Secrect Sharing Progress

Joan Ngure

Report

Perfect Secrecy:

1. Choose a prime p.
2. Choose randomly $a_1, \cdots, a_{t-1} \in \mathbb{Z}_p$
3. Form $f(x) = D + \sum_{i=1}^{t-1} a_i x^i$ mod p
4. Choose $(x_l, x_z, \cdots, x_n)$ uniformly and randomly from among all permutations of n distinct elements from $\{1, 2, \cdots, p-1\}$. Let $D_i = (x_i, d_i)$, where $d_i = f(x_i)$.

How step 4 is done:
let n = 5, p = 7
The possible permutations will be

$$\frac{6!}{(6-5)!}$$

For example:

$$\begin{array}{c} 12345 \\ 43261 \\ 51324 \\ \vdots \end{array}$$

Let's randomly and uniformly choose 43261

$$\begin{array}{c} x_1 = 4 \\ x_2 = 3 \\ x_3 = 2 \\ x_4 = 6 \\ x_5 = 1 \end{array}$$

If our scheme is (3,5) and the polynomial is

$$q(x_i) = 5 + 3x_i + 2x_i^2$$

Then the participants will get the following shares:
$P_1(4,0), P_2(3,4), P_3(2,5), P_4(6,4), P_5(1,3)$

1. This scheme just like shamir's satisfys correctness. If any 3 or more participants pool their shares, they will always reconstruct the secret.

2. Any participants less than 3 learn nothing about the secret.

3. Can any 2 participants deceive participant 3? Let's assume P_1, P_2, P_3 agree to pool their shares and P_1, P_2 know the polynomial $q(x_i)$ hence know the secret. They therefore submit fabricated value $(x_1', q(x_1')), (x_2', q(x_2'))$ to P_3. Each possible secret $D' \in \{0,1,2,3,4,5,6\}$ defines a distinct polynomial $q_{D'}(x_i)$ of degree at most 2 passing through the point (0, D$'$) and the fabricated points above. If $D' \neq D$, such a polynomial $q_{D'}(x_i)$ can intersect $q_D(x_i)$ in at most 2 points. Participant 3 will only reconstruct the incorrect secret if only if $q_{D'}(x_i) = q_D(x_i)$ and $D' \neq D$.

Cheaters still manage to deceive other participants although they are detected with a high probability. A simple solution to do this is to include a dummy variable say s which is never used as the real value of the secret. Thus our secret is encoded in $D^1, D^2 \cdots D^t$ where $D^i = D$ for some i uniformly and randomly chosen and $D^j = s$ for $i \neq j$. Each element of this sequence is then divided into shares using the protocol in the beginning of the report. For example:

$$\text{Let s} = 3 \text{ Let D} = 3 \text{ sequence} = \{3,3,3,5,3,3,3,3\}$$

When k participants agree to pool their secrets together, they construct $D^1, D^2 \cdots$ one at a time until some $D^j \neq s$ is obtained and the protocol terminates since cheating has occurred and the D^j is not legal.

(Probability that cheaters succeed to cheat in the ith round and obtain the secret while others get the wrong secret.)
Let i denote the round $D^i = D$. i is a random variable whose value is unknown to the cheaters.
Let e_i denote the event that the protocol does not terminate before round i and the cheaters submit fabricated shares at round i.
let $p(t) = Pr(e_i)$. Then $p(t) < (1-e)^{-1}t^{-1}$
By induction on t:
Basis$(t = 1)$. $p(t) \leq l < (1-\epsilon)^{-1}$.

Induction (t > 1). Let P_t denote the probability with which the cheaters decide to submit fabricated shares at round 1. Let s_t denote the event that the protocol does not terminate in round 1. Then

$$
\begin{aligned}
p(t) =& Pr(i=1)Pr(e_i|i=1) + Pr(i>1)Pr(s_1|i>1)Pr(e_i|i>1 \text{ and } s_1) \\
=& t^{-1}p_1 + (t-1)t^{-1}(p_1\epsilon + (1-p_1))p(t-1) \\
<& t^{-1}(p_1 + (t-1)(p_1\epsilon + (1-p_1))(1-e)^{-1}(t-1)^{-1}) \\
<& t^{-1}(p_1 \times \frac{1-\epsilon}{1-\epsilon} + (p_1\epsilon + (1-p_1))(1-e)^{-1}) \times \frac{1-\epsilon}{1-\epsilon} \\
=& (1-\epsilon)^{-1}t^{-1}
\end{aligned}
$$