Solution to Final Exam
Foundations of Cryptography 89-856-01

Dr. Yehuda Lindell

2nd Semester, Moed א
29th June, 2005

Instructions:

1. The exam is open book. You are allowed to use any material that you wish.
2. Length of the exam: 3 hours.
3. Answer both questions.
4. Your answers should be as detailed and formal as possible. Of course, most points will be awarded for presenting a correct construction together with the main idea behind the proof that it is correct (I stress, the idea behind the *proof* and not just the intuition about why it is secure). However, you should aim to give full and detailed proofs.
5. You may rely on any theorem that was stated in class.
6. **Good luck!**

Question 1: Let f be a length-preserving one-way function (i.e. $|f(x)| = |x|$). For each of the following, state if g is necessarily a one-way function. If yes, prove it. If not, present a counter-example (i.e., a one-way function f with the property that g is not one-way). Note that the counter-example also requires a proof (i.e., that the function f being used is one-way, while g is not).

1. $g(x) = f(f(x))$
2. $g(x) = f(xx)$
3. $g(x) = f(x), f(f(x))$

Solution 1:

1. *The function g is not necessarily one-way:* Let h be a length-preserving one-way function and define $f(x)$ as follows: If $x_{n/2+1} \cdots x_n = 0^{n/2}$, then $f(x) = 0^{|x|}$. Else, $f(x) = h(x_1 \cdots x_{n/2})0^{n/2}$. Clearly, f is length preserving. We now show that it is one-way. Intuitively, any adversary inverting f can be used to invert h. Formally, assume that there exists a PPT adversary $\mathcal{A}$ and a polynomial p such that for infinitely many n's

$$\Pr[\mathcal{A}(f(U_n)) \in f^{-1}(f(U_n))] \geq \frac{1}{p(n)}$$

Then, let $\mathcal{A}'$ be an adversary who receives a value $y \in \{0,1\}^{n/2}$ and attempts to find a value $x \in h^{-1}(y)$. The adversary $\mathcal{A}'$ just invokes $\mathcal{A}$ upon input $y0^{n/2}$ and outputs the first $n/2$ bits of $\mathcal{A}$'s output. We now analyze the success probability of $\mathcal{A}'$. First, denote $S_n = \{x \mid x_{n/2+1} \cdots x_n = 0^{n/2}\}$ and note that $\Pr[U_n \in S_n] = 2^{-n/2}$. Next, note that

$$\Pr[\mathcal{A}'(h(U_{n/2})) \in h^{-1}(h(U_{n/2}))] = \Pr[\mathcal{A}(f(U_n)) \in f^{-1}(f(U_n)) \mid U_n \notin S_n]$$

Now,

$$\begin{aligned}
\Pr[\mathcal{A}(f(U_n)) \in f^{-1}(f(U_n))] &= \Pr[\mathcal{A}(f(U_n)) \in f^{-1}(f(U_n)) \mid U_n \in S_n] \cdot \Pr[U_n \in S_n] \\
&\quad + \Pr[\mathcal{A}(f(U_n)) \in f^{-1}(f(U_n)) \mid U_n \notin S_n] \cdot \Pr[U_n \notin S_n] \\
&\leq \Pr[U_n \in S_n] + \Pr[\mathcal{A}(f(U_n)) \in f^{-1}(f(U_n)) \mid U_n \notin S_n] \\
&= \Pr[U_n \in S_n] + \Pr[\mathcal{A}'(h(U_{n/2})) \in h^{-1}(h(U_{n/2}))] \\
&= \frac{1}{2^{n/2}} + \Pr[\mathcal{A}'(h(U_{n/2})) \in h^{-1}(h(U_{n/2}))]
\end{aligned}$$

We therefore have that

$$\begin{aligned}
\Pr[\mathcal{A}'(h(U_{n/2})) \in h^{-1}(h(U_{n/2}))] &\geq \Pr[\mathcal{A}(f(U_n)) \in f^{-1}(f(U_n))] - \frac{1}{2^{n/2}} \\
&\geq \frac{1}{p(n)} - \frac{1}{2^{n/2}} \geq \frac{1}{q(n)}
\end{aligned}$$

for some polynomial q. Since $\mathcal{A}'$ is PPT, this contradicts the assumption that h is a one-way function. We therefore conclude that f is one-way.

Having established that f is one-way, it remains to show that g is not one-way. In order to see this, note that for every x, $f(f(x)) = 0^{|x|}$ (this is because the last $n/2$ bits of $f(x)$ equal zero, and so $f(f(x))$ equals $0^{|x|}$). Noting that it is easy to find a preimage of $0^{|x|}$ under g (just take $0^{|x|}$), we have that $g(x) = f(f(x))$ is *not* one-way.

2. *The function g is not necessarily one-way:* Let h be any one-way function, and define f as follows. Let S_n be the set of n-bit strings of the form xx where $x \in \{0,1\}^{n/2}$. Then, define $f(xy) = h(xy)$ for $x \neq y$, and $f(xx) = xx$ otherwise. In order to show that f is one-way, we rely on the one-wayness of h. That is, assume that there exists a PPT adversary $\mathcal{A}$ and a polynomial p such that for infinitely many n's

$$\Pr[\mathcal{A}(f(U_n)) \in f^{-1}(f(U_n))] \geq \frac{1}{p(n)}$$

Then, let $\mathcal{A}'$ be an adversary who receives a value $y \in \{0,1\}^n$ and attempts to find a value $x \in h^{-1}(y)$. The adversary $\mathcal{A}'$ just invokes $\mathcal{A}$ upon input y and outputs whatever $\mathcal{A}$ outputs. We now analyze the success probability of $\mathcal{A}'$. First, note that S_n as defined above contains only $2^{n/2}$ different strings. Therefore, $\Pr[U_n \in S_n] = 2^{-n/2}$. Next, note that

$$\Pr[\mathcal{A}'(h(U_n)) \in h^{-1}(h(U_n)) \mid U_n \notin S_n] = \Pr[\mathcal{A}(f(U_n)) \in f^{-1}(f(U_n)) \mid U_n \notin S_n]$$

Using the same analysis as in the previous solution (and not really worth repeating), we have that

$$\Pr[\mathcal{A}(f(U_n)) \in f^{-1}(f(U_n))] \leq \frac{1}{2^{n/2}} + \Pr[\mathcal{A}'(h(U_n)) \in h^{-1}(h(U_n)) \mid U_n \notin S_n]$$

and so
$$\Pr[\mathcal{A}'(h(U_n)) \in h^{-1}(h(U_n)) \mid U_n \notin S_n] \geq \frac{1}{p(n)} - \frac{1}{2^{n/2}} \geq \frac{1}{q(n)}$$
for some polynomial q. We conclude by noting that

$$\begin{aligned}
\Pr[\mathcal{A}(h(U_n)) \in h^{-1}(h(U_n))] &= \Pr[\mathcal{A}(h(U_n)) \in h^{-1}(h(U_n)) \mid U_n \in S_n] \cdot \Pr[U_n \in S_n] \\
&\quad + \Pr[\mathcal{A}(h(U_n)) \in h^{-1}(h(U_n)) \mid U_n \notin S_n] \cdot \Pr[U_n \notin S_n] \\
&\geq \Pr[\mathcal{A}(h(U_n)) \in h^{-1}(h(U_n)) \mid U_n \notin S_n] \cdot \Pr[U_n \notin S_n] \\
&\geq \frac{1}{q(n)} \cdot \left(1 - \frac{1}{2^{n/2}}\right) \geq \frac{1}{2q(n)}
\end{aligned}$$

Since $\mathcal{A}'$ is PPT, this contradicts the assumption that h is a one-way function. We therefore conclude that f is one-way.

It remains to show that g is not one-way. However, this follows by the fact that for every x it holds that $g(x) = xx$, and so g is easily invertible.

3. *The function g is necessarily one-way:* Assume by contradiction that there exists a PPT adversary $\mathcal{A}$ and a polynomial p such that for infinitely many n's
$$\Pr[\mathcal{A}(g(U_n)) \in g^{-1}(g(U_n))] \geq \frac{1}{p(n)}$$
We construct a PPT $\mathcal{A}'$ who inverts f. Namely, $\mathcal{A}'$ receives for input $y = f(x)$ for $x \in_R \{0,1\}^n$, computes $z = f(y)$ and invokes $\mathcal{A}$ upon input (y, z). Adversary $\mathcal{A}'$ then outputs whatever $\mathcal{A}$ outputs. Clearly,
$$\Pr[\mathcal{A}'(f(U_n)) \in f^{-1}(f(U_n))] = \Pr[\mathcal{A}(g(U_n)) \in g^{-1}(g(U_n))]$$
Therefore, for infinitely many n's, adversary $\mathcal{A}'$ inverts f with probability at least $1/p(n)$. This contradicts the one-wayness of f.

Question 2: Let G be a pseudorandom generator with $l(n) = n + 1$, and let $p(n)$ be a polynomial. Show that the function $G'(s) = G^{p(|s|)}(s)$, where G is applied iteratively $p(|s|)$ times, is a pseudorandom generator with $l(n) = n + p(n)$. (Formally, define $G^0(s) = s$, and for every $i > 0$ define $G^i(s) = G(G^{i-1}(s))$.) Notice that G is applied to seeds of increasingly growing lengths.

Hint: In order to prove this, you may rely on a game in which a PPT distinguisher receives input 1^n and returns a value 1^ℓ where $\ell \geq n$. Then, D receives a string R which is either sampled according to $G(U_\ell)$ or according to $U_{\ell+1}$. For your proof, you can take it as a fact (that follows from the pseudorandomness of G) that for every PPT D, the probability that D outputs 1 when receiving $G(U_\ell)$ is negligibly close to the probability that it outputs 1 when receiving $U_{\ell+1}$. Note, that this just gives you flexibility to request the length of the string that you want to distinguish.

Solution 2: We prove the claim using a hybrid argument. Assume, by contradiction, that there exists a PPT distinguisher D and a polynomial q such that for infinitely many n's
$$\left|\Pr[D(G'(U_n)) = 1] - \Pr[D(U_{n+p(n)}) = 1]\right| \geq \frac{1}{q(n)}$$

We define the hybrid distribution $H_n^i = G^{p(n)-i}(U_{n+i})$. Observe that on the one hand $H_n^0 = G^{p(n)}(U_n) = G'(U_n)$, and on the other hand, $H_n^{p(n)} = G^0(U_{n+p(n)}) = U_{n+p(n)}$. Therefore, by the contradicting assumption, for infinitely many n's it holds that

$$\Delta(n) \stackrel{\text{def}}{=} \left|\Pr[D(H_n^0)=1] - \Pr[D(H_n^{p(n)})=1]\right| \geq \frac{1}{q(n)}$$

Now, using a telescopic sum and the triangle inequality, we have that

$$\Delta(n) \leq \sum_{i=0}^{p(n)-1} \left|\Pr[D(H_n^i)=1] - \Pr[D(H_n^{i+1})=1]\right|$$

Therefore, there exists a j for which

$$\left|\Pr[D(H_n^j)=1] - \Pr[D(H_n^{j+1})=1]\right| \geq \frac{1}{p(n)q(n)}$$

A distinguisher D' for G works as follows. Upon input 1^n, distinguisher D' chooses a random index $i \in_R \{0,\ldots,p(n)-1\}$, outputs 1^{n+i} and receives back a string $r \in \{0,1\}^{n+i+1}$ (as in the game defined in the hint above). Distinguisher D' then computes $R = G^{p(n)-i-1}(r)$, hands it to D, and outputs whatever D does. Notice the following:

- If D' receives U_{n+i+1}, then R is distributed according to H_n^{i+1}. In order to see this, recall that $H_n^{i+1} = G^{p(n)-i-1}(U_{n+i+1})$ which is exactly what D' computes.
- If D' receives $G(U_{n+i})$, then R is distributed according to H_n^i. In order to see this, note that $H_n^i = G^{p(n)-i}(U_{n+i}) = G^{p(n)-i-1}(G(U_{n+i}))$ which is exactly what D' computes.

Since $i = j$ with probability $1/p(n)$, we have that for infinitely many n's, D' distinguishes between the case that it receives U_{n+i+1} from the case that it receives $G(U_{n+i})$ with probability at least $1/p^2(n)q(n)$, in contradiction to the assumption regarding the pseudorandomness of G (and its ramification in the above game).