

CHSH game:-

A

Input: $x \in \{0,1\}$

Output: $a \in \{0,1\}$

B

Input: $y \in \{0,1\}$

Output: $b \in \{0,1\}$

Goal: Ensure $x \oplus y = a \oplus b = x \wedge y$

Constraint: No communication.

Classical with shared randomness: Max Success probability $\leq 3/4$

Quantum: $\cos^2 \frac{\pi}{8} \approx 0.85$ (Can be shown to be optimal)

Given: $p(a,b|x,y)$; there is a "simple" statistical test that separates classically achievable $p(a,b|x,y)$ from the best quantumly achievable distribution.

Q. What if $p(a,b|x,y)$ gives a value 0.89 (bigger than the quantum bound)?

Note:- We do not allow "signalling" if $\sum_b p(a,b|x,y) = \sum_b p(a,b|x,y')$ for y, y' .

There exist a NS distribution which does better than quantum.

x	y	(0,0)	(0,1)	(1,0)	(1,1)
0	0	$\frac{1}{2}$	0	0	$\frac{1}{2}$
0	1	$\frac{1}{2}$	0	0	$\frac{1}{2}$
1	0	$\frac{1}{2}$	0	0	$\frac{1}{2}$
1	1	0	$\frac{1}{2}$	$\frac{1}{2}$	0

~~Given a PRG box,~~ It is impossible to design a randomized box that accepts a real PRG box from a fake one.

However, CHSH gives a promise version of this test, under the assumption that the PRG box consists of two non-signalling entities.

↳ We want to

① Devise a test similar to CHSH not depending upon randomization

② Extract randomness from the CHSH gadget.

Claim: Suppose that $p(a, b|x, y)$ s.t.

① $\Pr(\text{CHSH sat. by } p) \geq \frac{3}{4} + \epsilon$

② $\exists b_0 \Pr(B = b_0) \geq 0.99$

Then: $p(a, b|x, y)$ is signalling.

Guessing game:

A

B

$y \in \{0, 1\}$

Goal: Alice to output y , without communication.

A box satisfying the hypotheses of the claim above would be able to win the guessing game. (At least in the case ① and ② could be moved to "close to 1".)

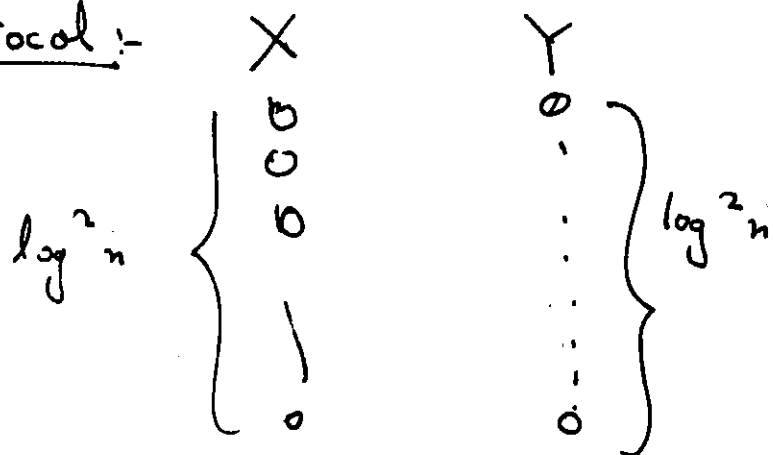
Randomness expansion:

- R'Colbeck '05

- Pironio, Acin, Navascués, ... '10.

t random bits $\rightarrow t^2$ random bits.

Protocol:-



AB
Check: $a \oplus b = 0$
for $> 84\%$ of iterations.

Do n -such blocks, where each block has $(0,0)$ with prob $1-p$ and a random (x,y) with prob p , where p is a highly biased coin ($p \approx \frac{1}{n}$).

$$X, Y, A, B \in \{0, 1\}^{m \log^2 n}$$

CHSH = $\{(x, y, a, b) \text{ that pass the protocol}\}$

Assume No signalling and $\Pr(\text{CHSH}) \geq \frac{1}{n^2}$.

Then $H_\infty^\epsilon(B|\text{CHSH}) \geq \frac{1}{2} \alpha m$ with $\left(\epsilon = \frac{1}{n^2}\right)$

where $\alpha = \frac{1}{1000}$

~~$H_\infty^\epsilon(D)$ can be expressed as a mixture of $(1-\epsilon)$~~

$$H_\infty^\epsilon(D) = \sup_{|D'-D| \leq \epsilon} H_\infty(D')$$

Proof:- Assume $H_\infty^\epsilon(B|\text{CHSH}) \leq \alpha m$

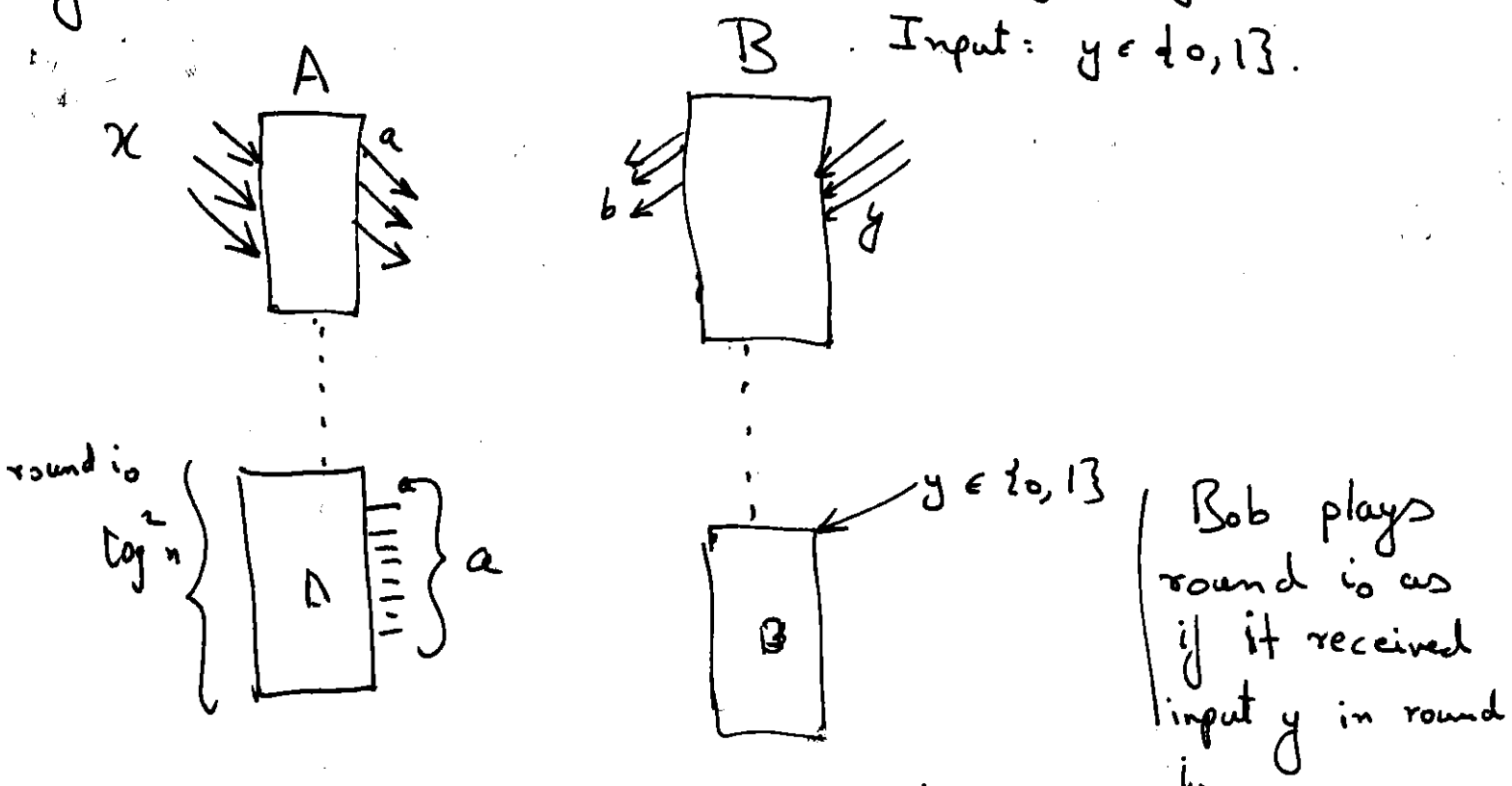
$\Rightarrow \exists \text{BAD s.t. } \Pr(\text{BAD}) \geq \epsilon$
and $\forall b \in \text{BAD}, \Pr(0=b) \geq 2^{-\alpha m}$

Want to show $p(a, b|x, y)$ is signalling.

Claim:- $\exists \tilde{\text{BAD}}, \Pr[\tilde{\text{BAD}}] \geq \frac{1}{2} \Pr(\text{BAD})$
 $\exists i_0 \in [m]$ s.t. (a) $\Pr(\text{CHSH}_{i_0} | \text{CHSH}_{i_0-1, \dots} \text{ and } \tilde{\text{BAD}}_{i_0-1, \dots}) \geq 1 - \frac{1}{100n}$
 (b) $\forall b \in \tilde{\text{BAD}}, \Pr(b_{i_0} = b_{i_0} | b_{i_0-1}, \dots, b_1) \geq 0.99$

The proof of the claim depends upon upon some accounting with the ~~fa~~ hypothesis that the total success probability is $\geq \frac{1}{n^2}$, while ~~the total~~ and that the protocol accepts ~~iff~~ the ~~if~~ and only if there is success in each block.

Assuming the game, we show how to play the guessing game, in order to show that there is signalling.



We can firstly ignore that Bob the part (b) of the claim holds even if the we condition on Bob getting ~~an~~ an input 0 rather than a random input (which happens with prob $p \approx \frac{1}{n}$) in the protocol. ~~Sup~~ Suppose $y = 0$.

Alice looks at a ; if $|a + b_{i_0}| < 20\%$ then claim "Bob's $y = 0$ " else "Bob's $y = 1$ ".

By the CHSH success rate, ~~at~~ $|a + b_{i_0}|$ is expected to be $\approx 15\%$ in case $y = 0$ at

If $y = 1$, then

If $x = 0$ then $|a_i \oplus b_i| \leq 20\%$

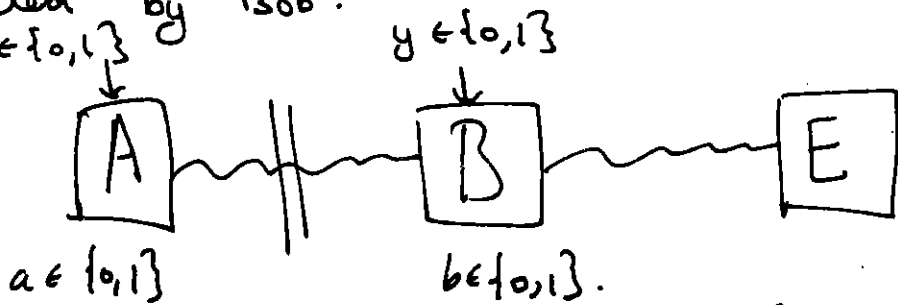
If $x = 1$ then $|a_i \oplus b_i| \geq 80\%$.

Alice says (1, 0) with prob $\frac{1}{2}$ each.

So, Alice succeeds with prob. ≈ 1 when $y = 0$
Alice succeeds with prob. $\approx \frac{1}{2}$ when $y = 1$

— There is signalling. (The required contradiction).

Cryptographic Key Generation:— ~~There is some~~ Consider the same set up tho with Eve entangled with Bob so she could gain information about the bits generated by Bob.



Suppose the combined state of ABC is a GHZ state $\frac{|000\rangle + |111\rangle}{\sqrt{2}}$. Assume:-

- Bob measures in $\{|0\rangle, |1\rangle\}$ basis on input a
- Eve measures in the computational $\{|0\rangle, |1\rangle\}$ basis too.

⇒ E gets access to all bits output by E.

— However the measurement by E completely destroys the entanglement between A and B, and so they would not be able to pass the CHSH test without entanglement.

This phenomenon is called the "monogamy of entanglement." The property of the Φ^+ state that as long as both parties do the same measurement they are guaranteed the same result is not satisfied by any state on 3-parties.

Monogamy of entanglement:

3 parties: A, B, C

w.p. $\frac{1}{2}$ play CHSH between A, B.

w.p. $\frac{1}{2}$ play CHSH between B, C.

Max success (Q) $\leq \frac{3}{4}$ (Quantum)

Max success (NS) $\leq \frac{3}{4}$

[Notice that the idea of using separate Φ^+ pairs between A, B and B, C does not work: since B won't know how which pair to use.]

↓
Recall that for no signalling, it was possible to get prob. of success 1.

Let Z be the output of the protocol, we want

$$\|Z - U_s\|_1 \leq \epsilon$$

(U_s is the uniform distribution on 5-bits)

In fact, to take care of ϵ , we require:

$$\left\| \rho_{ZE} - \left(\frac{1}{2^5} \sum_Z |Z\rangle\langle Z| \right) \otimes \rho^E \right\|_{tr} < \epsilon \quad (*)$$

Min Entropy: $H_\infty(Z) = -\log \frac{1}{2^5}$ [max prob. a sample from Z can be guessed]


Min Entropy: $H_\infty(Z|E) = -\log \frac{1}{2^5}$ [max prob. with which Eve can guess the output of Z]

One can prove $H_\infty(Z|E) \geq \alpha m$ and apply an extractor to get to (*) above.

Extractors :- Ob (1) \Rightarrow \exists Suppose $f: \{0,1\}^n \rightarrow \{0,1\}^m$
 $(n < m)$ s.t. ~~the min-entropy~~ for any distribution X .
 Then look at distribution D which is uniform
 on $f^{-1}(o^*)$ ($\log |f^{-1}(o^*)| > 2^{m-1}$).
 The ~~min Ent~~ $H_\infty(D) = m-1$, and yet the
 output is $\frac{1}{2}$ away from uniform.

Ext. constructions :-

① 2-universal hashing: Choose $p > 2^n$,
 $f(x) = (ax+b, a, b)$, $a, b \in \text{unif } \mathbb{F}_p$.

②  n bits
 $y \in \{0,1\}^{k \log n}$, and output $(x_i, \bigoplus_{j=1}^k x_{ij}, \bigoplus_{j=1}^k x_{i,j+1}, \dots)$
 and then shifted versions \dots)