ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

S. Mödersheim
Ch. Sprenger
AS 2009

Formal Methods for Information Security

Exercise Sheet 9

Hand-in date: Nov 30, 2009

Assignment 9.1: Security of encryption schemes

Let $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be an encryption scheme. In the lecture, we have defined that Π is type-0 secure if for all probabilistic polynomial-time adversaries A

$$Adv^0_{\Pi[\eta]}(A) = \Big| Pr[k, k' \xleftarrow{R} \mathcal{K}(\eta) : A^{\mathcal{E}_k(\cdot),\mathcal{E}_{k'}(\cdot)}(\eta) = 1] - Pr[k \xleftarrow{R} \mathcal{K}(\eta) : A^{\mathcal{E}_k(\bot),\mathcal{E}_k(\bot)}(\eta) = 1] \Big|$$

as a function of η is negligible.

(a) Show that Π is not type-0 secure, if $\mathcal{E}$ is deterministic.

(b) Suppose Π is which-key revealing. Show that it is not type-0 secure and modify the definition to capture the security of which-key revealing encryption schemes.

(c) Suppose Π is length-revealing. Show that it is not type-0 secure and adapt the definition to capture the security of length-revealing encryption schemes.

(d) Show that the modified definition obtained by replacing $\mathcal{E}_{k'}(\cdot)$ by $\mathcal{E}_{k'}(\bot)$ in the first probability is as strong as the original one. Hint: Consider all pairwise differences between the following probabilities and use the triangle inequality to relate them:

$$\begin{aligned} p(\eta) &= Pr[k, k' \xleftarrow{R} \mathcal{K}(\eta) : A^{\mathcal{E}_k(\cdot),\mathcal{E}_{k'}(\cdot)} = 1] \\ q(\eta) &= Pr[k, k' \xleftarrow{R} \mathcal{K}(\eta) : A^{\mathcal{E}_k(\cdot),\mathcal{E}_{k'}(\bot)} = 1] \\ r(\eta) &= Pr[k \xleftarrow{R} \mathcal{K}(\eta) : A^{\mathcal{E}_k(\bot),\mathcal{E}_k(\bot)} = 1] \end{aligned}$$

Assignment 9.2: Formal and computational equivalence

In this exercise, we explore the definitions of formal and computational equivalence of terms.

(a) Prove or disprove the following equivalences:

(1) $K \equiv K'$, $K \cong K'$, and $[\![K]\!]_\Pi \approx [\![K']\!]_\Pi$

(2) $(\{\!|0|\!\}_{K_4}, K_1) \equiv (\{\!|0|\!\}_{K_2}, K_1)$
(3) $(K_1, \{\!|0, \{\!|K_4|\!\}_{K_2}|\!\}_{K_1}) \cong (K_2, \{\!|0, \{\!|1, 1|\!\}_{K_7}|\!\}_{K_2})$ and same with $\equiv$.

(b) Model a length-sensitive variant of the formal equivalence relation $\equiv$, i.e., a relation that is able to distinguish undecryptable ciphertexts of cleartexts with different lengths.

(c) Prove that $[\![\{\!|0|\!\}_K]\!]_\Pi \approx [\![\{\!|1|\!\}_K]\!]_\Pi$.
Hint: do a specialized version of the computational soundness proof.