One-out-of-q OT Combiners

Oriol Farràs and Jordi Ribes-González

Universitat Rovira i Virgili, Tarragona, Spain
{oriol.farras,jordi.ribes}@urv.cat

Abstract. In 1-*out-of-q Oblivious Transfer (OT)* protocols, a sender Alice is able to send one of $q \geq 2$ messages to a receiver Bob, all while being oblivious to which message was transferred. Moreover, the receiver learns only one of these messages. *Oblivious Transfer combiners* take n instances of OT protocols as input, and produce an OT protocol that is secure if sufficiently many of the n original OT instances are secure.
We present new 1-out-of-q OT combiners that are perfectly secure against active adversaries. Our combiners arise from secret sharing techniques. We show that given an $\mathbb{F}_q$-linear secret sharing scheme on a set of n participants and adversary structure $\mathcal{A}$, we can construct n-server, 1-out-of-q OT combiners that are secure against an adversary corrupting either Alice and a set of servers in $\mathcal{A}$, or Bob and a set of servers B with $\bar{B} \notin \mathcal{A}$. If the normalized total share size of the scheme is ℓ, then the resulting OT combiner requires ℓ calls to OT protocols, and the total amount of bits exchanged during the protocol is $(q^2+q+1)\ell \log q$.
We also present a construction based on 1-out-of-2 OT combiners that uses the protocol of Crépeau, Brassard and Robert (FOCS 1986). This construction provides smaller communication costs for certain adversary structures, such as threshold ones: For any prime power $q \geq n$, there are n-server, 1-out-of-q OT combiners that are perfectly secure against active adversaries corrupting either Alice or Bob, and a minority of the OT candidates, exchanging $O(qn \log q)$ bits in total.

Keywords: Oblivious transfer · OT combiners · Secret sharing schemes

1 Introduction

Oblivious Transfer (OT) protocols involve two parties, a *sender* and a *receiver*, which we also respectively name Alice and Bob. The functionality provided by OT consists in allowing the sender to transfer part of its inputs to the receiver, while guaranteeing that the sender is oblivious to which part of its inputs is actually obtained by the receiver. It also guarantees that the receiver is not able learn more information than it is entitled to as per the protocol.

OT protocols were first introduced by Rabin [45] in 1981. In 1-*out-of-*2 *OT* protocols [23], the sender holds two messages, and the receiver chooses to receive one of them from the sender. Security here consists in the sender being oblivious to the message that was actually transferred, and the receiver getting information on only one of the messages. The type of OT that we study here is called 1-*out-of-q OT*. It is a generalization of 1-out-of-2 OT, first presented by Crépeau, Brassard and Robert [19] in 1986. It lets the sender hold $q \geq 2$ messages instead of just two, and allows the receiver to fetch only one of those messages. The relevance of OT protocols in cryptography lies in their role as a fundamental primitive in many cryptographic constructions. The main functionalities OT has found an application to are secure multi-party computation, zero-knowledge proofs and bit commitment schemes (see [10,32,33,48], for example).

The security of OT protocols is necessarily conditional, since perfectly secure OT protocols would yield unconditionally-secure two-party computation by [32], which is impossible to obtain for some functions (see [11,17]). Hence, the security of OT protocols is based on computational hardness assumptions such as the hardness of RSA [45], the DDH assumption [1,10], code-based assumptions [22] and also lattice-based assumptions [43]. Alternatively, the security of OT can be guaranteed by the existence of a noisy channel between both parties [20], the use of hardware tokens [25], restrictions on the storage [13], and other ways. The conditional security of OT protocols implies that the security guarantees of OT could be compromised. The standard method to mitigate this concern consists in grounding security on various assumptions at once, by simultaneously using several implementations. This motivates the use of OT combiners.

The notion of *combiner* consists of blending various cryptographic implementations into one, so that the resulting combination is secure even if some of the original implementations are insecure. Combiners have been previously studied in other areas of cryptography, for instance in multi-factor authentication, where many authentication methods are used concurrently, as well as in cascading of block ciphers or hybrid key encapsulation.

Using an *OT combiner*, a set of n candidate implementations of OT can be merged to realize a single OT protocol. In other words, an OT combiner can be used to instantiate a protocol between a sender Alice and a receiver Bob that realizes OT by internally using n candidate OT implementations. The resulting protocol is secure as long as sufficiently many of the initial implementations were secure to begin with.

An OT combiner is *black-box* if, during the combined protocol, the candidate OT implementations are used in a black-box way, i.e. ignoring their internal workings. In this work, we only consider black-box OT combiners. Under this assumption, as in [16], we view OT combiners as *server-aided* OT protocols. This means that we model each of the OT candidate implementations as a *server* that implements the 1-out-of-q OT functionality, i.e. that receives q messages $m_0, \ldots, m_{q-1}$ from Alice and an index b from Bob, and outputs the message m_b to Bob. We then say that an OT combiner is *n-server* if it takes n OT candidates as input. An OT combiner is *single-use* if each OT candidate is used only once during the execution of the protocol. In contrast, an OT combiner is *multi-use* if, during the protocol, an OT candidate can be used more than once.

1.1 Related Work

The study of OT combiners was initiated by Harnik, Kilian, Naor, Reingold and Rosen [27] in 2005. They define the notion of (n,t)-*OT combiner*, which consists in taking n candidate 1-out-of-2 OT implementations and combining them into a 1-out-of-2 OT protocol that is secure provided at most t of the OT candidates are faulty. They show that, when $t < n/2$, there exist (n, t)-OT combiners that are unconditionally secure against passive (i.e. semi-honest) adversaries. They prove the tightness of this bound and show that such OT combiners cannot exist for $n = 2, t = 1$. They also build a $(3, 1)$-OT combiner that uses each OT instance twice.

Meier, Przydatek and Wullschleger [39] present OT combiners that implement the 1-out-of-2 OT functionality and are unconditionally secure against passive adversaries that corrupt either Alice and a number t_A of OT candidates, or Bob and t_B OT candidates for any $t_A + t_B < n$. These protocols were later called (n, t_A, t_B)*-OT combiners*. Their combiner is multi-use, and it makes two calls to each OT candidate.

Harnik, Ishai, Kushilevitz and Nielsen [26] present a statistically secure (n, t, t)-OT combiner for $t = \Omega(n)$, which makes a constant number of calls to each OT candidate. Their solution is set in the 1-out-of-2 scenario. Additionally, [26] gives a computationally secure OT combiner against active adversaries. Subsequently, Ishai, Prabhakaran and Sahai [29] show that this construction can be turned into an (n, t, t)-OT combiner that is statistically secure against active adversaries for $t = \Omega(n)$. Ishai, Maji, Sahai and Wullschleger [28] present a single-use (n, t, t)-OT combiner that is statistically secure against passive adversaries for $t = n/2 - \omega(\log \kappa)$, where κ is the security parameter.

Regarding the relation between other primitives and OT, Przydatek and Wullschleger [44] study the relation of Oblivious Linear Function Evaluation (OLFE) with OT. A two-party OLFE protocol allows a receiver to learn the evaluation of a linear polynomial function f over $\mathbb{F}_q$ of its choice on an input value $x \in \mathbb{F}_q$ held by the receiver, so that each party learns no information about the input of the other party. Przydatek and Wullschleger consider combiners that take a set of n OLFE candidate implementations and produce a 1-out-of-2 OT protocol. Their solution is also unconditionally secure for $t_A + t_B < n$. However, it requires the size of the message space to be larger than the number n of candidate implementations of OLFE to combine.

Another variant of combiners for OT is that of *cross-primitive combiners*, studied by Meier and Przydatek in [38]. As in [44], here the combiner implements a different functionality than the candidates. They present a $(2, 1)$*-PIR-to-OT combiner*, which takes two Private Information Retrieval (PIR) schemes and produces a 1-out-of-2 OT protocol that is unconditionally secure for the sender, provided one of the two PIR schemes is also secure. This result comes in contrast with the impossibility result of [27]. Their construction only guarantees the privacy of Alice against a honest-but-curious adversary corrupting Bob and one of the two candidates.

Following [28], Cascudo, Damgård, Farràs and Ranellucci [16] achieve single-use 1-out-of-2 OT combiners. They generalize the security notion in [26] by defining the notion of *perfect security against active* $(\mathcal{A}, \mathcal{B})$*-adversaries* for some $\mathcal{A}, \mathcal{B} \subseteq 2^{\mathcal{P}_n}$, where $\mathcal{P}_n = \{1, \ldots, n\}$ denotes the set of OT candidates. We also adopt this notion. This definition considers an active adversary that can corrupt either Alice and a set $A \in \mathcal{A}$ of OT candidates, or Bob and a set $B \in \mathcal{B}$ of OT candidates, obtaining their inputs and full control of their outputs. Their OT combiner achieves perfect (unconditional, zero-error) security against $(\mathcal{A}, \mathcal{B})$-adversaries so that $A \cup B \neq \mathcal{P}_n$ for every $A \in \mathcal{A}$ and $B \in \mathcal{B}$. When this last condition is fulfilled, we say that the pair $(\mathcal{A}, \mathcal{B})$ of adversary structures is $\mathcal{R}_2$. They prove this to be a necessary condition for security.

All the works mentioned above combine 1-out-of-2 OT primitives into 1-out-of-2 OT. So far, to the best of our knowledge, there are no explicit 1-out-of-q OT combiner constructions in the literature. Two similar works [19,40] build 1-out-of-q OT for $q > 2$ by re-using a single 1-out-of-2 OT instance as many as $q - 1$ [19] or $\log q$ [40] times. However, seeing these constructions directly as 1-out-of-q OT combiners makes them insecure, as a single faulty 1-out-of-2 OT candidate results in an insecure 1-out-of-q OT protocol. In this work, we explore 1-out-of-q OT combiners with better security guarantees.

Our OT combiners are built using a specific kind of secret sharing schemes that has been studied in previous works. Given a Boolean function $f : \{0,1\}^n \to \{0,1\}$, consider the access structure on the set of participants $P = \{1, \ldots, n\} \times \{0,1\}$ whose minimal authorized subsets are $\{(1, x_1), \ldots, (n, x_n)\}$ that satisfy $f(x_1, \ldots, x_n) = 1$ and the subsets $\{(i,0), (i,1)\}$ for $1 \leq i \leq n$. Efficient constructions are known [7,47] for some of these structures. Liu, Vaikuntanathan and Wee [36] present more efficient schemes, and show a connection between these schemes and Conditional Disclosure of Secrets (CDS) protocols [24], namely for CDS protocols for the INDEX predicate. That connection is used to construct better general constructions for secret sharing [2,3,35,8]. In this work, we study access structures determined by functions $f : \{0, \ldots, q-1\}^n \to \{0,1\}$, a case studied for example in [2,3,24].

1.2 Our Work

This work deals with the construction of efficient 1-out-of-q OT combiners for any $q \geq 2$. We extend the security and consistency notions of [16] from the 1-out-of-2 case to the 1-out-of-q case, and we present OT combiners that attain perfect security against active $(\mathcal{A}, \mathcal{B})$-adversaries. As far as we know, this is the first work that achieves efficient 1-out-of-q OT combiners with active security for any $q \geq 2$. Our main result is the following theorem, which is constructive.

Theorem 1.1. *Let $\mathbb{F}_q$ be a finite field, let Σ be an $\mathbb{F}_q$-linear secret sharing scheme on $\mathcal{P}_n$ with adversary structure $\mathcal{A}$ and normalized total share size ℓ, and let $\mathcal{B} \subseteq 2^{\mathcal{P}_n}$ satisfying that $(\mathcal{A}, \mathcal{B})$ is $\mathcal{R}_2$. Then there exists an n-server, 1-out-of-q OT combiner for messages in $\mathbb{F}_q$ that is perfectly secure against any active $(\mathcal{A}, \mathcal{B})$-adversary and requires exchanging $(q^2 + q + 1)\ell \log q$ bits. If Σ is ideal, then the OT combiner is single-use.*

As a corollary of this theorem and [16], we have that $(\mathcal{A}, \mathcal{B})$ admits a 1-out-of-q OT combiner if and only if $(\mathcal{A}, \mathcal{B})$ is $\mathcal{R}_2$. It was already known for $q = 2$ [16], but not for greater q.

The communication cost of this theorem does not take into account the communication cost of the OT instantiations, because our combiner is black-box. Our combiner is stated in the server model, with each server representing a different OT instantiation, and all exchanged information passes through the servers. The communication cost thus refers to the length of the input and output of servers. Moreover it is worth noting that, while messages are assumed to be in $\mathbb{F}_q$, servers take messages in $\mathbb{F}_q^q$ as input. Hence, the used OT candidates are assumed to implement 1-out-of-q OT with $q \log q$-bit strings.

This OT combiner makes use of the OT implementations a total of ℓ times. That is, the communication complexity increases linearly with the normalized total share size of Σ. Therefore, in our construction, the search of efficient OT combiners is reduced to the search of efficient linear secret sharing schemes. We build 1-out-of-q OT combiners for those pairs of $\mathcal{R}_2$ adversary structures $(\mathcal{A}, \mathcal{B})$ for which there exist $\mathbb{F}_q$-linear secret sharing schemes with an adversary structure $\mathcal{C}$ satisfying $\mathcal{A} \subseteq \mathcal{C}$ and $\mathcal{B} \subseteq \mathcal{C}^* = \{C \subseteq \mathcal{P}_n : \mathcal{P}_n \setminus C \notin \mathcal{C}\}$. In the threshold case, we have the following result.

Corollary 1.2. *Let q be a prime power and let $2 \leq n \leq q$. There exists a single-use, n-server, 1-out-of-q OT combiner that is perfectly secure against active adversaries corrupting either Alice or Bob, and a minority of the OT candidates. The amount of bits exchanged during the protocol is $(q^2 + q + 1)n \log q$.*

In the process of building our 1-out-of-q OT combiners, we study secret sharing schemes associated to affine spaces. Namely, let $W \subseteq \mathbb{F}_q^n$ be an affine space, and let $f : \mathbb{F}_q^n \to \{0, 1\}$ be the Boolean function with $f(x_1, \ldots, x_n) = 1$ if and only if $(x_1, \ldots, x_n) \in W$. We present ideal linear secret sharing schemes on the set of nq participants $\{1, \ldots, n\} \times \mathbb{F}_q$ in which a subset $\{(1, v_1), \ldots, (n, v_n)\}$ is authorized if and only if $f(v_1, \ldots, v_n) = 1$. Moreover, from our schemes, it is possible to build n-server CDS protocols for f with domain of secrets $\mathbb{F}_q$, and with optimal message size and certain *robustness*, in the sense of [2].

We also describe a 1-out-of-q OT combiner with similar security properties that uses the 1-out-of-q OT construction by Crépeau, Brassard and Robert [19]. It consists in combining 1-out-of-2 OT combiners. This construction relies on $\mathbb{F}_2$-linear secret sharing schemes and 1-out-of-2 OT protocols. For threshold adversary structures and single-bit messages, the communication complexity is $(3q - 1)n \log n$. This construction allows for an arbitrary number of messages $q \geq 2$ instead of only a prime power. It is highly multi-use, as each of the 1-out-of-2 OT instances is executed $q \log n$ times. To support messages larger than one bit, the protocol is replicated and combined with zigzag functions [19].

Theorem 1.3. *Let $2 \leq n \leq q$ and $t < n/2$. There exists an n-server, 1-out-of-q OT combiner, with messages of bitsize $s \geq 1$, that is perfectly secure against active adversaries corrupting either Alice or Bob and less than t OT candidates. It requires exchanging $O(qns^{1.6} \log n)$ bits, and $O(qs^{1.6} \log n)$ calls to each 1-out-of-2 OT instance.*

In general, given an $\mathcal{R}_2$ pair $(\mathcal{A}, \mathcal{B})$, the convenience of one of the constructions proposed here over others will depend on the share size of $\mathbb{F}$-linear secret sharing schemes for $(\mathcal{A}, \mathcal{B})$ for $\mathbb{F} = \mathbb{F}_2$ or $\mathbb{F} = \mathbb{F}_q$. Notice that the power of linear secret sharing schemes over fields of different characteristics is incomparable. Indeed, there is a super-polynomial separation between any two fields with different characteristics [9].

For messages of $\log q$ bits, $q \geq n$, and for $t < n/2$, Corollary 1.2 provides 1-out-of-q OT-combiners for t-threshold structures $\mathcal{A}$ and $\mathcal{B}$ that are single-use and for which the number of exchanged bits is $O(q^2 n \log q)$. The construction of Theorem 1.3 requires less communication, $O(qn \log n \log^2 q)$, but requires $O(q \log n \log^2 q)$ calls to each one of the 1-out-of-2 OT instances.

1.3 Overview of Our Constructions

Next, we describe the structure of the main constructions of this work (laid out in Sections 4 and 7). Take n servers $S_1, \ldots, S_n$, each one performing the 1-out-of-q OT functionality. Bob holds $b \in \mathbb{F}_q$, and Alice holds some messages $m_0, \ldots, m_{q-1} \in \mathbb{F}_q$. At the end of the protocol, Bob can recover m_b, while Alice does not get information about b.

Bob creates n shares of b with an ideal secret sharing scheme Σ, and sends one share to each server. That is, the server S_i receives a share $b_i \in \mathbb{F}_q$, which will be the selection input of the OT functionality of S_i. Independently, Alice creates shares of her messages. Alice creates nq shares of the message m_0 with some special secret sharing scheme $\mathcal{S}_0$. These shares $m_0^{(i,j)} \in \mathbb{F}_q$ are indexed by $(i,j) \in \{1 \ldots n\} \times \{0 \ldots q-1\}$. Then, Alice creates shares of the rest of messages m_k, each with a different scheme $\mathcal{S}_k$, obtaining the shares $m_k^{(i,j)}$ with $(i,j) \in \{1 \ldots n\} \times \{0 \ldots q-1\}$. All these shares are packed in strings $u_i^j = m_0^{(i,j)} || m_1^{(i,j)} || \cdots || m_{q-1}^{(i,j)} \in \mathbb{F}_q^q$, and Alice sends $u_i^0, \ldots, u_i^{q-1}$ to server S_i for each $1 \leq i \leq n$. Then, server S_i performs the 1-out-of-q OT functionality with the inputs received from Alice and Bob. Namely, S_i outputs $u_i^{b_i}$ to Bob. Finally, Bob collects all messages sent by the servers, and recovers m_b. A diagram of the protocol for the case $q = 4$ and $n = 3$ is presented in Figure 1.

In this setting, Σ and $\mathcal{S}_0, \ldots, \mathcal{S}_{q-1}$ must be chosen in such a way that the functionality is performed correctly. Roughly speaking, if $b_1, \ldots, b_n$ is a valid sharing of b by Σ, then it must be possible to recover m_b from $u_1^{b_1}, \ldots, u_n^{b_n}$. Hence, the subsets $\{(1, b_1), \ldots, (n, b_n)\}$ must be authorized sets of $\mathcal{S}_b$ if $b_1, \ldots, b_n$ is a valid share of b. Regarding security, if Bob can recover m_b, he must not be able to obtain any information about other m_k for $k \neq b$. Hence, in this case, $u_1^{b_1}, \ldots, u_n^{b_n}$ must not provide any information about m_k, and so $\{(1, b_1), \ldots, (n, b_n)\}$ must be a forbidden subset of $\mathcal{S}_k$.

Additionally, our OT combiners guarantee protection against adversaries taking control of Alice and some servers $A \in \mathcal{A}$, or Bob and some servers $B \in \mathcal{B}$. This protection is guaranteed by restricting the access structures of the secret sharing schemes Σ and $\mathcal{S}_k$ to these requirements, while preserving correctness (see an introduction to secret sharing in Section 2.1). In general, given a secret sharing scheme Σ, it is not known if there exist efficient schemes $\mathcal{S}_0, \ldots, \mathcal{S}_{q-1}$ adapted to the shares of Σ.

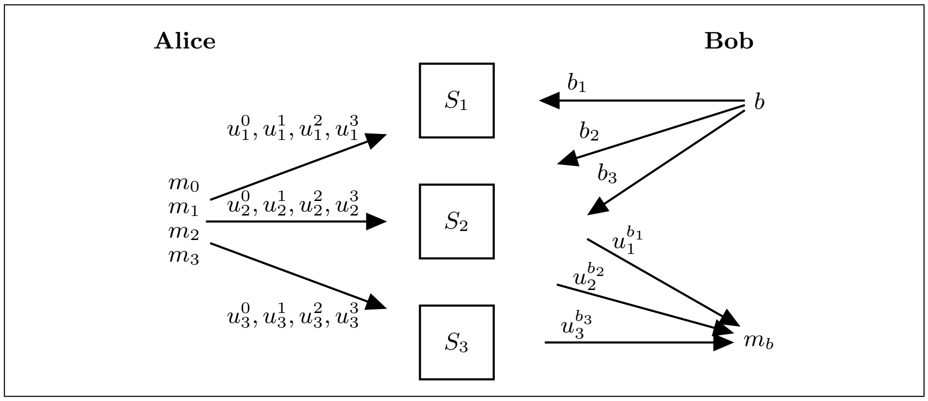

Fig. 1. Diagram of a 1-out-of-4 OT combiner for $n = 3$.

One of the main contributions of this work is that, when Σ is ideal and $\mathbb{F}_q$-linear, we find schemes $\mathcal{S}_0, \ldots, \mathcal{S}_{q-1}$ that are ideal, $\mathbb{F}_q$-linear, and satisfy the desired security restrictions. These schemes additionally satisfy the property that any set of shares is valid, as long as shares belong to the correct domain, in the sense that a corresponding secret can always be extracted from the shares received by Bob. As a consequence, we obtain an efficient, single-use, n-server, 1-out-of-q OT combiner. Hence, given an $\mathcal{R}_2$ pair of adversary structures $(\mathcal{A}, \mathcal{B})$, if $\mathcal{A}$ admits an ideal $\mathbb{F}_q$-linear secret sharing scheme, then the resulting OT combiner is perfectly secure against active $(\mathcal{A}, \mathcal{B})$-adversaries. Here, the main difficulty lies in constructing the schemes $\mathcal{S}_k$. As mentioned above, subsets $\{(1, b_1), \ldots, (n, b_n)\}$ for sharings of b must be authorized for $b = k$ and forbidden if $b \neq k$. Additionally, since we guarantee perfect security against an active adversary controlling Alice and servers $\{S_i\}_{i \in A}$ for any $A \in \mathcal{A}$, it must not be possible to obtain b from $\{b_i\}_{i \in A}$. And, since we guarantee perfect security against an active adversary controlling Bob and servers $\{S_i\}_{i \in B}$ for any $B \in \mathcal{B}$, the subset $\{(1, b_1), \ldots, (n, b_n)\} \cup \{(i, j) : i \in B, 0 \leq j < q\}$ must be forbidden in $\mathcal{S}_k$ for every $b \neq k$.

In the construction of Theorem 1.1 we use the fact that, if a secret sharing scheme Σ is $\mathbb{F}_q$-linear, then the family of sharings of $b \in \mathbb{F}_q$ form an affine space in $\mathbb{F}_q^n$. Our schemes $\mathcal{S}_k$, as the ones in [16] for $q = 2$, exploit this property. However, the case $q = 2$ differs from the case $q > 2$ in the following sense. For every $\mathbb{F}_2$-affine space W, there exists an ideal $\mathbb{F}_2$-linear secret sharing scheme whose minimal authorized subsets are vectors in W. However, for $q > 2$, $\mathbb{F}_q$-affine spaces do not admit ideal $\mathbb{F}_q$-linear secret sharing schemes, in general.

We circumvent this problem by finding a sufficient condition for a secret sharing scheme to be used as a building block of our OT combiner. We call this condition W-OT-compatibility. Then we prove that the schemes $\mathcal{S}_k$ that are the natural extension of the ones in [16] are indeed W-OT-compatible.

In case that Σ is a non-ideal $\mathbb{F}_q$-linear secret sharing scheme with adversary structure $\mathcal{A}$, we can still construct OT combiners that are perfectly secure against active $(\mathcal{A}, \mathcal{B})$-adversaries. However, they are multi-use, as they require some servers to perform more than one OT execution. The number of OT executions coincides with the normalized total share size of Σ. In this case, we transform Σ into an ideal $\mathbb{F}_q$-linear scheme Σ' defined on an extended set of participants, and we run the protocol for the ideal case with Σ'.

1.4 Paper Organization

In Section 2, we lay out the preliminaries on secret sharing and OT combiners. Section 3 states the correctness and security definitions of OT combiners. In Section 4, we present our single-use 1-out-of-q OT combiner. The results of this section imply Corollary 1.2. Section 5 analyzes the secret sharing schemes used in our constructions, and Section 6 presents the correctness and security proofs of this combiner. In Section 7, we extend our construction to the general case where the underlying scheme is not ideal, obtaining a multi-use OT combiner. Results in Sections 4 and 7 imply Theorem 1.1. Finally, we present constructions of 1-out-of-q OT combiners built from 1-out-of-2 OT combiners in Section 8, from which Theorem 1.3 is deduced.

2 Preliminaries

In this section, we lay out the background theory needed in the rest of the article. In Sections 2.1 and 2.2 we give an account of secret sharing and we present OT combiners in Section 2.3.

From now on, unless it is stated otherwise, q denotes an arbitrary positive prime power. By abuse of notation, we denote the finite field of q elements as $\mathbb{F}_q = \{0, \ldots, q-1\}$. The *power set* of a set P is $2^P := \{A \ : \ A \subseteq P\}$. Given an integer $n \geq 2$, we denote $\mathcal{P}_n := \{1, \ldots, n\}$ and $\mathcal{P}_{n,q} := \mathcal{P}_n \times \mathbb{F}_q = \{(i,j) \ : \ i \in \mathcal{P}_n,\, j \in \mathbb{F}_q\}$. We also consider the partition $\mathcal{P}_{n,q} = P_1 \cup \ldots \cup P_n$, where $P_i := \{(i,0), (i,1) \ldots, (i, q-1)\}$ for $i = 1, \ldots, n$. For any $A \subseteq \mathcal{P}_n$ we denote $\bar{A} = \mathcal{P}_n \setminus A$. For any $\mathcal{A} \subseteq 2^{\mathcal{P}_n}$ we define its *dual* as $\mathcal{A}^* = \{A \subseteq \mathcal{P}_n : \bar{A} \notin \mathcal{A}\}$.

2.1 Secret Sharing Schemes

For convenience, we take the definition of secret sharing scheme from [16], which is equivalent to the standard one [5]. For an introduction to this field, see [5,42].

Definition 2.1 ([16]). *A* secret sharing scheme *Σ on a set of participants $P = \{1, \ldots, n\}$ consists of the following two algorithms*

$(x_1, \ldots, x_n) \leftarrow \mathsf{Share}_\Sigma(s, \mathbf{r})$**:** *Probabilistic algorithm that takes as input a* secret *s, belonging to a finite set E_0, and some randomness $\mathbf{r}$ in a set Ω. It returns an array of values $(x_1, \ldots, x_n)$, where each x_i belongs to some finite set E_i. This array is called a* sharing *of s, and each of its elements is a* share *of s.*

$s \leftarrow \mathsf{Reconstruct}_\Sigma((i, x_i)_{i \in A})$**:** *Algorithm that takes a set of pairs $(i, x_i)_{i \in A}$ as input for some $A \subseteq P$, where $x_i \in E_i$. It returns either a secret s, or $\perp$.*

The normalized *total share size is* $\sum_{i=1}^{n} \log|E_i| / \log|E_0|$.

Following the notation of [16], given a secret s and randomness $\mathbf{r}$, we denote a sharing of the secret s by $[s, \mathbf{r}]_\Sigma = \mathsf{Share}_\Sigma(s, \mathbf{r})$. Whenever we can safely drop the randomness $\mathbf{r}$, we denote this sharing by $[s]_\Sigma$. The indexes i of shares x_i in the input to $\mathsf{Reconstruct}_\Sigma$ are omitted when implicitly clear. With this notation, we continue with more definitions. Let $A \subseteq P$. We say that

- A is *authorized* for Σ if, for every secret s, provided the shares $(x_i)_{i\in A}$ are part of a sharing of s, the function $\mathsf{Reconstruct}((i, x_i)_{i\in A})$ recovers s with probability one. That is, if, for every secret s,
$$\mathsf{Pr}[\mathsf{Reconstruct}_\Sigma((\mathsf{Share}_\Sigma(s, \mathbf{r}))_A) = s] = 1.$$
- A is *forbidden* for Σ when the shares $(x_i)_{i\in A}$ of participants in A do not reveal any information on the secret value s. That is, if, for every $s, s' \in E_0$, and every $(x_i)_{i\in A} \in \prod_{i\in A} E_i$,
$$\mathsf{Pr}[(\mathsf{Share}_\Sigma(s, \mathbf{r}))_A = (x_i)_{i\in A}] = \mathsf{Pr}[(\mathsf{Share}_\Sigma(s', \mathbf{r}))_A = (x_i)_{i\in A}].$$

We define the *access structure* of a scheme Σ as the family of all its authorized subsets, and the *adversary structure* of Σ is the family of its forbidden subsets. We say that Σ is *perfect* if every subset $A \subseteq P$ is either authorized or forbidden. A perfect scheme with total normalized share size n is called *ideal*.

Due to [30], access (resp. adversary) structures are just monotone increasing (resp. decreasing) families of subsets. For an access structure Γ, we define the *minimal access structure of* Γ by $\min\Gamma = \{A \in \Gamma : B \not\subset A \text{ for all } B \in \Gamma\}$. Analogously, given an adversary structure $\mathcal{A}$, we define the *maximal adversary structure of* $\mathcal{A}$ by $\max\mathcal{A} = \{A \in \mathcal{A} : A \not\subset B \text{ for all } B \in \mathcal{A}\}$. Given two adversary structures $\mathcal{A}, \mathcal{B} \subseteq 2^P$, we say that the pair $(\mathcal{A}, \mathcal{B})$ is $\mathcal{R}_2$ if $A \cup B \neq P$ for every $A \in \mathcal{A}$ and $B \in \mathcal{B}$. Notice that a pair $(\mathcal{A}, \mathcal{B})$ is $\mathcal{R}_2$ if and only if $\mathcal{B} \subseteq \mathcal{A}^*$.

2.2 Linear Secret Sharing Schemes

Linear Secret Sharing schemes (LSSS) are a type of secret sharing schemes that is key to building our 1-out-of-q OT constructions. For convenience, we use the definition in [5,16], where secrets are elements of a finite field.

Definition 2.2. *Let Σ be a secret sharing scheme, where secrets take values in E_0, and shares in $E_1 \times \cdots \times E_n$. Let $\mathbb{F}$ be a finite field. Then Σ is* $\mathbb{F}$-linear *if the following conditions hold*

1. *the randomness $\mathbf{r}$ is chosen uniformly over a set Ω,*
2. *$E_0 = \mathbb{F}$ and $\Omega, E_1, \ldots, E_n$ are vector spaces of finite dimension over $\mathbb{F}$, and*
3. *Share_Σ is an $\mathbb{F}$-linear map*
$$\mathsf{Share}_\Sigma : E_0 \times \Omega \to E_1 \times \cdots \times E_n$$
so that the induced linear maps $E_0 \times \Omega \to E_i$ are surjective.

For each $i \in P$, the i-th share space is $E_i = \mathbb{F}^{\ell_i}$ for some positive integer ℓ_i. Linear schemes are perfect and have normalized total share size $\ell = \sum_{i=1}^{n} \ell_i$.

Every adversary structure admits an $\mathbb{F}_q$-LSSS for every q [30]. However, almost all access structures require $\mathbb{F}_q$-LSSS with normalized share size at least $2^{n/3-o(n)}$ for every q [4]. The characterization of adversary structures admitting efficient LSSSs is an open problem.

Given a secret value $s \in \mathbb{F}_q$, we have that $[s]_\Sigma \in \mathbb{F}_q^{\ell} = \mathbb{F}_q^{\ell_1} \times \cdots \times \mathbb{F}_q^{\ell_n}$. We define $V \subseteq \mathbb{F}_q^{\ell}$ as the set of all possible shares $[0]_\Sigma$ of $0 \in \mathbb{F}_q$, i.e., $V = \{\mathsf{Share}_\Sigma(0, \mathbf{r}) \,:\, \mathbf{r} \in \Omega\}$, is a vector subspace of $\mathbb{F}_q^{\ell}$. Similarly, we denote by W_k the set of all possible shares $[k]_\Sigma$ of a secret value $k \in \mathbb{F}_q$. Notice that given a sharing $[k]_\Sigma$ of k, the set W_k can be described as $\Sigma\ W_k = [k]_\Sigma + V$ and $W_0 = V$. Hence, each W_k is a coset of V [37] and so it is an affine subspace of $\mathbb{F}_q^{\ell}$. The following result can be found in [18, Lemma 11.71], for example.

Lemma 2.3. *Let Σ be an $\mathbb{F}_q$-LSSS with $\dim E_0 = 1$. A subset $A \subseteq P$ is forbidden for Σ if and only if there exists a vector $\mathbf{r} \in \Omega$ for which $\mathsf{Share}_\Sigma(1, \mathbf{r}) = (x_1, \ldots, x_n)$ satisfies $x_i = \mathbf{0}$ for every $i \in A$.*

2.3 OT combiners

In 1-out-of-q OT protocols, the sender Alice is assumed to hold q messages $m_0, \ldots, m_{q-1}$, and the receiver Bob chooses a message index $b \in \mathbb{F}_q$. At the end of a protocol implementing this functionality, Bob receives m_b and Alice receives nothing.

Here we lay out the fundamental theory of OT combiners. Before proceeding further, and as in [16], we need to introduce the *ideal* 1*-out-of-q OT functionality* $\mathcal{F}_{OT}$. We make use of the ideal functionality $\mathcal{F}_{OT}$ in our security definitions. It consists of an ideal version of a 1-out-of-q OT protocol that implements the functionality correctly and that does not allow any kind of corruption. Hence, $\mathcal{F}_{OT}$ is an abstraction of an ideal OT protocol. Without loss of generality, in this work all 1-out-of-q OT protocols that are considered secure are assumed to follow the blueprint of $\mathcal{F}_{OT}$. Figure 2 depicts the $\mathcal{F}_{OT}$ ideal functionality. Next, we formally define OT combiners, following the notation of [16].

Definition 2.4. *Let $S_1, \ldots, S_n$ be candidate OT implementations. An* OT combiner *is an efficient two-party protocol $\pi = \pi(S_1, \ldots, S_n)$, with access to the candidates $S_1, \ldots, S_n$, that implements the OT functionality. An OT combiner is* 1-out-of-q *if it implements the* 1*-out-of-q OT functionality.*

From this point onward, we assume OT combiners to be 1-out-of-q, n-server, and black-box. Under these assumptions, we can formalize the notion of OT combiner according to the next definition. In this definition, we additionally assume that OT combiners are single-use, and that they combine various 1-out-of-q OT candidates into a 1-out-of-q OT protocol. For more general cases, such as the multi-use case and the case where OT candidates are 1-out-of-2, see Remark 2.6 below.

Ideal 1-out-of-q OT Functionality $\mathcal{F}_{OT}$

Outline of the functionality:

1. The receiver Bob selects $b \in \mathbb{F}_q$, and sends its input $(\texttt{transfer}, b)$ to $\mathcal{F}_{OT}$.
2. The functionality $\mathcal{F}_{OT}$ sends $(\texttt{ready})$ to Alice.
3. The sender Alice sends q messages $(\texttt{send}, m_0, \dots, m_{q-1})$ to $\mathcal{F}_{OT}$.
4. If $(\texttt{transfer}, b)$ has been received from Bob, $\mathcal{F}_{OT}$ sends $(\texttt{sent}, m_b)$ to Bob.

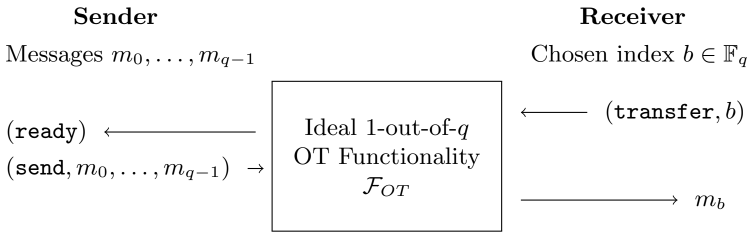
Sender
Messages $m_0, \dots, m_{q-1}$
Receiver
Chosen index $b \in \mathbb{F}_q$
$(\texttt{ready})$
$(\texttt{send}, m_0, \dots, m_{q-1})$
Ideal 1-out-of-q OT Functionality $\mathcal{F}_{OT}$
$(\texttt{transfer}, b)$
m_b

Fig. 2. The ideal 1-out-of-q Oblivious Transfer functionality.

Definition 2.5. *We define an n-server, black-box, single-use* 1*-out-of-*q OT *combiner $\pi = \pi(S_1, \dots, S_n)$ by means of the next three polynomial-time algorithms:*

$(b_1, \dots, b_n) \leftarrow \pi.\mathsf{Choose}(b)$**:** *Probabilistic algorithm run by the receiver Bob and taking as input a message index $b \in \mathbb{F}_q$. It returns an n-tuple $(b_1, \dots, b_n)$, where each $b_i \in \mathbb{F}_q$ is to be sent to server S_i.*

$(u_i^j)_{(i,j)\in\mathcal{P}_{n,q}} \leftarrow \pi.\mathsf{Send}(m_0, \dots, m_{q-1})$**:** *Probabilistic algorithm, run by the sender Alice, taking as input q chosen messages $m_0, \dots, m_{q-1}$. It returns a qn-tuple $(u_i^j)_{(i,j)\in\mathcal{P}_{n,q}}$, where each tuple $(u_i^0, \dots, u_i^{q-1})$ is to be sent to server S_i.*

$m \leftarrow \pi.\mathsf{Rec}(b, (v_1, \dots, v_n))$**:** *Algorithm, run by the receiver Bob, that takes as input the chosen message index $b \in \mathbb{F}_q$, along with the randomness used in* Choose*, and n elements $v_1, \dots, v_n$, where each v_i is received from server S_i. It returns a message m.*

Given an OT combiner $\pi = (\pi.\mathsf{Choose}, \pi.\mathsf{Send}, \pi.\mathsf{Rec})$ and given n servers $S_1, \dots, S_n$ implementing the 1-out-of-q OT functionality, we regard π as a protocol between a sender Alice and a receiver Bob. In this case, the resulting OT protocol $\pi(S_1, \dots, S_n)$ develops sequentially in five phases:

Choice phase: The receiver Bob chooses a message index $b \in \mathbb{F}_q$.
Bob generates the tuple $(b_1, \dots, b_n) \leftarrow \pi.\mathsf{Choose}(b)$.
Bob sends $(\texttt{transfer}, b_i)$ to server S_i for $i = 1, \dots, n$.

Ready phase: On receiving b_i from Bob, the server S_i sends $(\texttt{ready})$ to Alice.

Sending phase: The sender Alice chooses q messages $m_0, \dots, m_{q-1}$.
Alice generates the corresponding tuple

$$(u_i^j)_{(i,j)\in\mathcal{P}_{n,q}} \leftarrow \pi.\mathsf{Send}(m_0, \dots, m_{q-1}).$$

After receiving (`ready`) from every server, Alice sends the generated shares $(\texttt{send}, u_i^0, \ldots, u_i^{q-1})$ to S_i for $i = 1, \ldots, n$.

Transfer phase: The server S_i sends $(\texttt{sent}, u_i^{b_i})$ to Bob.

Output phase: Bob reconstructs the message m_b from the shares $u_1^{b_1}, \ldots, u_n^{b_n}$ he received by executing $\pi.\mathsf{Rec}(b, (u_1^{b_1}, \ldots, u_n^{b_n}))$.

Remark 2.6. In the multi-use setting, which is considered in Section 7, the i-th OT candidate is used a total of $n_i \geq 1$ times. We work with the same algorithms of Definition 2.5, but we take b_i, u_i^j and v_i as arrays of length n_i, and we assume that both parties sequentially feed the inputs to the i-th server across the n_i executions.

The case where the combiner takes 1-out-of-2 OT candidates as input is also considered in Section 8. Here, we also use the same algorithmic notation, but we instead impose $b_i \in \mathbb{F}_2$, and that the output of $\pi.\mathsf{Send}$ is $(u_i^j)_{(i,j)\in\mathcal{P}_{n,2}}$.

3 Correctness and Security Definitions

In this section, we state the definitions used to capture the correctness and security properties of our constructions. In the following discussions, $\mathcal{P}_n$ represents the set of servers.

3.1 Correctness Definition

The correctness property of OT combiners refers to the fact that, assuming all servers correctly implement the OT functionality and that both parties are honest, the protocol produced by the combiner implements the OT functionality correctly. Hence, we have to show that the message retrieved by Bob in the execution of the OT combiner is exactly the one that he should receive as per the OT functionality. This is expressed by the zero-error property formalized in the following definition, which is adapted from [16].

Definition 3.1. *An OT combiner π is* zero-error *if, for every message index $b \in \mathbb{F}_q$ and for any q messages $m_0, \ldots, m_{q-1}$, we have that*

$$m_b \leftarrow \pi.\mathsf{Rec}(b, (u_1^{b_1}, \ldots, u_n^{b_n})),$$

where $(b_1, \ldots, b_n) \leftarrow \pi.\mathsf{Choose}(b)$ and $(u_i^j)_{(i,j)\in\mathcal{P}_{n,q}} \leftarrow \pi.\mathsf{Send}(m_0, \ldots, m_{q-1})$.

3.2 Security Definitions

An OT combiner is *unconditionally secure* if its security rests solely on the security assumptions of the OT candidate implementations [16]. That is, if, provided the security of enough OT candidates holds, the resulting OT protocol is perfectly secure. Therefore, unconditional security guarantees that any attack on an OT combiner must forcibly break the security of sufficiently many of the OT candidate implementations in order to be successful. As in [16], an OT combiner is called *perfectly secure* if it is both unconditionally secure and correct.

In order to capture the notion of unconditional security, we formalize it into a simulator-based security definition [34]. We now give the definition of security that we employ in our work, namely *perfect security against active* $(\mathcal{A},\mathcal{B})$*-adversaries*, which is adapted from [16] and uses the Universal Composability framework [14].

Given two adversary structures $\mathcal{A},\mathcal{B} \subseteq 2^{\mathcal{P}_n}$, our security definition protects against two types of active adversaries: one that corrupts the sender Alice and a set of servers $A \in \mathcal{A}$, and one that corrupts the receiver Bob and a set of servers $B \in \mathcal{B}$. This respectively corresponds to the case that a set $A \in \mathcal{A}$ of the OT candidates are insecure for the receiver, and to the case that a set $B \in \mathcal{B}$ of the OT candidates are insecure for the sender. To deal with the Alice corruption case, we define the notion of *perfect security for the receiver against active* $\mathcal{A}$*-adversaries*, and in the Bob corruption case we define the notion of *perfect security for the sender against active* $\mathcal{B}$*-adversaries.*

In the Alice corruption case, we consider a malicious (i.e., active) adversary Adv that controls the sender Alice, that interacts with an honest receiver $\mathbb{B}$, and that is able to eavesdrop and fully operate each server in a set $A \in \mathcal{A}$. Our security aim here is to protect the confidentiality of the receiver's choice $b \in \mathbb{F}_q$. Hence, the ability to corrupt the servers in A must give Adv no information on b.

This definition uses the simulation paradigm [34], and compares the execution of the protocol in the real world and in the ideal world. In the real world, Adv and $\mathbb{B}$ interact through an OT combiner protocol π. In the ideal world, the whole view and output of Adv is controlled by the simulator Sim, and Sim and $\mathbb{B}$ interact exclusively through the ideal OT functionality $\mathcal{F}_{OT}$. Because of this, in the ideal experiment the adversary Adv does not receive any information on the choice $b \in \mathbb{F}_q$ of $\mathbb{B}$ from the interaction.

To provide security against malicious senders, Sim takes all the information viewed by Adv in the ideal world, which is the one herself produced, so as to transform it to a view that should be indistinguishable to the information seen by Adv in the real world. Hence, Sim also simulates the private inputs of $\mathbb{B}$ on the corrupted servers.

Definition 3.2. *Let π be an n-server, 1-out-of-q OT combiner protocol, and let $\mathcal{F}_{OT}$ denote the ideal 1-out-of-q OT functionality. Let Adv denote an adversary-controlled malicious sender, which is assumed to corrupt all the servers indexed by some set $A \in \mathcal{A}$. Let $\mathbb{B}$ denote an honest receiver, and let $\mathsf{Sim} = (\mathsf{Sim}_1, \mathsf{Sim}_{\mathsf{out}})$ be a stateful simulator. We define the probabilistic experiments $\mathsf{Real}^{\pi}_{\mathsf{Adv},\mathbb{B}}()$ and $\mathsf{Ideal}^{\mathcal{F}_{OT}}_{\mathsf{Adv},\mathbb{B},\mathsf{Sim}}()$ as follows:*

```
$\mathsf{Real}^{\pi}_{\mathsf{Adv},\mathbb{B}}()$ :
    $b \leftarrow \mathbb{B}()$
    $(b_1, \ldots, b_n) \leftarrow \pi.\mathsf{Choose}(b)$
    $((u_i^j)_{i \in \bar{A}, j \in \mathbb{F}_q}, (z_i)_{i \in A}) \leftarrow \mathsf{Adv}\,((b_i)_{i \in A})$
    $\mathit{output}\ ((b_i)_{i \in A}, (u_i^j)_{i \in \bar{A}, j \in \mathbb{F}_q}, (z_i)_{i \in A})$
```

```
$\mathsf{Ideal}^{\mathcal{F}_{OT}}_{\mathsf{Adv},\mathbb{B},\mathsf{Sim}}()$ :
    $b \leftarrow \mathbb{B}()$
    $(b_i)_{i \in A} \leftarrow \mathsf{Sim}_1()$
    $((u_i^j)_{i \in \bar{A}, j \in \mathbb{F}_q}, (z_i)_{i \in A}) \leftarrow \mathsf{Adv}((b_i)_{i \in A})$
    $\mathit{output}\ \mathsf{Sim}_{\mathsf{out}}((u_i^j)_{i \in \bar{A}, j \in \mathbb{F}_q}, (z_i)_{i \in A})$
```

We say that π *is* perfectly secure for the receiver against active $\mathcal{A}$-adversaries *if, for every set* $A \in \mathcal{A}$*, for all adversarial senders* Adv *corrupting the set of servers indexed by* A*, and for all honest receivers* $\mathbb{B}$*, there exists a simulator* Sim *such that the output values of* $\mathsf{Real}^{\pi}_{\mathsf{Adv},\mathbb{B}}()$ *and* $\mathsf{Ideal}^{\mathcal{F}_{OT}}_{\mathsf{Adv},\mathbb{B},\mathsf{Sim}}()$ *are identically distributed, where the probabilities are taken over the random coins of* π*,* Adv*,* $\mathbb{B}$ *and* Sim*.*

In the Bob corruption case, we consider a malicious (i.e., active) adversary Adv that controls the receiver Bob, that interacts with an honest sender $\mathbb{A}$, and that is able to eavesdrop on and fully operate each server in a set $B \in \mathcal{B}$. Our security aim here is to protect the confidentiality of the sender's messages $m_0, \ldots, m_{q-1}$. Hence, the ability to corrupt the servers in one set $B \in \mathcal{B}$ of servers must give Bob no information on $m_0, \ldots, m_{q-1}$ other than possibly one chosen message. As the previous definition, this definition uses the simulation paradigm [34] and compares the execution of the protocol in the real world and in the ideal world.

In the real world, $\mathbb{A}$ and Adv interact through an OT combiner protocol π. The sender $\mathbb{A}$, who is assumed to act honestly, holds messages $m_0, \ldots, m_{q-1}$ and uses the OT combiner π to generate the input $u_i^0, \ldots, u_i^{q-1}$ that is sent to server S_i for every $i \in \mathcal{P}_n$. The adversary Adv is assumed to completely corrupt every server in a set $B \in \mathcal{B}$, and so he sees all the inputs $(u_i^j)_{i \in B, j \in \mathbb{F}_q}$. He also acts as the receiver, generating an input b_i for the rest of servers $i \in \bar{B}$. Since the servers $i \in \bar{B}$ are assumed to behave as the ideal $\mathcal{F}_{OT}$ functionality, Adv receives $(u_i^{b_i})_{i \in \bar{B}}$ and learns no other information from that interaction.

In the ideal world, the whole view and output of Adv is controlled by the simulator Sim, and Sim and $\mathbb{A}$ interact through the ideal OT functionality $\mathcal{F}_{OT}$. By processing all the output that the adversary Adv generates, Sim produces a message index $\tilde{b}$ and handles it to the $\mathcal{F}_{OT}$ functionality. Then, after the sender $\mathbb{A}$ has sent the messages $m_0, \ldots, m_{q-1}$ to $\mathcal{F}_{OT}$, the adversary Adv receives the message $m_{\tilde{b}}$. To provide security against malicious receivers, Sim takes all the information viewed by Adv in the ideal world, so as to transform it to a view that should be indistinguishable to the one of the real world.

Definition 3.3. *Let* π *be an* n*-server,* 1*-out-of-*q *OT combiner, and let* $\mathcal{F}_{OT}$ *denote the* 1*-out-of-*q *OT functionality. Let* Adv *denote an adversary-controlled malicious receiver, which is assumed to corrupt all the servers indexed by some set* $B \in \mathcal{B}$*. Let* $\mathbb{A}$ *denote an honest sender, and let* $\mathsf{Sim} = (\mathsf{Sim}_1, \mathsf{Sim}_2, \mathsf{Sim}_{\mathsf{out}})$ *be a stateful simulator. We define the probabilistic experiments* $\mathsf{Real}^{\pi}_{\mathbb{A},\mathsf{Adv}}()$ *and* $\mathsf{Ideal}^{\mathcal{F}_{OT}}_{\mathbb{A},\mathsf{Adv},\mathsf{Sim}}()$ *as follows:*

```
$\mathsf{Real}^{\pi}_{\mathbb{A},\mathsf{Adv}}()$ :
    $(m_0, \ldots, m_{q-1}) \leftarrow \mathbb{A}()$
    $(u_i^j)_{(i,j) \in \mathcal{P}_{n,q}} \leftarrow \pi.\mathsf{Send}(\textit{send}, m_0, \ldots, m_{q-1})$
    $(b_i)_{i \in \bar{B}} \leftarrow \mathsf{Adv}((u_i^j)_{i \in B, j \in \mathbb{F}_q})$
    $\textit{output}\ ((u_i^j)_{i \in B, j \in \mathbb{F}_q}, (u_i^{b_i})_{i \in \bar{B}}, (b_i)_{i \in \bar{B}})$
```

```
$\mathsf{Ideal}^{\mathcal{F}_{OT}}_{\mathbb{A},\mathsf{Adv},\mathsf{Sim}}()$ :
    $(u_i^j)_{i \in B, j \in \mathbb{F}_q} \leftarrow \mathsf{Sim}_1()$
    $(b_i)_{i \in \bar{B}} \leftarrow \mathsf{Adv}((u_i^j)_{i \in B, j \in \mathbb{F}_q})$
    $\tilde{b} \leftarrow \mathsf{Sim}_2\left((b_i)_{i \in \bar{B}}\right)$
    $(\textit{ready}) \leftarrow \mathcal{F}_{OT}(\textit{transfer}, \tilde{b})$
    $(m_0, \ldots, m_{q-1}) \leftarrow \mathbb{A}()$
    $(\textit{sent}, m_{\tilde{b}}) \leftarrow \mathcal{F}_{OT}(\textit{send}, m_0, \ldots, m_{q-1})$
    $\textit{output}\ \mathsf{Sim}_{\mathsf{out}}(\tilde{b}, m_{\tilde{b}}, (b_i)_{i \in \bar{B}})$
```

We say that π is perfectly secure for the sender against active $\mathcal{B}$-adversaries *if, for every $B \in \mathcal{B}$, for all adversarial receivers* Adv *corrupting the set of servers indexed by B, and for all honest senders $\mathbb{A}$, there exists a simulator* Sim *such that the output values of* $\mathsf{Real}^{\pi}_{\mathbb{A},\mathsf{Adv}}()$ *and* $\mathsf{Ideal}^{\mathcal{F}_{OT}}_{\mathbb{A},\mathsf{Adv},\mathsf{Sim}}()$ *are identically distributed, where the probabilities are taken over the random coins of π, $\mathbb{A}$,* Adv *and* Sim*.*

The two previous definitions, on top of the correctness definition, make up the security definition considered in this work, namely perfect security against active $(\mathcal{A}, \mathcal{B})$-adversaries. We next formally state this.

Definition 3.4. *Let π be an n-server, 1-out-of-q OT combiner, and let $\mathcal{A}, \mathcal{B} \subseteq 2^{\mathcal{P}_n}$. We say that π is* perfectly secure against active $(\mathcal{A}, \mathcal{B})$-adversaries *if it is zero-error, and it is perfectly secure for the sender against active $\mathcal{B}$-adversaries and for the receiver against active $\mathcal{A}$-adversaries.*

4 Single-Use 1-out-of-q OT Combiners

In this section, we present our 1-out-of-q OT combiner in the particular setting where Σ is an ideal $\mathbb{F}_q$-LSSS. We achieve a single-use OT combiner with perfect security against active adversaries. In Section 7, we describe our construction for general LSSSs.

The proposed 1-out-of-q OT combiner is shown in Figure 3. It is described according to Definition 2.5 and follows the structure described in Section 1.3.

Theorem 4.1. *Let Σ be an ideal $\mathbb{F}_q$-LSSS with adversary structure $\mathcal{A}$. The OT combiner π_{OT} defined in Figure 3 is perfectly secure against active $(\mathcal{A}, \mathcal{A}^*)$-adversaries.*

The proof of Theorem 4.1 is split in three blocks: First, in Section 5, we analyze the secret sharing schemes S_k used in the construction, which are defined in Figure 4. In Section 6, we prove the correctness of the protocol and then its security. Theorem 4.1 implies Theorem 1.1 for the case that Σ is an ideal LSSS, and the non-ideal case is implied by Theorem 7.2. At the end of Section 6 we prove Corollary 1.2 by combining these results.

Single-use 1-out-of-q OT Combiner π_{OT}

$\pi_{OT}.\mathsf{Choose}(b)$: Given $b \in \mathbb{F}_q$, compute a sharing $[b]_\Sigma = (b_1, \ldots, b_n)$ of b using Σ.
Note that each $b_i \in \mathbb{F}_q$ because Σ is ideal.
Output $(b_1, \ldots, b_n)$.

$\pi_{OT}.\mathsf{Send}(m_0, \ldots, m_{q-1})$: For each message m_k, independently compute a sharing

$$[m_k]_{\mathcal{S}_k} = (m_k^{(i,j)})_{(i,j) \in \mathcal{P}_{n,q}}.$$

Then, for each $(i, j) \in \mathcal{P}_{n,q}$, compute the values

$$u_i^j := m_0^{(i,j)} || m_1^{(i,j)} || \cdots || m_{q-1}^{(i,j)}.$$

Output $(u_i^j)_{(i,j) \in \mathcal{P}_{n,q}}$, where each tuple $(u_i^0, \ldots, u_i^{q-1})$ is to be sent to server S_i.

$\pi_{OT}.\mathsf{Rec}(b, (v_1, \ldots, v_n))$: Parse each v_i, which is received from server S_i, as

$$v_i = n_0^{(i)} || n_1^{(i)} || \cdots || n_{q-1}^{(i)},$$

where $n_k^{(i)} \in \mathbb{F}_q$ for each $k \in \mathbb{F}_q$.
Retrieve m_b by evaluating

$$\mathsf{Reconstruct}_{\mathcal{S}_b}((n_b^{(i)})_{i \in \mathcal{P}_n}).$$

If the reconstruction fails at any step, output $\perp$. Otherwise, output m_b.

When the protocol follows correctly, $\pi_{OT}.\mathsf{Rec}$ is executed with $(v_1, \ldots, v_n) = (u_1^{b_1}, \ldots, u_n^{b_n})$ and retrieves $\mathsf{Reconstruct}_{\mathcal{S}_b}((m_b^{(1,b_1)}, \ldots, m_b^{(n,b_n)})$.

Fig. 3. Single-use 1-out-of-q OT combiner π_{OT} in the case Σ is an ideal $\mathbb{F}_q$-LSSS. The schemes $\mathcal{S}_k$ are defined in Figure 4.

Remark 4.2 (Structure). The protocol runs between a sender Alice and a receiver Bob, who communicate through a set of n servers $S_1, \ldots, S_n$ that implement the ideal 1-out-of-q OT functionality $\mathcal{F}_{OT}$ (described in Figure 2).

An ideal $\mathbb{F}_q$-LSSS Σ is used by the receiver Bob to request the message with the selected index $b \in \mathbb{F}_q$, in the following way. He generates a sharing $[b]_\Sigma = (b_1, \ldots, b_n)$ of b with Σ, and queries each server S_i with $b_i \in \mathbb{F}_q$. This corresponds to the $\pi_{OT}.\mathsf{Choose}$ function.

In order for Alice to distribute the messages $m_0, \ldots, m_{q-1} \in \mathbb{F}_q$, she makes use of q different secret sharing schemes $\mathcal{S}_0, \ldots, \mathcal{S}_{q-1}$, which are related to the affine subspaces $W_0, \ldots, W_{q-1}$, respectively. This step corresponds to function $\pi_{OT}.\mathsf{Send}$, and we note that each of the q messages sent to servers belong to $\mathbb{F}_q^q$, and so their length is expanded by factor of q with respect to the length of the original messages.

Then, the servers execute the OT functionality with the inputs they received, and send their outputs to Bob. Bob executes $\pi_{OT}.\mathsf{Rec}$ and retrieves the message.

Remark 4.3 (Communication complexity). In the Choice phase, Bob sends a total of $n \log q$ bits to servers. In the Sending phase, Alice sends a total of $q^2 n \log q$

The Secret Sharing Scheme $\mathcal{S}_k$

$\mathsf{Share}_{\mathcal{S}_k}$**:** To share a message $m \in \mathbb{F}_q$, first

- let $\mathbf{k} = (k_1, \ldots, k_n) \in \mathbb{F}_q^n$ be a sharing of k using Σ
- sample $r_1, \ldots, r_{n-1} \in \mathbb{F}_q$ uniformly at random, and let $r_n = m - \sum_{i=1}^{n-1} r_i$, so that $(r_1, \ldots, r_n)$ is an additive sharing of the message m
- sample $\mathbf{h} = (h_1, \ldots, h_n)$ uniformly at random from $V^\perp$

For every $i \in \mathcal{P}_n$ and for every $j \in \mathbb{F}_q$, define the (i, j)-th share as

$$m^{(i,j)} = r_i + (k_i - j)h_i.$$

$\mathsf{Reconstruct}_{\mathcal{S}_k}$**:** In this work we are just interested in reconstructing the message for subsets $A = \{(1, b_1), \ldots, (n, b_n)\}$ with $(b_1, \ldots, b_n) \in W_k$. In this case, the reconstruction function for $(m^{(i,j)})_{(i,j)\in A}$ is

$$\sum_{i=1}^{n} m^{(i,b_i)}.$$

Fig. 4. The $\mathbb{F}_q$-LSSS $\mathcal{S}_k$ related to the secret sharing scheme Σ, the affine subspace $W_k = [k]_\Sigma$, and $V = [0]_\Sigma$.

bits to the servers. In the Transfer phase, servers send a total of $qn \log q$ bits to Bob. Hence, the communication complexity is $(q^2 + q + 1)n \log q$.

Remark 4.4 (Adversary structure). Let $\mathcal{A}$ be an adversary structure. A protocol is secure against $(\mathcal{A}, \mathcal{A}^*)$-adversaries if and only if it is secure against $(\mathcal{A}, \mathcal{B})$-adversaries for any $\mathcal{B}$ such that the pair $(\mathcal{A}, \mathcal{B})$ is $\mathcal{R}_2$. This is equivalent to saying that it is secure against an adversary that corrupts either Alice and a set of servers in $\mathcal{A}$, or Bob and a set of servers B with $\bar{B} \notin \mathcal{A}$, as stated in the abstract. Such a 1-out-of-q OT combiner is also secure against any $(\mathcal{A}', \mathcal{B}')$-adversary satisfying $\mathcal{A}' \subseteq \mathcal{A}$ and $\mathcal{B}' \subseteq \mathcal{A}^*$.

Remark 4.5 (Variants). The first observation is that the protocol can be run for messages that are shorter than $\log q$. For instance, if the messages are just one bit, the protocol is not affected and the communication complexity is the same.

The second observation is that the protocol can be adapted to run 1-out-of-q' OT combiner for $q' < q$. In this case, Bob will choose m_b among $m_1, \ldots, m_{q'}$. We attain the same level of security, but the communication is reduced. Next, we detail the changes that should be done.

The $\pi_{OT}.\mathsf{Send}$ algorithm does not change. The algorithm $\pi_{OT}.\mathsf{Send}$ has only q' inputs, so the values u_i^j will be shorter, i.e., $u_i^j = m_0^{(i,j)}||m_1^{(i,j)}|| \cdots ||m_{q'-1}^{(i,j)}$. The servers will perform the 1-out-of-q OT functionality, and they will send to Bob a shorter v_i. The algorithm $\pi_{OT}.\mathsf{Rec}$ is executed analogously. The communication complexity now is $n \log q + qq'n \log q + q'n \log q = (qq' + q' + 1)n \log q$.

Consequently, given some integers q' and s, we can get 1-out-of-q' OT combiners of s-bit strings from our 1-out-of-q OT combiners, taking as q a prime power greater than k and 2^s.

The flexibility of the construction may be useful for certain adversary structures. It is known that there are adversary structures $\mathcal{A}$ for which there only exist efficient $\mathbb{F}$-LSSSs Σ for fields $\mathbb{F}$ of a certain characteristic [9].

Remark 4.6 (Efficiency of multisecret sharing schemes). In the Sending phase of our protocol, we share each of the q messages independently. For $q = 2$, this process was improved in [16] by creating sharings of the two messages at the same time, which reduces the number of shares from $4n$ to $2n$. The scheme in [16] can be seen as a *multisecret* sharing scheme [12,31]. In such schemes, n shares are generated from a sequence of $k > 1$ secrets, and each secret can be recovered from the shares, but each secret has its own access structure. Observe that we can define our 1-out-of-q constructions from multisecret sharing schemes. Since our multisecret sharing scheme is just a combination of independent secret sharing schemes, we decided to simplify the notation.

A natural question is what is the smallest size in bits of u_i^j, which leads to bounds on the communication complexity of the protocol. It can be proved that the randomized $\mathbb{F}_q$-linear mapping $\pi_{OT}.\mathsf{Send}$ in [16] cannot be generalized for $q > 2$ with u_i^j in $\mathbb{F}_q$, i.e., there are schemes Σ that require that the total amount of bits sent by Alice is greater than $qn \log q$ bits. The proof uses arguments that depend on the specific properties of the scheme Σ, and is displayed in Appendix A. A research line in the direction of this work is to build more efficient 1-out-of-q OT-combiners with multisecret sharing schemes and to know what is the optimal communication complexity.

5 Secret Sharing Schemes for OT Combiners

In this section, we introduce a family of secret sharing schemes that are useful to build 1-out-of-q OT combiners. In Section 5.2, we show that the schemes $\mathcal{S}_k$ in Figure 4 are indeed W_k-OT-compatible. This fact simplifies the security proof of our 1-out-of-q OT combiners.

5.1 *W*-OT-Compatible Secret Sharing Schemes

Recall the discussion in Section 1.3 about the properties involved in our construction. This section is dedicated to the study of the schemes $\mathcal{S}_k$ that guarantee the correctness and security of our protocol. Consider the following definition.

Definition 5.1. *Let $\mathbb{F}_q$ be a finite field, and let $W \subseteq \mathbb{F}_q^n$. We define Γ_W as the access structure on $\mathcal{P}_{n,q}$ determined by the minimal access structure*

$$\min \Gamma_W = \{\{(1, b_1), (2, b_2), \ldots, (n, b_n)\} : (b_1, b_2, \ldots, b_n) \in W\}.$$

The study of the share size of access structures Γ_W for general W is of independent interest. If $n = 2$, then Γ_W is a bipartite graph access structure, and this case is studied in several works as [6,21]. As a consequence of [35,2,3], improvements on the efficiency of schemes for Γ_W will result in improvements in the efficiency of CDS protocols, and in the efficiency of secret sharing schemes for general access structures.

Following the discussion in Section 1.3, here we are interested in the construction of secret sharing schemes with access structure Γ_W where W is the collection of sharings of b by Σ. Since we only consider linear schemes, the collection of sharings $[b]_\Sigma$ always defines an $\mathbb{F}_q$ affine space. Hence, from now on, we restrict to the study of the access structures Γ_W when W is an affine space.

If $W \subseteq \mathbb{F}_2^n$ is a binary affine subspace, then the access structure Γ_W described above always admits an ideal $\mathbb{F}_2$-LSSS [16]. However, in general, given an affine subspace $W \subseteq \mathbb{F}_q^n$, ideal $\mathbb{F}_q$-LSSS for the access structure Γ_W are not expected to exist.

Instead of looking for $\mathbb{F}_q$-LSSS with access structures of the form Γ_W, which will give rise to non-efficient OT combiners, we explore the possibility of relaxing the restrictions on the access structure of $\mathcal{S}_k$ while keeping our security needs. With the aim of building schemes $\mathcal{S}_k$ for the protocol in Figure 3, we define the notion of *W-OT-compatibility.*

Recall that we defined $P_i := \{(i,0),(i,1)\ldots,(i,q-1)\}$ for $i = 1,\ldots,n$, and $\mathcal{P}_{n,q} = P_1 \cup \ldots \cup P_n$ is the set of participants of the schemes $\mathcal{S}_k$.

Definition 5.2. *Let $W \subseteq \mathbb{F}_q^n$. Let $\Delta \subseteq 2^{\mathcal{P}_{n,q}}$ be the family of subsets defined by*

$$\Delta = \{A_1 \cup \ldots \cup A_n \,:\, A_i \subseteq P_i \text{ and } |A_i| = 1 \text{ or } q \text{ for } i = 1,\ldots,n\}.$$

We say that an access structure $\Gamma \subseteq 2^{\mathcal{P}_{n,q}}$ is W-OT-compatible *if $\Gamma \cap \Delta = \Gamma_W \cap \Delta$. Similarly, we say that a secret sharing scheme is* W-OT-compatible *if its access structure is W-OT-compatible.*

The motivation behind this definition is the following: The secret sharing schemes $\mathcal{S}_0,\ldots,\mathcal{S}_{q-1}$ used by Alice, which we can assume honest at this point, and are built so that an adversary controlling Bob, and possibly some servers, can learn from each server S_i either

- one share, e.g. in the case that the server S_i is not corrupted, or
- all q shares sent to S_i, in the case that an adversary corrupts Bob and S_i.

Under this assumption, since P_i corresponds to the shares sent to server S_i, the shares that an adversary controlling Bob is able to see in any execution of the OT combiner are always determined by some subset in Δ. Therefore, even if the obtained $\mathbb{F}_q$-LSSS has an access structure Γ other than Γ_W, it serves our security purposes as long as Γ coincides with Γ_W when restricting it to Δ. That is, as long as Γ is W-OT-compatible.

See the Appendix B for an example of W-OT-compatible access structures.

5.2 Analysis of $\mathcal{S}_k$

This subsection is dedicated to the analysis of the scheme $\mathcal{S}_k$ presented in Figure 4. See the Appendix B for an example for $q = n = 3$. The scheme $\mathcal{S}_k$ is an ideal $\mathbb{F}_q$-LSSS defined on the set of nq participants $\mathcal{P}_{n,q}$. It is used by Alice to generate a sharing of the k-th message m_k, which is distributed among the OT servers. Proposition 5.4 states that $\mathcal{S}_k$ is W_k-OT-compatible for $W_k = [k]_\Sigma$. First, we present a technical lemma needed for its proof.

Lemma 5.3. *Let $\mathbb{F}_q$ be a finite field, and $V \subsetneq \mathbb{F}_q^n$ be a vector subspace. Let $t \leq n$ and $y_1, \dots, y_t \in \mathbb{F}_q$. If $(y_1, \dots, y_t, x_{t+1}, \dots, x_n) \notin V$ for every $x_{t+1}, \dots, x_n \in \mathbb{F}_q$, then there exists $\mathbf{h} \in V^\perp$ such that $y_1h_1 + \cdots + y_th_t = 1$ and $h_{t+1} = \cdots = h_n = 0$.*

Proof. We prove this lemma by backward induction in t. The lemma holds for $t = n$ since, given $y = (y_1, \dots, y_n) \notin V$, there always exists an $\mathbf{h} \in V^\perp$ such that $\langle y, \mathbf{h} \rangle = 1$.

Assume that $t < n$. Suppose that there exist $y_1, \dots, y_t \in \mathbb{F}_q$ satisfying $(y_1, \dots, y_t, x_{t+1}, \dots, x_n) \notin V$ for all $x_{t+1}, \dots, x_n \in \mathbb{F}_q$. By induction hypothesis we have that, for every $x \in \mathbb{F}_q$, there exists an $\mathbf{h}^x = (h_1^x, \dots, h_n^x) \in V^\perp$ with

$$\sum_{i=1}^{t} y_i h_i^x + x h_{t+1}^x = 1 \quad \text{and} \quad h_{t+2}^x = \cdots = h_n^x = 0.$$

If $h_{t+1}^x = 0$ for some $x \in \mathbb{F}_q$, then $\mathbf{h}^x$ satisfies the lemma. Otherwise, by the pigeonhole principle, let x and z be two distinct elements of $\mathbb{F}_q$ such that $h_{t+1}^x = h_{t+1}^z \neq 0$. Define

$$\mathbf{h} = \frac{\mathbf{h}^x - \mathbf{h}^z}{h_{t+1}^x (z - x)}.$$

Since $\mathbf{h} = (h_1, \dots, h_n)$ is in $V^\perp$ and satisfies $h_{t+1} = \cdots = h_n = 0$ and

$$\begin{aligned} y_1h_1 + \cdots + y_th_t &= \frac{1}{h_{t+1}^x (z - x)} \left(\sum_{i=1}^{t} y_i h_i^x - \sum_{i=1}^{t} y_i h_i^z \right) \\ &= \frac{1}{h_{t+1}^x (z - x)} \big((1 - x h_{t+1}^x) - (1 - z h_{t+1}^z) \big) = 1, \end{aligned}$$

we have that $\mathbf{h}$ satisfies the lemma. □

Proposition 5.4. *Let Σ be an ideal $\mathbb{F}_q$-LSSS. For every $k \in \mathbb{F}_q$, the secret sharing scheme $\mathcal{S}_k$ defined in Figure 4 is an ideal $\mathbb{F}_q$-LSSS that is W_k-OT-compatible.*

Proof. In order to prove that $\mathcal{S}_k$ is W_k-OT-compatible, we prove that Γ, the access structure of $\mathcal{S}_k$, satisfies $\Gamma_{W_k} \cap \Delta = \Gamma \cap \Delta$.

Let $A = \{(1, b_1), \dots, (n, b_n)\}$ be a subset in $\min \Gamma_{W_k}$, and let $(m^{(i,j)})_{(i,j) \in A}$ be shares by $\mathcal{S}_k$. Since $\sum_{i=1}^{n} r_i = m$, then

$$\sum_{i=1}^{n} m^{(i,b_i)} = \sum_{i=1}^{n} (r_i + (k_i - b_i) h_i) = \sum_{i=1}^{n} r_i + \langle \mathbf{k} - \mathbf{b}, \mathbf{h} \rangle = m,$$

where we used that $\mathbf{h} \in V^\perp$ and $\mathbf{k} - \mathbf{b} \in V$ because $\mathbf{k}, \mathbf{b} \in W_k$. Hence, $\Gamma_{W_k} \subseteq \Gamma$ and so $\Gamma_{W_k} \cap \Delta \subseteq \Gamma \cap \Delta$.

Now, we prove $\Gamma_{W_k} \cap \Delta \supseteq \Gamma \cap \Delta$ by showing that, for every $A \in \Delta$, if $A \notin \Gamma_{W_k}$ then $A \notin \Gamma$. Let $A \in \Delta \setminus \Gamma_{W_k}$. Otherwise assume, without loss of generality, that for some $t \leq n$ we can express

$$A = \{(1, v_1), \dots, (t, v_t)\} \cup P_{t+1} \cup \cdots \cup P_n.$$

We now use Lemma 2.3. More concretely, we show that there exists randomness $r_1, \dots, r_{n-1} \in \mathbb{F}_q$ and $\mathbf{h} = (h_1, \dots, h_n) \in V^\perp$ so that the sharing of the message $m = 1$ satisfies $m^{(i,j)} = 0$ for every $(i, j) \in A$.

Since $A \notin \Gamma_{W_k}$, we have that $(v_1 - k_1, \dots, v_t - k_t, x_{t+1}, \dots, x_n) \notin V$ for every $x_{t+1}, \dots, x_n \in \mathbb{F}_q$. By Lemma 5.3, there exists an $\mathbf{h} = (h_1, \dots, h_n) \in V^\perp$ such that $\sum_{i=1}^{t} (v_i - k_i) h_i = 1$ and $h_{t+1} = \cdots = h_n = 0$. We choose as randomness this $\mathbf{h} \in V^\perp$ and

$$\begin{aligned} r_i &= -(k_i - v_i) h_i && \text{for } i = 1, \dots, t, \\ r_i &= 0 && \text{for } i = t+1, \dots, n-1. \end{aligned}$$

Since we want a sharing of the message $m = 1$, we take $r_n = 1 - \sum_{i=1}^{n-1} r_i = 0$. Then, for $(i, j) \in A$, the shares $m_{(i,j)} = r_i + (k_i - j) h_i$ of the message $m = 1$ are

$$\begin{aligned} m^{(i,v_i)} &= -(k_i - v_i) h_i + (k_i - v_i) h_i = 0 && \text{for } i = 1, \dots, t, \\ m^{(i,j)} &= 0 + (k_i - j) \cdot 0 = 0 && \text{for } i = t+1, \dots, n. \end{aligned}$$

□

As a consequence of this result, for every affine space $W \subseteq \mathbb{F}_q^n$ there exists an ideal $\mathbb{F}_q$-LSSS that is W-OT-compatible. For the particular case $q = 2$, the proofs of Lemma 5.3 and Proposition 5.4 can be simplified [15]. Indeed, for $q = 2$, the access structure of the scheme in Figure 4 is simply Γ_{W_k} [15].

Secret sharing schemes of this kind are connected to Conditional Disclosure of Secrets (CDS) protocols, as can be seen in [35,36,3], for example. Namely, the shares of this scheme are also the messages of an n-server CDS protocol for the Boolean function $f : \{0, \dots, q-1\}^n \to \{0, 1\}$ defined as follows: $f(x_1, \dots, x_n) = 1$ if and only if $(x_1, \dots, x_n) \in W$.

6 Correctness and security proofs

We start with the proof of correctness.

Proposition 6.1. *The OT combiner π_{OT} defined in Figure 3 is zero-error. That is, provided both Alice and Bob are semi-honest, π_{OT} implements the 1-out-of-q OT functionality correctly.*

Proof. If Alice and Bob follow the protocol honestly, at the end of the protocol Bob receives the shares $m_b^{(1,b_1)}, \dots, m_b^{(n,b_n)}$ of the message m_b, where $[b]_\Sigma = (b_1, \dots, b_n) \in W_b$ is some sharing of his input b. Since $\{(1, b_1), \dots, (n, b_n)\} \in \min \Gamma_{W_b}$ is authorized for $\mathcal{S}_b$, Bob can reconstruct the message m_b. □

The security properties of our constructions are stated in Theorem 4.1. To proceed with its proof, we first need to establish Lemma 6.2.

Suppose that an adversary controlling Bob corrupts a set $B \in \mathcal{B}$ of servers. As a consequence of the next lemma, if the shares $(b_i)_{i\in\bar{B}}$ sent to non-corrupted servers in $\bar{B}$ do not correspond to any sharing $[b]_\Sigma$ of b, the adversary can not get any information on the message m_b.

Lemma 6.2. *Let $m_0, \dots, m_{q-1} \in \mathbb{F}_q$ be arbitrary messages, and fix independent sharings $[m_k]_{\mathcal{S}_k} = (m_k^{(i,j)})_{(i,j)\in\mathcal{P}_{n,q}}$ for every $k \in \mathbb{F}_q$. Let $B \subseteq \mathcal{P}_n$ and $(b'_1, \dots, b'_n) \in \mathbb{F}_q^n$, and define the set $\mathcal{H} \subseteq \mathcal{P}_{n,q}$ by*

$$\mathcal{H} = \{(i, b'_i) \,:\, i \in \bar{B}\} \cup \{(i,j) \,:\, i \in B,\ j \in \mathbb{F}_q\}.$$

Fix $b \in \mathbb{F}_q$. Then, if the shares $(b'_i)_{i\in\bar{B}}$ are not part of any sharing $[b]_\Sigma$, the shares $\{m_k^{(i,j)} \,:\, (i,j) \in \mathcal{H},\ k \in \mathbb{F}_q\}$ give no information about m_b.

Proof. Since the sharing of every message is done independently, only the shares $(m_b^{(i,j)})_{(i,j)\in\mathcal{H}}$ could potentially give information on m_b. We prove that $\mathcal{H}$ is forbidden for $\mathcal{S}_b$. Since $\mathcal{S}_b$ is W_b-OT-compatible and since $\mathcal{H} \in \Delta$, if $\mathcal{H}$ were authorized for $\mathcal{S}_b$ then $\mathcal{H} \in \Gamma_{W_b}$, and thus it would contain a set $\{(1, b_1), \dots, (n, b_n)\}$ for some $(b_1, \dots, b_n) \in W_b$. However, then necessarily $b_i = b'_i$ for all $i \in \bar{B}$, and this would mean that $(b'_i)_{i\in\bar{B}}$ belongs to a sharing $[b]_\Sigma$, a contradiction. □

Now we can complete the proof of Theorem 4.1.

Proof (Proof of Theorem 4.1). Correctness is proved in Proposition 6.1.The rest of the proof is split in two parts, corresponding to Definitions 3.2 and 3.3. In each case, we define the simulators and compare the outputs of the ideal and real experiments. Let $A \in \mathcal{A}$ and $B \in \mathcal{A}^*$.

Perfect security for the receiver against active $\mathcal{A}$-adversaries:

$\mathsf{Sim}_1()$: Generate a sharing of $0 \in \mathbb{F}_q$,

$$[0]_\Sigma = (b_1^0, \dots, b_n^0).$$

Output $(b_i^0)_{i\in A}$.

$\mathsf{Sim}_{\mathsf{out}}((u_i^j)_{i\in\bar{A}, j\in\mathbb{F}_q}, (z_i)_{i\in A})$: Retrieve, from the state of Sim, the sharing $[0]_\Sigma = (b_i^0)_{i\in\mathcal{P}_n}$ that was generated in the previous execution of Sim_1.

Output $\Big((b_i^0)_{i\in A}, (u_i^j)_{i\in\bar{A}, j\in\mathbb{F}_q}, (z_i)_{i\in A}\Big)$.

Note that the shares $(b_i)_{i\in A}$ that the adversary Adv takes as input correspond to the set $A \in \mathcal{A}$, which is forbidden for Σ. Hence, they are distributed identically to the A-shares of a sharing of any other $b' \neq b$ (in particular, of $0 \in \mathbb{F}_q$), and so they do not carry any information on b. The messages $\Big((u_i^j)_{i\in\bar{A}, j\in\mathbb{F}_q}, (z_i)_{i\in A}\Big)$ generated by Adv are thus identically distributed in both worlds.

Since the shares $(b_i)_{i\in A}$ do not allow to distinguish between the real and the ideal world, we have proved indistinguishability.

Perfect security for the sender against active $\mathcal{B}$-adversaries:

$\mathsf{Sim}_1()$: For every $k \in \mathbb{F}_q$, choose $m'_k \in \mathbb{F}_q$ uniformly at random and generate the sharing $[m'_k]_{\mathcal{S}_k} = ({m'}_k^{(i,j)})_{(i,j)\in\mathcal{P}_{n,q}}$. Then, create the values $u_i^j = {m'}_0^{(i,j)}||\cdots||{m'}_{q-1}^{(i,j)}$ for every $(i,j) \in B \times \mathbb{F}_q$. Output $(u_i^j)_{i\in B, j\in\mathbb{F}_q}$.

$\mathsf{Sim}_2((b_i)_{i\in\bar{B}})$: Try to reconstruct the input b of the adversary Adv by executing $\mathsf{Reconstruct}_\Sigma$ on the input. If the reconstruction succeeds, output the reconstructed message index $\tilde{b}$. Otherwise, output $\perp$.

$\mathsf{Sim}_{\mathsf{out}}(\tilde{b}, m_{\tilde{b}}, (b_i)_{i\in\bar{B}})$: Retrieve, from the state of Sim and for every $k \in \mathbb{F}_q$, the messages m'_k, the sharings $[m'_k]_{\mathcal{S}_k} = ({m'}_k^{(i,j)})_{(i,j)\in\mathcal{P}_{n,q}}$ and the messages $(u_i^j)_{i\in B, j\in\mathbb{F}_q}$ that were generated in the previous execution of Sim_1.
Proceed as follows, depending on whether the reconstruction in Sim_2 failed or not:

- If $\tilde{b} \neq \perp$, let $\tilde{m}_{\tilde{b}} = m_{\tilde{b}}$. Generate a sharing $[\tilde{m}_{\tilde{b}}]_{\mathcal{S}_{\tilde{b}}} = (\tilde{m}_{\tilde{b}}^{(i,j)})_{(i,j)\in\mathcal{P}_{n,q}}$ subject to the restriction that $\tilde{m}_{\tilde{b}}^{(i,j)} = {m'}_{\tilde{b}}^{(i,j)}$ for every $(i,j) \in B \times \mathbb{F}_q$. Note that this is possible, since $B \times \mathbb{F}_q$ is forbidden for $\mathcal{S}_0, \ldots, \mathcal{S}_{q-1}$. For every $k \in \mathbb{F}_q \setminus \{\tilde{b}\}$ and every $(i,j) \in \bar{B} \times \mathbb{F}_q$, set $\tilde{m}_k^{(i,j)} := {m'}_k^{(i,j)}$.
- If $\tilde{b} = \perp$, for every $k \in \mathbb{F}_q$ and $(i,j) \in \bar{B} \times \mathbb{F}_q$, let

$$\tilde{m}_k^{(i,j)} = {m'}_k^{(i,j)}.$$

Create the values $u_i^{b_i} = \tilde{m}_0^{(i,b_i)}||\cdots||\tilde{m}_{q-1}^{(i,b_i)}$ for every $i \in \bar{B}$.
Output $\Big((u_i^j)_{i\in B, j\in\mathbb{F}_q}, (u_i^{b_i})_{i\in\bar{B}}, (b_i)_{i\in\bar{B}}\Big)$.

In order to prove indistinguishability we first note that, since $B \in \mathcal{A}^*$, the set $\bar{B}$ is not in $\mathcal{A}$ and so it is authorized for Σ. By the definition of $\mathcal{S}_k$, we see that at least one share per server is needed to reconstruct a message. Hence, the set $B \times \mathbb{F}_q$ is forbidden for $\mathcal{S}_0, \ldots, \mathcal{S}_{q-1}$, and so the shares $(u_i^j)_{i\in B, j\in\mathbb{F}_q}$ do not hold any information on the messages $m_0, \ldots, m_{q-1}$. Therefore, the shares $(b_i)_{i\in\bar{B}}$ generated by the adversary Adv in the real world and in the ideal world are identically distributed.

Since $\bar{B}$ is authorized for Σ, we have two possibilities as for the shares $(b_i)_{i\in\bar{B}}$ received by Sim: either they are part of a sharing $[b]_\Sigma$, or they are not part of any sharing for Σ (due to the malicious behavior of Adv).

In the first case, Sim_2 successfully reconstructs b. The set $\{(i, b_i) : i \in \bar{B}\} \cup (B \times \mathbb{F}_q)$ is then authorized for $\mathcal{S}_b$ and, by Lemma 6.2, it is forbidden for all the other $\mathbb{F}_q$-LSSS $\mathcal{S}_k$. Since the sharings for m_b generated by $\mathsf{Sim}_{\mathsf{out}}$ are distributed identically to those of the real world, this proves indistinguishability.

In the second case, Lemma 6.2 shows that the shares corresponding to the participants $\{(i, b_i) : i \in \bar{B}\} \cup (B \times \mathbb{F}_q)$ give no information about any message in the real world. Therefore, since here $\mathsf{Sim}_{\mathsf{out}}$ generates these shares from random messages in the ideal world, they obey the same distribution as in the real world, as required. □

Finally, we can prove Corollary 1.2.

Proof (Corollary 1.2). For $q > n$, we choose Σ to be the Shamir secret sharing scheme [46] over $\mathbb{F}_q$ with adversary structure $\mathcal{A} = \{A \subseteq \mathcal{P}_n \ : \ |A| < n/2\}$. If n is odd, then $\mathcal{A} = \mathcal{A}^*$; else $\mathcal{A}^* = \{A \subseteq \mathcal{P}_n \ : \ |A| \leq n/2\}$. For $q = n$, we choose the canonical one-participant-extension of the the Shamir secret sharing scheme with adversary structure $\mathcal{A}$. In both cases, Σ is ideal and $\mathbb{F}_q$-linear. Then the result follows from and Theorem 4.1 and Remark 4.3. □

7 Our Multi-Use, One-out-of-q OT Combiner

In this section, we show a generalization of our protocol π_{OT} from Section 4 that extends to the general case where the adversary structure $\mathcal{A}$ does not admit an ideal $\mathbb{F}_q$-LSSS. Theorems 4.1 and 7.2 imply Theorem 1.1.

First, we present a black-box transformation from n'-server single-use OT combiners to n-server OT combiners, with $n < n'$. This transformation illustrates the situation in which servers execute more than one OT instances of the protocol.

Lemma 7.1. *Let $n' > n$ be positive integers. Let π' be an n'-server, black-box,* 1-*out-of-q OT combiner that is perfectly secure against active $(\mathcal{A}', \mathcal{B}')$-adversaries. Let $(I_1, \dots, I_n)$ be a partition of $\mathcal{P}_{n'}$ and let*

$$\mathcal{A} = \{A \subseteq \mathcal{P}_n \ : \ \cup_{i \in A} I_i \in \mathcal{A}'\}$$
$$\mathcal{B} = \{B \subseteq \mathcal{P}_n \ : \ \cup_{i \in B} I_i \in \mathcal{B}'\}$$

Then the protocol π in 5 is an n-server, black-box, 1-*out-of-q OT combiner that is perfectly secure against active $(\mathcal{A}, \mathcal{B})$-adversaries. The amount of bits exchanged in the protocols π and π' are the same.*

Proof. The correctness of the protocol π follows from the correctness of π'. We next prove security against $(\mathcal{A}, \mathcal{B})$-adversaries. Note that each server S_i indexed by $i \in \mathcal{P}_n$ corresponds to the participants $I_i \subseteq \mathcal{P}_\ell$. Hence, any adversary that corrupts Alice and a set $A \in \mathcal{A}$ in π will have as many capabilities as an adversary corrupting Alice and $\cup_{i \in A} I_i$ in π', since the interaction with a particular OT implementation can be thought of as the concatenation of the interactions of the different calls to it. We have an analogous situation for an adversary corrupting Bob and the servers $B' = \cup_{i \in B} I_i$. Hence, π is secure against the active corruption of this adversary. □

Let Σ be an $\mathbb{F}_q$-LSSS for n participants with adversary structure $\mathcal{A}$. Since Σ is now not necessarily ideal, if $[b]_\Sigma = (b_1, \dots, b_n)$ is a sharing of b using Σ, we note that each share b_i belongs to some vector space $E_i = \mathbb{F}_q^{\ell_i}$ for some integer $\ell_i \geq 1$. Hence, unlike in the ideal case, b_i may not correspond to a single message index but a sequence of them.

Denote by $\ell = \sum_{i=1}^{n} \ell_i$ the normalized share size of Σ. Rather than looking at the sharings $(b_1, \dots, b_n)$ as elements of $\mathbb{F}_q^{\ell_1} \times \cdots \times \mathbb{F}_q^{\ell_n}$, we concatenate their

Construction of an n-server 1-out-of-q OT combiner π from an n'-server 1-out-of-q OT combiner π' with $n' > n$

$\pi.\mathsf{Choose}(b)$**:** Given $b \in \mathbb{F}_q$, compute $\pi'.\mathsf{Choose}(b) = (b_1, \ldots, b_{n'})$.
    Output $(b_1, \ldots, b_n)$, where $b_i = (b'_j)_{j \in I_i}$.
$\pi.\mathsf{Send}(m_0, \ldots, m_{q-1})$**:** Compute $\pi'.\mathsf{Send}(m_0, \ldots, m_{q-1}) = ({u'}_i^j)_{(i,j) \in \mathcal{P}_{n',q}}$.
    Output $(u_i^j)_{(i,j) \in \mathcal{P}_{n,q}}$, where $(u_i^j)_{(i,j)}$ is the concatenation of $({u'}_k^j)_{(k,j)}$ for $k \in I_i$.
$\pi.\mathsf{Rec}(b, (v_1, \ldots, v_n))$**:** Parse each v_i as $v_i = (v'_k)_{k \in I_i}$, obtaining $(v'_1, \ldots, v'_{n'})$
    Output $\pi.\mathsf{Rec}(b, (v'_1, \ldots, v'_{n'}))$.

Fig. 5. Black-box 1-out-of-q OT combiner transformation

components and we see them as elements of the vector space $\mathbb{F}_q^\ell$. Denote the corresponding vector space isomorphism by

$$\varphi : \mathbb{F}_q^{\ell_1} \times \cdots \times \mathbb{F}_q^{\ell_n} \to \mathbb{F}_q^\ell.$$

According to this, given Σ with the Share_Σ function, we can define the ideal scheme Σ' on $\mathcal{P}_\ell$ with share spaces $E'_i = \mathbb{F}_q$ for every i, satisfying that $[b]_{\Sigma'} = \varphi([b]_\Sigma) = (b'_1, \ldots, b'_\ell)$ for every $b \in \mathbb{F}_q$, where each $b'_i \in \mathbb{F}_q$.

We now generalize the 1-out-of-q OT combiner presented previously to the case where Σ is not ideal. The obtained OT combiner is still black-box and n-server, but it is no longer single-use, because we assume that each of the n OT candidate servers S_i are called a total of ℓ_i times. To this end, for $i \in \mathcal{P}_n$, denote by $I_i = \left\{\sum_{j=1}^{i-1} \ell_j + 1, \ldots, \sum_{j=1}^{i} \ell_j\right\}$ the set of indices of $\mathcal{P}_\ell$ whose shares are associated to i. We describe our multi-use OT combiner in Figure 6.

Theorem 7.2. *Let Σ be an $\mathbb{F}_q$-LSSS on the set $\mathcal{P}_n$ with adversary structure $\mathcal{A} \subseteq 2^{\mathcal{P}_n}$. The OT combiner π_{OT} defined in Figure 6 is perfectly secure against active $(\mathcal{A}, \mathcal{A}^*)$-adversaries.*

Proof. Let Σ' be the ideal $\mathbb{F}_q$-linear secret sharing scheme on $\mathcal{P}_\ell$ determined by Σ, as described above, and let $(I_1, \ldots, I_n)$ be the associated partition of $\mathcal{P}_\ell$. Let $\mathcal{A}'$ be the adversary structure of Σ'. Then, the 1-out-of-q OT combiner π_{OT} in Figure 3 for Σ' is perfectly secure against active $(\mathcal{A}', \mathcal{A}'^*)$-adversaries. By applying the transformation in Figure 5 and Lemma 7.1, we obtain a protocol that is perfectly secure against $(\mathcal{A}'', \mathcal{A}''^*)$ adversaries, where

$$\mathcal{A}'' = \{A \subseteq \mathcal{P}_n \, : \, \cup_{i \in A} I_i \in \mathcal{A}'\}$$

Notice that $\mathcal{A}''$ is equal to $\mathcal{A}$. □

Remark 7.3. The protocol in Figure 6 coincides with the protocol in Figure 3 when Σ is ideal. If the normalized total share size of Σ is $\ell > n$, then Bob sends a total of $\ell \log q$ bits to servers in the Choice phase. In the Sending phase, Alice sends a total of $q^2 \ell \log q$ bits to the servers. In the Transfer phase, servers

Our Generalized 1-out-of-q OT Combiner Protocol π_{OT}

- Let Σ' be the ideal $\mathbb{F}_q$-linear secret sharing scheme on $\mathcal{P}_\ell$ determined by Σ, as described above, and let $(I_1, \ldots, I_n)$ be the associated partition of $\mathcal{P}_\ell$.
- Let π' be the single-use ℓ-server 1-out-of-q OT combiner protocol defined in Figure 3 for the secret sharing scheme Σ'.
- The protocol π_{OT} is defined as the output of the transformation in Figure 5 applied to the protocol π' with the partition $(I_1, \ldots, I_n)$.

Fig. 6. Our multi-use 1-out-of-q OT combiner π_{OT} for a general $\mathbb{F}_q$-linear secret sharing scheme Σ on $\mathcal{P}_n$.

send a total of $q\ell \log q$ bits to Bob. Hence, the communication complexity is $(q^2 + q + 1)\ell \log q$. As in the ideal case, this protocol can be adapted as an 1-out-of-q' OT combiner for $q' < q$, in which case the communication complexity is $(qq' + q' + 1)\ell \log q$.

Proposition 7.4 ([16]). *If $(\mathcal{A}, \mathcal{B})$ is not an $\mathcal{R}_2$ pair of adversary structures, then perfectly secure* 1*-out-of-*2 *OT combiners against active $(\mathcal{A}, \mathcal{B})$-adversaries cannot exist.*

Corollary 7.5. *Let $(\mathcal{A}, \mathcal{B})$ be a pair adversary structures. There exist perfectly secure* 1*-out-of-q OT combiners against active $(\mathcal{A}, \mathcal{B})$-adversaries if and only if $(\mathcal{A}, \mathcal{B})$ is $\mathcal{R}_2$.*

Proof. Suppose that $(\mathcal{A}, \mathcal{B})$ is $\mathcal{R}_2$. By [30], $\mathcal{A}$ admits an $\mathbb{F}_q$-LSSS Σ. By Theorem 7.2, Σ provides a secure OT combiner for $(\mathcal{A}, \mathcal{B})$. Now suppose, for the sake of contradiction, that $(\mathcal{A}, \mathcal{B})$ is not $\mathcal{R}_2$. If there exists a secure 1-out-of-q combiner for $(\mathcal{A}, \mathcal{B})$, then there exists a secure 1-out-of-2 combiner for $(\mathcal{A}, \mathcal{B})$, which contradicts Proposition 7.4. □

8 One-out-of-q OT-combiners from 1-out-of-2 OT-combiners

We dedicate this section to construct 1-out-of-q OT combiners from 1-out-of-2 OT combiners. For this purpose, we adapt a technique to construct a 1-out-of-q OT instance from 1-out-of-2 OT instances that presented by Crépeau, Brassard and Robert [19]. As far as we know, this approach has not been studied in any previous works. As we will see, for certain adversary structures, it is possible to get better communication complexity than using the protocols described above. Moreover, the construction does not restrict the number of messages q to a prime power, and it allows for arbitrary $q \geq 2$. However, the construction is inherently multi-use, as it requires multiple calls to 1-out-of-2 OT instances. The suitability of this construction with respect the ones presented above will depend on the efficiency of $\mathbb{F}_2$-linear secret sharing schemes for the adversary structure with respect $\mathbb{F}_q$-linear secret sharing schemes, the efficiency of the OT instances involved, and the length of the messages.

1-out-of-q OT Combiner π_{OT} from a 1-out-of-2 OT Combiner π'

$\pi_{OT}.\mathsf{Choose}(b)$**:** Given $b \in \{0, 1, \dots, q-1\}$, let $(b_0, \dots, b_{q-2})$ so that

$$b_k = \begin{cases} 1, \text{ if } k < b \\ 0, \text{ otherwise.} \end{cases}$$

For $k = 0, \dots, q-2$, let

$$(b_1^{(k)}, \dots, b_n^{(k)}) = \pi'.\mathsf{Choose}(b_k)).$$

Output $\left((b_i^{(0)}, \dots, b_i^{(q-2)})\right)_{i \in \mathcal{P}_n}$.

$\pi_{OT}.\mathsf{Send}(m_0, \dots, m_{q-1})$**:** Sample $q-2$ bits $r_1, \dots, r_{q-2}$ uniformly at random. Then, compute the values $(w_0, \dots, w_{q-2})$ as

$$w_k = \begin{cases} \pi'.\mathsf{Send}(m_0, r_1) & \text{if } k = 0, \\ \pi'.\mathsf{Send}(m_k \oplus r_k, r_{k+1} \oplus r_k) & \text{if } 1 \leq k < q-2, \\ \pi'.\mathsf{Send}(m_{q-2} \oplus r_{q-2}, m_{q-1} \oplus r_{q-2}) & \text{if } k = q-2. \end{cases}$$

Parse $w_k = (w_i^{j,(k)})_{(i,j) \in \mathcal{P}_{n,2}}$.
For every $i = 1, \dots, n$, let $u_i = (w_i^{j,(k)})_{(k,j) \in \mathcal{P}_{q-1,2}}$.
Output $(u_1, \dots, u_n)$.

$\pi_{OT}.\mathsf{Rec}(b, (v_1, \dots, v_n))$**:** For every $i = 1, \dots, n$, parse $v_i = (v_i^0, \dots, v_i^{q-2})$.
For every $k < b$, let $y_k = \pi'.\mathsf{Rec}(1, (v_1^k, \dots, v_n^k))$.
If $b < q-1$, let $y_b = \pi'.\mathsf{Rec}(0, (v_1^b, \dots, v_n^b))$.
If the reconstruction fails at any step, output $\perp$.
Otherwise, if $b < q-1$, output $\bigoplus_{k=0}^{b} y_k$. Else, if $b = q-1$, output $\bigoplus_{k=0}^{q-2} y_k$.

Fig. 7. 1-out-of-q OT combiner π_{OT} from an 1-out-of-2 OT combiner π'.

We describe the 1-out-of-q OT combiner π_{OT} for bit messages in Figure 7. For messages of larger bitsize $s > 1$, the naive solution would be to run s times a 1-out-of-q protocol using Figure 7. This is secure as long as Bob acts honestly and chooses the same index b across the s OT executions. Otherwise, Bob could act maliciously, and choose different indexes in different executions, thus learning bits from more than one message when he should not. To prevent this, Crépeau et al. [19] propose zigzag functions. These functions extend the length of binary messages from s to $3^{\lceil \log s \rceil}$, so that independent bit-OT executions do not reveal information on more than one message.

Extending the construction of Figure 7 for s-bit messages using zigzag functions [19] requires $3^{\lceil \log s \rceil}$ executions of this bit-OT protocol. In the figure, we call π_{OT} the 1-out-of-2 n-server bit-OT combiner. For this construction, we can instantiate π_{OT} with the general 1-out-of-q OT combiner presented in Figure 6 for the case $q = 2$, which is equivalent to the one presented in [15] for non-ideal schemes. We can also use the combiner in [16] to reduce the size of messages taken as input by OT candidates.

One advantage of this construction is that it only uses 1-out-of-2 OT protocols. As mentioned above, it results in a highly multi-use solution, as in general it requires a multi-use combiner for each of the 1-out-of-2 OT combiners, and the multiple calls to it required by the 1-out-of-q combiner technique of [19].

Next, we evaluate the communication cost of this protocol for messages of one bit and general adversary structures. We instantiate it with the 1-out-of-2 OT combiner from Figure 6. Suppose that the pair $(\mathcal{A}, \mathcal{B})$ requires an $\mathbb{F}_2$-LSSS Σ with normalized share size ℓ. In the Choice phase, the output of each $\pi_{OT}.\mathsf{Choose}$ has ℓ bits, and the total is $(q-1)\ell$ bits. In the Sending phase, the output of each $\pi_{OT}.\mathsf{Send}$ is 4ℓ bits, so it outputs $4(q-1)\ell$ bits in total. In the Transfer phase, servers send 2ℓ bits, in total. Therefore, the communication cost is $(5q-3)\ell$ bits. If the 1-out-of-2 combiner in [16] is used instead of [15], this communication complexity can be reduced to $(3q-2)\ell$.

In order to compare it with the other construction of this work, we consider the threshold t adversary structure $\mathcal{A}$, for $1 < t < n$, and the pair $(\mathcal{A}, \mathcal{A}^*)$. This adversary pair requires a scheme with normalized share size $\ell = n \log n$. The resulting protocol exchanges $(3q-2)n \log n$ bits, and it uses each of the n 1-out-of-2 bit-OT candidates $(q-1)\log n$ times. For messages in $\mathbb{F}_q$, the use of zigzag functions implies increasing the communication cost and the OT calls by a factor of the order of $\log q$.

In this 1-out-of-q OT combiner, information is only exchanged through a 1-out-of-2 combiner, and its security properties rest exclusively on this 1-out-of-2 combiner. The corresponding result is summarized in Theorem 1.3 for the case of threshold adversary structures.

Acknowledgments

This article is supported by grant 2021 SGR 00115 from the Government of Catalonia, by the project HERMES, funded by the European Union NextGenerationEU/PRTR and INCIBE, and by the project ACITHEC PID2021-124928NB-I00, funded by MCIN/AEI/10.13039/501100011033/FEDER, EU.

References

1. Aiello, B., Ishai, Y., Reingold, O.: Priced oblivious transfer: How to sell digital goods. In: Pfitzmann, B. (ed.) EUROCRYPT 2001. LNCS, vol. 2045, pp. 119–135. Springer (2001)
2. Applebaum, B., Beimel, A., Nir, O., Peter, N.: Better secret sharing via robust conditional disclosure of secrets. In: STOC 2020. pp. 280–293 (2020)
3. Applebaum, B., Beimel, A., Farràs, O., Nir, O., Peter, N.: Secret-sharing schemes for general and uniform access structures. In: Ishai, Y., Rijmen, V. (eds.) EUROCRYPT 2019. LNCS, vol. 11478, pp. 441–471. Springer (2019)

4. Beimel, A., Farràs, O.: The share size of secret-sharing schemes for almost all access structures and graphs. In: TCC 2020. LNCS, vol. 12552, pp. 499–529. Springer (2020)
5. Beimel, A.: Secret-sharing schemes: A survey. In: International Conference on Coding and Cryptology - IWCC'11. p. 11–46. Springer-Verlag (2011)
6. Beimel, A., Farràs, O., Mintz, Y.: Secret-sharing schemes for very dense graphs. Journal of Cryptology **29**(2), 336–362 (2016)
7. Beimel, A., Ishai, Y.: On the power of nonlinear secret-sharing. SIAM Journal on Discrete Mathematics **19**(1), 258–280 (2005)
8. Beimel, A., Othman, H., Peter, N.: Degree-2 secret sharing and conditional disclosure of secrets. IACR Cryptol. ePrint Arch. **2021**, 285 (2021), `https://eprint.iacr.org/2021/285`
9. Beimel, A., Weinreb, E.: Separating the power of monotone span programs over different fields. SIAM J. Comput. **34**(5), 1196–1215 (2005)
10. Bellare, M., Micali, S.: Non-interactive oblivious transfer and applications. In: Brassard, G. (ed.) CRYPTO' 89. LNCS, vol. 435, pp. 547–557. Springer (1990)
11. Ben-Or, M., Goldwasser, S., Wigderson, A.: Completeness theorems for non-cryptographic fault-tolerant distributed computation. In: STOC '88. pp. 1–10. ACM (1988)
12. Blundo, C., De Santis, A., Di-Crescenzo, G., Giorgio Gaggia, A., Vaccaro, U.: Multi-secret sharing schemes. In: CRYPTO'94. LNCS, vol. 839, pp. 150–163 (1994)
13. Cachin, C., Crépeau, C., Marcil, J.: Oblivious transfer with a memory-bounded receiver. In: FOCS 1998. pp. 493–502 (1998)
14. Canetti, R.: Universally composable security: A new paradigm for cryptographic protocols. Cryptology ePrint Archive, Report 2000/067 (2000), `https://eprint.iacr.org/2000/067`
15. Cascudo, I., Damgård, I., Farràs, O., Ranellucci, S.: Server-aided two-party computation with minimal connectivity in the simultaneous corruption model. Cryptology ePrint Archive, Report 2014/809 (2014), `https://eprint.iacr.org/2014/809`
16. Cascudo, I., Damgård, I., Farràs, O., Ranellucci, S.: Resource-efficient OT combiners with active security. In: TCC 2017. LNCS, vol. 10678, pp. 461–486. Springer (2017)
17. Chor, B., Kushilevitz, E.: A zero-one law for boolean privacy. In: STOC '89. pp. 62–72. ACM (1989)
18. Cramer, R., Damgård, I.B., Nielsen, J.B.: Secure Multiparty Computation and Secret Sharing. Cambridge University Press (2015)
19. Crépeau, C., Brassard, G., Robert, J.M.: Information theoretic reductions among disclosure problems. In: FOCS 1986. pp. 168–173 (1986)
20. Crépeau, C., Kilian, J.: Achieving oblivious transfer using weakened security assumptions (extended abstract). In: FOCS'88. pp. 42–52 (1988)
21. Csirmaz, L., Ligeti, P., Tardos, G.: Erdös-pyber theorem for hypergraphs and secret sharing. Graphs and Combinatorics (2014)
22. Dowsley, R., van de Graaf, J., Müller-Quade, J., Nascimento, A.C.A.: Oblivious transfer based on the McEliece assumptions. In: Safavi-Naini, R. (ed.) Information Theoretic Security. pp. 107–117. Springer (2008)
23. Even, S., Goldreich, O., Lempel, A.: A randomized protocol for signing contracts. Communications of the ACM **28**(6), 637–647 (1985)
24. Gertner, Y., Ishai, Y., Kushilevitz, E., Malkin, T.: Protecting data privacy in private information retrieval schemes. J. Comput. Syst. Sci. **60**(3), 592–629 (2000)

25. Goyal, V., Ishai, Y., Sahai, A., Venkatesan, R., Wadia, A.: Founding cryptography on tamper-proof hardware tokens. IACR Cryptology ePrint Archive **2010**, 153 (2010)
26. Harnik, D., Ishai, Y., Kushilevitz, E., Buus Nielsen, J.: OT-combiners via secure computation. In: Canetti, R. (ed.) TCC 2008. pp. 393–411. LNCS, Springer (2008)
27. Harnik, D., Kilian, J., Naor, M., Reingold, O., Rosen, A.: On robust combiners for oblivious transfer and other primitives. In: Cramer, R. (ed.) EUROCRYPT 2005. pp. 96–113. LNCS, Springer (2005)
28. Ishai, Y., Maji, H.K., Sahai, A., Wullschleger, J.: Single-use OT combiners with near-optimal resilience. In: ISIT. pp. 1544–1548. IEEE (2014)
29. Ishai, Y., Prabhakaran, M., Sahai, A.: Founding cryptography on oblivious transfer - efficiently. In: CRYPTO 2008. pp. 572–591. LNCS, Springer-Verlag (2008)
30. Ito, M., Saito, A., Nishizeki, T.: Secret sharing scheme realizing general access structure. Electronics and Communications in Japan, Part III **72**(9), 56–64 (1989)
31. Jackson, W., Martin, K.M., O'Keefe, C.M.: Multisecret threshold schemes. In: CRYPTO'93. LNCS, vol. 773, pp. 126–135 (1994)
32. Kilian, J.: Founding cryptography on oblivious transfer. In: STOC '88. pp. 20–31. ACM (1988)
33. Kilian, J., Micali, S., Ostrovsky, R.: Minimum resource zero-knowledge proofs. In: Brassard, G. (ed.) CRYPTO'89. pp. 545–546. Springer (1990)
34. Lindell, Y.: How to simulate it - a tutorial on the simulation proof technique. In: Tutorials on the Foundations of Cryptography (2016)
35. Liu, T., Vaikuntanathan, V.: Breaking the circuit-size barrier in secret sharing. In: Diakonikolas, I., Kempe, D., Henzinger, M. (eds.) STOC 2018. pp. 699–708. ACM (2018)
36. Liu, T., Vaikuntanathan, V., Wee, H.: Towards breaking the exponential barrier for general secret sharing. In: Nielsen, J.B., Rijmen, V. (eds.) EUROCRYPT 2018. LNCS, vol. 10820, pp. 567–596. Springer (2018)
37. Massey, J.L.: Some applications of coding theory in cryptography. Codes and Ciphers: Cryptography and Coding IV pp. 33–47 (1995)
38. Meier, R., Przydatek, B.: On robust combiners for private information retrieval and other primitives. In: Dwork, C. (ed.) CRYPTO 2006. LNCS, vol. 4117, pp. 555–569. Springer (2006)
39. Meier, R., Przydatek, B., Wullschleger, J.: Robuster combiners for oblivious transfer. In: Vadhan, S.P. (ed.) TCC 2007. pp. 404–418. LNCS, Springer (2007)
40. Naor, M., Pinkas, B.: Computationally secure oblivious transfer. Journal of Cryptology **18**(1), 1–35 (2005)
41. Oxley, J.G.: Matroid Theory (1992)
42. Padró, C.: Lecture notes in secret sharing. IACR Cryptology ePrint Archive p. 674 (2012), `http://eprint.iacr.org/2012/674`
43. Peikert, C., Vaikuntanathan, V., Waters, B.: A framework for efficient and composable oblivious transfer. In: Wagner, D. (ed.) CRYPTO 2008. pp. 554–571. Springer (2008)
44. Przydatek, B., Wullschleger, J.: Error-tolerant combiners for oblivious primitives. In: Automata, Languages and Programming. pp. 461–472. Springer (2008)
45. Rabin, M.O.: How to exchange secrets with oblivious transfer. IACR Cryptology ePrint Archive (2005), `http://eprint.iacr.org/2005/187`
46. Shamir, A.: How to share a secret. Communications of the ACM **22**(11), 612–613 (1979)

47. Vaikuntanathan, V., Nalini Vasudevan, P.: Secret sharing and statistical zero knowledge. In: ASIACRYPT 2015. pp. 656–680. LNCS, Springer-Verlag, Inc. (2015)
48. Yao, A.C.C.: Protocols for secure computations. In: FOCS '82. pp. 160–164. IEEE Computer Society (1982)

A Lower bounds on the share size for linear multisecret secret sharing schemes

In our definition of $\pi_{OT}.\mathsf{Send}$, we treat each message separately. However, we could consider a multisecret scheme (as discussed in Remark 4.6) and not process messages separately, as done in [16]. With this generalization in mind, a natural question is what is the smallest size of the output of u_i^j, which leads to bounds on the communication complexity of the scheme. Next we show that the result in [16] cannot be generalized keeping u_i^j in $\mathbb{F}_q$.

Claim. Let $q > 2$ be a prime number. Consider the protocol in Figure 3. There is no compiler that, given an ideal $\mathbb{F}_q$-linear secret sharing scheme Σ with adversary structure $\mathcal{A}$, creates a randomized $\mathbb{F}_q$-linear mapping $\pi_{OT}.\mathsf{Send}(m_0, \dots, m_{q-1})$ so that $u_i^j \in \mathbb{F}_q$ and the resulting protocol is an OT combiner π_{OT} that is perfectly secure against active $(\mathcal{A}, \mathcal{A}^*)$-adversaries.

Proof. We prove that this compiler does not exist for $n = 3$ and $q = 3$. Take Σ the threshold secret sharing scheme over $\mathbb{F}_q$ defined as follows:

$(b_1, b_2, b_3) \leftarrow \mathsf{Share}_\Sigma(b)$**:** Let $a \overset{\$}{\leftarrow} \mathbb{F}_3$, and let $f(x) = a + bx \in \mathbb{F}_3[x]$. Return $(f(0), f(1), f(2))$.

$s \leftarrow \mathsf{Reconstruct}_\Sigma((i, x_i)_{i \in A})$**:** From shares $(i, f(i)), (j, f(j))$ return $b = \frac{f(i)-f(j)}{i-j}$.

This scheme is a variant of the Shamir secret sharing scheme. We have $\mathcal{A} = \mathcal{A}^* = \{\{1\}, \{2\}, \{3\}, \emptyset\}$, $W_0 = [0]_\Sigma = \langle(1, 1, 1)\rangle$, $W_1 = (0, 1, 2) + W_0$ and $W_2 = (0, 2, 1) + W_0$.

When choosing a message index $b \in \mathbb{F}_3$ and executing $\pi.\mathsf{Choose}(b)$, Bob creates $(b_1, b_2, b_3) \leftarrow \mathsf{Share}_\Sigma(b)$ and sends $b_i \in \mathbb{F}_3$ to server i.

When sharing messages $m_0, m_1, m_2 \in \mathbb{F}_3$ across servers, Alice uses the randomized linear function $\pi_{OT}.\mathsf{Send}$. We can assume that it is computed by means of mapping $\Pi : \mathbb{F}_3^3 \times \mathbb{F}_3^\ell \to \mathbb{F}_3^9$ for some $\ell \geq 0$ with

$$\Pi(m_0, m_1, m_2, \mathbf{r}) = (u_1^0, u_1^1, u_1^2, u_2^0, u_2^1, u_2^2, u_3^0, u_3^1, u_3^2)$$

for some randomly chosen $\mathbf{r} \in \mathbb{F}_3^\ell$. Hence, Π is determined by some vectors $\mathbf{v}_i^j \in \mathbb{F}_3^{3+\ell}$ satisfying that $u_i^j = (m_0, m_1, m_2, \mathsf{r}) \cdot \mathbf{v}_i^j$. For every $A \subseteq \mathcal{P}_{n,q}$, define $V_A = \langle \mathbf{v}_i^j \rangle_{(i,j) \in A}$. Also, let $\{\mathbf{e}_i\}_{0 \leq i \leq \ell+2}$ be the canonical basis of the vector space $V = \mathbb{F}_3^3 \times \mathbb{F}_3^\ell$. By the theory of linear secret sharing schemes, a subset $A \subseteq \mathcal{P}_{n,q}$ can recover m_i if and only if $\mathbf{e}_i \in V_A$ (see [42] , for example). Now, analyzing the properties of these vectors $\mathbf{v}_i^j$, we will reach a contradiction.

In order to simplify the discussion, we take $V' = V/V_{P_1}$ and from now on $\mathbf{e}_i$ and $\mathbf{v}_i^j$ refer to their classes in V'. Moreover, borrowing notation from matroid theory, we say a set of indices is a *circuit* if the corresponding vectors determine a minimally dependent set (for an introduction to matroid theory, see [41], for example). A set $A = A' \cup A''$ with $A' \subseteq \mathcal{P}_{n,q}$ and $A'' \subseteq \{0,1,2\}$ is a *circuit* if $\{\mathbf{v}_i^j : (i,j) \in A'\} \cup \{\mathbf{e}_i : i \in A''\}$ is a minimal dependent set in V'. By properties of linear dependence,

(C) if C_1 and C_2 are two different circuits and $p \in C_1 \cap C_2$, then there is a circuit C_3 such that $C_3 \subseteq (C_1 \cup C_2) \setminus \{p\}$

First, we prove that subsets of $\mathcal{P}_{n,q} \cup \{0,1,2\}$ of size one or two are not circuits. If $\{(i,j)\}$ is a circuit, then u_i^j can be computed from the shares of P_1. If $\{i\}$ is a circuit, then m_i can be computed with the shares of P_1. Both situations are not possible. Let $A = \{0,1\}$. If A is a circuit, then an adversary controlling Bob and Server 1 querying $(0,0,0)$ can reconstruct m_0 and also m_1, which is not possible. The proof is analogous for the set $\{1,(2,0)\}$. If $\{(2,0),(2,1)\}$ is a circuit, then an adversary controlling Bob and Server 1 querying $(0,0,0)$ can also compute u_2^1 and reconstruct m_0 and m_2, which is not possible. Finally, if $\{(2,0),(3,1)\}$ is a circuit, an adversary controlling Bob and Server 1 querying $(0,0,0)$ can also reconstruct m_0 and also m_1, can also compute u_3^1 and so reconstruct m_0 and m_1, which is not possible. The rest of cases of sets of size one or two can be proved analogously. Therefore, dependent sets are of size greater than two. Now we claim that the following sets are circuits:

- $A_1 = \{0,(2,0),(3,0)\}$
- $A_2 = \{0,(2,1),(3,1)\}$
- $A_3 = \{1,(2,0),(3,1)\}$
- $A_4 = \{2,(2,0),(3,0)\}$

Now we prove that A_1 is a circuit. It is a dependent set because m_1 can be recovered from $\{u_i^j : (i,j) \in P_1 \cup \{(2,0),(3,1)\}\}$ and so $\mathbf{e}_1 \in \langle \mathbf{v}_2^0, \mathbf{v}_3^1 \rangle$ in V'. It is minimal because dependent subsets are of size greater than two. Analogously, we can prove that A_2, A_3 and A_4 are circuits. Now we claim that $A_5 = \{1,0,(2,0),(2,1)\}$ and $A_6 = \{0,2,(2,0),(2,1)\}$ are also circuits.

Since A_2 and A_3 are circuits and $(3,1) \in A_2 \cap A_3$, then there exists a circuit contained in A_5 by property **(C)**. Now we see that A_5 is a circuit. It is enough to prove that proper subsets of A_5 of size 3 are not circuits. If $\{1,0,(2,0)\}$ is a circuit, then an adversary controlling Bob and Server 1 querying $(0,0,0)$ can also reconstruct m_0 and also m_1, which is not possible. Analogously, we can prove that $\{1,0,(2,1)\}$ is not a circuit. If $A = \{1,(2,0),(2,1)\}$ is a circuit, then an adversary controlling Bob and Server 1 querying $(0,1,2)$ can reconstruct m_1 and obtain u_2^1 because A is a circuit. Therefore, it is also possible to obtain m_2, a contradiction. Analogously, we can prove that $\{0,(2,0),(2,1)\}$ is not a circuit. Therefore, A_5 is a circuit. We can prove that A_6 is a circuit analogously.

Since A_5 and A_6 are circuits and $(2,1) \in A_5 \cap A_6$, then there exists a circuit contained in $A_7 = \{0,1,2,(2,0)\}$ by property **(C)**, but now we will see that we reach a contradiction. An adversary controlling Bob and Server 1 querying $(0,0,0)$ can reconstruct m_0 and, if A_7 is a circuit, can get partial information about m_1 and m_2, which is not possible. Hence, A_7 is not a circuit. Using the same argument, we can see that $\{0,1,2\}$ is not a circuit as well. We can prove that the other proper subsets of A_7 are not circuits following arguments used above to prove that proper subsets of A_5 are not circuits.

Notice that in this proof we only assumed that $u_i^j \in \mathbb{F}_3$ for $(i,j) \in \{(2,0),(2,1),(3,0),(3,1)\}$. For any other set of four indices with two from P_2 and two from P_3, we get the same contradiction. Hence, we have that $u_i^j \in \mathbb{F}_3^2$ for at least two indices (i,j). This proof can be adapted to other access structures.

B An Example of $\boldsymbol{\Sigma}$ and $\boldsymbol{\mathcal{S}_0}$ for $\boldsymbol{q = n = 3}$

Consider the case $q = n = 3$ and let $\mathcal{A}$ and $\mathcal{B}$ be adversary structures of threshold $t = 1$. Let Σ be a Shamir secret sharing over $\mathbb{F}_3$ with n participants and adversary structure of threshold 1. The secret is $b \in \mathbb{F}_3$. Bob chooses r at random, and the shares are $b + r$, $b + 2r$ and r, corresponding to the points 1, 2, and the point at infinity. The sharings of $b = 0$ are the following ones:

$$W_0 = V = \{(0,0,0),(1,2,1),(2,1,2)\}$$

Hence, we have that

$$\min \mathit{\Gamma}_{W_0} = \{\{(1,0),(2,0),(3,0)\},\{(1,1),(2,2),(3,1)\}\{(1,2),(2,1),(3,2)\}\}$$

Now we analyze the scheme $\mathcal{S}_0$, used by Alice and described in 4, which is run by Bob to share m_0. The share of the server (i,j) for $i \in \mathcal{P}_3$ and $j \in \mathbb{F}_3$ is $r_i + jh_i$, where r_i are additive shares of the secret m_0, and (h_1,h_2,h_3) is an element of $V^\perp$ chosen at random. Note that $V^\perp = \langle(1,1,0),(0,1,1)\rangle$.

Let $\mathit{\Gamma}$ be the access structure of $\mathcal{S}_0$. Observe that subsets of $\min \mathit{\Gamma}_{W_0}$ are in $\mathit{\Gamma}$, because the sum of the shares corresponding to these subsets equals the secret. Hence, $\mathit{\Gamma}_{W_0} \subseteq \mathit{\Gamma}$. Indeed, $\mathit{\Gamma}$ is strictly greater than $\mathit{\Gamma}_{W_0}$: For example, the subset

$$\{(1,0),(2,0),(3,1),(3,2)\}$$

is in $\mathit{\Gamma}$ because the sum of the shares corresponding to $(1,0)$ and $(2,0)$, plus the double of the shares corresponding to $(3,1)$ and $(3,2)$, equals the secret, and this subset it is not in $\mathit{\Gamma}_{W_0}$. We will see now that $\mathit{\Gamma}$ is W_0-OT compatible.

It can be seen to check that the minimal sets of $\mathit{\Gamma}$ are

$$\{(1,c_1),(2,c_2),(3,c_3)\},\ \{(i_1,c_{i_1}),(i_2,c_{i_2})\} \cup P_{i_3} \setminus \{(i_3,c_{i_3})\},\ \text{and}$$
$$\{(i_1,c_{i_1})\} \cup P_{i_2} \cup P_{i_3} \setminus \{(i_2,c_{i_2}),(i_3,c_{i_3})\}$$

for every $(c_1,c_2,c_3) \in W_0$ and every permutation (i_1,i_2,i_3) of $(1,2,3)$. It can be checked that $\mathit{\Gamma} \cap \mathit{\Delta}$ are the subsets

$$\{(1,c_1),(2,c_2),(3,c_3)\},\ \{(1,c_1),(2,c_2),(3,c_3)\} \cup P_i \text{ for } i \in \{1,2,3\},$$
$$\{(1,c_1),(2,c_2),(3,c_3)\} \cup P_i \cup P_j \text{ for } i,j \in \{1,2,3\},\ \text{and } P_1 \cup P_2 \cup P_3$$

for every $(c_1,c_2,c_3) \in W_0$. Since $\mathit{\Gamma} \cap \mathit{\Delta} = \mathit{\Gamma}_{W_0} \cap \mathit{\Delta}$, $\mathit{\Gamma}$ is W_0-OT compatible.