PRPs and PRFs

1. Abstract ciphers: PRPs and PRFs,
2. Security models for encryption,
3. Analysis of CBC and counter mode

Dan Boneh, Stanford University
PRPs and PRFs

• Pseudo Random Function (PRF) defined over (K,X,Y):
  \[ F: K \times X \rightarrow Y \]
such that exists “efficient” algorithm to evaluate \( F(k,x) \)

• Pseudo Random Permutation (PRP) defined over (K,X):
  \[ E: K \times X \rightarrow X \]
such that:
  1. Exists “efficient” algorithm to evaluate \( E(k,x) \)
  2. The function \( E(k, \cdot) \) is one-to-one
  3. Exists “efficient” inversion algorithm \( D(k,x) \)
Running example

- **Example PRPs**: 3DES, AES, ...

  - AES: \( K \times X \rightarrow X \) where \( K = X = \{0,1\}^{128} \)
  - DES: \( K \times X \rightarrow X \) where \( X = \{0,1\}^{64} \), \( K = \{0,1\}^{56} \)
  - 3DES: \( K \times X \rightarrow X \) where \( X = \{0,1\}^{64} \), \( K = \{0,1\}^{168} \)

- Functionally, any PRP is also a PRF.
  - A PRP is a PRF where \( X=Y \) and is efficiently invertible.
Secure PRFs

- Let $F: K \times X \rightarrow Y$ be a PRF

  \[ F_{\text{Funs}[X,Y]}: \text{the set of all functions from } X \text{ to } Y \]

  \[ S_F = \{ F(k, \cdot) \text{ s.t. } k \in K \} \subseteq F_{\text{Funs}[X,Y]} \]

- Intuition: a PRF is secure if a random function in $F_{\text{Funs}[X,Y]}$ is indistinguishable from a random function in $S_F$
Secure PRFs

• Let $F: K \times X \to Y$ be a PRF
  \[
  \begin{align*}
  \text{Funs}[X,Y]: & \quad \text{the set of all functions from } X \text{ to } Y \\
  S_F = \{ F(k, \cdot) \text{ s.t. } k \in K \} & \subseteq \text{Funs}[X,Y]
  \end{align*}
  \]

• **Intuition:** a PRF is **secure** if
  a random function in Funs[X,Y] is indistinguishable from
  a random function in $S_F$

???

\[f(x) \text{ or } F(k,x) \quad ?\]
Secure PRF: definition

• For \( b=0,1 \) define experiment \( \text{EXP}(b) \) as:

\[
\begin{align*}
\text{Chal.} & \quad b=0: \quad k \leftarrow K, \quad f \leftarrow F(k, \cdot) \\
& \quad b=1: \quad f \leftarrow \text{Funs}[X,Y]
\end{align*}
\]

\( x_i \in X \)

\( f(x_i) \)

\( b' \in \{0,1\} \)

• Def: \( F \) is a secure PRF if for all “efficient” \( A \):

\[
\text{PRF Adv}[A,F] = \left| \Pr[\text{EXP}(0)=1] - \Pr[\text{EXP}(1)=1] \right|
\]

is “negligible.”
Secure PRP

- For $b=0,1$ define experiment $\text{EXP}(b)$ as:

  - $b=0$: $k \leftarrow K$, $f \leftarrow E(k, \cdot)$
  - $b=1$: $f \leftarrow \text{Perms}[X]$

- Def: $E$ is a secure PRP if for all "efficient" $A$:

  $\text{PRP Adv}[A,E] = |\Pr[\text{EXP}(0)=1] - \Pr[\text{EXP}(1)=1]|$

  is "negligible."
Example secure PRPs

- **Example secure PRPs**: 3DES, AES, ...
  
  AES: $K \times X \rightarrow X$ where $K = X = \{0,1\}^{128}$

- **AES PRP Assumption** (example):
  
  All $2^{80}$–time algs A have $\text{PRP Adv}[A, AES] < 2^{-40}$
PRF Switching Lemma

• Any secure PRP is also a secure PRF.

• **Lemma:** Let $E$ be a PRP over (K,X) Then for any $q$-query adversary $A$:

$$\left| \text{PRF Adv}[A,E] - \text{PRP Adv}[A,E] \right| < \frac{q^2}{2|X|}$$

⇒ Suppose $|X|$ is large so that $\frac{q^2}{2|X|}$ is “negligible”

Then

$$\text{PRP Adv}[A,E] \text{ “negligible” } \Rightarrow \text{PRF Adv}[A,E] \text{ “negligible”}$$
Using PRPs and PRFs

- **Goal**: build “secure” encryption from a PRP.

- Security is always defined using two parameters:

  1. What “**power**” does adversary have?
     - examples:
       - Adv sees only one ciphertext (one-time key)
       - Adv sees many PT/CT pairs (many-time key, CPA)

  2. What “**goal**” is adversary trying to achieve?
     - examples:
       - Fully decrypt a challenge ciphertext.
       - Learn info about PT from CT (semantic security)
Incorrect use of a PRP

Electronic Code Book (ECB):

PT: \[ m_1 \quad m_2 \quad \cdots \quad \]

CT: \[ c_1 \quad c_2 \quad \cdots \quad \]

• Problem:
  - if \( m_1 = m_2 \) then \( c_1 = c_2 \)
In pictures

An example plaintext

Encrypted with AES in ECB mode

(courtesy B. Preneel)
Modes of Operation for One-time Use Key

Example application:
- Encrypted email. New key for every message.
Semantic Security for one-time key

- $E = (E,D)$ a cipher defined over $(K,M,C)$
- For $b=0,1$ define $\text{EXP}(b)$ as:

  $\text{Def} \text{: } E \text{ is sem. sec. for one-time key if for all "efficient" } A:$

\[
\text{SS Adv}[A,E] = \left| \Pr[\text{EXP}(0)=1] - \Pr[\text{EXP}(1)=1] \right|
\]

is "negligible."
Semantic security (cont.)

- Sem. Sec. $\Rightarrow$ no “efficient” adversary learns info about PT from a single CT.
- Example: suppose efficient $A$ can deduce LSB of PT from CT. Then $E = (E,D)$ is not semantically secure.

- Then $SS \text{Adv}[B, E] = 1 \Rightarrow E$ is not sem. sec.
Note: ECB is not Sem. Sec.

- Electronic Code Book (ECB):
  - Not semantically secure for messages that contain more than one block.

\[
b \in \{0,1\}
\]

Chal.
\[ k \leftarrow K \]

Two blocks

\[
m_0 = \text{“Hello World”}
\]

\[
m_1 = \text{“Hello Hello”}
\]

\[(C_1, C_2) \leftarrow E(k, m_b)\]

Adv. A

If \( C_1 = C_2 \) output 0, else output 1

- Then \( \text{SS Adv}[A, ECB] = 1 \)
Secure Constructions

- Examples of sem. sec. systems:
  1. \( \text{SS Adv}[A, \text{OTP}] = 0 \) for all \( A \)
  2. Deterministic counter mode from a PRF \( F \):
     - \( E_{\text{DETCTR}} (k,m) = \)
       
       \[
       \begin{array}{cccc}
       m[0] & m[1] & \cdots & m[L] \\
       \oplus \\
       F(k,0) & F(k,1) & \cdots & F(k,L) \\
       \hline
       c[0] & c[1] & \cdots & c[L] \\
       \end{array}
       \]

- Stream cipher built from PRF (e.g. AES, 3DES)
Det. counter-mode security

- **Theorem**: For any $L > 0$.
  
  If $F$ is a secure PRF over $(K,X,X)$ then $E_{DETCTR}$ is sem. sec. cipher over $(K,X^L,X^L)$.

  In particular, for any adversary $A$ attacking $E_{DETCTR}$ there exists a PRF adversary $B$ s.t.:
  
  $$\text{SS Adv}[A, E_{DETCTR}] = 2 \cdot \text{PRF Adv}[B, F]$$

  PRF Adv$[B, F]$ is negligible (since $F$ is a secure PRF)

  Hence, SS Adv$[A, E_{DETCTR}]$ must be negligible.
Modes of Operation for Many-time Key

Example applications:

1. File systems: Same AES key used to encrypt many files.
2. IPsec: Same AES key used to encrypt many packets.
Semantic Security for many-time key (CPA security)

Cipher \( E = (E,D) \) defined over \( (K,M,C) \).
For \( b=0,1 \) define \( \text{EXP}(b) \) as:

\[
\text{Def} \quad \text{E is sem. sec. under CPA if for all “efficient” A:}
\[
\text{Adv}_{\text{CPA}}[A,E] = \left| \Pr[\text{EXP}(0)=1] - \Pr[\text{EXP}(1)=1] \right|
\]

is “negligible.”
Security for many-time key

- **Fact:** stream ciphers are insecure under CPA.
  - More generally: if $E(k,m)$ always produces same ciphertext, then cipher is insecure under CPA.

![Security Diagram](image)

- If secret key is to be used multiple times ⇒
  given the same plaintext message twice, the encryption alg. must produce different outputs.
Nonce-based Encryption

- nonce $n$: a value that changes from msg to msg, (k,n) pair never used more than once
- **method 1**: encryptor picks a random nonce, $n \leftarrow \mathcal{N}$
- **method 2**: nonce is a counter (e.g. packet counter)
  - used when encryptor keeps state from msg to msg
  - if decryptor has same state, need not send nonce with CT
Construction 1: CBC with random nonce

- Cipher block chaining with a random IV (IV = nonce)

\[ \text{IV} \rightarrow m[0] \rightarrow m[1] \rightarrow m[2] \rightarrow m[3] \]

\[ \oplus \rightarrow E(k, \cdot) \rightarrow \oplus \rightarrow E(k, \cdot) \rightarrow \oplus \rightarrow E(k, \cdot) \rightarrow \oplus \rightarrow E(k, \cdot) \]

\[ \text{IV} \rightarrow c[0] \rightarrow c[1] \rightarrow c[2] \rightarrow c[3] \]

ciphertext

note: CBC where attacker can predict the IV is not CPA-secure. HW.
CBC: CPA Analysis

• **CBC Theorem:** For any $L>0$,
  
  If $E$ is a secure PRP over $(K,X)$ then $E_{\text{CBC}}$ is a sem. sec. under CPA over $(K, X^L, X^{L+1})$.

  In particular, for a $q$-query adversary $A$ attacking $E_{\text{CBC}}$ there exists a PRP adversary $B$ s.t.:

  $$SS_{\text{CPA}} \text{ Adv}[A, E_{\text{CBC}}] \leq 2 \cdot \text{PRP Adv}[B, E] + 2 \frac{q^2 L^2}{|X|}$$

• Note: CBC is only secure as long as $q^2 L^2 << |X|$
Construction 1’: CBC with **unique** nonce

- Cipher block chaining with **unique** IV \((IV = nonce)\)

  unique IV means: \((key, IV)\) pair is used for only one message

\[
\begin{align*}
  m[0] &\oplus E(k_2,\cdot) \\
  m[1] &\oplus E(k_1,\cdot) \\
  m[2] &\oplus E(k_1,\cdot) \\
  m[3] &\oplus E(k_1,\cdot) \\
\end{align*}
\]

\[
\begin{align*}
  c[0] &\oplus IV \\
  c[1] &\oplus IV \\
  c[2] &\oplus IV \\
  c[3] &\oplus IV \\
\end{align*}
\]

- Included only if unknown to decryptor
A CBC technicality: padding

 TLS: for $n>0$, $n+1$ byte pad is removed during decryption
if no pad needed, add a dummy block

IV

E($k_1, \cdot$)

m[0] m[1] m[2] m[3] \$\|\$ pad

$\oplus$

E($k, \cdot$) E($k, \cdot$) E($k, \cdot$) E($k, \cdot$)


IV

n n n n \ldots n
Construction 2: rand ctr-mode

IV - chosen at random for every message

note: parallelizable (unlike CBC)
Construction 2’: nonce ctr-mode

To ensure $F(K,x)$ is never used more than once, choose IV as:

- **IV**:
  - nonce: 64 bits
  - counter: 64 bits

IV starts at 0 for every msg.
rand ctr-mode: CPA analysis

- Randomized counter mode: random IV.

- **Counter-mode Theorem:** For any \( L > 0 \),
  
  If \( F \) is a secure PRF over \((K, X, X)\) then
  
  \( E_{\text{CTR}} \) is a sem. sec. under CPA over \((K, X^L, X^{L+1})\).

In particular, for a \( q \)-query adversary \( A \) attacking \( E_{\text{CTR}} \)
there exists a PRF adversary \( B \) s.t.:

\[
\text{SS}_{\text{CPA}} \text{ Adv}[A, E_{\text{CTR}}] \leq 2 \cdot \text{PRF Adv}[B, F] + 2 \cdot q^2 \frac{L}{|X|}
\]

- **Note:** ctr-mode only secure as long as \( q^2L \ll |X| \)

Better than CBC!
Summary

- PRPs and PRFs: a useful abstraction of block ciphers.

- We examined two security notions:
  1. Semantic security against one-time CPA.
  2. Semantic security against many-time CPA.

  Note: neither mode ensures data integrity.

- Stated security results summarized in the following table:

<table>
<thead>
<tr>
<th>Goal</th>
<th>Power</th>
<th>one-time key</th>
<th>Many-time key (CPA)</th>
<th>CPA and CT integrity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sem. Sec.</td>
<td>steam-ciphers</td>
<td>det. ctr-mode</td>
<td>rand CBC</td>
<td>later</td>
</tr>
</tbody>
</table>