols recently proposed by Carlton et al. [8] and Bourse et al. [4]. For a small public prime base p_0, any adversary with access to an element of order p_0 in $\mathbb{Z}_N^*$ in the two protocols would be able to employ such attacks, leading to privacy leakage. All of these attacks are grounded in higher reciprocity laws. Future work will investigate whether a more efficient algorithm exists for computing power residue symbols modulo a two-element representation ideal. The attacks we propose are currently ineffective against other famous power-residuosity-type assumptions, such as the Gap 2^k-residuosity assumption, which underpins the security of the Joye-Libert cryptosystem proposed in [1]. The Gap 2^k-residuosity assumption in $\mathbb{Z}_N^*$ consists in distinguishing a uniform element of $V_0 = \{x \in \mathcal{J}_N \setminus \mathcal{QR}_N\}$ from a uniform element of $V_1 = \{y^{2^k} \bmod N \mid y \in \mathbb{Z}_N^*\}$, given only $N = pq$. This ineffectiveness arises because the attacker cannot effectively find an element of order 2^k $(k \geq 2)$ in $\mathbb{Z}_N^*$ in advance. We hope that this paper will serve as a valuable resource for future protocol designers working with RSA-type problems. Additionally, we believe that the higher residuosity attacks discussed herein can be employed to analyze other number-theoretic hardness assumptions.

Acknowledgments. We would like to thank Professor Jun Shao for his constant encouragement and careful reading of the manuscript. We also extend our appreciation to all anonymous reviewers of PKC 2025 for their thorough reading of our manuscript and for their valuable comments. This work was supported by the Shanghai Science and Technology Commission [grant number 23YF1401000], the National Natural Science Foundation of China [grant number 62132005], and the Fundamental Research Funds for the Central Universities [grant number 2232022D-25].

Disclosure of Interests. All authors disclosed no relevant relationships.

References

1. Benhamouda, F., Herranz, J., Joye, M., Libert, B.: Efficient cryptosystems from 2^k-th power residue symbols. J. Cryptol. **30**(2), 519–549 (2017). https://doi.org/10.1007/S00145-016-9229-5
2. Blake, I.F., Kolesnikov, V.: Conditional encrypted mapping and comparing encrypted numbers. In: Proc. 10th International Conference on Financial Cryptography and Data Security - FC 2006. LNCS, vol. 4107, pp. 206–220. Springer, Heidelberg (2006). https://doi.org/10.1007/11889663_18
3. de Boer, K.: Computing the power residue symbol. Master's thesis. Nijmegen, Radboud University. (2016), www.koendeboer.com

4. Bourse, F., Sanders, O., Traoré, J.: Improved secure integer comparison via homomorphic encryption. In: Topics in Cryptology - CT-RSA 2020 - The Cryptographers' Track at the RSA Conference. LNCS, vol. 12006, pp. 391–416. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-40186-3_17
5. Brier, É., Ferradi, H., Joye, M., Naccache, D.: New number-theoretic cryptographic primitives. J. Math. Cryptol. **14**(1), 224–235 (2020)
6. Brier, E., Naccache, D.: The thirteenth power residue symbol. IACR Cryptology ePrint Archive **2019**, 1176 (2019), https://eprint.iacr.org/2019/1176
7. Caranay, P.C., Scheidler, R.: An efficient seventh power residue symbol algorithm. Int. J. Number Theory **6**(08), 1831–1853 (2010)
8. Carlton, R., Essex, A., Kapulkin, K.: Threshold properties of prime power subgroups with application to secure integer comparisons. In: Topics in Cryptology - CT-RSA 2018 - The Cryptographers' Track at the RSA Conference. LNCS, vol. 10808, pp. 137–156. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-76953-0_8
9. Cohen, H.: A course in computational algebraic number theory, vol. 138. Springer Science & Business Media, Heidelberg (2013)
10. Damgård, I., Frandsen, G.S.: Efficient algorithms for the gcd and cubic residuosity in the ring of eisenstein integers. J. Symb. Comput. **39**(6), 643–652 (2005). https://doi.org/10.1016/j.jsc.2004.02.006
11. Damgård, I., Geisler, M., Krøigaard, M.: Efficient and secure comparison for online auctions. In: Proc. 12th Australasian Conference on Information Security and Privacy - ACISP 2007. LNCS, vol. 4586, pp. 416–430. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-73458-1_30
12. Damgård, I., Geisler, M., Krøigaard, M.: A correction to "Efficient and Secure Comparison for On-Line Auctions". Int. J. Appl. Cryptogr. **1**(4), 323–324 (2009). https://doi.org/10.1504/IJACT.2009.028031
13. Fischlin, M.: A cost-effective pay-per-multiplication comparison method for millionaires. In: Topics in Cryptology - CT-RSA 2001, The Cryptographer's Track at RSA Conference. LNCS, vol. 2020, pp. 457–472. Springer, Heidelberg (2001). https://doi.org/10.1007/3-540-45353-9_33
14. Garay, J.A., Schoenmakers, B., Villegas, J.: Practical and secure solutions for integer comparison. In: Proc. 10th International Conference on Practice and Theory in Public-Key Cryptography - PKC 2007. LNCS, vol. 4450, pp. 330–342. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-71677-8_22
15. Goldwasser, S., Micali, S.: Probabilistic encryption and how to play mental poker keeping secret all partial information. In: Proc. 14th Annual ACM Symposium on Theory of Computing. pp. 365–377. ACM Press (1982). https://doi.org/10.1145/800070.802212
16. Groth, J.: Cryptography in subgroups of $\mathbb{Z}_n^*$. In: Proc. 2nd Theory of Cryptography Conference - TCC 2005. LNCS, vol. 3378, pp. 50–65. Springer, Heidelberg (2005). https://doi.org/10.1007/978-3-540-30576-7_4
17. Halter-Koch, F.: Quadratic irrationals: An introduction to classical number theory. CRC press, New York (2013)
18. Hilbert, D.: The theory of algebraic number fields. Springer Science & Business Media, Heidelberg (1998)
19. Ireland, K., Rosen, M.: A classical introduction to modern number theory, vol. 84. Springer Science & Business Media, Heidelberg (1990)
20. Joye, M.: Evaluating octic residue symbols. IACR Cryptol. ePrint Arch. p. 1196 (2019), https://eprint.iacr.org/2019/1196

21. Joye, M., Lapiha, O., Nguyen, K., Naccache, D.: The eleventh power residue symbol. J. Math. Cryptol. **15**(1), 111–122 (2021). https://doi.org/10.1515/jmc-2020-0077
22. Lemmermeyer, F.: The euclidean algorithm in algebraic number fields. Expo. Math. **13**, 385–416 (1995)
23. Lemmermeyer, F.: Reciprocity laws: from Euler to Eisenstein. Springer Science & Business Media, Heidelberg (2013)
24. Lenstra, H.W.: Euclid's algorithm in cyclotomic fields. J. London Math. Soc **10**, 457–465 (1975)
25. Lin, H., Tzeng, W.: An efficient solution to the millionaires' problem based on homomorphic encryption. In: Proc. 3rd International Conference on Applied Cryptography and Network Security - ACNS 2005. LNCS, vol. 3531, pp. 456–466. Springer, Heidelberg (2005). https://doi.org/10.1007/11496137_31
26. McKenzie, R.G.: The ring of cyclotomic integers of modulus thirteen is norm-euclidean. Ph.D. thesis, Michigan State University (1988)
27. Monnerat, J., Vaudenay, S.: Short undeniable signatures based on group homomorphisms. J. Cryptol. **24**, 545–587 (2011)
28. Neukirch, J.: Algebraic number theory, vol. 322. Springer Science & Business Media, Heidelberg (2013)
29. Rabin, M.O.: Digitalized signatures and public-key functions as intractable as factorization. Technical Report (1979)
30. Scheidler, R., Williams, H.C.: A public-key cryptosystem utilizing cyclotomic fields. Des. Codes Cryptogr. **6**(2), 117–131 (1995). https://doi.org/10.1007/BF01398010
31. Weilert, A.: Fast computation of the biquadratic residue symbol. J. Number Theory **96**(1), 133–151 (2002)
32. Williams, H.C.: An M^3 public-key encryption scheme. In: Proc. CRYPTO '85. LNCS, vol. 218, pp. 358–368. Springer, Heidelberg (1985). https://doi.org/10.1007/3-540-39799-X_26
33. Yao, A.C.: How to generate and exchange secrets (extended abstract). In: Proc. 27th Annual Symposium on Foundations of Computer Science. pp. 162–167 (1986). https://doi.org/10.1109/SFCS.1986.25