An Information-Theoretically Secure Threshold Distributed Oblivious Transfer Protocol

Christian L.F. Corniaux and Hossein Ghodosi

James Cook University, Townsville QLD 4811, Australia
chris.corniaux@my.jcu.edu.au, hossein.ghodosi@jcu.edu.au

Abstract. The unconditionally secure Distributed Oblivious Transfer (DOT) protocol presented by Blundo, D'Arco, De Santis, and Stinson at SAC 2002 allows a receiver to contact k servers and obtain one out of n secrets held by a sender.

Once the protocol has been executed, the sender does not know which secret was selected by the receiver and the receiver knows nothing of the secrets she did not choose. In addition, the receiver's privacy is guaranteed against a coalition of $k-1$ servers and similarly, the sender's security is guaranteed against a coalition of $k-1$ servers. However, after the receiver has obtained a secret, she is able to learn all secrets by corrupting one server only. In addition, an external mechanism is required to prevent the receiver from contacting more than k servers.

The one-round DOT protocol we propose is information-theoretically secure, allows the receiver to contact k servers or more, and guarantees the sender's security, even if the receiver corrupts $k-1$ servers after having obtained a secret.

Keywords: Cryptographic Protocol, Distributed Oblivious Transfer, Commodity Based Model, Information-Theoretic Security.

1 Introduction

Oblivious Transfer (OT) protocols allow two parties to exchange, in total privacy, one or more secret messages. The first OT protocol, introduced by Rabin [13], enables a sender to transmit a message to a receiver in such a way that the receiver gets the message with probability $\frac{1}{2}$ while the sender does not know whether the message was received. Even, Goldreich and Lempel [8] introduced a variant of the original OT for a contract signature application. This OT, identified as OT-$\binom{2}{1}$, is an exchange protocol between a receiver and a sender who has two secret messages; the receiver chooses one of the two messages and the sender transmits the chosen message to the receiver. At the end of the protocol, the sender does not know which message was selected and the receiver knows nothing of the other message.

A major drawback with OT-$\binom{2}{1}$ and with the more general OT-$\binom{n}{1}$ proposed by Brassard, Crépeau and Roberts [6] is the restriction in the availability of the secret messages, because if the unique sender is unavailable, the receiver cannot

T. Kwon, M.-K. Lee, and D. Kwon (Eds.): ICISC 2012, LNCS 7839, pp. 184–201, 2013.

execute the protocol. To increase the availability of messages, the sender may distribute them to m servers, like in the first unconditionally secure Distributed Oblivious Transfer (DOT) protocol introduced by Gertner and Malkin [10] in 1997. However, Gertner and Malkin's protocol does not guarantee the messages' confidentiality against curious or corrupted servers.

In 2000, Naor and Pinkas [11] proposed an unconditionally secure DOT protocol which takes non-fully trusted servers into account: servers are only provided with parts – called *shares* – of the original messages. This DOT protocol was generalized to n secrets by Blundo, D'Arco, De Santis and Stinson [4,5]. Both protocols are composed of two phases: (i) the *set-up phase* and (ii) the *transfer phase*. During the set-up phase, the sender generates and sends shares of his secrets to all the servers. In the transfer phase, the receiver chooses the index of a secret, selects k servers ($1 < k \leq m$) and sends them requests. From the k responses the receiver is able to determine the chosen secret.

Blundo et al. also defined a security model composed of four fundamental conditions that every DOT protocol should satisfy:

C_1. Correctness – The receiver is able to determine the chosen secret once she has received information from the k contacted servers.
C_2. Receiver's privacy – A coalition of up to $k-1$ servers cannot obtain any information on the choice of the receiver.
C_3. Sender's privacy with respect to $k-1$ servers and the receiver – A coalition of up to $k-1$ servers with the receiver does not obtain any information about the secrets.
C_4. Sender's privacy with respect to a "greedy" receiver – Given the transcript of the interaction with k servers, a coalition of up to $k-1$ dishonest servers and the receiver does not obtain any information about secrets which were not chosen by the receiver.

As it has been pointed out by Blundo et al. in [4,5], the protocol introduced by Naor and Pinkas only satisfies conditions C_1 and C_2. Their own protocol satisfies conditions C_1, C_2 and C_3 only. Actually, they have proven that condition C_4 cannot be guaranteed with a one-round DOT protocol – a round being defined as a set of consistent requests/responses exchanged between the receiver and k servers.

Besides, Nikov, Nikova, Preneel and Vanderwalle have demonstrated [12] that more generally, if the receiver's privacy is guaranteed against a coalition of $k_{\mathcal{R}}$ servers and the sender's security against a coalition of $k_{\mathcal{S}}$ servers, including when a secret had already been obtained, then the parameters $k_{\mathcal{S}}$ and $k_{\mathcal{R}}$ must satisfy the inequality $(k_{\mathcal{S}} + 1) + (k_{\mathcal{R}} + 1) < k$.

Recently, Beimel, Chee, Wang and Zhang [2] introduced communication-efficient DOT protocols. These protocols, based on information-theoretic private information retrieval (PIR) protocols, require that the number of servers contacted by the receiver is pre-determined.

In this paper, we introduce an information-theoretically secure threshold DOT protocol. That is, the number of servers the receiver needs to contact to obtain

a secret is not limited to k. Moreover, unlike other unconditionally secure DOT protocols, our protocol satisfies security conditions C_1, C_2 for a coalition of any size, C_3 and C_4. Actually, to circumvent the impossibility result established by Blundo et al., we use the commodity-based model introduced by Beaver [1]. More precisely, our protocol is based on Rivest's trusted initializer OT protocol [15]. In this protocol, an additional party – the trusted initializer – is involved in the set-up phase; he generates and distributes random values, but receives nothing from other parties (in particular, he obtains neither the sender's secrets, nor the receiver's choice). In addition, our protocol has an efficiency similar to the efficiency of the full protocol presented by Blundo et al. [4,5].

This paper is organized as follows: in Sect. 2, we give an overview of the OT protocol proposed by Rivest [15]. In Sect. 3, we introduce some definitions and notations, as well as our security model. The protocol is described in Sect. 4 and the security is analysed in Sect. 5. The last section is devoted to the performance of the protocol.

2 Background

The OT-$\binom{2}{1}$ protocol presented by Rivest [15] is based on the protocol introduced by Bennett, Brassard, Crépeau and Skubiszewska [3], adapted to the trusted initializer model.

We assume that a sender $\mathcal{S}$ holds two secrets $w_0, w_1 \in \{0,1\}^\ell$ ($\ell \in \mathbb{N}^* = \{1,2,\dots\}$) and that a receiver $\mathcal{R}$ wishes to learn the secret w_e ($e = 0$ or $e = 1$).

In the set-up phase, the trusted initializer $\mathcal{T}$ gives to $\mathcal{S}$ two random ℓ-bit strings r_0 and r_1. Then, $\mathcal{T}$ selects a random bit d and sends the pair (d, r_d) to $\mathcal{R}$.

In the transfer phase, $\mathcal{R}$ selects the index e of one secret and transmits $c = e \oplus d$ to $\mathcal{S}$. $\mathcal{S}$ replies with two values $f_0 = w_0 \oplus r_c$ and $f_1 = w_1 \oplus r_{1-c}$. To obtain w_e, $\mathcal{R}$ calculates $f_e \oplus r_d$.

Clearly, the receiver obtains one secret only and the sender cannot determine which secret was chosen by the receiver.

3 Preliminaries

3.1 Notations and Definitions

The setting of the DOT protocol described in this paper encompasses a sender $\mathcal{S}$ who owns n secrets $w_1, \dots, w_n$ ($n > 1$) in a finite field $\mathbb{K} = \mathbb{F}_p$ (p prime), a receiver $\mathcal{R}$ who wishes to learn a secret w_e ($1 \leq e \leq n$), a trusted initializer $\mathcal{T}$ who generates random elements of $\mathbb{K}$ and m servers $S_1, \dots, S_m$. We assume that $p > \max(n, w_1, \dots, w_n, m)$ and that all operations are executed in $\mathbb{K}$.

Our protocol is composed of three phases: a set-up phase, a commodity acquisition phase and a transfer phase. In the set-up phase, for each secret the sender generates shares thanks to Shamir's (k, m)-threshold secret sharing schemes [16] ($1 < k \leq m$). Then, the sender distributes the shares to the m servers and does

not intervene in the rest of the protocol. In the commodity acquisition phase, the receiver contacts the trusted initializer who generates and distributes consistent masks to the m servers and to the receiver. The trusted initializer's presence is only required in this phase. In the transfer phase, the receiver has to contact t servers ($k \leq t \leq m$) to collect enough shares to construct w_e.

The protocol requires the availability of private communication channels between the trusted initializer and the servers, between the trusted initializer and the receiver and between the sender and the servers. The receiver sends requests to the servers thanks to a private broadcast channel and collects responses thanks to private channels between servers and herself. We assume that private channels are secure, i.e., any party is unable to eavesdrop on them and that all channels guarantee that communications cannot be tampered with.

The set $\{1, \ldots, n\}$ of natural numbers is denoted $[n]$. The additive group of univariate polynomials of degree at most k with coefficients in $\mathbb{K}$ is denoted $\mathbb{K}_k[X]$. In addition, by an abuse of language, a polynomial and its corresponding polynomial function will not be differentiated.

Since security conditions are linked to the quantity of information received by parties, it seems appropriate to use Shannon's entropy function [17], and more generally information theory, to demonstrate the security of our protocol. The following definitions and properties will be used in the paper (for more details on information theory, see for example [7]).

An element v of a finite field V is described by a discrete random variable $\boldsymbol{V}$ over a finite set $\mathcal{V}$. The probability distribution $\Pr(\boldsymbol{V})$ is associated with $\boldsymbol{V}$.

Let $\boldsymbol{X}$ and $\boldsymbol{Y}$ be two random variables.

- The *entropy* of $\boldsymbol{X}$ is $H(\boldsymbol{X}) = -\sum_{x \in \mathcal{X}} \Pr(\boldsymbol{X} = x) \log_2 \Pr(\boldsymbol{X} = x)$.
- The *joint entropy* $H(\boldsymbol{X}, \boldsymbol{Y})$ of $\boldsymbol{X}$ and $\boldsymbol{Y}$ (joint distribution $\Pr(\boldsymbol{X}, \boldsymbol{Y})$) is

$$H(\boldsymbol{X}, \boldsymbol{Y}) = -\sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} \Pr(\boldsymbol{X} = x, \boldsymbol{Y} = y) \log_2 \Pr(\boldsymbol{X} = x, \boldsymbol{Y} = y).$$

- The *conditional entropy* $H(\boldsymbol{X} \mid \boldsymbol{Y})$ of $\boldsymbol{X}$ given $\boldsymbol{Y}$ is defined as

$$H(\boldsymbol{X} \mid \boldsymbol{Y}) = \sum_{y \in \mathcal{Y}} \Pr(\boldsymbol{Y} = y) H(\boldsymbol{X} \mid \boldsymbol{Y} = y),$$

  where the entropy $H(\boldsymbol{X} \mid \boldsymbol{Y} = y)$ is

$$H(\boldsymbol{X} \mid \boldsymbol{Y} = y) = -\sum_{x \in \mathcal{X}} \Pr(\boldsymbol{X} = x \mid \boldsymbol{Y} = y) \log_2 \Pr(\boldsymbol{X} = x \mid \boldsymbol{Y} = y).$$

Note that if $\Pr(\boldsymbol{X} = x) = 0$, then we adopt the convention that $\Pr(\boldsymbol{X} = x) \log_2 \Pr(\boldsymbol{X} = x) = 0$.

Let $\boldsymbol{X}$, $\boldsymbol{Y}$, $\boldsymbol{Z}$ and $\boldsymbol{X}_i$ ($i \in [n]$) be random variables. We use the following properties in the security demonstrations:

$$H(\boldsymbol{X}) \geq H(\boldsymbol{X} \mid \boldsymbol{Y}) \tag{1}$$
$$H(\boldsymbol{X}, \boldsymbol{Y}) = H(\boldsymbol{X}) + H(\boldsymbol{Y} \mid \boldsymbol{X}) = H(\boldsymbol{Y}) + H(\boldsymbol{X} \mid \boldsymbol{Y}) \tag{2}$$
$$0 \leq H(\boldsymbol{X}) \leq \log_2 |\mathcal{X}| \tag{3}$$
$$\text{If } H(\boldsymbol{Y} \mid \boldsymbol{Z}) = 0 \text{ then } H(\boldsymbol{X} \mid \boldsymbol{Y}) \geq H(\boldsymbol{X} \mid \boldsymbol{Z}) \tag{4}$$
$$\text{If } H(\boldsymbol{Y} \mid \boldsymbol{Z}) = 0 \text{ then } H(\boldsymbol{X} \mid \boldsymbol{Y}, \boldsymbol{Z}) = H(\boldsymbol{X} \mid \boldsymbol{Z}) \tag{5}$$
$$H(\boldsymbol{Z} \mid \boldsymbol{X}, \boldsymbol{Y}) = H(\boldsymbol{Z} \mid \boldsymbol{X}) \text{ iff } H(\boldsymbol{Y} \mid \boldsymbol{X}, \boldsymbol{Z}) = H(\boldsymbol{Y} \mid \boldsymbol{X}) \tag{6}$$
$$\text{If } H(\boldsymbol{Z} \mid \boldsymbol{X}, \boldsymbol{Y}) = H(\boldsymbol{Z}) \text{ then } H(\boldsymbol{X} \mid \boldsymbol{Y}, \boldsymbol{Z}) = H(\boldsymbol{X} \mid \boldsymbol{Y}) \tag{7}$$

and

$$\text{If } H(\boldsymbol{X} \mid \boldsymbol{Y}, \boldsymbol{Z}) = H(\boldsymbol{X}) \text{ then } H(\boldsymbol{X} \mid \boldsymbol{Y}) = H(\boldsymbol{X} \mid \boldsymbol{Z}) = H(\boldsymbol{X}) \tag{8}$$

3.2 Security Model

The point of the paper is not to propose a verifiable DOT protocol. This is why we assume that all parties wish to complete the protocol to allow the receiver to obtain the chosen secret. In particular, the trusted initializer and the sender are honest. However, even if they are not malicious, servers may actively collaborate to determine the receiver's choice (C_2) or the sender's secrets (C_3). The receiver may also actively cheat, either while cooperating with a coalition of active cheating servers (C_3), or by corrupting servers after having obtained a secret (C_4). In this latter case, the receiver has access to all data held by the corrupted servers.

4 Protocol Description

The key idea underlying our t-out-of-n DOT protocol is to extend Rivest's OT protocol in two directions:

1. Generalization to n secrets
2. Introduction of a distributed model with m servers

Furthermore, to prevent the servers from learning the sender's secrets, they receive shares of the secrets held by the sender. These shares are generated thanks to Shamir's secret sharing schemes [16].

In addition, to guarantee that the contacted servers do not receive requests related to different secrets, they all receive the same request and this request is broadcast.

The full protocol is described in Fig. 1.

5 Security of the Protocol

5.1 Formal Model

To prove the security of our protocol we use a formal model similar to the model introduced by Blundo et al. [4,5]. In this model, we assume that the

Input	The sender $\mathcal{S}$ contributes with n secrets $w_1, \ldots, w_n \in \mathbb{K}$ The trusted initializer $\mathcal{T}$ generates m sets of n random masks and randomly chooses one of the n sets The receiver $\mathcal{R}$ chooses an index $e \in [n]$, and contributes with a cyclic permutation $\pi \in \mathfrak{S}_n$
Output	$\mathcal{R}$ receives w_e, while $\mathcal{S}$ and $\mathcal{T}$ receive nothing.

Set-up Phase

1 - *Preparation of shares.* For each secret w_i ($i \in [n]$), the sender $\mathcal{S}$ generates, thanks to Shamir's (k, m)-threshold secret sharing scheme, a sharing polynomial F_i of degree at most $k-1$, such that $F_i(0) = w_i$.

2 - *Distribution of shares.* To each server S_j ($j \in [m]$), $\mathcal{S}$ transmits the n shares $F_1(j), \ldots, F_n(j)$.

Commodity Acquisition Phase

1 - *Preparation of masks.* The trusted initializer $\mathcal{T}$ generates mn random masks $r_{j,i} \in \mathbb{K}$ ($j \in [m]$, $i \in [n]$) and one random index $s \in [n]$.

2 - *Distribution of masks.* $\mathcal{T}$ distributes the n masks $r_{j,1}, \ldots, r_{j,n}$ to the server S_j ($j \in [m]$) and the index s as well as the m masks $r_{1,s}, \ldots, r_{m,s}$ to the receiver $\mathcal{R}$.

Transfer Phase

1 - *Selection of the secret index and generation of the corresponding request.* The receiver $\mathcal{R}$ chooses a secret index e and generates the cyclic permutation $\pi \in \mathfrak{S}_n$ which satisfies $\pi(e) = s$.

2 - *Selection of servers and broadcast of a query.* $\mathcal{R}$ selects a subset $\mathcal{I} \subset [m]$ of $t \geq k$ indices and broadcasts a query containing the first cyclic permutation item, $\pi(1)$, as well as the list $\mathcal{I}$.

3 - *Responses of the servers.* Each server S_ℓ such that $\ell \in \mathcal{I}$ returns $\mu_{\ell,i} = F_i(\ell) + r_{\ell,\pi(i)}$ ($i \in [n]$) to $\mathcal{R}$.

4 - *Construction of the requested secret.* For each of the t responses $\mu_{\ell,e}$, $\mathcal{R}$ calculates the share $\mu_{\ell,e} - r_{\ell,s} = F_e(\ell)$, interpolates F_e and obtains $w_e = F_e(0)$.

Fig. 1. Protocol Overview

parties execute publicly known programs whose data are private. These data are described by the following discrete random variables shown on Fig. 2.

By extension, if $\boldsymbol{X}_j$ is a random variable which describes a datum x_j held by a server S_j ($j \in [m]$) and $G = \{ j_1, \ldots, j_t \}$ ($t \in [m]$), we denote $\boldsymbol{X}_G = (\boldsymbol{X}_{j_1}, \ldots, \boldsymbol{X}_{j_t})$ the random variable describing the sequence $(x_{j_1}, \ldots, x_{j_t})$. By simplification, $\boldsymbol{X}_{[m]}$ is denoted $\boldsymbol{X}$.

- Each secret $w_i \in \mathbb{K}$ ($i \in [n]$) is described by a variable $\boldsymbol{W}^i$ and the sequence of secrets $w_1, \ldots, w_n$ by the variable $\boldsymbol{W} = (\boldsymbol{W}^1, \ldots, \boldsymbol{W}^n)$. Moreover, if $e \in [n]$, we denote $\boldsymbol{W}^{\bar{e}}$ the sequence $(\boldsymbol{W}^1, \ldots, \boldsymbol{W}^{e-1}, \boldsymbol{W}^{e+1}, \ldots, \boldsymbol{W}^n)$.
- The secret index $e \in [n]$ chosen by $\mathcal{R}$ is described by the random variable $\boldsymbol{E}$.

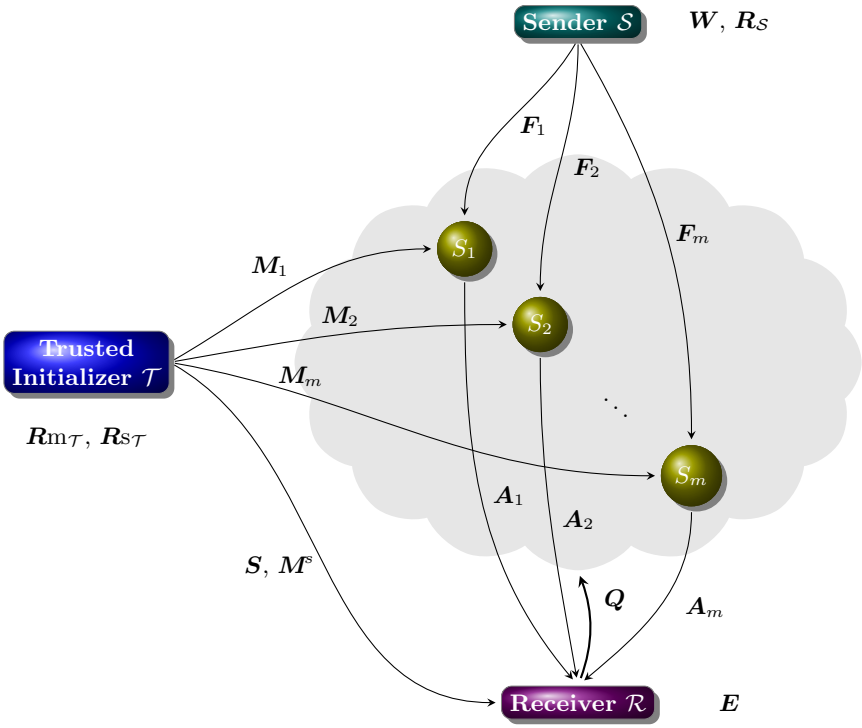

Fig. 2. Random Variables

- The random variable $\boldsymbol{M}_j^i$ ($j \in [m]$, $i \in [n]$) corresponds to the mask $r_{j,i}$ and the random variable $\boldsymbol{M}_j$ ($j \in [m]$) to the n ordered masks $(r_{j,1}, \ldots, r_{j,n})$ distributed by $\mathcal{T}$ to the server S_j. Similarly, the random variable $\boldsymbol{F}_j^i$ ($i \in [n]$, $j \in [m]$) corresponds to the share $F_i(j)$ and the random variable $\boldsymbol{F}_j$ ($j \in [m]$) to the n shares $(F_1(j), \ldots, F_n(j))$ distributed by $\mathcal{S}$ to the server S_j. By simplification $\boldsymbol{M}_j^{[n]} = (\boldsymbol{M}_j^1, \ldots, \boldsymbol{M}_j^n)$ is denoted $\boldsymbol{M}_j$ and $\boldsymbol{F}_j^{[n]} = (\boldsymbol{F}_j^1, \ldots, \boldsymbol{F}_j^n)$ is denoted $\boldsymbol{F}_j$.
- In addition, the random index $s \in [n]$ chosen by $\mathcal{T}$ is described by the random variable $\boldsymbol{S}$. The notation $\boldsymbol{M}_j^{\boldsymbol{s}}$ corresponds to the random variable describing $r_{j,s}$ and $\boldsymbol{M}^{\boldsymbol{s}}$ is a shorthand for $(\boldsymbol{M}_1^{\boldsymbol{s}}, \ldots, \boldsymbol{M}_m^{\boldsymbol{s}})$.
- The cyclic permutation $\pi \in \mathfrak{S}_n$ is described by the random variable $\boldsymbol{Q}$:

$$H(\boldsymbol{Q} \mid \boldsymbol{E}, \boldsymbol{S}) = 0. \tag{9}$$

- The transcript $T_j = (Q, A_j)$ is composed of a query $Q = \pi$ described by the random variable $\boldsymbol{Q}$ and of an answer $A_j = (F_j(1) + r_{j,\pi(1)}, \ldots, F_j(n) + r_{j,\pi(n)})$ described by the random variable $\boldsymbol{A}_j$. The random variable describing the answer $F_j(i) + r_{j,\pi(i)}$ ($j \in [m]$, $i \in [n]$) is denoted $\boldsymbol{A}_j^i$.
- A few uniform random variables are held by the parties involved in the protocol to allow them to produce private data:

- The trusted initialiser $\mathcal{T}$ holds two uniform random inputs, $\boldsymbol{R}\mathrm{m}_{\mathcal{T}}$, to generate the random masks $r_{j,i}$ $(i \in [n], j \in [m])$,

$$H(\boldsymbol{M}_j^i \mid \boldsymbol{R}\mathrm{m}_{\mathcal{T}}) = 0, \tag{10}$$

and $\boldsymbol{R}\mathrm{s}_{\mathcal{T}}$, to determine the secret index s,

$$H(\boldsymbol{S} \mid \boldsymbol{R}\mathrm{s}_{\mathcal{T}}) = 0. \tag{11}$$

Note that since $H(\boldsymbol{M}^{\mathrm{s}} \mid \boldsymbol{M}, \boldsymbol{S}) = 0$ then

$$H(\boldsymbol{M}^{\mathrm{s}} \mid \boldsymbol{R}\mathrm{m}_{\mathcal{T}}, \boldsymbol{R}\mathrm{s}_{\mathcal{T}}) = 0. \tag{12}$$

- The sender $\mathcal{S}$ holds a uniform random input $\boldsymbol{R}_{\mathcal{S}}$ to generate the shares $F_j(i)$ $(i \in [n], j \in [m])$:

$$H(\boldsymbol{F}_j^i \mid \boldsymbol{W}^i, \boldsymbol{R}_{\mathcal{S}}) = 0. \tag{13}$$

To show properties C_1, C_2, C_3 and C_4 is equivalent to show properties listed in Table 1.

Table 1. Security Conditions from an Information Theory Viewpoint

Security Condition	Number of Servers	Property
C_1	$k \leq \lvert G\rvert \leq m$	$H(\boldsymbol{W}^e \mid \boldsymbol{E} = e, \boldsymbol{S}, \boldsymbol{M}^{\mathrm{s}}, \boldsymbol{Q}, \boldsymbol{A}_G) = 0$
C_2	$\lvert G\rvert \leq m$	$H(\boldsymbol{E} \mid \boldsymbol{F}_G, \boldsymbol{M}_G, \boldsymbol{Q}) = H(\boldsymbol{E})$
C_3	$\lvert G\rvert \leq k-1$	$H(\boldsymbol{W} \mid \boldsymbol{F}_G, \boldsymbol{M}_G, \boldsymbol{E}, \boldsymbol{S}, \boldsymbol{M}^{\mathrm{s}}) = H(\boldsymbol{W})$
C_4	$k \leq \lvert G\rvert \leq m$ $\lvert G'\rvert \leq k-1$	$H(\boldsymbol{W}^{\bar{e}} \mid \boldsymbol{F}_{G'}, \boldsymbol{M}_{G'}, \boldsymbol{E} = e, \boldsymbol{S} = s, \boldsymbol{Q} = \pi, \boldsymbol{A}_G, \boldsymbol{M}^{\mathrm{s}} =$ $(r_{1,s}, \ldots, r_{m,s})) = H(\boldsymbol{W}^{\bar{e}})$

5.2 Correctness

Theorem 1. *The protocol is correct (condition C_1 is satisfied), i.e. if all parties follow the protocol, the receiver obtains the chosen secret w_e by contacting t servers S_j where $j \in G = \mathcal{I} = \{ j_1, \ldots, j_t \}$ $(k \leq t \leq m)$.*

Proof.

To demonstrate that $H(\boldsymbol{W}^e \mid \boldsymbol{E} = e, \boldsymbol{S}, \boldsymbol{M}^{\mathrm{s}}, \boldsymbol{Q}, \boldsymbol{A}_G) = 0$ is equivalent to demonstrate that once the protocol has been executed, $\Pr(\boldsymbol{W}^e = w_e \mid \boldsymbol{E} = e, \boldsymbol{S}, \boldsymbol{M}^{\mathrm{s}}, \boldsymbol{Q}, \boldsymbol{A}_G) = 1$.

Once $\mathcal{R}$ has chosen e, the cyclic permutation $\pi \in \mathfrak{S}_n$ such that $\pi(e) = s$ is determined. The response sent by the server S_ℓ $(\ell \in \mathcal{I})$ then contains the value $\mu_{\ell,e} = F_e(\ell) + r_{\ell,\pi(e)} = F_e(\ell) + r_{\ell,s}$. Since $\mathcal{R}$ knows $r_{\ell,s}$, she is able to calculate the t shares $F_e(\ell)$, to interpolate F_e (degree at most $k-1 < t$) and to determine $w_e = F_e(0)$. It follows that $\Pr(\boldsymbol{W}^e = w_e \mid \boldsymbol{E} = e, \boldsymbol{S}, \boldsymbol{M}^{\mathrm{s}}, \boldsymbol{Q}, \boldsymbol{A}_G) = 1$. □

5.3 Receiver's Privacy against a Coalition of Servers

Theorem 2. *The protocol guarantees the receiver's privacy against a coalition of h servers S_j where $j \in G = \{ j_1, \ldots, j_h \}$ $(0 \leq h \leq m)$, i.e. condition C_2 is satisfied.*

Proof.

To show that $H(\boldsymbol{E} \mid \boldsymbol{F}_G, \boldsymbol{M}_G, \boldsymbol{Q}) = H(\boldsymbol{E})$, first we demonstrate that

$$H(\boldsymbol{E} \mid \boldsymbol{F}_G, \boldsymbol{M}_G, \boldsymbol{Q}) = H(\boldsymbol{E} \mid \boldsymbol{Q})$$

and second that

$$H(\boldsymbol{E} \mid \boldsymbol{Q}) = H(\boldsymbol{E}).$$

For the first part of the demonstration, we adapt a technique applied by Beimel, Chee, Wang and Zhang [2] in a similar context.

1. First, we show that the conditional entropy of $\boldsymbol{E}$ given $\boldsymbol{F}_G$, $\boldsymbol{M}_G$ and $\boldsymbol{Q}$ satisfies
$$H(\boldsymbol{E} \mid \boldsymbol{F}_G, \boldsymbol{M}_G, \boldsymbol{Q}) = H(\boldsymbol{E} \mid \boldsymbol{Q}).$$
For this purpose, thanks to property (6), we show that
$$H(\boldsymbol{F}_G, \boldsymbol{M}_G \mid \boldsymbol{E}, \boldsymbol{Q}) = H(\boldsymbol{F}_G, \boldsymbol{M}_G \mid \boldsymbol{Q}).$$
The choice of the receiver is independent from the data held by the trusted initializer, by the sender, by the servers and by herself at the end of the commodity acquisition phase, so
$$H(\boldsymbol{E} \mid \boldsymbol{R}\mathrm{m}_{\mathcal{T}}, \boldsymbol{R}\mathrm{s}_{\mathcal{T}}, \boldsymbol{W}, \boldsymbol{R}_{\mathcal{S}}, \boldsymbol{F}, \boldsymbol{M}, \boldsymbol{S}, \boldsymbol{M}^s) = H(\boldsymbol{E}). \tag{14}$$
If we apply property (8), we obtain the particular case
$$H(\boldsymbol{E} \mid \boldsymbol{F}_G, \boldsymbol{M}_G, \boldsymbol{R}\mathrm{s}_{\mathcal{T}}) = H(\boldsymbol{E}). \tag{15}$$
Similarly, the uniform random variable $\boldsymbol{R}\mathrm{s}_{\mathcal{T}}$ held by the trusted initializer is independent from the uniform random variable $\boldsymbol{R}\mathrm{m}_{\mathcal{T}}$, from the sender's data and from the data held by the servers at the end of the commodity acquisition phase. It follows
$$H(\boldsymbol{R}\mathrm{s}_{\mathcal{T}} \mid \boldsymbol{R}\mathrm{m}_{\mathcal{T}}, \boldsymbol{W}, \boldsymbol{R}_{\mathcal{S}}, \boldsymbol{F}, \boldsymbol{M}) = H(\boldsymbol{R}\mathrm{s}_{\mathcal{T}}). \tag{16}$$
Once more, if we apply property (8), we obtain the particular case
$$H(\boldsymbol{R}\mathrm{s}_{\mathcal{T}} \mid \boldsymbol{F}_G, \boldsymbol{M}_G) = H(\boldsymbol{R}\mathrm{s}_{\mathcal{T}}). \tag{17}$$
The joint entropy between $\boldsymbol{F}_G$ and $\boldsymbol{M}_G$ is
$$\begin{aligned}
H(\boldsymbol{F}_G, \boldsymbol{M}_G) &\geq H(\boldsymbol{F}_G, \boldsymbol{M}_G \mid \boldsymbol{Q}) && \text{(from (1))} \\
&\geq H(\boldsymbol{F}_G, \boldsymbol{M}_G \mid \boldsymbol{Q}, \boldsymbol{E}) && \text{(from (1))} \\
&\geq H(\boldsymbol{F}_G, \boldsymbol{M}_G \mid \boldsymbol{R}\mathrm{s}_{\mathcal{T}}, \boldsymbol{E}) && \text{(from (9), (11) and (4))} \\
&= H(\boldsymbol{F}_G, \boldsymbol{M}_G \mid \boldsymbol{R}\mathrm{s}_{\mathcal{T}}) && \text{(from (15) and (7))} \\
&= H(\boldsymbol{F}_G, \boldsymbol{M}_G). && \text{(from (17) and (7))}
\end{aligned}$$

Therefore, $H(\boldsymbol{F}_G, \boldsymbol{M}_G \mid \boldsymbol{Q}) = H(\boldsymbol{F}_G, \boldsymbol{M}_G \mid \boldsymbol{Q}, \boldsymbol{E})$ and from property (6), $H(\boldsymbol{E} \mid \boldsymbol{Q}, \boldsymbol{F}_G, \boldsymbol{M}_G) = H(\boldsymbol{E} \mid \boldsymbol{Q})$.

2. To prove that $H(\boldsymbol{E} \mid \boldsymbol{Q}) = H(\boldsymbol{E})$, thanks to property (6), it is sufficient to show that $H(\boldsymbol{Q} \mid \boldsymbol{E}) = H(\boldsymbol{Q})$.
   First, we observe that given a secret index e and a cyclic permutation π, the random index s is uniquely determined: $s = \pi(e)$. Therefore, in terms of entropy, it follows that
   $$H(\boldsymbol{S} \mid \boldsymbol{Q}, \boldsymbol{E}) = 0. \tag{18}$$
   Second, the conditional joint entropy between $\boldsymbol{Q}$ and $\boldsymbol{S}$ given $\boldsymbol{E}$ is
   $$\begin{aligned} H(\boldsymbol{Q}, \boldsymbol{S} \mid \boldsymbol{E}) &= H(\boldsymbol{Q} \mid \boldsymbol{E}) + H(\boldsymbol{S} \mid \boldsymbol{Q}, \boldsymbol{E}) && \text{(from (2))} \\ &= H(\boldsymbol{Q} \mid \boldsymbol{E}) && \text{(from (18))} \end{aligned}$$
   and also
   $$\begin{aligned} H(\boldsymbol{Q}, \boldsymbol{S} \mid \boldsymbol{E}) &= H(\boldsymbol{S} \mid \boldsymbol{E}) + H(\boldsymbol{Q} \mid \boldsymbol{E}, \boldsymbol{S}) && \text{(from (2))} \\ &= H(\boldsymbol{S} \mid \boldsymbol{E}) && \text{(from (9))} \end{aligned}$$
   It follows that $H(\boldsymbol{Q} \mid \boldsymbol{E}) = H(\boldsymbol{S} \mid \boldsymbol{E})$.
   If we apply property (8) to equality (14), we obtain the particular case $H(\boldsymbol{E} \mid \boldsymbol{S}) = H(\boldsymbol{E})$ which, combined with property (6) gives $H(\boldsymbol{S} \mid \boldsymbol{E}) = H(\boldsymbol{S})$. Therefore, $H(\boldsymbol{Q} \mid \boldsymbol{E}) = H(\boldsymbol{S})$. Moreover, because the random variable $\boldsymbol{S}$ is uniform, it holds $H(\boldsymbol{S}) = \log_2 n$ and because the number of cyclic permutations of $\mathfrak{S}_n$ is n, we can write:
   $$\log_2 n \geq H(\boldsymbol{Q}) \geq H(\boldsymbol{Q} \mid \boldsymbol{E}) = H(\boldsymbol{S}) = \log_2 n.$$
   It follows that $H(\boldsymbol{Q} \mid \boldsymbol{E}) = H(\boldsymbol{Q})$ and from (6) that $H(\boldsymbol{E} \mid \boldsymbol{Q}) = H(\boldsymbol{E})$.

We have shown that $H(\boldsymbol{E} \mid \boldsymbol{Q}, \boldsymbol{F}_G, \boldsymbol{M}_G) = H(\boldsymbol{E} \mid \boldsymbol{Q})$ and $H(\boldsymbol{E} \mid \boldsymbol{Q}) = H(\boldsymbol{E})$. We conclude $H(\boldsymbol{E} \mid \boldsymbol{F}_G, \boldsymbol{M}_G, \boldsymbol{Q}) = H(\boldsymbol{E})$. □

5.4 Sender's Security against a Coalition of the Receiver and Servers

Theorem 3. *The protocol guarantees the sender's security against a coalition of the receiver and h servers S_j where $j \in G = \{ j_1, \ldots, j_h \}$ $(0 \leq h \leq k-1)$, before the protocol is executed (condition C_3 is satisfied).*

Proof.

The demonstration is symmetrical to the previous demonstration. First, we demonstrate that $H(\boldsymbol{W} \mid \boldsymbol{F}_G, \boldsymbol{M}_G, \boldsymbol{E}, \boldsymbol{S}, \boldsymbol{M}^{\mathrm{s}}) = H(\boldsymbol{W} \mid \boldsymbol{F}_G)$ and second that the secrets are independent from the shares received by any set of h servers ($h \leq k-1$) in the set-up phase, i.e., $H(\boldsymbol{W} \mid \boldsymbol{F}_G) = H(\boldsymbol{W})$. These two demonstrations will allow us to show that the secrets are independent from the data held by a coalition between the receiver and h servers.

1. The uniform random variable $\boldsymbol{R}\mathrm{m}_{\mathcal{T}}$ held by the trusted initializer is independent from the data held by the sender, by the servers and by herself at the end of the commodity acquisition phase, except masks. It follows

$$H(\boldsymbol{R}\mathrm{m}_{\mathcal{T}} \mid \boldsymbol{R}\mathrm{s}_{\mathcal{T}}, \boldsymbol{W}, \boldsymbol{R}_{\mathcal{S}}, \boldsymbol{F}) = H(\boldsymbol{R}\mathrm{m}_{\mathcal{T}}). \tag{19}$$

   If we apply property (8), we obtain the particular case

$$H(\boldsymbol{R}\mathrm{m}_{\mathcal{T}} \mid \boldsymbol{R}\mathrm{s}_{\mathcal{T}}, \boldsymbol{W}, \boldsymbol{F}_G) = H(\boldsymbol{R}\mathrm{m}_{\mathcal{T}}). \tag{20}$$

   Likewise, from (14) and (8) we can write

$$H(\boldsymbol{E} \mid \boldsymbol{W}, \boldsymbol{F}_G, \boldsymbol{R}\mathrm{s}_{\mathcal{T}}, \boldsymbol{R}\mathrm{m}_{\mathcal{T}}) = H(\boldsymbol{E}), \tag{21}$$

   and from (16) and (8) we can write

$$H(\boldsymbol{R}\mathrm{s}_{\mathcal{T}} \mid \boldsymbol{W}, \boldsymbol{F}_G) = H(\boldsymbol{R}\mathrm{s}_{\mathcal{T}}). \tag{22}$$

   The conditional entropy of $\boldsymbol{W}$ given $\boldsymbol{F}_G$ is

$$\begin{aligned} H(\boldsymbol{W} \mid \boldsymbol{F}_G) &\geq H(\boldsymbol{W} \mid \boldsymbol{F}_G, \boldsymbol{M}_G, \boldsymbol{E}, \boldsymbol{S}, \boldsymbol{M}^s) && \text{(from (1))} \\ &\geq H(\boldsymbol{W} \mid \boldsymbol{F}_G, \boldsymbol{E}, \boldsymbol{R}\mathrm{m}_{\mathcal{T}}, \boldsymbol{R}\mathrm{s}_{\mathcal{T}}) && \text{(from (10), (11), (12) and (4))} \\ &= H(\boldsymbol{W} \mid \boldsymbol{F}_G). && \text{(from (21), (22), (20) and (7))} \end{aligned}$$

   We conclude that $H(\boldsymbol{W} \mid \boldsymbol{F}_G, \boldsymbol{M}_G, \boldsymbol{E}, \boldsymbol{S}, \boldsymbol{M}^s) = H(\boldsymbol{W} \mid \boldsymbol{F}_G)$.
2. It is well-known that Shamir's secret sharing scheme [16] is perfect, i.e, for $i \in [n]$, we have $H(\boldsymbol{W}^i \mid \boldsymbol{F}_G^i) = H(\boldsymbol{W}^i)$. The n secrets $w_1, \ldots, w_n$ are shared thanks to independent schemes; Therefore, the previous equality may easily be generalized to a vector of secrets $(\boldsymbol{W}^1, \ldots, \boldsymbol{W}^n)$. It follows that $H(\boldsymbol{W} \mid \boldsymbol{F}_G^1, \ldots, \boldsymbol{F}_G^n) = H(\boldsymbol{W})$.
   Since $\boldsymbol{F}_G^1, \ldots, \boldsymbol{F}_G^n = \boldsymbol{F}_G^{[n]} = \boldsymbol{F}_G$, we obtain $H(\boldsymbol{W} \mid \boldsymbol{F}_G) = H(\boldsymbol{W})$.

We have demonstrated that $H(\boldsymbol{W} \mid \boldsymbol{F}_G, \boldsymbol{M}_G, \boldsymbol{E}, \boldsymbol{S}, \boldsymbol{M}^s) = H(\boldsymbol{W} \mid \boldsymbol{F}_G)$ and that $H(\boldsymbol{W} \mid \boldsymbol{F}_G) = H(\boldsymbol{W})$. We conclude

$$H(\boldsymbol{W} \mid \boldsymbol{F}_G, \boldsymbol{M}_G, \boldsymbol{E}, \boldsymbol{S}, \boldsymbol{M}^s) = H(\boldsymbol{W}).$$

□

5.5 Sender's Security against a "Greedy" Receiver

Theorem 4. *The protocol guarantees the sender's security against a coalition of the receiver and h servers $S_{j'}$ where $j' \in G' = \{ j'_1, \ldots, j'_h \}$ $(0 \leq h \leq k-1)$, after the protocol has been executed (condition C_4 is satisfied).*

Proof.

We assume that in the transfer phase of the protocol, t servers S_j are contacted by the receiver, where $j \in G = \{ j_1, \ldots, j_t \}$ $(1 < t \leq m)$. We introduce a random variable $\boldsymbol{K} = (\boldsymbol{E}, \boldsymbol{S}, \boldsymbol{M}^s)$ describing the data $K = (e, s, (r_{1,s}, \ldots, r_{m,s}))$. The theorem is demonstrated in four steps:

– First, we demonstrate that,

$$\begin{aligned} &H(\boldsymbol{W}^{\bar{e}} \mid \boldsymbol{F}_{G'}, \boldsymbol{M}_{G'}, \boldsymbol{A}_G, \boldsymbol{K} = K, \boldsymbol{Q} = \pi) \\ &= H(\boldsymbol{W}^{\bar{e}} \mid \boldsymbol{F}^{\bar{e}}_{G'}, \boldsymbol{F}^{e}_{G}, \boldsymbol{M}^{\bar{s}}_{G'}, \boldsymbol{A}^{\bar{e}}_{G\setminus G'}, \boldsymbol{K} = K). \end{aligned}$$

– Second, we show that

$$\begin{aligned} &H(\boldsymbol{W}^{\bar{e}} \mid \boldsymbol{F}^{\bar{e}}_{G'}, \boldsymbol{F}^{e}_{G}, \boldsymbol{M}^{\bar{s}}_{G'}, \boldsymbol{A}^{\bar{e}}_{G\setminus G'}, \boldsymbol{K} = K) \\ &= H(\boldsymbol{W}^{\bar{e}} \mid \boldsymbol{F}^{\bar{e}}_{G'}, \boldsymbol{F}^{e}_{G}, \boldsymbol{M}^{\bar{s}}_{G'}, \boldsymbol{K} = K). \end{aligned}$$

– Third, we show that

$$H(\boldsymbol{W}^{\bar{e}} \mid \boldsymbol{F}^{\bar{e}}_{G'}, \boldsymbol{F}^{e}_{G}, \boldsymbol{M}^{\bar{s}}_{G'}, \boldsymbol{K} = K) = H(\boldsymbol{W}^{\bar{e}} \mid \boldsymbol{F}^{\bar{e}}_{G'}, \boldsymbol{F}^{e}_{G}, \boldsymbol{K} = K).$$

– Lastly, we show that $H(\boldsymbol{W}^{\bar{e}} \mid \boldsymbol{F}^{\bar{e}}_{G'}, \boldsymbol{F}^{e}_{G}, \boldsymbol{K} = K) = H(\boldsymbol{W}^{\bar{e}})$.

1. The random variable $\boldsymbol{A}_G$ may be decomposed under the form $\boldsymbol{A}_G = (\boldsymbol{A}_{G\setminus G'}, \boldsymbol{A}_{G'})$. Since $H(\boldsymbol{A}_{G'} \mid \boldsymbol{F}_{G'}, \boldsymbol{M}_{G'}, \boldsymbol{Q} = \pi) = 0$, we apply property (5) which yields

$$\begin{aligned} &H(\boldsymbol{W}^{\bar{e}} \mid \boldsymbol{F}_{G'}, \boldsymbol{M}_{G'}, \boldsymbol{A}_G, \boldsymbol{K} = K, \boldsymbol{Q} = \pi) \\ &= H(\boldsymbol{W}^{\bar{e}} \mid \boldsymbol{F}_{G'}, \boldsymbol{M}_{G'}, \boldsymbol{A}_{G\setminus G'}, \boldsymbol{K} = K, \boldsymbol{Q} = \pi). \end{aligned}$$

   The random variable $\boldsymbol{A}_{G\setminus G'}$ may be decomposed under the form $\boldsymbol{A}_{G\setminus G'} = (\boldsymbol{A}^{\bar{e}}_{G\setminus G'}, \boldsymbol{A}^{e}_{G\setminus G'})$. Since for $j \in [m]$, we have $F_e(j) = (F_e(j) + r_{j,\pi(e)}) + r_{j,\pi(e)} = (F_e(j) + r_{j,\pi(e)}) + r_{j,s}$, it holds that

$$H(\boldsymbol{F}^{e}_{G\setminus G'} \mid \boldsymbol{A}^{e}_{G\setminus G'}, \boldsymbol{M}^{s}_{G\setminus G'}) = 0 \text{ and } H(\boldsymbol{A}^{e}_{G\setminus G'} \mid \boldsymbol{F}^{e}_{G\setminus G'}, \boldsymbol{M}^{s}_{G\setminus G'}) = 0.$$

   Applying (5) we obtain

$$\begin{aligned} &H(\boldsymbol{W}^{\bar{e}} \mid \boldsymbol{F}_{G'}, \boldsymbol{M}_{G'}, \boldsymbol{A}_{G\setminus G'}, \boldsymbol{K} = K, \boldsymbol{Q} = \pi) \\ &= H(\boldsymbol{W}^{\bar{e}} \mid \boldsymbol{F}_{G'}, \boldsymbol{F}^{e}_{G\setminus G'}, \boldsymbol{M}_{G'}, \boldsymbol{A}^{\bar{e}}_{G\setminus G'}, \boldsymbol{K} = K, \boldsymbol{Q} = \pi). \end{aligned}$$

   From properties (9) and (5), we obtain

$$\begin{aligned} &H(\boldsymbol{W}^{\bar{e}} \mid \boldsymbol{F}_{G'}, \boldsymbol{F}^{e}_{G\setminus G'}, \boldsymbol{M}_{G'}, \boldsymbol{A}^{\bar{e}}_{G\setminus G'}, \boldsymbol{K} = K, \boldsymbol{Q} = \pi) \\ &= H(\boldsymbol{W}^{\bar{e}} \mid \boldsymbol{F}_{G'}, \boldsymbol{F}^{e}_{G\setminus G'}, \boldsymbol{M}_{G'}, \boldsymbol{A}^{\bar{e}}_{G\setminus G'}, \boldsymbol{K} = K). \end{aligned}$$

   Because $\boldsymbol{M}_{G'} = (\boldsymbol{M}^{s}_{G'}, \boldsymbol{M}^{\bar{s}}_{G'})$ and $\boldsymbol{F}_{G'} = (\boldsymbol{F}^{e}_{G'}, \boldsymbol{F}^{\bar{e}}_{G'})$, we can apply (5). It follows

$$\begin{aligned} &H(\boldsymbol{W}^{\bar{e}} \mid \boldsymbol{F}_{G'}, \boldsymbol{F}^{e}_{G\setminus G'}, \boldsymbol{M}_{G'}, \boldsymbol{A}^{\bar{e}}_{G\setminus G'}, \boldsymbol{K} = K) \\ &= H(\boldsymbol{W}^{\bar{e}} \mid \boldsymbol{F}^{\bar{e}}_{G'}, \boldsymbol{F}^{e}_{G}, \boldsymbol{M}^{\bar{s}}_{G'}, \boldsymbol{A}^{\bar{e}}_{G\setminus G'}, \boldsymbol{K} = K). \end{aligned}$$

2. To prove that

$$H(\boldsymbol{W}^{\bar{e}} \mid \boldsymbol{F}^{\bar{e}}_{G'}, \boldsymbol{F}^{e}_{G}, \boldsymbol{M}^{\bar{s}}_{G'}, \boldsymbol{A}^{\bar{e}}_{G\setminus G'}, \boldsymbol{K} = K) = H(\boldsymbol{W}^{\bar{e}} \mid \boldsymbol{F}^{\bar{e}}_{G'}, \boldsymbol{F}^{e}_{G}, \boldsymbol{M}^{\bar{s}}_{G'}, \boldsymbol{K} = K),$$

thanks to property (7) and Lemma 1, it is enough to show that

$$H(\boldsymbol{A}^{\bar{e}}_{G\setminus G'} \mid \boldsymbol{F}^{\bar{e}}_{G'}, \boldsymbol{F}^{e}_{G}, \boldsymbol{M}^{\bar{s}}_{G'}, \boldsymbol{K}, \boldsymbol{W}^{\bar{e}}) = H(\boldsymbol{A}^{\bar{e}}_{G\setminus G'}).$$

We have:

$$\begin{aligned}
&H(\boldsymbol{A}^{\bar{e}}_{G\setminus G'}, \boldsymbol{M}^{\bar{s}}_{G\setminus G'} \mid \boldsymbol{F}^{\bar{e}}, \boldsymbol{F}^{e}_{G}, \boldsymbol{M}^{\bar{s}}_{G'}, \boldsymbol{K} = K, \boldsymbol{W}^{\bar{e}}) \\
&= H(\boldsymbol{M}^{\bar{s}}_{G\setminus G'} \mid \boldsymbol{F}^{\bar{e}}, \boldsymbol{F}^{e}_{G}, \boldsymbol{M}^{\bar{s}}_{G'}, \boldsymbol{K} = K, \boldsymbol{W}^{\bar{e}}) \\
&+ H(\boldsymbol{A}^{\bar{e}}_{G\setminus G'} \mid \boldsymbol{F}^{\bar{e}}, \boldsymbol{F}^{e}_{G}, \boldsymbol{M}^{\bar{s}}_{G'}, \boldsymbol{K} = K, \boldsymbol{W}^{\bar{e}}, \boldsymbol{M}^{\bar{s}}_{G\setminus G'}) \\
&= H(\boldsymbol{A}^{\bar{e}}_{G\setminus G'} \mid \boldsymbol{F}^{\bar{e}}, \boldsymbol{F}^{e}_{G}, \boldsymbol{M}^{\bar{s}}_{G'}, \boldsymbol{K} = K, \boldsymbol{W}^{\bar{e}}) \\
&+ H(\boldsymbol{M}^{\bar{s}}_{G\setminus G'} \mid \boldsymbol{F}^{\bar{e}}, \boldsymbol{F}^{e}_{G}, \boldsymbol{M}^{\bar{s}}_{G'}, \boldsymbol{K} = K, \boldsymbol{W}^{\bar{e}}, \boldsymbol{A}^{\bar{e}}_{G\setminus G'}).
\end{aligned}$$

For $i \in [n], i \neq e$ and $j \in [m]$, we have $F_i(j) = (F_i(j) + r_{j,\pi(i)}) + r_{j,\pi(i)}$. Using property (9), it holds that

$$H(\boldsymbol{A}^{\bar{e}}_{G\setminus G'} \mid \boldsymbol{F}^{\bar{e}}, \boldsymbol{F}^{e}_{G}, \boldsymbol{M}^{\bar{s}}_{G'}, \boldsymbol{K} = K, \boldsymbol{W}^{\bar{e}}, \boldsymbol{M}^{\bar{s}}_{G\setminus G'}) = 0$$

and symetrically

$$H(\boldsymbol{M}^{\bar{s}}_{G\setminus G'} \mid \boldsymbol{F}^{\bar{e}}, \boldsymbol{F}^{e}_{G}, \boldsymbol{M}^{\bar{s}}_{G'}, \boldsymbol{K} = K, \boldsymbol{W}^{\bar{e}}, \boldsymbol{A}^{\bar{e}}_{G\setminus G'}) = 0.$$

It follows that

$$\begin{aligned}
&H(\boldsymbol{M}^{\bar{s}}_{G\setminus G'} \mid \boldsymbol{F}^{\bar{e}}, \boldsymbol{F}^{e}_{G}, \boldsymbol{M}^{\bar{s}}_{G'}, \boldsymbol{K} = K, \boldsymbol{W}^{\bar{e}}) \\
&= H(\boldsymbol{A}^{\bar{e}}_{G\setminus G'} \mid \boldsymbol{F}^{\bar{e}}, \boldsymbol{F}^{e}_{G}, \boldsymbol{M}^{\bar{s}}_{G'}, \boldsymbol{K} = K, \boldsymbol{W}^{\bar{e}}).
\end{aligned}$$

Each mask $r_{j,i}$ ($i \in [n]$, $j \in [m]$) is randomly generated by the trusted initializer and is independent from the other variables held by the different parties at the beginning of the transfer phase. More precisely, if $G_1 \subset [m]$, $G_2 \subset [m]$, $H_1 \subset [n]$ and $H_2 \subset [n]$ are four subsets such that $G_1 \cap G_2 = \emptyset$ or $H_1 \cap H_2 = \emptyset$, we have

$$H(\boldsymbol{M}^{H_1}_{G_1} \mid \boldsymbol{E}, \boldsymbol{S}, \boldsymbol{W}, \boldsymbol{F}, \boldsymbol{M}^{H_2}_{G_2}) = H(\boldsymbol{M}^{H_1}_{G_1}). \tag{23}$$

If we apply property (8) and Lemma 1 (See Appendix A), we obtain the particular case

$$H(\boldsymbol{M}^{\bar{s}}_{G\setminus G'} \mid \boldsymbol{F}^{\bar{e}}, \boldsymbol{F}^{e}_{G}, \boldsymbol{M}^{\bar{s}}_{G'}, \boldsymbol{K} = K, \boldsymbol{W}^{\bar{e}}) = H(\boldsymbol{M}^{\bar{s}}_{G\setminus G'}).$$

Therefore, $H(\boldsymbol{A}^{\bar{e}}_{G\setminus G'} \mid \boldsymbol{F}^{\bar{e}}, \boldsymbol{F}^{e}_{G}, \boldsymbol{M}^{\bar{s}}_{G'}, \boldsymbol{K} = K, \boldsymbol{W}^{\bar{e}}) = H(\boldsymbol{M}^{\bar{s}}_{G\setminus G'})$.
Furthermore, the random variable $\boldsymbol{M}^{\bar{s}}_{G\setminus G'}$ is uniform, so

$$H(\boldsymbol{M}^{\bar{s}}_{G\setminus G'}) = \log_2 p^{(n-1)\times|G\setminus G'|}.$$

Thus,

$$H(\boldsymbol{A}^{\bar{e}}_{G\setminus G'}) \geq H(\boldsymbol{A}^{\bar{e}}_{G\setminus G'} \mid \boldsymbol{F}^{\bar{e}}, \boldsymbol{F}^{e}_{G}, \boldsymbol{M}^{\bar{s}}_{G'}, \boldsymbol{K} = K, \boldsymbol{W}^{\bar{e}}) \qquad \text{(from (1))}$$
$$= \log_2 p^{(n-1)\times|G\setminus G'|}.$$

By property (3), $H(\boldsymbol{A}^{\bar{e}}_{G\setminus G'}) \leq \log_2 p^{(n-1)\times|G\setminus G'|}$.
It follows that $H(\boldsymbol{A}^{\bar{e}}_{G\setminus G'}) = \log_2 p^{(n-1)\times|G\setminus G'|} = H(\boldsymbol{M}^{\bar{s}}_{G\setminus G'})$. We conclude

$$H(\boldsymbol{A}^{\bar{e}}_{G\setminus G'} \mid \boldsymbol{F}^{\bar{e}}, \boldsymbol{F}^{e}_{G}, \boldsymbol{M}^{\bar{s}}_{G'}, \boldsymbol{K} = K, \boldsymbol{W}^{\bar{e}}) = H(\boldsymbol{M}^{\bar{s}}_{G\setminus G'}) = H(\boldsymbol{A}^{\bar{e}}_{G\setminus G'}).$$

Applying property (8), we obtain $H(\boldsymbol{A}^{\bar{e}}_{G\setminus G'} \mid \boldsymbol{F}^{\bar{e}}_{G'}, \boldsymbol{F}^{e}_{G}, \boldsymbol{M}^{\bar{s}}_{G'}, \boldsymbol{K} = K, \boldsymbol{W}^{\bar{e}}) = H(\boldsymbol{A}^{\bar{e}}_{G\setminus G'})$ and consequently

$$H(\boldsymbol{W}^{\bar{e}} \mid \boldsymbol{F}^{\bar{e}}_{G'}, \boldsymbol{F}^{e}_{G}, \boldsymbol{M}^{\bar{s}}_{G'}, \boldsymbol{A}^{\bar{e}}_{G\setminus G'}, \boldsymbol{K} = K) = H(\boldsymbol{W}^{\bar{e}} \mid \boldsymbol{F}^{\bar{e}}_{G'}, \boldsymbol{F}^{e}_{G}, \boldsymbol{M}^{\bar{s}}_{G'}, \boldsymbol{K} = K).$$

3. Once again, we apply property (8) and Lemma 1 to (23) and obtain the particular case

$$H(\boldsymbol{M}^{\bar{s}}_{G'} \mid \boldsymbol{W}^{\bar{e}}, \boldsymbol{F}^{\bar{e}}_{G'}, \boldsymbol{F}^{e}_{G}, \boldsymbol{K} = K) = H(\boldsymbol{M}^{\bar{s}}_{G'}).$$

It follows, from property (7), that

$$H(\boldsymbol{W}^{\bar{e}} \mid \boldsymbol{F}^{\bar{e}}_{G'}, \boldsymbol{F}^{e}_{G}, \boldsymbol{M}^{\bar{s}}_{G'}, \boldsymbol{K} = K) = H(\boldsymbol{W}^{\bar{e}} \mid \boldsymbol{F}^{\bar{e}}_{G'}, \boldsymbol{F}^{e}_{G}, \boldsymbol{K} = K).$$

4. Thanks to Lagrange's interpolation theorem, we can write $H(\boldsymbol{F}^{e}_{G''}, \boldsymbol{W}^{e} \mid \boldsymbol{F}^{e}_{G}) = 0$ and $H(\boldsymbol{F}^{e}_{G} \mid \boldsymbol{F}^{e}_{G''}, \boldsymbol{W}^{e}) = 0$ where G'' is a set of $k-1$ distinct non-null indices. In particular, if $G'' = G'$ ($|G'| = h < k$), we obtain $H(\boldsymbol{F}^{e}_{G'}, \boldsymbol{W}^{e} \mid \boldsymbol{F}^{e}_{G}) = 0$ and $H(\boldsymbol{F}^{e}_{G} \mid \boldsymbol{F}^{e}_{G'}, \boldsymbol{W}^{e}) = 0$. Using property (5), it follows that

$$H(\boldsymbol{W}^{\bar{e}} \mid \boldsymbol{F}^{\bar{e}}_{G'}, \boldsymbol{F}^{e}_{G}, \boldsymbol{K}) = H(\boldsymbol{W}^{\bar{e}} \mid \boldsymbol{F}_{G'}, \boldsymbol{W}^{e}, \boldsymbol{K}).$$

In Sect. 5.4, we have demonstrated that if $|G| < k$ then

$$H(\boldsymbol{W} \mid \boldsymbol{F}_{G}, \boldsymbol{M}_{G}, \boldsymbol{E}, \boldsymbol{S}, \boldsymbol{M}^{\boldsymbol{s}}) = H(\boldsymbol{W}).$$

Applying this property to G' and combining it with property (8) gives

$$H(\boldsymbol{W} \mid \boldsymbol{F}_{G'}, \boldsymbol{K}) = H(\boldsymbol{W}).$$

From property (6), $H(\boldsymbol{W} \mid \boldsymbol{F}_{G'}, \boldsymbol{K}) = H(\boldsymbol{W})$ involves $H(\boldsymbol{F}_{G'}, \boldsymbol{K} \mid \boldsymbol{W}) = H(\boldsymbol{F}_{G'}, \boldsymbol{K})$ and from property (7), $H(\boldsymbol{F}_{G'}, \boldsymbol{K} \mid \boldsymbol{W}) = H(\boldsymbol{F}_{G'}, \boldsymbol{K} \mid \boldsymbol{W}^{e}, \boldsymbol{W}^{\bar{e}}) = H(\boldsymbol{F}_{G'}, \boldsymbol{K})$ involves $H(\boldsymbol{W}^{\bar{e}} \mid \boldsymbol{F}_{G'}, \boldsymbol{K}, \boldsymbol{W}^{e}) = H(\boldsymbol{W}^{\bar{e}} \mid \boldsymbol{W}^{e})$. We assume that the secrets are independent; consequently, $H(\boldsymbol{W}^{\bar{e}} \mid \boldsymbol{W}^{e}) = H(\boldsymbol{W}^{\bar{e}})$, which allows us to conclude $H(\boldsymbol{W}^{\bar{e}} \mid \boldsymbol{F}_{G'}, \boldsymbol{W}^{e}, \boldsymbol{K}) = H(\boldsymbol{W}^{\bar{e}})$, i.e., $H(\boldsymbol{W}^{\bar{e}} \mid \boldsymbol{F}^{\bar{e}}_{G'}, \boldsymbol{F}^{e}_{G}, \boldsymbol{K}) = H(\boldsymbol{W}^{\bar{e}})$. Using Lemma 1, it follows that $H(\boldsymbol{W}^{\bar{e}} \mid \boldsymbol{F}^{\bar{e}}_{G'}, \boldsymbol{F}^{e}_{G}, \boldsymbol{K} = K) = H(\boldsymbol{W}^{\bar{e}})$.

The demonstrations of the four steps above yield that $H(\boldsymbol{W}^{\bar{e}} \mid \boldsymbol{F}_{G'}, \boldsymbol{M}_{G'}, \boldsymbol{E} = e, \boldsymbol{S} = s, \boldsymbol{M}^{\boldsymbol{s}} = (r_{1,s}, \ldots, r_{m,s}), \boldsymbol{Q} = \pi, \boldsymbol{A}_{G}) = H(\boldsymbol{W}^{\bar{e}})$. □

6 Efficiency Consideration

Clearly, the number of shares returned by the servers to the receiver is higher with the proposed protocol (linear communication complexity in n) than with Beimel, Chee, Wang and Zhang's DOT protocols [2] (sublinear communication complexity in n for some PIR protocols). However, in this section, we show that the performance of Blundo et al.'s DOT protocol [4,5] and of our protocol are similar.

In Table 2, we list the main computations performed by each party, for Blundo et al.'s DOT protocol and for our DOT protocol.

Table 2. Computation Efficiency of DOT protocols

	Blundo et al.'s DOT Protocol	Our DOT Protocol
Set-up Phase		
$\mathcal{S}$	$2(n-1)$ random masks in $\mathbb{K}^*$, $2n$ sharing polynomials and $2mn$ shares	n sharing polynomials and mn shares
Commodity Acquisition Phase		
$\mathcal{T}$		mn random masks in $\mathbb{K}$ 1 random number in $[n]$
Transfer Phase		
$\mathcal{R}$	$(n-1)$ sharing polynomials and $k(n-1)$ shares, 4 polynomial interpolations	1 cyclic permutation of $\mathfrak{S}_n$, 1 polynomial interpolation
S_j $(j \in \mathcal{I})$	2 $(n-1)$-tuple scalar products and 2 additions	n additions

Similarly, in Table 3, we list for each protocol the number of shares exchanged between the sender and the servers, the receiver and the servers, and between the trusted initializer and (1) the sender and (2) the receiver in the case of our protocol. We assume that in both protocols, k servers are contacted by the receiver, i.e., $t = k$ in our protocol.

The operations performed off-line (set-up and commodity acquisition phases) for both protocols are close, but in our protocol these operations are distributed between the sender and the trusted initializer. As for the on-line operations, our protocol is more efficient than Blundo et al.'s one: on the receiver's side, only one cyclic permutation and one interpolation are required (vs. the generation of $k(n-1)$ shares from $(n-1)$ sharing polynomials and four interpolations in the case of Blundo et al.'s protocol), whereas on the servers' side, only n additions are required (vs. $2(n-1)$-tuple scalar products and two additions in the case of Blundo et al.'s protocol).

The number of shares distributed by the sender in the set-up phase is around $3n$ in Blundo et al.'s protocol and $2n$ in our protocol. However, our protocol requires an additional distribution of $m(n+1)$ shares by the trusted initializer in the commodity acquisition phase. In the transfer phase, the request sent to

Table 3. Communication Efficiency of DOT protocols (shares)

	Blundo et al.'s DOT Protocol	Our DOT Protocol
Set-up Phase		
$\mathcal{S} \to S_j$ $(j \in [m])$	$2n$ shares, $n-1$ elements of $\mathbb{K}$	n shares
Commodity Acquisition Phase		
$\mathcal{T} \to S_j$ $(j \in \mathcal{I})$		n masks
$\mathcal{T} \to \mathcal{R}$		1 index, m masks
Transfer Phase		
$\mathcal{R} \to S_j$ $(j \in \mathcal{I})$	$n-1$ shares	$t = k$ server indices, 1 number in $[n]$ (nota: broadcast data)
$S_j \to \mathcal{R}$ $(j \in \mathcal{I})$	$2n$ shares	n shares

a server contains $n-1$ shares (Blundo et al.'s protocol) whereas the broadcast request contains $k+1$ integers (our protocol). The receiver collects two times more shares in Blundo et al.'s protocol than in our protocol.

We also note that our DOT protocol can easily be extended to a DOT-$\binom{n}{\ell}$; instead of choosing one set of random masks, the trusted initializer randomly selects ℓ sets of random masks and distributes them to the receiver in the commodity acquisition phase, with the corresponding indices $s_1, \ldots, s_\ell$. In this scenario, the receiver selects ℓ indices $e_1, \ldots, e_\ell$ and generates a random permutation π, instead of a cyclic permutation, such that $\pi(e_1) = s_1, \ldots, \pi(e_\ell) = s_\ell$. The operations executed by the servers are the same as in the case where the receiver wishes to obtain one secret only. On reception of the responses, the receiver has to interpolate ℓ polynomials to determine the ℓ chosen secrets. Therefore, in our protocol, due to the constant number of operations performed by the servers and to the constant number of data exchanged between the servers and the receiver, the communication and computation performance, relative to ℓ, improves when ℓ increases. Blundo et al.'s DOT protocol would need to be executed ℓ times for ℓ secrets, which would be less efficient than our protocol.

In a similar vein, the protocol may easily be extended to a verifiable DOT, with the simple requirement that enough shares are collected by the receiver to identify – and discard – incorrect shares returned by malicious servers. Thus, a Reed-Solomon codes [14] decoding algorithm like the algorithm introduced by Gao [9] would allow the receiver to determine the chosen secret in spite of $u \leq \frac{t-k}{2}$ malicious servers.

Acknowledgements. We would like to thank the anonymous reviewers of ICISC 2012 for their helpful comments.

References

1. Beaver, D.: Commodity-based cryptography. In: Proceedings of the Twenty-Ninth Annual ACM Symposium on Theory of Computing, pp. 446–455. ACM (1997)
2. Beimel, A., Chee, Y.M., Wang, H., Zhang, L.F.: Communication-efficient distributed oblivious transfer. Journal of Computer and System Sciences 78(4), 1142–1157 (2012)
3. Bennett, C.H., Brassard, G., Crépeau, C., Skubiszewska, M.-H.: Practical Quantum Oblivious Transfer. In: Feigenbaum, J. (ed.) CRYPTO 1991. LNCS, vol. 576, pp. 351–366. Springer, Heidelberg (1992)
4. Blundo, C., D'Arco, P., De Santis, A., Stinson, D.R.: New Results on Unconditionally Secure Distributed Oblivious Transfer. In: Nyberg, K., Heys, H.M. (eds.) SAC 2002. LNCS, vol. 2595, pp. 291–309. Springer, Heidelberg (2003)
5. Blundo, C., D'Arco, P., De Santis, A., Stinson, D.R.: On Unconditionally Secure Distributed Oblivious Transfer. Journal of Cryptology 20(3), 323–373 (2007)
6. Brassard, G., Crépeau, C., Robert, J.M.: All-or-Nothing Disclosure of Secrets. In: Odlyzko, A.M. (ed.) CRYPTO 1986. LNCS, vol. 263, pp. 234–238. Springer, Heidelberg (1987)
7. Cover, T.M., Thomas, J.A.: Elements of Information Theory, 2nd edn. John Wiley & Sons, Inc., Hoboken (2006)
8. Even, S., Goldreich, O., Lempel, A.: A Randomized Protocol for Signing Contracts. Communications of the ACM 28, 637–647 (1985)
9. Gao, S.: A new algorithm for decoding Reed-Solomon codes. In: Bhargava, V.K., Poor, H.V., Tarokh, V., Yoon, S. (eds.) Communications, Information and Network Security, pp. 55–68. Kluwer Academic Publishers (2003)
10. Gertner, Y., Malkin, T.: Efficient Distributed (n choose 1) Oblivious Transfer. Tech. rep., MIT Lab of Computer Science (1997)
11. Naor, M., Pinkas, B.: Distributed Oblivious Transfer. In: Okamoto, T. (ed.) ASIACRYPT 2000. LNCS, vol. 1976, pp. 205–219. Springer, Heidelberg (2000)
12. Nikov, V., Nikova, S., Preneel, B., Vandewalle, J.: On Unconditionally Secure Distributed Oblivious Transfer. In: Menezes, A., Sarkar, P. (eds.) INDOCRYPT 2002. LNCS, vol. 2551, pp. 395–408. Springer, Heidelberg (2002)
13. Rabin, M.O.: How to Exchange Secrets with Oblivious Transfer. Tech. rep., Aiken Computation Lab, Harvard University (1981)
14. Reed, I., Solomon, G.: Polynomial codes over certain finite fields. Journal of the Society for Industrial and Applied Mathematics 8(2), 300–304 (1960)
15. Rivest, R.L.: Unconditionally Secure Commitment and Oblivious Transfer Schemes Using Private Channels and a Trusted Initializer (1999) (unpublished manuscript)
16. Shamir, A.: How to Share a Secret. Communications of the ACM 22(11), 612–613 (1979)
17. Shannon, C.E.: A Mathematical Theory of Communication. Bell System Technology Journal 27, 379–423, 623–656 (1948)

A Conditional Entropy with Fixed Condition

Let $\boldsymbol{X}$, $\boldsymbol{Y}$ and $\boldsymbol{Z}$ be three random variables.

Lemma 1. *If* $H(\boldsymbol{X} \mid \boldsymbol{Y}, \boldsymbol{Z}) = H(\boldsymbol{X})$ *then for* $z_i \in \mathcal{Z}$ *we have* $H(\boldsymbol{X} \mid \boldsymbol{Y}, \boldsymbol{Z} = z_i) = H(\boldsymbol{X})$.

Proof.

Because $H(\boldsymbol{X} \mid \boldsymbol{Y}, \boldsymbol{Z}) = H(\boldsymbol{X})$, the variables $\boldsymbol{X}$ and $(\boldsymbol{Y}, \boldsymbol{Z})$ are independent. Their corresponding probabilities satisfy the relation $\Pr(\boldsymbol{X} = x, \boldsymbol{Y} = y, \boldsymbol{Z} = z) = \Pr(\boldsymbol{X} = x) \Pr(\boldsymbol{Y} = y, \boldsymbol{Z} = z)$ for $(x, y, z) \in \mathcal{X} \times \mathcal{Y} \times \mathcal{Z}$. That is, $\Pr(\boldsymbol{X} = x \mid \boldsymbol{Y} = y, \boldsymbol{Z} = z) = \Pr(\boldsymbol{X} = x, \boldsymbol{Y} = y, \boldsymbol{Z} = z) / \Pr(\boldsymbol{Y} = y, \boldsymbol{Z} = z) = \Pr(\boldsymbol{X} = x)$. Hence

$$
\begin{aligned}
& H(\boldsymbol{X} \mid \boldsymbol{Y}, \boldsymbol{Z} = z_i) \\
&\quad = \sum_{y \in \mathcal{Y}} \Pr(\boldsymbol{Y} = y) \times H(\boldsymbol{X} \mid \boldsymbol{Y} = y, \boldsymbol{Z} = z_i) \\
&\quad = \sum_{y \in \mathcal{Y}} \Big(\Pr(\boldsymbol{Y} = y) \\
&\qquad \times - \sum_{x \in \mathcal{X}} \Pr(\boldsymbol{X} = x \mid \boldsymbol{Y} = y, \boldsymbol{Z} = z_i) \log_2 \Pr(\boldsymbol{X} = x \mid \boldsymbol{Y} = y, \boldsymbol{Z} = z_i) \Big) \\
&\quad = \sum_{y \in \mathcal{Y}} \Big(\Pr(\boldsymbol{Y} = y) \times - \sum_{x \in \mathcal{X}} \Pr(\boldsymbol{X} = x) \log_2 \Pr(\boldsymbol{X} = x) \Big) \\
&\quad = \sum_{y \in \mathcal{Y}} \Pr(\boldsymbol{Y} = y) \times H(\boldsymbol{X}) \\
&\quad = H(\boldsymbol{X})
\end{aligned}
$$

□