Cryptography

Lecture 12

Announcements

- HW5 due 3/13
- Midterm Upcoming on 3/15
 - Review sheet will be posted on course webpage by tonight
 - Solutions and Cheat Sheet posted soon on Canvas

Agenda

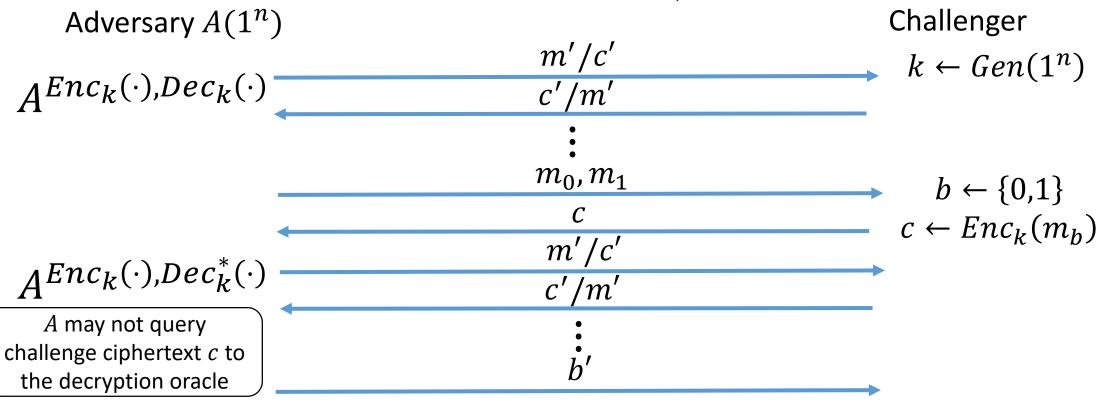
- Last time:
 - Domain Extension for MACs (K/L 4.4) and Class
 Exercise solutions
 - CCA security (K/L 3.7)
 - Unforgeability for Encryption (K/L 4.5)
- This time:
 - Authenticated Encryption (K/L 4.5)
 - Collision-Resistant Hash Functions (K/L 5.1)
 - Hash-and-Mac
 - Domain extension for CRHF

Chosen Ciphertext Security

CCA Security

Consider a private-key encryption scheme $\Pi = (Gen, Enc, Dec)$, any adversary A, and any value n for the security parameter.

Experiment $PrivK_{A,\Pi}^{cca}(n)$



 $PrivK_{A,\Pi}^{cca}(n) = 1$ if b' = b and $PrivK_{A,\Pi}^{cca}(n) = 0$ if $b' \neq b$.

CCA Security

The CCA Indistinguishability Experiment $PrivK^{cca}_{A,\Pi}(n)$:

1. A key k is generated by running $Gen(1^n)$.

- 2. The adversary A is given input 1^n and oracle access to $Enc_k(\cdot)$ and $Dec_k(\cdot)$, and outputs a pair of messages m_0, m_1 of the same length.
- 3. A random bit $b \leftarrow \{0,1\}$ is chosen, and then a challenge ciphertext $c \leftarrow Enc_k(m_b)$ is computed and given to A.
- 4. The adversary A continues to have oracle access to $Enc_k(\cdot)$ and $Dec_k(\cdot)$, but is not allowed to query the latter on the challenge ciphertext itself. Eventually, A outputs a bit b'.
- 5. The output of the experiment is defined to be 1 if b' = b, and 0 otherwise.

CCA Security

A private-key encryption scheme $\Pi = (Gen, Enc, Dec)$ has indistinguishable encryptions under a chosen-ciphertext attack if for all ppt adversaries A there exists a negligible function *negl* such that

$$\Pr\left[\operatorname{PrivK^{cca}}_{A,\Pi}(n)=1\right] \leq \frac{1}{2} + \operatorname{negl}(n),$$

where the probability is taken over the random coins used by A, as well as the random coins used in the experiment.

Authenticated Encryption

The unforgeable encryption experiment (simi) for MAC gave)

- 1. Run $Gen(1^n)$ to obtain key k.
- 2. The adversary A is given input 1^n and access to an encryption oracle $Enc_k(\cdot)$. The adversary outputs a ciphertext c. (and to forget)
- 3. Let $m \coloneqq Dec_k(c)$, and let Q denote the set of all queries that A asked its encryption oracle. The output of the experiment is 1 if and only if $(1) \ m \neq D$ and $(2) \ m \notin Q$.

" \bot" "\perp"

for for Enc, when dec we might get "1"

Authenticated Encryption

Definition: A private-key encryption scheme Π is <u>unforgeable</u> if for all ppt adversaries A, there is a negligible function neg such that:

 $\Pr[EncForge_{A,\Pi}(n) = 1] \leq neg(n).$

Definition: A private-key encryption scheme is an authenticated encryption scheme if it is CCAsecure and unforgeable.



Generic Constructions



Always choose independent keys for Enc, and Mac

Encryption and message authentication are computed independently in parallel.

Encrypt-and-authenticate

Encryption and message authentication are computed independently in parallel.

$$\begin{array}{c} c \leftarrow Enc_{k_E}(m) \quad t \leftarrow Mac_{k_M}(m) \\ \langle c, t \rangle \end{array}$$

Is this secure? NO! Tag can leak info on m



Authenticate-then-encrypt

Here a MAC tag t is first computed, and then the message and tag are encrypted together.

 $t \leftarrow Mac_{k_M}(m)$ $c \leftarrow Enc_{k_E}(m||t)$ Exis. Unfor c is sent Any CPA-secure the presence dCMA afact.

Is this secure?

Authenticate-then-encrypt

Here a MAC tag t is first computed, and then the message and tag are encrypted together.

 $t \leftarrow Mac_{k_M}(m)$ $c \leftarrow Enc_{k_E}(m||t)$

c is sent

Is this secure? NO! Encryption scheme may not be CCA-secure.

Encrypt-then-authenticate

The message m is first encrypted and then a MAC tag is computed over the result

$$c \leftarrow Enc_{k_E}(m) \quad t \leftarrow Mac_{k_M}(c)$$
$$\langle c, t \rangle$$

Encrypt-then-authenticate

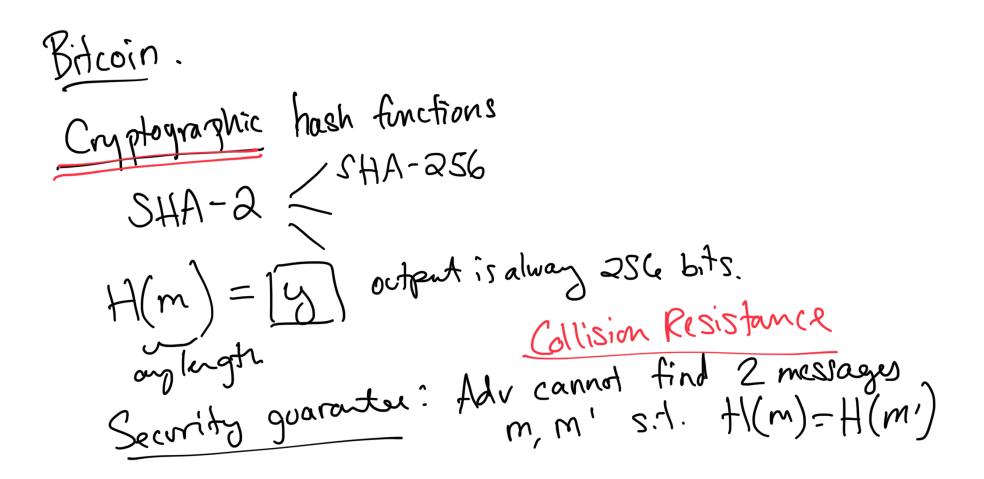
The message m is first encrypted and then a MAC tag is computed over the result

$$c \leftarrow Enc_{k_E}(m) \quad t \leftarrow Mac_{k_M}(c)$$
$$\langle c, t \rangle$$

Is this secure? YES! As long as the MAC is strongly secure.

Inorden to get CCA security

Collision Resistant Hashing



Collision Resistant Hashing

Definition: A hash function (with output length ℓ) is a pair of ppt algorithms (*Gen*, *H*) satisfying the following:

- *Gen* takes as input a security parameter 1ⁿ and outputs a key s. We assume that 1ⁿ is implicit in s.
 H takes as input a key s and a string x ∈ {0,1}* and
- *H* takes as input a key *s* and a string $x \in \{0,1\}^*$ and outputs a string $H^{\mathfrak{S}}(x) \in \{0,1\}^{\ell(n)}$.

256

512

If H^s is defined only for inputs $x \in \{0,1\}^{\ell'(n)}$ and $\ell'(n) > \ell(n)$ then we say that (Gen, H) is a fixed-length hash function for inputs of length ℓ' . In this case, we also call H a compression function.

The collision-finding experiment

$Hashcoll_{A,\Pi}(n)$:

- 1. A key s is generated by running $Gen(1^n)$.
- 2. The adversary A is given s and outputs $\underline{x, x'}$. (If Π is a fixed-length hash function for inputs of length $\ell'(n)$, then we require $x, x' \in \{0,1\}^{\ell'(n)}$.)
- 3. The output of the experiment is defined to be 1 if and only if $x \neq x'$ and $H^s(x) = H^s(x')$. In such a case we say that A has found a collision.

Given
$$H(x) = y$$
 find som pre-image.
(x) s.t. $H(x') = y$.

Security Definition

Definition: A hash function $\Pi = (Gen, H)$ is collision resistant if for all ppt adversaries Athere is a negligible function neg such that $\Pr[Hashcoll_{A,\Pi}(n) = 1] \leq neg(n).$

Message Authentication Using Hash Functions

Recap'. Mac fixed-lungth messages.

$$m \in 90,13^{n}$$

 $Mac_{\kappa}(m) = F_{\kappa}(m)$
Hash-and-Hac'. "Domain extension" for Macs.
Hash-and-Hac for fixed-lungth msgs \longrightarrow Mac for arbit length
 $F_{\kappa}(H(m)) = H$.

Hash-and-Mac Construction

Let $\Pi = (Mac, Vrfy)$ be a MAC for messages of length $\ell(n)$, and let $\Pi_H = (Gen_H, H)$ be a hash function with output length $\ell(n)$. Construct a MAC

 $\Pi' = (Gen', Mac', Vrfy')$ for arbitrary-length messages as follows:

- Gen': on input 1^n , choose uniform $k \in \{0,1\}^n$ and run $Gen_H(1^n)$ to obtain s. The key is $k' \coloneqq \langle k, s \rangle$.
- Mac': on input a key $\langle k, s \rangle$ and a message $m \in \{0,1\}^*$, output $t \leftarrow Mac_k(H^s(m))$.
- Vrfy': on input a key $\langle k, s \rangle$, a message $m \in \{0,1\}^*$, and a MAC tag t, output 1 if and only if $Vrfy_k(H^s(m), t) = 1$.

Security of Hash-and-MAC

Theorem: If Π is a secure MAC for messages of length ℓ and Π_H is collision resistant, then the construction above is a secure MAC for arbitrary-length messages.

Proof Intuition

Let Q be the set of messages m queried by adversary A.

Assume A manages to forge a tag for a message $m^* \notin Q$.

There are two cases to consider:

1. $H^{s}(m^{*}) = H^{s}(m)$ for some message $m \in Q$. Then A breaks collision resistance of H^{s} . 2. $(H^{s}(m^{*})) \neq H^{s}(m)$ for all messages $m \in Q$. Then A forges a valid tag with respect to MAC II.

 $H(m^{*}), -t$ cn Mack. M_{1}, M_{2}, M_{3} $H(m_{1}), H(m_{2}), H(m_{3})$ Queries mode to Mack(H(.))