Title: How to Verify a Quantum Computation

Date: Mar 30, 2016 04:00 PM

URL: http://pirsa.org/16030128

Abstract: <p>We give a new theoretical solution to a leading-edge experimental challenge, namely to the verification of quantum computations in the regime of high computational complexity. Our results are given in the language of quantum interactive proof systems. Specifically, we show that any language in BQP has a quantum interactive proof system with a polynomial-time classical verifier (who can also prepare random single-qubit pure states), and a quantum polynomial-time prover. Here, soundness is unconditional---i.e it holds even for computationally unbounded provers. Compared to prior work achieving similar results, our technique does not require the encoding of the input or of the computation; instead, we rely on encryption of the input (together with a method to perform computations on encrypted inputs), and show that the random choice between three types of input (defining a "computational run", versus two types of "test runs") suffice. As a proof technique, we use a reduction to an entanglement-based protocol; this enables a relatively simple analysis for a situation that has previously remained ambiguous in the literature.</p>

How to Verify a Quantum Computation

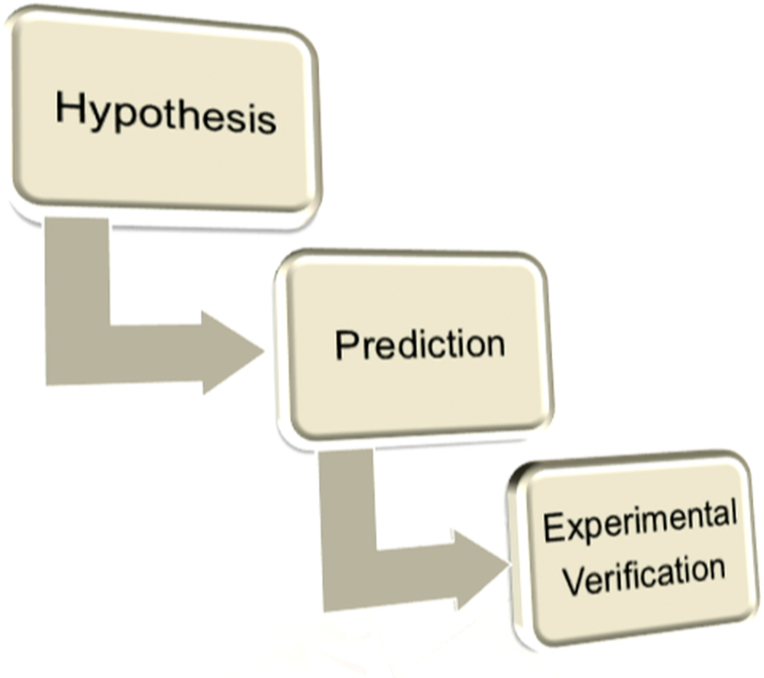
Anne Broadbent
Department of Mathematics and Statistics
University of Ottawa

PIQuDos seminar
March 30 2016

Scientific method

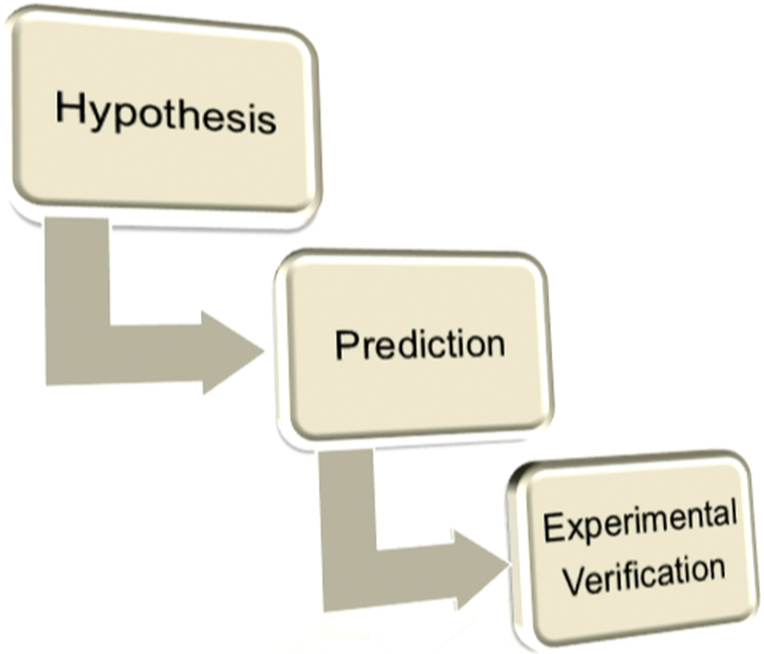
uOttawa

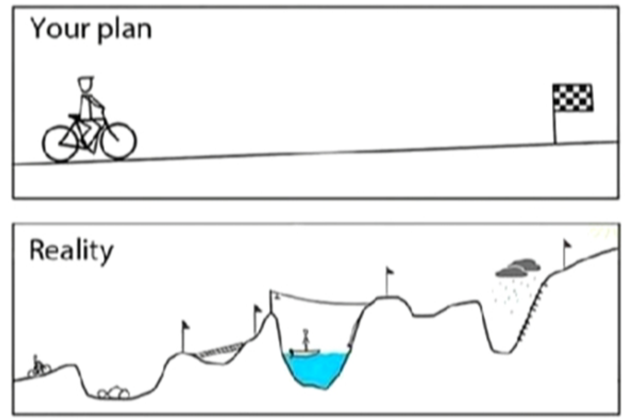
Scientific method



uOttawa

Scientific method





uOttawa

Testing a theory at various limits

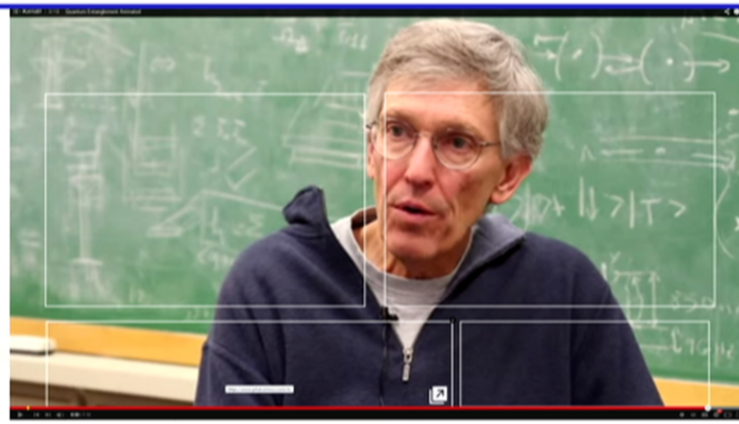
- high energy
- Planck scale,
- close to the speed of light
- ...

uOttawa

Testing a theory in various limits

- high energy
- Planck scale,
- close to the speed of light
- …

"If you know what you are doing, don't do it!"



Jeff Kimble, William L. Valentine Professor of Physics, California Institute of Technology

uOttawa

Quantum Computing

a new "limit" to test:

Quantum computations in the limit of high computational complexity

[Aharonov, Vazirani 2012]

uOttawa

Quantum Computing

a new "limit" to test:

Quantum computations in the limit of high computational complexity

The predictions of quantum mechanics are exponentially difficult to compute

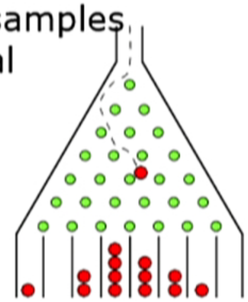
For large-scale experiments, need an alternative to "predict-and-verify"

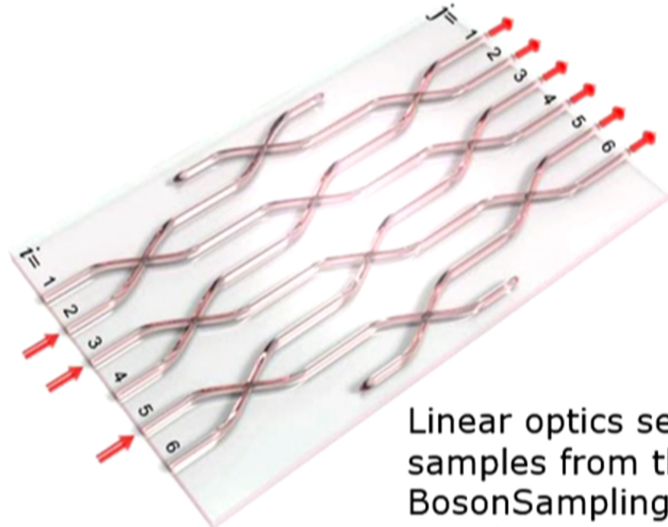
[Aharonov, Vazirani 2012]

uOttawa

Boson Sampling

Galton's board: samples from the Binomial distribution





Linear optics setup: samples from the BosonSampling distribution

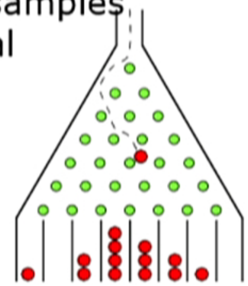
- Difficult to simulate classically

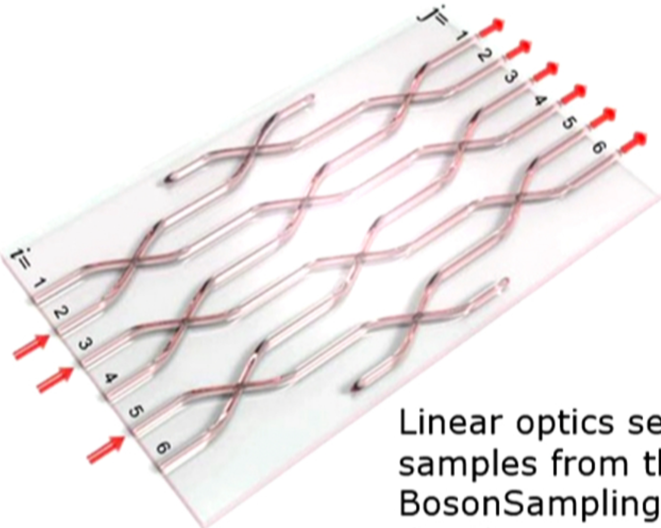
Recently, Groups in Brisbane, Oxford, Rome and Vienna reported the first 3- and 4-photon BosonSampling experiments

uOttawa

Boson Sampling

Galton's board: samples from the Binomial distribution





Linear optics setup: samples from the BosonSampling distribution

- Difficult to simulate classically

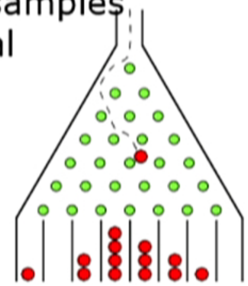
Recently, Groups in Brisbane, Oxford, Rome and Vienna reported the first 3- and 4-photon BosonSampling experiments

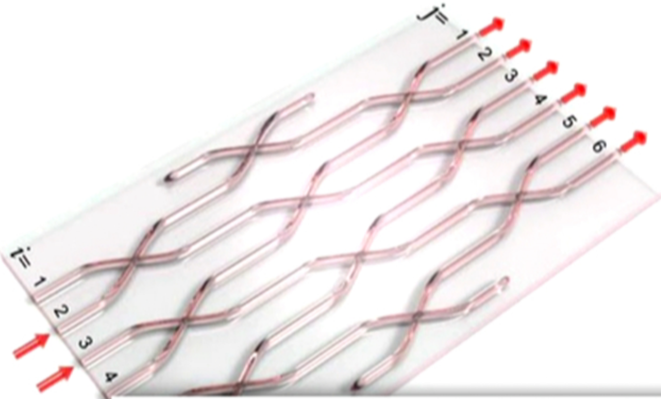
Big Question: How does one know that the outcome is correct? (in the regime that classical simulation is not possible)

uOttawa

Boson Sampling

Galton's board: samples from the Binomial distribution





Efficient experimental validation of photonic boson sampling against the uniform distribution

Nicolò Spagnolo,[1] Chiara Vitelli,[1,2] Marco Bentivegna,[1] Daniel J. Brod,[3] Andrea Crespi,[4,5] Fulvio Flamini,[1] Sandro Giacomini,[1] Giorgio Milani,[1] Roberta Ramponi,[4,5] Paolo Mataloni,[1,6] Roberto Osellame,[4,5,*] Ernesto F. Galvão,[3,†] and Fabio Sciarrino[1,6,‡]

Boson-Sampling in the light of sample complexity

C. Gogolin, M. Kliesch, L. Aolita, and J. Eisert

Dahlem Center for Complex Quantum Systems, Freie Universität Berlin, 14195 Berlin, Germany

September 17, 2013

Recently, Groups in Brisbane, Oxford, Rome and Vienna reported the first 3- and 4-photon BosonSampling experiments

Big Question: How does one know that the outcome is correct? (in the regime that classical ... is

classically

BosonSampling Is Far From Uniform

Scott Aaronson* Alex Arkhipov†

Stringent and efficient assessment of Boson-Sampling devices

Malte C. Tichy,[1] Klaus Mayer,[2] Andreas Buchleitner,[2] and Klaus Mølmer[1]

[1] *Department of Physics and Astronomy, Aarhus University, DK-8000 Aarhus, Denmark*
[2] *Physikalisches Institut, Albert-Ludwigs-Universität Freiburg, D-79104 Freiburg, Germany*
(Dated: December 12, 2013)

Boson-Sampling holds the potential to experimentally falsify the Extended Church Turing thesis. The computational hardness of Boson-Sampling, however, complicates the *certification* that an experimental device yields correct results in the regime in which it outmatches classical computers. We demonstrate the shortcomings of current protocols, which are bypassed by a model with randomly prepared independent particles. An alternative test based on Fourier matrices is shown to permit more stringent certification for arbitrarily many particles.

Verification of quantum computations

Verification of quantum computations

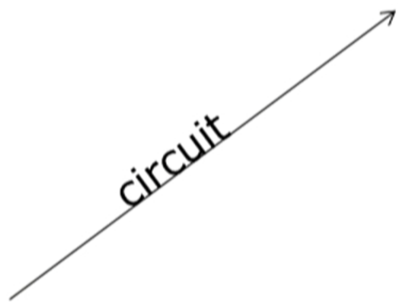
Prover
(quantum polynomial time)

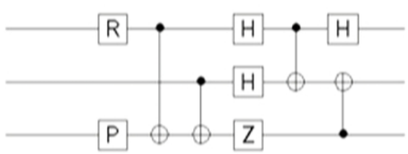
Verifier
(classical polynomial-time)

uOttawa

Verification of quantum computations

Prover
(quantum polynomial time)

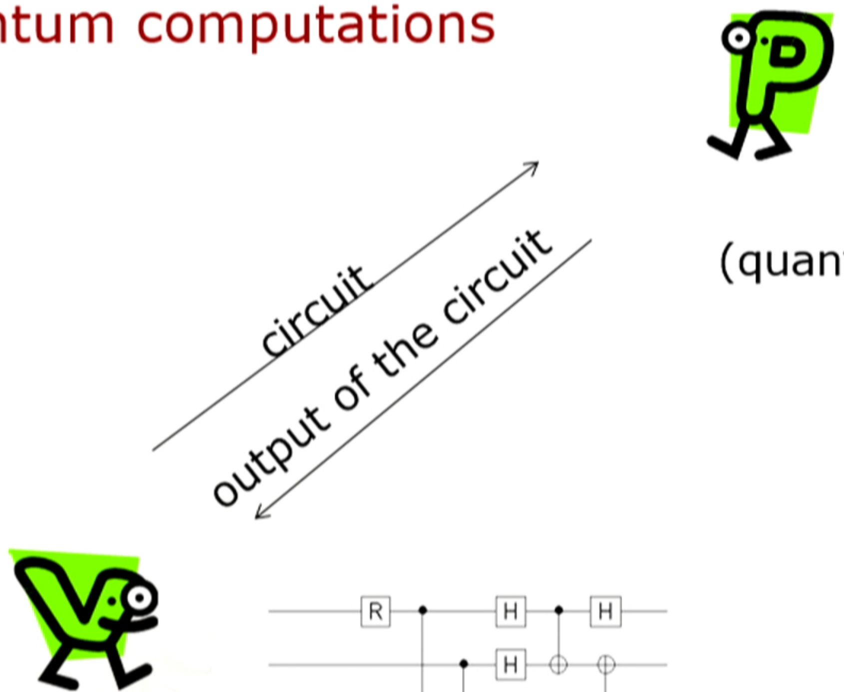




Verifier
(classical polynomial-time)

uOttawa

Verification of quantum computations



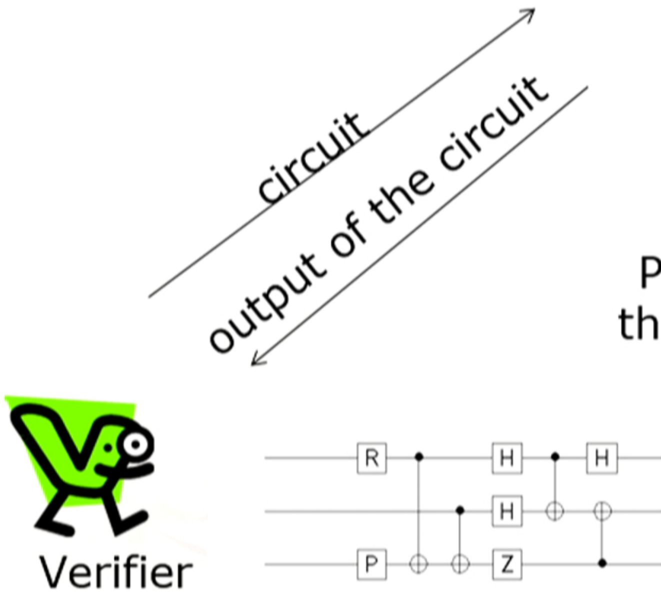
Prover
(quantum polynomial time)

Verifier
(classical polynomial-time)

uOttawa

Verification of quantum computations

Prover
(quantum polynomial time)



Prover wants to convince verifier that output is correctly computed*

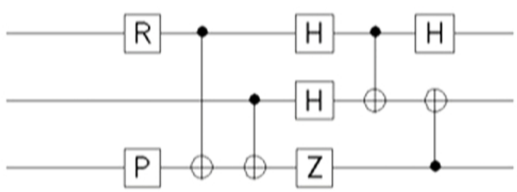
Verifier
(classical polynomial-time)

uOttawa

*modulo some probability of error.

How to verify a quantum computation?

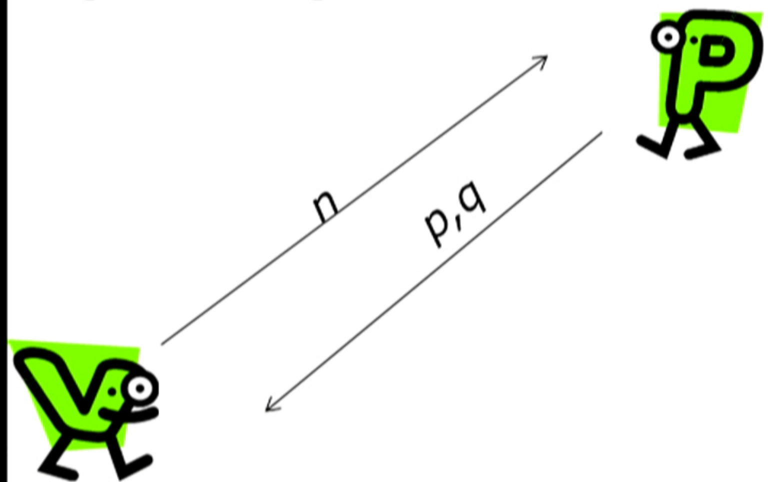
- test small parts, assume they work correctly together?
  - This is not testing at high computational complexity regime
- test computations that are easy to verify?
  (e.g. factoring)
  - does not encompass the *hardest* quantum problems.



uOttawa

Static Proofs

e.g. Factoring



$n = p \times q$?

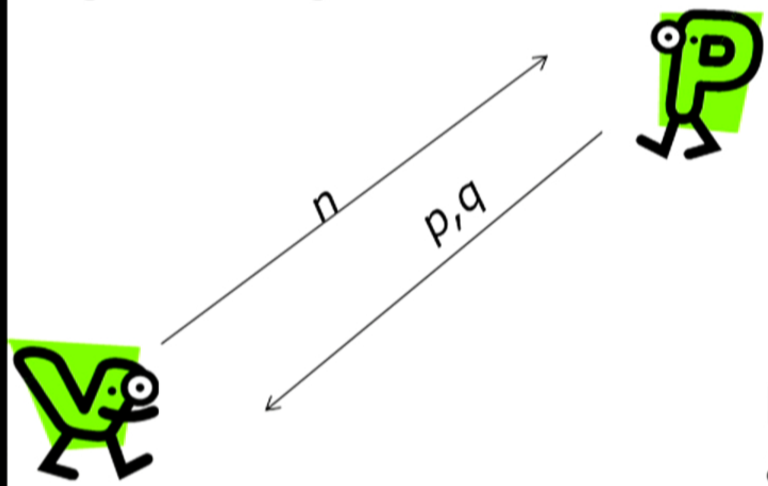
Completeness: "For a true assertion, there is a proof".

Soundness: "For a false assertion no proof exists."

uOttawa

Static Proofs

e.g. Factoring



$n = p \times q$?

Completeness: "For a true assertion, there is a proof".

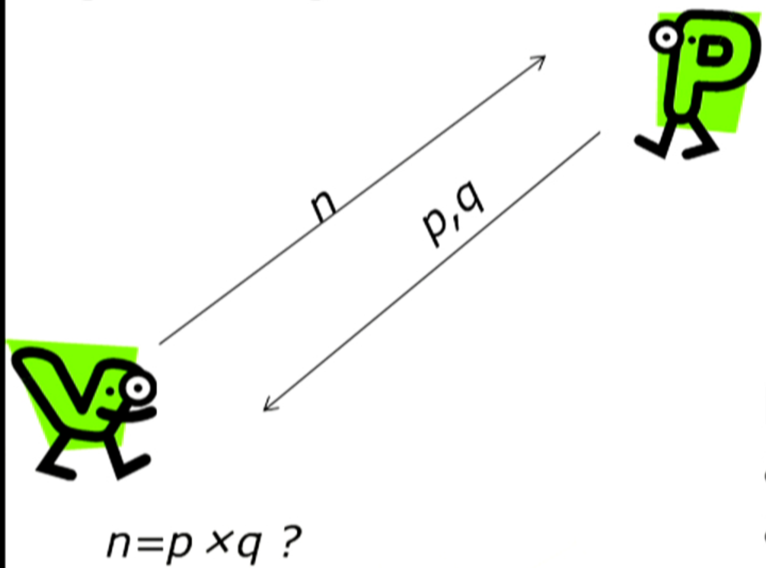
Soundness: "For a false assertion no proof exists."

NP: class of languages that admit a static proof (MA for a probabilistic verification)

uOttawa

Static Proofs

e.g. Factoring



Completeness: "For a true assertion, there is a proof".

Soundness: "For a false assertion no proof exists."

NP: class of languages that admit a static proof (MA for a probabilistic verification)

Can we verify more than MA?

uOttawa

The power of interaction

uOttawa

Interaction increases the power of the verification process

uOttawa

Interaction increases the power of the verification process

IP= PSPACE

uOttawa

Everything that can be computed in polynomial space can be proven in an interactive process.

The lady tasting tea
(Ronald Fisher, 1935)

uOttawa

Interactive verification of quantum computations

Prover is polynomial-time quantum computer

Verifier is almost-classical

uOttawa

The lady tasting tea
(Ronald Fisher, 1935)

uOttawa

Interactive verification of quantum computations

Prover is polynomial-time quantum computer

Verifier is almost-classical

As an experimenter, I can:

1. verify and characterize very simple quantum systems
2. predict the output of "trivial" quantum computations
3. interact with setup

Main result: 1-3 can be used to bootstrap the verification of a general quantum process.

uOttawa

Prior Approaches

Quantum Computing on Authenticated Data (QCAD) [1]

- Interactive Proofs for Quantum Computations [2]
- Quantum One-Time Programs [5]

Blind Quantum Computing [3]

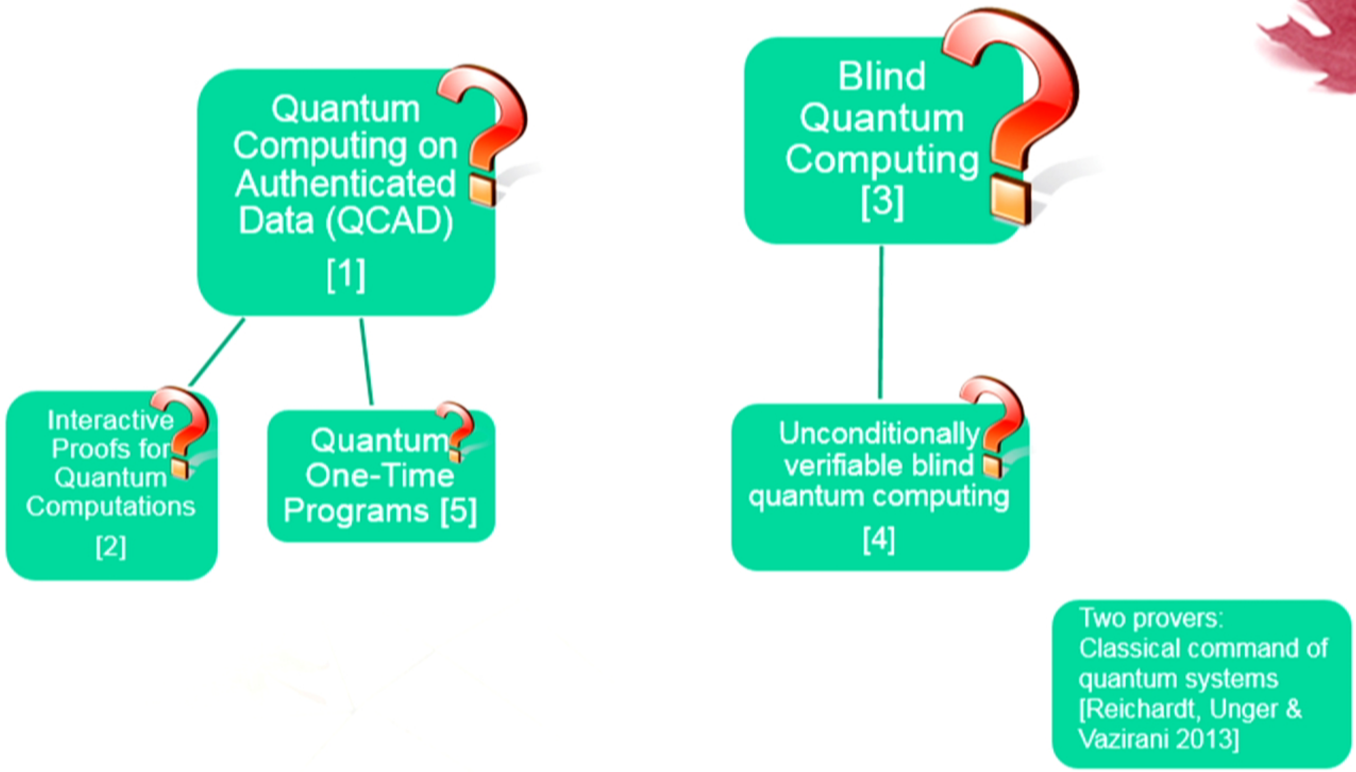
- Unconditionally verifiable blind quantum computing [4]

Two provers: Classical command of quantum systems [Reichardt, Unger & Vazirani 2013]

uOttawa

[1] Ben-Or, Crépeau, Gottesman, Hassidim & Smith 2006
[2]Aharonov, Ben-Or & Eban 2010
[3] Broadbent, Fitzsimons & Kashefi 2009
[4]Fitzsimons & Kashefi 2012
[5]Broadbent, Gutoski, & Stebila 2013

Prior Approaches



uOttawa

[1] Ben-Or, Crépeau, Gottesman, Hassidim & Smith 2006
[2]Aharonov, Ben-Or & Eban 2010
[3] Broadbent, Fitzsimons & Kashefi 2009
[4]Fitzsimons & Kashefi 2012
[5]Broadbent, Gutoski, & Stebila 2013

Back to the basics

What makes these protocols work?

How to prove soundness?

input privacy ⇒ indistinguishability of test/computation

Computation-by-teleportation⇒ verification of intermediate steps

“Equivalent” EPR-based interactive proof system

uOttawa

Main Theorem

For all of BQP, there exists an interactive proof system with a verifier V that runs in classical polynomial probabilistic time, augmented with the capacity to randomly generate states in each S_i, such that:

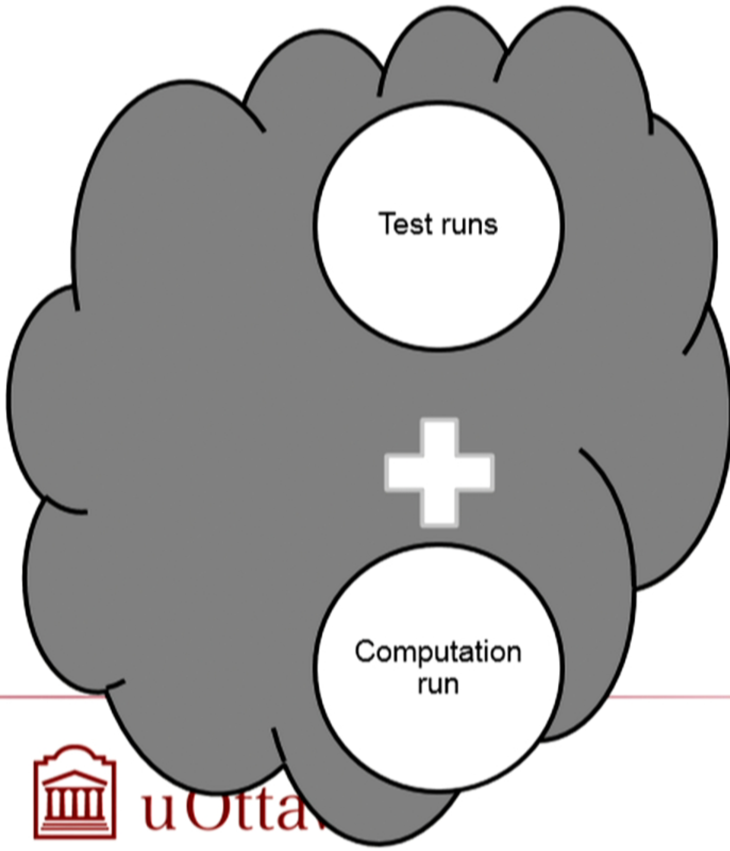
- (Completeness) for yes-instances, there exists a quantum polynomial time prover that can make V accept with probability ≥ 2/3.
- (Soundness) for no-instances, no prover (even unbounded) can make V accept with probability ≥ 1/3,

where $\{S_1, S_2, S_3, S_4\} =$

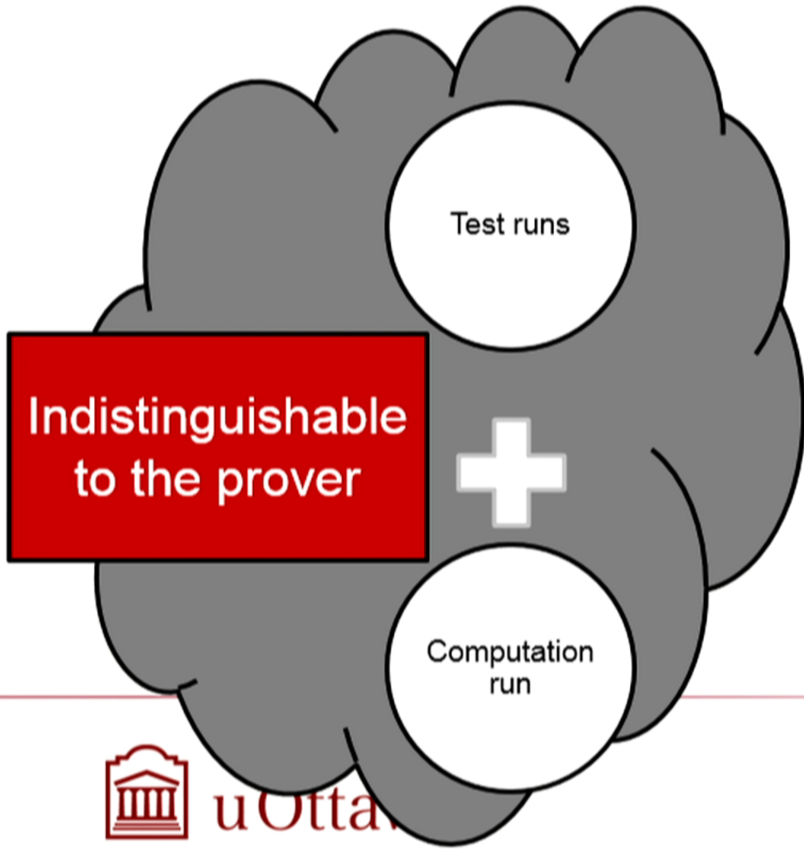
$$\{\{|0\rangle, |1\rangle\}, \{|+\rangle, |-\rangle\}, \{\mathsf{P}|+\rangle, \mathsf{P}|-\rangle\}, \{\mathsf{T}|+\rangle, \mathsf{T}|-\rangle, \mathsf{PT}|+\rangle, \mathsf{PT}|-\rangle\}\}$$

uOttawa

Interactive verification of quantum computations



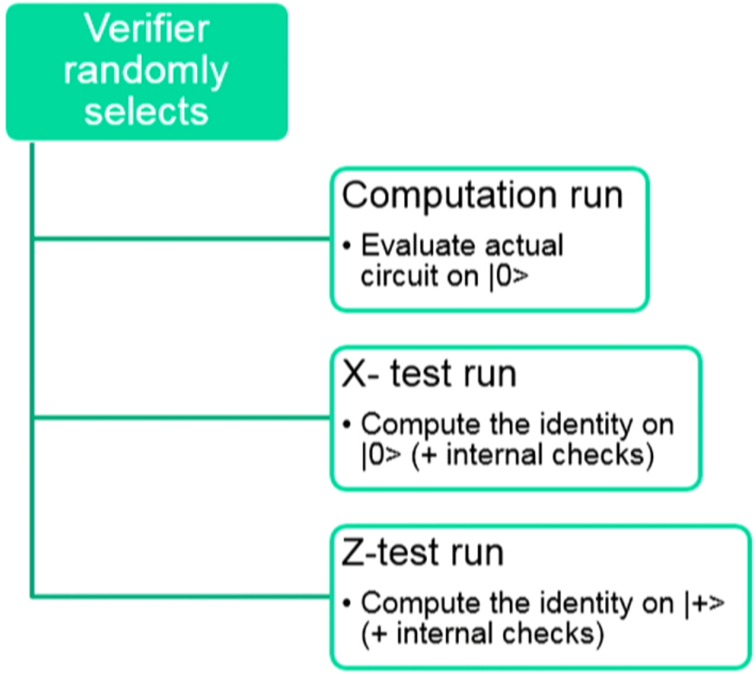
Interactive verification of quantum computations



Verifier randomly selects

- **Computation run**
  - Evaluate actual circuit on |0>
- **X- test run**
  - Compute the identity on |0> (+ internal checks)
- **Z-test run**
  - Compute the identity on |+> (+ internal checks)

uOttawa



How to achieve indistinguishability?

- Encrypt all communications to the prover
- Prover performs operations on encrypted data
- Prover's operations are the same is test and computation runs
- Only the verifier knows how to interpret results

uOttawa

The One-time Pad Encryption Scheme

1. The classical one-time pad

Plaintext	$x \in \{0,1\}$
Key	$k \in_R \{0,1\}$
Ciphertext	$x \oplus k$

Since the ciphertext is uniformly random (as long as k is random and unknown), the plaintext is perfectly concealed.

2. The quantum one-time pad

Plaintext	$\|\psi\rangle = \alpha\|0\rangle + \beta\|1\rangle$
Key	$(a,b) \in_R \{0,1\}^2$
Ciphertext	$\mathsf{Z}^a \mathsf{X}^b \|\psi\rangle$

$\mathsf{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ $\mathsf{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

Pauli gates

Without knowledge of the key, the ciphertext always appears as the maximally mixed state, $\frac{\mathbb{I}}{2}$.

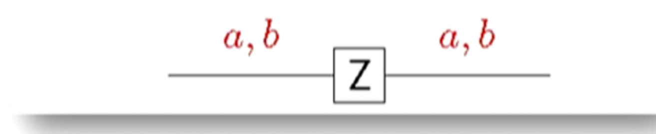
uOttawa

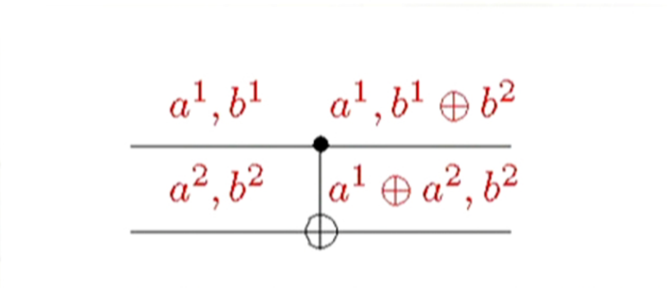
Quantum Computing on Encrypted Data

- Encryption is done via a random Pauli

$$\mathsf{Z}^a \mathsf{X}^b \left|\psi\right\rangle$$

- Gates are performed on encrypted data via gadgets



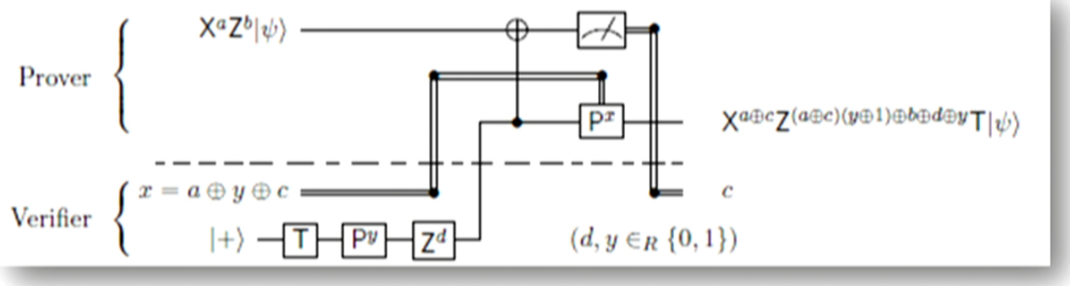


$$\mathsf{CNOT}(\left|0\right\rangle \left|0\right\rangle) = \left|0\right\rangle \left|0\right\rangle$$
$$\mathsf{CNOT}(\left|+\right\rangle \left|+\right\rangle) = \left|+\right\rangle \left|+\right\rangle$$

uOttawa

T gate gadget uses an auxiliary qubit

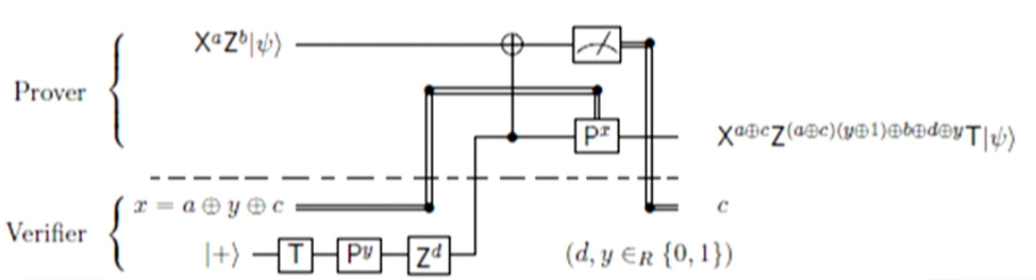
- Computation run:



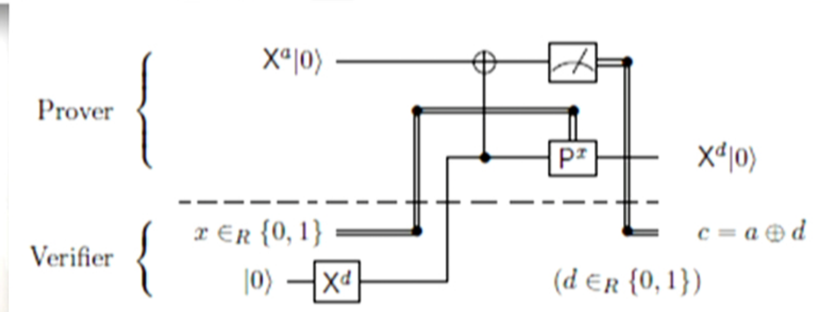
uOttawa

T gate gadget uses an auxiliary qubit

- Computation run:



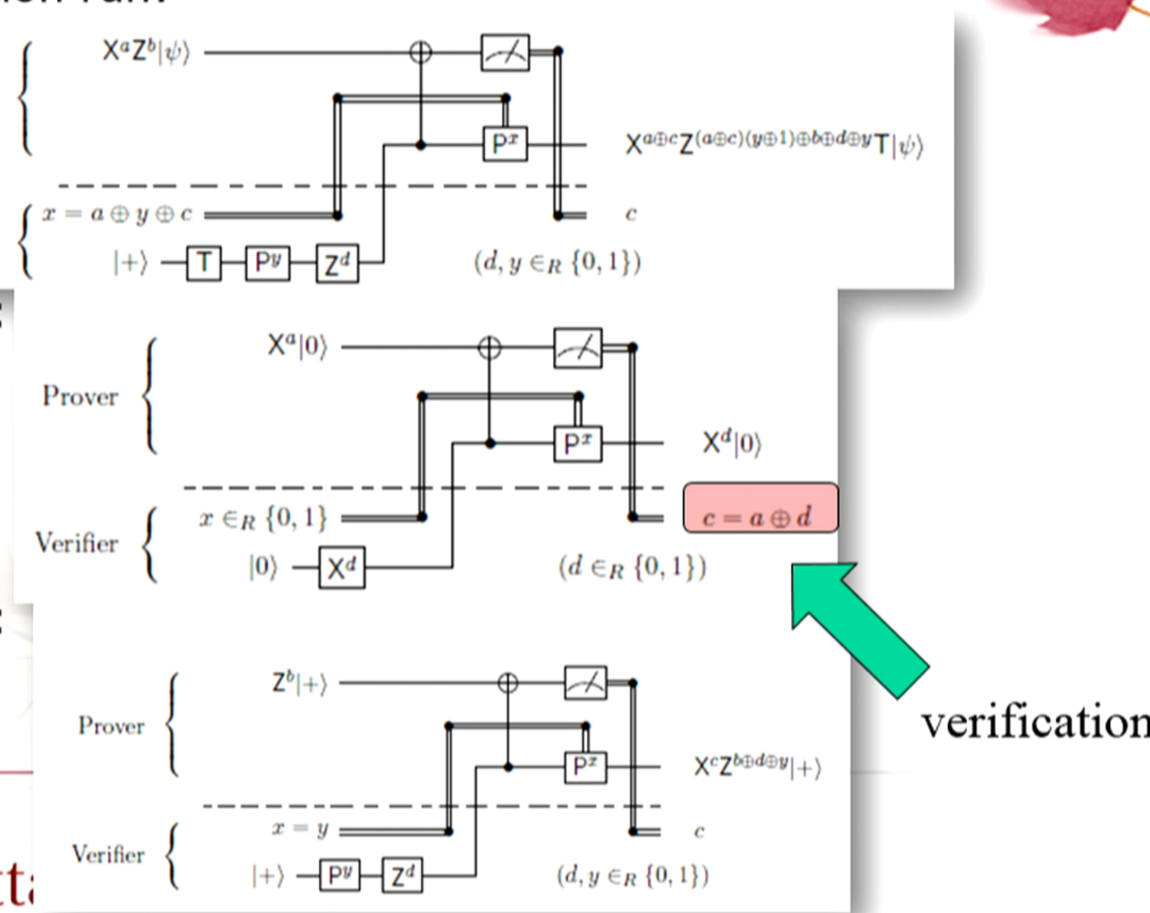
- X-test run:



uOttawa

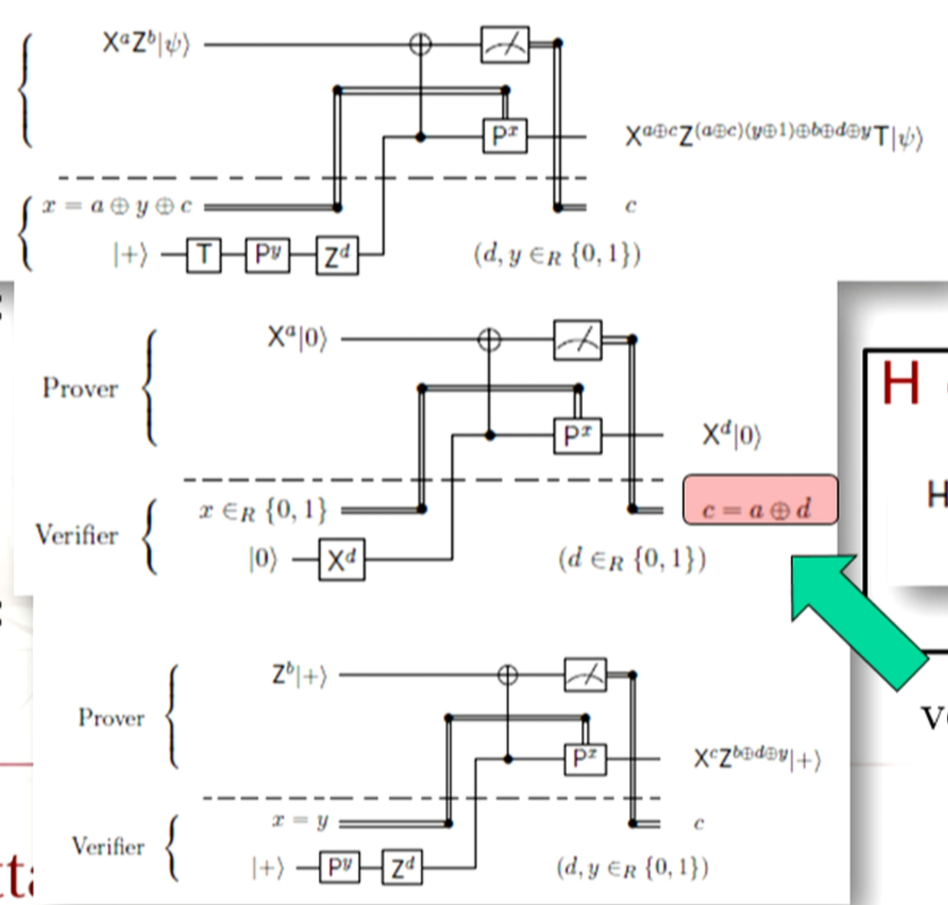
T gate gadget uses an auxiliary qubit

- Computation run:
- X-test run:
- Z-test run:



T gate gadget uses an auxiliary qubit

- Computation run:
- X-test run:
- Z-test run:



H gate

HPHPHPH = H

HHHH = I.

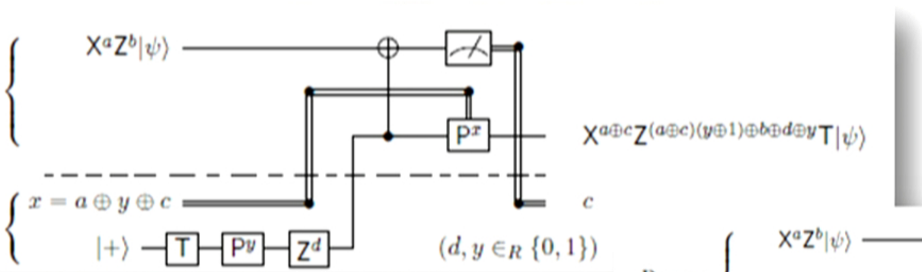
verification

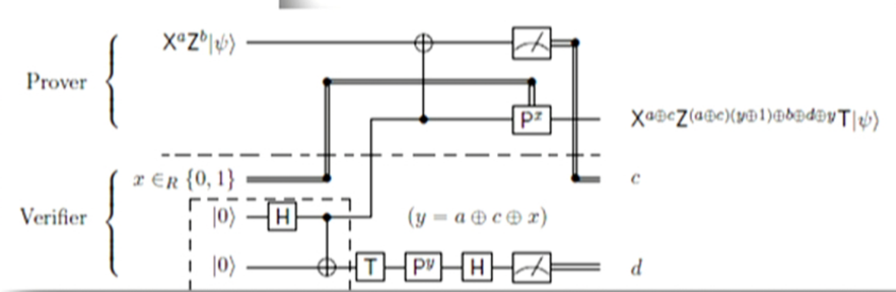
uOtt

Soundness:

- Analyse entanglement-based protocol [1]

1. Encrypted qubits replaced by half-EPR pairs





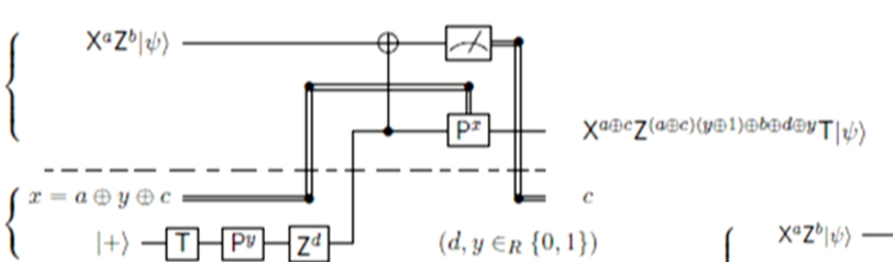
uOttawa

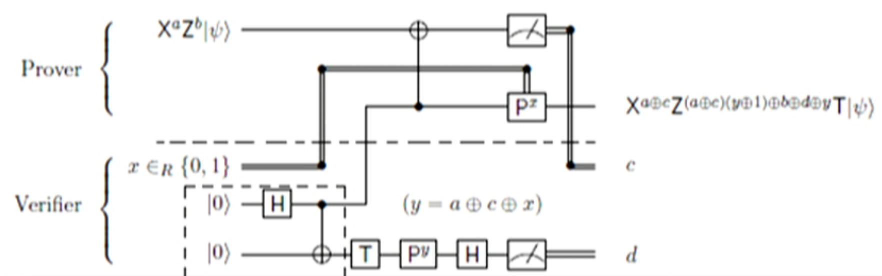
[1] Shor & Preskill 2000

Soundness:

– Analyse entanglement-based protocol [1]

1. Encrypted qubits replaced by half-EPR pairs





uOttawa

[1] Shor & Preskill 2000

Attacks on the quantum one-time pad

Encrypt → Attack U → Decrypt

$$\rho \mapsto \frac{1}{4^n} \sum_{\text{Paulis} P} P\rho P^* \mapsto \frac{1}{4^n} \sum_{\text{Paulis} P} UP\rho P^* U^*$$

$$= \frac{1}{4^n} \sum_{\text{Paulis} P, Q, Q'} \alpha_Q \alpha'_Q Q P \rho P^* Q'^*$$

$$U = \sum_{\text{Paulis} Q} \alpha_Q Q$$

$$U^* = \sum_{\text{Paulis} Q'} \alpha^*_{Q'} Q'^*$$

uOttawa

Simplifying a prover's strategy:

1. Delay all measurements.
2. Write P's strategy as the honest strategy, C, followed by a cheating map Φ with Kraus terms $\{E_k\}$. The system before measurements is:

$$\frac{1}{2^m}\sum_{P\in\text{Paulis}}\sum_{k} E_k C P \left|\psi\right\rangle \left\langle\psi\right| P^* C^* E_k^*$$

(Where $|\psi\rangle$ is some initial state prepared by V).

3. Let $CP = \tilde{P}C$. Quantumly apply the decryption operation :

$$\frac{1}{2^m}\sum_{\tilde{P}\in\text{Paulis}}\sum_{k} \tilde{P}^* E_k \tilde{P} C \left|\psi\right\rangle \left\langle\psi\right| C^* \tilde{P}^* E_k^* \tilde{P}$$

4. Write each E_k, E_k^* in the Pauli basis. By the Pauli twirl, we get:

$$\frac{1}{2^m}\sum_{Q\in\text{Paulis}} |\alpha_Q|^2 Q C \left|\psi\right\rangle \left\langle\psi\right| C^* Q^*$$

uOttawa

Attack= convex combination of Pauli attacks on output qubits

Simplifying a prover's strategy:

1. Delay all measurements.
2. Write P's strategy as the honest strategy, C, followed by a cheating map Φ with Kraus terms $\{E_k\}$. The system before measurements is:

$$\frac{1}{2^m} \sum_{P \in \text{Paulis}} \sum_k E_k C P \left|\psi\right\rangle \left\langle\psi\right| P^* C^* E_k^*$$

(Where $\left|\psi\right\rangle$ is some initial state prepared by V).

3. Let $CP = \tilde{P}C$. Quantumly apply the decryption operation :

$$\frac{1}{2^m} \sum_{\tilde{P} \in \text{Paulis}} \sum_k \tilde{P}^* E_k \tilde{P} C \left|\psi\right\rangle \left\langle\psi\right| C^* \tilde{P}^* E_k^* \tilde{P}$$

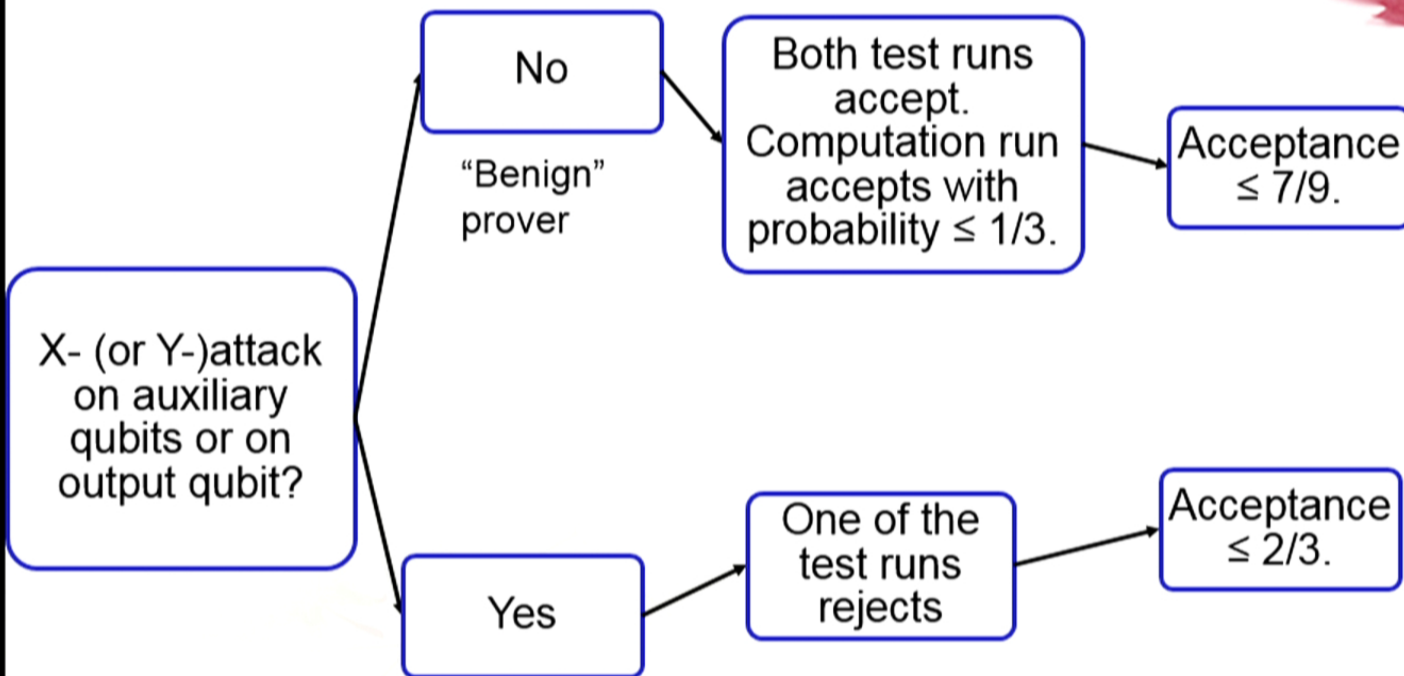
4. Write each E_k, E_k^* in the Pauli basis. By the Pauli twirl, we get:

$$\frac{1}{2^m} \sum_{Q \in \text{Paulis}} |\alpha_Q|^2 Q C \left|\psi\right\rangle \left\langle\psi\right| C^* Q^*$$

Attack= convex combination of Pauli attacks on output qubits

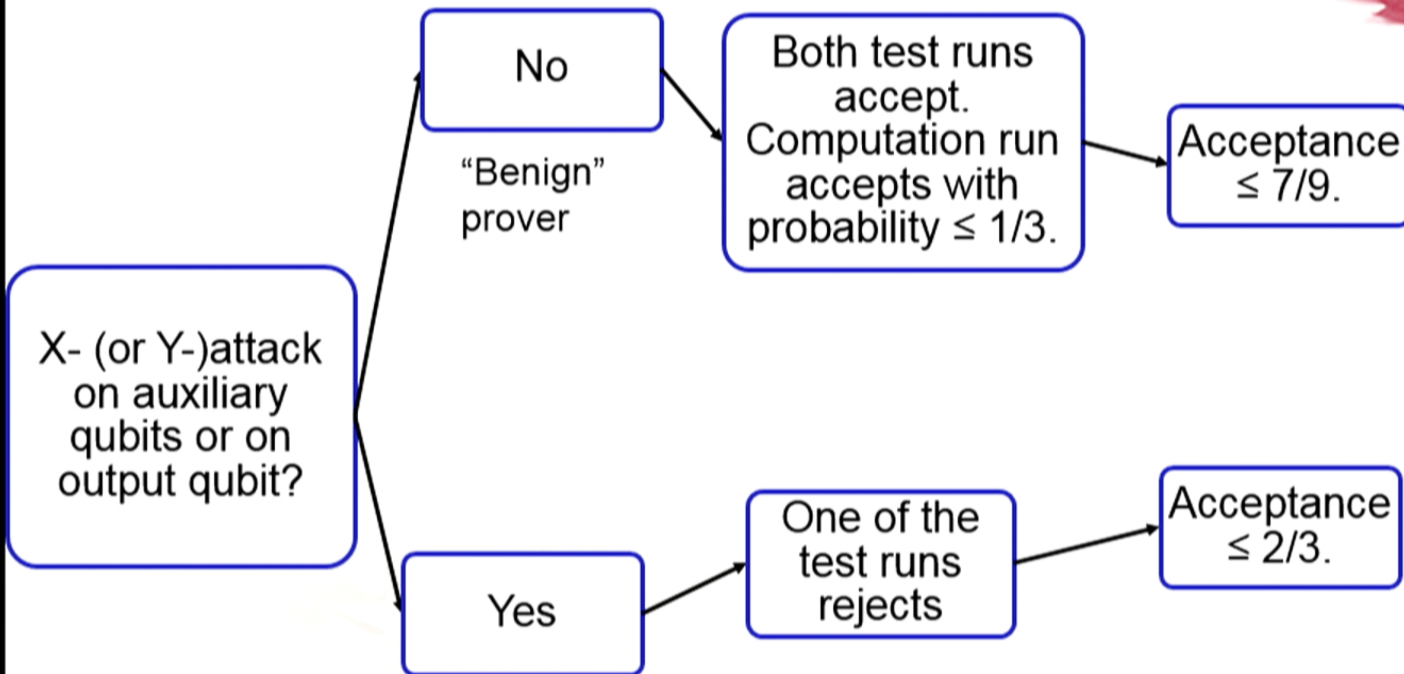
uOttawa

Detecting any Pauli attack



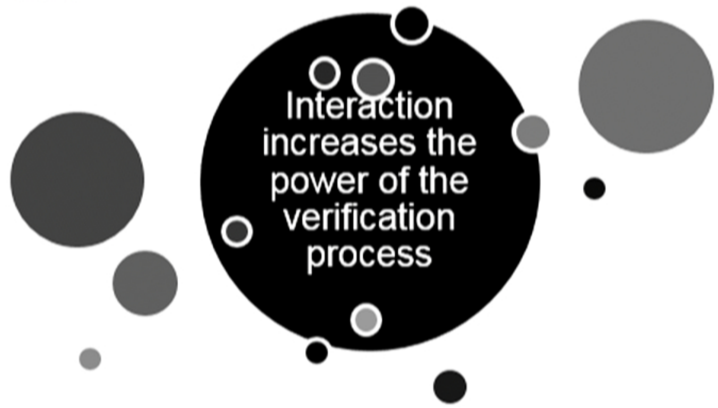
uOttawa

Detecting any Pauli attack

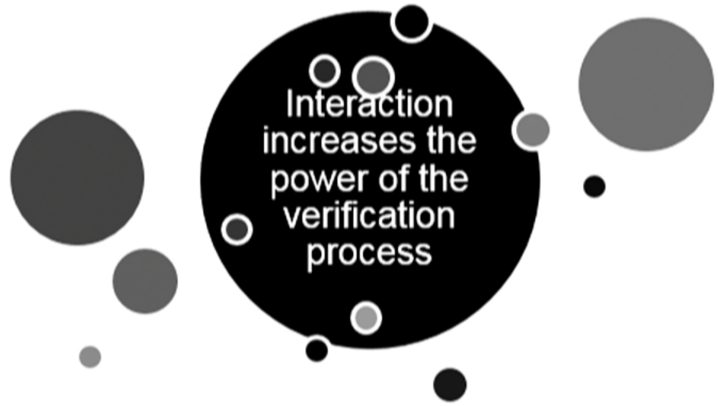


uOttawa

Conclusion


Interaction increases the power of the verification process

Conclusion



Open question: fully classical verifier?

uOttawa

Thank you!