6.5979 Lecture 5

Thm (Last time): If a ~~strat.~~ $S = (|\psi\rangle, A_{0/1}, B_{0/1})$ wins CHSH w/ prob. $\omega^*_{CHSH} - \varepsilon$ then $\exists$ local isometries V_A, V_B

$$\| (V_A \otimes V_B)|\psi\rangle - |EPR\rangle|aux\rangle\|^2 \le O(\varepsilon^{1/2})$$

$$\| (V_A \otimes V_B)(A_0 \otimes I)|\psi\rangle - (Z \otimes I|EPR\rangle)|aux\rangle\|^2 \le O(\varepsilon^{1/2})$$

$\vdots$

"Robust self-testing"

Self-testing more generally:

- We can self-test arbitrary bipartite $|\psi\rangle_{AB}$, but not very robustly (Coladangelo, Goh, Scarani)

  ε-close $\Longrightarrow$ $\varepsilon \cdot \mathrm{poly}(d)$ close to $|\psi\rangle$

- We can self-test many copies of $|EPR\rangle$
- Can self-test some multipartite states too (e.g. GHZ)
- Self-testing arbitrary measurements?
- Perfect completeness? (which states)
- Robustness for general states
- Are generic games self-tests? (∃ examples w/ non-unique qu. strategy)

Another caveat:
Self-testing is about the "nearly optimal" regime
$0.854 - \varepsilon$

What about $\frac{3}{4} + \varepsilon$

Kaniewski '18:
$\gtrsim 0.764 \Rightarrow$ some overlap w/ $|EPR\rangle$

Valcarce et al. '20
$\lesssim 0.756 \Rightarrow$ no self-testing

Today: applications of CHSH game (& self-testing)

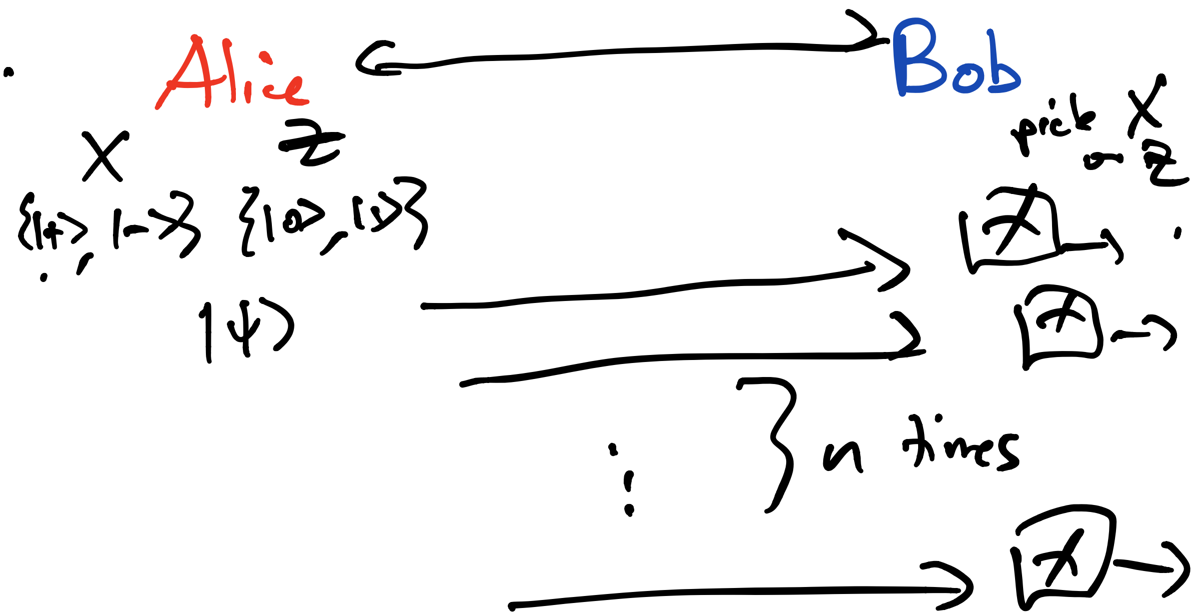
#1: Quantum key distribution (QKD)

Bennett & Brassard '84 BB84

Goal: Alice & Bob want to generate a shared private random string "key"

Private quantum channel
Public classical channel

1.



2. Alice reveal basis settings
Bob reveal basis settings
3. Out of rounds w/ same basis
Alice reveals state for 1/2 of them
4. Use the other 1/2 for your key

This is <u>secure</u> if Alice & Bob's devices are not faulty

<u>Attack "photon number splitting"!</u>

In real world, Alice's qubits are <u>photons</u>

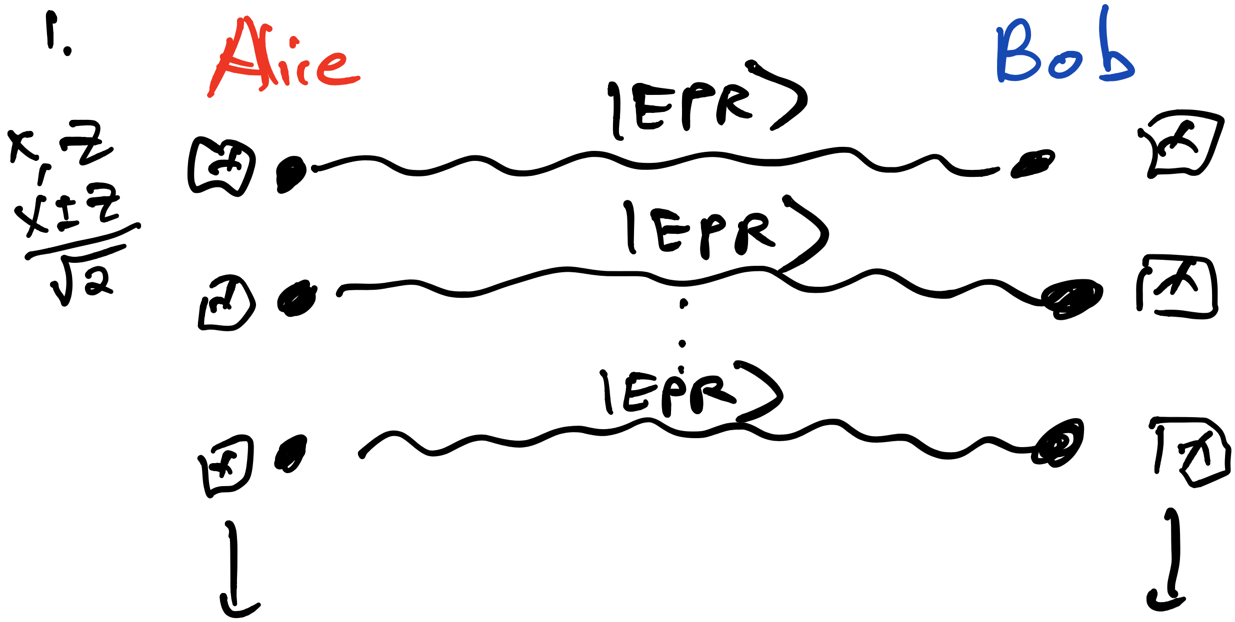
Photon source sometimes generates extra photon

Eve collects extra photons and can learn key

"Device independent security"

Ekert '91

1.



2. Reveal bases

3. Pick a fraction of rounds and test CHSH

4. Out of remaining rounds equal bases $\Rightarrow$ key

"Device-independent security proof"

Success in CHSH rounds

$\Longrightarrow |\psi\rangle_{AB} \approx |EPR\rangle_{AB} \otimes |aux\rangle$

$$|\psi\rangle_{ABE} \approx \underline{|EPR\rangle}_{\underline{AB}} \otimes |junk\rangle_{AB\,\underline{E}} \checkmark$$

$\Downarrow$

Eve's measurement outcomes are uncorrelated w/ Alice & Bob's

"monogamy of entanglement"

If A is highly entangled w/ B, then AB has low entanglement w/ everyone else

History:

- Ekert '91
- Mayers Yao 98
  introduced "self-testing" to quantum
- ....
- Vazirani & Vidick 12
  Play m rounds, can get $0.014 \cdot m$ bits of key out.

What did entanglement buy us?

- Certifiable ← CHSH
- Private ← "monogamy"

Application # 2:

Randomness expansion

random seed $\in \{0,1\}^n$ $\longrightarrow$ $\boxed{\text{Rand. expansion}}$ $\longrightarrow$ random string $\in \{0,1\}^N$

<u>Classically</u>:

"pseudorandom generators"

<u>Quantumly</u>:

Inherent randomness exists

CHSH → <u>certifiable</u> randomness

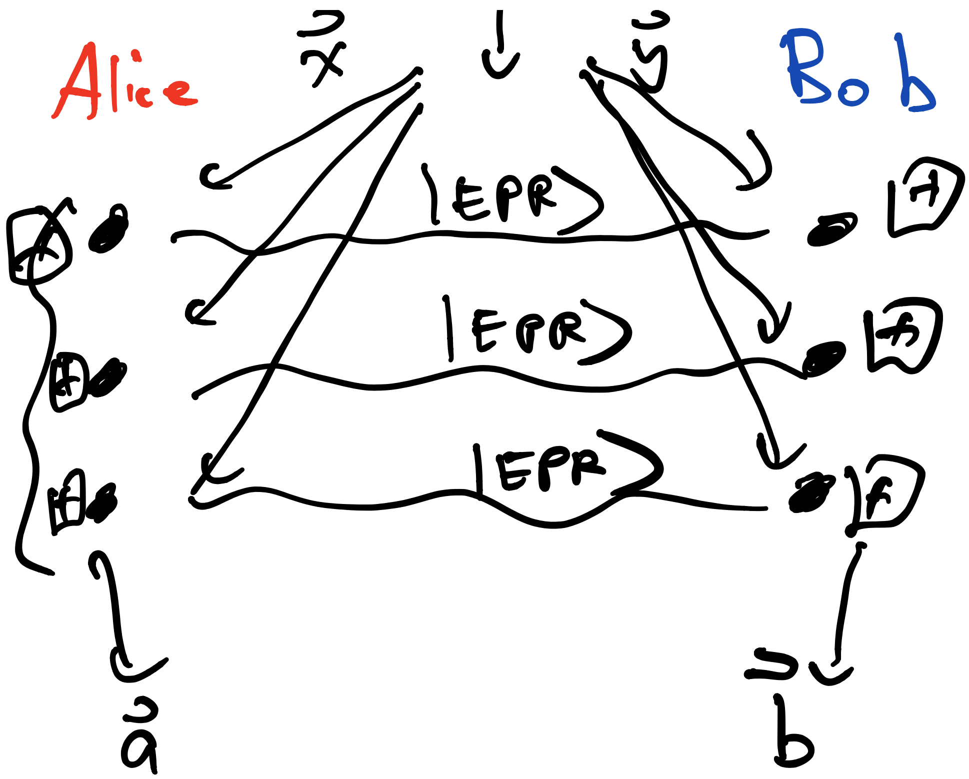
Roger Colbeck '06
Colbeck & Kent '09 $\Big\}$ $n \to kn$

Pironio et al. '10 $\quad n \to O(n^2)$

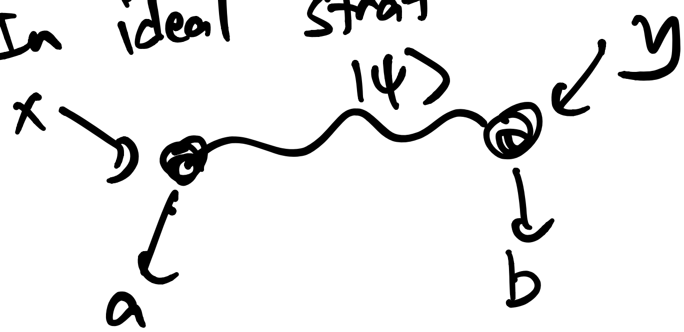
Vazirani Vidick '12 $\quad n \to 2^n$

Miller Shi '14

seed s

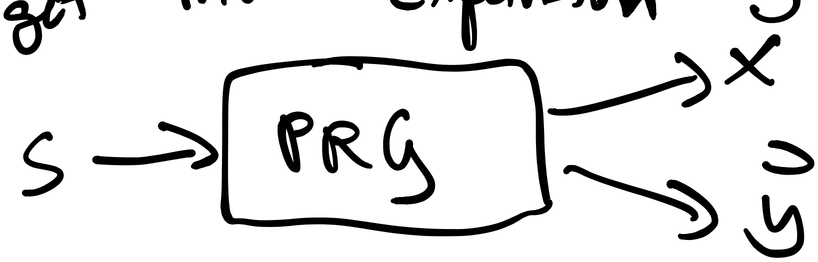


In ideal strat



2 random bits in $\longrightarrow$ 3+... random bits out

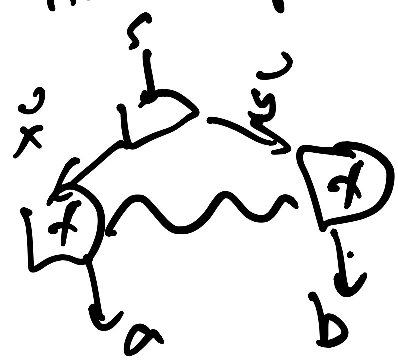
To get more expansion



Upper bound:

Coudron Vidick Yuen

"non-adaptive" can expand at most 2^{2^n}



With adaptivity, get infinite randomness expansion!

Coudron Yuen '14

self-testing   8 parties

V_{RCS}

Chung Shi Wu 4 parties

2 parties is open?

Noise-tolerant version?

Tolerant to realistic noise

General problem w/ self-testing

Other applications:

Self-testing is a "leash" on quantum devices

Delegated qc

Reichardt Unger Vazirani

- Serial repetition of CHSH
- Delegate a quantum circuit of size n using n^{8000} bits of communication

"Verifier on a leash"

Coladangelo Grilo Jeffries Vidick '16

- Use a generalization of CHSH called Pauli Braiding Test

Delegate size n circuit w/ $n \log n$ resources

- Understanding "quantum correlations"

Interactive proofs w/ quantum provers

Next time:

Detour to Magic Square game

Contextuality