A Note on Threshold Schemes with Disenrollment

Mingyan Li and Radha Poovendran[1]
Department of Electrical Engineering
University of Washington
e-mail:myli, radha@ee.washington.edu

Abstract — **Blakley, Blakley, Chan and Massey conjectured a lower bound on the entropy of public broadcast in a threshold scheme with disenrollment capability. In this paper, we first show that the conjecture need not be true in general. Then we establish a tight lower bound on the entropy of public information by introducing one property to the definition of threshold schemes with disenrollment. We also present a scheme that achieves the lower bound.**

Keywords: secret sharing, threshold schemes

I. Introduction

A (t, n) *threshold scheme* allows a secret to be distributed among a group of n participants in such a way that t or more participants can construct the secret by pooling their shares, but the secret remains undetermined to $(t-1)$ or fewer participants. Threshold schemes are useful in applications that require the shared control of a secret among multiple parties, for example, threshold encryption and signature. They also find direct application when protection against the loss of several shares is needed, for example, file sharing.

Shamir [9] and Blakley [2] have introduced and constructed threshold schemes independently. Since then, threshold schemes have been generalized to secret sharing schemes and attracted a great amount of research attention. An excellent survey on secret sharing can be found in [10], and a bibliography is provided online in [11]. Martin [7] considered the problem of managing a secret sharing scheme when a participant becomes untrustworthy. When a member is no longer trustworthy, the share held by that participant has to be assumed disclosed. The disclosure or the loss of one share decreases the threshold size t by 1, because $(t-1)$ shares plus the disclosed share can decrypt the secret. To keep the same level of secrecy in terms of threshold size, new shares have to be constructed, and the shared secret among the group has to be updated. The property of maintaining the same threshold in case of loss or disclosure of shares is known as *disenrollment capability*.

Blakley, Blakley, Chan, and Massey [3] are the first group who defined the disenrollment capability. In their model, the shares of a threshold scheme are issued securely by a trusted third party, *dealer*, to participants on initialization. They considered threshold schemes that allow disenrolling L members, one at a time, through an insecure public channel. They derived a lower bound on the size of the shares held by each participant in such a scheme. A conjecture on the lower bound of the public broadcast size was also proposed. In this paper, we will address the conjecture.

The paper is organized as follows: in section II, we review the definition of threshold schemes with disenrollment capability in an information theoretic approach given by [3]. We provide a different approach to establish the lower bound on the size of the shares. In section III, we show by two examples that the conjecture on the entropy of broadcast messages need not be valid. In section IV, we derive a lower bound on the size of broadcast messages by adding one property to the definition. We also give a construction that achieves the lower bound. Main contributions of this paper are summarized in section V.

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

II. Threshold Schemes with Disenrollment Capability

In this section, we review and revise the definition of threshold schemes with disenrollment given in [3], by noting that the original definition is incomplete. We also present an alternative approach to establish the lower bound on the share entropy. For consistency and ease of understanding, we will use the same notations as those in the original paper. $H(\cdot)$ indicates Shannon entropy [6].

Definition 1 *A (t, n) threshold scheme is a sharing of a secret K among n participants, and participant j $(1 \le j \le n)$ holds share S_j, so that for any set of k indices $\{l_1, l_2, ..., l_k\}$*

$$H(K|S_{l_1}, S_{l_2}, ..., S_{l_k}) = 0 \quad for \quad t \le k \le n \tag{1}$$

$$H(K|S_{l_1}, S_{l_2}, ..., S_{l_k}) > 0 \quad for \quad k < t. \tag{2}$$

In a (t, n) threshold scheme, the secret K is recoverable from t or more shares based on condition (1), but the secret remains uncertain even with the knowledge of $(t-1)$ shares according to (2) . The secret K and the shares S_j take values in the secret space $\mathcal{K}$ and the shares space $\mathcal{S}$, respectively. If $(t-1)$ or fewer shares reveal absolutely no information on the secret K, then the threshold scheme is said to be *perfect* in Shannon information theoretic sense.

A (t, n) threshold scheme is called *perfect* provided that

$$H(K|S_{l_1}, S_{l_2}, ..., S_{l_k}) = H(K) \quad \text{for} \quad k < t. \tag{3}$$

It has been shown in [8] that a necessary condition to have a perfect threshold scheme is

$$H(S_j) \ge H(K) \qquad \text{for} \qquad j = 1, 2, ..., n. \tag{4}$$

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

A (t, n) threshold scheme with L-fold disenrollment capability defined in [3] is (i) initially (i.e., at stage $i = 0$) a (t, n) threshold scheme that shares a secret K_0 among n participants (ii) able to disenroll a member at each update stage i $(i = 1, 2, ..., L)$ by updating the shared secret K_{i-1} to K_i through a broadcast message P_i. Let S_j denote the share held by participant j over the entire L updates.Without loss of generality, Blakley *et al* assume that participant i is disenrolled at the ith disenrollment and S_i corresponds to the share that is invalidated at the ith update.

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 $j = 1, 2, .., n$, shared secrets K_i for $i = 0, 1, ..., L$, and public broadcast messges P_l for $l = 1, 2, ..., L$, that satisfies the following conditions:*

$$H(K_i|\Delta_i(k), P_1, ..., P_i) = 0 \quad \text{for} \quad t \leq k \leq n - i \tag{5}$$

$$H(K_i|\Delta_i(k), P_1, ..., P_i, S_1, ..., S_i, K_0, ..., K_{i-1}) > 0 \quad \text{for} \quad k < t, \tag{6}$$

where $\Delta_i(k) = \{S_{i_1}, ..., S_{i_k}\} \subseteq \{S_{i+1}, ..., S_n\}$ with $k \leq n - i$. That is, $\Delta_i(k)$ is any set of k remaining valid shares at the ith disenrollment step.

Condition (5) requires that the key K_i can be solved by at least t shares from valid participants and broadcast messages $P_1, ..., P_i$. Condition (6) states that, given all broadcast information $P_1, ..., P_i$, all disenrolled shares $S_1, ..., S_i$ and all past keys $K_0, ..., K_{i-1}$, the secret key K_i is still unsolvable if the number of shares available is less than t. Note that condition (6) is different from the original definition in [3], which gave the condition as

$$H(K_i|\Delta_i(k), P_1, ..., P_i, S_1, ..., S_i) > 0 \qquad \text{for} \qquad k < t \tag{7}$$

Condition (6) is stronger than the original condition (7) because (6) requires $(t-1)$ shares plus all disenrolled shares are not sufficient to determine the new key K_i even if all the previous secrets $K_0, .., K_{i-1}$ are given. The reason we use (6) instead of (7) is that Blundo [4] has shown that the stronger condition (6) is necessary in deriving a lower bound on the entropy of the shares obtained in [3], and also it is a necessary condition to prove Lemma 5 in [3].

A (t, n) threshold scheme with L-fold capability is said to be *perfect* if

$$H(K_i|\Delta_i(k), P_1, ..., P_i, S_1, ..., S_i, K_0, ..., K_{i-1}) = H(K_i) \quad \text{for} \quad k < t. \tag{8}$$

From Definition 2, 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. Each participant must have a component in his share corresponding to K_i. Let $S_j^{(i)}$ denote the component held by participant j corresponding to K_i, and we call $S_j^{(i)}$ a *subshare* of participant j. S_j can be regarded as the union of all its subshares over L disenrollment stages, i.e., $S_j = \{S_j^{(0)}, S_j^{(1)}, ..., S_j^{(L)}\}$. We establish the independence of all the subshares held by one participant in the following lemma.

Lemma 1 *In a perfect (t, n) threshold scheme with L-fold disenrollment capability, subshares of participant j, $S_j^{(0)}, S_j^{(1)}, ..., S_j^{(L)}$ are independent.*

Proof: First we prove that the secrets K_i's for $i = 0, 1, ..., L$ are independent, i.e.,

$$H(K_0, K_1, ..., K_L) = \sum_{i=0}^{L} H(K_i). \tag{9}$$

$$\begin{aligned} H(K_0, K_1, ..., K_L) &\overset{(a)}{=} H(K_0) + \sum_{i=1}^{L} H(K_i|K_0, ..., K_{i-1}) \\ &\overset{(b)}{\geq} H(K_0) + \sum_{i=1}^{L} H(K_i|K_0, ..., K_{i-1}, P_1, ..., P_i, S_1, ..., S_i, \Delta_i(k)) \\ &\overset{(c)}{=} \sum_{i=0}^{L} H(K_i). \end{aligned} \tag{10}$$

Equality (a) holds because of chain rule, and inequality (b) holds from the fact that conditioning reduces entropy. Equality (c) is obtained from (8). From a known property of the entropy, we have

$$H(K_0, K_1, ..., K_L) \leq \sum_{i=0}^{L} H(K_i). \tag{11}$$

From (10) and (11), we can obtain (9), i.e., the secrets K_i's are independent.

Subshares $S_j^{(i)}$ are derived from K_i for $i = 0, ..., L$. Since the functions of independent random variables are independent, the independence between subshares $S_j^{(i)}$ for $i = 0, 1, ..., L$ thus follows. ∎

One major contribution of [3] is to establish a lower bound on the entropy of each share in a threshold scheme with disenrollment capability. The contribution is summarized in Theorem 1.

Theorem 1 *Let $S_1, ..., S_n, P_1, ..., P_L, K_0, ..., K_L$ form a perfect threshold scheme with L-fold disenrollment capability and $H(K_i) = m$ for $i = 0, 1, ..., L$. Then,*

$$H(S_j) \geq (L + 1)m \qquad \text{for} \quad j = 1, 2, ..., n. \tag{12}$$

On the observation that S_j can be regarded as the union of all its $L + 1$ subshares, we provide an alternative and simpler proof to Theorem 1.

Proof: we notice that the necessary condition in (4) can be extended to the size of subshares, i.e., we have

$$H(S_j^{(i)}) \geq H(K_i) \quad \text{for} \quad i = 0, 1, ..., L; \quad j = 1, ..., n. \tag{13}$$

Then,

$$\begin{aligned} H(S_j) &= H(S_j^{(0)}, S_j^{(1)}, ..., S_j^{(L)}) \\ &= \sum_{i=0}^{L} H(S_j^{(i)}) \\ &\geq \sum_{i=0}^{L} H(K_i) = (L + 1)m. \end{aligned}$$

The second equality follows from Lemma 1. ∎

III. Conjecture and Counterexamples

We now present and analyze the main conjecture on the lower bound for the entropy of public information in [3].

Conjecture 1 *A lower bound on the entropy of the broadcast message P_i at the ith disenrollment for $i = 1, ..., L$ is*

$$H(P_i) \geq iH(K) = im.$$

In the following, we show the size of broadcast information can be different from that given in the conjecture by two examples [7],[3].

- In [7], Martin noticed that a (t, n) threshold scheme can be constructed from a $(t + L, n)$ threshold scheme by publishing L additional shares. In Martin's threshold scheme with disenrollment capability, the share held by participant j is of the form

$$S_j = \{S_j^{(0)}, S_j^{(1)}, ..., S_j^{(L)}\}.$$

where $S_j^{(i)}$ is a share of a $(t+L, n)$ ideal perfect threshold scheme. At update stage i, i members have been disenrolled and their shares become public knowledge. In addition to the disclosed i shares, $L-i$ dummy shares are needed to be broadcasted so that with t shares collected from the group, the secret can be recovered. Therefore, the public message at stage i is the union of dummy shares as

$$P_i = \{S_{d_1}^{(i)}, S_{d_2}^{(i)}, ..., S_{d_{L-i}}^{(i)}\}.$$

The subscript d indicates that the shares are dummy shares, the superscript i indicates that they are for recovering K_i.

Claim 1 *In Martin's perfect threshold scheme with L-fold disenrollment capability, the broadcast message in the ith update phase contains* $(L-i)H(K_i) = (L-i)m$ *bits for* $i = 0, ..., L$.

The size of public messages in Martin's scheme linearly decreases with update stage i. This is an example that does not agree with the conjecture in [3]. To illustrate the difference, we consider the broadcast message at stage L. In Martin's scheme, there is no message published; but according to Conjecture 1, the length of broadcast message should be at least Lm.

- In 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 for participant j at disenrollment stage i and it is a random number of the same size as the shared key K_i. At the ith disenrollment, only $(n-i)$ valid participants need to be refreshed with new subshares. The dealer selects a new key K_i, generates the new subshares $S_j^{(i)}$ for legal members using a (t, n) perfect ideal threshold scheme, and publishes the encrypted version of new subshares as $S_j^{(i)} + R_j^{(i)}$. The broadcast message P_i is of the form

$$P_i = \{S_{i+1}^{(i)} + R_{i+1}^{(i)}, S_{i+2}^{(i)} + R_{i+2}^{(i)}, ..., S_n^{(i)} + R_n^{(i)}\}.$$

For Brickell-Stinson's scheme, $R_j^{(i)}$ with $j = 1, 2, ..., n$ are chosen independently, and we can claim the following.

Claim 2 *In Brickell-Stinson's perfect threshold scheme with L-fold disenrollment capability,*

$$H(P_i) = (n-i)H(K_i) = (n-i)m \qquad i = 1, ..., L.$$

The entropy of public information in Brickell-Stinson's scheme is decreasing with the stage i, and this violates Conjecture 1 that states the lower bound of broadcast entropy linearly increases with stage.

IV. Lower Bound on Broadcast Entropy

Having shown that the lower bound in Conjecture 1 need not hold in general, we now show that according to Definition 2 in [3], it is possible to construct a threshold scheme with disenrollment that requires no public broadcast. We also add a "correction" condition that will require a broadcast message at the time of disenrollment.

A model satisfying Definition 2 that requires no public broadcast: 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 subshare $S_j^{(i)}$ corresponds to a share of a $(t+i, n)$ threshold scheme sharing the secret K_i. At stage i, i subshares of disenrolled members plus t shares from the valid remaining participants are sufficient to decrypt K_i. Therefore, there is no need for broadcast information and the size of public information is zero in this scheme. However, the scheme is problematic. If all members collaborate by exchanging their shares, all members will decipher all K_i's at once and the disenrollment of any invalidated member is not under the control of dealer. In contrast, in Martin's scheme and Brickell-Stinson's scheme, broadcast P_i plays a role in reconstructing the secret K_i and hence the disenrollment involving update K_{i-1} to K_i at stage i is not possible without a broadcast message from the dealer.

The scheme presented above satisfies Definition 2 while requiring no broadcast. In order for the dealer to have the control over disenrollment at any stage, we suggest adding the following condition to make the definition complete: [1]

$$I(K_i; S_1, S_2, ..., S_n, P_1, ..., P_{i-1}) = 0 \quad \text{for} \quad i = 0, ...L. \quad (14)$$

where $I(\cdot)$ denotes mutual information [6]. Condition (14) states that the mutual information of K_i and all shares S_j for $j = 1...n$ and all previous broadcast message $P_1, P_2, ..., P_{i-1}$ is zero. It expresses the importance of broadcast message P_i at stage i: without the message, no information on the new key can be obtained even if all shares S_j and all previous broadcast message $P_1, P_2, ..., P_{i-1}$ are known.

With condition (14), the lower bound on the entropy of public information can be derived.

Theorem 2 *Let* $S_1, ..., S_n, P_1, ..., P_L, K_0, ..., K_L$ *form a perfect threshold scheme with L-fold disenrollment capability satisfying properties (5), (6)and (14), and* $H(K_i) = m$ *for* $i = 0, 1, ..., L$, *then*

$$H(P_i) \geq H(K_i) = m \qquad i = 1, ..., L. \quad (15)$$

Proof:

$$\begin{aligned}
H(P_i) &\overset{(a)}{\geq} H(P_i|S_1, ..., S_n, P_1, ..., P_{i-1}) \\
&\overset{(b)}{\geq} H(P_i|S_1, ..., S_n, P_1, ..., P_{i-1}) \\
&\qquad -H(P_i|S_1, ..., S_n, P_1, ...P_{i-1}, K_i) \\
&\overset{(c)}{=} I(P_i; K_i|S_1, ..., S_n, P_1, ..., P_{i-1}) \\
&\overset{(d)}{=} H(K_i|S_1, ..., S_n, P_1, ..., P_{i-1}) \\
&\qquad -H(K_i|S_1, ..., S_n, P_1, ..., P_{i-1}, P_i) \\
&\overset{(e)}{=} H(K_i|S_1, ..., S_n, P_1, ..., P_{i-1})
\end{aligned}$$

[1] Barwick *et al* also addressed the conjecture in [1], but they did not add the constraint that requires public broadcast at each disenrollment.

$$\stackrel{(f)}{=} H(K_i) - I(K_i; S_1, S_2, ..., S_n, P_1, ..., P_{i-1})$$
$$\stackrel{(g)}{=} H(K_i) = m.$$

Inequality (a) comes from the fact conditioning reduces entropy, inequality (b) holds due to nonnegativity of entropy, equalities (c) and (d) follow from the definition of mutual information. The second term of (d) is zero due to (5), so equality (e) follows. Equality (g) holds from property (14). ∎

Inequality (15) shows that the entropy of a broadcast message is at least that of the shared key for all updates.

Now we present a threshold scheme with disenrollment that is revised from Blundo's dynamic threshold scheme [5]. The difference between dynamic threshold schemes and threshold schemes with disenrollment capability is that dynamic threshold schemes do not consider disenrollment of participants but updates of the shared secret only.

- On initialization: given the keys K_i with $i = 0, ..., L$ to be shared, the dealer randomly chooses strings R_i of length $m = H(K_i)$, computes all subshares $S_j^{(i)}$ with $j = 1, ..., L$ and distributes S_j to participant j, where $S_j^{(i)}$ is a share of a $(t + i, n)$ perfect ideal threshold scheme sharing $K_i + R_i$.
- At update i, the dealer broadcasts R_i, i.e., $P_i = R_i$. A set of t shares from valid participants plus i disclosed shares suffices to recover $K_i + R_i$ and thus to decipher K_i on receiving R_i.

Claim 3 *The proposed perfect threshold scheme with L-fold disenrollment capability achieves the lower bound on share entropy in (12) and the lower bound on the entropy of broadcast in (15), i.e.,*

$$H(S_j) = (L+1)H(K_i) = (L+1)m,$$
$$H(P_i) = H(K_i) = m.$$

We have been assuming that the disenrolled shares become known to all remaining members. But if untrustworthy members do not reveal their shares to the public, the dealer needs to publish these shares in addition to R_i, and the broadcast message at stage i becomes

$$P_i = \{R_i, S_1^{(i)}, S_2^{(i)}, ..., S_i^{(i)}\}.$$

It is easy to verify that P_i contains exactly $(i + 1)H(K_i) = (i + 1)m$ bits. Namely, the size of broadcast information is directly proportional to stage i. In this case, the size of the broadcast message is close to Conjecture 1.

V. Conclusions

In this paper, we addressed a conjecture posed in [3] regarding the lower bound on the broadcast entropy for threshold schemes with disenrollment. We presented two counterexamples to show the conjecture does not hold. We identified incompleteness in the definition of threshold schemes with disenrollment in [3] and presented a correction term which ensures that the public broadcast from the dealer is required for disenrollment. We then derived the correct lower bound on the broadcast entropy.

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

[7] 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.

[8] 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.

[9] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, pp. 612-613, 197

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

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