University of Maryland
CMSC858K — Introduction to Cryptography
Professor Jonathan Katz

Problem Set 1 — Solutions

Thanks to Dov Gordon for helping with these solutions

1. Say the scheme is not perfectly secret. Then for some distribution $\mathcal{D}$ over the plaintext space $\mathcal{P}$, there exists a message $m \in \mathcal{P}$ with[1] $\Pr_{\mathcal{D}}[M = m] \neq 0$ and a ciphertext c with $\Pr_{\mathcal{D}}[C = c] \neq 0$ such that

$$\Pr_{\mathcal{D}}[M = m \mid C = c] \neq \Pr_{\mathcal{D}}[M = m]. \tag{1}$$

Assume $\Pr_{\mathcal{D}}[M = m \mid C = c] > \Pr_{\mathcal{D}}[M = m]$. (The proof can be modified in case the opposite holds. Alternately, it is possible to show that Equation (1) implies that there exists a $\tilde{c}$ with $\Pr_{\mathcal{D}}[C = \tilde{c}] \neq 0$ and $\Pr_{\mathcal{D}}[M = m \mid C = \tilde{c}] > \Pr_{\mathcal{D}}[M = m]$.) Using the definition of conditional probabilities, it is not hard to see that this implies $\Pr[C = c \mid M = m] > \Pr_{\mathcal{D}}[C = c]$. (Note that we have removed the subscript in the first case since this probability no longer depends on $\mathcal{D}$, but only on the choice of the key.)

Now,

$$\Pr[C = c \mid M = m] > \Pr_{\mathcal{D}}[C = c] = \textstyle\sum_{m \in \mathcal{P}} \Pr[C = c \mid M = m] \cdot \Pr_{\mathcal{D}}[M = m],$$

where the sum is taken over all m with $\Pr_{\mathcal{D}}[M = m] \neq 0$. It follows that there exists an $m' \in \mathcal{P}$ with

$$\Pr[C = c \mid M = m] > \Pr[C = c \mid M = m'].$$

Let m, m', c be as above, and consider the following adversary $\mathcal{A}$ in the indistinguishability experiment: $\mathcal{A}$ outputs the messages m, m'. It gets back a ciphertext C. If $\hat{c} = c$ it outputs $b' = 0$ and otherwise it outputs a random bit. What is the probability that $b' = b$? We have

$$\begin{aligned}
\Pr[b' = b] &= \frac{1}{2} \cdot \Pr[b' = 0 \mid b = 0] + \frac{1}{2} \cdot \Pr[b' = 1 \mid b = 1] \\
&= \frac{1}{2} \cdot \Big(\Pr[b' = 0 \mid b = 0 \wedge C = c] \cdot \Pr[C = c \mid b = 0] \\
&\quad + \Pr[b' = 0 \mid b = 0 \wedge C \neq c] \cdot \Pr[C \neq c \mid b = 0] \Big) \\
&\quad + \frac{1}{2} \cdot \Big(\Pr[b' = 1 \mid b = 1 \wedge C = c] \cdot \Pr[C = c \mid b = 1] \\
&\quad + \Pr[b' = 1 \mid b = 1 \wedge C \neq c] \cdot \Pr[C \neq c \mid b = 1] \Big) \\
&= \frac{1}{2} \cdot \left(\Pr[C = c \mid M = m] + \frac{1}{2} \cdot \Pr[C \neq c \mid M = m] \right) \\
&\quad + \frac{1}{2} \cdot \left(\frac{1}{2} \cdot \Pr[C \neq c \mid M = m'] \right),
\end{aligned}$$

[1] We use the notation $\Pr_{\mathcal{D}}[\cdot]$ to emphasize that the probability is taken over the distribution $\mathcal{D}$ on the plaintext space (in addition to random choice of key).

by definition of $\mathcal{A}$. Since $\Pr[C \neq c \mid M = m] = 1 - \Pr[C = c \mid M = m]$, we obtain

$$\Pr[b' = b] = \frac{1}{2} + \frac{1}{4} \cdot \Big(\Pr[C = c \mid M = m] - \Pr[C = c \mid M = m'] \Big) > \frac{1}{2} .$$

So the scheme is not perfectly indistinguishable.

2. Consider the following A: On input $x \in \{0,1\}^{2n}$, enumerate (in exponential time) the set $S = \{G(s) \mid s \in \{0,1\}^n\}$. Output 1 iff $x \in S$.

   Clearly, if $x = G(s)$ for some s then A outputs 1 with probability 1. On the other hand, if x is chosen uniformly at random then

$$\Pr[A(x) = 1] = \Pr[x \in S] = \frac{|S|}{2^{2n}} \leq \frac{2^n}{2^{2n}} = 2^{-n}.$$

   So, for n large enough, $|\Pr[A(G(s)) = 1] - \Pr[A(r) = 1]| = 1 - 2^{-n} > \frac{1}{2}$.

3. For any adversary A interacting with the given experiment, we have that

$$\begin{aligned}
\Pr[b' = b] &= \Pr[b' = 0 \mid b = 0] \cdot \Pr[b = 0] + \Pr[b' = 1 \mid b = 1] \cdot \Pr[b = 1] \\
&= \frac{1}{2} \cdot \Pr\left[A(G(s)) = 0\right] + \frac{1}{2} \cdot \Pr[A(r) = 1] \\
&= \frac{1}{2} \cdot \Big(1 - \Pr[A(G(s)) = 1]\Big) + \frac{1}{2} \cdot \Pr[A(r) = 1] \\
&= \frac{1}{2} + \frac{1}{2} \cdot \Big(\Pr[A(r) = 1] - \Pr[A(G(s)) = 1] \Big) .
\end{aligned}$$

   So $\left|\Pr[b' = b] - \frac{1}{2}\right| \leq \mathsf{negl}(n)$ iff $\Big| \Pr[A(r) = 1] - \Pr[A(G(s)) = 1] \Big| \leq \mathsf{negl}(n)$.