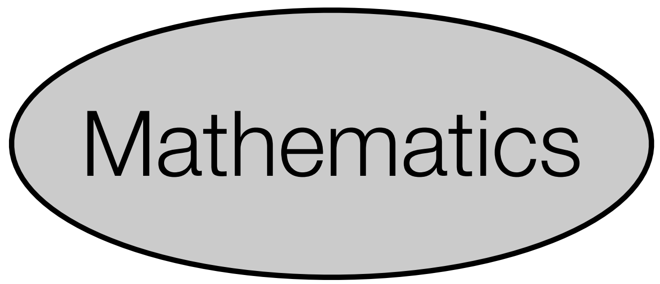
Entrapping Nature

Elham Kashefi

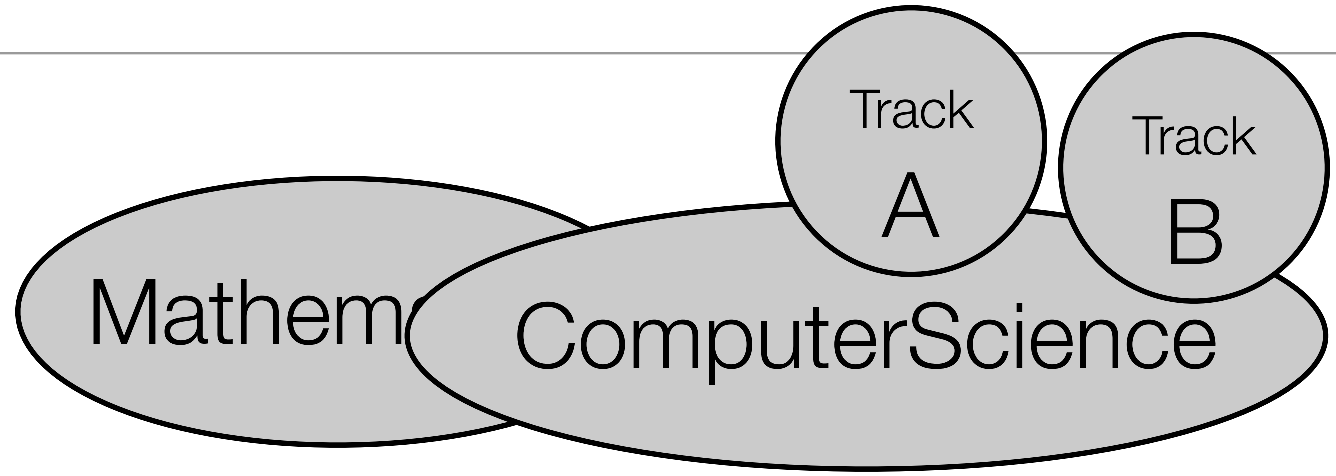
University of Edinburgh
UK Networked Quantum Information Technologies Hub
CNRS, Pierre and Marie Curie University
Paris Centre for Quantum Computing

Profile of a Quantum Person

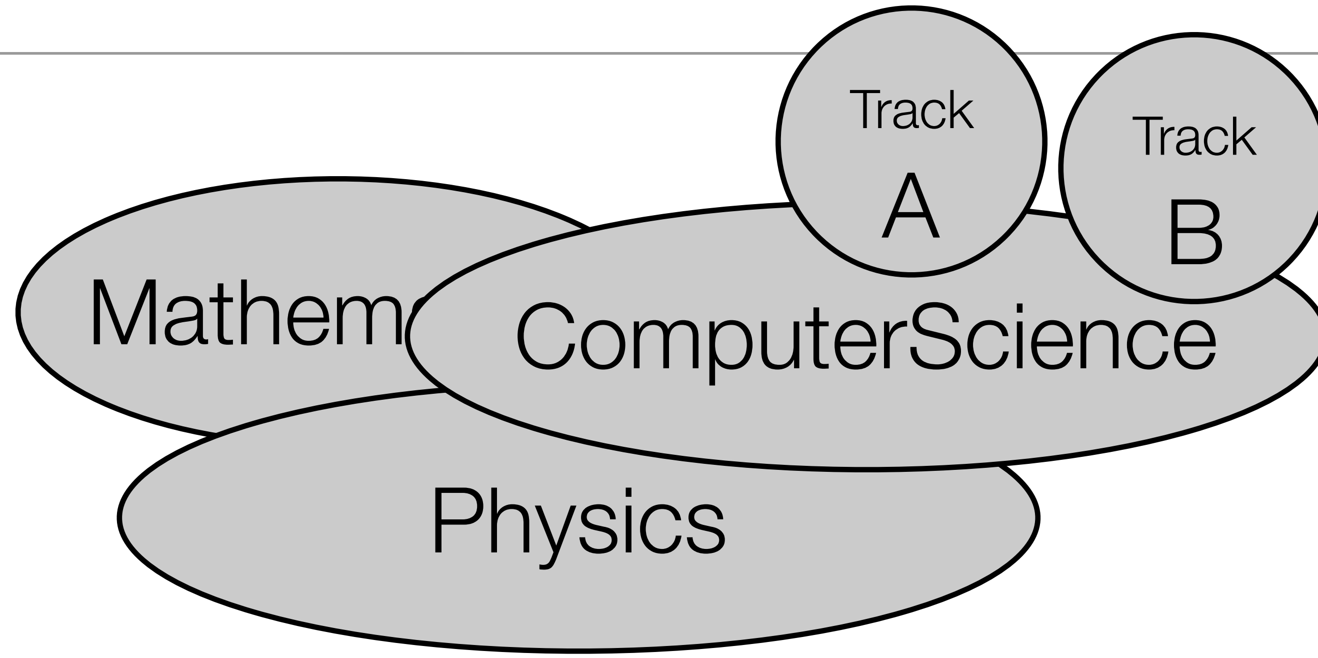
Profile of a Quantum Person



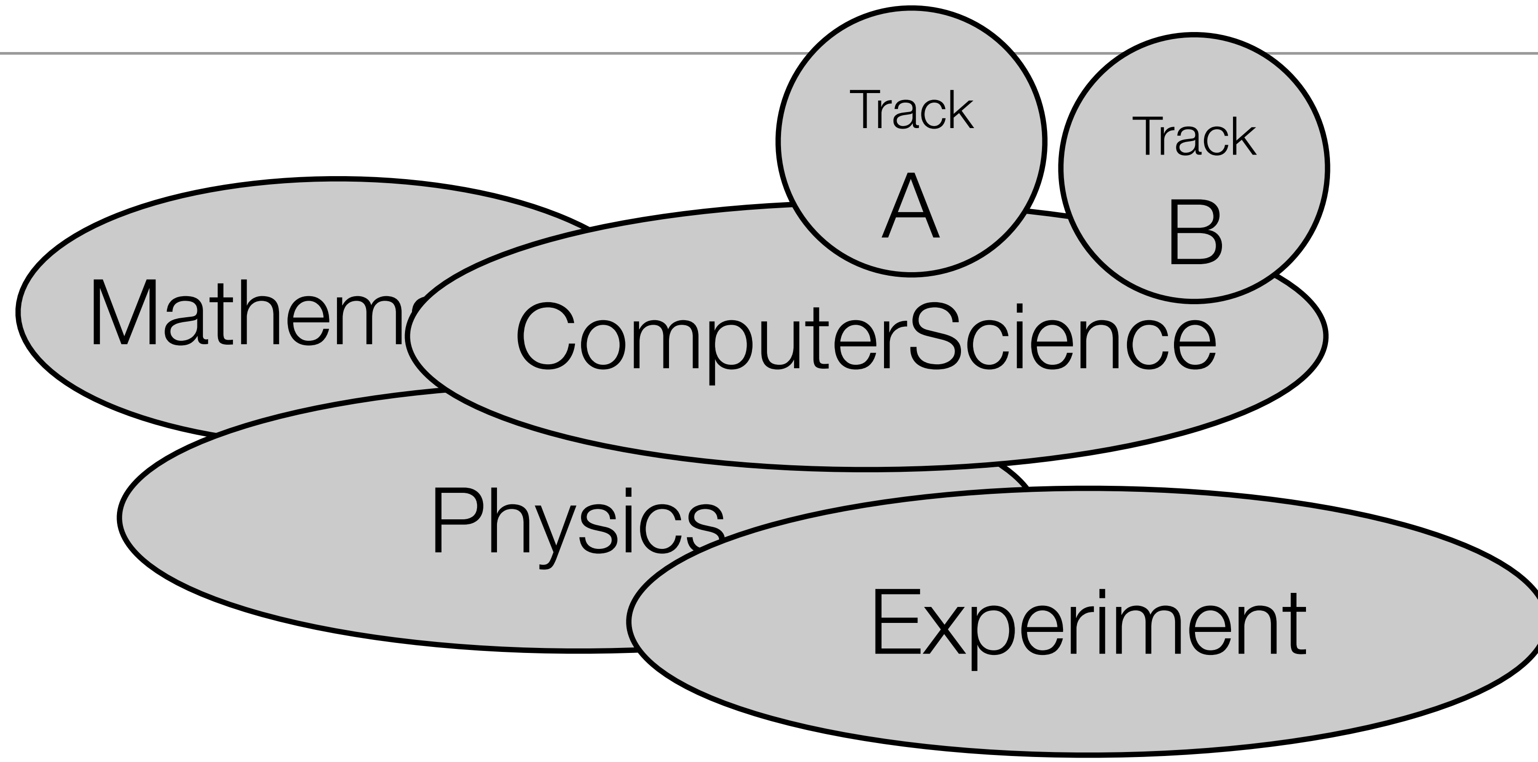
Profile of a Quantum Person



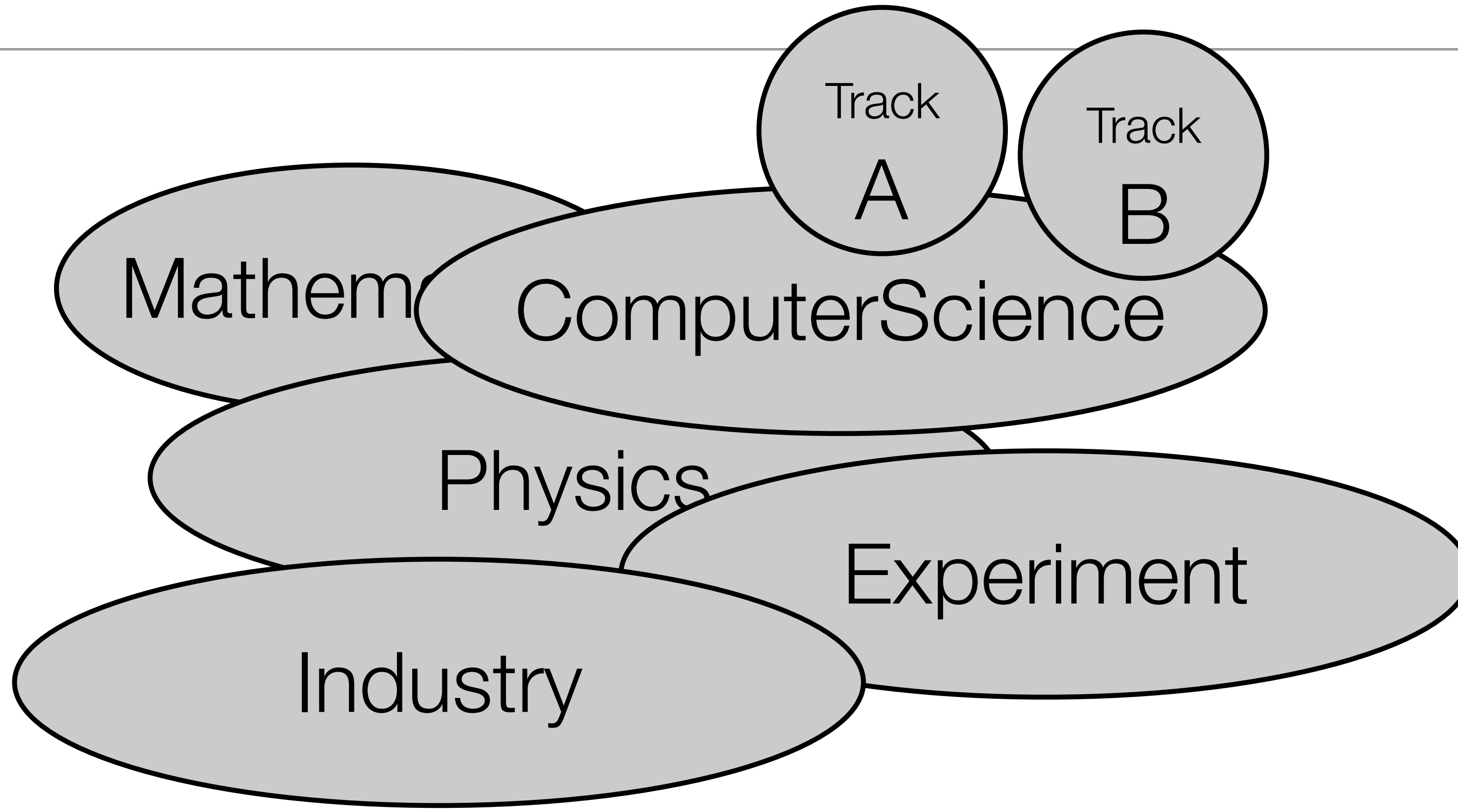
Profile of a Quantum Person



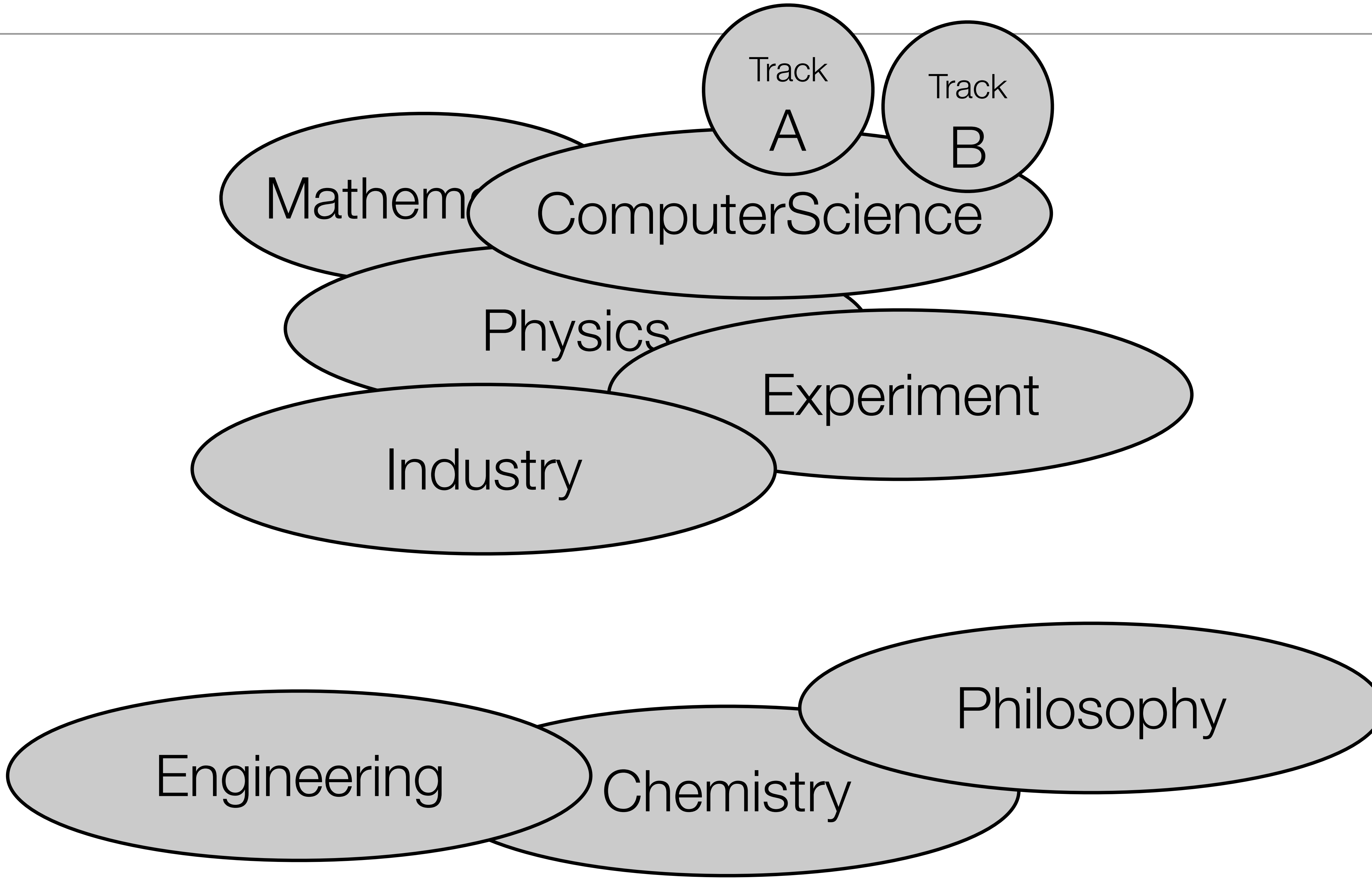
Profile of a Quantum Person



Profile of a Quantum Person



Profile of a Quantum Person



Feynman Vision - 82

Quantum Computing as the technology for simulating quantum systems

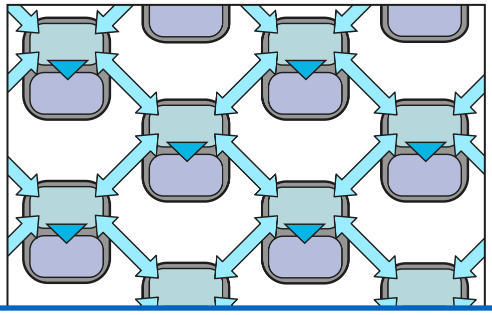
Feynman Vision - 82

Quantum Computing as the technology for simulating quantum systems

Spectacular Progress

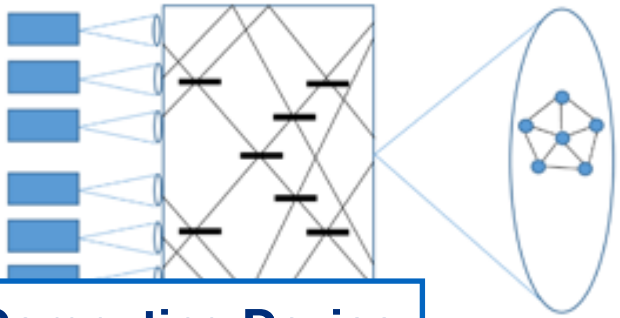
from complexity theory to cryptography
from simulation to sampling
from tomography to implementation
from foundation to interpretation

QSoft Vision of Quantum Technology



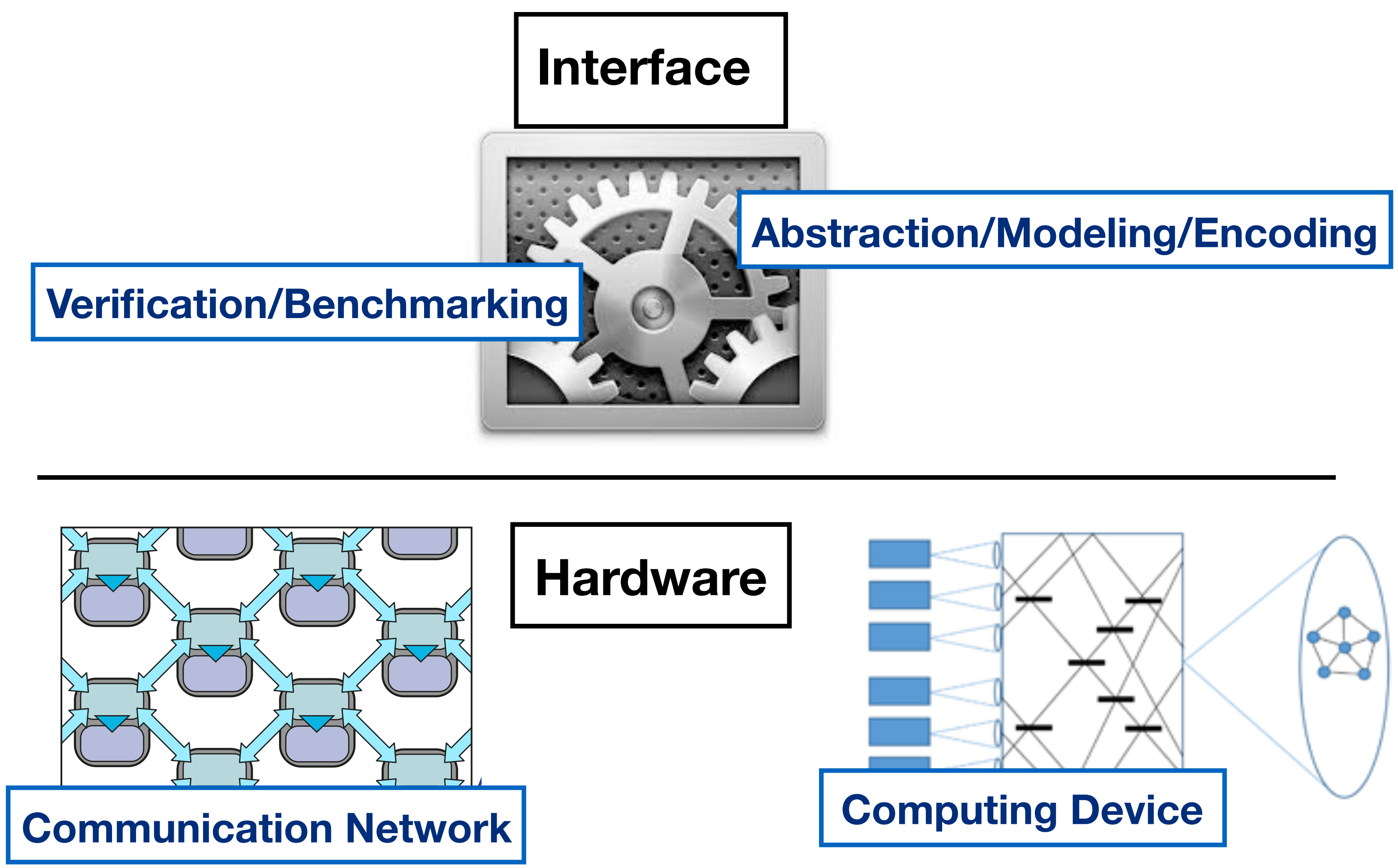
Communication Network

Hardware

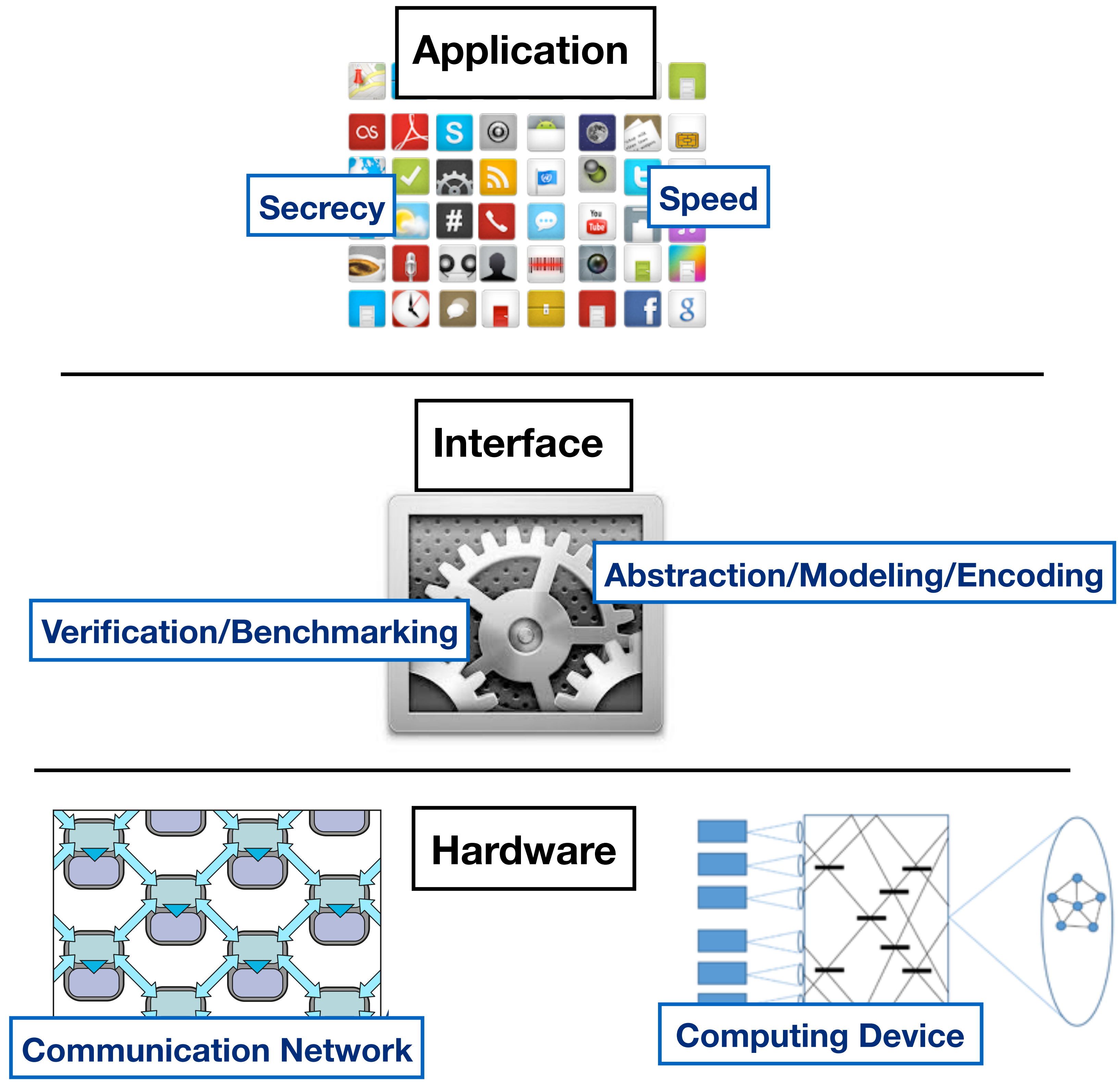


Computing Device

QSoft Vision of Quantum Technology



QSoft Vision of Quantum Technology



Quantum Era

National Investments

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

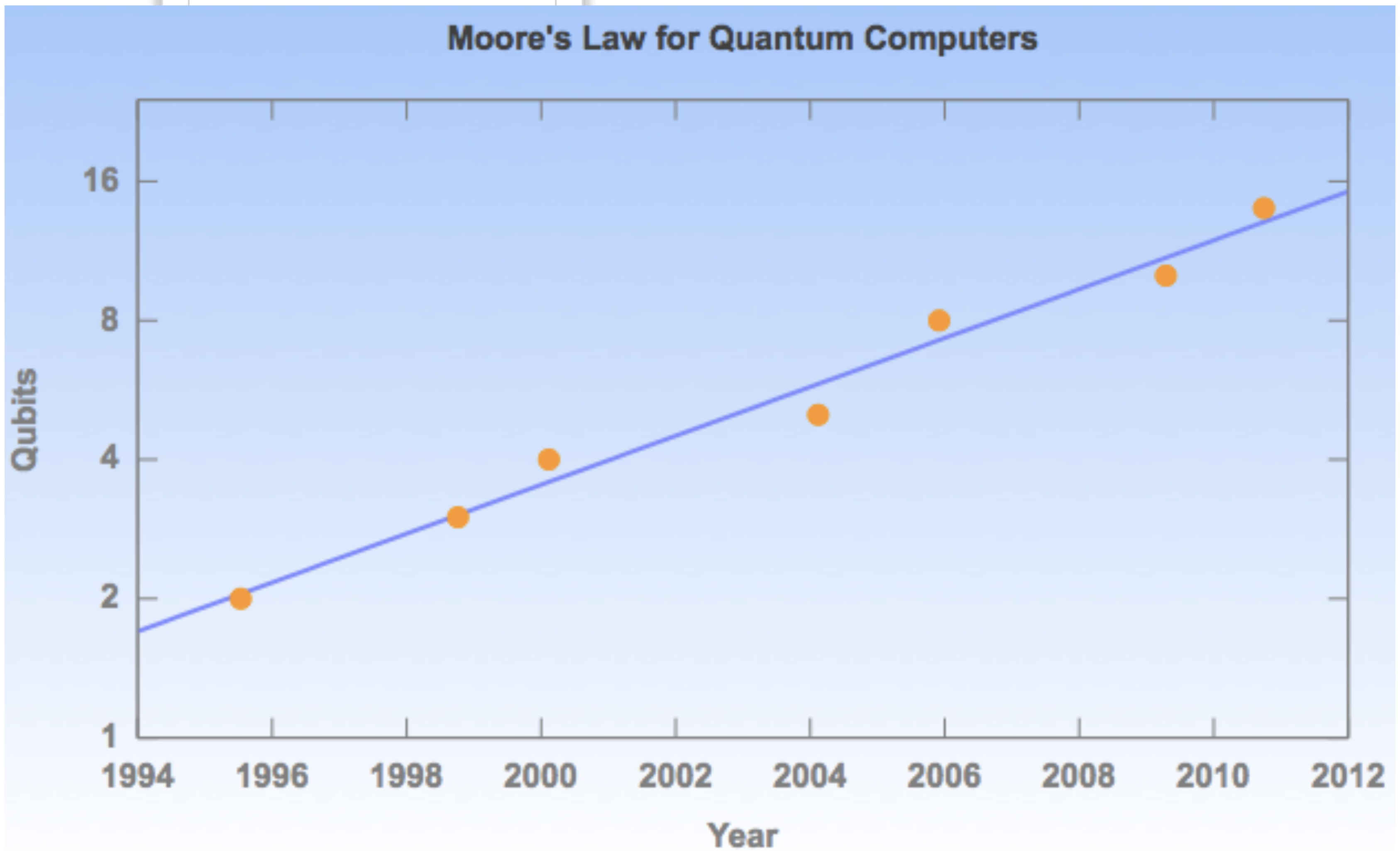
Quantum Machines

Private Investments

Google, IBM, Intel,ATOS,Alibaba
Big VC founds
Startups Companies

Quantum Era

National Investments

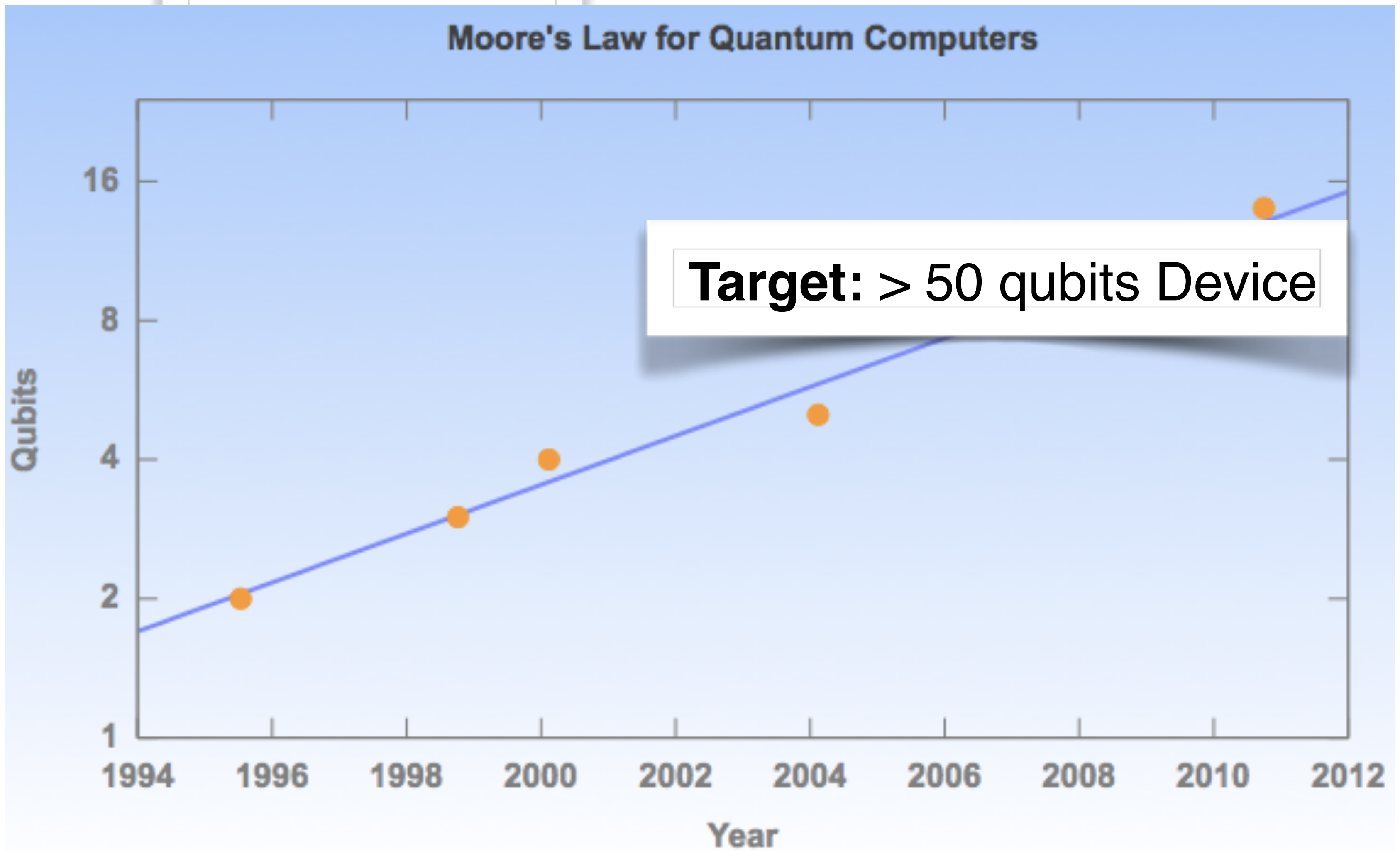


Private Investments

Google, IBM, Intel,ATOS,Alibaba
Big VC founds
Startups Companies

Quantum Era

National Investments



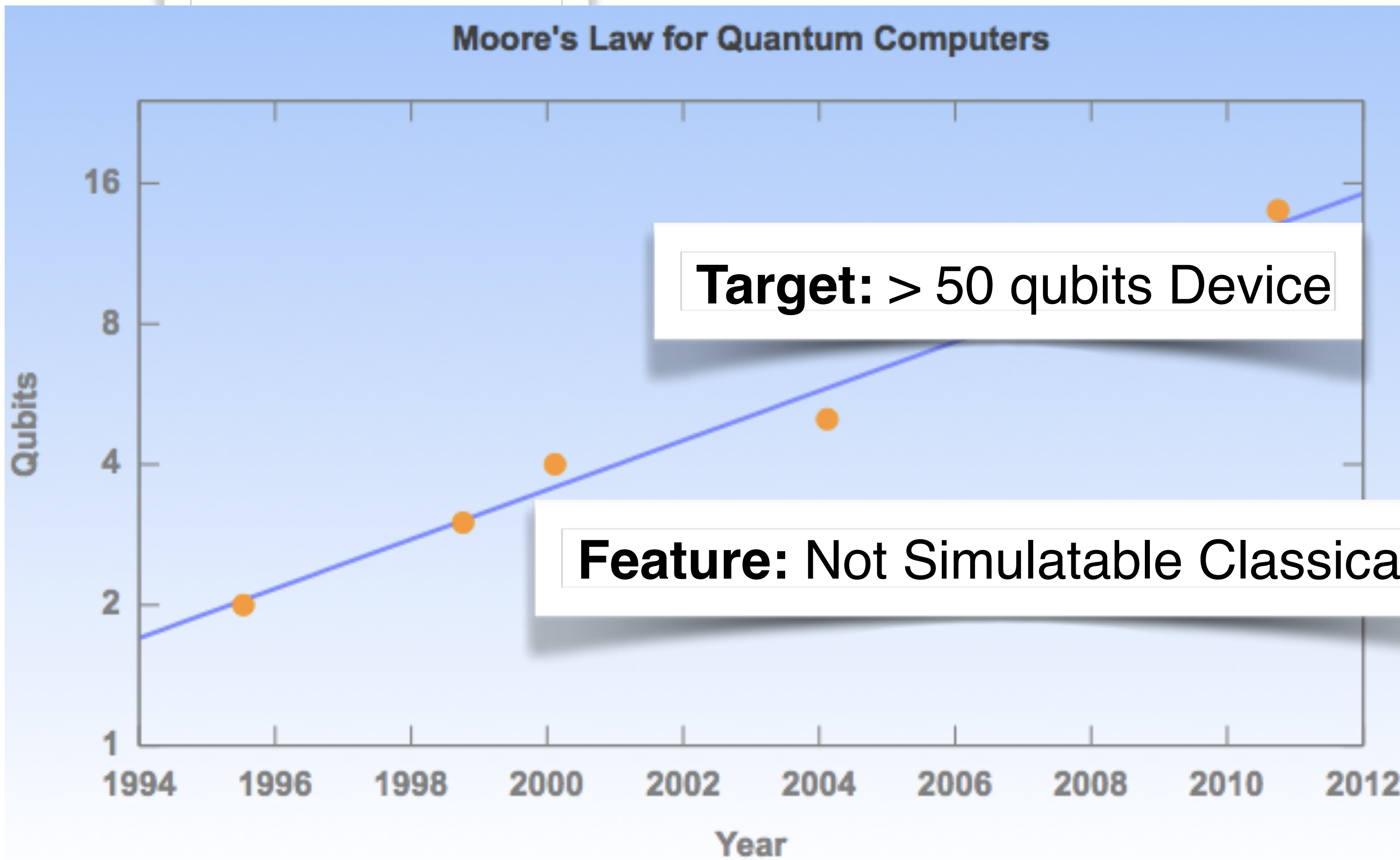
Target: > 50 qubits Device

Private Investments

Google, IBM, Intel,ATOS,Alibaba
Big VC founds
Startups Companies

Quantum Era

National Investments



Target: > 50 qubits Device

Feature: Not Simulatable Classically

Private Investments

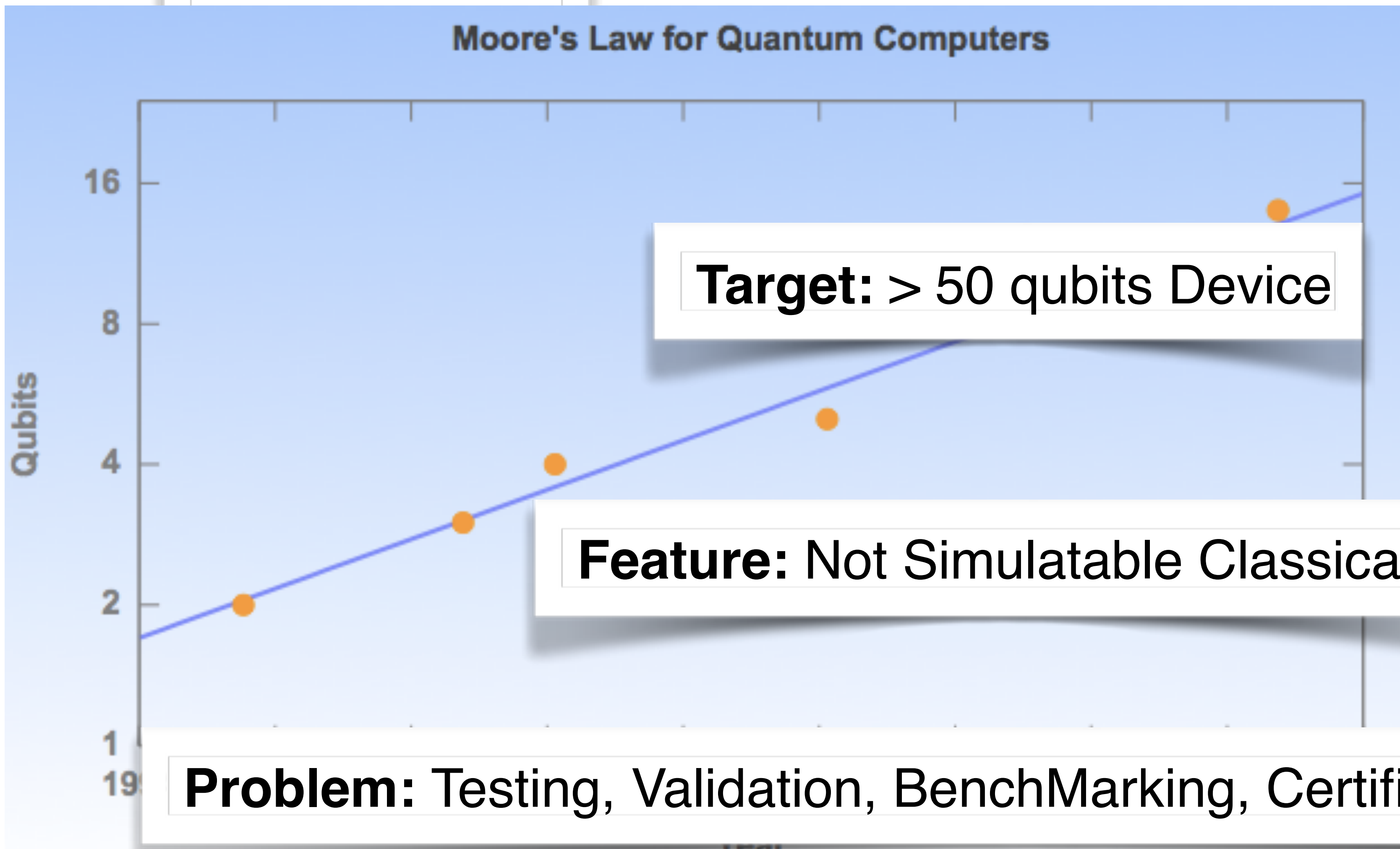
Google, IBM, Intel,ATOS,Alibaba
Big VC founds
Startups Companies

Quantum Era

National Investments

Private Investments

Google, IBM, Intel,ATOS,Alibaba
Big VC founds
Startups Companies



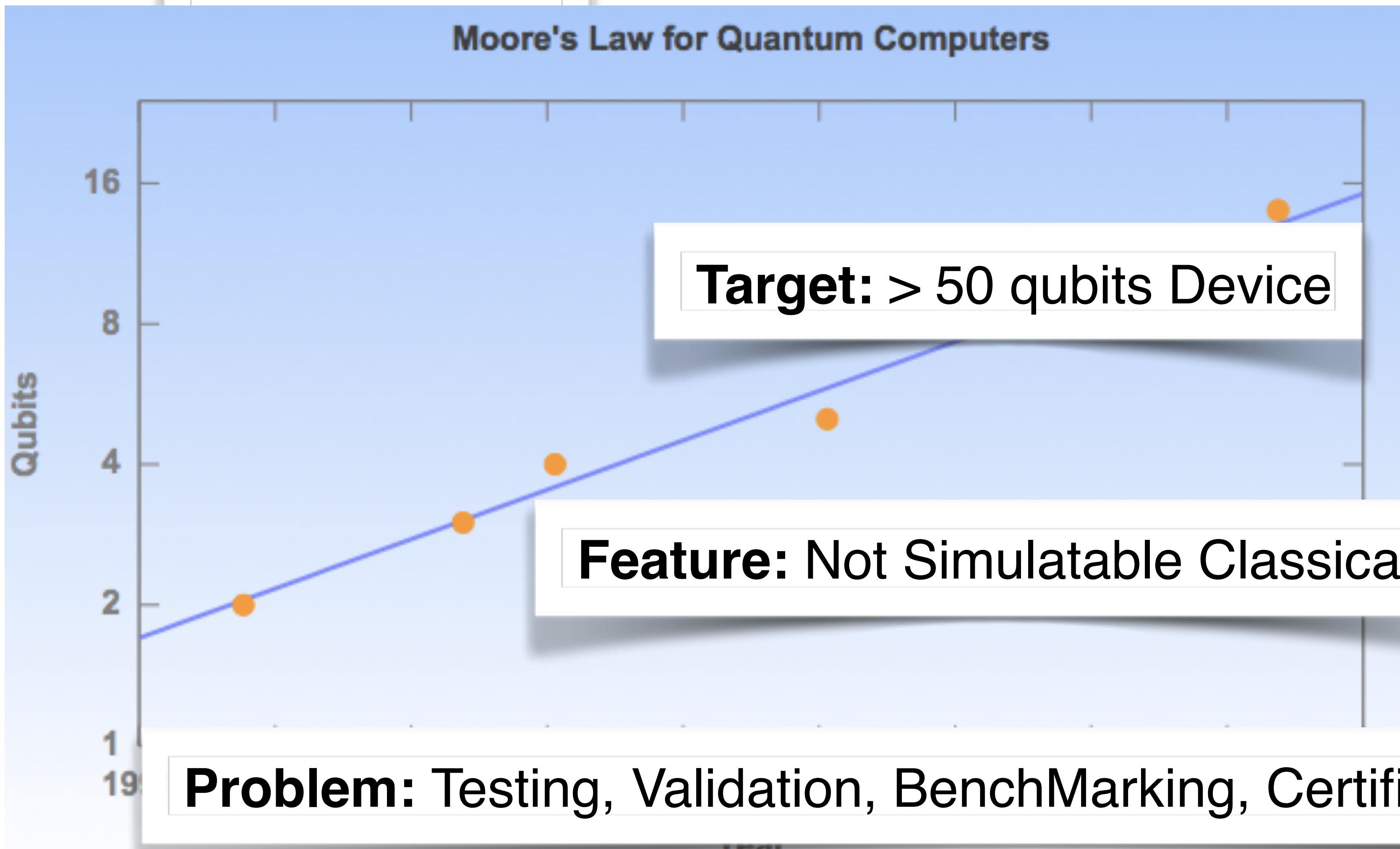
Target: > 50 qubits Device

Feature: Not Simulatable Classically

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

Quantum Era

National Investments



Private Investments

Google, IBM, Intel,ATOS,Alibaba
Big VC founds
Startups Companies

Target: > 50 qubits Device

Feature: Not Simulatable Classically

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

Can we BOOTSTRAP a smaller quantum device to test a bigger one?

Quantum Verification

Efficient verification methods for realistic quantum devices

Quantum Verification

Efficient verification methods for realistic quantum devices

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

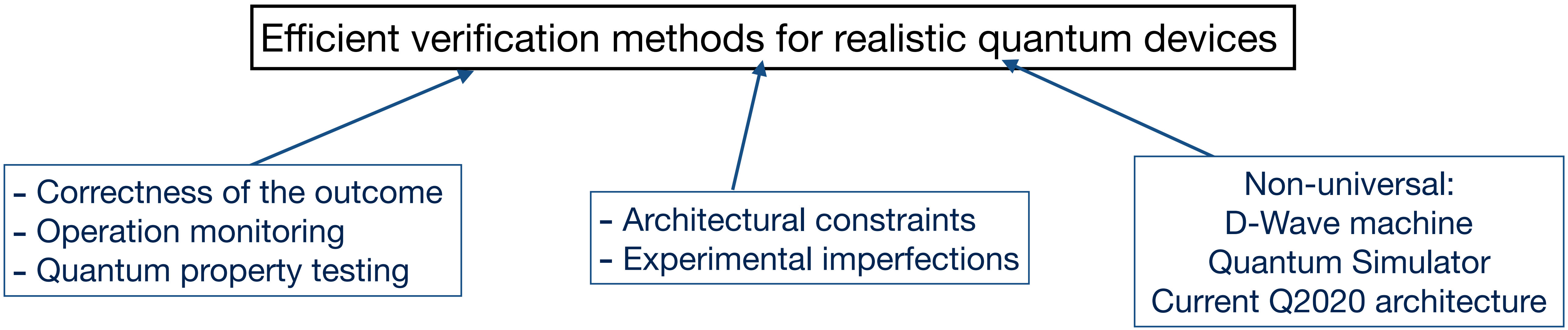
Quantum Verification

Efficient verification methods for realistic quantum devices

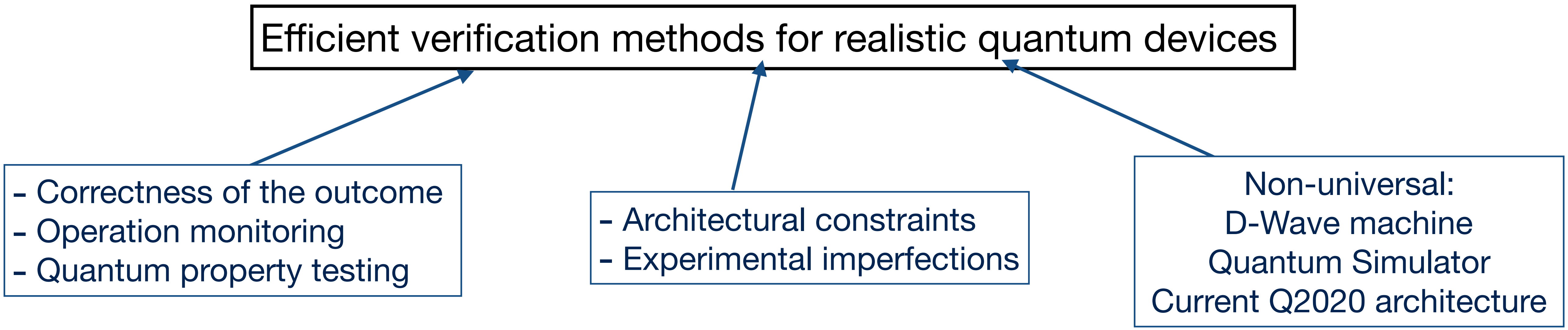
- Correctness of the outcome
- Operation monitoring
- Quantum property testing

- Architectural constraints
- Experimental imperfections

Quantum Verification



Quantum Verification



Goal

Criteria to test emerging quantum devices

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**

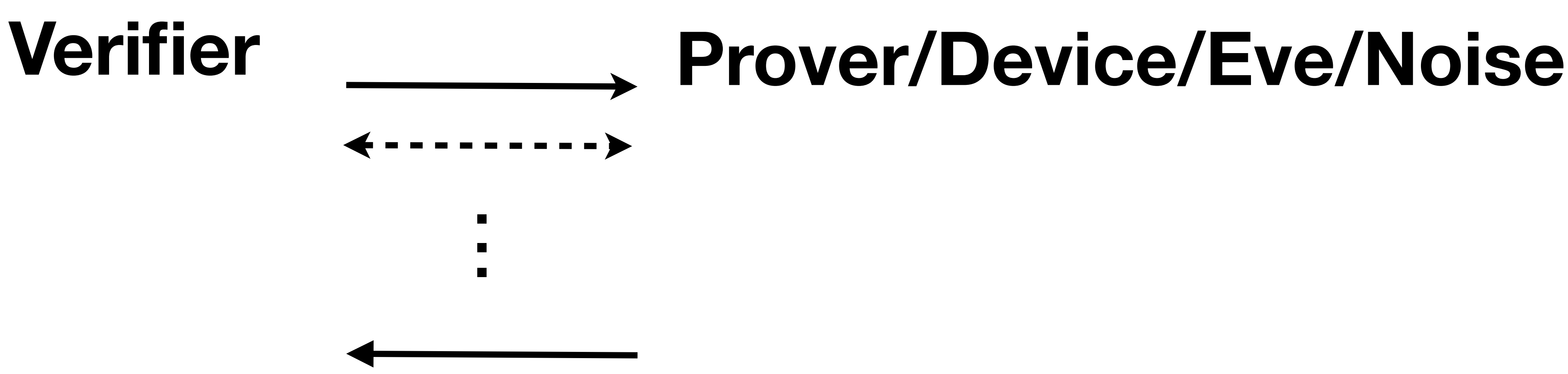
A mechanism that **probability** of witness is accepted and the outcome is **bad is bounded**

What is Verification

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

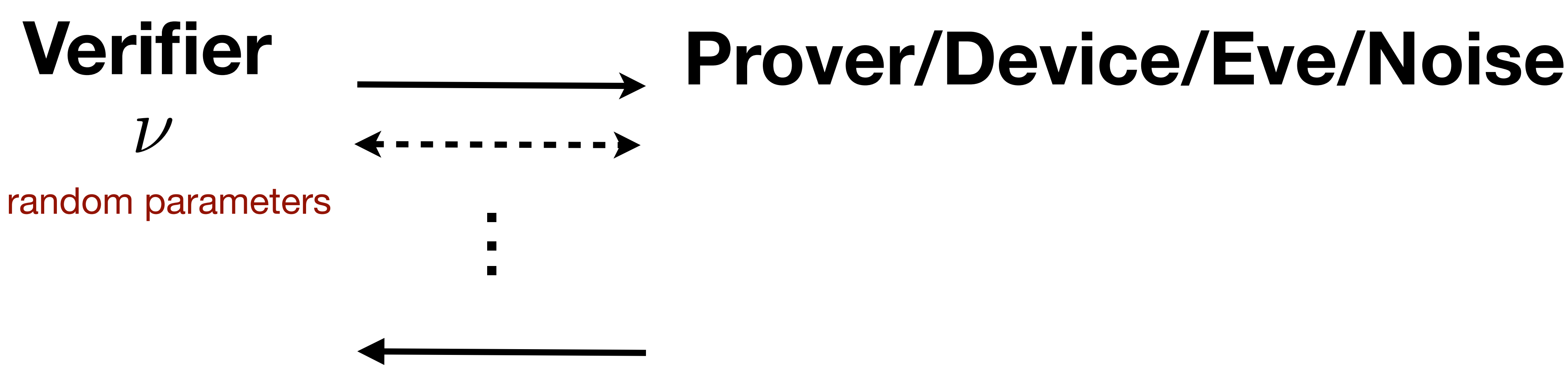
What is Verification

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



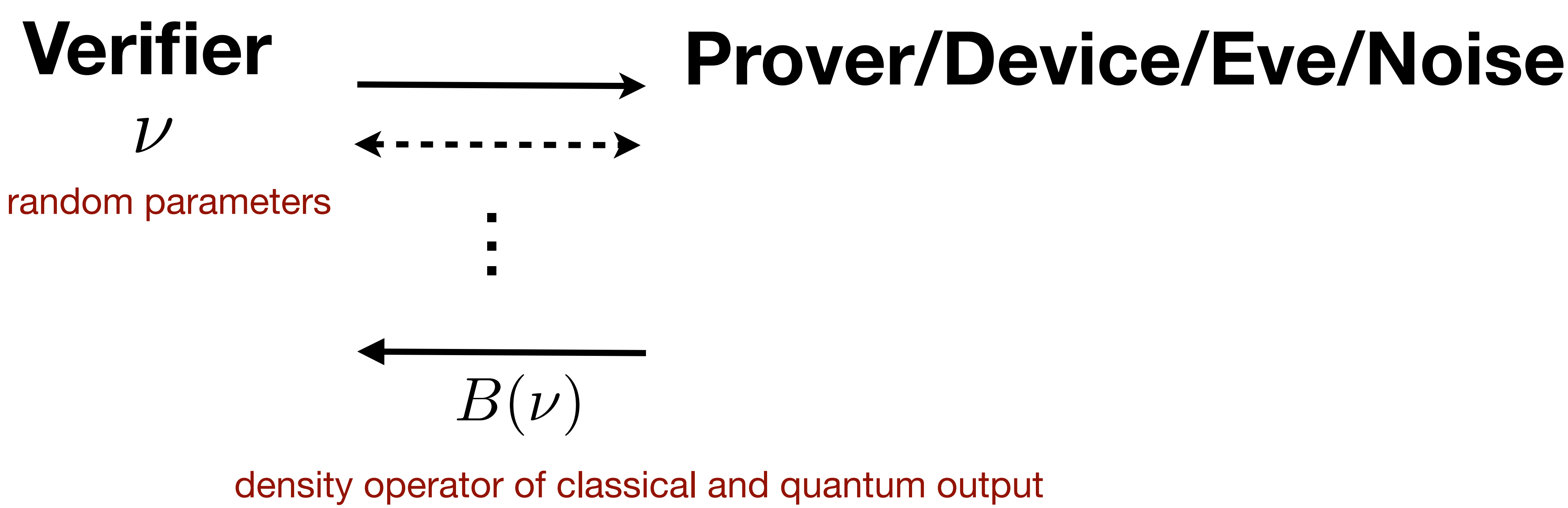
What is Verification

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



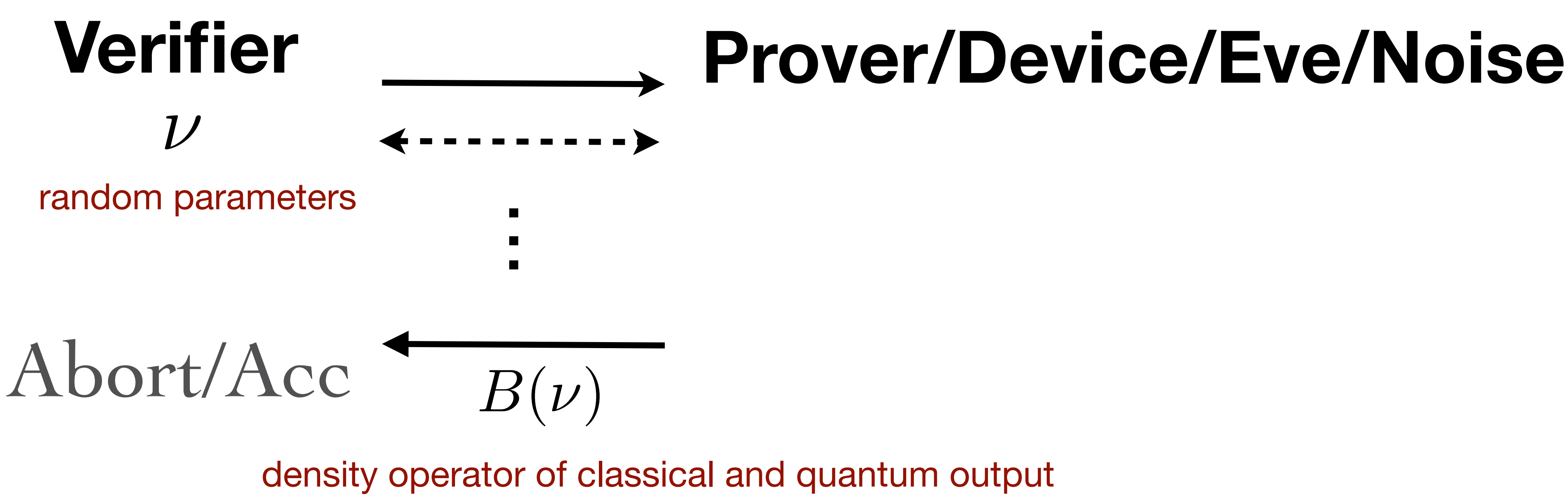
What is Verification

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

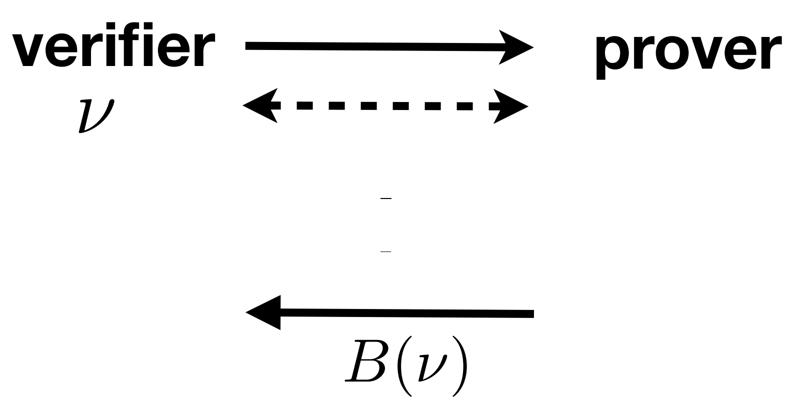


What is Verification

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

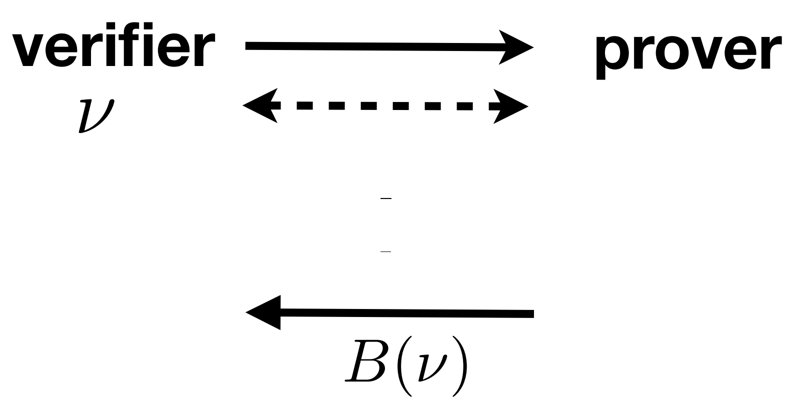


What is Verification



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

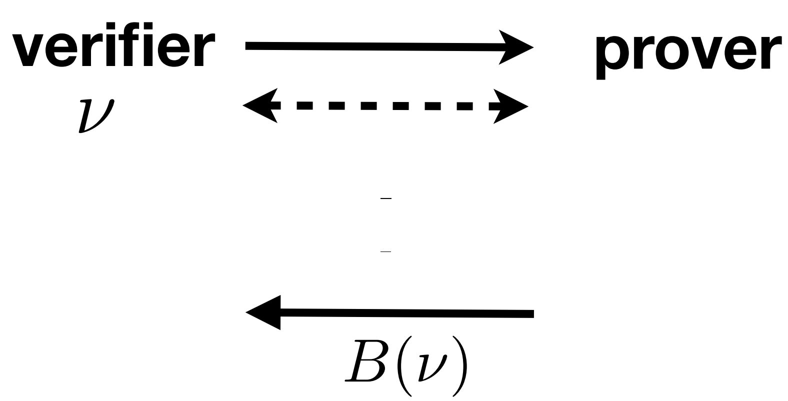
What is Verification



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

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

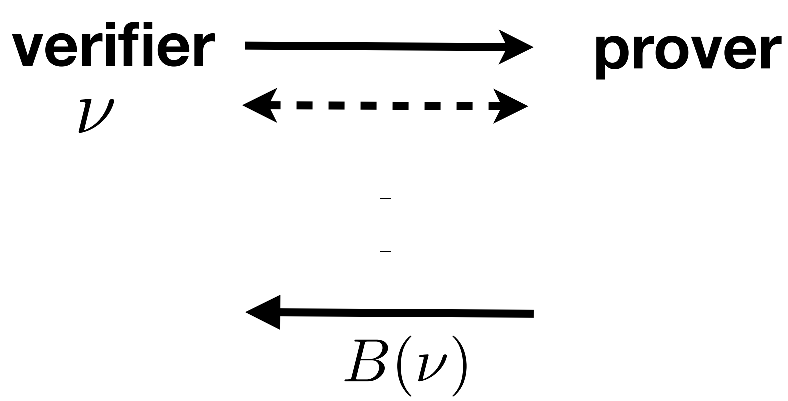
What is Verification



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

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

What is Verification

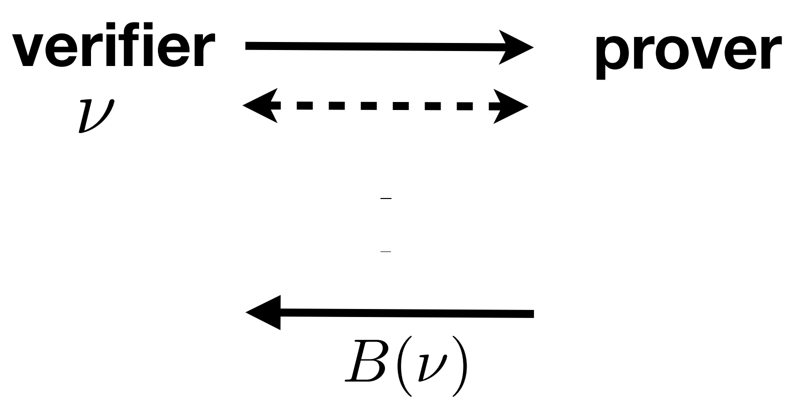


$$P^{\nu}_{incorrect} := P_{\perp} \otimes |acc\rangle\langle acc|$$

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

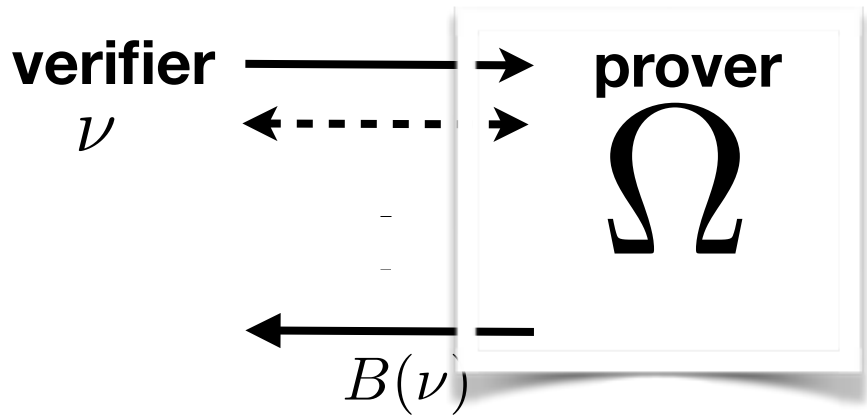


$$P^{\nu}_{incorrect} := P_{\perp} \otimes |acc\rangle\langle acc|$$

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

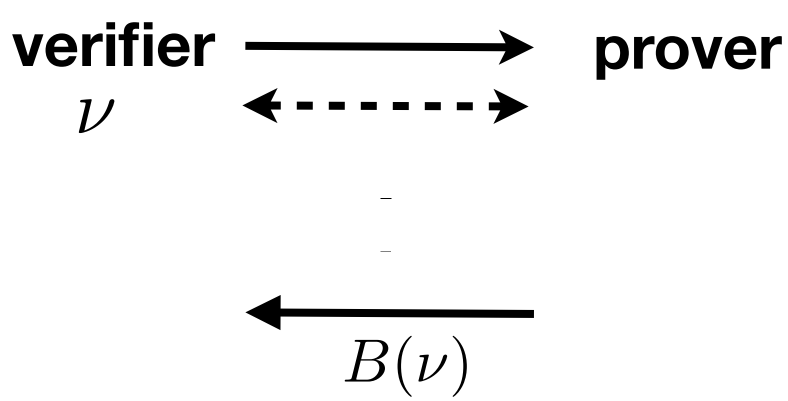


$$P^{\nu}_{incorrect} := P_{\perp} \otimes |acc\rangle\langle acc|$$

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

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

$$\Omega$$

How to deal with deviation

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

$$\Omega$$

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

How to deal with deviation

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

$$\Omega$$

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

$$\Omega_{Eve,system}$$

Quantum Hiding

Most General Deviation

$$\Omega_{Eve,system}$$

Quantum Hiding

$$\sigma_{testsubspace}$$

Most General Deviation

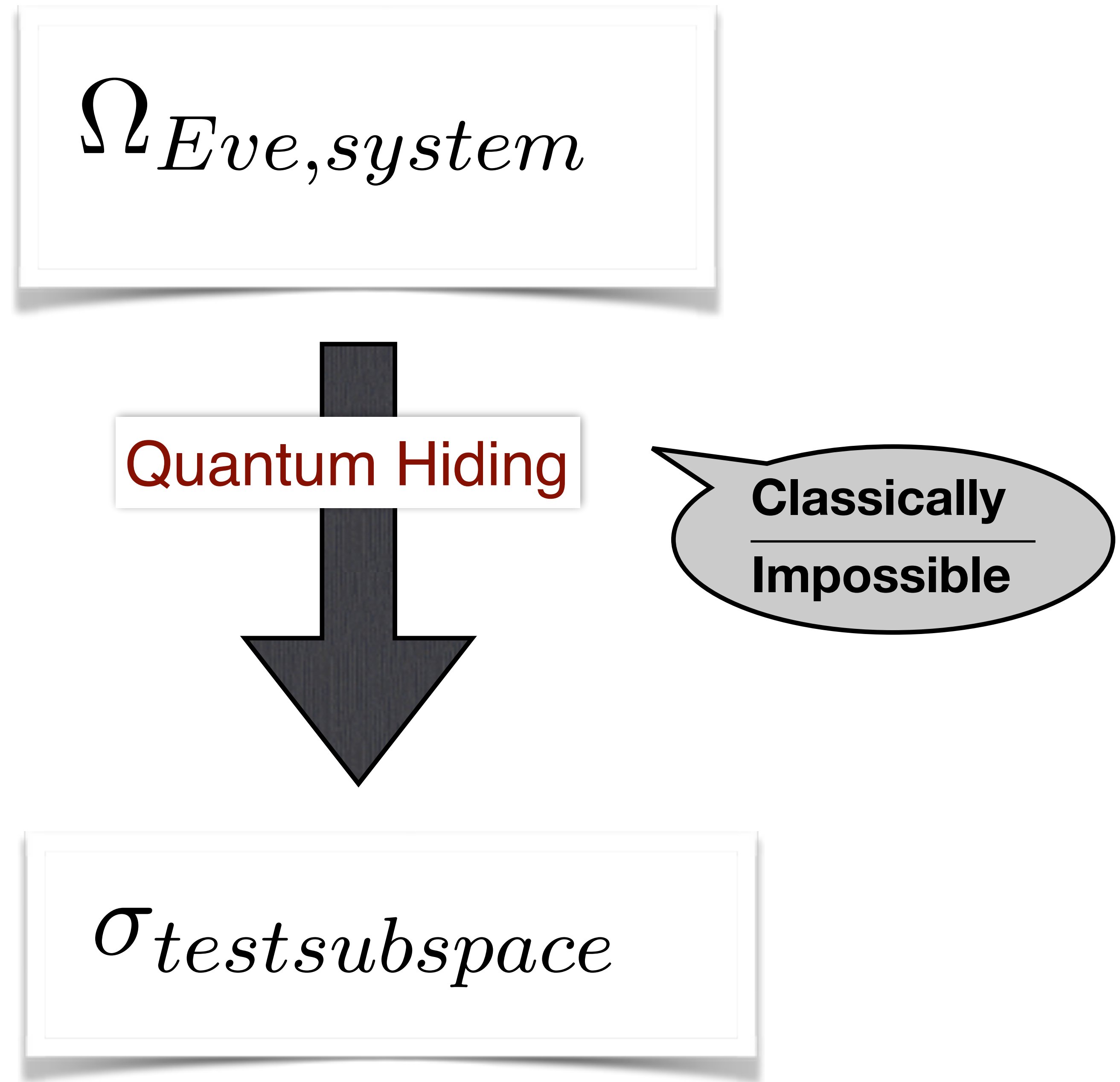
$$\Omega_{Eve,system}$$

Quantum Hiding

$$\sigma_{testsubspace}$$

Practical Protocols with No assumptions whatsoever

Most General Deviation



Practical Protocols with No assumptions whatsoever

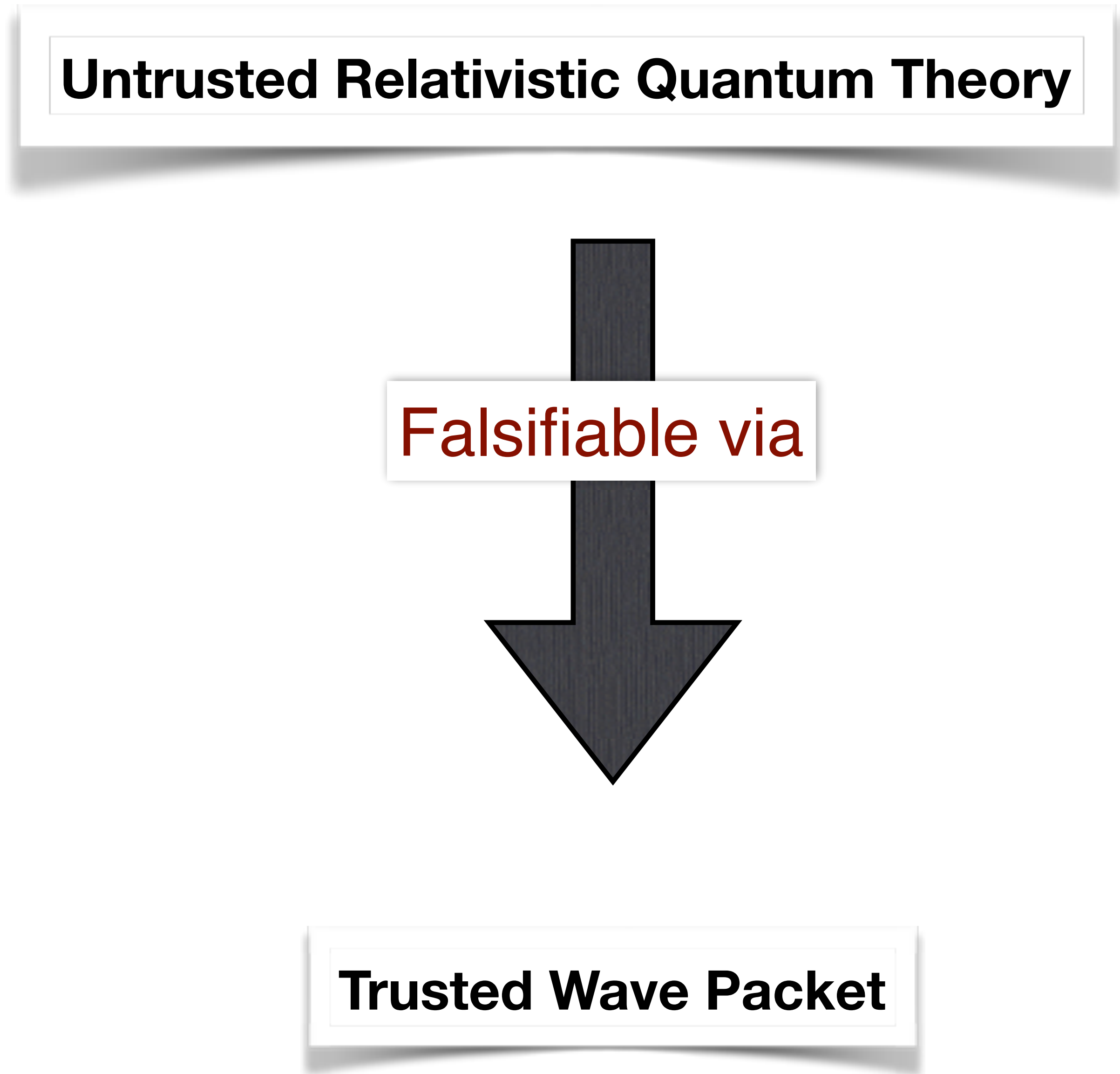
Entrapping Nature

Untrusted Quantum Theory

Falsifiable via

Trusted Quantum Measurement

Entrapping Nature



Global Directions on Verification

-

-

-

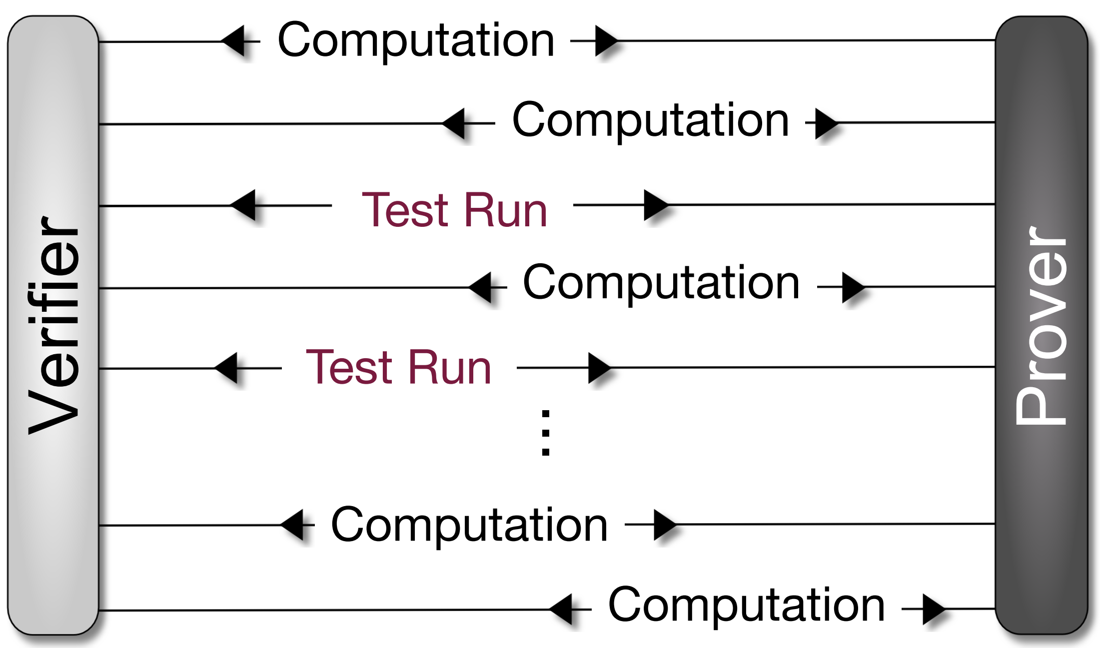
Global Directions on Verification

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

-
-
-

Global Directions on Verification

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



Global Directions on Verification

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

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

- It exists
- It is expanding

arXiv:1709.06984

Trust Worthy Quantum Information TyQi17 Paris

Verification of quantum computation:
An overview of existing approaches

- The overhead depends on the level of trust

Alexandru Gheorghiu, Theodoros Kapourniotis, Elham Kashefi

Measurements \ Entanglement	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 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

-

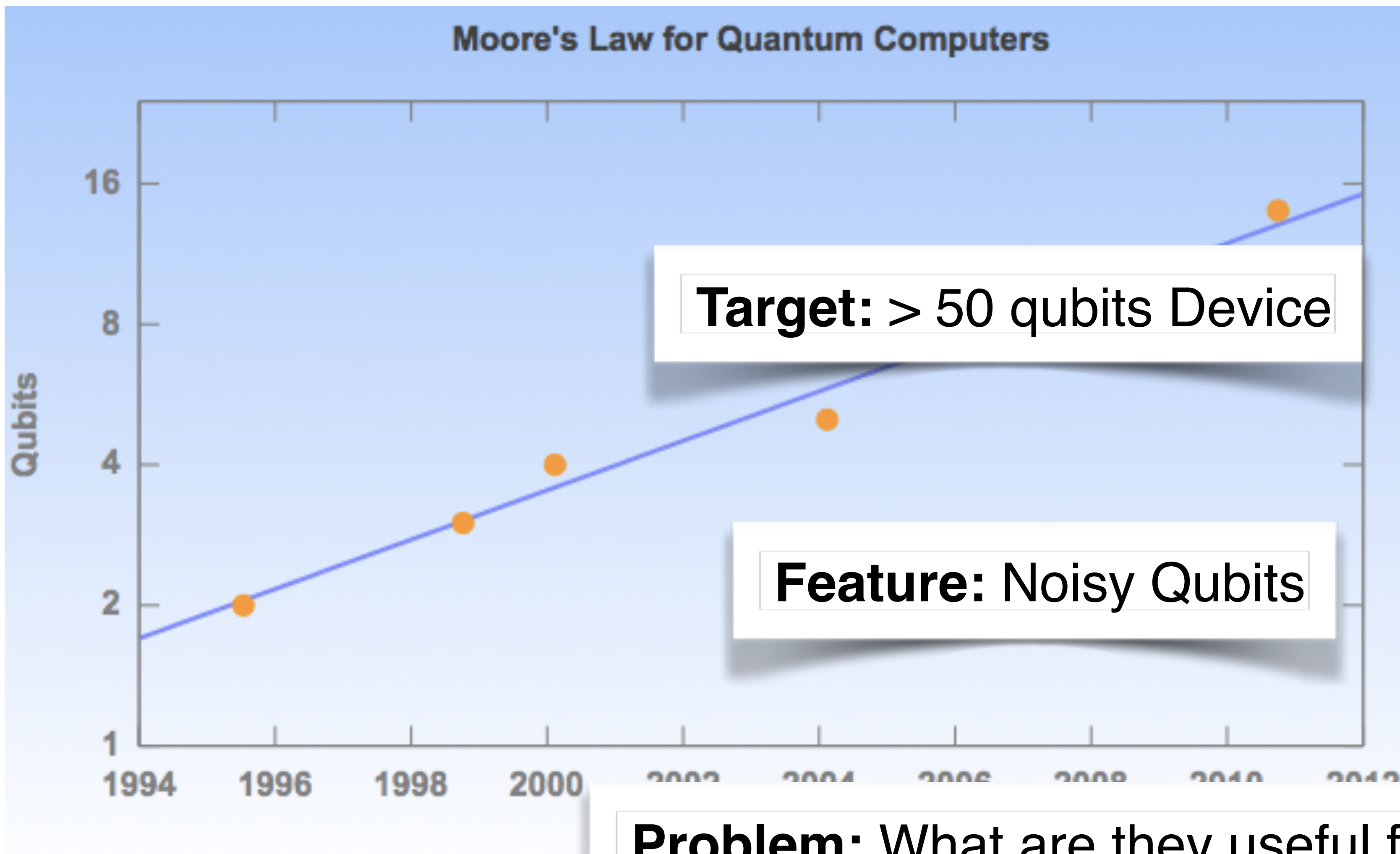
-

-

- Academic versus Industry's need

??? Objective improvements

Quantum Era



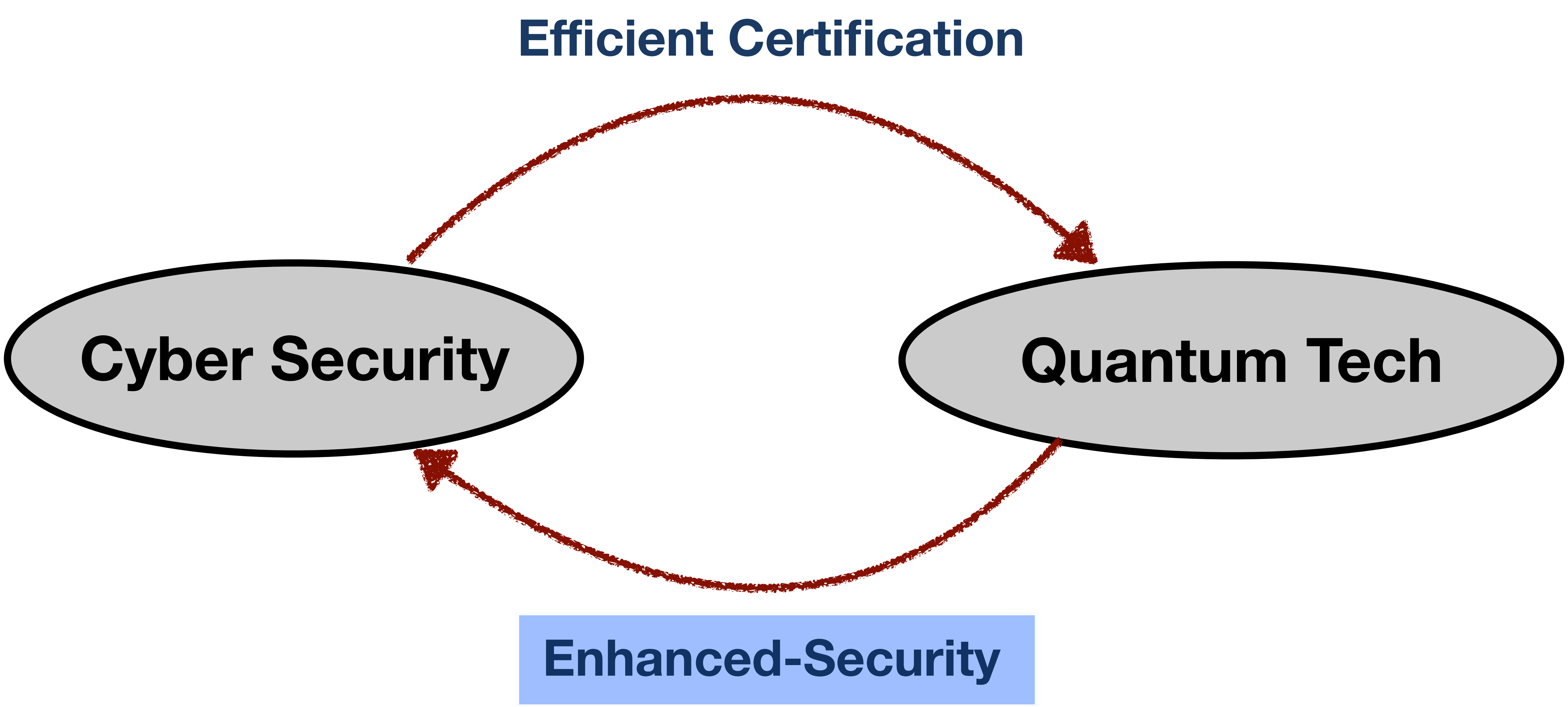
Target: > 50 qubits Device

Feature: Noisy Qubits

Problem: What are they useful for

Do we need to wait till error correcting codes became feasible

Classical - Quantum Collaboration Landscape



Quantum Cryptography

Protocols for hybrid classical-quantum communication network

- Electronic voting
- Fingerprinting
- Digital currency
- Secure cloud
- Blockchain
- Secure multi-party computing

Quantum Cryptography

Protocols for hybrid classical-quantum communication network

- Electronic voting
- Fingerprinting
- Digital currency
- Secure cloud
- Blockchain
- Secure multi-party computing

- Practical Security Analysis

Quantum Cryptography

Protocols for hybrid classical-quantum communication network

- Electronic voting
- Fingerprinting
- Digital currency
- Secure cloud
- Blockchain
- Secure multi-party computing

- Practical Security Analysis

- Standard telecom technology
- Long distance
- Long term stability
- Silicon-integrated
- Small scale devices

Quantum Crypto Status

-
-
-

Quantum Crypto Status

- It exists
- It is expanding

Quantum Cryptography QCrypt17 Cambridge

-

-

-

Quantum Crypto Status

- It exists
- It is expanding

Quantum Cryptography QCrypt17 Cambridge

-

-

-

- Quantum Protocols for Quantum Webs

- Q Fingerprinting
- Q Money
- Q Secure cloud
- Q Byzantine Agreement
- Q Secure multi-party computing

Quantum Crypto Status

- It exists
- It is expanding

Quantum Cryptography QCrypt17 Cambridge

-

-

-

- Quantum Protocols for Quantum Webs

- Q Fingerprinting
- Q Money
- Q Secure cloud
- Q Byzantine Agreement
- Q Secure multi-party computing

They need few qubits …. works with noisy one too

Quantum Crypto Challenge

Quantum Crypto Challenge

How to exploit them for Classical Web ?

Quantum Crypto Challenge

How to exploit them for Classical Web ?

- Academic versus Industry's need

Objective improvements

Quantum Crypto Challenge

How to exploit them for Classical Web ?

- Academic versus Industry's need

Objective improvements

Performances / Cost / Added values

Practical Classical SMPC

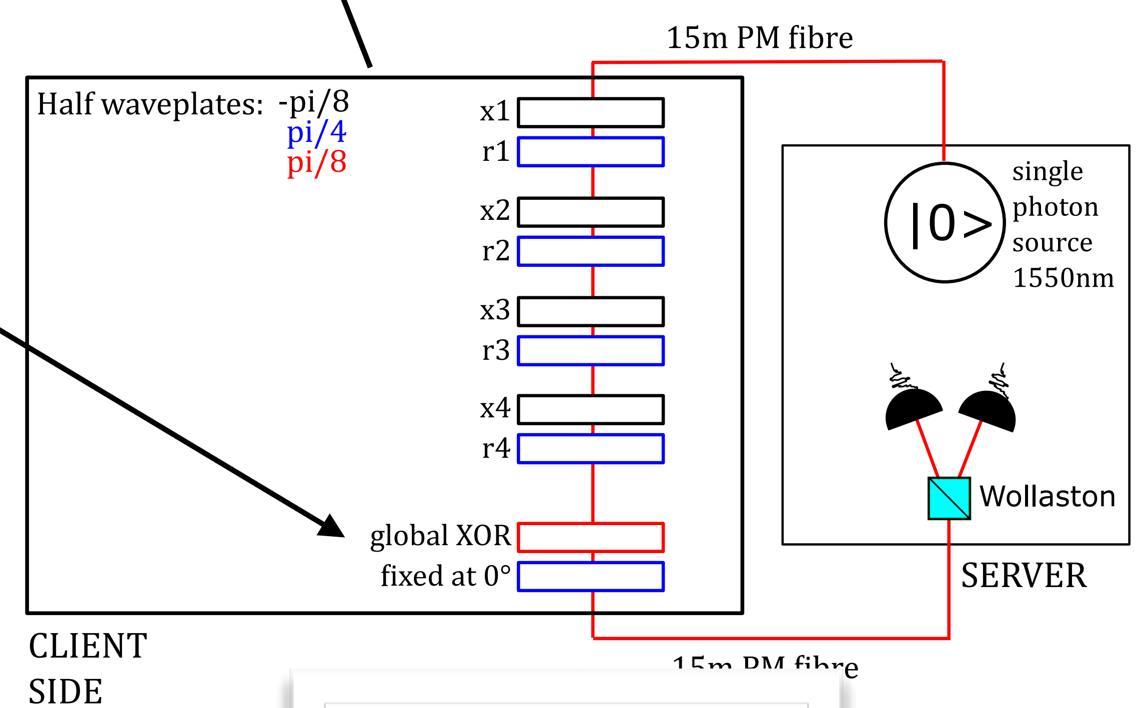
First large-scale practical experiment with SMPC to implement a secure auction 08

Recently: Efficient (low communication) computational SMPC

Computation represented by a series of additions and multiplications of elements in F_p.

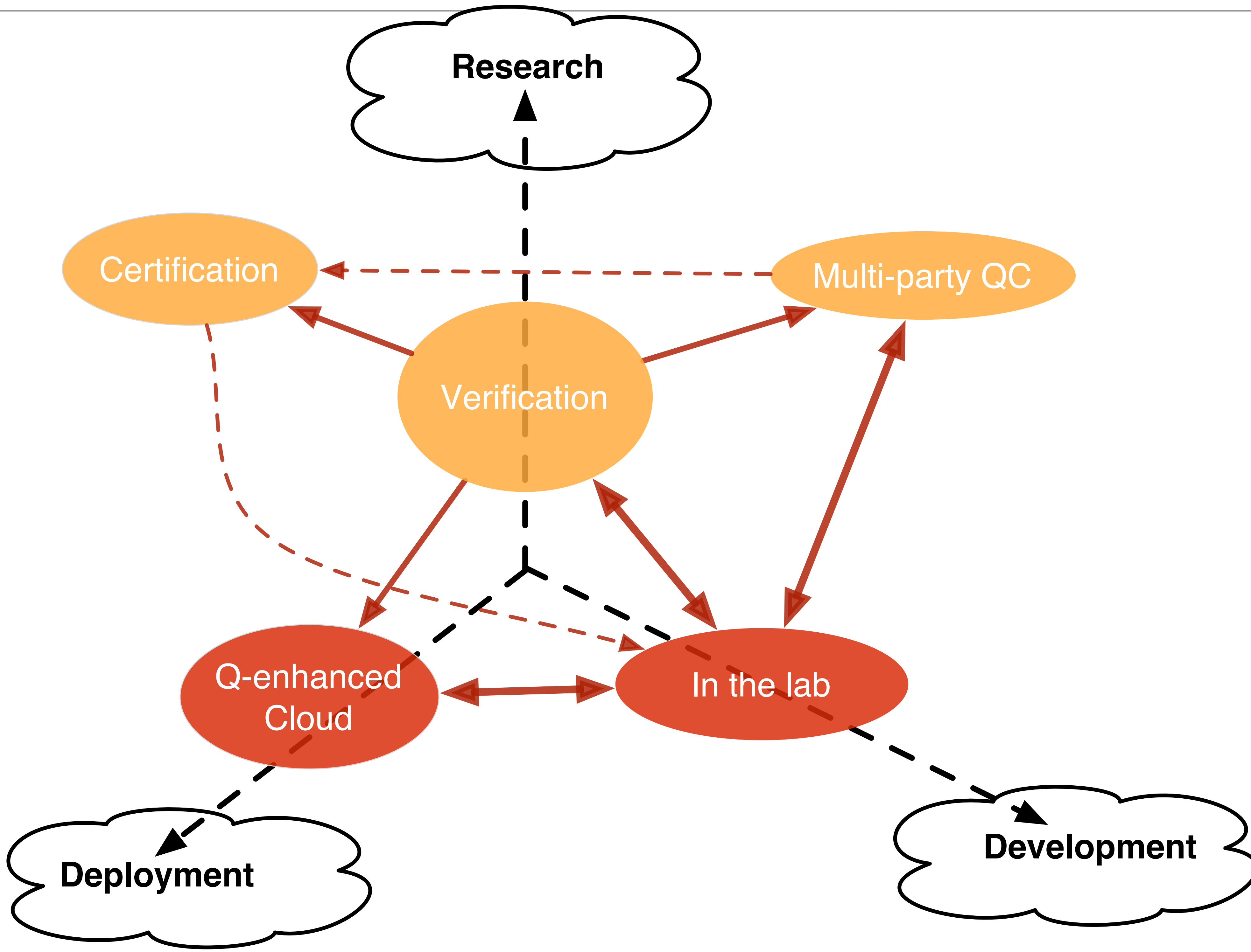
easy

Linear Verifiable Secret Sharing

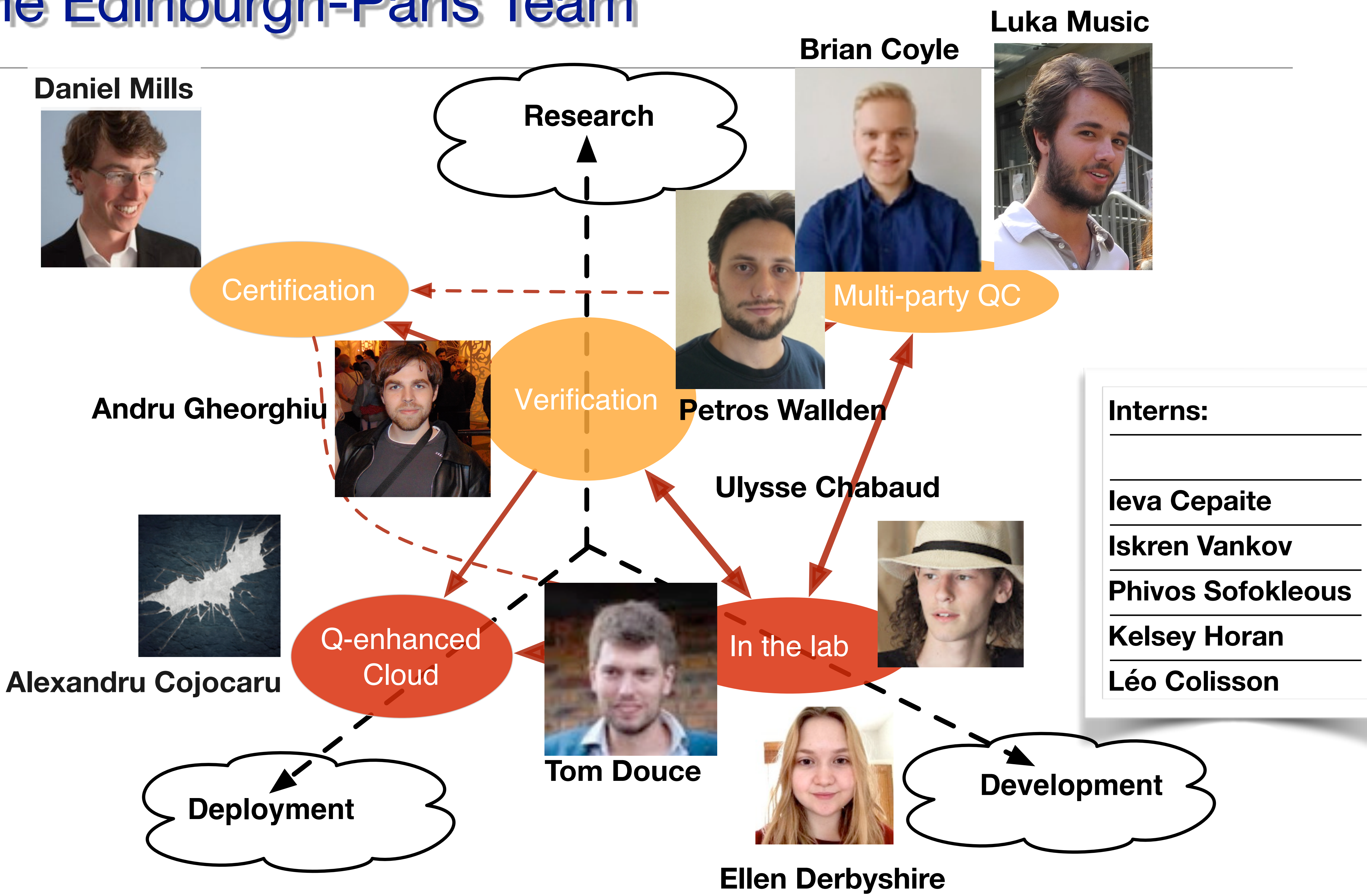


needs few qubits

The Edinburgh-Paris Team



The Edinburgh-Paris Team



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)

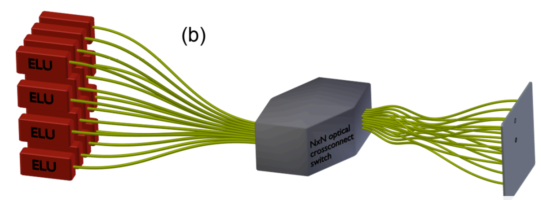
Experiment

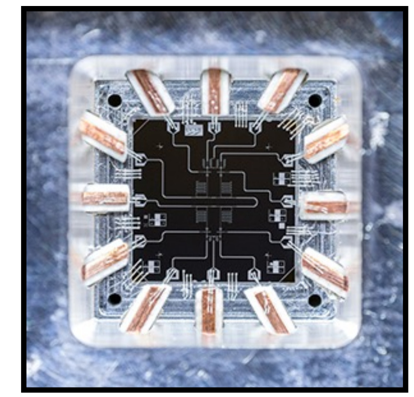
Stefanie Barz (Vienna,Oxford)
Philip Walther (Vienna)
Ian Walmsley (Oxford)

AIR FORCE OFFICE OF SCIENTIFIC RESEARCH
UNITED STATES AIR FORCE
EPSRC
Engineering and Physical Sciences Research Council
NQIT
UK NATIONAL QUANTUM TECHNOLOGIES PROGRAMME

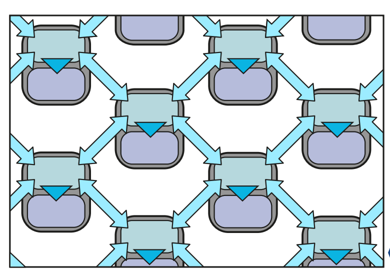
A girl simple dream

A girl simple dream

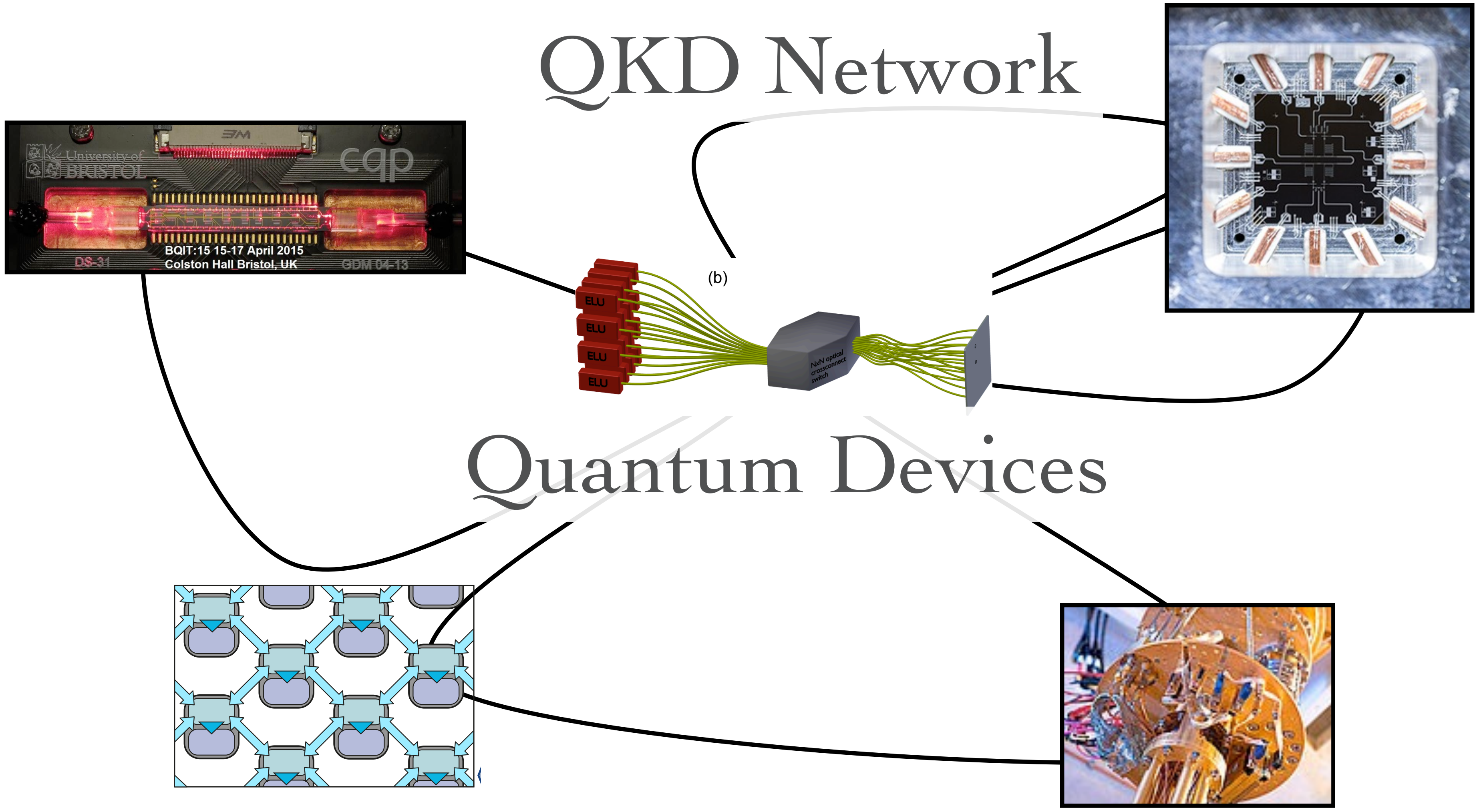




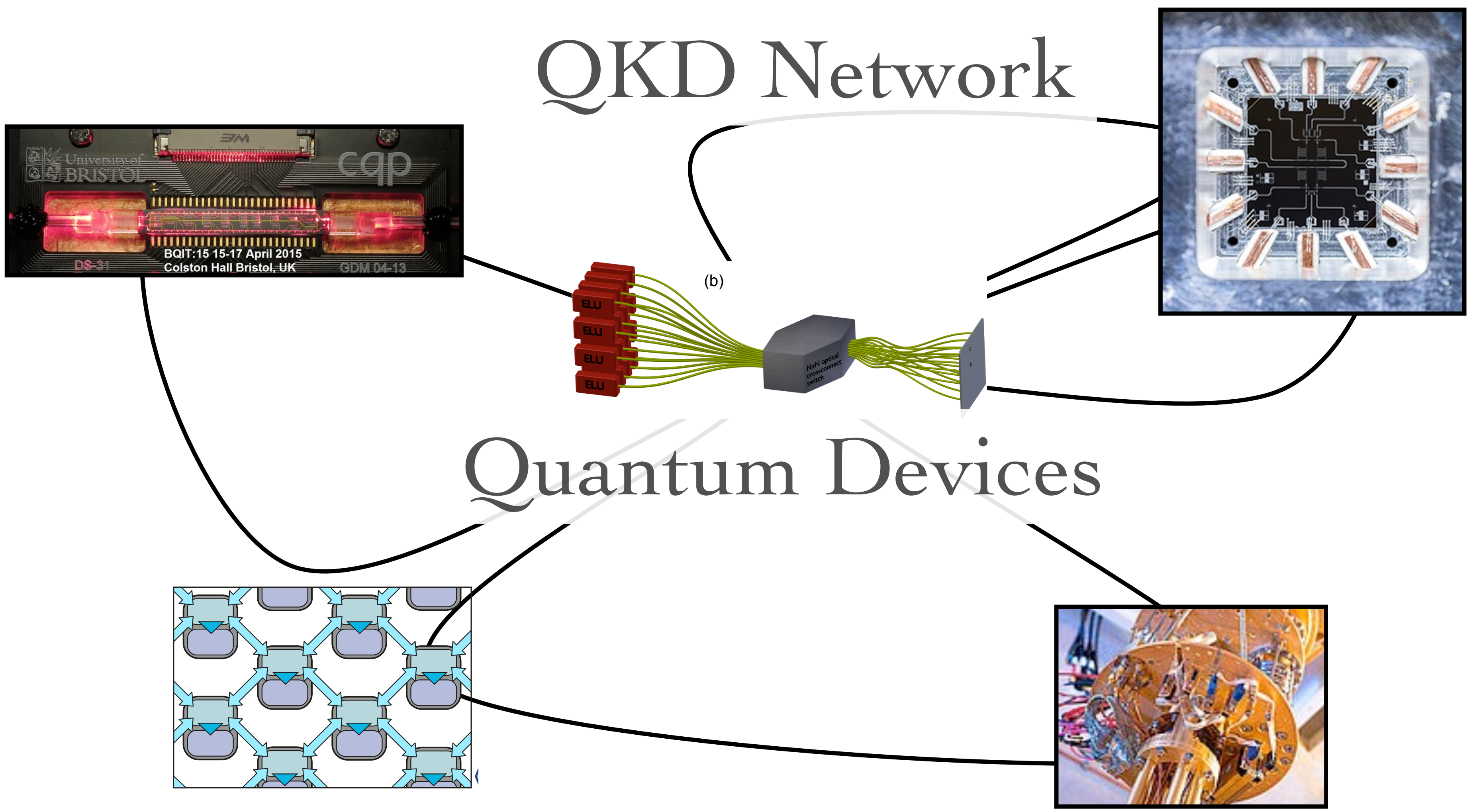
Quantum Devices



A girl simple dream



A girl simple dream



Global Verifiable Secure Quantum Web