Generalized Oblivious Transfer by Secret Sharing

Tamir Tassa *

Abstract

The notion of Generalized Oblivious Transfer (GOT) was introduced by Ishai and Kushilevitz in [12]. In a GOT protocol, Alice holds a set U of messages. A decreasing monotone collection of subsets of U defines the retrieval restrictions. Bob is allowed to learn any permissable subset of messages from that collection, but nothing else, while Alice must remain oblivious regarding the selection that Bob made. We propose a simple and efficient GOT protocol that employs secret sharing. We compare it to another secret sharing based solution for that problem that was recently proposed in [18]. In particular, we show that the access structures that are realized by the two solutions are related through a duality-type relation that we introduce here. We show that there are examples which favor our solution over the second one, while in other examples the contrary holds. Two applications of GOT are considered — priced oblivious transfer, and oblivious evaluation of multivariate polynomials.

Keywords. Oblivious transfer, Generalized oblivious transfer, Multiparty computation, Secret sharing, Access structures.

*Department of Mathematics and Computer Science, The Open University, Ra'anana, Israel. Telephone: +972-52-3646540. Email: `tamirta@openu.ac.il`

1 Introduction

Oblivious transfer (OT) is one of the fundamental building blocks for secure multiparty computation [20]. It was first introduced by Rabin [17]. A closely related variant, called "1-out-of-2 OT", was later introduced and discussed by Even, Goldreich and Lempel [8]. In their setting, Alice (the sender) has two bits, b_0 and b_1, and Bob (the receiver) has a selection bit s. The goal is for Bob to receive b_s and remain oblivious of b_{1-s} while Alice remains oblivious of s. The importance of OT was established in [11, 13] where it was shown that OT is necessary and sufficient for general multiparty computation. In the following two decades, many constructions of special-purpose multiparty computation protocols that are based on OT were introduced, e.g. [5, 9, 15].

Brassard, Crépeau and Robert [4] extended the basic notion of 1-out-of-2 OT to 1-out-of-n OT. Namely, the sender has n messages, and the receiver is allowed to learn exactly one of them, while the sender is required to remain oblivious regarding the receiver's selection. They gave information-theoretic reductions to construct 1-out-of-n OT protocols from $n-1$ invocations of a 1-out-of-2 OT protocol. More efficient implementations were later proposed by Naor and Pinkas [16].

The next step in extending the notion of OT was k-out-of-n OT. In such protocols, Alice holds a set of n messages; she is willing to allow Bob to learn any k messages from U, but she refuses to allow Bob to learn any information regarding the remaining $n-k$ messages. Bob, on the other hand, demands that Alice remains oblivious regarding his selection of k messages. Constructions for k-out-of-n OT were presented in [14] and [16]. The basic tools in the constructions in [14] are symmetric and asymmetric encryptions; they apply for all values of $0 < k < n$. The constructions in [16], on the other hand, use 1-out-of-2 OT, string OT [5] and pseudorandom functions; they work for $k \leq n^{\frac{1}{4}-\varepsilon}$, where $\varepsilon > 0$.

The final extension of OT, called *generalized oblivious transfer* (GOT), was introduced by Ishai and Kushilevitz in [12]. In a GOT protocol, Alice holds a set of n messages, $U = \{M_1, \ldots, M_n\}$. A decreasing monotone collection of subsets of U, $\mathcal{A} \subseteq 2^U$, defines the retrieval restrictions. The decreasing monotonicity means that if $B \in \mathcal{A}$ and $B' \subset B$ then also $B' \in \mathcal{A}$. Bob is allowed to retrieve any subset of messages $B \subset U$ provided that $B \in \mathcal{A}$. As before, Bob cannot learn any information on the complement set of messages, $U \setminus B$, while Alice must not learn any information on the subset B that Bob selected. The solution proposed in [12] uses parallel invocations of 1-out-of-2 OT.

Our contributions. In this study we propose a simple and efficient GOT protocol; the protocol invokes a k-out-of-n OT and a secret sharing scheme for a certain access structure that is induced by the GOT access structure $\mathcal{A}$.

Another GOT protocol that is based on secret sharing was recently proposed in [18]. That protocol too invokes a simpler notion of OT (1-out-of-2 OT) and a secret sharing scheme, but for a different access structure which is induced by $\mathcal{A}$. Specifically, while our protocol invokes a secret sharing scheme that realizes an access structure on U that is induced by the maximal sets in $\mathcal{A}$, the protocol in [18] invokes a secret sharing scheme that realizes an access structure on U that consists of the complements of the subsets in $\mathcal{A}$. We show that those two access structures are related through a duality-type relation, that we introduce and characterize herein. In particular, the two access structures may have different information rates. Moreover, we show here an example where the access structure that is invoked by our GOT protocol has a simple and ideal linear secret sharing scheme, while the related access structure which is invoked by the other GOT protocol does not seem to have a practical (even non-ideal) secret sharing scheme that realizes it.

Hence, depending on the collection $\mathcal{A}$, Alice and Bob may select the GOT protocol that relies on the access structure which admits a more efficient secret sharing scheme.

Organization of the paper. The paper is organized as follows. In Section 2 we describe our protocol. Then, in Section 3, we describe the protocol that was proposed in [18]. In Section 4 we discuss the underlying access structures in the two protocols and their relation. Here we define the novel duality-type notion of the *complemented access structure*, discuss its properties and characterize it. Finally, we describe in Section 5 two applications of GOT, and illustrate the above described differences in the information rate and complexities between the secret sharing access structures in the two GOT protocols.

2 A GOT protocol based on secret sharing

Let $\mathcal{A}$ be the monotone decreasing collection of subsets of U that Alice allows Bob to retrieve. Let $\mathcal{A}^0$ be the basis of $\mathcal{A}$, namely, the collection of all maximal subsets in $\mathcal{A}$,

$$\mathcal{A}^0 = \{B \in \mathcal{A} : B \subset C \Rightarrow C \notin \mathcal{A}\} .$$

Clearly, for any $B, C \in \mathcal{A}^0$, neither $B \subset C$, nor $C \subset B$. Hence, we may consider the monotone increasing closure of $\mathcal{A}^0$,

$$\Gamma = \{C \subseteq U : \exists B \in \mathcal{A}^0, B \subseteq C\} .$$

In other words, Γ is the access structure on U whose basis is $\mathcal{A}^0$. Our protocol will rely on a secret sharing scheme that realizes that access structure.

Hereinafter we let $\mathbb{F}$ be a large finite field of cardinality greater than $n = |U|$. We assume that U is embedded in $\mathbb{F}$, in the sense that every message $M_i \in U$ is a field element.

The case of uniform bases. We begin by considering the case where the basis $\mathcal{A}^0$ is uniform, in the sense that all sets in it have the same size, which we denote by k. In that case, the protocol proceeds as follows. Let Σ be a secret sharing scheme realizing Γ, let $s \in \mathbb{F}$ be a secret random value selected by Alice, and let s_i be the corresponding share of M_i. Then Alice and Bob engage in a k-out-of-n OT for the following set of pairs of values:

$$W := \{\langle M_i + x_i, s_i \rangle : 1 \leq i \leq n\} ;$$

here, $x_i \in \mathbb{F}$, $1 \leq i \leq n$, are random and independent field elements selected by Alice.

If Bob wishes to learn the values in the subset $B = \{M_{i_1}, \ldots, M_{i_k}\} \in \mathcal{A}^0$, he will chose to learn the corresponding k pairs of values in W, i.e.,

$$\langle M_{i_j} + x_{i_j}, s_{i_j} \rangle , \quad 1 \leq j \leq k .$$

As B is a permissable subset, Bob may then recover the secret s from the shares $s_{i_1}, \ldots, s_{i_k}$. Once he does, he will send the value s to Alice. Alice verifies the correctness of the value that Bob sent to her; if it is the correct value, she will send to him the complete set of random shifts, $\{x_1, \ldots, x_n\}$. Finally, Bob will use the values $x_{i_1}, \ldots, x_{i_k}$ in order to recover the sought-after messages in $B = \{M_{i_1}, \ldots, M_{i_k}\}$.

The general case. In the general case, $\mathcal{A}^0$ may have subsets of different sizes. Hence, there exists $k > 0$ and $d \geq 0$ for which

$$\min\{|B| : B \in \mathcal{A}^0\} = k - d , \quad \max\{|B| : B \in \mathcal{A}^0\} = k . \tag{1}$$

In that case, Alice augments the original set of messages, U, with d messages that are selected randomly and independently from $\mathbb{F}$,

$$U' := U \cup \{M_{n+1}, \ldots, M_{n+d}\} . \tag{2}$$

Next, we define a new monotone increasing access structure on U'. To that end, we let

$$\mathcal{A}_j = \{B \in \mathcal{A}^0 : |B| = k - j\} , \quad 0 \leq j \leq d , \tag{3}$$

and then set

$$\mathcal{A}' = \bigcup_{j=0}^{d} \{B \cup \{M_{n+1}, \ldots, M_{n+j}\} : B \in \mathcal{A}_j\} . \tag{4}$$

In other words, we turn the original, possibly non-uniform basis $\mathcal{A}^0$ to a uniform one, $\mathcal{A}'$, by augmenting every set in $\mathcal{A}^0$ with the required number of dummy messages so that its size becomes k. (Note that $\mathcal{A}'$ is a legal basis since it does not include two sets where one is a subset of the other.) Finally, Γ' is the access structure on U' that is induced by the basis $\mathcal{A}'$, i.e.,

$$\Gamma' = \{C \subseteq U' : \exists B \in \mathcal{A}', B \subseteq C\} . \tag{5}$$

Now, since all minimal subsets in Γ' are of the same size k, we may apply the previous protocol.

We proceed to prove that the protocol is correct (in the sense that it realizes its desired functionality) and secure (in the sense that it respects both Alice's and Bob's privacy).

Theorem 2.1. *Let $U = \{M_1, \dots, M_n\} \subset \mathbb{F}$ be a set of n messages and let $\mathcal{A}$ be a monotone decreasing collection of subsets of U. Let Γ' be a monotone increasing access structure on U', where U' and Γ' are defined in Eqs. (1)–(5). Then, assuming that the k-out-of-n OT protocol used by Alice and Bob is correct and secure, and assuming that Σ is a perfect secret sharing scheme realizing Γ', the above protocol is correct and secure.*

Proof. Assume that Bob wishes to learn the values of the messages in some permissable set $B \in \mathcal{A}^0$. Let $j = k - |B|$. Then Bob will select to learn the k pairs from W that correspond to the k messages in $B \cup \{M_{n+1}, \dots, M_{n+j}\}$. Since the shares s_i in the pairs that Bob retrieves correspond to an authorized set in Γ', he will be able to recover the secret s and, consequently, retrieve from Alice the random shifts that mask the value of the messages in $B \cup \{M_{n+1}, \dots, M_{n+j}\}$.

Next, we show that the above protocol respects Alice's privacy. Under our assumption regarding the OT protocol, Bob can learn the values of no more than k messages from W. If the k pairs of values that Bob selected do not correspond to k messages of the form $B \cup \{M_{n+1}, \dots, M_{n+j}\}$, for some $0 \le j \le d$ and $B \in \mathcal{A}_j$, then the shares delivered in those pairs do not correspond to an authorized set of Γ'. Hence, as Σ is perfect, Bob will not learn any information regarding the value of s. Consequently, Bob can only guess the value of s in order to convince Alice into sending him the values of the shifts x_i. Bob may succeed in doing so in probability $1/|\mathbb{F}|$.

Finally, Bob's privacy is respected under the assumption that the OT protocol respects his privacy; namely, Alice remains oblivious regarding the selection that Bob made. $\square$

3 A different GOT protocol

Given a collection $\mathcal{A} \subseteq 2^U$, we define the collection $\mathcal{A}^c$ as follows,

$$\mathcal{A}^c = \{U \setminus B : B \in \mathcal{A}\} . \tag{6}$$

As $\mathcal{A}$ is monotone decreasing, $\mathcal{A}^c$ is monotone increasing, whence it is a monotone access structure. The protocol of [18] implements a secret sharing scheme for $\mathcal{A}^c$. The protocol proceeds as follows:

1. Alice selects n random field elements $x_1, \dots, x_n \in \mathbb{F}$ and computes $y_i = M_i + x_i$, $1 \le i \le n$.

2. Alice chooses a random secret $s \in \mathbb{F}$ and creates n shares, s_i, $1 \leq i \leq n$, according to the access structure $\mathcal{A}^c$.
3. Alice and Bob engage in n invocations of 1-out-of-2 OT, where in the ith invocation Bob selects one of the two messages y_i or s_i.
4. Let $B \in \mathcal{A}$ be a set of messages that Bob wishes to receive. Then if $M_i \in B$ Bob will retrieve y_i, otherwise he will retrieve s_i.
5. Bob will recover s from the shares $\{s_i : M_i \in U \setminus B\}$ and will send it to Alice.
6. Alice verifies that the value received from Bob is the correct secret s. If it is, she will send to him the n random shifts $x_1, \ldots, x_n$.
7. Bob will use the values $\{x_i : M_i \in B\}$ to recover M_i from y_i for all $M_i \in B$.

It is easy to see that if the 1-out-of-2 OT protocol is correct and secure, and if Alice uses a perfect secret sharing scheme to realize $\mathcal{A}^c$, the above protocol is correct and secure.

4 Comparing the underlying access structures in the two protocols

Here we identify the relation between the access structure that is realized in our protocol and the one that is realized in the second protocol. We concentrate on the case where all sets in $\mathcal{A}^0$ are of the same size, in order not to obfuscate the discussion with the messages with which we augment U in our protocol in case where not all the sets in $\mathcal{A}^0$ are of the same size.

We begin with some definitions. Let U be a finite set and $\Gamma \subseteq 2^U$ be a monotone increasing access structure on U. Such an access structure induces the following collections in 2^U:

- The *dual access structure* is $\Gamma^* = \{U \setminus B : B \notin \Gamma\}$.
- The *basis* Γ_0 of Γ is the collection of all minimal sets in Γ.
- The *complemented basis* is defined as
$$\Gamma_0^c = \{U \setminus B : B \in \Gamma_0\} \, .$$
- The *complemented access structure*, Γ^c, is defined as the monotone increasing closure of Γ_0^c.

We refer to Γ_0^c as *the complemented basis* and not as the complement basis in order to distinguish it from the collection $2^U \setminus \Gamma_0$. It is easy to see that Γ_0^c is also a basis of an access structure since if $B, C \in \Gamma_0^c$ then neither $B \subset C$ nor $C \subset B$. Hence, we may speak of the complemented access structure that is induced by it,

$$\Gamma^c = \{B \subseteq U : \exists C \in \Gamma_0^c \text{ such that } C \subseteq B\} \, . \qquad (7)$$

Example 1. Let Γ be the k-threshold access structure on U, i.e. $\Gamma = \{B \subset U : |B| \geq k\}$, and assume that $|U| = n$. Then in this case:

- The dual access structure is $\Gamma^* = \{B \subseteq U : |B| \geq n - k + 1\}$;
- The basis is $\Gamma_0 = \{B \subset U : |B| = k\}$;
- The complemented basis is $\Gamma_0^c = \{B \subset U : |B| = n - k\}$;
- The complemented access structure is $\Gamma^c = \{B \subseteq U : |B| \geq n - k\}$.

Example 2. Let $U = \{1, 2, 3, 4\}$[1] and Γ be the access structure that consists of all subsets of size at least 2 that include participant 4. (This is an example of a hierarchical threshold access structure [19].) Here:

- $\Gamma^* = \{4, 14, 24, 34, 123, 124, 134, 234, 1234\}$;
- $\Gamma_0 = \{14, 24, 34\}$;
- $\Gamma_0^c = \{12, 13, 23\}$;
- $\Gamma^c = \{12, 13, 23, 123, 124, 134, 234, 1234\}$.

The action of duality is an involution, namely, $(\Gamma^*)^* = \Gamma$. It is easy to see that so is the action of complementing an access structure.

Lemma 4.1. *For any monotone access structure Γ on U, it holds that $(\Gamma^c)^c = \Gamma$.*

Proposition 4.2. *Let Γ be the access structure that is realized in the first protocol and Δ be the access structure that is realized in the second protocol. Then $\Delta = \Gamma^c$.*

Proof. Both access structures are defined through the decreasing monotone collection $\mathcal{A}$. While Γ is the monotone closure of the collection $\mathcal{A}^0$ of all maximal sets in $\mathcal{A}$, the second access structure, Δ, is defined through (6), namely,

$$\Delta = \{U \setminus B : B \in \mathcal{A}\} . \tag{8}$$

By (8), a minimal set in Δ is a complement of a maximal set in $\mathcal{A}$. Hence, the basis of Δ consists of the complements of all sets in $\mathcal{A}^0$. But as $\mathcal{A}^0$ is the basis of Γ, we infer that $\Delta = \Gamma^c$. $\Box$

Next, we characterize the structure of the complemented access structure and its relation to the dual access structure. To that end, we define circuit-free access structures.

Definition 4.3. *An access structure Γ is called circuit-free if for all unauthorized sets $B \notin \Gamma$ there exists a minimal authorized set $A \in \Gamma_0$ such that $B \subset A$.*

[1]Hereinafter we adopt a shorthanded style where the participants in U are denoted by digits, e.g. 1, 2, 3, and subsets are denoted by the corresponding number, e.g. 12, 234.

The terminology *circuit-free* is borrowed from the matroidal representation of ideal access structures. If an access structure is ideal, then there is a matroid that reflects its structure. On the other hand, every matroid that is representable over some finite field is the reflection of some ideal access structure. An ideal access structure is circuit-free if and only if the matroid reflection of any unauthorized set does not include circuits.

Example 3. A threshold access structure is circuit-free since any unauthorized set is of size which is smaller than the threshold and, hence, it may be expanded to a set of size that equals the threshold, which is a minimal authorized set.

Example 4. Assume that U is composed of two disjoint subsets, $U = U_1 \bigcup U_2$, where U_1 consists of all executives in the organization U. Let Γ be the access structure consisting of all $B \subset U$ in which there are at least t_1 executives, or t_2 participants in total (where $t_2 > t_1$). In this case, Γ_0 consists of all sets of exactly t_1 executives and all sets of exactly t_2 participants which do not include t_1 executives. It is easy to see that Γ is circuit-free since any unauthorized set may be extended to a minimal authorized set of the first kind, if it includes only executives, or to a minimal authorized set of the second kind otherwise.

Example 5. Assume the same structure of U as in Example 4, but this time Γ consists of all $B \subset U$ in which there are at least t_1 executives *and* t_2 participants in total (i.e., the authorized sets are characterized this time by the *conjunction* of the two threshold conditions, and not by their *disjunction* as in the previous example). Here, the minimal sets include exactly t_2 participants, of whom at least t_1 are executives. Hence, any subset that consists only of non-executives and is of size that is greater than $t_2 - t_1$ cannot be embedded in a minimal authorized subset.

We note that Examples 4 and 5 are of hierarchical access structures, that were characterized and studied in [19]. Using the terminology in [19], Example 4 is of a disjunctive hierarchical access structure (with two levels) while Example 5 is of the conjunctive type. All disjunctive hierarchical access structures are circuit-free, while all conjunctive hierarchical access structures are not circuit-free.

We are now ready to characterize the structure of the complemented access structure and its relation to the dual access structure.

Theorem 4.4. *The complemented access structure may be decomposed into the following disjoint union,* $\Gamma^c = \Gamma_1 \cup \Gamma_0^c$*, where* $\Gamma_1 \subseteq \Gamma^*$*. In addition,* $\Gamma_1 = \Gamma^*$ *if and only if* Γ *is circuit-free. Finally,* $\Gamma_0^c \bigcap \Gamma^* = \emptyset$*.*

Proof. Equality (7) that defines Γ^c implies that $\Gamma^c = \Gamma_1 \cup \Gamma_2$, where

$$\Gamma_1 = \{B \subseteq U : \exists C \in \Gamma_0^c \text{ such that } C \subsetneq B\},$$

and

$$\Gamma_2 = \{B \subseteq U : \exists C \in \Gamma_0^c \text{ such that } C = B\}.$$

The two collections Γ_1 and Γ_2 are disjoint since Γ_0^c is a basis (and, hence, it cannot contain two subsets in which one is a proper subset of the other). As Γ_2 clearly equals Γ_0^c, it is left to show that $\Gamma_1 \subseteq \Gamma^*$ in order to establish the first assertion of the theorem. Assume that $B \in \Gamma_1$. Then B is a proper superset of $U \setminus C$ for some $C \in \Gamma_0$. But then $U \setminus B$ is a proper subset of C. Since C is a minimal set in Γ then $U \setminus B \notin \Gamma$. Therefore, $B \in \Gamma^*$.

Next, we prove that $\Gamma_1 = \Gamma^*$ if and only if Γ is circuit-free. To that end, we shall show that if $\Gamma_1 \subsetneq \Gamma^*$ then Γ is not circuit-free. (The proof in the other direction is essentially the same and hence we omit it.) Assume that B is a set in Γ^* which is not in Γ_1. So, as $B \in \Gamma^*$, we infer that $U \setminus B \notin \Gamma$. On the other hand, as $B \notin \Gamma_1$, then B is not a proper superset of any set in Γ_0^c. In other words, $U \setminus B$ is not a proper subset of any set in Γ_0. Hence, $U \setminus B$ is an unauthorized set which is not a subset of any set in the basis of Γ. That means that Γ is not circuit-free.

Finally, we prove the third and last assertion of the theorem. On one hand, if $B \in \Gamma_0^c$ then $U \setminus B \in \Gamma_0 \subseteq \Gamma$. On the other hand, if $B \in \Gamma^*$ then $U \setminus B \notin \Gamma$. Hence, the intersection of Γ_0^c and Γ^* is empty. $\Box$

Examples 1 and 2 exemplify Theorem 4.4. The access structure in Example 1 is circuit-free and there $\Gamma^c = \Gamma^* \cup \Gamma_0^c$, while the one in Example 2 is not, and there $\Gamma^c = \Gamma_1 \cup \Gamma_0^c$ where $\Gamma_1 \subsetneq \Gamma^*$.

To summarize, we have shown that the relation between the two access structures that are realized by the two protocols, ours (Section 2), and the one that was proposed in [18] (Section 3), is that one is the complemented access structure of the other (Lemma 4.1 and Proposition 4.2). However, while the information rate of Γ^* always equals that of Γ (see [7]), it is not true for Γ^c and Γ, as we show in Example 6 below. Hence, it is possible that one of the two GOT protocols is relying on an access structure that has a better information rate than the other protocol and then it might be better suited for implementing the required GOT functionality.

Example 6. Let $U = \{1, 2, 3, 4\}$ and Γ be the access structure with the basis $\Gamma_0 = \{123, 14, 24, 34\}$. That access structure may be viewed as a weighted threshold access structure; indeed, if we associate with each of the first three players the weight 1, with the fourth player the weight 2, and take the threshold to be 3, then the above basis lists all minimal authorized subsets. As shown in [2, Example 4.9], that access structure is not ideal.

The complemented basis is $\Gamma_0^c = \{4, 23, 13, 12\}$. The corresponding access structure Γ^c is the monotone closure of that basis. That access structure may be viewed as either a weighted threshold access structure with the same weights as before, but with a threshold of 2 (rather than 3). The characterization in [2] shows that it is ideal. (It may also be viewed as a multilevel access structure or a hierarchical access structure with two levels, in which case its ideality follows from [6, 19].) Hence, Γ and Γ^c in this example do not have the same information rate.

5 Applications

Here we describe two applications of GOT. In one of those applications there are scenarios in which the secret sharing access structure in our protocol is ideal, while the one in the second protocol is not; and vice-a-versa, there are other scenarios in which the access structure in the second protocol is ideal while the one in our protocol is not. In the second application, the secret sharing access structure in our GOT protocol is always ideal, and realizable by a simple linear secret sharing scheme, while the one in the second protocol does not seem to have a practical (even non-ideal) secret sharing scheme that realizes it.

5.1 Priced OT

Aiello, Ishai and Reingold [1] presented a special case of GOT, which they called Priced OT. Assume that every message M_i in U has an associated cost c_i. If Bob has prepaid Alice an amount of T then he is entitled to retrieve any subset of messages whose total cost does not exceed T. Namely, in this case, the collection $\mathcal{A}$ is as follows:

$$\mathcal{A} = \{B \subseteq U : c(B) := \sum_{M_i \in B} c_i \leq T\} .$$

Let us consider the two access structures that should be realized by a secret sharing scheme in the two protocols. In the first protocol, the access structure Γ is the one that is induced by the basis $\mathcal{A}^0$ of maximal sets in $\mathcal{A}$. In the second protocol, on the other hand, it is the access structure

$$\mathcal{A}^c = \{B \subseteq U : c(U \setminus B) \leq T\} = \{B \subseteq U : c(B) \geq c(U) - T\} .$$

Hence, $\mathcal{A}^c$ is a weighted threshold access structure.

We proceed to show that there are cases in which Γ is ideal while $\mathcal{A}^c$ is not, and vice-a-versa.

Example 7. Let $U = \{1, 2, 3, 4\}$ and assume that the costs are $1, 1, 1, 2$ while the threshold is $T = 3$. The maximal permissable sets are $\mathcal{A}^0 = \{123, 14, 24, 34\}$. Since $\mathcal{A}^0$ includes sets of different sizes (two and three), we add to U an additional message and look at the set $U' = \{1, 2, 3, 4, 5\}$. The collection of maximal permissable sets now is $\mathcal{A}' = \{123, 145, 245, 345\}$ and then the access structure Γ' is the monotone closure of $\mathcal{A}'$. As implied by [10, Theorem 16], that access structure has an information rate of $2/3$, whence it is not ideal.

On the other hand, $\mathcal{A}^c$ in that case is the weighted threshold access structure on U with the same weights but with a threshold $c(U) - T = 5 - 3 = 2$. As explained in Example 6 above, $\mathcal{A}^c$ is ideal.

Hence, in this example, the second GOT protocol relies on an ideal access structure while the first one does not.

Example 8. Let $U = \{1, 2, 3, 4\}$ and assume that the costs are $1, 1, 1, 2$ while the threshold is $T = 2$. The maximal permissable sets are $\mathcal{A}^0 = \{12, 13, 23, 4\}$. Since $\mathcal{A}^0$ includes sets of different sizes (one and two), we add to U an additional message and look at the set $U' = \{1, 2, 3, 4, 5\}$. The collection of maximal permissable sets now is $\mathcal{A}' = \{12, 13, 23, 45\}$ and then the access structure Γ' is the monotone closure of $\mathcal{A}'$. As can be seen easily, Γ' is ideal as it is the union of a 2-out-of-3 threshold access structure on $\{1, 2, 3\}$ and a 2-out-of-2 threshold access structure on $\{4, 5\}$.

On the other hand, $\mathcal{A}^c$ in that case is the weighted threshold access structure on U with the same weights but with a threshold $c(U) - T = 5 - 2 = 3$. As explained in Example 6, $\mathcal{A}^c$ is not ideal.

Hence, in this example, the first GOT protocol relies on an ideal access structure while the second one does not.

5.2 Oblivious multivariate polynomial evaluation

Ben-Ya'akov [3] dealt with oblivious evaluation of multivariate polynomials. In such protocols, Alice holds an r-variate polynomial $P(\cdot)$ over a finite field $\mathbb{F}$, while Bob holds a point $\mathbf{y} \in \mathbb{F}^r$. The goal is to allow Bob to evaluate $P(\mathbf{y})$ without revealing to him any further information about the polynomial P, while Alice has to remain oblivious regarding the value of $\mathbf{y}$. (Oblivious polynomial evaluation was introduced, in the univariate case, by Naor and Pinkas in [15].)

A basic tool in evaluating polynomials is interpolation. An interpolation of a polynomial is the process of recovering all of the polynomial coefficients from a sufficient number of point values. A univariate polynomial of degree d has $d + 1$ undetermined coefficients; any selection of $d + 1$ point values enables to recover the polynomial coefficients through the solution of a system of linear equations. When dealing with an r-variate polynomial of degree d, the number of coefficients is $\binom{d+r}{r}$. Hence, in order to recover the polynomial it is necessary to know its values at $\binom{d+r}{r}$ points in $\mathbb{F}^r$. However, not all $\binom{d+r}{r}$ point values give rise to a uniquely solvable system of linear equations. Selections of $\binom{d+r}{r}$ points in $\mathbb{F}^r$ that give rise to an invertible interpolation matrix are called "proper interpolation points" while other selections are called "improper".

In the protocols presented in [3], Alice and Bob define together another r-variate polynomial, $R(\cdot)$, with the property that $R(\mathbf{0}) = R(0, \ldots, 0) = P(\mathbf{y})$. (The polynomial R is a composition of a polynomial that only Alice knows, which depends on her secret polynomial P, and polynomials that only Bob knows, which depend on his secret point $\mathbf{y}$). Bob's goal is then to recover the polynomial R by means of interpolation. Letting d_R denote the degree of R, Bob needs to learn $k = \binom{d_R+r}{r}$ point values of R. He selects such k points and hides them among $n-k$ other dummy points, where $n > k$ is some security parameter. He then sends all of the n points to Alice, who proceeds to evaluate R at those points. Finally, Bob engages in a k-out-of-n OT vis-a-vis Alice, in which he chooses to learn the value of R at the required k points. Alice must not know which are the points at which Bob selected to learn the value of R since that selection will reveal to her the value of Bob's $\mathbf{y}$. Bob, on the other hand, must not learn more than k values of R since then he might deduce more information on P than what Alice allows him to.

However, as shown in [3], the usage of a basic k-out-of-n OT in this case is problematic. A malicious Bob could try to get the values of R at k points which are not proper interpolation points; it turns out that such selections may allow Bob to learn information of P which he is not supposed to. Hence, Alice wishes to guarantee that Bob selects only k points which are proper interpolation points. That gives rise to a GOT, rather than a simple k-out-of-n OT (which suffices in the case of univariate polynomials since then all k interpolation points are proper).

The messages in the GOT are the point values of R, namely $M_i = R(\mathbf{x}_i)$, where $\mathbf{x}_i$ are the n points in $\mathbb{F}^r$ that Bob generated. Since R is an r-variate polynomial of degree d_R it has the form $R(\mathbf{x}) = \mathbf{X} \cdot \mathbf{a}$ where $\mathbf{a} = (a_0, \ldots, a_{k-1})$ is the vector of $k = \binom{d_R+r}{r}$ coefficients, and $\mathbf{X}$ is the vector of length k that holds all monomials in $\mathbf{x} = (x_1, \ldots, x_r)$ of degree less than or equal to d_R. For example, if $r = 2$ and $d_R = 2$ then $k = \binom{2+2}{2} = 6$ and then $\mathbf{x} = (x_1, x_2)$ and $\mathbf{X} = (1, x_1, x_2, x_1^2, x_1x_2, x_2^2)$. Hereinafter, we refer to $\mathbf{X}$ as the monomial vector of $\mathbf{x}$.

A set of k points $\mathbf{x}_1, \ldots, \mathbf{x}_k \in \mathbb{F}^r$ is proper if and only if the corresponding set of k monomial vectors $\mathbf{X}_1, \ldots, \mathbf{X}_k$ are independent in $\mathbb{F}^k$. Hence, the GOT in this case should restrict Bob to retrieve subsets of $U = \{M_i = R(\mathbf{x}_i)\}_{1 \le i \le n}$ for which the corresponding monomial vectors are independent.

The secret sharing access structure Γ that is used by our protocol consists of all subsets of U for which the corresponding monomial vectors span the space $\mathbb{F}^k$. That access structure is obviously ideal and realizable by the following linear secret sharing scheme. Alice selects a public target nonzero vector $\mathbf{t} \in \mathbb{F}^k$, a random secret $s \in \mathbb{F}$, and a random secret vector $\mathbf{z} \in \mathbb{F}^k$ for which $\mathbf{t} \cdot \mathbf{z} = s$. Then the share of message M_i is $\mathbf{X}_i \cdot \mathbf{z}$. Every set in Γ can recover the secret s since the corresponding monomial vectors span the space $\mathbb{F}^k$, whence they span the target vector $\mathbf{t}$. For sets which are not in Γ, the corresponding monomial vectors span a subspace of dimension $k - 1$ at the most. Hence, the shares of such a set do not reveal any information on s, unless the target vector happens to be in that subspace. The idea is that Alice selects the target vector only after Bob sent to her the points $\mathbf{x}_i$. Hence, she may test the corresponding monomial vectors and choose a target vector

t that is not spanned by the monomial vectors of any unauthorized subset.

On the other hand, the access structure $\mathcal{A}^c$ that is used in this case by the second protocol consists of all subsets of messages for which the *complement* set has independent monomial vectors. Namely, the status of any subset in such an access structure is determined by the monomial vectors which that subset does *not* possess. We were not able to devise a practical general construction of a secret sharing scheme for such access structures. Hence, while in this case our protocol has an efficient implementation, based on a simple and ideal linear secret sharing scheme, the second protocol does not seem to have a practical implementation.

Acknowledgement. The author thanks Benny Pinkas and Amos Beimel for fruitful discussions.

References

[1] B. Aiello, Y. Ishai and O. Reingold, *Priced oblivious transfer: how to sell digital goods*, Proc. of Eurocrypt01, LNCS 2045, 2001, , pp. 119-135.

[2] A. Beimel, T. Tassa and E. Weinreb, *Characterizing ideal weighted threshold secret sharing*, SIAM Journal of Discrete Mathematics, 22, 2008, pp. 360–397. A preliminary version appeared in The Proc. of TCC, 2005, pp. 600–619.

[3] Y. Ben-Ya'akov, *Oblivious evaluation of multivariate polynomials and applications*, M.Sc. Thesis, The Open University of Israel, 2007.

[4] G. Brassard, C. Crépeau and J.M. Robert, *All-or-nothing disclosure of secrets*, Advances in Cryptology - Crypto '86, Lecture Notes in Computer Science (LNCS) 263, Springer Verlag, 1987, pp. 234–238.

[5] G. Brassard, C. Crépeau and M. Sántha, *Oblivious transfers and intersecting codes*, IEEE Transaction on Information Theory, special issue on coding and complexity, Vol. 42, 1996, pp. 1769-1780.

[6] E. F. Brickell, *Some ideal secret sharing schemes*, J. of Combin. Math. and Combin. Comput. 6, 1989, pp. 105–113.

[7] A. Gál, *Combinatorial methods in Boolean function complexity*, Ph.D. thesis, University of Chicago, 1995.

[8] S. Even, O. Goldreich and A. Lempel, *A randomized protocol for signing contracts*, Communications of the ACM, Vol. 28, 1985, pp. 637–647.

[9] R. Fagin, M. Naor and P. Winkler, *Comparing information without leaking it*, Communications of the ACM 39, 1996, pp. 77–85.

[10] O. Farràs, J.R. Metcalf-Burton, C. Padró and L. Vázquez, *On the Optimization of Bipartite Secret Sharing Schemes*, ICITS 2009.

[11] O. Goldreich and R. Vainish, *How to solve any protocol problem: An efficiency improvement*, Advances in Cryptology (CRYPTO), LNCS 293, 1987, pp. 73–86.

[12] Y. Ishai and E. Kushilevitz, *Private simultaneous messages protocols with applications*, Proc. of ISTCS97, IEEE Computer Society, 1997, pp. 174-184.

[13] J. Killian, *Founding cryptogrpahy on oblivious transfer*, Proc. of the 20th Annual ACM Symposium on Theory of Computing (STOC), 1988, pp. 20–31.

[14] Y. Mu, J. Zhang and V. Varadharajan, *m out of n Oblivious Transfer*, ACISP 2002, LNCS 2384, 2002, pp. 395–405.

[15] M. Naor and B. Pinkas, *Oblivious polynomial evaluation*, Proc. of the 31st Annual ACM Symposium on Theory of computing (STOC), 1999, pp. 245-254.

[16] M. Naor and B. Pinkas, *Computationally secure oblivious transfer*, Journal of Cryptology, 18, 2005, pp. 1–35.

[17] M. O. Rabin, *How to exchange secrets by oblivious transfer*, Tech. Memo TR-81, Aiken Computation Laboratory, 1981.

[18] B. Shankar, K. Srinathan and C. Pandu Rangan, *Alternative protocols for generalized oblivious transfer*, Proc. of ICDCN08, LNCS 4904, 2008, pp. 304-309.

[19] T. Tassa, *Hierarchical threshold secret sharing*, Journal of Cryptology, 20, 2007, pp. 237–264. An earlier version appeared in Proc. of the First Theory of Cryptography Conference, 2004, pp. 473–490.

[20] A. C. Yao, *Protocols for secure computation*, Proc. of IEEE Foundations of Computer Science (FOCS), 1982, pp. 160–164.