A Monotone Circuit Construction for Individually-Secure Multi-Secret Sharing

Cailyn Bass*, Alejandro Cohen†, Rafael G.L. D'Oliveira*, and Muriel Médard‡
* School of Mathematical and Statistical Sciences, Clemson University, Clemson, SC, USA, {cailynb,rdolive}@clemson.edu
† Faculty of Electrical and Computer Engineering, Technion–Institute of Technology, Haifa, Israel, alecohen@technion.ac.il
‡ Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge, MA, USA, medard@mit.edu

2024 IEEE International Symposium on Information Theory (ISIT) | 979-8-3503-8284-6/24/$31.00 ©2024 IEEE | DOI: 10.1109/ISIT57864.2024.10619205

***Abstract*—In this work, we introduce a new technique for taking a single-secret sharing scheme with a general access structure and transforming it into an individually secure multi-secret sharing scheme where every secret has the same general access structure. To increase the information rate, we consider *Individual Security* which guarantees zero mutual information with *each secret individually*, for any unauthorized subsets. Our approach involves identifying which shares of the single-secret sharing scheme can be replaced by linear combinations of messages. When $m-1$ shares are replaced, our scheme obtains an information rate of $m/|S|$, where S is the set of shares. This provides an improvement over the information rate of $1/|S|$ in the original single-secret sharing scheme.**

I. Introduction

A secret sharing scheme is a method for sharing a secret amongst a set of participants in such a way that only certain authorized subsets of the participants are able to retrieve the secret. Any unauthorized subset that combines their shares should gain no new information about the secret. The first secret sharing schemes were introduced in 1979 by Blakely [1] and Shamir [2]. These initial schemes are now called (k, n)-threshold schemes since any set of participants of size greater than or equal to k is authorized to compute the secret. In 1988 Ito et. al. [3] introduced a multiple assignment scheme to produce secret sharing schemes for any general access structure. Monotone Boolean functions were then utilized by Benaloh et. al. [4] in 1992 to improve the efficiency of the multiple assignment scheme. These functions are the main idea behind the monotone circuit construction [5] that we use throughout this paper.

The notion of security utilized in the previous secret sharing works is that of perfect security, first introduced by Shannon [6] in 1949.[1] This same notion was utilized by Wyner in 1975 when proposing the wire-tap channel [9], [10]. Carleial and Hellman then proposed in 1977 the notion of individual security [11] to obtain higher data rates for the case where messages are uniformly and independently distributed. Since then, individual security has been applied to various communication and storage systems, e.g., single communication link [12], broadcast channels [13]–[16], multiple-access channels [17], [18], networks and multicast communications [19]–[21], algebraic security [22], [23], terahertz wireless systems [24], angularly dispersive links [25], and distributed storage systems [26]–[30]. Individual security guarantees that an eavesdropper, which can obtain any subset (up to a certain size) of the shared information, obtains no information about each message individually. Yet, an eavesdropper may obtain some insignificant controlled information about the mixture of all the messages.

Karnin et. al. in 1983 [31] brought the notion of individual security to secret sharing for the case of multiple secrets. This setting is known as multi-secret sharing.[2] Since then, much work has been done in multi-secret sharing, e.g., works on threshold schemes [31]–[34], generalizing ideal secret sharing schemes to ideal multi-secret schemes [35], and defining different access structures for different messages [34], [36], [37]. However, to the best of our knowledge, there is no general construction of individually-secure multi-secret sharing schemes for general access structures in the literature. For example, as the monotone circuit construction [5] for single-secret sharing.

Our main contributions are as follows. In Algorithm 1 we show how to convert a single-secret sharing scheme with a general access structure into an individually secure multi-secret sharing scheme where each message has the same access structure. The algorithm works by identifying which shares of the single-secret sharing scheme can be replaced by combinations of messages. In Theorem 1, we show that the scheme obtained from Algorithm 1 by performing $m-1$ shares replacements is a multi-secret sharing scheme with information rate of $m/|S|$, where S is the set of shares. This provides an improvement over the information rate of $1/|S|$ in the original single-secret sharing scheme. Moreover, we show in Theorem 2 that making extra replacements causes the decodability of the scheme to fail.

II. Preliminaries on Single-Secret Sharing

In this section, we first give definitions for a single-secret sharing scheme on a general access structure and its information rate. We then give an overview of the monotone circuit construction from [5].

A. Single-Secret Sharing

Given a group of n participants $\mathcal{P} = \{P_1, \ldots, P_n\}$ a secret message M_1, and a set of k authorized subsets $\Gamma =$

[1] Shannon published an earlier version of this paper in 1945 [7] which was classified. Interestingly, this precedes Shannon's *other* seminal paper [8].

[2] In order to better distinguish the settings, in the rest of the paper we refer to the traditional secret sharing as single-secret sharing.

Symbol	Description
$\mathbb{F}_q$	Finite Field of size q
$\mathcal{P} = \{P_1, \ldots, P_n\}$	Set of participants
n	Number of participants
Γ	Access structure (set of all authorized subsets)
$A_i \subseteq \mathcal{P}$	A minimal authorized subset
$\Gamma_0 = \{A_1, \ldots, A_r\}$	Basis of the access structure (set of minimal authorized subsets)
r	Number of minimal authorized subsets
$2^{\mathcal{P}} \setminus \Gamma$	Set of unauthorized subsets
U	An unauthorized subset
S_A	Set of shares belonging to authorized subset A
S_j^A	Share of P_j associated with A
$S_{P_j} = \{S_j^A\}_{A \in \Gamma_0}$	Set of shares belonging to P_j
$S = \bigcup_{P_j \in \mathcal{P}} S_{P_j}$	Set of all shares
S_U	Set of shares belonging to an unauthorized subset
m	Number of messages
$M = \{M_1, \ldots, M_m\}$	Set of all messages
$\mathcal{R}_{SS}$	Information rate of a secret sharing scheme
$\mathcal{R}_{MS}$	Information rate of a multi-secret sharing scheme

TABLE I
LIST OF SYMBOLS

$\{A_1, \ldots, A_k\}$, which we call an access structure, a single-secret sharing scheme consists in assigning to each participant a set of shares $S_{P_1}, \ldots, S_{P_n}$ in such a way that only authorized subsets of $\mathcal{P}$ are able to retrieve the secret, while unauthorized subsets $U \notin \Gamma$ remain completely ignorant about the secret.

As is common in the literature [3]–[5], we only consider monotone access structures, i.e., if $A \in \Gamma$ and $A' \supseteq A$, then $A' \in \Gamma$. Thus, it is sufficient to consider only the minimal authorized subsets $A_i \subseteq \mathcal{P}$. The set of minimal authorized subsets is called a basis for Γ which we denote by Γ_0.

We denote the set of all shares by $S = \bigcup_{P_j \in \mathcal{P}} S_{P_j}$, the shares held by an authorized subset by $S_A \subseteq S$, and the shares held by an unauthorized subset by $S_U \subseteq S$. This leads to the following definition.

Definition 1. Given a basis $\Gamma_0 = \{A_1, \ldots, A_r\}$ for an access structure Γ and a secret $M_1 \in \mathbb{F}_q$, a *single-secret sharing scheme realizing* Γ is one in which a set of shares $S \subseteq \mathbb{F}_q$ is created such that the following hold.

1) **Decodability**: The conditional entropy $\mathrm{H}(M_1|S_A) = 0$ for all $A \in \Gamma$. In other words, every authorized subset is able to compute the secret.
2) **Security**: The mutual information $\mathrm{I}(M_1; S_U) = 0$ for all $U \in 2^{\mathcal{P}} \setminus \Gamma$. In other words, no unauthorized subset learns any new information about the secret.

Remark 1. We only need to consider access structures where every authorized subset consists of more than one participant. If Γ is an access structure on n participants that has an authorized subset $A = \{P_i\}$ for some i, then we can consider the access structure Γ' on $n-1$ participants where $\Gamma'_0 = \Gamma_0 \setminus A$. This is due to the fact that P_i's share would be the secret itself.

We now define our performance metric.

Definition 2. The *information rate* of any secret sharing scheme (single or multi) is measured in terms of the ratio between the number of secrets and the total number of shares.

B. Monotone Circuit Construction

The monotone circuit construction [5] is a single-secret sharing scheme that can realize any access structure Γ. The scheme works as follows. Given a set of participants $\mathcal{P}$ and a basis of authorized subsets $\Gamma_0 = \{A_1, \ldots, A_r\}$ of Γ, we associate a monotone Boolean function that represents Γ_0. For example, if $\Gamma_0 = \{A_1, A_2\}$ where $A_1 = \{P_1, P_2\}$ and $A_2 = \{P_1, P_3\}$, then the monotone function representing Γ_0 is $(P_1 \wedge P_2) \vee (P_1 \wedge P_3)$. This monotone Boolean function is then utilized to create a circuit where the gates of the circuit correspond to the clauses of the function. Share assignment for the monotone circuit construction is carried out as follows. For participant $P_j \in A$, the share assigned to P_j associated with A is denoted by S_j^A. These shares are chosen uniformly at random but in such a way that their sum is equal to M_1, i.e., $\sum_{P_j \in A} S_j^A = M_1$. We achieve this by fixing one of the shares and choosing the others uniformly at random.

We remark here that to simplify the technical aspects and allow us to focus on the key methods and results, during this paper we have chosen to work with the monotone circuit construction for its simplicity. However, it is known that there are other, more efficient, constructions for general access structure secret sharing such as the vector space construction of [38], the decomposition construction of [5], and the geometric construction of [39]–[41].

III. MULTI-SECRET SHARING

Given a group of participants $\mathcal{P}$ and an access structure Γ as before along with a set of uniform and independently distributed messages $M = \{M_1, \ldots, M_m\}$, a multi-secret sharing scheme consists in creating a set of shares S in such a way that authorized subsets are able to reconstruct all m messages while unauthorized subsets remain completely ignorant about each individual message. Schemes that have this property are said to be individually secure. The following is a more formal definition.

Definition 3. Given a basis $\Gamma_0 = \{A_1, \ldots, A_r\}$ for an access structure Γ and a set of messages $M = \{M_1, M_2, \ldots, M_m\} \subseteq \mathbb{F}_q$ where each message is uniformly and independently distributed, a *multi-secret sharing scheme realizing* Γ is one in which a set of shares $S \subseteq \mathbb{F}_q$ is distributed amongst the participants such that the following hold.

1) **Decodability**: The conditional entropy $\mathrm{H}(M|S_A) = 0$ for all $A \in \Gamma$. In other words, every authorized subset can compute all m messages.
2) **Individual Security**: For any unauthorized subset $U \in 2^{\mathcal{P}} \setminus \Gamma$, the mutual information $\mathrm{I}(M_\ell; S_U) = 0$, for any $\ell \in \{1, \ldots, m\}$. In other words, unauthorized subsets learn no new information about each message individually.

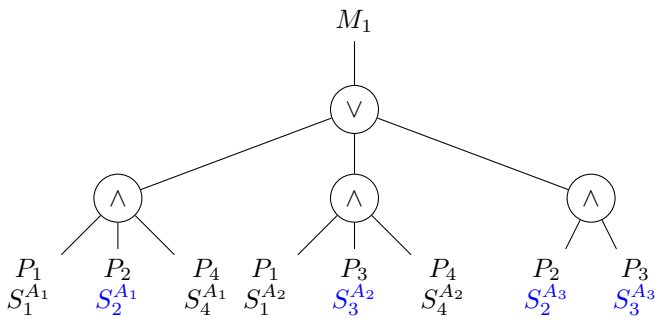

Fig. 1. The monotone circuit for Γ_0, which can be represented by the following monotone Boolean function: $(P_1 \wedge P_2 \wedge P_4) \vee (P_1 \wedge P_3 \wedge P_4) \vee (P_2 \wedge P_3)$. Each $\wedge$ gate corresponds to adding the shares on the input wires and thus represents a secret sharing scheme among the participants of A_i. These smaller schemes are the key to proving the monotone circuit single-secret sharing scheme is decodable and secure. The replaceable shares for our construction are shown in blue.

In Theorem 1 we show how to transform a single-secret sharing scheme for a general access structure into a multi-secret sharing scheme for the same access structure. In the next section, we present a detailed example of our approach to showcase the essential ingredients of the scheme.

IV. An Example of Our Approach

In the example given herein, we show how to convert a single-secret sharing scheme from [5], with a general access structure, into an individually secure multi-secret sharing scheme for the same access structure. Our technique consists in identifying shares from the original scheme which can be substituted with a linear combination of messages. We begin by presenting a single-secret sharing scheme.

A. Single-Secret Sharing for a General Access Structure

Let $\mathcal{P} = \{P_1, P_2, P_3, P_4\}$ be the set of participants and consider an access structure Γ with a basis

$$\Gamma_0 = \{\{P_1, P_2, P_4\}, \{P_1, P_3, P_4\}, \{P_2, P_3\}\}.$$

Thus, for example, participants $P_1, P_2,$ and P_4 can compute the secret but participants P_1 and P_2 cannot. Also, since participants P_2 and P_3 can compute the secret, so can participants P_1, P_2, and P_3, i.e., $\{P_1, P_2, P_3\} \in \Gamma$. The access structure Γ_0 can be represented by the monotone circuit in Figure 1.

The construction in [5] consists in assigning one share to each participant corresponding to each authorized subset $A \in \Gamma_0$. Denote the authorized subsets in Γ_0 by $A_1 = \{P_1, P_2, P_4\}$, $A_2 = \{P_1, P_3, P_4\}$, and $A_3 = \{P_2, P_3\}$. Then by [5], participant P_1 is assigned two shares, $S_1^{A_1}$ and $S_1^{A_2}$, participant P_2 is assigned two shares, $S_2^{A_1}$ and $S_2^{A_3}$, participant P_3 is assigned two shares, $S_3^{A_2}$ and $S_3^{A_3}$, and participant P_4 is assigned two shares, $S_4^{A_1}$ and $S_4^{A_2}$.

The shares in each authorized subset are chosen uniformly at random but such that their sum is equal to the secret M_1. In this example, this means that shares are constructed so that $S_1^{A_1} + S_2^{A_1} + S_4^{A_1} = M_1$, $S_1^{A_2} + S_3^{A_2} + S_4^{A_2} = M_1$, and $S_2^{A_3} + S_3^{A_3} = M_1$. One way to obtain this is by fixing one of the $S_j^{A_1}$'s, one of the $S_j^{A_2}$'s, and one of the $S_j^{A_3}$'s and choosing the other shares uniformly at random. For the single-secret sharing problem in [5], the choice of which share to fix is not relevant. In other words, fixing $S_2^{A_1}$ instead of fixing $S_4^{A_1}$ as is done in [5] does not affect the decodability or security of the scheme. This choice, however, is relevant in our construction when we replace shares with linear combinations of messages.

The decodability of the scheme is shown in [5], and follows from the fact that the shares associated with each authorized subset form an independent single-secret sharing scheme. The security of the scheme also follows from this fact since the schemes being independent means that no share is assigned to more than one participant. Note that since there are 8 total shares and 1 secret, the information rate of this single-secret sharing scheme is $\mathcal{R}_{SS} = \frac{1}{8}$.

B. The Conditions for Replacing a Share

In order to obtain a multi-secret sharing scheme with the same access structure, Γ, for all messages, our construction consists of replacing certain random shares from the single-secret sharing scheme with linear combinations of messages. The criterion for identifying which shares can be replaced is as follows. A share $S_j^{A_i}$ is replaceable if for every $A' \in \Gamma_0$ either $P_j \in A'$ or $A \backslash \{P_j\} \subseteq A'$. Thus, in our example, the share $S_2^{A_1}$ is replaceable since $P_2 \in A_1 \cap A_3$ and $A_1 \backslash P_2 \subseteq A_2$. However, the share $S_1^{A_1}$ is not, since $P_1 \notin A_3$ and $A_1 \setminus P_1 \not\subseteq A_3$.

The first step in our construction consists in determining which shares are replaceable. Checking for the replaceability conditions, we obtain that the replaceable shares for the access structure Γ_0 are $S_2^{A_1}, S_3^{A_2}, S_2^{A_3}$, and $S_3^{A_3}$, as illustrated in Figure 1. To show why the replaceability conditions are defined as so, consider the following two examples where we want to introduce a new message M_2 into the shares. For these examples, we choose $S_4^{A_1} = M_1 - S_1^{A_1} - S_2^{A_1}$ to be the fixed share of A_1.

Consider replacing the share $S_2^{A_1}$ with the linear combination of messages $2M_1 + M_2$. The authorized set A_1 can compute M_1 because the shares in A_1 still sum to M_1. They can then compute M_2 since they can subtract $2M_1$ from $S_2^{A_1} = 2M_1 + M_2$. Again, the authorized set A_2, can compute M_1 because its shares still sum to M_1. They can then compute M_2 since $M_2 = -S_1^{A_1} - S_4^{A_1} - M_1$. Finally, the authorized set A_3 can compute M_1 because the shares in A_3 still sum to M_1. Since A_3 contains participant P_2, the share $S_2^{A_1} = 2M_1 + M_2 \in S_{A_3}$. So they can compute M_2 by subtracting $2M_1$ from $S_2^{A_1}$. Thus, after computing M_1, all three authorized subsets can compute M_2.

We now show that if the replaceability condition is not satisfied, then our replacement technique does not work. As described above, the share $S_1^{A_1}$ does not satisfy the replacement condition. Suppose we instead replace the share $S_1^{A_1}$ with $2M_1 + M_2$. We show that the authorized set A_3 is not able to compute M_2. Note that the only shares A_3 has access to are $S_2^{A_1}, S_2^{A_3}, S_3^{A_2}$, and $S_3^{A_3}$. Since $S_1^{A_1} = M_1 - S_2^{A_1} - S_4^{A_1}$ and neither $S_1^{A_1}$ nor $S_4^{A_1}$ are accessible to the participants in A_3, there is no linear combination of the shares in S_{A_3} that

allow for the recovery of $S_1^{A_1}$. Thus, M_2 cannot be computed by the participants in authorized subset A_3.

The second step in our construction is to choose, for each authorized subset $A \in \Gamma_0$, which share S_j^A to fix. The choice is made as follows. For each authorized subset $A \in \Gamma_0$, if every share S_j^A is replaceable, then pick any of them to be fixed. Otherwise, pick a non-replaceable share S_j^A to be fixed. The choice of which share to fix is relevant for our construction since we want to maximize the number of messages we are able to introduce into the scheme.

The third and final step in our construction is to take the shares that are replaceable, but not fixed, and replace them with linear combinations of the message M_1 with a new message M_ℓ, for each replaced share. These linear combinations are of the form $aM_1 + bM_\ell$ where $a \notin \{0, 1\}$ and $b \neq 0$. It is necessary for both a and b to be different than zero, because no participant should have a share which consists of a single message M_ℓ, otherwise, we would have an authorized subset with a single participant. Furthermore, $a \neq 1$ since a fixed share S_j^A has the form $M_1 - \sum_{P_k \in A \setminus \{P_j\}} S_k^A$. Suppose that we replace the share S_i^A with $aM_1 + bM_\ell$ where $a = 1$. Then since $A \in \Gamma_0$ is a minimal authorized subset, $A \setminus \{P_i\}$ is an unauthorized subset. If the participants in $A \setminus P_i$ add their shares, they can compute $M_1 - S_i^A = M_1 - M_1 - bM_\ell = -bM_\ell$ which violates the security of the scheme.

C. From Single-Secret to Multi-Secret Sharing Schemes

We now show the details of converting the monotone circuit construction to our construction for the basis Γ_0 depicted in Figure 1 using the following steps:

1) Identify which shares are replaceable. A share $S_j^{A_i}$ is replaceable if $P_j \in A$ or $A_i \setminus \{P_j\} \subseteq A$ for all $A \in \Gamma_0$.
2) For each $A \in \Gamma_0$, if the share S_j^A is replaceable for all participants $P_j \in A$, pick one of them to fix. Otherwise, fix a non-replaceable share.
3) Replace all shares S_j^A such that S_j^A is replaceable but not fixed. The replacement is of the form $aM_1 + bM_\ell$ where $a \notin 0, 1$ and $b \neq 0$. Note that each M_ℓ appears in exactly one replacement.

We note that any remaining shares that have not been replaced or fixed are still uniform random over $\mathbb{F}_q$.

As mentioned earlier (and shown in Figure 1), the replaceable shares for $\Gamma_0 = \{\{P_1, P_2, P_4\}, \{P_1, P_3, P_4\}, \{P_2, P_3\}\}$ are $S_2^{A_1}, S_3^{A_2}, S_2^{A_3}$, and $S_3^{A_3}$. We choose to fix the shares $S_4^{A_1}$, $S_4^{A_2}$, and $S_3^{A_3}$. Thus, $S_4^{A_1} = M_1 - S_1^{A_1} - S_2^{A_1}$, $S_4^{A_2} = M_1 - S_1^{A_2} - S_3^{A_2}$, and $S_3^{A_3} = M_1 - S_2^{A_3}$. The replacements we make for this access structure are $S_2^{A_1} = 2M_1 + M_2$, $S_2^{A_3} = 2M_1 + M_3$, and $S_3^{A_2} = 2M_1 + M_4$.

We now prove that the scheme described above is decodable (all authorized subsets can compute all messages) and individually secure (no unauthorized subset gains any new information about any individual messages).

Proposition 1 (Decodability)**.** $\mathrm{H}(M_1, M_2, M_3, M_4 | S_A) = 0$ *where S_A is the set of shares held by an authorized subset, i.e. every subset $A \in \Gamma_0$ can compute all messages M_1, M_2, M_3, M_4.*

Proof. $\{\mathbf{P_1}, \mathbf{P_2}, \mathbf{P_4}\}$: For this authorized subset, $S_A = \{S_1^{A_1}, S_1^{A_2}, S_2^{A_1}, S_2^{A_3}, M_1 - S_1^{A_1} - S_2^{A_1}, M_1 - S_1^{A_2} - S_3^{A_2}\}$. Since $M_1 - S_1^{A_1} - S_2^{A_1} + S_1^{A_1} + S_2^{A_1} = M_1$, it follows that $S_2^{A_3} - 2M_1 = M_2$, $S_2^{A_1} - 2M_1 = M_3$, and $-(M_1 - S_1^{A_2} - S_3^{A_2}) - S_1^{A_2} - M_1 = M_4$. Thus, by [42, Lemma 3], $\mathrm{H}(M_1, M_2, M_3, M_4 | S_A) = 0$.

$\{\mathbf{P_1}, \mathbf{P_3}, \mathbf{P_4}\}$: For this authorized subset, $S_A = \{S_1^{A_1}, S_1^{A_2}, S_3^{A_2}, M_1 - S_2^{A_3}, M_1 - S_1^{A_1} - S_2^{A_1}, M_1 - S_1^{A_2} - S_3^{A_2}\}$. Since $M_1 - S_1^{A_2} - S_3^{A_2} + S_1^{A_2} + S_3^{A_2} = M_1$, it follows that $-(M_1 - S_1^{A_1} - S_2^{A_1}) - M_1 - S_1^{A_1} = M_2$, $-(M_1 - S_2^{A_3}) - M_1 = M_3$, and $S_3^{A_2} - 2M_1 = M_4$. Thus, by [42, Lemma 3], $\mathrm{H}(M_1, M_2, M_3, M_4 | S_A) = 0$.

$\{\mathbf{P_1}, \mathbf{P_2}\}$: For this authorized subset, $S_A = \{S_2^{A_1}, S_2^{A_3}, S_3^{A_2}, M_1 - S_2^{A_3}\}$. Since $M_1 - S_2^{A_3} + S_2^{A_3} = M_1$ it follows that $S_2^{A_1} - 2M_1 = M_2$, $S_2^{A_3} - 2M_1 = M_3$, and $S_3^{A_2} - 2M_1 = M_4$. Thus, by [42, Lemma 3], $\mathrm{H}(M_1, M_2, M_3, M_4 | S_A) = 0$. □

Proposition 2 (Individual Security)**.** $\mathrm{I}(M_\ell; S_U) = 0$ *for $\ell \in \{1, \ldots, 4\}$ where S_U is the set of shares held by unauthorized subset, i.e. no unauthorized subset learns any new information about any of the 4 messages.*

Proof. It is sufficient to consider only the maximal unauthorized subsets which are, for this example, $\{P_1, P_2\}$,$\{P_1, P_3\}$,$\{P_1, P_4\}$,$\{P_2, P_4\}$, and $\{P_3, P_4\}$. We prove the proposition for $\{P_1, P_2\}$ since analogous arguments work for the other unauthorized subsets. For this subset, $S_U = \{S_1^{A_1}, S_1^{A_2}, S_2^{A_1}, S_2^{A_3}\}$. By the definition of mutual information, $\mathrm{I}(M_1; S_U) = \mathrm{H}(S_U) - \mathrm{H}(S_U | M_1)$.

Note that S_U can be represented by the following matrix equation:

$$\mathcal{A} \begin{pmatrix} M_1 \\ M_2 \\ M_3 \\ M_4 \\ S_1^{A_1} \\ S_1^{A_2} \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 2 & 1 & 0 & 0 & 0 & 0 \\ 2 & 0 & 1 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} M_1 \\ M_2 \\ M_3 \\ M_4 \\ S_1^{A_1} \\ S_1^{A_2} \end{pmatrix} = \begin{pmatrix} S_1^{A_1} \\ S_1^{A_2} \\ 2M_1 + M_2 \\ 2M_1 + M_3 \end{pmatrix}$$

Since $\mathcal{A}$ is full rank and $S_1^{A_1}, S_1^{A_2}, M_1, M_2, M_3, M_4$ all follow a uniform distribution, by [42, Lemmas 5 and 6] we have that $\mathrm{H}(S_U) = 4 \log_2 q$.

Now, [42, Lemma 4], $\mathrm{H}(S_U | M_1) = \mathrm{H}(S_1^{A_1}, S_1^{A_2}, M_2, M_3)$. Thus, $S_U | M_1$ can be represented by the following:

$$\mathcal{A}_1 \begin{pmatrix} M_1 \\ M_2 \\ M_3 \\ M_4 \\ S_1^{A_1} \\ S_1^{A_2} \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} M_1 \\ M_2 \\ M_3 \\ M_4 \\ S_1^{A_1} \\ S_1^{A_2} \end{pmatrix} = \begin{pmatrix} S_1^{A_1} \\ S_1^{A_2} \\ M_2 \\ M_3 \end{pmatrix}$$

Since $\mathcal{A}_1$ is full rank we have that $\mathrm{H}(S_U | M_1) = 4 \log_2 q$ by [42, Lemmas 5 and 6].

Thus,

$$\begin{aligned} \mathrm{I}(M_1; S_U) &= \mathrm{H}(S_U) - \mathrm{H}(S_U|M_1) \\ &= 4\log_2 q - 4\log_2 q \\ &= 0. \end{aligned}$$

Showing $\mathrm{I}(M_\ell; S_U) = 0$ for $\ell \in \{2,3,4\}$ involves similar arguments. □

Since we now have 4 messages and we have not increased the number of shares, the information rate using our construction for this example is $\mathcal{R}_{MS} = \frac{4}{8} = \frac{1}{2}$, an improvement over the information rate $\mathcal{R}_{SS} = \frac{1}{8}$ of the single-secret sharing scheme.

V. Main Results

In this section, we show how to convert any single-secret sharing scheme with a general access structure into a multi-secret sharing scheme where every message has the same access structure. Given a single-secret sharing scheme with a monotone circuit, $(\mathcal{P}, \Gamma_0, S)$, we define a replaceable share as the following.

Definition 4. A share S_j^A is *replaceable* if, for every authorized subset $A' \in \Gamma_0$, either the participant $P_j \in A'$ or the subset $A \setminus P_j \subseteq A'$.

Then, as shown in Section IV, our method for replacing shares consists in the following algorithm.

Algorithm 1 (Replacement Algorithm)**.** Given a monotone circuit construction, we perform the following steps.

1) Identify replaceable shares S_j^A according to Definition 4.
2) For each authorized subset $A \in \Gamma_0$, if the share S_j^A is replaceable for every participant $P_j \in A$, pick any such share to be fixed. Otherwise, fix a non-replaceable S_j^A.
3) Replace every share S_j^A that is replaceable but not fixed with a linear combination of messages of the form $aM_1 + bM_\ell$ where $a \notin 0, 1$ and $b \neq 0$ for $\ell \in \{2, \ldots, m\}$. Each M_ℓ is allowed to appear in exactly one replacement.

We now present in Theorems 1 and 2 the main results of this paper for an individually secure multi-secret sharing scheme.

Theorem 1. *Let $(\mathcal{P}, \Gamma_0, S)$ be a single-secret sharing scheme with a monotone circuit. Then, by applying Algorithm 1, we construct an individually secure multi-secret sharing scheme that achieves an information rate of $\mathcal{R}_{MS} = \frac{m}{|S|}$ where $m-1$ is the number of replaced shares.*

The proof of Theorem 1 relies on the following two Lemmas 1 and 2 to show that the new scheme is decodable and individually secure.

Lemma 1 (Decodability)**.** *Let S_A be the set of shares held by an authorized subset A after applying Algorithm 1. For all $A \in \Gamma_0$, $\mathrm{H}(M_\ell|S_A) = 0$ for any ℓ. In other words, all authorized subsets can compute all messages.*

Proof. We prove Lemma 1 by showing that every message can be written as a linear combination of the shares held by an authorized subset. By construction, M_1 is equal to the sum of the shares $S_j^A \in S_A$, i.e., $M_1 = \sum_{P_j \in A} S_j^A$. Thus, $\mathrm{H}(M_1|S_A) = 0$ for all A by [42, Lemma 3].

For the remaining messages M_ℓ, $\ell \in \{2, \ldots, m\}$, there exists a participant $P_j \in A_i$ such that $S_j^{A_i} = aM_1 + bM_\ell$. For each authorized subset A, there are two cases to consider.

Case 1 ($P_j \in A$)**:** In this case, $S_j^{A_i} \in S_A$. Then, since we've already shown A can compute M_1, we can write M_ℓ as a linear combination of $S_j^{A_i}$ and M_1. More explicitly, $b^{-1}(S_j^{A_i} - aM_1) = b^{-1}(aM_1 + bM_\ell - aM_1) = M_\ell$. Thus, $\mathrm{H}(M_\ell|S_A) = 0$ by [42, Lemma 3].

Case 2 ($P_j \notin A$)**:** Since $P_j \notin A$, then $A_i \setminus \{P_j\} \subseteq A$ by our replaceability condition. Let $S' = S_{A_i} \setminus S_{P_j}$ be the set of shares held by $A_i \setminus \{P_j\}$. Then $S' \subseteq S_A$. By construction, we can recover $S_j^{A_i}$ as a linear combination of the shares $S_t^{A_i} \in S'$ for $t \neq j$, i.e., $S_j^{A_i} = M_1 - \sum_{t \neq j} c_t S_t^{A_i}$ for some constants $c_t \in \mathbb{F}_q$. Then, as in Case 1, we can write M_ℓ as a linear combination of $S_j^{A_i}$ and M_1. Thus, $\mathrm{H}(M_\ell|S_A) = 0$ by [42, Lemma 3]. □

Lemma 2 (Security)**.** *After applying Algorithm 1, no unauthorized subset gains any new information about any individual message, i.e. $\mathrm{I}(M_\ell; S_U) = 0$ for $\ell \in \{1, \ldots, m\}$ where $S_U = \bigcup_{P_j \in U} S_{P_j}$ is the set of shares held by an unauthorized subset.*

Proof: The proof is given in [42, Appendix A].

The proof of individual security given in [42, Appendix A] is done using an inductive argument where the base case follows from the underlying secret sharing scheme. The inductive step is proved by showing that the representative matrices for S_U and $S_U|M_\ell$ for $\ell \in \{1, \ldots, m-1\}$ remain full rank after the replacement since they are obtained by elementary column operations. To finish the inductive step, we show that the new representative matrix for $S_U|M_m$ is also full rank. This is done by way of contradiction. Thus, when $m-1$ shares are replaced, the information rate for our construction of a multi-secret sharing scheme is $\mathcal{R}_{MS} = \frac{m}{|S|}$.

Finally, we show that if a share S_j^A not satisfying Definition 4 is replaced, then the decodability of the scheme fails. Thus, our replacement procedure can only be applied to replaceable shares.

Theorem 2. *Suppose P_j's share $S_j^{A_i}$ is not replaceable. If we make the replacement $S_j^{A_i} = aM_1 + bM_\ell$ where $a \notin 0, 1$ and $b \neq 0$, then $\mathrm{H}(M_\ell|S_A) \neq 0$ where S_A is the set of shares held by the participants in A. In other words, replacing a share that does not satisfy Definiton 4 results in some authorized subset being unable to compute M_ℓ.*

Proof: The proof is given in [42, Appendix B].

The proof of Theorem 2 given in [42, Appendix B] follows from the fact that there exists an authorized subset that does not have S_j^A and also does not have enough shares of $S_A \setminus S_{P_j}$ in order to reconstruct S_j^A.

REFERENCES

[1] G. R. Blakely, "Safeguarding cryptographic keys," in *Proc. AFIPS*, vol. 48, 1979, pp. 313–317.

[2] A. Shamir, "How to share a secret," in *Commun. of the ACM*, vol. 22, 1979, pp. 612–613.

[3] M. Ito, A. Saito, and T. Nishizeki, "Secret sharing scheme realizing general access structure," in *Proc. IEEE Global Telecom. Conf. (Globecom '87)*, 1987, pp. 99–102.

[4] J. Benaloh and J. Leichter, "Generalized secret sharing and monotone functions," in *Advances in Cryptology — CRYPTO '88*, ser. Lecture Notes in Computer Science. Berlin: Springer-Verlag, 1990, no. 403, pp. 27–35.

[5] D. R. Stinson, "An explication of secret sharing schemes," in *Designs, Codes and Cryptography*. Springer, Dec. 1992, vol. 2, pp. 357–390.

[6] C. E. Shannon, "Communication theory of secrecy systems," *The Bell system technical journal*, vol. 28, no. 4, pp. 656–715, 1949.

[7] ——, "A mathematical theory of cryptography," *Bell System Technical Memo MM 45-110-02*, 1945.

[8] ——, "A mathematical theory of communication," *The Bell system technical journal*, vol. 27, no. 3, pp. 379–423, 1948.

[9] A. D. Wyner, "The wire-tap channel," *Bell system technical journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[10] L. H. Ozarow and A. D. Wyner, "Wire-tap channel II," *AT&T Bell Laboratories technical journal*, vol. 63, no. 10, pp. 2135–2157, 1984.

[11] A. Carleial and M. E. Hellman, "A note on wyner's wiretap channel (corresp.)," *IEEE Trans. Inform. Theory*, vol. 23, no. 3, pp. 387–390, May 1977.

[12] D. Kobayashi, H. Yamamoto, and T. Ogawa, "Secure multiplex coding attaining channel capacity in wiretap channels," *IEEE Trans. on Inf. Theory*, vol. 59, no. 12, pp. 8131–8143, 2013.

[13] A. S. Mansour, R. F. Schaefer, and H. Boche, "Secrecy measures for broadcast channels with receiver side information: Joint vs individual," in *2014 IEEE Information Theory Workshop (ITW 2014)*. IEEE, 2014, pp. 426–430.

[14] Y. Chen, O. O. Koyluoglu, and A. Sezgin, "On the individual secrecy rate region for the broadcast channel with an external eavesdropper," in *2015 IEEE International Symposium on Information Theory (ISIT)*. IEEE, 2015, pp. 1347–1351.

[15] A. S. Mansour, R. F. Schaefer, and H. Boche, "The individual secrecy capacity of degraded multi-receiver wiretap broadcast channels," in *2015 IEEE International Conference on Communications (ICC)*. IEEE, 2015, pp. 4181–4186.

[16] ——, "On the individual secrecy capacity regions of the general, degraded, and gaussian multi-receiver wiretap broadcast channel," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 9, pp. 2107–2122, 2016.

[17] M. Goldenbaum, R. F. Schaefer, and H. V. Poor, "The multiple-access channel with an external eavesdropper: Trusted vs. untrusted users," in *2015 49th Asilomar Conference on Signals, Systems and Computers*. IEEE, 2015, pp. 564–568.

[18] Y. Chen, O. O. Koyluoglu, and A. H. Vinck, "On secure communication over the multiple access channel," in *2016 International Symposium on Information Theory and Its Applications (ISITA)*. IEEE, 2016, pp. 350–354.

[19] K. Bhattad, K. R. Narayanan *et al.*, "Weakly secure network coding," *NetCod, Apr*, vol. 104, pp. 8–20, 2005.

[20] D. Silva and F. R. Kschischang, "Universal weakly secure network coding," in *2009 IEEE Information Theory Workshop on Networking and Information Theory*. IEEE, 2009, pp. 281–285.

[21] A. Cohen, A. Cohen, M. Medard, and O. Gurewitz, "Secure multi-source multicast," *IEEE Transactions on Communications*, vol. 67, no. 1, pp. 708–723, 2018.

[22] L. Lima, M. Médard, and J. Barros, "Random linear network coding: A free cipher?" in *2007 IEEE International Symposium on Information Theory*. IEEE, 2007, pp. 546–550.

[23] J. Claridge and I. Chatzigeorgiou, "Probability of partially decoding network-coded messages," *IEEE Communications Letters*, vol. 21, no. 9, pp. 1945–1948, 2017.

[24] A. Cohen, R. G. L. D'Oliveira, C.-Y. Yeh, H. Guerboukha, R. Shrestha, Z. Fang, E. Knightly, M. Médard, and D. M. Mittleman, "Absolute security in terahertz wireless links," *IEEE Journal of Selected Topics in Signal Processing*, 2023.

[25] C.-Y. Yeh, A. Cohen, R. G. L. D'Oliveira, M. Médard, D. M. Mittleman, and E. W. Knightly, "Securing angularly dispersive terahertz links with coding," *IEEE Trans. on Inf. Forensics and Security*, 2023.

[26] S. Kadhe and A. Sprintson, "Weakly secure regenerating codes for distributed storage," in *2014 International Symposium on Network Coding (NetCod)*. IEEE, 2014, pp. 1–6.

[27] ——, "On a weakly secure regenerating code construction for minimum storage regime," in *2014 52nd Annual Allerton Conference on Communication, Control, and Computing (Allerton)*. IEEE, 2014, pp. 445–452.

[28] N. Paunkoska, V. Kafedziski, and N. Marina, "Improved perfect secrecy of distributed storage systems using interference alignment," in *2016 8th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*. IEEE, 2016, pp. 240–245.

[29] ——, "Improving the secrecy of distributed storage systems using interference alignment," in *2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC)*. IEEE, 2018, pp. 261–266.

[30] J. Bian, S. Luo, Z. Li, and Y. Yang, "Optimal weakly secure minimum storage regenerating codes scheme," *IEEE Access*, vol. 7, pp. 151 120–151 130, 2019.

[31] E. D. Karnin, J. W. Greene, and M. E. Hellman, "On secret sharing systems," *IEEE Trans. Inform. Theory*, vol. 29, no. 1, pp. 35–41, Jan. 1983.

[32] W.-A. Jackson, K. M. Martin, and C. M. O'Keefe, "Multisecret threshold schemes," in *Advances in Cryptology — CRYPTO '93'*, ser. Lecture Notes in Computer Science, D. R. Stinson, Ed. Berlin: Springer-Verlag, 1994, vol. 773, pp. 126–135.

[33] W.-A. Jackson, K. M. Matrin, and C. M. O'Keefe, "A construction for multi-secret threshold schemes," *Designs, Codes, and Cryptography*, vol. 9, pp. 287–303, 1996.

[34] C. Blundo, A. D. Santis, G. D. Crescenzo, A. G. Gaggia, and U. Vaccaro, "Multi-secret sharing schemes," in *Advances in Cryptology — CRYPTO '94'*, ser. Lecture Notes in Computer Science. Berlin: Springer-Verlag, 1994, vol. 839, pp. 150–163.

[35] W.-A. Jackson, K. M. Martin, and C. M. O'Keefe, "Ideal secret sharing schemes with multiple secrets," *Journal of Cryptology*, vol. 9, pp. 233–250, 1996.

[36] G. D. Crescenzo, "Sharing one secret vs. sharing many secrets," *Theoretical Computer Science*, vol. 295, no. 1, pp. 123–140, Feb. 2003.

[37] C. Blundo, A. D. Santis, and U. Vaccaro, "Efficient sharing of many secrets," in *Proc. STACS '93'*, ser. Lecture Notes in Computer Science, vol. 665. Berlin: Springer-Verlag, 1993, pp. 692–703.

[38] E. F. Brickell, "Some ideal secret sharing schemes," in *Workshop on the Theory and Application of of Cryptographic Techniques*. Springer, 1989, pp. 468–475.

[39] G. J. Simmons, "How to (really) share a secret," in *Conference on the Theory and Application of Cryptography*. Springer, 1988, pp. 390–448.

[40] ——, "An introduction to shared secret and/or shared control schemes and their application," *Contemporary cryptology*, pp. 441–497, 1991.

[41] K. Martin, G. Simmons, and W.-A. Jackson, "The geometry of shared secret schemes," *Bulletin of the ICA*, vol. 1, pp. 71–88, 1991.

[42] C. Bass, A. Cohen, R. G. L. D'Oliveira, and M. Médard, "A monotone circuit construction for individually-secure multi-secret sharing," 2024.