Heuristic Ideal Obfuscation Based on Evasive LWR-Based Multilinear Maps and Its Underlying Problem Reduction

Zhuang Shan\textsuperscript{1}[0000–0003–4309–4505], Leyou Zhang\textsuperscript{1,*}[0000–0003–4950–1140], and Qing Wu\textsuperscript{2}[0000–0002–9400–236X]

\textsuperscript{1} School of Mathematics and Statistics, Xidian University, Xi’an 710126, China
\texttt{arcsec30@163com, lyzhang@mail.xidian.edu.cn}
\textsuperscript{2} School of Automation, Xi’an University of Posts and Telecommunications, Xi’an 710121, China
\texttt{xiyouwuq@126.com}

Abstract. This paper introduces a heuristic ideal obfuscation scheme grounded in the learning problem, which differs from that proposed by Jain, Lin, and Luo [JLLW23]. The approach in this paper follows a methodology akin to that of Brakerski, Dottling, Garg, and Malavolta [BDGM22,BDGM20] for building iO. We construct a new ideal obfuscation by leveraging a variant of LWR to build LHE and employing Evasive LWR to construct multilinear maps. In contrast to the methodology of Jain et al., this paper provides a more detailed approach. Initially, we reprove the hardness of LWR using the prime number theorem and the fixed-point theorem, showing that the statistical distance between $\lfloor As \rfloor_p$ and $\lfloor u \rfloor_p$ does not exceed $\exp\left(-\frac{n \log_2 n \log p}{\sqrt{5}}\right)$ when the security parameter $q > 2^n p$. Additionally, we provide definitions for Evasive LWR and composite homomorphic pseudorandom function, and based on these, we construct multilinear maps, thereby establishing the ideal obfuscation scheme proposed in this paper.

Keywords: Ideal obfuscation · Split FHE · Multilinear maps · Lattice problem reduction · Evasive Lattice.

1 Introduction

In 2000, Hada[Had00] first introduced the definition of virtual black box obfuscation, which is essential for embedding a circuit $C$ into an opaque black
box that cannot be opened. By inputting $x$ into one end of the black box, the other end automatically outputs $C(x)$. Since the entire circuit is hidden inside the black box, no specific information about the construction of $C$ can be obtained. The only action we can take is to provide input and observe the output on the other side.

VBB functions like a virtualized black box, where a circuit $C$ obfuscated by VBB prevents us from obtaining any information related to its construction through the obfuscated output. The only action possible is to provide input $x$ and compute $C(x)$ [Yue20]. Unfortunately, Barak et al. [BGI+01] have proven that virtual black box obfuscation does not exist.

In 2001, while Barak et al. proved the nonexistence of virtual black box obfuscation, they also presented a new definition for obfuscation: to obfuscate two circuits $C_1$ and $C_2$ such that the obfuscated circuits have the same functionality and an adversary cannot distinguish between the two circuits. This is known as indistinguishable obfuscation.

In 2013, Garg et al. introduced indistinguishable obfuscation based on multilinear maps [GGH+13b] and applied it to functional encryption. It is noteworthy that multilinear maps were also proposed by Garg et al. [GGH13a]. Subsequently, significant work using program obfuscation (e.g., [BZ17,GGHR14,SW21]) has shown that most interesting cryptographic applications can be realized using iO (and one-way functions).

Due to its importance, many scholars have begun to focus on researching how to construct indistinguishable obfuscation. One construction method is based on new multilinear maps, which extends its applicability to a wider range [GGH13a,CLT13,GGH15]. However, in 2016, Hu and Jia [HJ16] broke the indistinguishable obfuscation based on multilinear maps proposed by Garg et al. [GGH13a]. In the same year, Miles, Sahai, and Zhandry [MSZ16] partially broke another indistinguishable obfuscation scheme by Garg et al. [GGH+13b]. Since 2015, the field of obfuscation with multilinear pairings has entered a cycle where proposed schemes are quickly broken, leading to improvements based on the attacks, only to be broken again shortly thereafter.

Recently, Bitansky and Vaikuntanathan [BV18] and Ananth and Jain [AJ15] have independently proven through different methods that when Compact FE (Functional Encryption with compact ciphertexts) exists, then indistinguishable obfuscation can be achieved. Based on these results, the current construction
methods for indistinguishable obfuscation mainly fall into two categories, namely:

1. The first approach is to restrict the depth of multilinear maps to achieve indistinguishable obfuscation. For example, in 2016, Lin restricted the depth to 5 layers [Lin17], and later with Tessaro restricted it to 3 layers [LT17]. In 2020, Jain, Lin, and Sahai [JLS21] successfully constructed indistinguishable obfuscation based on bilinear pairings, LWE, LPN[YZ21], and sPFG.

2. The second approach is to achieve indistinguishable obfuscation through splitting fully homomorphic encryption. For example, Brakerski, Dottling, Garg, and Malavolta [BDGM22,BDGM20] combined fully homomorphic encryption (FHE) with leveled homomorphic encryption (LHE) (Damgård-Jurik). By cleverly leveraging circular-security assumptions, they enable ciphertexts to circulate between the two encryption systems, ultimately constructing indistinguishable obfuscation.

In 2023, Jain, Lin, and Luo introduced a new concept called ideal obfuscation [JLLW23]. This concept is a refinement of Jain’s work on indistinguishable obfuscation.

1.1 Our work

New LWR reduction The LWR problem is a variant of the LWE problem [Reg04], while being reduced to the SVP and CVP problem. In 2012, Banerjee, Peikert, and Rosen first proposed this problem, which is primarily used to construct pseudorandom functions and deterministic encryption [XXZ12]. In 2013, Alwen and others used information entropy theory to reduce the learning with rounding problem to the learning with errors problem, indirectly leading to a reduction to the SVP and CVP in lattices, and requires $q > \beta 2^n p$.

In 2024, Dr. Chen [Che24] published an article on quantum algorithms for LWE, although there are some issues with the proof process, but this also serves as a warning that not all lattice problems can be reduced to LWE. Therefore, this paper redefines the LWR problem without using any intermediate problems as reduction bridges. Instead, it calculates the maximum statistical distance between $\lfloor A \rfloor_p$ and $\lfloor u \rfloor_p$.

Define $S_q$ as the probability set for any $i \in \mathbb{Z}_q$, undoubtedly, $\Pr(i) = \frac{1}{q}$, for all $i \in \mathbb{Z}_q$. $S_q[i] = \Pr(i)$. Now, calculate the value when $Pr(i) \in \overline{S}_q := S_q \times S_q$. 

Define $S_q$ as the probability set for any $i \in \mathbb{Z}_q$, undoubtedly, $\Pr(i) = \frac{1}{q}$, for all $i \in \mathbb{Z}_q$. $S_q[i] = \Pr(i)$. Now, calculate the value when $Pr(i) \in \overline{S}_q := S_q \times S_q$. 

Since $\Pr(i)$ is related to the prime factorization of $i$, the value of $\Pr(i)$ is given based on the prime number theorem and the theory of prime factorization. Define its maximum value as $\Pr(A)$, with the corresponding element $A \in \mathbb{Z}_q$. At this point, we are calculating the probability of $a_1 s_1 = b_1 \rightarrow \mathbb{Z}_q$, then we calculate $\Pr(i) \in (\mathbb{S}_q + \mathbb{S}_q)$, which is the probability of $a_1 s_1 + a_2 s_2 = b_2 \rightarrow \mathbb{Z}_q$, and so on. We find that this relationship is consistent with the relationship $i_{n+1} = T_i n_i$, where

$$T_i = \begin{pmatrix}
  i^{(1)}_n & i^{(q)}_n & \cdots & i^{(2)}_n \\
  i^{(2)}_n & i^{(1)}_n & \cdots & i^{(3)}_n \\
  \vdots & \vdots & \ddots & \vdots \\
  i^{(q)}_n & i^{(q-1)}_n & \cdots & i^{(1)}_n
\end{pmatrix},$$

$i^{(j)} = \Pr(j)$. So the idea arose whether we could leverage the theory of fixed points to prove the convergence of this sequence, and perhaps even establish the hardness of LWR? Indeed, it is affirmative, because $T_i n_i$ satisfies the conditions of the fixed-point theorem, namely, $T_i n_i$ is a $\kappa$-contraction operator, and it converges to $\left(\frac{1}{q}, \ldots, \frac{1}{q}\right)$. However, it is worth noting that $T_i n_i$ has more than one fixed point. So why does it only converge to $\left(\frac{1}{q}, \ldots, \frac{1}{q}\right)$? This is because the other fixed points take the form $i^{(k)} = 1$, $i^{(l)} = 0$, where $l \neq k$, $k \in \mathbb{Z}_q$. However, the previous analysis on probabilities indicates that $i^{(j)}_n \in (0, 1)$. Therefore, it will only converge to $\left(\frac{1}{q}, \ldots, \frac{1}{q}\right)$. Furthermore, we can obtain

$$\|i_{n+1} - i_n\| \leq \kappa\|i_n - i_{n-1}\| \leq \cdots \leq \kappa^{n-1}\|i_2 - i_1\|. $$

Therefore, as long as $\kappa^{n-1}$ meets the requirement, we can complete the reduction to LWR. Based on the learning with rounding problem, provide two variants of the indistinguishability theorem, as follows:

**Theorem (Informal).** Let $q > 2^n p$ be prime numbers, $A \in \mathbb{Z}_q^{m \times n}$, $s \in \mathbb{Z}_q^n$, $u \in \mathbb{Z}_p^n$. If it is difficult to distinguish between $(A, \lfloor As \rfloor_p)$ and $(A, \lfloor u \rfloor_p)$, then for $a, b \in \mathbb{R} \mathbb{Z}_q$ (or $b \in \mathbb{R} \mathbb{Z}_q$, $a \in \mathbb{R} \mathbb{Z}_q^{m \times n}$), we have

$$(\circ_q(A, a), \lfloor u \rfloor_p) \approx_{\varepsilon} (\circ_q(A, a), \lfloor \circ_q(A, ab) \cdot s \rfloor_p).$$
Building on the work of Brakerski et al. [BDGM22, BDGM20], provide a heuristic notion of indistinguishability obfuscation. Leveraging the second variant problem (referred to for ease of exposition as the delta variant of learning with rounding, LWR.DV), we construct a linear homomorphic scheme. This LWR.DV-based linear homomorphic scheme theoretically possesses properties resistant to quantum attacks.

**Evasive LWR and multilinear maps** In 2015, Gentry, Gorbunov, and Halevi presented lattice-based Multilinear Maps [GGH15], defined as

\[ A, S_1 A_1 + E_1, \ldots, S_k A_k + E_k \rightarrow \prod_{i=1}^{n} S A + E \mod q. \]

Most notably, none of the current indistinguishability obfuscation candidates from GGH15 have any formal security guarantees against zeroizing attacks [BGMZ18].

To resist zeroizing attacks, in 2022, Wee introduced the definition of Evasive LWE [Wee22] and proposed new multilinear maps [VWW22], defined as

\[ A, (u M_1 \otimes S_1) A_1 + E_1, \ldots, A_{k-1}^{-1} ((M_k \otimes S_k) A_k + E_k)) \]

\[ \rightarrow \left( \left( u \prod_{i=1}^{n} M_i \right) \otimes \left( \prod_{i=1}^{n} S_i \right) \right) A + E \mod q. \]

Inspired by this, we attempt to construct a new GGH15 multilinear maps based on Evasive LWR. Here’s our first attempt.

**First attempt**

**KeyGen** \((n, m, q)\). Generate necessary parameters.

**Eval** \(M = (M_1, \ldots, M_t), (u, \{R_i\}_{i=1}^t)\).  * Set \(S_i\) as

\[ \widehat{S}_i = \begin{cases} 
 u(M_1 \otimes R_1), & \text{when } i = 1, \\
 M_i \otimes R_i, & \text{when } i > 1.
\end{cases} \]

* Output encrypted result

\[ \{ \lfloor u(M_1 \otimes R_1) A_1 \rfloor_p \}, \{ \lfloor A_{i-1}^{-1} (M_i \otimes R_i) A_i \rfloor_p \}_{i=1}^t. \]

**Remark 1**. \(M_i \otimes R_i\) is not a random matrix, hence it does not satisfy the Evasive LWR assumption.
Second attempt

**KeyGen**\((n, m, q)\). Generate necessary parameters.

**Eval**\((M = (M_1, \ldots, M_\ell), (u, \{R_i\}_{i=1}^\ell))\).

- Set \(S_i\) as
  \[
  \hat{S}_i = \begin{cases} 
  u(M_1 \odot R_1), & \text{when } i = 1, \\
  M_i \odot R_i, & \text{when } i > 1.
  \end{cases}
  \]

- Output encrypted result
  \[
  \{\lfloor u(M_1 \odot R_1)A_1 \rfloor_p\}, \{\lfloor A_{i-1}^{-1}(M_i \odot R_i)A_i \rfloor_p\}_{i=1}^\ell.
  \]

*Remark 2.* Although \(M_i \odot R_i\) meets the randomness requirement, its computational cost is slightly high. Therefore, considering increasing the randomness of \(M_i\) to reduce computational expenses.

Third Attempt

We refer to the following scheme as composite pseudorandom function.

**KeyGen**\((n, m, q)\). Generate necessary parameters.

**PRF.Enc**\((\{M_i\}_{i=1}^\ell, u, key, n, m, q)\).

\[
C_i = PRF(\{M_i\}_{i=1}^\ell, key)
\]

**Eval**\((C = (C_1, \ldots, C_\ell))\).

- Set \(S_i\) as
  \[
  \hat{S}_i = \begin{cases} 
  u(C_1), & \text{when } i = 1, \\
  C_i, & \text{when } i > 1.
  \end{cases}
  \]

- Output encrypted result
  \[
  \{\lfloor u(C_1)A_1 \rfloor_p\}, \{\lfloor A_{i-1}^{-1}(C_i)A_i \rfloor_p\}_{i=2}^\ell.
  \]

*Remark 3.* Using a pseudorandom function improves the randomness of \(M_i\) while also reducing computational overhead.

**Conceptual Ideal Obfuscation Scheme** Next, present a conceptual split FHE scheme (ideal obfuscation scheme), which is based on three main techniques: (i) Using multilinear maps to construct FHE scheme, (ii) short decryption gadgets for linear homomorphic encryption schemes (such as the scheme in this paper, based on the LWR.DV problem), and (iii) encrypted hash functions...
(used for a part of the linear homomorphic encryption scheme). The security of this scheme can be based on a new conjecture regarding the interaction of these primitives, which we believe is a natural strengthening of circular security.

We aim to instantiate the underlying primitives randomly rather than non-randomly, as non-random instantiations of primitives are insecure, and thus would lead to an insecure split FHE scheme. For randomly instantiated primitives, we can speculate about their security.

**Security Proof.** In order to prove the security of our scheme, demonstrate the existence of an oracle that interacts securely between the underlying primitives and a randomly instantiated scheme. This oracle is defined as $O((\hat{pk}, pk, q, \tilde{q}))(x)$: given a string $x \in \{0, 1\}^*$ and a ciphertext taken from the ciphertext space of the linear homomorphic scheme,

$c \leftarrow C,$

it then calculates

$c \leftarrow \text{Eval}(\hat{pk}, -[\text{DEC}(\cdot, c)/\tilde{q}] \cdot \tilde{q}, \hat{c}),$

and returns $(c, \hat{c})$. In this paper, we use this oracle for the security proof of the scheme.

**Theorem (Informal).** Assuming the sub-exponential hardness of the LWR problem and the Evasive LWR problem, there exists a sub-exponentially secure split fully homomorphic encryption scheme. Consequently, there exists an ideal obfuscation that can be applied to any circuit.

1.2 Technical Overview

Next, provide a generalized description of the method for constructing split FHE, and readers can refer to relevant literature for a more detailed description.

**Split FHE** In 2019, Brakerski et al. [BDGM19] introduced the concept of a split FHE scheme. Asymptotically, they aimed to design an efficient FHE scheme by eliminating linear noise in previous Evasive LWR-based FHE schemes. More specifically, given an FHE ciphertext $c$ and an Evasive LWR key $(s_1, \ldots, s_n)$, we can denote the decryption operator as a linear function $L_c(\cdot)$, that is

$L_c(s_1, \ldots, s_n) = \text{ECC}(m) + e.$
Here, $e$ is a noise term bounded by $B$, and ECC is the encoding operator for the text. Then, this paper introduces the construction of a linear homomorphic scheme using LWR.DV, and encrypts the key $(s_1, \ldots, s_n)$ with this homomorphic encryption scheme, allowing the compression of FHE ciphertexts through the computation of $L_c(\cdot)$. The public key of this scheme is $(r \in R \{0, 1\}^n, \circ_q(A, l))$, and it computes the encryption of a message $m$ as

$$c = [\circ_q(A, lu)(m + k)]_p.$$  

Here, $u = H(r)$, where $H : \{0, 1\}^n \rightarrow \mathbb{Z}_q$ and $k \in R \{0, \ell + 1\}$. Furthermore, this scheme possesses an additional property, which refer to as split decryption. If the decryption algorithm can be divided into a private subroutine and a public subroutine, then the scheme has split decryption:

- The private process takes a ciphertext $c$ and key $(\circ_q(A, lu), T_{sk})$ as input, outputs $\tilde{m} = \text{LWRInvert}(T_{sk}, \circ_q(A, lu), c)$. For each component $\tilde{m}_i$ of $\tilde{m}$,

$$
\begin{cases}
\hat{k}_i = 0, & \text{if } \tilde{m}_i \in \{0, 1\}, \\
\hat{k}_i = \tilde{m}_i, & \text{if } \tilde{m}_i \in \{(\ell + 1), \ldots, n(\ell + 1)\}, \\
\hat{k}_i = \tilde{m}_i - 1, & \text{if } \tilde{m}_i \notin \{0, 1, (\ell + 1), \ldots, n(\ell + 1)\}.
\end{cases}
$$

It returns the decryption primer $\hat{\rho} = \left( sk, \hat{k} = (\hat{k}_i)_{i \in \{1, \ldots, \ell\}} \right)$.

- The public process takes the ciphertext $c$ and decryption primer $\rho$ as inputs, outputs $\tilde{m} = \text{LWRInvert}(T_{sk}, \circ_q(A, lu), c)$, decrypts $m' = \tilde{m} - \hat{k}$.

In summary, $m$ can be fully recovered by passing a fixed-size decryption primer, especially independent of the norm of $m$. As we will discuss later, this property will be the main feature in constructing universal obfuscation.

**FHE scheme and sFHE scheme based on multilinear maps** Because Evasive LWR itself possesses certain homomorphic properties, namely

$$[A_i^{-1}(C^{(1)}_i)A_i]_p + [A_i^{-1}(C^{(2)}_i)A_i]_p \approx [A_i^{-1}(C^{(1)}_i + C^{(2)}_i)A_i]_p,$$

and

$$[A_i^{-1}(C_i)A_i]_p \cdot \frac{q}{p} [A_i^{-1}(C_{i+1})A_{i+1}]_p \approx [A_i^{-1}(C_iC_{i+1})A_{i+1}]_p.$$
Thus, it is possible to obtain $C_i^{(1)} + C_i^{(2)}$ and $C_iC_{i+1}$ using LWR gates. However, to obtain the corresponding $M_i^{(1)} + M_i^{(2)}$ and $M_iM_{i+1}$, the PRF.Enc function must also possess homomorphic and decryptable properties, which is not a feature of ordinary pseudorandom functions.

**The Security of Split FHE** We now discuss the security of the split FHE scheme. Our primary concern is ensuring that the decryption primer does not carry any information about the plaintext; otherwise, the simplicity of the split encryption process and straightforward output of keys in every scheme would be moot. We propose a more profound indistinguishability definition, meaning that for all plaintext pairs $(m_0, m_1)$ and any set of circuits $(C_1, \ldots, C_\beta)$, we have $C_i(m_0) = C_i(m_1)$. Even if an adversary knows the decryption primer $\rho_i$, they cannot distinguish between the encryptions of $(m_0, m_1)$ as $(c_0, c_1)$. The condition $C_i(m_0) = C_i(m_1)$ eliminates some other attacks, where the adversary only needs to check the obfuscator’s output. Here, $\beta = \beta(\lambda)$ is a priori bounded polynomial of a security parameter.

**Theorem (Informal).** Assuming the sub-exponential hardness of the LWR problem and the Evasive LWR problem, there exists a split FHE scheme secure under the $O$-hybrid security model.

**From Split FHE Scheme to Ideal Obfuscation** Utilize the split FHE scheme presented in this paper to construct ideal obfuscation. Building on the work of Lin et al. [Lin17], we achieve an obfuscated circuit $C$ with input domain $\{0, 1\}^n$ whose length does not exceed $\text{poly}(\lambda, |C|) \cdot 2\eta \cdot (1 - \varepsilon)$, where $\varepsilon > 0$. This implies that split FHE signifies the existence of an obfuscator with non-trivial efficiency (for circuits with polynomial-size input domains).

2 Preliminary

We define a function $\text{negl}(\cdot)$, which is an infinitesimal of any polynomial function $\text{poly}$, and we refer to it as “negligible”. Given a set $\mathcal{S}$, $s \in \mathcal{S}$ means randomly selecting an element $s$ from the set $\mathcal{S}$. When an algorithm can be computed within a polynomial function $\text{poly}$, we say that this algorithm is “computable in polynomial time”.
Lemma 1 ([AJLA+12, Smudging]). Let $B_1 = B_1(n), B_2 = B_2(n)$ be positive integers, and $e_1 \in [B_1]$. Let $e_2 \in_R [B_2]$. If $B_1/B_2 = \text{negl}(n)$, then the distribution of $e_2$ is computationally indistinguishable from the distribution of $e_2 + e_1$.

Definition 1 ([GSM18], page 32, Section 4.1.6). We say that $\varepsilon(n)$ is negligible associated with $n$ if $\varepsilon(n)$ can be expressed as

$$\varepsilon(n) = \frac{1}{O(e^n)},$$

and the notation $O(n)$ represents a quantity that grows at most as fast as $n$ approaches infinity.

2.1 The new reduction for LWR.

Dr. Chen Yilei’s attack does have some flaws. However, it also serves as a warning that we cannot reduce all difficult problems to LWE. We utilize the prime number theorem and fixed-point theory to reevaluate its reduction.

Lemma 2 ([Nor66]). For $q \in \mathbb{Z}$, the prime distribution over the set $S_q = \{1, \ldots, q\}$ satisfies the following relationship:

$$\lim_{q \to \infty} \frac{\pi(q)}{\int_{1}^{q} \frac{1}{\ln(t)} dt} = 1,$$

where $\pi(q)$ denotes the number of primes.

Claim 1. Let $\pi(q)$ denote the number of prime numbers in the set $S_q$, and let $P_q := \{p_1, \ldots, p_{\pi(q)}\}$ be the set of all prime numbers. Then, the number of prime numbers in the set $S_q \times S_q$ is still $\pi(q)$, and we have

$$\mathcal{S}_q := S_q \times S_q = S_{q^2} \setminus \{S_q \times (P_{q^2} \setminus P_q)\}.$$

Claim 2. For the set $S_q$, for an element $a \in \mathcal{S}_q$ with prime factorization $p_1^{\alpha_1} \cdots p_\ell^{\alpha_\ell}$, the probability of $a$ occurring in the set $\mathcal{S}_q$ is

$$\Pr(a) := \frac{CN_q(a)}{q^2} = \sum_{\mathcal{P}_1, \mathcal{P}_2 \in \mathcal{S}_q} \frac{2}{q^2},$$

where $\mathcal{P}_1 = p_1^{\alpha'_1} \cdots p_\ell^{\alpha'_\ell}$, $\mathcal{P}_2 = p_1^{\alpha''_1} \cdots p_\ell^{\alpha''_\ell}$, $\alpha'_i + \alpha''_i = \alpha_i$, $i \in S$. 
Claim 3. For the set $S_q$, where each event occurs with probability $q^{-1}$, then for the set $S_q \times S_q$, the probability of each event $a$ occurring is

$$\Pr(a) = \begin{cases} \frac{1}{q^2}, & a = 1, \\ \frac{2}{q^2}, & a \text{ is prime}, \\ \frac{CN_q(a)}{q^2}, & a \text{ is composite}. \end{cases}$$

Claim 4. For $A \in S_q$, and assuming $\Pr(A) = \max_{a \in S_q} \Pr(a) = \frac{CN_q(A)}{q^2}$, then for any $k \in (S_q + S_q) \mod q \to S_{q^2}$, we have

$$\frac{1}{q^2} \leq \Pr(k) \leq \frac{CN_q(A)}{q^2}.$$ 

Proof.

$$\Pr(k) = \sum_{i=1}^{k} \Pr(i) \Pr(k + i - 1) + \sum_{i=k+1}^{q+k-1} \Pr(i) \Pr(q + k + 1 - i)$$

$$= \sum_{i=1}^{k} a_i \frac{a_{k+i-1}}{q^2} + \sum_{i=k+1}^{q+k-1} a_i \frac{a_{q+k+1-i}}{q^2}$$

$$\leq \frac{CN_q(A)}{q^2} \sum_{i=1}^{q^2} a_i \frac{a_i}{q^2} = \frac{CN_q(A)}{q^2},$$

and

$$\Pr(k) = \sum_{i=1}^{k} \Pr(i) \Pr(k + i - 1) + \sum_{i=k+1}^{q+k-1} \Pr(i) \Pr(q + k + 1 - i)$$

$$\geq \frac{1}{q^2} \sum_{i=1}^{q^2} a_i \frac{a_i}{q^2} = \frac{1}{q^2}.$$

Definition 2 ([Ceg12], Definition 2.1.6). Let $\mathcal{H}$ be a Hilbert space, and let $T : \mathcal{H} \to \mathcal{H}$ be an operator. If $T(\cdot)$ satisfies

$$\|Tx - Ty\| < \|x - y\|, \forall x, y \in \mathcal{H},$$

then $T(\cdot)$ is called a contraction operator.
Lemma 3 ([Ceg12], Proposition 2.1.11). If \( \mathcal{H} \) is a closed set (every Cauchy sequence in \( \mathcal{H} \) converges to a point within \( \mathcal{H} \)), and \( T(\cdot) \) is a contraction operator, and \( \text{Fix}(T) \) is a closed convex set, then the algorithm \( x_{n+1} = Tx_n \) converges to some \( x \in \text{Fix}(T) \), where \( \text{Fix}(T) \) denotes the set of fixed points of the operator \( T(\cdot) \).

Remark 4. The convergence mentioned in Lemma 3 should be considered as strong convergence. However, this paper does not discuss the difference between strong and weak convergence, because in finite dimensions strong and weak convergence are equivalent.

Claim 5. For any vector \( a = (a^{(1)}, a^{(2)}, \ldots, a^{(q)}) \), where \( a_i \in [0, 1] \) and \( \sum_{i=1}^{q} a^{(i)} = 1 \), let \( A_k = \max_{i \in S_q} (a^{(i)}) \). Then, the matrix \( M_a \) defined as follows is a contraction operator

\[
M_a = \begin{pmatrix}
    a^{(1)} & a^{(q)} & \ldots & a^{(2)} \\
    a^{(2)} & a^{(1)} & \ldots & a^{(3)} \\
    \vdots & \vdots & \ddots & \vdots \\
    a^{(q)} & a^{(q-1)} & \ldots & a^{(1)}
\end{pmatrix}.
\]

Proof. For any vectors \( b = (b^{(1)}, b^{(2)}, \ldots, b^{(q)}) \) and \( c = (c^{(1)}, c^{(2)}, \ldots, c^{(q)}) \) satisfying the conditions of vector \( a \), and

\[
\|M_a b - M_a c\| = \|M_a (b-c)\| \leq \|M_a\| \|b-c\|
\]

\[
= \sqrt{CN_q^2(\mathfrak{A})} + \frac{q-2}{q^2} + \frac{(2q - CN_q(\mathfrak{A}))^2}{q^2} \|b-c\|
\]

\[
= \sqrt{5q - 4\sqrt{q}CN_q(\mathfrak{A}) + 2CN_q^2(\mathfrak{A}) + 2} \|b-c\|
\]

\[
< \|b-c\|.
\]

Lemma 4. For any initial vector \( a_0 = (a_0^{(1)}, a_0^{(2)}, \ldots, a_0^{(q)}) \), where \( a_0^{(i)} \in [0, 1] \) and \( \sum_{i=1}^{q} a_0^{(i)} = 1 \), and \( CN_q(\mathfrak{A}) = \max_{i \in S_q} (a_0^{(i)}) \), the matrix \( M_{a_0} \) is generated as follows:

\[
M_{a_0} = \begin{pmatrix}
    a_0^{(1)} & a_0^{(q)} & \ldots & a_0^{(2)} \\
    a_0^{(2)} & a_0^{(1)} & \ldots & a_0^{(3)} \\
    \vdots & \vdots & \ddots & \vdots \\
    a_0^{(q)} & a_0^{(q-1)} & \ldots & a_0^{(1)}
\end{pmatrix}.
\]
Then, let $a_{n+1} := M_{a_n}a_n := T a_n$, then $\{a_n\}_{n=1}^{\infty}$ is a Cauchy sequence and converges to $\left( \frac{1}{q}, \ldots, \frac{1}{q} \right)$.

**Proof.** According to Claim 5, we know that $M_{a_n}$ is a contraction operator, and

$$\|M_{a_n}\| \leq \frac{\sqrt{5q - 4 \sqrt{qCN_q(\mathbb{A})} + 2CN_q^2(\mathbb{A}) + 2}}{q}.$$  

Moreover, since $a_{n+1} := M_{a_n}a_n$ is itself an algorithm for finding fixed points, the sequence $\{a_n\}_{n=1}^{\infty}$ converges, and it converges to the fixed point of $T(\cdot)$.

**Lemma 5.** For the set $S_q^i := \{1, 2, \ldots, q\}$, where each event $j \in S_q$ has a probability of occurrence $a_j$, as $n$ approaches infinity, the probability of each event after taking modulo $q$ over $S_q := \prod_{i=1}^{n} S_q^i \mod q = \{1, 2, \ldots, q\}$ tends toward $\frac{1}{q}$.

**Theorem 1.** Given $\{a_j\}_{j=1}^{n}$ and $\{s_j\}_{j=1}^{n}$ such that $a_j, s_j \in R\mathbb{Z}_q$. Then for any $i \in R\mathbb{Z}_q$, we have

$$\max_{i \in S_q} \left| \Pr\left( \sum_{j=1}^{n} (a_j s_j) = i \right) - \Pr(u = i) \right| \leq \exp\left( 2n \ln \left( \frac{\sqrt{5q - 4 \sqrt{qCN_q(\mathbb{A})} + 2CN_q^2(\mathbb{A}) + 2}}{q} \right) \right).$$

**Corollary 1.** For any $A \in \mathbb{Z}_q^{m \times n}$, $s \in \mathbb{Z}_q^n$, and $u \in \mathbb{Z}_q^m$, where $q > 2^np$, the indistinguishability probability between $As$ and $u$ is bounded by

$$\exp \left( -2 \log_2 n \ln \left( \frac{q}{\sqrt{5q - 4 \sqrt{qCN_q(\mathbb{A})} + 2CN_q^2(\mathbb{A}) + 2}} \right) \right) \leq \exp \left( - \frac{n \log_2 n \ln p}{\sqrt{5}} \right).$$

**Theorem 2.** For any $A \in \mathbb{Z}_q^{m \times n}$, $s \in \mathbb{Z}_q^n$, and $u \in \mathbb{Z}_q^m$, where $q > 2^np$, the indistinguishability probability between $[As]_p$ and $[u]_p$ is bounded by

$$\exp \left( - \frac{n \log_2 n \ln p}{\sqrt{5}} \right).$$

That is, the adversary’s advantage in distinguishing between $[As]_p$ and $[u]_p$ can be neglected.
2.2 LWR Trapdoor Algorithm

**Algorithm 1** LWR Trapdoor Algorithm [AKPW13]

**GenTrap**($n,m,q$): A method that outputs $A \in \mathbb{Z}^{m \times n}_q$ and a trapdoor $T$ in polynomial time, where the input to this algorithm is an integer $n$, $q$, and a sufficiently large integer $m$. The matrix $A$ is uniformly distributed in $\mathbb{Z}^{m \times n}_q$.

**Invert**($T,A,c$): A method that outputs $s \in \mathbb{Z}^n_q$ from $c = As + e \in \mathbb{Z}^m_q$ in polynomial time, with $\|e\|_2 \leq \gamma$. The input to this algorithm is the output $A$ and trapdoor $T$ from the **GenTrap**($n,m,q$) algorithm.

**LWRInvert**($T,A,c$): A method that outputs $s \in \mathbb{Z}^n_q$ from $c = \lfloor As \rfloor_p \in \mathbb{Z}^m_p$ in polynomial time. The input to this algorithm is the output $A$ and trapdoor $T$ from the **GenTrap**($n,m,q$) algorithm.

**Lemma 6** (Existence Lemma of LWR Trapdoor Algorithm, [AKPW13]).
The LWR trapdoor algorithm definitely exists, that is, for integers $n$, $q$, sufficiently large integer $m \geq O(n \log q)$, and sufficiently large integer $p \geq O(\sqrt{n \log q})$, there exist algorithms **GenTrap**($n,m,q$) and **LWRInvert**($T,A,c$) that output results in polynomial time.

2.3 Variants of LWR and Their Applications

**Lemma 7.** If $a \in R \mathbb{Z}_q$, then for $r \in R \mathbb{Z}_p$, $a^r \mod q$ is indistinguishable from $u \in R \mathbb{Z}_q$.

*Proof.* According to Lemma 1, it is easy to prove.

**Lemma 8.** If $A \in R \mathbb{Z}^{m \times n}_q$, then $\odot_q(A,r) \in R \mathbb{Z}^{m \times n}_q$. Where the operation $\odot_q(A,r)$ is defined as follows:

$$
\odot_q(A,r) = \begin{cases} 
\tilde{A} \left( a_{ij} \in A, a_{ij}^r \in \tilde{A}, i \in \{1, \ldots, m\}, j \in \{1, \ldots, n\} \right) \mod q, & \text{for } r \in \mathbb{Z}_q, \\
\tilde{A} \left( a_{ij} \in A, a_{ij}^r \in \tilde{A}, i \in \{1, \ldots, m\}, j \in \{1, \ldots, n\} \right) \mod q, & \text{for } r \in \mathbb{Z}^{m \times n}_q.
\end{cases}
$$

*Proof.* From Lemma 7, if $a_{ij} \in R \mathbb{Z}_q$, then $a_{ij}^r \mod q \in R \mathbb{Z}_q$ (or $a_{ij}^r \mod q \in R \mathbb{Z}_q$). Therefore, $\odot_q(A,r) \in R \mathbb{Z}^{m \times n}_q$.

**Lemma 9.** If $(A, \lfloor As \rfloor_p)$ and $(A, \lfloor u \rfloor_p)$ are indistinguishable, then for $r \in R \mathbb{Z}_p$ (or $r \in R \mathbb{Z}^{m \times n}_q$), $(\odot_q(A,r), \lfloor \odot_q(A,r) \cdot s \rfloor_p)$ and $(\odot_q(A,r), \lfloor u \rfloor_p)$ are also indistinguishable.
Proof. According to the form of LWR, when \( A \in \mathbb{Z}_q^{m \times n} \), we have \( \tilde{A} = \circ_q(A, r) \in \mathbb{Z}_q^{m \times n} \). Therefore, \((\tilde{A}, \lfloor \tilde{A}s \rfloor)_p \) and \((\tilde{A}, \lfloor u \rfloor)_p \) still maintain indistinguishability.

Corollary 2. If there exists an algorithm \( O \) to solve the LWR problem, then there also exists an algorithm \( O' \) to solve the Variant LWR problem, and vice versa.

Proof. According to Lemma 8, the sufficiency of the proposition is established. Now, to prove the necessity, since \( f \) is a bijection, there exists \( f^{-1} \) such that \( f^{-1} \cdot f = f \cdot f^{-1} = Id \). It can be easily shown that \( f^{-1} \) is also a bijection. Hence, when \( \circ_q(A, r) \in \mathbb{Z}_q^{m \times n} \), it implies \( A \in \mathbb{Z}_q^{m \times n} \), thus the necessity is proved.

Lemma 10. If \((A, \lfloor As \rfloor)_p \) is indistinguishable from \((A, \lfloor u \rfloor)_p \), then for randomly chosen \( b \in \mathbb{Z}_p \) and \( a \in \mathbb{Z}_p^{m \times n} \), we have

\[
(\circ_q(A, a), \lfloor u \rfloor)_p \approx_c \left( \circ_q(A, ab), \lfloor \circ_q(A, ab) \cdot s \rfloor_p \right).
\]

Proof.

\[
(\circ_q(A, a), \lfloor u \rfloor)_p \approx_c \left( \circ_q(A, ab), \lfloor u \rfloor_p \right) \\
\approx_c \left( \circ_q(A, ab), \lfloor \circ_q(A, ab) \cdot s \rfloor_p \right) \\
\approx_c \left( \circ_q(A, a), \lfloor \circ_q(A, ab) \cdot s \rfloor_p \right).
\]

Corollary 3. If \((A, \lfloor As \rfloor)_p \) is indistinguishable from \((A, \lfloor u \rfloor)_p \), \( s \in \mathbb{Z}_3^n \), then for randomly chosen \( b \in \mathbb{Z}_p \) and \( a \in \mathbb{Z}_p^{m \times n} \), we have

\[
(\circ_q(A, a), \lfloor u \rfloor)_p \approx_c \left( \circ_q(A, a), \lfloor \circ_q(A, ab) \cdot s \rfloor_p \right).
\]

Proof. Let \( S_{q,3} := S_q \times S_3 \), and for all \( i \in \mathbb{Z}_q \), we have

\[
Pr(i) := \frac{CN_q(i)}{q^2} = \sum_{\varphi_1, \varphi_2 \in S_{q,3}} \frac{2}{q^2}.
\]

Similarly, we can prove that

\[
\frac{1}{q^2} \leq Pr(i) \leq \frac{CN_q(\mathfrak{A})}{q^2},
\]

thus, by utilizing fixed-point theory and Lemma 10, we obtain the conclusion.
2.4 ℵ-Graded Encoding System and composite homomorphic pseudorandom function

Definition 3 (ℵ-GES, [GGH13a]). Let ℵ ∈ ℤ+ be a τ > 0 dimensional natural number vector. An ℵ-GES consists of a ring ℱ and a set ℬ = {S_α(υ) ⊂ {0, 1}^* : α ∈ ℱ, υ ≤ ℵ} (each element of this set S_α(υ) is also a set, representing the set of all order-υ encodings for the ring element α) with the following properties:

1. For all υ, the sets {S_α(υ) : α ∈ ℱ} are disjoint, thus S_υ = ∪_α S_α(υ).
2. There exist a binary operator ‘+’ and a unary operator ‘-’, such that for all α_1, α_2 ∈ ℱ, υ ≤ ℵ, u_1 ∈ S_α(υ), and u_2 ∈ S_α(υ), the following operations hold:

   \[ u_1 + u_2 ∈ S_α(υ + υ), \text{ and } u_1 ∈ S_{-α}(υ). \]

Here, α_1 + α_2 and −α_1 denote addition and negation in the ring ℱ.  
3. There exists a binary operator ‘×’, such that for any α_1, α_2 ∈ ℱ, υ_1 + υ_2 ≤ ℵ, u_1 ∈ S_α(υ), and u_2 ∈ S_α(υ), the following operation holds:

   \[ u_1 × u_2 ∈ S_α(υ_1 + υ_2). \]

Here, α_1 · α_2 represents multiplication in the ring ℱ, and υ_1 + υ_2 represents addition in ℤ^τ.

Definition 4. Define homomorphic pseudorandom functions F_1 and F_2 such that:

1. F_1(x, key) → C_i, F_1(0, key) → 0, F_1(x_1, key) + F_1(x_2, key) = F_1(x_1 + x_2, key), and F_1(x_1, key) + F_1(x_2, key) = F_1(x_1 x_2, key).
2. F_2(C = (C_1, ... , C_ℓ), key) = F_2(F_1(C_1, key), ... , F_1(C_ℓ, key)) → y, where ℓ can be any value less than ℵ, and F_2 satisfies:

   \[ - F_2(C_1, key) + F_2(C_2, key) = F_2(C_1 + C_2, key), \]
   \[ - F_2(0, key) = 0. \]

2.5 Homomorphic Encryption and Ideal Obfuscation

Homomorphic encryption is defined as follows:

Definition 5 ([Gen09a]). A homomorphic encryption scheme consists of the following components:
– **KeyGen**(n): Given a security parameter n, the key generation part returns a key pair (sk, pk).
– **Enc**(pk, m): Given the public key pk and the plaintext message m, the encryption part returns the encrypted ciphertext c.
– **Eval**(pk, C, (c₁, . . . , c_ℓ)): Given the public key pk, a circuit C of depth ℓ, and a vector of ciphertexts (c₁, . . . , c_ℓ), the homomorphic operation part returns the ciphertext after homomorphic computation.
– **Dec**(sk, c): Given the private key sk and the ciphertext c, the decryption part returns the decrypted plaintext message m.

**Definition 6 (Correctness).** Let n ∈ N, and C be a circuit of depth ℓ. For an encryption scheme (KeyGen, Enc, Eval, Dec) with inputs (m₁, . . . , m_ℓ), key pair (pk, sk) generated by KeyGen(n), and ciphertexts cᵢ generated by Enc(pk, mᵢ) according to the scheme, we have

\[ \Pr[\text{Dec}(sk, \text{Eval}(pk, C, (c₁, . . . , c_ℓ))) = C(c₁, . . . , c_ℓ)] = 1. \]

Refer to such an encryption scheme as a homomorphic encryption scheme. We desire that the length of ciphertexts in the scheme does not increase due to the depth ℓ of circuit C, a property referred to as “compactness” (distinct from the concept of “compactness” in functional analysis).

**Definition 7 (Compactness).** Let n ∈ N, C be a circuit of depth ℓ, and poly(·) be a polynomial function. For a homomorphic encryption scheme (KeyGen, Enc, Eval, Dec) with inputs (m₁, . . . , m_ℓ), key pair (pk, sk) generated by KeyGen(n), and ciphertexts cᵢ generated by Enc(pk, mᵢ), if

\[ |\text{Eval}(pk, C, (c₁, . . . , c_ℓ))| = \text{poly}(n) \cdot |C(m₁, . . . , m_ℓ)|, \]

then one called the homomorphic encryption scheme compact. Define a weak security notion (implied by standard semantic security [38]) for convenience.

**Definition 8 (Semantic Security).** Let n ∈ N, C be a circuit of depth ℓ, and negl(·) be a negligible function. For a homomorphic encryption scheme (KeyGen, Enc, Eval, Dec) with inputs (m₀, m₁), key pair (pk, sk) generated by KeyGen(n), ciphertexts cᵢ generated by Enc(pk, mᵢ), and all polynomial-time distinguishers D, if

\[ |\Pr[1 = D(pk, \text{Enc}(pk, m₀))] − \Pr[1 = D(pk, \text{Enc}(pk, m₁))]| = \text{negl}(n), \]
then one called the homomorphic encryption scheme semantically secure. Here, the key pair \((pk, sk)\) is generated by \(\text{KeyGen}(n)\) of the scheme.

Definition 9 (\(\epsilon\)-Indistinguishability). Consider two distributions \(\mathcal{X} = \{X_\lambda\}_{\lambda \in \mathbb{N}}\) and \(\mathcal{Y} = \{Y_\lambda\}_{\lambda \in \mathbb{N}}\), and \(\epsilon : \mathbb{N} \to [0, 1]\). If for every sufficiently large \(\lambda \in \mathbb{N}\), it holds that
\[
\left| \Pr_{x \leftarrow X_\lambda} [A(1^\lambda, x) = 1] - \Pr_{y \leftarrow Y_\lambda} [A(1^\lambda, y) = 1] \right| \leq \epsilon(\lambda),
\]
one said that the two distributions \(\mathcal{X}\) and \(\mathcal{Y}\) are indistinguishable. Here, \(A\) is a probabilistic polynomial-time adversary. Specifically, when \(\epsilon(\lambda) = \text{negl}(\lambda)\), one called \(\mathcal{X}\) and \(\mathcal{Y}\) indistinguishable with respect to \(\epsilon\); when \(\epsilon(\lambda) = 2^{-\lambda}c\), one called \(\mathcal{X}\) and \(\mathcal{Y}\) sub-exponentially indistinguishable.

Definition 10 (Circuit Obfuscation). A circuit obfuscation scheme under the ideal model with an oracle \(O\) is said to be efficient \(\text{Obf}^O(\lambda, C)\) if, for a given input circuit \(C\), it outputs an obfuscated circuit \(\hat{C}\). The scheme is required to be correct, meaning that for all \(\lambda \in \mathbb{N}\), where the circuit \(C : \{0, 1\}^D \rightarrow \{0, 1\}^*\) and input \(x \in \{0, 1\}^D\), the following relation holds:
\[
\Pr[\hat{C} \leftarrow \text{Obf}^O(\lambda, C) : \hat{C}^O = C(x)] = 1.
\]

Definition 11 (Ideal Obfuscation). A circuit obfuscation scheme \(\text{Obf}^O(\lambda, C)\) is said to be ideal if there exists an efficient simulator \(S = (S_1, S_2, S_3)\) such that for all adversaries \(A = (A_1, A_2)\), the adversary's advantage is negligible, i.e.,
\[
\Pr \left[ C \leftarrow A_1^O(\lambda) : \hat{C}^* \leftarrow \text{Obf}^O(\lambda, C) \right] \cdot A_1^S(\lambda) \right] - \Pr \left[ C \leftarrow A_1^S(\lambda) : \hat{C}^* \leftarrow S_2^O(\lambda, D, S) \right] \cdot A_2^S(\lambda, \hat{C}^*) = 1
\]
where, \(D = |x|\) is the length of the input circuit \(C\), and \(S = |C|\) is the size of the circuit \(C\).

3 Evasive LWR and Multilinear Mapping

3.1 Evasive LWR

Definition 12 (Solution Evasive LWR). For \(A_i, S_i \in \mathbb{Z}_q^{n \times n}\), \(i = 1, \ldots, \ell\), where \(A_i^{-1}\) denotes the inverse of matrix \(A_i\) for \(i = 2, \ldots, \ell\), and \(u \in \mathbb{Z}_q^n\), the Solution Evasive LWR problem refers to finding \(S_i, i = 1, \ldots, \ell\), from \((\lfloor uS_1A_1 \rfloor_p, \lfloor A_1^{-1}S_2A_2 \rfloor_p, \ldots, \lfloor A_1^{-1}S_\ell A_\ell \rfloor_p)\).
**Theorem 3.** For $A_i, S_i \in \mathbb{Z}_q^{n \times n}$, $i = 1, \ldots, \ell$, where $A_i^{-1}$ denotes the inverse of matrix $A_i$ for $i = 2, \ldots, \ell$, and $u \in \mathbb{Z}_q^n$, we have

\[
\left\{ \{A_i\}_{i=1}^\ell, \left[ kS_1A_1 \right]_p, \left\{ \left[ A_i^{-1}S_iA_1 \right]_p \right\}_{i=2}^\ell \right\} \simeq_C \left\{ \{A_i\}_{i=1}^\ell, \left[ u_1 \right]_p, \left\{ \left[ U_i \right]_p \right\}_{i=2}^\ell \right\},
\]

as well as

\[
\left( A_1, \left[ u \left( \prod_{i=1}^\ell S_i \right) A_1 \right]_p \right) \simeq_C \left( A_1, \left[ u_1 \prod_{i=1}^\ell U_i \right]_p \right).
\]

**Proof.** Here is the translation of the provided text into English:

First, let

\[
O(n) = \frac{n \log_2 n \ln p}{\sqrt{5}}.
\]

On one hand, according to Theorem 2, it is known that

\[
|\Pr(\lfloor B_1 \rfloor_p = \lfloor uS_1A_1 \rfloor_p) - \Pr(\lfloor u_1 \rfloor_p)| \leq 2 \cdot e^{-O(n)} + e^{-2O(n)},
\]

and

\[
|\Pr(\lfloor B_i \rfloor_p = \lfloor A_i^{-1}S_iA_1 \rfloor_p) - \Pr(\lfloor U_i \rfloor_p)| \leq 2 \cdot e^{-O(n)} + e^{-2O(n)},
\]

thus we can obtain

\[
\left\{ \{A_i\}_{i=1}^\ell, \left[ uS_1A_1 \right]_p, \left\{ \left[ A_i^{-1}S_iA_1 \right]_p \right\}_{i=2}^\ell \right\} \simeq_C \left\{ \{A_i\}_{i=1}^\ell, \left[ u_1 \right]_p, \left\{ \left[ U_i \right]_p \right\}_{i=2}^\ell \right\},
\]

On the other hand, using the same principle, it can be derived that

\[
\left| \Pr \left( \left( A_1, \left[ u \left( \prod_{i=1}^\ell S_i \right) A_1 \right]_p \right) \right) - \Pr \left( \left( A_1, \left[ u_1 \prod_{i=1}^\ell U_i \right]_p \right) \right) \right| \leq \ell' \cdot e^{-O(n)},
\]

$\ell' \in (\ell, 2\ell)$.

**Definition 13 (Evasive LWR Decision).** For $A_i, S_i \in \mathbb{Z}_q^{n \times n}$, $i = 1, \ldots, \ell$, where $A_i^{-1}$ denotes the inverse of matrix $A_i$ for $i = 2, \ldots, \ell$, and $u \in \mathbb{Z}_q^n$,
the Evasive LWR decision problem refers to distinguishing, in polynomial time, between the distributions
\[(\lfloor b_1 = uS_1A_1 \rfloor_p, \lfloor B_2 = A_1^{-1}S_2A_2 \rfloor_p, \ldots, \lfloor B_\ell = A_{\ell-1}^{-1}S_\ell A_\ell \rfloor_p)\]
and
\[(\lfloor u_1 \rfloor_p, \lfloor U_2 \rfloor_p, \ldots, \lfloor U_\ell \rfloor_p),\]
as well as between the distributions
\[\left( A_1, \left\lfloor u_1 \left( \prod_{i=1}^\ell S_i \right) A_1 \right\rfloor_p \right) \text{ and } \left( A_1, \left\lfloor u_1 \prod_{i=1}^\ell U_i \right\rfloor_p \right).\]

3.2 Evasive LWR-base Multilinear Mapping

**Algorithm 2** Composite homomorphic pseudorandom function

**PRF.KeyGen** \(n, m, q\). Generate necessary parameters.

**PRF.Enc** \(\{M_i\}_{i=1}^\ell, key, n, m, q\).

\[C_i = PRF(\{M_i\}_{i=1}^\ell, key)\]

**PRF.Eval** \((C = (C_1, \ldots, C_\ell))\).

- Set \(S_i\) as

\[\hat{S}_i = \begin{cases} u(C_1), & \text{if } i = 1, \\ C_i, & \text{if } i > 1. \end{cases}\]

- Output encrypted result

\[\{\lfloor u(C_1)A_1 \rfloor_p\}, \{A_1^{-1}\lfloor ((C_i)A_i) \rfloor_p\}_{i=2}^\ell.\]

**Theorem 4.** Composite homomorphic pseudorandom function is a type of graded encoding system.

**Proof.** A usable asymmetric graded encoding system comprises the following effective algorithms: Instance Generation, Ring Element Sampling, Encoding, Addition and Multiplication Encodings, Zero Testing, and Extraction, denoted as \(\mathcal{GES} = (\text{InstGen}, \text{samp}, \text{enc}, \text{add}, \text{neg}, \text{mul}, \text{isZero}, \text{ext})\).

**Instance Generation.** Generates keys for ciphertext fully homomorphic pseudorandom functions, as well as algorithms like Enc and Eval. Security parameters \(n\), and noise \(\varepsilon\) such that \(\|\varepsilon\| \leq B\).
Encoding. For input plaintext to be encrypted \( \{m_i\}_{i=1}^{\ell} \), \( \ell \leq \aleph \), use the fully homomorphic encryption algorithm \( \text{Enc}(m_i, \text{key}) \) to obtain ciphertext \( \{c_i\}_{i=1}^{\ell} \).

**Addition and Multiplication Encodings.** According to the definition of fully homomorphic encryption schemes or ciphertext fully homomorphic pseudorandom functions:

\[
\begin{align*}
    c_a + c_b &= \text{Enc}(m_a + m_b, \text{key}), \\
    c_a \cdot c_b &= \text{Enc}(m_a \cdot m_b, \text{key}), \\
    -c_a &= \text{Enc}(-m_a, \text{key}).
\end{align*}
\]

Furthermore, for \( \{m_i\}_{i=1}^{\ell} \), we have that

\[
\sum_{i=1}^{\aleph} c_i = \text{Enc}(\sum_{i=1}^{\aleph} m_i, \text{key}) + \|\varepsilon\| \leq B.
\]

Additionally, we know that

\[
\prod_{i=1}^{\aleph} c_i = \text{Enc}(\prod_{i=1}^{\aleph} m_i, \text{key}) + \Xi, \|\Xi\| \leq B.
\]

Zero Testing. Since \( \text{Enc}(0, \text{key}) = \text{Enc}(m_a - m_a, \text{key}) = \text{Enc}(m_a, \text{key}) + \text{Enc}(-m_a, \text{key}) = c_a - c_a \leq B \), it’s easy to prove that zero testing holds.

**Extraction.** For \( \aleph \)-level encodings \( c, c' \), we have

\[
\|c - c'\| = \|\text{Enc}(m, \text{key}) + \varepsilon - \text{Enc}(m, \text{key}) - \varepsilon'\| \leq B.
\]

## 4 Linear Homomorphic Encryption Scheme based on LWR Variant Problems

### Scheme 3 LHE Scheme based on LWR Problem

**LWR.DV.KeyGen(\( n, m, q \)).** Choose a random vector \( r \in \{0,1\}^n \) and matrices \( A, l \in \mathbb{Z}_q^m \times n \). Let \( u = H(r) \in \mathbb{Z}_q^n \), output sample \((\circ_q(A, lu), T_{sk}) \leftarrow \text{GenTrap}(n, m, q)\), let \( pk = (r, \circ_q(A, l)) \) and \( sk = (\circ_q(A, lu), T_{sk}) \).

**LWR.DV.Enc(\( pk, s, q, p \)).** Let \( u = H(r) \in \mathbb{Z}_q \). For each element \( a_{ij}^l \) of \( \circ_q(A, l) \), compute \( (a_{ij}^l)^u \mod q = a_{ij}^lu \), thus obtaining \( \circ_q(A, lu) \). For plaintext \( s \in \{0,1\}^n \), choose a random vector \( k \in \{0, \ell + 1\}^n \), output \( c = [\circ_q(A, lu)(s + k)]_p \).

**LWR.DV.Eval(\( pk, q, p, f, (c_1, \ldots, c_\ell) \)).** Input ciphertext vector \( (c_1, \ldots, c_\ell) \) and linear function \( g = (\alpha_1, \ldots, \alpha_\ell) \in \{0,1\}^\ell \), compute

\[
c = \sum_{i=1}^{\ell} \alpha_ic_i \mod q.
\]
LWR.DV.PDec\((s_k, c)\). For ciphertext \(c \in \mathbb{Z}_p^n\), output \(\hat{s} = \text{LWRInvert}(T_{s_k}, \odot_{q}(A, lu), c)\), for each component \(\hat{s}_i\) of \(\hat{s}\),

\[
\begin{cases} 
\hat{k}_i = 0, & \text{when } \hat{s}_i \in \{0, 1\}, \\
\hat{k}_i = \hat{s}_i, & \text{when } \hat{s}_i \in \{(\ell + 1), \ldots, n(\ell + 1)\}, \\
\hat{k}_i = \hat{s}_i - 1, & \text{when } \hat{s}_i \not\in \{0, 1, (\ell + 1), \ldots, n(\ell + 1)\}.
\end{cases}
\]

Return \(\rho = (s_k, \tilde{k} = (\hat{k}_i)_{i \in \{1, \ldots, \ell\}})\).

LWR.DV.Rec\((\rho, c)\). For ciphertext \(c \in \mathbb{Z}_p^n\), output \(\hat{s} = \text{LWRInvert}(T_{s_k}, \odot_{q}(A, lu), c)\), decrypt \(s' = \hat{s} - \tilde{k}\).

Simulatable Decryption Hint. For given ciphertext \(c\) and plaintext message \(\hat{s}\) (where \(c\) and \(\hat{s}\) are unrelated), choose \(\tilde{k} \in_R \{0, \ell + 1, \ldots, n(\ell + 1)\}^n\), \(\tilde{u} \in_R \mathbb{F}_q\). Let \(s_k \leftarrow \text{GenTrap}(n, m, q)\), compute simulated ciphertext \(\tilde{c}\) and

\[
\tilde{c}_i = \left| c - (\odot_{q}(A, \tilde{u})(\hat{s} + \tilde{k}))_p \right|, i \in \{1, \ldots, n\}.
\]

Then output \(\hat{\rho} = (s_k, \tilde{k})\).

5 Splitting Fully Homomorphic Encryption Scheme

Next, we will introduce an instantiation of FHE with split decryption. First propose a scheme based on standard assumptions, which assumes the existence of a structured version of a random oracle, and then present a trusted candidate scheme for this oracle.

5.1 Defining a Special Oracle for Constructing Splitting Fully Homomorphic Schemes

Before presenting the split fully homomorphic scheme, define a special oracle. The parameters of this oracle are \((\tilde{p}, \tilde{p}, \tilde{q}, \tilde{q})\), where the input is a string \(x \in \{0, 1\}^*\), and it uniformly outputs encrypted values for LHE and FHE. The oracle is deterministic and accessible to all parties, so when given the same input \(x\), the oracle always outputs the same pair of ciphertexts. The formal definition of this oracle is as follows.
Definition 14 ([BDGM20]). $O_{(\hat{pk}, pk, q, \tilde{q})}$: Given input string $x \in \{0, 1\}^*$, outputs two ciphertexts that are uniformly distributed:

$$\hat{\text{Enc}}(pk, s)$$ and $$\text{Enc}(pk, -\lfloor s/\tilde{q} \rfloor \cdot \tilde{q})$$

where $s \leftarrow \mathbb{Z}_q$.

The oracle $O_{(\hat{pk}, pk, q, \tilde{q})}$ can encrypt the private key of FHE using LHE scheme, and the resulting ciphertexts follow a uniform distribution. This is because we use the decryption and multiplication algorithms $\text{DEC}\&\text{Mult}$ in the FHE scheme to compute $\hat{\text{Enc}}(pk, s - \lfloor s/\tilde{q} \rfloor \cdot \tilde{q} + \text{noise})$, where the noise is the decryption noise of the FHE scheme. By choosing appropriate parameters $\tilde{q}$, we can achieve

$$\hat{\text{Enc}}(pk, s - \lfloor s/\tilde{q} \rfloor \cdot \tilde{q} + \text{noise}) = \text{Enc}(pk, (s \mod \tilde{q}) + \text{noise}) \approx \text{Enc}(pk, (s \mod \tilde{q})).$$

Thus, one obtained ciphertexts that are statistically indistinguishable through the two encryption systems.

Description. Now, provide a formal description of our scheme. We assume the existence of the following primitives:

- $c\text{PRF} = (\hat{\text{KeyGen}}, \hat{\text{Enc}}, \hat{\text{Eval}}, \hat{\text{Dec}})$ with linear decryption-multiplication and noise constraint $B$.

- $\text{LHE} = (\text{KeyGen}, \text{Enc}, \text{Eval}, \text{PDec}, \text{Rec})$ with small decryption hints and simulatable decryption hints, then we refer to LHE as linear homomorphic encryption.

If the underlying FHE scheme is leveled out, then it will result in split FHE. Conversely, if the FHE scheme supports evaluation of unbounded circuits, then the resultant split FHE construction will also do so. The formal description of this scheme is as follows.

**Scheme 4** Split Homomorphic Encryption Scheme

- $\text{KeyGen}(n, m, q)$. Given security parameter $n$, output sample $(\overrightarrow{sk}, \overrightarrow{pk}) \leftarrow \text{KeyGen}(n)$. Let $\mathbb{Z}_q$ be the plaintext space under LHE definition, output sample $(sk, pk) \leftarrow \text{KeyGen}(n, m, q)$.

Let $sk = (T_1, \ldots, T_n) \in \{0, 1\}^{n \times n}$, then return

$$sk = \overrightarrow{sk}$$ and $$pk = (\overrightarrow{pk}, \overrightarrow{\tau}_1, \ldots, \overrightarrow{\tau}_n).$$

where, for any $i \in [n]$, define $\overrightarrow{\tau}_i \leftarrow \overrightarrow{\text{Enc}(pk, T_i)}$. 

**Enc**(\(pk, s\)). Return the ciphertext
\[ \hat{c} \leftarrow \hat{\text{Enc}}(\hat{pk}, s). \]

**Eval**(\(pk, f, c_1, \ldots, c_\ell\)). Given a circuit \(C\) of \(\ell\) bits and ciphertexts of length \(k\) bits \((c_1, \ldots, c_\ell)\). For any \(j \in [k]\), \(C_j\) is the \(j\)-th component of circuit \(C\), calculate
\[ d_j \leftarrow \hat{\text{Eval}}(\hat{pk}, C_j, (c_1, \ldots, c_\ell)). \]

Define the linear function over \(\mathbb{Z}_q\) as
\[ g(x_1, \ldots, x_n) = \sum_{j=1}^{k} \text{DEC}&\text{Mult} \left( (x_1, \ldots, x_n), d_j, 2^{\lceil \log(\tilde{q} + (k + 1)B) \rceil + j} \right). \]

Compute \(d \leftarrow \hat{\text{Eval}}(\hat{pk}, g, (\overline{x}_1, \ldots, \overline{x}_n))\), then query \((a, \tilde{a}) \leftarrow O(\hat{pk}, \overline{x}, \tilde{x}, \hat{q})\) and define the following linear function
\[ \tilde{g}(x_1, \ldots, x_n, x_{n+1}, x_{n+2}) = \text{DEC}&\text{Mult}((x_1, \ldots, x_n), \tilde{a}, 1) + x_{n+1} + x_{n+2}. \]

Return
\[ \hat{c} \leftarrow \hat{\text{Eval}}(\hat{pk}, \tilde{g}, (\overline{x}_1, \ldots, \overline{x}_n), d, a). \]

**PDec**(\(sk, c\)). Given an evaluable ciphertext \(c\), return
\[ \rho \leftarrow \text{PDec}(\hat{sk}, c). \]

**Rec**(\(\rho, c\)). Given an evaluable ciphertext \(c\), return
\[ \tilde{s} \leftarrow \text{Rec}(\rho, c), \]
and return the binary representation of \(\tilde{s}\) without the \(\lceil \log(\tilde{q} + (k + 1)B) \rceil\) least significant bits.

**Analysis**: During the analysis, set parameters as needed to ensure the scheme can decrypt correctly. Subsequently, demonstrate that our choices lead to a set of satisfiable constraints. These constraints satisfy the conditions of the underlying hard problems, thus the hardness problem assumptions still hold. The following theorem establishes correctness.

**Theorem 5 (Correctness of Split Homomorphic Encryption Scheme)**. Let \(q \geq 2^k + 2^{\lceil \log(\tilde{q} + (k + 1)B) \rceil}\). Assuming that FHE and LHE are correct, then **Scheme 4** satisfies the correctness of split homomorphism.
Proof. We rewrite
\[
\tilde{s} = \text{Rec}(\rho, c) = \text{Rec}(\text{PDec}(sk, c), c),
\]
where \(c = \text{Eval}(pk, \tilde{g}, (\tau_1, \ldots, \tau_n), d, a))\). By the correctness of the LHE scheme, we can rewrite \(d\) as
\[
d = \text{Eval}(pk, g, (\tau_1, \ldots, \tau_n))
= \text{Eval}(pk, g, (\text{Enc}(pk, T_1), \ldots, \text{Enc}(pk, T_n)))
= \text{Enc} \left( pk, \sum_{j=1}^{k} \text{DEC}&\text{Mult} \left( (T_1, \ldots, T_n), d_j, 2^{\left\lceil \log(\tilde{q} + (k+1)B) \right\rceil} \right) \right).
\]
Where
\[
d_j = \hat{\text{Eval}}(pk, C_j, (c_1, \ldots, c_\ell))
\]
and \(c_i = \text{Enc}(pk, s_i)\). Therefore, by the correctness of the FHE scheme for decryption-multiplication, we can rewrite as
\[
d = \text{Enc} \left( pk, \sum_{j=1}^{k} 2^{\left\lceil \log(\tilde{q} + (k+1)B) \right\rceil} \cdot C_j(s_1, \ldots, s_\ell) + \sum_{j=1}^{k} e_j \right).
\]
Let \(r \leftarrow \mathbb{Z}_q\) and define the oracle \(O_{(pk, pk, q, \tilde{q})}\) such that \(a = \text{Enc}(pk, r)\) and \(\tilde{g}(x_1, \ldots, x_n, x_{n+1}, x_{n+2}) = \text{DEC}&\text{Mult}((x_1, \ldots, x_n), \tilde{a}, 1) + x_{n+1} + x_{n+2}\). Then by the correctness of the FHE scheme, and \(c = \text{Enc}(pk, \tilde{s})\), where \(\tilde{s}\) is
\[
\tilde{s} = \text{DEC}&\text{Mult} \left( (T_1, \ldots, T_n), \tilde{a}, 1 \right) + \sum_{j=1}^{k} 2^{\left\lceil \log(\tilde{q} + (k+1)B) \right\rceil} \cdot C_j(s_1, \ldots, s_\ell) + \tilde{e} + r
= -\left\lfloor \frac{r}{\tilde{q}} \right\rfloor \cdot \tilde{q} + e + \sum_{j=1}^{k} 2^{\left\lceil \log(\tilde{q} + (k+1)B) \right\rceil} \cdot C_j(s_1, \ldots, s_\ell) + \tilde{e} + r
= \sum_{j=1}^{k} 2^{\left\lceil \log(\tilde{q} + (k+1)B) \right\rceil} \cdot C_j(s_1, \ldots, s_\ell) + e + r \mod \tilde{q}.
\]
Note that an upper bound for $\tilde{e} + e$ is $(k + 1) \cdot B$, and $\tilde{r}$ is a small perturbation due to the modulo $\tilde{q}$. This means that the output of the circuit is encoded as a high-order bit $\tilde{s}$ with probability 1 when $q$ is sufficiently large.

**Theorem 6 (Security of Split Homomorphic Encryption Scheme).** Let $q \geq 2^k + 2^\lceil \log(\tilde{q} + (k + 1)B) \rceil$. Assuming that the FHE scheme and the LHE scheme are secure schemes, then Scheme 4 satisfies the security model $O(\hat{pk}, \hat{pk}, q, \tilde{q})$ for split homomorphism.

**Proof.** Assume $(s_0, s_1, C_1, \ldots, C_\beta)$ is the adversary’s input chosen at the beginning of the generation of system $\pi$.

*Hybrid $H_0$:* Define the following original system. The challenger generates a distribution using a random coin toss as follows:

$$(pk, c = \widehat{Enc}(\hat{pk}, s_\delta), \rho_1, \ldots, \rho_\beta).$$

Where

$$pk = (\hat{pk}, \hat{pk}, \widehat{Enc}(\hat{pk}, T_1), \ldots, \widehat{Enc}(\hat{pk}, T_n)),$$

and $\rho_i$ is obtained from $PDec(sk, \text{Eval}(pk, C_i, c))$.

*Hybrids $H_1, \ldots, H_\beta$:* Let $\text{Eval}(pk, C_i, c)$ generate $d^{(i)}$. The $i$th $Hybrids$ $H_i$ is defined the same as $Hybrids$ $H_{i-1}$ except for the input $d^{(i)}$ and the output $a$ (or $\tilde{a}$) such that

$$c = \widehat{Enc}(\hat{pk}, \text{ECC}(C_i(s_\delta)) + \tilde{e} + e + r - \lfloor r/\tilde{q} \rfloor \cdot \tilde{q}),$$

where ECC is the high-order bit encoding defined in the homomorphic encryption part, $\tilde{e} + e$ is the decryption noise after homomorphic computation $(d^{(1)}, \ldots, d^{(k)}, \tilde{a})$, $r \leftarrow \mathbb{Z}_q$. $\hat{r}_i$ is the “decryption tweak” obtained using random coin toss $a$, which can be used to decrypt the ciphertext $c$.

Note that the decryption noise $\tilde{e} + e$ can be efficiently calculated using the FHE scheme key, therefore $\hat{r}_i$ can also be computed in polynomial time. The ciphertext distributions of $Hybrids$ $H_1, \ldots, H_\beta$ are consistent, with the only difference being the specific form of $\hat{r}_i$. This is because the LHE scheme has simulatable decryption tweaks, so the distribution of $H_i$ is consistent with the distribution of $H_{i-1}$, i.e.,

$$(pk, \widehat{Enc}(\hat{pk}, s_\delta), \hat{\rho}_1, \ldots, \hat{\rho}_{i-1}, \hat{\rho}_i, \hat{\rho}_{i+1}, \ldots, \hat{\rho}_\beta) = (pk, \widehat{Enc}(\hat{pk}, s_\delta), \hat{\rho}_1, \ldots, \hat{\rho}_{i-1}, \hat{\rho}_i, \hat{\rho}_{i+1}, \ldots, \hat{\rho}_\beta).$$
Hybrids $H_{\beta+1}, \ldots, H_{2\beta}$: The $\beta + i$th Hybrids and the previous $\beta$ Hybrids are different mainly in $a$, i.e.,

$$c = \overline{\text{Enc}}(pk, \text{ECC}(C_i(s_\beta))) + \check{e} + e + [r/\check{q}] \cdot \check{q} + \check{r} - [r/\check{q}] \cdot \check{q}$$

$$= \overline{\text{Enc}}(pk, \text{ECC}(C_i(s_\beta))) + \check{e} + e + \check{r}.$$

Where, $\check{r} \leftarrow Z_{\check{q}}$. Note that the distributions caused by these two Hybrids are different only when $r \in R$, where $R := \{q - (q \mod \check{q}), \ldots, q\}$. Because $\check{q}/q \leq 2^{-\lambda}$, these two distributions to be statistically close.

Hybrids $H_{2\beta+1}, \ldots, H_{3\beta}$: The $2\beta + i$th Hybrids are defined the same as the previous ones, except for the value of $a$, i.e.,

$$c = \overline{\text{Enc}}(pk, \text{ECC}(C_i(s_\beta)) + \check{y}).$$

Where the noise $\check{e}$ can be neglected in the calculation, therefore it is not reflected in the above equation. The difference between this and the previous Hybrids lies in whether the ciphertext contains $\check{e} + e$. Since an upper bound of the noise $\check{e} + e$ is $(k + 1) \cdot B$, and $\check{q} \geq 2^\lambda \cdot (k + 1) \cdot B$, according to Lemma 1, the distribution caused by this Hybrids is statistically indistinguishable from the previous one.

Hybrids $H_{3\beta+1}, \ldots, H_{3\beta+n}$: The $3\beta + i$th Hybrids are defined the same as the previous ones, except that the ciphertext $c(LHE,i)$ is derived from encrypting 0 with the public key. At this point, the LHE scheme key no longer contributes to $(\check{\rho}_1, \ldots, \check{\rho}_\beta)$, so use indistinguishability to demonstrate the semantic security of these Hybrids.

$$\begin{pmatrix}
\text{Enc}(pk, 0), \ldots, \text{Enc}(pk, 0), \text{Enc}(pk, T_1), \\
\text{Enc}(pk, T_{i+1}), \ldots, \text{Enc}(pk, T_n)
\end{pmatrix} 
\approx_c 
\begin{pmatrix}
\text{Enc}(pk, 0), \ldots, \text{Enc}(pk, 0), \\
\text{Enc}(pk, T_{i+1}), \ldots, \text{Enc}(pk, T_n)
\end{pmatrix}.$$

Hybrids $H_{3\beta+n}^{(0)}, \ldots, H_{3\beta+n}^{(b)}$: Fix the length of the challenge plaintext to $i$, and use the symbol $H_{3\beta+n}^{(i)}$ to represent the Hybrids at this point. The distribution of this Hybrids is

$$(pk, c = \overline{\text{Enc}}(pk, s_i), \check{\rho}_1, \ldots, \check{\rho}_\beta),$$

where

$$pk = (\hat{pk}, \overline{\text{Enc}}(pk, 0), \ldots, \overline{\text{Enc}}(pk, 0)).$$
Because the FHE scheme key is no longer encoded in the public parameters, there is no need to compute \((\tilde{\rho}_1, \ldots, \tilde{\rho}_\beta)\). Therefore, any advantage that the adversary has in distinguishing \(H_{3\beta+n}(0)\) and \(H_{3\beta+n}(1)\) cannot be greater than distinguishing \(\hat{\text{Enc}}(\hat{pk}, s_0)\) and \(\hat{\text{Enc}}(\hat{pk}, s_1)\). Therefore, the FHE scheme is computationally indistinguishable, thus proving the semantic security of the sFHE scheme.

5.2 Instantiation of Oracle Model

To complete the description of our scheme, we discuss some candidate instantiations \(O(\hat{pk}, pk, q, \tilde{q})\) of the oracle. We require the underlying LHE scheme to have a dense ciphertext space. We introduced the cyclic assumption introduced by Brakerski et al. [BDGM20] bridging the gap between FHE and LHE schemes. The oracle machine shown in Theorem 6 is just one of them, which is a special program obfuscation that enables the realization of split fully homomorphic schemes. Next, we introduce another oracle constructed by Brakerski et al. [BDGM20].

**Simple Candidate Quantum Oracle.** Let \(C\) be the ciphertext space of LHE. The first instantiation is to take the encryption algorithm in FHE and encrypt the key in LHE, \(\hat{c} \leftarrow \hat{\text{Enc}}(\hat{pk}, sk)\). Extract the ciphertext hash value of the homomorphic operation obtained through a hash function, which is used to fix the random coin in the algorithm. LHE ciphertext is sampled without knowing the underlying plaintext (which is why we need dense ciphertext), while FHE terms are calculated by homomorphically evaluating the decryption circuit and rounding the resulting message to the nearest multiple of \(\tilde{q}\).

Let \(D = (D_a)_{a \in C}\), where \(D_a\) is a set in the Hilbert space \(\mathcal{H}_{D_a} = \mathbb{C}[[0,1]^n \cup \{\bot\}]\). The Hilbert space \(\mathcal{H}_{D_a}\) can be seen as a space spanned by a set of orthogonal bases \(|b\rangle\), where \(b \in \{0, 1\}^n \cup \{\bot\}\). Let the unitary transformation \(U\) be defined as

\[
U|\bot\rangle = |\psi_0\rangle, U|\psi_0\rangle = |\bot\rangle \text{ and } U|\psi_b\rangle = |\psi_b\rangle, \forall b \in \{0, 1\}^n \setminus \{0\}^n.
\]

where \(|\psi_b\rangle := H|b\rangle\), and \(H\) is the Hadamard transform on \(\mathbb{C}[[0,1]^n] = (\mathbb{C}^2)^{\otimes n}\).

Let \(|b\rangle = 2^{-n/2} \sum_{\eta} (-1)^{\eta \cdot b} |\psi_{\eta}\rangle\), then we have

\[
U|b\rangle = |b\rangle + 2^{-n/2} (|\bot\rangle - |\psi_0\rangle).
\]
When the oracle is queried, the unitary transformation $O_{XYZ}$ acts on the query register $X$ and $Y$, and the database register $D$, with the specific expression

$$O_{XYZ} = \sum_a |a\rangle\langle a| \otimes O^a_{YD_a} \text{ and } O^a_{YD_a} = U_{D_a} \text{CNOT}_{YD_a} U_{D_a}.$$ 

where $\text{CNOT}|b\rangle|b\rangle = |b\rangle|b\oplus b\rangle$, $b, b_a \in \{0, 1\}^n$ and $\text{CNOT}|b\rangle|\perp\rangle = |b\rangle|\perp\rangle$. With these tools, present Don et al.’s quantum hash oracle model as follows:

$$y := \max_{a \in C} \left\{ b \in \{0, 1\}^n \mid \langle a, b \rangle \in R \right\}, \quad \tilde{y} \leftarrow \hat{\text{Eval}}(\hat{p}k, -\lfloor \hat{\text{Dec}}(\cdot, y) / \tilde{q} \rfloor \cdot \tilde{q}, \tilde{c})$$

Additionally, consider the following projector:

$$\Pi_{D_a} := \sum_{b, \langle a, b \rangle \in R} |b\rangle\langle b| \text{ and } \Pi^a_{D_a} := 1 - \sum_{a \in X} \Pi^a_{D_a} = \bigotimes_{a \in X} \Pi^a_{D_a}.$$

where $\Pi^a_{D_a} := 1_{D_a} - \Pi_{D_a}^a$. Furthermore, define the measurement $M = M^R$, and the following projector

$$\Sigma^a := \bigotimes_{a' < a} \Pi^a_{D_a'} \otimes \Pi^a_{D_a} \text{ and } \Sigma^0 := 1 - \sum_{a'} \Sigma^{a'} = \bigotimes_{a'} \Pi^{a'}_{D_a} = \Pi^0.$$ 

In addition, define the pure state measurement unitary transformation $M_{DP} = M^R_{DP} \in L(H_D \otimes H_R)$, i.e.,

$$M_{DP} := |\varphi\rangle_D |w\rangle_P \mapsto |\varphi\rangle_D |w + a\rangle_P.$$ 

Note that $y$ is an element in the ciphertext domain of LHE, and its form is

$$y = \text{Enc}(\hat{p}k, s).$$

For some $s \in \mathbb{Z}_q$, because LHE has a dense ciphertext domain. Furthermore, through the correctness of the FHE and LHE schemes, we have

$$\tilde{y} = \tilde{\text{Eval}}(\hat{p}k, -\lfloor \hat{\text{Dec}}(\cdot, y) / \tilde{q} \rfloor \cdot \tilde{q}, \tilde{c})$$

$$= \tilde{\text{Eval}}(\hat{p}k, -\lfloor \hat{\text{Dec}}(\cdot, y) / \tilde{q} \rfloor \cdot \tilde{q}, \hat{\text{Enc}}(\hat{p}k, \hat{s}k))$$

$$= \hat{\text{Enc}}(\hat{p}k, -\lfloor \hat{\text{Dec}}(\hat{s}k, y) / \tilde{q} \rfloor \cdot \tilde{q})$$

$$= \hat{\text{Enc}}(\hat{p}k, -\lfloor s / \tilde{q} \rfloor \cdot \tilde{q}).$$

Therefore, it can be seen that the formation of $(y, \tilde{y})$ is based on the following assumptions.

**Alternating Encryption Security.** The cyclic dependency introduced by $\tilde{c} = \hat{\text{Enc}}(\hat{p}k, \hat{s}k)$ in the security of LHE and FHE schemes (e.g., the split FHE construction in this paper includes the encryption of $\hat{s}k$ under $\hat{p}k$ in the public key) is considered a very mild assumption. Currently, it is the only known
method to construct FHE from the LWE problem through bootstrapping theorems [Gen09b].

**Perturbation.** In the case of $y := \max_{a \in C} | \{ b \in \{0, 1\}^n | \langle a, b \rangle \in \mathbb{R} \} |$, although $\tilde{y}$ is an FHE encryption of the correct value, it is not necessarily uniformly distributed. In particular, the randomness of $\tilde{y}$ may depend on the low-order bits of $s$ in a complex way. In the specific case of LWR-based schemes, the noise term may carry information about $s$ modulo $\tilde{q}$, which may introduce perturbation that interferes with decryption. However, the noise function is usually highly nonlinear, making it difficult to exploit. Therefore, we only consider the FHE.Eval algorithm.

**Perturbation Elimination.** Regarding the methods for eliminating the perturbation in LHE and FHE ciphertexts, we naturally think of ciphertext reprocessing techniques [DS16]: it can be expected that repeating bootstraping operations on FHE ciphertexts can eliminate the perturbation from LHE ciphertext noise. Unfortunately, our setting is different from the typical settings considered in the literature, as the ciphertext perturbation reprocessing algorithm must be executed by the distinguisher and cannot use private random coins. Although it seems difficult to formally analyze the effectiveness of these methods in our setting, we hope that these techniques may (at least heuristically) help mitigate the perturbation that interferes with decryption. This paper takes a different approach and provides a simple heuristic to alleviate perturbation. In short, the idea is to sample a set of random plaintexts and define a random string as the sum of a uniform subset $S$ of these plaintexts. For the construction described earlier, Brakerski et al.’s instantiation includes a ciphertext $\widehat{c} = \widehat{\text{Enc}}(\widehat{pk}, \overline{s\xi})$. The parameter $\sigma \in \text{poly}(n, m, q, p)$ of the scheme is determined by the length of the set $S$. The algorithm is presented randomly below, although this simplification can be easily bypassed using standard techniques (e.g., computing random coins using encrypted Hash($x$)).

$O(\widehat{pk}, \overline{pk}, q, \overline{q})(x)$: Input string $x \in \{0, 1\}^*$ and a random set $S \leftarrow \{0, 1\}^\sigma$. For all $i \in [\sigma]$, when $S_i = 1$, uniformly output sample

$$y_i := \max_{a \in C} | \{ b \in \{0, 1\}^n | \langle a, b \rangle \in \mathbb{R} \} |,$$
when $S_i = 0$, uniformly output sample $y_i \leftarrow \text{Enc}(pk, s_i)$, where $s_i$ is any known plaintext message. Then compute

$$\hat{y} \leftarrow \text{Eval} \left( \hat{pk}, -\sum_{i=1}^{\sigma} \frac{\text{Dec}(\cdot, y)}{\hat{q}} \cdot \hat{q}, c \right).$$

Let $g$ be a linear function defined as follows

$$g(x_1, \ldots, x_S) = \sum_{i \in S} x_i + \sum_{i \in \bar{S}} \left\lfloor \frac{x_i}{\hat{q}} \right\rfloor \cdot \hat{q}.$$ 

Then compute $\hat{y} \leftarrow \text{Eval}(pk, g, \{y_i\}_{i \in S})$ and return $(y, \hat{y})$. By the correctness of homomorphic operations in the FHE scheme, it shown that

$$\hat{y} = \text{Eval}(\hat{pk}, g, \{y_i\}_{i \in S}) = \text{Eval}(\hat{pk}, \sum_{i=1}^{\sigma} \frac{\text{Dec}(\cdot, y)}{\hat{q}} \cdot \hat{q}, \text{Enc}(\hat{pk}, \hat{s}))$$

$$= \text{Enc}(\hat{pk}, \sum_{i=1}^{\sigma} \frac{\text{Dec}(\hat{s}k, y)}{\hat{q}} \cdot \hat{q}) = \text{Enc}(\hat{pk}, \sum_{i=1}^{\sigma} \frac{s_i}{\hat{q}} \cdot \hat{q}).$$

Combining with the correctness of the LHE scheme, one obtain

$$y = \text{Eval}(pk, g, \{y_i\}_{i \in S}) = \text{Eval}(pk, g, \{\text{Enc}(pk, s_i)\}_{i \in S})$$

$$= \text{Enc}(pk, \sum_{i \in S} s_i + \sum_{i \in \bar{S}} \left\lfloor \frac{s_i}{\hat{q}} \right\rfloor \cdot \hat{q}) = \text{Enc}(pk, \sum_{i \in S} (s_i \mod \hat{q}) + \sum_{i \in \bar{S}} \left\lfloor \frac{s_i}{\hat{q}} \right\rfloor \cdot \hat{q}).$$

### 6 Constructing Ideal Obfuscation using Homomorphic Splitting Encryption Scheme

#### 6.1 Ideal Obfuscation

**Scheme 5** Ideal Obfuscation Scheme

**KeyGen**$(n, m, q)$. For $i \in [0, D)$, $j \in [0, B]$, randomly sample $k_{i,j} \leftarrow \{0,1\}^\lambda$ and compute

$$h_{i,j} = \text{PrO}(k_{i,j}, x).$$

Randomly sample $s_e \leftarrow \{0,1\}^\lambda$. For $d \in [0, D)$, input security parameter $n$, output sample $(sk_d, pk_d) \leftarrow \text{KeyGen}(n)$. Let $\mathbb{Z}_q$ be the plaintext space under
Define linear function over \( \mathbb{Z} \). Let \( \hat{sk}_d = (T_1, \ldots, T_n) \in \{0, 1\}^{n \times n} \), then return \( \hat{sk}_d = \hat{sk}_d \) and \( \hat{pk}_d = (\hat{pk}_d, \hat{pk}_d, c_1, \ldots, c_n) \).

where, for any \( i \in [n] \), we define \( \tau_i \leftarrow \text{Enc}(\hat{pk}_d, T_i) \).

**Enc(\( \hat{pk}_d, \text{info}_\varepsilon \)).** For input \( \text{info}_\varepsilon = (\text{normal}, \varepsilon, \{k_{i,j}\}_{i \in [0,D], j \in [1,B], s_\varepsilon}) \), return \( \text{ct}_\varepsilon \leftarrow \text{Enc}(\hat{pk}_d, \text{info}_\varepsilon) \).

**Eval(\( \hat{pk}_d, \text{f}_d, (c_1, \ldots, c_\ell) \)).** \( \text{f}_d \) is provided later. Input circuit \( C \) of \( \ell \) bits and ciphertext of length \( k \) bits \((c_1, \ldots, c_\ell) \). For any \( j \in [k] \), where \( C_j \) is the \( j \)-th component of circuit \( C \), compute

\[
\hat{d}_j \leftarrow \text{Eval}(\hat{pk}_d, C_j, (c_1, \ldots, c_\ell)).
\]

Define linear function over \( \mathbb{Z}_q \) as

\[
g(x_1, \ldots, x_n) = \sum_{j=1}^{k} \text{DEC&Mult} \left( (x_1, \ldots, x_n), \hat{d}_j, 2^{\log(\hat{\gamma}+(k+1)B)}+j \right).
\]

Compute \( \hat{d} \leftarrow \text{Eval}(\hat{pk}_d, g, (\tau_1, \ldots, \tau_n)) \), then query \( (a, \hat{\gamma}) \leftarrow \mathcal{O}_{(\hat{pk}_d, \hat{pk}_d, q, \hat{\gamma})}(\hat{d}) \) and define the following linear function

\[
\hat{\gamma}(x_1, \ldots, x_n, x_{n+1}, x_{n+2}) = \text{DEC&Mult}((x_1, \ldots, x_n), \hat{\gamma}, 1) + x_{n+1} + x_{n+2}.
\]

Output \( \text{ct}_\varepsilon \leftarrow \text{Eval}(\hat{pk}_d, \hat{\gamma}, (\tau_1, \ldots, \tau_n), \hat{d}, a) \).

Return the obfuscated circuit

\[
\hat{C} = (\{h_{i,j}\}_{i \in [0,D], j \in [1,B]}, \text{ct}_\varepsilon, \{sk_d\}_{d \in [0,D]}).
\]

**Eval&Expand.** (normal mode)

- For \( d \in [0, D) \), Eval&Expand encrypts \( \text{f}_d(\text{normal, } \chi, \{k_{i,j}\}_{i \in [0,D], j \in [1,B]}, s_\chi) \)
  1. Compute \( s_\chi \| r_\chi \| s_\chi \| 1 \| r_\chi \| 1 \leftarrow G(s_\chi) \).
  2. For \( b \in \{0, 1\} \), run \( \text{ct}_\chi \| b \leftarrow \text{Enc}(\hat{pk}_{d+1}, \text{info}_\chi \| b, r_\chi \| b) \) where,

\[
\text{info}_\chi \| b = (\text{normal, } C, \chi \| b, \{k_{i,j}\}_{i \in [d+1,D], j \in [1,B]}, s_\chi \| b),
\]

\( C \) is the circuit to be obfuscated. Output

\[
(H(k_{d,1}, \chi)) \cdots (H(k_{d,B}, \chi)) \oplus (\text{ct}_\chi \| 0 \| \text{ct}_\chi \| 1).
\]
For $d = D$, $f_D(\text{normal}, C, x, s_x)$, output $C(x)$. 

\[ \hat{C}_O[ct_x, \{sk_d\}_{d \in [0,D]}, \{h_{i,j}\}_{i \in [0,D], j \in [0,B]}](x) \]

**Hardwired.** $ct_x$, initial ciphertext.

$sk_d$, secret key.

$h_{i,j}$, handles generated by PrOM.

**Input.** $x \in \{0, 1\}^D$, input circuit.

**Output.** Compute as follows.

For $d = 0, \ldots, D - 1$:

\[ \chi_d \leftarrow x \leq d \]

\[ \nu_{x_d} \leftarrow \text{Rec}(\rho_{x_d}, ct_{x_d}), \quad \rho_{x_d} \leftarrow \text{PDec}(sk_d, ct_{x_d}) \]

\[ \text{otp}_{x_d} \leftarrow O(h_{\text{Eval}}, h_{d,1}, \chi_d[0^{D-d}]) \cdots || O(h_{\text{Eval}}, h_{d,B}, \chi_d[0^{D-d}]) \]

\[ ct_{x_d}[0 || ct_{x_d}[1] \leftarrow \nu_{x_d} \oplus \text{otp}_{x_d} \]

Output $\text{Dec}(sk_D, ct_x)$

**Fig. 1.** Obfuscated Circuit $(\hat{C}_O) \rightarrow \hat{C}^*_{x, \{sk_d\}_{d \in [0,D]}, \{h_{i,j}\}_{i \in [0,D], j \in [0,B]}]}$

**Correctness Analysis.** According to the obfuscation form $\hat{C}_O$ in Figure 3 and the tree structure in Figure 2.

\[ H(k_{d,1}, \chi_d[0^{D-d}]) \cdots || H(k_{d,B}, \chi_d[0^{D-d}]) = O(h_{\text{Eval}}, h_{d,1}, \chi_d[0^{D-d}]) \cdots || O(h_{\text{Eval}}, h_{d,B}, \chi_d[0^{D-d}]). \]

**6.2 Security Analysis**

**Lemma 11.** Assuming $H$ is a pseudo-random function, $G_{sr}$, $G_v$ are pseudo-random generators, and $(Gen, Enc, Enc)$ is adaptively secure, with appropriate parameters $L$ and $B$, then Construction 1 in [JLLW23] is an ideal obfuscation under PrOM.

**Theorem 7.** Assuming $H$ is a pseudo-random function, $G_{sr}$, $G_v$ are pseudo-random generators, algorithm 5 is an ideal obfuscation under PrOM.
Fig. 2. The binary tree of ciphertexts [JLLW23] in Scheme 5

Expand_{d,by_{d+1}}(\chi, \text{info}_\chi)

Hardwired. \(pk_{d+1}\), public key at level \((d + 1)\).

Input. \(x \in \{0, 1\}^4\); input appropriate circuit;

\(\text{info}_\chi = (C, \{k_{i,j}\}_{i \in \{d+1, D\}, j \in \{1, B\}}, s_\chi, \beta, \{\sigma_{\chi,j}\}_{j \in \{0, \beta\}}, w_\chi, \{k_{d,j}\}_{j \in \{\sigma, B\}})\):

- \(C\), circuit to be obfuscated.
- \(k_{i,j}\), keys of \(H\) at levels \((d + 1, \ldots, D - 1)\).
- \(s_\chi\), seed of pseudo-random generator \(G_{sr}\), related to \(\chi\).
- \(\beta\), mixing index.
- \(\sigma_{\chi,j}\), seed of pseudo-random generator \(G_v\), related to \(\chi\).
- \(w_\chi\), decryption result of the software module.
- \(k_{d,j}\), keys of \(H\) at level \((d + 1)\).

Output. Calculated as follows.

\(s_\chi \| r_{\chi,0} \| s_\chi \| r_{\chi,1} \leftarrow G_{sr}(s_\chi)\)

For \(\eta = 0, 1\):

- \(\text{flag}_\chi \| \eta \leftarrow \text{normal}\)
- \(\text{info}_\chi \| \eta \leftarrow (C, \{k_{i,j}\}_{i \in \{d+1, D\}, j \in \{1, B\}}, s_\chi \| \eta)\)
- \(ct_\epsilon \leftarrow \text{Enc}(pk_{d+1}, \text{flag}_\chi \| \eta, \chi \| \eta, \text{info}_\chi \| \eta)\)

Output \(\nu_\chi \leftarrow G_v(\sigma_{\chi, 1}) \| \cdots \| G_v(\sigma_{\chi, \beta - 1}) \| w_\chi\)

\(\|([ct_\chi \| ct_\chi]^{[\beta+1]} \oplus H(k_{d, \beta+1}, \chi \| [0^{D-d}])) \| \cdots \)

\(\|([ct_\chi \| ct_\chi]_B \oplus H(k_{d, B}, \chi \| [0^{D-d}]))\)

Fig. 3. Obfuscation circuit \((\hat{C}^\odot) \rightarrow \hat{C}^*\[ct_x, \{sk_d\}_{d \in \{0, D\}}, \{h_{i,j}\}_{i \in \{0, D\}, j \in \{0, B\}}]\)
Expand_{d}[pk_{d+1}](\text{flag}_x, \text{info}_x) - For Level $d \in [0, D)$

Hardwired. $pk_{d+1}$, $(d + 1)$ level public key.

Input. \text{flag}_x \in \{\text{normal}, \text{hyb}, \text{sim}\}$, flag matching with $\chi$.
$\chi \in \{0, 1\}^D$, input appropriate prefix for the circuit.
info$_x$, information matching with $\chi$, changes with flag$_x$.

Output.
\[
\begin{cases}
\text{Expand}_{d, \text{normal}}[pk_{d+1}](\chi, \text{info}_x), & \text{if flag}_x = \text{normal}; \\
\text{Expand}_{d, \text{hyb}}[pk_{d+1}](\chi, \text{info}_x), & \text{if flag}_x = \text{hyb}; \\
\text{Expand}_{d, \text{hyb}}(\chi, \text{sim}_x), & \text{if flag}_x = \text{sim}.
\end{cases}
\]

Eval(\text{flag}_x, \chi, \text{info}_x) - For Level $D$

Hardwired. $pk_{d+1}$, $(d + 1)$ level public key.

Input. \text{flag}_x \in \{\text{normal}, \text{sim}\}$, flag matching with $\chi$.
$\chi \in \{0, 1\}^D$, input circuit.
info$_x$, information matching with $\chi$, changes with flag$_x$.

Output.
\[
\begin{cases}
\text{Eval}_{d, \text{normal}}(\chi, \text{info}_x), & \text{if flag}_x = \text{normal}; \\
\text{Eval}_{d, \text{sim}}(\chi, \text{info}_x), & \text{if flag}_x = \text{sim}.
\end{cases}
\]

Expand$_{d, \text{normal}}[pk_{d+1}](\chi, \text{info}_x)$

Hardwired. $pk_{d+1}$, $(d + 1)$ level public key.

Input. $\chi \in \{0, 1\}^D$, input appropriate prefix for the circuit.

\begin{itemize}
  \item info$_x = (C, \{k_{i,j}\}_{i \in [d+1:D], j \in [1:B]}, s_x)$:
    \begin{itemize}
      \item $C$, circuit to be obfuscated.
      \item $k_{i,j}$, keys for hash functions $d, \ldots, D - 1H$.
      \item $s_x$, seed for pseudo-random generator $G_{sr}$ corresponding to $\chi$.
    \end{itemize}
\end{itemize}

Output. Perform the following calculations.
\[
s_x \| r_x^0 \| s_x \| r_x^{D-1} \leftarrow G_{sr}(s_x).
\]

for $\eta = 0, 1$:
\[
\begin{itemize}
  \item flag$_x|\eta \leftarrow \text{normal}$
  \item info$_x|\eta \leftarrow (C, \{k_{i,j}\}_{i \in [d+1:D], j \in [1:B]}, s_x|\eta)$.
  \item ct$_x|\eta \leftarrow \text{Enc}(pk_{d+1}, \text{flag}_x|\eta, \chi|\eta, \text{info}_x|\eta)$
  \item otp$_x \leftarrow H(k_{d,1}, \chi|0^{D-d}) \cdots H(k_{d,B}, \chi|0^{D-d})$
\end{itemize}

Output $\nu_x \leftarrow (ct_x^0 \| ct_x^1) \oplus \text{otp}_x$

Eval$_{\text{normal}}(\chi, \text{info}_x)$

Input. $\chi \in \{0, 1\}^D$, input circuit.

\begin{itemize}
  \item info$_x = (C, s_x)$:
    \begin{itemize}
      \item $C$, circuit to be obfuscated.
      \item $s_x$, unused seed.
    \end{itemize}
\end{itemize}

Output. $C(\chi)$, compute the evaluation of a generalized circuit $(C, \chi)$.
References


Steven Yue. Introduction to io 01: What is indistinguishability obfuscation (io)?, 2020.