VRF 计算

Jade Xie

2025 年 10 月 20 日

0.1 准备阶段

0.2 Porver 计算

- 输入：sk, pk, in

其中 sk 为进行签名和输出随机数的私钥，in 为输入。

1. 计算
$$preout = sk \cdot H_{\mathbb{G}}(in)$$
其中 $H_{\mathbb{G}}$ 是 hash to curve 操作，H 是一般的哈希函数。
2. 在 $\mathbb{F}_p$ 中选取随机数 r_1。
3. 计算
$$R = r_1 \cdot \mathbf{G}$$
$$R_m = r_1 \cdot H_{\mathbb{G}}(in)$$
4. 计算
$$c = H_p(in, pk, preout, R, R_m)$$
其中 H_p 是在有限域 $\mathbb{F}_p$ 上进行哈希，先进行哈希，再映射到有限域 $\mathbb{F}_p$ 内。
5. 计算
$$s_1 = r_1 + c \cdot sk$$

- 输出：$c, s_1, preout$

0.3 Verifier 验证计算

- 输入：$pk, in, c, s_1, preout$

1. 计算
$$R = s_1 \cdot G - c \cdot pk$$
$$R_m = s_1 \cdot H_{\mathbb{G}}(in) - c \cdot preout$$
2. 判断
$$c \stackrel{?}{=} H_p(in, pk, preout, R, R_m)$$
3. 上一步如果相等，计算
$$out = H(preout, in)$$
并输出 out ，否则输出 $false$ 。