Secret sharing

Dr.Talal Alkharobi

Information Theft

- Secret and confidential information theft is a major computer crime.
- In 2002, more than $70 million loss was reported due to information theft in US only.

3

Dead or Alive

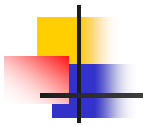
- Some criminals' tools (like viruses) tend to destroy information.
- More than 80% of organizations reported virus's attacks.

4

What to do?

- Having only one copy of this information means that if this copy is destroyed there is no way to retrieve it.
  What to do??
  Replicate!!!
- Replicating the important information will give more chance to intruders to gain access to it.
- Thus, there is a grate need to keep information in a secure and reliable way.
  What to do??
  Secret Sharing!!!

5



Secret Sharing

- The basic idea of secret sharing is to divide information into several pieces such that certain subsets of these pieces (shares) can be used to recover the information.
- Intruders wants to
  - GET the info. several shares need to be theft
  - Destroy. several shares need to be destroyed

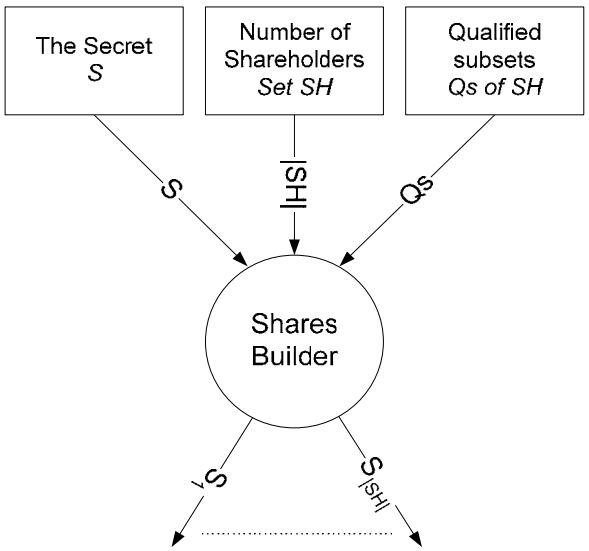
6

Secret Sharing Phases

- Shares building phase.
- Shares distribution phase.
- Secret reconstruction phase.
- **Shares update phase**

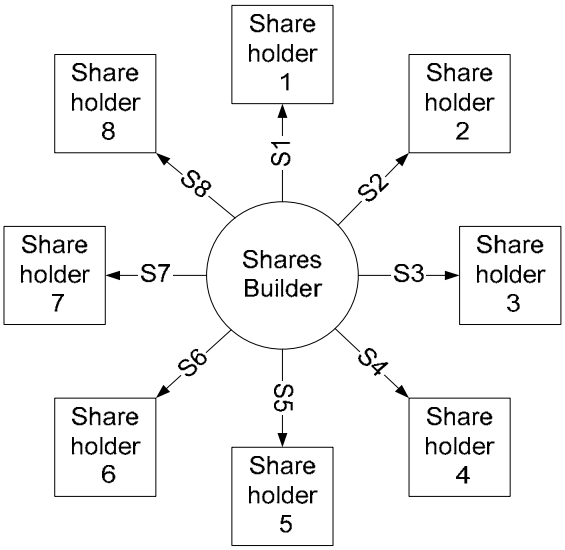
7

Shares building phase



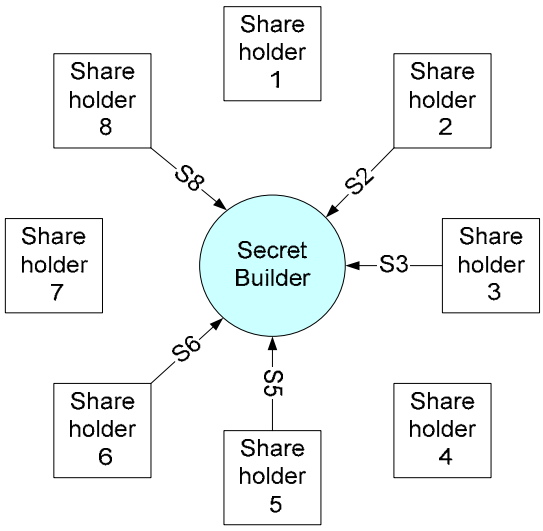
8

Shares distribution phase



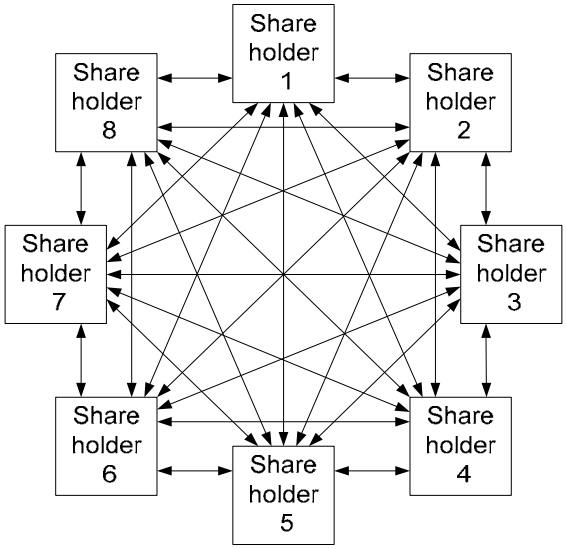
9

Secret reconstruction phase



10

Shares update phase



11

Classification of SSS

- Access structure schemes
  - Special Access Structure
    - Threshold schemes
    - All-or-nothing schemes
    - Vector space
    - Access structure with intersection number = 1
    - Sets of n (n=4, 5, …)
    - Graphs
    - Bipartite access structures
    - 3 or 4 minimal qualified subsets

12

Classification of SSS

- Access structure schemes (cont…)
  - General Access Structure
- Visual secret sharing schemes

13

All-or-nothing scheme

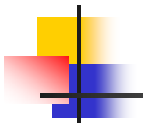
- Also called secret splitting,
- Break the secret into *n* parts and all *n* parts is needed to reconstruct the secret.
- A simple perfect ideal low cost all-or-nothing scheme is to generate *n*-1 random numbers of the same size as the secret. The n^{th} share is a bitwise XOR of the *n*-1 random numbers and the secret.
- To recover the secret, bitwise XOR between the *n* shares.
- Secret splitting scheme allows no margin of error. i.e. single missing/corrupted share will destroy the ability to recreate the secret.

14

Threshold scheme

- The most common SSS
- Two integer parameters *m* and *n* where $1 \leq m \leq n$. Thus, threshold SSS is also called
m-out-of-n SSS.
- The dealer divide the secret into *n* parts and gives each of the n participant one part such that at least *m* parts is needed to recover the secret.

15



General Access structure

- One of the most interesting open questions in this area is to characterize which access structures can be efficiently realized, i.e., with shares of polynomial size in the number of shares.
- Share size is exponential.
- Several lower bounds on the share size of secret-sharing were obtained.
- There is a huge gap between the lower bounds and the best known upper bounds.

16

How it has been done??

- For each qualified subset, split the secret to all members in the qualified subset
- Each shareholder will get a share of size |S| for each qualified subset containing it.
- i.e. if shareholder x is a member of y qualified subset, he will get y shares of size |S|

Visual secret sharing schemes

17

- Visual secret sharing schemes (VSSS) can be easily decoded by the human visual system (the naked eye) without the knowledge of cryptography and cryptographic computations.
- In VSSS, there is a secret picture to be shared among *n* participants.
- The picture is divided into *n* transparencies (shadows) such that if any *m* transparencies are placed together, the picture becomes visible.
- If fewer than *m* transparencies are placed together nothing can be seen.

Share Size

18

- The default complexity measure of secret sharing schemes is the total length of all shares distributed by the share builder.
- A measure of the amount of communication and/or storage required for sharing a secret.
- Mathematically, $\sum_{i=1}^{|SH|} |S_i|$
- A well-known secret sharing fact is that shares size of each shareholder must be at least as the secret itself.
- Most SSS each shareholder share size is strictly bigger than the secret size.

Share Size and computational security

19

- If computational security is sufficient, shares can be shorter than the secret.
- Very useful for large secrets (files).
- The size of the shares can be as short as

$$\frac{|S|}{|SH|} + C$$

- C is a constant that depends only on the security parameters.

Expansion Factor

20

- The length of all shares divided by the number of shareholders. Mathematically

$$Ef = \frac{\sum_{i=1}^{|SH|} |S_i|}{|SH|}$$

21

Information Rate

- Shareholders information rate is a measure of the amount of information that the shareholders need to keep.

$$I_j = \frac{|S|}{|S_j|}$$

- The information rate for the SSS is the average of shareholders information rates.

$$I = \frac{|S|}{Ef} = \frac{|SH|*|S|}{\sum_{i=1}^{|SH|}|S_i|}$$

22

Secret Sharing Properties

- Perfect SSS
- Ideal SSS
- Secret sharing homomorphism
- Linear SSS

23

Partial information disclosure

- S is 123456
  - Split S to 2 shareholders no one knows S exactly
  - S1: 123 & S2: 456 will do…. But
  - S1 knows that S is at least 123000

24

Partial information disclosure

- S is 6 characters password.
  - Each character has 256 possible values.
  - Split S to 2 shareholders no one knows S exactly
  - S1 and S2 will get 3 characters of the secret each, will do…But
  - There are 256^6 possible passwords.
  - Brute-force attacker with capability of generating and checking one password in 10^{-6} sec will need
    - $256^6 * 10^{-6}$ sec > 8 years to try all possible S values.
    - $256^3 * 10^{-6}$ sec < 17 sec to try all possible S1 (or S2) values given the other share

25

Perfect SSS

- SSS is called perfect when every share contains no information about the secret

$$P(S) = P(S \mid S_i) \forall i$$

$$P(S) = P(S \mid SSh_i) \forall SSh_i \notin Qs$$

26

Non-Perfect SSS

- Partial information discloser has been found useful in some cases
- Number of non-perfect secret sharing schemes have been
- The participants belonging to the semi-access subsets are able to obtain some, but not complete information about the secret.
- Usually in non-perfect SSS the size of the shares is less than the size of the secret (suitable to distribute large secrets)
- Making backups of computer files using this method provides insurance against the loss or destruction of valuable data.

27

Ideal secret sharing

- SSS is called ideal if the information rate for all shares is equal to one, i.e. the shares contain as much bits as the secret.
- EF=I=1
- Share size = |SH|*|S|

28

Secret sharing homomorphism

- Secret sharing homomorphism is to allows shares of multiple secrets to combine together to form a “composite share”.
- The composite shares are shares of composite secrets.
- Secret sharing homomorphism is very useful in several applications such as
  - verifiable secret sharing,
  - fault tolerant,
  - generalized SSS, and
  - secret-ballot elections.

29

Linear SSS

- A linear SSS is a linear mapping to the secret and several independent random finite field elements to produce the shares.
- Most known secret-sharing schemes are linear.
- Nearly nothing is known for general as opposed to linear secret sharing schemes.
- Several constructions of nonlinear secret sharing schemes have been suggested. However, none of these works provides evidence that nonlinear schemes are significantly more powerful than the linear counterparts schemes.

30

SSS with special capabilities

- Robustness against cheating
- Verifiability of the shares
- Proactive redistribution of shares
- Disenrollment
- Fault tolerance
- Veto capabilities
- Verifiability

31

Secret Sharing applications

- Access control
- Authentication
- Electronic cash system
- Electronic online voting
- Pass-phrases
- Publius (Secure and reliable file sharing)
- Recreational cards
- Secret broadcasting
- Sharing functions (multi-party computation)
- Threshold decryption

32

Shamir's secret sharing scheme

- Shamir's secret sharing scheme was introduced in 1979.
- His method is based on the well known fact: a polynomial of degree K-1 is uniquely determined by any K points on it.
- A (K-1)-degree polynomial is constructed such that the coefficient a0 (the constant) is the secret.
- All other coefficients are random numbers.

$$F(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{k-1} x^{k-1}$$

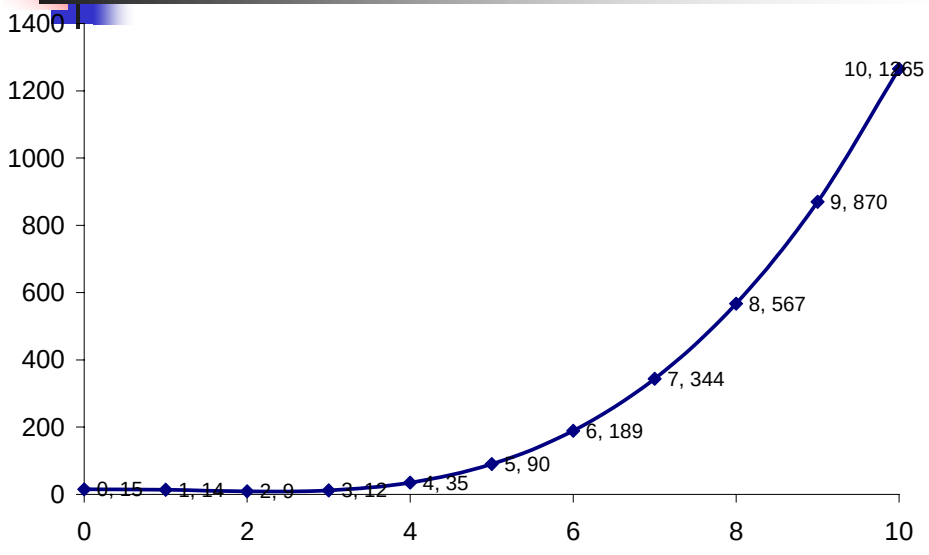
33

Shamir's secret sharing scheme

- Share i is a point (xi, yi) on the curve defined by F(x), where xi is not zero.
- Given any m points, the polynomial is uniquely determined and hence the value of F(0) = a0 (the secret) can be computed (using Lagrange interpolation).
- However, given up to (K-1) points, the polynomial parameters can not be determined.
- Thus, Shamir's scheme is a perfect secret sharing scheme.
- The arithmetic in Shamir scheme is defined over a finite field. i.e. Math is done Module some prime number P.

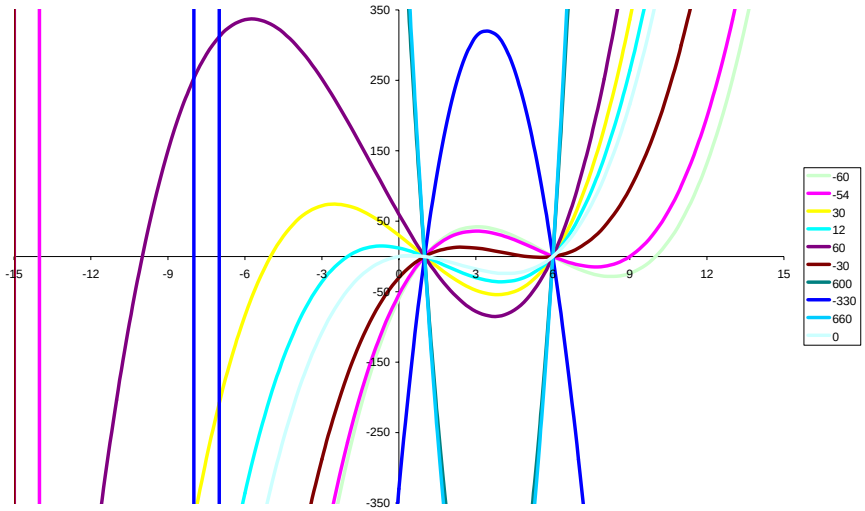
34

Polynomials of degree 3 requires at lest 4 points to find out the curve.
Any four of the 10 points will enable us to find the curve exactly.



10 Possible curves of polynomials of degree 4 knowing only three points (-5,0), (1,0) & (9,0). The legend shows the value of the polynomials when x = 0.

35



36

Secret recovery

- To recover the secret, we must use the shares, i.e. points, generated to reconstruct the polynomial described above and compute a0.
- In short, this technique yields the following formula for the secret S when the shares are K points of the form (xk, yk):

$$S = \sum_{k=1}^{m} y_k \prod_{j=1, j\neq k}^{m} \frac{-x_j}{x_k - x_j}$$