Broadcast Enforced Threshold Schemes with Disenrollment

Mingyan Li and Radha Poovendran*
Network Security Laboratory
Department of Electrical Engineering, University of Washington
email: myli, radha@ee.washington.edu

Abstract

Blakley, Blakley, Chan and Massey conjectured a lower bound on the entropy of broadcast messages in threshold schemes with disenrollment. In an effort to examine the conjecture, we identify their original scheme definition has a limitation: a coalition of participants can reconstruct all shared secrets without broadcast from the dealer, and hence render the dealer no control over disenrollment. We introduce a constraint that delays this lack of control of the dealer over disenrollment. We also establish the lower bounds on the entropy of broadcast messages in such a model. We demonstrate the need for new models by presenting a construction under open problems.

Keywords: secret sharing, threshold schemes with disenrollment, entropy

1 Introduction

A (t, n) threshold scheme is a technique to split a secret among a group of n participants in such a way that any subset of t or more participants can reconstruct the shared secret by pooling the information they have, while any subset of participants of cardinality less than t is unable to recover the secret [2], [14]. The information held by a participant is called a *share*, which is distributed securely by a trusted third party, called *dealer*, to the participant on initialization. Threshold schemes find important applications in cryptography and security, such as secure distributed storage of a master key, secure file sharing, and threshold signature [15].

Threshold schemes were first introduced by Shamir [14] and Blakley [2] and were generalized to secret sharing schemes, which allow reconstruction of a shared secret among a more general combination of subsets of participants. An excellent survey on secret sharing can be found in [15], and a bibliography is provided online in [16].

There are scenarios in which the share of a participant is stolen or is disclosed deliberately by the malicious participant. Then, for security reasons, the share has to be assumed to have become public knowledge, and the effective threshold among the group is reduced by 1, because any $t-1$ shares from the group plus the disclosed share suffice to reconstruct the secret. It is preferable that the same level of security, i.e., the same threshold size t, be preserved even if shares are disclosed. This may not present a problem if secure channel is available all the time, since the dealer can choose a new shared secret, construct a $(t, n-1)$ threshold scheme, and deliver new shares securely

*This research is funded in part by NSF grant ANI-0093187 and ARO grant DAAD 190210242.

to the remaining participants. However, an expensive secure channel is normally set up only to distribute initial shares and is no longer available after initialization. An alternative is to use public broadcast by the dealer. The problem of *maintaining the threshold via only broadcast* in case of share disclosure or loss was considered by Blakley, Blakley, Chan and Massey in [3], and the solutions were called *threshold schemes with disenrollment capability*. Blakley *et al.* formally defined *threshold schemes with L-fold disenrollment capability* as the schemes that have the capability of disenrolling L participants successively, one at a time, without reducing the threshold. In the model of a threshold scheme with disenrollment capability [3], it is assumed that no secure channel is available after initialization between the dealer and each participant or between participants, and a new secret is chosen to be shared among the group after each disenrollment. The scheme is different from a proactive secret sharing scheme [9], in which a long-term secret is protected against gradual break in by refreshing the share of each participant periodically using public key cryptosystems.

Share size and broadcast size are used to characterize a threshold scheme with disenrollment. While small share size may lead to low storage requirement, it reduces the search space of an adversary. Broadcast size indicates communication cost, and a broadcast message of smaller size is less likely to be corrupted during transmission when compared with a longer message. In [3], Blakley *et al.* established a lower bound on the size of shares in a threshold scheme with L-fold disenrollment capability and conjectured a lower bound on the size of public broadcast. Barwick *et al.* confirmed a revised version of the lower bound on the broadcast size in [1].

Our Contribution: We show that the model of a threshold scheme with disenrollment capability originally defined in [3] and also used in [1] can lead to *the disenrollment not under the control of the dealer*. We illustrate this point by studying a scheme in which a coalition of $t+i$ participants can recover the shared secret $K_0, ..., K_i$ before the i^{th} disenrollment, without requiring any broadcast from the dealer. In order to resolve the problem, we propose a broadcast enforced model of threshold schemes with disenrollment by adding one condition to the original scheme definition to ensure public broadcast from the dealer is necessary in the reconstruction of the current shared secret. Although Barwick *et al.* [1] stated that they do not constrain $t+i$ participants from constructing the shared secret K_i in advance, they also noted that if it is a potential problem, then a stronger model is necessary. Our broadcast enforced model can be viewed as the first step in seek of such a stronger model, and our model prevents the collusion of *any number* of participants from recovering new shared secrets without a broadcast message from the dealer. We establish lower bounds on broadcast messages in the new model. We also note that inherent limitation of the original disenrollment model by showing that even with our condition, the dealer can only delay the lack of control under user collusion. We discuss this problem in Section 5 and present examples showing the need for new directions.

Other related work on threshold schemes with disenrollment includes [4], [6], [8], [11], [12], [17]. In [11], disenrollment of untrustworthy participants was discussed for general secret sharing schemes, but no analytical study on the bounds of share size or broadcast size was provided. Blundo *et al.* [4] addressed a more general problem of enabling participants of different sets to reconstruct different secrets at different time via insecure public channel, and established lower bounds on share size. However, they did not investigate the lower bound on the broadcast size for a threshold scheme with disenrollment. Charnes *et al.* [6] presented a computationally secure threshold scheme with disenrollment using the hardness of discrete logarithm. In [8], secure channels between participants were employed to refresh valid participants with new shares in order to recover new secrets. A

scheme was proposed to realize disenrollment without changing shares in [17], but was later shown to be flawed in [12].

This paper is organized as follows. In Section 2, we review the definition of threshold schemes with disenrollment capability [3] and previous results on the lower bounds of share size [3] and broadcast size [1]. In Section 3, we show by one example that the original definition of threshold scheme with disenrollment potentially can render the dealer no control over disenrollment process. To fix the problem, we propose to add one broadcast enforcement term to the definition. In Section 4, we derive lower bounds on the size of broadcast messages in the model with the new property added. We finally conclude the paper with our contributions and one open problem in Section 5.

2 Preliminaries

In this section, we review the definitions of a threshold scheme and a threshold scheme with disenrollment in an information-theoretic approach, and summarize the results of previous study on the bounds of share size and broadcast size. For clarity of presentation, we list the notations used in this paper in Table 1.

Table 1: Notation

$H(\cdot)$	Shannon Entropy [7]
$I(\cdot)$	Mutual Information [7]
t	threshold
n	total number of participants
L	maximum allowable number of disenrollments
N	set of all the indices of n participants, i.e., $N = \{1, ..., n\}$
i	index for update stages
j	index for participants
S_j	share held by participant j
K_i	secret to be shared at stage i
P_i	broadcast message at stage i
d_i	index of the disenrolled participant at stage i
D_i	set of indices of all disenrolled participants up to stage i, i.e., $D_i = \{d_1, ..., d_i\}$
v_l	index of valid participants with a dummy counting index l
$S_j^{(i)}$	subshare of participant j corresponding to the shared secret K_i
R	random string used to hide a shared secret or a share
$X_{a:b}$	set $\{X_a, X_{a+1}, ...X_b\}$ for $a < b$

2.1 Threshold Schemes

A (t, n) threshold scheme is a protocol to divide a secret into n shares so that the knowledge of at least t shares allow full reconstruction of the secret [2], [14]. Let K be the shared secret that is a random variable that takes values from space $\mathcal{K}$, and S be a share that is a random variable that takes values from space $\mathcal{S}$. Let S_j be the share held by participant j, for $j \in N = \{1, .., n\}$.

Definition 1 *A (t, n) threshold scheme is a sharing of a secret K among n participants so that*

1. *The secret K is recoverable from at least t shares. That is, for any set of k $(t \leq k \leq n)$ indices $\{l_1, l_2, ..., l_k\} \subset \{1, ..., n\}$,*

$$H(K|S_{l_1:l_k}) = 0 \qquad for \qquad t \leq k \leq n \tag{1}$$

2. *The secret K remains uncertain with the knowledge of $(t-1)$ or less shares. That is,*

$$H(K|S_{l_1:l_k}) > 0 \qquad for \qquad k < t. \tag{2}$$

A (t, n) threshold scheme is called *perfect* in an information theoretic sense if $(t-1)$ or fewer shares reveal absolutely no information on the secret K. That is,

$$H(K|S_{l_1:l_k}) = H(K) \quad \text{for} \quad k < t. \tag{3}$$

It has been shown in [13] that a necessary condition to have a perfect threshold scheme is

$$H(S_j) \geq H(K) \qquad \text{for} \qquad j = 1, ..., n. \tag{4}$$

A perfect threshold scheme is called *ideal* if share size achieves the lower bound in (4), i.e., $H(S_j) = H(K)$ for all j.

2.2 Threshold Schemes with Disenrollment

A threshold scheme with L-fold disenrollment capability deals with the problem of maintaining a threshold via insecure broadcast channel when disenrolling an untrustworthy participant at each of L successive updates [3]. Let $i = 1, ..., L$ be the indices of update stages. At the i^{th} update, let K_i denote the shared secret, P_i denote the broadcast message, $d_i \in N \backslash D_{i-1}$ be the index of the disenrolled participant at the i^{th} update, and $v_l \in N \backslash D_i$ for $l = 1, ..., n-i$ be an index of one of the remaining valid participants.

Definition 2 *A (t, n) threshold scheme with L-fold disenrollment capability with $n - L \geq t$ is a collection of shares S_j for $j = 1, ..., n$; shared secrets K_i for $i = 0, ..., L$; and public broadcast messages P_i for $i = 1, ..., L$, that satisfies the following conditions:*

1. *Initially (i.e., at stage $i = 0$), the scheme is a (t, n) threshold scheme that shares the secret K_0 among n participants.*

2. *At stage i for $i = 1, ..., L$, one additional share S_{d_i} is disenrolled, any set of k $(t \leq k \leq n-i)$ valid shares $S_{v_1}, ..., S_{v_k}$ plus the broadcast messages $P_1, ..., P_i$ can reconstruct the new secret K_i, i.e.,*

$$H(K_i|S_{v_1:v_k}, P_{1:i}) = 0 \quad for \quad t \leq k \leq n-i. \tag{5}$$

3. *At stage i for $i = 1, ..., L$, given broadcast information $P_1, ..., P_i$ and all disenrolled shares $S_{d_1}, ..., S_{d_i}$, the shared secret K_i is not solvable if the number of valid shares is less than t. That is,*

$$H(K_i|S_{v_1:v_k}, S_{d_1:d_i}, P_{1:i}) > 0 \quad for \quad k < t. \tag{6}$$

A (t, n) threshold scheme with L-fold disenrollment capability is called *perfect* if

$$H(K_i|S_{v_1:v_k}, S_{d_1:d_i}, P_{1:i}) = H(K_i) \quad \text{for} \quad k < t. \tag{7}$$

From Definition 2, it follows that a threshold scheme with disenrollment capability at stage i is equivalent to a $(t, n-i)$ threshold scheme sharing K_i among $n-i$ valid participants. In order to be able to collectively reconstruct K_i, each participant must have a component in his share corresponding to K_i. Note that S_j is a collection of components to reconstruct $K_0, ..., K_L$. Let $S_j^{(i)}$ denote the component in S_j corresponding to K_i, and we call $S_j^{(i)}$ a *subshare* of participant j. The subshare satisfies

$$H(K_i|S^{(i)}_{v_1:v_k}, P_{1:i}) = 0 \quad \text{for} \quad t \le k \le n-i. \tag{8}$$

The necessary condition (4) can be extended to subshares as

$$H(S_j^{(i)}) \ge H(K_i) \quad \text{for} \quad j = 1, .., n \quad i = 0, ..., L \tag{9}$$

The share by participant j, S_j, is the union of all its subshares over L disenrollment stages, i.e., $S_j = \{S_j^{(0)}, S_j^{(1)}, ..., S_j^{(L)}\}$. Since the shared secrets K_i's at different stage $i = 0, ..., L$ are independent, the subshares of one participant that are used to recover different secrets are independent in a share size efficient scheme.

2.3 Previous Results on Bounds of Share Size and Broadcast Size

For a threshold scheme with disenrollment capability defined in Definition 2, Blakley *et al.* [3] established a lower bound on the entropy of each share, as stated in Theorem 1.

Theorem 1 *Let $S_{1:n}, P_{1:L}, K_{0:L}$ form a (t, n) perfect threshold scheme with L-fold disenrollment capability and $H(K_i) = m$ for $i = 0, 1, ..., L$. Then,*

$$H(S_j) \ge (L+1)m \qquad \textit{for} \quad j = 1, 2, ..., n. \tag{10}$$

The proof of Theorem 1 provided by Blakley *et al.* is built on their Lemma 5 in [3]. We find that the original proof of the Lemma 5 on page 543 of [3] fails in the last line. A correct proof of their Lemma 5 is presented in Appendix.

A perfect threshold scheme with disenrollment in which each share achieves its lower bound is called *share minimal* [1], i.e.,

$$H(S_j) = (L+1)m, \quad \text{for} \quad j = 1, ..., n \tag{11}$$

where $H(K_i) = m$ for $i = 0, ..., L$.

Blakley *et al.* [3] also proposed a conjecture on the lower bound of the entropy of broadcast. A modified version of the conjecture was proven by Barwick *et al.* in [1]. Theorem 2 summarizes the result of Barwick *et al.* on the entropy of broadcast.

Theorem 2 *Let $S_{1:n}, P_{1:L}, K_{0:L}$ form a (t, n) share minimal perfect threshold scheme with L-fold disenrollment capability satisfying properties (5), (7), and (11), then*

$$\sum_{l=1}^{i} H(P_l) \ge \sum_{l=1}^{i} \min(i, n-i-t+1)m \quad \textit{for} \quad i = 1, ..., L. \tag{12}$$

2.4 Useful Lemmas

In this section, we present some lemmas that will be useful in proving our theorems.

Lemma 1 *Let X, Y, Z and W be random variables. Given*

$$\begin{aligned} H(X|Y,W) &= 0, && (13)\\ H(X|Z,W) &= H(X), && (14)\\ H(X) &= H(Y) && (15) \end{aligned}$$

leads to

$$I(Y;Z) = 0. \quad (16)$$

Proof:

$$H(Y|Z) \geq H(Y|Z,W) \geq I(Y;X|Z,W) = H(X|Z,W) - H(Y|Z,W,Y) \overset{(a)}{=} H(X)$$

Equation (a) holds because of (13) and (14).

$$I(Y;Z) = H(Y) - H(Y|Z) \leq H(Y) - H(X) \overset{(b)}{=} 0.$$

Equation (b) holds because of (15). Furthermore, $I(Y;Z) \geq 0$ due to non-negativity of the mutual information of two random variables [7], it follows $I(Y;Z) = 0$. ■

Lemma 2 *Let X, Y and Z be random variables. Given*

$$\begin{aligned} H(X|Y,Z) &= 0, && (17)\\ H(X|Z) &= H(Y|Z) && (18) \end{aligned}$$

leads to

$$H(Y|X,Z) = 0. \quad (19)$$

Proof:

$$\begin{aligned} H(Y|X,Z) &= H(X,Y,Z) - H(X,Z)\\ &= H(X,Y,Z) - (H(Z) + H(X|Z))\\ &= H(X,Y,Z) - (H(Z) + H(Y|Z))\\ &= H(X,Y,Z) - H(Y,Z)\\ &= H(X|Y,Z) = 0 \end{aligned}$$

■

3 Broadcast Enforced Threshold Scheme with Disenrollment

In this section, we will show Definition 2 in Section 2.2 is not adequate when centralized control from the dealer is required, by examining a scheme that satisfies Definition 2 (originally appeared in [3] as Definition 2) but leaves the dealer no control over disenrollment process.

Let us consider the following scheme.

- Participant j holds the share $S_j = \{S_j^{(0)}, S_j^{(1)}, ..., S_j^{(L)}\}$ after initialization, where sub-share $S_j^{(i)}$ corresponds to a share of a $(t+i, n)$ ideal perfect threshold scheme sharing the secret K_i.
- At stage i, the dealer broadcasts $P_i = S_{d_i}$

If $t+i$ participants collaborate by exchanging their shares, then they can decipher $K_0, ..., K_i$ in advance and the disenrollment of an invalidated participant involving the update of K_{i-1} to K_i at stage i is not under the control of the dealer. Therefore, for the dealer to have control at each disenrollment, we should seek a model in which broadcast P_i is necessary in reconstructing the secret K_i, and each disenrollment is not possible without a broadcast message from the dealer.

The scheme presented above satisfies Definition 2 but *requires no broadcast from the dealer if $t+i$ participants collude*. In order for the dealer have control over each disenrollment, we suggest adding the following broadcast enforcement term:

$$I(K_i; S_{1:n}, P_{1:i-1}) = 0 \quad \text{for} \quad i = 1, ..., L. \tag{20}$$

Condition (20) states that the mutual information of K_i and all shares S_j for $j = 1...n$ and all previous broadcast message $P_1, ..., P_{i-1}$ is zero. By jointly considering (5) and (20), we note that (20) expresses the importance of broadcast message P_i at stage i: without the message, no information on the new shared secret K_i can be obtained even if all shares S_j and all previous broadcast messages $P_1, ..., P_{i-1}$ are known. Futhermore, by enforcing a broadcast message from the dealer, it allows the dealer the freedom to choose a secret to be shared when disenrolling untrustworthy participants; while in the scheme presented, all the shared secrets are predetermined before distributing shares to participants.

In [1], Barwick *et al.* used the same model defined in (5) and (7) when deriving a lower bound on the entropy of broadcast. However, one of their lemmas, Lemma 2, implies the necessity of broadcast in recovering the shared secret. From now on, we use capitalized **LEMMA** to refer to the lemmas cited from [1] and [3], and **Lemma** or Lemma for our lemmas.

LEMMA 2 in [1] In a $(1, n)$ threshold scheme with L-fold disenrollment capability, let $l_1, ..., l_L$ be distinct elements of $N = \{1, ..., n\}$,

$$H(K_i | S_{l_1:l_i}, K_{0:i-1}) = H(K_i) \qquad \text{for} \qquad i = 1, ..., L. \tag{21}$$

They claim that (21) holds regardless of $S_{l_1:l_i}$ being valid or not. We will show in the following lemma for (21) to hold when at least one of $S_{l_1:l_i}$ is valid, an additional condition that suggests the importance of broadcast message needs to be satisfied.

Lemma 3 *For (21) to hold for the case in which at least one of the shares $\{S_{l_1}, ..., S_{l_i}\}$ is valid at stage i, a necessary and sufficient condition is*

$$I(K_i; P_{1:i} | S_{l_1:l_i}, K_{0:i-1}) = H(K_i). \tag{22}$$

Proof:

Necessity: Since at least one of the shares $S_{l_1:l_i}$ is valid, for a $(1, n)$ threshold scheme, we have $H(K_i|S_{l_1:l_i}, P_{1:i}) = 0$ from (5), and thus $H(K_i|S_{l_1:l_i}, P_{1:i}, K_{0:i-1}) = 0$.

$$\begin{aligned} H(K_i) &= H(K_i|S_{l_1:l_i}, K_{0:i-1}) \\ &= H(K_i|S_{l_1:l_i}, K_{0:i-1}) - H(K_i|S_{l_1:l_i}, P_{1:i}, K_{0:i-1}) \\ &= I(K_i; P_{1:i}|S_{l_1:l_i}, K_{0:i-1}) \end{aligned} \tag{23}$$

Sufficiency:

$$\begin{aligned} H(K_i) &= I(K_i; P_{1:i}|S_{l_1:l_i}, K_{0:i-1}) \\ &= H(K_i|S_{l_1:l_i}, K_{0:i-1}) - H(K_i|S_{l_1:l_i}, P_{1:i}, K_{0:i-1}) \\ &\leq H(K_i|S_{l_1:l_i}, K_{0:i-1}) \end{aligned}$$

Since $H(K_i) \geq H(K_i|S_{l_1:l_i}, K_{0:i-1})$, we obtain that $H(K_i) = H(K_i|S_{l_1:l_i}, K_{0:i-1})$. ■

Condition (22) emphasizes the importance of broadcast messages, i.e., even with the knowledge of enough valid shares and all previous shared secrets, *broadcast messages up to now are needed in deciphering the current shared secret.* In fact, the proposed term (20) is a sufficient condition for **LEMMA 2** as shown in the following lemma.

Lemma 4 *Condition (20) is a sufficient condition for (21), where $l_i \in N$ for $i = 1, ..., L$.*

Proof:

$$\begin{aligned} H(K_i|S_{l_1:l_i}, K_{0:i-1}) &\geq H(K_i|S_{1:n}, K_{0:i-1}, P_{0:i-1}) \\ &= H(K_i|S_{1:n}, P_{0:i-1}) + I(K_i; K_{0:i-1}|S_{1:n}, P_{0:i-1}) \\ &= H(K_i|S_{1:n}, P_{0:i-1}) + H(K_{0:i-1}|S_{1:n}, P_{0:i-1}) - H(K_{0:i-1}|S_{1:n}, P_{0:i-1}, K_i) \\ &\overset{(a)}{=} H(K_i|S_{1:n}, P_{0:i-1}) \\ &= H(K_i) - I(K_i; S_{1:n}, P_{0:i-1}) \\ &\overset{(b)}{=} H(K_i) \end{aligned}$$

■

Equation (a) holds because of (5), and Equation (b) holds due to the broadcast enforcement term (20). Since $H(K_i|S_{l_1:l_i}, K_{0:i-1}) \leq H(K_i)$, it follows that (21) holds.

We will address how the broadcast enforcement term (20) affects the previously derived lower bounds on the broadcast size. Adding (20) to the definition only puts additional constraints on requiring broadcast at each disenrollment, and hence it will not affect the lower bounds on the share size.

4 Lower Bounds on Broadcast Entropy

In this section, we will establish lower bounds on the entropy of broadcast in a perfect threshold scheme with disenrollment satisfying (5), (7) and (20). We consider two cases, (i) no constraints on the share size; (ii) the size of each share achieves its lower bound (11), i.e., share minimal perfect threshold schemes with disenrollment.

Theorem 3 *Let $S_{1:n}, P_{1:L}, K_{0:L}$ form a perfect (t,n) threshold scheme with L-fold disenrollment capability satisfying properties (5), (7) and (20), and $H(K_i) = m$ for $i = 0, 1, ..., L$, then*

$$H(P_i) \geq H(K_i) = m \qquad i = 1, ..., L. \tag{24}$$

Proof:

$$\begin{aligned} H(P_i) &\overset{(a)}{\geq} H(P_i|S_{1:n}, P_{1:i-1}) \\ &\overset{(b)}{\geq} H(P_i|S_{1:n}, P_{1:i-1}) - H(P_i|S_{1:n}, P_{1:i-1}, K_i) \\ &\overset{(c)}{=} I(P_i; K_i|S_{1:n}, P_{1:i-1}) \\ &\overset{(d)}{=} H(K_i|S_{1:n}, P_{1:i-1}) - H(K_i|S_{1:n}, P_{1:i-1}, P_i) \\ &\overset{(e)}{=} H(K_i|S_{1:n}, P_{1:i-1}) \\ &\overset{(f)}{=} H(K_i) - I(K_i; S_{1:n}, P_{1:i-1}) \\ &\overset{(g)}{=} H(K_i) = m. \end{aligned}$$

Inequality (a) comes from the fact that conditioning reduces entropy. Inequality (b) holds due to non-negativity of entropy. Equations (c), (d) and (f) follow from the definition of mutual information. The second term of (d) is zero due to (5), so Equation (e) follows. Equation (g) holds from property (20). ■

Theorem 3 is the main result of our previous paper [10]. It shows that the entropy of a broadcast message is at least that of the shared secret for all updates. The same result is mentioned in [1] for the original threshold scheme with disenrollment model, but without rigorous proof.

Now we consider share minimal perfect threshold schemes with L-fold disenrollment, i.e., the case in which $H(S_j) = (L+1)m$ for $j = 1, .., n$. It will be proven for this case,

$$H(P_i) \geq \min(i+1, n-i-t+1)m \qquad i = 1, ..., L. \tag{25}$$

if all previous broadcast messages P_l's sastify their lower bounds $\min(l+1, n-l-t+1)m$ for $l = 1, .., i-1$.

In order to establish the bound (25), we first prove some lemmas as follows.

Lemma 5 *In a $(1,n)$ share minimal perfect threshold scheme with L-fold disenrollment, any $i+1$ subshares $S^{(i)}_{l_1}, ..., S^{(i)}_{l_{i+1}}$ are independent.*

Proof: A $(1,n)$ perfect threshold scheme with disenrollment satisfies the following two equations in terms of subshares.

$$H(K_i|S^{(i)}_{v_1}, P_{1:i}) = 0 \tag{26}$$

$$H(K_i|S^{(i)}_{d_1:d_i}, P_{1:i}) = H(K_i) = m \tag{27}$$

where (26) is from (8) and (27) is obtained from (7).

Substituting $X = K_i$, $Y = S^{(i)}_{v_1}$, $Z = S^{(i)}_{d_1:d_i}$ and $W = P_{1:i}$ into Lemma 1, we have from (26), (27) and $H(S^{(i)}_j) = H(K_i)$ that

$$I(S^{(i)}_{v_1}; S^{(i)}_{d_1}, ..., S^{(i)}_{d_i}) = 0. \tag{28}$$

We now prove the independence between subshares by contradiction.

Assume there is one set of $i+1$ subshares $\{S_{l_1}^{(i)}, ..., S_{l_{i+1}}^{(i)}\}$ that are not independent. That is, in $\{S_{l_1}^{(i)}, ..., S_{l_{i+1}}^{(i)}\}$, there is at least one subshare that is not independent of the rest i subshares. Without loss of generality, we assume that $S_{l_1}^{(i)}$ is dependent on $S_{l_2}^{(i)}, ..., S_{l_{i+1}}^{(i)}$

$$I(S_{l_1}^{(i)}; S_{l_2}^{(i)}, ..., S_{l_{i+1}}^{(i)}) > 0 \tag{29}$$

However, if $\{l_2, ..., l_{i+1}\} = \{d_1, .., d_i\}$, these subshares fail to form a valid $(1, n)$ threshold scheme with L-fold disenrollment since (29) contradicts with (28).

In order to be able to disenroll any i participants while maintaining the threshold at stage i, any $i+1$ subshares $S_{l_1}^{(i)}, ..., S_{l_{i+1}}^{(i)}$ have to be independent. ■

Lemma 6 *In a $(1, n)$ share minimal perfect threshold scheme with L-fold disenrollment,*

$$H(P_i) \geq \min(i+1, n-i)m, \tag{30}$$

if all previous broadcast messages meet their lower bound on entropy, i.e., $H(P_w) = \min(w+1, n-w)$ for $w = 0, ..., i-1$. When $H(P_i)$ achieves its minimum at $(i+1, n-i)m$, then $I(P_i; S_j^{(l)}) = 0$ for $l = i+1, ..., L$ and $j = 1, ..., n$, i.e., P_i is independent of subshares used to reconstruct future shared secrets.

Proof:

We will first show $H(S_{v_1:v_u}^{(i)}|K_i, P_{1:i}) = 0$, where $u = \min(i+1, n-i)$. Let S_{v_l} denote one valid share in the set $\{S_{v_1}, ..., S_{v_k}\}$.

$$\begin{aligned} H(S_{v_l}^{(i)}|P_{1:i}) &\geq I(S_{v_l}^{(i)}; K_i|P_{1:i}) \\ &= H(K_i|S_{v_l}^{(i)}) - H(K_i|S_{v_l}^{(i)}, P_{1:i}) \\ &= H(K_i) = m \end{aligned}$$

Since $H(S_{v_l}^{(i)}|P_{1:i}) \leq H(S_{v_l}^{(i)}) = m$, we have $H(S_{v_l}|P_{1:i}) = m$. From (27), we obtain $H(K_i|P_{1:i}) = H(K_i) = m$. By letting $X = K_i$, $Y = S_{v_l}^{(i)}$ and $Z = P_{1:i}$ and applying Lemma 2, we obtain $H(S_{v_l}^{(i)}|K_i, P_{1:i}) = 0$.

$$0 \leq H(S_{v_1:v_u}^{(i)}|K_i, P_{1:i}) \leq \sum_{l=1}^{u} H(S_{v_l}^{(i)}|K_i, P_{1:i}) = 0 \tag{31}$$

Therefore, $H(S_{v_1:v_u}^{(i)}|K_i, P_{1:i}) = 0$.

Then we will prove the lower bound of $H(P_i)$ by induction.

At stage $k = 1$, there are $n-1$ valid participants, $u = \min(k+1, n-k) = \min(2, n-1)$

$$\begin{aligned} H(P_1) &\geq I(P_i; S_{v_1:v_u}^{(1)}|K_1) \\ &= H(S_{v_1:v_u}^{(1)}|K_1) - H(S_{v_1:v_u}^{(1)}|K_1, P_1) \\ &\overset{(a)}{=} H(S_{v_1:v_u}^{(1)}, K_1) - H(K_1) \\ &= H(S_{v_1:v_u}^{(1)}) + H(K_1|S_{v_1:v_u}^{(1)}) - H(K_1) \\ &\overset{(b)}{=} H(S_{v_1:v_u}^{(1)}) + H(K_1) - H(K_1) \end{aligned}$$

$$\begin{aligned} & \stackrel{(c)}{=} \sum_{l=1}^{u} H(S_{v_l}^{(1)}) \\ & = um = \min(2, n-1)m \end{aligned}$$

Equation (a) holds because $H(S_{v_1:v_u}^{(1)}|K_1, P_1) = 0$. Without P_1, $H(K_1|S_{v_1:v_u}^{(1)}) = H(K_1)$ and hence (b) holds. Equation (c) holds due to the independence of $S_{v_l}^{(i)}$'s for $l = 1, ..., i+1$ shown in Lemma 5.

Now we show if $H(P_1) = \min(2, n-1)m$, then $I(P_1; S_j^{(l)}) = 0$ for $l = 2, ..., L$ and $j = 1, ..., n$.

$$\begin{aligned} H(P_1) &\geq I(P_1; S_j^{(l)}, K_1, S_{v_1:v_u}^{(1)}) \\ &\geq I(P_1; S_j^{(l)}) + I(P_i; S_{v_1:v_u}^{(1)}|K_1, S_j^{(l)}) \\ &= I(P_1; S_j^{(l)}) + H(S_{v_1:v_u}^{(1)}|K_1, S_j^{(l)}) - H(S_{v_1:v_u}^{(1)}|K_1, P_1, S_j^{(l)}) \\ &= I(P_1; S_j^{(l)}) + H(S_{v_1:v_u}^{(1)}|S_j^{(l)}) + H(K_1|S_j^{(l)}) - H(K_1) \\ &\stackrel{(d)}{=} I(P_1; S_j^{(l)}) + H(S_{v_1:v_u}^{(1)}) \\ &= I(P_1; S_j^{(l)}) + \min(2, n-1)m \end{aligned}$$

Equation (d) holds because of independence of subshares of one participant and condition (20). From $H(P_1) \geq I(P_1; S_j^{(l)}) + \min(2, n-1)m$, a necessary condition for $H(P_1)$ to achieve its lower bound is $I(P_1; S_j^{(l)}) = 0$ for $l = 2, ..., L$.

Assume Lemma 6 is true for stage $k = i-1$, i.e., $H(P_{i-1}) \geq \min(i, n-i+1)m$ if all previous broadcast messages reach their lower bound on entropy, i.e., $H(P_w) = \min(w+1, n-w)$ for $w = 0, ..., i-2$, and $I(P_{i-1}; S_j^{(l)}) = 0$ for $l = i, ..., L$.

When $k = i$, $u = \min(k+1, n-i) = \min(i+1, n-i)$

$$\begin{aligned} H(P_i) &\geq I(P_i; S_{v_1:v_u}^{(i)}|K_i, P_{1:i-1}) \\ &= H(S_{v_1:v_u}^{(i)}|K_i, P_{1:i-1}) - H(S_{v_1:v_u}^{(i)}|K_i, P_{1:i}) \\ &= H(S_{v_1:v_u}^{(i)}, K_i|P_{1:i-1}) - H(K_i|P_{1:i-1}) \\ &= H(S_{v_1:v_u}^{(i)}|P_{1:i-1}) + H(K_i|S_{v_1:v_u}^{(i)}, P_{1:i-1}) - H(K_i|P_{1:i-1}) \\ &= H(S_{v_1:v_u}^{(i)}|P_{1:i-1}) + H(K_i) - H(K_i) \\ &= H(S_{v_1:v_u}^{(i)}|P_{1:i-1}) \\ &= H(S_{v_1:v_u}^{(i)}) \\ &= um = \min(i+1, n-i)m \end{aligned}$$

The proof of $I(P_i; S_j^{(l)}) = 0$ for $l = i+1, ..., L$ when $H(P_i)$ achieves its minimum at $(i+1, n-i)m$ is similar to the base case ($k = 1$) and thus is omitted. ■

Now we can establish the lower bound of $H(P_i)$ for a share minimal perfect threshold scheme with disenrollment.

Theorem 4 *Let $S_{1:n}, P_{1:L}, K_{0:L}$ form a share minimal perfect (t, n) threshold scheme with L-fold disenrollment capability satisfying properties (5), (7), (11) and (20), then*

$$H(P_i) \geq \min(i+1, n-i-t+1)m \qquad i = 1, ..., L. \tag{32}$$

if all previous broadcast messages P_l's for $l = 1, .., i-1$ achieve their lower bounds as $\min(l+1, n-l-t+1)m$.

Proof:

As shown in [1], if $\{S_{1:n}, P_{1:L}, K_{0:L}\}$ form a (t, n) share minimal perfect threshold scheme with L-fold disenrollment capability, then $\{S_{l_1:l_{n-t+1}}|S_{v_1:v_{t-1}}, P_{1:L}|S_{v_1:v_{t-1}}, K_{0:L}|S_{v_1:v_{t-1}}\}$ form a $(1, n-t+1)$ share minimal perfect threshold scheme with L-fold disenrollment capability, where $|$ denote "conditioned on" and $\{l_1, ..., l_{n-t+1}\} = N\backslash\{v_1, ..., v_{t-1}\}$ For the $(1, n-t+1)$ threshold scheme with disenrollment, we have $H(P_i|S_{v_1:v_k}) \geq \min(i+1, n-t+1-i)m$ from Lemma 6, if all previous broadcast messages meet their lower bound on their entropy.

Since $H(P_i) \geq H(P_i|S_{v_1:v_k})$, then

$$H(P_i) \geq \min(i+1, n-t+1-i)m.$$

Therefore, Theorem 4 holds. ■

Comparing Theorem 2 and Theorem 4, we notice that when adding (20) into the definition to ensure the dealer to have control over disenrollment, the lower bound on broadcast size is different from (12) as expected.

5 Conclusions and An Open Problem

During the process of examining the conjecture on the lower bound of broadcast entropy [3], we found that the original model of threshold schemes with disenrollment [3] is inadequate to ensure the dealer of the control over each disenrollment. We presented a broadcast enforced model which ensures that the public broadcast from the dealer is required for disenrollment, by adding an additional term to the original definition. We showed that in related previous work to establish a lower bound on broadcast size [1], though the original model is used, the validity of **LEMMA 2** does require the broadcast from the dealer. In the new model, the coalition of any number of participants is unable to reconstruct the shared secret K_i before the i^{th} disenrollment stage. We also derived lower bounds on the entropy of broadcast messages in such a model, which are refined from the bound obtained in [1].

There is an open problem with threshold scheme with disenrollment. Consider the following schemes.

Scheme 1

- Participant j has share $S_j = \{S_j^{(0)}, S_j^{(1)}, ..., S_j^{(L)}\}$, where $S_j^{(i)}$ is a share of a $(t+i, n)$ ideal perfect threshold scheme sharing $K_i + R_i$ with R_i being a string of length m chosen by the dealer.
- At update i, the dealer broadcasts $P_i = \{R_i, S_{d_1}^{(i)}, ..., S_{d_i}^{(i)}\}$.

This scheme satisfies (5), (7) and (20) and achieves the lower bound (32) in Theorem 4 if $L < \lfloor \frac{n-t}{2} \rfloor$. But if $t+L$ participants collude in advance, then they can construct $K_0 + R_0, ..., K_L + R_L$. Under this construction, dealer looses the ability to disenroll a participant of its choice. The best the dealer can do is to delay broadcast and hence the reconstruction of the shared secrets! Therefore, there are schemes that satisfy all the properties including the broadcast requirement and still do not allow dealer to have no control over the disenrollment process. At first it might appear as the problem with the setup of the original model in [3].

We now present a model attributed to Brickell and Stinson in [3] and show that it is possible to construct schemes that allow dealer to have full control over the disenrollment with (5), (7) and (20).

Scheme 2 Brickell-Stinson's Scheme [3]

- The share held by participant j is $S_j = \{S_j^{(0)}, R_j^{(1)}, ..., R_j^{(L)}\}$ where $R_j^{(i)}$ denotes encryption/decryption key of m bits for participant j at disenrollment stage i.
- At stage i, the dealer updates only valid participants with new shares, so $P_i = \{S_{v_1}^{(i)} + R_{v_1}^{(i)}, ..., S_{v_{n-i}}^{(i)} + R_{v_{n-i}}^{(i)}\}$.

This scheme prevents a coalition of any number of participants from obtaining any shared secrets as long as the dealer does not update those colluded participants with new shares.

From the above observation, we note that the predistribution of multiple shares can lead to unwanted key exposure. Finding alternate models that allow more control to the dealer remains an open problem. [1]

Appendix

In the appendix, we present a correct proof to **LEMMA 5** in [3].

LEMMA 5 in [3] Let $S_{1:n}, P_{1:L}, K_{0:L}$ be a perfect (t, n) threshold scheme with L-fold disenrollment capability,

$$I(K_i; S_{v_1:v_k}, S_{d_1:d_i}, P_{1:i}, K_{0:i}) = 0 \quad \text{for} \quad k \leq t-1. \tag{33}$$

In the original proof of **LEMMA 5** in [3], they made use of (5), which holds for only $k \geq t$.

Proof:

Let us consider $k = t-1$ first. At stage $w = 0, ..., i-1$, $t-1$ valid shares plus S_{d_i} which was also valid at stage w suffice to recover K_w, i.e.,

$$H(K_w | S_{v_1:v_{t-1}}, S_{d_1:d_i}, P_{1:i}) = 0 \quad \text{for} \quad w = 0, ..., i-1, \tag{34}$$

which is a necessary condition for (7).

$$\begin{aligned}
& I(K_i; S_{v_1:v_{t-1}}, S_{d_1:d_i}, P_{1:i}, K_{0:i-1}) \\
&= I(K_i; S_{v_1:v_{t-1}}, S_{d_1:d_i}, P_{1:i}) + \sum_{w=0}^{i-1} I(K_i; K_w | S_{v_1:v_{t-1}}, S_{d_1:d_i}, P_{1:i}, K_{0:w-1}) \\
&= H(K_i) - H(K_i | S_{v_1:v_{t-1}}, S_{d_1:d_i}, P_{1:i}) \\
&\quad + \sum_{w=0}^{i-1} [H(K_w | S_{v_1:v_{t-1}}, S_{d_1:d_i}, P_{1:i}, K_{0:w-1}) - H(K_w | S_{v_1:v_{t-1}}, S_{d_1:d_i}, P_{1:i}, K_{0:w-1}, K_i)] \\
&\overset{(a)}{=} 0.
\end{aligned}$$

Equation (a) holds because of (7) and (34).

[1] We are currently working on this open problem and progress will be reported in a journal paper.

For $k < t-1$,

$$0 \leq I(K_i; S_{v_1:v_k}, S_{d_1:d_i}, P_{1:i}, K_{0:i-1}) \leq I(K_i; S_{v_1:v_{t-1}}, S_{d_1:d_i}, P_{1:i}, K_{0:i-1}) = 0$$

Therefore, **LEMMA 5** holds for $k \leq t-1$. ■

References

[1] S. G .Barwick, W. A. Jackson, K. M. Martin, and P .R. Wild, "Size of broadcast in threshold schemes with disenrollment," *ACISP 2002, Lecture Notes in Computer Science 2384*, pp. 71-88, 2002.

[2] G. R. Blakley, "Safeguarding cryptographic keys," *Proceedings AFIPS 1979 National Computer Conference*, pp. 313-317, 1979.

[3] B. Blakley, G. R. Blakley, A. H. Chan, and J. Massey, "Threshold schemes with disenrollment," *Advances in Cryptology – CRYPTO'92, E. F. Brickell, ed., Lecture Notes in Computer Science* vol. 740, pp. 540-548, 1993.

[4] C. Blundo, A. Cresti, A. De Santis, U. Vaccaro, "Fully dynamic secret sharing schemes," *Advances in Cryptology – CRYPTO '93, D. R. Stinson, ed., Lecture Notes in Computer Science*, vol. 773, pp. 110-125, 1994.

[5] C. Blundo, "A note on dynamic threshold schemes," *Information Processing Letters*, vol. 55, pp. 189-193, August 1995.

[6] C. Charnes, J. Pieprzyk, and R. Safavi-Naini, "Conditionally secure secret sharing schemes with disenrollment capability," *Proceedings of the 2nd ACM Conference on Computer and communications security*, pp. 89-95, 1994.

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

[8] Y. Desmedt and S. Jajodia, "Redistributing secret shares to new access structures and its application," *Technical Report ISSE TR-97-01*, George Mason University, July 1997

[9] A. Herzberg, S. Jarecki, H. Krawczyk, M. Yung, "Proactive secret sharing or: How to cope with perpetual leakage", *Advances in Cryptology – CRYPTO'95, Lecture Notes in Computer Science* vol. 963, Springer Verlag, pp. 339–352, 1995.

[10] M. Li and R. Poovendran, "A note on threshold schemes with disenrollment," *Proceedings of 37th annual Conference on Information Sciences and Systems (CISS)*, John Hopkins University, March 2003.

[11] K. M. Martin, "Untrustworthy participants in perfect secret sharing schemes," *Cryptography and Coding III*, M. J. Ganley, ed., Oxford University Press, pp. 255-264, 1993.

[12] K. M. Martin, J. Nakahara Jr, "Weakness of protocols for updating the parameters of an established threshold scheme," *IEE Proceedings Computers and Digital Techniques*, Vol. 148, No. 1, pp. 45-48, 2001.

[13] E. D. Karnin, J. W. Greene and M. E. Hellman, "On secret sharing systems," *IEEE Transactions on Information Theory*, vol. 29, pp. 35-41, 1983.

[14] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, pp. 612-613, 1979

[15] D. R. Stinson, "An explication of shared secret sharing schemes," *Design, Codes and Cryptography*, vol. 2, pp. 357-390, 1992

[16] D. R. Stinson, R. Wei, "Bibliography on secret sharing schemes," [Online], Available: http://cacr.math.uwaterloo.ca/ dstinson/ssbib.html.

[17] U. Tamura, M. Tada, and E. Okamoto, "Update of access structure in Shamire's (k, n) threshold scheme," *Proceedings of the 1999 symposium on cryptography and information security*, January 1999, pp. 26-29