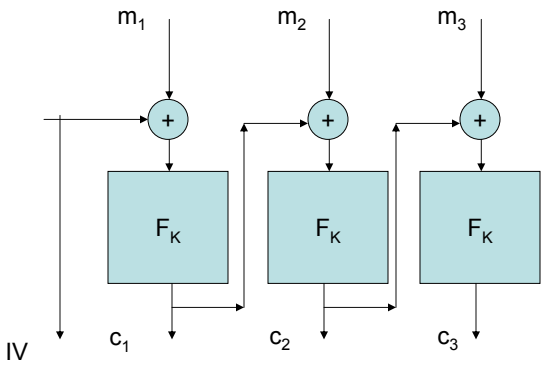
Left or Right Security (LOR)

Debdeep Mukhopadhyay
IIT Kharagpur

Lets look back at CBC…



CBC satisfies message indistinguishability even if IV is fixed for all messages.

But observe that if IV is fixed, messages with same prefixes have ciphertexts also with same prefixes. This is not desirable.

- Thus our notion of message indistinguishability is inadequate.
- So, we introduce a stronger security notion LOR (left or right security model).

Definition

Let $\xi_i(x_0, x_1) = x_i$. E is (t,q,μ,ε)-secure in the left or right sense against CPA if for all A running in time t and making q queries of total length $\leq \mu$,

$|\Pr[A^{E_K \circ \xi_0} = 1] - \Pr[A^{E_K \circ \xi_1} = 1]| \leq \varepsilon$

Finer Points:

1. Oracle provided to the adversary A chooses its left argument always or right argument always.
2. The message lengths are same.

CBC again…

- Consider a CBC without a counter.
- Consider a query to (R,AA) and another to (R,AB), where R is a random block message.
- Note that if the first blocks of the ciphertexts match, $\xi_i=\xi_1$.
- Thus LOR catches a security concern, which Message Indistinguishability cannot. Thus this is a stronger security notion.

Theorem

- LOR security implies security against key recovery attacks.
  - LOR => Key recovery security
  - If there is a key recovery attack, then there is a LOR attack.

Proof

If A^{E_K} is a key-recovery adversary, we construct a LOR adversary, $B^{E_K \circ \xi_i}$ as follows:

1. B runs the oracle $O=\xi_i$, on m=(R,R'), where both are randomly chosen messages. Obtains a ciphertext c.
1. Run A^{E_K}. Suppose it returns k'.
2. Uses k' to decrypt c. Checks where the corresponding plaintext is R. If so, output 1, else 0.

Clearly, if A was correct, B is correct unless ofcourse, R=R'.
The probability of this 2^{-n}, which can be reduced by increasing n.

Theorem

If (E,D) is (t,q,μ,ε')-secure in the LOR sense against CPA,
then $\Pr_{m \leftarrow M}[A^{E_k}(E_k(m)) = m] \le \varepsilon + \frac{1}{|M|}$

Proof:

Define $B^{E_k \circ \xi_i}$ to be an LOR-attacker as follows:
1. Pick R,R' uniformly from M.
2. Let $c=E_k(\xi_i(R,R'))$, that is either encrypt R or R'.
Suppose, $m=A^{E_k}(c)$. If m=R, B returns 1, else 0.

If, $\Pr_{m \leftarrow M}[A^{E_k}(E_k(m)) = m] > \varepsilon + \frac{1}{|M|}$,

$\Pr[B^{E_k \circ \xi_0} = 1] > \varepsilon + \frac{1}{|M|}$ and

$\Pr[B^{E_k \circ \xi_1} = 1] = \Pr[R = R'] + \Pr[R \neq R']\Pr[A \text{ gives a wrong answer}]$

$\le \frac{1}{|M|} + (1 - \frac{1}{|M|})(1 - \varepsilon - \frac{1}{|M|})$

$Thus, |\Pr[B^{E_k \circ \xi_0} = 1] - \Pr[B^{E_k \circ \xi_1} = 1]| > \varepsilon + \frac{1}{|M|} - \frac{1}{|M|} - (1 - \frac{1}{|M|})(1 - \varepsilon - \frac{1}{|M|})$

$= \frac{\varepsilon}{|M|} + (1 - \frac{1}{M})^2$