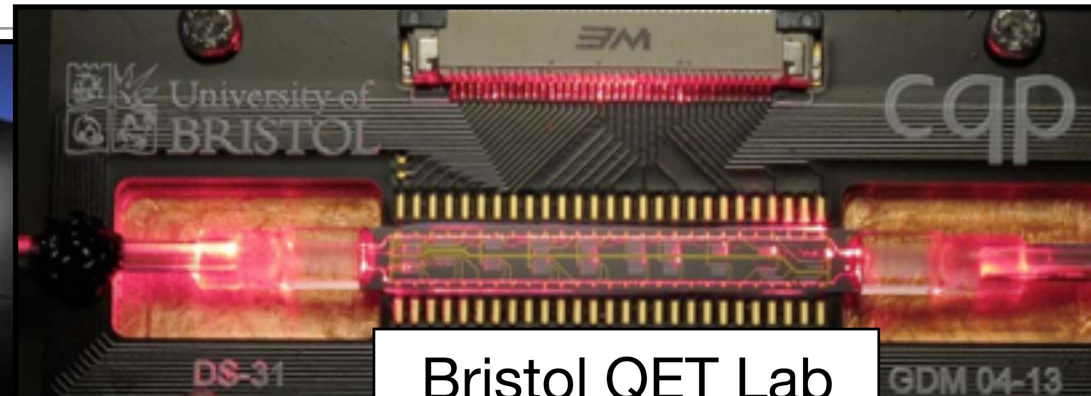
Verification of Quantum Computing

Elham Kashefi

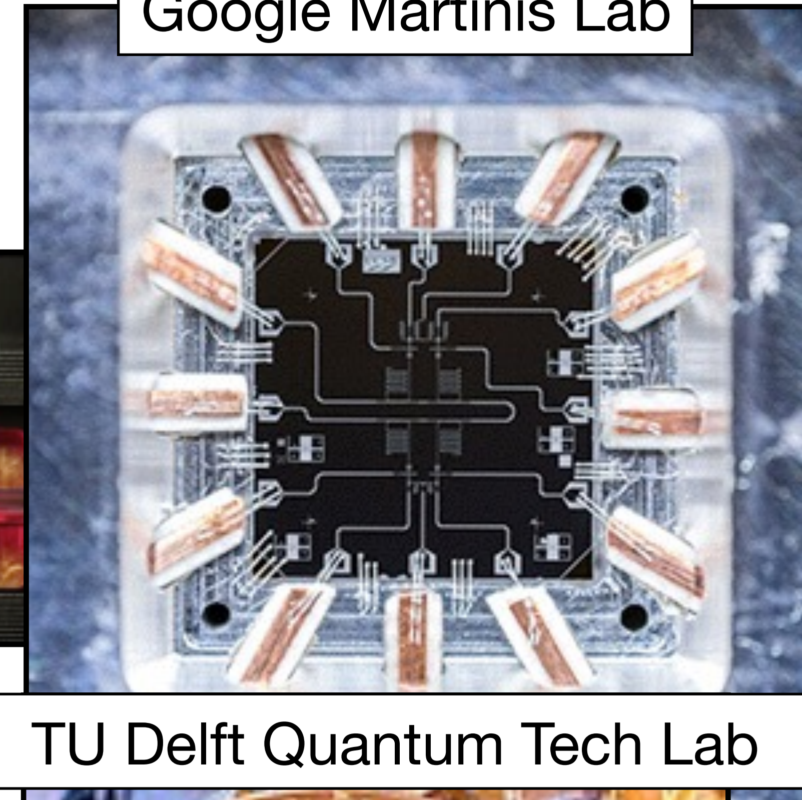
University of Edinburgh
Oxford Quantum Technology Hub
Paris Centre for Quantum Computing
Laboratoire traitement et communication de l'information

Motivation

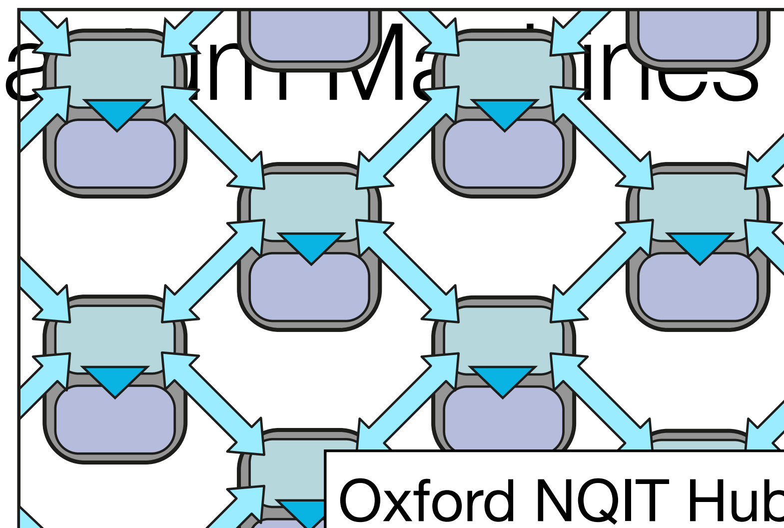
Lockheed Martin/NASA/Google Artificial Intelligence lab



Bristol QET Lab



Google Martinis Lab



Oxford NQIT Hub

TU Delft Quantum Tech Lab

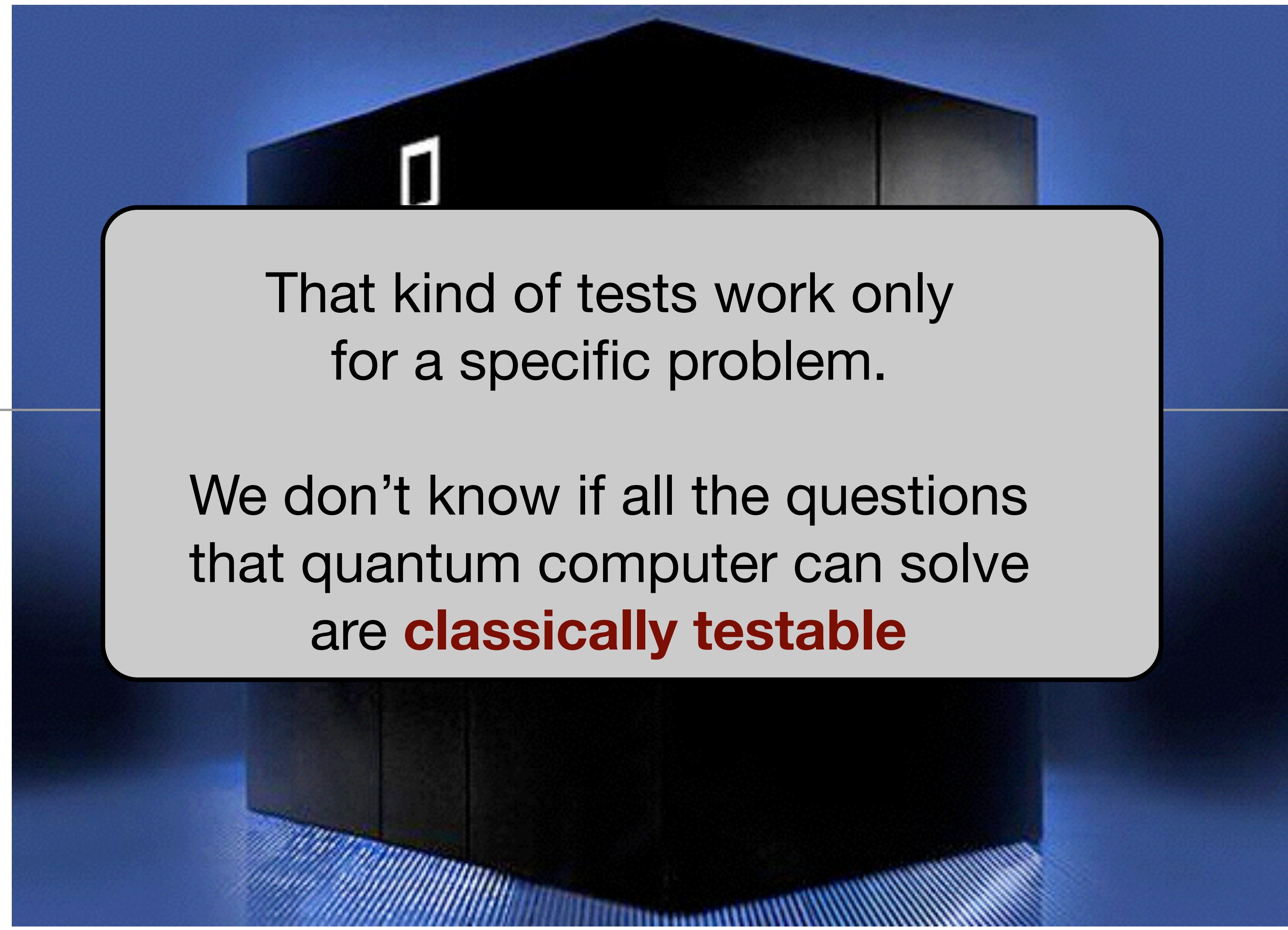
These devices become **relevant** at the moment they are no longer classically simulatable

Existing methods of Testing/Validation/Simulation/Monitoring/Tomography ... all become **IRRELEVANT**

What is Quantum Computer ?

Is it a Quantum BOX ?

Should we pay $10000000 for a quantum computer

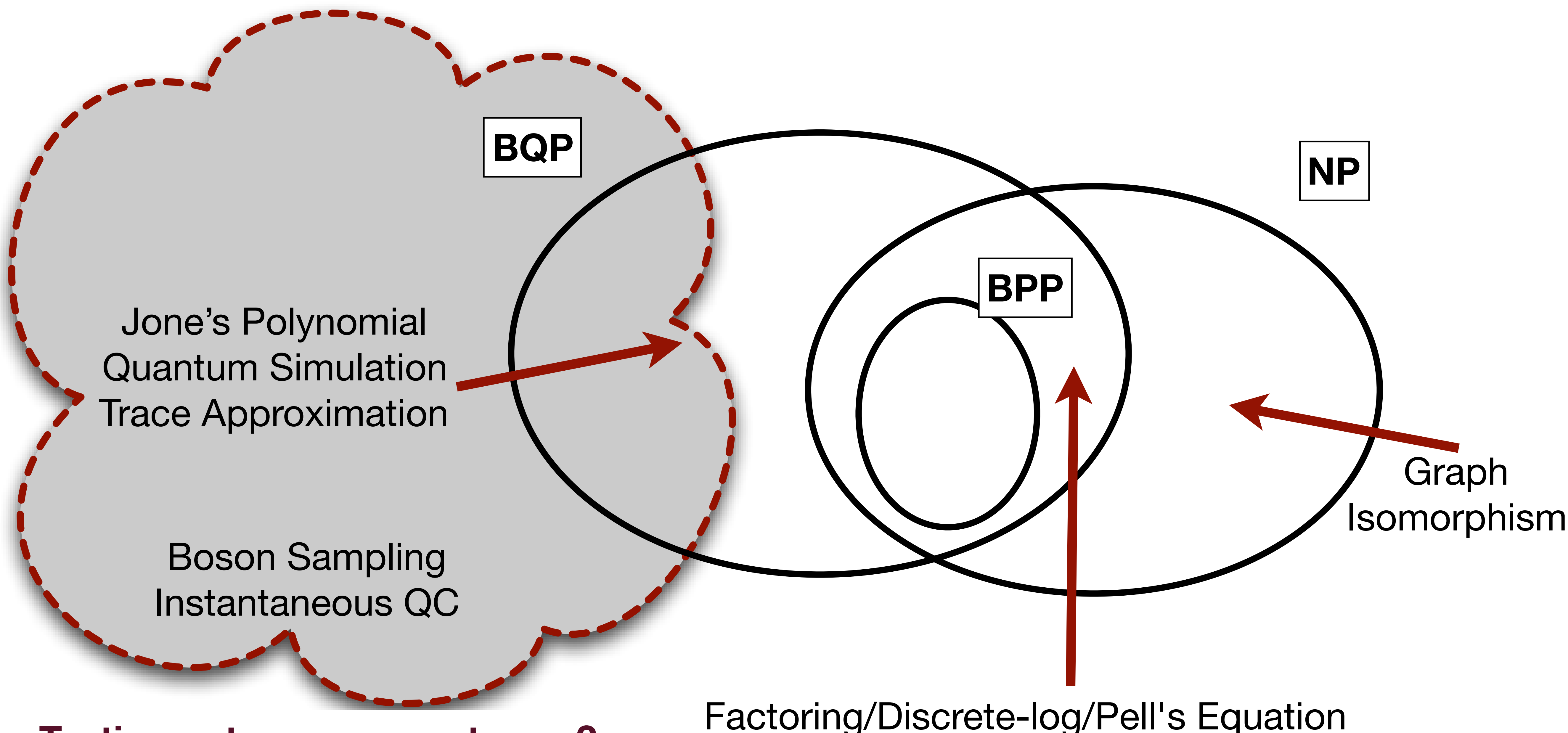


That kind of tests work only
for a specific problem.

We don’t know if all the questions
that quantum computer can solve
are **classically testable**

Simple test: We ask the box to factor a big number

Complexity Picture



Testing outcome correctness ?

Target

Efficient verification methods for realistic pseudo quantum computers

- Correctness of the outcome
- Operation monitoring
- Quantum property testing

- Architectural constraints
- Experimental imperfections

None-universal:
D-Wave machine
Quantum Simulator

How do we do it?

Verification of Classical Computing

business buy computing from
a service provider

outsourcing complex
computing to larger servers

- ➡ Cloud Computing
- ➡ Small Devices
- ➡ Large Scale Computation

Network-based computation

Methodology

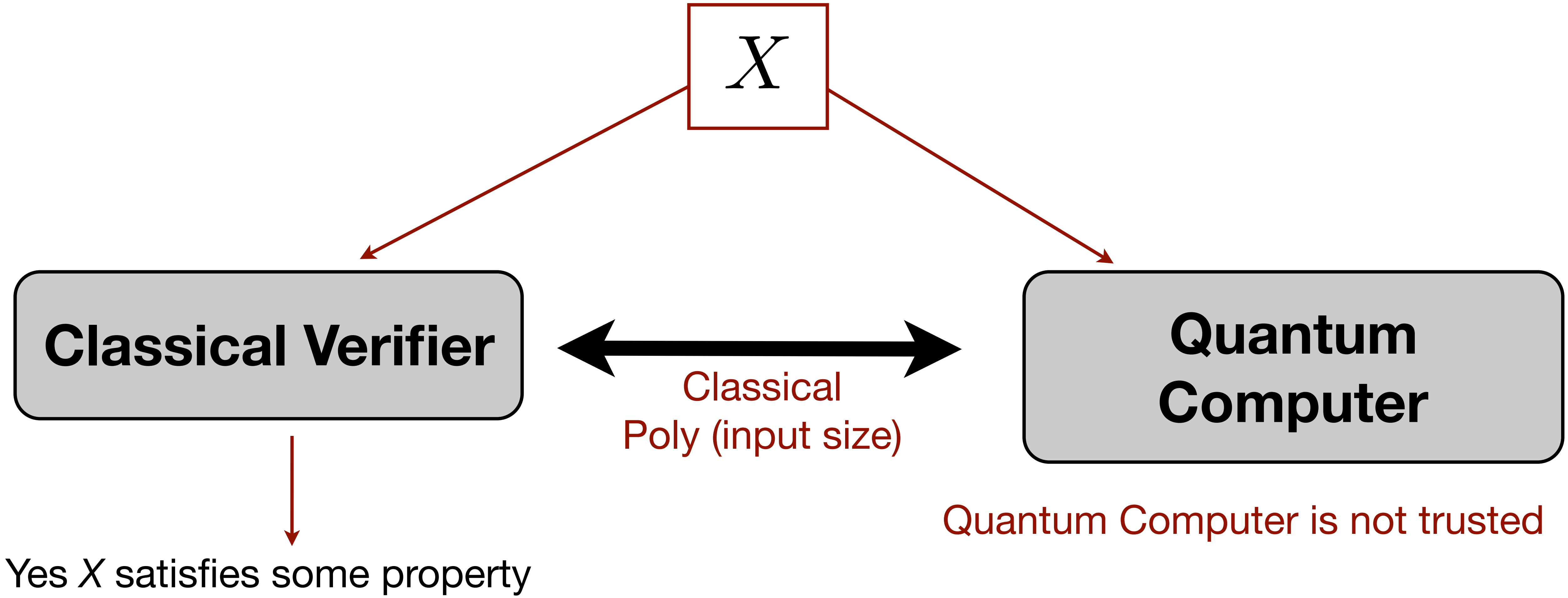
Combat the complexity

Formalising the Question

- ➡ Interactive Proof System
- ➡ Cryptographic Toolkit
- ➡ Classically controlled QC

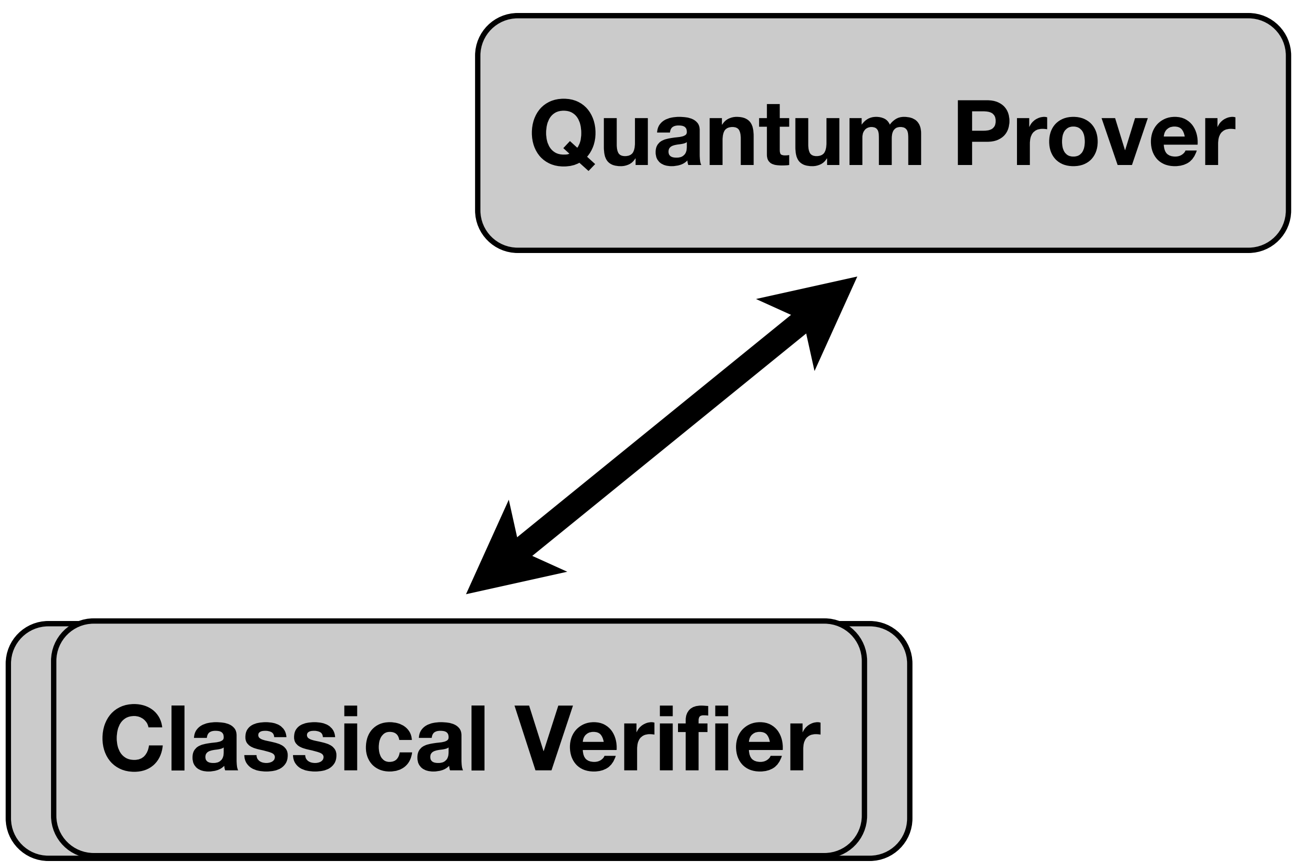
Implementation Platform

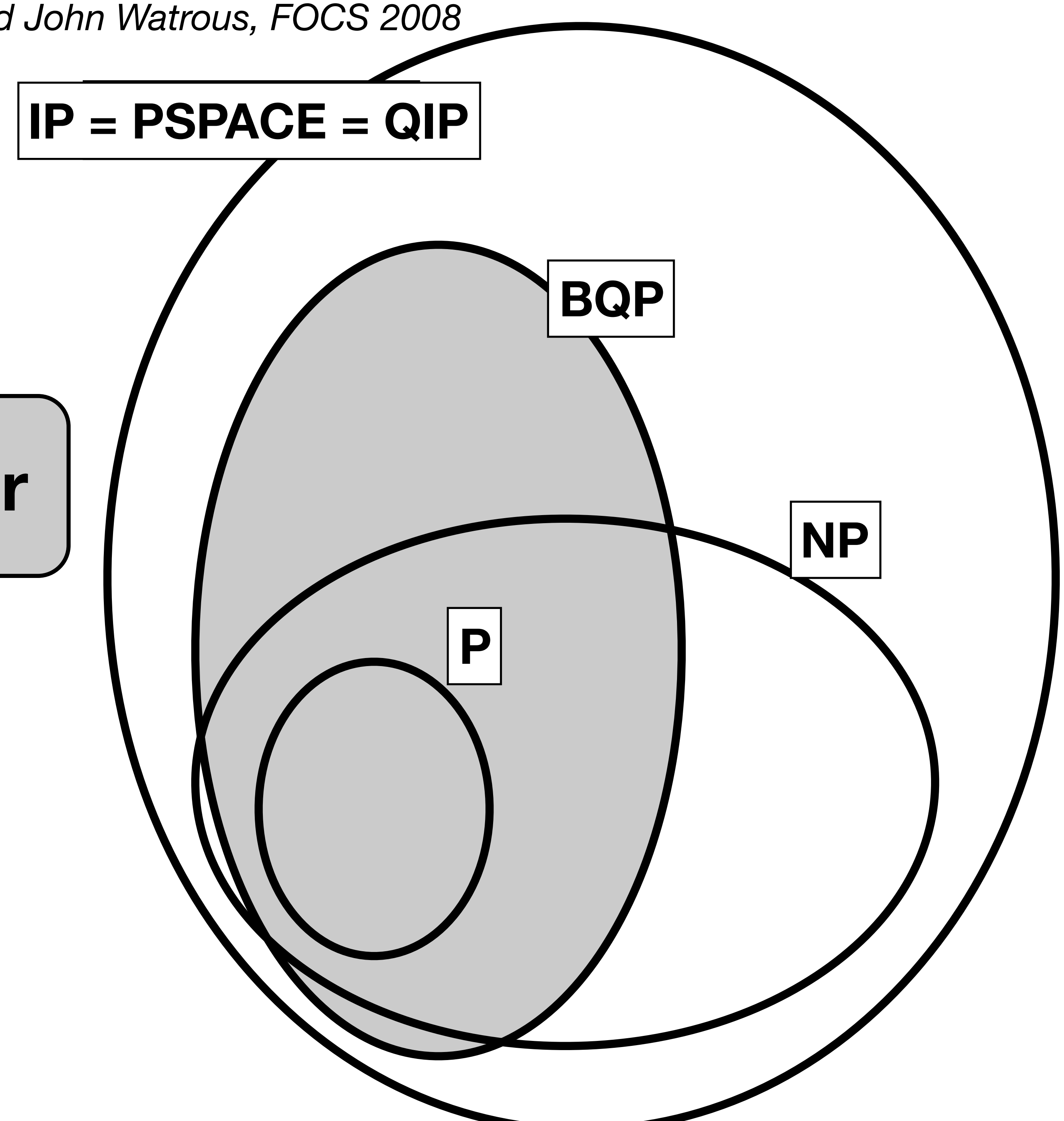
IP for Quantum Computing



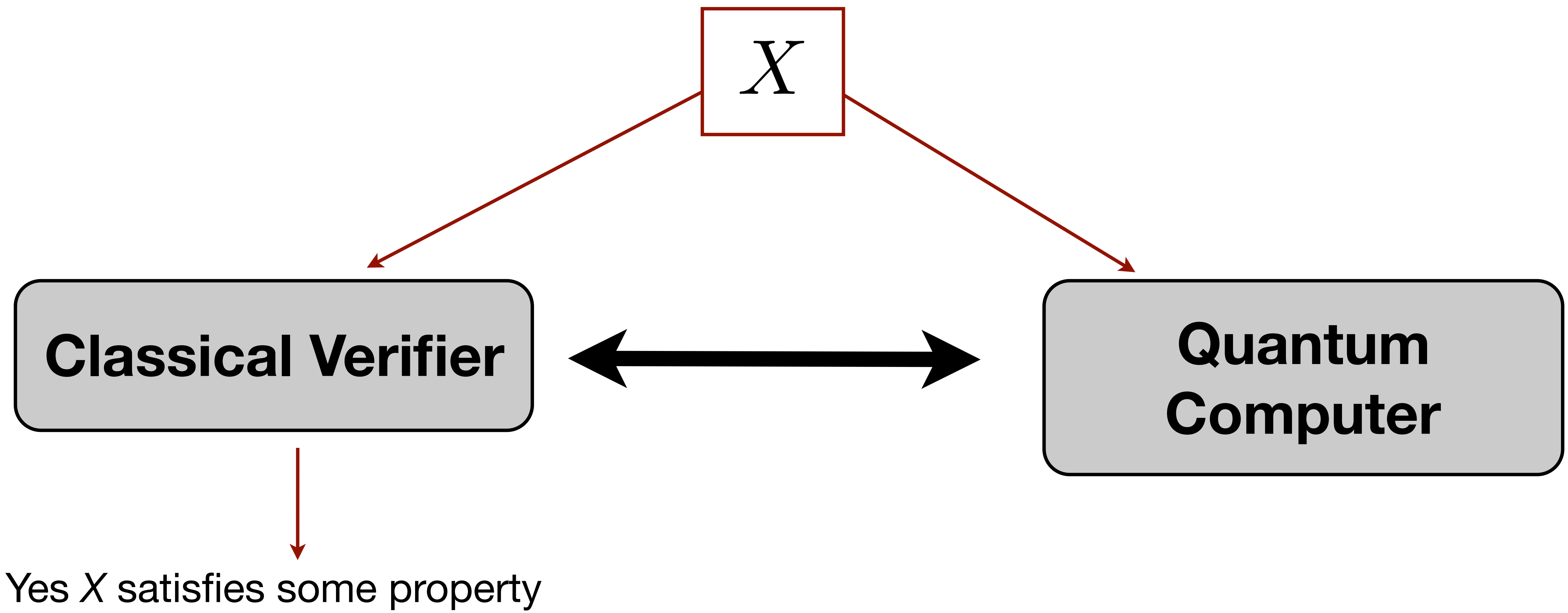
IP for Quantum Computing

Rahul Jain, Zhengfeng Ji, Sarvagya Upadhyay, and John Watrous, FOCS 2008





IP for Quantum Computing



Gottesman (04) - Vazirani (07)- Aaronson **$25** *Challenge (07)*

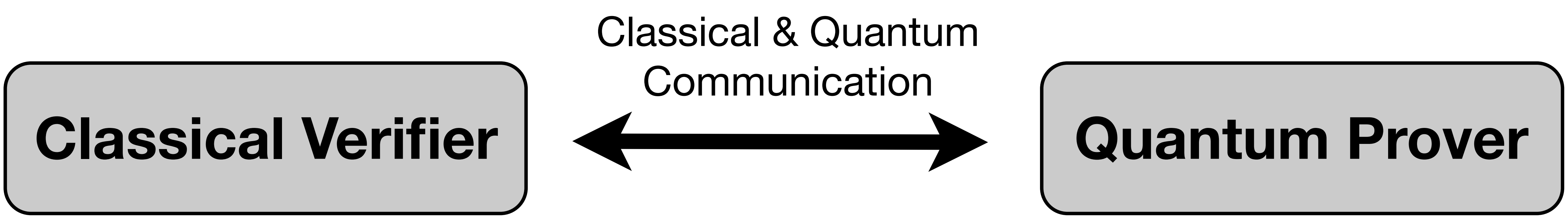
Does BQP admit an interactive protocol

where the prover is in BQP and the verifier is in BPP?

D. Aharonov and U. Vazirani, arXiv:1206.3686 (2012).

Yes we can but with

Semi Classical Verifier



+

Trusted

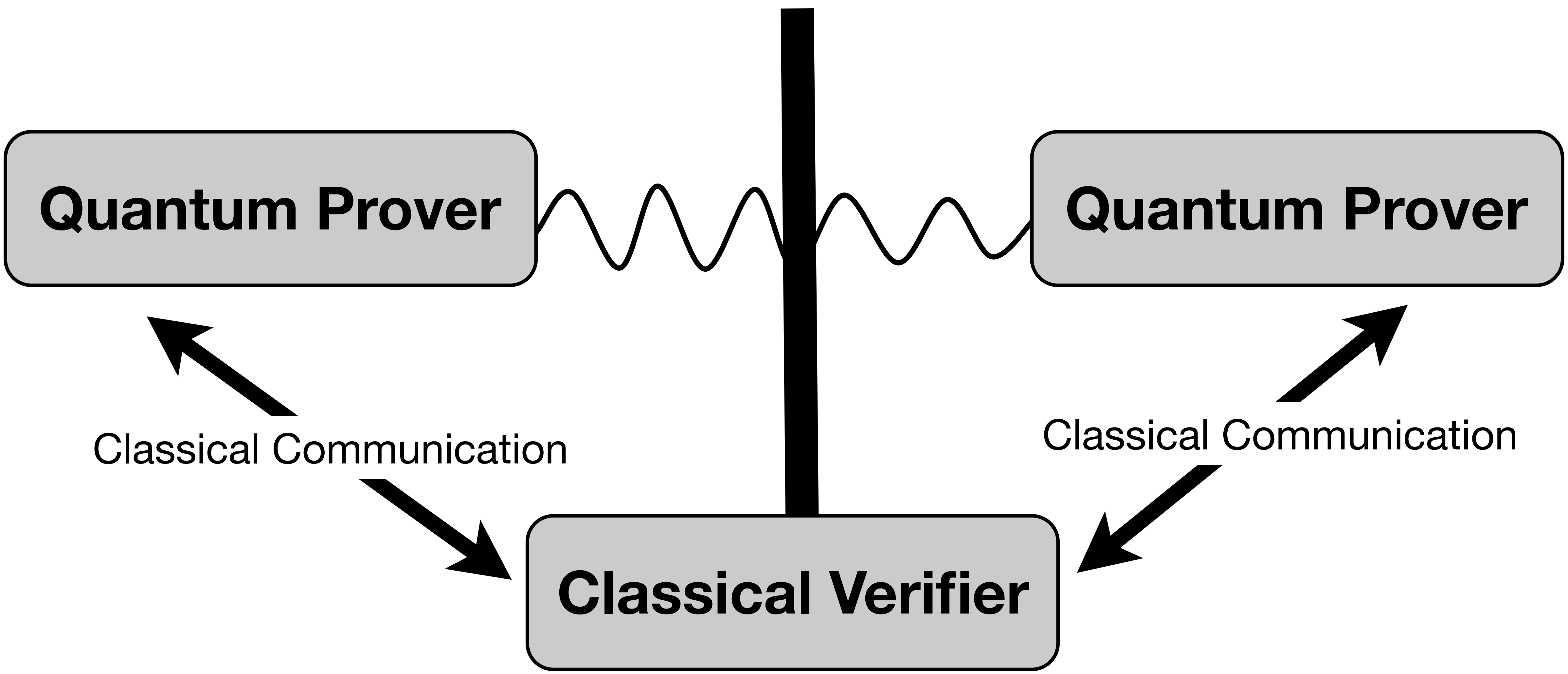
random single qubit generator

Broadbent, Fitzsimons and Kashefi, FOCS 2009

Fitzsimons and Kashefi, arXiv:1203.5217 2012

Yes we can but with

Entangled non-communicating Provers



Reichardt, Unger and Vazirani, Nature 2012
Gheorghiu, Kashefi, Wallden, NJP, 2015

Cryptographic Toolkit

Classical World

Gentry 09
A Lattice-based cryptosystem
that is fully homomorphic

Quantum World

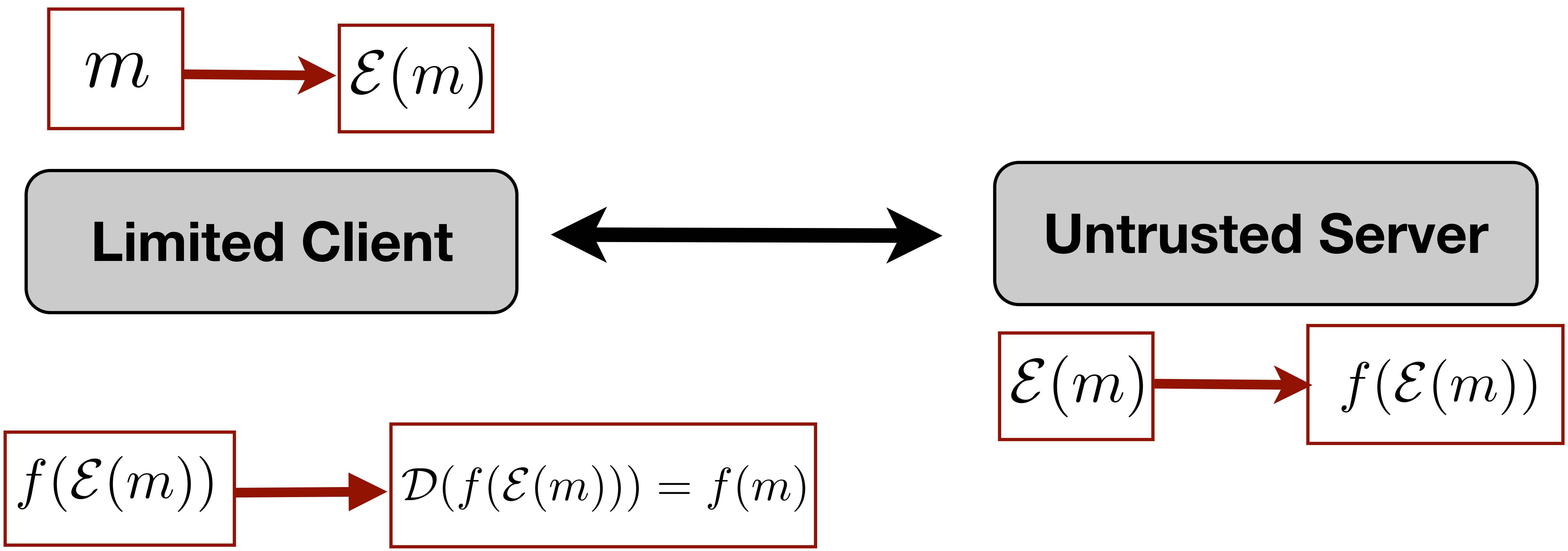
Broadbent, Fitzsimons and Kashefi 09
Blind Quantum Computing
QKD + Teleportation

Enables arbitrary computation on encrypted data ***without decrypting***

Holy Grail of Cryptography since 1987

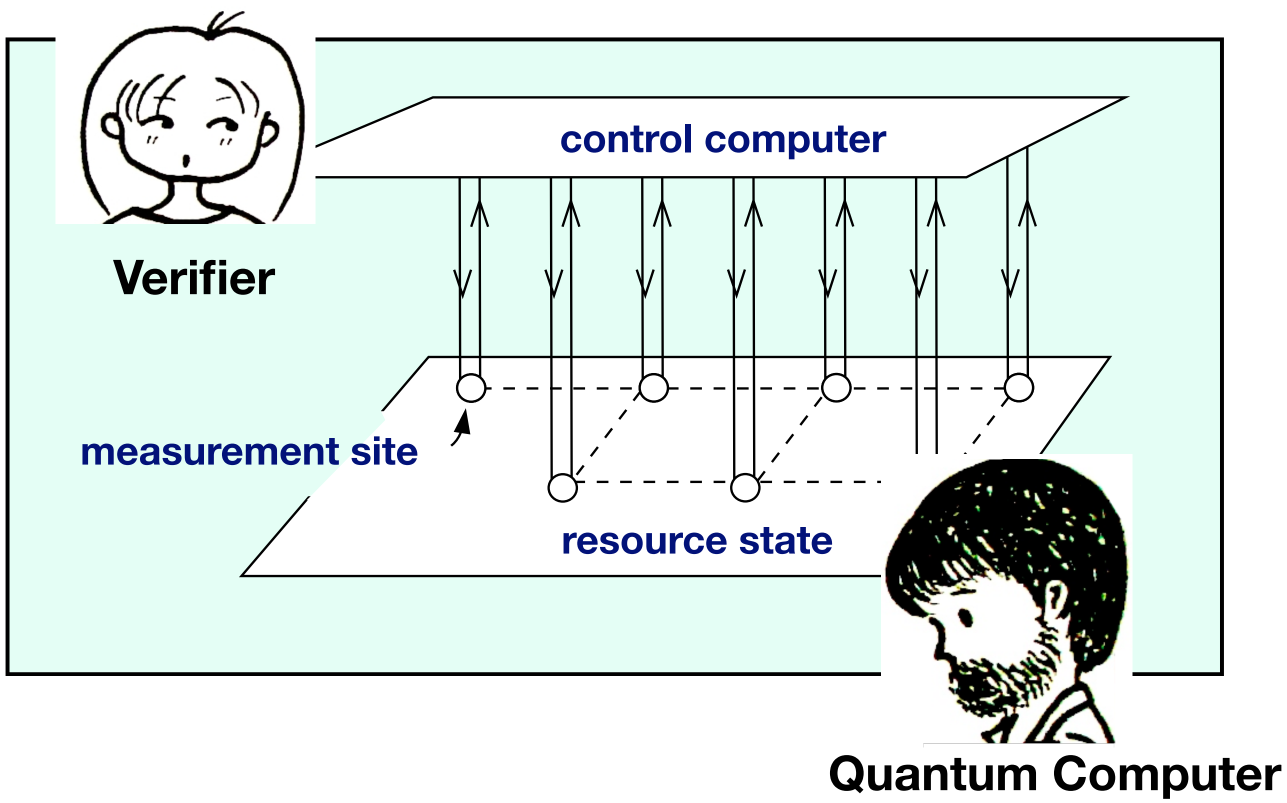
Rivest, Adleman and Dertouzos

Can we process encrypted data without decrypting it



Blind Quantum Computing

Program is encoded in the classical control computer
Computation Power is encoded in the entanglement



Hide

- Angles of measurements
- Results of Measurements

UBQC based on no-cloning assumption

given random single qubit

$$|0\rangle + e^{i\theta}|1\rangle$$

$$\theta \in_R \{0, \pi/4, 2\pi/4, \cdots, 7\pi/4\}$$

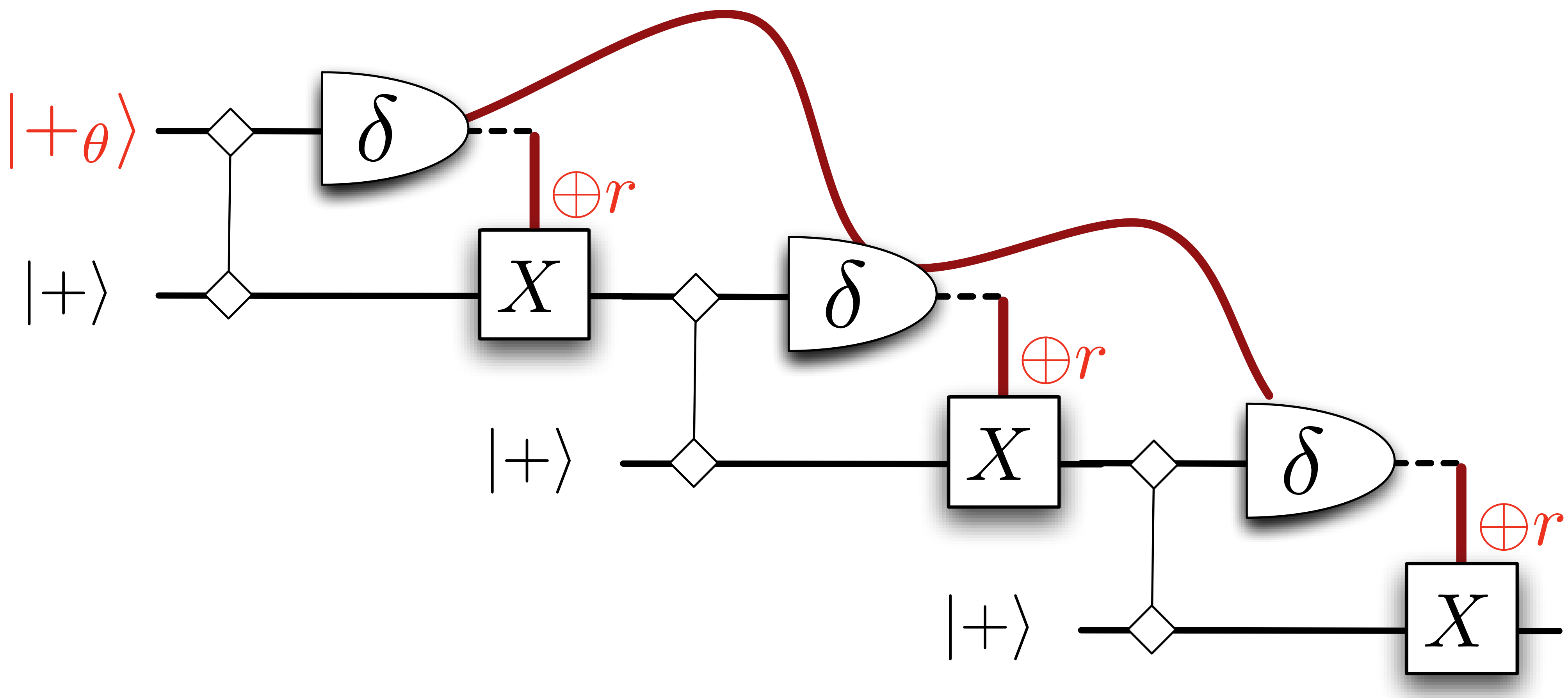
→ At most one-bit of information about θ could be leaked

$$\mathcal{E}(m) = (m + \theta + r\pi \;,\; |0\rangle + e^{i\theta}|1\rangle)$$

unconditionally secure

enables perfect removal of θ at each step

Gates Composition



Client-Server interactions

Universal Blind Quantum Computings

$X = (\tilde{U}, \{\phi_{x,y}\})$

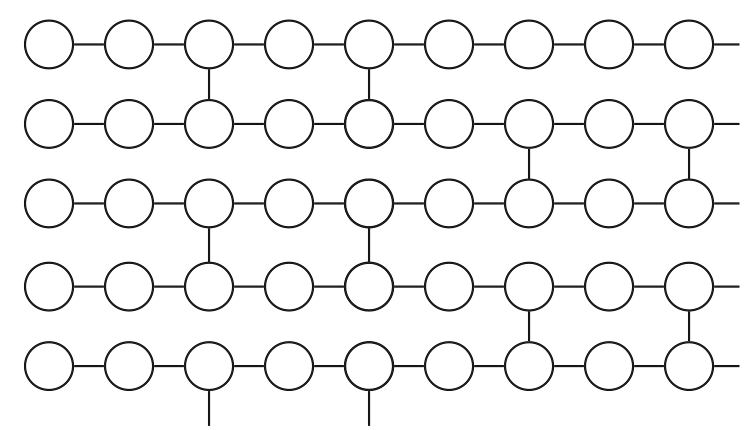
θ θ'

random single qubit generator

$$1/\sqrt{2}\left(|0\rangle + e^{i\theta}|1\rangle\right)$$

$$\theta = 0, \pi/4, 2\pi/4, \ldots, 7\pi/4$$

$\delta_{x,y}$



$r_{x,y} \in_R \{0,1\}$

$$\delta_{x,y} = \phi'_{x,y} + \theta_{x,y} + \pi r_{x,y}$$

$\{|+_{\delta_{x,y}}\rangle, |-_{\delta_{x,y}}\rangle\}$

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

$$s_{x,y} := s_{x,y} + r_{x,y}$$

Verification

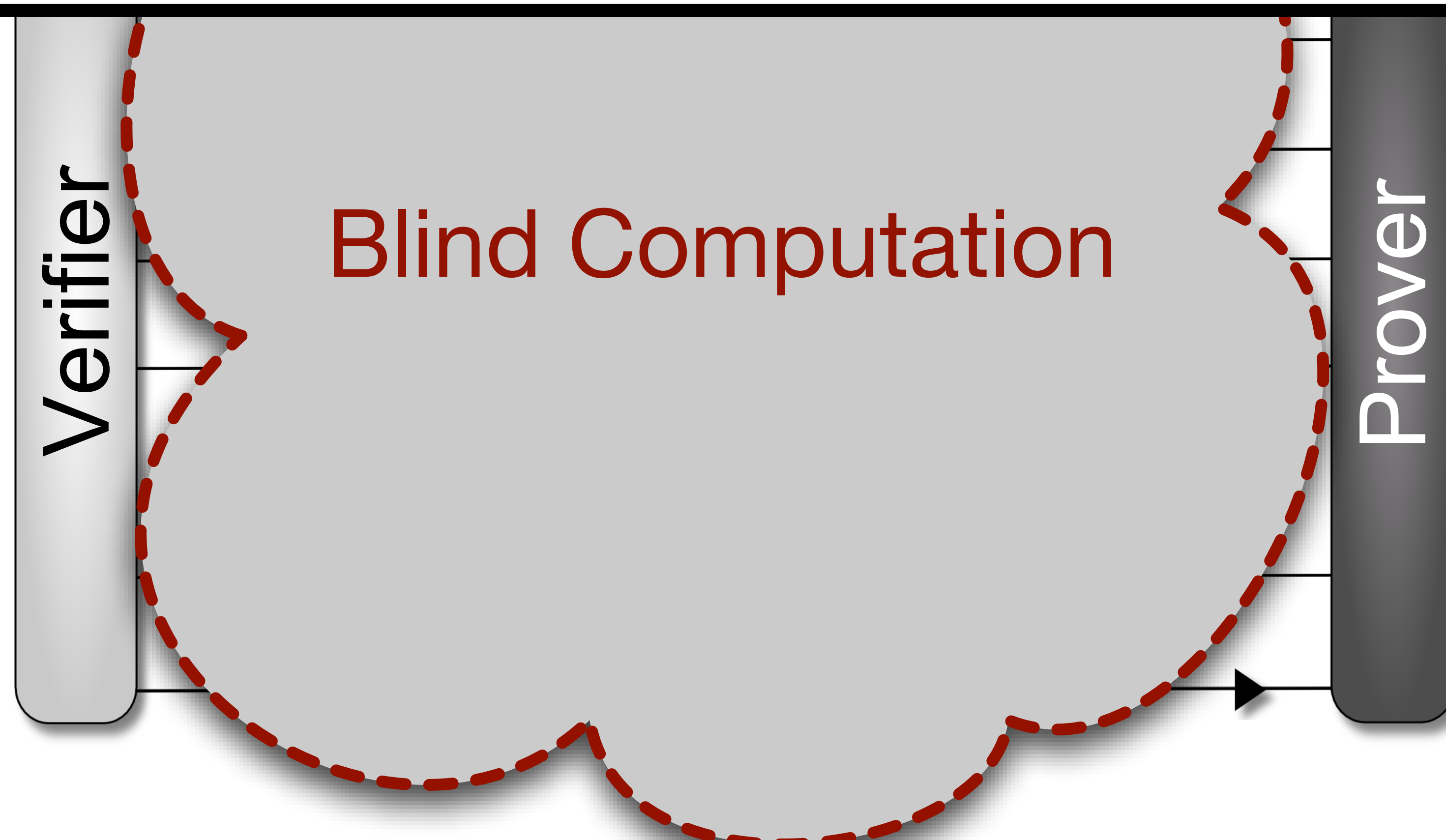
- Correctness: in the absence of any interference, client accepts and the output is correct

- Soundness: Client rejects an incorrect output, except with probability at most exponentially small in the security parameter

Fitzsimons and Kashefi, arXiv:1203.5217, 2012

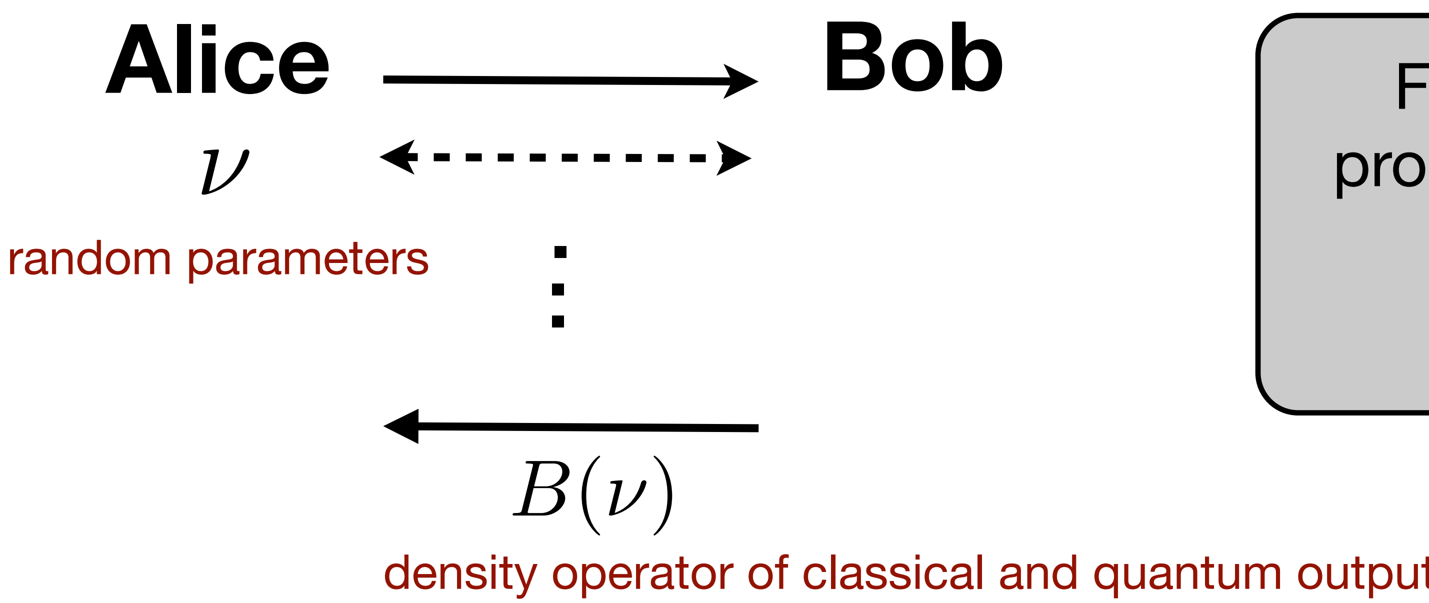
Verification

p (incorrect AND accept) < ε



Blind Computation
with **BPP*** Alice

ε-Verification



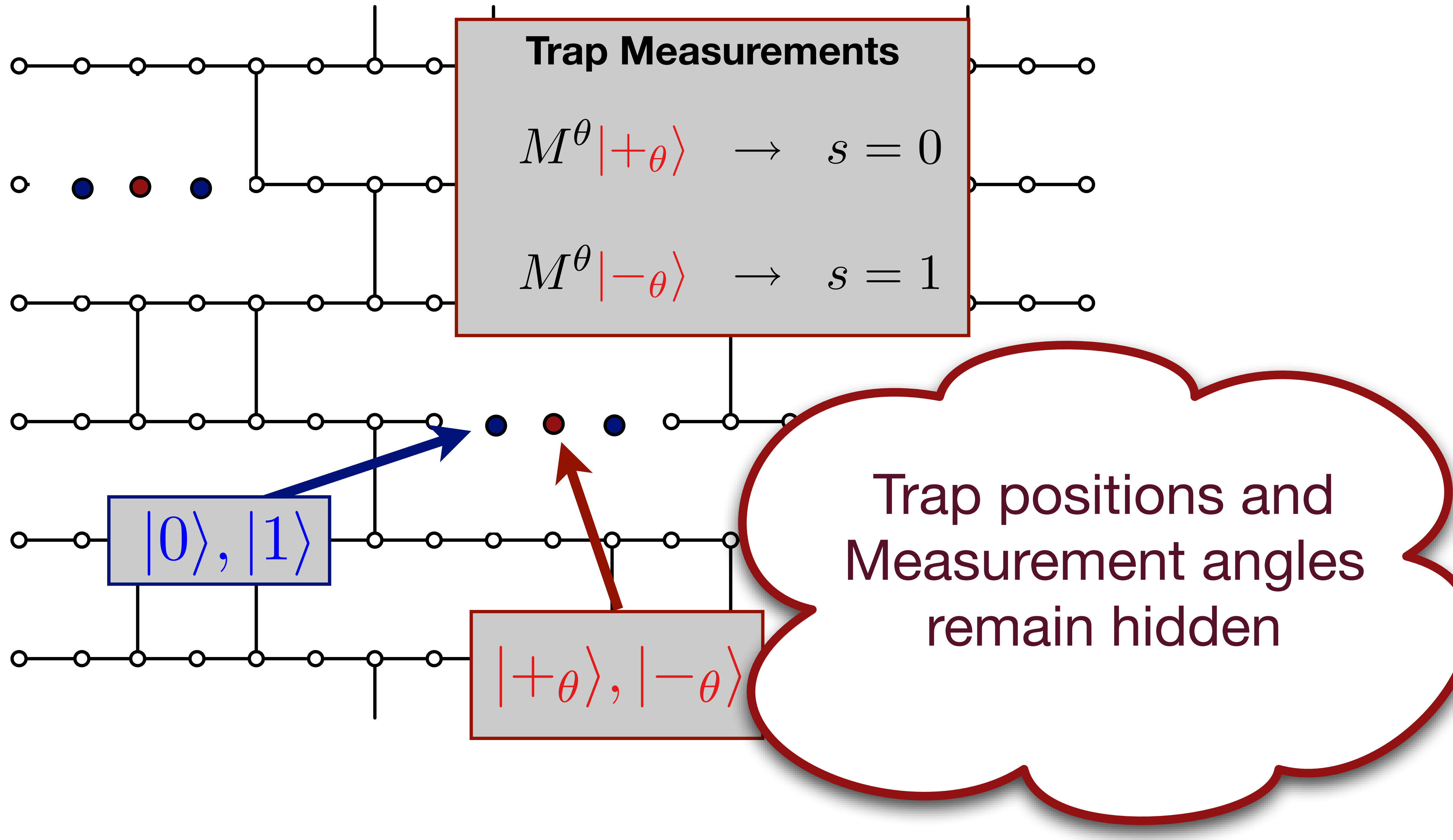
For any server's strategy the probability of client accepting an incorrect outcome density operator is bounded by ε:

$$P^{\nu}_{incorrect} = (\mathbb{I} - |\Psi^{\nu}_{ideal}\rangle\langle\Psi^{\nu}_{ideal}|) \otimes |r^{\nu}_{t}\rangle\langle r^{\nu}_{t}|$$

Accept Key

$$\sum_{\nu} p(\nu)\ Tr\left(P^{\nu}_{incorrect}\, B(\nu)\right) \leq \epsilon$$

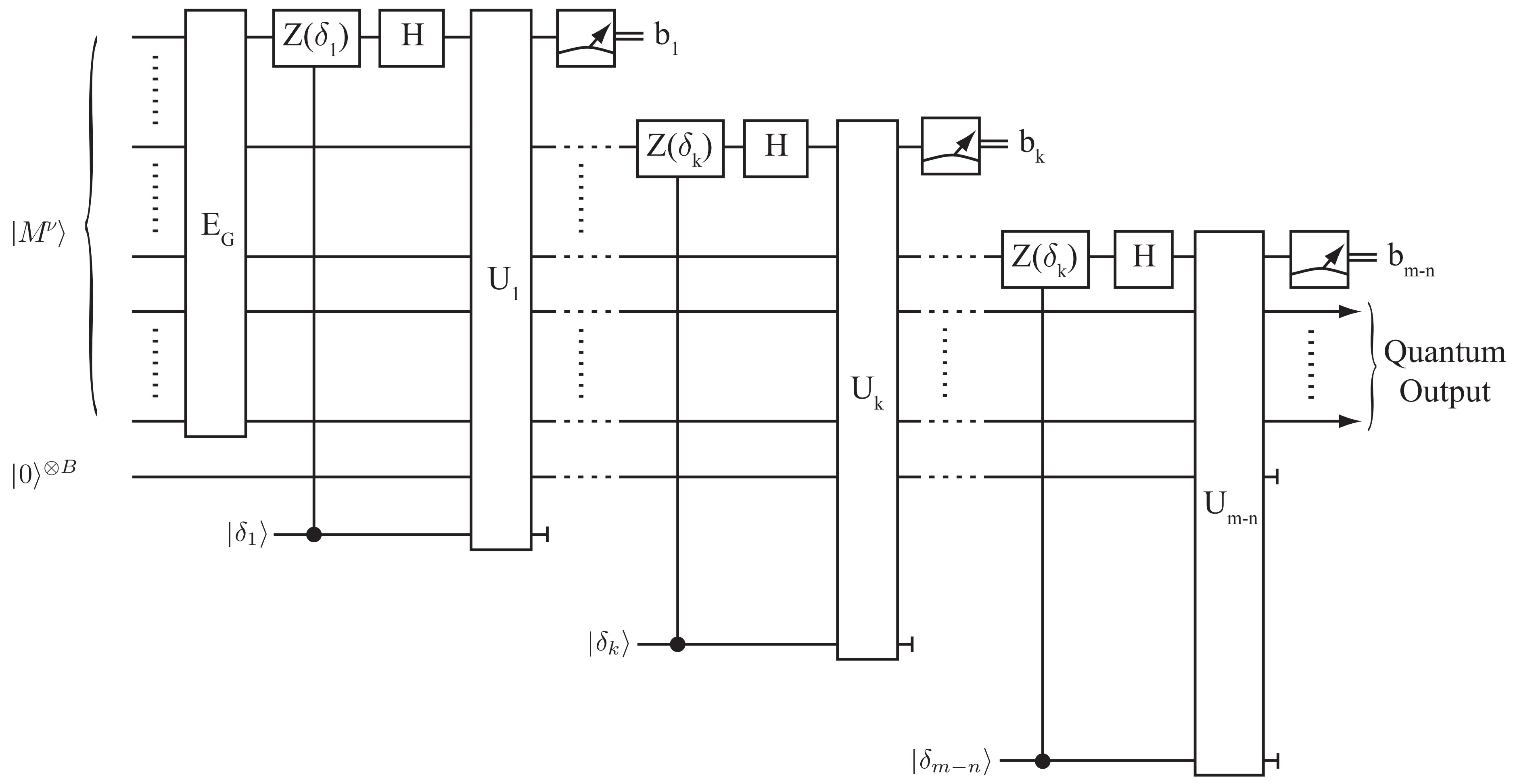
Adding Traps



Verification with single trap

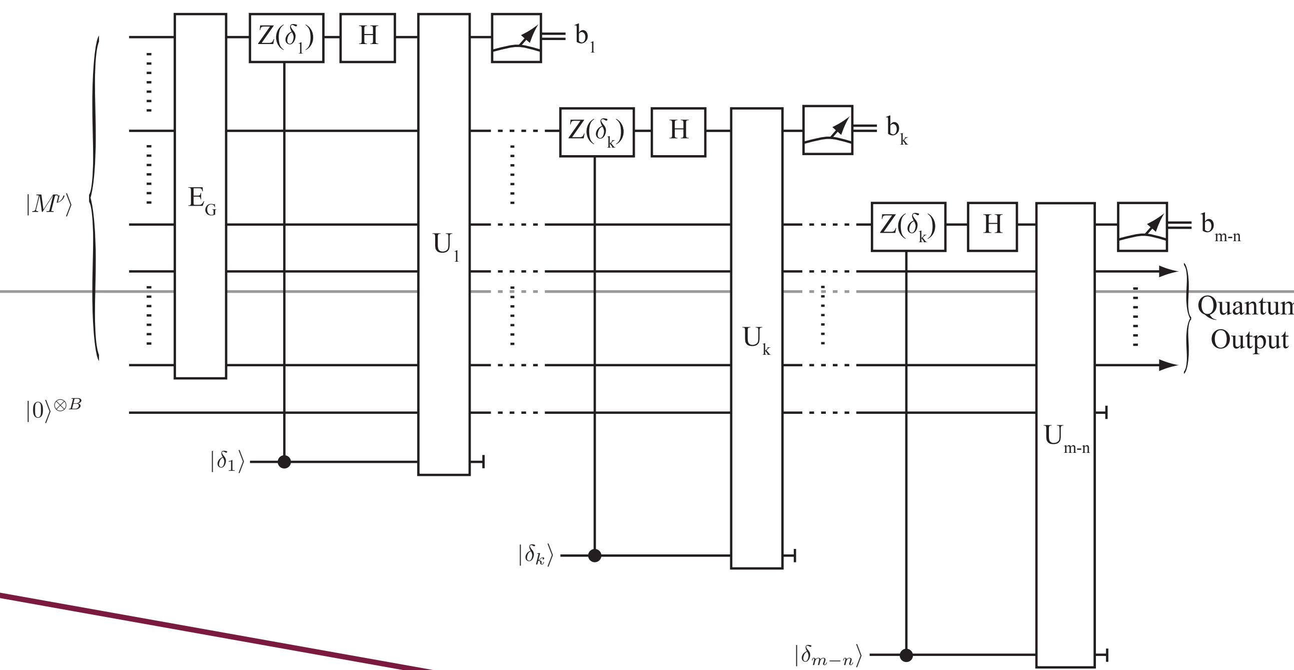
Theorem. Protocol is $(1 - 1/2N)$-verifiable in general, and in the case of purely classical output it is $(1 - 1/N)$-verifiable, where N is the total number of qubits in the protocol.

ε-Verification



$$B_j(\nu) = \mathrm{Tr}_B \left(\sum_b |b + c_r\rangle \langle b| \, C_{\nu_C, b} \Omega \mathcal{P} ((\otimes^B |0\rangle \langle 0|) \otimes \left|\Psi^{\nu,b}\right\rangle \left\langle \Psi^{\nu,b}\right|) \mathcal{P}^\dagger \Omega^\dagger C^\dagger_{\nu_C, b} \, |b\rangle \langle b + c_r| \right)$$

ε-Verification



Blindness

$$p_{\text{incorrect}} \leq \sum_{k,\nu_T} \sum_{i \in E_i} \alpha_{ik} \alpha_{ik}^* p(\nu_T) \mathrm{Tr}\left(\langle \eta_t^{\nu_T} | \sigma_i \left(|\eta_t^{\nu_T}\rangle \langle \eta_t^{\nu_T}| \otimes |\delta_t\rangle \langle \delta_t| \otimes \frac{I}{\mathrm{Tr}(I)} \right) \sigma_i |\eta_t^{\nu_T}\rangle \right)$$

⋮

$$= \frac{1}{16m} \sum_k \sum_{i \in E_i} |\alpha_{ki}|^2 \sum_{t, r_t, \theta_t} \left(\langle \eta_t^{\nu_T} | \sigma_{i|t} |\eta_t^{\nu_T}\rangle \right)^2$$

⋮

$$\leq 1 - \frac{1}{2m}$$

Probability Amplification

To increase the probability of any local error being detected

O(N) many traps in random locations

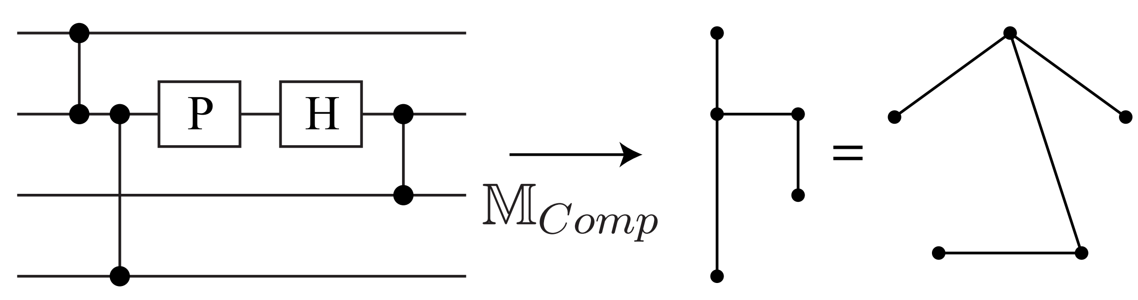
To increase the minimum weight of any operator which leads to an incorrect outcome

Fault-Tolerance

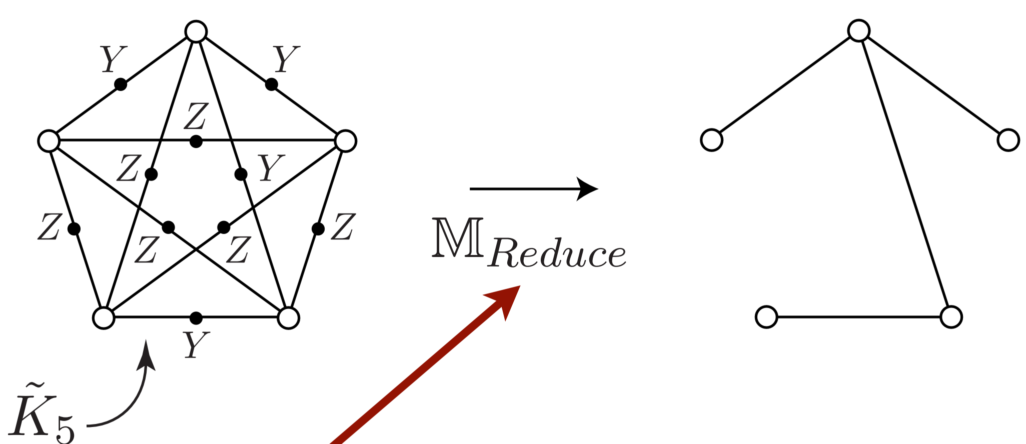
Probability Amplification

Challenge: Traps break the graph

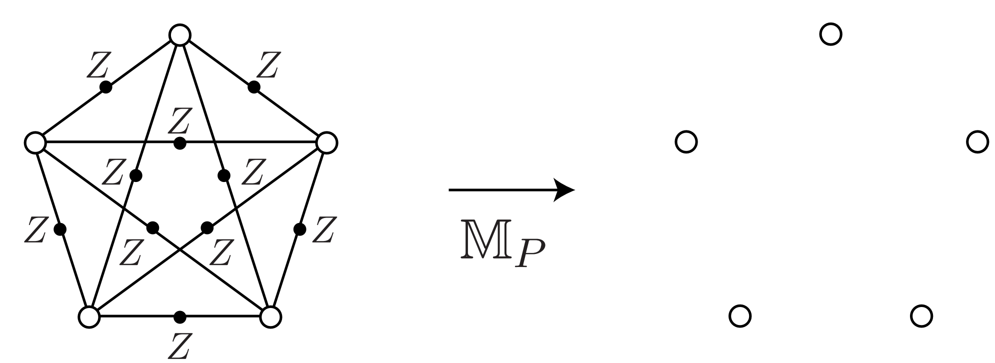
1.



2.

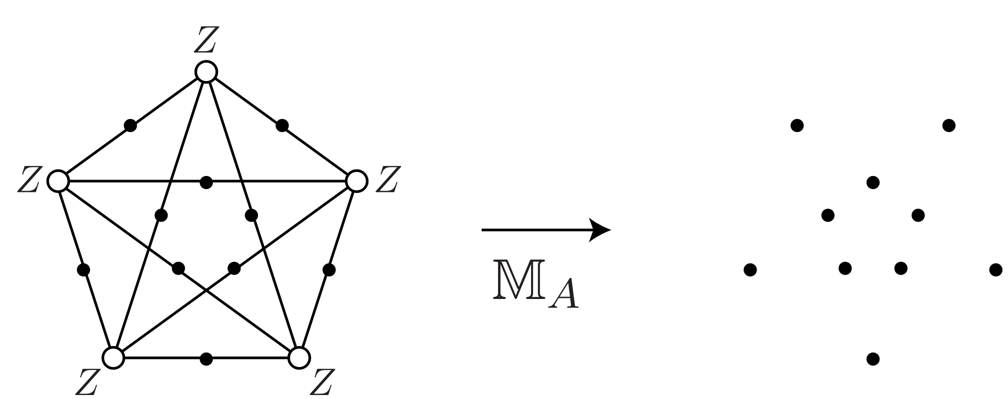


3.

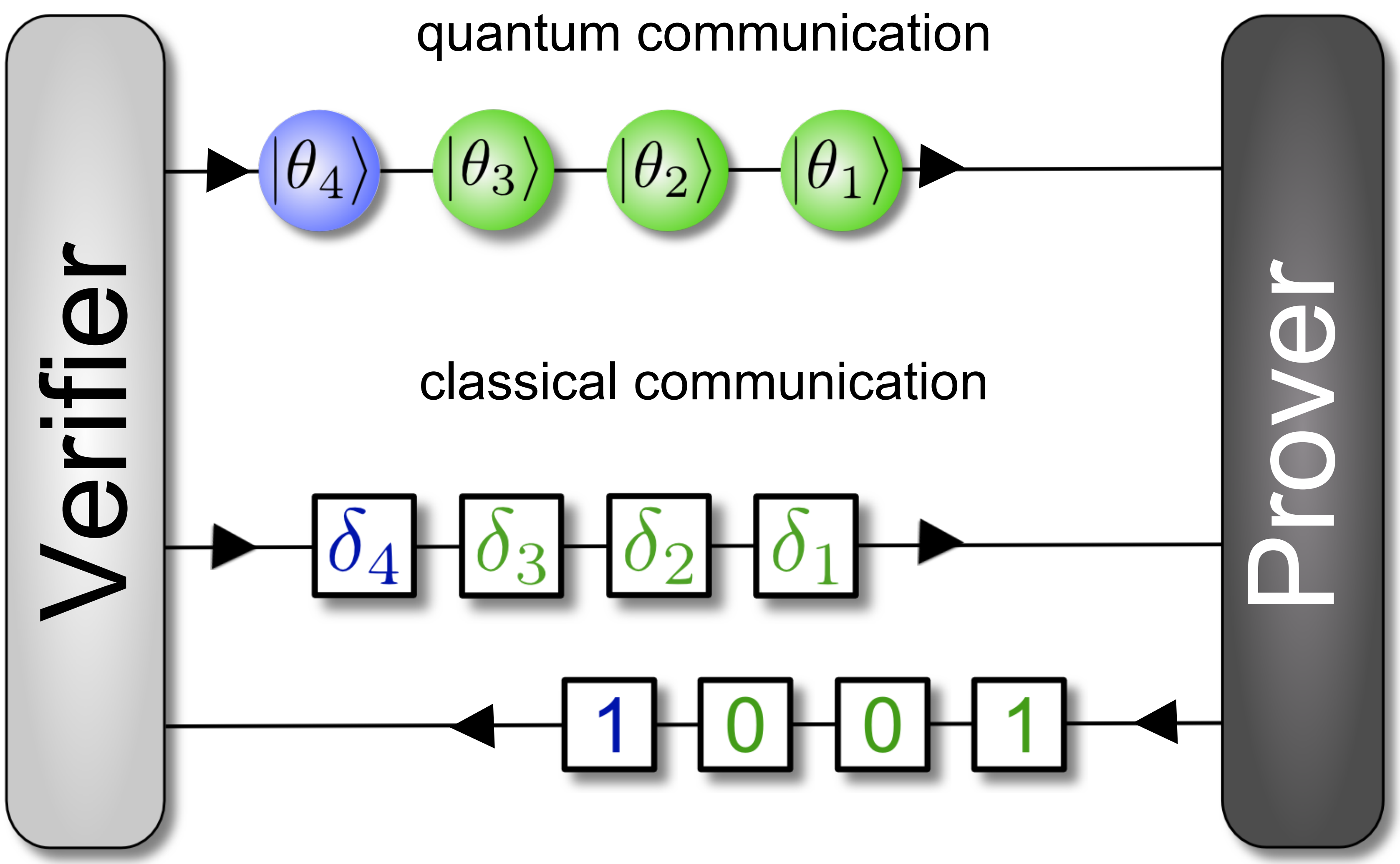


Required 3D lattice for Raussendorf, Harrington and Goyal Topological error-correcting code with defect thickness *d*

4.

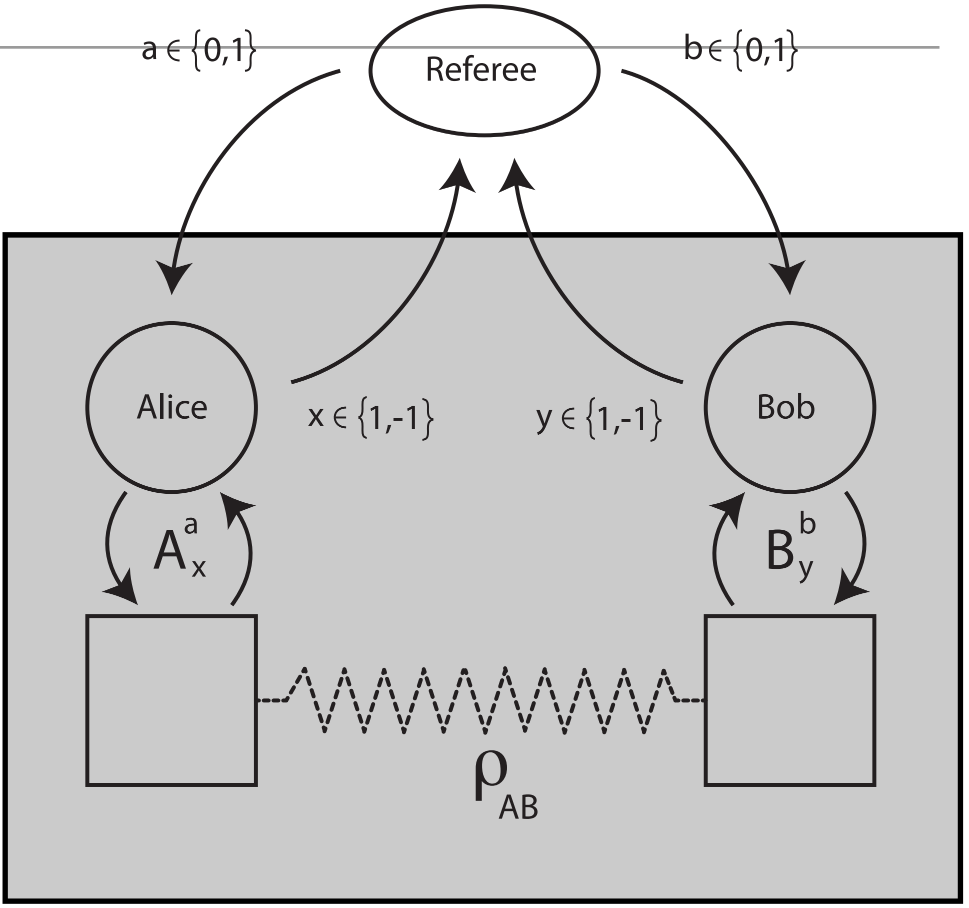


What can we do with 4-qubits



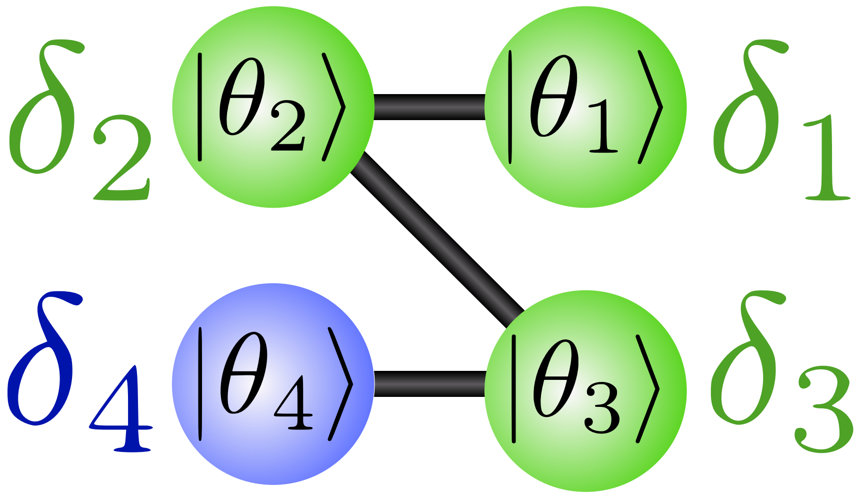
Blind Verification of Entanglement

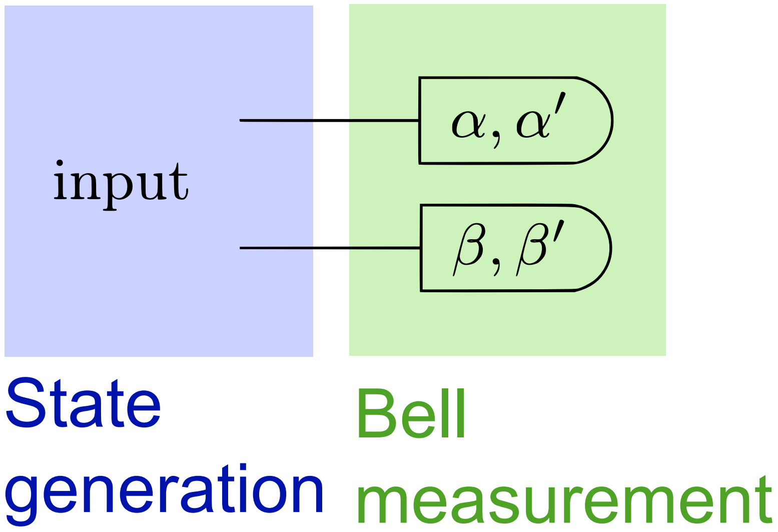
Perform by an untrusted server

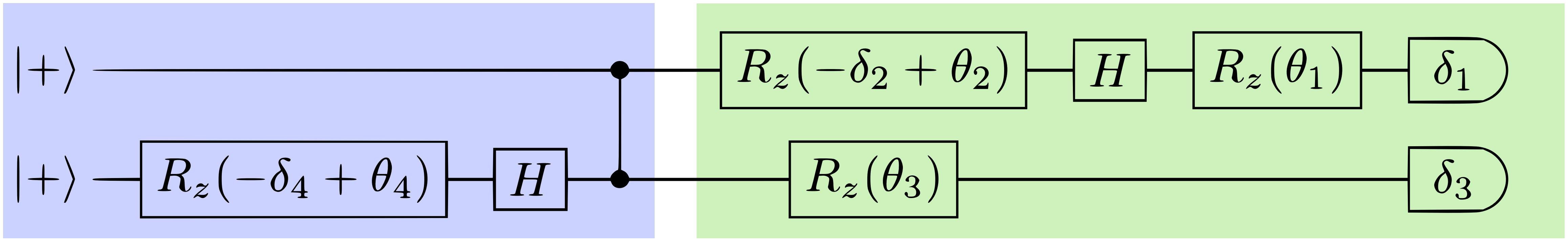


If server knows he is running Bell test,
he can create fake outcomes to violate the inequality,
the trapificaiton procedure in between prevents this to happen

Blind Verification of Entanglement







Blind state generation

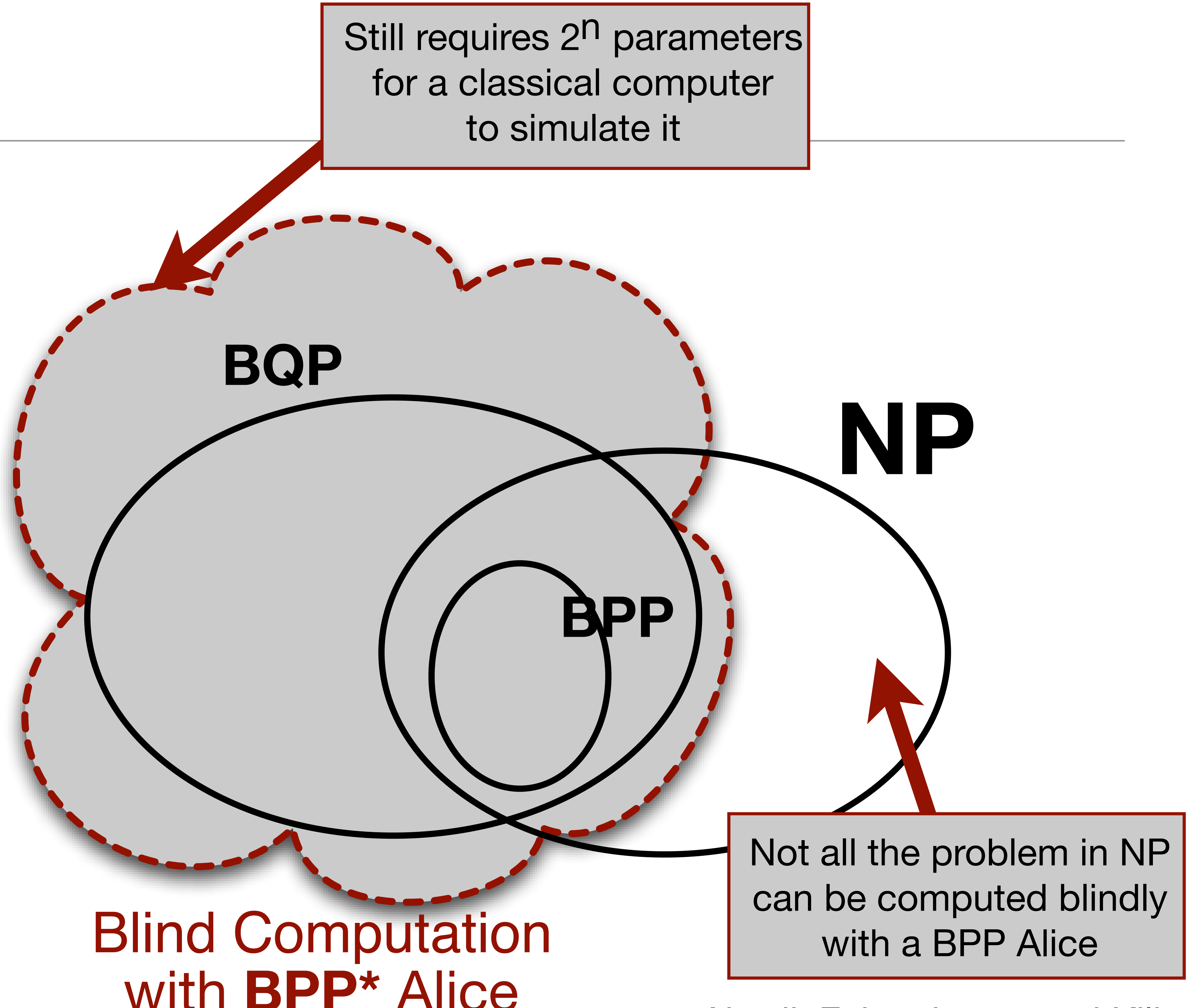
Blind Bell test

Barz, Fitzsimons, Kashefi, Walther, Nature Physics 13

Summery

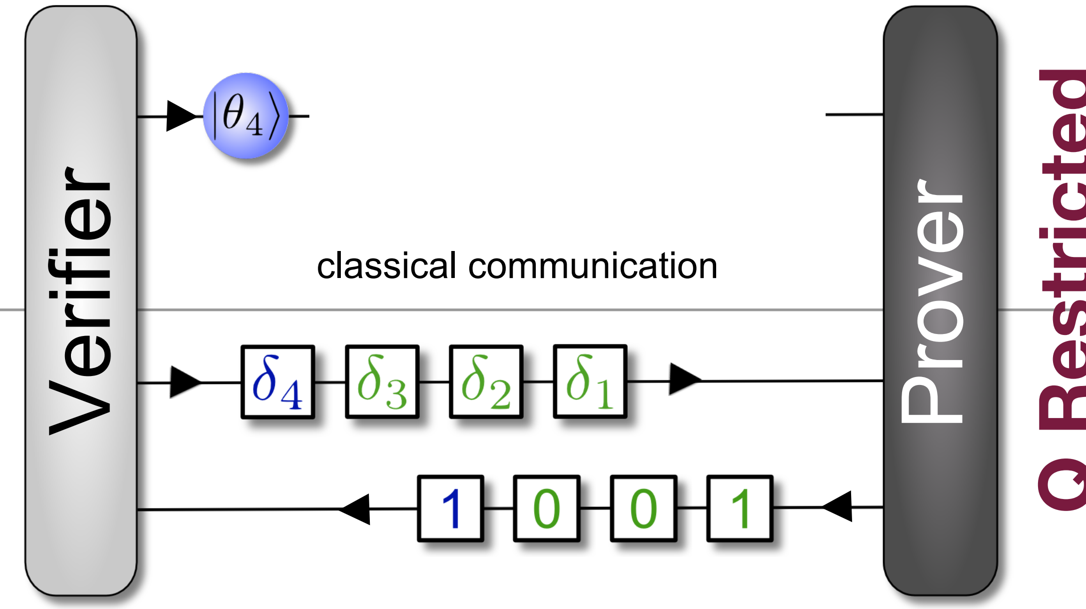
We can test efficiently

But we need quantum randomness

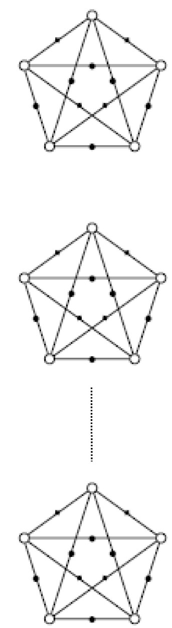


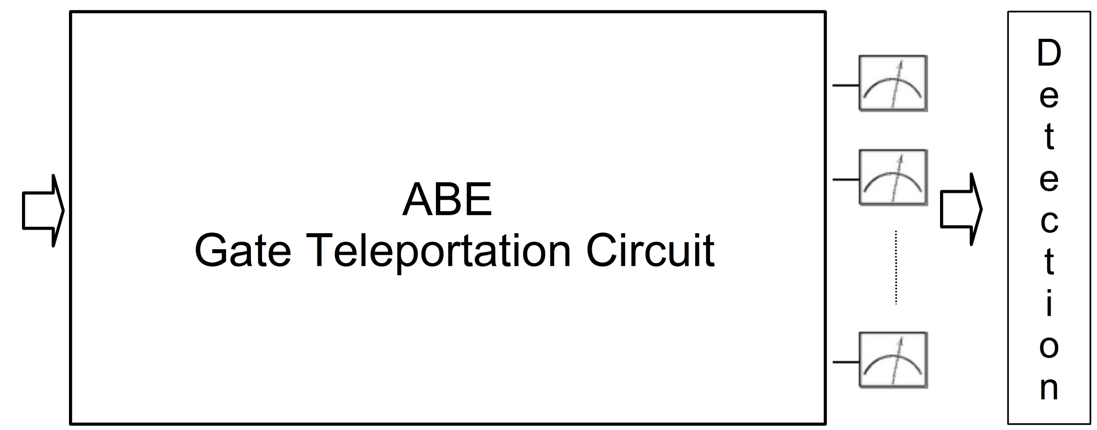
- Abadi, Feigenbaum and Kilian

VUBQC extension

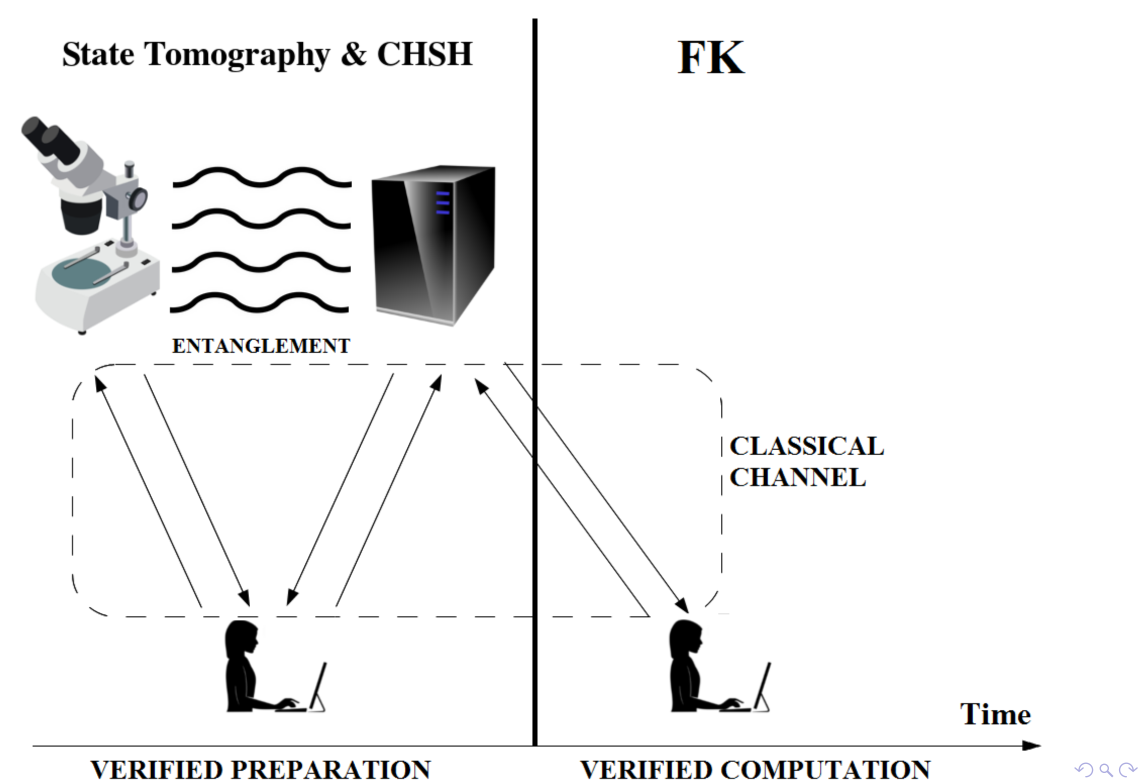


Verification of one-pure-qubit computation
Kapourniotis, Kashefi, Datta, TQC14

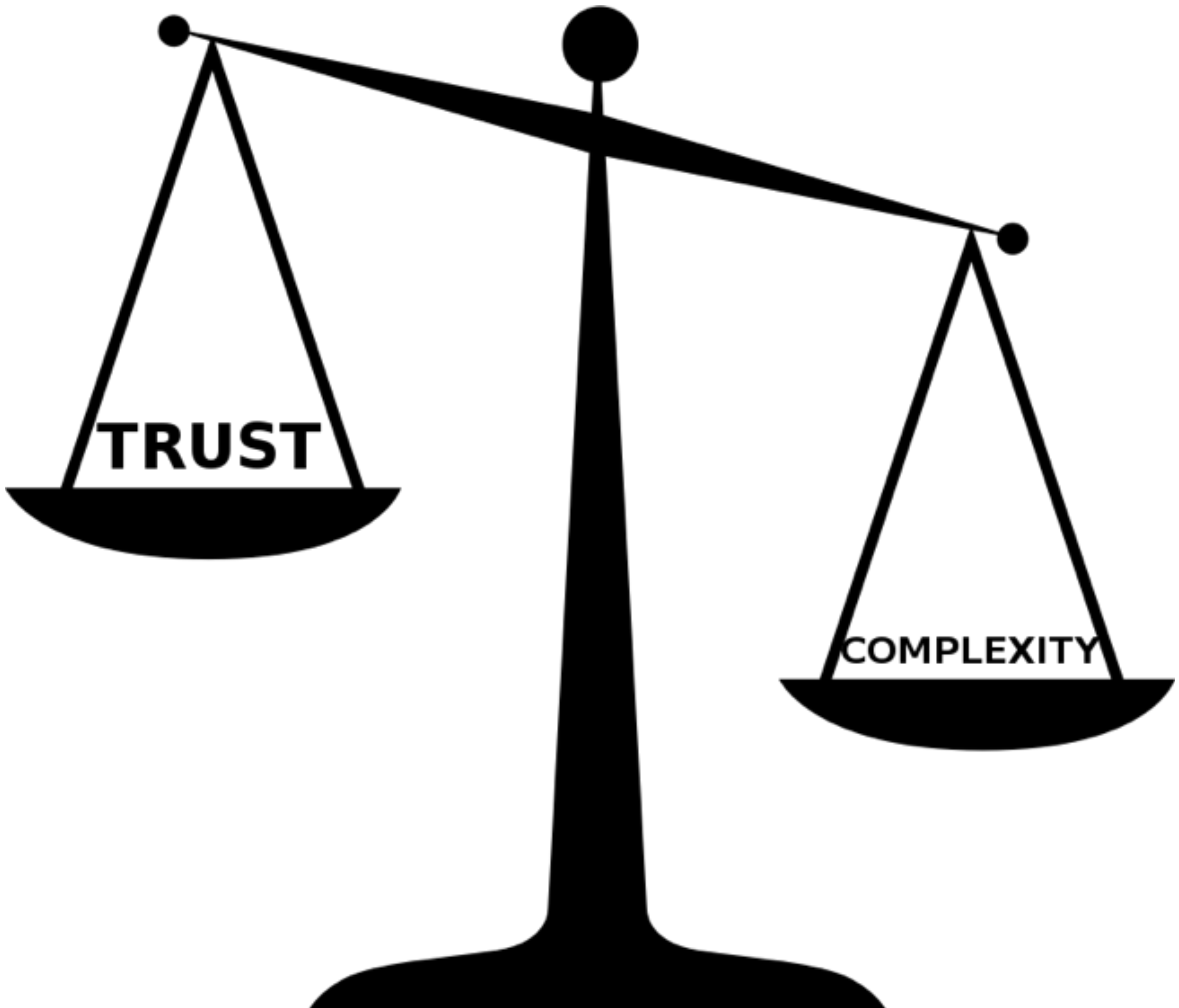




Verification with minimal communicatio
Kapourniotis, Dunjko, Kashefi ASQIC15



Robust and Device-independent Verification
Gheorghiu, Kashefi, Wallden NJP15


TRUST
COMPLEXITY

State of Art

Single Q Device
Restricted quantum verifier

[Aharonov, Ben-Or, Eban '10],
[Fitzsimons, Kashefi'12]
[Morimae '14], [Hayashi, Morimae '15]

Blowing Up the cost

Prepare and send vs. entanglement-based

Online vs. offline

Device-independent vs. one-sided device-independent

I.I.D. states vs. general states

Non-communicating Entangled Q Devices
Classical verifier

[Reichardt, Unger, Vazirani '12]
[McKague '13]

From QKD to verifiable quantum internet

Classical Verifier

1-way Quantum Communication

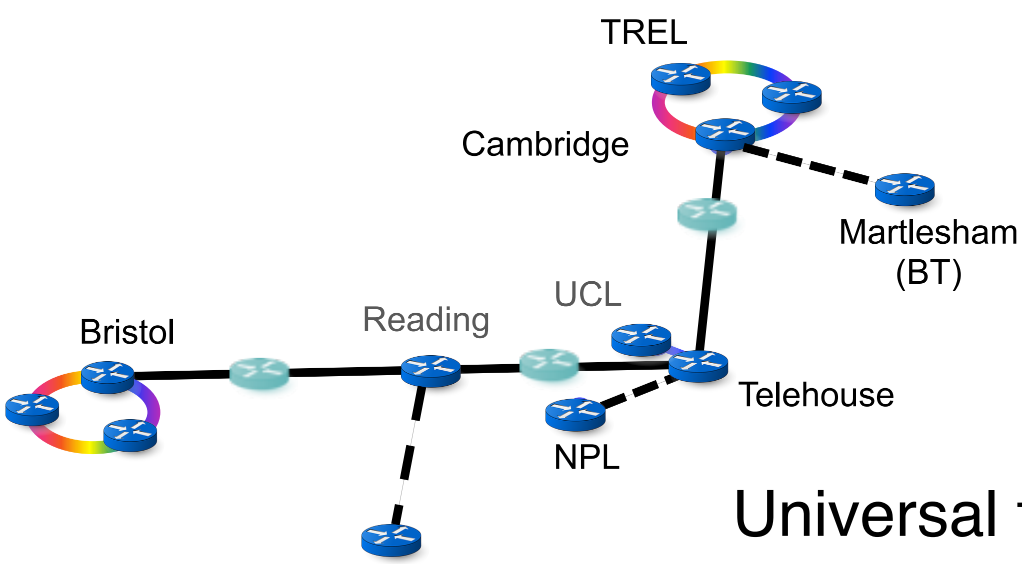
2-way Classical Communication

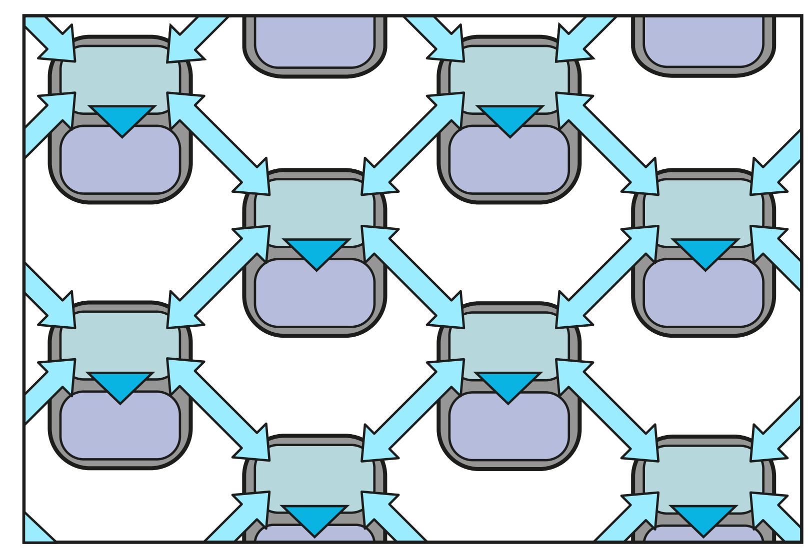
Quantum Device

+

Trusted

random single qubit generator

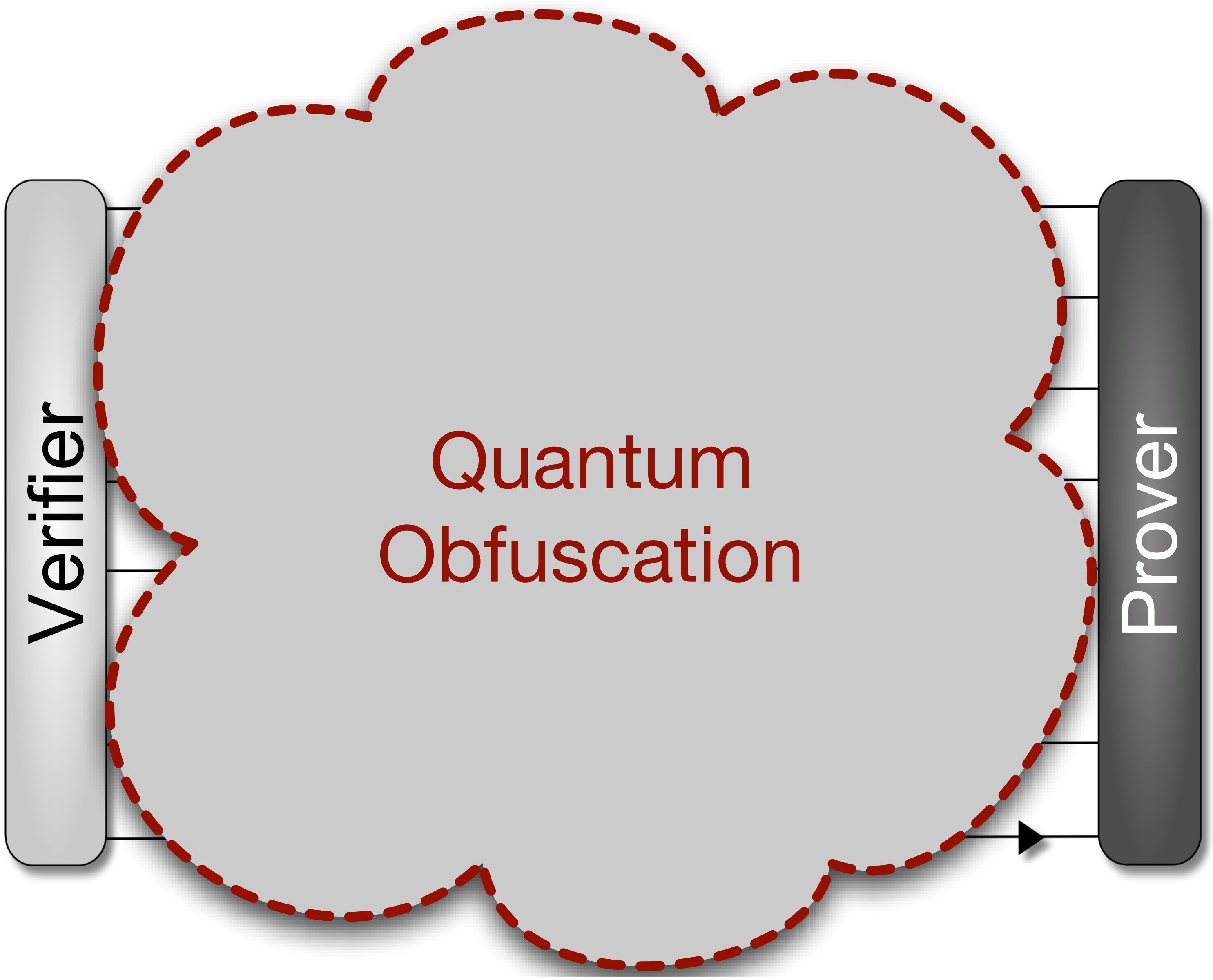




Universal for any quantum computations
Minimal quantum requirements for verifier
Server only learns size of computation (blindness)

Requires photonic interaction with the device

Can we get ride of qubit ?



Alagic, Fefferman, 2016

Perspective

Efficient verification methods for realistic pseudo quantum computers

- Correctness of the outcome
- Operation monitoring
- Quantum property testing

- Architectural constraints
- Experimental imperfections

Perspective

PRACTICAL verification methods for realistic pseudo quantum computers

- Correctness of the outcome
- Operation monitoring
- Quantum property testing

- Architectural constraints
- Experimental imperfections

None-universal:
D-Wave machine
Quantum Simulator

Classical Verification ⟷ **Quantum Verification**

Breakable Security

Server's Time

Universal Machine

Interaction

Thanks to My Collaborators

Theory

Joe Fitzsimons (SUTD)
Anne Broadbent (Ottawa)
Vedran Dunjko (Innsbruck)
Anthony Leverrier (INREA)
Animesh Datta (Oxford)
Tomoyuki Morimae (Japan)

(Edinburgh Group)
Petros Wallden
Anna Pappa
Theodoros Kapourniotis
Alexandru Gheorghiu
Danile Milles

Experiment

Stefanie Barz (Oxford, Vienna)
Philip Walther (Vienna)
Ian Walmsley (Oxford)

EPSRC
Engineering and Physical Sciences
Research Council

PDR positions available
ekashefi@gmail.com