ETH Zürich, D-INFK
Spring 2019

Prof. Ueli Maurer
Fabio Banfi
Daniel Jost
Jiamin Zhu

Cryptography Foundations
Solution Exercise 1

1.1 Variant of the IND-CPA Bit-Guessing Problem

a) The idea is to construct a distinguisher D' for the bit-guessing problem $[\![S_t^{\mathsf{ind}}; B']\!]$. D' internally runs the assumed distinguisher D and emulates a view towards D that is identical to the interaction that D would have with the bit-guessing problem $[\![S_t^{\mathsf{rrc}}; B]\!]$. This way, the decision of D will help D' to guess the bit B'. For this, D' first forwards every message queried by D during phase 2 to S_t^{ind} and returns the obtained encryptions back to D. Once D reaches phase 3 and provides a challenge message m, D' samples a uniformly random message $\widetilde{m}$ of length $|m|$ and provides as challenge the two messages m and $\widetilde{m}$ to S_t^{ind}. Upon receiving the encryption c (of either m or $\widetilde{m}$), D' forwards this to D. Should D query any other message during phase 4, those will be again forwarded by D', and the encryptions thereof given back to D. Finally, D' issues as its guess Z' the same bit Z that D issues in the emulated interaction. Since this emulation by D' perfectly mimics $[\![S_t^{\mathsf{rrc}}; B]\!]$ towards D, we have $\Pr^{D'(S_t^{\mathsf{ind}}, B')}[Z' = B'] = \Pr^{D(S_t^{\mathsf{rrc}}, B)}[Z = B]$, and thus

$$\begin{aligned}\Lambda^{D'}([\![S_t^{\mathsf{ind}}; B']\!]) &= 2 \cdot \Pr^{D'(S_t^{\mathsf{ind}}, B')}[Z' = B'] - 1 \\ &= 2 \cdot \Pr^{D(S_t^{\mathsf{rrc}}, B)}[Z = B] - 1 \\ &= \Lambda^{D}([\![S_t^{\mathsf{rrc}}; B]\!]).\end{aligned}$$

b) Again, the idea is to construct a distinguisher D' for $[\![S_t^{\mathsf{rrc}}; B']\!]$ which internally runs the distinguisher D. Messages from D during the phases 2 and 4 are again simply forwarded. In the third phase, however, D provides two messages m_0 and m_1, but D' can only input a single message to the bit-guessing problem. As a consequence, D' chooses a uniform random bit $\widetilde{B}$, with the goal that D will guess $\widetilde{B}$, and provides the message $m_{\widetilde{B}}$ as challenge to S_t^{rrc}. Now, we consider two cases:

- If $B' = 0$, then challenge message $m_{\widetilde{B}}$ is encrypted by S_t^{rrc}. Therefore, D essentially interacts with the bit-guessing problem $[\![S_t^{\mathsf{ind}}; \widetilde{B}]\!]$ and hence,

$$\Pr^{D'(S_t^{\mathsf{rrc}}, B')}[Z = \widetilde{B} \,|\, B' = 0] = \Pr^{D(S_t^{\mathsf{ind}}, \widetilde{B})}[Z = \widetilde{B}].$$

- If $B' = 1$, then the challenge message is ignored by S_t^{rrc} and a uniformly random message is encrypted instead. Therefore, the interaction that D sees is independent of $\widetilde{B}$ and hence,

$$\Pr^{D'(S_t^{\mathsf{rrc}}, B')}[Z = \widetilde{B} \,|\, B' = 1] = \Pr^{D'(S_t^{\mathsf{rrc}}, B')}[Z \neq \widetilde{B} \,|\, B' = 1] = \frac{1}{2}.$$

So in short, if $B' = 0$, then D should be able to guess $\widetilde{B}$, and if $B' = 1$ then not. Turned around, if the guess Z from D matches $\widetilde{B}$, then D' can assume that $B' = 0$ and otherwise that $B' = 1$.

It remains to show that this strategy actually yields the correct advantage. To this end, let $Z' := Z \oplus \widetilde{B}$ be the guess submitted by D'. We then have,

$$\begin{aligned}
\Lambda^{D'}([\![S_t^{\mathsf{rrc}}; B']\!]) &= 2 \cdot \Pr^{D'(S_t^{\mathsf{rrc}}, B')}[Z' = B'] - 1 \\
&= 2 \cdot \Pr^{D'(S_t^{\mathsf{rrc}}, B')}[Z \oplus \widetilde{B} = B'] - 1 \\
&= 2 \cdot \Big(\Pr^{D'(S_t^{\mathsf{rrc}}, B')}[Z = \widetilde{B} \mid B' = 0] \cdot \frac{1}{2} \\
&\qquad + \Pr^{D'(S_t^{\mathsf{rrc}}, B')}[Z \neq \widetilde{B} \mid B' = 1] \cdot \frac{1}{2} \Big) - 1 \\
&= 2 \cdot \Pr^{D(S_t^{\mathsf{ind}}, \widetilde{B})}[Z = \widetilde{B}] \cdot \frac{1}{2} + 2 \cdot \frac{1}{2} \cdot \frac{1}{2} - 1 \\
&= \Pr^{D(S_t^{\mathsf{ind}}, B)}[Z = B] - \frac{1}{2} \\
&= \frac{1}{2} \cdot \Lambda^{D}([\![S_t^{\mathsf{ind}}; B]\!]).
\end{aligned}$$

1.2 On the Security of the One-Time Pad

First note that for any $g, h \in \mathbb{G}$ we have

$$\begin{aligned}
\Pr[U + X = g, X = h] &= \Pr[U = g + (-h), X = h] \\
&= \Pr[U = g + (-h)] \cdot \Pr[X = h] \\
&= \frac{1}{|\mathbb{G}|} \Pr[X = h], \qquad (1)
\end{aligned}$$

where in the second step we used that U and X are independent, and in the last step that U is uniformly distributed. Then by the law of total probability, for any $g \in \mathbb{G}$ we have

$$\Pr[U + X = g] = \sum_{h \in \mathbb{G}} \Pr[U + X = g, X = h] \overset{(1)}{=} \frac{1}{|\mathbb{G}|} \sum_{h \in \mathbb{G}} \Pr[X = h] = \frac{1}{|\mathbb{G}|}. \qquad (2)$$

Finally, putting the two equalities together, for any $g, h \in \mathbb{G}$ we have

$$\Pr[U + X = g, X = h] \overset{(1)}{=} \frac{1}{|\mathbb{G}|} \Pr[X = h] \overset{(2)}{=} \Pr[U + X = g] \cdot \Pr[X = h],$$

which is exactly the definition of $U + X$ and X being independent.

Note that the proof of security for the one-time pad over bitstrings of length n as introduced in the lecture notes is simply the instantiation of the above where U is the key, X is the message, $\mathbb{G}$ is the set $\{0,1\}^n$, the operation $+$ is the bit-wise XOR, the inverse operation is the identity function on $\{0,1\}^n$, and the neutral element is 0^n (the bitstring consisting of n zeros).

1.3 Properties of the Distinguishing Advantage

a) We divide the proof in two parts: first, we design a concrete distinguisher $D^\star$, and show that it is indeed optimal; then we show that its advantage in distinguishing random variables X and Y is indeed equal to their statistical distance $\delta(X, Y)$.

In order to find the optimal distinguisher $D^\star$, first note that it must be *deterministic*, since probabilistically mixing several deterministic strategies will result in a (weighted) average of the corresponding advantages. We therefore restrict our attention to a distinguisher D, that on input a realization of a random variable $X \in \mathcal{X}$ produces a binary guess $Z := D(X)$ according to a deterministic function $\mathcal{X} \to \{0,1\}$. Now, consider the so-called *maximum-likelihood* distinguisher, which for $\mathcal{X}^\star := \{x \in \mathcal{X} \mid \mathsf{P}_Y(x) \geq \mathsf{P}_X(x)\}$ is defined as

$$D^\star(x) := \begin{cases} 1, & x \in \mathcal{X}^\star, \\ 0, & x \notin \mathcal{X}^\star. \end{cases}$$

We then have

$$\Delta^{D^\star}(X,Y) = \Pr[D^\star(Y)=1] - \Pr[D^\star(X)=1] = \Pr[Y \in \mathcal{X}^\star] - \Pr[X \in \mathcal{X}^\star].$$

We next argue that $D^\star$ is indeed optimal. To this end, consider an arbitrary deterministic distinguisher D', which is characterized by a set $\mathcal{X}' \subseteq \mathcal{X}$, i.e.,

$$D'(x) := \begin{cases} 1, & x \in \mathcal{X}', \\ 0, & x \notin \mathcal{X}'. \end{cases}$$

Observe, that by definition of $\mathcal{X}^\star$, for any $x \in \mathcal{X}^\star$ we have $\mathsf{P}_Y(x) \geq \mathsf{P}_X(x)$, and thus

$$\Pr[Y \in (\mathcal{X}^\star \setminus \mathcal{X}')] \geq \Pr[X \in (\mathcal{X}^\star \setminus \mathcal{X}')],$$

and analogously, since $\mathsf{P}_Y(x) \leq \mathsf{P}_X(x)$ for any $x \notin \mathcal{X}^\star$,

$$\Pr[Y \in (\mathcal{X}' \setminus \mathcal{X}^\star)] \leq \Pr[X \in (\mathcal{X}' \setminus \mathcal{X}^\star)].$$

Hence, we obtain

$$\begin{aligned}
\Delta^{D'}(X,Y) &= \Pr[Y \in \mathcal{X}'] - \Pr[X \in \mathcal{X}'] \\
&\leq \Pr[Y \in \mathcal{X}'] - \Pr[X \in \mathcal{X}'] + \underbrace{\Pr[Y \in (\mathcal{X}^\star \setminus \mathcal{X}')] - \Pr[X \in (\mathcal{X}^\star \setminus \mathcal{X}')]}_{\geq 0} \\
&\quad + \underbrace{\Pr[X \in (\mathcal{X}' \setminus \mathcal{X}^\star)] - \Pr[Y \in (\mathcal{X}' \setminus \mathcal{X}^\star)]}_{\geq 0} \\
&= \big(\Pr[Y \in \mathcal{X}'] + \Pr[Y \in (\mathcal{X}^\star \setminus \mathcal{X}')] - \Pr[Y \in (\mathcal{X}' \setminus \mathcal{X}^\star)]\big) \\
&\quad - \big(\Pr[X \in \mathcal{X}'] + \Pr[X \in (\mathcal{X}^\star \setminus \mathcal{X}')] - \Pr[X \in (\mathcal{X}' \setminus \mathcal{X}^\star)]\big) \\
&= \Pr[Y \in \mathcal{X}^\star] - \Pr[X \in \mathcal{X}^\star] \\
&= \Delta^{D^\star}(X,Y).
\end{aligned}$$

Overall, we have shown so far that

$$\Delta(X,Y) = \sup_{D:\mathcal{X}\to\{0,1\}} \Delta^D(X,Y) = \Delta^{D^\star}(X,Y).$$

In the second part of the proof, we show that indeed $\Delta^{D^\star}(X,Y) = \delta(X,Y)$. We have

$$\begin{aligned}
\delta(X,Y) &= \frac{1}{2}\sum_{x\in\mathcal{X}} |\mathsf{P}_X(x) - \mathsf{P}_Y(x)| \\
&= \frac{1}{2}\sum_{x\in\mathcal{X}^\star} (\mathsf{P}_Y(x) - \mathsf{P}_X(x)) + \frac{1}{2}\sum_{x\in\mathcal{X}\setminus\mathcal{X}^\star} (\mathsf{P}_X(x) - \mathsf{P}_Y(x)) \\
&= \frac{1}{2}\left(\Pr[Y \in \mathcal{X}^\star] - \Pr[X \in \mathcal{X}^\star]\right) + \frac{1}{2}\left(1 - \Pr[X \in \mathcal{X}^\star] - (1 - \Pr[Y \in \mathcal{X}^\star])\right) \\
&= \frac{1}{2}\left(\Pr[Y \in \mathcal{X}^\star] - \Pr[X \in \mathcal{X}^\star]\right) + \frac{1}{2}\left(\Pr[Y \in \mathcal{X}^\star] - \Pr[X \in \mathcal{X}^\star]\right) \\
&= \Pr[Y \in \mathcal{X}^\star] - \Pr[X \in \mathcal{X}^\star] \\
&= \Delta^{D^\star}(X,Y).
\end{aligned}$$

Therefore, as claimed, we have shown that $\Delta(X,Y) = \delta(X,Y)$.

b) First we define the new distinguisher D' which internally uses the distinguisher D: it simply provides D with access to S and gives D a uniformly sampled bit U. Once D outputs its decision bit Z, D' outputs its guess bit $Z' := Z \oplus U$, that is, D' outputs 0 if and only if $Z = U$ (see Figure 1). Then, using the law of total probability on the partition defined by the (disjoint) events $U = B$ and $U \neq B$ (each clearly occurring with probability $\frac{1}{2}$), we have

$$\begin{aligned}
\Lambda^{D'}([\![S;B]\!]) &= 2 \cdot \Pr^{D'(S,B)}[Z' = B] - 1 \\
&= 2 \cdot \Pr^{D'(S,B)}[Z \oplus U = B] - 1 \\
&= 2 \cdot \Pr^{D'(S,B)}[Z = U \oplus B \,|\, U = B] \cdot \frac{1}{2} \\
&\quad + 2 \cdot \Pr^{D'(S,B)}[Z = U \oplus B \,|\, U \neq B] \cdot \frac{1}{2} - 1 \\
&= \Pr^{D[S,B]}[Z = 0] + \Pr^{D[S,\overline{B}]}[Z = 1] - 1 \\
&= \Pr^{D[S,\overline{B}]}[Z = 1] - \Pr^{D[S,B]}[Z = 1] \\
&= \Delta^{D}([S,B],[S,\overline{B}]).
\end{aligned}$$

Recall from the lecture that we consider here the problem of distinguishing pairs $[S, B]$ and $[S, U]$ where $[S, U]$ stands for a pair that is sampled like $[S, B]$, but where the distinguisher does not see the bit B (correlated with S), but an independent and uniformly distributed bit U. We again apply the law of total probability on the event whether B and U are identical and conclude:

$$\begin{aligned}
\Delta^{D}([S,B],[S,U]) &= \Pr^{D[S,U]}[Z = 1] - \Pr^{D[S,B]}[Z = 1] \\
&= \Pr^{D[S,U]}[Z = 1 \,|\, U = B] \cdot \frac{1}{2} \\
&\quad + \Pr^{D[S,U]}[Z = 1 \,|\, U \neq B] \cdot \frac{1}{2} - \Pr^{D[S,B]}[Z = 1] \\
&= \frac{1}{2} \cdot \Pr^{D[S,B]}[Z = 1] \\
&\quad + \frac{1}{2} \cdot \Pr^{D[S,\overline{B}]}[Z = 1] - \Pr^{D[S,B]}[Z = 1] \\
&= \frac{1}{2} \cdot \Pr^{D[S,\overline{B}]}[Z = 1] - \frac{1}{2} \cdot \Pr^{D[S,B]}[Z = 1] \\
&= \frac{1}{2} \cdot \Delta^{D}([S,B],[S,\overline{B}]).
\end{aligned}$$

Finally, putting the two equalities together, we have

$$\Delta^{D}([S,B],[S,U]) = \frac{1}{2} \cdot \Lambda^{D'}([\![S;B]\!]).$$

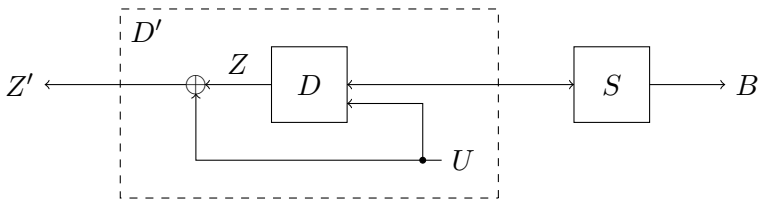

Figure 1: The mapping $D \mapsto D'$.