Poseidon2 哈希算法数学推导

1 参数定义

Poseidon2 哈希函数由元组 (n, t, d, R_F, R_P) 定义：

- n：安全参数（比特数），通常取 256
- t：状态大小（有限域元素个数）
- d：S-box 指数（通常取 5，要求 $\gcd(d, p-1) = 1$）
- R_F：全轮数（外部轮）
- R_P：半轮数（内部轮）

2 算法结构

2.1 状态表示

状态表示为 $\mathbb{F}_p$ 上的 t 维向量：

$$\mathbf{s} = (s_0, s_1, \ldots, s_{t-1}) \in \mathbb{F}_p^t$$

2.2 置换函数结构

Poseidon2 置换 $\mathcal{P} : \mathbb{F}_p^t \to \mathbb{F}_p^t$ 由以下部分组成：

$$\mathcal{P}(\mathbf{s}) = (\mathcal{E}_{R_F-1} \circ \cdots \circ \mathcal{E}_{R_F/2} \circ \mathcal{I}_{R_P-1} \circ \cdots \circ \mathcal{I}_0 \circ \mathcal{E}_{R_F/2-1} \circ \cdots \circ \mathcal{E}_0)(M_E \cdot \mathbf{s})$$

2.3 轮函数设计

2.3.1 全轮函数 ($\mathcal{E}$)

对每个全轮 $i \in \{0, \ldots, R_F - 1\}$：

$$\mathcal{E}_i(\mathbf{s}) = M_E \cdot \left((s_0 + c_0^{(i)})^d, (s_1 + c_1^{(i)})^d, \ldots, (s_{t-1} + c_{t-1}^{(i)})^d \right)$$

其中：

- M_E：MDS 矩阵保证完全扩散
- $c_j^{(i)}$：轮常数
- x^d：S-box 操作（$d = 5$ 时计算 x^5）

2.3.2 半轮函数 ($\mathcal{I}$)

对每个半轮 $i \in \{0, \ldots, R_P - 1\}$：

$$\mathcal{I}_i(\mathbf{s}) = M_I \cdot \left((s_0 + c_0^{(i)})^d, s_1, \ldots, s_{t-1} \right)$$

其中 M_I 为部分扩散矩阵：

$$M_I = \begin{pmatrix} \mu_0 & 1 & \cdots & 1 \\ 1 & \mu_1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & \mu_{t-1} \end{pmatrix}, \quad \mu_i \in \mathbb{F}_p \setminus \{0, 1\}$$

3 优化实现

3.1 MDS 矩阵 (M_E)

当 $t = 4$ 时的优化矩阵：

$$M_E = \begin{pmatrix} 5 & 7 & 1 & 3 \\ 4 & 6 & 1 & 1 \\ 1 & 3 & 5 & 7 \\ 1 & 1 & 4 & 6 \end{pmatrix}$$

3.2 约束数量计算

Plonk 算术化后的约束总数：

$$C_{\text{总}} = \underbrace{t \cdot R_F}_{\text{全轮约束}} + \underbrace{R_P}_{\text{半轮约束}} + \underbrace{t}_{\text{输入层约束}}$$

4 安全性分析

4.1 差分安全性

对于 $t = 3$，6 个全轮的最小活跃 S-box 数：

$$\text{概率} \leq \left(\frac{d-1}{p}\right)^{3(t+4)} \ll 2^{-256}$$

4.2 代数安全性

经过 R 轮后的代数次数：

$$\deg(\mathcal{P}^R) = d^{R_F+R_P} \geq 2^{128} \quad (\text{当} R_F = 8, R_P = 56 \text{时})$$