~~Attempt~~

Instantiating [BL20] using Coset States.

Story: • Given the basics ~~ab~~ above, (with using weirder states),

it may be worth exploring other states,

possessing some forms of uncloneability.

• One candidate is the so-called "coset states"

proposed first by Vidick & Zhang [VZ21]

in the context of proofs of quantum knowledge

&

later studied by Coladangelo, Liu, Liu & Zhandry [CLLZ'21]

for copy-protection schemes.

「Recall/Review: Coset States:

Specified by three parameters

(a) a subspace $A \subseteq \mathbb{F}_2^\lambda$ of dimension $\lambda/2$, &

(b) two vectors $s, s' \in \mathbb{F}_2^\lambda$

The states are specified using the cosets

$A + s$ &

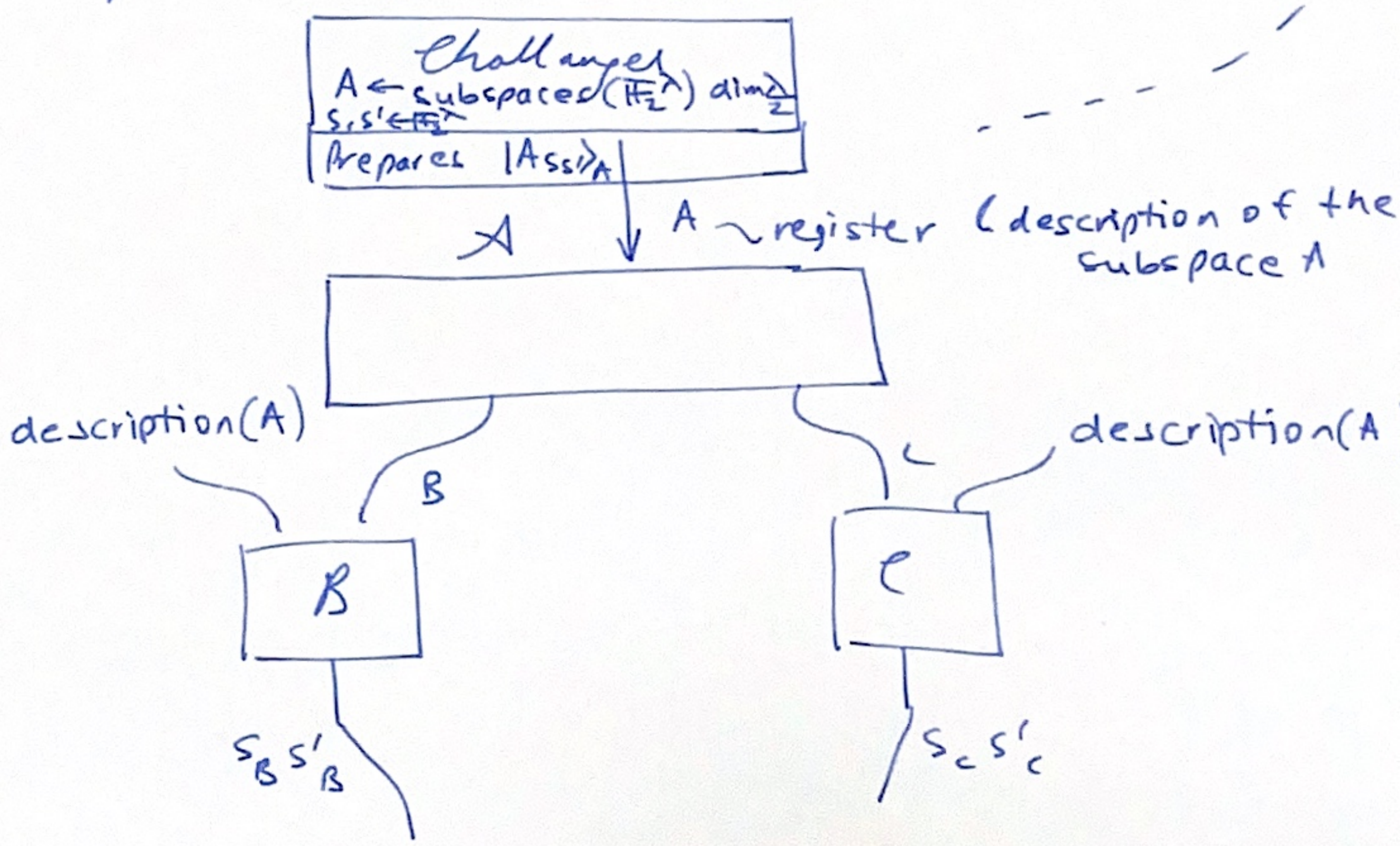
$A^\perp + s$ (where $A^\perp$ denotes the dual subspace of A (or orthogonal, if you will))

These states are written as $|A_{ss'}\rangle$ &

satisfy many properties. Here are some of them.

1. Given $|A_{s,s'}\rangle$ & a classical description of the subspace A,
∃ an efficient quantum algorithm that can compute both s & s'.

2. No adversary wins the MOE game (Fig 3) for coset states w.p. $\geq \sqrt{e} \cdot \cos^{\lambda}(\pi/8)$ (proved first in [CLLZ'21]).



win if ~~$s = s_B = s'_B$ &~~
$s = s_B = s_C$ &
$s' = s'_B = s'_C$.

Fig 3

Story: • Note the ~~remarkable~~ similarity b/w Wiesner states & coset states.

↳ There's a correspondence: $\theta \leftrightarrow A$ (the subspace)
$x \leftrightarrow (s, s')$

↳ Thus one can translate the [BL20] construction into one using coset states.

• So then why do we bother with coset states?

↳ coset states differ from Wiesner states in the following key way:

(i) Given $|x^\theta\rangle$ together with an oracle P_x (that outputs 1 only if input $y = x$)

∃ an efficient quantum adversary that learns x without knowing θ. [Lut '10]

(ii) This also applies to the MOE games for Wiesner states: if A additionally gets access to P_x, the MOE game is no longer secure.

(iii) However, the MOE games for coset states remain secure even if oracles for checking $s \& s'$ are given.

↳ More formally, i.e. let P_{A+s} be an oracle that outputs 1 if & only if the input $y \in A+s$ but $P_{A+s'}$ analogous for $y \in A+s'$.

called MOE games for coset states w/ membership checking oracle calls.

• Then, no adversary (A, B, C) can win the MOE games for coset states, (w.p. non-negl prob) even if $A\,B\,C$ are given poly many oracle calls to P_{A+s} & $P_{A+s'}$.

• We now look at the scheme that does satisfy unclonable indistinguisha.

essentially [BL20] w/ coset states instead of Weiner

Gen(1^λ): ~~Or~~ returns a random subspace $A \subseteq \mathbb{F}_2^\lambda$ of dimension $\lambda/2$.

$\text{Enc}^H(A, m)$: Samples $s, s' \in \mathbb{F}_2^{\lambda a}$

Outputs $(|A_{ss'}\rangle, m \oplus H(s,s'))$

$\text{Dec}^H(A, (|A_{ss'}\rangle, c))$: Recovers s, s' from the coset state,

Outputs $c \oplus H(s,s')$.

Remark 1: They got rid of the "α" in [BL20].

(They also think they can remove it from BL20])

Remark 2: In this construction, they only need coset states & random oracles.

They do not need to have access to membership checking oracles

Membership checking oracles are only used for proving security

This makes the security stronger (as we assume the adversary is stronger).

This, however, means that Weiner states cannot be used

To prove security using this approach.

Open question: Can [BL20] be proved secure, using Wiener states?

Basing Security on Reprogramming Games.

Story: what property do we require coset states to satisfy?

Simplification: We focus on the $n=1$ case.

Consider the following game.

- H be a random oracle w/ binary range.

$$H : \mathbb{F}_2^{\lambda} \times \mathbb{F}_2^{\lambda} \to \{0,1\}.$$

Additionally, let $\mathcal{A}$ & $\mathcal{C}$ have oracle access to P_{A+s} & $P_{A^{\perp}+s'}$.

- $H_{(s,s') \to \perp}$: Same as H except $H(s,s')$ is replaced w/ $\perp$.

- $H_0 := H$ the original random oracle

$H_1 := \begin{cases} H & \text{~~except~~ at all inputs other than } ss' \\ H(ss') \oplus & \text{at } ss' \end{cases}$

Challenge Modes: $b_B \leftarrow \{0,1\}$, $b_C \leftarrow \{0,1\}$

- (i) Identical: $b_B = b_C = b$ & $b \leftarrow \{0,1\}$; (ii) Independent:

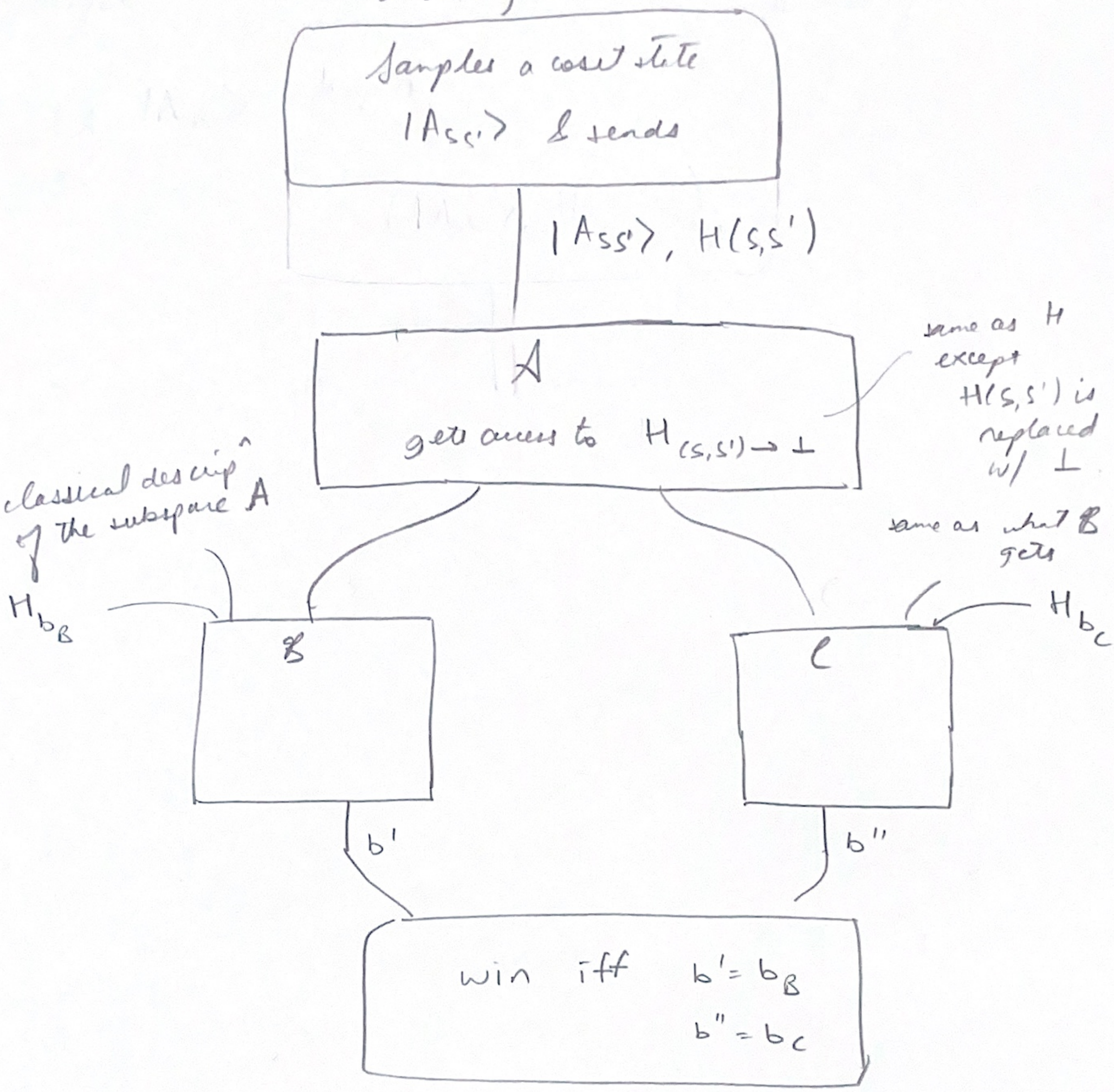


Fig 5: Reprogramming games for coset states in QROM.

Story: • In the game above, in the identical challenge mode,

the adversaries $\mathcal{B}, \mathcal{C}$ try to distinguish

b/w H_0 & H_1 (i.e. whether the random oracle

was reprogrammed or not).

• It turns out that by a sequence of

"standard variable substitution"

uncloneable indistinguishability of their new

scheme can be based on the

"identical challeye mode" of the

reprogramming game.

• Note that in the reprogramming game,

$\mathcal{A}$ has <u>no access</u> to y, H at (s, s').

the value of

↳ This is different from MOE or

uncloneable indistinguishability games.

↳ Nonetheless, the authors show that

one can assume $\mathcal{A}$ never queries

at (s, s') by introducing a small loss.

- The security of identical challenge mode can be reduced to the security of independent challenge mode.

↳ This follows from a careful analysis of Jordan's lemma.

↳ The authors believe this is non-trivial & leave it to the end of this overview

- Here, we look at how the security of the game in the independent challenge mode is proved.

↳ They take inspiration from Zhandry's [Zha'20] work that studies success probabilities of quantum programs.

↳ Informally, the following is shown:

Inf Claim. ∃ an efficient procedure that operates locally on both the entangled adversaries $(\mathcal{B}, \mathcal{C})$ & outputs $(\mathcal{B}', \rho_{\mathcal{B}})$, $(\mathcal{C}', \rho_{\mathcal{C}})$ s.t

- B' & C' are "un-entangled"
- The success prob. of B' on guessing whether it has H_0 or H_1 is p_B
- The " " of C' on " " " H_0 or H_1 is p_C
- The expectation of $p_B \cdot p_C$ equals (B, C)'s success prob. in the reprogramming game in the ind. challenge mode.

Remarks: To estimate $p_B \cdot p_C$, we want to run B' & C'.

To run B' & C', we will need to give access to H_0 & H_1

(in the ind. challenge mode, (B', C') get H_0 or H_1 independently each)

A only gets access to $H_{(S,S') \to \perp}$.

(For the procedure) To be useful in breaking the MDE game,

the procedure cannot know s or s' but it knows A & has access to oracles P_{A+s}, $P_{A+s'}$

Claim: Reprogramming of $H_{(s,s')\to\perp}$ is possible, given access to membership oracles & A

[c.g. H_1 can be obtained by reprograming as follows:

$$H_1(z,z') = \begin{cases} \neg H(s,s') & Q_s(z)=1 \ \wedge \\ & Q_{s'}(z')=1 \\ H_{(ss')\to\perp}(z,z') & \text{else} \end{cases}$$

where $Q_s(z)$ is a delta-function outputting 1 on $z=s$, 0 else. (aka point-function)

(similarly $Q_{s'}(z')$).

It remains to show that $Q_s(z)$ can be instantiated using A & the oracle P_{A+s}.

[Here's how: (1) Check if z is in $A+s$

(2) If z lexicographically the smallest in $A+s$.

NB: Step (1) can be checked via P_{A+S}.
(simply query it at z).

Step (2) can be done by knowing
(i) A (which we assumed is given) &
(ii) $z \in A+S$ (which is known from step 1).
as follows:
enumerate each coordinate & do
Gaussian elimination to see if
there is any z^* lexicographically
smaller than z s.t.

$$(z - z^*) \in \text{span}(A)$$

(They say this can be done efficiently.
Not really clear to me.

Similarly, one can implement $D_{S'}(z')$.

Remark (cont): Without membership checking oracles,
it is unclear how Q_S & $Q_{S'}$ can
be instantiated — & hence, its unclear
how to apply these ideas for
Wiesner states.

Story: - they now "prove" the security of the reprogramming game in the "independent challenge mode".

[Proof sketch

↪ Suppose an adversary (A, B, C) has non-trivial success probability $1/2 + \gamma$ for some large γ.

Then, the procedure above (i.e. in the inf. claim on page 28)

output large $p_B \cdot p_C > \frac{1}{2} + \frac{\gamma}{2}$ w/

non-negligible prob.

(Me: I suppose $\because \langle p_B \cdot p_C \rangle = \frac{1}{2} + \gamma$, one can argue that the individual terms must be at least some fraction, w/ non-negl prob.)

↪ If B' never queris H_0 & H_1 on (s, s'), the best prob. (of guessing which among H_0 or H_1 was given) is at most $1/2$.

Thus, it must be querying at (s, s') & this can be extracted by measuring the query register of B' at a random time, w/ non-negl prob.

↪ Similarly for c'.

↪ But this violates the MOT games for most states

— a contradiction.

□]

Relating Identical Challenge Mode to Independent Challenge Mode.

Story: We now see how the identical & independent challenge modes are related.

: they first consider the independent challenge mode & give a nice characterisation of the state produced by Alice.

Suppose: $A, s\, s'$ & the oracle $H_{(s,s')\to\perp}$ are chosen randomly.

Let: $|\sigma\rangle_{BC}$ denote the joint quantum state shared by Bob & Charlie, after Alice's stage.

Def^: Π_b^B & Π_b^C for $b \in \{0,1\}$ as follows:

Π_0^B: Run Bob on its own part $\sigma[B]$ of σ
w/ oracle access to H_0 (call it U)
project onto Bob outputting 0 & ($|0\rangle\langle 0|$)
rewind (call it $U^\dagger$)
(so $U^\dagger|0\rangle\langle 0|U$)

Π_1^B: same as Π_0^B except oracle access to H_1
& project onto Bob outputting 1.

Π^C_0 & Π^C_1 are defined analogously.

NB: Π^B_b is the projection for Bob's success on H_b &
Π^C_b is the projection for Charlie's success on H_b.

NB2: By definition, the success prob. in the independent challenge mode is:

[1] $$\mathrm{tr}\left[\left(\frac{\Pi^B_0+\Pi^B_1}{2}\right)\otimes\left(\frac{\Pi^C_0+\Pi^C_1}{2}\right)\ |\sigma\rangle\langle\sigma|\right]$$

Notation: Let $\{|\phi_p\rangle\}_{p\in\mathbb{R}}$ denote the eigenvectors of

$\frac{\Pi^B_0+\Pi^B_1}{2}$ w/ eigenvalues $p\in[0,1]$.

(assume for simplicity the eigenvalues are all distinct)

: Let $\{|\psi_q\rangle\}_{q\in\mathbb{R}}$ " $\frac{\Pi^C_0+\Pi^C_1}{2}$ ".

NB3: One can write $|\sigma\rangle$ in this basis as

$$|\sigma\rangle=\sum_{pq}\alpha_{pq}|\phi_p\rangle|\psi_q\rangle.$$

sub-Claim: From the analysis of "independent challenge mode" in the previous paragraph, one can show that p & q cannot both be simultaneously far from the trivial guessing prob. $\frac{1}{2}$, i.e.

for any inverse poly ϵ

$$\sum_{\substack{p:\,|p-1/2|>\epsilon \\ q:\,|q-1/2|>\epsilon}} |\alpha_{pq}|^2 \approx 0.$$

$\Rightarrow$ $|\sigma\rangle$ is very close to the summation of the following subnormalised states:

$$\underbrace{\sum_{\substack{p:\,|p-1/2|\le\epsilon \\ q:\,|q-1/2|>\epsilon}} \alpha_{pq}\,|\phi_p\rangle|\psi_q\rangle}_{\text{ii}} + \underbrace{\sum_{\substack{p:\,|p-1/2|>\epsilon \\ q:\,|q-1/2|\le\epsilon}} \alpha_{pq}\,|\phi_p\rangle|\psi_q\rangle}_{\approx|\sigma\rangle}$$

$|\sigma^{\text{bad}}_{B}\rangle$ $\qquad$ $|\sigma^{\text{bad}}_{\mathcal{C}}\rangle$

Notation:

NB 4: Recall Eq [1] & note that using $|\sigma\rangle$, it is bounded by at most $1/2+\epsilon$ for any inverse poly ϵ.

Story: We again get the security of the independent challenge mode. To extend to the identical challenge mode note that the characterisation of $|\sigma\rangle$ also holds in the identical challenge mode.

(∵ $|\sigma\rangle$ is the state received by $B, \mathcal{C}$;
how they use it does not change the fact that they hold $|\sigma\rangle$;
so, even though we characterised it assuming $B, \mathcal{C}$ proceed in the independent challenge mode, the characterisation stays valid, regardless)

NB: The success prob. in the identical challenge mode is

[2] $$\mathrm{tr}\left[\left(\frac{\Pi_0^B\otimes\Pi_0^C + \Pi_1^B\otimes\Pi_1^C}{2}\right)|\sigma\rangle\langle\sigma|\right].$$

NB2: Using $|\sigma\rangle = |\sigma_B^{bad}\rangle + |\sigma_C^{bad}\rangle$, this (i.e. [2]) is at most

$$\frac{1}{2} + \epsilon + \frac{1}{2}\Big(\big|\langle\sigma_B^{bad}|\,\Pi_0^B\otimes\Pi_0^C\,|\sigma_C^{bad}\rangle\big| + \big|\langle\sigma_B^{bad}|\,\Pi_1^B\otimes\Pi_1^C\,|\sigma_C^{bad}\rangle\big|$$

$$\underline{\Pi_0\otimes\Pi_0 + \Pi_1\otimes\Pi_1} = \underline{(\Pi_0+\Pi_1)\otimes(\Pi_0+\Pi_1)} - \Pi_1\otimes\Pi_0 - \Pi_0\otimes\Pi_1$$

$$\leq \qquad\qquad + \Pi_1\otimes\Pi_0 + \Pi_0\otimes\Pi_1$$

ME: They then argue that using a corollary of Jordan's lemma, one can prove that the cross terms are zero.

This last part is unclear to me —

I don't see how [2] & [1] differ only by

$$\langle\sigma_B^{bad}|\,\Pi_b^B\otimes\Pi_b^C\,|\sigma_C^{bad}\rangle$$