Fundamentals of Cryptography: Problem Set 5

Due Wed Oct 23 3PM

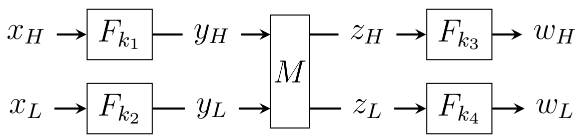
Collaboration is permitted (and encouraged); however, you must write up your own solutions and acknowledge your collaborators.

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

Problem 1 (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 $P : \{0,1\}^{4\lambda} \times \{0,1\}^{2n} \to \{0,1\}^{2n}$

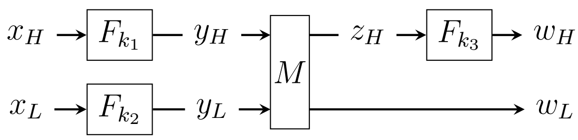
> $P(k, x)$: Parse the key evenly into $k_1, k_2, k_3, k_4 \in \{0,1\}^\lambda$. Parse the input evenly into $x_H, x_L \in \{0,1\}^n$. Compute $y_H = F_{k_1}(x_H)$, $y_L = F_{k_2}(x_L)$. Compute
>
> $$\begin{bmatrix} z_H \\ z_L \end{bmatrix} = M \begin{bmatrix} y_H \\ y_L \end{bmatrix}$$
>
> for a given 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.

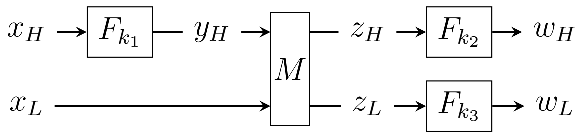


It is known that if F is a strong PRP, then P is a strong PRP as well. (The fixed public matrix needs M to satisfies some properties: All entries in M are non-zero. All entries in M^{-1} are non-zero.)

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 2 (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 3 (bonus 1000pt) A PRF $F : \{0,1\}^\lambda \times \{0,1\}^\lambda \to \{0,1\}^{\mathrm{poly}(\lambda)}$ is called an *invertible puncturable PRF* if

- There is a p.p.t. algorithm $\mathsf{puncture}$, which takes a key k, an input x, and outputs a "punctured key" k_{-x}.
- There is a p.p.t. algorithm eval, such that for any $x' \neq x$, we have $\mathsf{eval}(k_{-x}, x') = F_k(x')$, where $k_{-x} \leftarrow \mathsf{puncture}(k,x)$.
- There is a p.p.t. algorithm invert, such that for any x, $\mathsf{invert}(k, F_k(x)) = x$.
- If k, u are randomly sampled, $(k_{-x}, F_k(x))$ is indistinguishable from (k_{-x}, u).

  (More formally, consider a security game: the distinguisher $\mathcal{D}$ chooses x; the challenger samples random k, u, computes $k_{-x} \leftarrow \mathsf{puncture}(k,x)$, and sends

  - in case 0: $(k_{-x}, F_k(x))$, or
  - in case 1: (k_{-x}, u)

  to the distinguisher. We require that for any p.p.t. distinguisher $\mathcal{D}$, the distinguisher cannot tell which case it is with non-negligible advantage.)

Your task is to construct an invertible puncturable PRF. You may assume the existence of OWF (thus PRG, PRF and PRP).