Quantum Turing Test

Elhām Kashefi

THE UNIVERSITY *of* EDINBURGH
informatics

Feynman Vision - 82

Quantum Computing as the technology for simulating quantum systems

Spectacular Progress

from complexity theory to cryptography
from simulation to sampling
from tomography to implementation
from foundation to interpretation

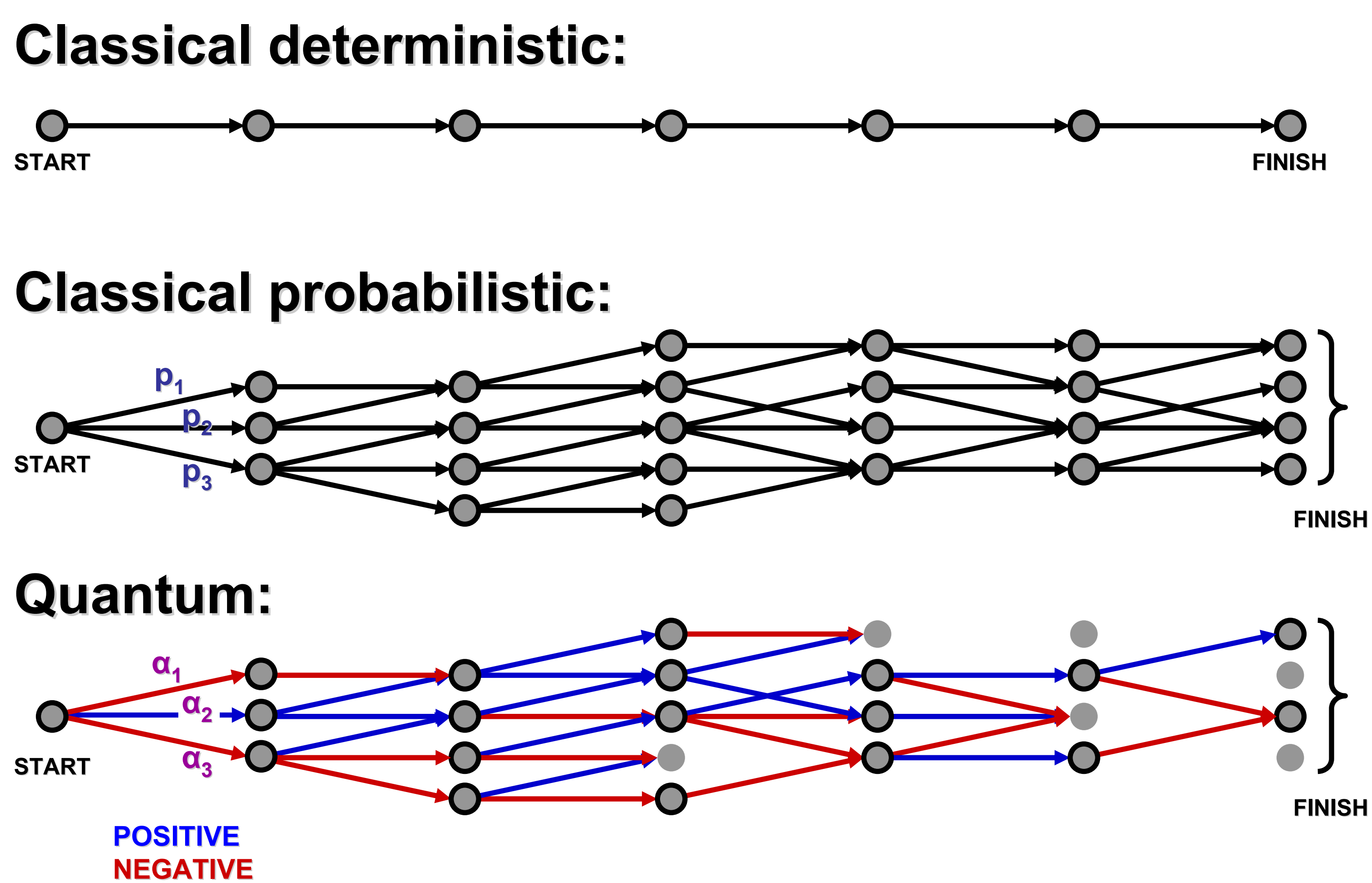
proving what we are actually performing and observing is indeed quantum

Quantum Algorithms - Speed Up

Superpositions

Non-local Correlations

Interference



Quantum Algorithms - History

1985 - Deutsch-Jozsa demonstrated the first speed up

Given a boolean function $f : \{0,1\}^n \rightarrow \{0,1\}$ determine if it is constant or balanced

$$|f\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} |x\rangle$$

The state for any constant function is orthogonal to
the state for any balanced function

Quantum Algorithms - History

1985 - Deutsch-Jozsa demonstrated the first speed up

Given a boolean function $f : \{0,1\}^n \to \{0,1\}$ determine if it is constant or balanced

1994 - Simon's Problem

Given a function $f : \{0,1\}^n \to \{0,1\}^n$ finds a such that $f(x+a) = f(x)$.

Breakthrough

1994 - Shor's Period Finding Problem

Given an n-bit integer, find the prime factorisation. Breaks the RSA cryptosystem

Quantum Algorithms - History

The Zoo - Stephen Jordan - 175 papers

http://math.nist.gov/quantum/zoo

Buchman-Williams cryptosystem

Elliptic curve cryptography

Algebraic and Number Theoretic Algorithms

Exponential Speed Up: Factoring, Discrete-log, Pell's Equation, Principal Ideal, Unit Group, Class Group, Gauss Sums, Matrix Elements of Group Representations

Oracular Algorithms

Broad Application: Unstructured Search, Amplitude Amplification, Collision Finding, Hidden subgroup Problem, Formula Evaluation, Linear Systems, Group Isomorphism, Network Flows

Approximation and Simulation Algorithms

Inspired by Physic : Quantum Walk, Quantum Simulation, Knot Invariants, Partition Functions, Adiabatic Optimization, Simulated Annealing

Quantum Algorithms - Perspective

Quantum Simulators

One controllable quantum system to investigate another, less accessible one

tackling problems that are too demanding for classical computers

Ultracold quantum gases, Trapped ions, Photonic, Superconducting circuits

Refuting the Strong Church-Turing Thesis

Our communication today is secure only if
we cannot build a large scale quantum computer

Quantum Cryptography - Security

Quantum cryptography relies on the laws of quantum mechanics
to offer unconditional security

Measurement perturbs the system

Uncertainty Principles

No Cloning

No perturbation ⇒ No measurement ⇒ No eavesdropping

Quantum Cryptography - History

Wiesner 1983

The first link between secrecy and quantum physics quantum money

Bennett and Brassard 1984, Ekert 1991

Public key distribution problem

Cleve, Gottesman and Lo, 1999; Crepeau, Gottesman and Smith, 2005

Quantum Secret Sharing

Quantum Cryptography - History

Lo, Chau, Mayers 1997
Impossibility of quantum bit commitment

Damgaard et al., 2005, 2007; Wehner, Schaffner and Terhal, 2008
New paradigms of bounded-storage models

Gottesman and Chuang 2001
Quantum digital signature

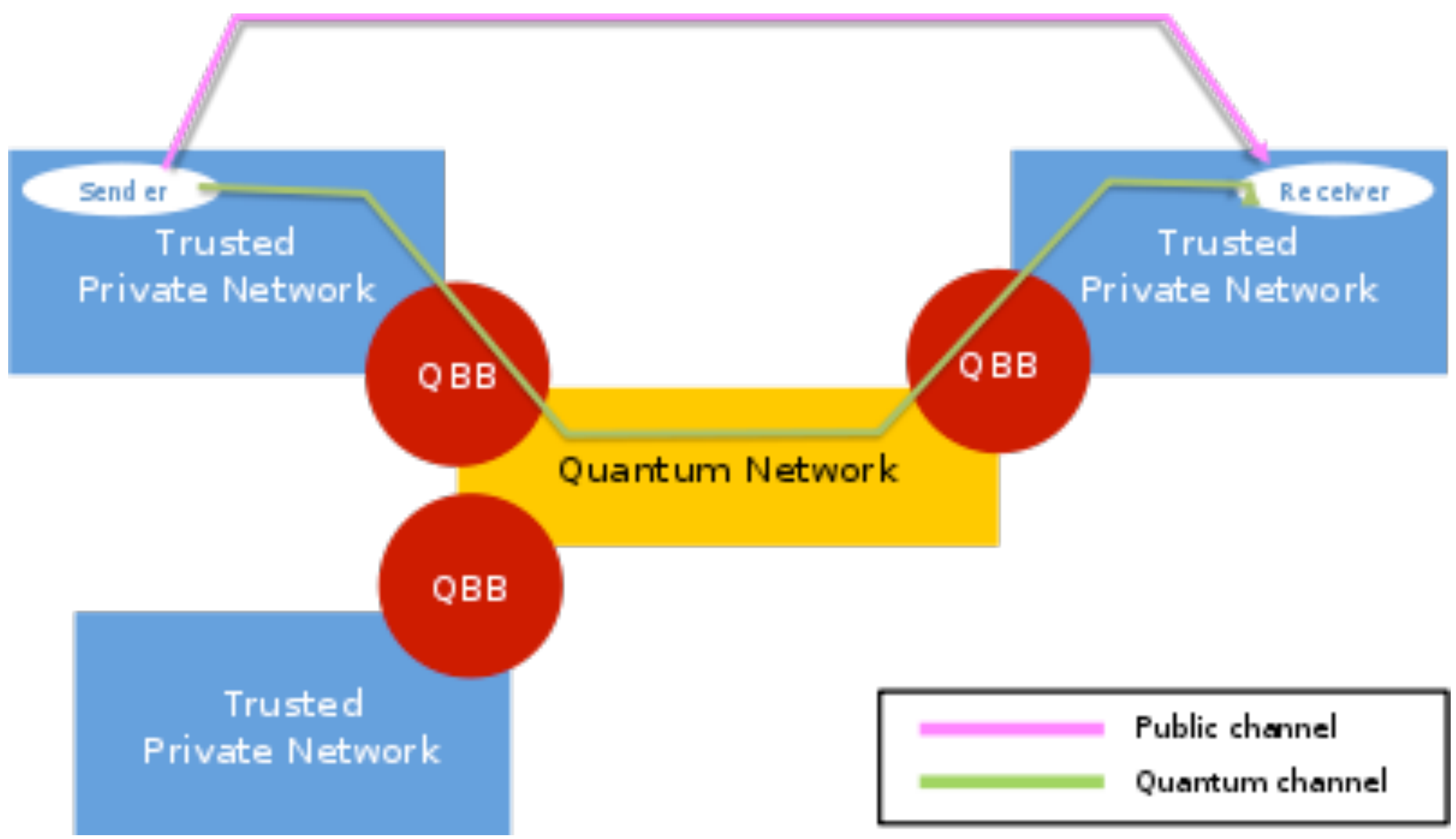
Kitaev 2003, Chailloux and Kerenidis 2009
Perfect quantum coin flipping is impossible, but better than classical protocols exist

Broadbent, Fitzsimons and Kashefi 2009
Unconditionally secure quantum delegated computation

Quantum Cryptography - Perspective

Quantum Key Distribution Networks

SECOQC: 2008, 200 km of standard fibre optic cable to interconnect six locations across Vienna and St Poelten



Quantum Cryptography - Perspective

Quantum Key Distribution Networks

DARPA: 10-node, has been running since 2004 in Massachusetts
BBN Technologies, Harvard University, Boston University and QinetiQ

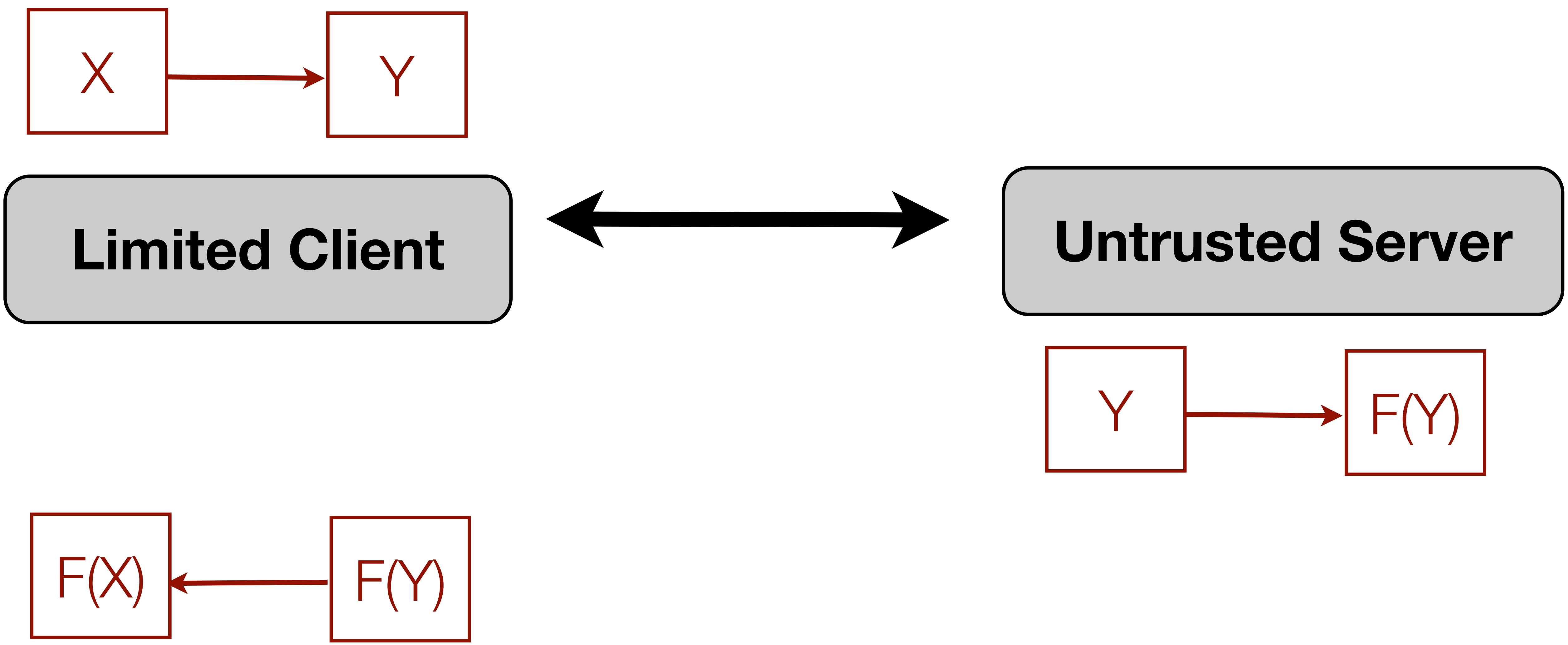
Tokyo QKD Network: 7 partners NEC, Mitsubishi Electric, NTT and NICT,
Toshiba Research Europe Ltd. (UK), Id Quantique (Switzerland) and All Vienna

China and Austria Earth - Satellite QKD

Secure Cloud Computing

How to make cloud computing safe?

A model for enabling convenient, on-demand network access to
a shared pool of configurable computing resources



Secure Cloud Computing

Rivest, Adleman and Dertouzos 1979
Can we process encrypted data without decrypting it first ?

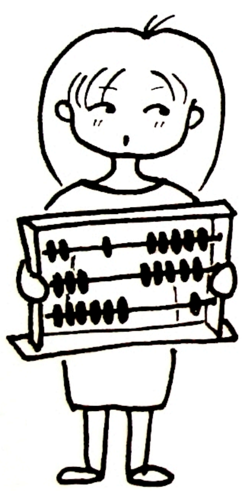
Fully homomorphic encryption

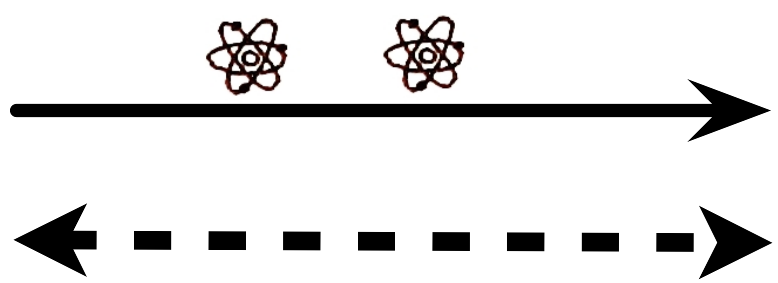
Classical: Gentry 2009
Only computational security

assumption of limited computational power of the adversary

Quantum: Broadbent, Fitzsimons, and Kashefi 2009
Unconditional security

Qcomputing + Qcryptography = Blind Q Computing





Classical Communication

Classical Computer

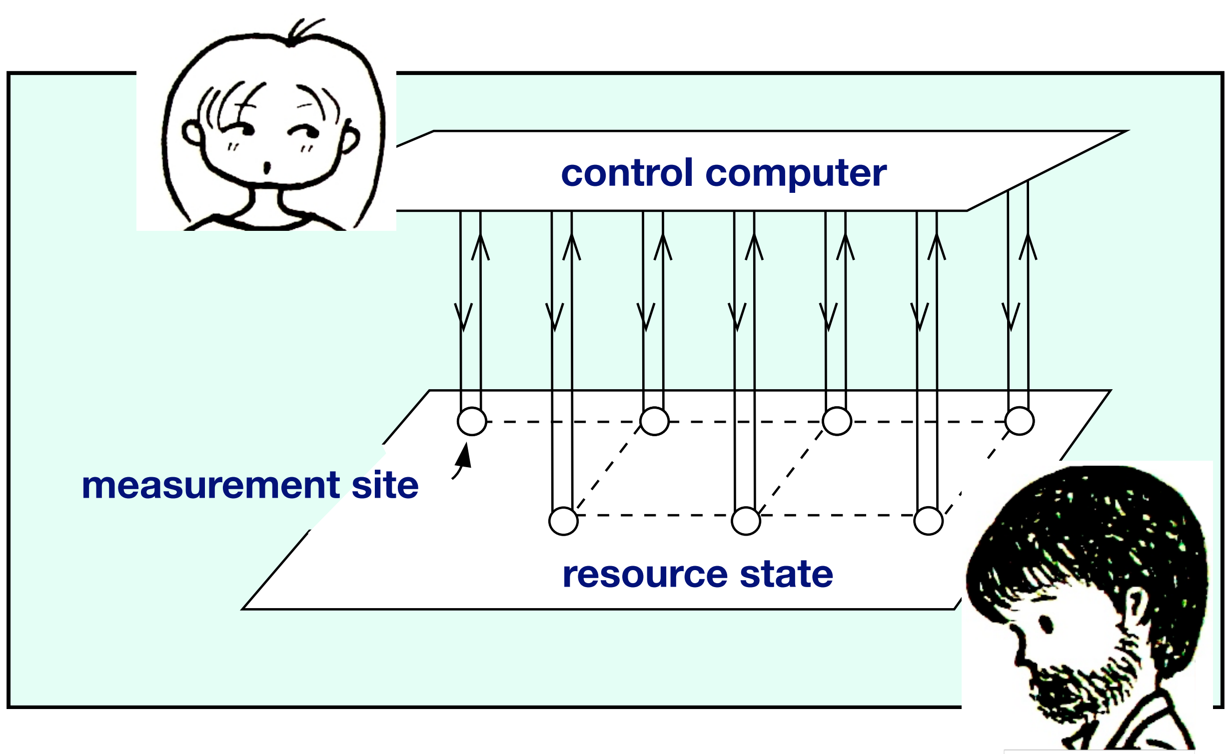
random single qubit generator

Unconditional Perfect Privacy

Server learns nothing about client's computation

Measurement-based Quantum Computing

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



Hide

- Angles of measurements
- Results of Measurements

Universal Blind Quantum Computings

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

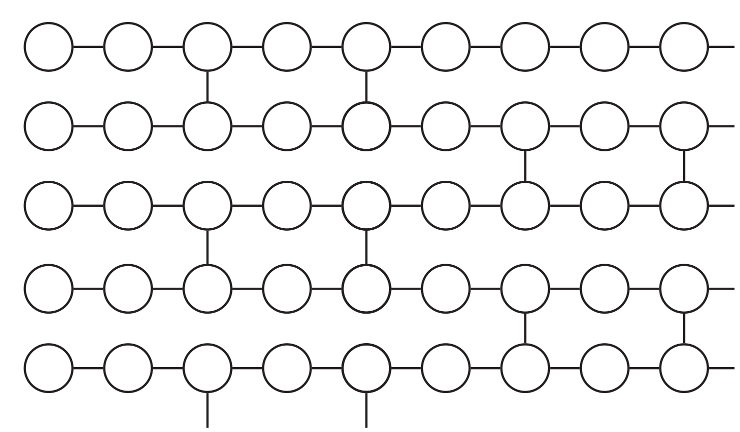
θ θ'

random single qubit generator

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

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

$\delta_{x,y}$



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

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

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

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

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

Blindness

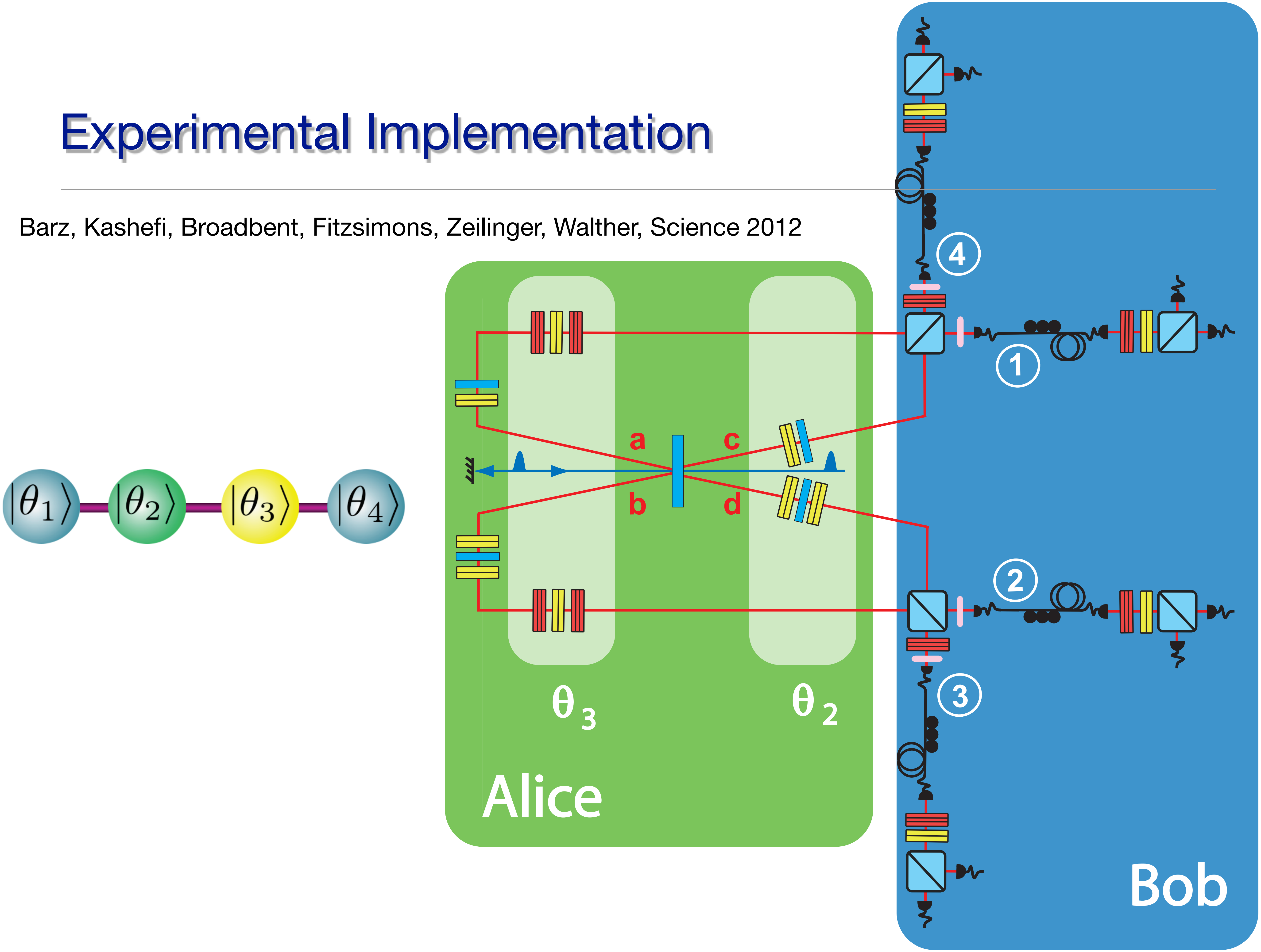
Protocol P on input $X = (\tilde{U}, \{\phi_{x,y}\})$ leaks at most $L(X)$

➡ The distribution of the classical information obtained by Bob is independent of X

➡ The quantum state is fixed and independent of X

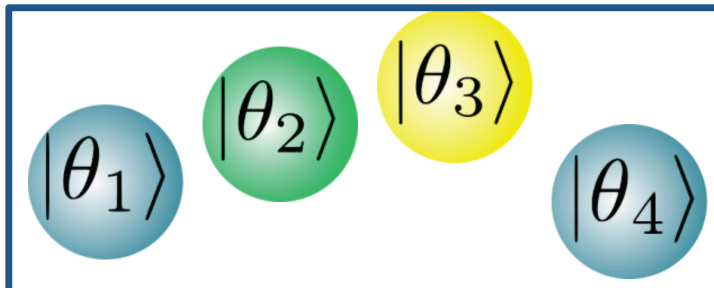
Experimental Implementation

Barz, Kashefi, Broadbent, Fitzsimons, Zeilinger, Walther, Science 2012



Experimental Implementation

Client:
limited computational power

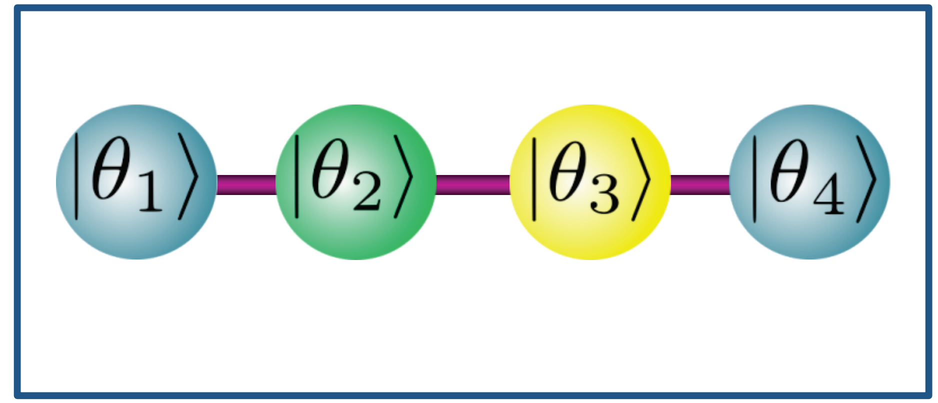


$$|\theta_j\rangle = 1/\sqrt{2}(|0\rangle + e^{i\theta_j}|1\rangle)$$

$$\theta_j \in \{0, \pi/4, \ldots, 7\pi/4\}$$

Prepares random qubits

Quantum server:
full power of Quantum Computation



Entangles qubits

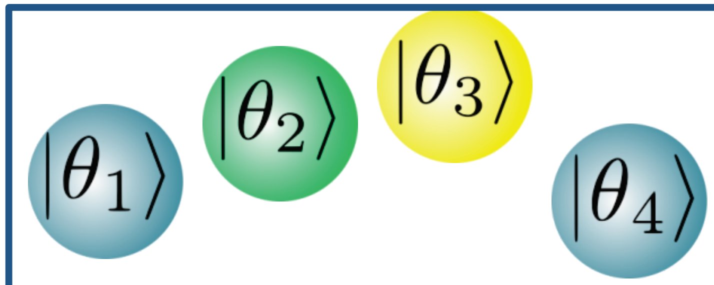
$$\delta_j = \theta_j + \phi_j + \pi r_j$$

Computes measurement angles

- Measurement instruction for server
- Initial rotation of the qubit
- Target rotation
- Random bit flip

Experimental Implementation

Client:
limited computational power

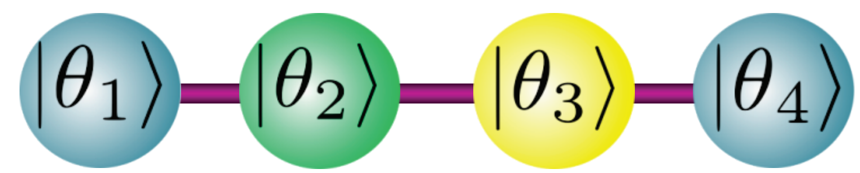


$|\theta_j\rangle = 1/\sqrt{2}(|0\rangle + e^{i\theta_j}|1\rangle)$

$\theta_j \in \{0, \pi/4, \ldots, 7\pi/4\}$

Prepares random qubits

Quantum server:
full power of Quantum Computation

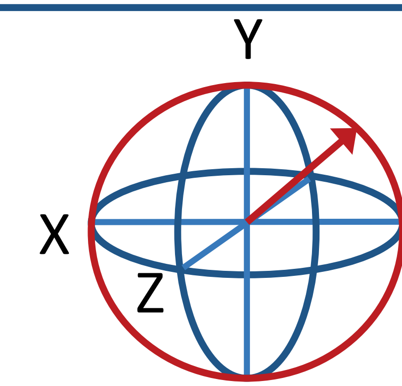


Entangles qubits

$$\delta_j = \theta_j + \phi_j + \pi r_j$$

Computes measurement angles

δ_j



Measurement in X-Y plane

$|\delta_j\rangle = 1/\sqrt{2}(|0\rangle + e^{i\delta_j}|1\rangle)$

0, 1

Decryption: Output of the computation

Quantum Cloud

BBC

Quantum computing could head to 'the cloud', study says

ComputeScotland

Girls lock-up quantum security

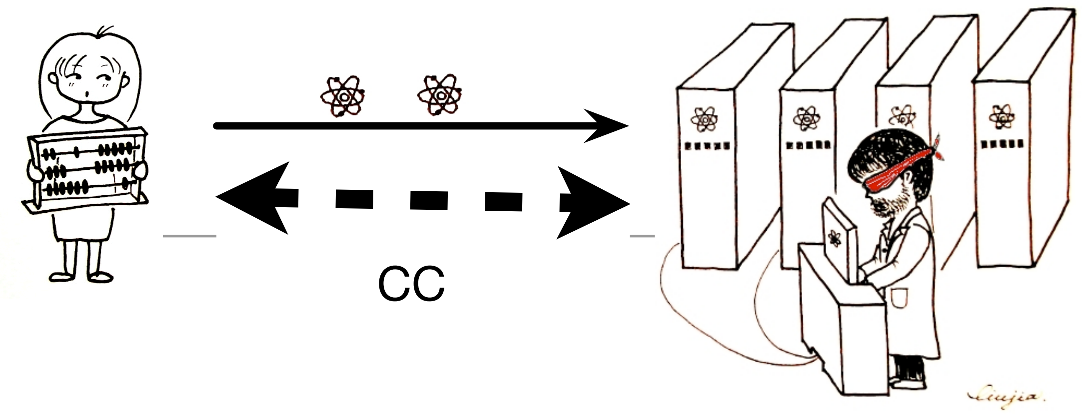
Almost as intriguingly, the research has been carried out by a team three of them being women.

TechNewsWorld
ALL TECH - ALL THE TIME

The Blind Quantum Security Eschaton

Quantum computers "can decrypt any non-quantum method near-instantly, in theory, rendering all existing forms of encryption obsolete," Enderle pointed out. "This will make the concerns surrounding Iran's nuclear efforts seem trivial by comparison if a [foreign] country gets there first."

Blind Q Computing World



Other approaches

D. Aharonov, M. Ben-Or, and E. Eban, ICS 10 (2010)
A. Childs, Quant. Inf. Compt. (2005)
P. Arrighi and L. Salvail, Int. J. Quant. Inf. (2006)

Approximate Protocol

Dunjko, Kashefi, Leverrier, PRL, 2012

Robust Protocol

Morimae, Dunjko, Kashefi, arXiv:1009.3486
Morimae, Fujii, Nature Communications, 2012
Morimae, PRL, 2012

Minimal Protocol

Dunjko, Kashefi, Markham

Composable Protocol

Dunjko, Fitzsimons, Portmann, Renner, arXiv:1301.3662 (2013)

Other Models

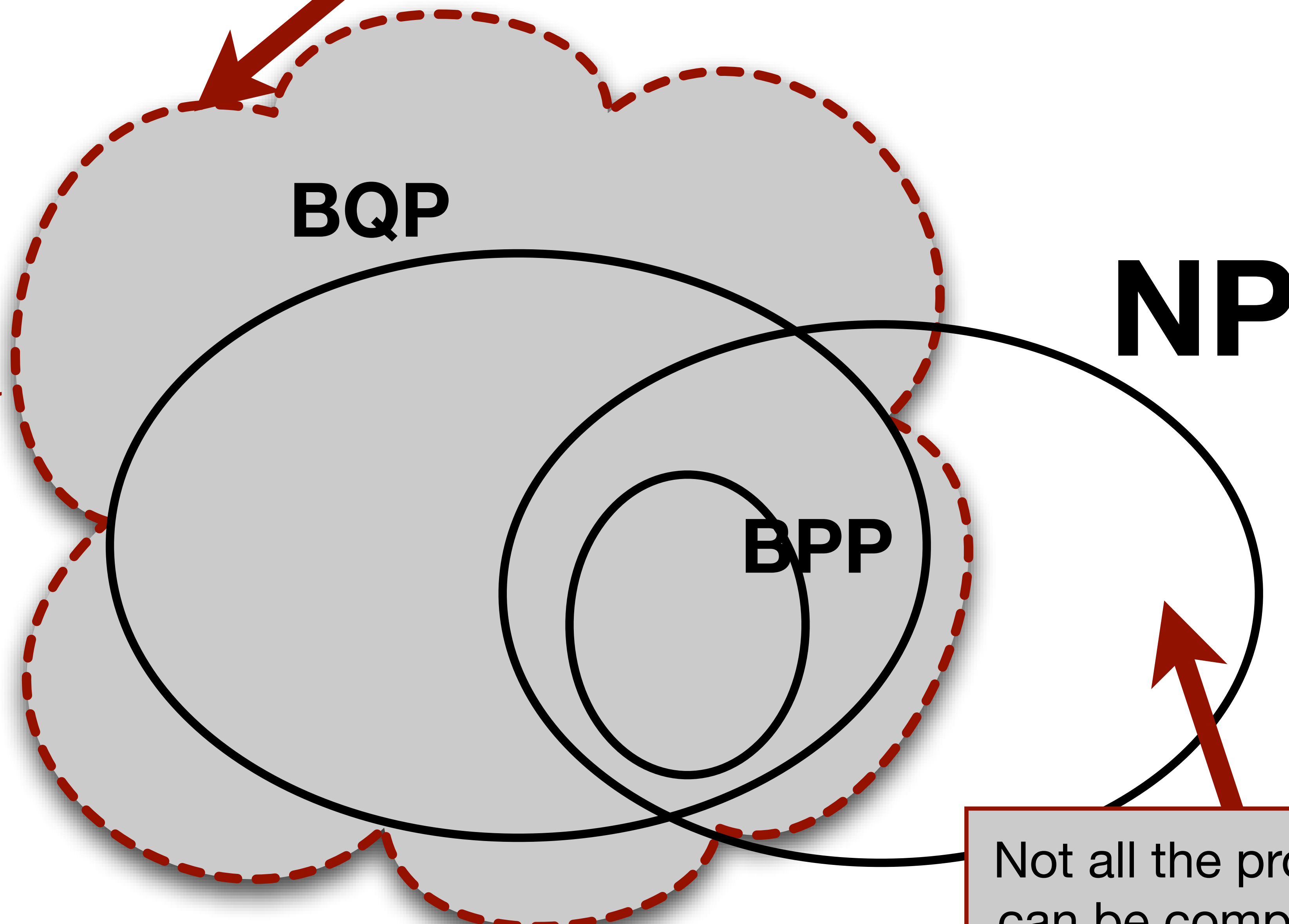
Datta, Kapourtionis, Kashefi, One-clean qubit

Big Picture

Still requires 2^n parameters for a classical computer to simulate it

How do we verify the Solution ?

Can we verify it with a classical Computer ?



Blind Computation with **BPP*** Alice

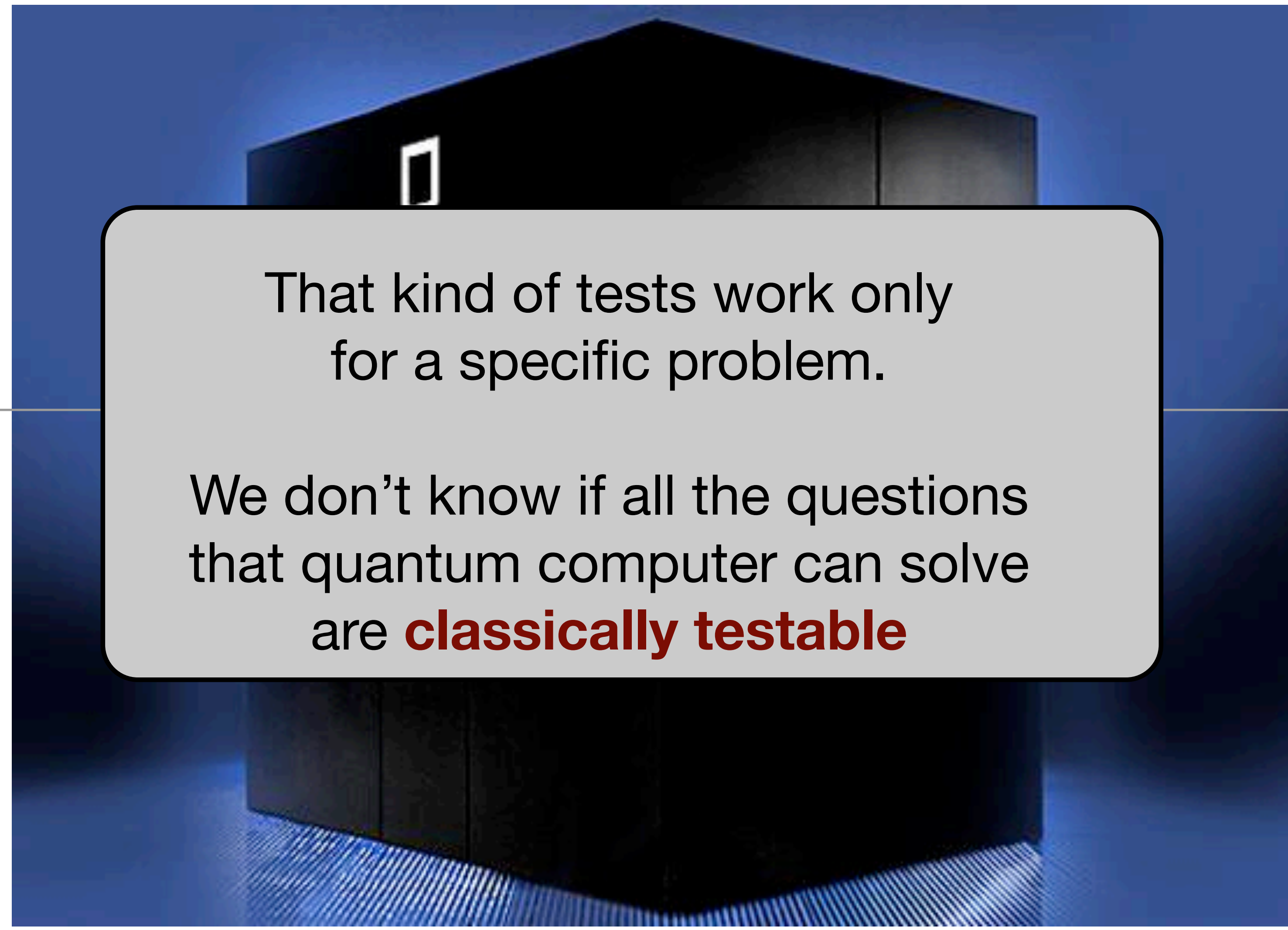
Not all the problem in NP can be computed blindly with a BPP Alice

- Abadi, Feigenbaum and Kilian

The Ultimate Challenge

Quantum Verification

Should we pay $10000000 for a quantum computer



That kind of tests work only for a specific problem.

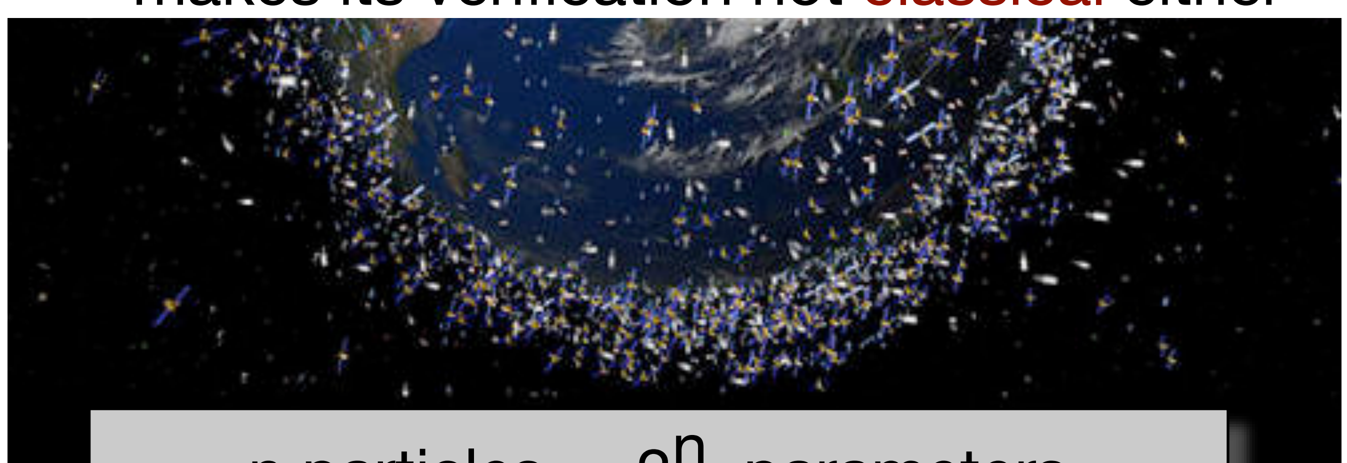
We don't know if all the questions that quantum computer can solve are **classically testable**

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

Exponential World

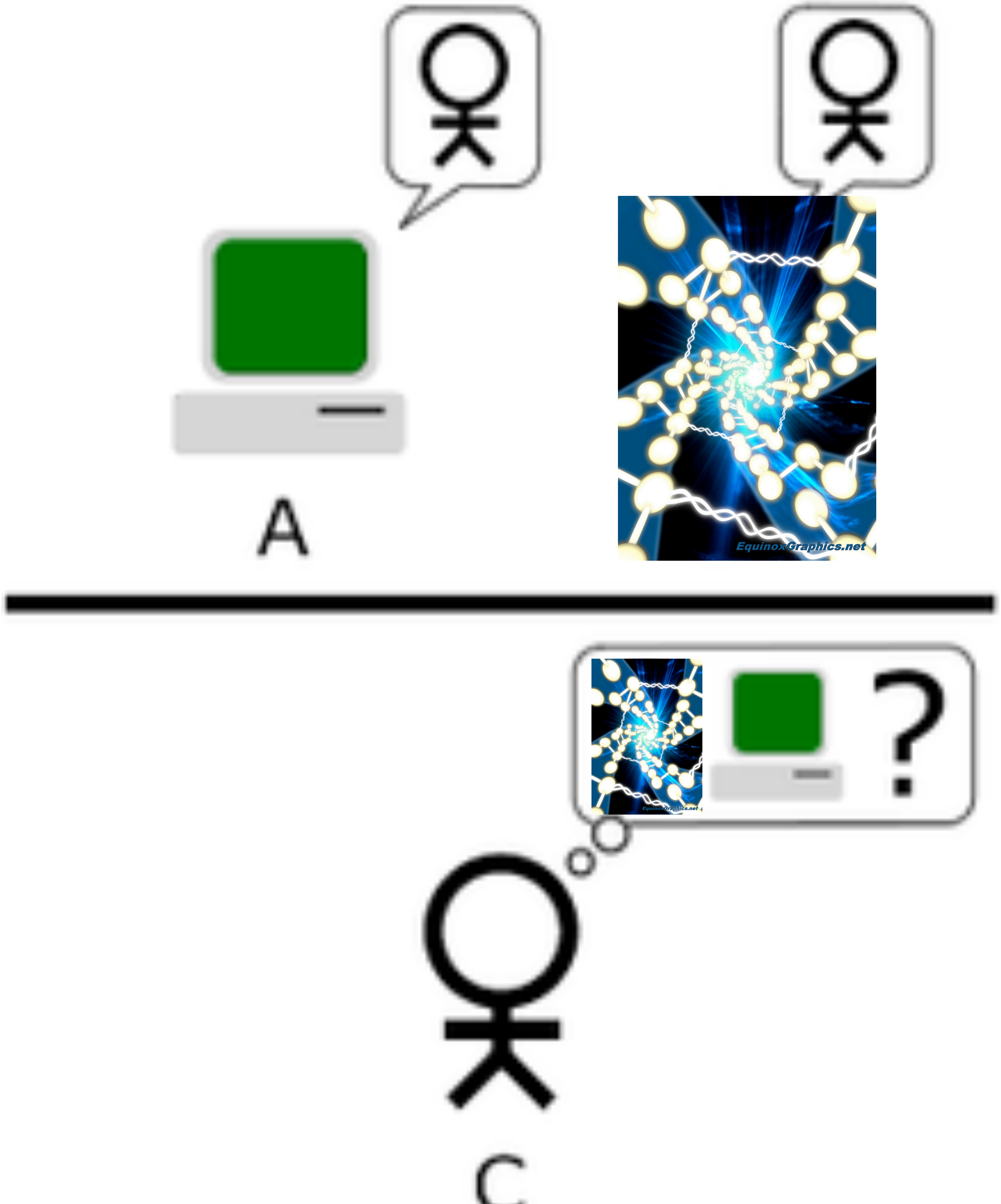
Hilbert space is a huge place.

What makes quantum not classical
makes its verification not classical either

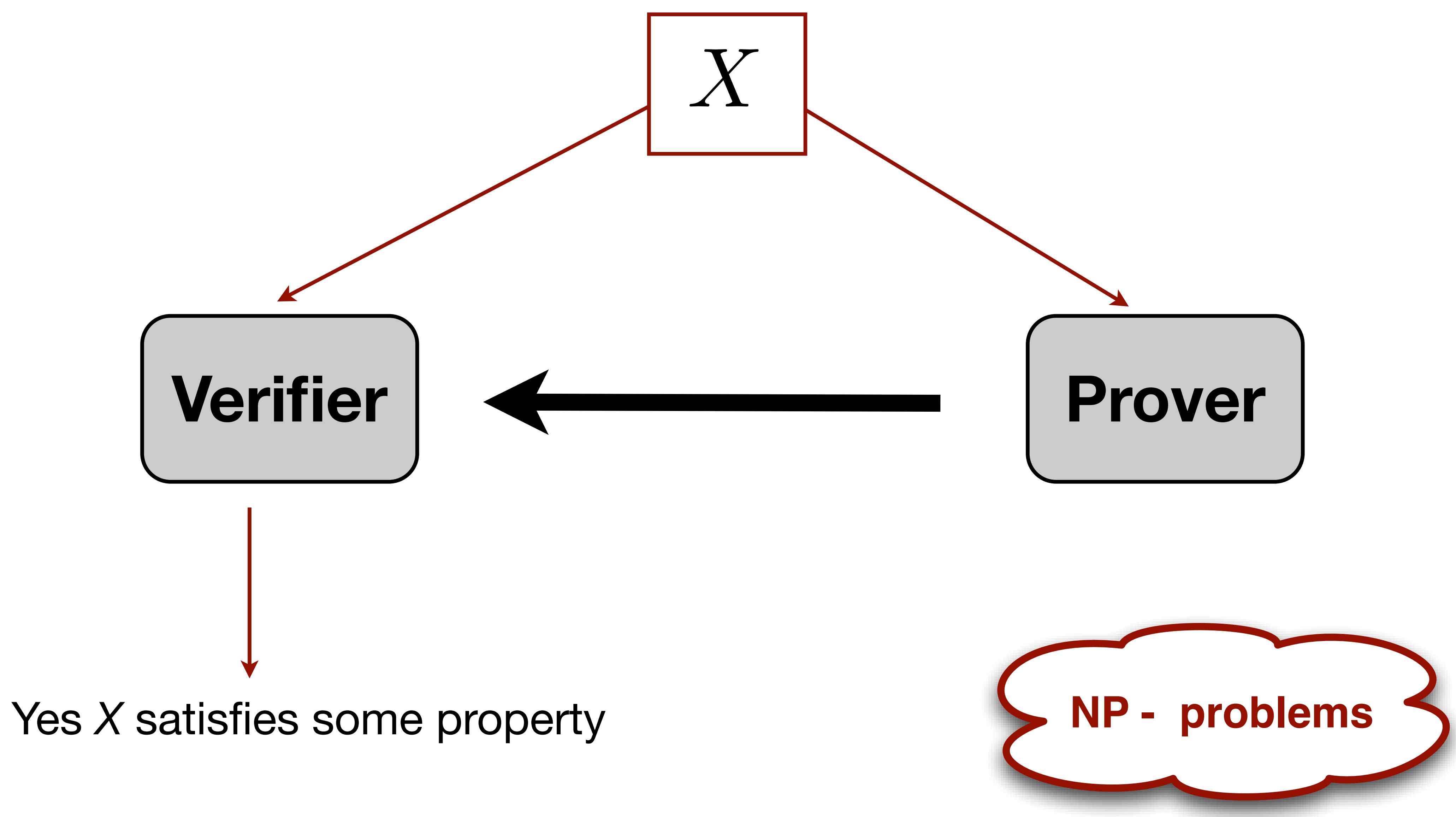


n particles $= 2^n$ parameters

Quantum Turing Test

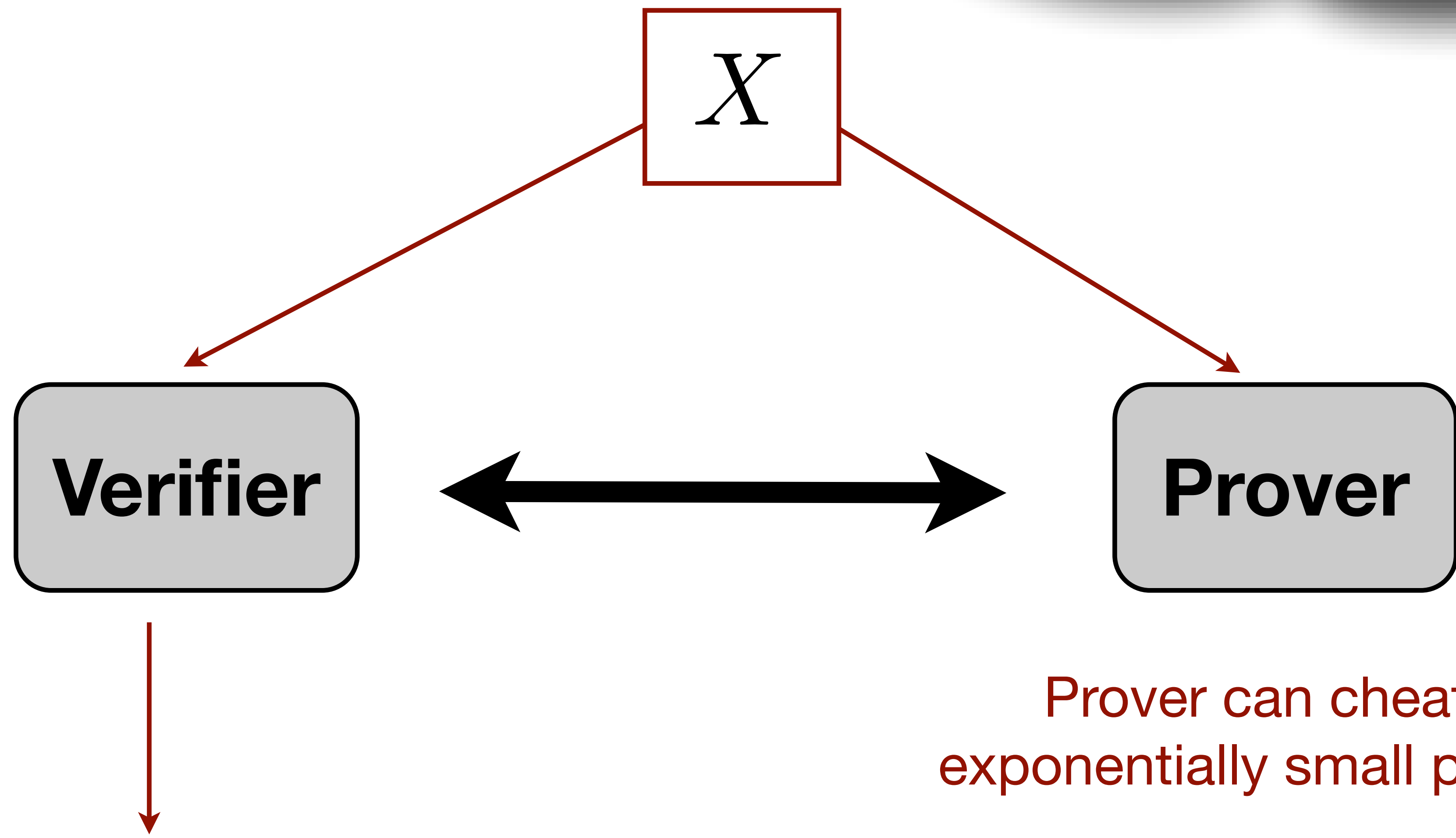


Proof System



Interactive Proofs

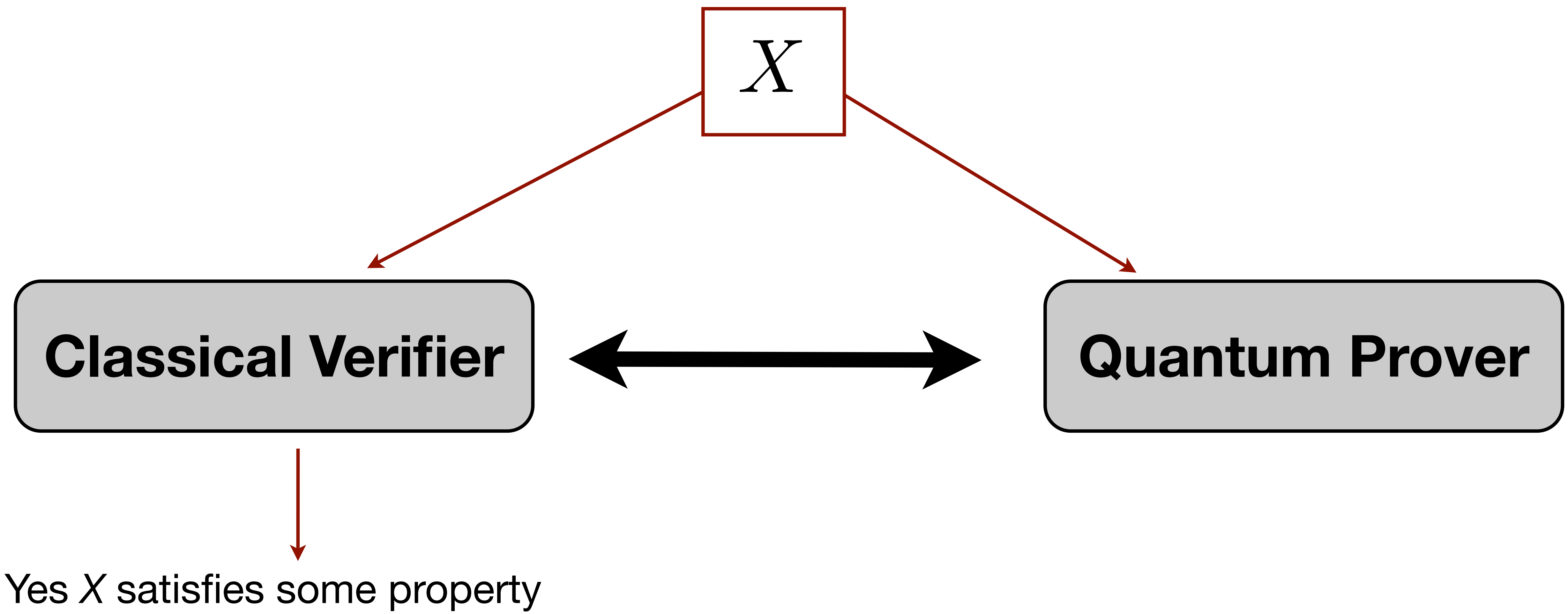
All problems



Prover can cheat with exponentially small probability

Yes X satisfies some property

Can we Classically test Quantum Mechanics ?



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

Does every language in the class BQP admit an interactive protocol where the prover is in BQP and the verifier is in BPP?

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 vs Authentication

$|\psi\rangle$

Eve

Alice

$k \in \mathcal{K}$

m-qubit message

$m + d$

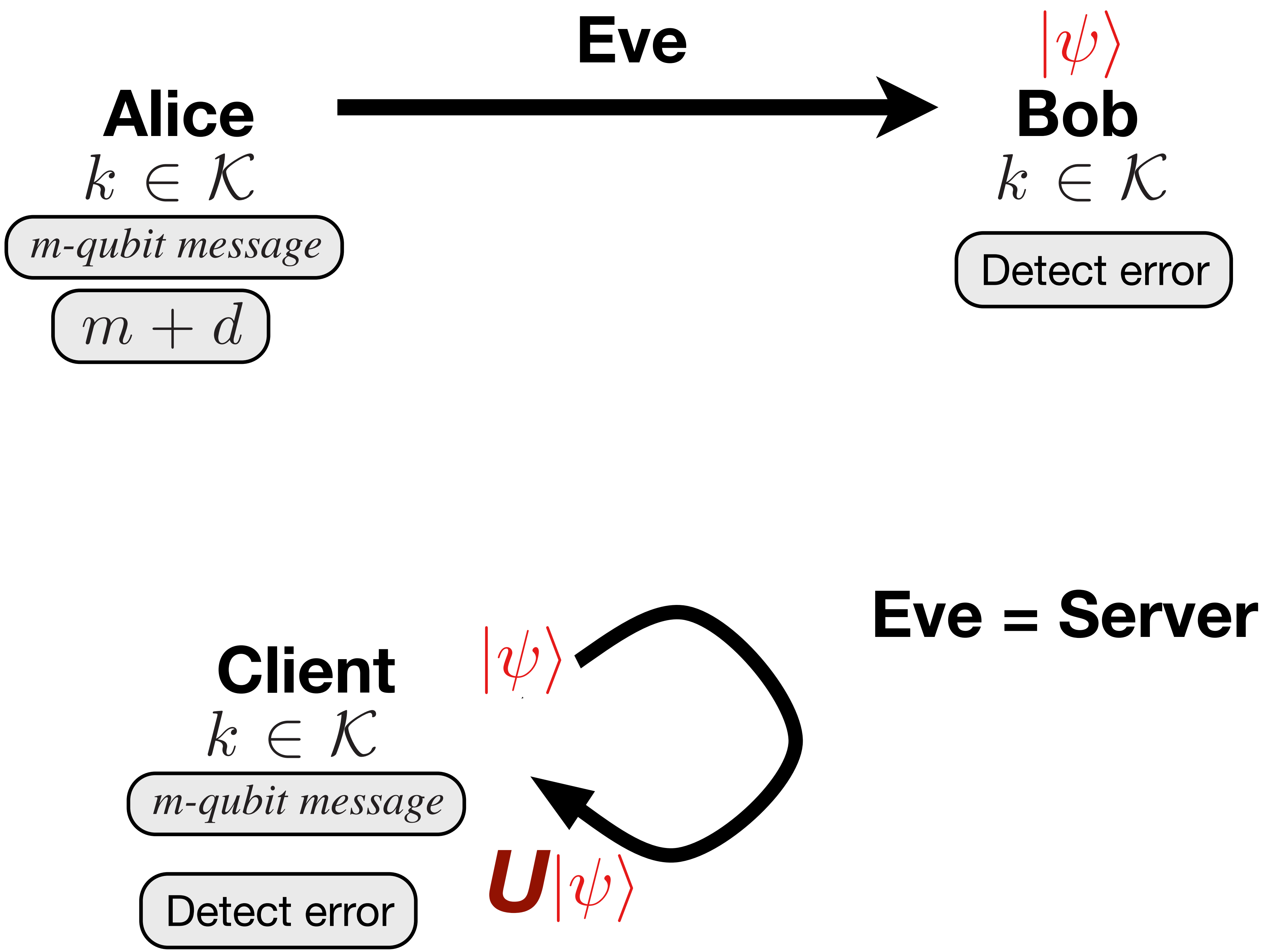
Bob

$k \in \mathcal{K}$

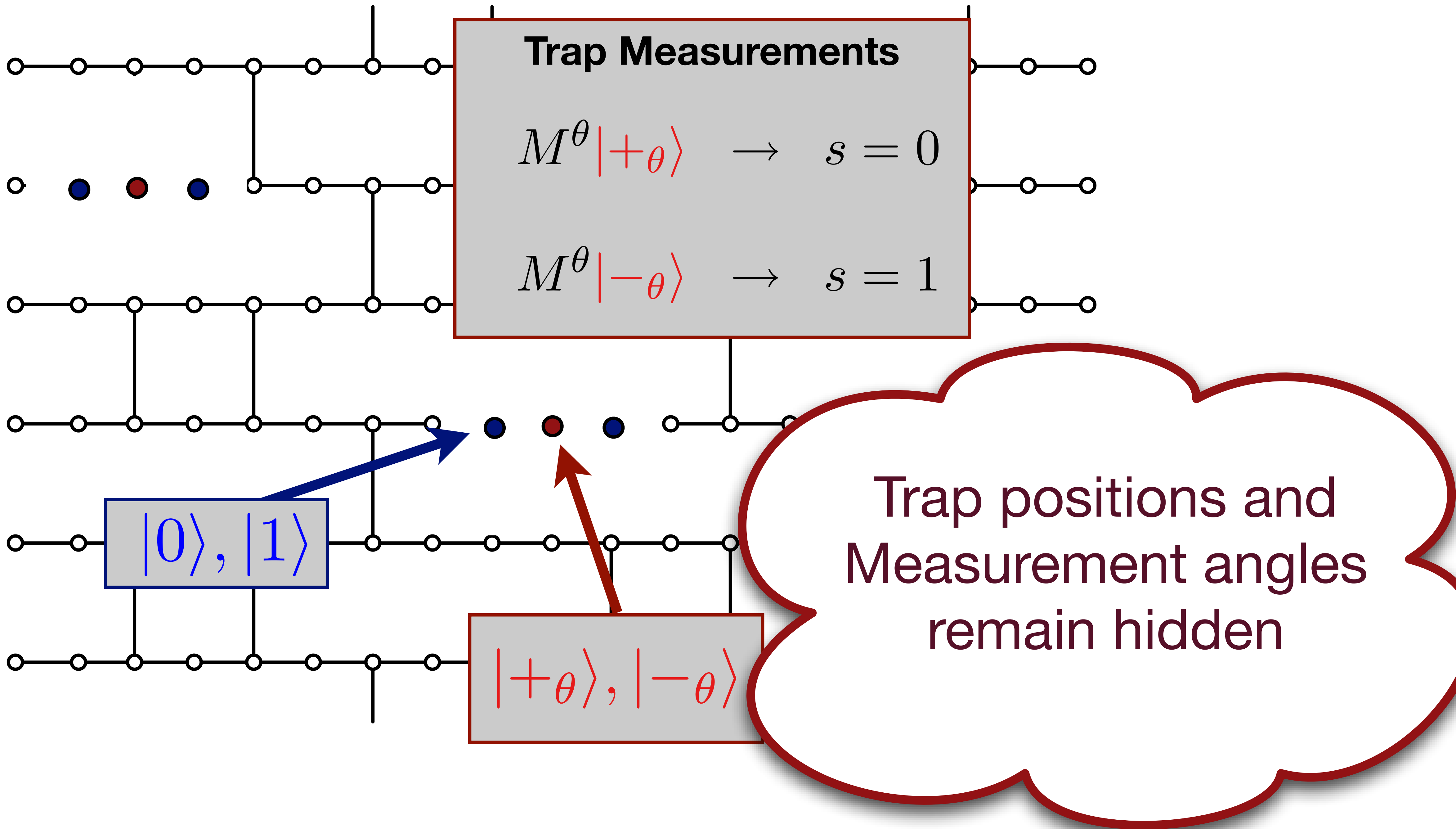
Detect error

Barnum, Crepeau, Gottesman, Smith and Tapp, FOCS02

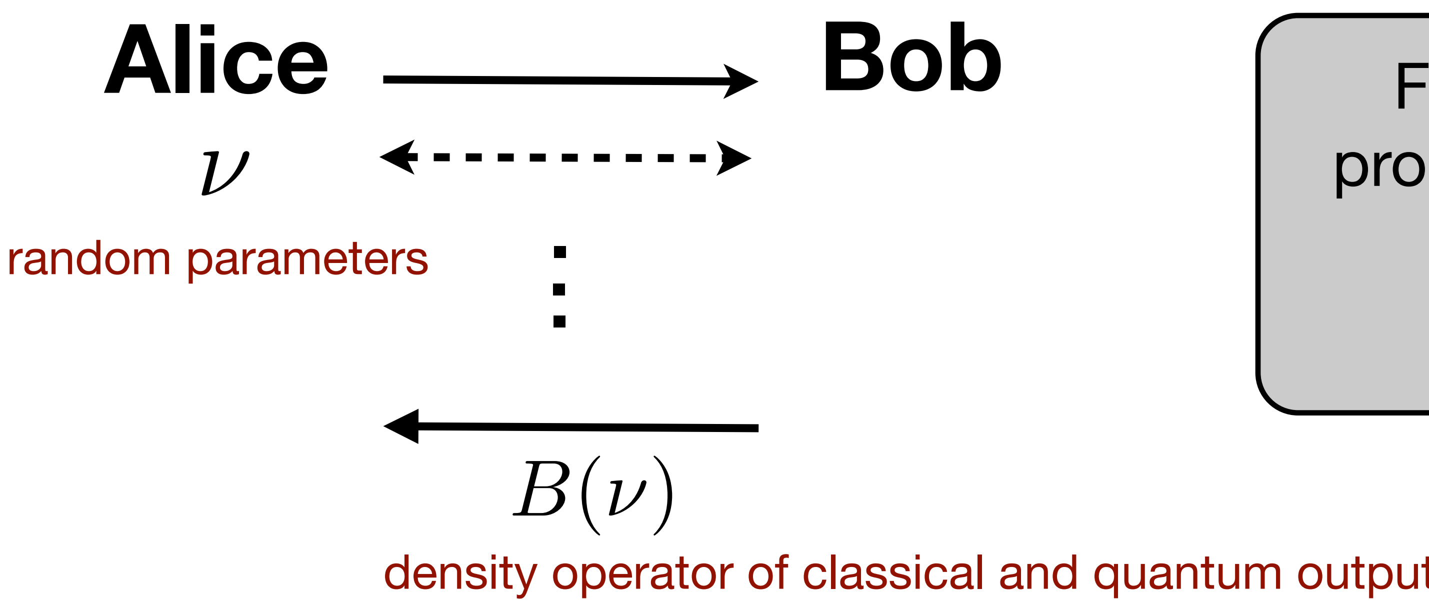
Verification vs Authentication



Adding Traps



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

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

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.

Probability Amplification

To increase the probability of any local error being detected

O(N) many traps in random locations

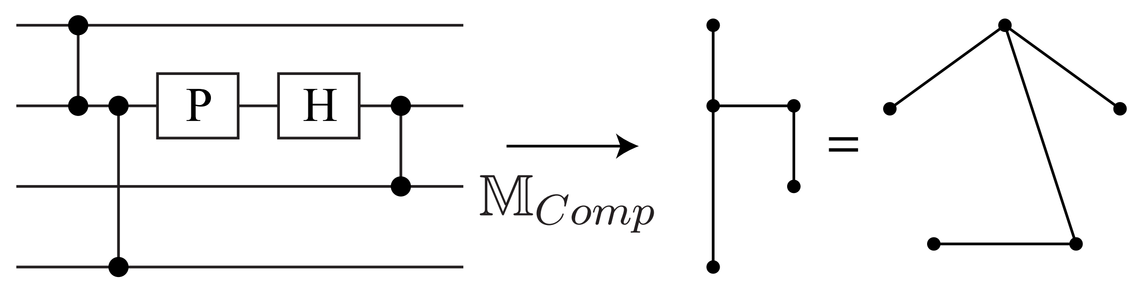
To increase the minimum weight of any operator which leads to an incorrect outcome

Fault-Tolerance

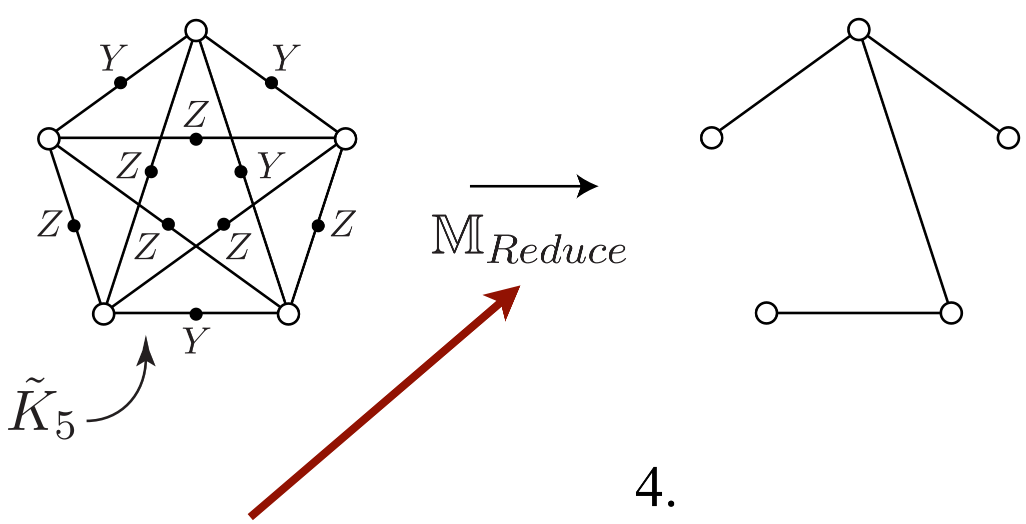
Probability Amplification

Challenge: Traps break the graph

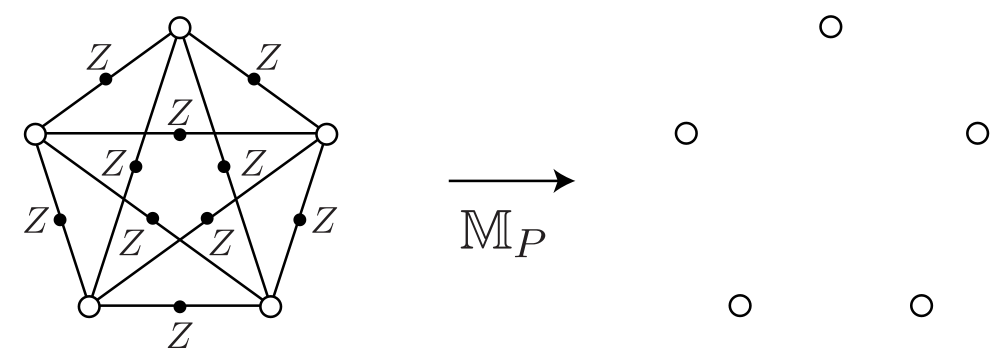
1.



2.

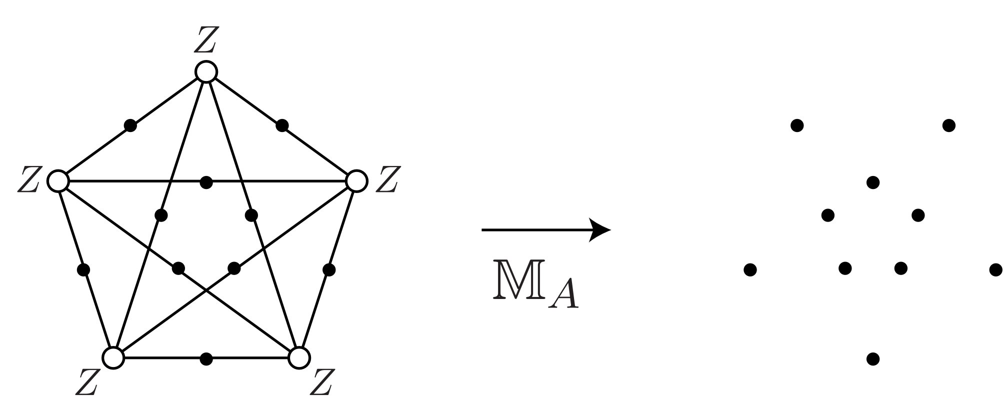


3.

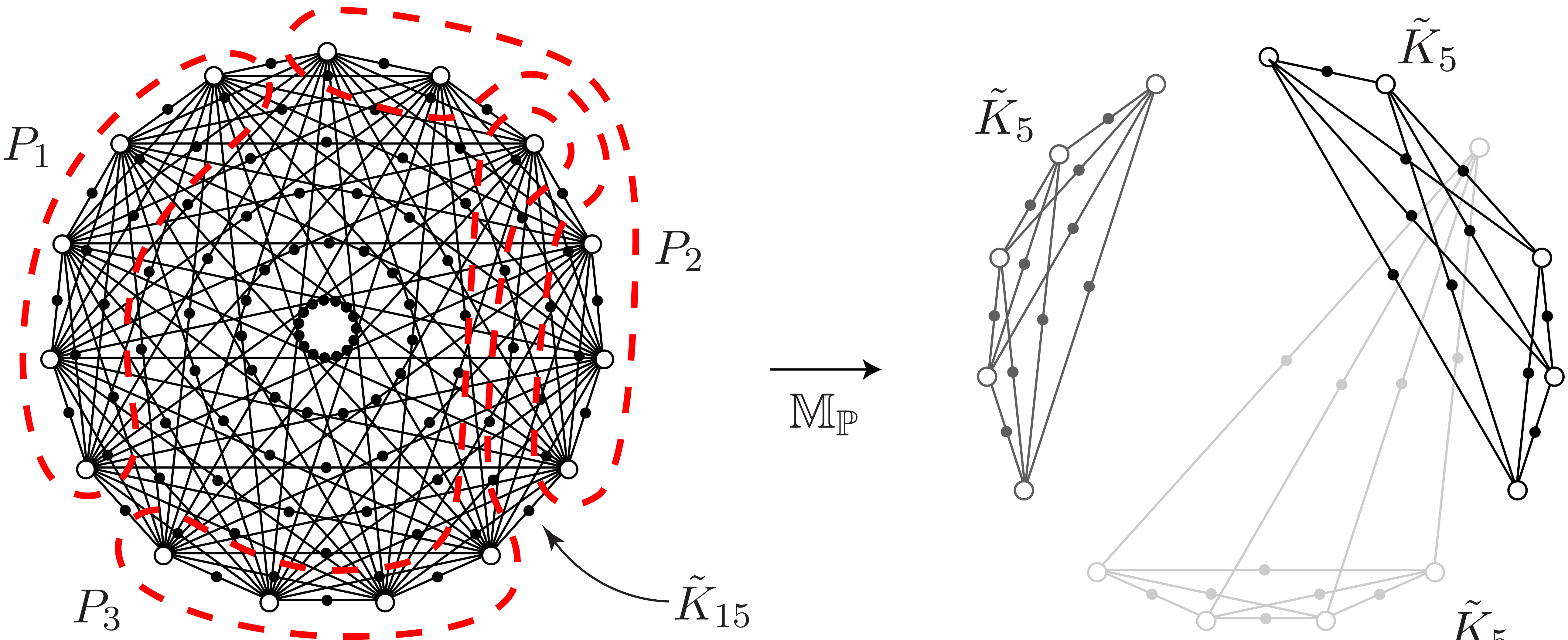


Required 3D lattice for Raussendorf, Harrington and Goyal Topological error-correcting code with defect thickness *d*

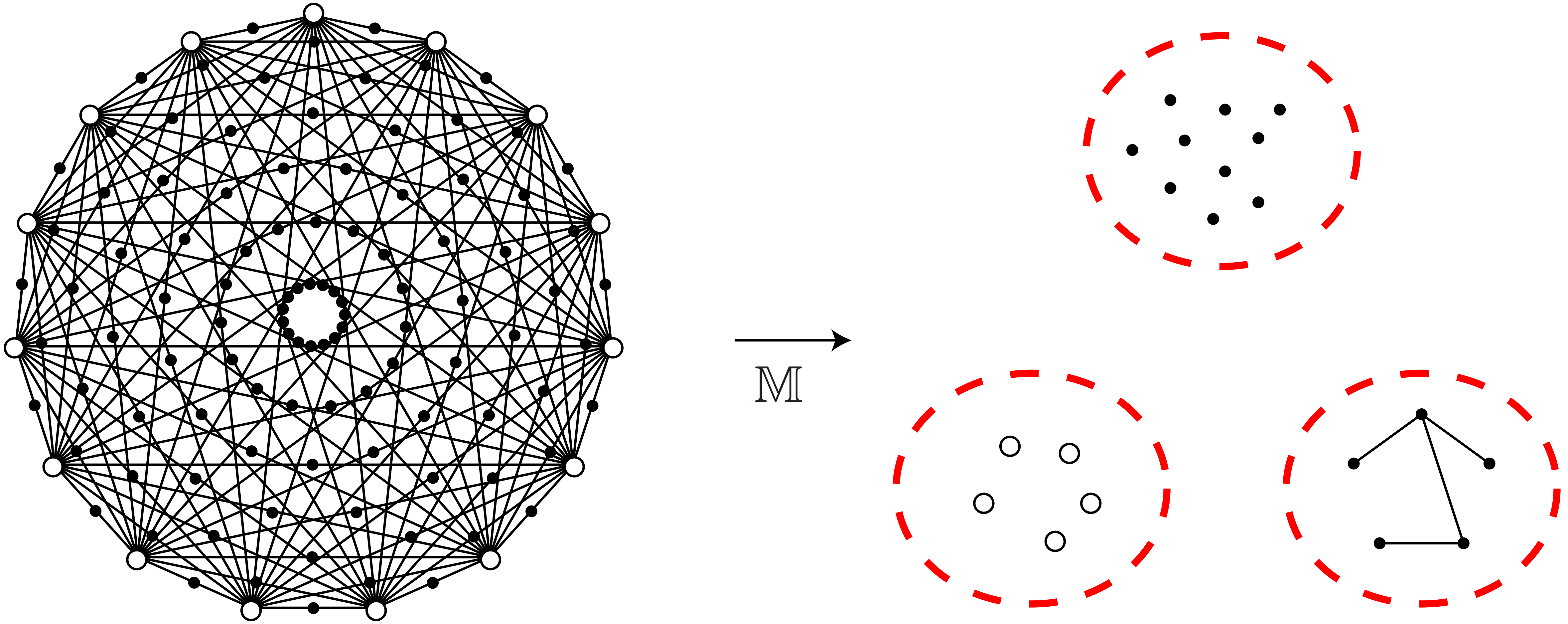
4.



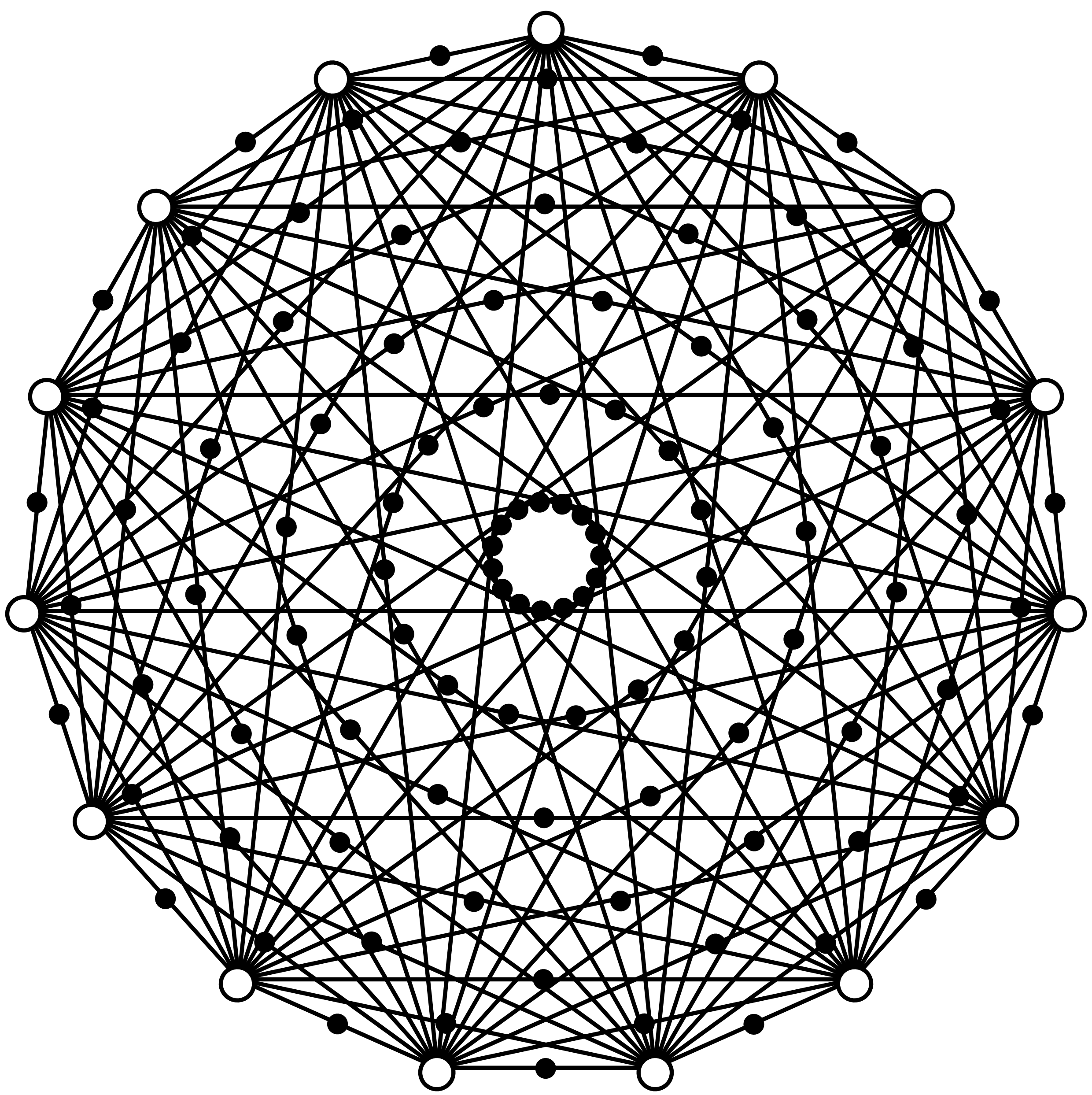
Probability Amplification

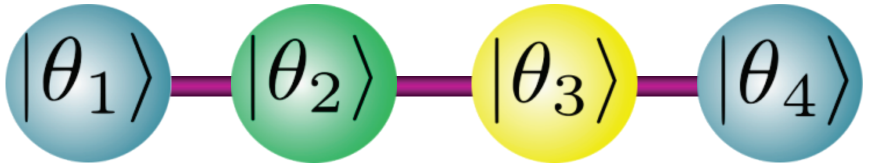


Probability Amplification

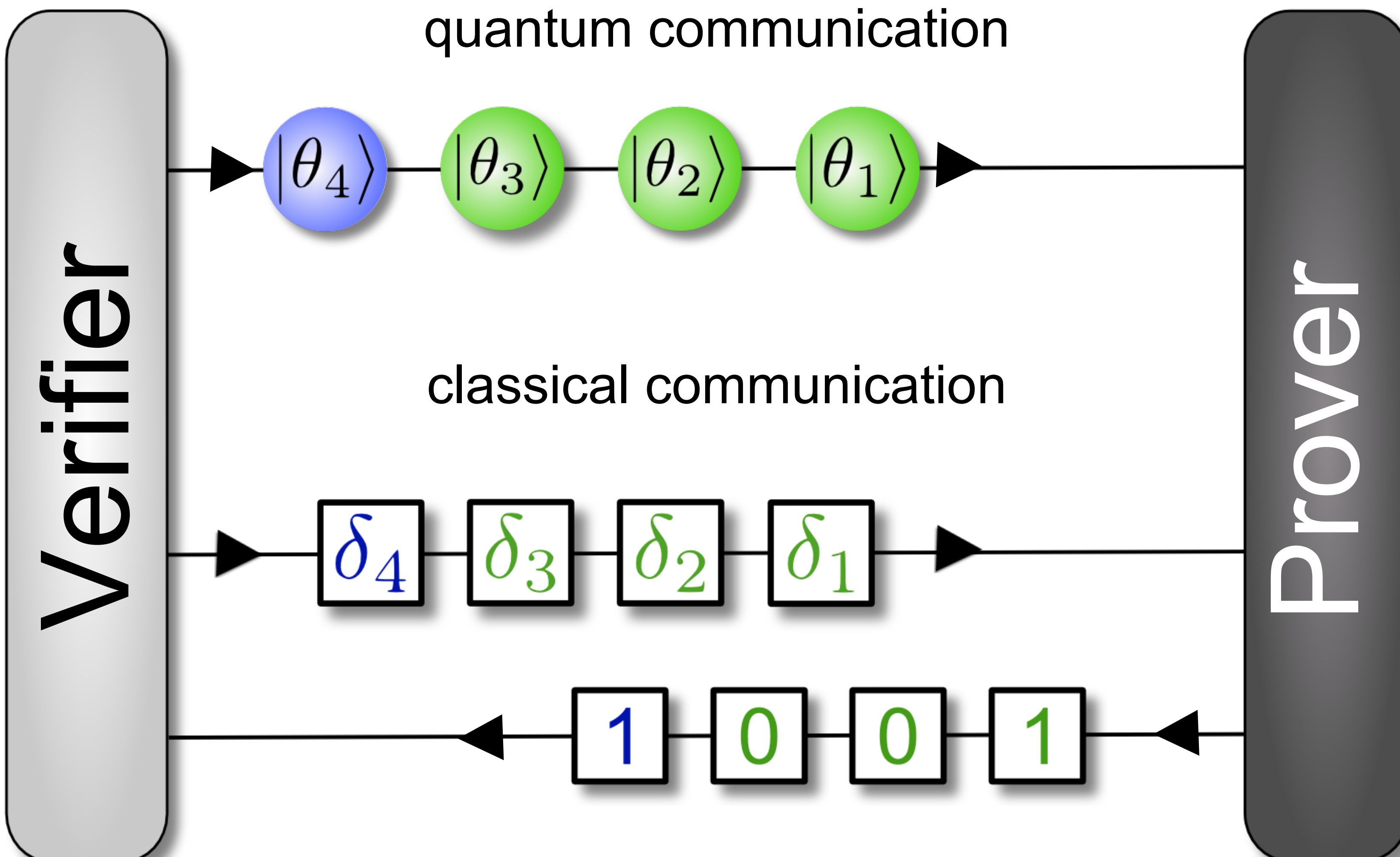


Off to Vienna

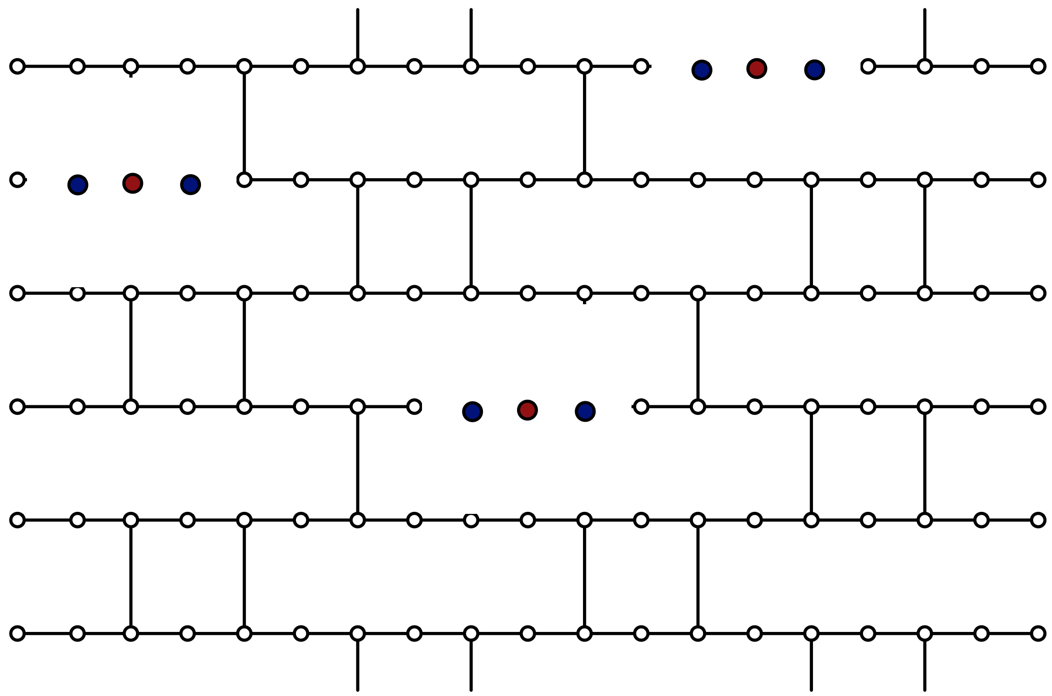


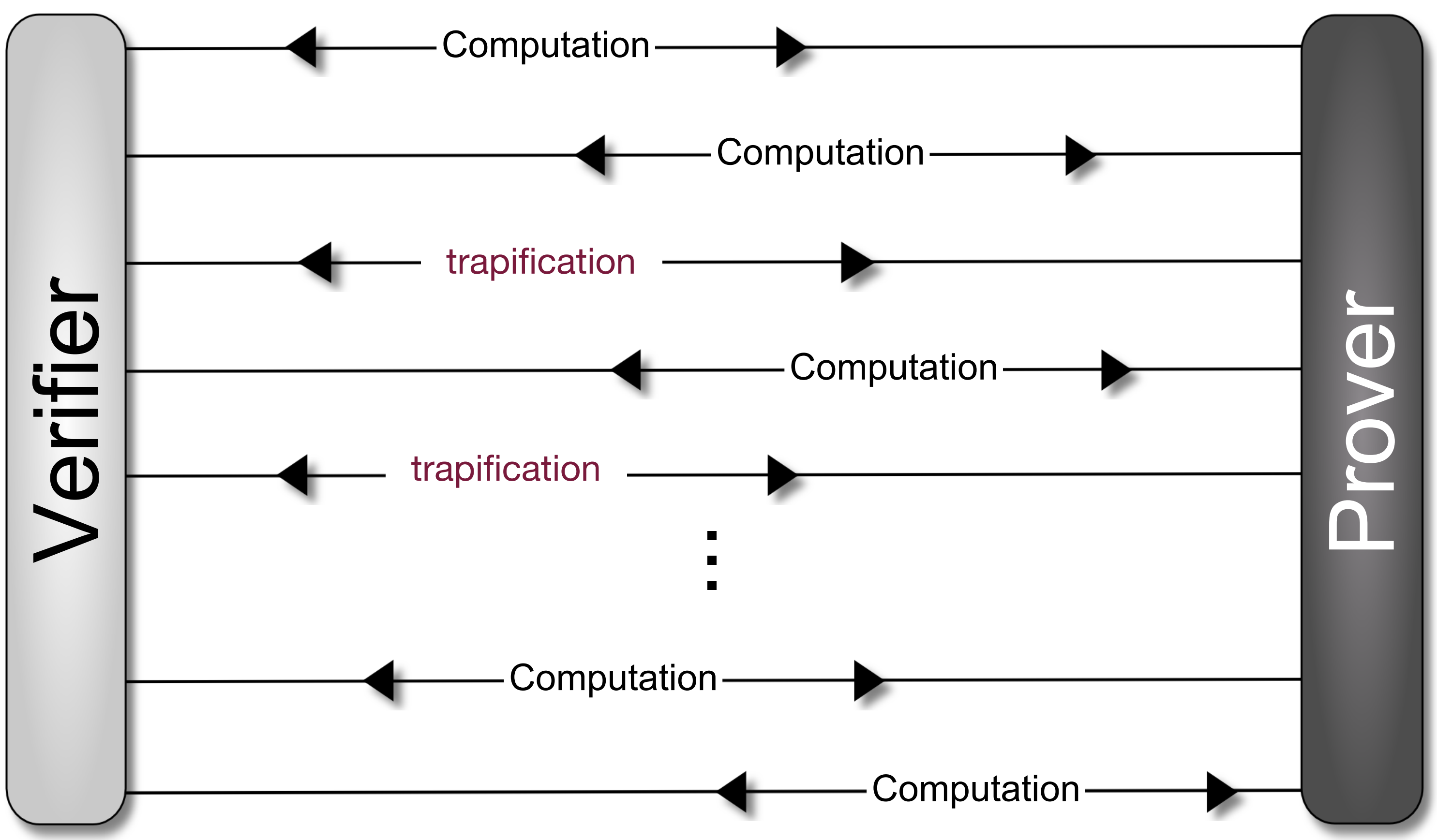


What can we do with 4-qubits



Restricting to Classical Input and Output





A Complete new proof of verification was required

Pauli (σ_i)	Trap Stabilizer Measurement			Overall
	$X \otimes \mathbb{I} \otimes Y \otimes Y$	$Y \otimes X \otimes X \otimes Y$	$Y \otimes Y \otimes \mathbb{I} \otimes X$	
$C \otimes C \otimes C \otimes C$	✓	✓	✓	✓
$C \otimes C \otimes C \otimes A$	✗	✗	✗	✗
$C \otimes C \otimes A \otimes C$	✗	✗	✓	✗
$C \otimes C \otimes A \otimes A$	✓	✓	✗	✗
$C \otimes A \otimes C \otimes C$	✓	✗	✗	✗
$C \otimes A \otimes C \otimes A$	✗	✓	✓	✗
$C \otimes A \otimes A \otimes C$	✗	✓	✗	✗
$C \otimes A \otimes A \otimes A$	✓	✗	✓	✗
$A \otimes C \otimes C \otimes C$	✗	✗	✗	✗
$A \otimes C \otimes C \otimes A$	✓	✓	✓	✓
$A \otimes C \otimes A \otimes C$	✓	✓	✗	✗
$A \otimes C \otimes A \otimes A$	✗	✗	✓	✗
$A \otimes A \otimes C \otimes C$	✗	✓	✓	✗
$A \otimes A \otimes C \otimes A$	✓	✗	✗	✗
$A \otimes A \otimes A \otimes C$	✓	✗	✓	✗
$A \otimes A \otimes A \otimes A$	✗	✓	✗	✗

Summery

Only 4 qubit computation can be verified
and
a particular type of attack cannot be detected !

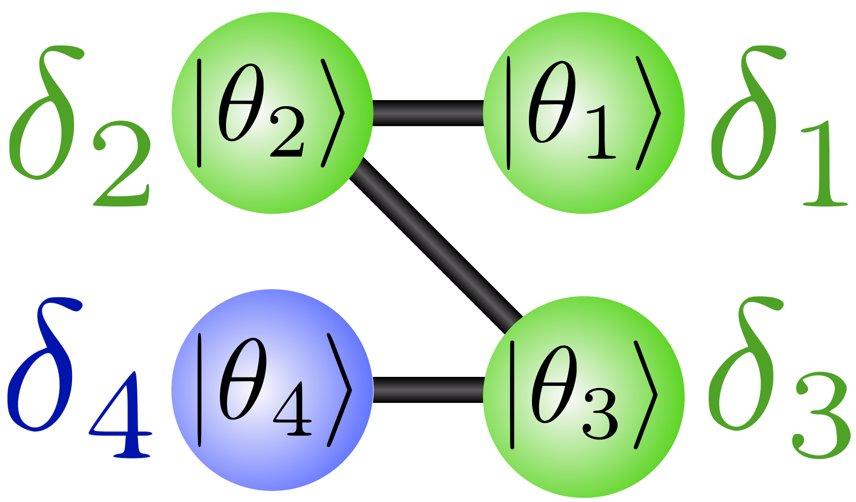
What about D-Wave Problem

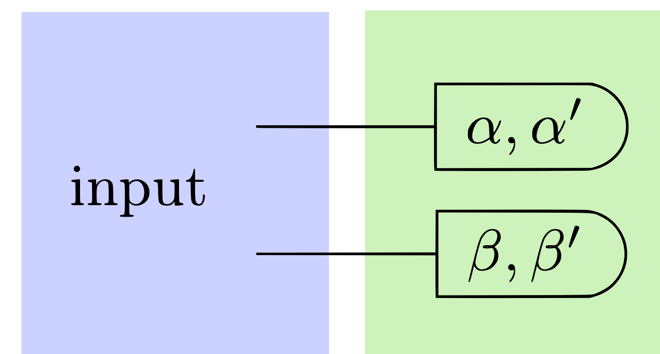
Verification of 2-qubit entanglement

Blind Verification of Entanglement

Blind Verification of Entanglement

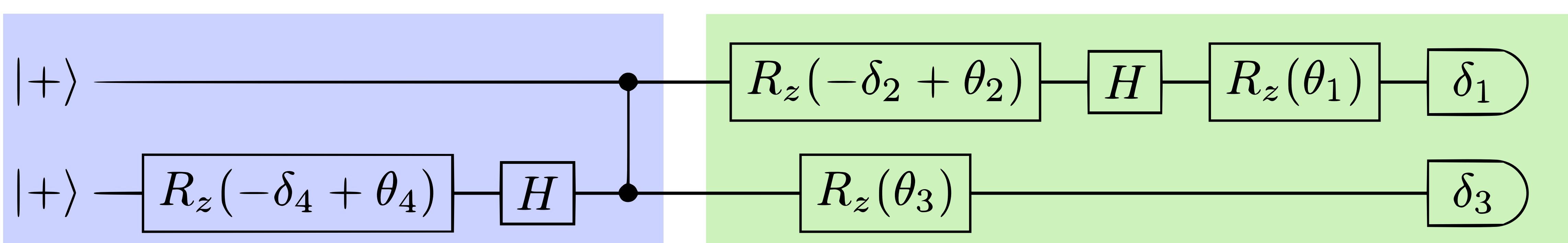
Barz, Fitzsimons, Kashefi, Walther, Nature Physics 2013





State generation

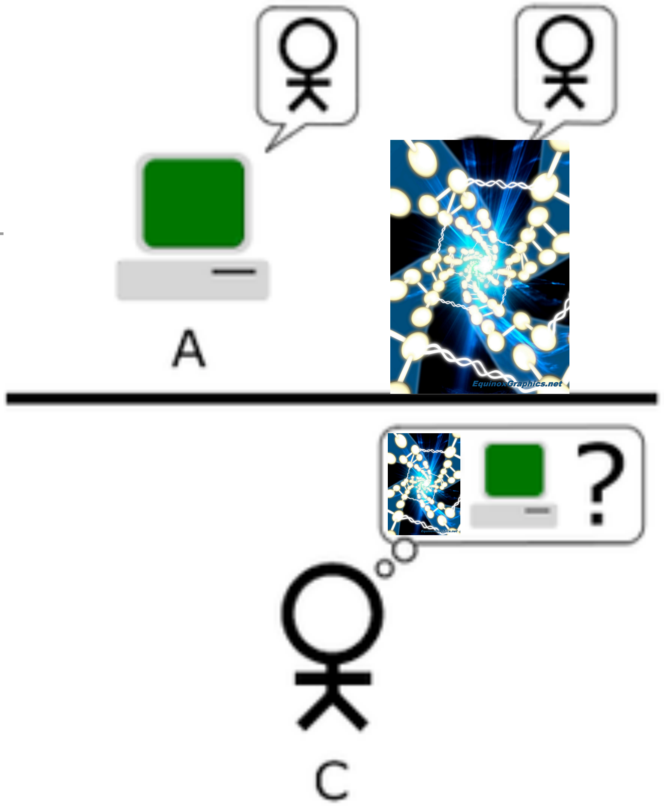
Bell measurement



Blind state generation

Blind Bell test

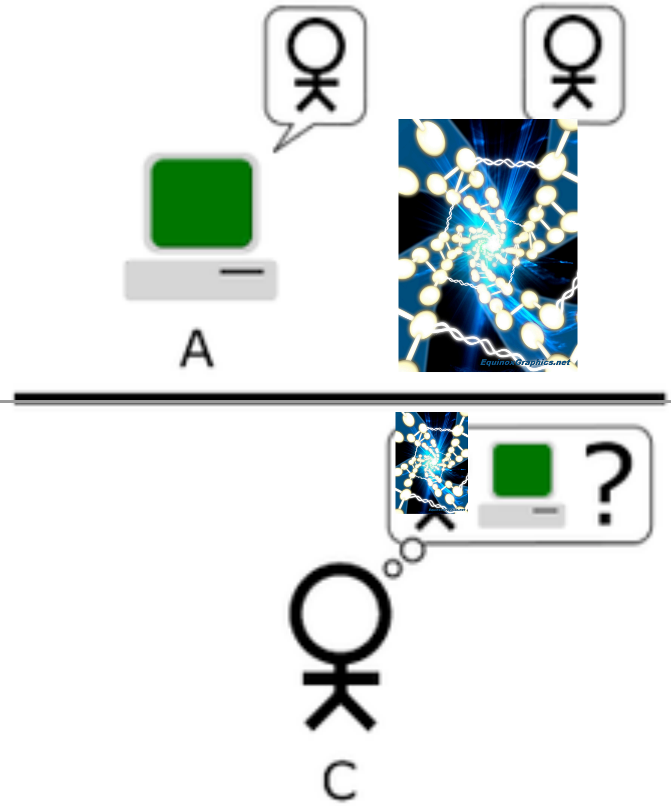
Quantum Turing Test



We can test efficiently a quantum computer

But we need quantum randomness

Perspective



What is the lower bound

Model independent Verification

Is Nature Classically verifiable

Quantum Turing Test