ETH Zürich, D-INFK
Spring 2018

Prof. Ueli Maurer
Christian Badertscher
Fabio Banfi

Cryptography Foundations
Exercise 1

1.1 Variants of the CPA Game for Symmetric Encryption Schemes

Goal*: We explore that there is not just one game to formalize the idea behind CPA security.*

Let the bit-guessing problem (S_t^{ind}, B) be the t-messages IND-CPA game from Definition 2.2 in the lecture notes (where B corresponds to b in the lecture notes, and Z to b'). We define new bit-guessing problems by modifying the game in each subtask in a specific way.

a) We replace steps 3 and 4 of the game by the following steps.

> 3. The adversary chooses just one challenge message m.
> 4. The challenger chooses a uniformly random bit B;
>   - If $B = 0$, it computes the encryption of m, i.e., $c = e(m, k, r)$ for fresh and independent randomness value $r \in \mathcal{R}$, and returns c to the adversary.
>   - If instead $B = 1$, the challenger chooses a uniformly random message $\widetilde{m}$ of length $|m|$ and computes the encryption of $\widetilde{m}$, i.e., $\widetilde{c} = e(\widetilde{m}, k, \widetilde{r})$ for fresh and independent randomness value $\widetilde{r} \in \mathcal{R}$, and returns $\widetilde{c}$ to the adversary.

We call this new game t-msg-RCH-CPA,[1] and we identify it by the bit-guessing problem (S_t^{rch}, B). Argue that the new game captures the "CPA-notion" equally good by proving the following two statements.

i. Given a distinguisher D for (S_t^{rch}, B), design a new distinguisher D' (which internally uses D) for (S_t^{ind}, B) so that $\Lambda^D\big((S_t^{\mathsf{rch}}, B)\big) = \Lambda^{D'}\big((S_t^{\mathsf{ind}}, B)\big)$.[2]

ii. Given a distinguisher D for (S_t^{ind}, B), design a new distinguisher D' (which internally uses D) for (S_t^{rch}, B) so that $\Lambda^D\big((S_t^{\mathsf{ind}}, B)\big) = 2 \cdot \Lambda^{D'}\big((S_t^{\mathsf{rch}}, B)\big)$.

b) Now, we consider an at first sight different game, called t-msg-ROR-CPA.[3] It consists of only three steps between the challenger and the adversary:

> 1. The challenger chooses a key k according to the key distribution as well as a uniformly random bit B.
> 2. The adversary can choose up to t messages; for each message m, the challenger acts as follows:
>   - If $B = 0$, it computes the encryption of m, i.e., $c = e(m, k, r)$ for fresh and independent randomness value $r \in \mathcal{R}$, and returns c to the adversary.
>   - If instead $B = 1$, the challenger chooses a uniformly random message $\widetilde{m}$ of length $|m|$ and computes the encryption of $\widetilde{m}$, i.e., $\widetilde{c} = e(\widetilde{m}, k, \widetilde{r})$ for fresh and independent randomness value $\widetilde{r} \in \mathcal{R}$, and returns $\widetilde{c}$ to the adversary.
> 3. The adversary guesses B by issuing a guess Z.

[1] This stands for random-challenge CPA game.
[2] Note that B is the same name for two random variables defined in two different random experiments!
[3] This stands for real-or-random CPA game.

We identify this new game by the bit-guessing problem (S_t^{ror}, B). We again ask to prove the following implications:

i. Given a distinguisher D for (S_t^{rch}, B), design a new distinguisher D' (which internally uses D) for $(S_{t+1}^{\mathsf{ror}}, B)$ so that $\Lambda^D\big((S_t^{\mathsf{rch}}, B)\big) = 2 \cdot \Lambda^{D'}\big((S_{t+1}^{\mathsf{ror}}, B)\big)$.
Hint: The total of $t+1$ queries is simply due to the fact that the challenge query is also a query.

ii. Given a distinguisher D for (S_t^{ror}, B), design a new distinguisher D' (which internally uses D) for $(S_{t-1}^{\mathsf{rch}}, B)$ so that $\Lambda^D\big((S_t^{\mathsf{ror}}, B)\big) = t \cdot \Lambda^{D'}\big((S_{t-1}^{\mathsf{rch}}, B)\big)$.
Hint: This is a hard task. Think again of distinguisher D' trying to mimic towards D an execution of the ROR-CPA game. At some point in this emulation, D' has to make its challenge query (e.g., choose i at random from $\{1, \dots, t\}$ and let the i-th query be the challenge query). Note also that D' gets true encryptions of all its queried non-challenge messages but can also decide to get encryptions to random messages at any time (by querying random messages). You should use both Lemma 2.2 and Lemma 2.3.

c) Explain in words why these implication statements of **a)** and **b)** are important in cryptography.

1.2 On the Security of the One-Time Pad

Goal*: We prove the security of the one time pad in general for finite groups.*

Let $\langle \mathbb{G}; + \rangle$ be a finite group (written in additive notation) and U, X two independent random variables over $\mathbb{G}$, with U uniformly distributed. Show that $U + X$ and X are independent.

Hint: As an intermediate step, you should show that since U is uniformly distributed, then so is $U + X$.

1.3 Properties of the Distinguishing Advantage

Goal*: We prove some basic results about the distinguishing advantage that are stated in the lecture notes without proof.*

a) Prove Lemma 2.1 in the lecture notes, i.e., show that for two random variables X and Y, the advantage of the best distinguisher for X and Y is the statistical distance between X and Y, that is,

$$\Delta(X, Y) = \delta(X, Y).$$

b) Prove Lemma 2.4 from the lecture notes, i.e., for a bit-guessing problem (S, B), show that from a distinguisher D which is given either the pair (S, B) or the pair (S, U) for U uniformly distributed and independent of S (that is, D can interact with the system S and receives either the bit B, correlated with S, or the uncorrelated bit U), we can construct a distinguisher D' for the bit-guessing problem (S, B) which has twice the same advantage, that is,

$$\Delta^D\big((S, B), (S, U)\big) = \frac{1}{2}\Lambda^{D'}\big((S, B)\big).$$

Hint: First show that $\Lambda^{D'}((S, B)) = \Delta^D((S, B), (S, \overline{B}))$, where D' should make use of D and a uniform bit U, and then show that $\Delta^D((S, B), (S, U)) = \frac{1}{2}\Delta^D((S, B), (S, \overline{B}))$ ($\overline{B}$ is the negation of the bit B).

Discussion of solutions:

26/27.2.2018 (Tasks 1.1a, 1.1c, 1.2 and 1.3a)

5/6.3.2018 (Tasks 1.1b, 1.3b)

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