6.875J/18.425J Cryptography and Cryptanalysis	November 7, 2001
Lecture 17	
Instructor: Anna Lysyanskaya	*Scribed by: Anna Lysyanskaya*

1 Pseudorandom permutations

References: Luby-Rackoff. This presentation is from Goldreich's book.

1.1 Definition

Definition 1 *A family of permutations $P.(\cdot)$ is pseudo-random if both P and P^{-1} are efficiently computable, and the output is indistinguishable from a random permutation, given only oracle access to P_s. More precisely, let $\Pi(1^k)$ be the uniform distribution of all permutations over $\{0,1\}^k$. Then $P.(\cdot)$ is a pseudo-random permutation if $\forall$ PPTF $\{A_k\}$, there exists a negligible function $\nu(k)$, such that*

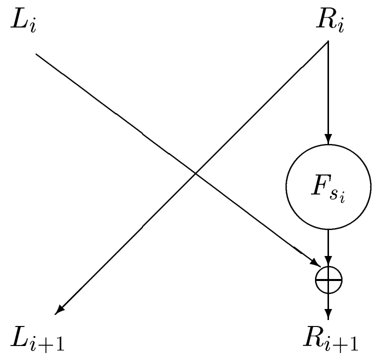
$$\begin{aligned}\Pr[s \leftarrow \{0,1\}^k; O_0 = P_s; O_1 \leftarrow \Pi(1^k) \quad &; \\ b \leftarrow \{0,1\}; b' \leftarrow A_k^{O_b}(1^k) \quad &: \quad b = b'] \leq 1/2 + \nu(k)\end{aligned}$$

Definition 2 *A family of permutations $P.(\cdot)$ is strongly pseudo-random if it is pseudo-random, and its output is indistinguishable from random given oracle access to both P_s and P_s^{-1}. More precisely,*

$$\begin{aligned}\Pr[s \leftarrow \{0,1\}^k; O_0 = P_s; O_1 \leftarrow \Pi(1^k) \quad &; \\ b \leftarrow \{0,1\}; b' \leftarrow A_k^{O_b, O_b^{-1}}(1^k) \quad &: \quad b = b'] \leq 1/2 + \nu(k)\end{aligned}$$

1.2 Construction

The following construction of a PRP on the basis of a one-way pseudo-random function $F_s(x) : \{0,1\}^{2k} \rightarrow \{0,1\}^{2k}$ is due to Luby and Rackoff. First, separate the input x into two parts, denoted by L_0 and R_0, of equal length: $x = L_0 \circ R_0, |L_0| = |R_0|$. Then we can obtain (L_{i+1}, R_{i+1}) from (L_i, R_i) as follows:



More precisely, $(L_{i+1}, R_{i+1}) = (R_i, L_i \oplus F_{s_i}(R_i))$, where $s_0 \circ s_1 \circ \cdots = s$, the seed for the PRP. The Luby-Rackoff construction uses repeated applications of this round (often referred to as a Feistel round) to construct a PRP and SPRP.

We saw last time that this results in a permutation. Now let us see why repeating this will result in a PRP.

Luby and Rackoff proved the following two theorems:

Theorem 3 *$LR-3 = P_3(x,y)$ is a PRP, for random s_1, s_2, s_3.*

Theorem 4

$LR-4 = P_4(x,y)$ is a SPRP, for random $s_1, \ldots, s_4$.

We will now prove Theorem 3; Theorem 4 will be a homework problem.

2 Proof for three rounds

The proof is broken up into the following three claims:

Claim 5 *If the PRFs F_1, F_2 and F_3 are replaced with random functions in the LR-3 construction, then the resulting function will be indistinguishable from a random function. (Call this resulting construction LR-3R). More precisely, let $\mathcal{F}(n)$ be the set of all functions $F : \{0,1\}^n \mapsto \{0,1\}^n$. Let $\mathcal{LR}$-3R$(2n)$ be the set of all functions obtained by choosing $F_i \leftarrow \mathcal{F}(n)$, $1 \le i \le 3$ and using these F_1, F_2, F_3 in the LR-3R construction. Then for all m, for all oracle machines $\mathcal{D}^?$ that make m queries*

$$\Pr[O_0 \leftarrow \mathcal{F}(2n); O_1 \leftarrow \mathcal{LR}\text{-}3R(2n); b \leftarrow \{0,1\}; b' \leftarrow \mathcal{D}^{O_b}(1^n) : b = b'] \le m^2/2^n$$

Proof of this claim will take the bulk of the lecture.

Claim 6 *If LR-3R is indistinguishable from a random function, then so is LR-3.*

This is easy to see.

Claim 7 *Let $\mathcal{F}(k)$ be the set of all functions $F : \{0,1\}^k \mapsto \{0,1\}^k$. Let $\mathcal{P}(k)$ be the set of all permutations over $\{0,1\}^k$. Then, for all oracle machines $\mathcal{D}^?$ that make a polynomial number of queries, there exists a negligible function $\nu(k)$ such that*

$$\Pr[O_0 \leftarrow \mathcal{F}(k); O_1 \leftarrow \mathcal{P}(k); b \leftarrow \{0,1\}; b' \leftarrow \mathcal{D}^{O_b}(1^k) : b = b'] \leq \nu(k)$$

This last claim will be left as a homework problem.

If we combine the claims, we get our theorem, because then it will follow, by the hybrid argument, that an adversary that distinguishes LR-3 from a random permutation, either distinguishes LR-3 from LR-3R (hence breaks the underlying PRF, by Claim 6) or distinguishes LR-3R form a random function (which contradicts Claim 5) or distinguishes a random function from a random permutation (which contradicts Claim 7).

Proof of Claim 5:

Suppose a distinguisher $\mathcal{D}$ makes m queries. Assume WLOG that all his queries are distinct.

Let A be an oracle that acts like a random function for this distinguisher with m queries: $\{0,1\}^{2n} \mapsto \{0,1\}^{2n}$. We can imagine that A works like this: Its random tape consists of $2m$ strings of length n, denote them $\{Y_i, Z_i : 1 \leq i \leq m\}$. On input L_i, R_i, A will output Y_i, Z_i. It's clear that A's behavior is the same as that of a random function.

Let B be an oracle that acts like the three-round Luby-Rackoff cipher with three random functions sitting in it. Let us look at B's code:

Fix random tape as consisting of $3m$ strings $\{X_i, Y_i, Z_i : 1 \leq i \leq m\}$.

For $1 \leq i \leq m$**, on input** (L_i, R_i) do:

- Let l_R be the least l index such that $R_i = R_l$. Let $\alpha_i = L_i \oplus X_{l_R}$.
- Let L_α be the least index l such that $\alpha_i = \alpha_l$. Let $\beta_i = R_i \oplus Y_{l_\alpha}$.
- Let L_β be the least index l such that $\beta_i = \beta_l$. Let $\gamma_i = \alpha_i \oplus \beta_{l_\beta}$.
- Output (β_i, γ_i).

Consider a different description for B, call it B':

Fix random tape as consisting of $3m$ strings $\{X_i, Y_i, Z_i : 1 \leq i \leq m\}$.

For $1 \leq i \leq m$**, on input** (L_i, R_i) do:

- Let l_R be the least l index such that $R_i = R_l$. Let If $l_R = i$ then let $\alpha_i = X_i$. Otherwise, let $\alpha_i = X_{l_R} \oplus L_{l_R} \oplus L_i$.
- Let l_α be the least index l such that $\alpha_i = \alpha_l$. If $l_\alpha = i$, then let $\beta_i = Y_i$. Otherwise, let $\beta_i = Y_{l_\alpha} \oplus R_{l_\alpha} \oplus R_i$.
- Let l_β be the least index l such that $\beta_i = \beta_l$. If $l_\beta = i$, then let $\gamma_i = Z_i$. Otherwise, let $\gamma_i = \alpha_i \oplus Z_{l_\beta} \oplus \alpha_{l_\beta}$.
- Output (β_i, γ_i).

B' is equivalent to B: for every setting of the random tape for B there is a unique setting of a random tape for B', so their behavior is identical.

In turn, B''s behavior is identical to that of A whenever for all i, $l_\alpha(i) = i$ and $l_\beta(i) = i$. This is simply because, whenever that is the case, B' outputs the contents of its random tape, just as A would do.

So, we wish to show that the probability that, for some $1 \leq l < i \leq m$, $l_\alpha(i) = l$ or $l_\beta(i) = l$, is at most $m^2/2^n$.

Suppose for all $l < i$, $l_\alpha(l) = l$ and $l_\beta(l) = l$. (As is the case for $i = 2$.)

What is the probability that, for a specific $l < i$, $\alpha_l = \alpha_i$? From the description of B', $\alpha_l = L_l \oplus X_{l_R(l)} \oplus L_{l_R(l)}$. $\alpha_i = L_i \oplus X_{l_R(i)} \oplus L_{l_R(i)}$. Suppose $R_l = R_i$. Then $X_{l_R(l)} \oplus L_{l_R(l)} = X_{l_R(i)} \oplus L_{l_R(i)}$, and therefore, $\alpha_i \neq \alpha_l$ since $L_l \neq L_i$, because we assumed that all queries were distinct. So, suppose $R_l \neq R_i$. Then $R(l) \neq R(i)$, so α_i and α_l are independently chosen random variables: $l_R(l) \neq l_R(i)$, so $X_{l_R(l)}$ and $X_{l_R(i)}$ are random variables that are independent of each other and also were chosen independently of the values $L_l, R_l, L_{l_R(l)}, L_i, R_i, L_{l_R(i)}$ (this is by assumption that for all $l < i$, $l_\alpha(l) = l$ and $l_\beta(l) = l$), so the probability that $\alpha_i = \alpha_l$ is the same as the probability that $L_l \oplus X_{l_R(l)} \oplus L_{l_R(l)} = L_i \oplus X_{l_R(i)} \oplus L_{l_R(i)}$ is, equivalently, the probability that $X_{l_R(l)} = X_{l_R(i)} \oplus L_l \oplus L_i \oplus L_{l_R(l)} \oplus L_{l_R(i)}$, is $1/2^n$.

Now, suppose for all $l < i$, $l_\alpha(l) = l$ and $l_\beta(l) = l$; also suppose that $l_\alpha(i) = i$. What is the probability that for a specific $l < i$, $l_\beta(i) = l$? $\beta_l = Y_l$ by the hypothesis that for all $l < i$, $l_\alpha(l) = l$ and $l_\beta(l) = l$. $\beta_i = Y_i$ because we of the hypothesis that $l_\alpha(i) = i$. Y_i and Y_l are independent random variables. So the probability that they are equal is $1/2^n$.

Now, by the union bound, the probability that for some $1 \leq l < i \leq m$, $\alpha_l = \alpha_i$ or $\beta_l = \beta_i$, is $\leq m^2/2^n$:

$$\begin{aligned} \Pr[\exists 2 \leq i \leq m \text{ s.t. } \exists l < i \text{ s.t. } \alpha_l = \alpha_i \text{ or } \beta_l = \beta_i] &= \\ \sum_{i=2}^{m} \Pr[\exists l < i \text{ s.t. } \alpha_l = \alpha_i \text{ or } \beta_l = \beta_i | \forall j_1 < j_2 < i \alpha_{j_1} \neq \alpha j_2 \wedge \beta_{j_1} \neq \beta j_2] &\leq \\ \sum_{i=2}^{m} 2(i-1)/2^n \leq m^2/2^n & \end{aligned}$$

Hence, we are done.