

## Table of contents

Old stuff - below

New stuff - after

## Protocol

Alice  $|H\rangle_x \leftarrow$  choice for  $x$   
 $|H\rangle_r \leftarrow$  choice for  $r$   
 $\downarrow |H\rangle \leftarrow$  Alice's part of  $|GHZ\rangle$   
 $|0\rangle_s \leftarrow$  message to Bob  
 $|0\rangle_A \leftarrow$  Alice's GHZ outcome, to be determined

$s_0 =$  Alice's state after measuring to get a +  
 creating  $S$ .

$T_{\mathcal{G}}(s_0) =$  Alice's state after sending  $S$  to  
 Bob.

Bob now has a purification of  $T_{\mathcal{G}}(s_0)$ ,  
 so purifying the post-measured state,  
 and  $S$ .

$s_1 = s_0 + G$  space. So  $T_{\mathcal{G}}(s_1) = T_{\mathcal{G}}(s_0)$

First check: Alice measures  $s_1$  to see if  $x \oplus y = 1$ .

$$\max \langle \Pi_{11} s_1 \rangle$$

$$T_{\mathcal{G}}(s_1) = T_{\mathcal{G}}(s_0)$$

This should give 0.75 (or less, perhaps).

# Full protocol SDP

Alice appends  $\frac{1}{2}\mathbb{I}_y$  to  $S_1$ , so Bob has a copy/a purification.

Bob responds w/  $d$  (in space D)  $d = b \oplus c$  here.

Alice checks if  $a \oplus d = xy(x \oplus y \oplus i) \oplus l$

SDP:  $\max \langle T\Gamma_2, S_2 \rangle$  checks if  $x \oplus y = l$   
and  $a \oplus d = \dots$

$$T\Gamma_D(S_2) = S_1 \otimes \frac{1}{2}\mathbb{I}_y$$

$$T\Gamma_G(S_1) = T\Gamma_S(S_0)$$

$$S_0 \in \text{Pos}(\text{HXRAS})$$

$$S_1 \in \text{Pos}(\text{HXRAS})$$

$$S_2 \in \text{Pos}(\text{HXRAYD})$$

$$\sigma_0 = \frac{1}{2}\mathbb{I}_H \otimes I_X + I_X \otimes I_R \otimes I_{QD_H} \otimes I_{QD_S}$$

$$\sigma_1 = U \left( \frac{1}{2}\mathbb{I}_H \otimes I_X + I_X \otimes I_R \otimes I_{QD_H} \otimes I_{QD_S} \right) U^\dagger \otimes I_{QD_S}$$

$$\sigma_2 = \text{creates } S \text{ from } a, x, r.$$

↑ This is  $S_0$ , broken up into steps.

## Continuity argument

### Totally made-up lemma

Keep doing GHZ  $n$  times.

$$\text{Then } \|S - S_{\text{actual}}\| \leq f(n)$$

↑  
 as defined  
 above      ↑  
 approximation      ↑  
 goes to 0 as  $n \rightarrow \infty$

### Lemma

$\lambda$  = SDR value from above.

$\lambda_{\text{actual}}$  = SDR value using  $S_{\text{actual}}$  instead of  $S$ .

$$|\lambda - \lambda_{\text{actual}}| \rightarrow 0 \text{ as } n \rightarrow \infty.$$

Proof: ① Take the dual

② SDR magic.

③ Profit.

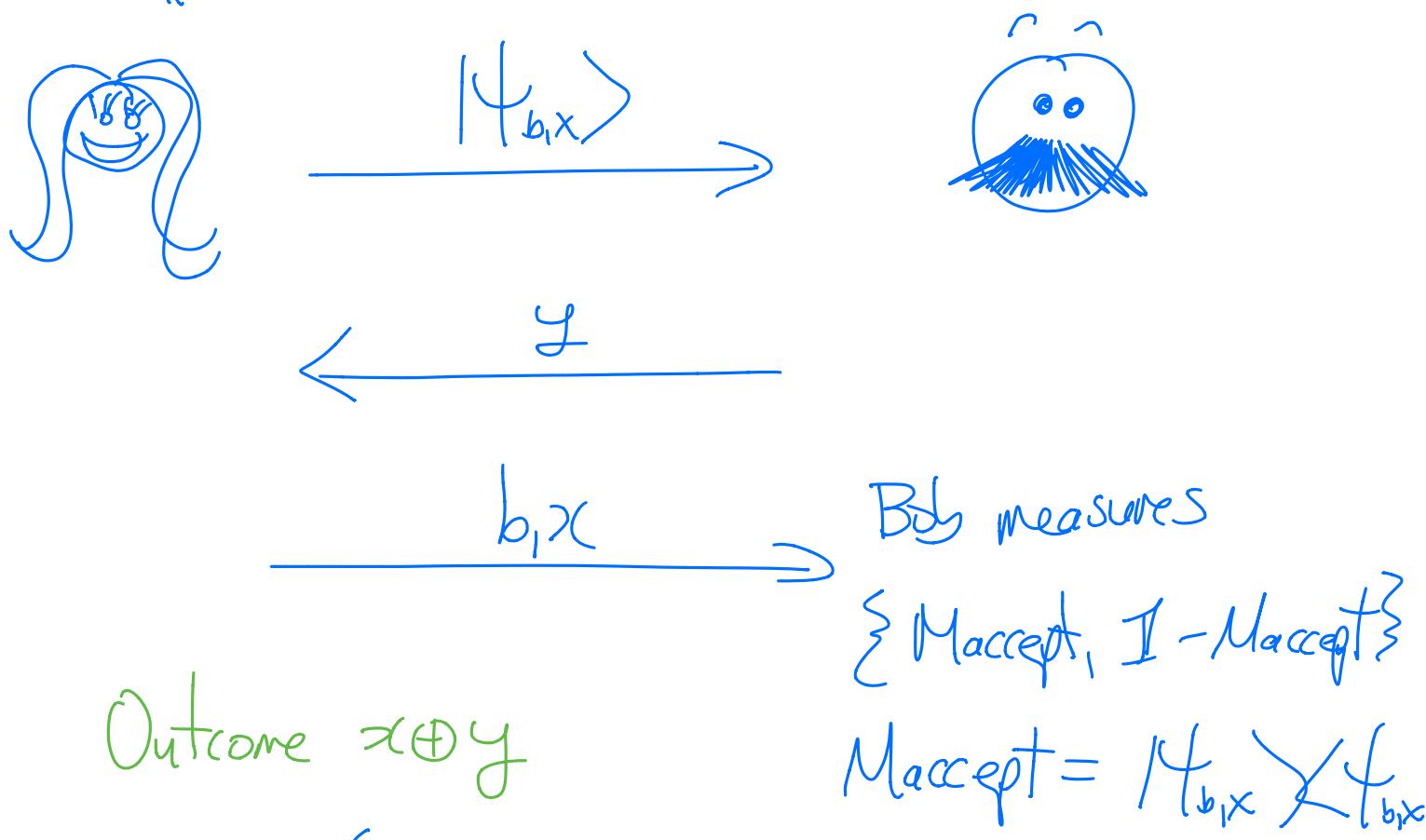
□

Concern: Since in this particular protocol implementation, Bob does not separate the "b & c boxes" there is not really much "Ghz" happening. I can't remember if this should be an issue or not. (In any case,  $\frac{3}{4}$  is an upper bound.)

Question: If Bob sends back boxes B+C to Alice, do we get a nice SDP still? We might need NPA at that point.

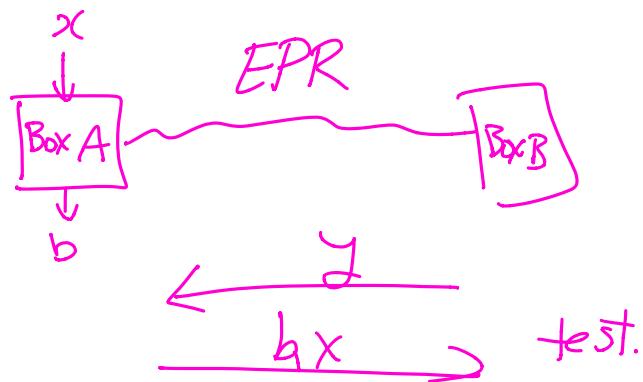
# Coin-flipping protocol, the first

$b, x \in \{0, 1\}$

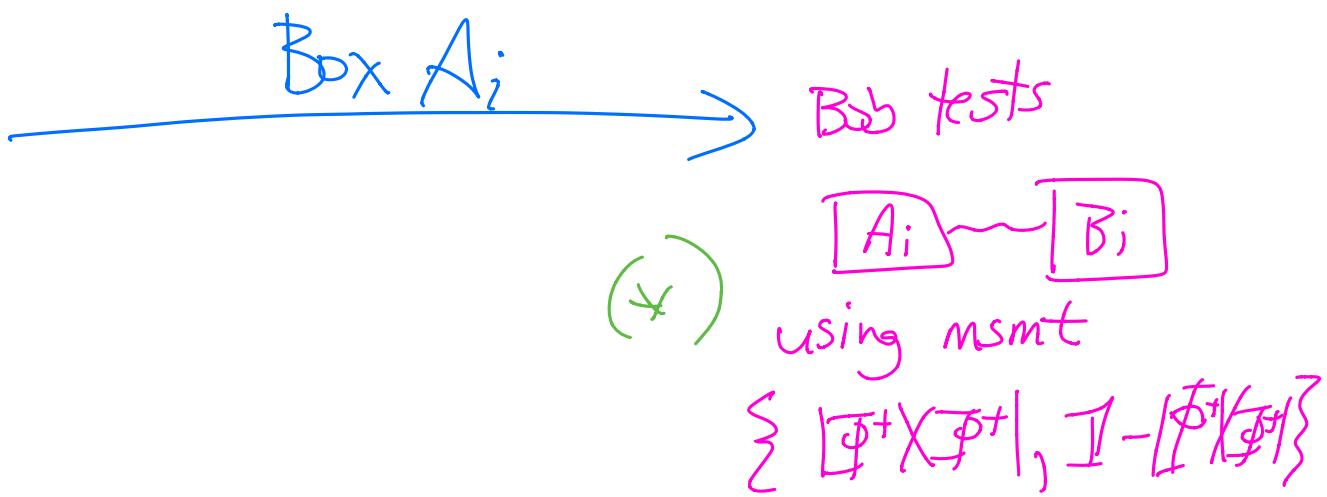
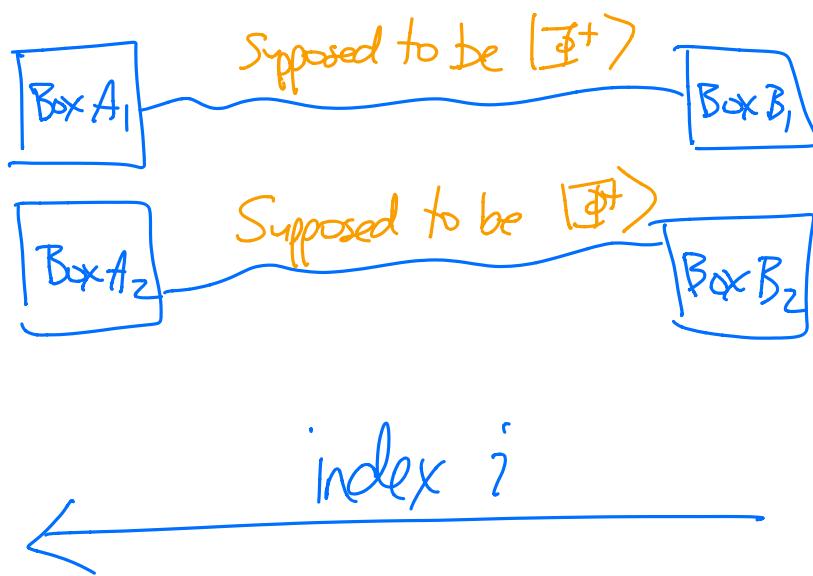


Can choose  $\{|\psi_{bx}\rangle : b, x \in \{0, 1\}\}$  to make this have  $P_{B,0}^*, P_{B,1}^*, P_{A,0}^*, P_{A,1}^* = 3/4$ .

Question: Can we make this DI?



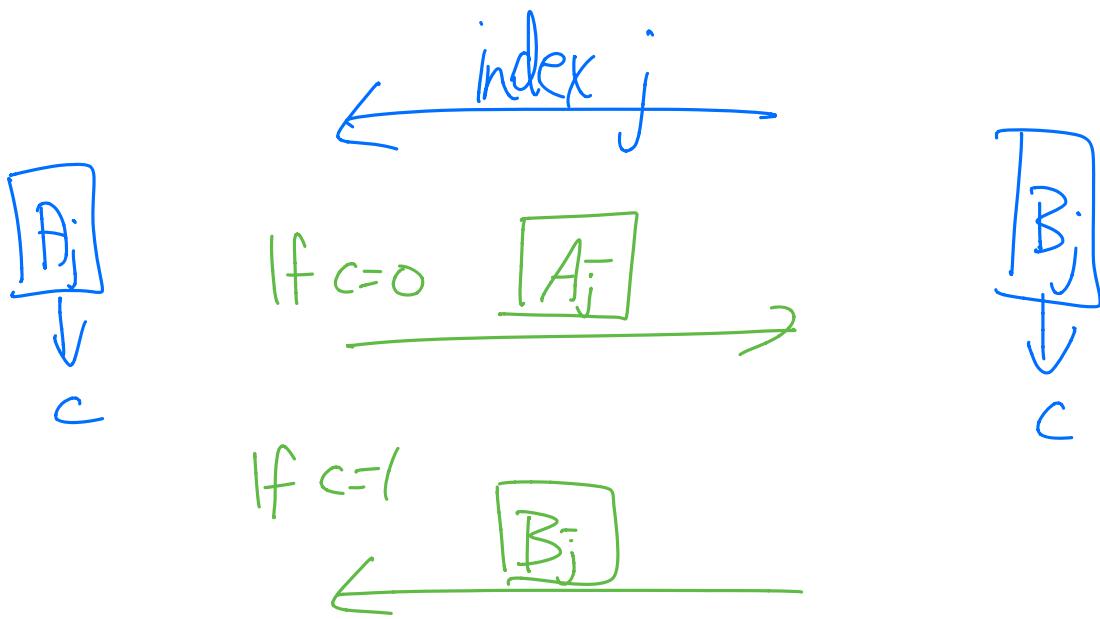
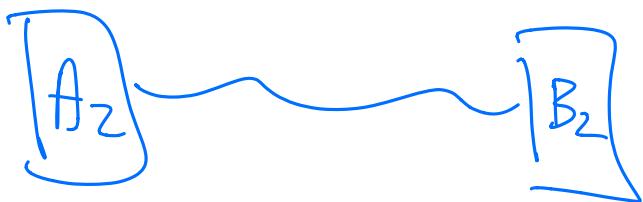
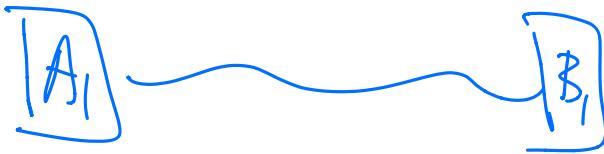
# Coin-flipping protocol, the second (GD version)



Outcome: They measure remaining boxes in computational basis.

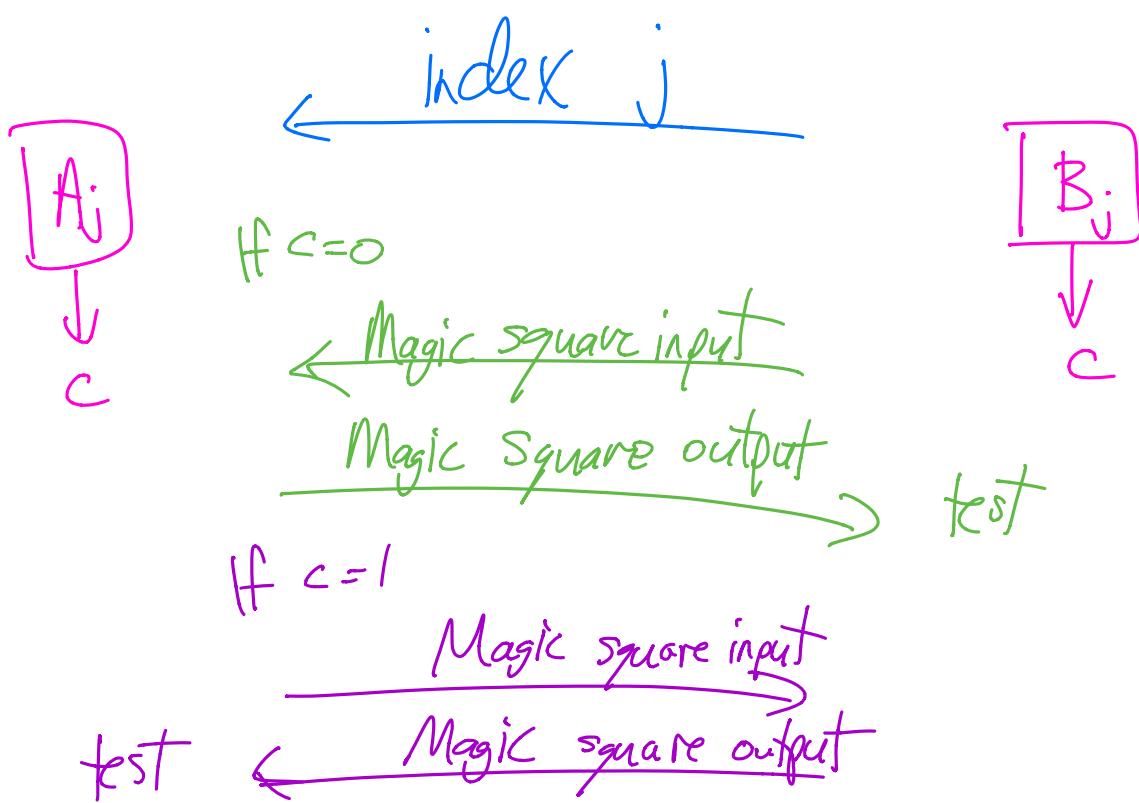
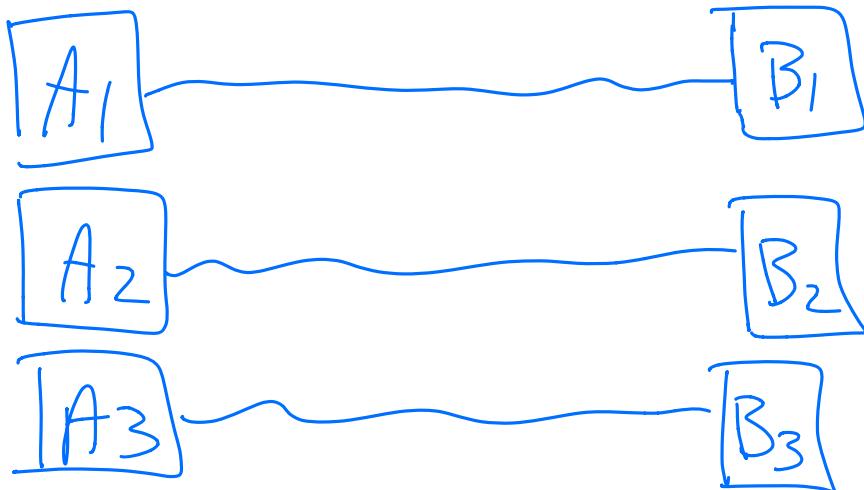
$$P_{B,0}^*, P_{B,1}^*, P_{A,0}^*, P_{A,1}^* = 3/4.$$

# Weak CF version



loser tests like (\*)

# DI Weak version



Bad news: In the DD model, Bob can cheat w.p.  $\frac{7}{8}$ .

Good news: In the DD model, Alice can cheat w.p.  $\approx \frac{5}{8}$   
(I think)

Not sure if this is a good DI protocol...

## Cheat vector

Old SDP:

SDP:  $\max \langle \Pi_2, S_2 \rangle$

$$\text{Tr}_D(S_2) = S_1 \otimes \frac{1}{2} \mathbb{I}_y$$

$$\text{Tr}_G(S_1) = \text{Tr}_S(S_0)$$

$$S_0 \in \text{Pos}(H X R A \underline{S})$$

$$S_1 \in \text{Pos}(H X R A \underline{G})$$

$$S_2 \in \text{Pos}(H X R A \underline{G} Y \underline{D})$$

## Cheat vector SDP:

3 outcomes for Alice, outcome 0, outcome 1, abort.

$\Pi_0$  = checks  $S_2$  to see if  $x \oplus y = 0$  (Alice wins, Bob is not tested)

$\Pi_1$  = checks  $S_2$  to see if  $x \oplus y = 1$  (Bob wins, but will be tested)

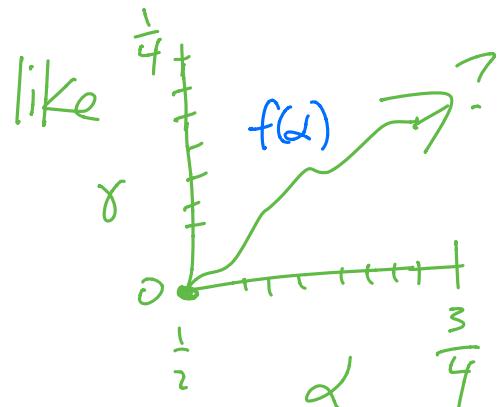
$\Pi_{GHZ}$  = checks  $S_2$  to see if Bob was honest  
 $x \oplus d = \dots$

$\Pi_{\text{abort}}$  = checks  $S_2$  to see if Bob was dishonest  
 $x \oplus d \neq \dots$

## New SDP

let  $\alpha = \text{probability Alice accepts } 0$       } with respect to a fixed  
 $\beta = \text{probability Alice accepts } 1$       } cheating strategy.  
 $\gamma = \text{probability Alice aborts}$

$\alpha + \beta + \gamma = 1$ . We want to graph  $(\alpha, \gamma)$



$$\alpha = \langle \Pi_0, \beta_2 \rangle$$

$$\beta = \langle \underbrace{\Pi_1 \Pi_{G+2}}_{\text{these commute}}, \beta_2 \rangle$$

these commute, don't call the projection police on me!

$$\gamma = \langle \Pi_1 \Pi_{\text{abort}}, \beta_2 \rangle$$

Cheat vector  $V(B) = \left\{ \begin{pmatrix} \alpha \\ \beta \\ \gamma \end{pmatrix} : \alpha, \beta, \gamma \text{ come from a cheating strategy of Bob} \right\}$

Define  $f: [\frac{1}{2}, \frac{3}{4}] \rightarrow [0, \frac{1}{4}]$  as  $f(\alpha) = \min_{(\alpha, \beta, \gamma) \in V(B)} \gamma$

Let's calculate  $f$ !

↑  
smallest aborting probability for a given Alice accept 1 probability.

$$f(\lambda) = \min \langle \Pi_2 \Pi_{\text{abot}}, S_2 \rangle (= \gamma)$$

Note

$$\begin{aligned} T_{D'}(S_2) &= S_1 \otimes \frac{1}{2} I_y \\ T_G(S_1) &= T_S(S_0) \end{aligned}$$

$$S_0 \in \text{Pos}(\text{HXRAS})$$

$$S_1 \in \text{Pos}(\text{HXRAG})$$

$$S_2 \in \text{Pos}(\text{HXRAGFD})$$

} from before

$$\langle \Pi_1 \Pi_{\text{abot}}, S_2 \rangle = \lambda$$

this is  $\Pi_{\text{accept}}$  from original SDF

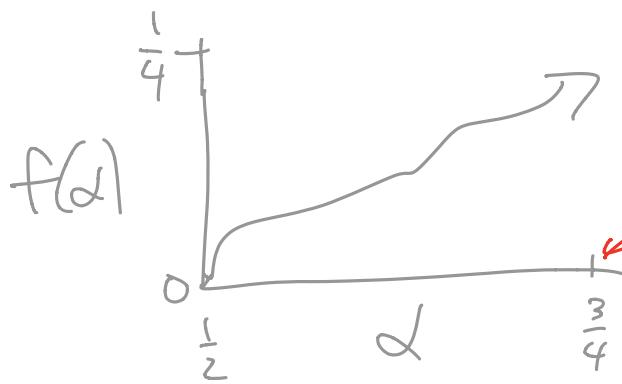
Matlab

$$\text{For } \lambda = 0.5 : 0.01 : 0.75$$

solve SDF above to get  $f(\lambda)$

end.

Graph



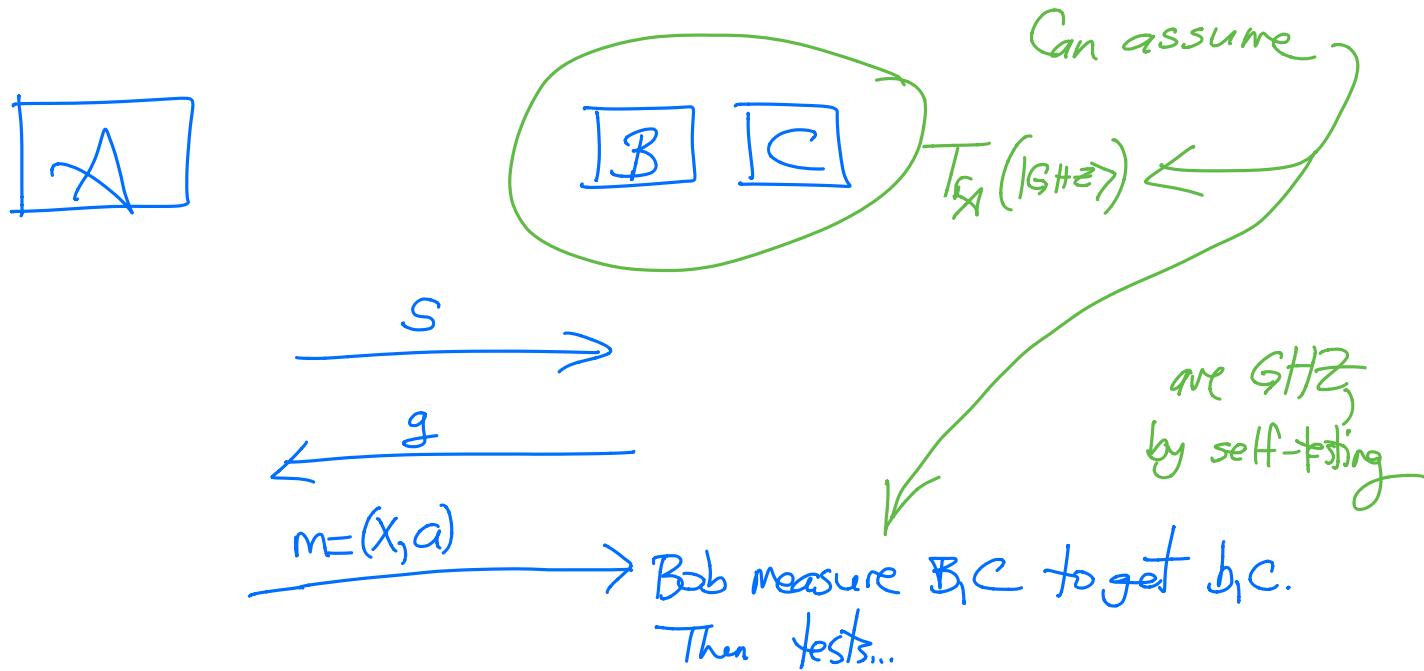
If  $f(3/4) > 0$ , then we have a brand new protocol for DI SCF AND DI WCF!

Perhaps a better approach...

Let's test Alice instead. So Bob self-tests Alice.

Bob's cheat vector:  $V(B) = \left\{ \begin{pmatrix} \alpha \\ \beta \\ \gamma \end{pmatrix} : \frac{1}{2} \leq \beta \leq \frac{3}{4}, \gamma = 0 \right\}$

Let's work on Alice's SDE/cheat vector...



$$S_0 = T_A(S_{GHZ} \otimes S_{GHZ})$$

$$T_S(S_1) = S_0 \quad \text{Alice gets purification}$$

$$T_M(S_2) = S_1 \otimes \frac{1}{2} I_S$$

Measure  $S_2$  to see if  $x \oplus g = 0$  or 1 and if test passes.

Alice always tested now...

Since Bob is too powerful! Boo Bob!

SDP for  $P_{A,0}^*$ ,  $P_{A,1}^*$ .

$$P_{A,0}^* = \max \langle \Pi_0^* \Pi_{\text{ACCEPT}}, S_2 \rangle$$

$$\text{Tr}_M(S_2) = S_1 \otimes \frac{1}{2} \mathbb{I}_S$$

$$\text{Tr}_S(S_1) = \text{Tr}_A(16 \times 8)$$

$$S_2 \in \text{Pos}(BCSM) \quad 32 \times 32$$

$$S_1 \in \text{Pos}(BCS) \quad 8 \times 8$$

Cheat vector

Fix  $S_2$ .

$$\alpha = \langle \Pi_0^* \Pi_{\text{ACCEPT}}, S_2 \rangle$$

$$\beta = \langle \Pi_1^* \Pi_{\text{ACCEPT}}, S_2 \rangle$$

$$\gamma = \langle \Pi_{\text{ABORT}}, S_2 \rangle$$

$$f(\alpha) = \min \langle \Pi_{\text{ABORT}}, S_2 \rangle$$

$$\text{Tr}_M(S_2) = S_1 \otimes \frac{1}{2} \mathbb{I}_S$$

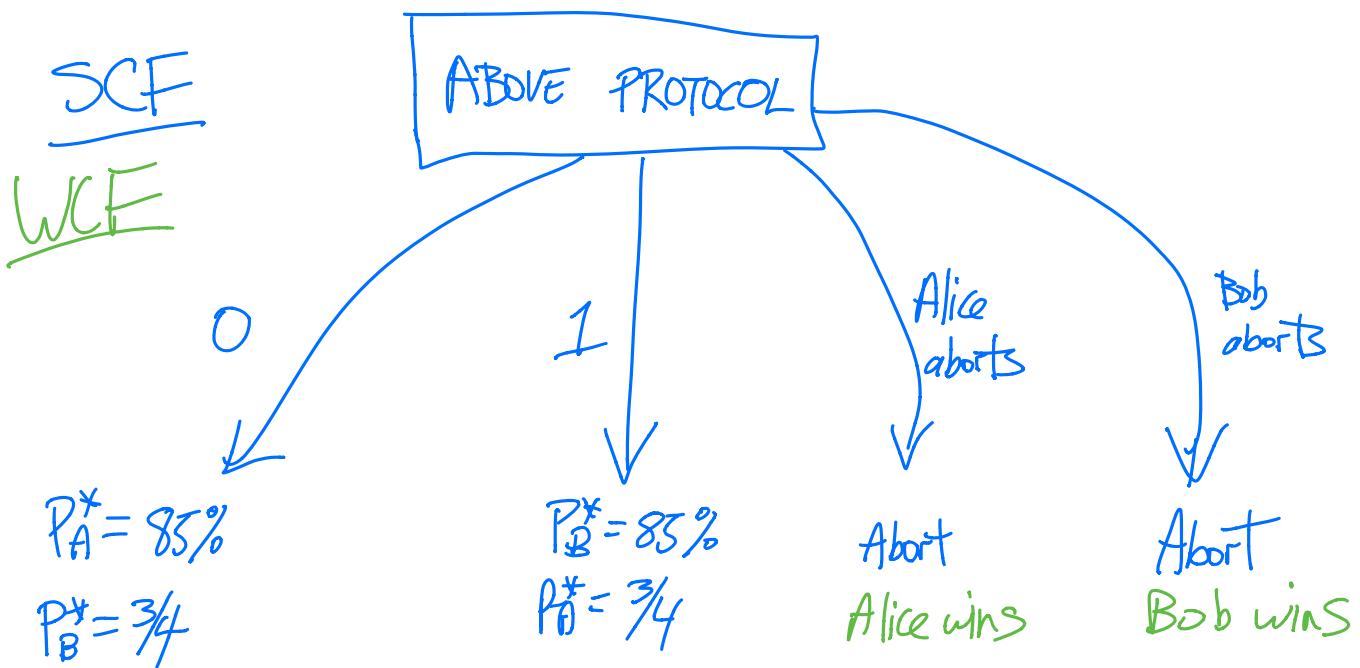
$$\text{Tr}_S(S_1) = \text{Tr}_A(16 \times 8)$$

$$S_2 \in \text{Pos}(BCSM) \quad 64 \times 64 \quad (M \text{ is 2 bits})$$

$$S_1 \in \text{Pos}(BCS) \quad 8 \times 8$$

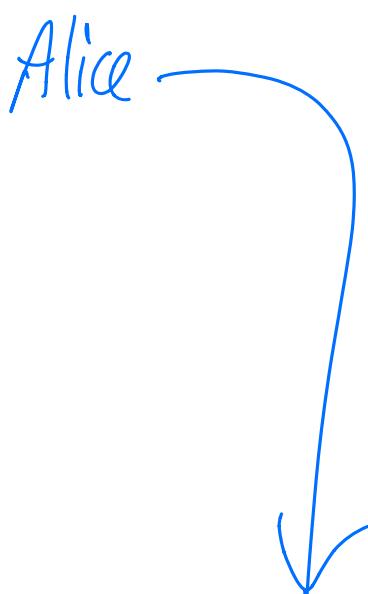
$$\langle \Pi_0^* \Pi_{\text{ACCEPT}}, S_2 \rangle = \alpha$$

Bias of whole protocol... Suppression Technique...



SCF: Bob's cheating prob:

$$\text{Max: } \alpha\left(\frac{3}{4}\right) + \beta(85\%) + \gamma(0) = \frac{3}{4} \cdot 85\% + \frac{1}{4} \cdot \frac{3}{4}$$
$$(\alpha, \beta, \gamma) \in V(B)$$
$$= 82.5\% \text{ Happy!}$$



$$P_{A,D}^* = \max \text{ } \overset{\text{ca}^2(7/8)}{0.85} \langle \Pi_0 \Pi_{\text{accept}}, \beta_2 \rangle + 0.75 \langle \Pi, \Pi_{\text{accept}}, \beta_2 \rangle + 0$$

$$\text{Tr}_M(\beta_2) = \beta_2 \otimes \frac{1}{2} I_S$$

$$\text{Tr}_S(\beta_1) = \text{Tr}_A(16 \text{Hz} \times 6 \text{Hz})$$

$$\beta_2 \in \text{Pos}(BCSGM)$$

$$\beta_1 \in \text{Pos}(BCS)$$

$$=? \quad 0.8123$$

Note: Still need GHz rigidity for self-testing...

$$\text{Bias} \approx 0.325$$

$$\begin{array}{l} \text{SCAKPM} ? \\ | \text{Bias} \leq 0.336 \\ (\text{SCF}) \end{array}$$