海联金汇
HYUNION HOLDINGS
股票代码：002537

UMF 联动优势
UNION MOBILE FINANCIAL TECHNOLOGY
海联金汇旗下企业

科技赋能普惠金融

分布式数字身份体系与密钥找回机制

王宇

MAKE
FINTECH
EVERYWHERE

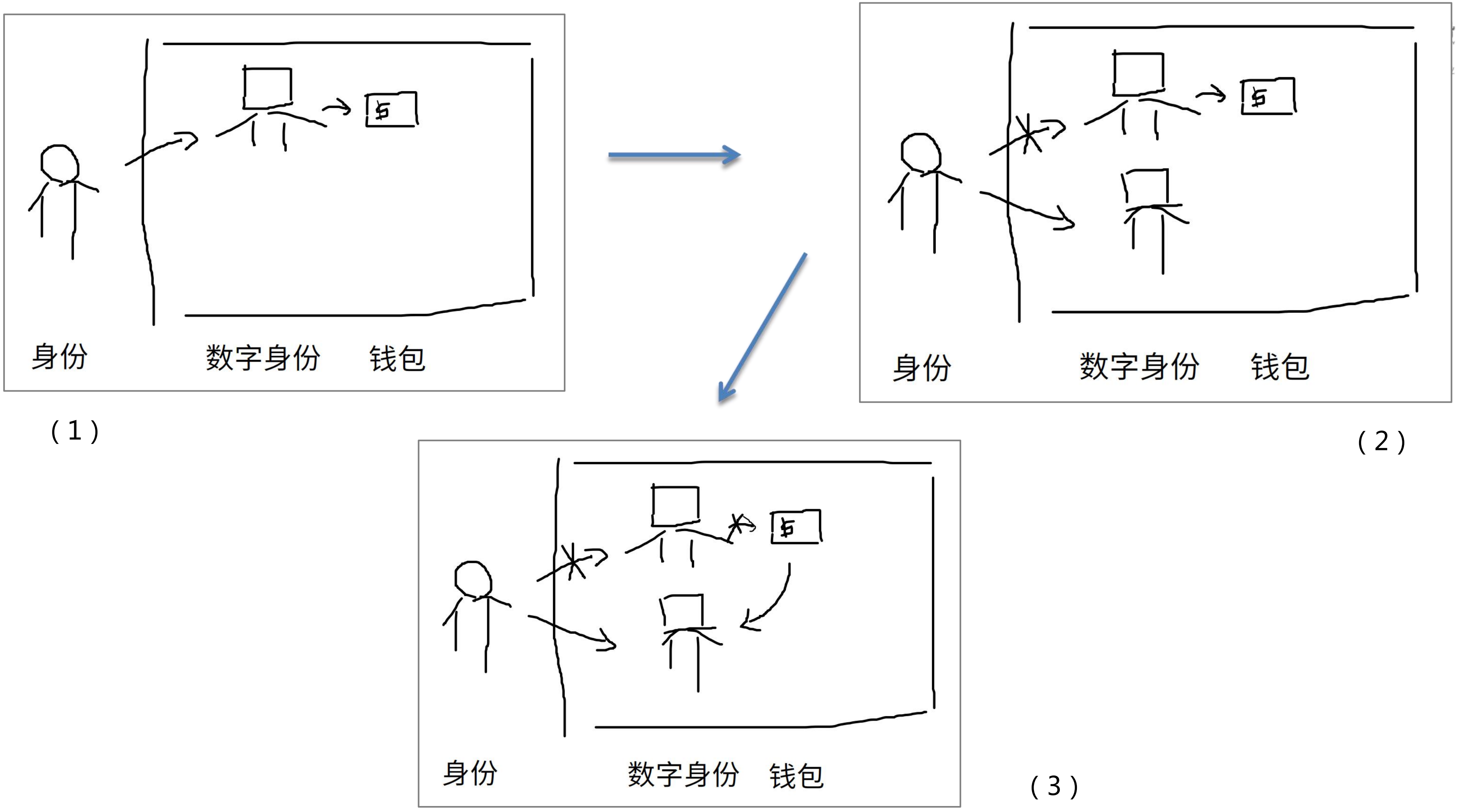
回顾

身份　　数字身份

目录

数字身份找回

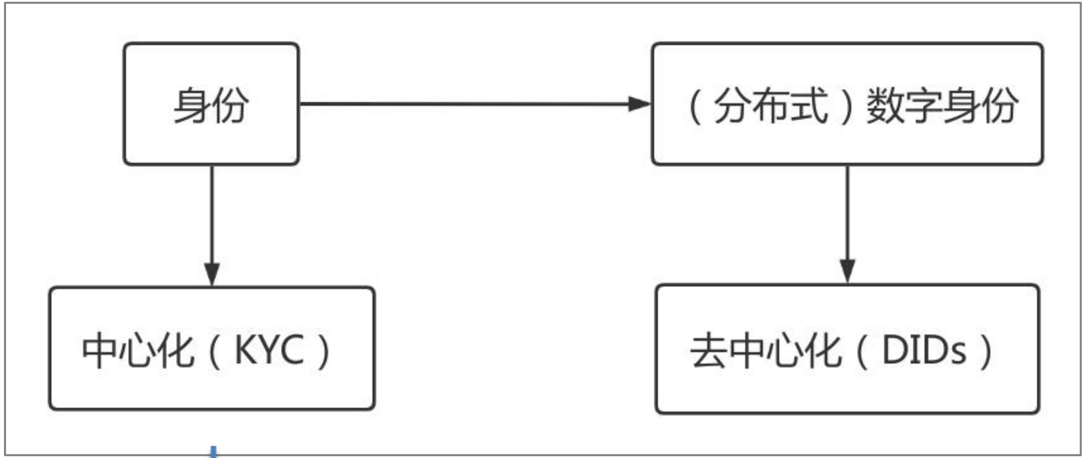
先看一种找回数字身份的方法（下一页）


身份
数字身份
钱包
（1）
身份
数字身份
钱包
（2）
身份
数字身份
钱包
（3）

先说结论

这种方法 不适用 于分布式数字身份（自主主权的数字身份，SSI）

分析



身份和数字身份的对应关系如何确定：

1. “身份”自己确认
2. “身份”需要 第三方 确认

找回数字身份涉及两种类型的操作：

1. 停用旧的身份
2. 转移数字资产到新的身份

1. “身份”需要KYC确认
2. 中心化机构拥有KYC信息

1. 去中心化节点没有KYC信息
2. 去中心化节点没有转移数字资产的能力

？

目前的结论

既需要 中心化系统的权力（认证身份+转移资产）
又需要 去中心化系统的自主主权（SSI）

是冲突的

目录

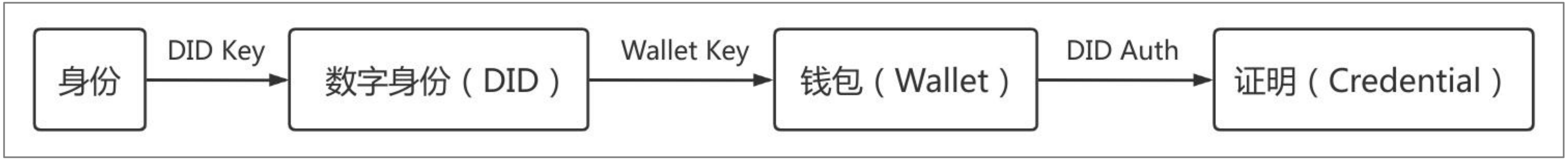
钱包丢失

钱包丢失：

1. 被偷
2. 丢了

钱包被偷

相关权限控制：



在其他设备上，注销钱包（by Sovrin）

钱包丢失

删号重来

目录

相关论文

Practical Key Recovery Model for Self-Sovereign Digital Wallets

Reza Soltani
Lassonde School of Engineering
York University
Toronto, Canada
Email: rts@cse.yorku.ca

Uyen Tran Nguyen, Aijun An
Lassonde School of Engineering
York University
Toronto, Canada
Email: utn@cse.yorku.ca

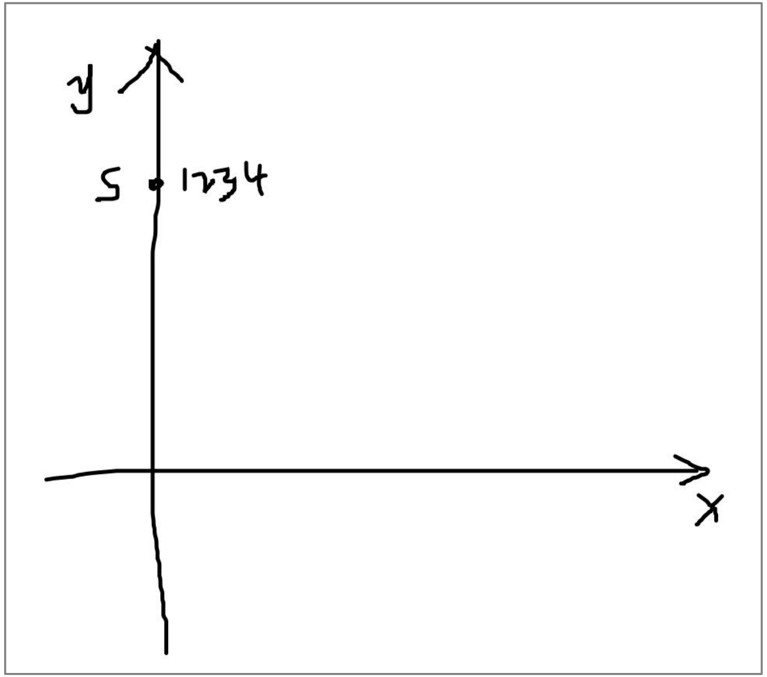
密钥备份和找回方式

1. 安全模块和可信执行环境（ARM TrustZone、Intel SGX）
2. 生物信息保护（指纹、照片）
3. 云环境备份
4. 助记符和二维码（CoinUs）
5. 阈值密钥分享（Shamir、Blakley、Chinese remainder theorem）

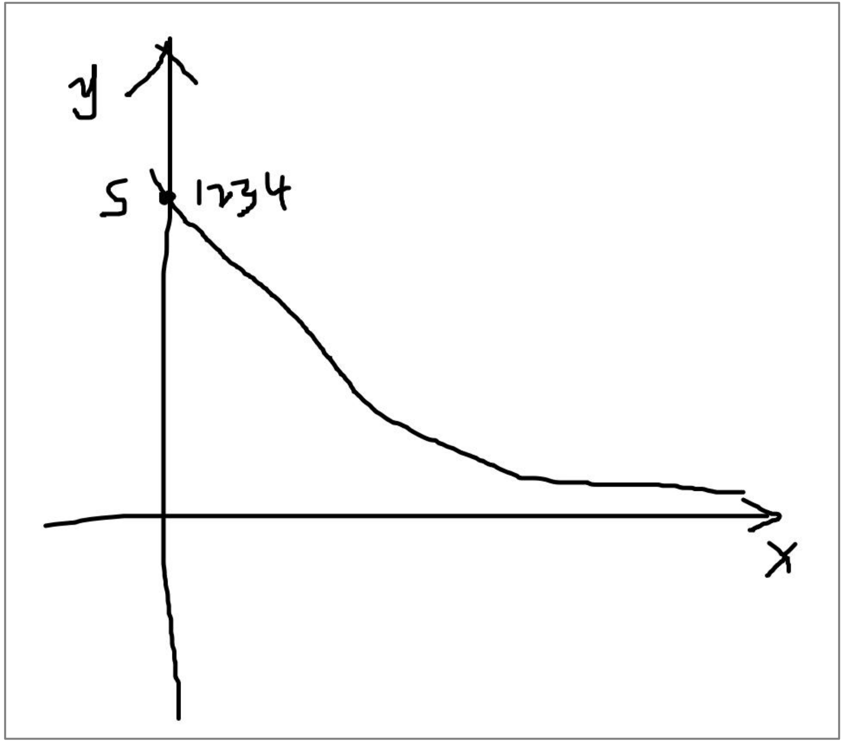
介绍一下

Shamir's Secrect Sharing

准备分享数据

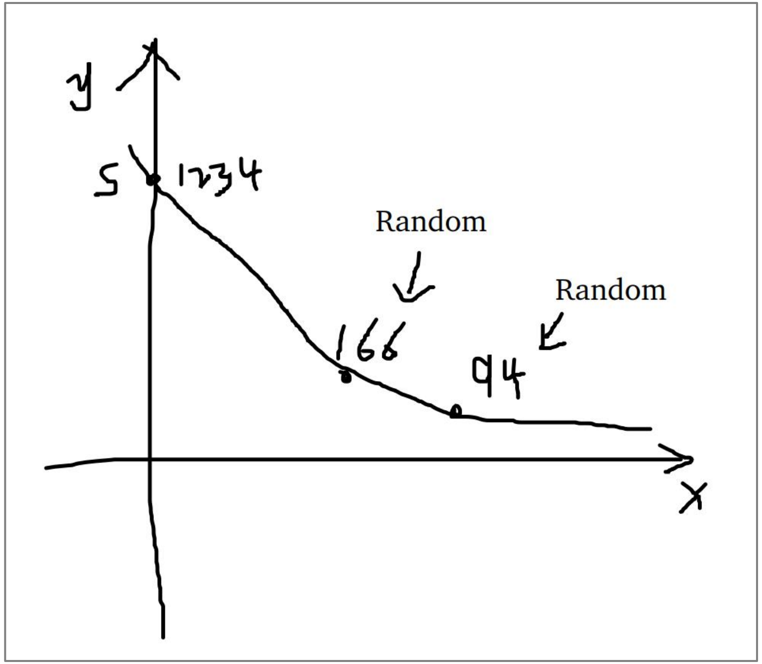


（1）



（2）

分享数据

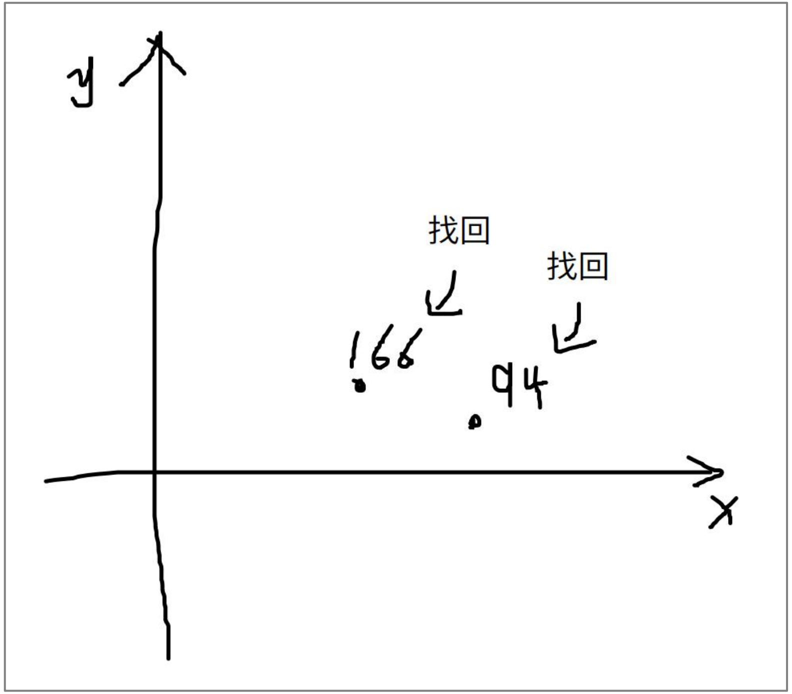


把随机的取点 166 和 94
分别交给信任的人保存

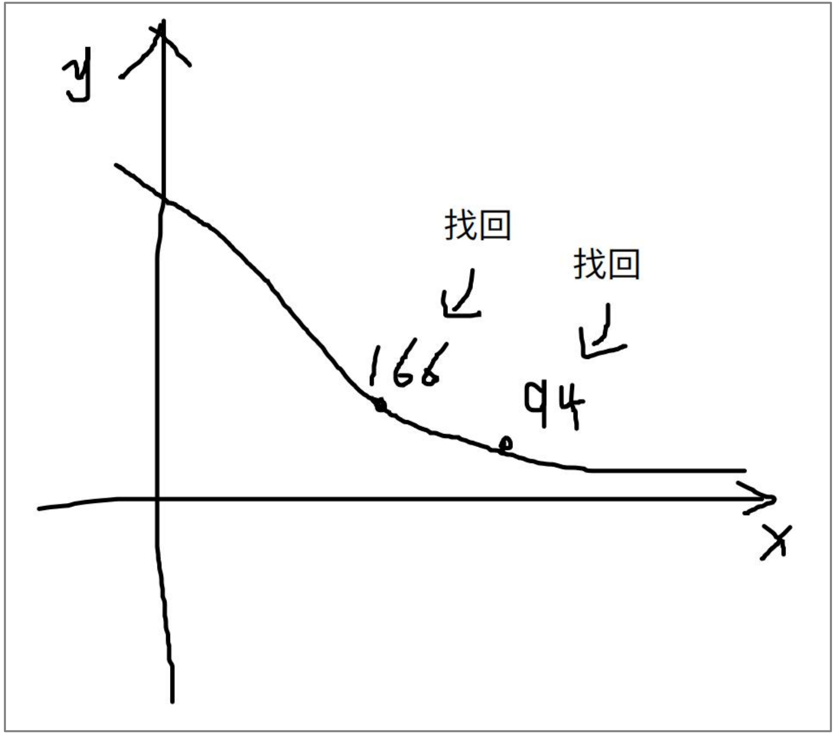
（3）

（4）

准备找回数据

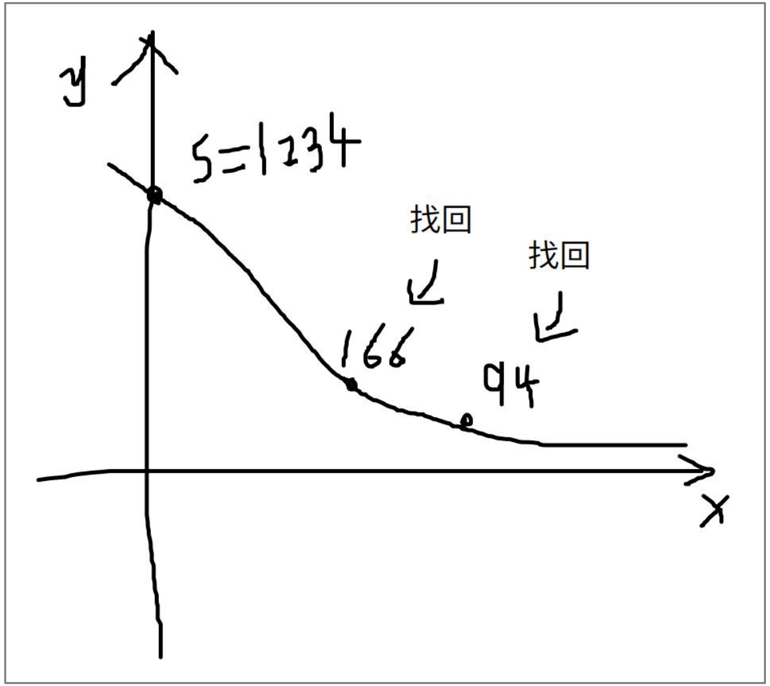


（5）



（6）

找回数据



根据找回的 166 和 94，画出曲线，找回密码 1234

（7） （8）

数学原理

拉格朗日插值法（Lagrange polynomials）：

对于给定的 n+1 个点，对应于它们的次数不超过 n 的拉格朗日多项式 L 只有一个。

维基百科上的示例

Preparation [edit]

Suppose that our secret is 1234 $(S = 1234)$.

We wish to divide the secret into 6 parts $(n = 6)$, where any subset of 3 parts $(k = 3)$ is sufficient to reconstruct the secret. At random we obtain $k - 1$ numbers: 166 and 94.

$(a_0 = 1234; a_1 = 166; a_2 = 94)$, where a_0 is secret

Our polynomial to produce secret shares (points) is therefore:

$$f(x) = 1234 + 166x + 94x^2$$

We construct six points $D_{x-1} = (x, f(x))$ from the polynomial:

$$D_0 = (1, 1494); D_1 = (2, 1942); D_2 = (3, 2578); D_3 = (4, 3402); D_4 = (5, 4414); D_5 = (6, 5614)$$

We give each participant a different single point (both x and $f(x)$). Because we use D_{x-1} instead of D_x the points start from $(1, f(1))$ and not $(0, f(0))$. This is necessary because $f(0)$ is the secret.

Reconstruction [edit]

In order to reconstruct the secret any 3 points will be enough.

Consider $(x_0, y_0) = (2, 1942)\,;(x_1, y_1) = (4, 3402)\,;(x_2, y_2) = (5, 4414)$.

We will compute Lagrange basis polynomials:

$$\ell_0(x) = \frac{x-x_1}{x_0-x_1} \cdot \frac{x-x_2}{x_0-x_2} = \frac{x-4}{2-4} \cdot \frac{x-5}{2-5} = \frac{1}{6}x^2 - \frac{3}{2}x + \frac{10}{3}$$

$$\ell_1(x) = \frac{x-x_0}{x_1-x_0} \cdot \frac{x-x_2}{x_1-x_2} = \frac{x-2}{4-2} \cdot \frac{x-5}{4-5} = -\frac{1}{2}x^2 + \frac{7}{2}x - 5$$

$$\ell_2(x) = \frac{x-x_0}{x_2-x_0} \cdot \frac{x-x_1}{x_2-x_1} = \frac{x-2}{5-2} \cdot \frac{x-4}{5-4} = \frac{1}{3}x^2 - 2x + \frac{8}{3}$$

Therefore

$$\begin{aligned} f(x) &= \sum_{j=0}^{2} y_j \cdot \ell_j(x) \\ &= y_0\ell_0(x) + y_1\ell_1(x) + y_2\ell_2(x) \\ &= 1942\left(\frac{1}{6}x^2 - \frac{3}{2}x + \frac{10}{3}\right) + 3402\left(-\frac{1}{2}x^2 + \frac{7}{2}x - 5\right) + 4414\left(\frac{1}{3}x^2 - 2x + \frac{8}{3}\right) \\ &= 1234 + 166x + 94x^2 \end{aligned}$$

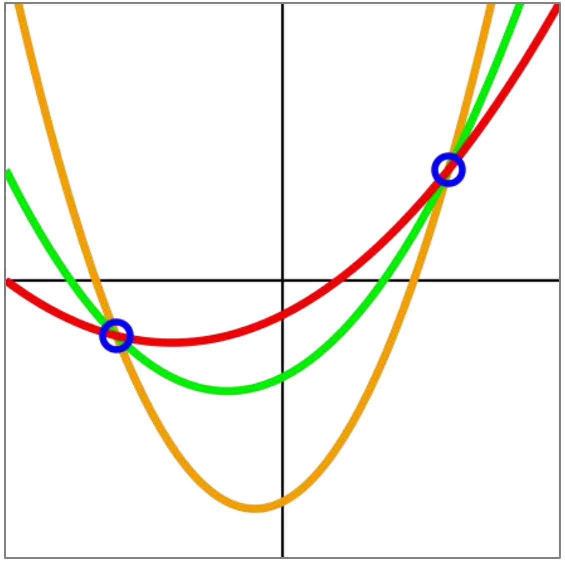
Recall that the secret is the free coefficient, which means that $S = 1234$, and we are done.

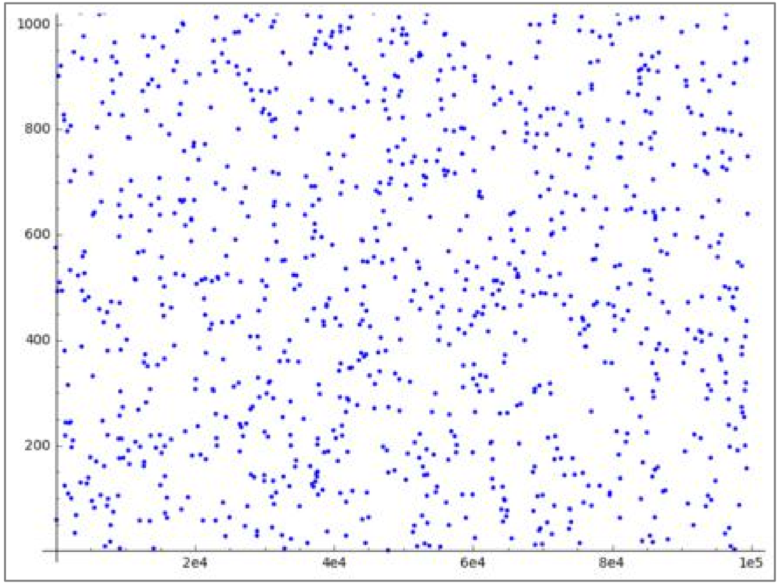
安全问题？

假设阈值为 3 （需要 3 份数据恢复），已知 2 份数据的情况下，可以将另 1 份数据的可能性降到 150 种以下。

没有安全问题

神奇的运算符：mod





密钥分享与找回

设定最小阈值（最少需要多少份数据才能找回），然后可以生成任意多份不相关的数据备份到信任的地方，就可以依据备份数据找回原数据。

目录

感谢聆听　敬请指正