Quantum Verification

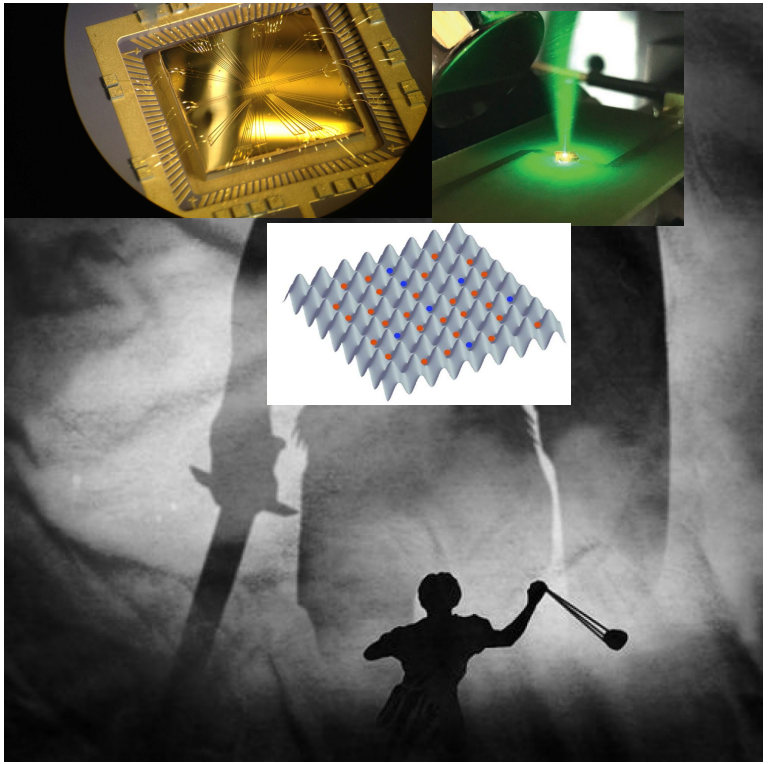
Elham Kashefi

University of Edinburgh
CNRS LIP6 Sorbonne Universite
VeriQloud Ltd

Quantum DRAMA

A powerful quantum device

Verifier (with restricted computational power)

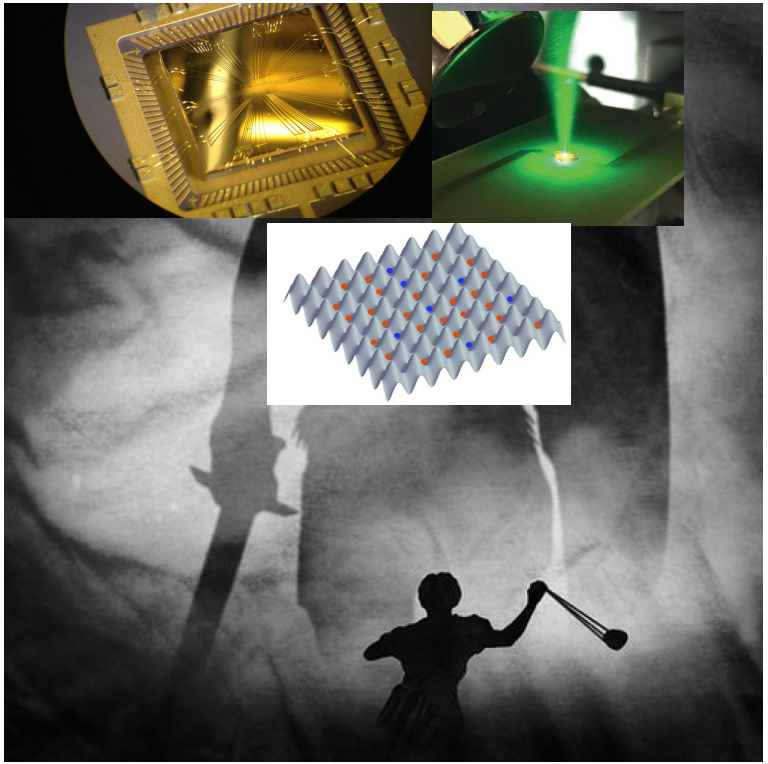


Quantum DRAMA

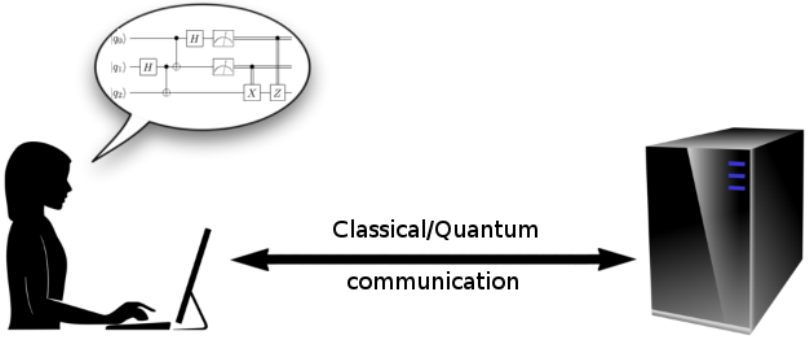
Quantum Advantage

VS

Quantum Devices Noise

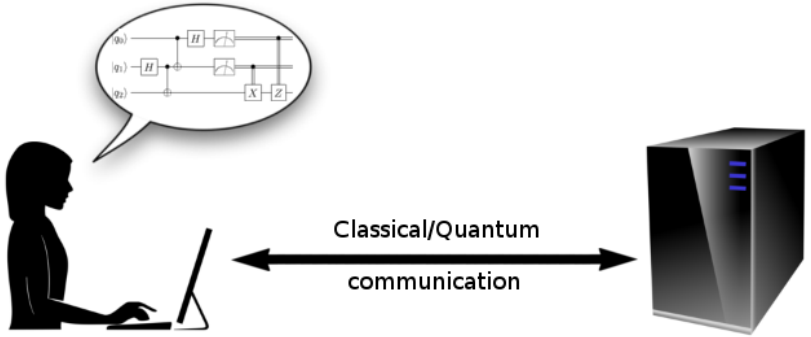


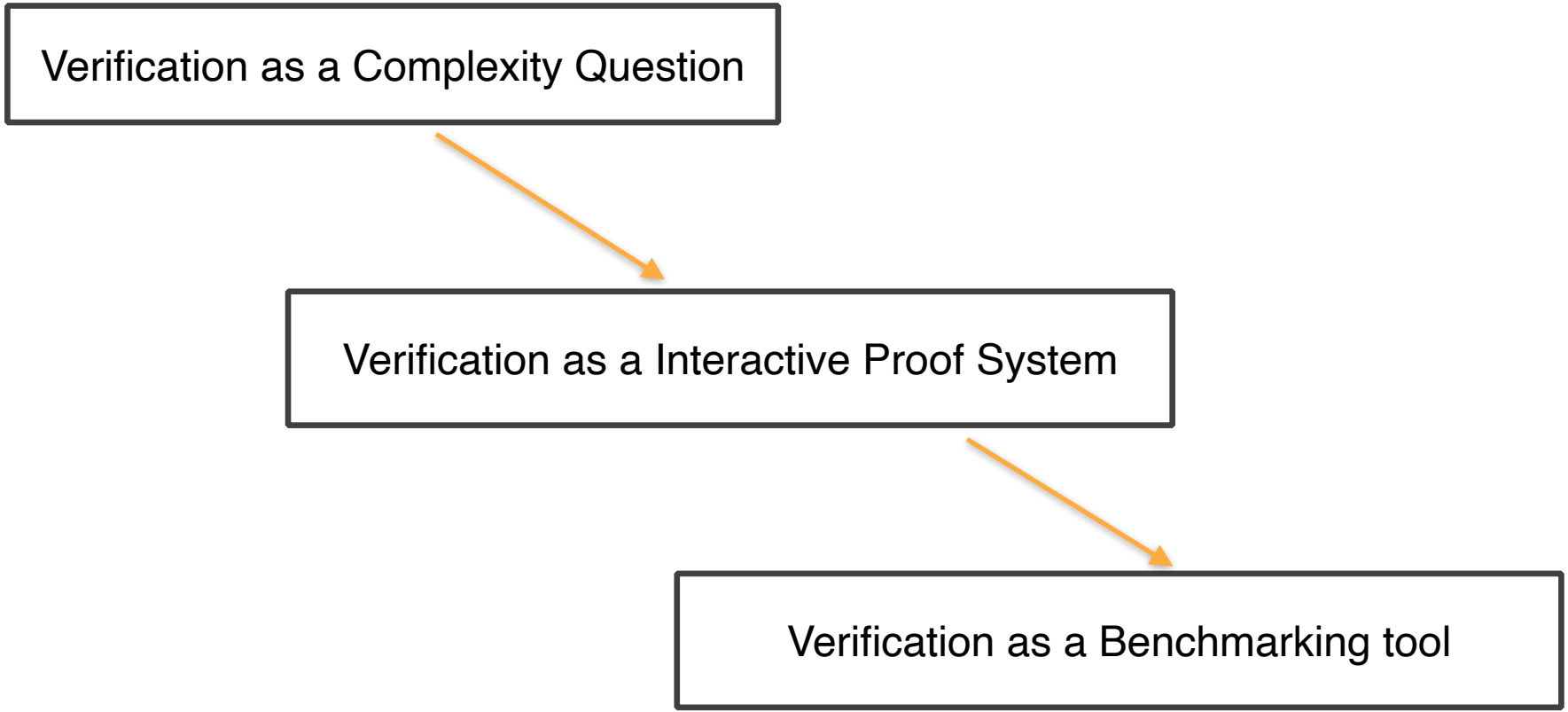
Quantum Verification



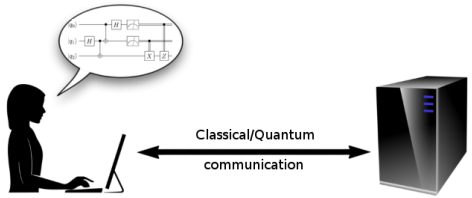
Quantum Verification

- Computationally limited verifier
- Powerful quantum server(s)
- Certify the correctness of the computation




Verification as a Complexity Question
Verification as a Interactive Proof System
Verification as a Benchmarking tool

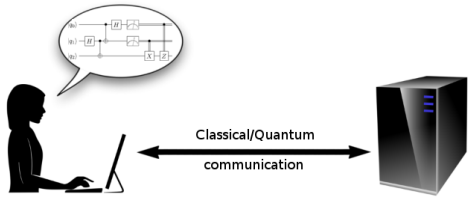
Complexity as Interactive Proof System



A **PROTOCOL** between

probabilistic polynomial-time verifier V
&
computationally unrestricted prover P

Complexity as Interactive Proof System

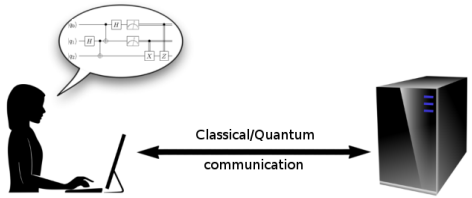


A **PROTOCOL** between

probabilistic polynomial-time verifier V
&
computationally unrestricted prover P

Completeness: $(\forall x \in L)\ \Pr\left[(V \leftrightarrow P)(x)\ accepts\right] = 1$

Complexity as Interactive Proof System



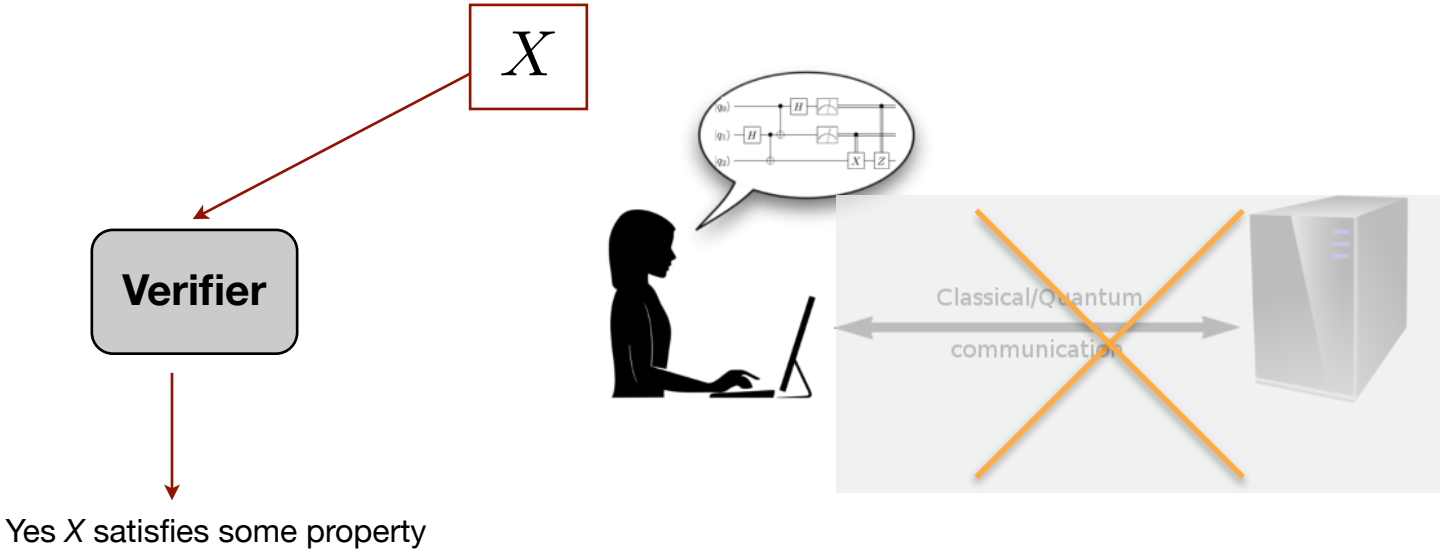
A **PROTOCOL** between

probabilistic polynomial-time verifier V
&
computationally unrestricted prover P

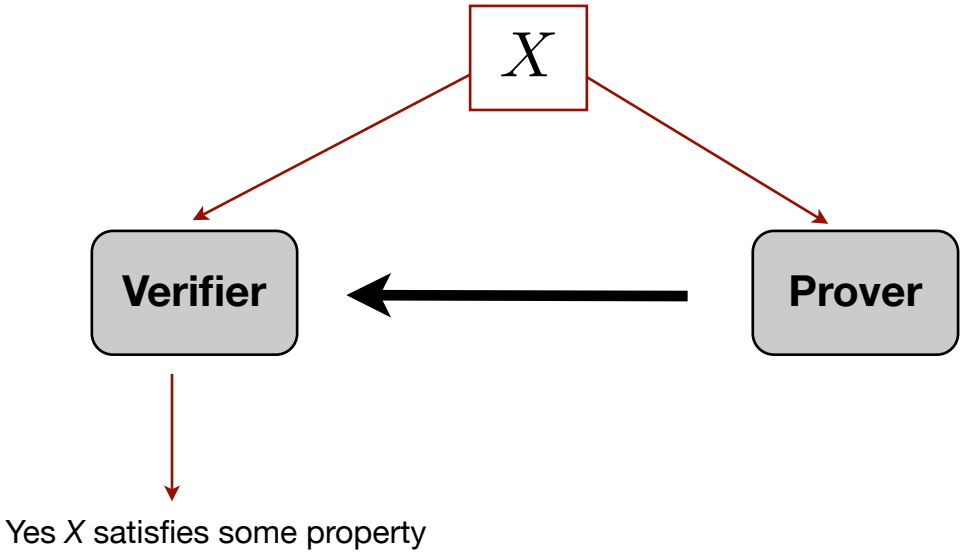
Completeness: $(\forall x \in L)\ \Pr\left[(V \leftrightarrow P)(x)\ accepts\right] = 1$

Soundness: $(\forall x \notin L)(\forall P')\ \Pr\left[(V \leftrightarrow P')(x)\ accepts\right] \leq \frac{1}{2}$

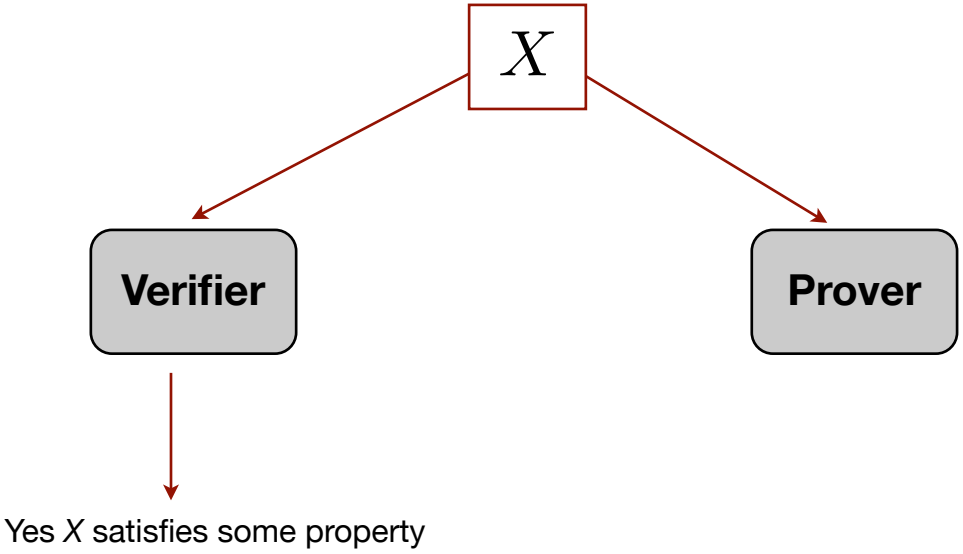
BPP as Interactive Proof System



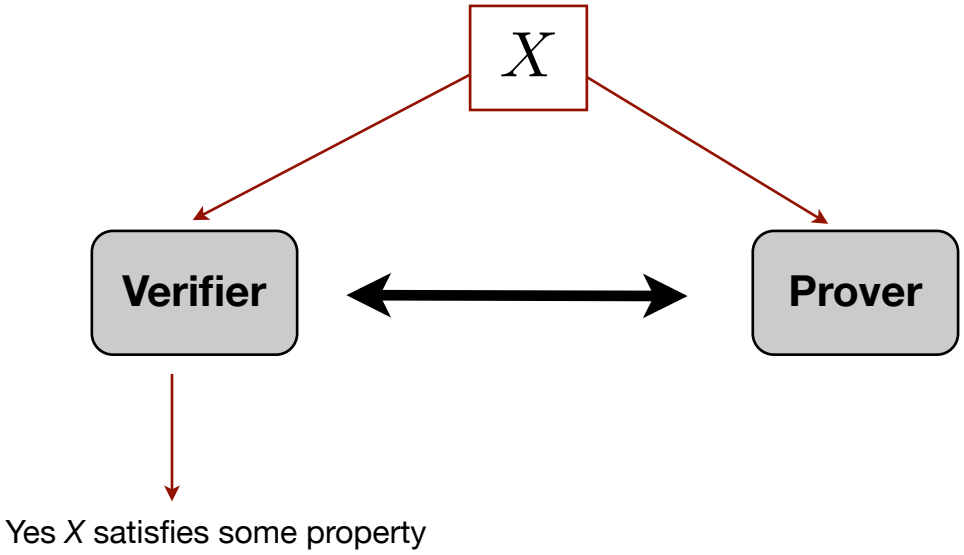
NP as Interactive Proof System



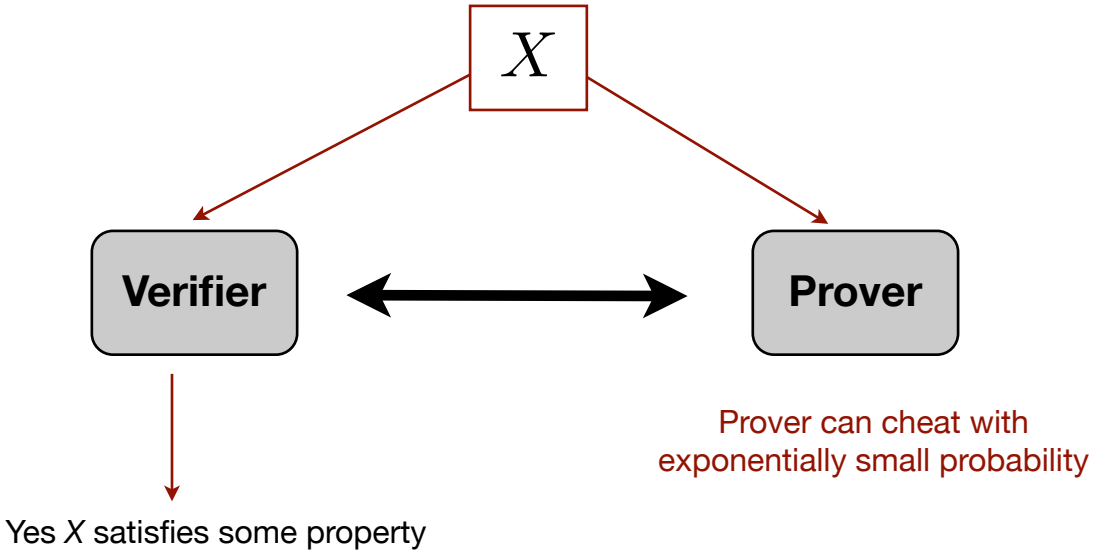
PolySpace as Interactive Proof System



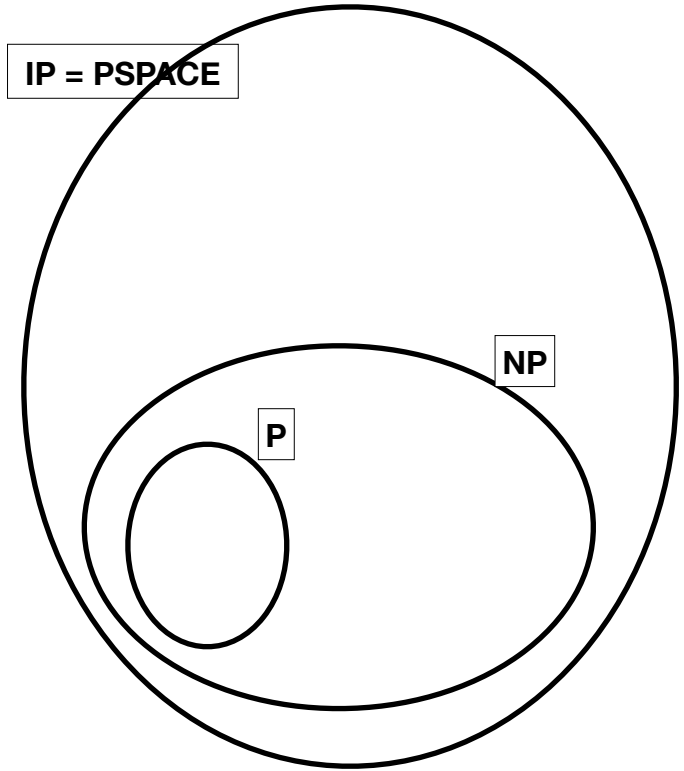
PolySpace as Interactive Proof System



PolySpace as Interactive Proof System

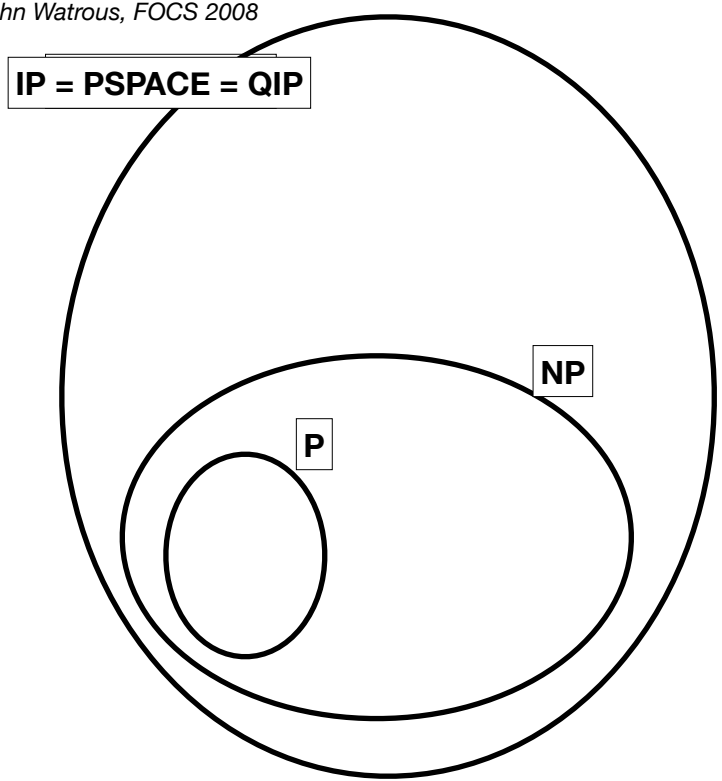


Complexity as Interactive Proof System



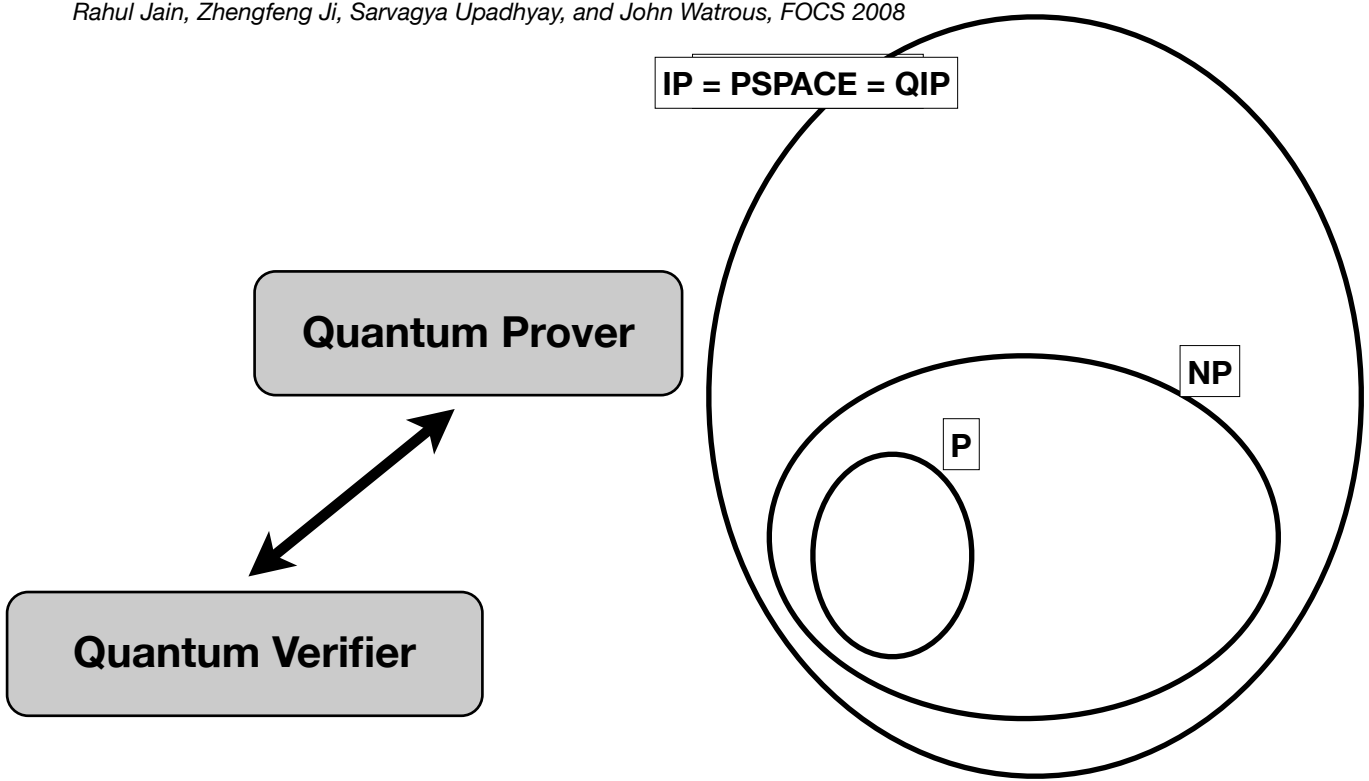
Complexity as Interactive Proof System

Rahul Jain, Zhengfeng Ji, Sarvagya Upadhyay, and John Watrous, FOCS 2008



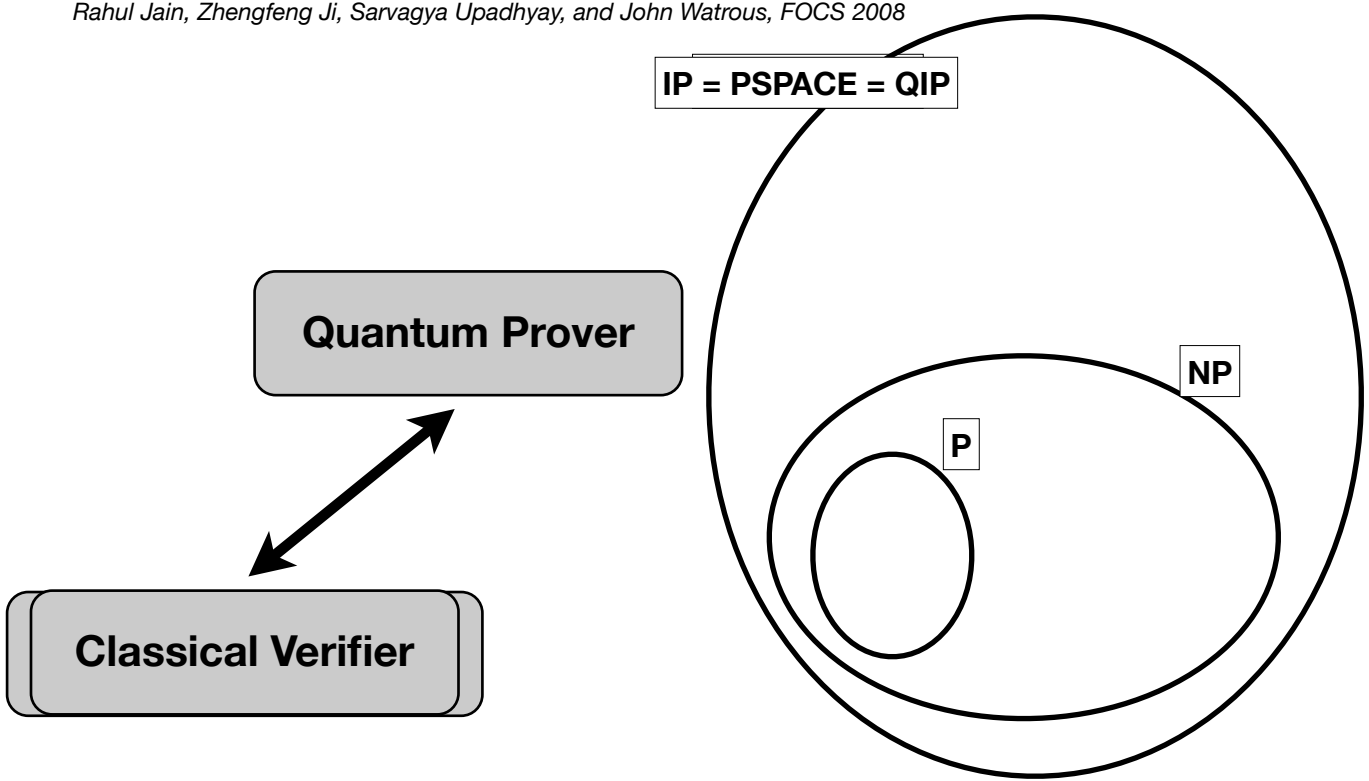
Complexity as Interactive Proof System

Rahul Jain, Zhengfeng Ji, Sarvagya Upadhyay, and John Watrous, FOCS 2008



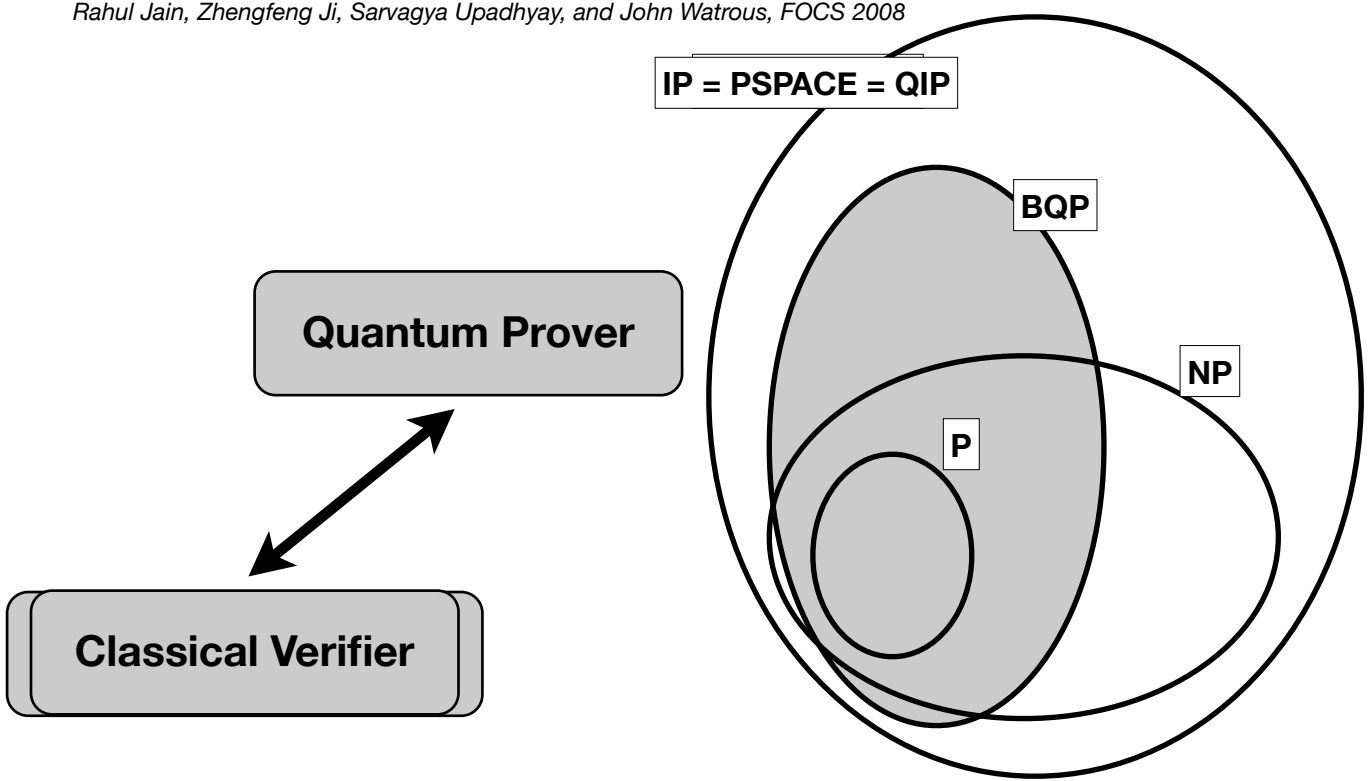
Complexity as Interactive Proof System

Rahul Jain, Zhengfeng Ji, Sarvagya Upadhyay, and John Watrous, FOCS 2008



Complexity as Interactive Proof System

Rahul Jain, Zhengfeng Ji, Sarvagya Upadhyay, and John Watrous, FOCS 2008



Towards Practical Verification

Gottesman (04) - Vazirani (07) - Aaronson $25 Challenge (07)

Does BQP admit a quantum interactive protocol
where the honest prover is in BQP and the verifier is in BPP?

Towards Practical Verification

Gottesman (04) - Vazirani (07) - Aaronson $25 Challenge (07)

Does BQP admit a quantum interactive protocol
where the honest prover is in BQP and the verifier is in BPP?

Yes, if verifier can prepare some random qubits

Aharonov, Ben-Or, and Eban, ICS 2010
Broadbent, Fitzsimons and Kashefi, FOCS 2009

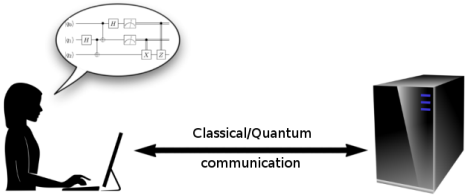
Yes, if provers are entangled but none-communicating

Reichardt, Unger, Vazirani, Nature 2013

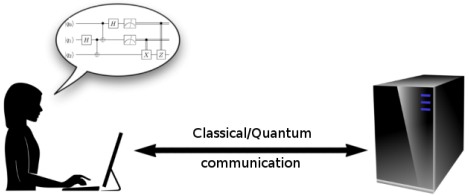
Yes, if malicious prover cannot break LWE

Mahadev, FOCS 2018

Quantum Interactive Proof System



Quantum Interactive Proof System



- Correctness: in the absence of any *interference/noise/deviation*, verifier accepts and the computation output is correct

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

Quantum Interactive Proof System

Gheorghiu, Kapourniotis, Kashefi

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

x the input to this circuit, then $n = |x|$, $N = |\mathcal{C}|$

Quantum Interactive Proof System

Gheorghiu, Kapourniotis, Kashefi

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

Quantum Interactive Proof System

Gheorghiu, Kapourniotis, Kashefi

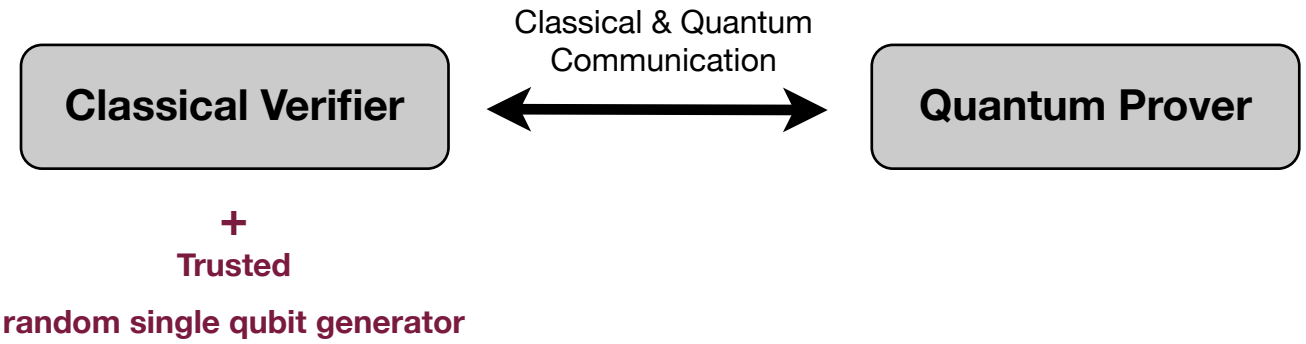
Multi-prover entanglement-based

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

Prepare and Send Verification



Soundness

Verifier

ν

random parameters

Soundness

Verifier **Prover/Device**

ν

random parameters

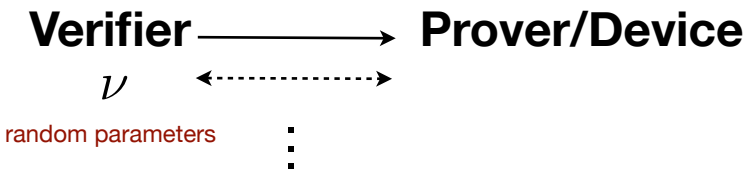
Soundness

Verifier $\longrightarrow$ **Prover/Device**

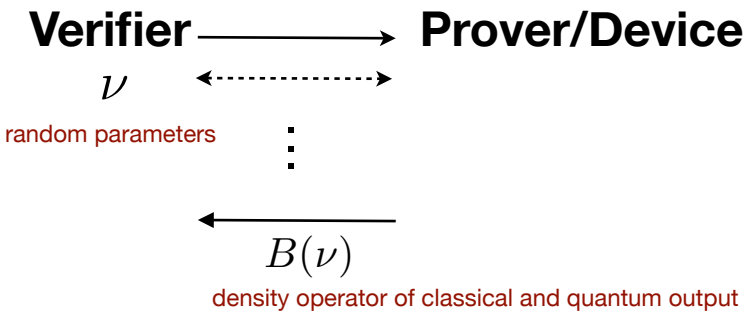
ν

random parameters

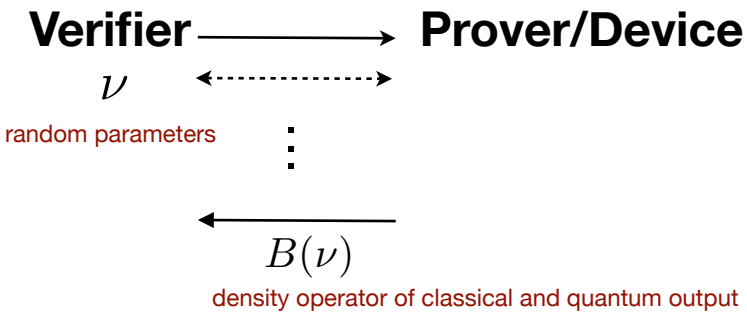
Soundness



Soundness


Verifier
Prover/Device
ν
random parameters
$B(\nu)$
density operator of classical and quantum output

Soundness

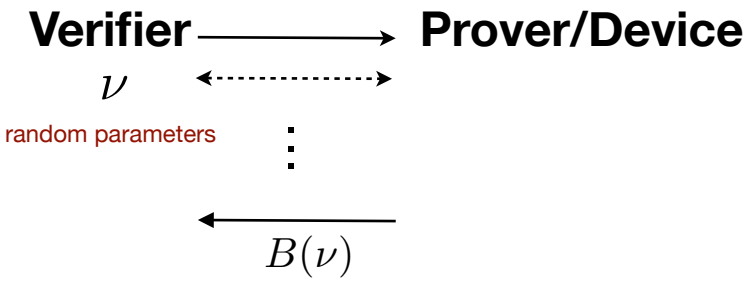


For any

Prover's deviation/cheating strategy
(Any noise/failure model)

the probability of verifier accepting an incorrect outcome density operator is bounded by ε:

Soundness



For any

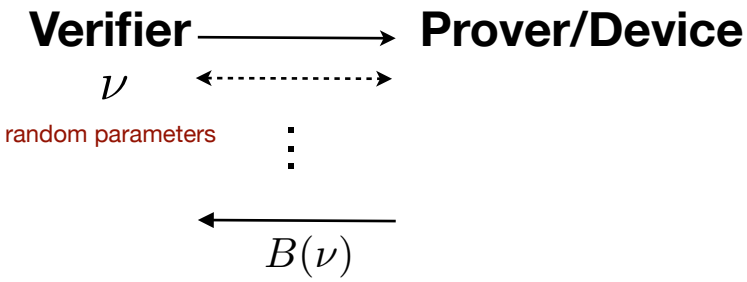
Prover's deviation/cheating strategy
(Any noise/failure model)

the probability of verifier accepting an incorrect outcome density operator is bounded by ε:

$$P^{\nu}_{incorrect} = (\mathbb{I} - |\Psi^{\nu}_{ideal}\rangle\langle\Psi^{\nu}_{ideal}|) \otimes |r^{\nu}_{t}\rangle\langle r^{\nu}_{t}|$$

Accept Key

Soundness



For any

Prover's deviation/cheating strategy
(Any noise/failure model)

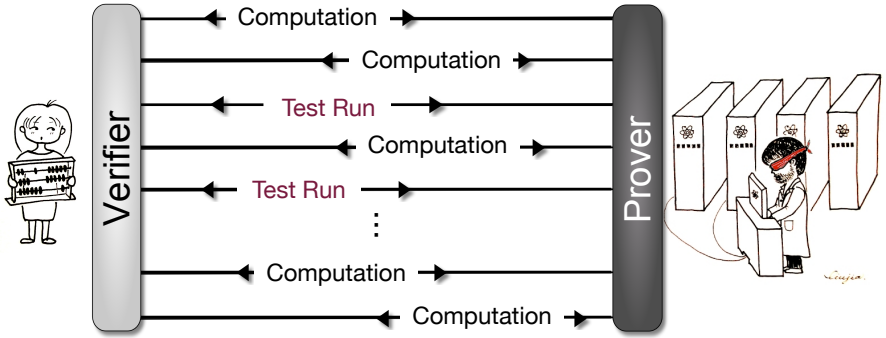
the probability of verifier accepting an incorrect outcome density operator is bounded by ε:

$$P^{\nu}_{incorrect} = (\mathbb{I} - |\Psi^{\nu}_{ideal}\rangle\langle\Psi^{\nu}_{ideal}|) \otimes |r^{\nu}_{t}\rangle\langle r^{\nu}_{t}|$$

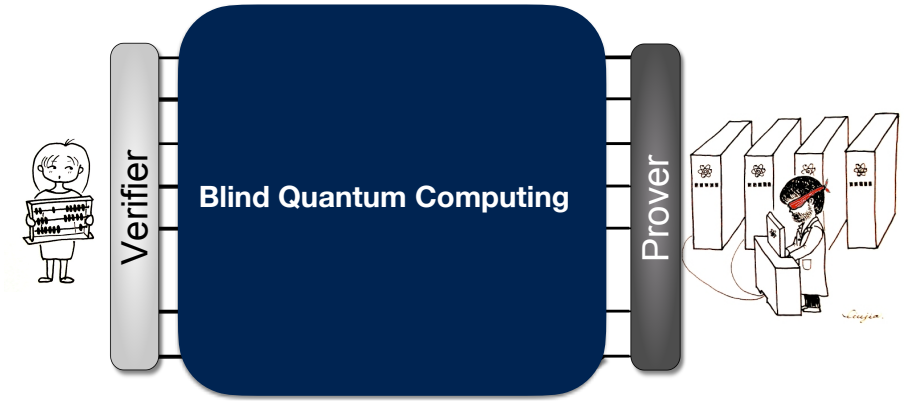
Accept Key

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

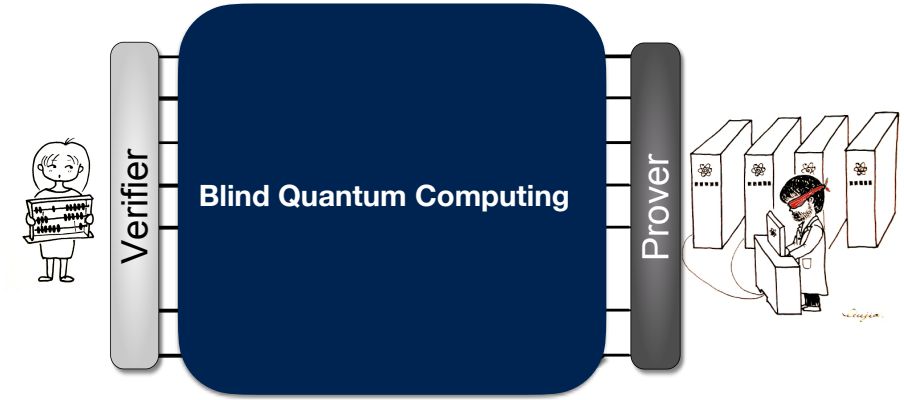
Test or Compute



Test or Compute



Test or Compute



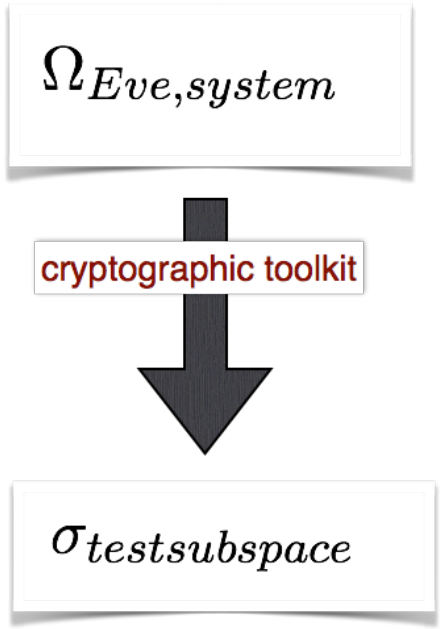
Computation round: Hard Task

Quantum Algorithm, Quantum Simulation, Quantum Sample …

Test round: Classically Simulatable Computation

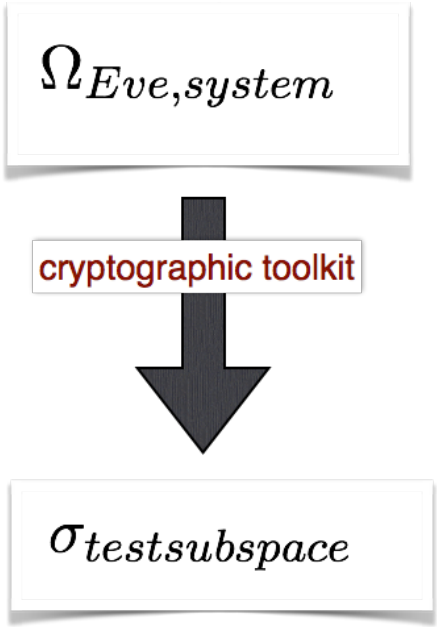
Clifford Circuit, Stabliser Code, Solvable Hamiltonian …

Reduction



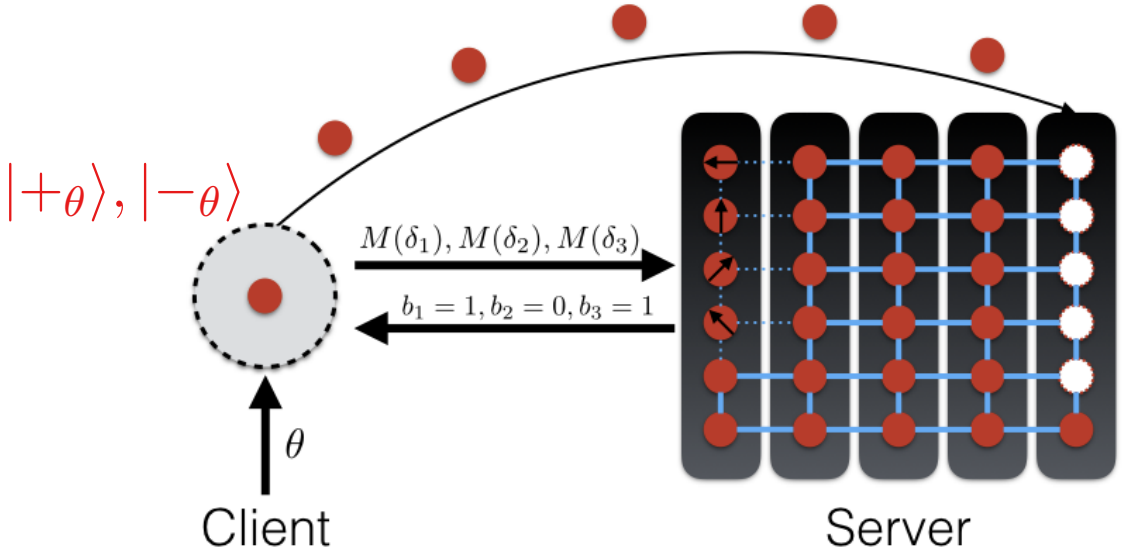
Practical Protocols with No assumptions whatsoever

Reduction



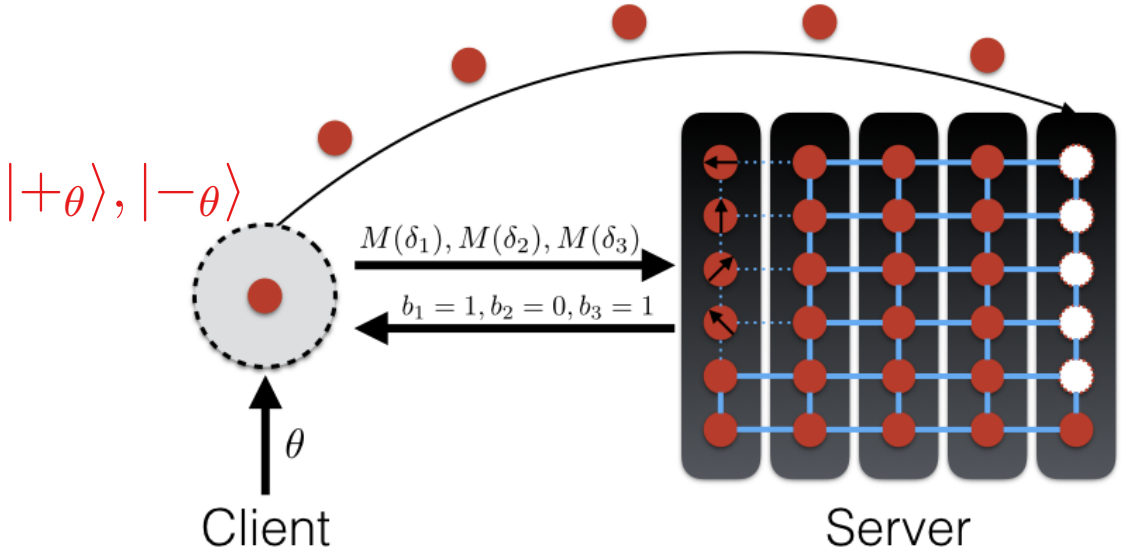
cryptography reduces the **verification** problem to **error-detection** procedure bypassing the complexity of simulation

Cryptography Toolkit



Broadbent, Fitzsimons and Kashefi, FOCS09

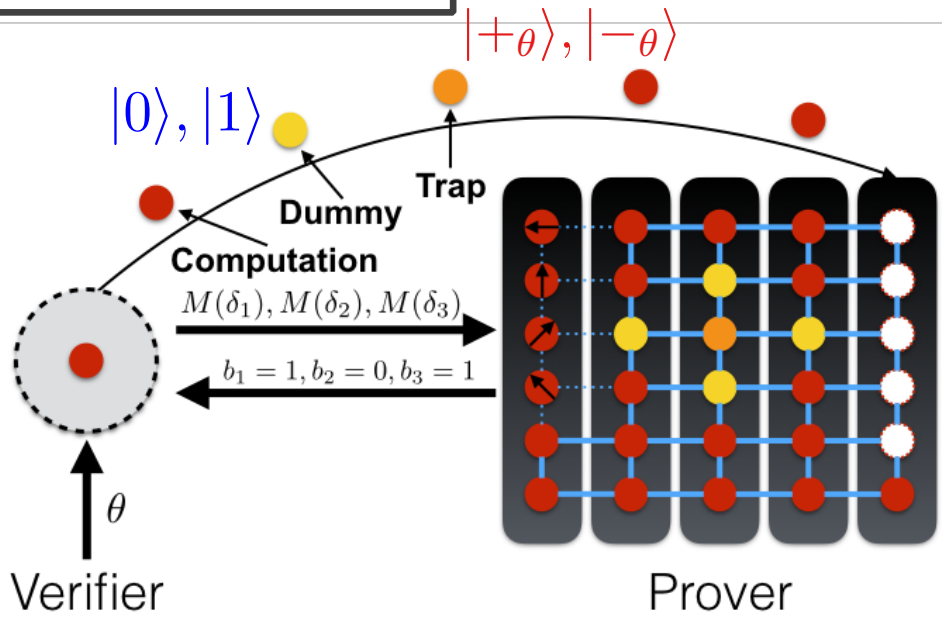
Cryptography Toolkit



Universal Blind Quantum Computing: QKD + Teleportation

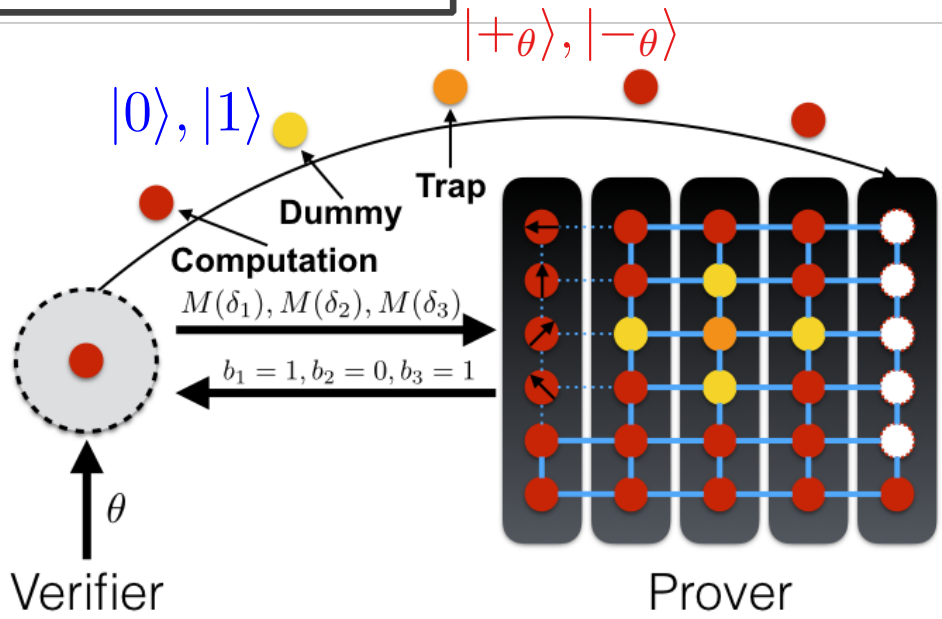
Broadbent, Fitzsimons and Kashefi, FOCS09

Prepare and Send Verification



Fitzsimons and Kashefi, 2012

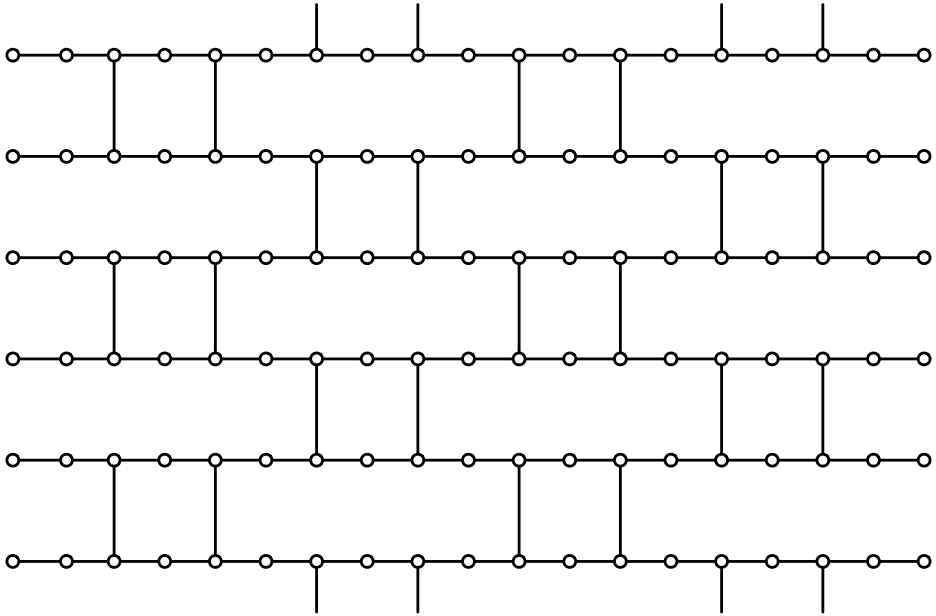
Prepare and Send Verification



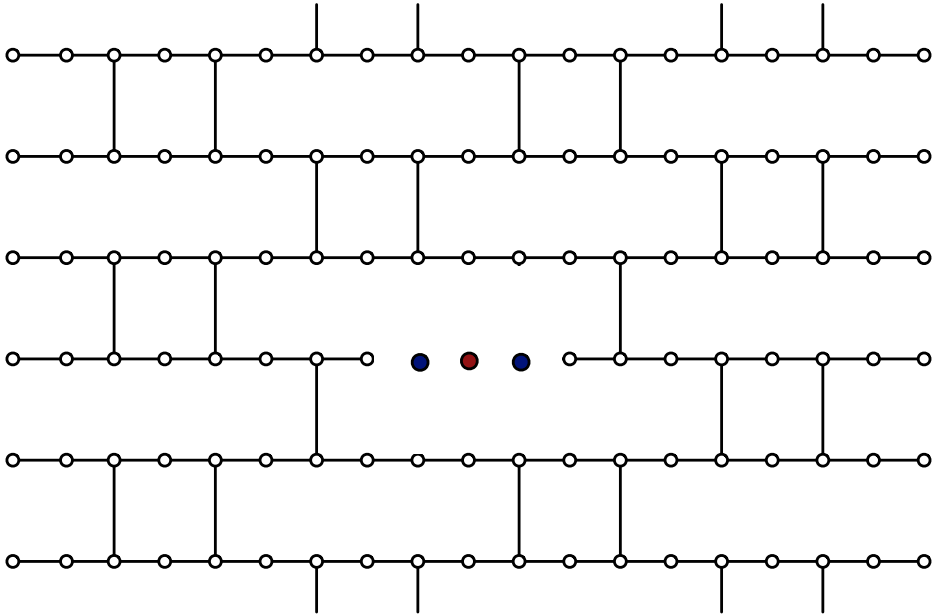
Verifiable Universal Blind Quantum Computing: QKD + Teleportation + Test

Fitzsimons and Kashefi, 2012

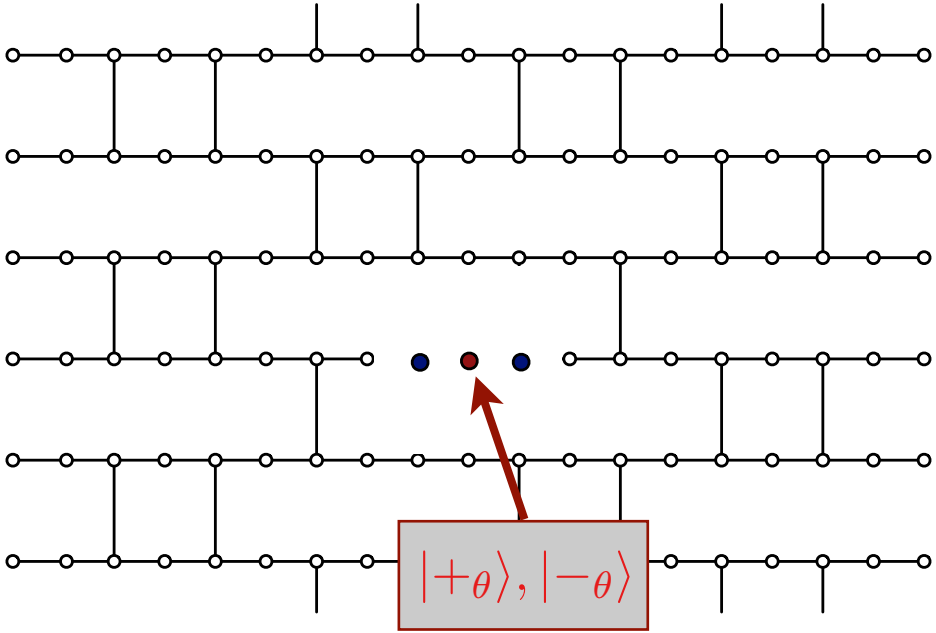
Prepare and Send Verification



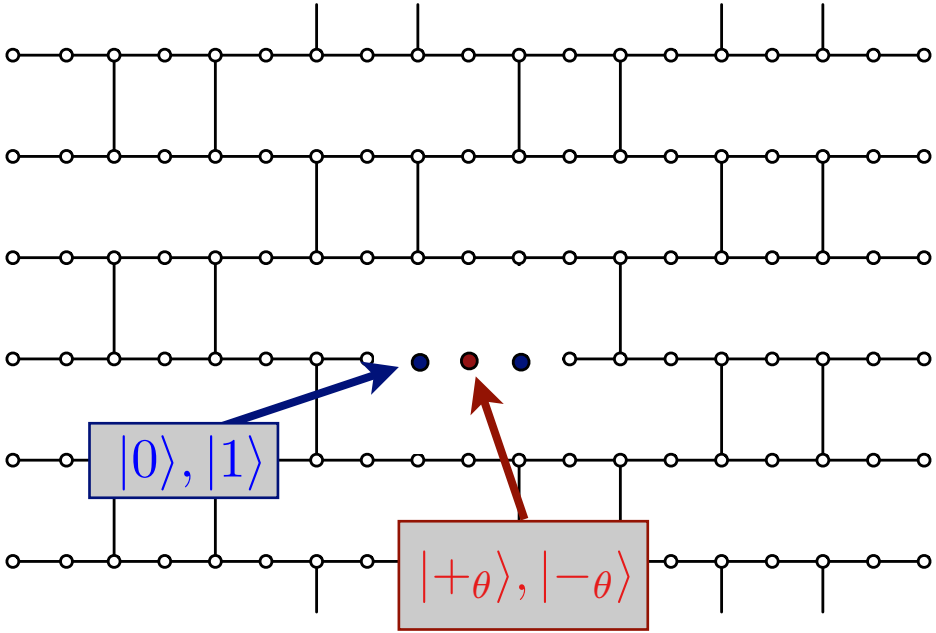
Prepare and Send Verification



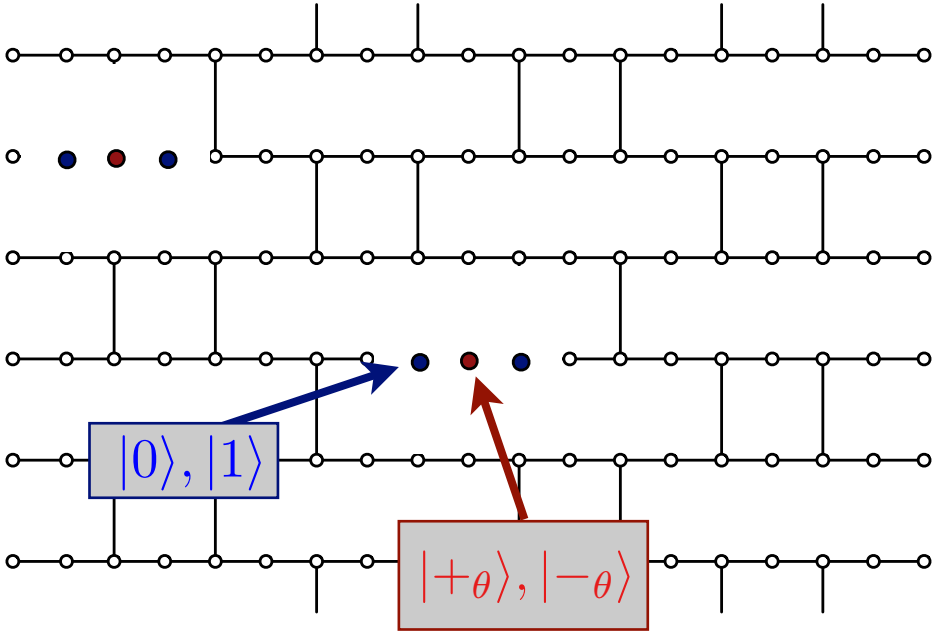
Prepare and Send Verification



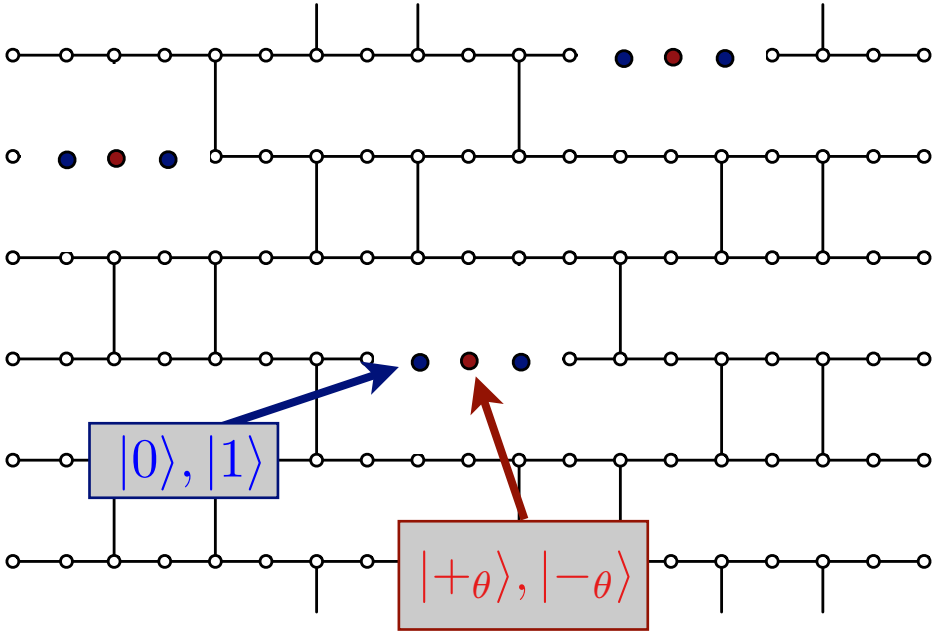
Prepare and Send Verification



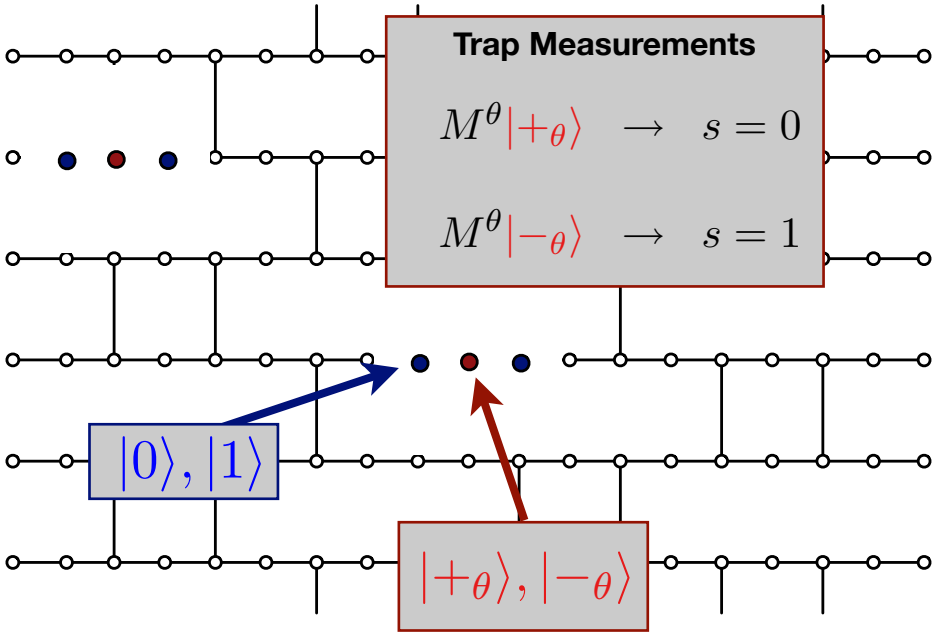
Prepare and Send Verification



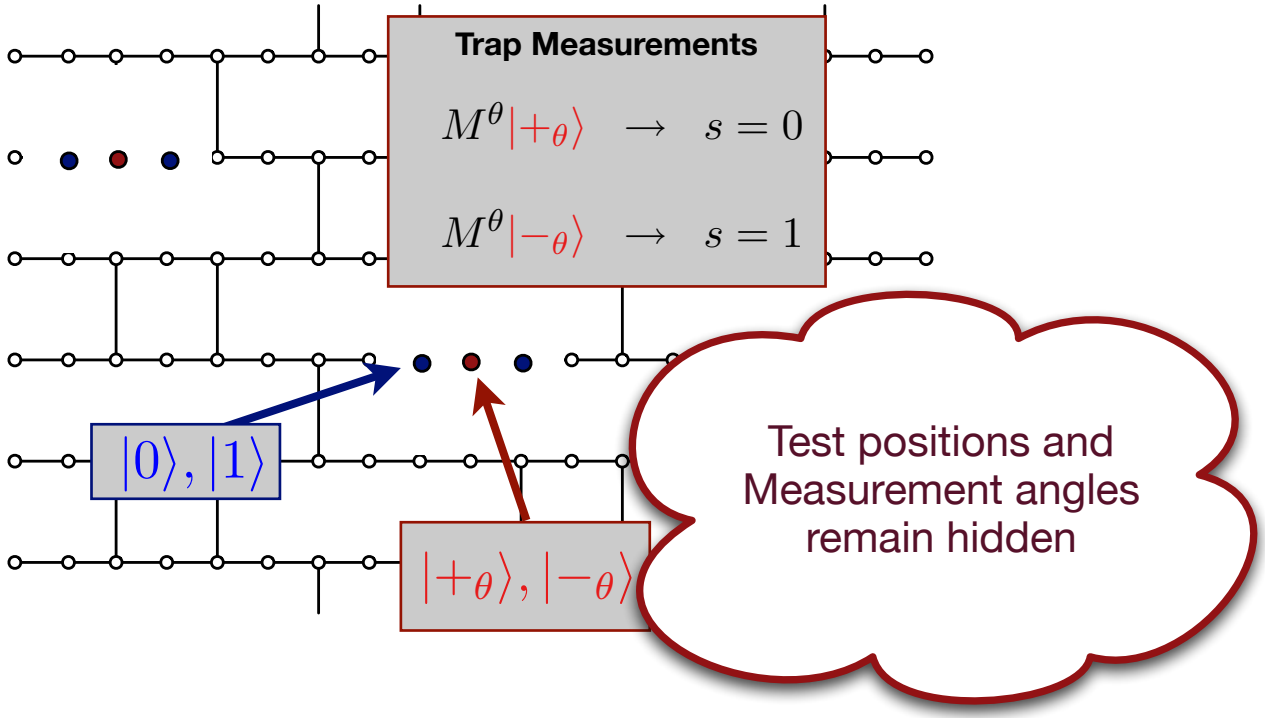
Prepare and Send Verification



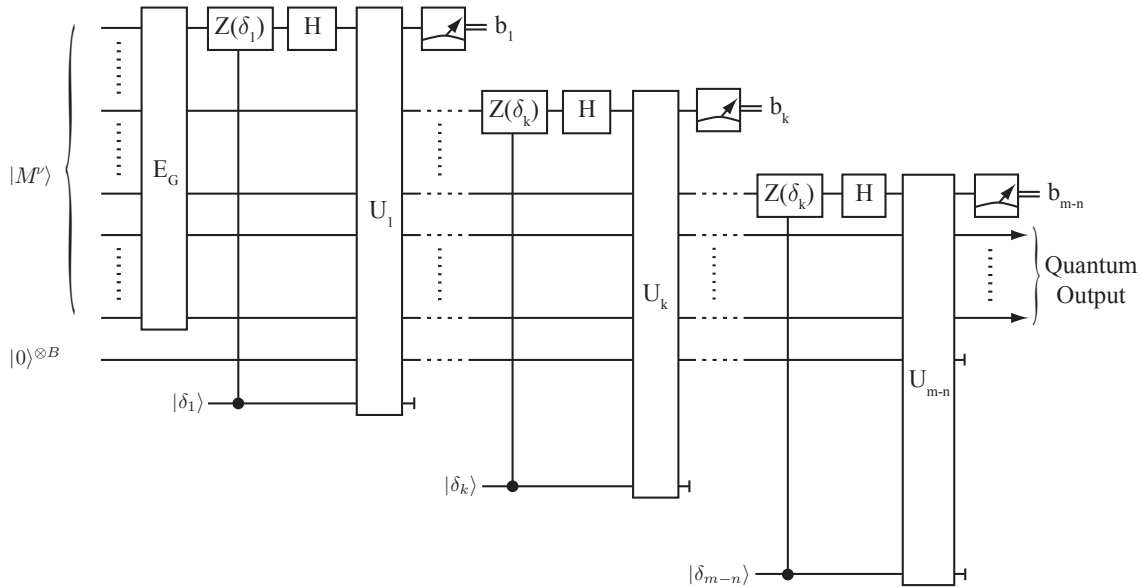
Prepare and Send Verification



Prepare and Send Verification

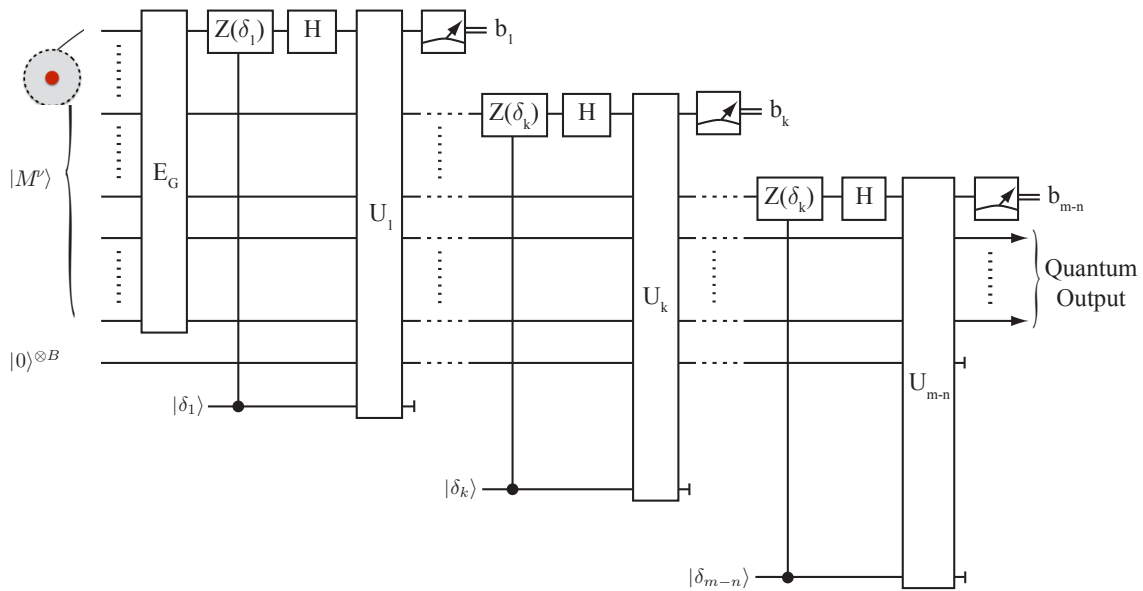


Soundness Proof



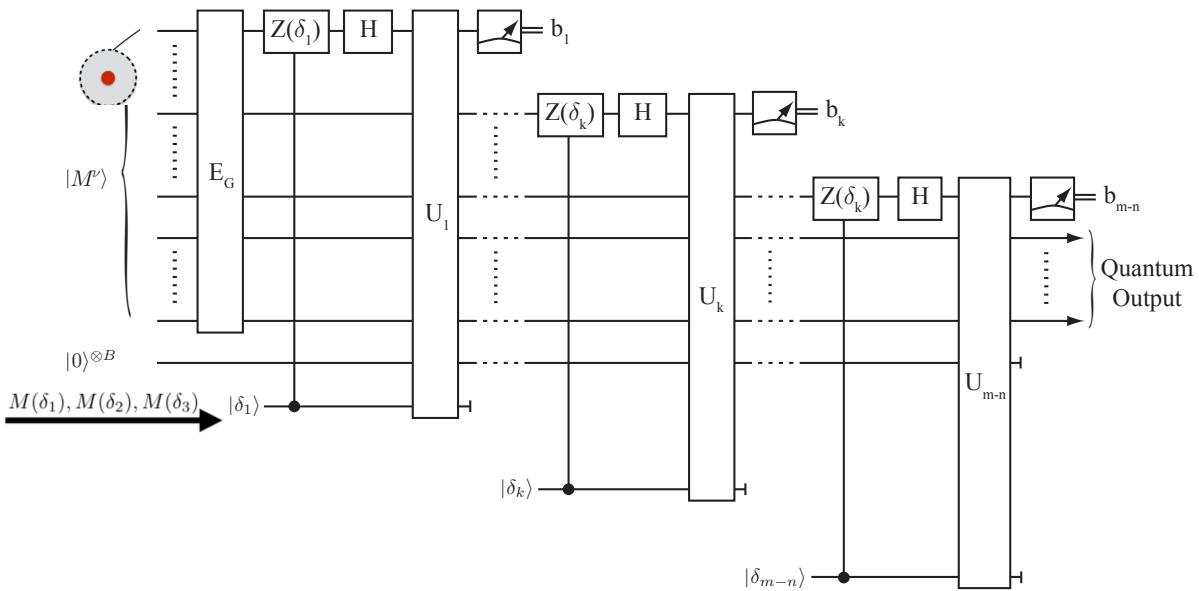
$$B_j(\nu) = \mathrm{Tr}_B \left(\sum_b |b + c_r\rangle \langle b| \, C_{\nu_C,b} \Omega \mathcal{P}((\otimes^B |0\rangle \langle 0|) \otimes \left|\Psi^{\nu,b}\right\rangle \left\langle \Psi^{\nu,b}\right|) \mathcal{P}^\dagger \Omega^\dagger C^\dagger_{\nu_C,b} |b\rangle \langle b + c_r| \right)$$

Soundness Proof



$$B_j(\nu) = \mathrm{Tr}_B \left(\sum_b |b + c_r\rangle \langle b| \, C_{\nu_C,b} \Omega \mathcal{P}((\otimes^B |0\rangle \langle 0|) \otimes \left|\Psi^{\nu,b}\right\rangle \left\langle \Psi^{\nu,b}\right|) \mathcal{P}^\dagger \Omega^\dagger C^\dagger_{\nu_C,b} |b\rangle \langle b + c_r| \right)$$

Soundness Proof



$$B_j(\nu) = \mathrm{Tr}_B \left(\sum_b |b + c_r\rangle \langle b| \, C_{\nu_C,b} \Omega \mathcal{P}((\otimes^B |0\rangle \langle 0|) \otimes \left|\Psi^{\nu,b}\right\rangle \left\langle \Psi^{\nu,b}\right|) \mathcal{P}^\dagger \Omega^\dagger C^\dagger_{\nu_C,b} |b\rangle \langle b + c_r| \right)$$

Soundness Proof

$$p_{incorrect} = \sum_{\nu} p(\nu) \mathrm{Tr}(P_{\perp} \otimes |\eta_t^{\nu}\rangle \langle \eta_t^{\nu}| \ (\Omega \mathcal{P}((\otimes^B |0\rangle \langle 0|) \otimes |\Psi^{\nu}\rangle \langle \Psi^{\nu}|) \mathcal{P}^{\dagger} \Omega^{\dagger})) .$$

Soundness Proof

$$p_{incorrect} = \sum_{\nu} p(\nu) \mathrm{Tr}(P_{\perp} \otimes |\eta_t^{\nu}\rangle \langle \eta_t^{\nu}| (\Omega \mathcal{P}((\otimes^B |0\rangle \langle 0|) \otimes |\Psi^{\nu}\rangle \langle \Psi^{\nu}|) \mathcal{P}^{\dagger} \Omega^{\dagger}))$$

$\vdots$

Blindness

Soundness Proof

$$p_{incorrect} = \sum_{\nu} p(\nu) \mathrm{Tr}(P_{\perp} \otimes |\eta_t^{\nu}\rangle \langle \eta_t^{\nu}| (\Omega \mathcal{P}((\otimes^B |0\rangle \langle 0|) \otimes |\Psi^{\nu}\rangle \langle \Psi^{\nu}|) \mathcal{P}^{\dagger} \Omega^{\dagger}))$$

$$\vdots$$

Blindness

$$p_{\text{incorrect}} \leq \sum_{k,\nu_T} \sum_{i \in E_i} \alpha_{ik} \alpha_{ik}^* p(\nu_T) \mathrm{Tr}\left(\langle \eta_t^{\nu_T}| \sigma_i \left(|\eta_t^{\nu_T}\rangle \langle \eta_t^{\nu_T}| \otimes |\delta_t\rangle \langle \delta_t| \otimes \frac{I}{\mathrm{Tr}(I)} \right) \sigma_i |\eta_t^{\nu_T}\rangle \right)$$

Soundness Proof

$$p_{incorrect} = \sum_{\nu} p(\nu)' \mathrm{Tr}(P_{\perp} \otimes |\eta_t^{\nu}\rangle \langle \eta_t^{\nu}| (\Omega \mathcal{P}((\otimes^B |0\rangle \langle 0|) \otimes |\Psi^{\nu}\rangle \langle \Psi^{\nu}|)\mathcal{P}^{\dagger}\Omega^{\dagger})) .$$

$$\vdots$$

Blindness

$$p_{\text{incorrect}} \leq \sum_{k,\nu_T} \sum_{i \in E_i} \alpha_{ik} \alpha_{ik}^* p(\nu_T) \mathrm{Tr}\left(\langle \eta_t^{\nu_T}| \sigma_i \left(|\eta_t^{\nu_T}\rangle \langle \eta_t^{\nu_T}| \otimes |\delta_t\rangle \langle \delta_t| \otimes \frac{I}{\mathrm{Tr}(I)} \right) \sigma_i |\eta_t^{\nu_T}\rangle \right)$$

Soundness Proof

$$p_{incorrect} = \sum_{\nu} p(\nu)\mathrm{Tr}(P_{\perp} \otimes |\eta_t^{\nu}\rangle\langle\eta_t^{\nu}| (\Omega\mathcal{P}((\otimes^B |0\rangle\langle 0|) \otimes |\Psi^{\nu}\rangle\langle\Psi^{\nu}|)\mathcal{P}^{\dagger}\Omega^{\dagger})) .$$

$$\vdots$$

Blindness

$$p_{\text{incorrect}} \leq \sum_{k,\nu_T} \sum_{i \in E_i} \alpha_{ik}\alpha_{ik}^* p(\nu_T)\mathrm{Tr}\left(\langle\eta_t^{\nu_T}| \sigma_i \left(|\eta_t^{\nu_T}\rangle\langle\eta_t^{\nu_T}| \otimes |\delta_t\rangle\langle\delta_t| \otimes \frac{I}{\mathrm{Tr}(I)} \right) \sigma_i |\eta_t^{\nu_T}\rangle \right)$$

$$\vdots$$

$$= \frac{1}{16m} \sum_{k} \sum_{i \in E_i} |\alpha_{ki}|^2 \sum_{t,r_t,\theta_t} \left(\langle\eta_t^{\nu_T}| \sigma_{i|t} |\eta_t^{\nu_T}\rangle \right)^2$$

Soundness Proof

$$p_{incorrect} = \sum_{\nu} p(\nu) \mathrm{Tr}(P_{\perp} \otimes |\eta_t^{\nu}\rangle \langle \eta_t^{\nu}| (\Omega \mathcal{P}((\otimes^B |0\rangle \langle 0|) \otimes |\Psi^{\nu}\rangle \langle \Psi^{\nu}|) \mathcal{P}^{\dagger} \Omega^{\dagger})) .$$

$$\vdots$$

Blindness

$$p_{\text{incorrect}} \leq \sum_{k,\nu_T} \sum_{i \in E_i} \alpha_{ik} \alpha_{ik}^* p(\nu_T) \mathrm{Tr} \left(\langle \eta_t^{\nu_T} | \sigma_i \left(|\eta_t^{\nu_T}\rangle \langle \eta_t^{\nu_T}| \otimes |\delta_t\rangle \langle \delta_t| \otimes \frac{I}{\mathrm{Tr}(I)} \right) \sigma_i |\eta_t^{\nu_T}\rangle \right)$$

$$\vdots$$

$$= \frac{1}{16m} \sum_{k} \sum_{i \in E_i} |\alpha_{ki}|^2 \sum_{t, r_t, \theta_t} \left(\langle \eta_t^{\nu_T} | \sigma_{i|t} |\eta_t^{\nu_T}\rangle \right)^2$$

$$\vdots$$

$$\leq 1 - \frac{1}{2m}$$

Soundness Proof

$$p_{incorrect} = \sum_{\nu} p(\nu) \mathrm{Tr}(P_{\perp} \otimes |\eta_t^{\nu}\rangle \langle \eta_t^{\nu}| \, (\Omega \mathcal{P}((\otimes^B |0\rangle \langle 0|) \otimes |\Psi^{\nu}\rangle \langle \Psi^{\nu}|) \mathcal{P}^{\dagger} \Omega^{\dagger}))$$

$$\vdots$$

Blindness

$$p_{\text{incorrect}} \leq \sum_{k,\nu_T} \sum_{i \in E_i} \alpha_{ik} \alpha_{ik}^* p(\nu_T) \mathrm{Tr}\left(\langle \eta_t^{\nu_T}| \sigma_i \left(|\eta_t^{\nu_T}\rangle \langle \eta_t^{\nu_T}| \otimes |\delta_t\rangle \langle \delta_t| \otimes \frac{I}{\mathrm{Tr}(I)} \right) \sigma_i |\eta_t^{\nu_T}\rangle \right)$$

(Pauli Twirl) Let P, P' be n-qubit Pauli operators. Then:

$$\frac{1}{|\mathbb{P}_n|} \sum_{Q \in \mathbb{P}_n} Q^* P Q \rho Q^* P'^* Q = \begin{cases} 0, & P \neq P' \\ P \rho P^*, & \text{otherwise}. \end{cases}$$

$$\vdots$$

$$\leq 1 - \frac{1}{2m}$$

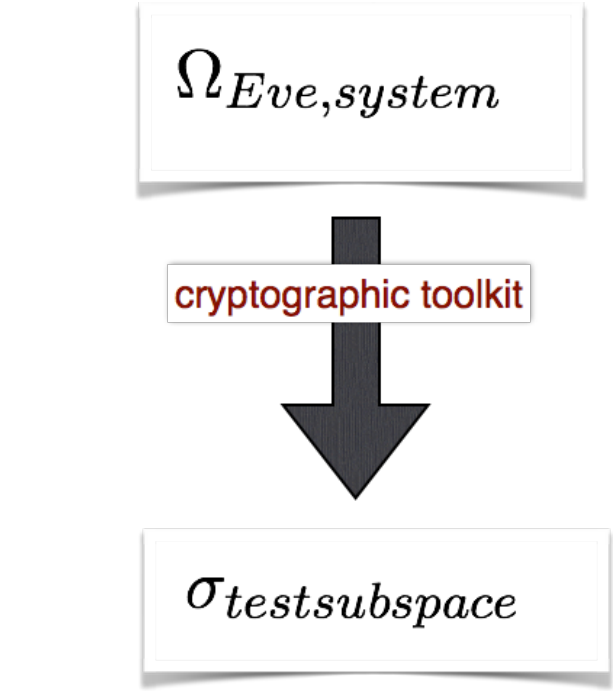
Summary

$\Omega_{Eve,system}$

$\sigma_{testsubspace}$

Practical Protocols with No assumptions whatsoever

Is it really practical ?



Practical Protocols with No assumptions whatsoever

Is it really practical ?

Practical for Verifier

Nightmare for Server

- Oversensitive
- Huge overhead

$\Omega_{Eve,system}$

cryptographic toolkit

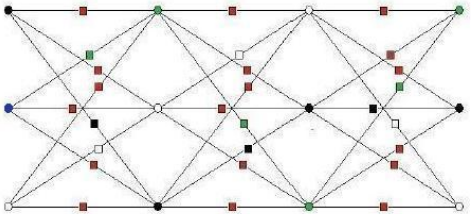
$\sigma_{testsubspace}$

Practical Protocols with No assumptions whatsoever

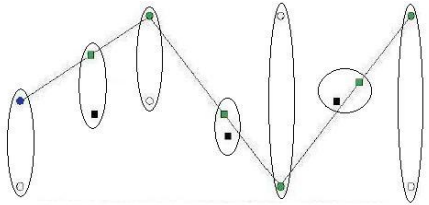
Is it really practical ?

Linear Server overhead

Kashefi, Walden, 2014



(a) Trap-colouring



The challenge of fault tolerant verification

Aharonov, Ben-Or, Eban, Mahadev, 2015

Is it really practical ?

Is it really practical ?

Linear Server overhead

Is it really practical ?

Linear Server overhead

Inverse-polynomial security

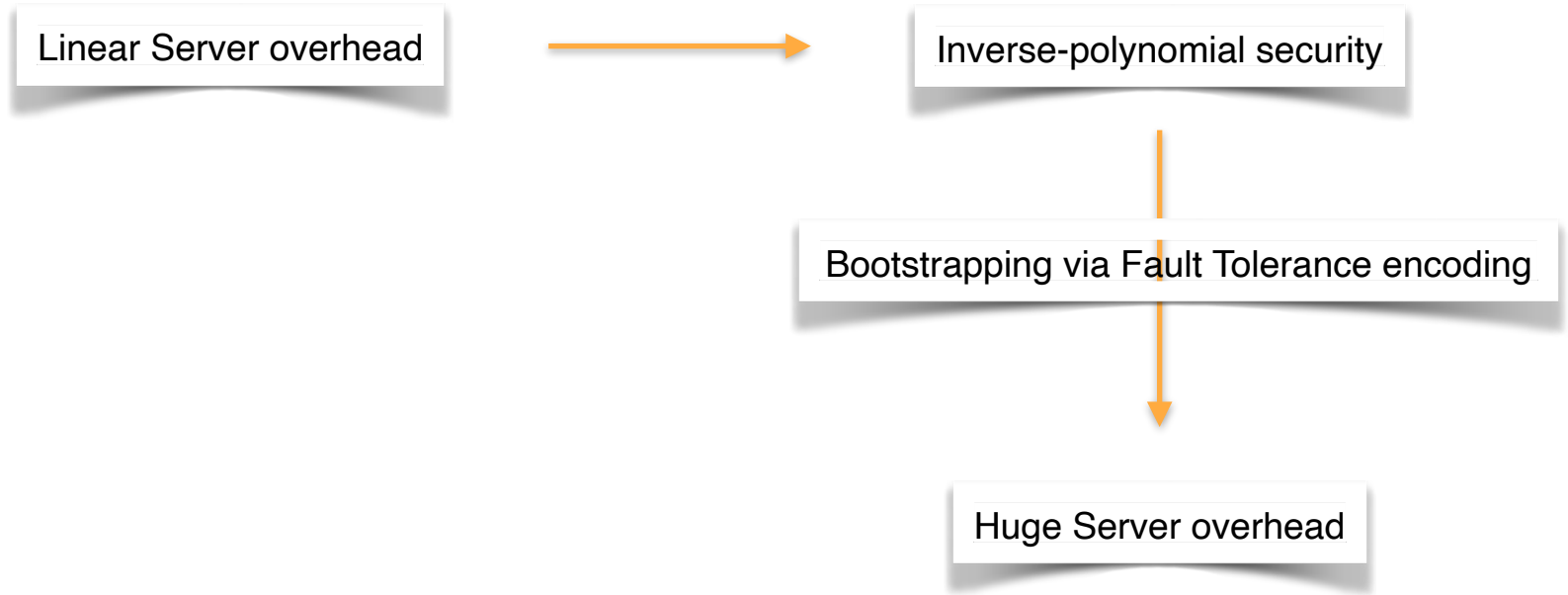
Is it really practical ?

Linear Server overhead

Inverse-polynomial security

Bootstrapping via Fault Tolerance encoding

Is it really practical ?



Is it really practical ?

Linear Server overhead

Inverse-polynomial security

Bootstrapping via Fault Tolerance encoding

Huge Server overhead

Prepare-and-send

Receive and Measure

Entangled Server

Post-Quantum Secure

New Result

Leichtle, Music, Kashefi, Ollivier, PRX, 2021

BQP: Classical Input/Output

New Result

Leichtle, Music, Kashefi, Ollivier, PRX, 2021

BQP: Classical Input/Output

No Server overhead

New Result

BQP: Classical Input/Output

Leichtle, Music, Kashefi, Ollivier, PRX, 2021

No Server overhead

Inverse-polynomial security

New Result

BQP: Classical Input/Output

Leichtle, Music, Kashefi, Ollivier, PRX, 2021

No Server overhead

Inverse-polynomial security

Classical Repetition Code

New Result

Leichtle, Music, Kashefi, Ollivier, PRX, 2021

BQP: Classical Input/Output

No Server overhead

Inverse-polynomial security

Classical Repetition Code

Exponential Correctness on honest but noisy device
Exponential Verification for Arbitrary Deviations

New Result

Leichtle, Music, Kashefi, Ollivier, PRX, 2021

BQP: Classical Input/Output

No Server overhead

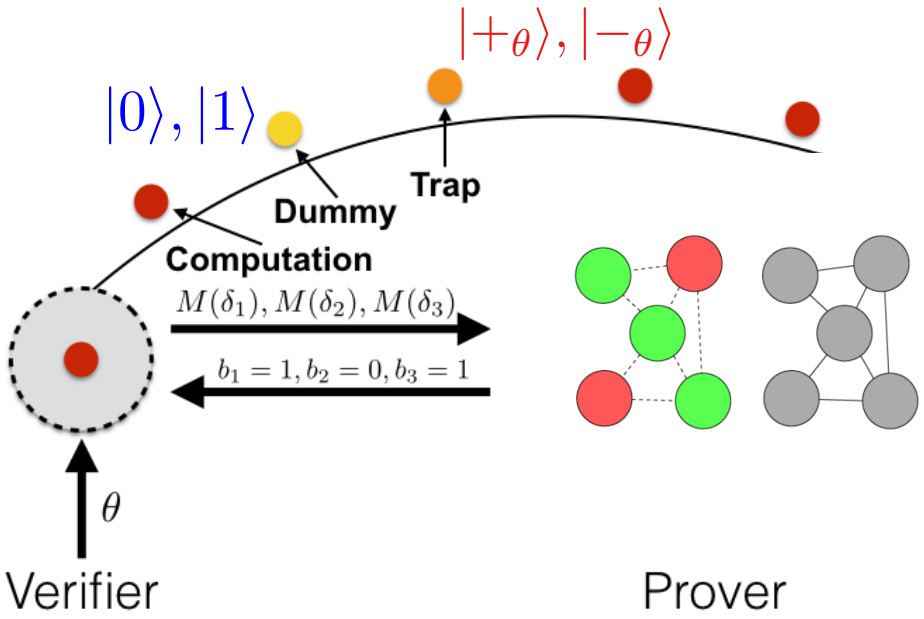
Inverse-polynomial security

Classical Repetition Code

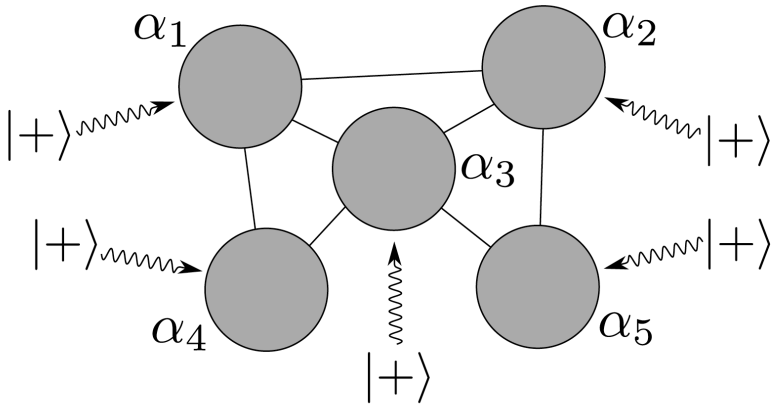
Server Efficiency

Exponential Correctness on honest but noisy device
Exponential Verification for Arbitrary Deviations

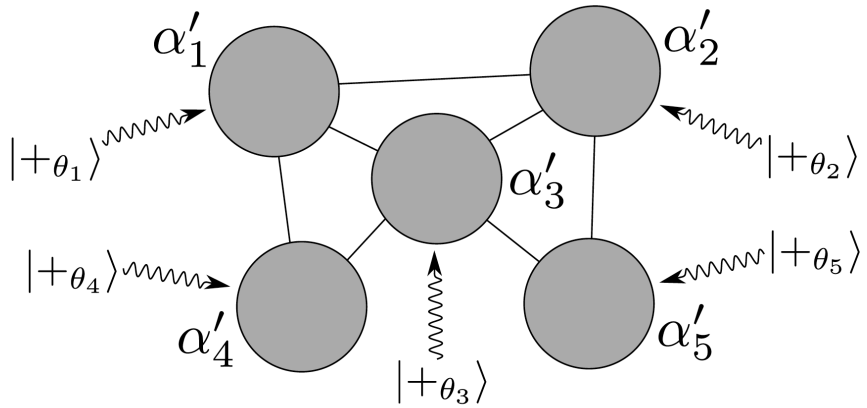
Prepare and Send Verification



Target computation

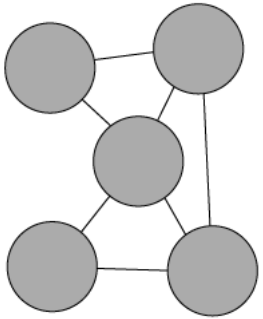


Blind Target computation

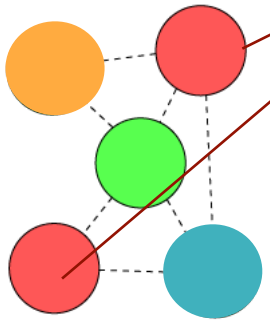


Insertion of Trap

Target Computation



Test Computation
k-colouring

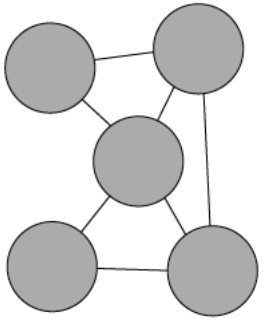


Trap $|+_\theta\rangle, |-_\theta\rangle$

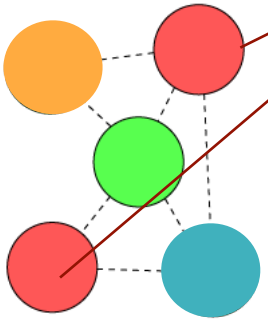
Dummy $|0\rangle, |1\rangle$

Insertion of Trap

Target Computation



Test Computation
k-colouring



Trap $|+_\theta\rangle, |-_\theta\rangle$

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

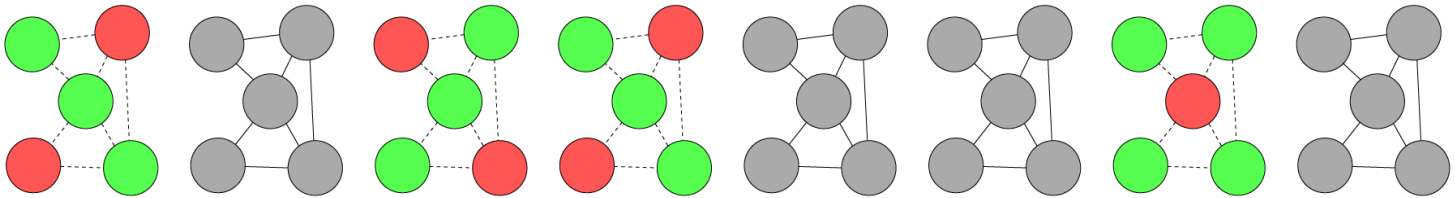
Trap Measurements

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

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

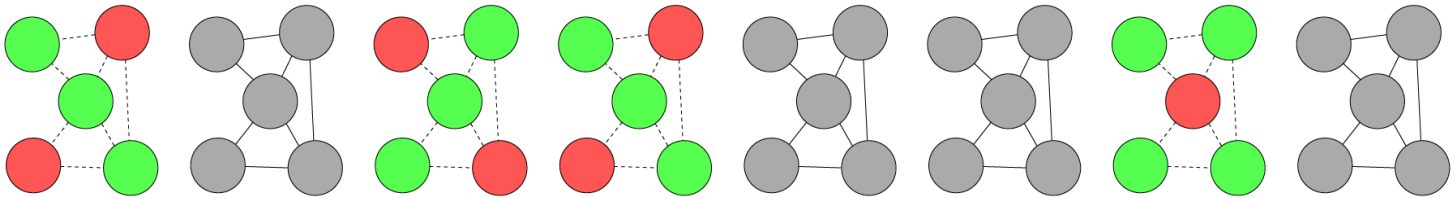
Test and Compute

$$n := t + d$$



Test and Compute

$$n := t + d$$



Verifier counts the number of failed test rounds If > threshold *w*, aborts

Otherwise accepts the majority outcome of the computation rounds as output

Protocol Features

Protocol Features

Redo Option

Verifier or Server may experience unintentional devices failures

Protocol Features

Redo Option

Verifier or Server may experience unintentional devices failures

Exponential Security Amplification

quantum attacks entangled across rounds are much more powerful than what classical correlations allow

Protocol Features

Redo Option

Verifier or Server may experience unintentional devices failures

Exponential Security Amplification

quantum attacks entangled across rounds are much more powerful than what classical correlations allow

Fine-Tuning the Number of Repetitions

Small *k*-colouring of the graph

Protocol Features

Redo Option

Verifier or Server may experience unintentional devices failures

Exponential Security Amplification

quantum attacks entangled across rounds are much more powerful than what classical correlations allow

Fine-Tuning the Number of Repetitions

Small *k*-colouring of the graph

Composable Security

Abstract Cryptography

Security Proof

Theorem 1 (Security of Protocol 1). *For $n = d + t$ such that d/n and t/n are fixed in $(0, 1)$ and w such that w/t is fixed in $(0, \frac{1}{k} \cdot \frac{2p-1}{2p-2})$, where p is the inherent error probability of the BQP computation, Protocol 1 with d computation rounds, t test rounds, and a maximum number of tolerated failed test rounds of w is ϵ-composably-secure with ϵ exponentially small in n.*

Robustness

On honest (but possibly noisy) devices, the protocol accepts with high probability

Robustness

On honest (but possibly noisy) devices, the protocol accepts with high probability

- The noise can be modelled by round-dependent Markovian processes – i.e. a possibly different arbitrary CPTP map acting on each round.
- The probability that at least one of the trap measurements fails in any single test round is upper-bounded by some constant $p_{max} < \frac{1}{k} \cdot \frac{2p-1}{2p-2}$ and lower-bounded by $p_{min} \leq p_{max}$.

Summary

Decoupling Verifiability and Fault-Tolerance

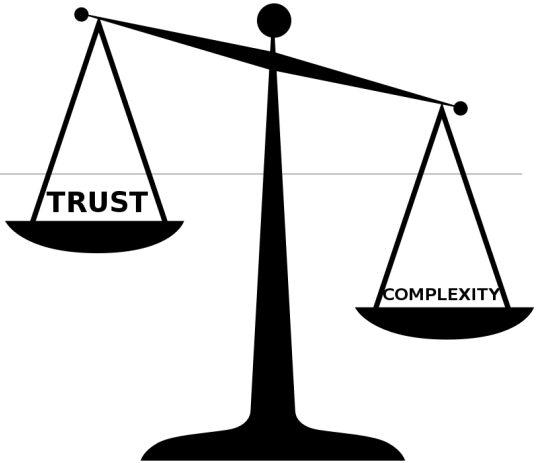
Summary

Decoupling Verifiability and Fault-Tolerance

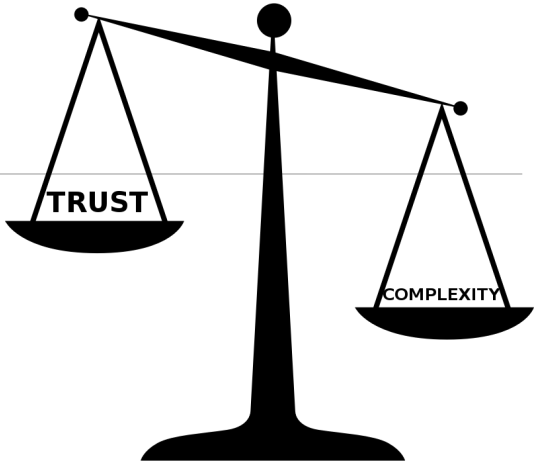
all qubits can be devoted to useful computations irrespective of the desired security

the average ratio of failed test rounds to be upper-bounded

Price of Verification



Price of Verification



- Prepare and send vs. entanglement-based
- Single vs. multiple servers
- Online vs. offine
- Device-independent vs. one-sided device-independent
- I.I.D. states vs. general states
- Privacy preserving vs non-hiding
- Universal vs non-universal
- And many others

Certification and Benchmarking tool

Eisert, Hangleiter, Walk, Roth, Markham, Parekh, Chabaud, Kashefi

Enforcing the ***correct functioning*** of a quantum device, using the minimum amount of ***resources***, while making as few ***assumptions*** as possible.

Certification and Benchmarking tool

Eisert, Hangleiter, Walk, Roth, Markham, Parekh, Chabaud, Kashefi

Figures of merit

Enforcing the ***correct functioning*** of a quantum device, using the minimum amount of ***resources***, while making as few ***assumptions*** as possible.

Certification and Benchmarking tool

Eisert, Hangleiter, Walk, Roth, Markham, Parekh, Chabaud, Kashefi

Figures of merit

Enforcing the ***correct functioning*** of a quantum device, using the minimum amount of ***resources***, while making as few ***assumptions*** as possible.

User/Device tunability resources

Certification and Benchmarking tool

Eisert, Hangleiter, Walk, Roth, Markham, Parekh, Chabaud, Kashefi

Figures of merit

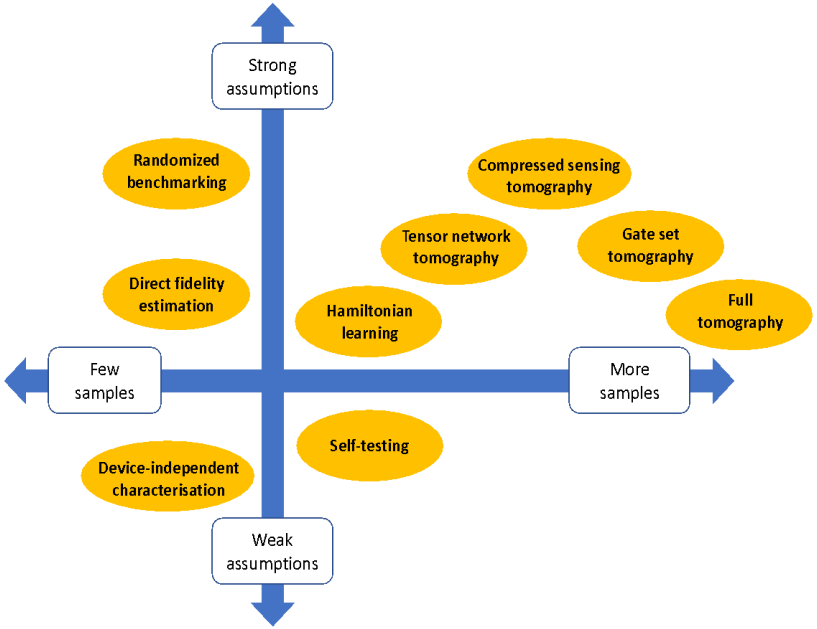
Enforcing the ***correct functioning*** of a quantum device, using the minimum amount of ***resources***, while making as few ***assumptions*** as possible.

User/Device tunability resources

Noise Model

Certification and Benchmarking tool

Eisert, Hangleiter, Walk, Roth, Markham, Parekh, Chabaud, Kashefi



Figures of merit

Enforcing the ***correct functioning*** of a quantum device, using the minimum amount of ***resources***, while making as few ***assumptions*** as possible.

User/Device tunability resources

Noise Model

Verification as a Benchmarking Tool

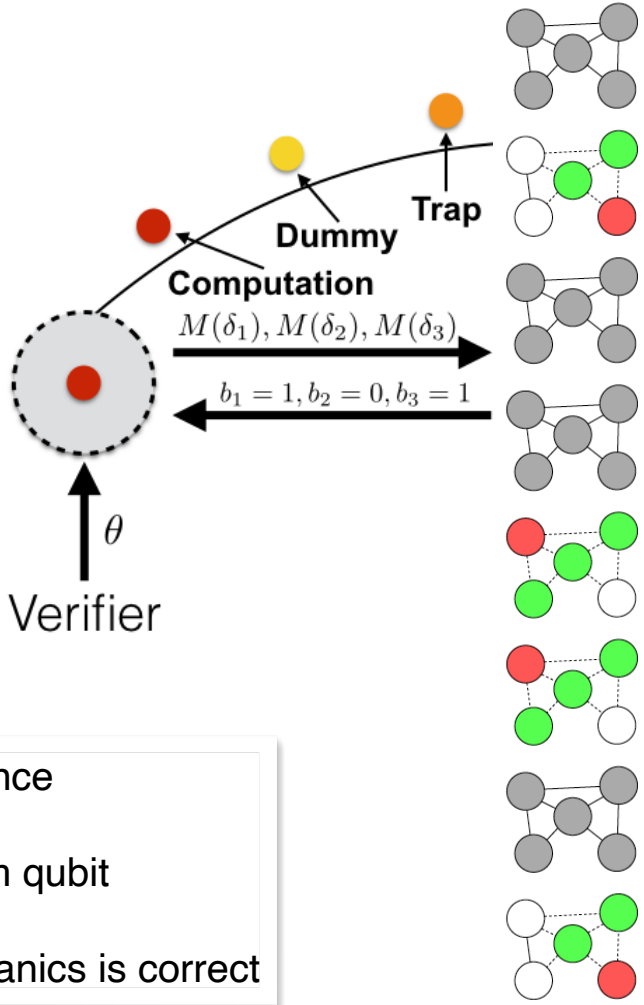


Figure of merit: trace-distance

User resources: single random qubit

Weakest assumptions: quantum mechanics is correct

Verification as a Benchmarking Tool

Noise independent of θ

VS

I.I.D
Testing only Clifford
…

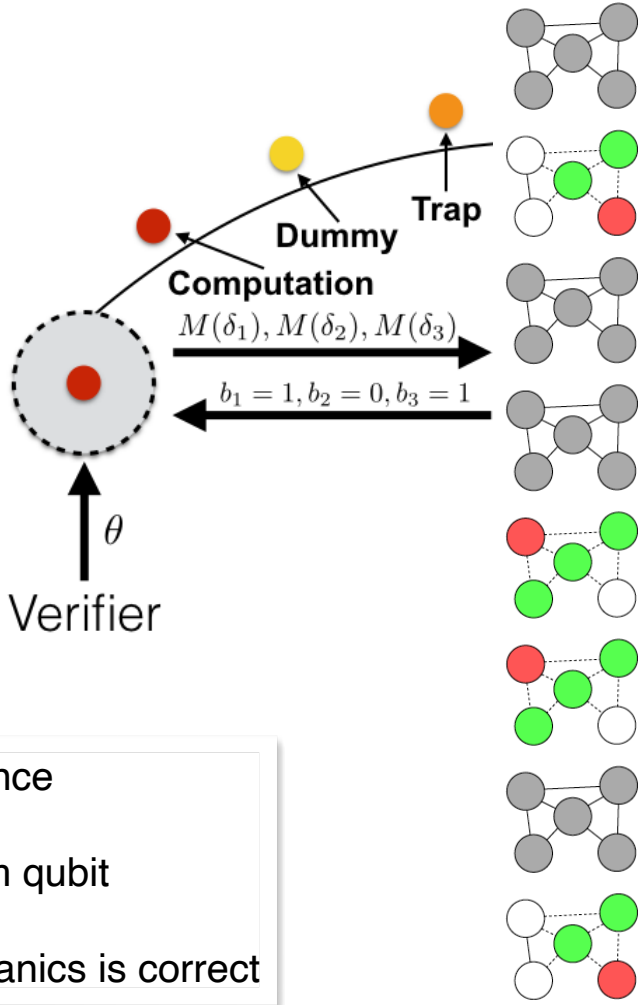


Figure of merit: trace-distance

User resources: single random qubit

Weakest assumptions: quantum mechanics is correct

Ongoing Project for Practical Implementation

Ongoing Project for Practical Implementation

Ongoing Project for Practical Implementation

QUANTUM INTERNET ALLIANCE

Ongoing Project for Practical Implementation

PASQAL

QUANTUM INTERNET ALLIANCE

Ongoing Project for Practical Implementation

PASQAL

QUANTUM INTERNET ALLIANCE

UKRI National Quantum Computing Centre

Quantum Computing & Simulation Hub