Cryptography for Computer Scientists 2017/18 Nov 8, 2017

Exercises 5

Stefan Dziembowski MIM UW

Exercise 1: Strongly universal hash functions

Let $\mathcal{K}, \mathcal{X}$ and $\mathcal{Y}$ be finite sets. A family of functions

$$\mathcal{H} = \{H_K : \mathcal{X} \to \mathcal{Y}\}_{K \in \mathcal{K}}$$

is called a *strongly universal hash function family* if for every $x_0, x_1 \in \mathcal{X}$ such that $x_0 \neq x_1$ and every $y_0, y_1 \in \mathcal{Y}$ we have

$$\Pr[H(x_0) = y_0 \wedge H(x_1) = y_1 \ : \ K \leftarrow_{\$} \mathcal{K}] = 1/|\mathcal{Y}|^2$$

For every n give an example of an (efficiently computable) strongly universal hash function family with $|\mathcal{Y}| \geq n$ and $|\mathcal{K}| = \mathsf{poly}(|\mathcal{Y}|)$.

Exercise 2: Information-theoretically secure MACs

Given a strongly universal hash function family $\mathcal{H}$ as above define a MAC as follows. The key space is $\mathcal{K}$, the plaintext space is $\mathcal{X}$, and the set of tags is $\mathcal{Y}$. The tagging algorithm is defined as:

$$\mathsf{Tag}_k(x) = H_k(x),$$

and the verification algorithms is defined as:

$$\mathsf{Vrfy}_k(x, y) = \begin{cases} \mathsf{yes} & \text{if } H_k(x) = y \\ \mathsf{no} & \text{otherwise.} \end{cases}$$

Suppose this MAC is attacked be an adversary $\mathcal{A}$ that has the following properties

- $\mathcal{A}$ is computationally unbounded,
- $\mathcal{A}$ can issue only one "message query" m_1 before he attempts to forge a tag (i.e. $w = 1$),

Show that for any such adversary $\mathcal{A}$ his probability of issuing a pair (m', t') such that $m' \neq m$ and $\mathsf{Vrfy}(m', t')$ is at most $1/|\mathcal{Y}|$.
How can you generalize it for $w > 1$?

Exercise 3: A motivation for CCA (chosen ciphertext attack)-security

In this exercise we assume that if a decryption algorithm gets as input a ciphertext c that "cannot be decrypted under a given k" (i.e. there does not exist any message m such that $\mathsf{Enc}_k(m) = c$) then it outputs $\perp$.
Give an example of an encryption scheme $(\mathsf{Enc}, \mathsf{Dec})$ with a ciphertext space $\{0,1\}^n$ (for a security parameter n) that has the following properties.

- $(\mathsf{Enc}, \mathsf{Dec})$ is CPA-secure,
- $(\mathsf{Enc}, \mathsf{Dec})$ can be broken (in the sense that a poly-time adversary can learn the entire message with probability 1) if the adversary has access to the following oracle Ω:

  $\Omega(1^n)$ on input $c \in \{0,1\}^n$ replies to $\mathcal{A}$ with

  $$\begin{array}{rl} \mathsf{error} & \text{if } \mathsf{Dec}_k(c) = \perp \\ \mathsf{ok} & \text{otherwise} \end{array}$$

Can you find a similar example if the message is additionally authenticated using

- the *authenticate-then-encrypt* method?
- the *encrypt-then-authenticate* method?

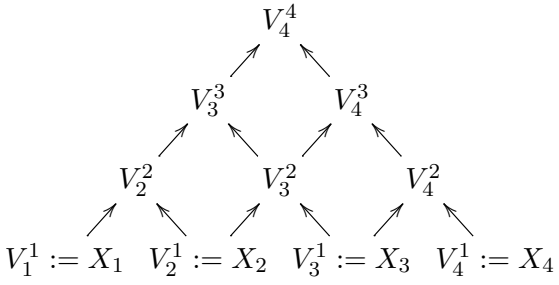
Exercise 4: Memory complexity of the *Pyramid* function *(homework)*

Let $L \in \mathbb{N}$ and $N \in \mathbb{N}$ be some parameters and let $H : (\{0,1\}^L)^2 \to \{0,1\}^L$ be a hash function (modeled as a random oracle). Define a function $Pyramid^N : (\{0,1\}^L)^N \to \{0,1\}^L$ using following algorithm.

$Pyramid^N(X_1, \ldots, X_N)$

$(V_1^1, \ldots, V_N^1) := (X_1, \ldots, X_N)$
for $i = 2, \ldots, N$ **do**
  for $j = i, \ldots, N$ **do**
    $V_j^i := H(V_{j-1}^{i-1}, V_j^{i-1})$
return V_N^N

Below is an example of the execution of this algorithm for $N = 4$:



Now consider algorithms that compute $Pyramid^N$ by issuing a sequence of instructions from the following set:

- *Load* V_j^1 into memory (for $j = 1, \ldots, N$).
- *Compute* V_j^i (for $1 \le i \le j \le N$) — only if V_{j-1}^{i-1} and V_j^{i-1} are in the memory,
- *Release* V_j^i (for $1 \le i \le j \le N$) from the memory.
- *Output* V_N^N.

(Note these algorithms *cannot* do any operations on the V_j^i variables other than computing H.) Prove that any algorithm from this class that computes $Pyramid^N$ with probability 1 for every L has memory complexity $L \cdot N$. Show that this bound is optimal by constructing an algorithm with this memory complexity.

Think how to prove a similar bound without restrictions on the set of instructions.