Oblivious Transfer and n-Variate Linear Function Evaluation

Yeow Meng Chee, Huaxiong Wang, and Liang Feng Zhang

School of Physical and Mathematical Sciences
Nanyang Technological University
21 Nanyang Link, Singapore 637371
{ymchee,hxwang}@ntu.edu.sg
liangf.zhang@gmail.com

Abstract. We define a new cryptographic primitive which is called *Oblivious n-variate Linear Function Evaluation with choice space $\mathcal{C}$* and denoted by $\mathcal{C}$-OLFE$_n$. The primitive captures a variety of well-known cryptographic primitives and is an interesting stepstone in secure protocol design. We present a statistically secure reduction from $\binom{n}{1}$-OT to kn invocations of $\mathcal{C}$-OLFE$_n$, where k is the security parameter and $\mathcal{C}$ contains all unit vectors of length n. The reduction allows us to reverse $\binom{n}{1}$-OT for any integer $n \geq 2$.

1 Introduction

This paper describes a new cryptographic primitive, Oblivious n-Variate Linear Function Evaluation with choice space $\mathcal{C}$ ($\mathcal{C}$-OLFE$_n$) which captures a variety of well-known cryptographic primitives. The primitive is always associated with a finite field $\mathbb{F}$ and involves a sender Alice who has an n-variate linear function $s(x) = \sum_{i=1}^{n} s_i x_i \in \mathbb{F}[x]$ and a receiver Bob who has a choice $c \in \mathcal{C} \subseteq \mathbb{F}^n$. It allows the receiver Bob to evaluate $s(c)$ in such a way that Alice cannot learn c and Bob learns no more information on $s(x)$ except $s(c)$. The $\mathcal{C}$-OLFE$_n$ is an interesting stepstone in secure OT protocol design.

Oblivious Transfer (OT) [14,10,4] is an important cryptographic primitive and has numerous applications in cryptographic study and protocol design [15,11,12]. Rabin's OT [14] allows a sender Alice to send a bit b to a receiver Bob such that with probability 1/2 Bob obtains the bit, and with the same probability he does not, while Alice does not know which event has occurred. The $\binom{n}{1}$-OT [10,4] involves a sender Alice who has n secrets $s_1, \ldots, s_n$ and a receiver Bob who has a choice $c \in [n]$. It allows Bob to obtain s_c and no more information while c is not revealed to Alice. A number of other variants of OT have been defined and extensively studied [6,5,2,1,3] as well. For example, one of them is the XOT, where the sender Alice has two bits b_0, b_1 and the receiver Bob is allowed to obtain b_c for a choice $c \in \{0, 1, \oplus\}$, where $b_\oplus = b_0 \oplus b_1$. Almost all variants of OT, including Rabin's OT, $\binom{n}{1}$-OT and the XOT, have been shown information-theoretically equivalent to each other [8,3]. The $\mathcal{C}$-OLFE$_n$ is also related to *Oblivious Polynomial Evaluation* (OPE) [13], which is a primitive

B. Fu and D.-Z. Du (Eds.): COCOON 2011, LNCS 6842, pp. 627–637, 2011.

between a sender Alice who has a polynomial $s(x) = \sum_{i=0}^{n-1} s_i x^i \in \mathbb{F}[x]$ and a receiver Bob who wants to evaluate $s(\alpha)$ for an $\alpha \in \mathbb{F}$. It requires that Alice cannot learn α and Bob learns no more information on $s(x)$ except $s(\alpha)$.

$\mathcal{C}$-OLFE$_n$ captures a number of well-known cryptographic primitives. For any integer $n \geq 2$, the $\binom{n}{1}$-OT with $s = (s_1, \ldots, s_n)$ as Alice's input is a $\mathcal{C}$-OLFE$_n$ with $s(x) = \sum_{i=1}^{n} s_i x_i$ and $\mathcal{C}$ be the set of all unit vectors. The XOT with (b_0, b_1) as Alice's input is a $\mathcal{C}$-OLFE$_n$ with $s(x) = b_0 x_0 \oplus b_1 x_1$ and $\mathcal{C} = \{0,1\}^2 \setminus \{(0,0)\}$. The OPE with $s(x) = \sum_{i=0}^{n-1} s_i x^i$ as Alice's input is a $\mathcal{C}$-OLFE$_n$ with $\mathcal{C} = \{(1, \alpha, \ldots, \alpha^{n-1}) : \alpha \in \mathbb{F}\}$. We show that $\mathcal{C}$-OLFE$_n$ and $\binom{n}{1}$-OT are equivalent primitives, in the sense that there are statistically secure reductions between them. In particular, we present a statistically secure reduction from $\binom{n}{1}$-OT to $\mathcal{C}$-OLFE$_n$ in the real/ideal model simulation paradigm.

Theorem I. *The $\binom{n}{1}$-OT can be statistically securely reduced to kn invocations of a $\mathcal{C}$-OLFE$_n$, where k is the security parameter and $\mathcal{C}$ contains all unit vectors of length n.*

Crépeau et al. [9] raised the question of whether it is possible to implement OT in one direction using several invocations of OT in the other. The question arises in a scenario where one party is much more powerful in terms of computational power or technology than the other party. In such a setting, one can make a computational assumption on the weaker party but not on the other. Crépeau et al. [9] proved that a $\binom{2}{1}$-OT in one direction can be reduced to $4k$ invocations of a $\binom{2}{1}$-OT in the other. Our reduction in Theorem I can be applied to reverse $\binom{n}{1}$-OT for *any* $n \geq 2$. More precisely, we have that

Theorem II. *The* $\binom{n}{1}$-OT *from Alice to Bob can be statistically securely reduced to $kn(n-1)$ invocations of the* $\binom{n}{1}$-OT *from Bob to Alice, where k is the security parameter.*

2 Preliminaries

For a positive integer n, we denote by $\mathbb{S}_n$ the set of all permutations of integers in $[n] = \{1, 2, \ldots, n\}$. The complement of a set P is denoted by $\bar{P}$. Let M be a $k \times n$ matrix. For $P \subseteq [k]$ and $Q \subseteq [n]$, the submatrix of M with rows indexed by P and columns indexed by Q is denoted by $M[\![P, Q]\!]$. We also denote $M[\![P, *]\!] = M[\![P, [n]]\!]$. The *support* of a vector v is defined to be $N(v) = \{t : v_t \neq 0\}$. $\mathbf{1}$ and $\mathbf{0}$ denote the all-one and all-zero vectors, respectively. A function $\delta : \mathbb{N} \to [0,1]$ is *negligible* if $\delta(k) < k^{-d}$ for any integer $d > 0$ and sufficiently large $k \in \mathbb{N}$.

We denote by $w \leftarrow \mathbb{W}$ the experiment of choosing a random element from $\mathbb{W}$. Let U and V be random variables. The *statistical distance* between U and V is defined to be $\mathcal{SD}(U,V) = \frac{1}{2}\sum_w |\Pr[U = w] - \Pr[V = w]|$. We denote by $\Pr[U = u | V = v]$ the *conditional probability* that $U = u$ given $V = v$. A *distribution ensemble* $X = \{X(k,a)\}_{k \in \mathbb{N}, a \in D}$ is an infinite sequence of probability distributions $X(k,a)$, where $k \in \mathbb{N}$ and $a \in D$.

Definition 1. *Two distribution ensembles X and Y are* equally distributed *(and write $X \equiv Y$) if $X(k,a)$ and $Y(k,a)$ are identical for all k and all a.*

Definition 2. *Two distribution ensembles X and Y are* statistically indistinguishable *(and write $X \approx Y$) if $\mathcal{SD}(X(k,a), Y(k,a)) < \delta(k)$, for all sufficiently large k and all a, where $\delta : \mathbb{N} \to [0,1]$ is a negligible function.*

The functionalities of $\binom{n}{1}$-OT and $\mathcal{C}$-OLFE$_n$ are defined as follows.

Definition 3. *Let $\mathbb{F}$ be a finite field. $\binom{n}{1}$-OT is a primitive between a sender Alice who has as input n secrets $s = (s_1, \ldots, s_n) \in \mathbb{F}^n$ and no output, and a receiver Bob who has as input a choice $c \in [n]$ and outputs s_c.*

Definition 4. *Let $\mathbb{F}$ be a finite field and $\mathcal{C} \subseteq \mathbb{F}^n$. $\mathcal{C}$-OLFE$_n$ is a primitive between a sender Alice who has as input $s(x) = \sum_{i=1}^{n} s_i x_i \in \mathbb{F}[x]$ and no output, and a receiver Bob who has as input a choice $c \in \mathcal{C}$ and outputs $s(c)$.*

We define their security in terms of general secure two-party function evaluation. Our definition follows the vein of [7]. Let f be a *two-party function* which maps any tuple (k, x_1, x_2) of security parameter k, inputs x_1 and x_2 to a pair of outputs. A *two-party protocol* for f is a pair $(\mathcal{P}_1, \mathcal{P}_2)$ of interactive Turing machines, where each machine $\mathcal{P}_i$ starts with (k, x_i). The definition is given by comparing the ideal model and hybrid model. In the *ideal model*, the two parties do not interact with each other and evaluate $f(k, x_1, x_2)$ with the help of a trusted third party $\mathcal{T}^f$ (which implements the functionality of f) and in the presence of an ideal model adversary $\mathcal{S}$. Let g be a two-party function as well. In the *g-hybrid model*, the two parties interact with each other and evaluate $f(k, x_1, x_2)$ with the help of a trusted third party $\mathcal{T}^g$ (which implements the functionality of g) and in the presence of a g-hybrid model adversary $\mathcal{H}$.

Ideal Model. Let $\mathcal{P}_i$ be the party corrupted by $\mathcal{S}$ and z be the auxiliary input of $\mathcal{S}$. The entities $\mathcal{P}_1$, $\mathcal{P}_2$, $\mathcal{T}^f$ and $\mathcal{S}$ start with $(k, x_1), (k, x_2), k$ and (k, x_i, z), respectively.

1. *Substitution: $\mathcal{S}$ instructs $\mathcal{P}_i$ to substitute its input x_i with x_i'.*
2. *Computation: The parties send x_{3-i} and x_i' to $\mathcal{T}^f$; then $\mathcal{T}^f$ computes $(f_1, f_2) = f(k, x_1', x_2)$ if $i = 1$ and $(f_1, f_2) = f(k, x_1, x_2')$ if $i = 2$, and sends f_1, f_2 to $\mathcal{P}_1, \mathcal{P}_2$, respectively.*
3. *Output: $\mathcal{P}_{3-i}$ outputs f_{3-i}, $\mathcal{P}_i$ outputs $\perp$ and $\mathcal{S}$ outputs an arbitrary function of its view of the computation.*

The *global output* $\mathrm{IDEAL}_{f,\mathcal{S}}(k, \boldsymbol{x}, z)$ of the ideal model is defined to be the concatenation of the outputs of $\mathcal{S}$ and $\mathcal{P}_1, \mathcal{P}_2$, where $\boldsymbol{x} = x_1 x_2$. We denote $\mathrm{IDEAL}_{f,\mathcal{S}} = \{\mathrm{IDEAL}_{f,\mathcal{S}}(k, \boldsymbol{x}, z)\}_{k \in \mathbb{N}, \langle \boldsymbol{x}, z \rangle \in \{0,1\}^*}$.

Hybrid Model. Let $\mathcal{P}_i$ be the party corrupted by $\mathcal{H}$ and z be an auxiliary input of $\mathcal{H}$. The entities $\mathcal{P}_1$, $\mathcal{P}_2$, $\mathcal{T}^g$ and $\mathcal{H}$ start with $(k, x_1), (k, x_2), k$ and (k, x_i, z), respectively.

1. *Computation: The computation consists of a number of* interactive rounds *and g-*rounds*.*

- *In each interactive round, only one party is active. If $\mathcal{P}_{3-i}$ is active, then it generates and sends a message m_{3-i} to $\mathcal{P}_i$ according to the protocol specification. If $\mathcal{P}_i$ is active, then the adversary $\mathcal{H}$ generates a message m_i and instructs $\mathcal{P}_i$ to send m_i to $\mathcal{P}_{3-i}$.*
- *In each g-round, both parties are active. $\mathcal{P}_{3-i}$ sends an input y_{3-i} to $\mathcal{T}^g$ which is specified by the protocol; $\mathcal{H}$ decides an input y_i and instructs $\mathcal{P}_i$ to send y_i to $\mathcal{T}^g$. At last, $\mathcal{T}^g$ evaluates $(g_1, g_2) = g(k, y_1, y_2)$ and sends g_1, g_2 to $\mathcal{P}_1$, $\mathcal{P}_2$, respectively.*

2. *Output: $\mathcal{P}_{3-i}$ outputs whatever specified by the protocol; $\mathcal{P}_i$ outputs $\perp$ and $\mathcal{H}$ outputs an arbitrary function of its* view *of the computation.*

The *global output* $\mathrm{EXEC}_{\pi^g,\mathcal{H}}(k, \boldsymbol{x}, z)$ of the hybrid model is defined to be the concatenation of the outputs of $\mathcal{H}$ and $\mathcal{P}_1, \mathcal{P}_2$, where $\boldsymbol{x} = x_1 x_2$. We denote $\mathrm{EXEC}_{\pi^g,\mathcal{H}} = \{\mathrm{EXEC}_{\pi^g,\mathcal{H}}(k, \boldsymbol{x}, z)\}_{k\in\mathbb{N},\langle \boldsymbol{x},z\rangle\in\{0,1\}^*}$.

Definition 5. *Let f and g be two-party functions. A two-party protocol π^g for f in the g-hybrid model* evaluates f statistically securely *if for every g-hybrid model adversary $\mathcal{H}$, there is an ideal model adversary $\mathcal{S}$ whose running time is polynomial in that of $\mathcal{H}$ such that* $\mathrm{IDEAL}_{f,\mathcal{S}} \approx \mathrm{EXEC}_{\pi^g,\mathcal{H}}$. *In particular, if* $\mathrm{IDEAL}_{f,\mathcal{S}} \equiv \mathrm{EXEC}_{\pi^g,\mathcal{H}}$, *then we say that π^g* evaluates f perfectly securely.

A *reduction* from f to g is a two-party protocol π^g for f in the g-hybrid model. We say that π^g *implements f statistically (resp. perfectly) securely* if π^g evaluates f statistically (resp. perfectly) securely in the g-hybrid model.

3 Statistically Secure Reduction from $\binom{n}{1}$-OT to $\mathcal{C}$-OLFE$_n$

Let $f = \binom{n}{1}$-OT and $g = \mathcal{C}$-OLFE$_n$, where $\mathcal{C}$ contains all unit vectors in $\mathbb{F}^n$. We present a statistically secure reduction from f to g in this section. As a basic step, we suppose that $\mathcal{C} = \mathbb{F}^n$. The reduction is depicted by Fig. 1.

The correctness of π^g is easy and shown by the following lemma.

Lemma 1. *If Alice and Bob are honest, then* $\mathrm{IDEAL}_{f,\mathcal{S}} = \mathrm{EXEC}_{\pi^g,\mathcal{H}}$, *where $\mathcal{S}$ is the ideal model adversary corrupting no party and $\mathcal{H}$ is the g-hybrid model adversary corrupting no party.*

- input: Alice has n secrets $s \in \mathbb{F}^n$ and Bob has a choice $c \in [n]$;
- subroutine: the trusted third party $\mathcal{T}^g$;

1. Alice: choose $\phi_j \leftarrow \mathbb{S}_n$, $X_j \leftarrow \mathbb{F}^{n\times n}$ for every $j \in [k]$ s.t. $\sum_{j=1}^{k} X_j[\![\phi_j(i), i]\!] = s_i$ for every $i \in [n]$;
2. $\mathcal{T}^g$: for $(j, i) \in [k] \times [n]$, Alice and Bob proceeds as follows
   - Alice: send $(X_j[\![i, 1]\!], \ldots, X_j[\![i, n]\!])$ to $\mathcal{T}^g$;
   - Bob: send the c-th unit vector in $\mathbb{F}^n$ to $\mathcal{T}^g$ and receive Y_{ji} from $\mathcal{T}^g$;
3. Alice: send the permutations $\phi_1, \ldots, \phi_k$ to Bob;
4. Bob: output $\sum_{j=1}^{k} Y_{j\phi_j(c)}$.

Fig. 1. A reduction from $\binom{n}{1}$-OT to $\mathcal{C}$-OLFE$_n$ (π^g)

- input: (k, s, z), where $s \in \mathbb{F}^n$ is Alice's input and z is an auxiliary input;
- subroutine: the g-hybrid model adversary $\mathcal{H}$ and the trusted third party $\mathcal{T}^f$;

1. feed $\mathcal{H}$ with (k, s, z);
2. receive the k matrices $X' = (X'_1, \ldots, X'_k)$ which are decided by $\mathcal{H}$ and then sent to $\mathcal{T}^g$ by Alice.
3. receive the k permutations $\phi' = (\phi'_1, \ldots, \phi'_k)$ which are decided by $\mathcal{H}$ and then sent to Bob by Alice.
4. for every $i \in [n]$, set $s'_i = \sum_{j=1}^{k} X'_j[\![\phi'_j(i), i]\!]$ and send $s' = (s'_1, \ldots, s'_n)$ to $\mathcal{T}^f$.
5. output whatever $\mathcal{H}$ outputs, say $\mathcal{H}(k, s, z, \phi', X')$.

Fig. 2. Ideal model adversary corrupting Alice for π^g

Proof. Given (k, s, c, z), we have that $\mathrm{IDEAL}_{f,\mathcal{S}}(k, s, c, z) = (\perp, \perp, s_c) \equiv (\perp, \perp, \sum_{j=1}^{k} X_j[\![\phi_j(c), c]\!]) = (\perp, \perp, \sum_{j=1}^{k} Y_{j\phi_j(c)}) = \mathrm{EXEC}_{\pi^g,\mathcal{H}}(k, s, c, z)$, where all random variables only depend on the uniform and independent coin tosses of Alice and Bob.

Next lemma shows that the receiver's privacy is achieved.

Lemma 2. *For any g-hybrid model adversary $\mathcal{H}$ corrupting Alice, there is an ideal model adversary $\mathcal{S}$ corrupting Alice whose running time is polynomial in that of $\mathcal{H}$ such that* $\mathrm{IDEAL}_{f,\mathcal{S}} \equiv \mathrm{EXEC}_{\pi^g,\mathcal{H}}$.

Proof. The ideal model adversary $\mathcal{S}$ is depicted by Fig. 2. Given (k, s, c, z), we have that $\mathrm{IDEAL}_{f,\mathcal{S}}(k, s, c, z) = (\mathcal{H}(k, s, z, \phi', X'), \perp, s'_c) = (\mathcal{H}(k, s, z, \phi', X'), \perp, \sum_{j=1}^{k} X'_j[\![\phi'_j(c), c]\!]) \equiv (\mathcal{H}(k, s, z, \phi, X), \perp, \sum_{j=1}^{k} X_j[\![\phi_j(c), c]\!]) = (\mathcal{H}(k, s, z, \phi, X), \perp, \sum_{j=1}^{k} Y_{j\phi_j(c)}) = \mathrm{EXEC}_{\pi^g,\mathcal{H}}(k, s, c, z)$, where the random variables only depend on the uniform and independent coin tosses of $\mathcal{H}$.

It remains to show the sender's privacy. Given (k, c), let $c_{ji} \in \mathbb{F}^n$ be the choice vector sent by Bob in the (j, i)-th invocation of $\mathcal{T}^g$ for every $(j, i) \in [k] \times [n]$. Given (k, s), the honest sender Alice always choose the matrices $X_1, \ldots, X_k$ according to π^g. For every $(j, i) \in [k] \times [n]$, a message Y_{ji} is sent to Bob by $\mathcal{T}^g$. Clearly, we have the following equation system:

$$\begin{cases} c_{ji} \cdot X_j[\![i, *]\!] = Y_{ji} & \text{for every } (j, i) \in [k] \times [n], \\ \sum_{j=1}^{k} X_j[\![\phi_j(i), i]\!] = s_i & \text{for every } i \in [n], \end{cases} \tag{1}$$

where the vector of unknowns is $X = (X_1[\![1, 1]\!], \ldots, X_1[\![n, n]\!], \ldots, X_k[\![n, n]\!])$ and the vector of constant terms is $Y = (Y_{11}, \ldots, Y_{1n}, \ldots, Y_{kn}, s_1, \ldots, s_n)$. Let C be the coefficient matrix of (1). Let V_{que} and V_{sec} be the vector spaces spanned by the first kn rows and the last n rows of C, respectively. For integers $i \in [n]$ and $j \in [k]$, we define the following sets of indices

$$P_i = \{(j-1)n + \phi_j(i) : j \in [k]\} \subseteq [kn], \tag{2}$$

$$Q_i = \{(j-1)n^2 + (\phi_j(i)-1)n + i : j \in [k]\} \subseteq [kn^2], \tag{3}$$

$$S_{ji} = \{h : (j-1)n^2 + (i-1)n + 1 \le h \le (j-1)n^2 + in\} \subseteq [kn^2]. \tag{4}$$

Lemma 3. *Let j be taken over $[k]$ and i, h be taken over $[n]$. Then*

1. *Both $\{Q_i\}$ and $\{S_{ji}\}$ are composed of pairwise disjoint sets;*
2. *$|Q_h \cap S_{ji}| \leq 1$ and it is equal to 1 only if $(j-1)n + i \in P_h$;*
3. *$C[\![(j-1)n+i, S_{ji}]\!] = c_{ji}$ and $C[\![(j-1)n+i, \bar{S}_{ji}]\!] = \mathbf{0}$;*
4. *$C[\![kn+i, Q_i]\!] = \mathbf{1}$ and $C[\![kn+i, \bar{Q}_i]\!] = \mathbf{0}$.*

Lemma 4. *Let $w = \sum_{i=1}^{n} \alpha_i \cdot C[\![kn+i, *]\!] \in V_{\text{sec}}$. Then $N(w) = \cup_{i \in N(\alpha)} Q_i$.*

Proof. By Lemma 3, the support of $C[\![kn+i, *]\!]$ is Q_i for every $i \in [n]$ and all Q_i are pairwise disjoint. Hence, $N(w) = \cup_{i \in N(\alpha)} Q_i$.

Lemma 5. *Let $V_{\text{int}} = V_{\text{que}} \cap V_{\text{sec}}$. If $\dim(V_{\text{int}}) = m$, then there is a subset I of $[n]$ of cardinality m such that V_{int} is equal to the row space of $C[\![kn + I, *]\!]$.*

Proof. For every $w \in V_{\text{int}}$, there exists $\alpha \in \mathbb{F}^n$ such that $w = \sum_{i=1}^{n} \alpha_i \cdot C[\![kn + i, *]\!]$. Let $I_w = N(\alpha)$ and $I = \cup_{w \in V_{\text{int}}} I_w$. Then w is in the row space of $C[\![kn + I, *]\!]$. For every $h \in I$, let $w \in V_{\text{int}}$ be such that $h \in I_w$. Let $w = \sum_{i=1}^{n} \alpha_i \cdot C[\![kn+i, *]\!]$ for some $\alpha \in \mathbb{F}^n$. Due to Lemma 4, $N(\alpha) = I_w$ and the support of w is the disjoint union of the supports of $C[\![kn+i, *]\!]$ (i.e. Q_i), where i is taken over I_w. Due to Lemma 3, Q_i intersects the support of $C[\![(\lambda-1)n+\tau, *]\!]$ only if $(\lambda-1)n+\tau \in P_i$. Since $w \in V_{\text{que}}$, $C[\![kn+i, *]\!]$ must be a linear combination of the $C[\![(\lambda-1)n+\tau, *]\!]$'s, where $(\lambda-1)n+\tau \in P_i$. Hence, $C[\![kn+i, *]\!] \in V_{\text{que}}$. In particular, $C[\![kn+h, *]\!] \in V_{\text{que}}$. It follows that $C[\![kn+h, *]\!] \in V_{\text{int}}$. Hence, V_{int} is equal to the row space of $C[\![kn + I, *]\!]$ and $|I| = \dim(V_{\text{int}}) = m$.

The following lemma shows that a dishonest receiver Bob can obtain more than one secret only with probability $\leq 2^{-k}$, which is negligible.

Lemma 6. *If $k \geq 2$, then $\Pr[2 \leq \dim(V_{\text{int}}) \leq n] \leq 2^{-k}$, where the probability is taken over the random permutations $\phi_1, \ldots, \phi_k \leftarrow \mathbb{S}_n$.*

Proof. Due to Lemma 5, for every $2 \leq m \leq n$, $\dim(V_{\text{int}}) = m$ if and only if there is a subset $I \subseteq [n]$ of cardinality m such that V_{int} is equal to the row space of $C[\![kn + I, *]\!]$. However, V_{int} is equal to the row space of $C[\![kn + I, *]\!]$ only if the support of $C[\![(j-1)n+\phi_j(i), *]\!]$ is equal to $\{(j-1)n^2+(\phi_j(i)-1)n+i\}$ for every $(j, i) \in [k] \times I$. The later event occurs only if Bob can correctly guess $\phi_j(i)$ for every $(j, i) \in [k] \times I$. Since $\phi_1, \ldots, \phi_k$ are totally random, the last event happens with probability at most $\left(\frac{(n-m)!}{n!}\right)^k$. It follows that $\Pr[2 \leq \dim(V_{\text{int}}) \leq n] = \sum_{m=2}^{n} \Pr[\dim(V_{\text{int}}) = m] \leq \sum_{m=2}^{n} \binom{n}{m} \left(\frac{(n-m)!}{n!}\right)^k \leq 2^{-k}$, where the probabilities are taken over the random permutations $\phi_1, \ldots, \phi_k \leftarrow \mathbb{S}_n$.

Let $H = \{t \in [kn] : C[\![t, *]\!] \neq \mathbf{0}\}$ and V_{int} be equal to the row space of $C[\![kn + I, *]\!]$, where $I \subseteq [n]$. The proofs of Lemma 7, 8 and 9 only involve simple linear algebra and omitted.

Lemma 7. *Let $R = H \cap [(k-1)n]$. Then for every $\alpha \in \mathbb{F}^{|R|}$ and $\beta \in \mathbb{F}^n$, $\Pr[Y[\![R]\!] = \alpha | s = \beta] = (1/|\mathbb{F}|)^{|R|}$, where the probability is taken over the random matrices $X_1, \ldots, X_k$ in (1).*

- input: (k, c, z), where $c \in [n]$ is Bob's input and z is an auxiliary input;
- subroutine: the g-hybrid model adversary $\mathcal{H}$ and the trusted third party $\mathcal{T}^f$.

1. choose k random permutations $\phi'_1, \ldots, \phi'_k \leftarrow \mathbb{S}_n$ and set $\phi' = (\phi'_1, \ldots, \phi'_k)$;
2. for every $i \in [n]$, define the following sets of indices
   - $P'_i = \{(j-1)n + \phi'_j(i) : j \in [k]\}$, $Q'_i = \{(j-1)n^2 + (\phi'_j(i)-1)n + i : j \in [k]\}$;
3. initialize a $(kn+n) \times kn^2$ matrix C' s.t. for every $j \in [k]$ and $i \in [n]$
   - $C'[\![(j-1)n + i, *]\!] = \mathbf{0}$, $C'[\![kn + i, Q'_i]\!] = \mathbf{1}$, $C'[\![kn + i, \bar{Q}'_i]\!] = \mathbf{0}$;
4. initialize k all-zero square matrices $X'_1, \ldots, X'_k$ of order n;
5. let $T = [kn] \subseteq [kn + n]$. initialize the following subspaces of the row space of C'
   - $V'_{\text{que}} = \text{span}\{C'[\![T, *]\!]\}$, $V'_{\text{sec}} = \text{span}\{C'[\![\bar{T}, *]\!]\}$, $V'_{\text{int}} = V'_{\text{que}} \cap V'_{\text{sec}}$;
6. initialize *counter* $= 0$. For $(j, i) = (1, 1), \ldots, (1, n), \ldots, (k, n)$,
   - if $(j, i) \neq (1, 1)$, set $\mathbb{C}'_{ji} = \{(c'_{\lambda\tau}, Y'_{\lambda\tau}) : (\lambda, \tau) \in [k] \times [n], \lambda n + \tau < jn + i\}$;
   - if $(j, i) = (1, 1)$, feed $\mathcal{H}$ with (k, c, z) and receive $c'_{ji} = \mathcal{H}_1(k, c, z)$ from $\mathcal{H}$;
   - if $(j, i) \neq (1, 1)$, feed $\mathcal{H}$ with $(k, c, z, \mathbb{C}'_{ji})$ and receive $c'_{ji} = \mathcal{H}_1(k, c, z, \mathbb{C}'_{ji})$;
   - update the $(j-1)n + i$-th row of C' s.t. $C'[\![(j-1)n + i, S_{ji}]\!] = c'_{ji}$;
   - update the vector spaces $V'_{\text{que}}, V'_{\text{sec}}, V'_{\text{int}}$ and check the value of *counter*,
     - if $\dim(V'_{\text{int}}) = 0$ or $\dim(V'_{\text{int}}) = 1$ and *counter* $= 1$
       - choose $x'_{ji} \leftarrow \mathbb{F}^n$, update X'_j s.t. $X'_j[\![i, *]\!] = x'_{ji}$ and set $Y'_{ji} = c'_{ji} \cdot x'_{ji}$;
     - if $\dim(V'_{\text{int}}) \geq 2$, output a failure message and halt;
     - if $\dim(V'_{\text{int}}) = 1$ and *counter* $= 0$
       - find $c' \in [n]$ s.t. $V'_{\text{int}} = \text{span}\{C'[\![kn + c', *]\!]\}$;
       - find $\rho' \in \mathbb{F}^k$ s.t. $C'[\![kn + c', *]\!] = \sum_{j=1}^{k} \rho'_j \cdot C'[\![(j-1)n + \phi'_j(c'), *]\!]$;
       - feed $\mathcal{T}^f$ with c' and receive $s_{c'}$ from $\mathcal{T}^f$;
       - choose $x'_{ki} \leftarrow \mathbb{F}^n$ subject to the following identity: $s_{c'} = \sum_{j=1}^{k-1} \rho'_j \cdot Y'_{j\ \phi'_j(c')} + \rho'_k \cdot C'[\![(k-1)n + \phi'_k(c'), *]\!] \cdot x'_{ki}$
       - update X'_k s.t. $X'_k[\![i, *]\!] = x'_{ki}$ and set $Y'_{ki} = c'_{ki} \cdot x'_{ki}$;
       - *counter* $=$ *counter* $+ 1$.
7. feed $\mathcal{H}$ with $(k, c, z, \mathbb{V}', \phi')$(where $\mathbb{V}' = \{(c'_{ji}, Y'_{ji}) : (j, i) \in [k] \times [n]\}$), output whatever $\mathcal{H}$ outputs , say $\mathcal{H}_2(k, c, z, \mathbb{V}', \phi')$, and then halt.

Fig. 3. Ideal model adversary corrupting Bob for π^g

Lemma 7 shows that, among the first $(k-1)n$ answers Bob receives from $\mathcal{T}^g$, those indexed by R are totally random. On the other hand, it is clear that the remaining ones are 0.

Lemma 8. *For every $i \in I$, there is a vector $\rho \in \mathbb{F}^k$ such that $Y_{(k-1)n+\phi_k(i)} = \rho_k^{-1} \cdot (s_i - \sum_{j=1}^{k-1} \rho_j \cdot Y_{(j-1)n+\phi_j(i)})$.*

Lemma 8 shows that if a secret s_i can be obtained by Bob, then the last answer (i.e., $Y_{(k-1)n+\phi_k(i)}$) regarding to s_i is always uniquely determined by the first $k-1$ answers (i.e., $Y_{(j-1)n+\phi_k(i)}$, where $1 \leq j \leq k-1$) regarding to s_i.

Lemma 9. *Let $i \in \bar{I}$ be such that $C[\![(k-1)n + \phi_k(i), *]\!] \neq \mathbf{0}$. Then for every $\alpha \in \mathbb{F}^{|R_i|}, \beta \in \mathbb{F}^n$ and $\gamma \in \mathbb{F}$, $\Pr[Y_{(k-1)n+\phi_k(i)} = \gamma | Y[\![R_i]\!] = \alpha, s = \beta] = 1/|\mathbb{F}|$, where $R_i = H \cap [(k-1)n + \phi_k(i) - 1]$ and the probability is taken over the random matrices $X_1, \ldots, X_k$ in (1).*

Lemma 9 shows that the receiver Bob learns essentially no information on s_i whenever $i \in \bar{I}$.

Lemma 10. *For any g-hybrid model adversary $\mathcal{H}$ corrupting Bob, there is an ideal model adversary $\mathcal{S}$ corrupting Bob whose running time is polynomial in that of $\mathcal{H}$ such that* $\text{IDEAL}_{f,\mathcal{S}} \approx \text{EXEC}_{\pi^g,\mathcal{H}}$.

Proof. The ideal model adversary $\mathcal{S}$ is depicted by Fig. 3. The proof is deferred to the full version of this paper.

Lemma 10 shows that a malicious receiver Bob cannot learn more information on the secrets of the sender Alice except with a negligible probability (In fact, the probability is $\leq 2^{-k}$ by Lemma 6). Due to Lemma 1, 2 and 10, we have

Theorem 1. *The $\binom{n}{1}$-OT can be statistically securely reduced to kn invocations of the $\mathbb{F}^n$-OLFE_n over a finite field $\mathbb{F}$, where k is the security parameter.*

Let $\mathcal{C} \subseteq \mathbb{F}^n$ contain all unit vectors and $g' = \mathcal{C}\text{-OLFE}_n$. Let $\pi^{g'}$ be obtained by substituting g with g' in Fig. 1. By the proof of Lemma 6, any hybrid model adversary $\mathcal{H}$ corrupting Bob in $\pi^{g'}$ cannot do better than it does in π^g.

Theorem 2. *The $\binom{n}{1}$-OT can be statistically securely reduced to kn invocations of a $\mathcal{C}$-OLFE_n over a finite field $\mathbb{F}$, where k is the security parameter and $\mathcal{C}$ contains all unit vectors of length n*

4 $\mathcal{C}$-OLFE_n and Reversing $\binom{n}{1}$-OT

In this section, we present a $\mathcal{C}$-OLFE_n which can be applied to reverse any $\binom{n}{1}$-OT, where $\mathcal{C} = \{(c_1, \ldots, c_n) : c_1 \oplus \cdots \oplus c_n = 1\} \subseteq \mathbb{F}_2^n$. More precisely, we present a $\mathcal{C}$-OLFE_n from Alice(as a sender) to Bob(as a receiver) by reducing it, in a perfectly secure way, to $n-1$ invocations of a given $\binom{n}{1}$-OT from Bob(as a sender) to Alice (as a receiver). Let g be the $\mathcal{C}$-OLFE_n and h be the $\binom{n}{1}$-OT from Bob to Alice. Fig. 4 is a two-party protocol for g in the h-hybrid model.

The correctness of σ^h is shown by the following lemma.

- input: Alice has n bits $b \in \{0,1\}^n$ and Bob has a choice vector $c \in \mathcal{C}$;
- subroutine: the trusted third party $\mathcal{T}^h$;

1. Bob: choose $r_i \leftarrow \{0,1\}$ and set $a_{ij} = r_i \oplus (j-1) \cdot c_i$ for $2 \leq i \leq n$ and $j \in [n]$;
2. $\mathcal{T}^h$: for $i = 2 \ldots n$, Bob and Alice proceed as follows:
   - Bob: send $(a_{i1}, \cdots, a_{in})$ to $\mathcal{T}^h$;
   - Alice: send $d_i = b_1 \oplus b_i$ to $\mathcal{T}^h$ and receive x_i from $\mathcal{T}^h$;
3. Alice: send $y = b_1 \oplus x_2 \oplus \cdots \oplus x_n$ to $\mathcal{R}$;
4. Bob: output $y \oplus r_2 \oplus \cdots \oplus r_n$.

Fig. 4. A construction of $\mathcal{C}$-OLFE_n out of $\binom{n}{1}$-OT (σ^h)

- input: (k, b, z), where $b \in \{0,1\}^n$ is Alice's input and z is an auxiliary input;
- subroutine: the h-hybrid model adversary $\mathcal{H}$ and the trusted third party $\mathcal{T}^g$.

1. feed $\mathcal{H}$ with (k, b, z);
2. for $i = 2, \ldots, n$ execute
   - receive d'_i from $\mathcal{H}$;
   - choose $x'_i \leftarrow \{0,1\}$ and feed $\mathcal{H}$ with x'_i;
3. receive y' from $\mathcal{H}$;
4. set $b'_1 = y' \oplus x'_2 \oplus \ldots \oplus x'_n$ and $b'_i = b'_1 \oplus d'_i$ for $2 \leq i \leq n$;
5. feed $\mathcal{T}^g$ with $b'_1, \ldots, b'_n$;
6. output whatever $\mathcal{H}$ outputs, say $\mathcal{H}(k, b, z, d', x', y')$, where $d' = (d'_2, \ldots, d'_n)$ and $x' = (x'_2, \ldots, x'_n)$.

Fig. 5. Ideal model adversary corrupting Alice for σ^h

Lemma 11. *If Alice and Bob are honest, then* $\mathrm{IDEAL}_{f,\mathcal{S}} \equiv \mathrm{EXEC}_{\sigma^h,\mathcal{H}}$, *where* $\mathcal{S}$ *is the ideal model adversary corrupting no party and* $\mathcal{H}$ *is the* h*-hybrid model adversary corrupting no party.*

Proof. Given (k, b, c, z), we have $\mathrm{IDEAL}_{f,\mathcal{S}}(k, b, c, z) = \left(\perp, \perp, \bigoplus_{i=1}^n (b_i \cdot c_i)\right) = \left(\perp, \perp, b_1 \cdot (1 \oplus \bigoplus_{i=2}^n c_i) \oplus \bigoplus_{i=2}^n (b_i \cdot c_i)\right) = \left(\perp, \perp, b_1 \oplus \bigoplus_{i=2}^n (b_1 \oplus b_i) \cdot c_i\right) = \left(\perp, \perp, b_1 \oplus \bigoplus_{i=2}^n (r_i \oplus (b_1 \oplus b_i) \cdot c_i) \oplus \bigoplus_{i=2}^n r_i\right) = \left(\perp, \perp, y \oplus \bigoplus_{i=2}^n r_i\right) = \mathrm{EXEC}_{\sigma^h,\mathcal{H}}(k, b, c, z)$ where the random variables only depend on the uniform and independent coin tosses of Bob.

Lemma 12. *For any* h*-hybrid model adversary* $\mathcal{H}$ *corrupting Alice, there is an ideal model adversary* $\mathcal{S}$ *corrupting Alice whose running time is polynomial in that of* $\mathcal{H}$ *such that* $\mathrm{IDEAL}_{f,\mathcal{S}} \equiv \mathrm{EXEC}_{\sigma^h,\mathcal{H}}$.

Proof. The ideal model adversary is depicted by Fig. 5. Given (k, b, c, z), we have that $\mathrm{IDEAL}_{f,\mathcal{S}}(k, b, c, z) = \left(\mathcal{H}(k, b, z, d', x', y'), \perp, b' \cdot c\right) = \left(\mathcal{H}(k, b, z, d', x', y'), \perp, b'_1 \cdot (1 \oplus \bigoplus_{i=2}^n c_i) \oplus \bigoplus_{i=2}^n b'_i \cdot c_i\right) = \left(\mathcal{H}(k, b, z, d', x', y'), \perp, b'_1 \oplus \bigoplus_{i=2}^n (b'_1 \oplus b'_i) \cdot c_i\right) = \left(\mathcal{H}(k, b, z, d', x', y'), \perp, y' \oplus \bigoplus_{i=2}^n x'_i \oplus \bigoplus_{i=2}^n d'_i \cdot c_i\right) \equiv \left(\mathcal{H}(k, b, z, d, x, y), \perp, y \oplus \bigoplus_{i=2}^n x_i \oplus \bigoplus_{i=2}^n d_i \cdot c_i\right) = \left(\mathcal{H}(k, b, z, d, x, y), \perp, y \oplus \bigoplus_{i=2}^n (r_i \oplus d_i \cdot c_i) \oplus \bigoplus_{i=2}^n d_i \cdot c_i\right) = \left(\mathcal{H}(k, b, z, d, x, y), \perp, y \oplus \bigoplus_{i=2}^n r_i\right) = \mathrm{EXEC}_{\sigma^h,\mathcal{H}}(k, b, c, z)$, where $b' = (b'_1, \ldots, b'_n), d = (d_2, \ldots, d_n)$ and $x = (x_2, \ldots, x_n)$.

Lemma 12 shows that a malicious sender learns essentially no information on the choice vector of the receiver.

Lemma 13. *For any* h*-hybrid model adversary* $\mathcal{H}$ *corrupting Bob, there is an ideal model adversary* $\mathcal{S}$ *corrupting Bob whose running time is polynomial in that of* $\mathcal{H}$ *such that* $\mathrm{IDEAL}_{f,\mathcal{S}} \equiv \mathrm{EXEC}_{\sigma^h,\mathcal{H}}$.

Proof. The ideal model adversary is depicted by Fig. 6. Given (k, b, c, z), we have that $\mathrm{IDEAL}_{f,\mathcal{S}}(k, b, c, z) = (\mathcal{H}(k, c, z, a', y'), \perp, \perp)$ and $\mathrm{EXEC}_{\sigma^h,\mathcal{H}}(k, b, c, z)$

- input: (k, c, z), where $c \in \mathcal{C}$ is Bob's input and z is an auxiliary input;
- subroutine: the h-hybrid model adversary $\mathcal{H}$ and the trusted third party $\mathcal{T}^g$.

1. feed $\mathcal{H}$ with (k, c, z) and receive $\{a'_{ij} : 2 \le i \le n \text{ and } j \in [n]\}$ from $\mathcal{H}$;
2. set $c'_i = a'_{i1} \oplus a'_{i2}$ for $2 \le i \le n$ and $c'_1 = 1 \oplus c'_2 \oplus \ldots \oplus c'_n$;
3. feed $\mathcal{T}^g$ with $c' = (c'_1, \ldots, c'_n)$ and receive $\bigoplus_{i=1}^n b_i \cdot c'_i$;
4. feed $\mathcal{H}$ with $y' = \bigoplus_{i=2}^n a'_{i1} \oplus \bigoplus_{i=1}^n b_i \cdot c'_i$ and output whatever $\mathcal{H}$ outputs, say $\mathcal{H}(k, c, z, a', y')$, where $a' = \{a'_{ij} : 2 \le i \le n \text{ and } j \in [n]\}$.

Fig. 6. Ideal model adversary corrupting Bob for σ^h

$= (\mathcal{H}(k, c, z, a, y), \perp, \perp)$, where $a = \{a_{ij} : 2 \le i \le n \text{ and } j \in [n]\}$. It suffices to show that $(a', y') \equiv (a, y)$. In fact, we have $(a', y') = \left(a', \bigoplus_{i=2}^n a'_{i1} \oplus \bigoplus_{i=1}^n b_i \cdot c'_i\right) = \left(a', \bigoplus_{i=2}^n a'_{i1} \oplus (b_1 \cdot c'_1) \oplus \bigoplus_{i=2}^n b_i \cdot (a'_{i1} \oplus a'_{i2})\right) = \left(a', \bigoplus_{i=2}^n a'_{i1} \oplus b_1 \cdot (1 \oplus \bigoplus_{i=2}^n (a'_{i1} \oplus a'_{i2})) \oplus \bigoplus_{i=2}^n b_i \cdot (a'_{i1} \oplus a'_{i2})\right) \equiv \left(a, \bigoplus_{i=2}^n a_{i1} \oplus (b_1 \cdot (1 \oplus \bigoplus_{i=2}^n (a_{i1} \oplus a_{i2}))) \oplus \bigoplus_{i=2}^n b_i \cdot (a_{i1} \oplus a_{i2})\right) = \left(a, b_1 \oplus \bigoplus_{i=2}^n (a_{i1} \oplus (b_1 \oplus b_i) \cdot (a_{i1} \oplus a_{i2}))\right) = (a, y)$.

Lemma 13 shows that a malicious receiver cannot learn more information on the sender's function except one evaluation at his choice vector.

Theorem 3. *The $\mathcal{C}$-OLFE$_n$ over $\mathbb{F}_2$ can be perfectly securely reduced to $n-1$ invocations of the $\binom{n}{1}$-OT, where $\mathcal{C} = \{(c_1, \ldots, c_n) : c_1 \oplus \ldots \oplus c_n = 1\}$.*

The choice space $\mathcal{C}$ in Theorem 3 contains all unit vectors in $\mathbb{F}_2^n$. Therefore, due to Corollary 2, the resulting $\mathcal{C}$-OLFE$_n$ can be transformed to an $\binom{n}{1}$-OT except for a negligible failure probability. By the composition theorem of secure two-party protocols [7], we have that

Theorem 4. *The $\binom{n}{1}$-OT from Alice to Bob can be statistically securely reduced to $kn(n-1)$ invocations of the $\binom{n}{1}$-OT from Bob to Alice, where k is the security parameter.*

Theorem 4 shows that $\binom{n}{1}$-OT can be efficiently reversed to for *any* $n \ge 2$.

5 Conclusion

In this paper, we define a new cryptographic primitive called $\mathcal{C}$-OLFE$_n$ and show that $\binom{n}{1}$-OT can be efficiently reduced to this primitive in a statistically secure way, where $\mathcal{C}$ contains all unit vectors of length n. Using the reduction, we show that the $\binom{n}{1}$-OT from Alice to Bob can be reduced to $kn(n-1)$ invocations of a given $\binom{n}{1}$-OT from Bob to Alice except for a negligible probability $\le 2^{-k}$.

Acknowledgements. The research is supported in part by the Singapore National Research Foundation under Research Grant NRF-CRP2-2007-03.

References

1. Beaver, D.: Precomputing oblivious transfer. In: Coppersmith, D. (ed.) CRYPTO 1995. LNCS, vol. 963, pp. 97–109. Springer, Heidelberg (1995)
2. Bennett, C.H., Brassard, G., Crépeau, C., Skubiszewska, H.: Practical quantum oblivious transfer. In: Feigenbaum, J. (ed.) CRYPTO 1991. LNCS, vol. 576, pp. 351–366. Springer, Heidelberg (1992)
3. Brassard, G., Crépeau, C., Robert, J.M.: Information theoretic reductions among disclosure problems. In: FOCS 1986, pp. 168–173. IEEE, Los Alamitos (1986)
4. Brassard, G., Crépeau, C., Robert, J.M.: All-or-nothing disclosure of secrets. In: Odlyzko, A.M. (ed.) CRYPTO 1986. LNCS, vol. 263, pp. 234–238. Springer, Heidelberg (1987)
5. Brassard, G., Crépeau, C., Wolf, S.: Oblivious transfers and privacy amplification. Journal of Cryptology 16(4), 219–237 (2003)
6. Cachin, C.: On the foundations of oblivious transfer. In: Nyberg, K. (ed.) EUROCRYPT 1998. LNCS, vol. 1403, pp. 361–374. Springer, Heidelberg (1998)
7. Canetti, R.: Security and composition of multiparty cryptographic protocols. Journal of Cryptology 13(1), 143–202 (2000)
8. Crépeau, C.: Equivalence between two flavors of oblivious transfers. In: Pomerance, C. (ed.) CRYPTO 1987. LNCS, vol. 293, pp. 350–354. Springer, Heidelberg (1988)
9. Crépeau, C., Sántha, M.: On the reversibility of oblivious transfer. In: Davies, D.W. (ed.) EUROCRYPT 1991. LNCS, vol. 547, pp. 106–113. Springer, Heidelberg (1991)
10. Even, S., Goldreich, O., Lempel, A.: A randomized protocol for signing contracts. Communications of the ACM 28(6), 637–647 (1985)
11. Goldreich, O., Micali, S., Wigderson, A.: How to play any mental game or a completeness theorem for protocols with honest majority. In: STOC 1987, pp. 218–229. ACM, New York (1987)
12. Kilian, J.: Founding cryptography on oblivious transfer. In: STOC 1988, pp. 20–31. ACM, New York (1988)
13. Naor, M., Pinkas, B.: Oblivious transfer and polynomial evaluation. In: STOC 1999, pp. 245–354. ACM, New York (1999)
14. Rabin, M.O.: How to exchange secrets by oblivious transfer. Technical Report TR-81, Aiken Computation Laboratory, Harvard University (1981)
15. Yao, A.C.C.: How to generate and exchange secrets. In: FOCS 1986, pp. 162–167. IEEE, Los Alamitos (1986)