Classical-Quantum Crypto Gadgets

Elham Kashefi

THE UNIVERSITY of EDINBURGH
informatics

Post Quantum Crypto

Post Quantum Crypto

There is **NO**

quantum danger or advantage

for classical cryptography **right now**

Quantum Danger

classical security against adversaries that exploit quantum effects

Quantum Danger

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

Quantum NO Danger

Quantum NO Danger

Learning with Error (LWE)

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

Regev, STOC 2005

Quantum NO Danger

Learning with Error (LWE)

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

Regev, STOC 2005

LWE-based Crypto Systems (FHE and etc)

Quantum NO Danger

Learning with Error (LWE)

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

Regev, STOC 2005

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**

Damgard and Lunemann, ASIACRYPT 2009
Damgard et.al. Crypto 2009
Lunemann, Ph.D. Thesis 2010
Lunemann and Nielsen, AFRICACRYPT 2011

Quantum NO Danger

Learning with Error (LWE)

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

Regev, STOC 2005

LWE-based Crypto Systems (FHE and etc)

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

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

Hallgren, Smith and Song, Crypto 11

Quantum Advantage

Quantum Advantage

qubits transmissions and classical post-processing

unconditional security based on physical laws

Quantum Advantage

qubits transmissions and classical post-processing

unconditional security based on physical laws

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

Examples

1970 - **quantum money** (Wiesner)

The first link between secrecy and quantum physics

The bill contains photons that bank “polarised” in random directions

(conjugate coding)

Examples

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

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

Examples

1970 - **quantum money** (Wiesner)

The first link between secrecy and quantum physics

The bill contains photons that bank "polarised" in random directions (conjugate coding)

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

Examples

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

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

Examples

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

Examples

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

Examples

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 - **coin flipping** (Chailloux and Kerenidis)

Perfect quantum CF is impossible, but better than classical protocols exist

with best possible bias 0.21 (Kitaev 03)

Examples

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 - **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 computing

Quantum NO Advantage

Quantum NO Advantage

Efficiency and Real Implementation

Quantum NO Advantage

Efficiency and Real Implementation

“what quantum mechanics takes away with one hand, it gives back with the other”

Nielsen and Chuang 2000

Quantum NO Advantage

Efficiency and Real Implementation

“what quantum mechanics takes away with one hand, it gives back with the other”

Nielsen and Chuang 2000

Pre-Post Quantum Crypto

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

boosting efficiency and security

of every task achievable against classical attackers against quantum attackers

Pre-Post Quantum Crypto - Examples

Pre-Post Quantum Crypto - Examples

Digital Signature

Coin Flipping

One Time Memory

Secure QMC

Delegated QC

Verification

Classically-controlled QC

Q Crypto: qubits transmissions and classical post-processing

Classically-controlled QC

Q Crypto: qubits transmissions and classical post-processing

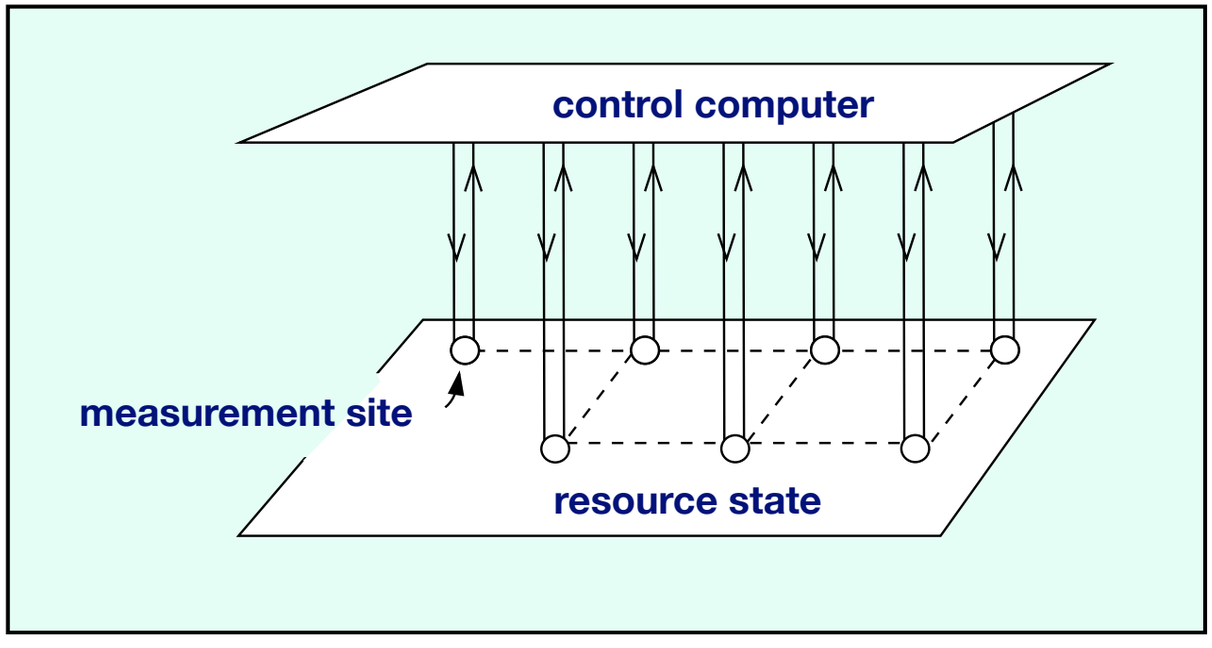
Teleportation Protocol

Classically-controlled QC

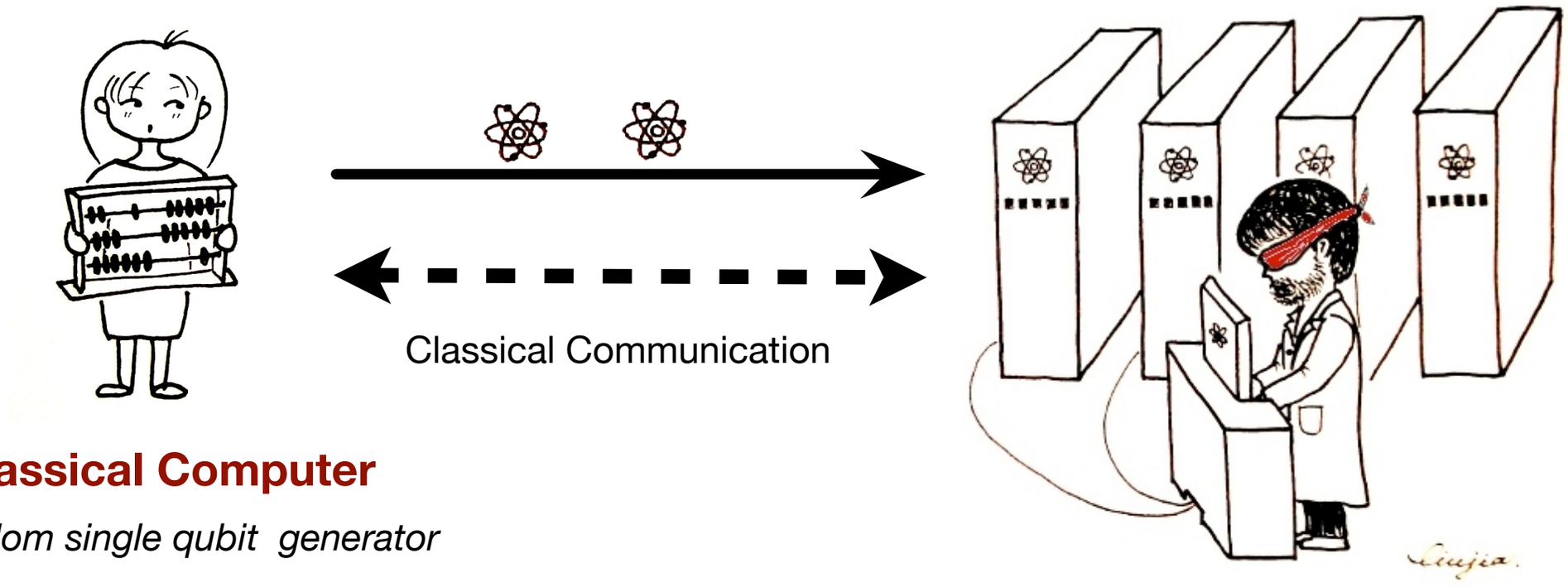
Q Crypto: qubits transmissions and classical post-processing

Teleportation Protocol

(universal) Q Comp: qubits transmissions and classical controlling



Q Crypt + Q Comp = Universal Blind QC



Classical Computer

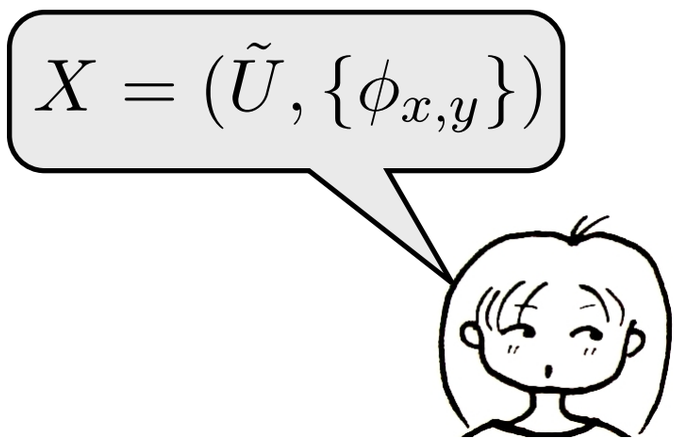
random single qubit generator

Unconditional Perfect Privacy

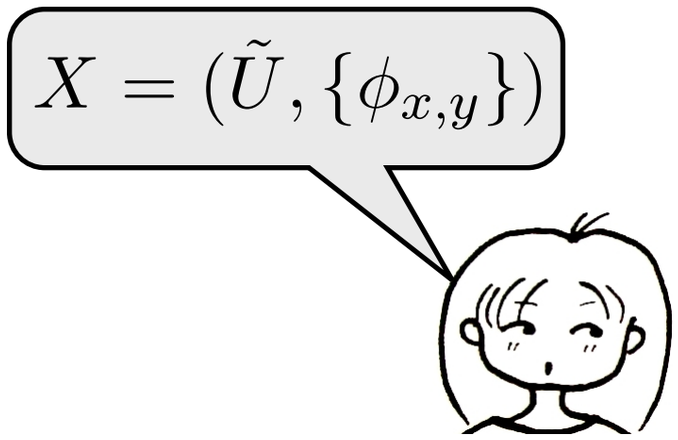
Server learns nothing about client's input/output/computation

Broadbent, Fitzsimons and Kashefi, FOCS 2009

UBQC Protocol

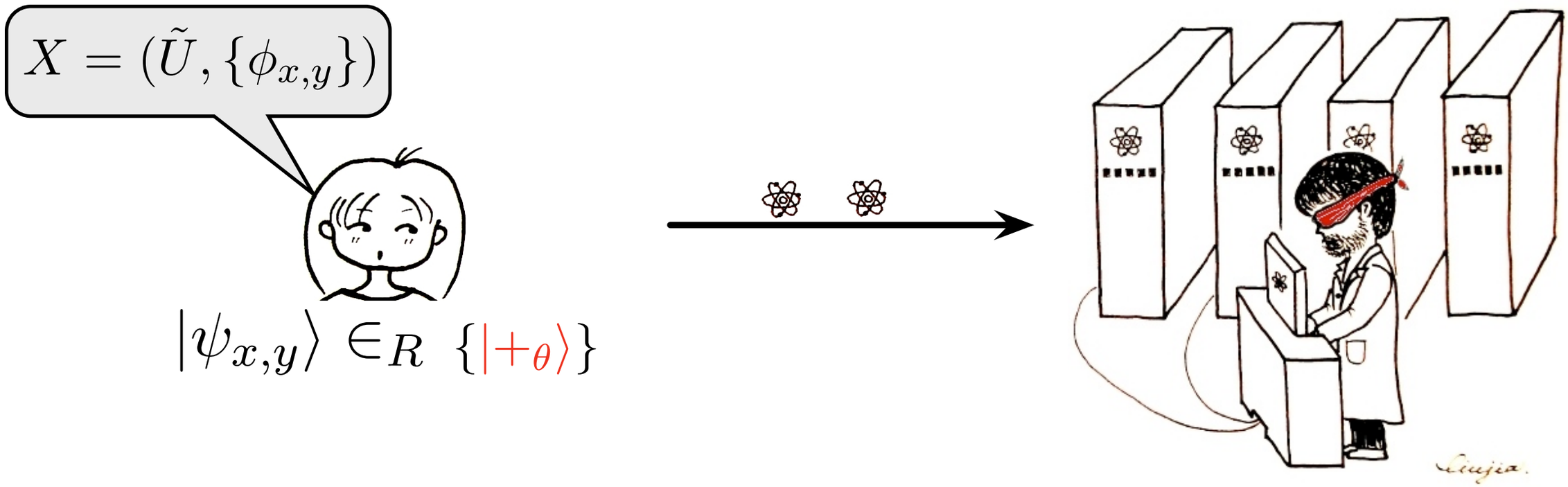


UBQC Protocol

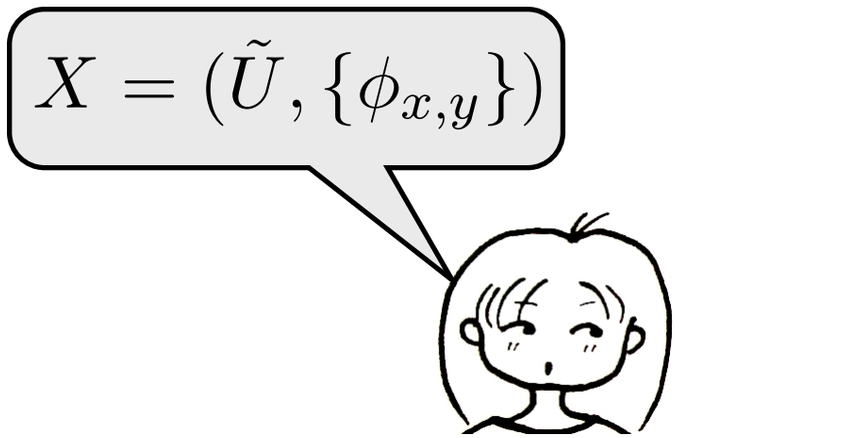


$|\psi_{x,y}\rangle \in_R \{|+_\theta\rangle\}$

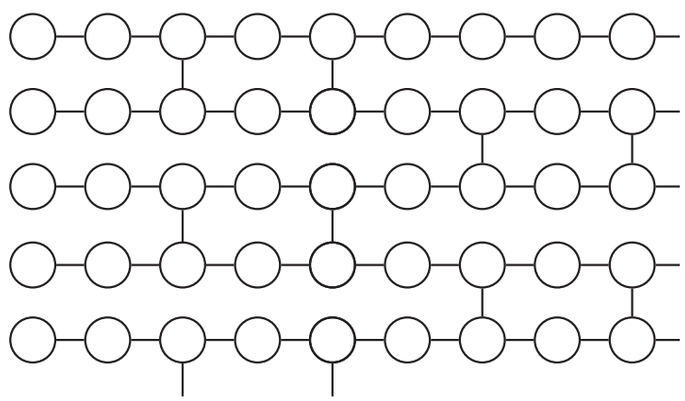
UBQC Protocol



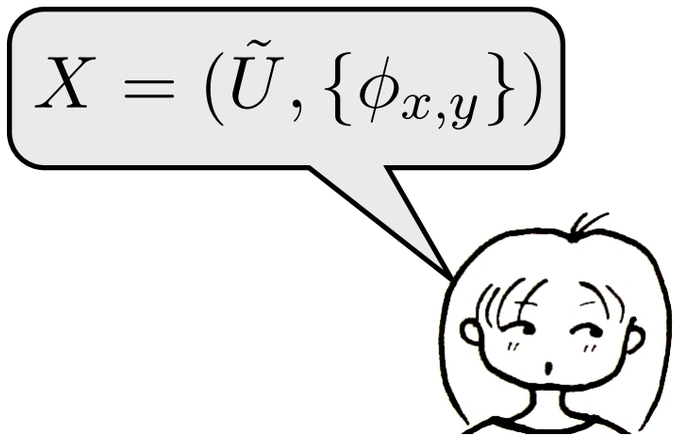
UBQC Protocol



$|\psi_{x,y}\rangle \in_R \{|+_\theta\rangle\}$

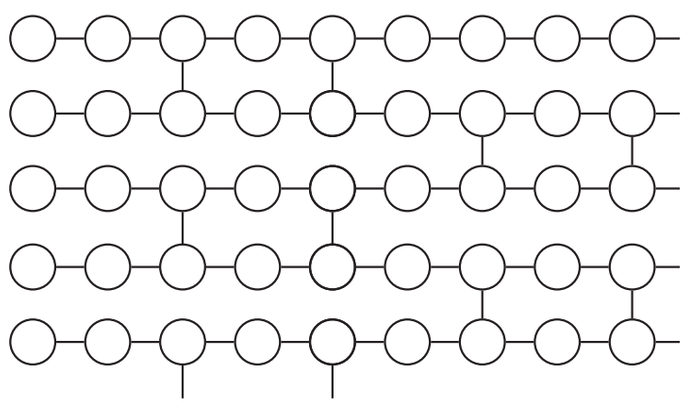


UBQC Protocol

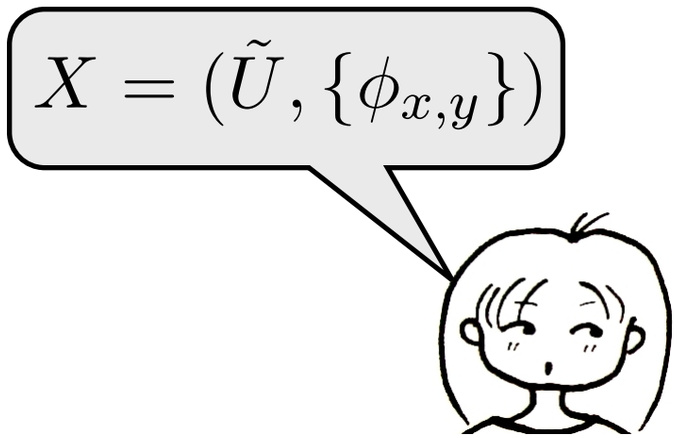


$|\psi_{x,y}\rangle \in_R \{|+_\theta\rangle\}$

$$\phi'_{x,y} = (-1)^{s^X_{x,y}} \phi_{x,y} + s^Z_{x,y} \pi$$



UBQC Protocol

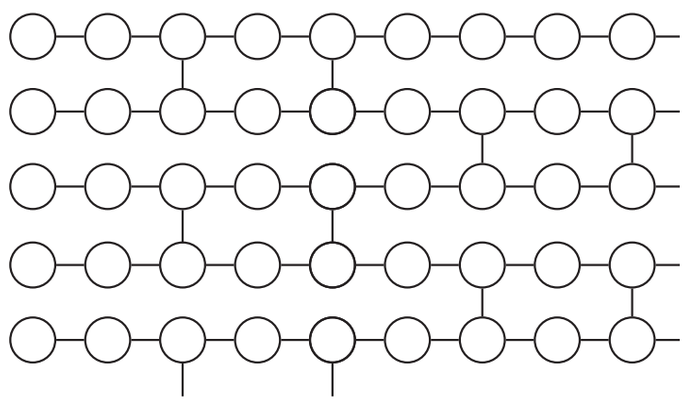


$$|\psi_{x,y}\rangle \in_R \{|+_\theta\rangle\}$$

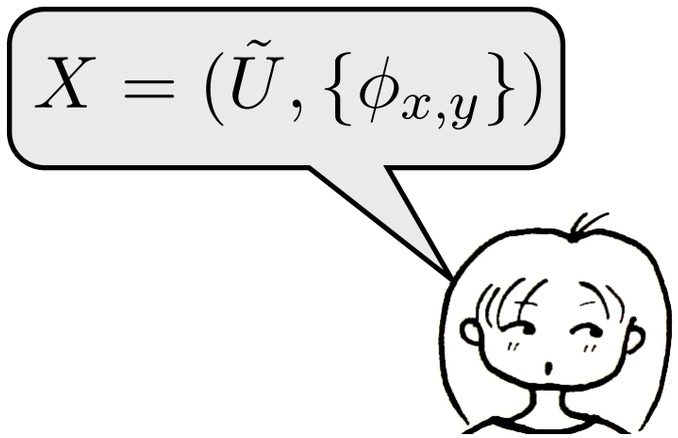
$$\phi'_{x,y} = (-1)^{s^X_{x,y}} \phi_{x,y} + s^Z_{x,y} \pi$$

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

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



UBQC Protocol

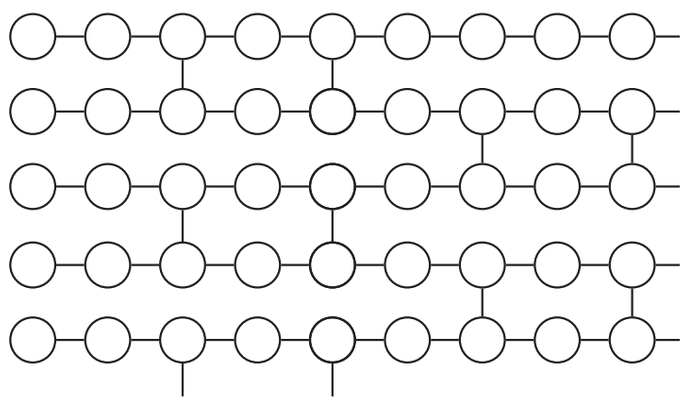


$|\psi_{x,y}\rangle \in_R \{|+_\theta\rangle\}$

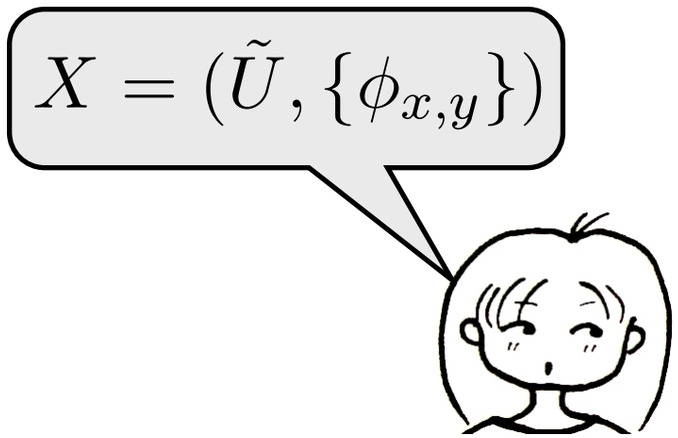
$$\phi'_{x,y} = (-1)^{s^X_{x,y}} \phi_{x,y} + s^Z_{x,y} \pi$$

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

$\delta_{x,y}$



UBQC Protocol



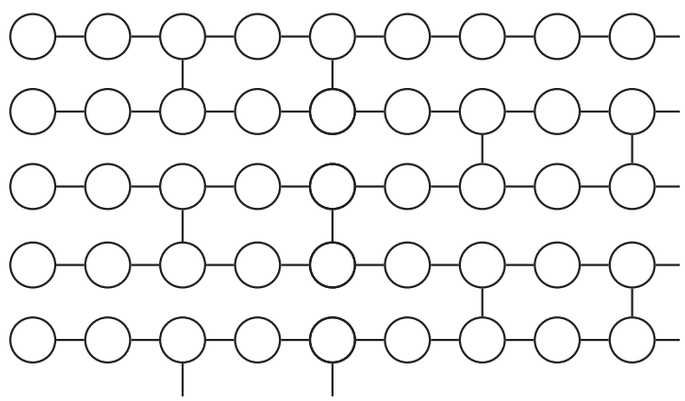
$|\psi_{x,y}\rangle \in_R \{|+_\theta\rangle\}$

$\phi'_{x,y} = (-1)^{s^X_{x,y}} \phi_{x,y} + s^Z_{x,y} \pi$

$\delta_{x,y}$

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

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



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

UBQC Protocol

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

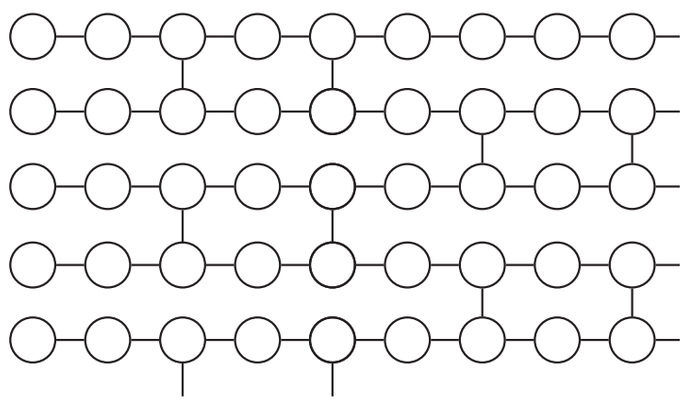
$|\psi_{x,y}\rangle \in_R \{|+_\theta\rangle\}$

$\phi'_{x,y} = (-1)^{s^X_{x,y}} \phi_{x,y} + s^Z_{x,y}\pi$

$\delta_{x,y}$

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

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



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

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

UBQC Protocol

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

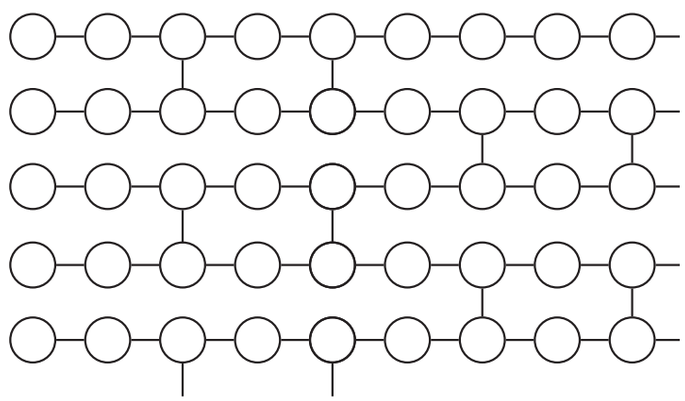
$|\psi_{x,y}\rangle \in_R \{|+_\theta\rangle\}$

$\phi'_{x,y} = (-1)^{s^X_{x,y}} \phi_{x,y} + s^Z_{x,y}\pi$

$\delta_{x,y}$

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

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



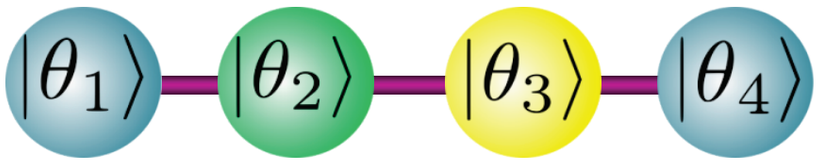
$\{|+_{\delta_{x,y}}\rangle, |-_{\delta_{x,y}}\rangle\}$

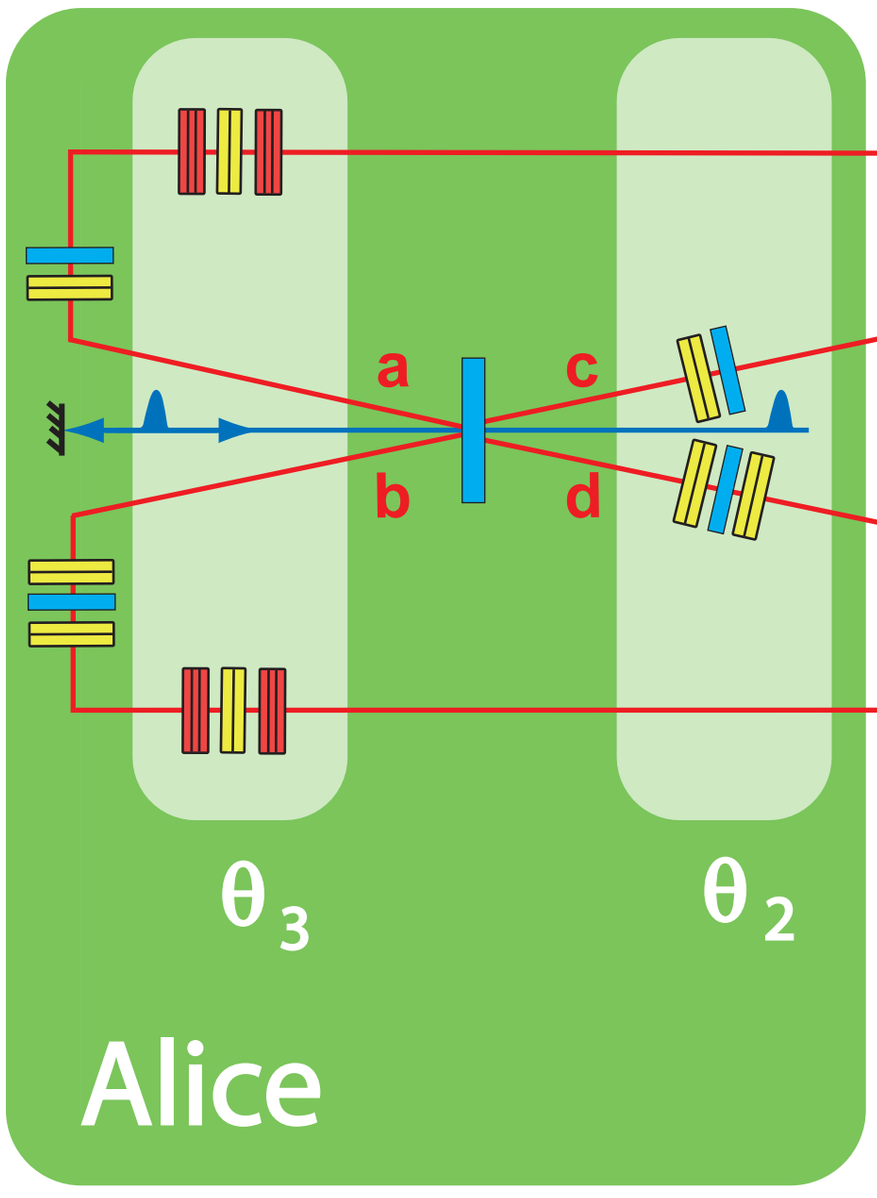
$s_{x,y} \in \{0,1\}$

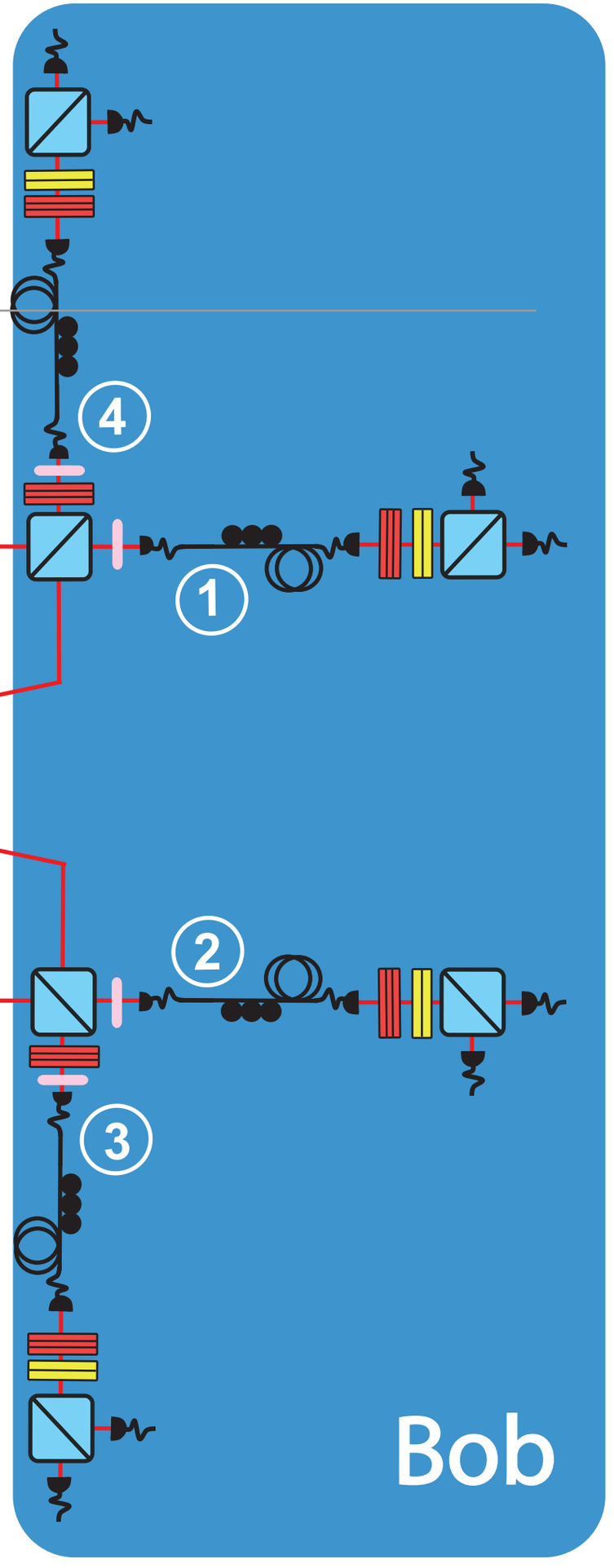
$s_{x,y} := s_{x,y} + r_{x,y}$

Experimental Implementation

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







UBQC for other tasks

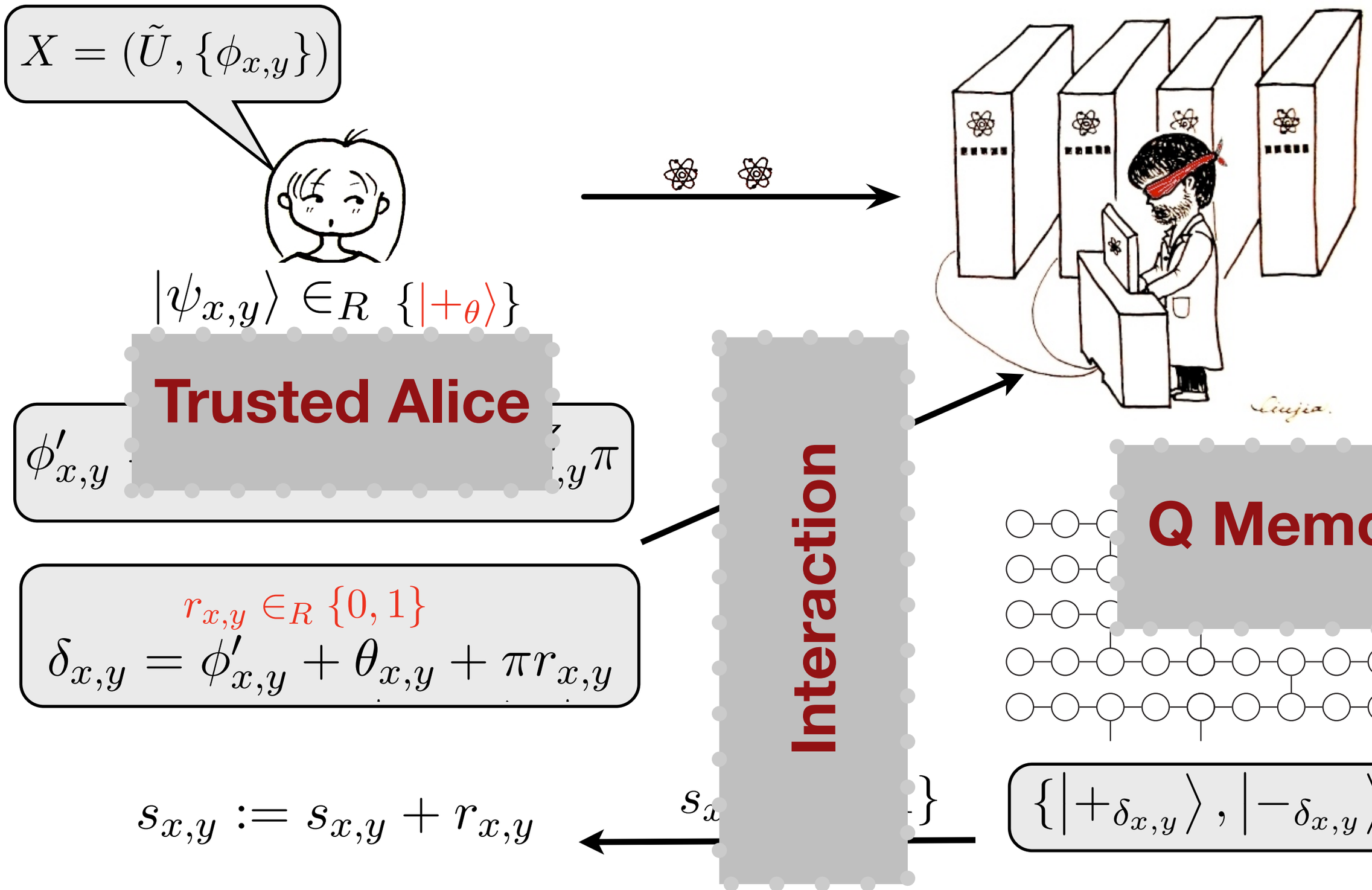
Yao Garbled Circuit

Fully Homomorphic Encryption

One-time program

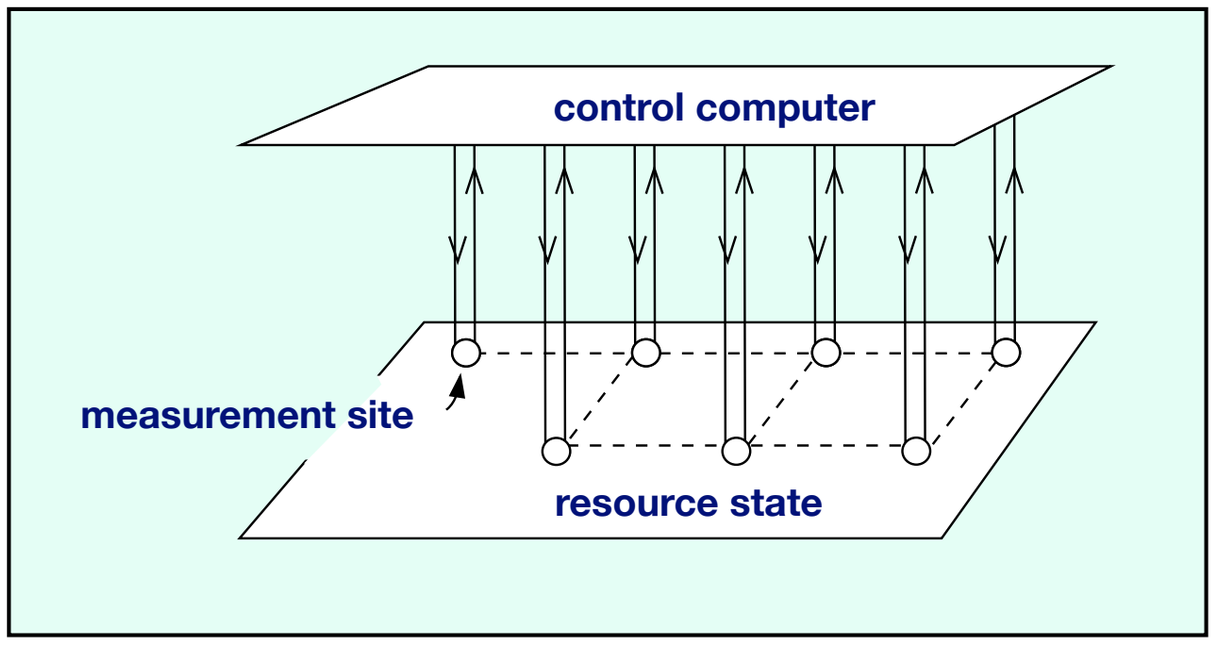
Secure Multi Party Computation

Issues about UBQC Protocol for other Crypto Tasks



Q Memory

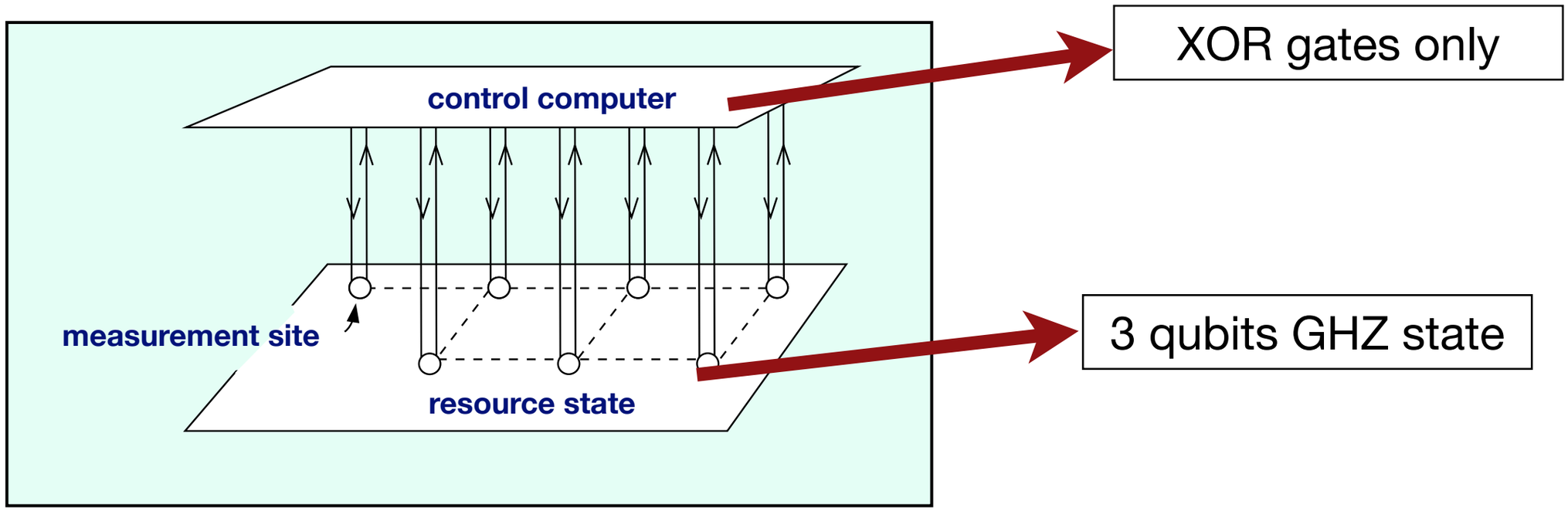
UBQC for secure evaluation of classical function



Anders and Browne, PRL, 2009

Q Memory

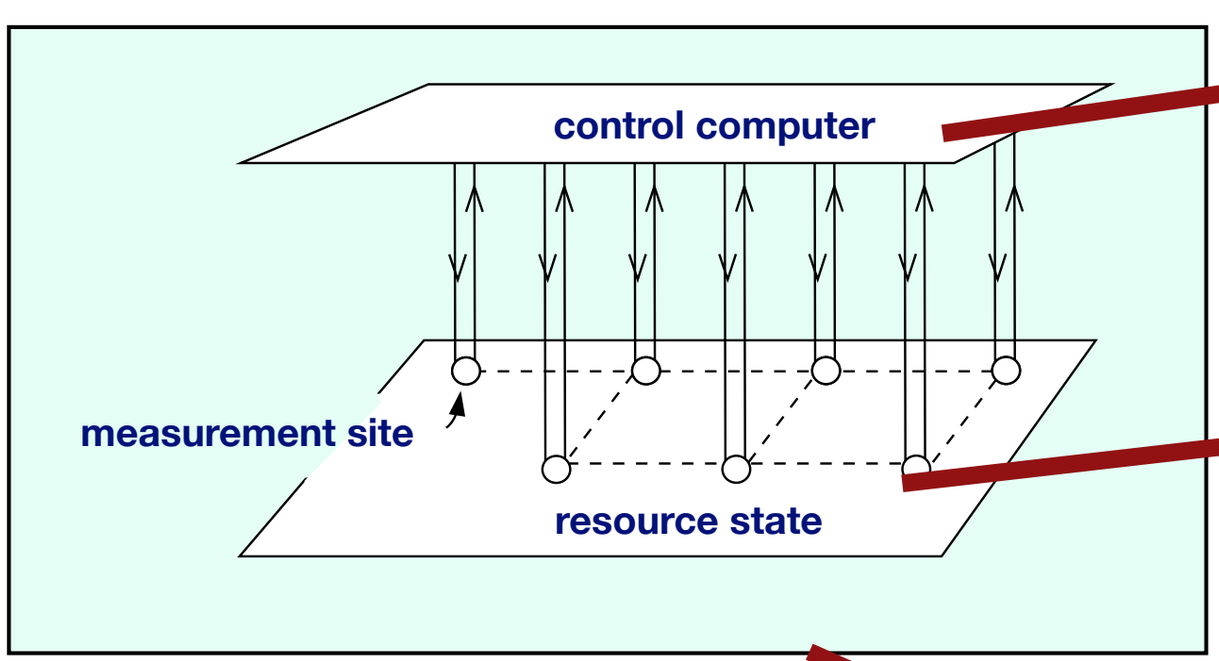
UBQC for secure evaluation of classical function



Anders and Browne, PRL, 2009

Q Memory

UBQC for secure evaluation of classical function



XOR gates only

3 qubits GHZ state

Universal Classical Computing

Anders and Browne, PRL, 2009

Restricted XOR Client

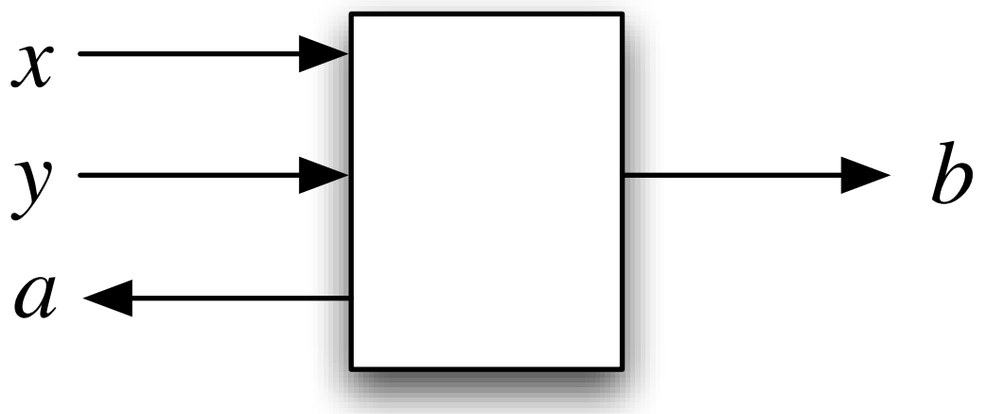
No classical protocol can delegate deterministically computation of NAND to a server while keeping the blindness

Dunjko and Kashefi, In preparation 2014

Restricted XOR Client

No classical protocol can delegate deterministically computation of NAND to a server while keeping the blindness

$$b = x.y + a$$

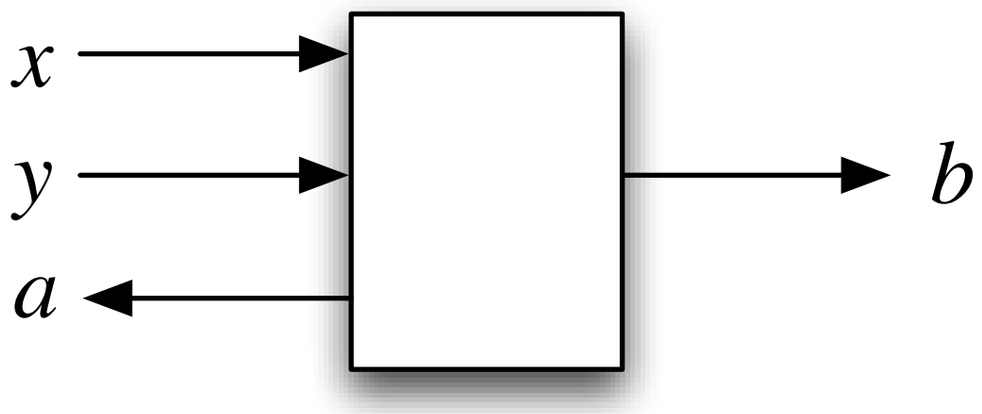


Dunjko and Kashefi, In preparation 2014

Restricted XOR Client

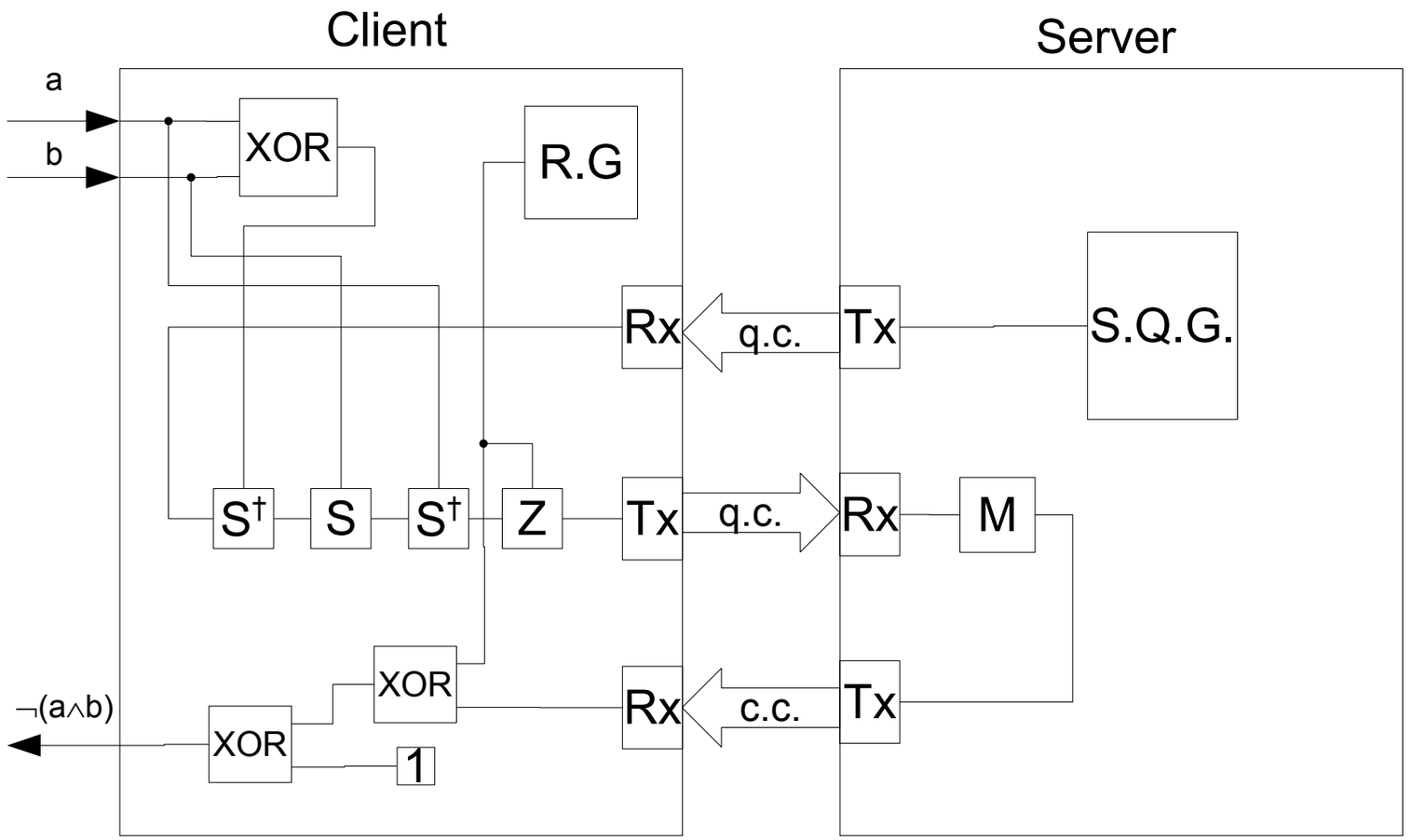
No **quantum offline** protocol can delegate deterministically computation of NAND to a server while keeping the blindness

$$b = x.y + a$$

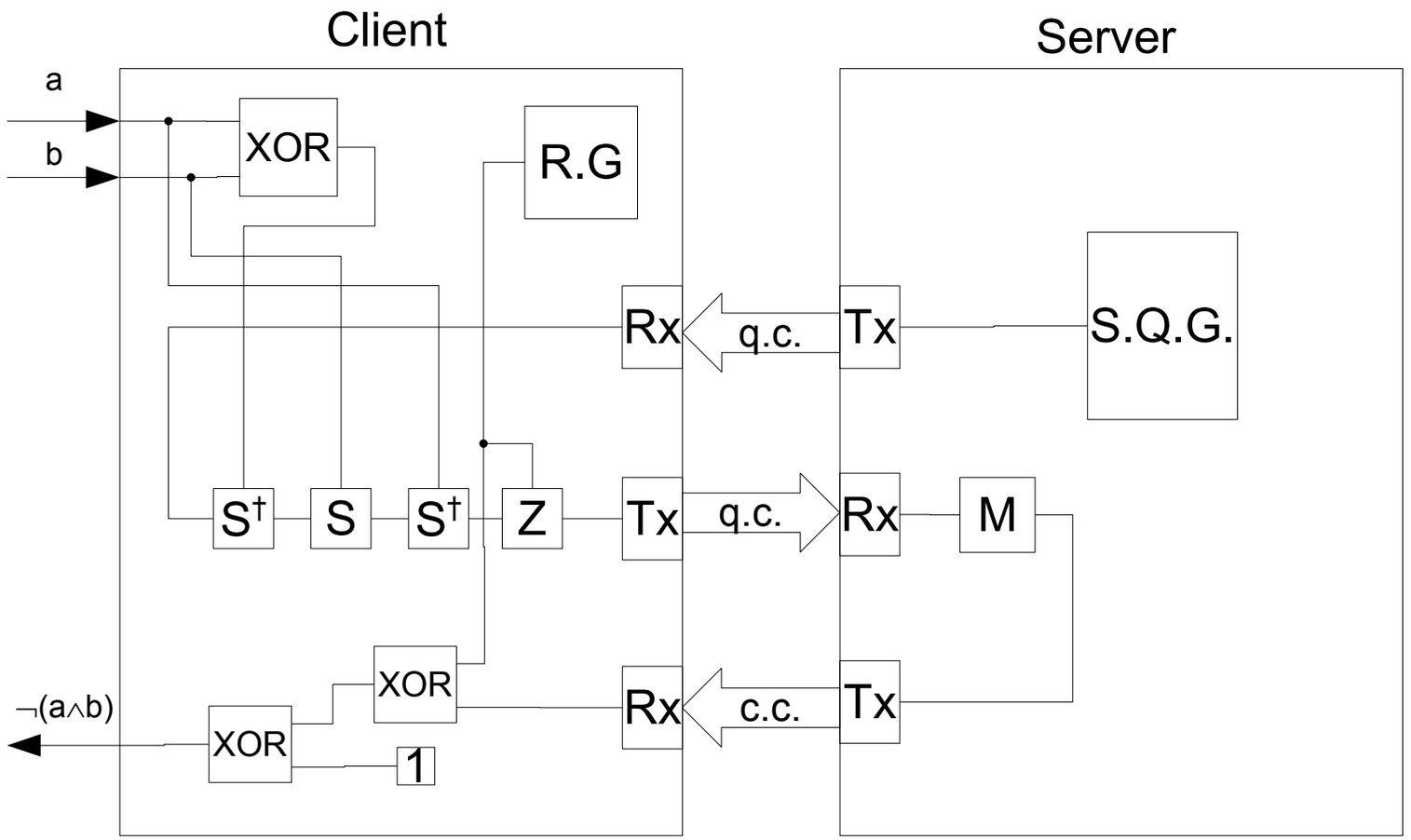


Quantum Communication

Quantum Communication



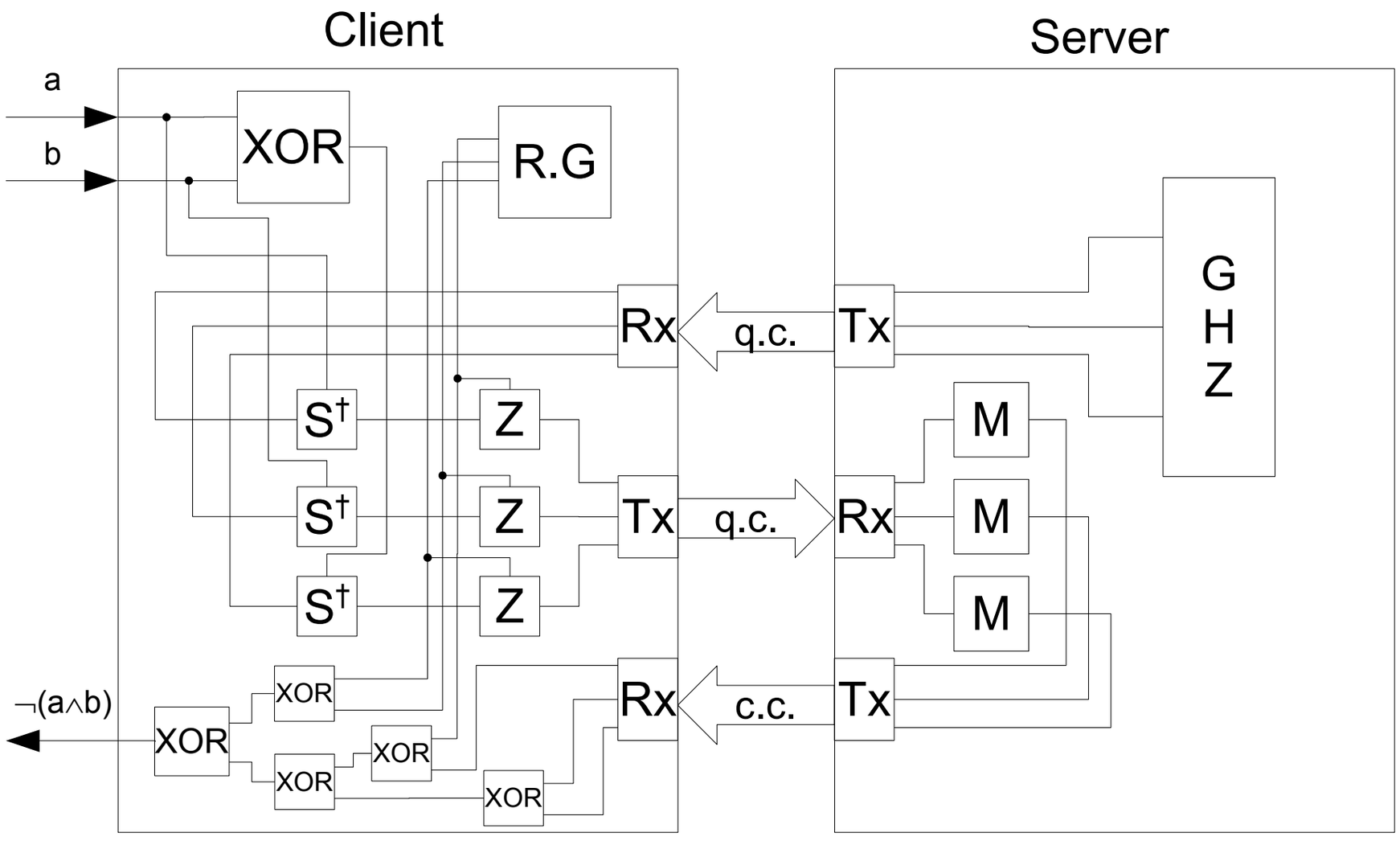
Quantum Communication



$$M^X\left(Z^a S^x S^y \left(S^\dagger\right)^{x\oplus y}|+\rangle\right)$$

measurement outcome $= x.y \oplus a \oplus 1$

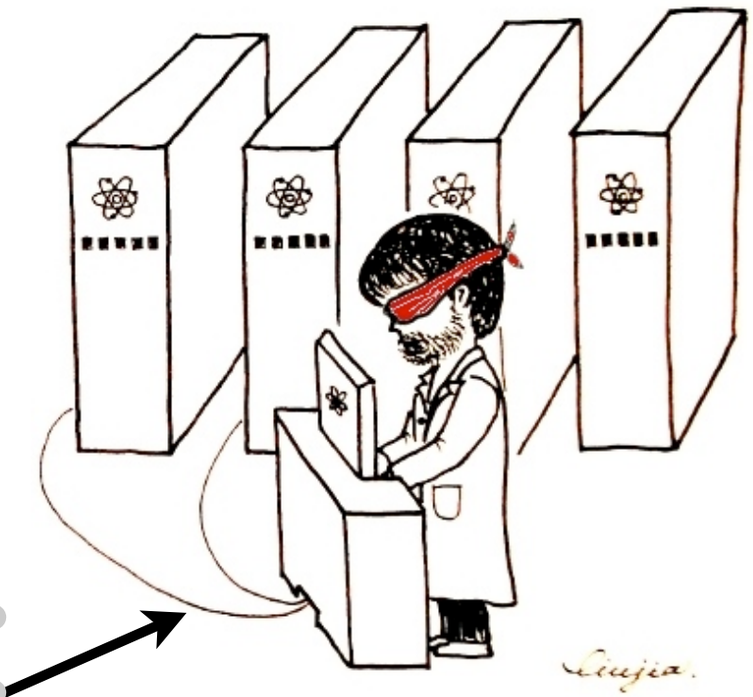
Quantum Communication



Issues about UBQC Protocol for other Crypto Tasks

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

$|\psi_{x,y}\rangle \in_R \{|+_\theta\rangle\}$

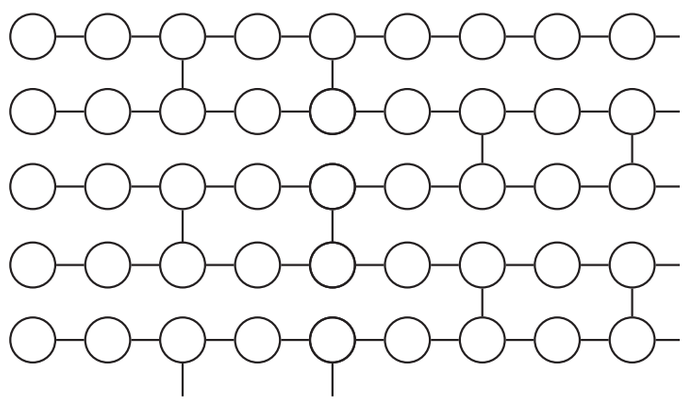


$\phi'_{x,y} = (-1)^{s^X_{x,y}} \phi_{x,y} + s^Z_{x,y}\pi$

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

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

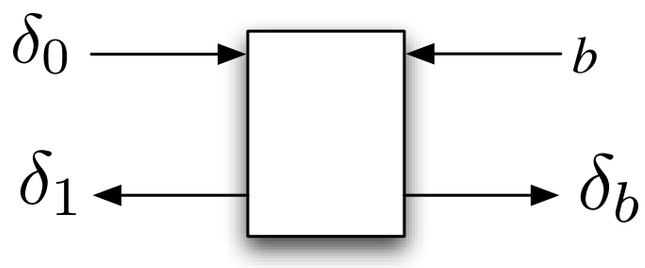
Interaction



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

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

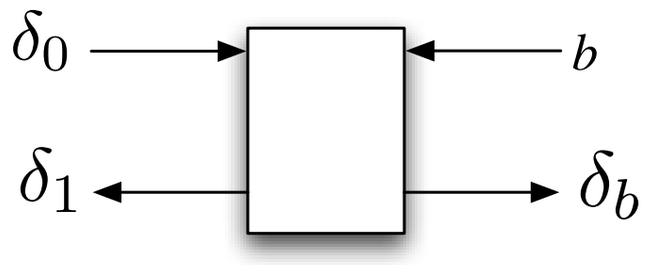
One-time Memory



Founding Cryptography on Tamper-Proof Hardware Tokens

Goldwasser, Kalai and Rothblum, Crypto, 2008
Goyal, Ishai, Sahai, Venkatesan, Wadai, TCC, 2010

One-time Memory



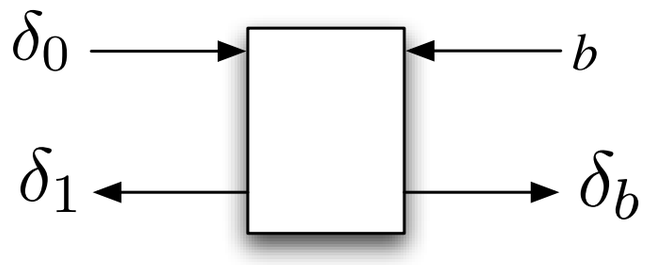
Founding Cryptography on Tamper-Proof Hardware Tokens

↓

Unconditional non-interactive secure computation

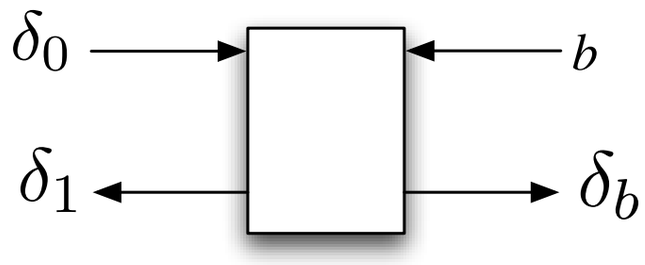
Goldwasser, Kalai and Rothblum, Crypto, 2008
Goyal, Ishai, Sahai, Venkatesan, Wadai, TCC, 2010

Non-interactive UBQC using OTM

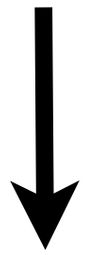


Kashefi, In preparation 2014

Non-interactive UBQC using OTM



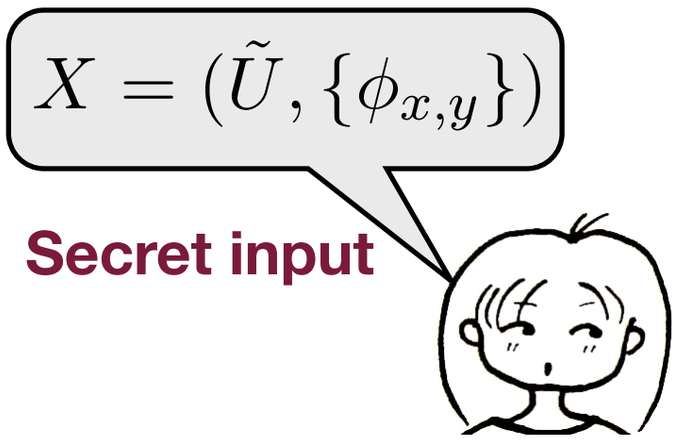
UBQC on a constant degree graph



Linear in the since of input circuit many OTM is required to make UBQC non-interactive

Kashefi, In preparation 2014

Somewhat QFHE



$$|\psi_{x,y}\rangle \in_R \{|+_\theta\rangle\}$$

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

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

Encryption

Somewhat QFHE

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

Secret input

Qubits and OTM

$$|\psi_{x,y}\rangle \in_R \{|+_\theta\rangle\}$$

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

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

Encryption

Somewhat QFHE

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

Secret input

Qubits and OTM

$$|\psi_{x,y}\rangle \in_R \{|+_\theta\rangle\}$$

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

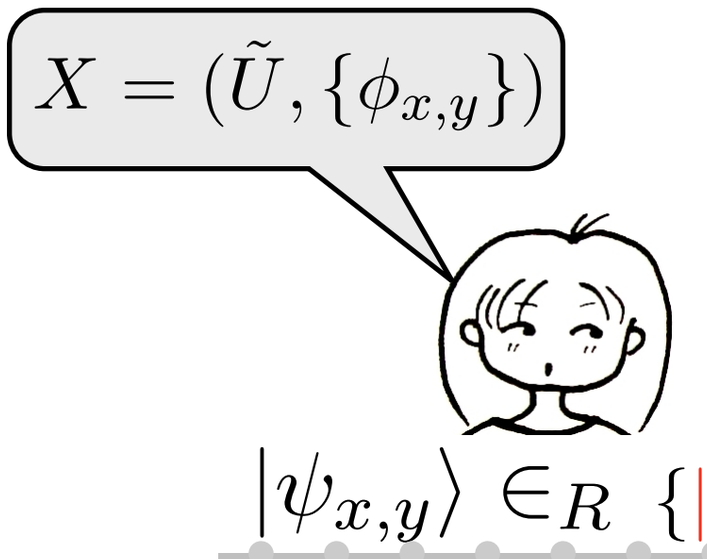
$$\delta_{x,y} = \phi'_{x,y} + \theta_{x,y} + \pi r_{x,y}$$

Encryption

Decryption

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

Verification



$|\psi_{x,y}\rangle \in_R \{|+_\theta\rangle\}$

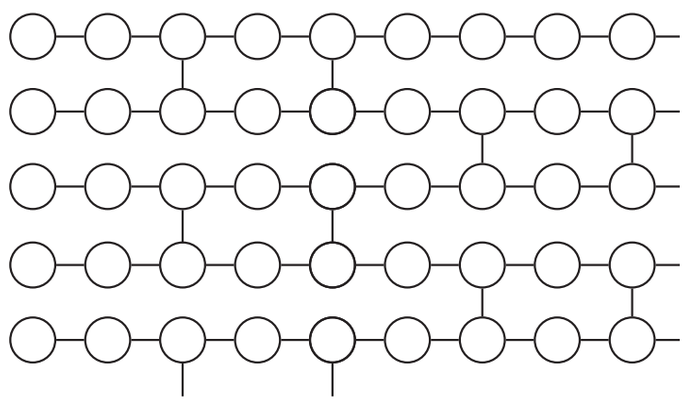
Trusted Alice

$\phi'_{x,y}$ ... $,y\pi$

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

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

$\delta_{x,y}$



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

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

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

Verification

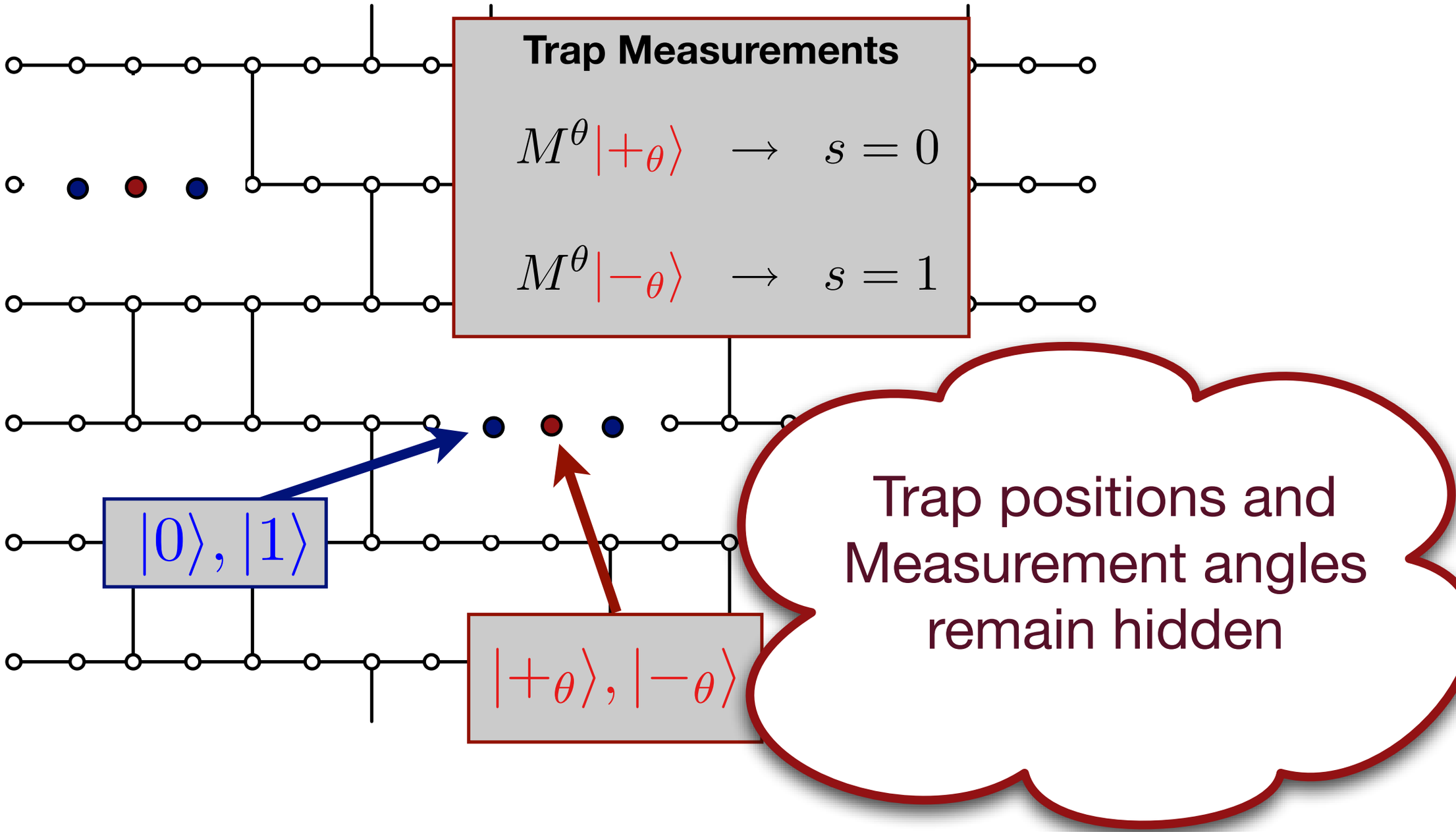
Verification

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

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

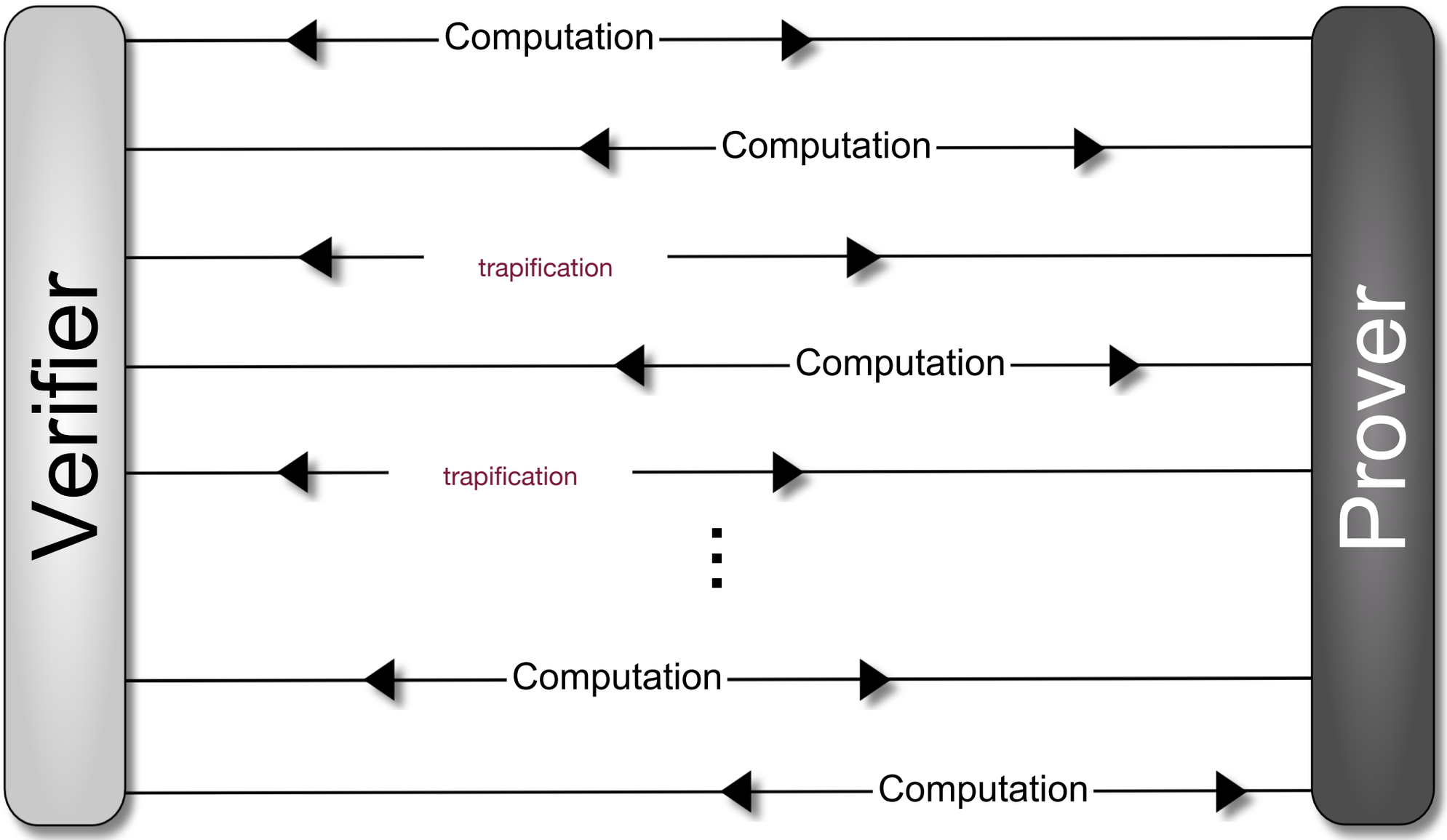
Fitzsimons and Kashefi, arXiv:1203.5217, 2012

Adding Traps - Verifying Bob only

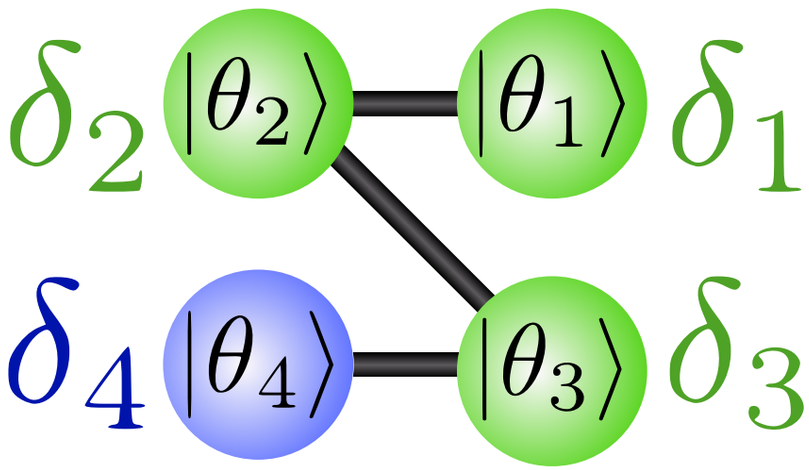


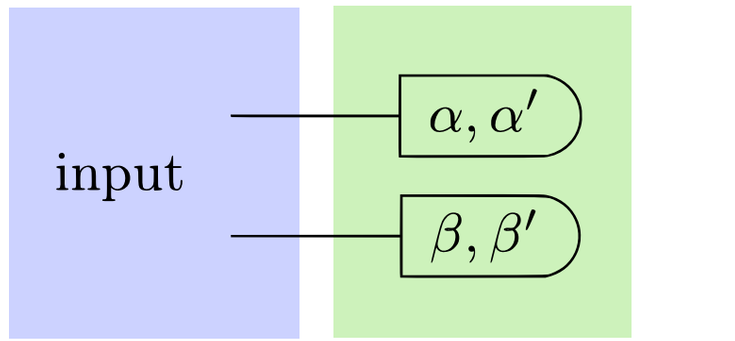
Verifying Bob

Verifying Bob



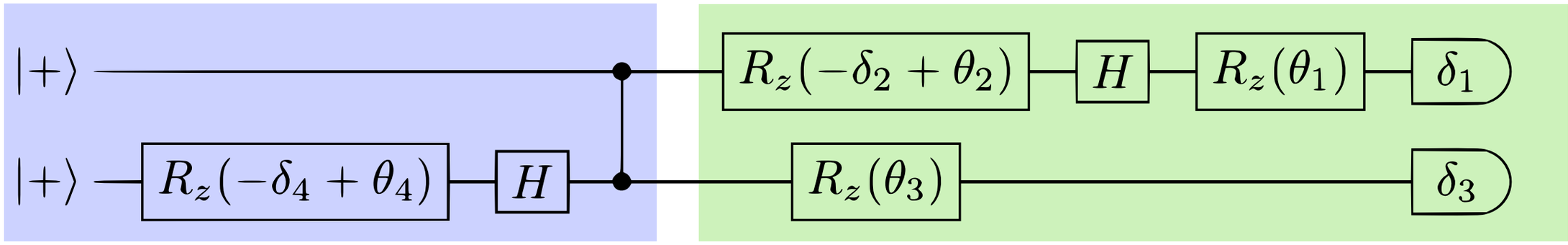
Blind Verification of Entanglement





State generation

Bell measurement



Blind state generation

Blind Bell test

Barz, Fitzsimons, Kashefi Walther. Nature Physcis 2013

Verifying Alice - Distributed UBQC - QSMC

Verifying Alice - Distributed UBQC - QSMC

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

Common Secret of Clients

Fulop, Kapourniotis, Kashefi,
In preparation 2014

Verifying Alice - Distributed UBQC - QSMC

$|\psi_1 x,y\rangle \in_R \{|+_\theta\rangle\}$

Private Secret of Client

$|\psi_2 x,y\rangle \in_R \{|+_\theta\rangle\}$

Private Secret of Client

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

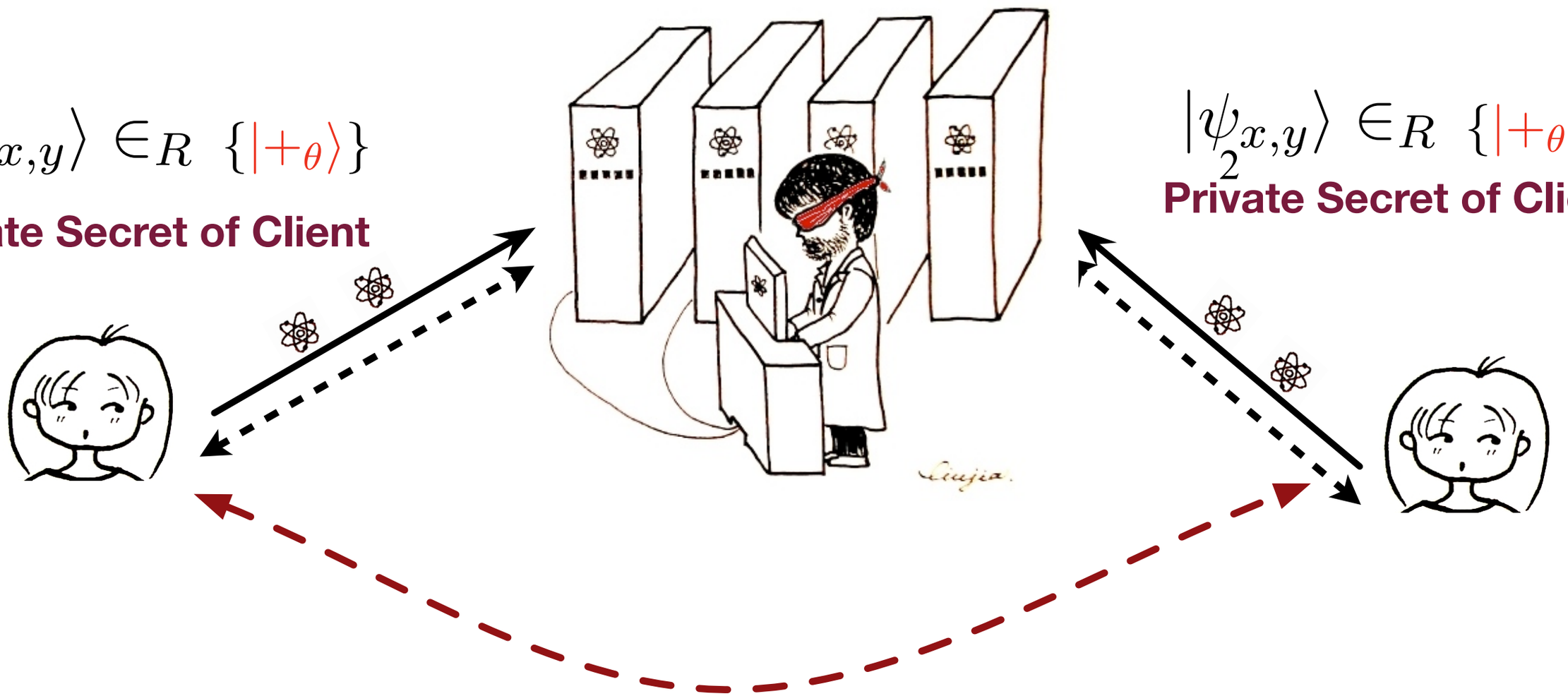
Common Secret of Clients

Fulop, Kapourniotis, Kashefi,
In preparation 2014

Verifying Alice - Distributed UBQC - QSMC

$|\psi_1 x,y\rangle \in_R \{|+_\theta\rangle\}$

Private Secret of Client



$|\psi_2 x,y\rangle \in_R \{|+_\theta\rangle\}$

Private Secret of Client

Classical Secure Function Evaluation

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

Common Secret of Clients

Fulop, Kapourniotis, Kashefi, In preparation 2014

Pre-Post Quantum Crypto

A hybrid network of **LWE-based FHE** with **UBQC gadgetds**

boosting efficiency and security

of classical delegated computing against quantum attackers