Secret Sharing Schemes

1 Motivation

Secret Sharing Schemes, are methods to share a secret. The question which arises first is why? If we want to share the secret to several people why not to give each the secret?

For example, look at the case when a big firm (like Microsoft) wants to share the access to the main safe (containing source code of $MS - Linux$). However, as they afraid one person will grab the contents of the safe, they prefer that only authorized group of people will be able to open the safe. This problem was first noted by Blakley and Shamir (independently) in 1979.

2 Simple Cases

Assume all the groups are in the same size. In that case we define $(k, n) - threshold\,scheme$ as a method for sharing a secret S to group of n people, in a way that each subgroup A of those n will be able to restore S iff $|A| \geq k$, and would get no information about S otherwise.

$Shamir\;(k, n) - threshold\,sceme$ is a very easy solution:

Let p be a prime number satisfying that $p > max(n, S)$

- Select at random $k - 2$ values - $a_1, a_2, \cdots, a_{k-1} \in Z_p$.
- Calculate the following polynomial: $q(x) = S + a_1 x + a_2 x^2 + \cdots + a_{k-1} x^{k-1}$
- Distribute the shares:

$$\begin{aligned} S_1 &= (x_1, q(x_1)) \\ S_2 &= (x_2, q(x_2)) \\ &\vdots \\ S_n &= (x_n, q(x_n)) \end{aligned}$$

Note that $q(0) = S$.

The reconstruction of the secret is done using Lagrange's procedure (Numerical Analysis) - given k points, we have an efficient algorithm to find the unique polynomial of degree $k - 1$ which pass through all of them.

Given k points (x_i, y_i), $\qquad i = 1, \cdots, k$:

$q(x) = \Sigma_{i=1}^{k} y_i \Pi_{j=1 j\neq i}^{k} \frac{x - x_j}{x_i - x_j}$

As we are interested in $q(0) = S$ we can directly compute:

$q(0) = \Sigma_{i=1}^{k} y_i \Pi_{j=1 j\neq i}^{k} \frac{-x_j}{x_i - x_j}$

Claim: Any group with less then k participants, cannot reconstruct the secret S.
Proof: Given $k-1$ shares (x_i, y_i), for each secret S, we can build a unique polynomial of degree $k-1$ for which $q(0) = S$. From the construction of the polynomial all polynomial are equiprobable.
Conclusion: $Shamir's\,(k,n) - threshold\,scheme$ is secure and its safety is not dependent in the computing power.

For $(n,n) - threshold\,schemes$ Shamir proposed the following algorithm (which is much simpler):

- Choose $n-1$ random shares - $a_1, a_2, \cdots, a_{n-1} \in Z_p$.
- Calculate - $a_n = S - (\Sigma_{i=1}^{n-1} a_i) \bmod p$.

Reconstruction:
According to the building of the scheme, it is easy to see that - $S = (\Sigma_{i=1}^{n} a_i) \bmod p$.
It is easily can be shown that the above is a secure $(n,n) - threshold$, as given less then n shares, for each value of a_n a new secret can be reconstruct.

3 Access Structures

Consider the case where we want to allow groups of different sizes to reconstruct the share. For example, if the company decided that it can trust the CEO and two directors, or 4 directors, or the CEO, his secretary, and a manger, And want those groups to be able to reconstruct the code for the safe.

$Access\,Structure\,\Gamma$ is a method of sharing a secret S among a set of n participants (denoted by $\mathcal{P}$), in such a way that the following properties are satisfied:

1. If an authorized subset of participants $B \subseteq \mathcal{P}$ pool their shares, they can determine S.
2. If an unauthorized subset of participants $B \subseteq \mathcal{P}$ pool their shares, they cannot gain any information about the value of S.

Note that if $B \in \Gamma$, i.e., B is a group of authorized people, than any subgroup C such $B \subseteq C \subseteq \mathcal{P}$, is also an authorized group of people. We define *minimal authorized subset* if for each $A \subset B$ when $B \in \Gamma$ holds $A \notin \Gamma$. We define the set of minimal authorized subset as the basis of Γ and denote it as Γ_0.

Question: Given Γ_0 how to build a secret sharing scheme satisfying the conditions for this access structure?
Answer: We show the Monotone Circuit Construction method. In this method, for each group in Γ_0 in size t, we create a $(t,t) - threshold\, scheme$. Example: If we want to let the subgroup $\{P_1, P_2, P_4\} \in \mathcal{P}$ to reconstruct the secret, we use Shamir's (3,3)-threshold, and give each of them a share.

Note that each person might get several shares, and he needs to remember, which share is used in each minimal authorized subset he is part of.

Another method is $Brickell\, Vector\, Space\, Construction$ presented at Stinson's book, page 345.

4 Visual Cryptography

A question which was asked at 1994 by Naor and Shamir, was is it possible to create secret sharing schemes, which requires no computer to reconstruct. This resolved in creating what is called $Visual\, Cryptography$. The secret is some picture (black and white, or grey level picture), and the shares are pixels, which look random, and contain no information about whether to consider the pixel as black or as white. Stacking the shares (printed on transparent) will give the original picture.

Their scheme is applicable for $(k,n) - threshold$ and even for access structures.[1]

[1]see $Visual\, Cryptography$, proceedings of EUROCRYPT'94, pp. 1-12