

## §2 Preliminaries

### § 2.1 Basics

$\lambda$   
poly(.)

overwhelming  $\geq 1 - \text{negl}$

$\mathcal{H}$

$S(\mathcal{H})$  is the unit sphere  $\{x : \|x\|_2 = 1\}$  in  $\mathcal{H}$

$U(\mathcal{H})$

density matrices

$\mathcal{H}_X$  Hilbert space for register  $X$ .

$$TD(\rho, \sigma) := \frac{1}{2} \|\rho - \sigma\|_{\text{tr}}$$

$\epsilon$ -close if  $TD(\rho, \sigma) \leq \epsilon$

POVM  $\{E_i\}$  on  $\mathcal{H}$ ;  $\sum E_i = I$

(  
projectors means  
projective measurement

"Def": "uncomputable".

A quant. alg. can be modelled as a

unitary  $U$  acting on  $\mathcal{H}$ ,

then performing a measurement on output registers  
w/o loss of generality.

(Here) Uncomputable means ~~not~~ apply  $U^+$  to the resulting state.

Informal claim: If the measurement outputs same result, w/ overwhelming prob.  
then the trace dist. b/w the final & the original state  
is negligible.

## §2 Preliminaries

### § 2.1 Basics

$\lambda$   
 $\text{poly}(\cdot)$

overwhelming  $\geq 1 - \text{negl}$

$\mathcal{H}$

$S(\mathcal{H})$  is the unit sphere  $\{x : \|x\|_2 = 1\}$  in  $\mathcal{H}$

$\mathcal{U}(\mathcal{H})$

$D(\mathcal{H})$  density matrices

$\mathcal{H}_X$  Hilbert space for register  $X$ .

$$\text{TD}(\rho, \sigma) := \frac{1}{2} \|\rho - \sigma\|_1$$

$\epsilon$ -close if  $\text{TD}(\rho, \sigma) \leq \epsilon$

POVM  $\{E_i\}$  on  $\mathcal{H}$ ;  $\sum E_i = I$

(  
projectors means  
projective measurement

"Def": "uncomputable".

A quant. alg. can be modelled as a

unitary  $U$  acting on  $\mathcal{H}$ ,

then performing a measurement on output registers  
w/o loss of generality.

(Here) Uncomputable means not apply  $U^\dagger$  to the result state.

Informal claim: If the measurement outputs same result, w/ overwhelming prob.  
then the trace dist. b/w the final & the original state  
is negligible.

"oracle for  $f$ "

$$O_f : \langle x | \rangle \otimes |y\rangle = \langle x | \rangle |y\rangle \oplus f(x)|y\rangle$$

"A quantum adversary  $\mathcal{A}$  w/ access to oracle(s) is query-bounded if it makes at most  $p(\lambda)$  queries to each oracle for some polynomial  $p(\cdot)$ ".

## § 2.2 Quantum Random Oracle Model (QROM)

$H$ : a random classical  $f$   
that can be accessed by an adversary in superposition  
modelled by  $|^0 H\rangle$ .

Story: The following taken from [BBBV '97] will be used to  
reprogram oracles w/o adversarial detection on  
inputs which are not queried w/ large  
weight:

Thm 2.1 ([BBBV '97]). Let:  $\mathcal{A}$  be an adversary w/  
oracle access to  $H : \{0,1\}^m \rightarrow \{0,1\}^n$   
making at most  $T$  queries.

Def<sup>n</sup>: (i)  $|\psi_i\rangle$  as the global state after  $\mathcal{A}$  makes  $i$  queries  
(ii)  $W_y(|\psi_i\rangle)$  as the sum of squared amplitudes  
in  $|\psi_i\rangle$  of terms in which  
 $\mathcal{A}$  queries  $H$  on input  $y$ .

Let: (i)  $\epsilon > 0$  &  
(ii)  $F \subseteq [0, T-1] \times \{0, 1\}^m$  be a set of time-step  
pairs s.t.  $\sum_{(i,y) \in F} w_y(|\phi_i\rangle) \leq \frac{\epsilon^2}{T}$ .

Let:  $H'$  be an oracle obtained after reprogramming  $H$   
on inputs  $(i, y) \in F$  to arbitrary outputs.

Define:  $|\phi'_i\rangle$  as above for  $H'$ .

Then,  $TD(|\phi_i\rangle, |\phi'_i\rangle) \leq \epsilon/2$

NB: The theorem can be extended to mixed states by  
convexity.

### § 2.3 More on Jordan's lemma

This version is, from [Reg05] & [Vid21]:  
adapted

**Lemma 2.2.** Let  $w \in [0, 1]$

- $\mathcal{H}$  be a finite-dimensional Hilbert space
- $\Pi_0, \Pi_1$  be any two projectors in  $\mathcal{H}$

Then, (i)  $\exists$  an orthogonal decomposition of  $\mathcal{H}$  into  
two dimensional subspaces

$\mathcal{H} = \bigoplus_i S_i$  that are invariant under both  
 $\Pi_0$  &  $\Pi_1$

(ii)  $S_i$  is spanned by one or two eigenvectors of  $w\Pi_0 + (1-w)\Pi_1$

(iii) Whenever  $S_i$  is 2-dimensional,

$\exists$  a basis for it in which  $\Pi_0 \& \Pi_1$   
(restricted on  $S_i$ )

take the form:

$$\Pi_{0,S_i} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad \& \quad \Pi_{1,S_i} = \begin{pmatrix} c_i^2 & c_i s_i \\ c_i s_i & s_i^2 \end{pmatrix}$$

where  $c_i = \cos\theta_i$ ,  $s_i = \sin\theta_i$  for some principle angle  $\theta_i \in [0, \pi/2]$ .

Proof. For the  $w=1$  case, see [Reg05] or [Vid21]  
& the generalization is apparently straightforward  
□

Story: They additionally show a relation b/w the eigenvalues in the same Jordan Block.

**Lemma 2.3** For any two projectors  $\Pi_0 \& \Pi_1$ ,

let  $(\cdot)S_i$  be a 2-dimensional subspace  
(as described in Lemma 2.2).

(ii)  $|0_0\rangle, |0_1\rangle$  be the two eigenvectors of

$w\Pi_0 + (1-w)\Pi_1$  that span  $S_i$

Then, it holds that  $\lambda_0 + \lambda_1 = 1$ , w/eigenvalues  $\lambda_0, \lambda_1$  resp.

Proof. Restrict to  $s_i$ . Then, (take  $w = \gamma_2$ ; general case goes through similarly)

$$\begin{aligned} \text{NB: } \lambda_0 + \lambda_1 &= \text{tr}((\Pi_{0,s_i} + \Pi_{1,s_i})/2) \\ &= \frac{1 + c_i^2 + s_i^2}{2} = 1. \end{aligned}$$

□

Corollary 2.4 For any two projectors  $\Pi_0, \Pi_1$ , let  $|\phi_0\rangle$  &  $|\phi_1\rangle$  be the eigenvectors of

$$\omega \Pi_0 + (1-\omega) \Pi_1$$

w/ eigenvalues  $\lambda_0, \lambda_1$ .

If  $\lambda_0 + \lambda_1 \neq 1$  &  $\lambda_0 \neq \lambda_1$ , then

$$\langle \phi_0 | \Pi_0 | \phi_1 \rangle = \langle \phi_0 | \Pi_1 | \phi_1 \rangle = 0.$$

Proof. If  $\lambda_0 + \lambda_1 \neq 1$ , then

NB1: Lemma 2.3 says that  $|\phi_0\rangle$  &  $|\phi_1\rangle$  cannot be in the same Jordan Block.

Also, we have

NB2:  $\Pi_0 |\phi_0\rangle$  stays in the same Jordan Block as  $|\phi_0\rangle$  (that's how we defined  $s_i$ ).

Conclusion  $|\phi_0\rangle$  is orthogonal to  $|\phi_1\rangle$ .

□

## § 2.4 Measuring Success Probability

**story:** Preliminaries on how to measure the success prob. of quantum programs (wrt a test distribution).  
(Me: quantum, I suppose)

- : classically, this is easy to estimate to inverse poly precision.
- suppose the test distribution can be sampled from efficiently.
- To estimate the success prob., simply run the program many times.
- : Quantumly : This idea doesn't work because the quantum program may get consumed — we are given only one copy.  
One must therefore "rewind the program"— but this is difficult in general.

### Measure Probability:

**Story:** In [Zha20], Shendy formulates a "measurement operator" for estimating the success prob. of a quantum program.

This operator is efficient to implement, but  
 /  
 discussed shortly  
 Zhandry also shows how to efficiently  
 estimate the probability w/  
 large statistical confidence in  
 the same work  
 (following the idea in QMA amplification [MW'05]).

- Intuition:**
- Suppose a POVM specifies whether a quantum program succeeds or not.
  - Note that this does not specify the post-measurement state.
  - Zhandry shows that,

$$\text{for any POVM } P = (P, \mathbb{I} - P)$$

there is a nice projective measurement  $E_{\text{pt}}$ .  
 the post-measurement state is an eigenvector of  $P$ .

**Me:** The whole point seems to be that one can measure using this projective measurement w/o affecting the "prob of success" when the POVM is measured later. (This happens  $\because$  the projective measurement commutes w/ the POVM  $P$ )

- ! The projector is constructed simply using the eigenvectors of  $P$  — but this process (and eigenvalues) may not be efficient

• More precisely,

(i)  $\mathcal{E}$  outputs a <sup>real</sup> number  $p \in [0, 1]$  from  
the "probability"

the set of eigenvalues of  $P$ .

(Yes,  $\mathcal{E}$  is taken to output a real number)

(ii) The post-measurement state

upon obtaining outcome  $p$  is

an eigenvector of  $P$

w/ eigenvalue  $p$

(it's also an eigenvector of  $\mathcal{Q} = \mathbb{I} - P$

w/ eigenvalue  $(1-p)$ )

[me:  $\mathcal{E}$  is basically constructed (sufficiently) as follows:

• NB:  $P$  &  $\mathcal{Q} = \mathbb{I} - P$  have common eigenvectors  
 $\therefore$  they commute.

•  $P$  has eigenvectors  $\{|q_i\rangle\}$  w/ eigenvalues  $\{p_{q_i}\}$ .

• The formal statement is as follows

(the construction above essentially proves the thm)

### Thm 2.5 (Inefficient Measurement).

Let  $P = (P, Q)$  be a binary outcome POVM.  
 Let  $D$  be the set of eigenvalues of  $P$ .

$\exists$  a projective measurement  $\Sigma = \{E_p\}_{p \in D}$   
 w/ index set  $D$  s.t.

(0)  $\rho_p := E_p P E_p$  is the sub-normalised post-measurement state  $\forall p$ .

(1)  $\forall p \in D$ ,  $\rho_p$  is an eigenvector of  $P$   
 w/ eigenvalue  $p$

(2) The prob. of  $p$  when measured w/

$$P \in \mathcal{U}[P] = \sum_{p \in D} \mathcal{U}[P \rho_p].$$

**Story:** suppose  $|+\rangle = \sum_i \omega_i |+\rangle_i$ . (recall:  $P = \sum_i \lambda_i |+\rangle_i \langle +|_i$ )

Then, measuring  $|+\rangle$  using  $\Sigma$  yields  $|+\rangle_i$  w.p.  $|\omega_i|^2$ .

### Thm 2.6 (Inefficient threshold measurement).

Let  $P = (P, Q)$  be a binary outcome POVM.

Let  $P$  have eigenbasis  $\{|+\rangle_i\}$  w/ eigenvalues  $\{\lambda_i\}$ .

Then,  $\forall r \in (0, 1)$   $\exists$  a projective measurement

$$\Sigma_r = (E_{\leq r}, E_{>r})$$
 s.t.

### Thm 2.5 (Inefficient Measurement).

Let  $P = (P, Q)$  be a binary outcome POVM.

Let  $\mathcal{D}$  be the set of eigenvalues of  $P$ .

$\exists$  a projective measurement  $\Sigma = \{E_p\}_{p \in \mathcal{D}}$   
w/ index set  $\mathcal{D}$  s.t.

(0)  $\rho_p := E_p P E_p$  is the sub-normalized  
post measurement state  
 $\forall p$ .

(1)  $\forall p \in \mathcal{D}$ ,  $\rho_p$  is an eigenvector of  $P$   
w/ eigenvalue  $p$ .

(2) The prob. of  $\rho$  when measured w.r.t

$$P \text{ is } u[P\rho] = \sum_{p \in \mathcal{D}} u[\rho_p].$$

**Story:** suppose  $|1\rangle = \sum_i \omega_i |1\rangle_i$ . (recall:  $P = \sum_i \lambda_i |1\rangle_i \langle 1|_i$ )

Then, measuring  $|1\rangle$  using  $\Sigma$  yields  $|1\rangle_i$  w.p.  $|\omega_i|^2$ .

### Thm 2.6 (Inefficient threshold measurement).

Let  $P = (P, Q)$  be a binary outcome POVM.

Let  $P$  have eigenbasis  $\{|1\rangle_i\}$  w/ eigenvalues  $\{\lambda_i\}$ .

Then,  $\forall r \in (0, 1) \exists$  a projective measurement

$$\Sigma_r = (E_{\leq r}, E_{>r}) \text{ s.t.}$$

$$(1) E_{\leq r} := \sum_{|\lambda_i - \frac{1}{2}| \leq r} |\psi_i\rangle\langle\psi_i|$$

$$(2) E_{>r} := \sum_{|\lambda_i - \frac{1}{2}| > r} |\psi_i\rangle\langle\psi_i|$$

Similarly,  $\forall r \in (0, \gamma_2)$ ,  $\exists$  projectors  $\tilde{\mathcal{E}}'_r = (\tilde{E}'_{\leq r}, \tilde{E}'_{>r})$  s.t.

$$(1) \tilde{E}_{\leq r} := \sum_{|\lambda_i - \frac{1}{2}| \leq r} |\psi_i\rangle\langle\psi_i|$$

$$(2) \tilde{E}_{>r} := \sum_{|\lambda_i - \frac{1}{2}| > r} |\psi_i\rangle\langle\psi_i|$$

**Me:** Don't know why any of these are called "theorems".

### Efficient Measurement.

**Story:** • The projective measurements  $\mathcal{E}$  above, cannot in general be efficiently computed.

• However, Zhandry [Zha20] shows that when the POVM is a mixture of projective measurements, efficient approximation is possible.

This uses a technique first introduced by Marriott &Watrous [MW05].

base of colored  
A random challenge is sampled,  
the program is evaluated & bisected  
and the output is checked.

may be captured by a bound  $P = (t, \theta)$   
as follows:

$$P = \frac{1}{R} \sum_{i=1}^R \sum_{j=1}^{n_i}$$

projector

base of challenge space.

process of 103 is a "program".

$V_{103}$  a kind of "universal machine" that reads  
the program & and awaiting input  
 $\Pi_1$ , some measurement that checks the output,  
then  $V_1$ , and  $V_2$ .

This is adapted from theorem 6.2 in [EHO 20] &  
Lemma 3 in [ALL 21]

(Efficient Threshold Measurement).

$P_b = (P_b, Q_b)$  be a binary outcome POVM  
on Hilbert space  $H_b$   
that is a mixture of projectors.  
 $\forall b \in \{1, 2\}$

$$P_b = \sum_i \lambda_i^b |v_i^b\rangle\langle v_i^b|.$$

- A situation of interest:

A random challenge  $\alpha$  is sampled,  
The program is evaluated on this input  
and the output is checked.

This may be captured by a POVM  $P = (P, \Omega)$   
as follows:

$$P = \frac{1}{R} \sum_{\alpha} \underbrace{U_{\alpha}}_{\substack{\text{projector} \\ \text{size of challenge space.}}}$$

Me:

I guess if  $|U\rangle$  is a "program",

$V_{\alpha}$  a kind of "universal machine" that reads  
the program & with auxiliary inputs  
set to  $\alpha$

$\Pi_{\alpha}$  some measurement that checks the output,

Then  $U_{\alpha}$  can be  $\Pi_{\alpha} V_{\alpha}$ .

- The following is adapted from Thm 8.2 in [Eha20] &  
Lemma 3 in [ALL+21]

**Thm 2.7 (Efficient Threshold Measurement).**

Let  $P_b = (P_b, Q_b)$  be a binary outcome POVM  
on Hilbert space  $\mathcal{H}_b$   
that is a mixture of projectors.  
 $\# b \in \{1, 2\}$

$$\bullet P_b = \sum_i \lambda_i^{(b)} |\psi_i^{(b)}\rangle\langle\psi_i^{(b)}|.$$

- A situation of interest:

A random challenge  $\alpha$  is sampled,  
The program is evaluated on this input  
and the output is checked.

This may be captured by a POVM  $P = (P_\lambda)$   
as follows:

$$P = \frac{1}{R} \sum_{\lambda} \underbrace{U_\lambda}_{\substack{\text{projector} \\ \text{size of challenge space}}}$$

Me:

I guess  $\psi$  (14) is a "program",

$V_\alpha$  a kind of "universal machine" that reads  
the program & with auxiliary inputs  
set to  $\alpha$

$\Pi_\alpha$  some measurement that checks the output,

Then  $U_\alpha$  can be  $\Pi_\alpha V_\alpha$ .

- The following is adapted from Thm 8.2 in [Eha20] &  
Lemma 3 in [ALL<sup>+</sup>21]

**Thm 2.7 (Efficient Threshold Measurement).**

Let  $\cdot P_b = (P_b, Q_b)$  be a binary outcome POVM  
on Hilbert space  $\mathcal{H}_b$   
that is a mixture of projectors.  
 $\mathbb{N}$  be  $\{1, 2\}$ .

- $P_b = \sum_i \lambda_i^b |\psi_i^b\rangle\langle\psi_i^b|$ .

$$\cdot \quad r_1, r_2 \in (0,1)$$

$$0 < \epsilon < \min\left(\frac{r_1}{2}, \frac{r_2}{2}, 1-r_1, 1-r_2\right)$$

$$\delta > 0$$

be arbitrarily chosen

Then,  $\exists$  efficient binary-outcome quantum algorithms,  
(interpreted as the POVM element corresponding  
to outcome 1)

$$\text{ATI}_{p_b, \gamma}^{\epsilon, \delta} \quad \text{s.t.}$$

+ quantum programs  $\rho \in \mathcal{D}(\mathcal{H}_1) \otimes \mathcal{D}(\mathcal{H}_2)$

the following about the product algorithm

$$\text{ATI}_{p_1 r_1}^{\epsilon, \delta} \otimes \text{ATI}_{p_2 r_2}^{\epsilon, \delta}$$

holds:

(i) Let  $(E_{\leq \gamma}^b, E_{>\gamma}^b)$  be the inefficient threshold measurement in Thm 2.6 for  $\mathcal{H}_b$ .

(ii) The prob. of measuring 1 on  $b$  registers  
satisfies

$$\text{Tr}\left[\left(\text{ATI}_{p_1 r_1}^{\epsilon, \delta} \otimes \text{ATI}_{p_2 r_2}^{\epsilon, \delta}\right)\rho\right] \geq$$

$$\text{Tr}\left[\left(E_{>r_1+\epsilon}^1 \otimes E_{>r_2+\epsilon}^2\right)\rho\right] - 2\delta$$

- (2) The post-measurement state  $\rho'$  after getting outcome  $(1,1)$   
 is  $4\delta$ -close to a state in  
 $\text{span} \{ |14\rangle\langle 14|, |24\rangle\langle 24| \}$  if  $\lambda_1' > r_1 - 2\epsilon$   
 $\lambda_2' > r_2 - 2\epsilon$
- (3) The running time of the algorithm is polynomial in  
 { the running time of  $P_1$ ,  
   "  "   $P_2$ ,  
    $\gamma_\epsilon$ ,  $\log(1/\delta) \}$ .

Intuition: The theorem says — if the quantum state  $\rho$  has weight  $w$  on eigenvectors of  $(P_1, P_2)$  w/ eigenvalues greater than  $(r_1 + \epsilon, r_2 + \epsilon)$  then, the quantum algorithm will produce a post-measurement state (w.p. at least  $w - 2\delta$ ) s.t. it has weight  $1 - 4\delta$  on eigenvectors w/ eigenvalues greater than  $(r_1 - 2\epsilon, r_2 - 2\epsilon)$ .

Story: In this paper, we focus on indistinguishability games — and therefore interested in projective measurements that “project onto” eigenvalues away from  $\gamma_2$  (i.e. doing better than random guessing.)

We therefore use the symmetric version of Theorem 2.7.

Thm 2.8 (Efficient symmetric threshold Measurement).

Let •  $P_b = (P_b, \gamma_b)$   
 •  $P_b = \sum_i \lambda_i^b |4_i^b\rangle\langle 4_i^b|$  be as before.

Let •  $\gamma_1, \gamma_2 \in (0, 1)$   
 •  $0 < \epsilon < \min(\gamma_1/2, \gamma_2/2)$

•  $\delta > 0$

be chosen arbitrarily.

Then,  $\exists$  binary-outcome quantum algorithm  
 (interpreted as the POVM element  
 corresponding to outcome 1),

$SATI_{P_b, \gamma}^{\epsilon, \delta}$  s.t.

•  $\forall \rho \in D(H_1) \otimes D(H_2)$ , the following about

$SATI_{P_1, \gamma_1}^{\epsilon, \delta} \otimes SATI_{P_2, \gamma_2}^{\epsilon, \delta}$  holds:

(1) Let  $(\tilde{E}_{\leq \gamma_b}^b, \tilde{E}_{> \gamma_b}^b)$  be as in Thm 2.6 for  $H_b$ .

(2) The post-measurement state  $\rho'$  after getting (1,1)  
 is  $4\delta$ -close to a state in

$$\text{span} \{ |4_i^1\rangle |4_j^2\rangle \}_{i,j: |\lambda_i^1 - \gamma_1| > \gamma_1 - 2\epsilon, |\lambda_j^2 - \gamma_2| > \gamma_2 - 2\epsilon}$$

(3) The run-time of the algorithm is polynomial in  
 the running time of  $P_1, P_2$  &  
 $\{\gamma_b, \log(\gamma_b)\}$ .

## § 2.5 Uncloneable Encryption

**Story**: In this subsection, we look at the def' of uncloneable encryption as in [AK21]

this is a variant of the original def' in [BL20]  
(where they forced  $m_0, m_1$  to be uniformly random).

; Here,  $m_0, m_1$  are arbitrary.

**Def' 2-9** An uncloneable encryption scheme, is a

triple of algorithms ( $\text{Gen}$ ,  $\text{Enc}$ ,  $\text{Dec}$ ) w/  
the following syntax.

- $\text{Gen}(1^\lambda)$  — on input a security parameter  $1^\lambda$ , return a classical key  $\text{sk}$
- $\text{Enc}(\text{sk}, \text{Im})(\text{ml})$  — on input the key  $\text{sk}$ , & the message  $\text{Im} \in \{0,1\}^{\text{pol}(\lambda)}$ ,  
outputs a quant. ciphertext  $\text{Pct}$
- $\text{Dec}(\text{sk}, \text{Pct})$  — takes as input the key  $\text{sk}$ ,  
outputs a message  $\text{Im}$  as a quantum state

## § 2.5 Uncloneable Encryption

**Story**: In this subsection, we look at the def' of uncloneable encryption as in [AK21]

this is a variant of the original def' in [BL20]  
(where they forced  $m_0, m_1$  to be uniformly random).

: Here,  $m_0, m_1$  are arbitrary.

- Def' 2-9** An uncloneable encryption scheme, is a triple of algorithms  $(\text{Gen}, \text{Enc}, \text{Dec})$  w/ the following syntax.
- $\text{Gen}(\lambda)$  — on input a security parameter  $\lambda$ , return a classical key  $\text{sk}$
  - $\text{Enc}(\text{sk}, \text{Im})(\text{cm})$  — on input the key  $\text{sk}$ , & the message  $\text{Im} \in \mathbb{C}^m$  for  $m \in \{0, 1\}^{\text{poly}(\lambda)}$ , output a quant. ciphertext  $\text{Pct}$
  - $\text{Dec}(\text{sk}, \text{Pct})$  — takes as input the key  $\text{sk}$ , & outputs a message  $\text{Im}$  as a quantum state

It must satisfy the following correctness & unclonability

which are defined as follows:

### Correctness.

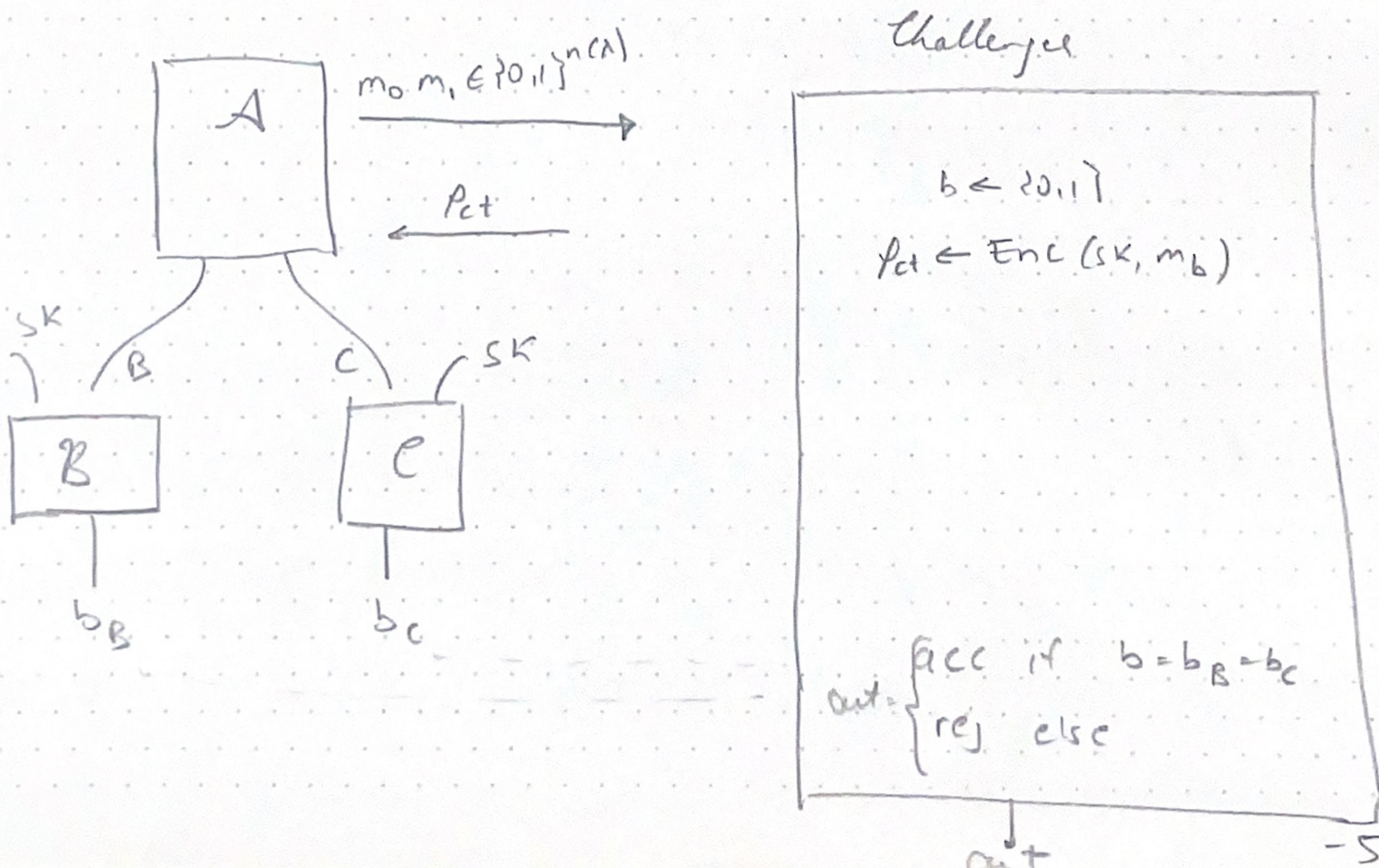
For  $\text{sk} \leftarrow \text{Gen}(1^\lambda)$ ,

$$\Pr[\text{Inv}_\text{cm}(\text{Dec}(\text{sk}, \text{Enc}(\text{sk}, \text{Inv}_\text{cm})))] \geq 1 - \text{negl}(\lambda)$$

### Unclonability. (we focus on uncloneable IND-CPA security)

(Def<sup>n</sup> 2.10 Uncloneable IND-CPA game).

- Let  $\lambda \in \mathbb{N}^+$
- Given an encryption scheme  $S$ , consider the following game against  $(A, B, C)$ .



- what is  $\mathcal{G}$ ?
- Let  $\text{adv}_{\mathcal{G}, \mathcal{A}, \mathcal{B}, \mathcal{C}}(\lambda)$  denote the prob. of winning the game above.
  - The  $\mathcal{S}$  is said to be information theoretically secure (computationally) if for all adversaries  $(\mathcal{G}, \mathcal{A}, \mathcal{B}, \mathcal{C})$  (all efficient)
 
$$\text{adv}_{\mathcal{G}, \mathcal{A}, \mathcal{B}, \mathcal{C}}(\lambda) \leq \frac{1}{2} + \text{negl}(\lambda)$$

### § 3 On the impossibility of Deterministic Schemes

**Story:** Let's define deterministic schemes first.

**Def' 3.1** (Deterministic Scheme). An encryption scheme  $(\text{Gen}, \text{Enc}, \text{Dec})$  is a deterministic enrypt scheme if

- $\text{Enc}$  can be realised as a unitary  $U_{\text{SK}}$  acting on the planted register  $|m\rangle \otimes |a\rangle$  if ancillary bits are init. to  $|0\rangle$ , resulting in a pure ciphertext  $|c_{\text{SK}}\rangle$  of length  $\lambda$ .
- $\text{Dec}$  acts as  $U_{\text{SK}}^{\dagger}$  & then measures in the

- Let  $\text{adv}_{G, A, B, C}(\lambda)$  denote the prob. of winning the game above.  
what is  $G$ ?
- The  $S$  is said to be information theoretically secure (computationally) if for all adversaries  $(G, A, B, C)$   
(all efficient).  
what is  $G$ ?

$$\text{adv}_{G, A, B, C}(\lambda) \leq \frac{1}{2} + \text{negl}(\lambda)$$

### § 3 On The impossibility of Deterministic Schemes

Story: Let's define deterministic schemes first.

**Def' 3.1** (Deterministic Scheme). An encryption scheme  $(\text{Gen}, \text{Enc}, \text{Dec})$  is a deterministic ency' scheme if

- $\text{Enc}$  can be realised as a unitary  $U_{SK}$  acting on the planted register  $|m\rangle$  & auxiliary bits  $a$  init. to  $|0\rangle$ , resulting in a pure ciphertext  $|c_{SK}\rangle$  of length  $\lambda$ .
- $\text{Dec}$  acts as  $U_{SK}^\dagger$  & then measures in the