E

- Let $adv_{\mathcal{G},\mathcal{A},\mathcal{B},\mathcal{C}}(\lambda)$ (what is $\mathcal{G}$?) 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) (what is $\mathcal{G}$?)

$$adv_{\mathcal{G},\mathcal{A},\mathcal{B},\mathcal{C}}(\lambda) \leq \frac{1}{2} + negl(\lambda)$$

§3 On the impossibility of Deterministic Schemes

Story: Let's define deterministic schemes first.

Def^ 3.1 (Deterministic Scheme). An encryption scheme (Gen, Enc, Dec) is a deterministic encryp^ scheme if

- Enc can be realised as a unitary

$$U_{SK}$$

acting on the plaintext register $|m\rangle$ & ancillary bits are init. to $|0\rangle$, resulting in a pure state ciphertext $|C_{SK}\rangle$ of length λ.

- Dec acts as $U_{SK}^{\dagger}$ & then measures in the

computational basis to recover the message.

Story:
- Note that "correctness" holds by def?
- Consider the following two simple examples of deterministic schemes.

e.g. 1
Suppose sk encodes two orthogonal states
$|\phi_0\rangle, |\phi_1\rangle$.
A message b is mapped to $|\phi_b\rangle$.

e.g. 2
The conjugate encryption defined in [BL'20]:
- Gen(1^λ) outputs $sk = (x, \theta)$ where $x, \theta \leftarrow \{0,1\}^\lambda$
(independent, uniformly sampled)
- $Enc(sk, m) = |(m \oplus x)^\theta\rangle\langle(m \oplus x)^\theta|$ where
$|x^\theta\rangle = H^\theta |x\rangle$ is the BB84 state.
- $Dec(\underbrace{sk}_{(x,\theta)}, \rho)$: computes $\rho' = H^\theta \rho H^\theta$,
measures ρ' (standard basis) to obtain c
& returns $c \oplus x = m'$ as the message

: [BL'20] already showed e.g. 2 does not satisfy uniformcalle IND-CPA.

Here, a universal attack is given for any uniformcalle IND-CPA game based on a deterministic encryption scheme.

Theorem 3.2 For any deterministic scheme,

$\exists$ a universal information theoretic adversary (f, A, B, C) that satisfies

$$adv_{f,A,B,C}(\lambda) \geq 0.568 \text{ as } \lambda \to \infty.$$

Story: Deterministic schemes can only offer one-time security

So it is natural to try to extend the impossibility result to schemes that allow Enc to use additional randomness.

$\therefore$ Here's an e.g. of such a scheme,

inspired by [GL '89]. ← Goldreich-Levin

$Gen(1^\lambda)$: returns $sk := (\theta, u)$ for $\theta, u \leftarrow \{0,1\}^\lambda$

$Enc_{sk}(m, r) = |\lambda\theta\rangle \,|\, (\lambda \cdot u) \oplus m\rangle$

for $m \in \{0,1\}$ &

$r \leftarrow \{0,1\}^\lambda$.

$Dec_{sk}(\rho)$: Apply H^θ on the first λ qubits. (to recover r)

$\overset{?}{=} (\theta, u)$

Measure ρ in the computational basis to get $ct \in \{0,1\}^\lambda$.

Return

$$m' = (ct_{1 \ldots \lambda} \cdot u) \oplus ct_{\lambda+1}.$$

$\therefore$ But this proof doesn't extend to such schemes.

Two high-level barriers are

(1) Encryption will produce mixed states as ciphertext.

Action of random unitaries on mixed states is

not well understood

(2) This adversary (A, B, C) relies on all information of the ciphertext state to decide its measurement.

If encryption takes additional randomness as input, then B & C are unable to determine which ciphertext was produced (∵ this additional randomness is not in general available to them)

& thus, the attack don't work.

§ 3.1 Preliminaries on Haar Measure

story: Quick introduction here — see [Wat '18] for more.

Notation: μ_n := The uniform spherical measure on the unit sphere $S((\mathbb{C}^2)^{\otimes n})$.

: η_n := The Haar measure on the unitary group $\mathcal{U}((\mathbb{C}^2)^{\otimes n})$

Re: For the moment, I am thinking of the Haar measure as a "uniform" distribution over the set of unitaries. I'll see if more than this is needed later.

Lemma 3.3 Let f be a function from

$$S(\mathbb{C}^{2\otimes n}) \times S(\mathbb{C}^{2\otimes n}) \to \mathbb{R}.$$

Then, for any two fixed vectors $|\phi_0\rangle, |\phi_1\rangle \in S(\mathbb{C}^{2\otimes n})$ s.t. $\langle\phi_0|\phi_1\rangle = 0$,

it holds that

$$\mathop{\mathbb{E}}_{U\leftarrow\eta_n} f(U|\phi_0\rangle, U|\phi_1\rangle) = \mathop{\mathbb{E}}_{|\psi_0\rangle,|\psi_1\rangle\leftarrow\mu_n,\ \langle\psi_0|\psi_1\rangle=0} f(|\psi_0\rangle, |\psi_1\rangle)$$

Me: The statement sounds quite intuitive to me.
(although why it holds only for orthogonal vectors,
is not clear to me — perhaps it does hold in
general but the proof is not known?)
Unlikely.

It is just saying — take any to fixed orthogonal vectors
rotate them both by the same uniformly sampled
"angle"
this is the same as
sample two orthogonal unit vectors,
on average.

Story: We now introduce "Lévy's lemma"
which is the counterpart of Chernoff bound on
the uniform spherical measure.

Me: I'm neglecting this for now. Will look at Watrous's note later.

Lemma 3.4 (Lévy's Lemma).
Let f be a function from $S(\mathbb{C}^{2^n}) \to \mathbb{R}$ satisfying

$$|f(|\phi\rangle) - f(|\psi\rangle)| \leq K \| |\phi\rangle - |\psi\rangle \|_2$$

for some $K > 0$. (presumably for all $|\psi\rangle, |\phi\rangle \in S(\mathbb{C}^{2^n})$)

Then, $\exists$ a universal constant $\delta > 0$ s.t.

$\forall\ \epsilon > 0$,

$$\Pr_{|\psi\rangle \leftarrow \mu_n}\left[\left| f(|\psi\rangle) - \mathop{\mathbb{E}}_{|\phi\rangle \leftarrow \mu_n} [f(|\phi\rangle)] \right| \geq \epsilon \right] \leq 3e^{-\frac{\delta \epsilon^2 n}{K^2}}$$

Me: Seems to say that if f "preserves" inner products up to a "factor of K",
then the prob. that f is ϵ-far from its expected value (when the input is uniformly sampled), decays exponentially

A Chernoff-like statement.

Recall: Chernoff usually gives stronger (exponential decay) bounds than Markov etc

Story: The following theorem is from [MZB '16] & plays a crucial role here.

Theorem 3.5 Let $|\psi_1\rangle, |\psi_2\rangle \in \mathcal{S}(\mathbb{C}^{2^{\otimes 2n}})$ be independently sampled from μ_{2n}.

- ρ_1 ρ_2 denote the corresponding density matrices in the first n qubit registers.

As $n \to \infty$, the $TD(\rho_1, \rho_2)$ almost surely converges to $\frac{1}{4} + \frac{1}{\pi}$,

i.e. $TD(\rho_1, \rho_2) \xrightarrow{a.s.} \frac{1}{4} + \frac{1}{\pi} \approx 0.568$.

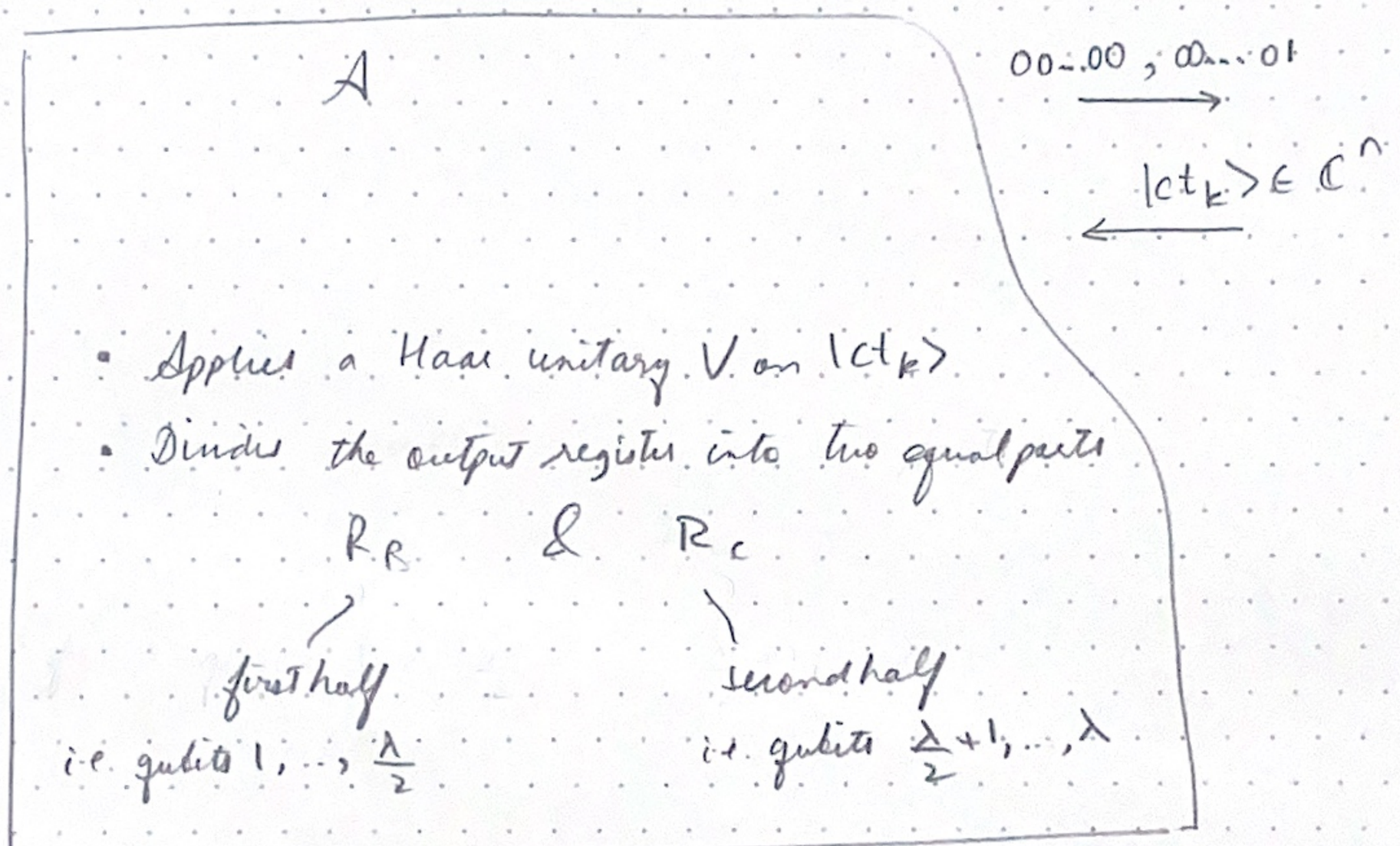
Notation: $\mathbb{E}_{|\psi\rangle}$ denotes expectation over $|\psi\rangle$ sampled from uniform spherical measure (on the corresponding Hilbert space)

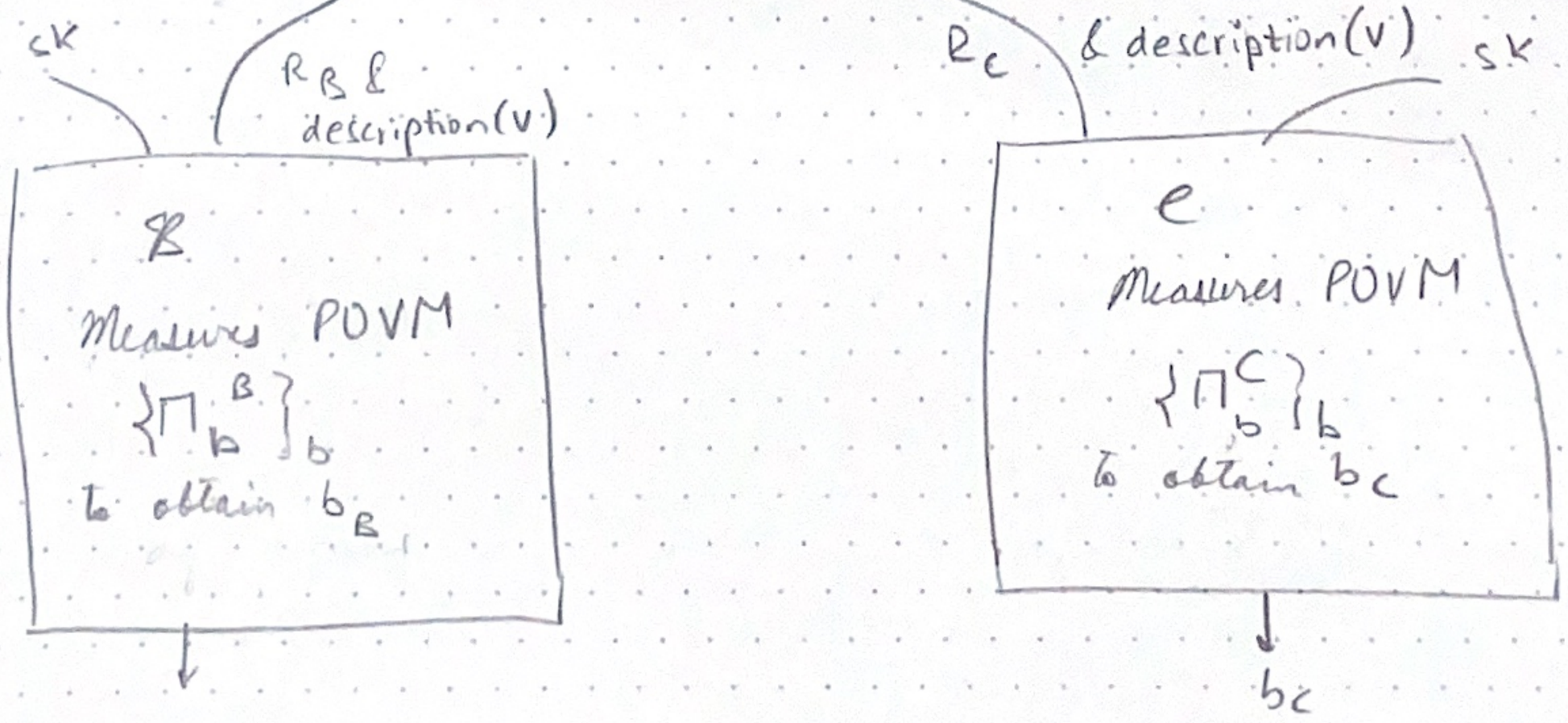
$\mathbb{E}_V$ denotes expectation over V sampled from the Haar measure.

§3.2 Attack Schemes

Story: We have all the pieces in place.
We can now describe the attack,
where no bounds are assumed on the
attacker, i.e. this is for information theoretic security.

Attack:





where $\{\Pi_b^B\}_b$ & $\{\Pi_b^C\}_b$ are obtained by solving an optimization problem, defined shortly.

story: • The success prob. of this attack is the same as that of the following game.

• description(V) is done using an "ϵ-net". This is OK because we get const. security in the end; ϵ can be chosen small enough.

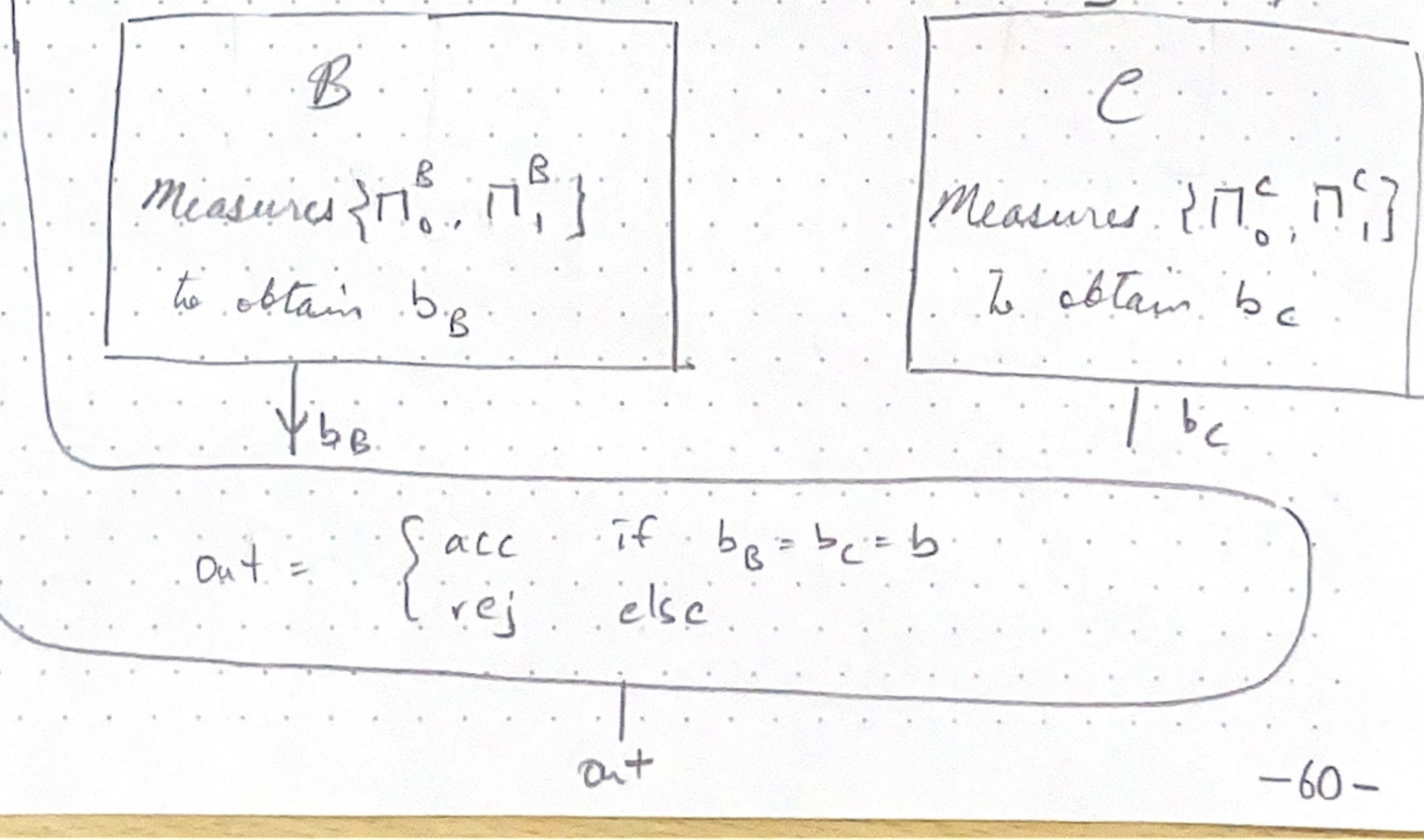
Definition 3.6

Let $\lambda \in \mathbb{N}^+$.

Consider the following game b/w a Challenger & an (unbounded) adversary $(\mathcal{B}, \mathcal{C})$.

Challenger

- $|\phi_0\rangle, |\phi_1\rangle$ are two independent "Haar random states", s.t. $\langle\phi_0|\phi_1\rangle = 0$
  (i.e. $|\phi_0\rangle, |\phi_1\rangle \leftarrow \mu_n$ s.t. $\langle\phi_0|\phi_1\rangle = 0$)
- samples $b \leftarrow \{0,1\}$
  divides $|\phi_b\rangle$ into two parts,
  - R_B are registers indexed from $\{1, \ldots \frac{\lambda}{2}\}$
  - R_C " " $\{\frac{\lambda}{2}+1, \ldots \lambda\}$
- $\text{desc}_{\phi_0\phi_1} := (\text{description}(|\phi_0\rangle), \text{description}(|\phi_1\rangle))$



Me: What is the difference b/w this &
the attack we described on encloneable-IND-CPA?

(a) $desc_{\phi_0\phi_1}$ instead of $desc(V)$

(b) no "sk" instead of sk being given to B & C

I suppose the point is that either

$U_{sk}|m_0\rangle|0\rangle$ is sent or

$U_{sk}|m_1\rangle|0\rangle$ is sent

by the challenger in the original game.

In the original attack, V was applied &

$VU_{sk}|m_b\rangle|0\rangle$ was split & sent

to B, C together w/ $desc(U)$ &

the sk

In Def^ 3.4, of two (Haar random) orthogonal vectors $|\phi_0\rangle, |\phi_1\rangle$

$|\phi_b\rangle$ is split & sent,

together w/ $desc_{\phi_0\phi_1}$

So the BC in Def^ 3.4 can do

everything BC in the original scheme can

∵ essentially, from $desc_{\phi_0\phi_1}$,

they can find a V & an sk s.t.

$desc(V U_{sk}|m_b\rangle) = desc(|\phi_b\rangle)$

And the other way, BC in the original scheme

can compute $desc(|\phi_b\rangle) = desc(V U_{sk}|m_b\rangle)$

& proceed to do whatever BC in Def^ 3.4 do.

Plus, the "distributions" are identical.

So these are indeed equivalent in terms of winning prob

story: We haven't yet said how the measurements are chosen.
Let's simply optimize over them &
try to lower bound the success prob.

NB: The success prob. of the game in Def° 3.6, in terms of $|\phi_0\rangle$ & $|\phi_1\rangle$
can be written as follows:

$$G(|\phi_0\rangle,|\phi_1\rangle) := \max_{\substack{\Pi_0^B \Pi_1^B \\ \Pi_0^C \Pi_1^C}} \frac{1}{2}\left(\langle\phi_0|\Pi_0^B\otimes\Pi_0^C|\phi_0\rangle + \langle\phi_1|\Pi_1^B\otimes\Pi_1^C|\phi_1\rangle\right)$$

$$\text{s.t.} \quad \Pi_0^B + \Pi_1^B = \mathbb{1} \quad (\text{on } \lambda/2 \text{ qubits})$$
$$\Pi_0^C + \Pi_1^C = \mathbb{1}$$
$$0 \le \Pi_i^B \quad \forall i \in \{0,1\}$$
$$0 \le \Pi_i^C \quad \forall i \in \{0,1\}$$

NB 2: The success prob of the game in Def° 3.6 is

$$\Pr(BC_{win}) = \mathop{\mathbb{E}}_{|\phi_0\rangle,|\phi_1\rangle \leftarrow \mu_n \,:\, \langle\phi_0|\phi_1\rangle = 0} G(|\phi_0\rangle,|\phi_1\rangle) \qquad [*]$$

NB 3: It is not hard to see, as explained in "Me"
that the success prob of the attack in
the unclonable IND-CPA game is

$$\mathop{\mathbb{E}}_{SK}\mathop{\mathbb{E}}_{V} G(V U_{SK}|0\ldots00\rangle, V U_{SK}|0\ldots01\rangle) \qquad [**]$$

NB 4: $[*] = [**]$ using Lemma 3.3.

Story: We now lower bound [*] as follows.

Notation: $\{\Pi^B_b\}_b$ & $\{\Pi^C_b\}_b$ are referred to as $\{\Pi^B\}$ & $\{\Pi^C\}$ for brevity.

NB: $\Pr(BC \text{ win} \mid |\phi_0\rangle|\phi_1\rangle)$

$$= \max_{\{\Pi^B\}\{\Pi^C\}} \Pr\left[(b_B = b) \wedge (b_C = b) \;\middle|\; \{\Pi^B\}\{\Pi^C\}\, |\phi_0\rangle|\phi_1\rangle \right]$$

$$\geq 1 - \min_{\{\Pi^B\}} \Pr\left[b_B \neq b \mid \{\Pi^B\}\, |\phi_0\rangle|\phi_1\rangle \right] - \min_{\{\Pi^C\}} \Pr\left[b_C \neq b \mid \{\Pi^C\}\, |\phi_0\rangle|\phi_1\rangle \right]$$

(using a union bound: $\Pr[A \wedge B] \geq 1 - \Pr[A] - \Pr[B]$)

$$= 1 - \frac{1}{2}\left(1 - TD(\rho_0^B, \rho_1^B)\right) - \frac{1}{2}\left(1 - TD(\rho_0^C, \rho_1^C)\right)$$

(left half of $|\phi_0\rangle, |\phi_1\rangle$ resp. ; right half of $|\phi_0\rangle, |\phi_1\rangle$ resp.)

(N.B: $p_{guess} = \frac{1}{2}\left(1 + tr\left(\Pi^B(\rho_0^B - \rho_1^B)\right)\right)$

$$p_{guess\,wrong} = \frac{1}{2}\left(1 - tr\left(\Pi^B(\rho_0^B - \rho_1^B)\right)\right)$$

$$p^{min}_{guess\,wrong} = \frac{1}{2}\left(1 + \min_{\Pi^B}\left(-tr\left(\Pi^B(\rho_0^B - \rho_1^B)\right)\right)\right.$$

$$= \frac{1}{2}\left(1 - \max_{\Pi^B} tr\left(\Pi^B(\rho_0^B - \rho_1^B)\right)\right)$$

$$\left. = \frac{1}{2}\left(1 - TD(\rho_0^B, \rho_1^B)\right)\right)$$

(recall: $TD(\rho_0, \rho_1) = \frac{1}{2}tr|\rho_0 - \rho_1| = \max_{1 \geq \Pi \geq 0} tr[\Pi(\rho_0 - \rho_1)]$)

$$= \frac{1}{2}\left(TD(\rho_0^B, \rho_1^B) + TD(\rho_0^C, \rho_1^C)\right)$$

Story: We now take expectation over $|\phi_0\rangle$ $|\phi_1\rangle$ to get $\Pr(BC \text{ win})$ as follows:

NB: $$\Pr((B,C) \text{ win}) = \mathop{\mathbb{E}}_{|\phi_0\rangle, |\phi_1\rangle \leftarrow \mu_n, \langle\phi_0|\phi_1\rangle = 0} \Pr\left[(B,C) \text{ win} \mid |\phi_0\rangle, |\phi_1\rangle\right]$$

$$\geq \mathop{\mathbb{E}}_{|\phi_0\rangle, |\phi_1\rangle \leftarrow \mu_n, \langle\phi_0|\phi_1\rangle = 0} \frac{1}{2}\left(TD(\rho_0^B, \rho_1^B) + TD(\rho_0^C, \rho_1^C)\right)$$

(using "NB" above)

$$[*] \quad \geq \mathop{\mathbb{E}}_{|\phi_0\rangle\,|\phi_1\rangle \leftarrow \mu_n} \frac{1}{2}\left(TD(\rho_0^B \rho_1^B) + TD(\rho_0^C \rho_1^C)\right) - \mathrm{negl}(\lambda)$$

(uses the concentration property of the Haar measure; proved shortly)

$$\geq \frac{1}{4} + \frac{1}{\pi} - \epsilon \geq 0.568 \qquad \text{for } \lambda \to \infty$$

(uses Theorem 3.5).

Story: Taking step [*] on faith, we have proved Theorem 3.2, i.e. deterministic schemes can be attacked (using "unbound" provers) in exp'd time.

It remains to show [*] holds — which we establish below.

NB: For an arbitrary $|\phi_1\rangle$, given $|\phi_0\rangle$, one can write

$$|\phi_1\rangle = \alpha|\phi_0\rangle + \sqrt{1-|\alpha|^2}\,|\phi_0^\perp\rangle$$

(phase absorbed)

where $\alpha = \langle\phi_0|\phi_1\rangle$ & $\langle\phi_0|\phi_0^\perp\rangle = 0$.

∴ By symmetry, we have that

$$\mathop{\mathbb{E}}_{|\phi_1\rangle \leftarrow \mu_n}\left(|\alpha|^2\right) = \frac{1}{2^\lambda}$$

$$\left(\because \sum_i |\alpha_i|^2 = 1 \Rightarrow \mathbb{E}\sum_i |\alpha_i|^2 = 1 \right.$$

$$\Rightarrow \sum_i \left(\mathbb{E}\,|\alpha_i|^2\right) = 1$$

$$\left. \& \text{ by symmetry } \mathbb{E}\,|\alpha_i|^2 = \mathbb{E}\,|\alpha_j|^2 \;\forall\, i,j\right.$$

where α_i are the components along $\{|\phi_0^\perp\rangle, |\phi_0\rangle, \ldots\}$ (* arbitrary but fixed vector s.t. the set is an orthonormal basis).

: Taking $\epsilon = \lambda 2^{-\frac{\lambda}{2}}$

$K = 2$

$f(|\psi\rangle) = |\langle\psi|\phi_0\rangle|^2$ in Lemma 3.4,

one can write down

$$\Pr_{|\phi_1\rangle \leftarrow M_n}\left[\left||\alpha|^2 - \frac{1}{2^\lambda}\right| \geq \frac{\lambda}{2^{\lambda/2}}\right] \leq \underbrace{3e^{-\frac{\delta\lambda^2}{4}}}_{\text{TODO: check.}}$$

or $M_{\frac{\Delta}{2}}$ maybe

: One can therefore derive that

$$\mathop{\mathbb{E}}_{|\phi_1\rangle \leftarrow M_n}[|\alpha|] \leq \underbrace{3\exp\left(-\frac{\delta\lambda^2}{4}\right)}_{= \text{negl}(\lambda)} \cdot 1 + 1 \cdot \frac{\sqrt{\lambda}+1}{2^{\lambda/4}}$$

$\Pr$ that $|\alpha|^2 > \frac{1}{2^\lambda}$ the contribution is still at most 1

the remaing prob is at most 1

given $|\alpha|^2 < \frac{\lambda}{2^{\lambda/2}} + \frac{1}{2^\lambda}$

$$\Rightarrow |\alpha| \leq \sqrt{\frac{\lambda}{2^{\lambda/2}} + \frac{1}{2^\lambda}}$$

$$\leq \sqrt{\frac{\lambda}{2^{\lambda/2}}} + \sqrt{\frac{1}{2^\lambda}}$$

NB 2 : $\mathop{\mathbb{E}}_{|\phi_0\rangle,|\phi_1\rangle} TD(\rho_0^B, \rho_1^B)$ where $\rho_b = \text{tr}_C |\phi_b\rangle\langle\phi_b|^{BC}$ $b \in \{0,1\}$

$$= \mathop{\mathbb{E}}_{|\phi_0\rangle|\phi_1\rangle} \left\| u_C[|\phi_0\rangle\langle\phi_0| - |\phi_1\rangle\langle\phi_1|] \right\|_1$$ by def^n of ρ_b.

(expand $|\phi_1\rangle = a|\phi_0\rangle + \sqrt{1-|a|^2}\,|\phi_0^\perp\rangle$ & substitute to get)

$$= \mathop{\mathbb{E}}_{\substack{|\phi_0\rangle\ |\phi_0^\perp\rangle \\ \langle\phi_0|\phi_1\rangle=0 \\ a}} \left[\frac{1}{2} \left\| \mathrm{tr}_C \left[(1-|a|^2)\left(|\phi_0\rangle\langle\phi_0| - |\phi_0^\perp\rangle\langle\phi_0^\perp|\right) - \right.\right.\right.$$
$$\left.\left.\left. \sqrt{1-|a|^2}\left(a|\phi_0\rangle\langle\phi_0^\perp| + a^*|\phi_0^\perp\rangle\langle\phi_0|\right) \right\|_1 \right]$$

(Me: TODO: check why it is ok to sample $|\phi_0^\perp\rangle \leftarrow \mu_a$ as well.)

$$\leq \mathop{\mathbb{E}}_{\substack{|\phi_0\rangle, |\phi_0^\perp\rangle \\ \langle\phi_0|\phi_0^\perp\rangle=0}} \left[\frac{1}{2} \left\| \mathrm{tr}_C \left[|\phi_0\rangle\langle\phi_0| - |\phi_0^\perp\rangle\langle\phi_0^\perp| \right] \right\|_1 \right] + \underbrace{\mathop{\mathbb{E}}_{a} [|a|]}_{\leq \Lambda}$$

(using the triangle inequality & neglecting smaller terms)

$$\leq \mathop{\mathbb{E}}_{\substack{|\phi_0\rangle, |\phi_1\rangle \\ \langle\phi_0|\phi_1\rangle=0}} \left[\frac{1}{2} \left\| \mathrm{tr}_C \left[|\phi_0\rangle\langle\phi_0| - |\phi_1\rangle\langle\phi_1| \right] \right\|_1 \right] + \overbrace{\mathrm{negl}(\lambda)}$$

(variable renamed)

$$\leq \mathop{\mathbb{E}}_{\substack{|\phi_0\rangle, |\phi_1\rangle \\ \langle\phi_0|\phi_1\rangle=0}} TD(\rho_0^R, \rho_1^R)$$

this establishes [*] on page 64.

(and proceeding similarly for $\rho_0^C \rho_1^C$)