Two-round Post-quantum Private Equality Test and OT from RLWE-encryption

Shengzhe Meng[1], Chengrui Dang[2], Bei Liang[2(✉)], and Jintai Ding[3]

[1] Department of Mathematical Sciences, Tsinghua University, 100084 Beijing, China
msz22@mails.tsinghua.edu.cn
[2] Beijing Institute of Mathematical Sciences and Application, China
lbei@bimsa.cn
[3] Yau Mathematical Sciences Center, Tsinghua University, 100084 Beijing, China
jintai.ding@gmail.com

Abstract. This work uses the RLWE-encryption scheme to construct a novel and efficient two-round post-quantum protocol for a private equality test(PET) between two parties. The basic idea of this protocol is that the private key holder can successfully decrypt a ciphertext only when the associated correct public key pair is used for encryption. In the protocol, only half of the public key pair will be published, while two parties will encode their private message to the other half of the public key pair. Leveraging this approach, we expand the protocol into two separate post-quantum two-round 1-out-of-2 Oblivious Transfer (OT) protocols. While prior OT schemes based on Public Key Encryption have significant communication overhead, our protocols provide novel and efficient frameworks for constructing OT from RLWE encryption. Additionally, our protocols are proven to be secure in a semi-honest adversary model, reflecting their robustness for practical post-quantum security applications. Our PET protocol is significantly more efficient than alternatives based on RLWE homomorphic encryption.

Keywords: RLWE · Equality Test · Oblivious Transfer · Post-quantum.

1 Introduction

A private equality test(PET) is a special secure computation problem. It enables two parties to ascertain if their private information matches without revealing it. This concept was initially introduced by Fagin, Naor, and Winkler [16]. A PET protocol can be a fundamental building block for other cryptographic protocols. For instance, it can be extended into an efficient Private Set Intersection (PSI) protocol using the cuckoo hashing technique as detailed in [36] or be integrated into a zero-knowledge proof protocol as proposed in [19]. Additionally, the application of the PET protocol has been explored in genomic computation [29] and in the realm of privacy-preserving data mining [20,24].

A naive solution of PET is for both parties to apply a cryptographic hash function to their input and then compare 2 hash values. This approach is efficient

but insecure if the input domain is not large enough or does not have high entropy. In this case, the party who receives the hash value could run a brute-force attack to obtain the private input of another party.

PET protocols have various implementation approaches. Protocols put forward by Naor and Pinkas [31] and Lipmaa [22] are constructed via the oblivious transfer technique. Further, Boudot et al. [8] and Mayer et al. [30] have built PET protocols utilizing Zero-Knowledge Proofs of Knowledge (ZKPOK)[15]. Magkos et al. [27] introduced a PET protocol that relies on public key encryption. Their protocol was proven secure under the Computational Diffie-Hellman (CDH) assumption. However, it is essential to note that these protocols will no longer be secure with the advent of quantum computers[43]. More recently, Saha and Koshiba [44,45] proposed PET protocols that homomorphically compute the Hamming distance between two private inputs using RLWE homomorphic encryption. Despite their quantum-resistant properties, it must be acknowledged that RLWE homomorphic encryption introduces substantial computational overhead. Therefore, in this paper, we intend to propose an efficient post-quantum PET protocol avoiding homomorphic encryption operation.

Oblivious transfer(OT) is a fundamental cryptographic primitive, first introduced by Rabin [39] and used as a building block in various other cryptographic protocols. It plays a crucial role in protocols for secure two-party and multi-party computation, including general secure computation protocols such as Yao's Garbled Circuits [46] and GMW [17], as well as special purpose protocols such as private set intersection [21,37,34,10,35,18,42,41,7]. The most commonly studied form of OT is 1-out-of-2 OT, where a sender with a pair of input string (x_0, x_1) interacts with a receiver who inputs a choice bit b. The goal of the protocol is that the receiver learns x_b without learning any information about x_{1-b}, while the sender learns nothing about b. There is an OT variant that is introduced by Beaver [4], called random OT (ROT). The ROT functionality is exactly the same as OT, except that the sender gets two random messages (x_0, x_1) and the receiver gets a random choice bit b and x_b as output.

Several OTs based on different cryptographic assumptions and adversarial models were introduced. In the semi-honest model, the most notable OT protocol is proposed by Naor-Pinkas [32], which has a cost of approximately 3 exponentiations per 1-out-of-2 OT and is among the most efficient today. However, such kind of cryptographic protocols based on discrete logarithm problems will suffer a polynomial-time quantum attack from Shor's algorithm [43]. Consequently, several post-quantum OT protocols have been proposed, including Peikert et al.'s lattice-based OT [38], code-based OTs [13,2], isogeny-based OTs [6,47,23].

Peikert et al. [38] propose a simple and general framework for constructing UC-secure OT protocols based on a dual-mode cryptosystem, which can be built upon various public-key cryptosystems. Barreto et al. [2] proposed another framework for obtaining OT, which is UC-secure against active adaptive adversaries from the public key encryption (PKE) scheme. By instantiating the frameworks of [38,2] under different hard problems, including the Diffie-Hellman

problem, quadratic residuosity problem, LPN problem, Learning with Errors (LWE) problem, etc., many OT protocols are obtained. However, those protocols have heavy communication overheads due to the usage of public key encryption systems, as public keys need to be sent between each other. Therefore, it is straightforward to consider if it is feasible to reduce the communication overhead by applying a more efficient cryptosystem to these frameworks.

RLWE problem introduced by Lyubashevsky, Peikert, and Regev [26] is a variant of the LWE problem, which enables us to construct more efficient and compact post-quantum cryptosystems. However, until now, it is unknown if it is possible to use the framework of [38] to construct an RLWE-based OT protocol since it has been unclear if there exists a dual-mode RLWE-PKE scheme. On the other hand, it is not applicable to instantiate the OT framework of [2] using the RLWE-PKE scheme since such a framework requires a group structure in the set of the public keys, whereas RLWE-PKEs do not have such a group structure. For this reason, we are motivated to propose a new OT construction method based on RLWE-PKE, which can be efficiently instantiated and implemented.

RLWE-based key exchange protocol [14] has been used to build a post-quantum UC-secure OT in the random oracle model[3,5]. Both OT protocols in [3,5] can be regarded as an adaption of the simplest OT protocols proposed by Chou and Orlandi [9] via using the RLWE key exchange instead of the Diffie-Hellman key exchange.

In this paper, we introduce innovative methods to construct protocols for PET and OT leveraging the RLWE encryption scheme. Our efforts are directed toward introducing new, post-quantum secure multi-party computation protocols, thereby contributing to the advancement of practical post-quantum cryptographic solutions.

1.1 Our Contributions and Techniques

This work introduces a novel 2-round private equality test protocol leveraging the RLWE encryption scheme. The basic idea of the protocol is that we assume the public keys in RLWE encryption are $a, as + 2e \in R_q$. We got a hash function H to convert the private messages x and y from each party into elements of R_q. Then, the first party will calculate the public keys $H(x), H(x)s + e$ while only publishing the second half of the public key to the other party. Without access to the first part of the public key $H(x)$, the second party must use the hash function H and his private input y to estimate the correct public key. He will then use the guessed public keys $H(y), H(x)s + 2e$ to encrypt some pre-determined message. The first party can decode and receive the correct message only when the other party uses the correct public key, which is only likely if x and y are identical. As a result, our protocol enables the parties to test for equality privately without revealing any additional information about their respective inputs. Furthermore, if the second party chooses the pre-determined message, the first party can receive the correct message only when they share the same input, x and y.

With this property, we extend this PET protocol into a 2-round 1-out-of-2 oblivious transform protocol. In the protocol, the receiver encodes his selection bits $s \in \{0, 1\}$ into public keys $H(s), H(s)s_r + 2e$ and only reveals the second part of the public key to the sender. The sender will guess the first part of the public key, which could be $H(0)$ or $H(1)$, and encrypt 2 OT messages m_0 and m_1. He will then send those two ciphertexts to the receiver. The receiver can only decrypt the ciphertext corresponding to his selection bit.

Notice that in our OT protocol, the sender has to send two ciphertexts to the receiver, while only one ciphertext can be decrypted by the receiver. In our improved OT protocol, we drew inspiration from the ideas presented in [5]. The receiver will set the public key $as + 2e$ as $as + 2e - h(r)$ when the selection bit is one and keep a and r as public. The sender will try to encrypt the OT messages m_0 and m_1 with the public key pair. In this case, the ciphertext $s_s m + e$ only needs to be sent to the receiver once.

Our PET protocol stands out for its exceptional efficiency compared to other RLWE-based protocols. Our protocol only requires a single round of RLWE encryption and decryption, whereas other protocols based on RLWE necessitate homomorphic operations. The computation cost of our PET protocol is only 4 multiplications in R_q and 5 random sampling from χ while the protocols provided by [44,45] require 3 homomorphic multiplications, 2 homomorphic additions, and 6 RLWE encryptions. At the same time, the communication overhead of our protocol is only 0.6 times that of theirs. Beyond efficiency, our PET protocol includes a unique feature. It allows both parties to obtain an identical message if their secret message is matched. With this property, we construct our 1-out-of-2 OT protocol. Our protocol has theoretical significance and provides a novel way to construct OT without [38,2] framework. We firmly believe that our PET protocol has further applications beyond its current scope, particularly as a foundational building block for more complex multi-party computation protocols. The potential for expansion and its flexibility present exciting avenues for future research and development in cryptographic techniques.

1.2 Paper Organization

Section 2 gives the security definition of PET, OT, and ROT. We will also introduce the RLWE problem in this section. We present our private equality test protocol from RLWE in Section 3. In Section 4, we provide a basic 1-out-of-2 oblivious transfer protocol based on the idea of the PET protocol. We also offer a more efficient 1-out-of-2 OT protocol in Section 5. We provide proof of security for the three protocols in the corresponding section. We analyze the complexity of communication and computation in Section 6.

2 Preliminary

2.1 Security Model

We define the security of a two-party protocol by following the definition of [33]. In a nutshell, security is defined by comparing two distributions of the outputs

of all parties in the real execution and the ideal model, respectively. In the real world, the corrupted party $\mathcal{A}$ runs the protocol by following some strategies, and the honest party runs the protocol honestly. We denote by $REAL_{\pi,\mathcal{A}}(x,y)$ the joint execution by protocol π in the real world, where inputs x and y are inputs of two parties. In the ideal world, we need to construct an algorithm $\mathcal{S}$ called a simulator for $\mathcal{A}$; $\mathcal{S}$ executes with input from the corrupted party and the output of the corrupted party in the ideal world. We denote by $IDEAL_{f,\mathcal{S}}(x,y)$ the joint execution of task f in the ideal world functionality, where inputs x and y are inputs of two parties. The protocol is secure if for every adversary $\mathcal{A}$, there exists a probabilistic polynomial time simulator $\mathcal{S}$, such that $REAL_{\pi,\mathcal{A}}(x,y) \stackrel{c}{=} IDEAL_{f,\mathcal{S}}(x,y)$. Hence, if a protocol is secure, the corrupted party cannot obtain more information about the real execution than in the ideal world.

The functionality is a secure computation task; it is defined as a trusted third party in the ideal world. $\mathcal{F}_{PET}$ enables one of the two parties to receive 0 if their private information matches without revealing it. $\mathcal{F}_{OT}$ allows the receiver to obtain one of two messages prepared by the sender. The functionality of $\mathcal{F}_{PET}$ and $\mathcal{F}_{OT}$ are detailed in Fig. 1 and Fig. 2 respectively.

Upon receiving (sid, x) from P_1 and (sid, y) from P_2, $\mathcal{F}_{PET}$ proceeds as follows:

- returns $(sid, 0)$ to P_1 if $x = y$.
- returns $(sid, 1)$ to P_1 if $x \neq y$.

Fig. 1. The functionality of $\mathcal{F}_{PET}$

Upon receiving (sid, x_0, x_1) from P_1 and (sid, b) from P_2, $\mathcal{F}_{OT}$ returns (sid, x_b) to P_2.

Fig. 2. The functionality of $\mathcal{F}_{OT}$

semi-honest model. A protocol is said to be secure under the semi-honest model if the adversary $\mathcal{A}$ is a passive adversary. $\mathcal{A}$ is not allowed to change the message during the execution, $\mathcal{A}$ runs the protocol honestly but tries to extract extra information after the execution of the protocol. We focus on this model in this paper.

2.2 Ring Learn With Errors

The ring learn with errors (RLWE) problem is introduced by Lyubashevsky, Peikert, and Regev [26]. This problem is the ring version of the learning with

errors (LWE) problem [40]. Let $f(X) = X^n + 1 \in \mathbb{Z}[X]$ and n is a power of 2. Let $q = 1 \mod 2n$ be a large public prime modulus. Let $R = \mathbb{Z}[X]/\langle f(X)\rangle$ and $R_q = R/\langle q\rangle = \mathbb{Z}_q[X]/\langle f(X)\rangle$. The element of R_q can be represented as a polynomial of degree less than n and coefficients ranging from $\{0, \cdots, q-1\}$. Let χ be a error distribution that satisfies $Pr[\|p\|_\infty > \beta : p \xleftarrow{\$} \chi] \leq negl(n)$ for some $\beta \in \mathbb{N}$. We usually use discrete Gaussian distribution in practical; we denote the standard deviation of the discrete Gaussian distribution as σ, hence $\chi = D_{\mathbb{Z}_n,\sigma}$. Let $\sigma = \alpha * q$. For $s \in R_q$ and choosing $a \xleftarrow{\$} R_q$, $e \xleftarrow{\$} \chi$, the RLWE distribution $A_{s,\chi}$ is $(a, as + e \mod q)$. The decision version of the ring learning with errors problem is defined below.

Definition 1 (RLWE problem). *Let n, q, χ be as above. Given $s \xleftarrow{\$} R_q$, distinguish whether it is given a polynomial number of samples from $A_{s,\chi}$ or uniformly chosen at random values from $R_q \times R_q$.*

When $\alpha q \geq 2\sqrt{n}$ and $q = poly(n)$, this problem is proven to be as hard as quantumly solving a worst-case lattice problem (the approximate Shortest Vector Problem (SVP) on ideal lattices) in [26]. In this paper, we use the Hermite Normal Form of the RLWE problem (HNF-RLWE). In this problem, s is sampled from χ instead of R_q. This problem is also assumed to be hard [1].

3 PET protocol from RLWE

Let n, q, R_q, χ, β as described in the previous section. Let A and B be two parties. Let $H()$ be a hash function with range R_q. In this protocol, A has an input x, and B has an input y. Before the protocol, we assume both parties share a message $m \in \{0,1\}^n$. Our new two rounds private equality test via RLWE is described below.

The Protocol. Initially, A will sample s_a and e_a from the error distribution χ, and B will sample s_b, e_b, and e_c from the same distribution. Then, A will transform her input x to an element of R_q by calculating $H(x)$. She will also calculate $P_a = H(x)s_a + 2e_a \mod q$. P_a can be viewed as half of the RLWE encryption public key, but the other public key $H(x)$ will be kept secret from B. A will transfer P_a to B. After receiving P_a, B will also transform his input y to an element of R_q by calculating $H(y)$. Without the other part of the public key $H(x)$, B will pretend the other part of the public key is $H(y)$ and calculate the encryption of m by the "public key" P_a and $H(y)$. Then B will transfer ciphertexts $c_1 = s_b P_a + m + 2e_b \mod q$ and $c_2 = s_b H(y) + 2e_c \mod q$ to A. A will decrypt the ciphertext with her private key s_a by calculating $m' = (c_1 - c_2 s_a) \mod q$. The correctness of the protocol is that:

$$m' = (c_1 - c_2 s_a) \mod q = s_b s_a (H(x) - H(y)) + m + 2 * error \mod q$$

The previous formula shows $m' = m$ if $x = y$. m' is not a short vector when $x \neq y$. Thus, A can determine whether $x = y$ by running our new PET protocol.

In simple terms, both parties do not need the public message m. They can set the message m as 0, so A only needs to check whether m' is a short vector in the last step. The protocol Π_{PET} is described below.

- Inputs:
  - Both parties: Ring R_q, a hash function $H : \{0,1\}^* \to R_q$, a error distribution χ, and some $m \in \{0,1\}^n$. m can be just set to 0 for convenience.
  - A: $x \in \{0,1\}^*$
  - B: $y \in \{0,1\}^*$
- Setup:
  - A samples $s_a, e_a \xleftarrow{\$} \chi$.
  - B samples $s_b, e_b, e_c \xleftarrow{\$} \chi$.
- Round 1:
  - A computes $P_a = H(x)s_a + 2e_a \mod q$ and sends P_a to B.
- Round 2:
  - B computes $c_1 = s_b P_a + m + 2e_b \mod q$.
  - B computes $c_2 = s_b H(y) + 2e_c \mod q$ and sends (c_1, c_2) to A.
- Output:
  - A computes $m' = c_1 - c_2 s_a \mod q$, if m' is short, output 0, else output 1.

Fig. 3. RLWE Private Equality Test Π_{PET}

Correctness We now show if A and B run the protocol honestly, they will know if $x = y$. The failure probability is the probability that A outputs incorrectly on the inputs x, y.

Lemma 1. *If $12n\beta^2 \leq q$, then the failure probability is negligible.*

Proof. If the protocol is executed correctly, then we have

$$\begin{aligned} m' &= c_1 - c_2 s_a - m \mod q \\ &= (s_b P_a + m + 2e_b) - (s_b H(y) + 2e_c)s_a - m \mod q \\ &= 2s_b e_a + 2e_b + 2s_a e_c \mod q \end{aligned} \tag{1}$$

From definitions in section 2.2, we have $\|s_b e_a + e_b + s_a e_c\| \leq 3n\beta^3$, then If $6n\beta^2 \leq q/2$, A will output correctly. □

Security. The proof of security follows the common security definitions of secure computation[33] for semi-honest adversaries.

Theorem 1. *The protocol Π_{PET} securely realizes the F_{PET} functionality against semi-honest adversaries, given that the HNF-RLWE assumption holds.*

Proof. We analyze two cases for the execution of the two-party PET protocol. Because F_{PET} is a deterministic functionality, the simulator outputs the simulated view of the adversary. The inputs of A and B are x and y.

Security against corrupted A. We first describe the simulator SIM for a corrupted A.

1. SIM starts by receiving b and x, where b is the output of $F_{PET}(x, y)$ to A, x is input of A.

2. if $b = 0$, then SIM sets $s_a, e_a \xleftarrow{\$} \chi$, $P_a = H(x)s_a + 2e_a \mod q$, and computes c_1, c_2 by following B in the real world with input x. SIM sets c_1, c_2 as the message the adversary receives.

In this case, the distribution of the simulated view is identical to that of the real execution.

3. if $b = 1$, SIM sets $s_a, e_a \xleftarrow{\$} \chi$, and sets $c_1, c_2 \xleftarrow{\$} R_q$ to be the message Adversary receives.

We now argue that the view of the adversary in the real execution of the protocol is indistinguishable from the simulated one. The proof follows from the following hybrid games.

Hybrid $\mathcal{H}_0$. The real-world execution of the protocol, the simulator interacts with A exactly as the honest B would do.

Hybrid $\mathcal{H}_1$. Identical to $\mathcal{H}_0$, except that if $b = 1$, the simulator samples $h \xleftarrow{\$} R_q$, and sets $c_2 = hs_b + 2e_c \mod q$

Hybrid $\mathcal{H}_2$. Identical to $\mathcal{H}_1$, except that if $b = 1$, the simulator sends $c_1, c_2 \xleftarrow{\$} R_q$ to Adversary.

The simulator in $\mathcal{H}_2$ is exactly SIM.

Lemma 2. *Hybrid games $\mathcal{H}_0$ and $\mathcal{H}_1$ are indistinguishable given that the HNF-RLWE assumption holds.*

Proof. First, when $b = 0$, the simulator in game $\mathcal{H}_2$ behaves the same as in $\mathcal{H}_0$.

When $b = 1$, which means $x \neq y$, the difference of $\mathcal{H}_1$ and $\mathcal{H}_2$ is h and $H(y)$. $H(y)$ and h are indistinguishable because that the output of hash function $H()$ is random in the view of corrupted A. Hence $\mathcal{H}_1$ and $\mathcal{H}_2$ are indistinguishable. □

Lemma 3. *Hybrid games $\mathcal{H}_1$ and $\mathcal{H}_2$ are indistinguishable given that the HNF-RLWE assumption holds.*

Proof. First, when $b = 0$, the simulator in game $\mathcal{H}_2$ behaves the same as in $\mathcal{H}_1$.

When $b = 1$, the differences lie on (c_1, c_2). In $\mathcal{H}_1$, $c_1 = s_b P_a + m + 2e_b \mod q$, $c_2 = hs_b + 2e_c \mod q$, where h and P_a are indistinguishable from random values sampled from R_q, and (c_1, c_2) are both RLWE samples. Hence, distinguishing $\mathcal{H}_1$ and $\mathcal{H}_2$ breaks the HNF-RLWE assumption by distinguishing an RLWE sample from a uniform value. □

In this case, the distribution of (c_1, c_2, P_a), which is the message A receives and sends, is indistinguishable from the uniform distribution by the HNF-RLWE assumption and the randomness of the output of the hash function. The simulator's output is identical to that of A in the real world. Hence, the distribution

of the simulated view is computationally indistinguishable from that of the real execution.

Security against corrupted B. Then we describe the simulator Sim for a corrupted B.

1. SIM starts by receiving y, where y is input of B.

2. SIM sets $P_a \xleftarrow{\$} R_q$ to be the message adversary receives, sets $s_b, e_b, e_c \xleftarrow{\$} \chi$.

Again, we argue the indistinguishability of the real and simulated view of corrupted B.

Hybrid $\mathcal{H}_0$. The real-world execution of the protocol, the simulator interacts with B exactly as the honest A would do.

Hybrid $\mathcal{H}_1$. Identical to $\mathcal{H}_0$, except that P_a is uniformly sampled from R_q. The simulator in $\mathcal{H}_1$ is exactly SIM.

Lemma 4. *Hybrid games $\mathcal{H}_0$ and $\mathcal{H}_1$ are indistinguishable given that the HNF-RLWE assumption holds.*

Proof. We can see $P_a = H(x)s_a + 2e_a \mod q$ in $\mathcal{H}_0$, where $H(x)$ is uniformly random in R_q, $s_a, e_a \xleftarrow{\$} \chi$. Hence, P_a is an RLWE sample. Clearly, distinguishing these two hybrid games is breaking the HNF-RLWE assumption. □

The distribution of the simulated view is computationally indistinguishable from that of the real execution under the HNF-RLWE assumption.

□

4 1-out-of-2 OT protocol from RLWE

In Section 3, we described a PET protocol from RLWE. Notice that the protocol we construct is more than a PET protocol. When B selects the public message m and keeps it secret from A, A can obtain the message m only when their secret messages x and y are the same. In this process, both parties will not leak their secret message. We will use this characteristic to construct a 1-out-of-2 OT protocol.

Let n, q, R_q, χ as described in the previous section. Sample $h_0, h_1 \xleftarrow{\$} R_q$ and set public. A 1 out of 2 OT protocol will occur between a receiver and a sender. The sender holds two messages $m_0, m_1 \in \{0,1\}^n$ and the receiver holds a selection bit $b \in \{0,1\}$. After the OT protocol, the receiver will obtain m_b and know nothing about m_{1-b}. Our new two rounds 1-out-of-2 OT protocol from RLWE is described below.

The Protocol. The receiver will sample s_r, e_r from the error distribution χ and the sender will sample $s_{s0}, s_{s1}, e_{s0}, e_{s1}, e_{s2}, e_{s3}$ from the distribution. Then, the receiver will calculate $P_r = h_b s_r + 2e_r \mod q$ and send P_r to the sender while keeping b secret. Since s_r is chosen by the receiver secretly, the sender cannot extract the selection bit b from P_r. Then the receiver will use the public key pairs $\{P_r, h_0\}$ and $\{P_r, h_1\}$ to encrypt messages m_0 and m_1 respectively. Only

$\{P_r, h_b\}$ is the valid public key pair the receiver can decrypt with his private key s_r. Thus, the receiver can only obtain m_b from the sender. The detailed protocol is described below.

- Inputs:
  - Both parties: Ring R_q, and random $h_0, h_1 \xleftarrow{\$} R_q$, a error distribution χ
  - Sender: $m_0, m_1 \in \{0,1\}^n$
  - Receiver: $b \in \{0,1\}$
- Setup:
  - Sender samples $s_{s0}, s_{s1}, e_{s0}, e_{s1}, e_{s2}, e_{s3} \xleftarrow{\$} \chi$.
  - Receiver samples $s_r, e_r \xleftarrow{\$} \chi$.
- Round 1:
  - Receiver computes $P_r = h_b s_r + 2e_r \mod q$ and sends P_r to Sender.
- Round 2:
  - Sender computes $c_{10} = s_{s0}P_r + m_0 + 2e_{s0} \mod q$, $c_{11} = s_{s1}P_r + m_1 + 2e_{s1} \mod q$, $c_{20} = s_{s0}h_0 + 2e_{s2} \mod q$, $c_{21} = s_{s1}h_1 + 2e_{s3} \mod q$ and sends $(c_{10}, c_{11}, c_{20}, c_{21})$ to Receiver.
- Output:
  - Receiver computes $m_b = (c_{1b} - c_{2b}s_r) \mod 2$ and output m_b.

Fig. 4. 1-out-of-2 OT Π_{OT}

Security. We prove the security of Π_{OT} under the HNF-RLWE assumption. The argument of hybrid games are similar to the previous proof of PET protocol, so we only present the construction of the simulator here.

Theorem 2. *The protocol Π_{OT} securely realizes the F_{OT} functionality against semi-honest adversaries, given that the HNF-RLWE assumption holds.*

Proof. We analyze two cases for the execution of the two-party OT protocol. Because F_{OT} is a deterministic functionality, the simulator outputs the simulated view of the adversary. The inputs of the Sender and Receiver are (m_0, m_1) and b.

Security against corrupted Sender. We first describe the simulator SIM for a corrupted sender.

1. SIM starts by receiving (m_0, m_1), the inputs of the Sender.

2. SIM sets $P'_r \xleftarrow{\$} R_q$ to be the message Sender receives, and samples $s_{s0}, s_{s1}, e_{s0}, e_{s1}, e_{s2}, e_{s3} \xleftarrow{\$} \chi$, and $c_{10}, c_{11}, c_{20}, c_{21}$ are computed following the protocol.

We now show that the view of the adversary in the real protocol is indistinguishable from the simulated one. The proof follows from the following hybrid games.

Hybrid $\mathcal{H}_0$. The real-world execution of the protocol, the simulator behaves as the honest Receiver.

Hybrid $\mathcal{H}_1$. Identical to $\mathcal{H}_0$, except that the simulator sets $P'_r \xleftarrow{\$} R_q$ and sends P'_r to Receiver.

The simulator in $\mathcal{H}_1$ is exactly SIM.

Lemma 5. *Hybrid games $\mathcal{H}_0$ and $\mathcal{H}_1$ are indistinguishable given that the HNF-RLWE assumption holds.*

Proof. The only difference between $\mathcal{H}_0$ and $\mathcal{H}_1$ is how P_r is generated. In $\mathcal{H}_0$, $P_r = h_b s_r + 2e_r$, and we know that (h_b, P_r) are computationally indistinguishable from (h_b, P'_r) under the HNF-RLWE assumption, where $P'_r \xleftarrow{\$} R_q$. Hence $\mathcal{H}_0$ and $\mathcal{H}_1$ are indistinguishable. □

Under the HNF-RLWE assumption, the distribution of the simulated view of the corrupted Sender is computationally indistinguishable from that of the real execution.

Security against corrupted Receiver. We then describe the simulator SIM for a corrupted sender.

1. SIM starts by receiving m_b and b, b is the input of the Receiver, m_b is the output of $F_{OT}((m_0, m_1), b)$ to Receiver.

2. SIM samples $s_r, e_r \xleftarrow{\$} \chi$, and computes $P_r = h_b s_r + 2e_r \mod q$ as the message Receiver sends to Sender.

3. SIM computes c_{1b} and c_{2b} by following the real execution, and sets $c_{0\ 1-b}, c_{1\ 1-b} \xleftarrow{\$} R_q$, as the message Receiver receives.

Again, we show that the views of the corrupt party are indistinguishable from those of the following hybrid games.

Hybrid $\mathcal{H}_0$. The real-world execution of the protocol, the simulator behaves as the honest Sender.

Hybrid $\mathcal{H}_1$. Identical to Hybrid game $\mathcal{H}_0$, except that simulator sets $c'_{1\ 1-b} \xleftarrow{\$} R_q$, to be the message Receiver receives.

The simulator in $\mathcal{H}_1$ is exactly SIM.

Lemma 6. *Hybrid games $\mathcal{H}_0$ and $\mathcal{H}_1$ are indistinguishable given that the HNF-RLWE assumption holds.*

Proof. In $\mathcal{H}_0$,

$$\begin{aligned} c_{1\ 1-b} &= s_{s\ 1-b} P_r + m_{1-b} + 2e_{s\ 1-b} \mod q \\ &= s_{s\ 1-b}(h_b s_r + 2e_r) + m_{1-b} + 2e_{s\ 1-b} \mod q \\ &= s_{s\ 1-b}(h_b s_r) + m_{1-b} + 2e_{s\ 1-b} + 2s_{s\ 1-b} e_r \mod q \\ c_{2\ 1-b} &= s_{s\ 1-b} h_{1-b} + 2e_{s\ 3-2b} \mod q \end{aligned}$$

It is clear that $h_b s_r$ and h_{1-b} are independent. Hence $(c_{1\ 1-b}, c_{2\ 1-b})$ are indistinguishable from $(c'_{1\ 1-b}, c'_{2\ 1-b})$ under the HNF-LWE assumption, and $\mathcal{H}_0$ and $\mathcal{H}_1$ are indistinguishable. □

The distribution of $(c_{1\ 1-b}, c_{1\ 1-b}, P_r)$ is computationally indistinguishable from $(c_{1\ 1-b}, c_{1\ 1-b}, P_r)$ in the real world under the HNF-RLWE assumption. Hence, the simulated view is computationally indistinguishable from the real execution. □

5 Improved 1-out-of-2 OT protocol from RLWE

Let n, q, R_q, χ as described in the previous section. In a 1-out-of-2 OT protocol, the receiver will input a selection bit $b \in \{0,1\}$, and the sender will input two messages $m_0, m_1 \in \{0,1\}^n$. After the OT protocol, the receiver will obtain m_b and know nothing about m_{1-b}. We assume both parties share random $m, t \in R_q$. Our new, improved 1-out-of-2 OT protocol from RLWE is described below.

The Protocol. The sender will sample $s_s, e_{s0}, e_{s1}, e_{s2} \xleftarrow{\$} \chi$, the receiver will sample $s_r, e_r \xleftarrow{\$} \chi$. s_s and s_r can be viewed as their secret key. If the selection bit $s = 0$, the receiver will calculate $P_r = ms_r + e_r \mod q$ and he will set $P_r = ms_r + 2e_r - t \mod q$ if $b = 1$. Then, he will send P_R to the sender. The sender cannot extract the selection bit b from the message. Then the sender will calculate a "encryption" of m_0 and m_1 by using the public key pair $\{m, P_r\}$ and $\{m, P_r + t\}$ respectively. When the selection bit $b = 0$, the ciphertext $\{S_0, S_2\}$ is valid, and the receiver can decrypt m_0 via secret key s_r. Otherwise, the ciphertext $\{S_1, S_2\}$ is valid, and the receiver can decrypt m_1 via secret key s_r. In this process, we prove that the message m_{1-b} will not leak to the receiver by the message S_{1-b}.

- Inputs:
  - Both parties: Ring R_q, and random $m, t \xleftarrow{\$} R_q$, a error distribution χ
  - Sender: $m_0, m_1 \in \{0,1\}^n$
  - Receiver: $b \in \{0,1\}$
- Setup:
  - Sender samples $s_s, e_{s0}, e_{s1}, e_{s2} \xleftarrow{\$} \chi$.
  - Receiver samples $s_r, e_r \xleftarrow{\$} \chi$.
- Round 1:
  - Receiver computes $P_r = ms_r + 2e_r \mod q$ if b = 0 while computes $P_r = ms_r + 2e_r - t \mod q$ if b = 1. The receiver sends P_r to the Sender.
- Round 2:
  - Sender computes $S_0 = s_s P_r + m_0 + 2e_{s0}$, $S_1 = s_s(P_r + t) + m_1 + 2e_{s1}$, $S_2 = s_s m + 2e_{s2}$ and sends (S_0, S_1, S_2) to Receiver.
- Output:
  - Receiver computes $m_b = S_b - S_2 s_R \mod 2$ and output m_b.

Fig. 5. Improved 1-out-of-2 OT Π'_{OT}

Security. We prove the semi-honest security of Π'_{OT}.

Theorem 3. *The protocol Π'_{OT} securely realizes the F_{OT} functionality against semi-honest adversaries under a random oracle model, given that the HNF-RLWE assumption holds.*

Proof. We construct a simulator that outputs the simulated view of the adversary. The inputs of the Sender and Receiver are (m_0, m_1) and b.

Security against corrupted Sender. We first describe the simulator SIM for a corrupted sender.

1. SIM starts by receiving (m_0, m_1), the inputs of sender.

2. SIM selects $P_r \xleftarrow{\$} \chi$, $t \xleftarrow{\$} R_q$,and sends (P_r, r) to Sender. SIM selects $s_s, e_{s0}, e_{s1}, e_{s2} \xleftarrow{\$} \chi$. The view of the Sender is computed following the protocol.

Next, we argue that the simulated view and the adversary's view are indistinguishable in the following hybrid games.

Hybrid $\mathcal{H}_0$. The real-world protocol, the simulator behaves as the honest Receiver.

Hybrid $\mathcal{H}_1$. Identical to $\mathcal{H}_0$, except that the simulator samples $P'_r \xleftarrow{\$} R_q$, and sends P'_r to Sender.

The simulator in $\mathcal{H}_1$ is exactly SIM.

Lemma 7. *Hybrid games $\mathcal{H}_0$ and $\mathcal{H}_1$ are indistinguishable given that the HNF-RLWE assumption holds.*

Proof. The only difference between $\mathcal{H}_0$ and $\mathcal{H}_1$ is the message the Receiver sends to the Sender. (m, P_r) are indistinguishable from (m, P'_r) according to the HNF-RLWE assumption. Hence, the view of the Sender in $\mathcal{H}_0$ and $\mathcal{H}_1$ are indistinguishable. □

Security against corrupted Receiver. We then describe the simulator SIM for a corrupted sender.

1. SIM starts by receiving m_b and b, b is the input of the Receiver, m_b is the output of $F'_{OT}((m_0, m_1), b)$ to Receiver.

2. SIM samples $s_r, e_r \xleftarrow{\$} \chi$, and computes P_r following the protocol, sets P_r as the message Receiver sends to Sender.

3. SIM samples $s_s, e_{s0}, e_{s1}, e_{s2} \xleftarrow{\$} \chi$, $S_{1-b} \xleftarrow{\$} R_q$, and computes S_b, S_{1-b} following the protocol, sets (S_0, S_1, S_2) as the message Sender sends to Receiver.

We then argue about hybrid games to prove that the views are indistinguishable.

Hybrid $\mathcal{H}_0$. In The real-world protocol, the simulator behaves as the honest Sender.

Hybrid $\mathcal{H}_1$. Identical to $\mathcal{H}_0$, except that the simulator samples $S'_{1-b} \xleftarrow{\$} R_q$ to be the message sent to Receiver.

The simulator in $\mathcal{H}_1$ is exactly SIM.

Lemma 8. *Hybrid games $\mathcal{H}_0$ and $\mathcal{H}_1$ are indistinguishable given that the HNF-RLWE assumption holds.*

Proof. In $\mathcal{H}_0$, We sets

$$S' = S_b - S_{1-b} = \pm s_s t + error \mod q$$

Since (t, m, P_r) are independent, (S_b, S_t, S_2) are indistinguishable from (S_b, S'_t, S_2) under the HNF-RLWE assumption, where $S'_t \xleftarrow{\$} R_q$. Hence $(S_b, S_b + S_t, S_3)$ are indistinguishable from $(S_b, S_b + S'_t, S_2)$. Because of $S'_t \xleftarrow{\$} R_q$ and $S'_{1-b} \xleftarrow{\$} R_q$, (S_b, S_{1-b}, S_3) are indistinguishable from (S_b, S'_{1-b}, S_2). So we can prove that $\mathcal{H}_0$ are indistinguishable from $\mathcal{H}_1$ □

In conclusion, the views of the adversary simulated by the above simulators are indistinguishable from that of the real execution under the HNF-RLWE assumption, □

6 Efficiency

Our PET protocol is significantly more efficient than alternatives based on RLWE homomorphic encryption[44,45]. Theoretically, our PET protocol only requires computing a single round of RLWE encryption and decryption. In contrast, other RLWE-based protocols need to perform homomorphic computations to determine the Hamming weight of two private messages, which incurs additional computational overhead. The communication cost of our protocol is a half public key along with a cipher-text, while other RLWE-based protocols need to transfer at least two cipher-texts. The comparison of communication and computational overhead between our PET protocol and other protocols is shown in Table 1. While our improved OT protocol introduces novel features, it does incur a higher communication cost, approximately $4n \log q$, compared to $2n \log q$ for OT protocols derived from RLWE key exchange. The theoretical communication and computation costs of our basic and improved 1-out-of-2 OT protocol are shown in Table 2. Given these considerations, in this section, we will focus exclusively on analyzing the parameters for our PET protocol. The aim is to transparently quantify the efficiency of our PET protocol in real-world settings, highlighting its potential for practical cryptographic applications.

Table 1. Communication complexity and computation complexity for our PET protocol and other protocols[44,45].

Scheme	Communication Cost	Computation Cost
Our protocol	$3n \log q$ bits	4 multiplications in R_q 5 samplings from χ
[44,45]	$5n \log q$ bits	3 homomorphic multiplications 2 homomorphic additions 6 encryptions

Table 2. Communication complexity and computation complexity for our basic and improved 1-out-of-2 OT protocol. Computational complexity is expressed in the number of multiplications in the ring R_q + the number of samplings from the distribution χ.

Scheme	Communication Cost	Computation Cost
1-out-of-2 OT protocol	$5n \log q$ bits	6+8
Improved 1-out-of-2 OT protocol	$4n \log q$ bits	5+6

Parameter selection. We analyze the RLWE parameters (n, q, σ) of PET following the work of [29]. The parameters should be chosen to ensure correctness and security; we have analyzed the correctness of the PET protocol in Lemma 1, and then we will analyze security. The parameters will be selected against several attacks on the general RLWE problem; for more details, the reader is referred to [28] and [25].

security. The security of LWE based cryptography scheme can be measured by the root Hermite factor. According to the analysis of the distinguishing attack, for given parameters (n, q, σ), we have the relation:

$$c \cdot q/\sigma = 2^{2\sqrt{n \log q \log \delta}} \tag{2}$$

Where δ is the root Hermite factor, c is determined by the attack advantage ϵ, $c \approx \sqrt{\log(1/\epsilon)/\log 2 \cdot \pi}$, we choose $c = 3.758$ corresponding to $\epsilon = 2^{-64}$.

Parameter. As in [29], We choose $\sigma = 8$ against combinatorial style attacks. combining the results of lemma 1, we have $12n^2\sigma^2 \leq q$. Hence, we can calculate q from σ and n, then we calculate δ root Hermite factor from equation (2).

We set $n = 2^{11}$, $q \approx 2^{61}$ and $\sigma = 8$ and those parameters are as same as[45]. According to the state-of-the-art security analysis of Chen and Nguyen [11], if the root Hermite factor is less than 1.0050, the scheme is estimated to have more than 80-bits security level.

7 Conclusions

This paper presents a novel, secure, post-quantum PET protocol from RLWE encryption. Our protocol stands out due to its simplicity and efficiency. It allows two parties to compare their secret messages with the approximately same computational cost of a single round RLWE encryption. Our new PET protocol is six times faster than the exciting RLWE-based PET protocols. We further demonstrate the versatility of our protocol: it is more than a mere tool for comparison. Two parties can derive a shared message when their secret message is identical. With this feature, We construct two novel OT protocols from RLWE encryption, independent of established frameworks. Our research underscores the potential of our PET protocol as a fundamental component for developing a spectrum of multi-party computation protocols. We also aim to adapt other post-quantum encryption methods to our PET protocol, diversifying our suite of tools and further enhancing efficiency in secure multi-party computation.

Acknowledgments. This work is supported by National Key R&D Program of China (No. 2021YFB2701304).

References

1. Applebaum B, Cash D, Peikert C, et al. Fast cryptographic primitives and circular-secure encryption based on hard learning problems[C]//Advances in Cryptology-CRYPTO 2009: 29th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2009. Proceedings. Springer Berlin Heidelberg, 2009: 595-618.
2. Barreto PSLM, David B, Dowsley R, et al. A framework for efficient adaptively secure composable oblivious transfer in the ROM[J]. arXiv preprint arXiv:1710.08256, 2017.
3. Branco P, Ding J, Goulao M, et al. Universally composable oblivious transfer protocol based on the RLWE assumption[J]. Cryptology ePrint Archive, 2018.
4. Beaver D. Precomputing oblivious transfer[C]//Annual International Cryptology Conference. Berlin, Heidelberg: Springer Berlin Heidelberg, 1995: 97-109.
5. Branco P, Fiolhais L, Goulão M, et al. Roted: Random oblivious transfer for embedded devices[J]. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2021: 215-238.
6. Barreto P, Nascimento A, Oliveira G, et al. Supersingular Isogeny Oblivious Transfer (SIOT)[J]. arXiv preprint arXiv:1805.06589, 2018.
7. Bienstock A, Patel S, Seo J Y, et al. Near-Optimal Oblivious Key-Value Stores for Efficient PSI, PSU and Volume-Hiding Multi-Maps[J]. Cryptology ePrint Archive, 2023.
8. Boudot F, Schoenmakers B, Traore J. A fair and efficient solution to the socialist millionaires' problem[J]. Discrete Applied Mathematics, 2001, 111(1-2): 23-36.
9. Chou T, Orlandi C. The simplest protocol for oblivious transfer[C]//Progress in Cryptology–LATINCRYPT 2015: 4th International Conference on Cryptology and Information Security in Latin America, Guadalajara, Mexico, August 23-26, 2015, Proceedings 4. Springer International Publishing, 2015: 40-58.
10. Chase M, Miao P. Private set intersection in the internet setting from lightweight oblivious PRF[C]//Advances in Cryptology–CRYPTO 2020: 40th Annual International Cryptology Conference, CRYPTO 2020, Santa Barbara, CA, USA, August 17–21, 2020, Proceedings, Part III 40. Springer International Publishing, 2020: 34-63.
11. Chen Y, Nguyen P Q. BKZ 2.0: Better lattice security estimates[C]//International Conference on the Theory and Application of Cryptology and Information Security. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011: 1-20.
12. David B, Dowsley R, Nascimento A C A. Universally composable oblivious transfer based on a variant of LPN[C]//International Conference on Cryptology and Network Security. Cham: Springer International Publishing, 2014: 143-158.
13. David B M, Nascimento A C A, Müller-Quade J. Universally composable oblivious transfer from lossy encryption and the McEliece assumptions[C]//International Conference on Information Theoretic Security. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012: 80-99.
14. Ding J, Xie X, Lin X. A simple provably secure key exchange scheme based on the learning with errors problem[J]. Cryptology ePrint Archive, 2012.
15. Fiege U, Fiat A, Shamir A. Zero knowledge proofs of identity[C]//Proceedings of the nineteenth annual ACM symposium on Theory of computing. 1987: 210-217.

16. Fagin R, Naor M, Winkler P. Comparing information without leaking it[J]. Communications of the ACM, 1996, 39(5): 77-85.
17. Goldreich O, Micali S, Wigderson A. How to play ANY mental game[C]//Proceedings of the nineteenth annual ACM symposium on Theory of computing. 1987: 218-229.
18. Garimella G, Pinkas B, Rosulek M, et al. Oblivious key-value stores and amplification for private set intersection[C]//Advances in Cryptology–CRYPTO 2021: 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16–20, 2021, Proceedings, Part II 41. Springer International Publishing, 2021: 395-425.
19. Jakobsson M, Yung M. Proving without knowing: On oblivious, agnostic and blindfolded provers[C]//Annual International Cryptology Conference. Berlin, Heidelberg: Springer Berlin Heidelberg, 1996: 186-200.
20. Kantarcioglu M, Kardes O. Privacy-preserving data mining in the malicious model[J]. International Journal of Information and Computer Security, 2008, 2(4): 353-375.
21. Kolesnikov V, Kumaresan R, Rosulek M, et al. Efficient batched oblivious PRF with applications to private set intersection[C]//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. 2016: 818-829.
22. Lipmaa H. Verifiable homomorphic oblivious transfer and private equality test[C]//Advances in Cryptology-ASIACRYPT 2003: 9th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, November 30–December 4, 2003. Proceedings 9. Springer Berlin Heidelberg, 2003: 416-433.
23. Lai Y F, Galbraith S D, Delpech de Saint Guilhem C. Compact, efficient and UC-secure isogeny-based oblivious transfer[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. Cham: Springer International Publishing, 2021: 213-241.
24. Lindell Y, Pinkas B. Secure Multiparty Computation for Privacy-Preserving Data Mining[J]. Journal of Privacy and Confidentiality, 2009, 1(1).
25. Lindner, Richard & Peikert, Chris. (2010). Better Key Sizes (and Attacks) for LWE-Based Encryption.. IACR Cryptology ePrint Archive. 2010. 592.
26. Lyubashevsky V, Peikert C, Regev O. On ideal lattices and learning with errors over rings[C]//Advances in Cryptology–EUROCRYPT 2010: 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, May 30–June 3, 2010. Proceedings 29. Springer Berlin Heidelberg, 2010: 1-23.
27. Magkos E, Kotzanikolaou P, Magioladitis M, et al. Towards secure and practical location privacy through private equality testing[C]//Privacy in Statistical Databases: UNESCO Chair in Data Privacy, International Conference, PSD 2014, Ibiza, Spain, September 17-19, 2014. Proceedings. Springer International Publishing, 2014: 312-325.
28. D. Micciancio and O. Regev, "Worst-case to average-case reductions based on Gaussian measures," 45th Annual IEEE Symposium on Foundations of Computer Science, Rome, Italy, 2004, pp. 372-381.
29. Masaya Yasuda, Takeshi Shimoyama, Jun Kogure, Kazuhiro Yokoyama, and Takeshi Koshiba. 2013. Secure pattern matching using somewhat homomorphic encryption. In Proceedings of the 2013 ACM workshop on Cloud computing security workshop (CCSW '13). Association for Computing Machinery, New York, NY, USA, 65–76. https://doi.org/10.1145/2517488.2517497

30. Mayer D A, Wetzel S. Verifiable private equality test: enabling unbiased 2-party reconciliation on ordered sets in the malicious model[C]//Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security. 2012: 46-47.
31. Naor M, Pinkas B. Oblivious transfer and polynomial evaluation[C]//Proceedings of the thirty-first annual ACM symposium on Theory of computing. 1999: 245-254.
32. Naor M, Pinkas B. Efficient oblivious transfer protocols[C]//SODA. 2001, 1: 448-457.
33. Oded Goldreich. The Foundations of Cryptography - Volume 2: Basic Applications[M]. Cambridge University Press,2004.
34. Pinkas B, Rosulek M, Trieu N, et al. SpOT-light: lightweight private set intersection from sparse OT extension[C]//Advances in Cryptology–CRYPTO 2019: 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18–22, 2019, Proceedings, Part III 39. Springer International Publishing, 2019: 401-431.
35. Pinkas B, Rosulek M, Trieu N, et al. PSI from PaXoS: fast, malicious private set intersection[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. Cham: Springer International Publishing, 2020: 739-767.
36. Pinkas B, Schneider T, Zohner M. Faster private set intersection based on OT extension[C]//23rd USENIX Security Symposium (USENIX Security 14). 2014: 797-812.
37. Pinkas B, Schneider T, Zohner M. Scalable private set intersection based on OT extension[J]. ACM Transactions on Privacy and Security (TOPS), 2018, 21(2): 1-35.
38. Peikert C, Vaikuntanathan V, Waters B. A framework for efficient and composable oblivious transfer[C]//Annual international cryptology conference. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008: 554-571.
39. Rabin M O. How to Exchange Secrets with Oblivious Transfer[J]. 1981.
40. Regev O. On lattices, learning with errors, random linear codes, and cryptography[C]//Proceedings of the thirty-seventh annual ACM symposium on Theory of computing. 2005: 84-93.
41. Raghuraman S, Rindal P. Blazing fast PSI from improved OKVS and subfield VOLE[C]//Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security. 2022: 2505-2517.
42. Rindal P, Schoppmann P. VOLE-PSI: fast OPRF and circuit-PSI from vector-OLE[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. Cham: Springer International Publishing, 2021: 901-930.
43. Shor P W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer[J]. SIAM review, 1999, 41(2): 303-332.
44. Saha T K, Koshiba T. Private equality test using ring-LWE somewhat homomorphic encryption[C]//2016 3rd Asia-Pacific World Congress on Computer Science and Engineering (APWC on CSE). IEEE, 2016: 1-9.
45. Saha T K, Koshiba T. Outsourcing private equality tests to the cloud[J]. Journal of information security and applications, 2018, 43: 83-98.
46. Yao A C C. How to generate and exchange secrets[C]//27th annual symposium on foundations of computer science (Sfcs 1986). IEEE, 1986: 162-167.
47. Vanessa Vitse. Simple oblivious transfer protocols compatible with supersingular isogenies. In AFRICACRYPT 2019, volume 11627 of Springer LNCS, pages 56–78, 2019.