CSCI 1510

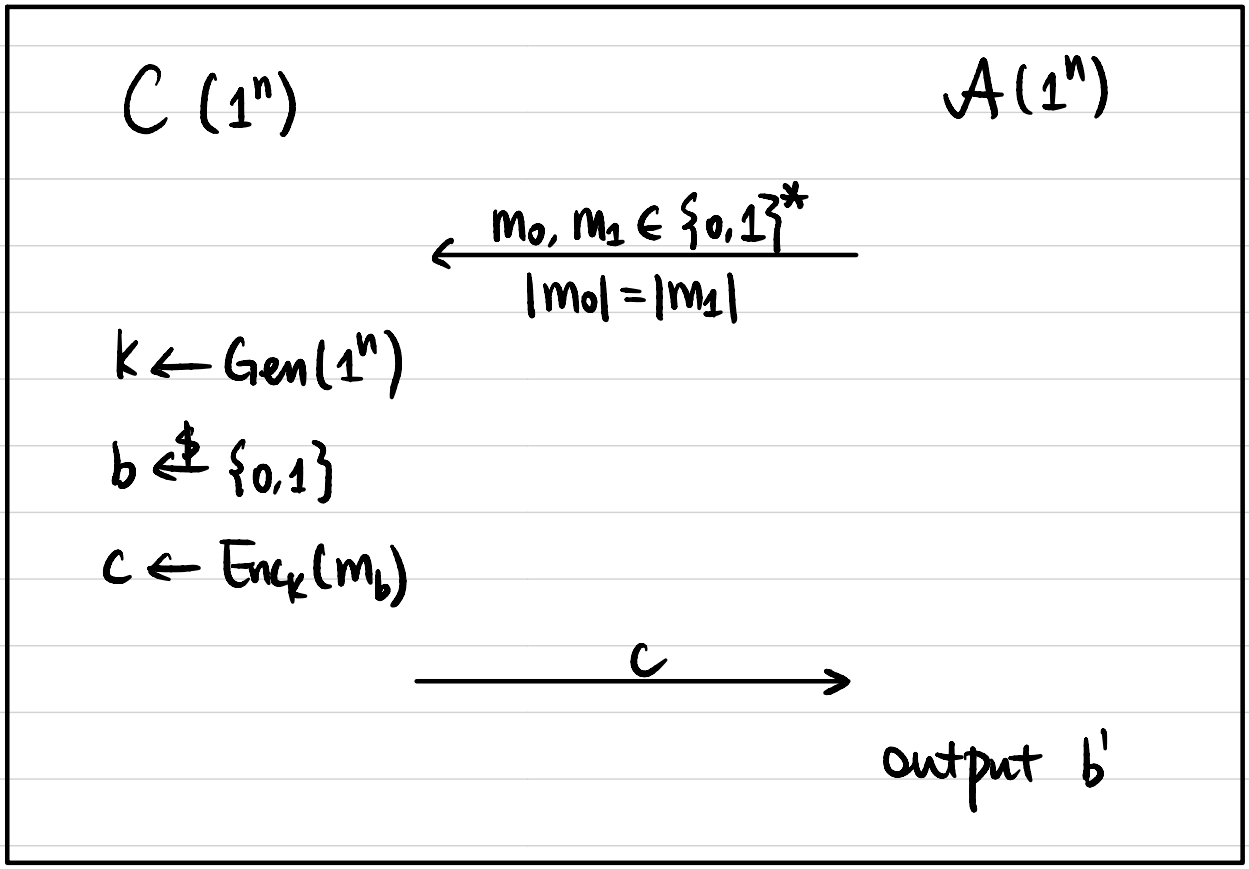
This Lecture:

- Chosen Plaintext Attack (CPA) Security
- Pseudorandom Function (PRF)
- CPA-Secure Encryption from PRF
- Hybrid Argument

Computationally Secure Encryption

Def 1 A symmetric-key encryption scheme (Gen, Enc, Dec) is **semantically secure** if $\forall$ PPT A, $\exists$ negligible function $\varepsilon(\cdot)$ s.t.

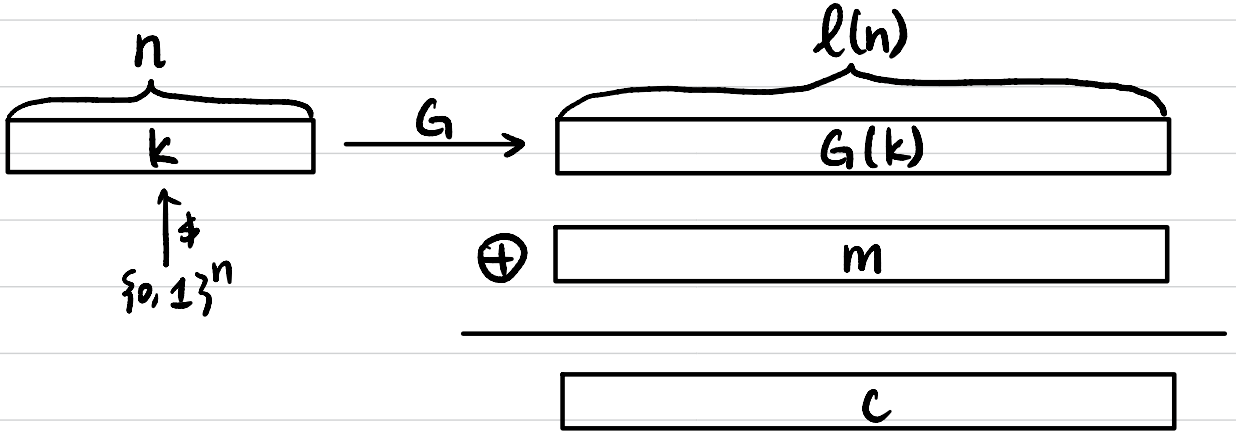
$$Pr[b = b'] \leq \frac{1}{2} + \varepsilon(n)$$



Fixed-Length Encryption Scheme

Let $G: \{0,1\}^n \to \{0,1\}^{\ell(n)}$ be a PRG.

- $\text{Gen}(1^n)$: sample $k \xleftarrow{\$} \{0,1\}^n$, output k.
- $\text{Enc}_k(m)$: $m \in \{0,1\}^{\ell(n)}$.
  output $c := G(k) \oplus m$.
- $\text{Dec}_k(c)$: $c \in \{0,1\}^{\ell(n)}$,
  output $m := G(k) \oplus c$.



"pseudo OTP"

Does Pseudo OTP allow encryption of multiple messages?

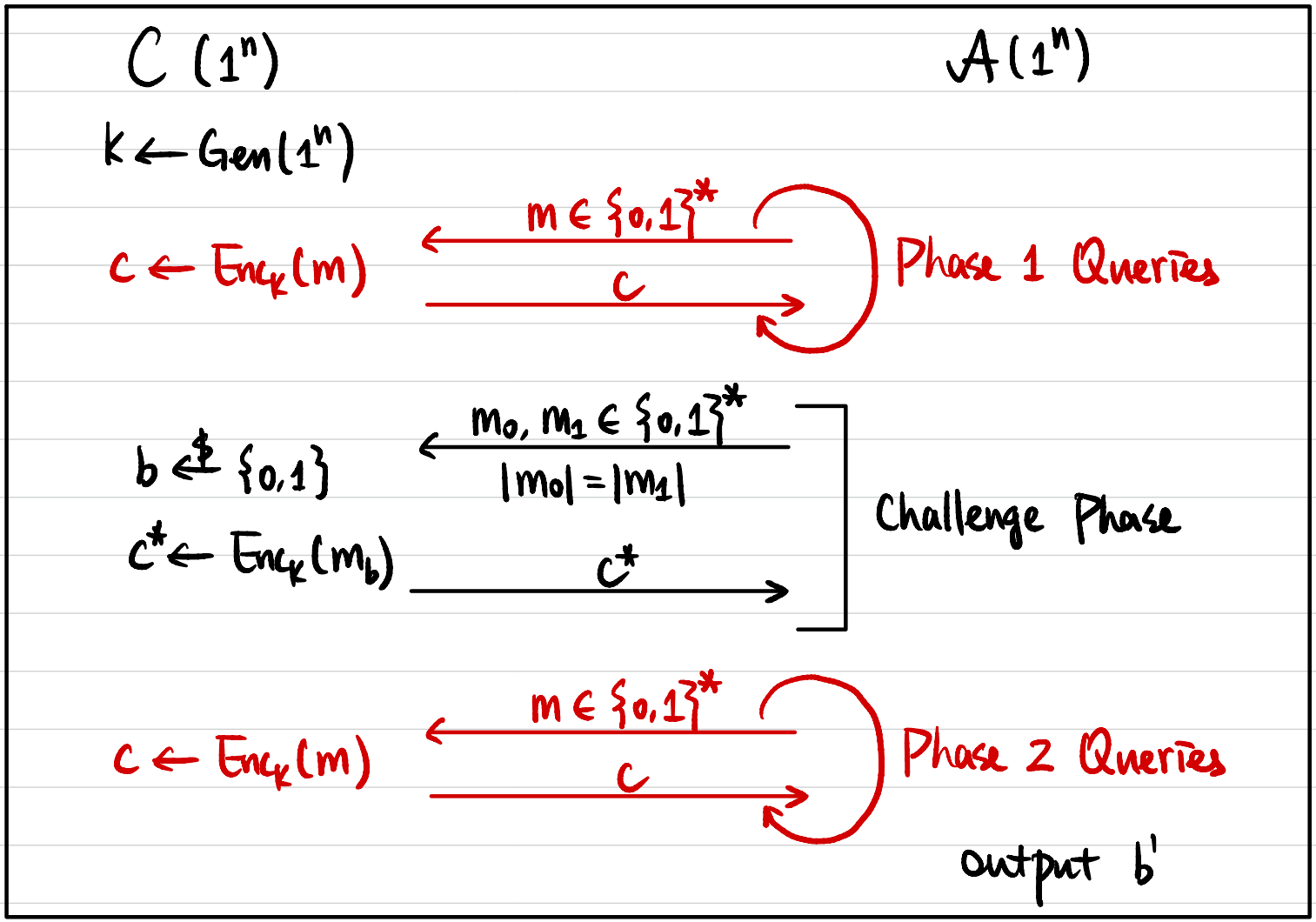
$C_1 = G_1(k) \oplus m_1$

$C_2 = G_1(k) \oplus m_2$

$\oplus \rightarrow m_1 \oplus m_2$

Chosen Plaintext Attack (CPA) Security

Def A symmetric-key encryption scheme (Gen, Enc, Dec) is **secure against chosen plaintext attacks**, or **CPA-secure**, if $\forall$ PPT $\mathcal{A}$, $\exists$ negligible function $\varepsilon(\cdot)$ s.t. $\Pr[b = b'] \leq \frac{1}{2} + \varepsilon(n)$



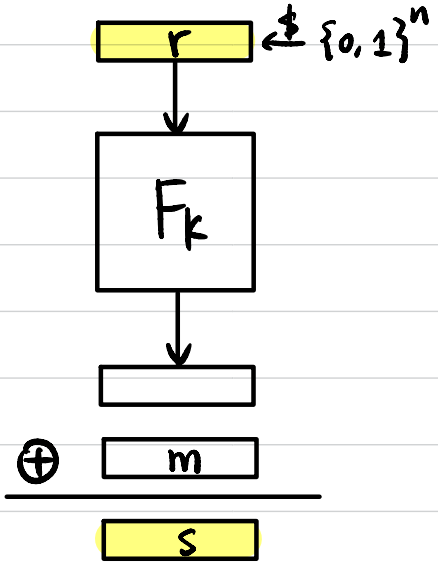
Is Pseudo OTP CPA-secure?

Thm If the Enc algorithm is deterministic on the secret key k and message m, then the encryption scheme can't be CPA-secure.

Constructing CPA-Secure Encryption

Pseudorandom Function (PRF)

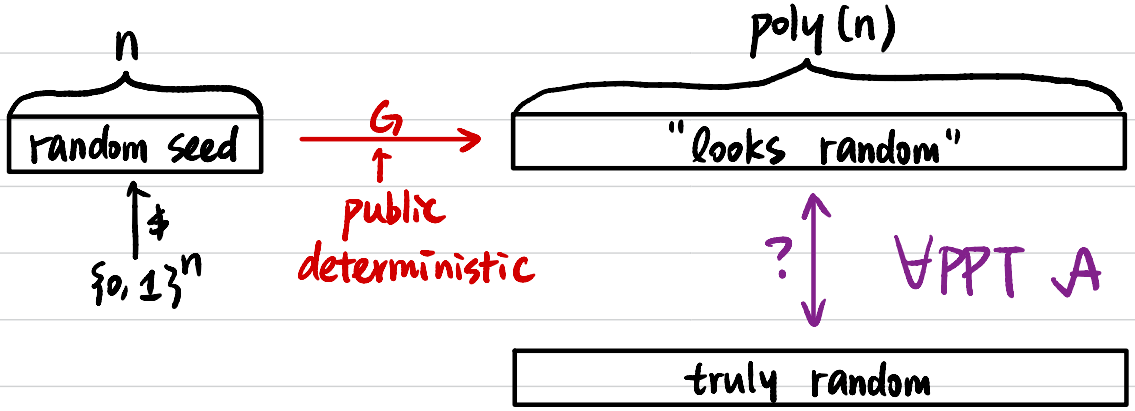
CPA-Secure Encryption



$C = \langle r, s \rangle$

Pseudorandom Function (PRF)

Pseudorandom Generator (PRG)



"random-looking" string

Pseudorandom Function (PRF):

"random-looking" function

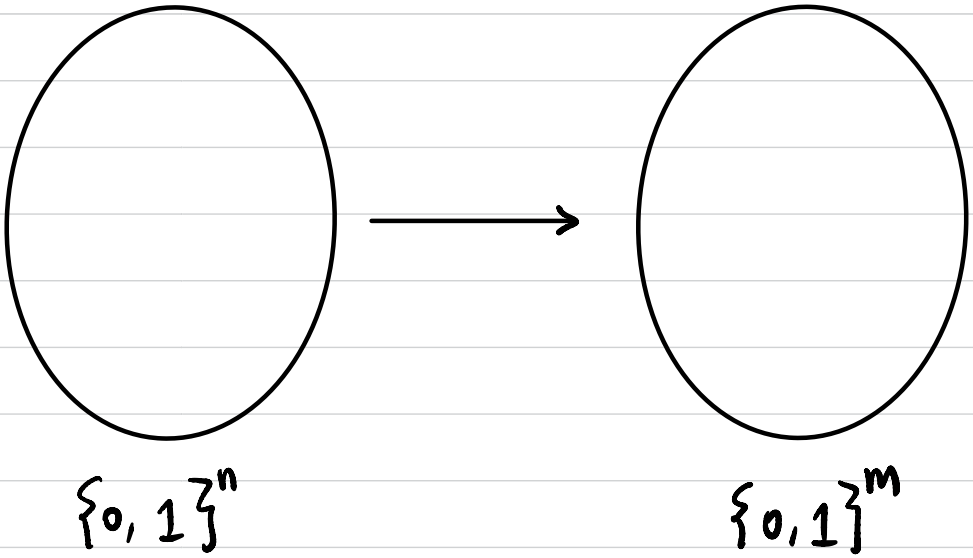
Pseudorandom Function (PRF)

Keyed Function $F: \{0,1\}^\lambda \times \{0,1\}^n \to \{0,1\}^m$

$F(k, x) \to y$

- F: deterministic poly-time
- k: key
- x: input
- y: output

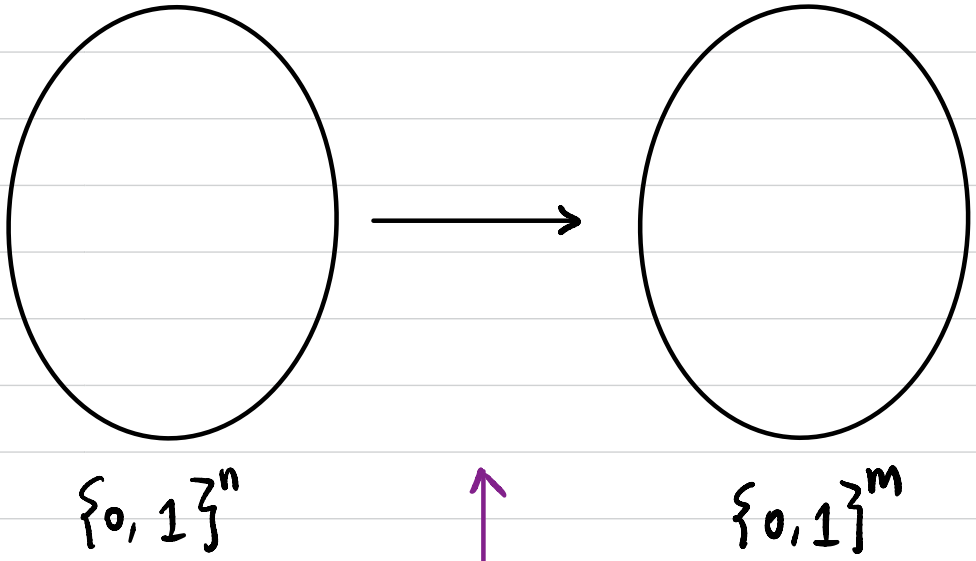
$k \xleftarrow{\$} \{0,1\}^\lambda$ $\quad F_k:$



"looks like a random function"

Pseudorandom Function (PRF)

$k \xleftarrow{\$} \{0,1\}^\lambda$ $\quad F_k :$

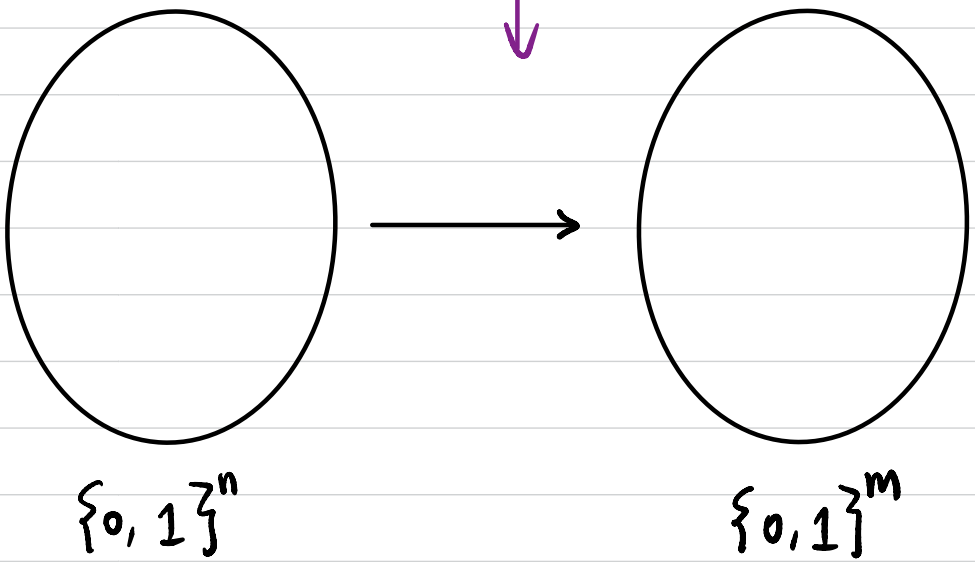


How many possible F_k's ?

$\forall$ PPT A
(not knowing k)

$f \xleftarrow{\$} \{ F \mid F: \{0,1\}^n \to \{0,1\}^m \}$

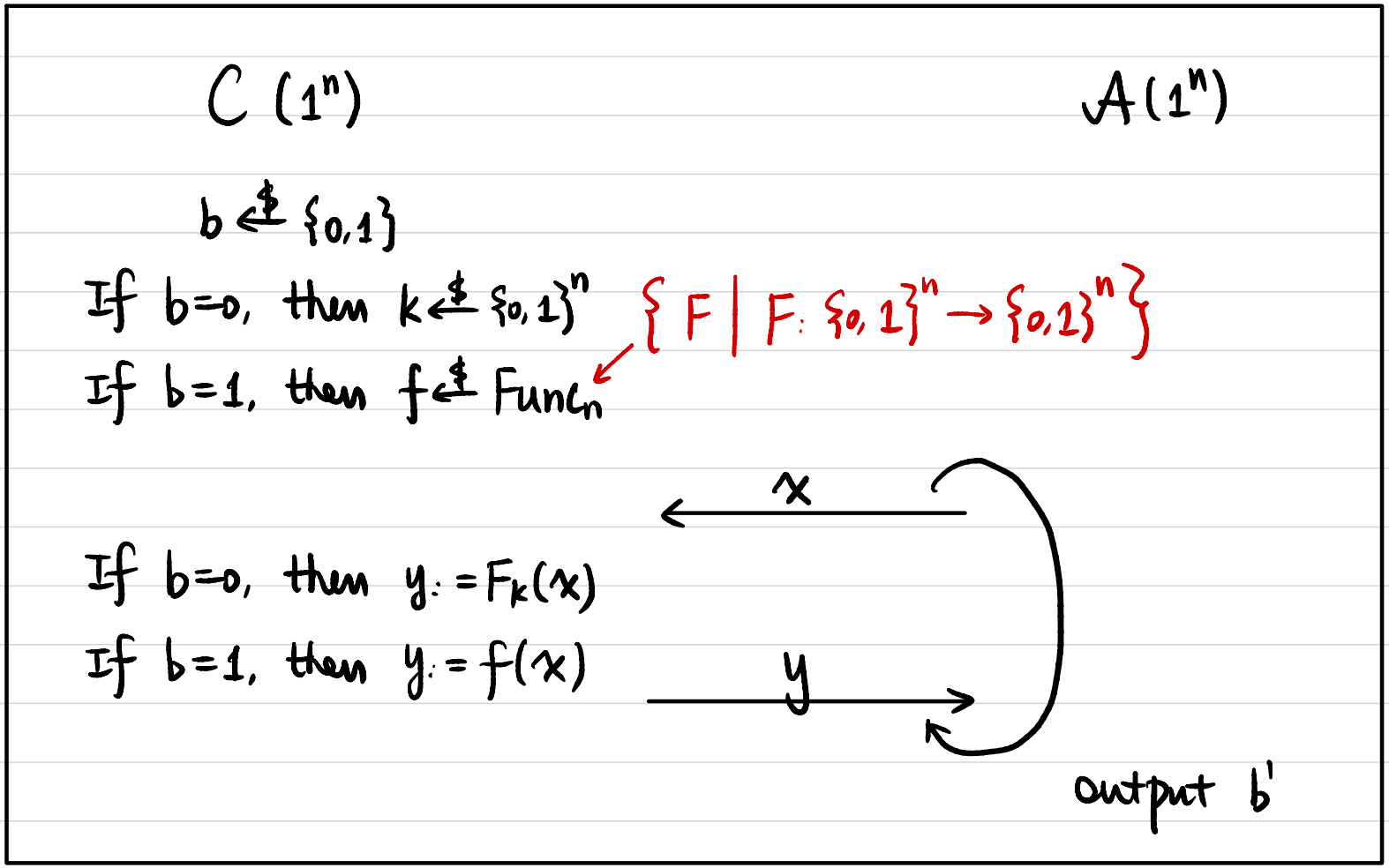
$f :$



How many possible f's ?

Pseudorandom Function (PRF)

Def 1 Let $F: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a deterministic, poly-time, keyed function. F is a **pseudorandom function (PRF)** if $\forall$ PPT A, $\exists$ negligible function $\varepsilon(\cdot)$ s.t. $\Pr[b = b'] \leq \frac{1}{2} + \varepsilon(n)$



Pseudorandom Function (PRF)

Def 2 Let $F: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a deterministic, poly-time, keyed function. F is a pseudorandom function (PRF) if $\forall$ PPT A, $\exists$ negligible function $\varepsilon(\cdot)$ s.t.

$$\left| \Pr_{k \leftarrow U_n}[A^{F_k(\cdot)}(1^n) = 1] - \Pr_{f \leftarrow \text{Func}_n}[A^{f(\cdot)}(1^n) = 1] \right| \leq \varepsilon(n)$$

Exercises

Let $F: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a PRF.

Define $F': \{0,1\}^n \times \{0,1\}^{n-1} \to \{0,1\}^{2n}$ as follows.

Is F' necessarily a PRF ?

a) $F_k'(x) = F_k(0\|x) \| F_k(0\|x)$ $\quad F_k(0\,\boxed{x}) \| F_k(0\,\boxed{x})$

b) $F_k'(x) = F_k(0\|x) \| F_k(1\|x)$ $\quad F_k(0\,\boxed{x}) \| F_k(1\,\boxed{x})$

c) $F_k'(x) = F_k(0\|x) \| F_k(x\|0)$ $\quad F_k(0\,\boxed{x}) \| F_k(\boxed{x}\,0)$

d) $F_k'(x) = F_k(0\|x) \| F_k(x\|1)$ $\quad F_k(0\,\boxed{x}) \| F_k(\boxed{x}\,1)$

PRF $\Leftrightarrow$ PRG

"$\Rightarrow$": Let $F: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a PRF,

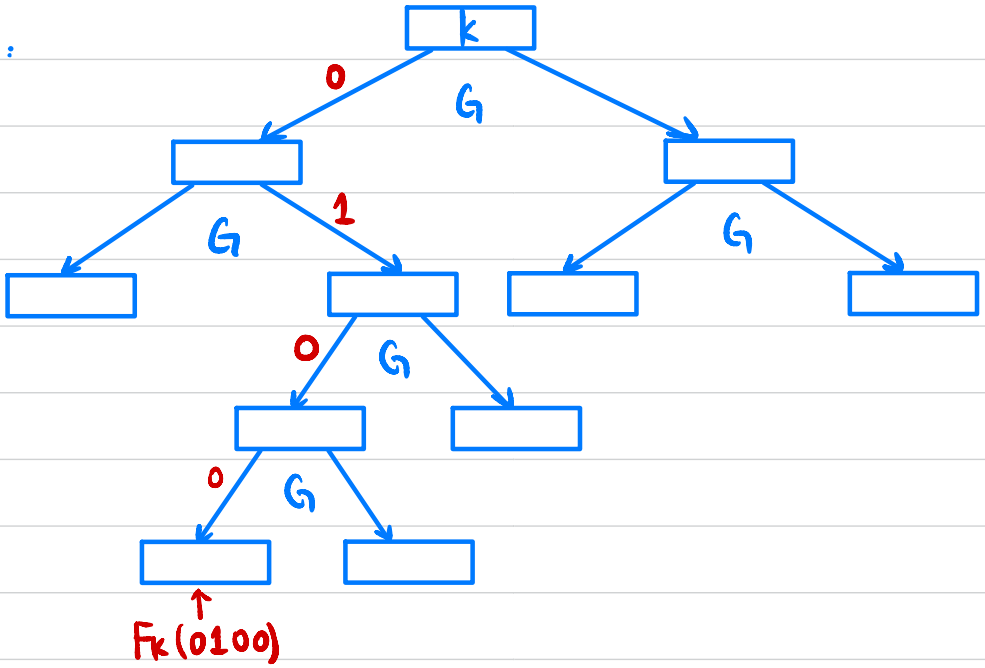
Construct $G: \{0,1\}^n \to \{0,1\}^{2n}$

$G(s) := ?$

"$\Leftarrow$": Let $G: \{0,1\}^n \to \{0,1\}^{2n}$ be a PRG,

Construct $F: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$

GGM tree:



CPA-Secure Encryption Scheme

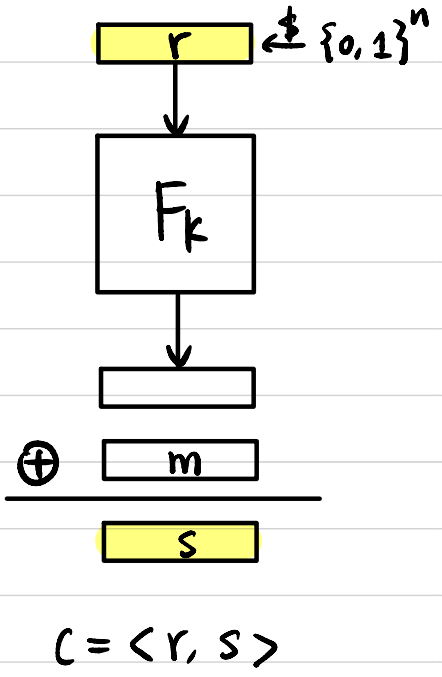
Let $F: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a PRF,

- $\text{Gen}(1^n)$: sample $k \xleftarrow{\$} \{0,1\}^n$, output k.
- $\text{Enc}_k(m)$: $m \in \{0,1\}^n$

  $r \xleftarrow{\$} \{0,1\}^n$

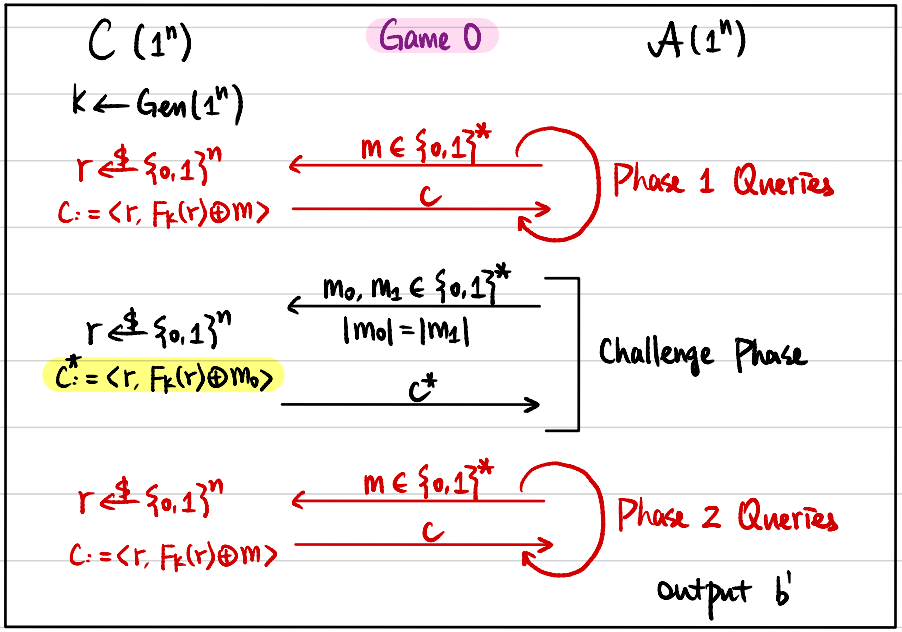
  output $c := \langle r, F_k(r) \oplus m \rangle$
- $\text{Dec}_k(c)$: $c = \langle r, s \rangle$

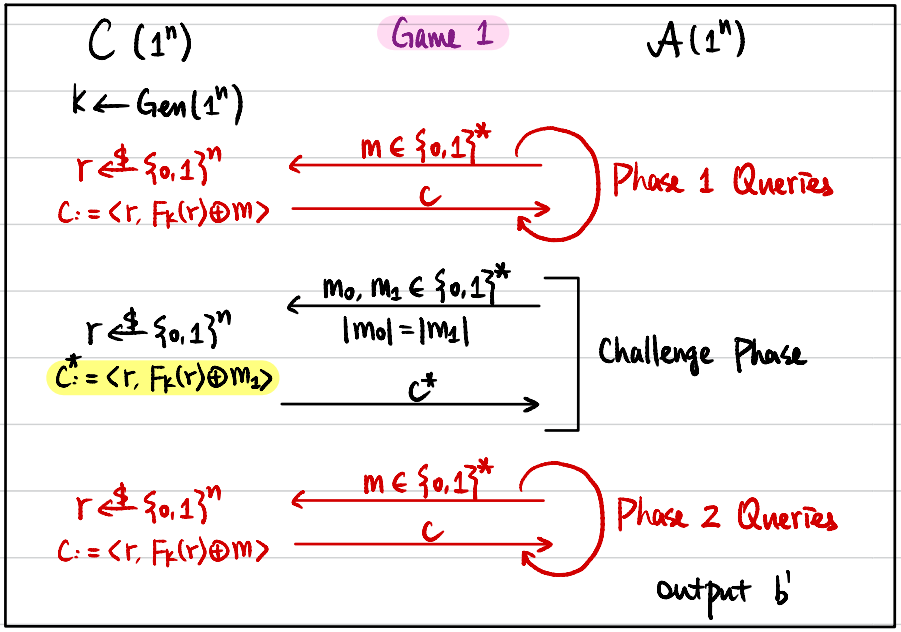
  output $m := F_k(r) \oplus s$



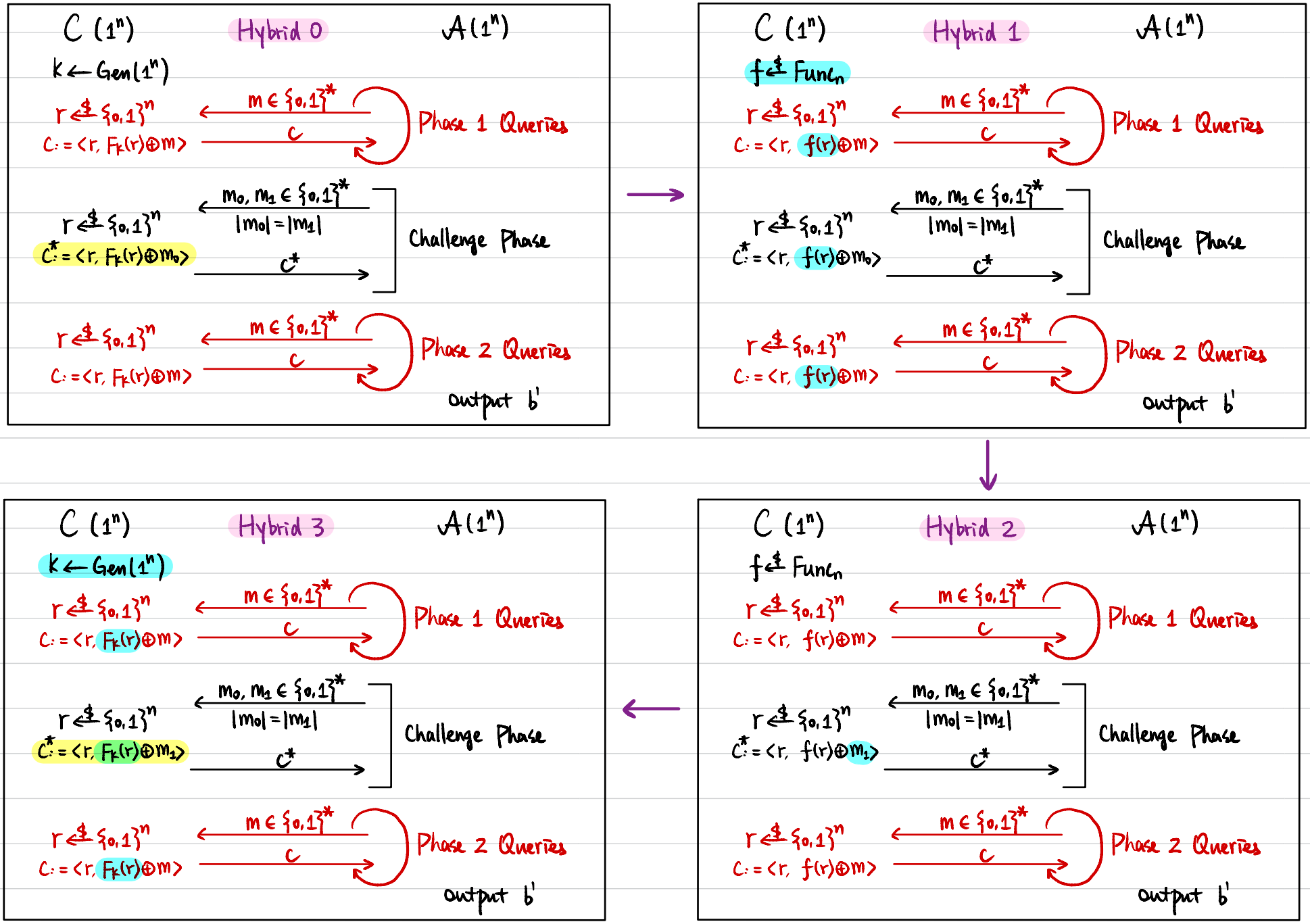
Theorem If F is a PRF, then $\Pi = (Gen, Enc, Dec)$ is CPA-secure.

Proof $\forall$ PPT $\mathcal{A}$,





$$\left| \Pr[\mathcal{A} \text{ outputs 1 in Game 0}] - \Pr[\mathcal{A} \text{ outputs 1 in Game 1}] \right| \leq \text{negl}(n) \ ?$$


C (1^n)
Hybrid 0
A (1^n)
k ← Gen(1^n)
r ←$ {0,1}^n
C := ⟨r, F_k(r) ⊕ m⟩
m ∈ {0,1}^*
c
Phase 1 Queries
r ←$ {0,1}^n
C* := ⟨r, F_k(r) ⊕ m_0⟩
m_0, m_1 ∈ {0,1}^*
|m_0| = |m_1|
c*
Challenge Phase
r ←$ {0,1}^n
C := ⟨r, F_k(r) ⊕ m⟩
m ∈ {0,1}^*
c
Phase 2 Queries
output b'
C (1^n)
Hybrid 1
A (1^n)
f ←$ Func_n
r ←$ {0,1}^n
C := ⟨r, f(r) ⊕ m⟩
m ∈ {0,1}^*
c
Phase 1 Queries
r ←$ {0,1}^n
C* := ⟨r, f(r) ⊕ m_0⟩
m_0, m_1 ∈ {0,1}^*
|m_0| = |m_1|
c*
Challenge Phase
r ←$ {0,1}^n
C := ⟨r, f(r) ⊕ m⟩
m ∈ {0,1}^*
c
Phase 2 Queries
output b'
C (1^n)
Hybrid 2
A (1^n)
f ←$ Func_n
r ←$ {0,1}^n
C := ⟨r, f(r) ⊕ m⟩
m ∈ {0,1}^*
c
Phase 1 Queries
r ←$ {0,1}^n
C* := ⟨r, f(r) ⊕ m_1⟩
m_0, m_1 ∈ {0,1}^*
|m_0| = |m_1|
c*
Challenge Phase
r ←$ {0,1}^n
C := ⟨r, f(r) ⊕ m⟩
m ∈ {0,1}^*
c
Phase 2 Queries
output b'
C (1^n)
Hybrid 3
A (1^n)
k ← Gen(1^n)
r ←$ {0,1}^n
C := ⟨r, F_k(r) ⊕ m⟩
m ∈ {0,1}^*
c
Phase 1 Queries
r ←$ {0,1}^n
C* := ⟨r, F_k(r) ⊕ m_1⟩
m_0, m_1 ∈ {0,1}^*
|m_0| = |m_1|
c*
Challenge Phase
r ←$ {0,1}^n
C := ⟨r, F_k(r) ⊕ m⟩
m ∈ {0,1}^*
c
Phase 2 Queries
output b'