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 probability say ϵ of the cheater going undetected.
To increase the probability of detecting cheaters, we can add 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 $i \neq j$. When k participants agree to pool there 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.

Let i denote the round $D^i = D$
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

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