内积证明

Jade

2024 年 3 月 11 日

目录

1 内积证明

参考这篇文章。

想对这样的结构 $C = \vec{a} \cdot g + \vec{b} \cdot h + (\vec{a} \cdot \vec{b})q$ 作出承诺。思想是进行折半，折半后的承诺和原来的承诺等价，不断对向量 $\vec{a}, \vec{b}$ 进行折半，直到最后变成标量，简单计算即可得到证明。

假设 $\vec{a}$ 与 $\vec{b}$ 的向量长度为 n，令 $m = \frac{n}{2}$. 记

$$z_L = a_m b_0 + a_{m+1} b_1 + \cdots + a_{n-1} b_{m-1} = \vec{a}_R \cdot \vec{b}_L$$

$$z_R = a_0 b_m + a_1 b_{m+1} + \cdots + a_{m-1} b_{n-1} = \vec{a}_L \cdot \vec{b}_R$$

从最后得到新的承诺 C' 来看这个构造的过程：

$$\begin{aligned}
C' &= xC_L + C + x^{-1} C_R \\
&= x(\vec{a}_R \cdot \vec{g}_L + \vec{b}_L \cdot \vec{h}_R + z_L q) \\
&\quad + \vec{a}_L \cdot \vec{g}_L + \vec{a}_R \cdot \vec{g}_R + \vec{b}_L \cdot \vec{h}_L + \vec{b}_R \cdot \vec{h}_R + \vec{a} \cdot \vec{b} q \\
&\quad + x^{-1}(\vec{a}_L \cdot \vec{g}_R + + \vec{b}_R \cdot \vec{h}_L + z_R q) \\
&= (x\vec{a}_R + \vec{a}_L) \cdot (\vec{g}_L + x^{-1}\vec{g}_R) \\
&\quad + (\vec{b}_L + x^{-1}\vec{b}_R) \cdot (\vec{h}_L + x\vec{h}_R) \\
&\quad + (xz_L + \vec{a} \cdot \vec{b} + x^{-1} z_R) q \\
&:= (x\vec{a}_R + \vec{a}_L) \cdot g' + (\vec{b}_L + x^{-1}\vec{b}_R) \cdot h' + (xz_L + \vec{a} \cdot \vec{b} + x^{-1} z_R) q
\end{aligned}$$

而恰好

$$\begin{aligned}
(x\vec{a}_R + \vec{a}_L)(\vec{b}_L + x^{-1}\vec{b}_R) &= x\vec{a}_R\vec{b}_L + \vec{a}_L\vec{b}_L + \vec{a}_R\vec{b}_R + x^{-1}\vec{a}_L\vec{b}_R \\
&= x\vec{a}_R\vec{b}_L + \vec{a} \cdot \vec{b} + x^{-1}\vec{a}_L\vec{b}_R \\
&= xz_L + \vec{a} \cdot \vec{b} + x^{-1} z_R
\end{aligned}$$

承诺 C' 也满足原来承诺 C 的内积结构。同时 g' 与 h' 相比原来的 g 与 h 已经折半了。

协议过程：

1. Prover 计算承诺

$$C_L = \vec{a}_R \cdot \vec{g}_L + \vec{b}_L \cdot \vec{h}_R + z_L q$$

$$C_R = \vec{a}_L \cdot \vec{g}_R + \vec{b}_R \cdot \vec{h}_L + z_R q$$

2. Verifier 发送挑战 $x \in \mathbb{F}_p$

3. Prover 计算新的向量

$$\vec{a}' = \vec{a}_L + x\vec{a}_R$$

$$\vec{b}' = \vec{b}_L + x^{-1}\vec{b}_R$$

4. Verifier 计算新的承诺 C'

$$C' = xC_L + C + x^{-1}C_R$$

更新基：

$$\vec{g}' = \vec{g}_L + x^{-1}\vec{g}_R$$

$$\vec{h}' = \vec{h}_L + x\vec{h}_R$$

可以证明，新的承诺 $C' = \vec{a}' \cdot \vec{g}' + \vec{b}' \cdot \vec{h}' + \vec{a}' \cdot \vec{b}' q$ 也是满足内积性质的。

5. 对 $C', \vec{g}', \vec{h}'$ 重复上述步骤，直到最后向量长度为 1，简单计算即可得出等式是否成立。