A Note on Threshold Schemes with Disenrollment

Mingyan Li R. Poovendran

Department of Electrical Engineering,

University of Washington

Email: myli, radha@ee.washington.edu

Outline

- Threshold Schemes
- Threshold Schemes with Disenrollment
- Conjecture regarding lower bound on broadcast entropy
- Counterexamples
- Correct lower bound on broadcast entropy
- Conclusions

Threshold Scheme

- First studied by Shamir and Blakley in 1979
- Applications:
  - Secure distributed storage of a file/key etc.
  - Collective control and computation: threshold encryption and signature
- (***t,n***) **threshold scheme** : divide a secret *K* into *n* shares so that
  - knowledge of *t* (**threshold**) or more shares allows reconstruction of *K* (**availability**)
  - knowledge of *t-1* or fewer leaves *K* undetermined (**confidentiality**)

Threshold Scheme – An example

Accessing a safe:

- At least 2 people need to input their secret codes to unlock a safe
- Any 2 out of *n* authorized people can unlock
- *(2,n) threshold scheme*
- Secret codes: *shares*;
- authorized people: *participants/members*.
- A trusted third party, the *dealer*, securely distributes initial shares to participants.

Threshold Scheme

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

$$\begin{aligned} H(K|S_{l_1}, S_{l_2}, ..., S_{l_k}) &= 0 \quad t \leq k \leq n \qquad (1) \\ H(K|S_{l_1}, S_{l_2}, ..., S_{l_k}) &> 0 \quad k < t. \qquad (2) \end{aligned}$$

Threshold Scheme (Cont.)

- A (t,n) threshold scheme is called *perfect* if $H(K|S_{l_1}, S_{l_2}, ..., S_{l_k}) = H(K) \qquad k < t$

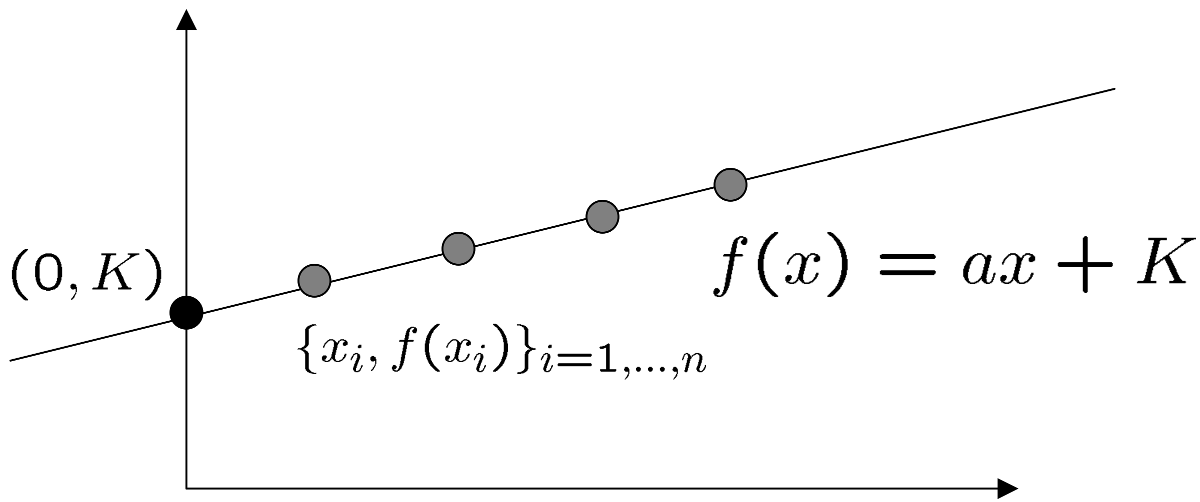
- A necessary condition to have a perfect threshold scheme (Karnin, 84)

$$H(S_j) \geq H(K) \quad j = 1, 2, ..., n$$

A perfect threshold scheme is called *ideal* if $H(S_j) = H(K)$

A (2,n) Threshold Scheme

- Select a random line through (0,*K*)



- Generalize to (*t*,*n*) threshold scheme

Shamir's Threshold Scheme

- Assume q is a large prime and the secret $K < q$.
- Randomly and uniformly choose a_i for $i = 1, .., t-1$ over finite field Z_q and construct

$$f(x) = K + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1}$$

- Share $S_j = f(j)$ for $j = 1, 2, ..., n$

Shamir's Scheme (Cont.)

- Given t shares S_j, there exists a unique polynomial $f(\cdot)$ of degree $t-1$ passing t points (j, S_j), and $K = f(0)$.
- Given $t-1$ shares, polynomial $f(\cdot)$ is undetermined. Every number from Z_q remains an equivalent candidate for the secret K.
- Shamir's sheme is an ideal perfect threshold scheme

Disenrollment

- What if a share is disclosed?
  - disclosed share becomes public knowledge
  - threshold *t* reduced by 1
- Can we **maintain the threshold *t*** when disenrolling an untrustworthy participant?
  - Select a shared key
  - Update the valid participants with new shares
- Can *t* be maintained **using broadcast channel only** from the dealer?
  - Threshold schemes with disenrollment capability (Blakley et al, 92)

Threshold Scheme with Disenrollment

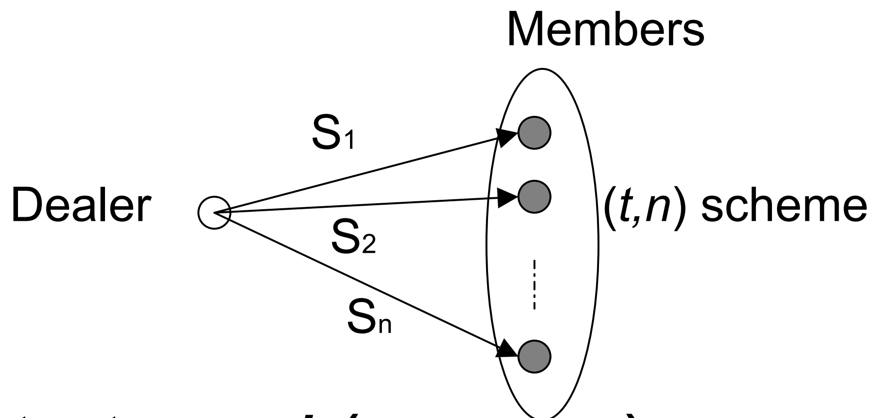
A (t, n) perfect threshold scheme with L-fold disenrollment capability is a collection of shares $\{S_j\}_{j=1\ldots n}$, shared secrets $\{K_i\}_{i=0\ldots L}$, broadcast messges $\{P_l\}_{l=1\ldots L}$, such that:

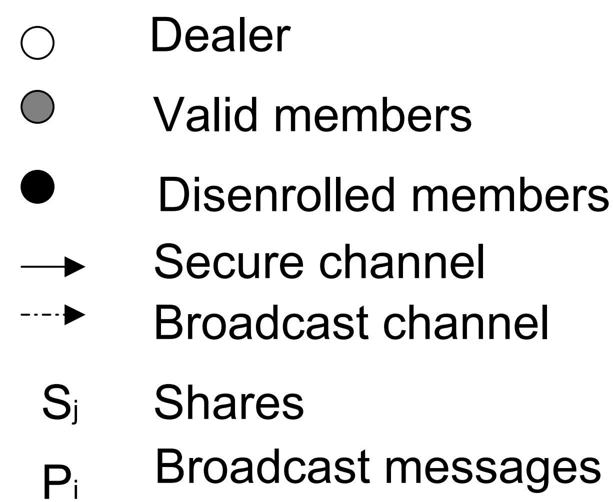
$$
\begin{aligned}
H(K_i|\Delta_i(k), P_1^i) &= 0 \quad t \le k \le n-i \\
H(K_i|\Delta_i(k), P_1^i, S_1^i, K_0^{i-1}) &= H(K_i) \quad k < t,
\end{aligned}
$$

where $\Delta_i(k)$ is any set of k remaining valid shares. w.l.o.g, S_i is disenrolled share at update stage i.

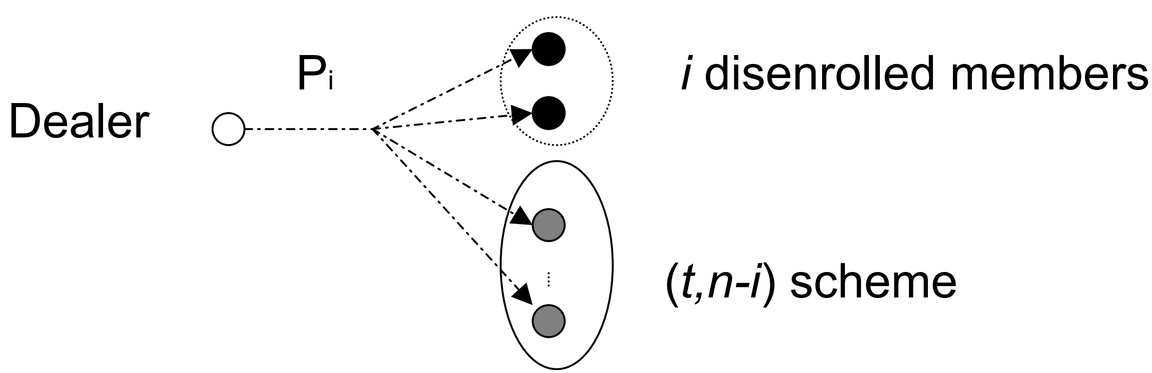
Threshold Scheme with Disenrollment (cont.)

- On initiliazation:





- At stage i (i=1,…,L)



Conjecture on Broadcast Entropy

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

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

Note that Conjecture 1 states that the lower bound of broadcast entropy linearly increases with stage.

Counterexample 1 – Brickell-Stinson scheme

In Brickell-Stinson's perfect threshold scheme (PST) with disenrollment,

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

where $R_j^{(i)}$ denotes encryption/decryption key for participant j at disenrollment stage i and $H(R^{(i)}) = H(K_i)$.

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

Counterexample 1 (Cont.)

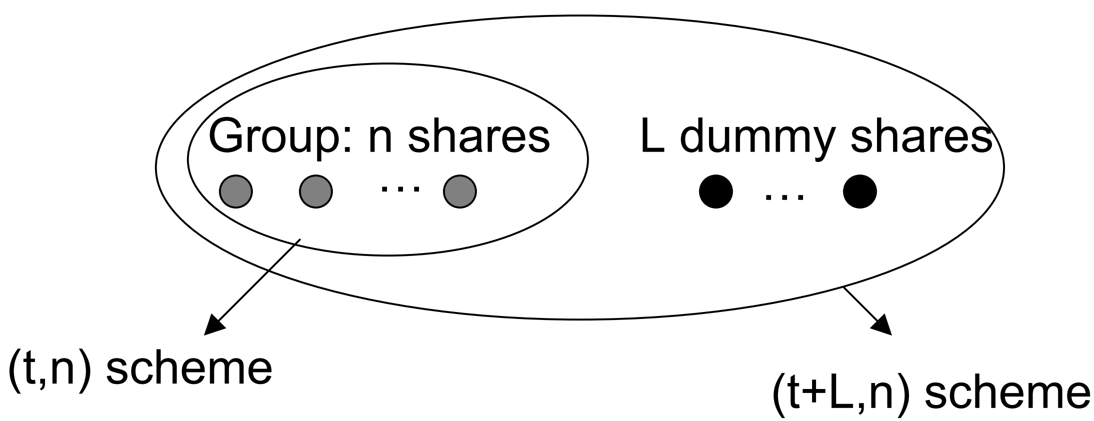
Claim 1 In Brickell-Stinson's PTS with L-fold disenrollment capability,

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

The entropy of public information in Brickell-Stinson's scheme is decreasing with stage i.

Counterexample 2 – Martin's Scheme

- Martin noticed a (t, n) threshold scheme can be constructed from a $(t + L, n)$ threshold scheme by publishing L additional shares



Counterexample 2 (Cont)

Claim 1 In Martin's threshold scheme with dis-enrollment, broadcast message P_i at stage i contains $(L-i)H(K_i) = (L-i)m$ bits

Note Broadcast size in Martin's scheme linearly decreases with update stage i

A Scheme Requiring No Broadcast

- Share $S_j = \{S_j^{(0)}, S_j^{(1)}, ..., S_j^{(L)}\}$, where $S_j^{(i)}$ is a share of a $(t+i, n)$ PTS sharing the secret K_i.
- At stage i, i shares of disenrolled members plus t shares from the remaining valid participants are sufficient to decrypt K_i.
- No need for broadcast information and the size of public information is zero!
- Problem – Disenrollment is not under the control of the dearler.

Incompleteness of Original Definition

- The scheme presented satisfies the original definition given by Blakley et al. while requiring no broadcast. It indicates *incompleteness* of the original definition.
- For the dealer to have the control over disenrollment at any stage, we suggest adding a "*correction*" condition

$$H(K_i|S_1, S_2, ..., S_n, P_1, ..., P_{i-1}) = H(K_i) \quad \forall i$$

which expresses the importance of broadcast message P_i.

Lower Bound on Broadcast Entropy

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 and $H(K_i) = m$, then

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

A Scheme Achieving Lower Bounds

- On initialization: given keys K_is, the dealer randomly chooses strings R_i of length $m = H(K_i)$, computes shares and distributes to participant j share $S_j = \{S_j^{(0)}, ..., S_j^{(L)}\}$ where $S_j^{(i)}$ is a share of a $(t+i, n)$ ideal PTS 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.

Difference between our work and Barwick et al

- Barwick et al disproved the conjecture in ACISP'02 and established the lower bound as

$$\sum_{l=1}^{i} H(P_l) \geq \sum_{l=1}^{i} \min(l, n-l-t+1) H(K)$$

- The difference

	Ours	Theirs
Assume disenrolled shares need not to be broadcasted	Yes	No
Identify the incompleteness of the original definition: disenrollment not under control	Yes	No

Contributions

- Identified incompleteness of the original definition of a threshold scheme with disenrollment and add a “correction” term
- Established a tight lower bound on the entropy of broadcast
- Constructed a scheme that achieves both lower bounds on share size and on broadcast size