Specification of the Identity Mixer Cryptographic Library

Version 3.0.36

IBM Research – Zurich

17th November 2017

Contents

If credentials are key-bound, they are required to be bound to the same (secret) key.

$$\text{NIZK}\{(m_1, m_2, m_3) : \text{Credential}(\mathit{ipk}, m_1, m_2, m_3)\} \tag{1}$$

$$\text{NIZK}\{() : \text{Nym}(\mathit{nym}, \mathit{scope})\} \tag{2}$$

$$\text{NIZK}\{(m) : \text{Enc}(\mathit{epk}, m, \mathit{ctxt})\} \tag{3}$$

$$\text{NIZK}\{(m) : \text{Range}(m, a, b)\} \tag{4}$$