Symmetric Encryption Revisited

Chanathip Namprempre

Computer Science
Reed College

Agenda: Symmetric Encryption Revisted

1. Modes of operation
2. Security definitions for confidentiality
   - IND-CPA: definition and example attacks
   - IND-CPA security of CTR and CBC modes
   - IND-CCA: definition and example attacks

Recall Syntax of Symmetric Encryption

Syntax

A symmetric encryption scheme $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ is a triple of algorithms.

alg	input	output	notation	maybe randomized?	maybe stateful?
$\mathcal{K}$	-	key K	$K \xleftarrow{\$} \mathcal{K}$	yes	no
$\mathcal{E}$	$K \in Keys(\mathcal{SE})$ $M \in \{0,1\}^*$	ciphertext $C \in \{0,1\}^* \cup \{\perp\}$	$C \xleftarrow{\$} \mathcal{E}_K(M)$	yes	yes
$\mathcal{D}$	$K \in Keys(\mathcal{SE})$ $C \in \{0,1\}^*$	plaintext $M \in \{0,1\}^* \cup \{\perp\}$	$M \leftarrow \mathcal{D}_K(C)$	no	no

Correctness

For all $K \in Keys(\mathcal{SE})$ and all $M \in \{0,1\}^*$,

$$\Pr\left[C = \perp \text{ OR } \mathcal{D}_K(C) = M \;:\; C \xleftarrow{\$} \mathcal{E}_K(M) \right] = 1\,.$$

Modes of operation

OTP is impractical. Most symmetric encryption schemes use block ciphers as building block.

Let E be a block cipher.

idea

$$C \leftarrow E_K(M)$$

- But oftentimes, M is longer than the block length and/or isn't of the length multiple of the block length!
- So we need to figure out how to chop up M and/or pad it.
- There are many methods to do this. These methods are called modes of operation.

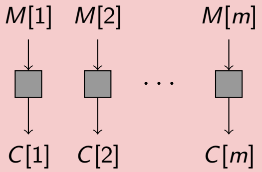
Electronic Code Book mode (ECB): key generation

Encryption scheme in ECB mode is **deterministic** and **stateless**.

Let $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher.

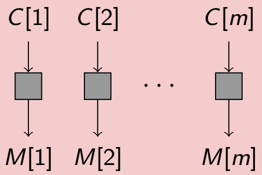
$\mathcal{K} : K \xleftarrow{\$} \{0,1\}^k$; return K
[This key generation algorithm will be used for all modes of operation.]

ECB: encryption and decryption



$\mathcal{E}_K(M)$:

  if $(|M| \bmod n \neq 0$ or $|M| = 0)$
  then return $\perp$
  Break M into n-bit blocks $M[1] \ldots M[m]$
  for $i \leftarrow 1$ to m do
    $C[i] \leftarrow E_K(M[i])$
  $C \leftarrow C[1] \ldots C[m]$
  return C

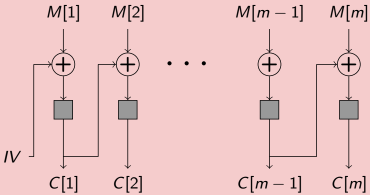


$\mathcal{D}_K(C)$:

  if $(|C| \bmod n \neq 0$ or $|C| = 0)$
  then return $\perp$
  Break C into n-bit blocks $C[1] \ldots C[m]$
  for $i \leftarrow 1$ to m do
    $M[i] \leftarrow E_K^{-1}(C[i])$
  $M \leftarrow M[1] \ldots M[m]$
  return M

Cipher Block Chaining mode ($CBC\$$): encryption and decryption

Encryption scheme in $CBC\$$ mode is **randomized** and **stateless**.



$\mathcal{E}_K(M)$:

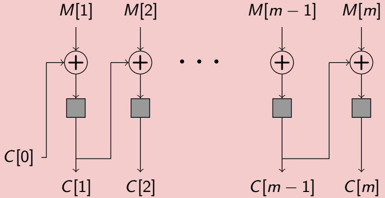
if $(|M| \bmod n \neq 0$ or $|M| = 0)$
then return $\perp$
Break M into n-bit blocks $M[1], \ldots, M[m]$
$C[0] \leftarrow IV \xleftarrow{\$} \{0,1\}^n$
for $i \leftarrow 1$ to m do
  $C[i] \leftarrow E_K(C[i-1] \oplus M[i])$
return $C[0] \| \ldots \| C[m]$

$\mathcal{D}_K(C)$:

??

Cipher Block Chaining mode ($CBCC$): encryption and decryption

Encryption scheme in $CBCC$ mode is **deterministic** and **stateful**.



$\mathcal{E}_K(M)$:
- if $(|M| \bmod n \neq 0$ or $|M| = 0)$
- then return $\perp$
- Break M into n-bit blocks $M[1], \ldots, M[m]$
- static $ctr \leftarrow 0$; $C[0] \leftarrow ctr$; $ctr \leftarrow ctr + 1$
- for $i \leftarrow 1$ to m do
  - $C[i] \leftarrow E_K(C[i-1] \oplus M[i])$
- return $C[0] \| \ldots \| C[m]$

$\mathcal{D}_K(C)$:

??

Counter mode

idea

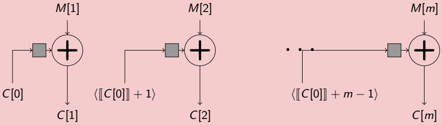
Try to be like OTP but use block cipher to generate the pad.

As usual, there are two versions:

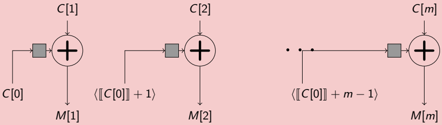
apply the block cipher to a random value	$\Longrightarrow$ *CTR$*
apply the block cipher to a counter	$\Longrightarrow$ *CTRC*

Counter mode (*CTRC*): encryption and decryption

Encryption scheme in *CTRC* mode is **deterministic** and **stateful**.



$\mathcal{E}_K(M)$:
- If $(|M| = 0)$ or $(|M| \bmod n \neq 0)$
  - then return $\perp$
- Parse M into n-bit blocks $M[1], \ldots, M[m]$
- static $ctr \leftarrow 0$; $C[0] \leftarrow ctr$
- $ctr \leftarrow ctr + m$
- if $ctr - 1 > 2^n - 1$ then return $\perp$
- For $i = 1$ to m do
  - $C[i] \leftarrow E_K(\langle [\![C[0]]\!] + i - 1 \rangle) \oplus M[i]$
- Return $C[0] \| \ldots \| C[m]$

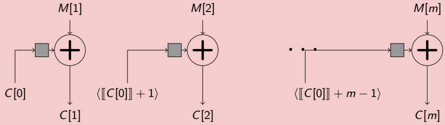


$\mathcal{D}_K(C)$:

??

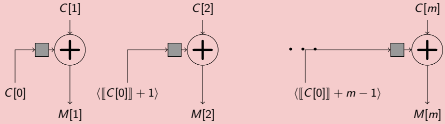
Counter mode ($CTR\$$): encryption and decryption

Encryption scheme in $CTR\$$ mode is **randomized** and **stateless**.



$\mathcal{E}_K(M)$:

If $(|M| = 0)$ or $(|M| \bmod n \neq 0)$
then return $\perp$
Parse M into n-bit blocks $M[1], \ldots, M[m]$
$C[0] \leftarrow IV \xleftarrow{\$} \{0,1\}^n$
For $i = 1$ to m do
$C[i] \leftarrow E_K(\langle [\![C[0]]\!] + i - 1 \rangle) \oplus M[i]$
Return $C[0] \| \ldots \| C[m]$



$\mathcal{D}_K(C)$:

??

Security definitions for confidentiality

Issues in confidentiality

Setting:

- First pick a key: $K \stackrel{\$}{\leftarrow} \mathcal{K}$
- sender and receiver know K
- adversary A does not know K
- adversary A can capture ciphertexts

What's considered insecure?

Definition for confidentiality: attempt 1

key recovery

From the ciphertexts, A can get K.

- For sure, this is true:
  A breaks key recovery $\Rightarrow$ scheme is insecure
- What about the inverse?
- counterexample: can you think of an encryption scheme secure under key recovery but does nothing to hide the message?

Definition for confidentiality: attempt 2

plaintext recovery

From the ciphertexts, A can get M.

What if the message format is such that some bits are more important than others?

In this case, what if A can't get the whole message M but can get at those important bits?

Definition for confidentiality: attempt 3

partial information recovery

From the ciphertexts, A can get partial information about M.

But which bits do we want to protect???

- 1st bit?
- i-th bit?
  For example, suppose
  the i-th bit of the plaintext is 0 iff we want to sell stock
- sum of all bits?

Bottom line :
We don't want to make assumptions about data format!

Definition for confidentiality

- We need to approach this more directly:
  $\boxed{\text{Q}}$: What would an ideal encryption scheme look like?

  $\boxed{\text{A}}$: An angel delivers your messages, i.e.
  no partial information gets leaked!

- We want to approximate this.
  [but we can't help but leak the length of M]

  So we aim for this :

A secure scheme shouldn't let A relate ciphertexts of messages of the same length.

Examples of insecure scheme: ECB

A can get information even if A can't break the block cipher.

example

$$
\begin{aligned}
0^n &= \text{don't fire missile} \\
1^n &= \text{fire missile}
\end{aligned}
$$

Suppose the two commands are to fire missiles.

1. A sees the first ciphertext C_0 followed by a missile.
2. A sees the second ciphertext C_1, which looks exactly the same as C_0.
3. What would A do??

Bottom line :
For ECB, ciphertexts of messages with the same contents look exactly the same!

Definition for confidentiality: first lesson

A secure encryption scheme cannot be both deterministic and stateless.

- one message should correspond to many possible ciphertexts.
- This is not what's historically done.

Indistinguishability against chosen-plaintext attacks IND-CPA

<u>Idea</u>

- Pick a hidden bit b at random.
- Let A choose two messages.
- One of the messages will get encrypted.
- The resulting ciphertext is given to A.
- A guesses what b is.

IND-CPA

Subroutine *Initialize*

$b \xleftarrow{\$} \{0,1\}$; $K \xleftarrow{\$} KG$

Subroutine $\texttt{Enc}(M_0, M_1)$

If $|M_0| \neq |M_1|$ then return $\perp$

Return $\mathrm{Enc}_K(M_b)$

Subroutine *Finalize*(d)

Return $(d = b)$

Experiment $\mathbf{Exp}^{\text{ind-cpa}}_{\mathsf{SE}}(A)$

Initialize

$d \xleftarrow{\$} A^{\texttt{Enc}}$

Return *Finalize*(d)

ind-cpa advantage

The **ind-cpa advantage** of an adversary A mounting a chosen-ciphertext attack against SE is

$$\mathbf{Adv}^{\text{ind-cpa}}_{\mathsf{SE}}(A) = 2 \cdot \Pr\left[\, \mathbf{Exp}^{\text{ind-cpa}}_{\mathsf{SE}}(A) \Rightarrow \text{true} \,\right] - 1 \; .$$

IND-CPA: observations

- $\mathcal{SE}$ is secure against IND-CPA if an adversary restricted to **practical** amount of resources can't obtain **significant** advantage.
- resources are
  1. time
     - the running time of A (over all coins of A and all return values)
     - size of A's code
     - time spent by A to read bits returned from oracle (return values in unit time)
  2. number of bits queried
     [length of query (M_0, M_1) = max length of M_0 and M_1]
  3. number of queries submitted

Bottom line : IND-CPA captures confidentiality.

IND-CPA: observations

As we'll see,

$$\begin{array}{lcl} \text{IND-CPA} & \Rightarrow & \text{key recovery is hard.} \\ & \Rightarrow & \text{message recovery is hard.} \\ & \Rightarrow & \text{partial information recovery is hard.} \\ & & \ldots \end{array}$$

Example IND-CPA attacks

Proposition : ECB is insecure.

Let $E : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$. Let $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be the ECB encryption scheme based on E. Then, there exists an ind-cpa adversary A such that,

$$Adv^{\text{ind-cpa}}_{\mathcal{SE}}(A) = 1$$

and A runs in time $O(n)$ and asks 1 query totalling $2n$ bits.

Notice

ECB is bad *even if* E is a perfectly good block cipher!
This is a design flaw!

Proposition : Any deterministic and stateless schemes are insecure.

Let $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be the deterministic, stateless symmetric encryption scheme.

Assume that there's an integer m such that the plaintext space of the scheme cantains at least 2 distinct strings of length m. Then, there is an adversary A such that

$$Adv_{\mathcal{SE}}^{\mathrm{ind\text{-}cpa}}(A) = 1$$

and A runs in time $O(m)$ and asks 2 queries totalling $2m$ bits.

Proposition : CBCC is insecure.

Let $E : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$.
Let $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be the CBCC scheme based on E.
Then, there exists A such that

$$Adv_{\mathcal{SE}}^{\text{ind-cpa}}(A) = 1$$

and A runs in time $O(n)$ and asking 2 queries totalling $2n$ bits.

Indistinguishability against chosen-ciphertext attacks IND-CCA: idea

- Similar to IND-CPA except that we also let A ask for decryption of ciphertexts of its choice.
- But to prevent a trivial attack, we do not let A ask for the decryption of the ciphertexts that it got back from the encryption oracle.
- Similar to IND-CPA, we also allow multiple adaptive queries.

IND-CCA: Left-or-right indistinguishability against chosen-ciphertext attacks: formal definition

Subroutine *Initialize*
$b \xleftarrow{\$} \{0,1\}$; $K \xleftarrow{\$} KG$; $S \leftarrow \emptyset$

Subroutine $\mathtt{Enc}(M_0, M_1)$
If $|M_0| \neq |M_1|$ then return $\perp$
Return $\mathrm{Enc}_K(M_b)$

Subroutine $\mathtt{Dec}(C)$
If $C \in S$ then return $\perp$
Return $\mathrm{Dec}_K(C)$

Subroutine *Finalize*(d)
Return $(d = b)$

Experiment $\mathbf{Exp}_{\mathsf{SE}}^{\text{ind-cca}}(A)$
Initialize
$d \xleftarrow{\$} A^{\mathtt{Enc},\mathtt{Dec}}$
Return *Finalize*(d)

ind-cca advantage

The **ind-cca advantage** of an adversary A mounting a chosen-ciphertext attack against SE is

$$\mathbf{Adv}_{\mathsf{SE}}^{\text{ind-cca}}(A) = 2 \cdot \Pr\left[\mathbf{Exp}_{\mathsf{SE}}^{\text{ind-cca}}(A) \Rightarrow \text{true}\right] - 1 .$$

Example IND-CCA attacks

Proposition : *CTR*\$ is insecure against chosen-ciphertext attacks.

Let $E : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^l$ be a family of functions. Let $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be the *CTR*\$ encryption scheme based on E. Then, there exists an ind-cca adversary A such that,

$$Adv^{\text{ind-cca}}_{\mathcal{SE}}(A) = 1$$

and A runs in time $O(n + l)$ plus the time for one application of E and asks 1 query totalling l bits to the encryption oracle and 1 query totalling $n + l$ bits to the decryption oracle.

Note

CTR\$ is secure against IND-CPA but insecure against IND-CCA.

Proposition : *CBC\$* is insecure against chosen-ciphertext attacks.

Let $E : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$ be a family of functions. Let $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be the *CBC\$* encryption scheme based on E. Then, there exists an ind-cca adversary A such that,

$$Adv_{\mathcal{SE}}^{\text{ind-cca}}(A) = 1$$

and A runs in time $O(n)$ plus the time for one application of E and asks 1 query totalling n bits to the encryption oracle and 1 query totalling $2n$ bits to the decryption oracle.

Note

CBC\$ is secure against IND-CPA but insecure against IND-CCA.

Proving positive results

CTR\$ and *CTRC* are secure under IND-CPA

proposition: *CTRC* is secure under IND-CPA

Let $E : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$ be a family of functions and let $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be the *CTRC* encryption scheme. Let A be an ind-cpa adversary that runs in time at most t and asks at most q queries, each of length at most m^* n-bit blocks. Then, there exists a prf adversary B such that

$$Adv_{\mathcal{SE}}^{\mathrm{ind\text{-}cpa}}(A) \leq 2 \cdot Adv_{E}^{\mathrm{prf}}(B) \; .$$

Furthermore, B runs in time at most $t' = t + O(q + nqm^*)$ and asks at most $q' = qm^*$ oracle queries.

proposition: *CTR*\$ is secure under IND-CPA

Let $E : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$ be a family of functions and let $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be the *CTR*\$ encryption scheme. Let A be an ind-cpa adversary that runs in time at most t and asks at most q queries, each of length at most m^* n-bit blocks. Then, there exists a prf adversary B such that

$$Adv_{\mathcal{SE}}^{\mathrm{ind\text{-}cpa}}(A) \leq 2 \cdot Adv_{E}^{\mathrm{prf}}(B) + \frac{q^2 m^*}{2^n} \; .$$

Furthermore, B runs in time at most $t' = t + O(q + nqm^*)$ and asks at most $q' = qm^*$ oracle queries.

CBC\$ is secure under IND-CPA

proposition

Let $E : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$ be a family of functions and let $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be the *CBC\$* encryption scheme. Let A be an ind-cpa adversary that runs in time at most t and asks at most q queries, these totalling at most σ n-bit blocks. Then there exists a prf adversary B such that

$$Adv^{\text{ind-cpa}}_{\mathcal{SE}}(A) \leq Adv^{\text{prf}}_{E}(B) + \frac{\sigma^2}{2^{n+1}} .$$

Furthermore B runs in time at most $t' = t + O(q + n\sigma)$ and asks at most $q' = \sigma$ oracle queries.

CTRC is secure under IND-CPA: Game-Hopping Proof

Let $E : \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$ be the underlying block cipher. Let A be an IND-CPA adversary making q queries the maximum length of which is m^* blocks long.

Game $G0$

$b \xleftarrow{\$} \{0,1\}$; $K \xleftarrow{\$} KG$
$ctr \leftarrow 0$; $d \leftarrow A^{\mathrm{Enc}}$
Return $(d = b)$

$\underline{\mathtt{Enc}(M_0, M_1)}$
If $|M_0| \neq |M_1|$ then return $\perp$
Parse M_b into m blocks
Let i be the current query number
$C_i[0] \leftarrow ctr$; $ctr \leftarrow ctr + m$
For $j = 1$ to m do
$X_i[j] \leftarrow C_i[0] + j - 1$
$P_i[j] \leftarrow E_K(X_i[j])$
$C_i[j] \leftarrow P_i[j] \oplus M_b[j]$
Return $C_i[0] \| \ldots \| C_i[m]$

Game $G1$

$b \xleftarrow{\$} \{0,1\}$; $f \xleftarrow{\$} Func(n,n)$
$ctr \leftarrow 0$; $d \leftarrow A^{\mathrm{Enc}}$
Return $(d = b)$

$\underline{\mathtt{Enc}(M_0, M_1)}$
If $|M_0| \neq |M_1|$ then return $\perp$
Parse M_b into m blocks
Let i be the current query
$C_i[0] \leftarrow ctr$; $ctr \leftarrow ctr + m$
For $j = 1$ to m do
$X_i[j] \leftarrow C_i[0] + j - 1$
$P_i[j] \leftarrow f(X_i[j])$
$C_i[j] \leftarrow P_i[j] \oplus M_b[j]$
Return $C_i[0] \| \ldots \| C_i[m]$

Game $G2$

$b \xleftarrow{\$} \{0,1\}$; $ctr \leftarrow 0$
$d \leftarrow A^{\mathrm{Enc}}$
For $i = 1$ to q
For $j = 1$ to m^*
$P_i[j] \xleftarrow{\$} \{0,1\}^n$
Return $(d = b)$

$\underline{\mathtt{Enc}(M_0, M_1)}$
If $|M_0| \neq |M_1|$ then return $\perp$
Parse M_b into m blocks
Let i be the current query
$C_i[0] \leftarrow ctr$; $ctr \leftarrow ctr + m$
For $j = 1$ to m do
$C_i[j] \leftarrow P_i[j] \oplus M_b[j]$
Return $C_i[0] \| \ldots \| C_i[m]$

CTRC is secure under IND-CPA: Game-Hopping Proof

Recall that

$$\mathbf{Adv}^{\mathrm{ind\text{-}cpa}}_{\mathsf{SE}}(A) = 2 \cdot \Pr\left[\, \mathbf{Exp}^{\mathrm{ind\text{-}cpa}}_{\mathsf{SE}}(A) \Rightarrow \mathsf{true} \,\right] - 1 \,.$$

Notice that

$$\begin{aligned}\Pr\left[\, \mathbf{Exp}^{\mathrm{ind\text{-}cpa}}_{\mathsf{SE}}(A) \Rightarrow \mathsf{true} \,\right] &= \Pr[\, G0(A) \Rightarrow \mathsf{true} \,] \\ &= \Pr[\, G0(A) \Rightarrow \mathsf{true} \,] + \Pr[\, G1(A) \Rightarrow \mathsf{true} \,] - \Pr[\, G1(A) \Rightarrow \mathsf{true} \,]\end{aligned}$$

We construct an adversary B attacking E in PRF game as follows:

Adversary B^g

$w \xleftarrow{\$} \{0,1\}$; $ctr \leftarrow 0$
Run A replying to its encryption queries (M_0, M_1) as follows:
  If $|M_0| \neq |M_1|$ then return $\perp$
  Parse M_w into m blocks
  Let i be the current query number
  $C_i[0] \leftarrow ctr$; $ctr \leftarrow ctr + m$
  For $j = 1$ to m do
    $X_i[j] \leftarrow C_i[0] + j - 1$
    $P_i[j] \leftarrow g(X_i[j])$
    $C_i[j] \leftarrow P_i[j] \oplus M_b[j]$
  Return $C_i[0] \| \ldots \| C_i[m]$ to A
Once A finishes running, it returns a bit d
If $d = w$ then return 0 else return 1.

CTRC is secure under IND-CPA: Game-Hopping Proof

Let b be the bit in the PRF game in which B plays.

$$
\begin{aligned}
&\Pr[\, G0(A) \Rightarrow \text{true} \,] + \Pr[\, G1(A) \Rightarrow \text{true} \,] && (1)\\
&\leq \Pr\left[\mathbf{Exp}_E^{\mathrm{prf}}(B) \Rightarrow \text{true} \mid b = 1 \right] + \Pr\left[\mathbf{Exp}_E^{\mathrm{prf}}(B) \Rightarrow \text{true} \mid b = 0 \right] && (2)\\
&= \Pr\left[\mathbf{Exp}_E^{\mathrm{prf}}(B) \Rightarrow \text{true} \mid b = 1 \right] + \left(1 - \Pr\left[\mathbf{Exp}_E^{\mathrm{prf}}(B) \Rightarrow \text{false} \mid b = 0 \right]\right) && (3)\\
&= \Pr\left[\mathbf{Exp}_E^{\mathrm{prf}}(B) \Rightarrow \text{true} \mid b = 1 \right] - \Pr\left[\mathbf{Exp}_E^{\mathrm{prf}}(B) \Rightarrow \text{false} \mid b = 0 \right] + 1 && (4)\\
&= \mathbf{Adv}_E^{\mathrm{prf}}(B) + 1 && (5)
\end{aligned}
$$

Or more relatably,

$$
\Pr[\, A \text{ guesses correctly when } E \text{ is real} \,] + \Pr[\, A \text{ guesses correctly when E is random} \Rightarrow \text{true} \,]
$$

$$
\begin{aligned}
&\leq \Pr[\, B \text{ guesses correctly when } g \text{ is real} \,] + \Pr[\, B \text{ guesses correctly when } g \text{ is random} \,]\\
&= \Pr[\, B \text{ guesses correctly when } g \text{ is real} \,] + (1 - \Pr[\, B \text{ guesses wrong when } g \text{ is random} \,])\\
&= \Pr[\, B \text{ guesses correctly when } g \text{ is real} \,] - \Pr[\, B \text{ guesses wrong when } g \text{ is random} \,] + 1\\
&= \mathbf{Adv}_E^{\mathrm{prf}}(B) + 1
\end{aligned}
$$

CTRC is secure under IND-CPA: Game-Hopping Proof

$$
\begin{aligned}
\Pr\left[\, \mathbf{Exp}_{\mathsf{SE}}^{\text{ind-cpa}}(A) \Rightarrow \mathsf{true} \,\right] &= \Pr[\, G0(A) \Rightarrow \mathsf{true} \,] + \Pr[\, G1(A) \Rightarrow \mathsf{true} \,] - \Pr[\, G1(A) \Rightarrow \mathsf{true} \,] && (6)\\
&\le \mathbf{Adv}_{E}^{\text{prf}}(B) + 1 - \Pr[\, G1(A) \Rightarrow \mathsf{true} \,] && (7)\\
&= \mathbf{Adv}_{E}^{\text{prf}}(B) + 1 - \Pr[\, G1(A) \Rightarrow \mathsf{true} \,] + \Pr[\, G2(A) \Rightarrow \mathsf{true} \,] - \Pr[\, G2(A) \Rightarrow \mathsf{true} \,] && (8)\\
&= \mathbf{Adv}_{E}^{\text{prf}}(B) + 1 - \Pr[\, G2(A) \Rightarrow \mathsf{true} \,] && (9)\\
&= \mathbf{Adv}_{E}^{\text{prf}}(B) + 1 - \frac{1}{2} && (10)
\end{aligned}
$$

Equation (9) follows from Equation (8) because

$$\Pr[\, G1(A) \Rightarrow \mathsf{true} \,] = \Pr[\, G2(A) \Rightarrow \mathsf{true} \,] \ .$$

Equation (10) follows from Equation (9) because

$$\Pr[\, G2(A) \Rightarrow \mathsf{true} \,] = \frac{1}{2} \ .$$

Substituting Equation (10) into the definition for $\mathbf{Adv}^{\text{ind-cpa}}$, we get

$$
\begin{aligned}
\mathbf{Adv}_{\mathsf{SE}}^{\text{ind-cpa}}(A) &\le 2 \cdot \left(\mathbf{Adv}_{E}^{\text{prf}}(B) + 1 - \frac{1}{2} \right) - 1\\
&= 2 \cdot \mathbf{Adv}_{E}^{\text{prf}}(B) + 2 - 1 - 1\\
&= 2 \cdot \mathbf{Adv}_{E}^{\text{prf}}(B) \ .
\end{aligned}
$$

CTR\$ is secure under IND-CPA: Game-Hopping Proof

Let $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be the underlying block cipher. Let A be an IND-CPA adversary making q queries the maximum length of which is m^* blocks long.

Game $G0$

$b \xleftarrow{\$} \{0,1\}$; $K \xleftarrow{\$} KG$
$d \leftarrow A^{\mathtt{Enc}}$
Return $(d = b)$

$\underline{\mathtt{Enc}(M_0, M_1)}$
If $|M_0| \neq |M_1|$
then return $\perp$
Parse M_b into m blocks
Let i be the current query
$C_i[0] \xleftarrow{\$} \{0,1\}^n$
For $j = 1$ to m do
$X_i[j] \leftarrow C_i[0] + j - 1$
$P_i[j] \leftarrow E_K(X_i[j])$
$C_i[j] \leftarrow P_i[j] \oplus M_b[j]$
Return $C_i[0] \| \ldots \| C_i[m]$

Game $G1$

$b \xleftarrow{\$} \{0,1\}$; $f \xleftarrow{\$} Func(n,n)$
$d \leftarrow A^{\mathtt{Enc}}$
Return $(d = b)$

$\underline{\mathtt{Enc}(M_0, M_1)}$
If $|M_0| \neq |M_1|$
then return $\perp$
Parse M_b into m blocks
Let i be the current query
$C_i[0] \xleftarrow{\$} \{0,1\}^n$
For $j = 1$ to m do
$X_i[j] \leftarrow C_i[0] + j - 1$
$P_i[j] \leftarrow f(X_i[j])$
$C_i[j] \leftarrow P_i[j] \oplus M_b[j]$
Return $C_i[0] \| \ldots \| C_i[m]$

Game $G2$

$b \xleftarrow{\$} \{0,1\}$; $d \leftarrow A^{\mathtt{Enc}}$
For $i = 1$ to q
For $j = 1$ to m^*
$P_i[j] \xleftarrow{\$} \{0,1\}^n$
Return $(d = b)$

$\underline{\mathtt{Enc}(M_0, M_1)}$
If $|M_0| \neq |M_1|$
then return $\perp$
Parse M_b into m blocks
Let i be the current query
$C_i[0] \xleftarrow{\$} \{0,1\}^n$
For $j = 1$ to m do
$X_i[j] \leftarrow C_i[0] + j - 1$
$C_i[j] \leftarrow P_i[j] \oplus M_b[j]$
If $X_i[j] = X'_i[j']$ for some $(i', j') < (i, j)$
then $P_i[j] \leftarrow P'_i[j']$
Return $C_i[0] \| \ldots \| C_i[m]$

$CTR\$$ is secure under IND-CPA: Game-Hopping Proof

Let $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be the underlying block cipher. Let A be an IND-CPA adversary making q queries the maximum length of which is m^* blocks long.

Game $G2$

$b \xleftarrow{\$} \{0,1\}$; $d \leftarrow A^{\mathrm{Enc}}$
For $i = 1$ to q
  For $j = 1$ to m^*
    $P_i[j] \xleftarrow{\$} \{0,1\}^n$
Return $(d = b)$

$\underline{\mathtt{Enc}(M_0, M_1)}$
If $|M_0| \neq |M_1|$
  then return $\perp$
Parse M_b into m blocks
Let i be the current query
$C_i[0] \xleftarrow{\$} \{0,1\}^n$
For $j = 1$ to m do
  $X_i[j] \leftarrow C_i[0] + j - 1$
  $C_i[j] \leftarrow P_i[j] \oplus M_b[j]$
  If $X_i[j] = X_i'[j']$ for some $(i', j') < (i, j)$
    then $P_i[j] \leftarrow P_i'[j']$
Return $C_i[0] \| \ldots \| C_i[m]$

Game $G3$

$b \xleftarrow{\$} \{0,1\}$; $d \leftarrow A^{\mathrm{Enc}}$
For $i = 1$ to q
  For $j = 1$ to m^*
    $P_i[j] \xleftarrow{\$} \{0,1\}^n$
Return $(d = b)$

$\underline{\mathtt{Enc}(M_0, M_1)}$
If $|M_0| \neq |M_1|$
  then return $\perp$
Parse M_b into m blocks
Let i be the current query
$C_i[0] \xleftarrow{\$} \{0,1\}^n$
For $j = 1$ to m do
  $C_i[j] \leftarrow P_i[j] \oplus M_b[j]$
Return $C_i[0] \| \ldots \| C_i[m]$

Difference Lemma

Fix a sample space. If two events are identical unless a particular (bad) event occurs, then the difference in the probabilities of the two events is bounded by the probability of the particular (bad) event.

Theorem 4.7 [Boneh-Shoup]. Let Z, W_0, W_1 be events defined over some probability space, and let $\overline{Z}$ denote the complement of the event Z. Suppose that $W_0 \wedge \overline{Z}$ occurs iff $W_1 \wedge \overline{Z}$ occurs. Then, we have

$$\Pr[\, W_0 \,] - \Pr[\, W_1 \,] \leq \Pr\left[\, \overline{Z} \,\right] .$$

Proof. We have

$$\begin{aligned}
\Pr[\, W_0 \,] - \Pr[\, W_1 \,] &= \Pr[\, W_0 \wedge Z \,] + \Pr\left[\, W_0 \wedge \overline{Z} \,\right] \\
&\quad - \Pr[\, W_1 \wedge Z \,] - \Pr\left[\, W_1 \wedge \overline{Z} \,\right] \\
&= \Pr[\, W_0 \wedge Z \,] - \Pr[\, W_1 \wedge Z \,] \\
&\leq \Pr[\, Z \,] .
\end{aligned}$$

$CTR\$$ is a little bit worse than $CTRC$

Let W_0 be the event that $G2(A) \Rightarrow \text{true}$.
Let W_1 be the event that $G3(A) \Rightarrow \text{true}$.
Let Z be the event that $\exists(i', j') < (i, j)$ such that $X_i[j] = X_i'[j']$.

Observation:

$$\boxed{W_0 \text{ and } W_1 \text{ are the same as long as } Z \text{ does not occurr.}}$$

Game $G2$

$b \xleftarrow{\$} \{0,1\}$; $d \leftarrow A^{\mathrm{Enc}}$
For $i = 1$ to q
  For $j = 1$ to m^*
    $P_i[j] \xleftarrow{\$} \{0,1\}^n$
Return $(d = b)$

$\underline{\mathtt{Enc}(M_0, M_1)}$
If $|M_0| \neq |M_1|$
  then return $\perp$
Parse M_b into m blocks
Let i be the current query
$C_i[0] \xleftarrow{\$} \{0,1\}^n$
For $j = 1$ to m do
  $X_i[j] \leftarrow C_i[0] + j - 1$
  $C_i[j] \leftarrow P_i[j] \oplus M_b[j]$
  If $X_i[j] = X_i'[j']$ for some $(i', j') < (i, j)$
    then $P_i[j] \leftarrow P_i'[j']$
Return $C_i[0] \| \dots \| C_i[m]$

Game $G3$

$b \xleftarrow{\$} \{0,1\}$; $d \leftarrow A^{\mathrm{Enc}}$
For $i = 1$ to q
  For $j = 1$ to m^*
    $P_i[j] \xleftarrow{\$} \{0,1\}^n$
Return $(d = b)$

$\underline{\mathtt{Enc}(M_0, M_1)}$
If $|M_0| \neq |M_1|$
  then return $\perp$
Parse M_b into m blocks
Let i be the current query
$C_i[0] \xleftarrow{\$} \{0,1\}^n$
For $j = 1$ to m do
  $C_i[j] \leftarrow P_i[j] \oplus M_b[j]$
Return $C_i[0] \| \dots \| C_i[m]$

CTR\$ Game Hopping

$G0$: *CTR*\$ based on E
$G1$: *CTR*\$ based on a random function f
$G2$: *CTR*\$ in which the pad blocks are chosen independently and uniform-randomly from each other while being mindful of repeated inputs to (what used to be) the block cipher
$G3$: *CTR*\$ in which the pad blocks are chosen independently and uniform-randomly from each other

$$
\begin{aligned}
\Pr[\,G0(A) \Rightarrow \text{true}\,] + \Pr[\,G1(A) \Rightarrow \text{true}\,] &= \mathbf{Adv}_E^{\text{ind-cpa}}(B) + 1 \\
\Pr[\,G1(A) \Rightarrow \text{true}\,] &= \Pr[\,G2(A) \Rightarrow \text{true}\,] \\
\Pr[\,G2(A) \Rightarrow \text{true}\,] - \Pr[\,G3(A) \Rightarrow \text{true}\,] &\le \Pr[\,\text{repeated inputs occur}\,] \\
&\le \frac{q^2 m^*}{2^n} \\
\Pr[\,G3(A) \Rightarrow \text{true}\,] &= \frac{1}{2}
\end{aligned}
$$

See Boneh-Shoup p. 193 Equation (5.20) for the third inequality.