Secrect Sharing Progress

Joan Ngure

August 2019

Report

Let N be a finite set of participants. Let t be the threshold (authorized subset in N). A secret sharing scheme on N is a collection $(s_i)_{i \in N}$ of discrete random variables and satisfies the following condition:

1. Correctness:
   $\forall m \in N \ \forall S = \{i_1, \cdots, i_t\} \subseteq \{1, \cdots, n\}$ of size t,

   $Pr_{\mathbf{share(m)} \to (s_1, \cdots, s_n)}[\mathbf{Reconstruct}(s_{i_1} \cdots s_{i_t}) = m] = 1$

Shamir's secret sharing scheme fits in the above definition because it has two algorithms share and reconstruct.The set here is $\mathbb{Z}_p$ where p is prime. Share is a randomized algorithm:

1. Choose n distinct elements non-zero elements in $\mathbb{Z}_p$.
2. Choose randomly $a_1, \cdots, a_{t-1} \in \mathbb{Z}_p$
3. Form $f(x) = m + \sum_{i=1}^{t-1} a_i x^i$ mod p

User P_i receives the share, $(x_i, y_i = f(x_i))$; x_i is public.
Any authorized subset t can find the secret:

$$H(m|s_1, \cdots s_t) = 0$$

Any subset of t-1 learns nothing about the secret

$$H(m|s_1, \cdots s_{t-1}) = H(m)$$

Correctness is satisfied that any t shares always reconstruct the secret.

Example:
Let m $\in \mathbb{Z}_7$. Let m =6, t = 3, n = 5, $a_1 = 2, a_2 = 4$. The polynomial is :

$$f(x) = 6 + 2x + 4x^2$$

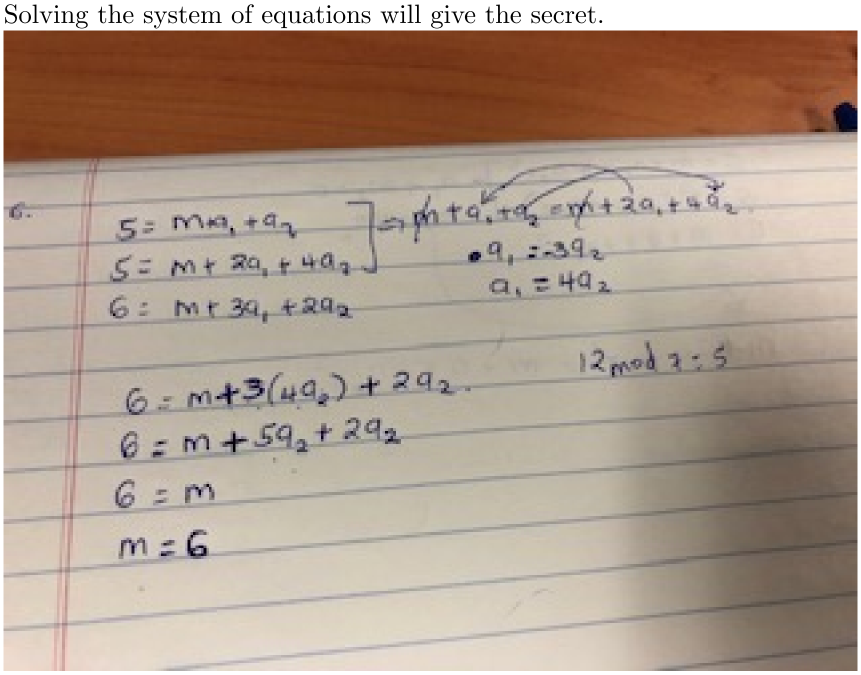
This polynomial will be used to generate shares. For instance:
x= 1 gives 5.
$P_1 : (1, f(1) = 5), P_2 : (2, f(2) = 5), P_3 : (3, f(3) = 6), P_4 : (4, f(4) = 1), P_5 : (5, f(5) = 4)$
Reconstruction:

$$f(x) = m + a_1 x + a_2 x^2$$

Using the first 3:

$$\begin{aligned}
5 &= m + a_1 + a_2 \\
5 &= m + 2a_1 + 4a_2 \\
6 &= m + 3a_1 + 2a_2
\end{aligned}$$

Solving the system of equations will give the secret.



Thus correctness is satisfied. Any t-1 (2 with 3 unknowns) cannot solve the system thus security is satisfied.