Introduction to Cryptography – LMAT2450
Practical Lesson 4 (2 sessions)

Clément Hoffmann (clement.hoffmann@uclouvain.be)
Yaobin Shen (yaobin.shen@uclouvain.be)

October 26, 2022

Exercise 1 (simple attacks) Let $\mathsf{MAC} = (\mathsf{Gen}, \mathsf{Mac}, \mathsf{Vrfy})$ be a variable-length MAC that is existentially unforgeable under an adaptive chosen-message attack. Consider the following schemes $\mathsf{MAC}' = (\mathsf{Gen}', \mathsf{Mac}', \mathsf{Vrfy}')$ based on MAC with $\mathsf{Gen}' = \mathsf{Gen}$ and where Mac' are defined as follows[1]:

a. $\mathsf{Mac}'_k(m) := (\mathsf{Mac}_k(m), \mathsf{Mac}_k(m \oplus 0...01))$

b. $\mathsf{Mac}'_k(m) := \mathsf{Mac}_k(\bigoplus_{i=1}^{l} m_i)$

c. $\mathsf{Mac}'_k(m) := (\mathsf{Mac}_k(m_1), ..., \mathsf{Mac}_k(m_l))$

d. $\mathsf{Mac}'_k(m) := (\mathsf{Mac}_k(m_1), \mathsf{Mac}_k(m_1||m_2), ..., \mathsf{Mac}_k(m_1||...||m_l))$

Show that those scheme are not existentially unforgeable under an adaptive chosen-message attack.

Let $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be a variable-length encryption scheme that is CCA-secure. Consider $\Pi' = (\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$ based on Π with $\mathsf{Gen}' = \mathsf{Gen}$ defined as follows:

i. $\mathsf{Enc}'_k(m) := (\mathsf{Enc}_k(m), \mathsf{Enc}_k(\bigoplus_{i=1}^{l} m_i))$

ii. $\mathsf{Enc}'_k(m) := (\mathsf{Enc}_k(m), \bigoplus_{i=1}^{l} m_i)$

iii. $\mathsf{Enc}'_k(m) := (\mathsf{Enc}_k(m), \mathsf{Enc}_k(m \oplus 110...0))$

iv. $\mathsf{Enc}'_k(m) := (\mathsf{Enc}_k(m||0), \mathsf{Enc}_k(m))$

Show that those schemes are not CCA-secure.

Exercise 2 (unsuccessful MAC length extension) Let F be a PRF. Below, we describe three *insecure variable-length* message authentication codes, Π_1, Π_2 and Π_3, which all use the same key generation algorithm Gen. The message space is *any number* of message blocks in $\{0,1\}^n$, where n is the security parameter.

$\mathsf{Gen}(1^n)$ outputs a random key $k \leftarrow \{0,1\}^n$.

[1] In some cases m is parsed in $m_1, ..., m_l$ with $|m_1| = ... = |m_{l-1}| = n$, $|m_l| \leq n$ and $m_1||...||m_l = m$ ($||$ is the concatenation) where n is the security parameter.

The scheme Π_3 is built from Π_2 which is itself built from Π_1 as an (unsuccessful) attempt to "patch" the previous scheme:

$\Pi_1 = (\mathsf{Gen}, \mathsf{Mac}^1, \mathsf{Vrfy}^1)$: *"Deterministic MAC – Chaining PRFs"*

$\mathsf{Mac}^1_k(m_1, \ldots, m_\ell)$ computes $t_1 = F_k(m_1)$ as well as $t_i = F_k(m_i \oplus t_{i-1})$, for $i = 2$ to ℓ, and returns $t := t_\ell$ (note that only the last block is returned).

$\mathsf{Vrfy}^1_k((m_1, \ldots, m_\ell), t)$ outputs 1 if $\mathsf{Mac}^1_k(m_1, \ldots, m_\ell) = t$, and 0 otherwise.

$\Pi_2 = (\mathsf{Gen}, \mathsf{Mac}^2, \mathsf{Vrfy}^2)$: *"Padding a random message block in the end"*

$\mathsf{Mac}^2_k(m_1, \ldots, m_\ell)$ first picks a random $r \leftarrow \{0,1\}^n$ and then runs $t = \mathsf{Mac}^1_k(m_1, \ldots, m_\ell, r)$ and outputs (r, t).

$\mathsf{Vrfy}^2_k((m_1, \ldots, m_\ell), (r, t))$ outputs 1 if $\mathsf{Mac}^1_k(m_1, \ldots, m_\ell, r) = t$, and 0 otherwise.

$\Pi_3 = (\mathsf{Gen}, \mathsf{Mac}^3, \mathsf{Vrfy}^3)$: *"Padding a random message block in the beginning"*

$\mathsf{Mac}^3_k(m_1, \ldots, m_\ell)$ first picks a random $s \leftarrow \{0,1\}^n$ and then runs $(r, t) = \mathsf{Mac}^2_k(s, m_1, \ldots, m_\ell)$ and outputs (r, s, t).

$\mathsf{Vrfy}^3_k((m_1, \ldots, m_\ell), (r, s, t))$ outputs 1 if $\mathsf{Mac}^1_k(s, m_1, \ldots, m_\ell, r) = t$, and 0 otherwise.

a) Describe $\mathsf{Mac}^3_k(m_1, \ldots, m_\ell)$ explicitly in terms of computations of F_k (and $\oplus$ of course).

b) Show the correctness of Π_3.

c) Mount a forgery attack on these MACs.

Exercise 3 (successful MAC length extension) Let $\Pi' := \langle \mathsf{Gen}', \mathsf{Mac}', \mathsf{Vrfy}' \rangle$ be a secure fixed-length MAC. We define a variable-length MAC $\Pi := \langle \mathsf{Gen}, \mathsf{Mac}, \mathsf{Vrfy} \rangle$ as follows:

- Gen: choose random $k \leftarrow \{0,1\}^n$
- Mac: on input $k \in \{0,1\}^n$ and $m \in \{0,1\}^*$ of length $l < 2^{\frac{n}{4}}$
  - Parse m into blocks $m_1, \ldots, m_d$ of length $\frac{n}{4}$ each (pad with 0's if necessary)
  - Choose random $r \leftarrow \{0,1\}^{\frac{n}{4}}$
  - Compute $t_i := \mathsf{Mac}'_k(r||l||i||m_i)$ for $1 \le i \le d$, with $|r| = |l| = |i| = \frac{n}{4}$
  - Output $t := \langle r, t_1, \ldots, t_d \rangle$
- Vrfy: on input $k, m, t = \langle r, t_1, \ldots, t_{d'} \rangle$,
  - Parse m into blocks $m_1, \ldots, m_d$ of length $\frac{n}{4}$ each
  - Output 1 iff $d = d'$ and, $\forall 1 \le i \le d$, $\mathsf{Vrfy}'_k(r||l||i||m_i, t_i) = 1$

The goal of this exercise is to prove by reduction that Π is existentially unforgeable. Let $\mathcal{A}$ (resp. $\mathcal{A}'$) be an adversary attacking the unforgeability of Π (resp. Π') and let $\epsilon(n) = \Pr[\textsc{MacForge}_{\mathcal{A},\Pi}(n) = 1]$ (resp. $\epsilon'(n) = \Pr[\textsc{MacForge}_{\mathcal{A}',\Pi'}(n) = 1]$) denotes its advantage.

a) Make a quick draw sketching the proof.

b) Describe formally how $\mathcal{A}'$ should react to a query $\textsc{Mac}_k(m)$.

c) Define what is a mac forgery for the scheme Π. Does it necessarily imply a forgery on the scheme Π' (justify your answer).

d) Express ϵ in function of ϵ' and conclude.

Exercise 4 Let F be a pseudorandom function, G be a pseudorandom permutation, T be a public n-bit constant, k be a n-bit secret key, m be a n-bit message, IV be a n-bit random value chosen by the party computing the encryption (resp. MAC) before each operation. Among the following algorithms, determine the ones that would be acceptable in a corresponding scheme and justify your answer.

a) $\mathsf{Enc}_k(m) := F_k(m \oplus T)$ as an encryption scheme secure against eavesdropping.

b) $\mathsf{Enc}_k(m) := G_k(m \oplus T)$ as an encryption scheme secure against eavesdropping.

c) $\mathsf{Enc}_k(m) := G_k(m \oplus T)$ as an encryption scheme secure against a CPA-adversary.

d) $\mathsf{Enc}_k(m) := (IV, G_k(m \oplus T \oplus IV))$ as an encryption scheme secure against a CPA-adversary.

e) $\mathsf{Mac}_k(m) := F_k(m \oplus T)$ as a MAC scheme existentially unforgeable under an adaptive chosen-message attack.

f) $\mathsf{Mac}_k(m) := (IV, G_k(m \oplus IV \oplus T))$ as a MAC scheme existentially unforgeable under an adaptive chosen-message attack.

Exercise 5 (authenticated encryption from pseudorandom permutation) Consider the following scheme $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ based on the strong pseudorandom permutation $F : \mathcal{K} \times \{0,1\}^n$. Π is defined as follow:

- $\mathcal{M} = \{0,1\}^{\frac{n}{2}}$ (the message space)
- Gen picks a random key $k \in \mathcal{K}$
- $\mathsf{Enc}_k(m)$ picks a random value $r \in \{0,1\}^{\frac{n}{2}}$, and computes $c \leftarrow F_k(m\|r)$
- $\mathsf{Dec}_k(c)$ computes $(m\|r) = F_k^{-1}(c)$ and outputs m (the first half).

a) Is Π unforgeable?

b) Is Π CCA-secure?

c) Is Π an authenticated encryption scheme?

Definition 1 (*Strong Pseudorandom Permutation*)

A function $F : \{0,1\}^* \times \{0,1\}^* \longmapsto \{0,1\}^*$ be an efficient, length-preserving, keyed permutation. F is a *strong pseudorandom permutation* if for all PPT distinguisher D, there exists a negligible function ϵ such that,

$$\left|\Pr\left[D^{F_k(\cdot),F_k^{-1}(\cdot)}(1^n) = 1\right] - \Pr\left[D^{f(\cdot),f^{-1}(\cdot)}(1^n) = 1\right]\right| \leq \epsilon(n)$$

where k is taken uniformly at random in $0,1^n$ and f is taken uniformly at random from the set of all permutations (bijections of $\{0,1\}^n$).

Exercise 6 Let $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be an authenticated encryption scheme where $0 \notin \mathcal{C}$ (that is, the string "0" is not a possible ciphertext for Π). Consider the following scheme $\Pi' := (\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$ with:

- $\mathsf{Gen}' = \mathsf{Gen}$
- $\mathsf{Enc}'_k = \mathsf{Enc}_k$
- $\forall k : \begin{cases} \mathsf{Dec}'_k(c) = \mathsf{Dec}_k(c) & \text{if } c \neq 0, \\ \mathsf{Dec}'_k(c) = 0 & \text{if } c = 0. \end{cases}$

a) Is Π' unforgeable?

b) Is Π' CCA secure?

Exercise 7 (August 2018) Let $\Pi = \langle \mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec} \rangle$ be an authenticated encryption scheme such that Enc encrypts messages of n bits. Do the following systems provide authenticated encryption? For those that do, briefly explain why. For those that do not, present an attack that breaks one of the security properties of an authenticated encryption scheme.

$\Pi^1 = \langle \mathsf{Gen}, \mathsf{Enc}^1, \mathsf{Dec}^1 \rangle$ with

- $\mathsf{Enc}^1_k(m) = (\mathsf{Enc}_k(m), \mathsf{Enc}_k(m \oplus (0^{n-1} \| 1)))$
- $\mathsf{Dec}^1_k(c_1, c_2) = \mathsf{Dec}_k(c_1)$ if $\mathsf{Dec}_k(c_1) \oplus \mathsf{Dec}_k(c_2) = 0^{n-1} \| 1$ and $\perp$ otherwise.

$\Pi^2 = \langle \mathsf{Gen}, \mathsf{Enc}^2, \mathsf{Dec}^2 \rangle$ with

- $\mathsf{Enc}^2_k(m) = (\mathsf{Enc}_k(m), \mathsf{Mac}_k(m))$
- $\mathsf{Dec}^2_k(c_1, c_2) = \mathsf{Dec}_k(c_1)$ if $\mathsf{Vrfy}_k(\mathsf{Dec}_k(c_1), c_2) = 1$ and $\perp$ otherwise.

Here, Mac and Vrfy are deterministic algorithms that are part of a secure MAC scheme that is compatible with Gen.

$\Pi^3 := (\mathsf{Gen}, \mathsf{Enc}^3, \mathsf{Dec}^3)$:

- $\mathsf{Enc}^3_k(m) := \mathsf{Enc}_k(m \oplus 1^n)$,
- $\mathsf{Dec}^3_k(c) := 1^n$ if $\mathsf{Dec}_k(c) = \perp$, $\mathsf{Dec}^2_k(c) := \mathsf{Dec}_k(c) \oplus 1^n$ otherwise.

Exercise 8 Let $F : \mathcal{K} \times \{0,1\}^n \longmapsto \{0,1\}^n$ be a PRF. Consider the following authenticated encryption scheme $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ as follow:

- Gen: pick a key uniformly at random in $\mathcal{K}$;
- Enc on input m and k:
  - Parse m in l block $m_1, ..., m_l$ with $|m_1| = ... = |m_l| = n$
  - Pick r uniformly at random in $\{0,1\}^{\frac{n}{2}}$
  - For $i = 1, ..., l$:
    $c_i = F_k(r||i) \oplus m_i$
  - $c_{l+1} = F_k(r||l+1) \oplus \left(\bigoplus_{i=1}^{n} m_i \right)$
  - Return (r, c) with $c = (c_1, ..., c_l, c_{l+1})$.
- Dec consequently (checks correctness of c_{l+1}).

a) Is Π unforgeable?

b) Is Π CCA-secure?

Exercise 9 (Fixed-length MAC.) Consider the fixed-length MAC $\Pi := \langle \mathsf{Gen}, \mathsf{Mac}, \mathsf{Vrfy} \rangle$ defined as follows:

- Gen: choose random $k \leftarrow \{0,1\}^n$
- Mac: on input $m, k \in \{0,1\}^n$, output $t := F_k(m)$
- Vrfy: on input $k, m, t \in \{0,1\}^n$ output 1 iff $t = F_k(m)$

Prove that, if F is a PRF, Π is existentially unforgeable under an adaptive chosen-message attack.

Exercise 10 (Blue-ray security) The movie industry wants to protect digital content distributed on DVD's. We study one possible approach. Suppose there are at most a total of n DVD players in the world (e.g. $n = 2^{32}$). We view these n players as the leaves of a binary tree of height $\log_2 n$. Each node ν_j in this binary tree contains an AES key K_j such that $\mathrm{Enc}_{K_j} : \{0,1\}^l \to \{0,1\}^l$ is assumed to be a *secure* encryption. These keys are kept secret from consumers and are fixed for all time. At manufacturing time each DVD player is assigned a serial number $i \in [0, n-1]$. Consider the set S_i of $\log_2(n) + 1$ nodes along the path from the root to leaf number i in the binary tree. The manufacturer of the DVD player embeds in player number i the $\log_2(n) + 1$ keys associated with the nodes in S_i. In this way each DVD player ships with $\log_2(n) + 1$ keys embedded in it (these keys are supposedly inaccessible to consumers).

1. Since all DVD players have the key *root* (noted K_{root}), find a way to protect the content $M \in \{0,1\}^l$ of a DVD such that all players can decrypt the movie (and then read it).

2. Now suppose that a hacker has been able to extract the key K_{root} embedded in his DVD player and has published it on the Internet. Show how the movie industry can encrypt the contents of a new DVD $M \in \{0,1\}^l$ such that only the owners of a DVD player can read it. Note that the movie industry does not want to produce several encryptions of the same content M *i.e.* there will be a single manner to protect the DVD.

3. Suppose the $\log_2(n) + 1$ keys embedded in DVD player number r are exposed by hackers and published on the Internet. Show that when the movie industry is about to distribute a new DVD movie they can encrypt the contents of the DVD using a ciphertext of size $\ell_{\mathrm{M}} + \ell_{\mathrm{key}} \cdot \log_2 n$ where ℓ_{M} is the length of content M and ℓ_{key} is the length of each key, so that all DVD players can decrypt the movie except for player number r. In effect, the movie industry disables player number r.