Assignment

Raju Shrestha
Roll No. 48

1.) Visual Secret sharing scheme :-

⇒ - Visual secret sharing (vss) is a cryptographic technique that allows a secret image to be divided into multiple shares, which individually do not reveal any information about the original image. The secret can only be reconstructed when a sufficient number of these shares are combined together. This concept was first introduced by Moni Naor & Adi shamir in 1994.

key concepts of visual secret sharing:-

1.) shares:- These are the pieces of the secret image, each of which looks like random noise. Each share by itself provides no information about the original image. The shares are typically printed on transparencies.

11.) Threshold Scheme :- In vss, the scheme is often defined by parameters (k,n), where,
n is the total number of shares generated.
k is the minimum number of shares required to construct the secret image.
For example, in a (3,5) scheme, 5 shares are generated & any 3 of them are sufficient to reconstruct the image.

111) Superimposition :- The secret image is reconstructed by superimposing (overlaying) the necessary number of shares. When the correct number of shares is overlaid, the secret image becomes visible. This process is usually done manually or with simple tools, without requiring any complex computation.

iv.) perfect security :- A fundamental feature of visual secret sharing is that any group of fewer than 'k' shares provides no information about the original image, ensuring perfect security. This means that the scheme is secure even against adversaries who may gain access to some of the shares.

How visual secret sharing works:-

i.) Secret image :- Start with the original image (often binary i.e. black & white) that you want to share securely.

ii.) Share creation:- The secret image is divided into multiple shares, usually two or more. Each share looks like random noise & does not reveal any information about the original image on its own. The number of shares created is determined by the scheme's parameters.

iii.) Reconstruction :- To reveal the secret, the shares are overlaid or combined. Depending on the visual secret sharing scheme used, a minimum number of shares (the threshold) must be combined to reconstruct the original image. The overlaying process can be done by hand or digitally using software.

Advantages:-

i.) No complex computations:- Visual secret sharing scheme requires only simple operations, such as splitting pixels

& overlaying shares, making it suitable for manual operations.

ii.) perfectSecurity :- Each share independently provides no information about the original image, ensuring strong security.

iii.) Easy verification :- The reconstructed image can be easily verified visually without the need for special equipment.

Applications:-

i.) Secure Image sharing :- Visual secret sharing can be used to securely share sensitive Images, such as identification photos or confidential documents.

ii.) Two-factor Authentication :- Visual secret sharing can be used in authentication systems where the possession of a share (eg. a printed transparency) is required alongside a password or PIN.

iii.) Watermarking :- Visual secret sharing can be applied to embed a watermark in an image that is only revealed when specific shares are combined.

2.) Threshold schemes with liars :-

=> Threshold schemes with liars is an extension of the traditional threshold cryptography & secret sharing schemes that is designed to handle situations where some of the participants (offen called liars) may provide false or incorrect information. The goal of such a scheme is to still allow the correct the correct reconstruction of the secret even when some participants are dishonest or compromised.

key concepts:-

i.) Threshold scheme :- A standard threshold scheme is defined by parameters (k,n), where;

- n is the total number of participants (or shares).
- k is the minimum number of shares required to reconstruct the secret.

In a typical (k,n) scheme, any subset of k shares can be used to reconstruct the secret, but any subset of fewer than k shares provides no information about the secret.

ii.) Liars :- Liars are participants who provide incorrect or deliberately false shares. These liars might be malicious or could have been compromised. The scheme needs to be robust against a certain number of such liars to ensure that the secret can still be accurately reconstructed.

iii.) Cheater detection :- A threshold scheme with liars often includes mechanism to detect & possibly exclude the liars from the reconstruction process. This could involve additional verification steps or using redundancy in the shares to identify inconsistencies.

iv.) Resilience :- The resilience of a scheme refers to its ability to tolerate a certain number of liars. For example, a (k,n) threshold scheme might be designed to tolerate t liars, meaning the secret can still be reconstructed as long as at least k out of the n participants provide correct information.

Example: Shamir's secret sharing with Liars
one of the most well-known secret sharing schemes is Shamir's secret sharing, which is based on polynomial interpolation. A threshold scheme with liars can be built on top of Shamir's scheme by adding redundancy & checks to handle dishonest participants.

i) Secret sharing:- The secret s is encoded as the constant term of a polynomial of degree k-1. The shares are points on this polynomial, & any k points can be used to reconstruct the polynomial & thus the secret.

ii) Redundancy & Error correction:- To handle liars, the scheme can add redundancy by distributing more than k shares, possibly using a higher-degree polynomial or incorporating error-correcting codes. This redundancy allows the scheme to correct or detect errors (from liars) during the reconstruction phase.

iii) Reconstruction :- During reconstruction, the participants provide their shares. The scheme uses the redundancy to cross-check the shares. If some shares are inconsistent (indicating the presence of liars), the scheme can detect these inconsistencies & correct them to reconstruct the correct secret.

iv) Cheater detection:- The scheme might use techniques like majority voting or consistency check across multiple shares to identify which participants are likely providing false information. Once identified, these liars shares can be excluded from the reconstruction process.

Applications:-

i) secure voting:- In a secure voting system, participants might try to cheat by submitting false votes. A theshold scheme with liars can ensure that the correct election outcome is computed, even if some votes (or voting machines) are compromised.

ii) Distributed key generation:- In a distributed key generation protocol, some parties might try to distrupt the key generation process by providing false shares. A threshold scheme with liars ensures that the correct key can still be generated.

iii) Secure multi-party computation:- In scenarios where multiple parties are computing a function on shared data, a threshold scheme with liars allows the correct result to be computed even if some parties provide false inputs. //

3) Access structure :-

⇒ Access structure is central to the design of secret sharing schemes. An access structure defines the conditions under which a secret can be reconstructed by a group of participants. specially, it determines which subsets of participants are authorized to reconstruct the secret & which are not.

Formal Definition:-

Given a set of participants $P = \{P_1, P_2, \dots P_n\}$, an access structure I is a collection of subsets of p such that;

- Monotonicity : If a set A is in I, then any superset of A is also in I. This means that if a certain group of participants can reconstruct the secret, then any larger group that includes this group can also reconstruct the secret.

- Authorized set : The subset in I are called authorized sets. These are the groups of participants who have enough information (or shares) to reconstruct the secret.

- unauthorized sets :- Subsets that are not in I are called authorized sets. These are the groups that do not have enough information to reconstruct the secret.

Types of Access structures:-

1) Threshold Access structure : This is the most common type of access structure. In a (k,n) threshold scheme, any subset of k or more participants is an authorized set, & any subset of fewer than k participants is unauthorized. The access structure can be defined as;

$$\Gamma = \{A \subseteq P \mid |A| \geq k\}$$

where $|A|$ denotes the cardinality of the set A.

ii.) General Access structure :- In a general access structure, the set of authorized subsets is not necessarily based on the number of participants but can be based on any criteria. For example, in a hierarchial organization, only certain combinations of participants (eg. a manager & an employee) might be authorized to access the secret.

Importance of Access structures:-

Understanding access structures is crucial in the design of secure systems because it ensures that only the intended groups of participants can reconstruct the secret. This concept is especially important in applications like;

- Secure voting systems:- Ensuring that only the correct combination of votes reveals the result.

- Distributed cryptographic keys:- Where only authorized combinations of participants can reconstruct the key.

- corporate secret sharing:- Ensuring that only certain groups within a corporation can access sensitive information.

Date
Page

A.) Schnorr's Identification scheme :-

⇒ Schnorr's Identification scheme is a cryptographic protocol used for identity verification. It is based on the difficultly of solving the discrete logarithm problem, which makes it secure under the assumption that this problem is hard to solve. Schnorr's scheme is an interactive protocol between two parties : a prover (who wants to prove their identity) & a verifier (who wants to verify the prover's identity).

Key concepts:-

- Discrete Logarithm problem:- Given a prime number p, a generator g of a cyclic group Zp^*, & an element $y = g^x$ in the group, finding x is called the discrete logarithm problem.

- public & private key:-
- private key:- x (a secret known on to the prover).
- public key:- $y = g^x \bmod p$ (shared with the verifier).

Steps of the schnorr's Identification scheme:-

1.) setup:-

- A large prime number p & a generator g of a subgroup of Zp^* are choosen.
- The prover has a private key x, & the corresponding public key is $y = g^x \bmod p$.

11.) commitment:-

- The prover randomly selects a value r & computes $a = g^x \bmod p$.

- The prover sends this value a (the commitment) to the verifier:

III.) Challenge:-

- The verifier sends a random challenge e (a non-negative integer) to the prover.

IV.) Response:-

- The prover computes the response $s = r + e \cdot x \bmod (p-1)$ & sends s to the verifier.

V.) Verification:-

- The verifier checks if $g^s \bmod p$ is equal to $a \cdot y^e \bmod p$.
- If the equation holds, the verifier accepts the identity of the prover. otherwise, the identity is rejected.

Schnorr's Identification Scheme:-

1.) Alice choose a random number, k, where $0 \le k \le q-1$, & she computes $\gamma = a^k \bmod p$. She sends cert (Alice) & γ to Bob.

II.) Bob verifies Alice's public key, v, on the certificate cert (Alice). Bob chooses a random challenge r, $1 \le r \le 2^t$, & he sends r to Alice.

III.) Alice computes $y = k + ar \bmod q$ & she sends the response y to Bob.

IV.) Bob verifies that $\gamma = a^y v^r \pmod{p}$. If so, then Bob "accepts"; otherwise, Bob "rejects".

Example:-

Suppose $p = 88667$, $q = 1031$ & $t = 10$. The element $a = 70322$ has order q in $\mathbb{Z}_p^*$. Suppose Alice's private key is $a = 755$; then

$$v = a^{-a} \bmod p$$
$$= 70322^{1031-755} \bmod 88667$$
$$= 13136$$

Now, Suppose Alice chooses the random number $k = 543$. Then she computes,

$$\gamma = a^k \bmod p$$
$$= 70322^{543} \bmod 88667$$
$$= 84109$$

And she sends γ, to Bob. Suppose Bob issues the challenge $r = 1000$. Then Alice computes,

$$y = k + ar \bmod q$$
$$= 543 + 755 \times 1000 \bmod 1031$$
$$= 851$$

And she sends y to Bob as her response. Bob then verifies that,

$$84109 \equiv 70322^{851}\ 13136^{1000} \pmod{88667}$$

Finally, Bob "accepts".

The schnorr's Identification scheme was designed to be very fast & efficient, both from a computational point of view & in the amount of information that needs to be exchanged in the scheme.