A LWE-based Oblivious Transfer Protocol from Indistinguishability Obfuscation

Shanshan Zhang[1,2]
(Corresponding author: Shanshan Zhang)

State Key Laboratory of Integrated Services Networks, Xidian University[1]
No. 2, Taibai South Road, Xi'an 710071, Shaanxi Province, China
School of Mathematics and Information Science, Baoji University of Arts and Sciences[2]
No. 44, Baoguang Road, Baoji 721013, Shaanxi Province, China
(Email: sszhang0801@163.com)
(Received Mar. 18, 2019; Revised and Accepted Aug. 4, 2019; First Online Jan. 29, 2020)

Abstract

Oblivious transfer is an important cryptographic primitive and served as a powerful tool in secure computation. Most existing oblivious transfer protocols are built upon the hardness of factoring or computing discrete logarithm problem. However, threatened by quantum computing, these protocols will be broken down directly in the presence of quantum computer. Therefore, it is essential to construct OT protocol based on post-quantum cryptography. As a subarea of post-quantum cryptography, lattice-based cryptography has some attractive features. Specifically, the learning with errors (LWE) problem has been used as an amazingly versatile basic tool to design cryptographic schemes. We are inspired by a result which proposed an oblivious transfer protocol using the decisional Diffie-Hellman assumption and indistinguishable obfuscation. Therefore, we propose a new secure LWE-based oblivious transfer protocol from indistinguishability obfuscation. The main tools consist of LWE-based dual-mode cryptosystem and a secure indistinguishability obfuscation which guarantee the security of our oblivious transfer protocol.

Keywords: Dual-mode Cryptosystem; Indistinguishability Obfuscation; Lattice-based; Oblivious Transfer

1 Introduction

Oblivious transfer (OT) is a fundamental cryptographic primitive, first proposed by Rabin [13] in 1981. It contains two participants, a sender (denoted by **S**), and a receiver (denoted by **R**), and requires that **S** sends a message to **R** with probability 1/2, while **S** is oblivious to whether or not the message was received by **R**. A well-known flavor of OT is called 1-out-of-2 OT (denoted by OT_1^2), where **S** has two inputs m_0 and m_1, and **R** has a chosen bit $b \in \{0, 1\}$, and **R** wishes to obtain m_b, without **S** learning b, while **S** wants to ensure that **R** receives only one of the two messages. Due to the simple functionality of OT, it has been widely exploited to construct cryptographic schemes, such as contract signing, secure multi-party computation, the exchange of secrets, and key agreement. Therefore, it is of great significance to design efficient OT protocols.

1.1 Our Motivation

As far as we know, most existing OT protocols are built upon number theoretical problems mainly consist of the hardness of factoring and computing discrete logarithm problem. However, threatened by quantum computing [16], these protocols will be broken down directly in the presence of quantum computer. Therefore, it is essential to construct OT protocol based on post-quantum cryptography, such as lattice-based protocol and code-based protocol. Lattice-based cryptography has some attractive properties when compared with other post-quantum research fields, for instance, strong security guarantees from worst-case hardness and algorithmic simplicity. Among lattice-based hard problems, the learning with errors (LWE) problem [14] has been used as an amazingly versatile basic tool to design cryptographic schemes. Specifically, Peikert *et al.* [11] proposed an efficient and universally composable OT protocol which is extracted from a dual-mode cryptosystem and can be instantiated with the decisional Diffie-Hellman assumption, the quadratic residuosity assumption and the worst-case lattice assumption, respectively.

Zheng *et al.* [17] researched the framework for composable oblivious transfer and proposed a secure OT protocol from indistinguishability obfuscation (iO), with a dual-mode cryptosystem and an iO as main technical tools. Their work mainly has the following contributions. First, a k-out-of-n OT protocol was presented. Second, it explored the applications of iO. iO is a weaker notation of obfuscation that was first formally defined by [2]. They suggested a definition of virtual black box obfuscation, and proved that this notion is impossible to realize. In order to avoid the impossibility result, they presented the notion of iO, which only requires that if two circuites compute the same functionality, then their obfuscation should be computational indistinguishable from each other. iO is both very useful and potentially achievable. Garg *et al.* [7] proposed the first candidate GGH13-based [6] iO for general circuits. Subsequently, many applications of iO were described in [15], such as public encryption, injective trapdoor function, deniable encryption, and so on.

The OT protocol of Zheng *et al.* has a main tool that is based on the hardness of the decisional Diffie-Hellman (DDH) problem. However, DDH assumption does not guarantee against quantum attack, and the selection of iO is the first candidate that have been attacked by [4]. For these reasons, we aim to remedy the insufficiency and try to design another new OT protocol that is security in quantum setting. Therefore, we take advantage of the LWE problem and a secure iO. Furthermore, if the security of OT protocol is proved only according to an ideal world simulator that is shown only for a cheating receiver, then they are not necessarily secure when integrated into a lager protocol. Thus, our protocol needs to satisfy the property of universally composable simultaneously.

1.2 Our Contribution

In this work, we combine LWE-based dual-mode cryptosystem [11] and a secure iO to design a new OT protocol. The key technique is an obfuscator of the dual-mode cryptosystem based on the hardness of LWE, versus based on DDH assumption in [17]. It is important that we choose GGH13-based obfuscator which against quantum attack when combined with the technique of [5] to prevent input partitioning. By utilizing these tools, we realize the oblivious transform functionality, and guarantee security of our OT protocol.

1.3 Organization

The rest of this paper is organized as follows. In Section 2, we introduce two useful definitions of LWE and iO. Then two corresponding building blocks are given in Section 3. In Section 4, we construct an LWE-based oblivious transfer protocol from iO, and the security proof of our OT protocol is presented in Section 5. Finally, conclusions are drawn in Section 6.

2 Preliminares

In this section, we introduce some notations and fundamental definitions.

2.1 Notation

We let $\mathbb{N}$ denote the set of natural numbers, for $n \in \mathbb{N}$, $[n]$ denotes the set $\{1, \ldots, n\}$. For an integer $q \geq 1$, $\mathbb{Z}_q$ denotes the quotient ring $\mathbb{Z}/q\mathbb{Z}$. Let " $\leftarrow$ " denote sampling an element from some distribution uniformly at random. We use bold lower-case letters to denote vectors in column form, and bold upper-case letters to denote matrices. Let $n \in \mathbb{N}$ denote the security parameter throughout this paper, and all other quantities are functions of n. We use standard notation o to classify the growth of functions, the function $\text{negl}(n)$ denotes an unspecified function $f(n) = o(n^{-c})$ for some constant $c > 0$, calling $\text{negl}(n)$ is negligible, and we say a probability is overwhelming if it is 1-$\text{negl}(n)$. We use the definition of computational indistinguishability, denoted by $\stackrel{c}{\approx}$.

2.2 Learning with Errors

The LWE problem was proposed by Regev [14], the hardness of it can be reduced by a quantum algorithm to some standard problems on lattices in the worst case.

For an integer $q = q(n) \geq 2$ and some probability distribution χ over $\mathbb{Z}_q$, we define $A_{s,\chi}$ as the distribution on $\mathbb{Z}_q^n \times \mathbb{Z}_q$ of the tuples $(\mathbf{a}, c) = (\mathbf{a}, \mathbf{a}^T\mathbf{s} + e)$ where $\mathbf{s}, \mathbf{a} \leftarrow \mathbb{Z}_q^n$ is uniform and $e \leftarrow \chi$, and all operations are performed in $\mathbb{Z}_q$. There are two versions of the LWE problem, search-LWE and decision-LWE, respectively.

Definition 1 (Search-LWE and decision-LWE)**.** *For an integer $q = q(n)$ and a distribution χ on $\mathbb{Z}_q$, for any $\mathbf{s} \in \mathbb{Z}_q^n$, search-LWE finds $\mathbf{s}$ given any independent samples $(\mathbf{a}, c)$ from $A_{s,\chi}$. The goal of decision-LWE is to distinguish between an oracle that returns independent samples from $A_{s,\chi}$ for some uniform $\mathbf{s} \leftarrow \mathbb{Z}_q^n$, and an oracle that returns independent samples from the uniform distribution on $\mathbb{Z}_q^n \times \mathbb{Z}_q$.*

Regev showed that these two versions are polynomially equivalent for $q = poly(n)$. He proved that for certain choices of q and χ, the decision-LWE problem is as hard as solving the shortest independent vectors problem (SIVP) using a quantum algorithm.

Theorem 1. *Let $q = q(n)$ be a prime and let $\alpha = \alpha(n) \in (0, 1)$ such that $\alpha q > 2\sqrt{n}$. If there exists an efficient algorithm that solves the decision-LWE problem, then there exists an efficient quantum algorithm for the SIVP within $\widetilde{O}(n/\alpha)$ in the worst case.*

Due to the hardness of SIVP, we choose the decision-LWE problem as underlying hardness in this paper.

2.3 Indistinguishability Obfuscation

Program obfuscation aims to make computer programs "unintelligible" while preserving their functionality. The systematic study of program obfuscation was initiated by Barak *et al.* in 2001. In their work, they gave a potentially realizable notion of iO. iO requires that, given any two equivalent circuits of the same size, the obfuscation of these two circuits should be computationally indistinguishable. The specific definition is as follows.

Definition 2 (Indistinguishiability obfuscation). *A PPT algorithm iO is said to be an indistinguishability obfuscator for a class of circuits $\mathbb{C}$, if it satisfies:*

Functionality: For any $C \in \mathbb{C}$ and security parameter n,

$$Pr[\forall x : iO(C, 1^n)(x) = C(x)] = 1.$$

Indistinguishability: For any PPT distinguisher D, there exists a negligible function $negl(\cdot)$, such that for any two circuits $C_0, C_1 \in \mathbb{C}$ that compute the same function are of the same size:

$$|Pr[D(iO(C_0, 1^n)) = 1] - Pr[D(iO(C_1, 1^n)) = 1]|$$

$$\leq negl(n).$$

Starting with the work of [7] constructing the first iO candidate for the polynominal-size circuit. Several iO candidates have appeared in literatures [1,3,9,10]. Unfortunately, many constructions are attacked by [10]. So we choose a secure iO [12] based on GGH13 multilinear map that haven't found classical attack and quantum attack.

3 Building Blocks

In order to construct an LWE-based oblivious transfer protocol from iO, we need two building blocks, including LWE-based dual-mode cryptosystem and a secure iO.

3.1 LWE-based Dual-mode Cryptosystem

The dual-mode cryptosystem is a simple and general framework, proposed by Peikert *et al.* [11]. Actually it is an encryption scheme that can operate in two modes, which are called *messy mode* and *decryption mode*. The trusted setup phase produces a common reference string (denoted by crs) and the corresponding trapdoor information according to one of two chosen modes. The crs may be uniformly random or be some specified distribution.

The dual-mode cryptosystem has four security properties:

1) It suffices decryption completeness with overwhelming probability over the randomness of the entire experiment;

2) Given crs, the first outputs of SetupMessy and SetupDec are computationally indistinguishable;

3) In Messy mode, for every pk, at least one of the derived public keys can statistically hide its encrypted message;

4) In decryption mode, the honest receiver's chosen bit σ is statistically hidden by its choice or the base key pk.

These security properties make the dual-mode cryptosystem able to derive a UC-secure OT protocol.

The instantiation of the dual-mode cryptosytem based on the hardness of LWE relies on existing techniques, including an LWE-based encryption and an efficient securely embedded a trapdoor algorithm. So, we first introduce an optimized version of the LWE-based encryption, then instancing the dual-mode cryptosystem, where the message space is $\mathbb{Z}_2 = \{0, 1\}$. Let the modulus $q = \text{poly}(n)$ be a prime, all operations are performed over $\mathbb{Z}_q$. For every message $M \in \mathbb{Z}_2$, the "center" of M is defined as $t(M) = M \cdot \lfloor q/2 \rfloor \in \mathbb{Z}_q$. Let χ denote an error distribution over $\mathbb{Z}_q$.

LWEKeyGen (1^n): Choose a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ and a secret key $\mathbf{s} \leftarrow \mathbb{Z}_q^{n\times 1}$ are both uniformly at random. To generate the public key, choose an error vector $\mathbf{x} \leftarrow \mathbb{Z}_q^{1\times m}$ where each entry $x_i \in \chi$ is chosen independently for all $i \in [m]$. Then compute $\mathbf{p} = \mathbf{s}^T\mathbf{A} + \mathbf{x}$, the public key is $(\mathbf{A}, \mathbf{p})$.

LWEEnc $((pk = (\mathbf{A}, \mathbf{p}), M)$: To encrypt a message $M \in \mathbb{Z}_2$, choose a vector $\mathbf{e} \in \mathbb{Z}_2^m$ uniformly at random. The ciphertext is the pair $(\mathbf{u}, c) = (\mathbf{Ae}, \mathbf{pe} + M \cdot \lfloor q/2 \rfloor) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$.

LEWDec $((sk = \mathbf{s}, (\mathbf{u}, c)))$: Compute $d = c - \mathbf{s}^T\mathbf{u} \in \mathbb{Z}_q$, output 0 if d is closer to 0 than $\lfloor q/2 \rfloor$ modulo q, otherwise output 1.

We verify the completeness of the encryption scheme based on the LWE. The decryption algorithm needs to compute

$$d = c - \mathbf{s}^T\mathbf{u} = (\mathbf{s}^T\mathbf{A} + \mathbf{x})\mathbf{e} + M \cdot \lfloor q/2 \rfloor - \mathbf{s}^T\mathbf{Ae}$$

$$= \mathbf{xe} + M \cdot \lfloor q/2 \rfloor \in \mathbb{Z}_q.$$

If $\mathbf{xe} + M \cdot \lfloor q/2 \rfloor$ is closer to 0 than $\lfloor q/2 \rfloor$ modulo q, then output 0, otherwise output 1.

The encryption scheme based on the LWE is secure under chosen plaintext attack, unless SIVP and GapSVP are easy for quantum algorithms.

We now give the construction of the LWE-based dual-mode cryptosystem using LWE-based encryption. It consists six probabilistic algorithms, and the last two algorithms are only used in the security proof.

SetupMessy (1^n): Choose a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ uniformly at random, together with a trapdoor $t = \{\mathbf{S}, \mathbf{A}\}$ as in [8]. Choose a row vector $\mathbf{w} \leftarrow \mathbb{Z}_q^{1\times m}$. For each $b \in \{0, 1\}$, choose an independent row vector $\tau_b \in \mathbb{Z}_q^{1\times m}$ uniformly at random. Let $crs = (\mathbf{A}, \tau_1, \tau_2)$ and output (crs, t).

SetupDec (1^n): Choose a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ and a row vector $\mathbf{w} \leftarrow \mathbb{Z}_q^{1\times n}$ are both at random. For each $b \in \{0, 1\}$, choose a secret $\mathbf{s}_b \leftarrow \mathbb{Z}_q^n$ and an error row vector $\mathbf{x}_b \leftarrow \chi$ are both uniformly at random. Let $\tau_b = s_b^T A + x_b - \mathbf{w}$, $crs = (\mathbf{A}, \tau_1, \tau_2)$, $t = (\mathbf{w}, \mathbf{s}_0, \mathbf{s}_1)$ and output (crs, t).

KeyGen (σ)**:** Choose a secret $\mathbf{s} \leftarrow \mathbb{Z}_q^n$ uniformly at random and a row vector $\mathbf{x} \leftarrow \chi^{1\times m}$. Let $pk = \mathbf{s}^T\mathbf{A} + \mathbf{x} - \tau_\sigma$, $sk = \mathbf{s}$, and output (pk, sk).

Enc(pk, b, M)**:** Output $y \leftarrow \text{LWEEnc}(\mathbf{A}, pk + \tau_b, M)$, where y is the pair $(\mathbf{u}, c)$.

Dec(sk, y)**:** Output $M \leftarrow \text{LWEDec}(sk, (\mathbf{u}, c))$.

Findmessy(t, pk)**:** Parse t as $(\mathbf{S}, \mathbf{A})$, run ISMessy $(\mathbf{S}, \mathbf{A}, pk + \tau_b)$ for each $b \in \{0, 1\}$, and output a b such that IsMessy can output messy on at least one branch correctly with overwhelming probability.

TrapKeyGen(t)**:** Parse t as $(\mathbf{w}, \mathbf{s}_0, \mathbf{s}_1)$, and output $(pk, sk_0, sk_1) = (\mathbf{w}, \mathbf{s}_0, \mathbf{s}_1)$.

According to [8], we know an efficient and UC-secure OT protocol based on LWE hardness can be directly derived when the LWE-based dual-mode cryptosystem built well. Although the LWE-based dual-mode cryptoystem is a relaxed version, it can still derive a UC-secure OT protocol based on the LWE hardness.

3.2 Secure Indistinguishability Obfuscation

In this section, we introduce a secure iO as another tool in our scheme. Indistinguishability obfuscation is a powerful notion, which holds for every pair functionally equivalent circuits C_0, C_1 that $iO(C_0)$ and $iO(C_1)$ are computationally indistinguishable. Almost all known candidate constructions of iO are based on multilinear-maps, which have been the subjects of various attacks. The first candidate branching program obfuscator can be attacked when the branching program has input partitioning. So we combine it with the prevent input partitioning technique to against cryptanalytic attacks.

In this section, we introduce the secure iO for all circuits. Firstly, we need to construct iO for NC^1 circuit. More specifically, an NC^1 circuit can be computed by branching programs. Let $f : \{0,1\}^n \rightarrow \{0,1\}$ be a function to be obfuscated. Fernando *et al.* [5] give a model which takes partitionable f as input and produces a function g with the same functionality, where g has no input partitions exist. In this way, GGH13 - based iO can defence the extension of annihilation attacks by [4]. Secondly, using iO for NC^1 circuit together with Fully Homomorphic Encryption (FHE) to achieve iO for all circuits. The process contains an obfuscation algorithm and an evaluation algorithm. To obfuscate a circuit C, we choose and publish two FHE keys PK_0 and PK_1. Obfuscate$(1^\lambda, C \in \mathbb{C}_\lambda)$, then output $\tau = (P, PK_{FHE}^1, PK_{FHE}^2, g_1, g_2)$, where $P = iO_{NC^1}(P1^{SK_{FHE}^1}, g_1, g_2)$, $g_1 = \text{Encrypt}_{FHE}(P1^{SK_{FHE}^1}, C)$ and $g_2 = \text{Encrypt}_{FHE}(P1^{SK_{FHE}^2}, C)$. We describe the two program classes in Figure 1 and Figure 2. The evaluate algorithm takes in the obfuscation output τ and program input M, denoted by Evaluate(τ, M). Compute the following procedure, where U_λ is a poly-sized universal circuit.

$P1$

Given input (M, e_1, e_2, ϕ), $(P1^{SK_{FHE}^1, g_1, g_2})$ proceeds as follows:
1. Check if ϕ is a valid low-depth proof for the NP-statement:

$$e_1 = \text{Eval}_{FHE}(PK_{FHE}^1, U_\lambda(\cdot, M), g_1),$$
$$e_2 = \text{Eval}_{FHE}(PK_{FHE}^2, U_\lambda(\cdot, M), g_2).$$

2. If the check fails output 0; otherwise, output

$$\text{Decrypt}_{FHE}(e_1, \text{SK}_{FHE}^1).$$

Figure 1: Program P1

$P2$

Given input (M, e_1, e_2, ϕ), $(P2^{SK_{FHE}^2, g_1, g_2})$ proceeds as follows:
1. Check if ϕ is a valid low-depth proof for the NP-statement:

$$e_1 = \text{Eval}_{FHE}(PK_{FHE}^1, U_\lambda(\cdot, M), g_1),$$
$$e_2 = \text{Eval}_{FHE}(PK_{FHE}^2, U_\lambda(\cdot, M), g_2).$$

2. If the check fails output 0; otherwise, output

$$\text{Decrypt}_{FHE}(e_2, \text{SK}_{FHE}^2).$$

Figure 2: Program P2

1) Compute
$$e_1 = \text{Eval}_{FHE}(PK_{FHE}^1, U_\lambda(\cdot, M), g_1),$$
$$e_2 = \text{Eval}_{FHE}(PK_{FHE}^2, U_\lambda(\cdot, M), g_2).$$

2) Compute a low depth proof ϕ that e_1 and e_2 were computed correctly.

3) Run $P(M, e_1, e_2, \phi)$ and output the result.

4 LWE-based Oblivious Transfer Protocol from Indistinguishability Obfuscation

4.1 Obfuscator for LWE-based Dual-mode Cryptosystem

The setup of a dual-mode cryptosystem has messy mode and decrytion mode, and they are computationally indistinguishable. Therefore, their obfuscating results are still indistinguishable. We know SetupMessy and SetupDec have two choices respectively, denoted as four circuits C_n that describe in Figure 3, 4, 5, 6, where $n = 1, 2, 3, 4$. We obfuscate these circuits to substitute the two modes in LWE-based dual-mode cryptosystem. The key is to describe the four circuits C_n, that are based on LWE encryption scheme.

The circuit C_1 and C_2 output truly random vectors, and the circuit C_3 and C_4 output LWE instantiations. Through obfuscating these circuits C_1, C_2, C_3 and C_4, we obtain the result that their outputs are computationally indistinguishable. The specific setup of the LWE-based dual-mode cryptosystem are called two obfuscation branches as follows.

Messy-obf-branch (1^n): Choose a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ uniformly at random, together with a trapdoor $t = \{\mathbf{S}, \mathbf{A}\}$ as in [8]. Choose a row vector $\mathbf{w} \leftarrow \mathbb{Z}_q^{1\times m}$. For each $b \in \{0, 1\}$, choose a secret $\mathbf{s}_b \leftarrow \mathbb{Z}_q^n$ and an error row vector $\mathbf{x}_b \leftarrow \chi$ are both uniformly at random. Let $\tau_1 = \text{Obfuscate}(1^\lambda, C_1)$, $\tau_2 = \text{Obfuscate}(1^\lambda, C_2)$, $crs = (\mathbf{A}, \tau_1, \tau_2)$ and output (crs, t).

Dec-obf-branch (1^n): Choose a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ and a row vector $\mathbf{w} \leftarrow \mathbb{Z}_q^{1\times n}$ are both uniformly at random. For each $b \in \{0, 1\}$, choose a secret $\mathbf{s}_b \leftarrow \mathbb{Z}_q^n$ and an error row vector $\mathbf{x}_b \leftarrow \chi$ are both uniformly at random. Let $\tau_1 = \text{Obfuscate}(1^\lambda, C_3)$, $\tau_2 = \text{Obfuscate}(1^\lambda, C_4)$, $crs = (\mathbf{A}, \tau_1, \tau_2)$, $t = (\mathbf{w}, \mathbf{s}_0, \mathbf{s}_1)$ and output (crs, t).

Next, we invoke the evaluate algorithm in KeyGen process, where we let $V_0 = \text{Obfuscate}(\tau_1, \mathbf{A})$ and $V_1 = \text{Obfuscate}(\tau_2, \mathbf{A})$. Comparing to the above LWE-based dual-mode cryptosystem, the rest of the steps are identical except that $\mathbf{V}_\sigma$ is substituted for $\mathbf{v}_\sigma$.

Circuit C_1

Input: choose a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ and a row vector $\mathbf{w} \leftarrow \mathbb{Z}_q^{1\times m}$ are both uniformly at random. Choose a secret $\mathbf{s}_0 \leftarrow \mathbb{Z}_q^n$ and an error row vector $\mathbf{x}_0 \leftarrow \chi^{1\times m}$ are all uniformly at random.
Output: a row vector $\mathbf{v}_0 \leftarrow \mathbb{Z}_q^{1\times m}$ uniformly at random.

Figure 3: Circuit C_1

Circuit C_2

Input: choose a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ and a row vector $\mathbf{w} \leftarrow \mathbb{Z}_q^{1\times m}$ are both uniformly at random. Choose a secret $\mathbf{s}_1 \leftarrow \mathbb{Z}_q^n$ and an error row vector $\mathbf{x}_1 \leftarrow \chi^{1\times m}$ are both uniformly at random.
Output: a row vector $\mathbf{v}_1 \leftarrow \mathbb{Z}_q^{1\times m}$ uniformly at random.

Figure 4: Circuit C_2

Circuit C_3

Input: choose a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ and a row vector $\mathbf{w} \leftarrow \mathbb{Z}_q^{1\times m}$ are both uniformly at random. Choose a secret $\mathbf{s}_0 \leftarrow \mathbb{Z}_q^n$ and an error row vector $\mathbf{x}_0 \leftarrow \chi^{1\times m}$ are both uniformly at random.
Output: $\mathbf{v}_0 = \mathbf{s}_0^T\mathbf{A} + \mathbf{x}_0 - \mathbf{w}$.

Figure 5: Circuit C_3

Circuit C_4

Input: choose a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ and a row vector $\mathbf{w} \leftarrow \mathbb{Z}_q^{1\times m}$ are both uniformly at random. Choose a secret $\mathbf{s}_1 \leftarrow \mathbb{Z}_q^n$ and an error row vector $\mathbf{x}_1 \leftarrow \chi^{1\times m}$ are both uniformly at random.
Output: $\mathbf{v}_1 = \mathbf{s}_1^T\mathbf{A} + \mathbf{x}_1 - \mathbf{w}$.

Figure 6: Circuit C_4

4.2 Oblivious Transfer Protocol from Indistinguishability Obfuscation

OT_1^2 is a two-party protocol, involving a sender **S** inputs M_0, M_1 and a receiver **R** inputs a choice bit $\sigma \in \{0, 1\}$. The result is that **R** learns M_σ and nothing about another message, while **S** learns nothing at all. Our OT protocol operate in the common reference string model, denoted by F_{crs}^D, where D denotes a PPT algorithm. F_{crs}^D runs with two parties and there is a trusted party which can produce crs for two parties before interacting. Once the obfuscator for LWE-based dual-mode cryptosystem is constructed well, our LWE-based OT protocol from iO denoted by $iO\text{dm}^{\text{branch}}$ can be derived directly, we describe the protocol in Table 1. It can realize the exact definition of the ideal OT functionality in the F_{crs}^D. $iO\text{dm}^{\text{branch}}$ operates in two branches, when D=Messsy-obf-branch, D runs in the Messsy-obf-branch; when D=Dec-obf-branch, D runs in the Dec-obf-branch.

Table 1: Protocol $iO\mathsf{dm}^{\mathsf{branch}}$ for oblivious transfer

Sender $(\mathsf{sid}, \mathsf{ssid}, M_0, M_1)$		**Receiver** $(\mathsf{sid}, \mathsf{ssid}, \sigma)$
Setup:		
	$\underset{(\mathsf{sid}, crs)}{\overset{(\mathsf{sid}, \mathbf{S}, \mathbf{R})}{\rightleftarrows}} F^{D}_{crs} \underset{(\mathsf{sid}, crs)}{\overset{(\mathsf{sid}, \mathbf{S}, \mathbf{R})}{\leftrightarrows}}$	
Multi-session OT:		
	$\xleftarrow{(\mathsf{sid}, \mathsf{ssid}, pk)}$	$(pk, sk) \leftarrow$ KeyGen-obf-branch(crs, σ)
$y_b \leftarrow \mathsf{Enc}(pk, b, M_b)$ for each $b \in \{0, 1\}$	$\xrightarrow{(\mathsf{sid}, \mathsf{ssid}, y_0, y_1)}$	outputs $(\mathsf{sid}, \mathsf{ssid}, \mathsf{Dec}(sk, y_\sigma))$

5 Security Proof

Obfuscator for LWE-based dual-mode cryptosystem includs two obf-branches, the trapdoor generation of keys in Dec-obf-branch, and the guaranteed existence and identification of messy branches in Messy-obf-branch. Its properties take the form of theorem as follows.

Theorem 2. *In the obfuscator for LWE-based encryption scheme construction, the Messy-obf-branch and Dec-obf-branch are indistinguishability, assuming LWE is hard.*

Proof. The output of Dec-obf-branch is of form $(\mathbf{A}, (\mathbf{s}_0^T\mathbf{A}+\mathbf{x}_0)-\mathbf{w}, (\mathbf{s}_1^T\mathbf{A}+\mathbf{x}_1)-\mathbf{w})$. Because of the hardness of LWE, we have $(\mathbf{A}, \mathbf{s}_1^T\mathbf{A}+\mathbf{x}_1) \overset{c}{\approx} (\mathbf{A}, \mathbf{w}_1)$, where $\mathbf{w}_1 \leftarrow Z_q^{1\times m}$ is uniformly random and independent. So we have $(\mathbf{A}, (\mathbf{s}_0^T\mathbf{A}+\mathbf{x}_0)-\mathbf{w}, (\mathbf{s}_1^T\mathbf{A}+\mathbf{x}_1)-\mathbf{w}) \overset{c}{\approx} (\mathbf{A}, (\mathbf{s}_0^T\mathbf{A}+\mathbf{x}_0)-\mathbf{w}, \mathbf{w}_1-\mathbf{w})$. The right side of the vector equation is totally uniform, because $\mathbf{w}$ and $\mathbf{w}_1$ are uniform and independent. By the output of Messy-obf-branch is entirely uniform, thus $(\mathbf{A}, (\mathbf{s}_0^T\mathbf{A}+\mathbf{x}_0)-\mathbf{w}, (\mathbf{s}_1^T\mathbf{A}+\mathbf{x}_1)-\mathbf{w}) \overset{c}{\approx} (\mathbf{A}, \mathbf{v}_0, \mathbf{v}_1)$. □

Theorem 3. *In the obfuscator for LWE-based encryption scheme construction satisfying for every $(crs, t) \leftarrow Dec-obf-branch(1^n)$, $TrapKenGen(t)$ outputs (pk, sk_0, sk_1) such that for every $\sigma \in \{0, 1\}$, $(pk, sk_\sigma) \approx KeyGen(\sigma)$, assuming LWE is hard.*

Proof. The case $\sigma = 0$ and $\sigma = 1$ are symmetrically, so we consider only one of them. Given the case $\sigma = 0$, we will prove that

$$(Dec-obf-branch(1^n), KeyGen(0)) \overset{c}{\approx} (crs, (pk, sk_0)),$$

where $(crs, t) \leftarrow Dec-obf-branch(1^n)$ and $(pk, sk_0, sk_1) \leftarrow TrapKeyGen(t)$. We get the result using a sequence of hybrid games. □

By the outputs of these two branches are indistinguishable, we have the first hybrid game expands as

$$(\mathbf{A}, \mathbf{v}_0, \mathbf{v}_1, \mathbf{s}^T\mathbf{A}+\mathbf{x}-\mathbf{v}_0, \mathbf{s}),$$

where $\mathbf{A}, \mathbf{v}_0, \mathbf{v}_1$ and $\mathbf{s}$ are uniform and $\mathbf{x} \leftarrow \chi^{1\times m}$.

Through defining $\mathbf{w} = \mathbf{s}^T\mathbf{A}+\mathbf{x}-\mathbf{v}_0$ and using $\mathbf{s}_0$ and $\mathbf{x}_0$ replace $\mathbf{s}$ and $\mathbf{x}$, the second game outputs

$$(\mathbf{A}, \mathbf{s}_0^T\mathbf{A}+\mathbf{x}_0-\mathbf{w}, \mathbf{v}_1, \mathbf{w}, \mathbf{s}_0),$$

where $\mathbf{w}$ is uniform. Because $\mathbf{v}_1$ is uniform and independent of the other variables, the third game outputs

$$(\mathbf{A}, \mathbf{s}_0^T\mathbf{A}+\mathbf{x}_0-\mathbf{w}, \mathbf{v}_1-\mathbf{w}, \mathbf{w}, \mathbf{s}_0).$$

The above three games are equivalent to each other.

The hardness of LWE implies that $(\mathbf{A}, \mathbf{v}_1)$ is distinguishable from $(\mathbf{A}, \mathbf{s}_1^T\mathbf{A}+\mathbf{x}_1)$, where $\mathbf{s}_1 \leftarrow Z_q^n$ and $\mathbf{x}_1 \leftarrow \chi^{1\times m}$. So the prior games are indistinguishable from the one that outputs

$$(\mathbf{A}, \mathbf{s}_0^T\mathbf{A}+\mathbf{x}_0-\mathbf{w}, \mathbf{s}_1^T\mathbf{A}+\mathbf{x}_1-\mathbf{w}, \mathbf{w}, \mathbf{s}_0).$$

This is the whole process, the final output is equivalent to $(crs, (pk, sk_0))$ by definition.

Theorem 4. *In the obfuscator for LWE-based encryption scheme construction using the parameters $m \geq 2(n+1)logq$ and $t \geq \sqrt{qm}\cdot log^2 m$, for $(crs, t) \leftarrow$ Messy-obf-branch(1^n) and every key pk, FindMessy(t, pk) outputs a messy branch with overwhelming probability.*

Proof. In [8], the facts are as follows. Let $m \geq 2(n+1)logq$ and $t \geq \sqrt{qm}\cdot log^2 m$, there is a negligible function $negl(m)$ such that with overwhelming probability over the choice of $\mathbf{A}, \mathbf{S}$, for all but an at most $(1/2\sqrt{q})^m$ fraction of vectors $\mathbf{p} \in Z_q^{1\times m}$, Ismessy$(\mathbf{S}, \mathbf{A}, \mathbf{p})$ outputs messy with overwhelming probability. Define $D \subseteq Z_q^{1\times m}$ to be the set of vectors $\mathbf{p}$, then we have

$$Pr[\mathbf{v} \notin D] \leq (1/2\sqrt{q})^m, \text{where } \mathbf{v} \in Z_q^{1\times m}.$$

□

For every $pk \in Z_q^{1\times m}$, there is a branch $pk+\mathbf{v}_b \in M$, where $b \in \{0, 1\}$ and $\mathbf{v}_0, \mathbf{v}_1 \in Z_q^{1\times m}$ in the crs. For any fixed pk, we have

$$Pr[pk+\mathbf{v}_0 \notin M \text{ and } pk+\mathbf{v}_1 \notin D]$$
$$= (Pr[\mathbf{v} \notin D])^2 \leq (1/4q)^m.$$

For $(crs, t) \leftarrow$ Messy-obf-branch(1^n) and every key pk, FindMessy(t, pk) outputs a messy branch with overwhelming probability, because of both branches lie outside D is at most $(1/4)^m$=negl(n).

From the above, we draw a conclusion that the obfuscator for LWE-based encryption scheme is a slightly relaxed dual-mode cryptosystem. On the basis of it, we obtain an OT protocol. The protocol operates in either obf-branches, which are obfuscation of the dual-mode encryption branches. The OT protocol based on dual-mode securely realizes the functionality F_{OT}. Therefore, our LWE-based oblivious transfer protocol from indistinguishability obfuscation is secure.

6 Conclusions

We can see that most existing OT protocols are based on the hardness of number theoretical problems. In this paper, we propose a secure LWE-based oblivious transfer protocol from iO, and give the proof of security. In addition to iO, our protocol is based on LWE-based dual-mode encryption, which is a framework for efficient and composable oblivious transfer. Thus, our protocol can realize the oblivious transform functionality. Compared with the protocol of Zheng *et al.*, our protocol is secure in the quantum environment. At present, using punctured programs technique to carry out some applications of iO gradually become a central primitive for cryptography, so we would like to use this technique to build another secure, efficient, and succinct oblivious transfer protocol.

Acknowledgments

This study was supported by the National Key R&D Program of China under Grant No.2017YFB0802000, the National Natural Science Foundations of China under Grant Nos.61972457, 61672412, 61402015, U1736111, the National Cryptography Development Fund under grant No.MMJJ20170104, the MOE Layout Foundation of Humanities and Social Sciences under Grant 19YJA790007, and the Research Program of Baoji University of Arts and Sciences under Grant No.ZK2018093. I acknowledge the anonymous reviewers for their valuable comments.

References

[1] S. Badrinarayanan, E. Miles, A. Sahai, and M. Zhandry, "Post-zeroizing obfuscation: New mathematical tools, and the case of evasive circuits," in *Advances in Cryptology*, pp. 764–791, 2016.

[2] B. Barak, O. Goldreich, R. Impagliazzo, S. Rudich, A. Sahai, S. Vadhan, and K. Yang, "On the (im)possibility of obfuscating programs," in *Advances in Cryptology*, pp. 1–18, 2001.

[3] N. Bitansky and V. Vaikuntanathan, "Indistinguishability obfuscation from functional encryption," in *Proceedings of the IEEE 56th Annual Symposium on Foundations of Computer Science (FOCS'15)*, pp. 171–190, 2015.

[4] Y. L. Chen, C. Gentry, and S. Halevi, "Cryptanalyses of candidate branching program obfuscators," in *Advances in Cryptology*, pp. 278–307, 2017.

[5] R. Fernando, P. M. R. Rasmussen, and A. Sahai, "Preventing CLT attacks on obfuscation with linear overhead," in *Advances in Cryptology*, pp. 242–271, 2017.

[6] S. Garg, C. Gentry, and S. Halevi, "Candidate multilinear maps from ideal lattices," in *Advances in Cryptology*, pp. 1–17, 2013.

[7] S. Garg, C. Gentry, S. Halevi, M. Raykova, A. Sahai, and B. Waters, "Candidate indistinguishability obfuscation and functional encryption for all circuits," in *IEEE 54th Annual Symposium on Foundations of Computer Science*, pp. 40–49, 2013.

[8] C. Gentry, C. Peikert, and V. Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions," in *Proceedings of 40th Annual ACM Symposium on Theory of Computing*, pp. 197–206, 2008.

[9] H. Lin, "Indistinguishability obfuscation from constant-degree graded encoding schemes," in *Advances in Cryptology*, pp. 28–57, 2016.

[10] E. Miles, A. Sahai, and M. Zhandry, "Annihilation attacks for multilinear maps: Cryptanalysis of indistinguishability obfuscation over GGH13," in *Advances in Cryptology*, pp. 629–658, 2016.

[11] C. Peikert, V. Vaikuntanathan, and B. Waters, "A framework for efficient and composable oblivious transfer," *LNCS*, vol. 5444, no. 72, pp. 554–571, 2009.

[12] A. Pellet-Mary, "Quantum attacks against indistinguishablility obfuscators proved secure in the weak multilinear map model," in *Advances in Cryptology – CRYPTO 2018*, pp. 153–183, 2018.

[13] M. O. Rabin, "How to exchange secrets by oblivious transfer," *Technical Report*, 1981. (`https://eprint.iacr.org/2005/187.pdf`)

[14] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," in *Proceedings of 37th Annual ACM Symposium on Theory of Computing*, pp. 84–93, 2005.

[15] A. Sahai and B. Waters, "How to use indistinguishability obfuscation: Deniable encryption, and more," *Proceedings of the Annual ACM Symposium on Theory of Computing*, pp. 475–484, 2014.

[16] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Review*, vol. 41, no. 2, pp. 303–332, 1999.

[17] Y. Zheng, W. Mei, and F. Xiao, "Secure oblivious transfer protocol from indistinguishability obfuscation," *The Journal of China Universities of Posts and Telecommunications*, vol. 23, no. 3, pp. 1–10, 2016.

Biography

Shanshan Zhang received her B.S. degree in 2004 from Baoji University of Arts and Sciences, and received her M.S. degree in 2007 from Huaibei Normal University. Now she is a PhD student in Xidian University. Her main research interests include public key cryptography and indistinguishable obfuscation.