Groth16 证明生成流程数学推导

1 协议参数定义

Groth16 协议基于三元组 $(p, \mathbb{G}_1, \mathbb{G}_2)$ 定义：

- p：有限域特征（来自 Poseidon2 电路）
- $\mathbb{G}_1, \mathbb{G}_2$：配对友好椭圆曲线群
- R_F, R_P：Poseidon2 的全轮与半轮数

2 算术电路表示

Poseidon2 电路转化为 R1CS 系统：

$$\begin{cases} A \cdot s \circ B \cdot s = C \cdot s \\ s = (1, x, w) \in \mathbb{F}_p^{n+1} \end{cases}$$

其中：

- x：公开输入（哈希值）
- w：隐私输入（原像）
- n：约束总数 $C_{\text{总}} = t(R_F + 1) + R_P$

3 Groth16 密钥生成

3.1 可信设置

生成结构化参考字符串（SRS）：

$$\tau \xleftarrow{\$} \mathbb{F}_p^*$$

$$\text{CRS} = \begin{pmatrix} [1]_1, [\tau]_1, \ldots, [\tau^{2n}]_1 \\ [1]_2, [\tau]_2, \ldots, [\tau^{n}]_2 \end{pmatrix}$$

3.2 密钥对推导

$$\text{证明密钥} = \begin{pmatrix} [A]_1, [B]_2, [C]_1, \\ [\alpha]_1, [\beta]_2, [\delta]_1 \end{pmatrix}$$

$$\text{验证密钥} = \begin{pmatrix} [\alpha]_1 \cdot [\beta]_2, \\ [\gamma]_2, [\delta]_2 \end{pmatrix}$$

4 证明生成算法

4.1 见证生成

给定输入 x，求解：

$$W(x, w) = 1 \quad \Rightarrow \quad w\text{满足}A \cdot s \circ B \cdot s = C \cdot s$$

4.2 证明构造

$$\pi = ([A]_1, [B]_2, [C]_1)$$

$$\text{其中} \quad A = \alpha + \sum_{i=0}^{n} a_i u_i(x) + r\delta$$

$$B = \beta + \sum_{i=0}^{n} b_i v_i(x) + s\delta$$

$$C = \frac{\sum_{i=0}^{n} a_i b_i (u_i(x) v_i(x)) + h(x)t(x)}{\delta} + As + Br - rs\delta$$

5 验证方程

验证者检查双线性配对：

$$e([A]_1, [B]_2) \stackrel{?}{=} e([\alpha]_1, [\beta]_2) \cdot e\left(\sum_{i=0}^{n} x_i[u_i]_1, \sum_{i=0}^{n} x_i[v_i]_2\right) \cdot e([C]_1, [\delta]_2)$$

6 Poseidon2 特定参数

对于 $(t, d) = (3, 5)$ 的实例：

$$\begin{cases} \text{约束数} = 3 \times (8+1) + 56 = 83 \\ \text{S-box 次数} = 8 \times 3 + 56 = 80 \end{cases}$$

Algorithm 1 Groth16 证明生成流程

1: 编译电路获得 R1CS（A, B, C 矩阵）
2: 加载可信设置 τ
3: 生成 (pk, vk)
4: 计算见证 $w \leftarrow \text{WitnessGen}(x)$
5: 生成证明 $\pi \leftarrow \text{Prove}(\text{pk}, x, w)$
6: 验证 $\text{Verify}(\text{vk}, x, \pi)$