Institute of Computer Science, University of Bern
Cryptography, HS 2019

Prof. Christian Cachin
Luca Zanolini

Exercise 3

3.1 Nested encryption scheme (3pt)

Let denote an encryption scheme where $\Sigma.\mathcal{C} \subseteq \Sigma.\mathcal{M}$ (so that it is possible to use the scheme to encrypt its own ciphertexts). Define Σ^2 to be de following nested-encryption scheme:

$\mathcal{K} = (\Sigma.\mathcal{K})^2$ $\mathcal{M} = \Sigma.\mathcal{M}$ $\mathcal{C} = \Sigma.\mathcal{C}$	$\underline{\mathsf{KeyGen}:}$ $k_1 \leftarrow \Sigma.\mathcal{K}$ $k_2 \leftarrow \Sigma.\mathcal{K}$ return (k_1, k_2)	$\underline{\mathsf{Enc}((k_1, k_2), m):}$ $c_1 := \Sigma.\mathsf{Enc}(k_1, m)$ $c_2 := \Sigma.\mathsf{Enc}(k_2, c_1)$ return c_2	$\underline{\mathsf{Dec}((k_1, k_2), c_2):}$ $c_1 := \Sigma.\mathsf{Dec}(k_2, c_2)$ $m := \Sigma.\mathsf{Dec}(k_1, c_1)$ return m

Prove that if Σ satisfies one-time secrecy, then so does Σ^2.

3.2 Negligible functions (2pt)

a) Which of the following are negligible functions in λ? Justify your answers.

$$\frac{1}{2^{\frac{\lambda}{2}}},\ \frac{1}{\lambda^2},\ \frac{1}{(\lambda)^{\frac{1}{\lambda}}},\ \frac{1}{\sqrt{\lambda}},\ \frac{1}{2^{\sqrt{\lambda}}}$$

b) Suppose f and g are negligible.

- Show that $f \cdot g$ is negligible.
- Give an example f and g which are both negligible, but where $\frac{f(\lambda)}{g(\lambda)}$ is not negligible.

3.3 Hashrate (2pt)

Let us consider a blockchain scenario and in particular the Bitcoin cryptocurrency. Miners inside the network repeatedly compute hashes of a block of size 1 MB until the resulting hash is smaller than a target. Let us assume that miners call one instance of SHA-256 per block.

The performance of fast SHA-256 implementations on Intel Architecture Processors are shown here `https://www.intel.com/content/dam/www/public/us/en/documents/white-papers/sha-256-implementations-paper.pdf`.

In particular, page 15 shows the performance in cycles/**byte** for varying sizes of an implementation-specific buffer.

a) Assuming you have one Intel CPU with 2GHz clock speed, how many cycles per block can one have in case of a single-threaded AVX1 implementation? How much is the hash rate?

b) How many such CPUs one should have to reach Bitcoin's current hash rate (consult `https://www.blockchain.com/` for example)?

3.4 A random cipher (3pt)

Consider a symmetric-key encryption scheme Σ that encrypts κ-bit strings into κ-bit ciphertexts.

a) Describe the algorithms of Σ formally.

b) Consider the following library, which uses Σ and gives an adversary $\mathcal{A}$ access to $\Sigma.\mathsf{Enc}()$, but not to $\Sigma.\mathsf{Dec}()$.

$$\boxed{\begin{array}{l} k \leftarrow \Sigma.\mathsf{KeyGen}() \\ \\ \underline{\textsc{encrypt}(x \in \{\mathtt{0},\mathtt{1}\}^\kappa)} \\ \quad \text{return } \Sigma.\mathsf{Enc}(k, x) \end{array}}$$

A random $m \leftarrow \{\mathtt{0},\mathtt{1}\}^\kappa$ is chosen and $\mathcal{A}$ receives $c := \textsc{encrypt}(m)$. $\mathcal{A}$ is allowed to access the library at most q times and the task of $\mathcal{A}$ is to guess m. Give an upper bound on the probability that $\mathcal{A}$ succeeds, that is, on

$$P[\mathcal{A}(c) \Rightarrow m].$$