现代密码学

第五十一讲 Shamir秘密共享

信息与软件工程学院

第五十一讲 Shamir秘密共享

- 秘密共享的概念
- Shamir秘密共享方案

秘密共享的概念

- 问题1：

保险柜中存放有10个人的共有财产，要从保险柜中取出物品，必须有半数以上的人在场才可取出，半数以下则不行。如何构造锁的设计方案？

秘密共享的概念

- 问题2：

导弹的发射控制、重要安保场所的通行检验，通常需要多人同时参与才能生效。因此，需要将秘密分给多人掌管，并且由一定掌管秘密的人数同时到场才能恢复秘密。方案如何设计？

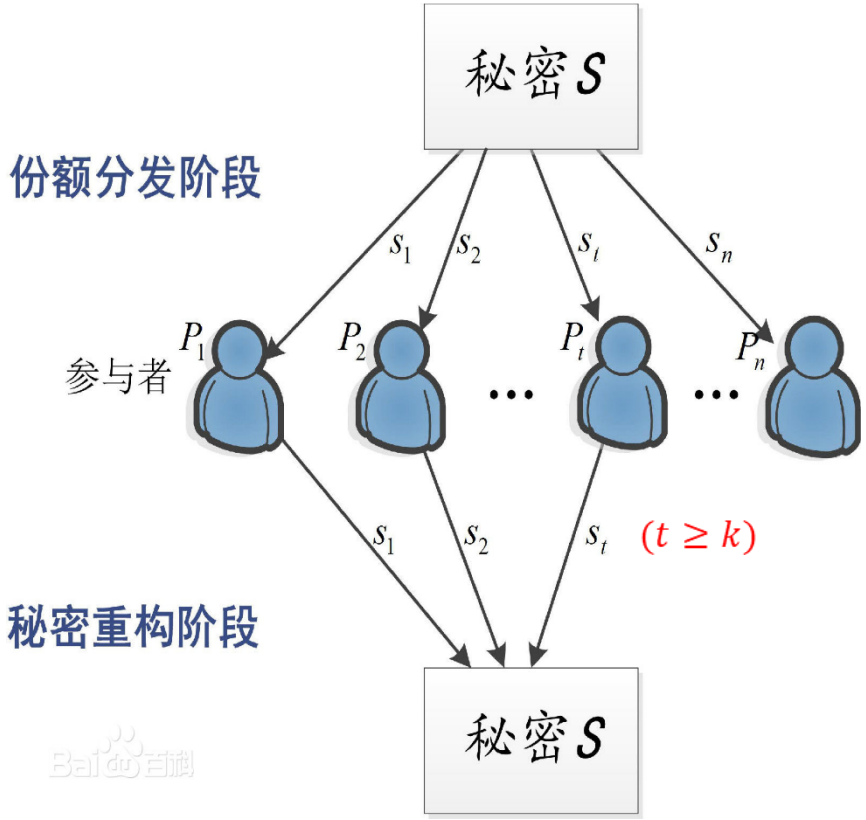
秘密共享的概念

秘密分割门限方案的定义

秘密s（通过某种方案）被分为n个部分，每个部分称为份额(share)或影子(shadow)，由一个参与者持有，使得

- 由k个或多于k个参与者所持有的部分信息可重构s；
- 由少于k个参与者所持有的部分信息则无法重构s，

称该方案为(k,n)秘密分割门限方案，k称为门限值。少于k个参与者所持有的部分信息得不到s的任何信息称该门限方案是完善的。

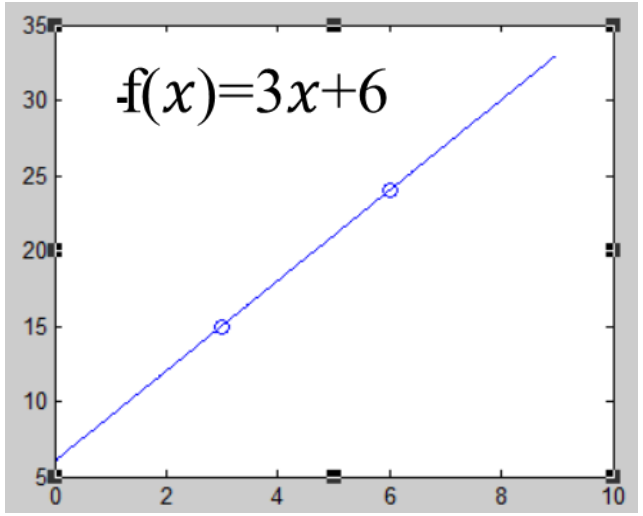


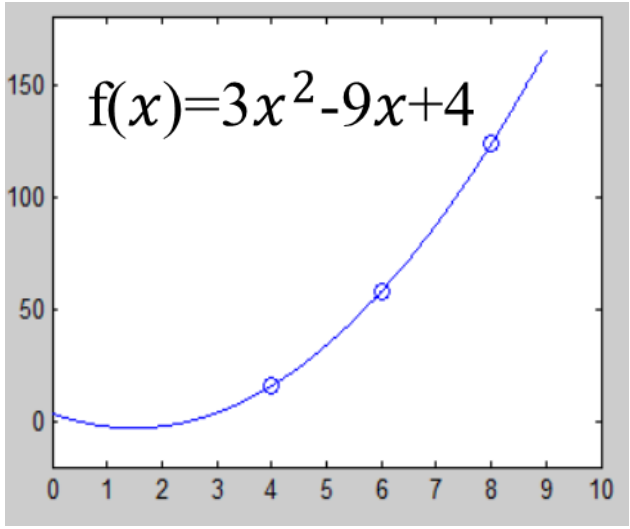
第五十讲 Diffie-Hellman 密钥交换

- 秘密共享的概念
- Shamir秘密共享方案

Shamir门限方案

Shamir门限方案的构造思路





一般的，设$\{(x_1, y_1), \ldots, (x_k, y_k)\}$是平面上$k$个不同的点构成的点集，那么在平面上存在唯一的$k-1$次多项式$f(x) = a_0 + a_1 x + \cdots + a_{k-1} x^{k-1}$通过这$k$个点.

若把秘密s取做$f(0)$，n个份额取做 $f(i)$ $(i = 1, \ldots n)$，那么利用其中任意k个份额可以重构$f(x)$，从而可以得到秘密s.

Shamir门限方案

Shamir门限方案

- 设$GF(q)$为大素数q生成的有限域，其中$q \geq n+1$.
- 秘密s是$GF(q)/\{0\}$上均匀选取的随机数，即$s \in_R GF(q)/\{0\}$.
- 在$GF(q)$上构造一个$k-1$次多项式$f(x)=a_0+a_1x+\cdots+a_{k-1}x^{k-1}$，其中：$a_0$ =s，$a_i \in_R GF(q)/\{0\}\ (i \neq 0)$
- n个参与者$P_1,\ldots,P_n$，其中，P_i的份额为$f(i)$。任意k个参与者要得到秘密s，可使用

$$\begin{cases} a_0+a_1(i_1)+\cdots+a_{k-1}(i_1)^{k-1}=f(i_1) \\ \vdots \\ a_0+a_1(i_k)+\cdots+a_{k-1}(i_k)^{k-1}=f(i_k) \end{cases}$$

Shamir门限方案

由Lagrange插值公式：

$$f(x)=\sum_{j=1}^{k} f(i_j)\prod_{\substack{l=1\\ l\neq j}}^{k}\frac{(x-i_l)}{i_j-i_l}\pmod q$$

故，

$$s=(-1)^{k-1}\sum_{j=1}^{k} f(i_j)\prod_{\substack{l=1\\ l\neq j}}^{k}\frac{i_l}{i_j-i_l}\pmod q$$

Shamir门限方案

Shamir门限方案的完善性

- 如果$k-1$个参与者想获得s，可构造$k-1$个方程，有k个未知量。
- 对任意s_0，设$f(0)=s_0$. 这样可以得到第k个方程，得到$f(x)$。
- 对每个s_0都有唯一的多项式满足，所有由$k-1$个份额得不到任何s的信息。
- 因此，该方案是完善的。

Shamir门限方案

- 例子: (3,5) 门限方案

设$k=3, n=5, q=19, s=11$。随机选择系数 $a_1=2, a_2=7$，则

$$f(x)=7x^2+2x+11 \bmod 19。$$

计算可知：$f(1)=1$，$f(2)=5$，$f(3)=4$，$f(4)=17$，$f(5)=6$

若已知$f(2), f(3), f(5)$，由拉格朗日插值公式可知：

$$f(x)=5\frac{(x-3)(x-5)}{(2-3)(2-5)}+4\frac{(x-2)(x-5)}{(3-2)(3-5)}+6\frac{(x-2)(x-3)}{(5-2)(5-3)}$$

$$=7x^2+2x+11$$

故，$s=f(0)=11.$

或者，$$s=(-1)^{3-1}[5\frac{3\times5}{(2-3)(2-5)}+4\frac{2\times5}{(3-2)(3-5)}+6\frac{2\times3}{(5-2)(5-3)}]=11$$

Shamir门限方案

课后练习

假定房间里有4个人，其中一个是国外特务，其余3人拥有Shamir秘密分享方案的数对，任何两个人都能确定秘密。国外特务随机选择了一个数对，人员和数对如下。所有的数对都是模11的。

A：（1，4） B：（3，7） C：（5，1） D：（7，2）

确定哪一个是特务，秘密是什么？

感 谢 聆 听!

djchen@uestc.edu.cn