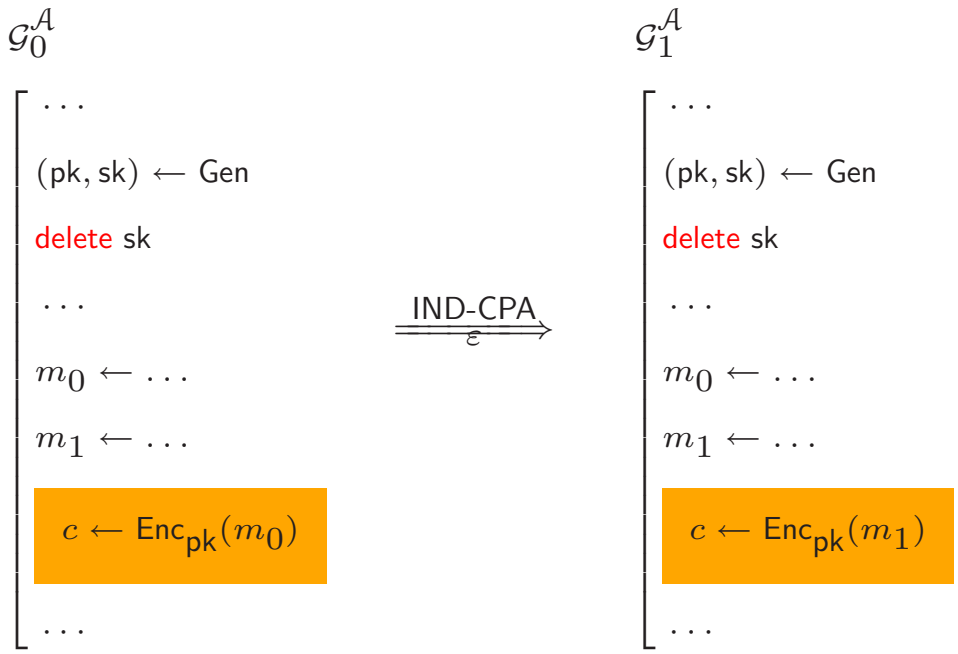
Rewriting Rules for Primitives

Sven Laur
swen@math.ut.ee

University of Tartu

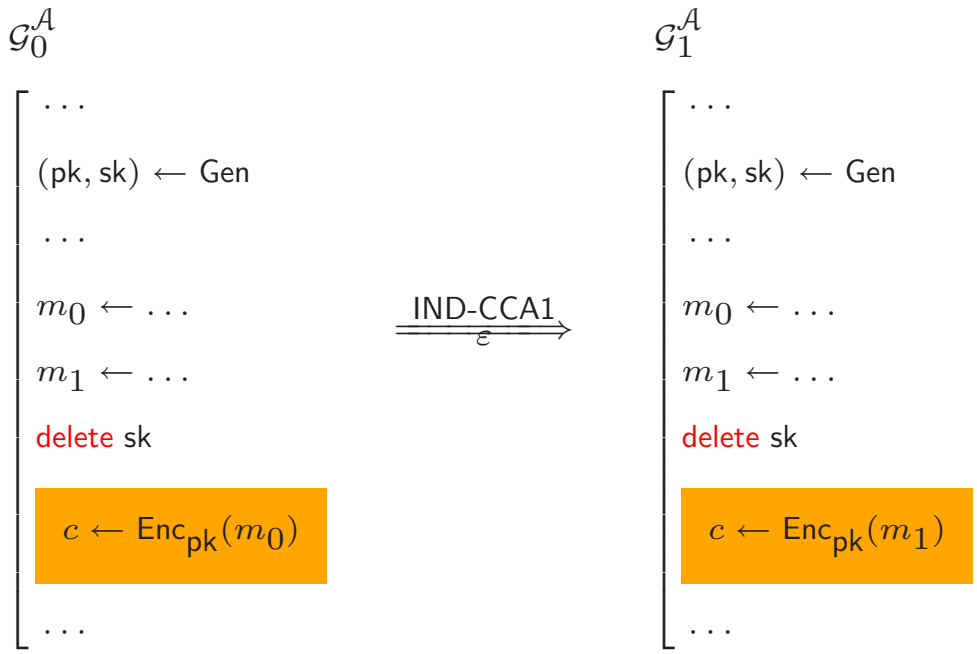
Encryption

IND-CPA security



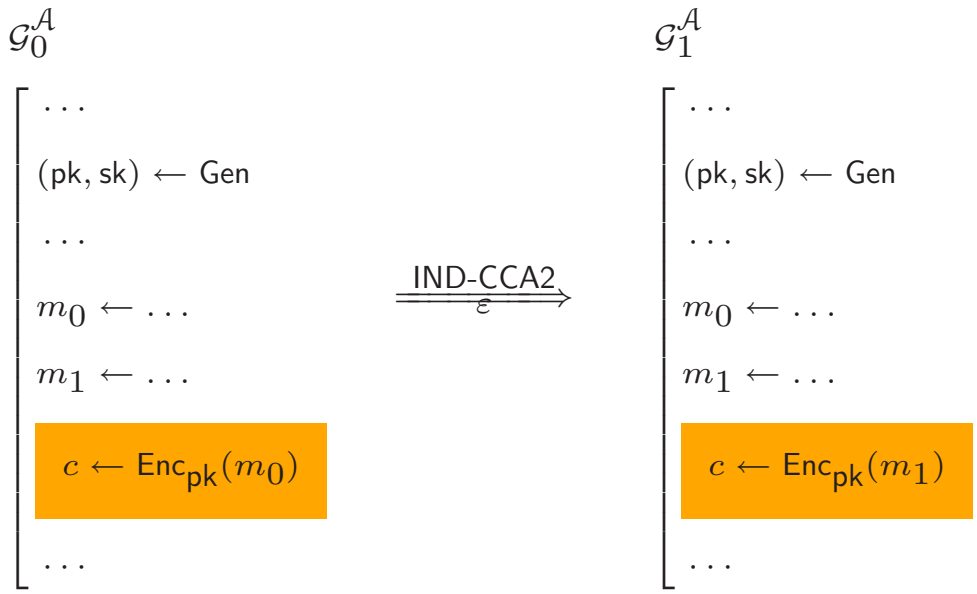
The complexity of the games must be less than t for (t, ε)-IND-CPA secure cryptosystem. In the formal reduction, the whole game is converted to the IND-CPA distinguisher.

IND-CCA1 security



The complexity of the games must be less than t for (t, ε)-IND-CCA1 secure cryptosystem. In the formal reduction, the whole game is converted to the IND-CCA1 distinguisher.

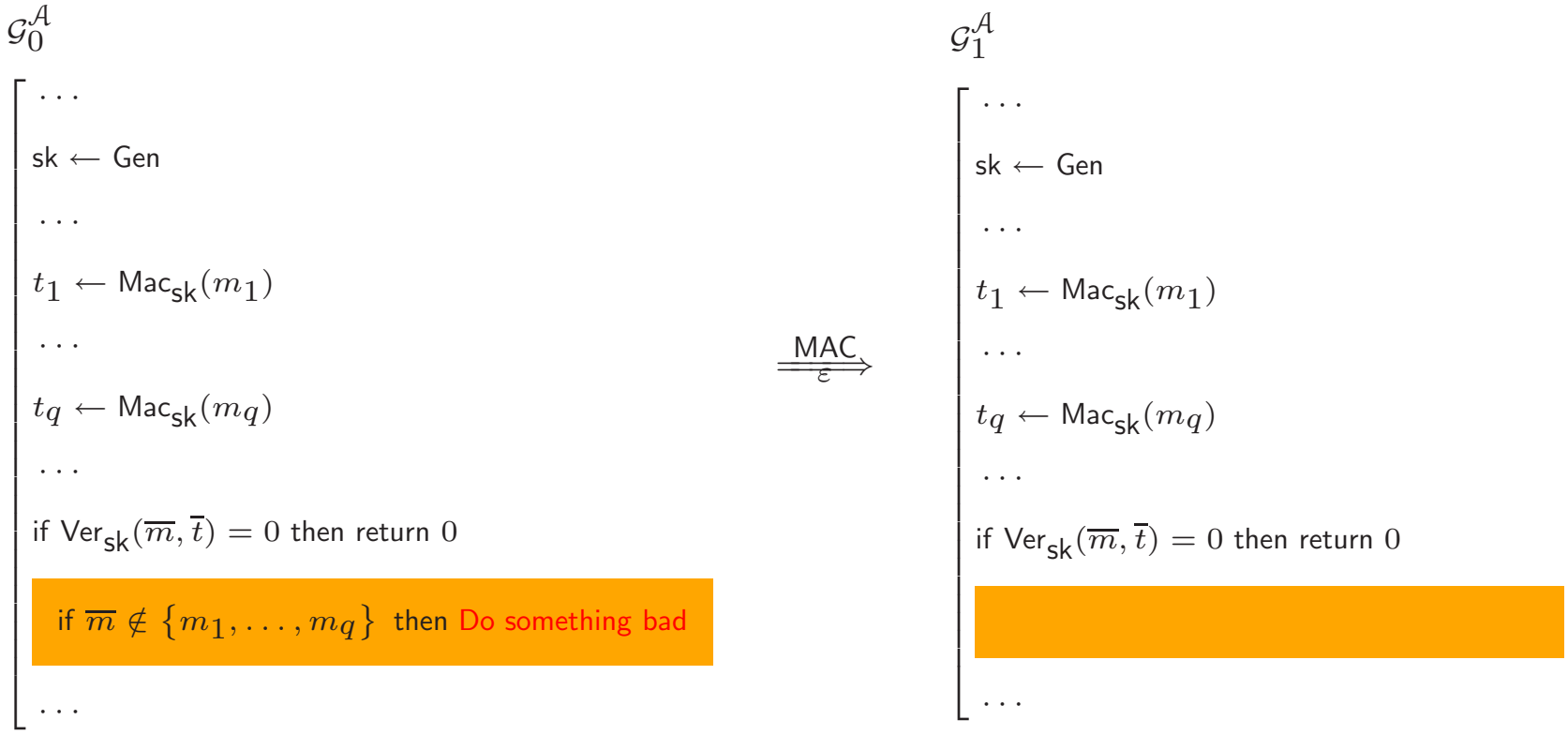
IND-CCA2 security



The reduction is valid if the challenge encryption c is never decrypted in the games $\mathcal{G}_0$ and $\mathcal{G}_1$. The complexity of the games must be less than t for (t, ε)-IND-CCA2 secure cryptosystem. In the formal reduction, the whole game is converted to the IND-CCA2 distinguisher.

Message Authentication

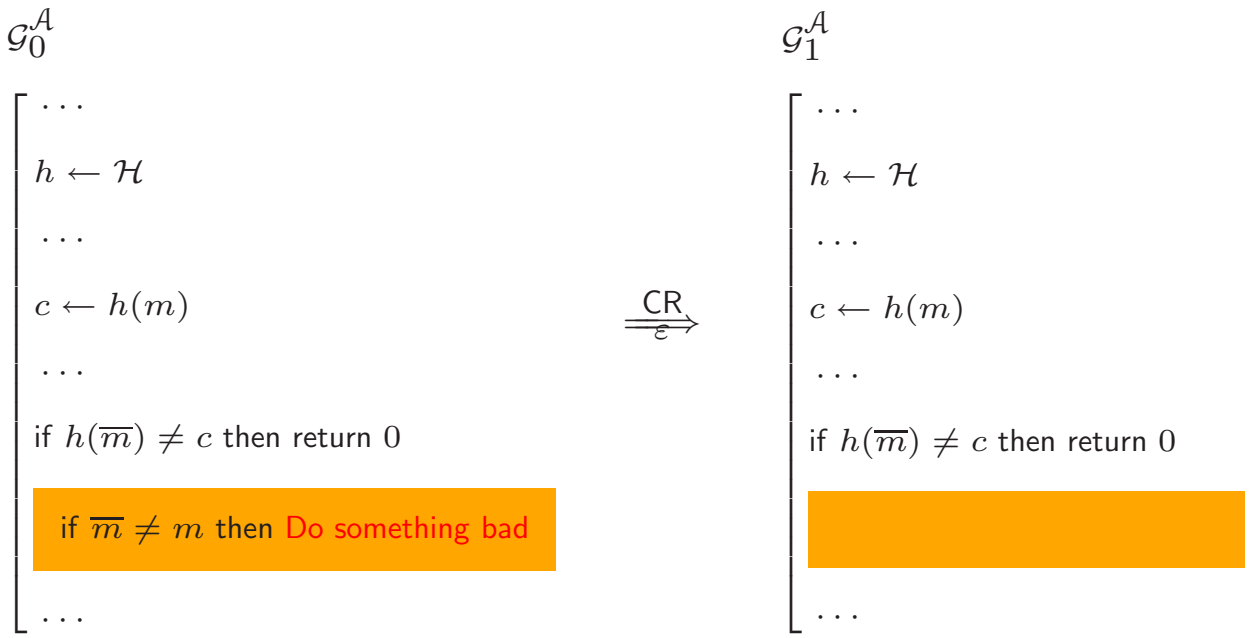
MAC security



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

Hash Functions

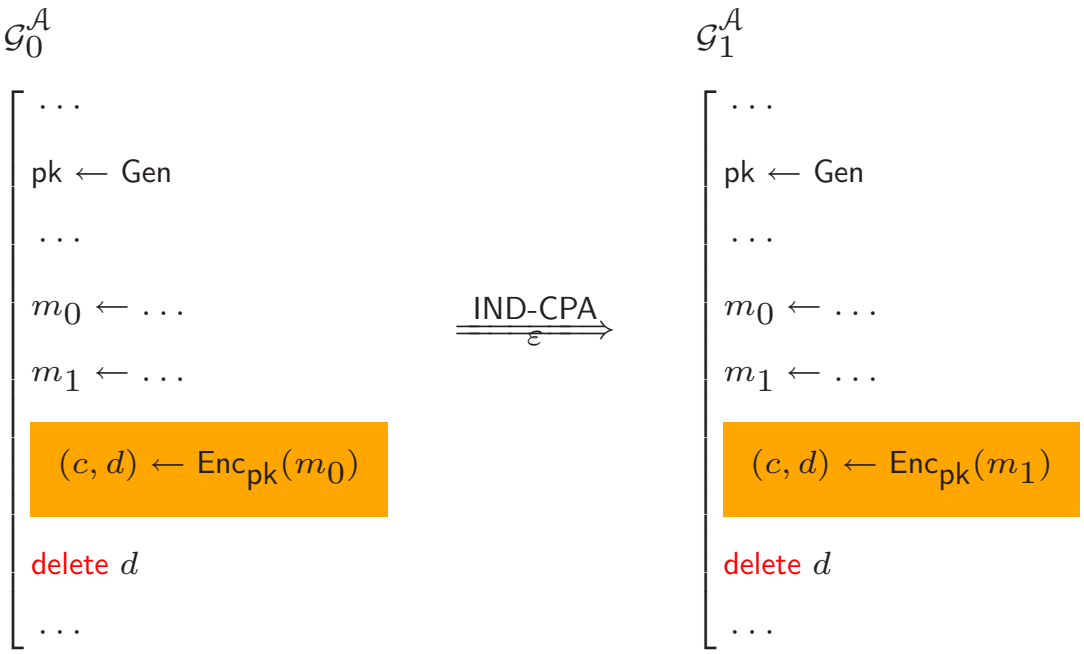
Collision resistance



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

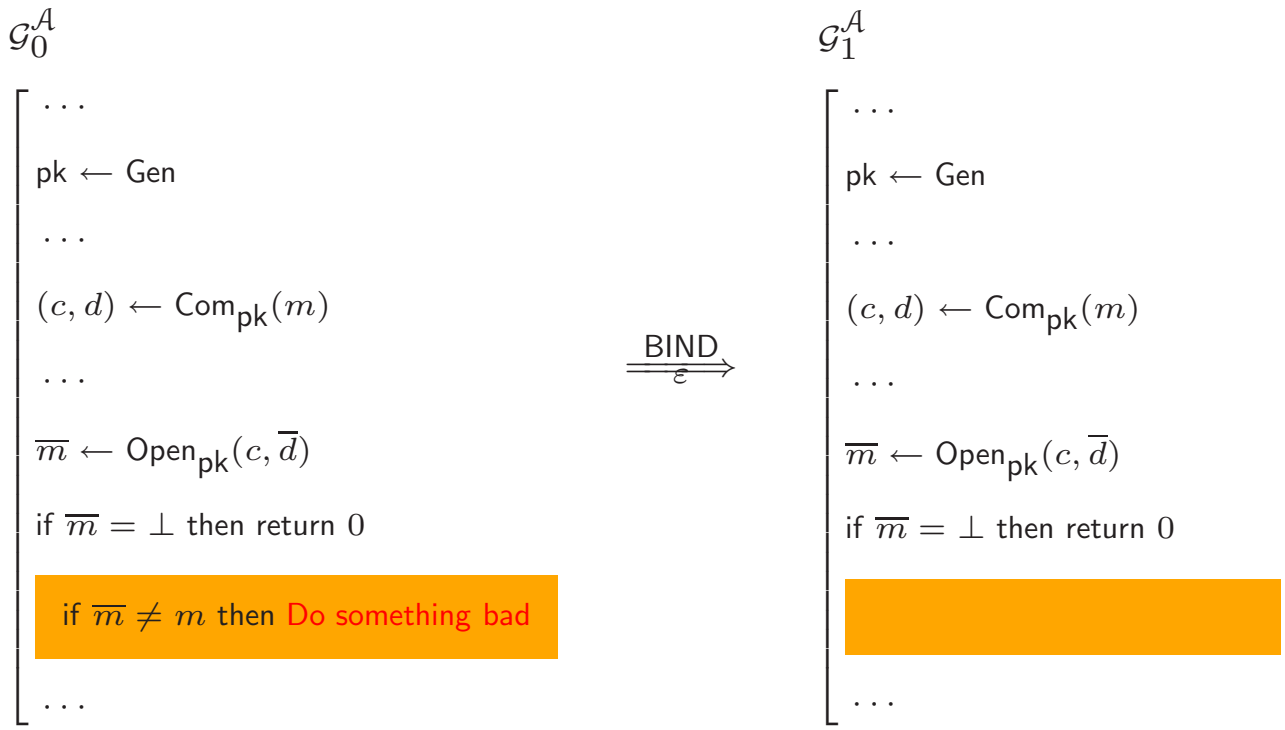
Commitment Schemes

Hiding



The complexity of the games must be less than t for (t, ε)-hiding secure commitment scheme.

Binding



The complexity of the games must be less than t for a (t, ε)-binding commitment scheme.