ETH Zürich, D-INFK
Spring 2018

Prof. Ueli Maurer
Christian Badertscher
Fabio Banfi

Cryptography Foundations

Exercise 12

12.1 Information-Theoretic Authentication Amplification

Goal: *We see that one mild synchronization assumption is sufficient to make information-theoretic authentication amplification possible.*

The idea of authentication amplification is that one constructs from authenticated channels with small message spaces (and insecure channels with large message spaces) an authenticated channel with a large message space, say $\mathcal{M}$.

Let $H : \mathcal{K} \times \mathcal{M} \to \mathcal{Z}$ be a δ-almost universal hash function and consider the following protocol idea: To send (just a single) message $m \in \mathcal{M}$, Alice first sends m over the insecure channel $\xrightarrow{\mathcal{M}}\!\!\!\!\!\rightarrow$. Once Bob activates, he fetches a message, say m' from the insecure channel and acknowledges the receipt via an authenticated (unary) channel $\xleftarrow{\{\diamond\}}\!\!\bullet$. Once Alice activates again and has received the acknowledgment, she chooses $K \in \mathcal{K}$ uniformly at random, computes $z := H_K(m)$ and sends the pair (K, z) over the authenticated channel $\bullet\xrightarrow{\mathcal{K}\times\mathcal{Z}}$. Bob (upon the next activation) receives this pair from the authenticated channel and outputs the message m' if and only if $H_K(m') = z$.

a) Describe with pseudo-code the resource AUTH' that we aim to construct: an authenticated channel that includes some form of coordination between Alice and Bob, i.e., with a particular condition on the activation sequence in order for Bob to output the message.

b) Let $\mathbf{R} := [\xrightarrow{\mathcal{M}}\!\!\!\!\!\rightarrow, \xleftarrow{\{\diamond\}}\!\!\bullet, \bullet\xrightarrow{\mathcal{K}\times\mathcal{Z}}]$ and $\mathbf{S} := \mathsf{AUTH}'$. Write down the above protocol idea as a pair of converters (π_1, π_2) and show that $\Delta(\pi_1^A \pi_2^B \mathbf{R}, \sigma^E \mathbf{S}) \leq \epsilon$ (for a non-trivial bound ϵ) holds and describe the corresponding simulator σ. To simplify your task, assume that Eve injects at most one message, i.e., that $q_E = 1$ for the insecure channel $\longrightarrow\!\!\!\!\!\rightarrow$.

Hint: The definitions of the channel resources $\longrightarrow\!\!\!\!\!\rightarrow$ (where you can use $q_A = q_E = 1$) and $\bullet\!\!\longrightarrow$ as pseudo-code are found in Exercise 2.3 (recall that $\longleftarrow\!\!\bullet$ is defined as $\bullet\!\!\longrightarrow$ but with A being the receiver interface and B being the sender interface).

12.2 CBC-MAC and Prefix-Free Encodings

Goal: *We have seen in the lecture that the CBC-MAC is secure if the encoding used by the block-former is prefix-free. We analyze such prefix-free encodings and discover that the CBC-MAC is not secure if the encoding is not prefix-free.*

The CBC-MAC is described by a converter CBC that connects to a $(\{0,1\}^n, \{0,1\}^n)$-system $\mathbf{F}$. In more detail, CBC takes inputs $x \in \{0,1\}^*$ and applies to them a block-former, which consists of using some encoding to obtain $\tilde{x} \in \{0,1\}^{\ell n}$ for $\ell \in \mathbb{N}$, and then splitting $\tilde{x}$ into $\tilde{x} = \tilde{x}_1 \mid \cdots \mid \tilde{x}_\ell$. CBC then iteratively computes y_j by invoking $\mathbf{F}$ on input $\tilde{x}_j \oplus y_{j-1}$ (where $y_0 = 0^n$), and finally outputs y_ℓ.

a) Consider the converter CBC' that uses the following encoding: On input a string $x \in \{0,1\}^*$, a "1"-bit is appended to x. Then, sufficiently many "0"-bits are appended to obtain $\tilde{x}$ such that n divides $|\tilde{x}|$.

Show that $\theta_r \mathsf{CBC}' \mathbf{R}_{n,n} \notin (\theta_r \mathbf{V}_n)^\epsilon$ for $\epsilon \leq \frac{1}{2} r^2 2^{-n}$, i.e., provide a distinguisher $\mathbf{D}$ such that $\Delta^{\mathbf{D}}(\theta_r \mathsf{CBC}' \mathbf{R}_{n,n}, \theta_r \mathbf{V}_n) > \frac{1}{2} r^2 2^{-n}$ (which is larger than bound shown in Theorem 6.1).

b) Describe a prefix-free encoding.

12.3 Uniform Random Functions with Variable Input-Length

Goal*: In this task we analyze how one can construct a VIL-URF* $\mathbf{V}_n$ only *from a random function* $\mathbf{R}_{m,n}$*, i.e., without assuming an additional key.*

In the lecture, we have seen a construction of a VIL-URF $\mathbf{V}_n$ from a URF $\mathbf{R}_{m,n}$ and a k-bit key $\mathbf{U}_k$, using a δ-AUH H with m-bit output. Describe such a construction of a VIL-URF *only* from $\mathbf{R}_{m,n}$, that is, find a *deterministic* converter α', an upper bound $\epsilon'_{r,l}$, and an $s_r \in \mathbb{N}$ such that

$$\tau_{r,l}\alpha'[s_r]\mathbf{R}_{m,n} \in (\tau_{r,l}\mathbf{V}_n)^{\epsilon'_{r,l}},$$

where $\tau_{r,l}$ denotes the converter that restricts access to at most r queries, each of length at most l.

Discussion of solutions:

28/29.5.2018 (Tasks 12.1, 12.2, and 12.3)

The Monday and Tuesday sessions of each week cover the same material.