

For the e-th power N of the signature of the given message m , we have the following:

$$\sigma(m)^e = \frac{\sigma(m_1)^e \cdot \sigma(m_2)^e}{\sigma(1)^e} \quad (1)$$

Calculating this using the signatures $\sigma(m_1), \sigma(m_2)$ and $\sigma(1)$ as retrieved from the python oracle and using the power function

$$\text{pow}(\sigma, e, N)$$

confirms that equation (1)

$$\frac{\text{pow}(\sigma(m_1), e, N) \cdot \text{pow}(\sigma(m_2), e, N)}{\text{pow}(\sigma(1), e, N)} = \mu \cdot m_1 \cdot m_2 = \mu m = \sigma(m)^e$$

However, calculating $\sigma(m)$ simply by taking its e-th root

$$\begin{aligned} \sigma(m)^{ed} &= \left(\frac{\sigma(m_1)^e \sigma(m_2)^e}{\sigma(1)^e} \right)^d \dots \text{mod} \dots N \\ &= \frac{\sigma(m_1)^{ed} \sigma(m_2)^{ed}}{\sigma(1)^{ed}} \dots \text{mod} \dots N \\ &= \frac{\sigma(m_1) \sigma(m_2)}{\sigma(1)} \dots \text{mod} \dots N \end{aligned}$$

fails to give the correct result.