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:
Using our previous example p=7, thus we randomly choose possible permutations of (1 2 3 4 5 6). The total permutations will be 6!. Choosing:

$$\begin{aligned} x_1 &= (1\ 2\ 3\ 4\ 5\ 6) \\ x_2 &= (2\ 3\ 1\ 5\ 6\ 4) \\ x_3 &= (3\ 2\ 5\ 6\ 4\ 1) \\ x_4 &= (6\ 5\ 4\ 3\ 1\ 2) \end{aligned}$$

Using the first three participants:
$P_1(1,5), P_2(2,5), P_3(3,6)$

$$\begin{aligned} x_1 &\to P_1(1,5), P_2(2,5), P_3(3,6) \\ x_2 &\to P_1(1,6), P_2(2,6), P_3(3,4) \\ x_3 &\to P_1(1,4), P_2(2,4), P_3(3,1) \\ x_4 &\to P_1(1,1), P_2(2,1), P_3(3,2) \end{aligned}$$

For example using x_4 we can see:

$$\begin{aligned} \alpha(1) &= 6 \\ \alpha(2) &= 5 \\ \alpha(3) &= 4 \\ \alpha(4) &= 3 \end{aligned}$$

$$\alpha(5) = 1$$
$$\alpha(6) = 2$$

Thus we replace for example $P_1(1,5)$ with $P_1(1,1)$ since $\alpha(5) = 1$
$D_i = (x_i, f(x_i))$
Calculating using interpolation formula we get:

$$D_1 = 6$$
$$D_2 = 5$$
$$D_3 = 5$$
$$D_4 = 3$$

Our set of possible secrets is S $= \{6, 5, 3\}$.
Recall our secret was 6. In case the three participants pool their secrets and the result $D_i \notin$ S then cheating occurred. However, it is possible to cheat and get $D_i \in$ S. Thus there is a possibility of the cheater going undetected.