Solution Sheet #4

Advanced Cryptography 2022

Solution 1 PRF Programming

This exercise is inspired from Boureanu-Mitrokotsa-Vaudenay, *On the Pseudorandom Function Assumption in (Secure) Distance-Bounding Protocols - PRF-ness alone Does Not Stop the Frauds!*, in LATINCRYPT 2012, LNCS vol. 7533, Springer.

1. This is a direct consequence of the definition of the PRF, for f.

2. We run Γ^g and Γ^f with the same coins for K and $\mathcal{A}$. By induction, $\mathcal{A}$ produce identical queries in both games and g and f produce identical answers. So, $\Pr[\Gamma^g \to 1 | \neg F(\Gamma^g)] = \Pr[\Gamma^f \to 1 | \neg F(\Gamma^f)]$ as same coins produce identical outcomes. Similarly, $\Pr[\neg F(\Gamma^g)] = \Pr[\neg F(\Gamma^f)]$.

3. We have

$$\Pr[\Gamma^g \to 1] = \Pr[\neg F(\Gamma^g)] \Pr[\Gamma^g \to 1 | \neg F(\Gamma^g)] + \Pr[\Gamma^g \to 1 \wedge F(\Gamma^g)]$$

and the same with f. So, by difference, due to the previous question, we have

$$\begin{aligned} |\Pr[\Gamma^g \to 1] - \Pr[\Gamma^f \to 1]| &\leq \max(\Pr[\Gamma^g \to 1 \wedge F(\Gamma^g)], \Pr[\Gamma^f \to 1 \wedge F(\Gamma^f)]) \\ &\leq \max(\Pr[F(\Gamma^g)], \Pr[F(\Gamma^f)]) \\ &\leq \Pr[F(\Gamma^f)] \end{aligned}$$

4. To any case where $F(\Gamma^f)$ occurs, we can define the index i of the first query equal to K and have $\Gamma_i^f \to 1$ with the same coins. So,

$$\Pr[F(\Gamma^f)] \leq \Pr\left[\bigvee_{i=1}^{P(s)} \Gamma_i^f \to 1\right] \leq \sum_{i=1}^{P(s)} \Pr[\Gamma_i^f \to 1]$$

5. We define a new adversary $\mathcal{A}'_i$ who simulates $k = \mathcal{A}_i$, then picks $x \in \{0,1\}^s$, then queries the oracle with x, then outputs 1 if and only if the response equals $f_k(x)$. We apply the PRF assumption on $\mathcal{A}'_i$ and obtain $\Pr[\Gamma_i^* \to 1] = \mathsf{negl}(s)$.

6. If x is a fresh query at the end of the Γ_i^* game, $f^*(x)$ is uniformly distributed and independent from $f_k(x)$. So, $f_k(x) = f^*(x)$ with probability 2^{-s} in that case. Now, since x is picked at random, the probability that it is not fresh is bounded by $P(s) \times 2^{-s}$. Overall, we obtain that $\Pr[\Gamma_i^* \to 1] \leq (P(s)+1)2^{-s}$ which is negligible.

7. We have

$$
\begin{aligned}
& |\Pr[\Gamma^g \to 1] - \Pr[\Gamma^* \to 1]| \\
\leq\ & |\Pr[\Gamma^g \to 1] - \Pr[\Gamma^f \to 1]| + |\Pr[\Gamma^f \to 1] - \Pr[\Gamma^* \to 1]| \\
\leq\ & |\Pr[\Gamma^g \to 1] - \Pr[\Gamma^f \to 1]| + \mathsf{negl}(s) && \text{(Q. 1)} \\
\leq\ & \Pr[F(\Gamma^f)] + \mathsf{negl}(s) && \text{(Q. 3)} \\
\leq\ & \textstyle\sum_{i=1}^{P(s)} \Pr[\Gamma_i^f \to 1] + \mathsf{negl}(s) && \text{(Q. 4)} \\
\leq\ & \textstyle\sum_{i=1}^{P(s)} (\Pr[\Gamma_i^* \to 1] + \mathsf{negl}(s)) && \text{(Q. 5)} \\
\leq\ & \textstyle\sum_{i=1}^{P(s)} \mathsf{negl}(s) && \text{(Q. 6)} \\
\leq\ & \mathsf{negl}(s)
\end{aligned}
$$

So, g is a PRF as well.

Solution 2 A Weird Signcryption (Midterm 2019)

See Exercise 3 in `https://lasec.epfl.ch/courses/exams_archives/AdvCrypto/ac19_midterm_sol.pdf`.
Note that the condition in line 3 and 1 of resp. SC.Receive and SC.Verify, should be $\mathsf{DS.Ver}(\mathsf{vk}_A, \mathsf{ct}, \sigma) ==$ **False**.