CIS 5371, Fall 2024

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

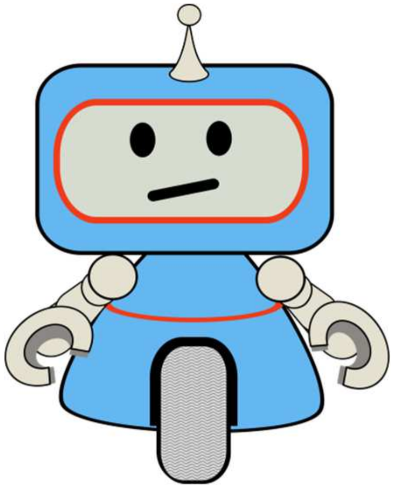
Recall

Possible Properties	Necessary	Sufficient
Security against key recovery	Yes	No
Hard to find M given $C \leftarrow E_K(M)$	Yes	No
…		

Want: a single "master" property that is sufficient to ensure security of common usage of blockcipher.

An Analogy: Turing Test

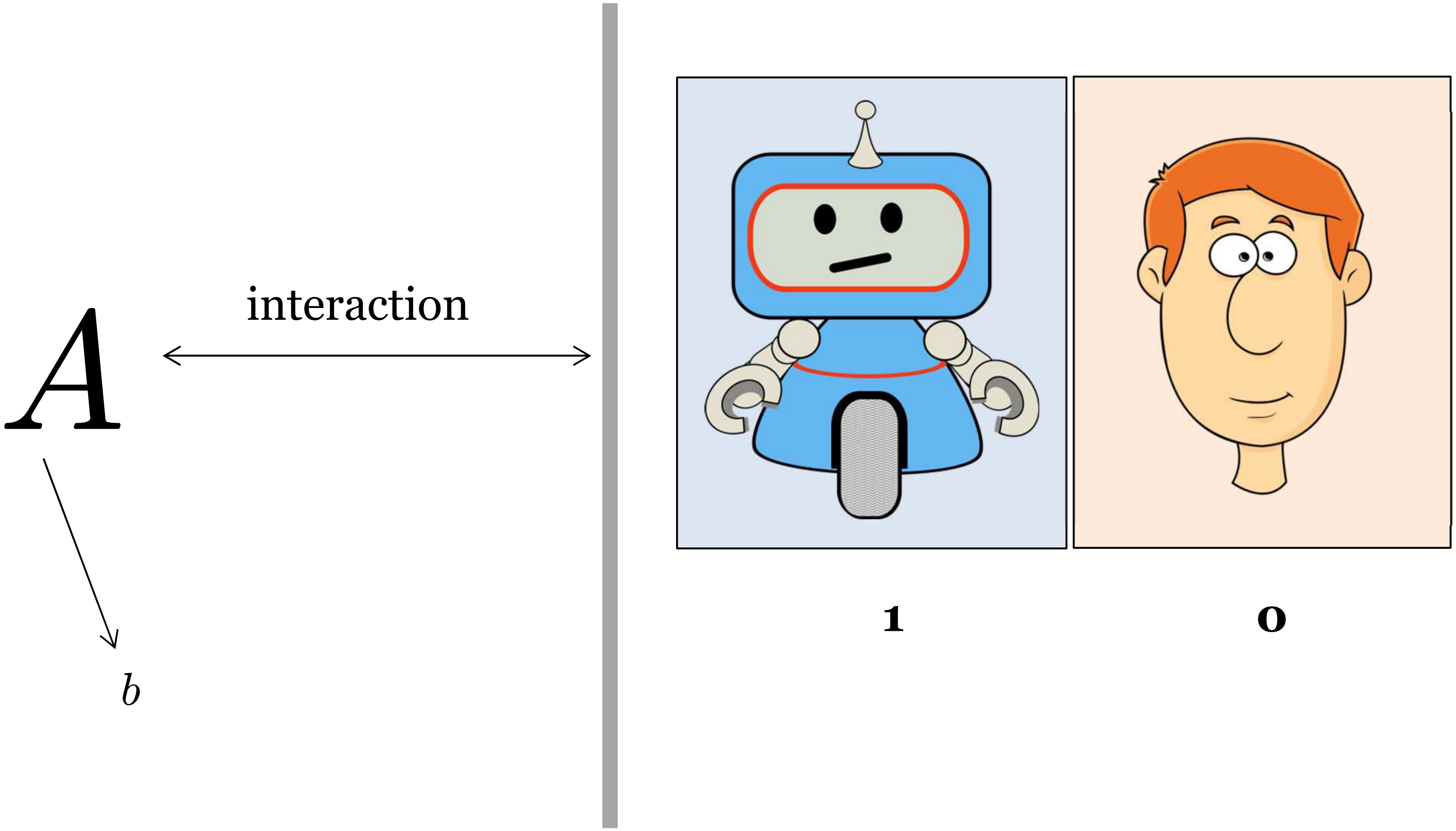
What does it mean for a machine to be “intelligent”?



Possible Answers
It can be happy
It recognizes pictures
…

But no such list is satisfactory

An Analogy: Turing Test



A

interaction

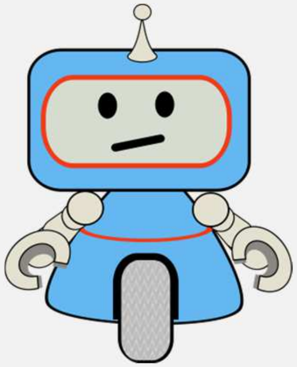
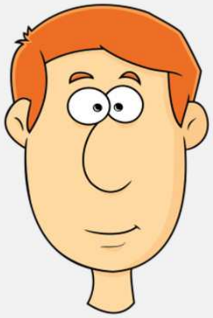
b

1

0

Man (0) or Machine (1)?

Real versus Ideal

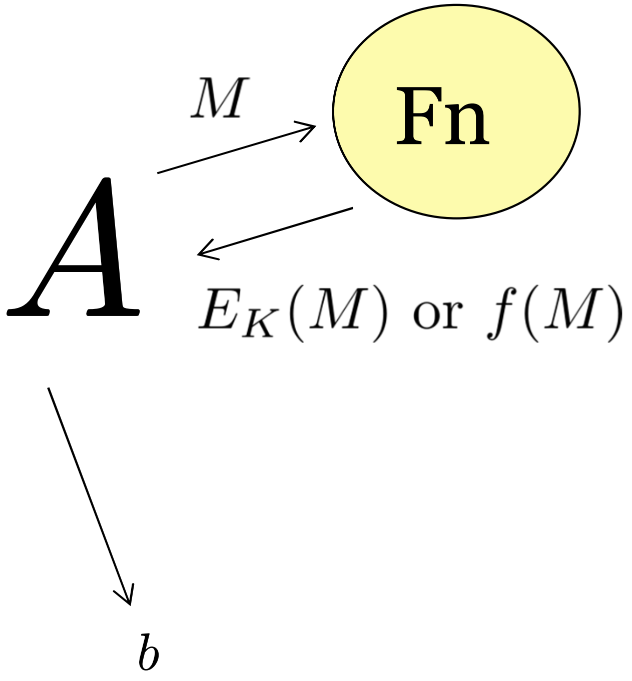
Notion	Real object	Ideal object
Intelligence		
PRF	E_K	Random function

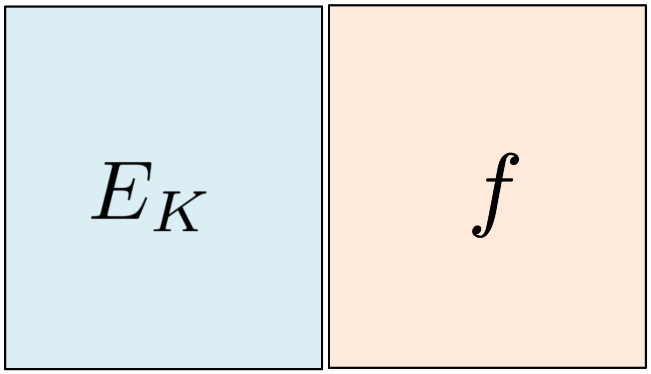
Informal View of PRF Security

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

Sample random $f : \{0,1\}^n \to \{0,1\}^n$

$K \xleftarrow{\$} \mathcal{K}$

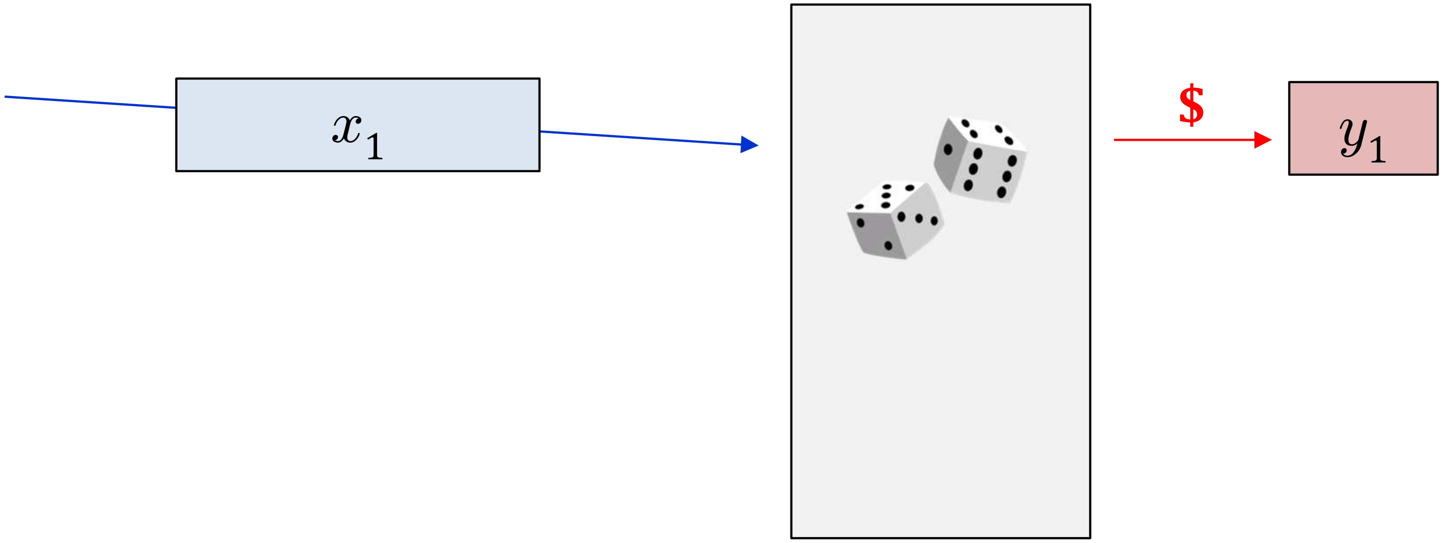




Adversary doesn't know K or f

Defining Random Function: Lazy Sampling

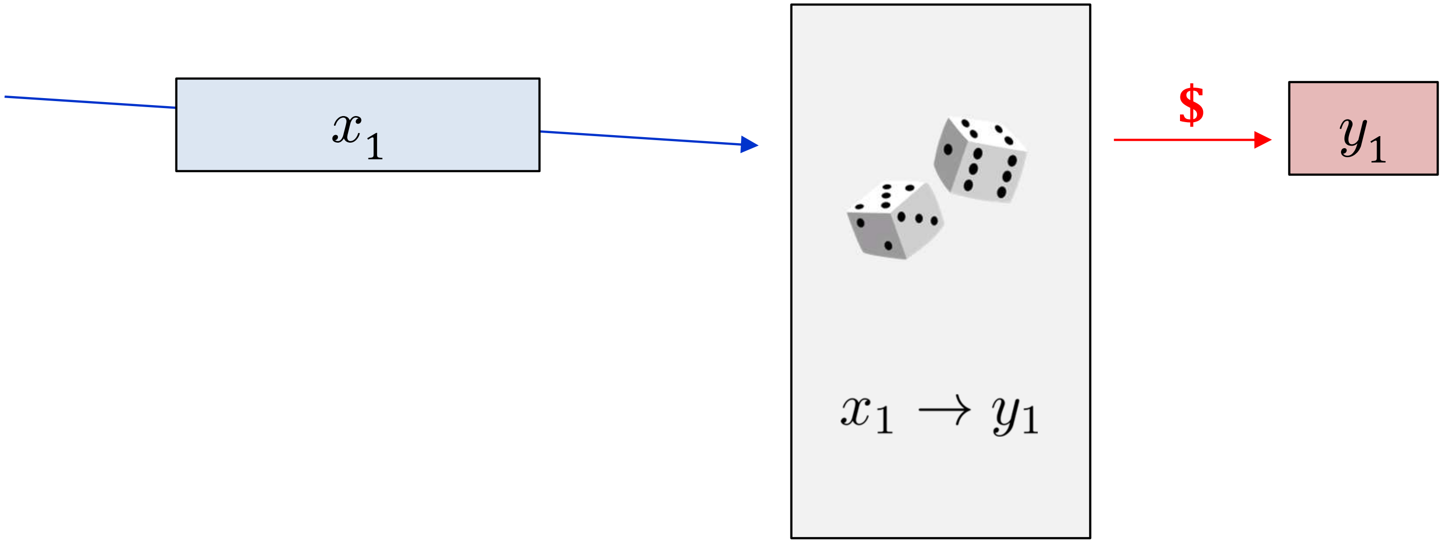
Want: a random function $f : \{0,1\}^n \to \{0,1\}^m$



Pick a fresh random answer for a new query, and remember the answer

Defining Random Function: Lazy Sampling

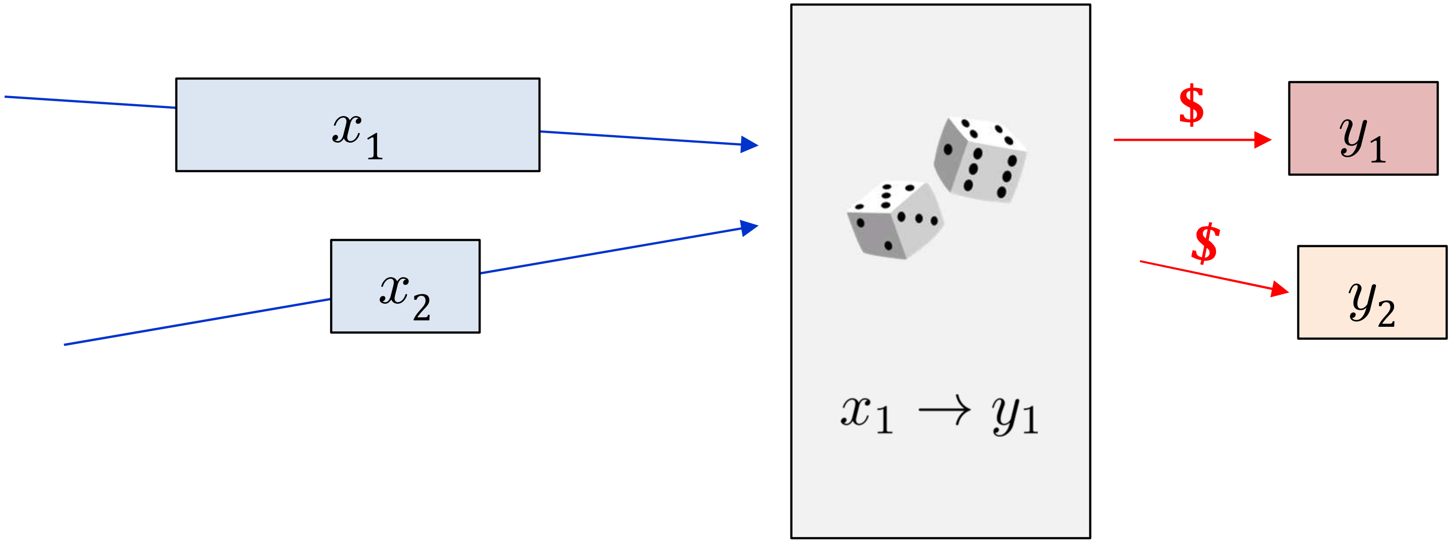
Want: a random function $f : \{0,1\}^n \rightarrow \{0,1\}^m$



Pick a fresh random answer for a new query, and remember the answer

Defining Random Function: Lazy Sampling

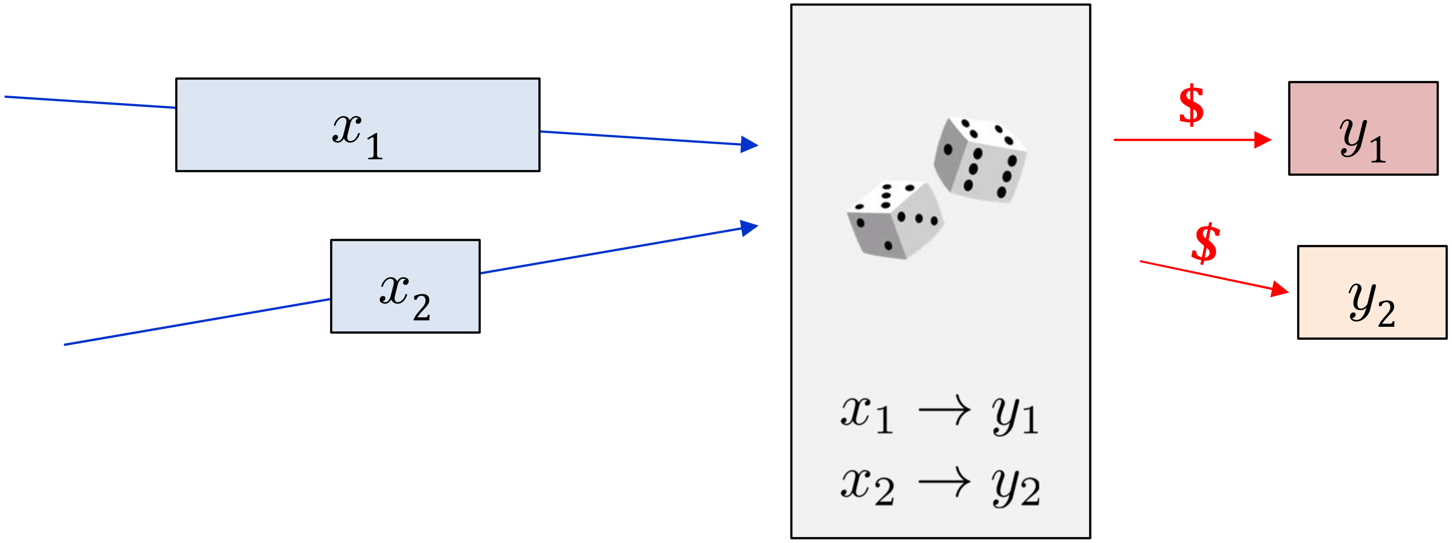
Want: a random function $f : \{0,1\}^n \to \{0,1\}^m$



Pick a fresh random answer for a new query, and remember the answer

Defining Random Function: Lazy Sampling

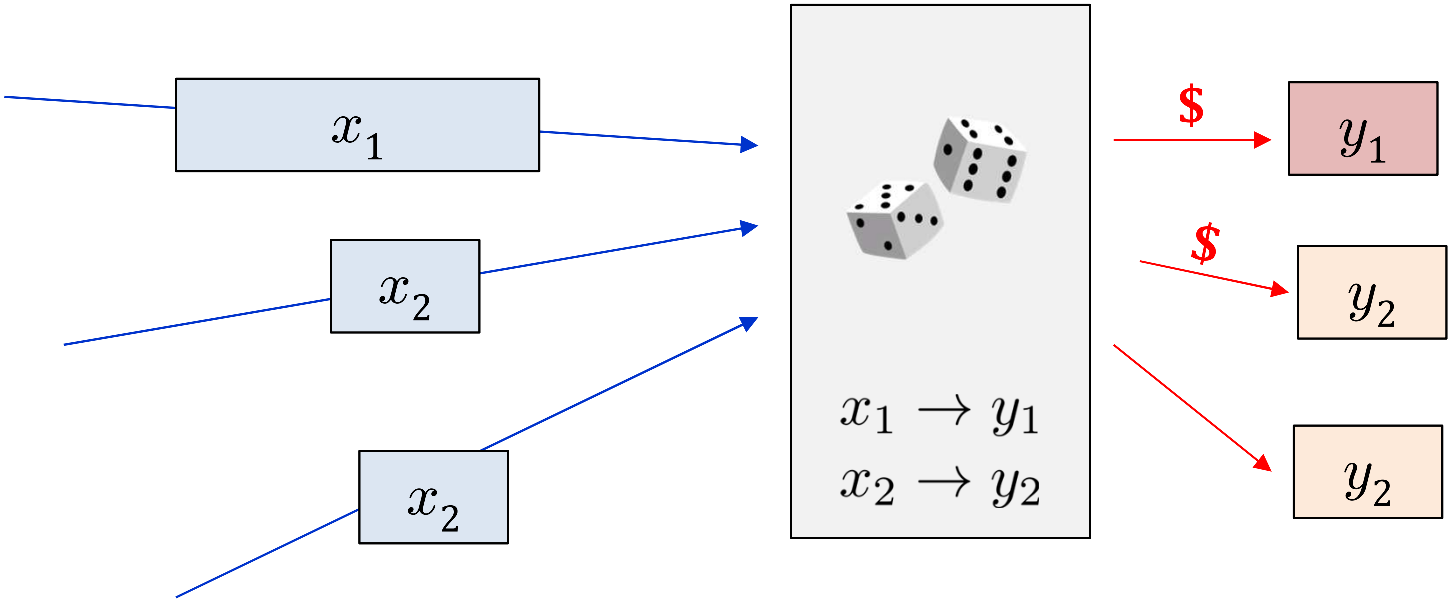
Want: a random function $f : \{0,1\}^n \to \{0,1\}^m$



Pick a fresh random answer for a new query, and remember the answer

Reuse Prior Answer for Old Query

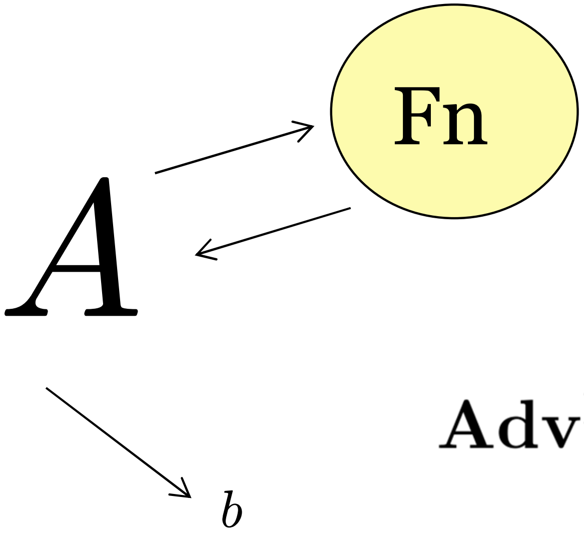
Want: a random function $f : \{0,1\}^n \to \{0,1\}^m$



Putting Things in Code

```
Game Real$_E$
procedure Initialize()
    $K \overset{\$}{\leftarrow} \mathcal{K}$
procedure Fn($M$)
    return $E_K(M)$
```

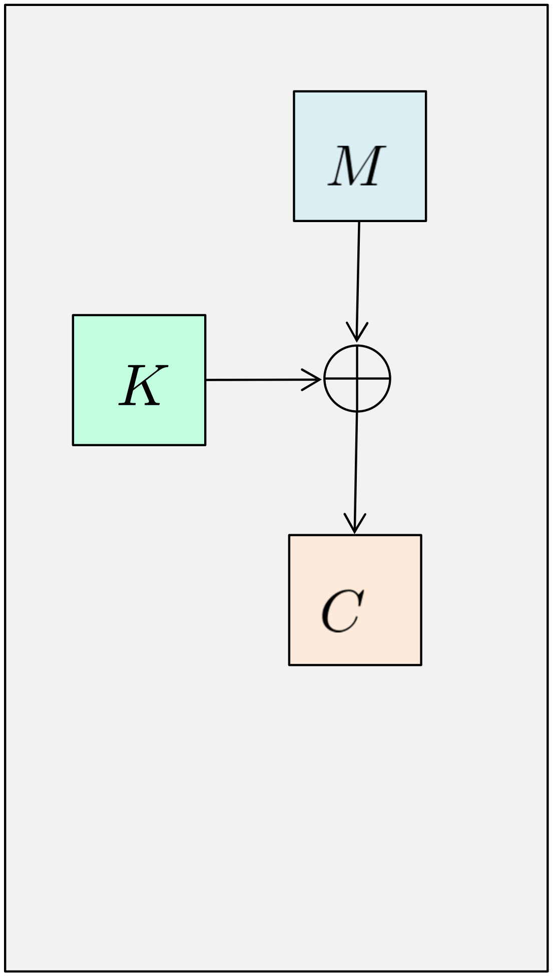
```
Game Rand$_E$
string array $T = \{\}$ // Global variable
procedure Fn($M$)
    If $T[M] = \perp$ then $T[M] \overset{\$}{\leftarrow} \{0,1\}^n$
    return $T[M]$
```



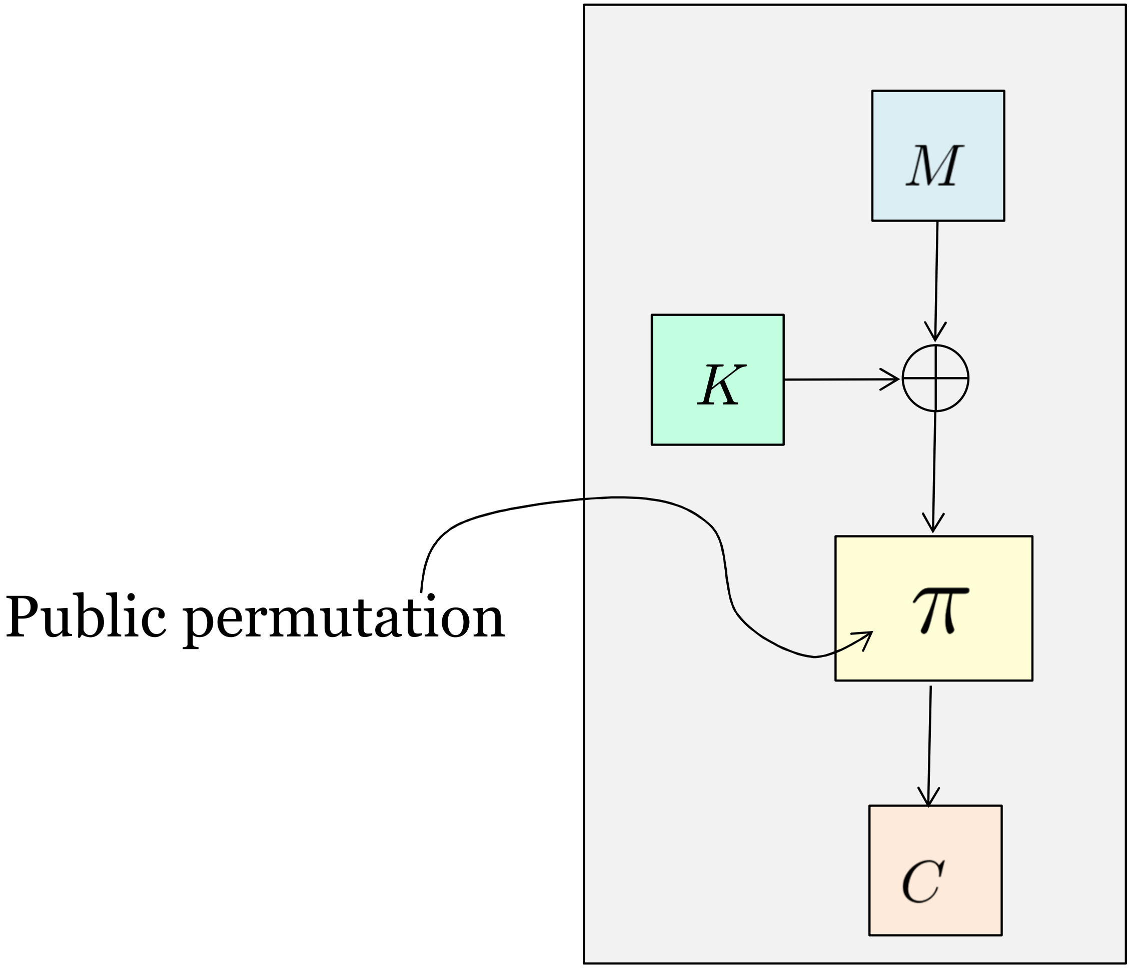
$$\mathbf{Adv}^{\mathrm{prf}}_E(A) = \Pr[\mathrm{Real}_E^A \Rightarrow 1] - \Pr[\mathrm{Rand}_E^A \Rightarrow 1]$$

Exercise: PRF Attacks

$$E_K(M) = M \oplus K$$



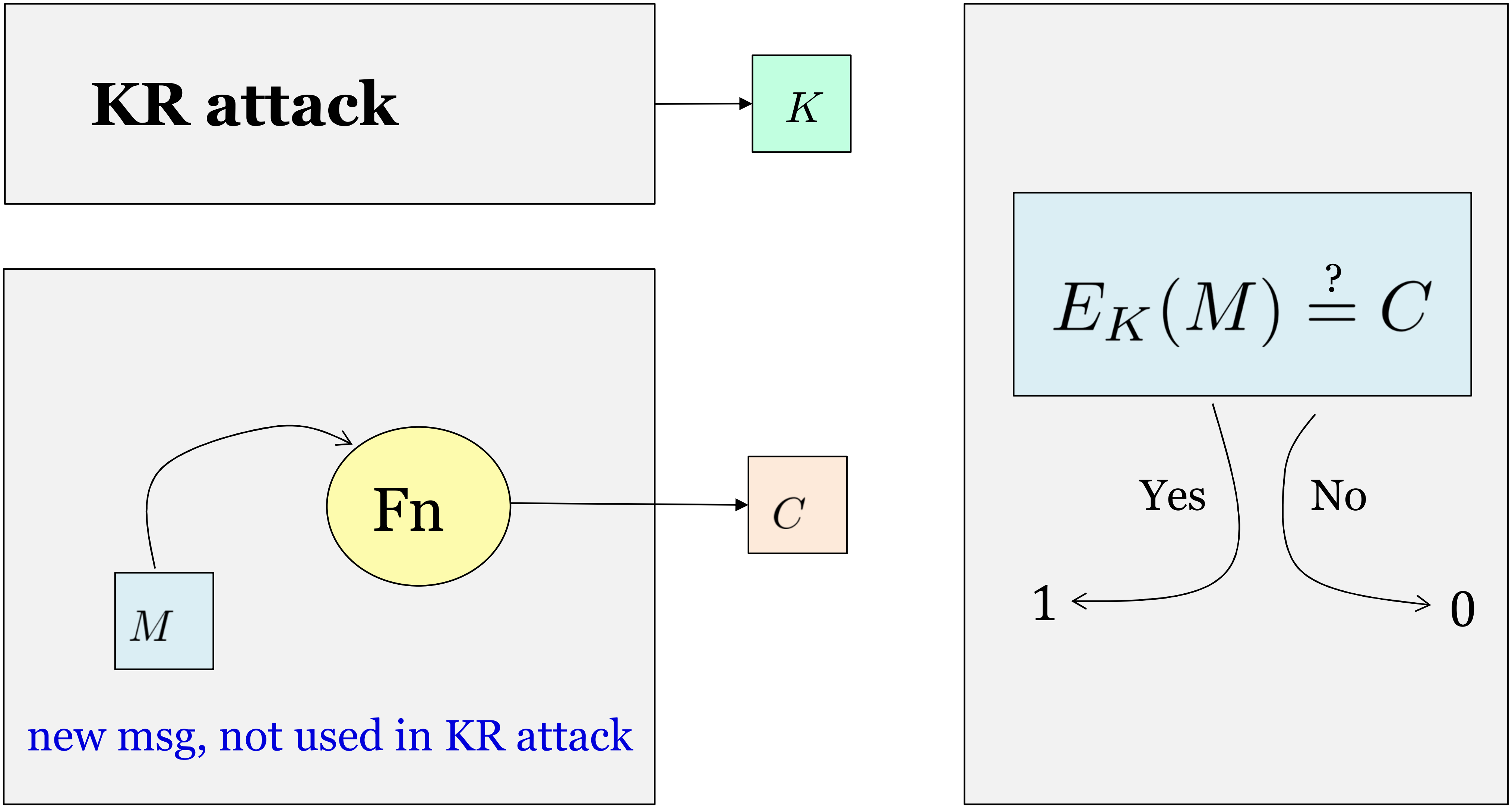
$$E_K(M) = \pi(M \oplus K)$$



Public permutation

π, π^{-1} are public

Easy to Break PRF Security After Key Recovery



KR attack

K

Fn

M

C

new msg, not used in KR attack

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

Yes

No

1

0

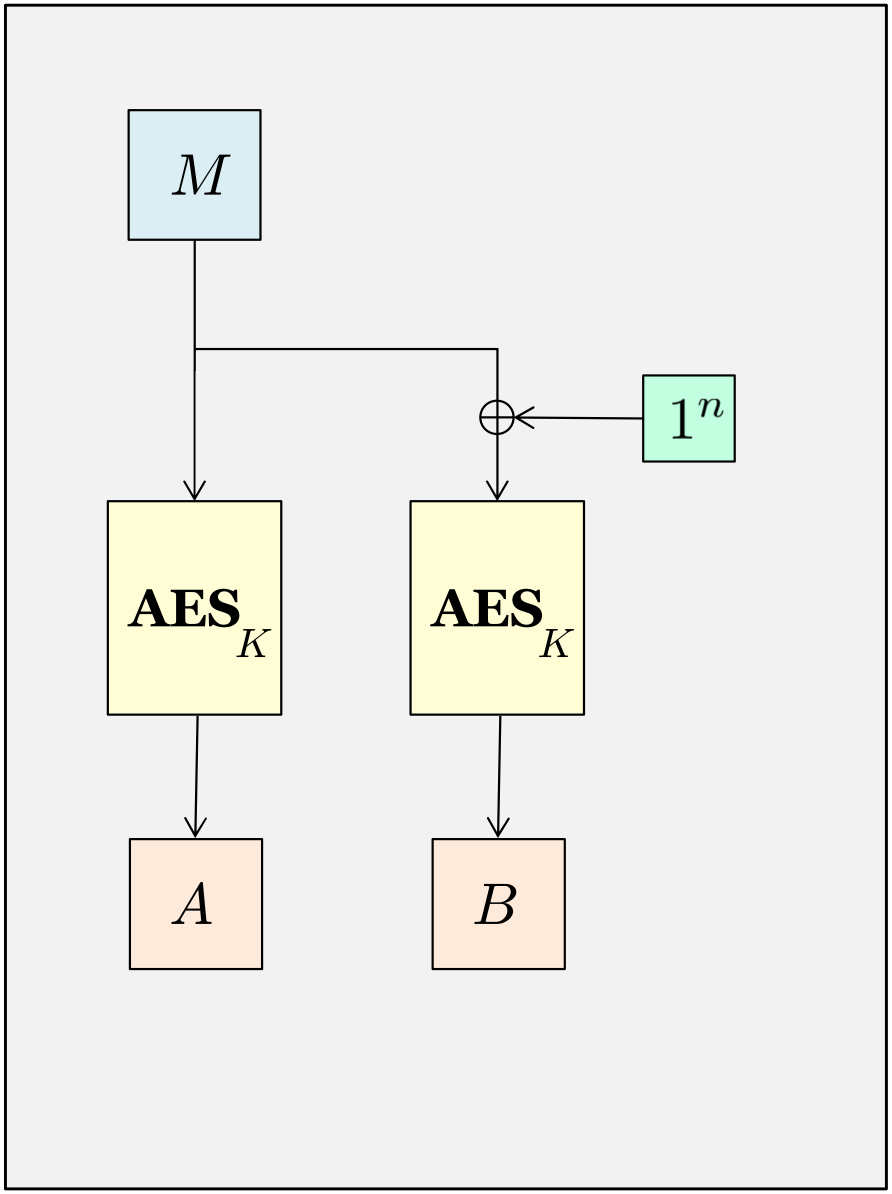
PRF Security

↓

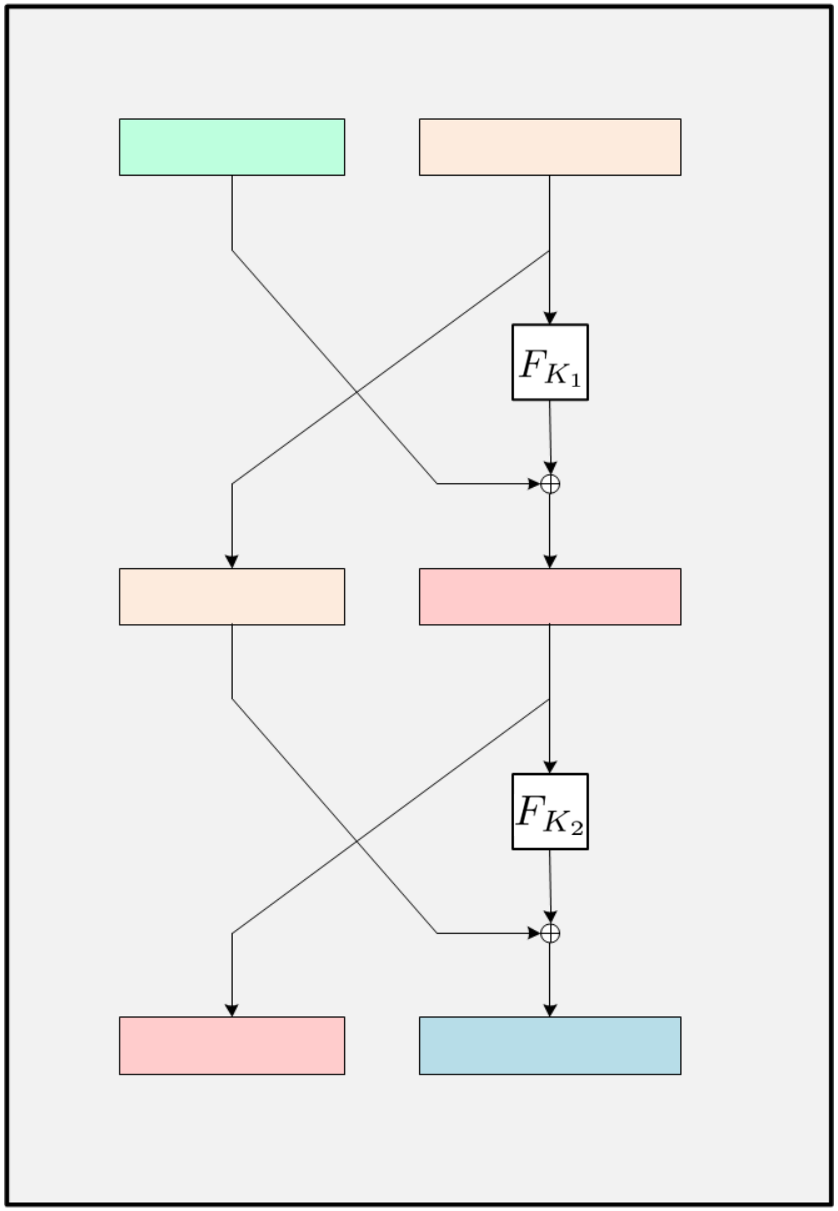
Key Recovery Security

Exercise: PRF Attacks

$$E_K(M) = \mathbf{AES}_K(M) \| \mathbf{AES}_K(\overline{M})$$



Two-round Feistel

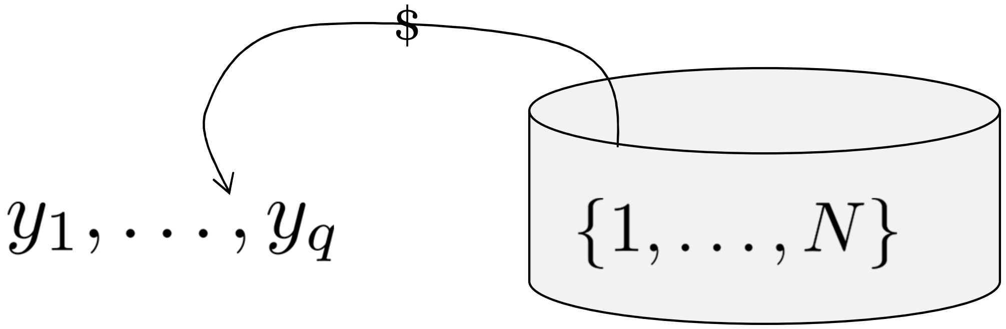


Agenda

1. Defining PRF Security

2. **Birthday Attack**

Birthday Problem

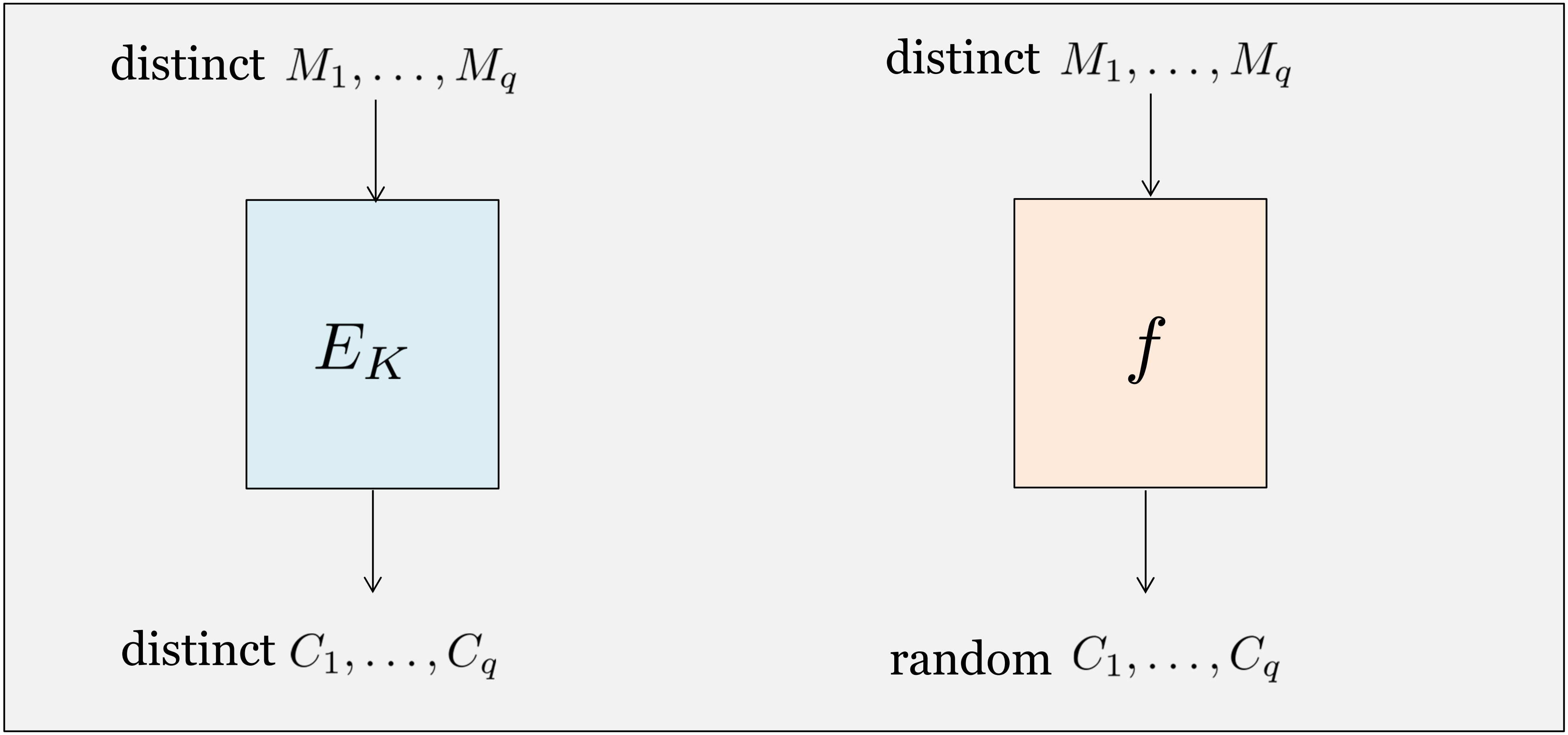


$$C(N, q) = \Pr[y_1, \ldots, y_q \text{ not distinct}]$$

Fact: For $q \leq \sqrt{2N}$,

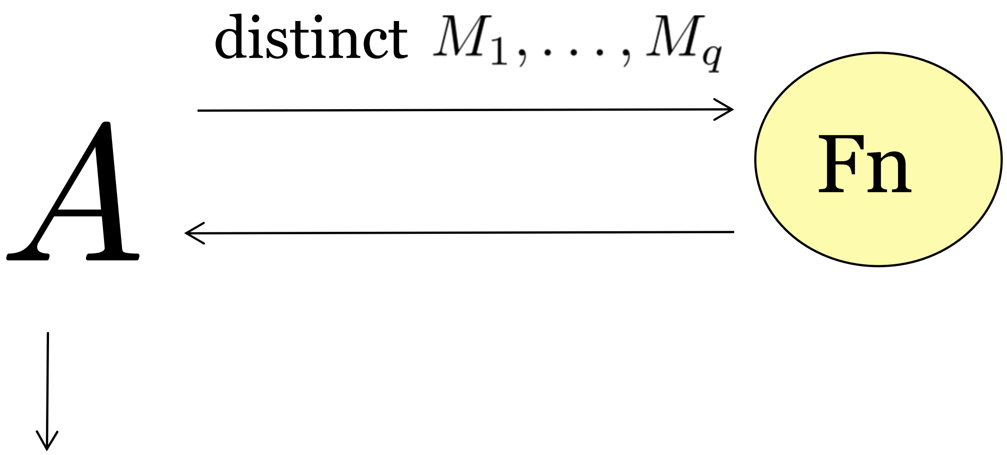
$$\frac{q(q-1)}{4N} \leq C(N, q) \leq \frac{q(q-1)}{2N}$$

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

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



Output 1 if $C_1, \ldots, C_q$ are distinct

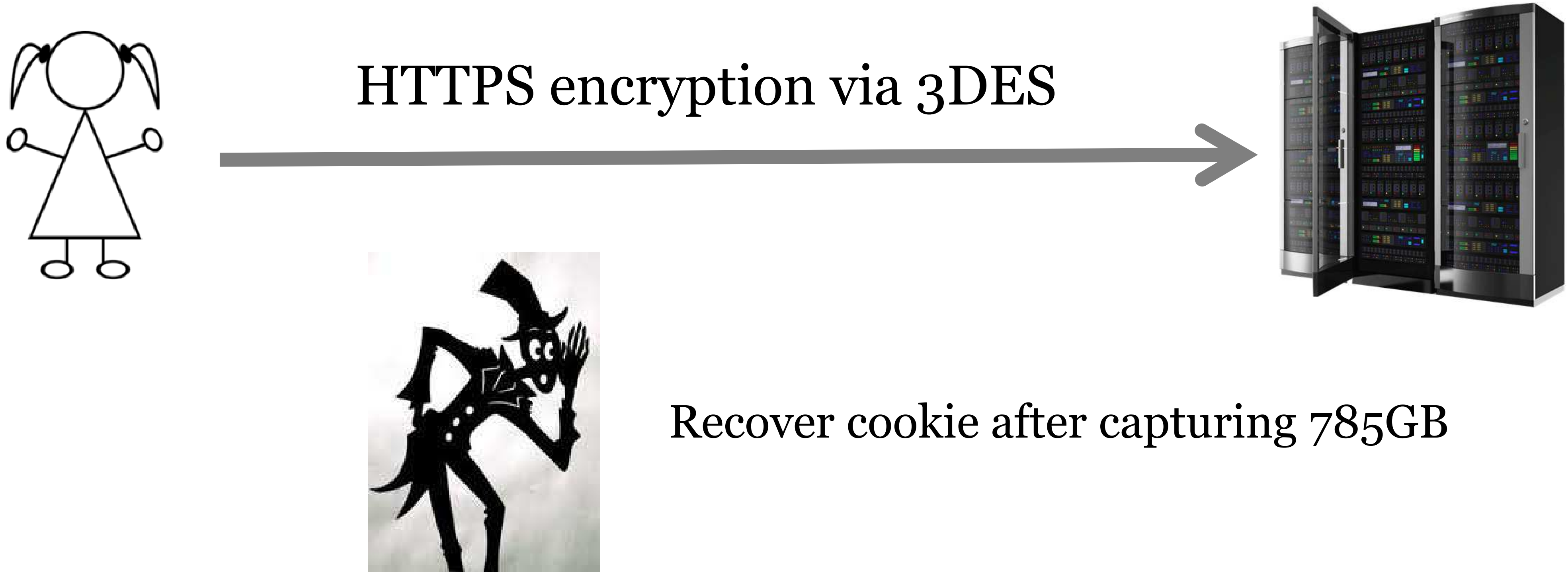
$$\boxed{\mathbf{Adv}_E^{\text{prf}}(A) = C(2^n, q) \approx \frac{q^2}{2^n}}$$

Need $2^{n/2}$ queries to break PRF security

Blockcipher	n	$2^{n/2}$	**Status**
DES, 2DES, 3DES	64	2^{32}	Insecure
AES	128	2^{64}	Secure

Does It Matter In Practice?

Sweet32: Birthday Attacks on 64-bit Blockciphers in TLS and OpenVPN [Bhargavan, Leurent 16]



HTTPS encryption via 3DES

Recover cookie after capturing 785GB