Lecture 4 – Pseudorandom Functions

CS466 - Applied Cryptography

Adam O'Neill

adapted from http://cseweb.ucsd.edu/~mihir/cse107/

What is a “good” blockcipher?

We want to define a notion of a “good” blockcipher, where “good” means natural uses of the blockcipher are secure.

What is a “good” blockcipher?

We want to define a notion of a “good” blockcipher, where “good” means natural uses of the blockcipher are secure.

One idea is to list requirements:

What is a “good” blockcipher?

We want to define a notion of a “good” blockcipher, where “good” means natural uses of the blockcipher are secure.

One idea is to list requirements:

- Key recovery is hard.

BAD APPROACH!

What is a "good" blockcipher?

We want to define a notion of a "good" blockcipher, where "good" means natural uses of the blockcipher are secure.

One idea is to list requirements:

- Key recovery is hard.
- Message recovery is hard.

- XOR of the inputs

- But... what if it's easy to recover "most" of the input
- one bit of the input

Analogy to Intelligence

What if we want to define the notion of "intelligent" for a computer program?

like a human

Analogy to Intelligence

What if we want to define the notion of "intelligent" for a computer program?

Again, one idea is to list requirements:

Analogy to Intelligence

What if we want to define the notion of "intelligent" for a computer program?

Again, one idea is to list requirements:

- It can be happy.

Analogy to Intelligence

What if we want to define the notion of "intelligent" for a computer program?

Again, one idea is to list requirements:

- It can be happy.
- It can multiply numbers

Analogy to Intelligence

What if we want to define the notion of "intelligent" for a computer program?

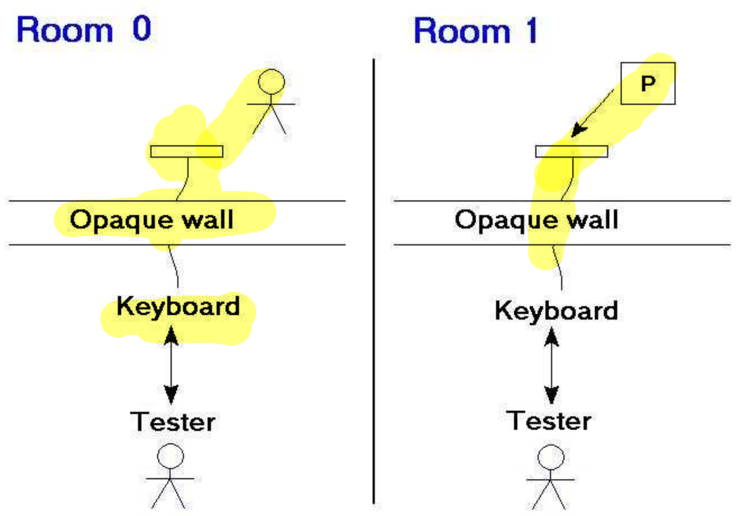
Again, one idea is to list requirements:

- It can be happy.
- It can multiply numbers
- … but only small numbers.

Turing’s Answer

A program is “intelligent” if its input/output behavior is indistinguishable from that of a human.

The Turing Test



Game:

- Put tester in room 0 and let it interact with object behind wall
- Put tester in rooom 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.

real-ideal paradigm

The Analogy

random function

Notion	Real object	Ideal object
Intelligence	Program	Human
PRF	Block cipher	?

pseudorandom function

new notion of security for a blockcipher

Output of Rand is output of adversary

Random Functions

Game Rand_R // here R is a set

procedure Fn(x)

if $\mathsf{T}[x] = \perp$ then $\mathsf{T}[x] \xleftarrow{\$} R$

return $\mathsf{T}[x]$

Stateful

Adversary A

- Make queries to **Fn**
- Eventually halts with some output

We denote by

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

the probability that A outputs d

$d = 1$ "I think I'm interacting w/ ~~the~~ real block cipher"

$R = \{0,1\}^3$

Random Functions

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

procedure Fn(x)

if $\mathsf{T}[x] = \perp$ then $\mathsf{T}[x] \xleftarrow{\$} \{0,1\}^3$

return $\mathsf{T}[x]$

adversary A

$y \leftarrow \mathbf{Fn}(01)$

return $(y = 000)$

$$\Pr\left[\mathrm{Rand}^{A}_{\{0,1\}^3} \Rightarrow \mathsf{true}\right] = \frac{1}{8}$$

Random Functions

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

procedure Fn(x)

if $\mathsf{T}[x] = \perp$ then $\mathsf{T}[x] \xleftarrow{\$} \{0,1\}^3$

return $\mathsf{T}[x]$

adversary A

$y_1 \leftarrow \mathbf{Fn}(00)$

$y_2 \leftarrow \mathbf{Fn}(11)$

return $(y_1 = 010 \wedge y_2 = 011)$

$$\Pr\left[\mathrm{Rand}^{A}_{\{0,1\}^3} \Rightarrow \mathsf{true}\right] = 1/64$$

uses independence!

Random Functions

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

procedure Fn(x)

if $\mathsf{T}[x] = \perp$ then $\mathsf{T}[x] \xleftarrow{\$} \{0,1\}^3$

return $\mathsf{T}[x]$

adversary A

$y_1 \leftarrow \mathbf{Fn}(00)$

$y_2 \leftarrow \mathbf{Fn}(11)$

return $(y_1 \oplus y_2 = 101)$

$$\Pr\left[\mathrm{Rand}^{A}_{\{0,1\}^3} \Rightarrow \mathsf{true}\right] = \underline{\underline{1/8}}$$

Function Families

A family of functions $F : \text{Keys}(F) \times \text{Dom}(F) \to \text{Range}(F)$ is a two-argument map. For $K \in \text{Keys}(F)$ we let $F_K : \text{Dom}(F) \to \text{Range}(F)$ be defined by

$$\forall x \in \text{Dom}(F) : F_K(x) = F(K, x)$$

Examples:

- DES: $\text{Keys} = \{0,1\}^{56}$, $\text{D} = \text{R} = \{0,1\}^{64}$
- Any block cipher: $\text{D} = \text{R}$ and each F_K is a permutation

but not just block ciphers

ie when the function induced by a key is not a permutation

We want to codify the definition now...

Intuition

Notion	Real object	Ideal object
PRF	Family of functions (eg. a block cipher)	Random function

F is a PRF if the input-output behavior of F_K looks to a tester like the input-output behavior of a random function.

Tester does not get the key K!

The Games

for block cipher E_K

exactly what we already discussed

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

If $T[x]$ is defined

Game Real_F	Game $\text{Rand}_{\text{Range}(F)}$
procedure Initialize $K \xleftarrow{\$} \text{Keys}(F)$ **procedure Fn**(x) Return $F_K(x)$	**procedure Fn**(x) $T[x] \xleftarrow{\$} \text{Range}(F)$ Return $T[x]$

assume DISTINCT queries

Associated to F, A are the probabilities

$$\Pr\left[\text{Real}_F^A \Rightarrow 1\right] \quad \middle| \quad \Pr\left[\text{Rand}_{\text{Range}(F)}^A \Rightarrow 1\right]$$

that A outputs 1 in each world. The advantage of A is

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

wlog advantage is btw 0 and 1

Steps to show E is not a PRF:

① give adversary A
(A can call F_n)

② Give lower bound on
$$\Pr[\text{Game-Real}_E^A \Rightarrow 1]$$
prove it.

② Give upper bound on
$$\Pr[\text{Game-Rand}_E^A \Rightarrow 1]$$
prove it.

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

PRF advantage

A's output d	Intended meaning: I think I am in game
1	Real
0	Random

$\mathbf{Adv}_F^{\mathrm{prf}}(A) \approx 1$ means A is doing well and F is not prf-secure.
$\mathbf{Adv}_F^{\mathrm{prf}}(A) \approx 0$ (~~or ≤ 0~~) means A is doing poorly and F resists the attack A is mounting.

Intuitive statement

PRF Security

bits of security

Adversary advantage depends on its

- strategy
- resources: Running time t and number q of oracle queries

Security: F is a (secure) PRF if $\mathbf{Adv}_F^{\mathrm{prf}}(A)$ 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

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

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

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

To show a function family F is not a PRF, we need to give an adversary A s.t.

$$\mathrm{Adv}_F^{prf}(A) := \Pr\left[\mathrm{REAL}_F^A \Rightarrow 1\right] - \Pr\left[\mathrm{RAND}_F^A \Rightarrow 1\right]$$

is LARGE.

Steps:

1. Give pseudocode for A.
2. LOWER-BOUND
3. UPPER-BOUND

$E : \{0,1\}^k \times \{0,1\}^\ell \to \{0,1\}^\ell$

$E_k(x) = x. \quad \forall k, x$

Claim. E is NO a PRF.

proof. Adversary A

$y \leftarrow Fn(0^\ell)$

If $y = 0^\ell$ ret 1

Else r

wants to guess whether $Fn = E_k$ or $F = \$$

① give adversary

② $\Pr[REAL_E^A \Rightarrow 1] = 1$

$\forall k,$

proof: If $Fn = E_k$ then

$Fn(0^\ell) = E_k(0^\ell) = 0^\ell$ ✓

by def of E.

③ $\Pr[RAND_E^A \Rightarrow 1] = \frac{1}{2^\ell}.$

proof of 3:

If $F_n = \$$ then

$$\Pr[F_n(0^\ell) = 0^\ell] = \frac{1}{2^\ell}$$

$\Rightarrow$ F_n implements $*$

Examples

"bot"
error or
empty
symbol

F 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?

def.

Game Real_F	Game $\mathrm{Rand}_{\{0,1\}^\ell}$
procedure Initialize	**procedure Fn**(x)
$K \xleftarrow{\$} \{0,1\}^\ell$	if $\mathsf{T}[x] = \perp$ then $\mathsf{T}[x] \xleftarrow{\$} \{0,1\}^\ell$
procedure Fn(x)	Return $\mathsf{T}[x]$
Return $K \oplus x$	

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

1

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

is close to 1?

2

3

Examples

Exploitable weakness of F: For all K we have

$$F_K(0^\ell) \oplus F_K(1^\ell) = (K \oplus 0^\ell) \oplus (K \oplus 1^\ell) = 1^\ell$$

proof of 1

Examples

e.g. $\ell = 2$

Exploitable weakness of F: For all K we have

$$F_K(0^\ell) \oplus F_K(1^\ell) = (\cancel{K} \oplus 0^\ell) \oplus (\cancel{K} \oplus 1^\ell) = 1^\ell$$

10   11 $= 11 \oplus 01$ $= 10$

1 F: $\{0,1\}^\ell \times \{0,1\}^\ell \to \{0,1\}^\ell$ is defined by $F_K(x) = K \oplus x$.

adversary A

if $\mathbf{Fn}(0^\ell) \oplus \mathbf{Fn}(1^\ell) = 1^\ell$ then return 1 else return 0

$c_1 = F_n(01)$ $\qquad 01 \oplus k$

$\rightarrow F_n(c_1)$ is it 01?

KEY RECOVERY ATTACK

(1) Adversary A

$K' \leftarrow F_n(0^\ell)$

$C \leftarrow F_n(1^\ell)$

If $C = K' \oplus 1^\ell$

return 1

Else return 0.

(2) $\Pr[\mathrm{REAL}_F^A \Rightarrow 1] = 1.$

by definition of F.

(3) $\Pr[\mathrm{RAND}_F^A \Rightarrow 1] = 2^{-\ell}$

Real game analysis

2

F: $\{0,1\}^\ell \times \{0,1\}^\ell \to \{0,1\}^\ell$ is defined by $F_K(x) = K \oplus x$.

adversary A
if $\mathbf{Fn}(0^\ell) \oplus \mathbf{Fn}(1^\ell) = 1^\ell$ then return 1 else return 0

Game Real_F

procedure Initialize
$K \xleftarrow{\$} \{0,1\}^\ell$

procedure Fn(x)
Return $K \oplus x$

$$\Pr\left[\mathrm{Real}_F^A \Rightarrow 1\right] = 1$$

3

Rand game analysis

$F\colon \{0,1\}^\ell \times \{0,1\}^\ell \to \{0,1\}^\ell$ is defined by $F_K(x) = K \oplus x$.

adversary A

if $\mathbf{Fn}(0^\ell) \oplus \mathbf{Fn}(1^\ell) = 1^\ell$ then return 1 else return 0

Game $\mathrm{Rand}_{\{0,1\}^\ell}$
procedure Fn(x)
if $\mathsf{T}[x] = \perp$ then $\mathsf{T}[x] \xleftarrow{\$} \{0,1\}^\ell$
Return $\mathsf{T}[x]$

$$\Pr\left[\mathrm{Rand}^A_{\{0,1\}^\ell} \Rightarrow 1\right] = \frac{1}{2^\ell}$$

Putting It Together

F: $\{0,1\}^\ell \times \{0,1\}^\ell \to \{0,1\}^\ell$ is defined by $F_K(x) = K \oplus x$.

adversary A
if $\mathbf{Fn}(0^\ell) \oplus \mathbf{Fn}(1^\ell) = 1^\ell$ then return 1 else return 0

Then

$$\begin{aligned}\mathbf{Adv}^{\mathrm{prf}}_F(A) &= \overbrace{\Pr\left[\mathrm{Real}^A_F \Rightarrow 1\right]}^{1} - \overbrace{\Pr\left[\mathrm{Rand}^A_{\{0,1\}^\ell} \Rightarrow 1\right]}^{2^{-\ell}} \\ &= 1 - 2^{-\ell}\end{aligned}$$

and A is efficient .

Conclusion: F is not a secure PRF.

Blockciphers as PRFs

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

Game Real_E

procedure Initialize
$K \xleftarrow{\$} \{0,1\}^k$

procedure Fn(x)
Return $E_K(x)$

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

procedure Fn(x)
if $\mathsf{T}[x] = \perp$ then $\mathsf{T}[x] \xleftarrow{\$} \{0,1\}^\ell$
Return $\mathsf{T}[x]$

Can we design A so that

$$\mathbf{Adv}^{\mathrm{prf}}_{E}(A) = \Pr\left[\mathrm{Real}_E^A \Rightarrow 1\right] - \Pr\left[\mathrm{Rand}_{\{0,1\}^\ell}^A \Rightarrow 1\right]$$

is close to 1?

Generic Attacks on blockciphers as PRFs

Generic Attacks on blockciphers as PRFs

Exhaustive Key Search Attack

Generic Attacks on blockciphers as PRFs

Generic Attacks on blockciphers as PRFs

Birthday Attack

Birthday Attack

We have q people $1, \ldots, q$ with birthdays $y_1, \ldots, y_q \in \{1, \ldots, 365\}$. Assume each person's birthday is a random day of the year. Let

$$
\begin{aligned}
C(365, q) &= \Pr[2 \text{ or more persons have same birthday}] \\
&= \Pr[y_1, \ldots, y_q \text{ are not all different}]
\end{aligned}
$$

- What is the value of $\boxed{C(365, q)?}$
- How large does q have to be before $C(365, q)$ is at least $1/2$?

Naive intuition:

- $C(365, q) \approx q/365$
- q has to be around 365

The reality

- $C(365, q) \approx q^2/365$
- q has to be only around 23

$C(n, q)$ is the probability of collision when q values are chosen from domain of size n.

Birthday Collision Bounds

$C(365, q)$ is the probability that some two people have the same birthday in a room of q people with random birthdays

q	$C(365, q)$
15	0.253
18	0.347
20	0.411
21	0.444
23	$\boxed{0.507}$
25	0.569
27	0.627
30	0.706
35	0.814
40	0.891
50	0.970

$1/2$

50

Birthday problem

Pick $y_1, \ldots, y_q \xleftarrow{\$} \{1, \ldots, N\}$ and let

$$C(N,q) = \Pr\left[y_1, \ldots, y_q \textbf{ not all distinct}\right]$$

Birthday setting: $N = 365$

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

Birthday collision formula

Let $y_1, \ldots, y_q \xleftarrow{\$} \{1, \ldots, N\}$. Then

$$\begin{aligned} 1 - C(N,q) &= \Pr\left[y_1, \ldots, y_q \text{ all distinct}\right] \\ &= 1 \cdot \frac{N-1}{N} \cdot \frac{N-2}{N} \cdot \cdots \cdot \frac{N-(q-1)}{N} \\ &= \prod_{i=1}^{q-1} \underline{\left(1 - \frac{i}{N}\right)} \end{aligned}$$

so

$$C(N,q) = 1 - \underline{\prod_{i=1}^{q-1} \left(1 - \frac{i}{N}\right)}$$

$1 - x \leq e^{-x}$

Birthday bounds

Let

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

Fact: Then

$$\boxed{0.3 \cdot \frac{q(q-1)}{N} \le C(N,q) \le 0.5 \cdot \frac{q(q-1)}{N}}$$

where the lower bound holds for $1 \le q \le \sqrt{2N}$.

Birthday attack adversary

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

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

- $\mathbf{Fn} = E_K \Rightarrow \mathbf{Fn}(x_1), \ldots, \mathbf{Fn}(x_q)$ distinct
- $\mathbf{Fn}$ random $\Rightarrow \mathbf{Fn}(x_1), \ldots, \mathbf{Fn}(x_q)$ not necessarily distinct

This leads to the following attack:

adversary A // bday attack adversary

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

What's the advantage of A?

Real game analysis

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

Game Real_E
procedure Initialize
$K \xleftarrow{\$} \{0,1\}^k$
procedure Fn(x)
Return $E_K(x)$

adversary A

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

Then

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

Since E_K is a permutation for every K.

Rand game analysis

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

Game $\mathrm{Rand}_{\{0,1\}^\ell}$
procedure Fn(x)
if $\mathsf{T}[x] = \perp$ then $\mathsf{T}[x] \xleftarrow{\$} \{0,1\}^\ell$
Return $\mathsf{T}[x]$

adversary A

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

Then

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

because $y_1, \ldots, y_q$ are randomly chosen from $\{0,1\}^\ell$.

$C(n,q) \approx \frac{q(q-1)}{2^\ell}$

Birthday attack conclusion

$E : \{0,1\}^k \times \{0,1\}^\ell \to \{0,1\}^\ell$ a block cipher

adversary A

Let $x_1, \ldots, x_q \in \{0,1\}^\ell$ be distinct

for $i = 1, \ldots, q$ do $y_i \leftarrow \mathbf{Fn}(x_i)$

if $y_1, \ldots, y_q$ are all distinct then return 1 else return 0

$$\begin{aligned}\mathbf{Adv}_E^{\mathrm{prf}}(A) &= \overbrace{\Pr\left[\mathrm{Real}_E^A \Rightarrow 1\right]}^{1} - \overbrace{\Pr\left[\mathrm{Rand}_{\{0,1\}^\ell}^A \Rightarrow 1\right]}^{1 - C(2^\ell, q)} \\ &= C(2^\ell, q) \geq 0.3 \cdot \frac{q(q-1)}{2^\ell}\end{aligned}$$

so

$$q \approx 2^{\ell/2} \Rightarrow \mathbf{Adv}_E^{\mathrm{prf}}(A) \approx 1 .$$

Conclusion: If $E : \{0,1\}^k \times \{0,1\}^\ell \to \{0,1\}^\ell$ 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!

	ℓ	$2^{\ell/2}$	Status
DES, 2DES, 3DES3	64	2^{32}	Insecure
AES	128	2^{64}	Secure

PRF-Security Implications

PRF-security can be seen as a "master property" for blockciphers that implies all other security properties we want.

PRF-Security Implications

PRF-security can be seen as a “master property” for blockciphers that implies all other security properties we want.

PRF-Security Implications

PRF-security can be seen as a "master property" for blockciphers that implies all other security properties we want.

E.g., we can show that PRF-security implies security against key-recovery.

KR security vs PRF security

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

- (T)KR-security: It should be hard to find the target key, or 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 (and hence TKR) security of E
- Many other security attributes of E

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

Reduction Sketch

Skip!

Conclusion

- We believe DES, AES are “good” blockciphers in the sense that there is no significantly “better than generic” attacks under the PRF notion.

Conclusion

- We believe DES, AES are "good" blockciphers in the sense that there is no significantly "better than generic" attacks under the PRF notion.
- Generic attacks:

Conclusion

- We believe DES, AES are “good” blockciphers in the sense that there is no significantly “better than generic” attacks under the PRF notion.
- Generic attacks:
  - Exhaustive key-search.

Conclusion

- We believe DES, AES are "good" blockciphers in the sense that there is no significantly "better than generic" attacks under the PRF notion.
- Generic attacks:
  - Exhaustive key-search.
  - Birthday attack.

Exercise

We are given a PRF F: $\{0,1\}^k \times \{0,1\}^k \to \{0,1\}^k$ and want to build a PRF G: $\{0,1\}^k \times \{0,1\}^k \to \{0,1\}^{2k}$. Which of the following work?

1. $\underline{\text{Function } G(K,x)}$
$y_1 \leftarrow F(K,x)$; $y_2 \leftarrow F(K,\overline{x})$; Return $y_1 \| y_2$

2. $\underline{\text{Function } G(K,x)}$
$y_1 \leftarrow F(K,x)$; $y_2 \leftarrow F(K,y_1)$; Return $y_1 \| y_2$

3. $\underline{\text{Function } G(K,x)}$
$L \leftarrow F(K,x)$; $y_1 \leftarrow F(L,0^k)$; $y_2 \leftarrow F(L,1^k)$; Return $y_1 \| y_2$

4. $\underline{\text{Function } G(K,x)}$
[Your favorite code here]