Cryptography Foundations

Exercise 12

12.1 Construction of an Authenticated Channel Using MACs

Goal: We prove that a secure MAC constructs an authenticated channel from an insecure one and a shared secret key.

a) Recall the $G^{\text{mac}}_t$ game from Definition 3.7 used to define a secure MAC (we instantiate here such system as a PDG and do not make the MOC $A$ explicit). Now let $G^{\text{mac-v}}_t$ be the same game, but where the winner $W$ has additionally access to the verification oracle for $t$ message-tag pairs $(m,a)$, for which it obtains a binary value indicating whether $a = f(m,k)$. $W$ wins ($A = 1$) as soon as such a pair represents a forgery which is new ($m$ was not queried before to the tagging oracle) and valid ($a = f(m,k)$). In particular, $W$ does not output a forgery upon termination. Show that any secure MAC is also secure with verification queries by providing a black-box reduction system $C$ and showing that

$$G^{\text{mac-v}}_t \leq t \cdot G^{\text{mac}}_t \gamma^C.$$ 

b) Informally argue the claim outlined in Section 3.4.5 of the lecture notes that a protocol $(\text{tag}, \text{vrf})$ using a secure MAC $f$ suffices to construct an authenticated channel $\text{AUT}$ for $t$ messages from an insecure channel $\text{INS}$ for $t$ messages and a shared secret key $\text{KEY}$, that is, define an adequate MOC such that

$$\langle \text{tag}^A \text{vrf}^B | \text{KEY}, \text{INS} \rangle | \text{sim}^E \text{AUT} \rangle \leq G^{\text{mac-v}}_t \gamma^C,$$

for an adequate simulator $\text{sim}$ and black-box reduction system $C'$.

12.2 Distinguishing URFs and URPs

Goal: In this exercise, we complete the proof of Lemma 6.7.

a) Prove the statement from Example 6.10, i.e., for the uniform random function $R_{n,n}$ and the uniform random permutation $P_n$, formalize a MOC $A$ such that $R_{n,n}^A \equiv P_n$ and prove the conditional equivalence.

b) Prove Lemma 6.6. In more detail, let $X_1, \ldots, X_q$ be uniformly-distributed independent random variables on some set $\mathcal{X}$ with $|\mathcal{X}| = t$. Denote by $p_{\text{coll}}(q,t)$ the probability that there exists a collision, i.e., there exist indices $i, j$ with $1 \leq i < j \leq q$ and $X_i = X_j$. Show that

$$p_{\text{coll}}(q,t) \leq \frac{1}{2} q^2 / t.$$

Hint: What is the probability (for some $i \neq j$) that $X_i = X_j$? How many such pairs $i \neq j$ are there?

---

1Technically, the insecure channel $\text{INS}$ is defined analogously to the authenticated channel $\text{AUT}$ from Exercise 2.2 b), but with an internal buffer of size $2t$ and the added capability of inputting messages at interface $E$, but only such that they were not previously input at interface $A$. 

---
12.3 Composability of Constructions

Goal: We prove Lemma 7.1 from the lecture notes.

Show that the construction notion from Definition 7.2 is composable, that is, for two constructions $\gamma : \Phi \rightarrow \Phi$, and specifications $\mathcal{R}, \mathcal{S},$ and $\mathcal{T}$, prove that

$$\mathcal{R} \xrightarrow{\gamma} \mathcal{S} \land \mathcal{S} \xrightarrow{\gamma'} \mathcal{T} \implies \mathcal{R} \xrightarrow{\gamma' \circ \gamma} \mathcal{T}.$$ 

12.4 Expansion of PRGs

Goal: We analyze a construction to expand pseudo-randomness using Constructive Cryptography.

Let $g : \{0, 1\}^k \rightarrow \{0, 1\}^{2k}$ be a function (think of a PRG). We want to use this function to generate $4^k$ (pseudo-random) bits from a $k$-bit seed and formulate it as a construction. Let $G$ be the resource that on the first input $s \in \{0, 1\}^k$ returns $g(s)$ (and ignores subsequent inputs). Let further denote $U_n$ the resource that upon the first invocation outputs a uniformly distributed random $n$-bitstring. Finally, let $\alpha[U_k, G]$ be the resource that on the first activation outputs $g(s)$ for a uniformly random $k$-bitstring $s$ (implemented by a converter $\alpha$ that routes the output of $U_k$ as input to $G$).

a) Describe the specification that we aim to construct (using Section 7.3.4 from the lecture notes) as a generic relaxation of $\{U_{4^k}\}$ that contains all systems $\mathcal{S}$ such that the distinction problem $\langle \alpha[U_k, G] | U_{2^k} \rangle$ reduces to the distinction problem $\langle U_{4^k} | \mathcal{S} \rangle$ (for some reduction $\rho$ with performance-translation $\lambda$).

b) Describe the assumed specification $\mathcal{R}$ based on the above resources. Then give a converter $\beta$ and show which specification $\mathcal{S}$ (of the type defined in a)) is constructed (cf. Definition 7.2 of the lecture notes) by providing the concrete reduction and performance-translation functions.

Hint: Think of the following construction: compute $s_1|s_2 := g(s)$ ($s_1, s_2 \in \{0, 1\}^k$) and output $g(s_1)|g(s_2)$. Note that $\mathcal{R}$ can also be a singleton set.