On Unconditionally Secure Distributed Oblivious Transfer*

Carlo Blundo[1], Paolo D'Arco[1]†, Alfredo De Santis[1], and Douglas Stinson[2]

[1] Dipartimento di Informatica ed Applicazioni
Università di Salerno, 84081 Baronissi (SA), Italy
e-mail: {carblu, paodar, ads}@dia.unisa.it

[2] School of Computer Science
University of Waterloo, N2L 3G1, Waterloo, Ontario, Canada
e-mail: dstinson@cacr.math.uwaterloo.ca

November 9, 2005

Abstract

This paper is about the Oblivious Transfer in the distributed model proposed by M. Naor and B. Pinkas. In this setting a Sender has n secrets and a Receiver is interested in one of them. During a set up phase, the Sender gives information about the secrets to m Servers. Afterwards, in a recovering phase, the Receiver can compute the secret she wishes by interacting with any k of them. More precisely, from the answers received she computes the secret in which she is interested but she gets no information on the others and, at the same time, any coalition of $k-1$ Servers can neither compute any secret nor figure out which one the Receiver has recovered.

We present an analysis and new results holding for this model: lower bounds on the resources required to implement such a scheme (i.e., randomness, memory storage, communication complexity); some impossibility results for one-round distributed oblivious transfer protocols; two polynomial-based constructions implementing 1-out-of-n distributed oblivious transfer, which generalize and strengthen the two constructions for 1-out-of-2 given by Naor and Pinkas; as well as new one-round and two-round distributed oblivious transfer protocols, both for threshold and general access structures on the set of Servers, which are optimal with respect to some of the given bounds. Most of these constructions are basically combinatorial in nature.

1 Introduction

Introduced by Rabin in [38], and subsequently defined in different forms [23, 9], the *oblivious transfer* (OT, for short) has found many applications in cryptographic studies and protocol design. Basically, such a protocol enables one party to transfer knowledge to another in an

*A preliminary version of this paper appeared in the Proceedings of SAC 2002, *Lecture Notes in Computer Science*, Vol. 2595, pp. 291-309, 2003.

†This research was partially done while the author was a Post-Doc Fellow at the Department of Combinatorics and Optimization of the University of Waterloo, Ontario, Canada.

"oblivious" way. Rabin's definition, for example, enables a Sender to transmit a message to a Receiver in such a way that the Receiver with probability $\frac{1}{2}$ gets the message while, with the same probability, she does not, and the Sender does not know which event has occurred. Rabin showed how this transfer can be used in order to exchange secrets, and subsequently several other researchers have shown some useful applications of this concept. The protocol proposed by Rabin was later strengthened in [24].

The second OT definition was given in [23]. In this form, the Sender has two secrets and the Receiver is interested in one of them. After the execution of the protocol, the Receiver gets the secret she wishes to recover, obtaining at the same time no information on the other, while the Sender does not know which secret the Receiver has recovered. The author of [23] showed a first application to signing contracts.

The last and more general form of OT was introduced in [9], under the name of *all-or-nothing Disclosure of Secrets*, even if the same concept was born in an artificial intelligence context [44], under the name of *multiplexing*. Here the Sender has n secrets and the Receiver is interested in one of them. After the execution of the protocol, the Receiver gets the secret she wishes to recover, obtaining at the same time no information on the others, while the Sender does not know which secret the Receiver has recovered.

All these forms were shown to be equivalent [10, 8, 14], and Kilian in [30] showed that the OT is a complete primitive, in the sense that it can be used as a building block for any secure function evaluation (multi-party computation).

A variety of slightly different definitions and implementations can be found in the literature as well as papers addressing issues such as the relation of the OT with other cryptographic primitives, the assumptions required to implement such a concept, reductions among "more complex" forms of OT to "simpler ones" and applicative environments (e.g., [14, 10, 22, 18, 3, 20, 21, 15, 28, 36, 27], just to name few examples).

Our Contribution. In this paper we study *unconditionally secure distributed oblivious transfer protocols*, introduced in [34] in order to strengthen the security of protocols designed for electronic auctions [36]. We present an analysis and some new results: lower bounds on the resources required by an implementation such as randomness, memory storage, and communication complexity; some impossibility results for one-round protocols; two polynomial-based constructions implementing 1-out-of-n distributed oblivious transfer which generalize and strengthen the two constructions for 1-out-of-2 schemes given by M. Naor and B. Pinkas; as well as new one-round and two-round distributed oblivious transfer protocols, both for threshold and general access structures on the set of Servers, which are optimal with respect to some of the given bounds. Most of these constructions are basically combinatorial in nature.

Related Work. In the literature there are many papers that address problems related to 1-out-of-n distributed oblivious transfer. In [1], for example, the authors show how to distribute a function between several Servers, in such a way that a user can compute the function by interacting with the Servers; the Servers cannot find out which value of the function the user computes, but the user can compute the function in *more than* one point. Another very close area is represented by PIR (Private Information Retrieval) schemes, introduced in [12]. A PIR scheme enables a user to retrieve an item of information from a public accessible database in such a way that the database manager cannot figure out from the query which item the user is interested in. However, the user can get information about more than one item. On the other hand, in SPIR (Symmetric Private Information Retrieval) schemes [25], the user can get information about *one and only one* item, i.e. even the privacy of the database is considered. In PIR and SPIR schemes, the emphasis is placed on the *communication complexity* of the interaction of user and Servers. Notice that a SPIR Scheme can be seen as a *communication-efficient* 1-out-of-n oblivious transfer scheme and the protocols given in [25] represent the first 1-round distributed implementation of 1-out-of-n oblivious transfer. However, the main differences between the model we are going to consider and (information theoretic) SPIR schemes are that in SPIR schemes the Receiver communicates with k out of k Servers in order to retrieve an item while in our setting the Receiver can choose k out of m Servers, where $k \leq m$. Moreover, in SPIR schemes, the security of the Sender against *coalitions* of Receiver and Servers is not of concern. Other PIR papers of interest, for the distributed OT scenario we consider, are [2, 26, 17].

Rivest's model in [39], where a trusted initializer participates *only* during the set up phase of the system (see also [7]), provides a very close setting to the one described in [34] and considered in this paper. A paper which deals with distributed oblivious transfer implementations, close to the setting introduced in [34] (but not unconditionally secure) is [43]. Finally, unconditionally secure distributed oblivious transfer schemes for general access structures have also been studied in [37].

In our constructions we use secret sharing schemes. Secret sharing schemes were introduced in 1979 by Blakley [4] and Shamir [40], and have been extensively studied during the last years. The reader can find an introduction in [42] and references to the literature in [41].

2 The Distributed Model

Let us define the model we are going to consider. We assume that the Sender holds n secrets and the Receiver is interested in one of them. Hence, we are concerned with a 1-out-of-n distributed oblivious transfer.

2.1 An Informal Description

In the distributed setting, the Sender $\mathcal{S}$ does not directly interact with the Receiver $\mathcal{R}$ in order to carry out the oblivious transfer. Rather, he *delegates* m Servers to accomplish this task for him. More precisely, we consider the following scenario (see Figure 1):

Set-up Phase. Let m and k be two integers such that $1 < k \leq m$. Let $S_1, \ldots, S_m$ be m Servers holding programs $P_1, \ldots, P_m$, respectively. The Sender $\mathcal{S}$ generates m data $D_1, \ldots, D_m$, and, for $i = 1, \ldots, m$ sends, *in a secure way*, the data D_i to Server S_i.

Oblivious Transfer Phase. The Receiver $\mathcal{R}$ holds a program R which enables her to interact with a subset $\{S_{i_1}, \ldots, S_{i_k}\}$ of the Servers at her choice. Using the knowledge acquired by exchanging messages with the Servers, $\mathcal{R}$ recovers the secret in which she is interested, but receives no information on the other secrets. At the same time, no subset of $k-1$ Servers, gains any information about the secret she has recovered[1]. More precisely, a distributed (k, m)-DOT-$\binom{n}{1}$ must guarantee:

[1]Along the same line of [34], we assume the existence of an external mechanism which guarantees that the Receiver can contact no more than k Servers. This issue is independent of the distributed oblivious transfer scheme and, hence, it is not considered in this paper. The reader is referred to [34] for some techniques to solve the problem.

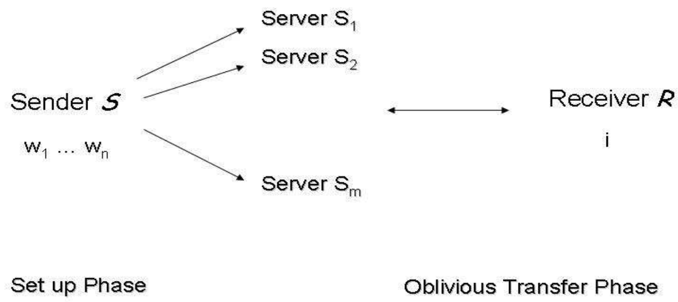

Figure 1: Distributed Oblivious Transfer

1. Correctness. If the Receiver gets information from k out of the m Servers, she can compute the secret.

2. Receiver's Privacy. No coalition of less than k Servers gains information about which secret the Receiver has recovered.

3. Sender's Privacy w.r.t. $k-1$ Servers and the Receiver. A coalition of the Receiver with $k-1$ dishonest Servers does not get any information about the n secrets.

4. Sender's Privacy w.r.t. a "Greedy" Receiver. Given the transcript of the interaction with k Servers, the Receiver should gain information about at most a single secret, and no information about the others. This property should be satisfied even if the Receiver, once has computed a secret, colludes with $k-1$ dishonest Servers.

Notice that, in [34], properties 3. and 4. are only guaranteed with respect to a threshold t and a threshold ℓ, respectively, which should be as close to k as possible.

2.2 A Formal Model

Notation. Let $W = W_1 \times \cdots \times W_n$ be the set of all possible sequences of n secrets, and let $T = \{1, \ldots, n\}$ be a set of n indices.

The Sender $\mathcal{S}$ holds a program $S(w, r)$, which takes in input a sequence $w \in W$ and a random string r, and outputs m data, $D_1, \ldots, D_m$. These data will be sent by $\mathcal{S}$ securely to the Servers $S_1, \ldots, S_m$, respectively.

The Servers $S_1, \ldots, S_m$ hold programs $P_1, \ldots, P_m$, for interacting with the Receiver, which are run on $D_1, \ldots, D_m$ and possibly random strings $r_1, \ldots, r_m$. However, to simplify the description, we assume that, for any $i = 1, \ldots, m$, the data D_i comprises also the random bits used by S_i in an execution of the program P_i.

The Receiver $\mathcal{R}$ holds also a program, $R(i, D_R)$, for interacting with the Servers, which receives in input an index of a secret $i \in T$ and a sequence D_R of random bits.

The $m+1$ programs $P_1, \ldots, P_m$ and R, with the associated input data $D_1, \ldots, D_m, i, D_R$, specify the computations to be performed to achieve (k, m)-DOT-$\binom{n}{1}$.

In order to represent dishonest behaviors, where a coalition of at most $k-1$ Servers tries to figure out which secret $\mathcal{R}$ has recovered from the transfer, we assume that dishonest Servers $S_{j_1}, \ldots, S_{j_{k-1}}$ execute modified versions of the programs $P_{j_1}, \ldots, P_{j_{k-1}}$, denoted by $\overline{P}_{j_1}, \ldots, \overline{P}_{j_{k-1}}$. Similarly, a dishonest $\mathcal{R}$, who tries to gain some information about more than one secret, executes a modified version of the program R, denoted by $\overline{R}$.

We require our schemes to be secure against all possible *probabilistic* and *deterministic* adversarial programs. However, since we are analysing *unconditionally secure* schemes, without loss of generality, we can assume that the modified programs $\overline{P}_1, \ldots, \overline{P}_m$ and $\overline{R}$ are *deterministic*. Indeed, let $\overline{P}_j$ be a probabilistic program which uses ℓ random bits. If a scheme is secure against 2^ℓ deterministic programs $\overline{P}_j^1, \ldots, \overline{P}_j^{2^\ell}$, where each of them is equal to $\overline{P}_j$, run by using one of the 2^ℓ possible random strings of ℓ bits, then it is clearly secure against $\overline{P}_j$. Any execution of $\overline{P}_j$ corresponds to an execution of one of the programs $\overline{P}_j^1, \ldots, \overline{P}_j^{2^\ell}$.

The programs held by the parties are publicly known. The data $w, i, D_1, \ldots, D_m$, and D_R, used by the programs, are private to the parties. They will be described by means of random variables, represented in bold face type, i.e., $\mathbf{W}, \mathbf{T}, \mathbf{D}_1, \ldots, \mathbf{D}_m$, and $\mathbf{D}_R$. Moreover, for $j = 1, \ldots, m$, we will use random variables $\mathbf{C}_j$ to denote the transcript of the communication between $\mathcal{R}$ and Server S_j, where both are honest, $\overline{\mathbf{C}}_j$ to denote the transcript of the communication between $\mathcal{R}$ and Server S_j where one of them is running a modified program (but over the same data D_j, D_R and i), and $\mathbf{W}_i$ for the i-th secret of the sequence held by the Sender. Finally, to simplify the discussion, if, for $i = 1, \ldots, n$, $\mathbf{A}_i$ is a random variable, and $X = \{j_1, \ldots, j_m\} \subseteq \{1, \ldots, n\}$ is a subset of indices such that $j_1 < \ldots < j_m$, then $\mathbf{A}_X$ will denote the sequence of random variables $\mathbf{A}_{j_1}, \ldots, \mathbf{A}_{j_m}$.

Receiver's Data. In our model the Receiver holds a program $R(i, D_R)$ where i represents the index of the secret she chooses, and D_R are truly random bits. No interaction is allowed between the Sender and the Receiver. However, we might generalise the model and assume that, during the set-up phase, the Sender sends also data to the Receiver. Hence D_R might represent data received by the Sender and truly random bits. The formal definitions we give in the following model this more general setting, and all properties and bounds we prove in Section 3 hold for this setting. On the other hand, the results we present in Section 4, by analysing one-round schemes, do assume that D_R are truly random bits.

Independence of the Receiver's choice and Communication in the Model. Notice that the choice of the Receiver is *independent* of the sequence of secrets w, the data $D_1, \ldots, D_m$ and D_R. Moreover, we assume that, for $i = 1, \ldots, n$, $Pr(\mathbf{T} = i) > 0$, i.e., any choice in $\{1, \ldots, n\}$ is possible. Since we focus our attention on unconditionally secure DOT protocols, we use the entropy function, which leads to a compact and concise description. The reader is referred to the Appendix for a short introduction to the entropy function and information theory. In terms of information theory the above assumption means that, for $X = \{1, \ldots, m\}$, it holds that:

$$H(\mathbf{T}|\mathbf{W}, \mathbf{D}_X, \mathbf{D}_R) = H(\mathbf{T}). \tag{1}$$

Then, *once the Receiver has chosen* an index of a secret, the program of the Receiver and the programs of the Servers, the private data and the random bits they use during the current execution of the programs, *completely determine* the transcript of the interaction Receiver-Servers. In other words, for any subset of indices $X \subseteq \{1, \ldots, m\}$, and for any $i \in \{1, \ldots, n\}$, it holds that:

$$H(\mathbf{C}_X | \mathbf{D}_X, \mathbf{D}_R,\ \mathbf{T} = i) = 0. \tag{2}$$

Notice that the above condition is equivalent to

$$H(\mathbf{C}_X | \mathbf{D}_X, \mathbf{D}_R, \mathbf{T}) = 0 \tag{3}$$

since $H(\mathbf{C}_X | \mathbf{D}_X, \mathbf{D}_R, \mathbf{T}) = \sum_{i=1}^{n} H(\mathbf{C}_X | \mathbf{D}_X, \mathbf{D}_R, \mathbf{T} = i) \cdot Pr(\mathbf{T} = i)$, and $Pr(\mathbf{T} = i) > 0$ for any $i = 1, \ldots, n$.

Definitions: Correctness and Privacy. By using the above notation, we define the conditions that a (k, m)-DOT-$\binom{n}{1}$ oblivious transfer protocol must satisfy.

Definition 2.1 *The sequence of programs* $[S, P_1, \ldots P_m, R]$ *is* correct *for* (k, m)*-DOT-*$\binom{n}{1}$ *if, for any subset of* k *indices* $X \subseteq \{1, \ldots, m\}$*, and for any* $i \in \{1, \ldots, n\}$*, it holds that*

$$H(\mathbf{W}_i | \mathbf{C}_X, \mathbf{D}_R, \mathbf{T} = i) = 0. \tag{4}$$

$\triangle$

Notice that the above definition means that, after interacting with any k Servers, an honest Receiver always recovers the secret in which she is interested.

Definition 2.2 *The sequence of programs* $[S, P_1, \ldots P_m, R]$ *is* private *for* (k, m)*-DOT-*$\binom{n}{1}$ *if,*

- Receiver's Privacy: *for any subset of* $k-1$ *indices* $X \subset \{1, \ldots, m\}$*, and for any sequence* $\overline{P}_X$*, it holds that*
$$H(\mathbf{T} | \mathbf{D}_X, \overline{\mathbf{C}}_X) = H(\mathbf{T}). \tag{5}$$
- Sender's Privacy w.r.t. $k-1$ Servers and the Receiver: *for any subset of* $k-1$ *indices* $X \subset \{1, \ldots, m\}$*, it holds that*
$$H(\mathbf{W} | \mathbf{D}_X, \mathbf{D}_R) = H(\mathbf{W}). \tag{6}$$
- Sender's Privacy w.r.t. a "Greedy" Receiver: *for any subset of* k *indices* $X \subseteq \{1, \ldots, m\}$*, for any* $i = 1, \ldots, n$*, for any possible* D_R*, and for any* $\overline{R}$*, there exists an index* $\widetilde{i} = f(i, D_R, \overline{R})$ *such that*
$$\begin{array}{lll} i) & H(\mathbf{W} | \mathbf{T} = i, \mathbf{D}_R = D_R, \overline{\mathbf{C}}_X, \mathbf{W}_{\widetilde{i}}) = H(\mathbf{W} | \mathbf{W}_{\widetilde{i}}), & \textit{if } \widetilde{i} \in \{1, \ldots, n\} \\ ii) & H(\mathbf{W} | \mathbf{T} = i, \mathbf{D}_R = D_R, \overline{\mathbf{C}}_X) = H(\mathbf{W}), & \textit{otherwise.} \end{array} \tag{7}$$

$\triangle$

Let us briefly describe the ideas the above definition captures.

Receiver's Privacy: Condition (5) of Definition 2.2 states that the index of the secret $\mathcal{R}$ chooses is independent of D_X and $\overline{C}_X$, for any subset X of size $k-1$. Therefore, it ensures that a coalition of $k-1$ dishonest Servers, by using their own private data D_X, and the transcript

$\overline{C}_X$ of the communication with the Receiver, obtained by running a sequence of malicious programs $\overline{P}_X$, does not gain any information about $\mathcal{R}$'s choice.

Sender's Privacy w.r.t. $k-1$ Servers and the Receiver: Condition (6) of Definition 2.2 states that the sequence of secrets held by $\mathcal{S}$ is independent of D_X, for any subset X of size $k-1$ and D_R. Hence, it guarantees that a coalition of $k-1$ dishonest Servers, with the cooperation of a dishonest Receiver $\mathcal{R}$, by using their own private data D_X and D_R, does not get any information about the sequence of secrets held by $\mathcal{S}$. Notice that, in stating our property, we could have also considered the transcript C_X and the index i of an interaction between S_X and R. Indeed, they are parts of the "view" held by the coalition. Hence we could have required that

$$H(\mathbf{W}|\mathbf{D}_X, \mathbf{C}_X, \mathbf{D}_R, \mathbf{T}) = H(\mathbf{W}). \tag{8}$$

However, the above one is equivalent to condition (6). Indeed, due to the independence of $\mathbf{T}$ from $\mathbf{W}, \mathbf{D}_X$, and $\mathbf{D}_R$, stated by (1), it follows that

$$H(\mathbf{W}|\mathbf{D}_X, \mathbf{D}_R) = H(\mathbf{W}|\mathbf{D}_X, \mathbf{D}_R, \mathbf{T}). \tag{9}$$

The above equality holds because condition (1) and property (39) of Appendix A, imply

$$H(\mathbf{T}) = H(\mathbf{T}|\mathbf{D}_X, \mathbf{D}_R, \mathbf{W}) \leq H(\mathbf{T}|\mathbf{D}_X, \mathbf{D}_R) \leq H(\mathbf{T}).$$

Therefore, from (38) of Appendix A, the mutual information $I(\mathbf{W}, \mathbf{T}|\mathbf{D}_X, \mathbf{D}_R)$ is equal to

$$H(\mathbf{W}|\mathbf{D}_X, \mathbf{D}_R) - H(\mathbf{W}|\mathbf{D}_X, \mathbf{D}_R, \mathbf{T}) = H(\mathbf{T}|\mathbf{D}_X, \mathbf{D}_R) - H(\mathbf{T}|\mathbf{D}_X, \mathbf{D}_R, \mathbf{W}) = 0.$$

Hence, $H(\mathbf{W}|\mathbf{D}_X, \mathbf{D}_R) = H(\mathbf{W}|\mathbf{D}_X, \mathbf{D}_R, \mathbf{T})$. Moreover, as stated by condition (3), the transcript C_X is function of D_X, D_R and T. Due to property (40), it holds that

$$H(\mathbf{W}|\mathbf{D}_X, \mathbf{D}_R, \mathbf{T}) = H(\mathbf{W}|\mathbf{C}_X, \mathbf{D}_X, \mathbf{D}_R, \mathbf{T}). \tag{10}$$

Therefore, we have preferred condition (6) to condition (8), since they are equivalent, and condition (6) is simpler than the latter.

Sender's Privacy w.r.t. a "Greedy" Receiver: Condition (7) of Definition 2.2 states that the amount of information about the sequence of secrets w, given the choice of the Receiver, her data set D_R, the transcript $\overline{C}_X$ of the communication with a subset X of k Servers, and possibly one of the secrets $W_{\widetilde{i}}$, is exactly $H(\mathbf{W}|\mathbf{W}_{\widetilde{i}})$, i.e., the amount of information on $\mathbf{W}$, once the Receiver has obtained $W_{\widetilde{i}}$. Such a condition guarantees that a dishonest $\mathcal{R}$, by interacting with a subset X of k Servers, infers *at most* one secret among the ones held by the Sender $\mathcal{S}$. From a technical point of view, we have used an index $\widetilde{i} = f(i, D_R, \overline{R})$ to represent the possibility that $\mathcal{R}$ gets a different secret from the one she should get through a correct use of her program R. Indeed, any program $\overline{R}$, attempting to get information about more than one secret, might get a certain secret $W_{\widetilde{i}}$, different from W_i, the one she should get once i is fixed and R is executed. Notice that condition (7) is stated in two parts because it might also happens that the Receiver's program $\overline{R}$ does not try to get a whole secret by interacting with Servers S_X, but just partial information she might use in order to get partial knowledge about more secrets. We model this attack by an index $\widetilde{i}$ which does not belong to $\{1, \ldots, n\}$.

Condition (7) of Definition 2.2 can be strengthened by considering an attack performed by the Receiver, once she has already recovered a secret, *with the cooperation* of other $k-1$ Servers. In other words, she might try to get more information about the secrets, helped by $k-1$ dishonest Servers.

We will say that the sequence of programs $[S, P_1, \dots P_m, R]$ defines a *strong* (k,m)-DOT-$\binom{n}{1}$ if a further security condition is satisfied. More precisely,

Definition 2.3 *The sequence of programs* $[S, P_1, \dots P_m, R]$ *defines a* strong (k,m)*-DOT-*$\binom{n}{1}$ *if it is correct and private and it holds that:*

- Sender's Privacy w.r.t. a "Greedy" Receiver and $k-1$ Servers: *for any subset of* $k-1$ *indices* $X \subset \{1, \dots, m\}$*, for any subset of* k *indices* $Y \subseteq \{1, \dots, m\}$*, for any* $i = 1, \dots, n$*, for any possible* D_R*, and for any* $\overline{R}$*, there exists an index* $\widetilde{i} = f(i, D_R, \overline{R})$ *such that*

$$\begin{array}{lll} i) & H(\mathbf{W}|\,\mathbf{T}=i, \mathbf{D}_R = D_R, \mathbf{D}_X, \overline{\mathbf{C}}_Y, \mathbf{W}_{\widetilde{i}}) = H(\mathbf{W}|\mathbf{W}_{\widetilde{i}}), & \textit{if } \widetilde{i} \in \{1,\dots,n\} \\ ii) & H(\mathbf{W}|\mathbf{T}=i, \mathbf{D}_R = D_R, \mathbf{D}_X, \overline{\mathbf{C}}_Y) = H(\mathbf{W}), & \textit{otherwise.} \end{array} \quad (11)$$

Condition (11) of Definition 2.3 states that the amount of information about the sequence of secrets w, given the choice of the Receiver, her data set D_R, the data D_X of $k-1$ dishonest Servers, the transcript $\overline{C}_Y$ of the communication with a subset Y of k Servers, and possibly one of the secrets $W_{\widetilde{i}}$, is exactly $H(\mathbf{W}|\mathbf{W}_{\widetilde{i}})$, i.e., the amount of information on $\mathbf{W}$, once the Receiver has obtained $W_{\widetilde{i}}$. Hence, a dishonest $\mathcal{R}$, interacting with a subset Y of k Servers, can recover a secret. Then, even if she colludes with a subset X of $k-1$ dishonest Servers, by putting together the information they possess and the transcript of the previous interaction, the coalition does not get any information about other secrets.

Notice that, in our model condition (11) implies condition (7). Later on we will show that condition (11) cannot be achieved with *only one round of interaction.* In other words, a strong (k,m)-DOT-$\binom{n}{1}$ cannot be realized by means of a one-round protocol. On the other hand, with two rounds of interaction, this level of privacy can be obtained.

Remark. It is straightforward to see that conditions (5), (6), (7), and (11) hold even if the coalition of dishonest Servers has size less than $k-1$. Formally, such a property can be derived by applying conditions (5), (6), (7), (11) and property (39) of Appendix A.

3 Lower Bounds

Using some information theory tools, we prove bounds on the memory storage, on the communication complexity, and on the randomness needed by a correct and private DOT scheme.

The following simple lemma shows that, given four random variables $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$ and $\mathbf{D}$, if $\mathbf{B}$ is a function of $\mathbf{C}$ and $\mathbf{D}$, then $\mathbf{B}$ and $\mathbf{D}$ give less information on $\mathbf{A}$ than $\mathbf{C}$ and $\mathbf{D}$.

Lemma 3.1 *Let* $\mathbf{A}$*,* $\mathbf{B}$*,* $\mathbf{C}$ *and* $\mathbf{D}$ *be four random variables such that* $H(\mathbf{B}|\mathbf{C},\mathbf{D}) = 0$*. Then,* $H(\mathbf{A}|\mathbf{B},\mathbf{D}) \geq H(\mathbf{A}|\mathbf{C},\mathbf{D})$.

Proof. We prove the lemma showing that

$$H(\mathbf{A}|\mathbf{B},\mathbf{D}) \geq H(\mathbf{A}|\mathbf{B},\mathbf{C},\mathbf{D}) = H(\mathbf{A}|\mathbf{C},\mathbf{D}).$$

Indeed, the left inequality follows from (39) of Appendix A. The equality on the right holds because, from (32) and (39) of Appendix A and the hypothesis,

$$0 \leq H(\mathbf{B}|\mathbf{A}, \mathbf{C}, \mathbf{D}) \leq H(\mathbf{B}|\mathbf{C}, \mathbf{D}) = 0.$$

Therefore, the mutual information $I(\mathbf{A}; \mathbf{B}|\mathbf{C}, \mathbf{D})$, from (38) of Appendix A, is equal to

$$H(\mathbf{A}|\mathbf{C}, \mathbf{D}) - H(\mathbf{A}|\mathbf{B}, \mathbf{C}, \mathbf{D}) = H(\mathbf{B}|\mathbf{C}, \mathbf{D}) - H(\mathbf{B}|\mathbf{A}, \mathbf{C}, \mathbf{D}) = 0.$$

Hence, $H(\mathbf{A}|\mathbf{B}, \mathbf{C}, \mathbf{D}) = H(\mathbf{A}|\mathbf{C}, \mathbf{D})$. ∎

Notice that condition (6) of Definition 2.2 implies that a coalition of $k-1$ Servers and the Receiver get no information about *any* single secret. We state the following:

Lemma 3.2 *In any correct and private (k, m)-DOT-$\binom{n}{1}$ scheme, for any set of $k-1$ indices $X \subset \{1, \ldots, m\}$, for any $j \in \{1, \ldots, n\}$, it holds that*

$$H(\mathbf{W}_j|\mathbf{D}_X, \mathbf{D}_R) = H(\mathbf{W}_j). \tag{12}$$

Proof. Indeed, denoting by $\mathbf{W} \setminus \mathbf{W}_j$ a random variable representing the sequence of all secrets in w but w_j, using condition (6), and properties (35) and (34) of Appendix A, it results

$$\begin{aligned} H(\mathbf{W}) &= H(\mathbf{W}_j, \mathbf{W} \setminus \mathbf{W}_j|\mathbf{D}_X, \mathbf{D}_R) \\ &= H(\mathbf{W}_j|\mathbf{D}_X, \mathbf{D}_R) + H(\mathbf{W} \setminus \mathbf{W}_j|\mathbf{D}_X, \mathbf{D}_R, \mathbf{W}_j) \\ &\leq H(\mathbf{W}_j) + H(\mathbf{W} \setminus \mathbf{W}_j|\mathbf{W}_i) = H(\mathbf{W}). \end{aligned}$$

Hence, it must be $H(\mathbf{W}_j|\mathbf{D}_X, \mathbf{D}_R) = H(\mathbf{W}_j)$. ∎

Due to the equivalence of condition (6) with condition (8), for any $j = 1, \ldots, n$, it also holds that,

$$H(\mathbf{W}_j|\mathbf{D}_X, \mathbf{C}_X, \mathbf{D}_R, \mathbf{T}) = H(\mathbf{W}_j). \tag{13}$$

The following lemma states that *any secret* of the sequence held by the Sender is independent from the index i. More precisely, we prove that, for any $j = 1, \ldots, n$, the $Pr(w_j|D_X, D_R) = Pr(w_j|D_X, D_R, i)$, for any $i = 1, \ldots, n$.

Lemma 3.3 *In any correct and private (k, m)-DOT-$\binom{n}{1}$ scheme, for any subset $X \subseteq \{1, \ldots, m\}$, and for any $j = 1, \ldots, n$, it holds that*

$$H(\mathbf{W}_j|\mathbf{D}_X, \mathbf{D}_R) = H(\mathbf{W}_j|\mathbf{D}_X, \mathbf{D}_R, \mathbf{T}). \tag{14}$$

Proof. Since $\mathbf{W} = (\mathbf{W}_1, \ldots, \mathbf{W}_n)$, property (1) and properties (39) and (32) of Appendix A, imply that, for any $j = 1, \ldots, n$,

$$H(\mathbf{T}) = H(\mathbf{T}|\mathbf{D}_X, \mathbf{D}_R, \mathbf{W}) \leq H(\mathbf{T}|\mathbf{D}_X, \mathbf{D}_R, \mathbf{W}_j) \leq H(\mathbf{T}|\mathbf{D}_X, \mathbf{D}_R) \leq H(\mathbf{T}).$$

Therefore, from (38) of Appendix A, the mutual information $I(\mathbf{W}_j, \mathbf{T}|\mathbf{D}_X, \mathbf{D}_R)$ is equal to

$$H(\mathbf{W}_j|\mathbf{D}_X, \mathbf{D}_R) - H(\mathbf{W}_j|\mathbf{D}_X, \mathbf{D}_R, \mathbf{T}) = H(\mathbf{T}|\mathbf{D}_X, \mathbf{D}_R) - H(\mathbf{T}|\mathbf{D}_X, \mathbf{D}_R, \mathbf{W}_j) = 0.$$

Hence, $H(\mathbf{W}_j|\mathbf{D}_X, \mathbf{D}_R) = H(\mathbf{W}_j|\mathbf{D}_X, \mathbf{D}_R, \mathbf{T})$. ∎

Using the above lemma we prove that the data held by any subset of k Servers and the information held by the Receiver are enough to recover all the secrets.

Lemma 3.4 *In any correct and private* (k,m)*-DOT-*$\binom{n}{1}$ *scheme, for any subset of* k *indices* $X \subseteq \{1,\dots,m\}$*, it holds that*

$$H(\mathbf{W}|\mathbf{D}_X,\mathbf{D}_R) = 0.$$

Proof. From (35) and (39) of Appendix A, it holds that

$$H(\mathbf{W}|\mathbf{D}_X,\mathbf{D}_R) \leq \sum_{j=1}^{n} H(\mathbf{W}_j|\mathbf{D}_X,\mathbf{D}_R)$$

Due to Lemma 3.3, for any $j = 1,\dots,n$, it holds that

$$H(\mathbf{W}_j|\mathbf{D}_X,\mathbf{D}_R) = H(\mathbf{W}_j|\mathbf{D}_X,\mathbf{D}_R,\mathbf{T}) = H(\mathbf{W}_j|\mathbf{D}_X,\mathbf{D}_R,\mathbf{T}=j).$$

It follows that

$$\sum_{j=1}^{n} H(\mathbf{W}_j|\mathbf{D}_X,\mathbf{D}_R) = \sum_{j=1}^{n} H(\mathbf{W}_j|\mathbf{D}_X,\mathbf{D}_R,\mathbf{T}=j).$$

Since condition (2) states that $H(\mathbf{C}_X|\mathbf{D}_X,\mathbf{D}_R,\mathbf{T}=j) = 0$, setting $\mathbf{A} = \mathbf{W}_j, \mathbf{B} = \mathbf{C}_X, \mathbf{C} = \mathbf{D}_X$, and $\mathbf{D} = (\mathbf{D}_R, \mathbf{T}=j)$, and applying Lemma 3.1, it holds that

$$H(\mathbf{W}_j|\mathbf{D}_X,\mathbf{D}_R,\mathbf{T}=j) \leq H(\mathbf{W}_j|\mathbf{C}_X,\mathbf{D}_R,\mathbf{T}=j).$$

The above inequality and Definition 2.1 imply that

$$\sum_{j=1}^{n} H(\mathbf{W}_j|\mathbf{D}_X,\mathbf{D}_R,\mathbf{T}=j) \leq \sum_{j=1}^{n} H(\mathbf{W}_j|\mathbf{C}_X,\mathbf{D}_R,\mathbf{T}=j) = 0.$$

Hence, $H(\mathbf{W}|\mathbf{D}_X,\mathbf{D}_R) = 0$. ■

We prove that the amount of information D_j, held by Server S_j, given the information held by any other $k-1$ Servers and the information held by the Receiver, is greater than or equal to the amount of information contained in the whole sequence of the n secrets. This property is formally stated by the following:

Lemma 3.5 *In any correct and private* (k,m)*-DOT-*$\binom{n}{1}$ *scheme, for any subset of indices* $X \subset \{1,\dots,m\}$*, where* $1 \leq |X| \leq k-1$*, and for any index* $j \notin X$*, it holds that*

$$H(\mathbf{D}_j|\mathbf{D}_X,\mathbf{D}_R) \geq H(\mathbf{W}).$$

Proof. Let $Y \subset \{1,\dots,m\}$, such that $|Y| = k - |X| - 1$, $j \notin Y$, and $X \cap Y = \emptyset$. According to Appendix A, the mutual information $I(\mathbf{W};\mathbf{D}_j|\mathbf{D}_{X\cup Y},\mathbf{D}_R)$ can be written as

$$H(\mathbf{W}|\mathbf{D}_{X\cup Y},\mathbf{D}_R) - H(\mathbf{W}|\mathbf{D}_{X\cup Y\cup\{j\}},\mathbf{D}_R) = H(\mathbf{D}_j|\mathbf{D}_{X\cup Y},\mathbf{D}_R) - H(\mathbf{D}_j|\mathbf{D}_{X\cup Y},\mathbf{D}_R,\mathbf{W}).$$

From condition (6) of Definition 2.2, it follows that $H(\mathbf{W}|\mathbf{D}_{X\cup Y},\mathbf{D}_R) = H(\mathbf{W})$. Then, from (32) of Appendix A, we get $H(\mathbf{D}_j|\mathbf{D}_{X\cup Y},\mathbf{W},\mathbf{D}_R) \geq 0$, and, from Lemma 3.4, we get $H(\mathbf{W}|\mathbf{D}_{X\cup Y\cup\{j\}},\mathbf{D}_R) = 0$. Therefore,

$$H(\mathbf{D}_j|\mathbf{D}_{X\cup Y},\mathbf{D}_R) \geq H(\mathbf{W}).$$

Applying property (39) of Appendix A, it holds that

$$H(\mathbf{D}_j|\mathbf{D}_X, \mathbf{D}_R) \geq H(\mathbf{D}_j|\mathbf{D}_{X\cup Y}, \mathbf{D}_R) \geq H(\mathbf{W}).$$

■

Using the above results, we establish a lower bound on the size of the data that each Server has to store to set up a correct and private (k, m)-DOT-$\binom{n}{1}$ scheme. More precisely, we show the following result:

Theorem 3.6 *In any correct and private (k, m)-DOT-$\binom{n}{1}$ scheme, for any subset $X \subseteq \{1, \ldots, m\}$, where $1 \leq |X| \leq k$, it holds that*

$$H(\mathbf{D}_X) \geq |X| \cdot H(\mathbf{W}).$$

Proof. Applying (35) and (39) of Appendix A, and Lemma 3.5, it holds that

$$\begin{aligned} H(\mathbf{D}_X) &\geq \sum_{\ell \in X} H(\mathbf{D}_\ell|\mathbf{D}_{X\setminus\{\ell\}}, \mathbf{D}_R) \\ &\geq |X| \cdot H(\mathbf{W}). \end{aligned}$$

■

The above theorem implies the following result:

- **Server Memory Storage.** Each Server S_j has to store at least $H(\mathbf{W})$ bits, since $H(\mathbf{D}_j) \geq H(\mathbf{W})$.

When we want to set up a cryptographic protocol we need random bits. This resource is usually referred to as the *randomness*. A detailed analysis of the randomness in distribution protocols can be found in [6]. The randomness of a scheme can be measured in different ways. Knuth and Yao [31] proposed the following approach: Let `Alg` be an algorithm that generates the probability distribution $P = \{p_1, \ldots, p_n\}$, using only independent and unbiased random bits. Denote by $T(\texttt{Alg})$ the average number of random bits used by `Alg` and let $T(\mathbf{P}) = \min_{\texttt{Alg}} T(\texttt{Alg})$. The value $T(\mathbf{P})$ is a measure of the average number of random bits needed to simulate the random source described by the probability distribution P. In [31] the following result was shown:

Theorem 3.7 $H(\mathbf{P}) \leq T(\mathbf{P}) < H(\mathbf{P}) + 2$.

Thus, the entropy of a random source is very close to the average number of unbiased random bits necessary to simulate the source. Hence, it is a natural measure of the randomness of a scheme. It is easy to see that the randomness needed to set up the m Servers can be lower bounded by $H(\mathbf{D}_1, \ldots, \mathbf{D}_m)$.

Theorem 3.6 also implies a lower bound on the randomness needed to set-up a (k, m)-DOT-$\binom{n}{1}$ scheme. More precisely:

- **Randomness.** In order to set up the scheme, the Sender needs at least $kH(\mathbf{W})$ random bits, since if $|X| = k$, then $H(\mathbf{D}_1, \ldots, \mathbf{D}_m) \geq H(\mathbf{D}_X) \geq kH(\mathbf{W})$.

Notice that Theorem 3.6 holds only for subsets X such that $1 \leq |X| \leq k$. For any X of size $|X| \geq k$, the bound stays the same (i.e., $H(\mathbf{D}_X) \geq kH(\mathbf{W})$).

The following lemma enables us to establish a lower bound on the complexity of each interaction Receiver-Servers.

Lemma 3.8 *In any correct and private (k, m)-DOT-$\binom{n}{1}$ scheme, for any subset of indices $X \subset \{1, \ldots, m\}$, where $1 \leq |X| \leq k-1$, for any index $j \notin X$, and for any $i = 1, \ldots, n$, it holds that*

$$H(\mathbf{C}_j|\mathbf{C}_X, \mathbf{D}_R, \mathbf{T} = i) \geq H(\mathbf{W}_i).$$

Proof. Let $Y \subset \{1, \ldots, m\}$, such that $|Y| = k - |X| - 1$, $j \notin Y$, and $X \cap Y = \emptyset$. The mutual information $I(\mathbf{W}_i; \mathbf{C}_j|\mathbf{C}_{X\cup Y}, \mathbf{D}_R, \mathbf{T} = i)$ can be written either as

$$H(\mathbf{W}_i|\mathbf{C}_{X\cup Y}, \mathbf{D}_R, \mathbf{T} = i) - H(\mathbf{W}_i|\mathbf{C}_{X\cup Y\cup\{j\}}, \mathbf{D}_R, \mathbf{T} = i)$$

or as

$$H(\mathbf{C}_j|\mathbf{C}_{X\cup Y}, \mathbf{D}_R, \mathbf{T} = i) - H(\mathbf{C}_j|\mathbf{C}_{X\cup Y}, \mathbf{D}_R, \mathbf{T} = i, \mathbf{W}_i).$$

Since from (32) of Appendix A, we get that $H(\mathbf{C}_j|\mathbf{C}_{X\cup Y}, \mathbf{D}_R, \mathbf{T} = i, \mathbf{W}_i) \geq 0$, it holds that

$$H(\mathbf{C}_j|\mathbf{C}_{X\cup Y}, \mathbf{D}_R, \mathbf{T} = i) \geq H(\mathbf{W}_i|\mathbf{C}_{X\cup Y}, \mathbf{D}_R, \mathbf{T} = i) - H(\mathbf{W}_i|\mathbf{C}_{X\cup Y\cup\{j\}}, \mathbf{D}_R, \mathbf{T} = i). \quad (15)$$

Setting $\mathbf{A} = \mathbf{W}_i$, $\mathbf{B} = \mathbf{C}_{X\cup Y}$, $\mathbf{C} = \mathbf{D}_{X\cup Y}$, and $\mathbf{D} = (\mathbf{D}_R, \mathbf{T} = i)$, due to condition (2) and Lemma 3.1, it follows that

$$H(\mathbf{W}_i|\mathbf{C}_{X\cup Y}, \mathbf{D}_R, \mathbf{T} = i) \geq H(\mathbf{W}_i|\mathbf{D}_{X\cup Y}, \mathbf{D}_R, \mathbf{T} = i).$$

Moreover, due to Lemma 3.3 and Lemma 3.2,

$$H(\mathbf{W}_i|\mathbf{D}_{X\cup Y}, \mathbf{D}_R, \mathbf{T} = i) = H(\mathbf{W}_i|\mathbf{D}_{X\cup Y}, \mathbf{D}_R, \mathbf{T}) = H(\mathbf{W}_i|\mathbf{D}_{X\cup Y}, \mathbf{D}_R) = H(\mathbf{W}_i).$$

Hence, $H(\mathbf{W}_i|\mathbf{C}_{X\cup Y}, \mathbf{D}_R, \mathbf{T} = i) \geq H(\mathbf{W}_i)$. Then, from Definition 2.1, we get that $H(\mathbf{W}_i|\mathbf{C}_{X\cup Y\cup\{j\}}, \mathbf{D}_R, \mathbf{T} = i) = 0$. Therefore, substituting the above inequality and equality in (15), it holds that

$$H(\mathbf{C}_j|\mathbf{C}_{X\cup Y}, \mathbf{D}_R, \mathbf{T} = i) \geq H(\mathbf{W}_i).$$

The result follows observing that (39) of Appendix A implies

$$H(\mathbf{C}_j|\mathbf{C}_X, \mathbf{D}_R, \mathbf{T} = i) \geq H(\mathbf{C}_j|\mathbf{C}_{X\cup Y}, \mathbf{D}_R, \mathbf{T} = i).$$

■

Notice that, as stated by condition (2), for any index $i \in \{1, \ldots, n\}$ and for any $X \subseteq \{1, \ldots, n\}$, it holds that $H(\mathbf{C}_X|\mathbf{D}_X, \mathbf{D}_R, \mathbf{T} = i) = 0$. Hence, the transcript is uniquely determined, i.e., there exists a function f such that $C_X = f(D_X, D_R, i)$. We could have stressed such a dependence by using a notation for the transcript like $C_{(X, D_R, i)}$. However, for any subset X of size at most $k-1$, it holds that $H(\mathbf{C}_X|\mathbf{T}) = H(\mathbf{C}_X)$. Indeed, due to property (39) of Appendix A and condition (5) of Definition 2.2, used in the special case in which $\overline{P}_X = P_X$, it holds that $H(\mathbf{T}) \geq H(\mathbf{T}|\mathbf{C}_X) \geq H(\mathbf{T}|\mathbf{C}_X, \mathbf{D}_X) = H(\mathbf{T})$. Hence, from property (33) of Appendix A, we get that

$$I(\mathbf{C}_X; \mathbf{T}) = H(\mathbf{C}_X) - H(\mathbf{C}_X|\mathbf{T}) = H(\mathbf{T}) - H(\mathbf{T}|\mathbf{C}_X) = 0.$$

Therefore,

$$H(\mathbf{C}_X|\mathbf{T}) = H(\mathbf{C}_X), \tag{16}$$

which means that any interaction C_X of the Receiver with any $k-1$ Servers could have been generated by any choice of a value $i \in T$.

Using the above lemma, we state the following theorem.

Theorem 3.9 *In any correct and private (k,m)-DOT-$\binom{n}{1}$ scheme, for any $X \subseteq \{1,\ldots,m\}$, where $1 \le |X| \le k$, and for any $i = 1,\ldots,n$, it holds that*

$$H(\mathbf{C}_X|\mathbf{T}=i) \ge |X| \cdot H(\mathbf{W}_i).$$

Proof. From (39) and (35) of Appendix A, and Lemma 3.8, it holds that

$$\begin{aligned} H(\mathbf{C}_X|\mathbf{T}=i) &\ge H(\mathbf{C}_X|\mathbf{D}_R,\mathbf{T}=i) \\ &\ge \sum_{\ell \in X} H(\mathbf{C}_\ell|\mathbf{C}_{X\setminus\{\ell\}},\mathbf{D}_R,\mathbf{T}=i) \\ &\ge |X| \cdot H(\mathbf{W}_i). \end{aligned}$$

■

Since condition (16) states that that the transcript C_X, as long as $1 \le |X| \le k-1$, is independent of i, the above bound, can be strengthened. Indeed, for any X such that $1 \le |X| \le k-1$, it results $H(\mathbf{C}_X) \ge |X| \cdot \max_i\{H(\mathbf{W}_i)\}$.

The above theorem implies the following results:

- **Interaction Receiver-Server.** The Receiver and a Server need to exchange at least $H(\mathbf{W}_i)$ bits, since $H(\mathbf{C}_j) \ge H(\mathbf{W}_i)$.
- **Interaction Receiver-Servers.** The Receiver and Servers S_X, where $|X| = k$, need to exchange at least $k \cdot H(\mathbf{W}_i)$ bits, since $H(\mathbf{C}_X|\mathbf{T}=i) \ge k \cdot H(\mathbf{W}_i)$.

Tightness of the Bounds. The lower bound on the randomness needed to set up a (k,m)-DOT-$\binom{n}{1}$, derived from Theorem 3.6, that is $H(\mathbf{D}_1,\ldots,\mathbf{D}_m) \ge kH(\mathbf{W})$, is tight since the protocol we give in Table 3 meets the bound by equality.

Distributed Oblivious Transfer (k,m)-DOT-$\binom{n}{r}$. An extended version of (k,m)-DOT-$\binom{n}{1}$, which we denote by (k,m)-DOT-$\binom{n}{r}$, enables the Receiver to recover, by interacting with a subset of k Servers at his own choosing, r secrets instead of a single one. Such a protocol can be defined by means of Definitions 2.1, 2.2, and 2.3 as well, by introducing a minor modification: Instead of a single index, the Receiver holds an r-tuple of indices, say $i = (i_1,\ldots,i_r)$. Therefore, $\mathbf{T}$ is a random variable taking values over T^r, and $\mathbf{W}_i$ is an r-tuple of random variables, representing an r-tuple of secrets the Receiver can recover. Therefore, the analysis we have done holds also for such an extension of the model, i.e., Theorems 3.6 and 3.9 apply.

4 Properties and Bounds for One-Round DOT

As we were claiming before, we show that with a one-round protocol a strong (k, m)-DOT-$\binom{n}{1}$ cannot be realized. First, notice that if the protocol is one-round, then the interaction between the Receiver and Server S_j is given by a query Q_j, sent by the Receiver, and an answer A_j, sent by S_j. Hence, for any $X \subseteq \{1, \ldots, m\}$, the transcript $C_X = (Q_X, A_X)$. Therefore, condition (3) becomes: for any subset $X \subseteq \{1, \ldots, m\}$,, and for any $i = 1, \ldots, n$, it holds that

$$H(\mathbf{Q}_X|\mathbf{D}_R, \mathbf{T} = i) = 0 \quad \text{and} \quad H(\mathbf{A}_X|\mathbf{Q}_X, \mathbf{D}_X) = 0. \tag{17}$$

Moreover, Definition 2.1 can be re-stated as follows:

Definition 4.1 *The sequence of programs $[S, P_1, \ldots P_m, R]$ is* correct *for one-round (k, m)-DOT-$\binom{n}{1}$ if, for any subset of k indices $X \subseteq \{1, \ldots, m\}$, and for any $i = 1, \ldots, n$, it holds that*

$$H(\mathbf{W}_i|\mathbf{Q}_X, \mathbf{A}_X, \mathbf{D}_R, \mathbf{T} = i) = 0. \tag{18}$$

Definition 2.2 can be restated along the same lines. For one-round schemes we prove that a single Server can help the Receiver to recover all the secrets, once the Receiver has legally retrieved the secret of her choice. The idea underlying the proof is the following: Because of condition (13), a set of $k - 1$ query-answer pairs, and the information held by the Receiver, do not give any information about the secret the Receiver is trying to recover. This property, along with Definition 4.1, implies that, given a sequence of $k - 1$ pairs, the k-th pair query-answer enables the recovering of *any* secret (otherwise, the sequence of $k-1$ query-answer pairs would leak partial information, i.e., that some secret cannot be reconstructed). Therefore, if the Receiver, after having legally recovered one secret, colludes with a single Server, using a subset of $k-1$ query-answer pairs from the transcript of the previous interaction, and a k-th pair, opportunely constructed with the help of the dishonest Server, can recover any other secret.

We assume that D_R, the bits used by the Receiver in an execution of her own program R, are truly random bits. However, the properties and results we prove hold even if a weaker assumption is satisfied: it is sufficient that the data D_X held by a set of servers S_X and D_R are statistically independent.

4.1 Properties of One-round Schemes

We show some properties which will be used in our proofs. We start by proving that the data D_X, held by a set of Servers S_X are independent from D_R, i, and the corresponding queries Q_X generated by the Receiver.

Lemma 4.2 *In any one-round (k, m)-DOT-$\binom{n}{1}$, for any $X \subseteq \{1, \ldots, m\}$, it holds that*

$$H(\mathbf{D}_X) = H(\mathbf{D}_X|\mathbf{Q}_X, \mathbf{D}_R, \mathbf{T}). \tag{19}$$

Proof. Due to property (38) of Appendix A, the mutual information $I(\mathbf{Q}_X; \mathbf{D}_X|\mathbf{D}_R, \mathbf{T})$ is equal to

$$H(\mathbf{Q}_X|\mathbf{D}_R, \mathbf{T}) - H(\mathbf{Q}_X|\mathbf{D}_X, \mathbf{D}_R, \mathbf{T}) = H(\mathbf{D}_X|\mathbf{D}_R, \mathbf{T}) - H(\mathbf{D}_X|\mathbf{Q}_X, \mathbf{D}_R, \mathbf{T}).$$

Condition (17) and property (39) of Appendix A, imply

$$0 = H(\mathbf{Q}_X|\mathbf{D}_R,\mathbf{T}) \geq H(\mathbf{Q}_X|\mathbf{D}_X,\mathbf{D}_R,\mathbf{T}) \geq 0.$$

Hence, it follows that $H(\mathbf{D}_X|\mathbf{D}_R,\mathbf{T}) = H(\mathbf{D}_X|\mathbf{Q}_X,\mathbf{D}_R,\mathbf{T})$. Moreover, D_R are truly random bits, and the index i, chosen by the Receiver, due to condition (1) is independent of D_X and D_R. Therefore, $H(\mathbf{D}_X) = H(\mathbf{D}_X|\mathbf{D}_R,\mathbf{T})$. ■

Notice that, if D_R are not truly random bits, the above lemma may not be true: the data D_X the Sender sends to Servers S_X and the data D_R, sent to the Receiver, might be related. Hence, in general $H(\mathbf{D}_X) \geq H(\mathbf{D}_X|\mathbf{Q}_X,\mathbf{D}_R,\mathbf{T})$. The protocol presented in Section 7 is an example of such a case.

Using techniques similar to the ones employed in proving the above lemma, we show that the answers generated by Servers S_X depend only on Q_X but not on D_R and i. More precisely:

Lemma 4.3 *In any one-round (k,m)-DOT-$\binom{n}{1}$, for any $X \subseteq \{1,\ldots,m\}$, it holds that*

$$H(\mathbf{A}_X|\mathbf{Q}_X) = H(\mathbf{A}_X|\mathbf{Q}_X,\mathbf{D}_R,\mathbf{T}). \tag{20}$$

Proof. Due to property (38) of Appendix A, the mutual information $I(\mathbf{A}_X\mathbf{D}_X|\mathbf{Q}_X)$ is equal to

$$H(\mathbf{A}_X|\mathbf{Q}_X) - H(\mathbf{A}_X|\mathbf{Q}_X,\mathbf{D}_X) = H(\mathbf{D}_X|\mathbf{Q}_X) - H(\mathbf{D}_X|\mathbf{Q}_X,\mathbf{A}_X).$$

Since, from condition (17), it holds that $H(\mathbf{A}_X|\mathbf{Q}_X,\mathbf{D}_X) = 0$, and Lemma 4.2 implies that $H(\mathbf{D}_X|\mathbf{Q}_X) = H(\mathbf{D}_X)$, it follows that

$$H(\mathbf{A}_X|\mathbf{Q}_X) = H(\mathbf{D}_X) - H(\mathbf{D}_X|\mathbf{Q}_X,\mathbf{A}_X). \tag{21}$$

On the other hand, due to property (38) of Appendix A, the mutual information $I(\mathbf{A}_X;\mathbf{Q}_X\mathbf{D}_X|\mathbf{D}_R,\mathbf{T})$ is equal to

$$H(\mathbf{A}_X|\mathbf{D}_R,\mathbf{T}) - H(\mathbf{A}_X|\mathbf{Q}_X,\mathbf{D}_X,\mathbf{D}_R,\mathbf{T}) = H(\mathbf{Q}_X,\mathbf{D}_X|\mathbf{D}_R,\mathbf{T}) - H(\mathbf{Q}_X,\mathbf{D}_X|\mathbf{D}_R,\mathbf{T},\mathbf{A}_X).$$

Hence, it follows that $H(\mathbf{A}_X|\mathbf{D}_R,\mathbf{T})$ is equal to

$$H(\mathbf{Q}_X,\mathbf{D}_X|\mathbf{D}_R,\mathbf{T}) - H(\mathbf{Q}_X,\mathbf{D}_X|\mathbf{D}_R,\mathbf{T},\mathbf{A}_X) + H(\mathbf{A}_X|\mathbf{Q}_X,\mathbf{D}_X,\mathbf{D}_R,\mathbf{T}). \tag{22}$$

Then, property (35) of Appendix A implies that

$$H(\mathbf{Q}_X,\mathbf{D}_X|\mathbf{D}_R,\mathbf{T}) = H(\mathbf{Q}_X|\mathbf{D}_R,\mathbf{T}) + H(\mathbf{D}_X|\mathbf{Q}_X,\mathbf{D}_R,\mathbf{T}),$$

and

$$H(\mathbf{Q}_X,\mathbf{D}_X|\mathbf{D}_R,\mathbf{T},\mathbf{A}_X) = H(\mathbf{Q}_X|\mathbf{D}_R,\mathbf{T},\mathbf{A}_X) + H(\mathbf{D}_X|\mathbf{Q}_X,\mathbf{D}_R,\mathbf{T},\mathbf{A}_X).$$

Therefore, using condition (17) and Lemma 4.2, from (22), it follows that

$$H(\mathbf{A}_X|\mathbf{D}_R,\mathbf{T}) = H(\mathbf{D}_X) - H(\mathbf{D}_X|\mathbf{Q}_X,\mathbf{D}_R,\mathbf{T},\mathbf{A}_X).$$

Moreover, since $H(\mathbf{Q}_X|\mathbf{D}_R,\mathbf{T}) = 0$, due to property (40) of Appendix A, it follows that $H(\mathbf{A}_X|\mathbf{D}_R,\mathbf{T}) = H(\mathbf{A}_X|\mathbf{Q}_X,\mathbf{D}_R,\mathbf{T})$. Hence,

$$H(\mathbf{A}_X|\mathbf{Q}_X,\mathbf{D}_R,\mathbf{T}) = H(\mathbf{D}_X) - H(\mathbf{D}_X|\mathbf{Q}_X,\mathbf{D}_R,\mathbf{T},\mathbf{A}_X). \tag{23}$$

At this point notice that, property (39) of Appendix A implies $H(\mathbf{A}_X|\mathbf{Q}_X) \geq H(\mathbf{A}_X|\mathbf{Q}_X, \mathbf{D}_R, \mathbf{T})$. Hence, from (21) and (23), it must be

$$H(\mathbf{D}_X|\mathbf{Q}_X, \mathbf{A}_X) \leq H(\mathbf{D}_X|\mathbf{Q}_X, \mathbf{D}_R, \mathbf{T}, \mathbf{A}_X).$$

Therefore, from property (39), we get that $H(\mathbf{D}_X|\mathbf{Q}_X, \mathbf{A}_X) = H(\mathbf{D}_X|\mathbf{Q}_X, \mathbf{D}_R, \mathbf{T}, \mathbf{A}_X)$, and it follows that

$$H(\mathbf{A}_X|\mathbf{Q}_X) = H(\mathbf{A}_X|\mathbf{Q}_X, \mathbf{D}_R, \mathbf{T}).$$

■

Hence, let $X \subset \{1, \ldots, m\}$ be a subset of size $k-1$. Lemma 4.3 implies that the answers A_X depend only on Q_X. Moreover, equality (16) implies that,

$$H(\mathbf{Q}_X|\mathbf{T}) = H(\mathbf{Q}_X). \tag{24}$$

Therefore, because of Lemma 4.3 and equality (24), any sequence (A_X, Q_X), obtained by interacting with the Servers in X holding data D_X, can be generated *for any* index i, by choosing a corresponding appropriate string D_R.

Using the above results, we show the following:

Theorem 4.4 *In any one-round protocol for (k,m)-DOT-$\binom{n}{1}$, for any subset of $k-1$ indices $X \subset \{1, \ldots, m\}$, for any sequence of possible queries Q_X and corresponding answers A_X, and for any $j \notin X$, an adversary, given only D_j and (Q_X, A_X), can compute all the secrets.*

Proof. For any $\ell = 1, \ldots, n$, an adversary can retrieve secret w_ℓ, in three steps as follows:

- *Computation of the queries.* He computes a string D_R and a query Q'_j such that the k queries $Q'_{X\cup\{j\}}$, which could be generated by the Receiver by using D_R and ℓ as inputs to her program R, satisfy the condition $Q'_X = Q_X$. Due to property (24) a string D_R for which the above condition holds can always be found.
- *Computation of the answers.* Then, he computes the answers $A'_{X\cup\{j\}}$ to $Q'_{X\cup\{j\}}$. He does not need the data D_X, held by Servers S_X, to compute the answers to $Q'_X = Q_X$ since $A'_X = A_X$. Indeed, due to Lemma 4.3, the answers do not depend directly on D_R and ℓ but only on Q'_X. Moreover, due to condition (17), using D_j, he computes an answer A'_j to the k-th query Q'_j.
- *Computation of the secret w_ℓ.* Finally, using $A'_{X\cup\{j\}}, Q'_{X\cup\{j\}}$, D_R and ℓ, he computes the secret w_ℓ. Indeed, from Definition 4.1, it follows that

$$H(\mathbf{W}_\ell|\mathbf{A}_{X\cup\{j\}} = A'_{X\cup\{j\}}, \mathbf{Q}_{X\cup\{j\}} = Q'_{X\cup\{j\}}, \mathbf{D}_R = D_R, \mathbf{T} = \ell) = 0.$$

■

A consequence of this impossibility result for one-round protocols is that the highest privacy level sought for in [36] with this approach cannot be achieved.

Remark. It is possible to show that, if conditions (5), (6), and (11) of Definitions 2.2 and 2.3 are weakened and we require that they must hold, in the threshold case, only against a coalition of Servers S_X such that $|X| \leq t$, for $t < k$, then an adversary, for any subset of $k-t$

Servers S_Y such that $Y \cap X = \emptyset$, given D_Y and (Q_X, A_X), can compute all the secrets. This extension of Theorem 4.4 is quite straightforward.

In our model, we have made no assumption on the probability distribution on the sequence of secrets w. Usually the secrets held by the Sender are independent. However, the results we have shown hold even if dependencies are present. With the following lemma, we show that, as long as for any i, j, where $i \neq j$, $H(\mathbf{W}_i|\mathbf{W}_j) > 0$, a sequence of k queries determines $\mathbf{T}$ *uniquely*. On the other hand notice that, if $H(\mathbf{W}_i|\mathbf{W}_j) = 0$, then w_i is a function of w_j. Hence, once w_j is known, w_i can be computed. In such a case, the value of the index i is not uniquely determined by k queries. Actually, we can say more. If some secrets imply other secrets, then the Receiver, in order to retrieve secrets, can consider a smaller subset of indices, by taking into account all implications. This case has no interest in the traditional oblivious transfer context, since there is no way to avoid that a Receiver, once recovered w_j, using the a-priori knowledge about the relations among the secrets, computes also w_i. Hence, we will not go further in our analysis along this line. In what follows we assume that for any i, j, where $i \neq j$, the entropy $H(\mathbf{W}_i|\mathbf{W}_j) > 0$, i.e., secrets might be related but implications are not present, and we say that the sequence of secrets is *implication-free*.

The idea behind the proof that as long as secrets are implication-free then a sequence of k queries determines $\mathbf{T}$ *uniquely*, is the following: if two indices, along with suitably chosen random strings, determine the same k-tuple of queries, since the answers depend only on the queries, the Receiver computes two different secrets. But such a possibility is excluded by condition (7) of Definition 2.2.

Lemma 4.5 *In any correct and private one-round (k, m)-DOT-$\binom{n}{1}$ scheme, if the sequence of secrets is implication-free, then for any subset $X \subseteq \{1, \ldots, m\}$ of k indices, it holds that*

$$H(\mathbf{T}|\mathbf{Q}_X) = 0. \tag{25}$$

Proof. For any $i = 1, \ldots, n$, condition (17) states that $H(\mathbf{Q}_X|\mathbf{D}_R, \mathbf{T} = i) = 0$. Hence, the sequence of queries Q_X is function only of D_R and i. Assume that there exist two possible pairs (D_{R_1}, i_1) and (D_{R_2}, i_2), where $i_1 \neq i_2$, for which the Receiver's program produces as output queries Q_X. Then, Lemma 4.3 and Definition 4.1 imply that

$$H(\mathbf{W}_{i_1}|\mathbf{A}_X, \mathbf{Q}_X = Q_X, \mathbf{D}_R = D_{R_1}, \mathbf{T} = i_1) = 0$$

and

$$H(\mathbf{W}_{i_2}|\mathbf{A}_X, \mathbf{Q}_X = Q_X, \mathbf{D}_R = D_{R_2}, \mathbf{T} = i_2) = 0.$$

Hence, due to Lemma 3.1, setting $\mathbf{A} = \mathbf{W}$, $\mathbf{B} = \mathbf{W}_{i_2}$, $\mathbf{C} = (\mathbf{A}_X, \mathbf{Q}_X = Q_X, \mathbf{D}_R = D_{R_2}, \mathbf{T} = i_2)$, and $\mathbf{D} = \emptyset$, it holds that

$$H(\mathbf{W}|\mathbf{T} = i_2, \mathbf{D}_R = D_{R_2}, \mathbf{A}_X, \mathbf{Q}_X = Q_X, \mathbf{W}_{i_1}) \leq H(\mathbf{W}|\mathbf{W}_{i_2}, \mathbf{W}_{i_1}). \tag{26}$$

Due to condition (7) of Definition 2.2, it holds

$$H(\mathbf{W}|\mathbf{T} = i_2, \mathbf{D}_R = D_{R_2}, \mathbf{A}_X, \mathbf{Q}_X = Q_X, \mathbf{W}_{i_1}) = H(\mathbf{W}|\mathbf{W}_{i_1}). \tag{27}$$

Indeed, the equality follows by considering an adversary who uses a program $\overline{R}$ defined as follows: on input i_2 and D_{R_2}, the program $\overline{R}$ ignores i_2 and behaves honestly in order to retrieve w_{i_1}, using D_{R_2} as random string. Hence, $\widetilde{i} = f(i_2, D_{R_2}, \overline{R}) = i_1$.

Therefore, from inequality (26) and equality (27), it follows that

$$H(\mathbf{W}|\mathbf{W}_{i_1}) \le H(\mathbf{W}|\mathbf{W}_{i_1}, \mathbf{W}_{i_2}). \tag{28}$$

Moreover, property (34) of Appendix A implies that

$$\begin{aligned} H(\mathbf{W}|\mathbf{W}_{i_1}) &= H(\mathbf{W}_{i_2}|\mathbf{W}_{i_1}) + H(\mathbf{W} \setminus \mathbf{W}_{i_2}|\mathbf{W}_{i_1}, \mathbf{W}_{i_2}) \\ &= H(\mathbf{W}_{i_2}|\mathbf{W}_{i_1}) + H(\mathbf{W}|\mathbf{W}_{i_1}, \mathbf{W}_{i_2}). \end{aligned}$$

Hence, inequality (28) holds only if $H(\mathbf{W}_{i_2}|\mathbf{W}_{i_1}) = 0$. But since the sequence of secrets is implication-free, this is clearly a contradiction. Therefore, a sequence of k queries uniquely determines the index of the secret. Hence, $H(\mathbf{T}|\mathbf{Q}_X) = 0$. ∎

4.2 Bounds for One-round Schemes

We show some bounds on the size of the queries, on the size of the answers, and on the randomness the Receiver needs to construct the queries for the Servers.

The first lemma shows that a query, given any sequence of at most $k-1$ other queries, can still determine any index.

Lemma 4.6 *In any correct and private one-round (k,m)-DOT-$\binom{n}{1}$ scheme, if the sequence of secrets is implication-free, then for any subset of indices $X \subset \{1,\ldots,m\}$, where $1 \le |X| \le k-1$, and for any $j \notin X$, it holds that*

$$H(\mathbf{Q}_j|\mathbf{Q}_X) \ge H(\mathbf{T}).$$

Proof. Let $Y \subset \{1,\ldots,m\}$, such that $|Y| = k - |X| - 1$, $j \notin Y$, and $X \cap Y = \emptyset$. Notice that, due to property (38) of Appendix A, $I(\mathbf{Q}_j; \mathbf{T}|\mathbf{Q}_{X\cup Y})$ is equal to

$$H(\mathbf{Q}_j|\mathbf{Q}_{X\cup Y}) - H(\mathbf{Q}_j|\mathbf{Q}_{X\cup Y}, \mathbf{T}) = H(\mathbf{T}|\mathbf{Q}_{X\cup Y}) - H(\mathbf{T}|\mathbf{Q}_{X\cup Y}, \mathbf{Q}_j).$$

Hence,

$$H(\mathbf{Q}_j|\mathbf{Q}_{X\cup Y}) = H(\mathbf{T}|\mathbf{Q}_{X\cup Y}) - H(\mathbf{T}|\mathbf{Q}_{X\cup Y}, \mathbf{Q}_j) + H(\mathbf{Q}_j|\mathbf{Q}_{X\cup Y}, \mathbf{T}).$$

Since condition (24) states that $H(\mathbf{T}|\mathbf{Q}_{X\cup Y}) = H(\mathbf{T})$, Lemma 4.5 proves that $H(\mathbf{T}|\mathbf{Q}_{X\cup Y}, \mathbf{Q}_j) = 0$, and property (32) establishes that $H(\mathbf{Q}_j|\mathbf{Q}_{X\cup Y}, \mathbf{T}) \ge 0$, applying property (39), it follows that

$$H(\mathbf{Q}_j|\mathbf{Q}_X) \ge H(\mathbf{Q}_j|\mathbf{Q}_{X\cup Y}) \ge H(\mathbf{T}).$$

∎

Using the above lemma, we show a lower bound on the size of k queries in terms of the uncertainty about $\mathbf{T}$.

Theorem 4.7 *In any correct and private one-round (k,m)-DOT-$\binom{n}{1}$ scheme, if the sequence of secrets is implication-free, then for any subset $X \subseteq \{1,\ldots,m\}$, where $1 \le |X| \le k$, it results*

$$H(\mathbf{Q}_X) \ge |X| \cdot H(\mathbf{T}).$$

Proof. Notice that

$$\begin{aligned} H(\mathbf{Q}_X) &\geq \sum_{j\in X} H(\mathbf{Q}_j|\mathbf{Q}_{X\setminus\{j\}}) \text{ (due to properties (35) and (34))} \\ &\geq |X|\cdot H(\mathbf{T}) \text{ (due to Lemma 4.6).} \end{aligned}$$

■

The following lemma shows that the amount of information provided by any answer sent by a Server, given any other $k-1$ answers, queries, random bits used by the Receiver and the chosen index, is greater than $H(\mathbf{W}_i)$.

Lemma 4.8 *In any correct and private one-round (k,m)-DOT-$\binom{n}{1}$ scheme, if the sequence of secrets is implication-free, then for any subset $X \subset \{1,\ldots,m\}$, where $1 \leq |X| \leq k-1$, for any $j \notin X$, and for any $i = 1,\ldots,n$, it holds that*

$$H(\mathbf{A}_j|\mathbf{A}_X, \mathbf{Q}_X, \mathbf{D}_R, \mathbf{T}=i) \geq H(\mathbf{W}_i).$$

Proof. Let $Y \subset \{1,\ldots,m\}$, such that $|Y| = k-|X|-1$, $j \notin Y$, and $X \cap Y = \emptyset$. Let us denote by $\mathbf{V} = (\mathbf{Q}_{X\cup Y\cup\{j\}}, \mathbf{D}_R, \mathbf{T}=i)$. From property (38) of Appendix A, the mutual information $I(\mathbf{A}_j;\mathbf{W}_i|\mathbf{A}_{X\cup Y},\mathbf{V})$ can be written as

$$H(\mathbf{A}_j|\mathbf{A}_{X\cup Y},\mathbf{V}) - H(\mathbf{A}_j|\mathbf{A}_{X\cup Y},\mathbf{W}_i,\mathbf{V})$$

or as

$$H(\mathbf{W}_i|\mathbf{A}_{X\cup Y},\mathbf{V}) - H(\mathbf{W}_i|\mathbf{A}_{X\cup Y},\mathbf{A}_j,\mathbf{V}).$$

Hence, $H(\mathbf{A}_j|\mathbf{A}_{X\cup Y},\mathbf{V})$ is equal to

$$H(\mathbf{W}_i|\mathbf{A}_{X\cup Y},\mathbf{V}) - H(\mathbf{W}_i|\mathbf{A}_{X\cup Y},\mathbf{A}_j,\mathbf{V}) + H(\mathbf{A}_j|\mathbf{A}_{X\cup Y},\mathbf{W}_i,\mathbf{V}).$$

Due to Definition 4.1, $H(\mathbf{W}_i|\mathbf{A}_{X\cup Y},\mathbf{A}_j,\mathbf{V}) = 0$ and because of property (32), $H(\mathbf{A}_j|\mathbf{A}_{X\cup Y},\mathbf{W}_i,\mathbf{V}) \geq 0$. Moreover, since $H(\mathbf{Q}_j|\mathbf{D}_R,\mathbf{T}=i) = 0$, applying condition (13), it follows that

$$H(\mathbf{W}_i|\mathbf{A}_{X\cup Y},\mathbf{V}) = H(\mathbf{W}_i|\mathbf{A}_{X\cup Y},\mathbf{Q}_{X\cup Y},\mathbf{D}_R,\mathbf{T}=i) \geq H(\mathbf{W}_i).$$

Therefore, applying property (39), we get

$$H(\mathbf{A}_j|\mathbf{A}_X,\mathbf{Q}_X,\mathbf{D}_R,\mathbf{T}=i) \geq H(\mathbf{A}_j|\mathbf{A}_{X\cup Y},\mathbf{V}) \geq H(\mathbf{W}_i).$$

■

Using the above lemma we show a lower bound on the size of the answers sent by a subset S_X of Servers.

Theorem 4.9 *In any correct and private one-round (k,m)-DOT-$\binom{n}{1}$ scheme, if the sequence of secrets is implication-free, then for any subset $X \subseteq \{1,\ldots,m\}$, where $1 \leq |X| \leq k$, and for any $i = 1,\ldots,n$, it holds that*

$$H(\mathbf{A}_X|\mathbf{Q}_X,\mathbf{T}=i) \geq |X|\cdot H(\mathbf{W}_i).$$

Proof. Notice that

$$\begin{aligned}
H(\mathbf{A}_X|\mathbf{Q}_X, \mathbf{T}=i) &\geq \sum_{j\in X} H(\mathbf{A}_j|\mathbf{Q}_X, \mathbf{A}_{X\setminus\{j\}}, \mathbf{T}=i) \\
&\quad \text{(due to properties (35) and (34))} \\
&\geq \sum_{j\in X} H(\mathbf{A}_j|\mathbf{Q}_X, \mathbf{A}_{X\setminus\{j\}}, \mathbf{D}_R = D_R, \mathbf{T}=i) \\
&\quad \text{(due to property (34))} \\
&= \sum_{j\in X} H(\mathbf{A}_j|\mathbf{Q}_{X\setminus\{j\}}, \mathbf{A}_{X\setminus\{j\}}, \mathbf{D}_R = D_R, \mathbf{T}=i) \\
&\quad \text{(since } H(\mathbf{Q}_j|\mathbf{D}_R = D_R, \mathbf{T}=i) = 0\text{)} \\
&\geq |X| \cdot H(\mathbf{W}_i) \text{ (due to Lemma 4.8).}
\end{aligned}$$

■

Using the above results, we show a lower bound on the size of both answers and queries. More precisely, we prove that:

Theorem 4.10 *In any correct and private one-round (k, m)-DOT-$\binom{n}{1}$ scheme, if the sequence of secrets is implication-free, then for any subset $X \subseteq \{1, \ldots, m\}$, where $1 \leq |X| \leq k-1$, and for any $i = 1, \ldots, n$, it holds that*

$$H(\mathbf{A}_X, \mathbf{Q}_X|\mathbf{T}=i) \geq |X| \cdot (H(\mathbf{T}) + H(\mathbf{W}_i)).$$

Proof. Notice that,

$$\begin{aligned}
H(\mathbf{A}_X, \mathbf{Q}_X|\mathbf{T}=i) &= H(\mathbf{Q}_X|\mathbf{T}=i) + H(\mathbf{A}_X|\mathbf{Q}_X, \mathbf{T}=i) \text{ (due to property (34))} \\
&= H(\mathbf{Q}_X) + H(\mathbf{A}_X|\mathbf{Q}_X, \mathbf{T}=i) \text{ (due to condition (24))} \\
&\geq |X| \cdot H(\mathbf{T}) + |X| \cdot H(\mathbf{W}_i) \text{ (due to Theorem 4.7 and Theorem 4.9)} \\
&= |X| \cdot (H(\mathbf{T}) + H(\mathbf{W}_i)).
\end{aligned}$$

■

Notice that, as we have already argued before, condition (16) implies that, as long as $1 \leq |X| \leq k-1$, any pair (A_X, Q_X) is independent of i. Hence, the above bound can be strengthened. More precisely, for any X such that $1 \leq |X| \leq k-1$, it follows that

$$H(\mathbf{A}_X, \mathbf{Q}_X) \geq |X| \cdot (H(\mathbf{T}) + \max_i\{H(\mathbf{W}_i)\}).$$

Moreover, if $|X| = k$, along the same line of the previous proof, it is easy to show that, for any $i = 1, \ldots, n$,

$$H(\mathbf{A}_X, \mathbf{Q}_X|\mathbf{T}=i) \geq kH(\mathbf{W}_i) + (k-1) \cdot H(\mathbf{T}).$$

Notice that Theorem 4.10 improves the lower bound given by Theorem 3.9 for general DOT schemes.

Finally, we show a lower bound on the randomness the Receiver needs to generate the queries in order to retrieve a certain secret.

Theorem 4.11 *In any correct and private one-round (k, m)-DOT-$\binom{n}{1}$ scheme, if the sequence of secrets is implication-free, then it results*

$$H(\mathbf{D}_R) \geq (k-1)H(\mathbf{T}).$$

Proof. Let $X = \{j_1, \ldots, j_k\} \subseteq \{1, \ldots, m\}$ be a subset of k indices. First notice that, from (38) of Appendix A,

$$\begin{aligned} I(\mathbf{D}_R; \mathbf{Q}_X | \mathbf{T}) &= H(\mathbf{D}_R|\mathbf{T}) - H(\mathbf{D}_R|\mathbf{Q}_X, \mathbf{T}) \\ &= H(\mathbf{Q}_X|\mathbf{T}) - H(\mathbf{Q}_X|\mathbf{D}_R, \mathbf{T}). \end{aligned}$$

From condition (17), we get that $H(\mathbf{Q}_X|\mathbf{D}_R, \mathbf{T}) = 0$, and, from (32) of Appendix A, we get $H(\mathbf{D}_R|\mathbf{Q}_X, \mathbf{T}) \geq 0$. It follows that

$$H(\mathbf{D}_R|\mathbf{T}) \geq H(\mathbf{Q}_X|\mathbf{T}). \tag{29}$$

Moreover, from (39) and (35) of Appendix A, we get that

$$H(\mathbf{Q}_X|\mathbf{T}) \geq H(\mathbf{Q}_{X\setminus\{j_k\}}|\mathbf{T}) = \sum_{\ell=1}^{k-1} H(\mathbf{Q}_{j_\ell}|\mathbf{Q}_{j_1}, \ldots, \mathbf{Q}_{j_{\ell-1}}, \mathbf{T}). \tag{30}$$

On the other hand, from (38) of Appendix A, denoting by $Y_\ell = \{j_1, \ldots, j_{\ell-1}\}$, we get

$$\begin{aligned} I(\mathbf{T}; \mathbf{Q}_{j_\ell}|\mathbf{Q}_{Y_\ell}) &= H(\mathbf{Q}_{j_\ell}|\mathbf{Q}_{Y_\ell}) - H(\mathbf{Q}_{j_\ell}|\mathbf{Q}_{Y_\ell}, \mathbf{T}) \\ &= H(\mathbf{T}|\mathbf{Q}_{Y_\ell}) - H(\mathbf{T}|\mathbf{Q}_{Y_{\ell+1}}), \end{aligned}$$

from which it follows that

$$H(\mathbf{Q}_{j_\ell}|\mathbf{Q}_{Y_\ell}, \mathbf{T}) = H(\mathbf{Q}_{j_\ell}|\mathbf{Q}_{Y_\ell}) - H(\mathbf{T}|\mathbf{Q}_{Y_\ell}) + H(\mathbf{T}|\mathbf{Q}_{Y_{\ell+1}}).$$

Moreover, in any one-round (k, m)-DOT-$\binom{n}{1}$, from condition (24) and property (33), for $\ell = 1, \ldots, k$, it follows that $H(\mathbf{T}|\mathbf{Q}_{Y_\ell}) = H(\mathbf{T})$. Therefore, for $\ell = 1, \ldots, k-1$, $H(\mathbf{T}|\mathbf{Q}_{Y_\ell}) = H(\mathbf{T}|\mathbf{Q}_{Y_{\ell+1}}) = H(\mathbf{T})$. Hence, for $\ell = 1, \ldots, k-1$,

$$H(\mathbf{Q}_{j_\ell}|\mathbf{Q}_{Y_\ell}, \mathbf{T}) = H(\mathbf{Q}_{j_\ell}|\mathbf{Q}_{Y_\ell}). \tag{31}$$

Moreover, due to Lemma 4.6, for $\ell = 1, \ldots, k-1$, $H(\mathbf{Q}_{j_\ell}|\mathbf{Q}_{Y_\ell}) \geq H(\mathbf{T})$. Therefore, from (29), (30) and (31), it results

$$H(\mathbf{D}_R|\mathbf{T}) \geq \sum_{\ell=1}^{k-1} H(\mathbf{Q}_{j_\ell}|\mathbf{Q}_{Y_\ell}, \mathbf{T}) \geq \sum_{\ell=1}^{k-1} H(\mathbf{Q}_{j_\ell}|\mathbf{Q}_{Y_\ell}) \geq (k-1)H(\mathbf{T}).$$

Hence, applying (34) of Appendix A, we get

$$H(\mathbf{D}_R) \geq H(\mathbf{D}_R|\mathbf{T}) \geq (k-1)H(\mathbf{T}).$$

■

TIGHTNESS OF THE BOUND. Notice that the above lower bound is tight. Indeed, the (one-round) combinatorial constructions we will present in Section 6, meet the bound by equality.

5 One-Round Protocols Based on Polynomial Interpolation

Two one-round protocols for (k,m)-DOT-$\binom{2}{1}$ have been proposed[2] in [34]. The first one uses *sparse* bivariate polynomials. The second one uses *fully* bivariate polynomials. Both constructions of (k,m)-DOT-$\binom{2}{1}$ use, as a building block, a sub-protocol from which a dishonest Receiver can infer at most a linear combination of the secrets held by the Sender. The (k,m)-DOT-$\binom{2}{1}$ protocol is then obtained by composing in a certain way multiple instances of the sub-protocol. The general structure of the sub-protocol is given in Table 1.

Structure of the sub-protocols used in the design of one-round (k,m)-DOT-$\binom{2}{1}$ in [34].
Let $w_0, w_1 \in F_p$ be $\mathcal{S}$'s secrets, and let $i \in \{0,1\}$ be $\mathcal{R}$'s choice.

Set-up Phase.

- The Sender $\mathcal{S}$ generates a bivariate polynomial $Q(x,y)$ with values in F_p such that $Q(0,0) = w_0$, and $Q(0,1) = w_1$.
- Then, for $j = 1,\ldots,m$, $\mathcal{S}$ sends the univariate polynomial $Q(j,\cdot)$ to Server $\mathcal{S}_j$.

Oblivious Transfer Phase.

- The Receiver $\mathcal{R}$ chooses a random polynomial Z such that $Z(0) = i$, and defines a univariate polynomial V to be $V(x) = Q(x, Z(x))$ such that the degree of V is $k-1$.
- Then, the Receiver $\mathcal{R}$ chooses a subset $X \subseteq \{1,\ldots,m\}$ of k indices and, for every $j \in X$, sends to Server $\mathcal{S}_j$ the value $Z(j)$, and receives from $\mathcal{S}_j$ the value $V(j) = Q(j, Z(j))$.
- After having received the k values $V(j)$, for $j \in X$, the Receiver $\mathcal{R}$ interpolates V and computes $V(0)$.

Table 1: The structure of the sub-protocol

In this section we describe one-round (k,m)-DOT-$\binom{n}{1}$ oblivious transfer protocols, which generalize and strengthen the one-round (k,m)-DOT-$\binom{2}{1}$ protocols proposed in [34]. We assume that $1 < k \leq m$, and implement our protocols over the finite field F_p, where $p > \max\{m,n\}$ is prime. In Table 2 we describe the sub-protocol used in the design of the one-round (k,m)-DOT-$\binom{n}{1}$ oblivious transfer protocol, which generalizes and strengthens the first one-round (k,m)-DOT-$\binom{2}{1}$ protocol. Then, we show how to compose such a sub-protocol in order to set up a (k,m)-DOT-$\binom{n}{1}$, and we exhibit a proof of correctness and privacy of the overall construction. Along the same line, in Table 4, we describe the sub-protocol used in the design of a *t-private* one-round oblivious transfer protocol (a notion we will define later on), which generalizes the second distributed oblivious transfer protocol. Due to the similarity of the strategy to construct such a scheme with the strategy to set up the first one, we will only sketch the description of the full scheme, resulting by composing multiple instances of the sub-protocol.

[2]Notice that, a (k,m)-DOT-$\binom{2}{1}$ can be used as a black box to set up "more complex" oblivious transfer protocols in the same distributed model (see [22, 18, 10] for unconditionally secure reductions). In this case, any improvement in the design of the available (k,m)-DOT-$\binom{2}{1}$, implies directly an improvement of the performance of the more complex protocols.

Let us start by analyzing the sub-protocol to set up a (k,m)-DOT-$\binom{n}{1}$ (see Table 2).

A Sub-Protocol for one-round (k,m)-DOT-$\binom{n}{1}$.
Let $w_0, w_1, \ldots, w_{n-1} \in F_p$ be $\mathcal{S}$'s secrets, and let $i \in \{0, \ldots, n-1\}$ be $\mathcal{R}$'s choice.

Set-up Phase.

- The Sender $\mathcal{S}$ generates independently and uniformly at random values $a_1, \ldots, a_{k-1}, r_1, \ldots, r_{n-1} \in F_p$. Then, he sets up an univariate polynomial $a(x) = \sum_{j=0}^{k-1} a_j x^j$, where $a_0 = w_0$, and an n-variate polynomial

$$Q(x, y_1, \ldots, y_{n-1}) = a(x) + b_1 y_1 + \cdots + b_{n-1} y_{n-1},$$

  where $b_i = r_i w_i - w_0$, for $i = 1, \ldots, n-1$. It follows that $Q(0, 0, \ldots, 0) = w_0, Q(0, 1, 0, \ldots, 0) = r_1 w_1, \ldots, Q(0, 0, \ldots, 1) = r_{n-1} w_{n-1}$.
- Then, for $\ell = 1, \ldots, n-1$, he shares independently r_ℓ, according to a Shamir's (k,m) threshold secret sharing scheme. Let r_ℓ^j, for $j = 1, \ldots, m$, the corresponding shares. For $j = 1, \ldots, m$, the Sender $\mathcal{S}$ sends the $(n-1)$-variate polynomial $Q(j, y_1, \ldots, y_{n-1})$ and the shares $r_1^j, \ldots, r_{n-1}^j$ to Server $\mathcal{S}_j$.

Oblivious Transfer Phase.

- The Receiver $\mathcal{R}$ constructs $n-1$ polynomials, $Z_1(x), \ldots, Z_{n-1}(x)$, of degree $k-1$, in such a way that $(Z_1(0), \ldots, Z_{n-1}(0))$ is an $(n-1)$-tuple of zeroes if the Receiver $\mathcal{R}$ is interested in w_0, i.e., $i = 0$, or an $(n-1)$-tuple of zeroes and a single 1 in position i, if the Receiver $\mathcal{R}$ is interested in w_i, i.e., $i \in \{1, \ldots, n-1\}$. The remaining coefficients of $Z_1(x), \ldots, Z_{n-1}(x)$ are chosen independently and uniformly at random in F_p.
- Then, the Receiver $\mathcal{R}$ chooses a subset $X \subseteq \{1, \ldots, m\}$ of k indices and, for every $j \in X$, sends to Server $\mathcal{S}_j$ the values $Z_1(j), \ldots, Z_{n-1}(j)$ and receives the value $V(j) = Q(j, Z_1(j), \ldots, Z_{n-1}(j))$, and all the shares $r_1^j, \ldots, r_{n-1}^j$.
- After having received the k values $V(j)$, for $j \in X$, the Receiver $\mathcal{R}$ interpolates a univariate polynomial $V(x) = Q(x, Z_1(x), \ldots, Z_{n-1}(x))$ of degree $k-1$, and computes $V(0)$ if $i = 0$, or $V(0)/r_i$, if $i \in \{1, \ldots, n-1\}$, where r_i is reconstructed through the shares r_i^j's.

Table 2: A sub-protocol for one-round (k,m)-DOT-$\binom{n}{1}$.

From the description given in Table 2, it is easy to see that condition (17) is satisfied. Indeed, every query Q_j is uniquely determined by the index of the secret chosen by the Receiver and her random values, as well as every answer A_j is uniquely determined by the query Q_j and the data D_j held by S_j.

Correctness. We show that the sub-protocol given in Table 2 satisfies Definition 4.1.
For $\ell = 1, \ldots, n-1$, let $Z_\ell(x) = \sum_{j=0}^{k-1} z_\ell^j x^j$ be the polynomial generated by $\mathcal{R}$, where z_ℓ^j, for $j = 1, \ldots, k-1$ are random values. The polynomial $V(x)$ interpolated by $\mathcal{R}$

$$V(x) = Q(x, Z_1(x), \ldots, Z_{n-1}(x))$$

can be written in explicit form as

$$\sum_{j=1}^{k-1} a_j x^j + a_0 + b_1(z_1^0 + \sum_{j=1}^{k-1} z_1^j x^j) + \cdots + b_{n-1}(z_{n-1}^0 + \sum_{j=1}^{k-1} z_{n-1}^j x^j)$$

which can be re-arranged as

$$\sum_{j=1}^{k-1}(a_j + b_1 z_1^j + \cdots + b_{n-1} z_{n-1}^j) x^j + a_0 + b_1 z_1^0 + \cdots + b_{n-1} z_{n-1}^0.$$

For $x = 0$, the polynomial becomes $V(0) = a_0 + b_1 z_1^0 + \cdots + b_{n-1} z_{n-1}^0$. If $(z_1^0, \ldots, z_{n-1}^0) = (0, \ldots, 0)$, then $V(0) = a_0 = w_0$. On the other hand, if $(z_1^0, \ldots, z_{n-1}^0) = (0, \ldots, 1, \ldots, 0)$ where 1 is in position i, for a certain $i \in \{1, \ldots, n-1\}$), then $V(0) = b_i - a_0 = r_i w_i$. From the k shares r_i^j, where $j \in X$, she reconstructs r_i. Therefore, $V(0)/r_i$ is exactly the desired secret, that is, w_i.

Privacy. About the privacy property, stated by Definition 2.2, notice that:

- Condition (5) is satisfied due to the degree of the polynomials chosen by the Receiver. Indeed, a coalition of $k-1$ Servers, say S_X, where $X = \{1, \ldots, k-1\}$, contacted by $\mathcal{R}$, gets, for each $j = 1, \ldots, n-1$, only $k-1$ points of the polynomial $Z_j(x)$. Therefore, for any possible choice of $Z_j(0) \in \{0, 1\}$, the coalition interpolates a different and *unique* polynomial $Z_j(x)$ of degree k, which agrees with the $k-1$ received values. Since, for $j = 1, \ldots, n-1$, all coefficients of $Z_j(x)$ but $Z_j(0)$ are chosen independently and uniformly at random, for any $(k-1)$-tuple of values $Z_j(1), \ldots, Z_j(k-1)$ and for any index $i \in \{0, \ldots n-1\}$ chosen by the Receiver, it holds that,

  $$Prob(Z_j(1), \ldots, Z_j(k-1)|i) = \frac{1}{p^{k-1}}.$$

  Denote with z the $n-1$ sequences of $k-1$ values $Z_j(1), \ldots, Z_j(k-1)$, for $j = 1, \ldots, n-1$. Then, for any index $i \in \{0, \ldots n-1\}$ chosen by the Receiver, there exists a *unique* sequence of $(n-1)$ polynomials interpolating z. Hence, it holds that $Prob(z|i) = \frac{1}{p^{(n-1)(k-1)}}$. Applying Bayes' theorem, we have

  $$\begin{aligned} Prob(i|z) &= \frac{Prob(i) \cdot Prob(z|i)}{\sum_{j \in \{0,\ldots,n-1\}} Prob(j) \cdot Prob(z|j)} \\ &= \frac{Prob(i) \cdot 1/p^{(n-1)(k-1)}}{\sum_{j \in \{0,\ldots,n-1\}} Prob(j) \cdot 1/p^{(n-1)(k-1)}} \\ &= \frac{Prob(i) \cdot 1/p^{(n-1)(k-1)}}{1/p^{(n-1)(k-1)} \cdot \sum_{j \in \{0,\ldots,n-1\}} Prob(j)} \\ &= Prob(i). \end{aligned}$$

  Hence, the probability distribution $Prob(i|z)$ of the n indices, given the "view" of the $k-1$ Servers (i.e., the $(k-1)$ tuples of $(n-1)$ values, obtained by interacting with $\mathcal{R}$), is equal to the a-priori probability distribution of the n indices $Prob(i)$, induced by the Receiver's choice. Moreover, the data D_X held by the Servers, are independent of z and i. Hence, $Prob(i|z, D_X) = Prob(i|z)$. As a consequence, the choice of the Receiver is private.

- Condition (6). First notice that the Receiver does not get any information during the set-up phase about the secrets. Then, let us assume w.l.o.g. that the coalition is composed by Servers $S_1, \ldots, S_{k-1}$. They hold polynomials $Q(1, y_1, \ldots, y_{n-1}), \ldots, Q(k-1, y_1, \ldots, y_{n-1})$, and shares $r_1^1, \ldots, r_1^{k-1}, \ldots, r_{n-1}^1, \ldots, r_{n-1}^{k-1}$. We show that, *for any* choice of n secrets $w_0, \ldots, w_{n-1}$, and shares $r_1^1, \ldots, r_1^{k-1}, \ldots, r_{n-1}^1, \ldots, r_{n-1}^{k-1}$, there exists a sequence of random values $r_1, \ldots, r_{n-1}$ such that the n-variate polynomial $P(x, y_1, \ldots, y_{n-1}) = a(x) + b_1 y_1 + \cdots + b_{n-1} y_{n-1}$, with coefficients a_0 and b_j, for $j = 1, \ldots, n-1$, defined as in Table 2, satisfies the following property: for any $\ell \in \{1, ..., k-1\}$, it holds that $P(\ell, y_1, \ldots, y_{n-1}) = Q(\ell, y_1, \ldots, y_{n-1})$ and the shares $r_1^1, \ldots, r_1^{k-1}, \ldots, r_{n-1}^1, \ldots, r_{n-1}^{k-1}$ are consistent with $r_1, \ldots, r_{n-1}$.

  The polynomial $P(x, y_1, \ldots, y_{n-1}) = a(x) + b_1 y_1 + \cdots + b_{n-1} y_{n-1}$ is constructed as follows: for $i = 1, \ldots, n-1$ the coefficients $b_1, \ldots, b_{n-1}$ are equal to the coefficients of $y_1, \ldots, y_{n-1}$ in the $(n-1)$-variate polynomials $Q(1, y_1, \ldots, y_{n-1}), \ldots, Q(k-1, y_1, \ldots, y_{n-1})$ held by $S_1, \ldots, S_{k-1}$. Moreover, since $a_0 = w_0$ and $b_i = r_i w_i - w_0$, for $i = 1, \ldots, n-1$, for *any* choice of the secrets $w_0, \ldots, w_{n-1}$ the coefficient a_0 and the values $r_1, \ldots, r_{n-1}$ are uniquely determined. Then, the coefficients of $\sum_{j=1}^{k-1} a_j x^j$ are the solution to the system of $k-1$ linear equations given by $P(\ell, 0, \ldots, 0) = Q(\ell, 0, \ldots, 0)$, for $\ell = 1, \ldots, k-1$, whose variables are $a_1, \ldots, a_{k-1}$. The solution is unique since, in matrix form, the above system of linear equations is such that the matrix of coefficients is a $(k-1) \times (k-1)$ Vandermonde matrix.

  Therefore, given a sequence of secrets $w_0, \ldots, w_{n-1}$ and the sequence of random values $r_1, \ldots, r_{n-1}$, there exists a one-to-one correspondence between the choices of a set of coefficients $a_1, \ldots, a_{k-1}$, and the sequences of polynomials $Q(1, y_1, \ldots, y_{n-1}), \ldots, Q(k-1, y_1, \ldots, y_{n-1})$. Moreover, due to the properties of secret sharing schemes, the shares $r_1^1, \ldots, r_1^{k-1}, \ldots, r_{n-1}^1, \ldots, r_{n-1}^{k-1}$ are consistent with $r_1, \ldots, r_{n-1}$, and do not give any information about them. Indeed, $r_1, \ldots, r_{n-1}$ and the shares $r_1^1, \ldots, r_1^{k-1}, \ldots, r_{n-1}^1, \ldots, r_{n-1}^{k-1}$ are statistically independent, i.e.,. denoting by *Shares* the shares $r_1^1, \ldots, r_1^{k-1}, \ldots, r_{n-1}^1, \ldots, r_{n-1}^{k-1}$, and by r the values $r_1, \ldots, r_{n-1}$, it holds that

  $$Prob(Shares|w, r) = Prob(Shares|r) = \frac{1}{p^{(n-1)(k-1)}}.$$

  Since the Sender $\mathcal{S}$ chooses the coefficients independently and uniformly at random then, it holds that the probability of getting polynomials $Q(1, y_1, \ldots, y_{n-1}), \ldots, Q(k-1, y_1, \ldots, y_{n-1})$, once the Sender has chosen a sequence of secrets $w =< w_0, \ldots, w_{n-1} >$ with $Prob(w) > 0$, and the sequence of random values $r =< r_1, \ldots, r_{n-1} >$, is

  $$Prob(Q(1, y_1, \ldots, y_{n-1}), \ldots, Q(k-1, y_1, \ldots, y_{n-1})|w, r) = 1/p^{k-1}.$$

  Therefore, denoting with q the polynomials $Q(1, y_1, \ldots, y_{n-1}), \ldots, Q(k-1, y_1, \ldots, y_{n-1})$, the joint probability of q and *Shares*, given w and r is:

  $$Prob(q, Shares|w, r) = Prob(q|w, r) \cdot Prob(Shares|q, w, r) = \frac{1}{p^{k-1}} \cdot \frac{1}{p^{(n-1)(k-1)}}.$$

Applying Bayes' theorem, we have

$$\begin{aligned} Prob(w,r|q,Shares) &= \frac{Prob(w,r)\cdot Prob(q,Shares|w,r)}{\sum_{w'\in F_p^n:Prob(w')>0,r'\in F_p} Prob(w',r')\cdot Prob(q,Shares|w',r')} \\ &= \frac{Prob(w,r)\cdot 1/p^{(n-1)(k-1)(k-1)}}{\sum_{w'\in F_p^n:Prob(w')>0,r'\in F_p} Prob(w',r')\cdot 1/p^{(n-1)(k-1)(k-1)}} \\ &= \frac{Prob(w,r)\cdot 1/p^{(n-1)(k-1)(k-1)}}{1/p^{(n-1)(k-1)(k-1)}\cdot \sum_{w'\in F_p^n:Prob(w')>0,r'\in F_p} Prob(w',r')} \\ &= Prob(w,r). \end{aligned}$$

Hence, it follows that the probability distribution $Prob(w|q,Shares)$ of the n secrets, given the $k-1$ polynomials held by $S_1,\ldots,S_{k-1}$ and the shares $Shares$ held by the Servers, is equal to the a-priori probability distribution of the n secrets $Prob(w)$, induced by the Sender's choices. Finally, since D_R are truly random bits independent of $w, r, Shares$ and q, it holds that $Prob(w|q,Shares,D_R) = Prob(w|q,Shares)$.

- Condition (7) is *not* satisfied. Indeed, it is possible to show that in the protocol given in Table 2 the Receiver can learn a linear combination of the secrets. Indeed, if the Receiver does not follow the protocol and chooses certain values $(Z_1(0),\ldots,Z_{n-1}(0))$, say for example $(2,3,\ldots,1)$, then she gets a linear combination of the secrets $w_0,\ldots,w_{n-1}$.

Notice that, in [34], for the case of two secrets, a proof that the Receiver can get *no more than a single* linear combination of the two secrets by running the sub-protocol described in Table 2 with k Servers was given. It is not difficult to show that the proof easily generalises to our scheme for n secrets, i.e., after receiving information from k servers, the Receiver cannot learn more than a single linear combination of $w_0, w_1, \ldots, w_{n-1}$. Indeed, our scheme extends the scheme in [34] to deal with n secrets. Moreover, it enjoys a further security properties i.e., Condition (6), which *is not* satisfied by the scheme of [34]. Indeed, in the protocol of [34], each Server can compute a linear combination of the secrets.

The above protocol can be used to construct a (k,m)-DOT-$\binom{n}{1}$, forcing the Receiver to get *at most one of the secrets* held by the Sender and no joint information about the secrets, by using *multiple instances* of the sub-protocol. More precisely, the sub-protocol given in Table 2, can be used as a building block to set up a (k,m)-DOT-$\binom{n}{1}$. The idea is the following: the Sender executes with the Receiver 2 parallel *instances* of the sub-protocol of Table 2, with the constraint that the Receiver asks *the same* queries, i.e., sends the same values for both instances. The first instance hides "masked" secrets, i.e., for $i = 0,\ldots,n-1$, the value $c_i w_i$ instead of simply w_i. The other instance hides the masks c_i which are needed in order to recover the corresponding secret w_i. If the Receiver sends correct values, then she obtains one and only one masked secret from the first instance and the mask from the other instance. Otherwise, she gets no information about the secrets.

The scheme is given in Table 3. We use parts of the sub-protocol described in Table 2, which, to simplify the description, we denote as $SubDOT(\cdot)$. The inputs to the instances of $SubDOT(\cdot)$ we use are sequences of suitably chosen secrets.

We show that the protocol given in Table 3 implements a (k,m)-DOT-$\binom{n}{1}$.

A Protocol for (k,m)-DOT-$\binom{n}{1}$.
Let $w_0, w_1, \ldots, w_{n-1} \in F_p$ be $\mathcal{S}$'s secrets, and let $i \in \{0, \ldots, n-1\}$ be $\mathcal{R}$'s choice.

Set-up Phase.

- The Sender $\mathcal{S}$ executes simultaneously and independently the Set-up Phase of 2 instances $SubDOT_1(\cdot)$ and $SubDOT_2(\cdot)$ of the sub-protocol given in Table 2 as follows: let $c_0, c_1, \ldots, c_{n-1}$ be values, different from zero, chosen independently and uniformly at random in F_p. Then, he executes:

  Set-up Phase of $SubDOT_1(c_0w_0, c_1w_1, \ldots, c_{n-1}w_{n-1})$
  Set-up Phase of $SubDOT_2(c_0, c_1, c_2, \ldots, c_{n-1})$

  Every Server S_j receives from $\mathcal{S}$, for $\ell = 1, 2$, the polynomial and the shares corresponding to the random values $r_0^\ell, \ldots, r_{n-1}^\ell$, associated with $SubDOT_\ell(\cdot)$.

Oblivious Transfer Phase.

- Let $X \subseteq \{1, \ldots, m\}$ be a subset of k indices. The Receiver $\mathcal{R}$ sends, for every $j \in X$, to Server S_j, *the same* values described in Table 2, that is, $\mathcal{R}$ sends to Server $\mathcal{S}_j$ the values $Z_1(j), \ldots, Z_{n-1}(j)$. However, she receives, from each of the k Servers, 2 values, according to the instances $SubDOT_1(c_0w_0, c_1w_1, \ldots, c_{n-1}w_{n-1})$ and $SubDOT_2(c_0, c_1, c_2, \ldots, c_{n-1})$ and the sequences of shares.
- If the Receiver's choice is $i \in \{0, 1, \ldots, n-1\}$, then she obtains from $SubDOT_1(c_0w_0, c_1w_1, \ldots, c_{n-1}w_{n-1})$ the value c_iw_i, and from the other instance $SubDOT_2(c_0, c_1, c_2, \ldots, c_{n-1})$, the value c_i.
- Then, a simple division in F_p, i.e., c_iw_i/c_i, yields the desired secret.

Table 3: A one-round (k,m)-DOT-$\binom{n}{1}$ scheme: Set-up.

Correctness. From the description of the Oblivious Transfer Phase, it is easy to see that Definition 4.1 is satisfied. The correctness of the sub-protocol of Table 2 guarantees that the Receiver gets a masked secret and the mask. Then, a simple computation (i.e. division in F_p) enables recovering the secret by removing the mask.

Privacy. The privacy property, stated by Definition 2.2, can be shown as follows:

- Condition (5) follows exactly from the same argument we have applied discussing the protocol given in Table 2. We are repeating 2 times the protocol of Table 2, with the constraint that the Receiver sends a *single* sequence of values instead of 2 distinct sequences of values.
- Condition (6) holds because the two instances $SubDOT_1(\cdot)$ and $SubDOT_2(\cdot)$ are independent and, each of them, does not lack any information about its own input, i.e., masked secrets and masks are all equiprobable.
- Condition (7) can be shown by analysing two cases. The Receiver uses a malicious program $\overline{R}$. In order to learn information about more than one secret, such a program

cheats by sending an incorrect sequence of values z to the Servers S_X. Notice that, for any subset of k indices X, for any $i = 0, \ldots, n-1$, for any possible random string D_R, and for any malicious program $\overline{R}$, the values computed through $\overline{R}$ and sent to S_X, *uniquely* determine an index $\tilde{i}$, represented as a tuple $(0, Z_1(0), \ldots, Z_{n-1}(0))$. Indeed, the values sent by the Receiver can always be sees as evaluation of certain interpolated polynomials $Z_1(x) = \sum_{j=0}^{k-1} z_1^j x^j, \ldots, Z_{n-1}(x) = \sum_{j=0}^{k-1} z_{n-1}^j x^j$ of degree $k-1$, i.e., as a sequence z given by $Z_1(j), \ldots, Z_{n-1}(j)$, for $j \in X$. Such an index $\tilde{i}$ either is a value in $\{0, \ldots, n-1\}$ or does not belong to $\{0, \ldots, n-1\}$.

Case i). If $\tilde{i} \in \{0, \ldots, n-1\}$, then, from the values the Receiver gets from the Servers S_X, she computes the secret $w_{\tilde{i}}$ and gets no additional information about the others. Indeed, it is easy to check that, the interpolating polynomial $V_1(x)$ associated to $SubDOT_1(\cdot)$ is equal to

$$\begin{aligned} V_1(x) &= \sum_{j=1}^{k-1} (a_j + b_1 z_1^j + \cdots + b_{n-1} z_{n-1}^j) x^j + a_0 + b_1 z_1^0 + \cdots + b_{n-1} z_{n-1}^0 \\ &= \sum_{j=1}^{k-1} e_j x^j + c_{\tilde{i}} r_{\tilde{i}} w_{\tilde{i}} \end{aligned}$$

where $e_j = a_j + b_1 z_1^j + \cdots + b_{n-1} z_{n-1}^j$, for $j = 1, \ldots, k-1$ and, similarly, for the second instance $SubDOT_2(\cdot)$, the polynomial $V_2(x)$ is equal to $V_2(x) = \sum_{j=1}^{k-1} g_j x^j + c_{\tilde{i}} r'_{\tilde{i}}$, where $g_j = a'_j + b'_1 z_1^j + \cdots + b'_{n-1} z_{n-1}^j$, for $j = 1, \ldots, k-1$, and $r_0 = r'_0 = 1$.

Hence, the Receiver could gain information about the other secrets by analysing the coefficients e_j and g_j, for $j = 1, \ldots, k-1$. Indeed, the polynomials $V_1(x)$ and $V_2(x)$ are an *equivalent* representation of the information (i.e., sets of points) that the Receiver gets by interacting with the Servers. Therefore, there in no loss of generality in focusing on them.

Notice that, the Receiver has full control over the elements z_j^i's but has no control over $a_1, \ldots, a_{k-1}$ and $a'_1, \ldots, a'_{k-1}$, and over the coefficients $c_0, \ldots, c_{n-1}$, hidden in $b_1, \ldots, b_{n-1}, b'_1, \ldots, b'_{n-1}$, which are chosen uniformly at random by the Sender.

We show that the probability of getting $e_1, \ldots, e_{k-1}$ and $g_1, \ldots, g_{k-1}$ is equal to $(1/p^{k-1})^2$, independently of the remaining secrets. Indeed, once fixed the values of b_i, b'_i and z_j^i's, the sums $b_1 z_1^j + \cdots + b_{n-1} z_{n-1}^j$ and $b'_1 z_1^j + \cdots + b'_{n-1} z_{n-1}^j$ are determined, and any choice of a_j and a'_j implies different values for e_j and g_j. Therefore, for $i = 1, \ldots, n-1$, *independently* of the values b_i and b'_i (and, hence, of the remaining secrets), the choice of the values $a_1, \ldots, a_{k-1}$ and $a'_1, \ldots, a'_{k-1}$, determines the values $e_1, \ldots, e_{k-1}$ and $g_1, \ldots, g_{k-1}$.

Let us denote with w^* the choices of the remaining secrets, with z the sequence of values sent by the Receiver, and with r and r' the sequences of random values used by the Sender. Then, the transcript $\overline{C_X}$ of the conversation between the Receiver and the Servers is equivalent to $(z, e_1, \ldots, e_{k-1}, g_1, \ldots, g_{k-1}, w_{\tilde{i}} c_{\tilde{i}} r_{\tilde{i}}, c_{\tilde{i}} r'_{\tilde{i}}, Shares)$. It follows that:

$$Prob(\overline{C_X} | i, D_R, w_{\tilde{i}}, c_{\tilde{i}}, w^*, r, r') = (1/p^{k-1})^{2n}.$$

Therefore, due to Bayes' theorem and the independence of w^* from i, D_R, r, r' and $c_{\underset{i}{\sim}}$, we have that the $Prob(w^*|i, D_R, \overline{C_X}, w_{\underset{i}{\sim}}, c_{\underset{i}{\sim}}, r, r')$ is equal to

$$\frac{Prob(w^*|i, D_R, w_{\underset{i}{\sim}}, c_{\underset{i}{\sim}}, r, r') \cdot Prob(\overline{C_X}|i, D_R, w_{\underset{i}{\sim}}, c_{\underset{i}{\sim}}, r, r', w^*)}{\sum_{w':Prob(w'>0)} Prob(w'|i, D_R, w_{\underset{i}{\sim}}, c_{\underset{i}{\sim}}, r, r') \cdot Prob(\overline{C_X}|i, D_R, w_{\underset{i}{\sim}}, c_{\underset{i}{\sim}}, r, r', w')}$$
$$= Prob(w^*|i, D_R, w_{\underset{i}{\sim}}, c_{\underset{i}{\sim}}, r, r') = Prob(w^*|w_{\underset{i}{\sim}}).$$

Hence, from the Receiver's point of view, once a secret is known, the other $n-1$ secrets still have the same a-priori probabilities, i.e., $Prob(\overline{w}|i, D_R, \overline{C}_X, w_{\underset{i}{\sim}}, c_{\underset{i}{\sim}}, r, r') = Prob(\overline{w}|w_{\underset{i}{\sim}})$.

Case *ii*). We prove that, from the values the Receiver gets from the Servers S_X, she computes no information about the secrets at all. Indeed, as we have discussed before, the sub-protocol $SubDOT(\cdot)$ leaks at most one linear combination of the secrets. Such a result can be formally proved by applying the same argument used in [34] for the case of two secrets. The sub-protocol $SubDOT_1(\cdot)$ hides the secrets $c_0w_0, c_1w_1, \ldots, c_{n-1}w_{n-1}$; while, the sub-protocol $SubDOT_2(\cdot)$ hides the secrets $c_0, c_1, \ldots, c_{n-1}$. Hence, the Receiver, running the protocol, gets at most two linear combinations:

$$\begin{aligned}\gamma_1 &= \alpha_0c_0w_0 + \ldots + \alpha_{n-1}c_{n-1}w_{n-1}\\ \gamma_2 &= \alpha_0c_0 + \ldots + \alpha_{n-1}c_{n-1}\end{aligned}$$

which can be expressed in a matrix form as follows:

$$\begin{bmatrix} \alpha_0w_0 & \cdots & \alpha_{n-1}w_{n-1} \\ \alpha_0 & \cdots & \alpha_{n-1} \end{bmatrix} \times \begin{bmatrix} c_0 \\ \\ \vdots \\ \\ c_{n-1} \end{bmatrix} = \begin{bmatrix} \gamma_1 \\ \gamma_2 \end{bmatrix}$$

We have to show that $Prob(w|i, D_R, \overline{C}_X) = Prob(w)$. The transcript of the interaction $\overline{C}_X$ is equal to (z, a), where z is the sequence of values the Receiver sends to the Servers S_X, and a is the sequence of answers she receives. Since from $(i, D_R, \overline{C}_X)$ the Receiver gets at most the above two linear combinations, in order to prove our claim it is enough to show that $Prob(w|\gamma_1, \gamma_2) = Prob(w)$, once the coefficients α_i's are fixed and known.

Let us assume that the secrets $w_0, \ldots, w_{n-1}$ are all distinct, i.e., we add a unique pad to each of them, and that *at least* two coefficients among the α_i's are different from zero. Indeed, if all coefficients are zero, then the Receiver does not get information about the secrets at all, while, if only one coefficient is different from zero, then the Receiver gets the corresponding secret and no information on the others. Let us say that these two coefficients are α_i and α_j. Then, the determinant of the corresponding 2×2 sub-matrix is equal to $\alpha_i\alpha_jw_i - \alpha_j\alpha_iw_j \neq 0$. Hence, the two rows of the matrix of the system are linearly independent. Therefore, the above system has p^{n-2} solution vectors $(c_0, \ldots, c_{n-1})$, and the $Prob(\gamma_1, \gamma_2|w)$ is equal to $\frac{1}{p^{n-2}}$. Applying Bayes' theorem we have that:

$$Prob(w|\gamma_1, \gamma_2) = \frac{Prob(w) \cdot Prob(\gamma_1, \gamma_2|w)}{\sum_{w':Prob(w')>0} Prob(w') \cdot Prob(\gamma_1, \gamma_2|w')} = Prob(w).$$

Remark. To set up the scheme the Sender needs $(k-1)+(n-1)$ random values $a_1, \ldots, a_{k-1}, r_1^\ell, \ldots, r_{n-1}^\ell$ in F_p to construct $Q(x, y_1, \ldots, y_{n-1})$, and $(k-1)(n-1)$ random values to share $r_1^\ell, \ldots, r_{n-1}^\ell$, required by the set-up phase of $SubDOT_\ell(\cdot)$, for $\ell = 1, 2$. Moreover, he needs n additional random values $c_0, \ldots, c_{n-1}$. Hence, $H(\mathbf{D}_1, \ldots, \mathbf{D}_m) = (2kn+n-2)\log p$. However, we can show that *the same* random values $a_1, \ldots, a_{k-1}$ can be used in both instances of $SubDOT(\cdot)$ and the values $r'_1, \ldots, r'_{n-1}$ can be computed as function of $r_1, \ldots, r_{n-1}$. Thus the randomness can be reduced to $(kn+n-1)\log p$.

A sub-protocol for t-private weak one-round (k,m)-DOT-$\binom{n}{1}$.
Let $w_0, w_1, \ldots, w_{n-1} \in F_p$ be $\mathcal{S}$'s secrets, and let $i \in \{0, \ldots, n-1\}$ be $\mathcal{R}$'s choice.

Set-up Phase.

- Let d_x, d_y and d_z be integers such that $d_x + d_z d_y(n-1) = k-1$. The Sender $\mathcal{S}$ generates independently and uniformly at random values $r_0, r_1 \ldots, r_{n-1} \in F_p$, and sets up an n-variate polynomial with values in F_p

$$Q(x, y_1, \ldots, y_{n-1}) = \sum_{j=0}^{d_x} \sum_{\ell_1=0}^{d_y} \cdots \sum_{\ell_{n-1}=0}^{d_y} a_{j,\ell_1,\ldots,\ell_{n-1}} x^j y_1^{\ell_1} \cdots y_{n-1}^{\ell_{n-1}}$$

  where $a_{0,\ldots,0} = r_0 w_0$, for $i = 1, \ldots, n-1$, $\sum_{\ell_i=0}^{d_y} a_{0,\ldots,\ell_i,\ldots,0} = r_i w_i$, and all other coefficients are chosen uniformly at random. It holds that, $Q(0,0,\ldots,0) = r_0 w_0, Q(0,1,0,\ldots,0) = r_1 w_1, \ldots, Q(0,0,\ldots,1) = r_{n-1} w_{n-1}$.

- Then, for $\ell = 0, \ldots, n-1$, he shares independently r_ℓ, according to a Shamir's (k,m) threshold secret sharing scheme. Let r_ℓ^j, for $j = 1, \ldots, m$, the corresponding shares. For $j = 1, \ldots, m$, $\mathcal{S}$ sends the $(n-1)$-variate polynomial $Q(j, y_1, \ldots, y_{n-1})$ and the shares $r_0^j, \ldots, r_{n-1}^j$ to Server $\mathcal{S}_j$.

Oblivious Transfer Phase.

- The Receiver $\mathcal{R}$ chooses $n-1$ random polynomials $Z_1(x) \ldots, Z_{n-1}(x)$ of degree d_z such that $(Z_1(0), \ldots, Z_{n-1}(0))$ is an $(n-1)$-tuple of zeroes if $i = 0$ or an $(n-1)$-tuple of zeroes and a single 1 in position i, if $i \in \{1, \ldots, n-1\}$.
- Then, the Receiver $\mathcal{R}$ chooses a subset $X \subseteq \{0, \ldots, n-1\}$ of k indices, and sends, for every $j \in X$, to Server $\mathcal{S}_j$ the values $Z_1(j), \ldots, Z_{n-1}(j)$, and receives the value $V(j) = Q(j, Z_1(j), \ldots, Z_{n-1}(j))$ and all the shares $r_1^j, \ldots, r_{n-1}^j$.
- After having received the k values $V(j)$, for $j \in X$, the Receiver $\mathcal{R}$ interpolates a univariate polynomial $V(x) = Q(x, Z_1(x), \ldots, Z_{n-1}(x))$ of degree $k-1$, and computes $V(0)/r_i$, where r_i is reconstructed through the shares r_i^j's.

Table 4: A sub-protocol for t-private weak one-round (k,m)-DOT-$\binom{n}{1}$.

Strengthening and generalising the second construction of [34], which uses fully n-variate polynomials, we can set up a sort of DOT protocol in which condition (5) of Definition 2.2 holds against subsets of Servers S_X, such that $|X| < k-1$, and in which condition (11) of Definition 2.3 is satisfied with respect to a coalition among the Receiver and a subset of Servers S_X, such that $|X| = t < k-1$. We refer to such a protocol as to a t-private weak one-round (k,m)-DOT-$\binom{n}{1}$. In Table 4 we describe the sub-protocol that can be used to set up a t-private weak one-round (k,m)-DOT-$\binom{n}{1}$.

Correctness. Definition 4.1 is satisfied. Indeed, denoting as before by $Z_j(x) = \sum_{r=0}^{d_z} z_j^r x^r$ the polynomials generated by $\mathcal{R}$, the polynomial $V(x)$ interpolated by $\mathcal{R}$

$$V(x) = Q(x, Z_1(x), \ldots, Z_{n-1}(x))$$

can be written as

$$\sum_{j=0}^{d_x}\sum_{\ell_1=0}^{d_y}\cdots\sum_{\ell_{n-1}=0}^{d_y} a_{j,\ell_1,\ldots,\ell_{n-1}} x^j (z_1^0 + \sum_{j=1}^{d_z} z_1^j x^j)^{\ell_1} \cdots (z_{n-1}^0 + \sum_{j=1}^{d_z} z_{n-1}^j x^j)^{\ell_{n-1}}$$

Therefore, it is immediate to see that, if for $j = 1, \ldots, n-1$, $z_j^0 = 0$, then $V(0) = a_{0,\ldots,0}$. On the other hand, assuming that $z_i^0 = 1$, while, for $j \neq i$ it is $z_j^0 = 0$, the only term which appears in $V(0)$ is $\sum_{l_i=0}^{d_y} a_{0,\ldots,0,\ell_i,0\ldots,0} y_i^{l_i}$ and it is easy to see that

$$V(0) = \sum_{l_i=0}^{d_y} a_{0,\ldots,0,\ell_i,0\ldots,0}.$$

Privacy. Along the same lines of the proof given for the sub-protocol described in Table 2, we can show that condition (5) of Definition 2.2 holds with respect to a coalition of d_z Servers, and condition (6) of Definition 2.2 is satisfied with respect to a coalition of d_x Servers. However, the protocol given in Table 4 does not satisfy condition (7) of Definition 2.2 and, hence, condition (11) of Definition 2.3, but it guarantees that the Receiver can learn at most a linear combination of the secrets. The same strategy applied in Table 3 can be used to set up a t-private weak one-round (k,m)-DOT-$\binom{n}{1}$, where condition (7) of Definition 2.2 holds, and condition (11) of Definition 2.3 is also satisfied, with respect to a coalition of size $t < k-1$ Servers and the Receiver. The threshold t depends on the particular choices of d_x, d_y, d_z and k.

6 Combinatorial Constructions

In this section we propose some combinatorial constructions for distributed oblivious transfer. Some of these constructions require trivial computations once the scheme has been set up by the Sender. The one-round protocols meet the lower bound on the number of random bits the Receiver must use to set up the queries, given by Theorem 4.11. However, they are not so efficient in terms of Server memory storage and communication complexity.

6.1 One-Round Constructions

We start by giving protocols which require one round of interaction to recover a secret. The constructions are based on well-known combinatorial structures. In order to provide an intuition of the ideas underlying the following protocols, we start by looking at an example of a one-round $(2,2)$-DOT-$\binom{3}{1}$.

Set-up Phase. Assume that the three secrets held by the Sender are w_0, w_1 and w_2. The Sender constructs a 2×3^2 matrix A with values chosen in F_p

$$A = \begin{bmatrix} a_{1,0} & a_{1,1} & a_{1,2} & a_{1,3} & a_{1,4} & a_{1,5} & a_{1,6} & a_{1,7} & a_{1,8} \\ a_{2,0} & a_{2,1} & a_{2,2} & a_{2,3} & a_{2,4} & a_{2,5} & a_{2,6} & a_{2,7} & a_{2,8} \end{bmatrix}$$

in such a way that the sum of the values mod$p$ of every column is one of the secrets. Therefore, we say that every column of A *hides* a secret. The rule used to hide a secret by means of a column is depicted in Table 5 and explained below.

Index column	0	1	2	3	4	5	6	7	8
Representation in base 3	00	01	02	10	11	12	20	21	22
Corresponding secret index	0	1	2	1	2	0	2	0	1

Table 5: Correspondence secret-column

The indices of the columns of A, i.e., $0, 1, \ldots, 8$, represented in base 10 are given in the first row. The representations of such indices in base 3 are given in the second row. The third row contains the sum mod3 of the digits of the representations in base 3. For example, the column whose index is 0 has representation in base 3 equal to 00. Hence, $0 + 0 \bmod 3 = 0$, which is the value reported in the third row. The column whose index is 1 has representation 01. Hence, $0 + 1 \bmod 3 = 1$. The column whose index is 5 has representation 12. Hence, $1{+}2 \bmod 3 = 0$, and so on. In general, the column whose index is $j \in \{0, 1, \ldots, 8\}$, represented in base 3 by $c_1^j c_2^j$, hides the secret w_i, for $i \in \{0, 1, 2\}$, *if and only if* $c_1^j + c_2^j \bmod 3 = i$. Therefore, it is easy to check that columns whose indices are $0, 5$ and 7 hide w_0, columns whose indices are $1, 3$ and 8 hide w_1, and columns whose indices are $2, 4$ and 6 hide w_2. Once the matrix A has been set up, the Sender sends the first row of A to S_1 and the second to S_2.

Oblivious Transfer Phase. To recover a secret among w_0, w_1, w_2, let us say w_1, the Receiver chooses one of the columns which hides w_1, for example column 3, and sends $c_1^3 = 1$ to S_1 and $c_2^3 = 0$ to S_2. Every Server sends to the Receiver a subset of the values of his own row. More precisely, S_1 compares 1 with the first digit c_1^j of the representation in base 3 of column j, for $j \in \{0, 1, \ldots, 8\}$. If they are equal, then S_1 sends the value $a_{1,j}$. Server S_2 does the same by comparing 0 with the second digit c_2^j of the representation in base 3 of column j, for $j \in \{0, 1, \ldots, 8\}$. Therefore, the Receiver gets the values $a_{1,3}, a_{1,4}, a_{1,5}$ from S_1 and $a_{2,0}, a_{2,3}, a_{2,6}$ from S_2, and computes $w_1 = a_{1,3} + a_{2,3} \bmod p$. ■

The reader can check by hand that the above example yields a one-round $(2,2)$-DOT-$\binom{3}{1}$. The protocol for the general case is given in Table 6. We show that this protocol implements a One-Round (k,k)-DOT-$\binom{n}{1}$.

A One-Round (k,k)-DOT-$\binom{n}{1}$ Construction.
Let $w_0, w_1, \ldots, w_{n-1} \in F_p$ be $\mathcal{S}$'s secrets and let $i \in \{1, \ldots, n\}$ be $\mathcal{R}$'s index.

Set-up Phase

- $\mathcal{S}$ sets up a $k \times n^k$ matrix A of random values in F_p as follows: for $j \in \{0, \ldots, n^k - 1\}$, the sum of the values of column $A[\cdot, j]$ is equal to w_i if, denoting by $c_1^j \cdots c_k^j$ the representation in base n of j, then $\sum_{\ell=1}^{k} c_\ell^j \bmod n = i$.
- $\mathcal{S}$, for $q = 1, \ldots, k$, sends the q-th row $A[q, \cdot]$ to the Server S_q.

Oblivious Transfer Phase

- $\mathcal{R}$ chooses a value $j \in \{0, \ldots, n^k - 1\}$ such that $\sum_{\ell=1}^{k} c_\ell^j \bmod n = i$ and, for $q = 1, \ldots, k$, she sends the digit c_q^j to Server S_q.
- Server S_q, for $\ell = 0, \ldots, n^k - 1$, sends to the Receiver the pair $(\ell, A[q, \ell])$ if and only if the q-th digit of the n-ary representation of ℓ is equal to c_q^j.
- $\mathcal{R}$ sums up the values $A[1, j], \ldots, A[k, j]$, recovering the secret, that is $w_i = \sum_{h=1}^{k} A[h, j] \bmod p$.

Table 6: A One-Round (k,k)-DOT-$\binom{n}{1}$ Construction

Correctness. Definition 4.1 is satisfied since, once $\mathcal{R}$ has chosen column j, whose n-ary representation is $c_1^j \ldots c_k^j$ and has sent, for $q = 1, \ldots, k$ the digit c_q^j to Server S_q, among other values, certainly she receives back $A[1, j], \ldots, A[k, j]$. Hence, $\mathcal{R}$ can compute w_i as $\sum_{h=1}^{k} A[h, j] \bmod p$.

Privacy. The privacy property, stated by Definition 2.2, can be shown as follows:

- Condition (5) is satisfied: a coalition of $k-1$ Servers, say S_X, where $X = \{1, \ldots, k-1\}$, contacted by $\mathcal{R}$, cannot infer in which secret she is interested. Indeed, assume that column j, chosen by $\mathcal{R}$ to recover the secret, has n-ary representation $c_1^j \ldots c_k^j$. Then $S_1, \ldots, S_{k-1}$, receive *only* $c_1^j \ldots c_{k-1}^j$ from $\mathcal{R}$. Since the index i of the secret w_i, hidden by column j, is given by $\sum_{\ell=1}^{k} c_\ell^j \bmod n$, for any index $i \in \{0, \ldots, n-1\}$ chosen by the Receiver, there is *exactly one* value c_k^j such that $\sum_{\ell=1}^{k-1} c_\ell^j + c_j^k \bmod n = i$. Hence, $Prob(c_1^j, \ldots, c_{k-1}^j | i) = \frac{1}{n}$. Therefore, using Bayes' theorem, it follows that $Prob(i | c_1^j, \ldots, c_{k-1}^j) = Prob(i)$. Finally, since the private information D_X is independent of $c_1^j, \ldots, c_{k-1}^j$, it holds that $Prob(i | D_X, c_1^j, \ldots, c_{k-1}^j) = Prob(i | c_1^j, \ldots, c_{k-1}^j)$.
- Condition (6) basically holds for the same reason we have seen discussing Condition (5). For any coalition of $k-1$ servers, say S_X, where $X = \{1, \ldots, k-1\}$, S_X does not gain information about any secret from the data D_X they possess. Indeed, let D_X be the set of values $\{A[1, j], \ldots, A[k-1, j],$ for $j = 0, \ldots, n^k - 1\}$. Since for any $i = 0, \ldots, n-1$, secret w_i is hidden by $\sum_{q=1}^{k} A[q, j] \bmod p$, for certain columns $j \in \{0, \ldots, n^k - 1\}$, then, from S_X's point of view, for any secret w_i, there is *exactly one* value $A[k, j]$ such that $\sum_{q=1}^{k-1} A[q, j] + A[k, j] \bmod n = w_i$. Simple algebra and Bayes' theorem show that, for

all w such that $Prob(w) > 0$, it holds that $Prob(w|D_X) = Prob(w)$. Finally, since D_R are truly random bits, independent of w and D_X, it holds that $Prob(w|D_X, D_R) = Prob(w|D_X)$.

- In order to show condition (7) we have to consider only one case, i.e., Case i). Indeed, in the above protocol, for any index i and for any possible random string D_R, even if the Receiver's program is malicious, the integer values it sends to the Servers uniquely identify a column $j \in \{0, \ldots n^k - 1\}$ and the corresponding index $\tilde{i} \in \{0, \ldots, n-1\}$. Such an invariant holds because if the Receiver sends out to a Server a value which does not belong to $\{0, \ldots, n-1\}$, then the Server just does not reply. Hence, the Receiver surely computes $w_{\tilde{i}}$. However, all the values of a column are needed to compute a secret, and each value is essential to determine the secret. Therefore, for $j \in \{0, \ldots, n^k - 1\}$, whose representation is given by $c_1^j \ldots, c_k^j$, and for $q = 1, \ldots, k$, denote by $Values_{q,j} = \{(\ell, A[q, \ell]) | \ell = 0, \ldots, n^k - 1, \text{ and } c_q^\ell = c_q^j\}$ the set of pairs of values the Receiver gets from Server S_q. Then, the transcript C_X is equal to $(c_1^j, \ldots, c_k^j, Values_{1,j}, \ldots, Values_{k,j})$, and it follows that $Prob(w|i, D_R, C_X, w_{\tilde{i}}) = Prob(w|w_{\tilde{i}})$.

Using some well-known combinatorial structures, we can generalize the above construction, in order to set up a (k,m)-DOT-$\binom{n}{1}$. More precisely, let t, q, r and λ be integers such that $1 \le t \le q$ and $r \ge 2$. An *orthogonal array* $OA_\lambda(t, q, r)$ is a $\lambda r^t \times q$ array of r symbols, say $\{0, 1, \ldots, r-1\}$, such that within any t columns, every possible t-tuple of symbols occurs in exactly λ rows (see [29] for constructions and references). Using an orthogonal array and threshold secret sharing schemes[3], we can set up a (k,m)-DOT-$\binom{n}{1}$ (see Table 7).

Example. We present a one-round $(2,3)$-DOT-$\binom{3}{1}$ using the protocol described in Table 7.

Set-up Phase. The Sender constructs and publishes the following matrix obtained by transposing an $OA_1(2, 4, 3)$:

$$I = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \\ 0 & 1 & 2 & 1 & 2 & 0 & 2 & 0 & 1 \\ 0 & 1 & 2 & 2 & 0 & 1 & 1 & 2 & 0 \end{bmatrix}.$$

Then, he shares the secret associated with each column by means of an independent copy of a $(2,3)$-threshold secret sharing scheme. Finally, he sends the shares associated to row j to S_j for $j \in \{1, 2, 3\}$.

Oblivious Transfer Phase. Let $X = \{2, 3\}$ be a 2-subset of $\{1, 2, 3\}$, denoting Servers S_2, S_3. Suppose that $\mathcal{R}$ wishes to recover the secret w_1. Hence, she chooses one of the columns $3, 4, 5$, say $c = 5$, and sends 0 to S_2 and 1 to S_3. The contacted Servers reply by sending the following values

- S_2 sends $(0, sh_{2,0}), (5, sh_{2,5})$ and $(7, sh_{2,7})$
- S_3 sends $(1, sh_{3,1}), (5, sh_{3,5})$ and $(6, sh_{3,6})$.

[3] A (k,m)-threshold secret sharing scheme is a method by means of which a dealer shares a secret among a set of m participants in such a way that: 1) any subset of participants of size greater than or equal to k reconstructs the secret; 2) any subset of size less than k does not get any information about the secret [40].

A One-Round (k, m)-DOT-$\binom{n}{1}$ Construction
Let $w_0, w_1, \ldots, w_{n-1} \in F_p$ be $\mathcal{S}$'s secrets, and let $i \in \{1, \ldots, n\}$ be $\mathcal{R}$'s choice.

Set-up Phase.

- The Sender $\mathcal{S}$ sets up an orthogonal array $OA_1(k, m+1, n)$. We denote the transpose of such an $OA_1(k, m+1, n)$ by I and we assume that it is public. The first row $I[0, \cdot]$ of I establishes "which column hides which secret".
- Then $\mathcal{S}$, for each $c \in \{0, \ldots, n^k - 1\}$, shares the secret $w_{I[0,c]}$ using a (k, m)-threshold secret sharing scheme. Let us denote the shares by $sh_{1,c}, \ldots, sh_{m,c}$. For each column is used a different scheme, i.e., threshold secret sharing schemes are independent.
- Finally, for $j = 1, \ldots, m$, $\mathcal{S}$ sends $sh_{j,0}, \ldots, sh_{j,n^k-1}$ to Server S_j.

Oblivious Transfer Phase

- Let $X = \{p_1, \ldots, p_k\}$ be a subset of k elements of $\{1, \ldots, m\}$. $\mathcal{R}$ chooses a random column c of the matrix I such that $I[0, c] = i$, and, for $j \in \{1, \ldots, k\}$, sends the value $y_j = I[p_j, c]$ to Server S_{p_j}.
- For $j \in \{1, \ldots, k\}$, Server S_{p_j} sends $(d, sh_{p_j,d})$ to the Receiver $\mathcal{R}$, for all d such that $I[p_j, d] = y_j$. $\mathcal{R}$ gets n shares from each of the k Servers.
- Finally, $\mathcal{R}$ applies the reconstruction function of the threshold secret sharing scheme to $sh_{p_1,c}, \ldots, sh_{p_k,c}$, and she reconstructs the secret w_i.

Table 7: A One-Round (k, m)-DOT-$\binom{n}{1}$ Construction

Therefore, the Receiver can recover w_1 using $(5, sh_{2,5})$ and $(5, sh_{3,5})$. ■

Correctness. The protocol satisfies Definition 4.1 since the Receiver, for any secret and for any column she has chosen to retrieve the secret, gets from the contacted Servers a sufficient number of shares. Indeed, assume that to recover w_i she has chosen column c and, without loss of generality, has sent for $j = 1, \ldots, k$, the value $y_j = I[j, c]$ to Server S_j. Then, she has received, among others, certainly the k pairs $(c, sh_{1,c}), \ldots, (c, sh_{k,c})$, enabling her to recover w_i.

Privacy. The privacy property, stated by Definition 2.2, can be shown as follows:

- Condition (5) is satisfied: Indeed, assume that $k-1$ Servers contacted by $\mathcal{R}$, say S_X where $X = \{1, \ldots, k-1\}$, collude in order to figure out the index i. If $\mathcal{R}$ has chosen column c to recover w_i, they have received the values $y_1 = I[1, c], \ldots, y_{k-1} = I[k-1, c]$. It is not difficult to see that, due to the structure of an $OA_1(k, m+1, n)$, this $(k-1)$-tuple appears along *any* k-restriction of the matrix exactly k times, and for each instance, the corresponding value of the k-th row is different. In particular, let us consider the k-restriction defined by rows $0, 1, \ldots, k-1$, i.e., the row which represents the indices of secrets and the rows associated with the Servers S_X. Since each instance of the $(k-1)$-tuple $y_1, \ldots, y_{k-1}$ is completed *exactly once* with a different value of y_0 in $\{0, \ldots, n-1\}$ (which represents an index of a possible secret), then using Bayes' theorem, it follows that $Prob(i|y_1,\ldots,y_{k-1}) = Prob(i)$. Since data D_X are independent of $y_1,\ldots,y_{k-1}$, it follows that $Prob(i|D_X, y_1,\ldots,y_{k-1}) = Prob(i|y_1,\ldots,y_{k-1})$.

- Condition (6) also holds: a coalition of $k-1$ Servers, say S_X where $X = \{1,\ldots,k-1\}$, does not get any information about any secret. Indeed, each secret is shared according to a (k,m) threshold secret sharing scheme. Let D_X be the set of pairs $\{(d, sh_{j,d})|j = 1,\ldots,k-1,$ and $d = 0,\ldots,n^k-1\}$. Due to the properties of secret sharing schemes, for any sequence of secrets w such that $Prob(w) > 0$, it holds that, $Prob(w|D_X) = Prob(w)$. Finally, since D_R are truly random bits independent of w and D_X, then $Prob(w|D_R, D_X) = Prob(w|D_X)$.

- Condition (7) holds due to the structure of an orthogonal array $OA_1(k, m+1, n)$. We need to consider only Case i). Indeed, for any index i and for any possible random string D_R, even if the Receiver's program is malicious, the integer values it sends to a set of Servers, say S_X where $X = \{1,\ldots,k-1\}$, uniquely identify a column $j \in \{0,\ldots,n^k-1\}$ and the corresponding index $\tilde{i} \in \{0,\ldots,n-1\}$. Then, $\mathcal{R}$, from some of the shares received as reply to the values she sends to the Servers S_X, belonging to the restriction of a column j of the orthogonal array, reconstructs $w_{\tilde{i}}$. However, analysing the remaining shares, she misses *at least one share* needed to recover the secret associated to any other column. More precisely, for $j = 1,\ldots,k$, denote by $Values_j$ the set of pairs $\{(d, sh_{j,d})|I[j,d] = y_j$ for $d = 0,\ldots,n^k-1\}$. Then, the transcript C_X of the interaction with the Servers S_X is equal to $(y_1,\ldots,y_k, Values_1,\ldots,Values_k)$. It holds that $Prob(w|i, D_R, C_X, w_{\tilde{i}}) = Prob(w|w_{\tilde{i}})$.

Server memory storage and communication complexity of the combinatorial schemes are quite heavy. The following technique enables us to reduce both resources. Indeed, looking at the protocol described in Table 6 in the particular case of 2 secrets, notice that it is not necessary that *all* the $k \times 2^k$ values $a_{i,j}$ are independent. For example, they can be chosen in such a way that the following relation holds: let j and j' be two different columns of the matrix A whose binary representations are $b_1^j \ldots b_k^j$ and $b_1^{j'} \ldots b_k^{j'}$. Then, for $i = 1,...,k$, let

$$A[i,j] = A[i,j'] \text{ if and only if } b_1^j = b_1^{j'},\ldots,b_i^j = b_i^{j'}.$$

Let us consider an example assuming that $k = 3$. For 3 Servers, we have:

000	001	010	011	100	101	110	111
$a_{1,0}$	$a_{1,1}$	$a_{1,2}$	$a_{1,3}$	$a_{1,4}$	$a_{1,5}$	$a_{1,6}$	$a_{1,7}$
$a_{2,0}$	$a_{2,1}$	$a_{2,2}$	$a_{2,3}$	$a_{2,4}$	$a_{2,5}$	$a_{2,6}$	$a_{2,7}$
$a_{3,0}$	$a_{3,1}$	$a_{3,2}$	$a_{3,3}$	$a_{3,4}$	$a_{3,5}$	$a_{3,6}$	$a_{3,7}$

The values $a_{i,j}$ can be grouped as

$$a_{1,0} = a_{1,1} = a_{1,2} = a_{1,3}, \text{ and } a_{1,4} = a_{1,5} = a_{1,6} = a_{1,7}$$

for the first row,

$$a_{2,0} = a_{2,1},\ a_{2,2} = a_{2,3},\ a_{2,4} = a_{2,5}, \text{ and } a_{2,6} = a_{2,7}$$

for the second row, and

$$a_{3,0},\ a_{3,1},\ a_{3,2},\ a_{3,3},\ a_{3,4},\ a_{3,5},\ a_{3,6},\ a_{3,7}$$

for the third row. In this example, Server S_1 gets 2 values, Server S_2 gets 4 values and Server S_3 gets 8 values. Hence, Server memory storage and communication complexity are reduced. An interesting open problem is to find more efficient representations for the matrix of values.

A Protocol for General Access Structures. The main idea underlying the combinatorial schemes is that an orthogonal array is used as an *indexing structure* for several sharings of the secrets[4]. We can pursue the same idea in order to support general access structures.

Let us start by informally clarifying the notion of DOT for a general access structure.

Let $S = \{S_1, \ldots, S_m\}$ be a set of Servers. An access structure $\mathcal{A}$ on S is a collection of subsets $\mathcal{A} \subseteq 2^S \backslash \{\emptyset\}$. An $\mathcal{A}$-DOT-$\binom{n}{1}$ is a protocol satisfying the following requirements:

- Correctness. From each subset $A \in \mathcal{A}$, called qualified, the Receiver $\mathcal{R}$ gets enough information to recover any one of the secrets at her choice.
- Receiver's Privacy. Any subset $A \notin \mathcal{A}$, called forbidden, does not get any information about the index of the secret $\mathcal{R}$ recovers.
- Sender's Privacy w.r.t. a forbidden subset and the Receiver. A coalition of the Receiver and a subset of Servers $A \notin \mathcal{A}$, does not get any information about the n secrets.
- Sender's Privacy w.r.t. a "Greedy" Receiver. Given the transcript of the interaction with a subset of Servers $A \in \mathcal{A}$, the Receiver gets information about at most a single secret, and no information about the others. This property holds even if the Receiver, once has computed a secret, colludes with $A \notin \mathcal{A}$, a subset of dishonest Servers.

A formal definition of an $\mathcal{A}$-DOT-$\binom{n}{1}$ can be stated along the same lines of Definitions 2.1 and 2.2.

To explain the protocol and how to construct the *indexing structure*, let us consider a simple case. Let $S = \{S_1, S_2, S_3, S_4\}$ be a set of 4 Servers, and let $\mathcal{P}_3 = \{\{S_1, S_2\}, \{S_2, S_3\}, \{S_3, S_4\}\}$ be an access structure on the set of Servers S. This access structure is well-known in the secret sharing scheme theory and its information rate ρ, which is the maximum ratio between the size of the secret and the size of the share given to the user[5], is equal to $\frac{2}{3}$. Assume that the secret is a pair of values (k_1, k_2) belonging to $F_{p'} \times F_{p'}$. The secret can be shared among $\mathcal{P}_3$ as shown in Table 8.

Servers	Shares for:	(k_1, k_2)	
S_1	x,	z	
S_2	$k_1 + x \bmod p'$,	$k_2 + z \bmod p'$,	w
S_3	$k_1 + w \bmod p'$,	$k_2 + y \bmod p'$,	z
S_4	w,	y	

Table 8: A secret sharing scheme for $\mathcal{P}_3$.

[4]Indeed, notice that also the constructions given in Table 6, can be re-phrased along the same line of the protocol described in Table 7. In this case the orthogonal array used is an $OA_1(k, k+1, n)$.

[5]The reader is referred to [42] for background on secret sharing schemes.

The values x, y, z, and w are random values chosen in $F_{p'}$. The dealer computes the shares given in Table 8 and sends row i to Server S_i.

We can construct a $\mathcal{P}_3$-DOT-$\binom{n}{1}$ using this secret sharing scheme as building block. More precisely, each secret is shared many times with different instances of the secret sharing scheme. At the same time, an indexing matrix which represents all these sharings can be setup using as "rule" to fill in the entries of each column the same secret sharing scheme.

To exemplify, assume that we have $9 = 3^2$ secrets. Each secret (k_i, k_j) can be indexed by $(i, j) \in F_3 \times F_3$. An indexing matrix I can be set up considering 3^4 sharings for each key (i.e., the number of possible choices for x, y, z, and w when seen as elements belonging to F_3). For example, the restriction of the indexing matrix I to the key (k_1, k_2) indexed by $(1, 2)$ is reported in Table 9.

	$(\mathbf{1}, \mathbf{2})$			$\cdots$	$(\mathbf{1}, \mathbf{2})$		
S_1	0,	0		$\cdots$	2,	2	
S_2	1,	2,	0	$\cdots$	0,	1,	2
S_3	1,	2,	0	$\cdots$	0,	1,	2
S_4	0,	0,		$\cdots$	2,	2	

Table 9: Partial view of the indexing matrix I, corresponding to the 3^4 sharings of the secret (k_1, k_2).

Notice that, the share for S_2 corresponding to the first sharing of $(1, 2)$ is $(1, 2, 0)$. Indeed, it is easy to check that choosing $x = 0, y = 0, z = 0$, and $w = 0$ it holds that $1 + 0 \bmod 3 = 1, 2 + 0 \bmod 3 = 2$, and $0 \bmod 3 = 0$. Similarly, the share for S_2 corresponding to the last sharing of $(1, 2)$ is $(0, 1, 2)$. Indeed, it is easy to check that choosing $x = 2, y = 2, z = 2$, and $w = 2$, it holds that $1 + 2 \bmod 3 = 0, 2 + 2 \bmod 3 = 1$, and $2 \bmod 3 = 2$.

In Table 9, each of the 3^4 columns indexed by $(1, 2)$ represents a sharing of $(k_1, k_2) \in F_{p'} \times F_{p'}$. We assume that the $3^2 \cdot 3^4$ sharings for the 3^2 secrets are maintained in another (corresponding) matrix A: more precisely, each column of A contains a sharing of a certain key (k_i, k_j) (see Table 10).

	(k_1, k_2)	$\cdots$	(k_1, k_2)
S_1	$sh^{(1,2)}_{(0,0)}$	$\cdots$	$sh^{(1,2)}_{(2,2)}$
S_2	$sh^{(1,2)}_{(1,2,0)}$	$\cdots$	$sh^{(1,2)}_{(0,1,2)}$
S_3	$sh^{(1,2)}_{(1,2,0)}$	$\cdots$	$sh^{(1,2)}_{(0,1,2)}$
S_4	$sh^{(1,2)}_{(0,0)}$	$\cdots$	$sh^{(1,2)}_{(2,2)}$

Table 10: Partial view of the matrix A, containing the 3^4 sharings of the secret (k_1, k_2).

The Receiver can choose one of the column of I and can ask a subset $B \in \mathcal{P}_3$ to receive the shares in A, whose indices match the entries of the column of the matrix I, in correspondence of the Servers in B. In our example, the Receiver, to retrieve (k_1, k_2), can choose the first column of the partial view of matrix I and can send $(1, 2, 0)$ to S_3 and $(0, 0)$ to S_4, receiving from S_3 all the shares (belonging to the third row of matrix A) whose indices are $(1, 2, 0)$ (and, among these, surely $sh^{(1,2)}_{(1,2,0)}$), and from S_4 all the shares (belonging to the fourth row of matrix A) whose indices are $(0,0)$ (and, among these, surely $sh^{(1,2)}_{(0,0)}$).

It is not difficult to see that the construction is correct, due to the reconstruction property of the secret sharing scheme. In our example $sh^{(1,2)}_{(1,2,0)}$ and $sh^{(1,2)}_{(0,0)}$ enable the Receiver to recover (k_1, k_2). Moreover the scheme is private since, from each subset of Servers belonging to $\mathcal{P}_3$, the Receiver can recover one and only one secret of her choice, getting no information on the others. On the other hand, a forbidden subset of Servers $F \notin \mathcal{P}_3$ neither get information about the secret $\mathcal{R}$ wishes to recover from the values sent by her nor can compute information about any secret, due to the security property of the secret sharing scheme.

Notice that, if we have $n = p^2$ secrets, the construction seen before requires p^4 sharing for each secret, and an indexing matrix I with p^6 columns.

At this point it is not difficult to figure out how the same strategy can be applied to any access structure. We would like just to point out the use of the secret sharing for the construction of *both* the indexing structure I and the sharing of the secrets. Perhaps this design technique can be applied successfully also to other cryptographic protocols. The protocol can be generalized to *arbitrary* access structures $\mathcal{A}$ on the set of Servers.

Let $n = p^r$ and, for $i = 1, \ldots, n$, let $w_i \in F^r_{p'}$ be $\mathcal{S}$'s secrets. Let each index i be represented by $(i_1, \ldots, i_r) \in F^r_p$. Moreover, let $\mathcal{A}$ be an access structure on the set of the m Servers, and let Σ be a secret sharing scheme for $\mathcal{A}$ with information rate $\rho = \frac{r}{u}$ represented, as before, in tabular form. Finally, assume that Σ uses, to share a secret, t random values belonging to $F_{p'}$. The protocol is described in Tables 11 and 12.

In order to show the correctness and the privacy of the protocol it is enough to prove that the indexing structure, given by the matrix I, satisfies the *same properties* of an orthogonal array, the combinatorial structure we have used in the threshold case. Indeed, notice that, when the general access structure considered in the above construction is a threshold structure, a secret sharing scheme with information rate $\rho = 1$ (called *ideal* [42]), i.e., where each share has the same size of the secret, realizing the access structure does exist. As shown by K. Martin [32] and, independently by Dawson et al. [19], if we represent such a secret sharing scheme by means of a distribution table, this table is exactly an orthogonal array. For the general case, a proof that the indexing structure satisfies the same properties of an orthogonal array can be achieved arguing by contradiction: for any fixed set of rows of the matrix I, corresponding to a qualified subset of Servers, if two different columns j and j' have the same t-tuples, row by row, then $j = j'$, due to the matrix generation rule. The correctness and privacy properties of the DOT construction easily follow from the same observations we have made in analysing the threshold case.

Remark. Notice that all results and bounds presented in Sections 3 and 4, by using standard techniques, can be opportunely stated and proved for DOT schemes for general access structures. In particular, concerning with one-round protocols, Theorem 4.4 can be easily extended to $\mathcal{A}$-DOT-$\binom{n}{1}$. If X denotes a subset of indices of Servers such that $S_X \notin \mathcal{A}$ but $S_X \cup \{S_j\} \in \mathcal{A}$, where $j \notin X$, an adversary, given only D_j and (Q_X, A_X), can compute all the secrets.

6.2 Two-Round Constructions

It is possible to gain in terms of privacy and efficiency of computations if we allow *one more round* of interaction between the Receiver and the Servers. A simple protocol is described in Table 13.

A One-Round $\mathcal{A}$-DOT-$\binom{n}{1}$ Protocol.

Set-up Phase

- $\mathcal{S}$ sets up a public indexing matrix I, of order $(m+1) \times p^{r+t}$, which *represents*, for each of the p^r secrets, p^t different sharings according to Σ. The matrix I is filled in as follows: the first row says which secret the column hides. More precisely, for $i = 1, \ldots, p^r$ and $j = 1, \ldots, p^t$, the value $I[0, j + (i-1)p^t] = i = (i_1, \ldots, i_r)$. Then, for $q = 1, \ldots, m$, the entry $I[q, j + (i-1)p^t]$ represents the index of the share given to Server S_q for the j-th sharing of the i-th secret, and is equal to $(v^j_{q,1}, \ldots, v^j_{q,\ell_i}) \in F_p^{\ell_i}$ where $\ell_i \leq u$, These values are computed using Σ as "rule", and by considering $(i_1, \ldots, i_r)$ (i.e., the representation of i in F_p^r) *as the secret*, and all possible sequences $(d_1, \ldots, d_t) \in F_p^t$. These sequences correspond to the p^t random values belonging to $F_{p'}$, used by Σ to generate the p^t sharings for w_i.
- Once the indexing matrix has been set up, for each secret $w_i \in (F_{p'})^r$, $\mathcal{S}$ computes the p^t sharings. Let us denote, for the j-th sharing of the secret, by

  $$sh^i_{(v^j_{q,1},\ldots,v^j_{q,\ell_i})}$$

  the share for Server S_q according to Σ. We assume that a matrix A, of order $m \times p^{r+t}$, contains in each column one of such sharings.
- For $i = 1, \ldots, n$, for $q = 1, \ldots, m$, and for $j = 1, \ldots, p^t$, $\mathcal{S}$ sends to Server S_q the share $sh^i_{v^j_{q,1},\ldots,v^j_{q,\ell_i}}$, i.e., all the shares belonging to the q-th row of the matrix A.

Table 11: A One-Round $\mathcal{A}$-DOT-$\binom{n}{1}$ Protocol: Set up Phase

Correctness. The Receiver, once she has received all the values of a column, computes the secret by means of a simple sum.

Privacy (sketch). The Privacy property, stated by Definition 2.2, can be shown developing the following arguments:

- Condition (5) of Definition 2.2 is satisfied because a coalition of $k-1$ Servers does not get any information about which secret $\mathcal{R}$ wishes to recover, since the $k-1$ Servers do not know which secret is hidden by which vector.
- Condition (6) holds because the Receiver and a coalition of $k-1$ Servers, does not get any information about any secret. Indeed, each secret is actually shared according to a (k,k) threshold secret sharing scheme, and they hold only $k-1$ shares for each of them.
- Condition (7) holds because the Receiver $\mathcal{R}$ can retrieve at most one secret: Indeed, *all* the values of a single vector are needed for computing one of the secrets. Hence, if she gets all the values of a vector, then she gets no information about the secret hidden by the other vector. On the other hand, if she gets values belonging to the two different vectors from different Servers, then she gets no information on *both* secrets at all.

A One-Round $\mathcal{A}$-DOT-$\binom{n}{1}$ Protocol.

Oblivious Transfer Phase

- $\mathcal{R}$, to recover w_i, chooses a column of I say the g-th one, such that $I[0,g] = (i_1, \ldots i_r)$, chooses a subset of Servers $B \in \mathcal{A}$ and sends, to each $S_q \in B$, the tuple $y^q = I[q,g]$.
- Each Server $S_q \in B$ sends to $\mathcal{R}$, for any column z such that $I[q,z] = y^q$, the pair column-share $(z, A[q,z])$.
- $\mathcal{R}$ reconstructs the secret by using the pairs $(g, A[q,g])$ sent by Servers $S_q \in B$.

Table 12: A One-Round $\mathcal{A}$-DOT-$\binom{n}{1}$ Protocol: Oblivious Transfer Phase

It is worthwhile to point out that the two-round construction above described enjoys condition (11) of Definition 2.3, i.e., the further privacy property that is impossible to achieve using a one-round protocol: Indeed, a coalition of $k-1$ Servers and the Receiver, after the latter has recovered one of the secrets, still cannot compute the other without the help of the last Server, due to the sharing of secrets by means of a (k,k) secret sharing scheme.

Notice that, if we compress the above protocol into one round, we can obtain a *random* DOT where the Receiver *can recover one secret but she cannot choose which one.* This functionality can be realized if the Servers simply send to the Receiver the "addressing bits", that is r_j's, and *all but one* of the values $v_0[j]$ and $v_1[j]$, for $j = 1, \ldots, k$. In such a case, one of the Servers, say S_j, chooses uniformly at random which of the two values $v_0[j], v_1[j]$ to send $\mathcal{R}$.

The above protocol can be extended to realize a DOT for a *general access structure* on the set of Servers as well as a DOT for any number of secrets. The extensions can be done as follows: in order to implement a DOT for a general access structure $\mathcal{A}$ on the set of Servers, say an $\mathcal{A}$-DOT-$\binom{2}{1}$, the bit r, which establishes which vector hides w_0, is shared among the m Servers, according to a secret sharing scheme for $\mathcal{A}$. Then, if $r = 0$, the secret w_0 is shared by the first vector and w_1 by the second, according to a secret sharing scheme for $\mathcal{A}$; otherwise, w_0 is shared by the second vector and w_1 by the first. Once the Receiver has recovered the value of r, contacting a subset of Servers belonging to $\mathcal{A}$, she can recover one of the secrets by sending a request for shares to the same subset of Servers that were contacted before.

On the other hand, an $\mathcal{A}$-DOT-$\binom{n}{1}$ requires that, instead of a bit, r is a value in $\{0, \ldots, n-1\}$ and, instead of two vectors sharing w_0 and w_1, there are exactly n vectors $v_0, \ldots, v_{n-1}$, sharing the secrets $w_0, \ldots, w_{n-1}$, respectively. The value r, shared among the Servers through a secret sharing scheme for $\mathcal{A}$, establishes the correspondence between the vectors and the n secrets. In other words, if $r = 2$ then the third vector v_2 shares w_0, the fourth shares w_1, and so on, following a cyclic order modulo n. Applying the same argument described before for the case of two secrets, it is not difficult to show that also this is correct and private.

A Strong (k,k)-DOT-$\binom{2}{1}$
Let $w_0, w_1 \in F_p$ be $\mathcal{S}$'s secrets.

Set-up Phase.

- $\mathcal{S}$ chooses k random bits r_j, and computes the bit r, xoring the r_j's, i.e., $r = \bigotimes_{j=1}^{k} r_j$.
- Moreover, $\mathcal{S}$ sets up two vectors with k entries in F_p, v_0 and v_1, choosing the first $k-1$ entries at random and computing

$$v_0[k] = w_r - \sum_{j=1}^{k-1} v_0[j] \bmod p, \text{ and } v_1[k] = w_{1-r} - \sum_{j=1}^{k-1} v_1[j] \bmod p.$$

- Then, for $j = 1, \ldots, k$, he sends the bit r_j and the values $v_0[j]$ and $v_1[j]$ to Server S_j.

Oblivious Transfer Phase.

- In a first round of communication, $\mathcal{R}$ asks to each Server S_j the bit r_j, and computes r. Then, for $j = 1, \ldots, k$, if $\mathcal{R}$ is interested in w_0 and $r = 0$, asks Server S_j the value $v_0[j]$; otherwise, if $r = 1$, asks $v_1[j]$. Symmetrically, to recover w_1, if $r = 1$, she asks $v_0[j]$, while if $r = 0$, she asks $v_1[j]$.
- Finally, $\mathcal{R}$ sums up mod$p$ the received values.

Table 13: A Two-Round (k,k)-DOT-$\binom{2}{1}$

7 Data to the Receiver

In this section we consider the setting in which the Receiver holds some data. More precisely, we assume that during the setup phase, the Sender $\mathcal{S}$ sends data not only to the m Servers but *also to the Receiver* $\mathcal{R}$. Intuitively, by giving information to the Receiver we should be able to achieve a stronger privacy condition. The two-round protocol described in Table 13 (and all its generalizations) can be transformed in a one-round protocol for the new model. Indeed, notice that the random bit each Server transmits to the Receiver during the first round, can be eliminated if the Sender, during the set up, privately says to the Receiver which vector which secret hides (see Table 14).

Notice that, $k-1$ Servers do not have any information about the secrets. At the same time, the Receiver is still not able to gain extra-information about other secrets, apart the one that she recovers honestly. Actually the above protocol is very simple: each secret is shared according to a (k,k) threshold scheme and *only* the Receiver knows which shares correspond to which secret. The generalization of the above protocols to the case of a general access structure on the set of Servers and to n secrets can be done along the same line of the two-round protocol without information in set up phase to the Receiver.

We point out that the protocol given in Table 14 shows also that the results of Section 4 do not hold if D_R is information sent by the Sender to the Receiver in set-up phase. Indeed, $D_1, \ldots, D_k$ and D_R are related, the lower bound on the size of D_R given by Theorem 4.11 is not satisfied, and the protocol realizes a strong (k,k)-DOT-$\binom{2}{1}$.

A Strong (k,k)-DOT-$\binom{2}{1}$ with information to the Receiver
Let $w_0, w_1 \in F_p$ be $\mathcal{S}$'s secrets.

Set-up Phase

- $\mathcal{S}$ chooses a random bit, say r.
- Then, $\mathcal{S}$ sets up two vectors with entries in F_p, v_0 and v_1, choosing the $k-1$ entries at random and computing

$$v_0[k] = w_r - \sum_{j=1}^{k} v_0[j] \bmod q, \text{ and } v_1[k] = w_{1-r} - \sum_{j=1}^{k} v_1[j] \bmod q.$$

- Finally, for $j = 1, \ldots, k$, $\mathcal{S}$ sends the values $v_0[j]$ and $v_1[j]$ to Server S_i and the bit r to $\mathcal{R}$.

Oblivious Transfer Phase

- If $\mathcal{R}$ is interested in w_0 and $r = 0$, then, for $j = 1, \ldots, k$, asks to Server S_j the value $v_0[j]$; otherwise, if $r = 1$, asks $v_1[j]$. Symmetrically, to recover w_1, if $r = 0$, she asks $v_1[j]$, while if $r = 1$, she asks $v_0[j]$.
- Then, $\mathcal{R}$ sums up mod$q$ the received values v_i with r_i, recovering the secret.

Table 14: One-Round (k,k)-DOT-$\binom{2}{1}$

8 Applications

The protocols described before have several interesting applications and connections with other cryptographic protocols. Let us quickly describe some of them.

Privacy Preserving Auctions and Mechanism Design [36]. The notion of DOT was introduced in [34] to improve the protocol of [36]. More precisely, in that protocol, there are three parties: an auctioneer, many bidders, and an agency supporting the auction. The auctioneer advertises the auction and its rules. The bidders submit their bids in "encrypted form" to the auctioneer, and the auctioneer, with the help of the agency, can compute the winner of the auction in such a manner that the privacy of the bidders (i.e., non-essential information about their own bids) is preserved. The weak point of the protocol is that if *the auctioneer and the agency collude*, then the privacy of the bids is lost. In order to strengthen the protocol, the agency can be split in two parts: a central agency, that operates only in a set up phase, and m Servers, with which the auctioneer communicates in order to compute the auction. In this case the auctioneer needs to collude with k out of the m Servers in order to violate the privacy of the bidders. The impossibility result for one-round (k,m) protocols private against a coalition of $k-1$ Servers and the Receiver we have shown in Section 4, in this setting means that the highest degree of privacy sought for in [36] with this approach cannot be achieved. On the positive side, the two-round protocols described in Section 6 can be applied to this framework but the *communication pattern* changes and some more details must be taken into account.

Symmetric Private Information Retrieval. Distributed Oblivious Transfer protocols have connections with symmetric private information retrieval schemes [25]. A PIR scheme [12] enables a user to retrieve an item of information from a public accessible database in such a way that the database manager cannot figure out from the query which item the user is interested in. However, the user can get information about more than one item. On the other hand, in SPIR (Symmetric Private Information Retrieval) schemes [25], the user can get information about *one and only one* item, i.e. even the privacy of the database is considered. In PIR and SPIR schemes, the emphasis is placed on the *communication complexity* of the interaction of user and Servers. Therefore, a SPIR Scheme can be seen as a *communication-efficient* 1-out-of-n oblivious transfer scheme. The main differences between the model we have considered and (information theoretic) SPIR schemes are that in SPIR schemes the Receiver communicates with k out of k Servers in order to retrieve an item while in our setting the Receiver can choose k out of m Servers, where $k \leq m$. This property is useful since it guarantees a sort of *Robustness* for the SPIR scheme, in the sense that even if some Server crashes, the item can still be retrieved by the user by means of the other available ones. Hence, *a communication-efficient threshold DOT scheme realizes a robust SPIR scheme*. Another important difference is that in information theoretic PIR and SPIR schemes the database is *replicated* among the Servers. Hence, every Server knows the content. In our model only a k-subset of Servers can reconstruct the database.

Another interesting relation of the DOT model we have studied is with information theoretic PIR schemes with preprocessing [2]. The set up phase performed by the dealer can be seen as the preprocessing stage performed by the database owner in [2]. The combinatorial constructions we have shown are communication-inefficient but they require trivial computation for the Servers, once the scheme has been set up.

Just to emphasize the connection, notice that, using the DOT constructions presented in Section 7, we can set up a robust unconditionally secure symmetric private retrieval scheme. The database $\mathcal{D}$ is simply distributed by the owner among m Servers, according to the (k, m)-DOT scheme for n secrets of Section 7.

9 Conclusions

In this paper we have studied unconditionally secure distributed oblivious transfer protocols. We have presented lower bounds on the resources required to implement such protocols, some impossibility results for one-round schemes, and new constructions which are optimal with respect to some of the given bounds. Moreover, we have shown that with a second round of interaction the highest possible privacy level in this model can be achieved with, at the same time, a suitable reduction of resources (randomness, memory storage and communication complexity). The same effect can be achieved modifying the model for DOT by allowing the Sender to send information during the set up phase even to the Receiver. In this case the two-round protocol we have shown in the previous section can be simply transformed in a one-round protocol. This is another example of a tradeoff. Several questions and interesting open problems come up from this study. Among others:

- The design of a one-round DOT protocol meeting all the bounds given by the information theoretic analysis.
- Techniques to improve the communication complexity of some of the presented schemes with application to SPIR with preprocessing.

- Identification of applicative settings which can benefit from this distributed implementation of the oblivious transfer.

10 Acknowledgment

We thank the anonymous referee for his helpful comments and suggestions.

D. R. Stinson's research is supported by the Natural Sciences and Engineering Research Council of Canada (NSERC) through grant RGPIN 203114 − 02.

The work described in this paper has been supported in part by the European Commission through the IST Programme under Contract IST-2002-507932 ECRYPT. The information in this document reflects only the author's views, is provided as is and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

References

[1] D. Beaver, J. Feigenbaum, J. Kilian, and P. Rogaway, *Locally Random Reductions: Improvements and Applications*, Journal of Cryptology, vol. 10, No.1, pp. 17-36, 1997.

[2] A. Beimel, Y. Ishai, and T. Malkin, *Reducing the Servers Computation in Private Information Retrieval: PIR with Preprocessing*, Advances in Cryptology: Proceedings of Crypto 2000, LNCS, Springer-Verlag, vol. 1880, pp. 55-73, 2000.

[3] M. Bellare and S. Micali, *Non-interactive Oblivious Transfer and Applications*, Advances in Cryptology: Proceedings of Crypto 1989, LNCS, Springer-Verlag, vol. 435, pp. 547-559, 1990.

[4] G. R. Blakley, *Safeguarding Cryptographic Keys*, Proceedings of AFIPS National Computer Conference, Vol. 48, pp. 313–317, 1979.

[5] M. Blum, *How to Exchange (Secret) Keys*, ACM Transactions of Computer Systems, vol. 1, No. 2, pp. 175-193, 1993.

[6] C. Blundo, A. De Santis, and U. Vaccaro, *Randomness in Distribution Protocols*, Information and Computation, vol. 131, No. 2, pp. 111–139, 1996.

[7] C. Blundo, B. Masucci, D.R. Stinson and R. Wei, *Constructions and Bounds for Unconditionally Secure Non-Interactive Commitment Schemes*, Designs, Codes, and Cryptography, vol. 26, pp. 97–110, 2002.

[8] G. Brassard, C. Crepéau, and J.-M. Roberts, *Information Theoretic Reductions Among Disclosure Problems*, Proceedings of 27th IEEE Symposium on Foundations of Computer Science, pp. 168-173, 1986.

[9] G. Brassard, C. Crepéau, and J.-M. Roberts, *All-or-Nothing Disclosure of Secrets*, Advances in Cryptology: Proceedings of Crypto 1986, LNCS, Springer-Verlag, vol. 263, pp. 234-238, 1987.

[10] G. Brassard, C. Crepéau, and M. Sántha, *Oblivious Transfer and Intersecting Codes*, IEEE Transaction on Information Theory, Special Issue in Coding and Complexity, Vol. 42, No. 6, pp. 1769-1780, 1996.

[11] R.M. Capocelli, A. De Santis, L. Gargano and U. Vaccaro, *On the Size of the Shares in Secret Sharing Schemes*, Advances in Cryptology: Proceedings of Crypto 1991, LNCS, vol. 576, pp. 101–113, 1992.

[12] B. Chor, O. Goldreich, E. Kushilevitz, and M. Sudan, *Private Information Retrieval*, Proceedings of the 36th IEEE Symposium on Foundations of Computer Science (FOCS), pp. 41–50, 1995.

[13] T. M. Cover and J. A. Thomas, **Elements of Information Theory**, John Wiley & Sons, 1991.

[14] C. Crepéau, *Equivalence between to flavors of oblivious transfers*, Advances in Cryptology: Proceedings of Crypto 1987, LNCS, Springer Verlag, vol. 293, pp. 350-354, 1988.

[15] C. Crepéau, *A Zero-Knowledge Poker Protocol that achieves confidentiality of the players' strategy or how to achieve an electronic poker face*, Advances in Cryptology: Proceedings of Crypto 1986, LNCS, Springer-Verlag, vol. 263, pp. 239-247, 1987.

[16] G. Di Crescenzo, T. Malkin, and R. Ostrovsky, *Single Database Private Information Retrieval Implies Oblivious Transfer*, Advances in Cryptology: Proceedings of Eurocrypt 2000, LNCS, Springer-Verlag, vol. 1807, pp. 122-138, 2000.

[17] G. Di Crescenzo, Y. Ishai, and R. Ostrovsky, *Universal Service-Providers for Database private Information Retrieval*, Proceedings of 17th Annual ACM Symposium on Principles of Distributed Computing (PODC), 1998.

[18] P. D'Arco and D.R. Stinson, *Generalized Zig-zag Functions and Oblivious Transfer Reductions*, Selected Areas in Cryptography SAC 2001, LNCS, Springer Verlag, vol. 2259, pp. 87-103, 2001.

[19] E. Dawson, E. S. Mahmoodian and A. Rahilly, *Orthogonal arrays and ordered threshold schemes*, Australasian Journal of Combinatorics, No. 8, pp. 27–44, 1993.

[20] A. De Santis and G. Persiano, *Public-Randomness in Public Key Cryptography*, Advances in Cryptology: Proceedings of Eurocrypt 1990, LNCS, Springer-Verlag, vol. 437, pp. 46–62, 1990.

[21] A. De Santis, G. Di Crescenzo, and G. Persiano, *Zero-Knowledge Arguments and Public Key Cryptography*, Information and Computation, vol. 121, no. 1, pp. 23-40, 1995.

[22] Y. Dodis and S. Micali, *Lower Bounds for Oblivious Transfer Reduction*, Advances in Cryptology: Proceedings of Eurocrypt 1999, LNCS, Springer Verlag, vol. 1592, pp. 42-54, 1999.

[23] S. Even, O. Goldreich, and A. Lempel, *A Randomized Protocol for Signing Contracts*, Communications of the ACM, Vol. 28, pp. 637-647, 1985.

[24] M. Fisher, S. Micali, and C. Rackoff, *A Secure Protocol for the Oblivious Transfer*, Journal of Cryptology vol. 9, No 3, pp. 191-195, 1996.

[25] Y. Gertner, Y. Ishai, E. Kushilevitz, and T. Malkin, *Protecting Data Privacy in Private Information Retrieval Schemes*, Proc. of the 30th Annual ACM Symposium on Theory of Computing (STOC), pp. 151-160, 1998.

[26] Y. Gertner, S. Goldwasser, and T. Malkin, *A Random Server Model for Private Information Retrieval or How to Achieve Information Theoretic PIR Avoiding Database Replication*, Proceedings of RANDOM 1998, LNCS, Springer Verlag, vol. 1518, pp. 200-217, 1998.

[27] Y. Gertner, S. Kannan, T. Malkin, O. Reingold, and M. Viswanathan, *The Relationship between Public Key Encryption and Oblivious Transfer*, Proceedings of the 41st Annual Symposium on Foundations of Computer Science (FOCS 2000), pp. 325-339, 2000.

[28] O. Goldreich, S. Micali, and A. Wigderson, *How to play ANY mental game or: A Completeness Theorem for Protocols with Honest Majority*, Proceedings of 19th Annual Symposium on Theory of Computing, pp. 20-31, 1987.

[29] A.S. Hedayat, N.J.A Sloane, and J. Stufken, **Orthogonal Arrays: Theory and Applications**, Springer Verlag, 2001.

[30] J. Kilian, *Founding Cryptography on Oblivious Transfer*, Proceedings of the 20th Annual Symposium on Theory of Computing, pp. 20-31, 1988.

[31] D. E. Knuth and A. C. Yao, *The Complexity of Nonuniform Random Number Generation*, Algorithms and Complexity, Academic Press, pp. 357–428, 1976.

[32] K. Martin, *Discrete Structures in the Theory of Secret Sharing*, PhD Thesis, University of London, 1991.

[33] M. Naor and B. Pinkas, *Computationally Secure Oblivious Transfer*, Advances in Cryptology: Proceedings of Crypto 1999, LNCS, Springer-Verlag, vol. 1666, pp. 205-219, 2000.

[34] M. Naor and B. Pinkas, *Distributed Oblivious Transfer*, Advances in Cryptology: Proceedings of Asiacrypt 2000, LNCS, Springer-Verlag, vol. 1976, pp. 205-219, 2000.

[35] M. Naor and B. Pinkas, *Efficient Oblivious Transfer Protocols*, Proceedings of SODA 2001, pp. 448-457, 2001.

[36] M. Naor, B. Pinkas, and R. Sumner, *Privacy Preserving Auctions and Mechanism Design*, proceedings of ACM Conference on Electronic Commerce, pp. 129–139, 1999.

[37] V. Nikov, S. Nikova, B. Preneel, and J. Vandewalle, *On Unconditionally Secure Distributed Oblivious Transfer*, Progress in Cryptology: Proceedings of Indocrypt 2002, LNCS, Springer-Verlag, vol. 2551, pp. 395–408, 2002.

[38] M. Rabin, *How to Exchange Secrets by Oblivious Transfer*, Technical Memo TR-81, Aiken Computation Laboratory, Harvard University, 1981.

[39] R. Rivest, *Unconditionally Secure Committment and Oblivious Transfer Schemes Using Private Channels and a Trusted Initializer*, manuscript. Available: http://theory.lcs.mit.edu/∼rivest/publications.html

[40] A. Shamir, *How to Share a Secret*, Communications of ACM, vol. 22, n. 11, pp. 612–613, 1979.

[41] D. R. Stinson and R. Wei, *Bibliography on Secret Sharing Schemes.* http://www.cacr.math.uwaterloo.ca/∼dstinson/ssbib.html.

[42] D. R. Stinson, *An Explication of Secret Sharing Schemes*, Designs, Codes, and Cryptography, Vol. 2, pp. 357–390, 1992.

[43] W. Tzeng, *Efficient* 1*-out-of-n Oblivious Transfer Schemes*, Proceedings of PKC 2002, LNCS, Springer Verlag, Vol. 2274, pp. 159–171, 2002.

[44] S. Wiesner, *Conjugate Coding*, SIGACT News 15, pp. 78-88, 1983.

A Information Theory Elements

In this appendix we briefly recall some concepts of information theory. The reader is referred to [13] for details.

A *discrete random experiment* is defined by a finite set, called *sample space*, consisting of all elementary events, and a *probability measure* assigning a non-negative real number to every elementary event, such that the sum of all these probabilities is equal to 1. An *event* of a discrete random experiment is a subset of the sample space, and the probability assigned to it is the sum of the probabilities of its elementary events.

A *discrete random variable* $\mathbf{X}$ is a mapping from a sample space to a certain range X, and is characterized by its probability distribution $\{P_{\mathbf{X}}(x)\}_{x\in X}$ that assigns to every $x \in X$ the probability $P_{\mathbf{X}}(x)$ of the event that $\mathbf{X}$ takes on the value x.

The *entropy* of $\mathbf{X}$, denoted by $H(\mathbf{X})$, is a real number that measures the uncertainty about the value of $\mathbf{X}$ when the underlying random experiment is carried out. It is defined by

$$H(\mathbf{X}) = -\sum_{x\epsilon X} P_{\mathbf{X}}(x) \log P_{\mathbf{X}}(x),$$

assuming that the terms of the form $0 \log 0$ are excluded from the summation, and where the logarithm is relative to the base 2. The entropy of a random variable satisfies $0 \leq H(\mathbf{X}) \leq \log |X|$, where $H(\mathbf{X}) = 0$ if and only if there exists $x_0 \in X$ such that $Pr(\mathbf{X} = x_0) = 1$; whereas, $H(\mathbf{X}) = \log |X|$ if and only if $Pr(\mathbf{X} = x) = 1/|X|$, for all $x \in X$. The deviation of the entropy $H(\mathbf{X})$ from its maximal value can be used as a measure of non-uniformity of the distribution $\{P_{\mathbf{X}}(x)\}_{x\in X}$. The entropy is also interpreted as a measure of the amount of information given on average by the random variable, i.e., the amount of information given on average by the result of the random experiment associated with it.

Given two random variables $\mathbf{X}$ and $\mathbf{Y}$, taking values on sets X and Y, respectively, according to a probability distribution $\{P_{\mathbf{XY}}(x, y)\}_{x\in X, y\in Y}$ on their Cartesian product, the conditional uncertainty of $\mathbf{X}$, given the random variable $\mathbf{Y}$, called *conditional entropy* and denoted by $H(\mathbf{X}|\mathbf{Y})$, is defined as

$$H(\mathbf{X}|\mathbf{Y}) = -\sum_{y\in Y}\sum_{x\in X} P_{\mathbf{Y}}(y) P_{\mathbf{X}|\mathbf{Y}}(x|y) \log P_{\mathbf{X}|\mathbf{Y}}(x|y).$$

Notice that the conditional entropy is not the entropy of a probability distribution but the *average* over all entropies $H(\mathbf{X}|\mathbf{Y}=y)$. Simple algebra shows that

$$H(\mathbf{X}|\mathbf{Y}) \geq 0 \tag{32}$$

with equality if and only if X is a function of Y. The conditional entropy is a measure of the amount of information on $\mathbf{X}$, once given $\mathbf{Y}$.

The *mutual information* between $\mathbf{X}$ and $\mathbf{Y}$ is given by

$$I(\mathbf{X};\mathbf{Y}) = H(\mathbf{X}) - H(\mathbf{X}|\mathbf{Y}).$$

Since,

$$I(\mathbf{X};\mathbf{Y}) = I(\mathbf{Y};\mathbf{X}) \text{ and } I(\mathbf{X};\mathbf{Y}) \geq 0, \tag{33}$$

it is easy to see that

$$H(\mathbf{X}) \geq H(\mathbf{X}|\mathbf{Y}), \tag{34}$$

with equality if and only if $\mathbf{X}$ and $\mathbf{Y}$ are independent. The mutual information is a measure of the common information between $\mathbf{X}$ and $\mathbf{Y}$.

Given $n+1$ random variables, $\mathbf{X}_1,\ldots,\mathbf{X}_n,\mathbf{Y}$, the entropy of $\mathbf{X}_1,\ldots,\mathbf{X}_n$ given $\mathbf{Y}$ can be written as

$$H(\mathbf{X}_1,\ldots,\mathbf{X}_n|\mathbf{Y}) = H(\mathbf{X}_1|\mathbf{Y}) + H(\mathbf{X}_2|\mathbf{X}_1,\mathbf{Y}) + \cdots + H(\mathbf{X}_n|\mathbf{X}_1,\ldots,\mathbf{X}_{n-1},\mathbf{Y}). \tag{35}$$

Therefore, for any sequence of n random variables, $\mathbf{X}_1,\ldots,\mathbf{X}_n$, it holds that

$$H(\mathbf{X}_1,\ldots,\mathbf{X}_n) = \sum_{i=1}^{n} H(\mathbf{X}_i|\mathbf{X}_1,\ldots,\mathbf{X}_{i-1}) \leq \sum_{i=1}^{n} H(\mathbf{X}_i). \tag{36}$$

Moreover, the above relation implies that, for each $k \leq n$,

$$H(\mathbf{X}_1,\ldots,\mathbf{X}_n) \geq H(\mathbf{X}_1,\ldots,\mathbf{X}_k). \tag{37}$$

Given three random variables, $\mathbf{X}$, $\mathbf{Y}$, and $\mathbf{Z}$, the *conditional mutual information* between $\mathbf{X}$ and $\mathbf{Y}$ given $\mathbf{Z}$ can be written as

$$I(\mathbf{X};\mathbf{Y}|\mathbf{Z}) = H(\mathbf{X}|\mathbf{Z}) - H(\mathbf{X}|\mathbf{Z},\mathbf{Y}) = H(\mathbf{Y}|\mathbf{Z}) - H(\mathbf{Y}|\mathbf{Z},\mathbf{X}) = I(\mathbf{Y};\mathbf{X}|\mathbf{Z}). \tag{38}$$

Since the conditional mutual information $I(\mathbf{X};\mathbf{Y}|\mathbf{Z})$ is always non-negative we get

$$H(\mathbf{X}|\mathbf{Z}) \geq H(\mathbf{X}|\mathbf{Z},\mathbf{Y}). \tag{39}$$

Finally, given three random variables, $\mathbf{X}$, $\mathbf{Y}$, and $\mathbf{Z}$, such that $\mathbf{Z}$ is a function of $\mathbf{Y}$, i.e., $\mathbf{Z}=f(\mathbf{Y})$, then it holds that

$$H(\mathbf{X}|\mathbf{Y}) = H(\mathbf{X}|\mathbf{Z},\mathbf{Y}). \tag{40}$$