ETH Zürich, D-INFK
Spring 2018

Prof. Ueli Maurer
Christian Badertscher
Fabio Banfi

Cryptography Foundations

Solution Exercise 13

13.1 Key-Agreement Using a Trapdoor One-Way Permutation in the ROM

First note that the correctness condition is satisfied by the correctness of the underlying TOWP.
Consider the inversion game $\mathbf{G}$ from Definition 2.19 where the adversary can input arbitrarily many guesses x. We now define a simulator σ as follows:

- At the beginning, σ sets up an empty list $\mathcal{L}$ of pairs $(m, x) \in \{0,1\}^* \times \{0,1\}^k$.
- It then uses the trapdoor generator to obtain an algorithm F that implements a function f and a trapdoor, and outputs F at the outside sub-interface corresponding to $\longleftarrow\!\bullet$. Moreover, σ chooses K in the domain of f uniformly at random and outputs $f(K)$ at the outside sub-interface corresponding to $\bullet\!\longrightarrow$.
- At any point in time, σ answers queries at the interface simulated for $\mathbf{PO}_k$. Given a value $q \in \{0,1\}^*$, σ checks whether a pair (q, x) with $x \in \{0,1\}^k$ exists in the list $\mathcal{L}$. If this is not the case, a new value $x \in \{0,1\}^k$ is chosen uniformly at random and the tuple (q, x) is stored in $\mathcal{L}$. In both cases, the value x is provided as the output of $\mathbf{PO}_k$.

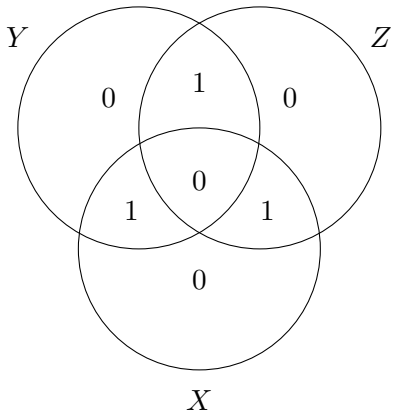
Let $\rho(\mathbf{D}) := \mathbf{DC}$ for the system $\mathbf{C}$, that will be connected to a distinguisher with the outside and to the game $\mathbf{G}$ with the inside interface, defined as follows. When the system $\mathbf{C}$ obtains the value F at the inside interface, it outputs F at the outside sub-interface E corresponding to $\longleftarrow\!\bullet$. On input y at the inside interface, $\mathbf{C}$ outputs y at the outside sub-interface of E corresponding to $\bullet\!\longrightarrow$. It further outputs a uniformly random $\kappa \in \{0,1\}^k$ at the outside sub-interfaces A and B. On input $q \in \{0,1\}^*$ at the outside sub-interface of E corresponding to $\mathbf{PO}_k$, $\mathbf{C}$ outputs q at the inside interface and outputs a uniformly random $x \in \{0,1\}^k$ at the outside sub-interface of E corresponding to $\mathbf{PO}_k$ if q is a fresh input; otherwise repeated inputs are answered consistently (by keeping a list as σ).
Let $\mathbf{R}' := \pi_1^A \pi_2^B[\bullet\!\longrightarrow, \longleftarrow\!\bullet, \mathbf{PO}_k]$ and $\mathbf{S}' := \sigma^E \bullet\!\!=\!\!=\!\!\bullet$. We define a monotone binary output A_i on both systems $\mathbf{R}'$ and $\mathbf{S}'$ such that $A_i = 0$ as long as the value K such that $f(K) = y$ has not been queried at the E-interface of $\mathbf{PO}_k$, where f is the function implemented by the algorithm F send over $\longleftarrow\!\bullet$ and y is the message transmitted over the channel $\bullet\!\longrightarrow$. We denote the systems enhanced with this MBO by $\hat{\mathbf{R}}'$ and $\hat{\mathbf{S}}'$, respectively. We have that $\hat{\mathbf{R}}' \overset{g}{\equiv} \hat{\mathbf{S}}' \overset{g}{\equiv} \mathbf{CG}$, i.e., they are equivalent as games since the values obtained from the channels are distributed identically in all systems, the key provided at the interfaces A and B is a uniformly random element from $\{0,1\}^k$, and the values returned by $\mathbf{PO}_k$ for fresh queries are uniformly random and independent of all other outputs as long as $A_i = 0$ (and consistency of the outputs is maintained).
Hence, we can use Lemma 4.16 and Lemma 4.15 to obtain

$$\overline{\langle \mathbf{R}' \,|\, \mathbf{S}' \rangle} \;\leq\; \overline{\hat{\mathbf{S}}'} \;=\; \overline{\mathbf{CG}} \;=\; \overline{\mathbf{G}}\,\rho^{\mathbf{C}} \;=\; \overline{\mathbf{G}}\,\rho.$$

13.2 Entropies and Information-Theoretical Key Agreement

a) Each of the random variables X, Y, and Z is distributed uniformly over the 2-bit strings, and hence $H(X) = H(Y) = H(Z) = 2$. Also, any two of the random variables uniquely

determine the remaining one, so $H(X|YZ) = H(Y|XZ) = H(Z|XY) = 0$. Furthermore, $H(XYZ) = H(A_1A_2A_3) = 3$ (since knowledge of $[X, Y, Z]$ is equivalent to knowledge of $[A_1.A_2, A_3]$) and $H(YZ) = H(XZ) = H(XY) = 3$. We further have $I(X;Y|Z) = H(XZ)+H(YZ)-H(XYZ)-H(Z) = 1$ and similarly $I(X;Z|Y) = 1$ and $I(Y;Z|X) = 1$. The resulting entropy diagram is given below.



b) We show that deleting a value X' after having computed U by A does not increase the conditional mutual information:

$$\begin{aligned} I(U;Y'|Z') &= H(UZ') + H(Y'Z') - H(UY'Z') - H(Z') \\ &\leq H(UZ') + H(Y'Z') - H(UY'Z') - H(Z') \\ &\quad + \underbrace{I(X';Y'|UZ')}_{H(X'UZ')+H(Y'UZ')-H(X'Y'UZ')-H(UZ')} \\ &= H(Y'Z') - H(Z') + H(X'UZ') - H(X'Y'UZ') \\ &= I(X'U;Y'|Z'). \end{aligned}$$

c) Using Corollary 7.4 from the lecture notes, we have that if Eve is required to have no information about the key, then

$$H(K) \leq \min(I(X;Y), I(X;Y|Z)),$$

where K is the key shared between Alice and Bob.
The mutual information is computed as

$$I(X;Y) = H(X) + H(Y) - H(XY) = 6 + 3 - 6 = 3$$

and

$$I(X;Y|Z) = H(XZ) + H(YZ) - H(XYZ) - H(Z) = 6 + 5 - 6 - 3 = 2.$$

Hence, $H(K) \leq 2$, which implies that the shared key is of length at most 2.
Alice and Bob simply take the bits B_4 and $B_5 \oplus B_6$. As all bits $B_1, \ldots, B_6$ are independent, Eve has no information about $B_5 \oplus B_6$ since she does not know B_5, and she has no information about B_4 as she only knows $B_2 \oplus B_4$ but neither B_2 nor B_4.

13.3 Privacy Amplification

Recall Jensen's inequality: for $\lambda_i \geq 0$ with $\sum_{i=1}^n \lambda_i = 1$ and $x_i \geq 0$ we have that

$$f\left(\sum_{i=1}^n \lambda_i x_i\right) \leq \sum_{i=1}^n \lambda_i f(x_i) \qquad \text{for convex } f\colon \mathbb{R}_{\geq 0} \to \mathbb{R} \tag{1}$$

$$f\left(\sum_{i=1}^n \lambda_i x_i\right) \geq \sum_{i=1}^n \lambda_i f(x_i) \qquad \text{for concave } f\colon \mathbb{R}_{\geq 0} \to \mathbb{R}. \tag{2}$$

a) We first prove the lower bound on $p_{\text{coll}}(X)$:

$$\begin{aligned} p_{\text{coll}}(X) &= \sum_{x\in\mathcal{X}} (\mathsf{P}_X(x))^2 = |\mathcal{X}| \sum_{x\in\mathcal{X}} \frac{1}{|\mathcal{X}|} (\mathsf{P}_X(x))^2 \\ &\overset{(1)}{\geq} |\mathcal{X}| \left(\sum_{x\in\mathcal{X}} \frac{1}{|\mathcal{X}|} \mathsf{P}_X(x)\right)^2 = |\mathcal{X}| \left(\frac{1}{|\mathcal{X}|} \sum_{x\in\mathcal{X}} \mathsf{P}_X(x)\right)^2 = \frac{1}{|\mathcal{X}|}, \end{aligned}$$

where in the third step we used Jensen's inequality for $f(x) = x^2$, which is convex on $\mathbb{R}_{\geq 0}$.

Using the fact that the maximum is greater than or equal to every element, we obtain the upper bound

$$\begin{aligned} p_{\text{coll}}(X) &= \sum_{x\in\mathcal{X}} (\mathsf{P}_X(x))^2 \\ &\leq \sum_{x\in\mathcal{X}} \left(\mathsf{P}_X(x) \cdot \max_{x'\in\mathcal{X}} (\mathsf{P}_X(x'))\right) \\ &= \max_{x'\in\mathcal{X}} (\mathsf{P}_X(x')) \cdot \underbrace{\sum_{x\in\mathcal{X}} \mathsf{P}_X(x)}_{=1} = p_{\max}(X). \end{aligned}$$

b) We have

$$\begin{aligned} (2 \cdot d(X))^2 &= \left(\sum_{x\in\mathcal{X}} \left|\mathsf{P}_X(x) - \tfrac{1}{|\mathcal{X}|}\right|\right)^2 \\ &= \left(\sum_{x\in\mathcal{X}} \tfrac{1}{|\mathcal{X}|} \left|\mathsf{P}_X(x)|\mathcal{X}| - 1\right|\right)^2 \\ &\overset{(1)}{\leq} \sum_{x\in\mathcal{X}} \left(\tfrac{1}{|\mathcal{X}|} \left|\mathsf{P}_X(x)|\mathcal{X}| - 1\right|^2\right) \\ &= \sum_{x\in\mathcal{X}} \left((\mathsf{P}_X(x))^2 |\mathcal{X}| - 2\mathsf{P}_X(x) + \tfrac{1}{|\mathcal{X}|}\right) \\ &= |\mathcal{X}| \underbrace{\sum_{x\in\mathcal{X}} (\mathsf{P}_X(x))^2}_{=p_{\text{coll}}(X)} - 2 \underbrace{\sum_{x\in\mathcal{X}} \mathsf{P}_X(x)}_{=1} + \underbrace{\sum_{x\in\mathcal{X}} \tfrac{1}{|\mathcal{X}|}}_{=1} \\ &= |\mathcal{X}| \cdot p_{\text{coll}}(X) - 1. \end{aligned}$$

Since $d(X)$, $(2 \cdot d(X))^2$, and $(|\mathcal{X}| \cdot p_{\text{coll}}(X) - 1)$ are non-negative quantities (the last one due to Lemma 7.6), taking the square root and dividing by two implies the desired result.

c) We first describe the protocol and the simulator involved in the construction. Let π_1 be the converter that, on input $x \in \{0,1\}^n$ at the inside interface (from the key with leakage):

1. chooses $g \in \mathcal{G}$ uniformly at random
2. computes $y = g(x)$
3. outputs g at the inside interface corresponding to $\bullet\!\!\longrightarrow$
4. outputs y at the outside interface.

Moreover, let π_2 denote the converter that upon having received both x and g at the inside interface, outputs $y = g(x)$ at the outside interface.

The simulator σ_f works as follows:

1. Chooses $g \in \mathcal{G}$ and $x \in \{0,1\}^n$ uniformly at random.
2. Outputs $f(x)$ (as the output of $\bullet\!\!\overset{\{0,1\}^n,\, f}{=\!=}\!\!\bullet$) and g (as the output of $\bullet\!\!\longrightarrow$) at the outside interface.

In the following let $f \in \{0,1\}^n \to \{0,1\}^m$, $\mathbf{R} := \pi_1^A \pi_2^B \left[\bullet\!\!\overset{\{0,1\}^n,\, f}{=\!=}\!\!\bullet,\ \bullet\!\!\longrightarrow \right]$ and $\mathbf{S} := \sigma_f^E \bullet\!\!\overset{\{0,1\}^r}{=\!=}\!\!\bullet$.

Observe that those systems do not take any inputs and, thus, are characterized only by the output distribution. Moreover, observe that $\mathbf{R}$ outputs the same key $y = g(x)$ at both interfaces A and B, and outputs g and $f(x)$ at interface E. Hence, the system $\mathbf{R}$ is uniquely determined by the triple $(G, G(X), f(X))$ where X is distributed uniformly over $\{0,1\}^n$ and G is independent and distributed uniformly over $\mathcal{G}$. Similarly, the system $\mathbf{S}$ is described by the triple $(G, Y, f(X))$ where Y is distributed uniformly over $\{0,1\}^r$ (here X and G are chosen independently of Y by the simulator σ).

Using Lemma 2.1 we obtain

$$\overline{\langle \mathbf{R} \,|\, \mathbf{S} \rangle} \leq \delta\Big(\big(G, G(X), f(X)\big),\ \big(G, Y, f(X)\big) \Big).$$

We now upper-bound this statistical distance by ϵ_s. In the following, let $f^{-1}(\{z\}) = \{x \mid f(x) = z\}$ denote the preimage z under f and, for every z, let X_z denote a random variable with the uniform distribution over $f^{-1}(\{z\})$.

$$\begin{aligned}
&\delta\Big(\big(G,G(X), f(X)\big),\ \big(G, Y, f(X)\big) \Big) \\
&\quad = \frac{1}{2} \sum_{g \in \mathcal{G}} \sum_{y \in \{0,1\}^r} \sum_{z \in \{0,1\}^m} \big| \mathsf{P}_{G,G(X),f(X)}(g,y,z) - \mathsf{P}_{G,Y,f(X)}(g,y,z) \big| \\
&\quad = \frac{1}{2} \sum_{g \in \mathcal{G}} \sum_{y \in \{0,1\}^r} \sum_{\substack{z \in \{0,1\}^m \\ \mathsf{P}_{f(X)}(z) \neq 0}} \mathsf{P}_{f(X)}(z) \cdot \big| \underbrace{\mathsf{P}_{G,G(X)|f(X)}(g,y,z)}_{=\mathsf{P}_{G,G(X_z)}(g,y)} - \underbrace{\mathsf{P}_{G,Y|f(X)}(g,y,z)}_{=\mathsf{P}_{G,Y}(g,y)} \big| \\
&\quad = \sum_{z \in \{0,1\}^m} \Bigg(\mathsf{P}_{f(X)}(z) \cdot \underbrace{\tfrac{1}{2} \sum_{g \in \mathcal{G}} \sum_{y \in \{0,1\}^r} \big| \mathsf{P}_{G,G(X_z)}(g,y) - \mathsf{P}_{G,Y}(g,y) \big|}_{=d((G,G(X_z)))} \Bigg) \\
&\quad = \sum_{z \in \{0,1\}^m} \mathsf{P}_{f(X)}(z) \cdot d((G, G(X_z))) \\
&\quad = \sum_{z \in \{0,1\}^m} \frac{|f^{-1}(\{z\})|}{2^n} \cdot d((G, G(X_z))),
\end{aligned}$$

where in the third step we used for the first term that the probability distribution of X given $f(X) = z$ is the uniform distribution over $f^{-1}(\{z\})$, and in the last step we used that $f(X) = z$ iff $X \in f^{-1}(\{z\})$ and that X is uniformly distributed.

We now apply Theorem 7.9 to bound this term.

$$d((G, G(X_z))) \leq \frac{1}{2} \sqrt{2^r \cdot p_{\mathrm{coll}}(X_z)} = \frac{1}{2} \sqrt{2^r} \cdot \sqrt{\frac{1}{|f^{-1}(\{z\})|}}$$

where we used that the collision probability $p_{\text{coll}}(W)$ is $1/|\mathcal{W}|$ for a uniformly distributed random variable W over $\mathcal{W}$. Therefore,

$$\begin{aligned}
\delta\Big(\big(G, G(X), f(X)\big),\ \big(G, Y, f(X)\big)\Big) &\leq \sum_{z\in\{0,1\}^m} \frac{|f^{-1}(\{z\})|}{2^n} \cdot \frac{1}{2}\sqrt{2^r} \cdot \sqrt{\frac{1}{|f^{-1}(\{z\})|}} \\
&= \frac{1}{2} \cdot \frac{\sqrt{2^r}}{2^n} \cdot 2^m \sum_{z\in\{0,1\}^m} \frac{1}{2^m} \sqrt{|f^{-1}(\{z\})|} \\
&\overset{(2)}{\leq} \frac{1}{2} \cdot \frac{\sqrt{2^r}}{2^n} \cdot 2^m \sqrt{\sum_{z\in\{0,1\}^m} \frac{1}{2^m} |f^{-1}(\{z\})|} \\
&= \frac{1}{2} \cdot \frac{\sqrt{2^r}}{2^n} \cdot 2^m \sqrt{\frac{1}{2^m} \sum_{z\in\{0,1\}^m} |f^{-1}(\{z\})|},
\end{aligned}$$

where in the last step we used Jensen's inequality with $x \mapsto \sqrt{x}$, which is concave on $\mathbb{R}_{\geq 0}$. Using

$$\sum_{z\in\{0,1\}^m} \big|f^{-1}(\{z\})\big| = 2^n$$

we finally obtain

$$\delta\Big(\big(G, G(X), f(X)\big),\ \big(G, Y, f(X)\big)\Big) \leq \frac{1}{2} \cdot \frac{\sqrt{2^r}}{2^n} \cdot 2^m \sqrt{\frac{1}{2^m} 2^n} = \frac{1}{2}\sqrt{2^{r+m-n}}.$$

and hence $\overline{\langle \mathbf{R} \,|\, \mathbf{S} \rangle} \leq \frac{1}{2}\sqrt{2^{r+m-n}}$.