Indistinguishability under Chosen-Ciphertext Attack (CCA)

Consider the two worlds:

World 0: The adversary is provided the oracle $E_K(LR(\cdot,\cdot,0))$ as well as the oracle $D_K(\cdot)$.

World 1: The adversary is provided the oracle $E_K(LR(\cdot,\cdot,1))$ as well as the oracle $D_K(\cdot)$.

The adversary's goal is to find out which world it is in. There is one easy way to do this: query the lr-encryption oracle on two distinct, equal length messages M_0, M_1 to get back a ciphertext C, and now call the decryption oracle on C. If the message returned by the decryption oracle is M_0 then the adversary is in world 0, and if the message returned by the decryption oracle is M_1 then the adversary is in world 1. We restrict the adversary so that this call to the decryption oracle is not allowed. This restriction is for modelling the situation in which the adversary has access to the decryption equipment for a limited period of time. We imagine that after the adversary has lost access to the decryption equipment, it sees some ciphertexts, and we are capturing the security of these ciphertexts in the face of previous access to the decryption oracle.

Let $SE = (K, E, D)$ be a symmetric encryption scheme, let A (Adversary) be an algorithm that has access to two oracles, and let b be a bit. We consider the following experiment:

Experiment $\mathrm{Exp}_{SE}^{ind-cca-b}(A)$

{ $k' \xleftarrow{\$} K$;

  $b \xleftarrow{\$} A^{E_K(LR(\cdot,\cdot,b)),\, D_K(\cdot)}$;

  if (A queried $D_K(\cdot)$ on a ciphertext previously returned by $E_K(LR(\cdot,\cdot,b))$)

  { return $\perp$; }

  else

  { return b; }

}

The IND-CCA advantage of A is defined as:

$$\mathrm{Adv}_{SE}^{ind-cca}(A) = \Pr[\mathrm{Exp}_{SE}^{ind-cca-1}(A)=1] - \Pr[\mathrm{Exp}_{SE}^{ind-cca-0}(A)=1].$$

We consider an encryption scheme to be "secure against CPA" if a "reasonable" adversary cannot obtain "significant" advantage in distinguishing the cases $b=0$ and $b=1$ given access to the oracles, where reasonable reflects its resource usage.

<u>CCA on CTR$ scheme</u>: Let $F: K \times \{0,1\}^n \to \{0,1\}^l$ be a family of functions and let $SE = (K, E, D)$ be the associated CTR$ symmetric encryption scheme. Then $\mathrm{Adv}_{SE}^{ind-cca}(t, 1, l, 1, n+l) = 1$ for $t = O(n+l)$ plus the time for one application of F. We take advantage of a weakness of CTR$: Suppose $\langle r, C\rangle$ is a ciphertext of some l-bit message M, and we flip bit i of C, resulting in a new ciphertext $\langle r, C'\rangle$. Let M' be the message obtained by decrypting the new ciphertext. Then M' equals M with the i-th bit flipped.

Consider the following adversary:

Adversary $A^{E_K(LR(\cdot,\cdot,b)),\, D_K(\cdot)}$

$\{$ $M_0 \leftarrow 0^l;$

$M_1 \leftarrow 1^l;$

$\langle r, C\rangle \leftarrow E_K(LR(M_0, M_1, b));$

$C' \leftarrow C \oplus 1^l;$

$M \leftarrow D_K(\langle r, C'\rangle);$

if $(M = M_0)$

$\{$ return 1; $\}$

else

$\{$ return 0; $\}$

$\}$

A has time complexity t, makes 1 query to its lr-encryption oracle of length l, makes 1 query to its decryption oracle of length $n+l$.

We can easily show that $\Pr[\mathrm{Exp}_{SE}^{ind-cca-1}(A)=1] = 1$ and

$\Pr[\mathrm{Exp}_{SE}^{ind-cca-0}(A)=1] = 0.$

$\Rightarrow \mathrm{Adv}_{SE}^{ind-cca}(A) = 1-0 = 1 \Rightarrow$ CTR\$ is insecure under CCA.

In world 1, let $\langle r, C\rangle$ denote the ciphertext returned by the lr-encryption oracle. Then

$C = F_K(r+1) \oplus M_1 = F_K(r+1) \oplus 1^l$

$M = D_K(\langle r, C'\rangle) = F_K(r+1) \oplus C' = F_K(r+1) \oplus C \oplus 1^l$

$= F_K(r+1) \oplus (F_K(r+1) \oplus 1^l) \oplus 1^l = 0^l = M_0$

$\Rightarrow \underline{\Pr[\mathrm{Exp}_{SE}^{ind-cca}(A)=1] = 1}$

In world 0, let $\langle r, C \rangle$ denote the ciphertext returned by the lr-encryption oracle. Then

$C = F_K(r+1) \oplus M_0 = F_K(r+1) \oplus 0^l$

$M = D_K(\langle r, C' \rangle) = F_K(r+1) \oplus C' = F_K(r+1) \oplus C \oplus 1^l$

$= F_K(r+1) \oplus (F_K(r+1) \oplus 0^l) \oplus 1^l = 1^l = M_1 \neq M_0$

$\Rightarrow \Pr[\mathrm{Exp}_{SE}^{ind-cca-0}(A) = 1] = 0$

CCA on CBC\$: Let $E: K \times \{0,1\}^n \longrightarrow \{0,1\}^n$ be a block cipher and let $SE = (K, E, D)$ be the corresponding CBC\$ encryption scheme. Then $Adv_{SE}^{ind-cca}(t, 1, n, 1, 2n) = 1$ for $t = O(n)$ plus the time for one application of F.

We take advantage of a weakness of CBC\$: Suppose $\langle IV, C(1) \rangle$ is a ciphertext of some n-bit message M, and we flip bit i of the IV, resulting in a new ciphertext $\langle IV', C(1) \rangle$. Let M' be the message obtained by decrypting the new ciphertext. Then M' equals M with the i-th bit flipped.

Consider the following adversary:

Adversary $A^{E_K(LR(\cdot,\cdot,b)), D_K(\cdot)}$

```
{ M0 <- 0^n;
  M1 <- 1^n;
  <IV, C(1)> <- E_K(LR(M0, M1, b));
  IV' <- IV ⊕ 1^n;
  M <- D_K(<IV', C(1)>);
  if (M = M0)
  { return 1; }
  else
  { return 0; }
}
```

We can easily show that $\Pr[\mathrm{Exp}_{SE}^{ind-cca-1}(A)=1]=1$ and $\Pr[\mathrm{Exp}_{SE}^{ind-cca-0}(A)=1]=0$.

$\Rightarrow \mathrm{Adv}_{SE}^{ind-cca}(t,1,n,1,2n)=1 \Rightarrow$ CBC\$ is insecure under CCA.

In world 1, the lr-encryption oracle returns $\langle IV, C(1)\rangle$ with $C(1)=E_K(IV\oplus M_1)=E_K(IV\oplus 1^n)$

$M=D_K(\langle IV', C(1)\rangle)=E_K^{-1}(C(1))\oplus IV'$

$=E_K^{-1}(E_K(IV\oplus 1^n))\oplus IV'=(IV\oplus 1^n)\oplus IV'$

$=(IV\oplus 1^n)\oplus(IV\oplus 1^n)=0^n=M_0 \Rightarrow \Pr[\mathrm{Exp}_{SE}^{ind-cca-1}(A)=1]=1$.

In world 0, the lr-encryption oracle returns $\langle IV, C(1)\rangle$ with $C(1)=E_K(IV\oplus M_0)=E_K(IV\oplus 0^n)$

$M=D_K(\langle IV', C(1)\rangle)=E_K^{-1}(C(1))\oplus IV'$

$=E_K^{-1}(E_K(IV\oplus 0^n))\oplus IV'=(IV\oplus 0^n)\oplus IV'$

$=(IV\oplus 0^n)\oplus(IV\oplus 1^n)=1^n=M_1\neq M_0$

$\Rightarrow \Pr[\mathrm{Exp}_{SE}^{ind-cca-0}(A)=1]=0$