Symmetric Encryption

Mike Reiter

Based on Chapter 5 of Bellare and Rogaway, "Introduction to Modern Cryptography".

A symmetric encryption scheme is a triple \( SE = \langle K, E, D \rangle \) of efficiently computable algorithms

- \( K \) is a randomized “key generation algorithm” that outputs a “key”
  \[ K \leftarrow K() \]
  We let \( \text{Keys}(SE) \) denote all keys that are output by \( K() \) with nonzero probability.

- \( E \) is a randomized or stateful “encryption algorithm” that takes a key \( K \) and “plaintext” \( M \in \{0,1\}^* \) as input, and outputs \( \perp \) or a “ciphertext”
  \[ C \leftarrow E_K(M) \]
  The “plaintext space” is \( \{M : E_K(M) \neq \perp\} \).

- \( D \) takes a ciphertext \( C \) and key \( K \) as input, and outputs \( \perp \) or a plaintext
  \[ M \leftarrow D_K(C) \]

If \( C \leftarrow E_K(M) \) and \( C \neq \perp \) then \( M \leftarrow D_K(C) \)
One-Time Pad Encryption

Algorithm $\mathcal{K}(\cdot)$:
\[ K \leftarrow \{0,1\}^k \]

Algorithm $\mathcal{E}_K(M)$:
\[ \text{static } ctr \leftarrow 0 \]
\[ m \leftarrow |M| \]
\[ \text{if } (ctr + m > k) \text{ return } \bot \]
\[ C \leftarrow M \oplus K[ctr \ldots ctr + m - 1] \]
\[ ctr \leftarrow ctr + m \]

Algorithm $\mathcal{D}_K((ctr, C))$:
\[ m \leftarrow |M| \]
\[ \text{if } (ctr + m > k) \text{ return } \bot \]
\[ M \leftarrow C \oplus K[ctr \ldots ctr + m - 1] \]

ECB Encryption

- ECB = “Electronic Code Book”
- Let $f : \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$ be a pseudorandom permutation

Algorithm $\mathcal{K}(\cdot)$:
\[ K \leftarrow \{0,1\}^k \]

Algorithm $\mathcal{E}_K(M)$:
\[ \text{if } (|M| \mod n \neq 0 \text{ or } |M| = 0) \text{ return } \bot \]
\[ M_1 | \ldots | M_m \leftarrow M : M_i \in \{0,1\}^n \]
\[ \text{for } i = 1 \ldots m \text{ do } C_i \leftarrow f_K(M_i) \]
\[ \text{return } C_1 | \ldots | C_m \]

Algorithm $\mathcal{D}_K(C)$:
\[ \text{if } (|C| \mod n \neq 0 \text{ or } |C| = 0) \text{ return } \bot \]
\[ C_1 | \ldots | C_m \leftarrow C : C_i \in \{0,1\}^n \]
\[ \text{for } i = 1 \ldots m \text{ do } M_i \leftarrow f_K^{-1}(C_i) \]
\[ \text{return } M_1 | \ldots | M_m \]
Randomized CBC Encryption

- "CBC" = Cipher Block Chaining
- Let \( f: \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n \) be a pseudorandom permutation

Algorithm \( E_K(M) \):

1. if (|M| mod \( n \) ≠ 0 or |M| = 0) return ⊥
2. \( M_1|...|M_m \leftarrow M: M_i \in \{0,1\}^n \)
3. \( C_0 \leftarrow \{0,1\}^n \)
4. for \( i = 1...m \) do \( C_i \leftarrow f_K(C_{i-1} \oplus M_i) \)
5. return \( C_0 \mid C_1 \mid ... \mid C_m \)

Algorithm \( D_K(C) \):

1. if (|C| mod \( n \) ≠ 0 or |C| = 0) return ⊥
2. \( C_0 \mid C_1 \mid ... \mid C_m = C: C_i \in \{0,1\}^n \)
3. for \( i = 1...m \) do \( M_i \leftarrow f_K^{-1}(C_i) \oplus C_{i-1} \)
4. return \( M_1 \mid ... \mid M_m \)

Stateful CBC Encryption

- Let \( f: \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n \) be a pseudorandom permutation

Algorithm \( E_K(M) \):

1. static ctr ← 0
2. if (|M| mod \( n \) ≠ 0 or |M| = 0) return ⊥
3. \( M_1|...|M_m \leftarrow M: M_i \in \{0,1\}^n \)
4. if (ctr + \( m \) ≥ \( 2^n \)) return ⊥
5. \( C_0 \leftarrow ctr \)
6. for \( i = 1...m \) do \( C_i \leftarrow f_K(C_{i-1} \oplus M_i) \)
7. \( ctr \leftarrow ctr + m \)
8. return \( C_0 \mid C_1 \mid ... \mid C_m \)

Algorithm \( D_K(C) \):

1. if (|C| mod \( n \) ≠ 0 or |C| = 0) return ⊥
2. \( C_0 \mid C_1 \mid ... \mid C_m = C: C_i \in \{0,1\}^n \)
3. if (\( C_0 + m \geq 2^n \)) return ⊥
4. for \( i = 1...m \) do \( M_i \leftarrow f_K^{-1}(C_i) \oplus C_{i-1} \)
5. return \( M_1 \mid ... \mid M_m \)
Randomized Counter Mode Encryption

Let \( f : \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^l \) be a pseudorandom function

Algorithm \( E_K(M) \):
- if \((|M| \text{ mod } l \neq 0 \text{ or } |M| = 0 \text{ or } |M| > 2^n)\) return \( \perp \)
- \( M_1, \ldots, M_m \leftarrow M : M_i \in \{0,1\}^l \)
- \( R \leftarrow \text{R} \{0,1\}^n \)
- for \( i = 1 \ldots m \) do \( C_i \leftarrow f_K(R+i \text{ mod } 2^n) \oplus M_i \)
- return \( R \mid C_1 \mid \ldots \mid C_m \)

Algorithm \( D_K(C) \):
- if \((|C| - n \text{ mod } l \neq 0 \text{ or } |C| < n \text{ or } |C| > n + l^2)\) return \( \perp \)
- \( R \mid C_1 \mid \ldots \mid C_m \leftarrow C : R \in \{0,1\}^n \text{ and } C_i \in \{0,1\}^l \)
- for \( i = 1 \ldots m \) do \( M_i \leftarrow f_K(R+i \text{ mod } 2^n) \oplus C_i \)
- return \( M_1 \mid \ldots \mid M_m \)

Stateful Counter Mode Encryption

Let \( f : \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^l \) be a pseudorandom function

Algorithm \( E_K(M) \):
- static \( ctr \leftarrow 0 \)
- if \((|M| \text{ mod } l \neq 0 \text{ or } |M| = 0)\) return \( \perp \)
- \( M_1, \ldots, M_m \leftarrow M : M_i \in \{0,1\}^l \)
- if \((\text{ctr} + m \geq 2^n)\) return \( \perp \)
- for \( i = 1 \ldots m \) do \( C_i \leftarrow f_K(\text{ctr}+i) \oplus M_i \)
- \( \text{ctr} \leftarrow \text{ctr} + m \)
- return \( \text{ctr} \mid C_1 \mid \ldots \mid C_m \)

Algorithm \( D_K(C) \):
- if \((|C| - n \text{ mod } l \neq 0 \text{ or } |C| < n \text{ or } |C| \geq n + l^2)\) return \( \perp \)
- \( \text{ctr} \mid C_1 \mid \ldots \mid C_m \leftarrow C : \text{ctr} \in \{0,1\}^n \text{ and } C_i \in \{0,1\}^l \)
- for \( i = 1 \ldots m \) do \( M_i \leftarrow f_K(\text{ctr}+i \text{ mod } 2^n) \oplus C_i \)
- \( \text{ctr} + m \)
- return \( M_1 \mid \ldots \mid M_m \)
IND-CPA

- IND-CPA = “Indistinguishability under Chosen Plaintext Attack”
- Let $SE = \langle K, E, D \rangle$ be a symmetric encryption scheme
- Consider an adversary $A$ that is given access to a “left or right encryption oracle” $E_K(\text{LR}(\cdot, \cdot, b))$, $b \in \{0,1\}$ defined as:

  Oracle $E_K(\text{LR}(M_0, M_1, b))$
  
  $C \leftarrow E_K(M_b)$
  
  return $C$

- $A$ can invoke this oracle repeatedly with arguments $M_0, M_1$ of its choosing
- Intuitively, $A$’s job is to determine $b$

Unfortunately, $A$ can easily determine $b$ if it makes certain types of queries:

- $|M_0| \neq |M_1|$
- $E_K(M_0) = \bot$ but $E_K(M_1) \neq \bot$

So, in our definition we rule out “illegitimate” adversaries, defined as those that can ever call $E_K(\text{LR}(M_0, M_1, b))$ where

- $|M_0| \neq |M_1|$
- $E_K(M_0) = \bot$ or $E_K(M_1) = \bot$

“Legitimate” adversaries are those that are not illegitimate.
**IND-CPA**

- **Definition:** Let \( SE = (K, E, D) \) be a symmetric encryption scheme, and let \( A \) be an algorithm that has access to an oracle that takes as input a pair of strings and returns a string. Define

  \[
  \text{Experiment } \text{Exp}^{\text{ind-cca}}(A) \\
  K \leftarrow \mathcal{K}() \\
  b' \leftarrow A_{E, D}(LR(M_0, M_1, b)) \\
  \text{return } b'
  \]

  The **IND-CPA advantage of** \( A \) is defined as

  \[
  \text{Adv}^{\text{ind-cca}}(A) = \text{Pr}[\text{Exp}^{\text{ind-cca}}(A) = 1] - \text{Pr}[\text{Exp}^{\text{ind-cca}}(A) = 0]
  \]

  if \( A \) is legitimate, and 0 otherwise.

---

**IND-CPA**

- For any \( t, q, \mu \) we define the **IND-CPA advantage of** \( SE \) as

  \[
  \text{Adv}^{\text{ind-cca}}(t, q, \mu) = \max_A \left\{ \text{Adv}^{\text{ind-cca}}(A) \right\}
  \]

  where the maximum is over all \( A \) having time complexity \( t \) and making at most \( q \) oracle queries, the sum of the lengths of these queries being at most \( \mu \) bits.

  - Time complexity is the worst-case time for the entire experiment
  - Length of a query \( X(LR(M_0, M_1, b)) \) is \( |M_0| \)

- Informally, \( SE \) is “IND-CPA secure” if the IND-CPA advantage of \( SE \) is small.
IND-CPA Advantage for ECB

**Proposition:** Let $SE = \langle K, E, D \rangle$ denote ECB encryption using pseudorandom permutation $f$: $\{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$. Then,

$$\text{Adv}^{\text{ind-CPA}}_{SE}(t,1,2n) = 1$$

where $t = O(n)$ plus the time for two applications of $f$.

**Proof:** We describe an adversary $A$ that makes 1 query to its oracle of length $2n$, and having

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

Now it is easy to see that

$$\Pr\left[\text{Expt}^{\text{ind-CPA}^{-1}}_{SE}(A) = 1\right] = 1$$

$$\Pr\left[\text{Expt}^{\text{ind-CPA}^{-0}}_{SE}(A) = 1\right] = 0$$
Deterministic and Stateless Encryption

Proposition: Let $SE = \langle K, E, D \rangle$ denote a deterministic, stateless symmetric encryption system. Assume there is an integer $m$ such that the plaintext space of $SE$ contains two elements of length $m$. Then

$$Adv_{SE}^{\text{ind-adv}}(t, 2, 2m) = 1$$

where $t = O(m)$ plus the time for two encryptions.

Proof: Consider the following adversary:

- Adversary $A_{E}(LR(\cdot, \cdot, b))$
- Let $X, Y$ be distinct $m$-bit plaintexts
- $C_1 \leftarrow E_K(LR(X, Y, b))$
- $C_2 \leftarrow E_K(LR(Y, Y, b))$
- If $(C_1 = C_2)$ return 1 else return 0

IND-CPA Advantage for Stateful CBC

Proposition: Let $SE = \langle K, E, D \rangle$ denote stateful CBC encryption using pseudorandom permutation $f: \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$. Then,

$$Adv_{SE}^{\text{ind-adv}}(t, 2, 2n) = 1$$

for $t = O(n)$ plus time for two applications of the block cipher.
IND-CPA Advantage of Stateful CBC

Proof. Consider the following adversary $A$:

Adversary $A^{E_{K}(LR(\cdot, \cdot, b))}$

- $M_0^1 \leftarrow 1^{n-1}0; \ M_0^1 \leftarrow 0^{n-1}1$
- $M_0^2 \leftarrow 1^{n-1}0; \ M_0^2 \leftarrow 0^n$
- $\langle C_0^1, C_1^1 \rangle \leftarrow E_{K}(LR(M_0^1, M_1^1, b))$
- $\langle C_0^2, C_1^2 \rangle \leftarrow E_{K}(LR(M_0^2, M_1^2, b))$
- if ($C_1^1 = C_1^2$) return 1 else return 0

First note that $C_0^1 = 0^n$ and $C_0^2 = 0^{n-1}1$ because in the stateful CBC, the initialization vector is determined by a counter.

If $b = 1$, then

- $M_1^1 \oplus C_0^1 = 0^{n-1}1 \oplus 0^n = 0^{n-1}1$
- $M_1^2 \oplus C_0^2 = 0^n \oplus 0^{n-1}1 = 0^{n-1}1$

If $b = 0$, then

- $M_1^1 \oplus C_0^1 = 1^{n-1}0 \oplus 0^n = 1^{n-1}0$
- $M_1^2 \oplus C_0^2 = 1^{n-1}0 \oplus 0^{n-1}1 = 1^n$

So, $C_1^1 = C_1^2$ iff $b = 1$. 
Plaintext Recovery

- **Definition:** Let $SE = \langle \mathcal{K}, \mathcal{E}, \mathcal{D} \rangle$ denote a stateless symmetric encryption scheme whose plaintext space includes $\{0,1\}^m$, and let $B$ be an algorithm that has access to an oracle. Consider the following experiment:

Experiment $\text{Expt}_{SE}^{pr-adv}(B)$

- $K \leftarrow \mathcal{K}()$
- $M' \leftarrow \mathcal{R}\{0,1\}^m$
- $C \leftarrow \mathcal{E}_K(M')$
- $M \leftarrow B^{\mathcal{E}_K}(C)$
- if $(M = M')$ return 1 else return 0

The pr-advantage of $B$ is defined as

$$\text{Adv}_{SE}^{pr-adv}(B) = \Pr \left[ \text{Expt}_{SE}^{pr-adv}(B) = 1 \right]$$

For any $t$, $q$, and $\mu$ we define the pr-advantage of $SE$ as

$$\text{Adv}_{SE}^{pr-adv}(t, q, \mu) = \max_B \left\{ \text{Adv}_{SE}^{pr-adv}(B) \right\}$$

where the maximum is over all $B$ having time complexity $t$ and making at most $q$ oracle queries, the sum of the lengths of these queries being at most $\mu$ bits.
Indistinguishability and Plaintext Recovery

**Proposition:** Let $\mathcal{SE} = \langle \mathcal{K}, \mathcal{E}, \mathcal{D} \rangle$ denote a stateless symmetric encryption scheme whose plaintext space includes $\{0,1\}^m$. Then,

$$\text{Adv}^{\text{pr-cca}}_{\mathcal{SE}}(t, q, \mu) \leq \text{Adv}^{\text{ind-cca}}_{\mathcal{SE}}(t, q + 1, \mu + m) + \frac{1}{2^m}$$

*Proof:* Given any adversary $B$ with resources restricted to $t$, $q$, $\mu$, we construct an adversary $A_B$ that uses resources $t$, $q+1$, $\mu+m$, such that

$$\text{Adv}^{\text{pr-cca}}_{\mathcal{SE}}(B) \leq \text{Adv}^{\text{ind-cca}}_{\mathcal{SE}}(A_B) + \frac{1}{2^m}$$

---

**Indistinguishability and Plaintext Recovery**

Given $B$, define $A_B$ as follows:

Algorithm $A_B^{\mathcal{E},\mathcal{D}(\cdot,\cdot)}$

- $M_0 \leftarrow_R \{0,1\}^m$
- $M_1 \leftarrow_R \{0,1\}^m$
- $C \leftarrow \mathcal{E}_K(\text{LR}(M_0, M_1, b))$

Execute $B(C)$, replying to its oracle queries as follows:

- When $B$ makes oracle query $X$, return $Y \leftarrow \mathcal{D}_K(\text{LR}(X, X, b))$
- Until $B$ stops and outputs a plaintext $M$
- if ($M = M_1$) return 1 else return 0
Indistinguishability and Plaintext Recovery

First note that

\[ \Pr \left[ \text{Expt}_{SE}^{\text{ind-cpa}^{-1}}(A_B) = 1 \right] \geq \text{Adv}_{SE}^{\text{pr-cpa}}(B) \]

since when \( B \) succeeds, so does \( A_B \) if \( b = 1 \).

If \( b = 0 \), then since \( B \) is given \( M_0 \) and has no other information about \( M_1 \),

\[ \Pr \left[ \text{Expt}_{SE}^{\text{ind-cpa}^{-0}}(A_B) = 1 \right] \leq \frac{1}{2^m} \]

So,

\[ \text{Adv}_{SE}^{\text{ind-cpa}}(A_B) = \Pr \left[ \text{Expt}_{SE}^{\text{ind-cpa}^{-1}}(A_B) = 1 \right] - \Pr \left[ \text{Expt}_{SE}^{\text{ind-cpa}^{-0}}(A_B) = 1 \right] \geq \text{Adv}_{SE}^{\text{pr-cpa}}(B) - \frac{1}{2^m} \]

\[ \square \]

IND-CPA-CG

- **Definition:** Let \( SE = \langle \mathcal{K}, E, D \rangle \) be a symmetric encryption scheme, and let \( A \) be an algorithm that has access to an oracle that takes as input a pair of strings and returns a string. Define

  \[ \text{Experiment} \ \text{Expt}_{SE}^{\text{ind-cpa-cq}}(A) \]
  \[ b \leftarrow \{0,1\} \]
  \[ K \leftarrow \mathcal{K}() \]
  \[ b' \leftarrow A_{SE,E}(b, K) \]
  \[ \text{if} \ (b = b') \text{ return } 1 \text{ else return } 0 \]

  Let \( \text{Adv}_{SE}^{\text{ind-cpa-cq}}(A) = 2 \cdot \Pr \left[ \text{Expt}_{SE}^{\text{ind-cpa-cq}}(A) = 1 \right] - 1 \)

- **Proposition:** Let \( SE = \langle \mathcal{K}, E, D \rangle \) be a symmetric encryption scheme, and let \( A \) be an adversary. Then

  \[ \text{Adv}_{SE}^{\text{ind-cpa-cq}}(A) = \text{Adv}_{SE}^{\text{ind-cpa}}(A) \]
IND-CPA-CG

Proof:

\[ \Pr\left[ \text{Exp}_{SE}^{\text{ind-CPA-CG}}(A) = 1 \right] \]
\[ = \Pr[b = b'] \]
\[ = \Pr[b' = 1 \mid b = 1] \cdot \Pr[b = 1] + \Pr[b' = 0 \mid b = 0] \cdot \Pr[b = 0] \]
\[ = \Pr[b' = 1 \mid b = 1] \cdot \frac{1}{2} + \Pr[b' = 0 \mid b = 0] \cdot \frac{1}{2} \]
\[ = \frac{1}{2} + \frac{1}{2} \cdot (\Pr[b' = 1 \mid b = 1] - \Pr[b' = 1 \mid b = 0]) \cdot \frac{1}{2} \]
\[ = \frac{1}{2} + \frac{1}{2} \cdot \text{Adv}_{SE}^{\text{ind-CPA}}(A) \]

Security for Stateful Counter Mode

Proposition: Let \( F: \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^l \) be a family of functions and let \( SE = (K, E, D) \) denote stateful counter mode encryption. For any \( t, q, \) and \( \mu \) with \( \mu < l \cdot 2^n \),

\[
\text{Adv}_{SE}^{\text{ind-CPA}}(t, q, \mu) \leq 2 \cdot \text{Adv}_{F}^{\text{prf}}(t, q', n q')
\]

where \( q' = \mu / l \).

Proof: Let \( A \) be any IND-CPA adversary attacking \( SE \) that uses resources bounded by \( t, q, \) and \( \mu \).
Security for Stateful Counter Mode

First define a generalized version of stateful counter mode encryption that uses a function \( g : \{0,1\}^n \rightarrow \{0,1\}^l \) as the key.

Algorithm \( E_g(M) \):

\[
\begin{align*}
\text{static } ctr &\leftarrow 0 \\
\text{if } (|M| \mod l \neq 0 \text{ or } |M| = 0) &\text{ return } \\
M_1|\ldots|M_m &\leftarrow M : M_i \in \{0,1\}^l \\
\text{if } (ctr + m \geq 2^n) &\text{ return } \\
\text{for } i = 1 \ldots m &\text{ do } C_i \leftarrow g(ctr+i) \oplus M_i \\
ctr &\leftarrow ctr + m \\
\text{return } (ctr - m) \mid C_1 \mid \ldots \mid C_m
\end{align*}
\]

Let \( S\mathcal{E}[G] \) denote this encryption scheme in which key generation selects a random element of the family \( G \).

Lemma: \( \text{Adv}_{S\mathcal{E}[\text{Func}(n,l)]}^{\text{ind-cca}}(A) = 0 \)

Security for Stateful Counter Mode

We construct a distinguisher \( D_A \) for \( F \) that makes \( q' \) queries to its oracle, as follows:

Algorithm \( D_A^{q'}(b) \):

\[
\begin{align*}
b &\leftarrow_R \{0,1\} \\
\text{Run } A, \text{ replying to its oracle queries as follows:} & \\
\text{When } A \text{ makes oracle query } (M_0, M_f) &\text{ return } C \leftarrow E_g(M_b) \\
\text{Until } A \text{ stops and outputs a bit } b' & \\
\text{if } (b = b') &\text{ return } 1 \text{ else return } 0
\end{align*}
\]

That is, \( D_A \) guesses that \( g \) is a random member of \( F \) if \( A \) guesses correctly, and that \( g \) is a random member of \( \text{Func}(n, l) \) otherwise.
Security for Stateful Counter Mode

Note: \[ \Pr[\text{Expt}_F^{\text{prf}}(D_A) = 1] = \Pr[\text{Expt}_E^{\text{ind-cpa-cg}}(A) = 1] \]
\[ \Pr[\text{Expt}_F^{\text{prf-o}}(D_A) = 1] = \Pr[\text{Expt}_E^{\text{ind-cpa-cg}}(\text{Func}(n.J)) (A) = 1] \]

So,
\[ \Pr[\text{Expt}_F^{\text{prf}}(D_A) = 1] = \frac{1}{2} + \frac{1}{2} \cdot \text{Adv}_{\text{ind-cpa}}^{\text{SE}}(F)(A) \]
\[ \Pr[\text{Expt}_F^{\text{prf-o}}(D_A) = 1] = \frac{1}{2} + \frac{1}{2} \cdot \text{Adv}_{\text{ind-cpa}}^{\text{SE}[\text{Func}(n.J)]}(A) \]

And then
\[ \text{Adv}_F^{\text{prf}}(D_A) = \Pr[\text{Expt}_F^{\text{prf}}(D_A) = 1] - \Pr[\text{Expt}_F^{\text{prf-o}}(D_A) = 1] \]
\[ = \frac{1}{2} \cdot \text{Adv}_{\text{ind-cpa}}^{\text{SE}}(F)(A) - \frac{1}{2} \cdot \text{Adv}_{\text{ind-cpa}}^{\text{SE}[\text{Func}(n.J)]}(A) \]
\[ = \frac{1}{2} \cdot \text{Adv}_{\text{ind-cpa}}^{\text{SE}[F]}(A) \]

Security for Randomized Counter Mode

Proposition: Let \( F: \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^l \) be a family of functions and let \( \text{SE} = \langle \mathcal{K}, \mathcal{E}, \mathcal{D} \rangle \) denote randomized counter mode encryption. For any \( t, q, \) and \( \mu \) with \( \mu < l \cdot 2^n \),
\[ \text{Adv}_{\text{ind-cpa}}^{\text{SE}}(t, q, \mu) \leq 2 \cdot \text{Adv}_F^{\text{prf}}(t, q', nq') + \frac{\mu(q-1)}{l \cdot 2^n} \]
where \( q' = \frac{\mu}{l} \).

Proof: Very similar to previous, given the following lemma:

Lemma: For any \( A \),
\[ \text{Adv}_{\text{ind-cpa}}^{\text{SE}[\text{Func}(n.J)]}(A) \leq \frac{\mu(q-1)}{l \cdot 2^n} \]
Practical Implications

- These theorems give us a basis for answering questions that you will probably have to tackle “in the wild”
- Ex: you wish to encrypt $q = 2^{40}$ plaintexts, each $2^{10}$ bits long
  - That is, a total of $\mu = 2^{50}$ bits of data
- Suppose you estimate any reasonable adversary to invest at most $t = 2^{60}$ compute cycles
- Finally, suppose you encrypt using AES and assume that
  \[
  \text{Adv}_{\text{AES}}^{\text{prf}}(t, q', 128q') = c_1 \cdot \frac{t}{T_{\text{AES}}} + \frac{(q')^2}{2^{128}}
  \]
  - first term captures cost of key search
  - $c_1$ is a small constant
  - $T_{\text{AES}}$ is number of cycles required for one AES computation
  - $q' = \mu / 128 = 2^{43}$

Practical Implications

- If you encrypt using stateful counter mode, then
  \[
  \text{Adv}_{\text{SIV-CPA}}^{\text{ind-cpa}}(t, q, \mu) \leq 2 \cdot \text{Adv}_{\text{AES}}^{\text{prf}}(t, q', 128q')
  \]
  \[
  = 2c_1 \cdot \frac{t}{T_{\text{AES}}} + \frac{2(q')^2}{2^{128}}
  \]
  \[
  = \frac{c_1}{T_{\text{AES}}} \cdot \frac{2^{60+1}}{2^{128}} + \frac{2^{43+2+1}}{2^{128}}
  \]
  \[
  = \frac{c_1}{T_{\text{AES}}} \cdot \frac{1}{2^{57}} + \frac{1}{2^{41}}
  \]
  \[
  \leq \frac{1}{2^{40}} \text{ assuming } \frac{c_1}{T_{\text{AES}}} \leq 2^{26}
  \]