# Quantum Computing as a Service

## *Secure and Verifiable Multi-Tenant Quantum Data Centre*


**Elham Kashefi**

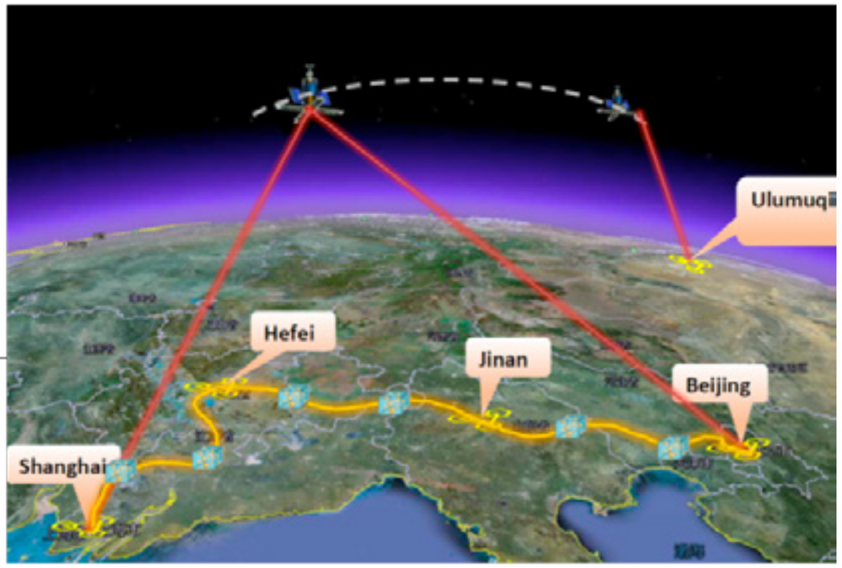
**University of Edinburgh**
**Quantum Computing and Simulation Hub**

**CNRS Sorbonne University**
**Quantum Internet Alliance**

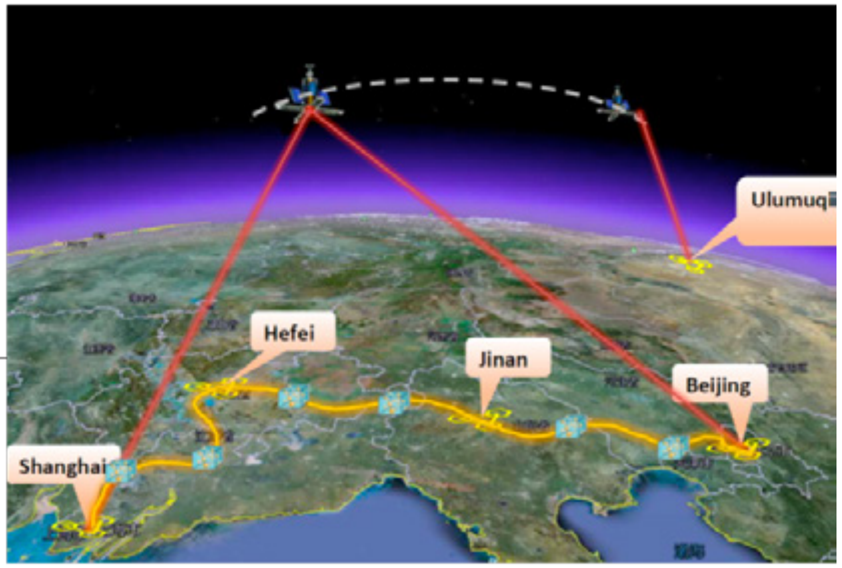
**VeriQloud**

# Currently

# Quantum Links

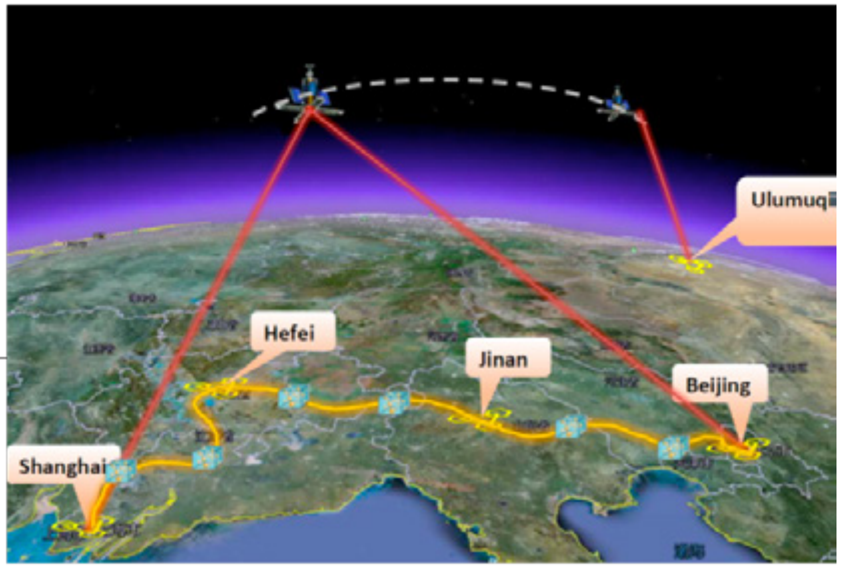
# Quantum Links


**Unclonable / Measurement disturbance … - security**

**QKD, Quantum Coin Flipping, …**

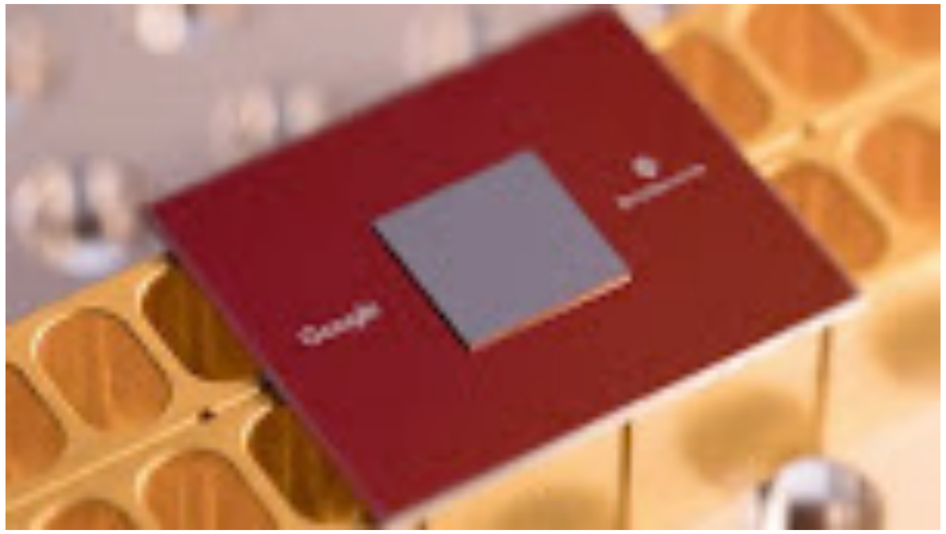
# Quantum Links

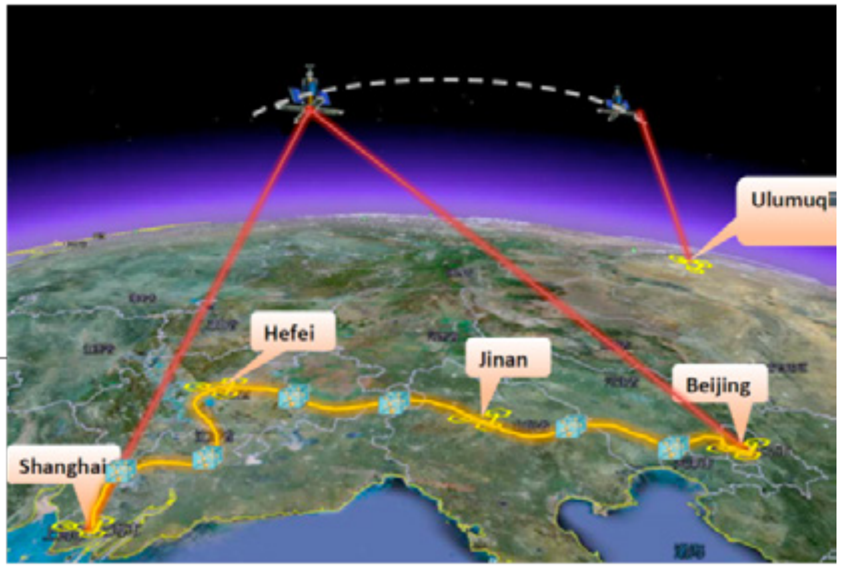

**Unclonable / Measurement disturbance … - security**

**QKD, Quantum Coin Flipping, …**

# Quantum Nodes



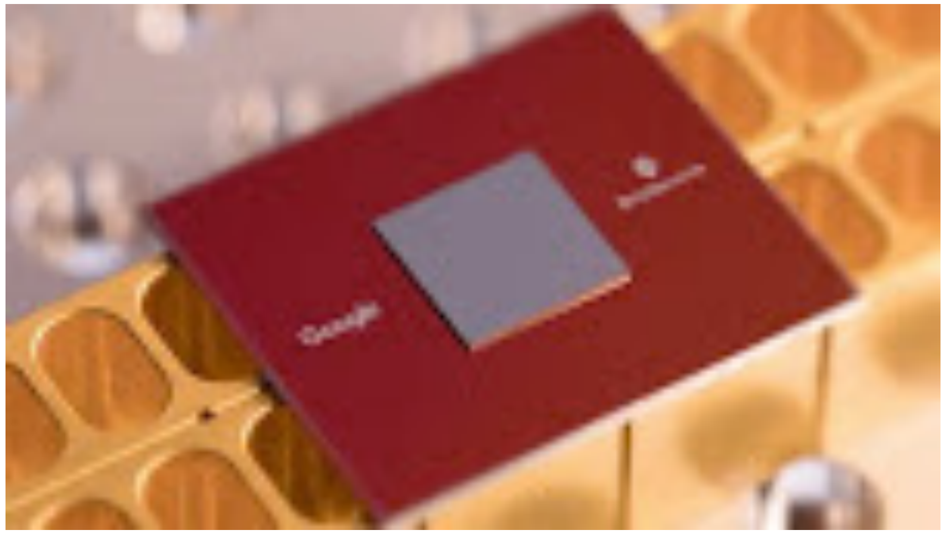
# Quantum Links


**Unclonable / Measurement disturbance … - security**

**QKD, Quantum Coin Flipping, …**

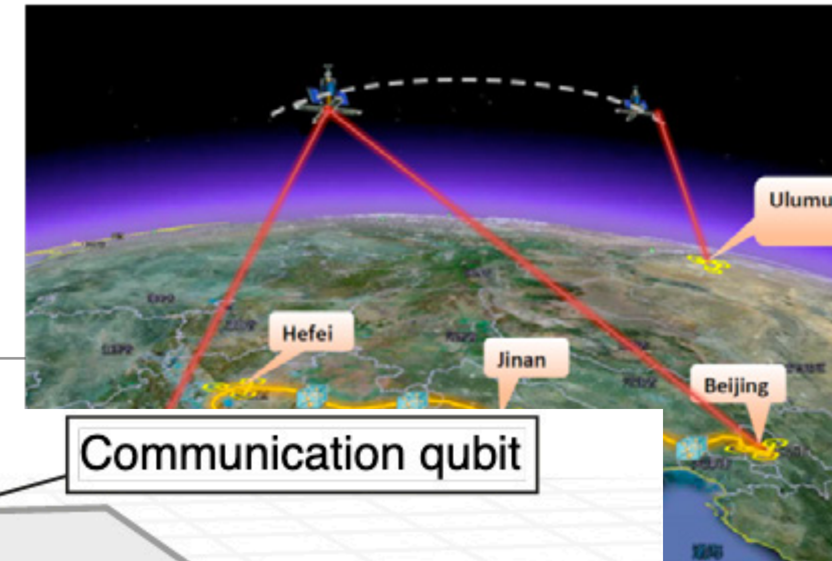
# Quantum Nodes



**Superposition / Entanglement… - speed**

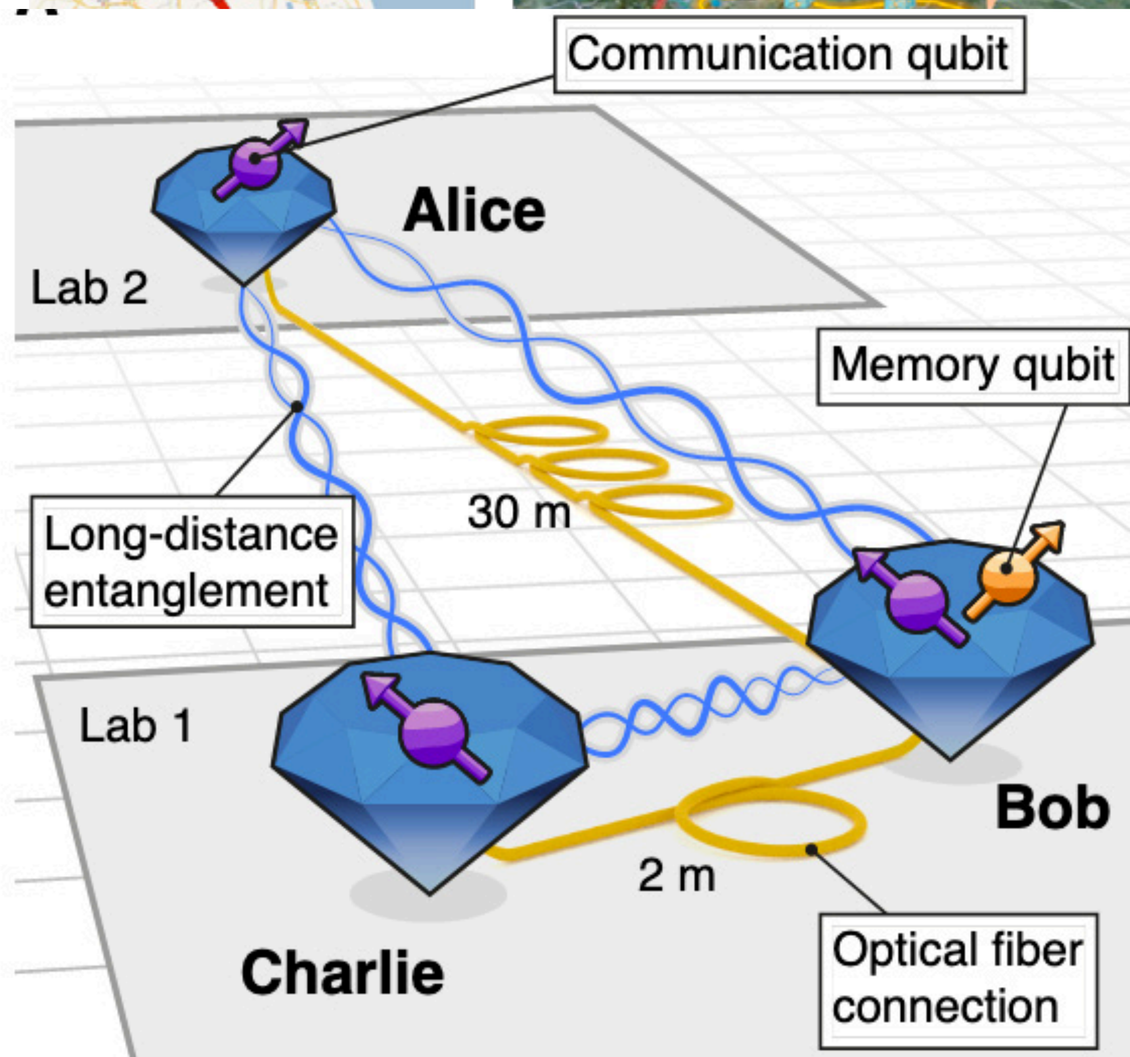
**Random Walk, Machine Learning, …**

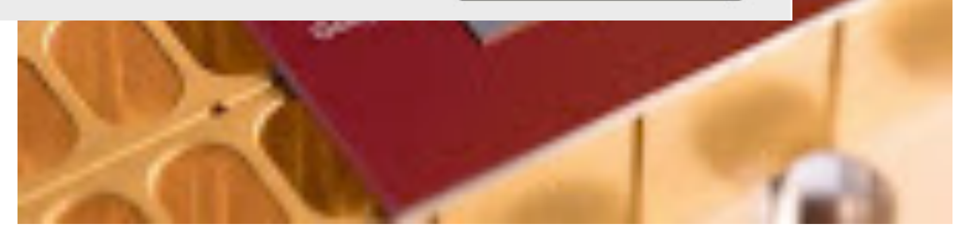
# Quantum Links


Unclonable / Measurement disturbance

QKD, Quantum Coin Flipping, …



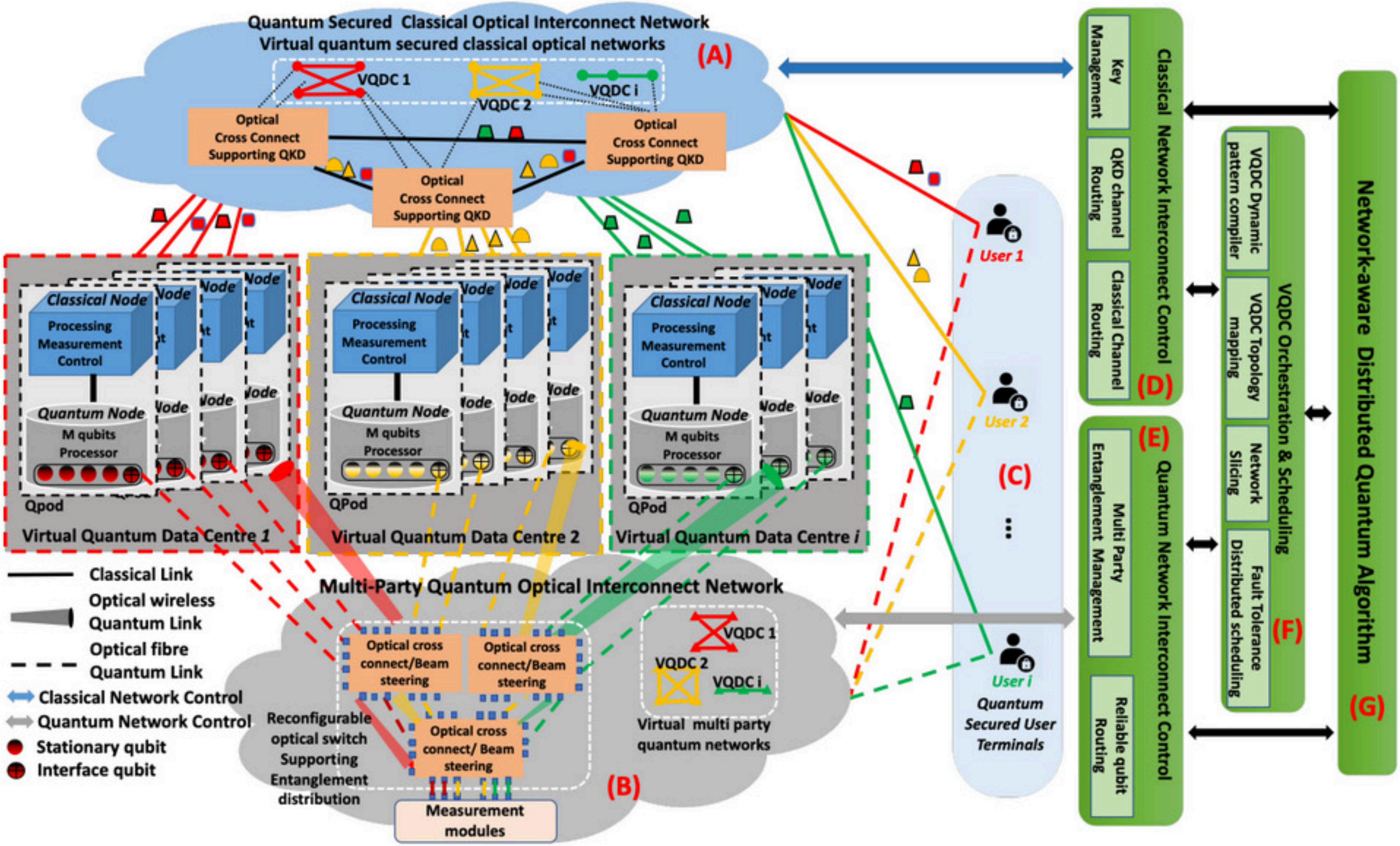
# Quantum Nodes

Superposition / Entanglement… - speed

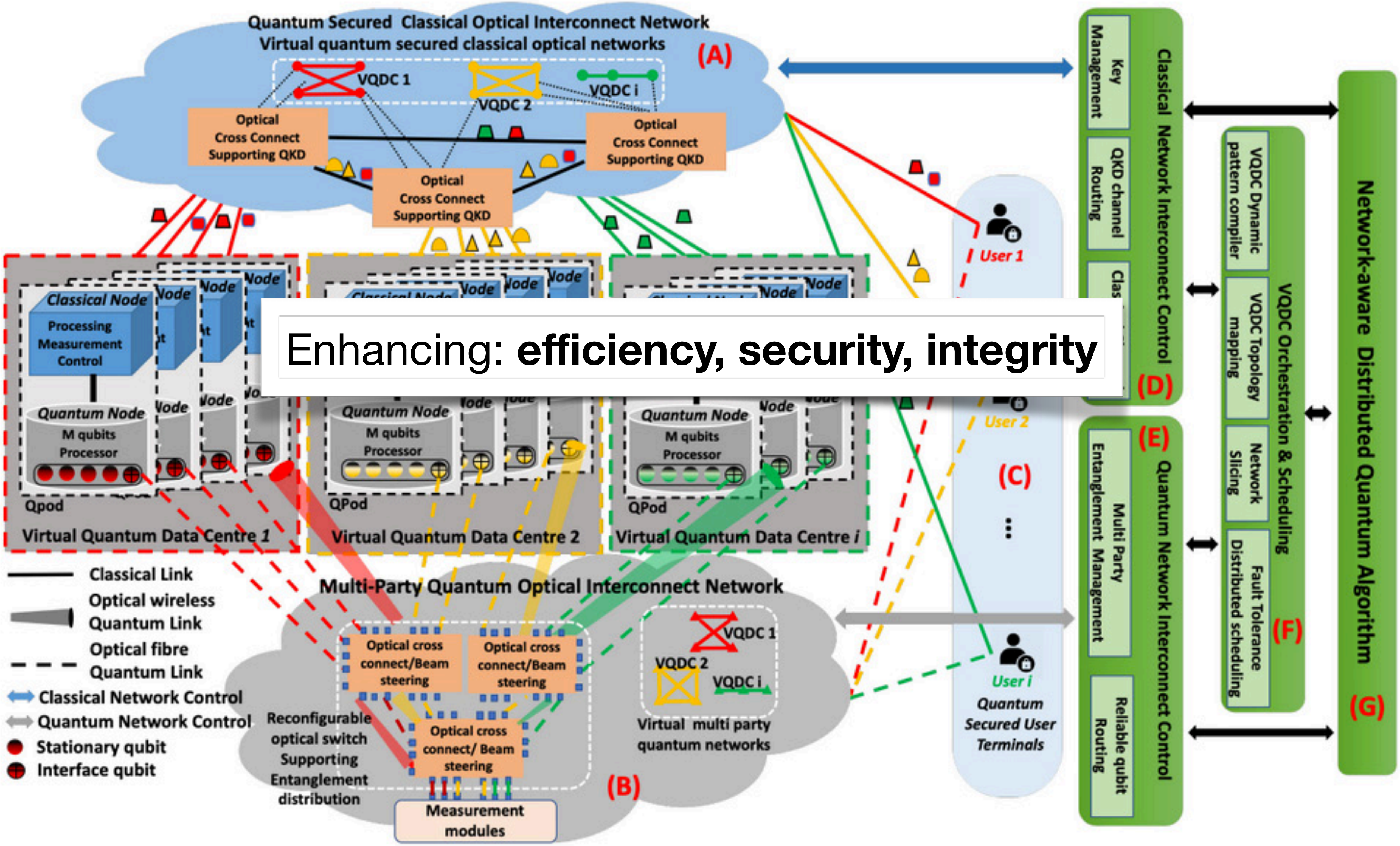
Random Walk, Machine Learning, …

# Future

# Multi-Tenant Quantum Data Centre

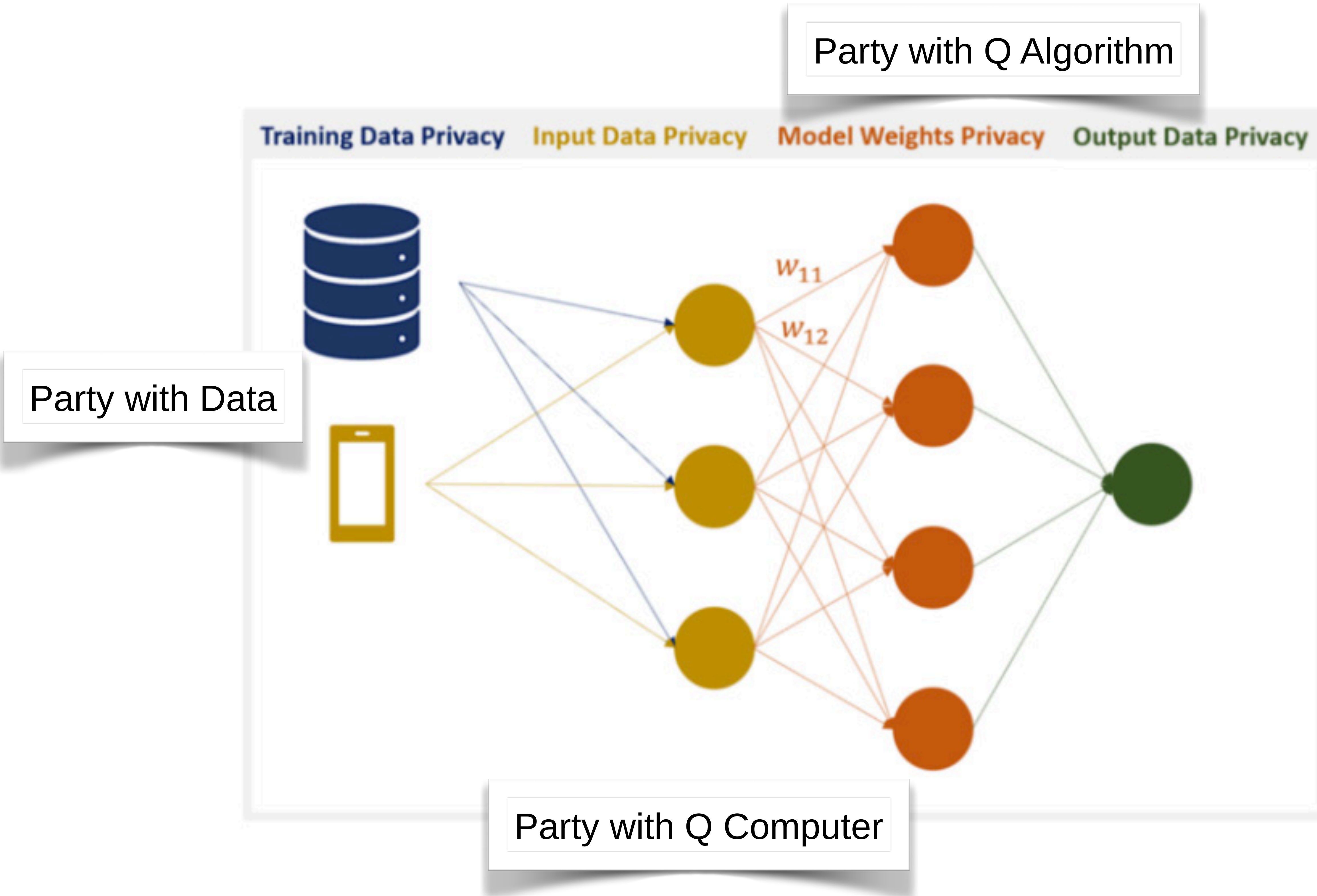


# Multi-Tenant Quantum Data Centre



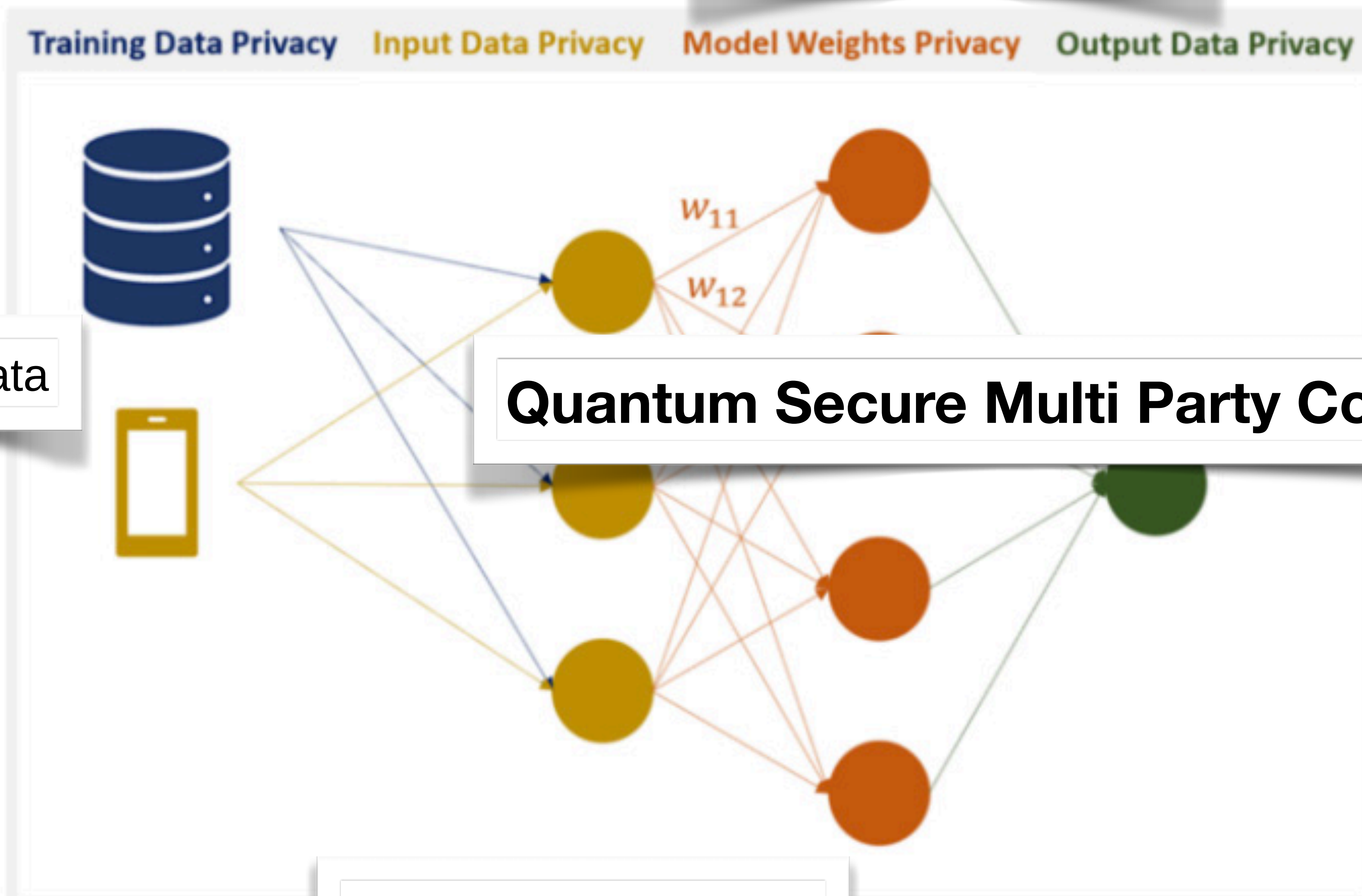

Enhancing: **efficiency, security, integrity**

# Use-Case Example: Privacy Preserving QML



# Use-Case Example: Privacy Preserving QML

Party with Q Algorithm




Party with Data

**Quantum Secure Multi Party Computing**

Party with Q Computer

# Plan

# Plan

- 2 party QC: Honest Client - Malicious Server

# Plan

- 2 party QC: Honest Client - Malicious Server
    - What is possible ?
    - Building Blocks: QKD, Teleportation, Self-Testing
    - Verifiable Universal Blind Quantum Computing

# Plan

- 2 party QC: Honest Client - Malicious Server
  - What is possible ?
  - Building Blocks: QKD, Teleportation, Self-Testing
  - Verifiable Universal Blind Quantum Computing
- 2 party QC: Malicious Client - Malicious Server

# Plan

- 2 party QC: Honest Client - Malicious Server
    - What is possible ?
    - Building Blocks: QKD, Teleportation, Self-Testing
    - Verifiable Universal Blind Quantum Computing
- 2 party QC: Malicious Client - Malicious Server
    - Quantum Cut and Choose Technique

# Plan

- 2 party QC: Honest Client - Malicious Server
    - What is possible ?
    - Building Blocks: QKD, Teleportation, Self-Testing
    - Verifiable Universal Blind Quantum Computing
- 2 party QC: Malicious Client - Malicious Server
    - Quantum Cut and Choose Technique
- Multi party QC: Malicious Clients - Malicious Server

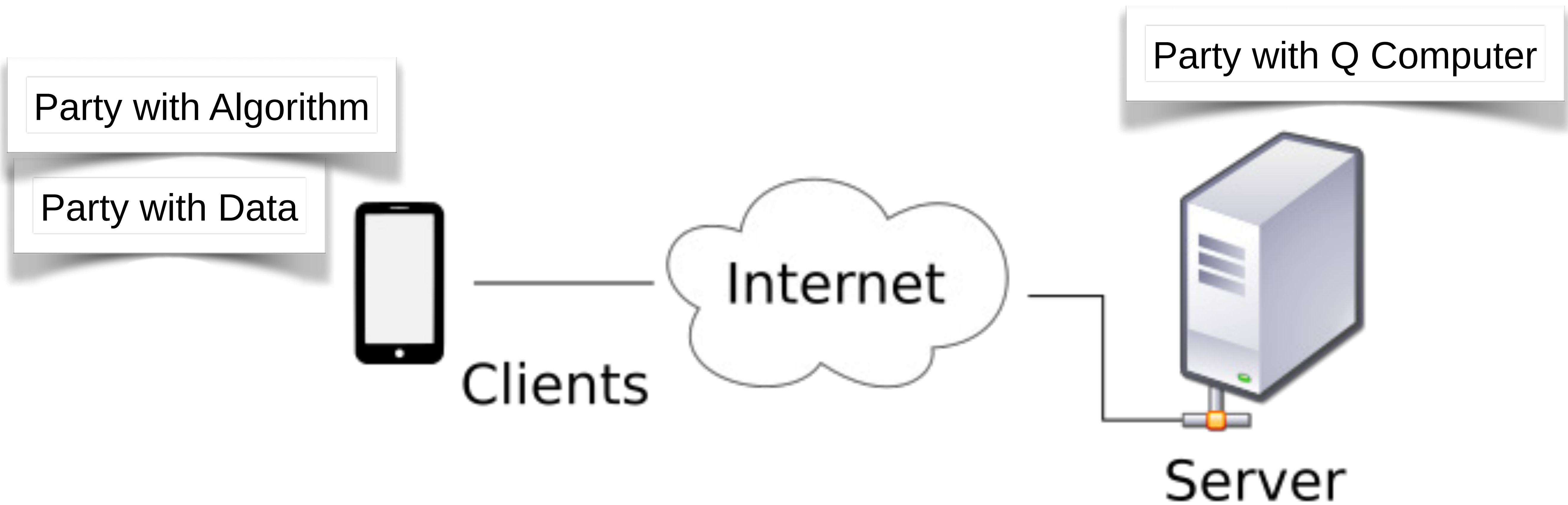
# Plan

- 2 party QC: Honest Client - Malicious Server
    - What is possible ?
    - Building Blocks: QKD, Teleportation, Self-Testing
    - Verifiable Universal Blind Quantum Computing
- 2 party QC: Malicious Client - Malicious Server
    - Quantum Cut and Choose Technique
- Multi party QC: Malicious Clients - Malicious Server
    - Lifting Classical SMPC to QSMPC

# Plan

- 2 party QC: Honest Client - Malicious Server
  - What is possible ?
  - Building Blocks: QKD, Teleportation, Self-Testing
  - Verifiable Universal Blind Quantum Computing
- 2 party QC: Malicious Client - Malicious Server
  - Quantum Cut and Choose Technique
- Multi party QC: Malicious Clients - Malicious Server
  - Lifting Classical SMPC to QSMPC
- When can we have it for real ?

# Honest Client - Malicious Server

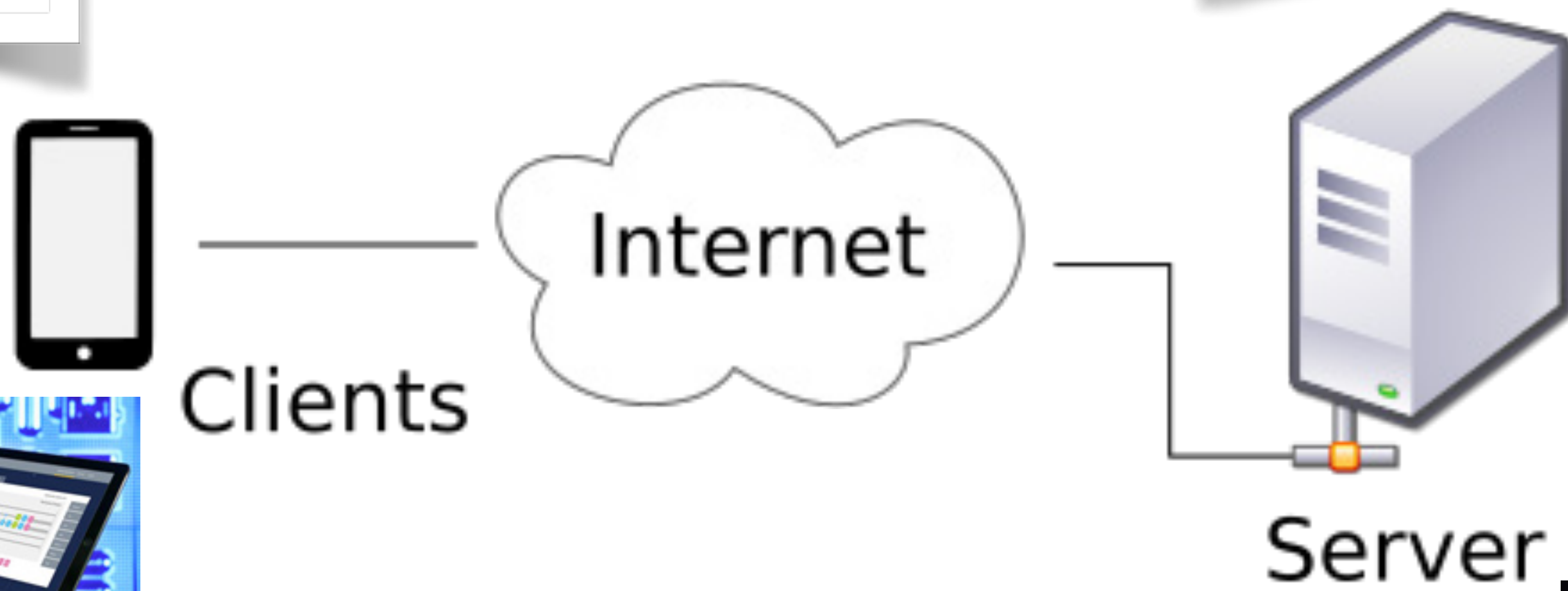


# Honest Client - Malicious Server

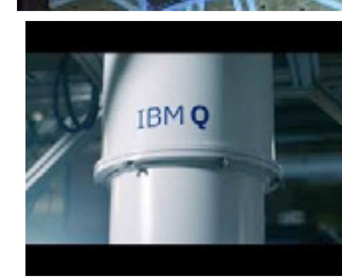
Party with Algorithm

Party with Data

Party with Q Computer





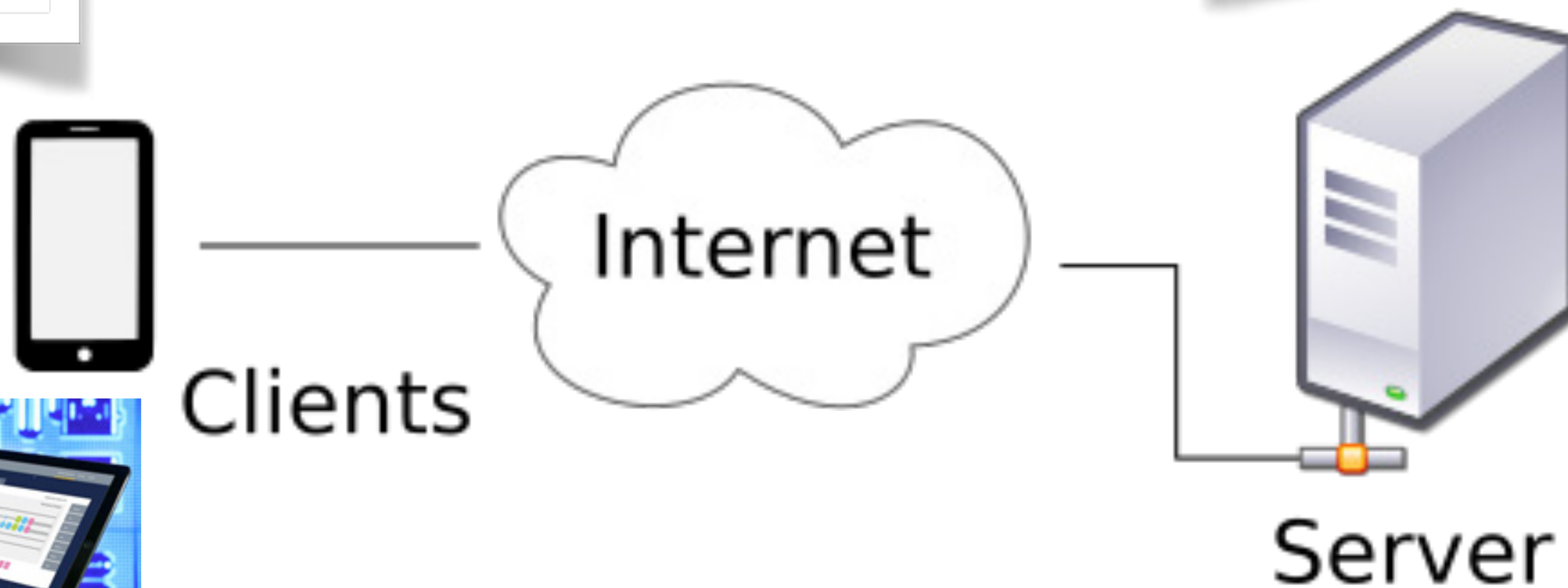


# Honest Client - Malicious Server

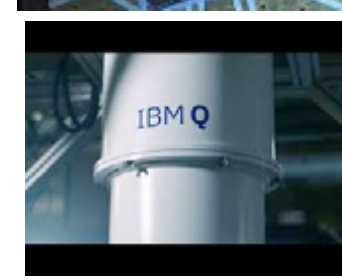
Party with Algorithm

Party with Data

Party with Q Computer








**No privacy:** Data, Algorithms, Results are all public
**No Verification:** The results are not classically simulatable

# Secure Cloud Computing

Rivest, Adleman and Dertouzos 1979

Can we process encrypted data without decrypting it first ?

# Secure Cloud Computing

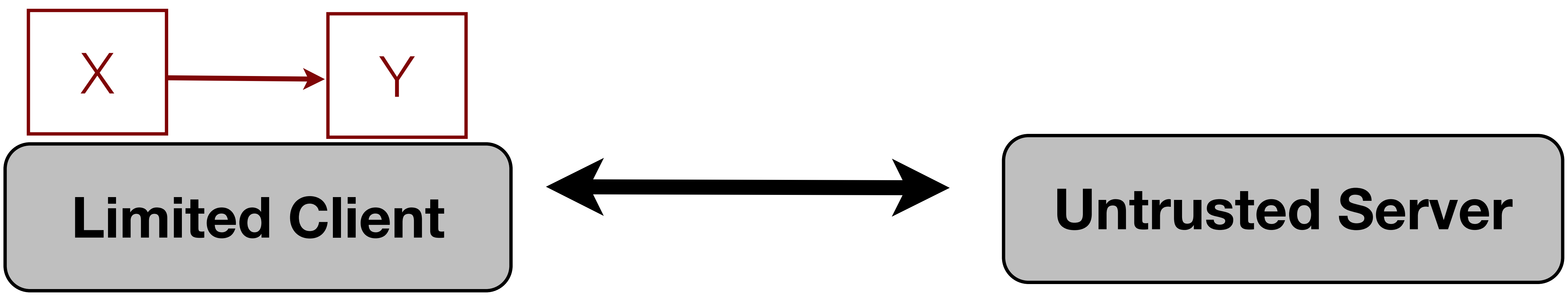
Rivest, Adleman and Dertouzos 1979

Can we process encrypted data without decrypting it first ?

# Secure Cloud Computing

Rivest, Adleman and Dertouzos 1979

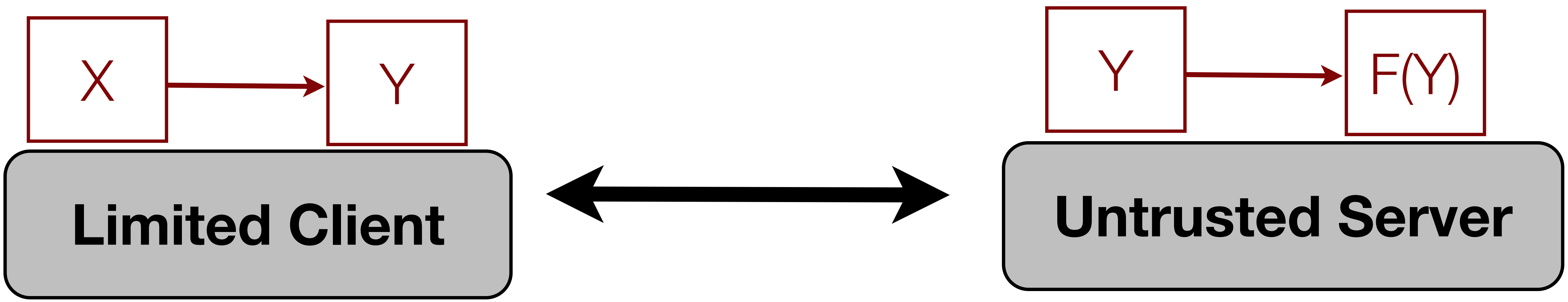
Can we process encrypted data without decrypting it first ?



# Secure Cloud Computing

Rivest, Adleman and Dertouzos 1979

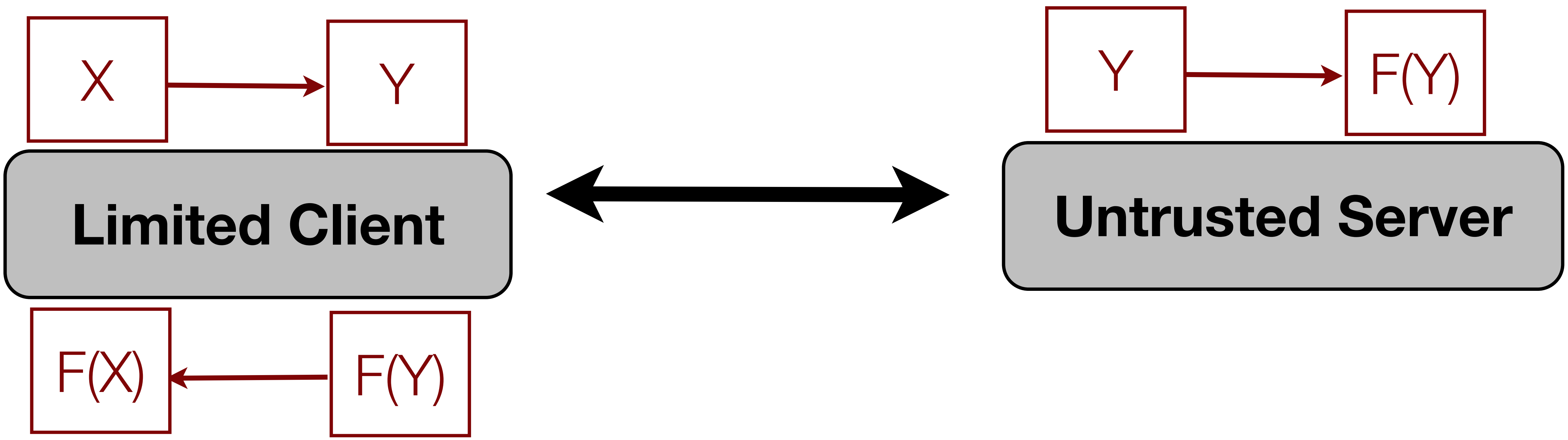
Can we process encrypted data without decrypting it first ?



# Secure Cloud Computing

Rivest, Adleman and Dertouzos 1979

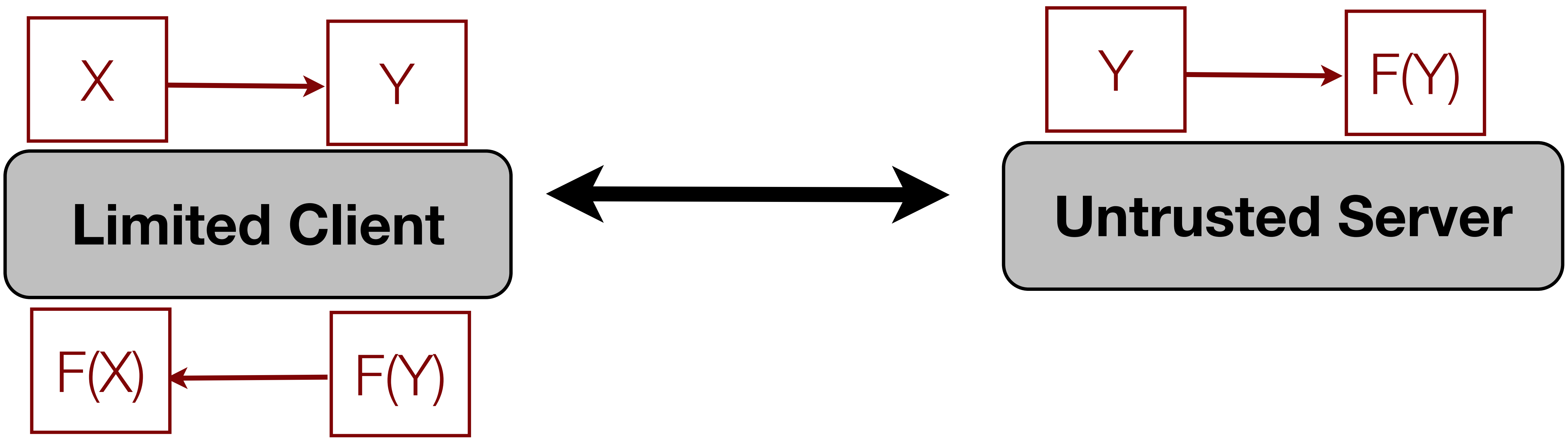
Can we process encrypted data without decrypting it first ?



# Secure Cloud Computing

Rivest, Adleman and Dertouzos 1979

Can we process encrypted data without decrypting it first ?




Gentry 2009 - Fully Homomorphic Encryption

computational security

# Secure Classical access to Quantum Cloud ?

Fillinger: No efficient informationally secure classical FHE scheme exist

# Secure Classical access to Quantum Cloud ?

Fillinger: No efficient informationally secure classical FHE scheme exist

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

# Secure Classical access to Quantum Cloud ?

Fillinger: No efficient informationally secure classical FHE scheme exist

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

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

# Secure Classical access to Quantum Cloud ?

Fillinger: No efficient informationally secure classical FHE scheme exist

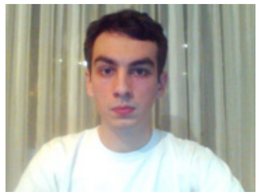
Newman and Shi: No efficient informationally secure quantum FHE scheme exist

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

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

# Secure Classical access to Quantum Cloud ?

# Secure Classical access to Quantum Cloud ?

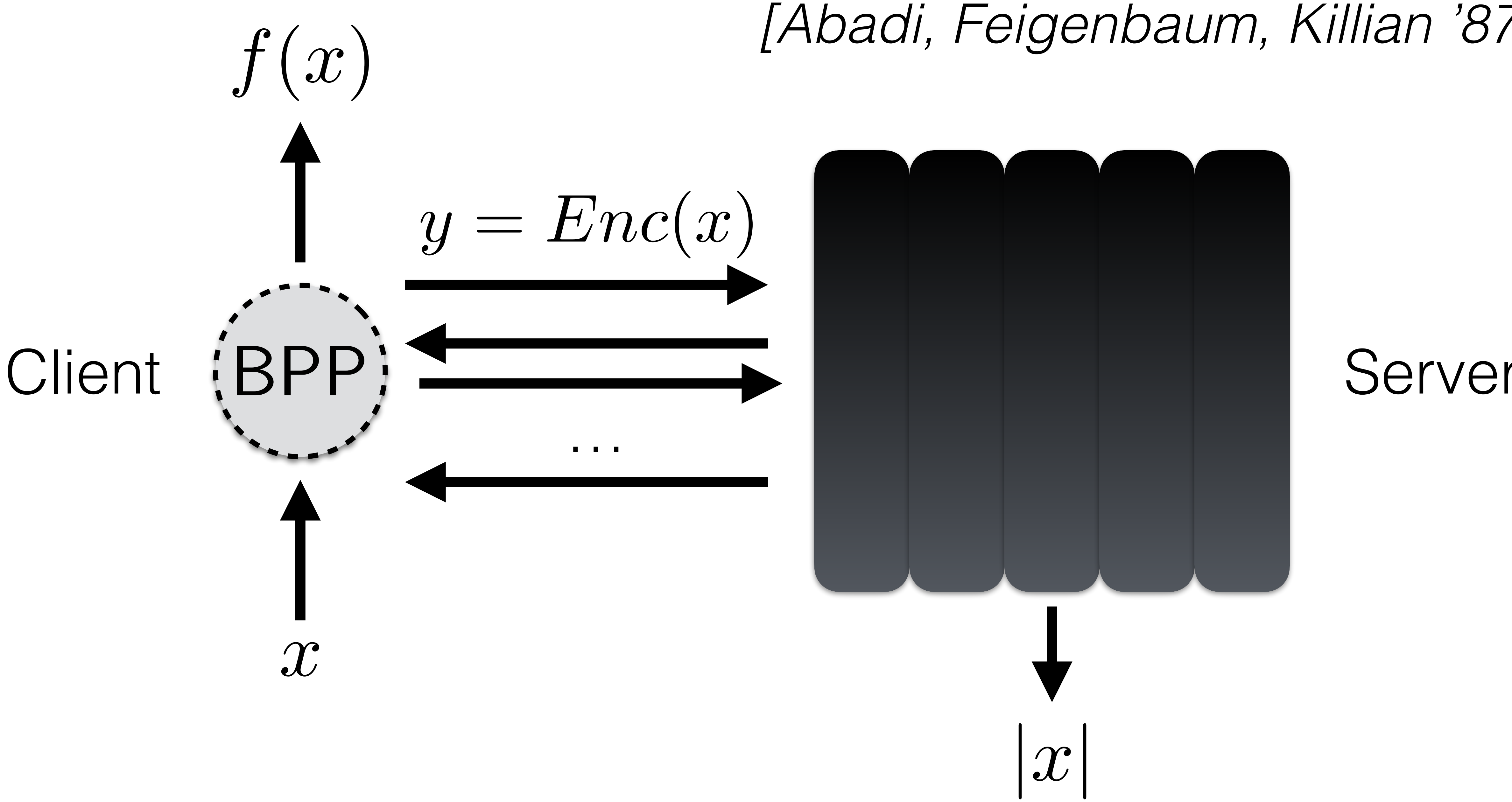


On the implausibility of informationally secure quantum cloud computing with Classical Client
*(PH collapses at the third level)*

*Aaronson, Cojocaru, Gheorghiu, Kashefi, 2017*

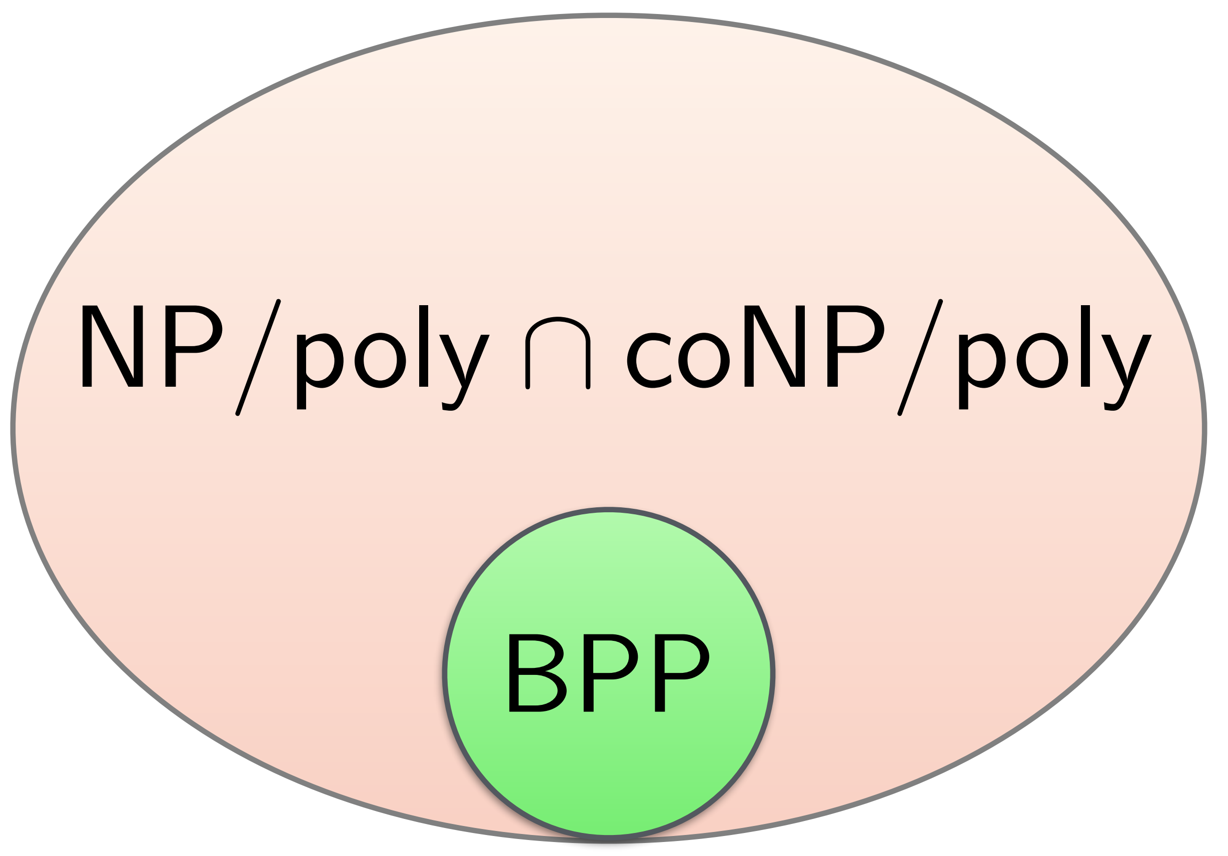
# Generalised Encryption Scheme (GES)

[Abadi, Feigenbaum, Killian '87]

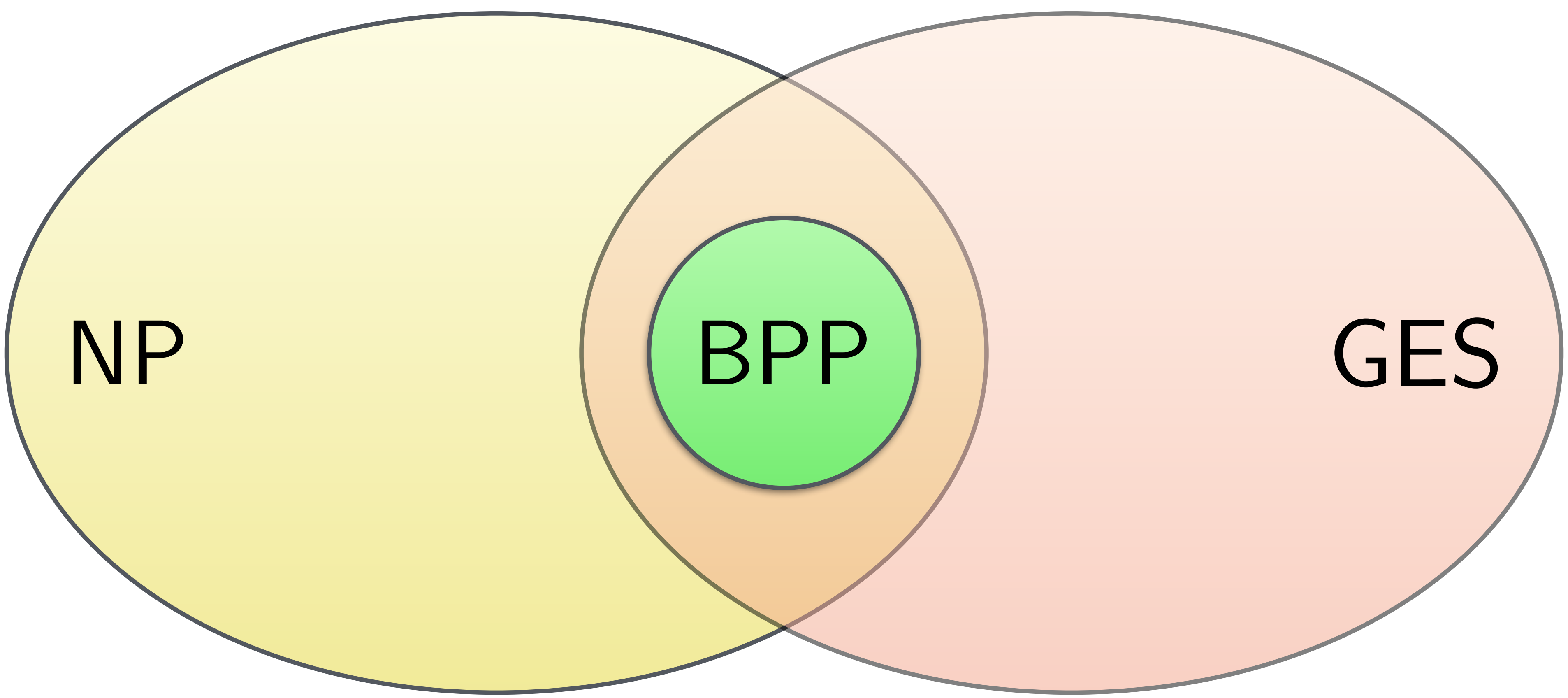



*Information-theoretic security*

Which functions admit a GES?



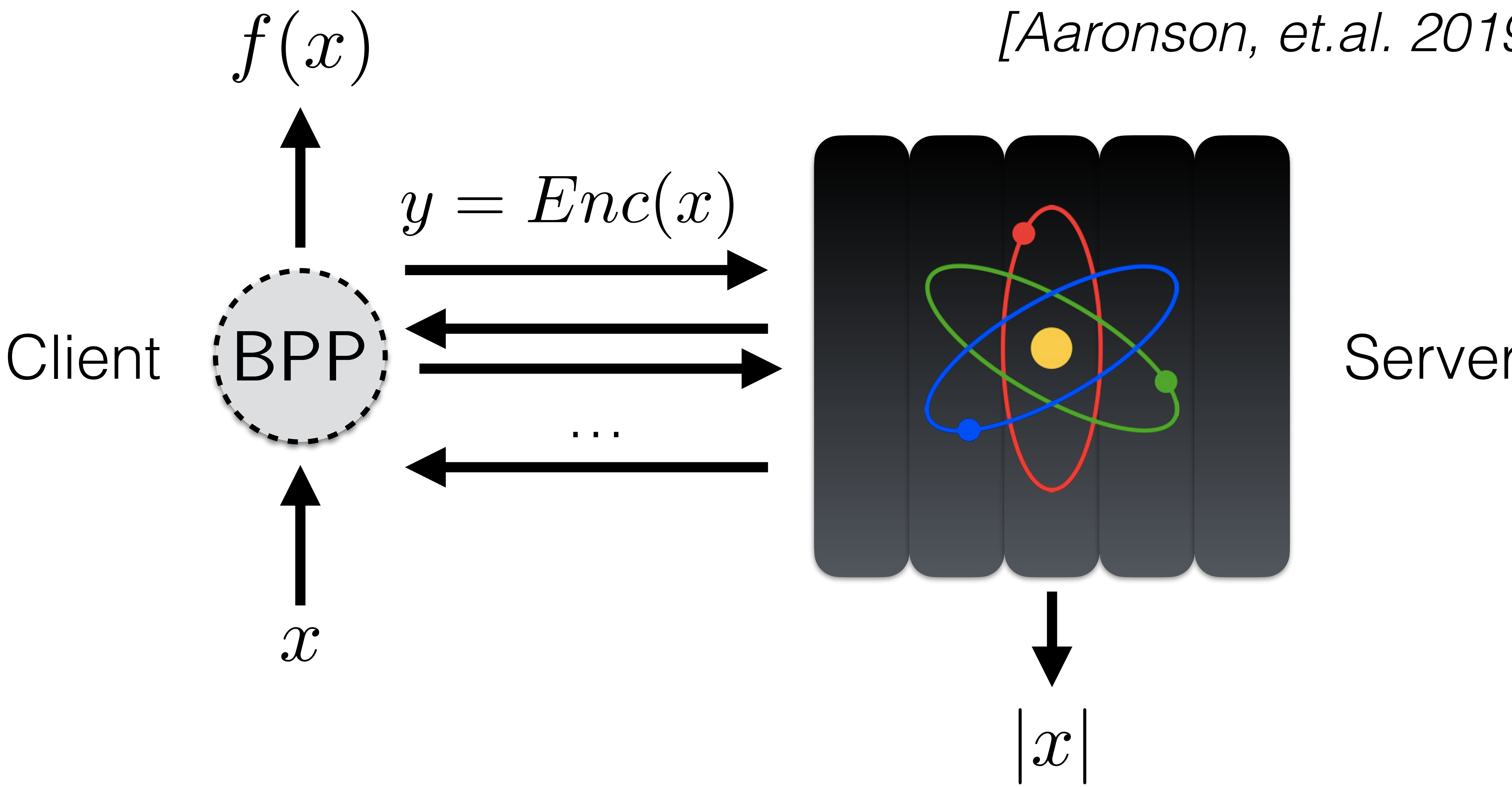
What about **NP** functions?




Unless **PH** collapses

# Generalised Encryption Scheme for QC (GES)

*[Aaronson, et.al. 2019]*



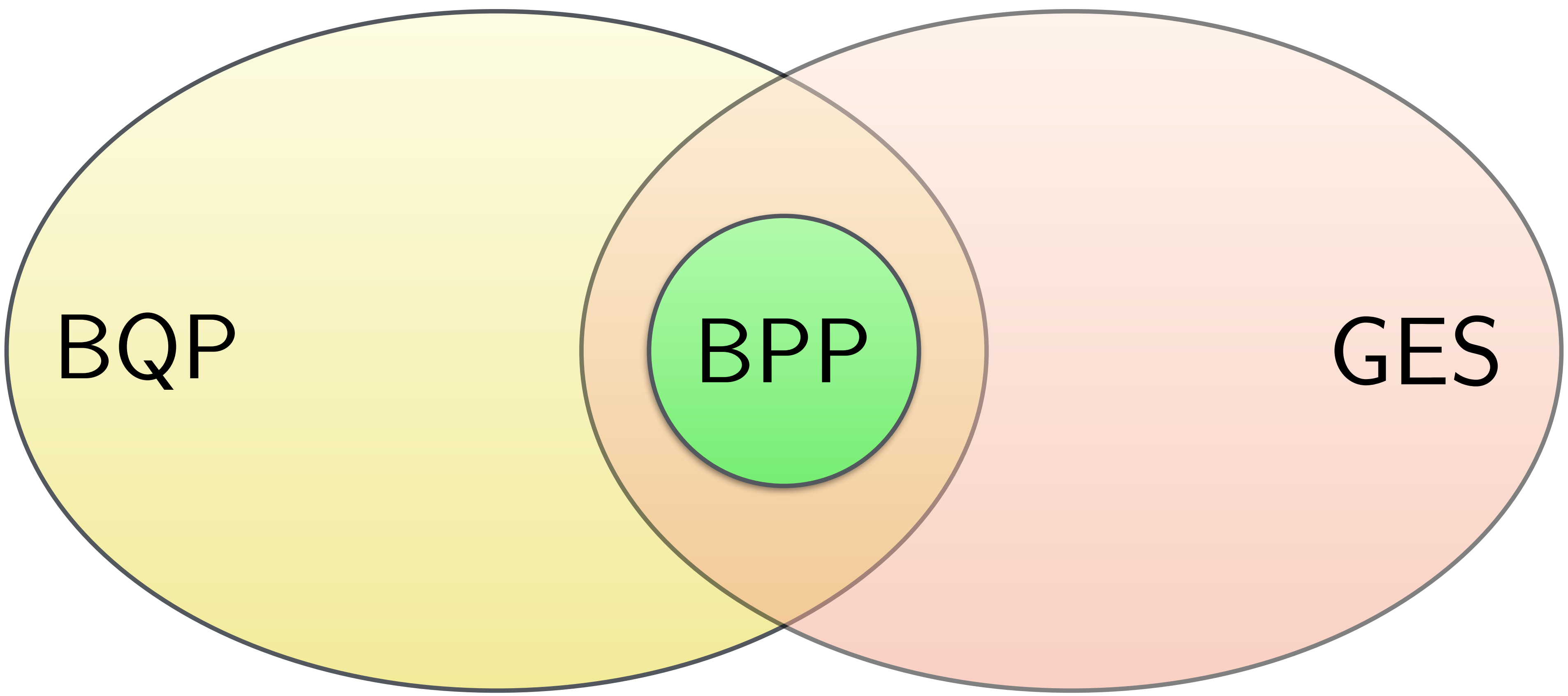

$f \in$ BQP

***Information-theoretic security***

# Our work

1. Do **BQP** functions admit a GES?

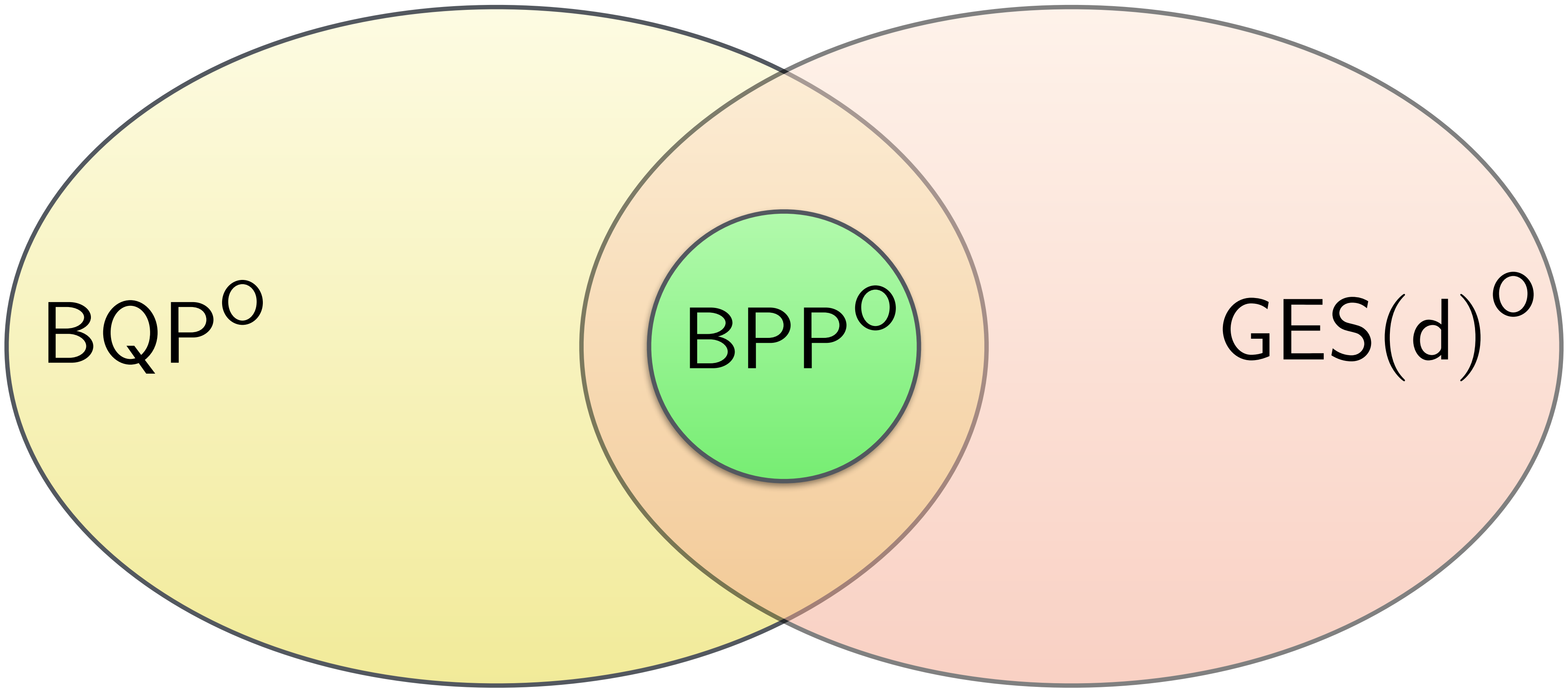
We give evidence that the answer is **NO**




Conjectured relationship between classes

# An oracle result

For each d, there exists an oracle, O, such that:



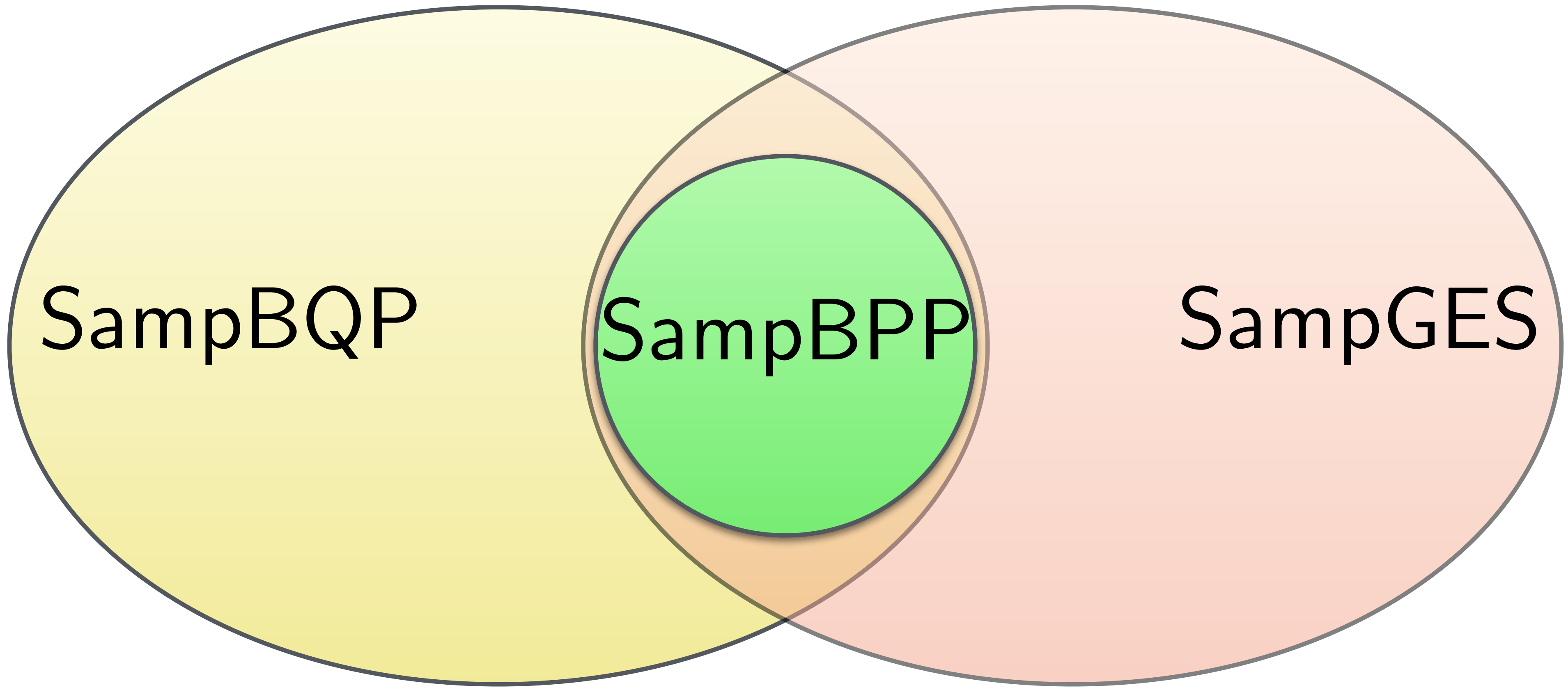

The oracle is based on Simon's problem

$$O(n,x) = f_n(x)$$

Is $f_n$ 1-to-1 or does it have Simon's property?

Simon's property: $f_n$ is 2-to-1 and periodic

# A sampling result




Unless, there exist circuits $\{C_n\}_n$ having the properties:

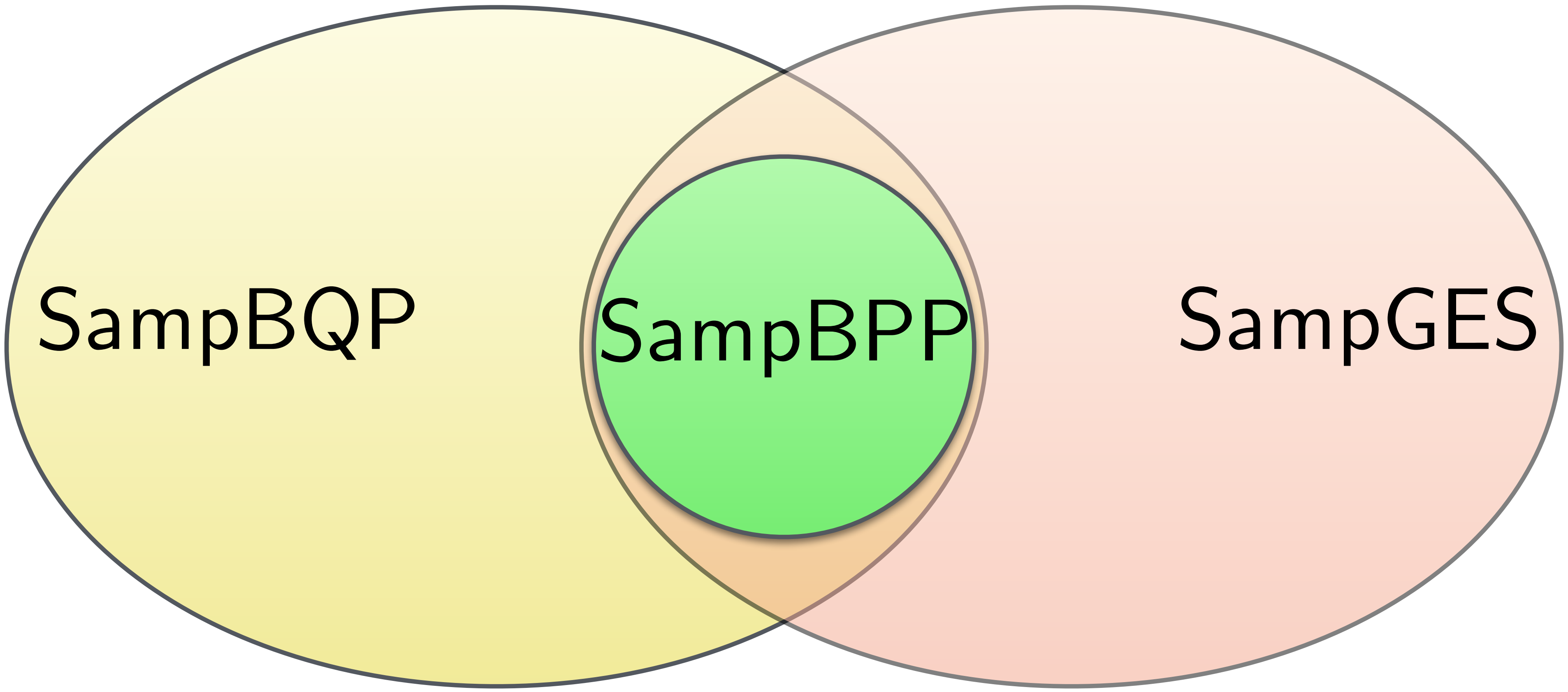
$$|C_n| = 2^{n-\Omega(n/log(n))}$$

$$C_n \; queries \; \mathrm{NP}^{\mathrm{NP}}$$

Computes <u>exactly</u> the permanent of n x n matrix

Best known algorithm for permanent (*Ryser '63*): $O(n2^n)$

# A sampling result




GES for **SampBQP** → "efficient" circuits for permanent

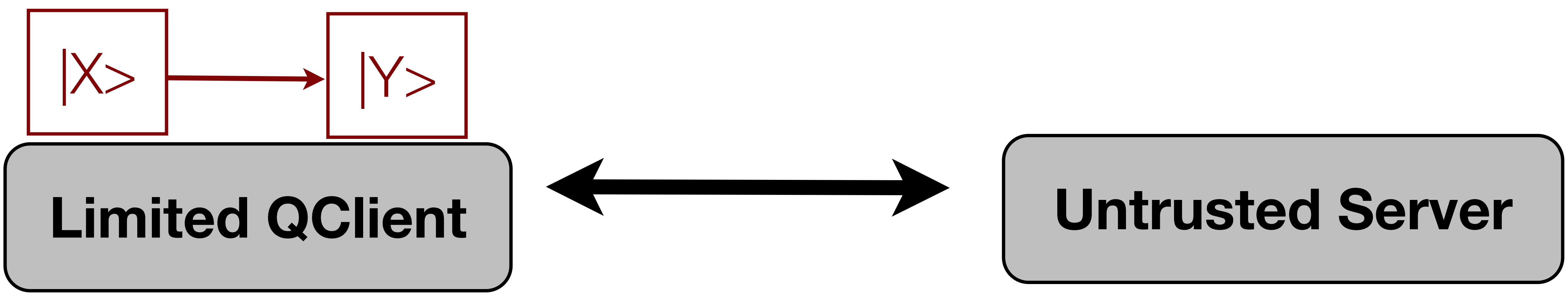
Best known algorithm for permanent (*Ryser '63*): $O(n2^n)$

# Secure Classical Access to Quantum Cloud

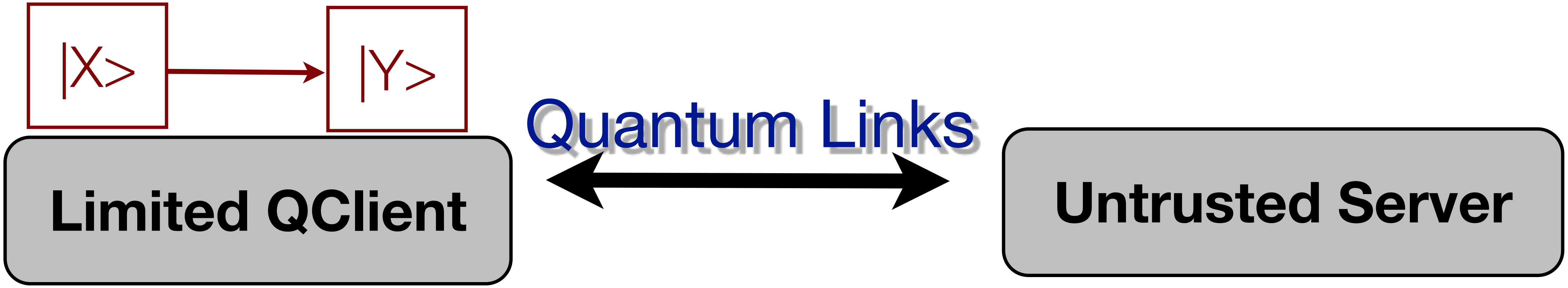
# Secure Quantum access to Quantum Cloud

# Secure Quantum access to Quantum Cloud

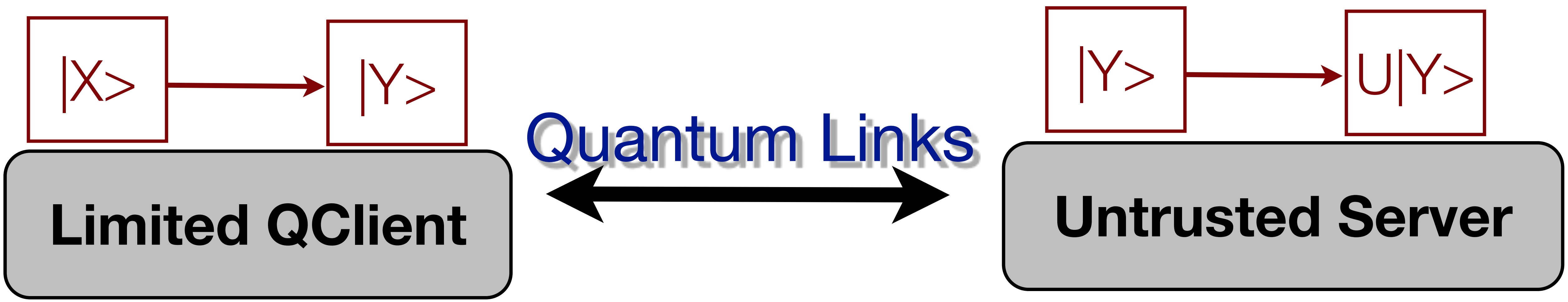
# Secure Quantum access to Quantum Cloud



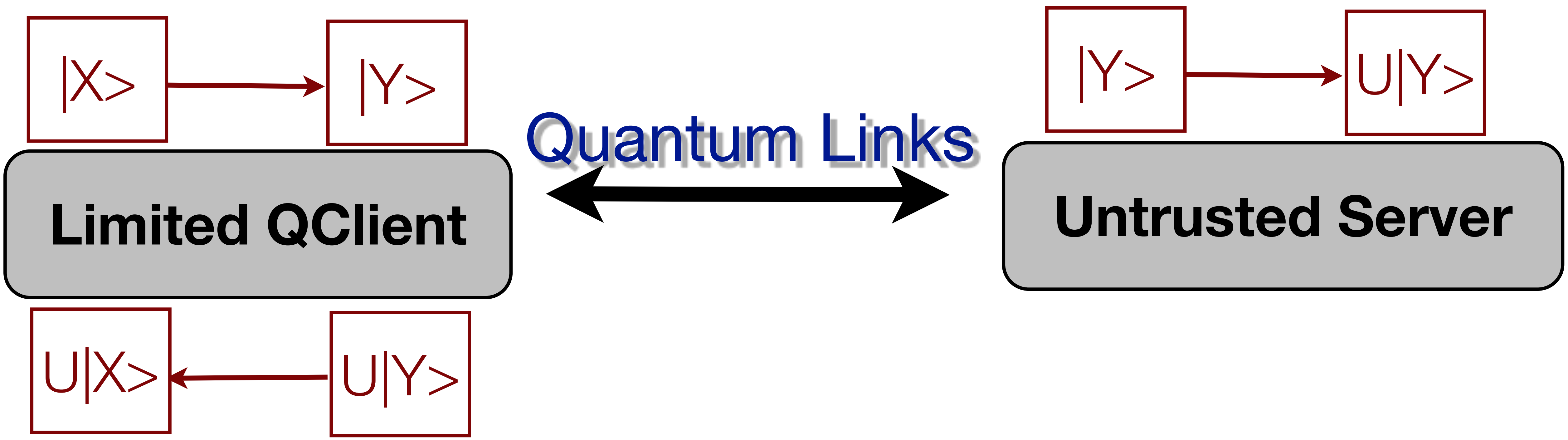
# Secure Quantum access to Quantum Cloud



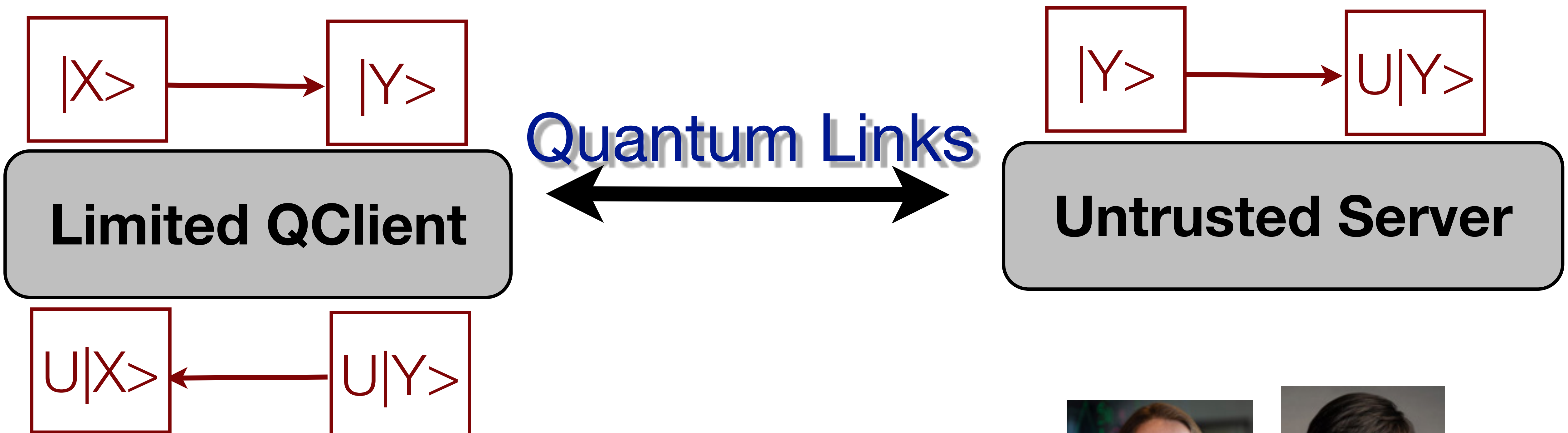
# Secure Quantum access to Quantum Cloud



# Secure Quantum access to Quantum Cloud



# Secure Quantum access to Quantum Cloud




Broadbent, Fitzsimons, and Kashefi 2009 - Universal Blind Quantum Computing

Informational security

# Secure Quantum access to Quantum Cloud

**QKD** for encoding

|X> → |Y>

**Limited QClient**

U|X> ← U|Y>

Quantum Links

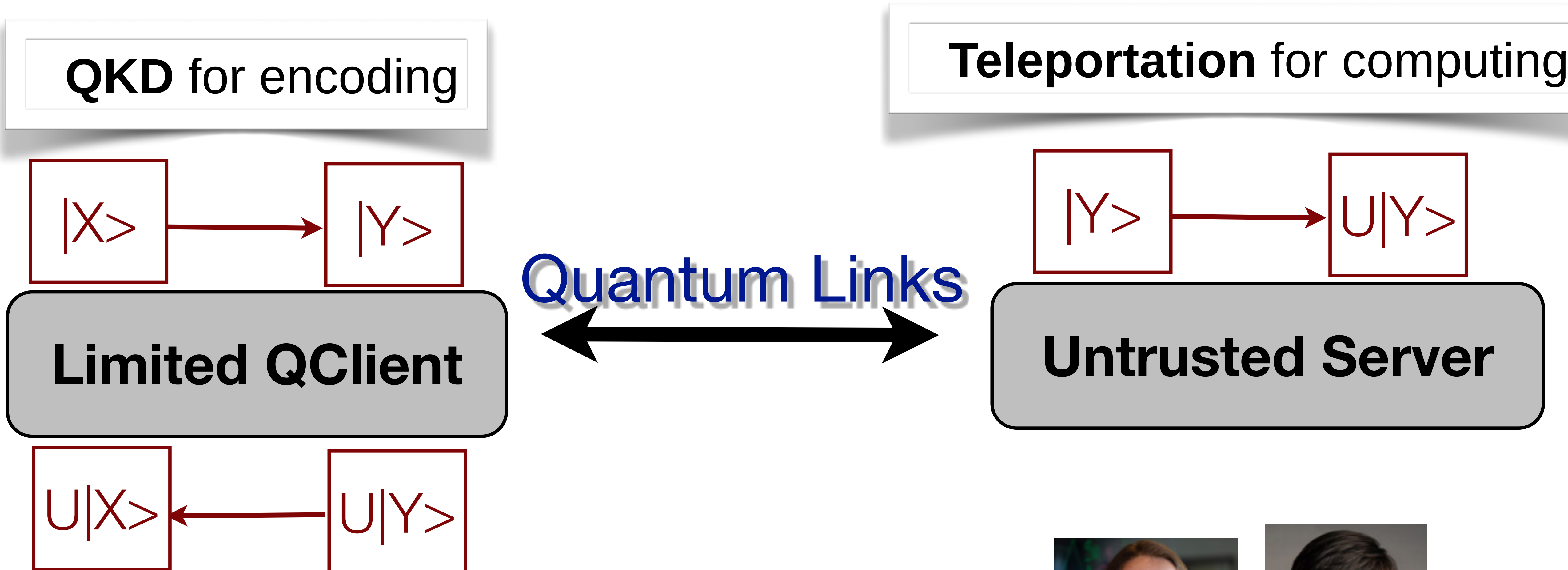
|Y> → U|Y>

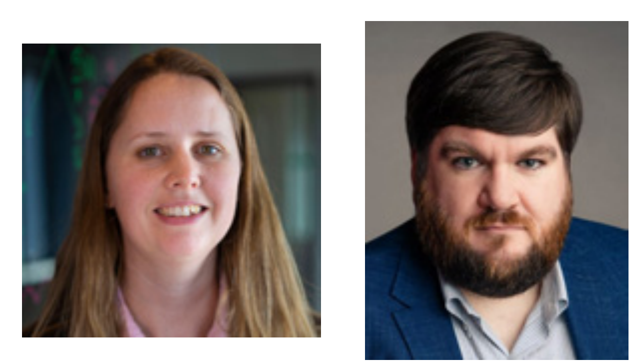
**Untrusted Server**

Broadbent, Fitzsimons, and Kashefi 2009 - Universal Blind Quantum Computing

Informational security

# Secure Quantum access to Quantum Cloud



Broadbent, Fitzsimons, and Kashefi 2009 - Universal Blind Quantum Computing

Informational security

# Secure Quantum access to Quantum Cloud

**QKD** for encoding

|X> → |Y>

**Limited QClient**

U|X> ← U|Y>

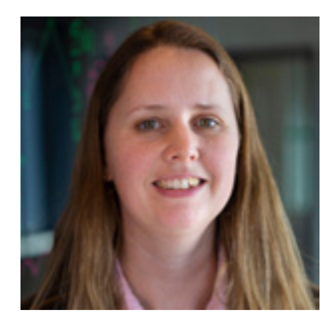
**Testing** for verification

Quantum Links

**Teleportation** for computing

|Y> → U|Y>

**Untrusted Server**



Broadbent, Fitzsimons, and Kashefi 2009 - Universal Blind Quantum Computing

Informational security

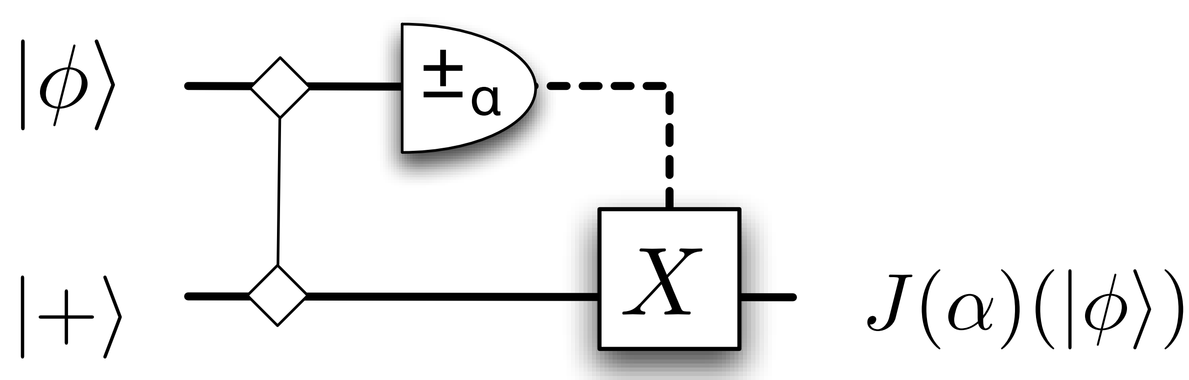
# Computing with Teleportation

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

# Computing with Teleportation

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

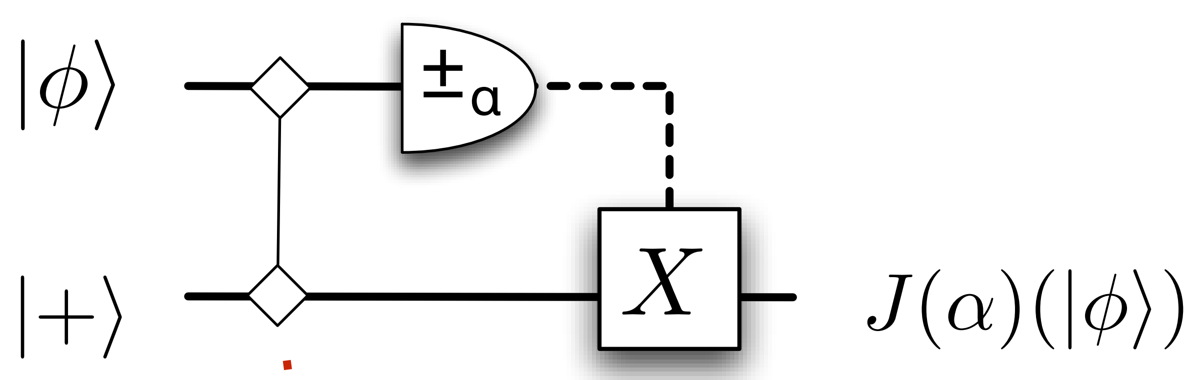
**gate teleportation**



# Computing with Teleportation

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

**gate teleportation**



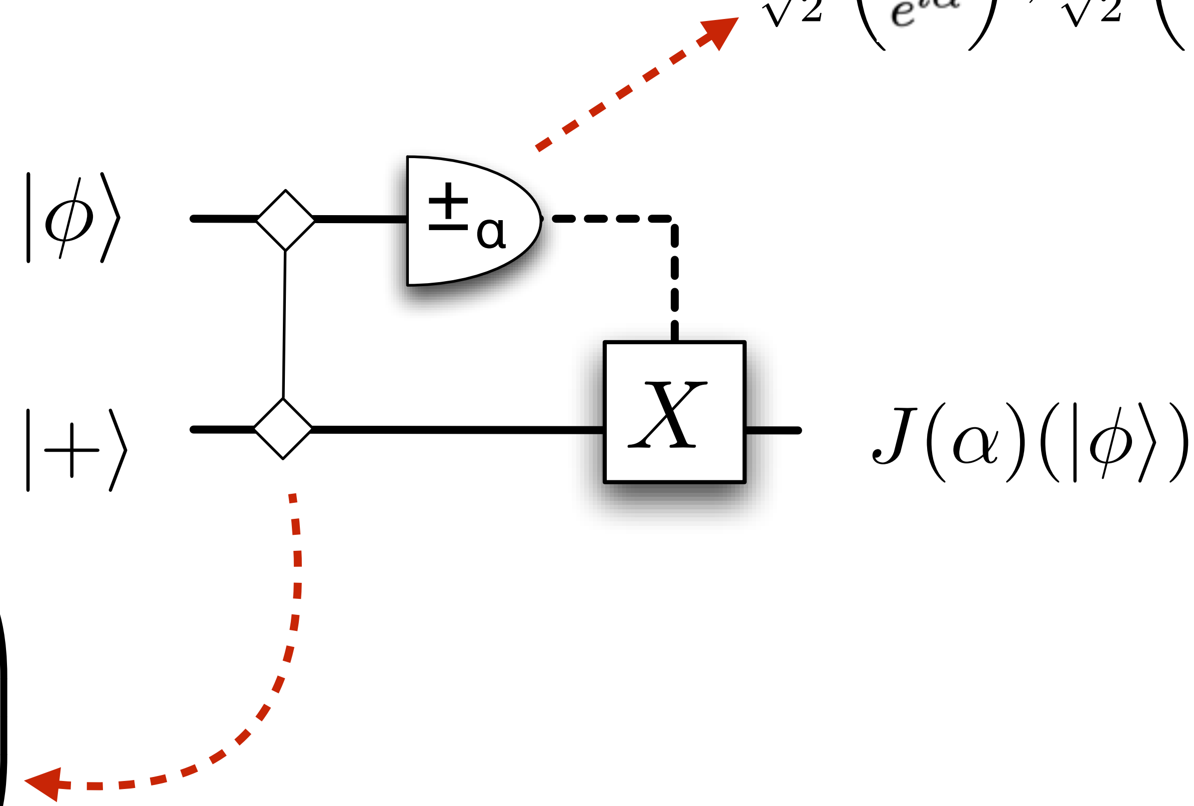

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

# Computing with Teleportation

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

**gate teleportation**

$$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ e^{i\alpha} \end{pmatrix}, \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -e^{i\alpha} \end{pmatrix}$$



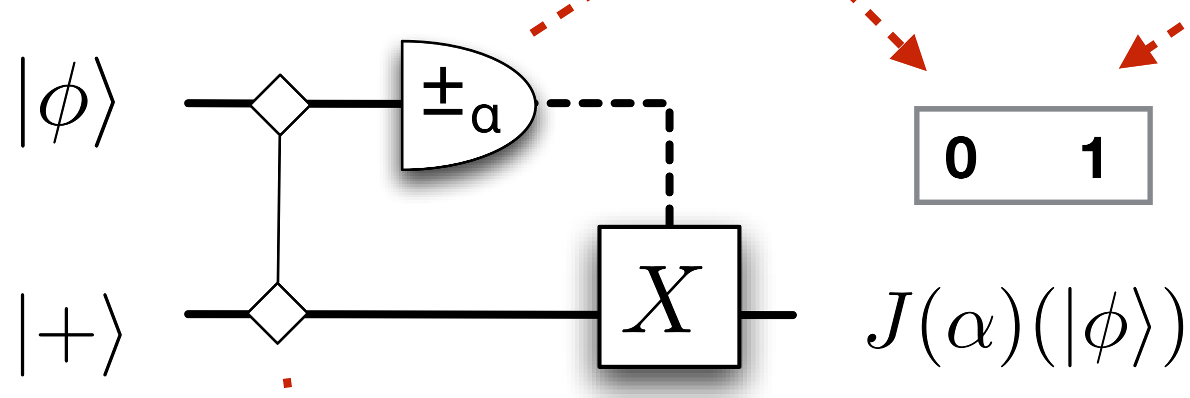

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

# Computing with Teleportation

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

**gate teleportation**

$$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ e^{i\alpha} \end{pmatrix}, \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -e^{i\alpha} \end{pmatrix}$$



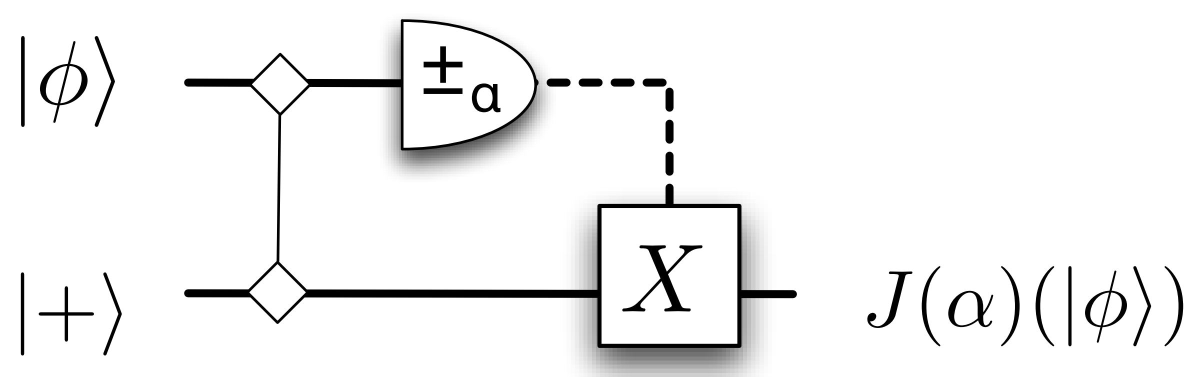

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

# Hiding with Teleportation

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

Single qubit rotation

Quantum Computer

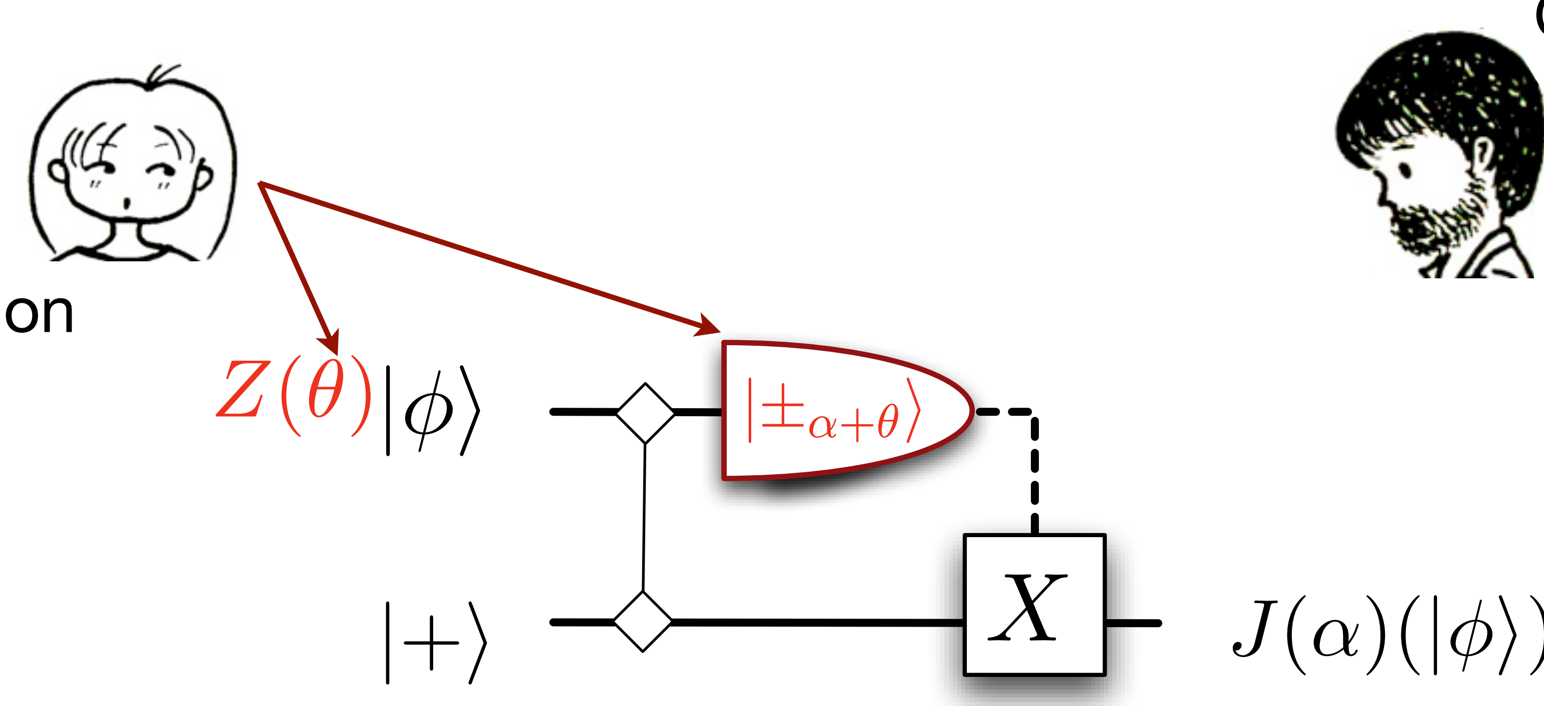


# Hiding with Teleportation

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

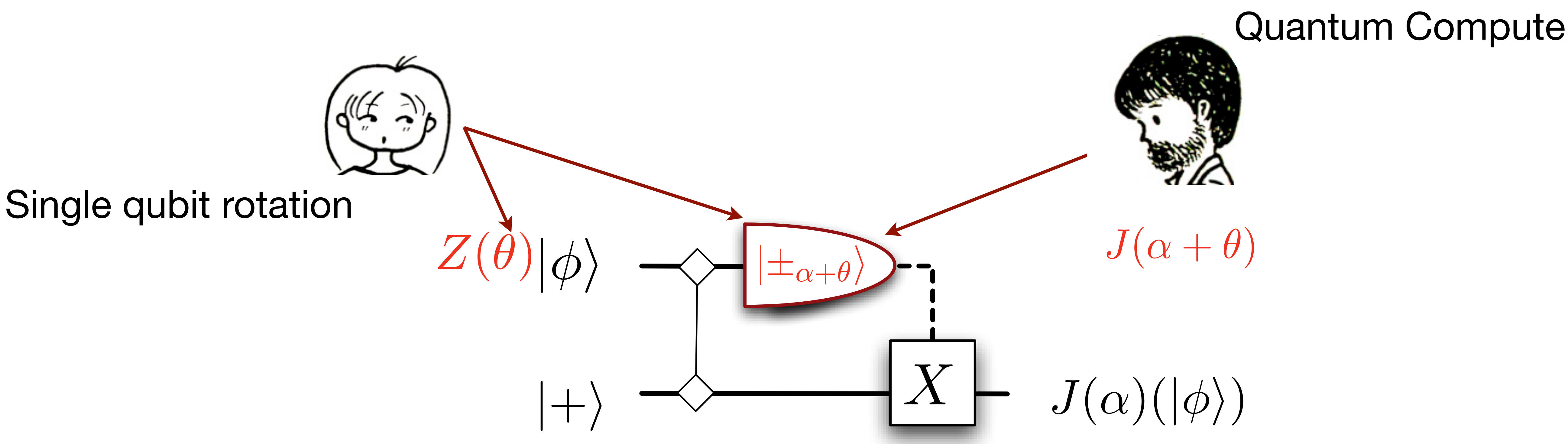
Quantum Computer

Single qubit rotation



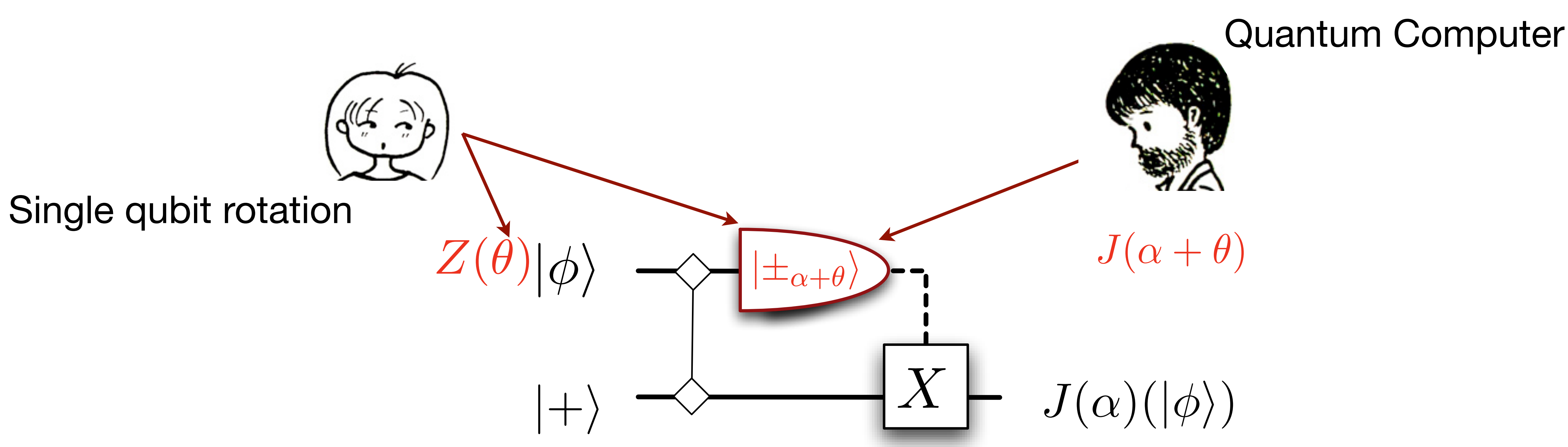
# Hiding with Teleportation

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



# Hiding with Teleportation

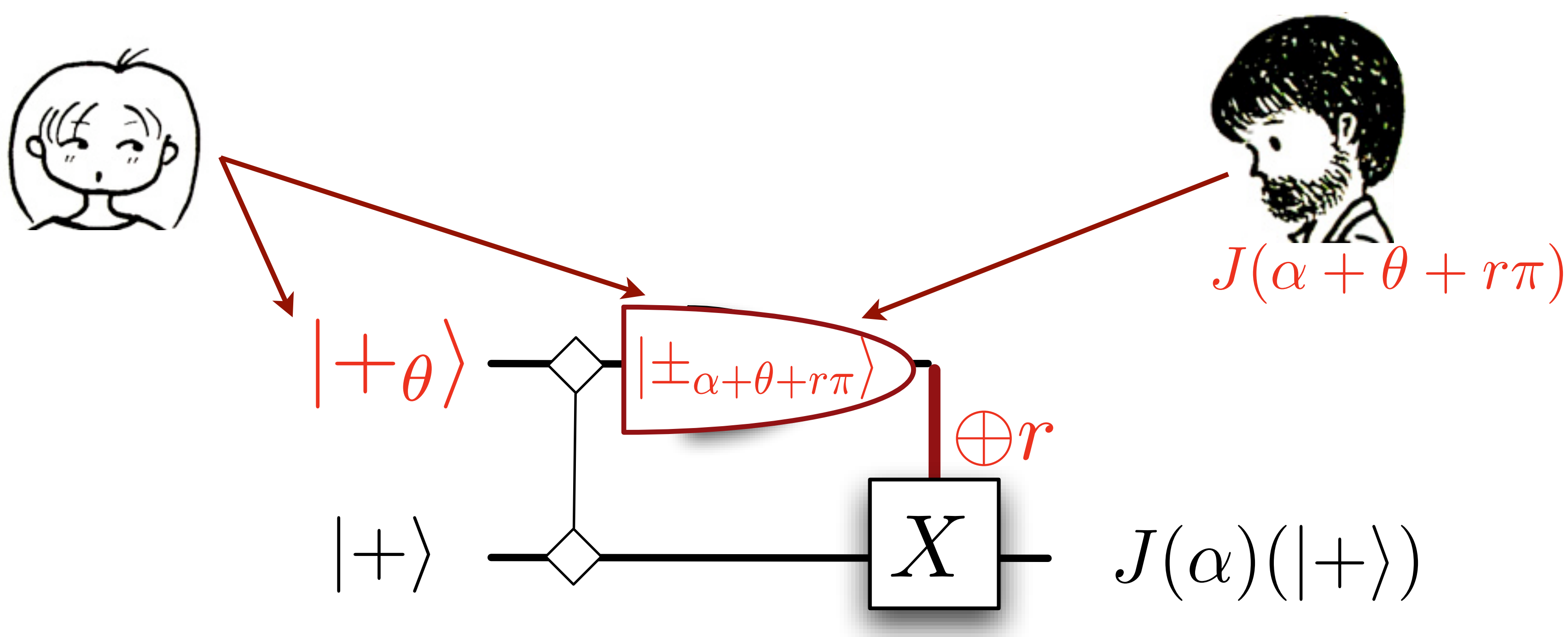
$$J(\alpha) \;:=\; \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & e^{i\alpha} \\ 1 & -e^{i\alpha} \end{pmatrix}$$




Hiding the Angles

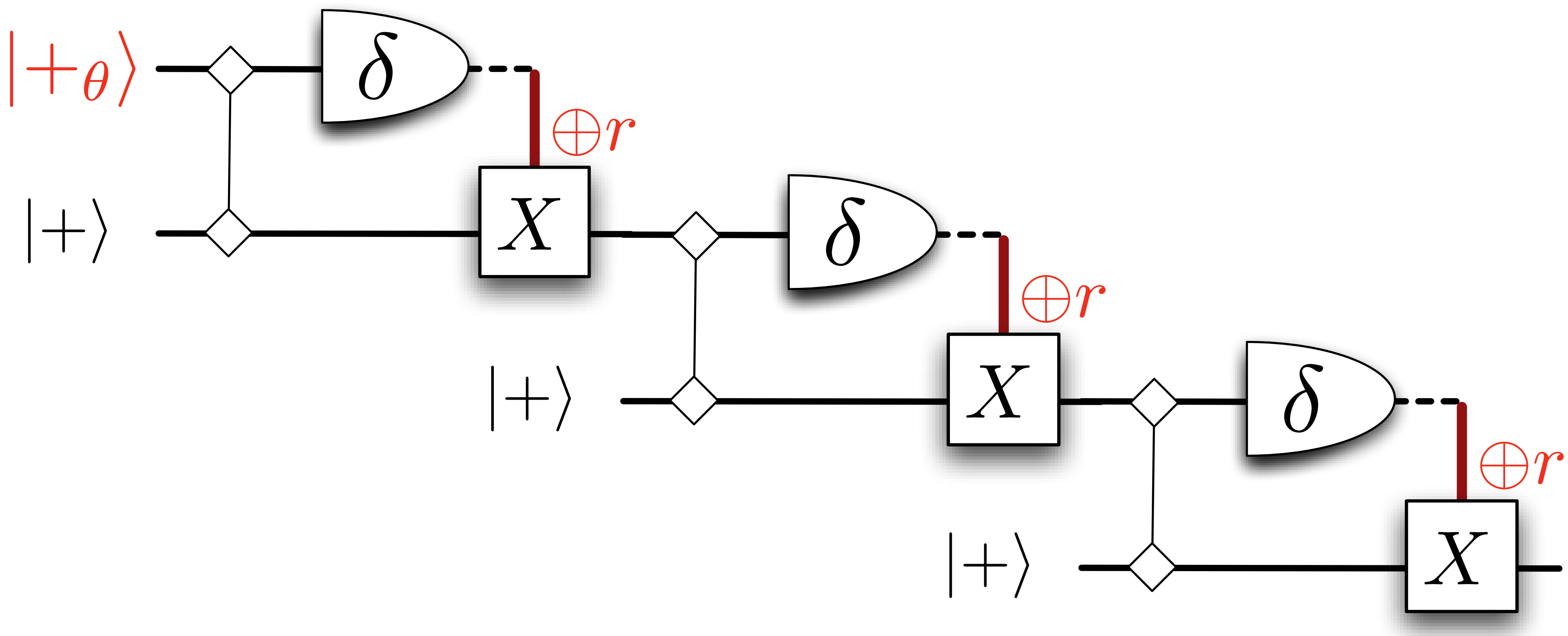
# Hiding with Teleportation

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

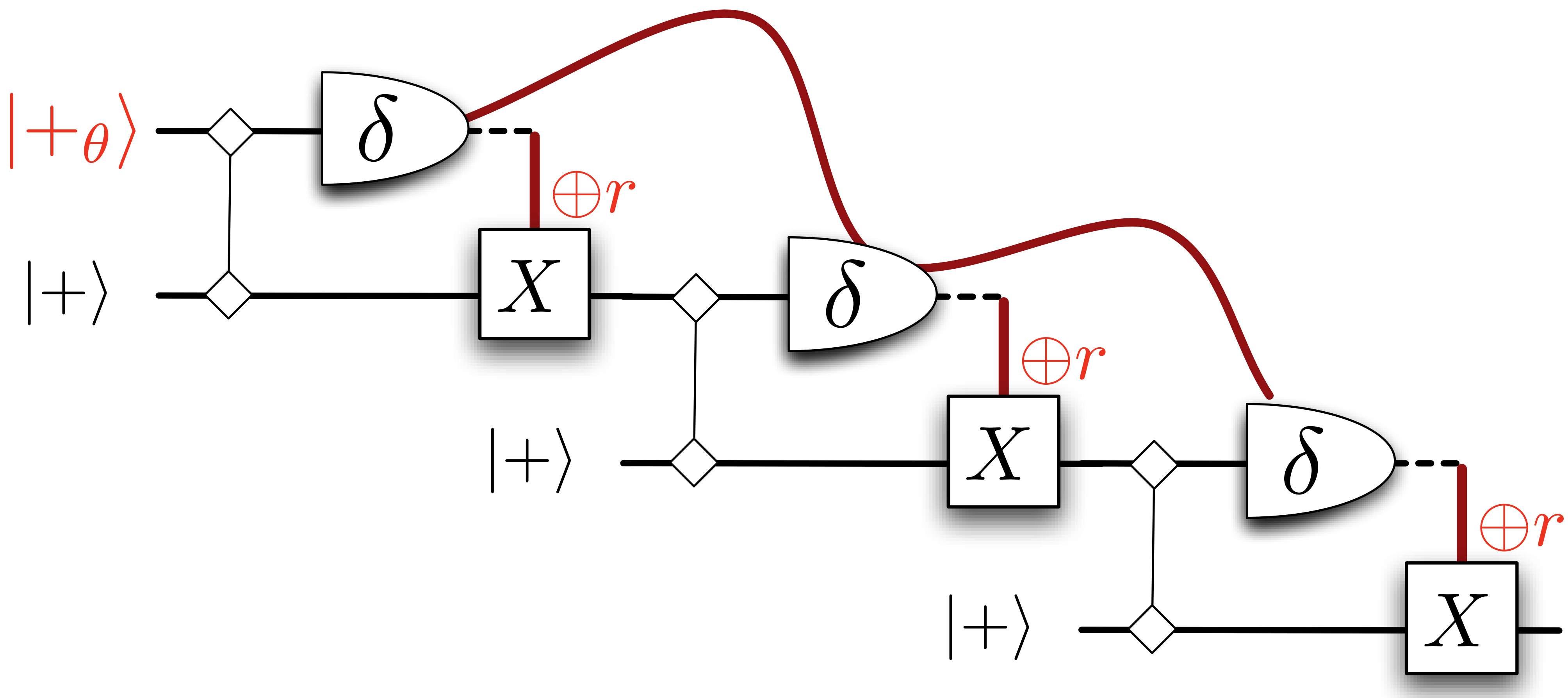



Hiding the measurement result

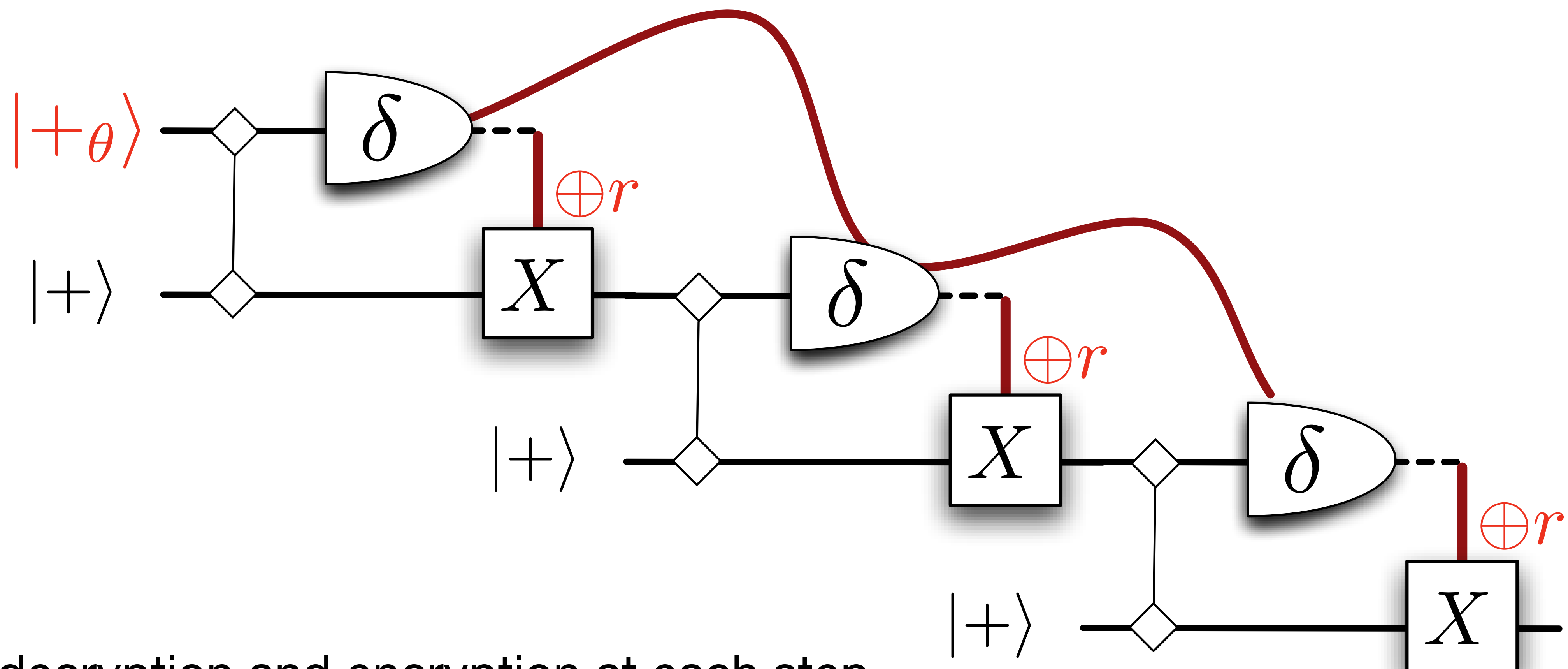
# Gates Composition



# Gates Composition



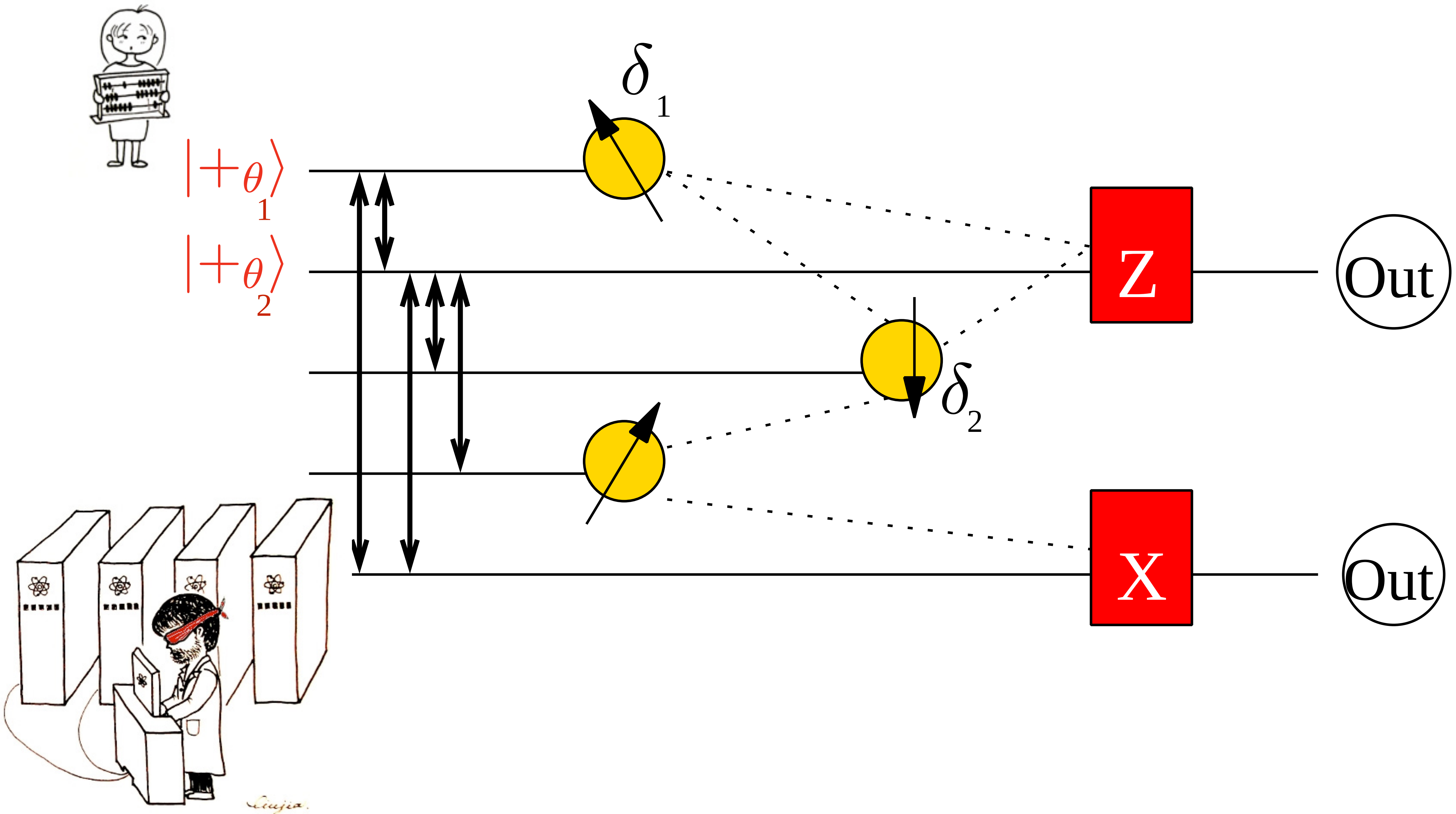
# Gates Composition



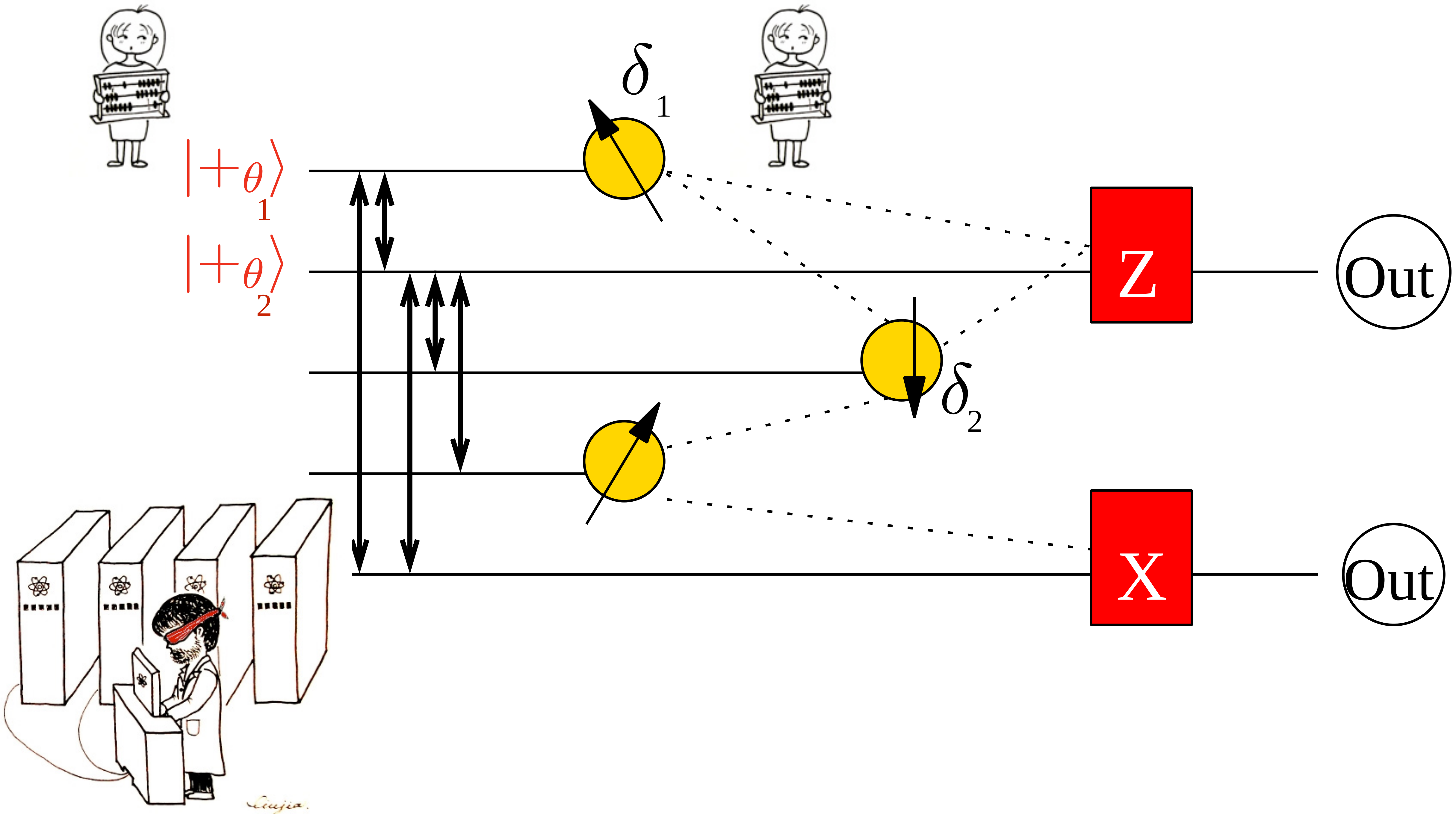

Perfect decryption and encryption at each step

Client-Server interactions

# Re-writing



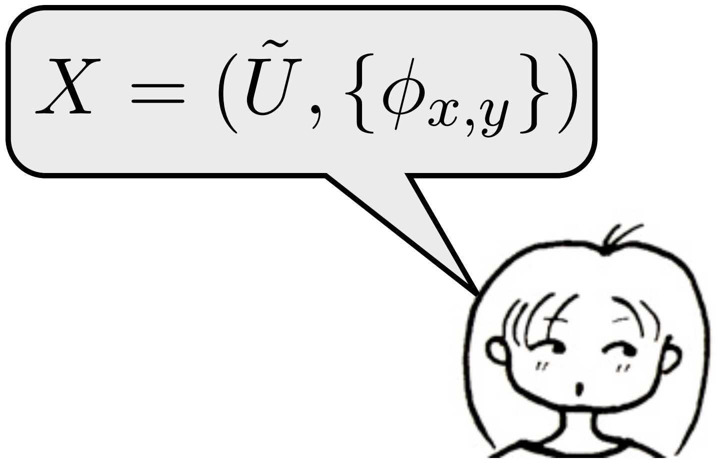
# Re-writing



# Universal Blind Quantum Computings

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

# Universal Blind Quantum Computings

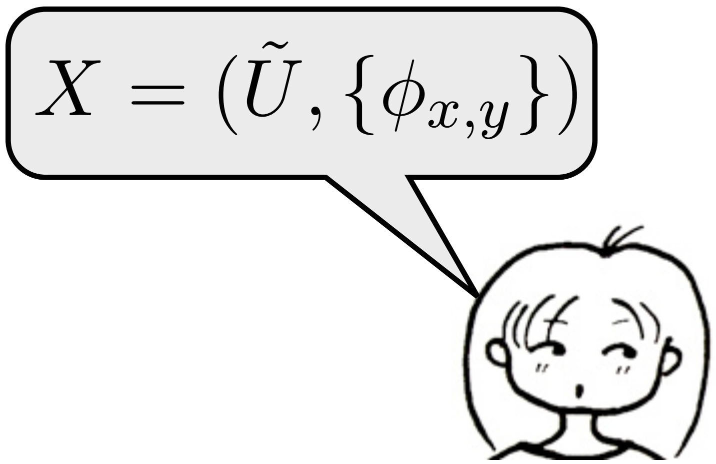


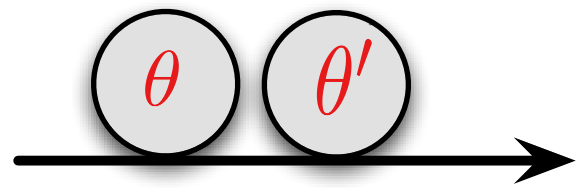

*random single qubit  generator*

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

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

# Universal Blind Quantum Computings



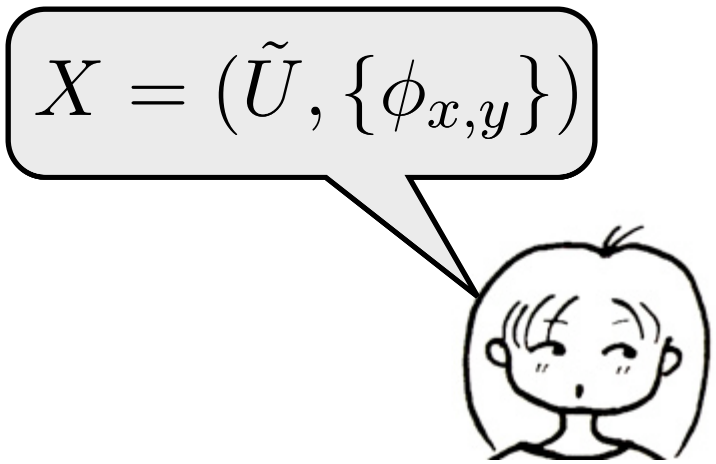




*random single qubit generator*

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

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

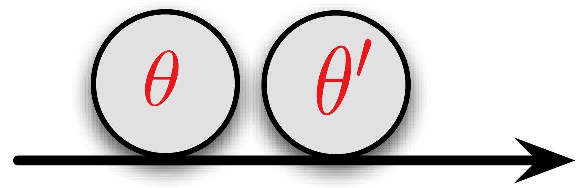
# Universal Blind Quantum Computings

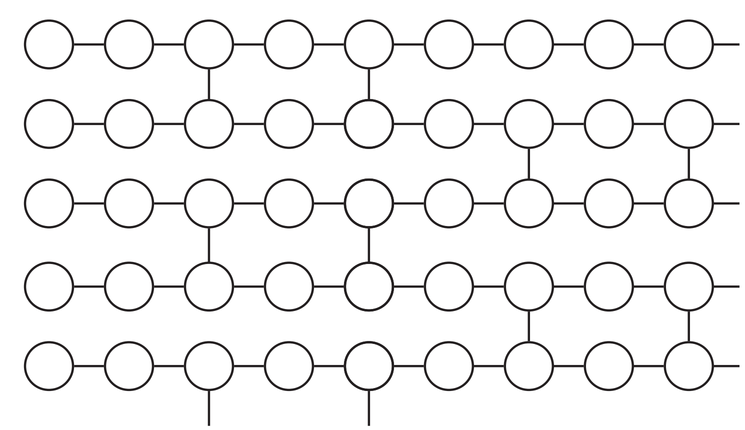



*random single qubit generator*

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

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



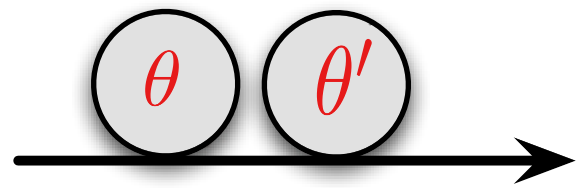
# Universal Blind Quantum Computings

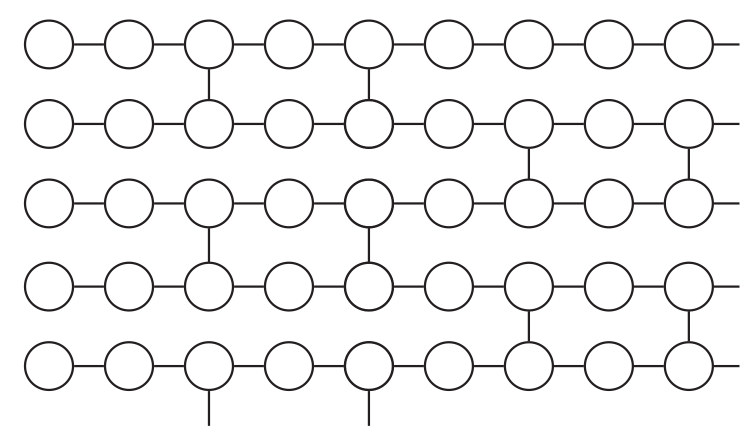
$$X = (\tilde{U}, \{\phi_{x,y}\})$$

*random single qubit generator*

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

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



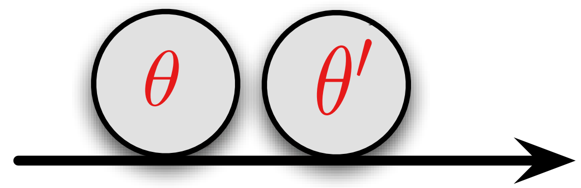



$$r_{x,y} \in_R \{0,1\}$$

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

# Universal Blind Quantum Computings

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




*random single qubit generator*

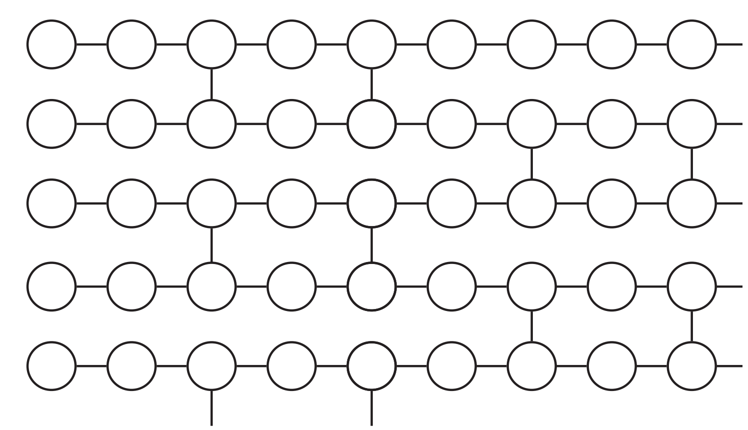
$$1/\sqrt{2}\left(|0\rangle + e^{i\theta}|1\rangle\right)$$

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

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

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

$$\delta_{x,y}$$



# Universal Blind Quantum Computings

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

$\theta$ $\theta'$

*random single qubit generator*

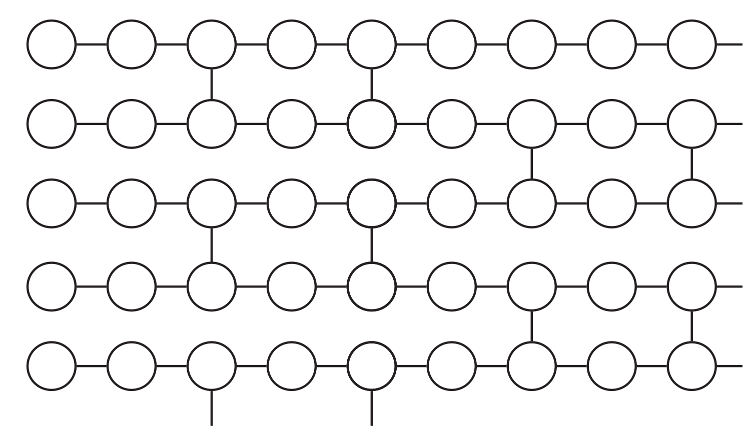
$$1/\sqrt{2}\left(|0\rangle + e^{i\theta}|1\rangle\right)$$

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

$\delta_{x,y}$

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

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



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

# Universal Blind Quantum Computings

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

$\theta$ $\theta'$

*random single qubit generator*

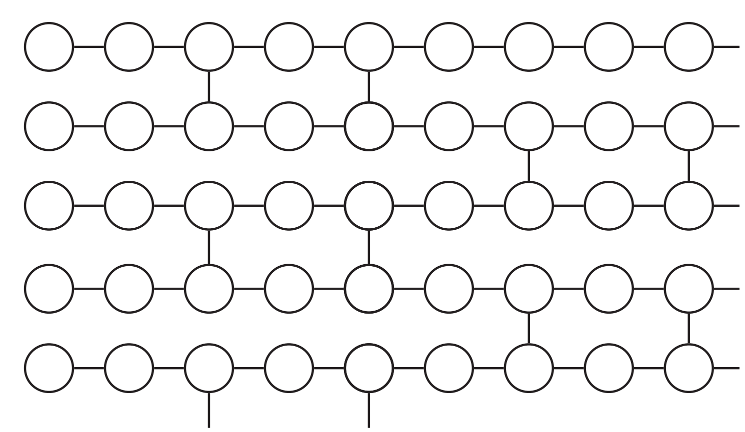
$$1/\sqrt{2}\left(|0\rangle + e^{i\theta}|1\rangle\right)$$

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

$\delta_{x,y}$

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

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



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

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

# Universal Blind Quantum Computings

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

$\theta$ $\theta'$

random single qubit generator

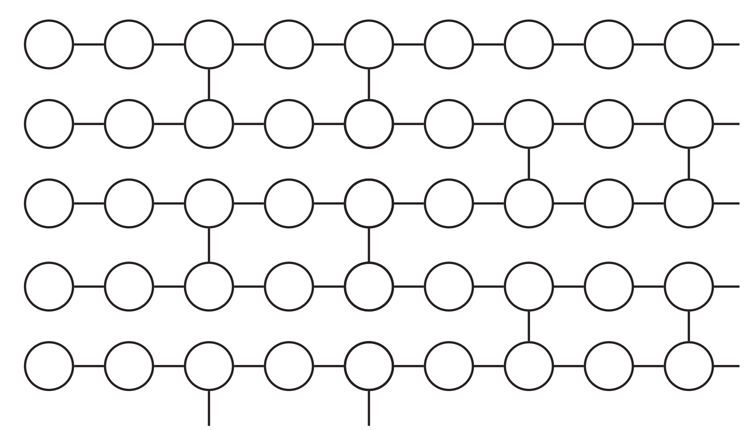
$$1/\sqrt{2}\left(|0\rangle + e^{i\theta}|1\rangle\right)$$

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

$\delta_{x,y}$

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

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



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

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

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

# Security Definition

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

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

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

# What about correctness ?

# What about correctness ?

- Correctness: in the absence of any deviation, client accepts and the output is correct

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

# Verification of Quantum Computing

**Self Testing 2005**

Decide if the physical devices simulate their specification

# Verification of Quantum Computing

**Single-prover prepare-and-send**

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

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

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

# Verification of Quantum Computing

**Single-prover receive-and-measure**

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

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

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

# Verification of Quantum Computing

**Multi-prover entanglement-based**

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

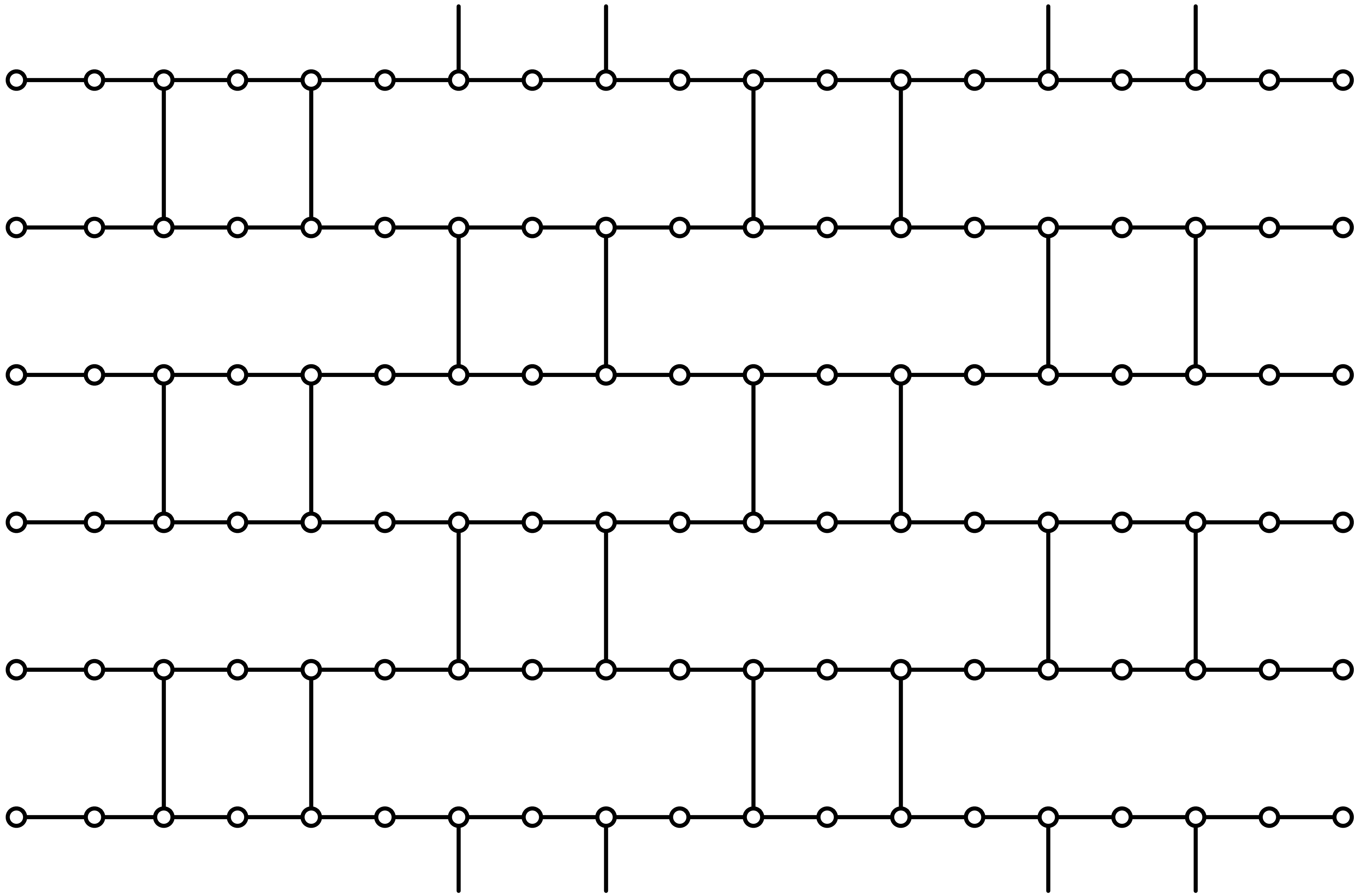
- CHSH game Rigidity
- Self-testing graph states
- Pauli Braiding

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

# Verification of Quantum Computing

Overhead
Noise
Scalability

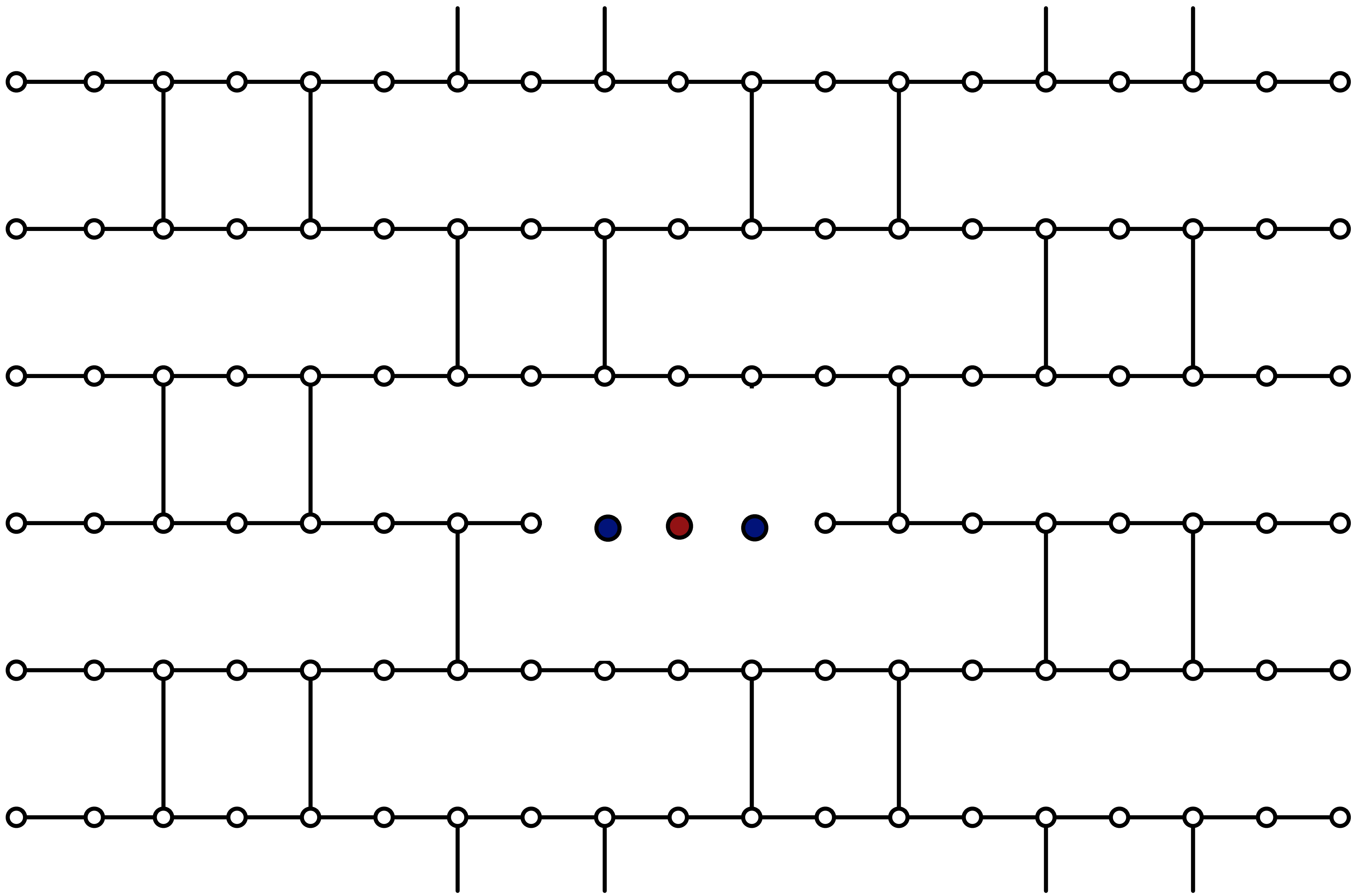
# Trapification



Unconditionally Verifiable Blind Quantum Computing

Fitzsioms Kashefi, 2012

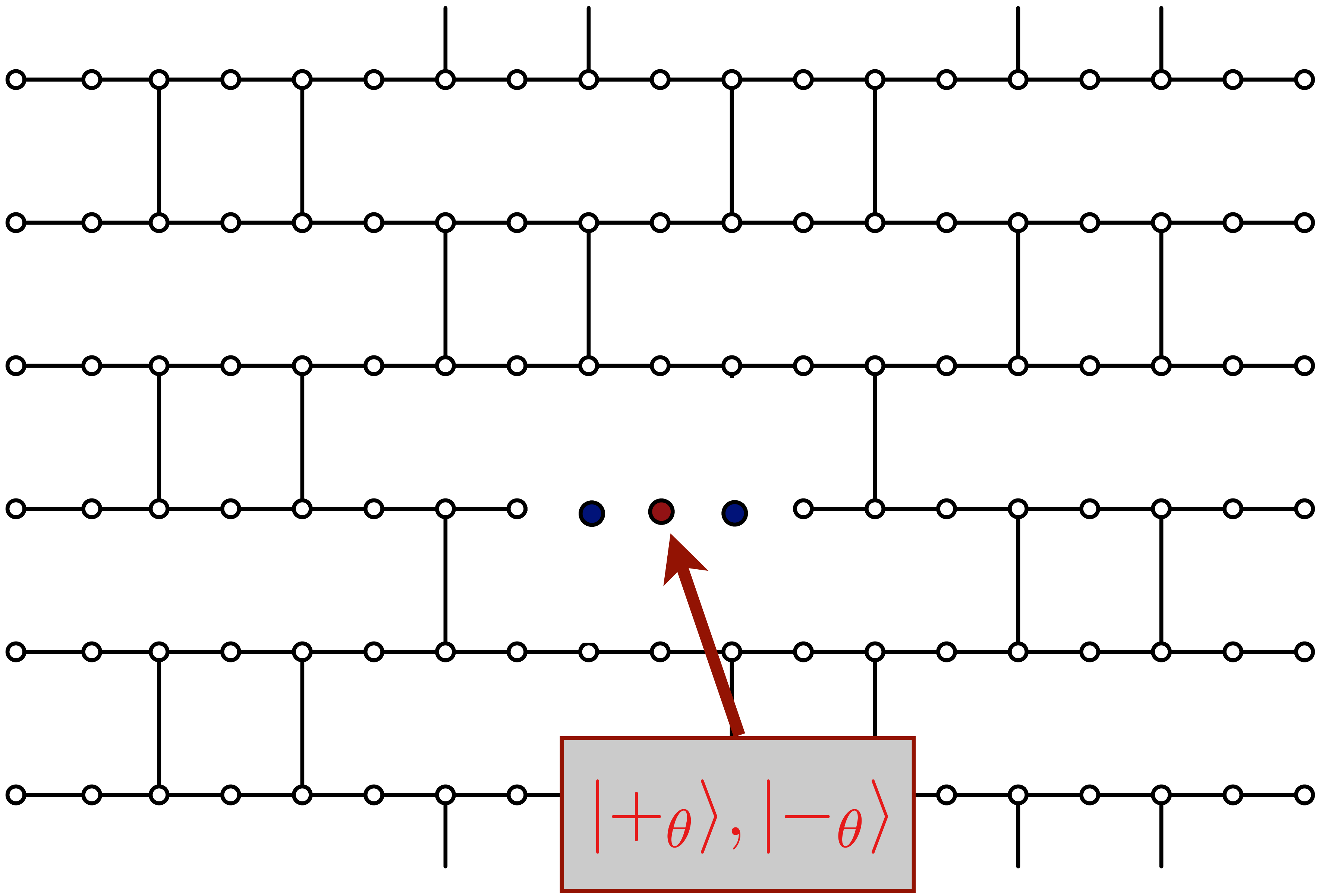
# Trapification



Unconditionally Verifiable Blind Quantum Computing

Fitzsioms Kashefi, 2012

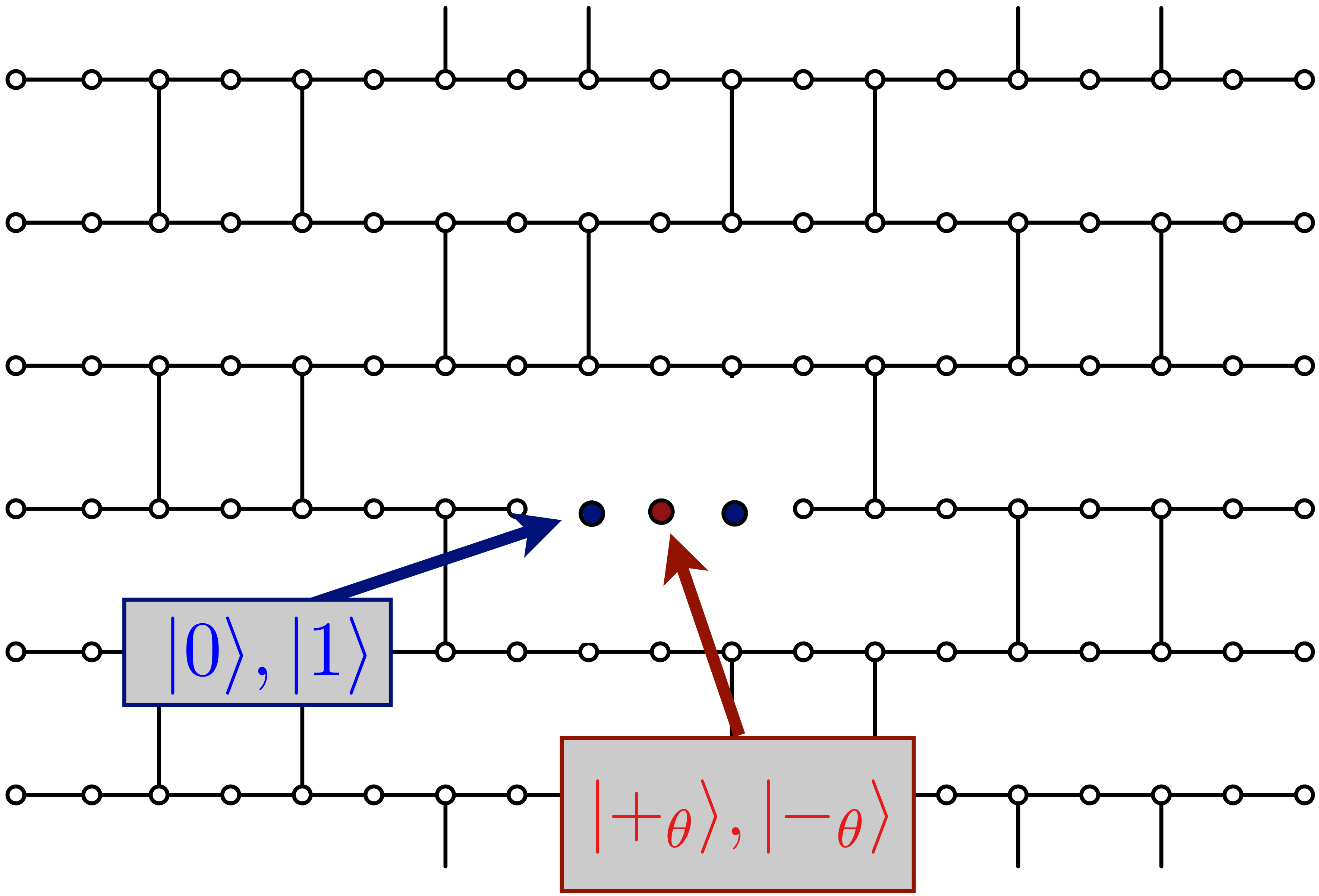
# Trapification




Unconditionally Verifiable Blind Quantum Computing

Fitzsioms Kashefi, 2012

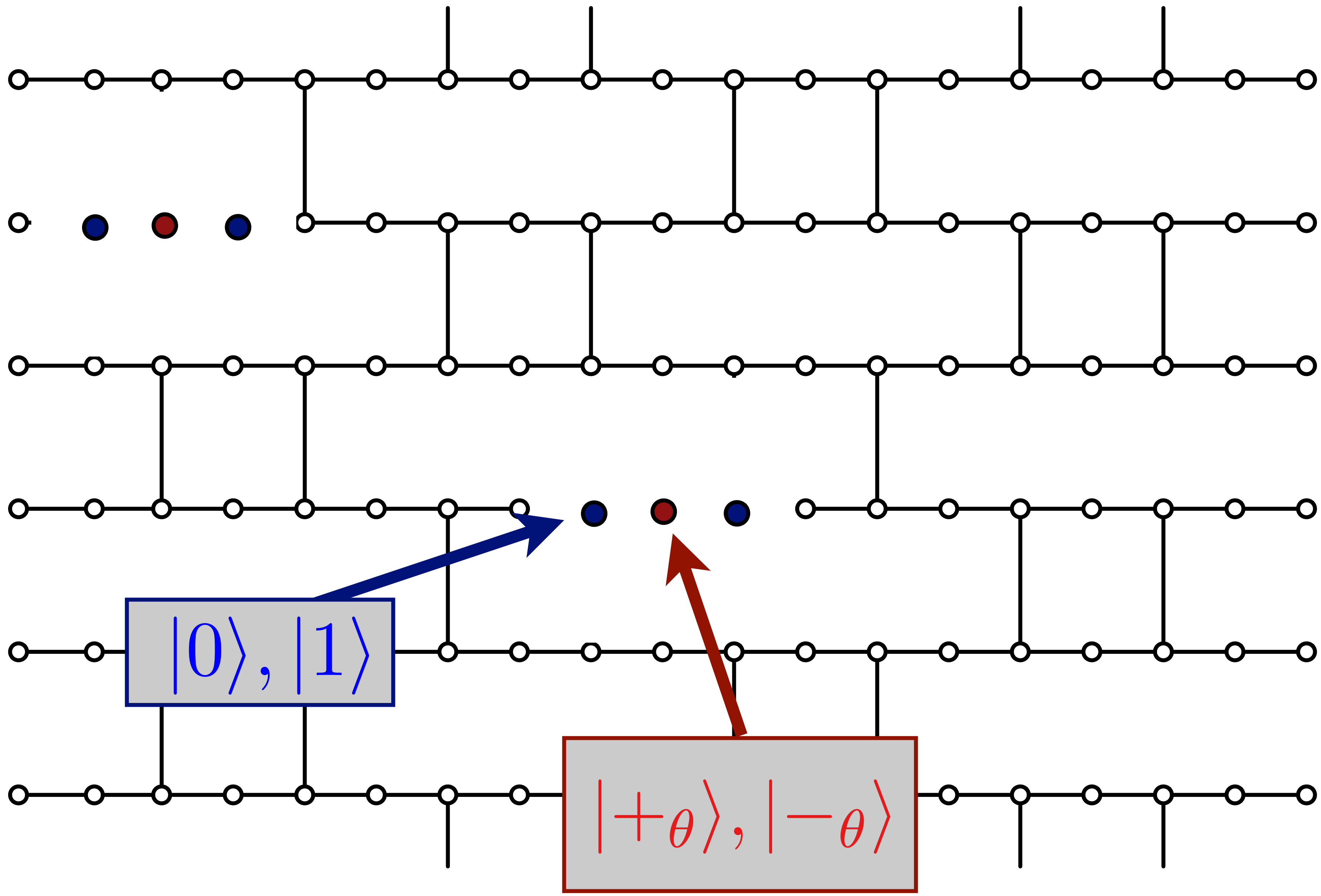
# Trapification




Unconditionally Verifiable Blind Quantum Computing

Fitzsioms Kashefi, 2012

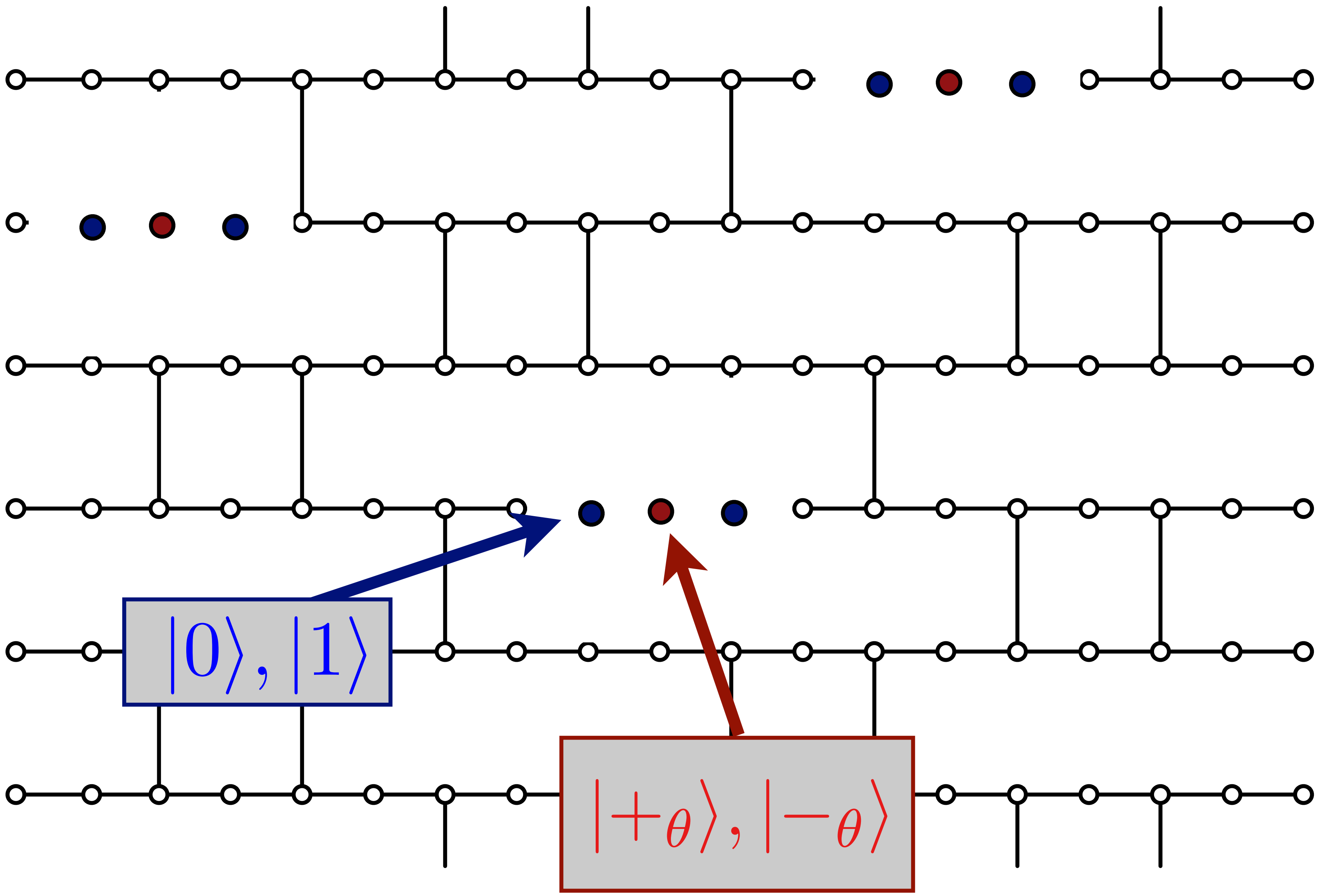
# Trapification




Unconditionally Verifiable Blind Quantum Computing

Fitzsioms Kashefi, 2012

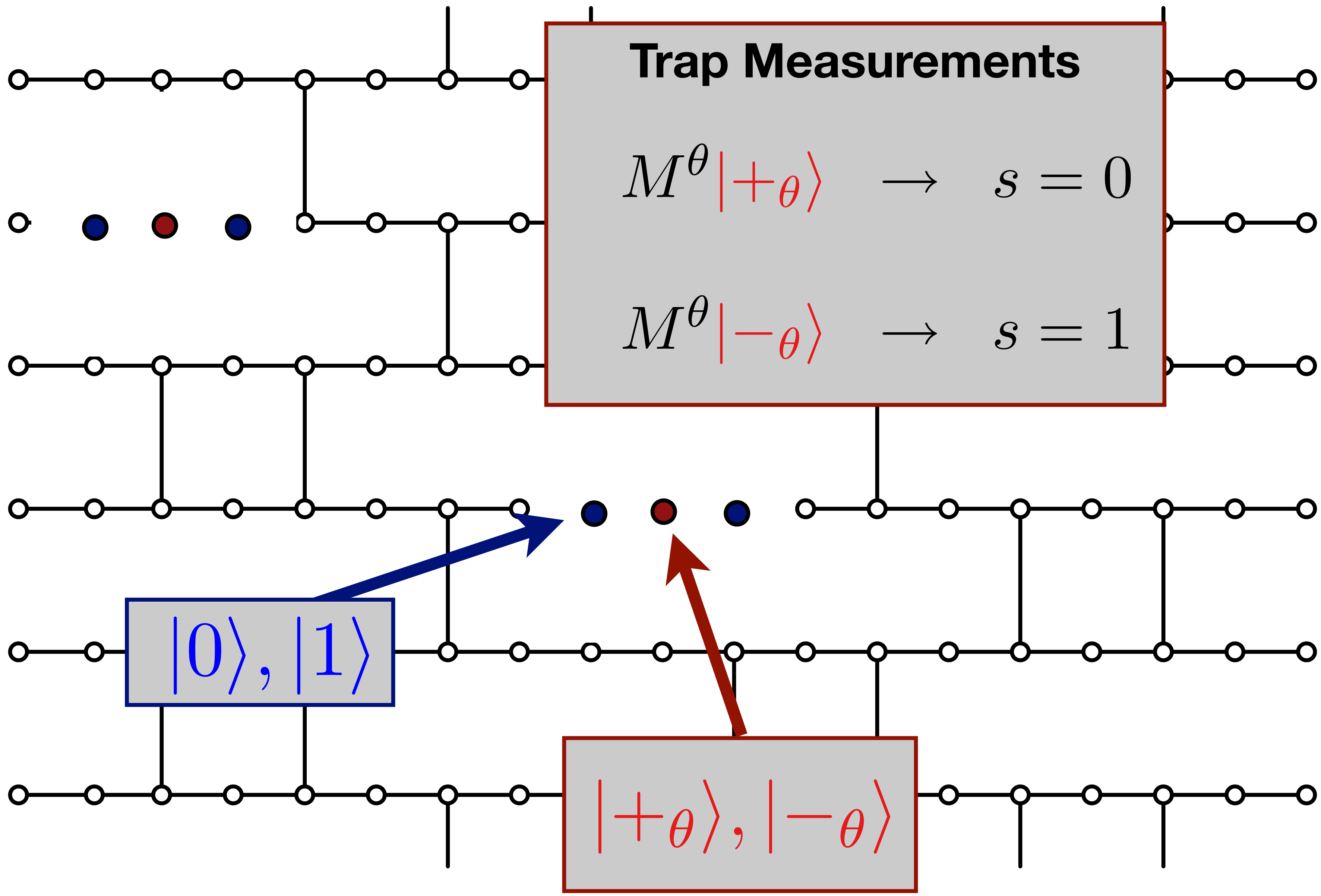
# Trapification




Unconditionally Verifiable Blind Quantum Computing

Fitzsioms Kashefi, 2012

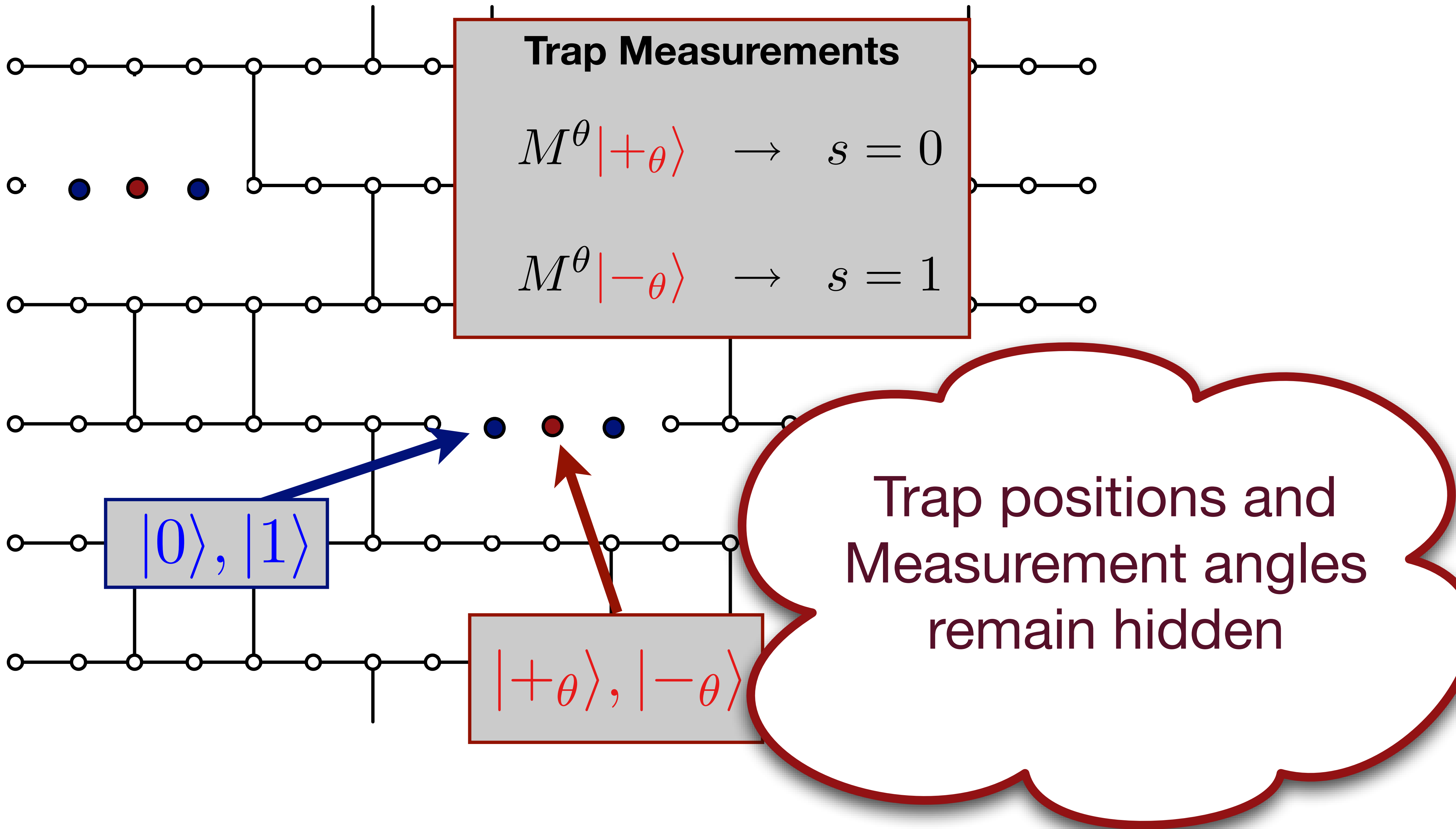
# Trapification




Unconditionally Verifiable Blind Quantum Computing

Fitzsioms Kashefi, 2012

# Trapification




Unconditionally Verifiable Blind Quantum Computing

Fitzsioms Kashefi, 2012

# Trapification

$$\Omega_{Eve,system}$$

# Trapification

$$\begin{array}{c}\boxed{\Omega_{Eve,system}}\\ \Big\downarrow \text{Security}\\ \boxed{\sigma_{testsubspace}}\end{array}$$

# Trapification

$$\Omega_{Eve,system}$$

$$\Big\downarrow \text{Security}$$

$$\sigma_{testsubspace}$$

**Trap Measurements**

$$M^{\theta}|+_{\theta}\rangle \quad \longrightarrow \quad s=0$$

$$M^{\theta}|-_{\theta}\rangle \quad \longrightarrow \quad s=1$$

# Trapification

$$\Omega_{Eve,system}$$

Security

$$\sigma_{testsubspace}$$

**Trap Measurements**

$$M^{\theta}|+_{\theta}\rangle \quad \rightarrow \quad s=0$$

$$M^{\theta}|-_{\theta}\rangle \quad \rightarrow \quad s=1$$

Prob trap being correct and
the computation is wrong is bounded

# Trapification

$$\Omega_{Eve,system}$$

Security ↓

$$\sigma_{testsubspace}$$

**Trap Measurements**

$$M^{\theta}|+_{\theta}\rangle \quad \longrightarrow \quad s=0$$

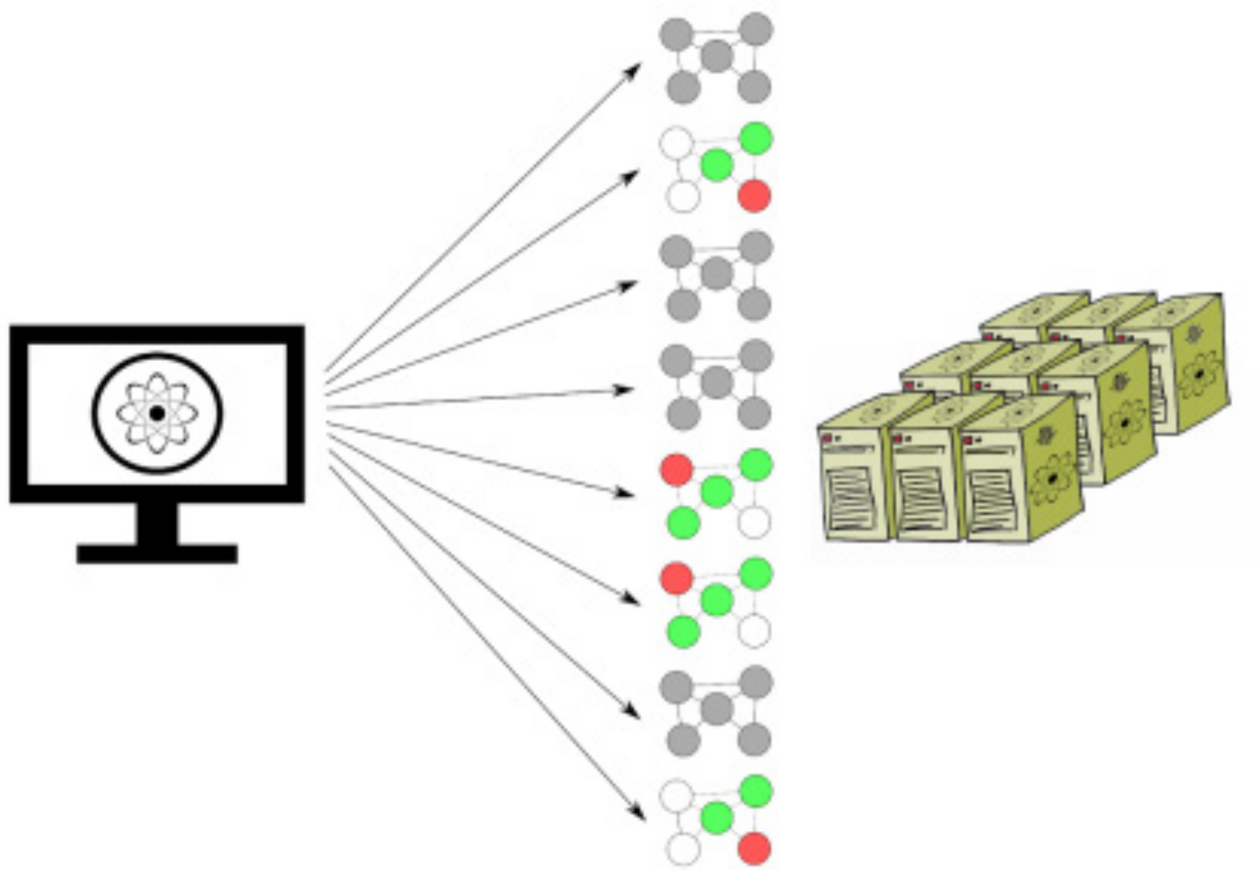
$$M^{\theta}|-_{\theta}\rangle \quad \longrightarrow \quad s=1$$

Prob trap being correct and
the computation is wrong is bounded

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

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

# Robust Verifiable Secure Quantum Access to Noisy Quantum Qloud



Classical input/output

Perfect blindness and exponential verification

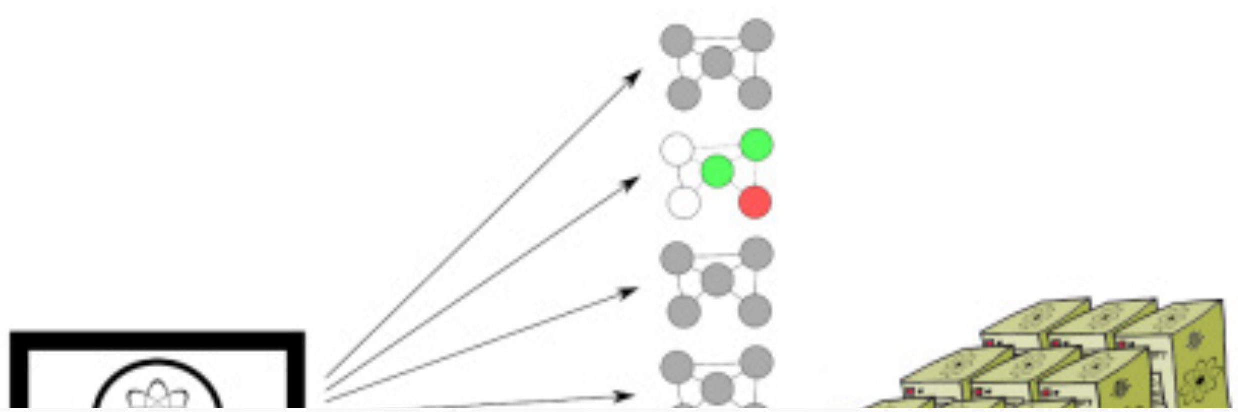
Exponential correctness on honest-but-noisy device

No overhead  besides repetitions

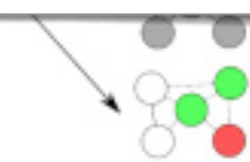
Securing Quantum Computations in the NISQ Era

*Kashefi, Leichtle, Music, Ollivier, 2020*

# Robust Verifiable Secure Quantum Access to Noisy Quantum Qloud



## ✓ Practical Efficient Honest Client - Malicious Server



Classical input/output

Perfect blindness and exponential verification

Exponential correctness on honest-but-noisy device

No overhead  besides repetitions

Securing Quantum Computations in the NISQ Era

*Kashefi, Leichtle, Music, Ollivier, 2020*

# Robust Verifiable Secure Quantum Access to Noisy Quantum Qloud

✓ Practical Efficient Honest Client - Malicious Server

Classical input/output

Perfect blindness and exponential verification

Exponential correctness on honest-but-noisy device

No overhead  besides repetitions

Securing Quantum Computations in the NISQ Era

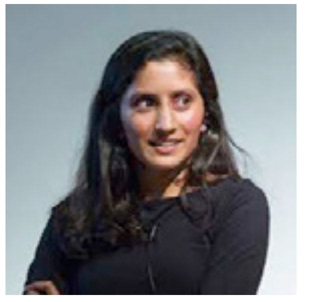
*Kashefi, Leichtle, Music, Ollivier, 2020*

# Secure Classical Access to Quantum Cloud

# Computationally Secure (Post-quantum safe) Classical Access to Quantum Cloud ?

# Computationally Secure (Post-quantum safe) Classical Access to Quantum Cloud ?

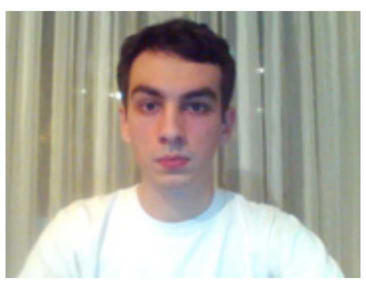
Classical Client Quantum FHE
Mahadev, FOCS 2018

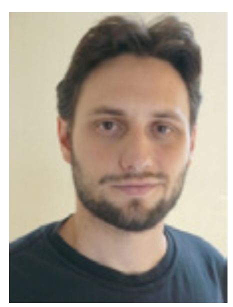


# Computationally Secure (Post-quantum safe) Classical Access to Quantum Cloud ?

Classical Client Quantum FHE
Mahadev, FOCS 2018

Delegated Pseudo-Secret Random Qubit Generator
Cojocaru, Colisson, Kashefi, Wallden, AsiaCrypt 2019

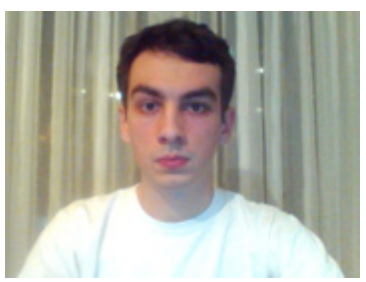


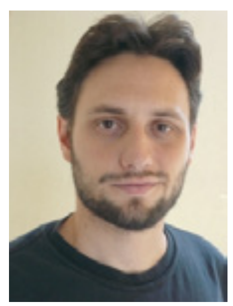


# Computationally Secure (Post-quantum safe) Classical Access to Quantum Cloud ?

Classical Client Quantum FHE
Mahadev, FOCS 2018

Delegated Pseudo-Secret Random Qubit Generator
Cojocaru, Colisson, Kashefi, Wallden, AsiaCrypt 2019



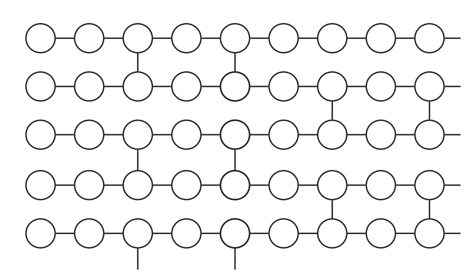


$X = (\tilde{U}, \{\phi_{x,y}\})$

$\theta$ $\theta'$

$\delta_{x,y}$

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



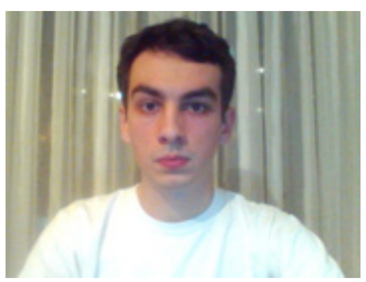
$s_{x,y} := s_{x,y} + r_{x,y}$ $s_{x,y} \in \{0,1\}$

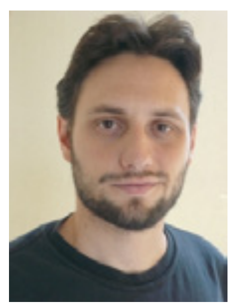
$\{|+_{\delta_{x,y}}\rangle, |-_{\delta_{x,y}}\rangle\}$

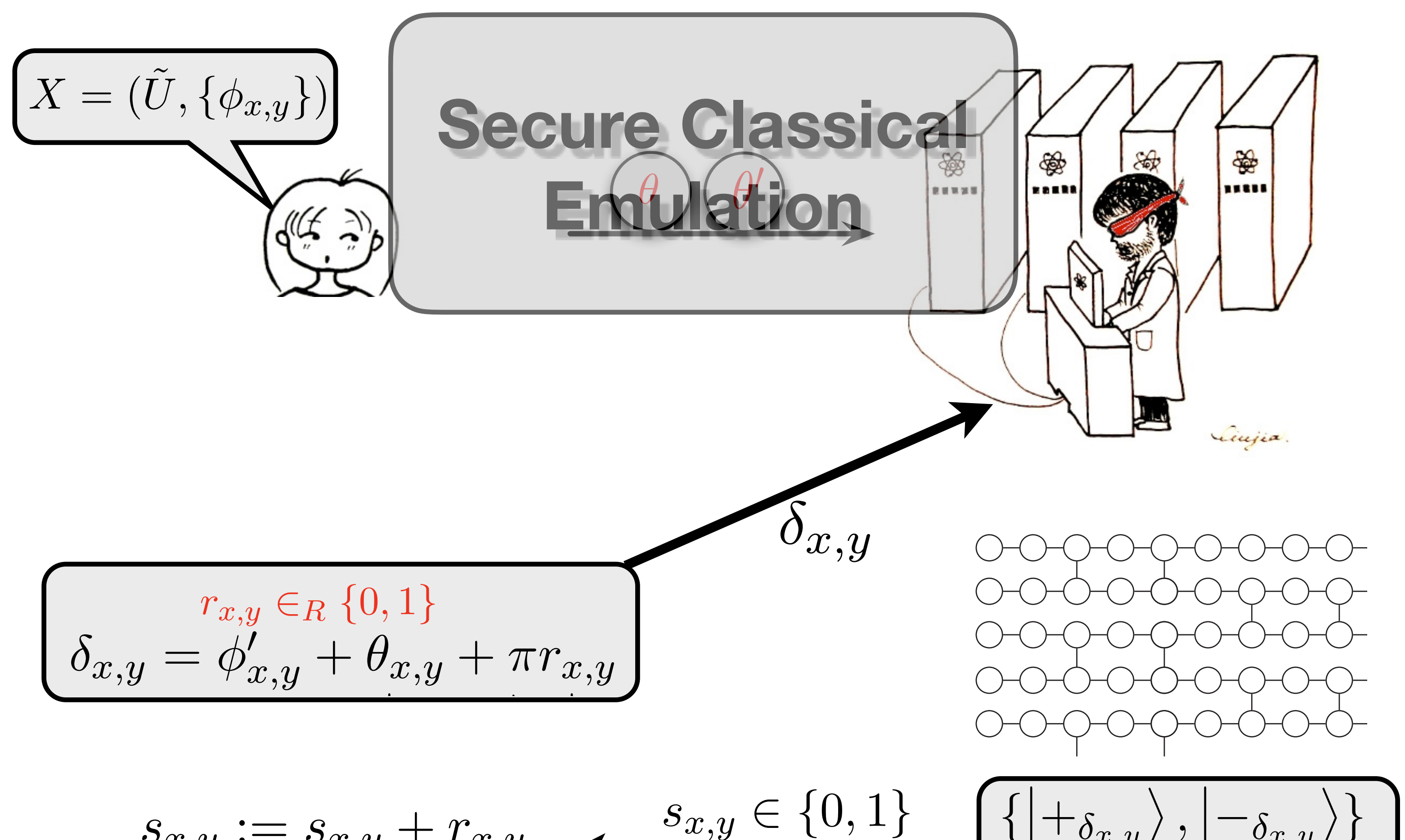
# Computationally Secure (Post-quantum safe) Classical Access to Quantum Cloud ?

Classical Client Quantum FHE
Mahadev, FOCS 2018

Delegated Pseudo-Secret Random Qubit Generator
Cojocaru, Colisson, Kashefi, Wallden, AsiaCrypt 2019



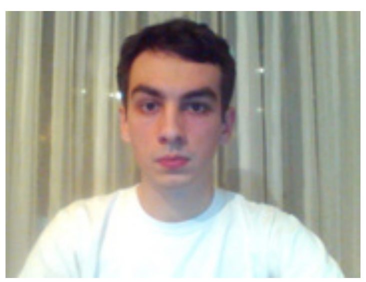


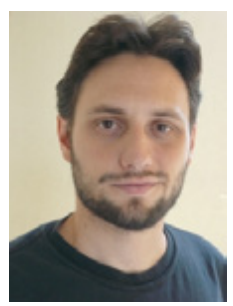


# Computationally Secure (Post-quantum safe) Classical Access to Quantum Cloud ?

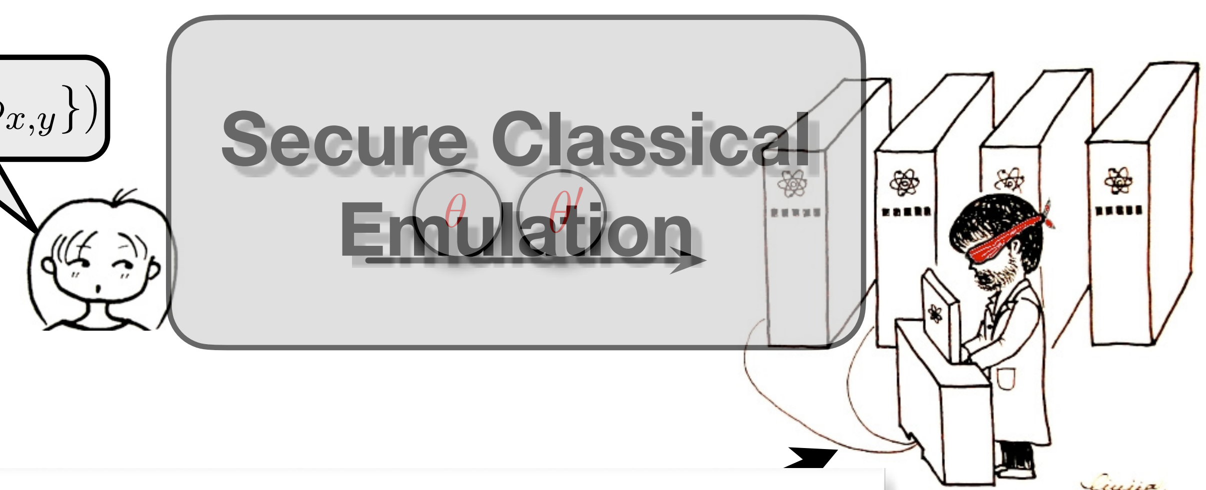
Classical Client Quantum FHE
Mahadev, FOCS 2018

Delegated Pseudo-Secret Random Qubit Generator
Cojocaru, Colisson, Kashefi, Wallden, AsiaCrypt 2019





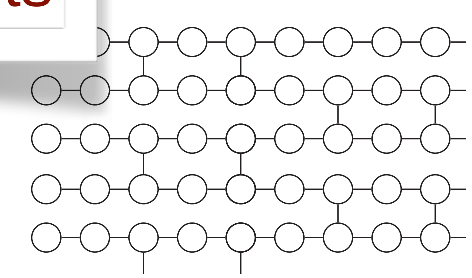
$X = (\tilde{U}, \{\phi_{x,y}\})$




*O(1000)* server qubits for randomising one single client qubits

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

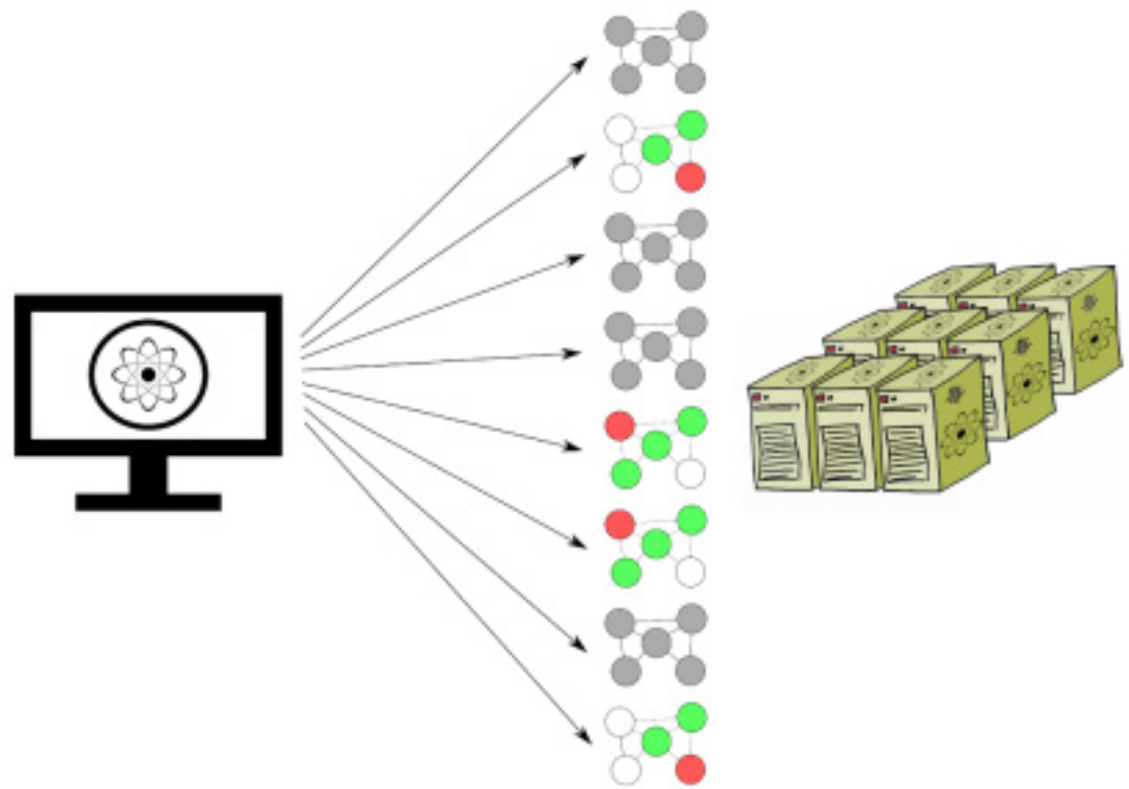
$\delta_{x,y} = \phi'_{x,y} + \theta_{x,y} + \pi r_{x,y}$

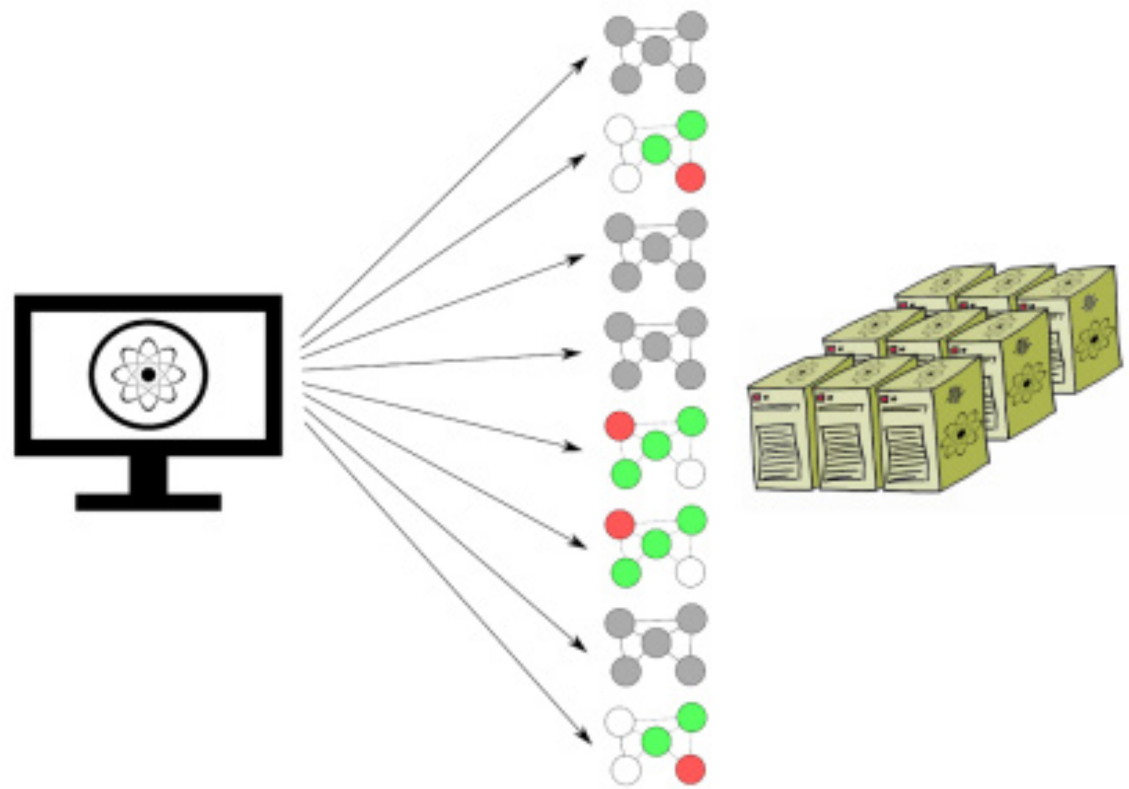


$s_{x,y} := s_{x,y} + r_{x,y}$

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

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



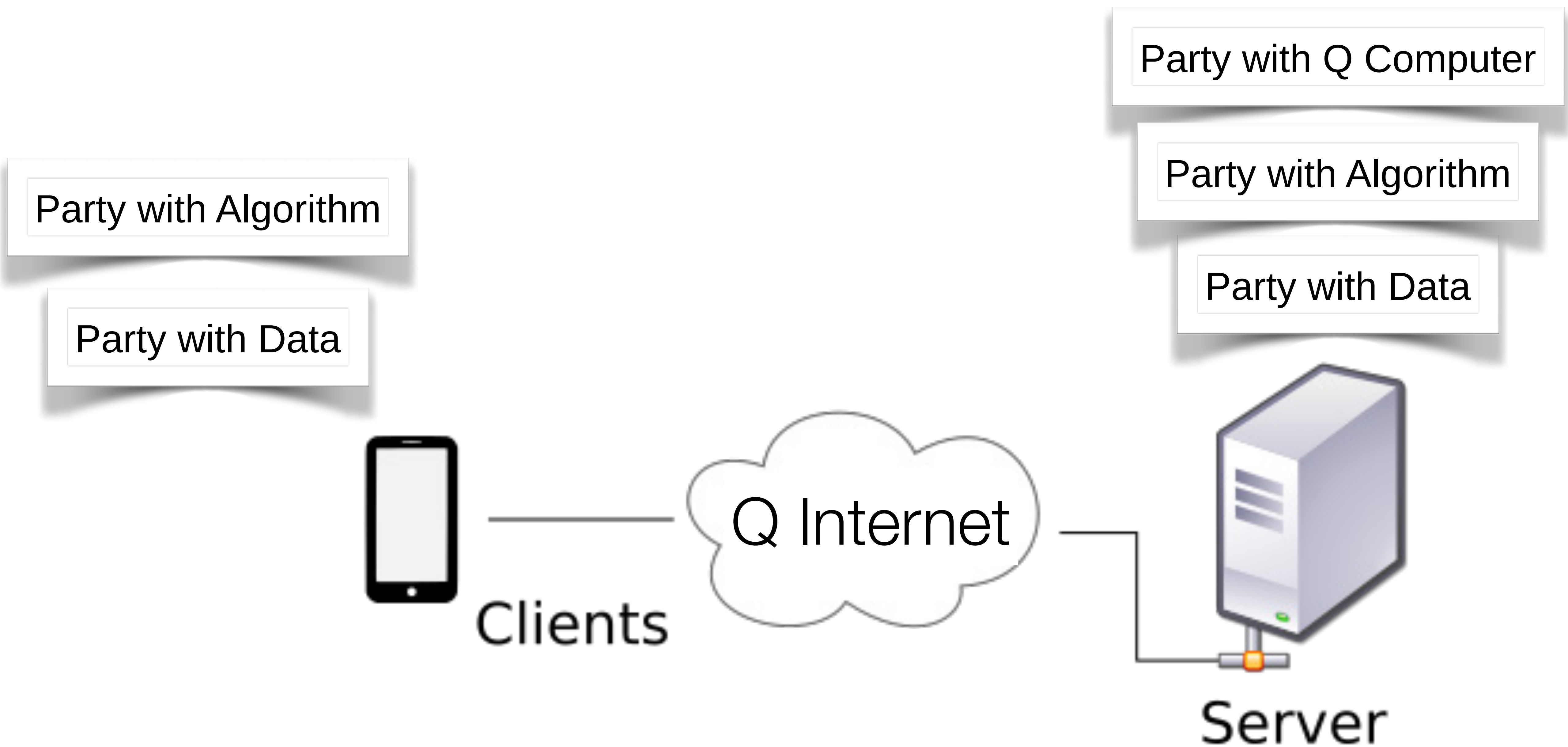


Secure Access to Quantum Cloud

=

Quantum Communication

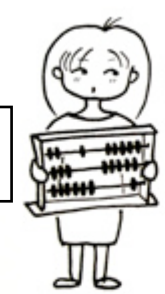
# Malicious Client - Malicious Server



# Yao Garbled Circuit - Secure 2-party Computing

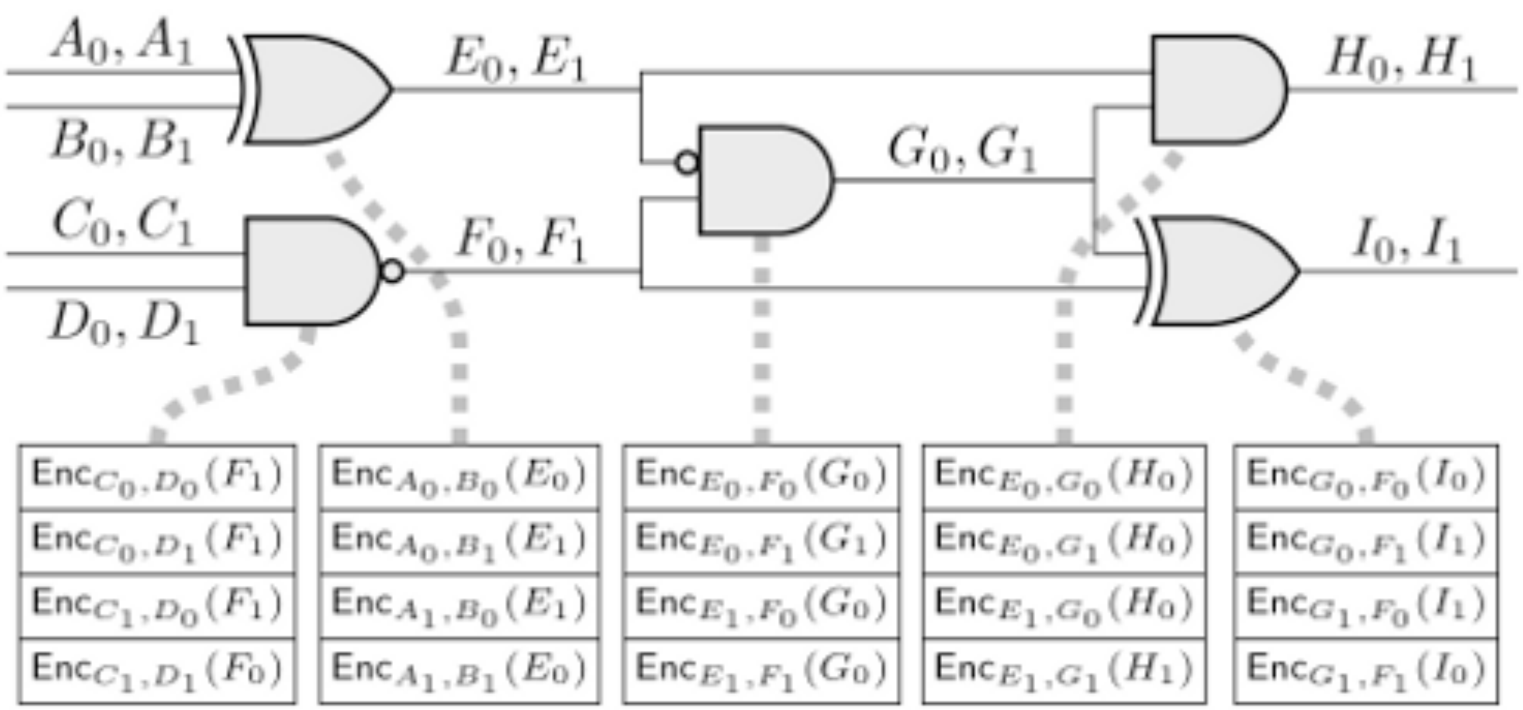
Secret input a

Garbled Program f



*Yao 1986*

# Yao Garbled Circuit - Secure 2-party Computing

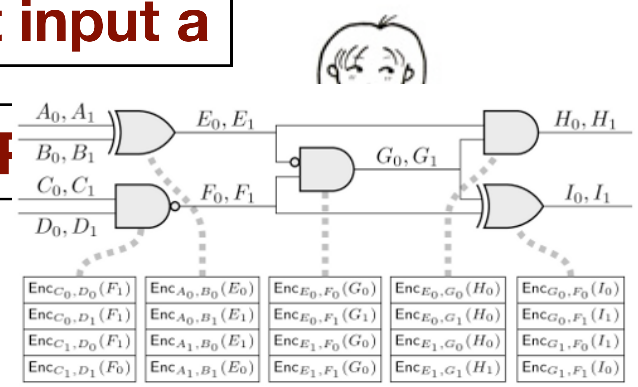



*Yao 1986*

# Yao Garbled Circuit - Secure 2-party Computing

**Secret input a**

**Garbled F**

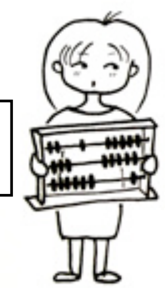


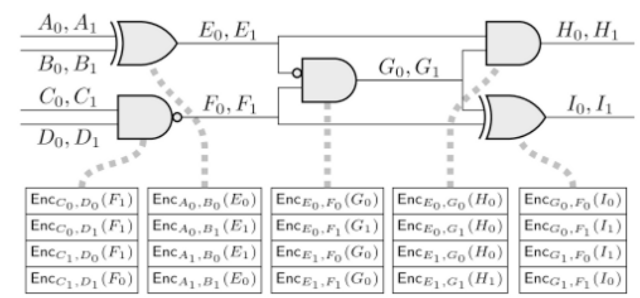

*Yao 1986*

# Yao Garbled Circuit - Secure 2-party Computing

**Secret input a**

**Garbled Program f**



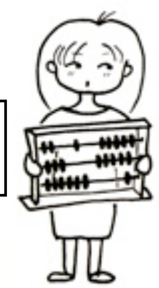


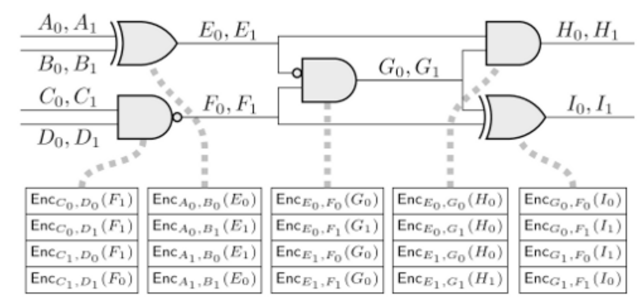

*Yao 1986*

# Yao Garbled Circuit - Secure 2-party Computing

**Secret input a**

**Garbled Program f**





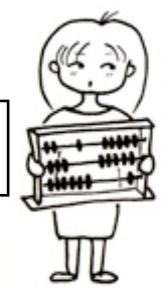

**Insert secret input b**
**Evaluate f(a,b)**

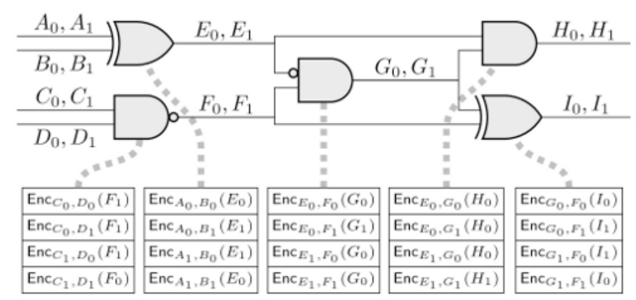
*Yao 1986*

# Yao Garbled Circuit - Secure 2-party Computing

**Secret input a**

**Garbled Program f**






**Insert secret input b**
**Evaluate f(a,b)**

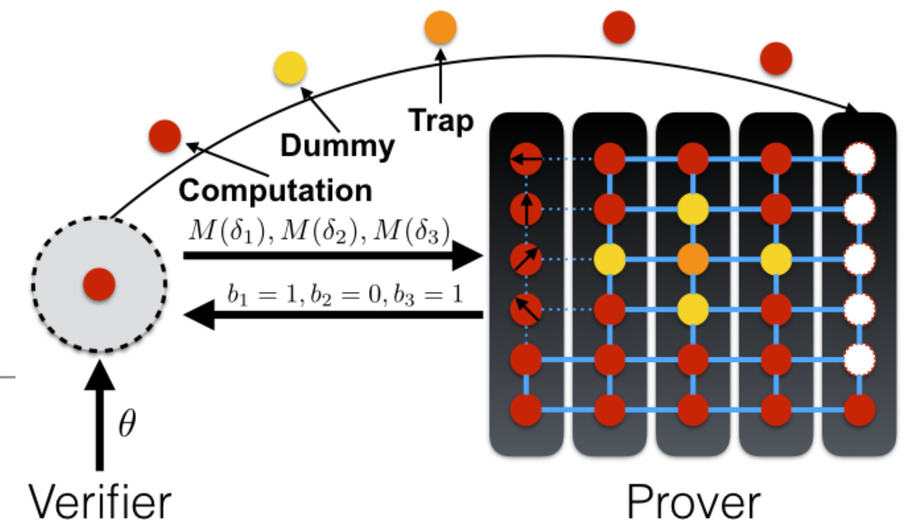
Computational Security

Requires OT

Honest but Curious Adversary

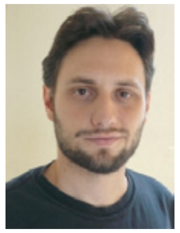
*Yao 1986*

# Verifiable Quantum Yao



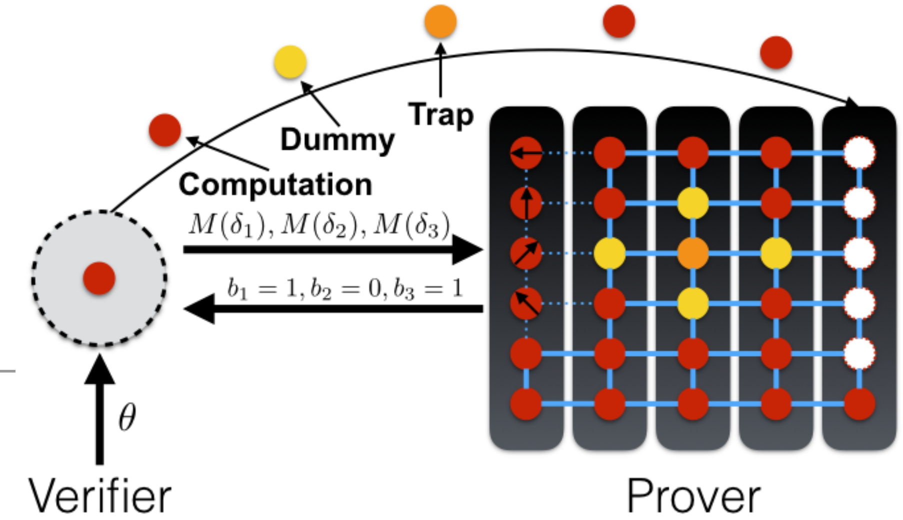

**Secret input q_c**

**Garbled CP map**



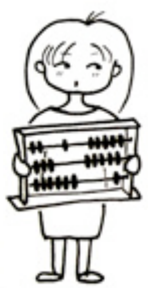
*Kashefi, Walden 16*
*Kashefi, Music, Wallden 17*

# Verifiable Quantum Yao




**Secret input q_c**

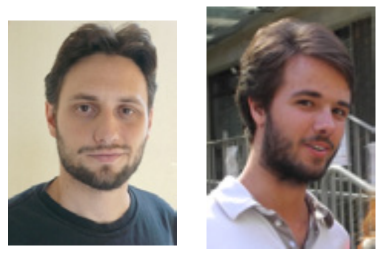
**Garbled CP map**



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

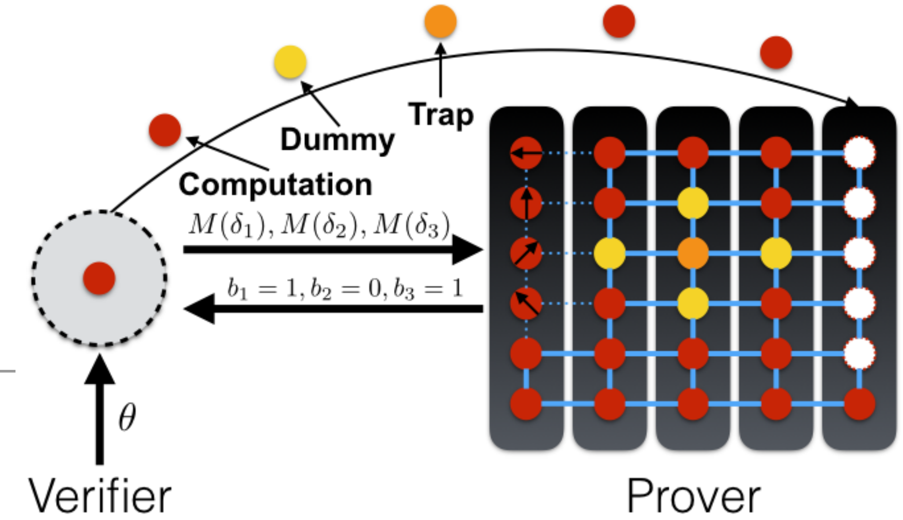
$$1/\sqrt{2}\left(|0\rangle + e^{i\theta}|1\rangle\right)$$

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



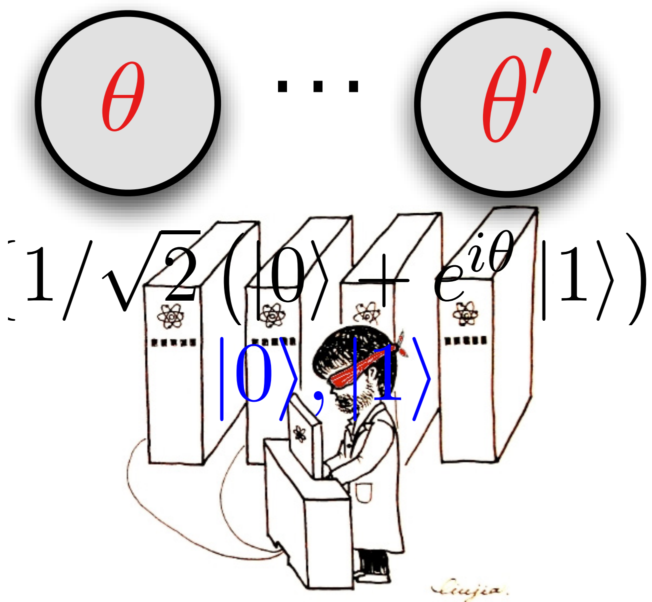
*Kashefi, Walden 16*
*Kashefi, Music, Wallden 17*

# Verifiable Quantum Yao




**Secret input q_c**

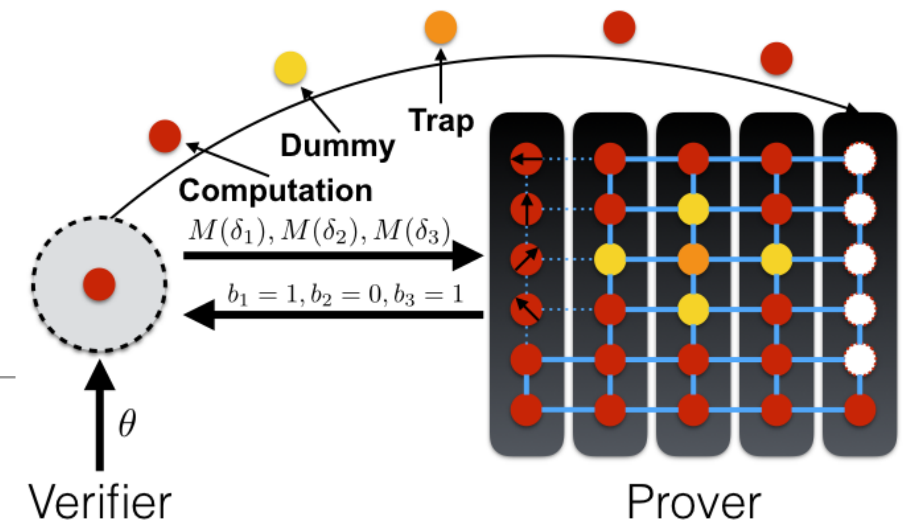
**Garbled CP map**



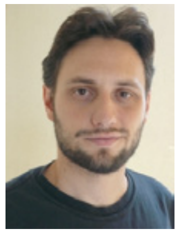
*Kashefi, Walden 16*
*Kashefi, Music, Wallden 17*

# Verifiable Quantum Yao



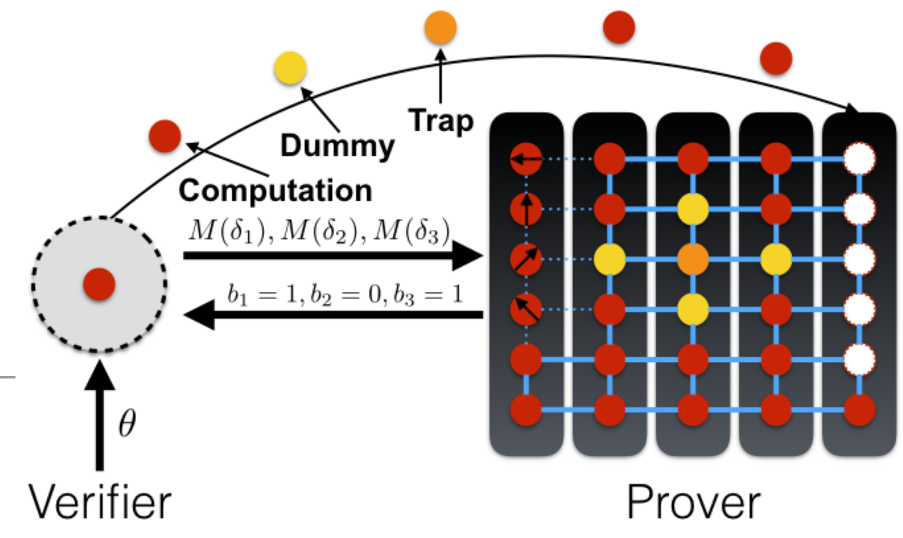

**Secret input q_c**

**Garbled CP map**



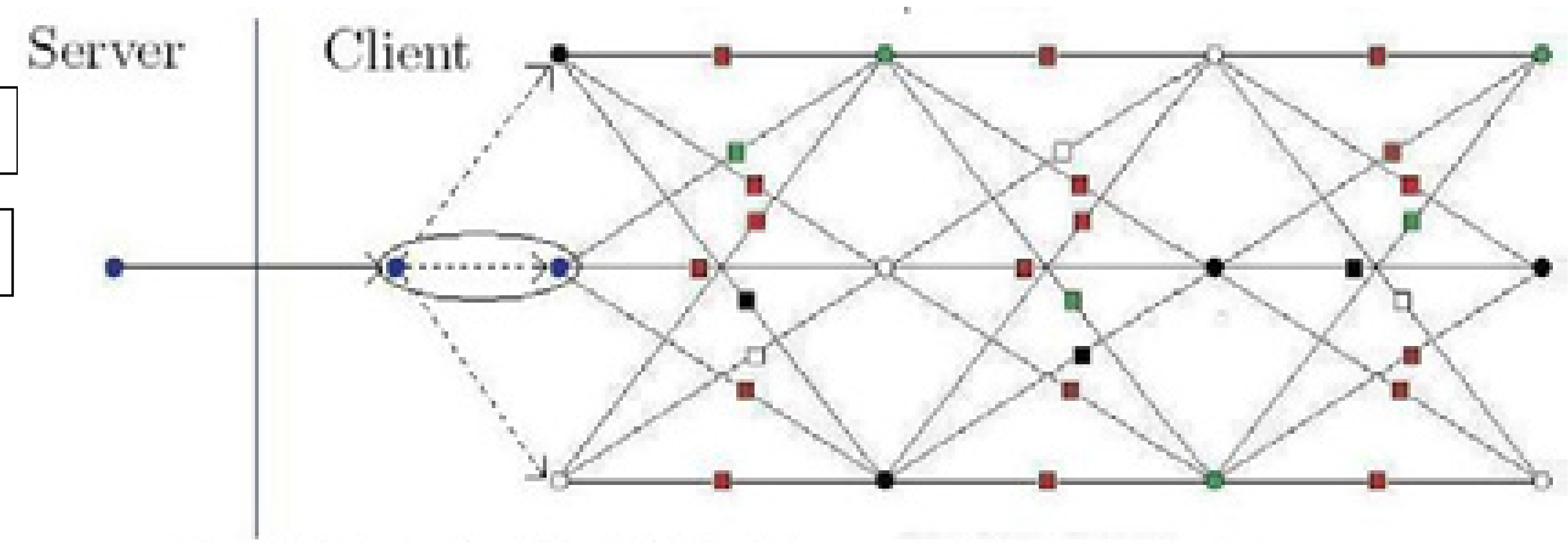
*Kashefi, Walden 16*
*Kashefi, Music, Wallden 17*

# Verifiable Quantum Yao

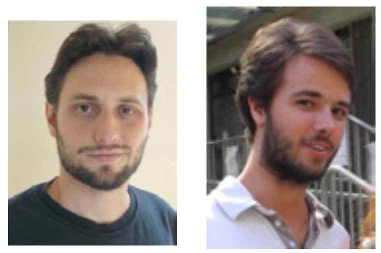



**Secret input q_c**

**Garbled CP map**

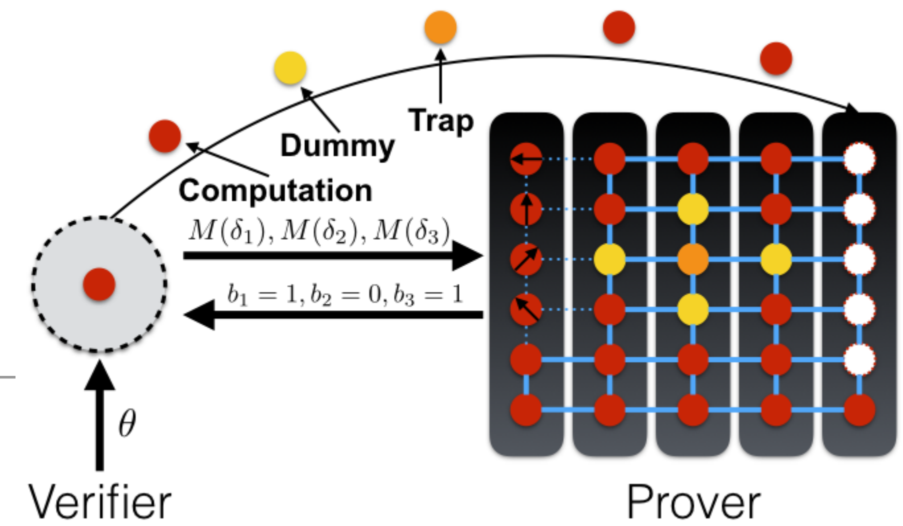



Server's input placed in DT(G) with correspoding trap-colouring



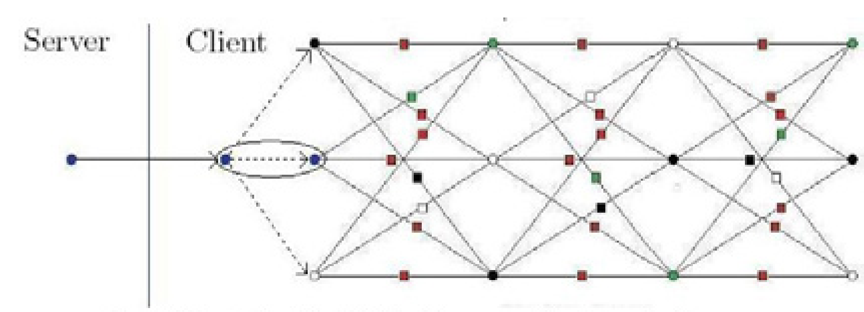
*Kashefi, Walden 16*
*Kashefi, Music, Wallden 17*

# Verifiable Quantum Yao

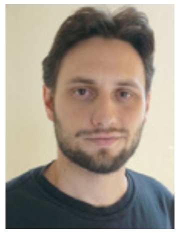



**Secret input q_c**

**Garbled CP map**



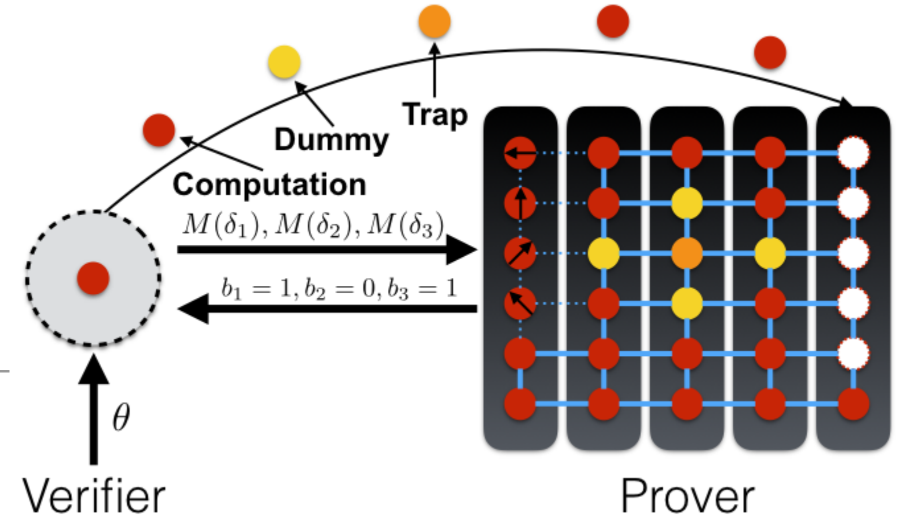

Server's input placed in DT(G) with correspoding trap-colouring



*Kashefi, Walden 16*

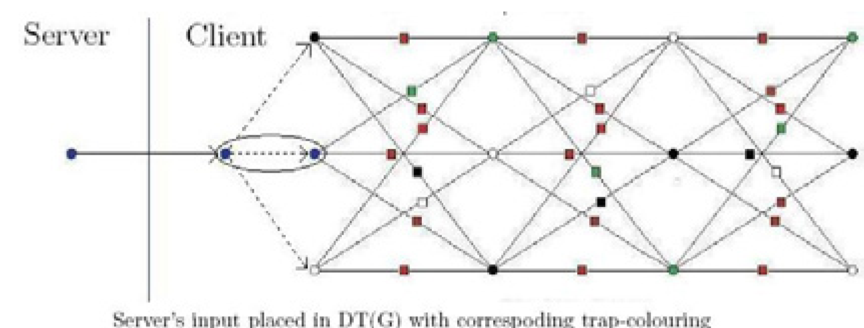
*Kashefi, Music, Wallden 17*

# Verifiable Quantum Yao

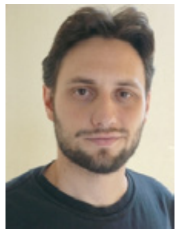



**Secret input q_c**

**Garbled CP map**

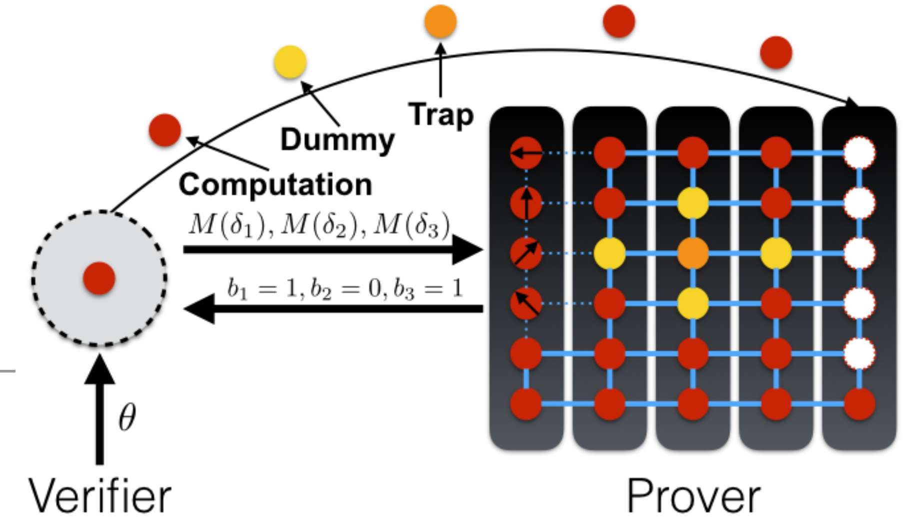



$$r_{x,y} \in_R \{0,1\}$$
$$\delta_{x,y} = \phi'_{x,y} + \theta_{x,y} + \pi r_{x,y}$$



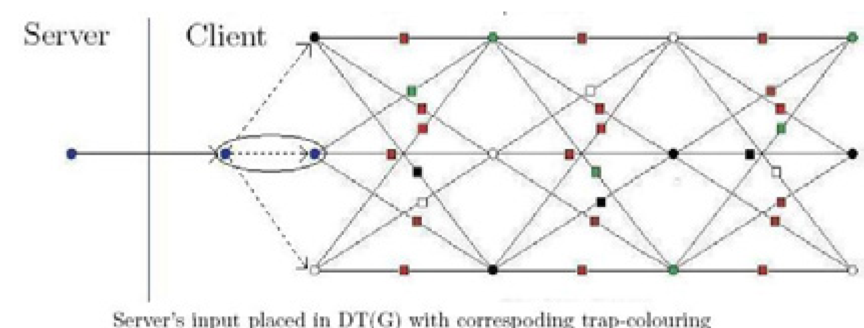

*Kashefi, Walden 16*
*Kashefi, Music, Wallden 17*

# Verifiable Quantum Yao



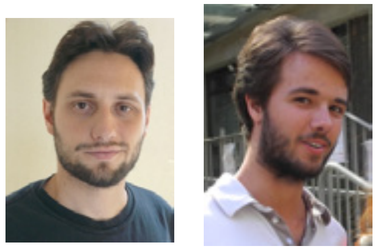

**Secret input q_c**

**Garbled CP map**



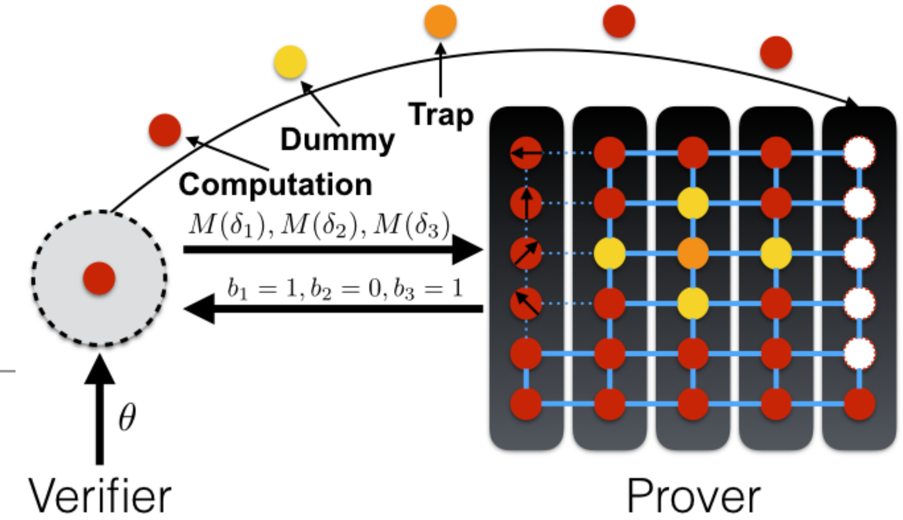

$$r_{x,y} \in_R \{0,1\}$$
$$\delta_{x,y} = \phi'_{x,y} + \theta_{x,y} + \pi r_{x,y}$$

**Insert secret input q_c**
**Evaluate CP(q_c,q_s)**



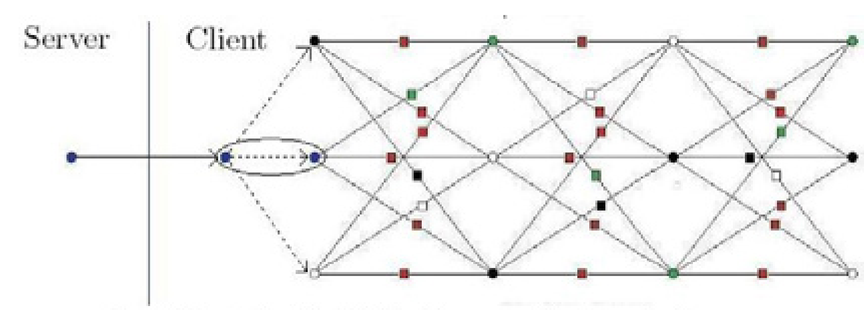
*Kashefi, Walden 16*
*Kashefi, Music, Wallden 17*

# Verifiable Quantum Yao




**Secret input q_c**

**Garbled CP map**




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

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

**Insert secret input q_c**
**Evaluate CP(q_c,q_s)**

Informationally Secure

*(needs classical SMPC for angle evaluations)*

Quantum Honest but Curious Client

Requires classical O(N) online communication

*Kashefi, Walden 16*
*Kashefi, Music, Wallden 17*

# Boosting Security
## *(Semi-Malicious Client to Fully Malicious one)*

**Cut** : Sender sends multiple copies of a state and message (with independent randomness) to the Receiver

✓ **Practical Efficient Malicious Client - Malicious Server**

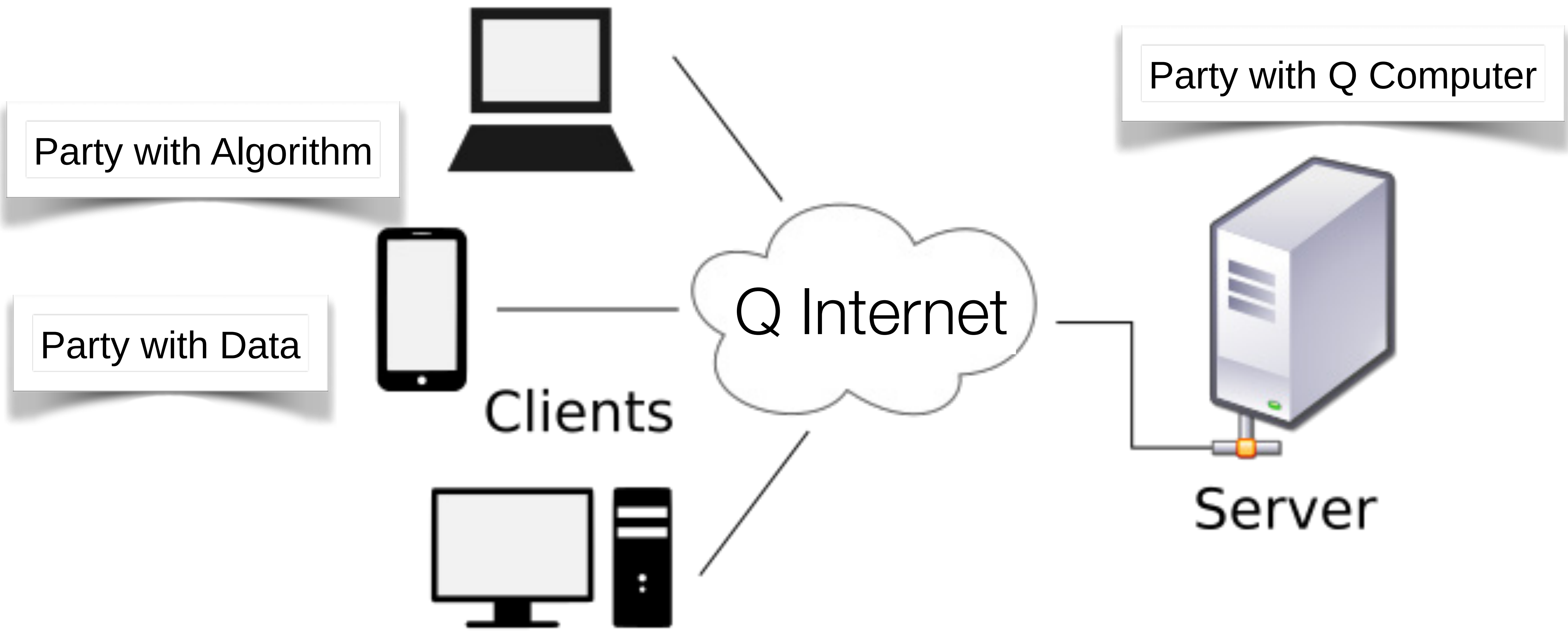
states) where correctly constructed by asking the Sender to send proofs and measuring them accordingly

Conditions for applying Q-CC ⟶ Client manipulates single qubit



*Kashefi, Music, Unruh, Wallden 2021*

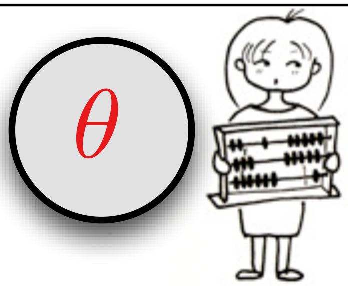
# Malicious Clients - Malicious Server



# Multiparty Delegated Quantum Computing 2017

**Secret input q_1**

**Garbled her part of the CP map**



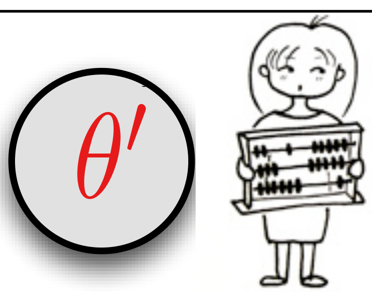

.

.

.

**Secret input q_n**

**Garbled her part of the CP map**




*Kashefi, Pappa 2017*

# Multiparty Delegated Quantum Computing 2017

Secret input q_1

Garbled her part of the CP map

$\theta$

$\theta'$

.

.

.

Secret input q_n

Garbled her part of the CP map

*Kashefi, Pappa 2017*

# Multiparty Delegated Quantum Computing 2017

**Secret input q_1**

**Garbled her part of the CP map**

.

.

.

**Secret input q_n**

**Garbled her part of the CP map**

*Kashefi, Pappa 2017*

# Multiparty Delegated Quantum Computing 2017

**Secret input q_1**

**Garbled her part of the CP map**

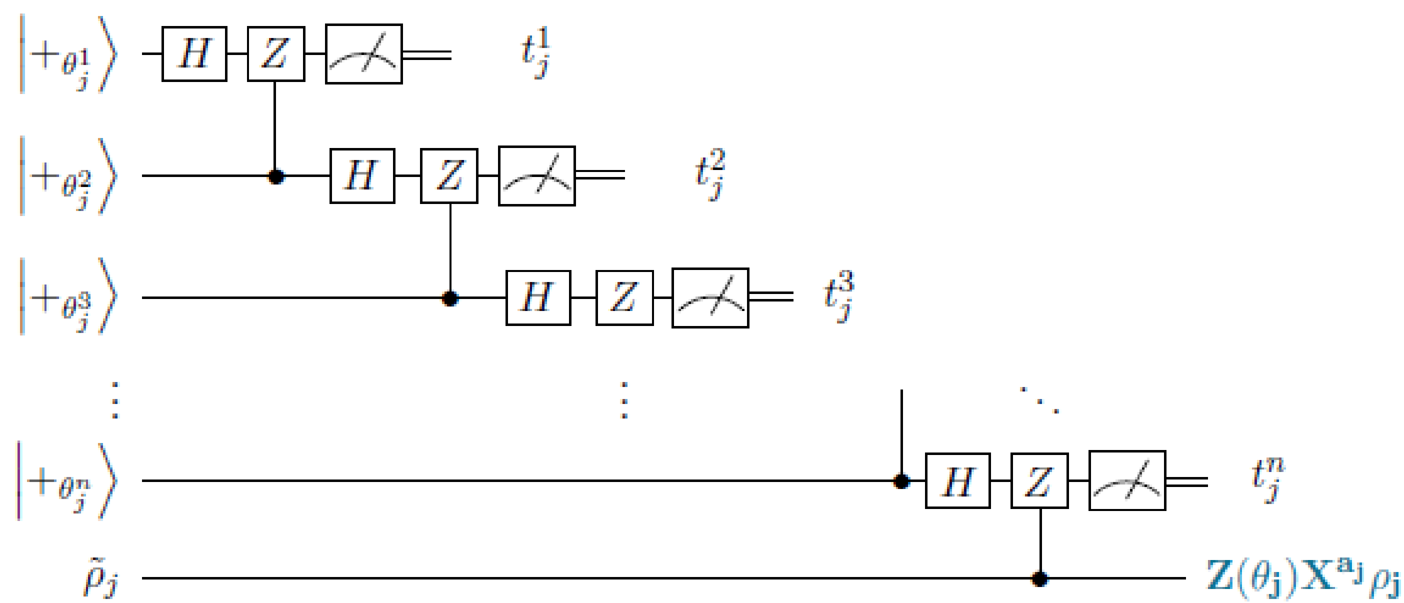
.

.

.

**Secret input q_n**

**Garbled her part of the CP map**



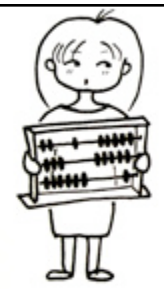

$$\theta_j = \theta_j^j + \sum_{k=1,k\neq j}^{n} (-1)^{\bigoplus_{i=k}^{n} t_j^i} \theta_j^k$$

*Kashefi, Pappa 2017*

# Multiparty Delegated Quantum Computing 2017

Secret input q_1

Garbled her part of the CP map



.

.

.

Secret input q_n

Garbled her part of the CP map

*Kashefi, Pappa 2017*

# Multiparty Delegated Quantum Computing 2017

Secret input q_1

Garbled her part of the CP map

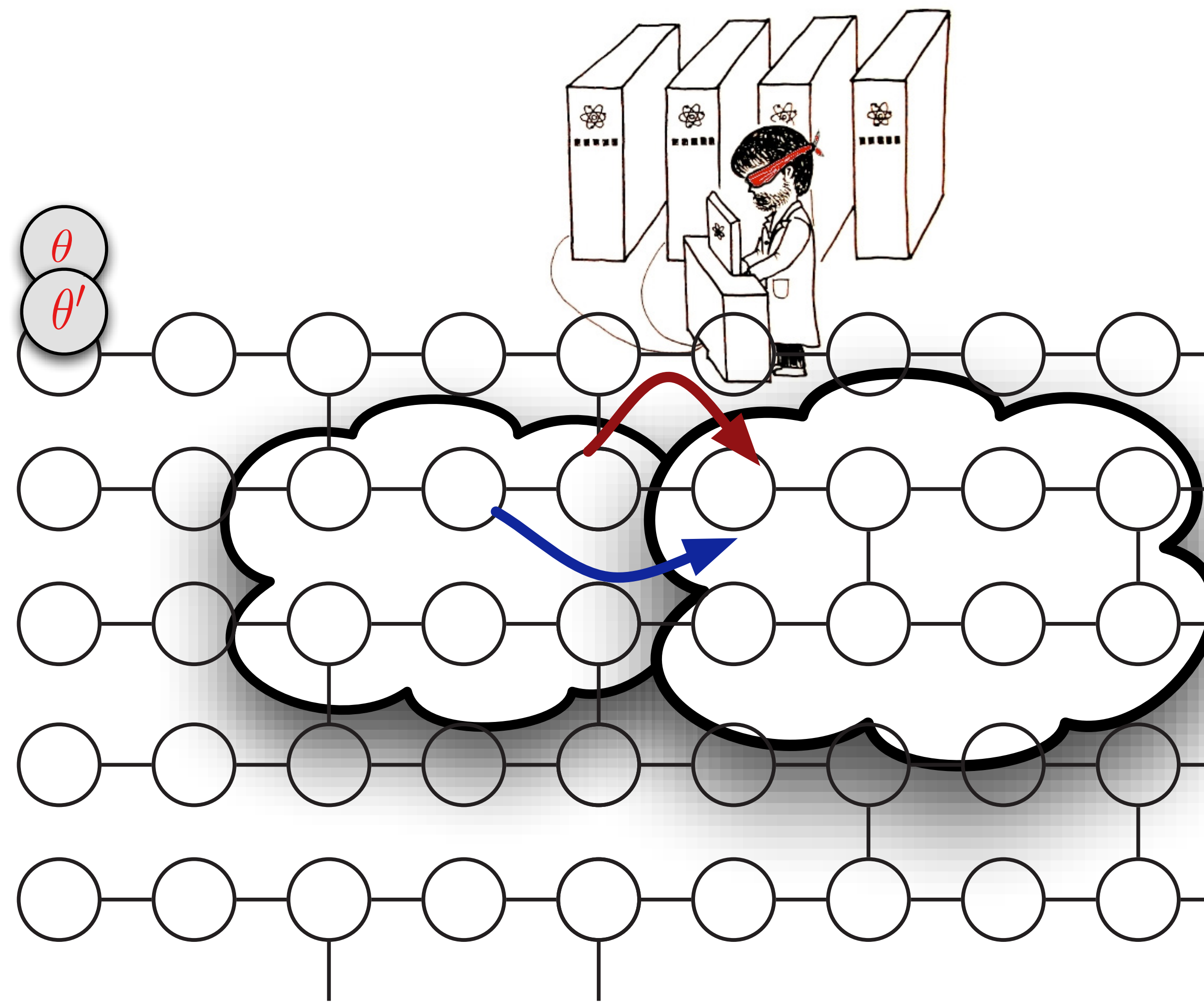
.

.

.

Secret input q_n

Garbled her part of the CP map



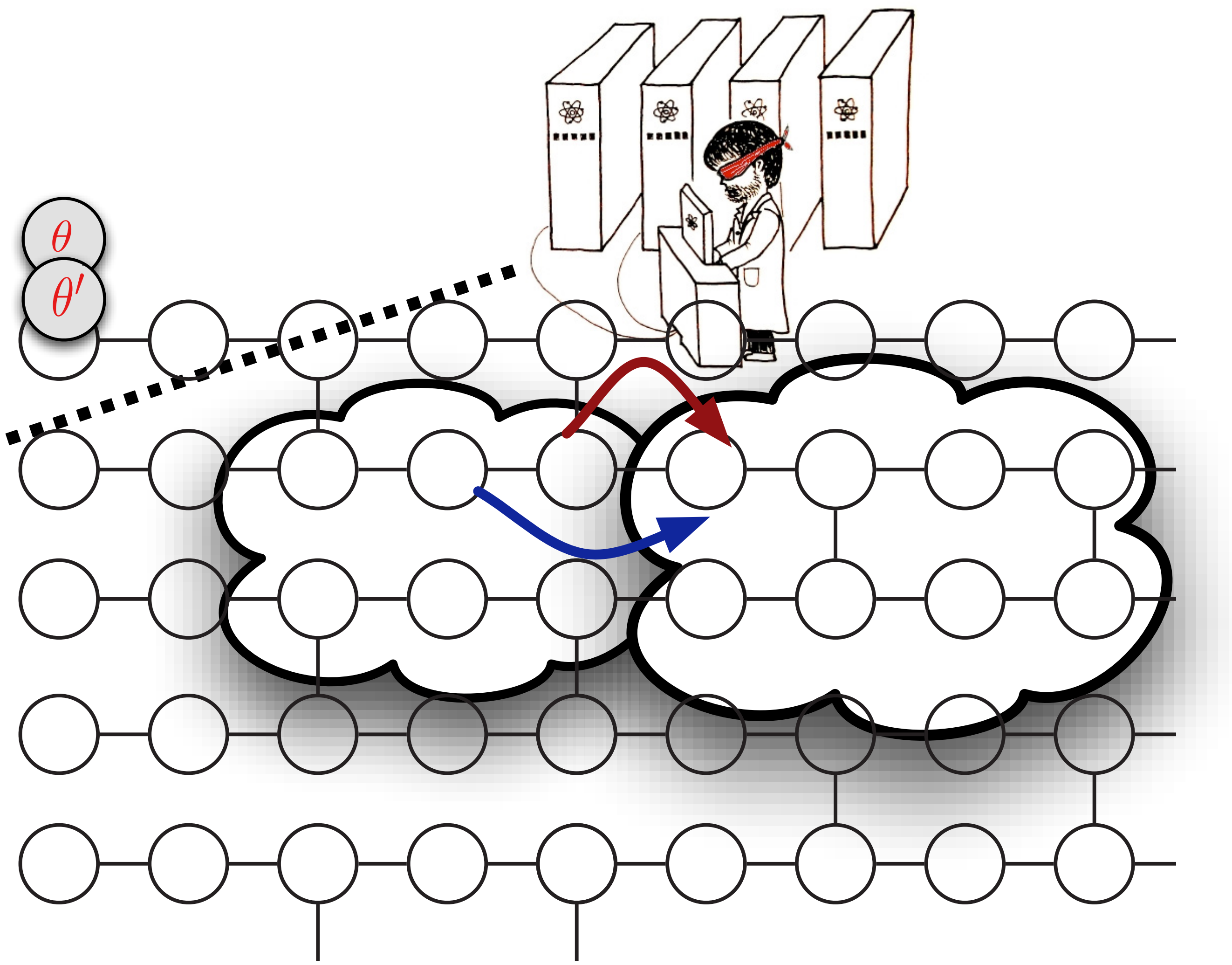

*Kashefi, Pappa 2017*

# Multiparty Delegated Quantum Computing 2017

**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**

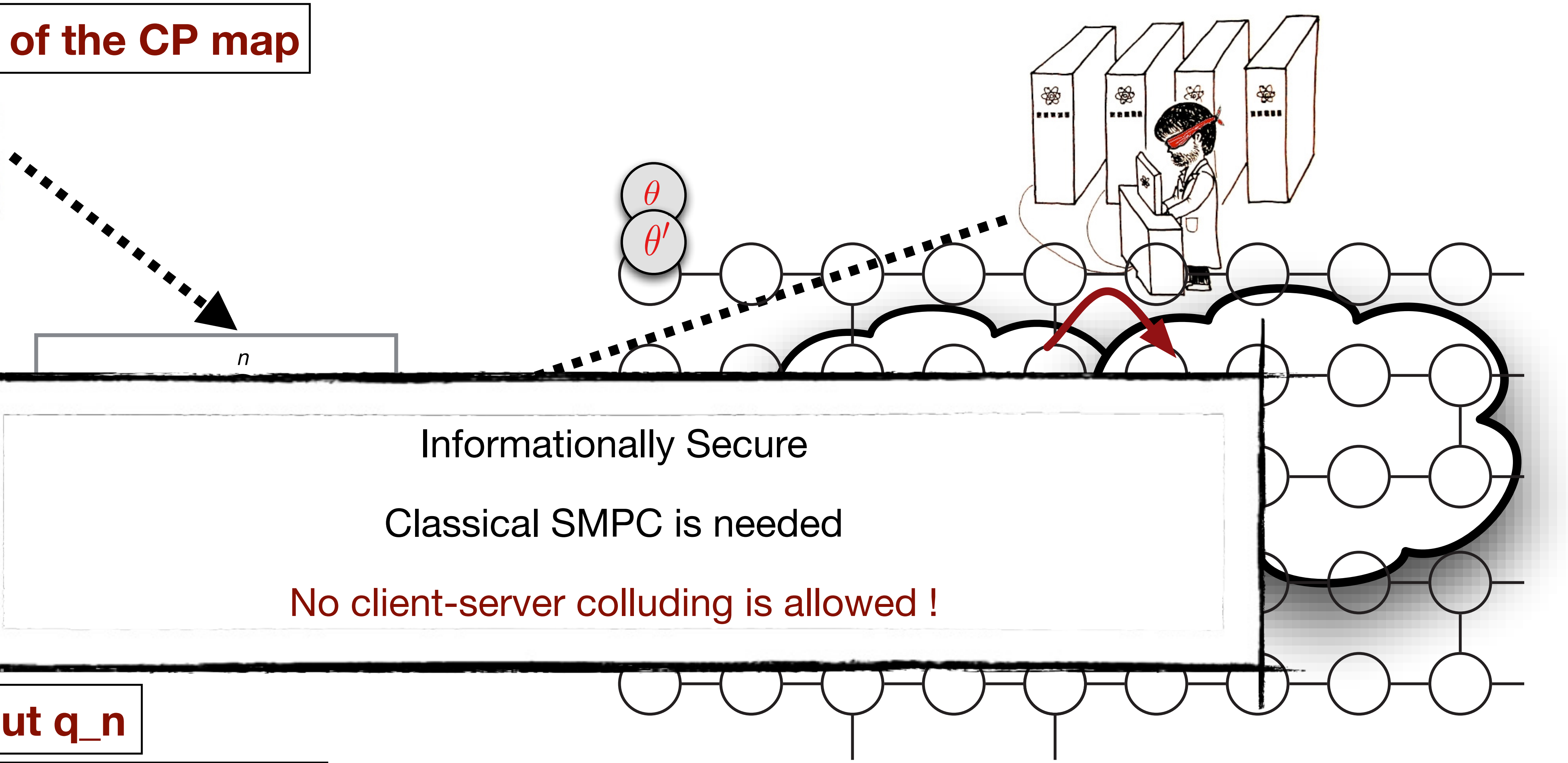
**Garbled her part of the CP map**

*Kashefi, Pappa 2017*

# Multiparty Delegated Quantum Computing 2017

**Secret input q_1**

**Garbled her part of the CP map**




**Secret input q_n**

**Garbled her part of the CP map**

*Kashefi, Pappa 2017*

# Multiparty Delegated Quantum Computing 2017

# Multiparty Delegated Quantum Computing 2017

Clients can insert traps only in their subgraphs

**But**

A connected path for computation can be obtained only if they collaborate

**But**

They need not to leak the position of traps

# Multiparty Delegated Quantum Computing 2017

Clients can insert traps only in their subgraphs

**But**

A connected path for computation can be obtained only if they collaborate

**But**

They need not to leak the position of traps





*In Symmetric Case these issues are resolved by*

*Dulek, Grilo, Jeffery, Majenz, Schaffner 2020*

# Multiparty Delegated Quantum Computing 2021

**Double Blind QC** - a classically orchestrated delegation

**Good Enough State** - correct up to a deviation independent of the inputs and security parameters

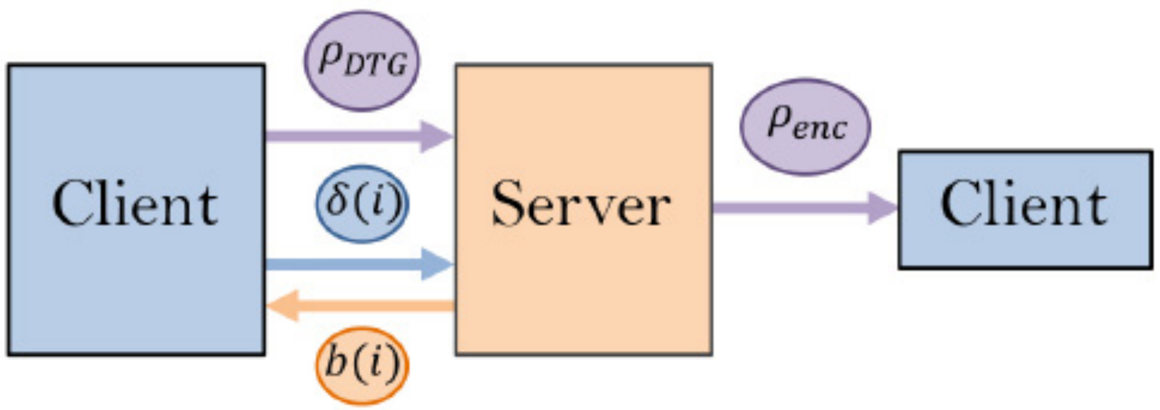
*Kapourniotis, Kashefi , Music, Ollivier 2021*

# VUBQC Deconstruction - Reconstruction

Steps to be updated to transform into a multi-client setting
&
Conditions that these replacement need to satisfy

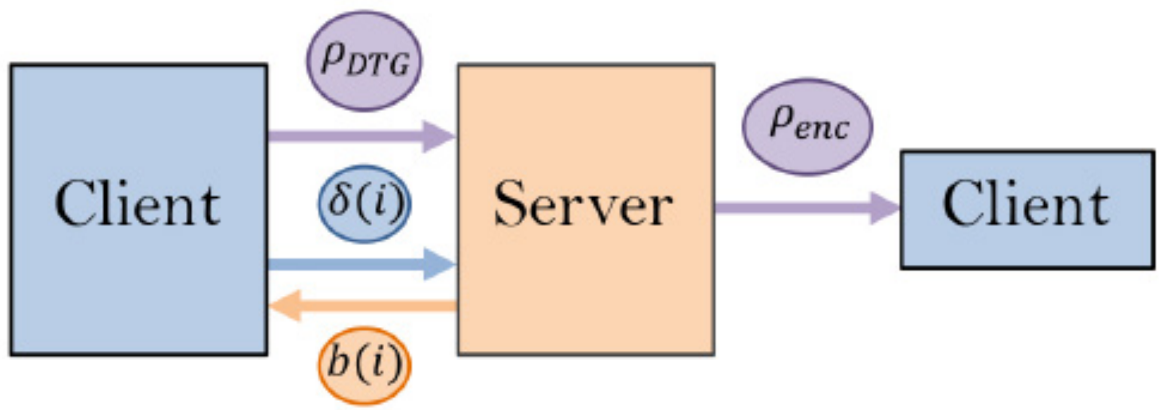
# VUBQC Deconstruction - Reconstruction

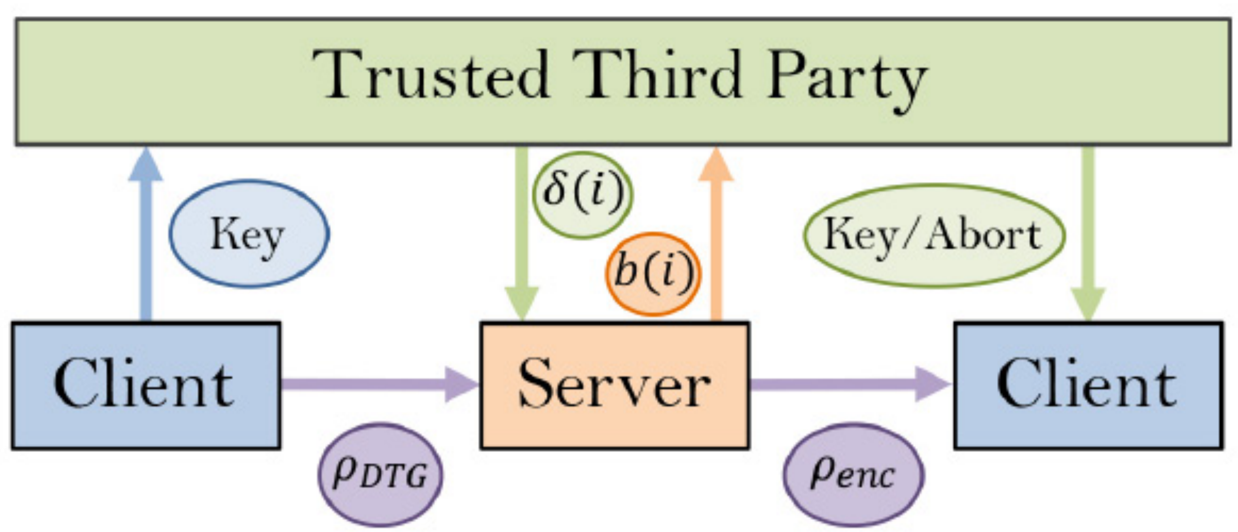
Steps to be updated to transform into a multi-client setting
&
Conditions that these replacement need to satisfy



# VUBQC Deconstruction - Reconstruction

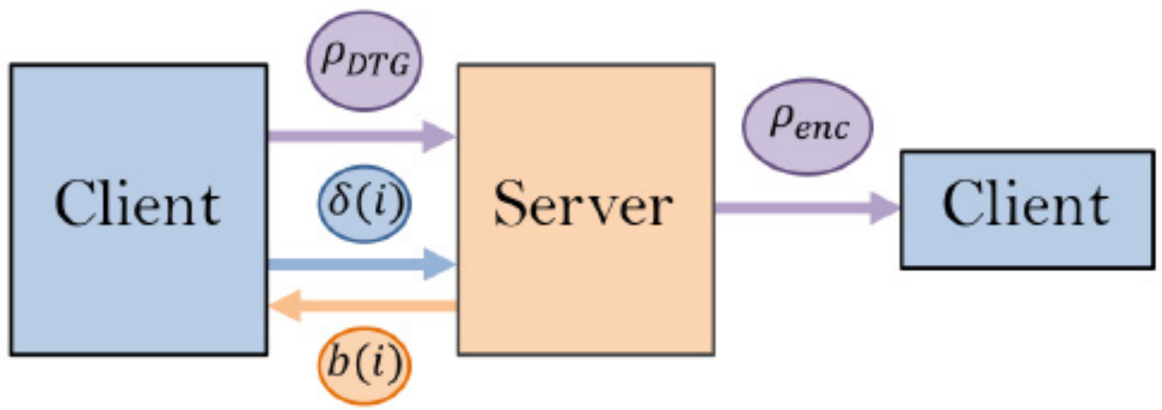
Steps to be updated to transform into a multi-client setting
&
Conditions that these replacement need to satisfy

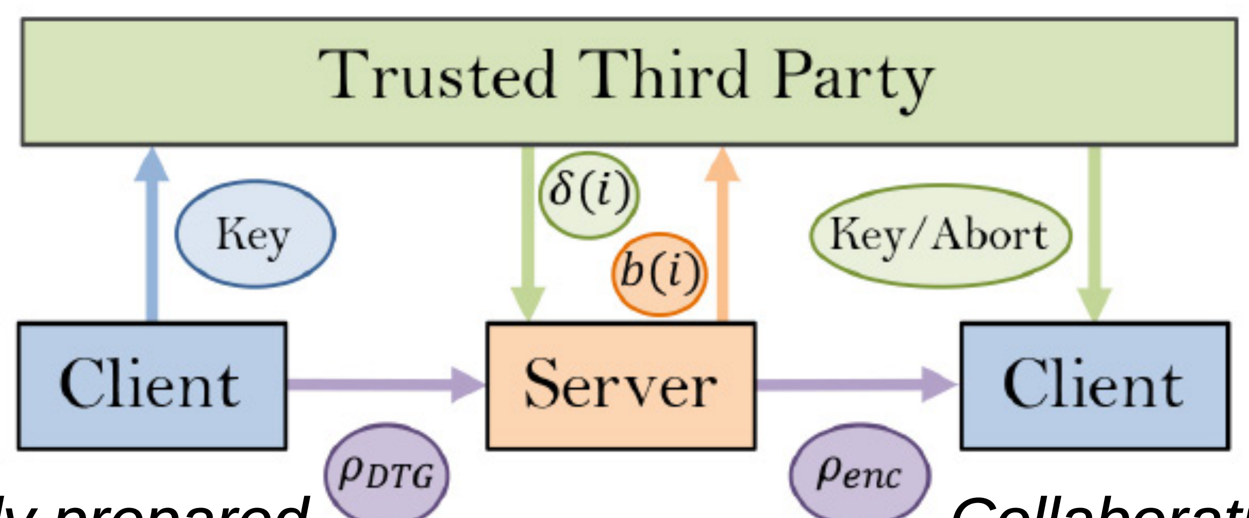


# VUBQC Deconstruction - Reconstruction

Steps to be updated to transform into a multi-client setting
&
Conditions that these replacement need to satisfy

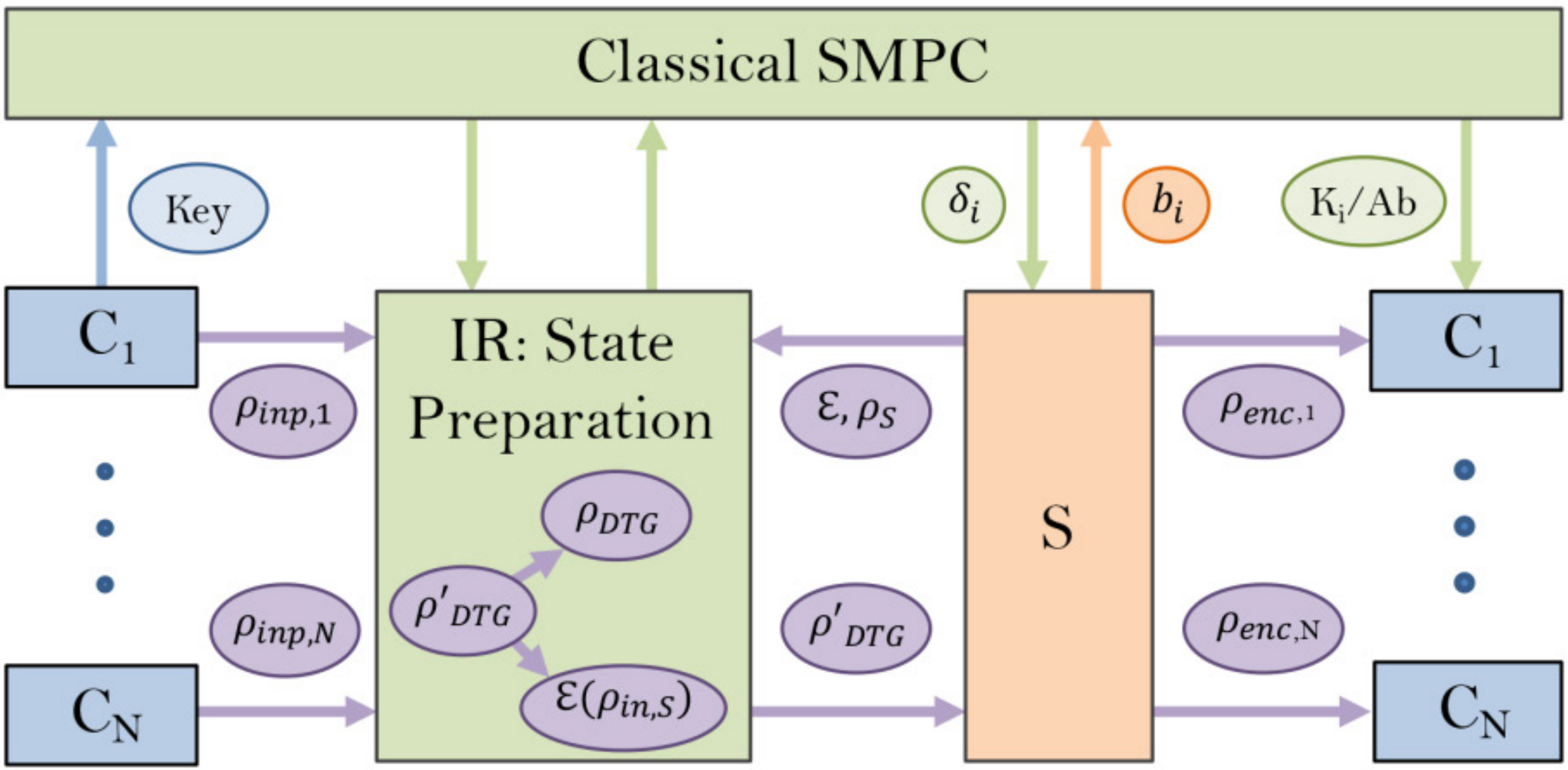


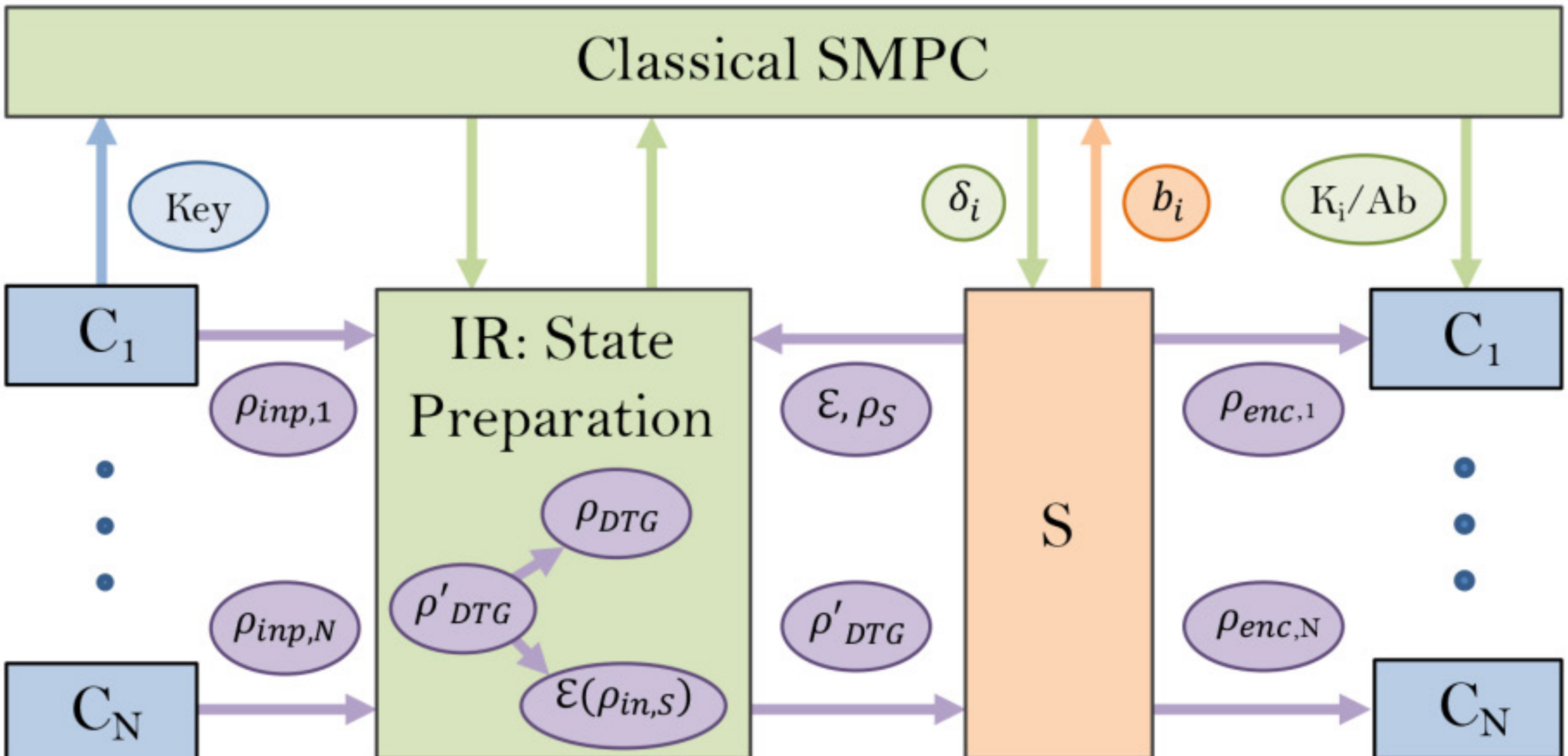

*Collaboratively prepared*

*Collaboratively measured*

# Replacing Classical Steps with Classical SMPC

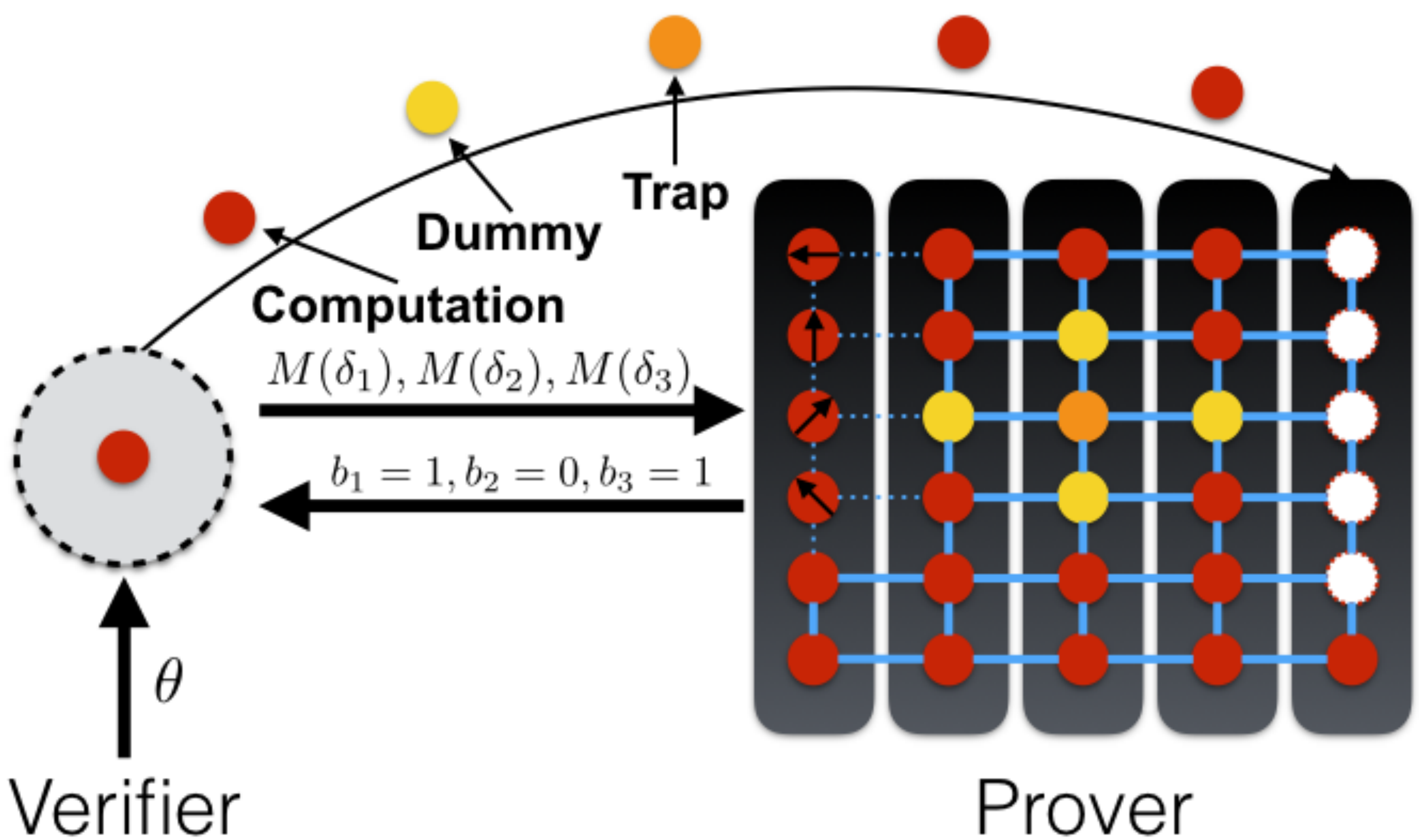


# Replacing Classical Steps with Classical SMPC

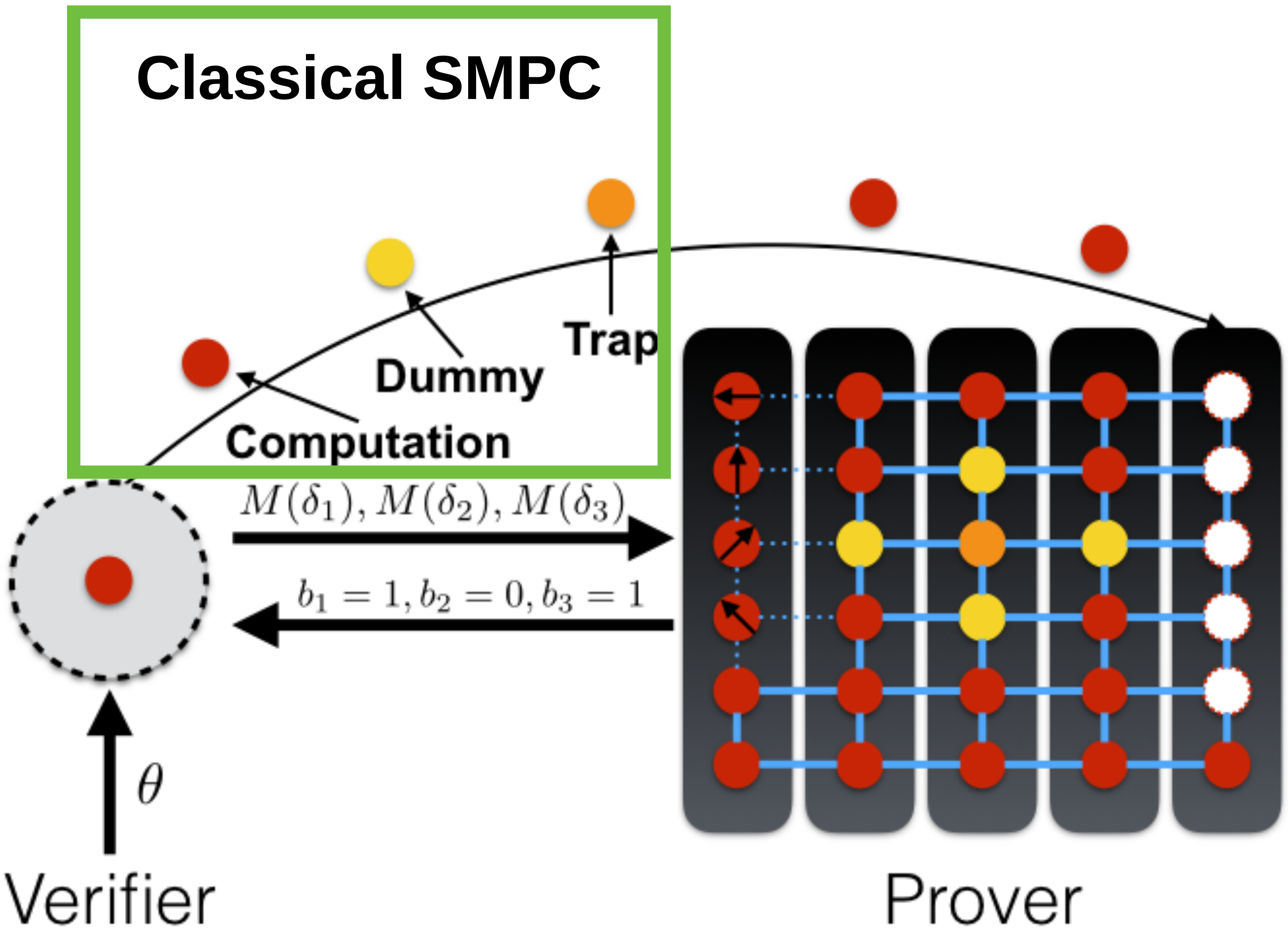



*Possibly deviated multi party encrypted state (independent of secret parameters)*

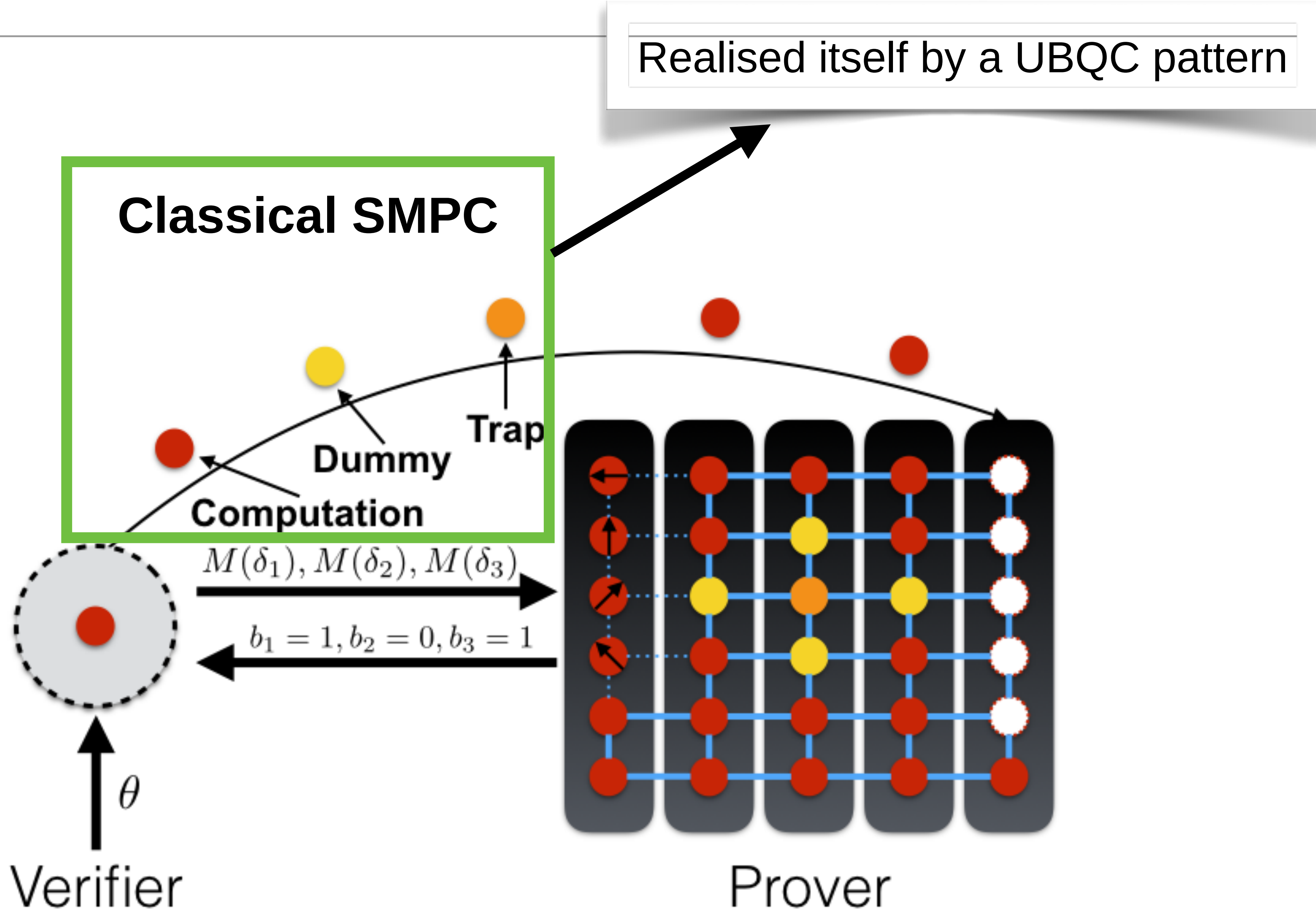
# Double Blind QC



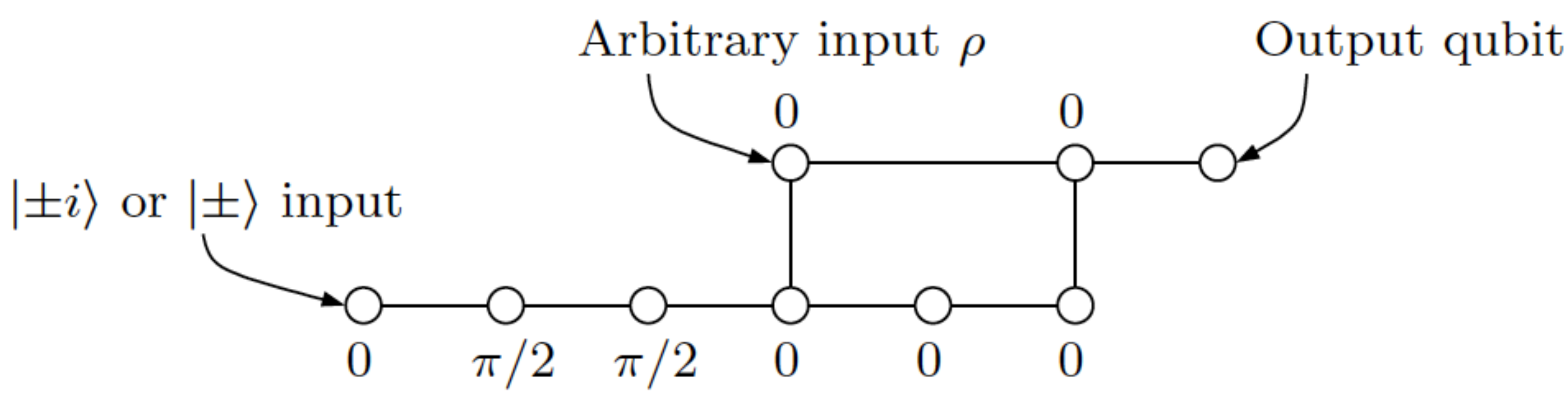
# Double Blind QC



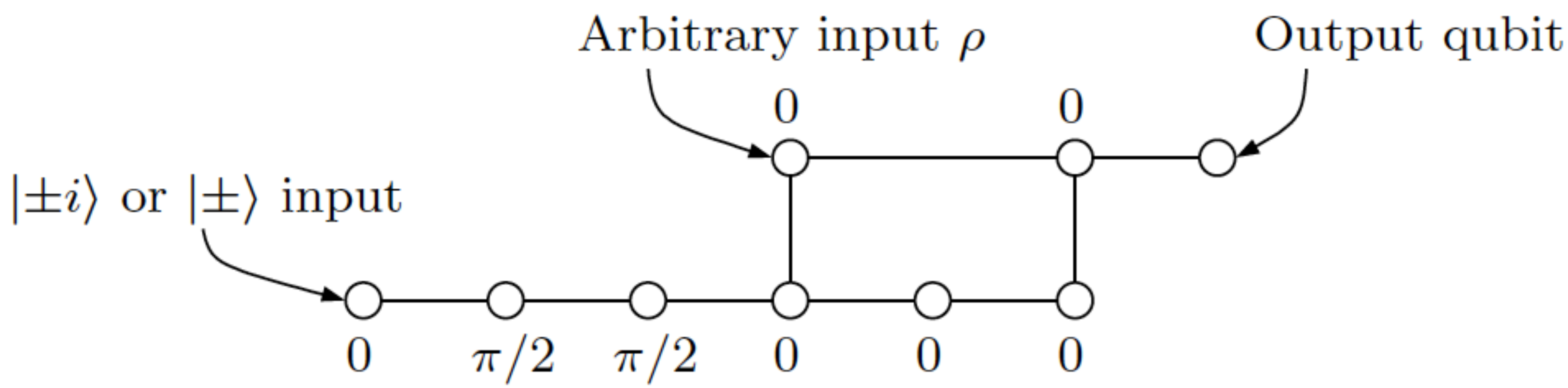
# Double Blind QC



# Double Blind Gadgets for *H* or *I*



# Double Blind Gadgets for *H* or *I*




**Clients:** sends encrypted input and rotated states

**SMPC:** redistribute them to become dummy or trap

# Multiparty Delegated Quantum Computing 2021

*Dulek, Grilo, Jeffery, Majenz, Schaffner 2020*    *Alon, Chung, Chung, Huang, Lee, Shen*

| Metric | [9] | [26] | [1] | This work |
|---|---|---|---|---|
| Type | Stat. upgrade of CSMPC | Statistical | Comp. (FHE + CSMPC) | Stat. upgrade of CSMPC |
| Abort | Unanimous | Unanimous | Identifiable | Unanimous |
| Composability | Composable | Stand-Alone | Stand-Alone | Composable |
| Max Malicious Players | $N-1$ | $\lfloor \frac{C_{dist}-1}{2} \rfloor$ | $N-1$ | $N-1$ |
| Protocol Nature | Symmetric | Symmetric | Semi-Delegated | Delegated |
| Network Topology | Q and C: Complete | Q and C: Complete | Q and C: Complete | Q: Star / C: Complete |
| Q Operations | F.T. Q. Comp | FT Q Comp | FT Q Comp | Cl.: Single Qubit<br>Serv.: FT Q Comp |
| Classical SMPC | Clifford Computation,<br>Operations in $\mathbb{Z}_2$, CT | CT | Clifford Computation,<br>FHE verification | Operations in $\mathbb{Z}_8$, $\mathbb{Z}_2$, CT |
| Rounds (C or CSMPC) | $\mathcal{O}(g+\eta(N+t))$ | $d+2$ | $\mathcal{O}(1)$ | $d+5$ |
| Rounds (Q) | Par.: $\mathcal{O}(Nd)$<br>Seq.: $\mathcal{O}(N(N+t+c))$ | Par.: 3 (2 if C output)<br>Seq.: $\mathcal{O}(\eta^2(N+t))$ | Par.: $\mathcal{O}(N^4)$ | Par.: 2 (1 if C output)<br>Seq.: $\mathcal{O}(\eta N d)$ |
| Size of Q Memory | Par.: $\mathcal{O}(\eta^2(N+t)))$<br>Seq.: $\mathcal{O}(\eta^2 N)$ | Par.: $\mathcal{O}(\eta^2 N(N+t))$<br>Seq.: $\mathcal{O}(N^2)$ | Par.: $\mathcal{O}(tN^9\eta^2)$ | Cl.: 3 (0 if C I&O)<br>Serv. (par.): $\mathcal{O}(\eta N^2 d)$<br>Serv. (seq.): $\mathcal{O}(\eta N d)$ |

*Lipinska, Ribeiro, Wehner 2020*

# Practical Efficient Malicious Clients - Malicious Server ?

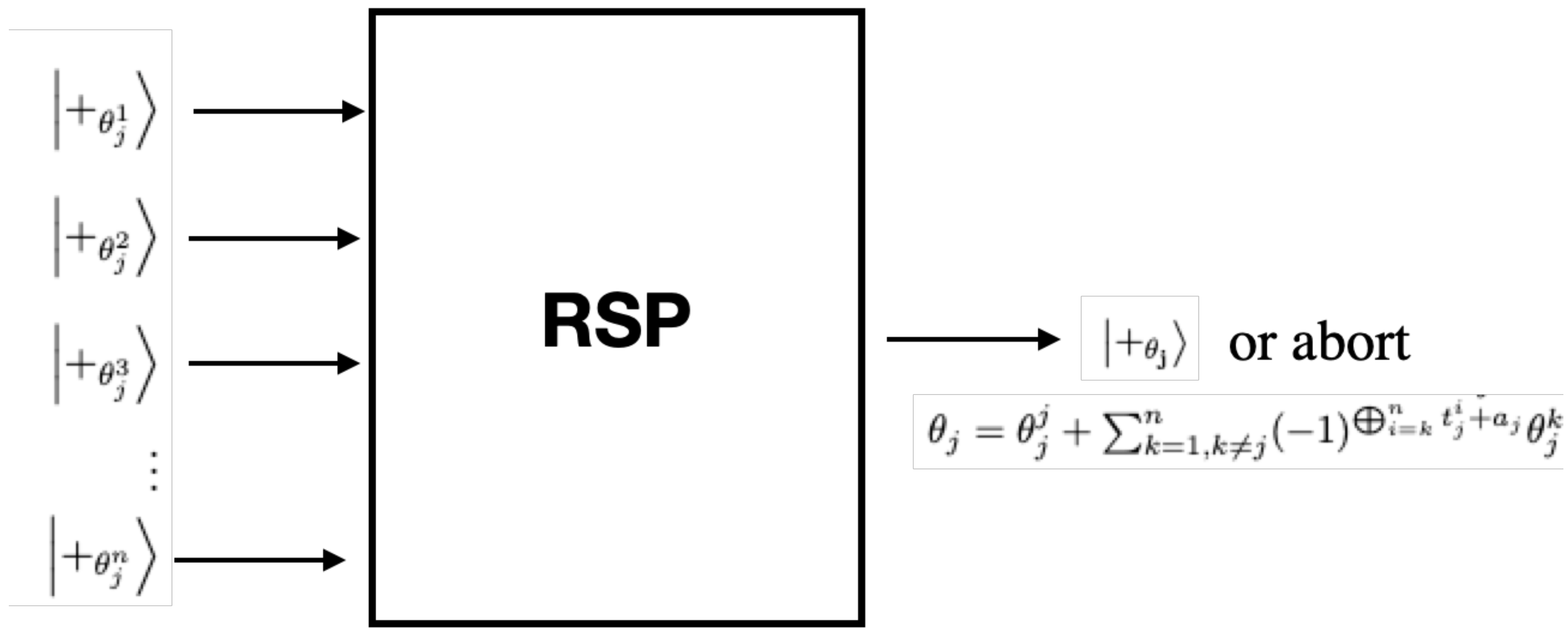
# Practical Efficient Malicious Clients - Malicious Server ?

**Each Module Can be Optimised**

- SMPC : angles evaluations and permutations
- Remote State Prep : Hardware Dependent
- Blind QC : Not every qubits being hidden
- Verifiable QC : No Need for dummies

# Key component - Remote State Preparation

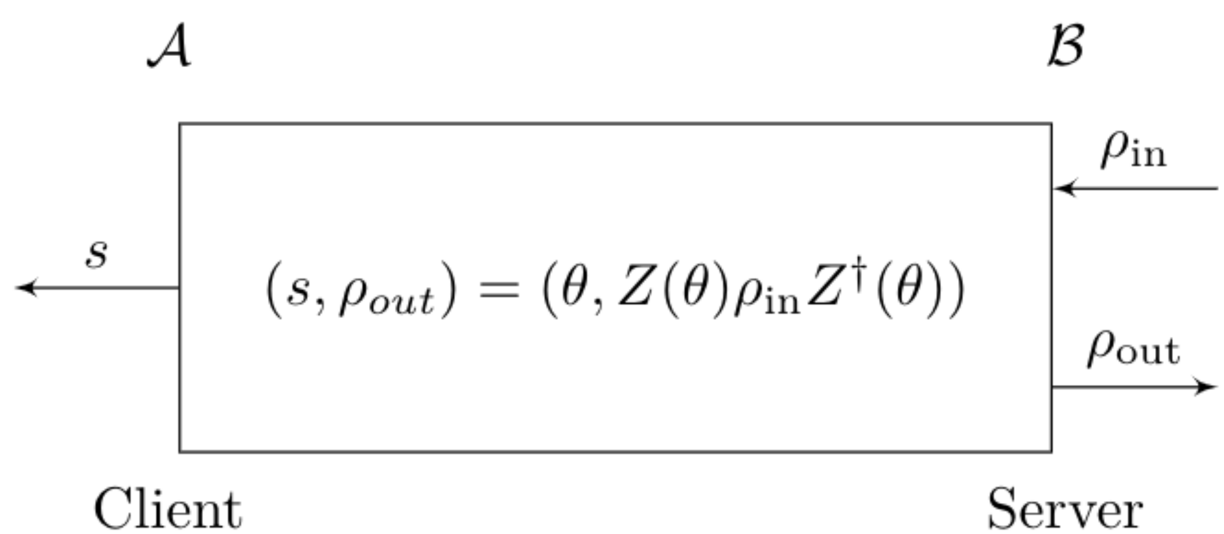
# Key component - Remote State Preparation



# The Most Optimal Client-Server RSP



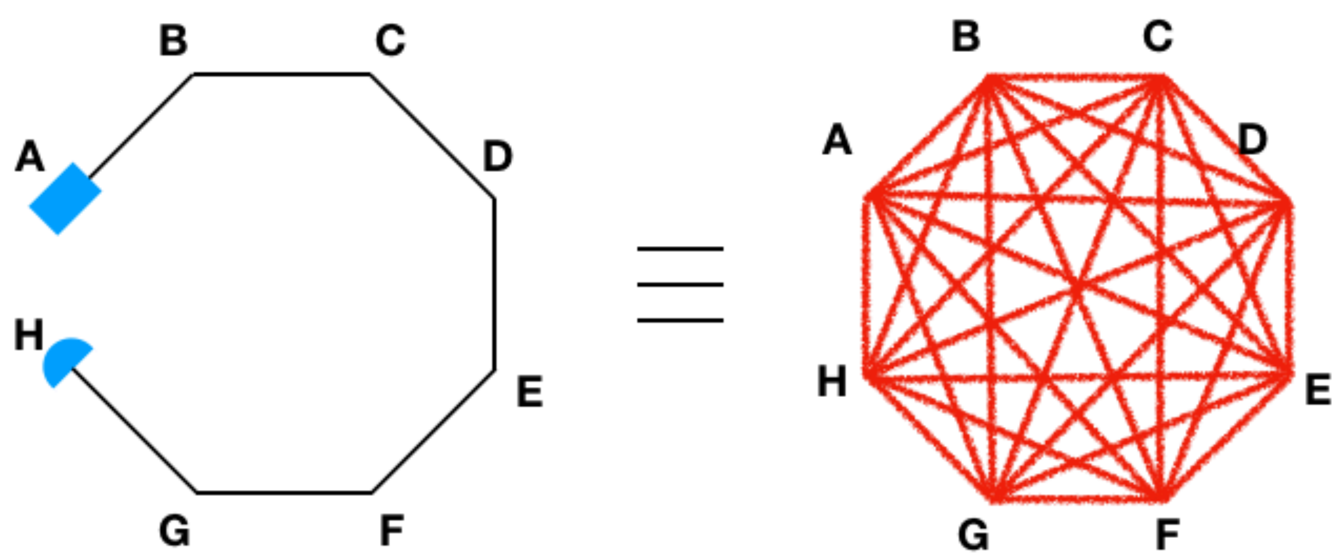

**Quantum Enclave - Remote State Rotation**



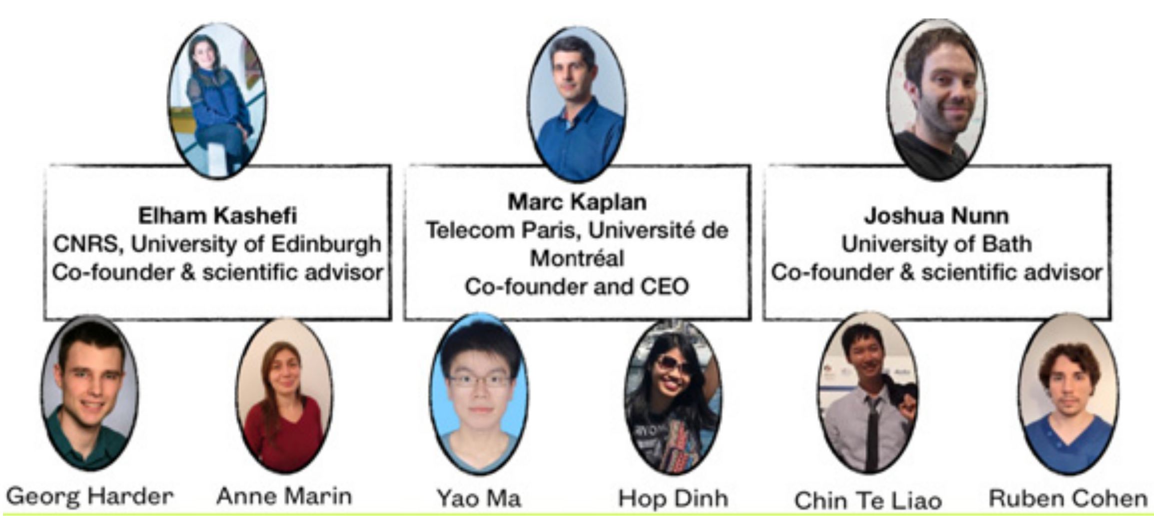

Arapinis, Chakraborty, Kaplan, Kashefi, Ma, 2021

# The Most Optimal Multi Party QSMPC

**Qline Architecture + Remote State Rotation + QSMPC**




VeriQloud's fully connected quantum network with a single optical fibre



# A Secure New World