Cryptography Exercise Sheet 6

Prof. Dr. Thomas Wilke, Dr.-Ing. Kim-Manuel Klein

15. Mai 2020

1. **Problem:** *The 802.11b insecure Mac (Exercise 6.1 in BS)*

   Consider the following MAC (a variant of this was used for WiFi encryption in 802.11b WEP). Let F be a PRF defined over $(\mathcal{K}, \mathcal{R}, \mathcal{X})$ where $\mathcal{X} := \{0,1\}^{32}$. Let CRC32 be a simple and popular error-detecting code meant to detect random errors; CRC32 is a function that takes as input $m \in \{0,1\}^{\leq \ell}$ and outputs a 32-bit string. Define the following MAC system *(S, V)*:

   $$S(k,m) := \left\{ \; r \xleftarrow{\text{R}} \mathcal{R},\; t \leftarrow F(k,r) \oplus \text{CRC32}(m),\; \text{output(r,t)} \; \right\}$$
   $$V(k,m,(r,t)) := \left\{ \; \textbf{accept} \text{ if } t = F(k,r) \oplus \text{CRC32}(m) \text{ and } \textbf{reject} \text{ otherwise} \; \right\}$$

   Show that this MAC system is insecure.

2. **Problem:** *MAC combiners (Exercise 6.5 in BS)*

   We want to build a MAC system $\mathcal{I}$ using two MAC systems $\mathcal{I}_1 = (S_1, V_1)$ and $\mathcal{I}_2 = (S_2, V_2)$, so that if at some time one of $\mathcal{I}_1$ or $\mathcal{I}_2$ is broken (but not both) then $\mathcal{I}$ is still secure. Put another way, we want to construct $\mathcal{I}$ from $\mathcal{I}_1$ and $\mathcal{I}_2$ such that $\mathcal{I}$ is secure if either $\mathcal{I}_2$ or $\mathcal{I}_2$ is secure.

   (a) Define $\mathcal{I} = (S, V)$, where

   $$S((k_1,k_2),m) := ((S_1(k_1,m), S_2(k_2,m)),$$

   and V is defined in the obvious way: on input $(k, m, (t_1, t_2))$, V accepts iff both $V_1(k_1, m, t_1)$ and $V_2(k_2, m, t_2)$ accept. Show that $\mathcal{I}$ is secure if either $\mathcal{I}_1$ or $\mathcal{I}_2$ is secure.

   (b) Suppose that $\mathcal{I}_1$ and $\mathcal{I}_2$ are deterministic MAC systems (see the definition on page 214), and that both have tag space $\{0,1\}^n$. Define the deterministic MAC system $\mathcal{I} = (S, V)$, where

   $$S((k_1,k_2),m) := S1(k_1,m) \oplus S_2(k_2,m).$$

   Show that $\mathcal{I}$ is secure if either $\mathcal{I}_1$ or $\mathcal{I}_2$ is secure.