CCA-Security and Authenticated Encryption

Chosen-Ciphertext Attacks and CCA-Security

- Consider a scenario
  - A sender encrypts a message m and then transmits the resulting ciphertext c.
  - An attacker generates another ciphertext c^0 that is received by the other party.
  - This receiver will then decrypt c^0 to obtain a message m^0.
  - If $m' \neq m$ Is a violation of integrity
  - If the attacker learns partial information about m^0—say, from subsequent behavior of the receiver—might that reveal information about the original message m
- Type of attack, in which an adversary causes a receiver to decrypt ciphertexts that the adversary generates, is called a chosen-ciphertext attack.

Defining CCA-Security

- Define two things: the assumed abilities of the attacker, and what constitutes a successful attack.
- For the second one : give the attacker a challenge ciphertext c that is generated by encrypting one of two possible messages m0,m1 and consider the scheme to be broken if the attacker can determine which message was encrypted with probability significantly better than 1/2.
- Attacker's capabilities : the ability not only to obtain the encryption of messages of its choice -to obtain the decryption of ciphertexts of its choice
- Give the adversary access to a decryption oracle $dec_k(\cdot)$ in addition to an encryption oracle $enc_k(\cdot)$.

Private-key encryption scheme - indistinguishable for CCA

For any private-key encryption scheme Π = (Gen,Enc,Dec), adversary A, and value n for the security parameter

The CCA indistinguishability experiment $\mathsf{PrivK}^{\mathsf{cca}}_{\mathcal{A},\Pi}(n)$**:**

1. *A key k is generated by running* $\mathsf{Gen}(1^n)$.
2. $\mathcal{A}$ *is given input* 1^n *and oracle access to* $\mathsf{Enc}_k(\cdot)$ *and* $\mathsf{Dec}_k(\cdot)$. *It outputs a pair of equal-length messages* m_0, m_1.
3. *A uniform bit* $b \in \{0,1\}$ *is chosen, and then a* challenge ciphertext $c \leftarrow \mathsf{Enc}_k(m_b)$ *is computed and given to* $\mathcal{A}$.
4. *The adversary* $\mathcal{A}$ *continues to have oracle access to* $\mathsf{Enc}_k(\cdot)$ *and* $\mathsf{Dec}_k(\cdot)$, *but is not allowed to query the latter on the challenge ciphertext itself. Eventually,* $\mathcal{A}$ *outputs a bit* b'.
5. *The output of the experiment is 1 if* $b' = b$, *and 0 otherwise. If the output of the experiment is 1, we say that* $\mathcal{A}$ succeeds.

Private-key encryption scheme - indistinguishable for CCA

DEFINITION 5.1 A private-key encryption scheme Π *has* indistinguishable encryptions under a chosen-ciphertext attack, *or is* CCA-secure, *if for all probabilistic polynomial-time adversaries* A *there is a negligible function* negl *such that:*

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

where the probability is taken over all randomness used in the experiment.

Authenticated Encryption

- The aim of authenticated encryption, is to achieve both goals: secrecy (using encryption) and integrity (using message authentication codes) simultaneously
- Secrecy notion: CCA-security
- Integrity notion: unforgeability
  - Adversary cannot generate ciphertext that decrypts to a previously unencrypted message

Defining Authenticated Encryption

Consider the following experiment defined for a private-key encryption scheme $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$, adversary $\mathcal{A}$, and value n for the security parameter:

The unforgeable encryption experiment $\mathsf{Enc\text{-}Forge}_{\mathcal{A},\Pi}(n)$**:**

1. *A key k is generated by running* $\mathsf{Gen}(1^n)$.
2. *The adversary $\mathcal{A}$ is given input 1^n and access to an encryption oracle* $\mathsf{Enc}_k(\cdot)$. *The adversary eventually outputs a ciphertext c. Let $m := \mathsf{Dec}_k(c)$ and let $\mathcal{Q}$ denote the set of all queries that $\mathcal{A}$ submitted to its oracle.*
3. $\mathcal{A}$ succeeds *if and only if (1) $m \neq \perp$ and (2) $m \notin \mathcal{Q}$. In that case the output of the experiment is defined to be* 1.

Defining Authenticated Encryption

DEFINITION 5.2 *A private-key encryption scheme* Π *is* unforgeable *if for all probabilistic polynomial-time adversaries* $\mathcal{A}$, *there is a negligible function* negl *such that:*

$$\Pr[\mathsf{Enc\text{-}Forge}_{\mathcal{A},\Pi}(n) = 1] \leq \mathsf{negl}(n).$$

DEFINITION 5.3 *A private-key encryption scheme is an* authenticated encryption (AE) scheme *if it is CCA-secure and unforgeable.*

Authenticated Encryption Schemes

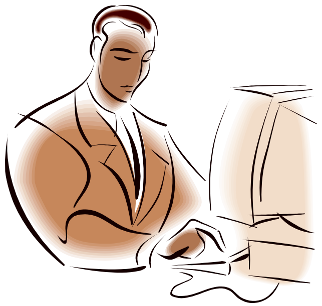
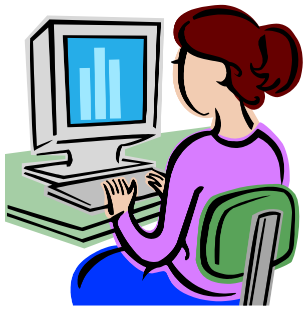
- Let Π_E = (Enc,Dec) be a CPA-secure encryption scheme and let Π_M = (Mac,Vrfy) denote a strongly secure MAC
- There are three natural approaches to combining encryption and message authentication using independent keys k_E and k_M for Π_E and Π_M, respectively:
- Generic constructions
  - Encrypt and authenticate $\quad c \leftarrow \mathsf{Enc}_{k_E}(m) \quad \text{and} \quad t \leftarrow \mathsf{Mac}_{k_M}(m).$
  - Authenticate then encrypt $\quad t \leftarrow \mathsf{Mac}_{k_M}(m) \quad \text{and} \quad c \leftarrow \mathsf{Enc}_{k_E}(m\|t).$
  - Encrypt then authenticate $\quad c \leftarrow \mathsf{Enc}_{k_E}(m) \quad \text{and} \quad t \leftarrow \mathsf{Mac}_{k_M}(c).$

Generic constructions

- Generically combine an encryption scheme and a MAC
  - Useful when these are already available in some library

- Goal: the combination should be an authenticated encryption scheme when instantiated with *any* CPA-secure encryption scheme and *any* secure MAC

Encrypt and authenticate

k1, k2  $\xrightarrow{c,\ t}$  k1, k2

m

$c \leftarrow \mathrm{Enc}_{k1}(m)$

$t = \mathrm{Mac}_{k2}(m)$

$m = \mathrm{Dec}_{k1}(c)$

$\mathrm{Vrfy}_{k2}(m, t) = 1?$

Problems

- The tag t might leak information about m!
  - Nothing in the definition of security for a MAC implies that it hides information about m
  - So the combination may not even be EAV-secure
- If the MAC is deterministic (as is CBC-MAC), then the tag leaks whether the same message is encrypted twice
  - I.e., the combination will not be CPA-secure