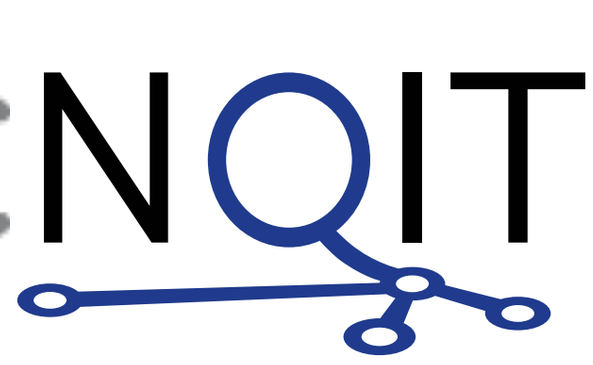
Verification of Quantum Computing

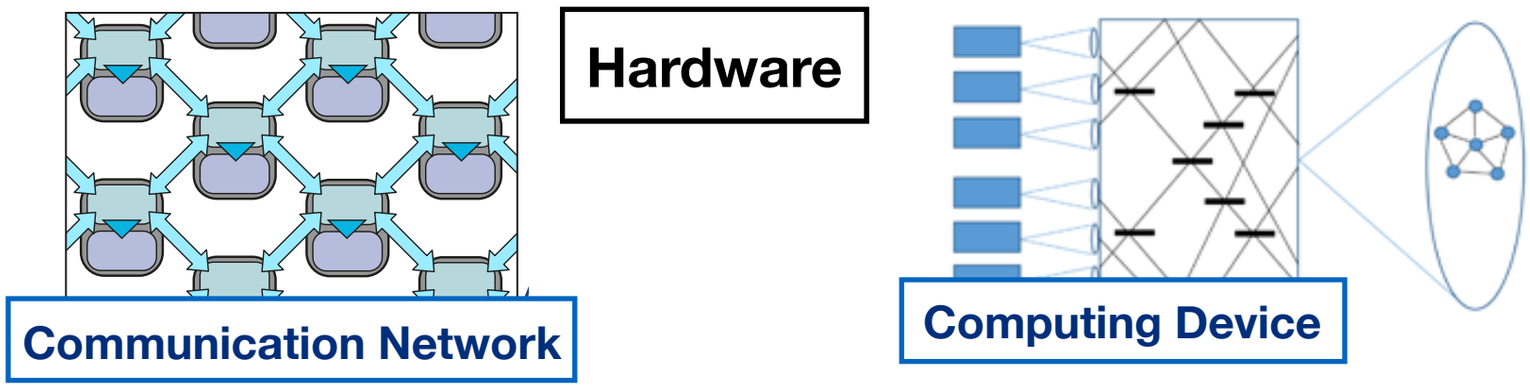
Elham Kashefi

CNRS, LIP6, Sorbonne Universite
Paris Center for Quantum Computing

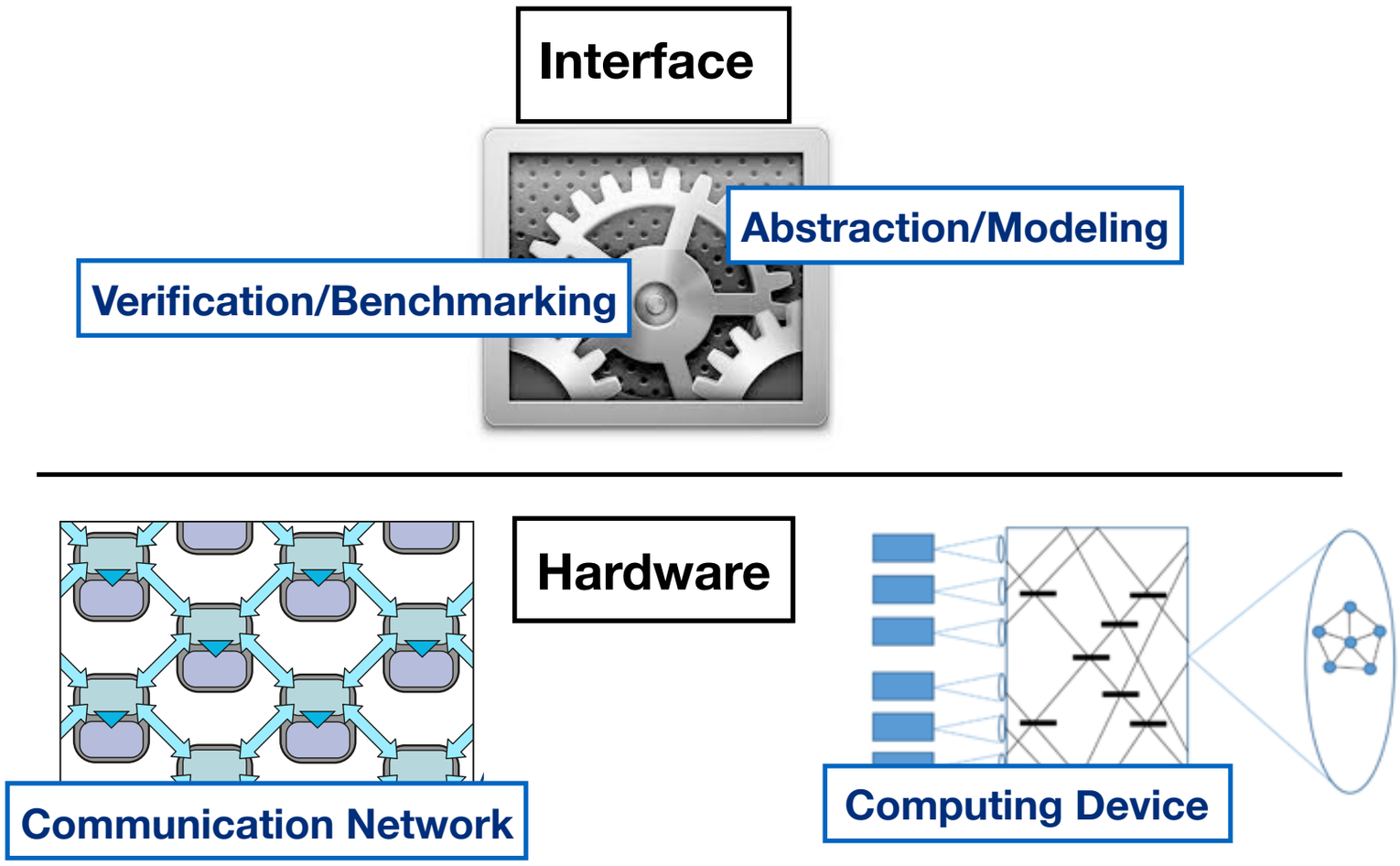
University of Edinburgh
NQIT UK Quantum Technology Hub



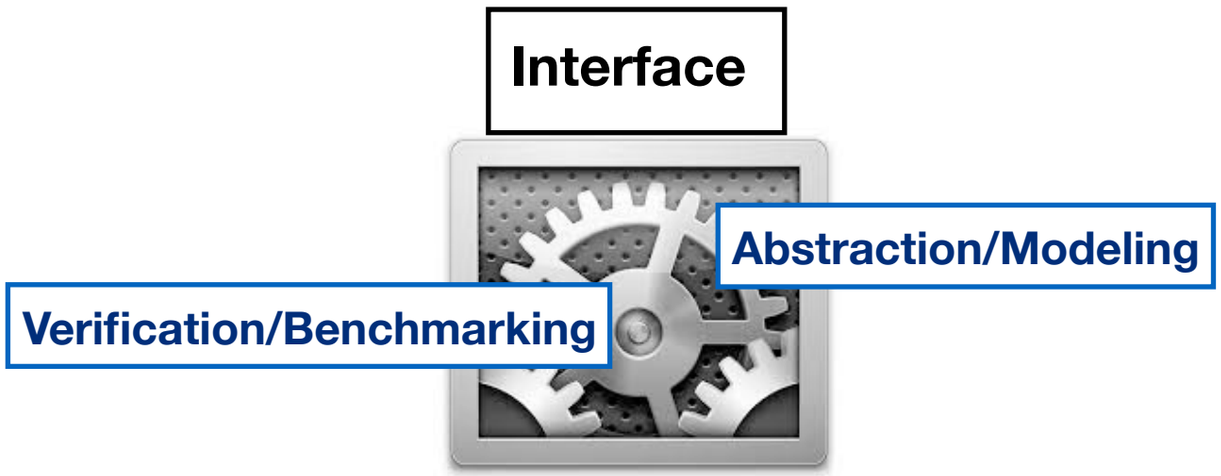
Our Vision of Quantum Technology

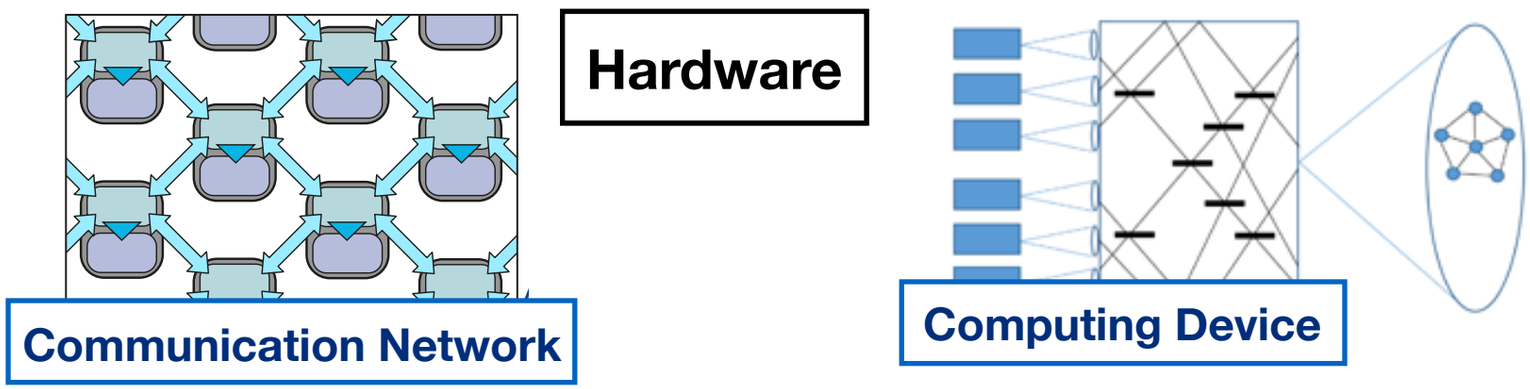


Our Vision of Quantum Technology

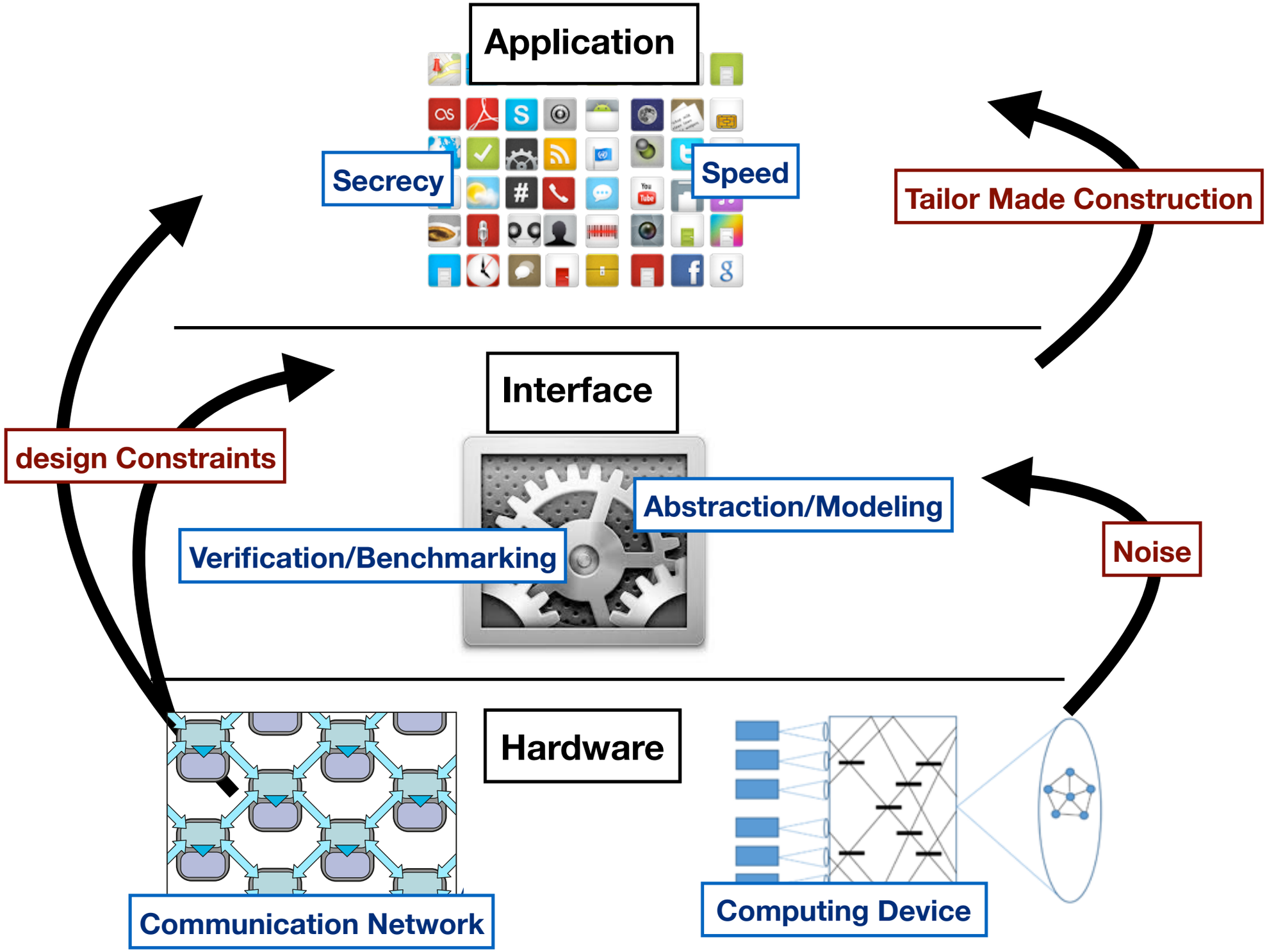


Our Vision of Quantum Technology

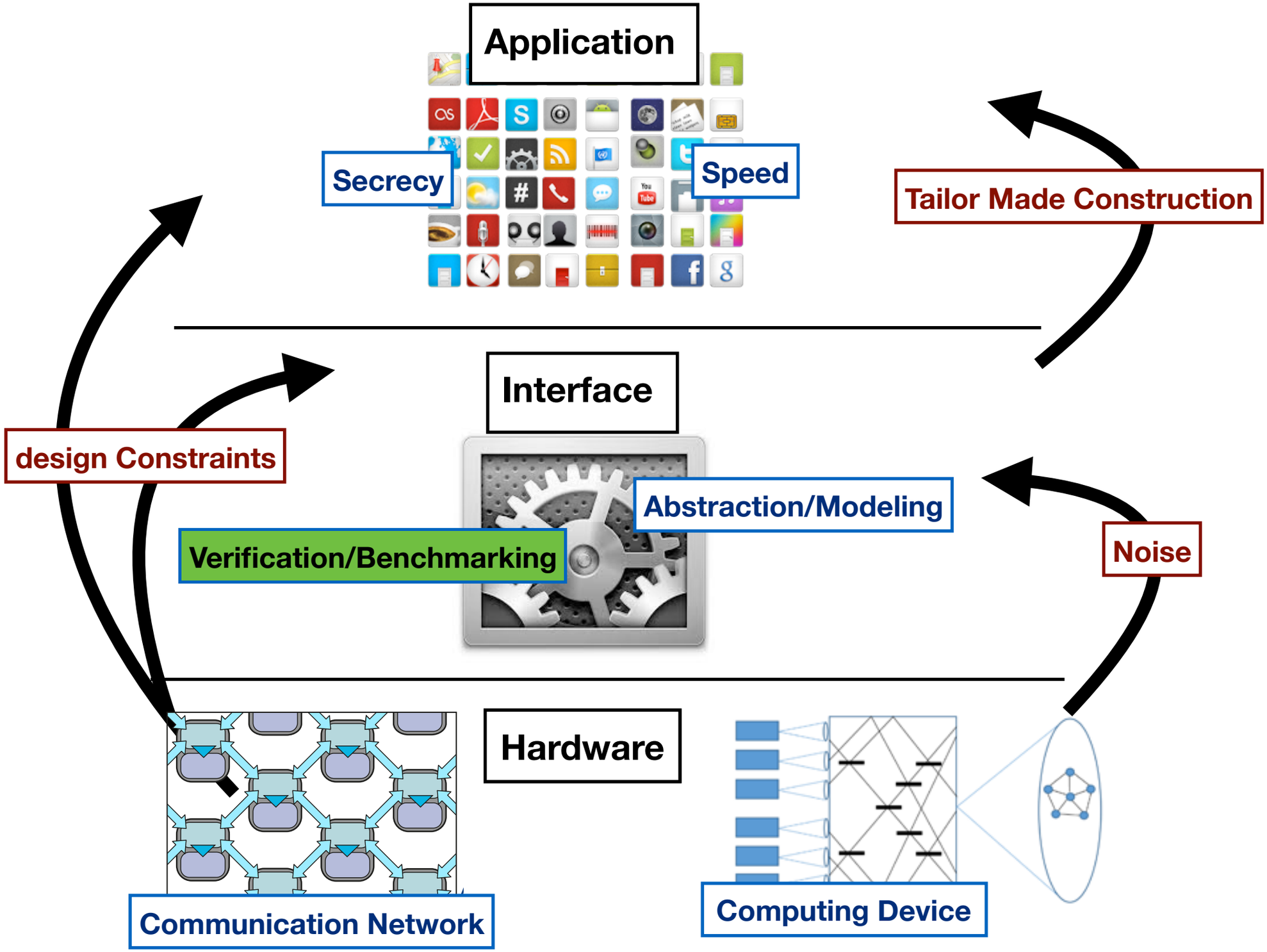




Our Vision of Quantum Technology



Our Vision of Quantum Technology



Quantum Era

National Investments

Europe 1bn€
UK 270M £
Netherlands 80M $
US, Singapore,Canada

Quantum Machines

Private Investments

Google, IBM, Intel
Big VC founds
Startups Companies: D-Wave

Quantum Era

National Investments

Europe 1bn€
UK 270M £
Netherlands 80M $
US, Singapore,Canada

Quantum Machines

Private Investments

Google, IBM, Intel
Big VC founds
Startups Companies: D-Wave

Target: > 100 qubits Device

Quantum Era

National Investments

Europe 1bn€
UK 270M £
Netherlands 80M $
US, Singapore,Canada

Quantum Machines

Private Investments

Google, IBM, Intel
Big VC founds
Startups Companies: D-Wave

Target: > 100 qubits Device

Feature: Not Simulatable Classically

Quantum Era

National Investments

Europe 1bn€
UK 270M £
Netherlands 80M $
US, Singapore,Canada

Quantum Machines

Private Investments

Google, IBM, Intel
Big VC founds
Startups Companies: D-Wave

Target: > 100 qubits Device

Feature: Not Simulatable Classically

Problem: Testing, Validation, BenchMarking, Certification, Verification …

Quantum Era

National Investments

Europe 1bn€
UK 270M £
Netherlands 80M $
US, Singapore,Canada

Quantum Machines

Private Investments

Google, IBM, Intel
Big VC founds
Startups Companies: D-Wave

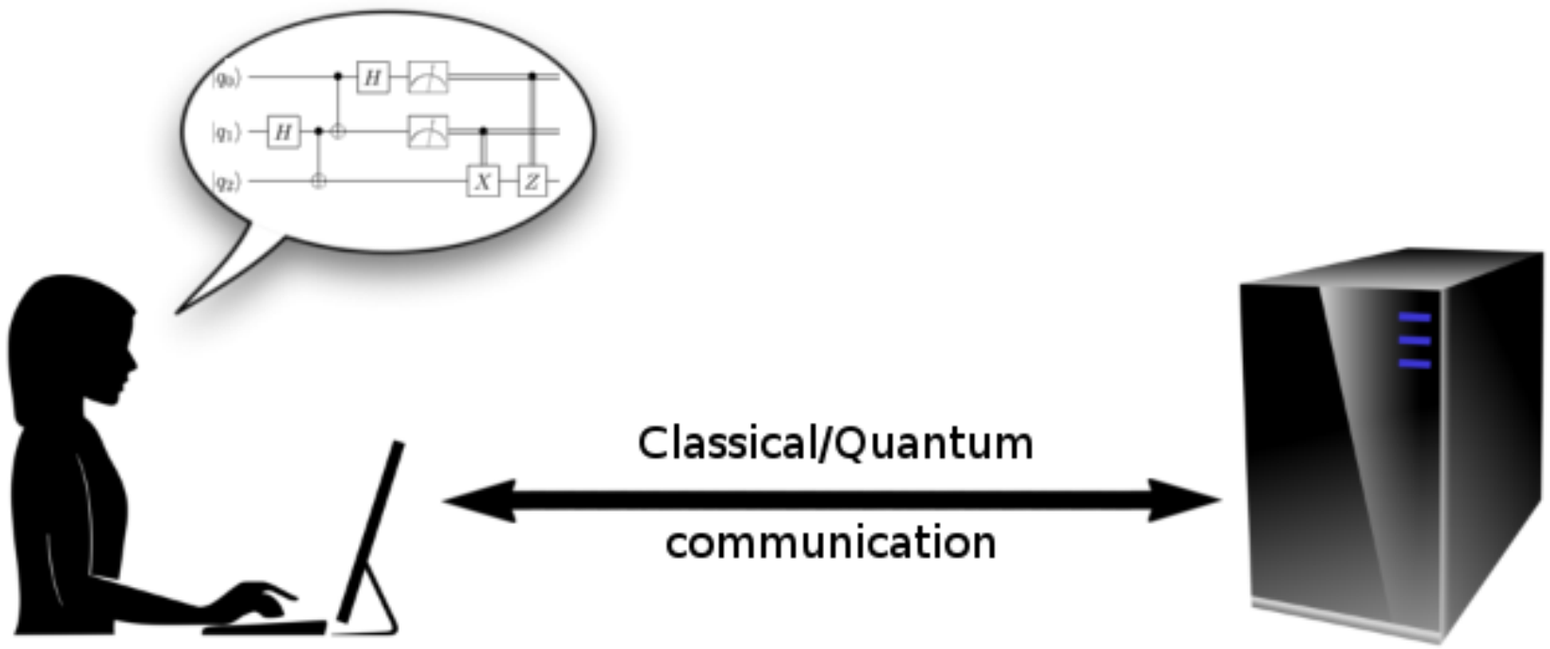
Target: > 100 qubits Device

Feature: Not Simulatable Classically

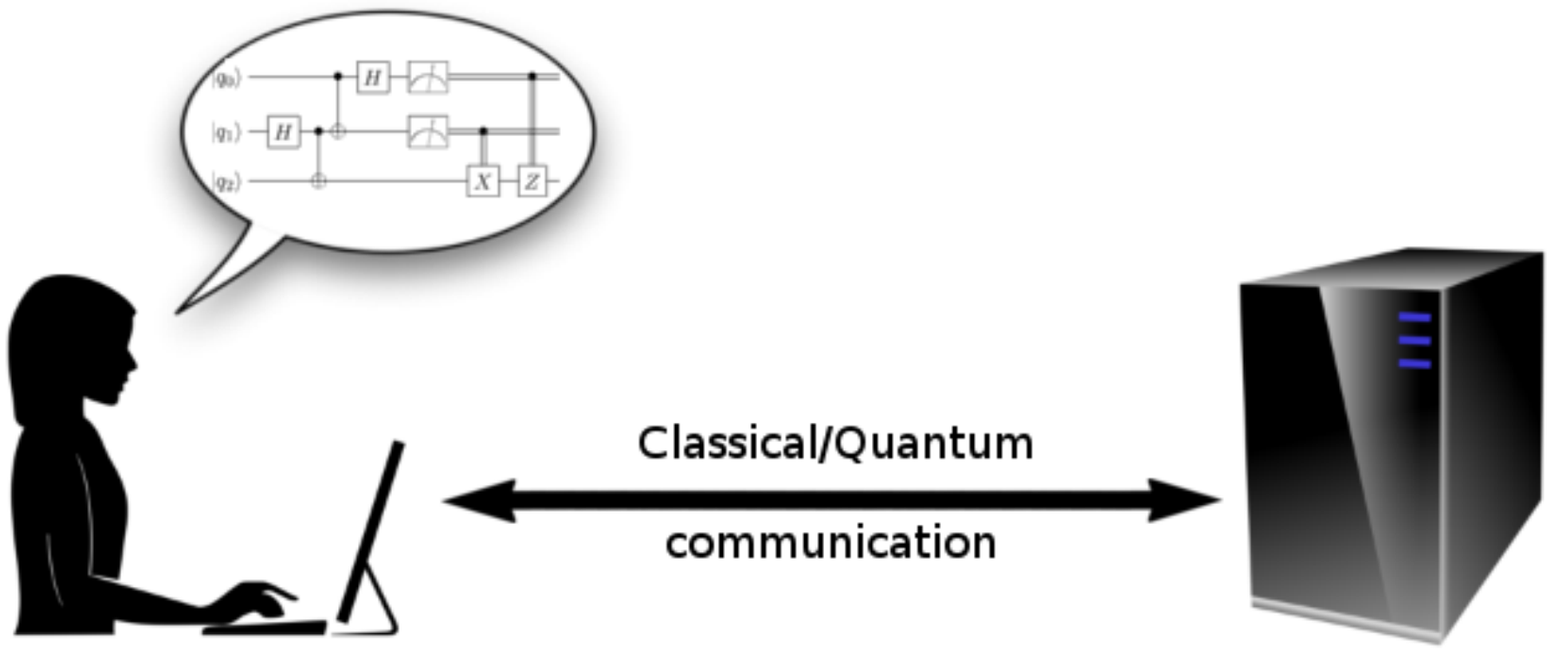
Problem: Testing, Validation, BenchMarking, Certification, Verification …

Do we need another quantum computer to test a quantum computer or
can we bootstrap a mini quantum device to test a bigger one

Quantum Verification

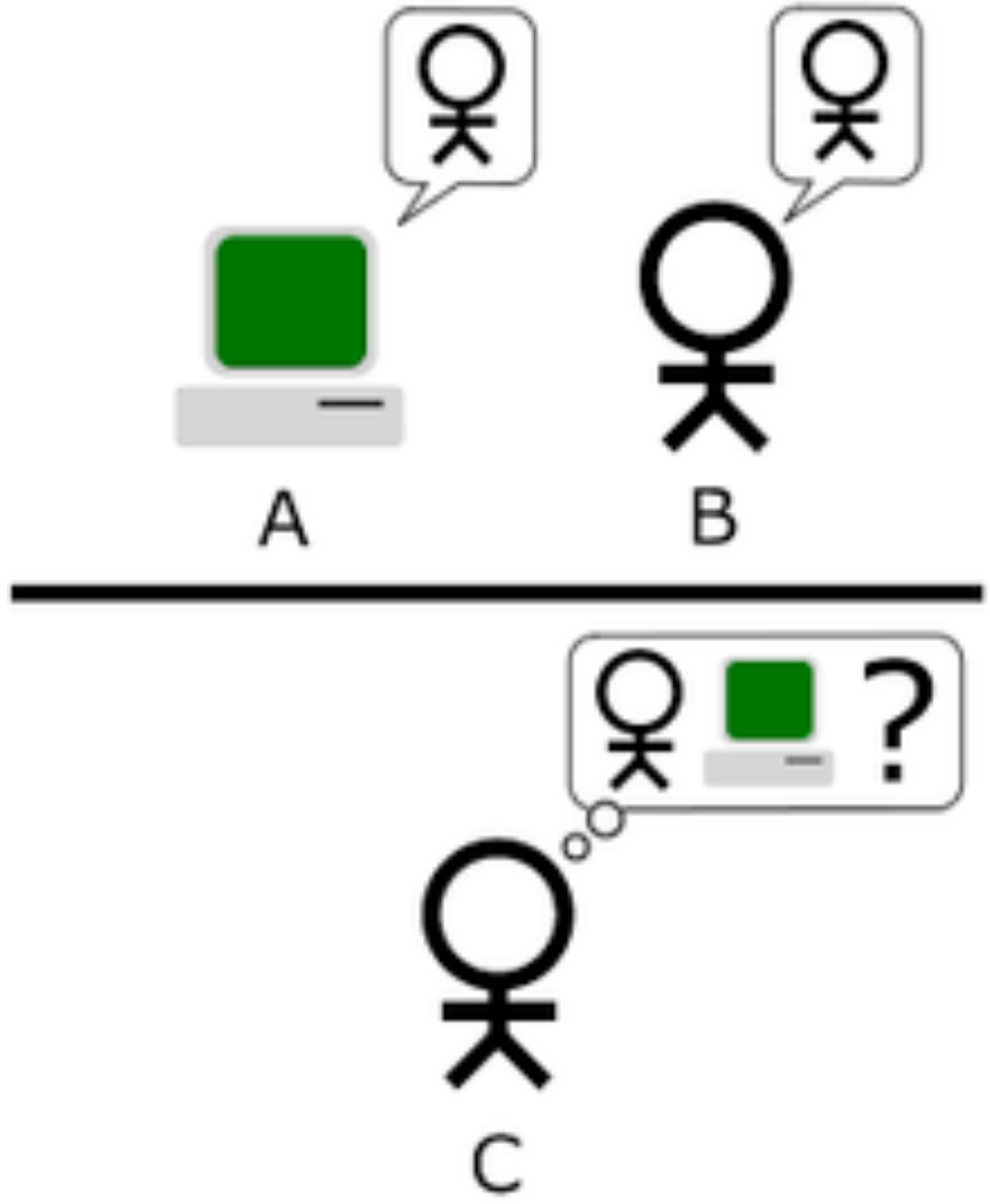


Quantum Verification

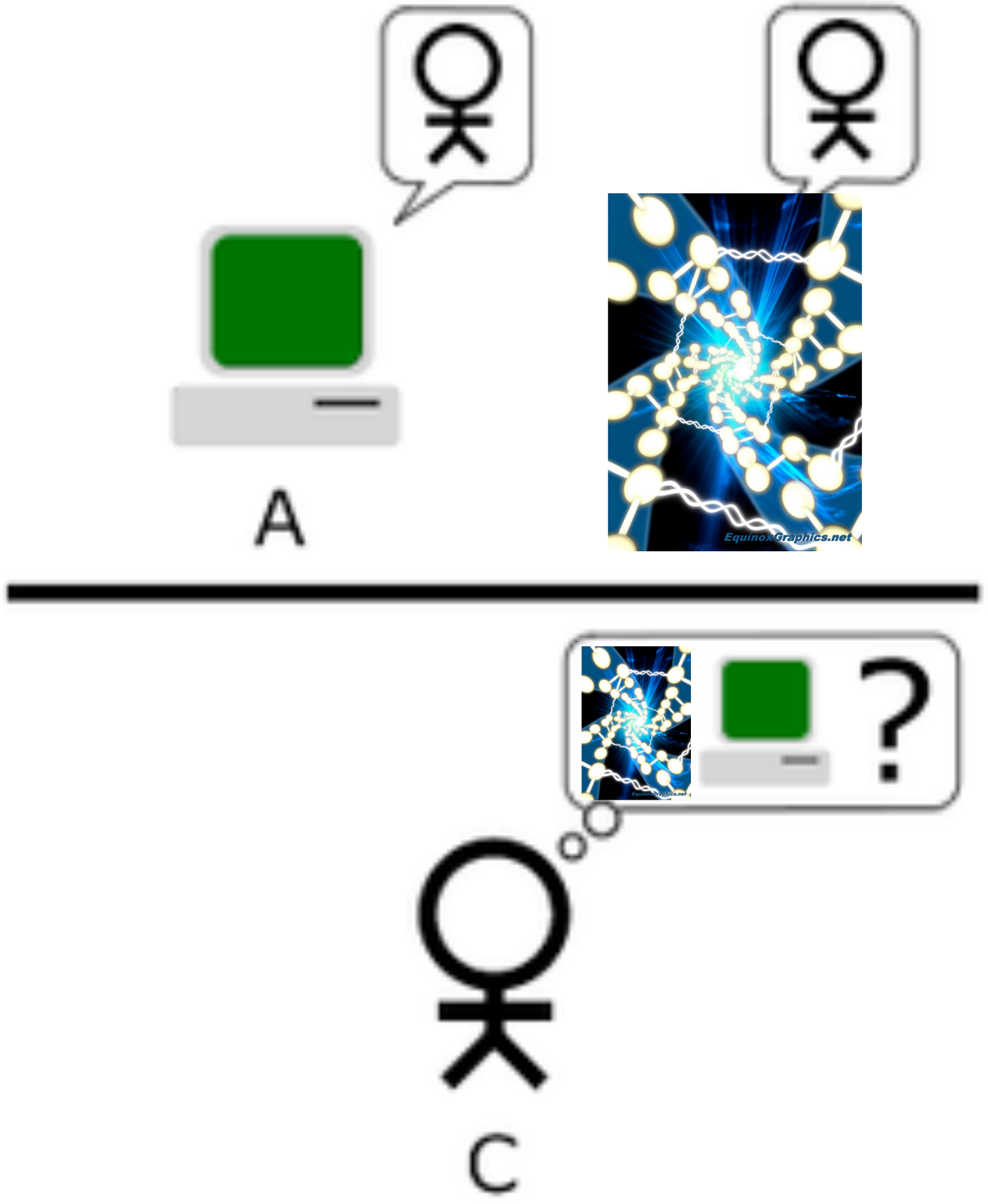


- Computationally limited verifier
- Powerful quantum server(s)
- Certify the correctness of the computation

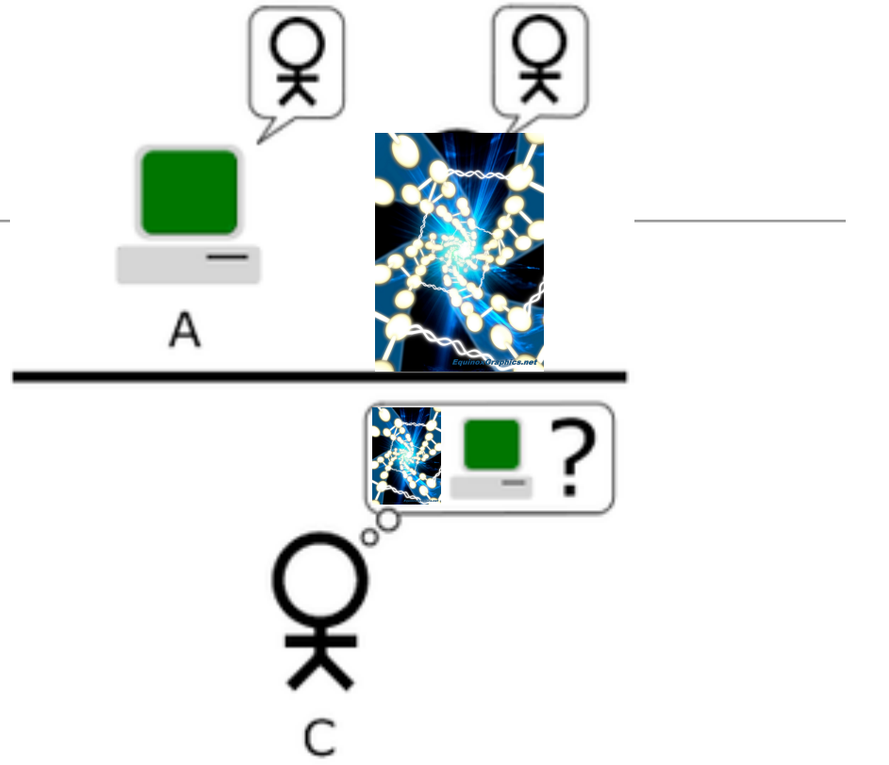
Quantum Turing test



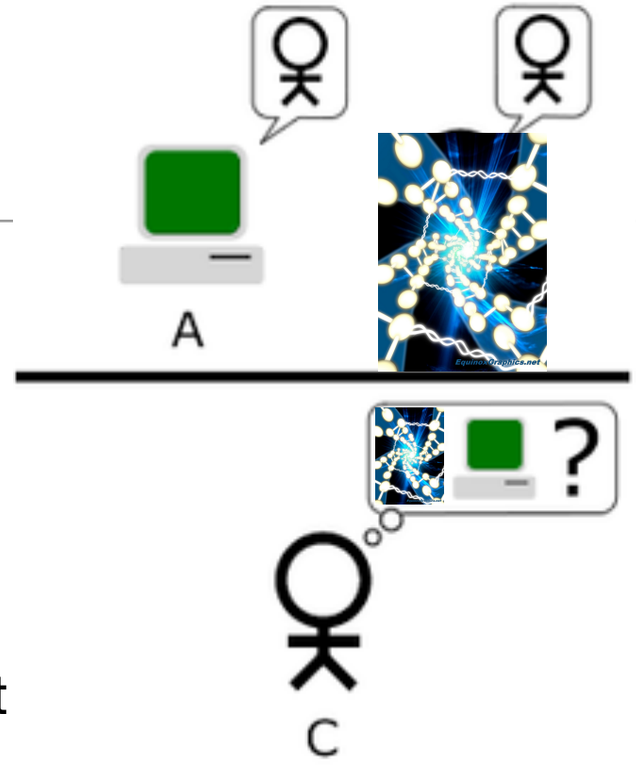
Quantum Turing test



Quantum Turing test



Quantum Turing test



- Can we classically communicate or do we need a bit of “quantumness” to test quantum computer
- Can we do the test efficiently or do we need super powerful computer to test quantum computer

What is Verification

What is Verification

A mechanism that when witness is accepted the outcome is good

What is Verification

A mechanism that when witness is accepted the outcome is good

A mechanism that when witness is accepted the outcome is **not bad**

What is Verification

A mechanism that when witness is accepted the outcome is good

A mechanism that when witness is accepted the outcome is **not bad**

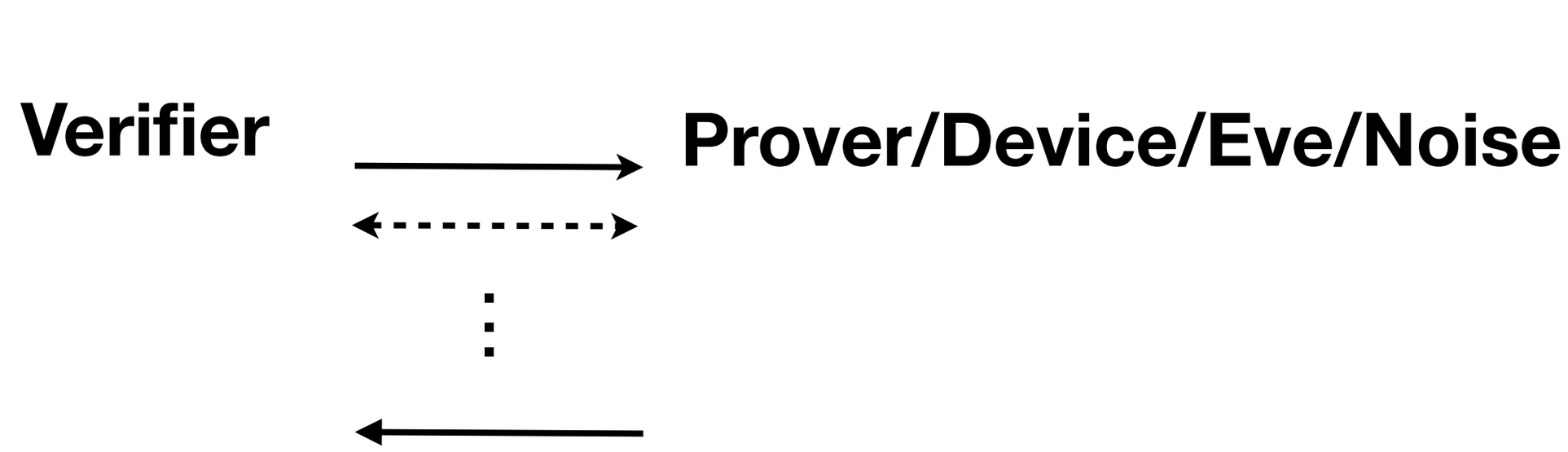
A mechanism that **probability** of witness is accepted and the outcome is **bad is bounded**

What is Verification

A **mechanism** that prob of witness is acc and outcome is bad is bounded

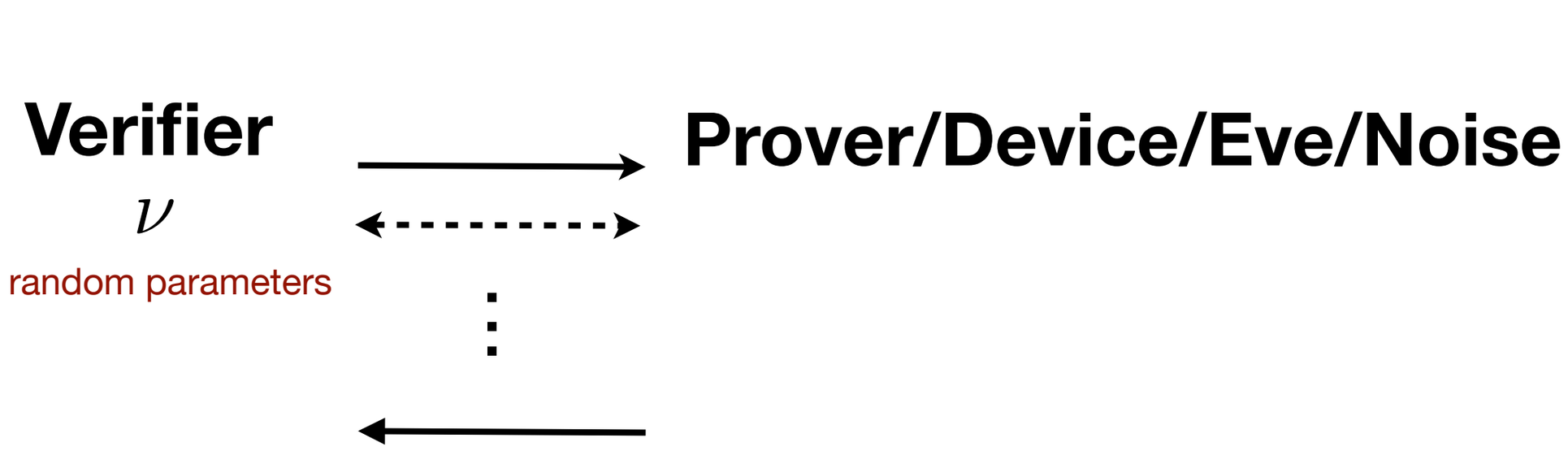
What is Verification

A **mechanism** that prob of witness is acc and outcome is bad is bounded



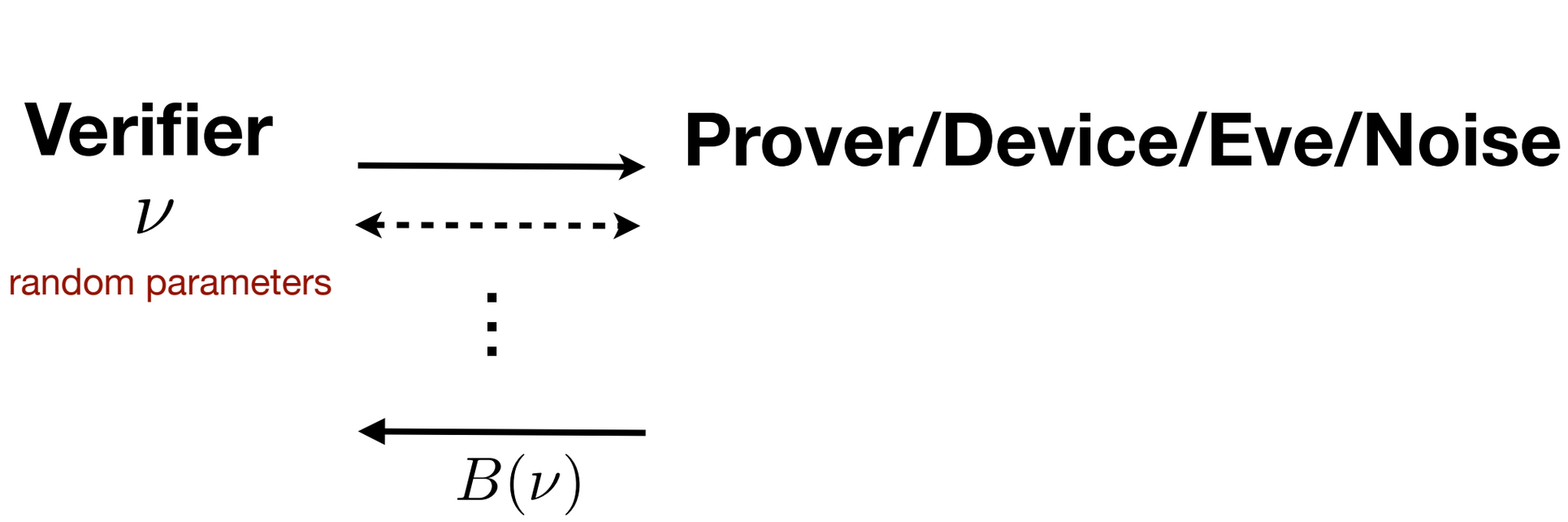
What is Verification

A **mechanism** that prob of witness is acc and outcome is bad is bounded



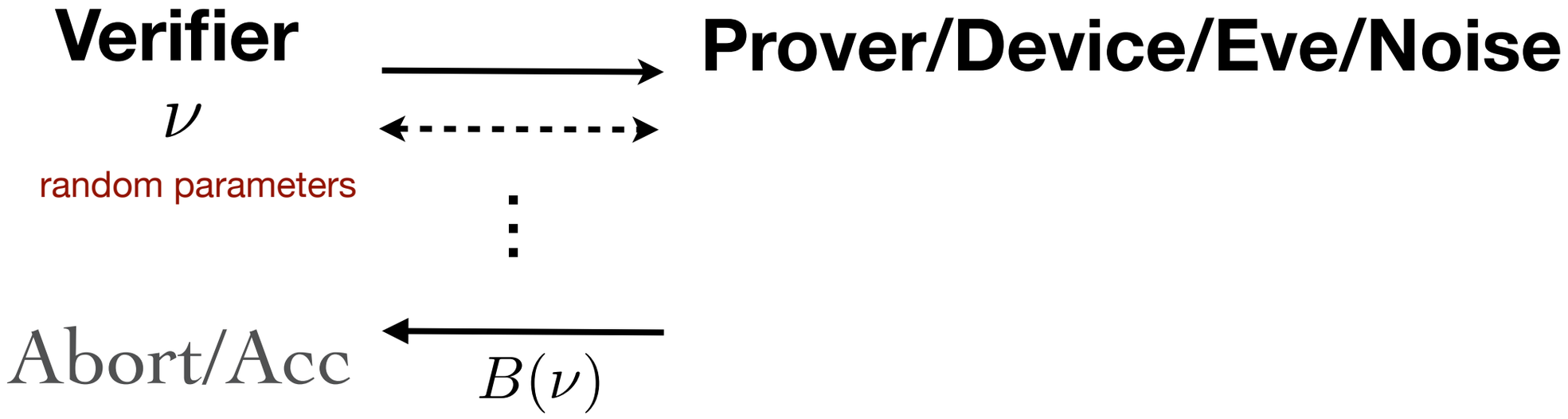
What is Verification

A **mechanism** that prob of witness is acc and outcome is bad is bounded

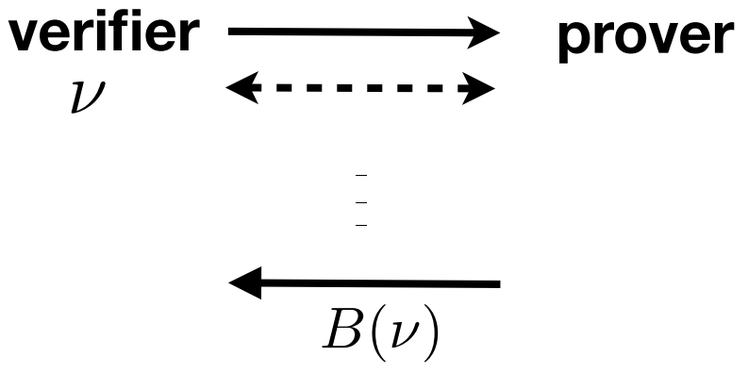


What is Verification

A **mechanism** that prob of witness is acc and outcome is bad is bounded

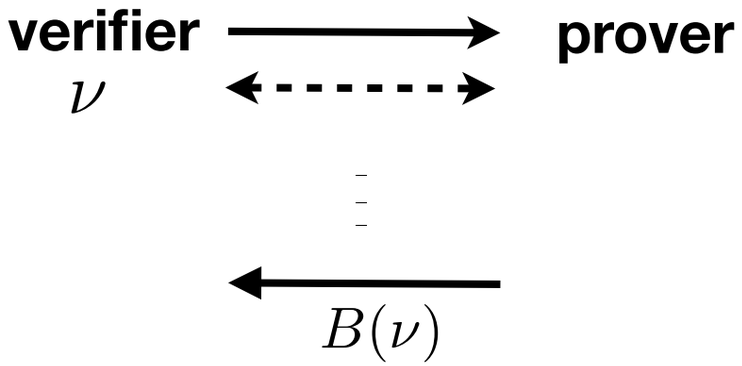


What is Verification



A mechanism that prob of **witness is acc and outcome is bad** is bounded

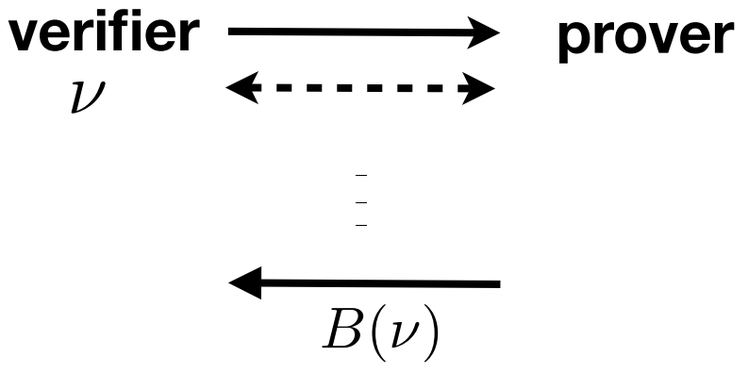
What is Verification



A mechanism that prob of **witness is acc and outcome is bad** is bounded

$$P^{\nu}_{incorrect} := P_{\perp} \otimes |acc\rangle\langle acc|$$

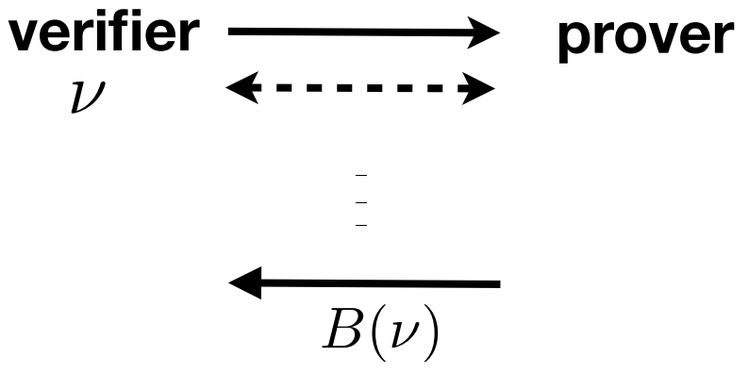
What is Verification



$$P^{\nu}_{incorrect} := P_{\perp} \otimes |acc\rangle\langle acc|$$

A mechanism that **prob** of witness is acc and outcome is bad **is bounded**

What is Verification

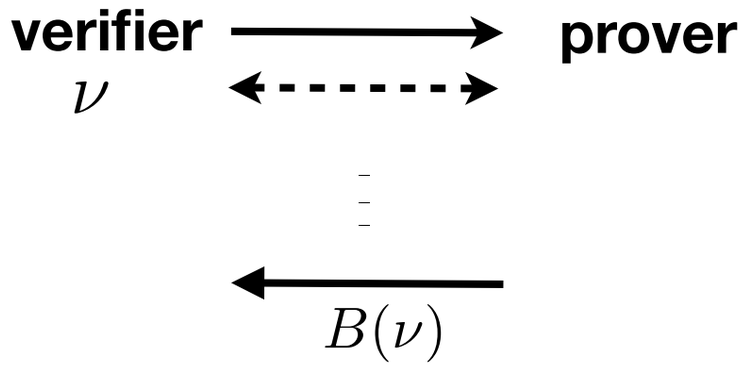


$$P^{\nu}_{incorrect} := P_{\perp} \otimes |acc\rangle\langle acc|$$

A mechanism that **prob** of witness is acc and outcome is bad **is bounded**

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

What is the challenge

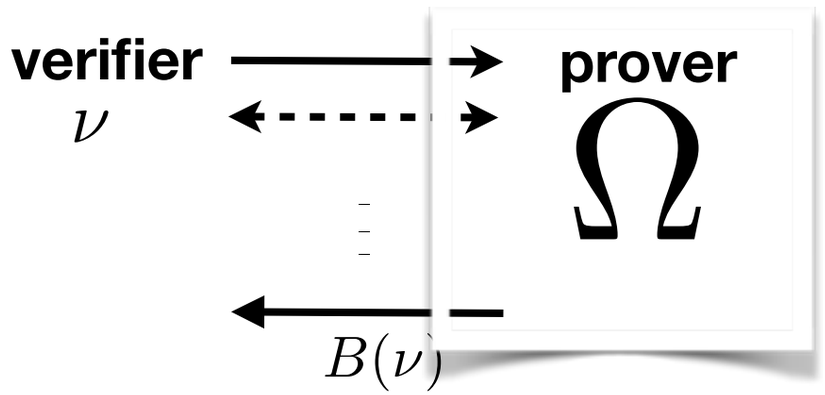


$$P^{\nu}_{incorrect} := P_{\perp} \otimes |acc\rangle\langle acc|$$

A mechanism that **prob** of witness is acc and outcome is bad **is bounded**

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

What is the challenge

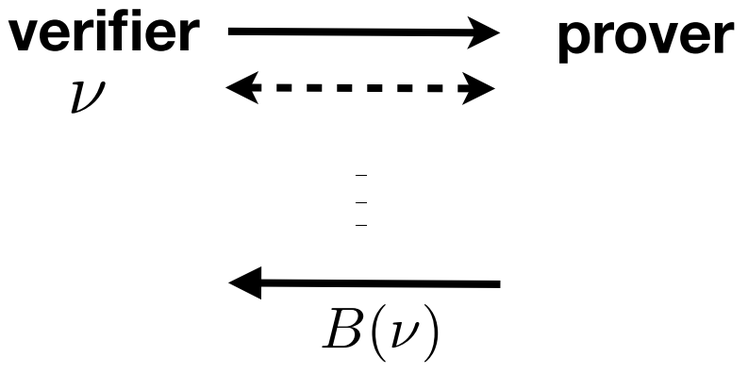


$$P^{\nu}_{incorrect} := P_{\perp} \otimes |acc\rangle\langle acc|$$

A mechanism that **prob** of witness is acc and outcome is bad **is bounded**

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

What is the challenge



$$P^{\nu}_{incorrect} := P_{\perp} \otimes |acc\rangle\langle acc|$$

A mechanism that **prob** of witness is acc and outcome is bad **is bounded**

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

How to deal with deviation

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

How to deal with deviation

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

Ω

Different toolkits / Different tasks / Different witness / Different properties / Different assumptions / …..

How to deal with deviation

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

Ω

Different toolkits / Different tasks / Different witness / Different properties / Different assumptions / …..

Hypothesis Test, Certification, Self Testing, Entanglement detection, Quantum signature, Proof System, Hardware Testing, Post-hoc verification, Randomised benchmarking, Authentication, Blind Verification

Today Lecture : Most General Deviation

$$\Omega_{Eve,system}$$

cryptographic toolkit

Today Lecture : Most General Deviation

$$\Omega_{Eve,system}$$

cryptographic toolkit

$$\sigma_{testsubspace}$$

Today Lecture : Most General Deviation

$$\Omega_{Eve,system}$$

cryptographic toolkit

$$\sigma_{testsubspace}$$

Practical Protocols with No assumptions whatsoever

Today Lecture : Most General Deviation

$$\Omega_{Eve,system}$$

arXiv:1709.06984

Verification of quantum computation:
An overview of existing approaches

Alexandru Gheorghiu, Theodoros Kapourniotis, Elham Kashefi

$$\sigma_{testsubspace}$$

Practical Protocols with No assumptions whatsoever

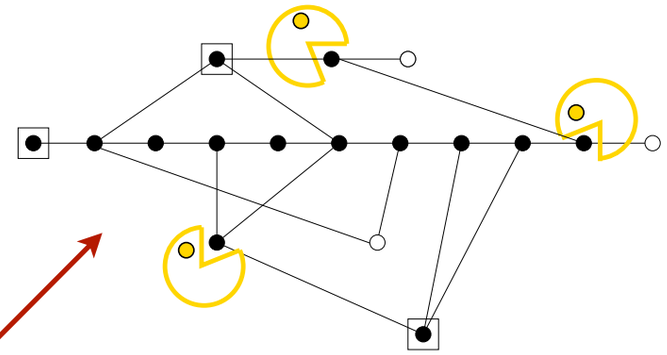
Roadmap for Quantum Verification

➡ **Classically controlled QC**

➡ Cryptographic Toolkit

➡ Interactive Proof System

Roadmap for Quantum Verification



➡ **Classically controlled QC**

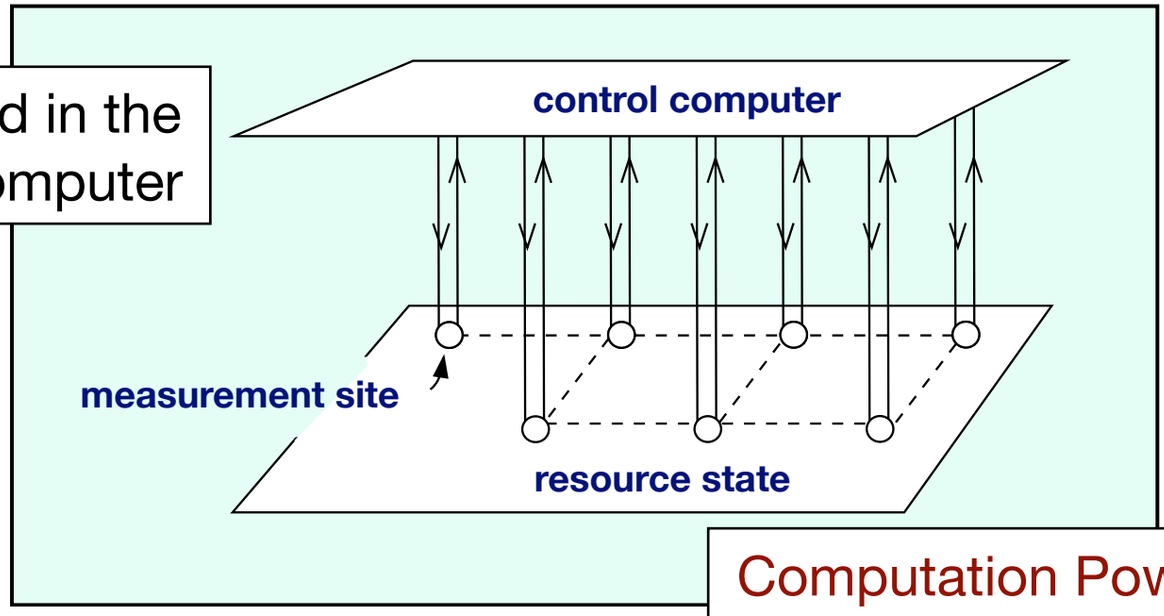
➡ Cryptographic Toolkit

➡ Interactive Proof System

Classically-controlled QC

MBQC - Cluster State - Gate Teleportation

Program is encoded in the classical control computer

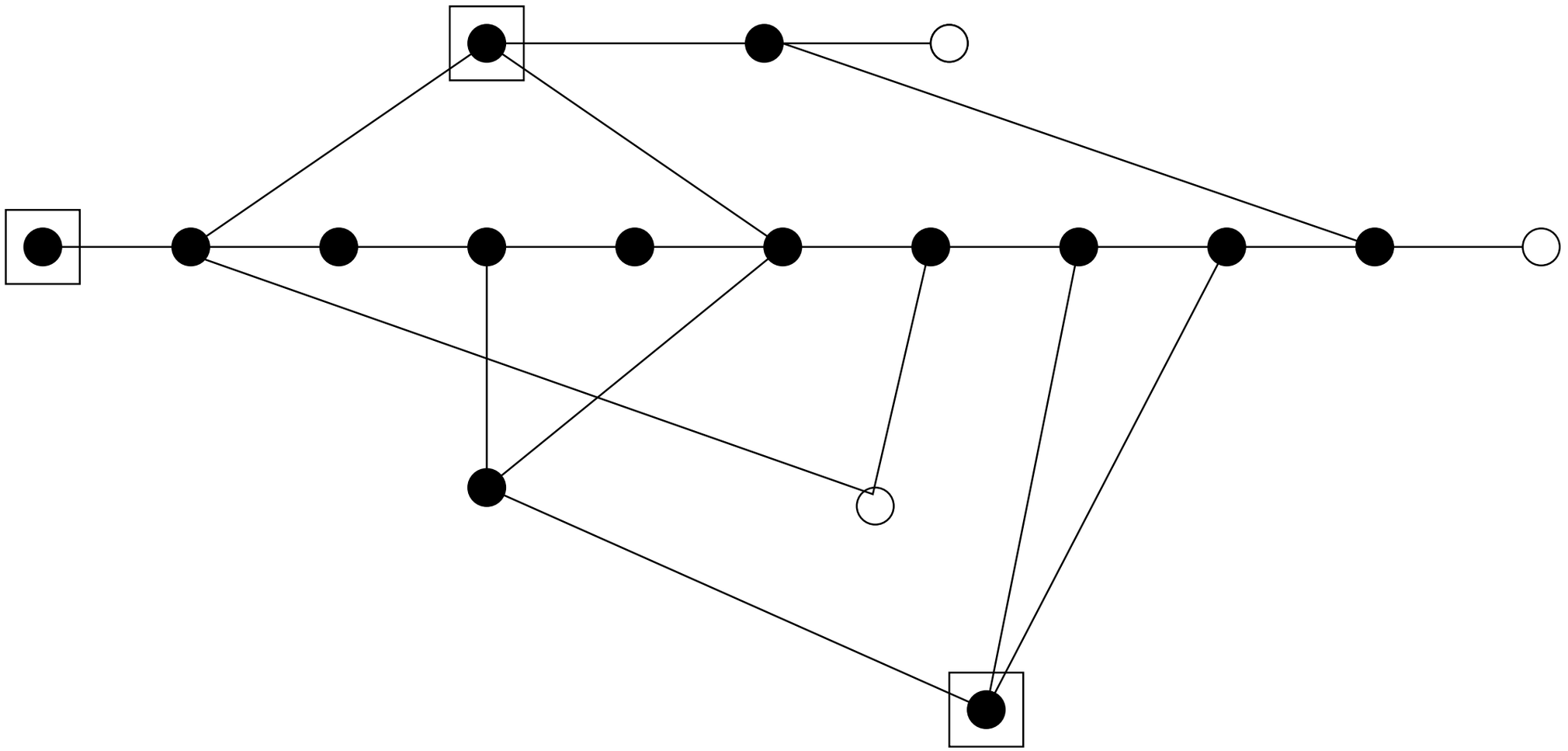


Computation Power is encoded in the quantum entanglement

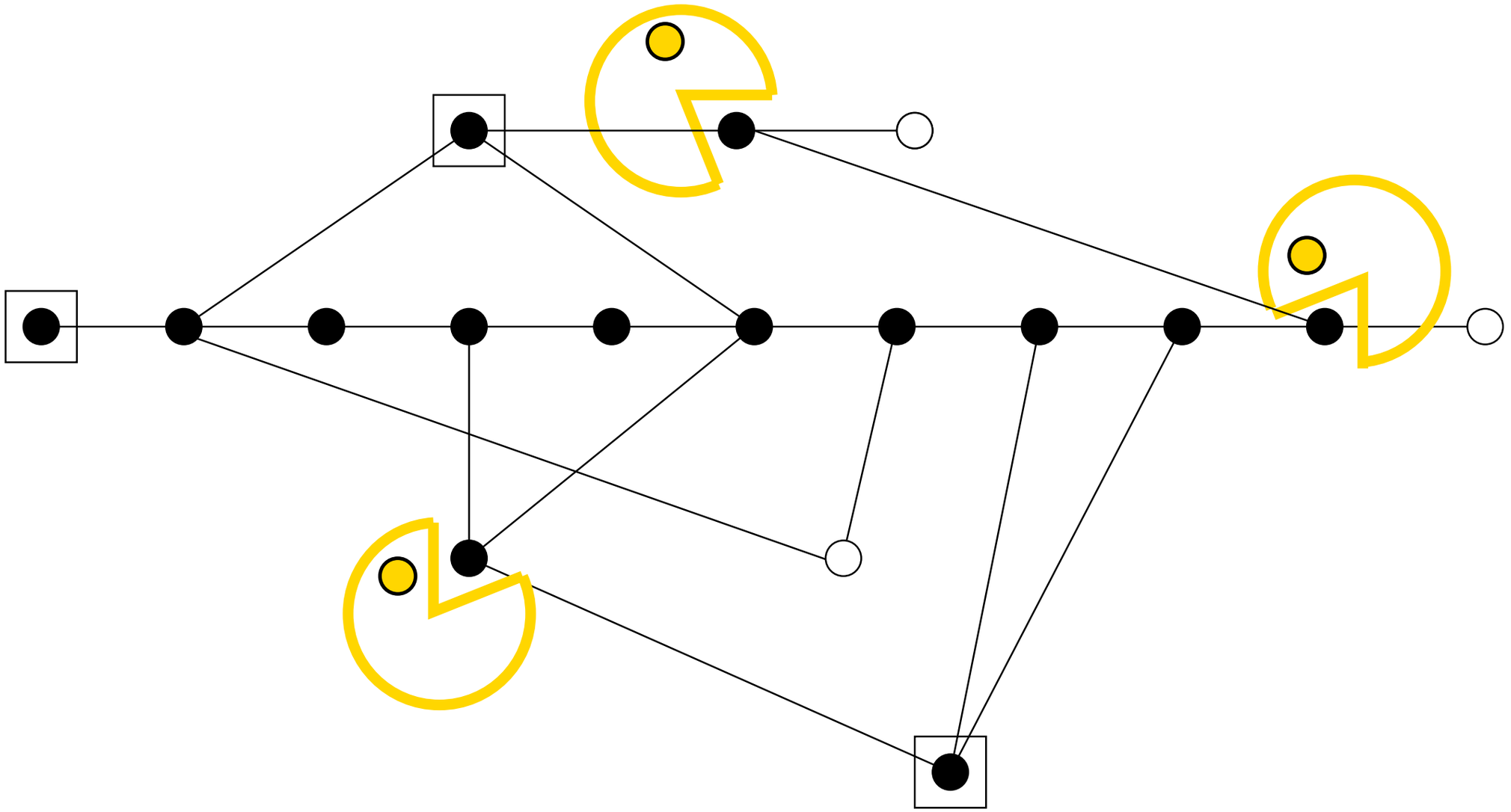
Abstract Model : Measurement-based QC

- New qubits, to prepare the auxiliary qubits: N
- Entanglements, to build the quantum channel: E
- Measurements, to propagate (manipulate) qubits: M
- Corrections, to make the computation deterministic: C

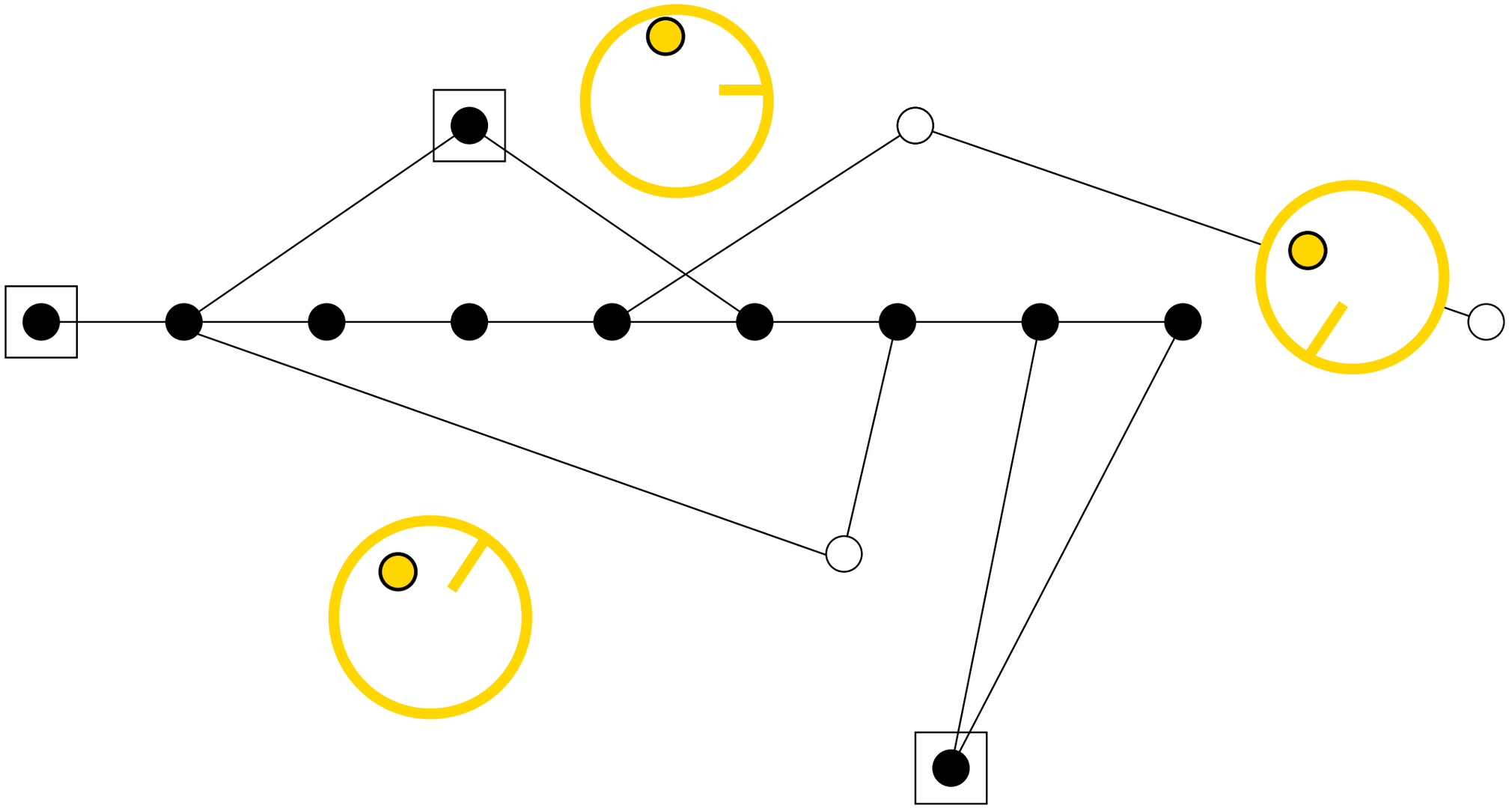
Quantum Pacman



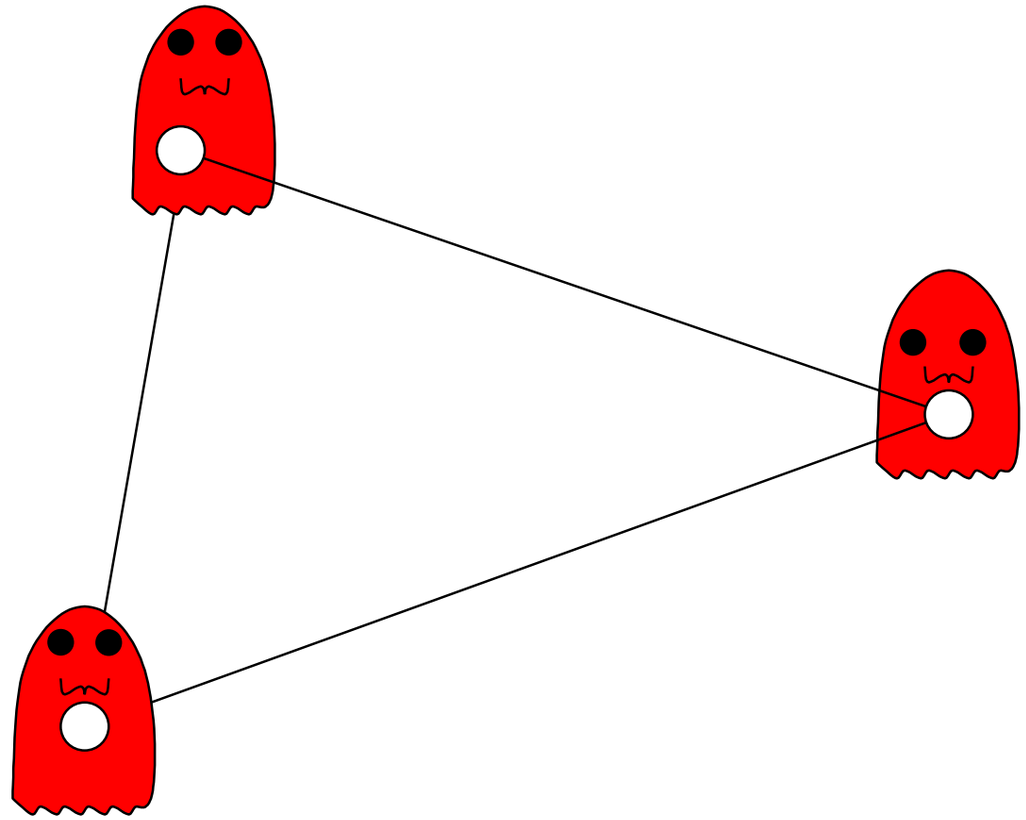
Quantum Pacman



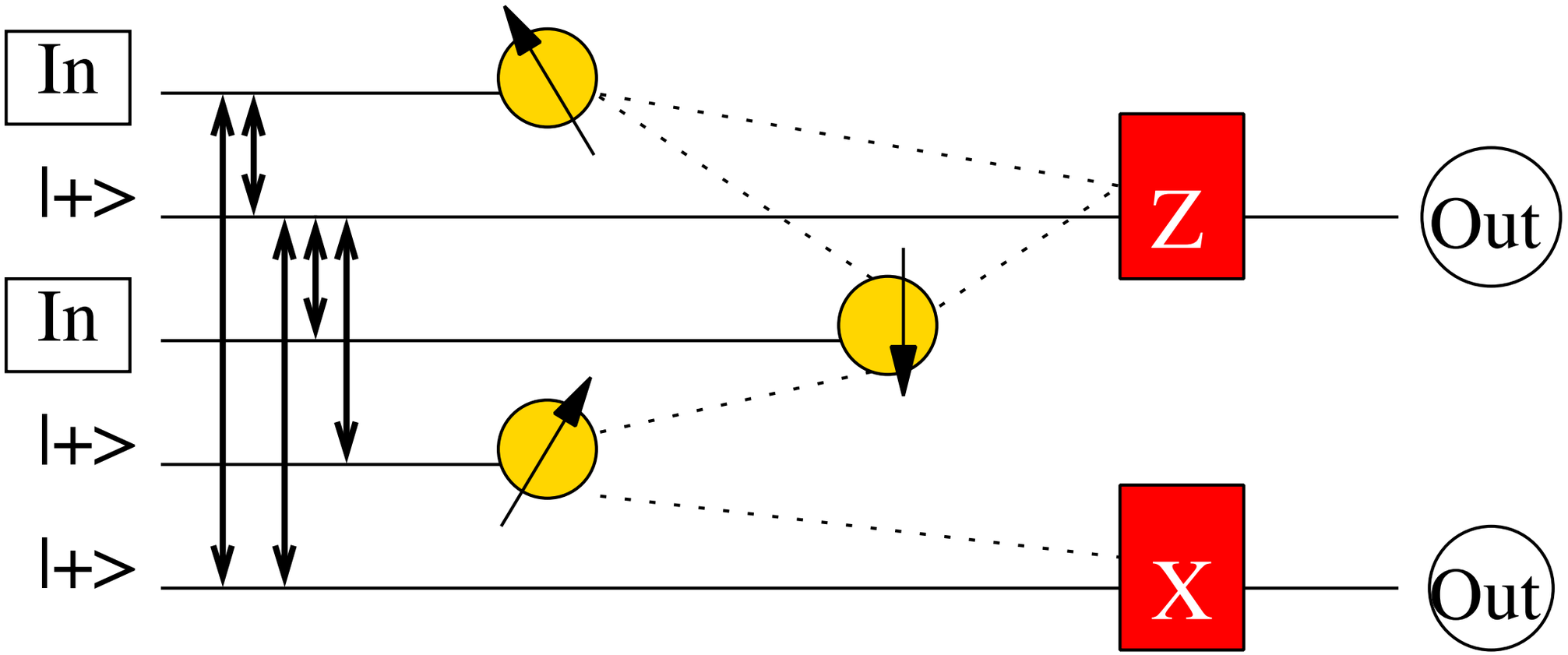
Quantum Pacman



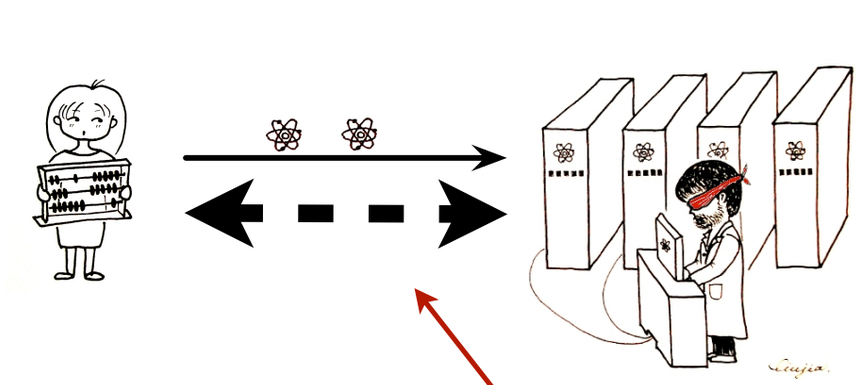
Quantum Pacman

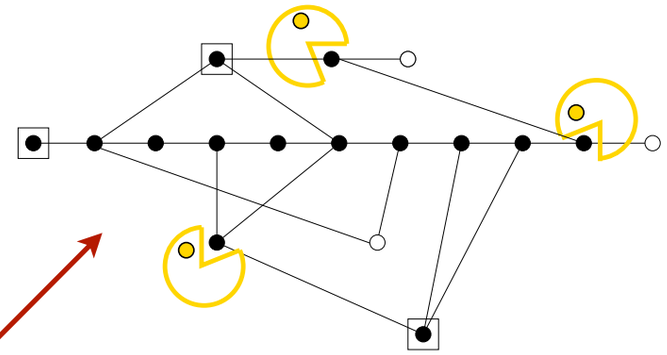


Circuit Picture



Roadmap for Quantum Verification





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

Hiding Complexity

Hiding Complexity

Encryption

Enables Secure Communication

Access to data is all or nothing

Hiding Complexity

Encryption

Enables Secure Communication

Access to data is all or nothing

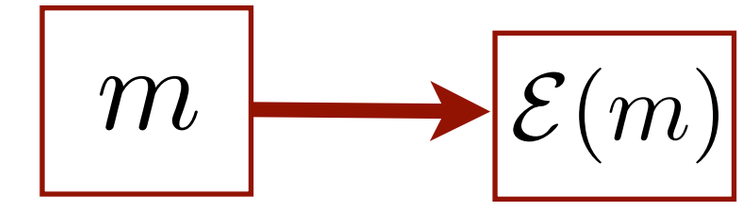
Modern Encryption

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

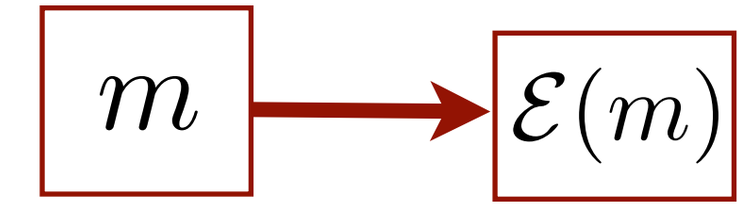
Holy Grail of Cryptography since 1987

Holy Grail of Cryptography since 1987

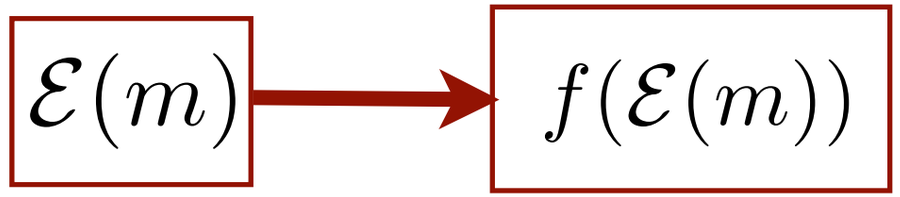
Holy Grail of Cryptography since 1987



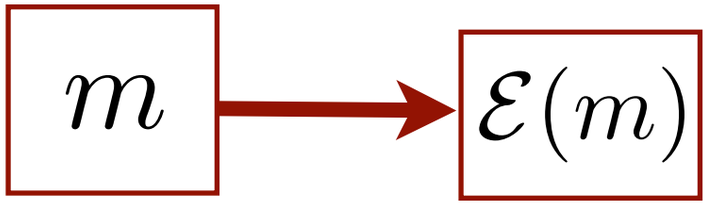
Holy Grail of Cryptography since 1987



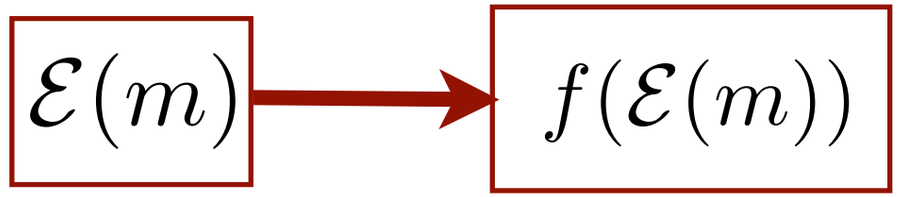
Limited Client ⟷ **Untrusted Server**

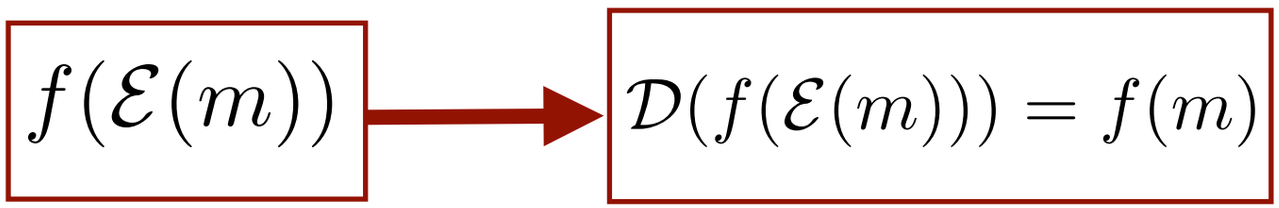


Holy Grail of Cryptography since 1987



Limited Client ⟷ **Untrusted Server**





Holy Grail of Cryptography since 1987

Holy Grail of Cryptography since 1987

Classical World

Gentry 09
A Lattice-based cryptosystem that is fully homomorphic

Holy Grail of Cryptography since 1987

Classical World

Quantum World

Gentry 09
A Lattice-based cryptosystem that is fully homomorphic

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

Applications

Secure Cloud

Remote File Storage

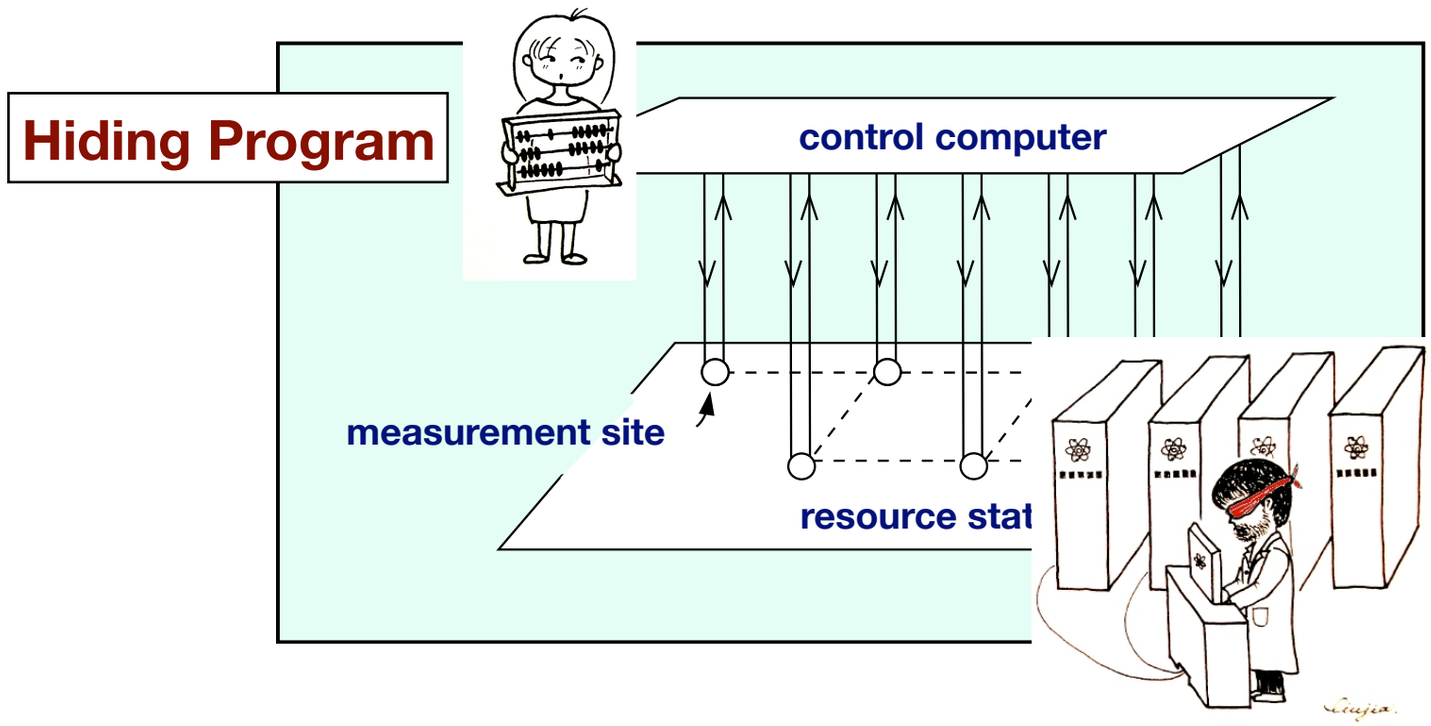
Secure Multi Party Computation

Verification of Outsourced Computation

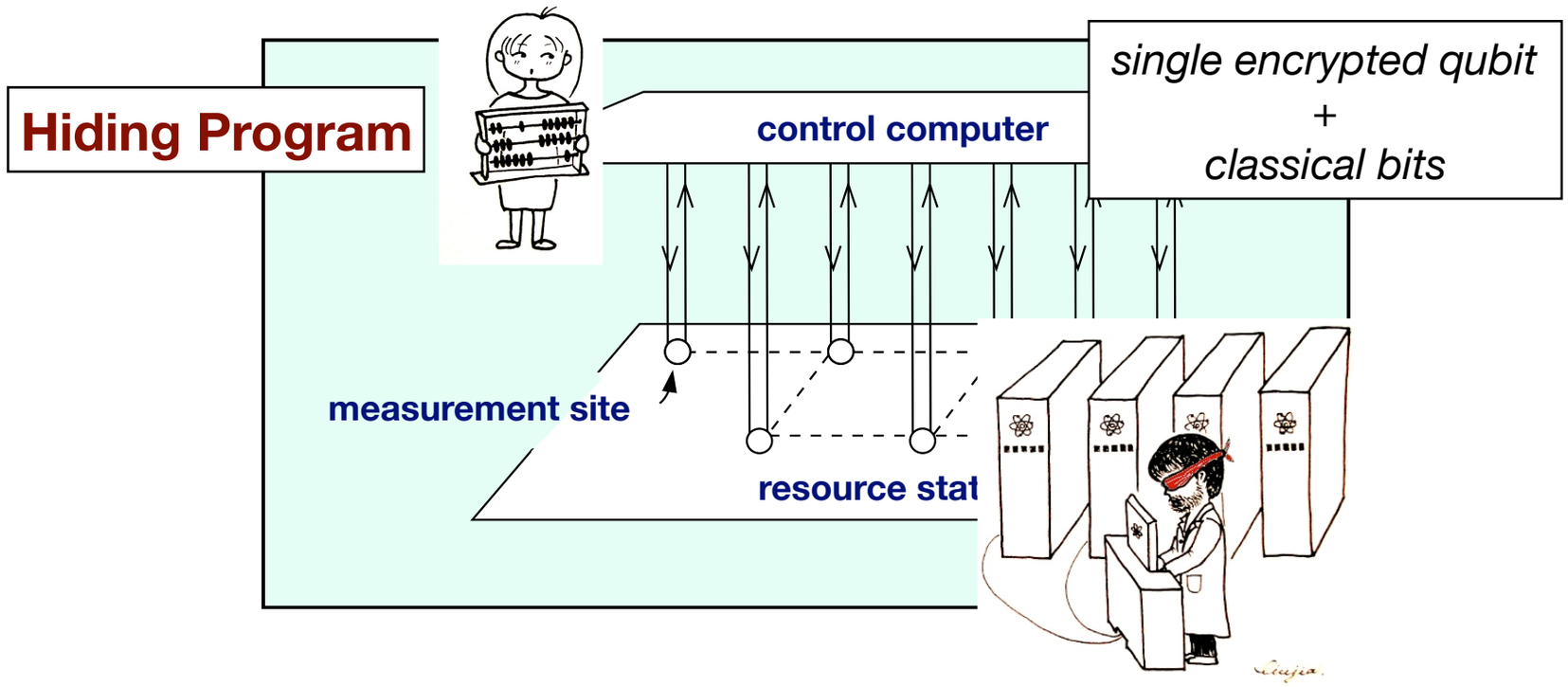
Short Proof of Knowledge

....

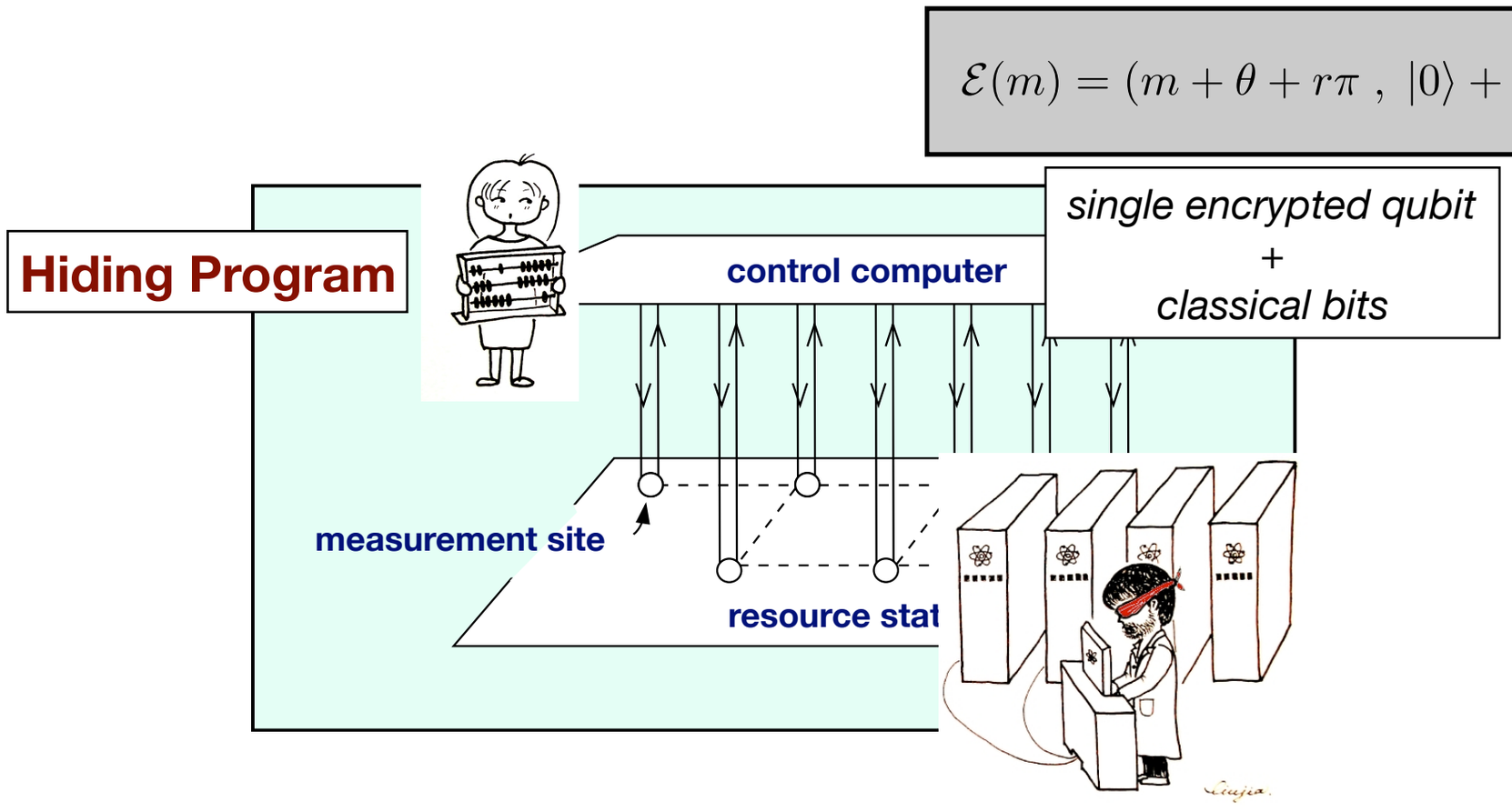
Universal Blind Quantum Computing



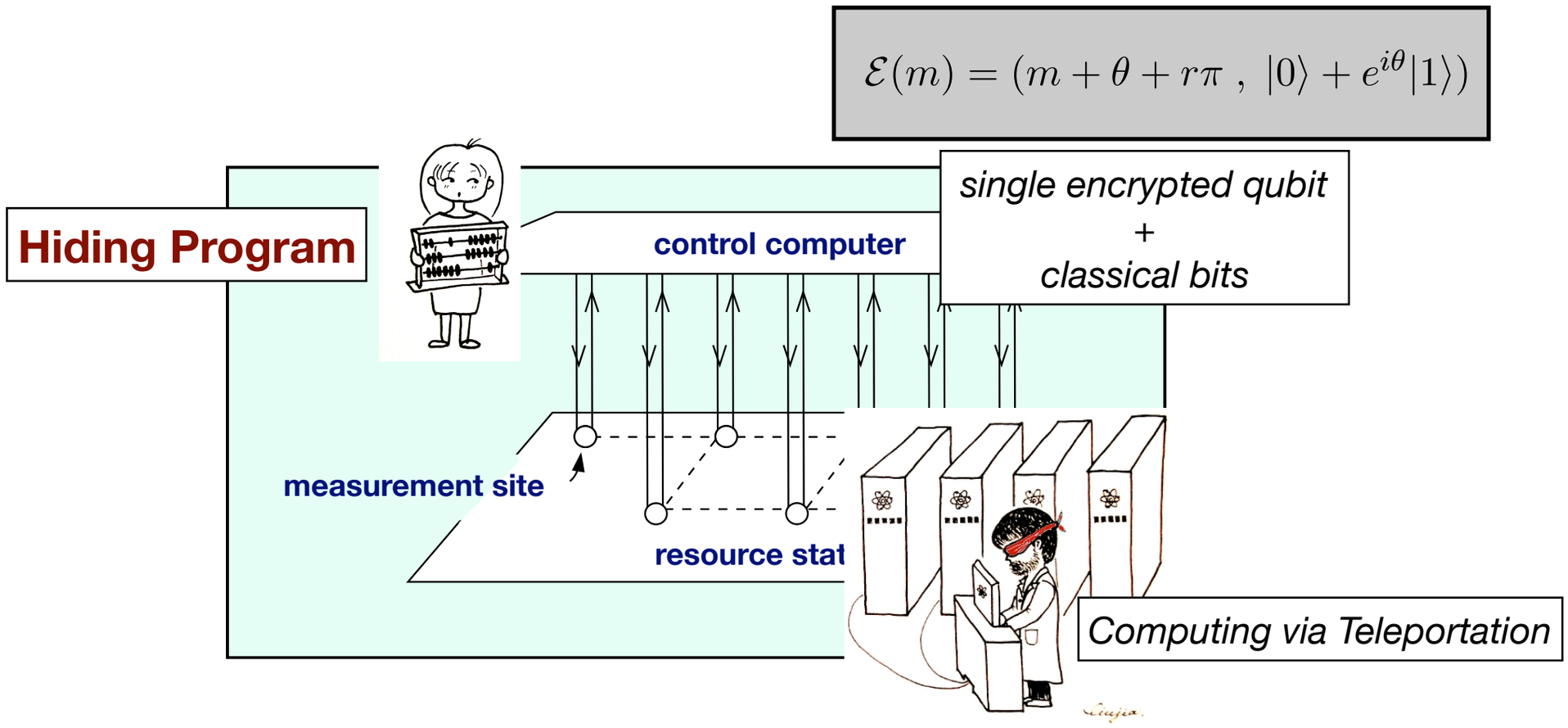
Universal Blind Quantum Computing



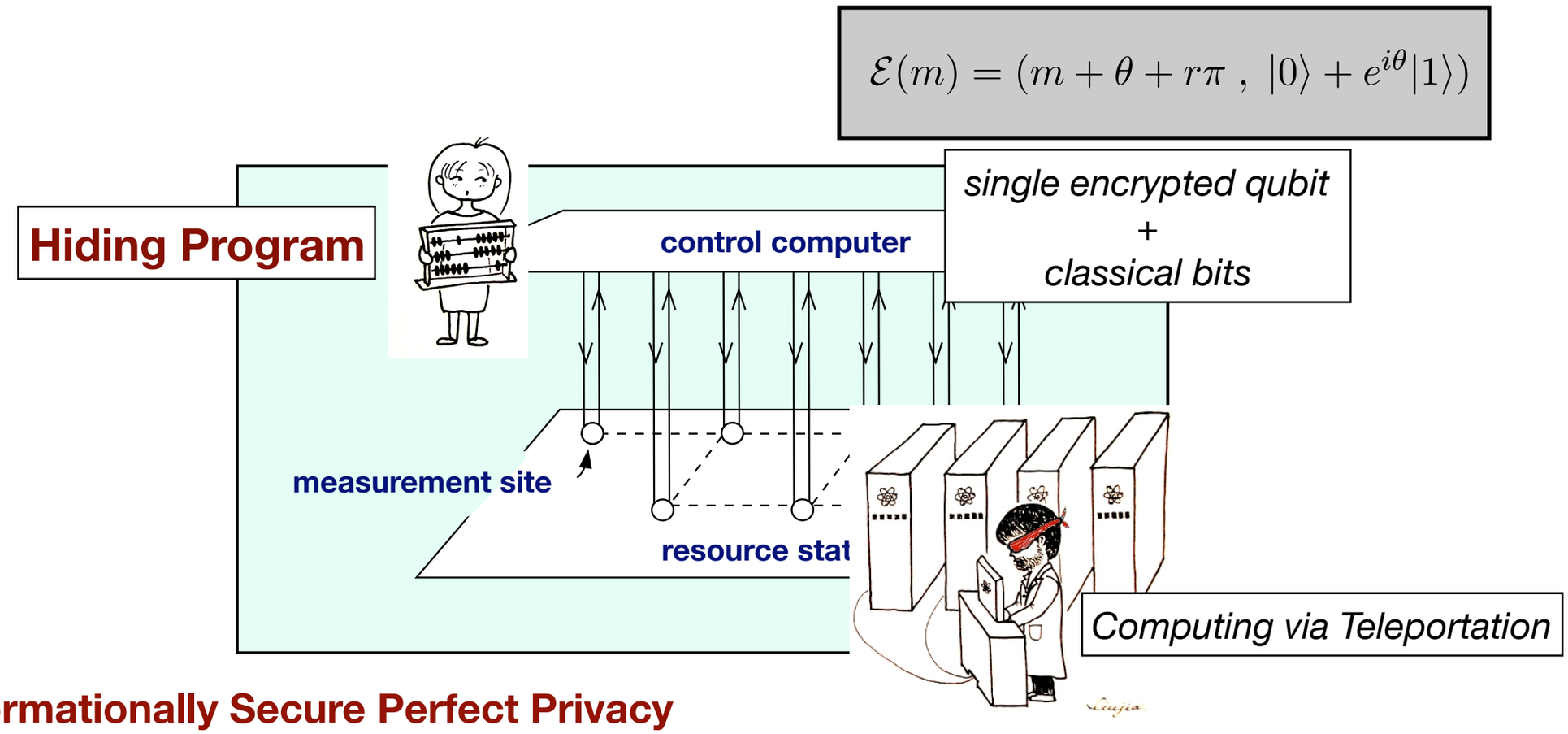
Universal Blind Quantum Computing



Universal Blind Quantum Computing



Universal Blind Quantum Computing



Informationally Secure Perfect Privacy

Server learns nothing about client's input/output/function

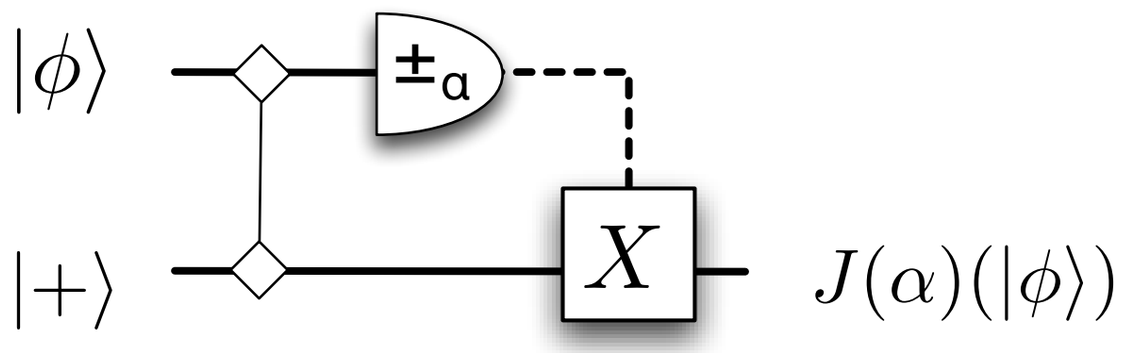
Hiding in MBQC

$$J(\alpha) \;:=\; \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 & e^{i\alpha} \\ 1 & -e^{i\alpha} \end{pmatrix}$$

Hiding in MBQC

$$J(\alpha) \;:=\; \tfrac{1}{\sqrt{2}}\begin{pmatrix} 1 & e^{i\alpha} \\ 1 & -e^{i\alpha} \end{pmatrix}$$

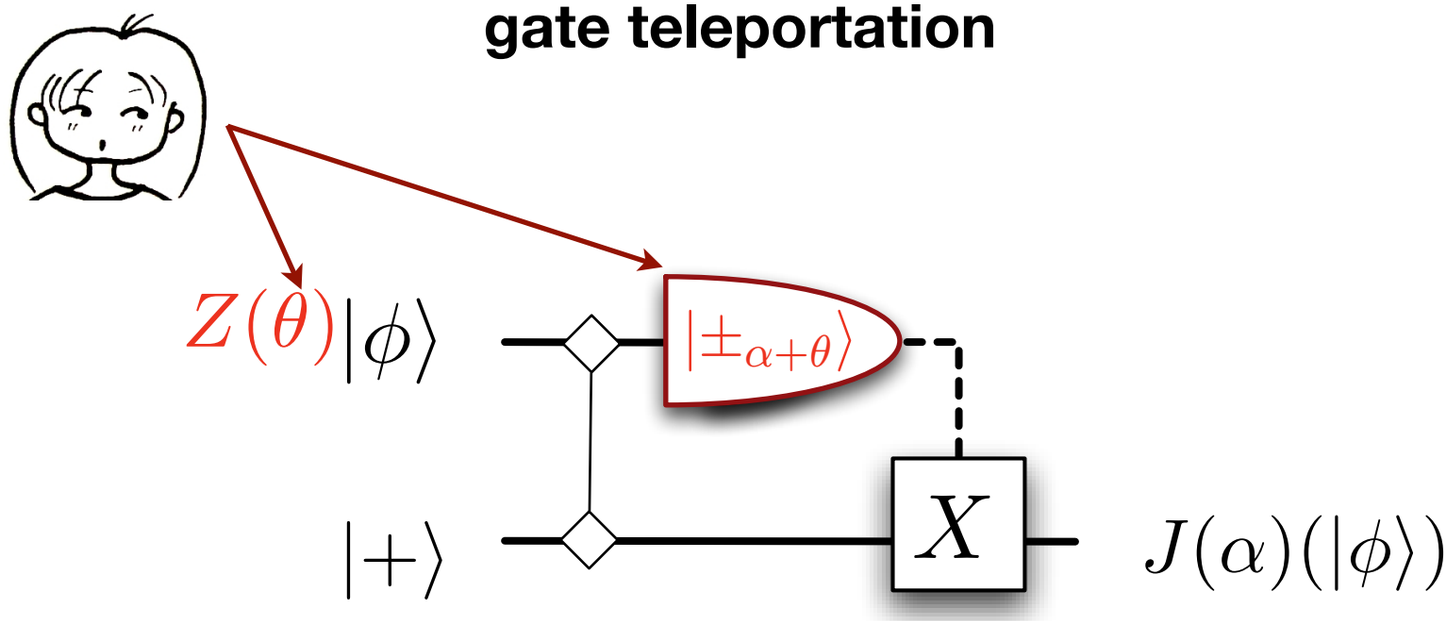
gate teleportation



Hiding in MBQC

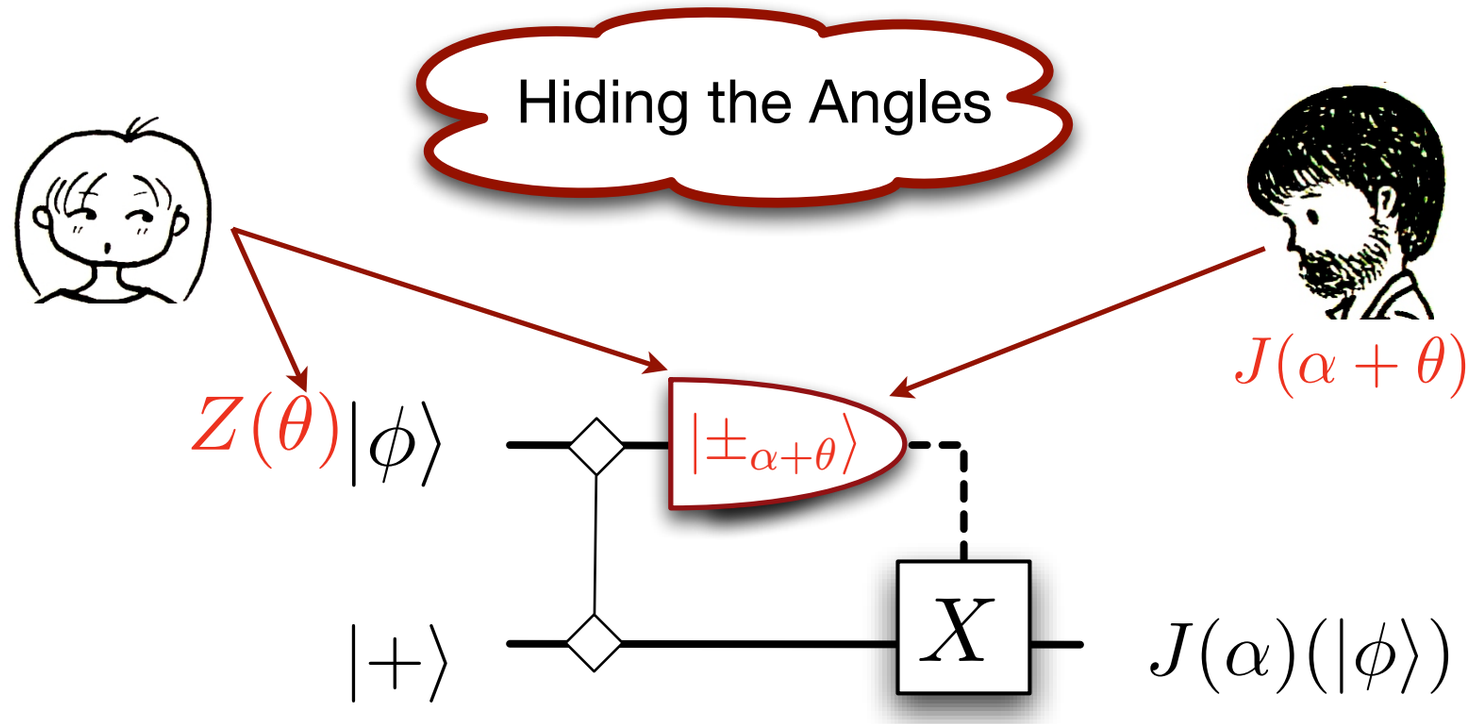
$$J(\alpha) \;:=\; \tfrac{1}{\sqrt{2}}\begin{pmatrix} 1 & e^{i\alpha} \\ 1 & -e^{i\alpha} \end{pmatrix}$$

gate teleportation



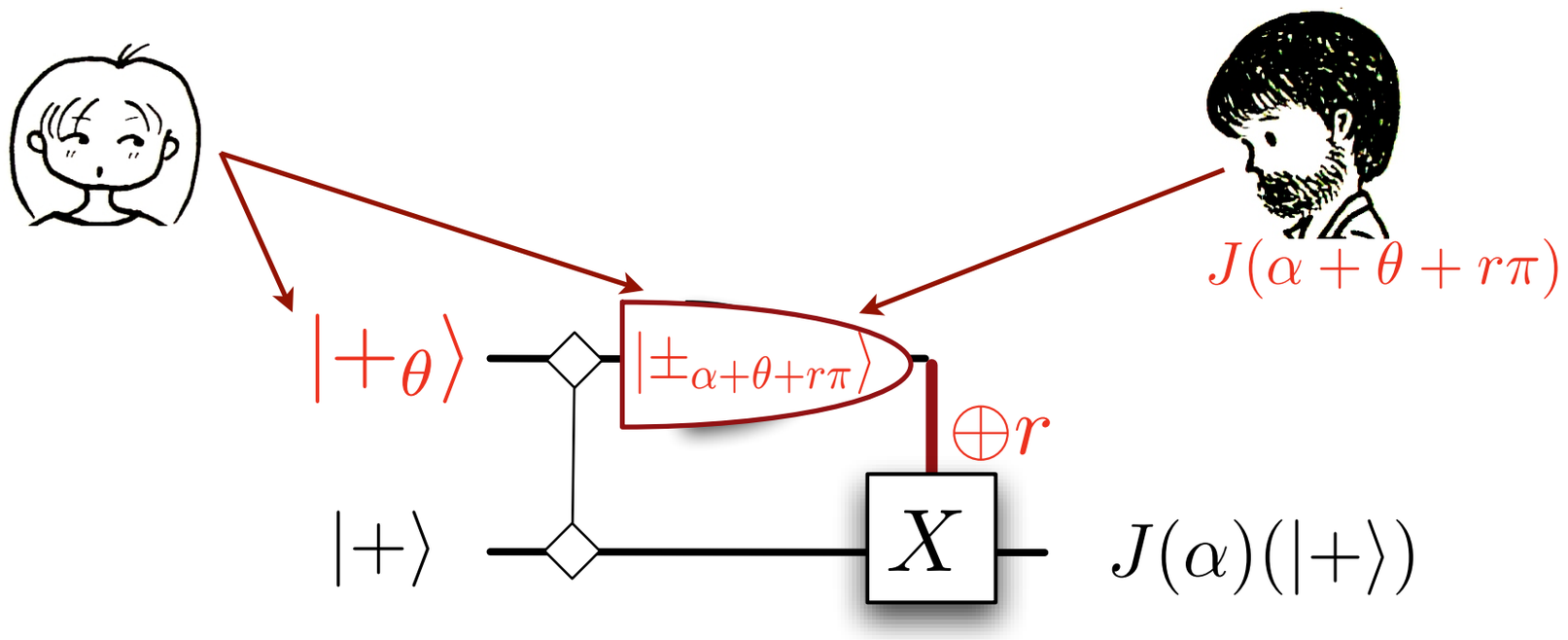
Hiding in MBQC

$$J(\alpha) \;:=\; \tfrac{1}{\sqrt{2}}\begin{pmatrix} 1 & e^{i\alpha} \\ 1 & -e^{i\alpha} \end{pmatrix}$$



Thinking inside the box

$$J(\alpha) \;:=\; \tfrac{1}{\sqrt{2}}\begin{pmatrix} 1 & e^{i\alpha} \\ 1 & -e^{i\alpha} \end{pmatrix}$$



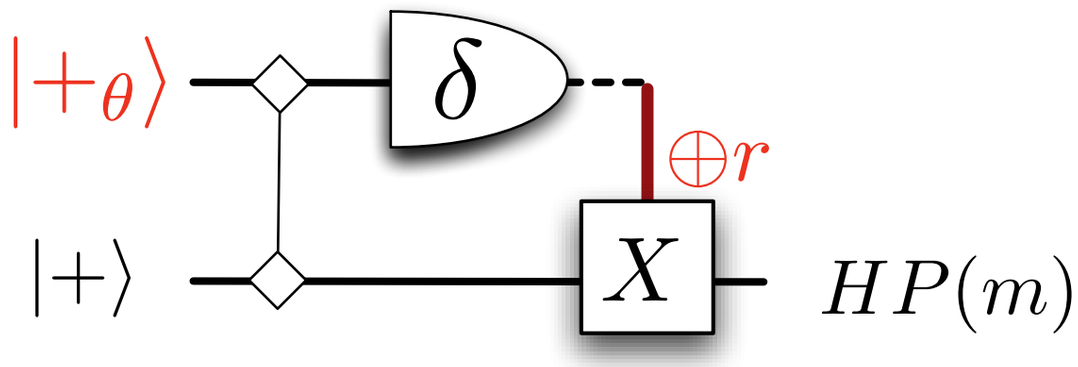
Hiding the measurement result

Hiding Operations via Gate Teleportation

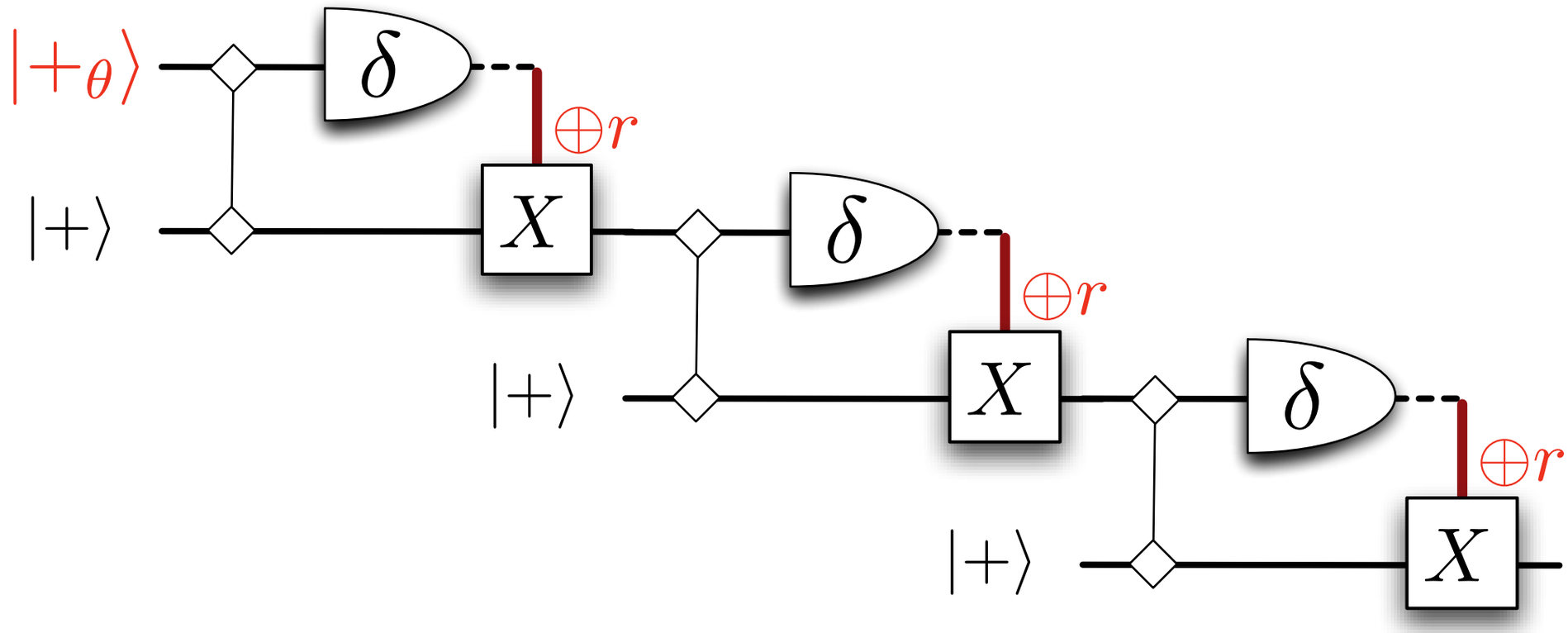
$$\theta \in_R \{0, \pi/4, 2\pi/4, \cdots, 7\pi/4\}$$

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

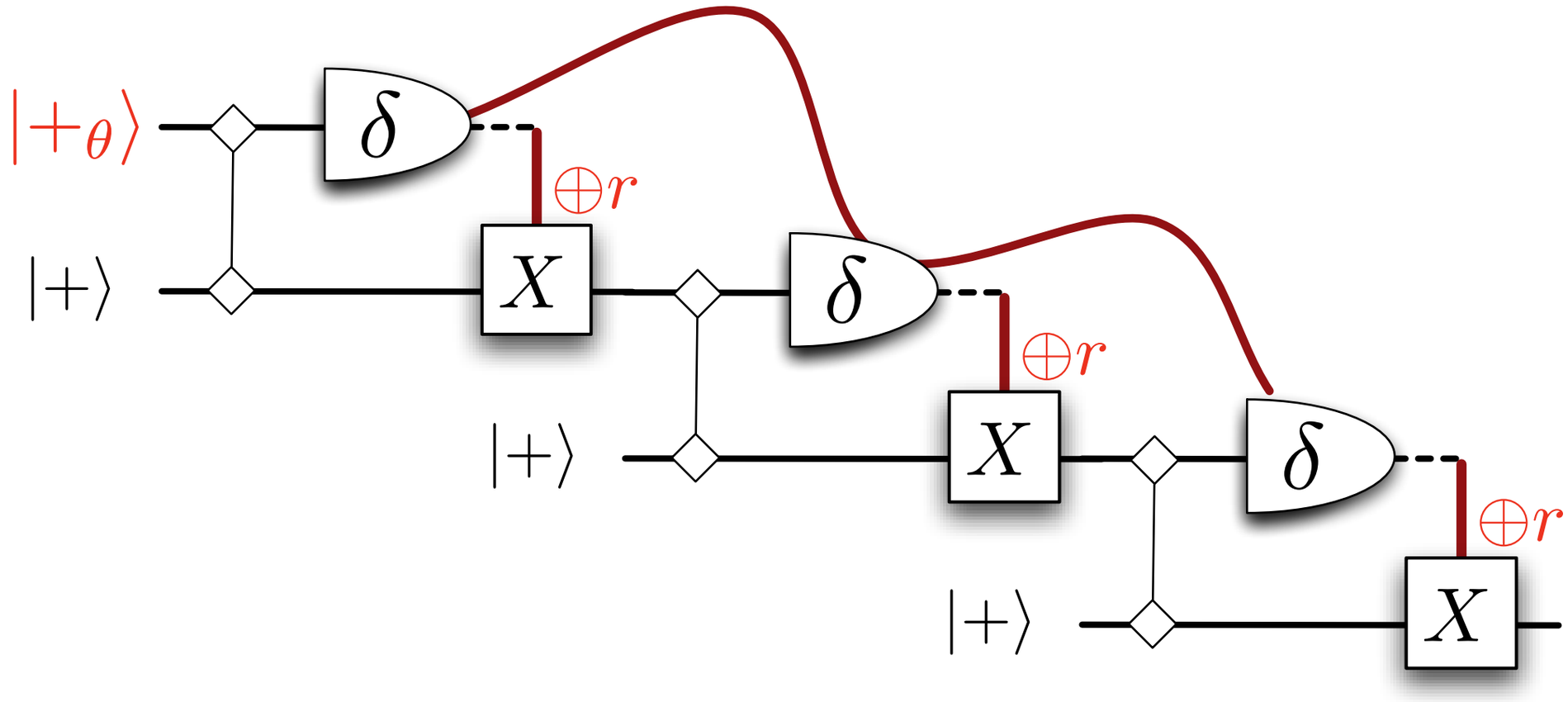
Limited Client → **Untrusted Server**



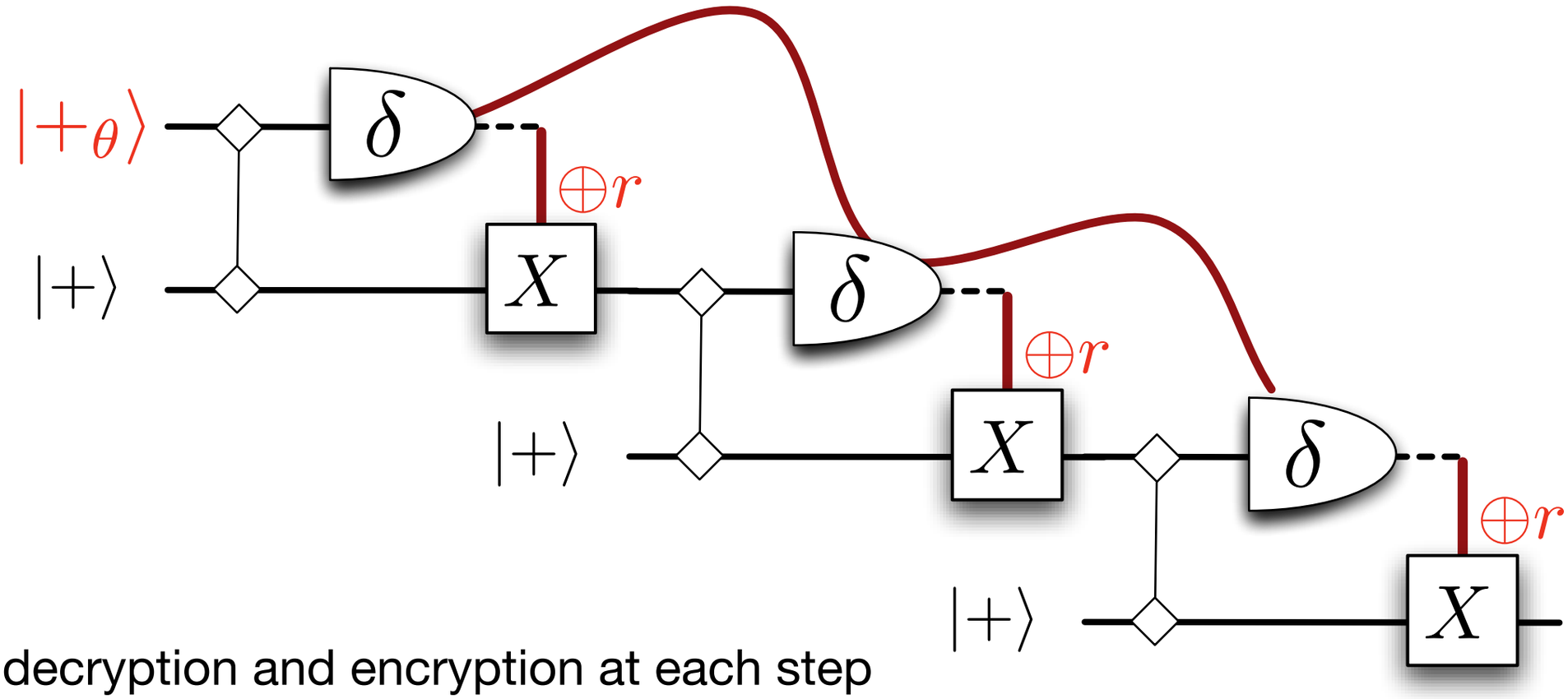
Gates Composition



Gates Composition



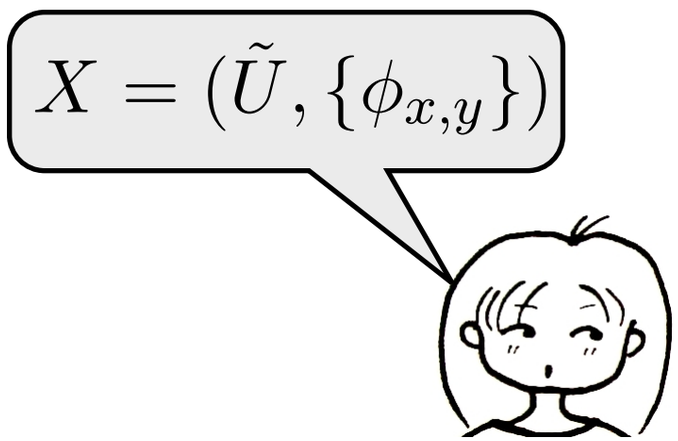
Gates Composition



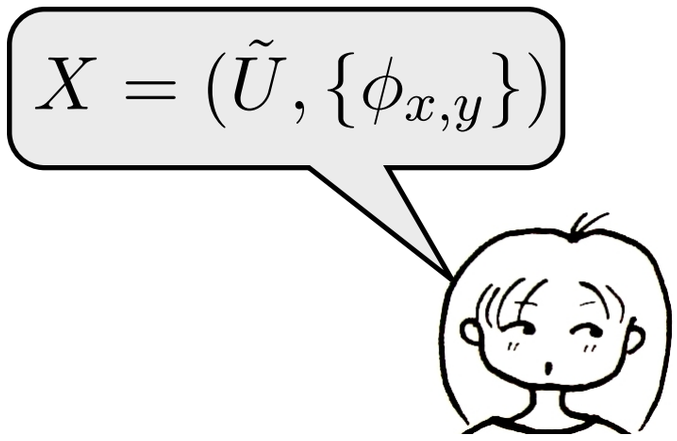
Perfect decryption and encryption at each step

Client-Server interactions

Universal Blind Quantum Computings



Universal Blind Quantum Computings

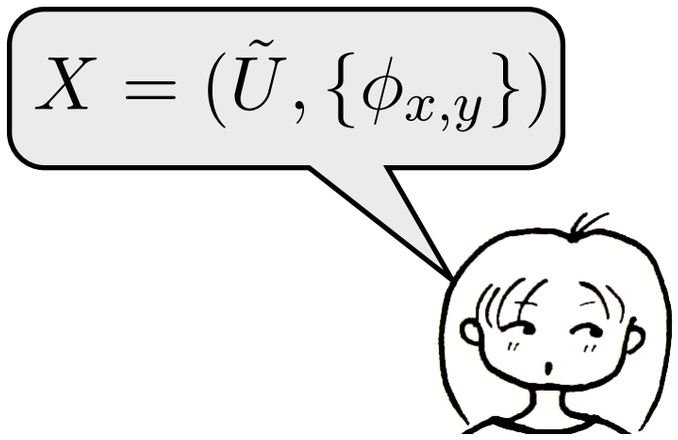


random single qubit generator

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

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

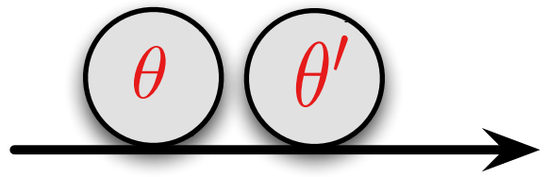
Universal Blind Quantum Computings



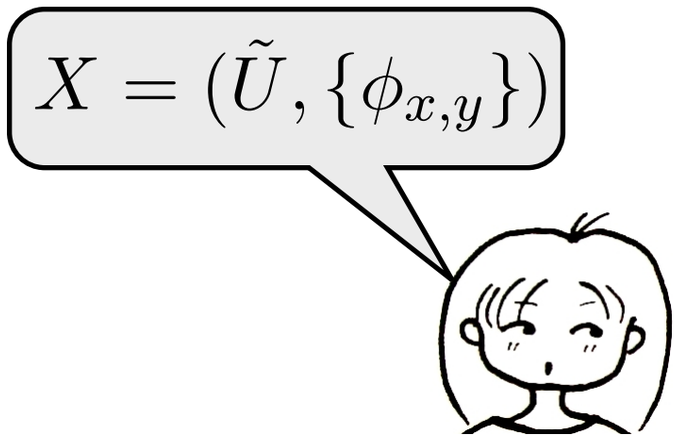
random single qubit generator

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

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



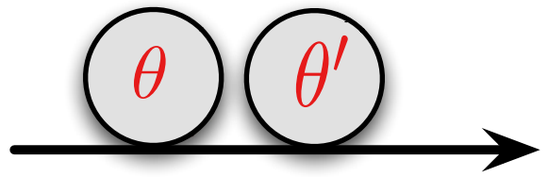
Universal Blind Quantum Computings

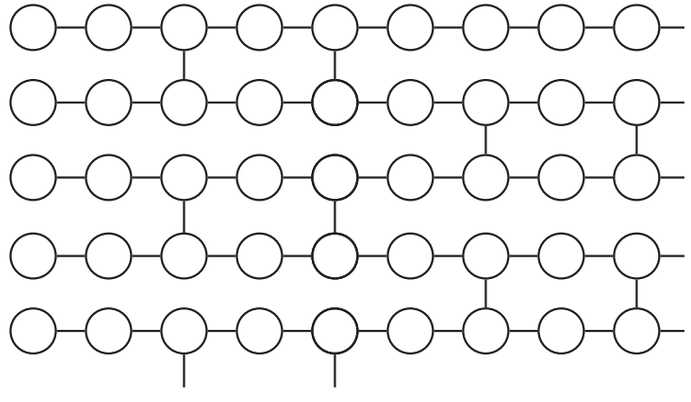


random single qubit generator

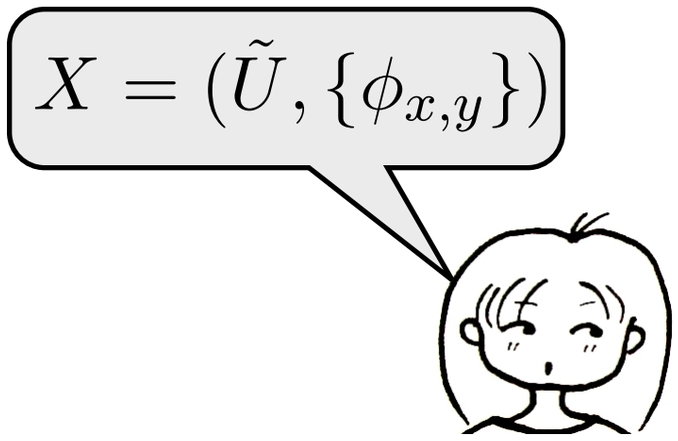
$$1/\sqrt{2}\left(|0\rangle + e^{i\theta}\,|1\rangle\right)$$

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





Universal Blind Quantum Computings



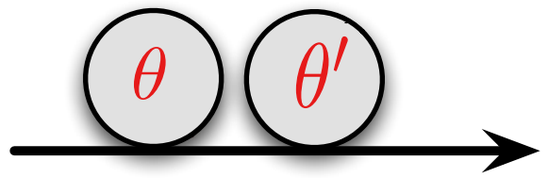
random single qubit generator

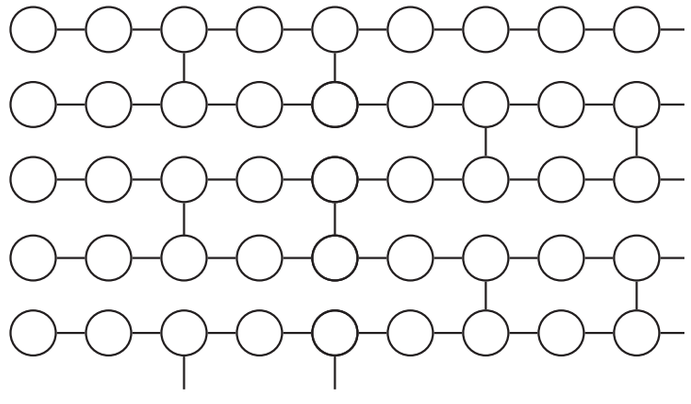
$$1/\sqrt{2}\left(|0\rangle + e^{i\theta}\,|1\rangle\right)$$

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

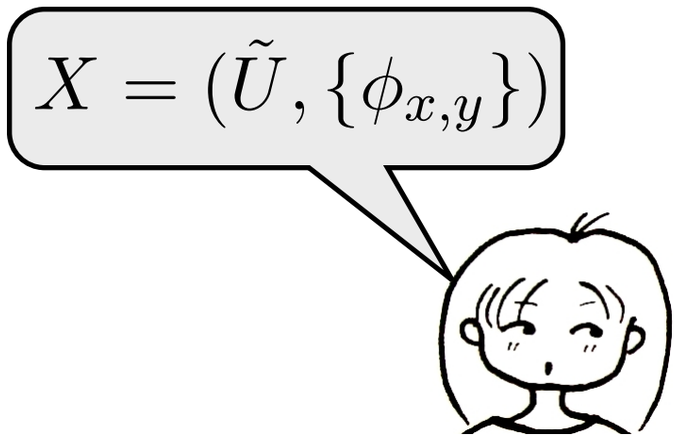
$$r_{x,y} \in_R \{0,1\}$$

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





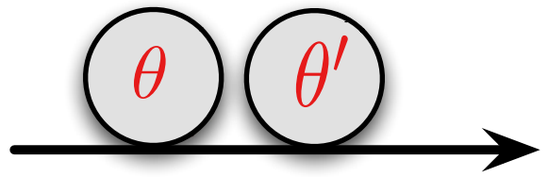
Universal Blind Quantum Computings



random single qubit generator

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

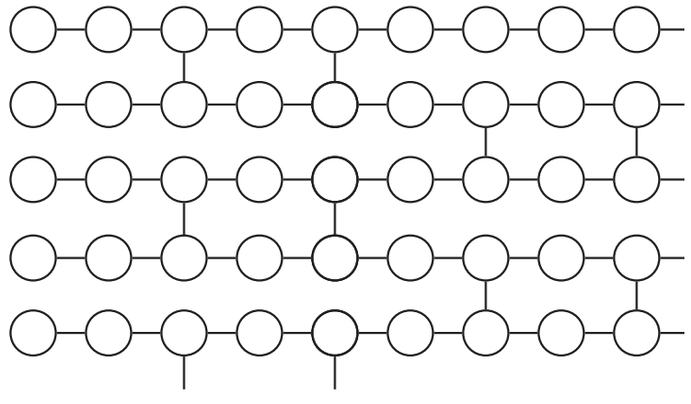
$$\theta = 0, \pi/4, 2\pi/4, \ldots, 7\pi/4$$



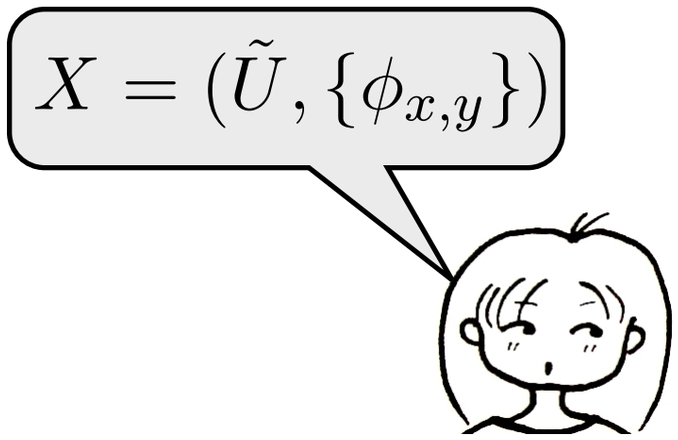
$\delta_{x,y}$

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

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



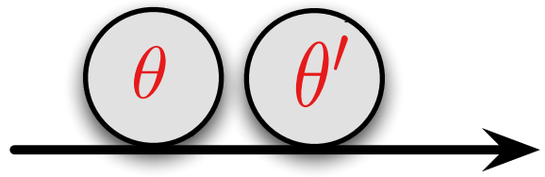
Universal Blind Quantum Computings



random single qubit generator

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

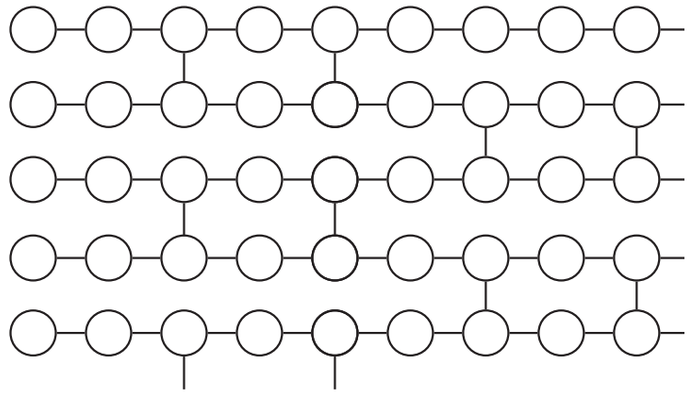
$$\theta = 0, \pi/4, 2\pi/4, \ldots, 7\pi/4$$



$\delta_{x,y}$

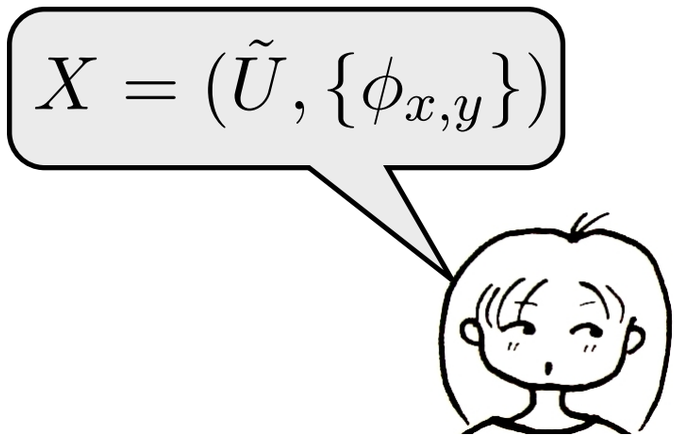
$$r_{x,y} \in_R \{0,1\}$$

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



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

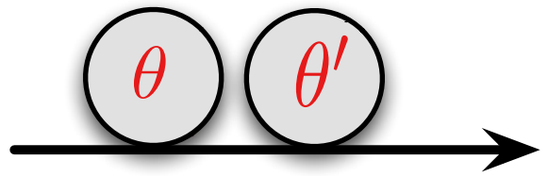
Universal Blind Quantum Computings



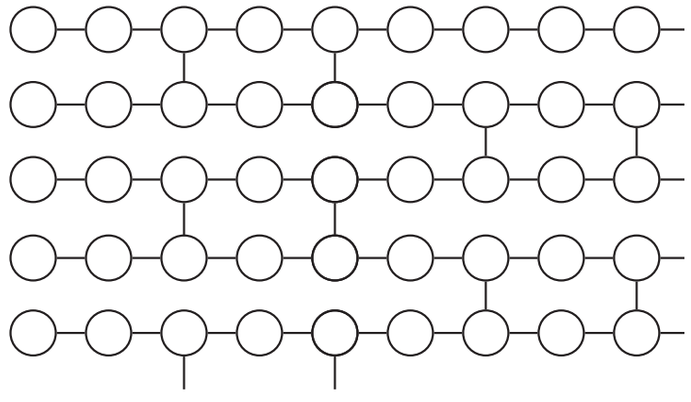
random single qubit generator

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

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



$\delta_{x,y}$



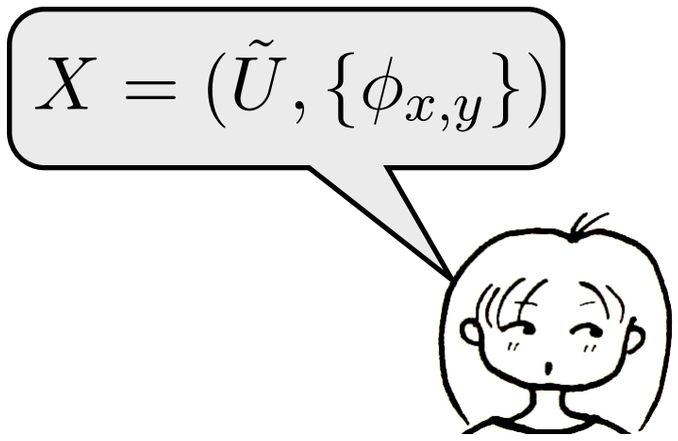
$r_{x,y} \in_R \{0, 1\}$

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

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

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

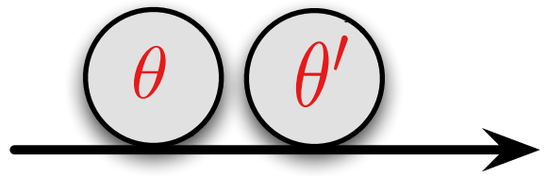
Universal Blind Quantum Computings



random single qubit generator

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

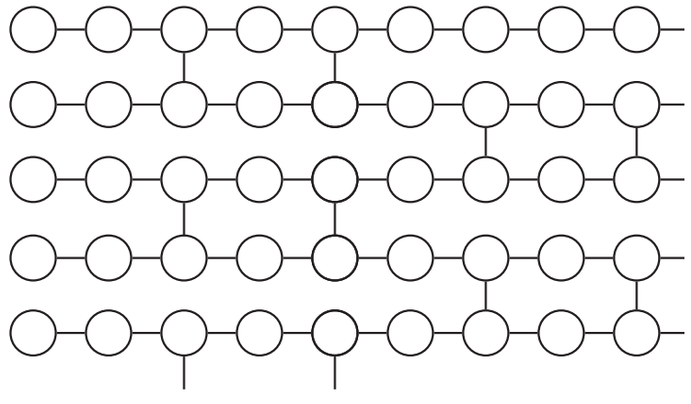
$$\theta = 0, \pi/4, 2\pi/4, \ldots, 7\pi/4$$



$\delta_{x,y}$

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

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

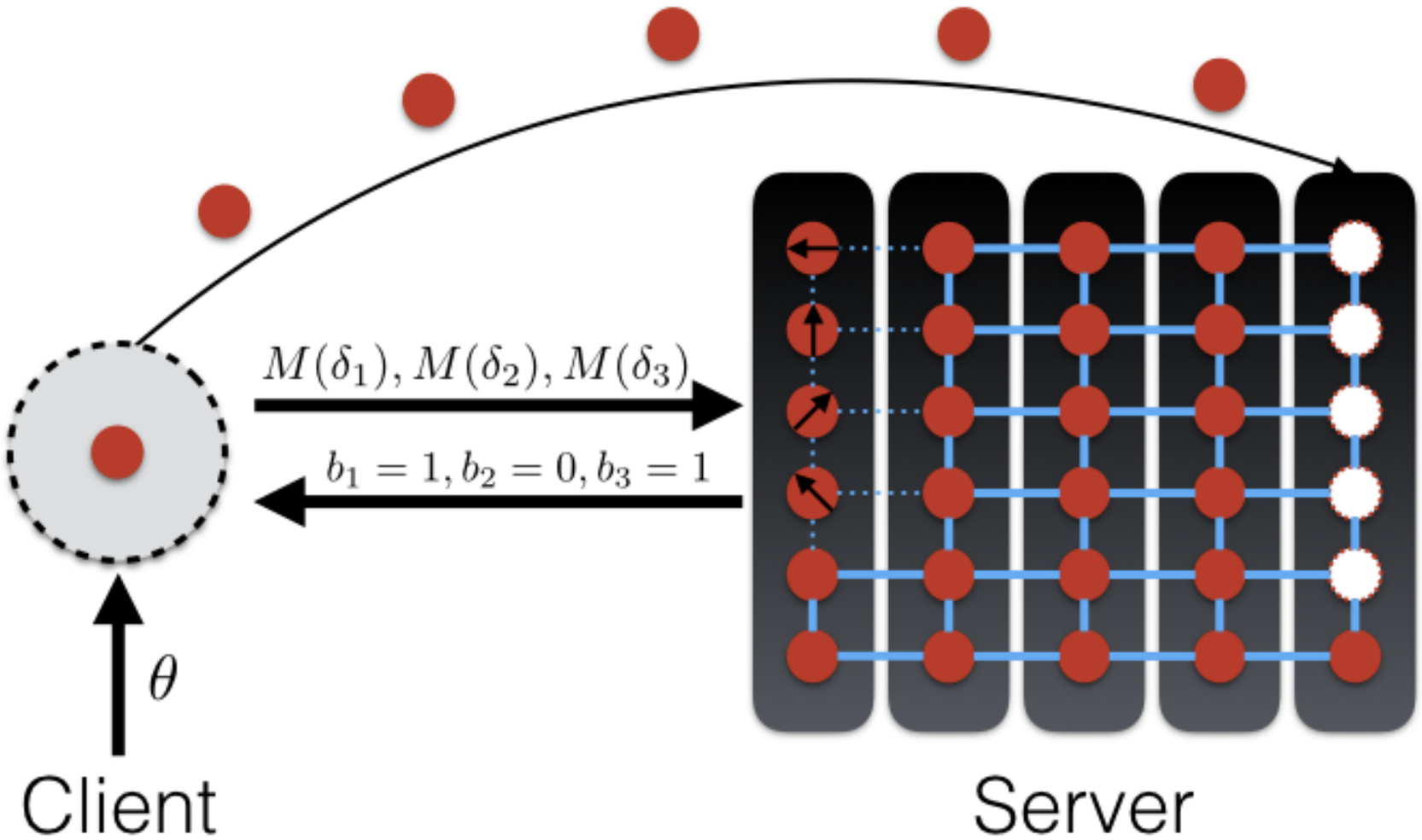


$$\{\left|+\delta_{x,y}\right\rangle, \left|-\delta_{x,y}\right\rangle\}$$

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

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

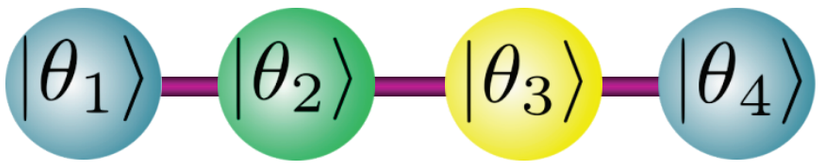
Unconditionally Secure Quantum Cloud in Theory

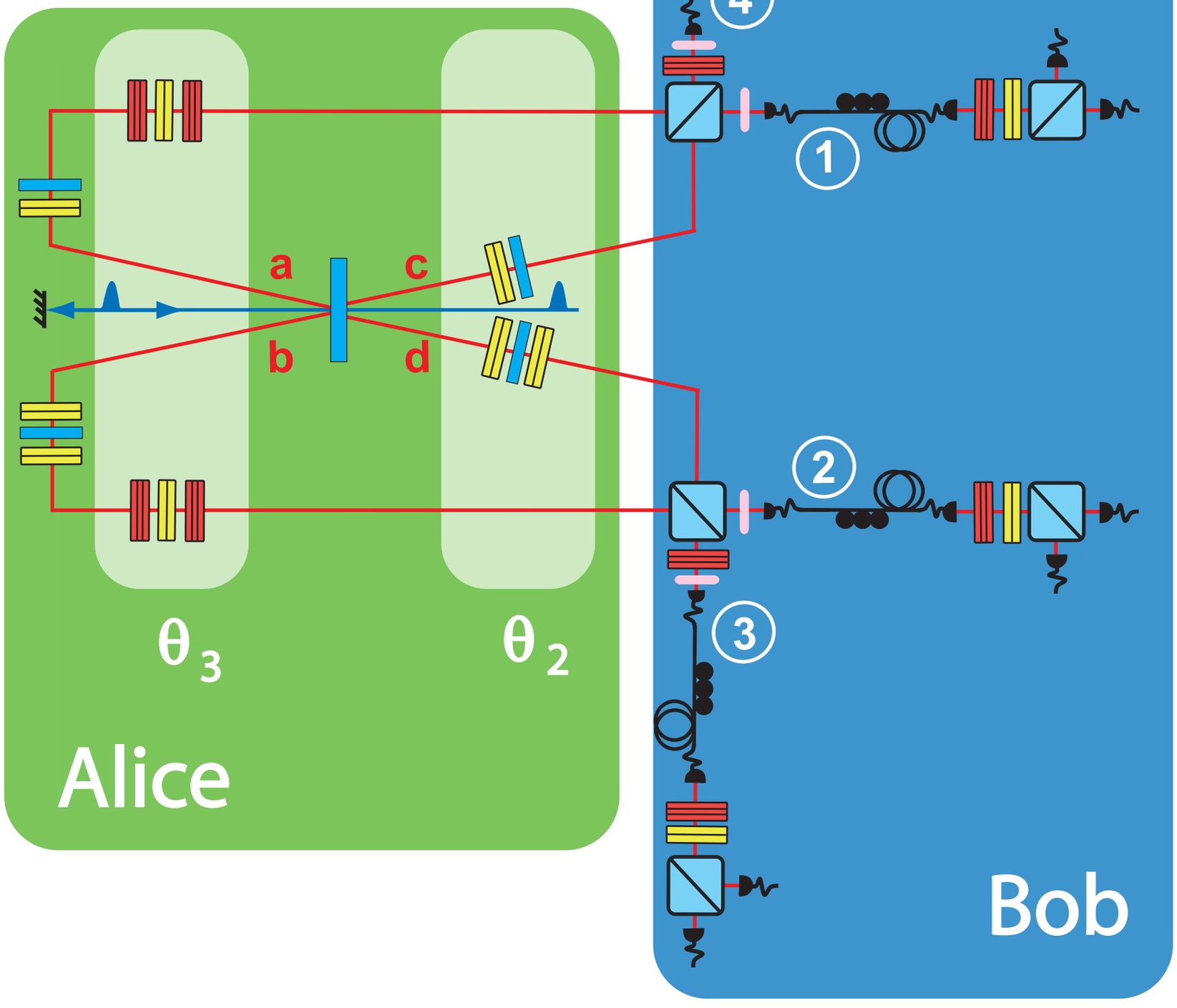


Broadbent, Fitzsimons and Kashefi, FOCS09

In practice

S. Barz, E. Kashefi, A. Broadbent, J. Fitzsimons, A. Zeilinger, P. Walther, Science 2012





Do we really need Photonic Link ?

Fillinger: No efficient informationally secure classical FHE scheme exist

Do we really need Photonic Link ?

Fillinger: No efficient informationally secure classical FHE scheme exist

Newman and Shi: No efficient informationally secure quantum FHE scheme exist

Do we really need Photonic Link ?

Fillinger: No efficient informationally secure classical FHE scheme exist

Newman and Shi: No efficient informationally secure quantum FHE scheme exist

No classical Group Homomorphic Encryption can be IND-CPA secure

Do we really need Photonic Link ?

Fillinger: No efficient informationally secure classical FHE scheme exist

Newman and Shi: No efficient informationally secure quantum FHE scheme exist

No classical Group Homomorphic Encryption can be IND-CPA secure

→ electronic voting
private information retrieval
multiparty computation

Do we really need Photonic Link ?

Fillinger: No efficient informationally secure classical FHE scheme exist

Newman and Shi: No efficient informationally secure quantum FHE scheme exist

No classical Group Homomorphic Encryption can be IND-CPA secure

→ electronic voting
private information retrieval
multiparty computation

What if we add interactivity (classical communication) ?

Do we really need Photonic Link ?

Do we really need Photonic Link ?

What if we add interactivity (classical communication) ?

Do we really need Photonic Link ?

What if we add interactivity (classical communication) ?

Dunjko et.al. : No informationally secure quantum scheme for classical function evaluation (for restricted classical client)

Do we really need Photonic Link ?

What if we add interactivity (classical communication) ?

Dunjko et.al. : No informationally secure quantum scheme for classical function evaluation (for restricted classical client)

Murimae: No informationally secure quantum scheme for quantum function evaluation (for restricted classical client)

Do we really need Photonic Link ?

What if we add interactivity (classical communication) ?

Dunjko et.al. : No informationally secure quantum scheme for classical function evaluation (for restricted classical client)

Murimae: No informationally secure quantum scheme for quantum function evaluation (for restricted classical client)

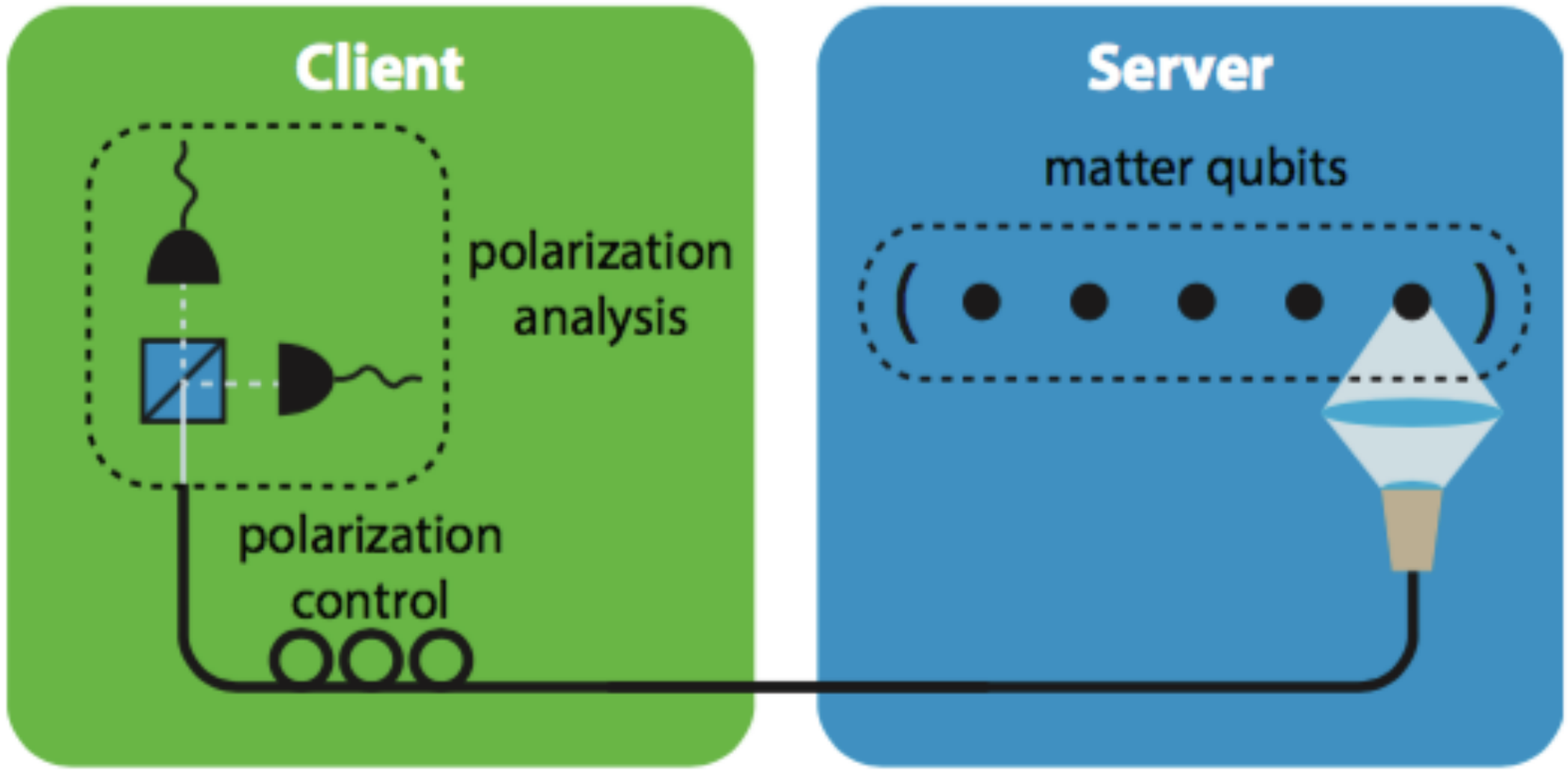
Linear Encryption

On the Impossibility of Secure Quantum Cloud Computing without Photonic Link

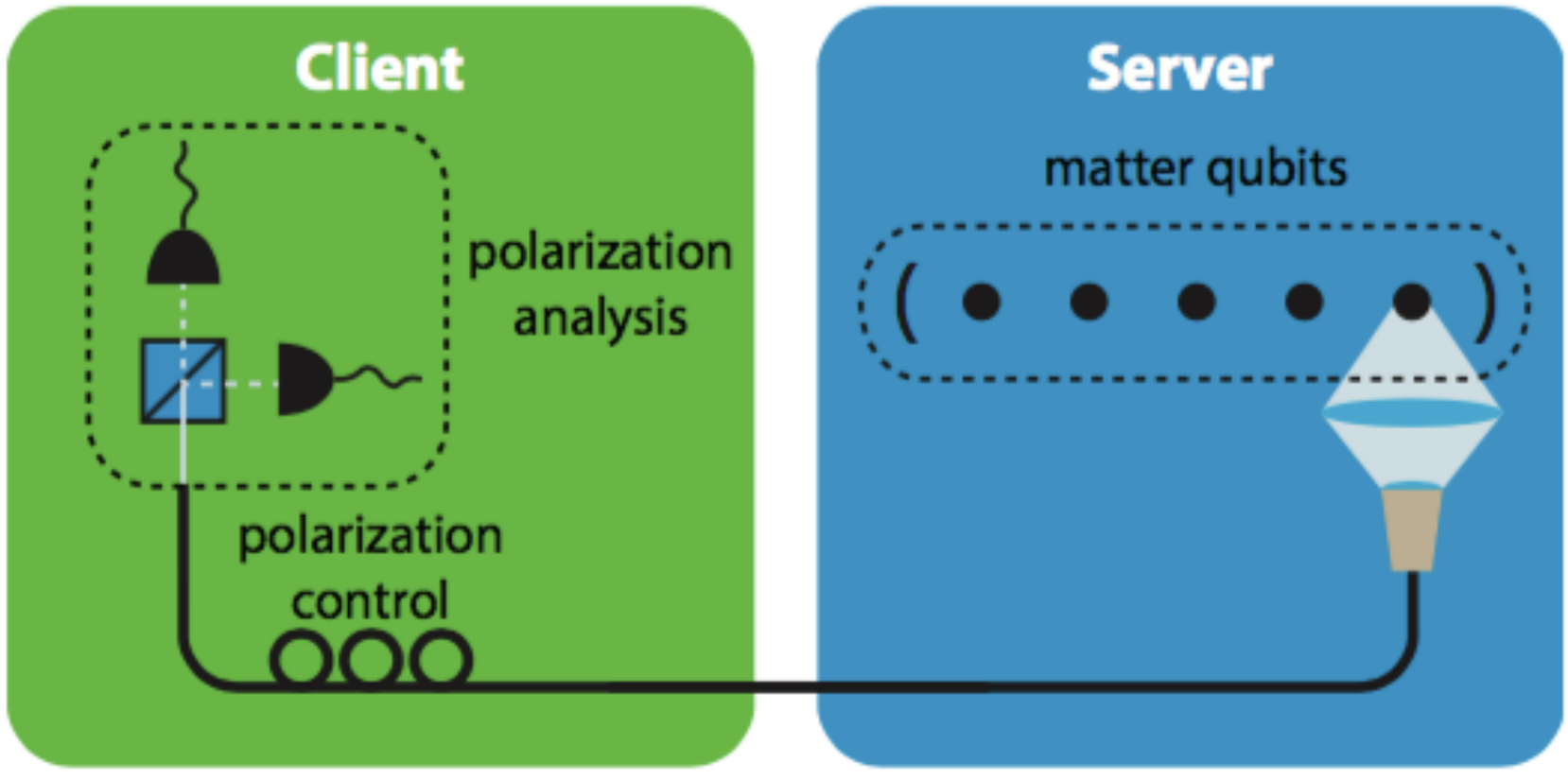
On the implausibility of classical client blind quantum computing

Aaronson, Cojocaru, Gheorghiu, Kashefi, Quantum Crypto 2017

Fundamental Equation of Universe

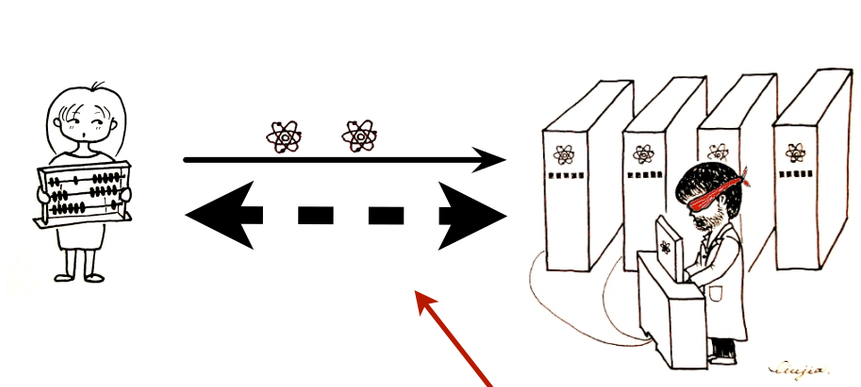


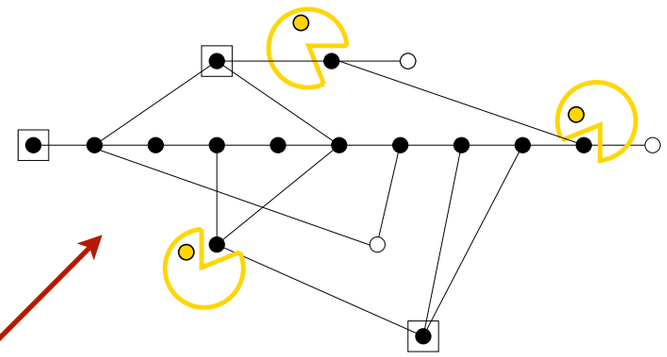
Fundamental Equation of Universe



Informationally Secure Quantum Cloud =
Classically-controlled QC =
Optically-controlled Device

Roadmap for Quantum Verification

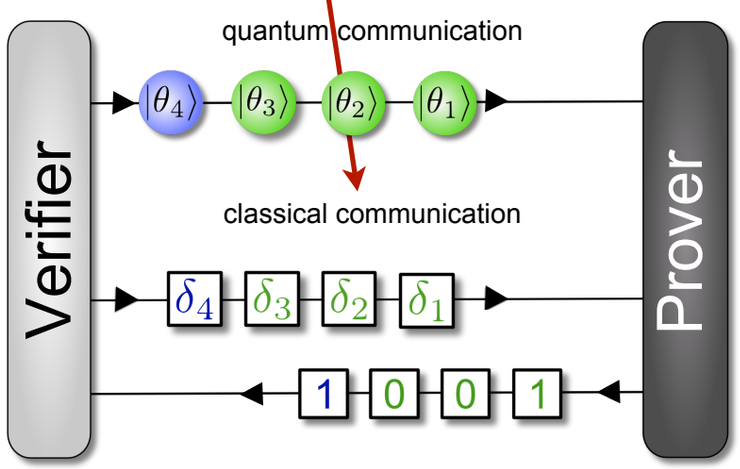




➡ Classically controlled QC

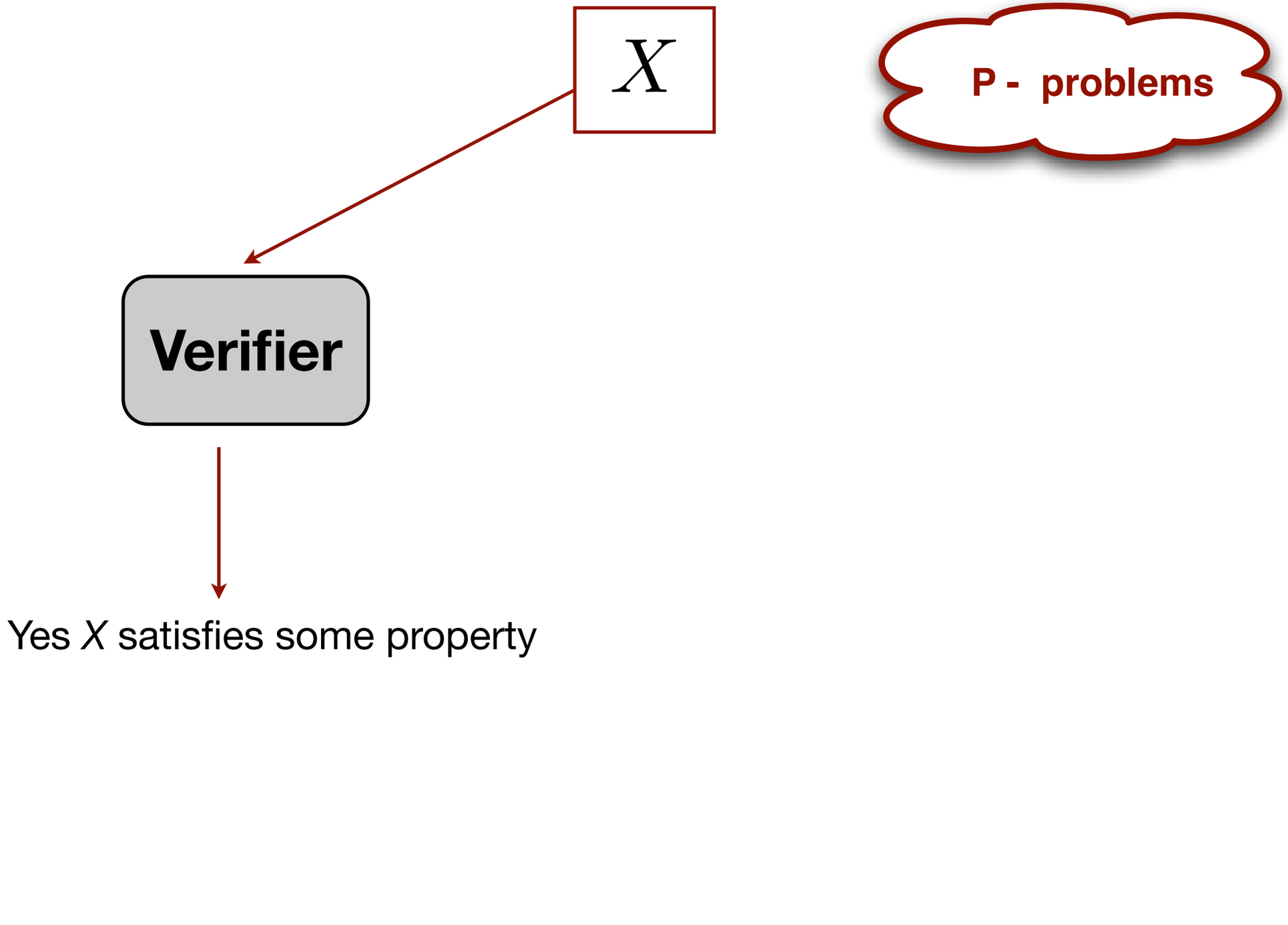
➡ Cryptographic Toolkit

➡ **Interactive Proof System**

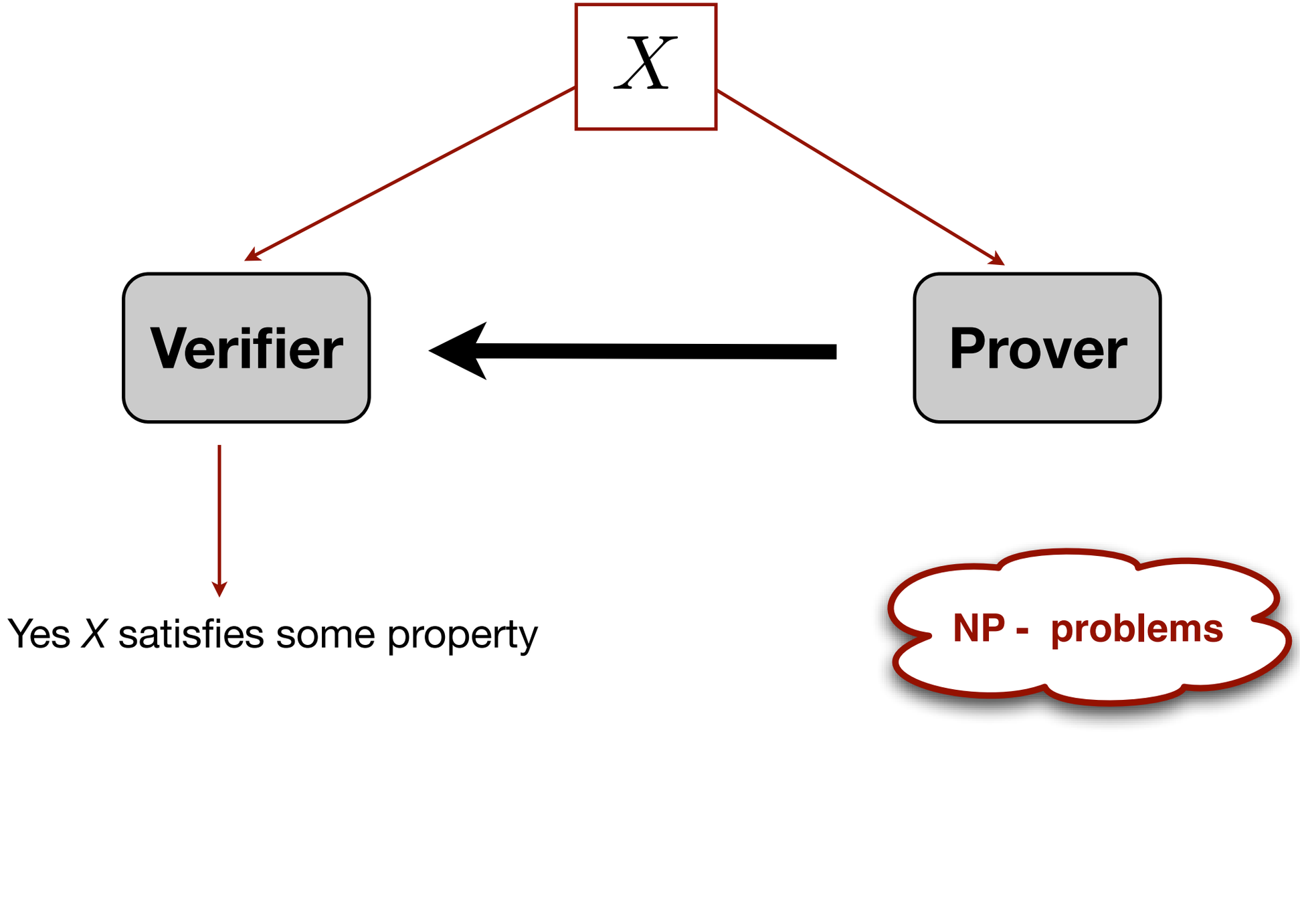


Complexity as Proof System

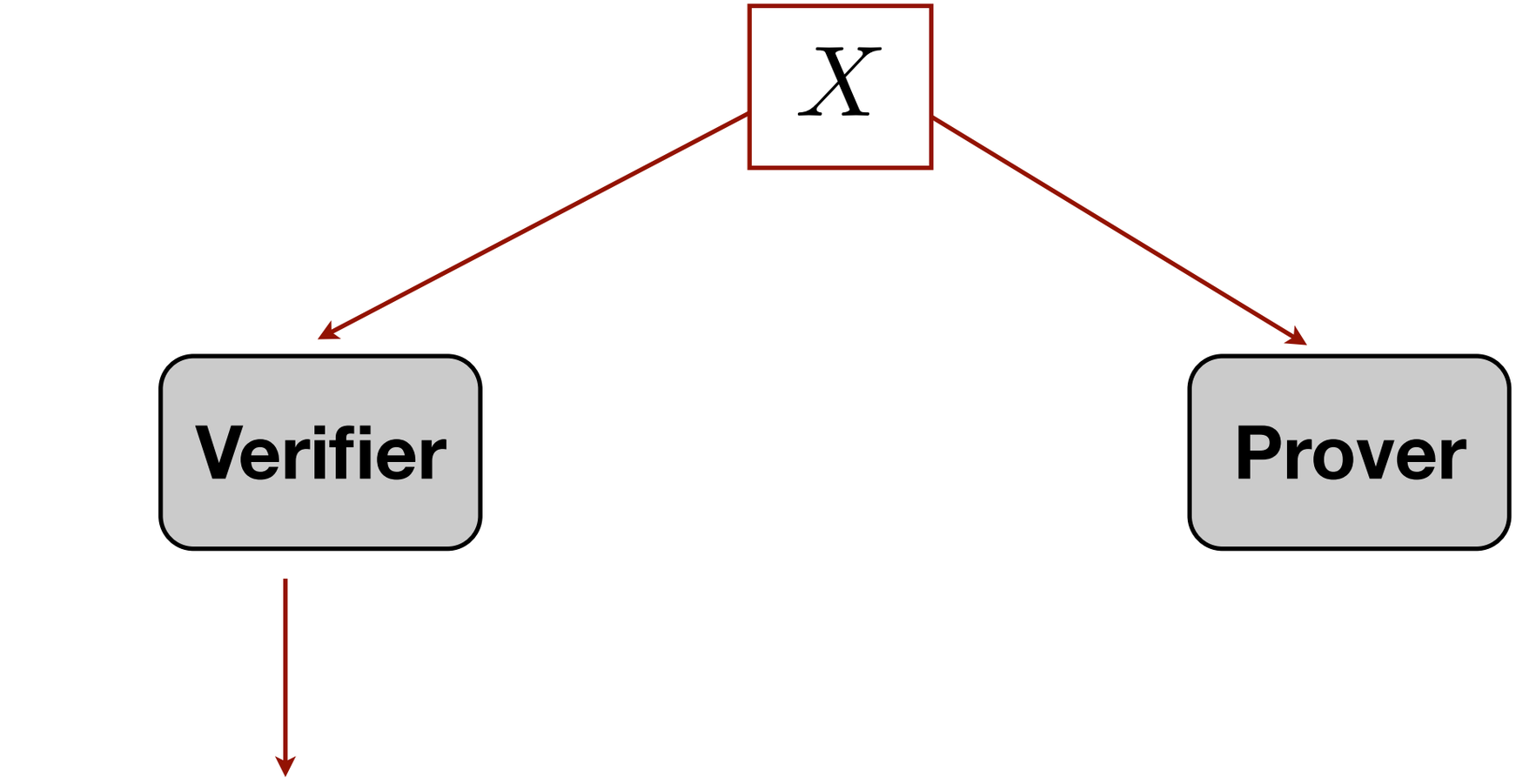
Complexity as Proof System



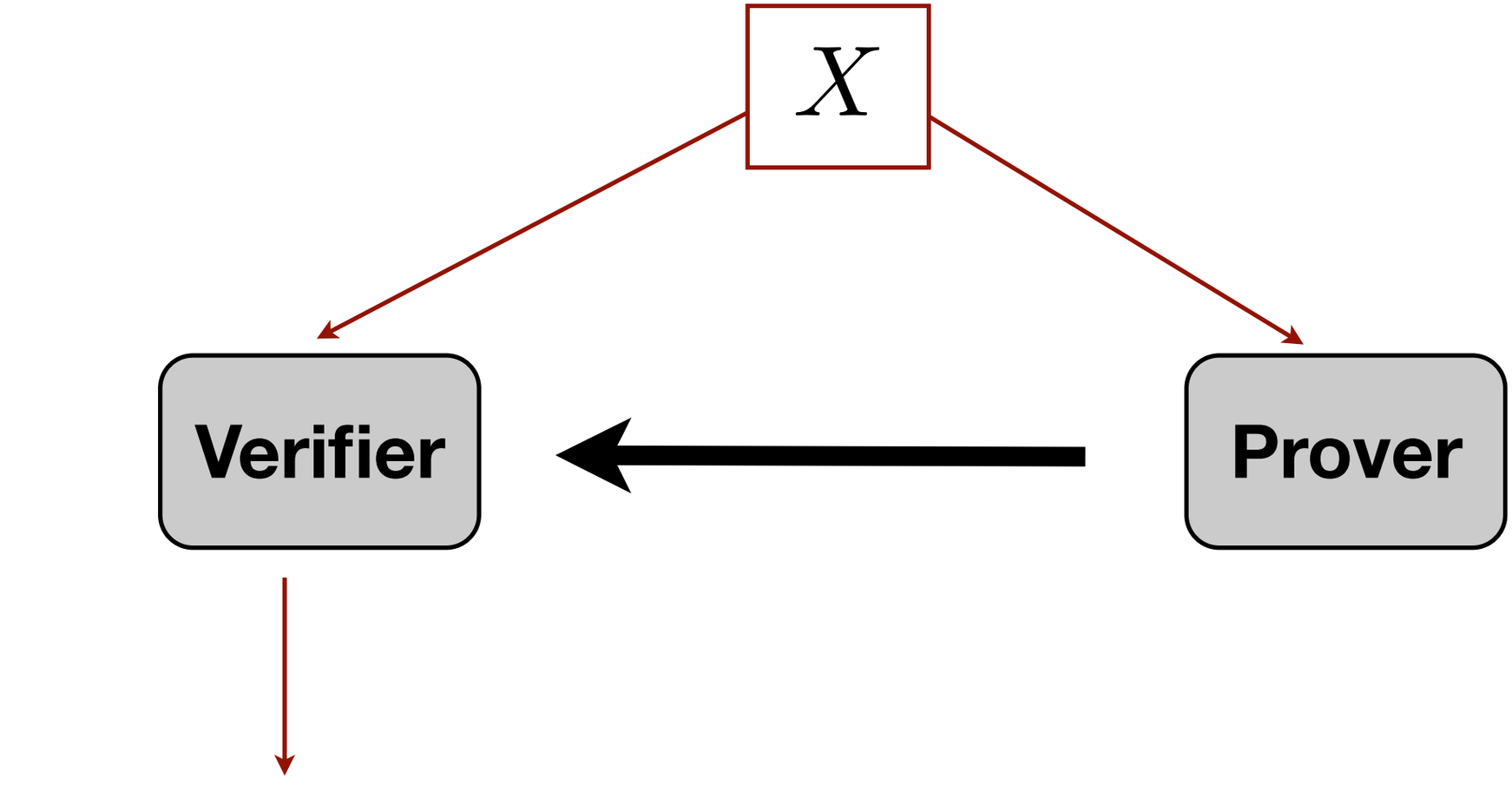
Complexity as Proof System



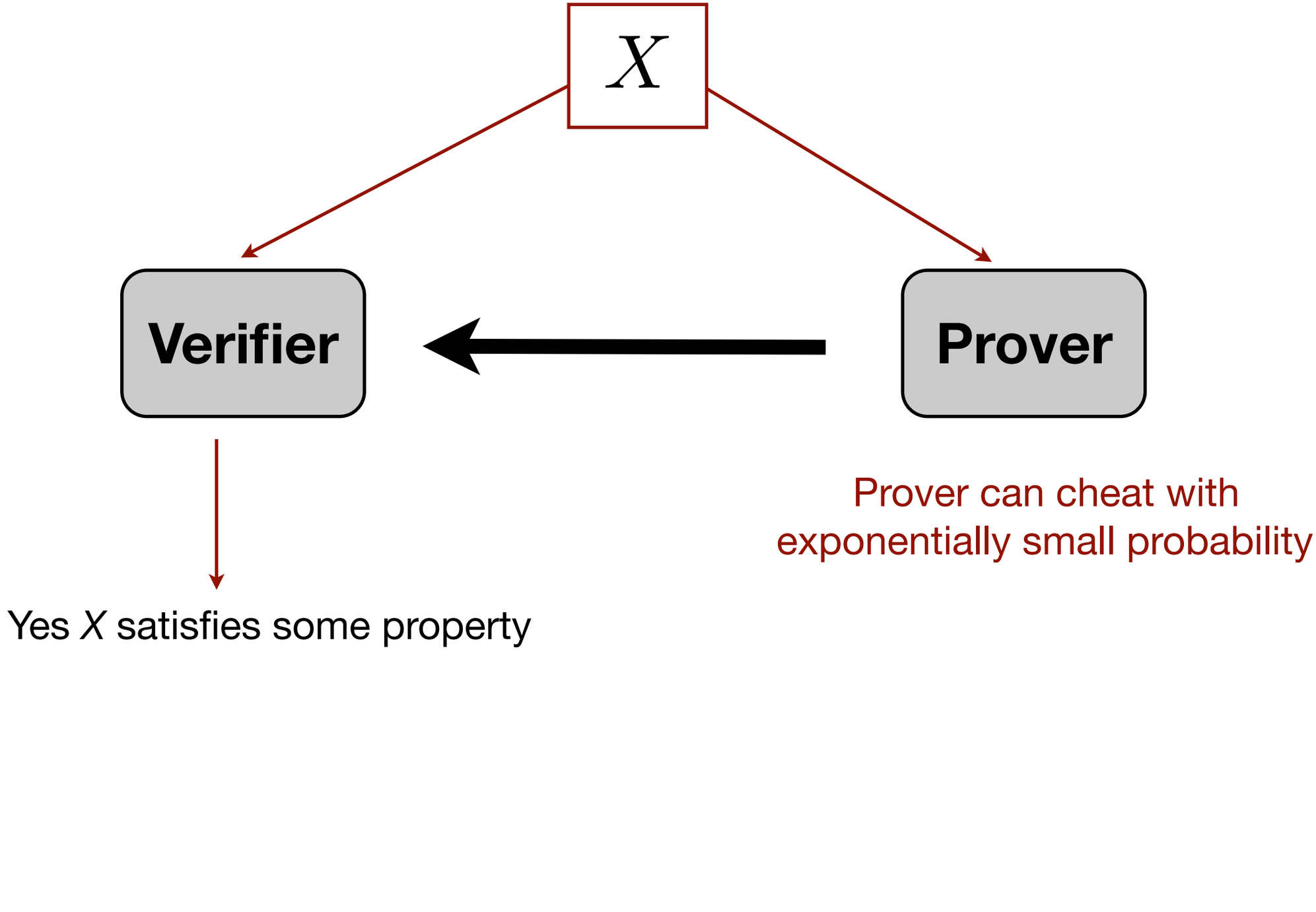
Generalisation: Interactive Proofs



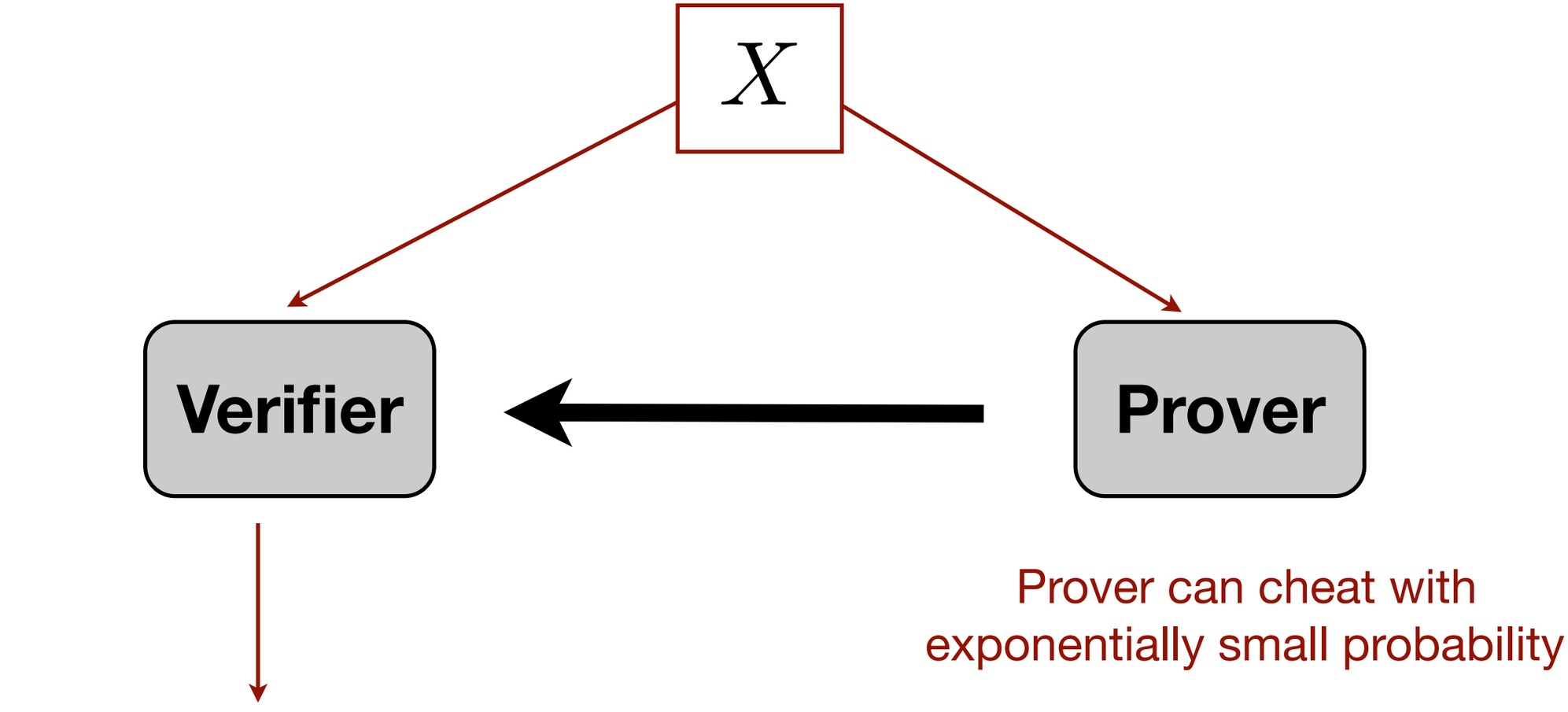
Generalisation: Interactive Proofs



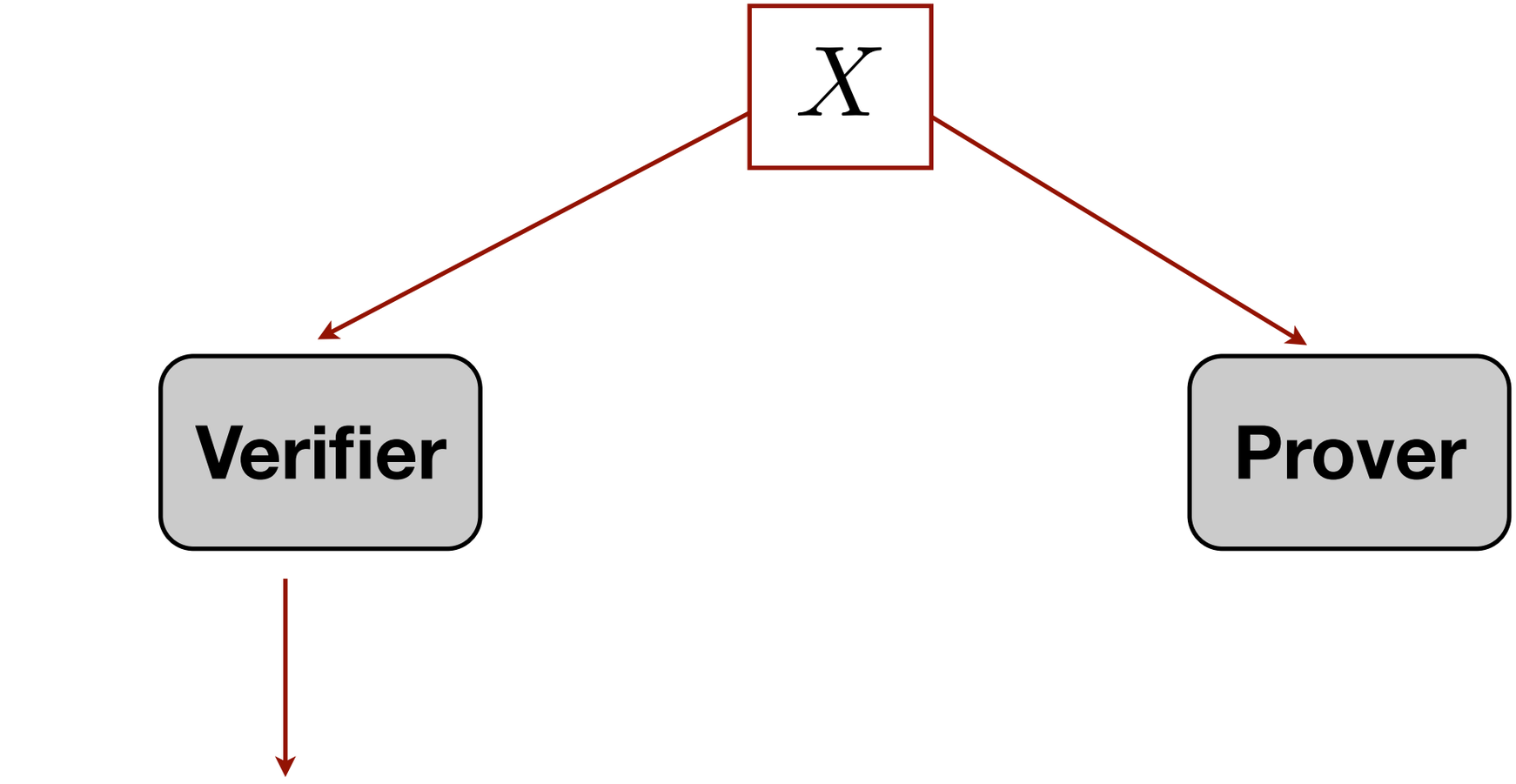
Generalisation: Interactive Proofs



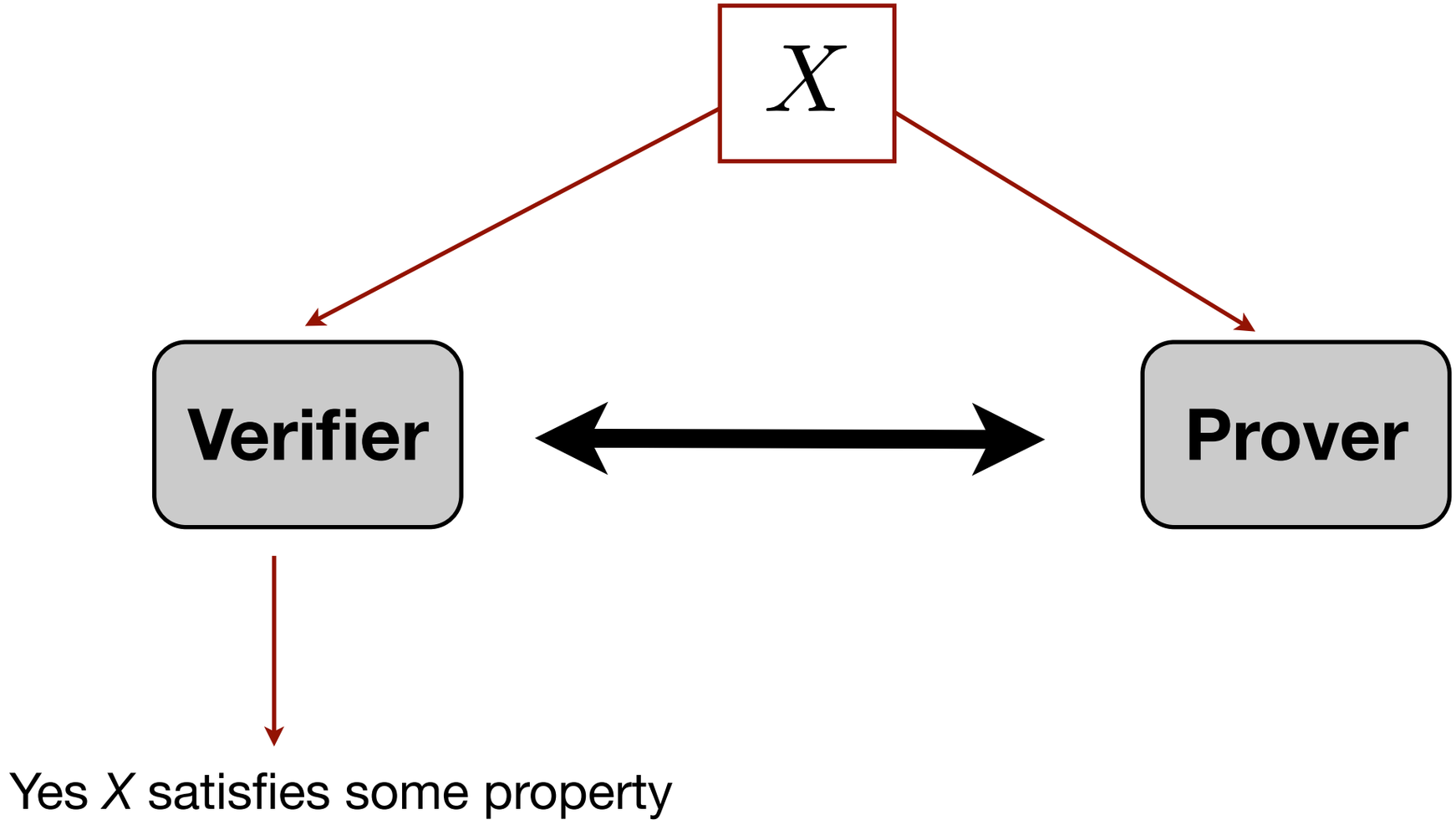
Generalisation: Interactive Proofs



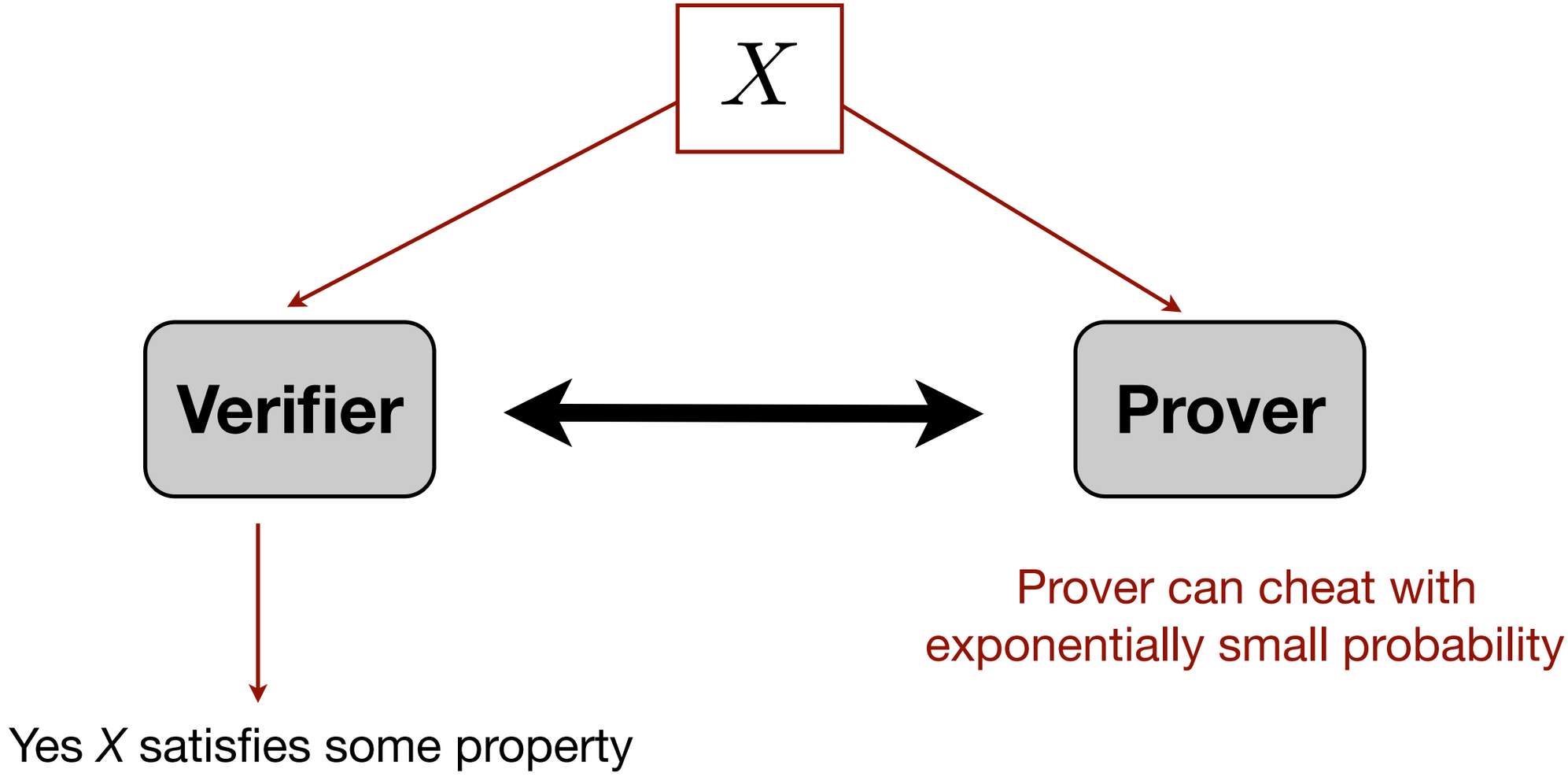
Generalisation: Interactive Proofs



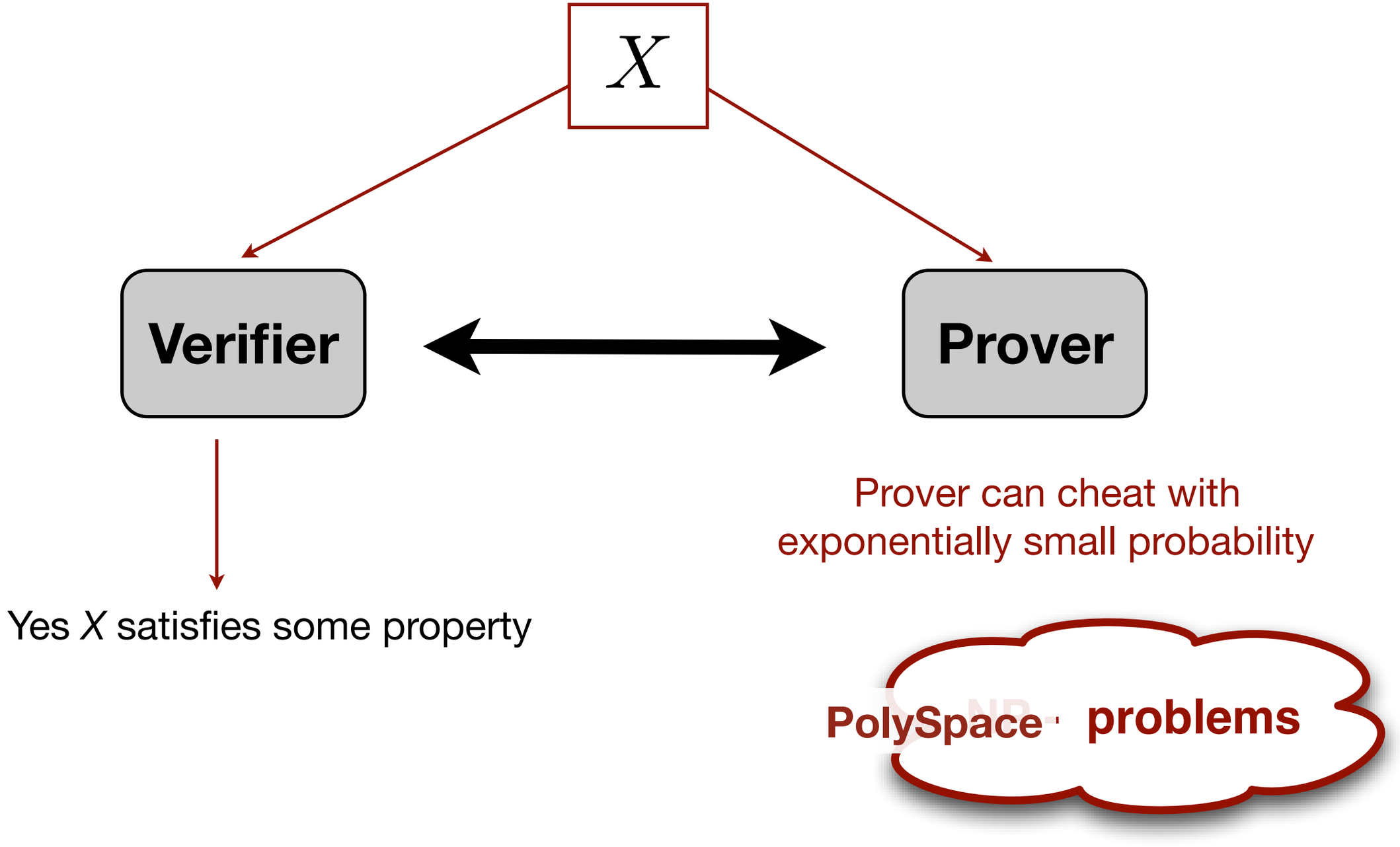
Generalisation: Interactive Proofs



Generalisation: Interactive Proofs



Generalisation: Interactive Proofs



Interactive Proofs

A **PROTOCOL** between a

computationally unrestricted prover P
and
a probabilistic polynomial-time verifier V

Interactive Proofs

A **PROTOCOL** between a

computationally unrestricted prover P
and
a probabilistic polynomial-time verifier V

Completeness: $(\forall x \in L)\ \ \Pr\left[(V \leftrightarrow P)(x)\ \ accepts\right] = 1$

Interactive Proofs

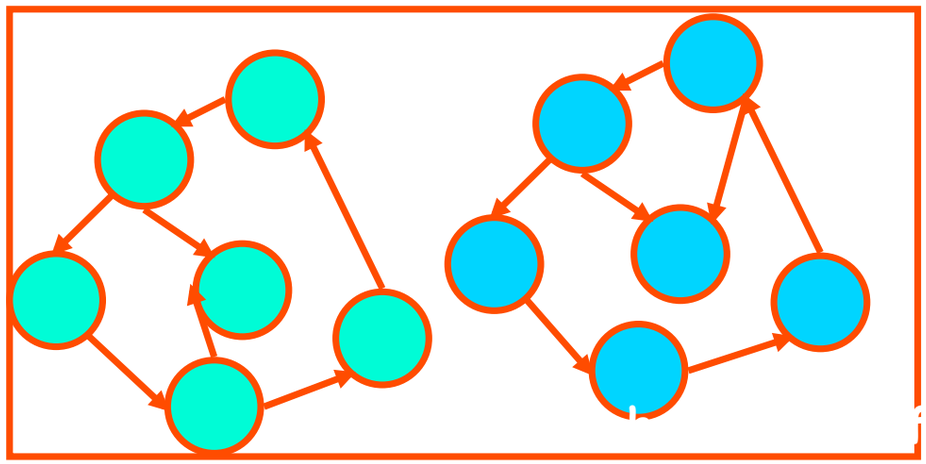
A **PROTOCOL** between a

computationally unrestricted prover P
and
a probabilistic polynomial-time verifier V

Completeness: $(\forall x \in L)\ \ \Pr\left[(V \leftrightarrow P)(x)\ \ accepts\right] = 1$

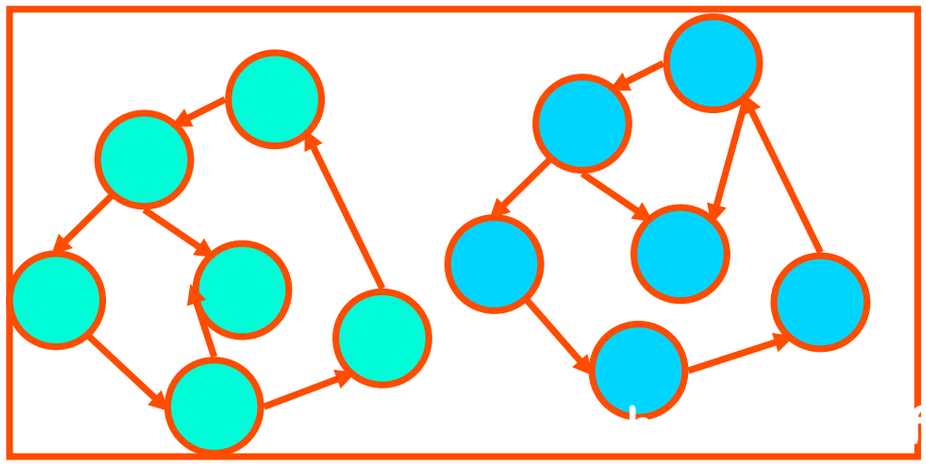
Soundness: $(\forall x \notin L)(\forall P')\ \ \Pr\left[(V \leftrightarrow P')(x)\ \ accepts\right] \leq \frac{1}{2}$

Graph Non-Isomorphism



The common input

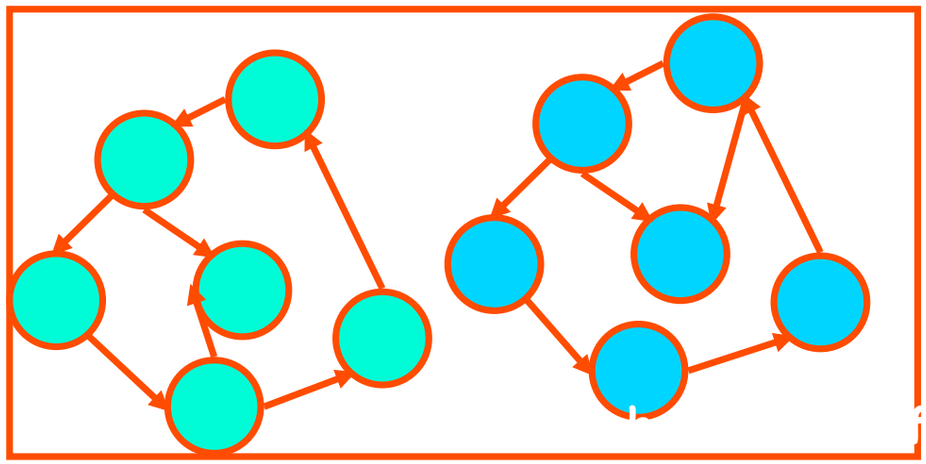
Graph Non-Isomorphism



The common input

Verifier chooses one of the two graphs randomly

Graph Non-Isomorphism

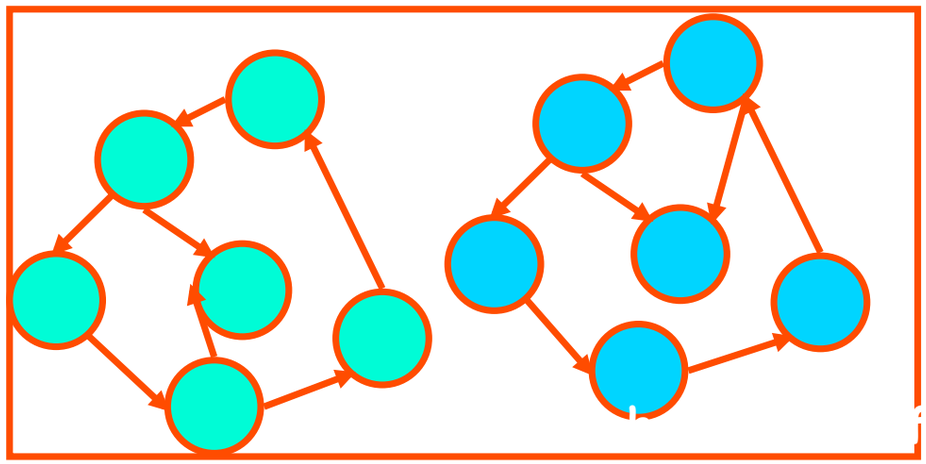


The common input

Verifier chooses one of the two graphs randomly

Verifier constructs a graph isomorphic to her choice and send it to the Prover

Graph Non-Isomorphism



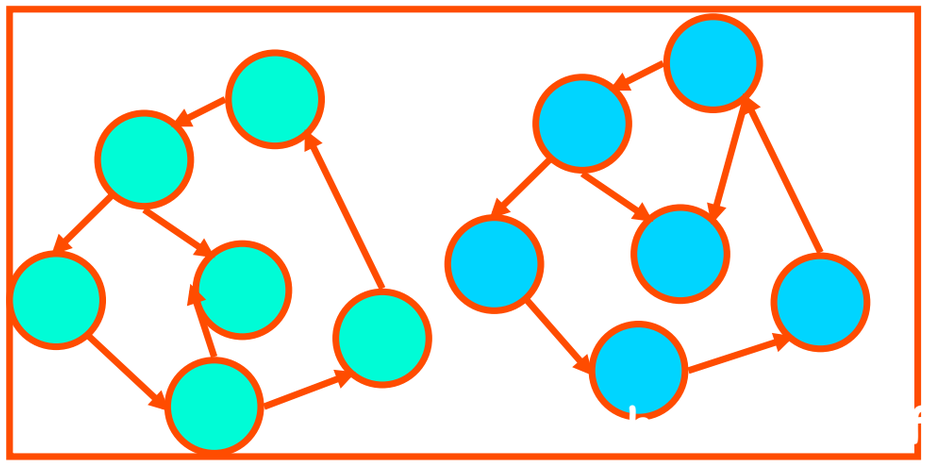
The common input

Verifier chooses one of the two graphs randomly

Verifier constructs a graph isomorphic to her choice and send it to the Prover

If $G \ncong H$ prover can find which of the two graphs was send by the verifier

Graph Non-Isomorphism



The common input

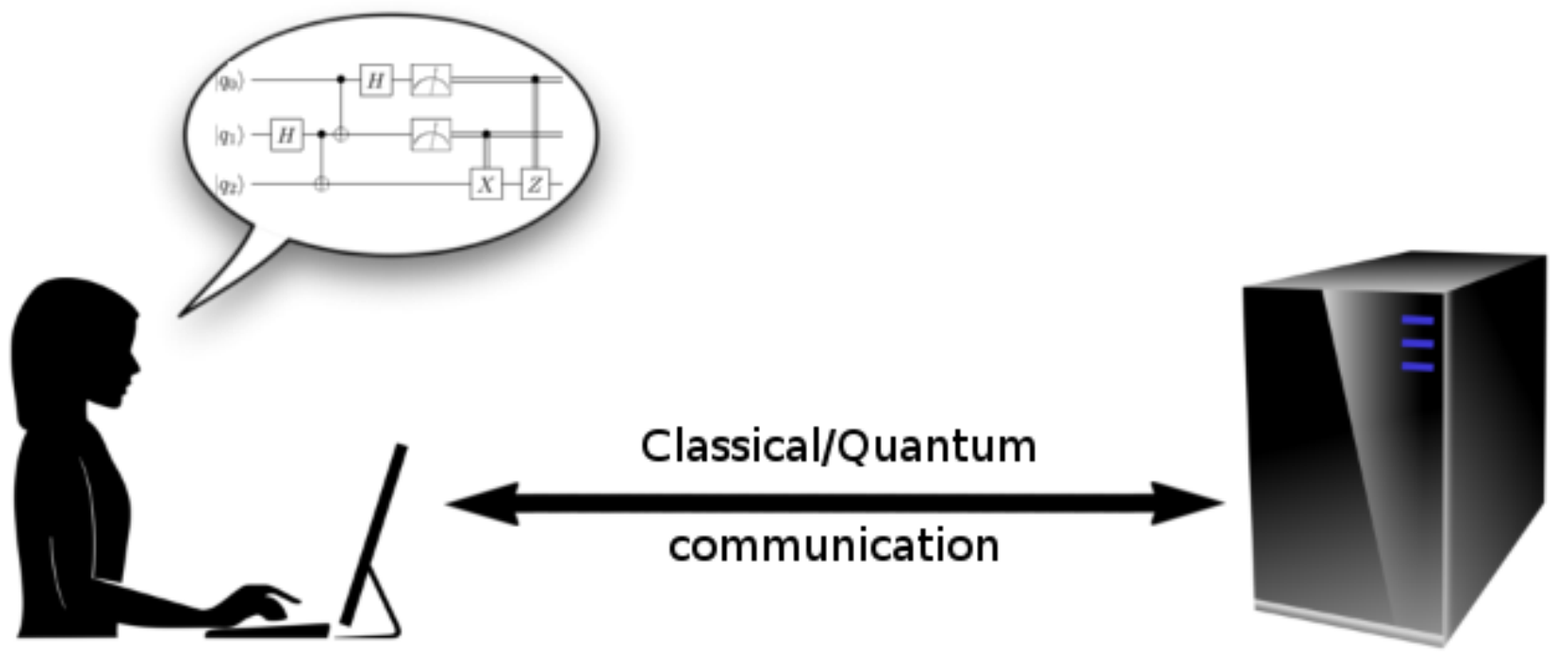
Verifier chooses one of the two graphs randomly

Verifier constructs a graph isomorphic to her choice and send it to the Prover

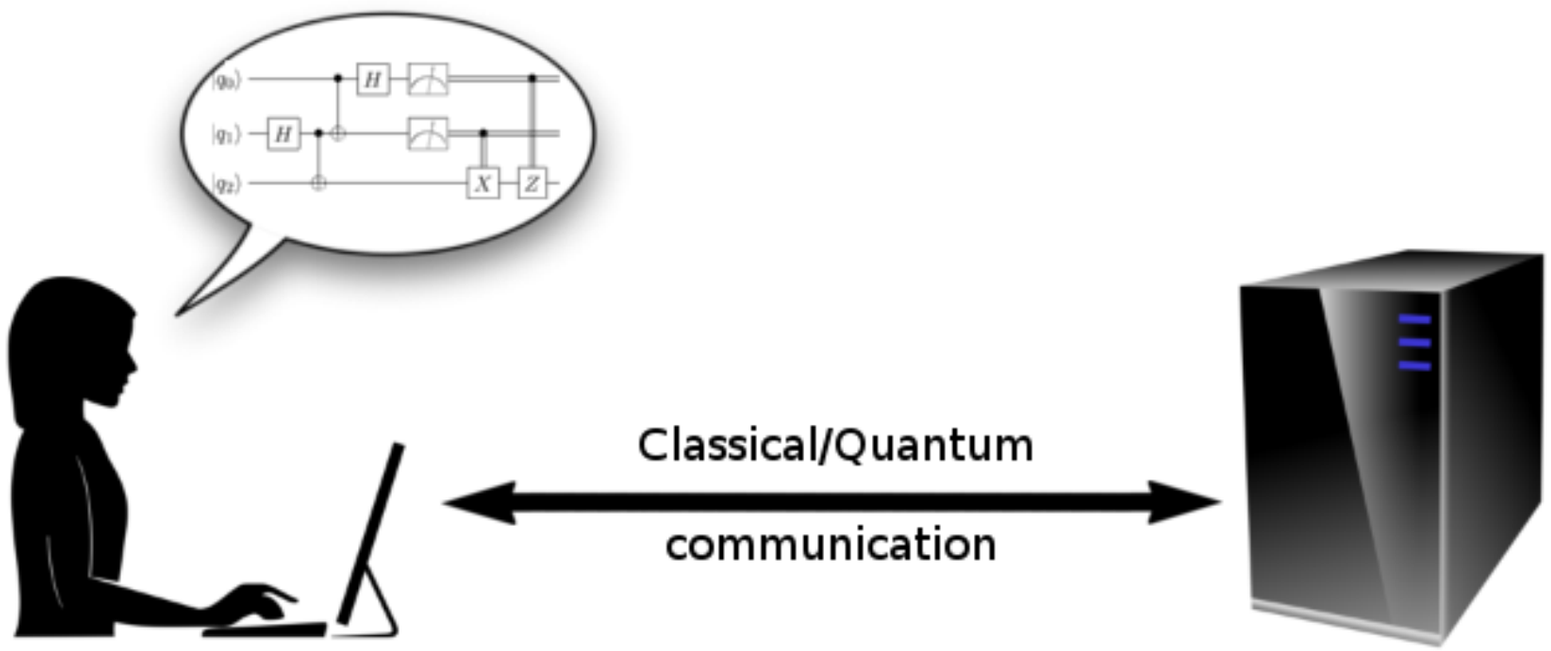
If $G \ncong H$ prover can find which of the two graphs was send by the verifier

The verifier can check the answer easily

Quantum Interactive Proof System

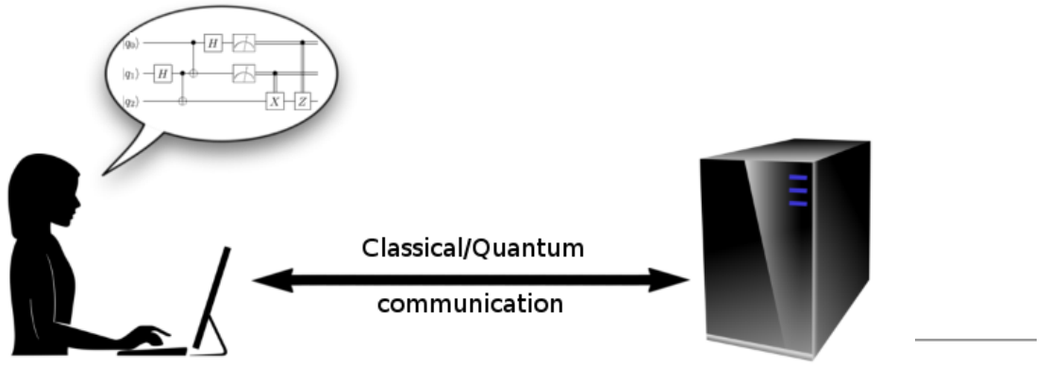


Quantum Interactive Proof System

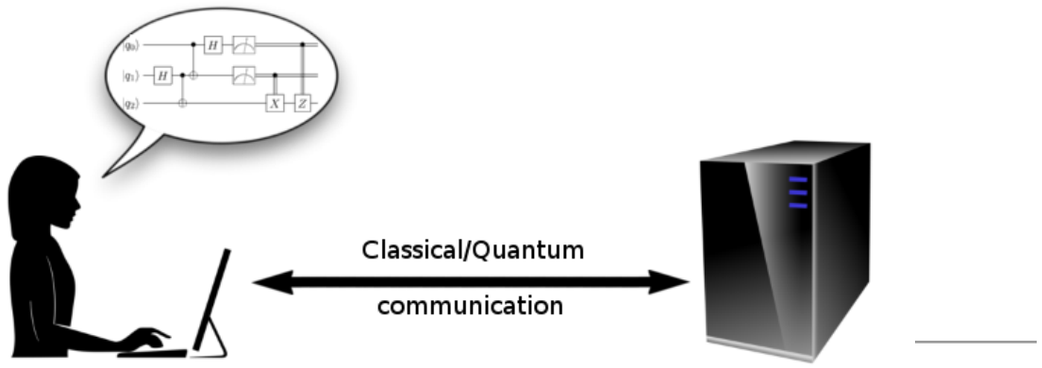


- Computationally limited verifier
- Powerful quantum server(s)
- Certify the correctness of the computation

Interactive Proof System



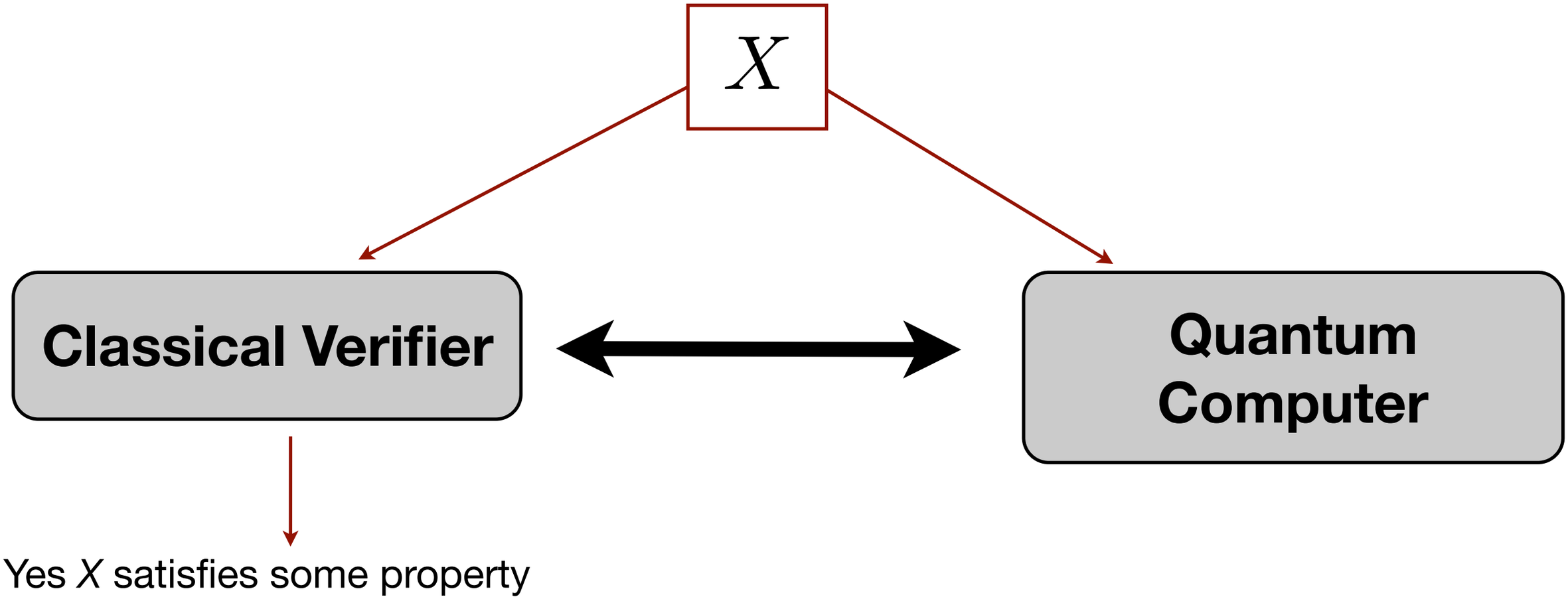
Interactive Proof System



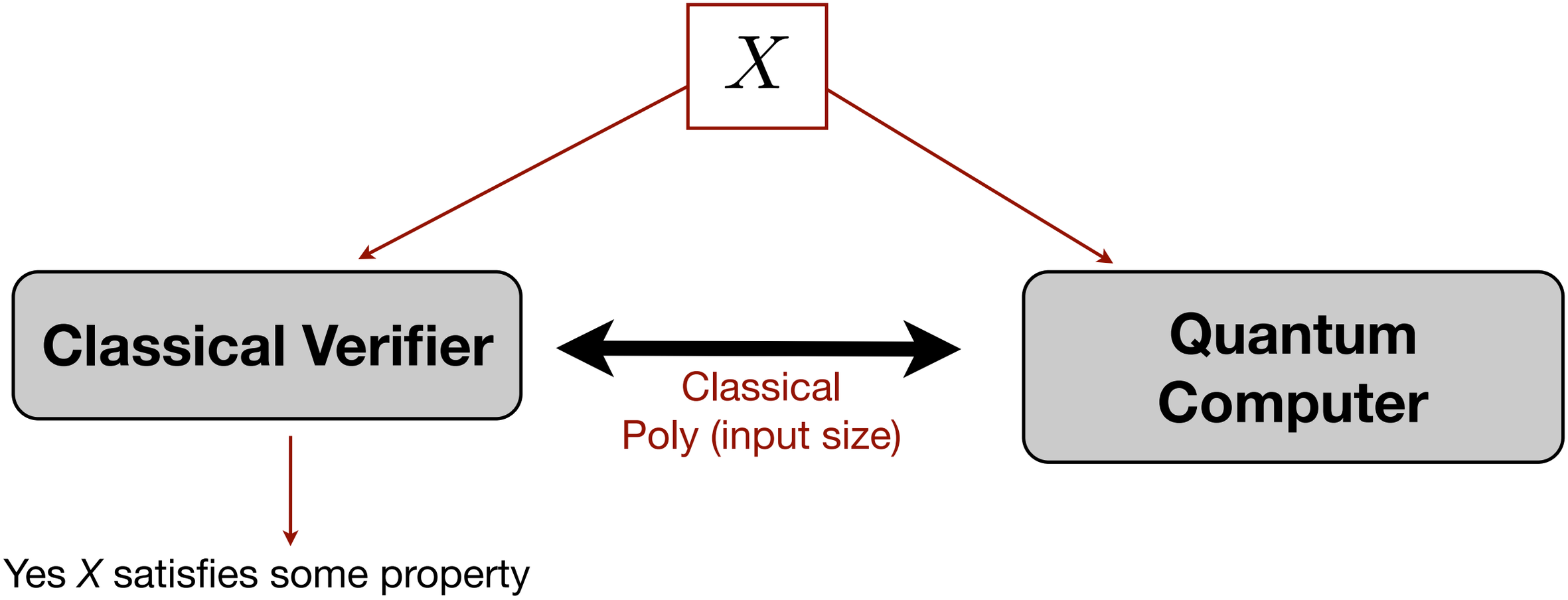
- Correctness: in the absence of any interference, verifier accepts and the output is correct

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

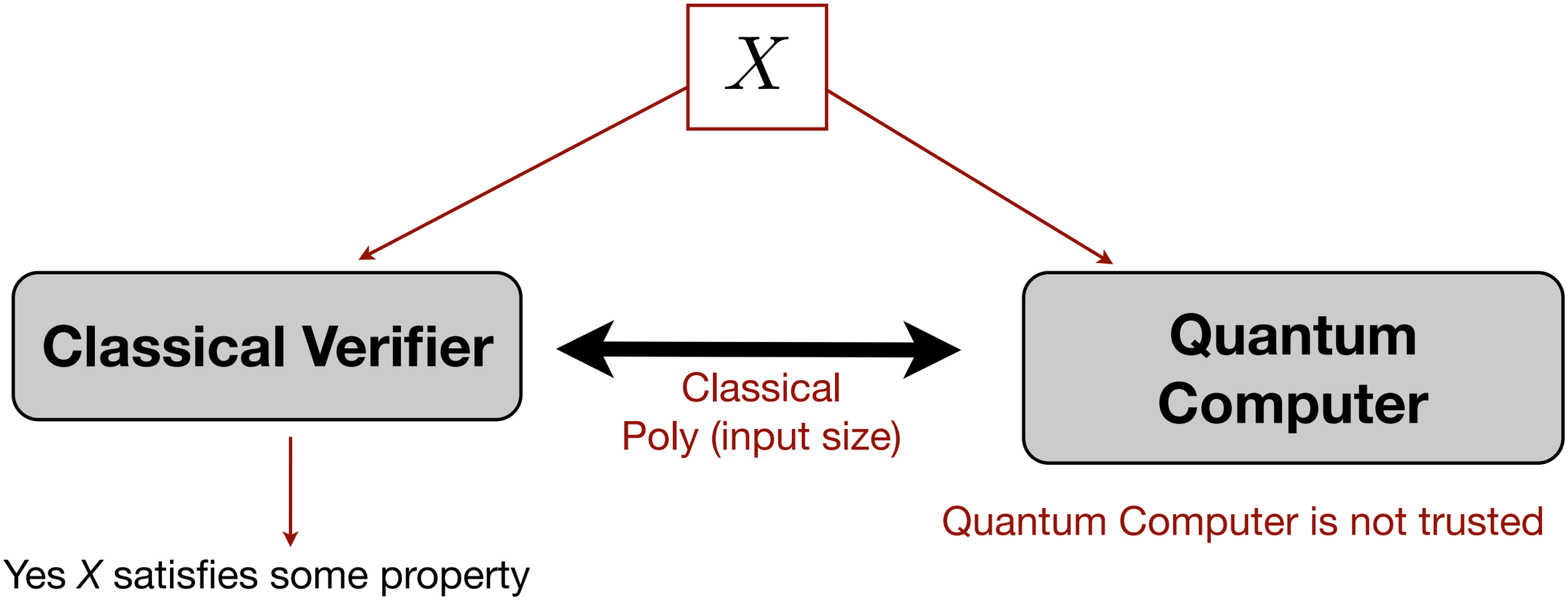
IP for Quantum Computing



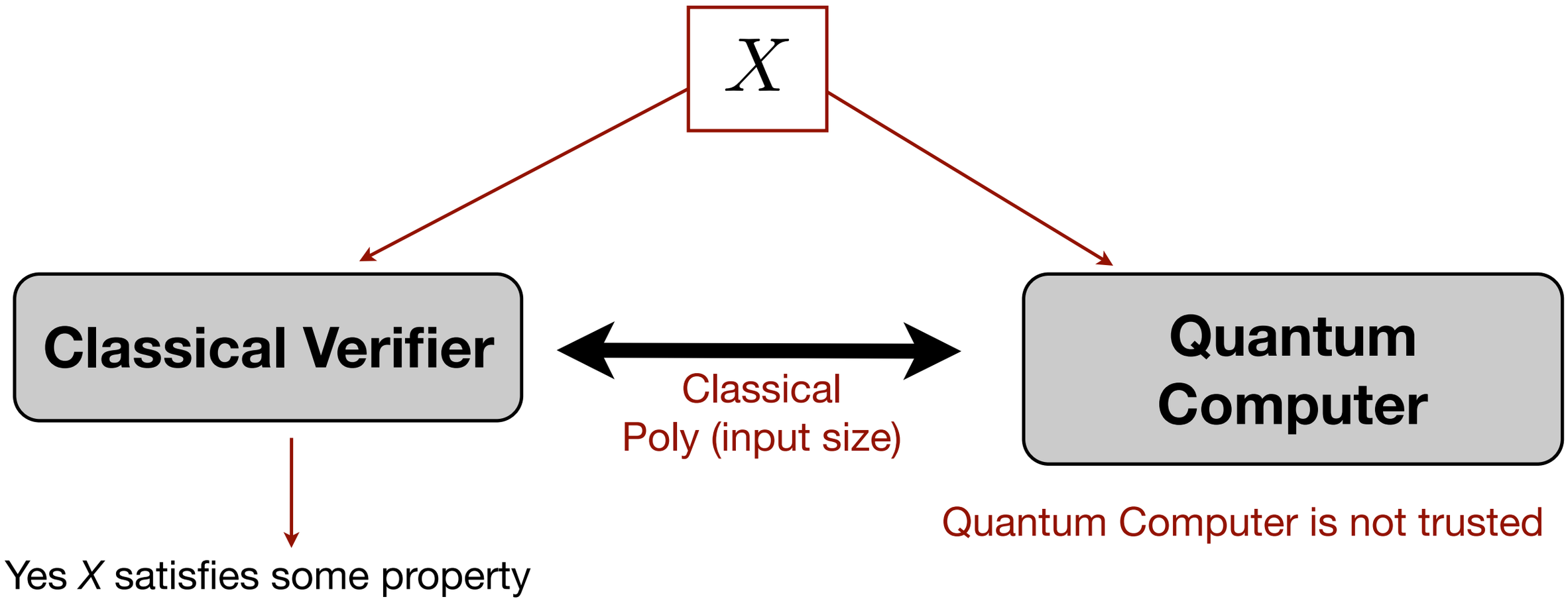
IP for Quantum Computing



IP for Quantum Computing



IP for Quantum Computing

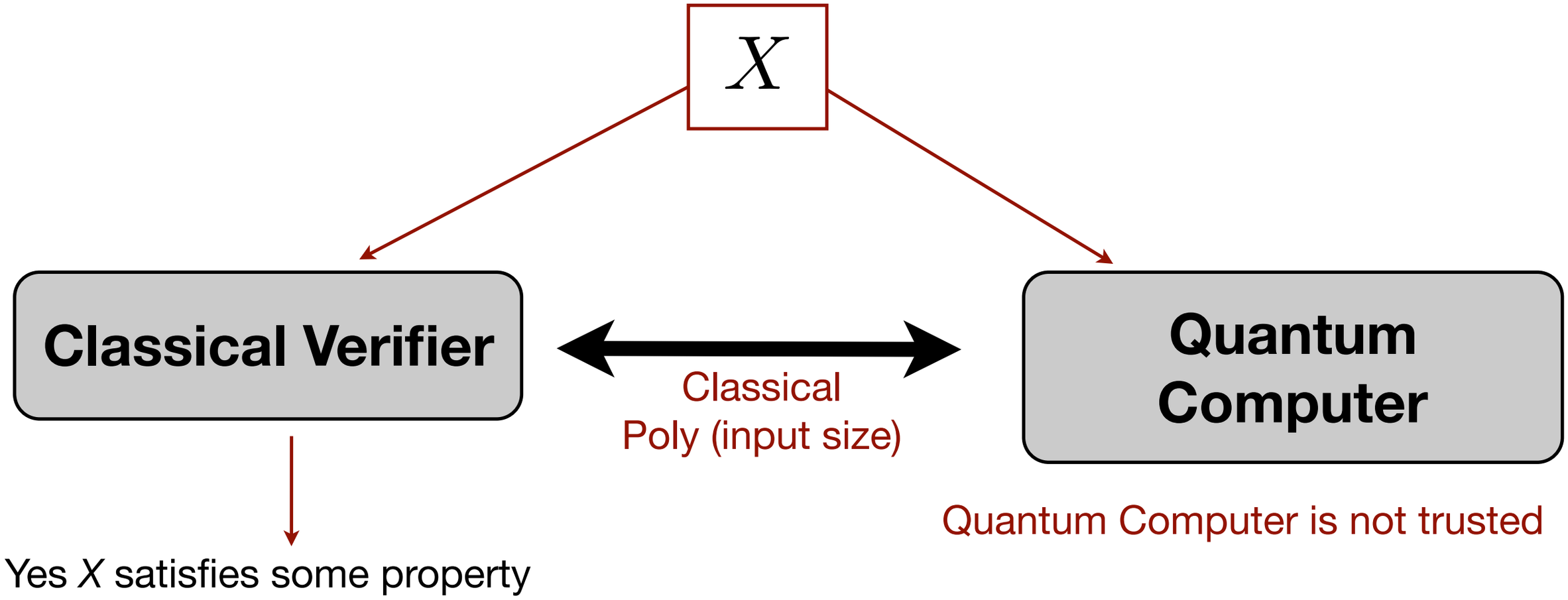


Gottesman (04) - Vazirani (07)- Aaronson ***$25*** *Challenge (07)*

Does BQP admit an interactive protocol

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

IP for Quantum Computing



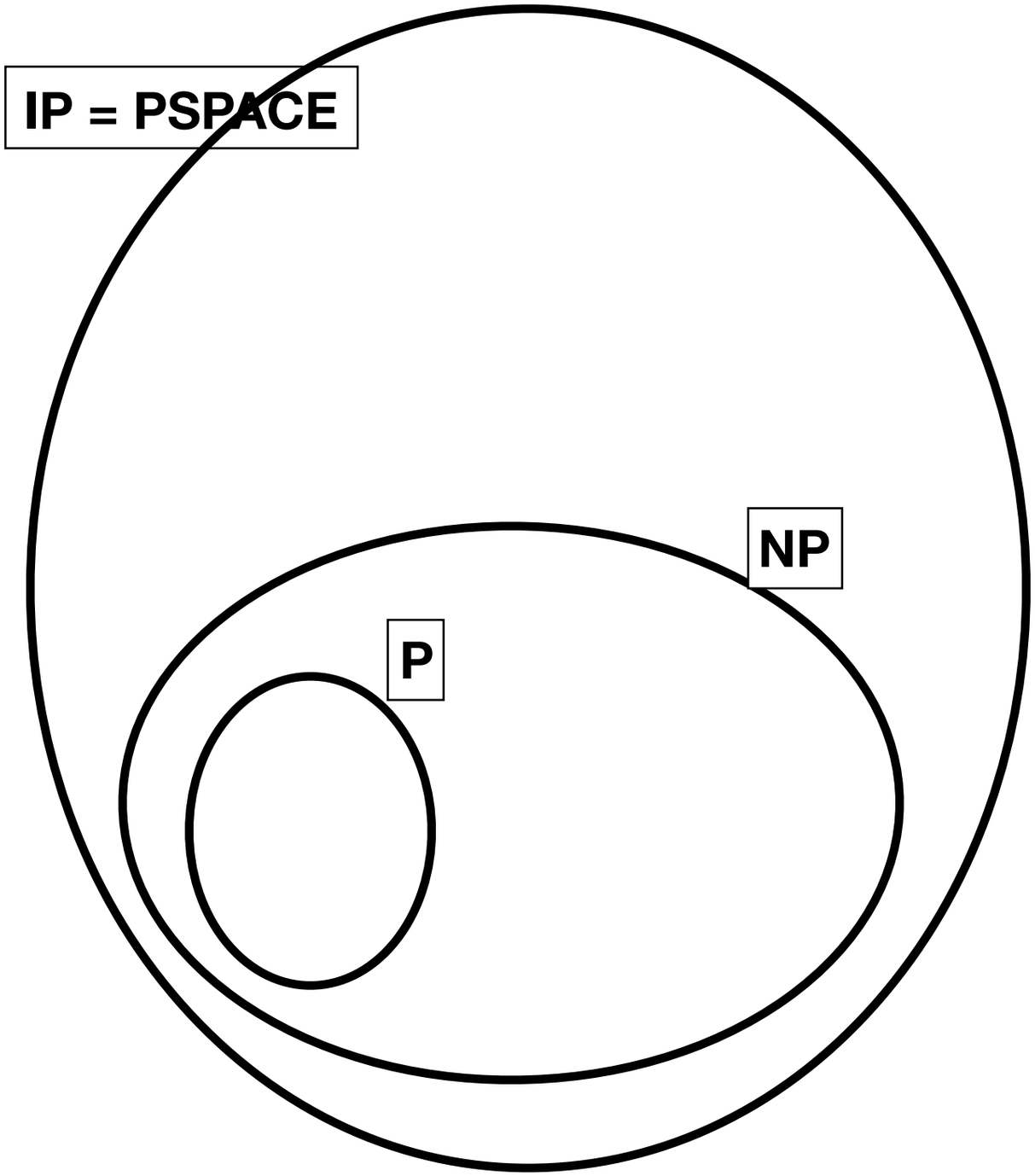
Gottesman (04) - Vazirani (07)- Aaronson ***$25*** *Challenge (07)*

Does BQP admit an interactive protocol

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

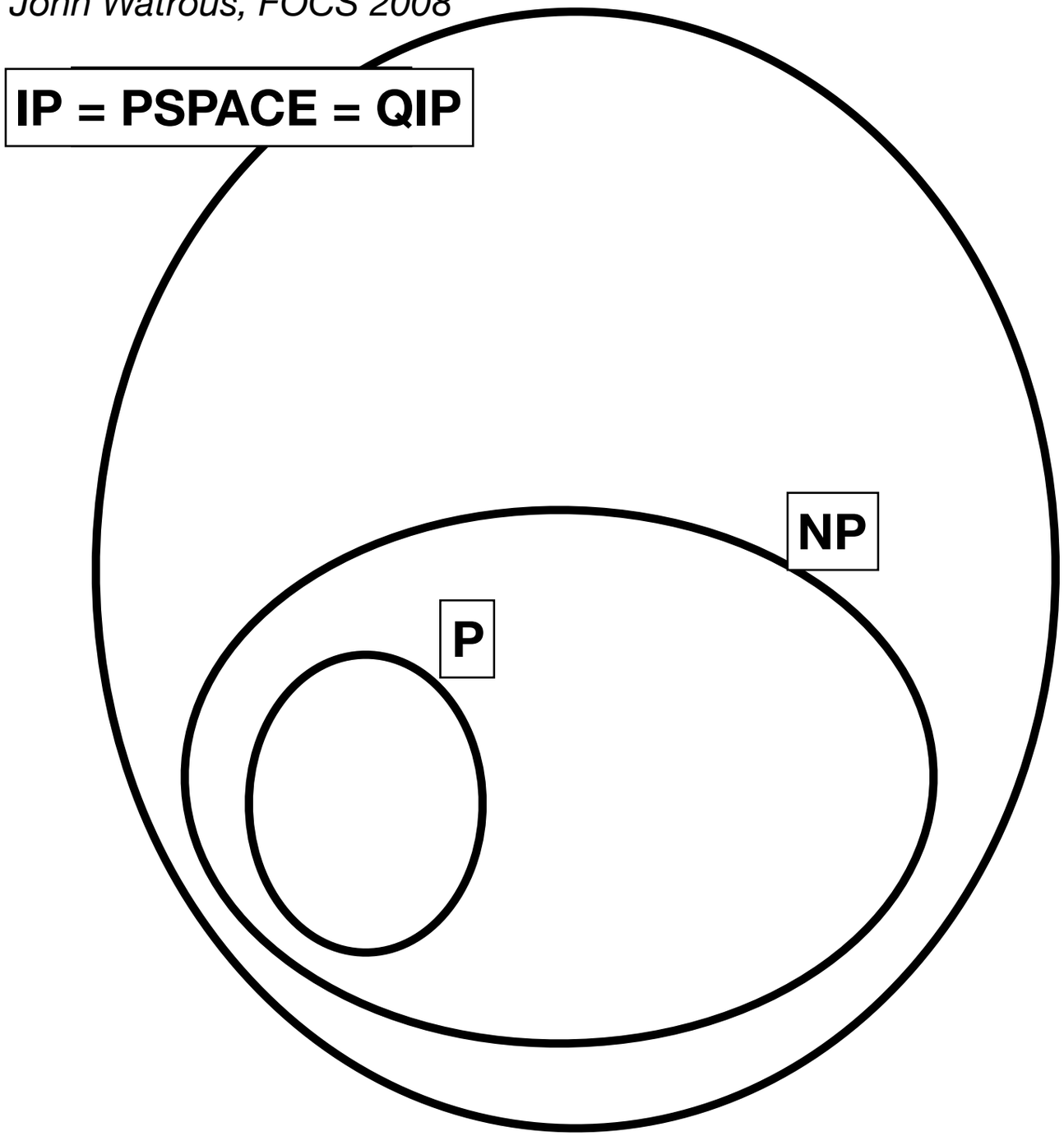
D. Aharonov and U. Vazirani, arXiv:1206.3686 (2012).

IP for Quantum Prover



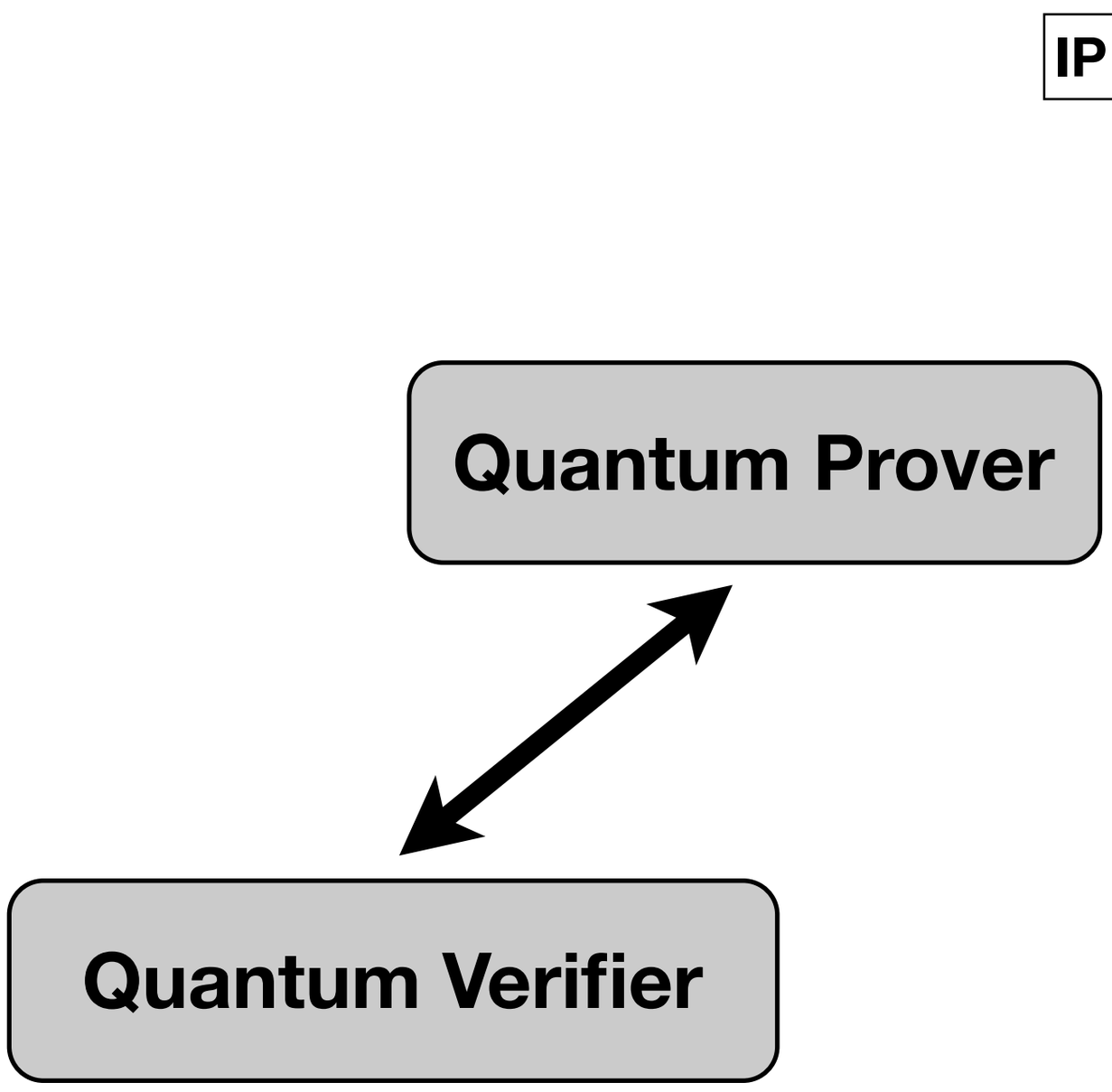
IP for Quantum Prover

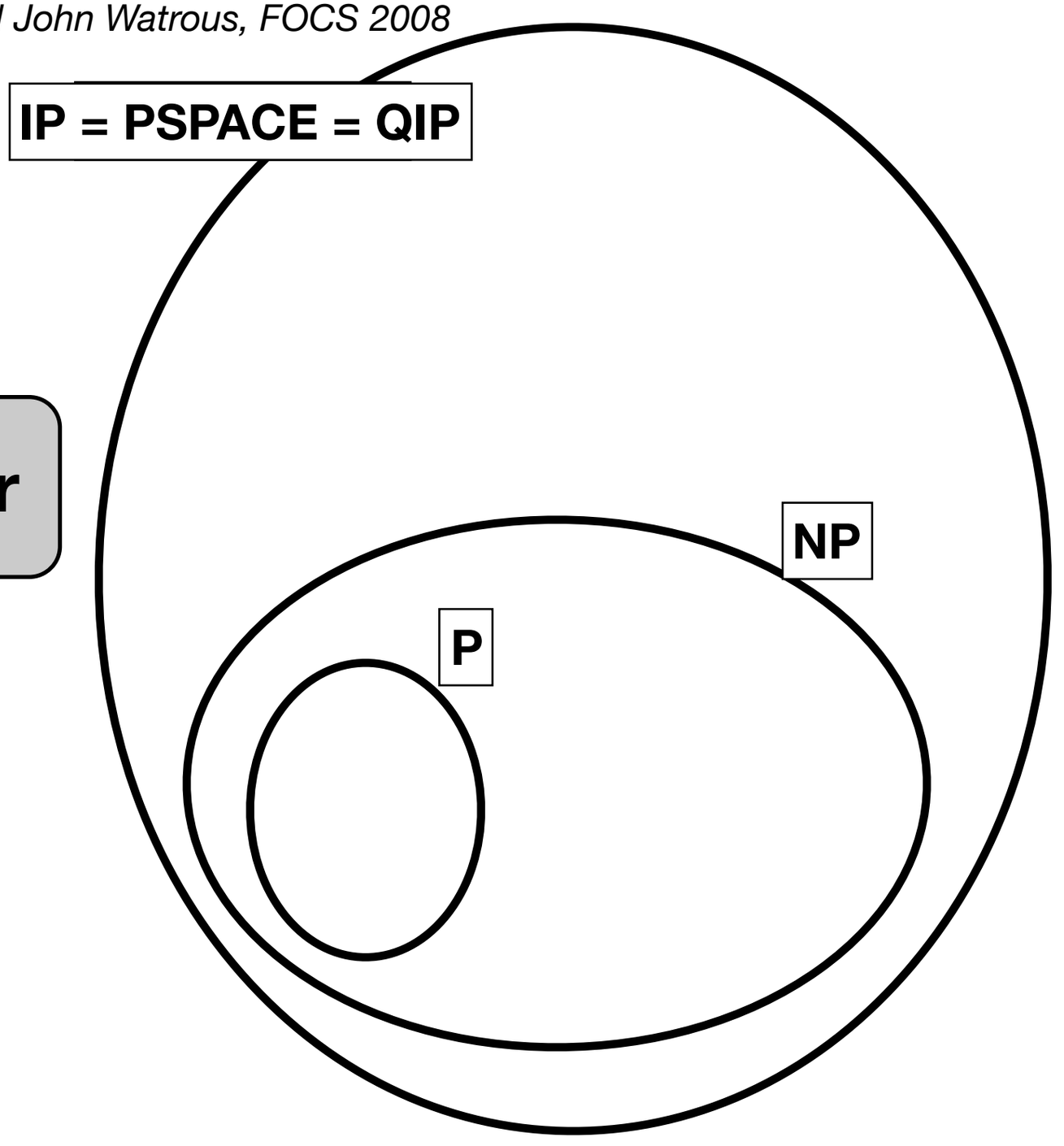
Rahul Jain, Zhengfeng Ji, Sarvagya Upadhyay, and John Watrous, FOCS 2008



IP for Quantum Prover

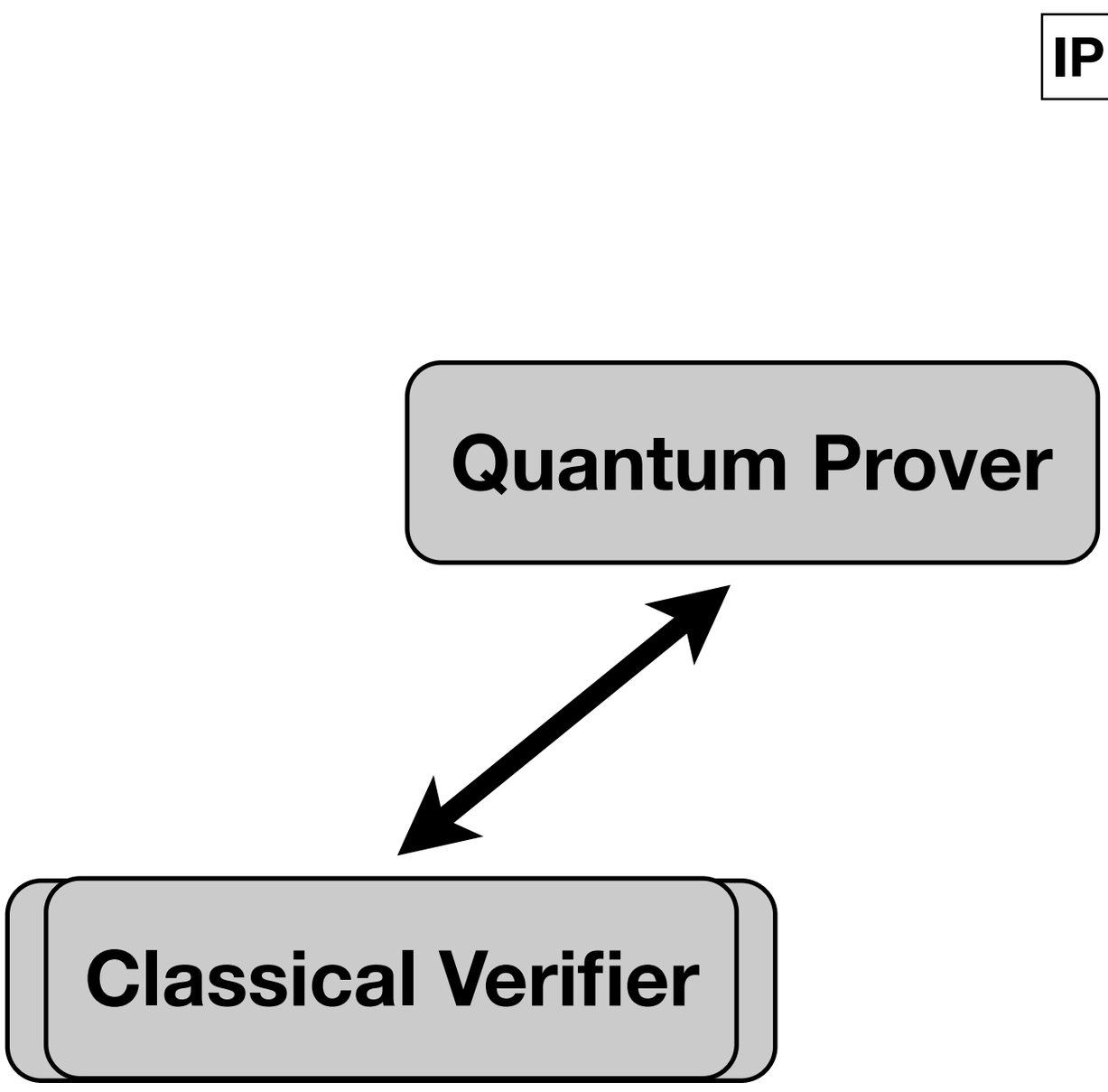
Rahul Jain, Zhengfeng Ji, Sarvagya Upadhyay, and John Watrous, FOCS 2008

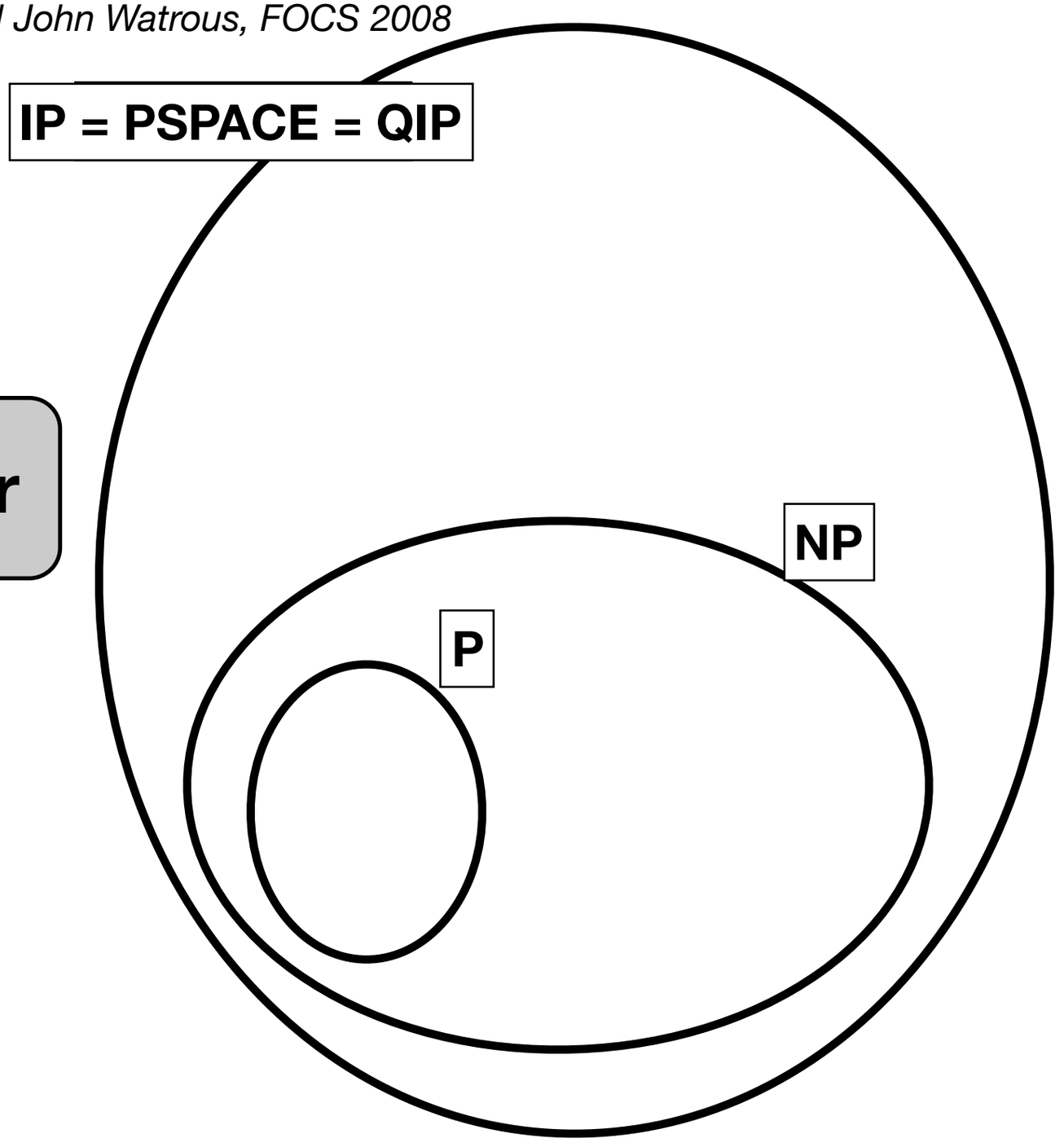




IP for Quantum Prover

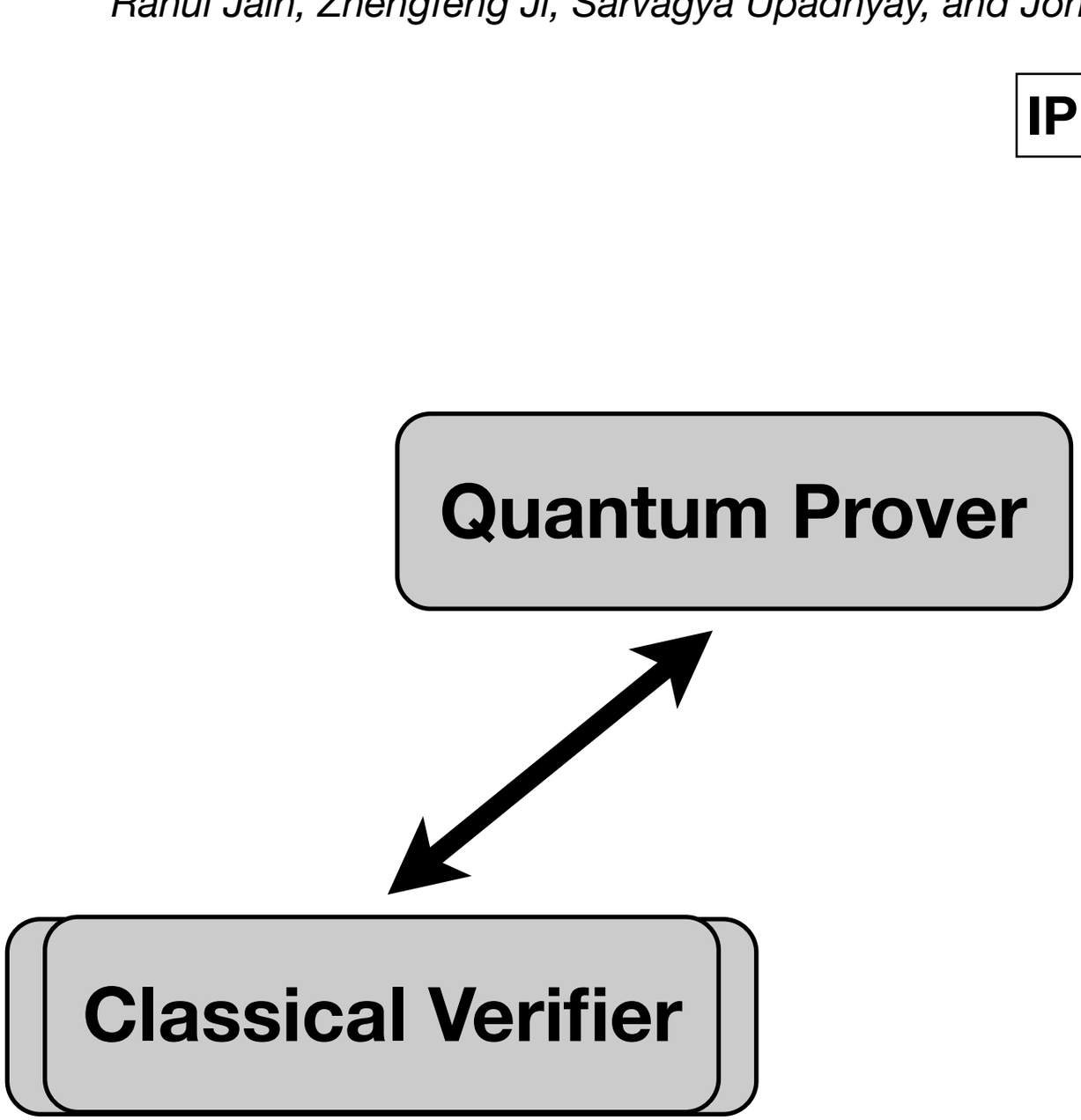
Rahul Jain, Zhengfeng Ji, Sarvagya Upadhyay, and John Watrous, FOCS 2008

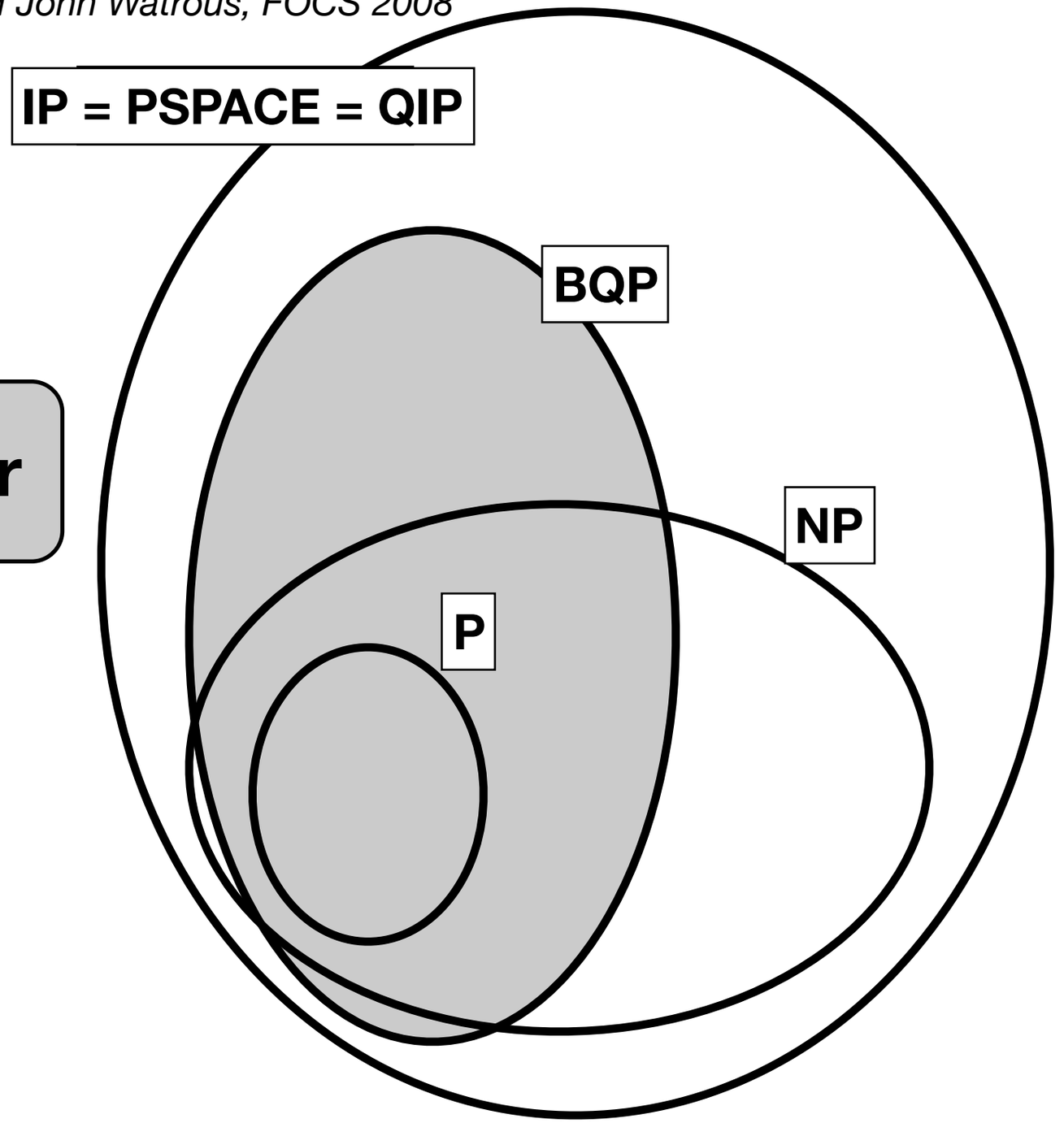




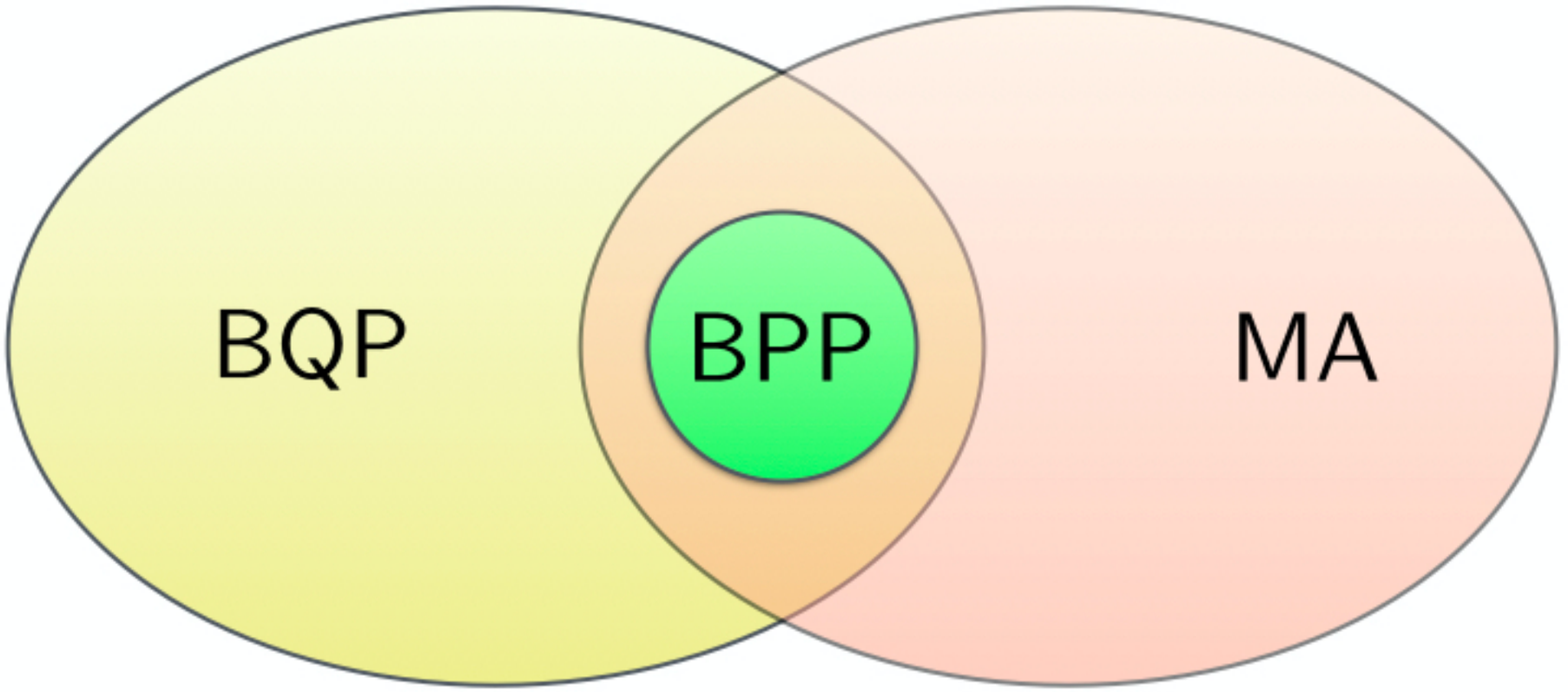
IP for Quantum Prover

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





IP for Quantum Prover



See recent breakthrough result of Mahadev on computationally secure classical verification of BQP (FOCS 2018)

The rest of lecture is focused on informationally secure verification schemes

IP for Quantum Computing

Single-prover prepare-and-send

verifier has the ability to prepare quantum states and send them to the prover

- State authentication-based protocols
- Trapification-based protocols
- Test or Compute

IP for Quantum Computing

Single-prover prepare-and-send

verifier has the ability to prepare quantum states and send them to the prover

- State authentication-based protocols
- Trapification-based protocols
- Test or Compute

Single-prover receive-and-measure

verifier receives quantum states from the prover and has the ability to measure them

- Post-hoc Verification (none hiding)
- Measuring only blind QC

IP for Quantum Computing

Multi-prover entanglement-based

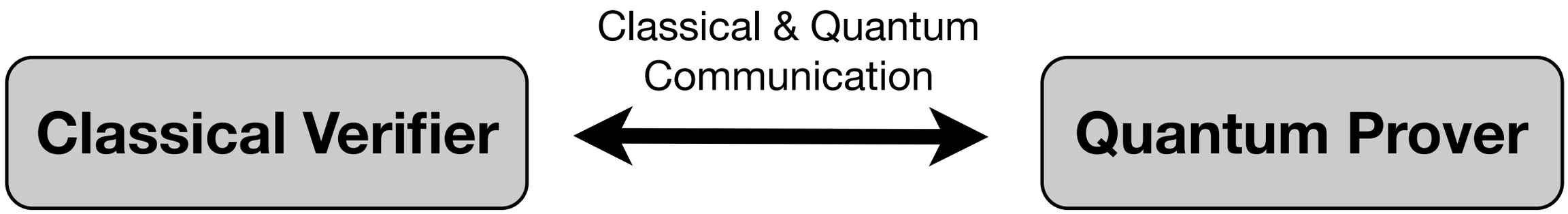
Classical Verifier interacts with more than one provers that are not allowed to communicate during the protocol

- CHSH game Rigidity
- Self-testing graph states
- Pauli Braiding

Single Server Prepare and Send

Semi Classical Verifier

Trapification-based

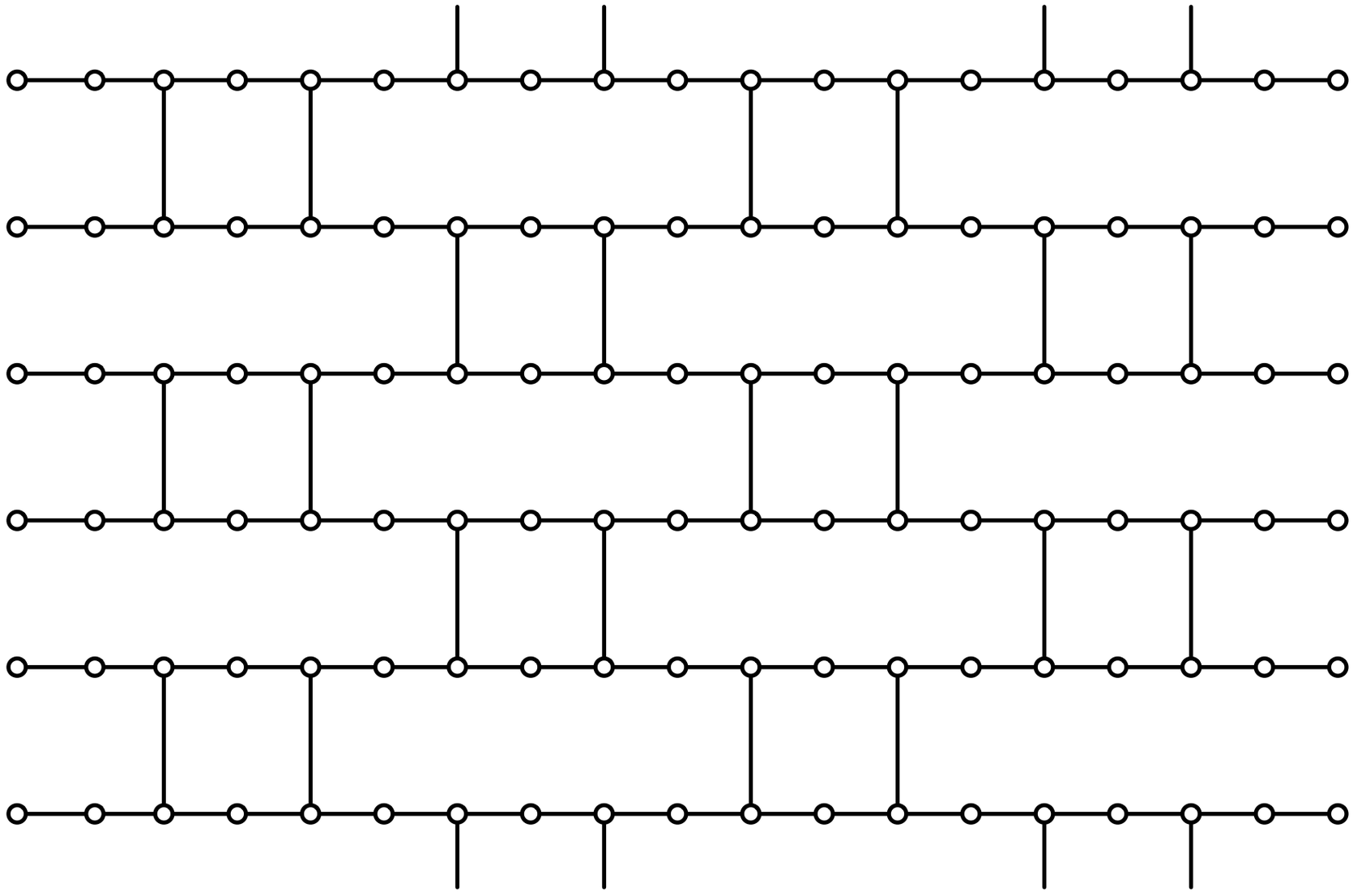


+

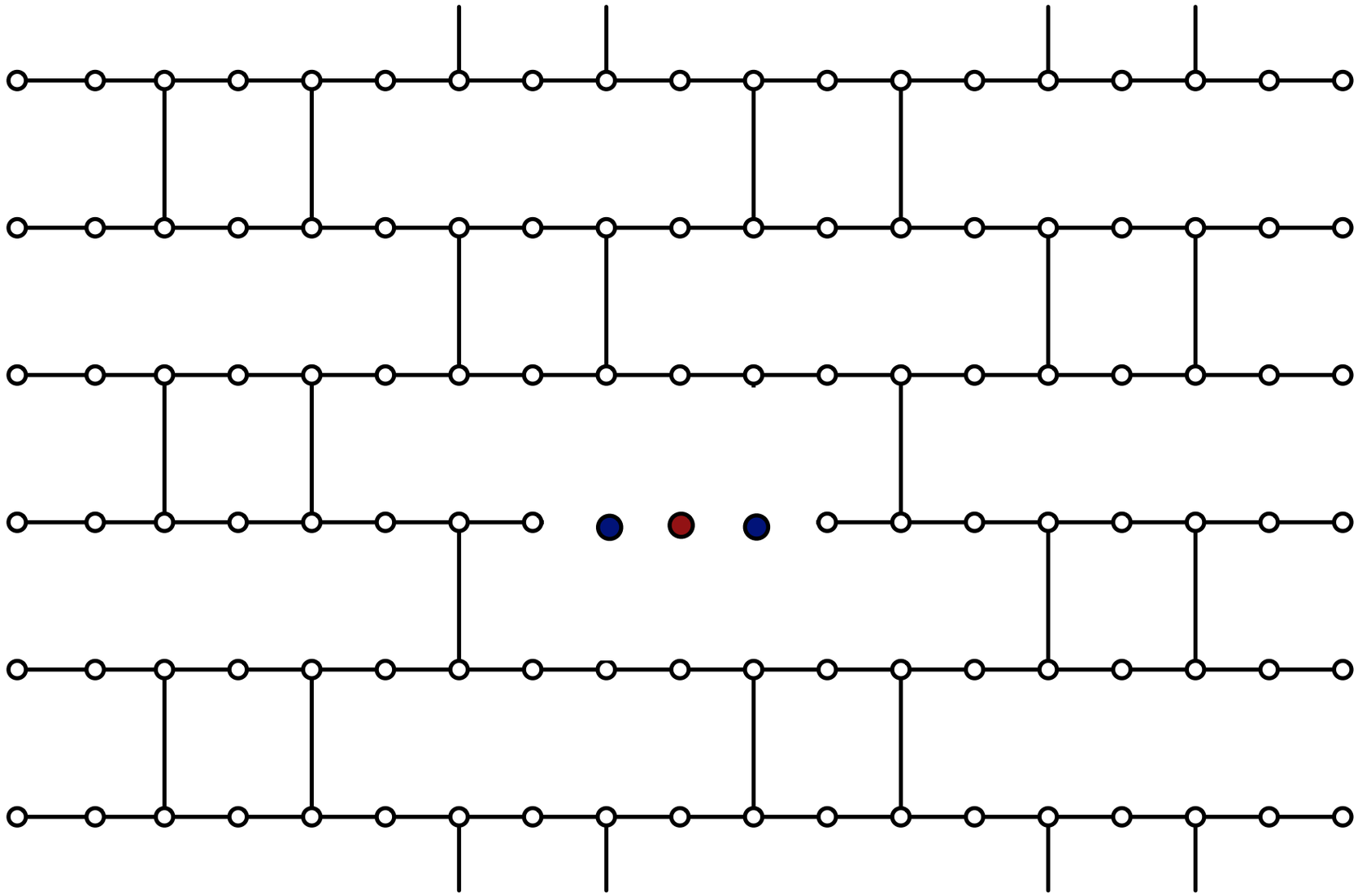
Trusted

random single qubit generator

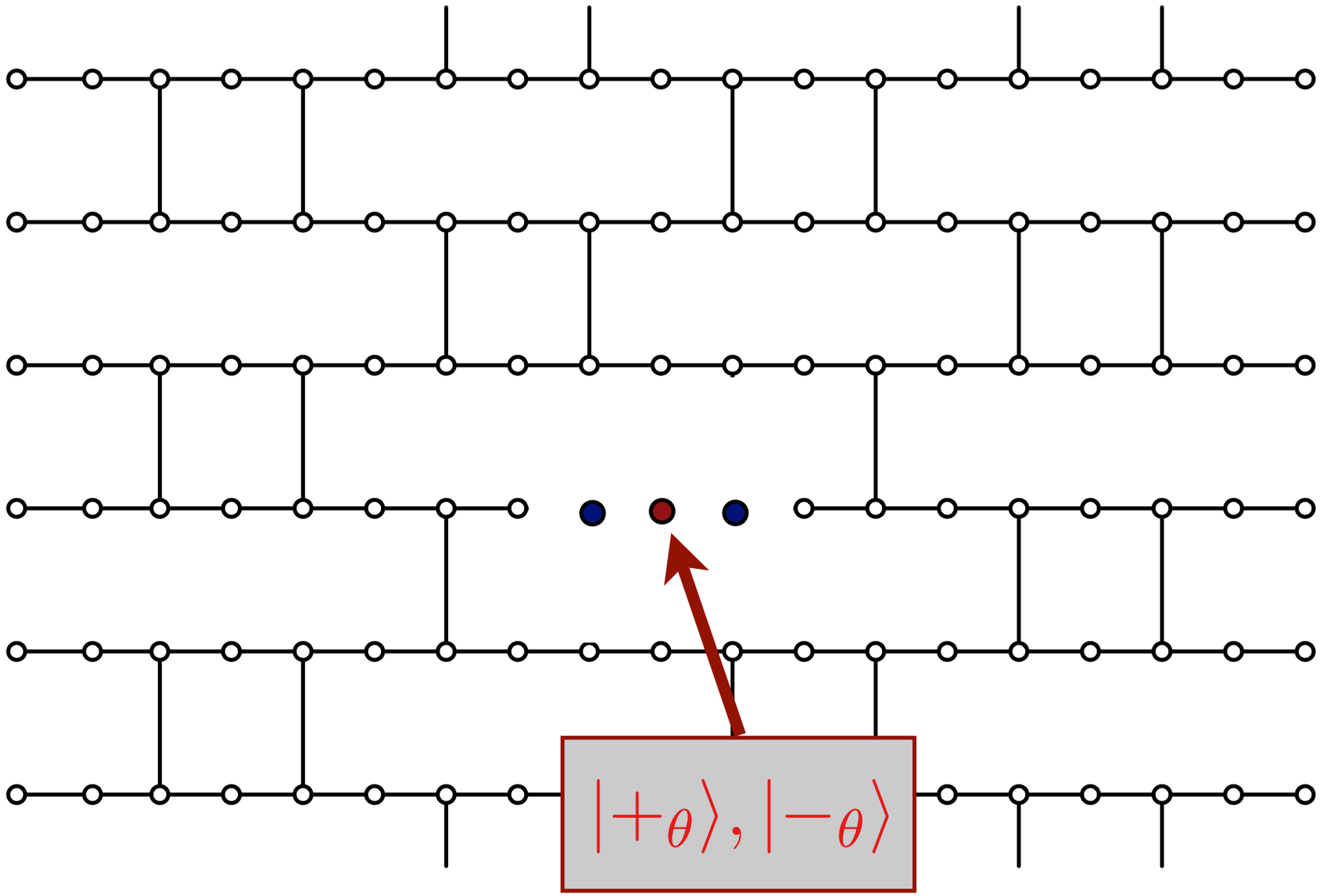
Adding Traps



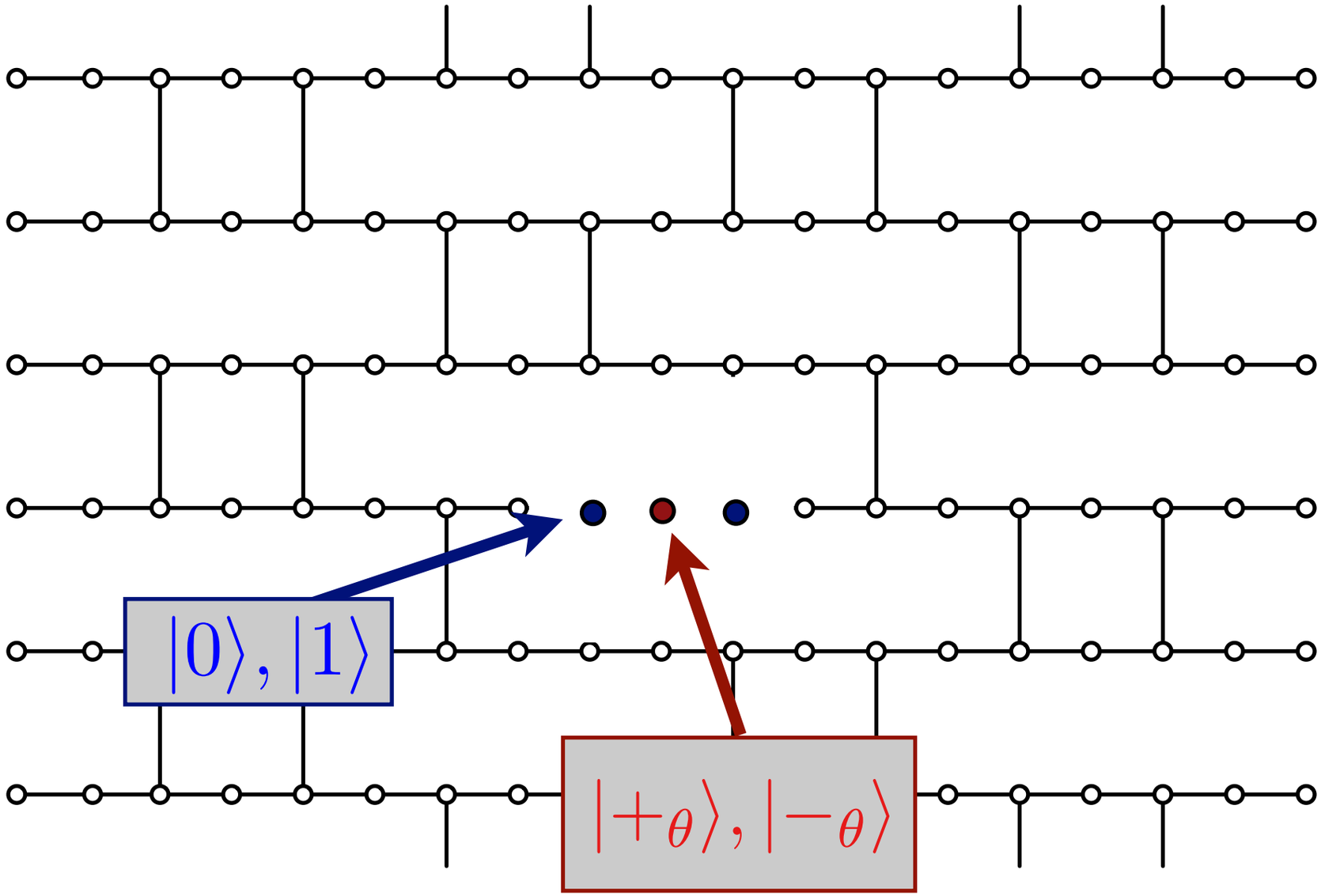
Adding Traps



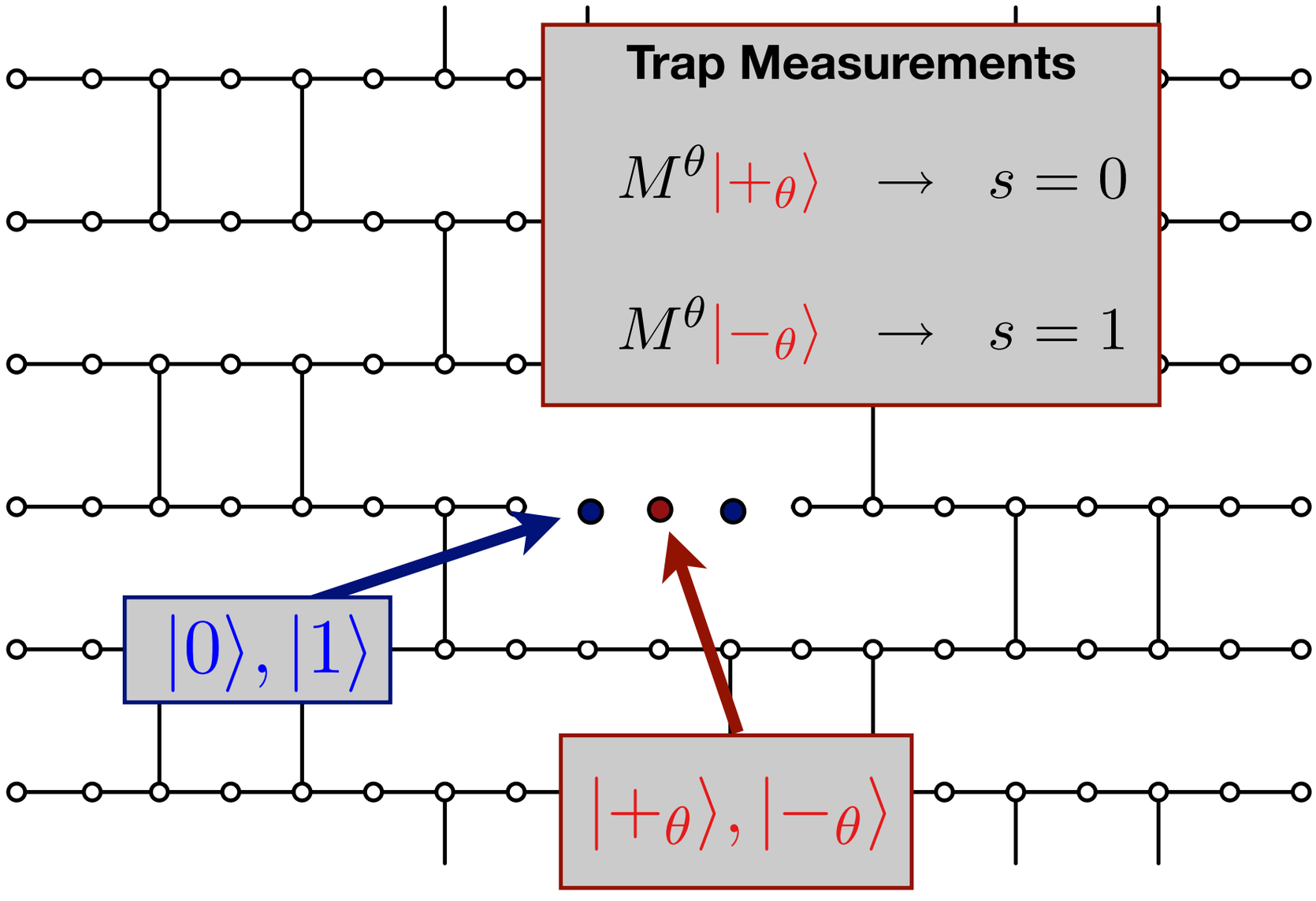
Adding Traps



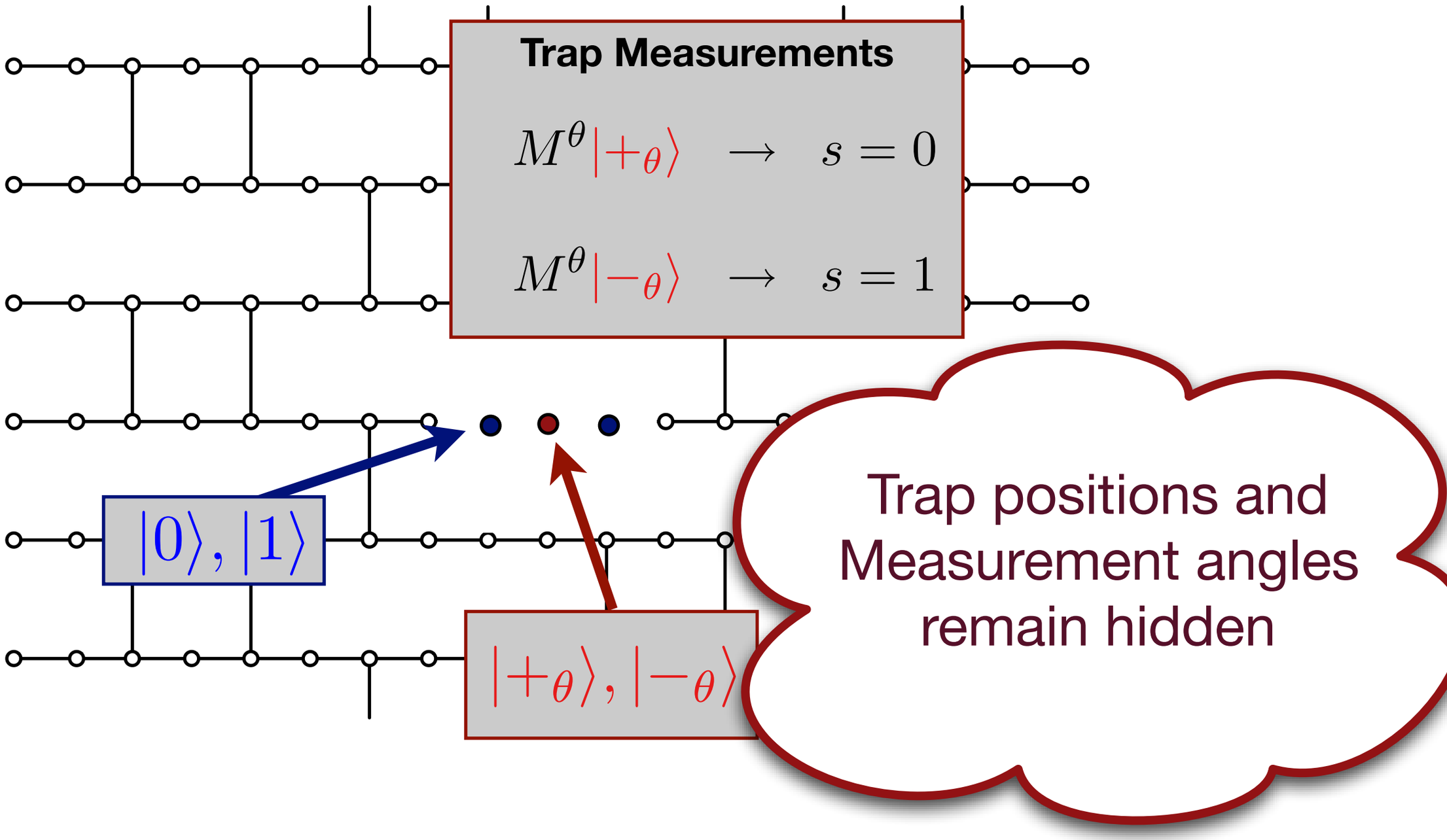
Adding Traps



Adding Traps



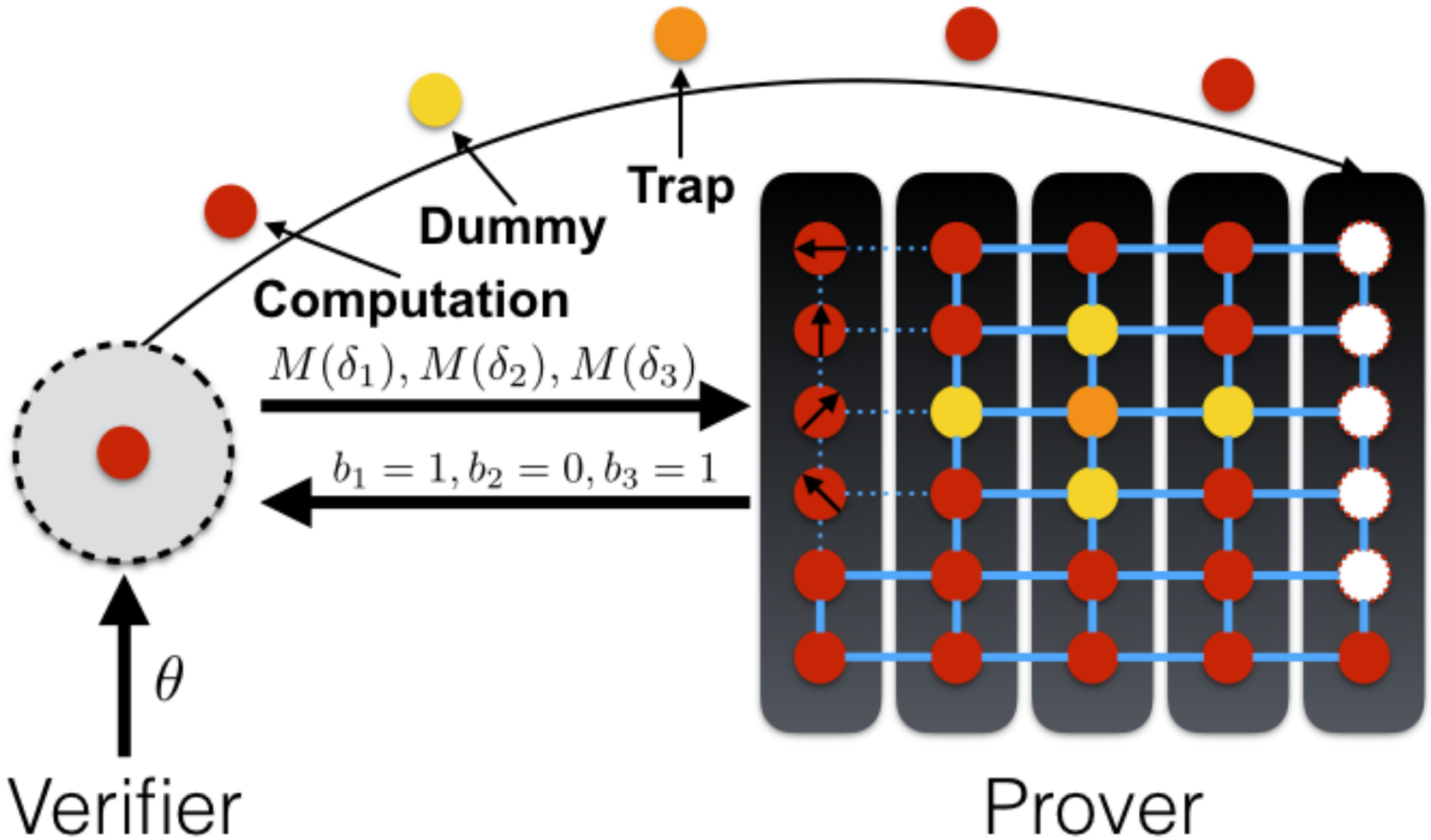
Adding Traps



Verification with single trap

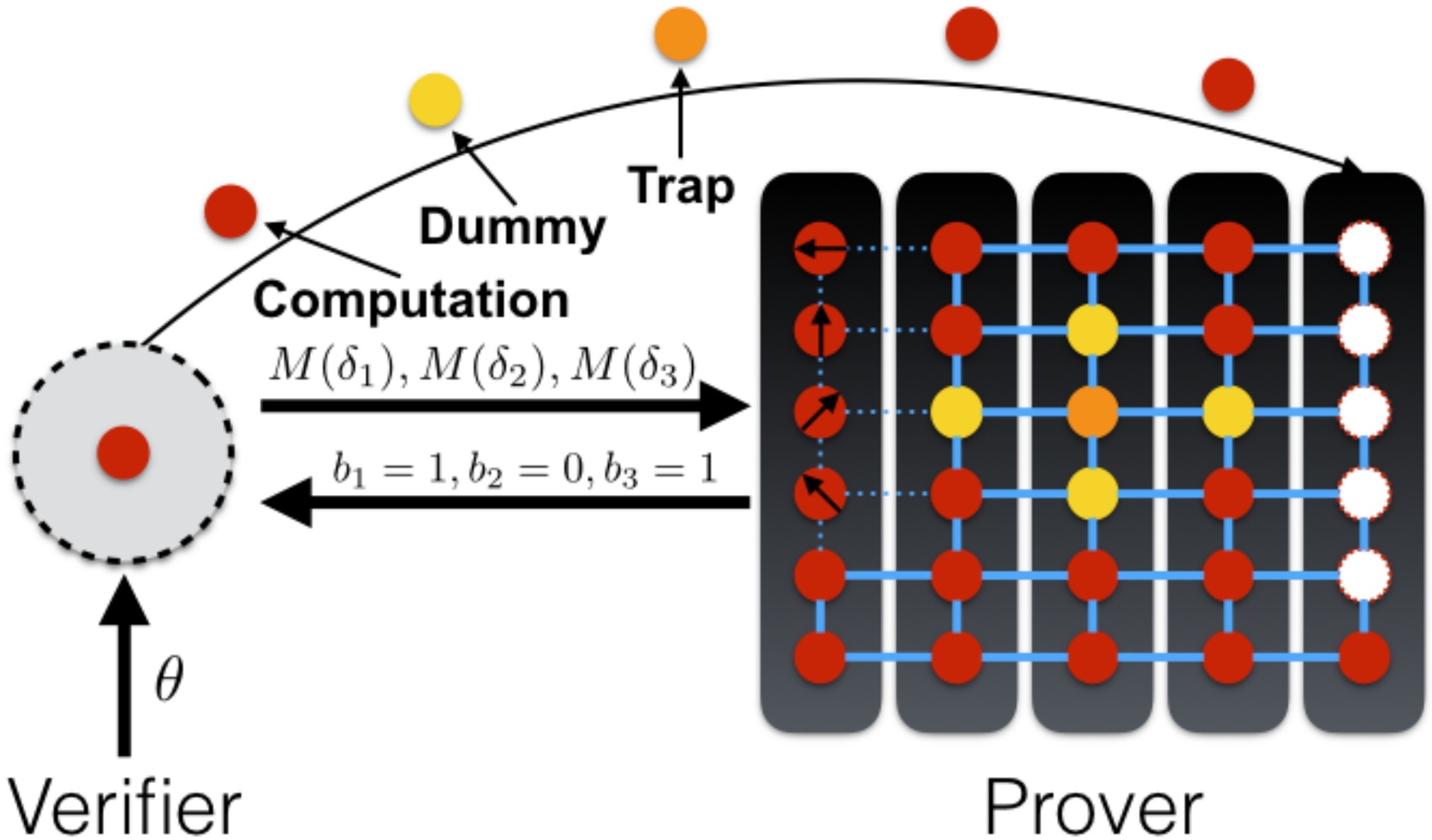
Theorem. Protocol is $(1 - 1/2N)$-verifiable in general, and in the case of purely classical output it is $(1 - 1/N)$-verifiable, where N is the total number of qubits in the protocol.

Verifiable Quantum Cloud in Theory



Aharonov, Ben-Or, and Eban, ICS 2010
Fitzsimons and Kashefi, 2012

Verifiable Quantum Cloud in Theory



Verifiable Universal Blind Quantum Computing: QKD + Teleportation + Test

Aharonov, Ben-Or, and Eban, ICS 2010
Fitzsimons and Kashefi, 2012

ε-Verification

Alice

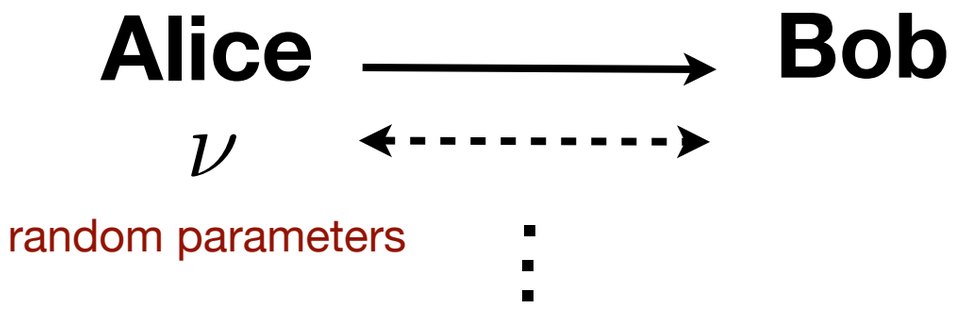
ν

random parameters

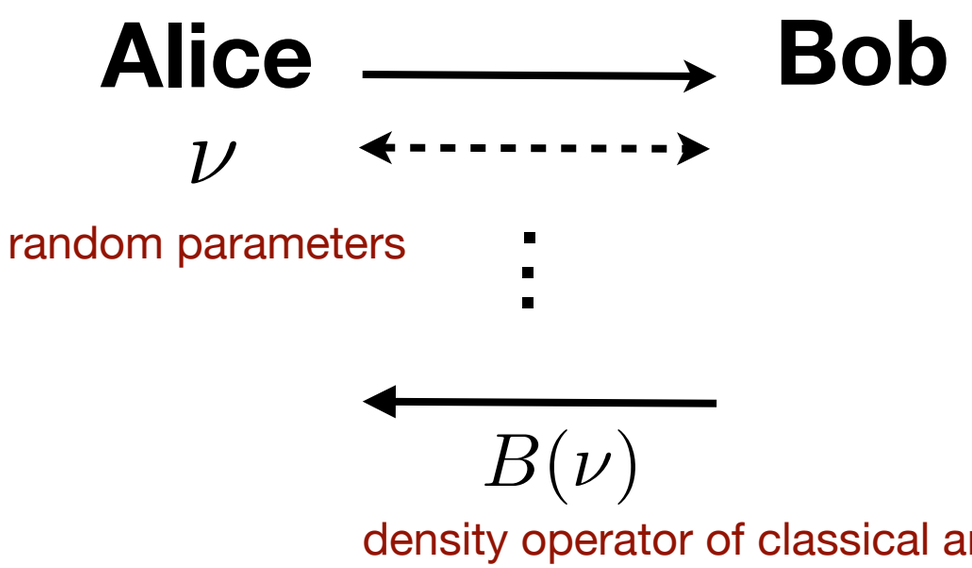
Bob

ε-Verification

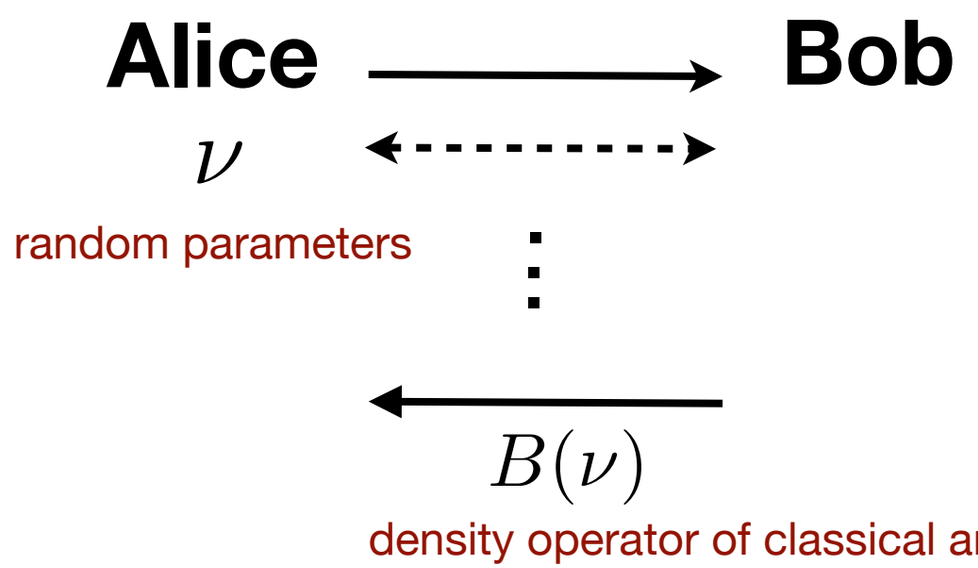
ε-Verification



ε-Verification

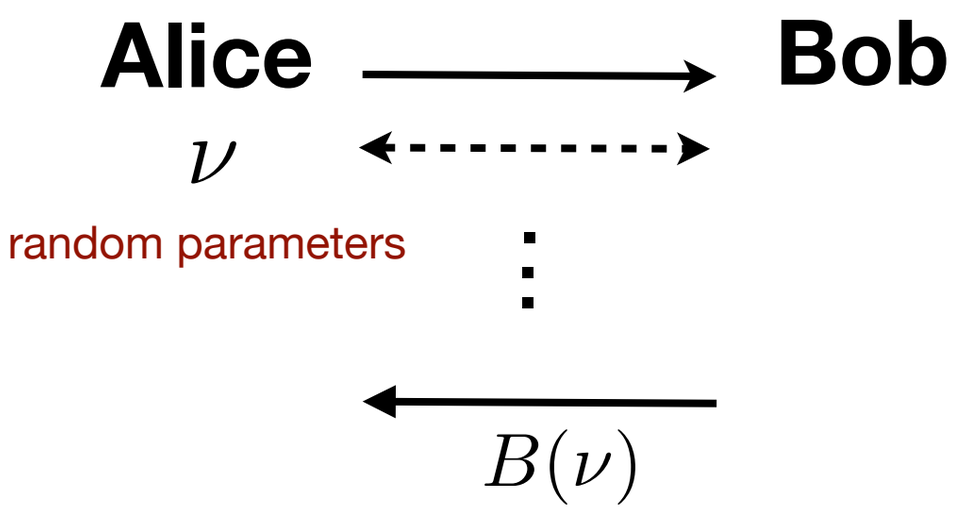


ε-Verification



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

ε-Verification

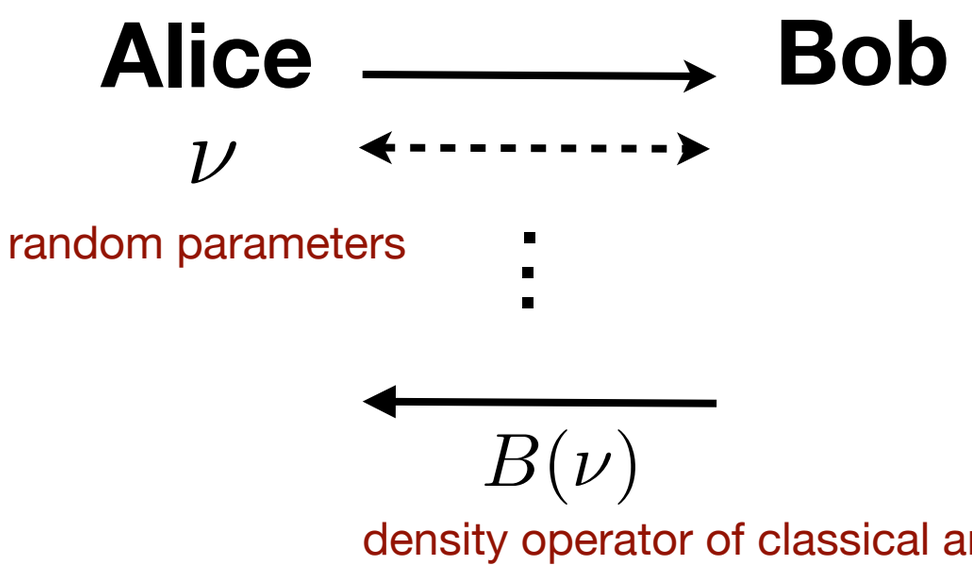


For any server's strategy the probability of client accepting an incorrect outcome density operator is bounded by ε:

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

Accept Key

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

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

ε-Verification

$$P^s_{incorrect} = (I - |\Psi^s_{out}\rangle \langle \Psi^s_{out}|) \otimes |acc^s\rangle \langle acc^s|$$

ε-Verification

private random string, sampled by the verifier from some distribution p(s)

$$P^s_{incorrect} = (I - |\Psi^s_{out}\rangle \langle \Psi^s_{out}|) \otimes |acc^s\rangle \langle acc^s|$$

ε-Verification

private random string, sampled by the verifier from some distribution p(s)

$$P^s_{incorrect} = (I - |\Psi^s_{out}\rangle \langle \Psi^s_{out}|) \otimes |acc^s\rangle \langle acc^s|$$

$$|\Psi^s_{out}\rangle \langle \Psi^s_{out}| = Tr_{flag}(\mathcal{P}_{honest}(Enc_s(|\psi\rangle \langle \psi| \otimes |acc\rangle \langle acc|)))$$

ε-Verification

private random string, sampled by the verifier from some distribution p(s)

$$P^s_{incorrect} = (I - |\Psi^s_{out}\rangle \langle \Psi^s_{out}|) \otimes |acc^s\rangle \langle acc^s|$$

$$|\Psi^s_{out}\rangle \langle \Psi^s_{out}| = Tr_{flag}(\mathcal{P}_{honest}(Enc_s(|\psi\rangle \langle \psi| \otimes |acc\rangle \langle acc|)))$$

$$|acc^s\rangle \langle acc^s| = Tr_{input}(\mathcal{P}_{honest}(Enc_s(|\psi\rangle \langle \psi| \otimes |acc\rangle \langle acc|)))$$

ε-Verification

private random string, sampled by the verifier from some distribution p(s)

$$P^s_{incorrect} = (I - |\Psi^s_{out}\rangle \langle \Psi^s_{out}|) \otimes |acc^s\rangle \langle acc^s|$$

$$|\Psi^s_{out}\rangle \langle \Psi^s_{out}| = Tr_{flag}(\mathcal{P}_{honest}(Enc_s(|\psi\rangle \langle \psi| \otimes |acc\rangle \langle acc|)))$$

$$|acc^s\rangle \langle acc^s| = Tr_{input}(\mathcal{P}_{honest}(Enc_s(|\psi\rangle \langle \psi| \otimes |acc\rangle \langle acc|)))$$

$$Tr\left(\sum_s p(s) P^s_{incorrect} \mathcal{P}(Enc_s(|\psi\rangle \langle \psi| \otimes |acc\rangle \langle acc|))\right) \leq \epsilon$$

ε-Verification

private random string, sampled by the verifier from some distribution p(s)

$$P^s_{incorrect} = (I - |\Psi^s_{out}\rangle \langle \Psi^s_{out}|) \otimes |acc^s\rangle \langle acc^s|$$

$$|\Psi^s_{out}\rangle \langle \Psi^s_{out}| = Tr_{flag}(\mathcal{P}_{honest}(Enc_s(|\psi\rangle \langle \psi| \otimes |acc\rangle \langle acc|)))$$

$$|acc^s\rangle \langle acc^s| = Tr_{input}(\mathcal{P}_{honest}(Enc_s(|\psi\rangle \langle \psi| \otimes |acc\rangle \langle acc|)))$$

$$Tr\left(\sum_s p(s) P^s_{incorrect} \mathcal{P}(Enc_s(|\psi\rangle \langle \psi| \otimes |acc\rangle \langle acc|))\right) \leq \epsilon$$

$$Pr(incorrect, accept) \leq \epsilon$$

δ -Correctness

$$P^s_{correct} = |\Psi^s_{out}\rangle \langle \Psi^s_{out}| \otimes |acc^s\rangle \langle acc^s|$$

δ -Correctness

$$P^s_{correct} = |\Psi^s_{out}\rangle \langle \Psi^s_{out}| \otimes |acc^s\rangle \langle acc^s|$$

$$|\Psi^s_{out}\rangle \langle \Psi^s_{out}| = Tr_{flag}(\mathcal{P}_{honest}(Enc_s(|\psi\rangle \langle \psi| \otimes |acc\rangle \langle acc|)))$$

$$|acc^s\rangle \langle acc^s| = Tr_{input}(\mathcal{P}_{honest}(Enc_s(|\psi\rangle \langle \psi| \otimes |acc\rangle \langle acc|)))$$

δ -Correctness

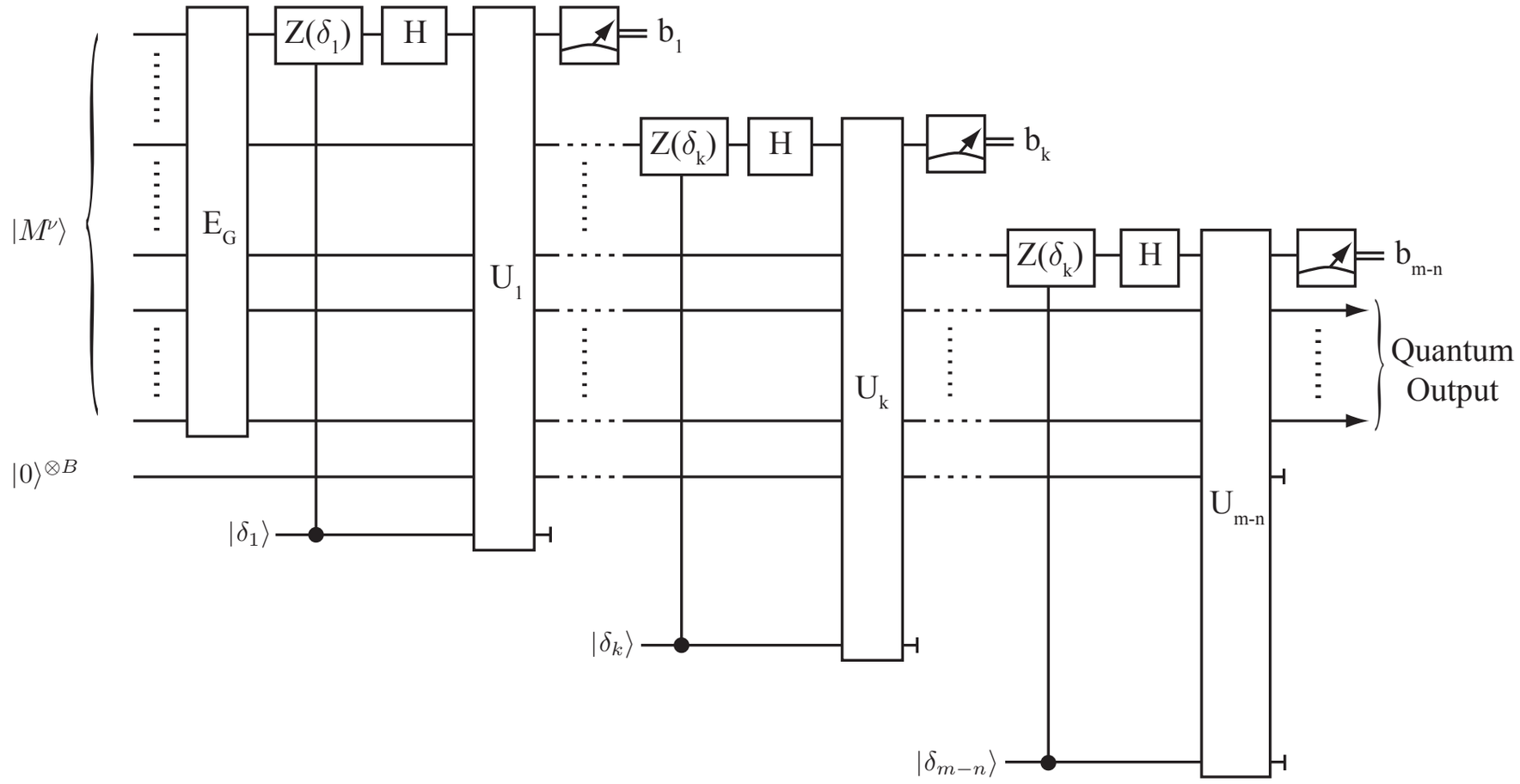
$$P^s_{correct} = |\Psi^s_{out}\rangle \langle \Psi^s_{out}| \otimes |acc^s\rangle \langle acc^s|$$

$$|\Psi^s_{out}\rangle \langle \Psi^s_{out}| = Tr_{flag}(\mathcal{P}_{honest}(Enc_s(|\psi\rangle \langle \psi| \otimes |acc\rangle \langle acc|)))$$

$$|acc^s\rangle \langle acc^s| = Tr_{input}(\mathcal{P}_{honest}(Enc_s(|\psi\rangle \langle \psi| \otimes |acc\rangle \langle acc|)))$$

$$Tr\left(P^s_{correct}\mathcal{P}_{honest}(Enc_s(|\psi\rangle \langle \psi| \otimes |acc\rangle \langle acc|))\right) \geq \delta$$

ε-Verification



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

Verification Proof Technique

$$p_{incorrect} = \sum_{\nu} p(\nu) \mathrm{Tr}(P_{\perp} \otimes |\eta_t^{\nu}\rangle \langle \eta_t^{\nu}| \ (\Omega \mathcal{P}((\otimes^B |0\rangle \langle 0|) \otimes |\Psi^{\nu}\rangle \langle \Psi^{\nu}|) \mathcal{P}^{\dagger} \Omega^{\dagger})) .$$

Verification Proof Technique

$$p_{incorrect} = \sum_{\nu} p(\nu) \mathrm{Tr}(P_{\perp} \otimes |\eta_t^{\nu}\rangle \langle \eta_t^{\nu}| (\Omega \mathcal{P}((\otimes^{B} |0\rangle \langle 0|) \otimes |\Psi^{\nu}\rangle \langle \Psi^{\nu}|) \mathcal{P}^{\dagger} \Omega^{\dagger})) .$$

$\vdots$

Blindness

Verification Proof Technique

$$p_{incorrect} = \sum_{\nu} p(\nu) \mathrm{Tr}(P_{\perp} \otimes |\eta_t^{\nu}\rangle \langle \eta_t^{\nu}| (\Omega \mathcal{P}((\otimes^B |0\rangle \langle 0|) \otimes |\Psi^{\nu}\rangle \langle \Psi^{\nu}|) \mathcal{P}^{\dagger} \Omega^{\dagger})) .$$

$$\vdots$$

Blindness

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

Verification Proof Technique

$$p_{incorrect} = \sum_{\nu} p(\nu) \mathrm{Tr}(P_{\perp} \otimes |\eta_t^{\nu}\rangle \langle \eta_t^{\nu}| (\Omega \mathcal{P}((\otimes^B |0\rangle \langle 0|) \otimes |\Psi^{\nu}\rangle \langle \Psi^{\nu}|) \mathcal{P}^{\dagger} \Omega^{\dagger})) .$$

$$\vdots$$

Blindness

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

Verification Proof Technique

$$p_{incorrect} = \sum_{\nu} p(\nu) \mathrm{Tr}(P_{\perp} \otimes |\eta_t^{\nu}\rangle \langle \eta_t^{\nu}| (\Omega \mathcal{P}((\otimes^B |0\rangle \langle 0|) \otimes |\Psi^{\nu}\rangle \langle \Psi^{\nu}|) \mathcal{P}^{\dagger} \Omega^{\dagger})) .$$

$$\vdots$$

Blindness

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

$$\vdots$$

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

Verification Proof Technique

$$p_{incorrect} = \sum_{\nu} p(\nu) \mathrm{Tr}(P_{\perp} \otimes |\eta_t^{\nu}\rangle \langle \eta_t^{\nu}| (\Omega \mathcal{P}((\otimes^B |0\rangle \langle 0|) \otimes |\Psi^{\nu}\rangle \langle \Psi^{\nu}|) \mathcal{P}^{\dagger} \Omega^{\dagger})) .$$

$$\vdots$$

Blindness

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

$$\vdots$$

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

$$\vdots$$

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

Verification Proof Technique

$$p_{incorrect} = \sum_{\nu} p(\nu) \mathrm{Tr}(P_{\perp} \otimes |\eta_t^{\nu}\rangle \langle \eta_t^{\nu}| (\Omega \mathcal{P}((\otimes^B |0\rangle \langle 0|) \otimes |\Psi^{\nu}\rangle \langle \Psi^{\nu}|) \mathcal{P}^{\dagger} \Omega^{\dagger})) .$$

$$\vdots$$

Blindness

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

(Pauli Twirl) Let P, P' be n-qubit Pauli operators. Then:

$$\frac{1}{|\mathbb{P}_n|} \sum_{Q \in \mathbb{P}_n} Q^* P Q \rho Q^* P'^* Q = \begin{cases} 0, & P \neq P' \\ P \rho P^*, & otherwise . \end{cases}$$

$$\vdots$$

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

Probability Amplification

To increase the probability of any local error being detected

O(N) many traps in random locations

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

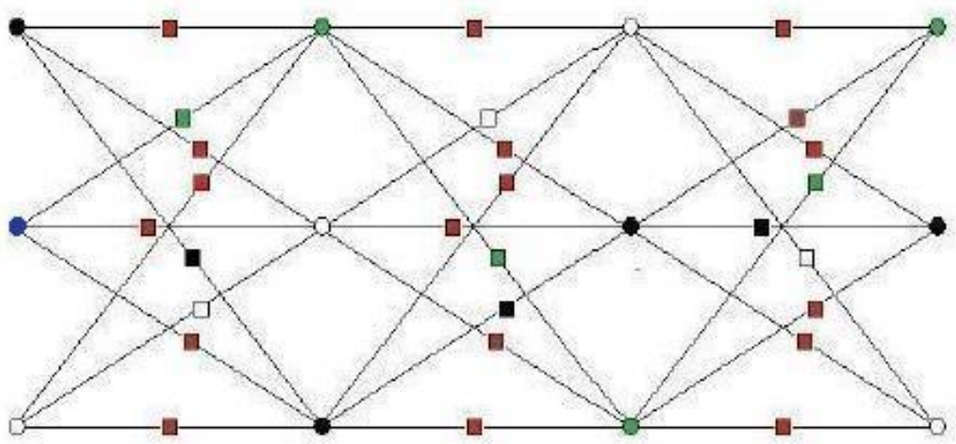
Fault-Tolerance

Efficient Verifiable UBQC

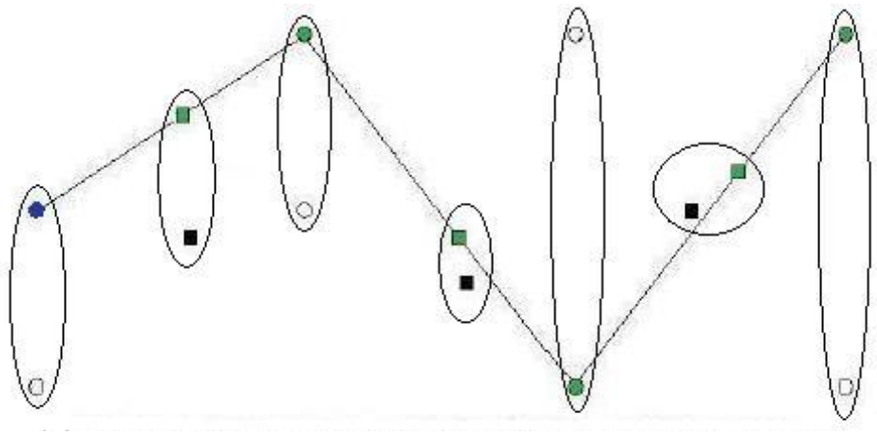
[Kashefi-Wallden 16]

Dotted triple-graph construction ⟶ O(N) overheads for VUBQC

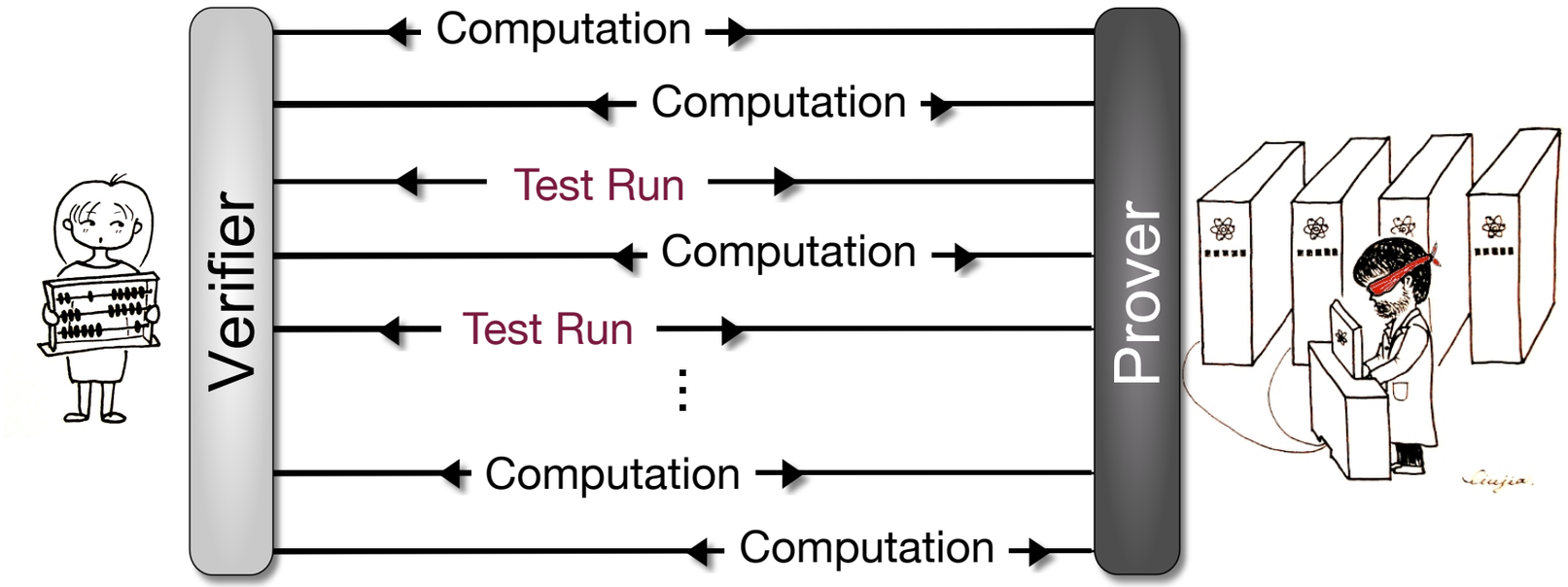
generic resource state, that one can insert multiple independent traps without revealing anything or disrupting the computation



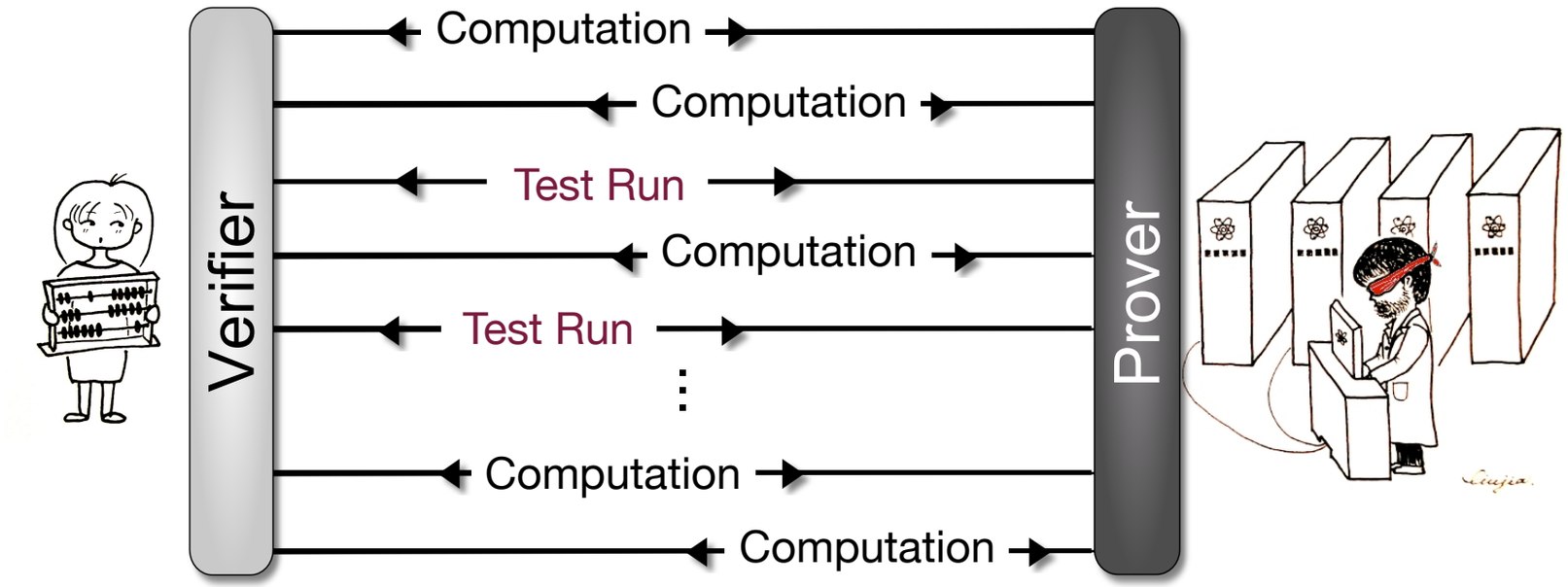
(a) Trap-colouring



Test or Compute

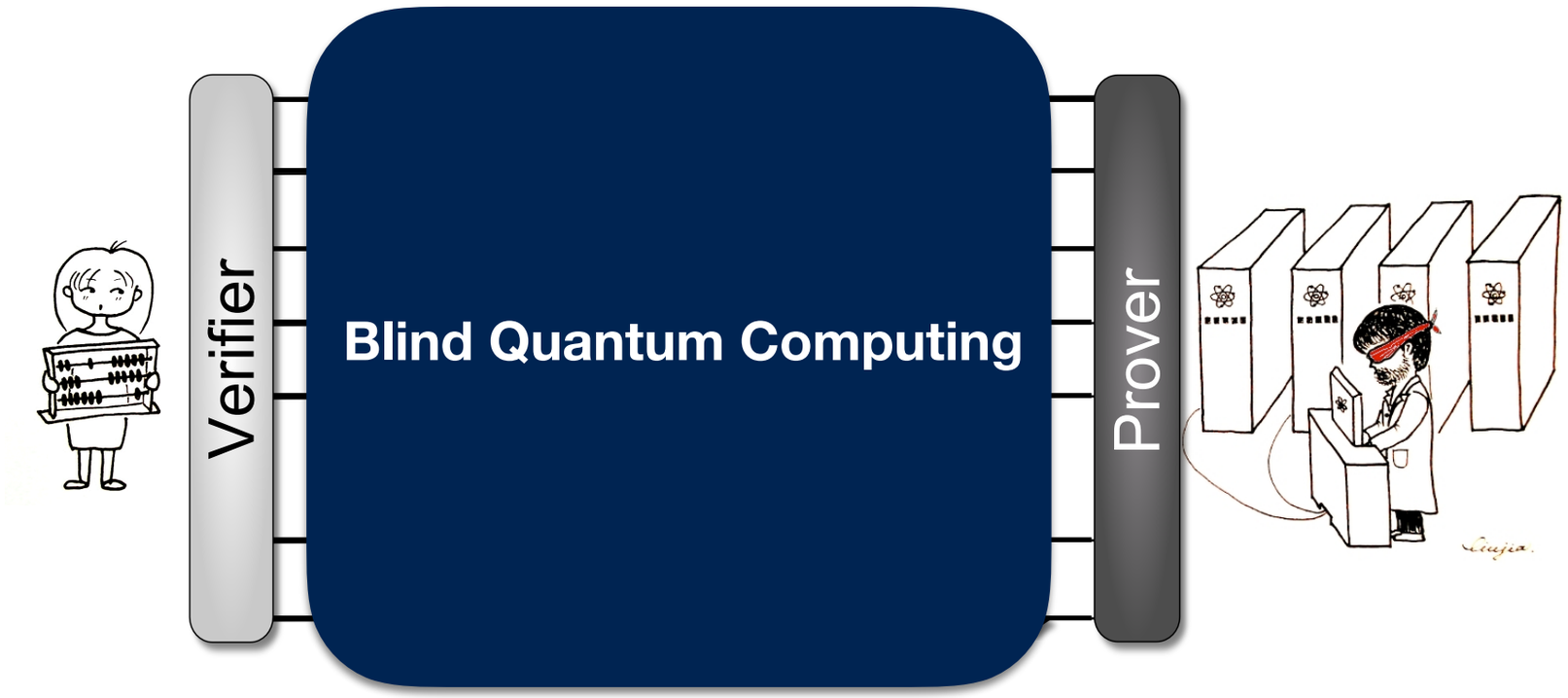


Test or Compute



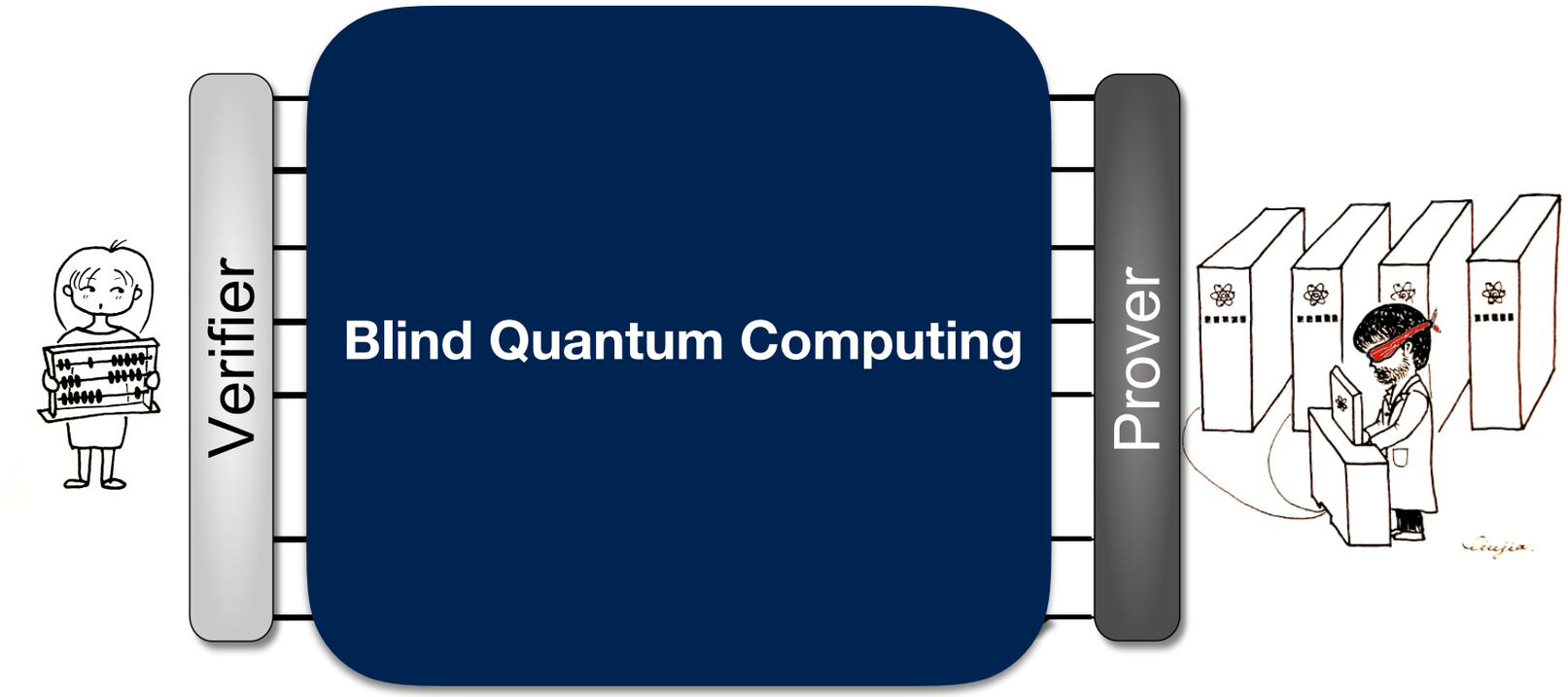
- **Computation run**. The verifier delegates $\mathcal{C}\,|0\rangle^{\otimes n}$ to the prover.
- **X-test run**. The verifier delegates the identity computation on the $|0\rangle^{\otimes n}$ state to the prover.
- **Z-test run**. The verifier delegates the identity computation on the $|+\rangle^{\otimes n}$ state to the prover.

Test or Compute



- **Computation run**. The verifier delegates $\mathcal{C}\,|0\rangle^{\otimes n}$ to the prover.
- **X-test run**. The verifier delegates the identity computation on the $|0\rangle^{\otimes n}$ state to the prover.
- **Z-test run**. The verifier delegates the identity computation on the $|+\rangle^{\otimes n}$ state to the prover.

Test or Compute



- **Computation run**. The verifier delegates $\mathcal{C}\,|0\rangle^{\otimes n}$ to the prover.
- **X-test run**. The verifier delegates the identity computation on the $|0\rangle^{\otimes n}$ state to the prover.
- **Z-test run**. The verifier delegates the identity computation on the $|+\rangle^{\otimes n}$ state to the prover.

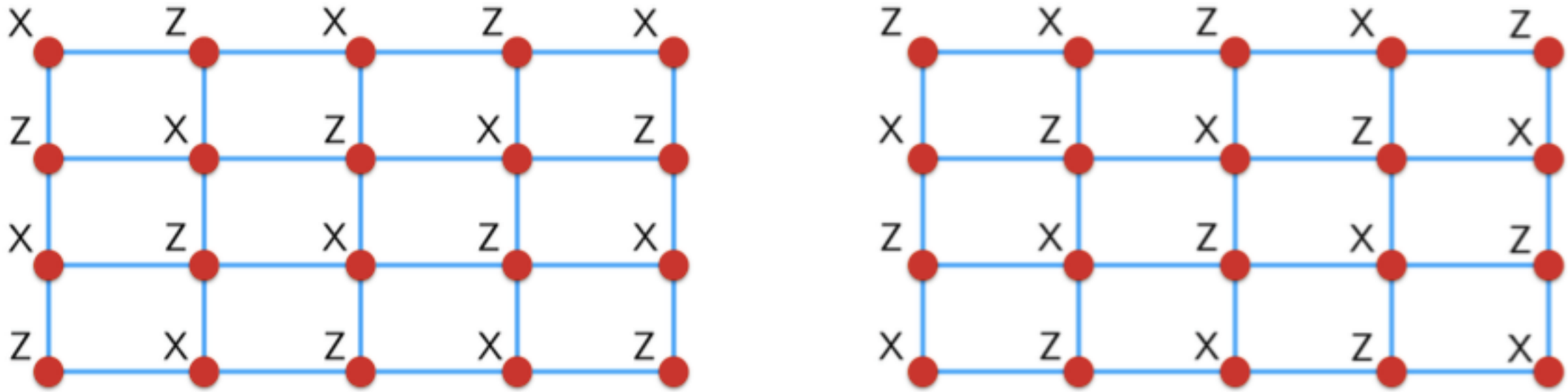
cryptography reduces the **verification** problem to **error-detection** procedure bypassing the complexity of simulation

Summery of Prepare and Sent

Protocol	Verifier resources	Communication	2-way quantum comm.
Clifford-QAS VQC	$O(log(1/\epsilon))$	$O(N \cdot log(1/\epsilon))$	Y
Poly-QAS VQC	$O(log(1/\epsilon))$	$O((n+L) \cdot log(1/\epsilon))$	N
VUBQC	$O(1)$	$O(N \cdot log(1/\epsilon))$	N
Test-or-Compute	$O(1)$	$O((n+T) \cdot log(1/\epsilon))$	N

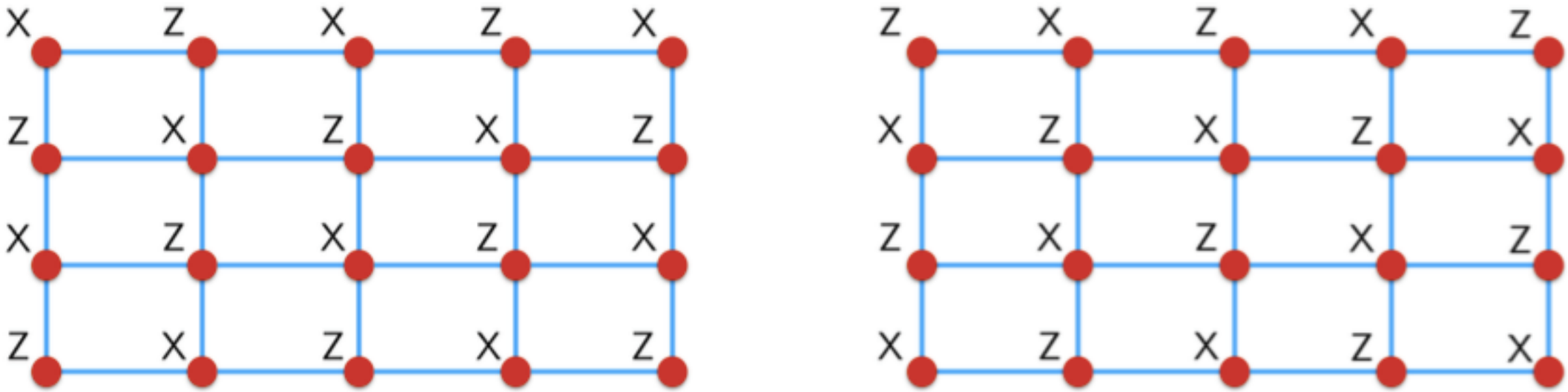
x the input to this circuit, then $n = |x|$, $N = |\mathcal{C}|$

Receive and Measure



Stabiliser measurements

Receive and Measure



Stabiliser measurements

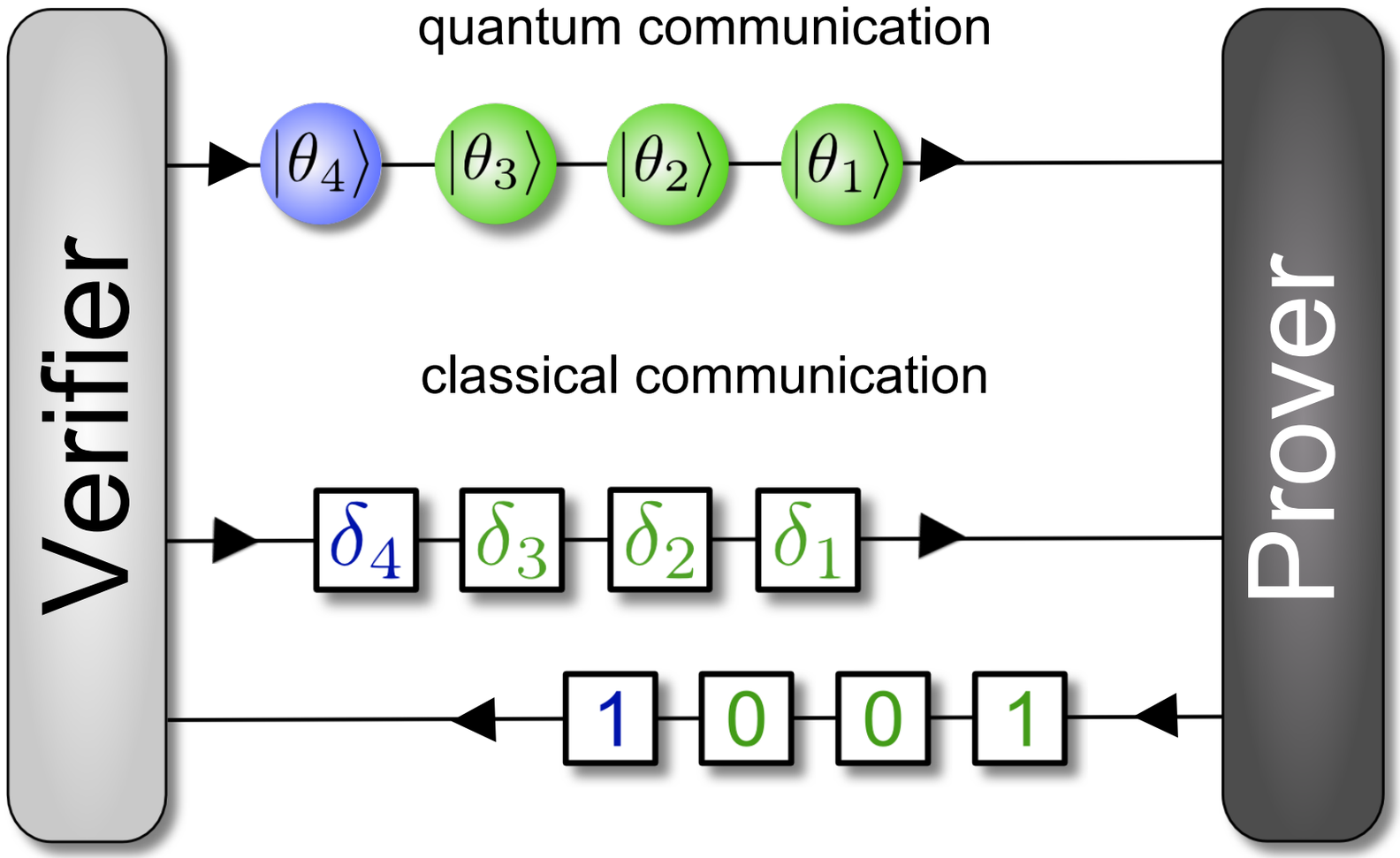
The verifier randomly picks one copy to run the computation of $\mathcal{C}$ on x in an MBQC fashion. The remaining $2k$ copies are randomly divided into the XZ groups and the ZX group and measured, as described above, so as to check the stabilizers of $|G\rangle$.

Summery of Receive and Measure

confidence level of the verifier in the hypothesis test

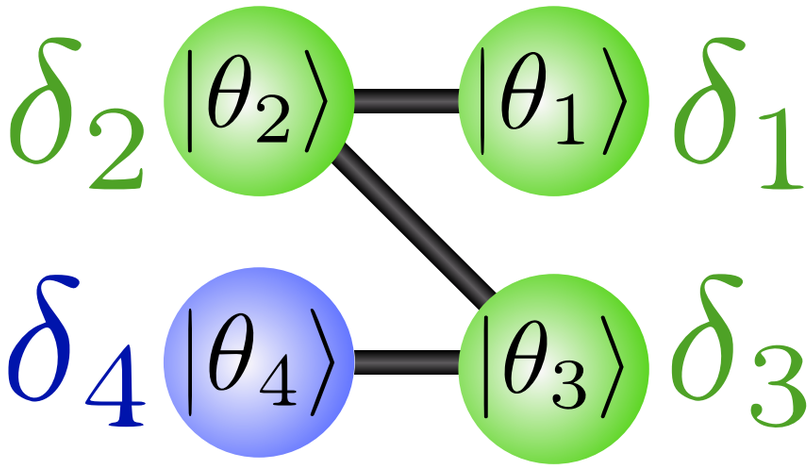
Protocol	Measurements	Observables	Blind
Measurement-only	$O(N \cdot 1/\alpha \cdot 1/\epsilon^2)$	5	Y
Hypergraph measurement-only	$O(max(N, 1/\epsilon^2)^{22})$	3	Y
1S-Post-hoc	$O(N^2 \cdot log(1/\epsilon))$	2	N
Steering-based VUBQC	$O(N^{13} log(N) \cdot log(1/\epsilon))$	5	Y

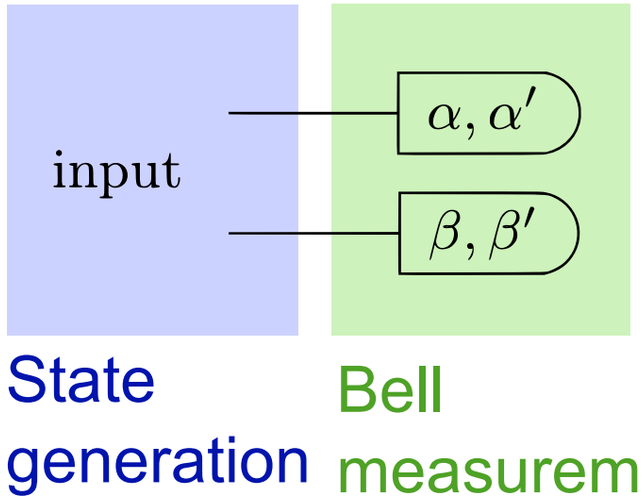
What can we do with 4-qubits

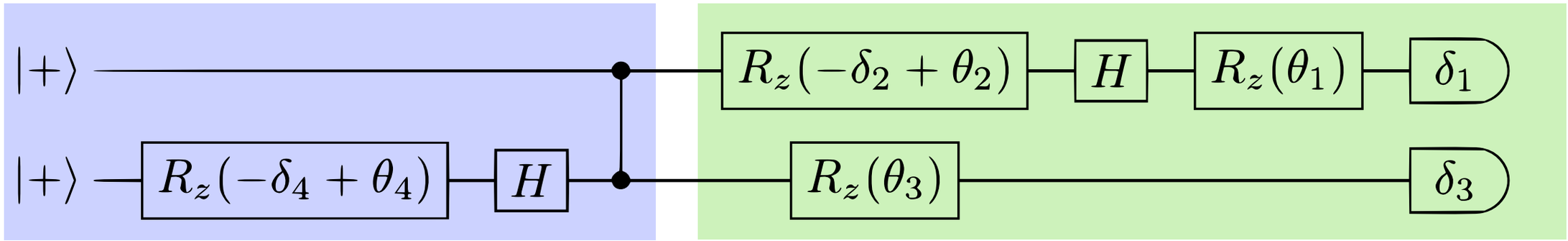


Blind Verification of Entanglement

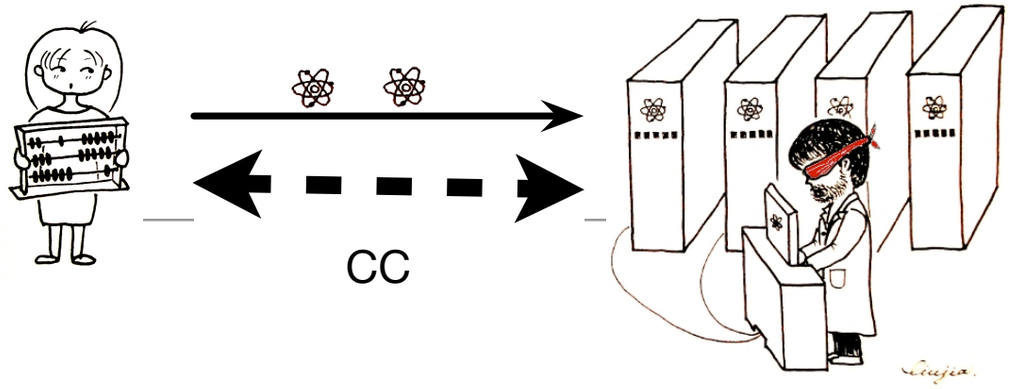
S. Barz, J. Fitzsimons, E. Kashefi, P. Walther, Nature Physics 2013



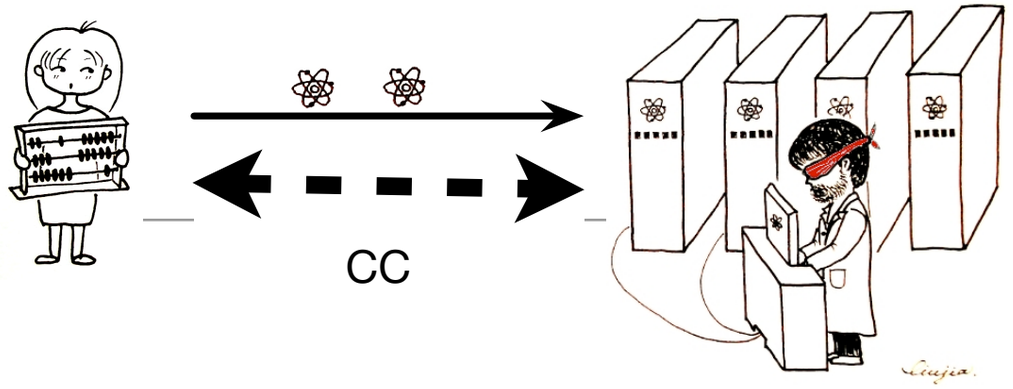




Quantum Property Testing



Quantum Property Testing



Non-classical Correlation

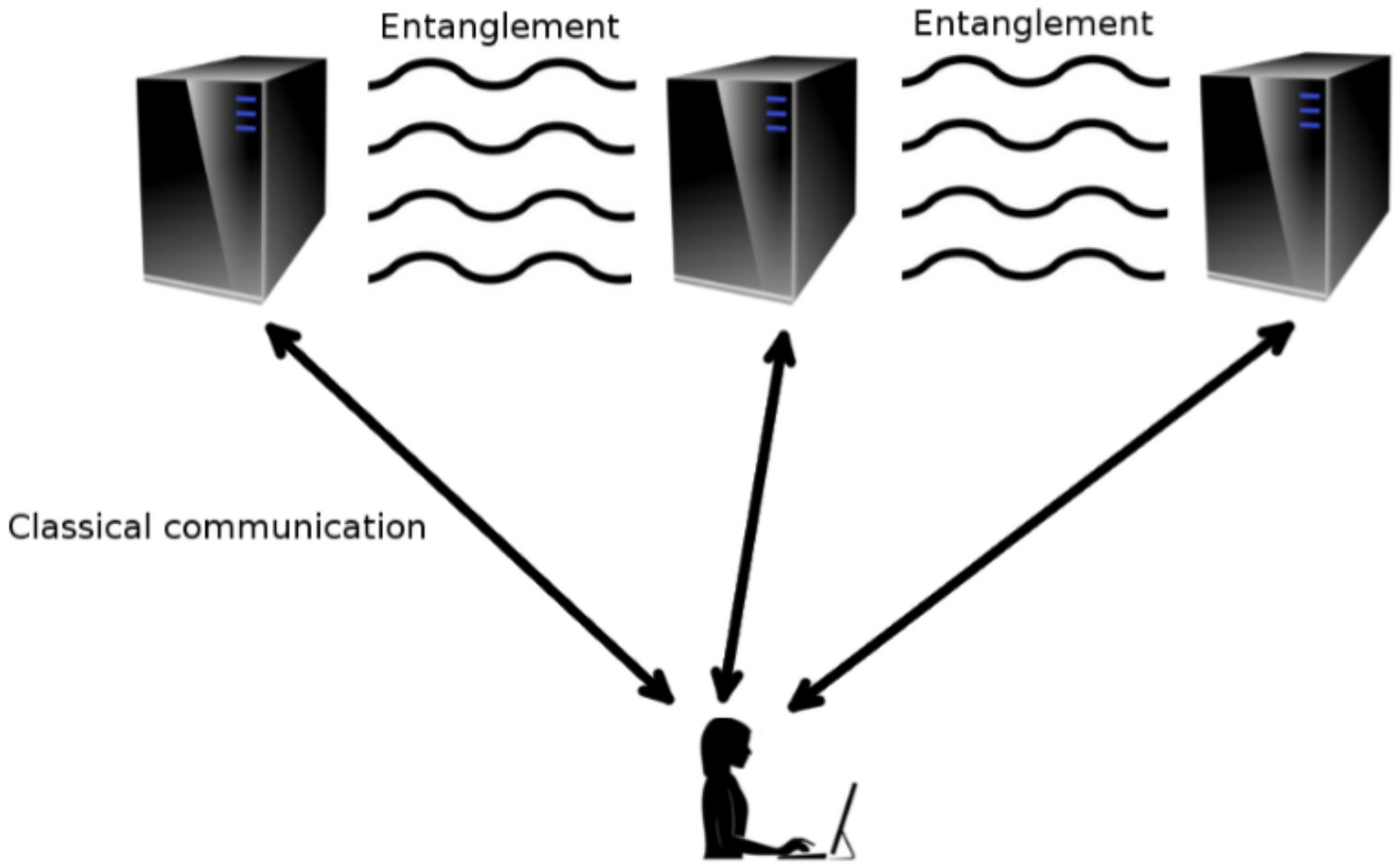
Contextuality

Dimentionality

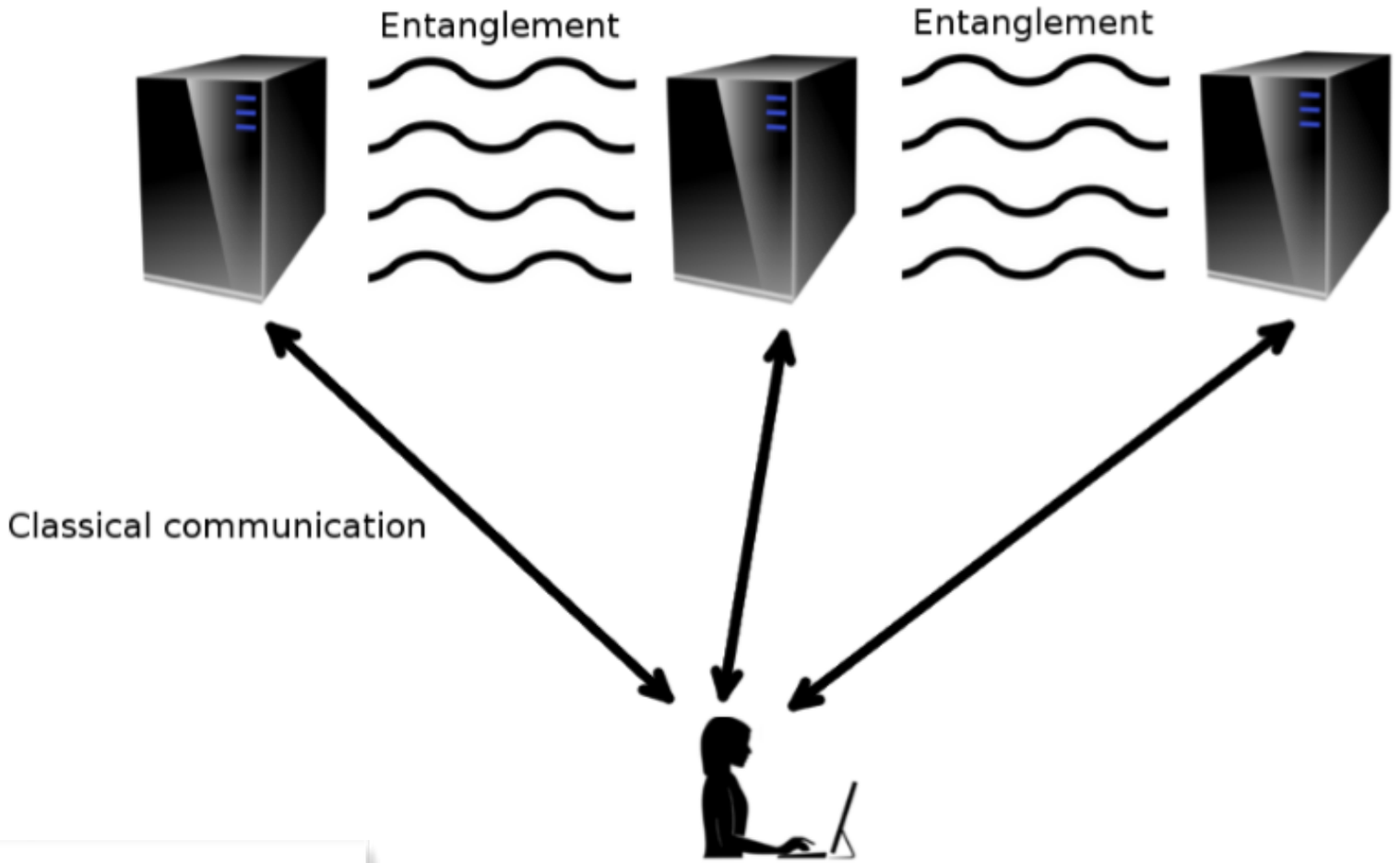
Superposition

Multi-provers entangled-based

Multi-provers entangled-based



Multi-provers entangled-based

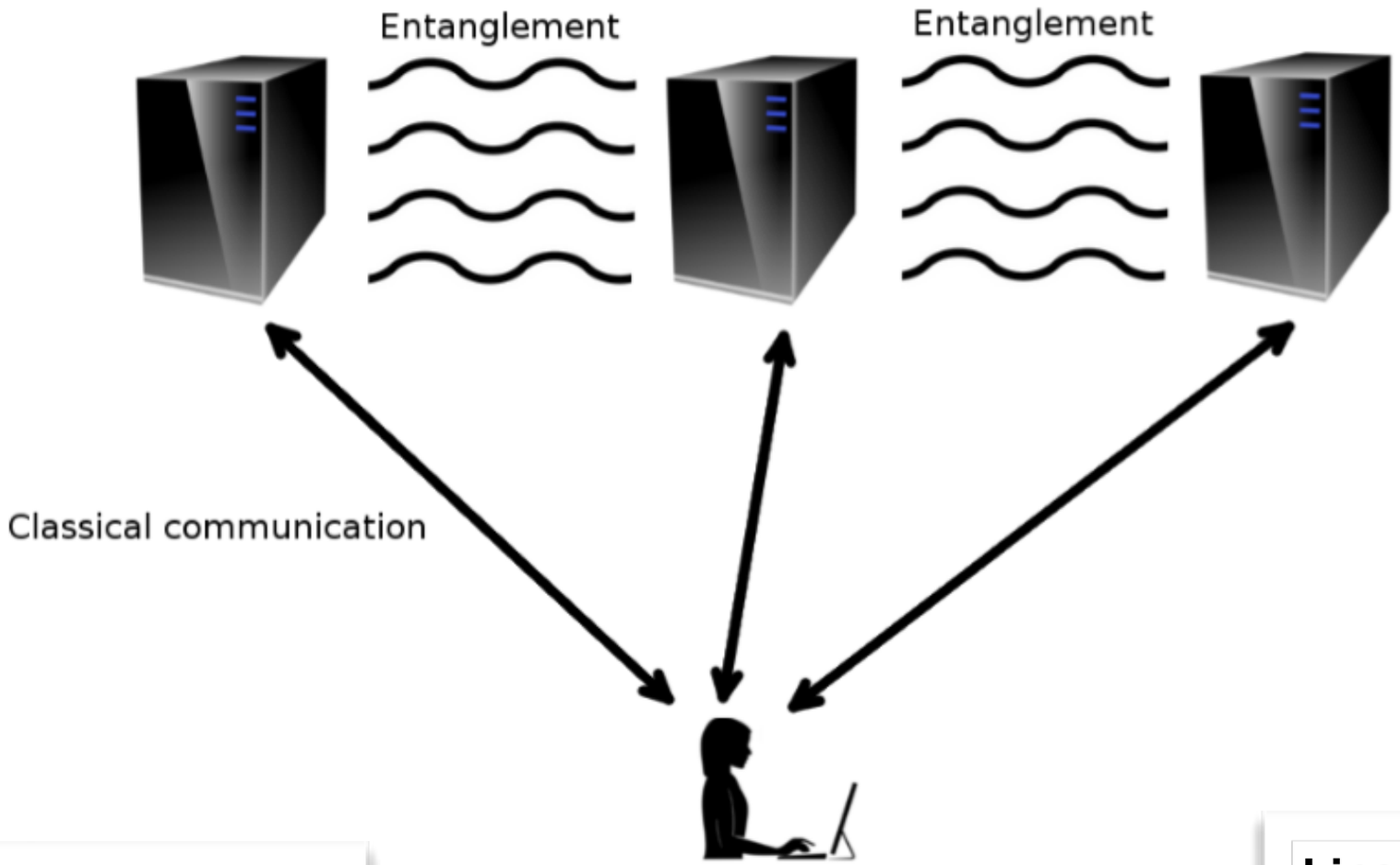


Constant number of servers

Reichardt et. al. Nature 2012
Based on rigidity of CHSH games
Certifying entanglement and measurements
Huge overhead for establishing tensor product of Bell pairs

Round complexity: $O(N^{8192})$

Multi-provers entangled-based



Constant number of servers

Reichardt et. al. Nature 2012
Based on rigidity of CHSH games
Certifying entanglement and measurements
Huge overhead for establishing tensor product of Bell pairs

Round complexity: $O(N^{8192})$

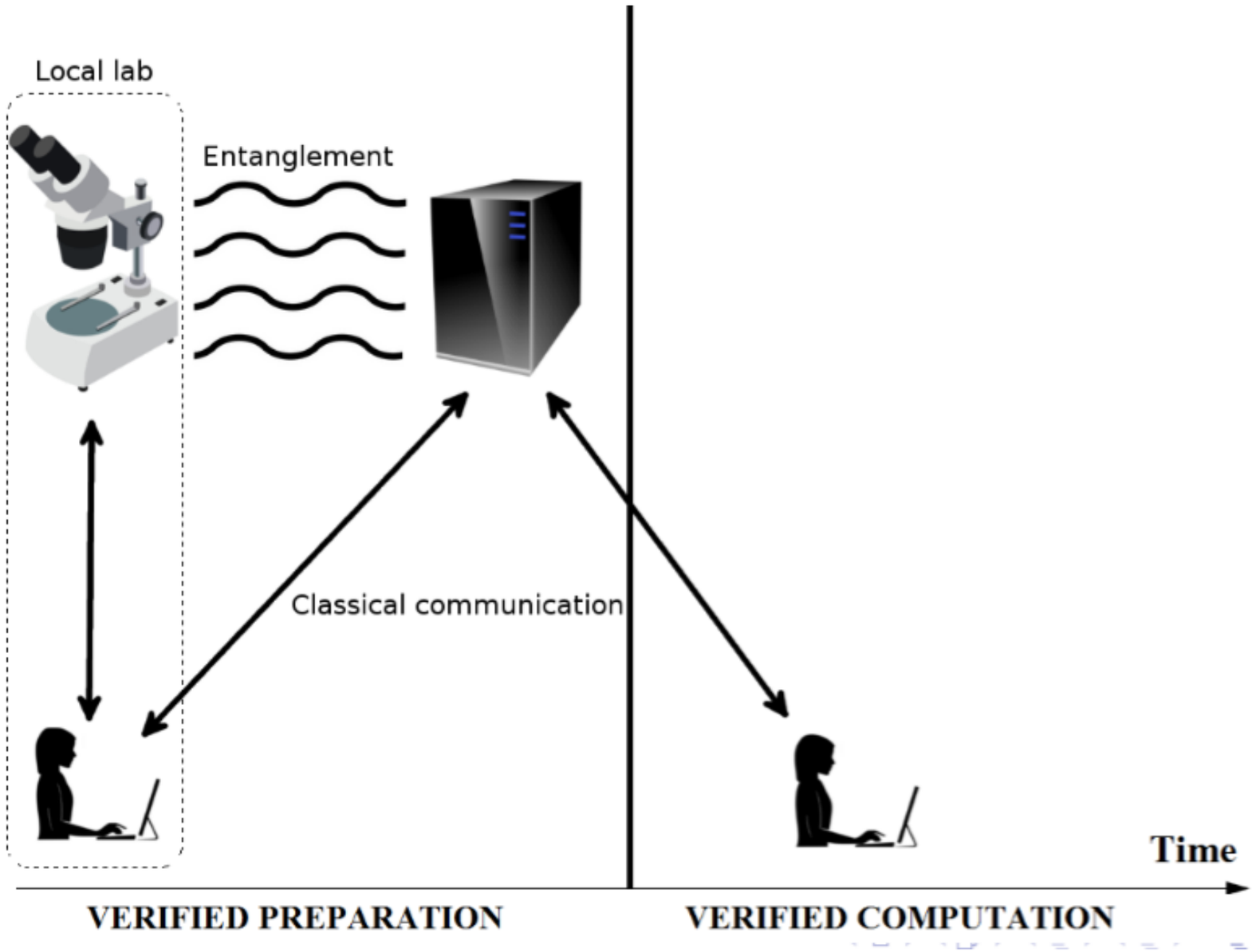
Linear number of servers

McKague et. al. JoC 2013
Based on rigidity of CHSH games
Assumed tenor product structure

Round complexity: $O(N^{22})$

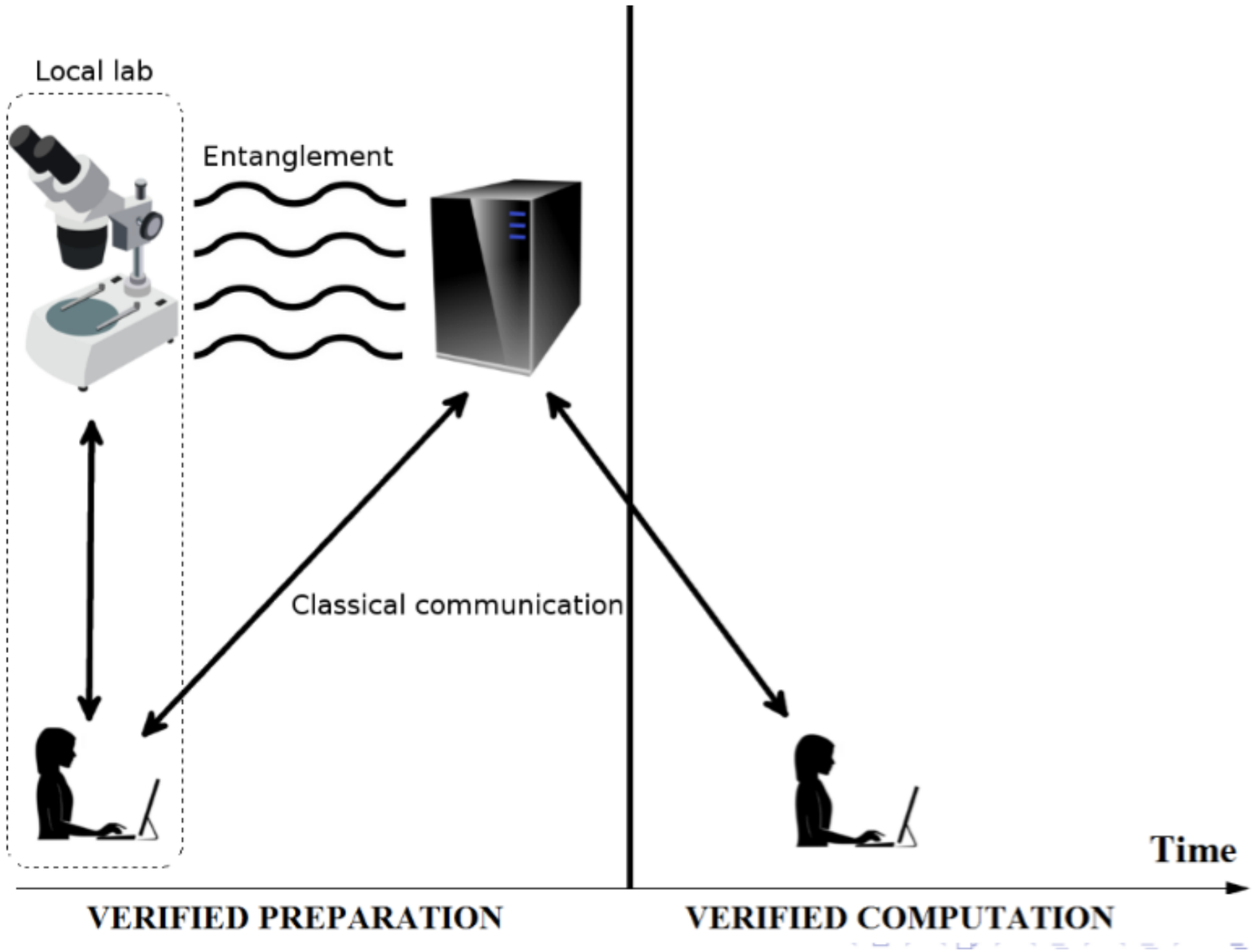
DI - Verification

Kashefi et.al.
Device independent VUBQC
New Journal of Physics 2015



DI - Verification

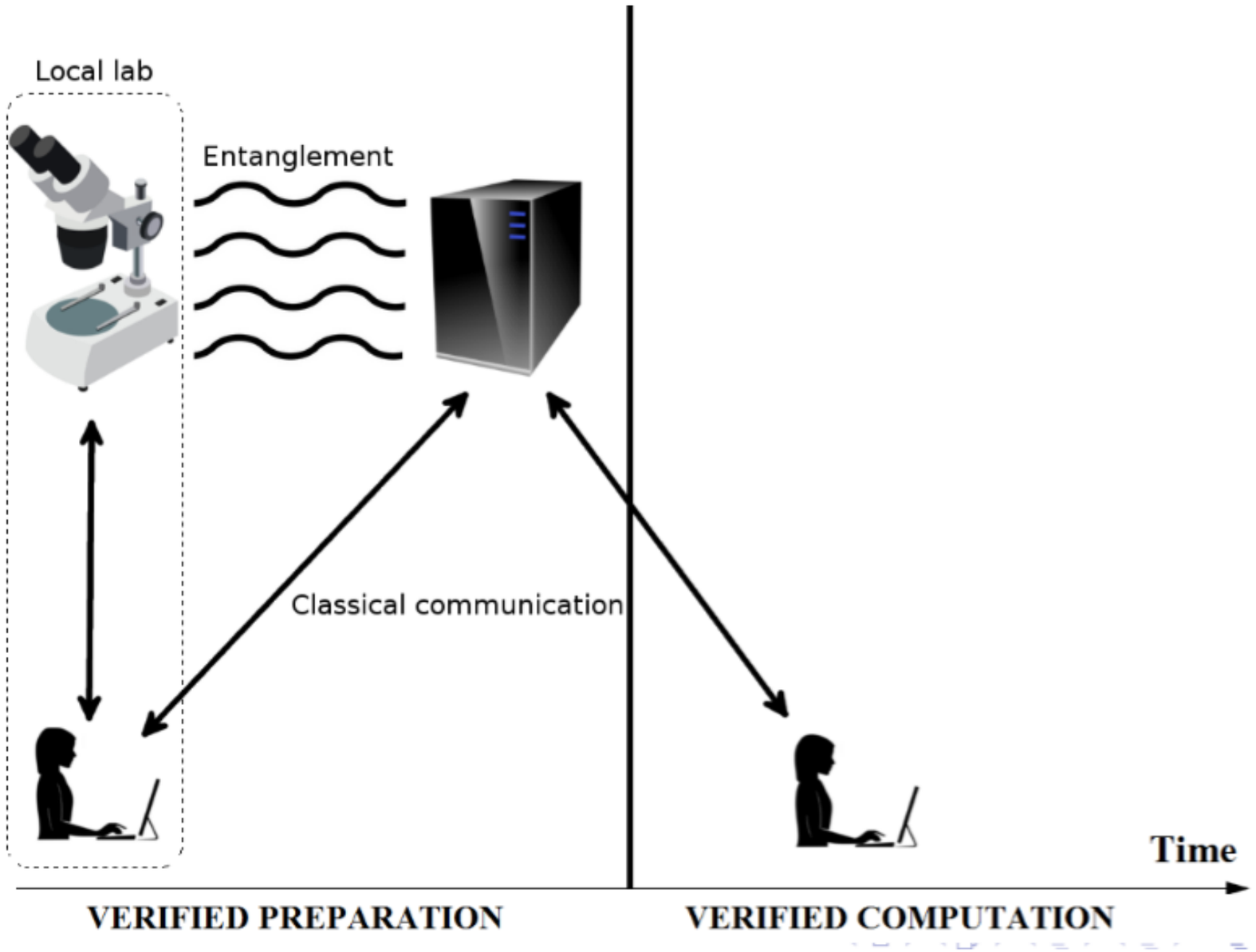
Kashefi et.al.
Device independent VUBQC
New Journal of Physics 2015



- Based on rigidity of CHSH games
- Certify tensor product of Bell pairs
- Certify correct measurements
- Verified preparation of single random qubit
- Verified computation = previous linear protocol

DI - Verification

Kashefi et.al.
Device independent VUBQC
New Journal of Physics 2015

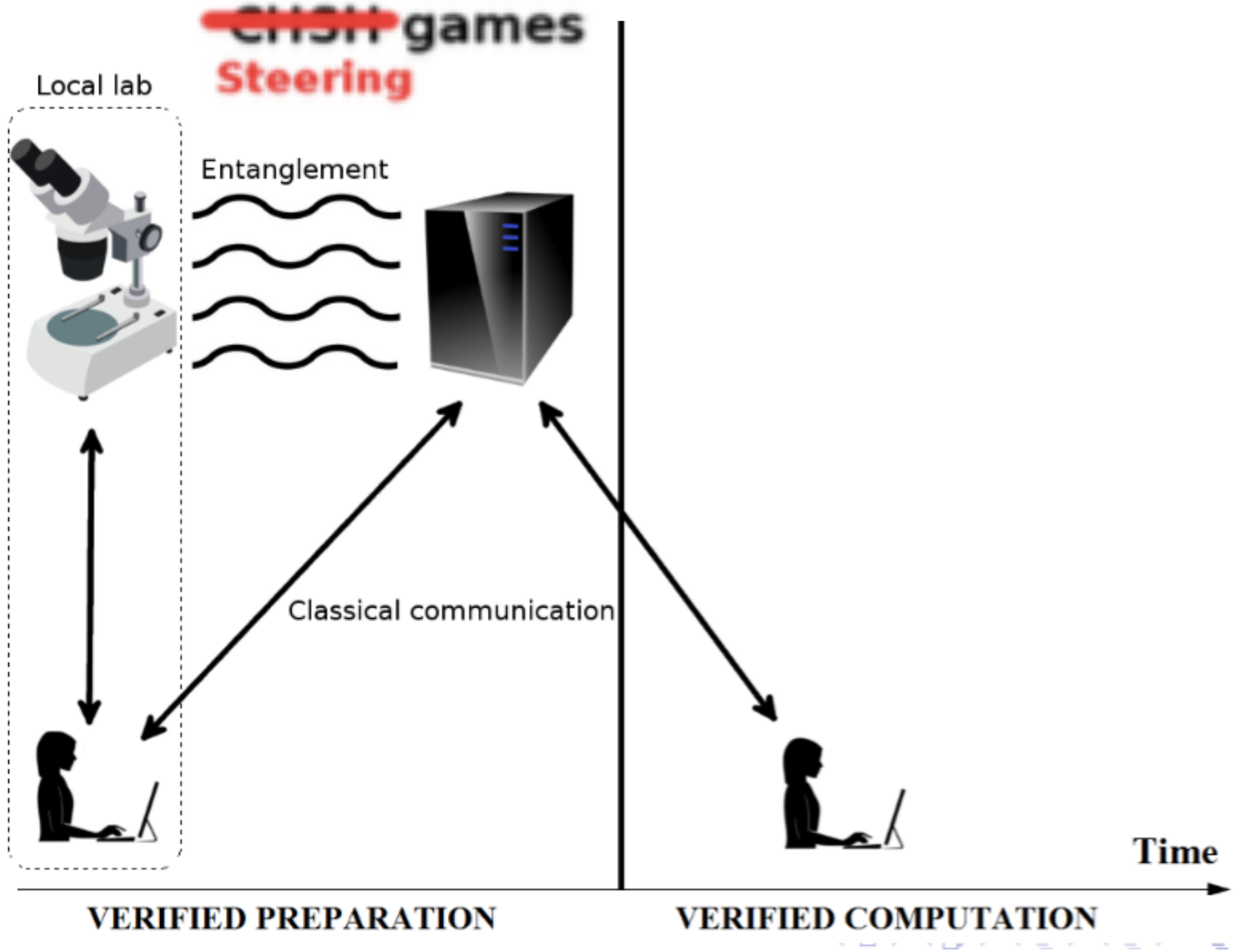


- Based on rigidity of CHSH games
- Certify tensor product of Bell pairs
- Certify correct measurements
- Verified preparation of single random qubit
- Verified computation = previous linear protocol

Round complexity: $O(N^{64})$

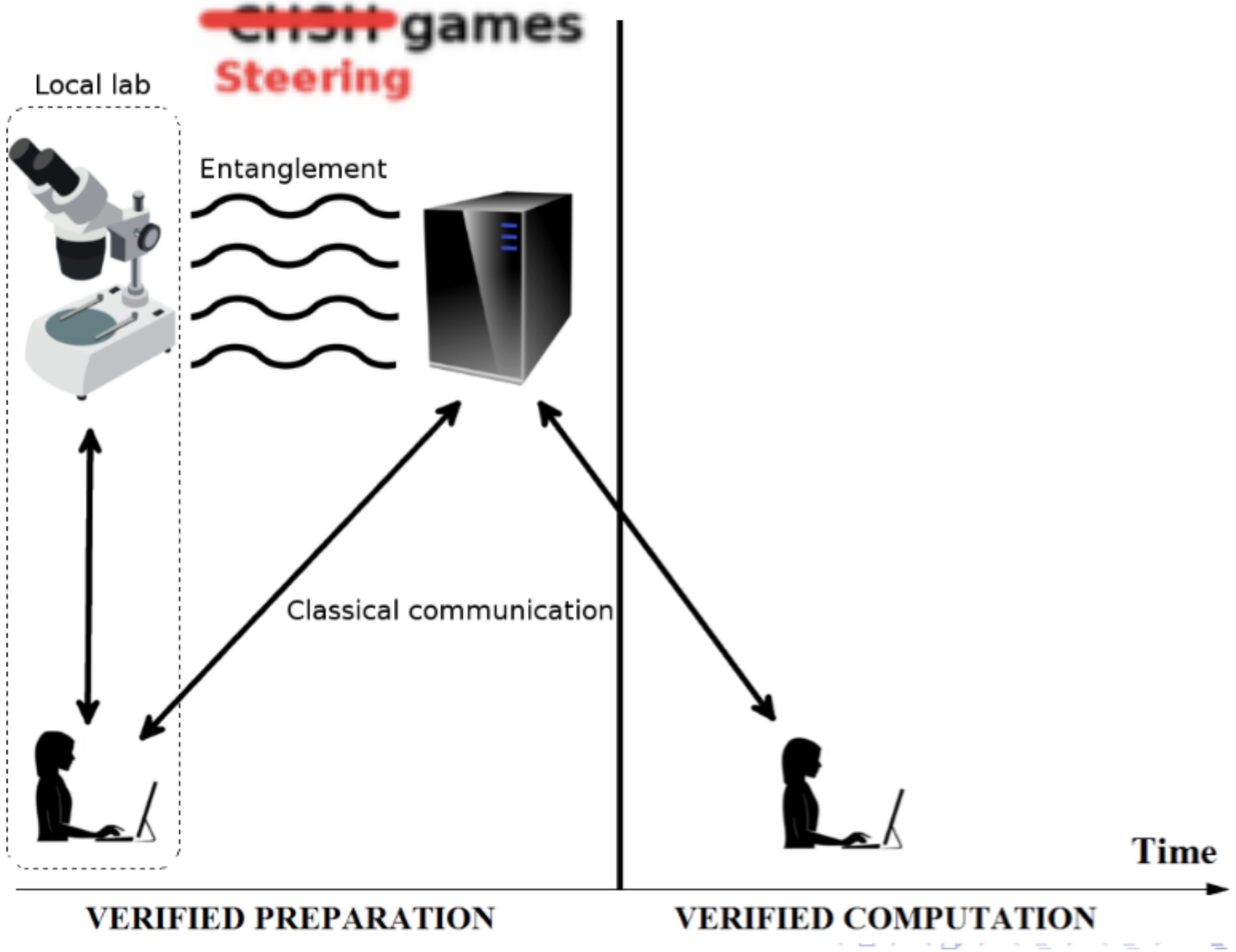
MDI - Verification

Kashefi et.al.
Semi-Device independent
VUBQC
New Journal of Physics 2016



MDI - Verification

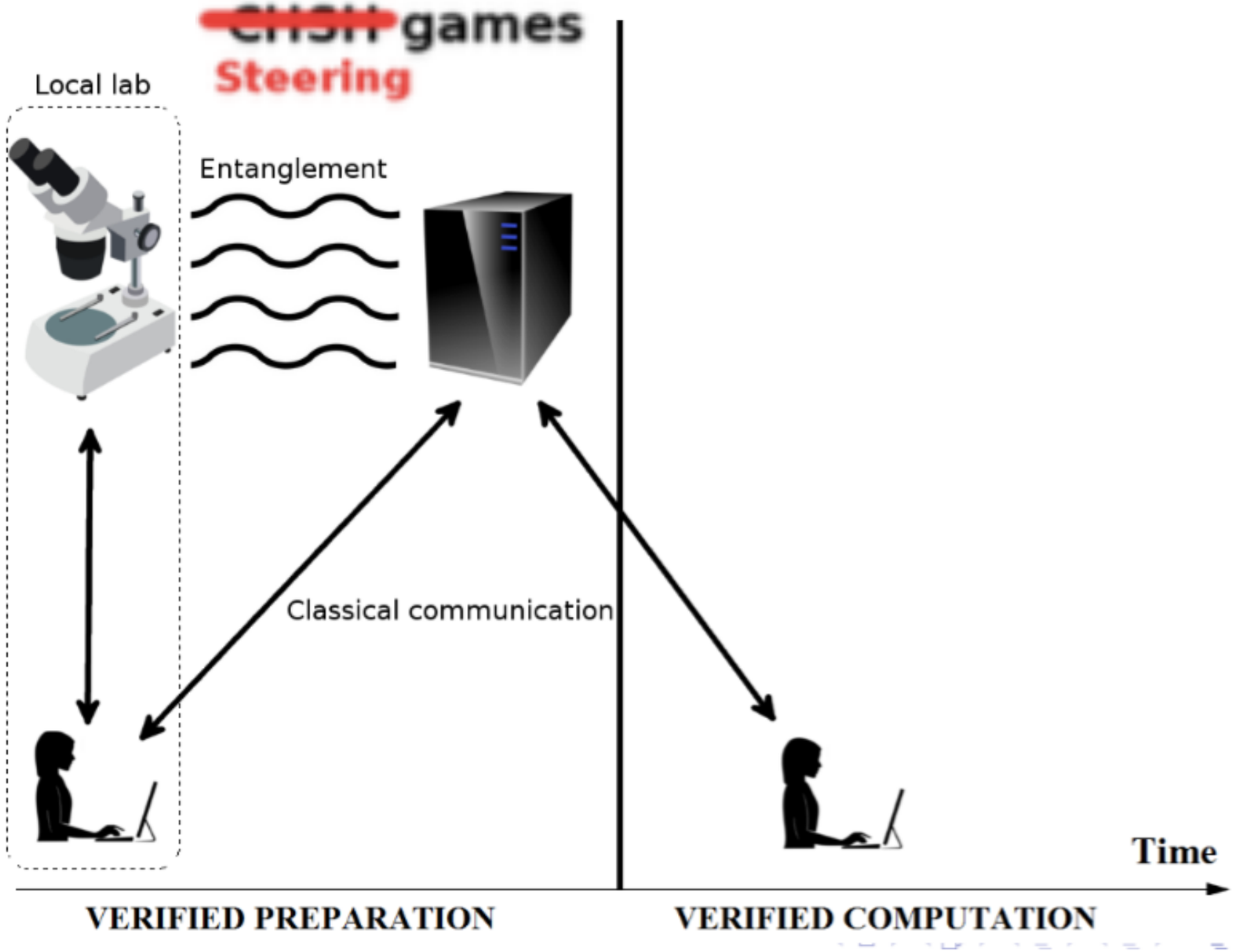
Kashefi et.al.
Semi-Device independent
VUBQC
New Journal of Physics 2016



- Based on rigidity of Steering games
- Certify tensor product of Bell pairs
- Certify correct measurements
- Reduced overhead because of added trust

MDI - Verification

Kashefi et.al.
Semi-Device independent
VUBQC
New Journal of Physics 2016



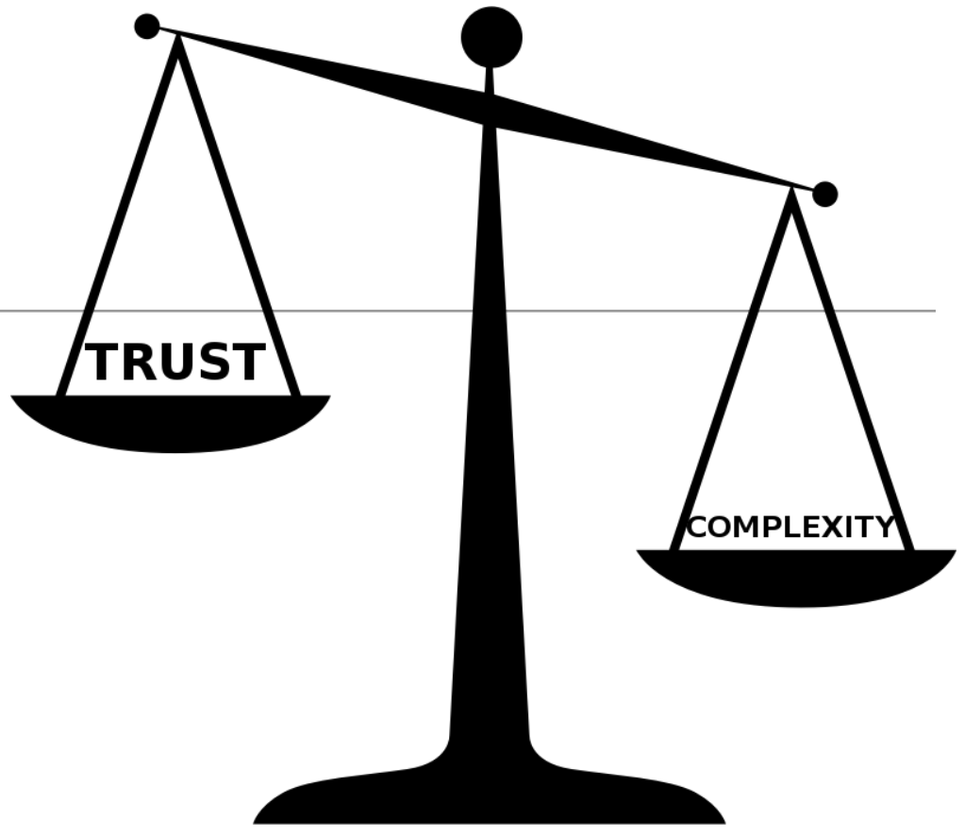
- Based on rigidity of Steering games
- Certify tensor product of Bell pairs
- Certify correct measurements
- Reduced overhead because of added trust

Round complexity: $O(N^{13})$

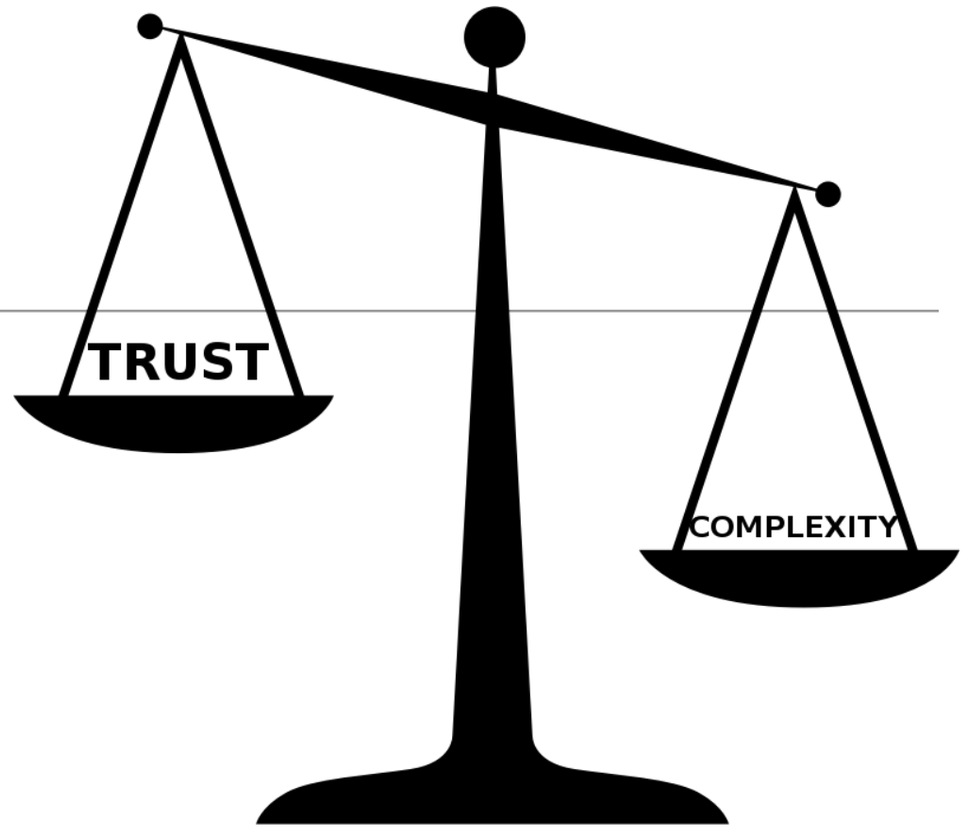
Summery of Entangled Provers

Protocol	Provers	Qmem provers	Rounds	Communication	Blind
RUV	2	2	$O(N^{8192} \cdot log(1/\epsilon))$	$O(N^{8192} \cdot log(1/\epsilon))$	Y
McKague	$O(N^{22} \cdot log(1/\epsilon))$	0	$O(N^{22} \cdot log(1/\epsilon))$	$O(N^{22} \cdot log(1/\epsilon))$	Y
GKW	2	1	$O(N^{2048} \cdot log(1/\epsilon))$	$O(N^{2048} \cdot log(1/\epsilon))$	Y
HPDF	$O(N^4 log(N) \cdot log(1/\epsilon))$	$O(log(1/\epsilon))$	$O(N^4 log(N) \cdot log(1/\epsilon))$	$O(N^4 log(N) \cdot log(1/\epsilon))$	Y
FH	5	5	$O(N^{16} \cdot log(1/\epsilon))$	$O(N^{19} \cdot log(1/\epsilon))$	N
NV	7	7	$O(1)$	$O(N^3 \cdot log(1/\epsilon))$	N

Price of Trust

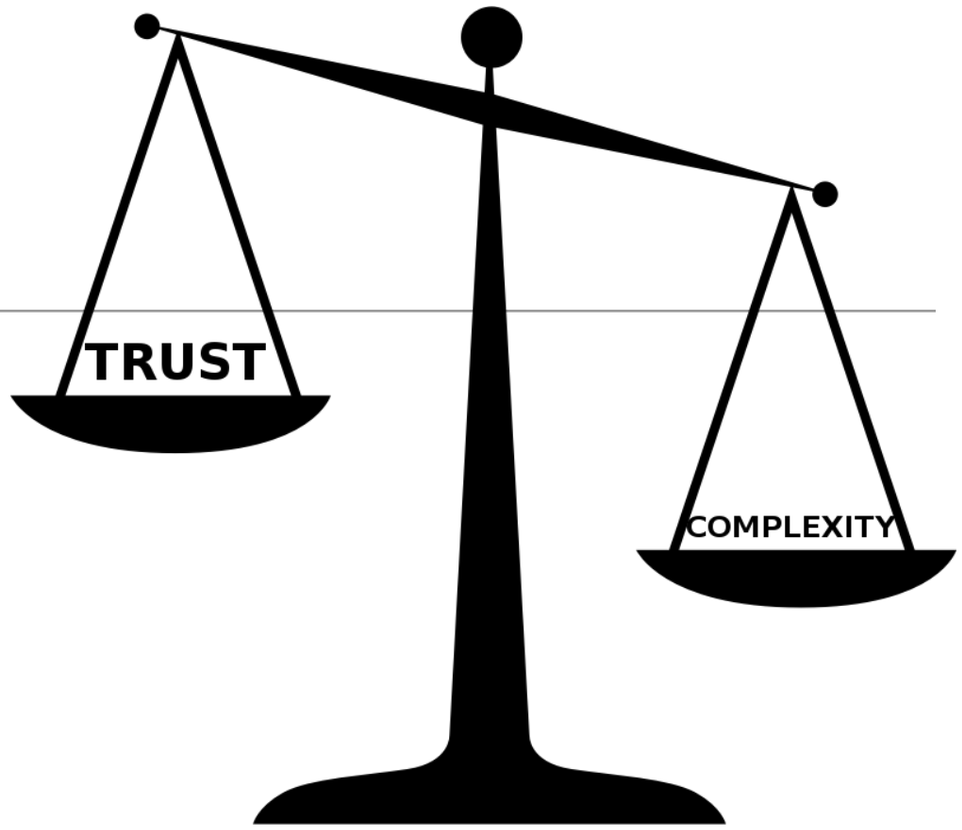


Price of Trust

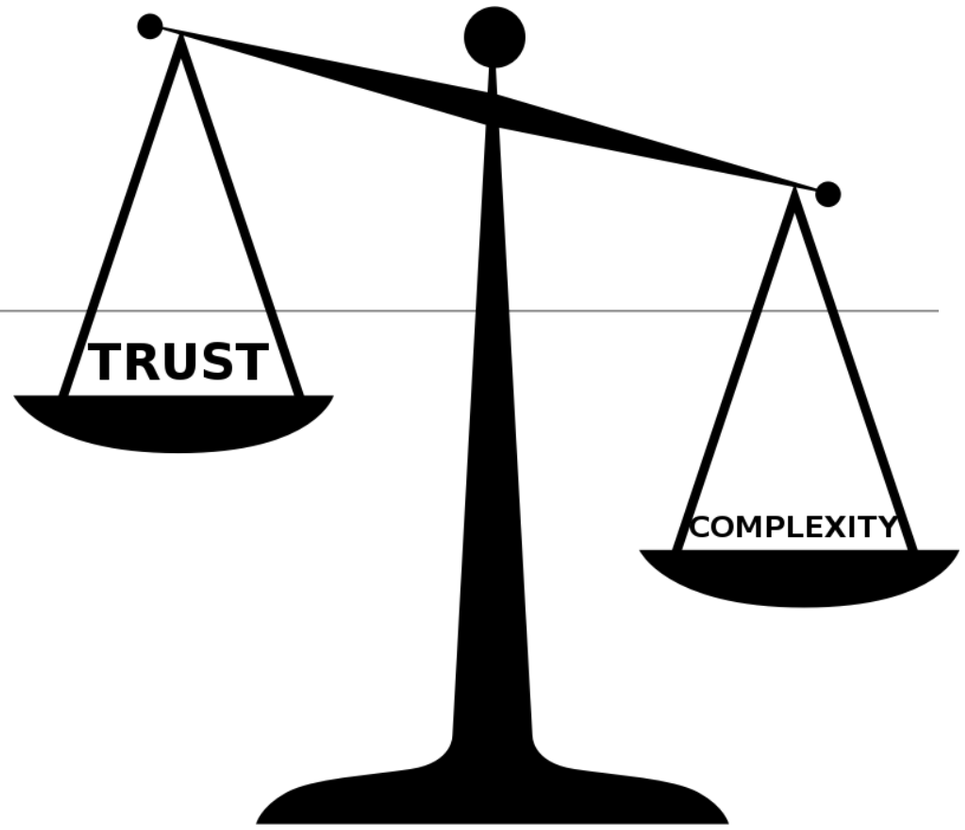


- Prepare and send vs. entanglement-based
- Single vs. multiple servers
- Online vs. offine
- Device-independent vs. one-sided device-independent
- I.I.D. states vs. general states
- Privacy preserving vs non-hiding
- Universal vs non-universal
- And many others

Price of Trust

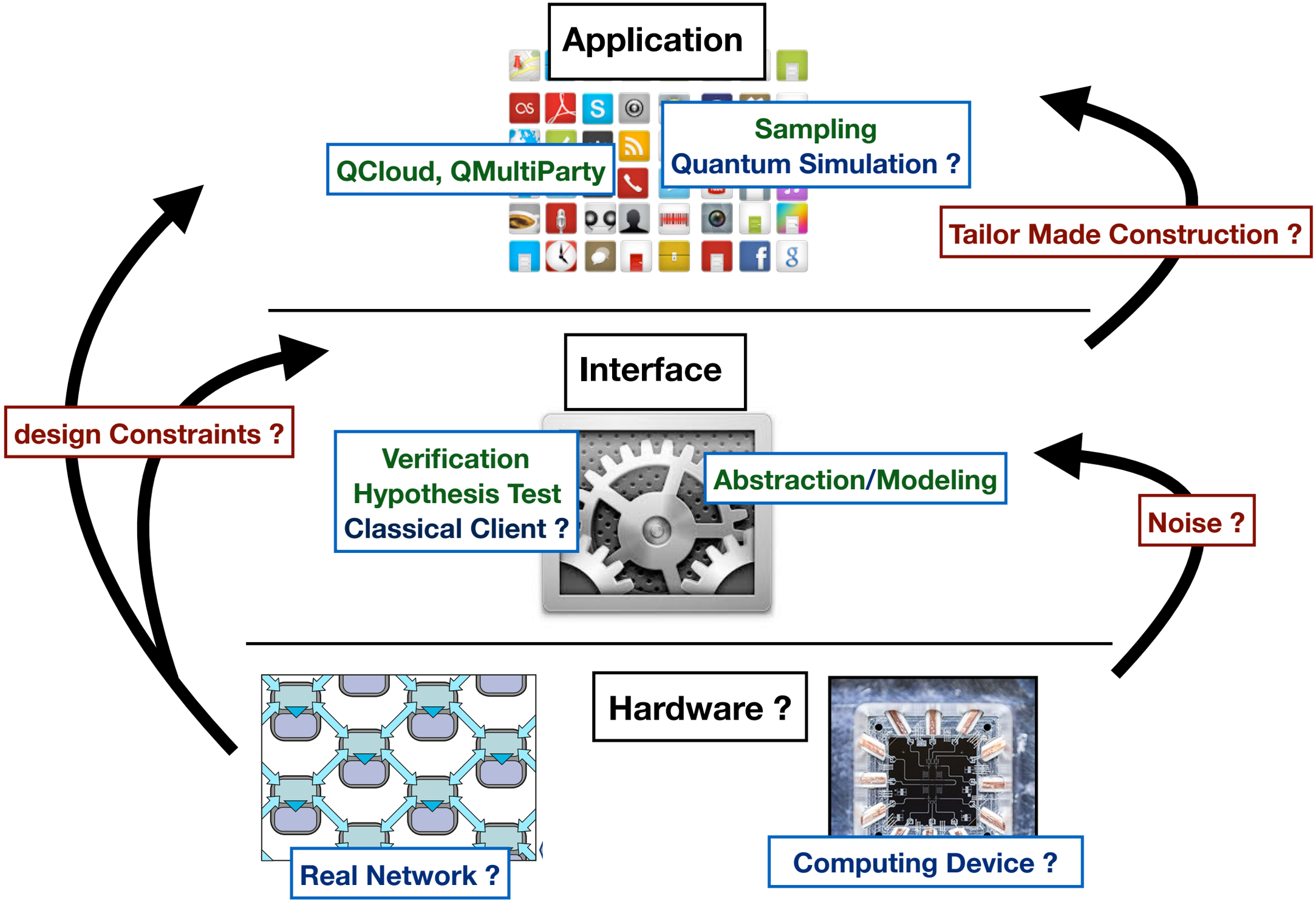


Price of Trust



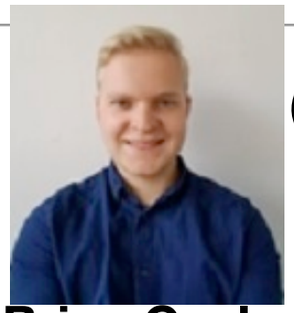
- Prepare and send vs. entanglement-based
- Single vs. multiple servers
- Online vs. offine
- Device-independent vs. one-sided device-independent
- I.I.D. states vs. general states
- Privacy preserving vs non-hiding
- Universal vs non-universal
- And many others

Where we stand



The Edinburgh-Paris Team

Daniel Mills



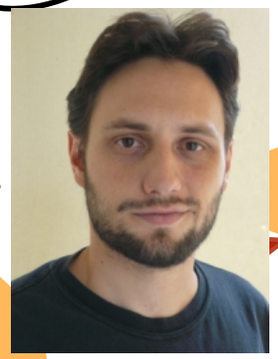
Brian Coyle

Research

Certification

Verification

Multi-party QC



Petros Wallden

Luka Music

Andru Gheorghiu

Alexandru Cojocaru

Q-enhanced Cloud

Tom Douce

In the lab

Ulysse Chabaud

Ellen Derbyshire

Deployment

Development

Interns:

- Ieva Cepaite
- Iskren Vankov
- Phivos Sofokleous
- Kelsey Horan
- Léo Colisson

Other collaborators

Theory

Joe Fitzsimons (SUTD)
Anna Pappa (UCL)
Anne Broadbent (Ottawa)
Vedran Dunjko (Innsbruck)
Anthony Leverrier (INREA)
Animesh Datta (Warwick)
Theodoros Kapourniotis (Warwick)

Experiment

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

Other collaborators

Theory

Joe Fitzsimons (SUTD)
Anna Pappa (UCL)
Anne Broadbent (Ottawa)
Vedran Dunjko (Innsbruck)
Anthony Leverrier (INREA)
Animesh Datta (Warwick)
Theodoros Kapourniotis (Warwick)

Experiment

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

AIR FORCE OFFICE OF SCIENTIFIC RESEARCH
UNITED STATES AIR FORCE

EPSRC
Engineering and Physical Sciences Research Council

NQIT

UK NATIONAL QUANTUM TECHNOLOGIES PROGRAMME