Wedpr-VCL 加法、乘法证明过程

假设存在三个明文 c_1, c_2, c_3，g_1, g_2 为生成元。对应的 Commitment 为：

- $A = Com(c_1; r_1) = g_1^{c_1} \cdot g_2^{r_1}$
- $B = Com(c_2; r_2) = g_1^{c_2} \cdot g_2^{r_2}$
- $C = Com(c_3; r_3) = g_1^{c_3} \cdot g_2^{r_3}$

其中 r_i 为随机参数

1 加法

证明 $c_1 + c_2 = c_3$ 的过程如下：
Statement：A,B,C,$c_1 + c_2 = c_3$
Witness: c_1, c_2, r_1, r_2, r_3
Prover:

1. $a, b, c, d, e \xleftarrow{\$} Z_q$
2. Compute $C' = g_1^{c_1+c_2} \cdot g_2^{r_3}$
3. Compute $T_1 = g_1^a g_2^b$, $T_2 = g_1^c g_2^d$, $T_3 = g_1^{a+c} g_2^e$
4. Compute hash $h = Hash(T_1, T_2, T_3, A, B, C', g_1)$
5. Compute $m_1 = a - h \cdot c_1$, $m_2 = b - h \cdot r_1$, $m_3 = c - h \cdot c_2$, $m_4 = d - h \cdot r_2$, $m_5 = e - h \cdot r_3$
6. proof $\pi = (m_1, m_2, m_3, m_4, m_5, h)$

Verifier:

1. Compute $T_1' = g_1^{m_1} g_2^{m_2} A^h$, $T_2' = g_1^{m_3} g_2^{m_4} B^h$, $T_3' = g_1^{m_1+m_3} g_2^{m_5} C^h$
2. Compute hash $h' = Hash(T_1', T_2', T_3', A, B, C, g_1)$
3. Check $h' \stackrel{?}{=} h$

2 乘法

证明 $c_1 \cdot c_2 = c_3$ 的过程如下：
Statement：A,B,C,$c_1 \cdot c_2 = c_3$
Witness: c_1, c_2, r_1, r_2, r_3
Prover:

1. $a, b, c, d, e \xleftarrow{\$} Z_q$
2. Compute $C' = g_1^{c_1 \cdot c_2} \cdot g_2^{r_3}$
3. Compute $T_1 = g_1^a g_2^b$, $T_2 = g_1^c g_2^d$, $T_3 = g_1^{a \cdot c} g_2^e$
4. Compute hash $h = Hash(T_1, T_2, T_3, A, B, C', g_1)$
5. Compute $m_1 = a - h \cdot c_1$, $m_2 = b - h \cdot r_1$, $m_3 = c - h \cdot c_2$, $m_4 = d - h \cdot r_2$
6. Compute $m_5 = e + h \cdot h \cdot (c_1 \cdot r_2 - r_3 + c_2 \cdot r_1) - h \cdot (a \cdot r_2 + c \cdot r_1)$
7. proof $\pi = (m_1, m_2, m_3, m_4, m_5, h)$

Verifier:

1. Compute $T_1' = g_1^{m_1} g_2^{m_2} A^h$, $T_2' = g_1^{m_3} g_2^{m_4} B^h$,
   $T_3' = g_1^{m_1 \cdot m_3} g_2^{m_5} C^{h \cdot h} A^{h \cdot m_3} B^{h \cdot m_1}$
2. Compute hash $h' = Hash(T_1', T_2', T_3', A, B, C, g_1)$
3. Check $h' \stackrel{?}{=} h$