ZK SHANGHAI

零知识证明工作坊

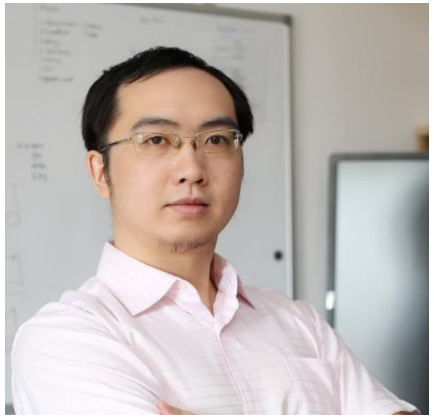
承诺方案

现代零知识密码学

Hosted by **SutuLabs** & **Kepler42B-ZK Planet**

课程资源：zkshanghai.xyz

个人介绍



梁爽

区块链 架构师

上海交大 计算机博士生

（休学创业中）

微信：icerdesign
微博：@wizicer
Github: @wizicer
Twitter: @icerdesign
LinkedIn: www.linkedin.com/in/icerdesign

1999年	• 正式开始学习写程序
2009年	• 在新媒传信（飞信）做高性能服务器程序架构及开发
2012年	• 在Honeywell工业控制部门做PLC、RTU上位机组态软件架构及开发
2017年	• 接触区块链，并开始创业开发区块链数据库
2020年	• 入学上海交大攻读博士学位，研究零知识证明数据库
2022年	• 获Chia全球开发大赛第一名，并开始Pawket钱包的开发
2023年	• 获得零知识链Mina的项目资助

今日课程内容

- 模块化SNARK概述
- 承诺方案定义
- 向量承诺
  - Pedersen承诺
  - 向量Pedersen承诺
  - Merkle树承诺
- 多项式承诺
  - 双线性映射密码学
  - KZG承诺

今日课程将回答以下问题

- τ 是什么？
- 可信设置生成了什么？
- 如何做到证据的简洁？
- 证据里面包含了什么？
- 为什么电路改变需要重做设置步骤？

模块化SNARK

算术电路

↓

算术化
Arithmetization

→

信息论

IOP
Interactive Oracle Proof

对于<u>无界算力</u>的参与者
<u>也能</u>提供可靠性和零知识

→

密码学

承诺方案
Commitment Scheme

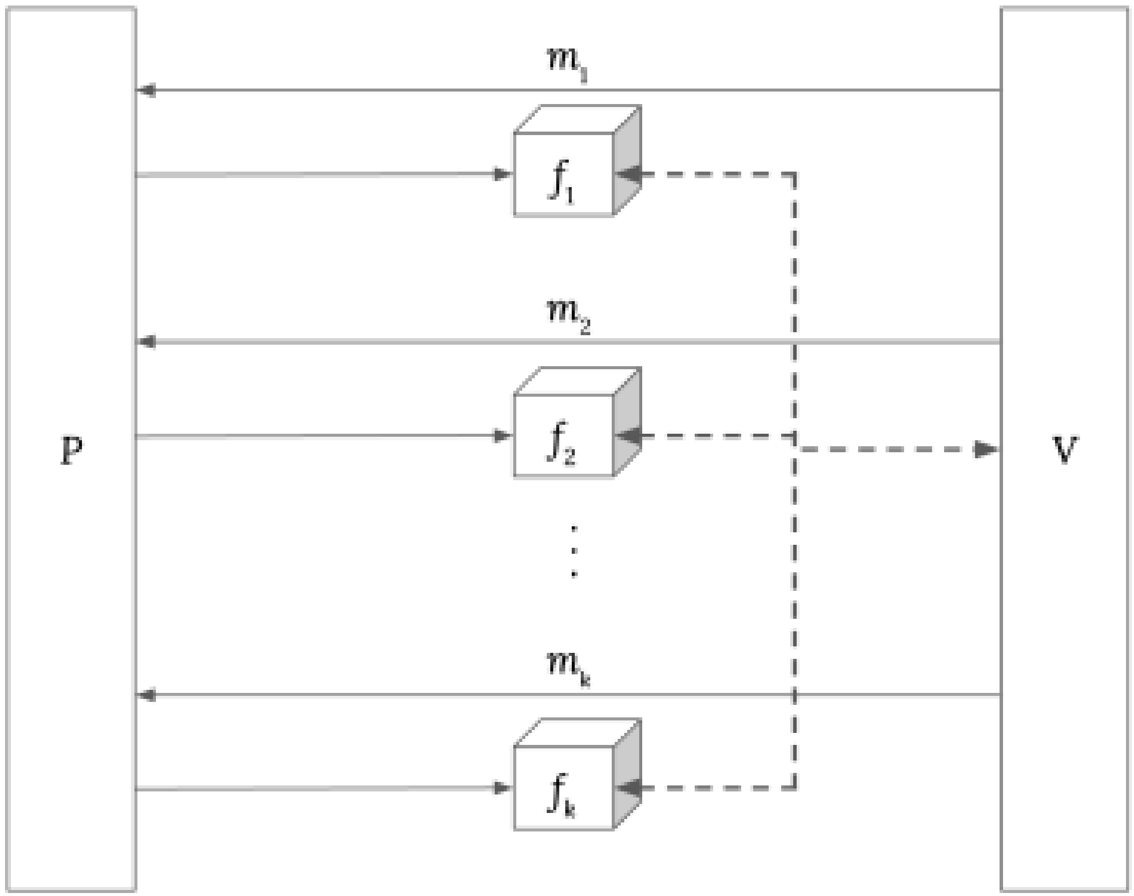
对于<u>有界算力</u>的参与者
<u>才能</u>提供可靠性和零知识

↓

论证系统

IOP

Interactive Oracle Proof



注意：IOP是理想协议
因此可以在无界算力条件
下保证可靠性和零知识性

汉密尔顿回路

目的：证明者想向验证者证明他知道图G的一个汉密尔顿回路，而不泄露任何额外信息。

证明者

验证者

- 根据随机排列，为每个顶点分配一个1到n之间的标签，并记住这个排列。
- 对于每一对顶点ij，将B_{ij}放进加密盒子，其代表ij是否是G的一条边。

所有的加密盒子B_{ij} →

随机选择$b \in \{0,1\}$

挑战：$\begin{cases} 如果b=0: 给我看图 \\ 如果b=1: 给我看汉密尔顿回路 \end{cases}$ ←

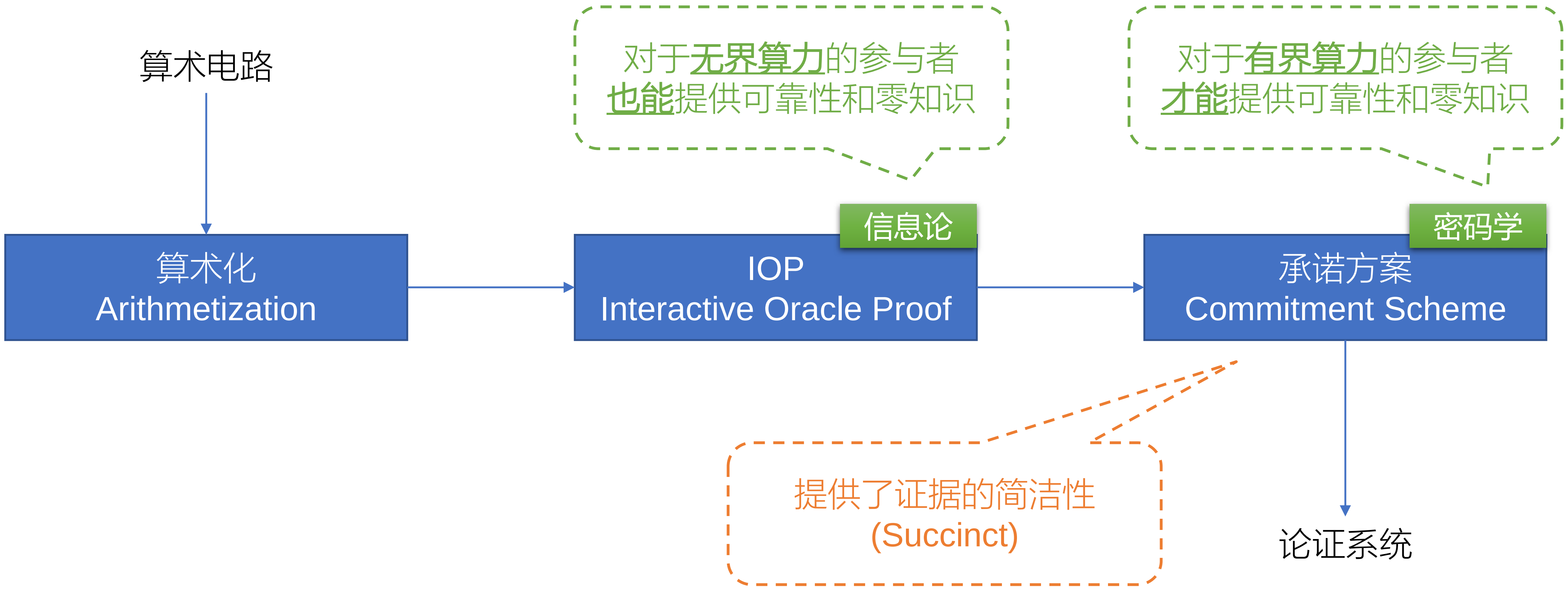
挑战：$\begin{cases} 如果b=0: 解密所有盒子及排列规则 \\ 如果b=1: 解密包含汉密尔顿回路的盒子 \end{cases}$ →

检查：

$\begin{cases} 如果b=0: 是同一幅图 \\ 如果b=1: 是汉密尔顿回路 \end{cases}$

汉密尔顿回路是不是IOP？

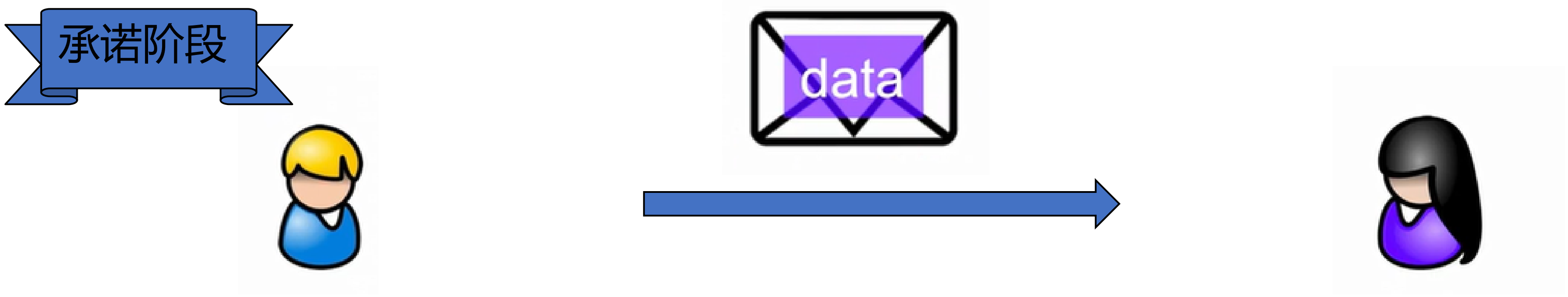
模块化SNARK


算术电路
对于无界算力的参与者
也能提供可靠性和零知识
对于有界算力的参与者
才能提供可靠性和零知识
信息论
密码学
算术化
Arithmetization
IOP
Interactive Oracle Proof
承诺方案
Commitment Scheme
提供了证据的简洁性
(Succinct)
论证系统

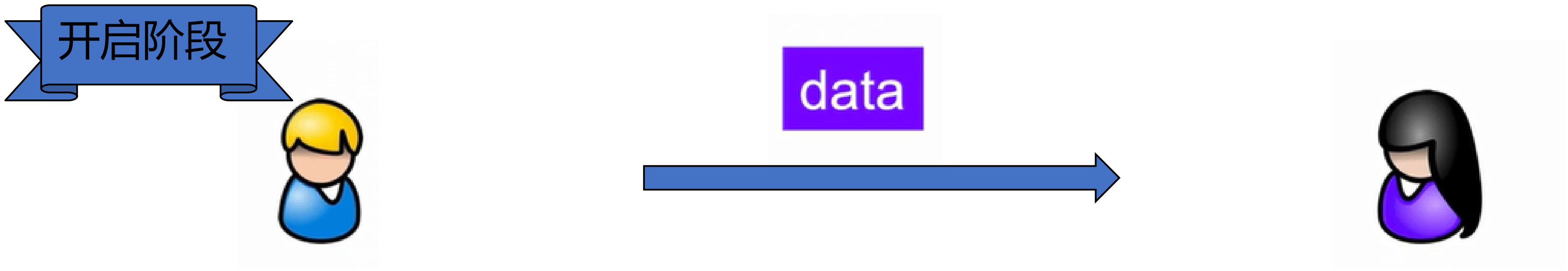
承诺方案的定义

- 承诺方案是 PPT 算法的元组 $\Gamma =（Setup, Commit, Open）$，其中：
  - $Setup(1^{\lambda}) \to pp$ 采用安全参数 λ（一元）并生成公共参数 pp；
  - $Commit(pp; m) \to (C; r)$ 获取秘密消息 m 并输出公开承诺 C 和（可选）秘密打开提示 r（可能为随机数）。
  - $Open(pp, C; m, r) \to b \in \{0,1\}$ 利用打开提示 r，验证承诺 C 对消息 m 的打开。
- 其中$m \in \mathcal{M}$

承诺方案的特性



- 隐藏性 hiding：  不会泄漏任何关于 data 任何信息



- 绑定性 binding：  只能由 data “开启”

承诺方案的特性

- 绑定性

$$\Pr\left[b_0 = b_1 \neq 0 \wedge m_0 \neq m_1 : \begin{array}{l} \mathrm{pp} \leftarrow \mathrm{Setup}\left(1^\lambda\right) \\ (C, m_0, m_1, r_0, r_1) \leftarrow \mathcal{A}(\mathrm{pp}) \\ b_0 \leftarrow \mathrm{Open}\left(\mathrm{pp}, C, m_0, r_0\right) \\ b_1 \leftarrow \mathrm{Open}\left(\mathrm{pp}, C, m_1, r_1\right) \end{array}\right] \leq \mathrm{neg}(\lambda)$$

- 隐藏性

$$\left|\Pr\left[b_0 = b' : \begin{array}{l} \mathrm{pp} \leftarrow \mathrm{Setup}\left(1^\lambda\right) \\ (m_0, m_1, st) \leftarrow \mathcal{A}(\mathrm{pp}) \\ b \xleftarrow{\$} \{0,1\} \\ (C_b; r_b) \leftarrow \mathrm{Commit}\left(\mathrm{pp}; m_b\right) \\ b' \leftarrow \mathcal{A}\left(\mathrm{pp}, st, C_b\right) \end{array}\right] - 1/2\right| = \mathrm{negl}(\lambda)$$

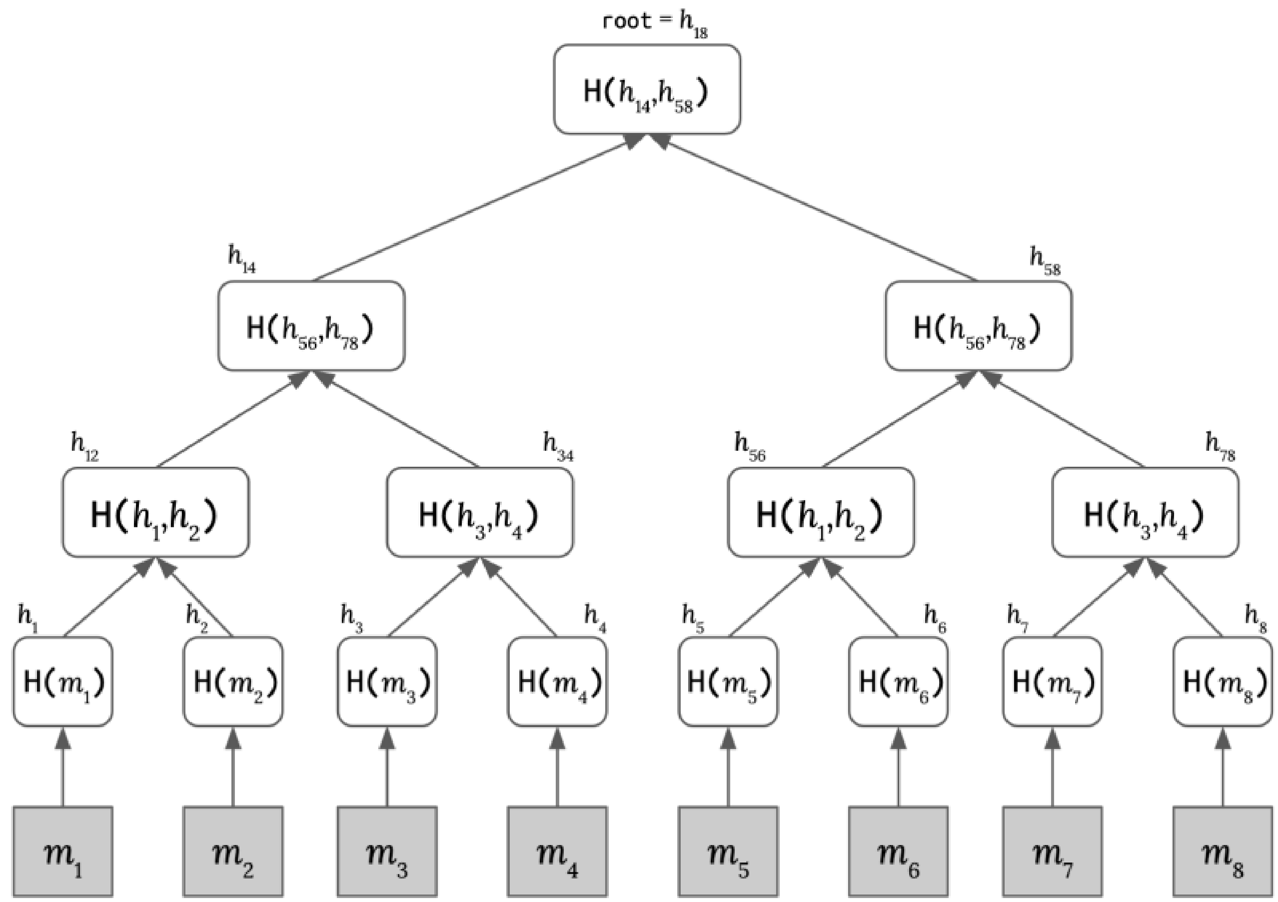
Pedersen承诺

- Pedersen 承诺是一个在消息空间 $\mathbb{F}_q$ 上具有绑定性和隐藏性的承诺方案。对于一个秘密消息 $m \in \mathbb{F}_q$：
  - $Setup\ (1^\lambda, q) \rightarrow pp: pp = G, H \in \mathbb{G}$，其中 $\mathbb{G}$ 是一个阶为 q 的群。
  - $Commit\ (pp; m) \rightarrow (C; r): C = [m]G + [r]H$， $r \xleftarrow{\$} \mathbb{F}_q$
  - $Open\ (pp, C; m, r) \rightarrow \{0,1\}$: 证明者 P 揭示 m 和 r，验证者 V 检查 $C \overset{?}{\rightarrow} [m]G + [r]H$。
- Pedersen 承诺具有加法同态性：
  - $$\begin{aligned} Commit(m, r) + Commit(m', r') \\ &= [m]G + [r]H + [m']G + [r']H \\ &= [m + m']G + [r + r']H \\ &= Commit(m + m', r + r'). \end{aligned}$$

向量Pedersen承诺

- 我们可以将 Pedersen 承诺方案扩展到消息空间 $\mathbb{F}_q^k$ 中的向量。对于一个消息 $\vec{m} = (m_0, \dots, m_{k-1})$：
  - $Setup\ (1^\lambda, q, k) \rightarrow pp$: $pp = (G_0, \dots, G_{k-1}), H \in \mathbb{G}$，其中 $\mathbb{G}$ 是一个阶为 q 的群。
  - $Commit\ (pp; \vec{m}) \rightarrow (C; r)$: $C = [r]H + \sum_{i=0}^{k-1}[m_i]G_i$， $r \overset{\$}{\leftarrow} \mathbb{F}_q$。
  - $Open\ (pp, C; \vec{m}, r) \rightarrow \{0,1\}$:
    - 证明者 P 揭示 $\vec{m}$ 和 r
    - 验证者 V 检查 $C \overset{?}{\leftarrow} [r]H + \sum_{i=0}^{k-1}[m_i]G_i$。

Merkle树承诺


root = h_{18}
H(h_{14},h_{58})
h_{14}
H(h_{56},h_{78})
h_{58}
H(h_{56},h_{78})
h_{12}
H(h_1,h_2)
h_{34}
H(h_3,h_4)
h_{56}
H(h_1,h_2)
h_{78}
H(h_3,h_4)
h_1
h_2
h_3
h_4
h_5
h_6
h_7
h_8
H(m_1)
H(m_2)
H(m_3)
H(m_4)
H(m_5)
H(m_6)
H(m_7)
H(m_8)
m_1
m_2
m_3
m_4
m_5
m_6
m_7
m_8

Merkle树承诺

- $Commit\ (pp; \vec{m}) \rightarrow C$：
  - 对于 $\vec{m}$ 中的每个 m_i，计算哈希值 $h_i = Hash(m_i)$。
  - 计算 Merkle 树的内部节点 $h_{ij} = Hash(h_i, h_j)$。
  - 输出 $C = root = h_{1q}$。
- $Open\ (pp, C, i, \vec{m}) \rightarrow b \in \{0,1\}$：
  - a) $Prove\ (pp, C, i, \vec{m}) \rightarrow \pi = (m_i, path)$。
  - b) $Verify\ (pp, C, i, \pi) \rightarrow b \in \{0,1\}$。

双线性映射密码学

- 给定循环群 $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$，所有的阶均为素数 p，其映射关系是一个<u>非退化</u>的<u>双线性</u>映射
$$e: \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$$
- 双线性:
  - $e([a]P, Q) = [a]e(P, Q) = e(P, [a]Q)$
  - $e([a]P, [b]Q) = [a \cdot b]e(P, Q) = e(P, Q)^{a \cdot b}$
- 非退化:
  - 对于生成元 $G_1 \in \mathbb{G}_1$ 和 $G_2 \in \mathbb{G}_2$，$G_T := e(G_1, G_2) \in \mathbb{G}_T$ 是一个生成元。

双线性映射密码学

- 符号
  - $[x]G = \underbrace{G + \cdots + G}_{x\ times}$
  - $[x]_1 = [x]G_1$
  - $[x]_2 = [x]G_2,$

KZG承诺

- 单变量多项式承诺方案是针对消息空间 $\mathbb{F}^{\leq d}[X]$ 的一种承诺方案。
  - $Setup\ (1^{\lambda}, d) \rightarrow srs = (ck, vk) = (\left\{[\alpha^i]_1\right\}_{i=0}^{d-1}, [\alpha]_2)$.
    - α 是一个秘密元素，必须在 $Setup$ 后丢弃。
  - $Commit\ (ck; f(X)) \rightarrow C$: 对于 $f(X) = \sum_{i=0}^{d-1} f_i X^i$, $C = \sum_{i=0}^{d-1} [f_i][\alpha^i]_1 = [f(\alpha)]_1$.
  - $Open(srs, C, z, y; f(X)) \rightarrow \{0,1\}$: 在评估点 z 上打开对于 y 的承诺
    - $Prove\ (ck, C, z, y; f(X)) \rightarrow \pi$:
      - 商多项式 $q(X) = \frac{f(X)-y}{X-z}$, $\pi = Commit\ (ck; q(X)) = [q(\alpha)]_1$
    - $Verify\ (vk, C, z, y, \pi) \rightarrow \{0,1\}$:
      - 检查 $e(C - [y]_1, [1]_2) \overset{?}{\leftarrow} e(\pi, [\alpha]_2 - [z]_2)$.