

Fully Device-Independent Quantum Key Distribution

Thomas Vidick,
Massachusetts Institute of Technology

Joint work with Umesh Vazirani, UC
Berkeley

CHSH Game



Input: $x \in_R \{0,1\}$
Output: $a \in \{0,1\}$

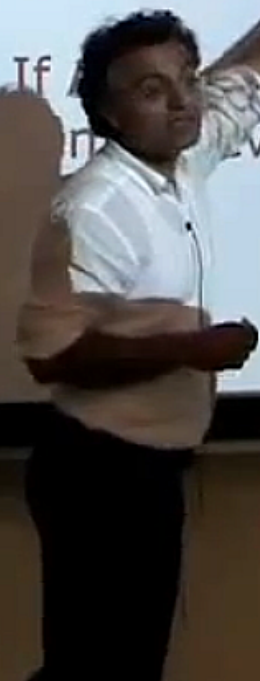


Input: $y \in_R \{0,1\}$
Output: $b \in \{0,1\}$

Maximize $\Pr[xy = a+b \pmod{2}]$

Classically it is impossible to do better than 0.75

If Alice and Bob share entangled qubits, then they can achieve success probability $\cos^2 \pi/8 \approx 0.85$



Quantum key distribution

Two main approaches:

1. Prepare-and-measure [BB'84, Bennett'92]

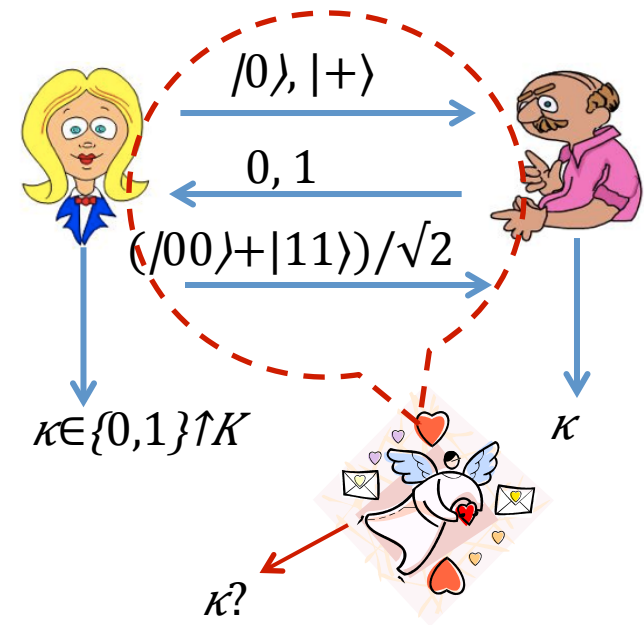
- Alice sends photons encoded in comp. or Had. basis
- Bob measures in random basis
- key \mathcal{K} : identical bases \rightarrow identical outcomes
- Uncertainty principle: Eve cannot learn information without disturbing the state

2. Entanglement-based [Ekert'91]

- Alice prepares EPR pairs and sends half of each to Bob
- Alice measures in comp., Had. or $\pi/8$ basis. Bob measures in Had., $\pi/8$ or $3\pi/8$
- key \mathcal{K} : identical bases \rightarrow identical outcomes
- Verification of CHSH violation ensures Eve has not tampered with the EPR pairs

Search for rigorous security proofs has spawned host of novel theoretical works

- [Mayers'96, Koashi'06] Uncertainty relations
- [LC'99, SP'00] Entanglement distillation, error-correcting codes
- [Renner'05] Conditional entropy measures, privacy amplification



Unconditional security?

QKD is major field of experimentation

- Dedicated fiber optic networks (SECOQC; Tokyo)
- Free-space links (Zelinger, Vienna; Pan, Heifei)
- Satellite-based relays
- Commercially available systems (idQuantique; MagiQ)



Unconditional security is major selling point. But what if...

- » Alice or Bob's measurement bases are misaligned?
- » Alice's device generates not one but many photons, some of which go to Eve (e.g. information copied in extra degrees of freedom)?
- » Bob's detector can be controlled to only register certain events?

Security of QKD critically depends on quality of devices

[Home](#)[News](#)[Blog](#)[Multimedia](#)[In depth](#)[Jobs](#)[Events](#)

News archive

[▶ 2013](#)[▶ 2012](#)[▼ 2011](#)[▶ December 2011](#)[▶ November 2011](#)[▶ October 2011](#)[▶ September 2011](#)[▶ August 2011](#)[▶ July 2011](#)[▶ June 2011](#)[▶ May 2011](#)[▶ April 2011](#)[▶ March 2011](#)[▶ February 2011](#)[▶ January 2011](#)[▶ 2010](#)[▶ 2009](#)[▶ 2008](#)[▶ 2007](#)[▶ 2006](#)

Hackers steal quantum code

Jun 17, 2011 [5 comments](#)



Bag of quantum tricks

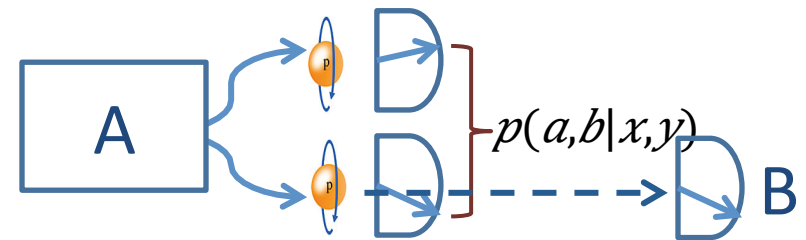
While in principle unbreakable, quantum cryptography is known to have weaknesses in practice. One shortcoming has now been graphically illustrated by physicists in Singapore and Norway, who have been able to copy a secret quantum key without revealing their presence to either sender or receiver. The researchers are now working to remove the loophole they have exposed.

The challenge of device independence

Can we **guarantee security without making assumptions on the QM devices?**

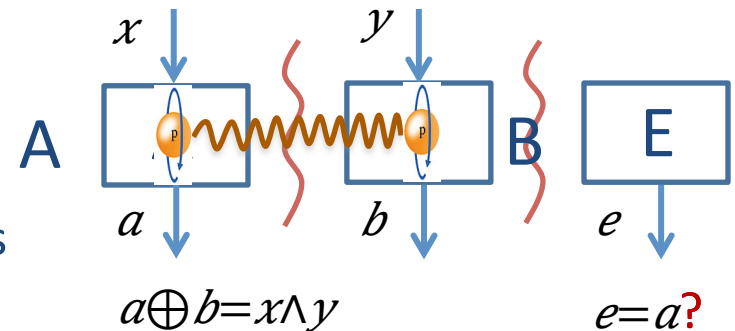
- [MY'98] propose self-checking of the photon source

- Observing the correct correlations guarantees generation of EPR pair
- Result not robust: need to check for *exact* correlations



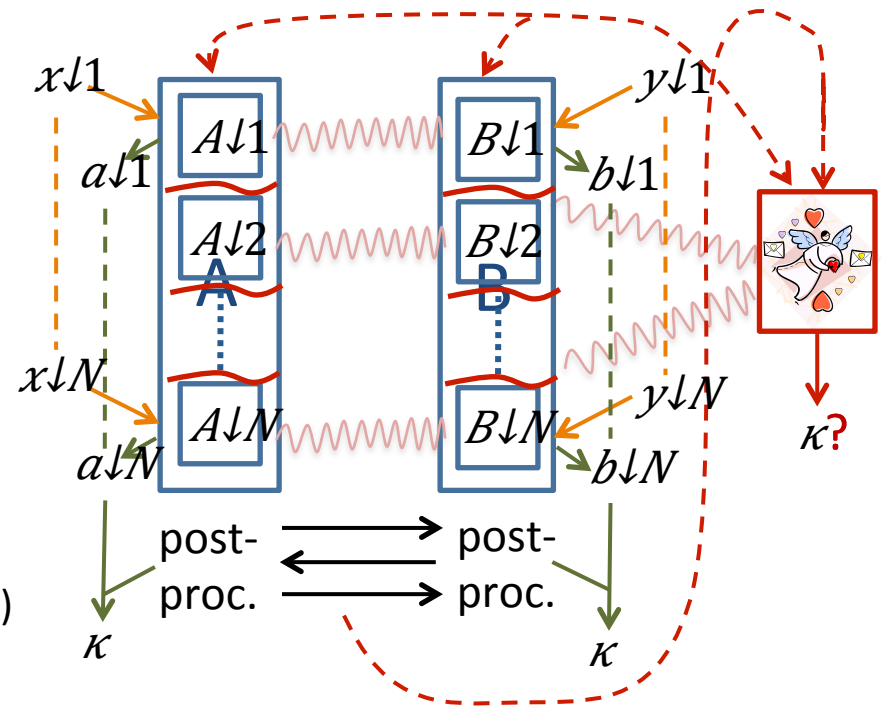
- [BLM+'05, BHK'05]: No need to fully characterize systems

- Key observation [Eke'91]: **violation of Bell inequality implies privacy**
- General argument in no-signaling setting
Manifestation of *monogamy* of correlations



The DIQKD challenge

- Devices designed by adversary Eve
- Execute protocol. No signaling between labs, but all communication public
- Goal: protocol does not abort
 - A,B share identical secure key κ
- Targets: efficiency, noise tolerance
(“honest” devices allowed to err 1% of the time)



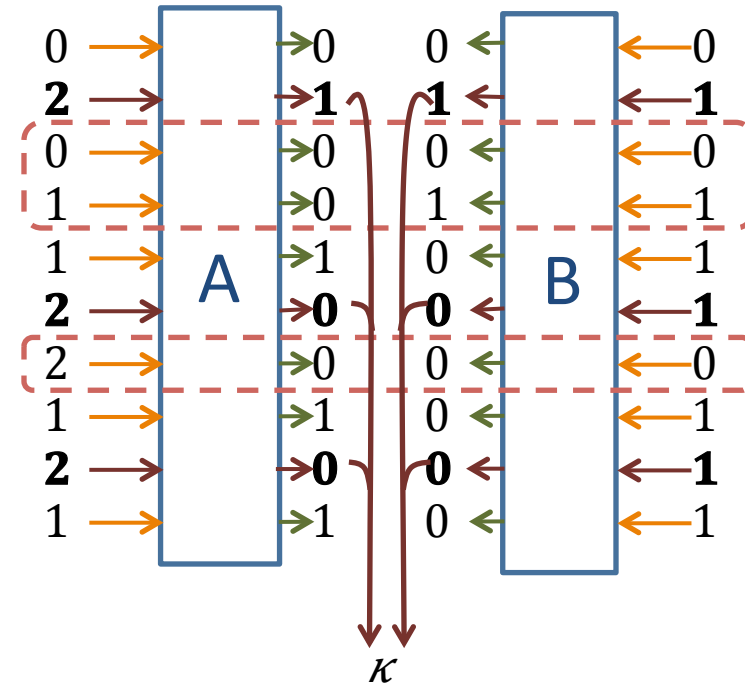
- Previous work: Security against collective attacks, but for $(2N+1)$ devices
 - [AGMMPS+'05-09] sharp quantitative results for no-signaling adversaries.
 - [ABGMPS+,HR'07-11] better rates for quantum adversaries
- [BCK'12a,RUV'12]: DIQKD possible without additional no-signaling assumptions
 - Protocols inefficient, vanishingly small noise tolerance
- [This work] DIQKD can be achieved in a realistic setting
 - [BCK'12b] No independence + noise \Rightarrow open door for elaborate adversarial strategies

A protocol for efficient DIQKD

Result: **an efficient, noise-tolerant protocol secure against arbitrary quantum devices & adversary**

Simple variant of [Eke'91]. N rounds:

- A takes inputs in $\{0,1,2\}$, B in $\{0,1\}$
 - Inputs (0/1, 0/1): CHSH $a \oplus b = x \wedge y$.
 - Inputs (2,1): identical outputs
- Check correlations in random subset of rounds
 - Communicate inputs/outputs
 - Abort if violation $< \text{opt} - \eta$ (“noise”)
- Raw key extracted from (2,1) rounds
 - Final key obtained after information reconciliation and privacy amplification

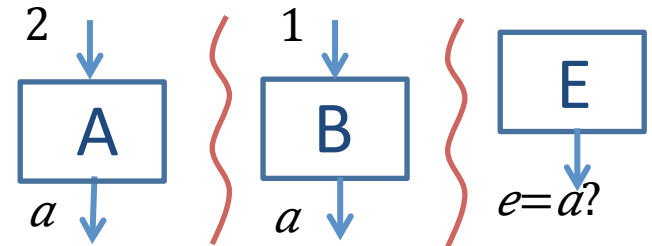


Thm: w.p. $\geq 1 - \epsilon$, a key κ of length $\approx 0.3(N/6)$ is extracted such that $\|\rho \downarrow KE - U \downarrow K \otimes \rho \downarrow E\| \leq \epsilon$
 (devices subject to $\eta \leq 2\%$ noise are accepted w.p. $\geq 1 - \epsilon$)

The basic intuition

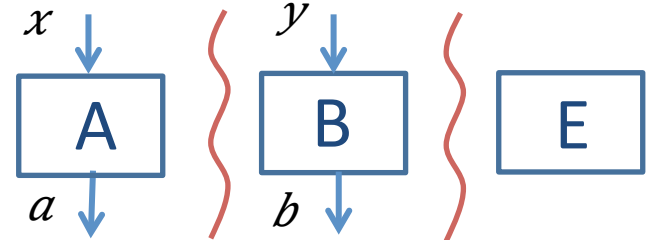
- Adversary's goal: create devices such that, in any round:

- Inputs are (2,1): she obtains the same output as both players



- Inputs are (0/1,0/1): the devices satisfy the CHSH condition

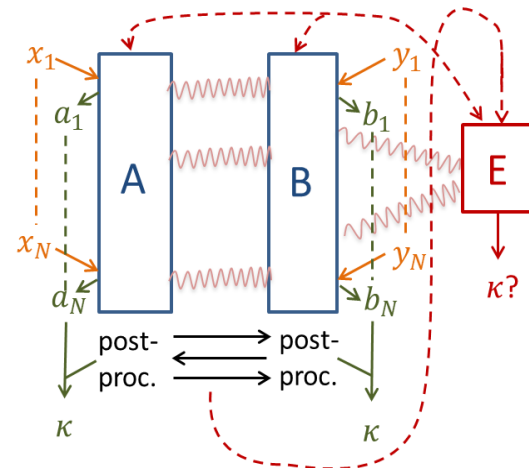
\rightarrow EPR pair $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$



$$a \oplus b = x \wedge y?$$

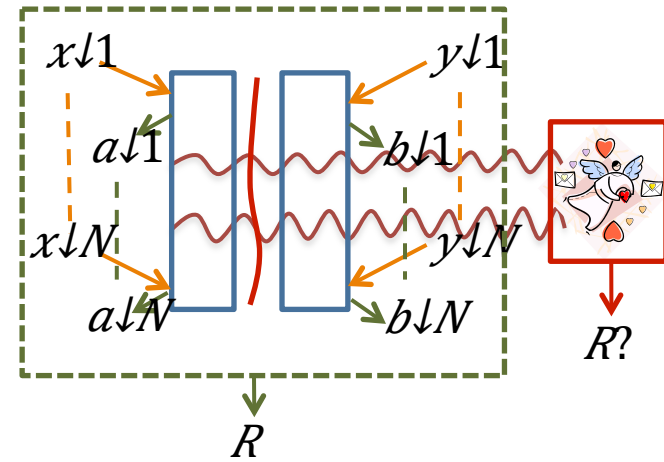
- No state is simultaneously “EPR-like” and “GHZ-like”!
- Monogamy statements are notoriously hard to formalize

- Eve is not restricted to attacking individual rounds separately
- Breaking the protocol only requires to obtain diffuse information about all rounds (e.g. a few parities)
- The protocol leaks substantial amounts of information



Generating certified randomness

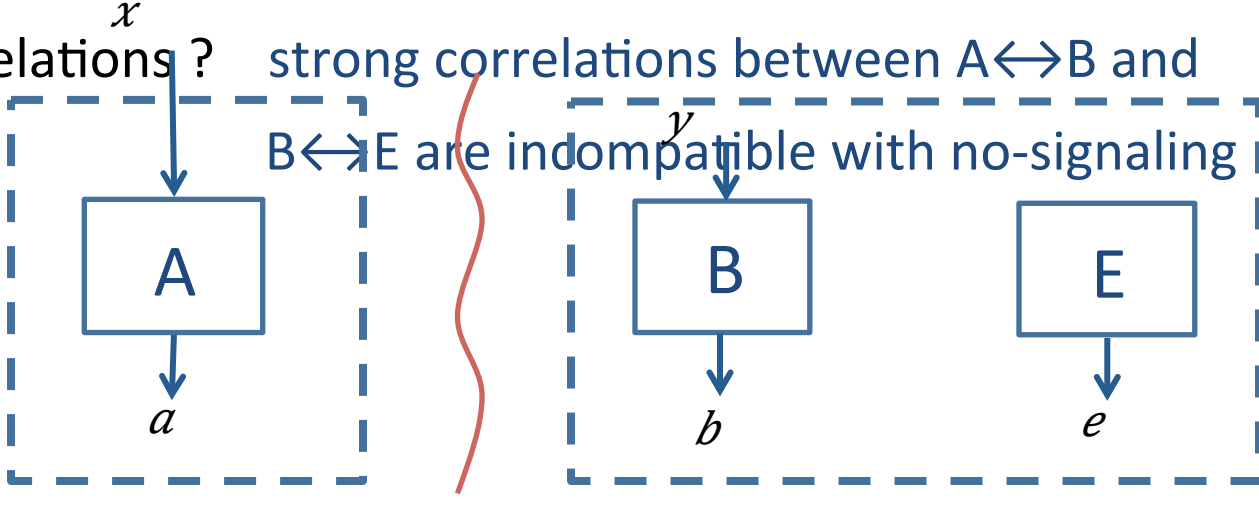
- Trusted random bits are prerequisite for QKD
(Generated key should appear random to Eve)



- [Col'09,PAM+'10]: randomness certified based on average Bell violation
 - No independence assumption
 - Classical adversary only
- [VV'12]: extend to quantum adversaries
 - Protocol tailored to randomness generation, no noise tolerance
 - Two useful tools:
 - The “guessing game”, or how to think about monogamy
 - The “quantum reconstruction paradigm”, or how to leverage the adversary’s low distinguishing probability

1. The guessing game

- Monogamy of quantum states: $\rho \downarrow AB = |\psi \downarrow EPR\rangle \langle \psi \downarrow EPR| \Rightarrow B, E$ uncorrelated

- Monogamy of correlations? strong correlations between $A \leftrightarrow B$ and $B \leftrightarrow E$ are indompatible with no-signaling
- Simple scenario:
 

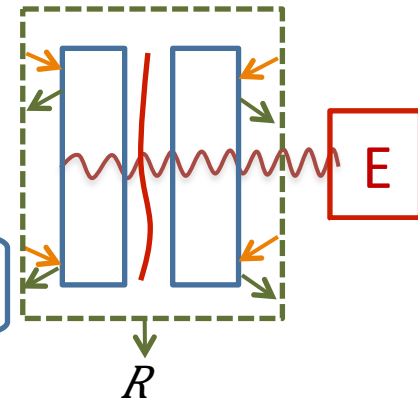
$a \oplus b = x \wedge y?$ $e = a?$

- Set $v=1 \Rightarrow a \oplus b = x \wedge v = x$, and $e = a$ so $e \oplus b = x$

2. The quantum reconstruction paradigm

- Eve's "information" about R quantified by $H_{\infty}^{\epsilon}(R|E)$

Smooth conditional min-entropy quantifies E 's ignorance about R



Lemma [DVPR'11]: Assume $H_{\infty}^{\epsilon}(R|E) \ll 0.1N$.

There exists $\approx 0.1N$ "advice bits" $g \downarrow Adv(R)$ such that, given $g \downarrow Adv(R)$, Eve can guess R with success $poly(\epsilon/N)$

- Introduced in [Tre'01] to analyze classical extractors
- [DV'11, DVPR'12] Generalization to quantum setting requires more work: reconstruction involves repeated measurement of E
- [KT06]: can assume Eve applies specific measurement (PGM)
→ simultaneously refines all required measurements

Back to the DIQKD protocol

- A takes inputs in $\{0,1,2\}$, B in $\{0,1\}$

- Inputs (0/1, 0/1): CHSH $a \oplus b = x \wedge y$.

- Inputs (2,1): identical outputs

- Check correlations in random subset of rounds

- Communicate inputs/outputs

- Abort if violation $< \text{opt} - \eta$ ("noise")

- Raw key extracted from (2,1) rounds

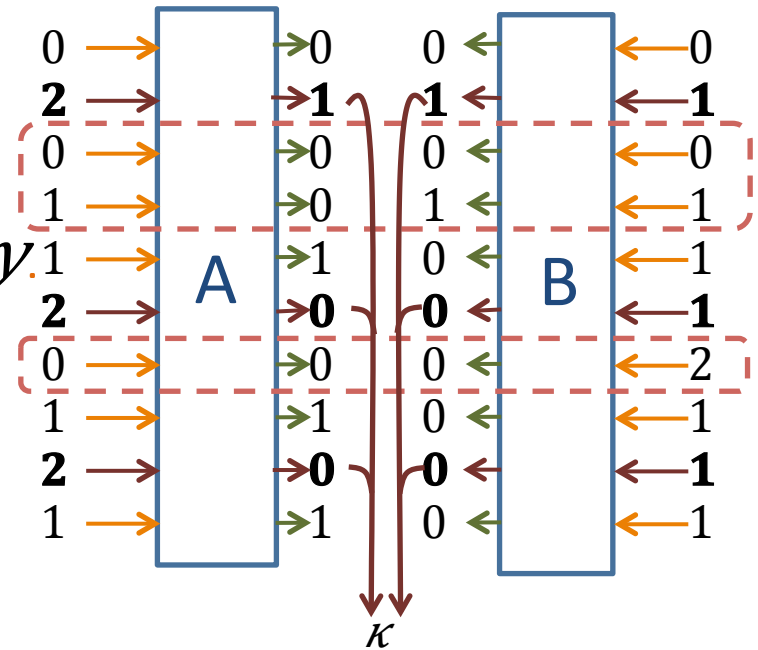
- Suppose Eve can distinguish \mathcal{K} from uniform with advantage $\epsilon \approx$

$$2^{-c} \downarrow 0 \quad N$$

- Reconstruction paradigm: she can recover B's raw key

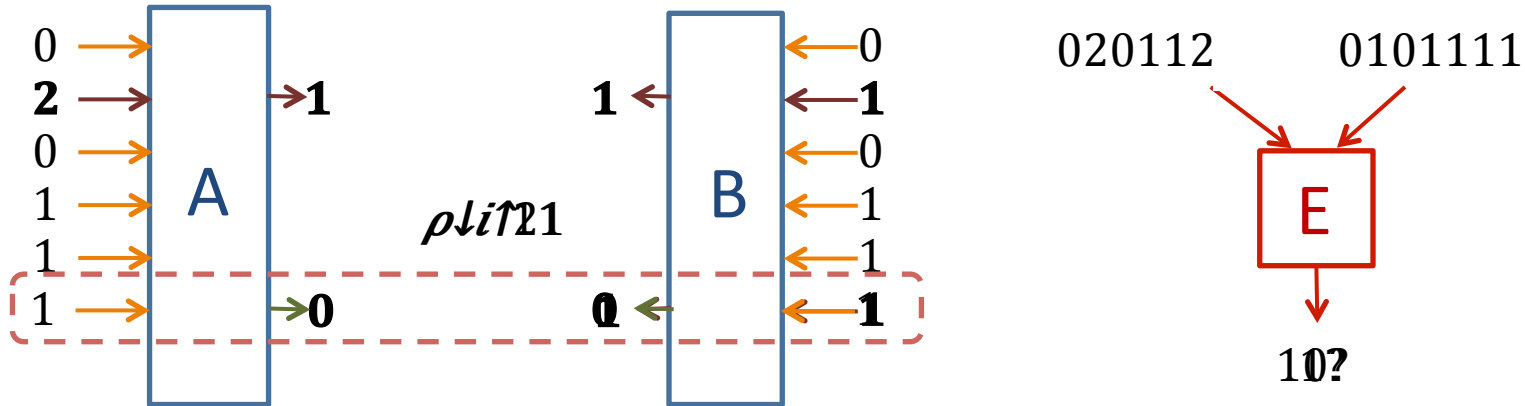
$$\Pr \text{Eve guesses } b \downarrow 1 \dots b \downarrow N \text{ public info. + advice} \geq \epsilon \approx$$

$$2^{-c} \downarrow 0 \quad N$$



3. Identifying a “good” round

- Suppose Eve can guess $b \downarrow 1 \dots b \downarrow N$ with small success ϵ
 $\rightarrow \exists$ round i such that $\Pr_{\text{guess } b \downarrow i} \text{ guess } b \downarrow 1, \dots, b \downarrow i-1} \geq 0.99$



- Eve's measurement may depend on inputs to i -th round
- Eve's prediction correct on $\rho \downarrow i \uparrow 21$, CHSH violation on $\rho \downarrow i \uparrow xy$ for $x, y \in \{0, 1\}$
- No contradiction in “guessing game” unless $\rho \downarrow i \uparrow xy \approx \text{independent}(x, y)$
 - Suppose $\rho \downarrow i \uparrow xy$ carries a lot of information about xy
 - Use coding argument to argue Eve could signal to (A, B)
- Completes reduction to guessing game: reach contradiction \rightarrow security

Summary

- Variant of Ekert's protocol secure for DIQKD with quantum adversary
- Efficient: linear key rate, tolerates constant noise
- Proof introduces tools to manipulate quantum adversary. Three steps:
 - **Reconstruction paradigm**: leverage adversary's limited & diffuse information
 - Identify "good" round, in which Eve can guess B's output bit
 - Use tools from information theory to **bound correlations from conditioning**
 - **Guessing game**: intuitive way to make final monogamy statement

Some questions

- Improve analysis & apply to other settings
(two-way protocols; meas-device-indep. protocols)
- Technical statement intermediate between "robust testing" and "privacy of no-signalling correlations". **What is the most appropriate level of granularity?**
- **New tools for study of monogamy**, but much more needed to really understand its extent in complex interaction scenarios