Tightly Coupled (t,n)-Secret Sharing

Miao Fuyou

School of Computer Sci. & Tech.,USTC

2017.9.28


64% 14:10
大二班(35人)
2月28日 早上09:31
王淑华！语竹！
各位家长您好:
大二班全体教师诚挚的邀请您于3月1日9:30分参加本班的家长会。
王淑华！语竹！
收到请回复。
小v
子萌收到
雅祺妈
收到
延吉新闻网
www.yanjinews.com


27B/s 92% 10:22
聊天信息(88)
黄翠...
薛军...
平步...
张永...
张力...
苏栋
安阳...
蓝胖纸
安阳...
葛云飞
郑轻...
一棵松
河工...
河南...
河工...
信阳...
丽燕...
武汉...
大连...
在路上
中山...
会务...
肖静...
平顶...
么贵永


19B/s 92% 10:28
高招咨询会群(88)
6月30日 晚上18:11
主任 许昌咨询会"邀请"cherry"加入了群聊
"cherry"与群里其他人都不是微信朋友关系，请注意隐私安全
6月30日 晚上18:38
主任 许昌咨询会
欢迎同济大学张老师加入！
6月30日 晚上18:47
组委会1560 99"邀请"木南"加入了群聊
组委会1560 99

Don’t want the wrong person to get any information, How to?

Authenticate each person one by one:

n(n-1)/2 rounds

How to improve the efficiency in authentication?

→Each person authenticates the others at once.

- (t,m,n)-Tightly Coupled Secret Sharing
  -A new tool to address the problem

Outline

- (t,n)-Secret Sharing
- 2 Attacks Against (t,n)-SS
- Noisy Channel Solutions
  -Information Theoretical View
- Randomized Component
- (t,m,n)-Tightly Coupled Secret Sharing

What is Secret Sharing (SS)

- (t,n)-Secret Sharing
  - a secret s is divided into n shares such that:
    - (1) any t or more than t shares →s;
    - (2) less than t shares \→s;
  - Applications
    - Threshold encryption/signature
    - Key Distribution
    - Secure Multiparty Computation
    - Group authentication
    - Image Processing –Visual Secret Sharing
    - Access Control
    - …

(3,n)-SS

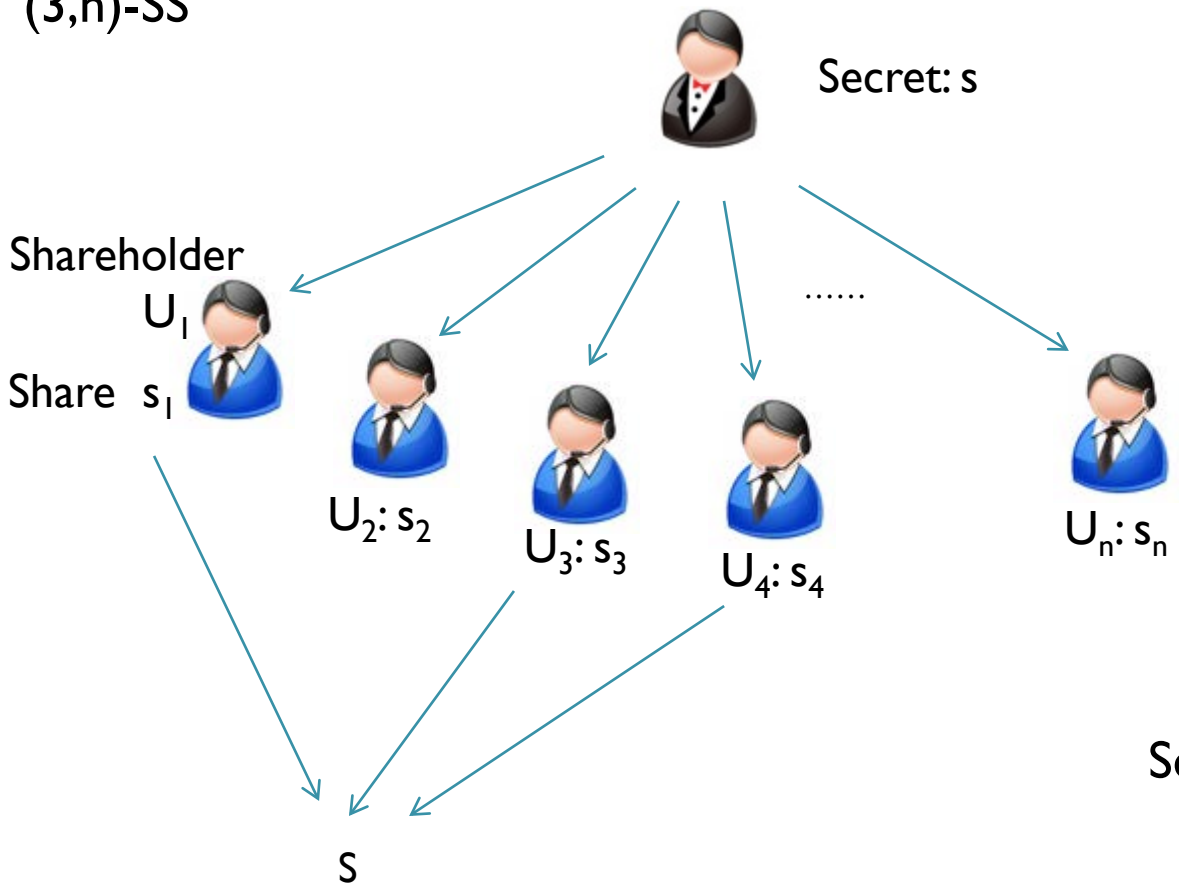


Fig 1. An example of (3,n)-SS

Typical (t,n)-SS

- Shamir's (t,n)-SS
  - Dealer D: $f(x) = a_0 + a_1 x + \ldots + a_{t-1} x^{t-1} \bmod p,$

    $s = f(0) = a_0 \quad a_j \in F_p, j = 0,1,2,\ldots,t-1$
  - Share distribution:
    - Dealer D: for n shareholders $\{U_1, U_2, \ldots, U_n\}$,

      $f(x_i) \rightarrow U_i$, *the share of* $U_i : s_i = f(x_i)$, *public* inf : x_i
  - Secret Reconstruction
    - m shareholders $J_m = \{U_1, U_2, \ldots, U_m\}$, (n≥m ≥ t)

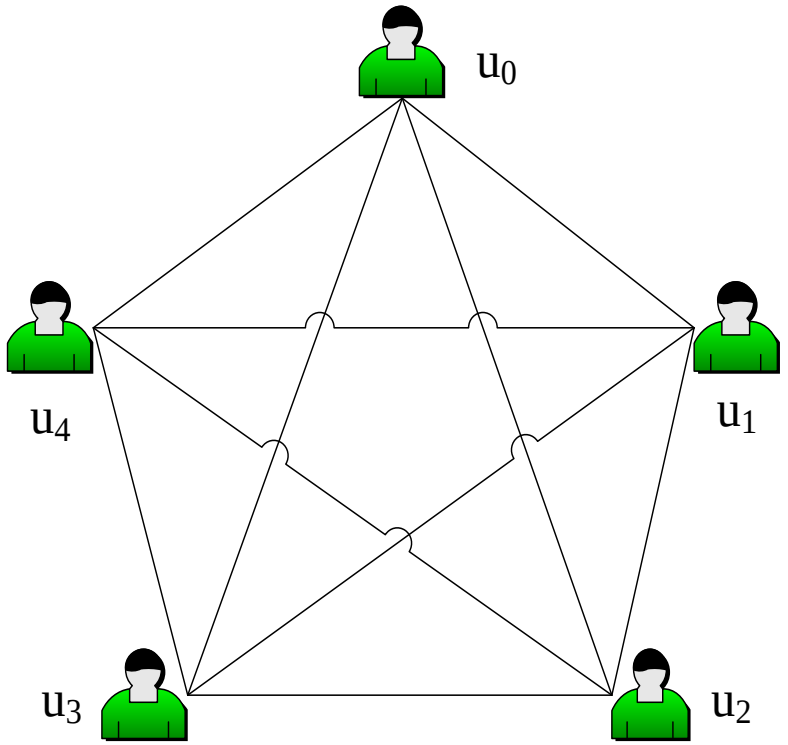
$$s = f(0) = \sum_{U_j \in J_m} s_j \prod_{\substack{U_j \in J_m \\ j \neq r}} \frac{-x_r}{x_j - x_r} \bmod p$$

Other SS

- Mignotte's SS and Asmuth-Bloom's SS (CRT based)
- Blakely's SS (Geometry based)
- Massey's SS (Linear Code based)

Communication Model

Symmetrical Private Channel (or SPC) between each pair of shareholders



(3,n)-SS

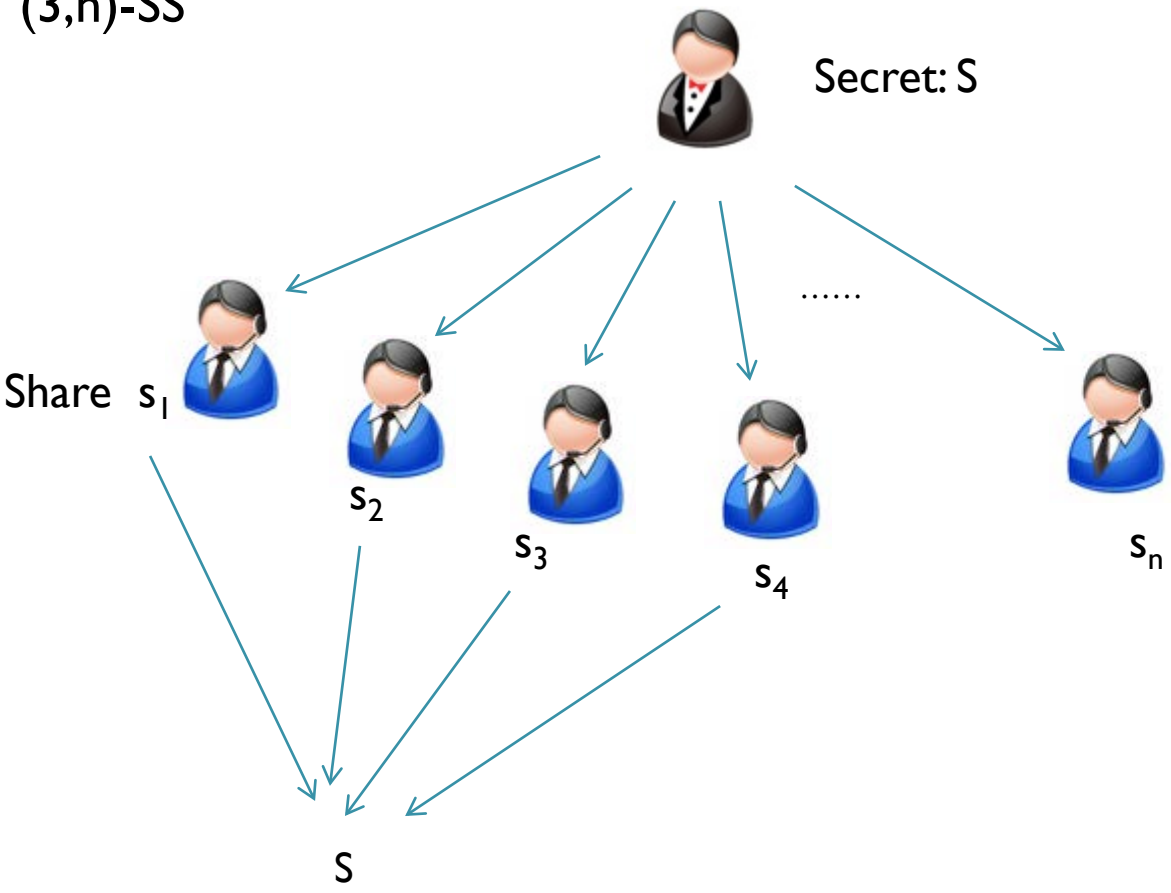
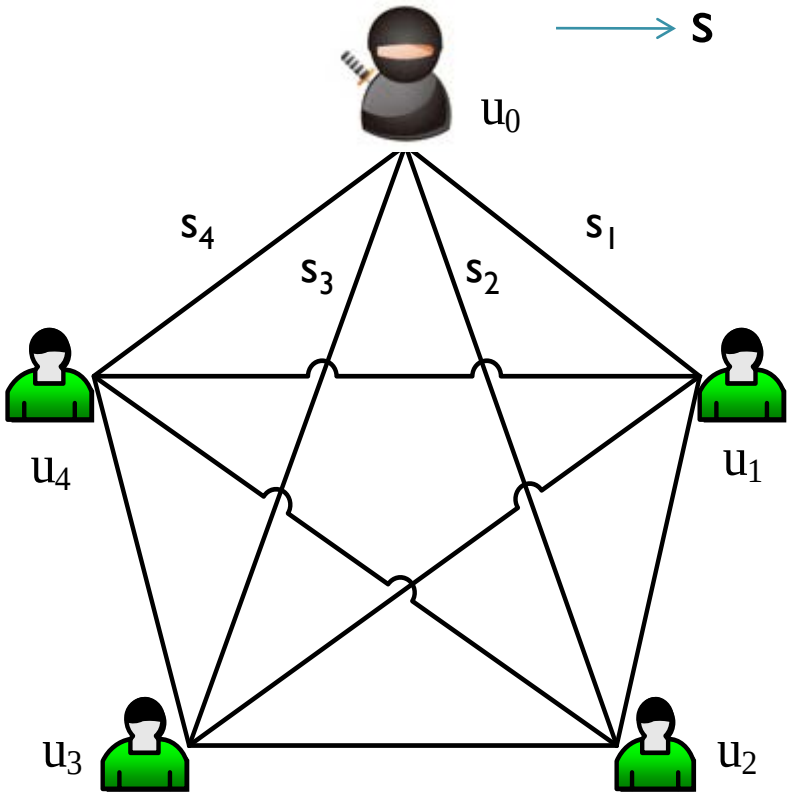


Fig 1. An example of (3,n)-SS

Illegal Participant Attack-IP

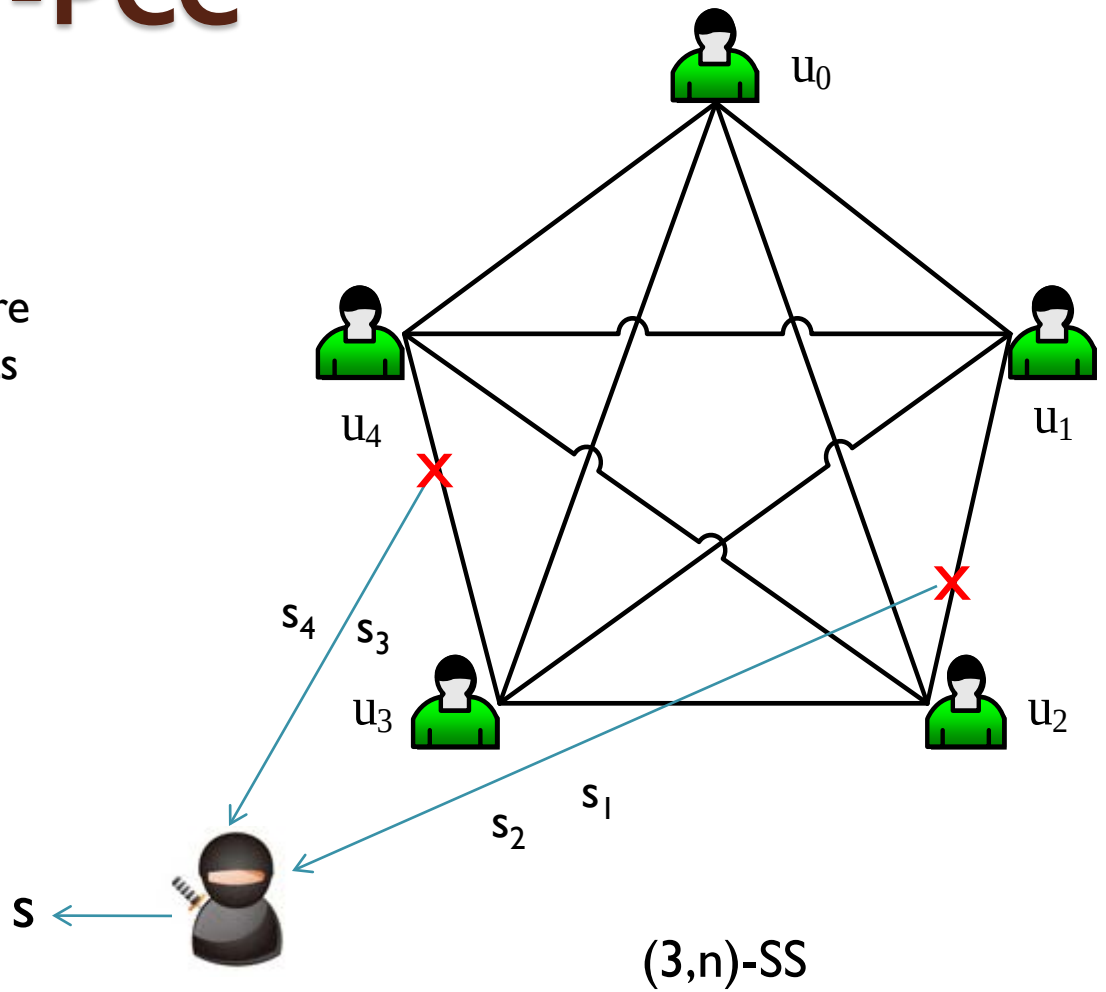


(3,n)-SS

Private Channel Cracking Attack -PCC

Only to crack t/2 SPCs to obtain S Even if much more than t participants recover S.

How to improve the robustness?



How to
thwart IP attack and *improve the robustness*
against PCC attack?

Existing Countermeasure against IP attack

- Verifiable Secret Sharing
  - verify each share of participant before secret reconstruction
- Participant Authentication
  - verify the identity of participants
- Weakness

  Individual Verification, Complexity

Existing ways to improve the robustness against PCC attack

- Full-shuffling

  each participant needs to exchange a random number with every other participant. $m(m-1)/2$ random numbers to exchange. Lower bound: $m/2$ SPCs.

- Partial-shuffling

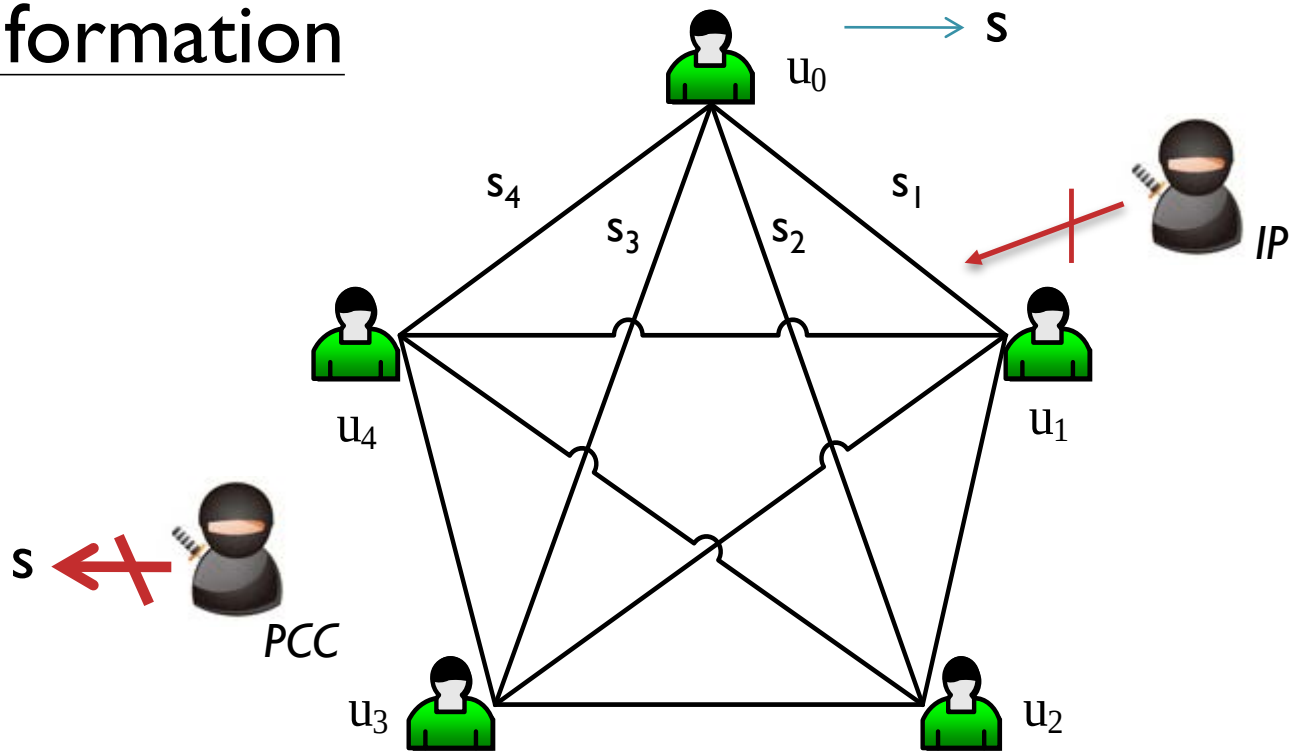
  m random numbers need to be exchanged

  lower bound: $\min\{m/2,t\}$ SPCs , 2 SPCs to get a share

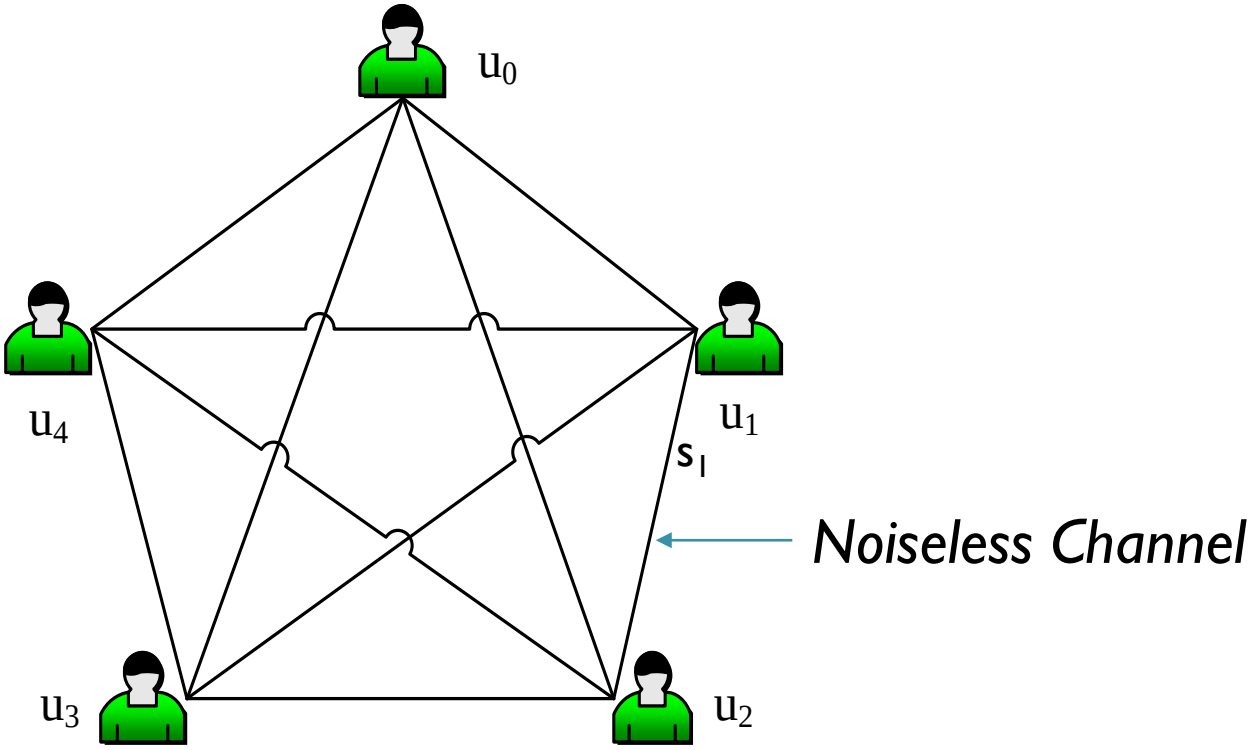
Disadvantage: Extra communications

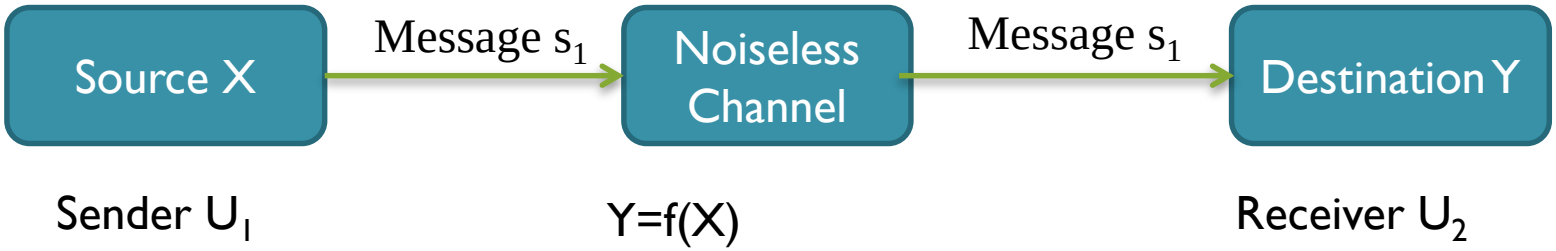
Our Objects

- *thwart IP attack* and *maximize the robustness against PCC attack*
- Requirement: No need to exchange extra information

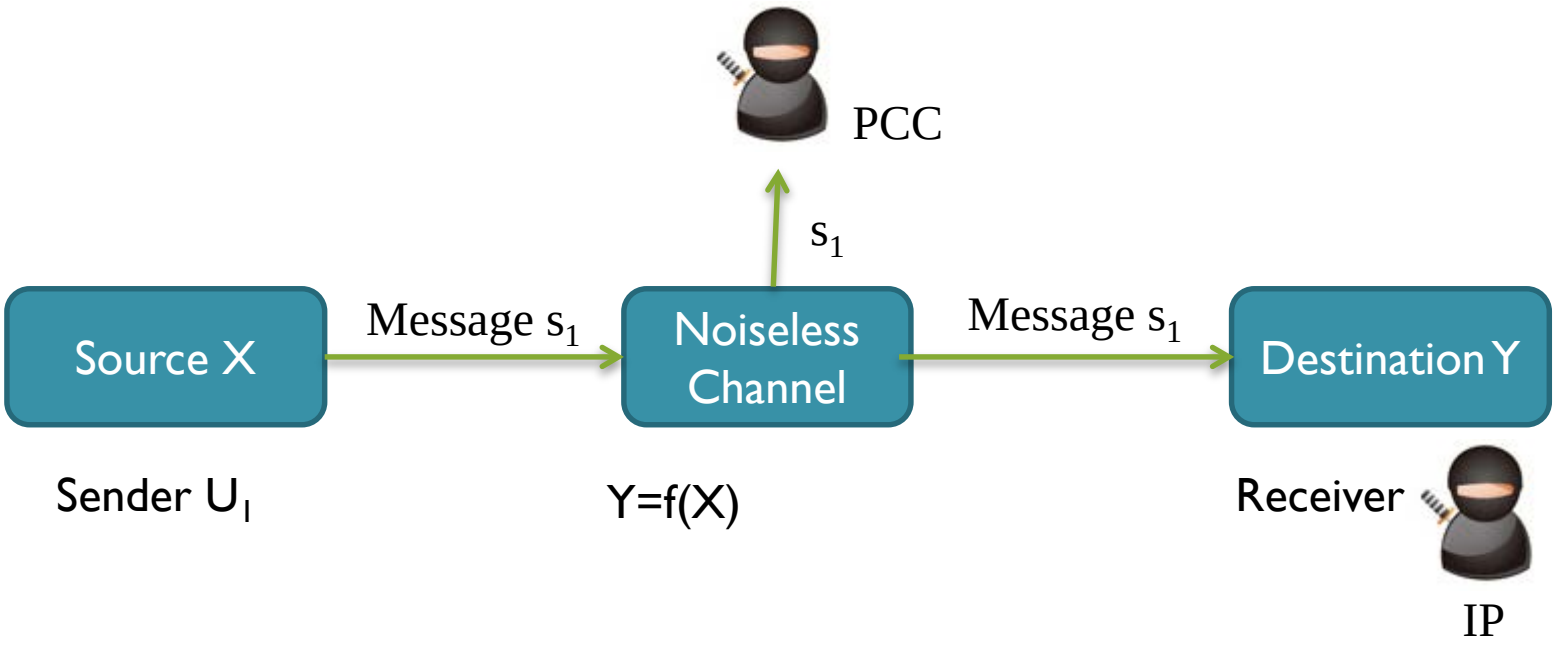


Analysis of Existing Solutions -Information Theoretical View



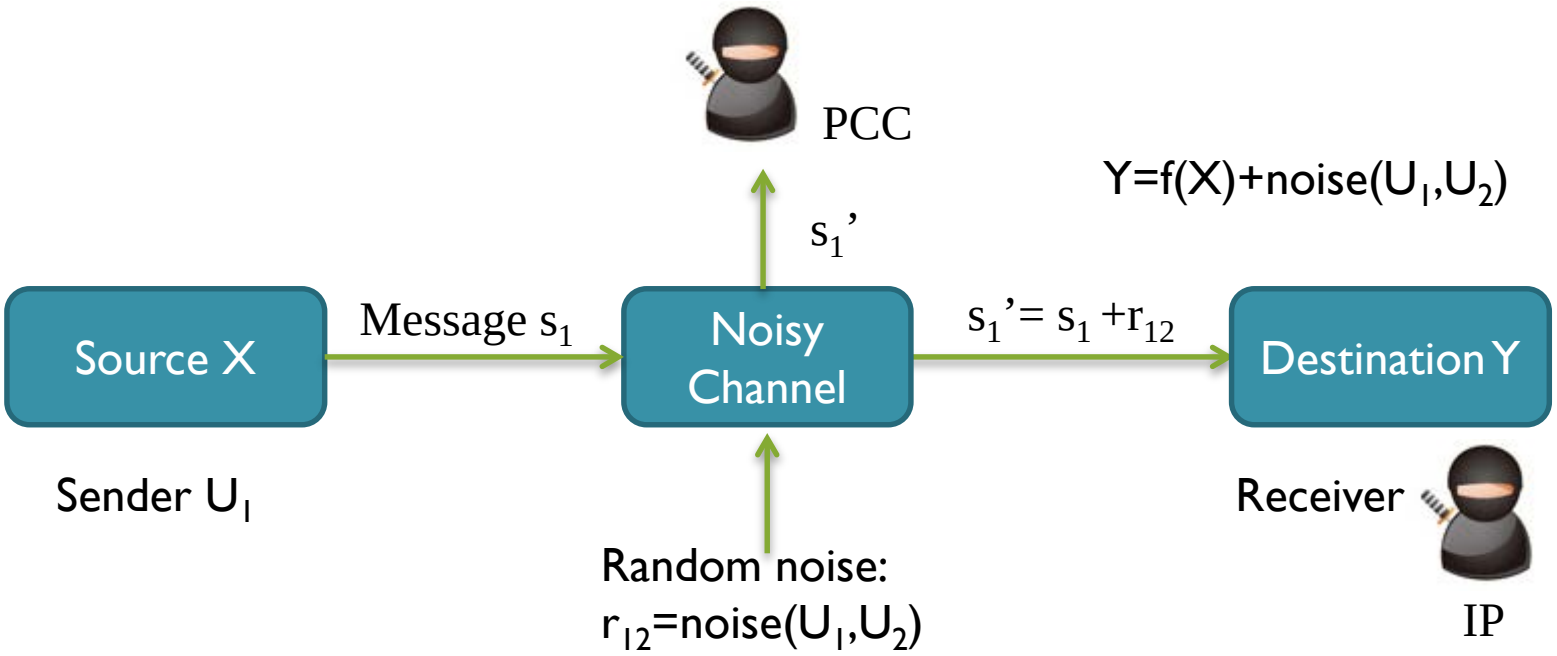


Analysis of Existing Solutions -Information Theoretical View



Existing Noiseless Channel Model

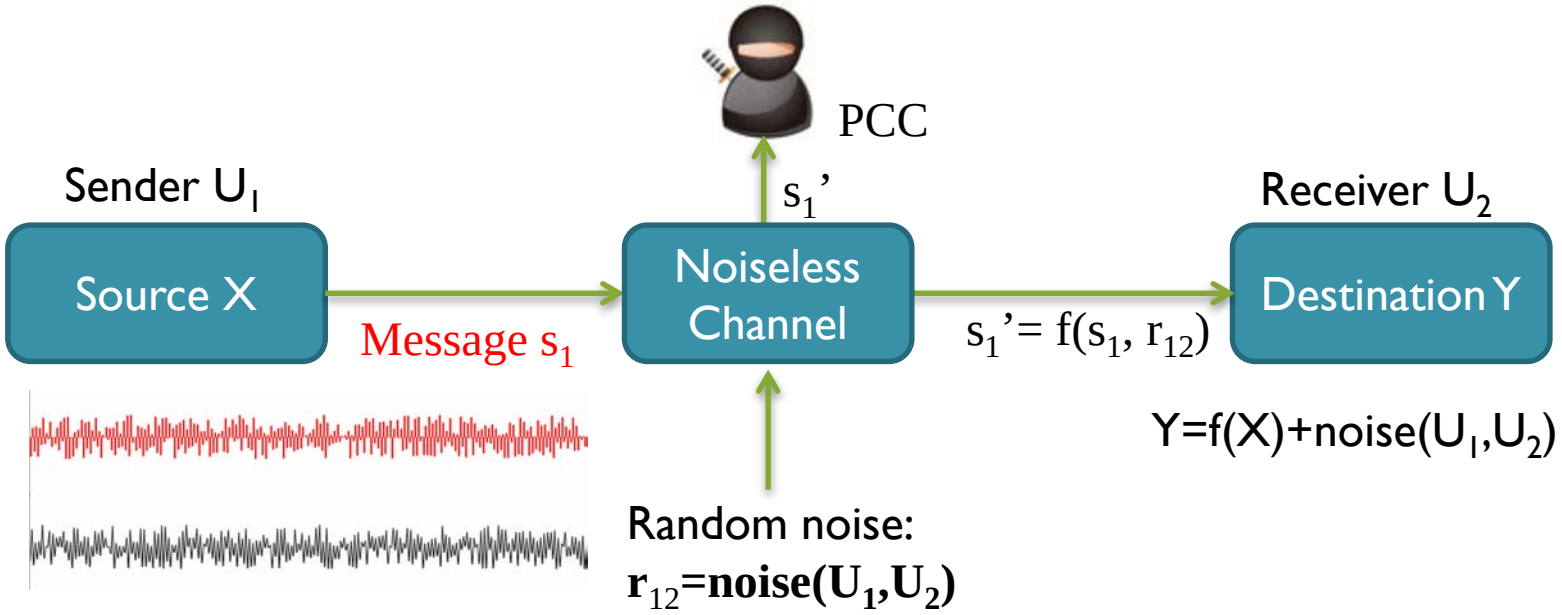
Noisy Channel Solutions -Information Theoretical View



Noisy Channel Model

Prevention from obtaining s_1 in PCC and IP attack

Noisy Channel Solutions -Information Theoretical View



Noisy Channel Model

1. If $|\mathbf{noise(U_1,U_2)}| \geq |\mathbf{s_1}|$, the signal $\mathbf{s_1}$ is completely covered/perturbed.
2. However, normal receiver U_2 cannot obtain the signal $\mathbf{s_1}$ too.
3. Without extra interaction, the noise $\mathbf{r_{12}}$ cannot be removed.

Noisy Channel Solutions -Information Theoretical View

- *Original Objects*
  - *thwart IP attack* and *maximize the robustness against PCC attack* ✓
  - Requirement: ***No need to exchange extra information*** ?

Noisy Channel Solutions -Information Theoretical View

- How to

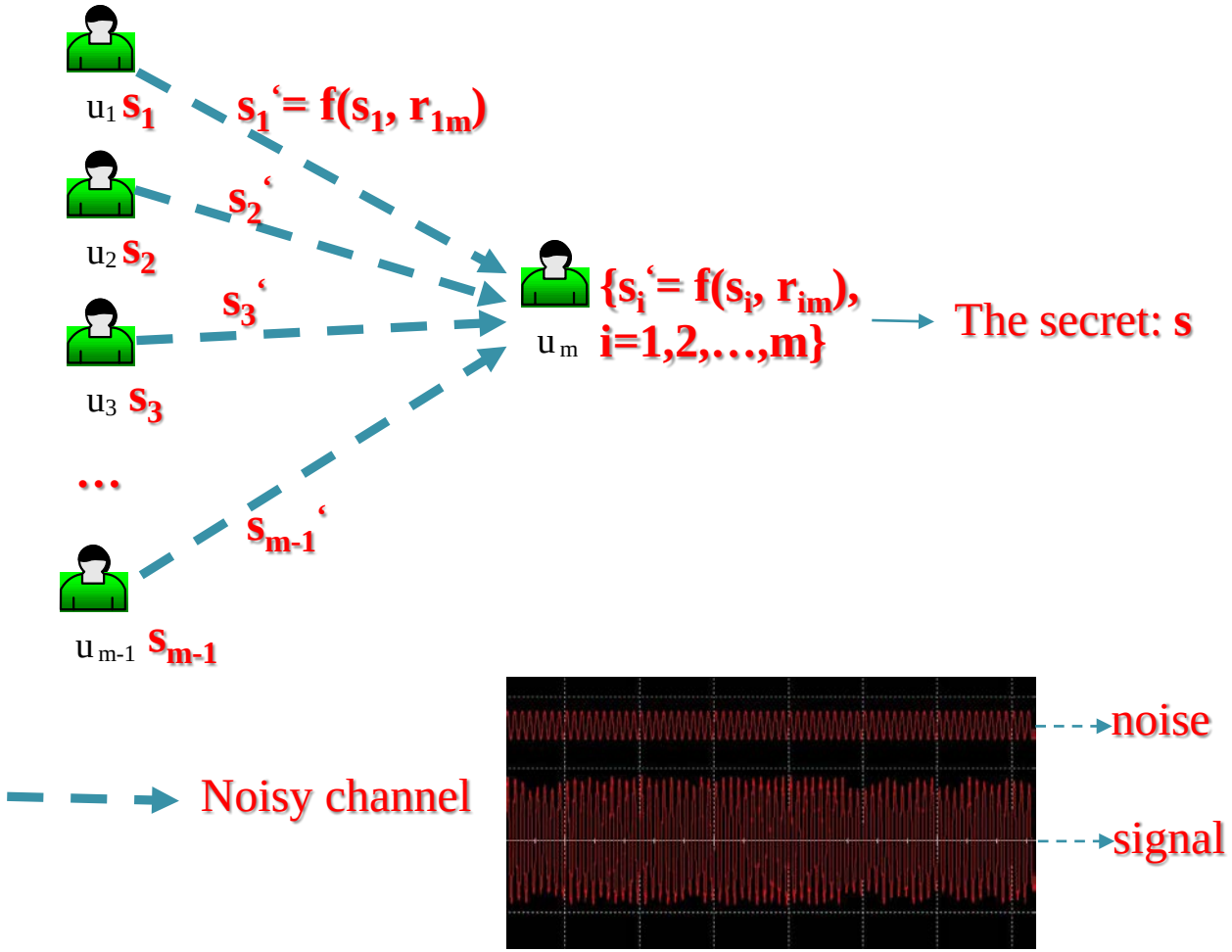
  Remove random noise r

  without extra interaction

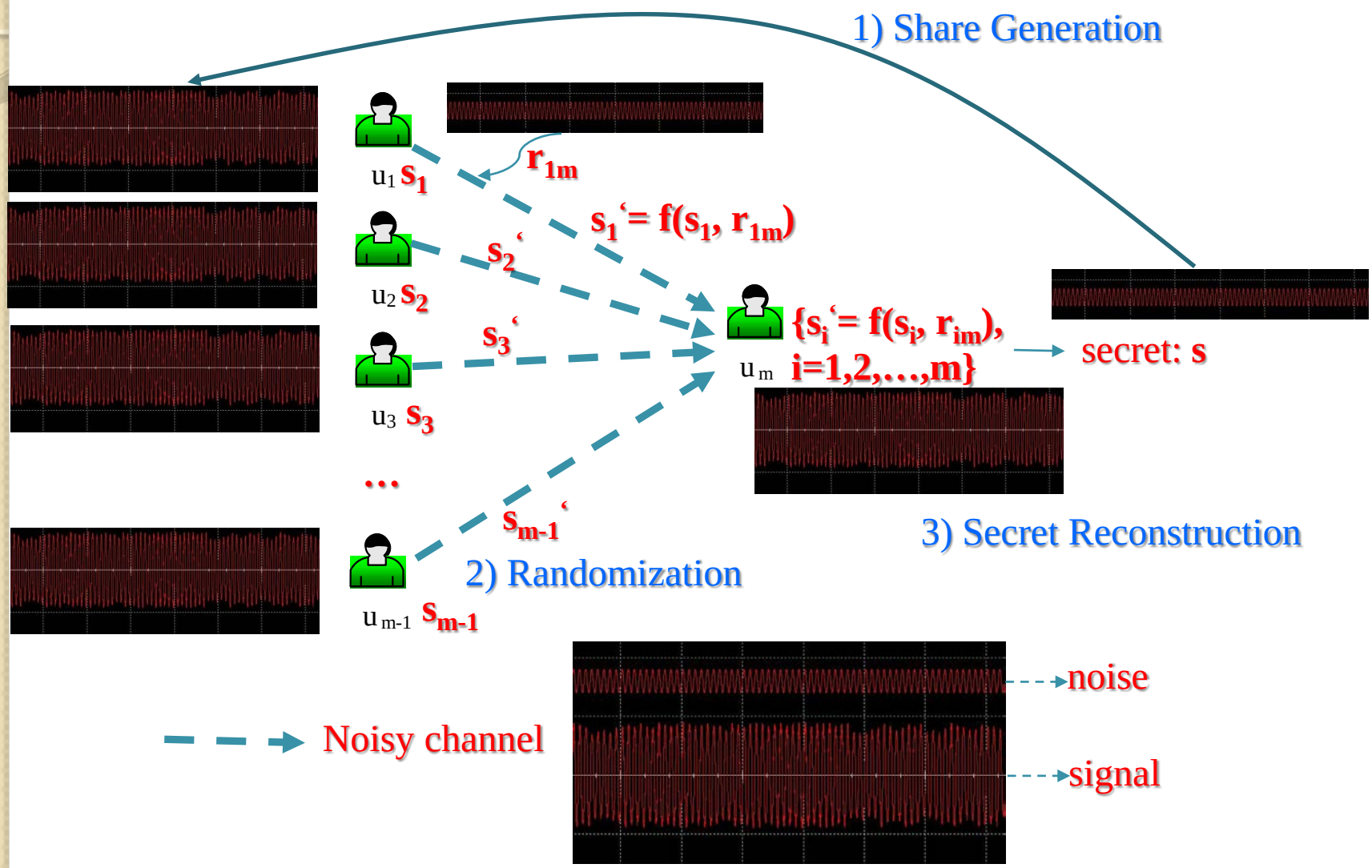
  in recovering the secret s ?

Noisy Channel Solutions -Information Theoretical View

- Information Theoretical Requirement



Noisy Channel Solutions -Information Theoretical View



Randomized Component

- Functionality:
  - Protecting a share from exposure during transimition
  - Capability of secret reconstruction
  - All participants have to join in the secret reconstruction

$$s_i' = f(s_i, U, r_i), \quad i=1,2,\ldots,m$$

How to construct the function f(.)?

Randomized Component

- Basic Idea
- If s is a secret value in [0,99] to be hide, we can add a private random number r in[0,9], to obtain a number c=(s+r) mod 100
- Suppose you know c =55, what is the probability to guess s?
- Obviously it is 1/10.

Randomized Component

- $g : F_p \times F_p \times F_q \rightarrow F_p$ is a function, $c_i = g(s_k, INF_{I_m}, r_i)$ is called the Randomized Component of the participant U_k, where s_k is the share of U_k, INF_{I_m} is the public information related to , the group of all m participants in a secret reconstruction , r_i is a random integer uniformly distributed in F_q.

Polynomial-based Randomized Component (PRC)

- If m participants, $\{U_1, U_2, \ldots, U_m\}$ need to recover the secret $s = f(0) = a_0 \bmod q$, each participant, e.g., U_i constructs the RC as

$$c_i = \left(f(x_i) \prod_{v=1, v \neq i}^{m} \frac{-x_v}{x_i - x_v} + r_i q \right) \bmod p,$$

- $p > nq^2 + q$, r_i is uniformly distributed in F_q.
- p, q are primes.

Using PRC to protect the share

Given

$$c_i = (f(x_i) \prod_{v=1, v \neq i}^{m} \frac{-x_v}{x_i - x_v} + r_i q) \bmod p,$$

An adversary has the probability of $1/q$ to figure out the share $f(x_i)$.

Secret Reconstruction based PRC

- Each participant, e.g., U_{i_j} ,$(1 \leq j \leq m)$,

computes the secret as

$$s = (\sum_{j=1}^{m} c_{i_j} \ mod \ p) mod \ q$$

(t,m,n)- TCSS

- Tightly Coupled Secret Sharing with threshold t, m participants and totally n shareholders.

Set of n shareholders: $\mathcal{U} = \{U_1, U_2, \ldots U_n\}$ with respective public information $\{x_1, x_2, \ldots, x_n\}$;

Group of m participants: $\{U_{i_1}, U_{i_2}, \ldots U_{i_m}\} \subseteq \mathcal{U}, (m \geq t)$

Parameters:

Primes: p, q with $p > q + nq^2$;

Polynomial in F_p : $f(x) = a_0 + a_1 x + \ldots + a_{t-1} x^{t-1} \bmod p$,

$a_i \in F_p$, for $i = 1, \ldots t-1$, $a_{t-1} \neq 0$, $a_0 \in F_q$;

Secret: $s = a_0$;

Algorithms:

A. Share Generation

D computes and sends share $s_i = f(x_i)$ to U_i secretly, for $i = 1, 2, \ldots n$.

B. Randomized Component Construction

Given $\{U_{i_1}, U_{i_2}, \ldots U_{i_m}\} \subseteq \mathcal{U}$, each participant, e.g., $U_{i_j}, (1 \leq j \leq m)$, constructs the RC, c_{i_j} and releases it to the others through private channels:

$$c_{i_j} = \left(f(x_{i_j}) \prod_{v=1, v \neq j}^{m} \frac{-x_{i_v}}{x_{i_j} - x_{i_v}} + r_{i_j} q \right) \bmod p$$

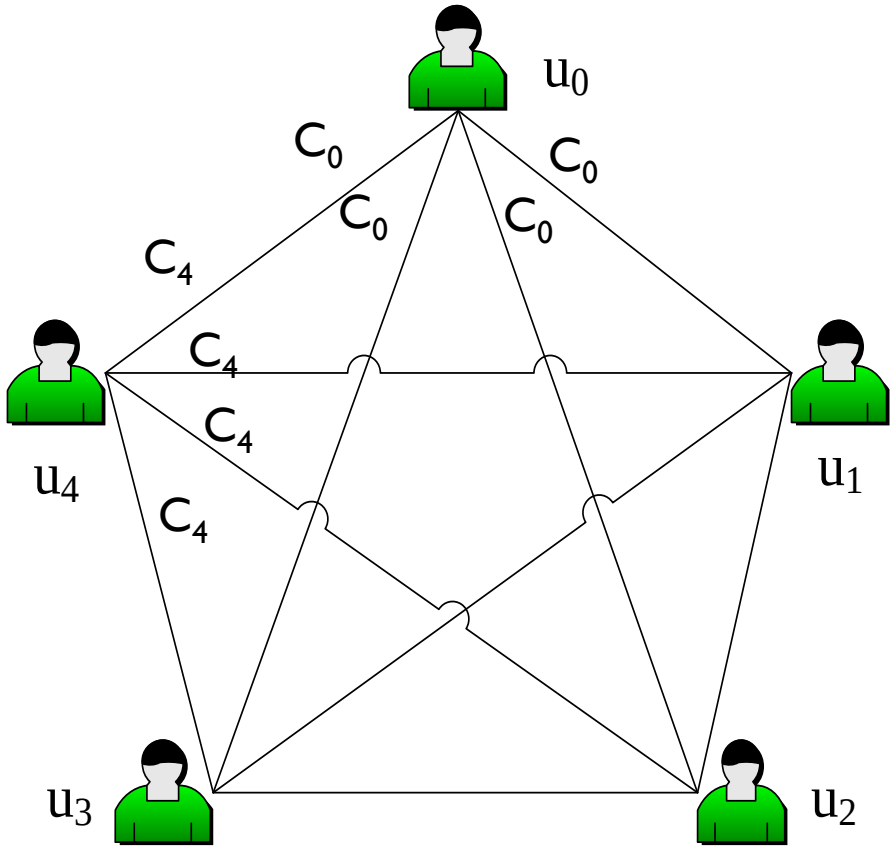
$$(r_{i_j} \in_R F_q, \text{ for } j = 1, 2, \ldots m)$$

C. Secret Reconstruction

Each participant, e.g., $U_{i_j}, (1 \leq j \leq m)$, computes the secret as $s = \left(\sum_{j=1}^{m} c_{i_j} \bmod p \right) \bmod q$.

Fig. 1. (t, m, n)-Group oriented SS based on PRC.

$$s = (\sum_{j=1}^{m} RC_j \bmod p) \bmod q$$



Correctness of (t,m,n)-TCSS

$$(\sum_{i_j \in I_m} c_{i_j} mod\ p) mod\ q$$

$$= \sum_{j=1}^{m} (f(x_{i_j}) \prod_{v=1, v \neq j}^{m} \frac{-x_{i_v}}{x_{i_j} - x_{i_v}} + r_{i_j} q) mod\ p\ mod\ q$$

$$= (f(0) + \sum_{j=1}^{m} r_{i_j} q) mod\ p\ mod\ q \qquad (4\text{-}1)$$

$$= (f(0) + \sum_{j=1}^{m} r_{i_j} q) mod\ q \qquad (4\text{-}2)$$

$$= f(0)$$

Step (4-1) is equivalent to step (4-2) because of $f(0) \in F_q$, $\sum_{j=1}^{m} r_{i_j} q \leq \sum_{j=1}^{n} r_{i_j} q < nqq = nq^2$ and thus $(f(0) + \sum_{j=1}^{m} r_{i_j} q) < q + nq^2 < p$.

Security Analysis

- An adversary without any valid share, almost has no information about the secret in (t,m,n)-TCSS even if it has up to m-1 PRCs .
  - (lower bound: m/2 SPCs)
- (t-1) Insiders almost obtains no information about the secret even if they conspire in (t,m,n)-TCSS.

Properties of (t,m,n)-TCSS

- ***Single share***
- Without user authentication or share verification
- Tightly Coupled
- Unconditionally secure
- Directly applied to Group Authentication

- the secret can be reconstructed only if each participant has a valid share and releases its valid RC honestly.
- Information rate:

IR=(size of secret) / (size of share)

=log q/log p (1/3, 1/2)

Conclusion

- 2 attacks against (t,n)-SS
- Noisy Channel Solutions
  -Information Theoretical View
- Randomized Component
  - Protect shares
  - Bind a participant with all the others
  - Also suitable for other (t,n)-SSs
- (t,m,n)-TCSS
  - Guarantees the secret can be recovered only if all m participants have valid shares and act honestly.

Thanks!