Fundamentals of Cryptography: Problem Set 4

Due Wed Oct 22 3PM

Collaboration is permitted (and encouraged); however, you must write up your own solutions and acknowledge your collaborators.

If a problem has **0pt**, it will not be graded.

Problem 0 Read Section 3.4, 3.5, 3.6 and the rest of Section 7 of "Introduction to Modern Cryptography (2nd ed)" by Katz & Lindell **or** Section 4, 5 of "A Graduate Course in Applied Cryptography" by Dan Boneh and Victor Shoup.

Problem 1 (6pt, Exercise 3.26 from KL) For any function $g : \{0,1\}^\lambda \to \{0,1\}^\lambda$, define $g^{\$}(\cdot)$ to be a *probabilistic* oracle, on input 1^λ it samples uniform $r \in \{0,1\}^\lambda$ and returns $(r, g(r))$. A keyed function F is called *weak PRF* if for all p.p.t. algorithms $\mathcal{D}$, there exists a negligible function negl such that:

$$\left|\Pr[\mathcal{D}^{F_k^{\$}(\cdot)}(1^\lambda) = 1] - \Pr[\mathcal{D}^{f^{\$}(\cdot)}(1^\lambda) = 1]\right| \leq \text{negl}(\lambda),$$

where $k \in \{0,1\}^\lambda$, $f : \{0,1\}^\lambda \to \{0,1\}^\lambda$ are chosen uniformly.

Part A Prove that if F is PRF then it is weak PRF.

Part B Let F' be a PRF, define

$$F_k(x) := \begin{cases} F'_k(x) & \text{if } x \text{ is even} \\ F'_k(x+1) & \text{if } x \text{ is odd.} \end{cases}$$

Show that F is a weak PRF, but *not* a PRF.

Part C Is CTR-mode encryption using a weak PRF necessarily CPA-secure? Does it necessarily have indistinguishable encryptions in the presence of an eavesdropper? Prove your answers.

Part D Prove that following construction is CPA-secure if F is a weak PRF.

Construction 3.28 from Katz & Lindell
Let $F : \{0,1\}^\lambda \times \{0,1\}^\lambda \to \{0,1\}^\lambda$ be a PRF. Define a fixed-length, private-key encryption scheme for messages of length λ as follows:

- $\mathsf{Gen}(1^\lambda)$: choose uniform $k \in \{0,1\}^\lambda$ and output it
- $\mathsf{Enc}(k, m)$: choose uniform $r \in \{0,1\}^\lambda$ and output the ciphertext

$$c := (r, F_k(r) \oplus m).$$

- $\mathsf{Dec}(k, (r, s))$: output the message $m = F_k(r) \oplus s$.

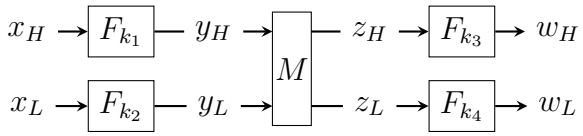
Problem 2 (6pt) Let $F : \{0,1\}^\lambda \times \{0,1\}^n \to \{0,1\}^n$ be a keyed permutation for some $n(\lambda) \geq \lambda$. Consider the keyed permutation $P : \{0,1\}^{4\lambda} \times \{0,1\}^{2n} \to \{0,1\}^{2n}$

$P(k, x)$: Parse the key evenly into $k_1, k_2, k_3, k_4 \in \{0,1\}^\lambda$. Parse the input evenly into $x_H, x_L \in \{0,1\}^n$. Compute $y_H = F_{k_1}(x_H)$, $y_L = F_{k_2}(x_L)$. Compute

$$\begin{bmatrix} z_H \\ z_L \end{bmatrix} = M \begin{bmatrix} y_H \\ y_L \end{bmatrix}$$

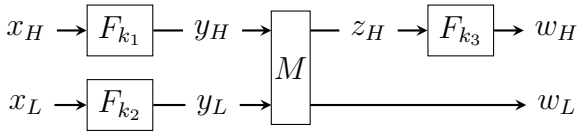
for a given invertible 2-by-2 matrix M over GF(2^n). That is, y_H, y_L are interpreted as elements in the finite field GF(2^n). Compute $w_H = F_{k_3}(z_H)$, $w_L = F_{k_4}(z_L)$. Output (w_H, w_L).

The construction can be visualized as the following.

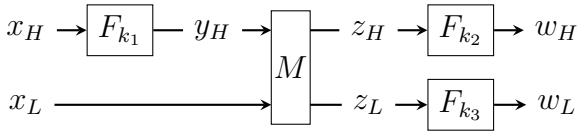


It is known that if F is a strong PRP, then P is a strong PRP as well. (The fixed public matrix needs M to satisfies some properties: All entries in M are non-zero. All entries in M^{-1} are non-zero.)

Part A. If F is a PRP, is $P' : \{0,1\}^{3\lambda} \times \{0,1\}^{2n} \to \{0,1\}^{2n}$ a PRP? P' is illustrated as follows:



Part B. If F is a PRP, is $P'' : \{0,1\}^{3\lambda} \times \{0,1\}^{2n} \to \{0,1\}^{2n}$ a PRP? P'' is illustrated as follows:



Problem 3 (8pt) Assume $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ is a PRP, who has an efficient inversion algorithm. For each of the following statement, prove the statement, or show a counterexample.

Part A F is a strong PRP.

Part B Define $F'(k, x) = x \oplus F(k, x)$. Then F' is a PRF.

Part C Let $F'(k, x) = F(k_2, F(k_1, x))$, where $k = k_1 \| k_2$. Then F' is a PRP.

Part D Let $F'(k, x) = F(k, F(k, x))$. Then F' is a PRP.

Part E (bonus 100pt) Let $F'(k, x) = F^{-1}(k_1, F(k_2, x))$, where $k = k_1 \| k_2$. Then F' is a strong PRP.

Part F (bonus 100pt) Let $F'(k, x) = F(k_1, F^{-1}(k_2, x))$, where $k = k_1 \| k_2$. Then F' is a strong PRP.

Problem 4 (6pt) Given functions $h_1, \ldots, h_t : \{0,1\}^n \to \{0,1\}^n$, the t-round Feistel network is defined as:

> $\text{Feistel}_{h_1,\ldots,h_t}(x_0, x_1)$ takes (x_0, x_1) as the input.
>
> For each $1 \le i \le t$:
>
> Set $x_{i+1} \leftarrow x_{i-1} \oplus h_i(x_i)$.
>
> Output (x_t, x_{t+1}) as the output.

Let $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a secure PRF, we know that

$$f_1((k_1, k_2, k_3), (x_0, x_1)) = \text{Feistel}_{f(k_1,\cdot),f(k_2,\cdot),f(k_3,\cdot)}(x_0, x_1)$$
$$f_2((k_1, k_2, k_3, k_4), (x_0, x_1)) = \text{Feistel}_{f(k_1,\cdot),f(k_2,\cdot),f(k_3,\cdot),f(k_4,\cdot)}(x_0, x_1)$$

are PRP and strong PRP respectively. In this problem, we wonder what if the round keys in Feistel network are not independent.

Part A. Is $f_3((k_1, k_2), (x_0, x_1)) = \text{Feistel}_{f(k_1,\cdot),f(k_2,\cdot),f(k_2,\cdot)}(x_0, x_1)$ a PRP? Briefly prove your claim.

Part B. Is $f_4((k_1, k_2), (x_0, x_1)) = \text{Feistel}_{f(k_1,\cdot),f(k_2,\cdot),f(k_2,\cdot),f(k_1,\cdot)}(x_0, x_1)$ a strong PRP? Briefly prove your claim.