



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

A decorative blue horizontal bar with white horizontal stripes is positioned to the left of the title.

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？

A decorative blue horizontal bar with white horizontal stripes is positioned to the left of the title.

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？

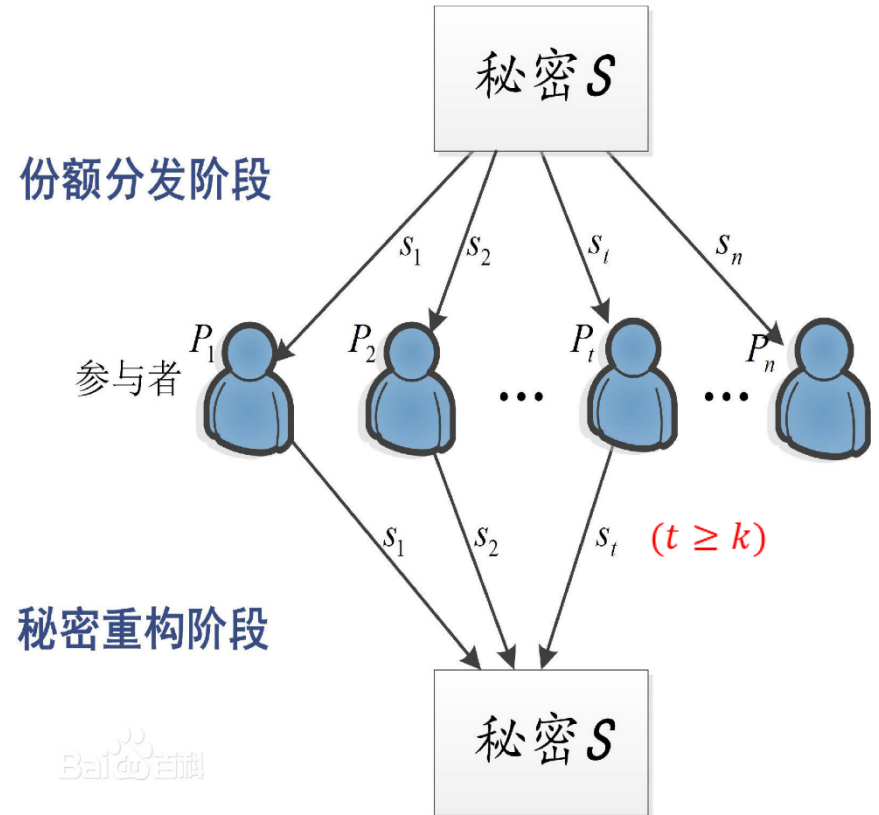
秘密共享的概念

□ 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**。



A decorative graphic consisting of several horizontal blue lines of varying lengths, stacked vertically, is positioned in the top left corner.

第五十讲 Diffie-Hellman 密钥交换

A vertical line with two white circles is positioned on the left side of the slide. The top circle is connected to the top blue bar, and the bottom circle is connected to the bottom blue bar.

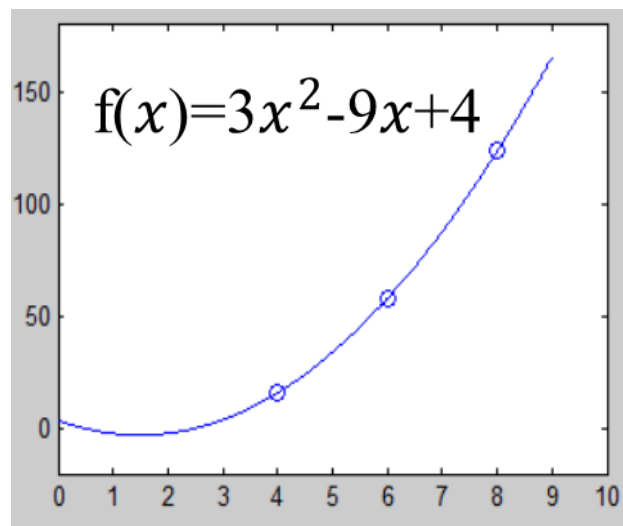
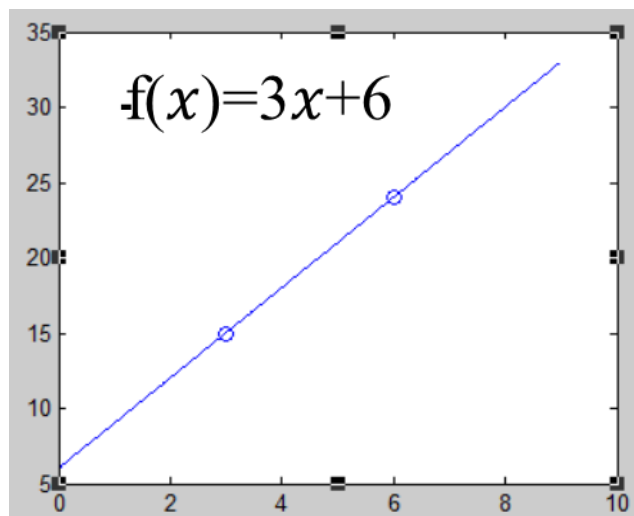
秘密共享的概念

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 $\{(x_1, y_1), \dots, (x_k, y_k)\}$ 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 $f(x) = a_0 + a_1x + \dots + a_{k-1}x^{k-1}$ 通过这 k 个点。

若把秘密 s 取做 $f(0)$ ， n 个份额取做 $f(i)$ ($i = 1, \dots, n$)，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, \dots, 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,

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

A decorative blue horizontal bar with white horizontal stripes is positioned to the left of the title.

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:

$$\begin{aligned} f(x) &= 5 \frac{(x-3)(x-5)}{(2-3)(2-5)} + 4 \frac{(x-2)(x-5)}{(3-2)(3-5)} + 6 \frac{(x-2)(x-3)}{(5-2)(5-3)} \\ &= 7x^2 + 2x + 11 \end{aligned}$$

故, $s = f(0) = 11$.

$$\text{或者, } s = (-1)^{3-1} \left[5 \frac{3 \times 5}{(2-3)(2-5)} + 4 \frac{2 \times 5}{(3-2)(3-5)} + 6 \frac{2 \times 3}{(5-2)(5-3)} \right] = 11$$



Shamir门限方案

□ 课后练习

假定房间里有4个人，其中一个国外特务，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
