Solutions to Shannon Ciphers and Perfect Security

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

11. April 2020

1. **Problem:** *Multiplicative one-time pad*

   Correctness: $D(k, E(k,m)) = D(k, k \cdot m \mod p) = k^{-1(p)} \cdot (k \cdot m \mod p) \mod p = k^{-1(p)} \cdot k \cdot m \mod p = m$

   Perfect security: $\Pr[E(k, m_0) = c] = \Pr[k \cdot m_0 = c] = \frac{1}{p-1} = \Pr[k \cdot m_1 = c] = \Pr[E(k, m_1) = c]$.

   For every fixed $m \in \mathcal{M}$, consider the function $e(k) = E(k, m)$. The fundamental principle of the one-time pad is that we have for each cipher text $c \in \mathcal{C}$ a key $k \in \mathcal{K}$ such that $e(k) = c$ and vice versa. Hence e is a bijection. This is also the case for the above multiplicative one-time pad as k can be chosen by $k = c \cdot m^{-1(p)}$ for every $c \in \mathcal{C}$ and hence

   $$e(k) \equiv km \equiv c \cdot m^{-1(p)} m \equiv c \mod p$$

2. **Problem:** *A good substitution cipher*

   Let $m_0, m_1 \in \mathcal{M}$ and $c[0], \ldots, c[L-1] \in \mathcal{C}$

   $$\begin{aligned} &\Pr[E(k, m_0) = c[0], \ldots, c[L-1]] \\ &= \Pr[k[0](m_0[0]), \ldots, k[L-1](m_0[L-1]) = c[0], \ldots, c[L-1]] \\ &= \Pr[k[0](m_0[0]) = c[0]] \cdot \ldots \cdot, \Pr[k[L-1](m_0[L-1]) = c[L-1]] \end{aligned}$$

   The probability that a random permutation maps an element $x \in \Sigma$ to $c[i]$ is exactly $\frac{1}{|\Sigma|}$, i.e. $\Pr[k[i](m_0[i]) = c[i]] = \frac{1}{|\Sigma|} = \Pr[k[i](m_1[L-1]) = c[i]]$. Hence we obtain

   $$\begin{aligned} &\Pr[k[0](m_0[0]) = c[0]] \cdot \ldots \cdot \Pr[k[L-1](m_0[L-1]) = c[L-1]] \\ &= \Pr[k[0](m_1[0]) = c[0]] \cdots \Pr[k[L-1](m_1[L-1]) = c[L-1]] \\ &= \Pr[E(k, m_1) = c[0], \ldots, c[L-1]] \end{aligned}$$

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

   - Let $k \in \mathcal{K}$ be uniformly chosen, then $\Pr[E(0^L, k) = 0^{L-1}1] = 0$ as it is not possible to produce a string with an odd number of 1′s from 0^L. However, the probability for $m_1 = 0^{L-1}1$ is $\Pr[E(k, 0^{L-1}1) = 0^{L-1}1] = \frac{1}{2^{L-1}}$ as $0^{L-1}1 \oplus 0^L = 0^{L-1}1$, where 0^L is a key with an even number of 1's. Hence this variant of the one-time pad is not perfectly secure.
   - Consider the property $\Phi(c) = \begin{cases} 1 & \text{if } c \text{ contains an odd number of 1's} \\ 0 & \text{otherwise} \end{cases}$

     By the same argumentation as above, we obtain that $\Pr[\Phi(E(k, 0^L))] = 0$ while $\Pr[\Phi(E(k, 0^{L-1}1))] = 1$. Hence this variant of the one-time pad is not semantically secure.

- The probability distribution of $E(k, 0^L)$ is different to the probability distribution of $E(k, 0^{L-1}1)$ as for example, by the argumentation in the first part, $\Pr[E(0^L, k) = 0^{L-1}1] = 0$ while $\Pr[E(k, 0^{L-1}1) = 0^{L-1}1] = \frac{1}{2^{L-1}}$. Hence this variant of the one-time pad is not ciphertext independent.