Pseudorandom Functions

Adam O’Neill
Based on http://cseweb.ucsd.edu/~mihir/cse207/
Defining “Good” blockcipher

- What is a good blockcipher?
Defining “Good” blockcipher

- What is a good blockcipher?
  - Key-recovery is hard
Defining “Good” blockcipher

- What is a good blockcipher?
  - Key-recovery is hard
  - Recovering M from $C = E(K,M)$ is hard
Defining “Good” blockcipher

- What is a good blockcipher?
  - Key-recovery is hard
  - Recovering M from $C = E(K,M)$ is hard
  - Recovering a bit of M from $C = E(K,M)$ is hard
Defining “Good” blockcipher

- What is a good blockcipher?
  - Key-recovery is hard
  - Recovering M from $C = E(K,M)$ is hard
  - Recovering a bit of M from $C = E(K,M)$ is hard
  - ...

Defining “Good” blockcipher

- What is a good blockcipher?
  - Key-recovery is hard
  - Recovering $M$ from $C = E(K,M)$ is hard
  - Recovering a bit of $M$ from $C = E(K,M)$ is hard
  - ...
- Clearly such a list cannot be exhaustive or correct
Defining “intelligent” computer

- What does it mean for a computer to be “intelligent” (in the sense of a human)?
Defining “intelligent” computer

• What does it mean for a computer to be “intelligent” (in the sense of a human)?

• It can be happy
Defining “intelligent” computer

- What does it mean for a computer to be “intelligent” (in the sense of a human)?
  - It can be happy
  - It can recognize pictures
Defining “intelligent” computer

• What does it mean for a computer to be “intelligent” (in the sense of a human)?
  • It can be happy
  • It can recognize pictures
  • It can multiply (small) numbers
Defining “intelligent” computer

• What does it mean for a computer to be “intelligent” (in the sense of a human)?
  
  • It can be happy
  
  • It can recognize pictures
  
  • It can multiply (small) numbers
  
  • …
Defining “intelligent” computer

- What does it mean for a computer to be “intelligent” (in the sense of a human)?
  - It can be happy
  - It can recognize pictures
  - It can multiply (small) numbers
  - ...
- Turing had a “functional” answer to this question
Q: What does it mean for a program to be “intelligent” in the sense of a human?

Turing’s answer: A program is intelligent if its input/output behavior is indistinguishable from that of a human.
Turing Test

Behind the wall:

- Room 1: The program \( P \)
- Room 0: A human
**Turing Test**

Game:

- Put tester in room 0 and let it interact with object behind wall
- Put tester in room 1 and let it interact with object behind wall
- Now ask tester: which room was which?

The measure of “intelligence” of $P$ is the extent to which the tester fails.
Analogy

- In the case of human intelligence the “real object” is a computer and the “ideal object” is a human
Analogy

- In the case of human intelligence the “real object” is a computer and the “ideal object” is a human

- Turing’s idea is to ask whether computer and human can be distinguished
Analogy

• In the case of human intelligence the “real object” is a computer and the “ideal object” is a human

• Turing’s idea is to ask whether computer and human can be distinguished

• In the case of blockcipher goodness the “real object” is a blockcipher and the “ideal object” is a random function
Analogy

• In the case of human intelligence the “real object” is a computer and the “ideal object” is a human

• Turing’s idea is to ask whether computer and human can be distinguished

• In the case of blockcipher goodness the “real object” is a blockcipher and the “ideal object” is a random function

• Asking whether they can be distinguished leads to a famous notion of pseudorandom function due to Goldreich, Goldwasser, and Micali (1986).
Random Functions

Game $\text{Rand}_R$  // here $R$ is a set

procedure $\text{Fn}(x)$
    if $T[x] = \perp$ then $T[x] \leftarrow R$
    return $T[x]$

Adversary $A$

- Make queries to $\text{Fn}$
- Eventually halts with some output

We denote by

$$\Pr \left[ \text{Rand}_R^A \Rightarrow d \right]$$

the probability that $A$ outputs $d$
Example

Game $\text{Rand}_{\{0,1\}^3}$

procedure $\text{Fn}(x)$
if $T[x] = \bot$ then $T[x] \leftarrow \{0, 1\}^3$
return $T[x]$

adversary $A$

$y \leftarrow \text{Fn}(01)$
return $(y = 000)$

$$\Pr \left[ \text{Rand}^A_{\{0,1\}^3} \Rightarrow \text{true} \right] = \left(\frac{1}{2}\right)^3 = \frac{1}{8}$$
Another Example

Game $\text{Rand}_{\{0,1\}^3}$

procedure $\text{Fn}(x)$
if $T[x] = \bot$ then $T[x] \leftarrow \{0, 1\}^3$
return $T[x]$

adversary $A$
$y_1 \leftarrow \text{Fn}(00)$
$y_2 \leftarrow \text{Fn}(11)$
return $(y_1 \oplus y_2 = 101)$

$$\Pr \left[ \text{Rand}_A^{\{0,1\}^3} \Rightarrow \text{true} \right] = \frac{1}{8}$$
The Games

Let \( F: \text{Keys} \times \text{Dom} \to \text{Rng} \) be a family of functions.

\[
\begin{array}{ll}
\text{Game Real}_F \\
\text{procedure Initialize} \\
K \leftarrow^\$ \text{Keys} \\
\text{procedure Fn}(x) \\
\text{Return } F_K(x)
\end{array}
\quad
\begin{array}{ll}
\text{Game Rand}_{\text{Rng}} \\
\text{procedure Fn}(x) \\
\text{if } T[x] = \bot \text{ then } T[x] \leftarrow^\$ \text{Rng} \\
\text{Return } T[x]
\end{array}
\]

Associated to \( F, A \) are the probabilities

\[
\Pr \left[ \text{Real}_F^A \Rightarrow 1 \right] \quad \text{and} \quad \Pr \left[ \text{Rand}_{\text{Rng}}^A \Rightarrow 1 \right]
\]

that \( A \) outputs 1 in each world. The \textit{advantage} of \( A \) is

\[
\text{Adv}_{F}^{\text{prf}}(A) = \Pr \left[ \text{Real}_F^A \Rightarrow 1 \right] - \Pr \left[ \text{Rand}_{\text{Rng}}^A \Rightarrow 1 \right]
\]
Advantage

<table>
<thead>
<tr>
<th>A's output ( d )</th>
<th>Intended meaning: I think I am in game</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Real</td>
</tr>
<tr>
<td>0</td>
<td>Random</td>
</tr>
</tbody>
</table>

\( \text{Adv}^\text{prf}_F (A) \approx 1 \) means \( A \) is doing well and \( F \) is not prf-secure.

\( \text{Adv}^\text{prf}_F (A) \approx 0 \) (or \( \leq 0 \)) means \( A \) is doing poorly and \( F \) resists the attack \( A \) is mounting.
Security

Adversary advantage depends on its
- strategy
- resources: Running time $t$ and number $q$ of oracle queries

Security: $F$ is a (secure) PRF if $\text{Adv}^\text{prf}_F(A)$ is “small” for ALL $A$ that use “practical” amounts of resources.

Example: 80-bit security could mean that for all $n = 1, \ldots, 80$ we have

$$\text{Adv}^\text{prf}_F(A) \leq 2^{-n}$$

for any $A$ with time and number of oracle queries at most $2^{80-n}$.

Insecurity: $F$ is insecure (not a PRF) if we can specify an $A$ using “few” resources that achieves “high” advantage.
Example

Define $F: \{0, 1\}^\ell \times \{0, 1\}^\ell \to \{0, 1\}^\ell$ by $F_K(x) = K \oplus x$ for all $K, x \in \{0, 1\}^\ell$. Is $F$ a secure PRF?

<table>
<thead>
<tr>
<th>Game Real$_F$</th>
<th>Game Rand$_{{0,1}^\ell}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>procedure Initialize</td>
<td>procedure Fn$_x$</td>
</tr>
<tr>
<td>$K \leftarrow^$ Keys</td>
<td>if $T[x] = \perp$ then $T[x] \leftarrow^$ ${0, 1}^\ell$</td>
</tr>
<tr>
<td>procedure Fn$_x$</td>
<td>Return $T[x]$</td>
</tr>
<tr>
<td>Return $K \oplus x$</td>
<td></td>
</tr>
</tbody>
</table>

So we are asking: Can we design a low-resource $A$ so that

$$\text{Adv}^\text{prf}_F(A) = \Pr[\text{Real}_F^A \Rightarrow 1] - \Pr[\text{Rand}_{\{0,1\}^\ell}^A \Rightarrow 1]$$

is close to 1?
The Adversary

Adversary $A$

$y \leftarrow \text{Fn}(0^e)$

$y' \leftarrow \text{Fn}(1^e)$

If $y = y'$ then return 1
Else return 0

$\text{Adv Prof}_F(A) = \Pr[\text{REAL}_F \rightarrow 1]$

$- \Pr[\text{RAND}_{0,1}^e \rightarrow 1]$
Real Game Analysis

Claim.

\[
\Pr[\text{REAL}^+ F \Rightarrow 1] = 1
\]

Proof: by code of A and of F.
Claim

\[
\Pr[\text{RAND}_{\mathcal{E}}^A \Rightarrow 1] = \frac{1}{2^x}.
\]

Proof: \( y, y' \) are iid random.
Conclusion

By claims, 

$$\text{Adv}^{prf}_f(\mathcal{A}) = 1 - 2^{-\ell} \approx 1.$$
Blockcipher Attacks

Let \( E : \{0, 1\}^k \times \{0, 1\}^\ell \rightarrow \{0, 1\}^\ell \) be a block cipher.

<table>
<thead>
<tr>
<th>Game Real(_E)</th>
<th>Game Rand(_{{0,1}^\ell})</th>
</tr>
</thead>
<tbody>
<tr>
<td>procedure (\text{Initialize}) (K \leftarrow {0, 1}^k)</td>
<td>procedure (\text{Fn}(x)) if (T[x] = \perp) then (T[x] \leftarrow {0, 1}^\ell)</td>
</tr>
<tr>
<td>procedure (\text{Fn}(x)) Return (E_K(x))</td>
<td>Return (T[x])</td>
</tr>
</tbody>
</table>

Can we design \(A\) so that

\[
\text{Adv}^{\text{prf}}_E (A) = \Pr \left[ \text{Real}^A_E \rightarrow 1 \right] - \Pr \left[ \text{Rand}^A_{\{0,1\}^\ell} \rightarrow 1 \right]
\]

is close to 1?
Idea

Defining property of a block cipher: $E_K$ is a permutation for every $K$

So if $x_1, \ldots, x_q$ are distinct then

- $F_n = E_K \Rightarrow F_n(x_1), \ldots, F_n(x_q)$ distinct
- $F_n$ random $\Rightarrow F_n(x_1), \ldots, F_n(x_q)$ not necessarily distinct

This leads to the following attack:

**adversary $A$**

Let $x_1, \ldots, x_q \in \{0, 1\}^\ell$ be distinct
for $i = 1, \ldots, q$ do $y_i \leftarrow F_n(x_i)$
if $y_1, \ldots, y_q$ are all distinct then return 1
else return 0

$\text{Adv}_{E}^{\text{prf}}(A) = \Pr \left[ \text{REAL}_{e} \Rightarrow 1 \right]$
Real World Analysis

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

<table>
<thead>
<tr>
<th>Game $\text{Real}_E$</th>
<th>adversary $A$</th>
</tr>
</thead>
</table>
| **procedure Initialize**  
$K \leftarrow \{0, 1\}^k$  
**procedure $\text{Fn}(x)$**  
Return $E_K(x)$ | Let $x_1, \ldots, x_q \in \{0, 1\}^\ell$ be distinct  
for $i = 1, \ldots, q$ do $y_i \leftarrow \text{Fn}(x_i)$  
if $y_1, \ldots, y_q$ are all distinct  
then return 1 else return 0 |

Then

$$\Pr \left[ \text{Real}_E^A \Rightarrow 1 \right] = 1$$

Proof: $\text{Fn} = E_K$ is a permutation $\Rightarrow$ $y_1, \ldots, y_q$ distinct.
Ideal World Analysis

Let $E: \{0, 1\}^K \times \{0, 1\}^\ell \rightarrow \{0, 1\}^\ell$ be a block cipher.

Game $\text{Rand}_{\{0,1\}^\ell}$

procedure $\text{Fn}(x)$
if $T[x] = \bot$ then $T[x] \leftarrow \{$0, 1$\}^\ell$
Return $T[x]$

adversary $A$
Let $x_1, \ldots, x_q \in \{0, 1\}^\ell$ be distinct
for $i = 1, \ldots, q$ do $y_i \leftarrow \text{Fn}(x_i)$
if $y_1, \ldots, y_q$ are all distinct then return 1 else return 0

$\Pr[\text{RAND}^{\text{A}}_{\{0,1\}^\ell} = 1] \geq 1 - \frac{q^2}{2^\ell}$
Birthday Bound

Pick \( y_1, \ldots, y_q \leftarrow \{1, \ldots, N\} \) and let

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

Birthday setting: \( N = 365 \)

Fact: \( C(N, q) \approx \frac{q^2}{2N} \)

\[
\geq 0.3 \frac{q^2}{N}
\]
Ideal game analysis

Let \( E : \{0, 1\}^K \times \{0, 1\}^\ell \to \{0, 1\}^\ell \) be a block cipher

<table>
<thead>
<tr>
<th>Game Rand_{0,1}^\ell</th>
</tr>
</thead>
<tbody>
<tr>
<td>procedure ( \text{Fn}(x) )</td>
</tr>
<tr>
<td>if ( T[x] = \perp ) then ( T[x] \leftarrow {0, 1}^\ell )</td>
</tr>
<tr>
<td>Return ( T[x] )</td>
</tr>
</tbody>
</table>

adversary \( A \)

Let \( x_1, \ldots, x_q \in \{0, 1\}^\ell \) be distinct for \( i = 1, \ldots, q \) do \( y_i \leftarrow \text{Fn}(x_i) \)
if \( y_1, \ldots, y_q \) are all distinct then return 1 else return 0

Then

\[
\Pr \left[ \text{Rand}_{0,1}^A \Rightarrow 1 \right] = \Pr [y_1, \ldots, y_q \text{ all distinct}] = 1 - C(2^\ell, q)
\]

because \( y_1, \ldots, y_q \) are randomly chosen from \( \{0, 1\}^\ell \).
Key vs block length

Conclusion: If $E : \{0, 1\}^k \times \{0, 1\}^\ell \rightarrow \{0, 1\}^\ell$ is a block cipher, there is an attack on it as a PRF that succeeds in about $2^{\ell/2}$ queries.

Depends on block length, not key length!

<table>
<thead>
<tr>
<th></th>
<th>$\ell$</th>
<th>$2^{\ell/2}$</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>DES, 2DES, 3DES3</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>
**KR-security vs PRF-security**

We have seen two possible metrics of security for a block cipher $E$

- **KR-security:** It should be hard to find a key consistent with input-output examples of a hidden target key.
- **PRF-security:** It should be hard to distinguish the input-output behavior of $E_K$ from that of a random function.

**Fact:** PRF-security of $E$ implies

- KR-security of $E$
- Many other security attributes of $E$

This is a validation of the choice of PRF security as our main metric.
Proposition

**Proposition:** Let $E : \{0, 1\}^k \times \{0, 1\}^\ell \rightarrow \{0, 1\}^\ell$ be a blockcipher. Given a kr-adversary $B$ making $q$ (distinct!) oracle queries, we can construct a PRF adversary $A$ making $q$ oracle queries such that

$$\text{Adv}^\text{kr}_E(B) \leq \text{Adv}^\text{prf}_E(A) + 2^{k-q\ell}.$$ 

The running time of $A$ is that of $B$ plus $O(q\ell)$.

**Interpretation:**

- $E$ is PRF secure $\Rightarrow$ $\text{Adv}^\text{prf}_E(A)$ is small
  $\Rightarrow$ $\text{Adv}^\text{kr}_E(B)$ is small
  $\Rightarrow$ $E$ is KR-secure.

**Example:** If $E = AES$ and $q = 2$ then $2^{k-q\ell} = 2^{-128}$.

Our first example of a reduction and a proof by reduction!
Adversary

Given KR-adversary $B$, define

$\text{Adversary } A \leftarrow \text{For REAL game } \text{Fn}(\cdot) \leftarrow \text{Fn}(x) = Fk_c(x_i) \text{ for } 1 \leq i \leq q$

Run $B$

- When $B$ makes $i$-th $\text{Fn}$-query $x_i$ do:
  $y_i \leftarrow \text{Fn}(x_i)$ for REAL game
  Return $y_i$. This is $F_k(x_i)$

When $B$ halts with output $1$

Return 1 if $\forall 1 \leq i \leq q \ y_i = F_k(x_i)$
Else return 0
Real game analysis

\[ P \left[ \text{REAL}_F^A \Rightarrow 1 \right] = P \left[ \text{REAL}_F^B \Rightarrow 1 \right] = \text{Ad}_{\chi_F}^{\text{RR}} (B) \]
Ideal game analysis

Claim: \[ \Pr[\text{RAND} \text{ is } 17] \geq 2^{k-92} \]
Our Assumptions

• We can assume DES and AES are “ideal” blockciphers in are “as PRF-secure as possible”
Our Assumptions

- We can assume DES and AES are “ideal” blockciphers in are “as PRF-secure as possible”

- Note exhaustive key search, birthday attacks
PRP-Security
2 The PRP/PRF Switching Lemma

The Lemma. The natural and conventional assumption to make about a blockcipher is that it behaves as a pseudorandom permutation (PRP). However, it usually turns out to be easier to analyze the security of a blockcipher-based construction assuming the blockcipher is secure as a pseudorandom function (PRF). The gap is then bridged (meaning, a result about the security of the construct assuming the blockcipher is a PRP is obtained) using the following lemma. In what follows, we denote by \( A^P \Rightarrow 1 \) the event that adversary \( A \), equipped with an oracle \( P \), outputs the bit 1. Let \( \text{Perm}(n) \) be the set of all permutations on \( \{0,1\}^n \) and let \( \text{Func}(n) \) be the set of all functions from \( \{0,1\}^n \) to \( \{0,1\}^n \). We assume below that \( \pi \) is randomly sampled from \( \text{Perm}(n) \) and \( \rho \) is randomly sampled from \( \text{Func}(n) \).

Lemma 1 [PRP/PRF Switching Lemma] Let \( n \geq 1 \) be an integer. Let \( A \) be an adversary that asks at most \( q \) oracle queries. Then

\[
| \Pr [ A^\pi \Rightarrow 1 ] - \Pr [ A^\rho \Rightarrow 1 ] | \leq \frac{q(q-1)}{2^{n+1}}. \]
