Modern Cryptography

Indistinguishability under CCA

Sep 12, 2025

Dr Shashank Singh

Table of Contents

CCA Security

Consider the following experiment:

$\mathrm{PrivK}^{\mathrm{cca}}_{\mathscr{A},\Pi}(n)$:

1. $k \leftarrow \mathrm{GEN}(n)$
2. $\mathscr{A}$ is given $\Pi(n)$, and oracles $\mathrm{ENC}_k(\cdot)$, $\mathrm{DEC}_k(\cdot)$. The adversary $\mathscr{A}$ produces $m_0, m_1 \in \{0,1\}^\star$ with $|m_0| = |m_1|$.
3. $b \xleftarrow{\$} \{0,1\}$ and $c \leftarrow \mathrm{ENC}(k, m_b)$ is given to the adversary $\mathscr{A}$.
4. $\mathscr{A}$ is not allowed to query c to the oracle $\mathrm{DEC}_k(\cdot)$. The adversary $\mathscr{A}$ returns a bit b'.
5. The output of the experiment is $b' \stackrel{?}{=} b$.

♣

Definition 1

A private key encryption scheme $\Pi(n)$ has an indistinguishable encryption under chosen ciphertext attack, or is CCA-secure, if for all PPT adversaries $\mathscr{A}$, there is a negligible function $\varepsilon()$ such that, for all n,

$$\Pr\left[\mathrm{PrivK}^{\mathrm{cca}}_{\mathscr{A},\Pi}(n) = 1\right] \leq \frac{1}{2} + \varepsilon(n). \tag{1}$$

♣

Theorem 2

♡

Definition 3 (Encryption Scheme)

Let F be a pseudorandom function. Define a private-key encryption scheme, $\Pi = (\text{GEN}, \text{ENC}, \text{DEC})$, for messages of length n as follows:

- The key $k \leftarrow \text{GEN}(n)$ is uniform on $\{0,1\}^n$.
- For $m \in \{0,1\}^n$, $\text{ENC}(k, m)$ picks $r \xleftarrow{\$} \{0,1\}^n$ and outputs c, where

$$c := \langle r, F_k(r) \oplus m \rangle$$

- On input $c = \langle r, s \rangle$ and a key k, $\text{DEC}(k, c)$ outputs m, where

$$m := F_k(r) \oplus s$$

♣

Exercise. Show that the above encryption scheme given by Definition 3 is not CCA-secure.

A practical CCA: Padding Oracle Attack

- The CBC mode of operation requires plaintext to be a multiple of the block length. If this is not the case, a suitable padding scheme must be used.

PKCS #5 padding Scheme

Let L be a block length (in bytes). If the message is falling short of b-bytes ($1 \leq b \leq L$), this scheme appends b as one-byte b times to the message.

- For the block length $L = 8$, and message $\texttt{1A} \mid \texttt{2B}$, the padded message would be $\texttt{1A} \mid \texttt{2B} \mid \texttt{06} \mid \texttt{06} \mid \texttt{06} \mid \texttt{06} \mid \texttt{06} \mid \texttt{06}$.
- Even if the message size is a multiple of L bytes, a whole new block of padding is applied in this scheme. This method assists in verifying proper padding and allows for easy unpadding.

♣

- In the CBC decryption, it is easy to detect and remove the PKCS #5 padding. (Why?)
- In implementations, the standard involves removing valid padding and raising an exception for an invalid one. E.g.

  `javax.crypto.BadPaddingException.`
- Such exceptions give adversary $\mathscr{A}$ a tool, that we call a PARTIAL DECRYPTION ORACLE.
- The adversary $\mathscr{A}$ can use it to mount an attack to recover some part of the message comunicated secretly using CBC-MOP.