Constructing Secure Encryption

Recap

- Perfect Secrecy
- Indist under eavesdropping
- Semantic Security
- Indist ≡ Semantic

Pseudo-random Generator (PRG)

$G(s) = x$

$s \in \{0,1\}^n$

$x \in \{0,1\}^{\ell(n)}$

$\ell(n) > n+s$

$(s \geq 1)$

PRG

If One Way Function (OWF) exists, then PRG exists

Let G be a deterministic algorithm that takes an n-bit i/p & o/ps an $\ell(n)$-bit string. G is called PRG if for all PPT adversary $\mathcal{D}$,

(i) $\ell(n) > n$,

(ii) $\left| \Pr_{\substack{s \xleftarrow{R} \{0,1\}^n \\ r_{\mathcal{D}}}} [\mathcal{D}(G(s)) = 1] - \Pr_{\substack{r \xleftarrow{R} \{0,1\}^{\ell(n)} \\ r_{\mathcal{D}}}} [\mathcal{D}(r) = 1] \right| \leq negl(n)$

$s \rightarrow$ seed

- behaves similar as key.
- large enough.

Stream Cipher

$(\text{Init}, \text{SGen})$ $\quad |s| = n$

$st_0 \leftarrow \text{Init}(s, IV)$ — s: seed; IV: optional initialization vector

$(y_i, st_i) \leftarrow \text{SGen}(st_{i-1})$, $\forall i = 1(1)\ell(n)$

$y_i \in \{0,1\}$

return $y_1 y_2 \cdots y_{\ell(n)}$

Encryption Scheme using PRG

Π {

Key Gen: $k \xleftarrow{\$} \{0,1\}^n$

Enc: $c \leftarrow G(k) \oplus m$

Dec: $m := G(k) \oplus c$

}

$G: \{0,1\}^n \to \{0,1\}^{\ell(n)}$

PRG

Th^m: If G is PRG, then Π is indistinguishable under eavesdropping adversary.

Encryption Scheme using PRG

Π {

Key Gen: $k \xleftarrow{\$} \{0,1\}^n$

Enc: $c \leftarrow G(k) \oplus m$

Dec: $m := G(k) \oplus c$

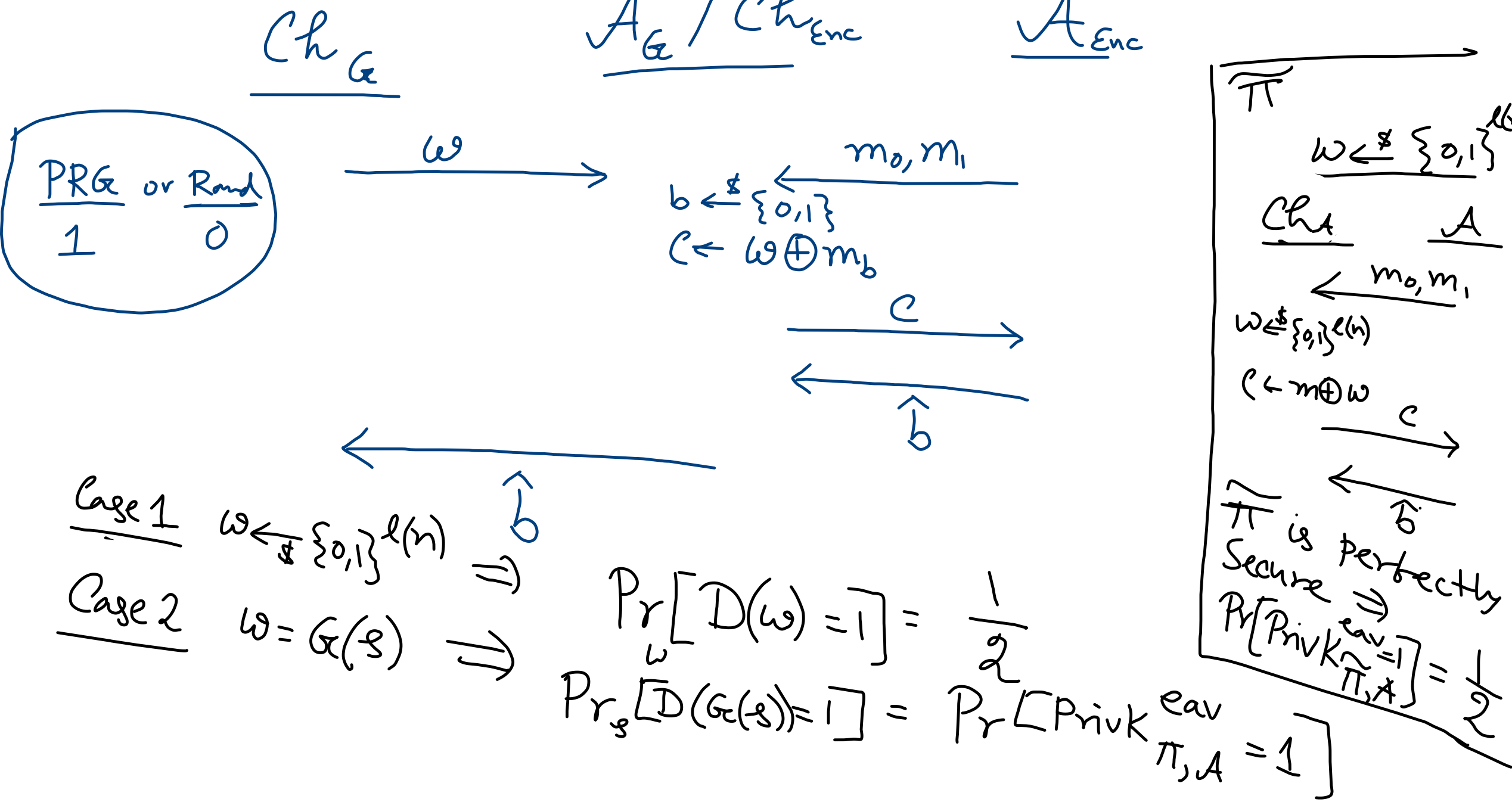
}

$G: \{0,1\}^n \to \{0,1\}^{\ell(n)}$

PRG

Th^m: If G is PRG, then Π is indistinguishable under eavesdropping adversary.

Prove: (By reduction)



$$\left| \Pr[D(\omega)=1] - \Pr[D(G(s))=1] \right|$$

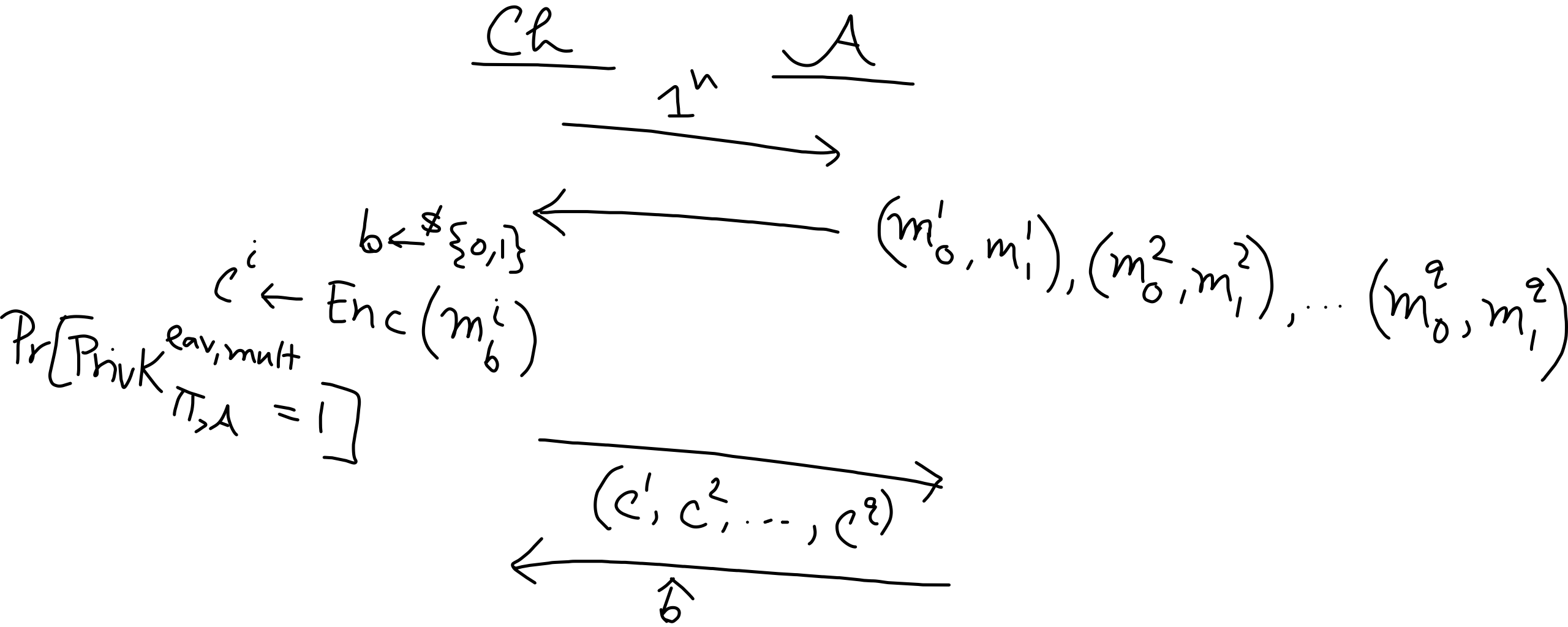
$$= \left| \frac{1}{2} - \Pr\left[PrivK^{eav}_{A,\Pi}=1\right] \right| \quad -(1)$$

<u>G is PRG</u> then L.H.S of (1) $\leq$ negl(n)

From (1), $\Pr\left[PrivK^{eav}_{A,\Pi}=1\right] \leq \frac{1}{2} + negl(n)$

How About Multiple-Encryptions?

Indistinguishability under eavesdropping under mult encryption



$Pr[PrivK^{eav,mult}_{\pi,A} = 1]$

Π → using PRG

Ch ⟷ $\mathcal{A}$

$\mathcal{A}$ → $((m_0, m_1), (m_0, m_2))$

Ch → (c_0, c_1)

* Power of the Adv
↳ Ciphertext Only

* Any deterministic Encryption is insecure under indist against eavesdropping (multiple queries)

if $(c_0 \equiv c_1)$ Return 0

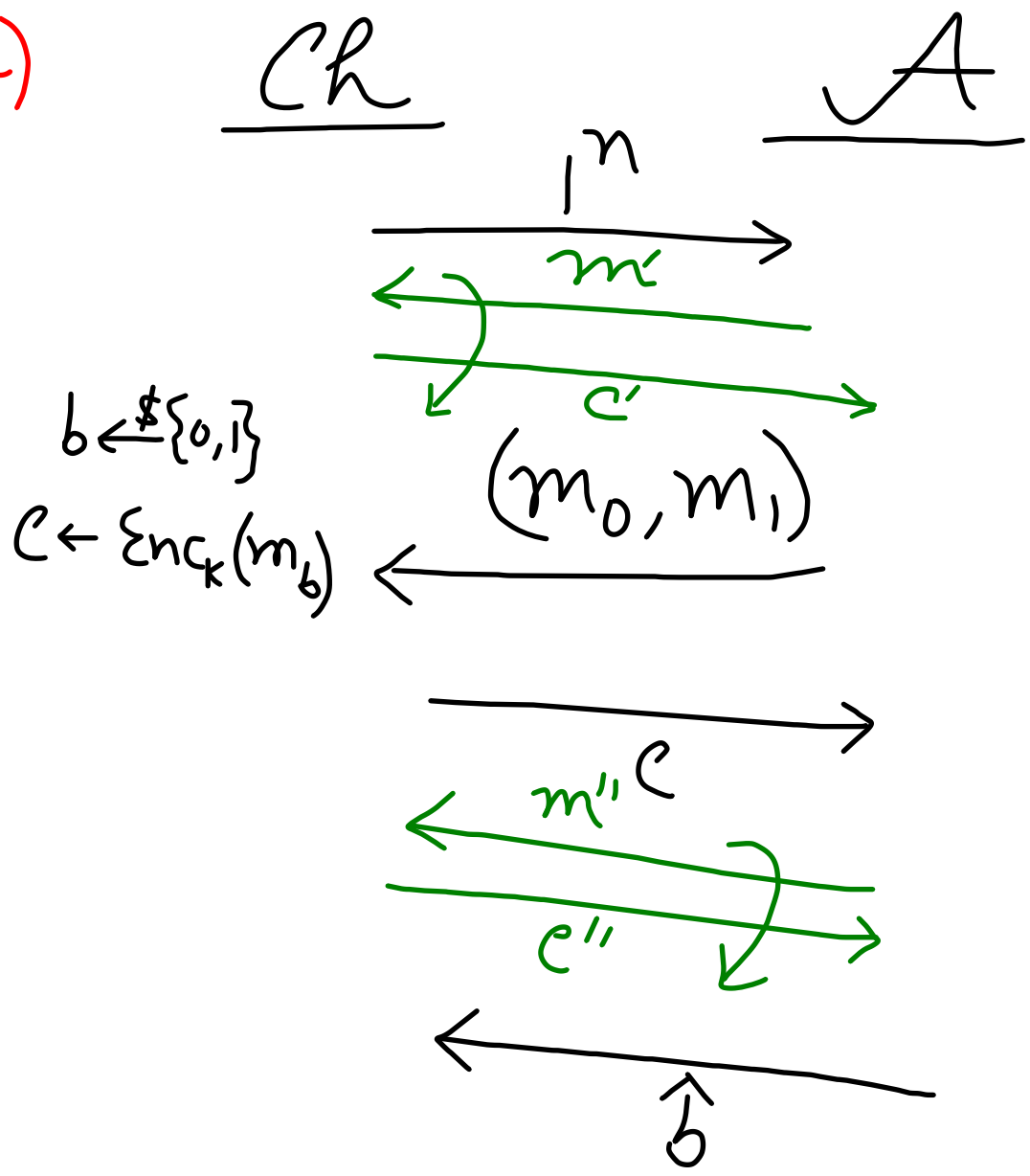
O/W Return 1

Indistinguishability under CPA

(IND-CPA: goal = IND, power = CPA)

(Single Message)

{Chosen Plaintext Attack}

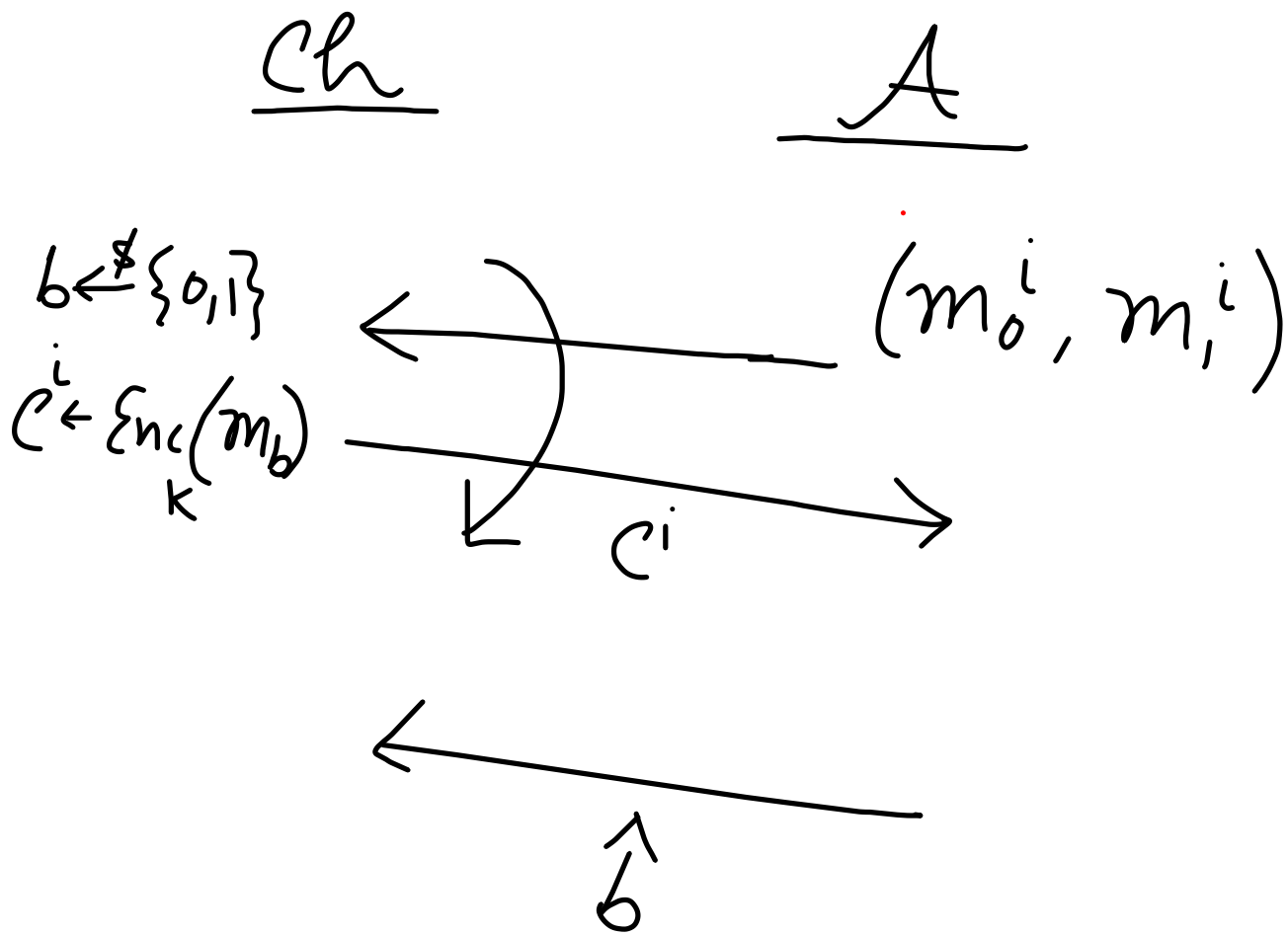


IND-CPA (Multiple Messages)

LOR

↓

{ Left or Right



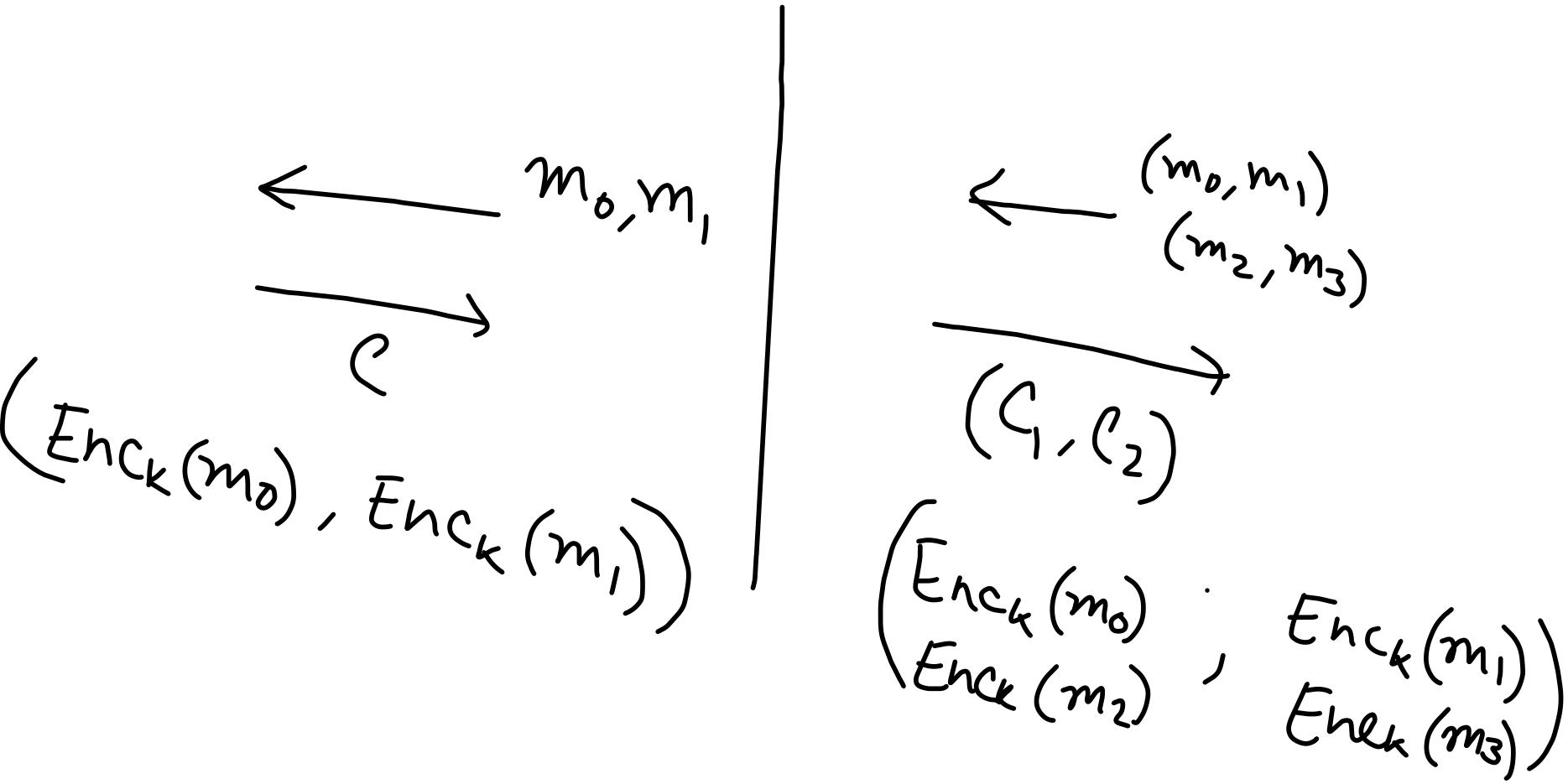
CPA Queries

(m, m)

c

Th^m

If Π is ind-cpa under single message, Π is ind-cpa in LOR (i.e. for multiple messages)



Ex

$G \to PRG$ with $\ell(n) > 2n$ → expansion factor

Home work

Say whether G' is PRG or not?

- $G'(s) = G(s_1, \ldots, s_{n/2})$, $s = s_1 \ldots s_{n/2}$
- $G'(s) = G(0^{|s|} \| s)$
- $G'(s) = G(s) \| G(s+1)$

$|s| = n$

$G'(s) = G(0^n \| s)$

s: n

$0^n \| s$: $2n$

$s = 0111 = 7$

$s+1 = 1000 = 8$