CS276: Cryptography

Lecture Notes 2/26/02

Umesh Shankar (ushankar@cs.berkeley.edu)

---

**Goal: Build a a pseudorandom permutation.**

**Definition (Pseudorandom Permutation).** Let $\pi \in_R$ {permutations on X}. Then $E : K \times X \to X$ is a $(t, q, e)$**-pseudorandom permutation (PRP)** if $\forall$ adversaries $A$ in time $\leq t$, making $q$ oracle queries, $\text{Adv}(A) \leq e$, where $\text{Adv}(A) = |\Pr_{k\in K}[A^{E_k, E_k^{-1}} = 1] - \Pr_\pi[A^{\pi,\pi^{-1}} = 1]|$.

In other words, no adversary with access to encryption and decryption oracles should be able to distinguish a random permutation from a permutation generated by using E with a random key with advantage greater than $e$.

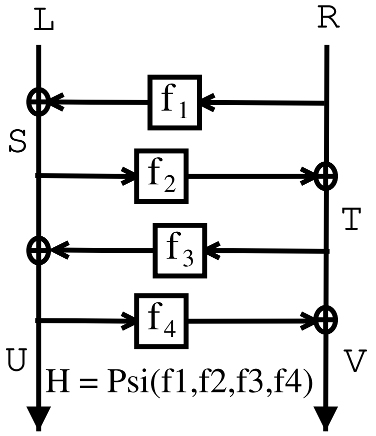


Figure 1: The four-round Luby-Rackoff construction

**Theorem 1 (Security of four-round Luby-Rackoff construction)**
*If $F : K \times \{0,1\}^n \to \{0,1\}^n$ is a $(t, q, e)$ secure pseudorandom function, then $H = \Psi[f_{K_1}, f_{K_2}, f_{K_3}, f_{K_4}]$ is a $(t - O(q), q, \frac{2q^2}{2^n} + 4e)$ secure pseudorandom permutation.*

PROOF (THEOREM 1) Intuition: The only information we have about $f$ is that it will produce the same output for a given input. Thus any attack must try to force an input collision to an $f$ function (which we will show is hard). We then use a hybrid argument, showing that $\Psi$ with random functions is secure, then working our way to using $F$ instead.

**Lemma 1** *If $f_1, ..., f_4$ are random functions and $A$ is any adversary making $\leq q$ queries, $|\Pr[A^{H,H^{-1}} = 1] - \Pr[A^{\pi,\pi^{-1}} = 1]| \leq \frac{2q^2}{2^n}$, where $\pi$ is a random permutation.*

PROOF (LEMMA 1) Assume $A$ is deterministic. This is reasonable because for every randomized algorithm, we can fix the optimal random choices to get a deterministic one that is at least as good.

We also assume no repeated or redundant oracle queries.

Define a **transcript** as a record of all oracle queries and responses $<(x_1, y_1), ..., (x_q, y_q)>$ during a run of $A$ where the $x_i$ are the inputs to the supplied function and $y_i$ the outputs. We don't distinguish between forward and inverse requests. Note that the output of the algorithm is purely a function of the transcript.

Define functions $R^+, R^-$:

- On query $x_i$ to $R^+$: if $\exists j < i : x_i = x_j$, output $y_j$ else output random $y_i$.
- On query $y_i$ to $R^-$: if $\exists j < i : y_i = y_j$, output $x_j$ else output random $x_i$.

Note that these are not random permutations since two different $x$ could be mapped to the same $y$.

Define a **consistent transcript** T to be one such that $x_i = x_j \Leftrightarrow y_i = y_j$.

**Lemma 2** *(Closeness of $\pi$ and $\Psi[R]$)*

$|\Pr[A^{R^+,R^-} = 1] - \Pr[A^{\pi,\pi^{-1}}] = 1| \leq \frac{q^2}{2^{2n+1}}$

PROOF (LEMMA 2) Fix any consistent transcript $T$. Then
$\Pr_\pi[\text{Transcript}(A^{\pi,\pi^{-1}}) = T] \leq \frac{1}{2^2n} \cdot \frac{1}{2^{2n}-1} \cdots \frac{1}{2^{2n}-q+1} = \frac{(2^{2n}-q)!}{2^{2n}!}$

$$\begin{aligned} \Pr[\text{Transcript}(A^{R^+,R^-}) = T | \text{Transcript}(A^{R^+,R^-}) \quad \text{consistent}] &= \\ \frac{\Pr(\text{transcript matches } T)}{Pr(\text{transcript consistent})} &\leq \\ \frac{2^{-2nq}}{(1)(1-\frac{1}{2^{2n}})(1-\frac{2}{2^{2n}})\cdots(1-\frac{q}{2^{2n}})} = \frac{(2^{2n}-q)!}{2^{2n}!} \end{aligned}$$

So when the transcript is consistent, the two can not be distinguished.

We also have

$$\Pr(T\text{inconsistent}) \leq \sum_{(i,j)} \Pr[\text{inconsistent at}(i,j)] = \frac{q^2}{2} * \frac{1}{2^{2n}} = \frac{q^2}{2^{2n+1}}$$

So we get

$$
\begin{aligned}
|\Pr[A^{R+,R-}=1]-\Pr[A^{pi,pi^{-1}}=1]| &= |\Pr[A^R=1|\text{Trans}(A^R)\text{ consistent}]\times\Pr[\text{Trans}(A^R)\text{ consistent}]\\
&\quad+\Pr[A^R=1|\text{Trans}(A^R)\text{ inconsistent}]\times\Pr[\text{Trans}(A^R)\text{ inconsistent}]\\
&\quad-\Pr[A^\pi=1]\times\Pr[\text{Trans}(A^R)\text{ consistent}]\\
&\quad+\Pr[A^\pi=1]\times\Pr[\text{Trans}(A^R)\text{ inconsistent}])|\\
&\le |\Pr[A^R=1|\text{Trans}(A^R)\text{ consistent}]-\Pr[A^\pi=|1]|\\
&\quad\times\Pr[\text{Trans}(A^R)\text{ consistent}]\\
&\quad+|\Pr[A^R=1|\text{Trans}(A^R)\text{ inconsistent}]-\Pr[A^\pi=|1]|\\
&\quad\times\Pr[\text{Trans}(A^R)\text{ inconsistent}]\\
&\le 0+\Pr[\text{Trans}(A^R)\text{ inconsistent}]\\
&\le \frac{q^2}{2^{2n+1}}
\end{aligned}
$$

Thus the distinguishing probability is bounded by the probability that the transcript is inconsistent, and we get the desired result. ■

(Proof of Lemma 1, continued.)

We showed that there is not much of a difference between $R$ and $\pi$. Now we show that there is not much of a difference between $R$ and $H$

**Lemma 3** *Consider any consistent $T$. Define the event BAD to means that $\exists i,j: S_i=S_j$ or $T_i=T_j$ where the indices refer to a particular query to the function (see diagram). We also define $L_i$ and $R_i$ to be the left and right halves, respectively, of the input to $x_i$ to $\Psi$. We use $U_i$ and $V_i$ for the outputs. We claim that $\Pr[BAD|\mathit{Transcript}(H)=T]\le\frac{q^2}{2^n}$.*

PROOF (LEMMA 3) Let us first note that given a transcript, the values of $S_i$ and $T_i$ for query $i$ can be determined solely from the transcript element $<x_i,y_i>$ and the functions $f_1$ and $f_4$ (see diagram).

$$
\begin{aligned}
\Pr[\text{BAD}|\text{Transcript}(H)=T] &\le \sum_{i,j}\Pr_{f_1,f_4}[f_1(R_i)-f_1(R_j)=L_j-L_i \quad \text{or}\\
&\qquad f_4(U_i)-f_4(U_j)=U_i-U_j]\\
&\le \sum_{i,j}\frac{1}{2^n}+\frac{1}{2^n}\\
&= \binom{q}{2}\frac{2}{2^n}\\
&\le \frac{q^2}{2^n}
\end{aligned}
$$
■

**Lemma 4** *Fix a consistent transcript $T$. Then*
$\Pr[\mathit{Transcript}(A^H)=T|\overline{BAD}]=\Pr[\mathit{Transcript}(A^R)=T]$ .

Proof (Lemma 4) First we assume that there are no repeated queries. This is reasonable since for every adversary that makes repeated queries, we can make another that remembers all past queries (a cache) and uses those values when possible rather than making another query.

Fix $f_1, f_4$ such that $\overline{BAD}$. Notice that

$$y_i = H(x_i) \leftrightarrow f_2(S_i) = T_i - R_i and f_3(T_i) = U_i - S_i$$

So for $q$ queries,

Once $f_1, f_4$ are chosen and the transcript $T$ is fixed, this fixes all the $S_i, T_i$. Also, $S_i \neq S_j$ and $T_i \neq T_j \forall i, j$ since we're conditioning on not BAD. Since all the $S_i$ are distinct and all the $T_i$ are distinct and $f2, f3$ are chosen independently, all the $2q$ events $f2(S_i) = T_i - R_i$ and $f3(T_i) = U_i - S_i$ are independent. Each of these $2q$ events has probability $2^{-n}$, since $f2, f3$ are random functions, so $Pr[Trans(A^H) = T|\text{not BAD}] = 2^{-2qn}$.

It is clear that $\Pr[\text{Transcript}(A^R) = T] = 2^{-2nq}$ as well.

(Proof of Lemma 1, continued)

We now have the following relation between $H$ and $R$:

$$\begin{aligned}
|\Pr[A^H = 1] - \Pr[A^R = 1]| &\leq |\Pr[A^H = 1 \text{ and Trans consistent}] \\
&\quad - \Pr[A^R = 1 \text{ and Trans consistent}]| \\
&\quad + \Pr[\text{Trans}(A^R) \text{ is inconsistent}] \\
&= |\Pr[A^H = 1 \text{ and Trans consistent} \mid \text{not BAD}] \Pr[notBAD] \\
&\quad + \Pr[A^H = 1 \text{ and Trans consistent} \mid \text{BAD}] \Pr[BAD] \\
&\quad - \Pr[A^R = 1 \text{ and Trans consistent}](\Pr[notBAD] + \Pr[BAD])| \\
&\quad + \Pr[\text{Trans}(A^R) \text{ is inconsistent}] \\
&\leq |\Pr[A^H = 1 \text{ and Trans consistent} \mid \text{not BAD}] \\
&\quad - \Pr[A^R = 1 \text{ and Trans consistent}]| * \Pr[notBAD] \\
&\quad + |\Pr[A^H = 1 \text{ and Trans consistent} \mid \text{BAD}] \\
&\quad - \Pr[A^R = 1 \text{ and Trans consistent}]| * \Pr[BAD] \\
&\quad + \Pr[\text{Trans}(A^R) \text{ is inconsistent}] \\
&\leq 0 \qquad \text{(by Lemma 4)} \\
&\quad + \Pr[\text{BAD}] \qquad \text{(trivially)} \\
&\quad + q^2/2^{2n+1} \qquad (\text{by Lemma 2, since } \Pr[\text{Trans}(A^\pi) \text{ is inconsistent}] = 0) \\
&\leq q^2/2^n + q^2/2^{2n+1} \qquad \text{(by Lemma 3)}
\end{aligned}$$

■

(Proof of Theorem 1, continued.)

At this point there's not much left. We just put the result of Lemma 1 together with the security of $F$. A key step in the hybrid argument is that no adversary can $e$-distinguish $\Psi[R_1, R_2, R_3, R_4]$ and $\Psi[F_{K_1}, R_2, R_3, R_4]$. If there were such an adversary $A'$, we could use it to $e$-distinguish $F$ and a random function $R$: on input $(F, R)$ we could choose 3 more randomly functions $F_2, F_3, F_4$, then use them with $F$ and $R_1 = R$ as input to $A'$. Since $F$ is not $e$-distinguishable from random by definition, our claim holds. The same argument can be used to show the $e$-indistinguishability of $\Psi[F_{K_1}, R_2, R_3, R_4]$ and $\Psi[F_{K_1}, F_{K_2}, R_3, R_4]$ etc.:

$$
\begin{array}{cl}
 & \text{random permutation } \pi \\
\xrightarrow{\frac{2q^2}{2^n}\text{(Lemma 1)}} & \Psi[R_1, R_2, R_3, R_4] \\
\xrightarrow{e \text{ (above)}} & \Psi[F_{K_1}, R_2, R_3, R_4] \\
\xrightarrow{3e \text{ (above)}} & \Psi[F_{K_1}, F_{K_2}, F_{K_3}, F_{K_4}]
\end{array}
$$

■