Pseudorandom Function

Viet Tung Hoang

The slides are loosely based on those of Prof. Mihir Bellare, UC San Diego.
Agenda

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”?

<table>
<thead>
<tr>
<th>Possible Answers</th>
<th>But no such list is satisfactory</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>
An Analogy: Turing Test

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

\( K \leftarrow \mathcal{K} \)
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, and remember the answer
Defining Random Function: Lazy Sampling

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

Pick a fresh random answer for a new query, and remember the answer
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, and remember the answer
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, and remember the answer
Want: a random function $f : \{0, 1\}^n \rightarrow \{0, 1\}^m$
Putting Things in Code

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

**procedure** Initialize()

\( K \leftarrow \mathcal{K} \)

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

return \( E_K(M) \)

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

string array \( T = \{} \) // Global variable

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

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

return \( T[M] \)

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

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

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

\( \pi, \pi^{-1} \) are public
Easy to Break PRF Security After Key Recovery

KR attack

new msg, not used in KR attack

$E_K(M) \overset{?}{=} C$

Yes  No

1  0
PRF Security

Key Recovery Security
Exercise: PRF Attacks

\[ E_K(M) = \text{AES}_K(M) \parallel \text{AES}_K(\overline{M}) \]

Two-round Feistel
Agenda

1. Defining PRF Security

2. Birthday Attack
Birthday Problem

$y_1, \ldots, y_q \rightarrow \{1, \ldots, N\}$

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

**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

distinct $M_1, \ldots, M_q$

$E_K$

distinct $C_1, \ldots, C_q$

distinct $M_1, \ldots, M_q$

$f$

random $C_1, \ldots, C_q$
Birthday Attack on PRF Security

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

A \rightarrow \text{distinct } M_1, \ldots, M_q \rightarrow \text{Fn} \leftarrow A

Output 1 if \( C_1, \ldots, C_q \) are distinct

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

\begin{tabular}{|c|c|c|c|}
\hline
\text{Blockcipher} & \( n \) & \( 2^{n/2} \) & \text{Status} \\
\hline
DES, 2DES, 3DES & 64 & \( 2^{32} \) & Insecure \\
\hline
AES & 128 & \( 2^{64} \) & Secure \\
\hline
\end{tabular}