A Security

We shall give a proof for our one-time ring signature scheme. At some point it coincides with the parts of the proof in [24], but we decided to rewrite them with a reference rather than to force a reader to rush about from one paper to another.

These are the properties to be established:

- **Linkability.** Given all the secret keys $\{x_i\}_{i=1}^n$ for a set $\mathcal{S}$ it is impossible to produce $n+1$ valid signatures $\sigma_1, \sigma_2, \ldots, \sigma_{n+1}$, such that all of them pass the **LNK** phase (i.e. with $n+1$ different key images I_i). This property implies the double spending protection in the context of CryptoNote.
- **Exculpability.** Given set $\mathcal{S}$, at most $n-1$ corresponding private keys x_i (excluding $i = j$) and the image I_j of the keys x_j it is impossible to produce a valid signature σ with I_j. This property implies theft protection in the context of CryptoNote.
- **Unforgeability.** Given only a public keys set $\mathcal{S}$ it is impossible to produce a valid signature σ.
- **Anonymity.** Given a signature σ and the corresponding set $\mathcal{S}$ it is impossible to determine the secret index j of the signer with a probability $p > \frac{1}{n}$.

Linkability

Theorem 1. *Our one-time ring signature scheme is linkable under the random oracle model.*

Proof. Suppose an adversary can produce $n+1$ valid signatures σ_i with key images $I_i \neq I_j$ for any $i, j \in [1 \ldots n]$. Since $\#\mathcal{S} = n$, at least one $I_i \neq x_i \mathcal{H}_p(P_i)$ for every i. Consider the corresponding signature $\sigma = (I, c_1, \ldots, c_n, r_1, \ldots, r_n)$. $\mathbf{VER}(\sigma) =$ "true", this means that

$$\begin{cases} L'_i = r_i G + c_i P_i \\ R'_i = r_i \mathcal{H}_p(P_i) + c_i I \\ \sum\limits_{i=1}^{n} c_i = \mathcal{H}_s(m, L'_1, \ldots, L'_n, R'_1, \ldots, R'_n) \mod l \end{cases}$$

The first two equalities imply

$$\begin{cases} \log_G L'_i = r_i + c_i x_i \\ \log_{\mathcal{H}_p(P_i)} R'_i = r_i + c_i \log_{H_p(P_i)} I \end{cases}$$

where $\log_A B$ informally denotes the discrete logarithm of B to the base A.

As in [24] we note that $\nexists i : x_i = \log_{\mathcal{H}_p(P_i)} I$ implies that all c_i's are uniquely determined. The third equality forces the adversary to find a pre-image of $\mathcal{H}_s$ to succeed in the attack, an event whose probability is considered to be negligible. □

Exculpability

Theorem 2. *Our one-time ring signature scheme is exculpable under the discrete logarithm assumption in the random oracle model.*