Broadcast Enforced Threshold Schemes with Disenrollment

Mingyan Li   Radha Poovendran

Department of Electrical Engineering

University of Washington
Email: myli, radha@ee.washington.edu

Outline

- Threshold schemes with disenrollment
- A scheme: the dealer has no control over disenrollment
- Broadcast enforced threshold scheme with disenrollment
- Observations/Open Problems

Threshold Schemes

- First studied by Shamir and Blakley in 1979
- **(t,n) threshold scheme** : divides a secret K into n shares so that
  - knowledge of **t** (**threshold**) or more shares allows reconstruction of K
  - knowledge of t-*1* or fewer leaves K undetermined
  - called **perfect** if t-*1* or fewer shares reveal nothing about K

- Applications:
  - Secure distributed storage of a file/key etc.
  - Collective control and computation: threshold encryption and signature

Threshold Scheme – An Example

- To access a safe
  - At least 2 people need to combine their shares to have the key to the safe
  - Any 2 out of n authorized people can obtain the key
  - (2, n) threshold scheme
- Authorized people: *participants/members*
- A Trusted Third Party, (here denoted as *dealer)*,
  - securely distributes initial shares to participants
  - updates the secret and the membership in the group via broadcast

Disenrollment in Threshold Scheme

- The dealer may want to delete/remove a member
  - Its share is treated as disclosed and assumed to become public knowledge for security reasons
  - What happens to threshold? It **reduces** from t to t-1
- Can we **maintain the threshold t** when disenrolling an untrustworthy participant?
  - Need to change the shared key/secret
  - Update the valid participants with new shares
- Can t be maintained **using broadcast channel only** from the dealer?
  - Threshold schemes with disenrollment capability (Blakley, Blakley, Chan, Massey, Crypto'92)
  - Threshold schemes with L-fold disenrollment capability

Threshold Scheme with Disenrollment – A Seminal Model by Blakley *et. al.*

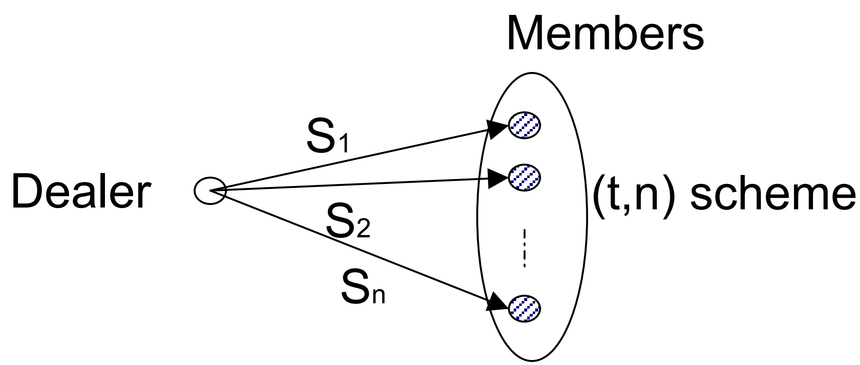
A (t, n) perfect threshold scheme with L-fold disenrollment capability is a collection of shares $S_{1:n}$, shared secrets $K_{0:L}$, broadcast messages $P_{1:L}$ that satisfies:

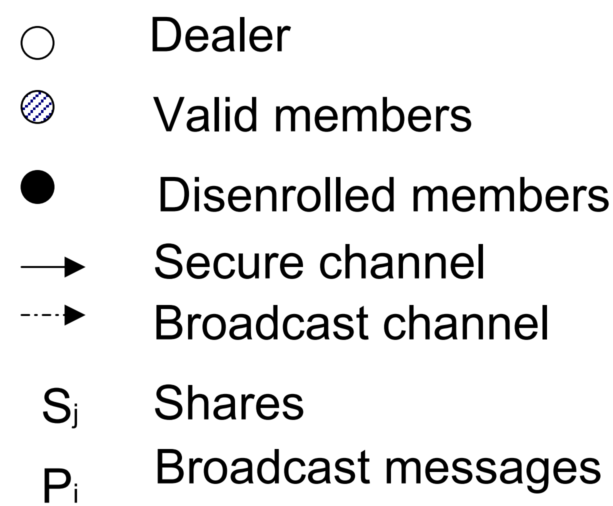
$$\begin{aligned} H(K_i \mid S_{v_1:v_k}, P_{1:i}) &= 0 \quad t \le k \le n-i \\ H(K_i \mid S_{v_1:v_k}, S_{d_1:d_i}, P_{1:i}) &= H(K_i) \quad k < t, \end{aligned}$$

where S_v, S_d denote shares of valid and disenrolled participants.

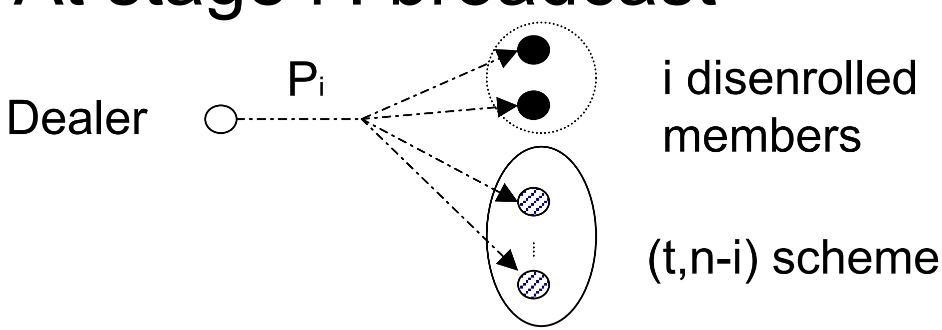
Interpretations of Disenrollment Model by Blakley *et. al.*

- On initialization: secure channel



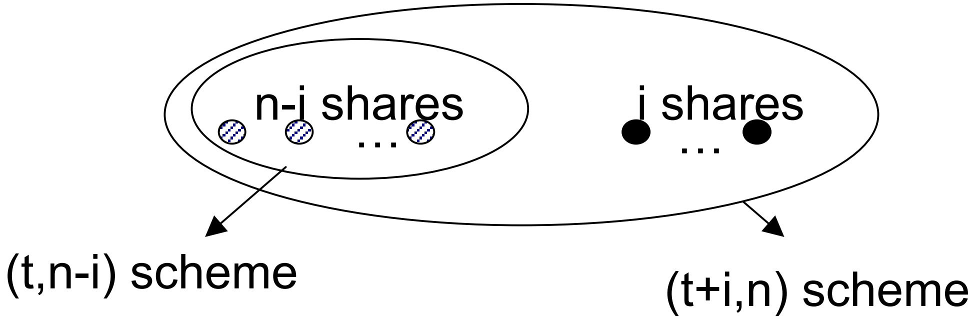


- At stage i : broadcast



A Construction Maintaining t-Threshold under Disenrollment

- A (t, n-i) threshold scheme can be constructed from a (t+i, n) threshold scheme by publishing i shares



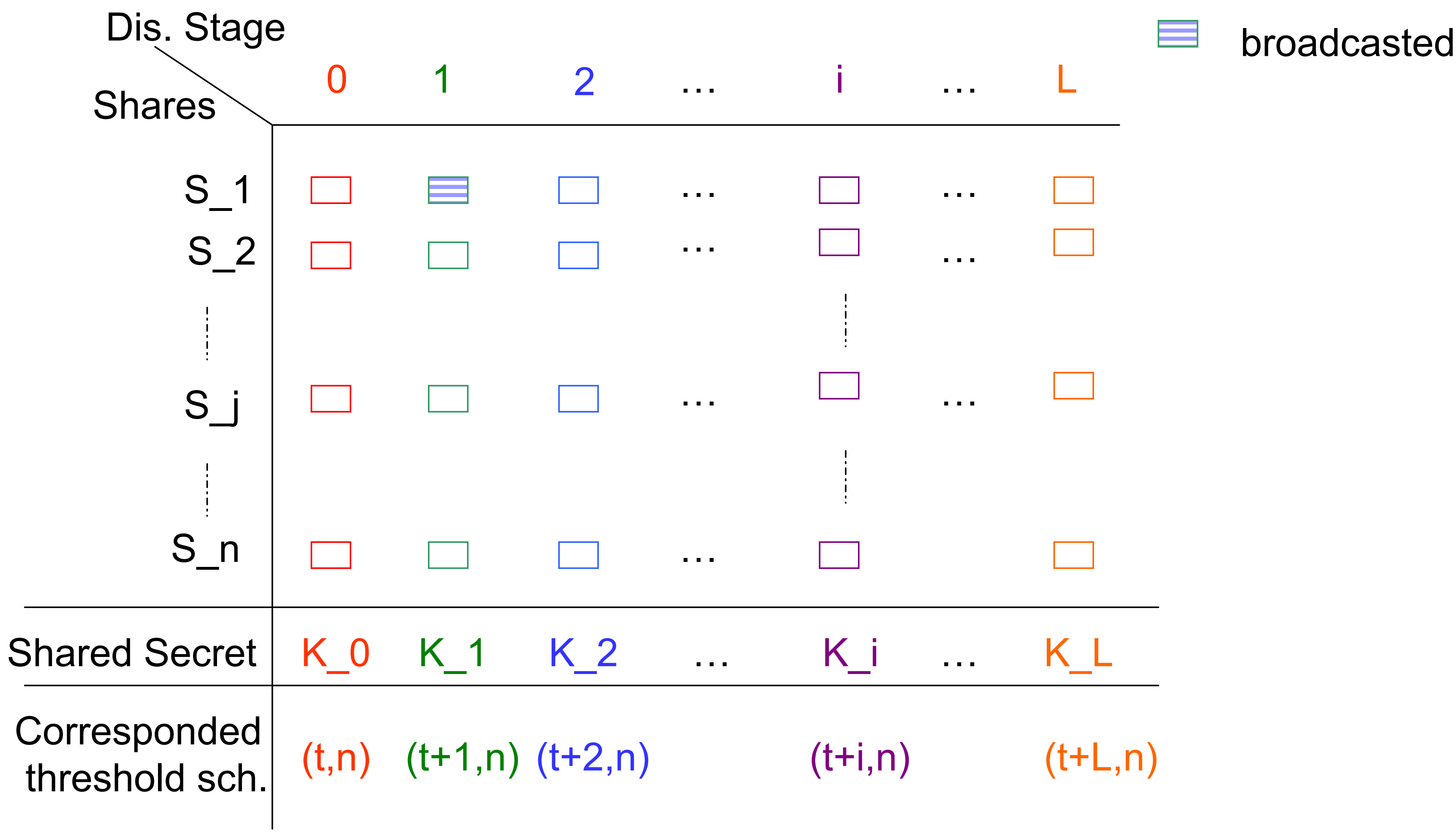
- We are interested in the case where the dealer has full control over disenrollment – has the capability to disenroll any participant at any time and prevents the disenrolled participant from getting current and future secrets.

A Scheme Satisfying Original Model but Renders Dealer Lack of Control Over Disenrollment

Dis. Stage / Shares	0	1	2	…	i	…	L
S_1				…		…	
S_2				…		…	
⋮					⋮		
S_j				…		…	
⋮					⋮		
S_n				…			
Shared Secret	K_0	K_1	K_2	…	K_i	…	K_L
Corresponded threshold sch.	(t,n)	(t+1,n)	(t+2,n)		(t+i,n)		(t+L,n)

A Scheme Satisfying Original Model but Renders Dealer Lack of Control Over Disenrollment

Disenrolling participant 1 at stage 1:



What Is Missing in the Original Definition?

- In the scheme presented: a coalition of t+i participants at stage 0 can obtain future shared secrets K_1 up to K_i in advance
- The dealer cannot disenroll any of t+i colluders of its choice.
- To prevent any set of colluders from obtaining future secrets so to allow the dealer to have the control over disenrollment, the model should ensure that the broadcast P_i is needed in the reconstruction of K_i

Enforcing the Broadcast Constraint

- We add the constraint:

$$I(K_i; S_{1:n}, P_{1:i-1}) = 0$$

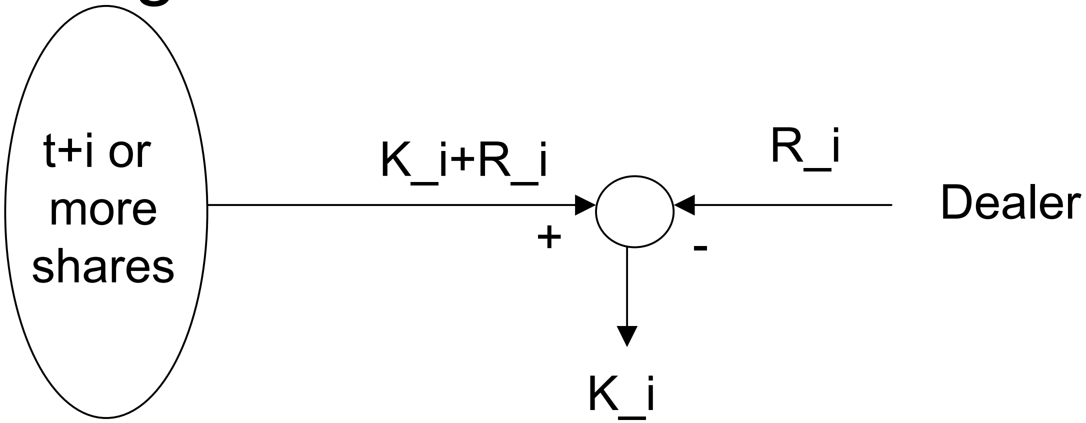
➔without P_i, K_i cannot be reconstructed even given all shares and all previous broadcast

- Schemes satisfying the constraint are called **broadcast enforced** threshold scheme with disenrollment
- No colluders can obtain the shared secret K_i in advance without having P_i

A Broadcast Enforced Threshold Scheme with Disenrollment

- Consider
  - Share $S_j = \{S_j^{(0)}, ..., S_j^{(i)}, ..., S_j^{(L)}\},$

    where $S_j^{(i)}$ is a share of a (t+i, n) threshold scheme sharing K_i+R_i, with R_i being a random seed.
  - Broadcast $P_i = \{R_i, S_{d_1}^{(i)}, ..., S_{d_i}^{(i)}\}.$
- It prevents any set of colluders from obtaining K_i before stage i.



Is Broadcast Enforcement Sufficient for Dealer to Have Control Over Disenrollment?

- A collusion of t+i can recover $K_1+R_1, \ldots, K_i+R_i$ and obtain K_i once the dealer broadcasts
  - The dealer can't disenroll any of the t+i colluders at its choice
- Not all the broadcast enforcement schemes ensure the dealer of control over disenrollment.

A Scheme with Dealer's Control – Attributed to Brickell-Stinson

- Share given to j: $S_j = \{S_j^{(0)}, R_j^{(1)}, ..., R_j^{(L)}\}$, where $R_j^{(i)}$ denotes encryption/decryption key for participant j at stage i.
- Broacast $P_i = \{S_{v_1}^{(i)} + R_{v_1}^{(i)}, S_{v_2}^{(i)} + R_{v_2}^{(i)}, ..., S_{v_{n-i}}^{(i)} + R_{v_{n-i}}^{(i)}\}$, S_v being the share of a valid participant
- If the dealer knows who are colluders, it can disenroll them by not updating them with new shares - disenrolling more than one member at a time.

Lower bound on the entropy of broadcast

- Conjecture in the original paper

  $H(P_i)$¸ $iH(K_i) = im$

- Barwick et. al. proved in ACISP'02 the bound for original model:

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

- In the broadcast enforcement model, we prove

  $H(P_i)$¸ $\min(i+1, n-t-i+1)\, m$

Conclusions and Problems

- Demonstrated that there are schemes that satisfy original mathematical definitions but do not allow the dealer to disenroll a member of choice
- The enforcement that requires the broadcast from the dealer is needed in the reconstruction of current shared secret is not enough to give dealer the control over the disenrollment
- We find the lack of control of the dealer in presence of collusion is partially due to the dealer’s ability to disenroll only *one* participant at a time
- How to characterize the model in which the dealer has full control over disenrollment remains an open problem