CS276: Cryptography October 6, 2015

Lecture 12

Instructor: Alessandro Chiesa *Scribe: Tongzhou Wang*

1 CCA2 from Combining Encryption and Authentication

Theorem (has a bug)**.** *CPA*(E, D) + *MAC*$(T, V) \to$ *CCA2*(E', D')

Proof. We use a construction called "encrypt then authenticate".

$$E'(1^k, sk, m) := \left[\begin{array}{ll} 1. & c \leftarrow E(1^k, sk_1, m) \\ 2. & t \leftarrow T(1^k, sk_2, c) \\ 3. & \text{output } (c, t) \end{array}\right.$$

$$D'(1^k, sk, c') := \left[\begin{array}{ll} 1. & c, t \leftarrow c' \\ 2. & \text{check if } V(1^k, sk_2, c, t) = 1 \\ 3. & \text{if so, output } D(1^k, sk_1, c) \\ 4. & \text{otherwise, output } \perp \end{array}\right.$$

The idea here is to quantify over all $\{m_k^{(0)}\}_k$ and $\{m_k^{(1)}\}_k$, so that if they were chosen by A, we are still guaranteed security.

Suppose $\exists$ ppt $A, \{m_k^{(0)}\}, \{m_k^{(1)}\}$ s.t.

$$\left| \mathbb{P}\left[A^{E'(1^k, sk, \cdot), D'(1^k, sk, \cdot)}(\overbrace{E'(1^k, sk, m_k^{(0)})}^{\text{not}}) = 1 \right] - \mathbb{P}\left[A^{E'(1^k, sk, \cdot), D'(1^k, sk, \cdot)}(\overbrace{E'(1^k, sk, m_k^{(1)})}^{\text{not}}) = 1 \right] \right|$$

is not $negl(k)$.

WLOG, assume that A does not query D' on cipher text received from E'.

Construct B to attack (E, D),

$$B^{\mathcal{O}=E(sk,\cdot)}(c) := \left[\begin{array}{l} 1.\ \ \text{sample } sk_2 \text{ for } (T, V) \text{ at random} \\ 2.\ \ t \leftarrow T(1^k, sk_2, c) \\ 3.\ \ \text{output } A^{\mathcal{O}_1, \mathcal{O}_2}(c, t), \text{ where} \\ \qquad \mathcal{O}_1(m_i) := \left[\begin{array}{ll} 1. & c_i \leftarrow \mathcal{O}(m_i) \\ 2. & t_i \leftarrow T(sk_2, c_i) \\ 3. & \text{output } (c_i, t_i) \end{array}\right. \\ \qquad \mathcal{O}_2(c_i) := \perp \end{array}\right.$$

For $b \in \{0, 1\}$, let b represent $E'(m_b)$. We have

$$\begin{aligned} \left| \mathbb{P}\left[A^{E',D'}(0) = 1\right] - \mathbb{P}\left[A^{E',D'}(1) = 1\right] \right| \leq & \left| \mathbb{P}\left[A^{E',D'}(0) = 1\right] - \mathbb{P}\left[B^{E}(0) = 1\right] \right| \\ & + \left| \mathbb{P}\left[B^{E}(0) = 1\right] - \mathbb{P}\left[B^{E}(1) = 1\right] \right| \\ & + \left| \mathbb{P}\left[B^{E}(1) = 1\right] - \mathbb{P}\left[A^{E',D'}(1) = 1\right] \right| \end{aligned}$$

1. If $\left|\mathbb{P}\left[B^E(0)=1\right]-\mathbb{P}\left[B^E(1)=1\right]\right|$ is non-negligible, B breaks CPA. Contradiction.

2. If $\left|\mathbb{P}\left[A^{E',D'}(b)=1\right]-\mathbb{P}\left[B^E(b)=1\right]\right|$ is non-negligible for a $b\in\{0,1\}$, then A must call D' and get an output other than $\perp$. Moreover, the query isn't from E'. Construct C to attack (T,V),

$$C^{\mathcal{O}=T(sk,\cdot)}(1^k) := \left[\begin{array}{l} 1.\ \text{pick } j \text{ at random} \\ 2.\ \text{sample } sk_1 \text{ for (E, D) at random} \\ 3.\ c \leftarrow E(1^k, sk_1, m_k^{(b)}) \\ 4.\ t \leftarrow \mathcal{O}(c) \\ 5.\ c' \leftarrow (c,t) \\ 6.\ \text{run } A^{\mathcal{O}_1,\mathcal{O}_2}(c',t), \text{ where} \\ \qquad \mathcal{O}_1(m_i) := \left[\begin{array}{l} 1.\ c_i \leftarrow E(1^k, sk, m_i) \\ 2.\ t_i \leftarrow \mathcal{O}(c_i) \\ 3.\ \text{output } (c_i,t_i) \end{array}\right. \\ \qquad \mathcal{O}_2(c_i') := \perp \\ \qquad \text{if } i=j, \text{ stop simulation and output } c_i'=(c_i,t_i) \end{array}\right.$$

□

Observation. Problem with the construction: attacks can modify parts of the tag and still have a valid tag (e.g. random garbage at the beginning of the tag), but D as an oracle can decrypt if for the attacker. Specifically, C can query (m,t) and output (m,t'), and thus fails to attack (T,V).

Theorem (Fix the bug)**.** *CPA*(E,D) + *MAC with unique tags*$(T,V) \implies$ *CCA2*(E',D')

Definition (MAC with unique tags)**.** A MAC (T,V) has unique tags if

$$\forall sk, \forall m, \exists! t \text{ s.t. } V(1^k, sk, m, t)=1$$

Remark. To make a MAC with unique tags, we can

1. make T deterministic: randomness $\leftarrow$ PRF $f_{sk}(m)$, and

2. make V canonical: use T to verify.

2 Other Forms of CPA+MAC

1. **Construction:** "Encrypt and authenticate"

$$E := \left[\begin{array}{l} 1.\ c \leftarrow E(1^k, sk_1, m) \\ 2.\ t \leftarrow T(1^k, sk_2, m) \\ 3.\ \text{output } (c,t) \end{array}\right.$$

Problem: (T,V), as a MAC, can be secure even if

(a) T is deterministic, and/or
(b) T includes message in output.

So this construction can be completely insecure.

2. **Construction:** "Authenticate then encrypt"

$$E := \left[\begin{array}{l} 1.\ \ t \leftarrow T(1^k, sk_2, m) \\ 2.\ \ c \leftarrow E(1^k, sk_1, t) \\ 3.\ \ \text{output } c \end{array}\right.$$

Problem: This construction is at least CPA secure, but not CCA2 secure. e.g. E puts garbage bits at beginning of output.

3 Collision Resistant Function (CRF)

An efficient function for which collisions are hard to find.

Definition. $\mathcal{F} := \{F_k\}_k$ is CRF if $\forall$ ppt A,

$$\mathbb{P}\left[\begin{array}{c} x \neq x' \\ f(x) = f(x') \end{array} \middle| \begin{array}{c} f \leftarrow F_k \\ (x, x') \leftarrow A(1^k, f) \end{array}\right] \text{ is } negl(k)$$

Observation. Here we hand to the adversary the function description rather than only oracle access.

Remark. Any injection is a CRF! CRFs are more interesting when f is length decreasing.

Lemma. *length decreasing CRF $\implies$ OWF*

Intuition. Suppose not. We can have

$$\exists A \text{ s.t. } \mathbb{P}\left[A(f(y)) \in f^{-1}(f(y)) \setminus \{y\}\right] > negl(k)$$

□

3.1 Attack CRF

For CRF $f : \{0,1\}^{n(k)} \to \{0,1\}^k$, $n(k) > k$,

3.1.1 Enumeration Attack

$2^k + 1$ trials at most. Attack takes time $O(Time(f) \times 2^k)$.

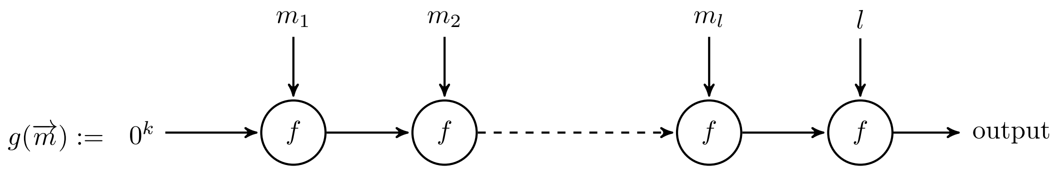
3.1.2 Birthday Attack

Pick $x_1, x_2, \ldots, x_m$ at random and check for collisions across all pairs.

$$\mathbb{P}\left[collision\right] \geq 1 - e^{-\frac{m^2}{2^{k+1}}}$$

3.2 Merkle-Damgård Transform

Given CRF $\mathcal{F} = \{F_k\}_k$ with $f : \{0,1\}^{2k} \to \{0,1\}^k$, construct CRF $\mathcal{G} = \{G_k\}_k$ with $g : \{0,1\}^* \to \{0,1\}^k$.



Proof. Suppose $\exists$ ppt A that finds collision for $\mathcal{G}$ with non-negligible probability δ.

Let $\overrightarrow{m}$ and $\overrightarrow{m}'$ be the output of A s.t. $g(\overrightarrow{m}) = g(\overrightarrow{m}')$ but $\overrightarrow{m} \neq \overrightarrow{m}'$.

If

1. $|\overrightarrow{m}| \neq |\overrightarrow{m}'|$, $l \neq l'$, then collision in last block.
2. $l = l'$, then $\exists i$ s.t. $m_i \neq m_i'$ and $(m_{i+1}, \ldots, m_l) = (m_{i+1}', \ldots, m_{l'})$, collision somewhere earlier.

Construct B to attack $\mathcal{F}$,

$$B(1^k, f) := \left[\begin{array}{ll} 1. & \text{construct } g \text{ from } f \\ 2. & \overrightarrow{m}, \overrightarrow{m}' \leftarrow A(1^k, g) \\ 3. & \text{compute } g(\overrightarrow{m}) \text{ and } g(\overrightarrow{m}') \text{ to find the collision and output it} \end{array}\right.$$

$\square$