CSL759: Cryptography and Computer Security

Ragesh Jaiswal

CSE, IIT Delhi

Recap.

CPA Security for Encryption Schemes

- $Left_{SE,A}$
  - Randomly pick key $K \leftarrow \{0,1\}^k$.
  - When A queries message pair (M_0^i, M_1^i) return $E_K(M_0^i)$ to A.
  - Finally A outputs b.
  - Output b.

- $Right_{SE,A}$
  - Randomly pick key $K \leftarrow \{0,1\}^k$.
  - When A queries message pair (M_0^i, M_1^i) return $E_K(M_1^i)$ to A.
  - Finally A outputs b.
  - Output b.

- The IND-CPA advantage of an adversary A is defined as follows:

  $$Adv_{ind-cpa}(A, SE) = \left|\Pr\left[Left_{SE,A} = 1\right] - \Pr\left[Right_{SE,A} = 1\right]\right|$$

- A symmetric encryption scheme $SE = (E, D)$ is called (t, q, ϵ)-ind-cpa secure if for every adversary A that runs in time $\leq t$ and asks $\leq q$ quesries, $Adv_{ind-cpa}(A, SE) \leq \epsilon$.

Pseudorandom Function

- The PRF advantage of an adversary A is defined as follows:
  $Adv_{PRF}(A, F) = \left|\Pr\left[Real_{A,F} = 1\right] - \Pr[Random_A = 1]\right|$
- A function $F: \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ is called (t, q, ϵ)-secure PRF if for every adversary A that runs in time $\leq t$ and asks $\leq q$ queries, $Adv_{PRF}(A, F) \leq \epsilon$.

- $Real_{A,F}$
  - Randomly pick $K \leftarrow \{0,1\}^k$.
  - When A queries with an input $x \in \{0,1\}^n$, return $F_K(x)$.
  - Finally A outputs a bit b.
  - Output b.

- $Random_A$
  - When A queries with an input $x \in \{0,1\}^n$, return a random value from $\{0,1\}^n$.
  - Finally A outputs a bit b.
  - Output b.

The adversary is not allowed to repeat a query.

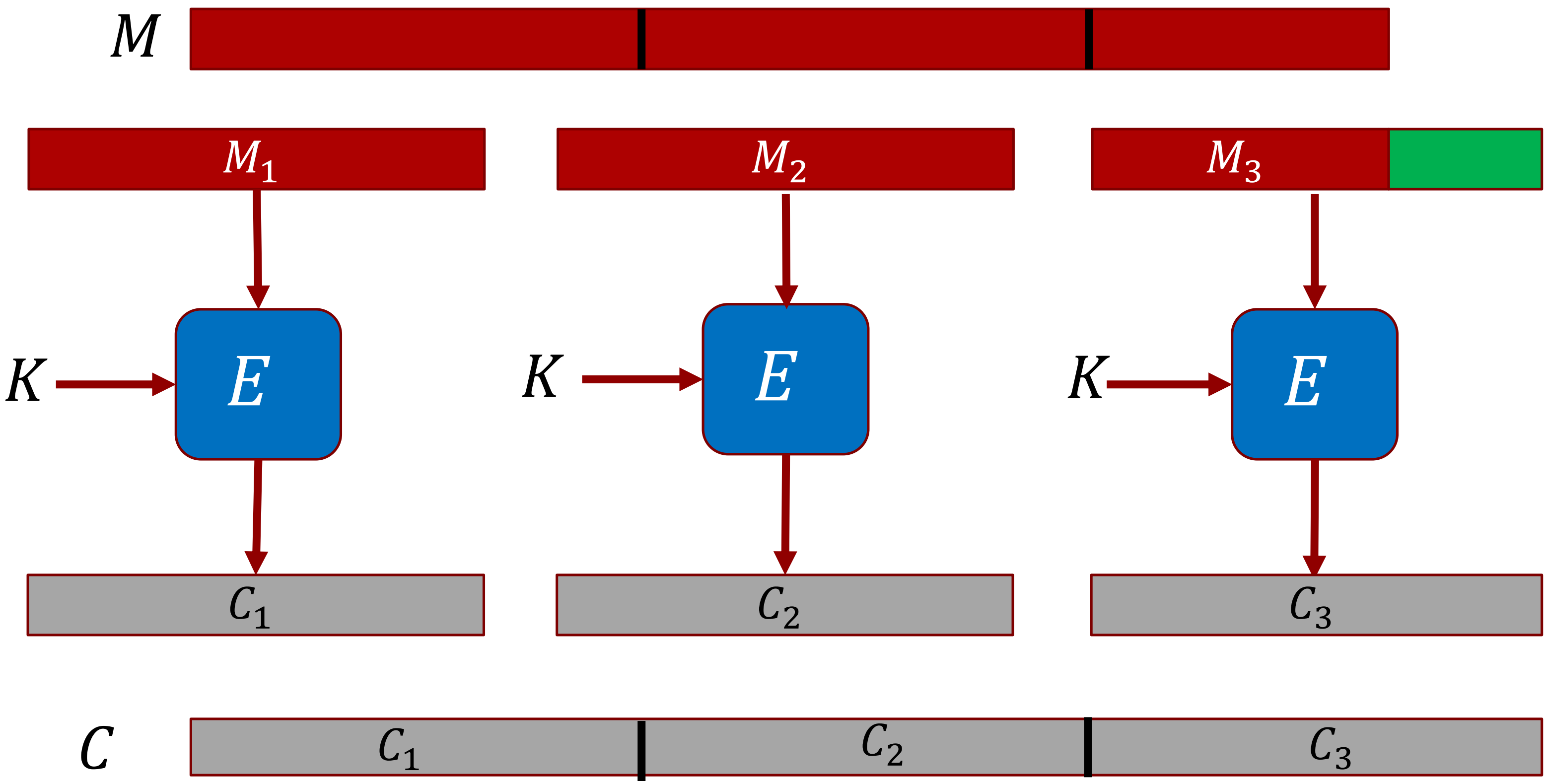
CPA-Security for Encryption Schemes

- Suppose we have a *secure* pseudorandom permutation family $F: \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$.
  - We saw a few examples(AES, 3DES etc.) in the last lecture.
- Consider the following encryption scheme $SE = (E, D)$ that encrypts messages of length n.
  - $E_K(M)$
    - Pick a random $r \leftarrow \{0,1\}^n$
    - Output $\mathrm{C} = < r, F_K(r) \oplus M >$
  - $D_K(C)$
    - Parse C as $< r, s >$
    - Output $M = F_K(r) \oplus s$
- Theorem (informal): If F is a secure PRF, then SE is ind-cpa secure symmetric encryption scheme.

Modes of Operation

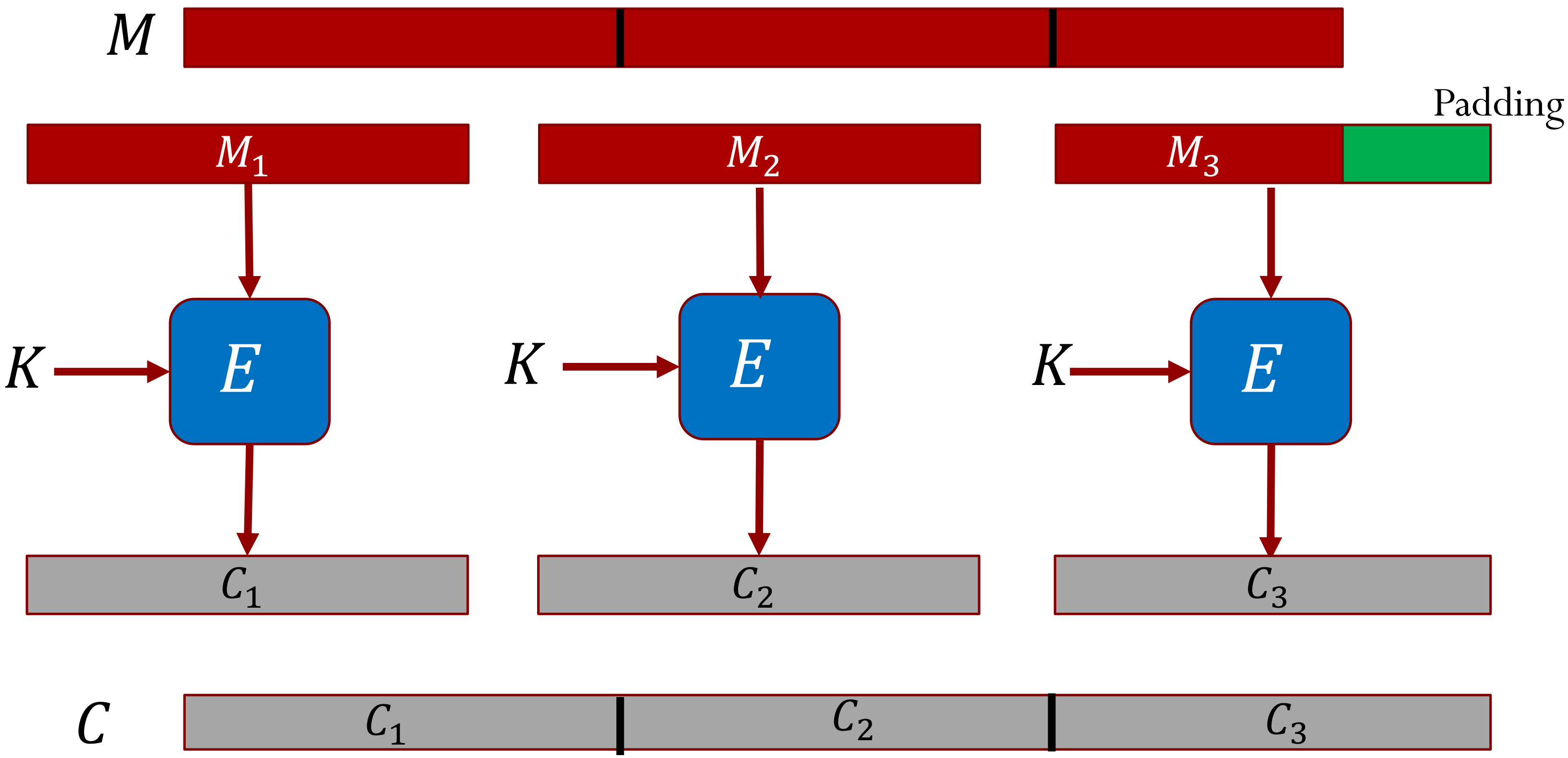
Using PRPs to design IND-CPA secure encryption schemes.

ECB Mode: Electronic Codebook Mode



- Is the encryption scheme using the ECM mode IND-CPA secure?

ECB Mode: Electronic Codebook Mode



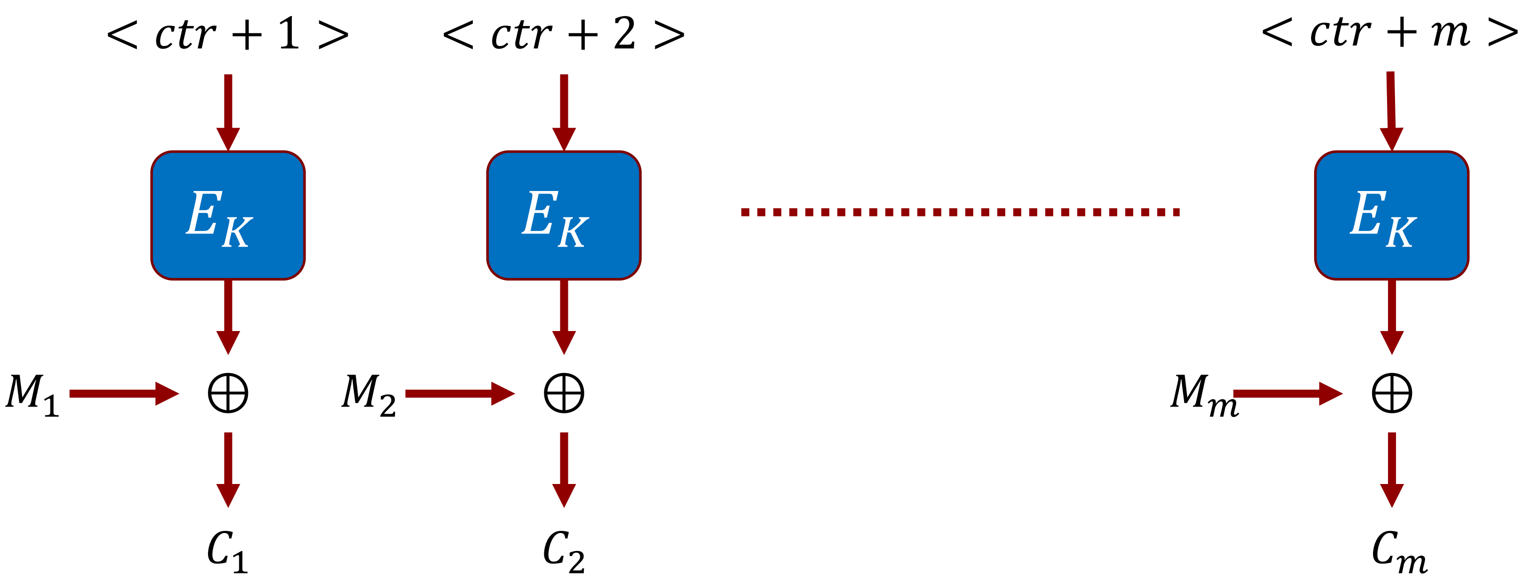
- Is the encryption scheme using the ECM mode IND-CPA secure?
  - No. Adversary queries $(0^n, 1^n)$ and then $(1^n, 1^n)$.

ECB Mode: Electronic Codebook Mode

- Is the encryption scheme using the ECM mode IND-CPA secure?
  - No. Adversary queries $(0^n, 1^n)$ and then $(1^n, 1^n)$.
- No deterministic (same ciphertext for same message) encryption scheme can be IND-CPA secure.
  - This means that a IND-CPA secure encryption scheme should output different ciphertexts for the same message.
  - There are two ways to achieve this:
    - <u>Randomized encryption (CBC$)</u>: The encryption algorithm is randomized.
    - <u>Stateful encryption (CTRC)</u>: The encryption algorithm maintains a state and the encryption depends on this state.

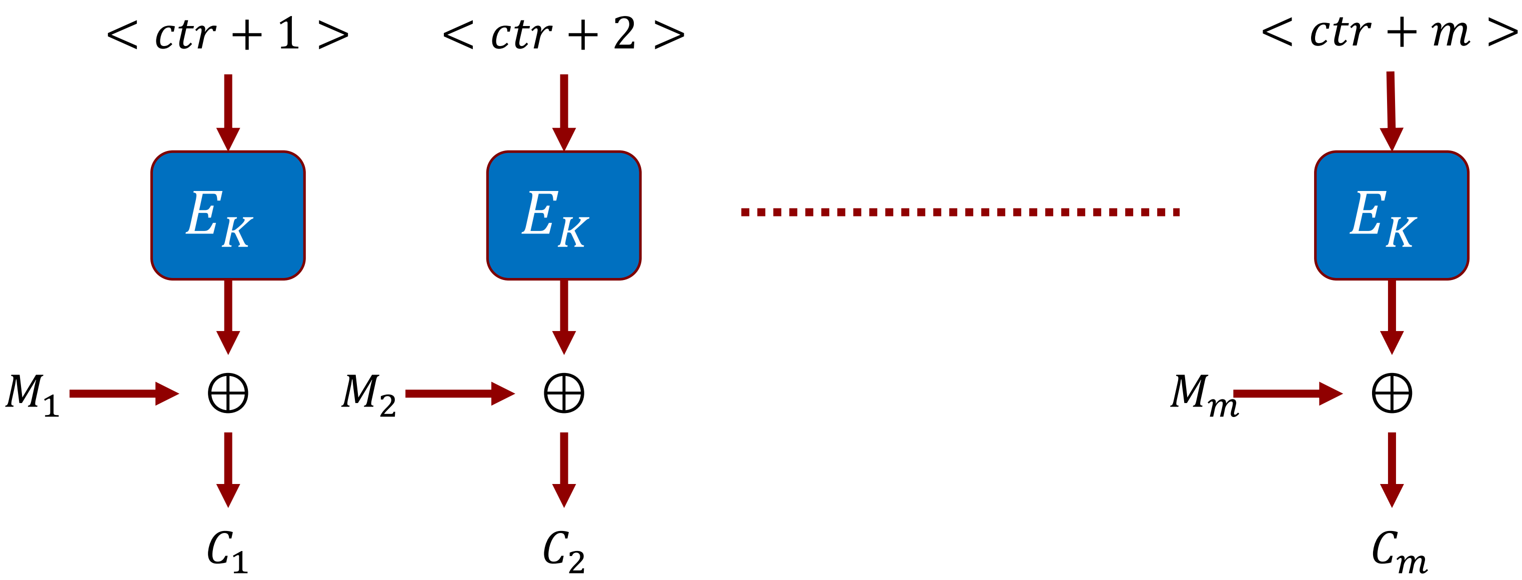
CTRC mode: Counter mode

CTRC Mode



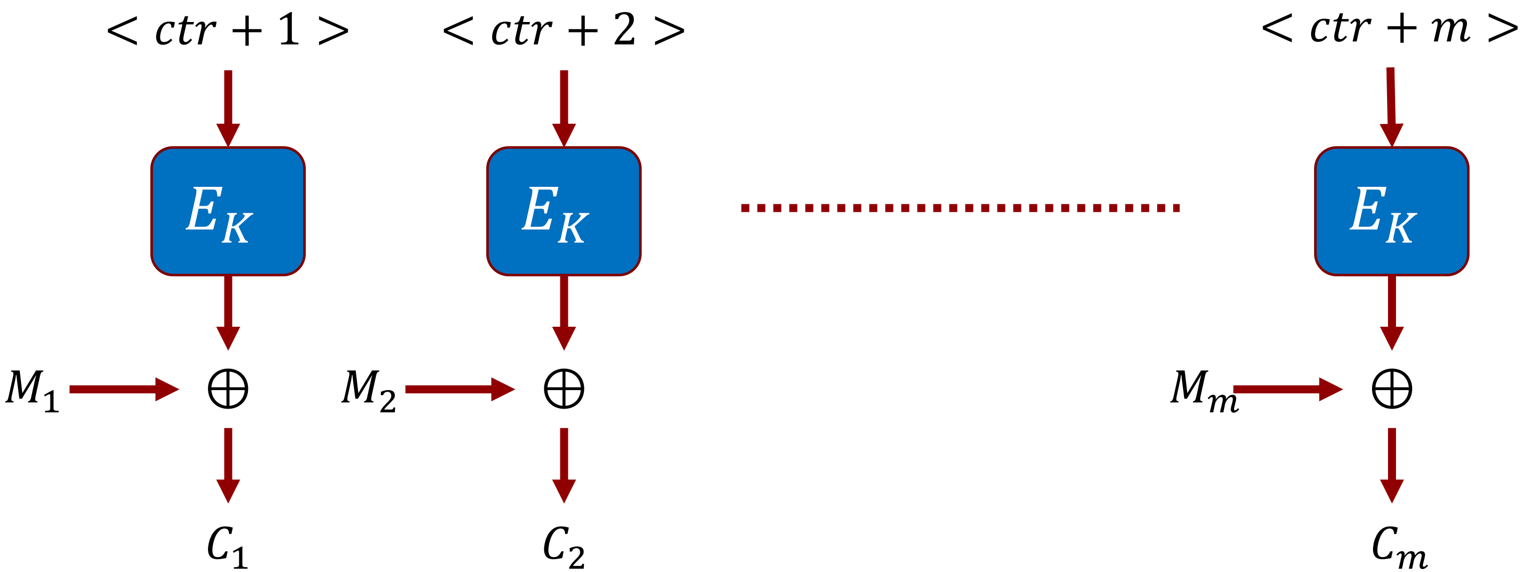
- The encryption algorithm maintains a counter ctr that is initialized to 0.
- For a m block message $M_1, \dots, M_m$ the ciphertext $C_0, C_1, \dots C_m$ is sent where $C_0 = ctr$.

CTRC Mode



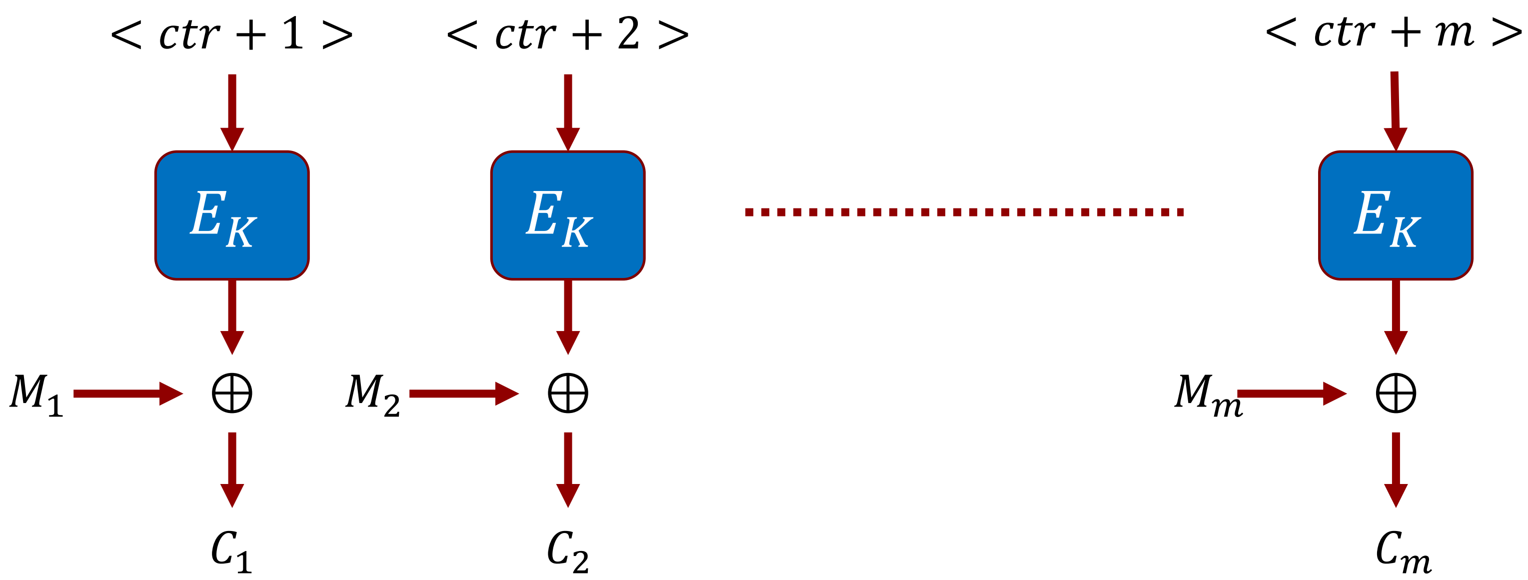
- The encryption algorithm maintains a counter ctr that is initialized to 0.
- For a m block message $M_1, \ldots, M_m$ the ciphertext $C_0, C_1, \ldots C_m$ is sent where $C_0 = ctr$.
- Few observations:
  - Decryptor does not need to maintain a counter.
  - Decryptor does not need E_K^{-1}.
  - Encryption decryption are parallalizable.

CTRC Mode



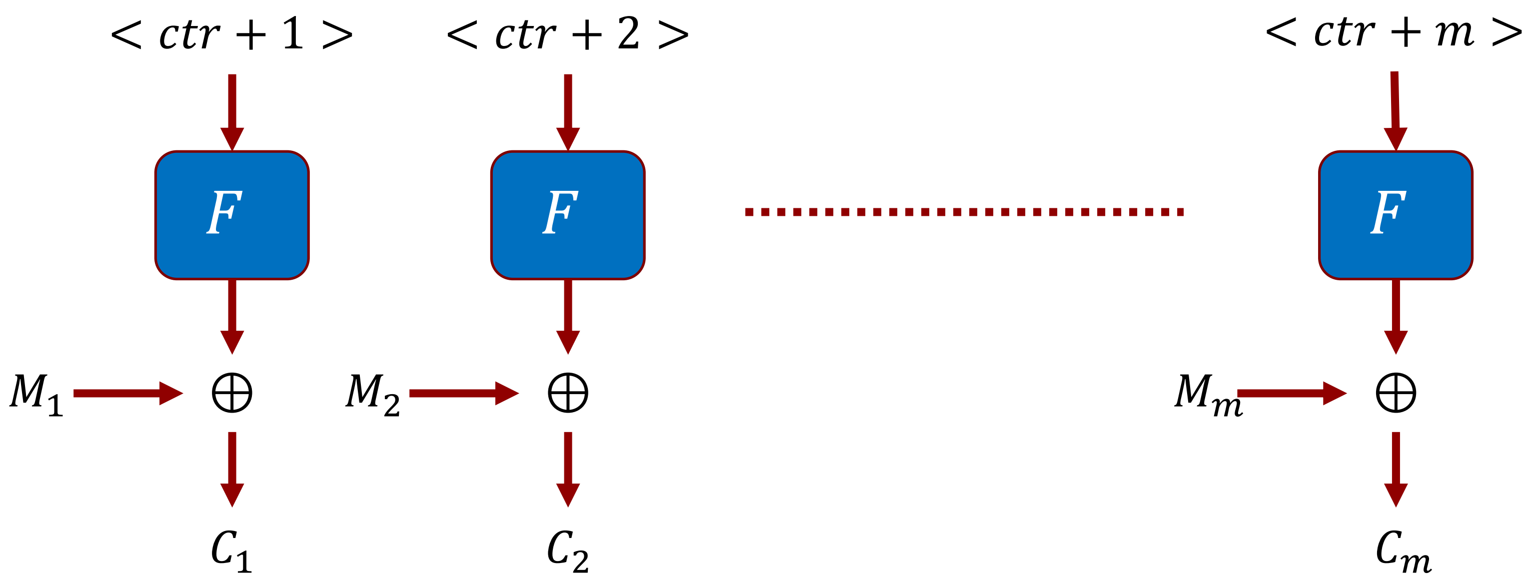
- Is this encryption scheme IND-CPA secure?

CTRC Mode



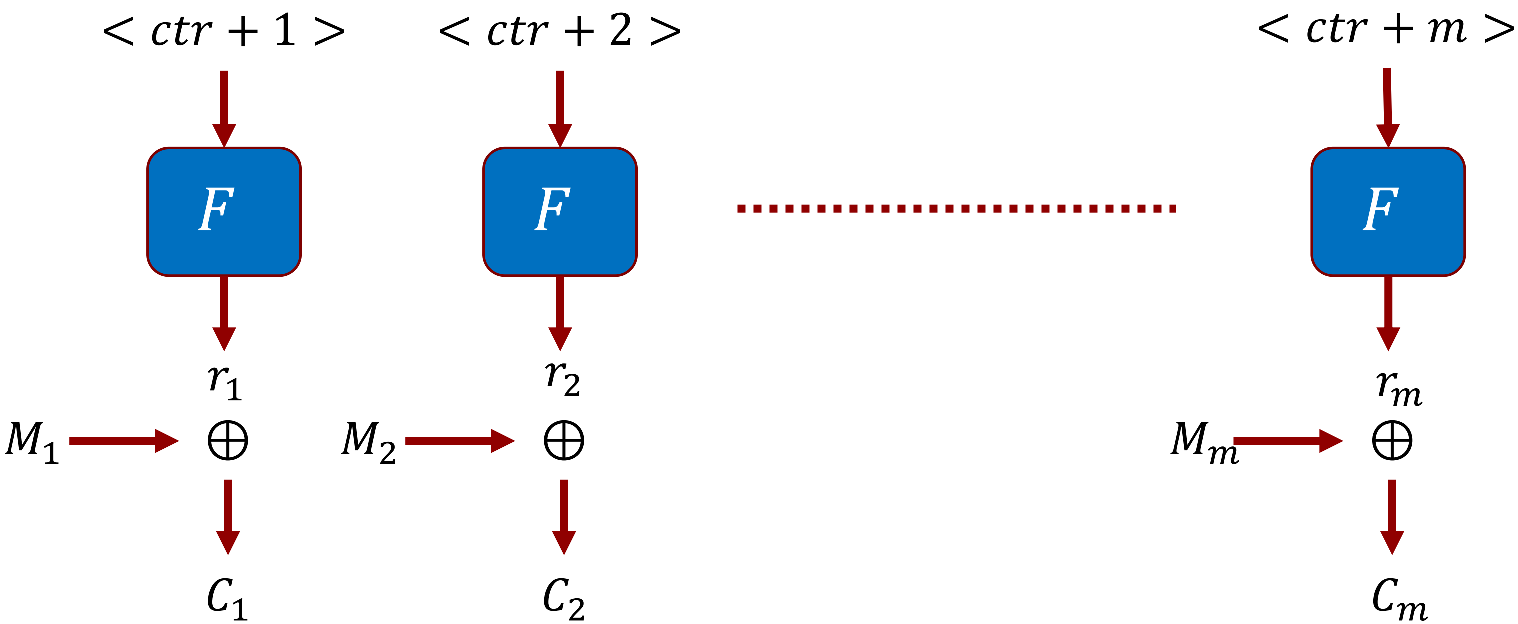
- Is this encryption scheme IND-CPA secure?
  - Yes if E is a secure PRF.
  - <u>Intuition</u>: What if instead of E, we use a purely random function.

CTRC Mode



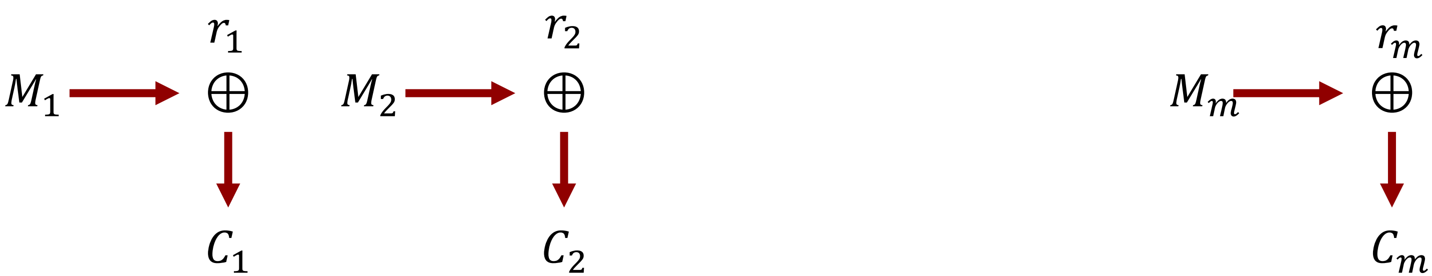
- Is this encryption scheme IND-CPA secure?
  - Yes if E is a secure PRF.
  - <u>Intuition</u>: What if instead of E, we use a purely random function.

CTRC Mode



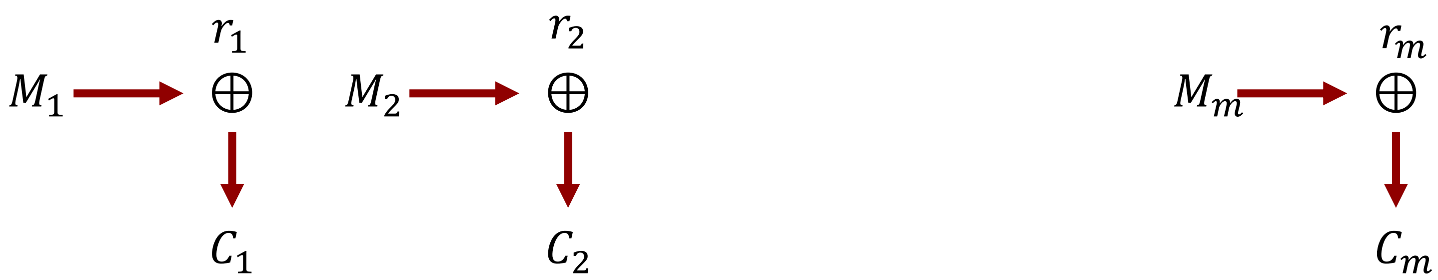
- Is this encryption scheme IND-CPA secure?
  - Yes if E is a secure PRF.
  - <u>Intuition</u>: What if instead of E, we use a purely random function.

CTRC Mode



- Is this encryption scheme IND-CPA secure?
  - Yes if E is a secure PRF.
  - <u>Intuition</u>: What if instead of E, we use a purely random function.
  - This is just One Time Pad. This reveals no information about the message and hence will be IND-CPA secure.

CTRC Mode



- Is this encryption scheme IND-CPA secure?
  - Yes if E is a secure PRF.
  - <u>Intuition</u>: What if instead of E, we use a purely random function.
  - This is just One Time Pad. This reveals no information about the message and hence will be IND-CPA secure.
  - But then, E *behaves* like a random function so should also be IND-CPA secure.

CTRC Mode

- Theorem: Let $E: \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$ be a function family and let $SE = (E, D)$ denote the CTRC mode encryption scheme using E. Let A be an adversary that attacks SE in the IND-CPA sense thatruns in time t and makes q queries involving a total of σ message blocks. Then there is a PRF adversary B such that

  $$Adv_{ind-cpa}(A, SE) \leq 2 \cdot Adv_{PRF}(B, E)$$

  Moreover, B only makes σ queries and runs in time at most $t + \theta(n\sigma)$.

CTRC Mode

- Theorem: Let $E: \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a function family and let $SE = (E, D)$ denote the CTRC mode encryption scheme using E. Let A be an adversary that attacks SE in the IND-CPA sense and makes q queries involving a total of σ message blocks. Then there is a PRF adversary B such that
$$Adv_{ind-cpa}(A, SE) \leq 2 \cdot Adv_{PRF}(B, E)$$
Moreover, B only makes σ queries and runs in time at most $t + \theta(n\sigma)$.

- First, we define an experiment that captures IND-CPA.
- $LRGuess_{SE,A}$
  - Randomly pick a key $K \leftarrow \{0,1\}^n$.
  - Pick a random bit $b \leftarrow \{0,1\}$
  - When A makes query (M_0^i, M_1^i), return the value $E_K(M_b^i)$.
  - Finally, A outputs a bit b'
  - If $(b = b')$ output 1 else output 0
- Claim 1: $\Pr[LRGuess_{SE,A} = 1] = \frac{1}{2} + \frac{1}{2} \cdot Adv_{ind-cpa}(A, SE)$.

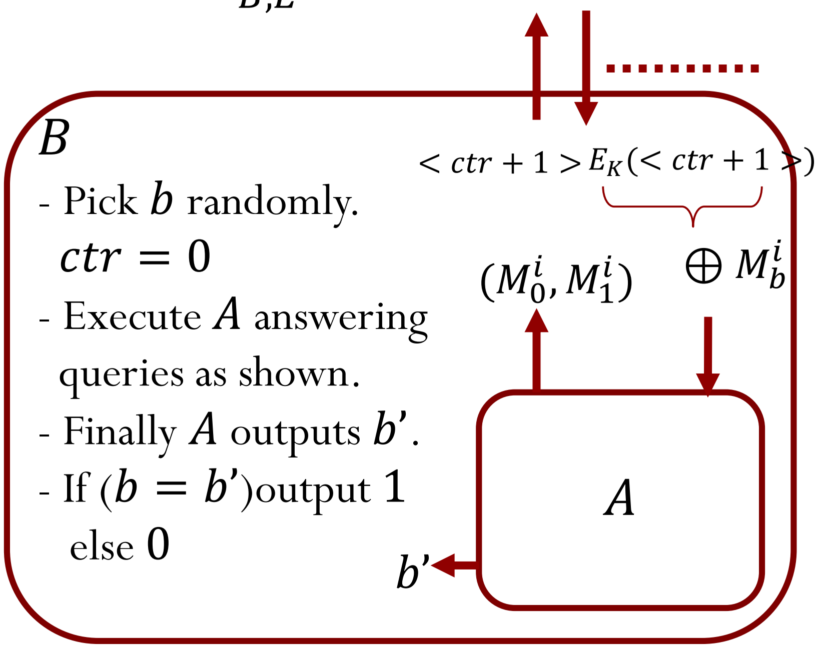
CTRC Mode

- <u>Theorem</u>: Let $E: \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$ be a function family and let $SE = (E, D)$ denote the CTRC mode encryption scheme using E. Let A be an adversary that attacks SE in the IND-CPA sense and makes q queries involving a total of σ message blocks. Then there is a PRF adversary B such that

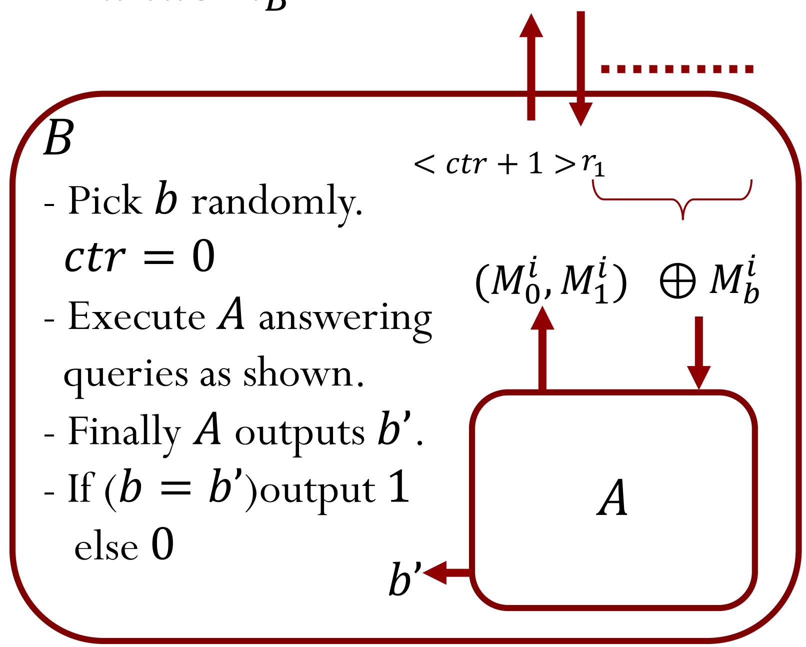
$$Adv_{ind-cpa}(A, SE) \leq 2 \cdot Adv_{PRF}(B, E)$$

Moreover, B only makes σ queries and runs in time at most $t + \theta(n\sigma)$.

$Real_{B,E}$



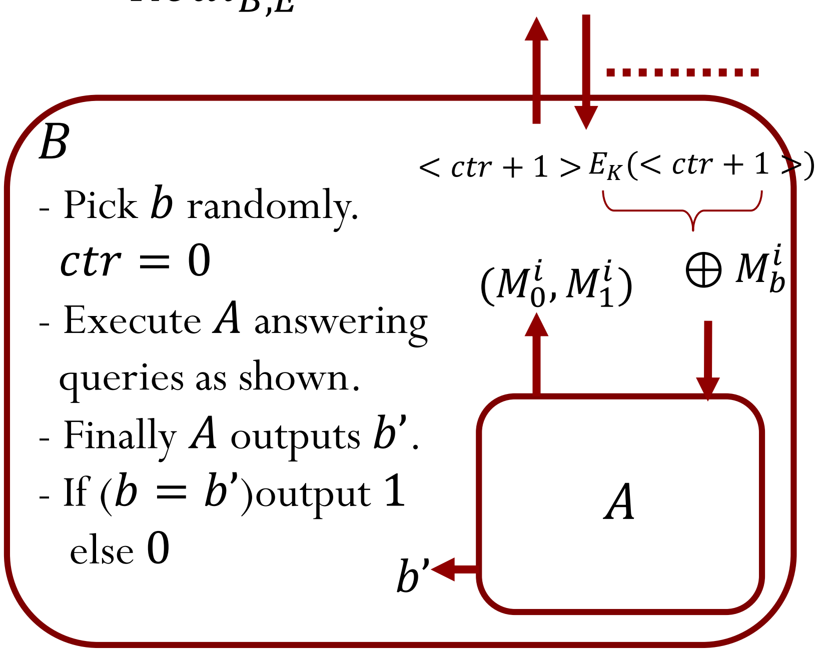
$Random_B$



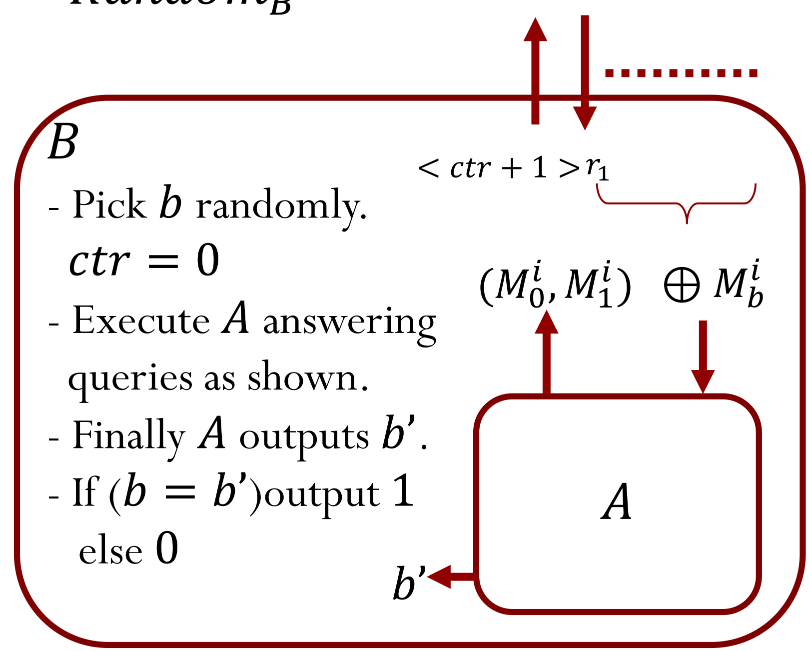
CTRC Mode

- Theorem: Let $E: \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$ be a function family and let $SE = (E, D)$ denote the CTRC mode encryption scheme using E. Let A be an adversary that attacks SE in the IND-CPA sense and makes q queries involving a total of σ message blocks. Then there is a PRF adversary B such that
$$Adv_{ind-cpa}(A, SE) \leq 2 \cdot Adv_{PRF}(B, E)$$
Moreover, B only makes σ queries and runs in time at most $t + \theta(n\sigma)$.

$Real_{B,E}$



$Random_B$

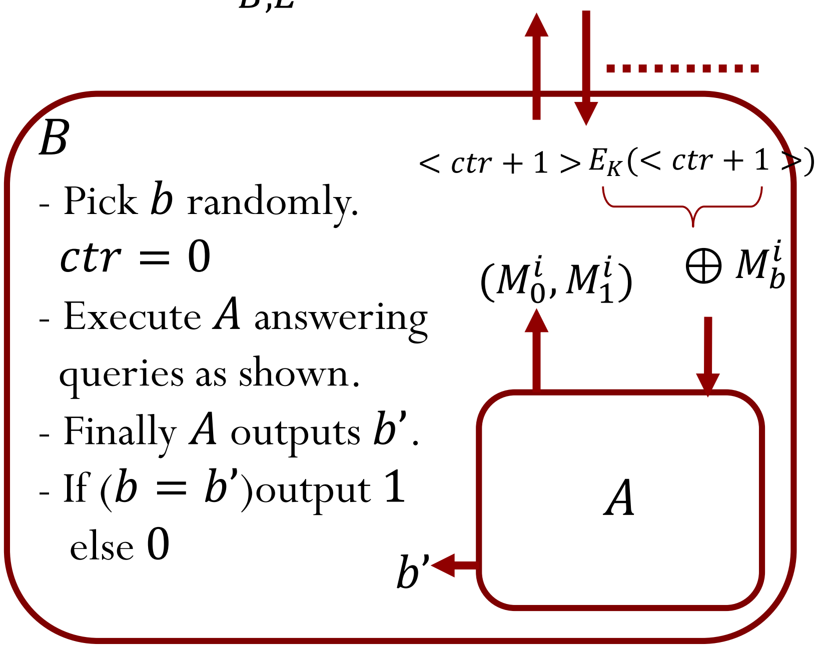


$\Pr[Real_{B,E} = 1] = ?$

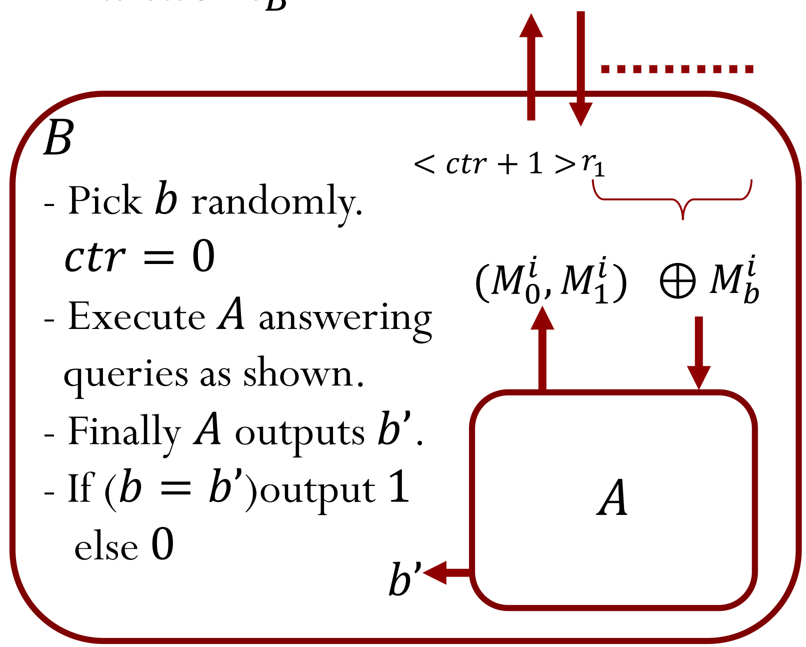
CTRC Mode

- Theorem: Let $E: \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$ be a function family and let $SE = (E, D)$ denote the CTRC mode encryption scheme using E. Let A be an adversary that attacks SE in the IND-CPA sense and makes q queries involving a total of σ message blocks. Then there is a PRF adversary B such that
$$Adv_{ind-cpa}(A, SE) \leq 2 \cdot Adv_{PRF}(B, E)$$
Moreover, B only makes σ queries and runs in time at most $t + \theta(n\sigma)$.

$Real_{B,E}$



$Random_B$



$$\Pr[Real_{B,E} = 1] = \Pr[LRGuess_{A,SE} = 1]$$

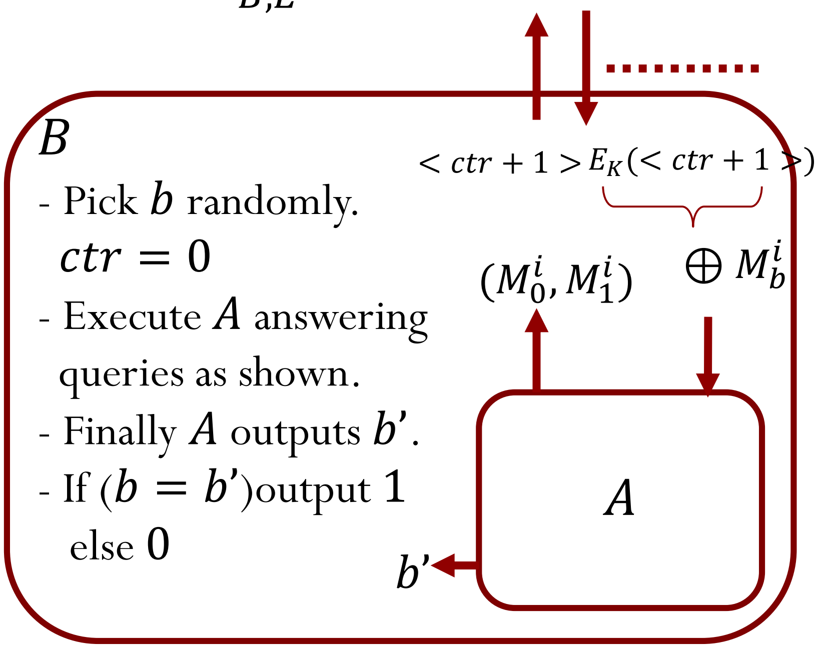
CTRC Mode

- Theorem: Let $E: \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$ be a function family and let $SE = (E, D)$ denote the CTRC mode encryption scheme using E. Let A be an adversary that attacks SE in the IND-CPA sense and makes q queries involving a total of σ message blocks. Then there is a PRF adversary B such that

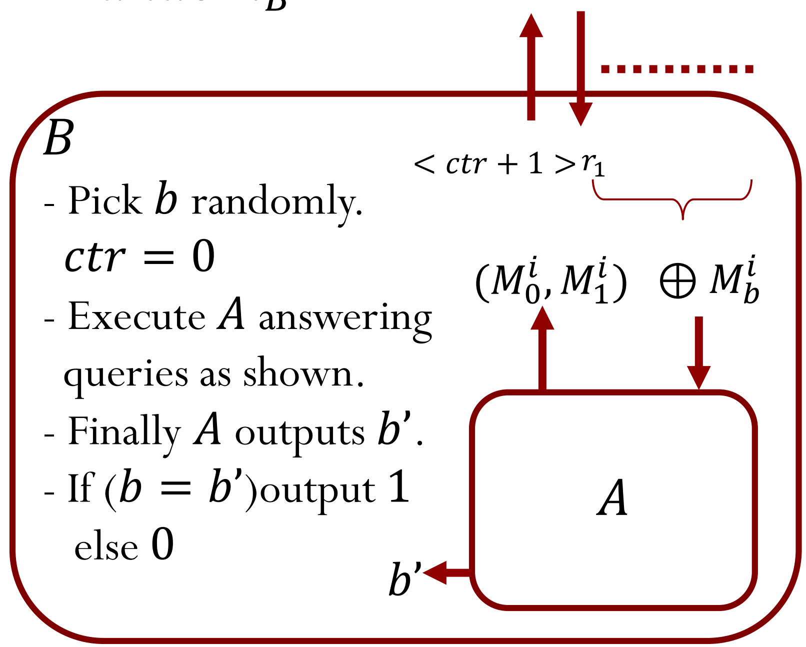
$$Adv_{ind-cpa}(A, SE) \leq 2 \cdot Adv_{PRF}(B, E)$$

Moreover, B only makes σ queries and runs in time at most $t + \theta(n\sigma)$.

$Real_{B,E}$



$Random_B$

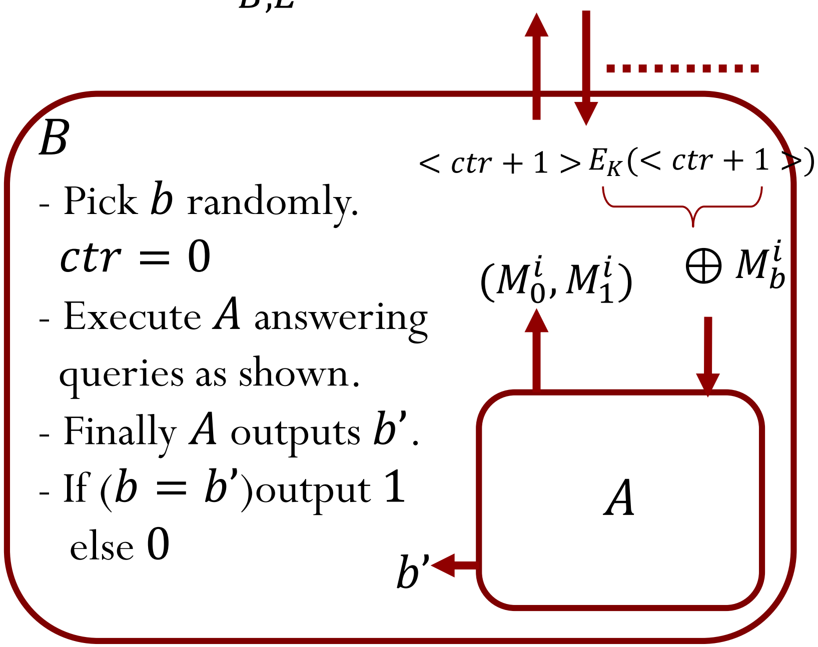


$$\Pr[Real_{B,E} = 1] = \frac{1}{2} + \frac{1}{2} \cdot Adv_{ind-cpa}(A, SE)$$

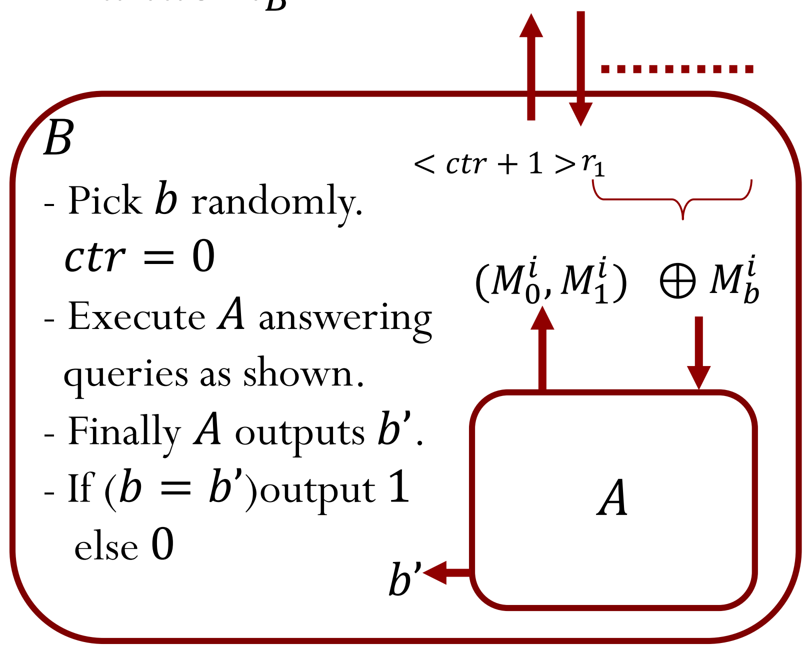
CTRC Mode

- Theorem: Let $E: \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$ be a function family and let $SE = (E, D)$ denote the CTRC mode encryption scheme using E. Let A be an adversary that attacks SE in the IND-CPA sense and makes q queries involving a total of σ message blocks. Then there is a PRF adversary B such that
$$Adv_{ind-cpa}(A, SE) \leq 2 \cdot Adv_{PRF}(B, E)$$
Moreover, B only makes σ queries and runs in time at most $t + \theta(n\sigma)$.

$Real_{B,E}$



$Random_B$



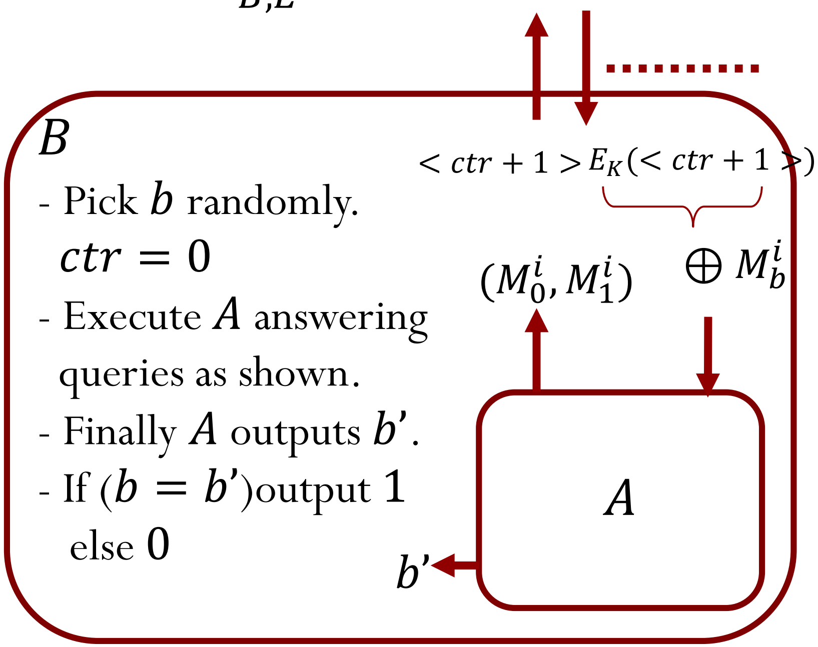
$$\Pr[Real_{B,SE} = 1] = \frac{1}{2} + \frac{1}{2} \cdot Adv_{ind-cpa}(A, SE)$$

$$\Pr[Random_B = 1] = ?$$

CTRC Mode

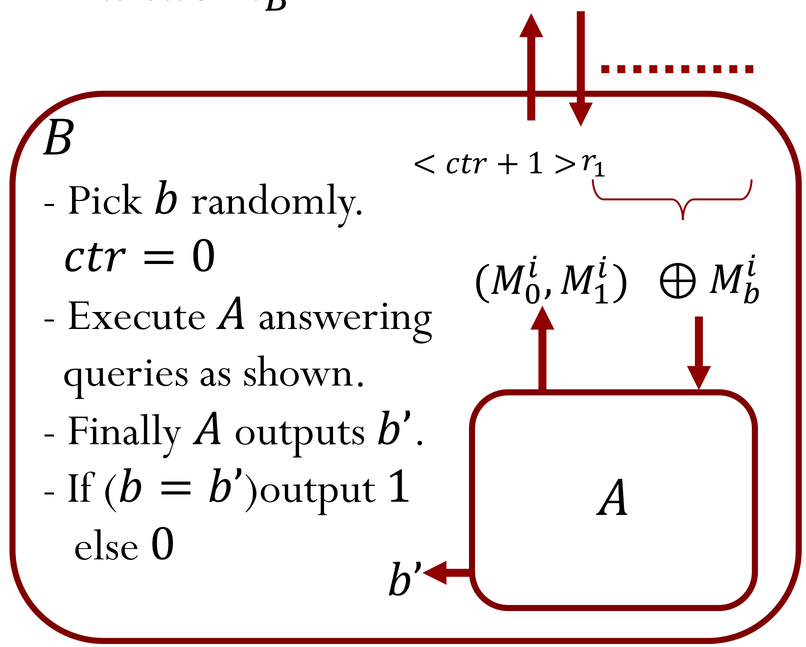
- Theorem: Let $E: \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$ be a function family and let $SE = (E, D)$ denote the CTRC mode encryption scheme using E. Let A be an adversary that attacks SE in the IND-CPA sense and makes q queries involving a total of σ message blocks. Then there is a PRF adversary B such that
$$Adv_{ind-cpa}(A, SE) \leq 2 \cdot Adv_{PRF}(B, E)$$
Moreover, B only makes σ queries and runs in time at most $t + \theta(n\sigma)$.

$Real_{B,E}$



$$\Pr[Real_{B,SE} = 1] = \frac{1}{2} + \frac{1}{2} \cdot Adv_{ind-cpa}(A, SE)$$

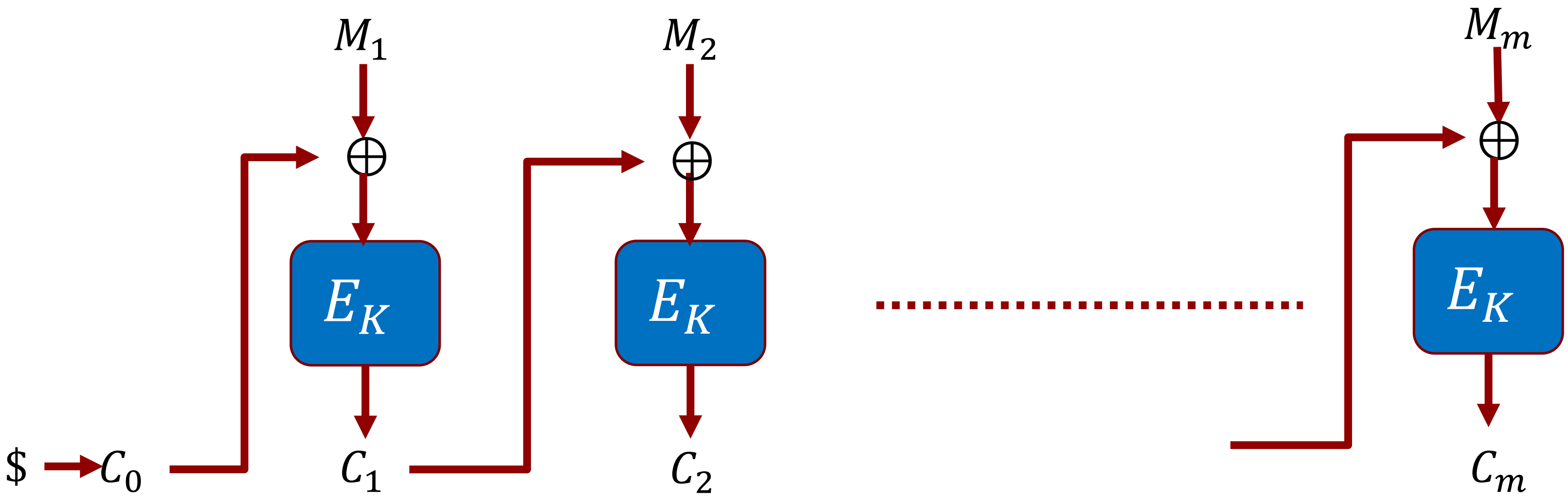
$Random_B$



$$\Pr[Random_B = 1] = \frac{1}{2}$$

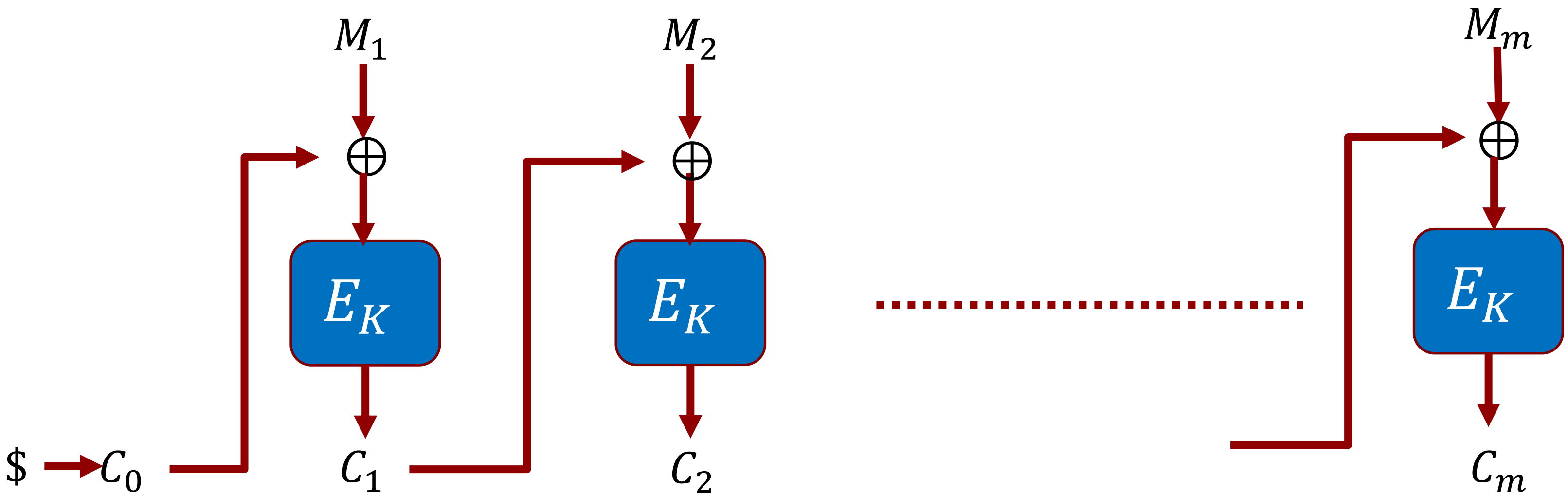
CBC$ Mode: Cipher Block Chaining

CBC$ Mode



- C_0 is chosen randomly from $\{0,1\}^n$.
- The ciphertext corresponding to $M_1, \ldots, M_m$ is $C_0, C_1, \ldots, C_m$.
- E_K needs to be a block cipher (i.e., it should be invertible).

Birthday attack on CBC$



- Consider the following adversary that attacks this encryption scheme in the IND-CPA sense:
- A
  - For $i = 1$ to q
    - Make a query $(< i >, < 0 >)$ and let $C_0^i C_1^i$ be the reply.
  - If there exists $i \neq j$ s.t. $C_0^i = C_0^j$,
    - then if $C_1^i = C_1^j$, then output 1
  - Output 0

Birthday attack on CBC$

- Consider the following adversary that attacks this encryption scheme in the IND-CPA sense:
- A
  - For $i = 1$ to q
    - Make a query $(< i >, < 0 >)$ and let $C_0^i C_1^i$ be the reply.
  - If there exists $i \neq j$ s.t. $C_0^i = C_0^j$,
    - then if $C_1^i = C_1^j$, then output 1
  - Output 0
- What is $\Pr[Left_{A,SE} = 1] =$?

Birthday attack on CBC$

- Consider the following adversary that attacks this encryption scheme in the IND-CPA sense:
- A
  - For $i = 1$ to q
    - Make a query $(<i>, <0>)$ and let $C_0^i C_1^i$ be the reply.
  - If there exists $i \neq j$ s.t. $C_0^i = C_0^j$,
    - then if $C_1^i = C_1^j$, then output 1
  - Output 0
- What is $\Pr\left[Left_{A,SE} = 1\right] = 0.$
- What is $\Pr\left[Right_{A,SE} = 1\right] =?$

Birthday attack on CBC$

- Consider the following adversary that attacks this encryption scheme in the IND-CPA sense:
- A
  - For $i = 1$ to q
    - Make a query $(< i >, < 0 >)$ and let $C_0^i C_1^i$ be the reply.
  - If there exists $i \neq j$ s.t. $C_0^i = C_0^j$,
    - then if $C_1^i = C_1^j$, then output 1
  - Output 0
- What is $\Pr[Left_{A,SE} = 1] = 0$.
- What is $\Pr[Right_{A,SE} = 1] = C(q, 2^n)$.
  - $C(i, N)$: This is defined to be the probability that a "collision" happens when i elements are chosen independently and randomly from the set $\{1, \ldots, N\}$.

Digression

Birthday Problem: The value of $C(i, N)$

Birthday Problem

- Birthday Problem: You uniformly sample i items with replacement from a collection of N items. What is the probability that two items are the same?

- Birthday Problem(popular version): There are i people in a room. What is the value of i such that the probability of two people having the same birthday is at least ½. Each person's birthday is assumed to be a random day in the year.

Birthday Problem

- Birthday Problem: You uniformly sample i items with replacement from a collection of N items. What is the probability that two items are the same?

- Question: Can we get a closed form expression for $C(i, N)$, the probability of collision?
- Balls and bins: We throw i balls into N bins randomly. What is the probability that there is a bin that has more than one ball?
  - This is the same problem. The probability is $C(i, N)$.

Birthday Problem

- Balls and bins: We throw i balls into N bins randomly. What is the probability that there is a bin that has more than one ball?

- Claim 1: $C(i, N) \leq \frac{i(i-1)}{2N}$.
  - Proof:
    - Let C_i be the event that the i^{th} ball collides with one of the previous balls.
    - Lemma: $\Pr[C_i] \leq (i-1)/N$.
    - $$\begin{aligned} C(i, N) &= \Pr[C_1 \cup C_2 \cup \cdots \cup C_i] \\ &\leq \Pr[C_1] + \Pr[C_2] + \ldots + \Pr[C_i]. \\ &\leq 0 + \frac{1}{N} + \ldots + \frac{i-1}{N} \\ &= \frac{i(i-1)}{2N}. \end{aligned}$$

Birthday Problem

- Balls and bins: We throw i balls into N bins randomly. What is the probability that there is a bin that has more than one ball?

- Claim 2: $C(i, N) \geq 1 - e^{-\frac{i(i-1)}{2N}}$.
  - Proof:
    - Let D_i be the event there are no collisions after i balls are thrown.
    - Lemma: $\Pr[D_{i+1}|D_i] = 1 - \frac{i}{n}$ and $\Pr[D_1] = 1$.
    - $1 - C(i, N) = \Pr[D_i] = \Pr[D_i|D_{i-1}].\Pr[D_{i-1}]$

$$= \prod \Pr[D_{j+1}|D_j]$$

$$= \prod \left(1 - \frac{j}{n}\right) \leq e^{-\frac{\sum j}{N}}$$

$$= e^{-\frac{i(i-1)}{2N}}.$$

Birthday Problem

- Balls and bins: We throw i balls into N bins randomly. What is the probability that there is a bin that has more than one ball?

- Claim 2: $C(i,N) \geq 1 - e^{-\frac{i(i-1)}{2N}}$.
- Corollary: If $1 \leq i \leq \sqrt{2n}$,

  then $C(i,N) \geq (1 - \frac{1}{e}).i(i-1)/2N$.
  - Proof:
    - Use the fact that for $0 < x \leq 1, 1 - e^{-x} \geq \left(1 - \frac{1}{e}\right) \cdot x$.

Birthday attack on CBC$

- A
  - For $i = 1$ to q
    - Make a query $(< i >, < 0 >)$ and let $C_0^i C_1^i$ be the reply.
  - If there exists $i \neq j$ s.t. $C_0^i = C_0^j$,
    - then if $C_1^i = C_1^j$, then output 1
  - Output 0
- What is $\Pr[Left_{A,SE} = 1] = 0$.
- What is $\Pr[Right_{A,SE} = 1] = C(q, 2^n)$.
  - $C(i, N)$: This is defined to be the probability that a "collision" happens when i elements are chosen independently and randomly from the set $\{1, \ldots, N\}$.
- $Adv_{ind-cpa}(A, SE) \geq 0.3 \cdot \frac{q \cdot (q-1)}{2^{n+1}}$.
- The advantage is large if $q > 2^{n/2}$

Birthday attack on CBC$

- A
  - For $i = 1$ to q
    - Make a query $(< i >, < 0 >)$ and let $C_0^i C_1^i$ be the reply.
  - If there exists $i \neq j$ s.t. $C_0^i = C_0^j$,
    - then if $C_1^i = C_1^j$, then output 1
  - Output 0
- What is $\Pr\left[Left_{A,SE} = 1\right] = 0$.
- What is $\Pr\left[Right_{A,SE} = 1\right] = C(q, 2^n)$.
- $1 \leq q \leq 2^{\frac{n+1}{2}}, Adv_{ind-cpa}(A, SE) \geq 0.3 \cdot \frac{q \cdot (q-1)}{2^{n+1}}$.
- The advantage is large (constant) if $q > 2^{n/2}$.
- We should not encrypt more than $2^{n/2}$ blocks for a key.

Birthday attack on CBC$

- We should not encrypt more than $2^{n/2}$ blocks for a key.
- Block size is important!
  - Examples:
    - DES: $n = 64$, so $2^{n/2} = 2^{32}$ which is not a large number.
    - AES: $n = 128$, so $2^{n/2} = 2^{64}$. This is sufficiently large for practical purposes.

- We saw a q-query adversary that has an advantage (in the IND-CPA sense) $\approx q^2/2^{n+1}$. Is there a better adversary?
  - No if the block cipher is a secure PRP.

IND-CPA security of CBC$

- Theorem: Let $E: \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$ be a block cipher and $SE = (E, D)$ be the corresponding CBC$ encryption scheme. Let A be an IND-CPA adversary that runs in time t and makes q queries totalling σ blocks. Then there is a PRF adversary B against E such that:

$$Adv_{ind-cpa}(A, SE) \leq 2 \cdot Adv_{PRF}(B, E) + \frac{\sigma^2}{2^n}.$$

Morever, B makes at most σ oracle queries and has a running time $t + \theta(\sigma \cdot n)$.

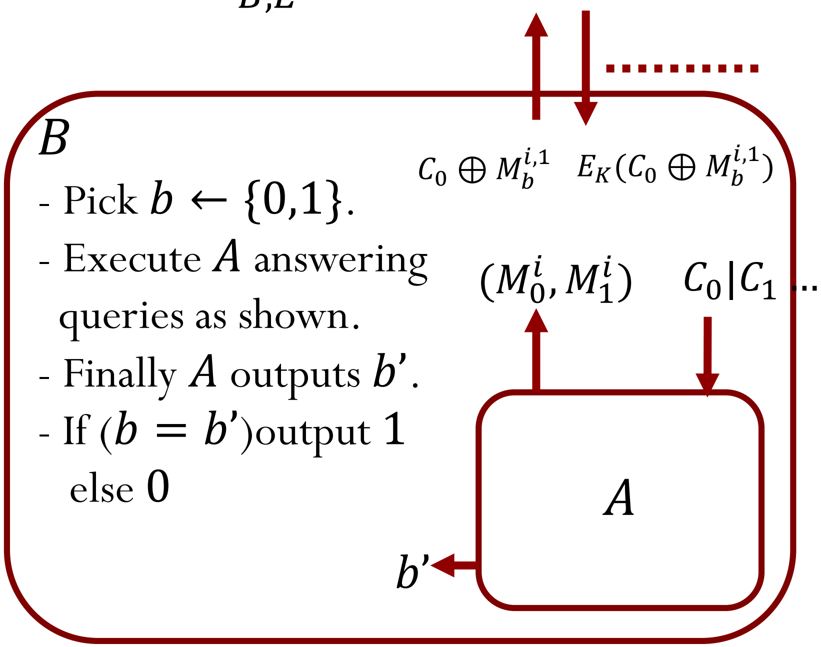
IND-CPA security of CBC$

- Theorem: Let $E: \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$ be a block cipher and $SE = (E, D)$ be the corresponding CBC$ encryption scheme. Let A be an IND-CPA adversary that runs in time t and makes q queries totalling σ blocks. Then there is a PRF adversary B against E such that:

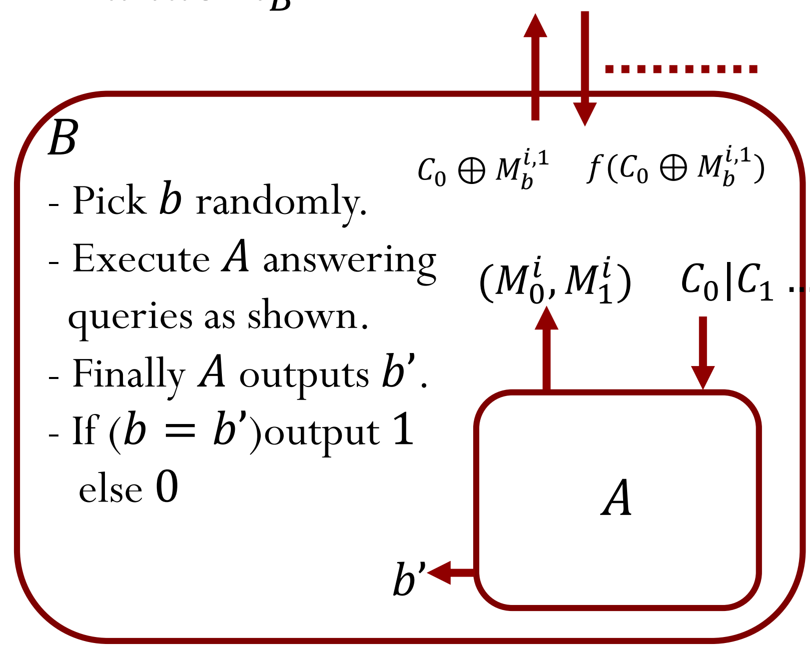
$$Adv_{ind-cpa}(A, SE) \leq 2 \cdot Adv_{PRF}(B, E) + \frac{\sigma^2}{2^n}.$$

Morever, B makes at most σ oracle queries and has a running time $t + \theta(\sigma \cdot n)$.

$Real_{B,E}$



$Random_B$



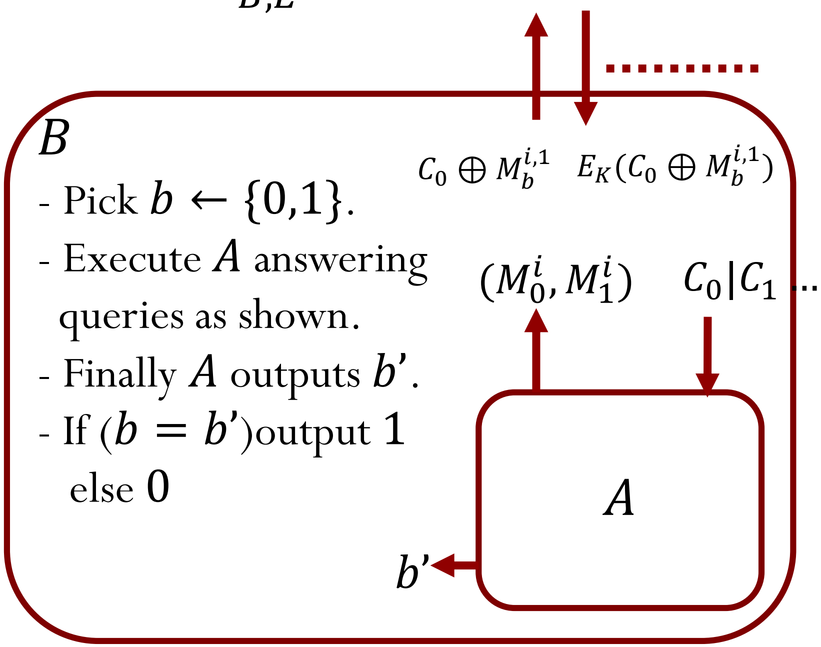
IND-CPA security of CBC$

- Theorem: Let $E: \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$ be a block cipher and $SE = (E, D)$ be the corresponding CBC$ encryption scheme. Let A be an IND-CPA adversary that runs in time t and makes q queries totalling σ blocks. Then there is a PRF adversary B against E such that:

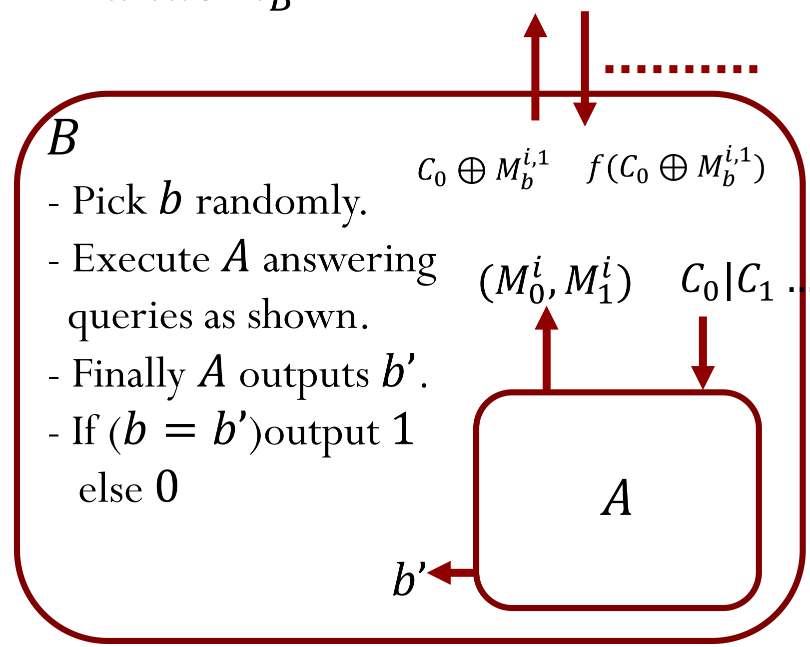
$$Adv_{ind-cpa}(A, SE) \leq 2 \cdot Adv_{PRF}(B, E) + \frac{\sigma^2}{2^n}.$$

Morever, B makes at most σ oracle queries and has a running time $t + \theta(\sigma \cdot n)$.

$Real_{B,E}$



$Random_B$



$\Pr[Real_{B,E} = 1] = ?$

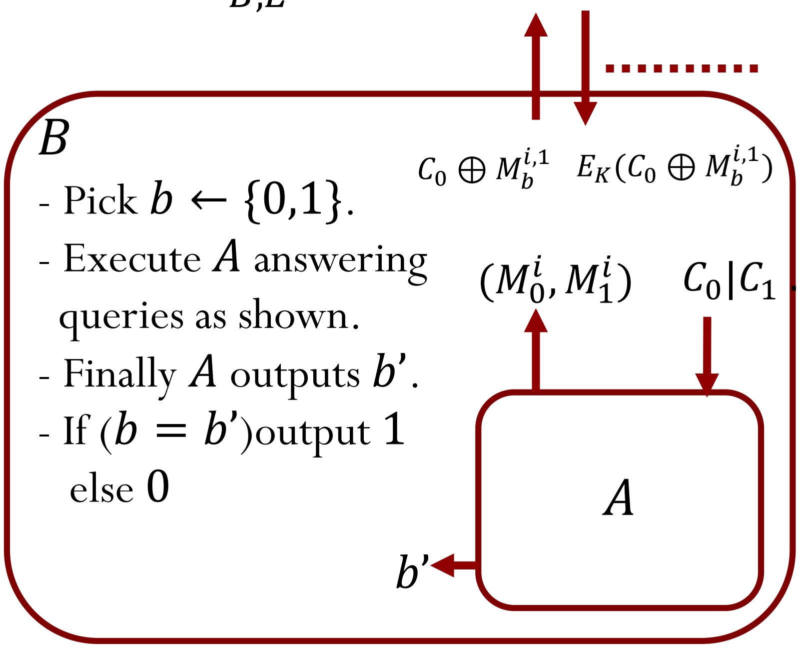
IND-CPA security of CBC$

- Theorem: Let $E: \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$ be a block cipher and $SE = (E, D)$ be the corresponding CBC\$ encryption scheme. Let A be an IND-CPA adversary that runs in time t and makes q queries totalling σ blocks. Then there is a PRF adversary B against E such that:

$$Adv_{ind-cpa}(A, SE) \leq 2 \cdot Adv_{PRF}(B, E) + \frac{\sigma^2}{2^n}.$$

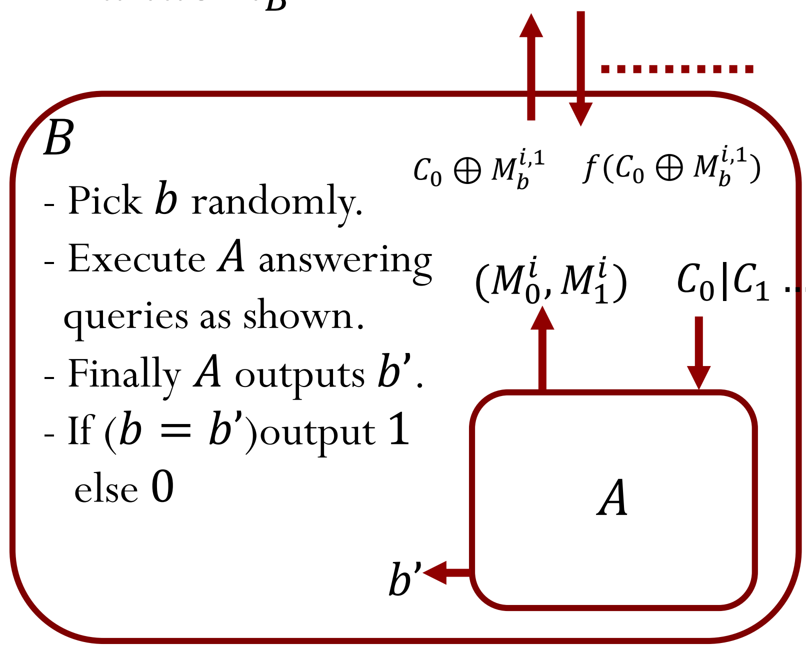
Morever, B makes at most σ oracle queries and has a running time $t + \theta(\sigma \cdot n)$.

$Real_{B,E}$



$$\Pr[Real_{B,E} = 1] = \frac{1}{2} + \frac{1}{2} \cdot Adv_{ind-cpa}(A, SE)$$

$Random_B$



$$\Pr[Random_B = 1] = ?$$

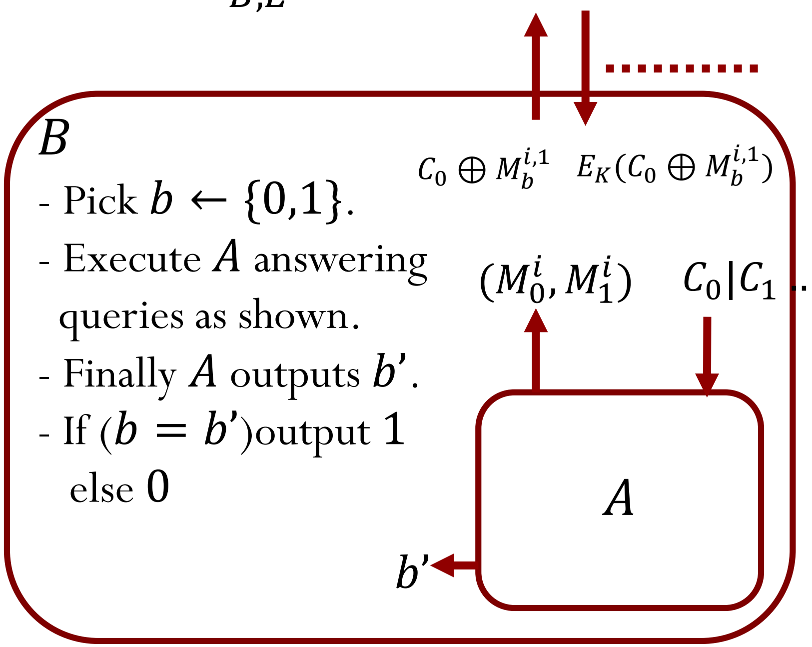
IND-CPA security of CBC$

- Theorem: Let $E: \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher and $SE = (E, D)$ be the corresponding CBC$ encryption scheme. Let A be an IND-CPA adversary that runs in time t and makes q queries totalling σ blocks. Then there is a PRF adversary B against E such that:

$$Adv_{ind-cpa}(A, SE) \leq 2 \cdot Adv_{PRF}(B, E) + \frac{\sigma^2}{2^n}.$$

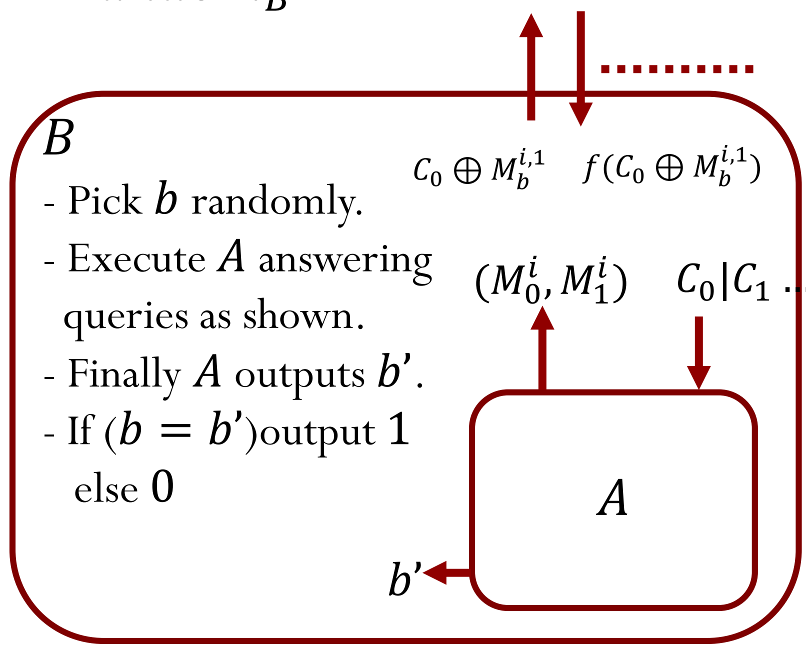
Morever, B makes at most σ oracle queries and has a running time $t + \theta(\sigma \cdot n)$.

$Real_{B,E}$



$$\Pr[Real_{B,E} = 1] = \frac{1}{2} + \frac{1}{2} \cdot Adv_{ind-cpa}(A, SE)$$

$Random_B$



$\Pr[Random_B = 1] \leq \Pr[Random_B = 1 | \neg X] + \Pr[X]$

X is the event that a "collision" happens

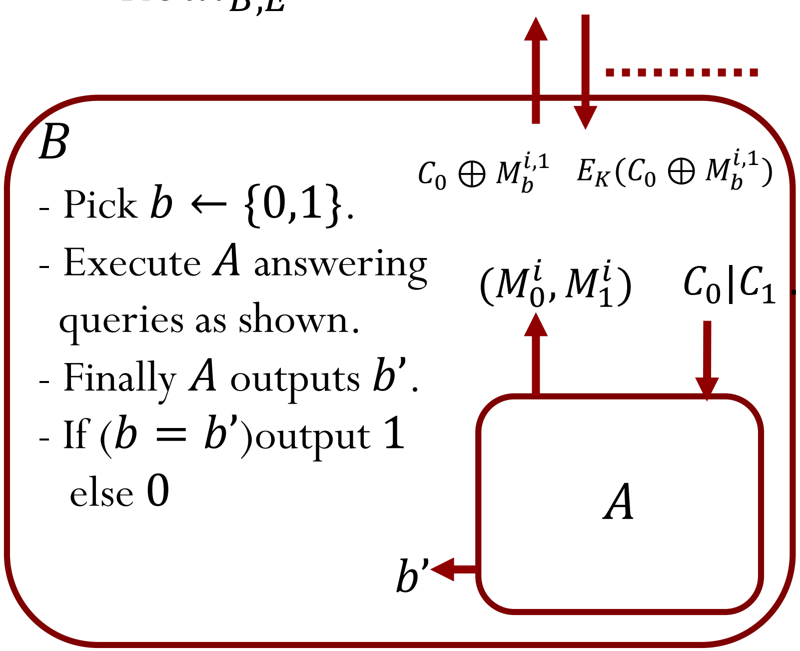
IND-CPA security of CBC$

- Theorem: Let $E: \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher and $SE = (E, D)$ be the corresponding CBC$ encryption scheme. Let A be an IND-CPA adversary that runs in time t and makes q queries totalling σ blocks. Then there is a PRF adversary B against E such that:

$$Adv_{ind-cpa}(A, SE) \leq 2 \cdot Adv_{PRF}(B, E) + \frac{\sigma^2}{2^n}.$$

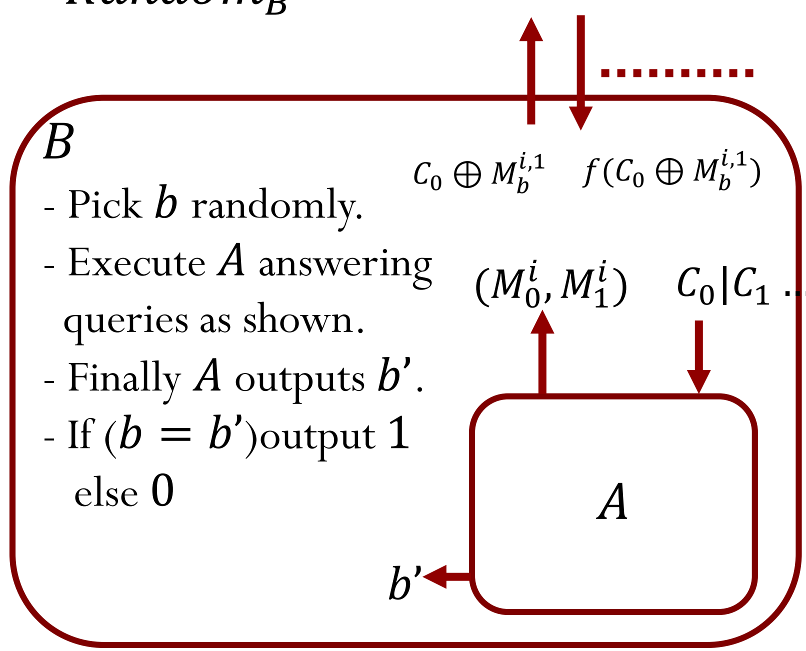
Morever, B makes at most σ oracle queries and has a running time $t + \theta(\sigma \cdot n)$.

$Real_{B,E}$



$$\Pr[Real_{B,E} = 1] = \frac{1}{2} + \frac{1}{2} \cdot Adv_{ind-cpa}(A, SE)$$

$Random_B$



$$\Pr[Random_B = 1] \leq \frac{1}{2} + \Pr[X]$$

X is the event that a "collision" happens

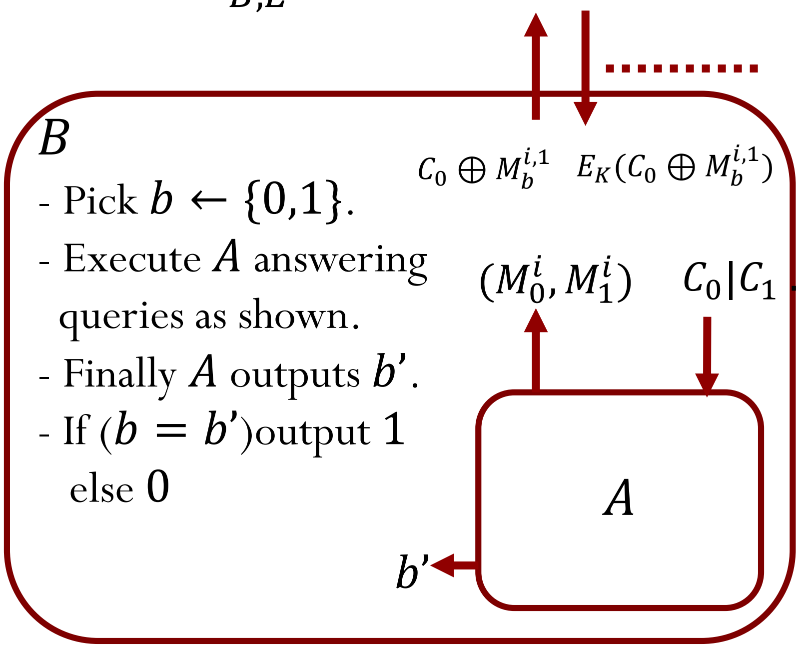
IND-CPA security of CBC$

- Theorem: Let $E: \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher and $SE = (E, D)$ be the corresponding CBC$ encryption scheme. Let A be an IND-CPA adversary that runs in time t and makes q queries totalling σ blocks. Then there is a PRF adversary B against E such that:

$$Adv_{ind-cpa}(A, SE) \leq 2 \cdot Adv_{PRF}(B, E) + \frac{\sigma^2}{2^n}.$$

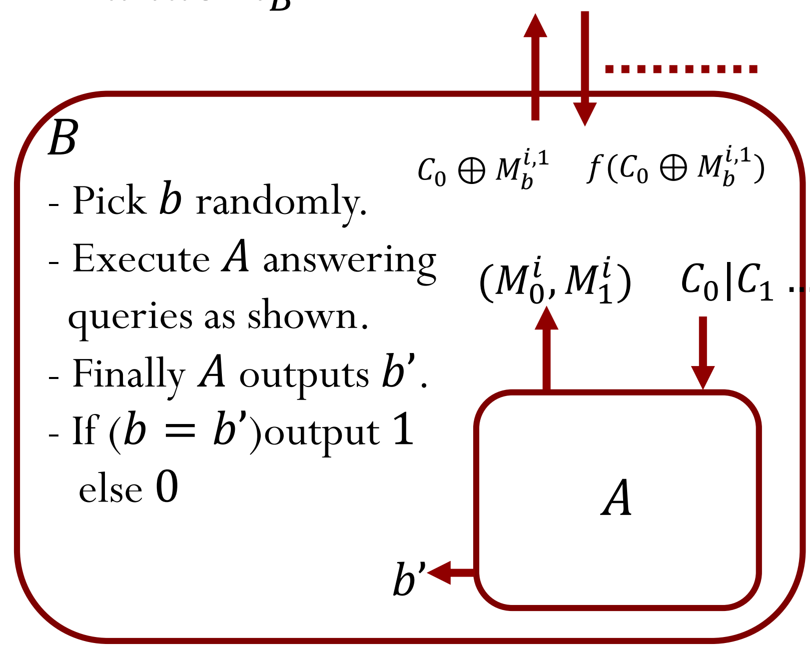
Morever, B makes at most σ oracle queries and has a running time $t + \theta(\sigma \cdot n)$.

$Real_{B,E}$



$$\Pr[Real_{B,E} = 1] = \frac{1}{2} + \frac{1}{2} \cdot Adv_{ind-cpa}(A, SE)$$

$Random_B$



$$\Pr[Random_B = 1] \leq \frac{1}{2} + C(\sigma, 2^n)$$

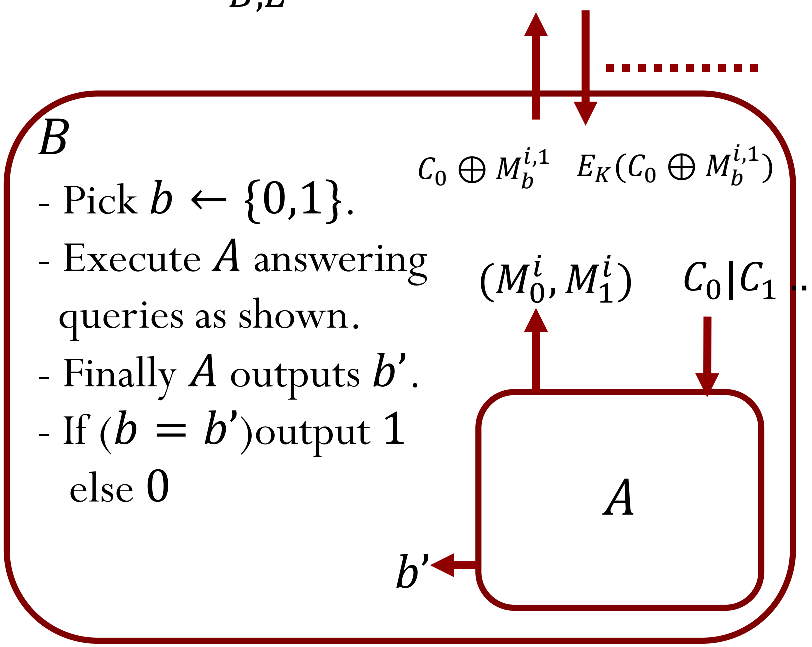
IND-CPA security of CBC$

- Theorem: Let $E: \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher and $SE = (E, D)$ be the corresponding CBC$ encryption scheme. Let A be an IND-CPA adversary that runs in time t and makes q queries totalling σ blocks. Then there is a PRF adversary B against E such that:

$$Adv_{ind-cpa}(A, SE) \leq 2 \cdot Adv_{PRF}(B, E) + \frac{\sigma^2}{2^n}.$$

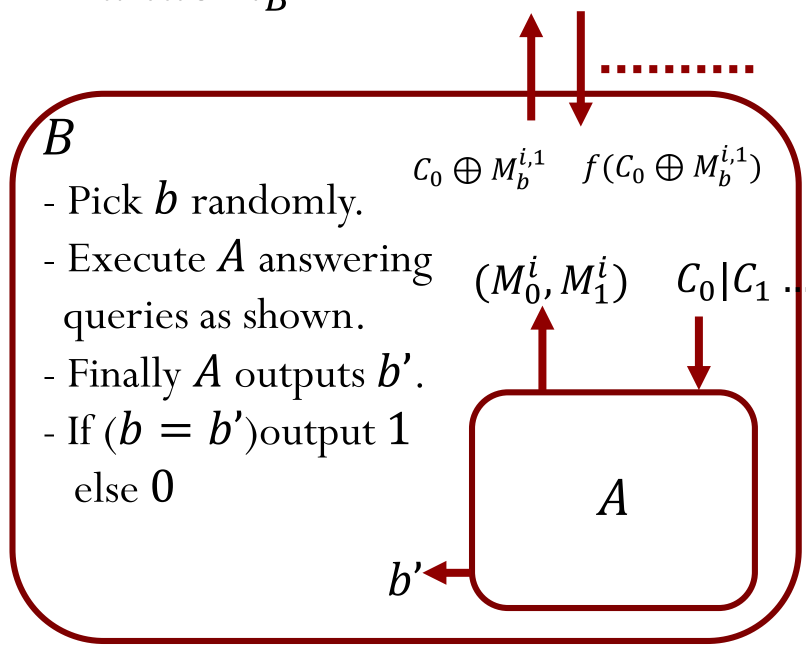
Morever, B makes at most σ oracle queries and has a running time $t + \theta(\sigma \cdot n)$.

$Real_{B,E}$



$$\Pr[Real_{B,E} = 1] = \frac{1}{2} + \frac{1}{2} \cdot Adv_{ind-cpa}(A, SE)$$

$Random_B$



$$\Pr[Random_B = 1] \leq \frac{1}{2} + \frac{\sigma^2}{2^{n+1}}.$$

CCA Security

Chosen Ciphertext Attack

CCA Security

- Chosen Ciphertext Attack scenario.

CCA Security

I am A

C

Decrypt C and send M'

- Chosen Ciphertext Attack scenario.

IND-CCA Security for Encryption Schemes

- $Left_{SE,A}$
  - Randomly pick key $K \leftarrow \{0,1\}^k$.
  - When A queries message pair (M_0^i, M_1^i) return $E_K(M_0^i)$ to A.
  - When A makes a decryption query C^j return $D_K(C^j)$.
  - Finally A outputs b.
  - Output b.

- $Right_{SE,A}$
  - Randomly pick key $K \leftarrow \{0,1\}^k$.
  - When A queries message pair (M_0^i, M_1^i) return $E_K(M_1^i)$ to A.
  - When A makes a decryption query C^j return $D_K(C^j)$.
  - Finally A outputs b.
  - Output b.

- The IND-CCA advantage of an adversary A is defined as follows:

  $$Adv_{ind-cca}(A, SE) = \left|\Pr\left[Left_{SE,A} = 1\right] - \Pr\left[Right_{SE,A} = 1\right]\right|$$

- A symmetric encryption scheme $SE = (E, D)$ is called (t, q, ϵ)-ind-cca secure if for every adversary A that runs in time $\leq t$ and asks $\leq q$ quesries, $Adv_{ind-cca}(A, SE) \leq \epsilon$.

IND-CCA Security for Encryption Schemes

- $Left_{SE,A}$
  - Randomly pick key $K \leftarrow \{0,1\}^k$.
  - When A queries message pair (M_0^i, M_1^i) return $E_K(M_0^i)$ to A.
  - When A makes a decryption query C^j return $D_K(C^j)$.
  - Finally A outputs b.
  - Output b.

- $Right_{SE,A}$
  - Randomly pick key $K \leftarrow \{0,1\}^k$.
  - When A queries message pair (M_0^i, M_1^i) return $E_K(M_1^i)$ to A.
  - When A makes a decryption query C^j return $D_K(C^j)$.
  - Finally A outputs b.
  - Output b.

- The IND-CCA advantage of an adversary A is defined as follows:

$$Adv_{ind-cca}(A, SE) = \left|\Pr\left[Left_{SE,A} = 1\right] - \Pr\left[Right_{SE,A} = 1\right]\right|$$

- Is there an issue with this definition?

IND-CCA Security for Encryption Schemes

- $Left_{SE,A}$
  - Randomly pick key $K \leftarrow \{0,1\}^k$.
  - When A queries message pair (M_0^i, M_1^i) return $E_K(M_0^i)$ to A.
  - When A makes a decryption query C^j return $D_K(C^j)$.
  - Finally A outputs b.
  - Output b.

- $Right_{SE,A}$
  - Randomly pick key $K \leftarrow \{0,1\}^k$.
  - When A queries message pair (M_0^i, M_1^i) return $E_K(M_1^i)$ to A.
  - When A makes a decryption query C^j return $D_K(C^j)$.
  - Finally A outputs b.
  - Output b.

- The IND-CCA advantage of an adversary A is defined as follows:

  $$Adv_{ind-cca}(A, SE) = \left|\Pr\left[Left_{SE,A} = 1\right] - \Pr\left[Right_{SE,A} = 1\right]\right|$$

- Is there an issue with this definition?
  - No encryption scheme can be ind-cca secure as per this definition.

IND-CCA Security for Encryption Schemes

- $Left_{SE,A}$
  - Randomly pick key $K \leftarrow \{0,1\}^k$.
  - When A queries message pair (M_0^i, M_1^i) return $E_K(M_0^i)$ to A.
  - When A makes a decryption query C^j return $D_K(C^j)$.
  - Finally A outputs b.
  - Output b.

- $Right_{SE,A}$
  - Randomly pick key $K \leftarrow \{0,1\}^k$.
  - When A queries message pair (M_0^i, M_1^i) return $E_K(M_1^i)$ to A.
  - When A makes a decryption query C^j return $D_K(C^j)$.
  - Finally A outputs b.
  - Output b.

- The IND-CCA advantage of an adversary A is defined as follows:
  $$Adv_{ind-cca}(A, SE) = \left|\Pr\left[Left_{SE,A} = 1\right] - \Pr\left[Right_{SE,A} = 1\right]\right|$$
- Is there an issue with this definition?
  - No encryption scheme can be ind-cca secure as per this definition.
- We only consider *valid* adversaries. These adversaries never make a decryption query C such that C is the reply of an earlier LR-query.

IND-CCA Security for Encryption Schemes

- $Left_{SE,A}$
  - Randomly pick key $K \leftarrow \{0,1\}^k$.
  - When A queries message pair (M_0^i, M_1^i) return $E_K(M_0^i)$ to A.
  - When A makes a decryption query C^j return $D_K(C^j)$.
  - Finally A outputs b.
  - Output b.

- $Right_{SE,A}$
  - Randomly pick key $K \leftarrow \{0,1\}^k$.
  - When A queries message pair (M_0^i, M_1^i) return $E_K(M_1^i)$ to A.
  - When A makes a decryption query C^j return $D_K(C^j)$.
  - Finally A outputs b.
  - Output b.

- The IND-CCA advantage of an adversary A is defined as follows:

$$Adv_{ind-cca}(A, SE) = \left|\Pr\left[Left_{SE,A} = 1\right] - \Pr\left[Right_{SE,A} = 1\right]\right|$$

- We only consider *valid* adversaries. These adversaries never make a decryption query C such that C is the reply of an earlier LR-query.
- Is IND-CCA security strictly stronger than IND-CPA?

IND-CCA Security for Encryption Schemes

- $Left_{SE,A}$
  - Randomly pick key $K \leftarrow \{0,1\}^k$.
  - When A queries message pair (M_0^i, M_1^i) return $E_K(M_0^i)$ to A.
  - When A makes a decryption query C^j return $D_K(C^j)$.
  - Finally A outputs b.
  - Output b.

- $Right_{SE,A}$
  - Randomly pick key $K \leftarrow \{0,1\}^k$.
  - When A queries message pair (M_0^i, M_1^i) return $E_K(M_1^i)$ to A.
  - When A makes a decryption query C^j return $D_K(C^j)$.
  - Finally A outputs b.
  - Output b.

- The IND-CCA advantage of an adversary A is defined as follows:
  $$Adv_{ind-cca}(A, SE) = \left|\Pr\left[Left_{SE,A} = 1\right] - \Pr\left[Right_{SE,A} = 1\right]\right|$$
- We only consider *valid* adversaries. These adversaries never make a decryption query C such that C is the reply of an earlier LR-query.
- Is IND-CCA security strictly stronger than IND-CPA?
  - Yes. A successful IND-CPA attack is also an IND-CCA attack.

IND-CCA Security for Encryption Schemes

- $Left_{SE,A}$
  - Randomly pick key $K \leftarrow \{0,1\}^k$.
  - When A queries message pair (M_0^i, M_1^i) return $E_K(M_0^i)$ to A.
  - When A makes a decryption query C^j return $D_K(C^j)$.
  - Finally A outputs b.
  - Output b.

- $Right_{SE,A}$
  - Randomly pick key $K \leftarrow \{0,1\}^k$.
  - When A queries message pair (M_0^i, M_1^i) return $E_K(M_1^i)$ to A.
  - When A makes a decryption query C^j return $D_K(C^j)$.
  - Finally A outputs b.
  - Output b.

- The IND-CCA advantage of an adversary A is defined as follows:
  $$Adv_{ind-cca}(A, SE) = \left|\Pr\left[Left_{SE,A} = 1\right] - \Pr\left[Right_{SE,A} = 1\right]\right|$$
- We only consider *valid* adversaries. These adversaries never make a decryption query C such that C is the reply of an earlier LR-query.
- IS CBC$(using a secure PRP) IND-CCA secure?

IND-CCA Security for Encryption Schemes

- IS CBC\$(using a secure PRP) IND-CCA secure?
- Adversary A
  - Make an LR query $(<0>,<1>)$ and let $C_0|C_1$ be the reply.
  - Make a decryption query $C_0 \oplus 100\ldots0|C_1$ and let M' be the reply.
  - If $(M = 10\ldots0)$ then output 1 else output 0.

- What is $\Pr[Left_{A,SE} = 1] = ?$
- What is $\Pr[Right_{A,SE} = 1] = ?$

IND-CCA Security for Encryption Schemes

- IS CBC$ IND-CCA secure?
- Adversary A
  - Make an LR query $(<0>,<1>)$ and let $C_0|C_1$ be the reply.
  - Make a decryption query $C_0 \oplus 100\ldots0|C_1$ and let M' be the reply.
  - If $(M = 10\ldots0)$ then output 0 else output 1.

- What is $\Pr[Left_{A,SE} = 1] = 1$.
- What is $\Pr[Right_{A,SE} = 1] = 0$.
- So, $Adv_{ind-cca}(A, SE) = 1$.

End