Shamir 秘密共享算法

Shamir’s Secret Share (SSS)

—可厉害的土豆

Bilibili可厉害的土豆

目录

- 背景介绍
- 基本原理
- 计算示例
- 参考资料

Bilibili可厉害的土豆

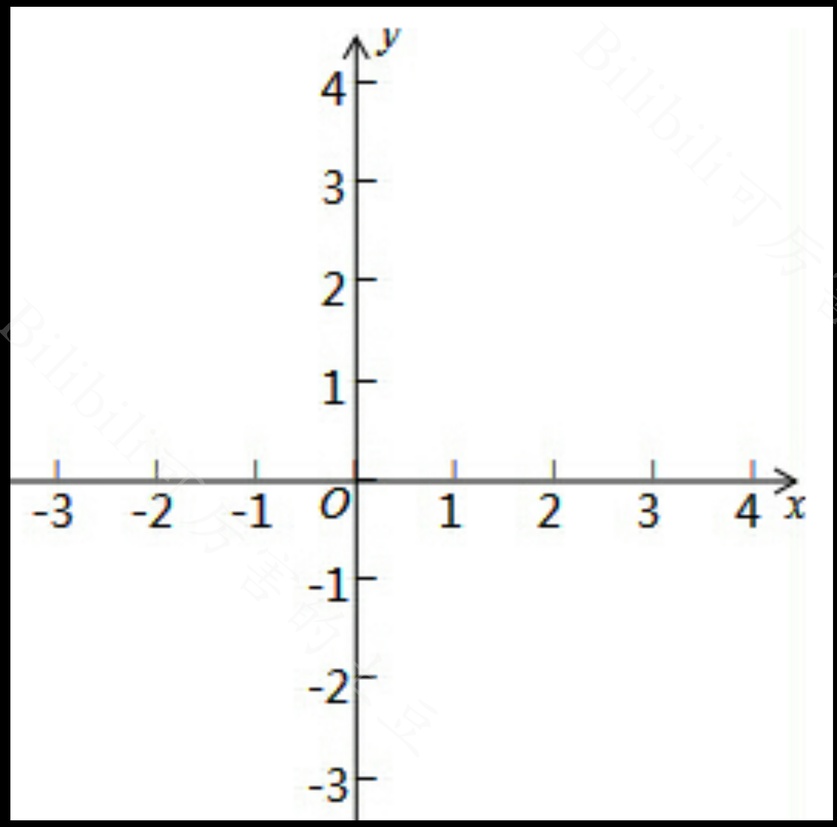
背景介绍

- 由著名密码学家 Adi Shamir 于 1979年提出。
- 用于实现 门限秘密共享。

Bilibili可厉害的土豆

基本原理

- 基本数学属性： k-1次多项式 需要由k个点唯一确定。



Bilibili可厉害的土豆

基本原理

$Y = aX^2 + bX + S$　　a,b 为随机数，S为需要保守的秘密

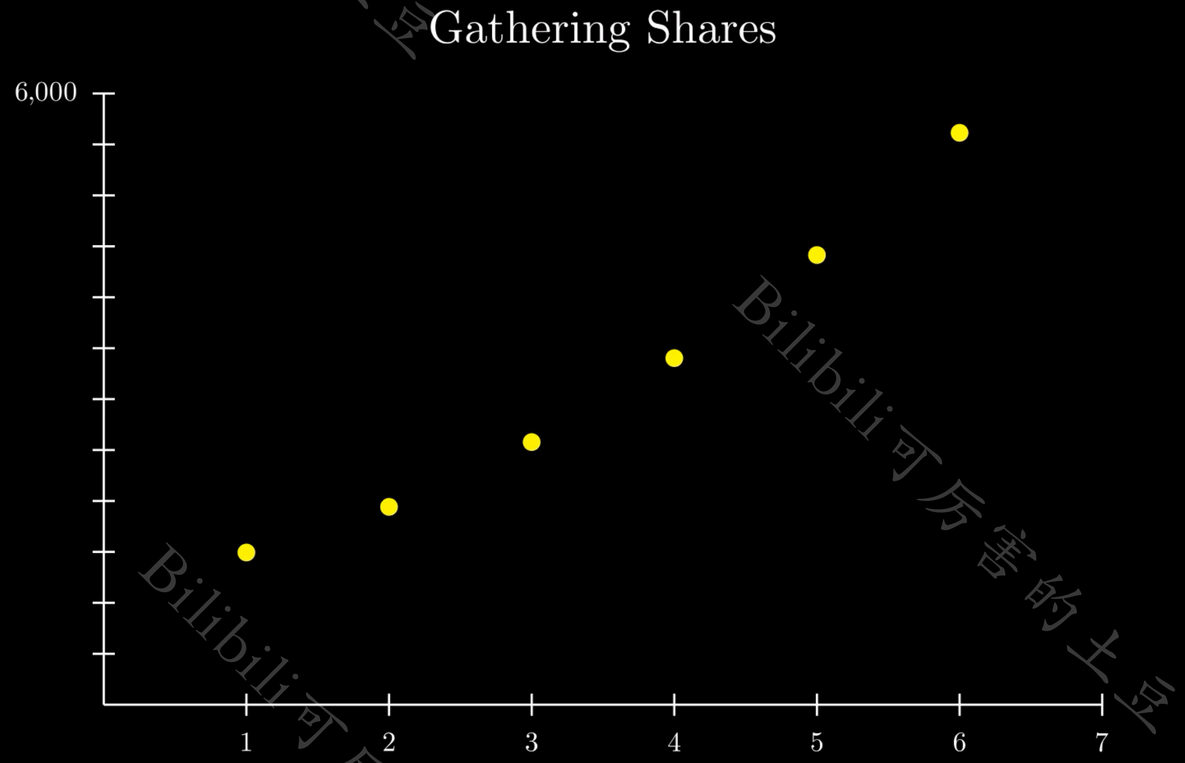
$Y = 94X^2 + 166X + 1234$　　假如将秘密分为 6 份

（1，1494）
（2，1942）
（3，2578）
（4，3402）
（5，4414）
（6，5614）

Bilibili可厉害的土豆

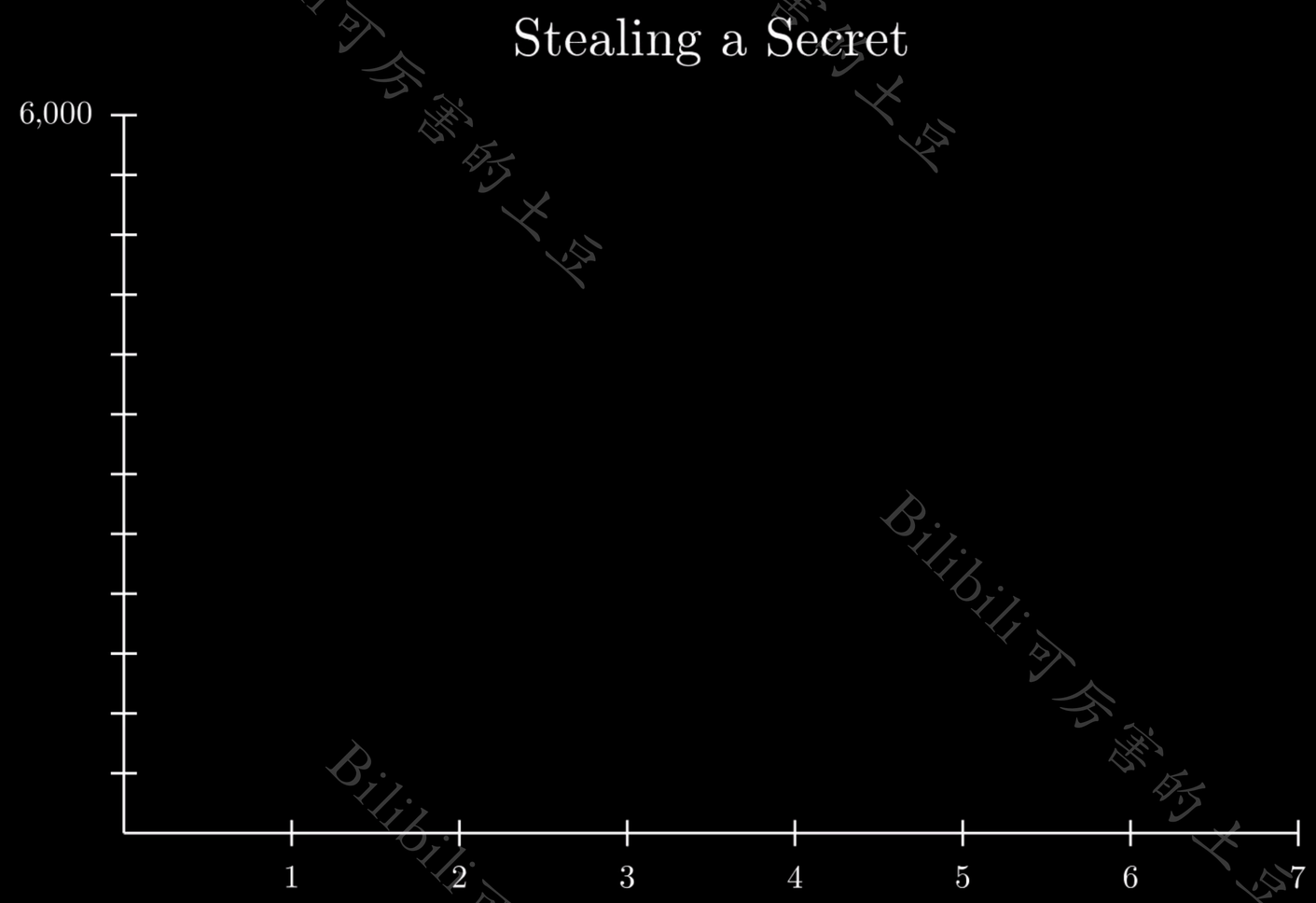
基本原理

$$Y = 94X^2 + 166X + 1234$$



Bilibili可厉害的土豆

基本原理



Bilibili可厉害的土豆

基本原理

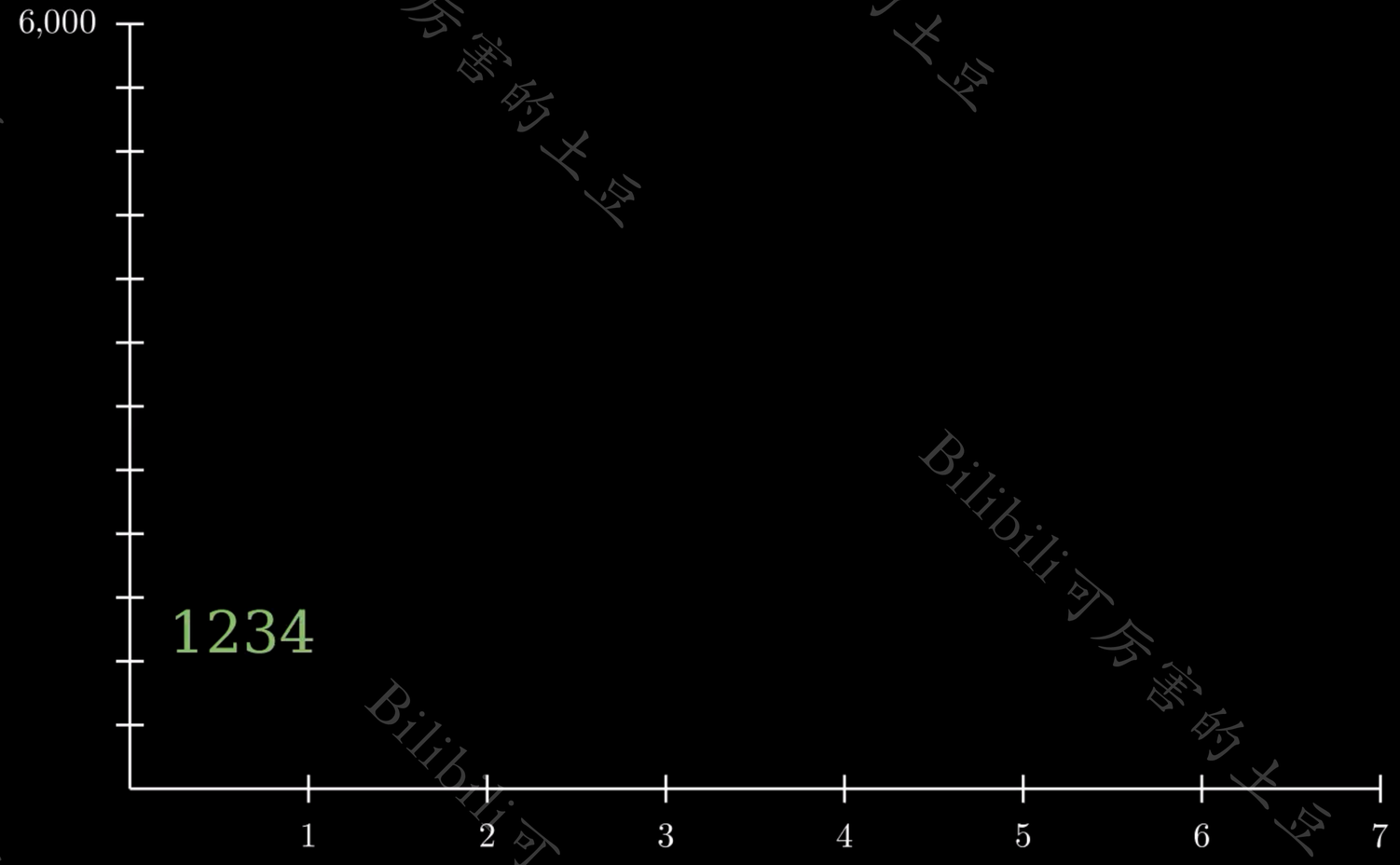
将多项式定义在有限域上，通过应用模数 (取余数) 将 普通多项式 转换为 循环多项式，使得这些点从 有规律，可穷举 的上图 转换为 无规律，难穷举的下图。

$$Y = aX^2 + bX + S \bmod p$$

Bilibili可厉害的土豆

基本原理

Secure Secret Sharing



Bilibili可厉害的土豆

基本原理

- 拉格朗日插值法计算基多项式

拉格朗日插值法的公式如下，用于计算基多项式 $L_i(x)$：

$$L_i(x) = \prod_{\substack{j=1 \\ j \neq i}}^{n} \frac{x - x_j}{x_i - x_j}$$

其中 n 是提供碎片的总数，x_i 和 x_j 是碎片对应的 x 值。

- 假如有t个秘密碎片，则秘密S的计算公式如下：

$$S = \sum_{i=1}^{t} y_i \cdot L_i(0) \pmod{p}$$

Bilibili可厉害的土豆

计算示例

$$Y = 2X^2 + 3X + 2 \bmod 23$$

假如将秘密分为 4 份

(1，7)
(2，16)
(3，6)
(4，0)

(1，7)
(3，6)
(4，0)

利用三组数据进行秘密恢复

Bilibili可厉害的土豆

计算基多项式

$$L_i(x) = \prod_{\substack{j=1 \\ j \neq i}}^{n} \frac{x - x_j}{x_i - x_j}$$

(1，7)
(3，6)
(4，0)

Bilibili可厉害的土豆

计算秘密S

$$S = \sum_{i=1}^{t} y_i \cdot L_i(0) \pmod{p}$$

(1，7)
(3，6)
(4，0)

Bilibili可厉害的土豆

1. 秘密生成多项式：

- 选择一个素数 p，作为模数。
- 构造一个多项式 $F(x) = S + a_1x + a_2x^2 + \ldots + a_{t-1}x^{t-1}$，其中 S 是原始秘密，a_i 是随机选择的系数。

2. 计算份额：

- 为每个参与者 i（i 从1到 n，其中 n 是参与者总数）选择一个唯一的标识符 x_i。
- 计算每个 x_i 对应的多项式值 $y_i = F(x_i)$，并将 (x_i, y_i) 作为份额分发给第 i 个参与者。

3. 秘密恢复：

- 当 t 个或更多的参与者合作时，他们可以使用拉格朗日插值法来恢复秘密：
  - 构造基多项式 $L_i(x)$，使得对于每个 i，$L_i(x_i) = 1$ 且对于所有 $j \neq i$，$L_j(x_i) = 0$。
  - 使用基多项式和每个参与者的份额 y_i，通过以下公式计算秘密：$S = \sum_{i=1}^{t} y_i \cdot L_i(0) \mod p$

Bilibili可厉害的土豆

参考资料

[1] Edony. (2023, November 11). 可视化理解 Shamir's Secret Share 密钥共享算法的数学原理. https://www.edony.ink/visual-understanding-shamirs-secret-share-algorithm/

[2] Wagner, L. (2022, May 23). Shamir 的秘密共享密码算法简介. HACKERNOON. https://www.edony.ink/visual-understanding-shamirs-secret-share-algorithm/

[3] 橘小白. (2019, April 17). Shamir门限秘密共享方案 秘密分配及还原过程详解 【橘小白】. CSDN. https://blog.csdn.net/kety_gz/article/details/89366868

Bilibili 可厉害的土豆

“
感谢观看
祝你
每顿吃饱
每晚睡好
身体健康
学业有成
工作顺利
天天开心
”

—可厉害的土豆

Bilibili可厉害的土豆

例：$f(x)=2+3x+2x^2 \bmod 23$　(2,7)(3,6)(4,0)

(1) 取 $x_1=1, x_2=2, x_3=3, x_4=4$　4个秘密碎片

得 $y_1=7, y_2=16, y_3=6, y_4=0$

假设用 (1,7) (3,6) (4,0) 作为恢复秘密的碎片

(2) 使用拉格朗日插值法计算基函数式：$L_i(x)=\prod_{\substack{j=1 \\ j\neq i}}^{n} \frac{x-x_j}{x_i-x_j}$

$$L_1(0)=\frac{x-x_3}{(x_1-x_3)}\times\frac{x-x_4}{(x_1-x_4)}=\frac{(0-3)(0-4)}{(1-3)(1-4)}=2$$

$$L_3(0)=\frac{x-x_1}{(x_3-x_1)}\times\frac{x-x_4}{(x_3-x_4)}=\frac{(0-1)(0-4)}{(3-1)(3-4)}=-2$$

$$L_4(0)=\frac{(x-x_1)}{(x_4-x_1)}\times\frac{x-x_3}{(x_4-x_3)}=\frac{(0-1)(0-3)}{(4-1)(4-3)}=1$$

(3) 计算 $S=\sum_{i=1}^{t} y_i \times L_i(0) \bmod p$

$$=[y_1\times L_1(0)+y_3\times L_3(0)+y_4\times L_4(0)] \bmod 23$$

$$=(7\times 2-6\times 2+0) \bmod 23$$

$$=2$$

∴ 求得秘密 $S=2$.

Bilibili可厉害的土豆