Trustworthy Quantum Information

Yaoyun Shi
University of Michigan

MICHIGAN ENGINEERING
UNIVERSITY OF MICHIGAN

National Science Foundation
WHERE DISCOVERIES BEGIN

QI 2.0

QI 2.0

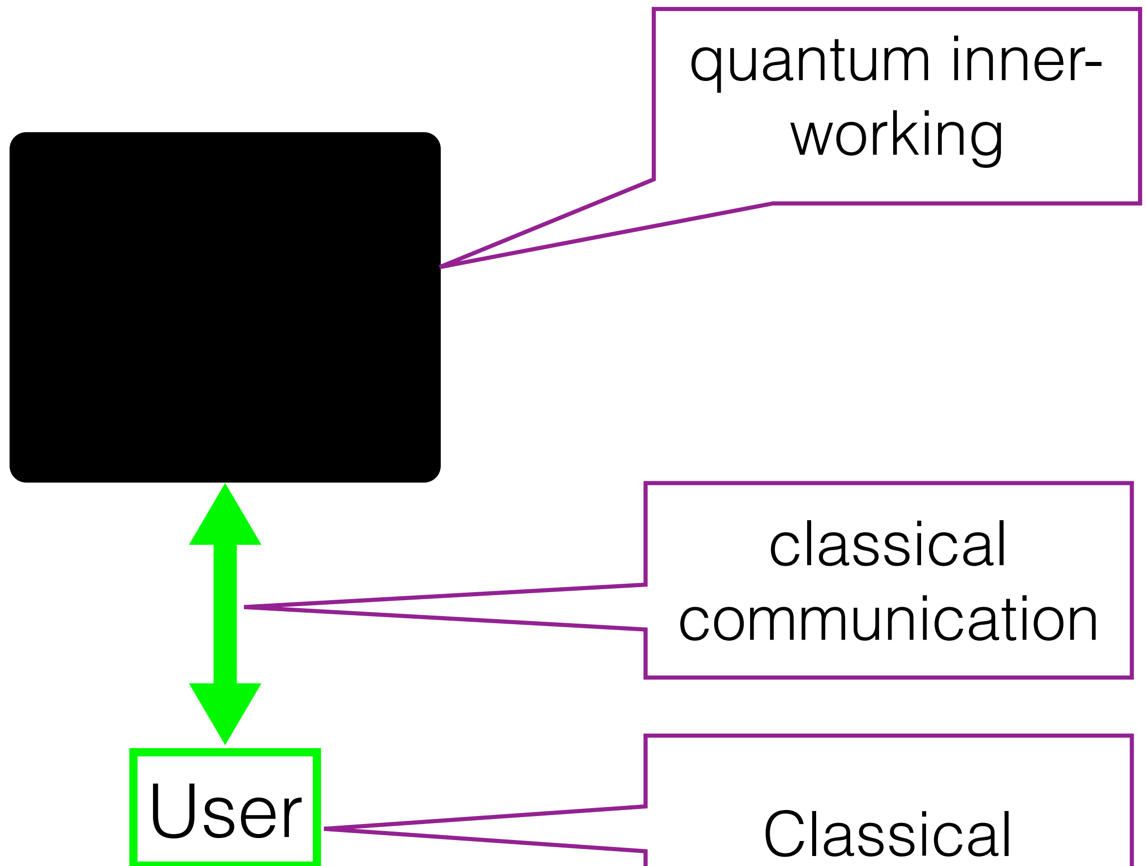
Some hairy questions

QI 1.0: using trusted q. device

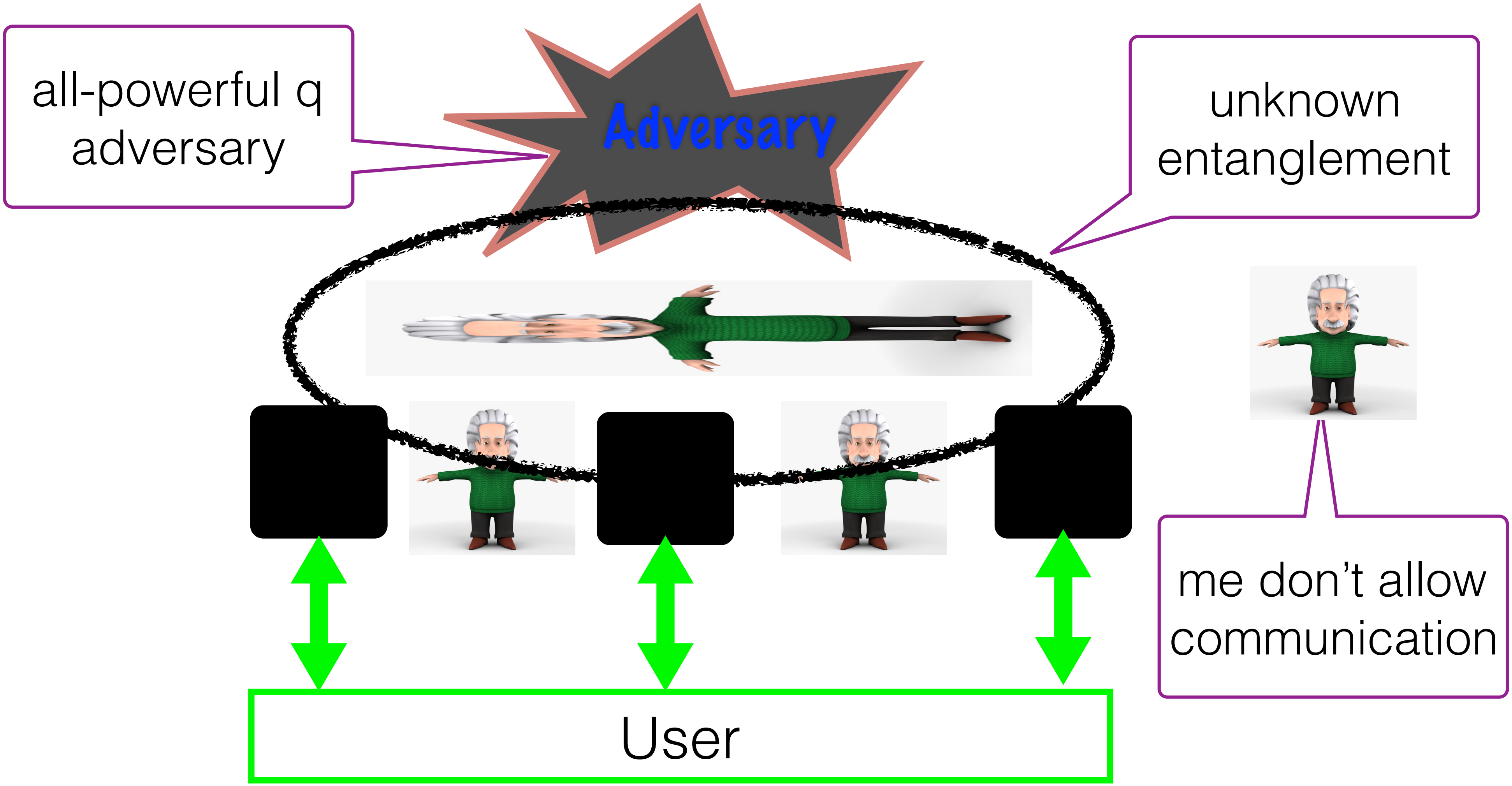
QI 2.0: using untrusted q. device

The device(s) prove to you their trustworthiness

Untrusted quantum device



Untrusted quantum devices



The question: What can we do with untrusted quantum devices?

Why should we care?

- We mortals are classical beings, can’t directly experience quantum states or operations
- Is this working according to specs?
- What if the device has been tampered with?
- Could there be harmful quantum side information?
- Pioneered by Mayers & Yao [98], Barrett, Hardy & Kent [05]

Q1. Self-testing

Can we know the unknown?

$\boxed{\text{Can we know the unknown?}}$

Self-testing (Rigidity): classical interaction uniquely determines the quantum inn-working

The CHSH Game

x	y	win if
0	0	a=b
0	1	a=b
1	0	a=b
1	1	a!=b

- CHSH Game: $x, y, a, b \in \{0, 1\}$
- Classical Strategy: share randomness, apply deterministic function
- Quantum Strategy: share entanglement, apply local measurement
- When x, y are uniform, the prob. of winning
  - OPT(classical) = 3/4
  - OPT(quantum) = $\cos^2$Pi/8≈.853

Self-Testing/Rigidity of CHSH

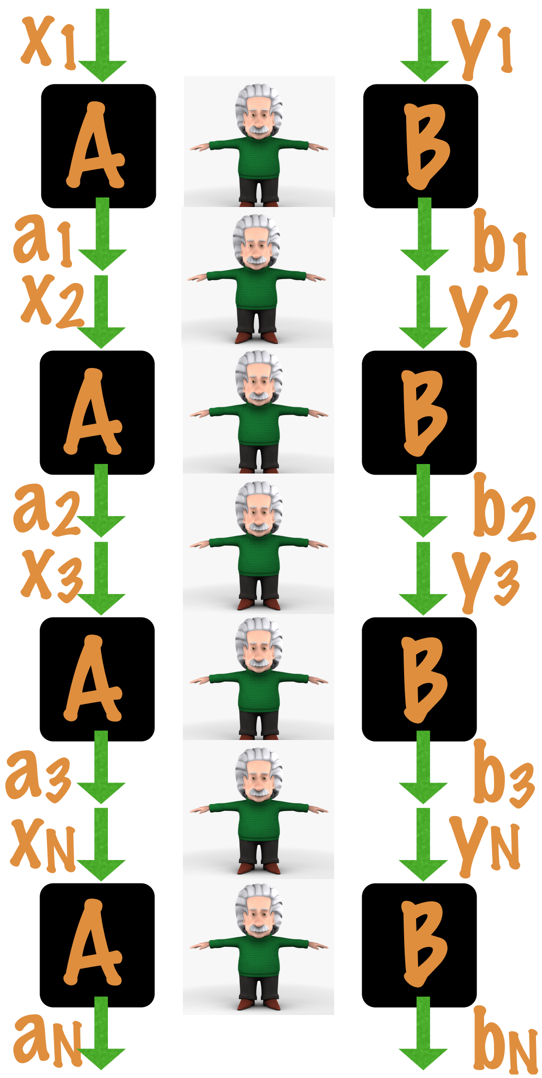
- There is a unique OPT q. strategy. (Popescu-Rohrlich92)
- Any approximately OPT q. strategy must be close to the OPT q. strategy (McKagueYS12, MillerS12, ReichardtUV12)

Other self-testing results

- Concepts proposed by Mayer-Yao98, BardynLMMS09
- Several other states are robust self-testing

- Q1.1 Which games are (robust) self-testing?
  - All games with a q. advantage?
- Q1.2 Which states can be (robustly) self-tested?
  - All pure entangled states?

Sequential games



- The same devices sequentially play the game
- Count the winning frequency f
- If f ≈ OPT(quantum), what can we say the strategy?

Sequential games

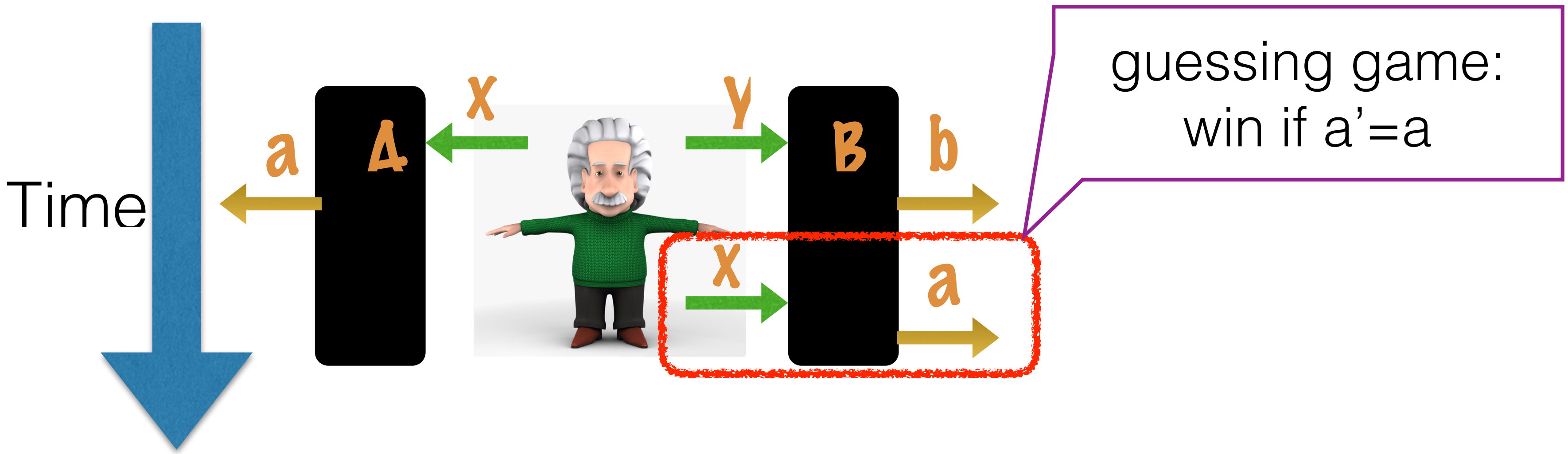
If f is essentially OPT(q.), the strategy for a random subsequence of a substantial size must be close to OPT q. strategy. (ReichardtUV12)

- What if OPT-f=const?
- Q1.3: Characterize close-to-OPT sequential strategies

Parallel games

Q1.4 Characterize close-to-OPT parallel strategies.

Rigidity of quantum causality



- Non-local games are special cases of quantum causal relations
- Winning the guessing game prob.=1, the first stage strategy must be essentially classical (MillerS16)

Q1.5 Which causal relations are (robust) self-testing?

Q2. Certifiable Randomness

Is cryptography possible?

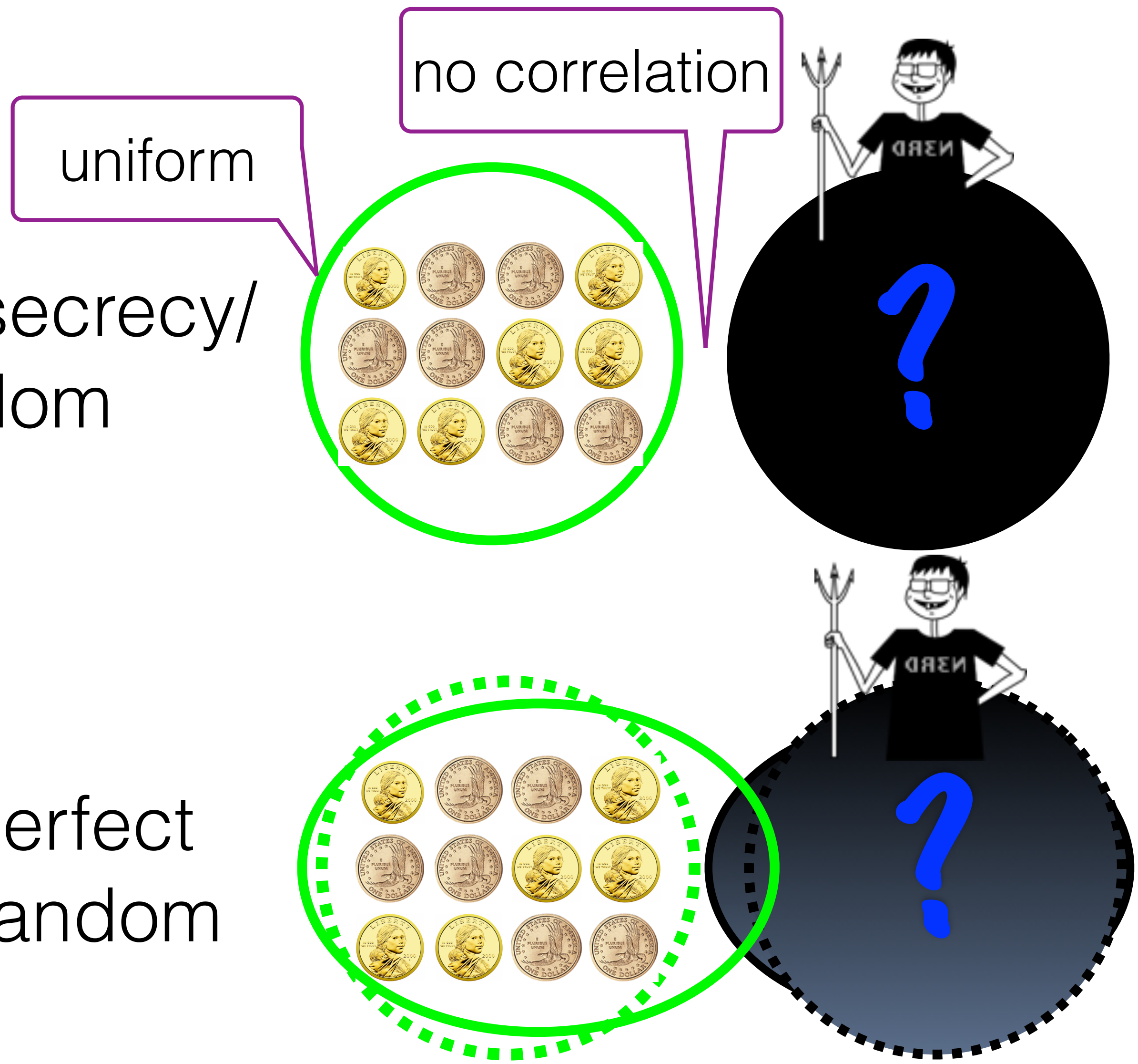
Q2. Certifiable Randomness

Is randomness possible?

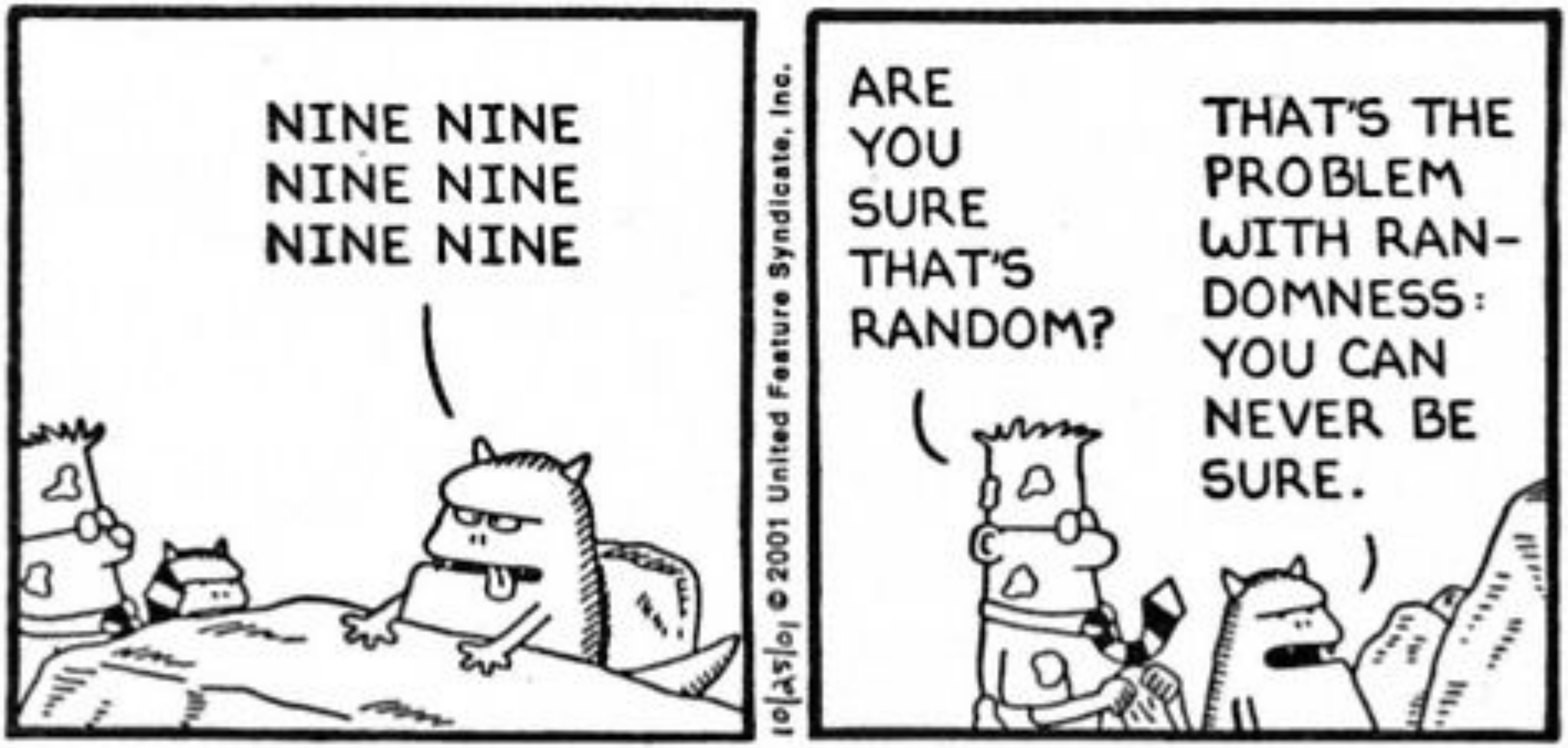
Randomness = Secrecy

Perfect secrecy/
random

Almost perfect
secrecy/random



Randomness is a faith

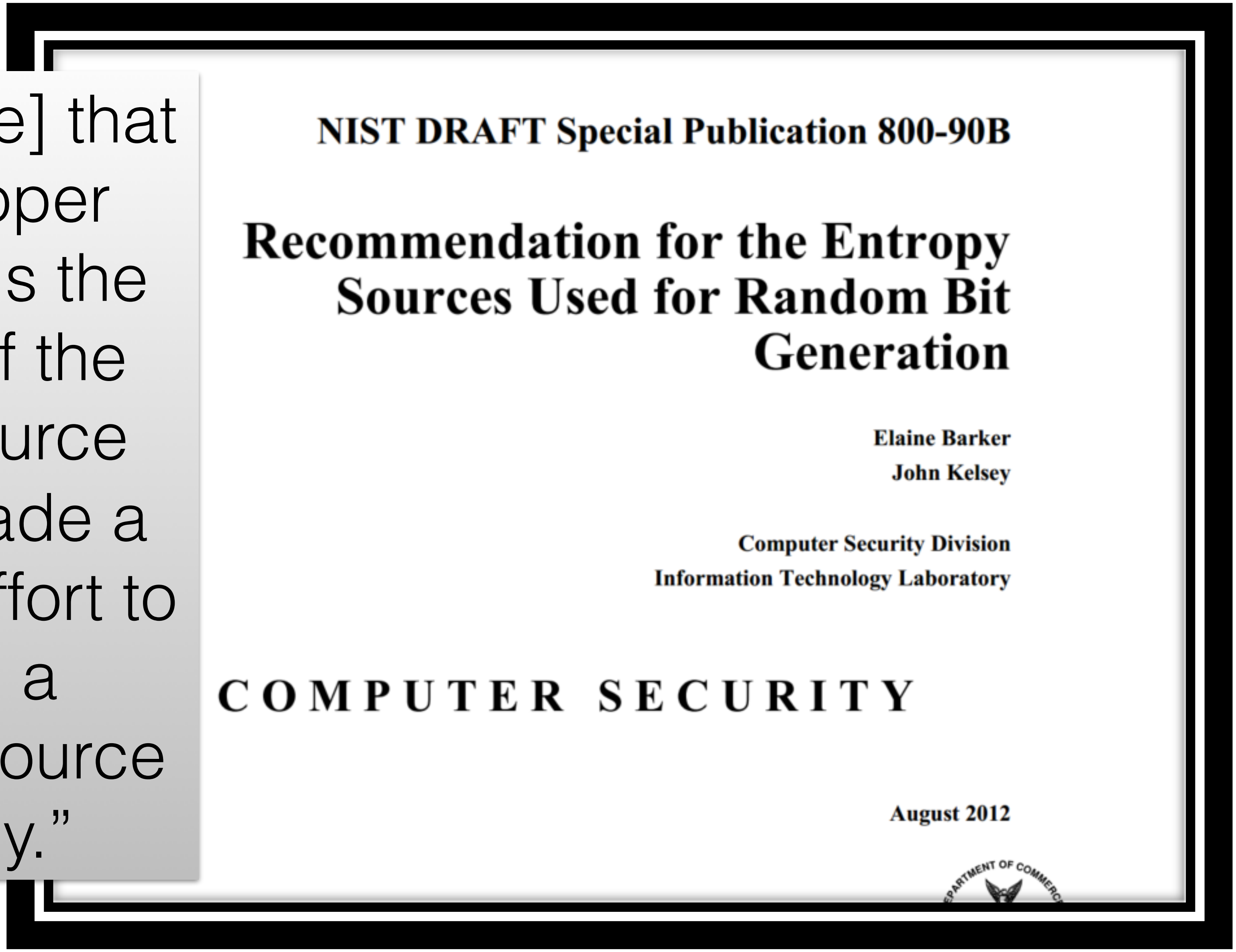


Randomness is impossible to test directly

- All randomness test is a binary function
  - Always says “Random” on any fixed input from the acceptance pre-image

Randomness is a faith

"[We assume] that the developer understands the behavior of the entropy source and has made a good faith effort to produce a consistent source of entropy."



NIST DRAFT Special Publication 800-90B

Recommendation for the Entropy Sources Used for Random Bit Generation

Elaine Barker
John Kelsey

Computer Security Division
Information Technology Laboratory

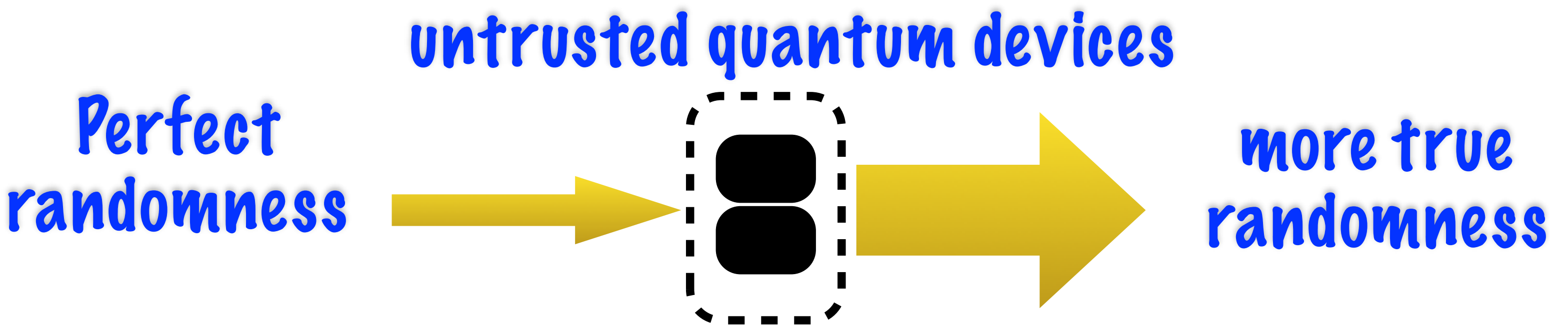
COMPUTER SECURITY

August 2012

What are the minimal assumptions for generating randomness?

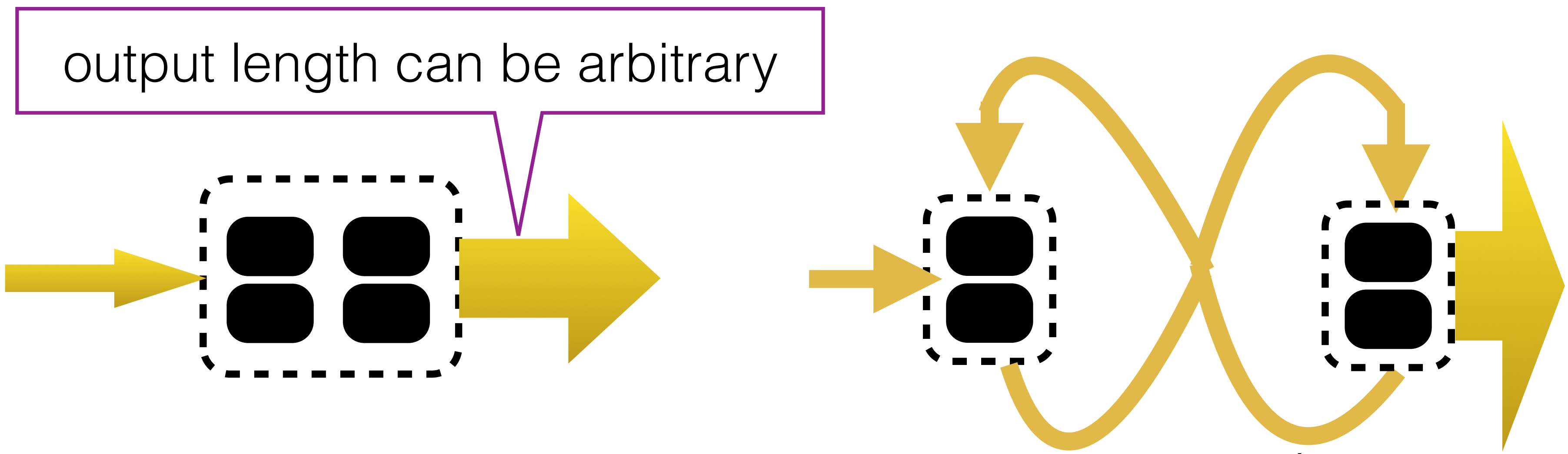
- There may be incomparable sets of “minimal” assumptions
- Trusted quantum device gives a trivial answer
- What if we don’t trust the quantum devices?
  - Must assume the existence of randomness

Randomness Expansion (Colbeck06, Colbeck&Kent11)



- Known: 2-device, exponential expansion (VaziraniVidick12), robust, cryptographic level of security (MillerS14)

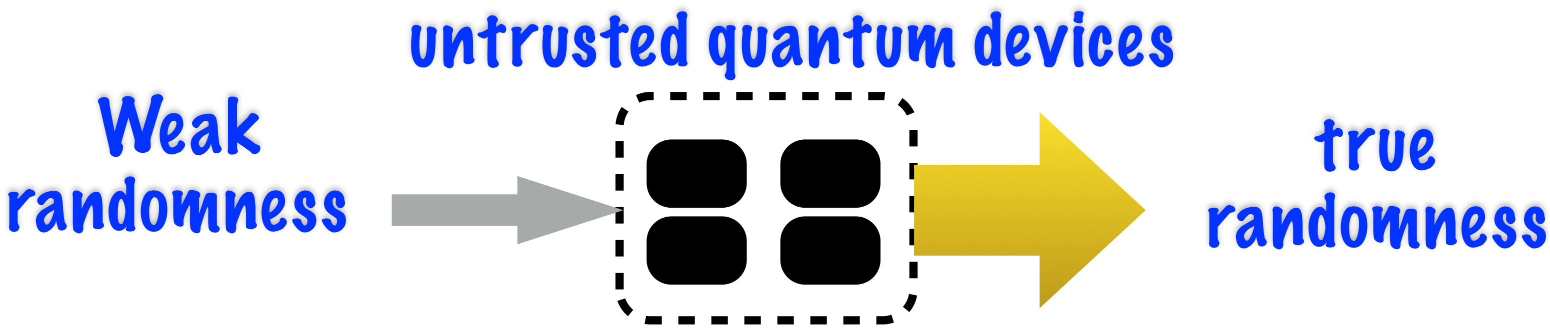
Unbounded Expansion



Known: 8 devices (Coudron&Yuan14); 4 devices (and robust) (MillerS14, ChungCS14)

Q2.1 What is the minimum number of devices required for unbounded expansion?

Randomness Amplification
(Colbeck&Renner12)



Known: uses a single min-entropy source (the most general weak source) but not efficient (ChungSW14)

- Q2.2 Is there an efficient protocol?
- Efficient = cryptographic-level security

Other questions

- Q2.3 Are there secure parallel protocols for randomness expansion, unbounded expansion, and min-entropy source amplification?
- Q2.4 What is the lowest possible detector efficiency to observe a Bell violation?

Q3. Lifting Security

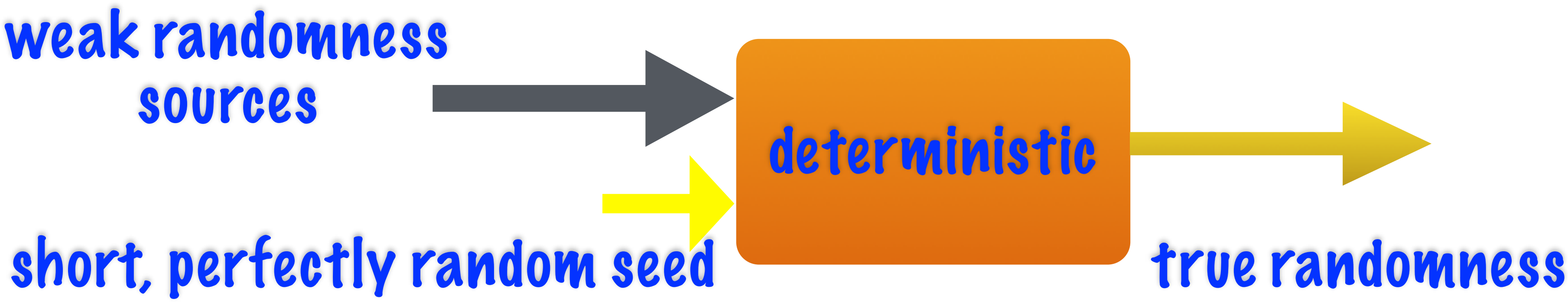
Could classical security imply quantum security?

From classical security to quantum security

- Untrusted-device (Device-Independent) protocols are typically simple
- Quantum-security proofs are quite difficult
- Classical-security is relatively simple

- Q3.1 Is there a general principle translating classical security to quantum security?
- Restrict to the states from the protocols

Classical (seeded) randomness extractors



- Randomness extractors: deterministically transform weak sources to true randomness
- Requires two independent sources
- Well-understood when one source (seed) is uniform
    - The seed length can be made very small
    - A random function is an ideal extractor
    - Explicit near-ideal contractions are known

Quantum-proof classical extractors

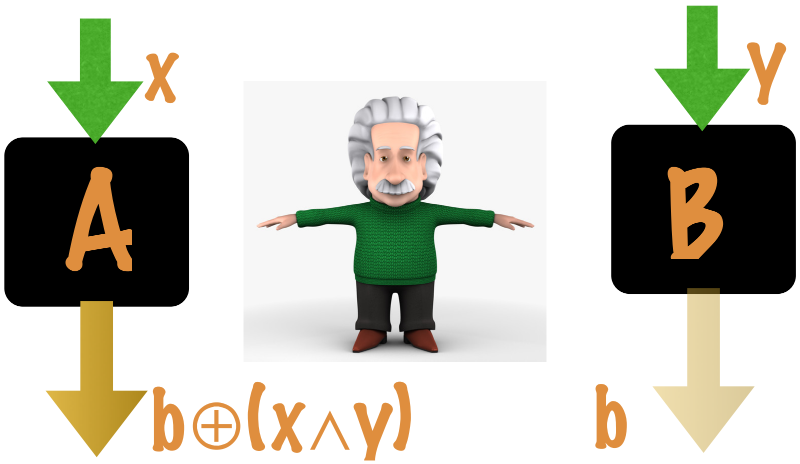
- Quantum security: adversary has quantum side information
- Known: many classically-secure extractors are also quantum-secure but these don’t have the ideal pars

- Q3.2 Are all classically-secure extractors quantum-secure?
- Q3.3 Are most functions an ideal quantum-proof extractor?

Q4. Non-signaling security

A non-signaling information theory?

Non-signaling

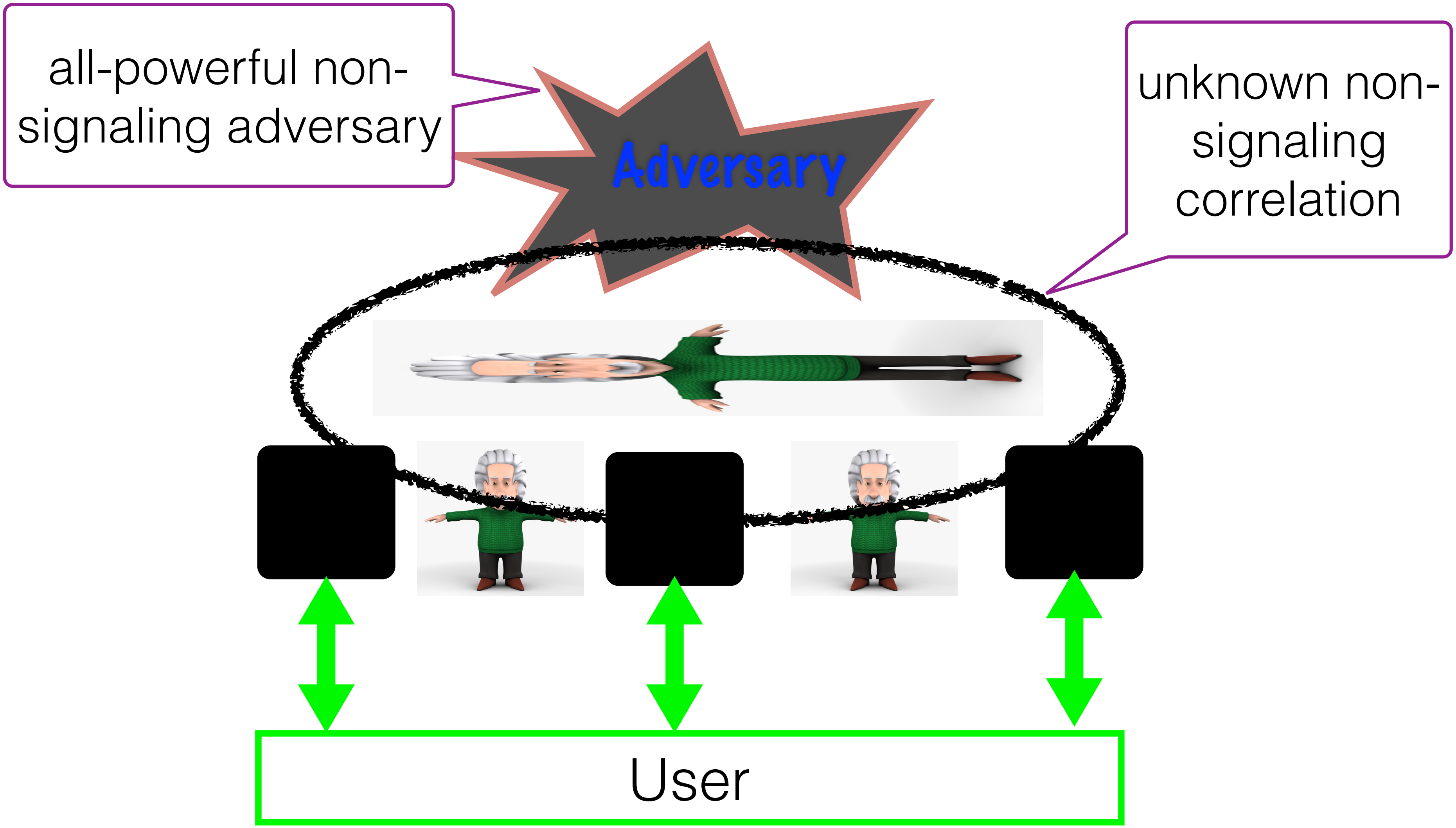


x	y	output distr
0	0	(0,0), (1,1)
0	1	(0,0), (1,1)
1	0	(0,0), (1,1)
1	1	(0,1), (1,0)

PR box

- No-signaling boxes: a box's input has no influence on other boxes' behavior
- True for the quantum boxes but also include non-quantum boxes

Non-signaling security



Why should we care?

- Perhaps quantum mechanics is not complete?
- What are the essential reasons for security?
- “Simpler” security proofs?
  - Non-signaling boxes are defined by linear constraints
  - Quantum boxes are much more complicated

- Proposed: Barrett, Hardy & Kent05
- Strong results known for NS security for Key Distribution (MasanesRCWB14) & randomness amplification (ChungSW16)
- Significant gaps with ideal parameters

Q4.1 Prove NS security for rand. expansion/amplification/KD with ideal pars

Q4.2 Formulate NS version of standard q. info concepts and results.

Other topics

- Delegated quantum computation: verifiable/blind/homomorphic (AharonovBE10, BroadbentFK09, BroadbentJ15, Schaffner16)
- Measurement-Device Independent (LoCQ12)

Conclusion

- A lot can be done even without trusting q. devices
- Many fundamental questions remain open
- Addressing these questions also raises fundamental QI questions

Trustworthy Quantum Information Workshop (TyQI.org)

- 2015: Ann Arbor
- 2016: Shanghai (Qiang Zhang@USTC)
- 2017: Paris (Diamenti & Kashefi)