Vojtech Brtnik – vojtech@brtnik.eu

Problem 1

Assume that we require only that an encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ over a message space $\mathcal{M}$ satisfiees the following: for all $m \in \mathcal{M}$, the probability that $\mathsf{Dec}_k(\mathsf{Enc}_k(m)) = m$ is at least 2^{-t}. (This probability is taken over choice of $k \leftarrow \mathsf{Gen}$ as well as any randomness that may be used during encryption.)

(a) Show that perfect secrecy can be achieved with $|\mathcal{K}| < |\mathcal{M}|$ when $t \geq 1$.

Solution:

I am not absolutely sure, what is requested. That is why solution to this exercise is rather long.

First a simple example. Let $\mathcal{K} = \{0\}$, $\mathcal{M} = \mathcal{C} = \{0, 1\}$. Conditions are met, $|\mathcal{K}| = 1 < 2 = |\mathcal{M}|$. Now define

$$\begin{aligned}\mathsf{Pr}[\mathsf{Enc}(0) = 0] = \mathsf{Pr}[\mathsf{Enc}(0) = 1] &= \mathsf{Pr}[\mathsf{Enc}(1) = 0] = \mathsf{Pr}[\mathsf{Enc}(1) = 1] = \\ \mathsf{Pr}[\mathsf{Dec}(0) = 0] = \mathsf{Pr}[\mathsf{Dec}(0) = 1] &= \mathsf{Pr}[\mathsf{Dec}(1) = 0] = \mathsf{Pr}[\mathsf{Dec}(1) = 1] = 1/2.\end{aligned}$$

The Dec algorithm is probabilistic, we have

$$\mathsf{Pr}[\mathsf{Dec}_k(\mathsf{Enc}_k(m)) = m] = 1/2,$$

thus $t = 1$. Scheme is perfectly secret by Lemma 2.3.

$$\forall m_0, m_1 \in M, c \in C : \mathsf{Pr}[C = c | M = m_0] = \mathsf{Pr}[C = c | M = m_1] = 1/2.$$

To prove that lemma 2.3 holds in this case, we can exhaustively check all the possibilities.

The key space could be in this case even empty, since the algorithm is not dependant on the selected key at all.

Now we will present a scheme, which is also perfectly secure and where $|\mathcal{K}| = 2^{-t}|\mathcal{M}|$ and where the decryption is correct only with probability 2^{-t}. Here the encryption and decryption will depend on a key.

Let $\mathcal{M} = \{0, 1\}^n$ and $\mathcal{C} = \mathcal{K} = \{0, 1\}^{n-t}$. Futhermore, let $c = \mathsf{Enc}_k(m) = k \oplus \tilde{m}$, where $\tilde{m}$ is the substring of m with the last t bits cut off, i.e $\tilde{m} = m_1, \ldots, m_{n-t}$. The decryption algorithm decrypts c as $c \oplus k$ concatinated with a random string of length $n - t$.

Since the decryption algorithm picks a random bitstring of length t and only one of them leads to desired message m, it is clear that the decryption is correct[1] with probability 2^{-t}.

Futhermore we want to show, that this scheme is perfectly secret. The proof a copy of the proof 2.6 (perfect secrecy of one-time pad). Idea: for every possible m, c there exists a key k such that $c = \mathsf{Enc}_k(m)$; namely $\tilde{m} \oplus c$.

Fix some distribution over $\mathcal{M}$ and fix an arbitrary message $m \in \mathcal{M}$ and $c \in \mathcal{C}$.

$$\begin{aligned} \mathsf{Pr}[C = c | M = m] &= \mathsf{Pr}[\tilde{M} \oplus K = c | M = m] \\ &= \mathsf{Pr}[\tilde{m} \oplus K = c] \\ &= \mathsf{Pr}[K = \tilde{m} \oplus c] = 1/2^{n-t}. \end{aligned}$$

Since this holds for all distributions and all m, we have that for every probability distribution over $\mathcal{M}$, every m_0, $m_1 \in \mathcal{M}$ and every $c \in \mathcal{C}$, $\mathsf{Pr}[C = c|M = m_0] = 1/2^{n-t} = \mathsf{Pr}[C = c|M = m_1]$. By Lemma 2.3, this implies that the encryption scheme is perfectly secret.

□

(b) Prove a lower bound on the required size of $\mathcal{K}$.

Solution:

We claim that the bound presented in previous example is actually a lower bound. In other words, if $|\mathcal{K}| < 2^{-t}|\mathcal{M}|$ then encryption with the property that $\mathsf{Pr}[\mathsf{Dec}_k(\mathsf{Enc}_k(m)) = m] \geq 2^{-t}$ *cannot* be perfectly secure.

I did not figure out a proof.

Problem 2

Let negl_1 and negl_2 be negligible functions. Prove the following.

(a) The function negl_3 defined by $\mathsf{negl}_3(n) = \mathsf{negl}_1(n) + \mathsf{negl}_2(n)$ is negligible.

[1] in the sence that $\mathsf{Dec}(\mathsf{Enc}(m)) = m$

Solution:

Take an arbitrary polynomial $p(.)$; $2p(.)$ is also a polynomial and based on assumptions (def. 3.4 of negligible function), we know that:

$$(\exists N_1 \in \mathbb{N})(\forall n > N_1)\left(\mathsf{negl}_1(n) \leq \frac{1}{2p(n)}\right),$$
$$(\exists N_2 \in \mathbb{N})(\forall n > N_2)\left(\mathsf{negl}_2(n) \leq \frac{1}{2p(n)}\right).$$

Put $N_3 = \max\{N_1, N_2\}$. Then for all $n > N_3$ holds:

$$\mathsf{negl}_3(n) = \mathsf{negl}_1(n) + \mathsf{negl}_2(n) \leq \frac{1}{2p(n)} + \frac{1}{2p(n)} = \frac{1}{p(n)}.$$

We have shown that

$$(\forall p(.))(\forall n > N_3)(\mathsf{negl}_3(n) \leq 1/p(n))$$

and thus negl_3 is negligible function.

□

(b) For any (positive) polynomial p, the function negl_4 defined by $\mathsf{negl}_4(n) = p(n) \cdot \mathsf{negl}_1(n)$ is negligible.

Solution:

Take an arbitrary polynomial $q(.)$. Since $q(.) \cdot p(.)$ is also a polynomial[2] and negl_1 is negligible, we know that

$$(\exists n_0)(\forall n n_0)\left(\mathsf{negl}_1(n) \leq \frac{1}{q(n)p(n)}\right).$$

Hence for all $n > n_0$

$$\mathsf{negl}_4(n) = p(n) \cdot \mathsf{negl}_1 \leq \frac{p(n)}{q(n)p(n)} = \frac{1}{q(n)}.$$

We have shown that for arbitrary polynomial $q(n)$ exists $n \in \mathbb{N}$ such that for all $n > n_0$ is $\mathsf{negl}_4(n) \leq 1/q(n)$ and thus negl_4 is negligible.

□

[2]this does not need a proof I hope

Problem 3

Say $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is such that for $k \in \{0,1\}^n$, algorithm Enc_k is only defined for messages of length at most $\ell(n)$ (for some polynomial ℓ). Construct a scheme satisfying Definition 3.8 (indistinguishable ciphertexts) even when the adversary is not restricted to output equal-length messages in experiment $\mathsf{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi}$.

Solution:

Let $(\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$ is an encryption scheme, that'll be secure under Def. 3.8 even for unequal-length messages up to $\ell(n)$. Put Gen' equal to Gen. Let $k \in \{0,1\}^k$ be a key, $m \in \{0,1\}^p$ be a message, where $p \leq \ell(n)$. Now $\mathsf{Enc}'_k(m)$ first pads the message with single 1 and then pads 0 until the length reaches $\ell(n)+1$, i.e.

$$c := \mathsf{Enc}_k([m|10^{\ell(n)-|m|}]).$$

The Dec' algorithm first deciphers, then removes the zeros and the first 1 at the end of the message m' and output the new message m.

Adversary cannot tell the difference between padded messages m'_0 and m'_1 given c according to construction 3.15 (and see theorem 3.16). So neither can it tell the difference between original messages m_0 and m_1.

□

Problem 4

Let G be a pseudorandom generator where $|G(s)| > 2|s|$. Prove or disprove if the following are pseudorandom generators.

(a) $G_1(s) = G(s\|0^{|s|})$. (Here $\|$ denotes the "append" operation for strings.)

Solution:

Consider input $s \in \{0,1\}^n$. First, $\ell_{G_1}(n) = |G_1(s)| = |G(s\|0^{|s|})| > 2 \cdot 2n > n$. The expansion condition is satisfied.

G_1 is not a pseudorandom generator. Let $\hat{G}$ be any pseudorandom generator that has expansion factor $4n$. Define $G(s) = G(s_1 s_2) = \hat{G}(s_2)$, where $|s_1| = |s_2| = |s|/2$. First, we see that G is length

doubling, because $|\hat{G}(s_2)| = 4|s|/2 = 2|s|$. Next, we prove that G is a pseudorandom generator. Assume, by contradiction, that there exists a PPT distinguisher D and a non-negligible function e, that for infinitely many n's

$$|\mathsf{Pr}[D(G(U_n)) = 1] - \mathsf{Pr}[D(U_{2n}) = 1]| \geq e(n)$$

Then, we construct aa PPT distinguisher $\hat{D}$ for the generator $\hat{G}$. Upon input a string $r \in \{0,1\}^{2r}$, distinguisher $\hat{D}$ invokes D upon input r and outputs whatever D does. We have that

$$\mathsf{Pr}[\hat{D}(\hat{G}((U_{n/2})) = 1] = \mathsf{Pr}[D(G(U_n)) = 1]$$

and

$$\mathsf{Pr}[\hat{D}(U_{2n}) = 1] = \mathsf{Pr}[D(U_{2n}) = 1].$$

Therefore, for infinitely many n's we have that

$$\left|\mathsf{Pr}[\hat{D}(\hat{G}(U_{n/2})) = 1] - \mathsf{Pr}[\hat{D}(U_{2n}) = 1]\right| \geq e(n)$$

in contradiction to the pseudorandomness of $\hat{G}$. Having proven that G is pseudorandom, it remains to show that G_1 is not. However, for every s, $G_1(s) = G(s0^{|s|}) = \hat{G}(0^{|s|})$. Therefore G_1 can easily be distinguished from random (by computing $\hat{G}(0^{|s|})$ and comparing it to the input).

□

(b) $G_2(s) = G(s_1 \dots s_{n/2})$, where $s = (s_1, \dots, s_n)$ is the binary representation of s.

Solution: We could give here a proof, that follows the exact same proof as shown in the previous solution. However, I will try introduce more intuitive and easier approach.

Consider input $s \in \{0,1\}^n$. Since $\ell_{G_2}(n) = |G_2(s)| = |G(s_1 \dots s_{n/2})| > 2 \cdot n/2 > n$, the expansion condition is again satisfied.

The idea is simple, if a string is (pseudo)random, first half of it must be (pseudo)random as well.

If r, s is uniformly chosen at random from $\{0,1\}^k$, then first half of r, s is uniformly chosen at random from $\{0,1\}^{k/2}$. This is clear, since in multiset that consists of first halfs of all elements $\{0,1\}^k$, is each item exactly $\{0,1\}^{k/2}$ times. And thus the distribution is uniform.

Now we claim that G_2 is a PRG. To prove, asume, that it isn't. There exist "non-neligible distinguisher", i.e. PPT algorithm D satisfying

$$|\mathsf{Pr}[D(r) = 1] - \mathsf{Pr}[D(G_2(s)) = 1]| > \mathsf{negl}(n).$$

where r is uniformly chosen from $U_{ell_{G1}(n))}$ and s is uniformly chosen from U_n.
Take D and aply it to the first half of the string. It means that

$$|\mathsf{Pr}[D(r/2) = 1] - \mathsf{Pr}[D(G(s_1, \ldots, s_{n/2})) = 1]| > \mathsf{negl}(n).$$

This is contradiction with the assumption, since it would mean that G is also not PRG.

□