Quantum Cyber Security
Past - Present - Future

Elham Kashefi

University of Edinburgh
CNRS, Pierre and Marie Curie University

Oxford Quantum Technology Hub
Paris Centre for Quantum Computing

Dec 1969

Dec 1969

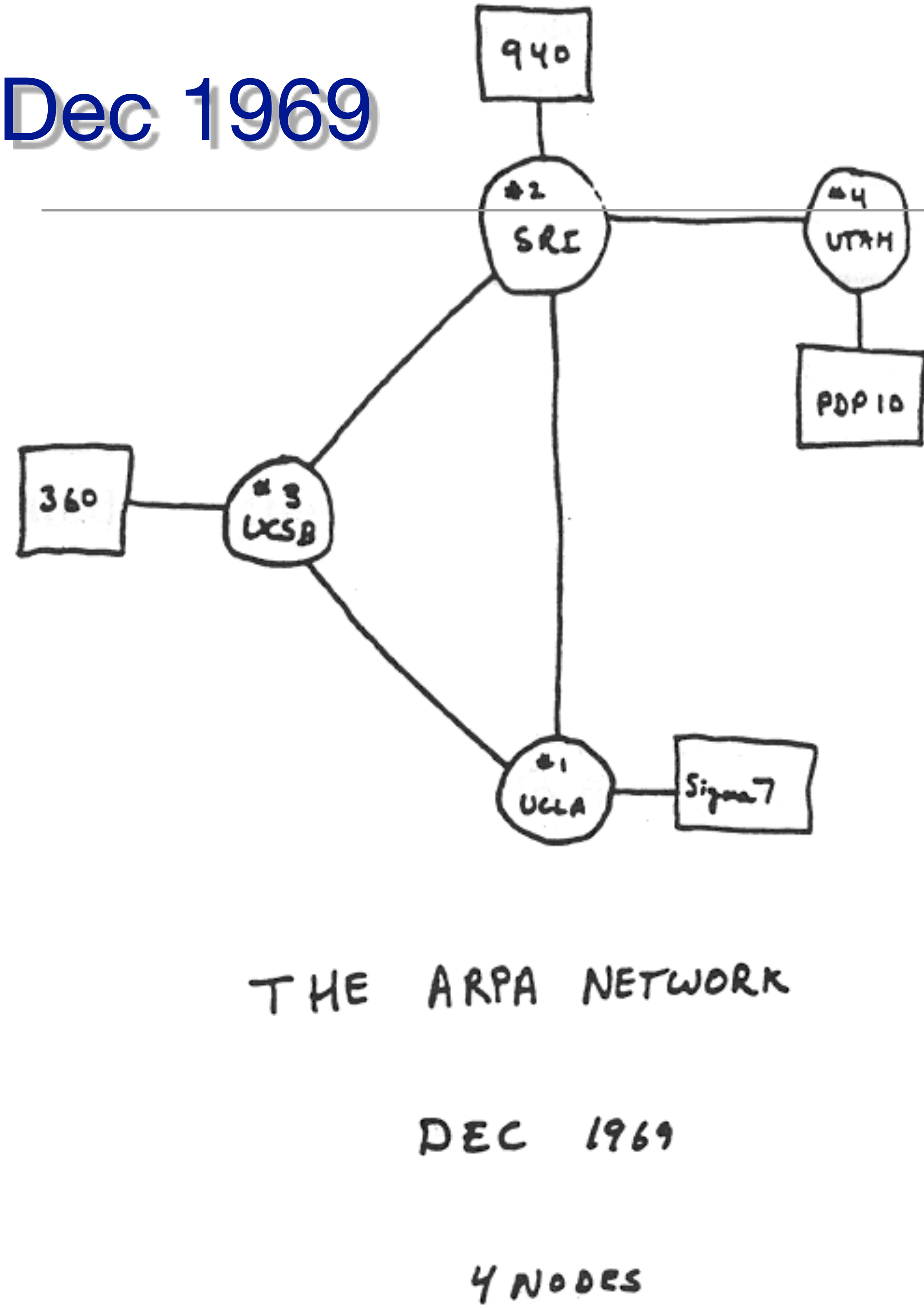


FIGURE 6.2 Drawing of 4 Node Network
(Courtesy of Alex McKenzie)

Dec 1969

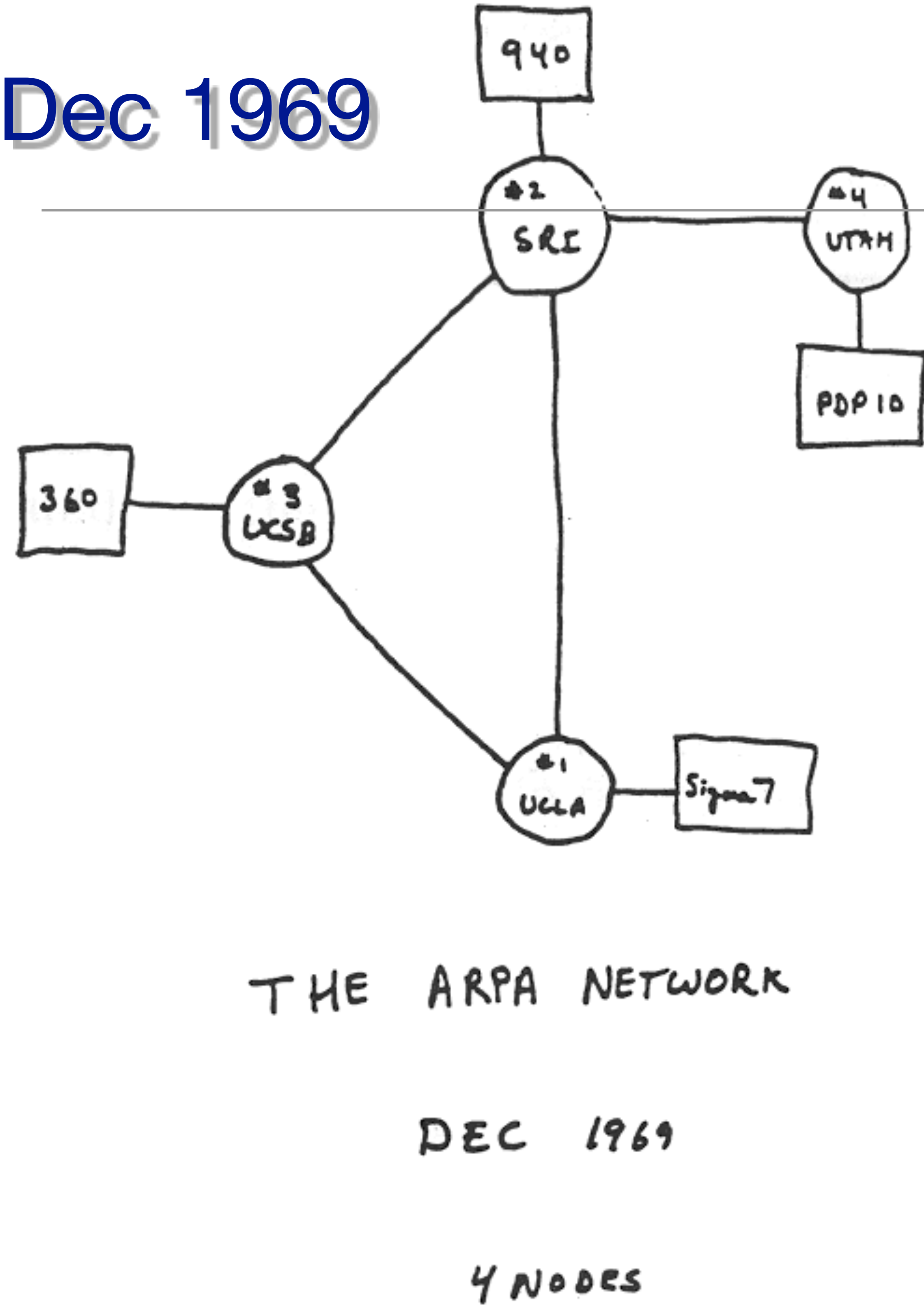
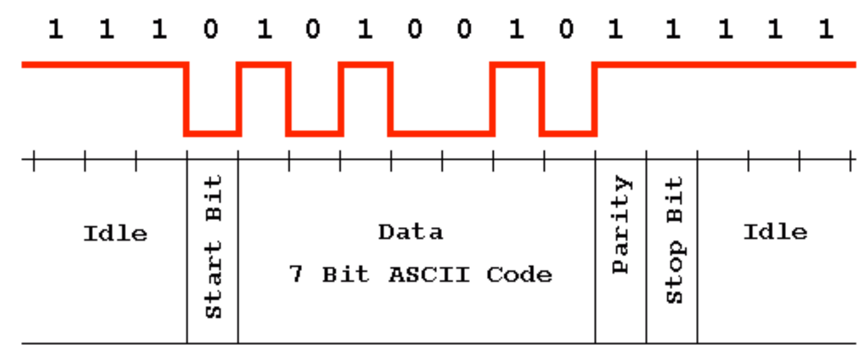


FIGURE 6.2 Drawing of 4 Node Network (Courtesy of Alex McKenzie)

bits communications



Dec 1969

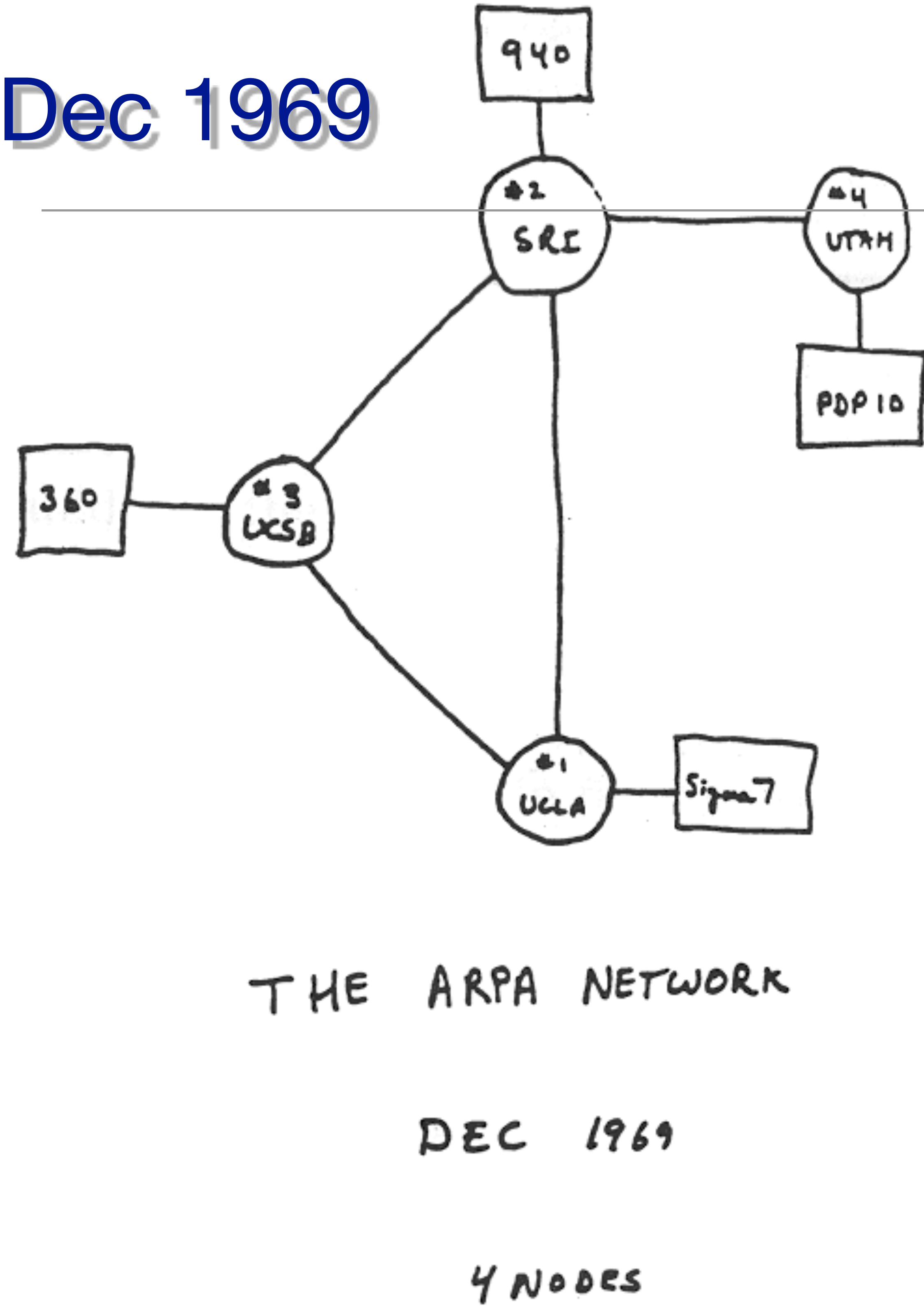
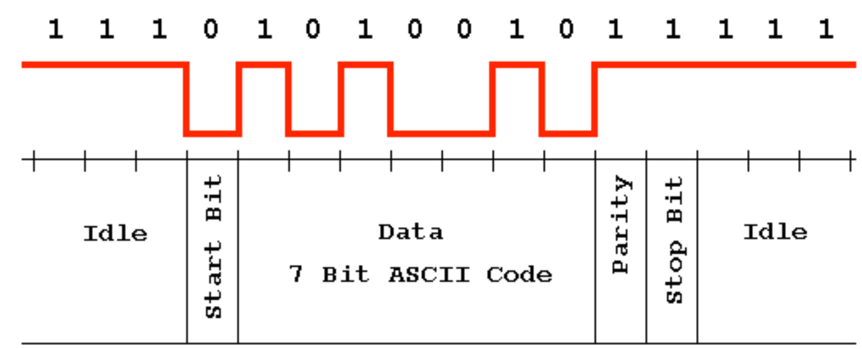
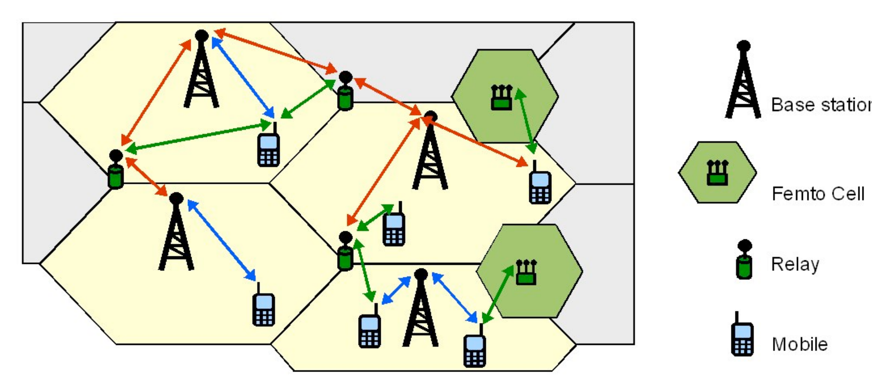
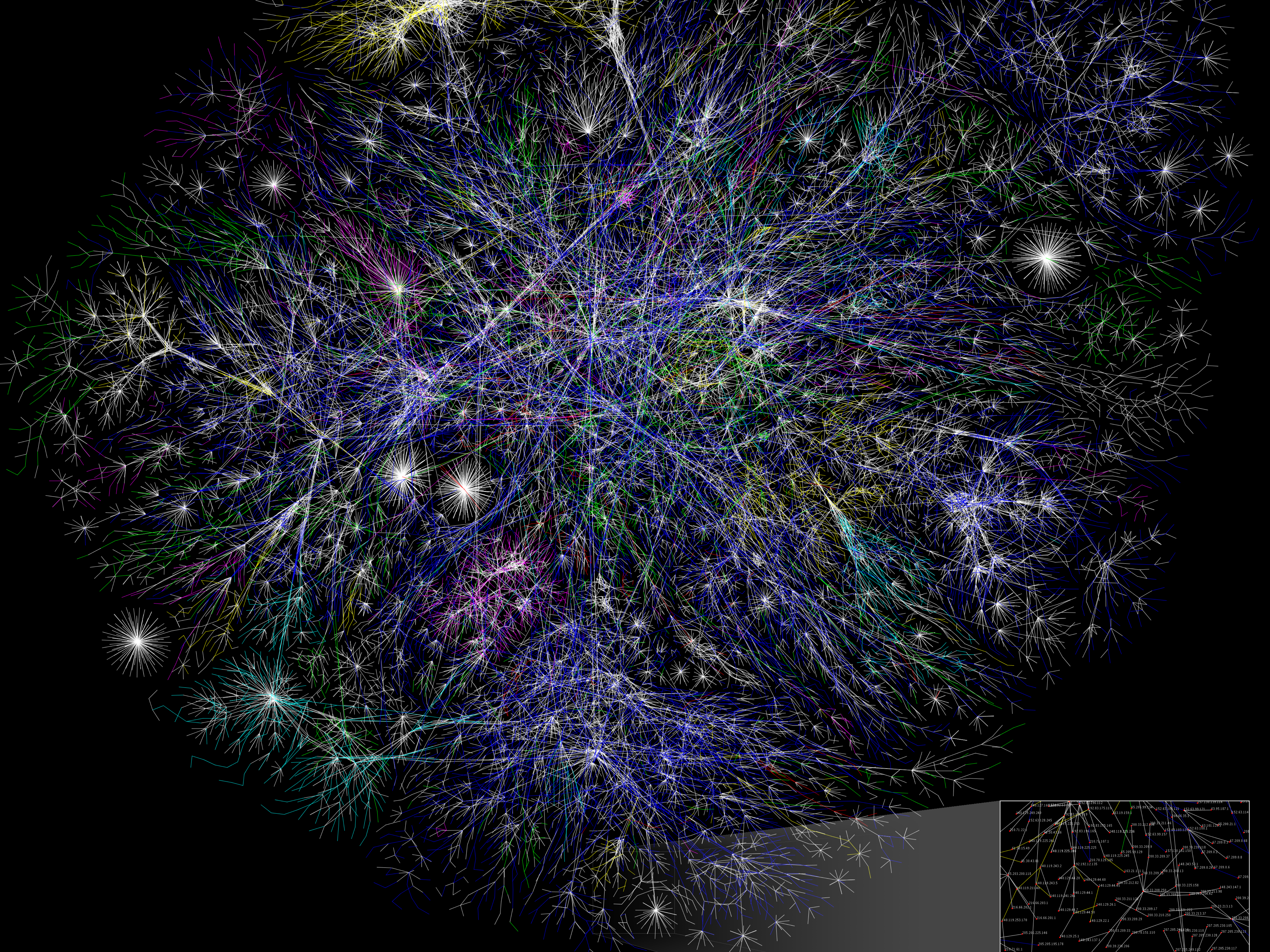


FIGURE 6.2 Drawing of 4 Node Network
(Courtesy of Alex McKenzie)

bits communications

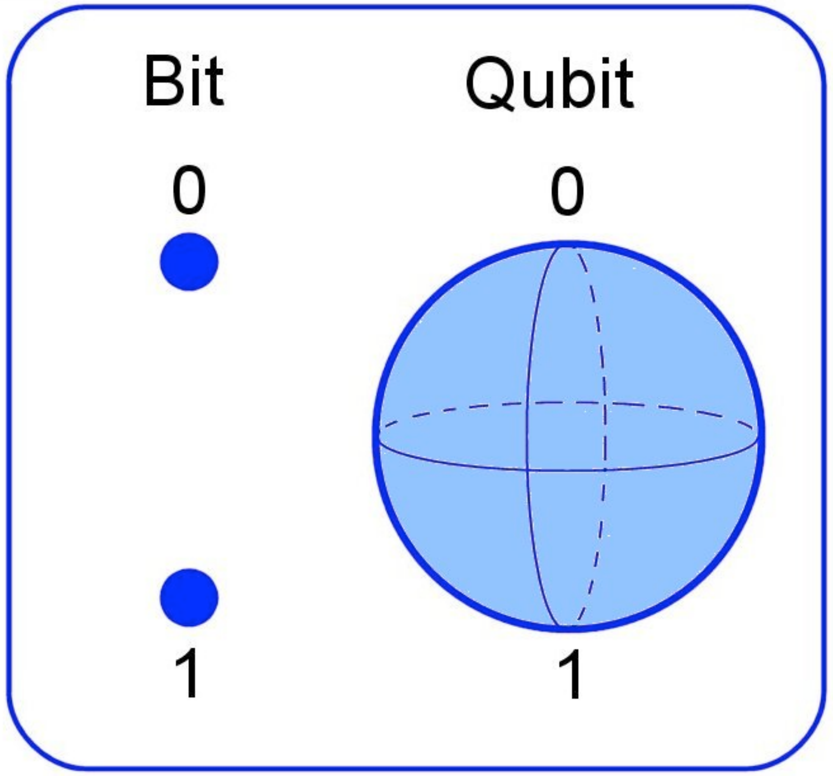






History repeats

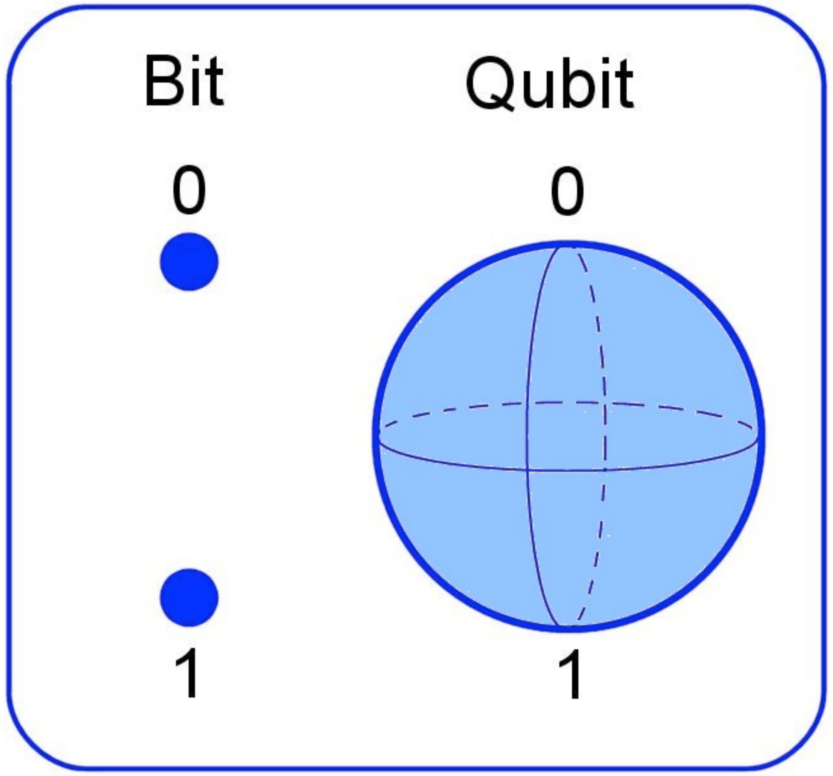
History repeats



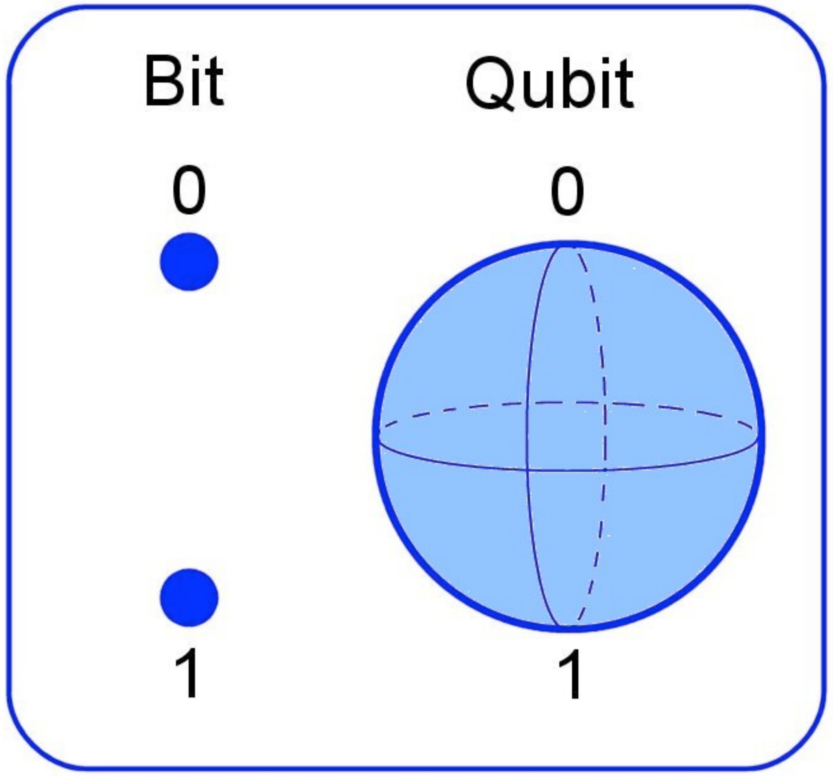
single qubits communications

History repeats

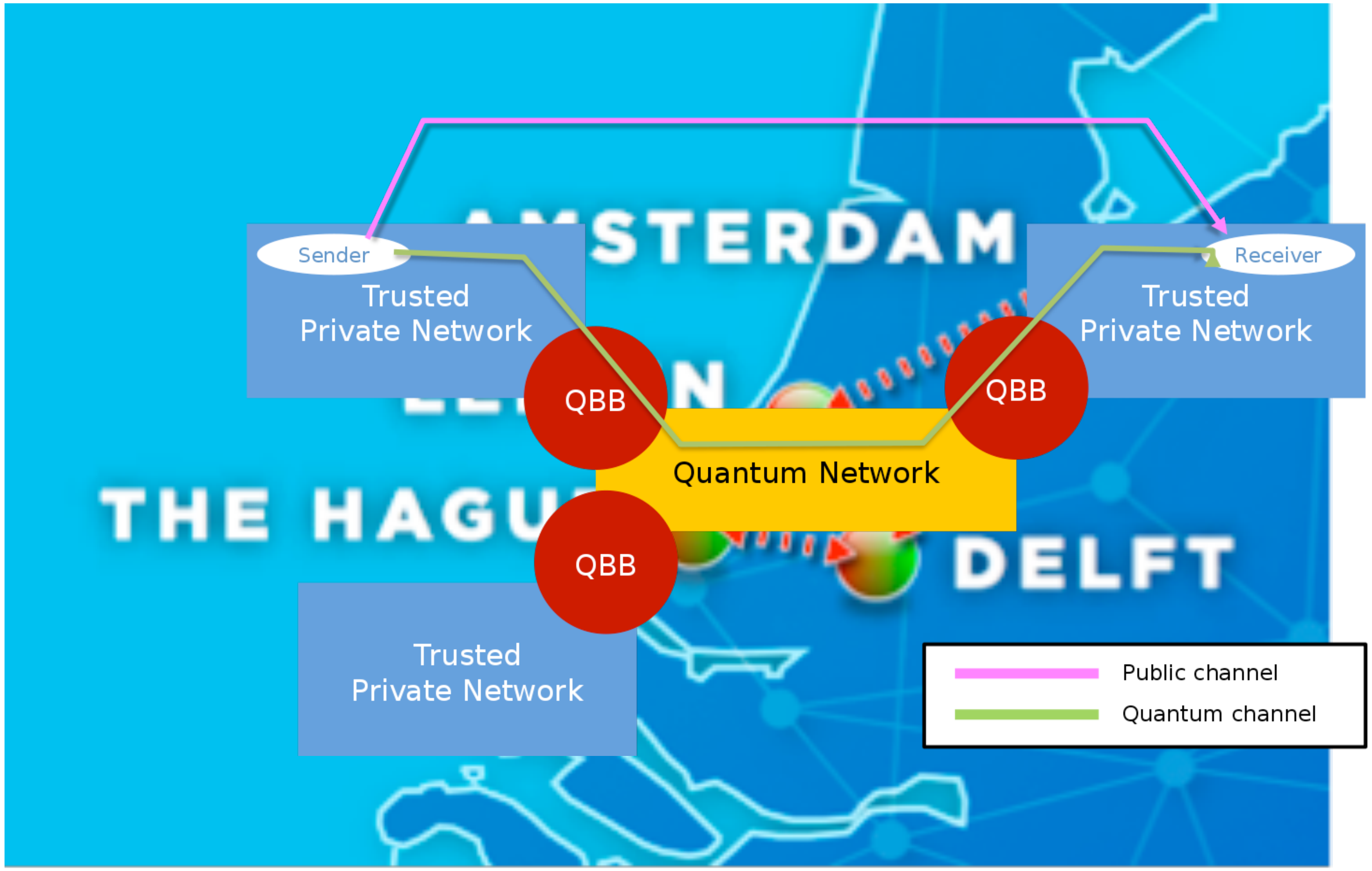
single qubits communications



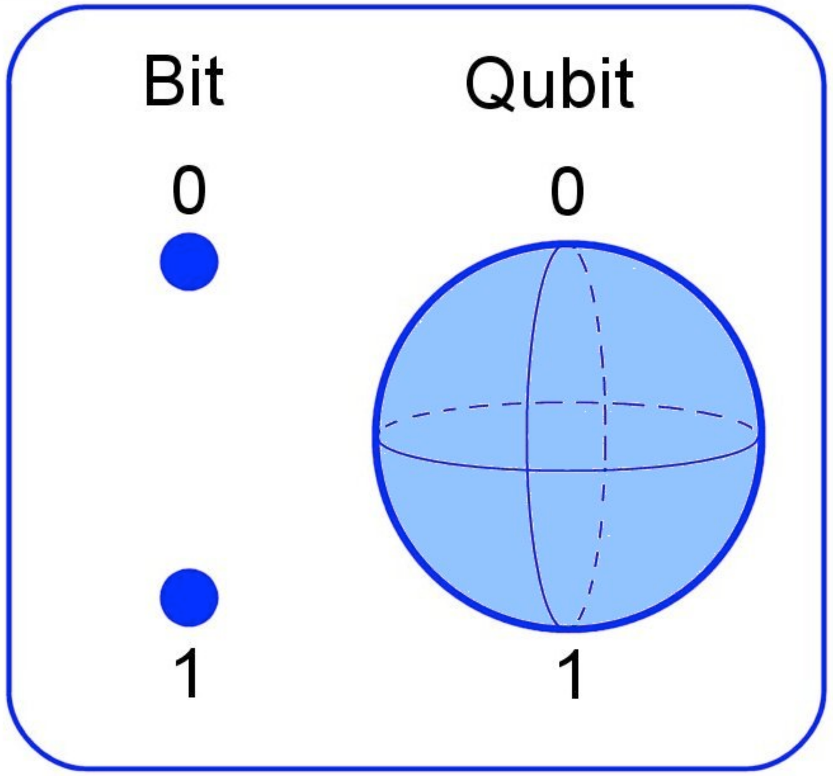
History repeats



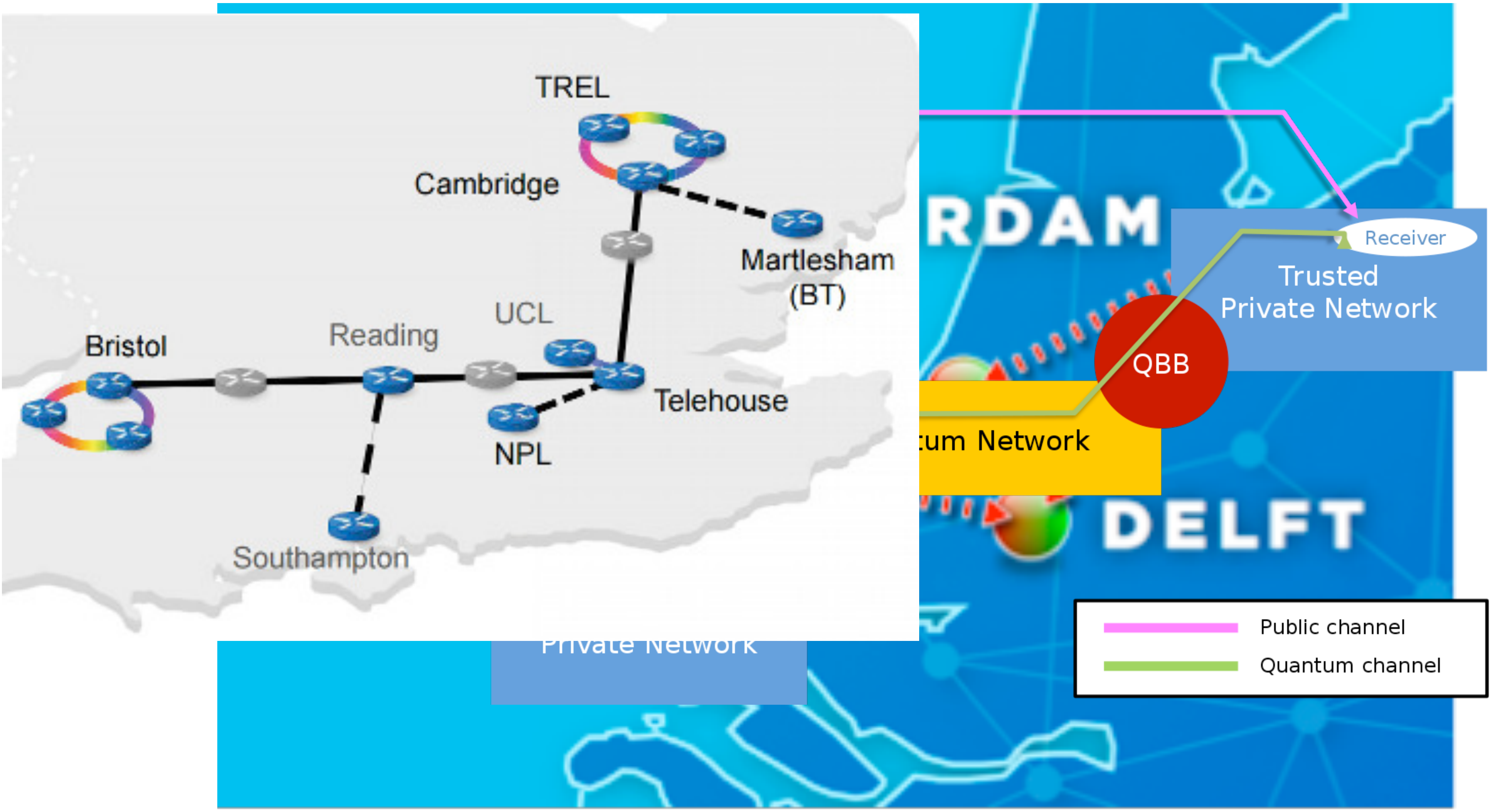
single qubits communications



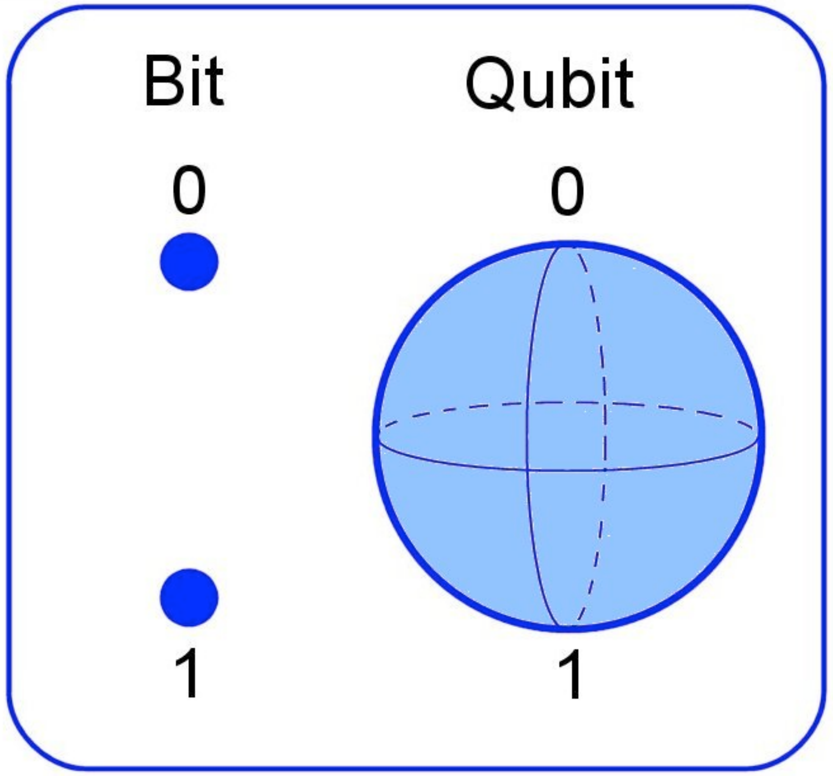
History repeats



single qubits communications



History repeats



single qubits communications

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,IonQ, Rigetti

Quantum Era

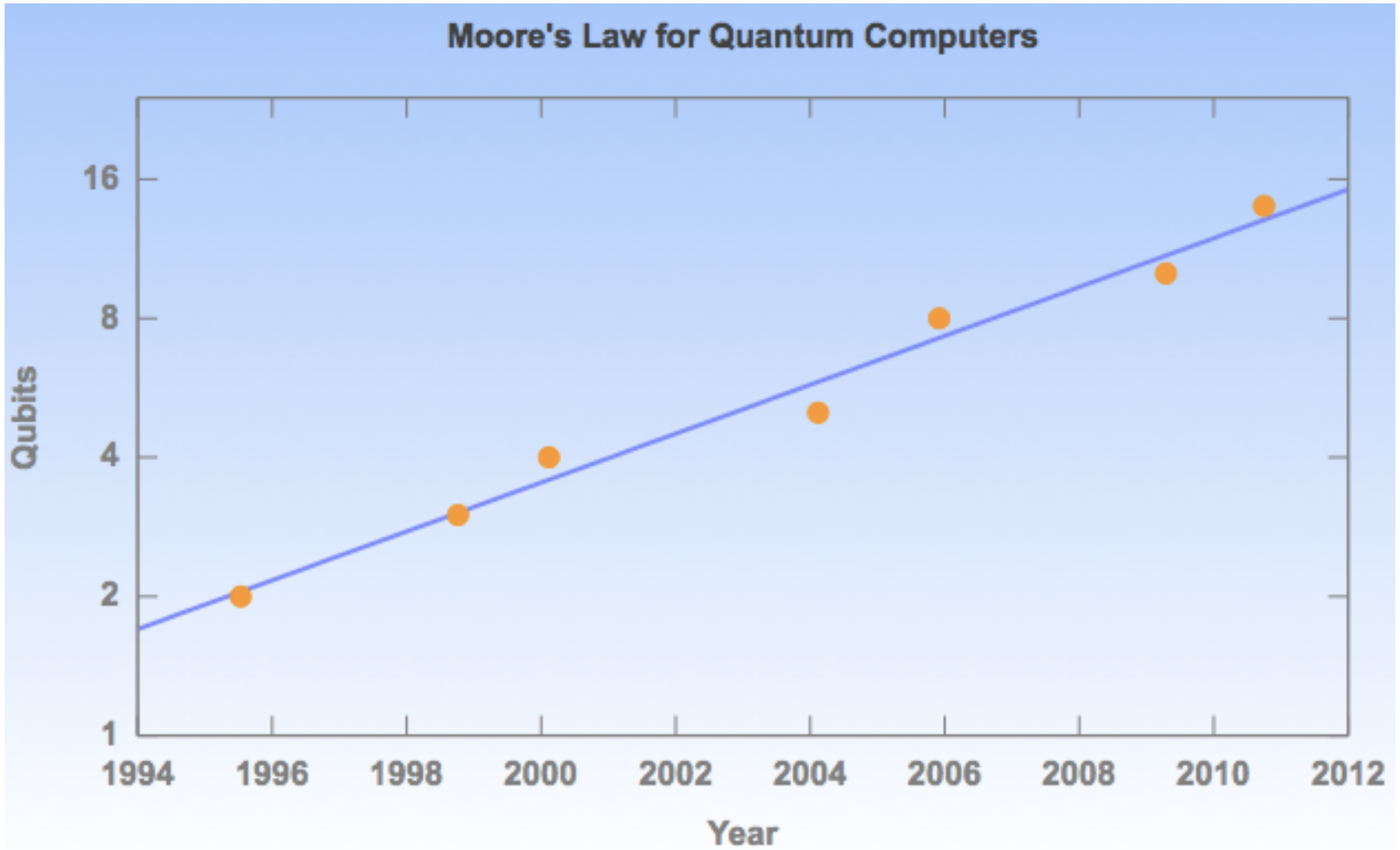
National Investments

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

Quantum Machines

Private Investments

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



Quantum Era

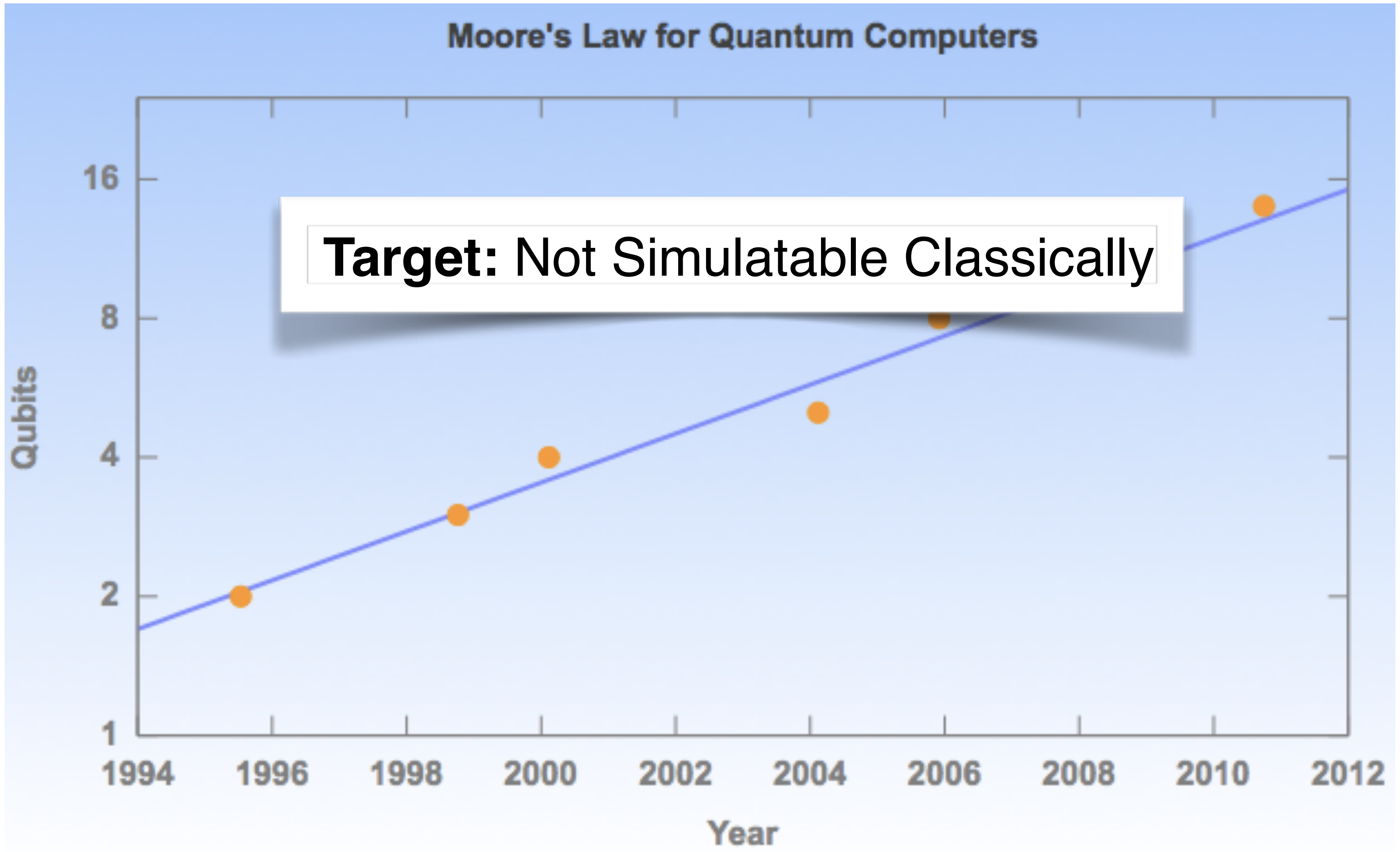
National Investments

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

Quantum Machines

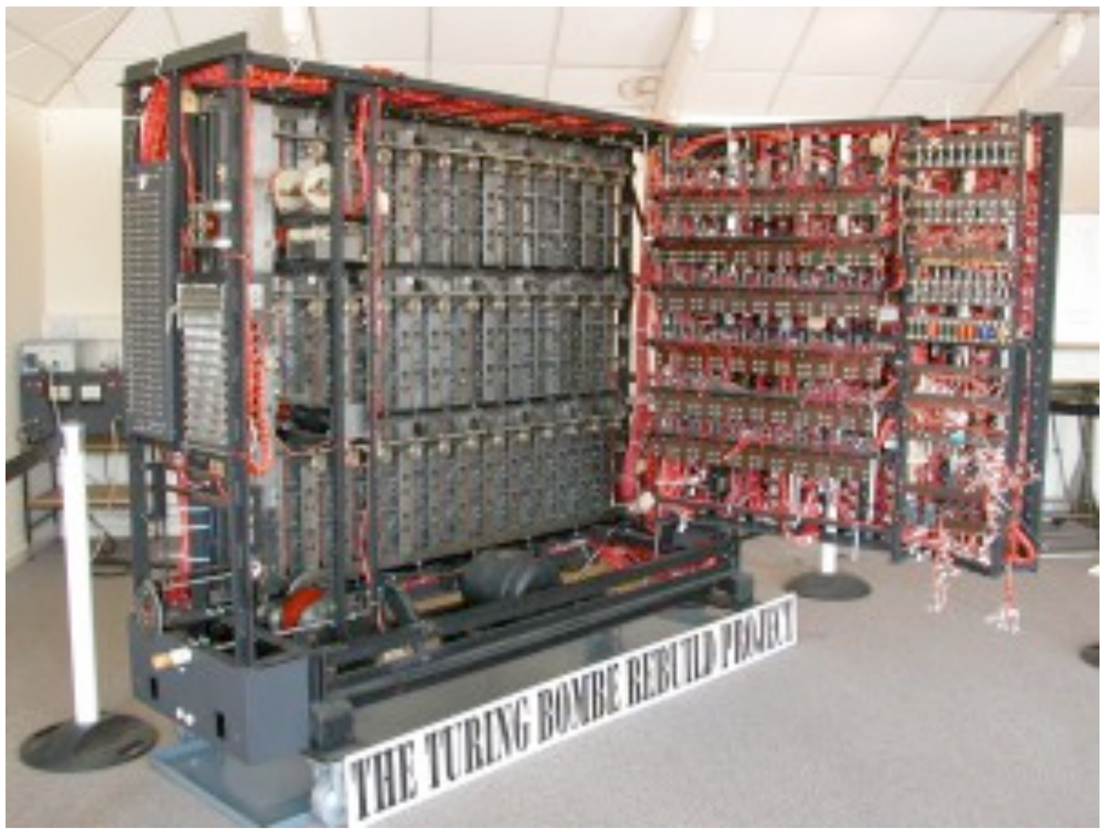
Private Investments

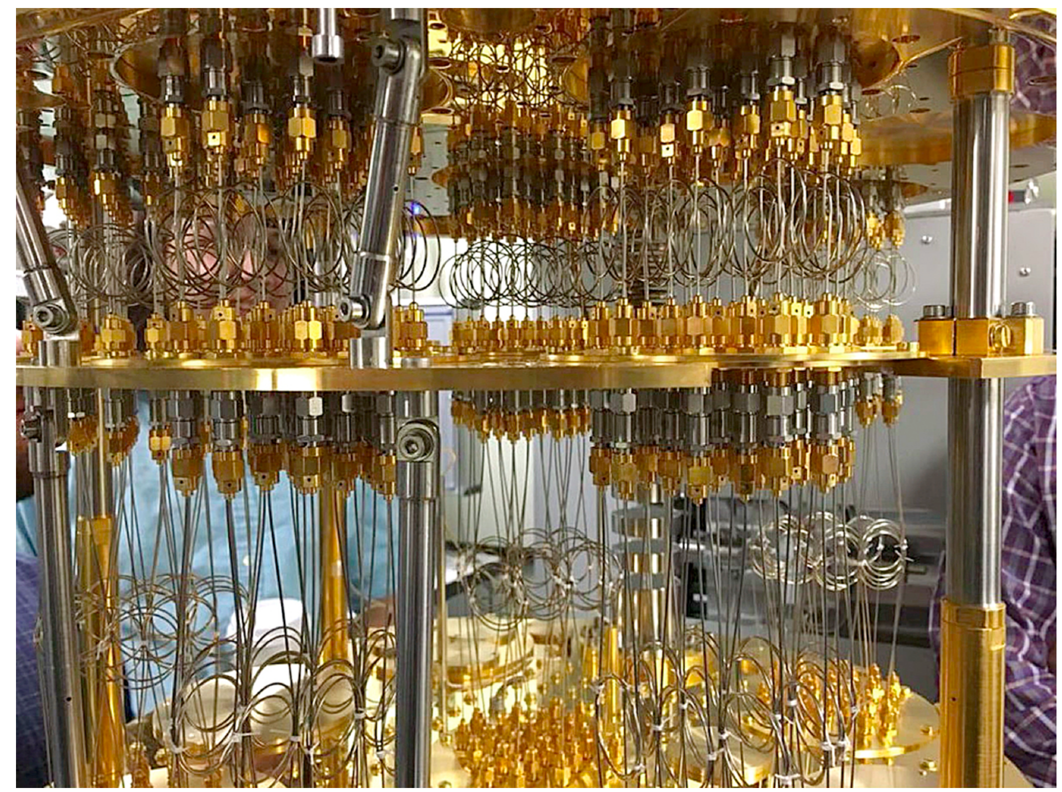
Google, IBM, Intel
Big VC founds
Startups Companies: D-Wave,IonQ, Rigetti



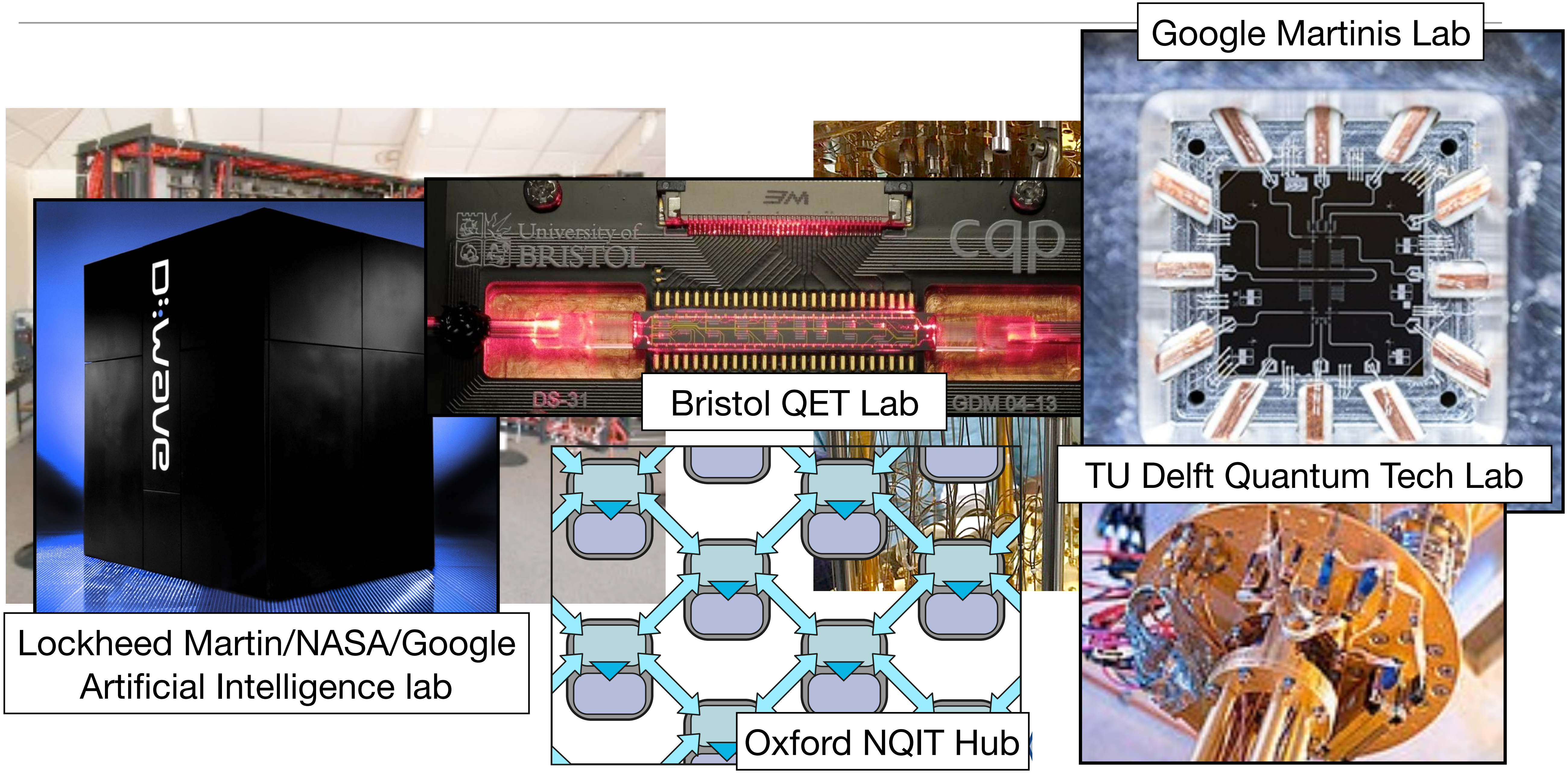
Target: Not Simulatable Classically

Turing Machine vs Quantum Machine

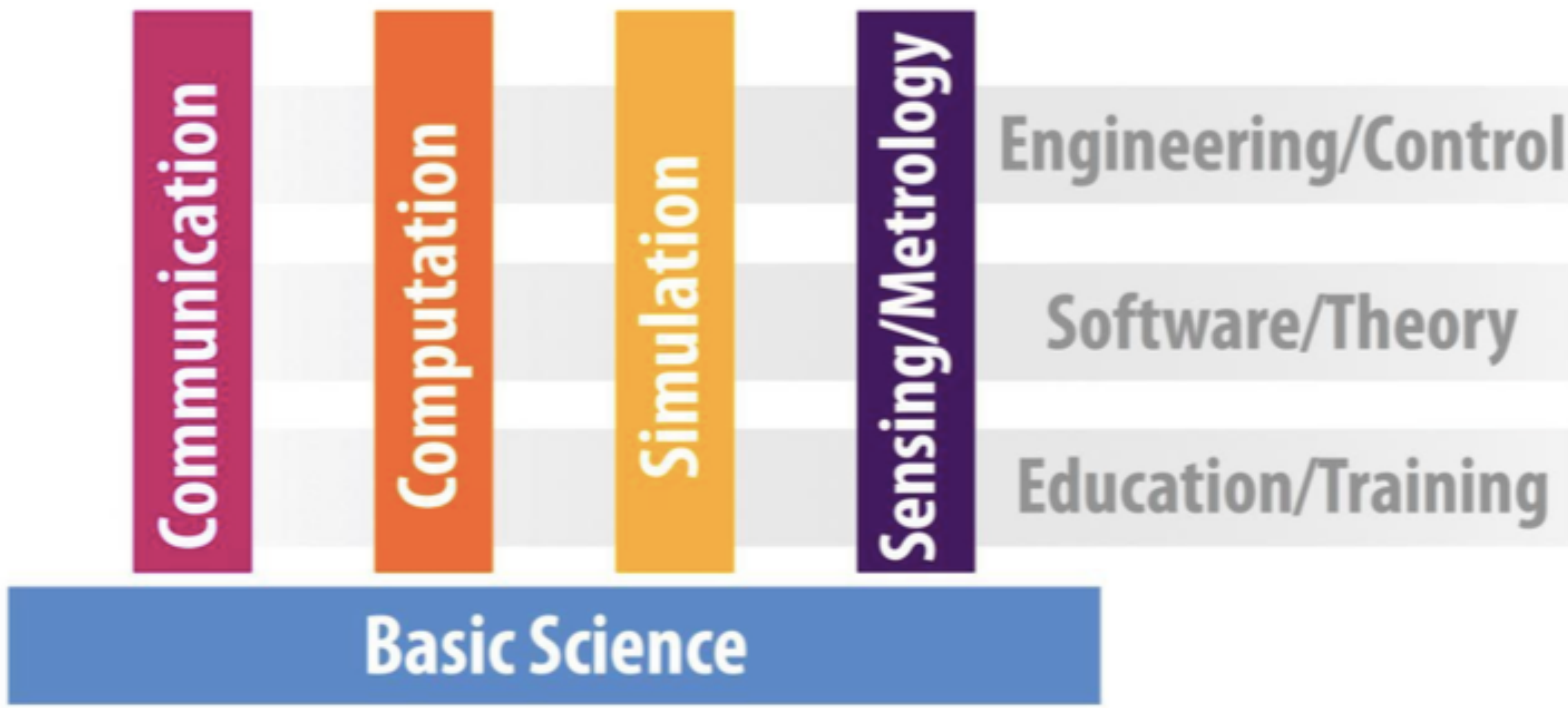




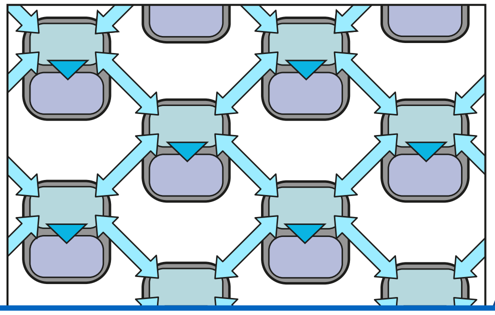
Turing Machine vs Quantum Machine



Quantum Flagship

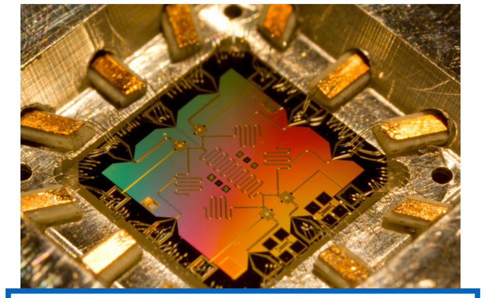


Vision of Quantum Technology



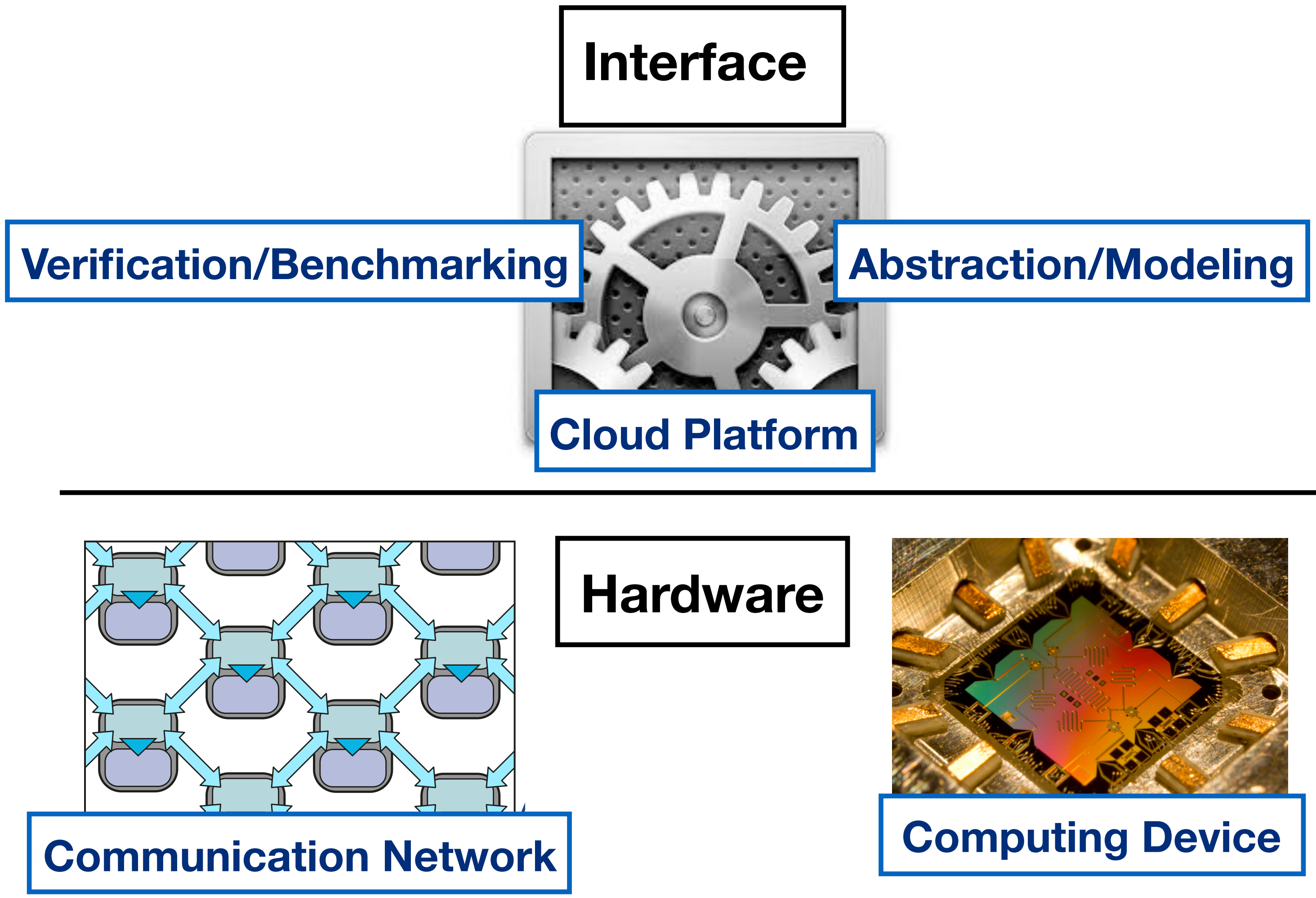
Communication Network

Hardware

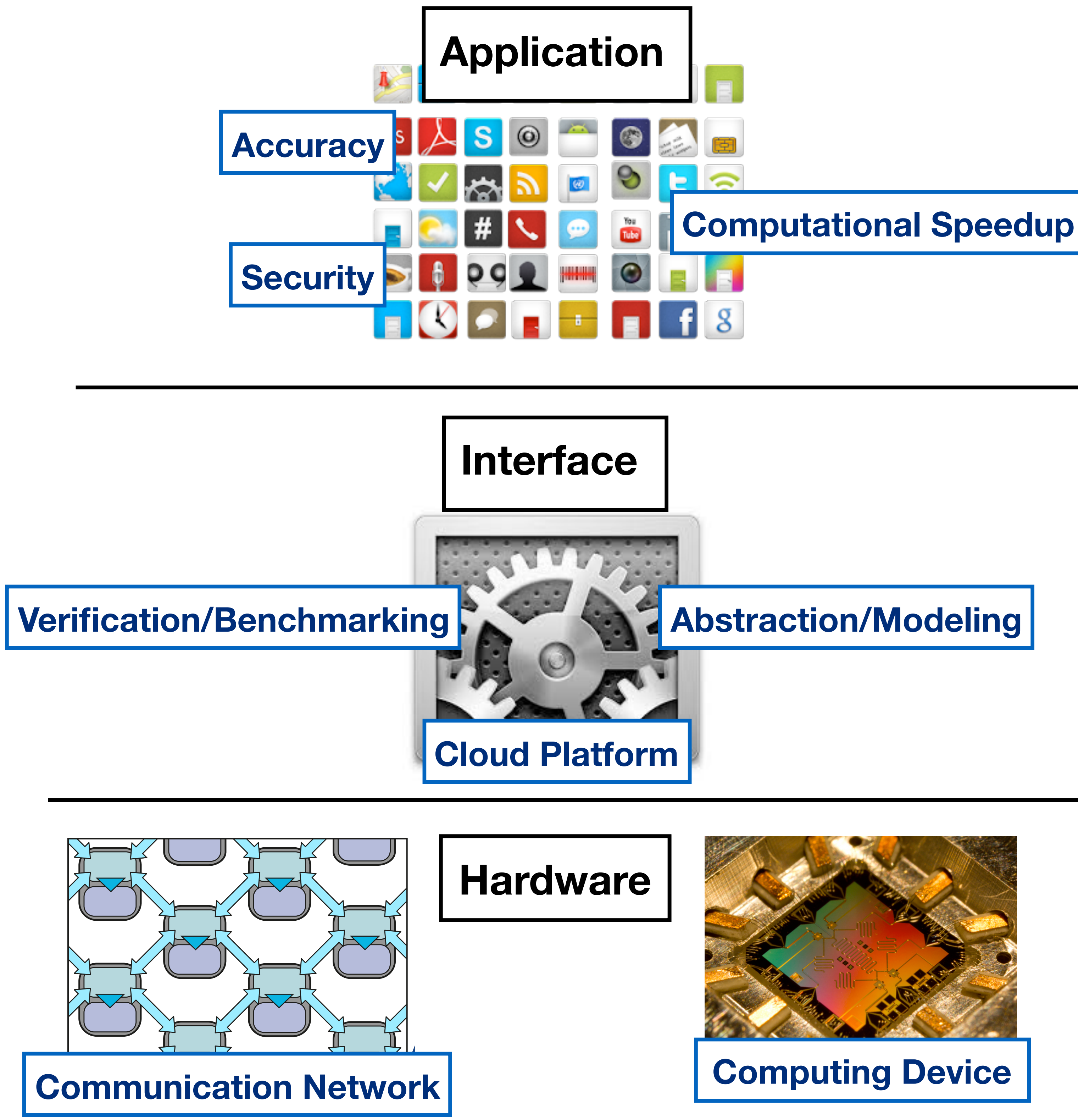


Computing Device

Vision of Quantum Technology



Vision of Quantum Technology



Quantum Internet

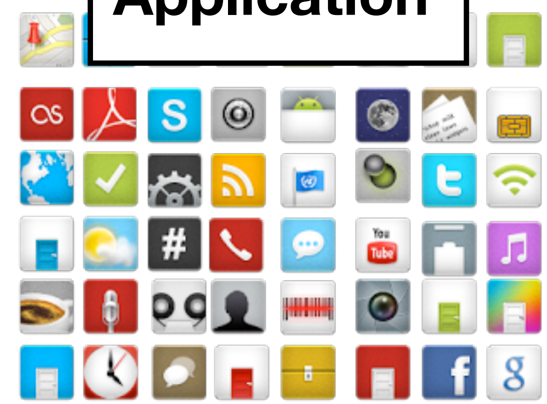
Quantum Internet

- Secure communication
- Clock synchronisation
- Combining distant telescopes
- Communication Complexity Advantage
- Secure access to Quantum Cloud
- Bootstrapping small Quantum Computer

Quantum Internet

- Secure communication
- Clock synchronisation
- Combining distant telescopes
- Communication Complexity Advantage
- Secure access to Quantum Cloud
- Bootstrapping small Quantum Computer

Application



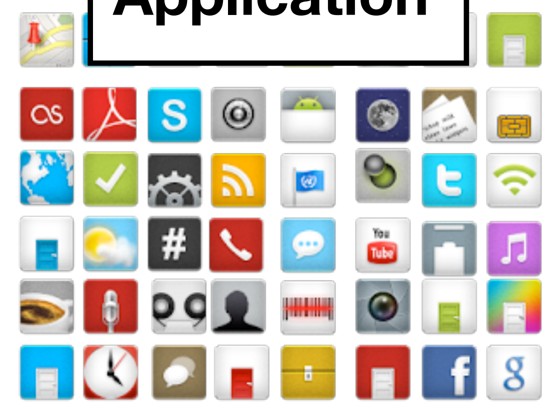
- Quantum Network Modules
- Network simulation and benchmarking
- Control Stack
- HAL Operating System
- Code optimization and compiling
- Bootstrapping small Quantum Computer

Interface

Quantum Internet

- Secure communication
- Clock synchronisation
- Combining distant telescopes
- Communication Complexity Advantage
- Secure access to Quantum Cloud
- Bootstrapping small Quantum Computer

Application

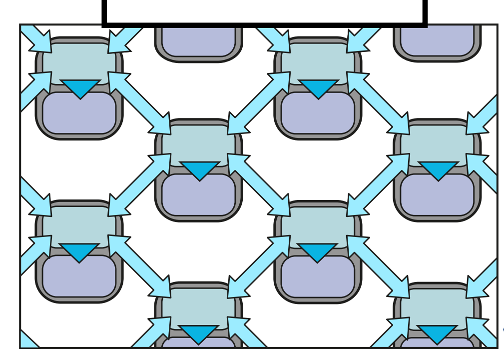


- Quantum Network Modules
- Network simulation and benchmarking
- Control Stack
- HAL Operating System
- Code optimization and compiling
- Bootstrapping small Quantum Computer

Interface

- Server and Client Nodes
- Hybrid Architecture
- Quantum Memory and Repeater
- Integration to long distance network

Hardware



Quantum Computing

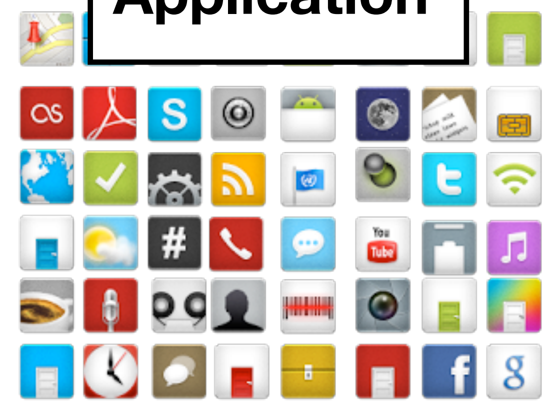
Quantum Computing

- Machine Learning
- Optimisation
- Quantum Chemistry

Quantum Computing

- Machine Learning
- Optimisation
- Quantum Chemistry

Application

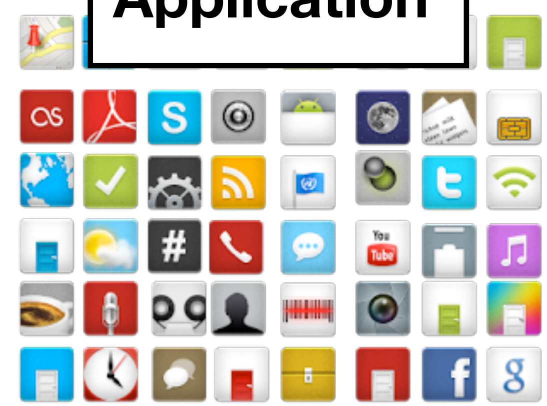


Interface

- Programming Language
- Verification
- HAL Operating System
- Code optimization and compiling
- Architecture Design

Quantum Computing

Application

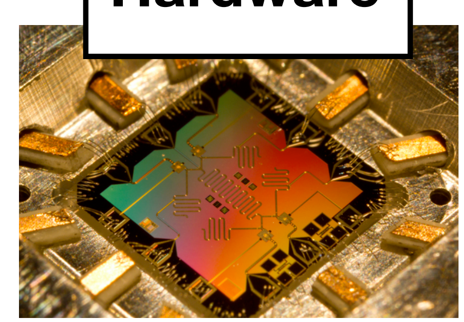


- Machine Learning
- Optimisation
- Quantum Chemistry

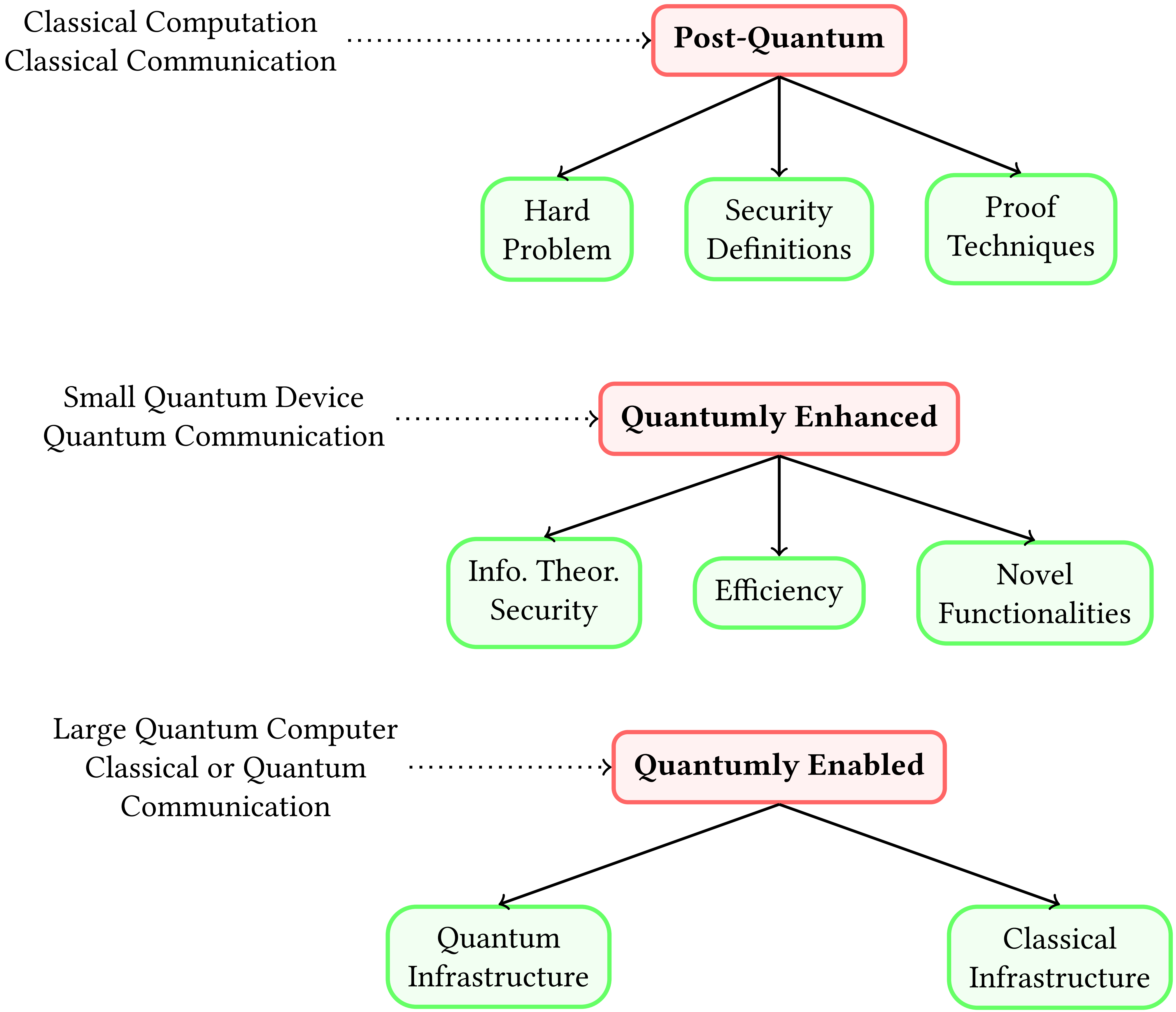
Interface

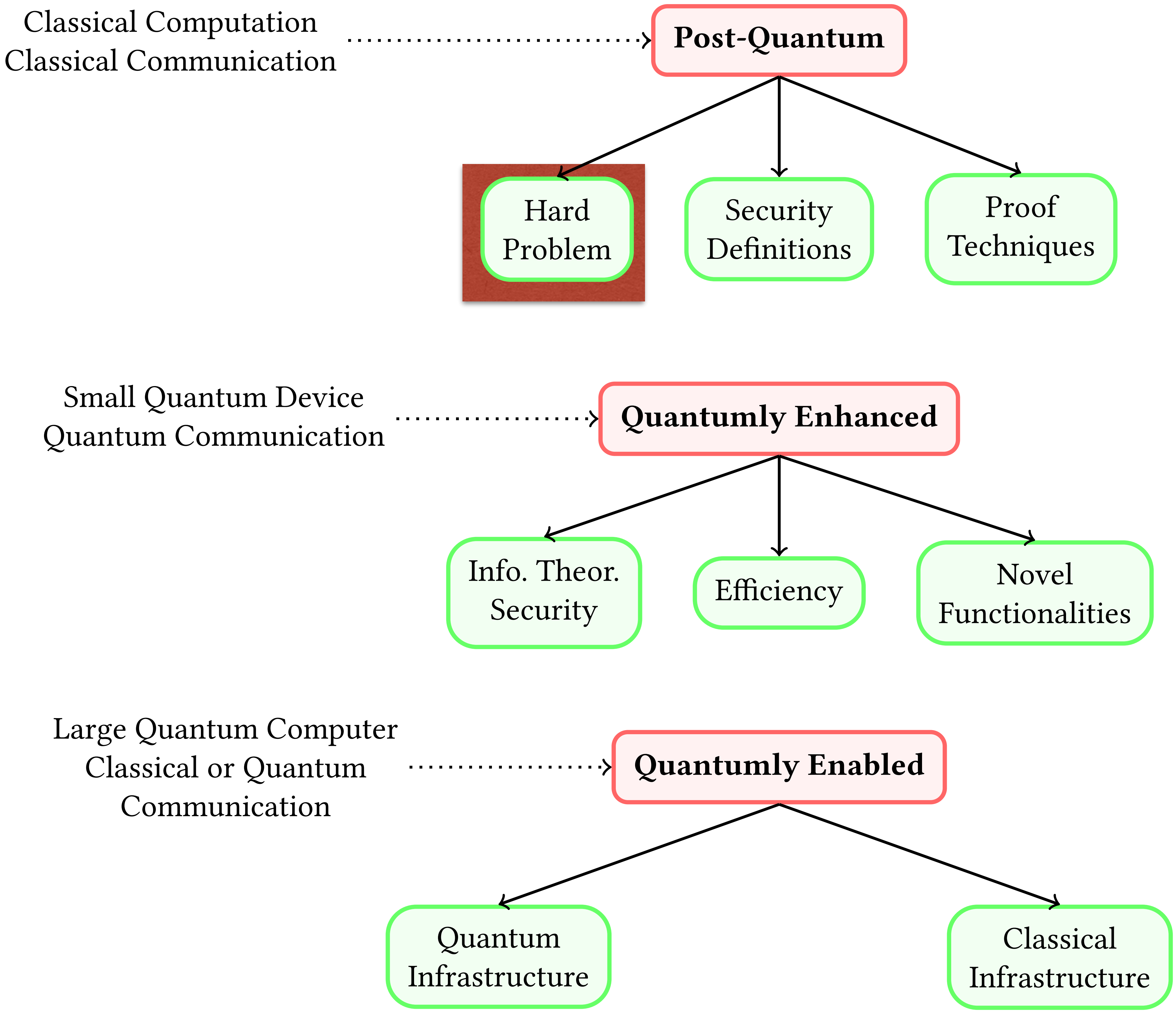
- Programming Language
- Verification
- HAL Operating System
- Code optimization and compiling
- Architecture Design

Hardware



- Server and Client Nodes
- Hybrid Architecture
- Fault Tolerance
- Scaling


Classical Computation
Classical Communication
Post-Quantum
Hard Problem
Security Definitions
Proof Techniques
Small Quantum Device
Quantum Communication
Quantumly Enhanced
Info. Theor. Security
Efficiency
Novel Functionalities
Large Quantum Computer
Classical or Quantum Communication
Quantumly Enabled
Quantum Infrastructure
Classical Infrastructure


Classical Computation
Classical Communication
Post-Quantum
Hard Problem
Security Definitions
Proof Techniques
Small Quantum Device
Quantum Communication
Quantumly Enhanced
Info. Theor. Security
Efficiency
Novel Functionalities
Large Quantum Computer
Classical or Quantum Communication
Quantumly Enabled
Quantum Infrastructure
Classical Infrastructure

Post-Quantum

classical security against adversaries that exploit quantum effects

Post-Quantum

classical security against adversaries that exploit quantum effects

Quantum algorithms breaking computational assumptions

Factoring and Discrete Logarithm [Shor 94] Principal ideal problem [Hallgren 02]

Quantum effects breaking Information-theoretical assumptions

commitment scheme becomes non-binding [Crepeau,Salvail,Simard,Tapp 06]

Classical proof techniques no longer apply

rewinding

Post-Quantum

Post-Quantum

Learning with Error (LWE)

as hard as worst-case lattice problems, believed to be exponentially hard against QC

Post-Quantum

Learning with Error (LWE)

as hard as worst-case lattice problems, believed to be exponentially hard against QC

↓

LWE-based Crypto Systems (FHE and etc)

Post-Quantum

Learning with Error (LWE)

as hard as worst-case lattice problems, believed to be exponentially hard against QC

↓

LWE-based Crypto Systems (FHE and etc)

↓

(classical) **mixed commitment schemes** (secure against quantum)

lifting classical security proof to the quantum setting, **coin flipping protocols**

Post-Quantum

Learning with Error (LWE)

as hard as worst-case lattice problems, believed to be exponentially hard against QC

↓

LWE-based Crypto Systems (FHE and etc)

↓

(classical) **mixed commitment schemes** (secure against quantum)

lifting classical security proof to the quantum setting, **coin flipping protocols**

(classical) **Zero-Knowledge Proof-of-Knowledge** (secure against quantum)

lifting classical security proof to the quantum setting, **secure function evaluation**

Algebraic Problems

Andrew M. Childs and Wim van Dam, 2008

The hidden subgroup problem

Let G be a finite Abelian group with group operations written additively

consider a function $f : G \to S$, where S is some finite set. We say that f *hides* the subgroup H

$f(x) = f(y)$ if and only if $x - y \in H$

find a generating set for H given the ability to query the function f

The hidden subgroup problem

Problem
Factorisation
Discrete log
Elliptic curve discrete log
Principal ideal
Shortest lattice vector
Graph isomorphism

The hidden subgroup problem

Problem	*Group*
Factorisation	$\mathbb{Z}$
Discrete log	$\mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1}$
Elliptic curve discrete log	Elliptic curve
Principal ideal	$\mathbb{R}$
Shortest lattice vector	Dihedral group
Graph isomorphism	Symmetric group

The hidden subgroup problem

Problem	*Group*	*Cryptosystem*
Factorisation	$\mathbb{Z}$	RSA
Discrete log	$\mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1}$	Diffie-Hellman, DSA,...
Elliptic curve discrete log	Elliptic curve	ECDH, ECDSA,...
Principal ideal	$\mathbb{R}$	Buchmann-Williams
Shortest lattice vector	Dihedral group	NTRU, Ajtai-Dwork,...
Graph isomorphism	Symmetric group	—

The hidden subgroup problem

Problem	*Complexity*	*Cryptosystem*
Factorisation	Polynomial[11]	RSA
Discrete log	Polynomial[11]	Diffie-Hellman, DSA,…
Elliptic curve discrete log	Polynomial[92]	ECDH, ECDSA,…
Principal ideal	Polynomial[93]	Buchmann-Williams
Shortest lattice vector	Subexponential[94,95]	NTRU, Ajtai-Dwork,…
Graph isomorphism	Exponential	—

The hidden subgroup problem

Problem	*Complexity*	*Cryptosystem*
Factorisation	Polynomial[11]	RSA
Discrete log	Polynomial[11]	Diffie-Hellman, DSA,..
Elliptic curve discrete log	Polynomial[92]	ECDH, ECDSA,...
Principal ideal	Polynomial[93]	Buchmann-Williams
Shortest lattice vector	Subexponential[94,95]	NTRU, Ajtai-Dwork,...
Graph isomorphism	Exponential	—

Quantum algorithms: an overview

Ashley Montanaro

The hidden subgroup problem

Algebraic Problems
Andrew M. Childs and Wim van Dam, 2008

The hidden subgroup problem

Algebraic Problems
Andrew M. Childs and Wim van Dam, 2008

Fourier transforms over finite Abelian groups

The hidden subgroup problem

Algebraic Problems

Andrew M. Childs and Wim van Dam, 2008

Fourier transforms over finite Abelian groups

$$|x\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{y \in \mathbb{Z}/N\mathbb{Z}} \omega_N^{xy} |y\rangle,$$

$$\omega_N := e^{2\pi i/N}$$

The hidden subgroup problem

Algebraic Problems

Andrew M. Childs and Wim van Dam, 2008

Fourier transforms over finite Abelian groups

$$|x\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{y \in \mathbb{Z}/N\mathbb{Z}} \omega_N^{xy} |y\rangle,$$

$$|x\rangle \mapsto \frac{1}{\sqrt{|G|}} \sum_{\psi \in \hat{G}} \psi(x) |\psi\rangle$$

$$\omega_N := e^{2\pi i/N}$$

The hidden subgroup problem

Algebraic Problems

Andrew M. Childs and Wim van Dam, 2008

Fourier transforms over finite Abelian groups

$$|x\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{y\in\mathbb{Z}/N\mathbb{Z}} \omega_N^{xy}|y\rangle,$$

$$|x\rangle \mapsto \frac{1}{\sqrt{|G|}} \sum_{\psi\in\hat{G}} \psi(x)|\psi\rangle$$

$$\omega_N := e^{2\pi i/N}$$

one-dimensional irreducible representations

$$\psi : G \to \mathbb{C} \quad \psi(a+b) = \psi(a)\psi(b)$$

The hidden subgroup problem

Algebraic Problems

Andrew M. Childs and Wim van Dam, 2008

Fourier transforms over finite Abelian groups

$$|x\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{y \in \mathbb{Z}/N\mathbb{Z}} \omega_N^{xy} |y\rangle,$$

$$|x\rangle \mapsto \frac{1}{\sqrt{|G|}} \sum_{\psi \in \hat{G}} \psi(x) |\psi\rangle$$

$$\omega_N := e^{2\pi i/N}$$

one-dimensional irreducible representations

$\psi : G \to \mathbb{C} \quad \psi(a+b) = \psi(a)\psi(b)$

Efficient quantum circuit for the QFT

The hidden subgroup problem

Algebraic Problems

Andrew M. Childs and Wim van Dam, 2008

Fourier transforms over finite Abelian groups

$$|x\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{y \in \mathbb{Z}/N\mathbb{Z}} \omega_N^{xy} |y\rangle,$$

$$|x\rangle \mapsto \frac{1}{\sqrt{|G|}} \sum_{\psi \in \hat{G}} \psi(x) |\psi\rangle$$

$$\omega_N := e^{2\pi i/N}$$

one-dimensional irreducible representations

$$\psi : G \to \mathbb{C} \quad \psi(a+b) = \psi(a)\psi(b)$$

Efficient quantum circuit for the QFT

$$F_{\mathbb{Z}/N\mathbb{Z}} = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega_N & \omega_N^2 & \cdots & \omega_N^{N-1} \\ 1 & \omega_N^2 & \omega_N^4 & \cdots & \omega_N^{2N-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega_N^{N-1} & \omega_N^{2N-2} & \cdots & \omega_N^{(N-1)(N-1)} \end{pmatrix}$$

The hidden subgroup problem

Algebraic Problems
Andrew M. Childs and Wim van Dam, 2008

Fourier transforms over finite Abelian groups

$$|x\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{y \in \mathbb{Z}/N\mathbb{Z}} \omega_N^{xy} |y\rangle,$$

$$|x\rangle \mapsto \frac{1}{\sqrt{|G|}} \sum_{\psi \in \hat{G}} \psi(x) |\psi\rangle$$

$$\omega_N := \mathrm{e}^{2\pi \mathrm{i}/N}$$

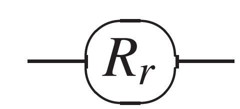
one-dimensional irreducible representations

$$\psi : G \to \mathbb{C} \quad \psi(a+b) = \psi(a)\psi(b)$$

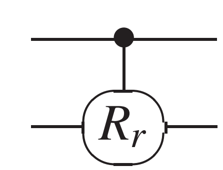
Efficient quantum circuit for the QFT

$$F_{\mathbb{Z}/N\mathbb{Z}} = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega_N & \omega_N^2 & \cdots & \omega_N^{N-1} \\ 1 & \omega_N^2 & \omega_N^4 & \cdots & \omega_N^{2N-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega_N^{N-1} & \omega_N^{2N-2} & \cdots & \omega_N^{(N-1)(N-1)} \end{pmatrix}$$

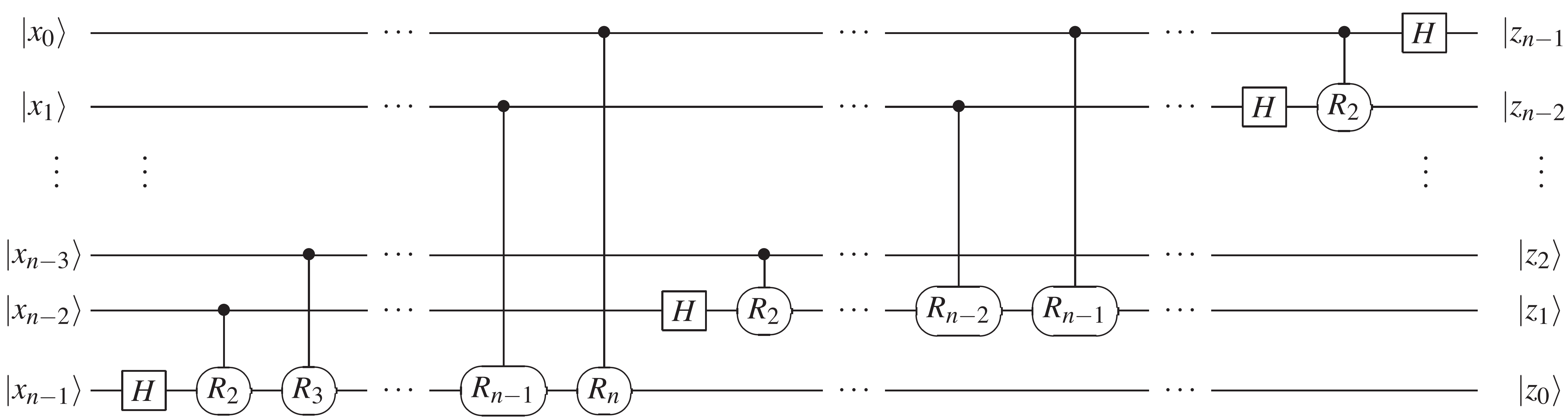
$$R_r := \begin{pmatrix} 1 & 0 \\ 0 & \mathrm{e}^{2\pi \mathrm{i}/2^r} \end{pmatrix} \simeq$$



$$\Lambda(R_r) := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \mathrm{e}^{2\pi \mathrm{i}/2^r} \end{pmatrix} \simeq$$



QFT



An efficient (size $O(n^2)$) quantum circuit for the quantum Fourier transform over $Z/2^nZ$

Period Finding Over Z/NZ

$$\boxed{f : \mathrm{Z}/N\mathrm{Z} \rightarrow S \ \text{ with period } r}$$

$$f(x) = f(y) \text{ if and only if } \frac{x-y}{r} \in \mathbb{Z}$$

Period Finding Over Z/NZ

$f: \mathrm{Z}/N\mathrm{Z} \rightarrow S$ with period r

$$f(x) = f(y) \text{ if and only if } \frac{x-y}{r} \in \mathbb{Z}$$

We can find the period r efficiently using the HSP over the additive group Z/NZ.

Period Finding Over Z/NZ

$f : \mathrm{Z}/N\mathrm{Z} \rightarrow S$ with period r

$$f(x) = f(y) \text{ if and only if } \frac{x-y}{r} \in \mathbb{Z}$$

We can find the period r efficiently using the HSP over the additive group $\mathrm{Z}/N\mathrm{Z}$.

Represent $x \in \mathrm{Z}/N\mathrm{Z}$ uniquely as an integer $x \in \{0, \ldots, N-1\}$

The irreducible representations $\psi : \mathrm{Z}/N\mathrm{Z} \rightarrow \mathrm{C}$ can be labeled by integers $y \in \{0,\ldots,N-1\}$

Period Finding Over Z/NZ - Algorithm

1. Apply the Fourier transform over Z/NZ to the state $|0\rangle$

$$|\mathbb{Z}/N\mathbb{Z}\rangle = \frac{1}{\sqrt{N}} \sum_{x \in \mathbb{Z}/N\mathbb{Z}} |x\rangle$$

Period Finding Over Z/NZ - Algorithm

1. Apply the Fourier transform over Z/NZ to the state $|0\rangle$

$$|\mathbb{Z}/N\mathbb{Z}\rangle = \frac{1}{\sqrt{N}} \sum_{x \in \mathbb{Z}/N\mathbb{Z}} |x\rangle$$

2. Query the function f in an ancilla register

$$\frac{1}{\sqrt{N}} \sum_{x \in \mathbb{Z}/N\mathbb{Z}} |x, f(x)\rangle$$

Period Finding Over Z/NZ - Algorithm

3. Measure the ancilla register.

The first register will be in a superposition of those x consistent with the observed function value.

Period Finding Over Z/*N*Z - Algorithm

3. Measure the ancilla register.

The first register will be in a superposition of those x consistent with the observed function value.

$$\sqrt{\frac{r}{N}}\sum_{j=0}^{\frac{N}{r}-1}|s+jr\rangle$$

Period Finding Over Z/NZ - Algorithm

3. Measure the ancilla register.

The first register will be in a superposition of those x consistent with the observed function value.

$$\sqrt{\frac{r}{N}}\sum_{j=0}^{\frac{N}{r}-1}|s+jr\rangle$$

for unknown offset $s \in \{0,\ldots,r-1\}$ *corresponding to the uniformly random observed function value* $f(s)$

Period Finding Over Z/NZ - Algorithm

4. Apply the Fourier transform over $\mathbb{Z}/N\mathbb{Z}$

Period Finding Over Z/NZ - Algorithm

4. Apply the Fourier transform over Z/*N*Z

$$\sqrt{\frac{r}{N}} \sum_{y \in \mathbb{Z}/N\mathbb{Z}} \sum_{j=0}^{\frac{N}{r}-1} \omega_N^{(s+jr)y} |y\rangle.$$

Period Finding Over Z/NZ - Algorithm

4. Apply the Fourier transform over Z/NZ

$$\sqrt{\frac{r}{N}} \sum_{y \in \mathbb{Z}/N\mathbb{Z}} \sum_{j=0}^{\frac{N}{r}-1} \omega_N^{(s+jr)y} |y\rangle .$$

Let $M = N/r$ *so* $\omega_N^{jry} = \omega_M^{jy}$ *hence* $\sum_{j=0}^{M-1} \omega_M^{jy} = M \delta_{j,y \bmod M}$

Period Finding Over Z/NZ - Algorithm

4. Apply the Fourier transform over Z/NZ

$$\sqrt{\frac{r}{N}} \sum_{y \in \mathbb{Z}/N\mathbb{Z}} \sum_{j=0}^{\frac{N}{r}-1} \omega_N^{(s+jr)y} |y\rangle .$$

Let $M = N/r$ *so* $\omega_N^{jry} = \omega_M^{jy}$ *hence* $\sum_{j=0}^{M-1} \omega_M^{jy} = M\,\delta_{j,y \bmod M}$

only the values $y \in \{0, N/r, 2N/r, \ldots, (r-1)N/r\}$ *experience constructive interference*

Period Finding Over Z/NZ - Algorithm

4. Apply the Fourier transform over Z/NZ

$$\sqrt{\frac{r}{N}} \sum_{y \in \mathbb{Z}/N\mathbb{Z}} \sum_{j=0}^{\frac{N}{r}-1} \omega_N^{(s+jr)y} |y\rangle .$$

Let $M = N/r$ *so* $\omega_N^{jry} = \omega_M^{jy}$ *hence* $\sum_{j=0}^{M-1} \omega_M^{jy} = M\,\delta_{j,y \bmod M}$

only the values $y \in \{0, N/r, 2N/r, \ldots, (r-1)N/r\}$ *experience constructive interference*

$$\frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \omega_r^{sk} |kN/r\rangle$$

Period Finding Over Z/NZ - Algorithm

5. Measure the state in the computational basis.

giving kN/r and hence the fraction k/r

which, when reduced to lowest terms, has r/gcd(r,k) as its denominator.

Period Finding Over Z/NZ - Algorithm

5. Measure the state in the computational basis.

giving kN/r and hence the fraction k/r

which, when reduced to lowest terms, has r/gcd(r,k) as its denominator.

6. Repeat the procedure to get a second denominator $r/\gcd(r,k')$.

If k and k' *are relatively prime, the least common multiple of* $r/\gcd(r,k)$ *and* $r/\gcd(r,k')$ *is r.*

Period Finding Over Z/NZ - Algorithm

5. Measure the state in the computational basis.

giving kN/r and hence the fraction k/r

which, when reduced to lowest terms, has r/gcd(r,k) as its denominator.

6. Repeat the procedure to get a second denominator $r/gcd(r,k')$.

If k and k' *are relatively prime, the least common multiple of* $r/\gcd(r,k)$ *and* $r/\gcd(r,k')$ *is r.*

$$\prod_{p\ prime}\left(1-\frac{1}{p^2}\right)=6/\pi^2\approx 0.61$$

Search and Optimisation

Search and Optimisation

Unstructured search problem:

Given oracle $f:\{0, 1\}^n \rightarrow \{0, 1\}$, find x such that $f(x) = 1$

Search and Optimisation

Unstructured search problem:

Given oracle $f:\{0, 1\}^n \rightarrow \{0, 1\}$, find x such that $f(x) = 1$

Grover $O(\sqrt{N})$ evaluations of f in the worst case

Search and Optimisation

Quantum algorithms: an overview

Ashley Montanaro

Unstructured search problem:

Given oracle $f:\{0, 1\}^n \to \{0, 1\}$, find x such that $f(x) = 1$

Grover $O(\sqrt{N})$ evaluations of f in the worst case

Heuristic search problem

Given a probabilistic guessing algorithm A,

a checking function f, such that

$$\Pr[\mathcal{A} \text{ outputs } w \text{ such that } f(w) = 1] = \varepsilon$$

output w such that $f(w) = 1$

Search and Optimisation

Quantum algorithms: an overview

Ashley Montanaro

Unstructured search problem:

Given oracle $f:\{0, 1\}^n \rightarrow \{0, 1\}$, find x such that $f(x) = 1$

Grover $O(\sqrt{N})$ evaluations of f in the worst case

Heuristic search problem

Given a probabilistic guessing algorithm A,

a checking function f, such that

$$\Pr[\mathcal{A} \text{ outputs } w \text{ such that } f(w) = 1] = \varepsilon$$

output w such that f(w) = 1

Amplitude Amplification $O(1/\sqrt{\varepsilon})$ evaluations of f in the worst case

Grover as a subroutine

Finding the minimum of an unsorted list of N integers

Grover as a subroutine

Finding the minimum of an unsorted list of N integers

Apply Grover to

$g:\{0,\ 1\}^n \to \{0,\ 1\}$ defined by $g(x) = 1$, if and only if $f(x) < T$

for random threshold T that will be updated as inputs x are found such that f(x) is below the threshold

Grover as a subroutine

Finding the minimum of an unsorted list of N integers

Apply Grover to

$$g:\{0,\ 1\}^n \rightarrow \{0,\ 1\} \text{ defined by } g(x)=1, \text{ if and only if } f(x) < T$$

for random threshold T that will be updated as inputs x are found such that f(x) is below the threshold

Solving systems of boolean multivariate quadratic equations

Grover as a subroutine

Finding the minimum of an unsorted list of N integers

Apply Grover to

$g:\{0, 1\}^n \to \{0, 1\}$ defined by $g(x) = 1$, if and only if $f(x) < T$

for random threshold T that will be updated as inputs x are found such that f(x) is below the threshold

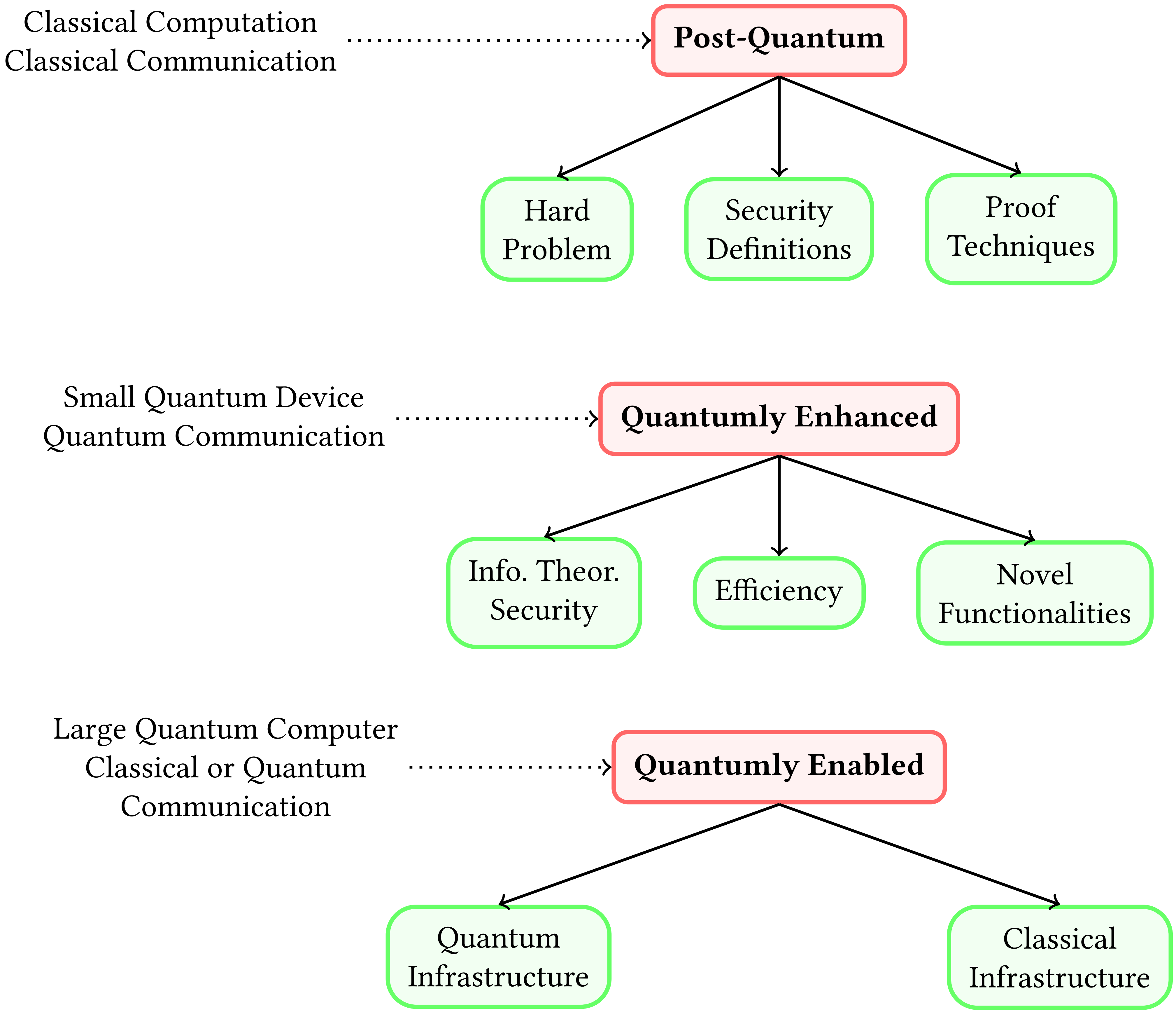
Solving systems of boolean multivariate quadratic equations

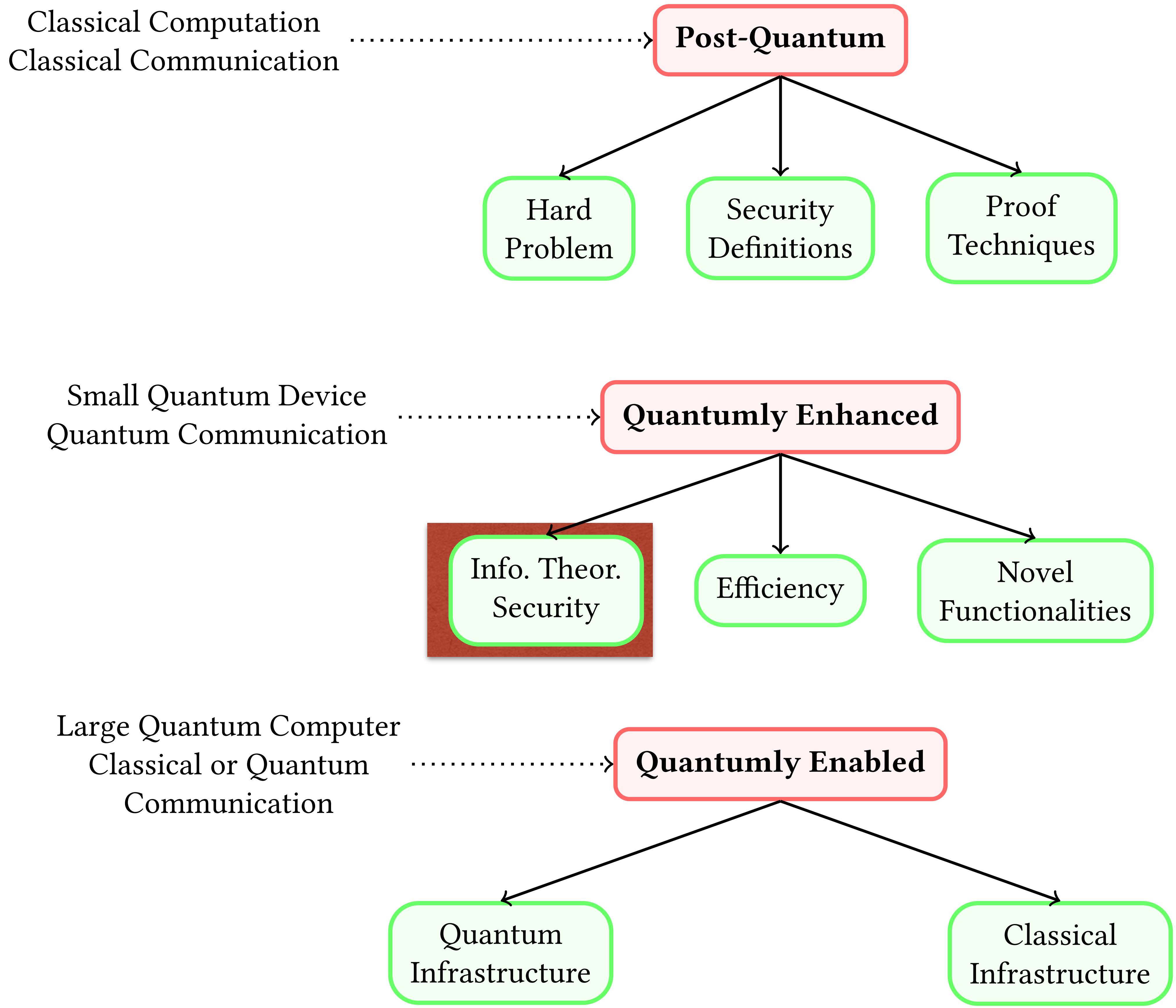
Input. $f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n) \in \mathbb{F}_2[x_1, \ldots, x_n]$.
Goal. Find – if any – a vector $(z_1, \ldots, z_n) \in \mathbb{F}_2^n$ such that:

$$f_1(z_1, \ldots, z_n) = 0, \ldots, f_m(z_1, \ldots, z_n) = 0.$$

combine Grover's technique with a Grobner basis-based algorithm

$$O(2^{0.47n})$$


Classical Computation
Classical Communication
Post-Quantum
Hard Problem
Security Definitions
Proof Techniques
Small Quantum Device
Quantum Communication
Quantumly Enhanced
Info. Theor. Security
Efficiency
Novel Functionalities
Large Quantum Computer
Classical or Quantum Communication
Quantumly Enabled
Quantum Infrastructure
Classical Infrastructure


Classical Computation
Classical Communication
Post-Quantum
Hard Problem
Security Definitions
Proof Techniques
Small Quantum Device
Quantum Communication
Quantumly Enhanced
Info. Theor. Security
Efficiency
Novel Functionalities
Large Quantum Computer
Classical or Quantum Communication
Quantumly Enabled
Quantum Infrastructure
Classical Infrastructure

Quantumly-Enhanced

Quantumly-Enhanced

qubits transmissions and classical post-processing

↓

unconditional security based on physical laws

Quantumly-Enhanced

qubits transmissions and classical post-processing

↓

unconditional security based on physical laws

Information gain vs. disturbance No Cloning Spooky actions at a distance

History

1970 - **quantum money** (Wiesner)

The first link between secrecy and quantum physics

The bill contains photons that bank "polarised" in random directions

History

1970 - **quantum money** (Wiesner)
The first link between secrecy and quantum physics
The bill contains photons that bank "polarised" in random directions

1984 - **quantum key distribution** (Bennett and Brassard; Ekert)
Become the most promising task of quantum cryptography

History

1970 - **quantum money** (Wiesner)
The first link between secrecy and quantum physics
The bill contains photons that bank "polarised" in random directions

1984 - **quantum key distribution** (Bennett and Brassard; Ekert)
Become the most promising task of quantum cryptography

1999 - **quantum secret sharing** (Hillery, Buzek and Berthiaume; Cleve, Gottesman and Lo)
To distribute secret such that only the authorised partners could recover it

History

1970 - **quantum money** (Wiesner)
The first link between secrecy and quantum physics
The bill contains photons that bank “polarised” in random directions

1984 - **quantum key distribution** (Bennett and Brassard; Ekert)
Become the most promising task of quantum cryptography

1999 - **quantum secret sharing** (Hillery, Buzek and Berthiaume; Cleve, Gottesman and Lo)
To distribute secret such that only the authorised partners could recover it

1997 - **bit commitment and oblivious transfer** (Lo and Chau, Mayers)
contrary to the case of QKD and secret sharing
quantum physics cannot guarantee unconditional security

History

2007 - **bounded-storage models** (Damgaard et al; Wehner, Schaffner, Terhal)

unconditionally secure OT and BC is possible

where honest parties need no quantum memory, whereas an adversarial must store

at least n/2 qubits to break the protocol, where n is the number of qubits

History

2007 - **bounded-storage models** (Damgaard et al; Wehner, Schaffner, Terhal)
unconditionally secure OT and BC is possible
where honest parties need no quantum memory, whereas an adversarial must store
at least n/2 qubits to break the protocol, where n is the number of qubits

2001- **quantum digital signature** (Gottesman and Chuang)
Similar to the classical case, based on one-way quantum function

History

2007 - **bounded-storage models** (Damgaard et al; Wehner, Schaffner, Terhal)
unconditionally secure OT and BC is possible
where honest parties need no quantum memory, whereas an adversarial must store
at least n/2 qubits to break the protocol, where n is the number of qubits

2001- **quantum digital signature** (Gottesman and Chuang)
Similar to the classical case, based on one-way quantum function

2009 - **2-party coin flipping** (Chailloux and Kerenidis)
Perfect quantum CF is impossible, but better than classical protocols exist
with best possible bias 0.21 (Kitaev 03)

History

2007 - **bounded-storage models** (Damgaard et al; Wehner, Schaffner, Terhal)
unconditionally secure OT and BC is possible
where honest parties need no quantum memory, whereas an adversarial must store
at least n/2 qubits to break the protocol, where n is the number of qubits

2001- **quantum digital signature** (Gottesman and Chuang)
Similar to the classical case, based on one-way quantum function

2009 - **2-party coin flipping** (Chailloux and Kerenidis)
Perfect quantum CF is impossible, but better than classical protocols exist
with best possible bias 0.21 (Kitaev 03)

2009 - **blind quantum computing** (Broadbent, Fitzsimons and Kashefi)
Unconditionally secure quantum delegated cmputing
with implementation (Barz, et.al. 2012)

QKD

Unconditionally secure authentication of the classical channel
requires Alice and Bob to pre-share an initial secret key
or at least partially secret but identical random strings

QKD

Unconditionally secure authentication of the classical channel
requires Alice and Bob to pre-share an initial secret key
or at least partially secret but identical random strings

QKD therefore does not create a secret key out of nothing:
it will expand a short secret key into a long one,
so strictly speaking it is a way of **key-growing**

Bennett Brassard - on paper

Bennett Brassard - on paper

Alice prepares a photon in one of the four states and sends it to Bob

Bob measures it in either the + or the × basis

This step is repeated N times. Both Alice and Bob have a list of N pairs **(bit,basis)**

Bennett Brassard - on paper

Alice prepares a photon in one of the four states and sends it to Bob
Bob measures it in either the + or the × basis
This step is repeated N times. Both Alice and Bob have a list of N pairs **(bit,basis)**

Alice and Bob communicate over the classical channel and compare the basis
discard those in which they have used different bases
Alice and Bob have a list of approximately N/2 bits, this is called **raw key**

Bennett Brassard - on paper

Alice prepares a photon in one of the four states and sends it to Bob
Bob measures it in either the + or the × basis
This step is repeated N times. Both Alice and Bob have a list of N pairs **(bit,basis)**

Alice and Bob communicate over the classical channel and compare the basis
discard those in which they have used different bases
Alice and Bob have a list of approximately N/2 bits, this is called **raw key**

Alice and Bob reveal a random sample of their raw keys and estimate the error rate
They have to correct them and to erase the information that Eve obtains by
communication on the classical channel, **(classical post-processing)**
Alice and Bob share either a secret key or abort

Security

a non-secret key is never used

Either the authorised partners can create a secret key (a common list of secret bits known only to themselves), or they **abort** the protocol.

After classical communication Alice and Bob estimate
how much information about their lists of bits has leaked out to Eve
Such an estimate is impossible in classical communication.

In a quantum channel, leakage of information is quantitatively related to a perturbation of the communication.

Security

fundamental principles of quantum physics

Security

fundamental principles of quantum physics

Any action, by which Eve extracts some information out of quantum states, is a generalised form of ***measurement*** in quantum physics measurement in general modifies the state of the measured system.

Security

fundamental principles of quantum physics

Any action, by which Eve extracts some information out of quantum states, is a generalised form of ***measurement*** in quantum physics measurement in general modifies the state of the measured system.

Eve's goal is to have a perfect copy of the state that Alice sends to Bob
This is forbidden by the ***no-cloning theorem***
one cannot duplicate an unknown quantum state while keeping the original intact

Security

fundamental principles of quantum physics

Any action, by which Eve extracts some information out of quantum states, is a generalised form of ***measurement*** in quantum physics measurement in general modifies the state of the measured system.

Eve's goal is to have a perfect copy of the state that Alice sends to Bob
This is forbidden by the ***no-cloning theorem***
one cannot duplicate an unknown quantum state while keeping the original intact

Quantum correlations obtained by separate measurements
on entangled pairs violate ***Bell's inequalities***
They cannot be created by pre-established agreement
The outcomes of the measurements did not exist before the measurements
but then, in particular, Eve could not know them.

Post processing

(In the absence of system errors) the spy will get detected
by the errors she induces in the communication

But all practical systems have innocent errors!

Post processing

(In the absence of system errors) the spy will get detected
by the errors she induces in the communication

But all practical systems have innocent errors!

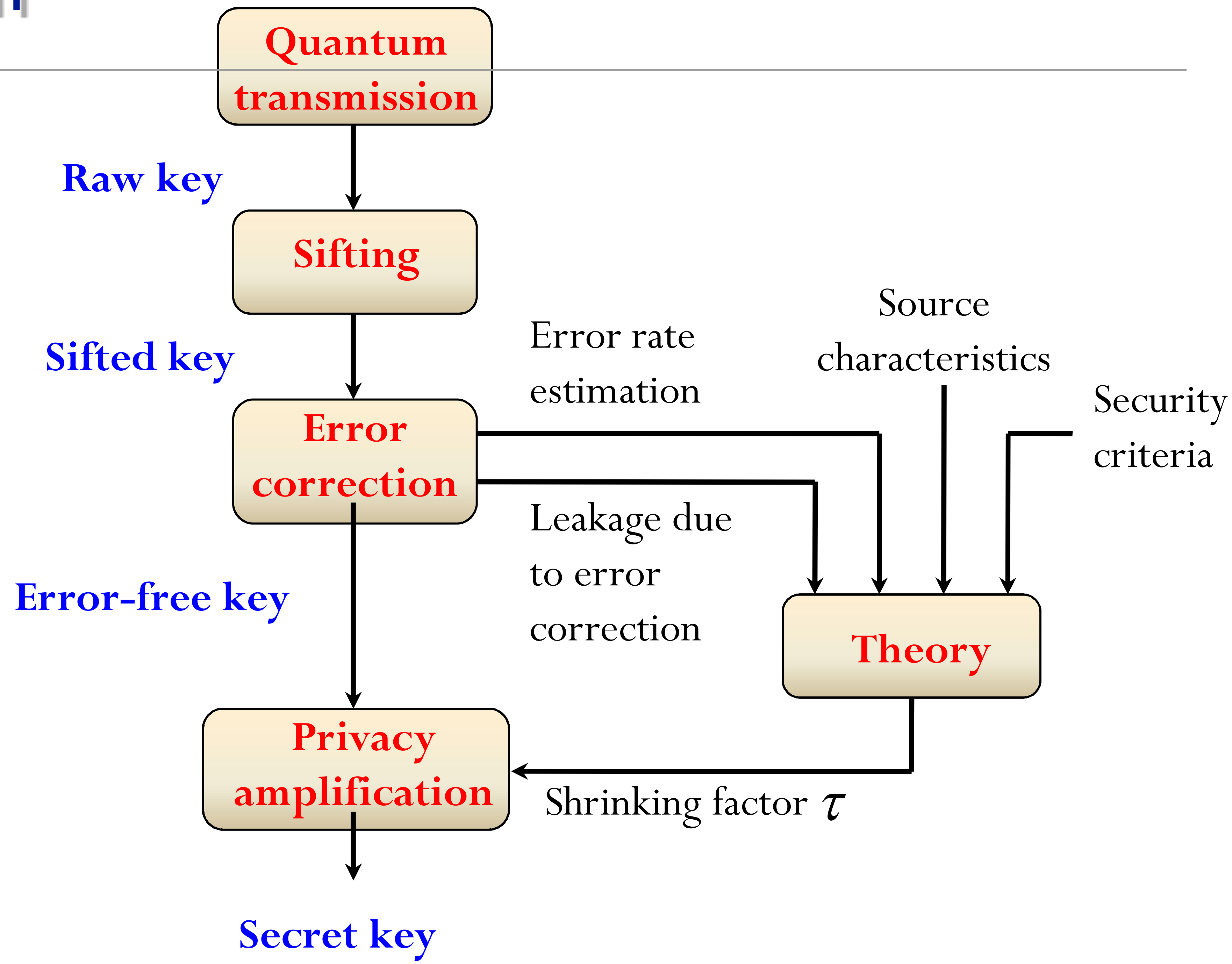
A complete QKD protocol should consider all errors as errors due to Eve, take into account possible information leakage, and bound this leakage as a function of the error rate

this is performed by two additional processes

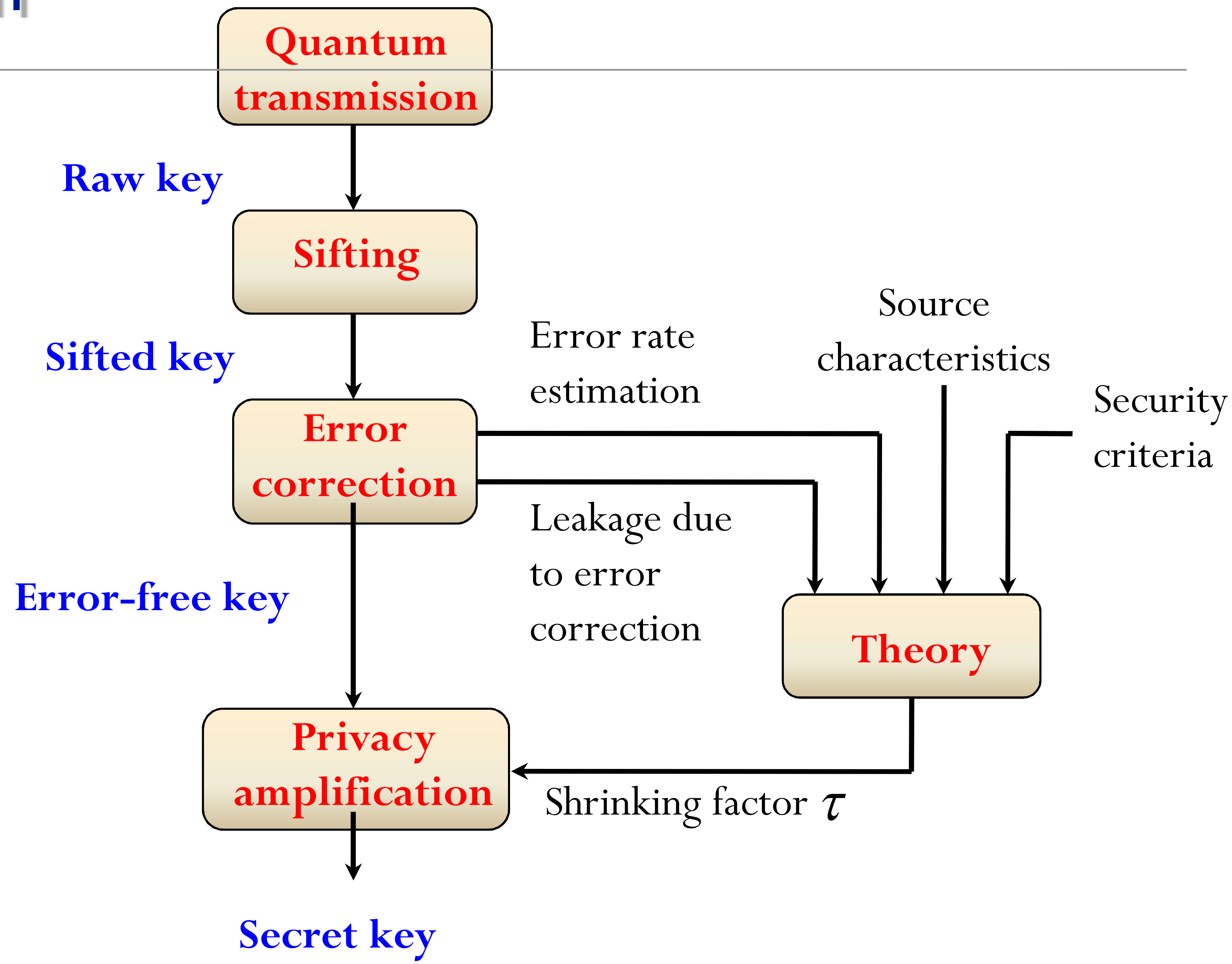
Error correction + Privacy amplification

both are classical procedures

A QKD algorithm



A QKD algorithm



A security proof of a QKD protocol, which provides a given **shrinking factor** is a very difficult theoretical exercise with still many open questions

Composable security

A composable definition of security is the one based on the trace-norm (Ben-Or et al., 2005; Renner and Konig, 2005):

$$\frac{1}{2}\|\rho_{\mathcal{K}E} - \tau_{\mathcal{K}} \otimes \rho_E\|_1 \leq \varepsilon$$

Composable security

A composable definition of security is the one based on the trace-norm (Ben-Or et al., 2005; Renner and Konig, 2005):

any state of Eve

$$\frac{1}{2}\|\rho_{\mathcal{K}E} - \tau_{\mathcal{K}} \otimes \rho_E\|_1 \leq \varepsilon$$

actual state containing some correlations between the final key and Eve

the completely mixed state on the set of possible final keys

Composable security

A composable definition of security is the one based on the trace-norm (Ben-Or et al., 2005; Renner and Konig, 2005):

any state of Eve

$$\frac{1}{2}\left\|\rho_{\mathcal{K}E} - \tau_{\mathcal{K}} \otimes \rho_E\right\|_1 \leq \varepsilon$$

actual state containing some correlations between the final key and Eve

the completely mixed state on the set of possible final keys

This is an extension of simulation-based definitions of universally composable security

Trace-norm contracts under QM transformations
plays the role of “statistical distance” or total variation

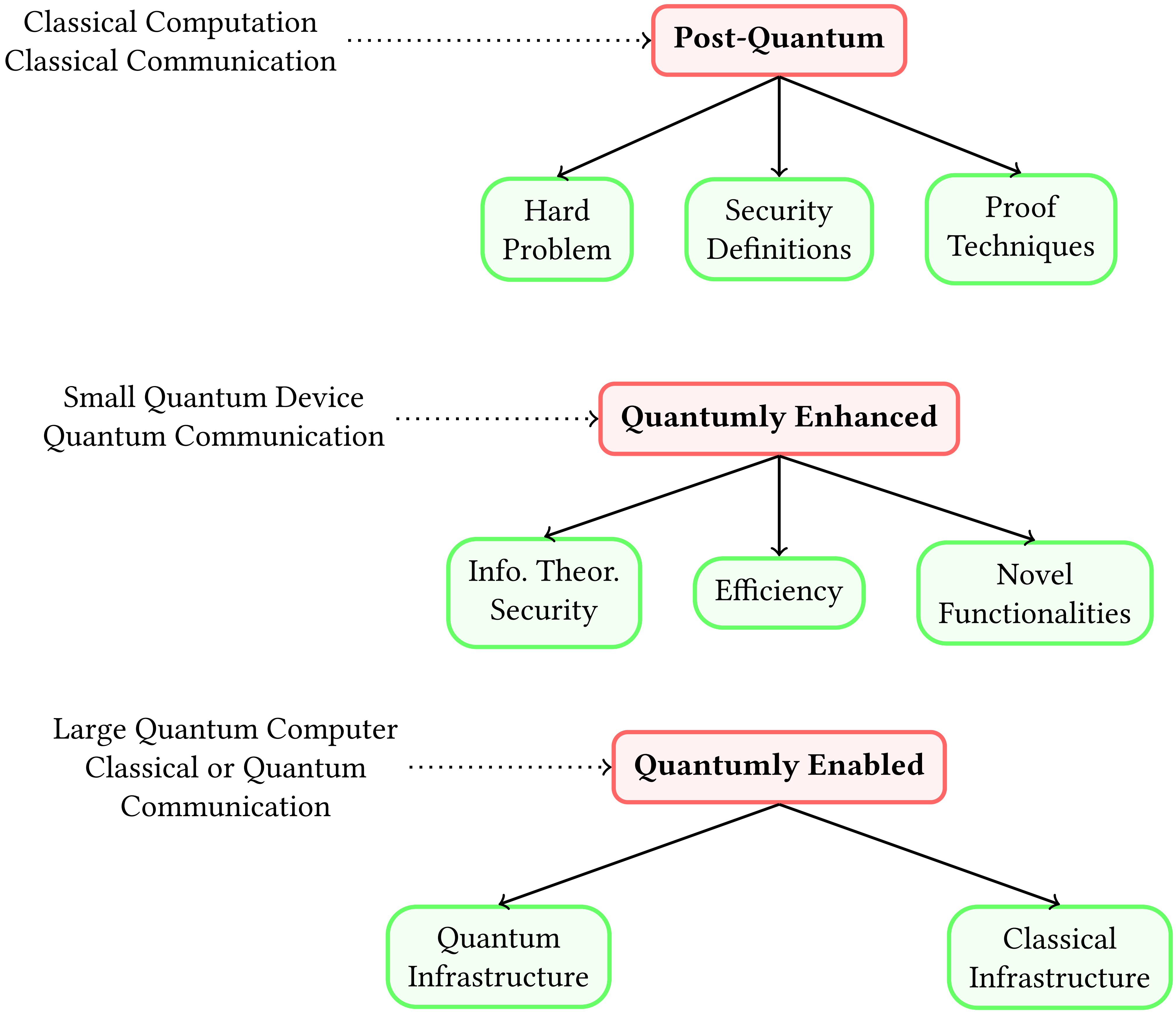
Security property - finally!

$$\frac{1}{2}\|\rho_{\mathcal{K}E} - \tau_{\mathcal{K}} \otimes \rho_E\|_1 \leq \varepsilon$$

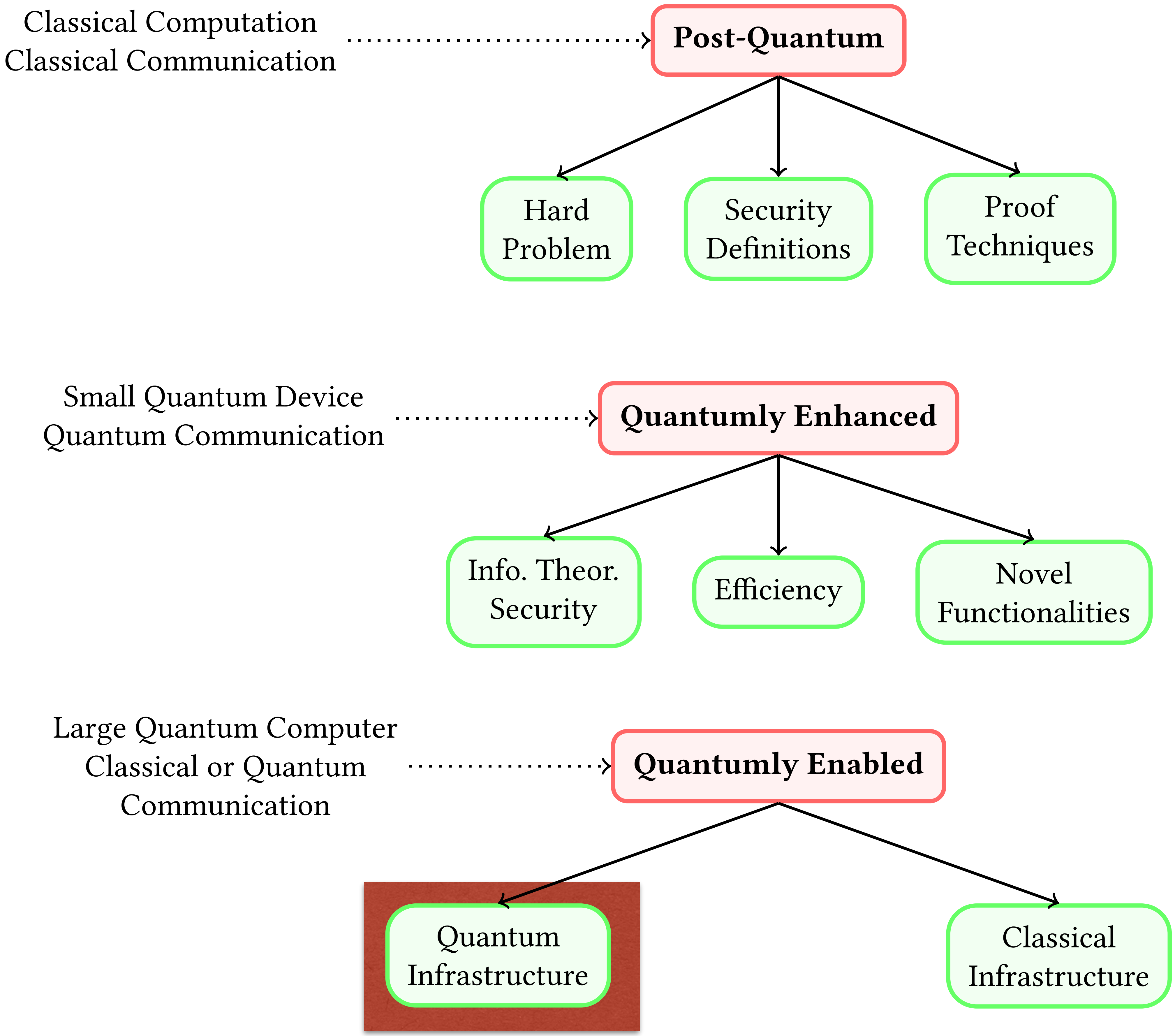
the security requirement holds with high probability

$$\mathrm{Prob}\left[\|\rho_{\mathcal{K}E} - \tau_{\mathcal{K}} \otimes \rho_E\|_1 > 2\varepsilon\right] \lesssim e^{\ell - F(\rho_{\mathcal{K}E},\varepsilon)}$$

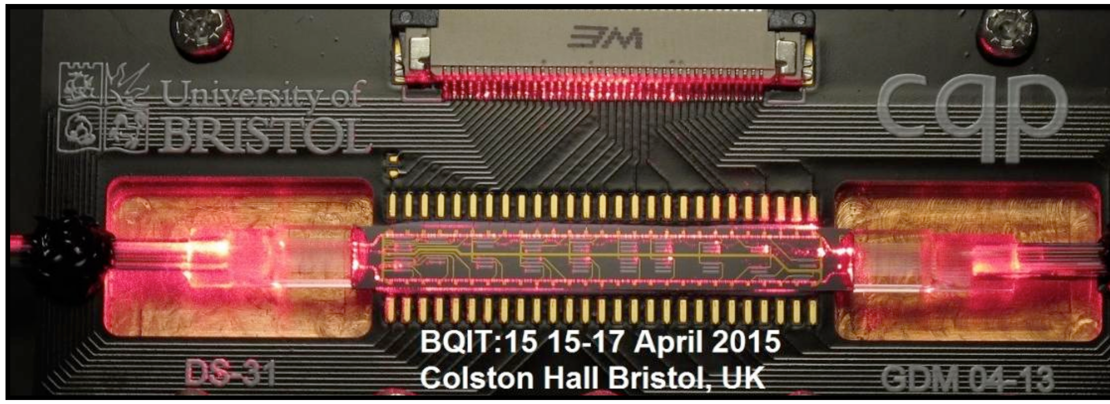
concretely, *F* will be depending on the protocol, and gives the length *l* of the secret key that can be extracted as a function of the indistinguishability/security parameter ε for a certain level of risk



Classical Computation
Classical Communication
Post-Quantum
Hard Problem
Security Definitions
Proof Techniques
Small Quantum Device
Quantum Communication
Quantumly Enhanced
Info. Theor. Security
Efficiency
Novel Functionalities
Large Quantum Computer
Classical or Quantum Communication
Quantumly Enabled
Quantum Infrastructure
Classical Infrastructure


Classical Computation
Classical Communication
Post-Quantum
Hard Problem
Security Definitions
Proof Techniques
Small Quantum Device
Quantum Communication
Quantumly Enhanced
Info. Theor. Security
Efficiency
Novel Functionalities
Large Quantum Computer
Classical or Quantum Communication
Quantumly Enabled
Quantum Infrastructure
Classical Infrastructure

Quantum Cloud Service



Quantumly Enabled

Quantum Delegated Computing

Quantum Yao Garbled Circuit

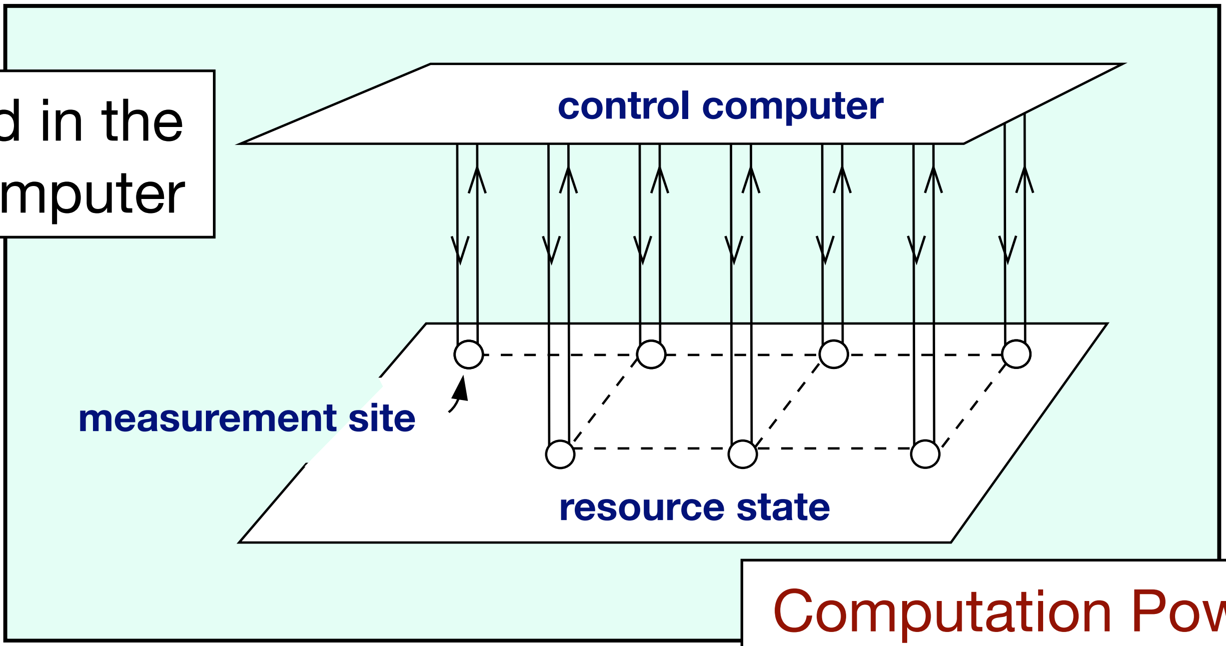
Quantum Fully Homomorphic Encryption

Quantum One-time program

Quantum Secure Multi Party Computation

Trusted Quantum Cloud Computing

Program is encoded in the classical control computer

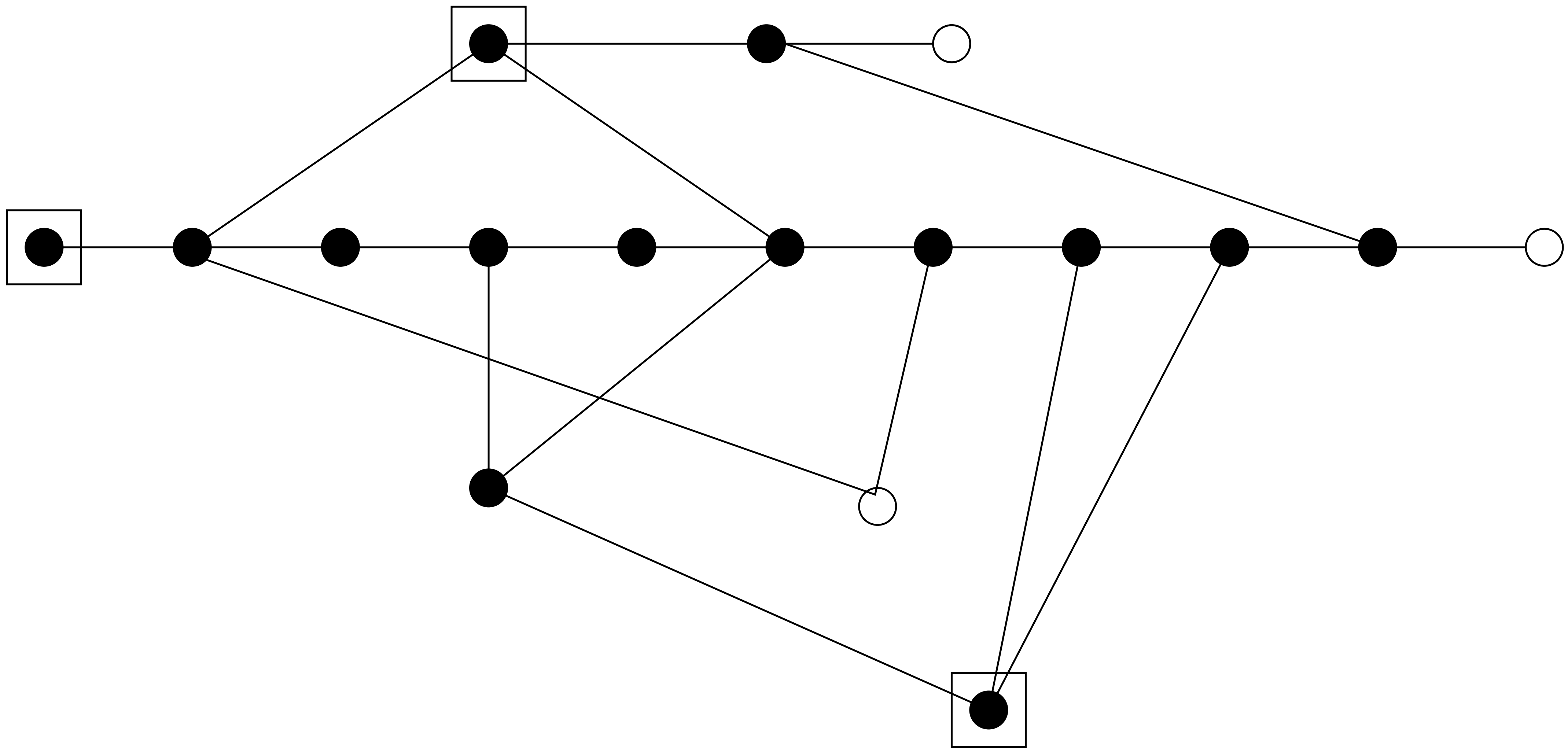


Computation Power is encoded in the quantum entanglement

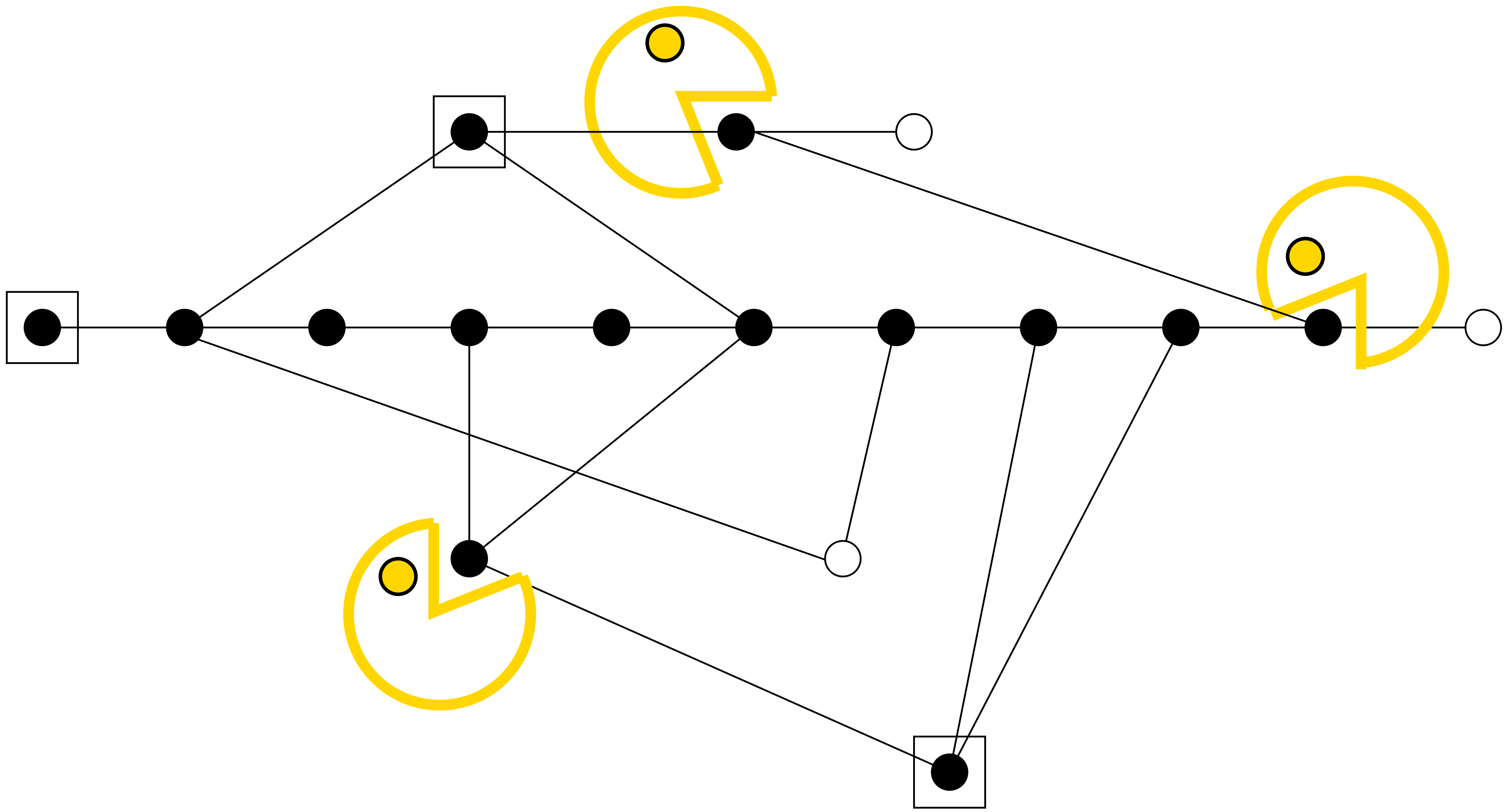
Abstract Model : Measurement-based QC

- 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

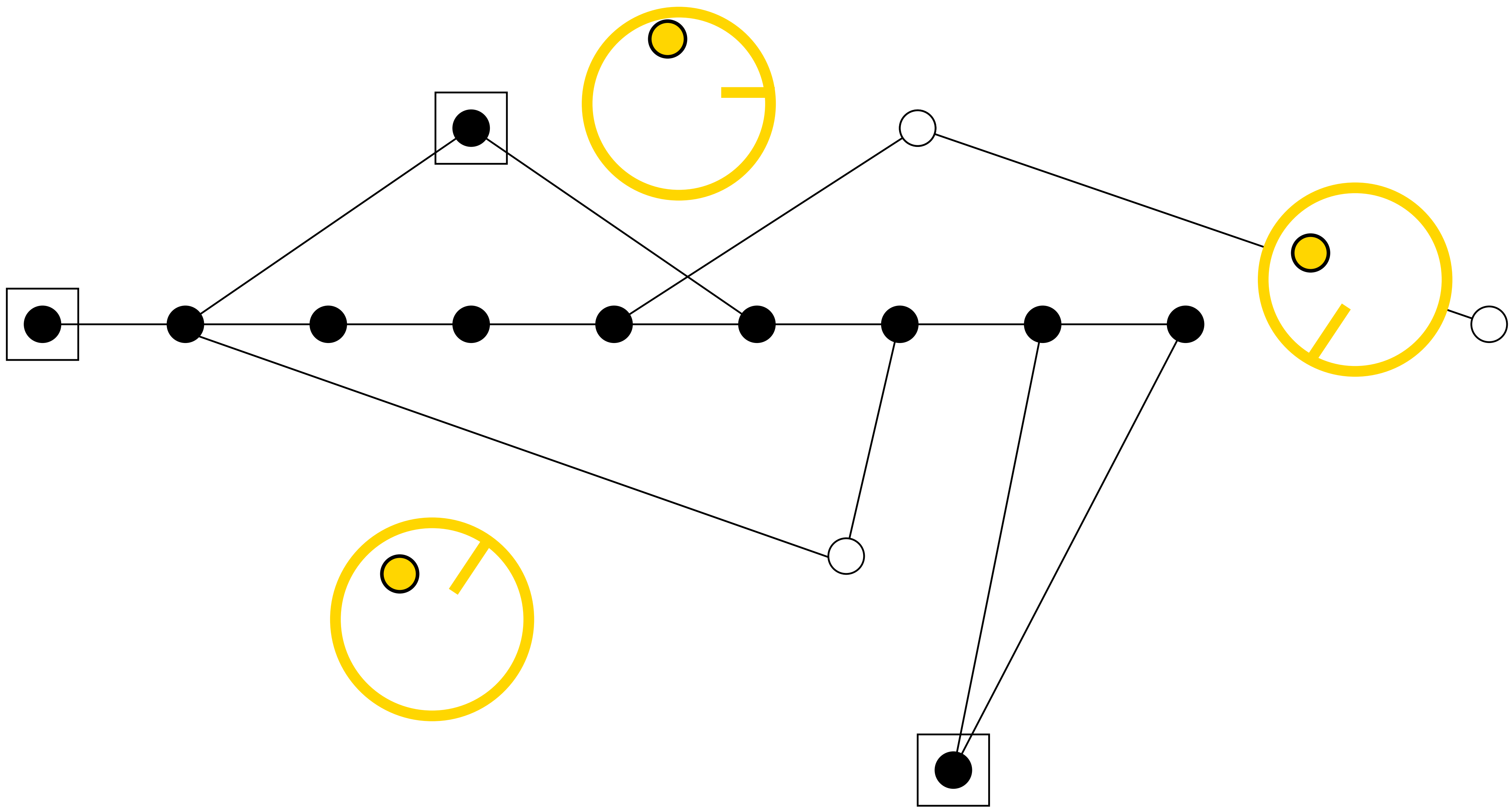
Quantum Pacman



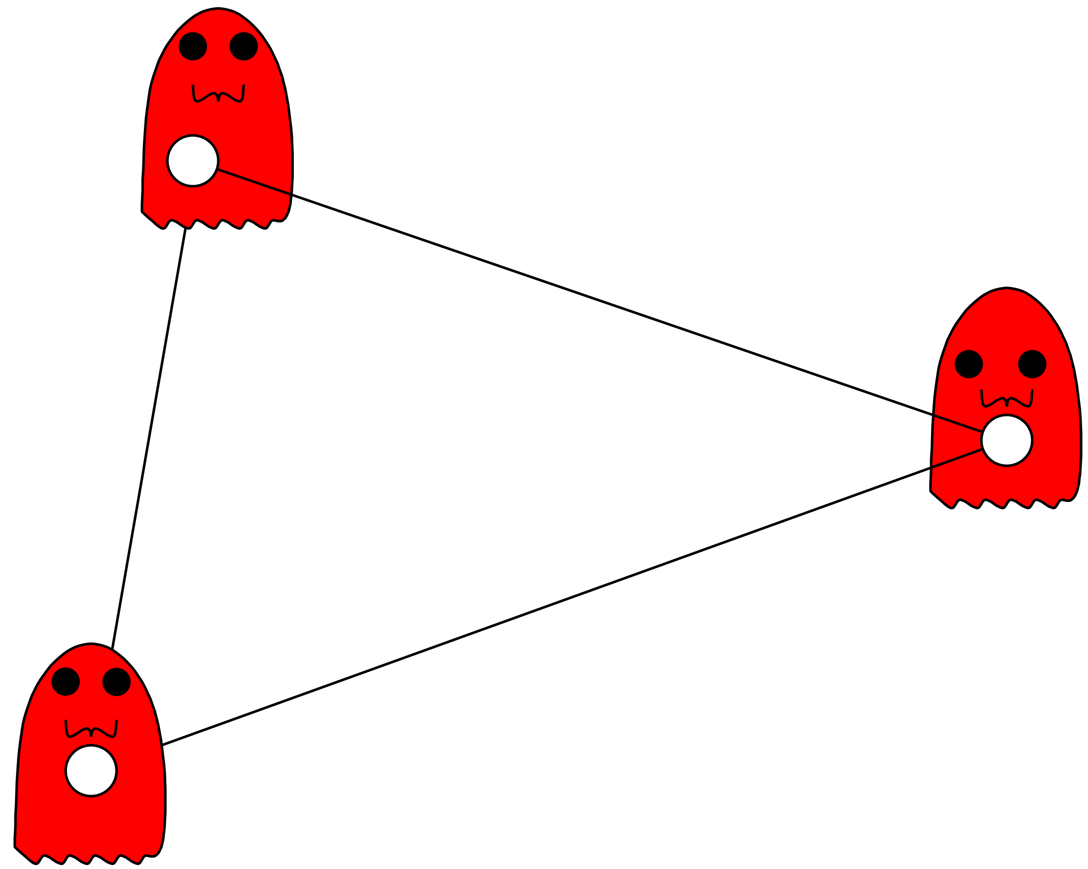
Quantum Pacman



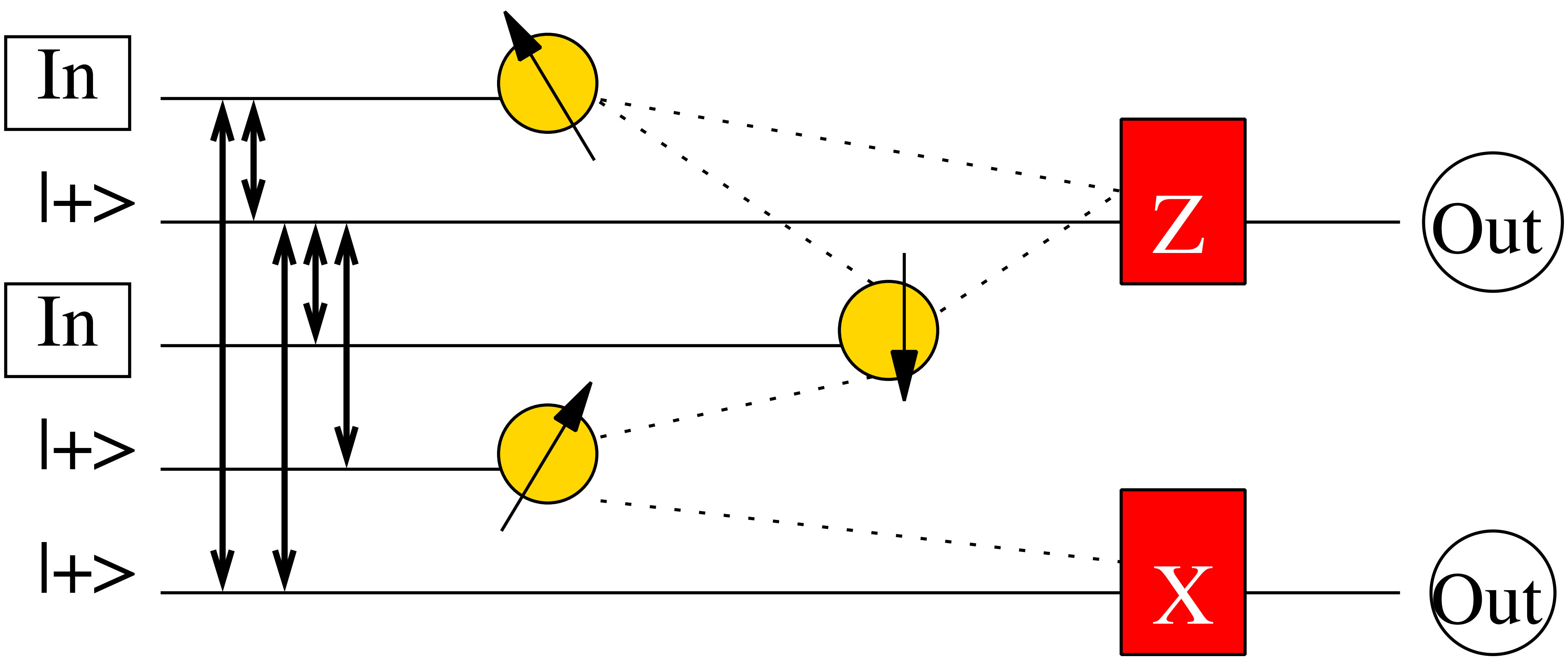
Quantum Pacman



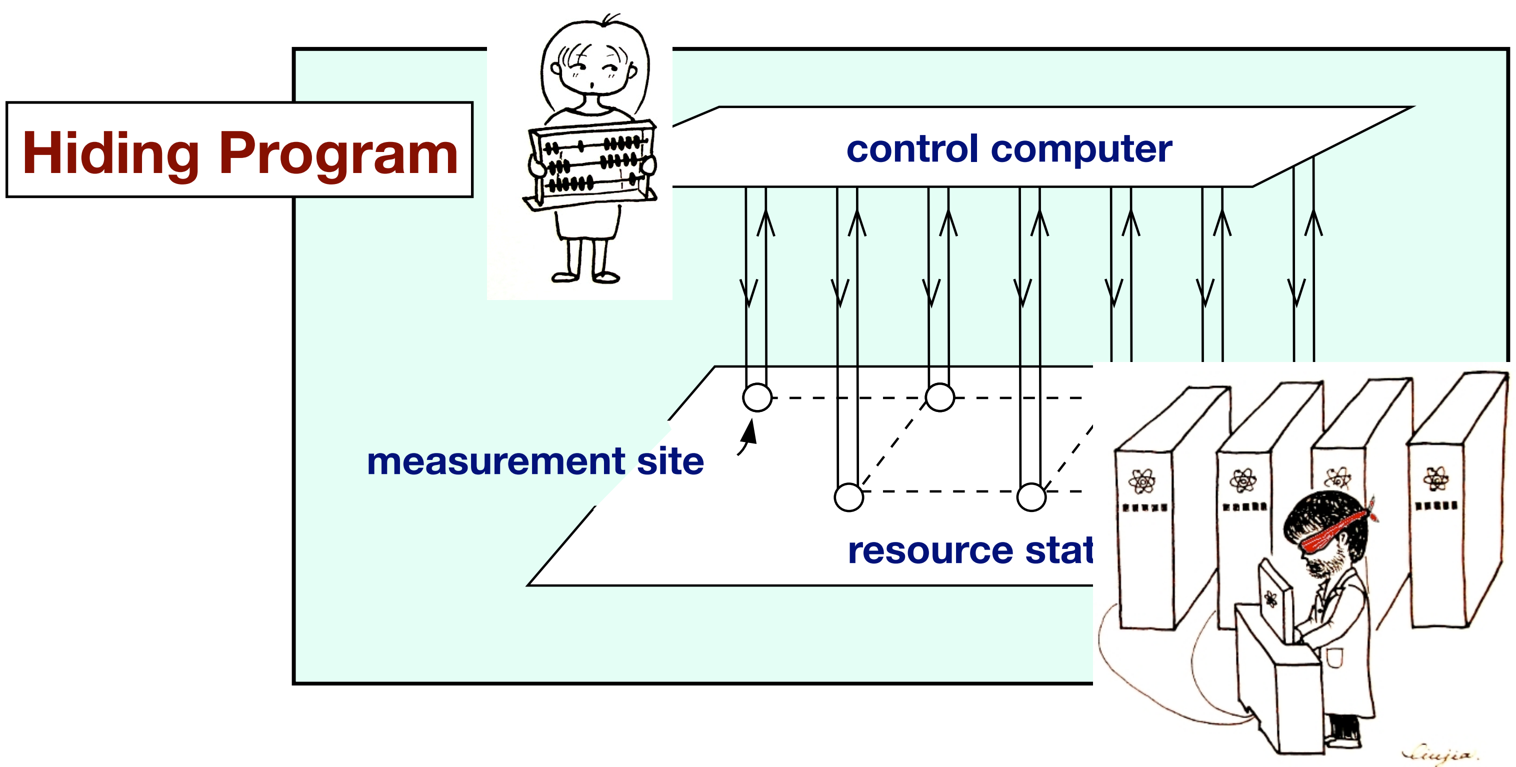
Quantum Pacman



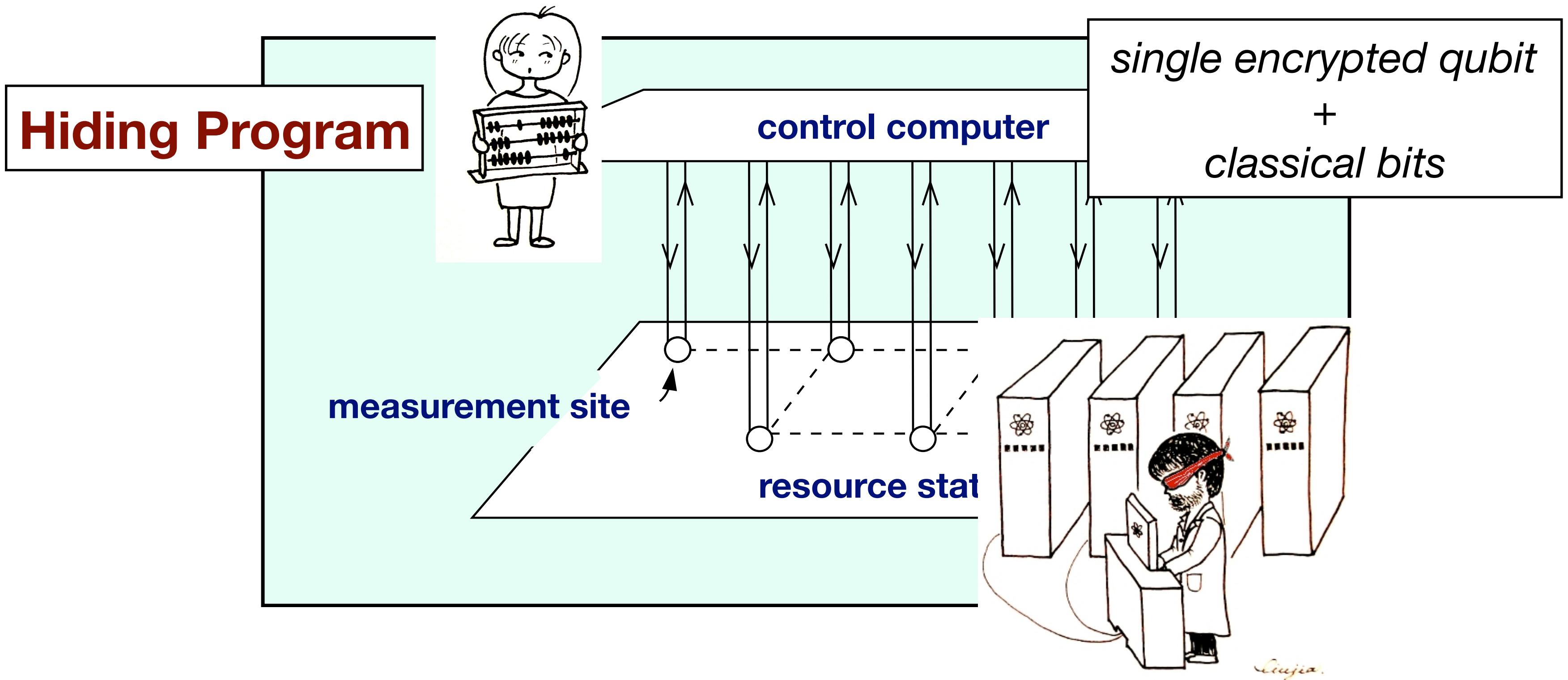
Circuit Picture



Untrusted Quantum Cloud Computing

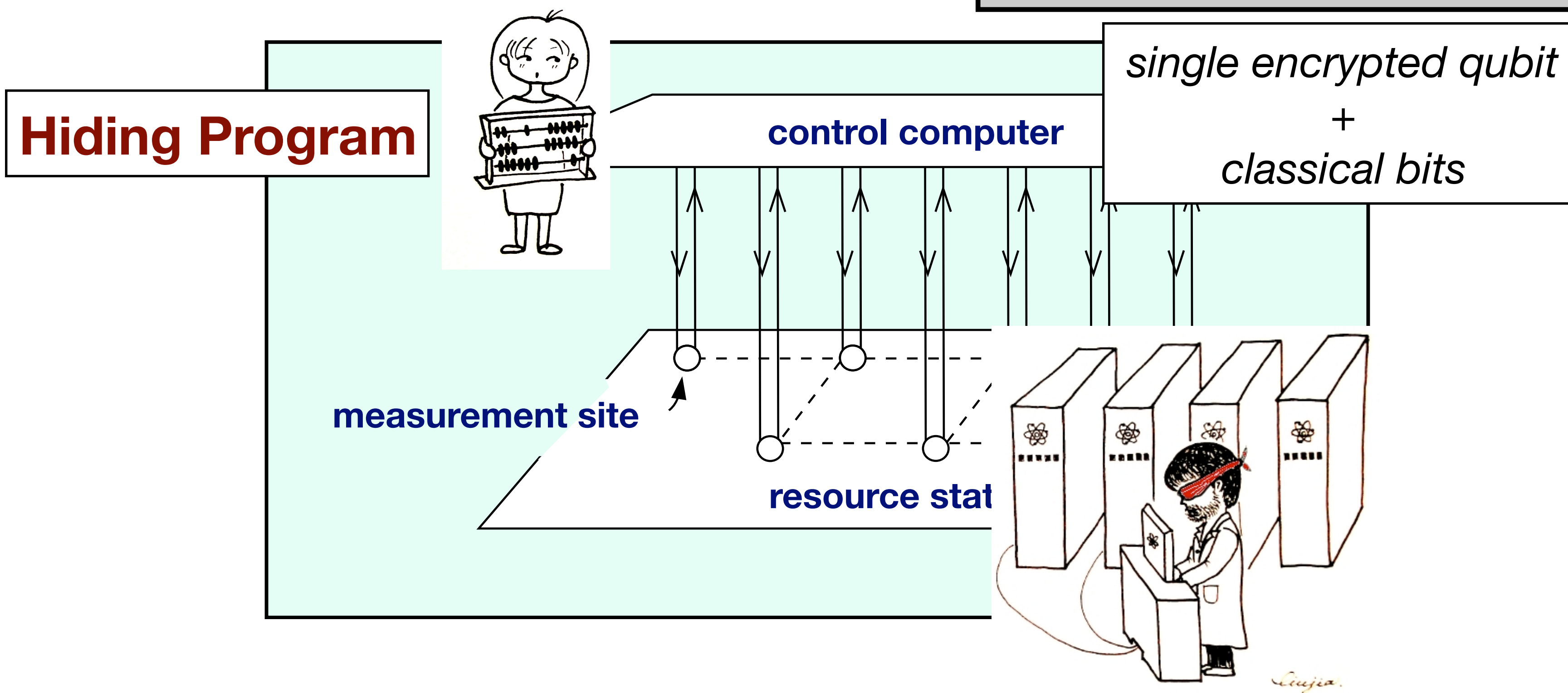


Untrusted Quantum Cloud Computing

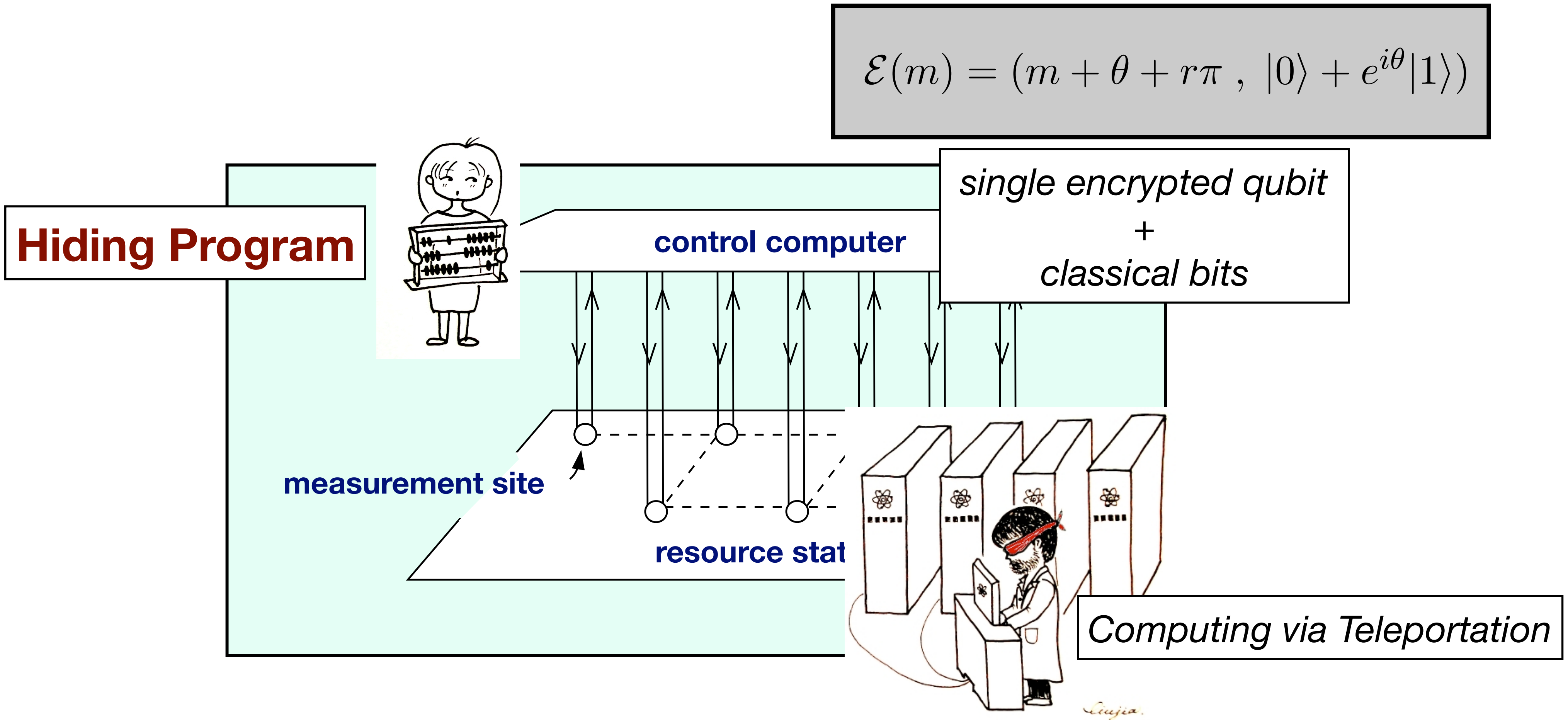


Untrusted Quantum Cloud Computing

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



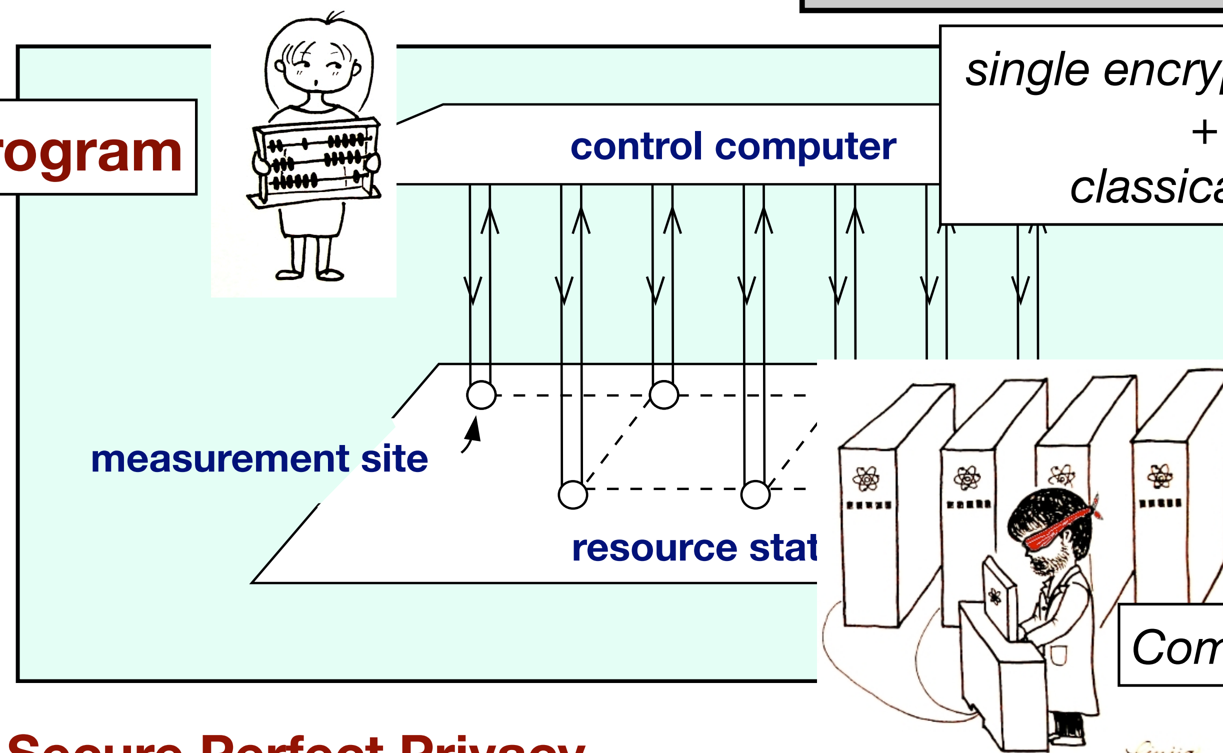
Untrusted Quantum Cloud Computing



Untrusted Quantum Cloud Computing

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

Hiding Program



single encrypted qubit
+
classical bits

Computing via Teleportation

Informationally Secure Perfect Privacy

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

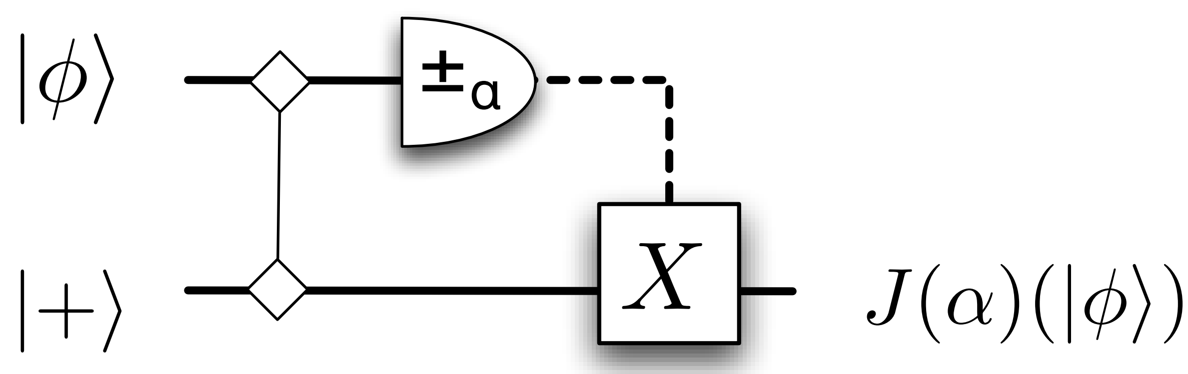
Hiding One Gate

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

Hiding One Gate

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

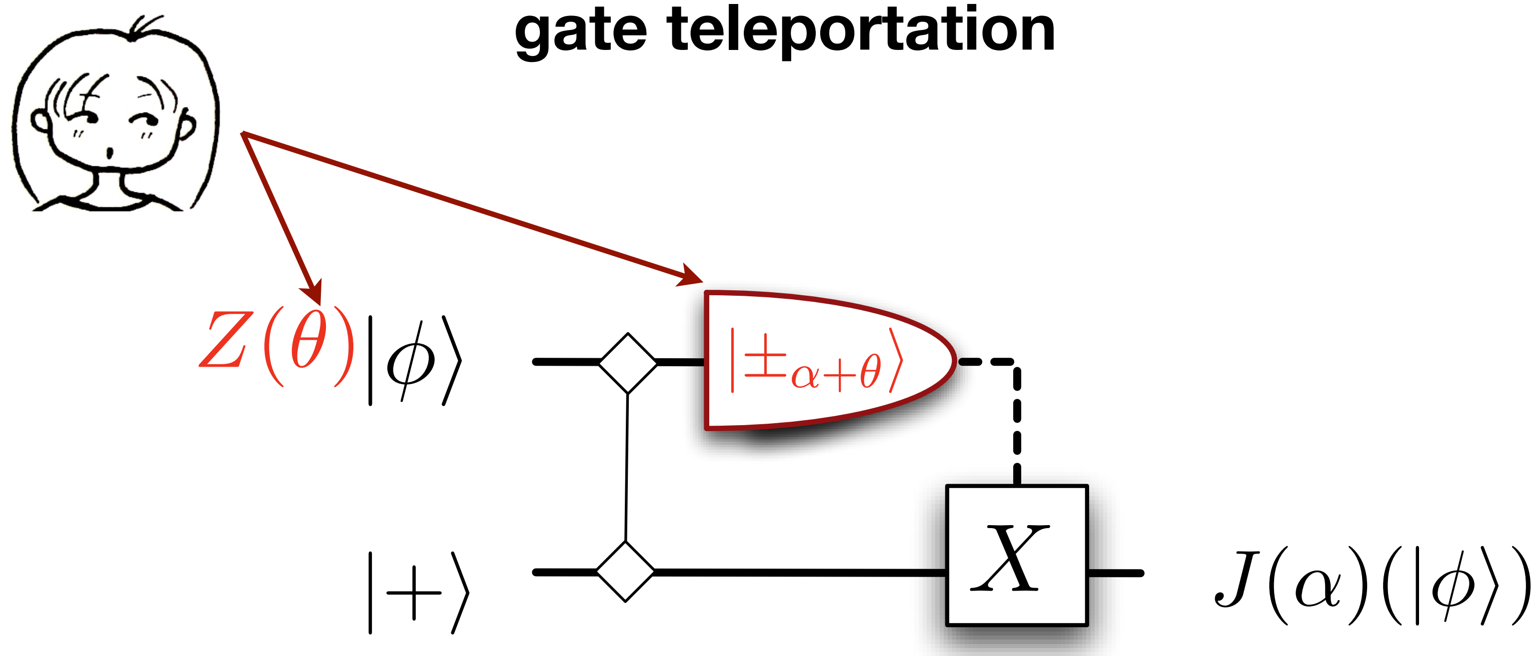
gate teleportation



Hiding One Gate

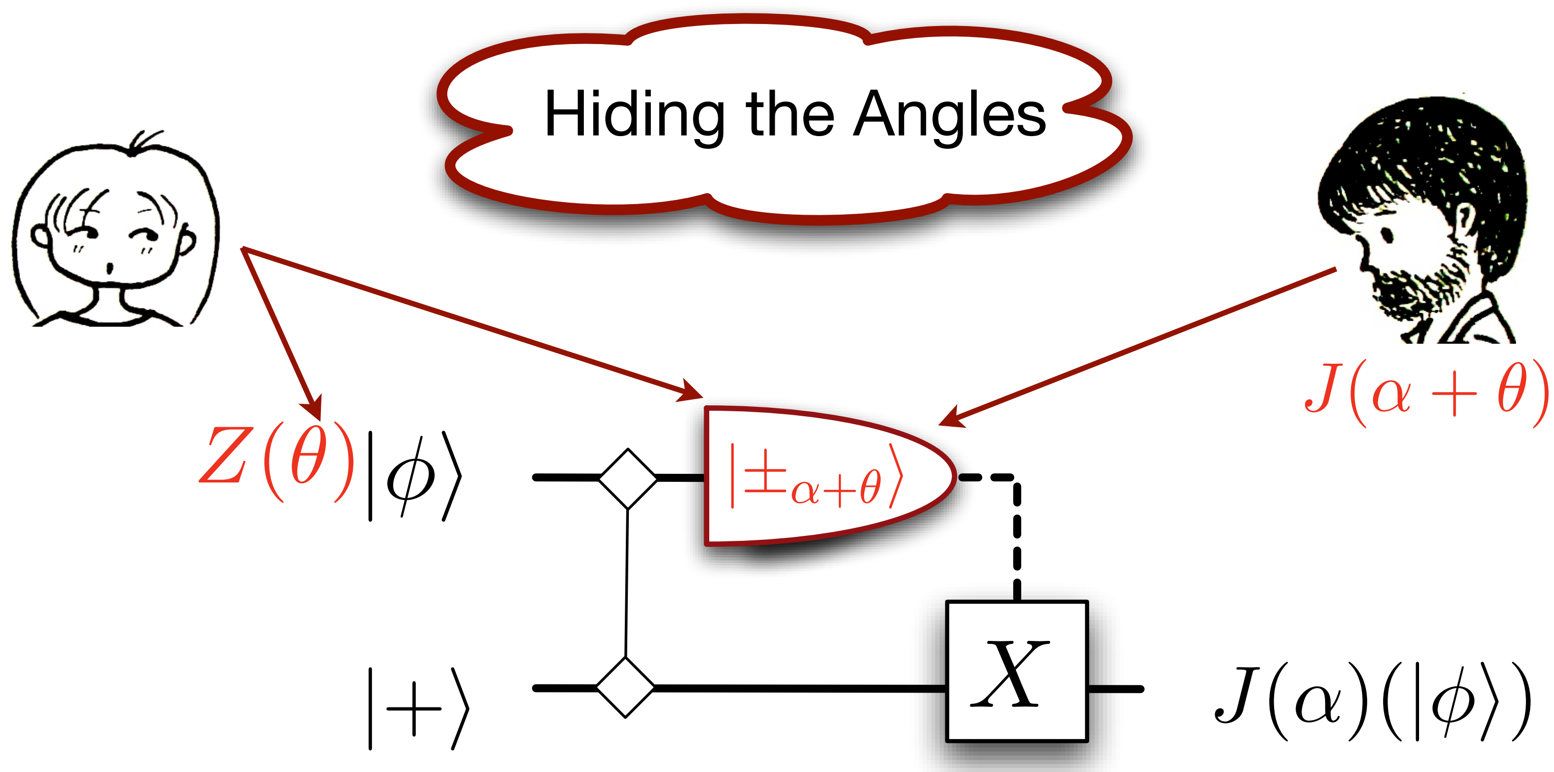
$$J(\alpha) \;:=\; \frac{1}{\sqrt{2}}\begin{pmatrix}1 & e^{i\alpha}\\ 1 & -e^{i\alpha}\end{pmatrix}$$

gate teleportation



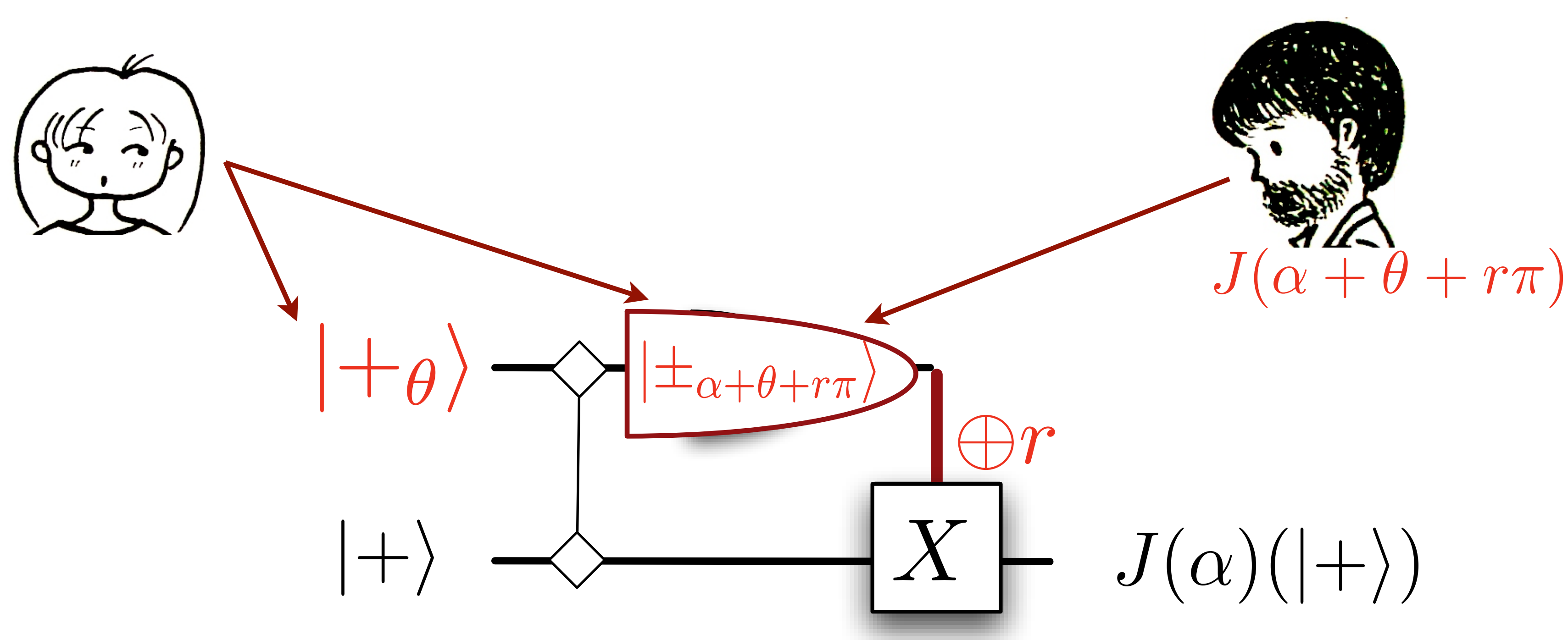
Hiding One Gate

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



Hiding One Gate

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

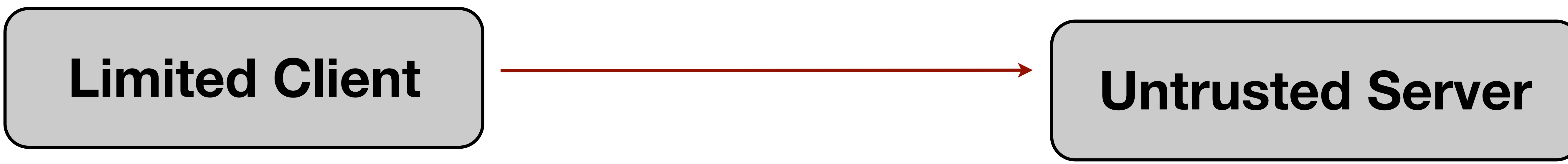


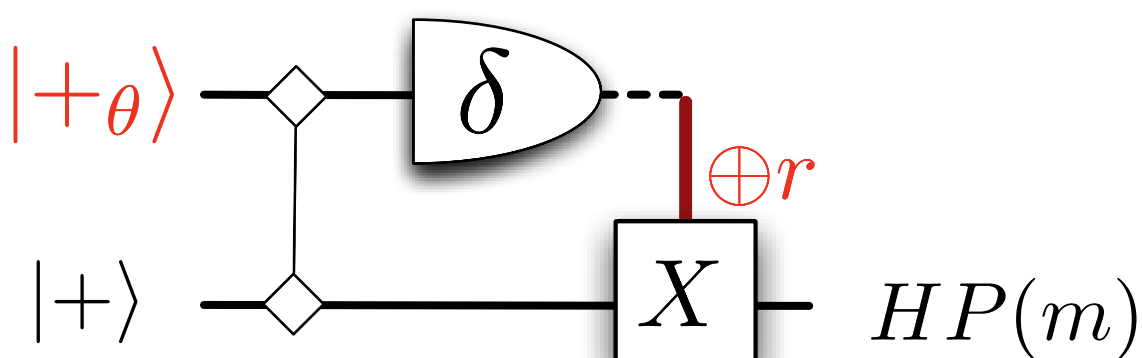
Hiding the measurement result

Hiding One Gate

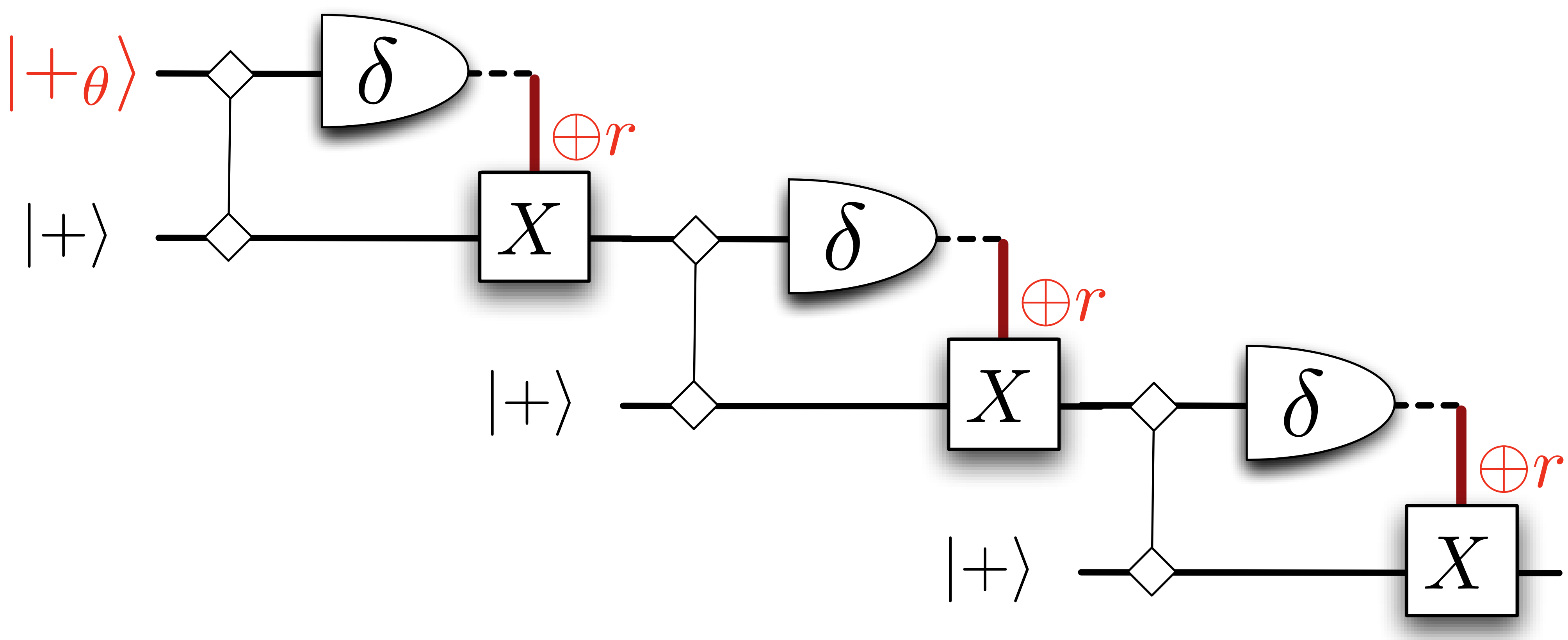
$$\theta \in_R \{0, \pi/4, 2\pi/4, \cdots, 7\pi/4\}$$

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

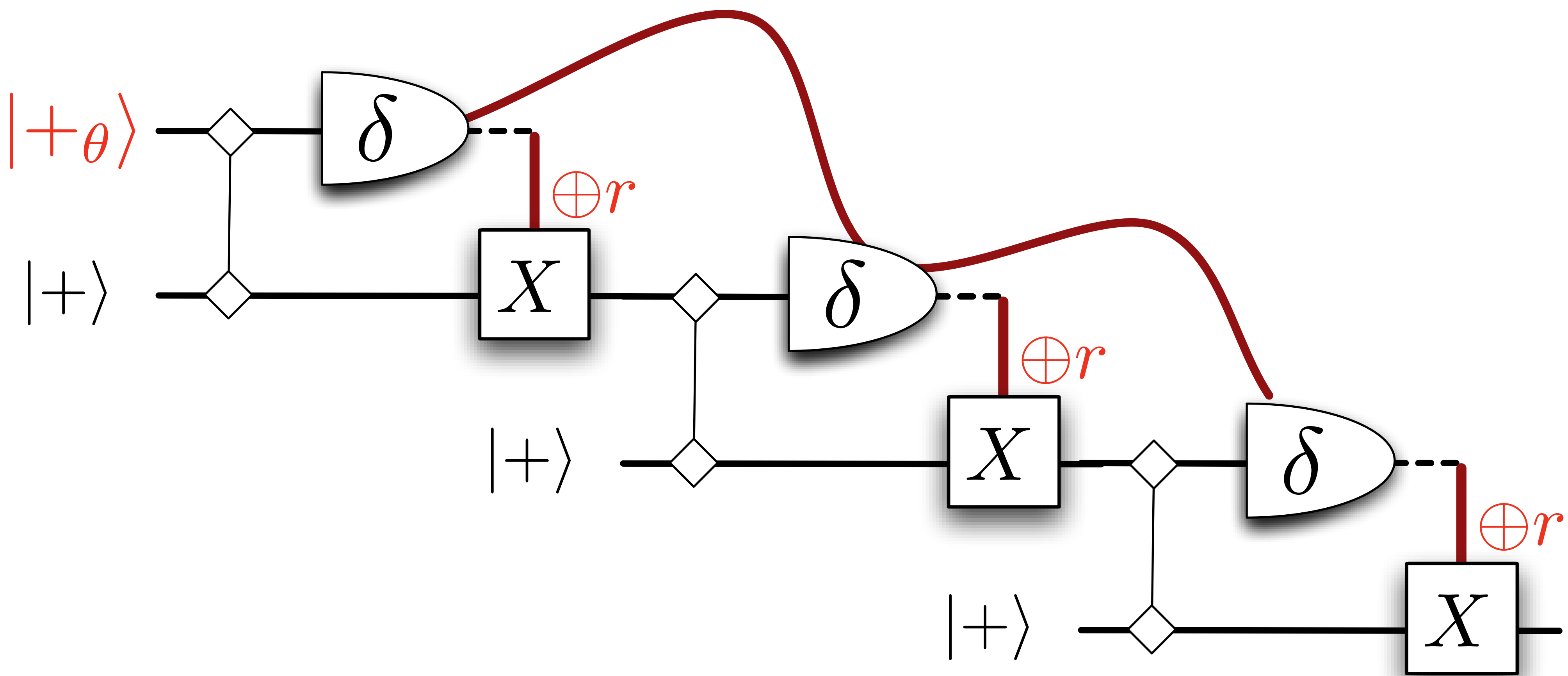




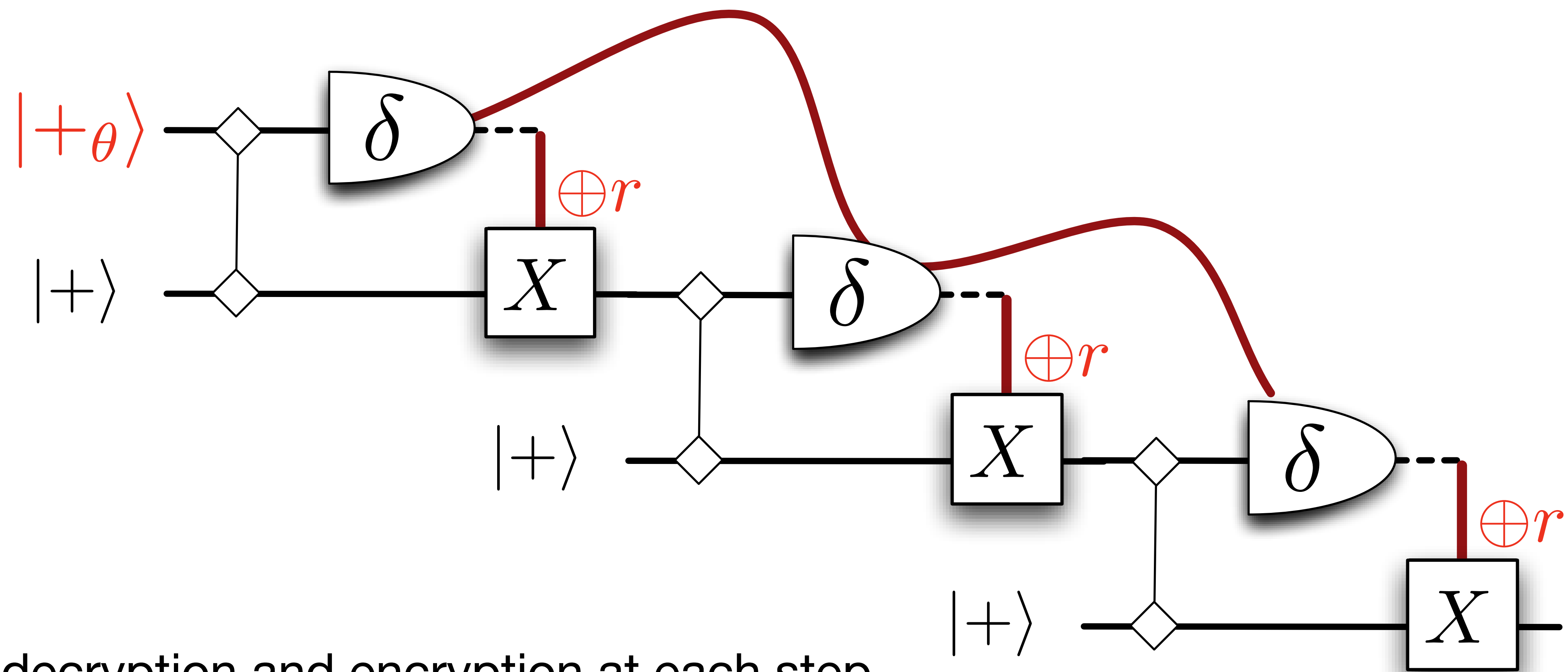
Gates Composition



Gates Composition



Gates Composition



Perfect decryption and encryption at each step

Client-Server interactions

Universal Blind Quantum Computings

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

Universal Blind Quantum Computings

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

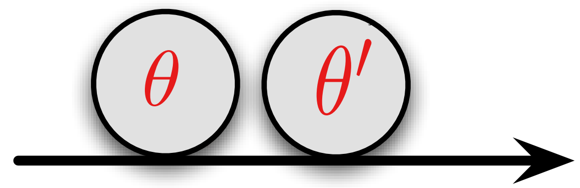
random single qubit generator

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

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

Universal Blind Quantum Computings

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

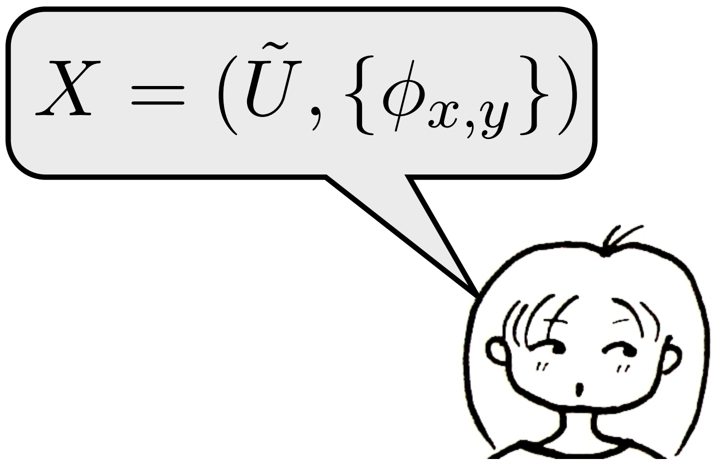


random single qubit generator

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

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

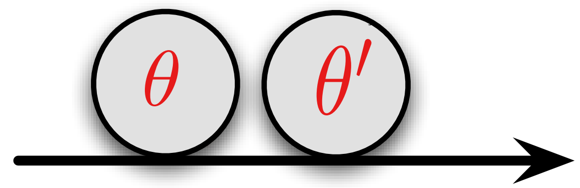
Universal Blind Quantum Computings

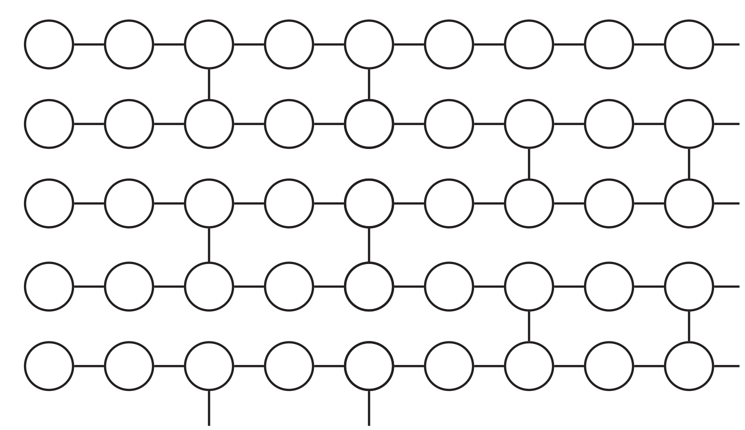


random single qubit generator

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

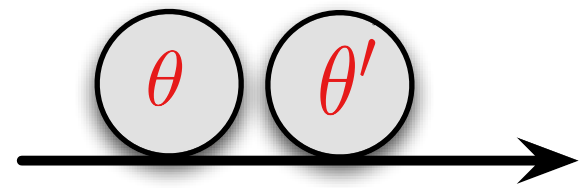
$$\theta = 0, \pi/4, 2\pi/4, \ldots, 7\pi/4$$





Universal Blind Quantum Computings

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



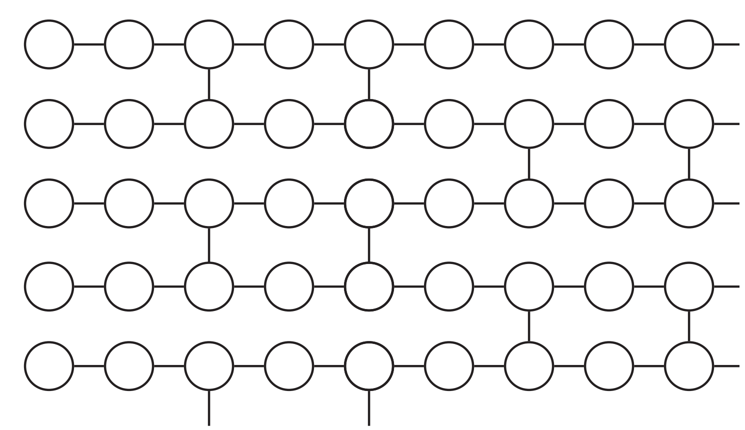
random single qubit generator

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

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

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

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



Universal Blind Quantum Computings

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

θ θ'

random single qubit generator

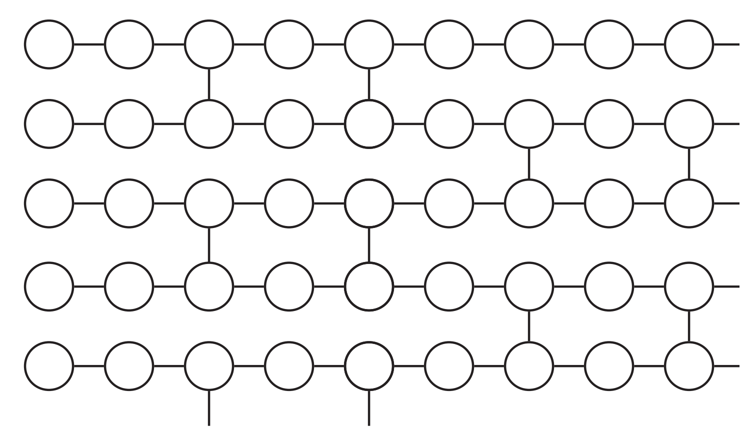
$$1/\sqrt{2}\left(|0\rangle + e^{i\theta}|1\rangle\right)$$

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

$\delta_{x,y}$

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

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



Universal Blind Quantum Computings

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

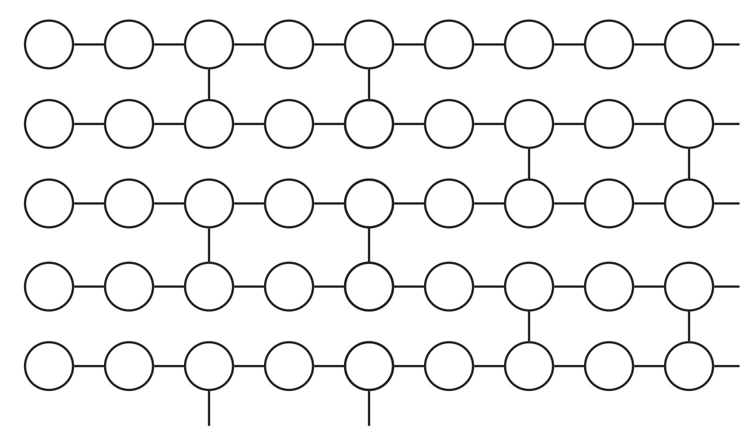
θ θ'

random single qubit generator

$$1/\sqrt{2}\left(|0\rangle + e^{i\theta}|1\rangle\right)$$
$$\theta = 0, \pi/4, 2\pi/4, \ldots, 7\pi/4$$

$\delta_{x,y}$

$r_{x,y} \in_R \{0,1\}$
$$\delta_{x,y} = \phi'_{x,y} + \theta_{x,y} + \pi r_{x,y}$$



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

Universal Blind Quantum Computings

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

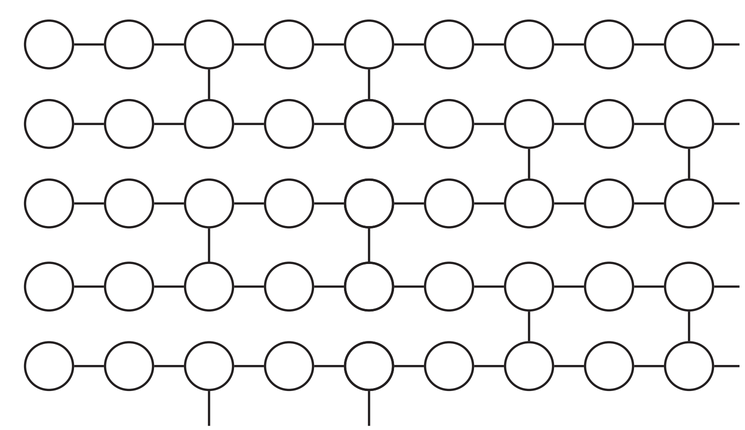
θ θ'

random single qubit generator

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

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

$\delta_{x,y}$



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

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

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

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

Universal Blind Quantum Computings

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

random single qubit generator

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

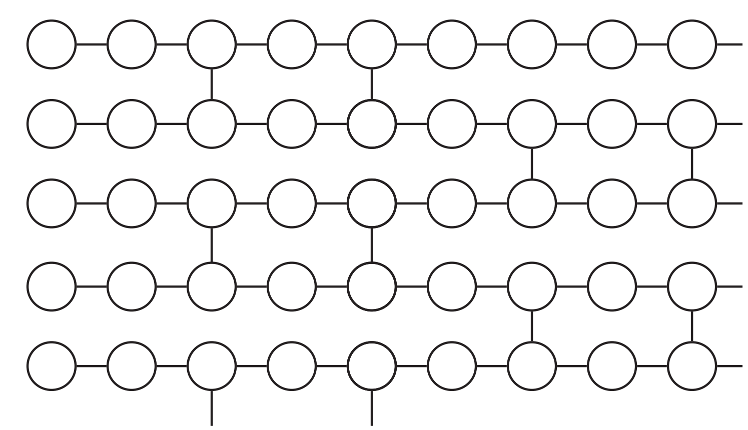
$$\theta = 0, \pi/4, 2\pi/4, \ldots, 7\pi/4$$

θ θ'

$\delta_{x,y}$

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

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



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

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

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

Blindness

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

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

➡ Given the above distribution, the quantum state is fixed and independent of X

Proof (L(X)=m,n)

- Independence of Bob’s classical information

Proof (L(X)=m,n)

➡ Independence of Bob's classical information

$$\theta_{x,y} \in_R \{0, \cdots, 7\pi/4\}$$

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

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

Proof (L(X)=m,n)

➡ Independence of Bob's classical information

$$\theta_{x,y} \in_R \{0, \cdots, 7\pi/4\}$$

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

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

➡ Independence of Bob's quantum information for a fixed δ

Proof (L(X)=m,n)

➡ Independence of Bob's classical information

$$\theta_{x,y} \in_R \{0, \cdots, 7\pi/4\}$$

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

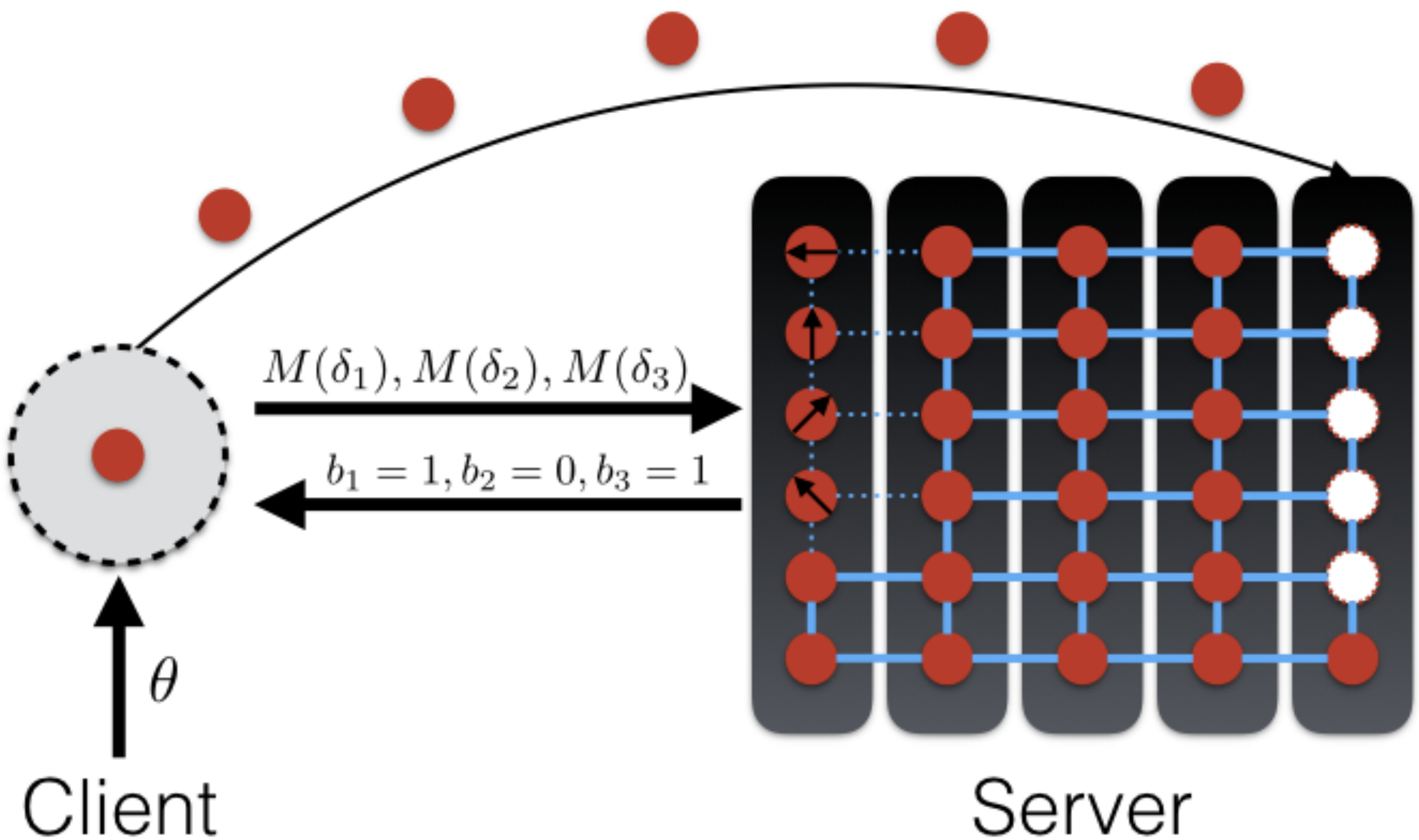
$$\delta_{x,y} = \phi'_{x,y} + \theta_{x,y} + \pi r_{x,y}$$

➡ Independence of Bob's quantum information for a fixed δ

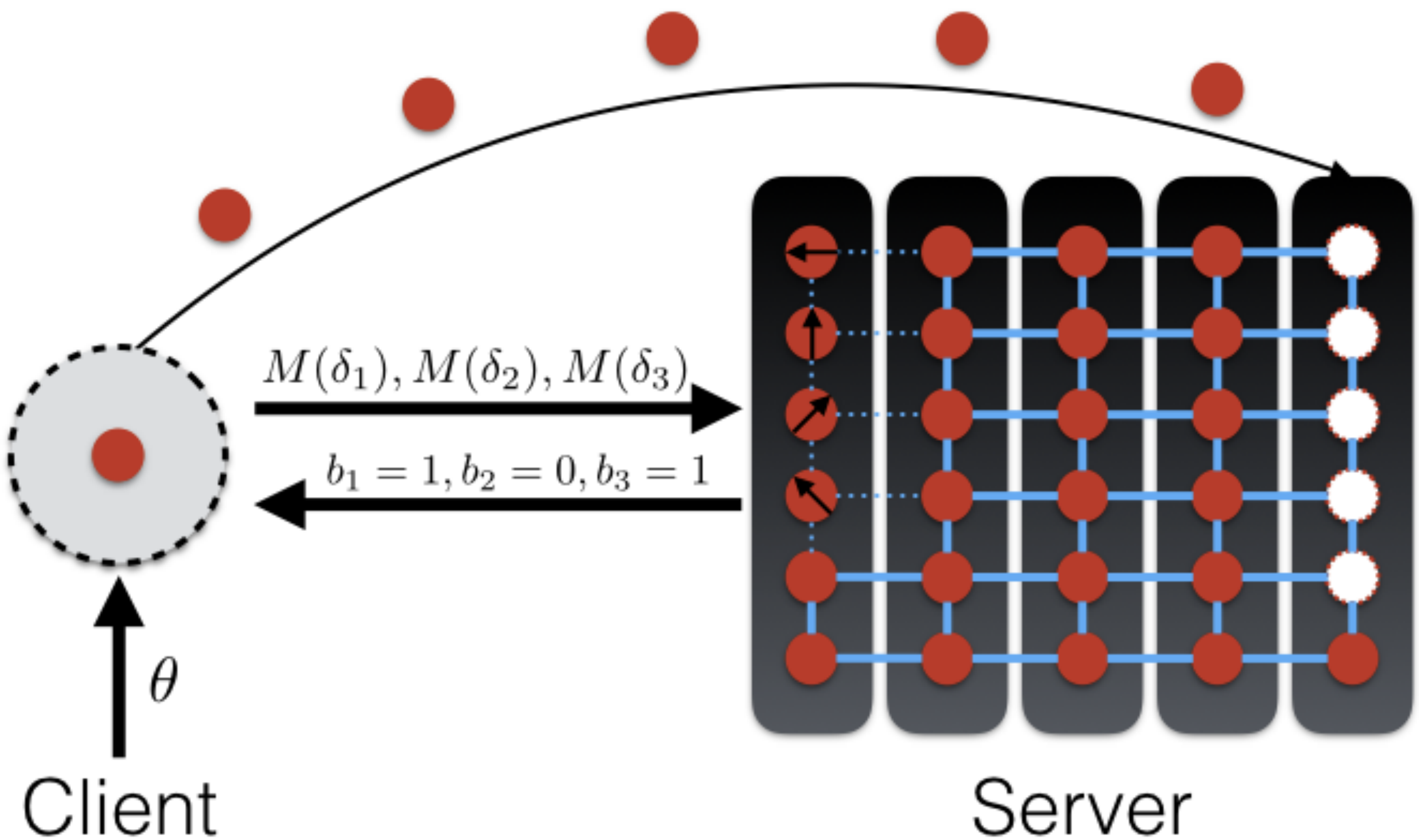
1. $r_{x,y} = 0$ so $\delta_{x,y} = \phi'_{x,y} + \theta'_{x,y}$ and $|\psi_{x,y}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i(\delta_{x,y} - \phi'_{x,y})}|1\rangle)$.

2. $r_{x,y} = 1$ so $\delta_{x,y} = \phi'_{x,y} + \theta'_{x,y} + \pi$ and $|\psi_{x,y}\rangle = \frac{1}{\sqrt{2}}(|0\rangle - e^{i(\delta_{x,y} - \phi'_{x,y})}|1\rangle)$.

Informationally Secure Quantum Cloud

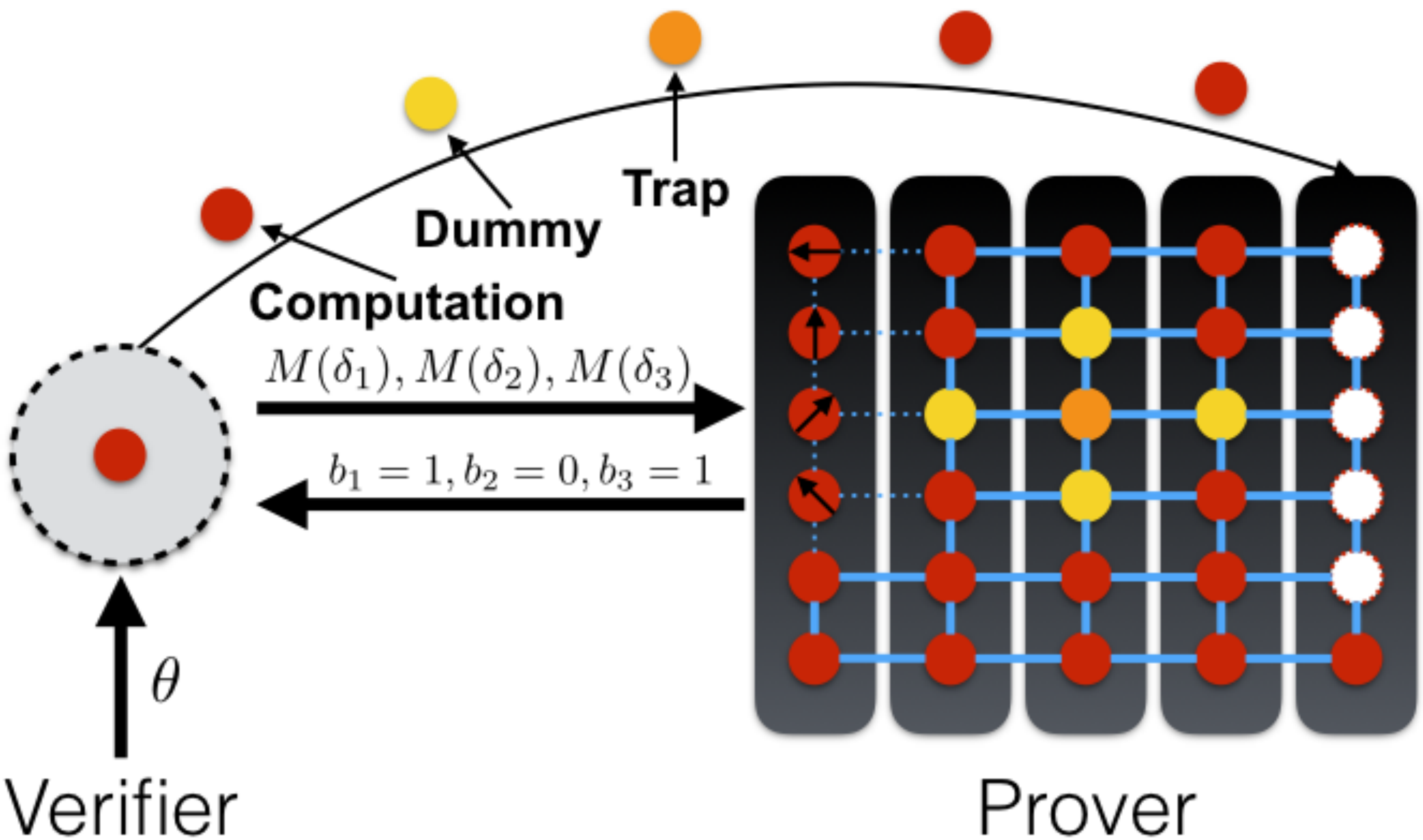


Informationally Secure Quantum Cloud

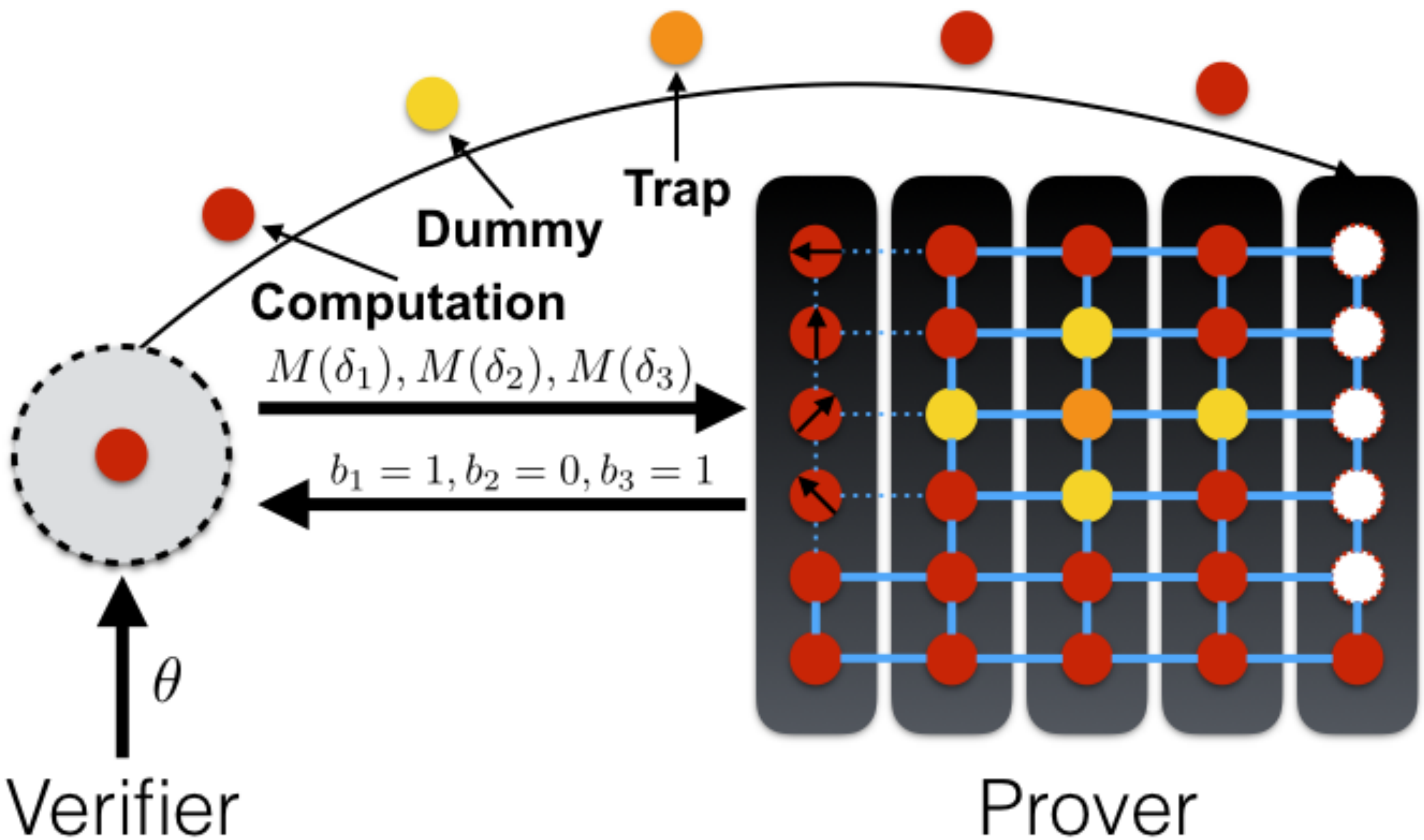


Universal Blind Quantum Computing: QKD + Teleportation

Verifiable Outsourced Computing

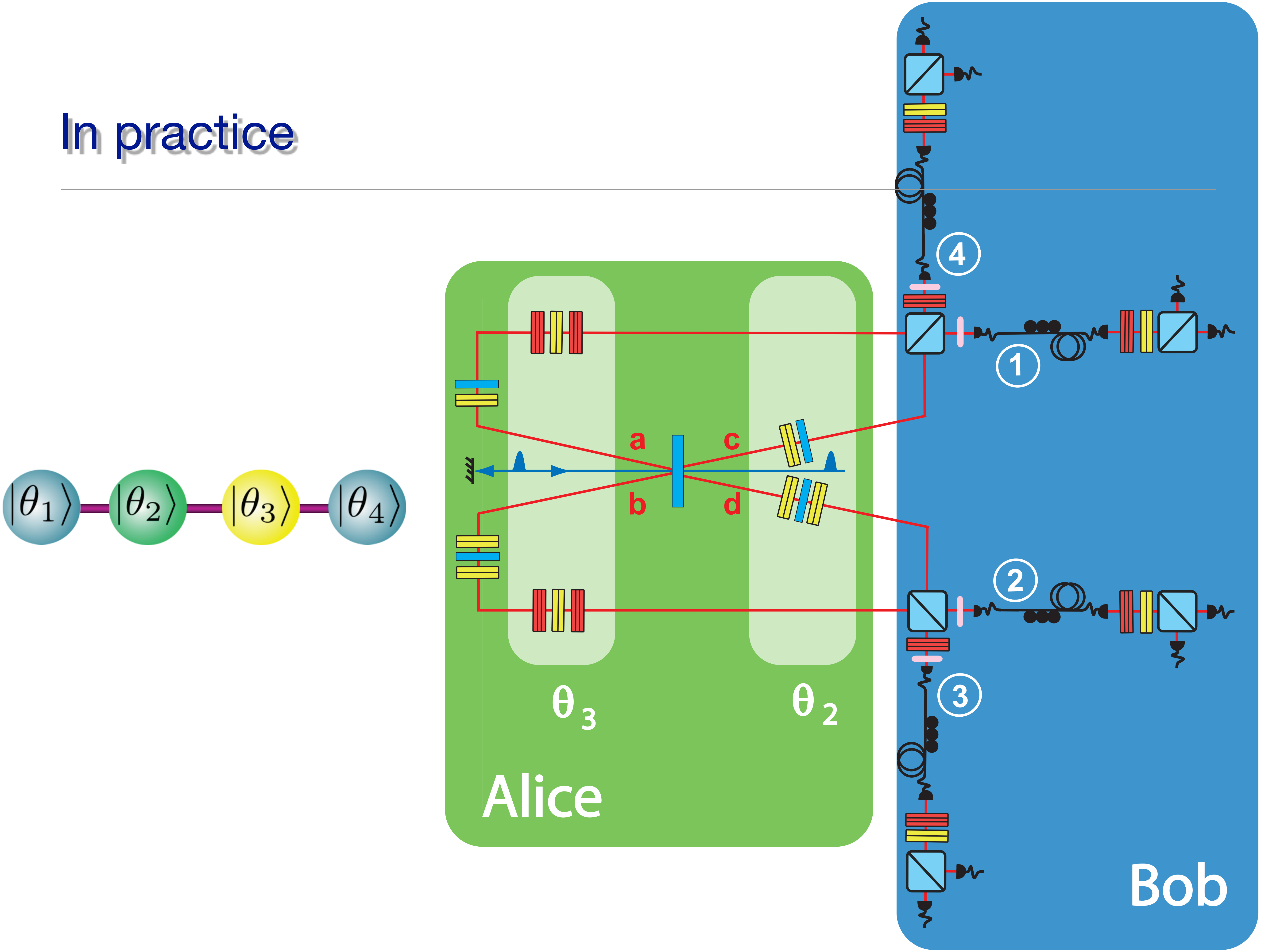


Verifiable Outsourced Computing



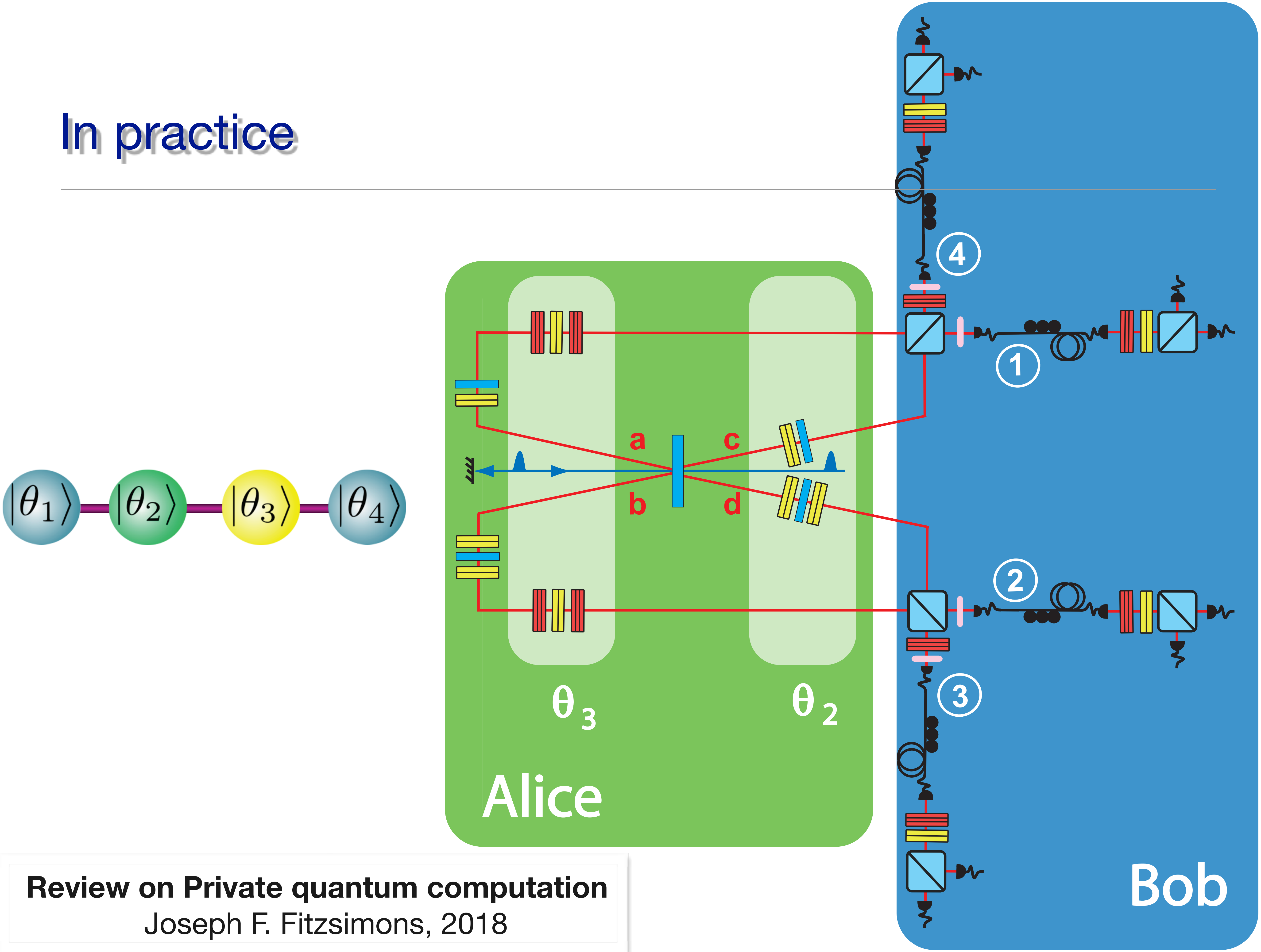
Verifiable Universal Blind Quantum Computing: QKD + Teleportation + Test

In practice



$|\theta_1\rangle$
$|\theta_2\rangle$
$|\theta_3\rangle$
$|\theta_4\rangle$
a
b
c
d
θ 3
θ 2
Alice
1
2
3
4
Bob

In practice

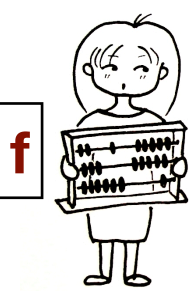


Review on Private quantum computation
Joseph F. Fitzsimons, 2018

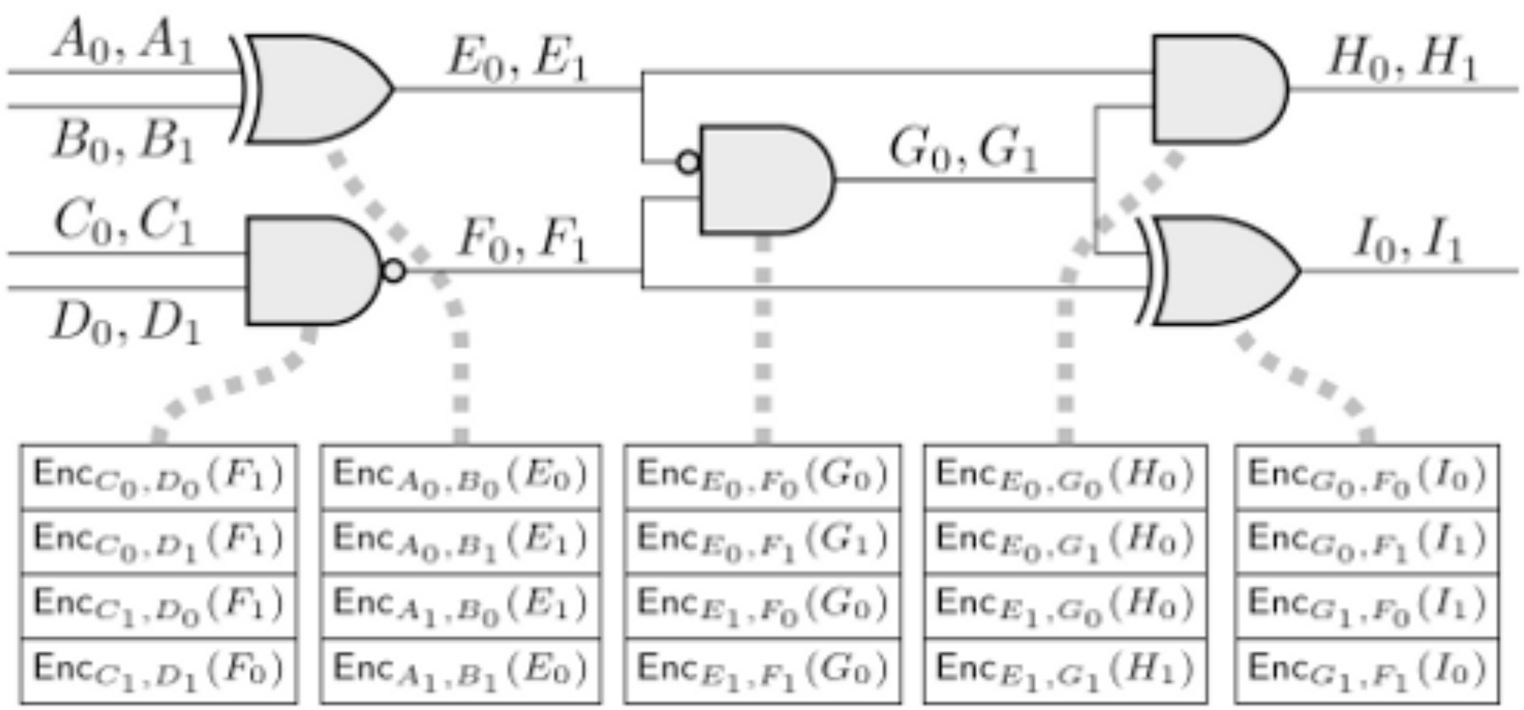
Yao Garbled Circuit - Secure 2-party Computing

Secret input a

Garbled Program f



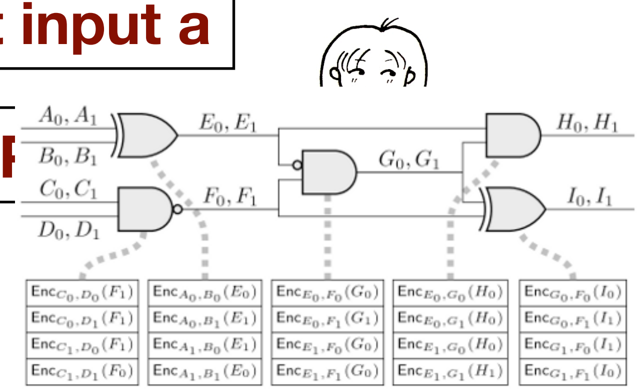
Yao Garbled Circuit - Secure 2-party Computing



Yao Garbled Circuit - Secure 2-party Computing

Secret input a

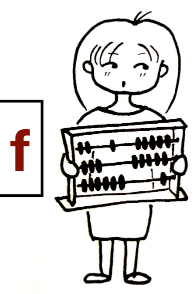
Garbled F

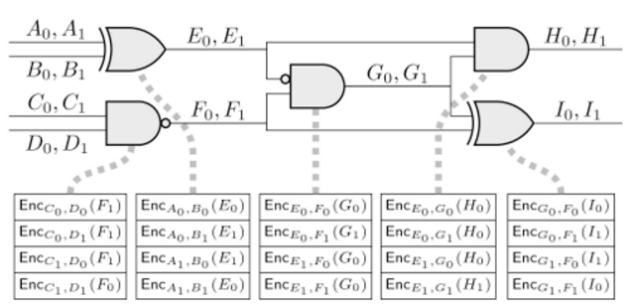


Yao Garbled Circuit - Secure 2-party Computing

Secret input a

Garbled Program f

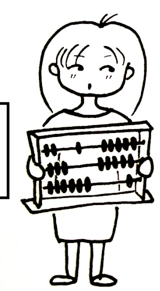


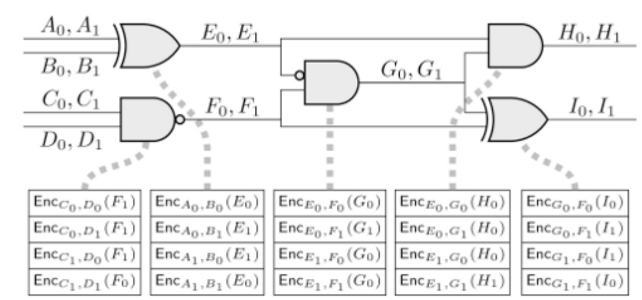


Yao Garbled Circuit - Secure 2-party Computing

Secret input a

Garbled Program f



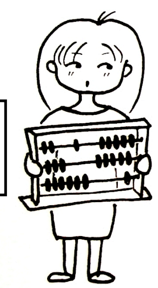


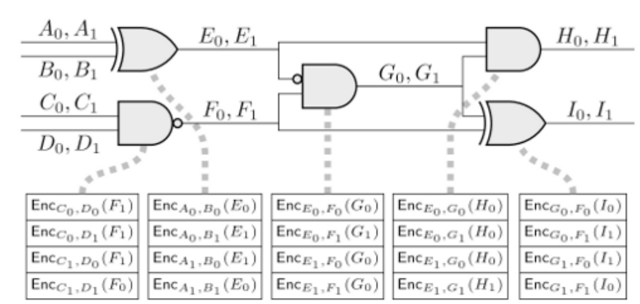
Insert secret input b
Evaluate f(a,b)

Yao Garbled Circuit - Secure 2-party Computing

Secret input a

Garbled Program f





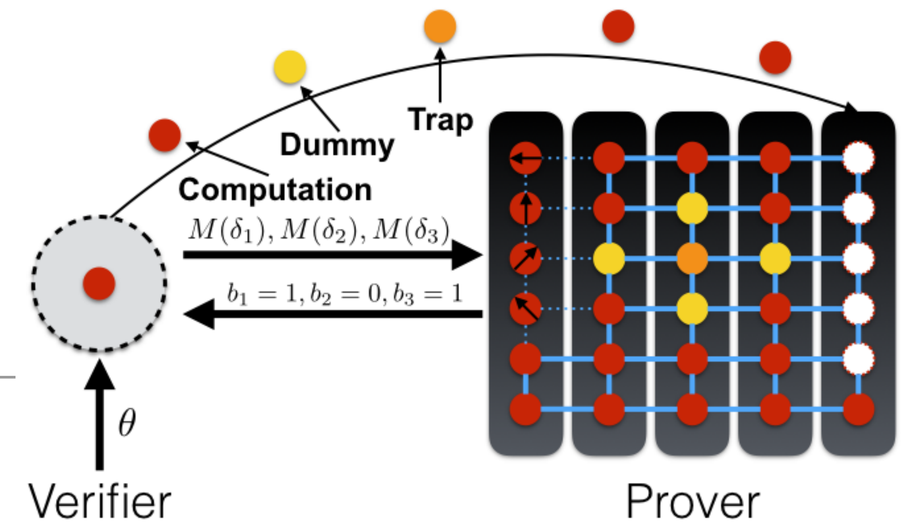
Insert secret input b
Evaluate f(a,b)

Computational Security

Requires OT

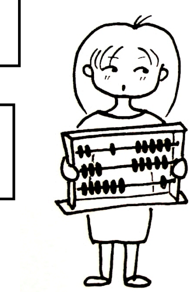
Honest but Curious Adversary

Verifiable Quantum Yao

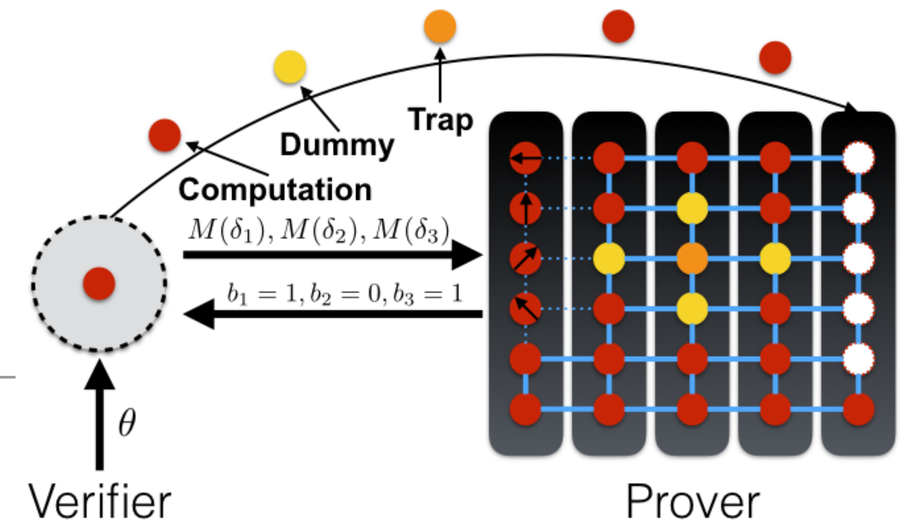


Secret input q_c

Garbled CP map

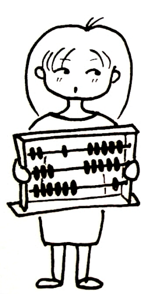


Verifiable Quantum Yao



Secret input q_c

Garbled CP map

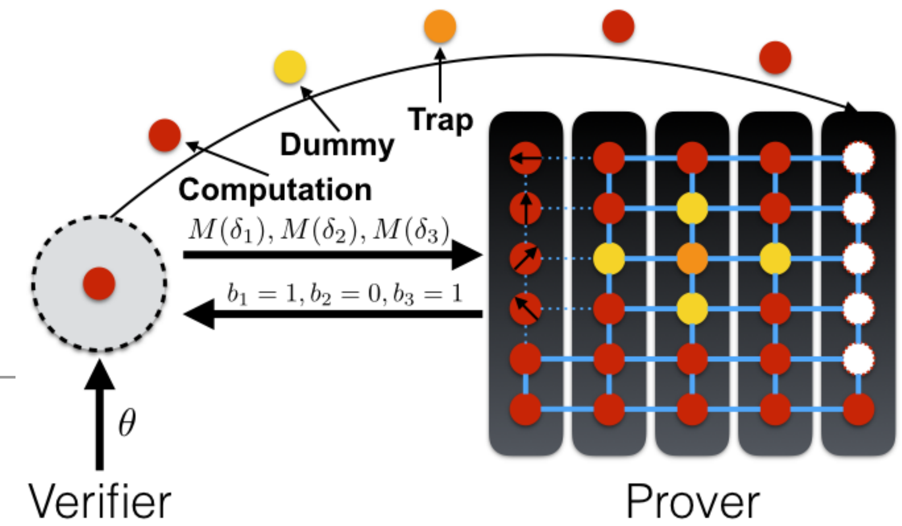


θ $\cdots$ θ'

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

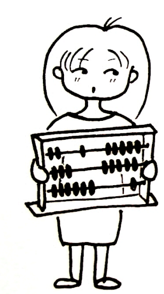
$$|0\rangle, |1\rangle$$

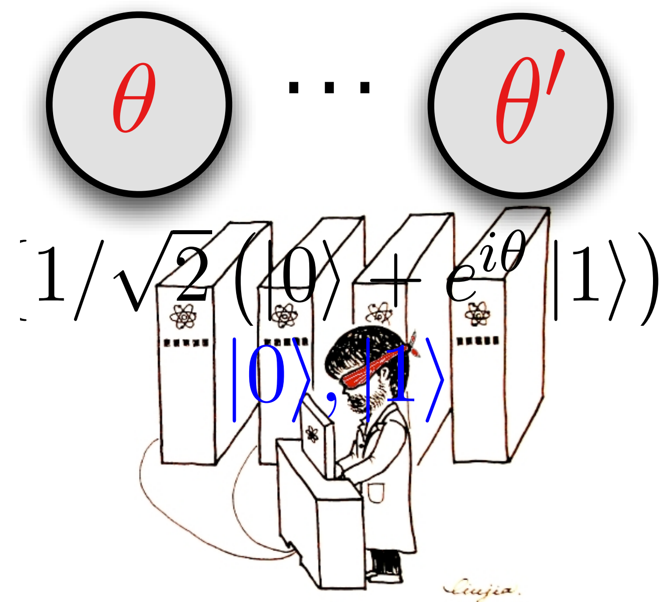
Verifiable Quantum Yao



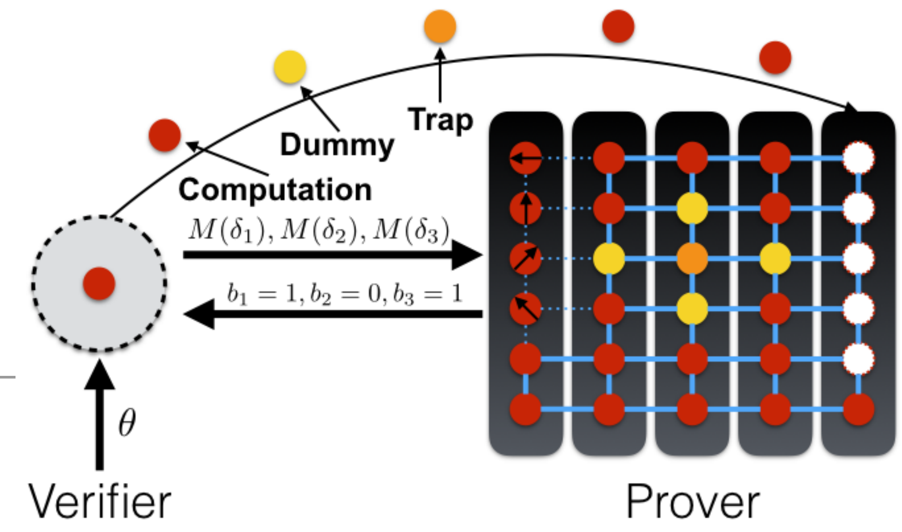
Secret input q_c

Garbled CP map



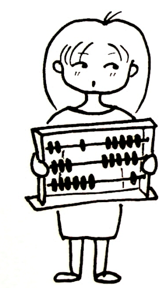


Verifiable Quantum Yao

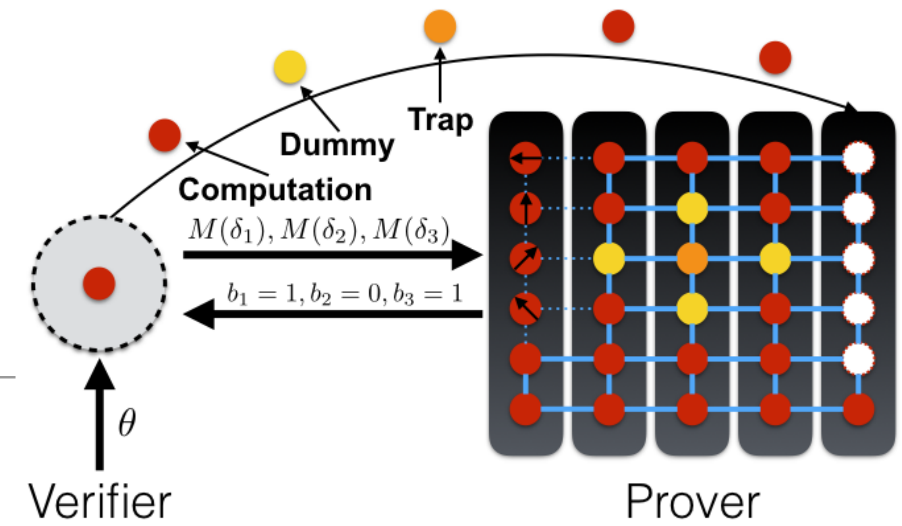


Secret input q_c

Garbled CP map

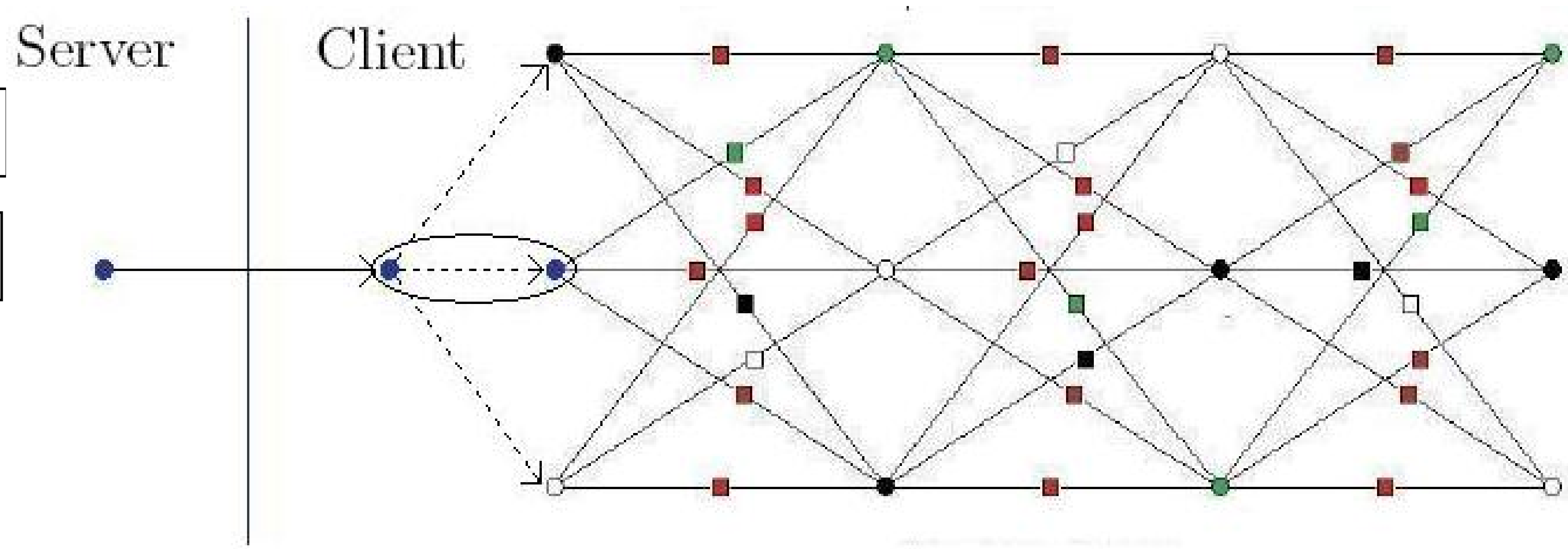


Verifiable Quantum Yao



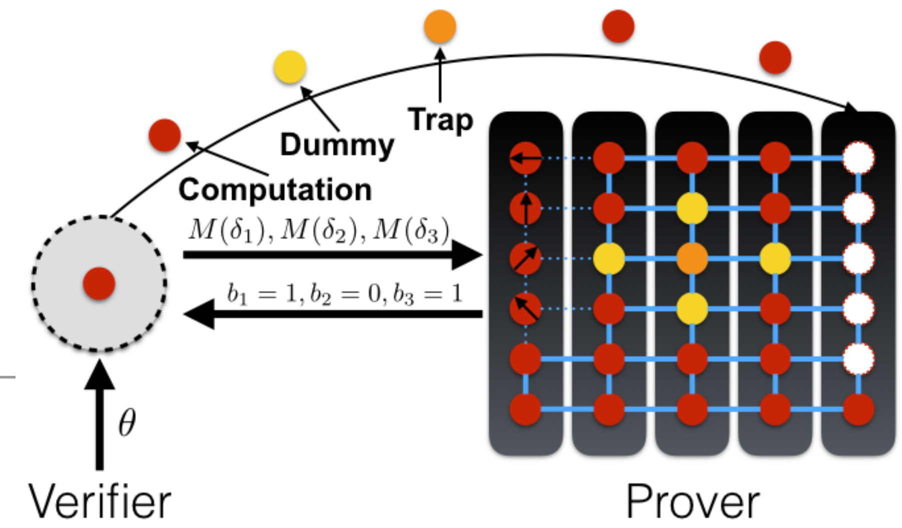
Secret input q_c

Garbled CP map



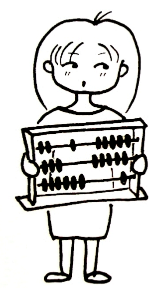
Server's input placed in DT(G) with correspoding trap-colouring

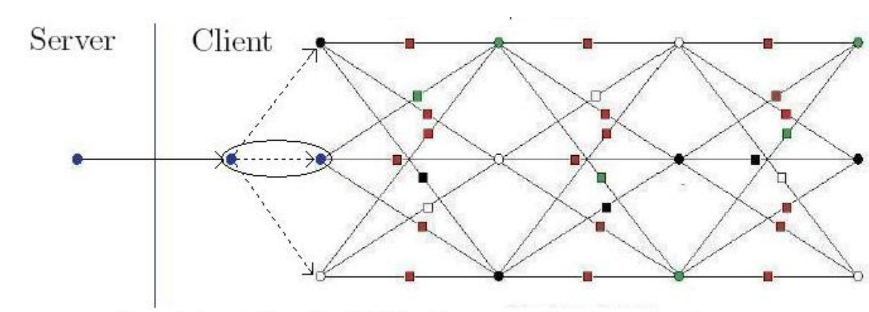
Verifiable Quantum Yao



Secret input q_c

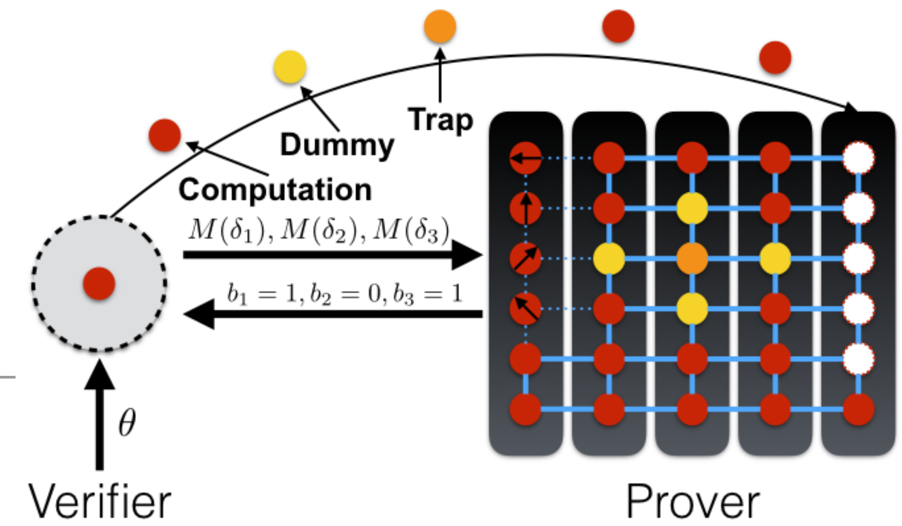
Garbled CP map





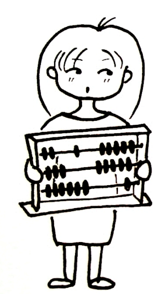
Server's input placed in DT(G) with correspoding trap-colouring

Verifiable Quantum Yao



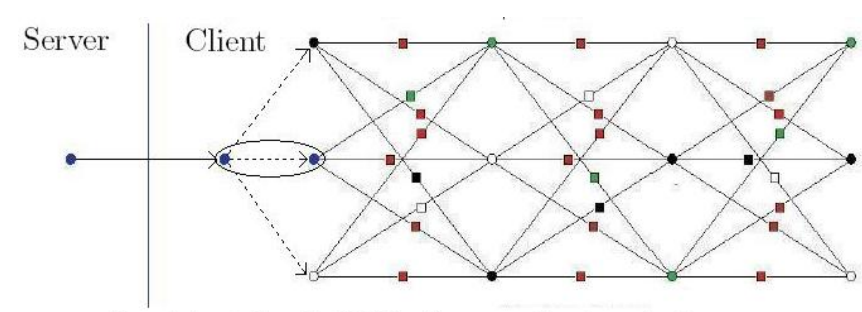
Secret input q_c

Garbled CP map



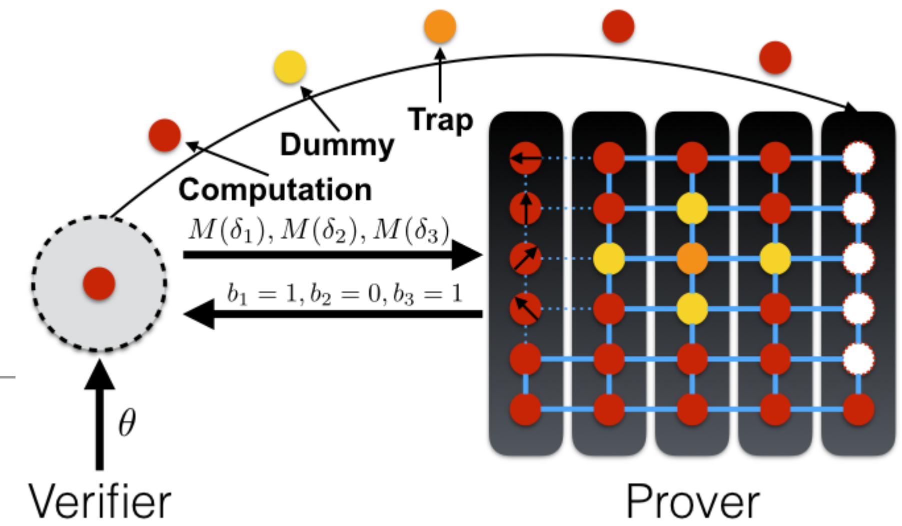
$r_{x,y} \in_R \{0,1\}$

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



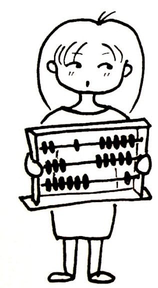
Server's input placed in DT(G) with correspoding trap-colouring

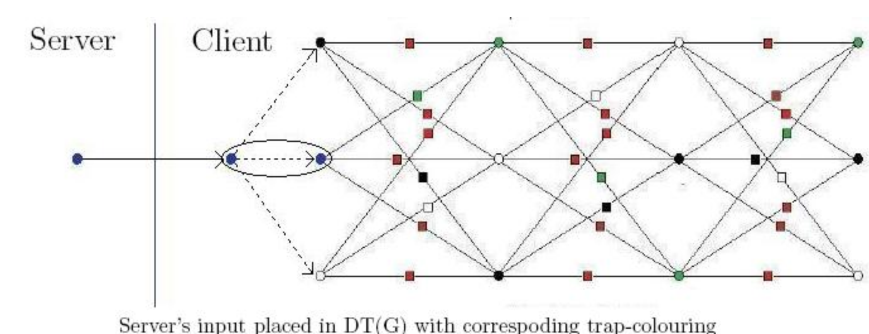
Verifiable Quantum Yao



Secret input q_c

Garbled CP map



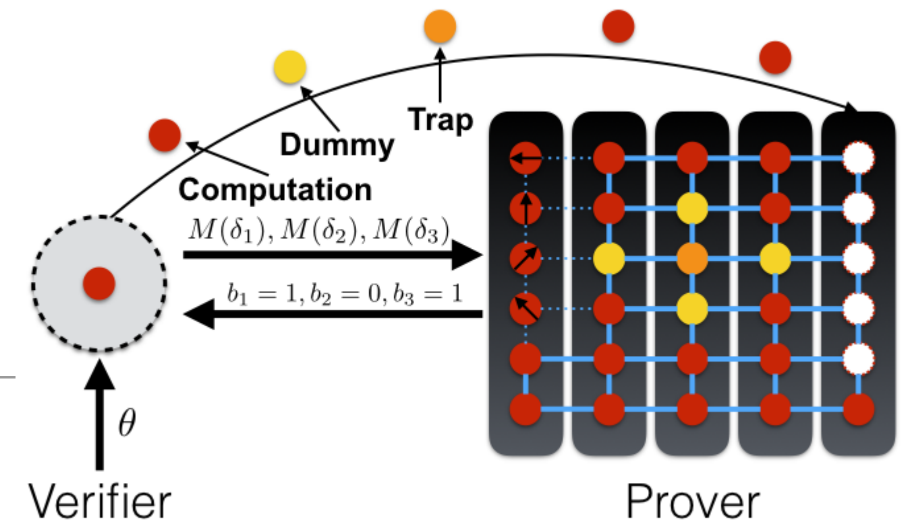


$r_{x,y} \in_R \{0,1\}$

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

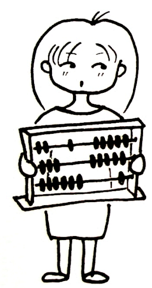
Insert secret input q_c
Evaluate CP(q_c,q_s)

Verifiable Quantum Yao

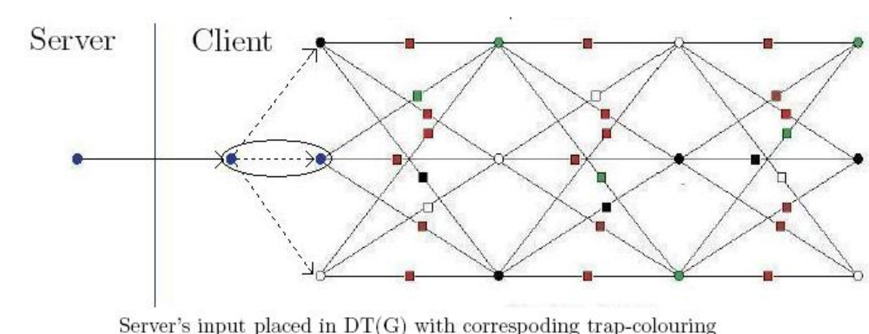


Secret input q_c

Garbled CP map



$$r_{x,y} \in_R \{0,1\}$$
$$\delta_{x,y} = \phi'_{x,y} + \theta_{x,y} + \pi r_{x,y}$$



Insert secret input q_c
Evaluate CP(q_c,q_s)

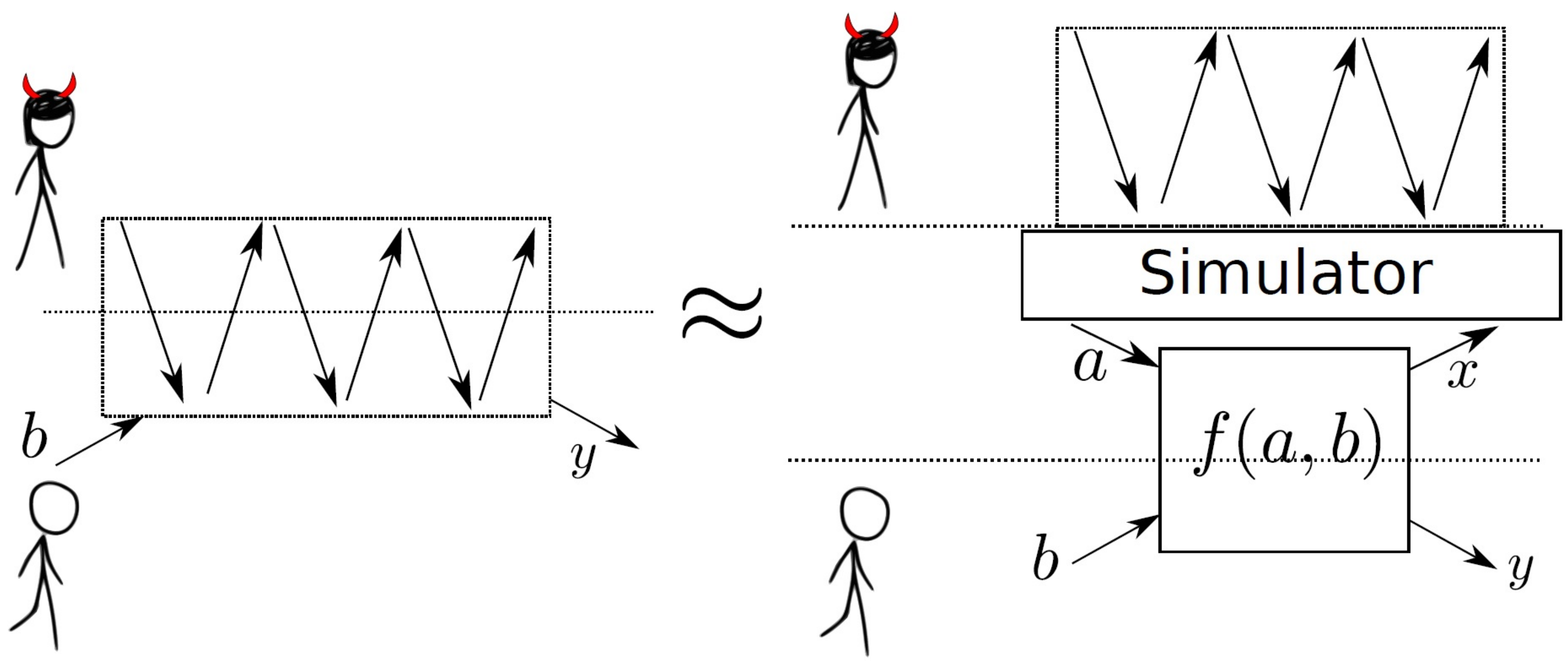
Unconditional Security

no OT is needed

Quantum Honest but Curious Client

Requires classical O(N) online communication

Security Model



The adversary cannot distinguish between the actual protocol

or

interacting with the ideal functionality and the simulator

Quantum Adversaries

Malicious Server: Can deviate in any possible quantum way

Specious Client: Can deviate in any way, provided that for every step of the protocol they can reproduce the honest state of that step by acting only on their system. i.e. can pass an audit at all steps of the protocol.

Quantum Adversaries

Malicious Server: Can deviate in any possible quantum way

Specious Client: Can deviate in any way, provided that for every step of the protocol they can reproduce the honest state of that step by acting only on their system. i.e. can pass an audit at all steps of the protocol.

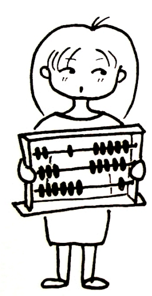
Formally, an adversary $\mathcal{A}$ is ϵ-specious if there exists a family of CP-maps $\mathcal{T}_i : L(\tilde{\mathcal{A}}_i) \to L(\mathcal{A}_i)$ one for each step i of the protocol such that for *every* allowed input ρ_{in}

$$\Delta(\mathcal{T}_i \otimes \mathbb{I} \cdot \tilde{\rho}_i(\tilde{A}, \rho_{in}), \rho_i(\rho_{in})) \leq \epsilon$$

where $\rho_i(\rho_{in})$ is the honest state at step i and $\tilde{\rho}_i(\tilde{A}, \rho_{in})$ the state of the real (deviated) protocol at the same step.

Malicious Client with Cut and Choose

1-way Q communication
Client is QKD
Linear Q + Poly C overhead

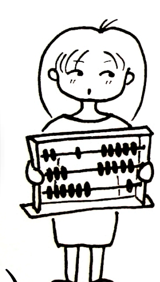


Malicious Client with Cut and Choose

com(r), com(θ),
com(δ),
com(δ_{input}),
com(keys for P_2),
com(position of
traps in final)

1-way Q communication
Client is QKD
Linear Q + Poly C overhead

θ $\cdots$ θ'



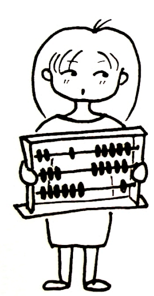
$1/\sqrt{2}\left(|0\rangle + e^{i\theta}|1\rangle\right)$

$|0\rangle, |1\rangle$

commitment to *S* version of circuit

Malicious Client with Cut and Choose

1-way Q communication
Client is QKD
Linear Q + Poly C overhead



com(r), com(θ), com(δ), com(δ_{input}), com(keys for P_2), com(position of traps in final)

θ $\cdots$ θ'

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

$$|0\rangle, |1\rangle$$

commitment to *S* version of

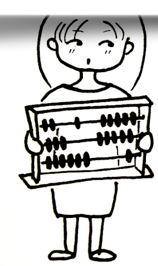
Kashefi Music Wallden 17

Malicious Client with Cut and Choose

1-way Q communication
Client is QKD
Linear Q + Poly C overhead

com(r), com(θ),
com(δ),
com(δ_{input}),
com(keys for P_2),
com(position of
traps in final)

coin tossing protocol to decide the evaluation graph



θ $\cdots$ θ'

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

$$|0\rangle, |1\rangle$$

commitment to *S* version of

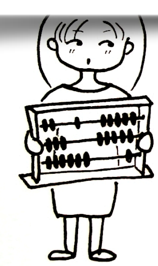
Kashefi Music Wallden 17

Malicious Client with Cut and Choose

1-way Q communication
Client is QKD
Linear Q + Poly C overhead

$\mathrm{com(r)}, \mathrm{com}(\theta),$
$\mathrm{com}(\delta),$
$\mathrm{com}(\delta_{input}),$
$\mathrm{com(keys\ for\ P_2)},$
$\mathrm{com(position\ of}$
$\mathrm{traps\ in\ final)}$

coin tossing protocol to decide the evaluation graph



$\theta \quad \cdots \quad \theta'$

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

$|0\rangle, |1\rangle$

Server checks Client

commitment to *S* version of

Kashefi Music Wallden 17

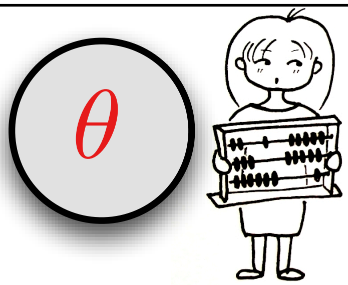
Malicious Client and Server with Cut and Choose

- Client chooses values for circuits
- Client creates commitments
- OT protocols => Server gets his inputs
- Client prepares and sends qubits
- Client sends commitments
- Coin-tossing protocol => Eval graph chosen
- Client decommits for the check graphs
- Server performs consistency checks
- Server run VUBQC protocol
- Key exchange protocol

Secure Multi Party Quantum Computing

Secret input q_1

Garbled her part of the CP map



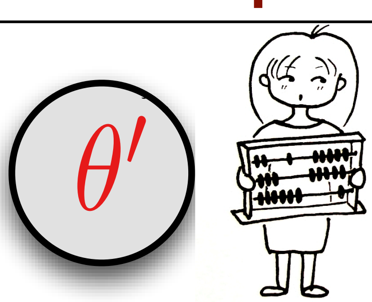
.

.

.

Secret input q_n

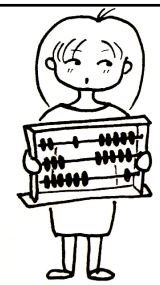
Garbled her part of the CP map



Secure Multi Party Quantum Computing

Secret input q_1

Garbled her part of the CP map



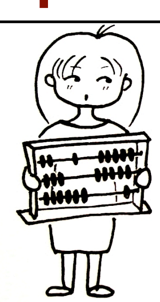
.

.

.

Secret input q_n

Garbled her part of the CP map



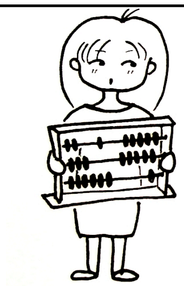
θ

θ'

Secure Multi Party Quantum Computing

Secret input q_1

Garbled her part of the CP map



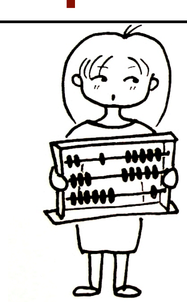
.

.

.

Secret input q_n

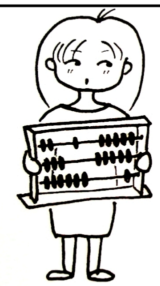
Garbled her part of the CP map



Secure Multi Party Quantum Computing

Secret input q_1

Garbled her part of the CP map



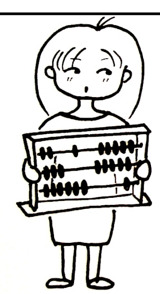
.

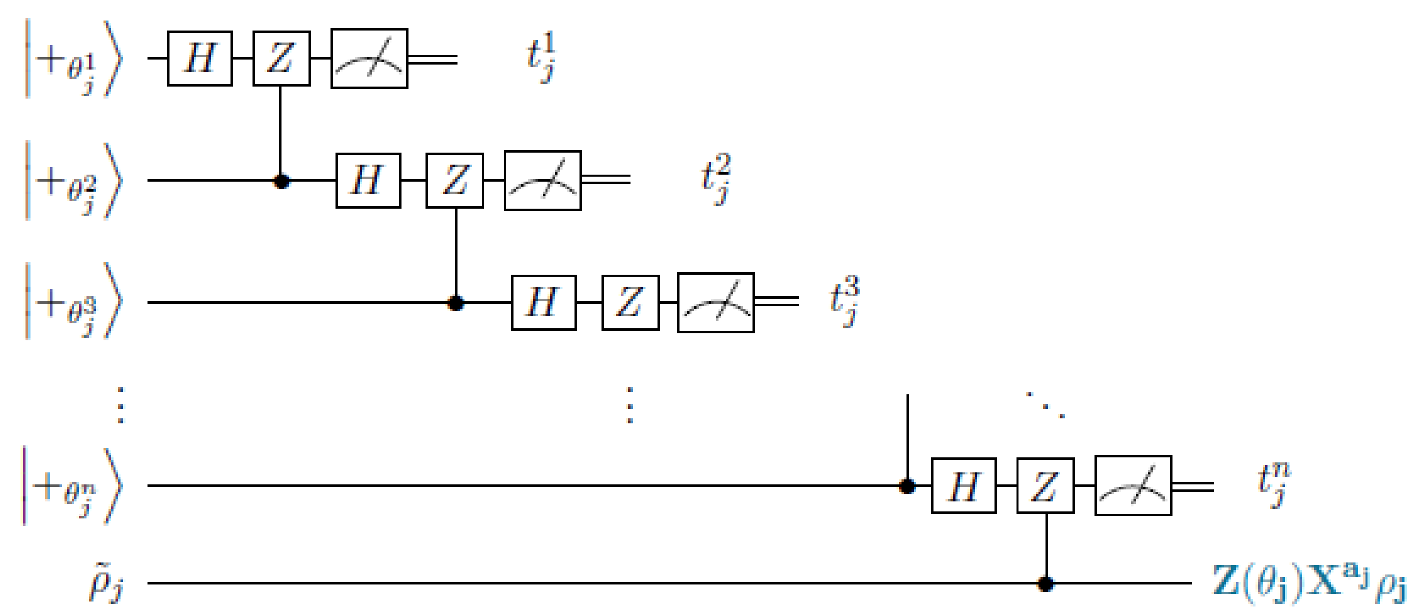
.

.

Secret input q_n

Garbled her part of the CP map



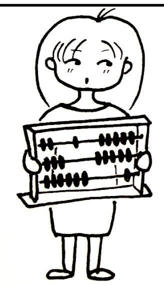


$$\theta_j = \theta_j^j + \sum_{k=1,k\neq j}^{n} (-1)^{\bigoplus_{i=k}^{n} t_j^i}\, \theta_j^k$$

Secure Multi Party Quantum Computing

Secret input q_1

Garbled her part of the CP map



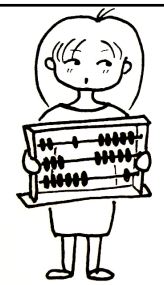
.

.

.

Secret input q_n

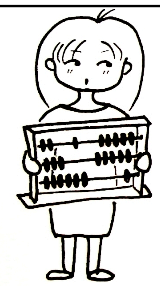
Garbled her part of the CP map



Secure Multi Party Quantum Computing

Secret input q_1

Garbled her part of the CP map



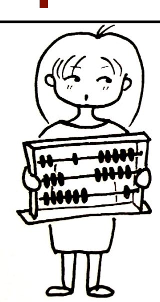
.

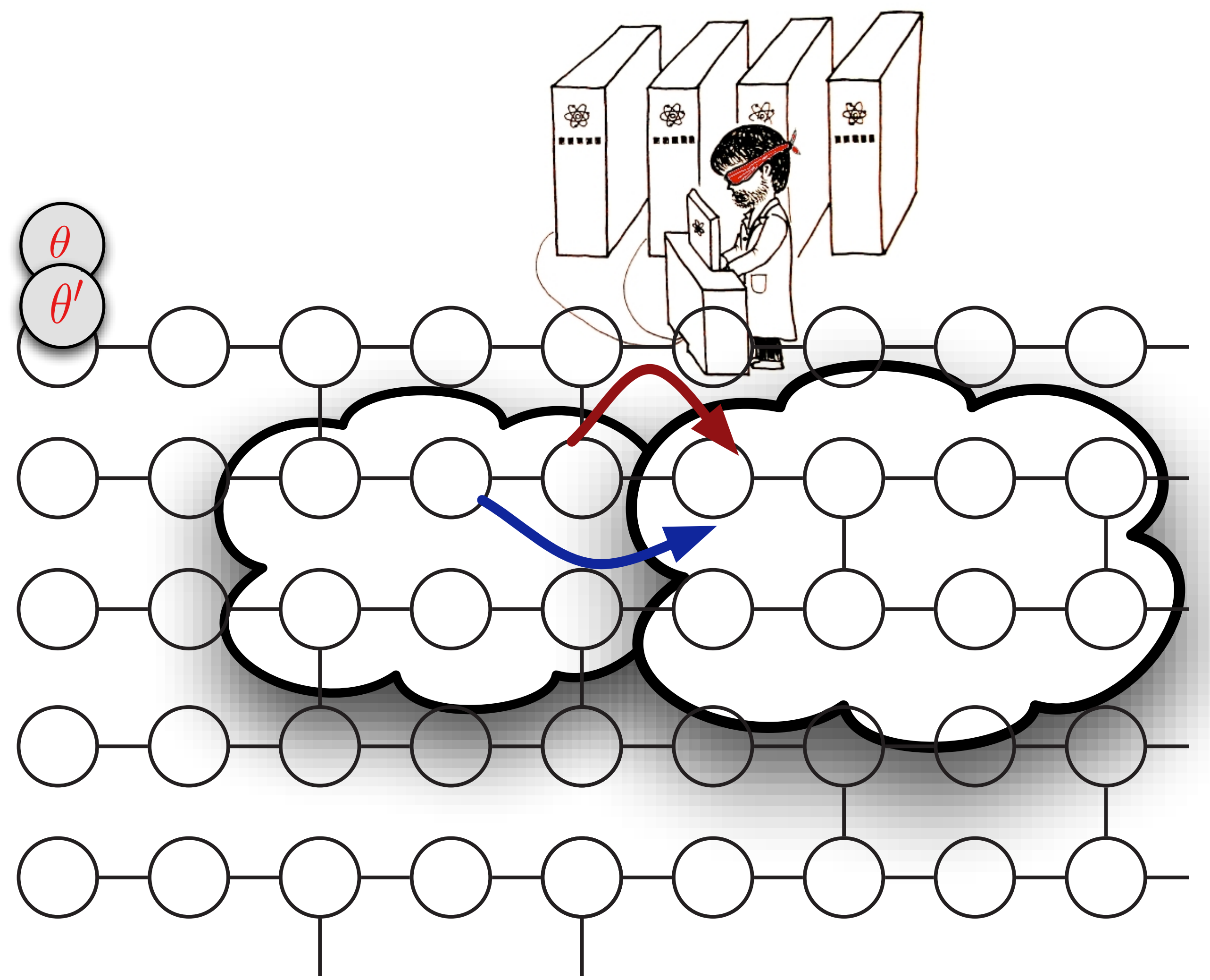
.

.

Secret input q_n

Garbled her part of the CP map

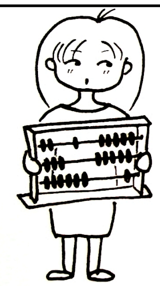




Secure Multi Party Quantum Computing

Secret input q_1

Garbled her part of the CP map

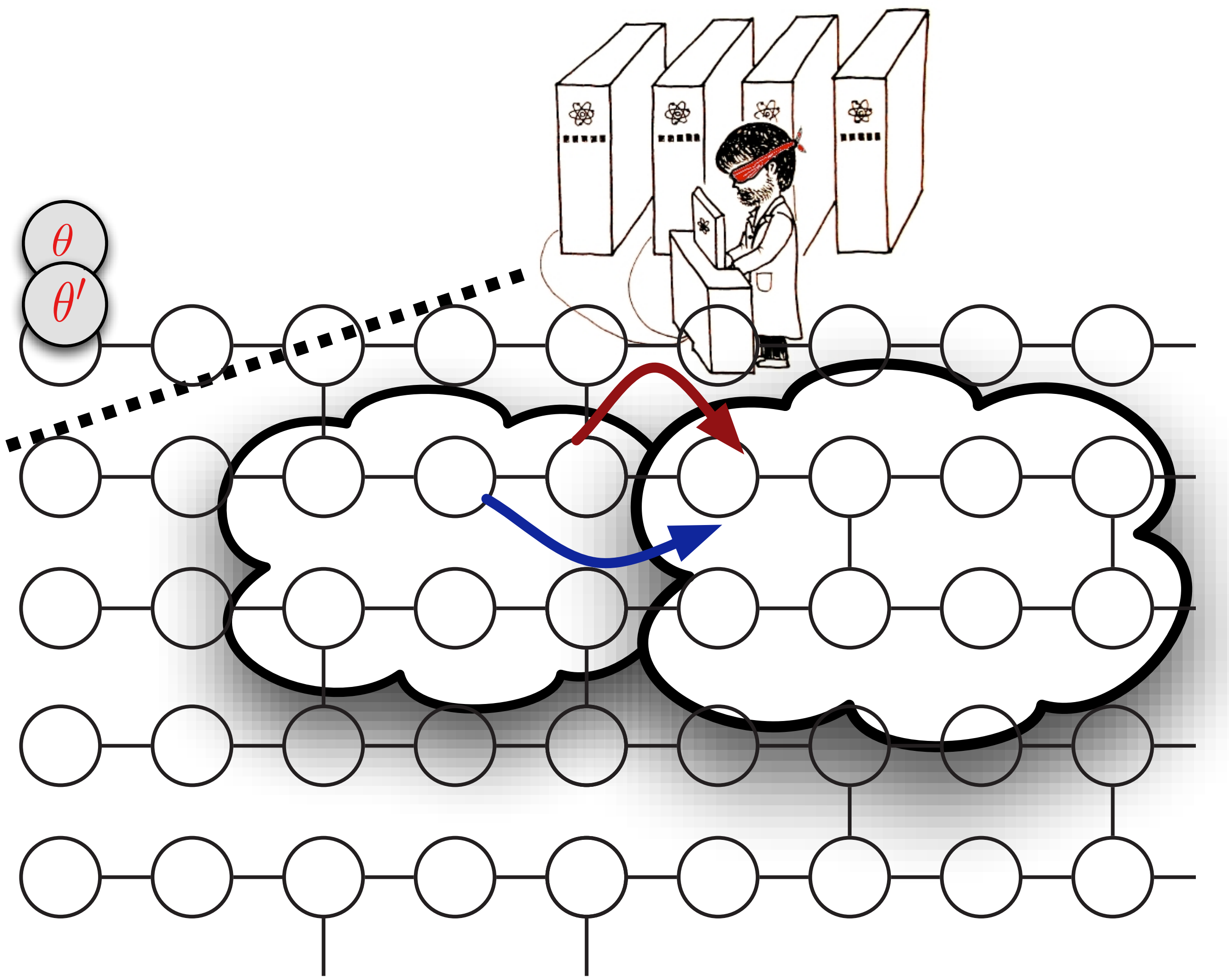


.

.

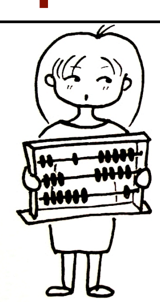
.

$$\delta_j = \phi'_j + \pi \bigoplus_{k=1}^{n} r_j^k + \theta_j$$

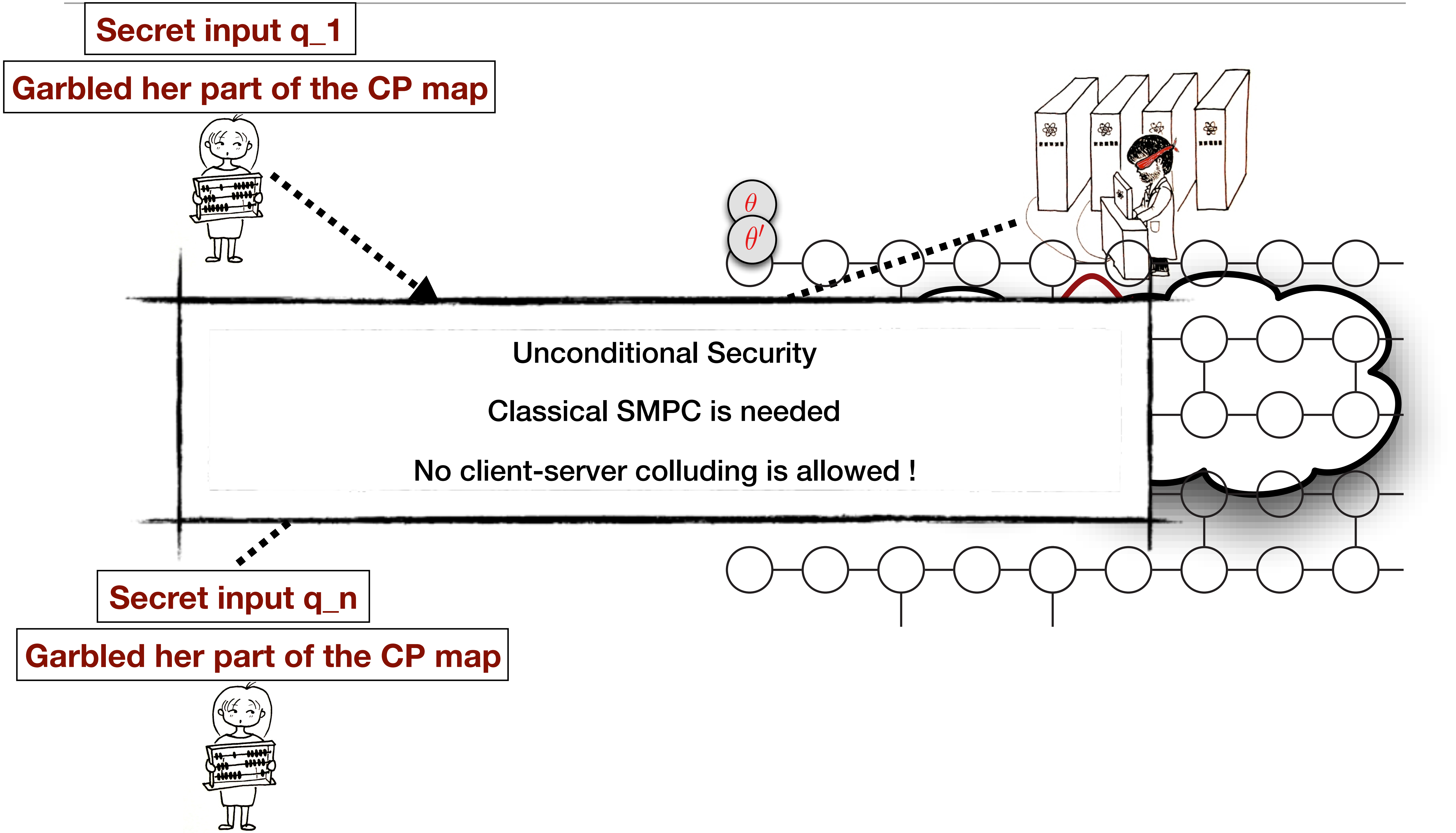


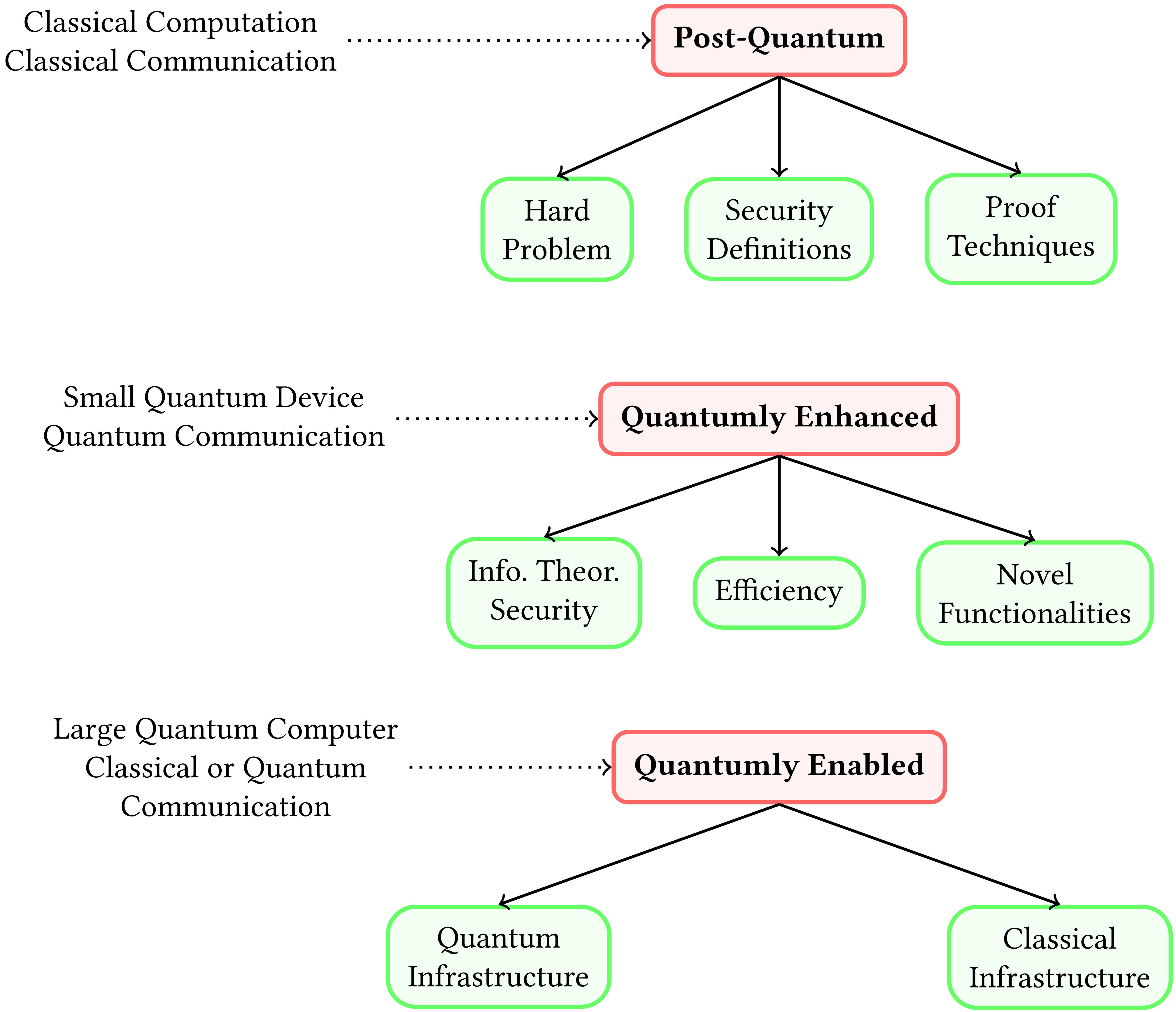
Secret input q_n

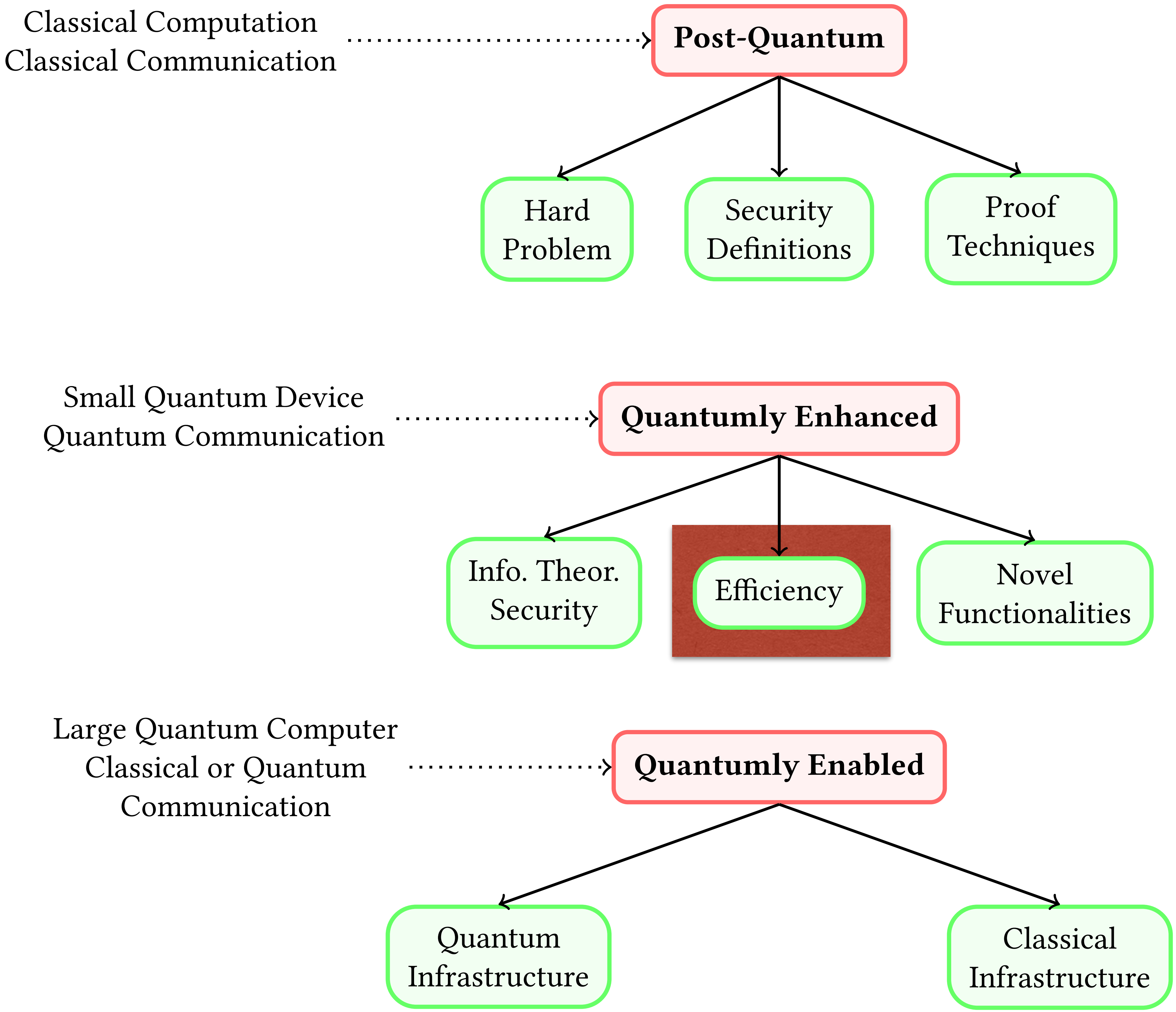
Garbled her part of the CP map



Secure Multi Party Quantum Computing




Classical Computation
Classical Communication
Post-Quantum
Hard Problem
Security Definitions
Proof Techniques
Small Quantum Device
Quantum Communication
Quantumly Enhanced
Info. Theor. Security
Efficiency
Novel Functionalities
Large Quantum Computer
Classical or Quantum Communication
Quantumly Enabled
Quantum Infrastructure
Classical Infrastructure


Classical Computation
Classical Communication
Post-Quantum
Hard Problem
Security Definitions
Proof Techniques
Small Quantum Device
Quantum Communication
Quantumly Enhanced
Info. Theor. Security
Efficiency
Novel Functionalities
Large Quantum Computer
Classical or Quantum Communication
Quantumly Enabled
Quantum Infrastructure
Classical Infrastructure

Practical Classical SMPC

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

Bogetoftx- Christensen-Damgardz-Geislerz-Jakobsen-Krigaard-Nielsen-Nielseny-Pagter-Schwartzbachz-Toftyy08

Recently: Efficient (low communication) computational SMPC

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

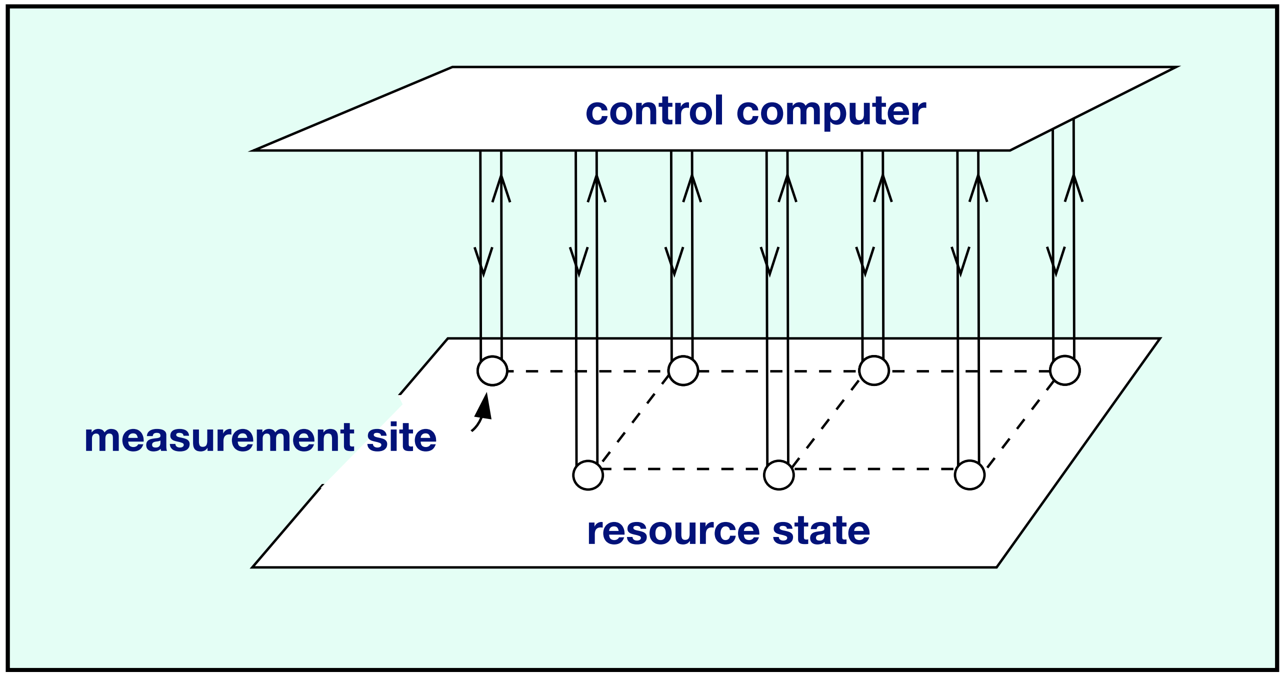
easy

Linear Verifiable Secret Sharing

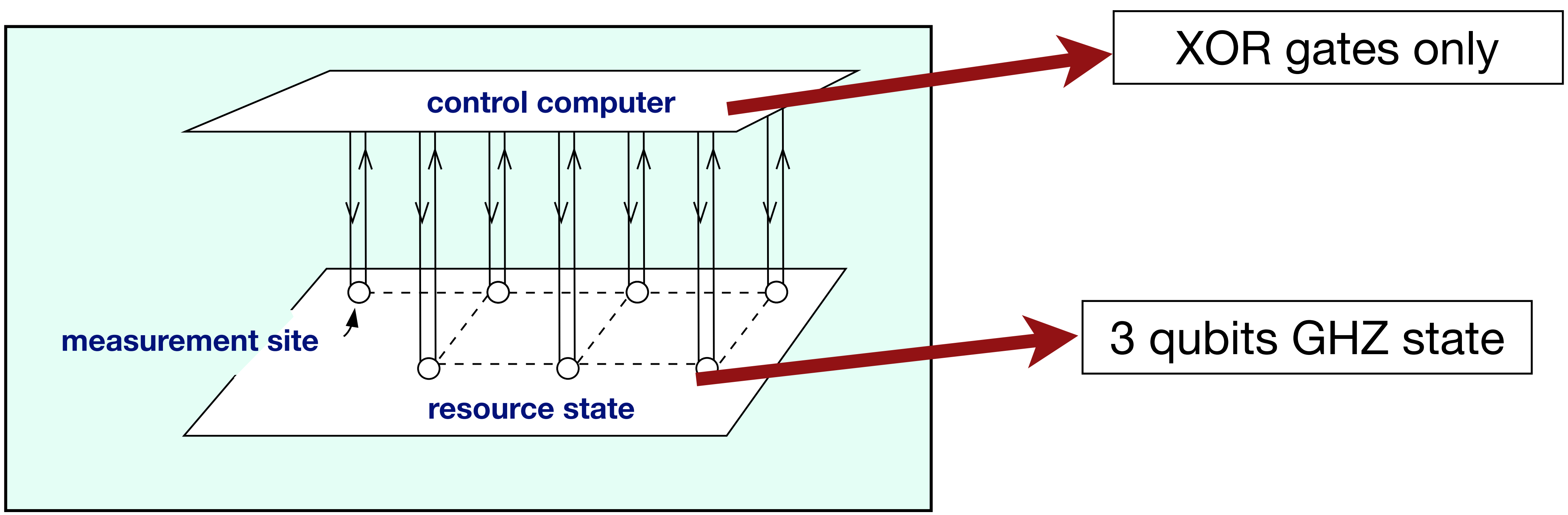
hard

costly but offline FHE

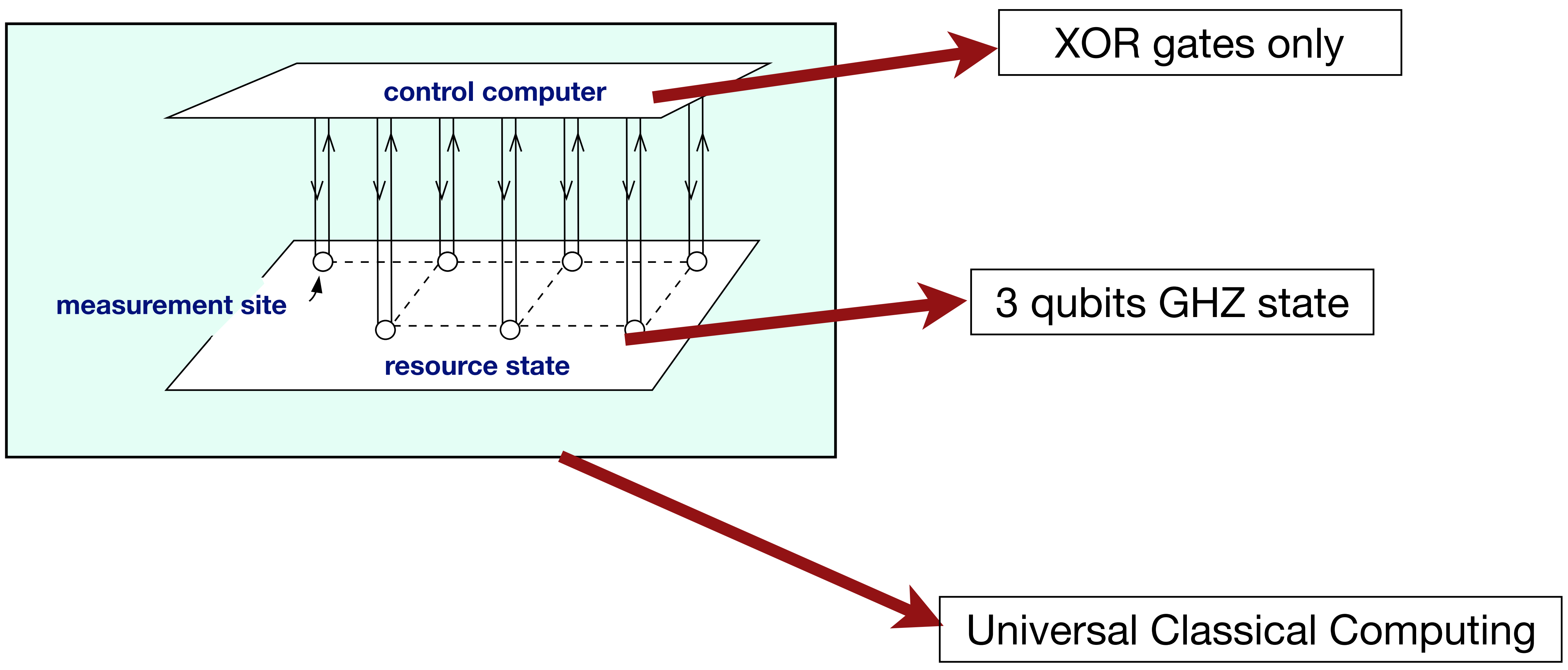
From Linear to Non-linear - MBQC



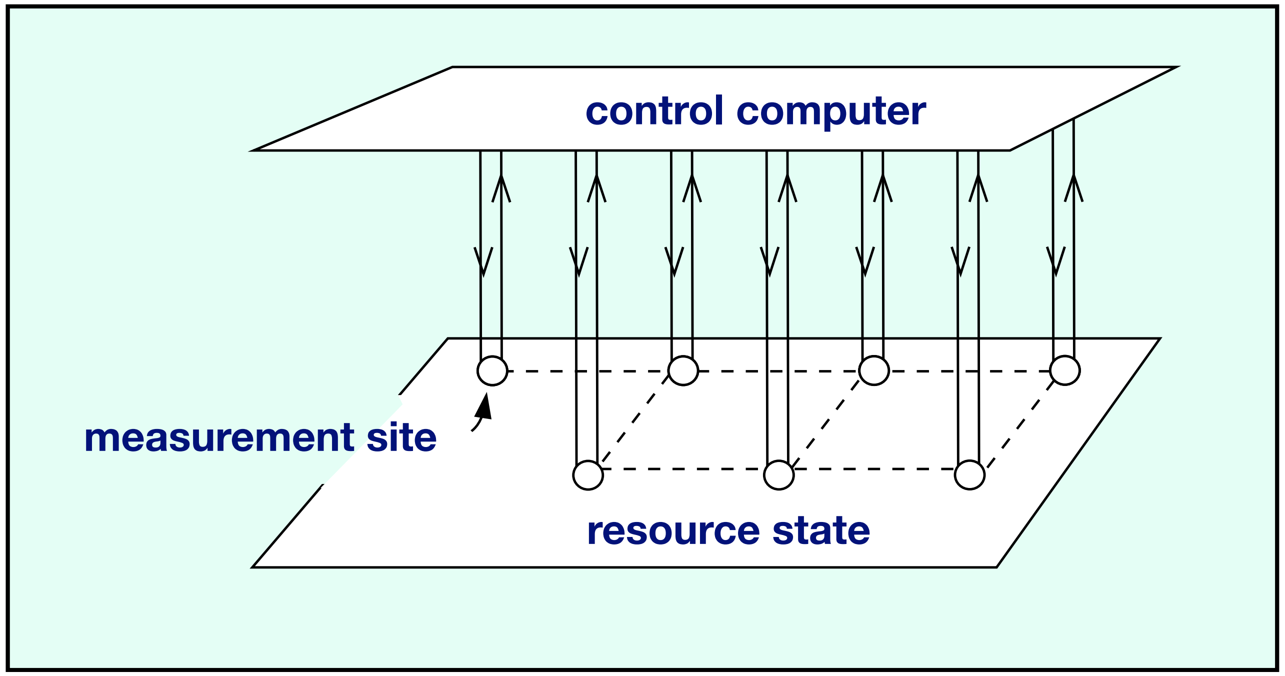
From Linear to Non-linear - MBQC



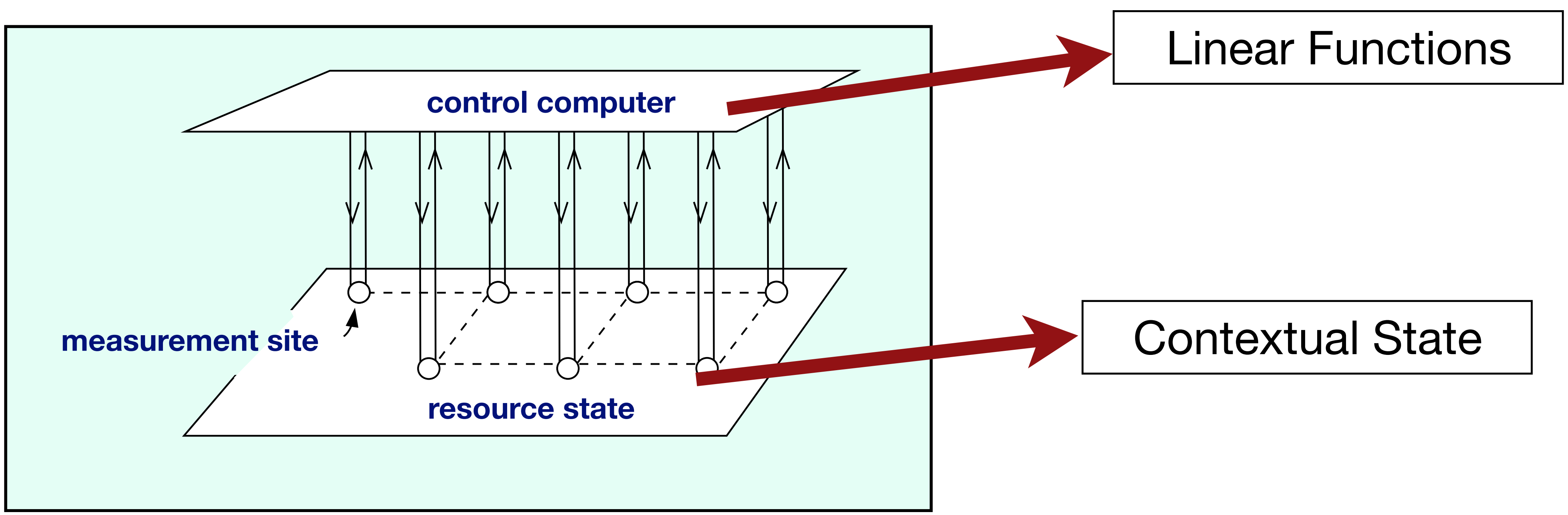
From Linear to Non-linear - MBQC



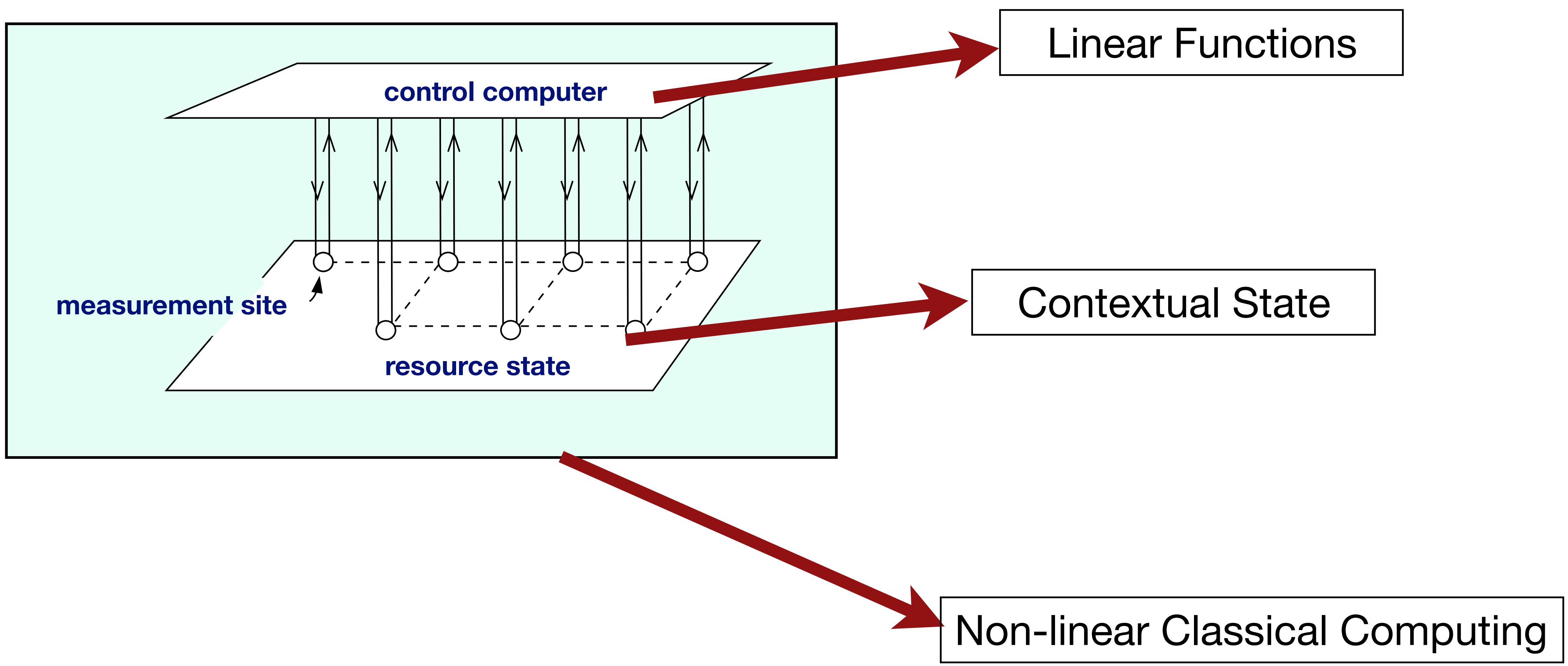
From Linear to Non-linear - MBQC



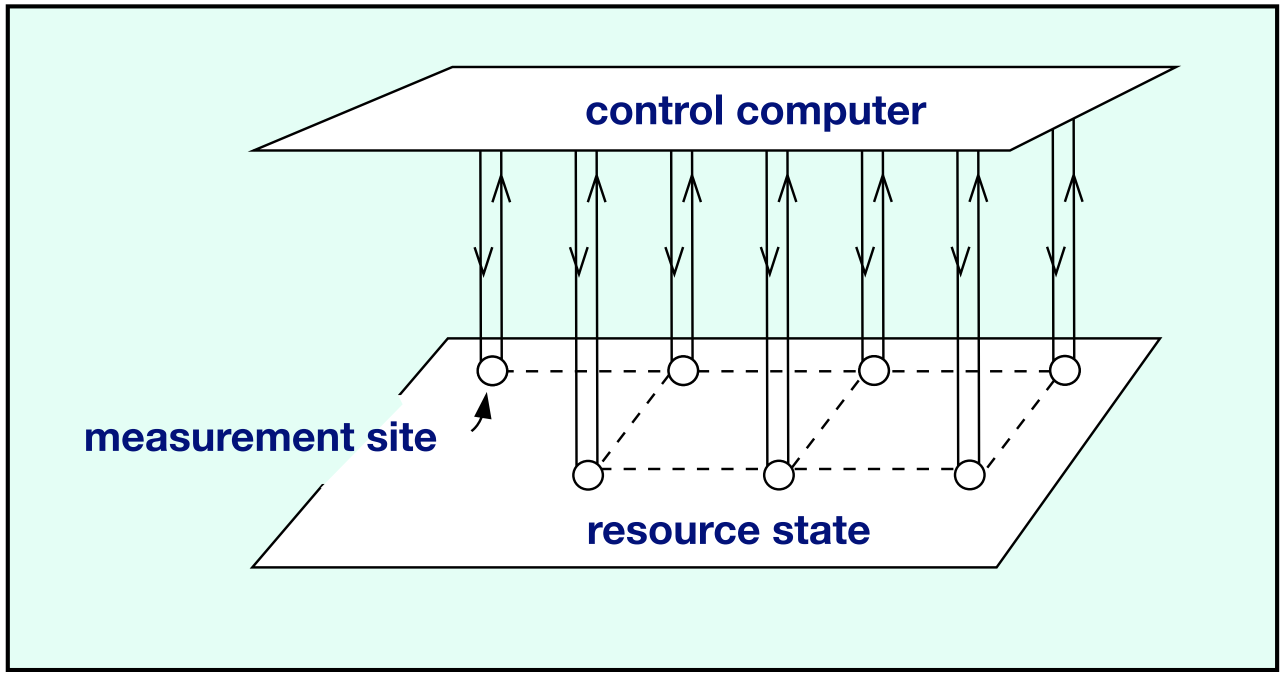
From Linear to Non-linear - MBQC



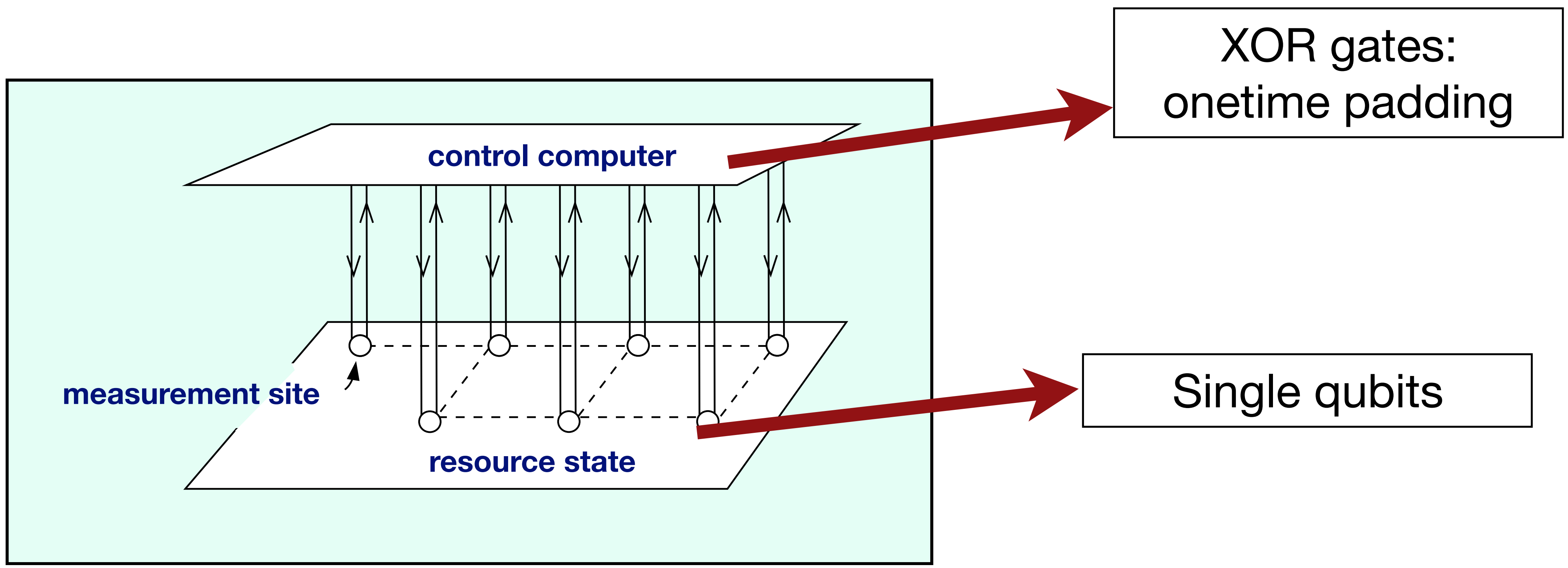
From Linear to Non-linear - MBQC



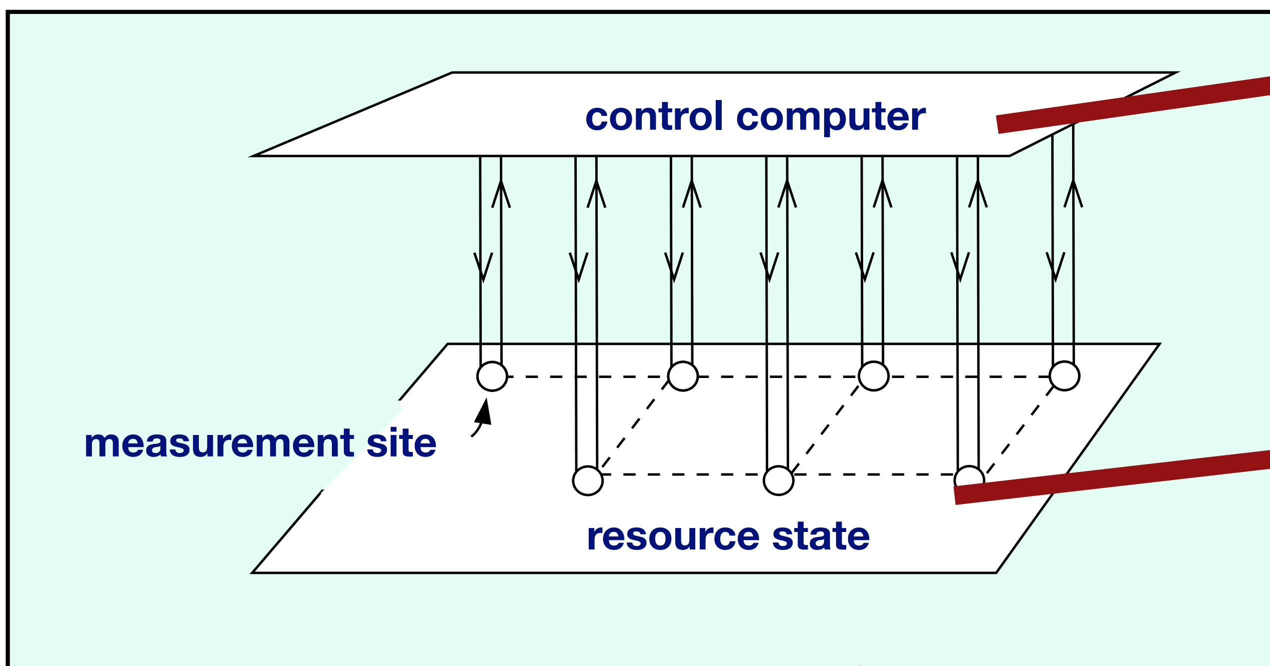
From Linear to Non-linear - Secure Computing



From Linear to Non-linear - Secure Computing



From Linear to Non-linear - Secure Computing



XOR gates:
onetime padding

Single qubits

Secure NAND

Restricted XOR Client

No classical protocol, with XOR client can securely delegate deterministic computation of NAND to a server.

Dunjko, Kapourniotis, Kashefi, arXiv:1405.4558, 2014

Restricted XOR Client

No classical protocol, with XOR client can securely delegate deterministic computation of NAND to a server.

Client's encoding: $C_1(a, b, \overrightarrow{x})$

Dunjko, Kapourniotis, Kashefi, arXiv:1405.4558, 2014

Restricted XOR Client

No classical protocol, with XOR client can securely delegate deterministic computation of NAND to a server.

Client's encoding: $C_1(\underbrace{a, b}_{\text{input}}, \overset{\text{random}}{\overrightarrow{x}})$ **XOR computable function independent of the input**

Dunjko, Kapourniotis, Kashefi, arXiv:1405.4558, 2014

Restricted XOR Client

No classical protocol, with XOR client can securely delegate deterministic computation of NAND to a server.

Client's encoding: $C_1(\underbrace{a, b}_{\text{input}}, \overbrace{\overrightarrow{x}}^{\text{random}})$ **XOR computable function independent of the input**

Server's computation: $S(C_1(a, b, \overrightarrow{x}))$

Dunjko, Kapourniotis, Kashefi, arXiv:1405.4558, 2014

Restricted XOR Client

No classical protocol, with XOR client can securely delegate deterministic computation of NAND to a server.

Client's encoding: $C_1(\underbrace{a, b}_{\text{input}}, \overbrace{\overrightarrow{x}}^{\text{random}})$ **XOR computable function independent of the input**

Server's computation: $S(C_1(a, b, \overrightarrow{x}))$

Client's decoding: $C_2(a, b, \overrightarrow{x}, S(C_1(a, b, \overrightarrow{x}))) = NAND(a, b)$ **XOR computable function**

Dunjko, Kapourniotis, Kashefi, arXiv:1405.4558, 2014

Restricted XOR Client

No classical protocol, with XOR client can securely delegate deterministic computation of NAND to a server.

Client's encoding: $\underbrace{C_1(a, b}_{\text{input}}, \overbrace{\overrightarrow{x}}^{\text{random}})$ **XOR computable function independent of the input**

Server's computation: $S(C_1(a, b, \overrightarrow{x}))$

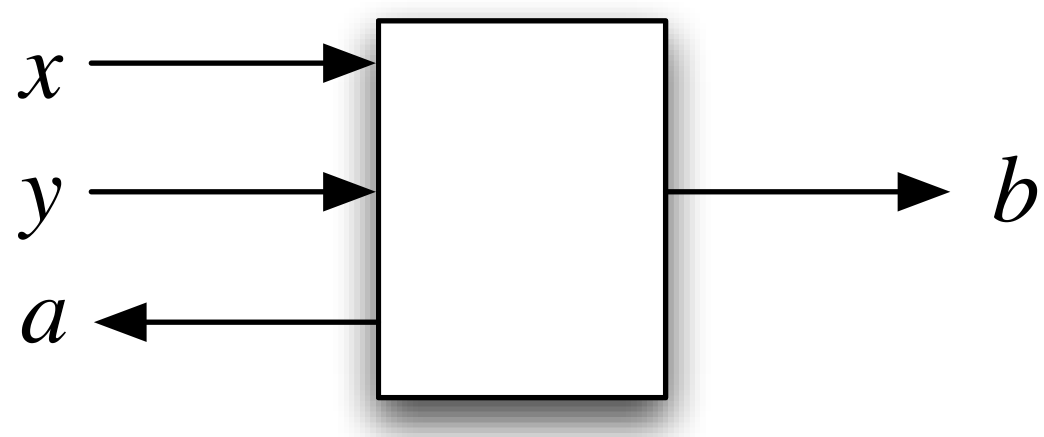
Client's decoding: $C_2(a, b, \overrightarrow{x}, \underbrace{S(C_1(a, b, \overrightarrow{x}))}_{\text{Constant}}) = NAND(a, b)$ **XOR computable function**

Dunjko, Kapourniotis, Kashefi, arXiv:1405.4558, 2014

Restricted XOR Client

No **quantum offline** protocol can delegate deterministically computation of NAND to a server while keeping the blindness

$$b = x.y + a$$



Quantum Communication

$$Z^r S^a S^b \left(S^\dagger\right)^{a \oplus b} |+\rangle \quad = \quad Z^r Z^{a \wedge b} |+\rangle$$

Quantum Communication

$$Z^r S^a S^b \left(S^\dagger\right)^{a\oplus b}|+\rangle = Z^r Z^{a\wedge b}|+\rangle$$

$$\begin{pmatrix}1 & 0\\ 0 & e^{ib\pi/2}\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & e^{ia\pi/2}\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & e^{-i(a\oplus b)\pi/2}\end{pmatrix}\begin{pmatrix}1\\ -1\end{pmatrix} = \begin{pmatrix}1 & 0\\ 0 & e^{-i(a\wedge b)\pi}\end{pmatrix}\begin{pmatrix}1\\ -1\end{pmatrix}$$

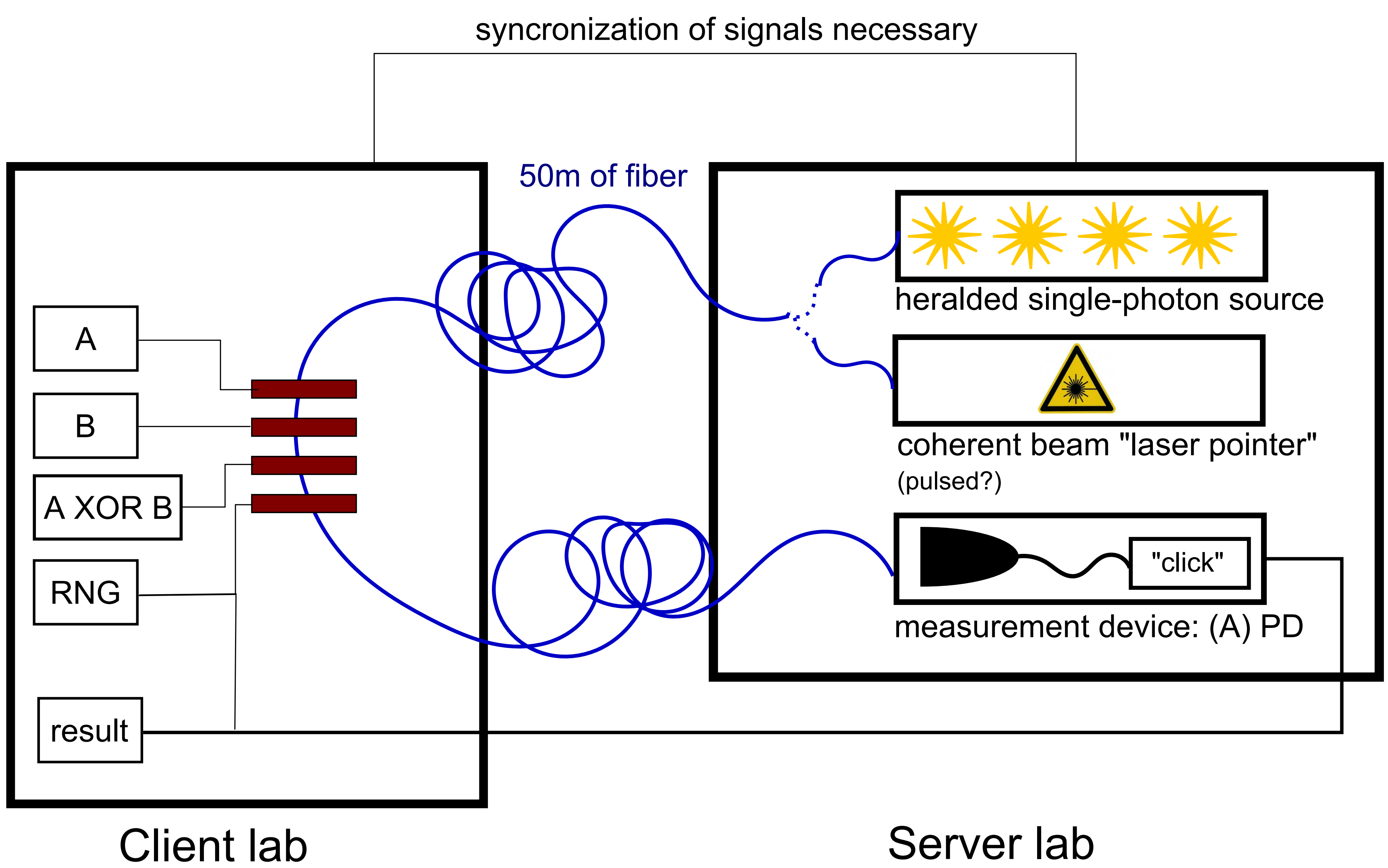
Quantum Communication

$$Z^r S^a S^b \left(S^\dagger\right)^{a\oplus b}|+\rangle \quad = \quad Z^r Z^{a\wedge b}|+\rangle$$

$$\begin{pmatrix}1 & 0\\ 0 & e^{ib\pi/2}\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & e^{ia\pi/2}\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & e^{-i(a\oplus b)\pi/2}\end{pmatrix}\begin{pmatrix}1\\ -1\end{pmatrix} = \begin{pmatrix}1 & 0\\ 0 & e^{-i(a\wedge b)\pi}\end{pmatrix}\begin{pmatrix}1\\ -1\end{pmatrix}$$

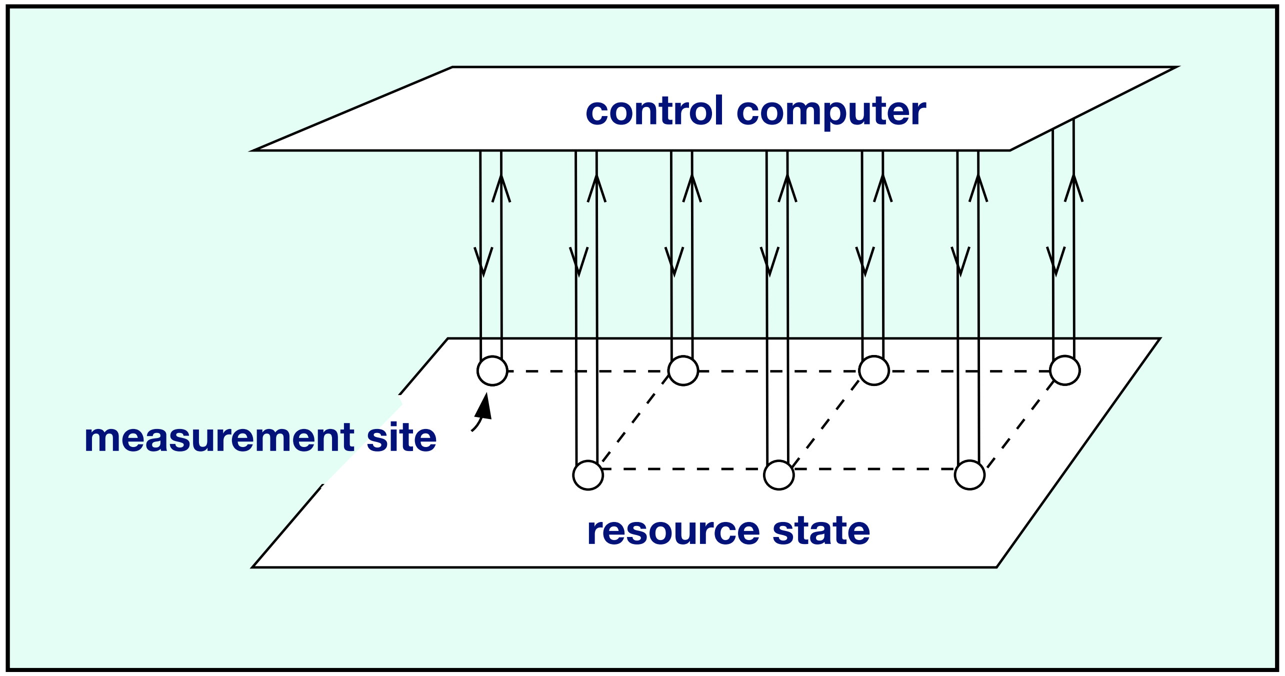
$$\begin{aligned}
\sigma_z \otimes \sigma_z \otimes \sigma_z \, |\psi\rangle &= |\psi\rangle \,, \\
\sigma_z \otimes \sigma_x \otimes \sigma_x \, |\psi\rangle &= |\psi\rangle \,, \\
\sigma_x \otimes \sigma_z \otimes \sigma_x \, |\psi\rangle &= |\psi\rangle \,, \\
\sigma_x \otimes \sigma_x \otimes \sigma_z \, |\psi\rangle &= - \, |\psi\rangle \,,
\end{aligned}$$

Secure NAND

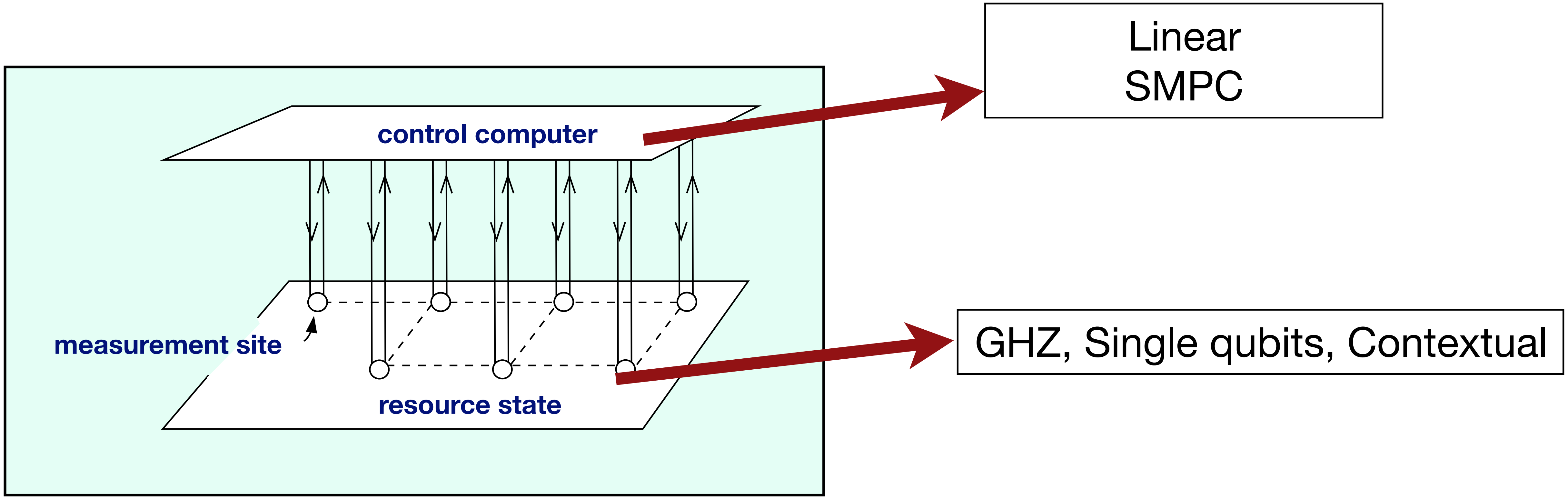


syncronization of signals necessary
50m of fiber
A
B
A XOR B
RNG
result
heralded single-photon source
coherent beam "laser pointer"
(pulsed?)
"click"
measurement device: (A) PD
Client lab
Server lab

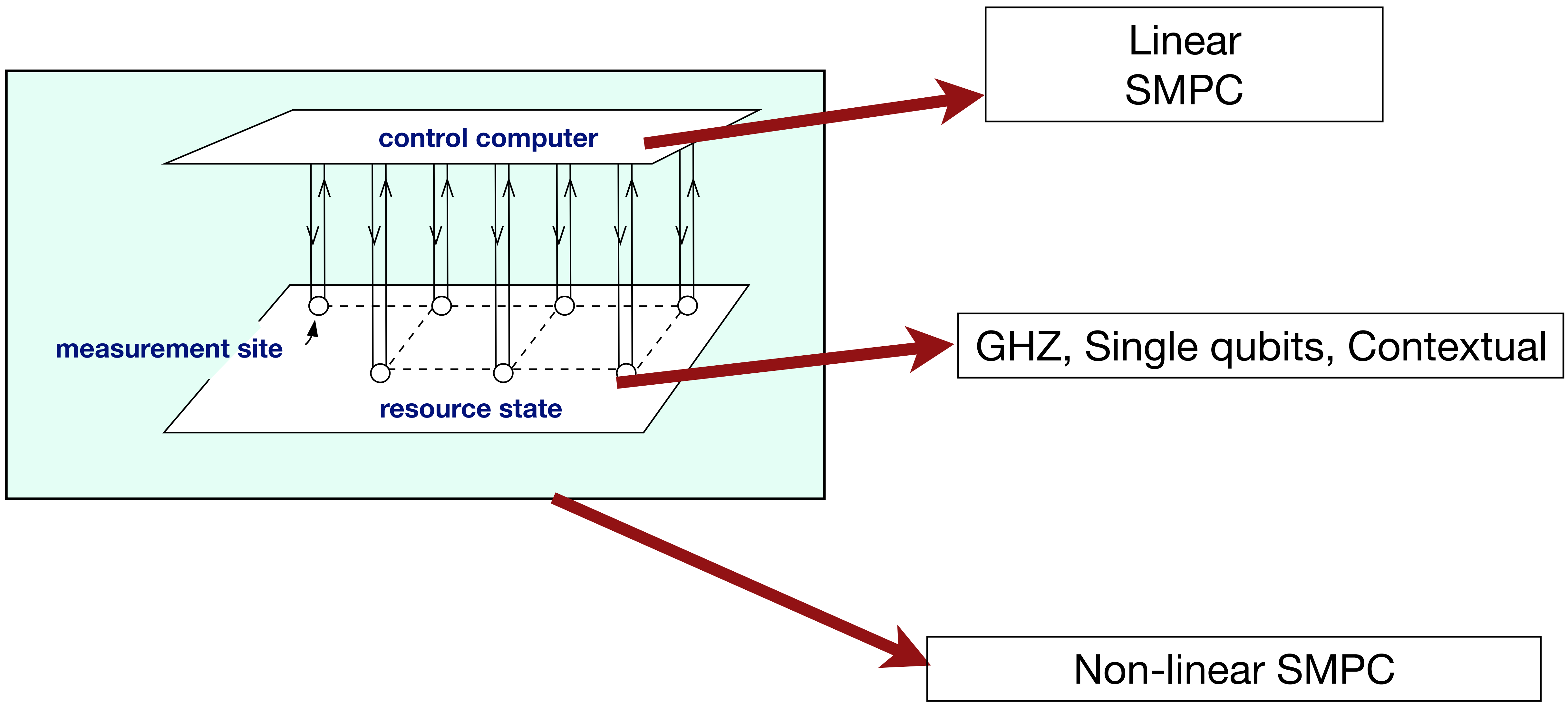
From Linear to Non-linear - SMPC



From Linear to Non-linear - SMPC



From Linear to Non-linear - SMPC



From Linear to Non-linear - SMPC

$$(S^\dagger)^{\oplus x_i} S^{x_n} \dots S^{x_1} \left|+\right\rangle = Z^{f(x_1,\dots,x_n)} \left|+\right\rangle$$

$$f(x_1,\dots,x_n) = \begin{cases} 1, \text{ if } \sum x_i = 2 \pmod 4 \text{ or } \sum x_i = 3 \pmod 4 \\ 0, \text{ if } \sum x_i = 0 \pmod 4 \text{ or } \sum x_i = 1 \pmod 4 \end{cases}$$

From Linear to Non-linear - SMPC

$$(S^\dagger)^{\oplus x_i} S^{x_n} \dots S^{x_1} \left|+\right\rangle = Z^{f(x_1,\dots,x_n)} \left|+\right\rangle$$

$$f(x_1,\dots,x_n) = \begin{cases} 1, \text{ if } \sum x_i = 2 \pmod 4 \text{ or } \sum x_i = 3 \pmod 4 \\ 0, \text{ if } \sum x_i = 0 \pmod 4 \text{ or } \sum x_i = 1 \pmod 4 \end{cases}$$

$$f(x_1,\dots,x_n) = x_1 \cdot x_2 + (x_1 + x_2) \cdot x_3 + (x_1 + x_2 + x_3) \cdot x_4 + \dots + (x_1 + \dots x_{n-1}) \cdot x_n$$

From Linear to Non-linear - SMPC

$$(S^\dagger)^{\oplus x_i} S^{x_n} \dots S^{x_1} |+\rangle = Z^{f(x_1,\dots,x_n)} |+\rangle$$

$$f(x_1,\dots,x_n) = \begin{cases} 1, \text{ if } \sum x_i = 2 \pmod 4 \text{ or } \sum x_i = 3 \pmod 4 \\ 0, \text{ if } \sum x_i = 0 \pmod 4 \text{ or } \sum x_i = 1 \pmod 4 \end{cases}$$

$$f(x_1,\dots,x_n) = x_1 \cdot x_2 + (x_1 + x_2) \cdot x_3 + (x_1 + x_2 + x_3) \cdot x_4 + \dots + (x_1 + \dots x_{n-1}) \cdot x_n$$

$$\boxed{(S^\dagger)^{\oplus x_i} Z^{y_n} S^{x_n} \dots Z^{y_1} S^{x_1} |+\rangle = Z^{\oplus y_n} Z^{f(x_1,\dots,x_n)} |+\rangle}$$

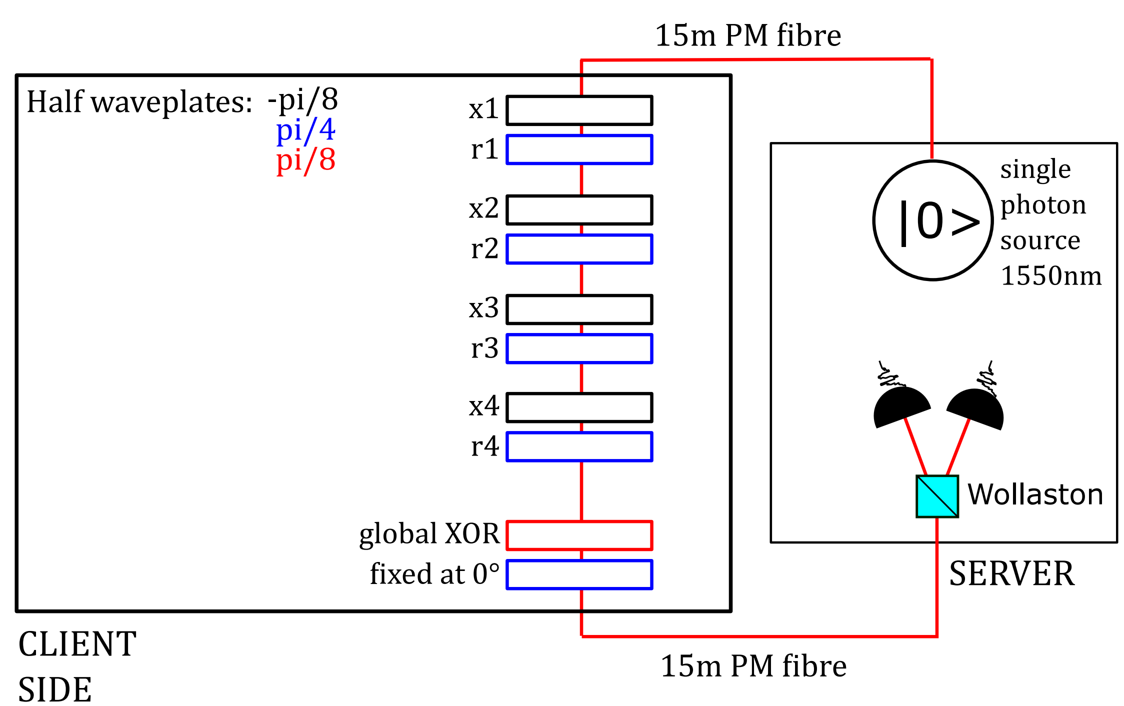
From Linear to Non-linear - SMPC

$$(S^\dagger)^{\oplus x_i} S^{x_n} \dots S^{x_1} \left|+\right\rangle = Z^{f(x_1,\dots,x_n)} \left|+\right\rangle$$

$$f(x_1,\dots,x_n) = \begin{cases} 1, \text{ if } \sum x_i = 2 \pmod 4 \text{ or } \sum x_i = 3 \pmod 4 \\ 0, \text{ if } \sum x_i = 0 \pmod 4 \text{ or } \sum x_i = 1 \pmod 4 \end{cases}$$

$$f(x_1,\dots,x_n) = x_1 \cdot x_2 + (x_1 + x_2)\cdot x_3 + (x_1 + x_2 + x_3)\cdot x_4 + \dots + (x_1 + \dots x_{n-1})\cdot x_n$$

$$\boxed{(S^\dagger)^{\oplus x_i} Z^{y_n} S^{x_n} \dots Z^{y_1} S^{x_1} \left|+\right\rangle = Z^{\oplus y_n} Z^{f(x_1,\dots,x_n)} \left|+\right\rangle}$$



From Linear to Non-linear - SMPC

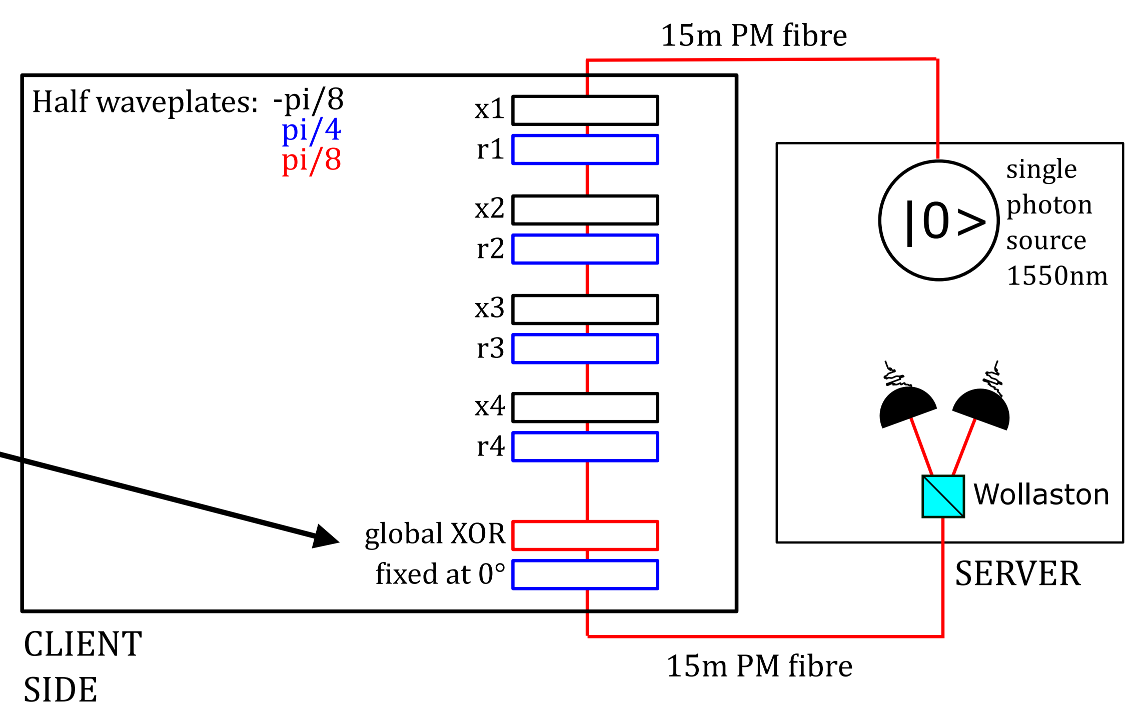
$$(S^\dagger)^{\oplus x_i} S^{x_n} \dots S^{x_1} |+\rangle = Z^{f(x_1,\dots,x_n)} |+\rangle$$

$$f(x_1,\dots,x_n) = \begin{cases} 1, \text{ if } \sum x_i = 2 \pmod 4 \text{ or } \sum x_i = 3 \pmod 4 \\ 0, \text{ if } \sum x_i = 0 \pmod 4 \text{ or } \sum x_i = 1 \pmod 4 \end{cases}$$

$$f(x_1,\dots,x_n) = x_1 \cdot x_2 + (x_1 + x_2) \cdot x_3 + (x_1 + x_2 + x_3) \cdot x_4 + \dots + (x_1 + \dots x_{n-1}) \cdot x_n$$

$$\boxed{(S^\dagger)^{\oplus x_i} Z^{y_n} S^{x_n} \dots Z^{y_1} S^{x_1} |+\rangle = Z^{\oplus y_n} Z^{f(x_1,\dots,x_n)} |+\rangle}$$

Classical Linear SMPC



Perspective

Can we do something with even few qubits ?

Classical Linear SMPC

Contextual States

Classical Non-linear SMPC

versus

Classical SMPC

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

easy

Linear Verifiable Secret Sharing

hard

costly but offline FHE

Future Network

A **hybrid** network of classical protocols with quantum gadgets

boosting efficiency and security

of every task achievable against classical attackers against quantum attackers

Future Network

A **hybrid** network of classical protocols with quantum gadgets

boosting efficiency and security

of every task achievable against classical attackers against quantum attackers