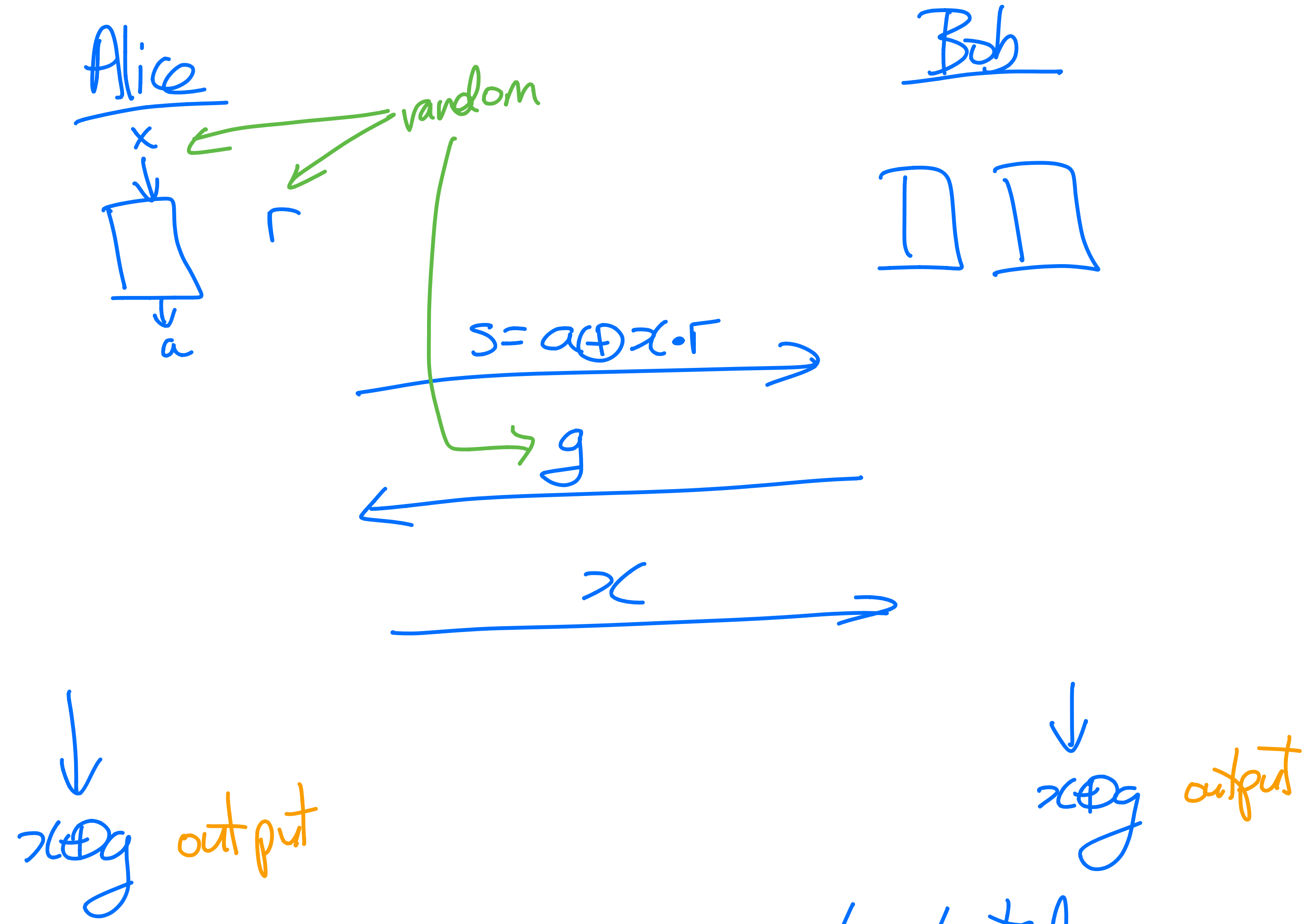
Protocol



Test: If $x \oplus g = 0$, Alice wins, gets tested. Cheating Bob cries, but doesn't really test.

If $x \oplus g = 1$, Bob is tested. Now we're talking.

Alice send y to Bob. And defines z: $x \oplus y \oplus z = 1$.

Bob sends back b, c. Alice checks if

$$a \oplus b \oplus c = xyz \oplus 1.$$

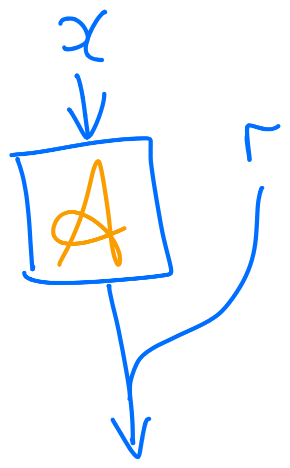
i.e. $$a \oplus b \oplus c = xy(1 \oplus x \oplus y) \oplus 1.$$

i.e. $$s \oplus x \cdot r \oplus b \oplus c = xy(1 \oplus x \oplus y) \oplus 1$$

Removed a, z. Factor 4 savings! Happy!

Simplified Protocol concerning cheating Bob

Key: At this point, Bob only cares about $x \oplus g = 1$ + Alice passing the test. Everything else is a failure.



s

$\xrightarrow{s}$

$\xleftarrow{g}$

$y_1 y_2$ $\xrightarrow{y_2}$

$\xleftarrow{b, c}$

Test.

Since Bob is just some mystery man holding purifications of everything, we can simplify again!

Even more simplified protocol

Alice creates $\rho = \mathcal{U}(\mathbb{1}_A \otimes |+\rangle\langle+|_x \otimes |+\rangle\langle+|_R \otimes |0\rangle\langle 0|_S)\mathcal{U}^\dagger$

$\mathcal{U}$ creates $s = a \oplus x \cdot r$ (with a suppressed)

$\xrightarrow{s}$

ρ_1 $\xleftarrow{g}$

$\xrightarrow{y}$

ρ_2 $\xleftarrow{b, c}$

Alice creates $\frac{1}{2}\mathbb{1}_y$ (Bob holds purification already, by magic)

Notice Bob holds purifications of A + y

Alice tests (x, r, s, y, b, c)

SDP

$$\max \ \langle \Pi, \rho_2 \rangle$$

$$\mathrm{Tr}_{BC}(\rho_2) = \rho_1 \otimes \frac{\mathbb{1}_y}{2}$$

$$\mathrm{Tr}_G(\rho_1) = \rho$$

$$\rho_2 \in \mathrm{Pos}(XRSGY\underline{BC})$$

$$\rho_1 \in \mathrm{Pos}(XRS\underline{G})$$

Happiness!

↓

128×128

16×16

Notice the parts traced out are on the ends. So...

Matlab:

$\rho = \ldots$ (fixed) ← hard part

$\Pi = \ldots$ (fixed) ← hard part

$\rho_2 = \mathrm{Pos}(BCYGSRX)$

$\rho_1 = \mathrm{Pos}(GXRS)$

(variable, spaces reversed)

$$\max \ \langle \Pi, \rho_2 \rangle$$

$\rho_2[1{:}32, 1{:}32] + \rho_2[33{:}64, 33{:}64]$
$\quad + \rho_2[65{:}96, 65{:}96] + \rho_2[97{:}128, 97{:}128]$
$= \frac{1}{2} * \mathrm{kron}(\mathrm{eye}(2), \rho_1);$

$\rho_1[1{:}8, 1{:}8] + \rho_1[9{:}16, 9{:}16] = \rho;$

Continuity argument

Totally made-up lemma

Keep doing GHZ n times.

Then $\|\rho - \rho_{actual}\| \leq f(n)$

as defined above — approximation — goes to 0 as $n \to \infty$

Lemma

$\alpha =$ SDP value from above.

$\alpha_{actual} =$ SDP value using ρ_{actual} instead of ρ.

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

Proof: ① Take the dual

② SDP magic.

③ Profit.

$\square$

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.

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

Below is scratch work!

(Read at your own risk!)

SDP (~~DD setting~~)

Alice's registers X (for x) A (for a)
R (for r) B (for B)
S (for s) C (for c)

Variable: $|\psi\rangle = |GHZ\rangle = \frac{1}{\sqrt{2}}|000\rangle + \frac{1}{\sqrt{2}}|111\rangle$

$$\rho_0 = \mathrm{Tr}_{BC}(|\psi\rangle\langle\psi|)$$

Alice's actions: create $|+\rangle \in X$
create $|+\rangle \in R$
unitary: $\underbrace{XRA}_{\text{control}} \otimes \underbrace{S}_{\text{target}}$

$$\rho_0' = \mathcal{U}\left(\underset{A}{\rho_0} \otimes \underset{X}{|+\rangle\langle +|} \otimes \underset{R}{|+\rangle\langle +|} \otimes |0\rangle\langle 0|_S\right)\mathcal{U}^\dagger$$

$$\rho_0'' = \mathrm{Tr}_S(\rho_0')$$

Bob sends back G. Alice now has ρ_1.

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

Bob succeeds if $x \oplus y = 1$ (but we'll assume this)

Alice adds the registers $Y_1 Y_2$ in state $|\Phi^+\rangle$

Alice sends Y_2.

$$\rho_1' = \mathrm{Tr}_{Y_2}(\rho_1 \otimes |\Phi^+\rangle\langle\Phi^+|)$$

Bob sends back $B \otimes C$.

Alice now has ρ_2

Alice measures to see if

$x \oplus y = 1$ $\boxed{\text{AND}}$ $s \oplus x \cdot r \oplus c = xy(1 \oplus x \oplus y) \oplus 1$

SDP: max $\langle \Pi_1, \rho_2 \rangle$

$$\mathrm{Tr}_{BC}(\rho_2) = \mathrm{Tr}_{y_2}(\rho_1 \otimes |\Phi^+\rangle\langle\Phi^+|)$$

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

$$\rho_0' = U(\mathbb{1}_A \otimes |+\rangle\langle+|_X \otimes |+\rangle\langle+|_R \otimes |0\rangle\langle 0|_S) U^\dagger$$

Clean up time!

SDP max $\langle \Pi_1, \rho_2 \rangle$

$$\mathrm{Tr}_{BC}(\rho_2) = \rho_1 \otimes \mathbb{1}_{y_1}$$

$$\mathrm{Tr}_G(\rho_1) = \rho \leftarrow \text{fixed: } \mathrm{Tr}_S(\rho_0')$$

$$\rho_1 \in \mathrm{Pos}(XRS\underline{G}) \qquad 16 \times 16$$

$$\rho_2 \in \mathrm{Pos}(XRSGY_1\underline{BC}) \qquad 128 \times 128$$

Advantage! The trace out parts are on the ends. This makes the partial trace much tidier! Probably don't need partial trace command now. Only mess: Π.