Cryptography Exercise Sheet 2

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

8. Mai 2020

1. **Problem:** *A broken one-time pad*

   Consider a variant of the one time pad with message space $\{0,1\}^L$ where the key space $\mathcal{K}$ is restricted to all L-bit strings with an even number of 1s. Give an efficient adversary whose semantic security advantage is 1.

2. **Problem:** *Exercising the definition of semantic security*

   Let $\mathcal{E} = (E, D)$ be a semantically secure cipher defined over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$, where $\mathcal{M} = \mathcal{C} = \{0,1\}^L$. Which of the following encryption algorithms yields a semantically secure scheme? Either give an attack or provide a security proof via an explicit reduction.

   (a) $E_1(k, m) := 0 \parallel E(k, m)$
   (b) $E_2(k, m) := E(k, m) \parallel parity(m)$
   (c) $E_3(k, m) := reverse(E(k, m))$
   (d) $E_4(k, m) := E(k, reverse(m))$

   Here, for a bit string s, parity(s) is 1 if the number of 1s in s is odd, and 0 otherwise; also, reverse(s) is the string obtained by reversing the order of the bits in s, e.g., reverse(1011) = 1101.

3. **Problem:** *Key recovery attacks*

   Let $\mathcal{E} = (E, D)$ be a cipher defined over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$. A key recovery attack is modeled by the following game between a challenger and an adversary $\mathcal{A}$: the challenger chooses a random key k in $\mathcal{K}$, a random message m in $\mathcal{M}$, computes $c \xleftarrow{R} E(k, m)$, and sends (m, c) to $\mathcal{A}$. In response $\mathcal{A}$ outputs a guess $\hat{k}$ in $\mathcal{K}$. We say that $\mathcal{A}$ wins the game if $D(\hat{k}, c) = m$ and define $KRadv[\mathcal{A}, \mathcal{E}]$ to be the probability that $\mathcal{A}$ wins the game. As usual, we say that $\mathcal{E}$ is secure against key recovery attacks if for all efficient adversaries $\mathcal{A}$ the advantage $KRadv[\mathcal{A}, \mathcal{E}]$ is negligible.

   (a) Show that the one-time pad is not secure against key recovery attacks.
   (b) Show that if $\mathcal{E}$ is semantically secure and $e = |\mathcal{K}|/|\mathcal{M}|$ is negligible, then $\mathcal{E}$ is secure against key recovery attacks. In particular, show that for every efficient key-recovery adversary $\mathcal{A}$ there is an efficient semantic security adversary $\mathcal{B}$, where $\mathcal{B}$ is an elementary wrapper around $\mathcal{A}$, such that

   $$KRadv[\mathcal{A}, \mathcal{E}] \leq SSadv[\mathcal{B}, \mathcal{E}] + e \tag{1}$$

   Hint: Your semantic security adversary $\mathcal{B}$ will output 1 with probability $KRadv[\mathcal{A}, \mathcal{E}]$ in the semantic security Experiment 0 and output 1 with probability at most e in Experiment 1. Deduce from this a lower bound on $SSadv[\mathcal{B}, \mathcal{E}]$ in terms of e and $KRadv[\mathcal{A}, \mathcal{E}]$ from which the result follows.

4. Deduce from part (b) that if $\mathcal{E}$ is semantically secure and $|\mathcal{M}|$ is super-poly then $|\mathcal{K}|$ cannot be poly-bounded.

   Note: $|\mathcal{K}|$ can be poly-bounded when $|\mathcal{M}|$ is poly-bounded, as in the one-time pad.