EXPLORING CRYPTOGRAPHY PROTOCOLS

WITH LIMITED EMPHASIS ON MATHEMATICS ☺

Presented By
@7eRoM

ATTENTION

THESE SLIDES HAVE BEEN CRAFTED USING THE FOUNDATION OF MY MSC COURSE IN CRYPTOGRAPHY PROTOCOLS AT THE UNIVERSITY OF ISFAHAN.

I'VE MADE ADJUSTMENTS TO THE CONTENT TO ALIGN WITH THE SPECIFIC OBJECTIVES OF THIS PRESENTATION.

ALSO, MY INTENTION HAS BEEN TO MINIMIZE THE USE OF MATHEMATICAL CONCEPTS, WHICH MAY RESULT IN SOME CONCEPTS BEING SIMPLIFIED OR LESS PRECISE.

Presented By
@7eRoM

Agenda

1. Identification and Entity Authentications Protocols
2. Zero Knowledge Protocols
3. Key Establishment Protocols
4. **Threshold Cryptography and Secret Sharing Protocols**
5. Special Purpose Protocols (like simultaneous contract signing, mental poker, fair exchange)
6. Identity Based Cryptography
7. Types of Digital Signatures
8. Secure Multiparty Computations

Secret Sharing

Content

- Secret Splitting
- Secret Sharing (SS)
- Threshold Secret Sharing (TSS)
- Verifiable Secret Sharing (VSS)
- Key Escrow Systems (KES)
- Proactive Secret Sharing (PSS)

Secret Sharing

Secret Splitting

- Given a secret s, we would like n parties to share the secret so that the following properties hold:
  - All n parties can get together and recover s.
  - Less than n parties cannot recover s.

Secret Sharing

Secret Splitting – Map Example

- You and your friend accidentally discovered a map that you believe would lead you to an island full of treasure.
- You and your so-called friend do not really trust each other
- Here the map is s.
- We split the secret into n pieces $s_1, s_2, \ldots, s_n$ and give one piece to each party.
- Each piece here is called a *share*.

Secret Sharing

Secret Splitting – Salary Example

- Assume that your salary is stored as a number 12345678.
- You want to split your salary into two shares for two parties.
- We can apply the same approach as we did to the map.
- We can split the digits into two sets and give one set to each party as a share.
  - For example, can give the first 4 digits to party 1 and the other 4 to party 2.

1234 5678

- The first party who gets the most significant 4 digits of your salary. It is true that he doesn't know exactly how much your salary is, but he has a pretty good idea about the range of your salary (>= 12340000)

Partial Information Disclosure

Secret Sharing

Partial Information Disclosure

- A share may not contain all the information about a secret, but could disclose partial information.

- In certain cases, such partial information disclosure could be fatal.

Secret Sharing

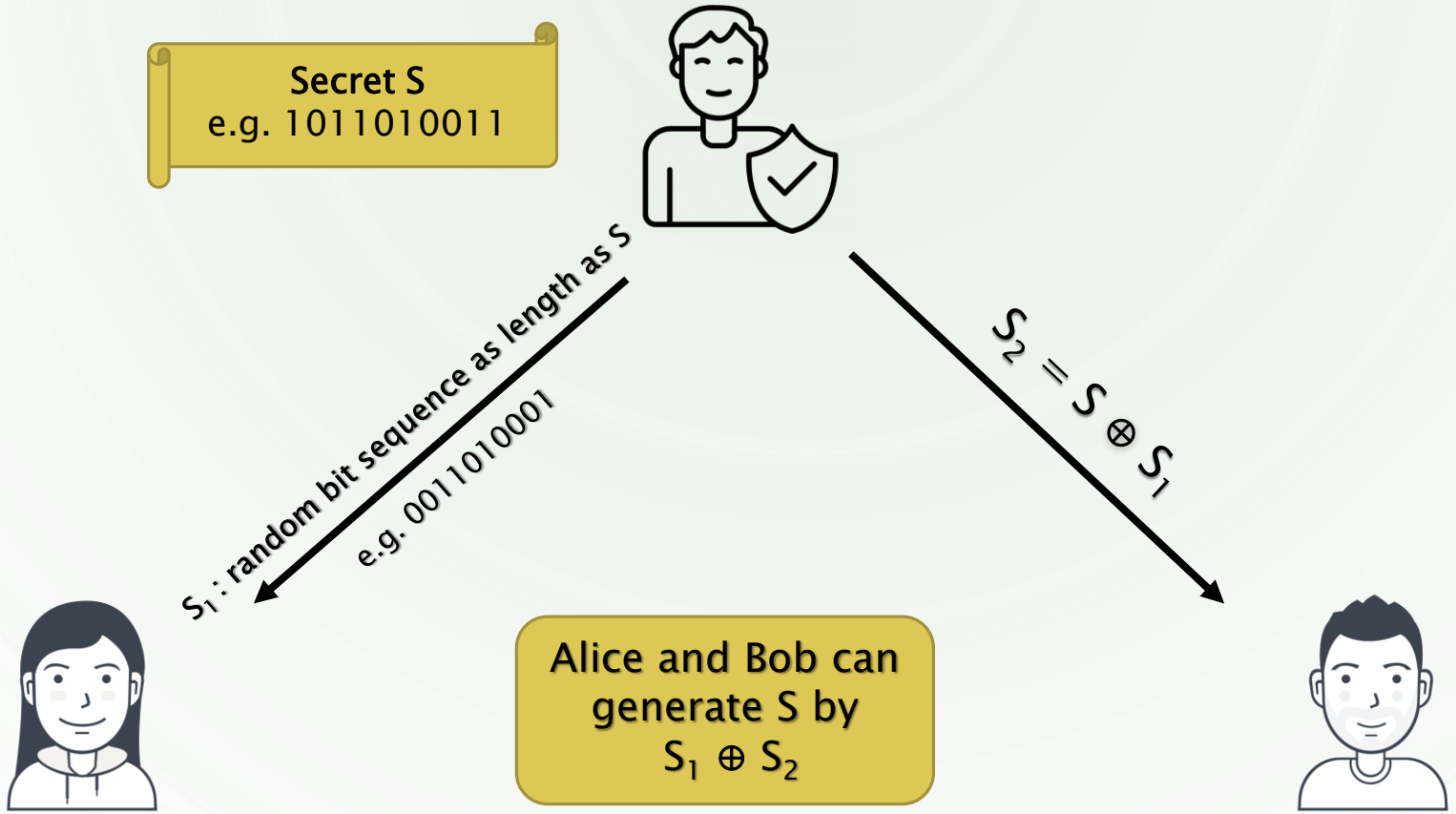
Secret Splitting – Password Example

- Two parties are going to share a password.
- Here a password consists of 8 characters, with each selected from a set of 100 possible characters.
- If we split the password into two shares and each share has 4 characters of the password
- Then each share effectively gives out the secret under a brute-force attack.
- There are 100^8 possible passwords. If it takes 1 microsecond to generate and check one password, then it takes $100^8 * 10^{-6}$ seconds ~ 300 years.
- For a party, there are only 100^4 possible passwords to check against. It would only take $100^4 * 10^{-6} = 100$ sec to find the password.

Partial Information Disclosure

Secret Sharing

Secret Sharing – Password Example



No Information Disclosure

Secret Sharing

Secret Sharing – Generalized Password Example

- There is a bit sequence called S that we want to share between $U_1, U_2, \ldots, U_n$
- TTP generates random bit sequence $S_1, S_2, S_3, \ldots, S_{n-1}$ (as length as S and delivers to users $U_1, U_2, U_3, \ldots, U_{n-1}$
- TTP calculates $S_n = S \oplus S_1 \oplus S_2 \oplus S_3 \oplus \ldots \oplus S_{n-1}$ and sends to U_n
- All users can generate S by $S_1 \oplus S_2 \oplus \ldots \oplus S_n$

No Information Disclosure

Secret Sharing

Threshold Secret Sharing – Nuclear Missile Example

- There is a secret key to launch the nuclear missile
- There are 3 generals who are in charge of a missile launch

- Give the secret code to these three generals
  - it is possible for a lunatic general to start a war and destroy the planet.
- Each general get only one share and knows no information about the secret code
  - what if one general is a spy from a hostile country or even is sick or is on vacation?

- Solution:
  - A missile can be launched with 2 or more generals
  - Less than 2 generals may not launch a missile.

Secret Sharing

(n,t) Secret Sharing

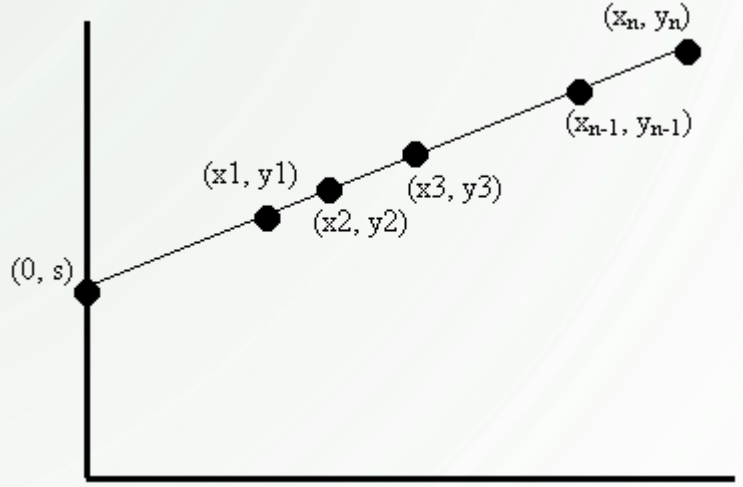
- Given a secret S, to be shared among n parties, that sharing should satisfy the following properties:
  - **Availability**: greater than or equal to t parties can recover S.
  - **Confidentiality**: less than t parties have no information about S.

- In the missile launch example, we are in fact using a (3,2)-secret sharing scheme

Secret Sharing

(n,t) Secret Sharing – Example t=2

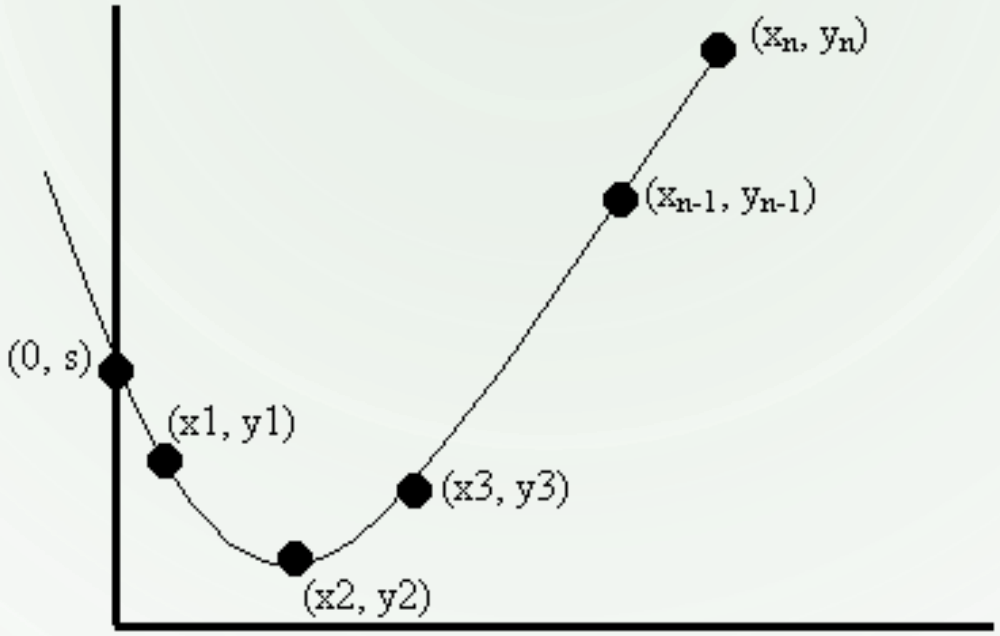
- Select the point (0, s) on the Y axis that corresponds to the secret.
- Randomly draw a line that goes through this point
- Pick n points on that line: $(x_1, y_1), (x_2, y_2), \ldots, (x_n, y_n)$
- Each point that is picked represents a share.



$$y = a_1 * x + S$$

Secret Sharing

(n,t) Secret Sharing – Example t=3



$$y = a_2 * x^2 + a_1 * x + S$$

Generalized for (n, t)–secret sharing scheme (*Shamir – 1979)*

$$y = a_{t-1} * x^{t-1} + a_{t-2} * x^{t-2} + \ldots + a_1 * x + S$$

Secret Sharing

(n,t) Secret Sharing – Shamir (1979)

$$y = a_{t-1}*x^{t-1} + a_{t-2}*x^{t-2} + \ldots + a_1*x + S$$

- How to recover S?
  - Lagrange Interpolation

$$y = f(x) = \sum_{i=1}^{t} y_i \prod_{j=1, j\neq i}^{t} \frac{x - x_j}{x_i - x_j} \mod(p).$$

$$s = f(0) = \sum_{i=1}^{t} y_i \prod_{j=1, j\neq i}^{t} \frac{x_j}{x_j - x_i} \mod(p).$$

Secret Sharing

(n,t) Secret Sharing – Example n=5,t=3

$y_1=f(1)=7+8+11=0 \bmod 13$

$y_2=f(2)=28+16+11=3 \bmod 13$

$y_3=f(3)=63+24+11=7 \bmod 13$

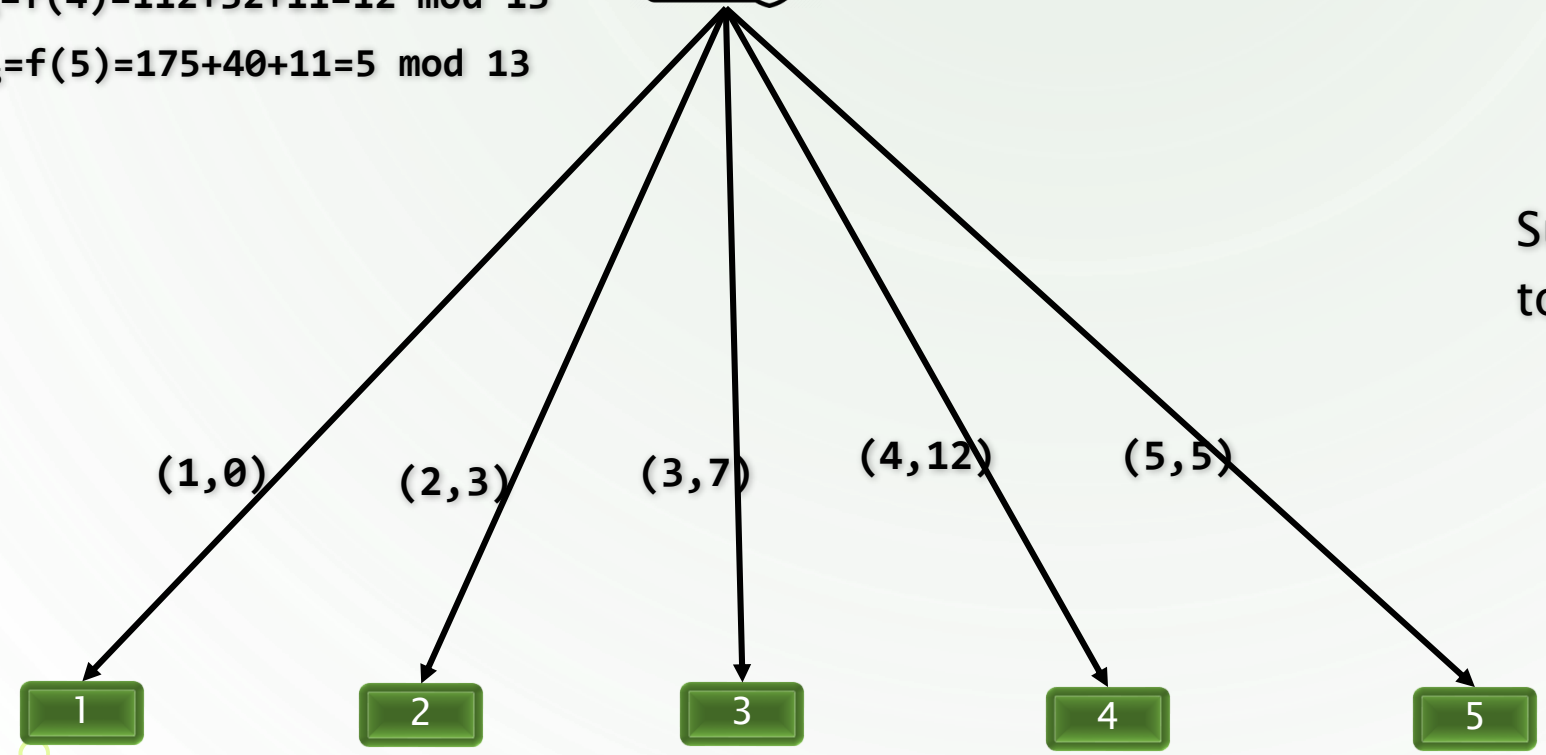
$y_4=f(4)=112+32+11=12 \bmod 13$

$y_5=f(5)=175+40+11=5 \bmod 13$

$y = 7x^2+8x+11 \bmod 13$

$a_1=8$ S=11

$a_2=7$ p=13



Suppose u_2 , u_3 and u_5 wants to recover the secret S

Secret Sharing

(n,t) Secret Sharing – Example n=5,t=3

- 2 (2,3)
- 3 (3,7)
- 5 (5,5)

$$s = f(0) = \sum_{i=1}^{t} y_i \prod_{j=1, j\neq i}^{t} \frac{x_j}{x_j - x_i} \mod(p).$$

$$S = 3 * \frac{3}{3-2} * \frac{5}{5-2} + 7 * \frac{2}{2-3} * \frac{5}{5-3} + 5 * \frac{2}{2-5} * \frac{3}{3-5}$$

$$= 15 - 35 + 5 \mod 13$$

$$= 11$$

Secret Sharing

Verifiable Secret Sharing

- What if a user is malicious?
- The shares must be verifiable

Secret Sharing

Verifiable Secret Sharing – Shamir Scheme

- Initialization
  - Random big prime P
  - Generator g
  - Public version of secret: $E_0 = g^s \bmod p$
- Generate polynomial function
  - Choose random $a_1, a_2, \ldots, a_{t-1}$
  - $f(x) = a_{t-1} * x^{t-1} + a_{t-2} * x^{t-2} + \ldots + a_1 * x + S \bmod p$
- Sending $(i , f(i))$ to user u_i
- Broadcasting $E_j = g^{aj} \bmod p$ for $j=1,2,\ldots,t-1$
- Verification by each user through $g^{f(i)} \stackrel{?}{=} \prod_{j=0}^{t-1} (E_j)^{i^j} \bmod p$
- Recover secret S as before

Secret Sharing

Key Escrow System

- Ability of secure connection between two citizens though an unsecure channel
- Ability of restoring of messages of particular citizens
- Avoid of possible misuse of government representatives

- **So, here is a paradox:**
  - **Citizens need to privacy and secure connection**
  - **Government needs to considering the connections**

Secret Sharing

Key Escrow System

So, What is the solution?

Oh no, Thanks!

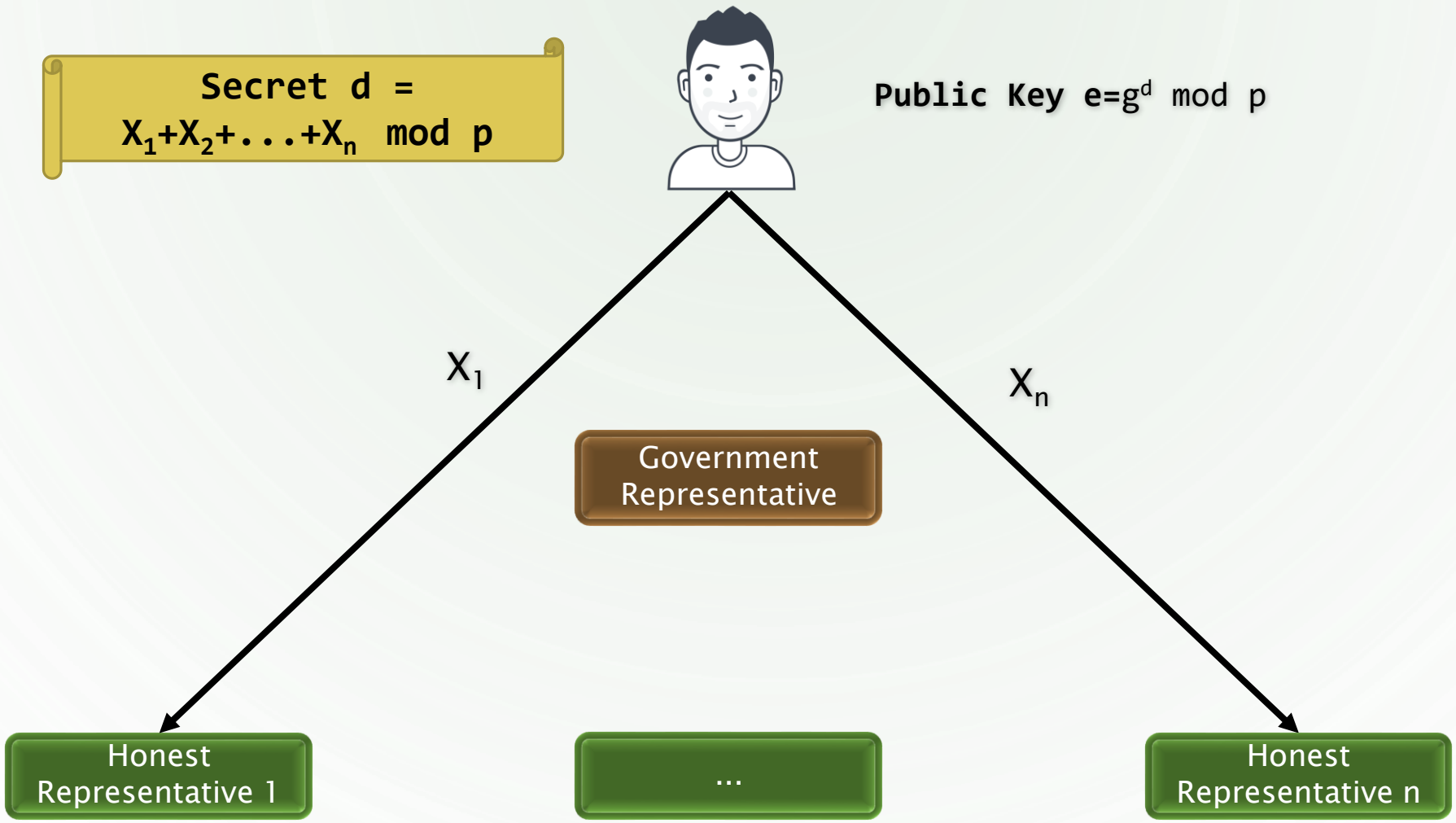
Secret Sharing

Key Escrow System

- Types of trust in government
  - Full trust in the government.
  - Complete distrust in the government; requiring permission from all representatives to restore the key.
  - Partial trust in representatives; requiring permission from t representatives out of n representatives to restore the key.

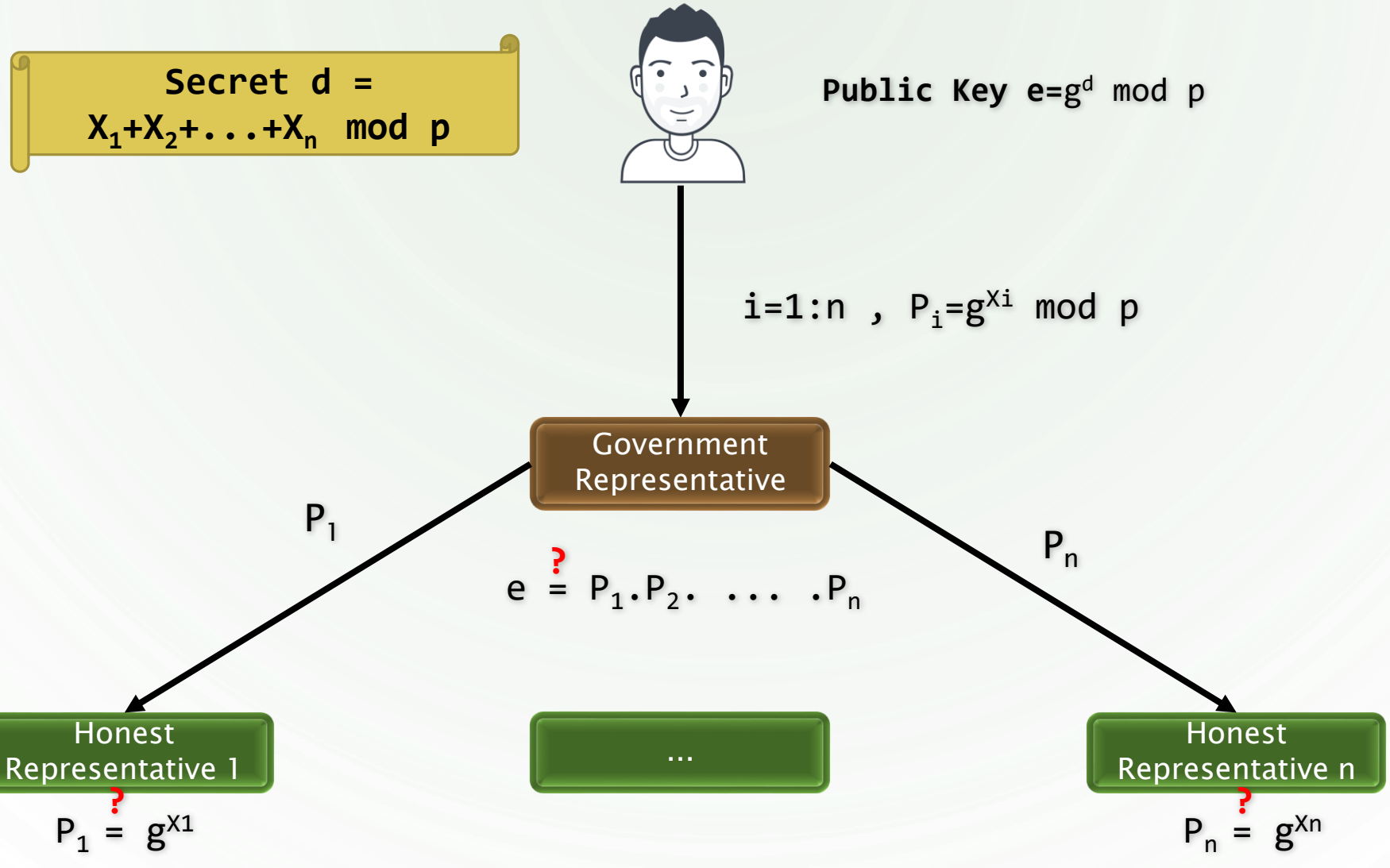
Secret Sharing

Key Escrow System – Diffie–Hellman



Secret Sharing

Key Escrow System – Diffie–Hellman



Secret Sharing

Key Escrow System – Diffie–Hellman

- Reducing probability misuse of government representatives

- The citizen can prevent restoring the key by coalescing with just one representative
  - Solution: Using Verifiable Secret Sharing instead of Secret Splitting
  - The scheme is secure against coalition of the citizen with $n-t$ representatives

Secret Sharing

Proactive Secret Sharing

- Suppose a secret S has been shared between 3 servers using a (3,2) secret sharing scheme.

- If one of the servers is compromised, and the adversary gains access to its share, there is a potential risk that the adversary could acquire shares from other servers, allowing them to reconstruct the secret.

Secret Sharing

Proactive Secret Sharing

In a (n,t) secret share, what if a share would be disclosed?

$S_A+S_B=S \mod p$

Sends S_{A1} through a secure channel

$S_{A1}+S_{A2}=S_A \mod p$

$S_{B1}+S_{B2}=S_B \mod p$

Sends S_{B1} through a secure channel

$S_{A2}+S_{B1}=S'_A \mod p$

$S_{A1}+S_{B2}=S'_B \mod p$


All right, then. Keep your secrets.

Ref

1. Cryptography Protocols Course, Dr. Hamid Mala, University of Isfahan
2. https://www.cs.cornell.edu/courses/cs513/2000SP/SecretSharing.html
3. https://www.iconfinder.com/UsersInsights
4. https://www.iconfinder.com/Chanut-is
5. https://www.iconfinder.com/iconsets/softwaredemo