Problem Set 1 Solutions

ECS 227 — Phil Rogaway — Winter 2009

An excellent solution turned in by a student

Problem 1

Is the following notion of privacy achievable by a stateless, probabilistic encryption scheme? Scheme $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ is perfectly private against an adversary that asks two queries if for all distributions on plaintexts $\mathcal{M}$ and all $m_1, m_2 \in \mathcal{M}$ and all $c_1, c_2 \in \mathcal{C}$,

$$\Pr[M_1 = m_1 \wedge M_2 = m_2 \mid C_1 = c_1 \wedge C_2 = c_2] = \Pr[M_1 = m_1 \wedge M_2 = m_2]$$

where M_1 and M_2 are sampled independently from $\mathcal{M}$ and C_1 and C_1 are obtained by encrypting them. (Assume that c_1, c_2 are restricted such that $Pr[C_1 = c_1 \wedge C_2 = c_2] > 0$].)

Solution. No. Suppose there exists a scheme satisfying the above definition. Let $c_1 = c_2$, $m_1 \neq m_2$, we have

$$\begin{aligned}
&\Pr[M_1 = m_1 \wedge M_2 = m_2 \mid C_1 = c_1 \wedge C_2 = c_2] = 0, \\
&\Pr[M_1 = m_1 \wedge M_2 = m_2] = \Pr[M_1 = m_1] \Pr[M_2 = m_2] \neq 0,
\end{aligned}$$

which is a contradiction to the fact that

$$\Pr[M_1 = m_1 \wedge M_2 = m_2 \mid C_1 = c_1 \wedge C_2 = c_2] = \Pr[M_1 = m_1 \wedge M_2 = m_2].$$

Problem 2

Secrecy from a random shuffle. *Alice shuffles a deck of cards and deals it out to herself and Bob so that each gets half of the 52 cards. Alice now wishes to send a secret message M to Bob by saying something aloud. Eavesdropper Eve is listening in: she hears everything Alice says (but Eve can't see the cards).*

Part A. *Suppose Alice's message M is a string of 48-bit. Describe how Alice can communicate M to Bob in such a way that Eve will have no information about what is M.*

Solution. The shuffle of the 52 cards provides us with a key space $\mathcal{K}$. We have the following three observations:

- $|\mathcal{K}| = C_{52}^{26}$, since we have C_{52}^{26} different combinations for the cards in Alice's hand.
- Bob also knows $\mathcal{K}$, since the cards are dealt out evenly to two persons.
- $\mathcal{K}$ has a uniform distribution, since the cards are randomly shuffled.

Let $\mathcal{M}$ denote the message space of 48-bit strings, and $\mathcal{C}$ denote the ciphertext space s.t. $|\mathcal{C}| = |\mathcal{K}|$. Since $|\mathcal{M}| = 2^{48} < C_{52}^{26} = |\mathcal{K}|$, we have $|M| < |\mathcal{C}| = |\mathcal{K}|$.

Consider the cryptosystem $(\mathcal{M}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$. Define the encryption algorithm as

$$\mathcal{E}_k(m) = (m + k) \mod C_{52}^{26},$$

for each $k \in \mathcal{K}, m \in \mathcal{M}$. Correspondingly, define the decryption algorithm as

$$\mathcal{D}_k(c) = (c - k) \mod 2^{48},$$

for each $k \in \mathcal{K}, c \in \mathcal{C}$.

Both $\mathcal{E}$ and $\mathcal{D}$ are deterministic.

This scheme achieves the perfect secrecy. This is true because for each $m \in \mathcal{M}, c \in \mathcal{C}$,

$$\Pr[\text{Alice says } c \mid M = m] = \Pr[k = (c - m) \mod C_{52}^{26}] = 1/C_{52}^{26}.$$

This implies that

$$\Pr[\text{Alice says } c \mid M = m_1] = \Pr[\text{Alice says } c \mid M = m_2],$$

for all $m_1, m_2 \in \mathcal{M}, c \in \mathcal{C}$.

Therefore, the event "Alice says c" is independent of the event "$M = m$". Hence the perfect secrecy.

Part B. *Now suppose Alice's message M is 49-bit. Prove that there exists no protocol that allows Alice to communicate M to Bob in such a way that Eve will have no information about M.*

Proof. Let $\mathcal{M}$ denote the message space of 49-bit strings. Unfortunately, we have $|\mathcal{M}| = 2^{49} > C_{52}^{26} = |\mathcal{K}|$. Suppose we have a protocol that achieves the perfect secrecy. Let $c \in \mathcal{C}$ s.t. $\Pr[\text{Alice says } c] \neq 0$. Define the set

$$D_c = \{m \in \mathcal{M} \mid \mathcal{D}_k(c) = m, k \in \mathcal{K}\}.$$

Since $\mathcal{D}$ is deterministic, we can only have one $m \in \mathcal{M}$ for each $k \in \mathcal{K}$. Hence $|D_c| \leq |K|$.

Therefore, $|D_c| < |M|$. It follows that there exists at least a $m^* \in \mathcal{M}$ s.t. $m^* \notin D_c$. Hence, we have

$$\Pr[M = m^* \mid \text{Alice says } c] = 0.$$

We also have

$$\Pr[M = m^*] \neq 0,$$

which implies that

$$\Pr[M = m^* \mid \text{Alice says } c] \neq \Pr[M = m^*].$$

This is a contradiction to the definition of the perfect secrecy.