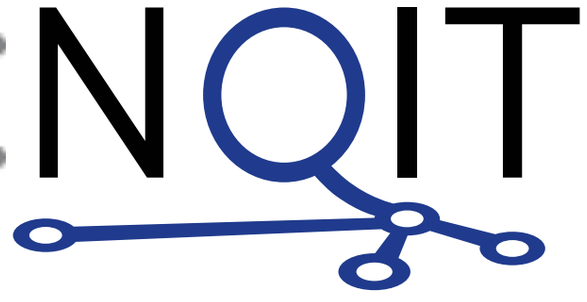
Verification of Quantum Computing

Elham Kashefi

University of Edinburgh
CNRS, Pierre and Marie Curie University

Oxford Quantum Technology Hub
Paris Centre for Quantum Computing



Quantum Software Mission

Develop knowledge and expertise
for science, technology and business

to **evaluate** and **program** today's quantum devices

so we can effectively exploit tomorrow's

Quantum Software Mission

Develop knowledge and expertise
for science, technology and business

to **evaluate** and **program** today's quantum devices

so we can effectively exploit tomorrow's

- What it is good for ?
- Is it working ?

Quantum Software Mission

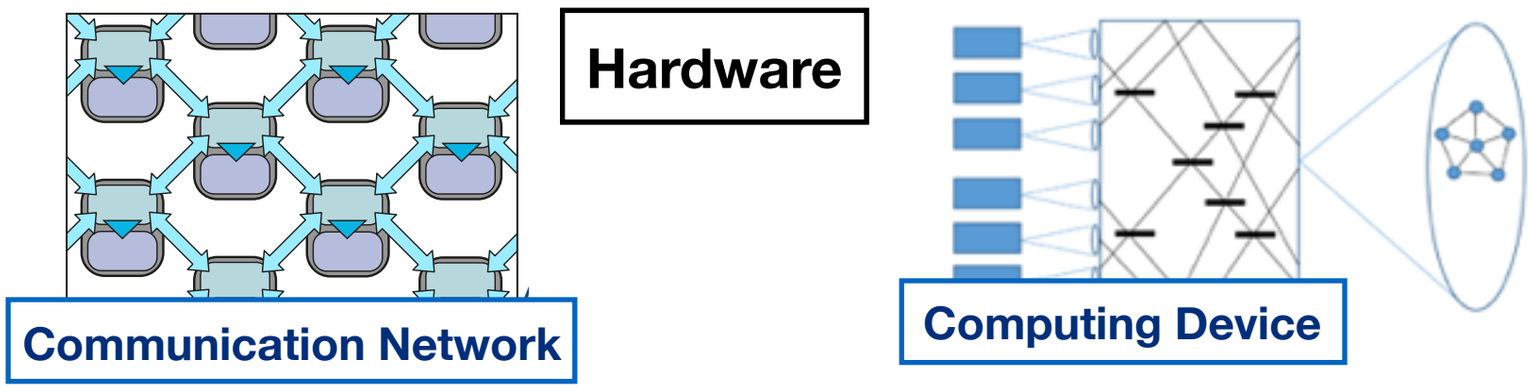
Develop knowledge and expertise
for science, technology and business

to **evaluate** and **program** today's quantum devices
so we can effectively exploit tomorrow's

- **What it is good for ?**
- **Is it working ?**

- **How much details do I need to know ?**
- **How could I encode my computation ?**

QSoft Vision of Quantum Technology



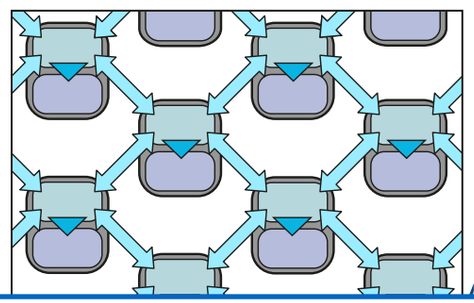
QSoft Vision of Quantum Technology

Interface

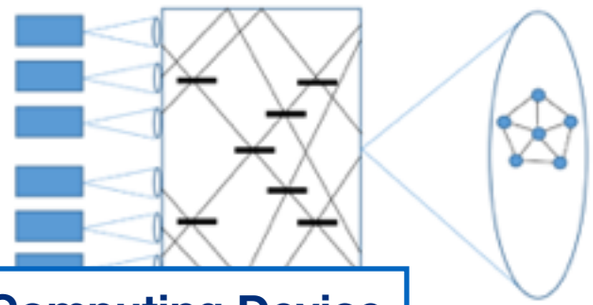
Verification/Benchmarking

Abstraction/Modeling/Encoding

Hardware

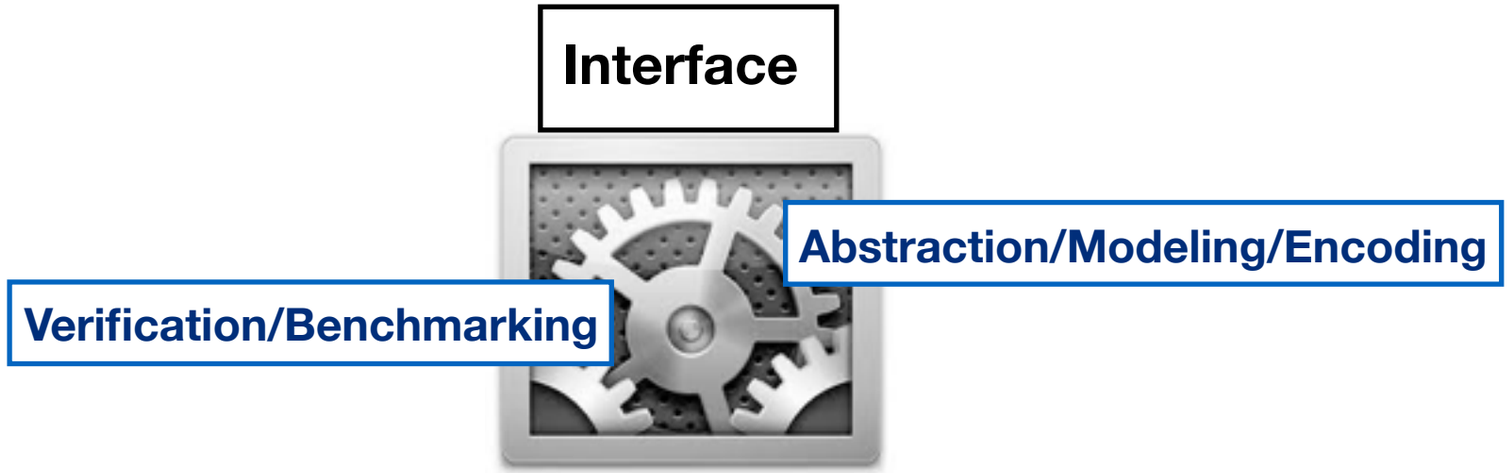


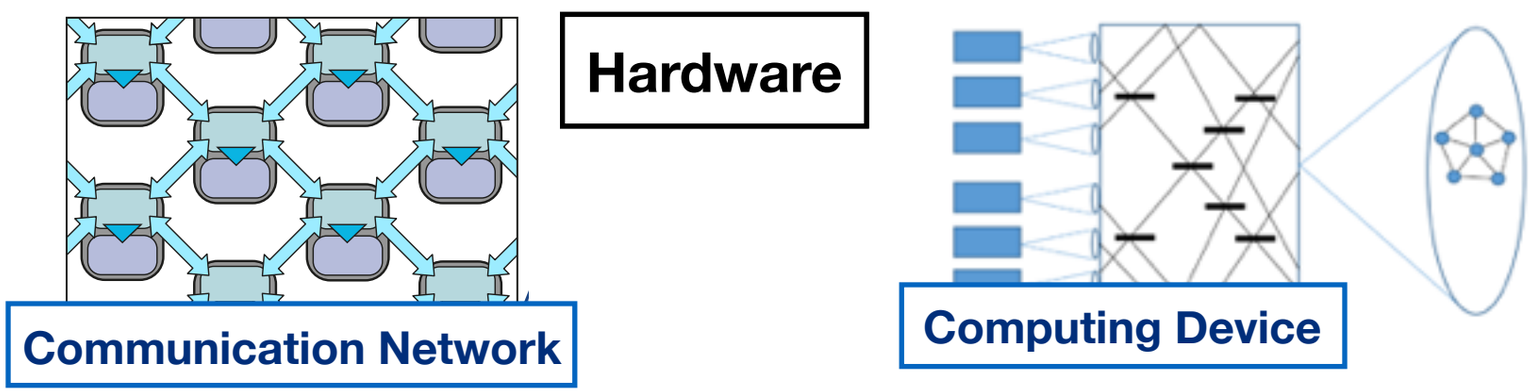
Communication Network



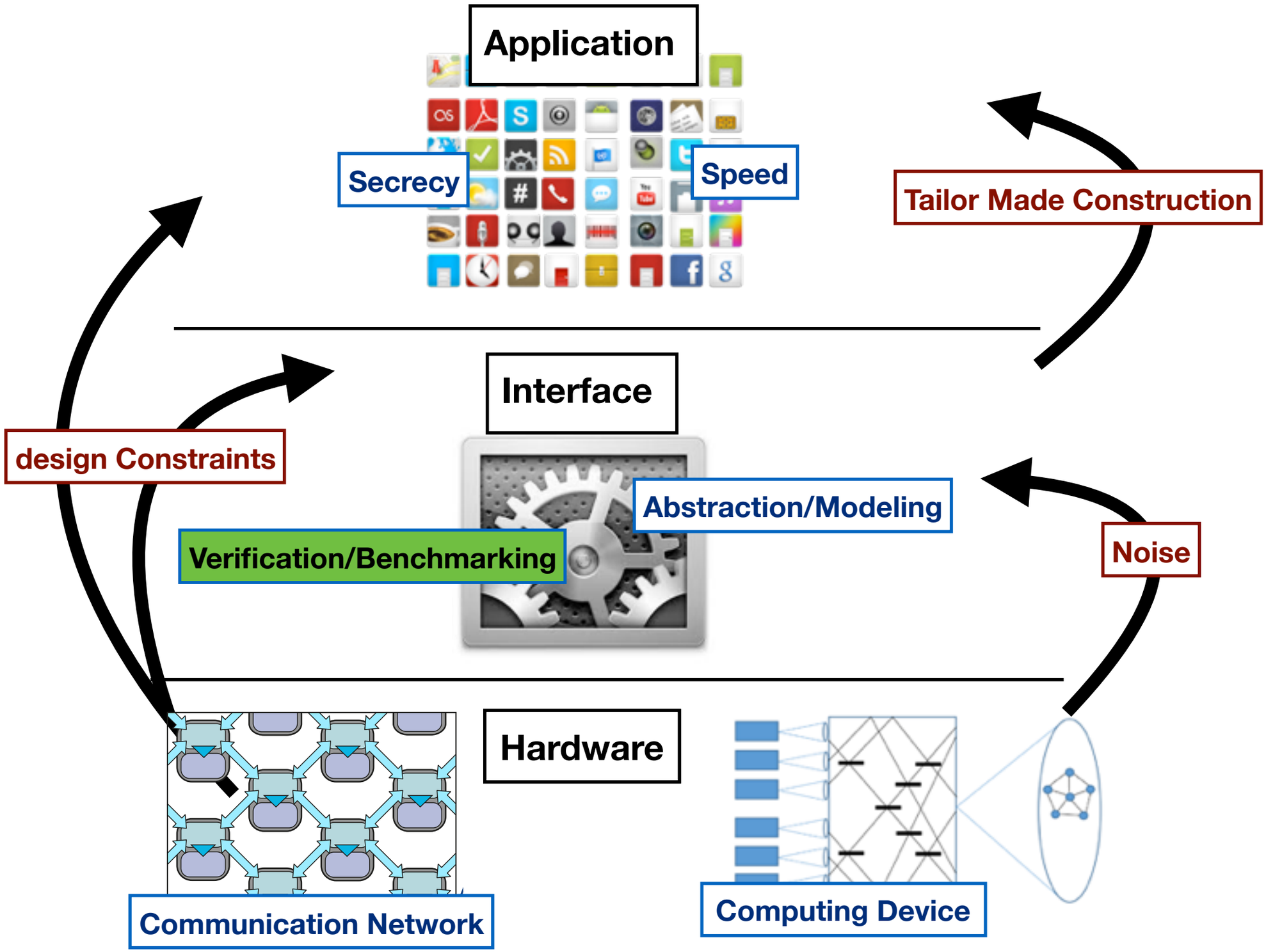
Computing Device

QSoft Vision of Quantum Technology





QSoft Vision of Quantum Technology



What is Verification

What is Verification

Sensors and Metrology:	Certification of Enhancement

What is Verification

Sensors and Metrology: Certification of Enhancement

Simulation: Validation

What is Verification

Sensors and Metrology: Certification of Enhancement

Simulation: Validation

Communications: Adversarial detection

What is Verification

Sensors and Metrology: Certification of Enhancement

Simulation: Validation

Communications: Adversarial detection

Computations: Correctness

Quantum Era

National Investments

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

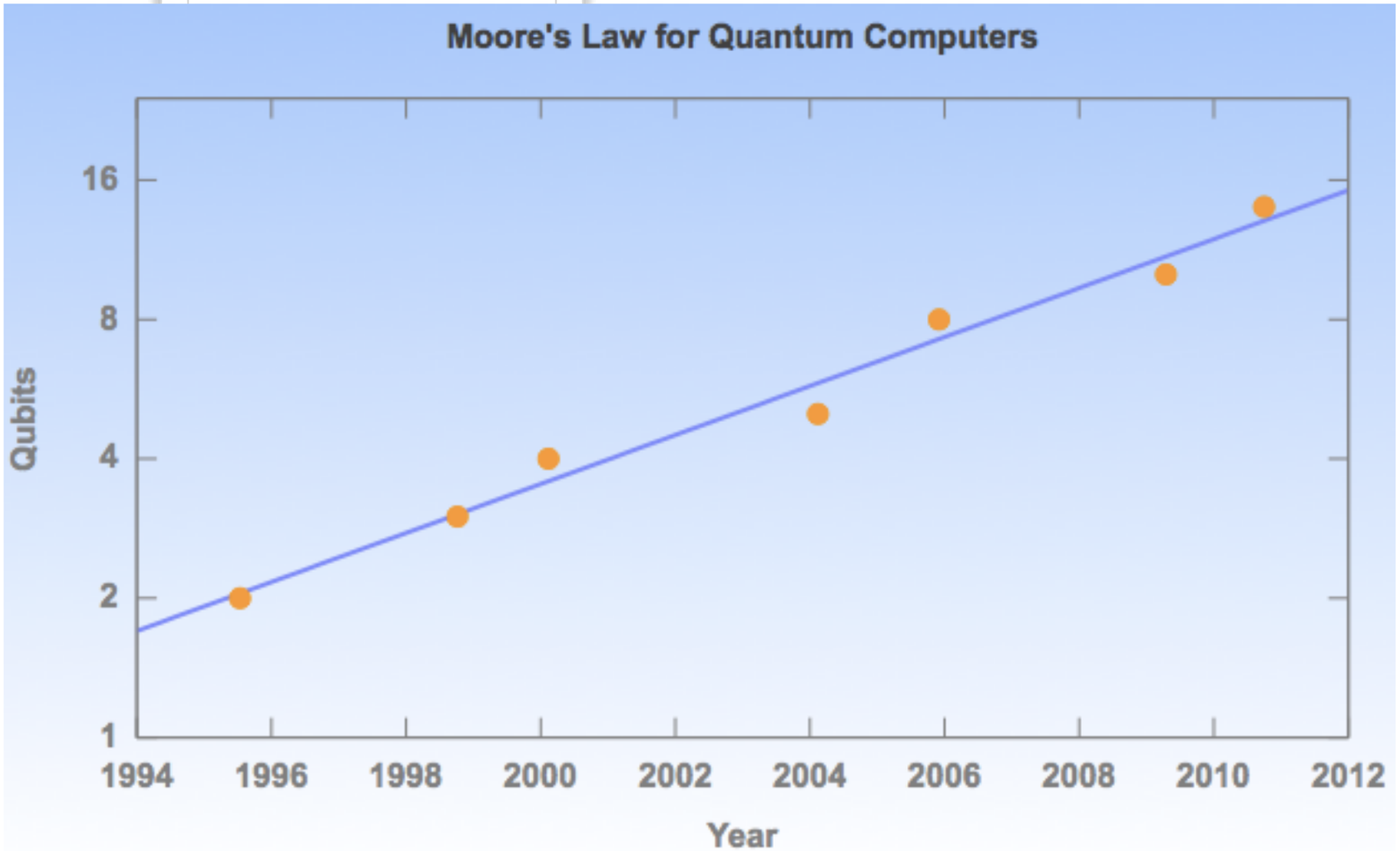
Quantum Machines

Private Investments

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

Quantum Era

National Investments

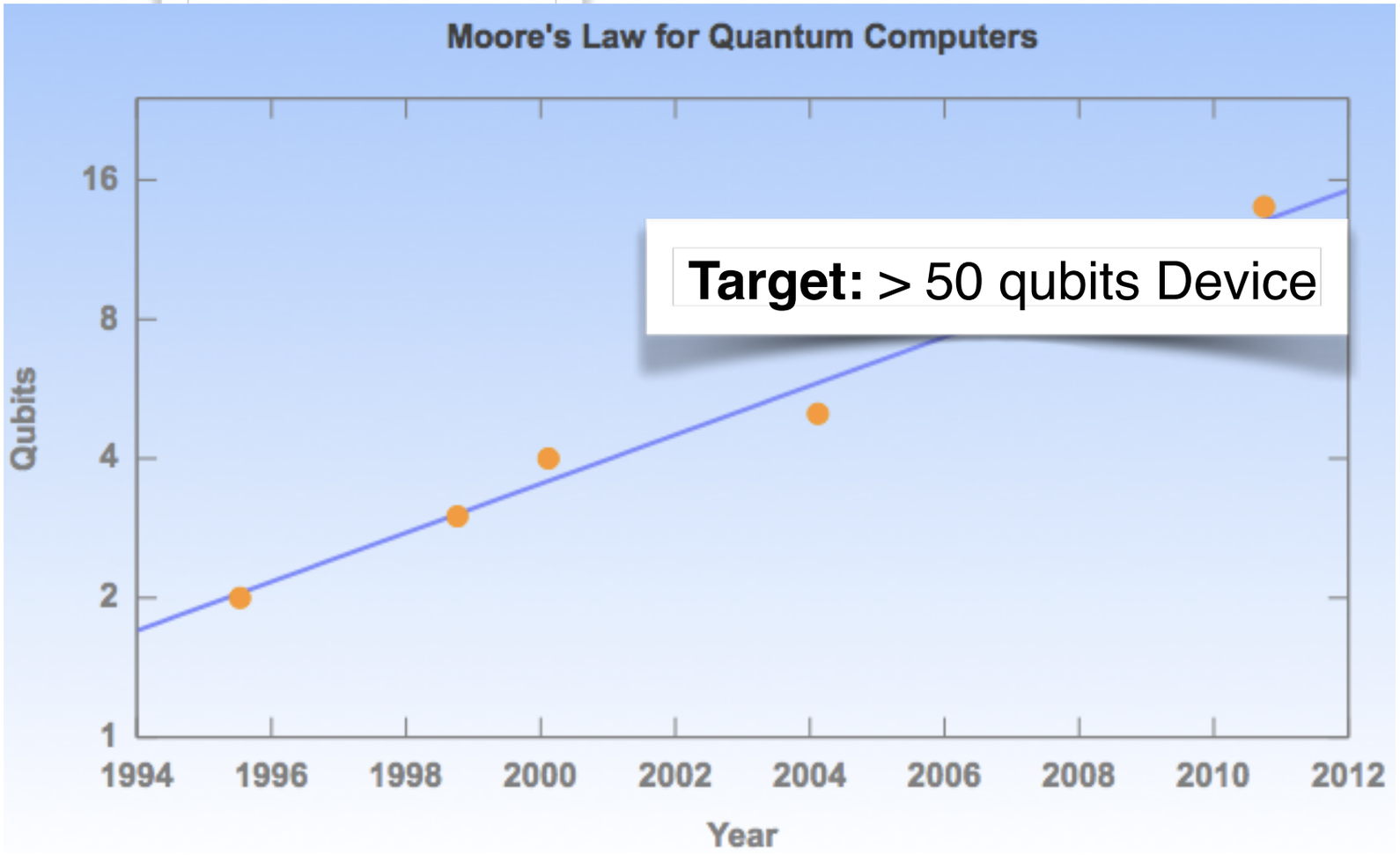


Private Investments

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

Quantum Era

National Investments

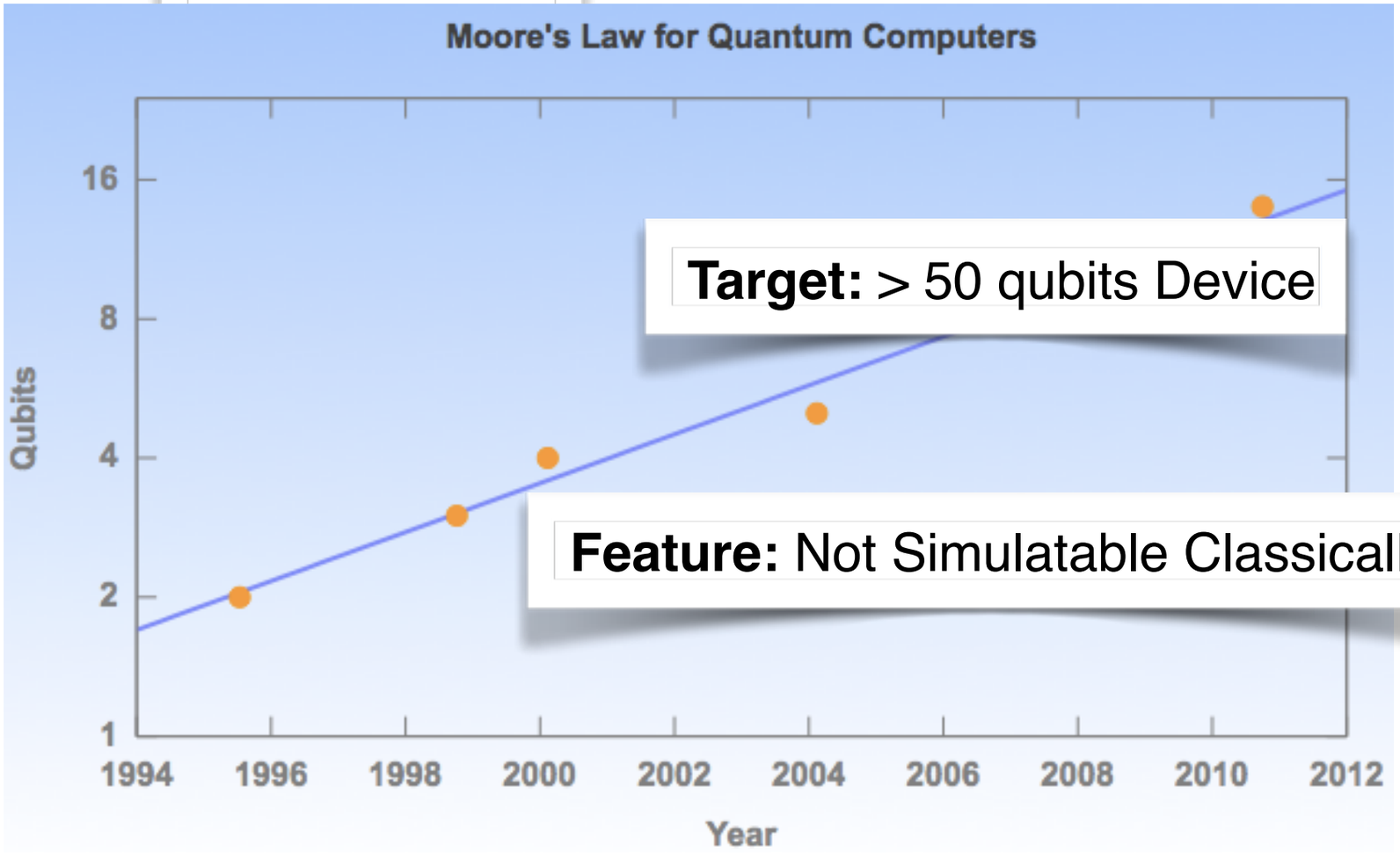


Private Investments

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

Quantum Era

National Investments

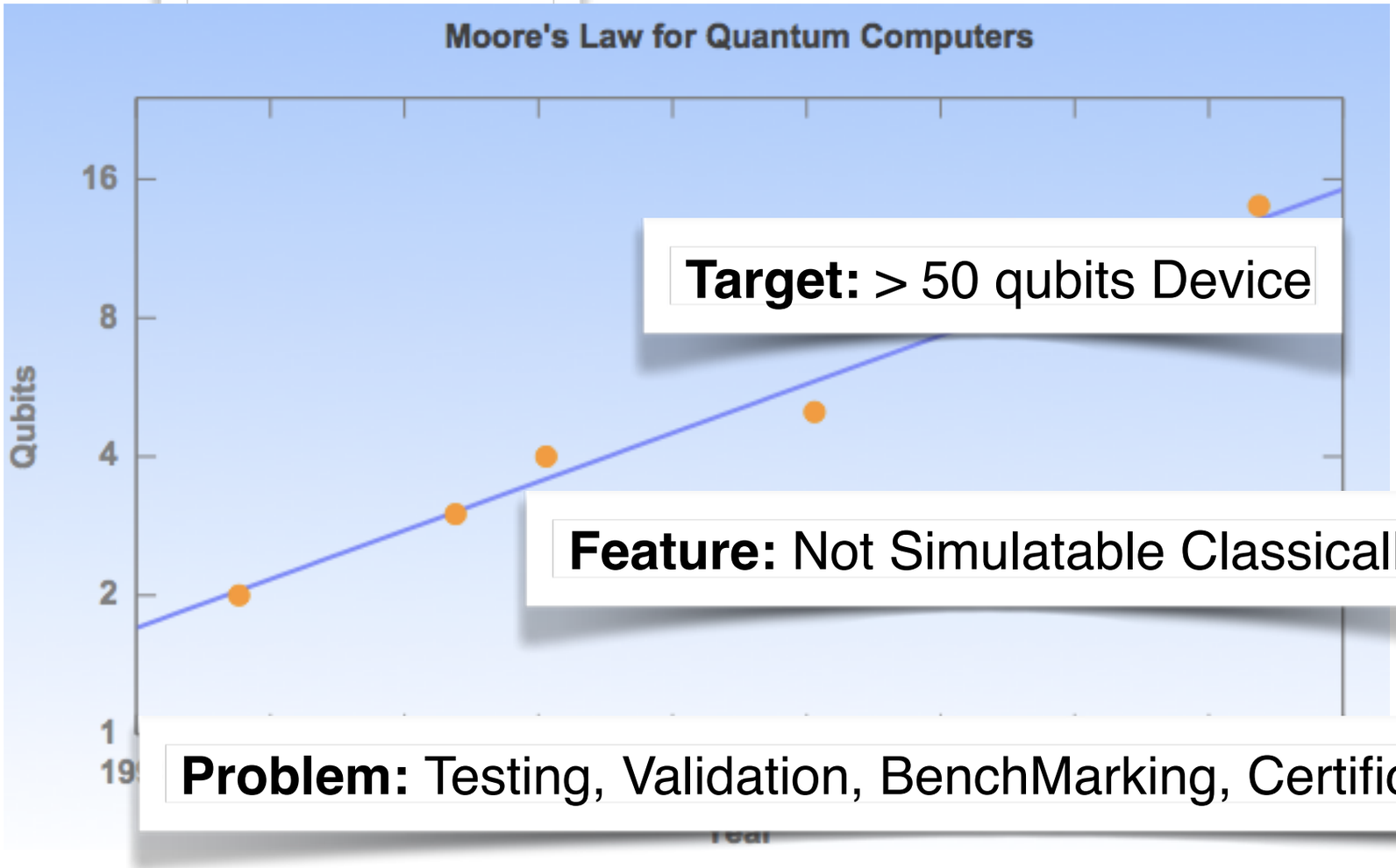


Private Investments

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

Quantum Era

National Investments

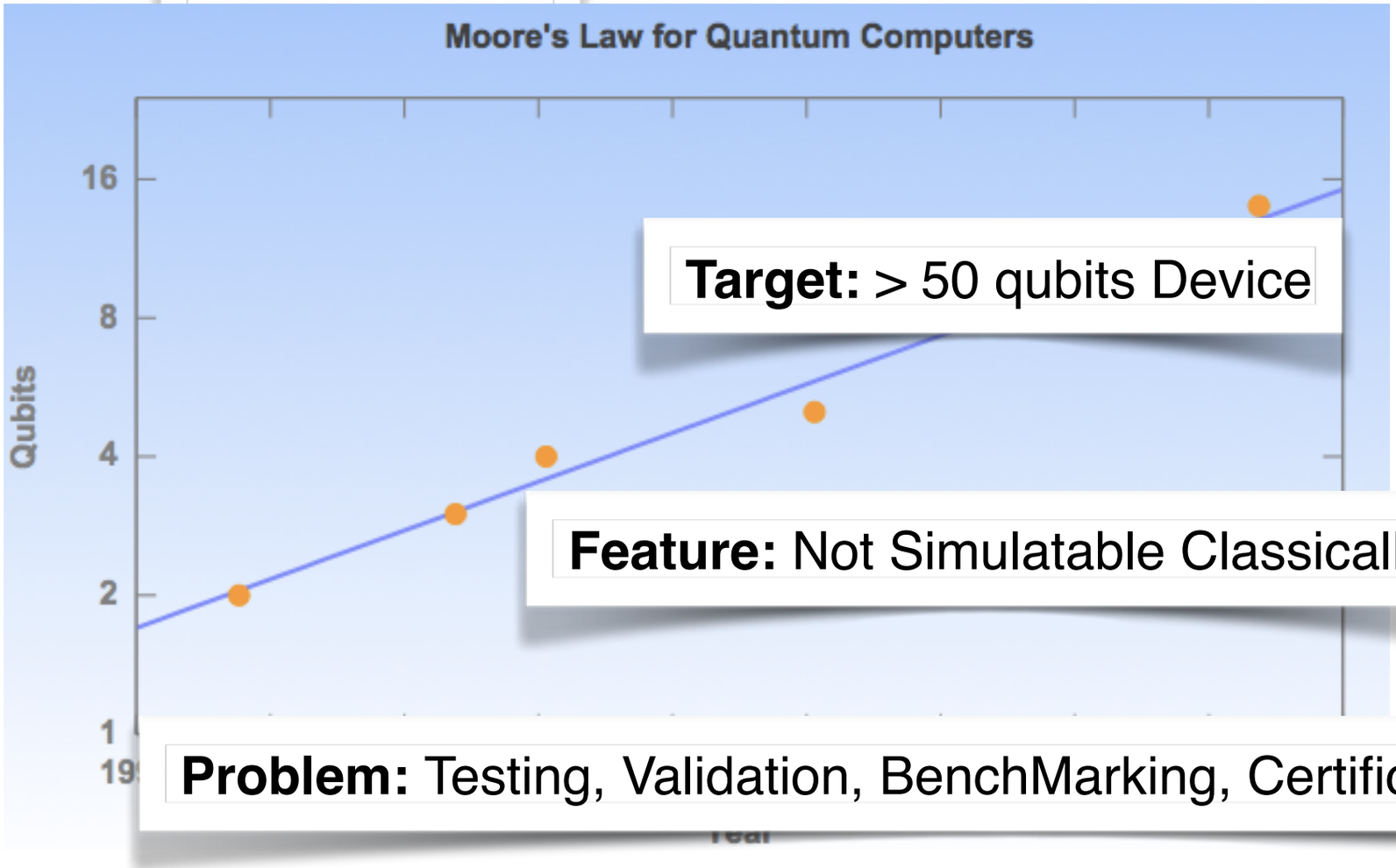


Private Investments

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

Quantum Era

National Investments



Private Investments

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

We can BOOTSTRAP a smaller quantum device to test a bigger one

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**

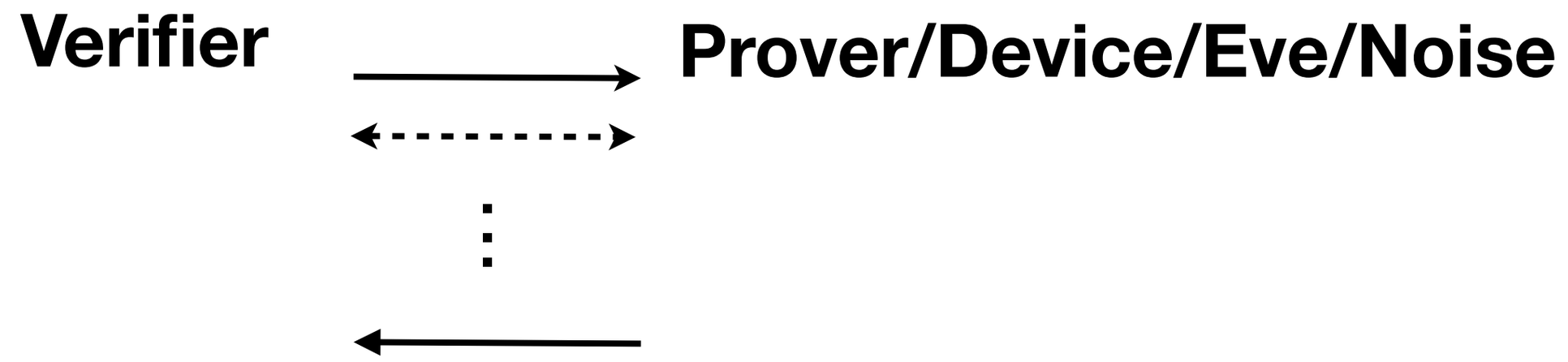
A mechanism that **probability** of witness is accepted and the outcome is **bad is bounded**

What is Verification

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

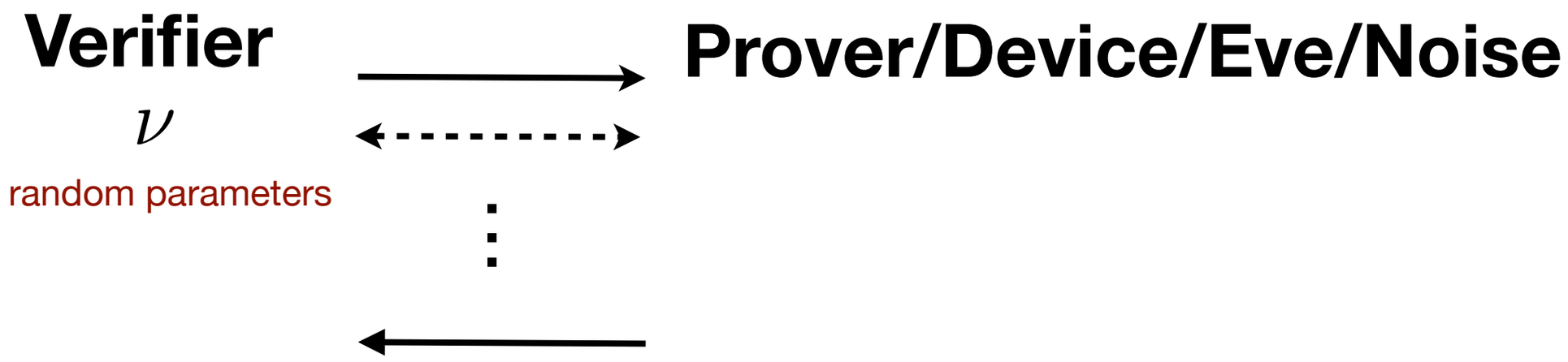
What is Verification

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



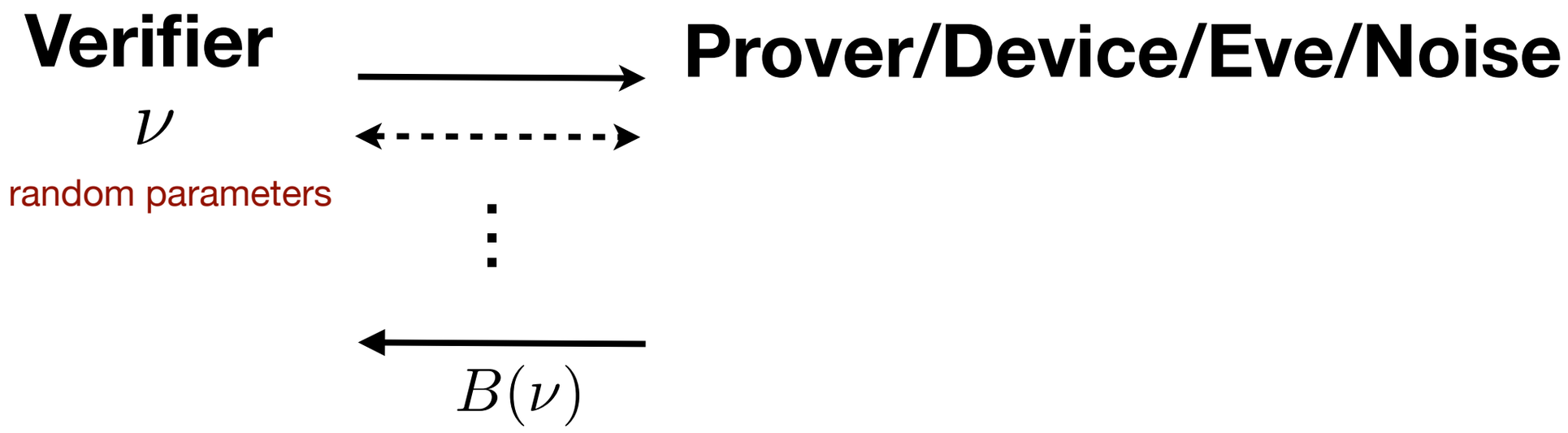
What is Verification

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



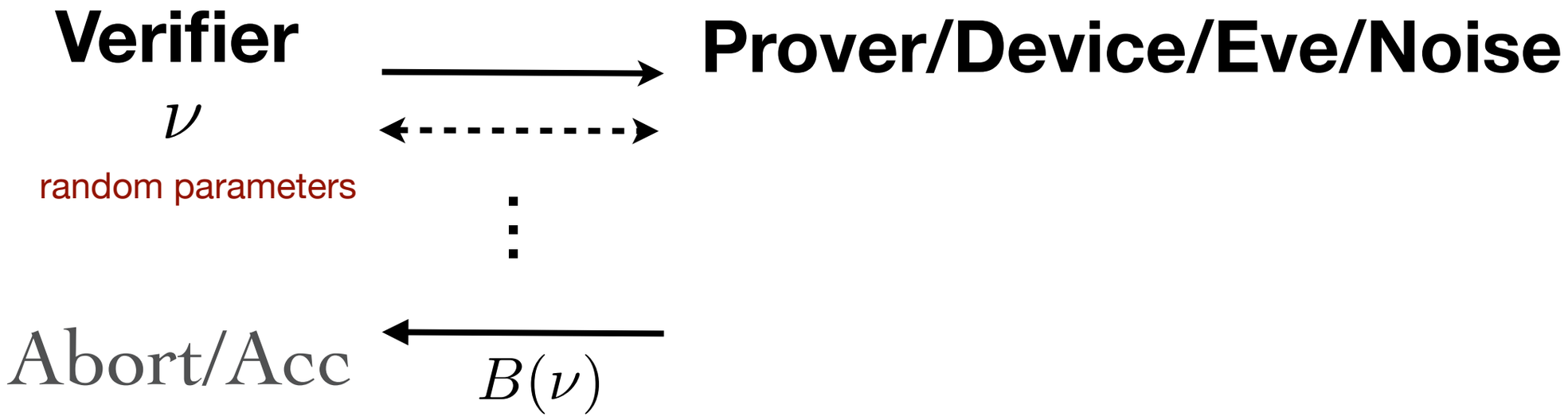
What is Verification

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

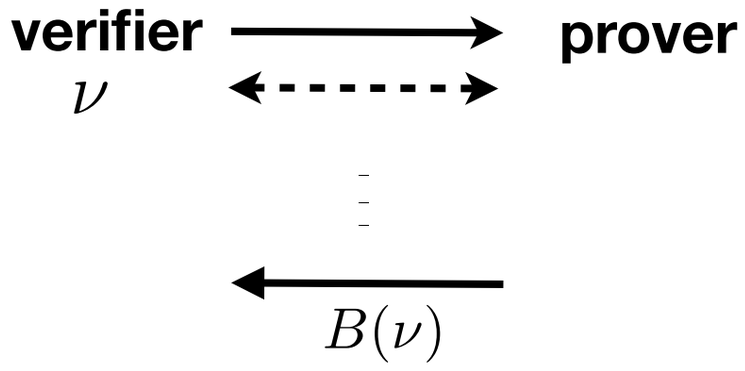


What is Verification

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

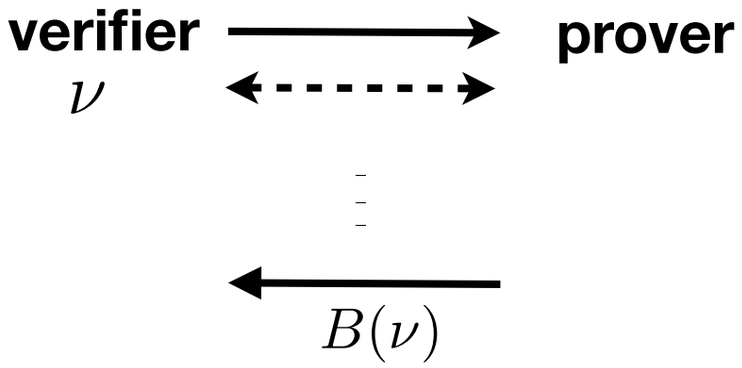


What is Verification



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

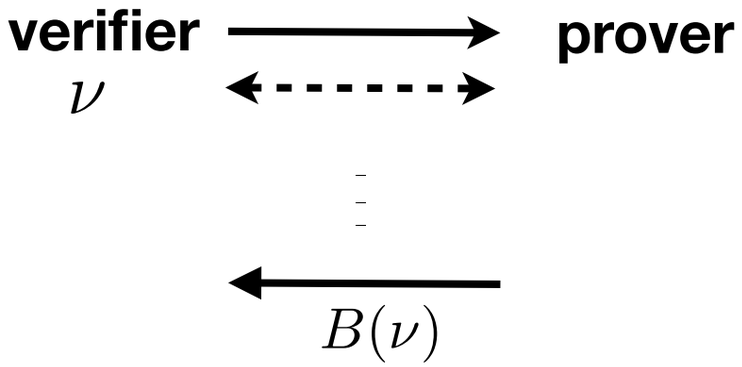
What is Verification



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

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

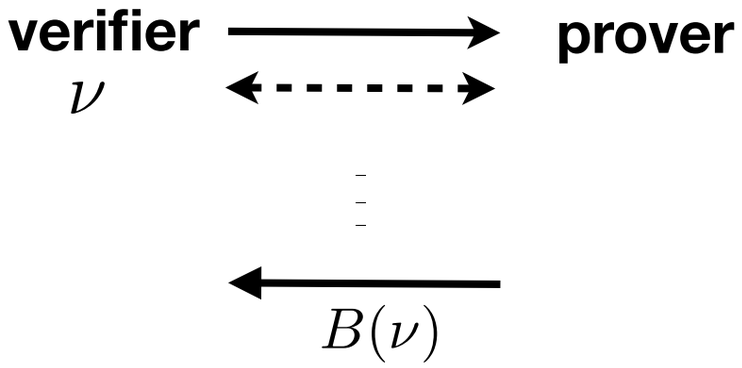
What is Verification



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

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

What is Verification

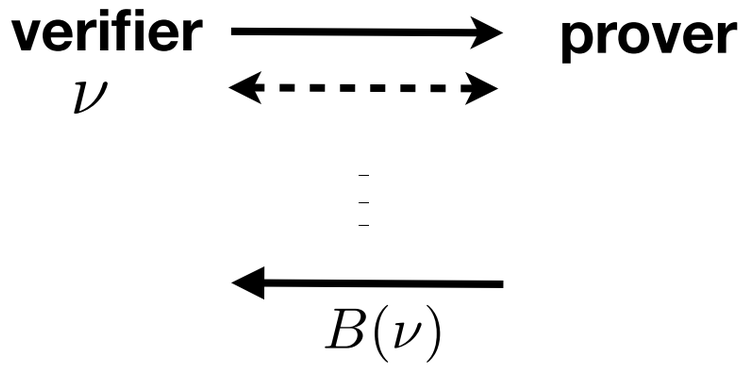


$$P^{\nu}_{incorrect} := P_{\perp} \otimes |acc\rangle\langle acc|$$

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

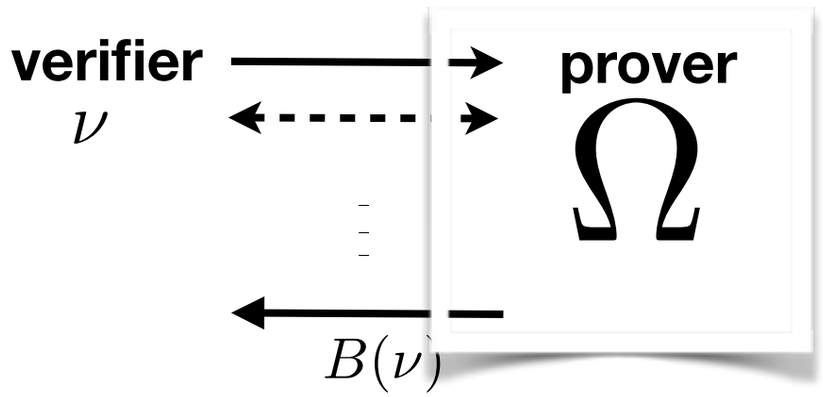


$$P^{\nu}_{incorrect} := P_{\perp} \otimes |acc\rangle\langle acc|$$

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

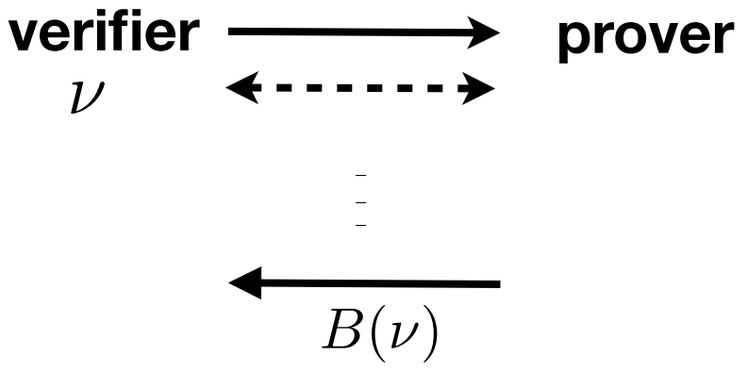


$$P^{\nu}_{incorrect} := P_{\perp} \otimes |acc\rangle\langle acc|$$

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

Most General Deviation

$$\Omega_{Eve,system}$$

cryptographic toolkit

Most General Deviation

$$\Omega_{Eve,system}$$

cryptographic toolkit

$$\sigma_{testsubspace}$$

Most General Deviation

$$\Omega_{Eve,system}$$

cryptographic toolkit

$$\sigma_{testsubspace}$$

Practical Protocols with No assumptions whatsoever

Most General Deviation

$$\Omega_{Eve,system}$$

arXiv:1709.06984

Verification of quantum computation:
An overview of existing approaches

Alexandru Gheorghiu, Theodoros Kapourniotis, Elham Kashefi

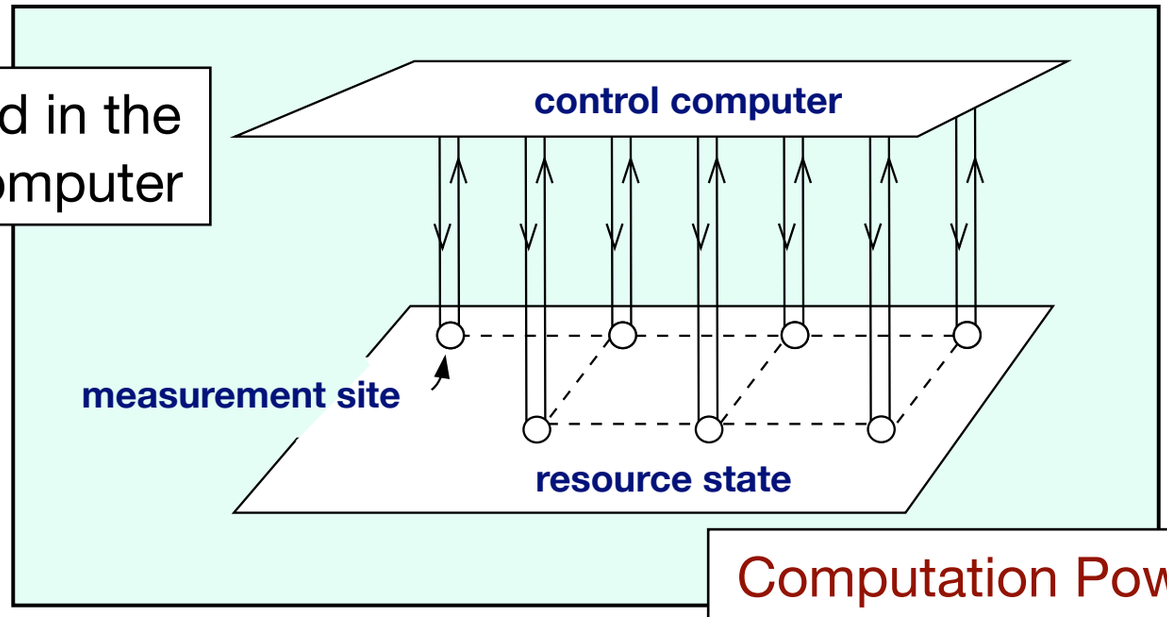
$$\sigma_{testsubspace}$$

Practical Protocols with No assumptions whatsoever

Classically-controlled QC

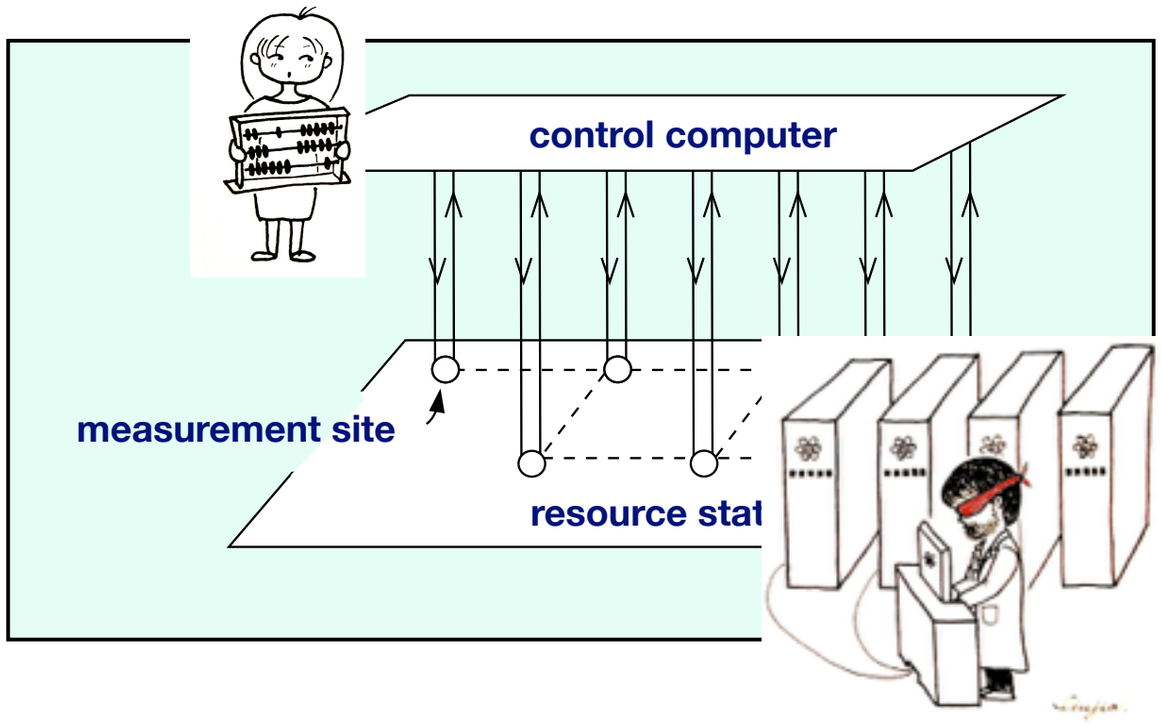
MBQC - Cluster State - Gate Teleportation

Program is encoded in the classical control computer

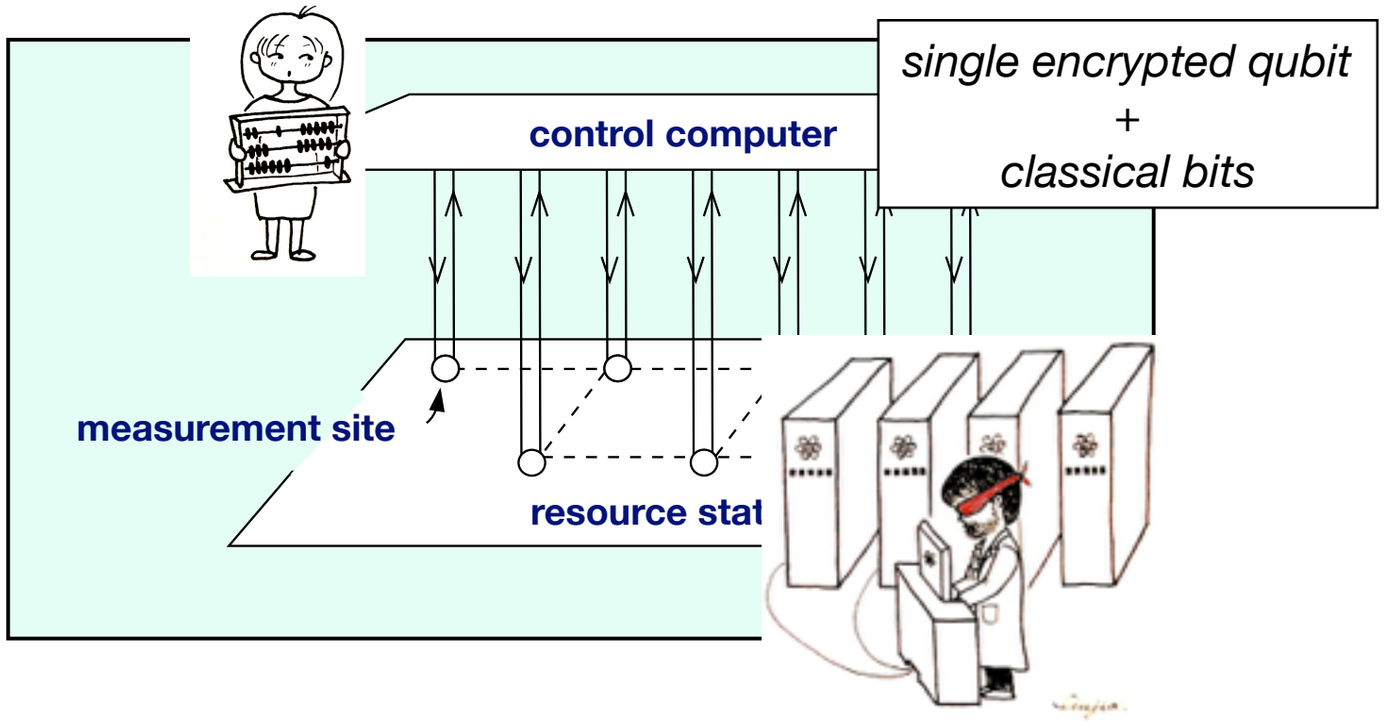


Computation Power is encoded in the quantum entanglement

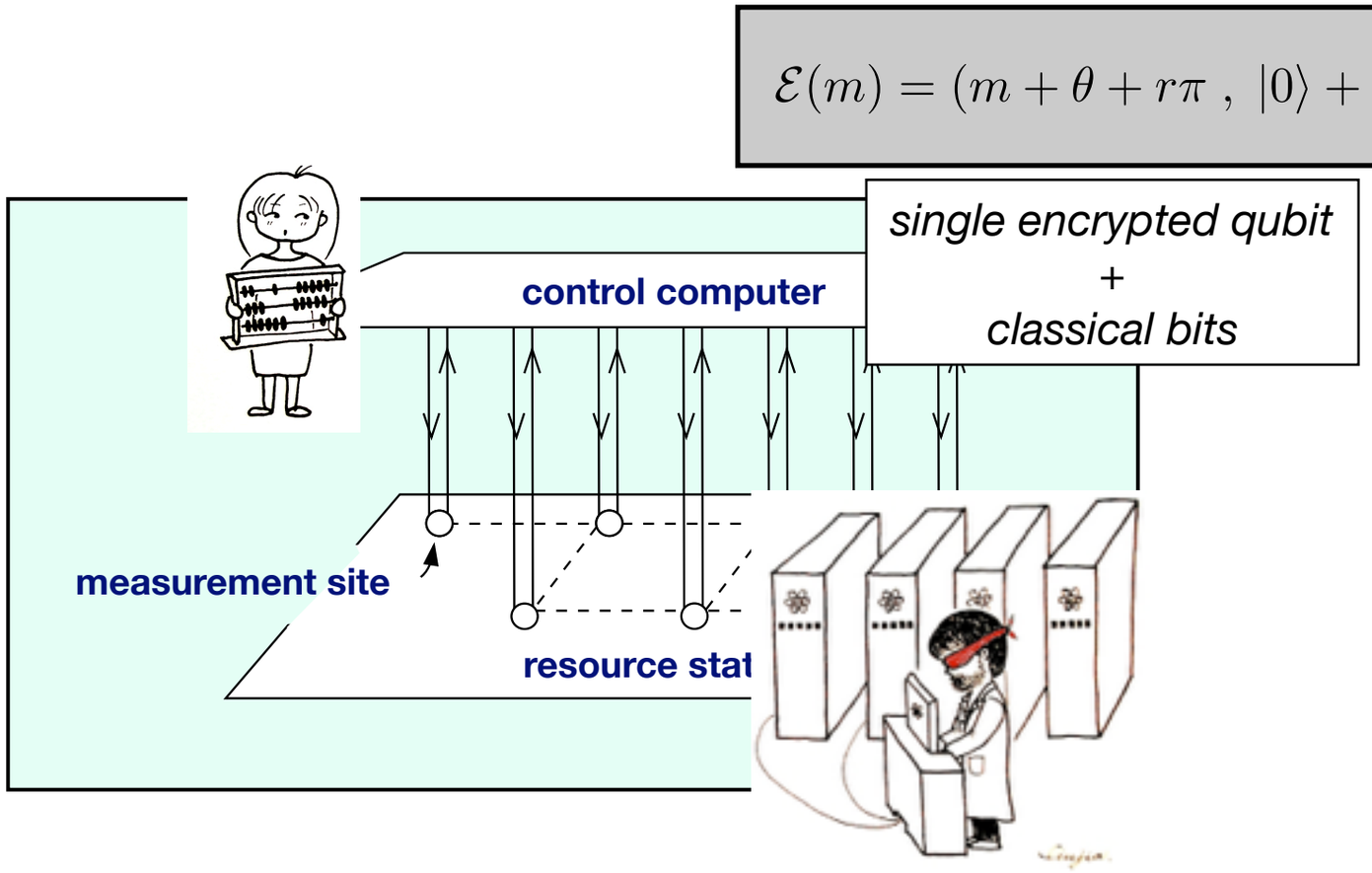
Hiding Program



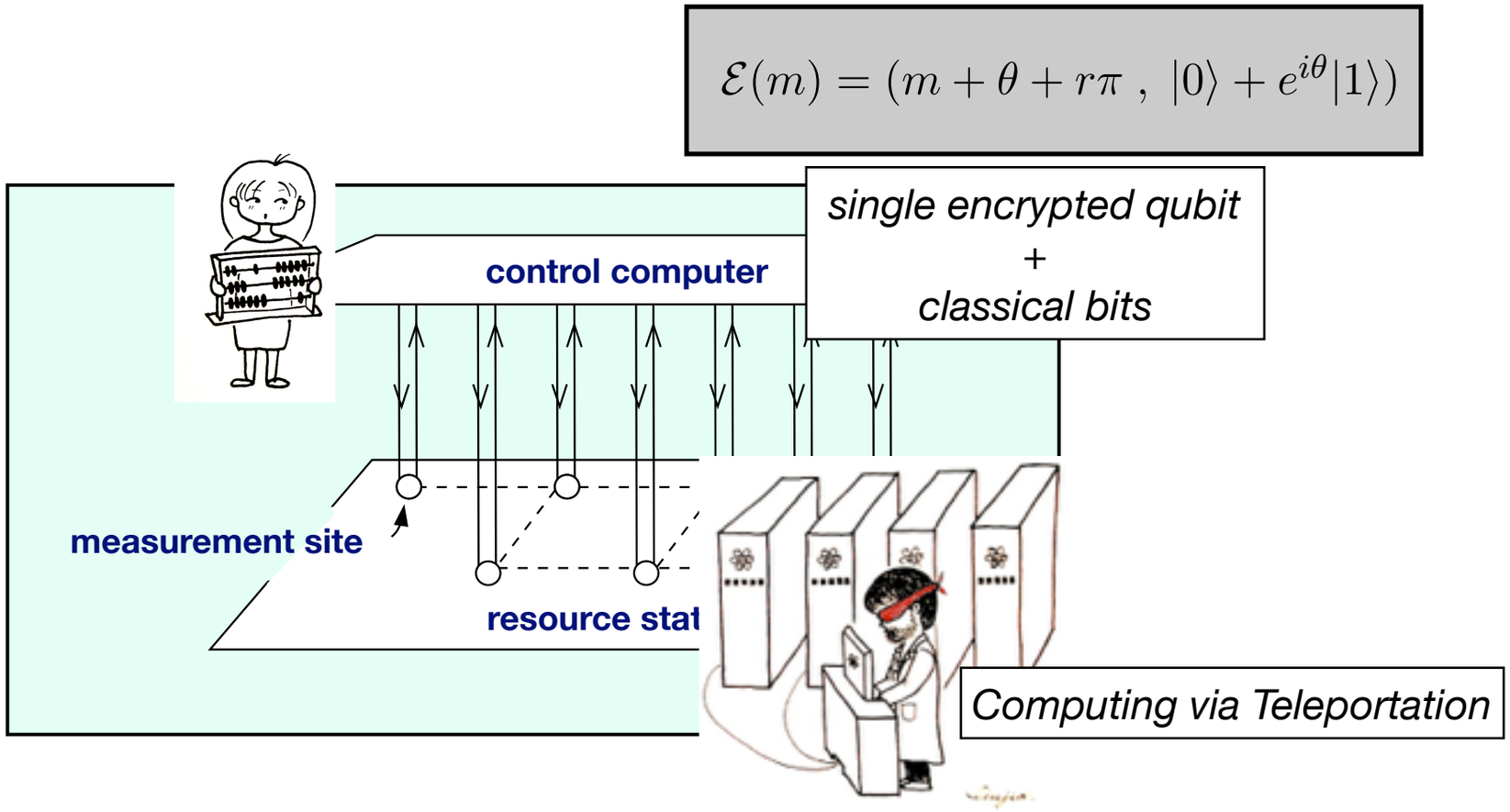
Hiding Program



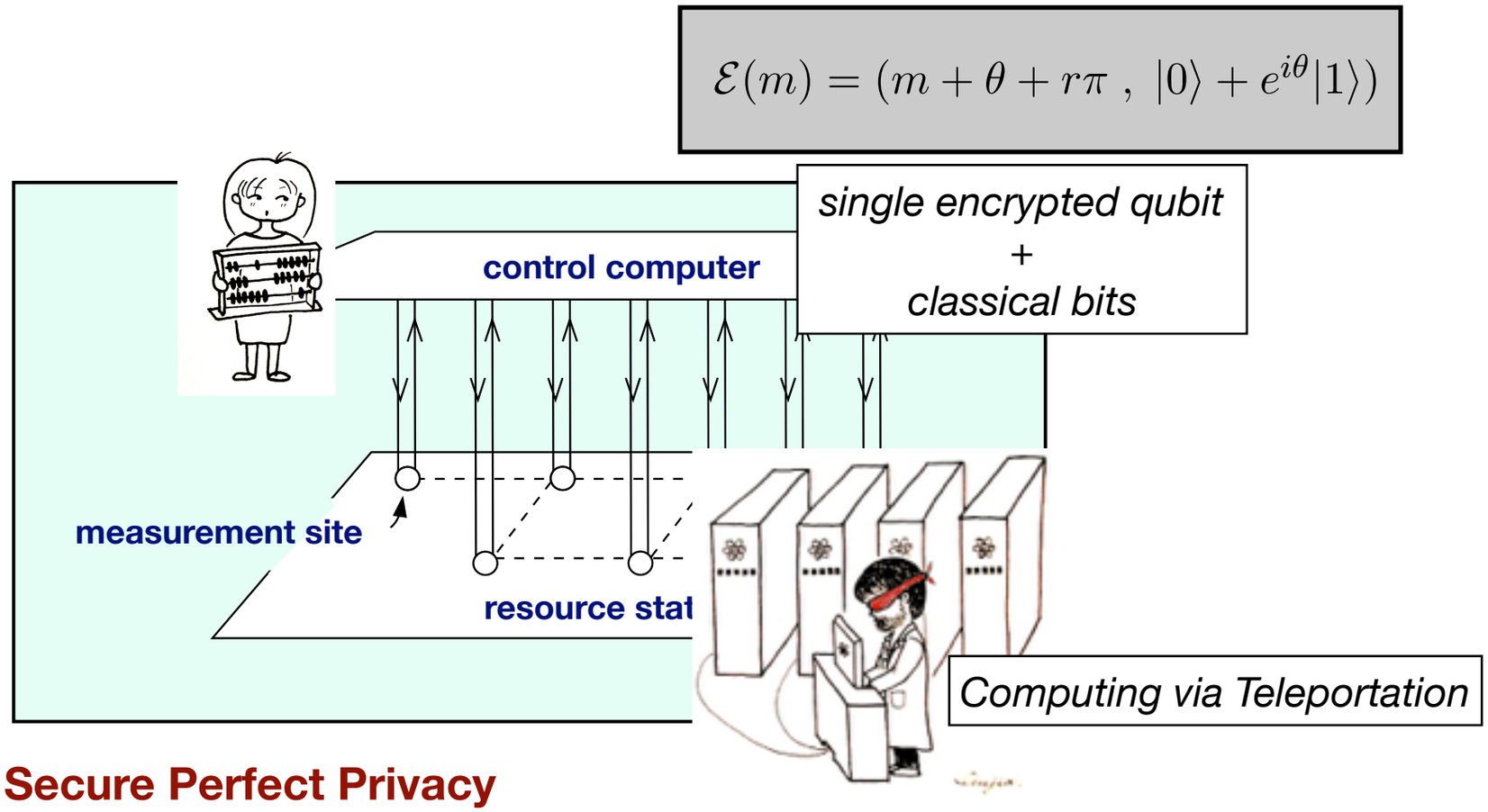
Hiding Program



Hiding Program



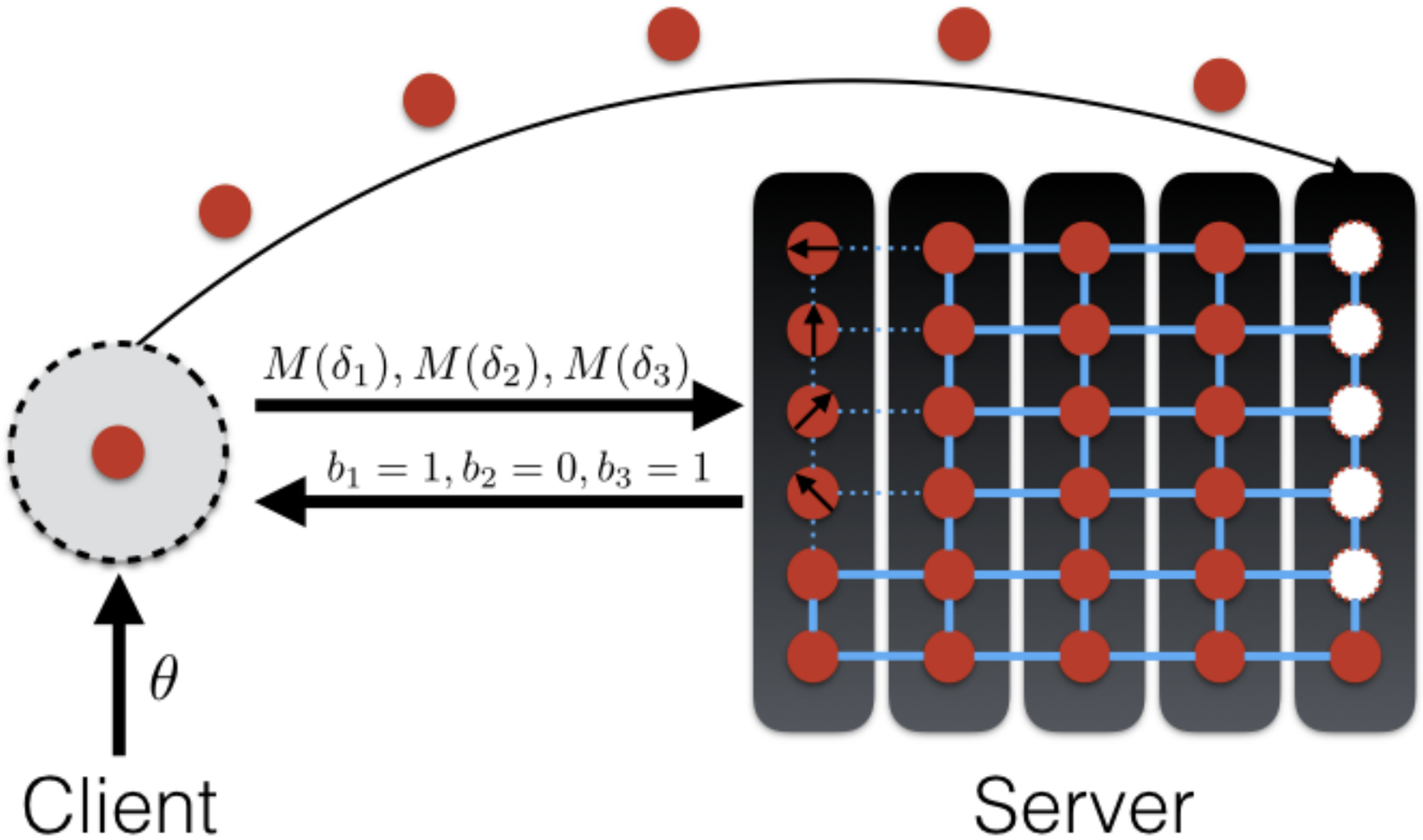
Hiding Program



Informationally Secure Perfect Privacy

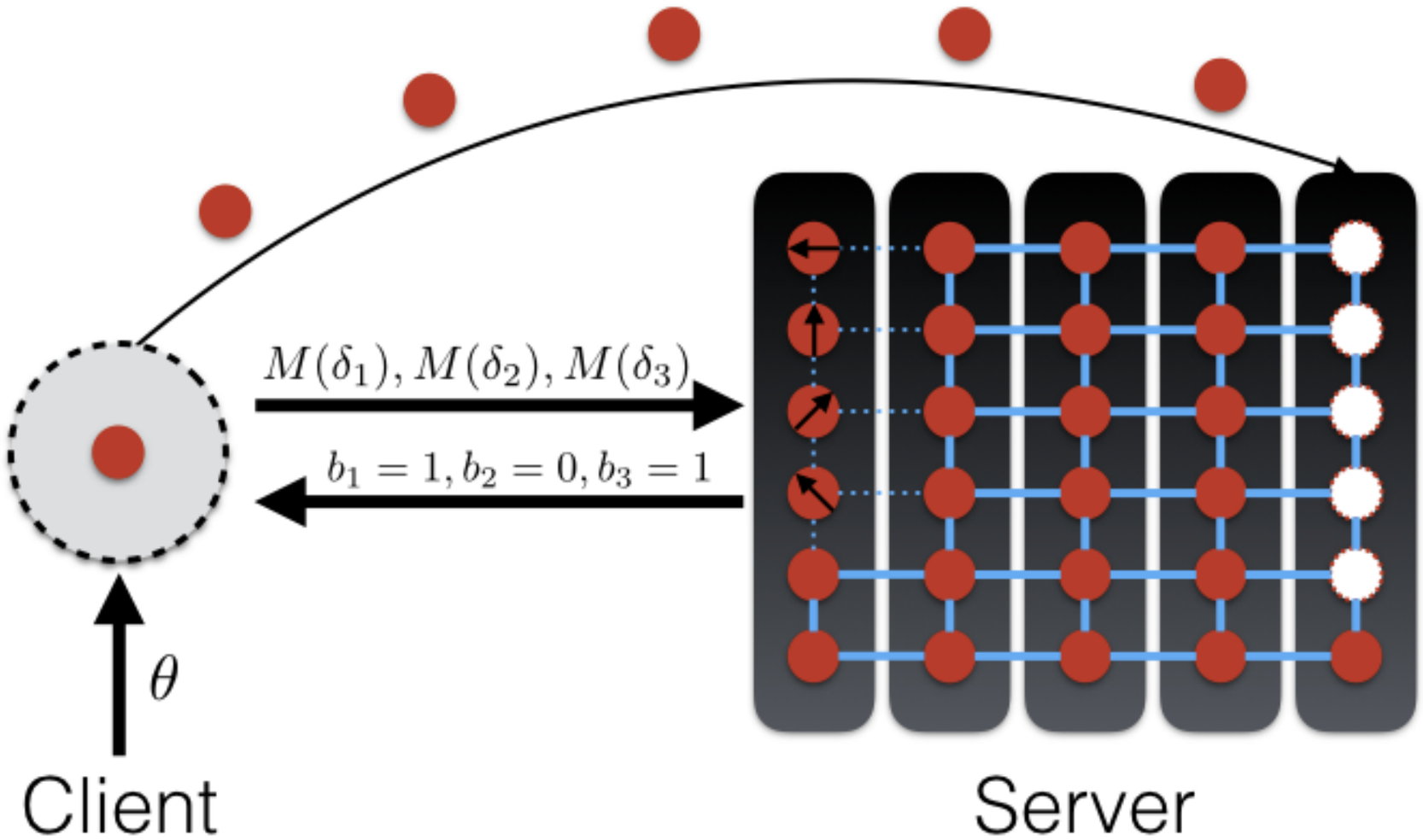
Server learns nothing about client's input/output/function

Unconditionally Secure Quantum Cloud in Theory



Broadbent, Fitzsimons and Kashefi, FOCS09

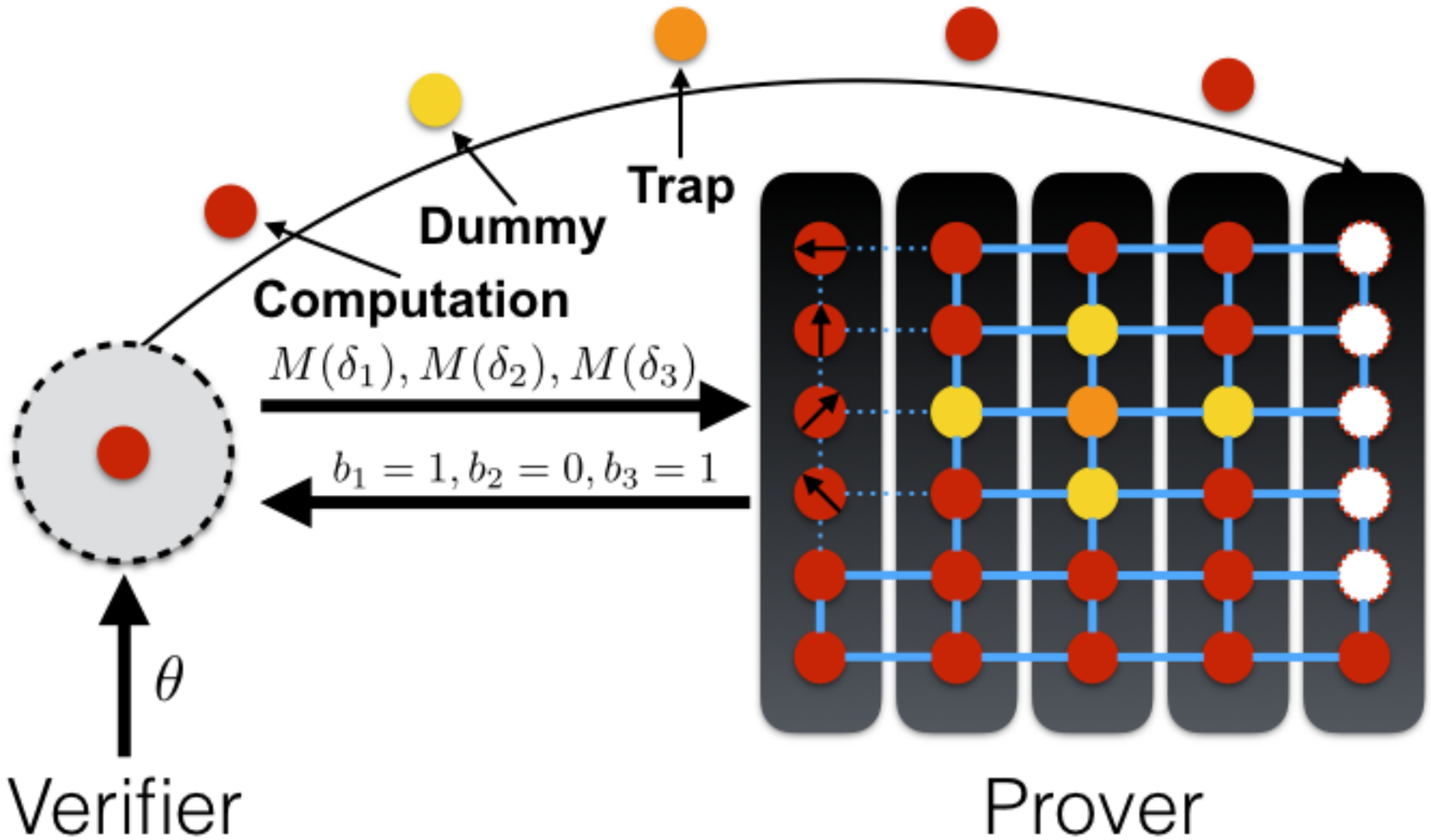
Unconditionally Secure Quantum Cloud in Theory



Universal Blind Quantum Computing: QKD + Teleportation

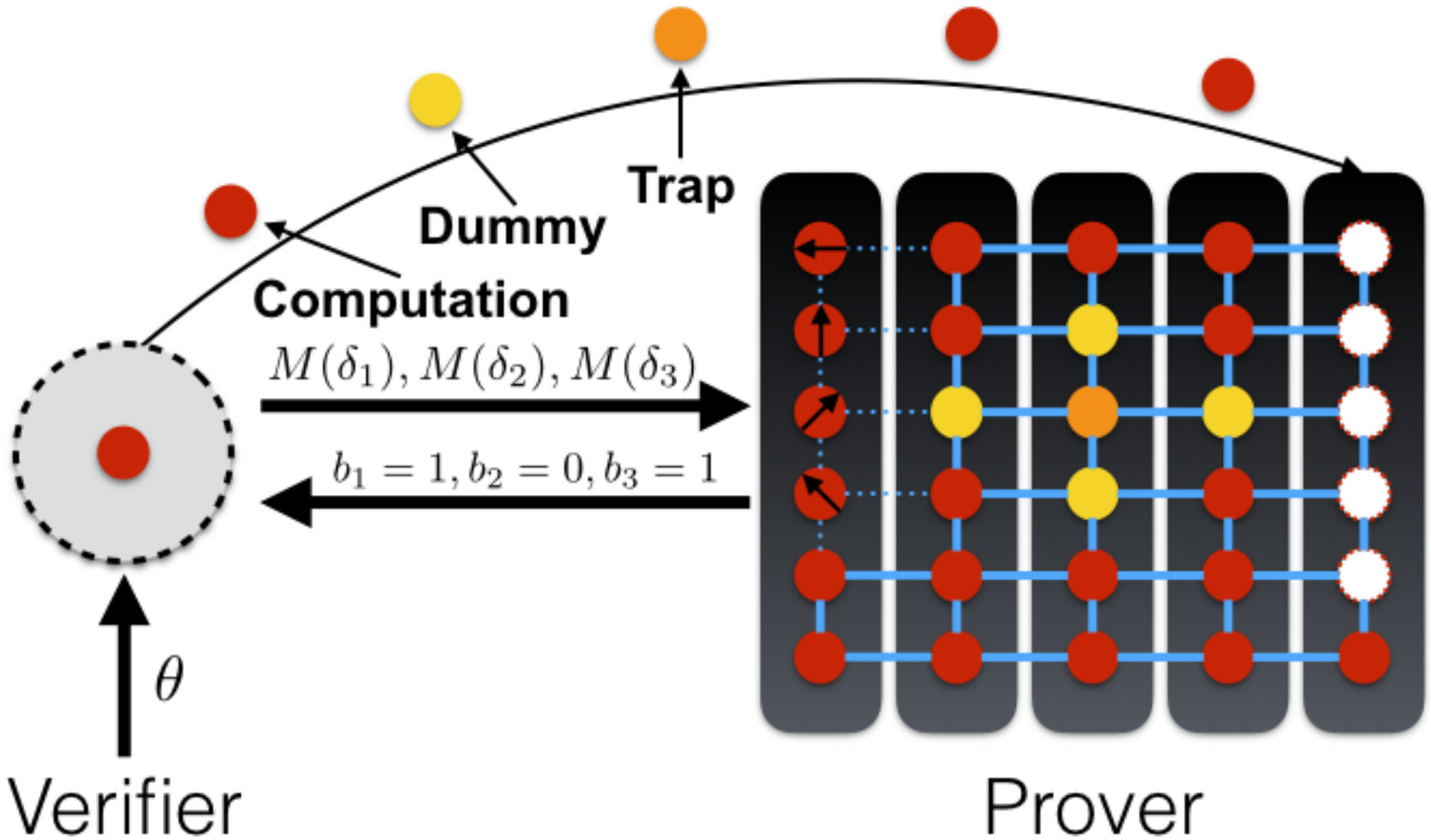
Broadbent, Fitzsimons and Kashefi, FOCS09

Verifiable Quantum Cloud in Theory



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

Verifiable Quantum Cloud in Theory

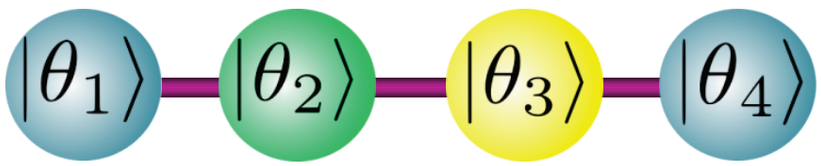


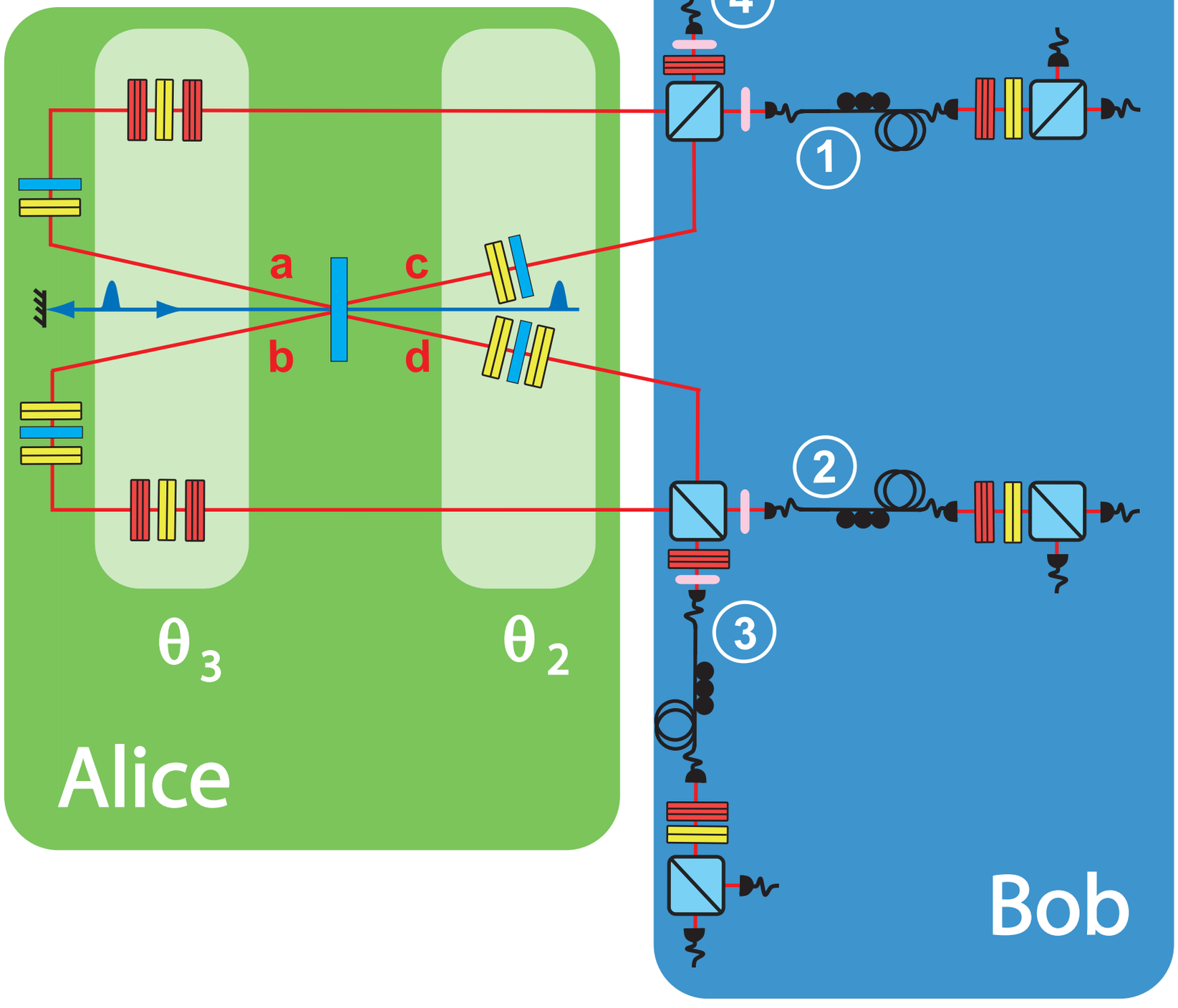
Verifiable Universal Blind Quantum Computing: QKD + Teleportation + Test

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

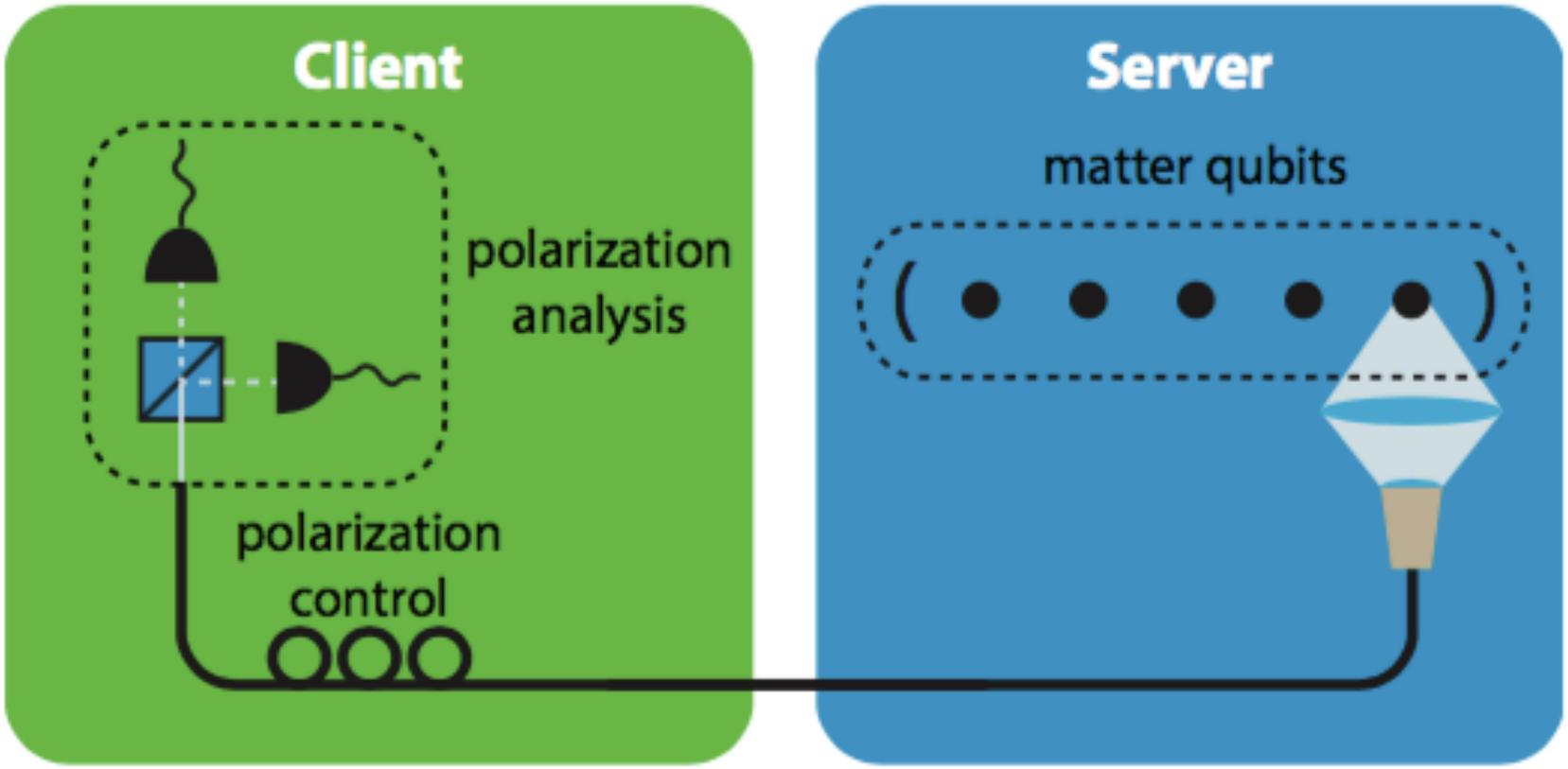
Photonic Implement

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

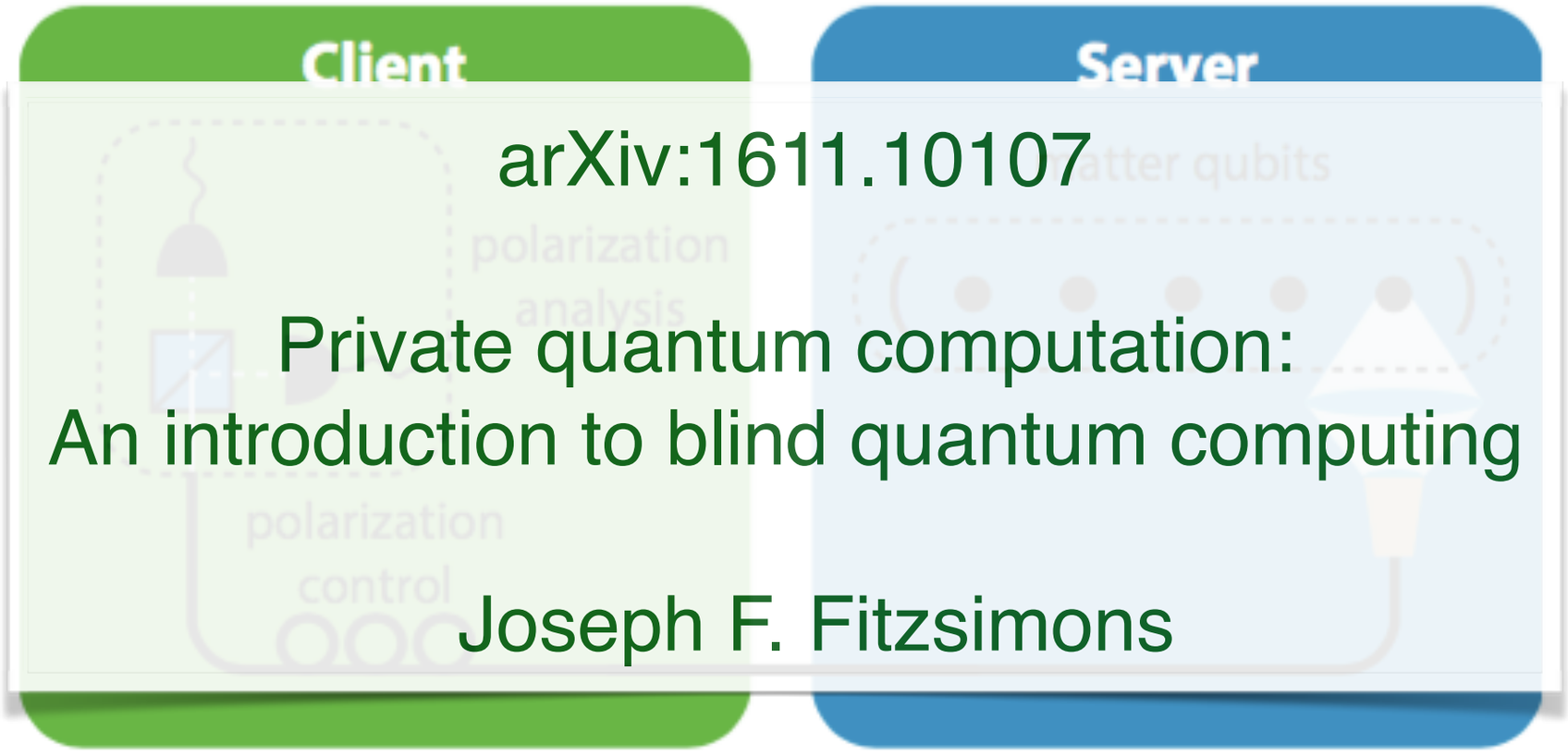




Hybrid Architecture



Hybrid Architecture



Global Directions on Verification

via **Hiding** : Cloud-based Crypto App Distributed Network

-

-

-

Global Directions on Verification

via **Hiding** : Cloud-based Crypto App Distributed Network

via **Proof System** : Quantum Simulation

Global Directions on Verification

via **Hiding** : Cloud-based Crypto App Distributed Network

via **Proof System** : Quantum Simulation

via **Hypothesis Testing** : Bench Marking Quantum Supremacy

Global Directions on Verification

via **Hiding** : Cloud-based Crypto App Distributed Network

- EPSRC UK
- NRF Singapore
- USAirforce
- EU QFlagship

via **Proof System** : Quantum Simulation

via **Hypothesis Testing** : Bench Marking Quantum Supremacy

Global Directions on Verification

via **Hiding** : Cloud-based Crypto App Distributed Network

- EPSRC UK
- NRF Singapore
- USAirforce
- EU QFlagship

via **Proof System** : Quantum Simulation

- Number Crunching
- Noise Handling
- Architecture Adaptation
- New Methods Development

via **Hypothesis Testing** : Bench Marking Quantum Supremacy

Verification Status

-

-

-

Verification Status

- It exists
- It is expanding

Trust Worthy Quantum Information TyQi17 Paris

-

-

-

Verification Status

- It exists
- It is expanding

Trust Worthy Quantum Information TyQi17 Paris

-

-

-

- The overhead depends on the level of trust

Entanglement / Measurements	Trusted	Semi-trusted (i.i.d.)	Untrusted
Trusted	$O(N)$	$O(N^4 logN)$	$O(N^{13} log(N))$
Untrusted	$O(N^4 logN)$	$O(N^4 logN)$	$O(N^{64})$

Verification Status

-

-

-

Verification Status

Robust and Efficient Fault Tolerant Verification of various architectures is possible

Verification Challenge

-

-

-

Verification Challenge

- uniform platform versus tailored made

Standardisation ??? Given the unknown nature of the emerging devices

-

-

-

Verification Challenge

- uniform platform versus tailored made

Standardisation ??? Given the unknown nature of the emerging devices

-

-

-

- Academic versus Industry's need

Objective improvements

Verification Challenge

- uniform platform versus tailored made

Standardisation ??? Given the unknown nature of the emerging devices

-

-

-

- Academic versus Industry's need

Objective improvements

VeriQloud spinoff of LIP6

Certifiable Quantum Advantage

Certifiable Quantum Advantage

Computational Problem	Quantum Hardware	**Verification Technique**

Certifiable Quantum Advantage

Computational Problem	Quantum Hardware	**Verification Technique**
Boson Sampling	Photonics Hardware	**Noise Certification**

Certifiable Quantum Advantage

Computational Problem	Quantum Hardware	**Verification Technique**
Boson Sampling	Photonics Hardware	**Noise Certification**
IQP	Cold Atoms	**Blind Verification**

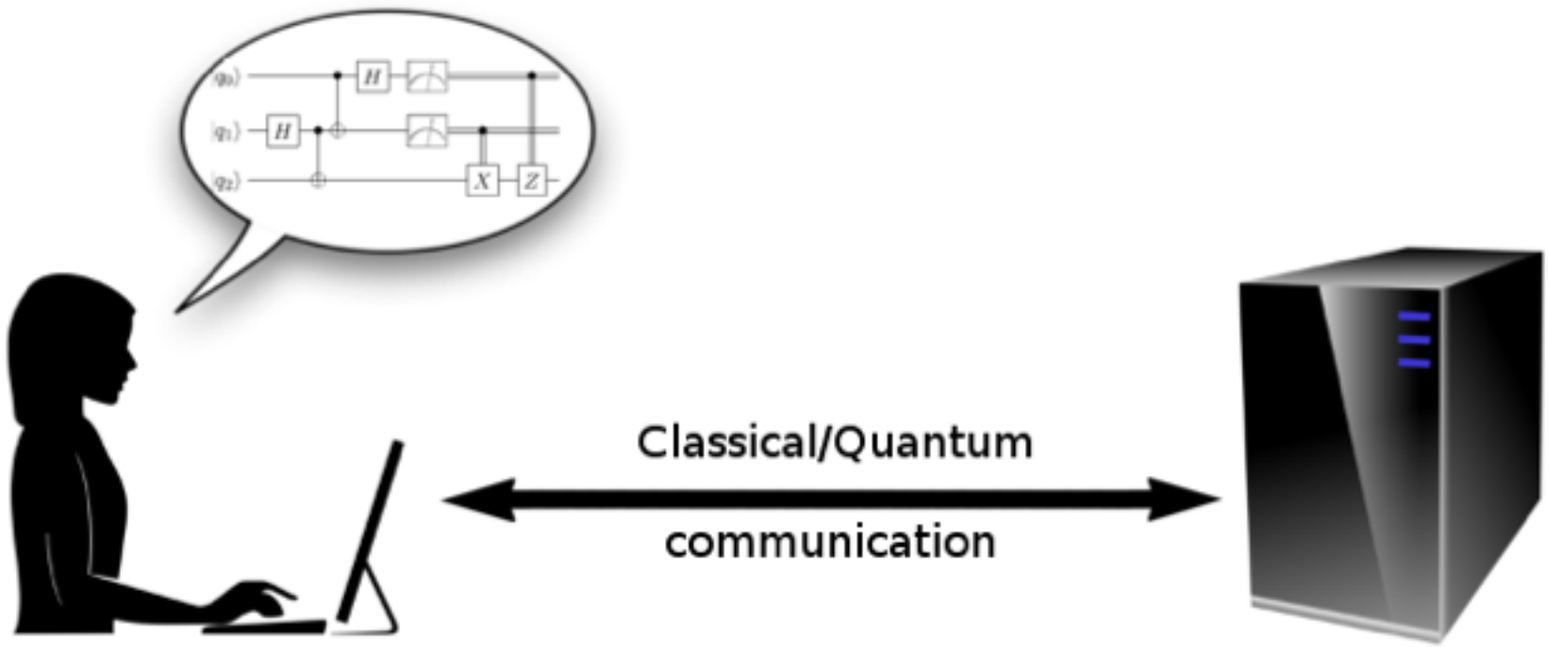
Certifiable Quantum Advantage

Computational Problem	Quantum Hardware	**Verification Technique**
Boson Sampling	Photonics Hardware	**Noise Certification**
IQP	Cold Atoms	**Blind Verification**
Randomised Circuit	Superconducting	**Hypothesis Test**

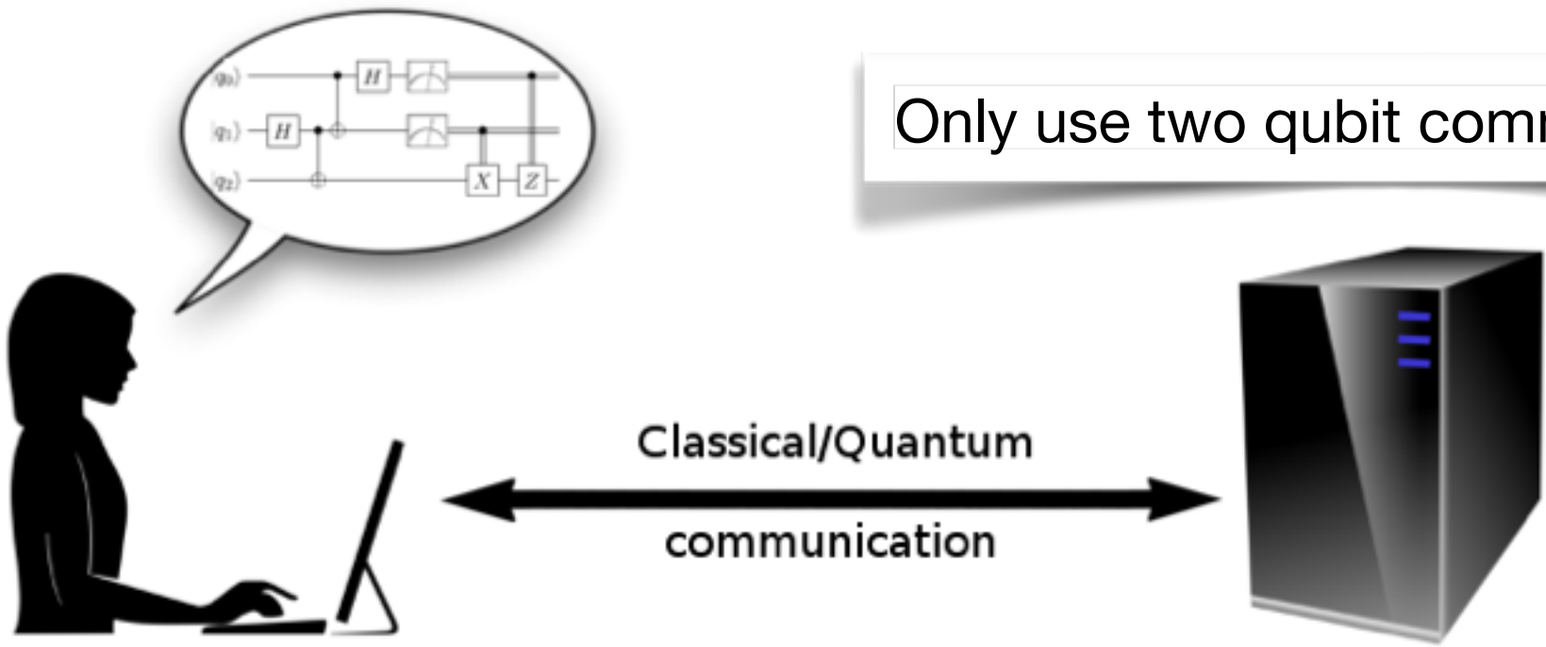
Certifiable Quantum Advantage

Computational Problem	Quantum Hardware	Verification Technique
Boson Sampling	Photonics Hardware	**Noise Certification**
IQP	Cold Atoms	**Blind Verification**
Randomised Circuit	Superconducting	**Hypothesis Test**
Trace Estimation	NMR	**Blind Verification**

Instantaneous quantum poly-time machine

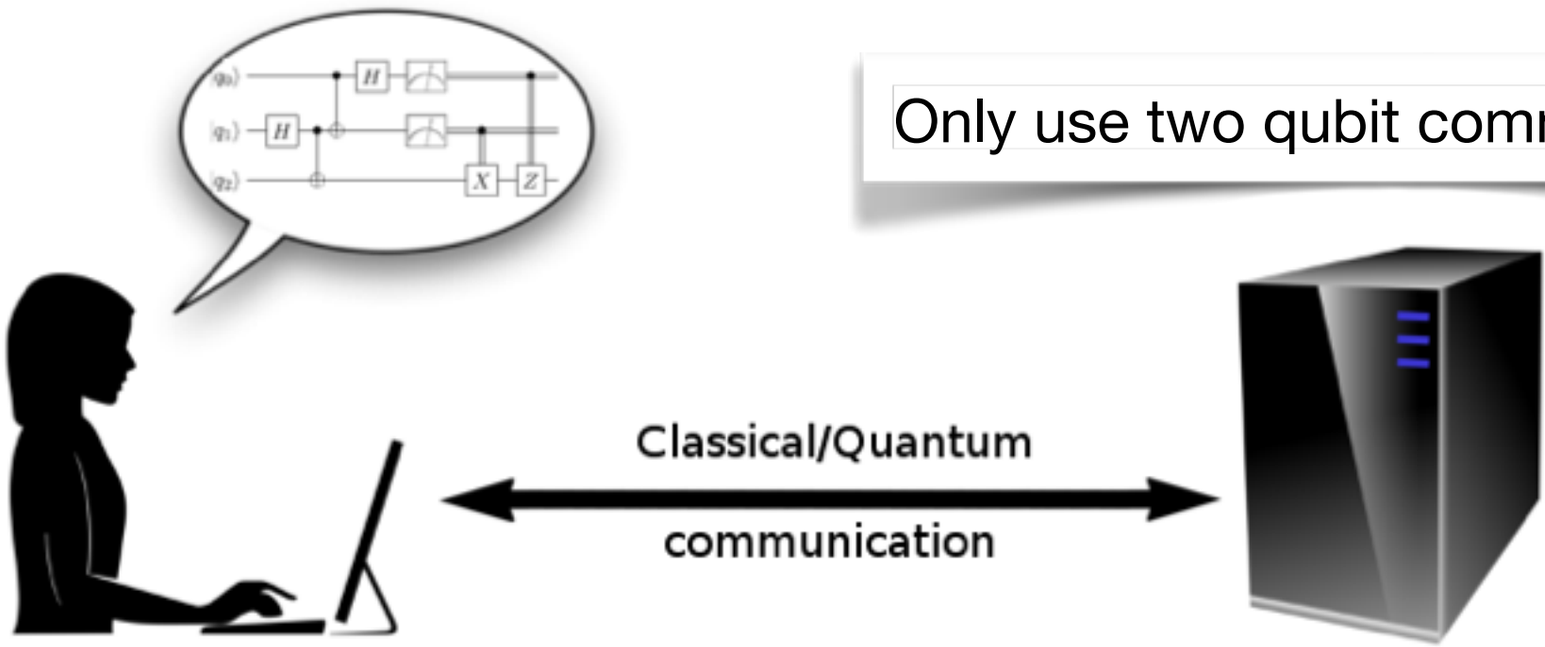


Instantaneous quantum poly-time machine



Only use two qubit commuting gates

Instantaneous quantum poly-time machine



Only use two qubit commuting gates

- Almost Classical Verifier
- Certify the machine is capable of computing IQP

IQP Hypothesis Test - Theory

IQP Hypothesis Test - Theory

Theory Step 1

If IQP computation was classically simulatable then PH collapses

IQP Hypothesis Test - Theory

Theory Step 1

If IQP computation was classically simulatable then PH collapses

Theory Step 2

Hide Test Round among the Sampling Round

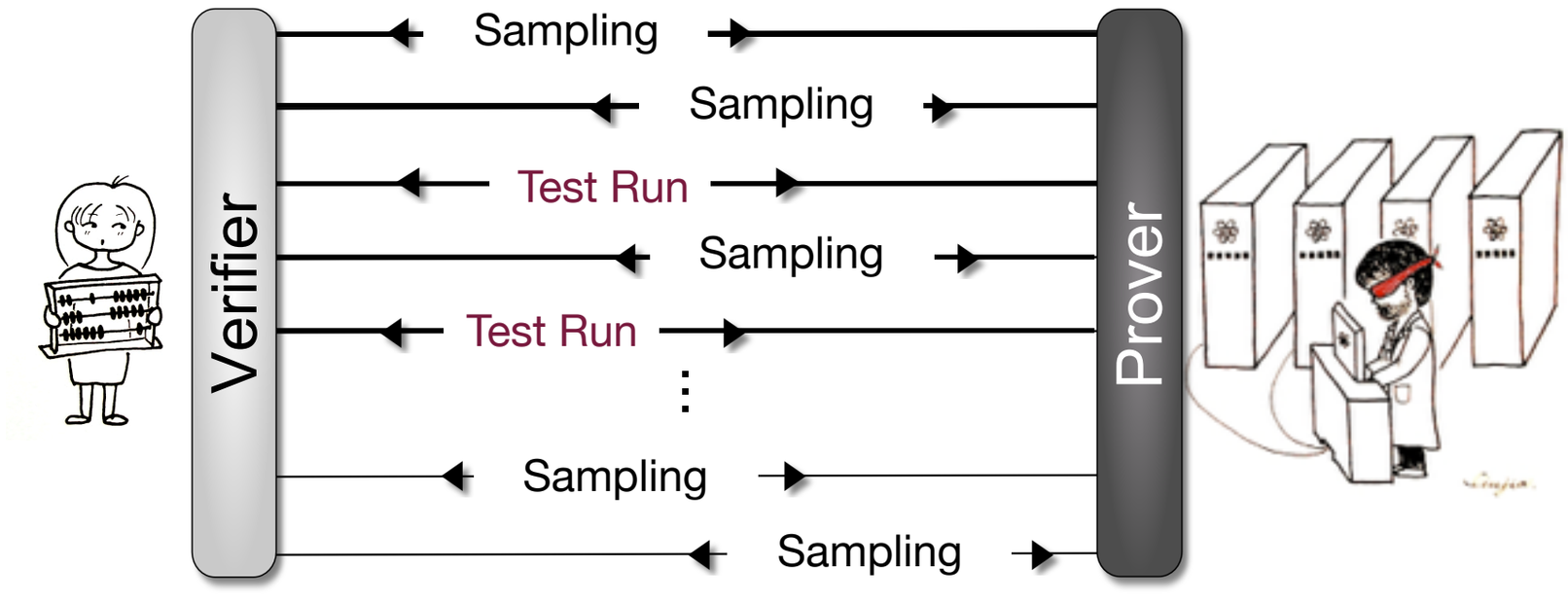
IQP Hypothesis Test - Theory

Theory Step 1

If IQP computation was classically simulatable then PH collapses

Theory Step 2

Hide Test Round among the Sampling Round



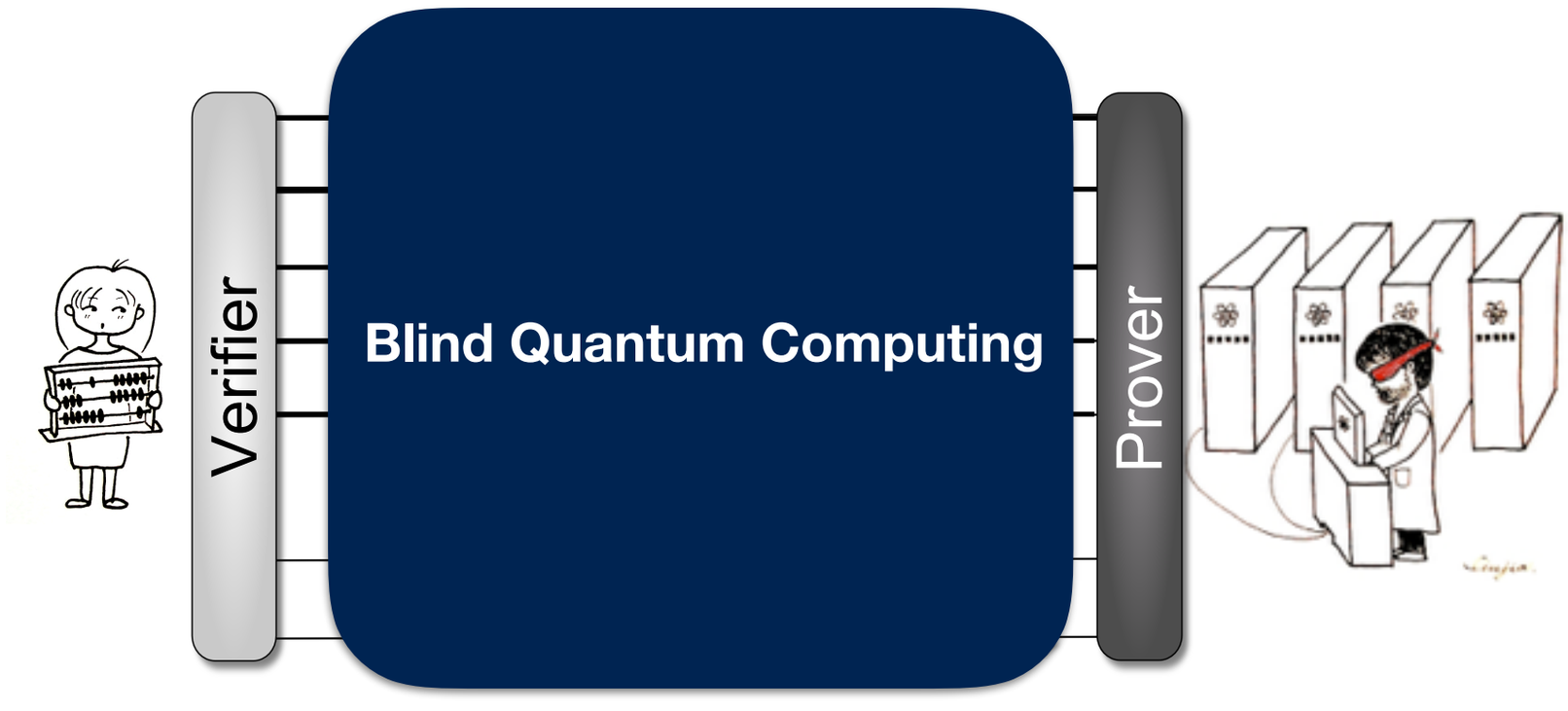
IQP Hypothesis Test - Theory

Theory Step 1

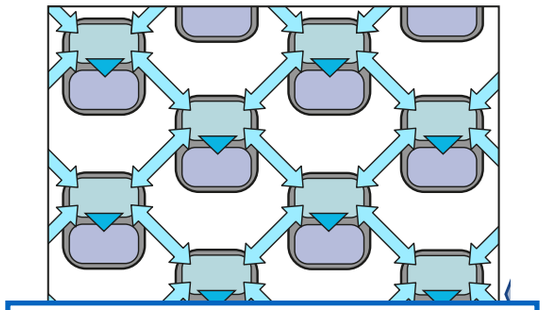
If IQP computation was classically simulatable then PH collapses

Theory Step 2

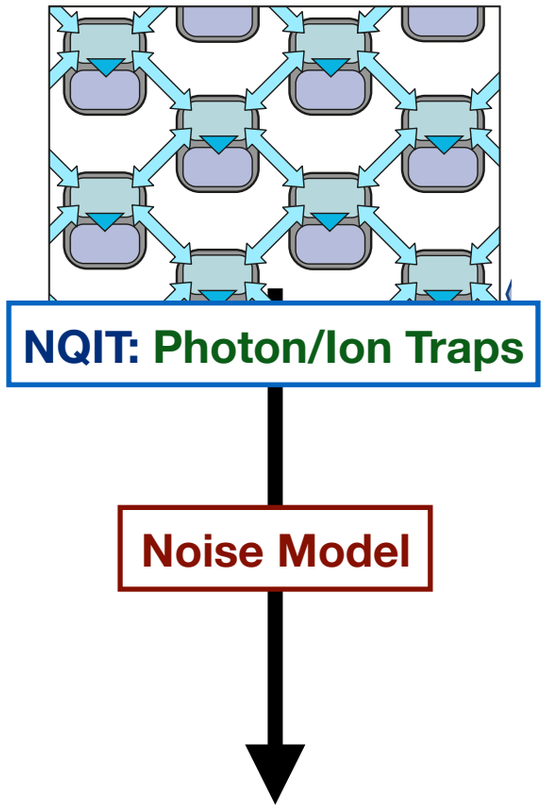
Hide Test Round among the Sampling Round



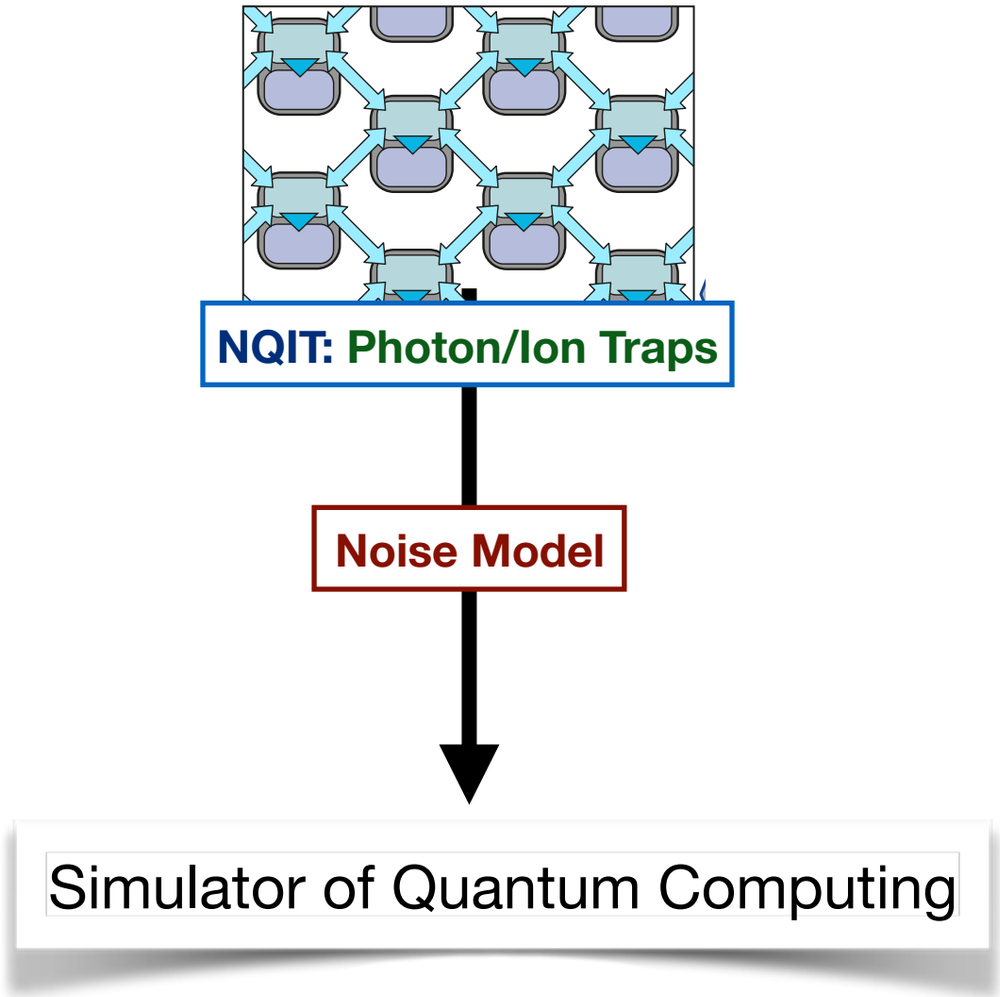
IQP Hypothesis Test - Practice



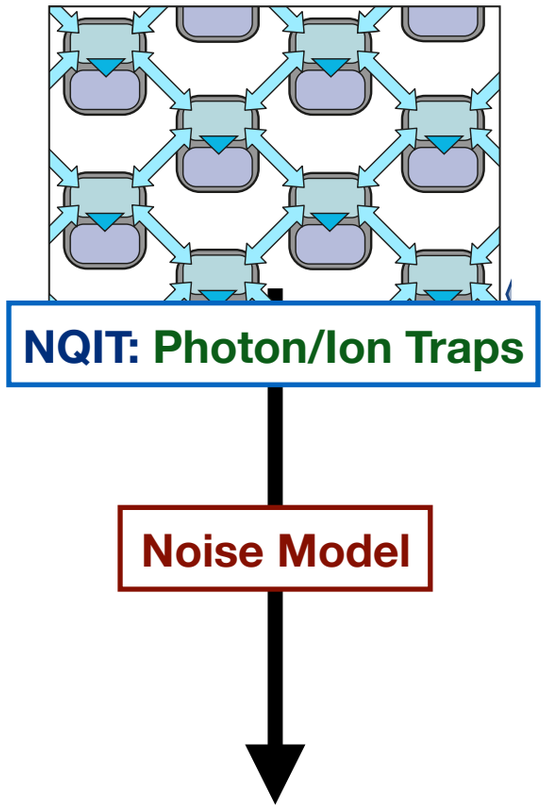
IQP Hypothesis Test - Practice



IQP Hypothesis Test - Practice



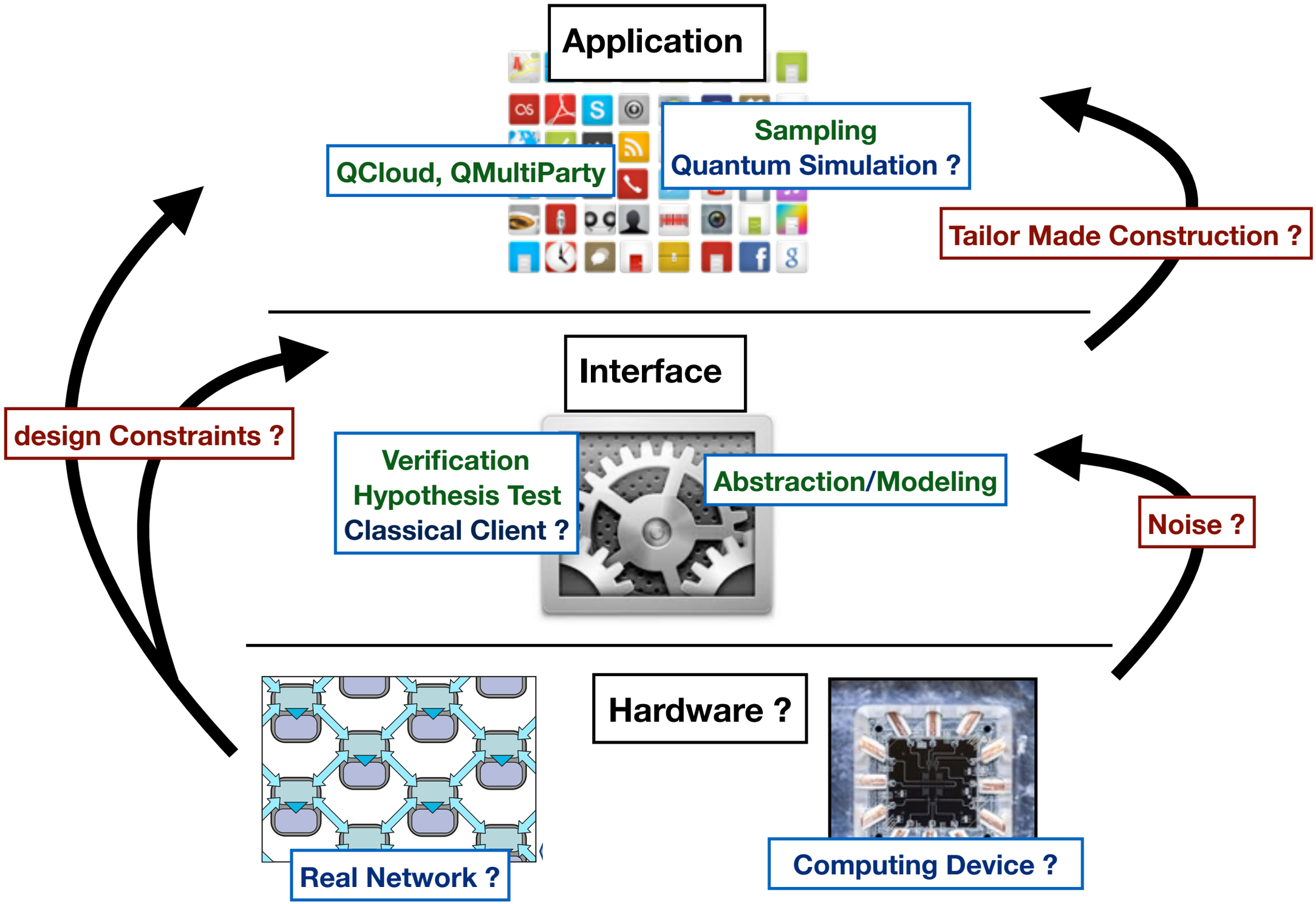
IQP Hypothesis Test - Practice



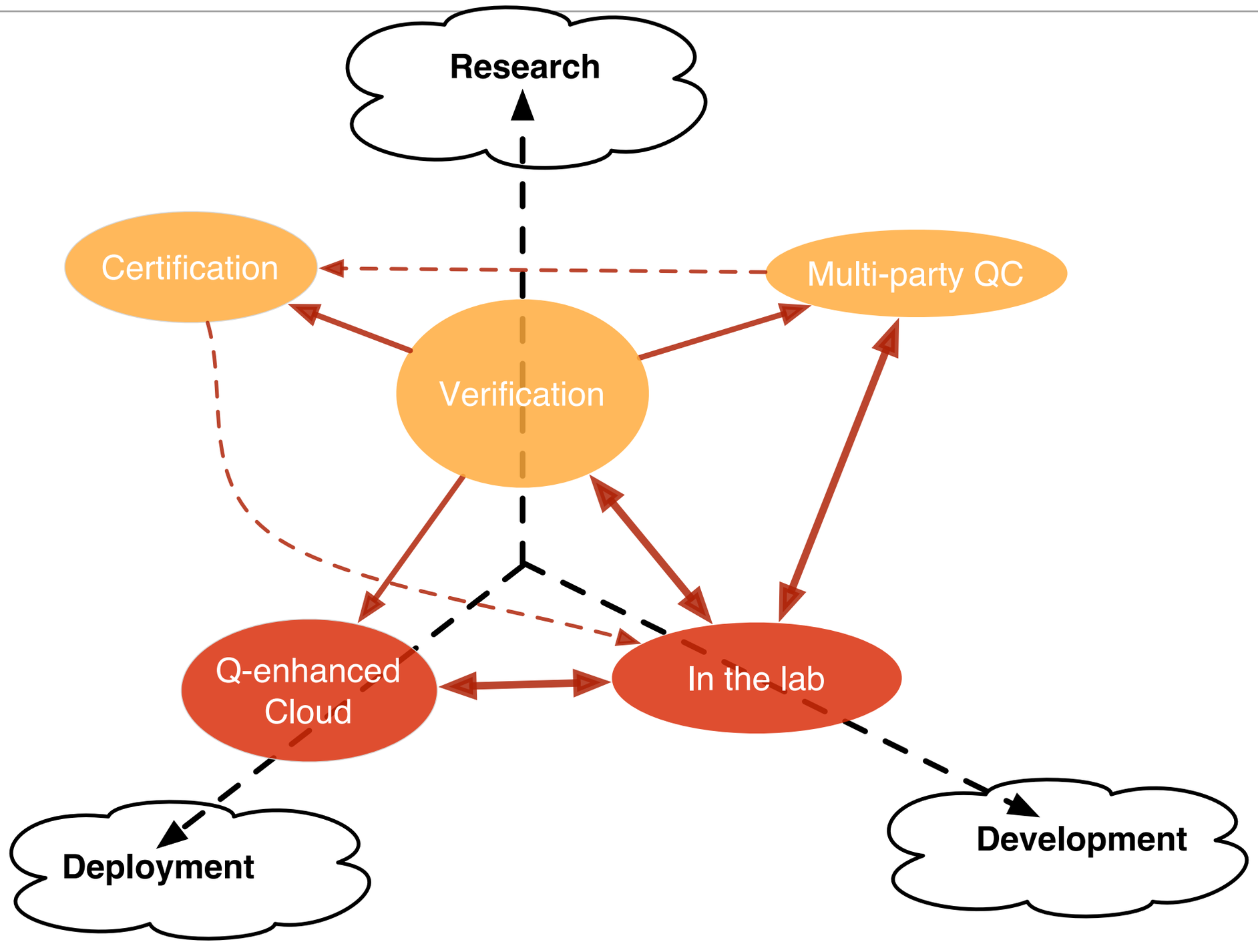
Simulator of Quantum Computing

HT is very fragile

Where we stand

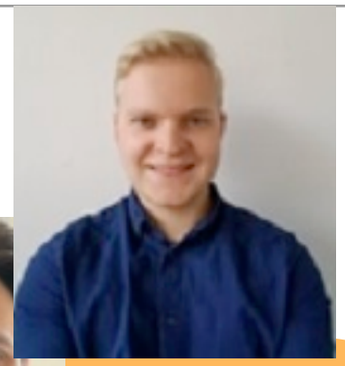


The Edinburgh-Paris Team



The Edinburgh-Paris Team


Daniel Mills


Brian Coyle


Luka Music

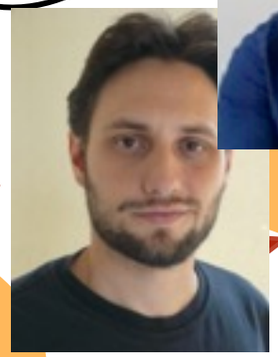
Research

Certification

Verification

Multi-party QC


Andru Gheorghiu


Petros Wallden

Ulysse Chabaud


Alexandru Cojocaru

Q-enhanced Cloud


Tom Douce

In the lab

Deployment


Ellen Derbyshire

Development

Interns:

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

Other collaborators

Theory

Damian Markham (LIP6)
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

Damian Markham (LIP6)
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)

EPSRC
Engineering and Physical Sciences Research Council

NQIT

UK NATIONAL QUANTUM TECHNOLOGIES PROGRAMME