Rewriting Rules for Primitives

Sven Laur
swen@math.ut.ee

University of Tartu
Encryption
The complexity of the games must be less than $t$ for $(t, \varepsilon)$-IND-CPA secure cryptosystem. In the formal reduction, the whole game is converted to the IND-CPA distinguisher.
The complexity of the games must be less than $t$ for $(t, \varepsilon)$-IND-CCA1 secure cryptosystem. In the formal reduction, the whole game is converted to the IND-CCA1 distinguisher.
IND-CCA2 security

The reduction is valid if the challenge encryption $c$ is never decrypted in the games $G_0$ and $G_1$. The complexity of the games must be less than $t$ for $(t, \varepsilon)$-IND-CCA2 secure cryptosystem. In the formal reduction, the whole game is converted to the IND-CCA2 distinguisher.
Message Authentication
MAC security

\[ G_0^A \]

\[
\begin{align*}
\text{sk} & \leftarrow \text{Gen} \\
\ldots
\text{t}_1 & \leftarrow \text{Mac}_{sk}(m_1) \\
\ldots \\
\text{t}_q & \leftarrow \text{Mac}_{sk}(m_q) \\
\ldots \\
\text{if } \text{Ver}_{sk}(m, t) = 0 \text{ then return } 0 \\
\text{if } m \notin \{m_1, \ldots, m_q\} \text{ then Do something bad}
\end{align*}
\]

\[ G_1^A \]

\[
\begin{align*}
\text{sk} & \leftarrow \text{Gen} \\
\ldots \\
\text{t}_1 & \leftarrow \text{Mac}_{sk}(m_1) \\
\ldots \\
\text{t}_q & \leftarrow \text{Mac}_{sk}(m_q) \\
\ldots \\
\text{if } \text{Ver}_{sk}(m, t) = 0 \text{ then return } 0
\end{align*}
\]

The reduction is valid if sk is used only for computing the \( \text{Ver}_{sk}(\cdot) \) predicate and for computing \( \text{Mac}_{sk}(m_1), \ldots, \text{Mac}_{sk}(m_q) \). The complexity of the games must be less than \( t \) for \((t, q, \varepsilon)\)-secure message authentication code.
Hash Functions
Collision resistance

The complexity of the games must be less than $t$ for $(t, \varepsilon)$-collision resistant hash function family $\mathcal{H}$. 
Commitment Schemes
Hiding

The complexity of the games must be less than $t$ for $(t, \varepsilon)$-hiding secure commitment scheme.
The complexity of the games must be less than \( t \) for a \((t, \varepsilon)\)-binding commitment scheme.