ETH Zürich, D-INFK
Spring 2019

Prof. Ueli Maurer
Fabio Banfi
Daniel Jost
Jiamin Zhu

Cryptography Foundations

Exercise 9

9.1 Random Self-Reducibility of the Computational Diffie-Hellman Problem

Goal*: We consider the computational Diffie-Hellman problem as an example of random-self reducible problems.*

Prove that the CDH problem is random self-reducible.

9.2 Properties of the Distinguishing Advantage

Goal*: Recall the notion of a pseudo-metric and prove a related lemma of the lecture notes.*

Prove Lemma 4.10 from the lecture notes, i.e., show that for any $\mathcal{D}$ that is closed under complementing the output bit, $\Delta^{\mathcal{D}}$ is a pseudo-metric.

9.3 Cloning the MAC-forgery Game

Goal*: The MAC-forgery game as presented in the lecture notes is not clonable. This task explores the reason and investigates a weaker variant of the game which can be cloned.*

A MAC for message space $\mathcal{M}$, key space $\mathcal{K}$, and tag space $\mathcal{T}$ is a function $f : \mathcal{M} \times \mathcal{K} \to \mathcal{T}$. The security of a MAC can be defined by a game $\mathbf{G}$ that allows the adversary to obtain valid MACs for chosen messages, and finally takes as input a pair (m, t) such that m has not been queried before. The game is won if the pair (m, t) constitutes a valid message/MAC-pair. We strengthen this definition such that the adversary has multiple attempts to forge; the game is won if at least one such attempt is successful.

a) Show that the "straightforward" system $\mathbf{K}$ that emulates q copies of the MAC-forgery game by simply forwarding the inputs and outputs does not achieve cloning, even if the MAC-forgery game allows multiple attempts to forge.

In a *fixed-target MAC-forgery game* the message for which the adversary has to forge a MAC is fixed in the beginning by the game system $\mathbf{G}_{\mathsf{fix}}$. More detailed, the game $\mathbf{G}_{\mathsf{fix}}$ can be described as:

- Generate the key $k \in \mathcal{K}$ uniformly at random and choose the target message $\hat{m} \in \mathcal{M}$ according to some distribution.[1] Output $\hat{m}$ at the right interface.
- On input a message $m \in \mathcal{M}$ at the right interface, if $m = \hat{m}$, then answer with $\perp$. Otherwise, compute $t = f(m, k)$ and answer with t.
- On input a MAC $\hat{t} \in \mathcal{T}$ at the right interface, set the output on the left interface to 1 if $\hat{t} = f(\hat{m}, k)$.

b) Show that the fixed-target MAC-forgery game with multiple verification queries is clonable by some efficient system $\mathbf{K}$.

[1] The distribution can be seen as a parameter of the game. The clonability holds independently of this distribution.