西安交通大學
XI'AN JIAOTONG UNIVERSITY

第 7 章：隐私计算基础

赵俊舟
junzhou.zhao@xjtu.edu.cn

2025 年 4 月 11 日

目录

目录

目录

秘密共享（Secret Sharing, SS）

- 秘密共享在安全多方计算、分布式系统共识算法等应用中有重要应用。

例

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？

例

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？

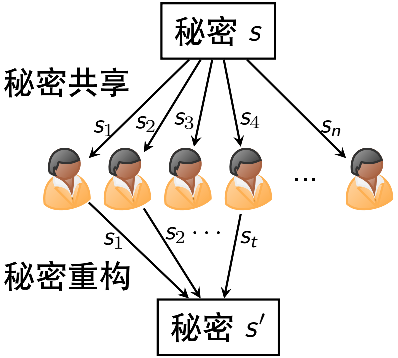
门限秘密共享（Threshold Secret Sharing）

定义 ((t,n)-门限秘密共享)

秘密 s 被分为 n 个部分，每个部分称为一个份额（share），由一个参与者持有。如果

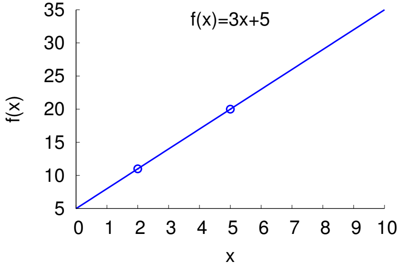
- 由 t 个或多于 t 个参与者所持有的部分信息可以重构 s；
- 由少于 t 个参与者所持有的部分信息无法重构 s。

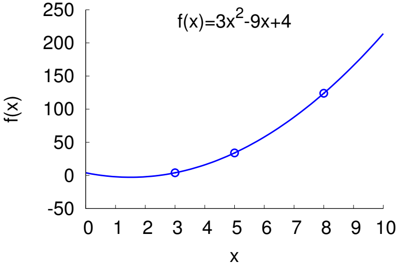
则称该方案为 (t,n)-门限秘密共享，t 称为门限值（Threshold）。



目录

Shamir 门限秘密共享的思想





- 一般的，设 $\{(x_1, y_1), \ldots, (x_t, y_t)\}$ 是平面上 t 个不同点，那么存在唯一的不超过 $t-1$ 次多项式
$$f(x) = a_0 + a_1 x + \cdots + a_{t-1} x^{t-1}$$
经过这 t 个点。
- 若把秘密 s 取为 $f(0)$，n 个份额取为 $f(i), i = 1, \ldots, n$，那么利用其中任意 t 个份额便可重构 $f(x)$，从而得到 $s = f(0)$。

Shamir 门限秘密共享

- 设 $\mathrm{GF}(p)$ 为大素数 p 生成的有限域，其中 $p > n$。
- 在 $\mathrm{GF}(p)$ 上构造一个 $t-1$ 次多项式
$$f(x) = a_0 + a_1 x + \cdots + a_{t-1} x^{t-1}$$
其中 $a_0 = s, a_i \in_R \mathbb{Z}_p \backslash \{0\}, i \neq 0$。
- n 个参与者 $u_1, \ldots, u_n$，其中 u_i 持有的份额为 $f(i)$。
- 任意 t 个参与者 $u_{i_1}, u_{i_2}, \ldots, u_{i_t}$ 要重构 s，可以联立方程组
$$\begin{cases} f(i_1) = a_0 + a_1 i_1 + \cdots + a_{t-1} i_1^{t-1} \\ f(i_2) = a_0 + a_1 i_2 + \cdots + a_{t-1} i_2^{t-1} \\ \ldots \\ f(i_t) = a_0 + a_1 i_t + \cdots + a_{t-1} i_t^{t-1} \end{cases}$$
求出 $a_0 = s$。

Shamir 门限秘密共享

- 也可以利用 Lagrange 插值公式进行重构

$$f(x) = \sum_{j=1}^{t} f(i_j) \prod_{l=1, l \neq j} \frac{x - i_l}{i_j - i_l} \pmod{p}$$

- 从而得到

$$s = f(0) = (-1)^{t-1} \sum_{j=1}^{t} f(i_j) \prod_{l=1, l \neq j} \frac{i_l}{i_j - i_l} \pmod{p}$$

Shamir 门限秘密共享的安全性

- 如果有 $t-1$ 个参与者想重构 s，他们可以构造 $t-1$ 个方程，但是有 t 个未知数。
- 由这 $t-1$ 个方程无法得到第 t 个方程的任何信息，第 t 的方程为 $f(0)=s$。
- 可以证明，由 $t-1$ 个份额得不到关于秘密 s 的任何信息。
- 因此 Shamir 门限秘密共享是安全的。

目录

目录

密码学承诺的应用场景

例 (在线拍卖)

在拍卖中，竞标者在拍卖开始时使用承诺方案来提交他们的出价，而不透露具体的出价金额。拍卖结束时，所有出价可以被揭示并验证，以确保竞标者的出价是诚实的。

例 (电子投票)

在电子投票系统中，承诺方案可以确保选民在投票时能够保密其选择，同时在投票结束后能够验证其投票的有效性。

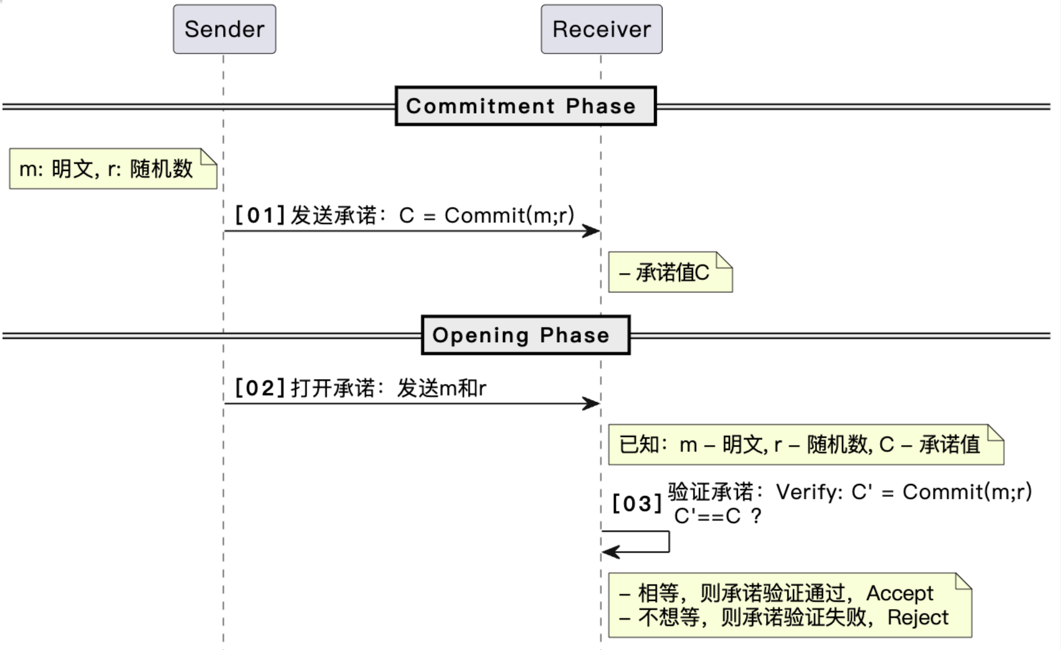
例 (加密货币)

在区块链技术中，承诺方案可以用于确保交易的隐私和安全性。例如，某些隐私币（如 Zcash）使用承诺方案来隐藏交易金额和发送者信息。

密码学承诺的基本概念

- 承诺方案（Commitment Scheme）是一个重要的密码学原语（Cryptographic Primitive）。承诺方案是一种加密协议，允许发送者承诺一个选择的值（或声明），同时对接收者保持隐藏，而接收者能够在稍后验证所承诺的值。
- 承诺方案通常可以分为两个阶段。
  - 承诺阶段：发送方发送一个承诺值给接收方，这个值是发送方选择的，接收方无法知道这个值的内容。
  - 打开阶段：发送方打开这个承诺，接收方可以验证这个值的内容。
- 密码学承诺具有两个属性：
  - 隐藏性（Hiding）：接收方无法知道发送方所承诺的值。
  - 绑定性（Binding）：发送方无法修改承诺值对应的明文。

密码学承诺的基本流程


Sender
Receiver
Commitment Phase
m: 明文, r: 随机数
[01] 发送承诺：C = Commit(m;r)
– 承诺值C
Opening Phase
[02] 打开承诺：发送m和r
已知：m – 明文, r – 随机数, C – 承诺值
[03] 验证承诺：Verify: C' = Commit(m;r)
C'==C ?
– 相等，则承诺验证通过，Accept
– 不想等，则承诺验证失败，Reject

目录

哈希承诺

- 哈希承诺是密码学承诺中最简单的一种实现方式。
- 哈希承诺通过以下公式计算关于敏感数据 v 的承诺：
$$c = H(v)$$
其中 H 是密码学安全哈希函数。
- 隐藏性：基于哈希函数的单向性，难以通过哈希值 $H(v)$ 反推出敏感数据 v；
- 绑定性：基于哈希函数的抗碰撞性，难以找到不同的敏感数据 v' 产生相同的哈希值 $H(v)$。
- 局限性：
  - 隐匿性比较有限，不具备随机性；
  - 不支持在密文形式下的直接运算。

Pedersen 承诺

- Pedersen 承诺是目前隐私保护方案中使用广泛的密码学承诺。
- 设 G_q 是 $\mathbb{Z}_p^*$ 的阶为 q 的子群，g, h 为 G_q 的生成元。
- **承诺阶段**：发送方选择一个明文 m 和一个随机数 r，计算承诺值 $C = g^m h^r \bmod p$，并发送 C 给接收方。
- **打开阶段**：发送方揭示明文 m 和随机数 r。
- **验证阶段**：接收方重新计算承诺值 $C' = g^m h^r \bmod p$，并验证 C' 和 C 是否相等。
- Pedersen 承诺的隐藏性和绑定性是基于 DLP 问题的困难性：
  - **隐藏性**：接收方无法从承诺值 C 推导出明文 m；
  - **绑定性**：发送方无法找到两个不同的 (r_1, m_1) 和 (r_2, m_2)，使得 $C = g^{m_1} h^{r_1} = g^{m_2} h^{r_2} \pmod p$。

Pedersen 承诺的绑定性

- 假设发送方找到两个不同的 (r_1, m_1) 和 (r_2, m_2)，使得 $C = g^{m_1}h^{r_1} = g^{m_2}h^{r_2} \pmod p$
- 则有
$$g^{m_1}h^{r_1} = g^{m_2}h^{r_2} \Rightarrow g^{m_1-m_2} \equiv h^{r_2-r_1} \pmod p$$
- 由于 g 和 h 是独立生成元，即它们生成的子群没有重叠，这意味着只有在 $m_1 - m_2 = 0$ 和 $r_2 - r_1 = 0$ 时才成立，即：$m_1 = m_2, r_1 = r_2$。
- 与假设矛盾，因此 Pedersen 承诺具有绑定性。

Pedersen 承诺

- Pedersen 承诺是目前隐私保护方案中使用广泛的密码学承诺。
- 相比哈希承诺，构造略微复杂，但提供了一系列优异的特性：
  - 信息论安全的理论最强隐藏性；
  - 基于离散对数困难问题的强绑定性；
  - 具有同态加法特性的密文形式。
- 加法同态性：两个 Pedersen 承诺的积等于明文的和的 Pedersen 承诺。假设 $C_1 = g^{m_1}h^{r_1}$ 和 $C_2 = g^{m_2}h^{r_2}$ 是两个 Pedersen 承诺，则有：

$$C_1 \cdot C_2 = g^{m_1}h^{r_1} \cdot g^{m_2}h^{r_2} = g^{m_1+m_2}h^{r_1+r_2}$$

即

$$\mathrm{commit}(m_1, r_1) \cdot \mathrm{commit}(m_2, r_2) = \mathrm{commit}(m_1 + m_2, r_1 + r_2)$$

小结

1. 秘密共享协议
2. 密码学承诺