COS433/Math 473: Cryptography

Mark Zhandry

Princeton University

Spring 2017

Previously on COS 433…

Perfect Security for Multiple Messages

Definition: A stateless scheme **(Enc,Dec)** has **perfect secrecy for n messages** if, for any two sequences of messages $(m_0^{(i)})_{i\in[d]}$, $(m_1^{(i)})_{i\in[d]} \in M^d$

$$\left(Enc(K,\ m_0^{(i)}\ )\right)_{i\in[d]} \overset{d}{=} \left(Enc(K,\ m_1^{(i)}\ )\right)_{i\in[d]}$$

Notation: $(\ f(i)\ )_{i\in[d]} = (\ f(1),\ f(2),\ \ldots,\ f(n)\ )$

Theorem: No stateless deterministic encryption scheme can have perfect security for multiple messages

Randomized Encryption

Syntax:

- Key space **K** (usually $\{0,1\}^\lambda$)
- Message space **M** (usually $\{0,1\}^n$)
- Ciphertext space **C** (usually $\{0,1\}^m$)
- **Enc: K×M → C** (potentially probabilistic)
- **Dec: K×C → M** (usually deterministic)

Correctness:

- For all $k \in K$, $m \in M$,

$$\Pr[\ \mathrm{Dec}(k, \mathrm{Enc}(k,m)\,) = m\ ] \quad = \quad 1$$

Theorem: No stateless *randomized* encryption scheme can have perfect security for multiple messages

What do we do now?

Tolerate tiny probability of distinguishing

- If $\Pr[c^{(0)} = c^{(1)}] = 2^{-128}$, in reality never going to happen

How small is ok?

- Usually 2^{-80}, 2^{-128}, or maybe 2^{-256}

Next time: formalize weaker notion of secrecy to allow for small probability of detection

Statistical Distance

Given two distributions $\mathbf{D_1}$, $\mathbf{D_2}$ over a set $\mathbf{X}$, define

$$\Delta(D_1,D_2) = ½\Sigma_x \mid Pr[D_1=x] - Pr[D_2=x] \mid$$

Observations:

$$0 \leq \Delta(D_1,D_2) \leq 1$$

$$\Delta(D_1,D_2) = 0 \iff D_1 \overset{d}{=} D_2$$

$$\Delta(D_1,D_2) \leq \Delta(D_1,D_3) + \Delta(D_3,D_2)$$

(**Δ** is a metric)

Another View of Statistical Distance

Theorem: $\Delta(D_1,D_2) \geq \varepsilon$ iff $\exists A$ s.t.

$$| \Pr[A(D_1) = 1] - \Pr[A(D_2) = 1] | \geq \varepsilon$$

Terminology: for any A,

$$| \Pr[A(D_1) = 1] - \Pr[A(D_2) = 1] |$$

is called the “advantage” of A in distinguishing D_1 and D_2

Another View of Statistical Distance

Theorem: $\Delta(D_1,D_2) \geq \varepsilon$ iff $\exists A$ s.t.

$$\left|\ \Pr[A(D_1) = 1] - \Pr[A(D_2) = 1]\ \right| \geq \varepsilon$$

To lower bound **Δ**, just need to show adversary **A** with that advantage

Examples

D_1 = Uniform distribution over $\{0,1\}^n$

- $\Pr[D_1=x] = 2^{-n}$

D_2 = Uniform subject to even parity

- $\Pr[D_2=x] = 2^{-(n-1)}$ if x has even parity, 0 otherwise

$$\begin{aligned}\Delta(D_1,D_2) &= \tfrac{1}{2}\Sigma_{\text{even } x}\, |2^{-n} - 2^{-(n-1)}| \\ &\quad + \tfrac{1}{2}\Sigma_{\text{odd } x}\, |2^{-n} - 0| \\ &= \tfrac{1}{2}\Sigma_{\text{even } x}\, 2^{-n} + \tfrac{1}{2}\Sigma_{\text{odd } x}\, 2^{-n} \\ &= \tfrac{1}{2}\end{aligned}$$

Examples

$D_1 =$ Uniform over $\{1,\ldots,n\}$
$D_2 =$ Uniform over $\{1,\ldots,n+1\}$

$$\Delta(D_1,D_2) = \tfrac{1}{2}\Sigma_{x=1}^{n} |1/n - 1/(n+1)| + \tfrac{1}{2} |0 - 1/(n+1)|$$

$$= \tfrac{1}{2}\Sigma_{x=1}^{n} 1/n(n+1) + \tfrac{1}{2} 1/(n+1)$$

$$= \tfrac{1}{2} 1/(n+1) + \tfrac{1}{2} 1/(n+1) = 1/(n+1)$$

Statistical Security

Definition: A scheme **(Enc,Dec)** has **ε-statistical secrecy for d messages** if ∀ two sequences of messages $(m_0^{(i)})_{i\in[d]}$, $(m_1^{(i)})_{i\in[d]} \in M^d$

$$\Delta\left[\left(Enc(K, m_0^{(i)})\right)_{i\in[d]}, \left(Enc(K, m_1^{(i)})\right)_{i\in[d]} \right] < \varepsilon$$

We will call such a scheme **(d,ε)**-secure

Statistical Security

We will consider a scheme “secure” for **d** messages if it is **(d,ε)**-secure for very small **ε**

- E.g. 2^{-80}, 2^{-128}, etc

For comparison: chance of

- Being struck by lightning twice: 2^{-23}
- Winning the lottery: 2^{-26}
- World-ending asteroid while on this slide: 2^{-46}

Stateless Encryption with Multiple Messages

Ex:

$\mathbf{M} = \mathbf{C} = \mathbb{Z}_{\mathbf{p}}$ ($\mathbf{p}$ a prime of size $\mathbf{2^{-128}}$)
$\mathbf{K} = \mathbb{Z}_{\mathbf{p}}^{*} \times \mathbb{Z}_{\mathbf{p}}$
$\mathbf{Enc((a,b), m) = (am + b) \bmod p}$
$\mathbf{Dec((a,b), c) = (c-b)/a \bmod p}$

Q: Is this statistically secure for two messages?

Example

Ex:

$M = \mathbb{Z}_p$ (p a prime of size 2^{-128})

$C = \mathbb{Z}_p{}^2$

Random in $\mathbb{Z}_p$

$K = \mathbb{Z}_p{}^2$

$\mathrm{Enc}(\ (a,b),\ m) = (r,\ \ (ar+b) + m\ )$

$\mathrm{Dec}(\ (a,b),\ (r,c)\ ) = c - (ar+b)$

Q: Is this statistically secure for two messages?

Proof of Example

Let $\mathbf{D_b}$ be distribution of $\mathbf{(\ Enc(k,m_b^{(i)})\ )_I}$
Let $\mathbf{D_b}'$ be $\mathbf{D_b}$, but conditioned on $\mathbf{r_0 \neq r_1}$

Fix $\mathbf{r_0 \neq r_1,\ m_0, m_1, c_0, c_1}$

$$\Pr_{(a,b)}[ar_0+b+m_0=c_0,\ ar_1+b+m_1=c_1] = 1/p^2$$

So $\mathbf{D_0' \overset{d}{=} D_1'}$ $\mathbf{(\ \Delta(D_0', D_1') = 0\ )}$

Proof of Example

Lemma: $\Delta(D_1,D_2) \leq \Pr[\text{bad}|D_1] + \Pr[\text{bad}|D_2] + \Delta(D_1', D_2')$

Where:

- "**bad**" is some event
- $\Pr[\text{bad}|D_b]$ is probability "**bad**" when sampling from D_b
- D_b' is D_b, but conditioned on **not** "**bad**"

Proof of Lemma

$$\Delta(D_1,D_2) = \Sigma_x | \Pr[D_1=x] - \Pr[D_2=x] |$$

$$= \Sigma_{x:bad} | \Pr[D_1=x\ ] - \Pr[D_2=x\ ] |$$
$$+ \Sigma_{x:good} | \Pr[D_1=x\ ] - \Pr[D_2=x\ ] |$$

$$\leq \Sigma_{x:bad} | \Pr[D_1=x\ ] | + \Sigma_{x:bad} | \Pr[D_2=x\ ] |$$
$$+ \Sigma_{x:good} | \Pr[D_1=x] - \Pr[D_2=x] |$$

$$\leq \Pr[bad|D_1] + \Pr[bad|D_2] + \Delta(D_{1,good},D_{2,good})$$

Proof of Example

Let $\mathbf{D_b}$ be distribution of $\mathbf{(\ Enc(k,m_b^{(i)})\ )_I}$
Let **bad** be when $\mathbf{r_0=r_1}$
Let $\mathbf{D_b'}$ be $\mathbf{D_b}$, but conditioned on **not bad**

$\mathbf{Pr[bad|D_b] = 1/p}$
$\mathbf{\Delta(D_0', D_1') = 0}$

Therefore, $\mathbf{\Delta(D_0, D_1) \leq 2/p}$

Summary so Far

Stateless encryption for multiple messages ✓

But, key length grows with number of messages ✘

And, key length grows with length of message ✘

Limits of Statistical Security

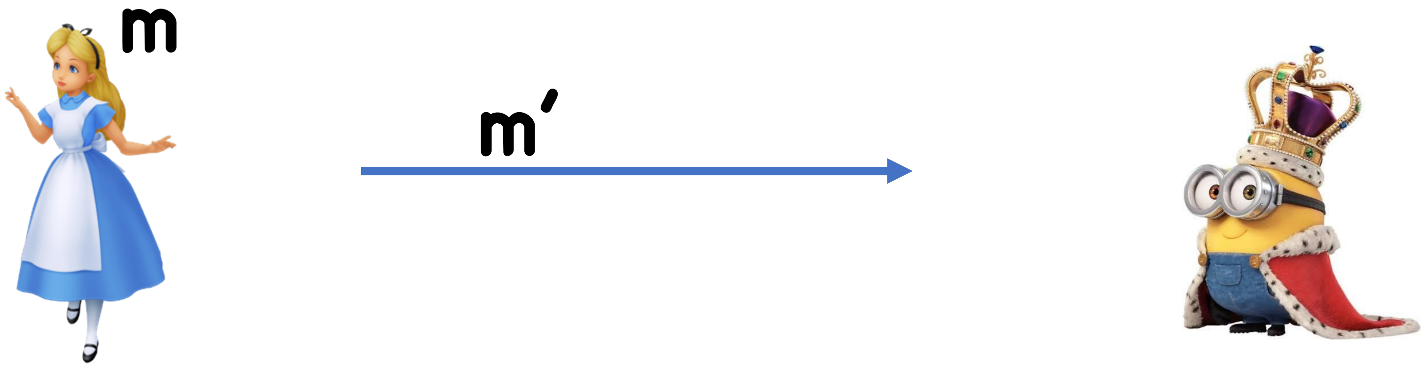
Theorem: Suppose **(Enc,Dec)** has plaintext space $\mathbf{M} = \{0,1\}^n$ and key space $\mathbf{K} = \{0,1\}^t$. Moreover, assume it is **(d,⅓)**-secure. Then:

$$t \geq d\, n$$

In other words, the key must be at least as long as the total length of all messages encrypted

Proof Idea

Use an encryption protocol to build a compression protocol

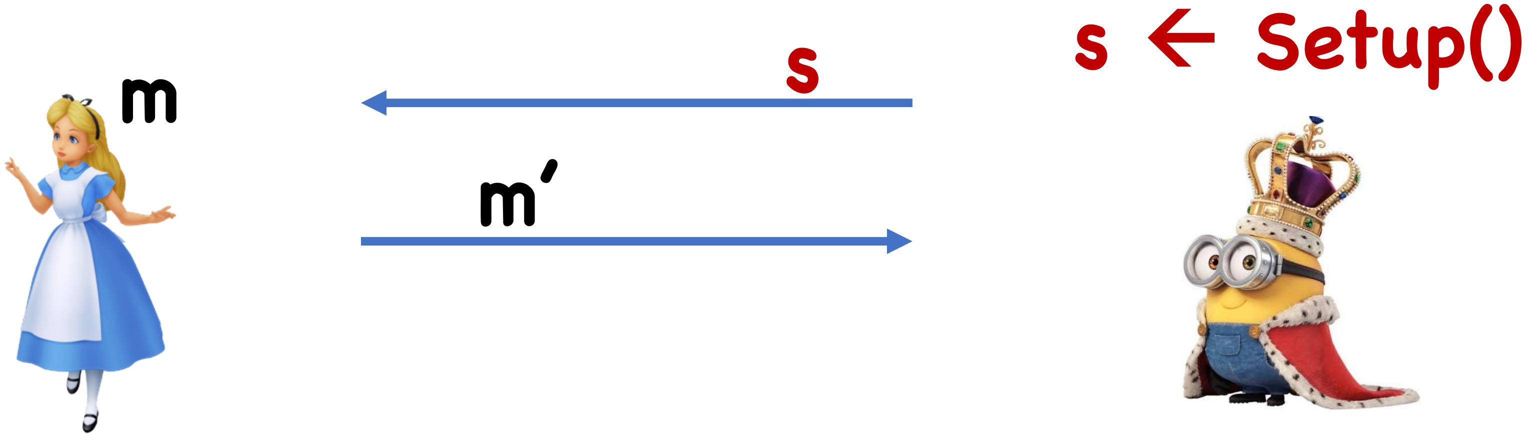


m′ ← Comp(m)

m ← Decomp(m′)

Goal: |m′| < |m|

For Now: Easier Goal



m

$s \leftarrow \mathrm{Setup}()$

s

m′

m′ ← Comp(s,m)

m ← Decomp(s,m′)

Goal: $|m'| < |m|$

The Protocol

Let $\mathbf{m_0}$ be some message in $\mathbf{M}$

Setup():

- Choose random $\mathbf{k_0 \leftarrow K}$
- **Let** $\mathbf{c_1 \leftarrow Enc(k_0,m_0), \ldots, c_d \leftarrow Enc(k_0,m_0)}$
- **Output** $\mathbf{(c_1,\ldots,c_d)}$

In $\mathbf{M^d}$

Comp($(c_1,\ldots,c_d)$, $(m_1,\ldots,m_d)$):

- Find $\mathbf{k,r_1,\ldots,r_d}$ such that $\mathbf{c_i=Enc(k,m_i;\ r_i)}$ $\forall \mathbf{i}$
- If no such values exist, abort
- Output $\mathbf{k}$

The Protocol

Let $\mathbf{m_0}$ be some message in $\mathbf{M}$

In $\mathbf{M^d}$

$\mathbf{Comp(\ (c_1,\ldots,c_d),\ (m_1,\ldots,m_d)\ ):}$

- Find $\mathbf{k,r_1,\ldots,r_d}$ such that $\mathbf{c_i=Enc(k,m_i;\ r_i)}\ \forall\mathbf{i}$
- If no such values exist, abort
- Output $\mathbf{k}$

$\mathbf{Decomp((c_1,\ldots,c_d),\ k\ ):}$

- Compute $\mathbf{m_i = Dec(k,c_i)}$
- Output $\mathbf{(m_1,\ldots,m_d)}$

Analysis of Protocol

If **Comp** succeeds, **Decomp** must succeed by correctness

- Since $\mathbf{c_i=Enc(k,m_i;\ r_i)}$, $\mathbf{Dec(k,c_i)}$ must give $\mathbf{m_i}$

Therefore, must figure out when **Comp** succeeds

Claim: For any sequence of messages $\mathbf{m_1,\ldots,m_d}$, **Comp** succeeds with probability at least $\mathbf{1-\varepsilon}$

(Probability over the randomness used by **Setup()**)

Claim: For any sequence of messages $\mathbf{m_1,\ldots,m_d}$, **Comp** succeeds with probability at least $\mathbf{1-\varepsilon}$

Proof:

- Suppose **Comp** succeeds with probability $\mathbf{1-p}$ for messages $\mathbf{m_1,\ldots,m_d}$
- Let $\mathbf{A(c_1,\ldots,c_d)}$ be the algorithm that runs $\mathbf{Comp((c_1,\ldots,c_d),\ (m_1,\ldots,m_d))}$ and outputs **1** if **Comp** succeeds

- If $\mathbf{c_i = Enc(k_0,m_i)}$, then $\mathbf{Pr[A(c_1,\ldots,c_d)=1] = 1}$
- If $\mathbf{c_i = Enc(k_0,m_0)}$, then $\mathbf{Pr[A(c_1,\ldots,c_d)=1] = 1-p}$

- By $\mathbf{(d,\varepsilon)}$statistical security of **Enc**, **p** must be $\mathbf{\leq\varepsilon}$

Claim: For any sequence of messages $\mathbf{m_1,\ldots,m_d}$, **Comp** succeeds with probability at least $\mathbf{1-\varepsilon}$

Claim: For **a random** sequence of messages $\mathbf{m_1,\ldots,m_d}$, **Comp** succeeds with prob at least $\mathbf{1-\varepsilon}$

(Probability over the randomness used by **Setup()** and the random choices of $\mathbf{m_1,\ldots,m_d}$)

Next step: Removing Setup

We know:

$$\Pr\left[\text{Comp succeeds: } \begin{matrix}(c_1,\ldots,c_d)\leftarrow\text{Setup}(), \\ m_i\leftarrow M\end{matrix}\right] \geq 1-\varepsilon$$

Therefore, there must exist *some* $(c_1{}^*,\ldots,c_d{}^*)$ such that

$$\Pr[\text{Comp succeeds: } m_i\leftarrow M] \geq 1-\varepsilon$$

Define: $M' = \{(m_1,\ldots,m_d)\text{: Comp}$ succeeds$\}$

- Note that $|M'| \geq (1-\varepsilon)\ |M|^d$

The Protocol

$m \in M'$

k →

Find $k, r_1, \ldots, r_d$ such that
$c_i^* = Enc(k, m_{i;}\ r_i)\ \forall i$

For each i,
Let $m_i \leftarrow Dec(k, c_i^*)$
Output $(m_1, \ldots, m_d)$

By previous analysis,

- Alice always successfully compresses
- Bob always successfully decompresses

Final Touches

Can compress messages in $\mathbf{M'}$ into keys in $\mathbf{K}$

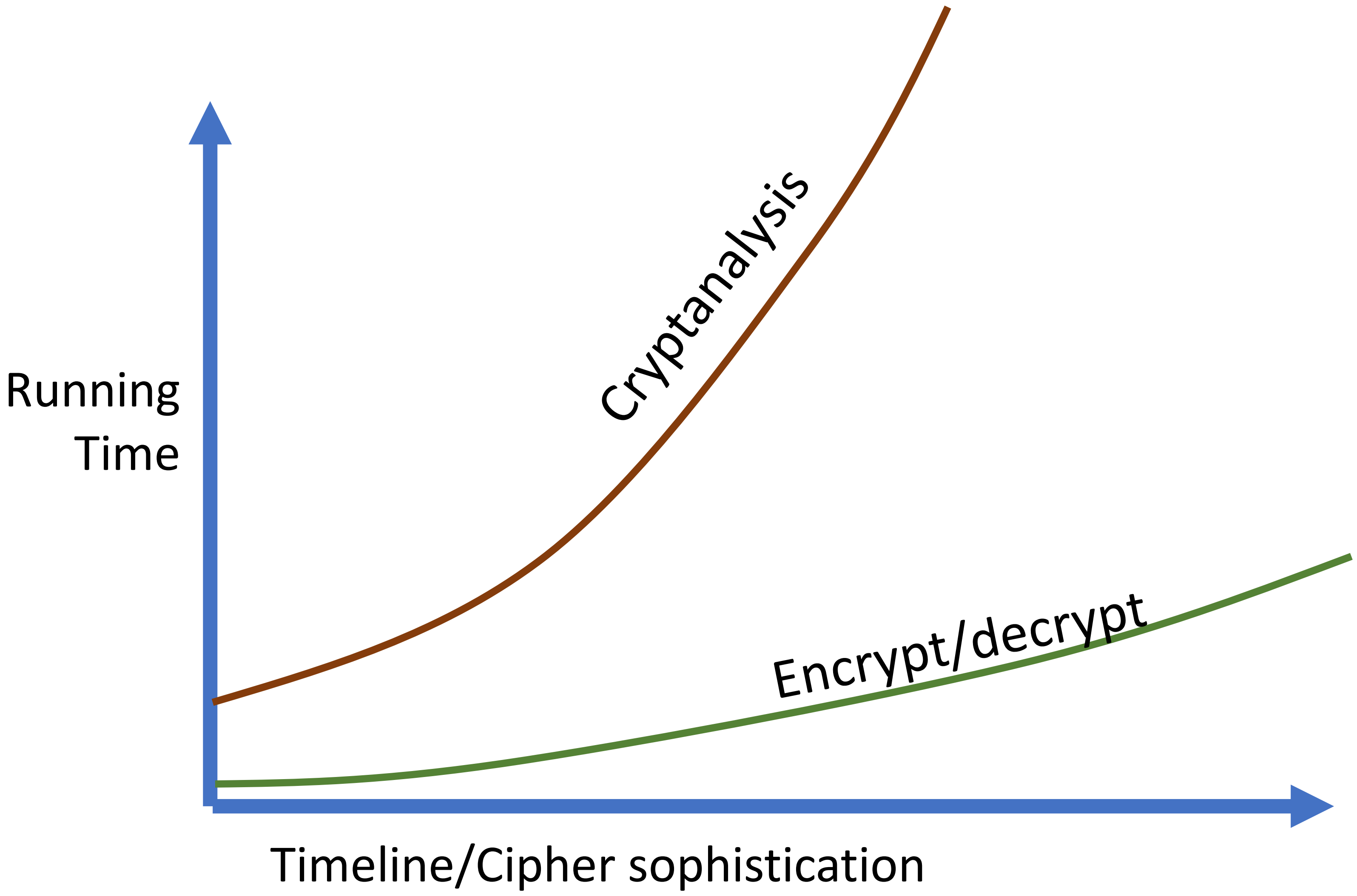
Therefore, it must be that $|M'| \leq |K|$

$$
\begin{aligned}
\textbf{Meaning } t &= \log |K| \\
&\geq \log |M'| \\
&\geq \log [\, (1-\varepsilon)\, |M|^d \,] \\
&= d \log |M| + \log [1-\varepsilon] \\
&\geq dn - 2\varepsilon \\
&\geq dn \text{ (as long as } \varepsilon<½\text{)}
\end{aligned}
$$

Takeaway

If you don’t want to physically exchange keys frequently, you cannot obtain statistical security

So, now what?


Running Time
Cryptanalysis
Encrypt/decrypt
Timeline/Cipher sophistication

Computational Security

We are ok if adversary takes a really long time

Usually measure in machine operations

- Though depends on architecture, so rough approx
- 2^{80}, 2^{128}, or maybe 2^{256} are probably ok

For comparison:

- Lifetime of universe in nanoseconds: 2^{58}
- Number of atoms in known universe: 2^{265}

Brute Force Attacks

Simply try every key until find right one

Relevant as long as key length is smaller than total length of messages encrypted

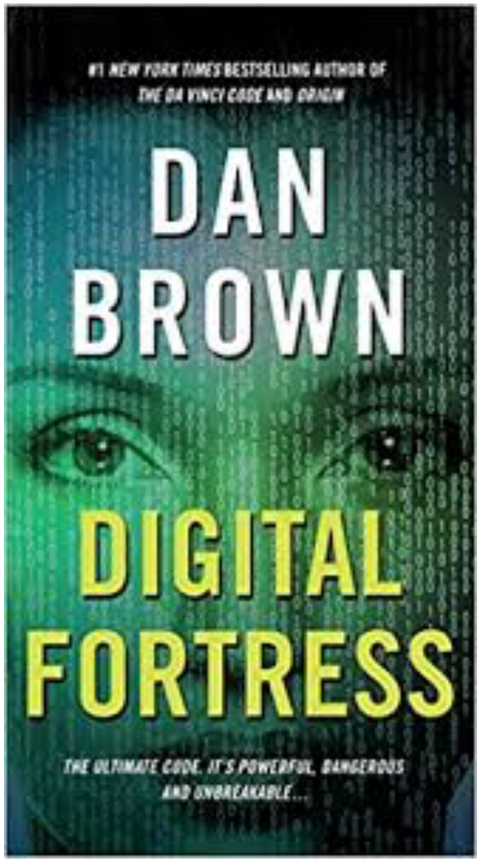
If keys have length $\boldsymbol{\lambda}$, $\mathbf{2}^{\lambda}$ is upper bound on attack

Crypto and P vs NP

What if P = NP?

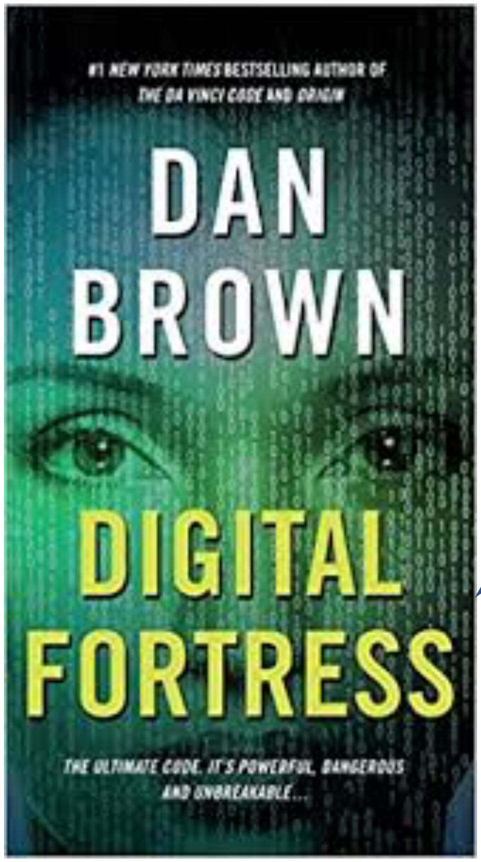
From this point forward, almost all crypto we will see depends on computational assumptions

Holiwudd Criptoe!


#1 NEW YORK TIMES BESTSELLING AUTHOR OF
THE DA VINCI CODE AND ORIGIN
DAN BROWN
DIGITAL FORTRESS
THE ULTIMATE CODE. IT'S POWERFUL, DANGEROUS
AND UNBREAKABLE...

[TRANSLTR]'s three million processors would all work in parallel ... trying every new permutation as they went

Holiwudd Criptoe!


#1 NEW YORK TIMES BESTSELLING AUTHOR OF
THE DA VINCI CODE AND ORIGIN
DAN BROWN
DIGITAL FORTRESS
THE ULTIMATE CODE. IT'S POWERFUL, DANGEROUS AND UNBREAKABLE...

“What’s the longest you’ve ever seen TRANSLTR take to break a code?”

“About an hour, but it had a ridiculously long key—ten thousand bits”

Defining Security

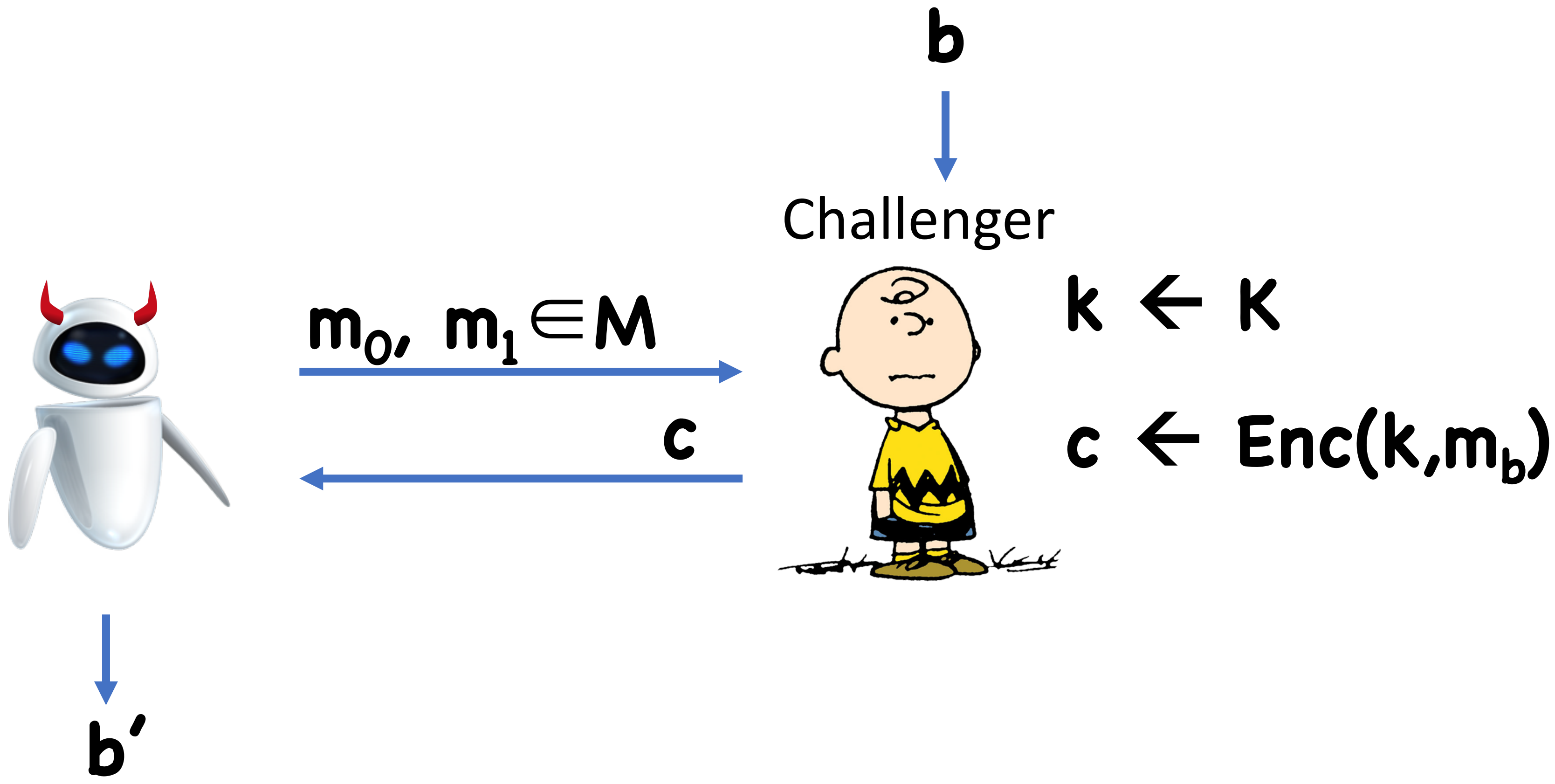
Consider an attacker as a probabilistic efficient algorithm

Attacker gets to choose the messages

All attacker has to do is distinguish them

Security Experiment/Game

(One-time setting)



b

Challenger

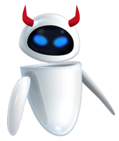
$m_0, m_1 \in M$

c

$k \leftarrow K$

$c \leftarrow \mathrm{Enc}(k,m_b)$

b′

$\mathrm{IND\text{-}Exp}_b($$)$

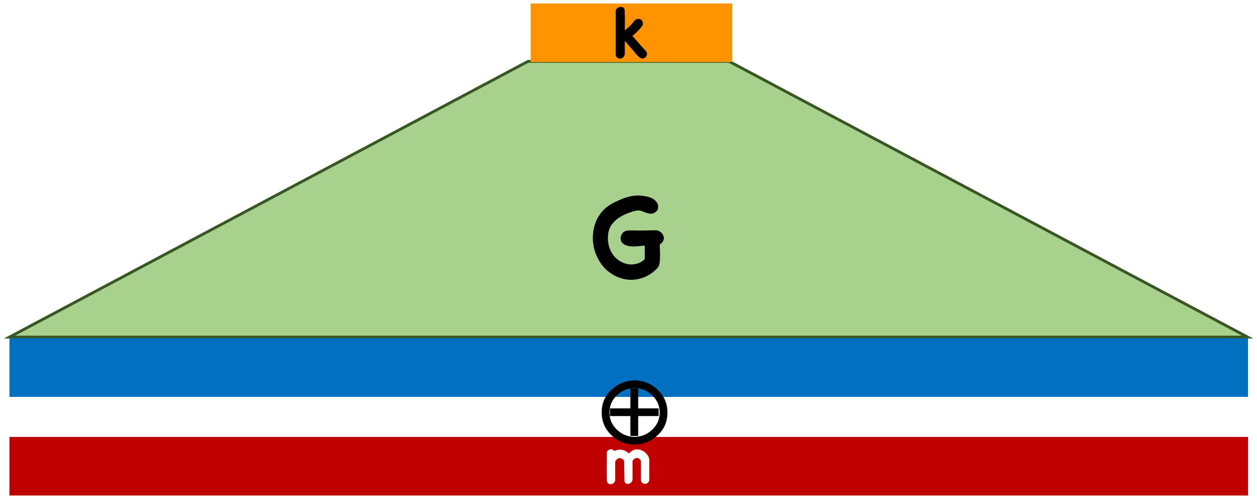
Security Definition (One-time setting)

Definition: (Enc, Dec) has **(t,ε)–ciphertext indistinguishability** if, for all 🤖 running in time at most **t**

$$\Big| \Pr[1 \leftarrow \text{IND-Exp}_0(\text{🤖})\,] \\ \quad - \Pr[1 \leftarrow \text{IND-Exp}_1(\text{🤖})\,] \Big| \leq \varepsilon$$

Construction with |k| << |m|

Idea: use OTP, but have key generated by some expanding function **G**



What Do We Want Out of **G**?

Definition: $G:\{0,1\}^\lambda \rightarrow \{0,1\}^n$ is a **(t,ε)-secure pseudorandom generator** (PRG) if:

- $n > \lambda$
- **G** is deterministic
- For all running in time at most **t**,

$\Big|\, \Pr[$ $(G(s))=1 : s \leftarrow \{0,1\}^\lambda]$

$-\ \Pr[$ $(x)=1 : x \leftarrow \{0,1\}^n] \,\Big| \leq \varepsilon$

Secure PRG → Ciphertext Indistinguishability

$K = \{0,1\}^{\lambda}$
$M = \{0,1\}^{n}$
$C = \{0,1\}^{n}$

$\mathrm{Enc}(k,m) = \mathrm{PRG}(k) \oplus m$
$\mathrm{Dec}(k,c) = \mathrm{PRG}(k) \oplus c$

Security?

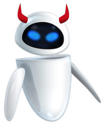
Intuitively, security is obvious:

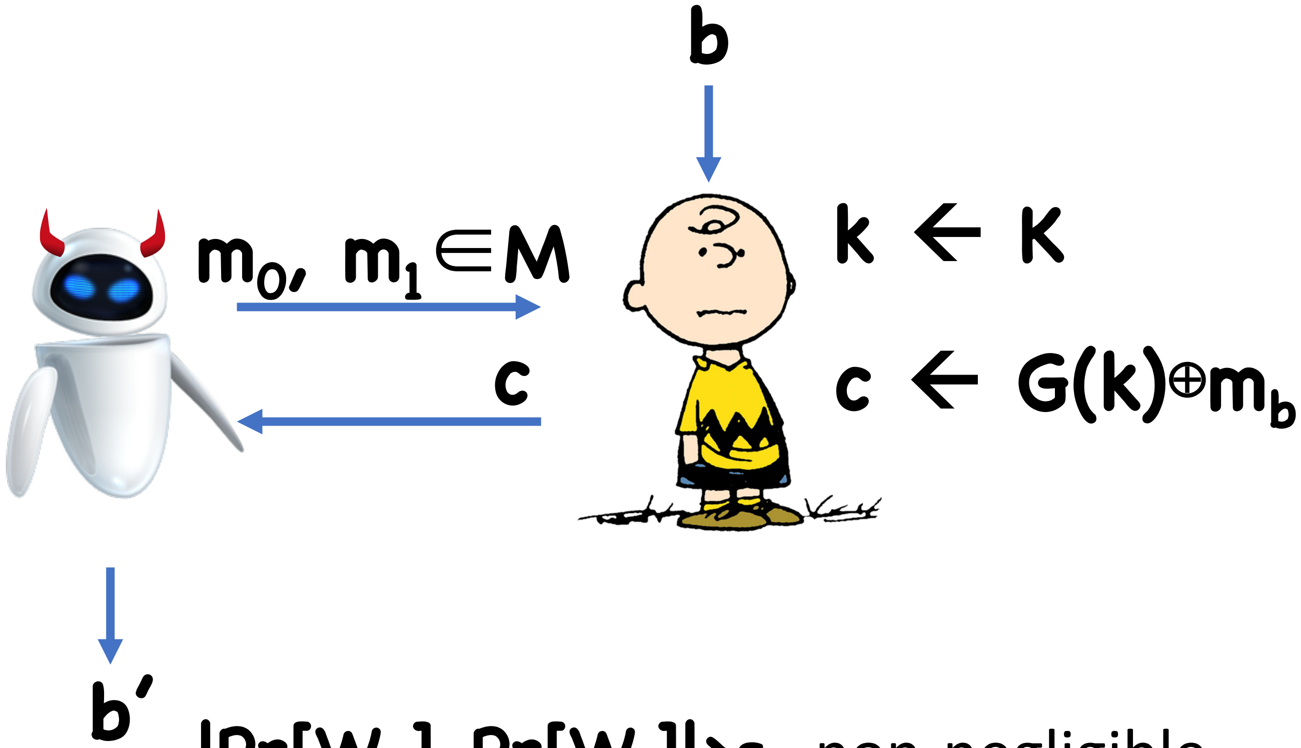
- **PRG(k)** ”looks” random, so should completely hide **m**
- However, formalizing this argument is non-trivial.

Solution: reductions

- Assume toward contradiction an adversary for the encryption scheme, derive an adversary for the PRG

Security

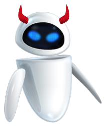
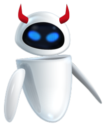
Assume towards contradiction that there is a  such that

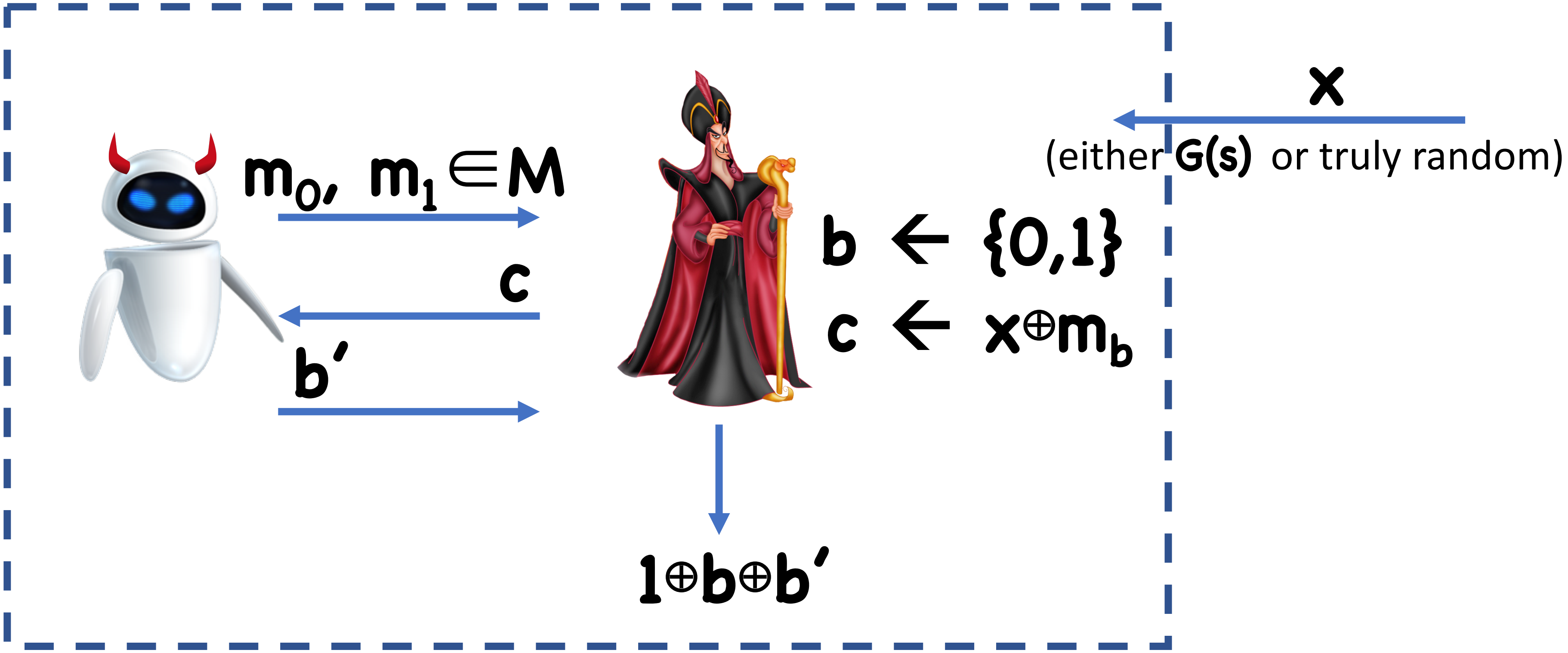


$|\Pr[W_0] - \Pr[W_1]| \geq \varepsilon$, non-negligible

W_b: $b' = 1$ in IND-Exp_b

Security

Use  to build . will run  as a subroutine, and pretend to be



$m_0, m_1 \in M$

c

b'

$b \leftarrow \{0,1\}$

$c \leftarrow x \oplus m_b$

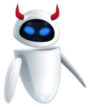
x

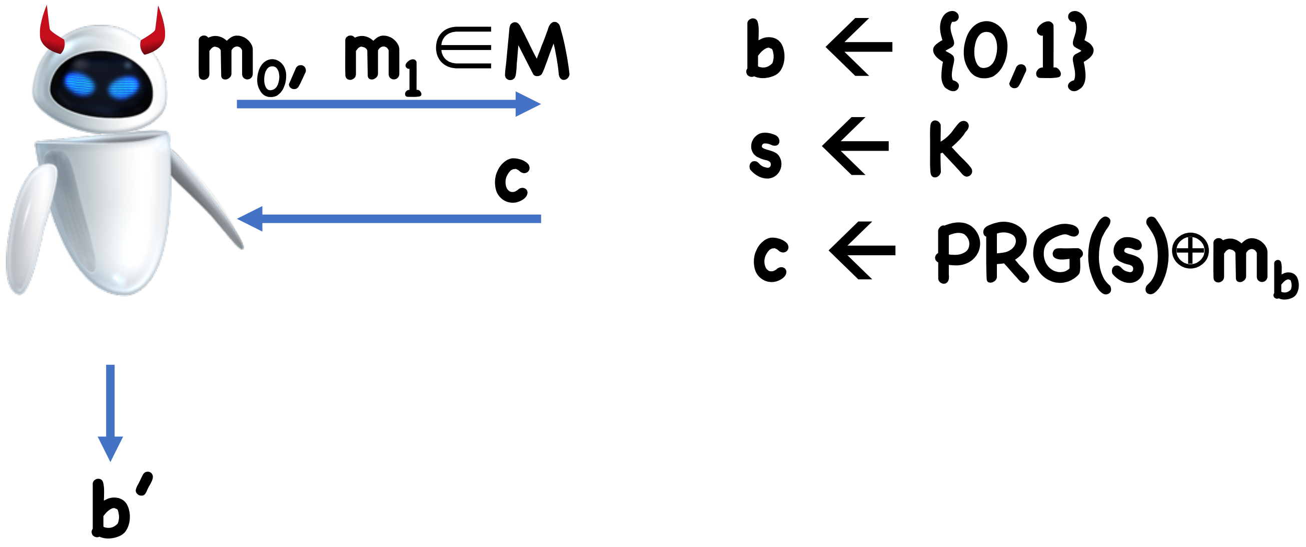
(either $G(s)$ or truly random)

$1 \oplus b \oplus b'$

Security

Case 1: **x = PRG(s)** for a random seed **s**

-  "sees" **IND-Exp**$_b$ for a random bit **b**



$m_0, m_1 \in M$

c

b'

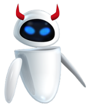
$b \leftarrow \{0,1\}$

$s \leftarrow K$

$c \leftarrow PRG(s) \oplus m_b$

Security

Case 1: $\mathbf{x} = \mathbf{PRG(s)}$ for a random seed **s**

-  “sees” $\mathbf{IND\text{-}Exp_b}$ for a random bit **b**
- $\Pr[1 \oplus b \oplus b' = 1] = \Pr[b = b']$

$$= \tfrac{1}{2} \Pr[b'=1 \mid b=1\ ]$$

$$+ \tfrac{1}{2}\ (1 - \Pr[b'=1 \mid b=0])$$

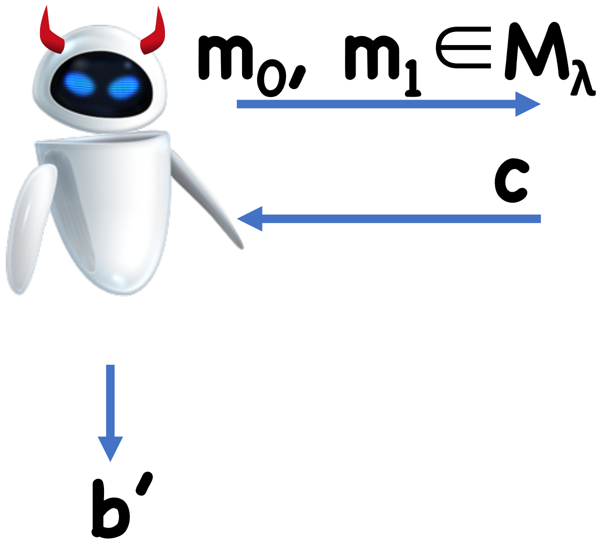
$$= \tfrac{1}{2}(1 + \Pr[W_0] - \Pr[W_1])$$

$$= \tfrac{1}{2}(\ 1 \pm \varepsilon\ )$$

Security

Case 2: **x** is truly random

- “sees” OTP encryption



$m_0, m_1 \in M_\lambda$

c

b'

$b \leftarrow \{0,1\}$

$x \leftarrow \{0,1\}^n$

$c \leftarrow x \oplus m_b$

Security

Case 2: x is truly random

- 😈 “sees” OTP encryption
- Therefore $\Pr[b'=1 \mid b=0] = \Pr[b'=1 \mid b=1]$
- $\Pr[1 \oplus b \oplus b'=1] = \Pr[b=b']$

$$= \tfrac{1}{2} \Pr[b'=1 \mid b=1\ ]$$

$$+ \tfrac{1}{2} (1 - \Pr[b'=1 \mid b=0])$$

$$= \tfrac{1}{2}$$

Security

Putting it together:

- $\Pr[$ $(G(s))=1 : s \leftarrow \{0,1\}^{\lambda}] = \tfrac{1}{2}(\, 1 \pm \varepsilon(\lambda)\,)$
- $\Pr[$ $(x)=1 : x \leftarrow \{0,1\}^{n}] = \tfrac{1}{2}$
- Absolute Difference: **½ε,** $\Rightarrow$ Contradiction!

Security

Thm: If **G** is a **(t+t',ε/2)**-secure PRG, then **(Enc,Dec)** is has **(t,ε)**-ciphertext indistinguishability, where **t'** is the time to:

- Flip a random bit **b**
- XOR two **n**-bit strings

Security

Thm: If **G** is a **$(t+\text{poly},\varepsilon/2)$**-secure PRG, then **(Enc,Dec)** is has **(t,ε)**-ciphertext indistinguishability

An Alternate Proof: Hybrids

Idea: define sequence of “hybrid” experiments “between” **IND-Exp**$_0$ and **IND-Exp**$_1$

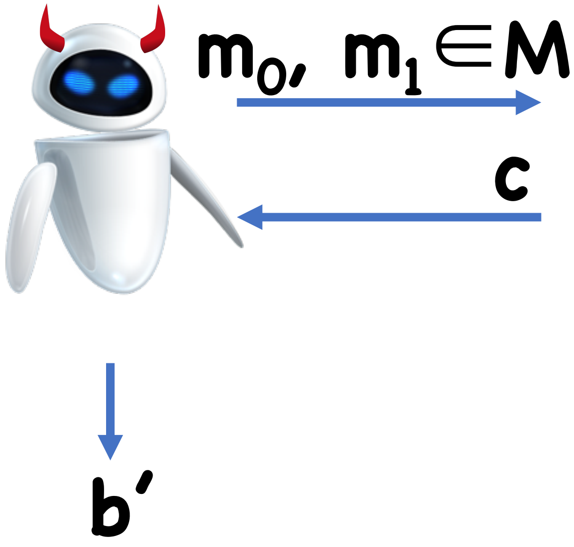
In each hybrid, make small change from previous hybrid

Hopefully, each small change is undetectable

Using triangle inequality, overall change from **IND-Exp**$_0$ and **IND-Exp**$_1$ is undetectable

An Alternate Proof: Hybrids

Hybrid 0: IND-Exp$_0$



$m_0, m_1 \in M$

c

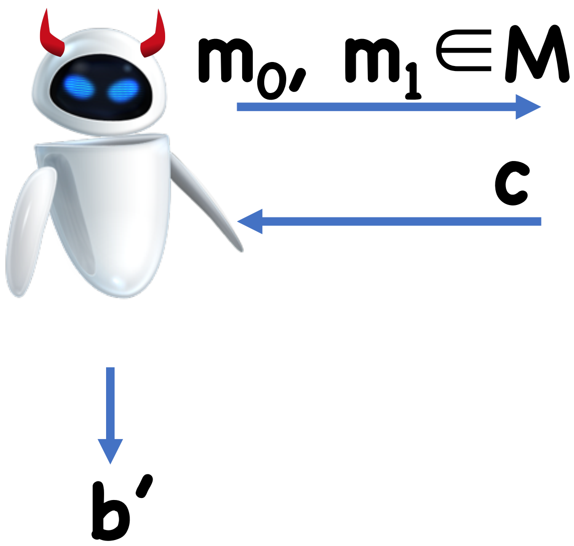
b'

$k \leftarrow K$

$c \leftarrow G(k) \oplus m_0$

An Alternate Proof: Hybrids

Hybrid 1:



$m_0, m_1 \in M$

c

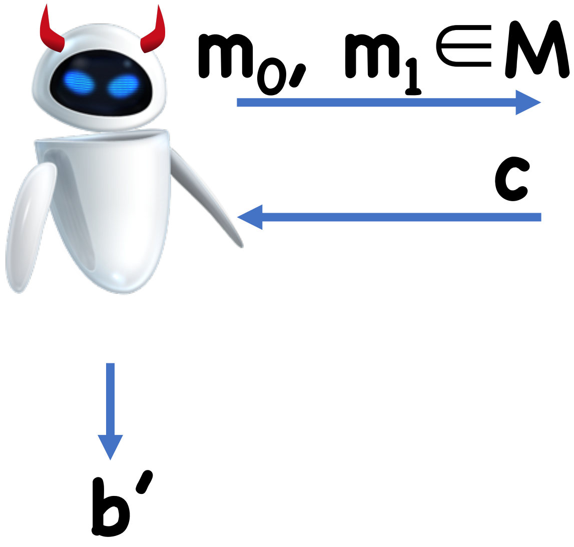
b'

$x \leftarrow \{0,1\}^n$

$c \leftarrow x \oplus m_0$

An Alternate Proof: Hybrids

Hybrid 2:



$m_0, m_1 \in M$

c

b'

$x \leftarrow \{0,1\}^n$

$c \leftarrow x \oplus m_1$

An Alternate Proof: Hybrids

Hybrid 3: IND-Exp$_1$

$m_0, m_1 \in M$

c

b'

$k \leftarrow K$

$c \leftarrow G(k) \oplus m_1$

An Alternate Proof: Hybrids

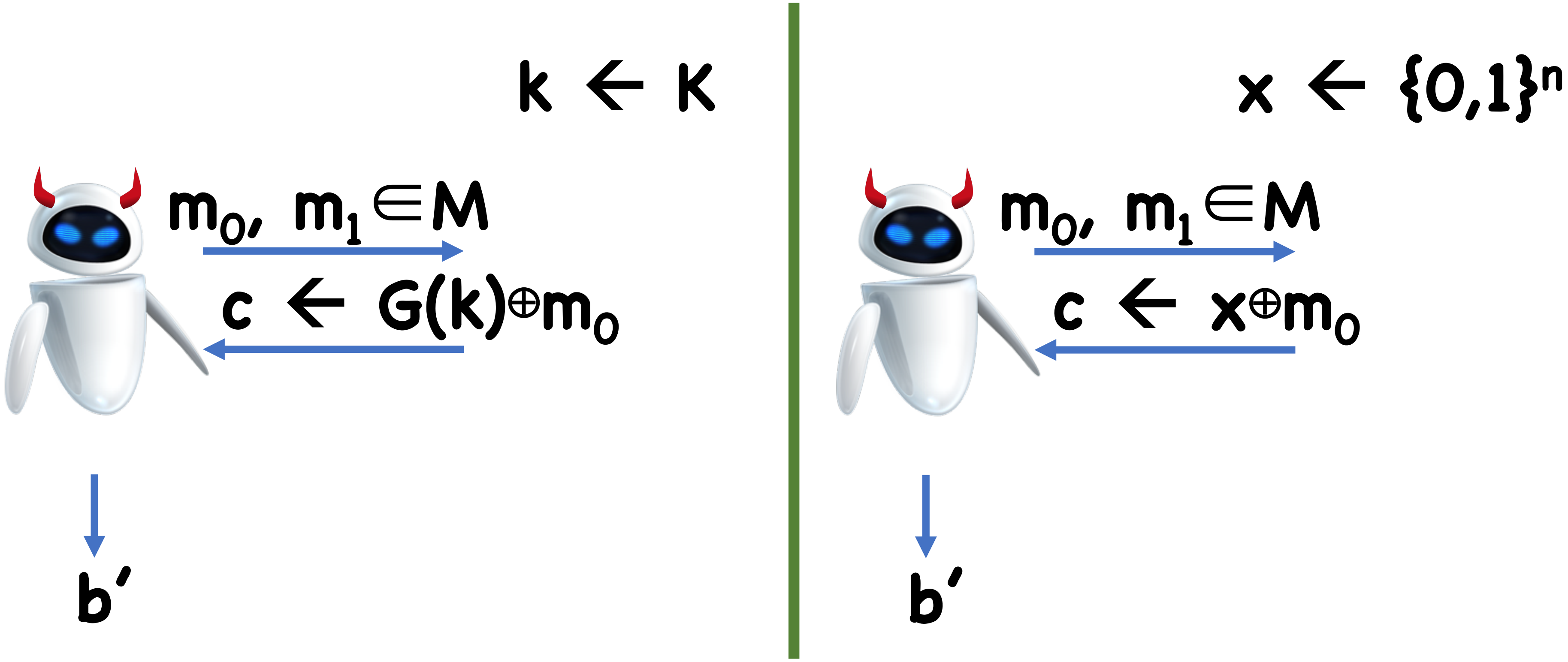
$$
\begin{aligned}
&|\ \Pr[b'=1 : \text{IND-Exp}_0] - \Pr[b'=1 : \text{IND-Exp}_1]\ | \\
&\qquad = |\ \Pr[b'=1 : \text{Hyb } 0] - \Pr[b'=1 : \text{Hyb } 3]\ | \\
&\qquad \leq |\ \Pr[b'=1 : \text{Hyb } 0] - \Pr[b'=1 : \text{Hyb } 1]\ | \\
&\qquad\quad + |\ \Pr[b'=1 : \text{Hyb } 1] - \Pr[b'=1 : \text{Hyb } 2]\ | \\
&\qquad\quad + |\ \Pr[b'=1 : \text{Hyb } 2] - \Pr[b'=1 : \text{Hyb } 3]\ |
\end{aligned}
$$

If $|\Pr[b'=1:\text{IND-Exp}_0]-\Pr[b'=1:\text{IND-Exp}_1]| \geq \varepsilon$,
Then for some $i=0,1,2$,

$$|\Pr[b'=1:\text{Hyb } i]-\Pr[b'=1:\text{Hyb } i+1]| \geq \varepsilon/3$$

An Alternate Proof: Hybrids

Suppose distinguishes **Hybrid 0** from **Hybrid 1** with advantage **$\varepsilon/3$**



$k \leftarrow K$

$m_0, m_1 \in M$

$c \leftarrow G(k) \oplus m_0$

b'

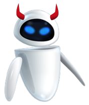
$x \leftarrow \{0,1\}^n$

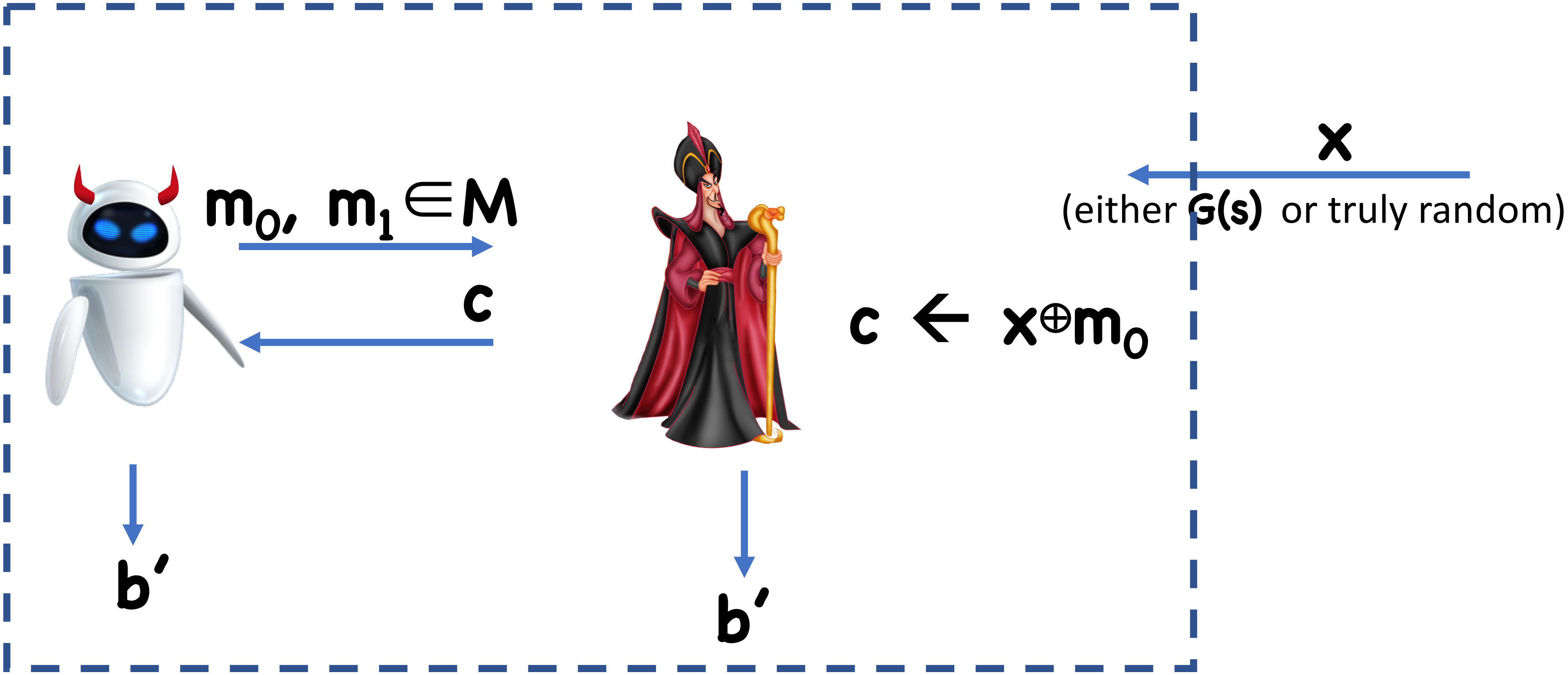
$m_0, m_1 \in M$

$c \leftarrow x \oplus m_0$

b'

An Alternate Proof: Hybrids

Suppose  distinguishes **Hybrid 0** from **Hybrid 1** with advantage **ε/3** ⇒ Construct



$m_0, m_1 \in M$

c

b'

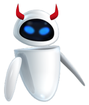
$c \leftarrow x \oplus m_0$

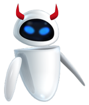
b'

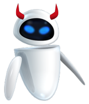
x

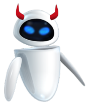
(either **G(s)** or truly random)

An Alternate Proof: Hybrids

Suppose  distinguishes **Hybrid 0** from **Hybrid 1** with advantage **ε/3** ⇒ Construct

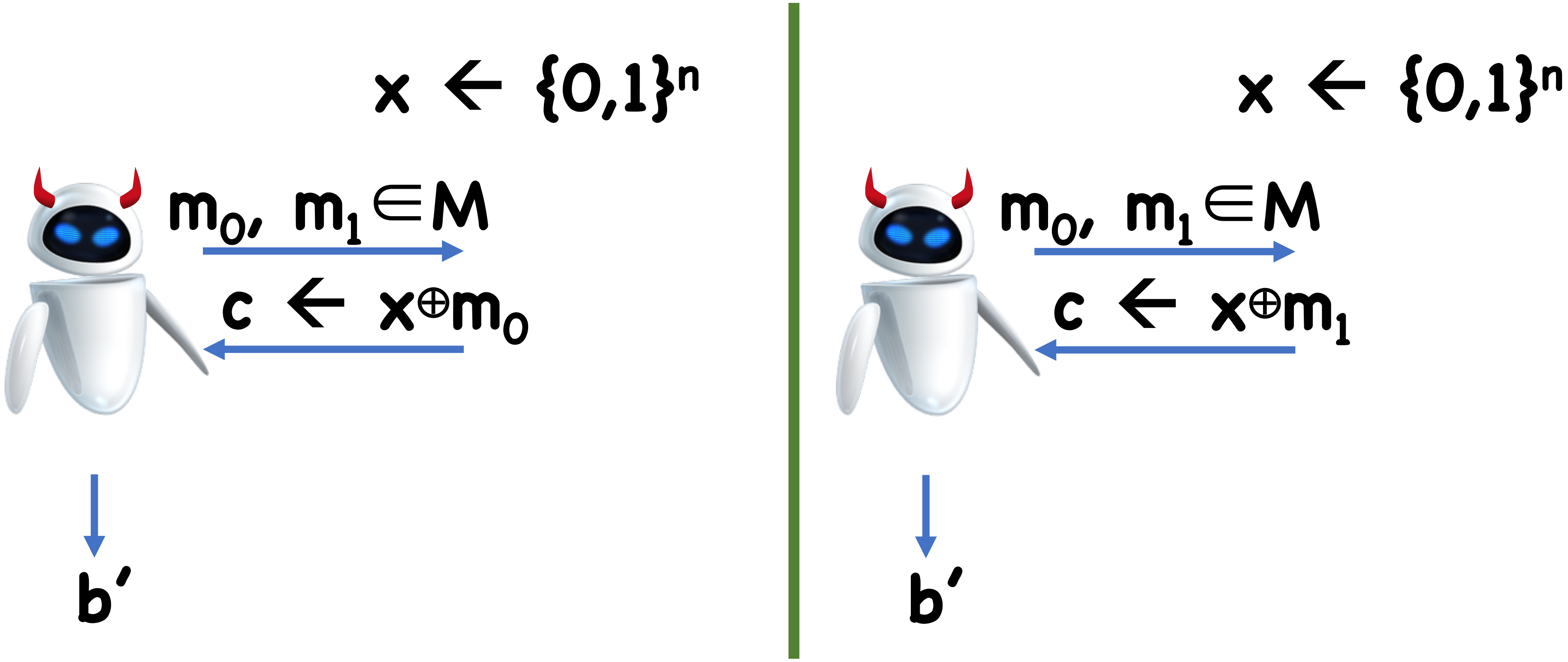
If is given **G(s)** for a random **s**,  sees **Hybrid 0**

If is given x for a random **x**,  sees **Hybrid 1**

Therefore, advantage of is equal to advantage of  which is at least **ε/3** ⇒ Contradiction!

An Alternate Proof: Hybrids

Suppose distinguishes **Hybrid 1** from **Hybrid 2** with advantage **$\varepsilon/3$**



$x \leftarrow \{0,1\}^n$

$m_0, m_1 \in M$

$c \leftarrow x \oplus m_0$

b'

$x \leftarrow \{0,1\}^n$

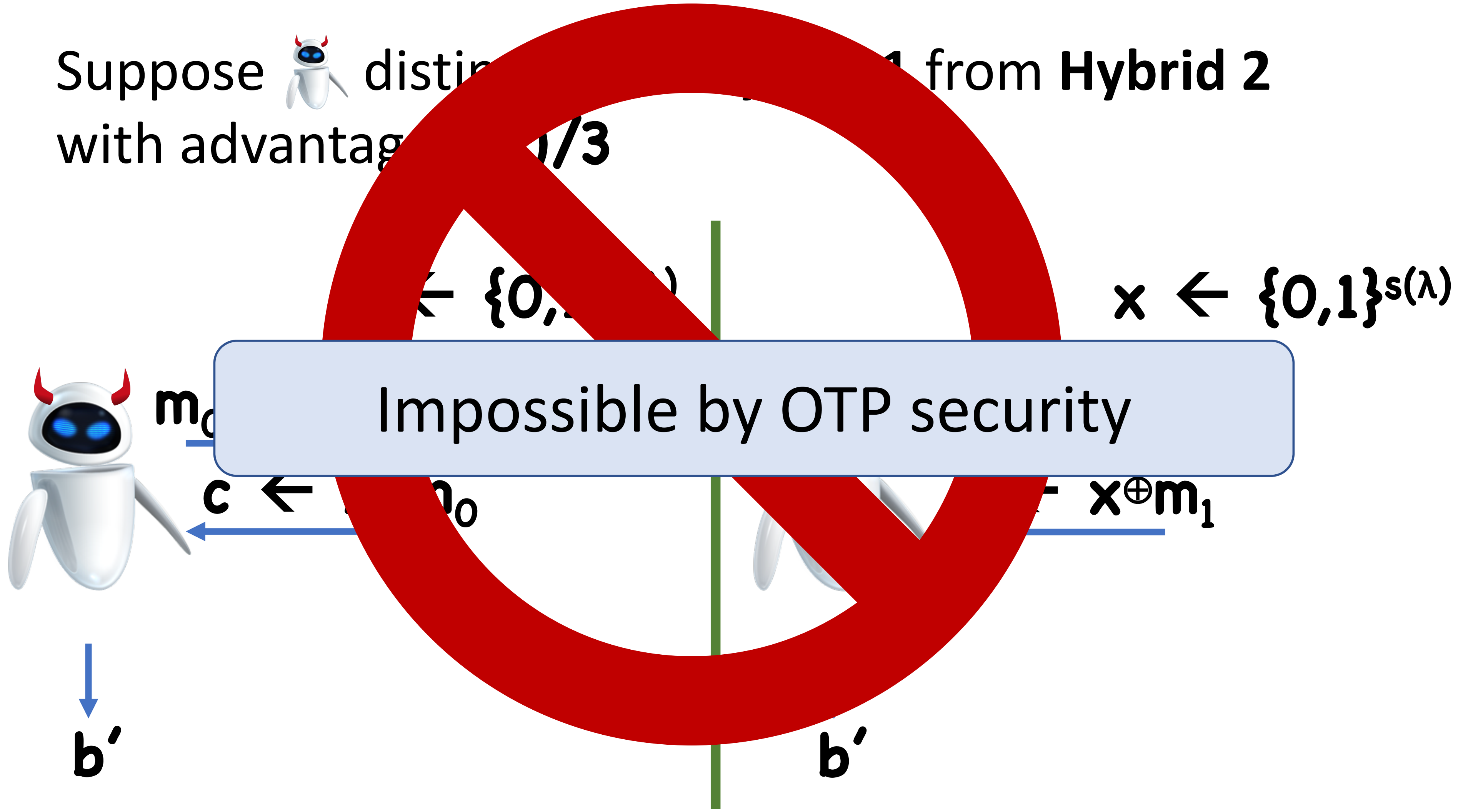
$m_0, m_1 \in M$

$c \leftarrow x \oplus m_1$

b'

An Alternate Proof: Hybrids

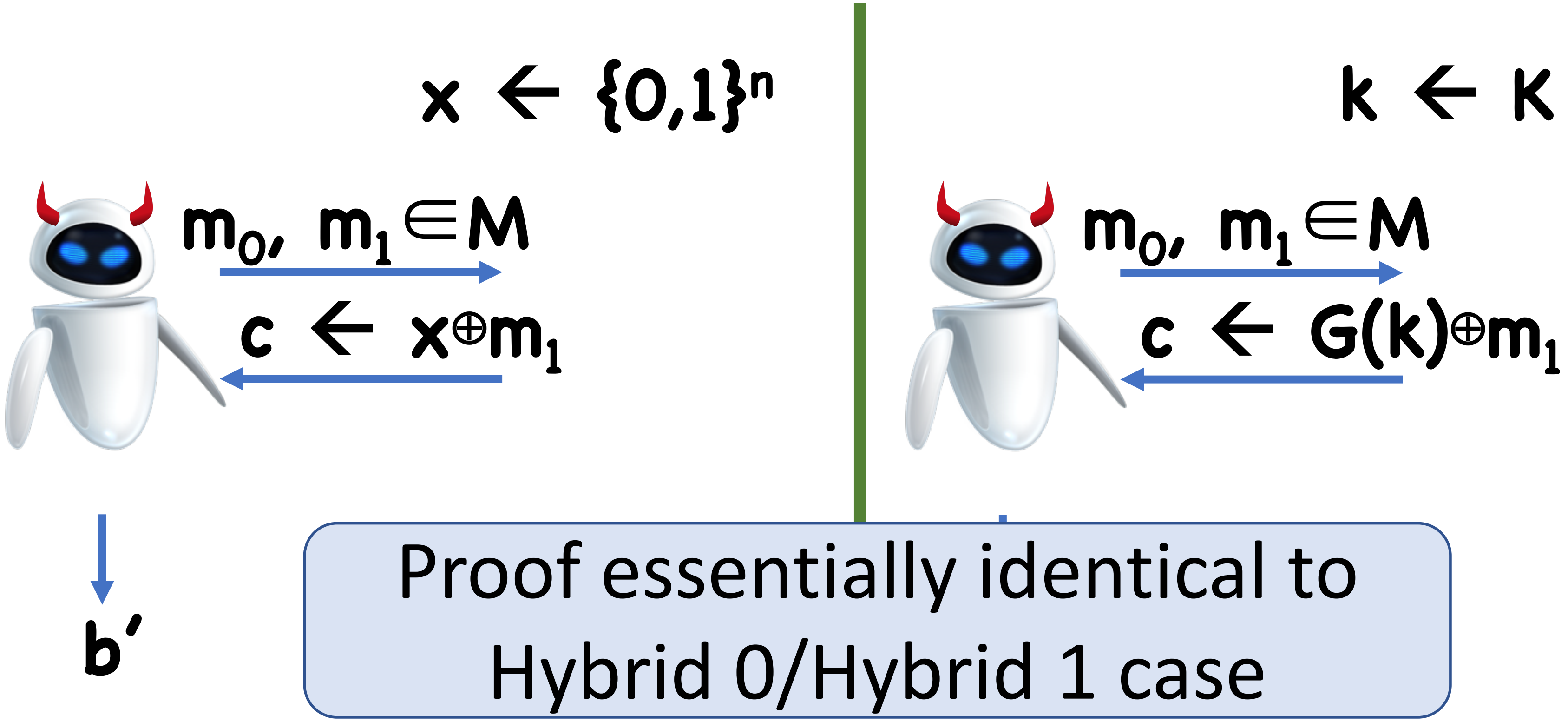
Suppose disti 1 from **Hybrid 2** with advantag **/3**



Impossible by OTP security

An Alternate Proof: Hybrids

Suppose 🤖 distinguishes **Hybrid 2** from **Hybrid 3** with advantage **$\varepsilon/3$**



$x \leftarrow \{0,1\}^n$

$m_0, m_1 \in M$

$c \leftarrow x \oplus m_1$

b'

$k \leftarrow K$

$m_0, m_1 \in M$

$c \leftarrow G(k) \oplus m_1$

Proof essentially identical to Hybrid 0/Hybrid 1 case

Reminders

PR1 Part 1 Due Tuesday, Feb 20th