Table of contents

Old stuff - below

New stuff - after

Protocol

Alice $|+\rangle_x$ ← Choice for x

$|+\rangle_r$ ← Choice for r

$\frac{1}{2}\mathbb{1}_H$ ← Alice's part of $|GHZ\rangle$

$|0\rangle_s$ ← message to Bob

$|0\rangle_A$ ← Alice's GHZ outcome, to be determined

ρ_0 = Alice's state after measuring to get a $+$ creating S.

$Tr_S(\rho_0)$ = Alice's state after sending S to Bob.

Bob now has a purification of $Tr_S(\rho_0)$, so purifying the post-measured state, and S.

$\rho_1 = \rho_0 + G$ space. So $Tr_G(\rho_1) = Tr_S(\rho_0)$

First check: Alice measures ρ_1 to see if $x \oplus y = 1$.

$$\max \langle \Pi_{11}, \rho_1 \rangle$$

$$Tr_G(\rho_1) = Tr_S(\rho_0)$$

This should give 0.75 (or less, perhaps).

Full protocol SDP

Alice appends $\frac{1}{2}\mathbb{I}_y$ to ρ_1 So Bob has a copy/ a purification.

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

Alice checks if $a \oplus d = xy(x \oplus y \oplus 1) \oplus 1$

SDP: $\max \langle \Pi_2, \rho_2 \rangle$ ← checks if $x \oplus y = 1$ and $a \oplus d = \ldots$

$$\mathrm{Tr}_D(\rho_2) = \rho_1 \otimes \tfrac{1}{2}\mathbb{I}_y$$

$$\mathrm{Tr}_G(\rho_1) = \mathrm{Tr}_S(\rho_0)$$

$\rho_0 \in \mathrm{Pos}(HXRAS)$

$\rho_1 \in \mathrm{Pos}(HXRAG)$

$\rho_2 \in \mathrm{Pos}(HXRAYD)$

$$\sigma_0 = \tfrac{1}{2}\mathbb{I}_H \otimes |+\rangle\langle+|_X \otimes |+\rangle\langle+|_R \otimes |0\rangle\langle 0|_A \otimes |0\rangle\langle 0|_S$$

$$\sigma_1 = U\left(\tfrac{1}{2}\mathbb{I}_N \otimes |+\rangle\langle+|_X \otimes |+\rangle\langle+|_R \otimes |0\rangle\langle 0|_A\right)U^\dagger \otimes |0\rangle\langle 0|_S$$

$U = U_{CHZ}$

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

↑ This is ρ_0, broken up into steps.

Continuity argument

Totally made-up lemma

Keep doing GHZ n times.

Then $\|s - s_{actual}\| \leq f(n)$

- s: as defined above
- s_{actual}: approximation
- $f(n)$: goes to 0 as $n \to \infty$

Lemma

α = SDP value from above.

α_{actual} = SDP value using s_{actual} instead of s.

$|\alpha - \alpha_{actual}| \to 0$ as $n \to \infty$.

Proof: ① Take the dual

② SDP 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, 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

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

$|\psi_{b,x}\rangle$ →

← y

b, x →

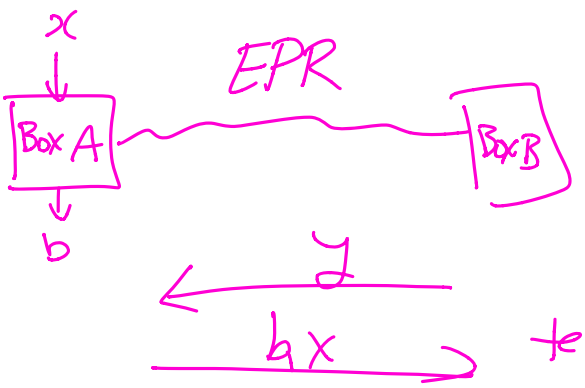
By measures $\{M_{accept}, I - M_{accept}\}$

Outcome $x \oplus y$

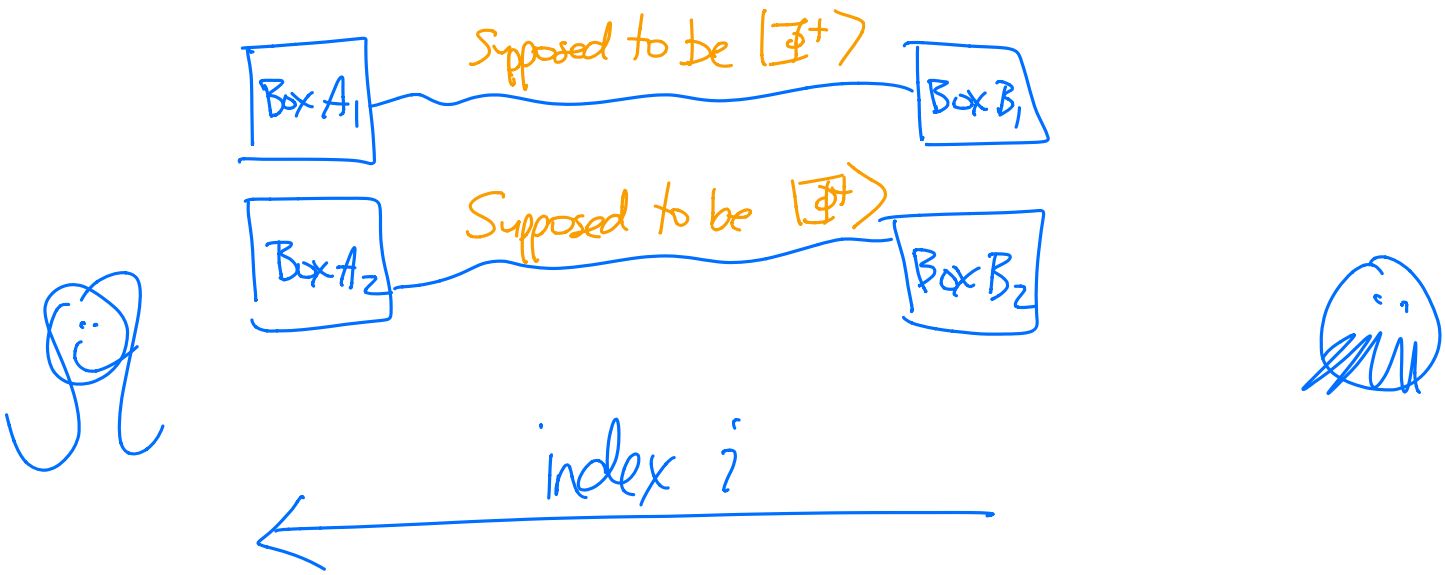
$M_{accept} = |\psi_{b,x}\rangle\langle\psi_{b,x}|$

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 (DD version)



index i

Box A_i

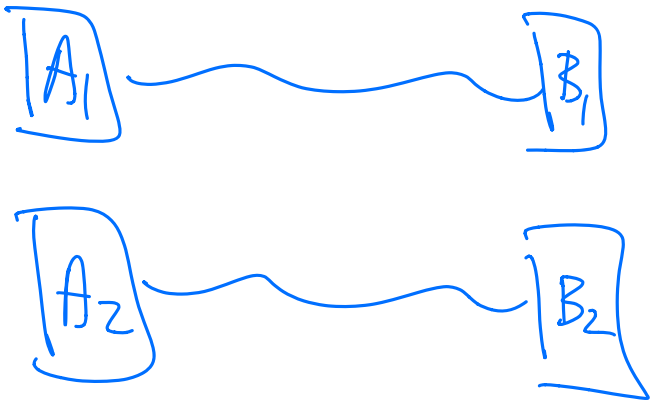
Bob tests A_i ~ B_i using msmt $\{|\Phi^+\rangle\langle\Phi^+|, I - |\Phi^+\rangle\langle\Phi^+|\}$

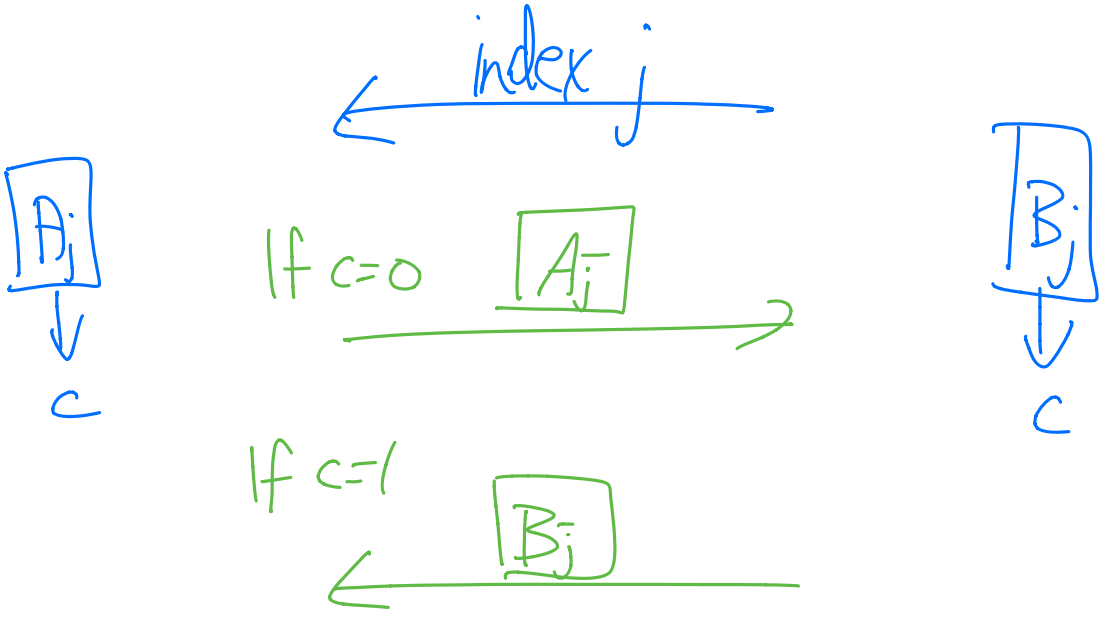
(*)

Outcome: They measure remaining boxes in computational basis.

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

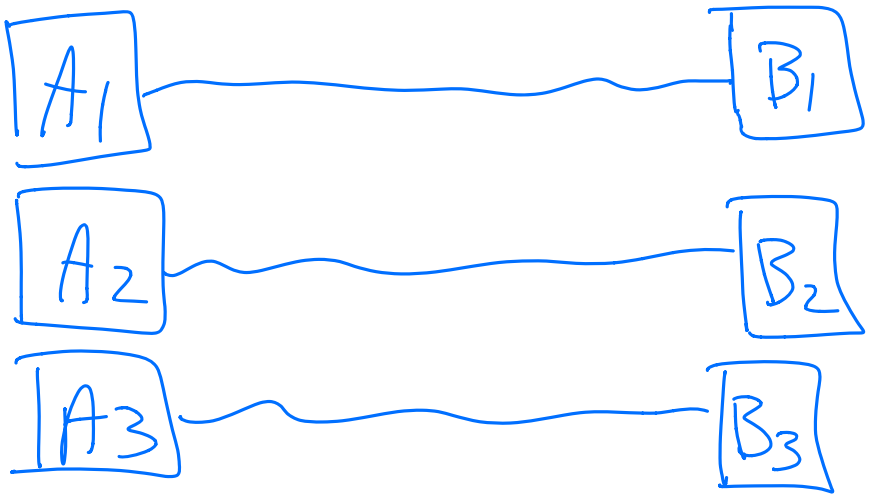
Weak CF version

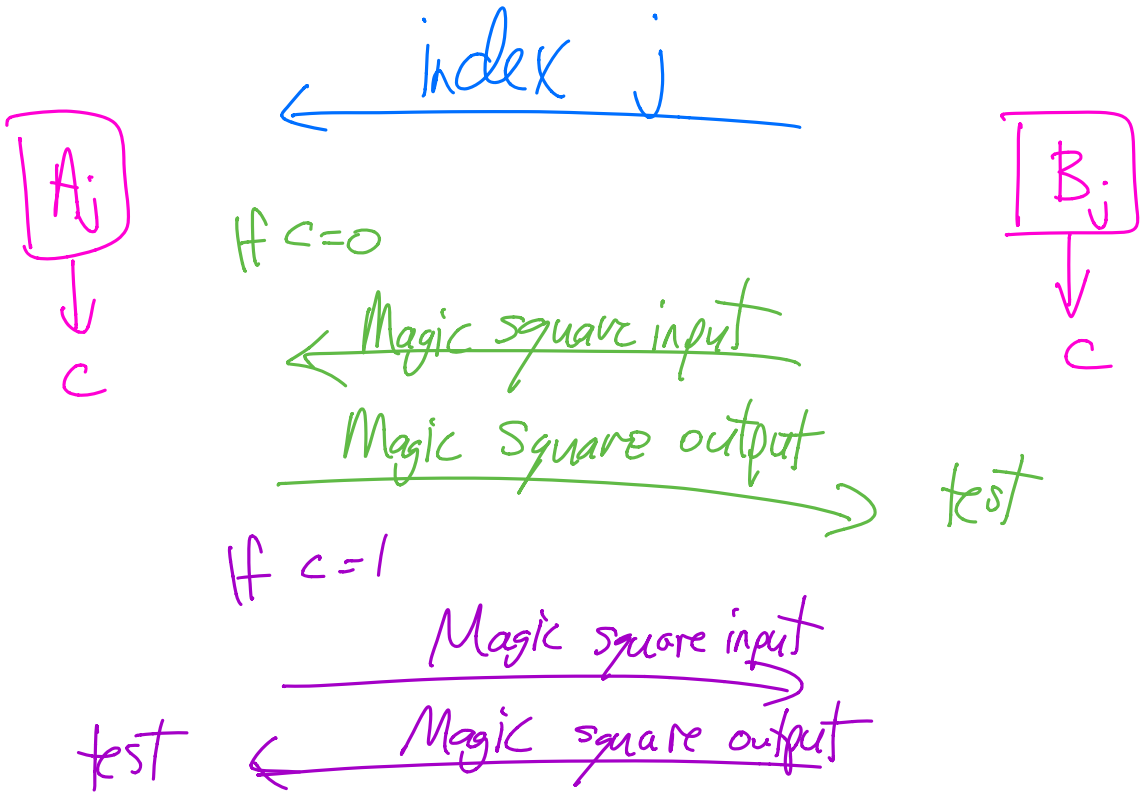




loser tests like (*)

DI Weak version





Bad news: In the DD model, Bob can cheat w.p. 7/8.

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

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

Cheat vector

Old SDP:

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

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

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

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

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

$S_2 \in \mathrm{Pos}(HXRAGYD)$

Cheat vector SDP:

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

Π_0 = checks S_2 to see if $x \oplus g = 0$ (Alice wins, Bob is not tested

Π_1 = checks S_2 to see if $x \oplus g = 1$ (Bob wins, but will be tested)

Π_{GHz} = checks S_2 to see if Bob was honest $x \oplus d = \cdots$

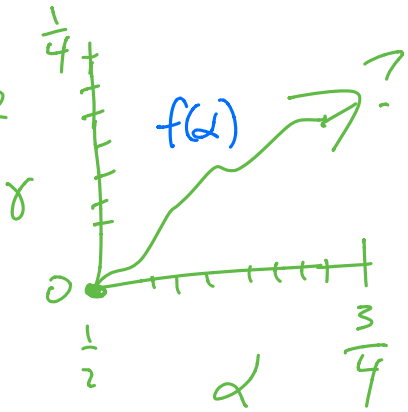
Π_{abort} = checks S_2 to see if Bob was dishonest $x \oplus d \neq \cdots$

New SDP

Let α = probability Alice accepts 0
β = probability Alice accepts 1
γ = probability Alice aborts

} with respect to a fixed cheating strategy.

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



$\alpha = \langle \Pi_0, \rho_2 \rangle$

$\beta = \langle \Pi_1 \Pi_{G\mathcal{H}\mathcal{Z}}, \rho_2 \rangle$

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

$\gamma = \langle \Pi_1 \Pi_{abort}, \rho_2 \rangle$

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

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

Let's calculate f!

$$f(\alpha) = \min \langle T_{12} \Pi_{abort}, S_2 \rangle \quad (= \gamma)$$

Note

$$\mathrm{Tr}_D(S_2) = S_1 \otimes \tfrac{1}{2} I_y$$
$$\mathrm{Tr}_G(S_1) = \mathrm{Tr}_S(S_0)$$

$S_0 \in \mathrm{Pos}(H_X R_A S)$
$S_1 \in \mathrm{Pos}(H_X R_A G)$
$S_2 \in \mathrm{Pos}(H_X R_A G Y D)$

} from before

$$\langle \Pi_1 \Pi_{GHZ}, S_2 \rangle = \alpha$$

this is Π_{accept} from original SDP

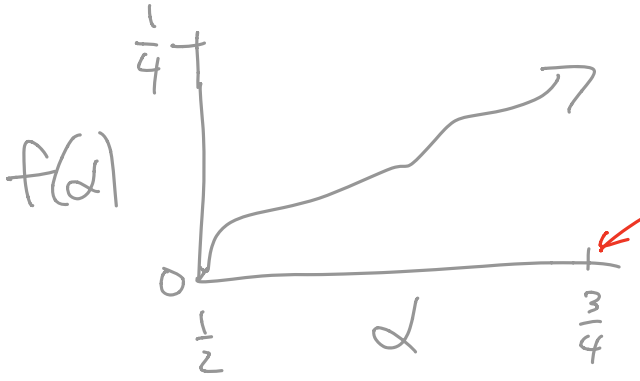
Matlab

For $\alpha = 0.5 : 0.01 : 0.75$

solve SDP above to get $f(\alpha)$

end.

Graph



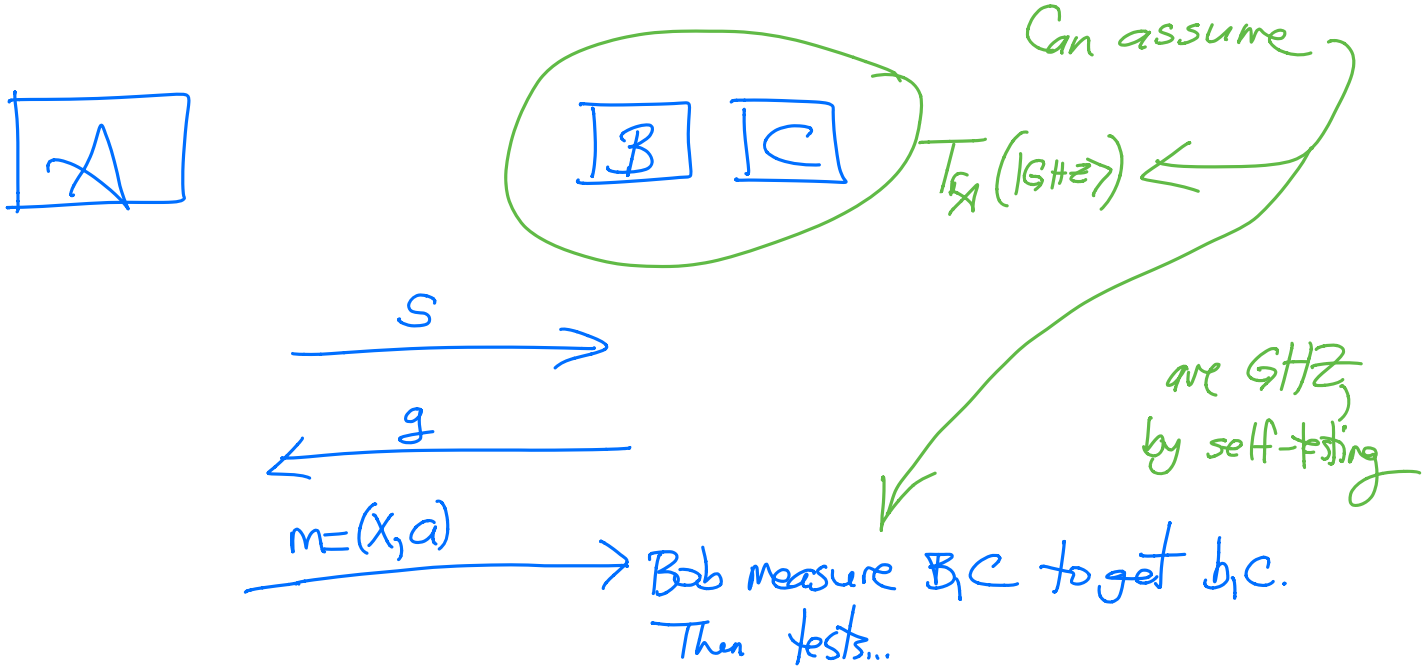
If $f(3/4) > 0$, then we have a brand new protocol for DI SCF AND DI WCF!

Perhaps a better approach...

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

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

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



$\rho_0 = Tr_A(|GHZ\rangle\langle GHZ|)$

$Tr_S(\sigma_1) = \rho_0$

$Tr_M(\sigma_2) = \sigma_1 \otimes \frac{1}{2} \mathbb{1}_S$

Alice gets purification

Measure σ_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 $p^*_{A,0}, p^*_{A,1}$.

$$p^*_{A,0} = \max \langle \Pi_0 * \Pi_{ACCEPT}, \rho_2 \rangle$$

$$Tr_M(\rho_2) = \rho_1 \otimes \frac{1}{2} \mathbb{1}_S$$

$$Tr_S(\rho_1) = Tr_A(1\text{GHz} \times 1\text{Hz})$$

$$\rho_2 \in Pos(BCSGM) \quad 32 \times 32$$

$$\rho_1 \in Pos(BCS) \quad 8 \times 8$$

Cheat vector

Fix ρ_2.

$$\alpha = \langle \Pi_0 * \Pi_{ACCEPT}, \rho_2 \rangle$$

$$\beta = \langle \Pi_1 * \Pi_{ACCEPT}, \rho_2 \rangle$$

$$\gamma = \langle \Pi_{ABORT}, \rho_2 \rangle$$

$$f(\alpha) = \min \langle \Pi_{ABORT}, \rho_2 \rangle$$

$$Tr_M(\rho_2) = \rho_1 \otimes \frac{1}{2} \mathbb{1}_S$$

$$Tr_S(\rho_1) = Tr_A(1\text{GHz} \times 1\text{Hz})$$

$$\rho_2 \in Pos(BCSGM) \quad 64 \times 64 \text{ (M is 2 bits)}$$

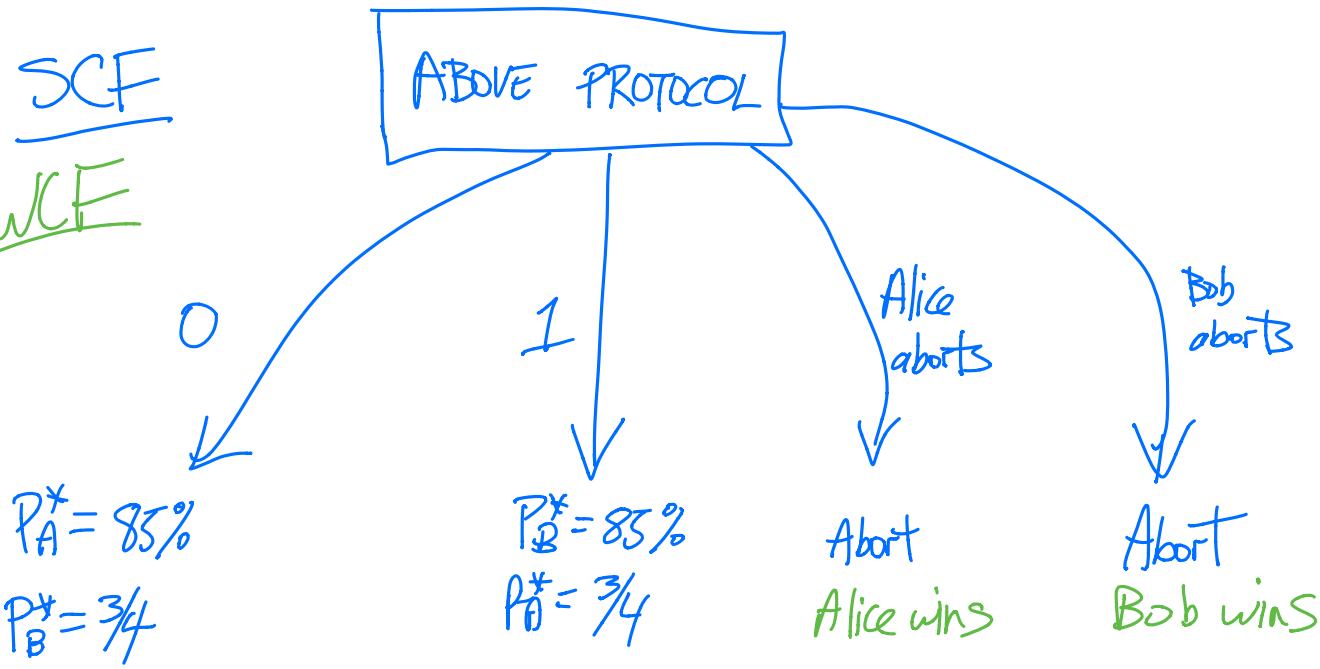
$$\rho_1 \in Pos(BCS) \quad 8 \times 8$$

$$\langle \Pi_0 * \Pi_{ACCEPT}, \rho_2 \rangle = \alpha$$

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

SCF

WCF



SCF: Bob's cheating prob:

$$\max: \alpha\left(\frac{3}{4}\right) + \beta(85\%) + \gamma(0) = \frac{3}{4}\cdot 85\% + \frac{1}{4}\cdot\frac{3}{4}$$

$$(\alpha,\beta,\gamma) \in V(B) \qquad = 82.5\% \text{ Happy!}$$

$$P^*_{A,0} = \max 0.85\langle \Pi_0 \Pi_{\text{accept}}, \rho_2\rangle + 0.75\langle \Pi_1 \Pi_{\text{accept}}, \rho_2\rangle + 0$$

$$\mathrm{Tr}_M(\rho_2) = \rho_1 \otimes \tfrac{1}{2} I_S$$

$$\mathrm{Tr}_S(\rho_1) = \mathrm{Tr}_A(|GHZ\rangle\langle GHZ|)$$

$$\rho_2 \in \mathrm{Pos}(BCS_{GM})$$

$$\rho_1 \in \mathrm{Pos}(BCS)$$

$= ?$ 0.8099

Note: Still need GHZ rigidity ~~for~~ self-testing...

Bias $\simeq 0.325$

| SCAKPM '11

Bias $\lesssim 0.336$ (SCF)