

Assuming that $(m_1, \sigma = (\sigma_{1,1} = H(m_1)^d r_1^d, r_1))$ and $(m_2, \sigma_2 = (\sigma_{2,1} = H(m_2)^d r_2^d, r_2))$ are known:

1. such that a hash value $H(m_3) = H(m_1)H(m_2)$,

and $\sigma_3 = (\sigma_{3,1} = \sigma_{1,1}\sigma_{2,1}, r_3 = r_1r_2)$:

◦ verification:

$$\sigma_{3,1}^e = (\sigma_{1,1}\sigma_{2,1})^e = H(m_1)H(m_2) \cdot r_1r_2 = H(m_3)r_3 \bmod n, \text{ accept.}$$

2. such that a hash value $H(m_4) = \frac{H(m_1)}{H(m_2)}$,

and $\sigma_4 = (\sigma_{4,1} = \frac{\sigma_{1,1}}{\sigma_{2,1}}, r_4 = \frac{r_1}{r_2})$:

◦ verification:

$$\sigma_{4,1}^e = (\frac{\sigma_{1,1}}{\sigma_{2,1}})^e = \frac{H(m_1)}{H(m_2)} \cdot \frac{r_1}{r_2} = H(m_4)r_4 \bmod n, \text{ accept.}$$