§2.3 Quantum Rewinding.

Story: The following from Watrous's famous paper [Wat'06] will be used here.

(I'll look into the proof later.)

Lemma 2.4 Let • Q be a quantum circuit w/
input: n-qubit register
output: b a classical bit
m-qubit register

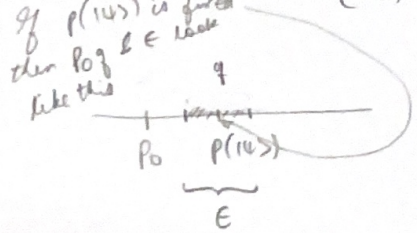
• $p(|\psi\rangle)$:= Prob that $b=0$ when executing Q on $|\psi\rangle$.
($|\psi\rangle$: n-qubit state)

• $p_0, q \in (0,1)$ &
$\epsilon \in (0, 1/2)$ be c.t.

(i) $\forall$ $|\psi\rangle$ (n-qubit), $p_0 \le p(|\psi\rangle)$

(ii) $\forall$ $|\psi\rangle$, $|p(|\psi\rangle) - q| < \epsilon$

(iii) $p_0(1-p_0) \le q(1-q)$



Then,

there is a quantum circuit $\hat{Q}$ of size $O\left(\frac{\log(1/\epsilon)}{4 \cdot p_0(1-p_0)}\right)$ w/

input: n-qubit state

output: m qubit state s.t.

the following holds:

Let: $Q_0(|\psi\rangle)$ be the output of Q on $|\psi\rangle$, conditioned on $b=0$.

: $\hat{Q}(|\psi\rangle)$ be the output of $\hat{Q}$ on $|\psi\rangle$.

Then, $\forall$ $\overbrace{|\psi\rangle}^{n\text{-qubit}}$

$$TD\left(Q_0(|\psi\rangle), \hat{Q}(|\psi\rangle)\right) \leq 4 \frac{\sqrt{\epsilon}\log(1/\epsilon)}{p_0(1-p_0)}$$

Re: q only appears in (iii) to restrict p_0:

not in the final TD expression

Then,

there is a quantum circuit $\hat{Q}$ of size $O\left(\frac{\log(1/\epsilon)}{4 \cdot p_0(1-p_0)}\right)$ w/

input: n-qubit state

output: m qubit state $\quad c+$

The following holds:

Let: $Q_0(|\psi\rangle)$ be the output of Q on $|\psi\rangle$, conditioned on $b=0$.

: $\hat{Q}(|\psi\rangle)$ be the output of $\hat{Q}$ on $|\psi\rangle$.

Then, $\forall$ $\overbrace{|\psi\rangle}^{n\text{-qubit}}$

$$TD\left(Q_0(|\psi\rangle), \hat{Q}(|\psi\rangle)\right) \leq 4 \frac{\sqrt{\epsilon}\,\log(1/\epsilon)}{p_0(1-p_0)}$$

Re: q only appears in (iii) to restrict p_0:

not in the final TD expression

§ 3 Main Theorem

Theorem: Let (i) $\{Z_\lambda(\cdot,\cdot,\cdot)\}_{\lambda\in\mathbb{N}}$ be a quantum operation w/ three arguments:

- a λ-bit string θ
- a bit b'
- a λ-qubit register A

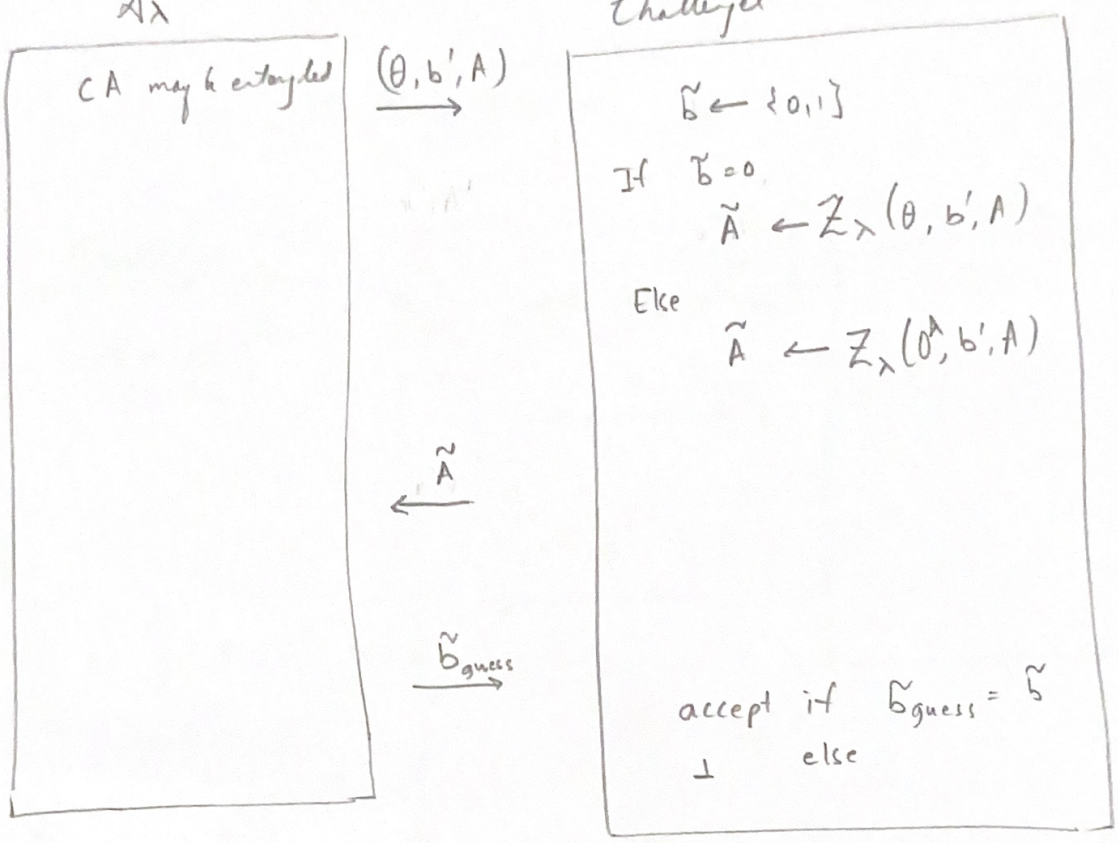
(ii) $\{\mathcal{A}_\lambda\}_{\lambda\in\mathbb{N}}$ be a class of adversaries s.t.

$\forall$ $\theta\in\{0,1\}^\lambda$
$b'\in\{0,1\}$ &
$|\psi\rangle \in A\otimes C$ arbitrary.

$$\left| Pr\left[\underbrace{\mathcal{A}_\lambda}_{\text{its output is parsed as } (x',A')}\left(Z_\lambda(\theta,b',A),C\right)=1\right] - Pr\left[\mathcal{A}_\lambda\left(Z_\lambda(0^\lambda,b',A),C\right)=1\right]\right| \leq negl(\lambda)$$

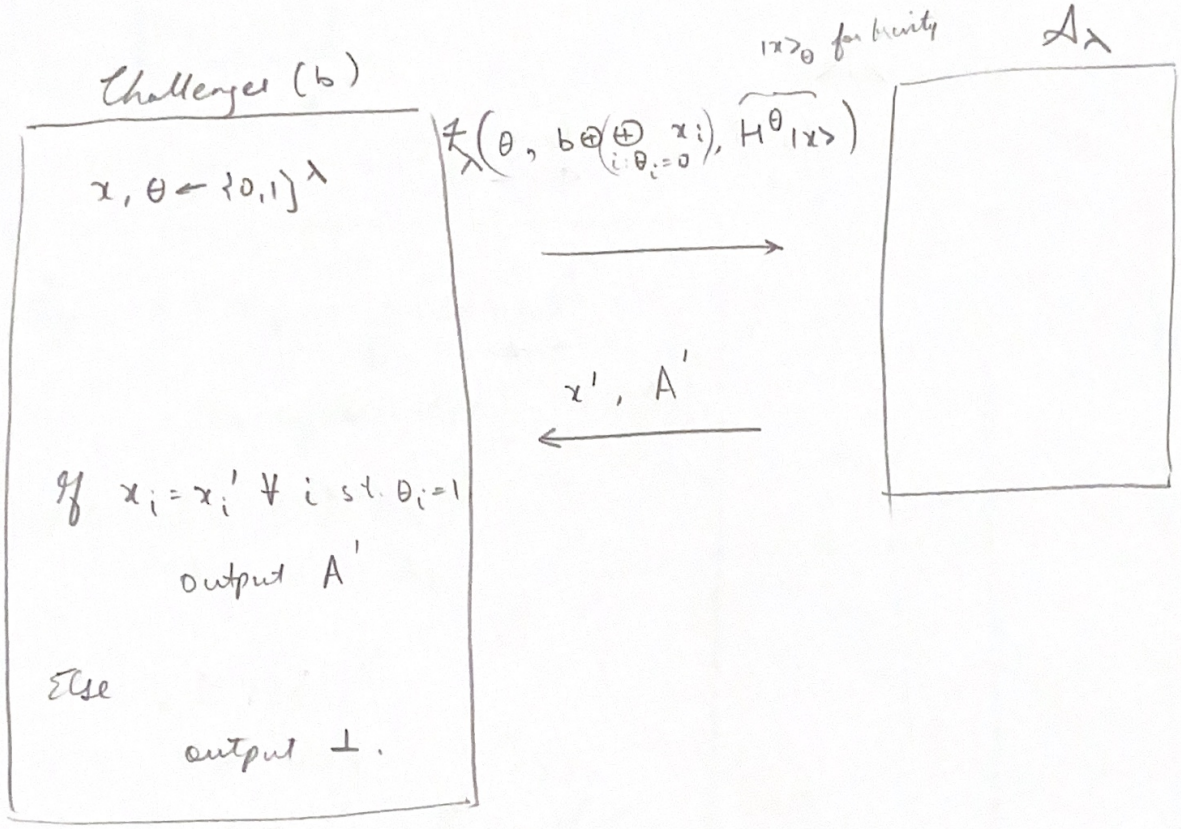
(i.e. Z_λ is semantically secure against $\mathcal{A}_\lambda$ wrt the first input)

Story 4 It is useful to view the "semantic security" as a game, for Claim 3.4 later.



$P_\lambda[\text{Challenger Accepts}] \leq \text{negl}(\lambda)$.

(iii) For any $\{A_\lambda\}_{\lambda\in\mathbb{N}}$, consider the distribution $\{\tilde{Z}_\lambda^{A_\lambda}(b)\}_{\lambda\in\mathbb{N},b\in\{0,1\}}$ produced by the following process.



Then, it holds that $TD(\tilde{Z}_\lambda^{A_\lambda}(0), \tilde{Z}_\lambda^{A_\lambda}(1)) = \mathrm{negl}(\lambda)$.

Remark: The theorem above holds even when x, θ are $\omega(\log\lambda)$ bits long.

Me. So one doesn't need too many additional qubits to perform deletion

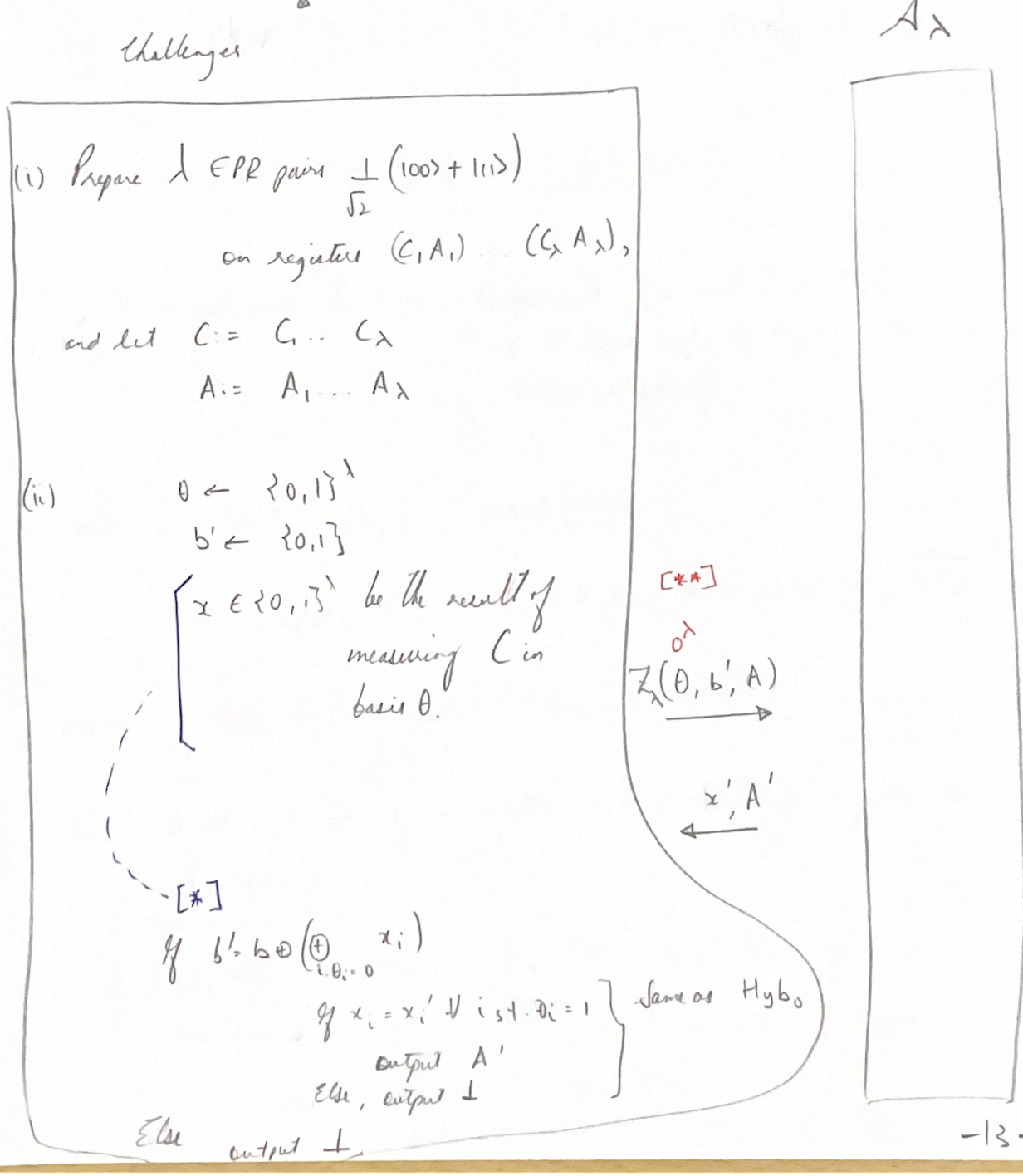
Proof

Story: We define a sequence of hybrids as follows:

$\text{Hyb}_0(b)$: The same as distribution $\{\tilde{Z}_\lambda^{A_\lambda}(b)\}_{\lambda\in\mathbb{N}}$ above.

$\text{Hyb}_1(b)$:

Challenger



$\boxed{Hyb_2(b)}$ The same as $Hyb_1(b)$ except that the measurement to obtain x, is performed after the Adversary's response is received (at [*])

Story. It would be useful to define the distance b/w $Hyb_i(0)$ & $Hyb_i(1)$, i.e. the distinguishing advantage of Hyb_i as follows.

Def^: $Adv_t(Hyb_i) := TD(Hyb_i(0), Hyb_i(1))$

NB1: $Adv_t(Hyb_1) \geq \frac{Adv_t(Hyb_0)}{2}$.

Γ: A distinguisher for Hyb_0, also distinguish Hyb_1 w.p. at least $1/2$
: w.p. at least half, the two, i.e. Hyb_0 & Hyb_1, behave identically.

$\lfloor$

NB2: $Adv_t(Hyb_2) = Adv_t(Hyb_1)$

register C is distinct from the register A_λ acts on.

Goal: Show that $Adv_t(Hyb_2) = negl(\lambda)$.

Story: To this end, we define another hybrid that uses a junk string 0^λ instead of 0

$\boxed{Hyb_2'(b):}$ Same as $Hyb_2(b)$ except that A_λ is given $(0^\lambda, b', A)$ as input (at [**]) (instead of $(0, b', A)$)

Story: We introduce some notation, to analyse $Hyb'_2(b)$.

Notation: Consider Register C immediately after receiving (x', A') from $A_\lambda(b$

(for any $b \in \{0,1\}$)

: For any $\theta \in \{0,1\}^\lambda$,

$$\theta_0 := \{i : \theta_i = 0\}$$
$$\theta_1 := \{i : \theta_i = 1\}$$

: $$\Pi_{x',\theta} := \left(H^{\otimes|\theta_1|}\,|x'_{\theta_1}\rangle\langle x'_{\theta_1}|\,H^{\otimes|\theta_1|}\right)^{C_{\theta_1}} \otimes \sum_{y \in \{0,1\}^{|\theta_0|} \text{ s.t. } \Delta(y, x'_{\theta_0}) \geq \frac{1}{2}} \left(H^{\otimes|\theta_0|}\,|y\rangle\langle y|\,H^{\otimes|\theta_0|}\right)^{C_{\theta_0}}$$

where, recall $\Delta(\cdot,\cdot)$ denotes relative Hamming distance.

Story: To make sure the notation is clear:

Suppose: $\theta = 000111$. Then

$$\theta_0 = \{1,2,3\}$$
$$\theta_1 = \{4,5,6\}$$

: $x' = \underbrace{101}_{x'_{\theta_0}}\underbrace{011}_{x'_{\theta_1}}$

Then: $\Pi_{x',\theta} = \left(H^{\otimes 3}\,|011\rangle\langle 011|\,H^{\otimes 3}\right)^{C_{\theta_1}} \otimes \sum_{y \in \{0,1\}^3 \atop \Delta(y, x'_{\theta_0}) \geq 1/2} \left(H^{\otimes 3}\,|y\rangle\langle y|\,H^{\otimes 3}\right)$

: The measurement is basically checking that

(a) after measuring the C register, wherever θ was 0, in the Hadamard basis, the result is indeed what A_λ reported in x', and given this

(b) the state in the remaining part of C, when measured in Hadamard, returns a y s.t. $\Delta(y, x'_{\theta_0}) \geq 1/2$

Notation (cont.)

: $\Pr\left[\Pi_{x',\theta}, \mathrm{Hyb}_2'(b)\right]$:= Probability that measuring

$\left\{\underbrace{\Pi_{x',\theta}}_{\text{"accepts"}}, \underbrace{\mathbb{1} - \Pi_{x',\theta}}_{\text{"rejects"}}\right\}$ results in

accepts in $\mathrm{Hyb}_2'(b)$.

Claim 3.3 For any $b \in \{0,1\}$,

$$\Pr\left[\Pi_{x'\theta}, \mathrm{Hyb}_2'(b)\right] \leq \mathrm{negl}(\lambda)$$

Proof:

Suppose: $\mathrm{Hyb}_2'(b)$ is executed until $\mathcal{A}_\lambda$ outputs x' & registers A!

NB: A' may be entangled w/ register C.

NB2: One can sample $\theta \leftarrow \{0,1\}^\lambda$ independent of $\mathcal{A}_\lambda$'s actions

(∵ in Hyb_2', θ is never sent to $\mathcal{A}_\lambda$).

NB3: $\Pi_{x',\theta}$ is diagonal in the Hadamard basis.

Suppose: x' & θ are sampled as above.

y is the result of measuring register C in the Hadamard basis.

Then: $$\Pr\left[\Pi_{x'\theta}, \mathrm{Hyb}_2'(b)\right] = \Pr_{x',\theta,y}\left[y_{\theta_1} = x'_{\theta_1} \wedge \Delta(y_{\theta_0}, x'_{\theta_0}) \geq 1/2\right]$$

Sub Claim: (BF10, Appendix B.3) For any fixed x', this probability can be bounded using standard Hoeffding inequalities, as $4e^{-\frac{\Delta(1/2)^2}{32}} = \mathrm{negl}(\lambda)$

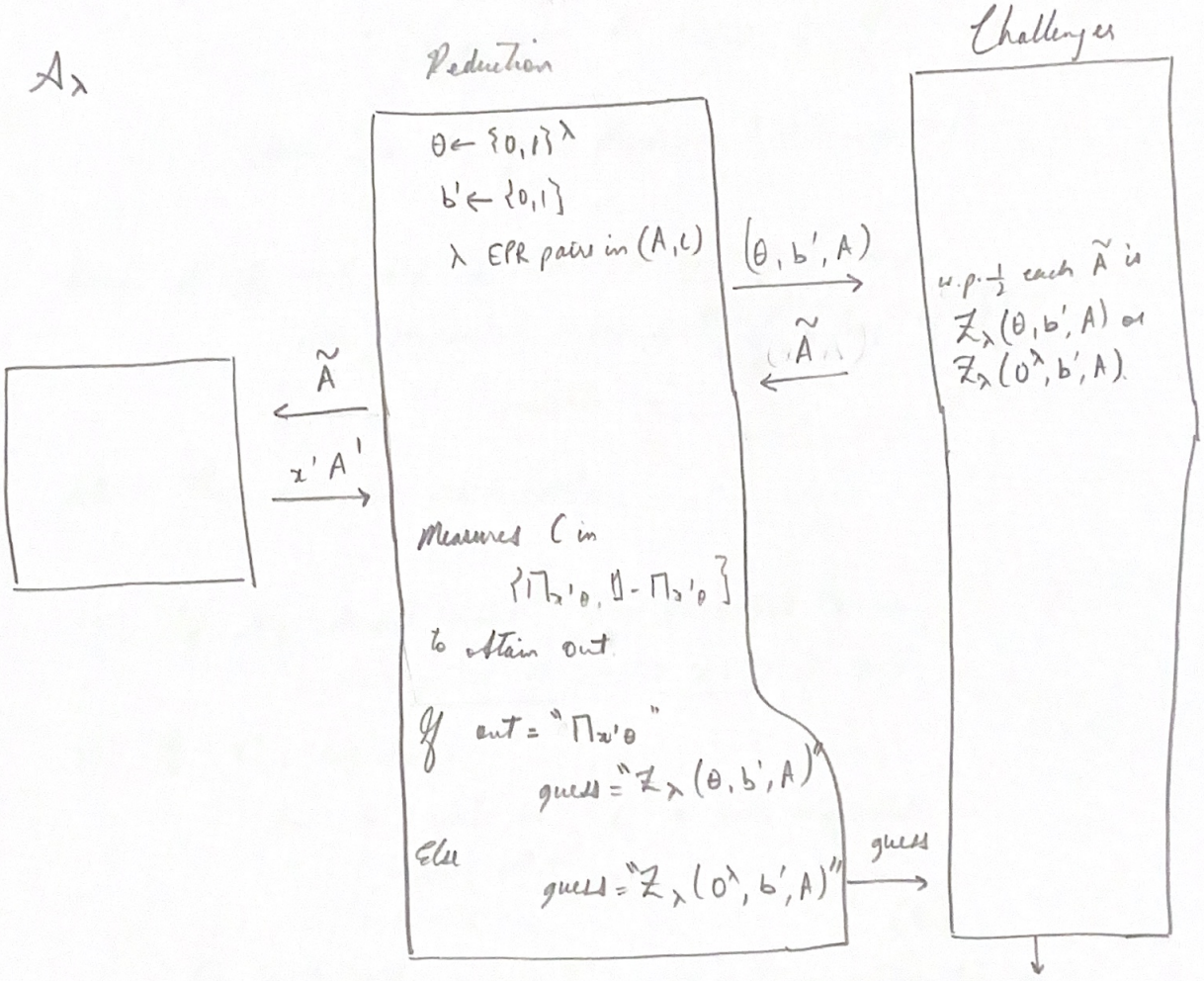
(Story: Basically saying even if you hold a purification of C, you cannot send me a string s.t. when I measure C in Hadamard, on a random subset C_{θ_1} it matches but on the rest, i.e. C_{θ_2}, it differs on at least half places)

□

Notation: $\Pr[\Pi_{x'\theta}, Hyb_2(b)]$ denotes the corresponding event in $Hyb_2(b)$.

Claim 3.4. For any $b \in \{0,1\}$, $\Pr[\Pi_{x'\theta}, Hyb_2(b)] = negl(\lambda)$.

Proof. Story follows by a direct reduction to the symantic security of $\{Z_\lambda\}_\lambda$ (wrt the first input)



If $\Pr[\Pi_{x'\theta}, Hyb_2(b)]$ were non-negligible,
the reduction would succeed w/ non-negligible prob.
at making Challenger accept (using Claim 3.3) □

Story. We have all the pieces in place now to complete the proof.

Claim 3.5. $\mathsf{Adv}_{\mathcal{A}}(\mathsf{Hyb}_2) = \mathsf{ncgl}(\lambda)$

Proof.

NB: For any $b \in \{0,1\}$,
the global state of $\mathsf{Hyb}_2(b)$ immediately after $\mathcal{A}_\lambda$ outputs x',
is within negligible trace distance of a state (call it)
$\tau_{\text{Ideal}}^{C,\mathcal{A}'}$ in the image of $\mathbb{1} - \Pi_{x';\theta}$ [*]

$\because$ Claim 3.4 & Gentle Measurement (Lemma 2.1)

Story: At the next step, the challenger (in Hyb_2) checks whether Hadamard measurement of C_{θ_1} of $\tau_{\text{Ideal}}^{C\mathcal{A}'}$ matches x'_{θ_1}.

NB: There are two possibilities.

(i) If x'_{θ_1} doesn't match, Then the output is $\perp$ irrespective of whether $b=0$ or $b=1$.

(ii) If x'_{θ_1} does match,
then the state on C_{θ_0} is only supported on
$\mathrm{span}\{H^{\otimes|\theta_0|}|y\rangle\}$.
$y : \Delta(y, x'_{\theta_0}) < n/2$ $\because$ [*]

The Challenger then measures these qubits in the computational basis to obtain $\{x_i\}_{i:\theta_i=0}$.

If $\bigoplus_{i:\theta_i=0} x_i \neq b' \oplus b$ outputs $\perp$

Else outputs $\mathcal{A}'$

NB: This is the only step that depends on b.

NB2: Imported Theorem 2.2

↓ (explained in a bit)

$\bigoplus_{i:\theta_i=0} x_i$ is uniformly random and independent of A'

(important: d_2 can b & this A' is the residual state so could potentially be correlated w/ b & then the output when $b=0$ & $b=1$ may be different)

Thus, the output of the challenger (in case (ii)) is also distributed identically, irrespective of whether $b=0$ or $b=1$.

To see this,

recall: Imported Theorem 2.2 says

making a Hadamard basis measurement of a register which is in an equal superposition of computational basis vectors w/ relative Hamming weight $< \frac{1}{2}$

will produce a set of bits $\{x_i\}_{i:\theta_i=0}$ s.t. $\bigoplus_{i:\theta_i=0} x_i$ is uniform, even given quantum side information.

To apply in our case:

- We apply this to C_{D_0}, A' registers.
-