Introduction to cryptology
TD#2

2022-W06,...

Exercise 1: PRPs

Let $\mathcal{E} : \{0,1\}^\kappa \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher for which there is a subset $\mathcal{K}' \subset \{0,1\}^\kappa$ of *weak keys* of size 2^w such that if $k \in \mathcal{K}'$, $\mathcal{E}(k, \cdot) : x \mapsto x$.

Q. 1: Give a lower-bound for $\mathbf{Adv}_{\mathcal{E}}^{\mathrm{PRP}}(1,1)$.

Q. 2: Some mode of operation of block ciphers rely on the fact that $\mathcal{E}(k, 0)$ is an unpredictable value when k is picked uniformly at random and kept secret (with 0 denoting the all-zero binary string).

Show that this is a reasonable assumption. More precisely, give a lower-bound on $\mathbf{Adv}_{\mathcal{E}}^{\mathrm{PRP}}(1,1)$ assuming that one can predict this value with unit time and success probability p.

Exercise 2: Format-preserving encryption *(Adapted from M2's exam, 2021)*

A *format-preserving* block cipher is a block cipher $\mathcal{E} : \{0,1\}^\kappa \times \mathcal{S} \to \mathcal{S}$ where $\mathcal{S}$ is an arbitrary finite set (that is $\mathcal{S}$ is not necessarily equal to $\{0,1\}^n$ for some n). For instance, $\mathcal{S}$ could be $\Pi_{\leq 2^{128}}$, the set of primes less than 2^{128}.

The *cycle walking* algorithm is a method to convert a block cipher $\mathcal{E} : \{0,1\}^\kappa \times \{0,1\}^n \to \{0,1\}^n$ into $\mathcal{E}' : \{0,1\}^\kappa \times \mathcal{S} \to \mathcal{S}$ for any $\mathcal{S} \subseteq \{0,1\}^n$ as long as it is efficient to test if an element of $\{0,1\}^n$ is in $\mathcal{S}$. It works as follows: to encrypt $x \in \mathcal{S}$ with the key k, compute $x' := \mathcal{E}(k, x)$. If $x' \in \mathcal{S}$ then return x'; otherwise iterate the process by computing $x'' = \mathcal{E}(k, x')$ and testing if it is in $\mathcal{S}$, etc.

Q.1

1. Give an algorithm for the inverse $\mathcal{E}'^{-1} : \{0,1\}^\kappa \times \mathcal{S} \to \mathcal{S}$ of a block cipher $\mathcal{E}'$ over $\mathcal{S}$ obtained from cycle walking applied to some suitable block cipher $\mathcal{E}$.
2. Show that the condition that $\mathcal{S} \subseteq \{0,1\}^n$ be efficiently testable is not enough to guarantee that cycle walking will result in an efficient block cipher.

We now suppose the existence of a black-box algorithm that efficiently converts a block cipher $\mathcal{E} : \{0,1\}^\kappa \times \{0,1\}^n \to \{0,1\}^n$ into $\mathcal{E}' : \{0,1\}^\kappa \times \{0,1\}^{n'} \to \{0,1\}^{n'}$ for any $0 < n' < n$.

Q.2

1. How does the existence of this black-box allow to remedy the efficiency problem from the previous question in some cases?
2. Are there still sets for which cycle walking is inefficient?

Exercise 3: PRP-PRF switching *(Exam '21)*

We first consider an oracle $\mathbb{O} : \{0,1\}^n \rightarrow \{0,1\}^n$, which can be one of two things:

— In the *PRP world*, $\mathbb{O} \twoheadleftarrow \text{Perms}(\{0,1\}^n)$. Said otherwise, it samples its outputs uniformly from $\{0,1\}^n$ *without* replacement.

— In the *PRF world*, $\mathbb{O} \twoheadleftarrow \text{Funcs}(\{0,1\}^n)$. Said otherwise, it samples its outputs uniformly from $\{0,1\}^n$ *with* replacement.

Q.1: We consider an algorithm $A_q^{\mathbb{O}}$ which makes q (distinct) queries $x_1, \ldots, x_q$ to its oracle $\mathbb{O}$.

Give an estimate for the probability $\in [0,1]$ that there is a collision between two outputs of $\mathbb{O}$ in the PRP (resp. PRF) world, i.e. estimate the following:

1. $p_q^P := \Pr[\exists\, i, j \neq i, \mathbb{O}(x_i) = \mathbb{O}(x_j) : \mathbb{O} \twoheadleftarrow \text{Perms}(\{0,1\}^n)]$;
2. $p_q^F := \Pr[\exists\, i, j \neq i, \mathbb{O}(x_i) = \mathbb{O}(x_j) : \mathbb{O} \twoheadleftarrow \text{Funcs}(\{0,1\}^n)]$.

Only a brief justification of your answers is necessary.

Q.2: *Using your answers to the previous question*:

1. Specify a distinguisher $A^{\mathbb{O}}$ that returns 1 if $\mathbb{O}$ is believed to be in the PRP world, and 0 if it is believed to be in the PRF world.
2. Estimate its advantage $|\Pr[A_q^{\mathbb{O}}() = 1 : \mathbb{O} \twoheadleftarrow \text{Perms}(\{0,1\}^n)] - \Pr[A_q^{\mathbb{O}}() = 1 : \mathbb{O} \twoheadleftarrow \text{Funcs}(\{0,1\}^n)]|$ in function of the number of queries q made to the oracle only (i.e. where its running time may be arbitrary).[1]

Q.3: We now consider a block cipher $\mathcal{E} : \{0,1\}^\kappa \times \{0,1\}^n \rightarrow \{0,1\}^n$ s.t. $\mathbf{Adv}_{\mathcal{E}}^{\text{PRP}}(q,t) = t/2^\kappa$ when $q = \Omega(n/\kappa)$. We wish to analyse $\mathcal{E}$ in a "PRF setting". You may now assume that the advantage of your distinguisher from **Q.2** remains the same as the one you computed as long as $t = \Omega(q)$.

1. Based on your distinguisher from **Q.2** and the definition of $\mathcal{E}$, give a lower-bound for $\mathbf{Adv}_{\mathcal{E}}^{\text{PRF}}(q,t)$. You do not need to specify a matching distinguisher.

Q.4: We now consider a family of functions $\mathcal{F} : \{0,1\}^\kappa \times \{0,1\}^n \rightarrow \{0,1\}^n$ s.t. one has $\mathbf{Adv}_{\mathcal{F}}^{\text{PRF}}(q,t) = t/2^\kappa$ when $q = \Omega(n/\kappa)$.

1. Is it possible to analyse $\mathcal{F}$ in a "PRP setting", i.e. to study $\mathbf{Adv}_{\mathcal{F}}^{\text{PRP}}(q,t)$?

Q.5:

1. Is it possible and meaningful to use a "good PRP" block cipher $\mathcal{E} : \{0,1\}^\kappa \times \{0,1\}^n \rightarrow \{0,1\}^n$ in a context where a "good PRF" family of functions $\mathcal{F} : \{0,1\}^\kappa \times \{0,1\}^n \rightarrow \{0,1\}^n$ is expected? If yes, what would one "lose" by doing so?
2. Is it possible and meaningful to use a "good PRF" family of functions $\mathcal{F} : \{0,1\}^\kappa \times \{0,1\}^n \rightarrow \{0,1\}^n$ in a context where a "good PRP" block cipher $\mathcal{E} : \{0,1\}^\kappa \times \{0,1\}^n \rightarrow \{0,1\}^n$ is expected? If yes, what would one "lose" by doing so?

[1] This is usually called an *information-theoretic* distinguisher, or a distinguisher in the *information theory* setting.