

Cryptography: Assignment 4

Topics: Message Authentication Codes, Authenticated Encryption

- Let F be a secure PRF defined over $(\{0, 1\}^n, \{0, 1\}^n, \{0, 1\}^n)$. Consider the following MAC construction. On input a key $K \in \{0, 1\}^n$ and a message $M \in (\{0, 1\}^{n/6})^+$, parse M into ℓ blocks $M_1, \dots, M_\ell$, each of length $n/6$ bits and generate the tag T as follows:

$$\begin{aligned} R &\leftarrow_{\$} \{0, 1\}^{n/2} \\ T_i &\leftarrow F_K(M_i \| \langle \ell \rangle \| \langle i \rangle \| R) \\ T &\leftarrow (R, (T_1 \oplus \dots \oplus T_\ell)) \end{aligned}$$

- What is the maximum possible message length (in bits) supported by the MAC construction?
- Write down the corresponding verification algorithm.
- Prove that the construction achieves CMA-EUF security. Explicitly calculate the advantage of an adversary trying to mount existential forgery attack under chosen message attack model.

Note: We use the notation $\langle x \rangle$ to denote the encoding of x as strings of length $n/6$ bits.

- Let F be a pseudorandom function. Show that each of the following MACs is insecure, even if used to authenticate fixed-length messages. (In each case Gen outputs a uniform $k \in \{0, 1\}^n$. Let $\langle i \rangle$ denote an $n/2$ -bit encoding of the integer i .)
 - To authenticate a message $M = M_1 \| M_2 \| \dots \| M_\ell$, where $M_i \in \{0, 1\}^n$, compute the tag $t := F_k(M_1) \oplus \dots \oplus F_k(M_\ell)$.
 - To authenticate a message $M = M_1 \| M_2 \| \dots \| M_\ell$, where $M_i \in \{0, 1\}^{n/2}$, compute the tag $t := F_K(\langle 1 \rangle \| M_1) \oplus \dots \oplus F_K(\langle \ell \rangle \| M_\ell)$.
 - To authenticate a message $M = M_1 \| M_2 \| \dots \| M_\ell$, where $M_i \in \{0, 1\}^n$, choose uniform $r \leftarrow \{0, 1\}^n$ and compute $t := F_K(r) \oplus F_K(M_1) \oplus \dots \oplus F_K(M_\ell)$, and let the tag be (r, t) .
- Suppose you are given two MAC systems $\text{MAC}_1 = (\text{KG}_1, \text{TG}_1, \text{Vrfy}_1)$ and $\text{MAC}_2 = (\text{KG}_2, \text{TG}_2, \text{Vrfy}_2)$. Define $\text{MAC} = (\text{KG}, \text{TG}, \text{Vrfy})$, where $\text{KG}(1^n) = (\text{KG}_1(1^n), \text{KG}_2(1^n))$,

$$\text{TG}((K_1, K_2), m) = \text{TG}_1(K_1, m) \| \text{TG}_2(K_2, m).$$

Vrfy is defined in the obvious way: on input $((k_1, k_2), m, (t_1, t_2))$,

V accepts iff both $V_1(k_1, m, t_1)$ and $V_2(k_2, m, t_2)$ accept.

Show that MAC is secure if either MAC_1 or MAC_2 is secure.

4. Let $\Pi = (\text{KG}, \text{TG}, \text{Vrfy})$ be a EUF-CMA secure message authentication code. Consider the following message authentication code $\Pi^* = (\text{KG}, \text{TG}^*, \text{Vrfy}^*)$ as given below:

$$\text{TG}^*(K, M) := 0 \parallel \text{TG}(K, M), \quad \text{Vrfy}^*(K, b \parallel C) := \text{Vrfy}(K, C).$$

Show that Π^* is EUF-CMA secure but not SUF-CMA secure.

5. Let F be a strong pseudorandom permutation, and define the following fixed-length encryption scheme: On input a message $m \in \{0, 1\}^{n/2}$ and key $k \in \{0, 1\}^n$, algorithm Enc chooses a uniform $r \in \{0, 1\}^{n/2}$ and computes $c := F_k(m \parallel r)$. Prove that this scheme is CCA-secure, but not an authenticated encryption scheme.
6. Let $(\text{KG}_E, \text{Enc}, \text{Dec})$ be a IND-CPA secure randomized encryption scheme. Consider the encryption scheme $(\text{KG}_E, \text{Enc}^*, \text{Dec}^*)$ as given below:

$$\text{Enc}^*(K, M) := 0 \parallel \text{Enc}(K, M), \quad \text{Dec}^*(K, b \parallel C) := \text{Dec}(K, C).$$

- (a) Prove that the encryption scheme $(\text{KG}_E, \text{Enc}^*, \text{Dec}^*)$ is CPA-secure.
- (b) Prove that MAC-then-Encryption is not generically secure. [Hint: Can you exploit some weakness of the above encryption scheme?]
7. Let $(\text{KG}_E, \text{Enc}, \text{Dec})$ be a IND-CPA secure randomized encryption scheme. Let $(\text{KG}_M, \text{TG}, \text{Vrfy})$ be a EUF-CMA secure MAC. Consider the following Encrypt-then-MAC type derived cipher $\Pi := (\text{KG}, \text{AE}, \text{VD})$, where

$$\text{AE}_{K_1, K_2}(m) := \{(r, c) \leftarrow \text{Enc}_{K_1}(m), t \leftarrow \text{TG}_{K_2}(c), \text{return } (r, c, t)\}.$$

- (a) Prove that the authenticated encryption is not secure.
- (b) How can you justify your answer? Remember that we know the following result: “Encrypt-then-MAC achieves secure AE given that the underlying Encryption and MAC schemes are secure.”