Lecture 3: PRF

Viet Tung Hoang

The slides are loosely based on those of Prof. Mihir Bellare, UC San Diego.
1. Defining PRF Security

2. Birthday Attack
Recall

<table>
<thead>
<tr>
<th>Possible Properties</th>
<th>Necessary</th>
<th>Sufficient</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security against key recovery</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Hard to find $M$ given $C \leftarrow E_K(M)$</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Want: a single “master” property that is sufficient to ensure security of common usage of blockcipher.
An Analogy: Turing Test

What does it mean for a machine to be “intelligent”?

Possible Answers

<table>
<thead>
<tr>
<th>Possible Answers</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>It can be happy</td>
<td></td>
</tr>
<tr>
<td>It recognizes pictures</td>
<td></td>
</tr>
<tr>
<td>...</td>
<td></td>
</tr>
</tbody>
</table>

But no such list is satisfactory
An Analogy: Turing Test

interaction

Man (0) or Machine (1)?
# Real versus Ideal

<table>
<thead>
<tr>
<th>Notion</th>
<th>Real object</th>
<th>Ideal object</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intelligence</td>
<td><img src="image1" alt="Robot" /></td>
<td><img src="image2" alt="Person" /></td>
</tr>
<tr>
<td>PRF</td>
<td>$E_K$</td>
<td>Random function</td>
</tr>
</tbody>
</table>
Informal View of PRF Security

\[ E : \{0, 1\}^k \times \{0, 1\}^n \rightarrow \{0, 1\}^n \]

Adversary doesn’t know \( K \) or \( f \)

Sample random \( f : \{0, 1\}^n \rightarrow \{0, 1\}^n \)

\( K \overset{\$}{\leftarrow} \mathcal{K} \)
Defining Random Function: Eager Sampling

Want: a random function \( f : \{0, 1\}^n \rightarrow \{0, 1\}^m \)

Let \( \text{Func}(n, m) \) be the set of all functions \( g : \{0, 1\}^n \rightarrow \{0, 1\}^m \)

Pick \( f \leftarrow \text{Func}(n, m) \)
PRF Security

Game \ Real_E

procedure Initialize()

\[ K \leftarrow \mathcal{K} \]

procedure \ Fn(M)\n
return \ E_K(M)\n
Game \ Rand_E

procedure Initialize()

\[ f \leftarrow \text{Func}(n, n) \]

procedure \ Fn(M)\n
return \ f(M)\n
Real (1) or Random (0)?

\[
\text{Adv}^\text{prf}_E(A) = \Pr[\text{Real}_E^A \Rightarrow 1] - \Pr[\text{Rand}_E^A \Rightarrow 1]
\]

\[
\text{Adv}^\text{prf}_E(A) \approx 0 \text{ means } A \text{ is doing poorly}
\]
Defining Random Function: Lazy Sampling

*Want:* a **random** function $f : \{0, 1\}^n \rightarrow \{0, 1\}^m$

- Pick a fresh random answer for a new query
- Reuse the consistent answer for an old query
An Alternative Way to Define PRF Security

**Game** \( \text{Real}_E \)

**procedure** Initialize()

\[ K \leftarrow \mathcal{K} \]

**procedure** \( \text{Fn}(M) \)

return \( E_K(M) \)

**Game** \( \text{Rand}_E \)

**procedure** \( \text{Fn}(M) \)

If \( T[M] = \perp \) then \( T[M] \leftarrow \{0, 1\}^n \)

return \( T[M] \)

\[ \text{Adv}^{\text{prf}}_E(A) = \Pr[\text{Real}_E^A \Rightarrow 1] - \Pr[\text{Rand}_E^A \Rightarrow 1] \]
Practicing PRF Attack

\[ E_K(M) = M \oplus K \]

\[ E_K(M) = \pi(M \oplus K) \]

Public permutation

\[ \pi, \pi^{-1} \text{ are public} \]
Practicing PRF Attack

\[ E_K(M) = AES_M(K) \]
1. Defining PRF Security

2. Birthday Attack
Birthday Problem

\[ y_1, \ldots, y_q \] \quad \{1, \ldots, N\}

\[ C(N, q) = \Pr[y_1, \ldots, y_q \text{ not distinct}] \]

(Incorrect) intuition: \[ C(N, q) \approx \frac{q}{N} \]

**Fact:** For \( q \leq \sqrt{2N} \),

\[ \frac{q(q - 1)}{4N} \leq C(N, q) \leq \frac{q(q - 1)}{2N} \]
Birthday Attack on PRF Security

\[ \text{distinct } M_1, \ldots, M_q \]

\[ \text{distinct } C_1, \ldots, C_q \]

\[ E_K \]

\[ \text{distinct } M_1, \ldots, M_q \]

\[ f \]

\[ \text{random } C_1, \ldots, C_q \]
Birthday Attack on PRF Security

\[ E : \{0, 1\}^k \times \{0, 1\}^n \rightarrow \{0, 1\}^n \]

A \hspace{1cm} \text{distinct } M_1, \ldots, M_q \hspace{1cm} \text{Fn}

\[ \text{Output 1 if } C_1, \ldots, C_q \text{ are distinct} \]

\[ \text{需 } 2^{n/2} \text{ queries to break PRF security} \]

\[ \text{Adv}_{E}^{\text{prf}}(A) = C(2^n, q) \approx \frac{q^2}{2^n} \]

<table>
<thead>
<tr>
<th>Blockcipher</th>
<th>(n)</th>
<th>(2^{n/2})</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>DES, 2DES, 3DES</td>
<td>64</td>
<td>(2^{32})</td>
<td>Insecure</td>
</tr>
<tr>
<td>AES</td>
<td>128</td>
<td>(2^{64})</td>
<td>Secure</td>
</tr>
</tbody>
</table>