Higher Residuosity Attacks on Small RSA Subgroup Decision Problems

Xiaopeng Zhao, Zhenfu Cao, Xiaolei Dong, and Zhusen Liu

Donghua University, East China Normal University, and Hangzhou Innovation Institute of Beihang University

PKC 2025 · Røros, Norway

Content

Secure Two-Party Comparison

Secure two-party comparison, known as Yao's millionaires' problem, has been a fundamental challenge in privacy-preserving computation.

- Yao's Garbled Circuit
- Homomorphic encryption
  - Fischlin (CT-RSA 2001) first constructed a secure comparison of two numbers using a Boolean circuit based on the XOR-homomorphic Goldwasser-Micali cryptosystem.
  - Damgård, Geisler, and Krøigaard (ACISP 2007) enhanced this approach.
  - Drawing inspiration from the strong RSA subgroup assumption (related to high residuosity assumptions) proposed by Groth (TCC 2005) and the DGK comparison protocol, Carlton et al. (CT-RSA 2018) constructed a protocol that efficiently compares two encrypted integers through the (nearly) direct application of the homomorphism on a single encrypted value
  - Bourse et al. (CT-RSA 2020) improved the CEK protocol by avoiding one round induced by the plaintext equality test

This Talk

- Study of the *small RSA subgroup decision problems*
  - Both the CEK and BST protocols have been proven to be secure under the small RSA subgroup decision problems

Our Main Contribution

Extend the classical quadratic residuosity attack on the DDH problem to higher residuosity scenarios.

- break the small RSA subgroup decision problems 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
- serve as a resource for future protocol designers working with RSA-type problems

Definition 1 (RSA Quintuple)

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; (e.g., 128-bit security level requires $u = 256$.)
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:

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

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.

Small RSA Subgroup Decision Problems

Definition 2 (Small RSA Subgroup Decision Problem in [BourseST20] (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 in [CarltonEK18] ($\widetilde{\text{SRSDP}}$))

Given an RSA quintuple (N, p_0, d, g, u), distinguish the two uniform distributions over $\mathcal{QR}_N$ and over $\{x \in \mathcal{QR}_N \mid x \text{ has order } p_s q_s \text{ in } \mathbb{Z}_N^*\}$, respectively.

Theorem 4

If there exists a PPT *distinguisher being able to solve the SRSDP with light advantage then one can solve the* $\widetilde{\text{SRSDP}}$ *in polynomial time with non-negligible advantage.*

DDH Doesn't Hold in $\mathbb{Z}_p^*$

The DDH Problem

Fix a cyclic multiplicative group $\mathbb{G} = \langle g \rangle$ of order q, distinguish

$$(g^a, g^b, g^{ab}) \quad \text{from} \quad (g^a, g^b, g^c),$$

where $a, b, c \xleftarrow{\$} \mathbb{Z}_q$.

The DDH Problem is *Not Hard* in $\mathbb{Z}_p^*$

Given the tuple (g^a, g^b, T), compute the Legendre symbol $\left(\frac{T}{p}\right)$:

If $T = g^c$, then $\left(\frac{g^c}{p}\right) = \left(\frac{g}{p}\right)^c = (-1)^{c \bmod 2} = 1$ happens with probability $1/2$.

If $T = g^{ab}$, then $\left(\frac{g^{ab}}{p}\right) = \left(\frac{g}{p}\right)^{ab} = (-1)^{ab \bmod 2} = 1$ happens with probability $3/4$.

Key Insight: The quadratic residue symbol leaks the structure of $\mathbb{Z}_p^*$.

The Quartic Jacobi Symbol

Definition 5 (Quartic Residue Symbol)

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

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

Computing the Quartic Jacobi Symbol

Theorem 6 (Quartic Reciprocity Law)

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

Computing the Quartic Jacobi Symbol

Theorem 7 (Supplement to the Quartic Reciprocity Law)

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,*

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

The quartic reciprocity law together with its supplement gives an efficient method for computing $\left(\frac{\alpha}{\beta}\right)_4$ in $O\left((\log N)^3\right)$ time.

Attacking the SRSDP via the Quartic Jacobi Symbol

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

1: Compute $h = g^{p_0^d/4} \bmod N$. // $h^2 \equiv -1 \pmod N$
2: Compute $\rho = \gcd(N, h - \mathrm{i})$ by the Euclidean Algorithm in $\mathbb{Z}[\mathrm{i}]$.
3: Compute $c = \left(\frac{x}{\rho}\right)_4$ by applying Theorem 6 and Theorem 7.
4: **if** c == 1 **then**
5: Output "yes".
6: **else**
7: Output "no".
8: **end if**

Main Observation: 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 $\gcd(y, \rho) = \gcd(y, N) = 1$.

Examples

Table 1: Parameters of the SRSDP

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, $\mathscr{D}$ can efficiently calculate

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

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

Examples (cont'd)

Table 2: Procedures for calculating $\left(\frac{200003}{2815-288\mathrm{i}}\right)_4$

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

Security Analysis

Theorem 8

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*

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

The Power Residue Symbol

Let K be a number field and let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_K$ prime to an integer $\ell \geq 1$. We have

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

Definition 9

Suppose that $\zeta_\ell \in K$. We 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

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

Suppose 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

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

Computing Higher Power Residue Symbols

Theorem 10 (Kummer's Reciprocity Law)

Let ℓ be a regular prime number and let α and β be two primary elements in $\mathbb{Z}[\zeta_\ell]$. Then

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

Table 3: Algorithms for Computing the ℓ^{th} Power Residue Symbol

ℓ	3	5	7	11	13
References	[Williams85]	[ScheidlerW95]	[Caranay10]	[JoyeLNN2020]	[BrierD2019]

The general case of computing higher power residue symbols was tackled by de Boer and the resulting algorithms are probabilistic. For degrees around 100 the computation of one single power residue symbol might last for several weeks.

Attacking the SRSDP via the Power Residue Symbol

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:

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

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 $c = \left(\frac{x}{\mathfrak{a}}\right)_{p_0}$, it outputs "yes" if $c = 1$ and "no" otherwise.

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

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

Main Observation: If x is of the form $y^{p_0^d p_t q_t}$ with $y \in \mathcal{QR}_N$ then $c = 1$.

Security Analysis

Theorem 11

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*

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

Conclusion

- Description of higher residuosity attacks against two efficient two-party comparison protocols recently proposed by Carlton et al. and Bourse et al.
- (More results in the paper)

Future work will:

- investigate whether a more efficient algorithm exists for computing power residue symbols modulo a two-element representation ideal
- analyze other power-residuosity-type assumptions, such as the Gap 2^k-residuosity assumption, which underpins the security of the Joye-Libert cryptosystem

Comments/Questions?

Thank you!

zxp@dhu.edu.cn