Proof of Theorem 1

Sarang Noether

June 22, 2020

Proof. Let $\mathtt{A}$ be a (t, ϵ, q)-solver of the unforgeability game of Definition 7. We show how to construct an algorithm $\mathtt{B}$ that executes $\mathtt{A}$ in a black box and is a solver of the non-slanderability game of Definition 8. Observe that the signing and corruption oracles are identical in both definitions, so such queries may be seamlessly passed between players, as we describe below. Formally, $\mathtt{B}$ operates in the following manner:

- $\mathtt{B}$ receives a set of public keys $S = \{pk_i\}_{i=0}^{q-1}$ from its challenger. It samples messages and rings (in the manner of Definition 7) and generates a set of tuples $\{(m_i, Q_i, \sigma_i)\}_{i=0}^{q-1}$ by queries of the form $\mathtt{SO}(m_i, Q_i, l_i) \rightarrow \sigma_i$, where each l_i is the index of pk_i in Q_i. It passes the public key set S to $\mathtt{A}$
- $\mathtt{B}$ accepts $\mathtt{SO}$ and $\mathtt{CO}$ oracle queries from $\mathtt{A}$, passes them to its challenger, and returns the results to $\mathtt{A}$.
- $\mathtt{A}$ returns a tuple (m, Q, σ) satisfying the conditions in Definition 7.
- $\mathtt{B}$ outputs (m, Q, σ).

Since $\mathtt{A}$ is a solver of the unforgeability game, then with advantage ϵ there exists an index $i \in [0, q)$ such that $\mathtt{LINK}((m, Q, \sigma), (m_i, Q_i, \sigma_i)) = 1$ and $pk_i \in S \cap Q \setminus C$. Further, $\mathtt{B}$ obtained σ_i by an oracle query $\mathtt{SO}(m_i, Q_i, l_i)$, so by construction $pk_i \in Q_i$ as well. Since $\mathtt{B}$ uses additional time t' for its initial q signing oracle queries and transcript lookup and has identical advantage ϵ as $\mathtt{A}$ does, we have constructed a $(t + t', \epsilon, q)$-solver of the non-slanderability game of Definition 8.

We now show the converse of the statement, and assume that $\mathtt{A}$ is a (t, ϵ, q)-solver of the non-slandeability game of Definition 8. We will construct an algorithm $\mathtt{B}$ that executes $\mathtt{A}$ in a black box and is a solver of the unforgeability game of Definition 7.

- $\mathtt{B}$ receives a set of public keys $S = \{pk_i\}_{i=0}^{q-1}$ from its challenger. It passes the public key set S to $\mathtt{A}$
- $\mathtt{B}$ accepts $\mathtt{SO}$ and $\mathtt{CO}$ oracle queries from $\mathtt{A}$, passes them to its challenger, and returns the results to $\mathtt{A}$.
- $\mathtt{A}$ returns a tuple (m, Q, σ) satisfying the conditions in Definition 8.
- $\mathtt{B}$ outputs (m, Q, σ).

Since $\mathtt{A}$ is a solver of the non-slanderability game, then with advantage ϵ there exists a signing oracle query $\mathtt{SO}(m^*, Q^*, l^*) \rightarrow \sigma^*$ such that $\mathtt{LINK}((m, Q, \sigma), (m^*, Q^*, \sigma^*)) = 1$ and $pk_{l^*}^* \in S \cap Q^* \cap Q \setminus C$. But since $pk_{l^*}^* = pk_i \in S$ for some index $i \in [0, q)$, the unforgeability challenger produced a valid signature σ_i on some message m_i and ring Q_i where $pk_i \in Q_i$. Hence it must be the case that $\mathtt{LINK}((m^*, Q^*, \sigma^*), (m_i, Q_i, \sigma_i)) = 1$, and by transitivity it follows that $\mathtt{LINK}((m, Q, \sigma), (m_i, Q_i, \sigma_i)) = 1$ as well. We therefore have shown that $\mathtt{B}$ is a (t, ϵ, q)-solver of the unforgeability game, which completes the proof. □