# Relativistic and Device-Independent Verifiable Quantum Computation

Petros Wallden

Workshop on Continuous Variables and Relativistic Quantum Information

6th International Conference on New Frontiers in Physics

Crete, Greece, 21st August 2017

# Motivation I

based on: Gheorghiu, Kashefi, Wallden NJP 2015; Kashefi, Wallden JPA 2017; Gheorghiu, Kashefi, Unruh, Wallden 2017 in preparation

**Central Question for Quantum Verification**

Can we verify a quantum computation without a quantum computer?

- Quantum computers are believed to be more powerful than classical computers ⇒ Cannot simulate classically
- How do we know the computation was correct?
- Under what conditions can we classically verify a quantum computation?
- Can "little" quantumness help us verify a quantum computation?
- Can we classically verify a restricted class of quantum computation?

# Motivation I

**Verifiable Blind Quantum Computation (VBQC)**

A client with limited quantum abilities can delegate a computation to a quantum server, without the server learning the input or computation and the client can verify that the result is correct.

- This protocol can be used to:
    1. Test quantumness – verify a quantum device
    2. As a crypto tool for secure delegated computation and for secure multiparty quantum computation
- We will focus on protocols based on Measurement-Based Quantum Computation (MBQC)

# Motivation II

## Device Independence

Cryptographic protocols where parties do not trust their own devices (potentially prepared by adversaries), and are treated as black boxes.

- Ultimate security guarantee allowed by nature
- Possible due to unique quantum property of non-locality
- Certain assumptions still exist (e.g.):
  - Fair sampling
  - Non-communication of devices of parties
- Non-communication could be imposed by spacelike separation of parties

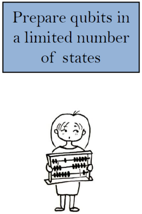
**This talk:** Device Independent VBQC with no assumption of non-communication

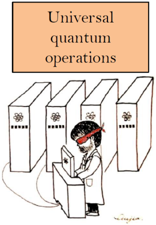
# Outline

- Verifiable Blind Quantum Computation
- Device-Independent VBQC
  1. Robustness
  2. Rigidity
- Relativistic VBQC
  1. A resource state that does not leak information
  2. How to correct $\phi = \pi/4$ gates blindly
  3. A stepwise verification protocol
- Conclusion

# Background: Measurement-Based Quantum Computation

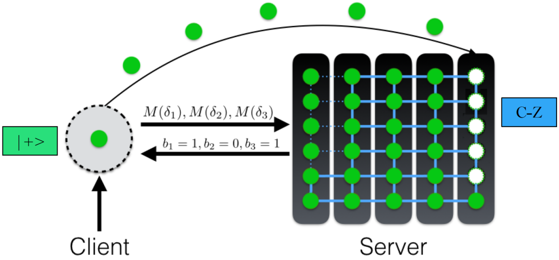
- Equivalent with circuit quantum computation (universal)
- Prepare large entangled state (resource)
- Computation is performed by single-qubit measurements
- Angles/instructions modified according to previous outcomes
- Default (pre-correction) angles determine computation
- Separation of classical-quantum parts of computation



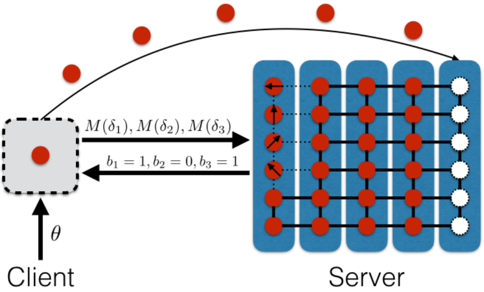

- Can view it as Client - Server setting (delegated computation)
- Client (almost) classical Vs Server full Quantum Computer

# Background: MBQC




- Client sends single qubits, Server entangles them
- Client sends instructions on how to measure them
- Default angle $\phi_i$ determines computation.
  Standard corrections that depend on previous outcomes:
  $\phi'_i = (-1)^{S_x(b_{j<i})}\phi_i + \pi S_z(b_{j<i})$

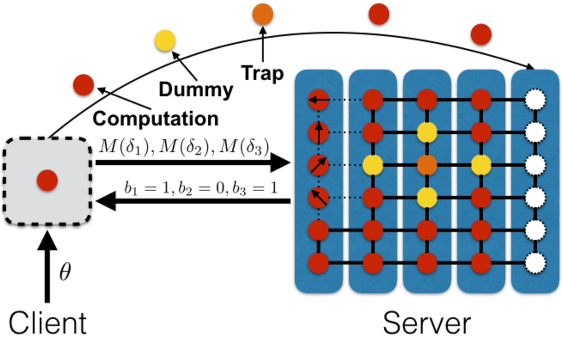
# Background: Blind Quantum Computation




- Can make computation blind to Server (Broadbent, FItzsimons, Kashefi 2009)
- Client send pre-rotated qubits $|+_{\theta_i}\rangle$ while also adds a mask on outcomes $r_i$
- Instructs Server to measure at angle that hides the true computation angle: $\delta_i = \phi'_i + \theta_i + \pi r_i$
- Interest for secure delegated computation

Verify: Client tests Server (VBQC)

# Background: Verifiable Blind Quantum Computation



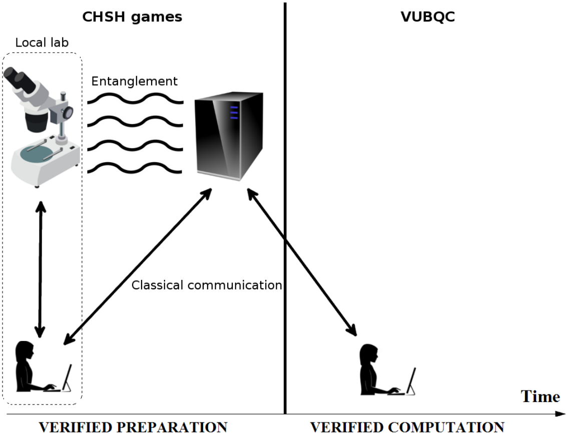

- Resource with multiple indep traps (Fitzsimons, Kashefi 2012)
- Traps deterministic outcome – position unknown to Server
- **Honest behaviour enforced** or traps detect it!
- If secure against malicious server can be certain of correctness "against" faulty devices

# Background: VBQC

- Computation encoded with QECC.
- Computation $\Rightarrow$ logical qubits, traps $\Rightarrow$ physical qubits.
- Single error on trap $\Rightarrow$ abort, multiple errors on computation in order to corrupt the computation.
- Protocol fails with $\epsilon$-probability for "corrupt AND not-abort"
- **verification (VBQC) = blindness + traps**
  1. Client prepares qubits $|+_{\theta_i}\rangle = |0\rangle + \exp(i\theta_i)|1\rangle$ where $\theta_i \in \{0, \pi/4, \cdots, 7\pi/4\}$ known **only** to her.
  2. Blindness of **position of traps** and **secret parameters** is crucial for the proof.

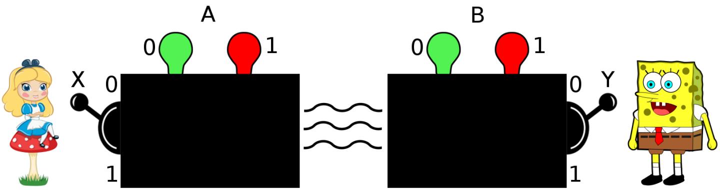
# General Idea

1. Verified preparation: Use (untrusted) devices to prepare the $|+_\theta\rangle$ states at the server side
2. Verified computation: Run the VBQC protocol



# Verified Preparation

- Prepare tensor product of Bell pairs (check CHSH violation)
- Have Alice measure (remaining) pairs in $|\pm_{\theta_i}\rangle$ basis and prepare $|\pm_{\theta_i}\rangle$ states on Bob side




NOTE: Alice cannot prepare deterministically the states she wishes (there is a $\pi$ random phase)

# Verified Computation

- Client (Alice) instructs Bob to entangle and measure according to VBQC the qubits **not used** for CHSH tests
- Any deviation by Bob (after preparation of single qubits) does not affect the VBQC protocol by construction

Issues:

1. Need to be sure after CHSH tests of **tensor product of Bell pairs** [Rigidity]
2. Need to make VBQC secure if $|+_\theta\rangle$ are $\epsilon$-deviated [Robustness]
3. The instruction $\delta$ to Bob, are adaptive and need to happen **after** Alice measures her qubits
4. Should make sure that nothing leaks about the position of traps or secret parameters

# Device Independent VBQC (GKW2015)

- Proved robustness: $\epsilon$ deviated inputs lead to $\sqrt{\epsilon}$-verifiable VBQC protocol
  Extra cost due to correlations between attacks in the verified preparation stage and the verified computation stage (c.f. coherent attacks)
- Modified Reichardt, Unger, Vazirani 2012 to prove rigidity of CHSH games. Very costly!
  Any improvement (Natarajan, Vidick 2016) or increased trust (GWK2017) of verified preparation can be used directly

- Assumed non-communication of the devices is enforced "externally"
Due to adaptivity of angles $\delta$ we cannot have Alice and Bob spacelike separated for all the run of the protocol
- Same time that is required to learn the correct angles, "malicious devices" can leak information (trap position) that breaks VBQC

# Three Problems Imposing Non-Communication

One could have Alice - Bob spacelike separated and have multiple rounds of verified preparation (CHSH games) and verified computation (VBQC).

However:

1. Revealing part of the resource leaks information about traps in other places
2. For $\phi = \pi/4$ Alice needs to know the outcome of her measurement of **that** round before sending the classical instruction (cannot "correct" retrospectively)
3. The proof of VBQC should be done in a stepwise way (guarantee security for intermediate steps, i.e. without measuring the final "layer" traps).

# Three Problems Imposing Non-Communication

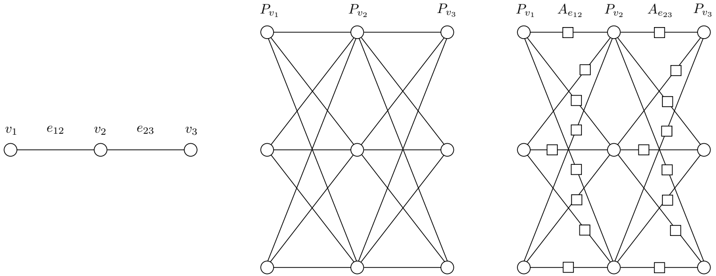
One could have Alice - Bob spacelike separated and have multiple rounds of verified preparation (CHSH games) and verified computation (VBQC).

However:

1. Revealing part of the resource leaks information about traps in other places
2. For $\phi = \pi/4$ Alice needs to know the outcome of her measurement of **that** round before sending the classical instruction (cannot "correct" retrospectively)
3. The proof of VBQC should be done in a stepwise way (guarantee security for intermediate steps, i.e. without measuring the final "layer" traps).

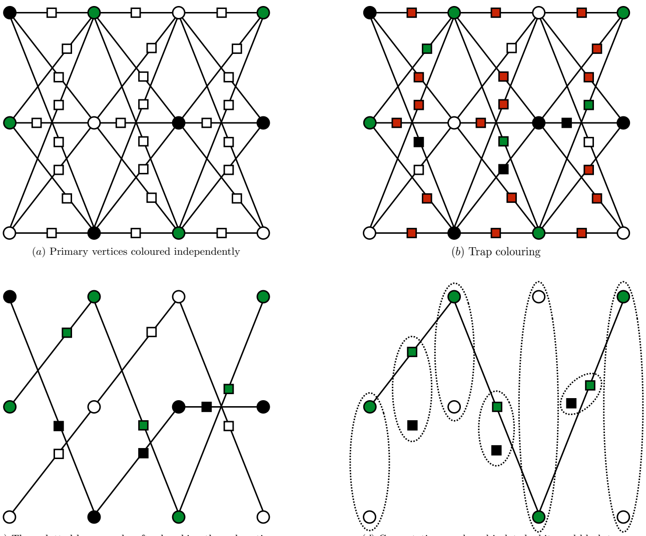
# Solution for Problem 1 (KW2017)

- New resource: **Dotted-triple Graph** (DTG)
- Positions of traps are independent at each part of the MBQC "base"-graph
- Leaking trap positions at one layer leaks nothing about traps at later layers
- Bonus: smaller cost. Linear in the number of the computation graph (compared to quadratic previously)
- Security parameter $\epsilon = \left(\frac{8}{9}\right)^d$




$(a)$ $(b)$ $(c)$

# Solution for Problem 1 (KW2017)



(a) Primary vertices coloured independently

(b) Trap colouring

(c) Three dotted base graphs after breaking the red vertices

(d) Computation graph and isolated white and black traps

# Three Problems Imposing Non-Communication

One could have Alice - Bob spacelike separated and have multiple rounds of verified preparation (CHSH games) and verified computation (VBQC).

However:

1. Revealing part of the resource leaks information about traps in other places
2. For $\phi = \pi/4$ Alice needs to know the outcome of her measurement of **that** round before sending the classical instruction (cannot "correct" retrospectively)
3. The proof of VBQC should be done in a stepwise way (guarantee security for intermediate steps, i.e. without measuring the final "layer" traps).

# Solution for Problem 2

- If we measure at $\delta' = \delta + \pi$, is the same measurement but with the labels of the (classical) result flipped!
- Alice can prepare at Bob states $|+_{(\theta + r\pi)}\rangle$, where $r$ is the outcome of her measurement
- However: resource is such that there are **correlations between the trap positions of two consecutive layers**
- Each "round" of CHSH games/verified preparation, should contain qubits of two layers
- **Result of measurements** and info about **trap positions** of that layer "arrive" at the **same time** in Bob's lab.
- Need to **delay** the need for knowledge of the outcome $b_1$, until a round the trap positions do not depend on those of layer one

# Solution for Problem 2

- As we have seen $\phi_2' = (-1)^{b_1}\phi_2$ where $b_1$ is the previous layer outcome
- If $\phi_2 \in \{0, \pi/2, \pi, 3\pi/2\}$ the measurement does not change
- If $\phi_2 \in \{pi/4, 3\pi/4, 5\pi/4, 7\pi/4\}$ the measurement changes if $b_1 = 1$
- i.e. if we instruct to measure $\phi_2 = \pi/4$ it may result to the gate $J(\pi/4)$ or $J(-\pi/4)$ depending on $b_1$

NOTE: $J(\phi) = HZ(\phi)$ and $Z(\phi)$ is $\phi$ rotation in $Z$-basis

# Solution for Problem 2

- If we make the preparation in rounds, Alice can correct the "mistake" in future rounds
- We note that: $J(0)J^{b_1}(0)J^{b_1}(\pi/2)J(0)J((-1)^{b_1}\pi/4) = J(\pi/4)$
- To do a $\pi/4$-gate (r.h.s), we measure at the fixed $\phi_2$ angle and at later layers we apply (or not) correction gates (l.h.s.)
- We have Alice delaying the correction.
  - At the step/layer she needs to know $b_1$ (3rd), it leaks no information about the positions of the traps of that layer
  - Correlations of trap positions exist within 2-layers in DTG!

# Three Problems Imposing Non-Communication

One could have Alice - Bob spacelike separated and have multiple rounds of verified preparation (CHSH games) and verified computation (VBQC).

However:

1. Revealing part of the resource leaks information about traps in other places
2. For $\phi = \pi/4$ Alice needs to know the outcome of her measurement of **that** round before sending the classical instruction (cannot "correct" retrospectively)
3. The proof of VBQC should be done in a stepwise way (guarantee security for intermediate steps, i.e. without measuring the final "layer" traps).

# Solution for Problem 3

- The security guarantee of VBQC concerns the final state **after** final layer traps have been measured
- We need a stepwise protocol, where the guarantee for the output layer/state:
  1. does not need measured output traps
  2. has no dependence on the input secret parameters
- In the proof, deviations of different layers are (mathematically) all commuted to a single deviation at the end
- That deviation depends on the secret parameters of all layers, **including** the input layers

# Solution for Problem 3

- New functionality: **Authenticated Stepwise Computation**

  *Takes input an authenticated quantum state (from a Quantum Authenticated Scheme - QAS) and gives output the "time-evolved" state encrypted with QAS with* **fresh** *secret parameters*

- VBQC modified to match this functionality requires **totally** new proof
- We defined intermediate protocols, each close to the previous. Started from the real protocol and ended at the ideal

# Solution for Problem 3

- Key idea:
  1. Terms with more than $d$-errors, abort w.h.p. $\Rightarrow$ approx same as if they had errors on *all* qubits
  2. Terms with fewer than $d$-errors cannot cause an error on the computation, since it is encoded in a QECC

  Any dependency on secret parameters of different terms is "washed-out"
- Similar to total-QAS where "total" guarantees that the state is authenticated for **each** choice of secret parameters w.h.p. and not on average
- Used this type of QAS to prove equivalence of intermediate protocols, and ensure security against all attacks
  - Includes attacks involving coherent manipulation of different layers qubits

# Summary

1. Reviewed VBQC
2. Gave a DI-VBQC where non-communication is imposed externally.
   Robustness of VBQC and Rigidity of CHSH were the key elements.
3. Listed three problems and the solutions for imposing non-communication by spacelike separation

REFERENCES


- Broadbent, Fitzsimons, Kashefi FOOCS 2009
- Fitzsimons, Kashefi arXiv:1203.5217 2012
- (GKW2015) Gheorghiu, Kashefi, Wallden NJP 2015
- Reihardt, Unger, Vazirani Nature 2013
- Natarajan, Vidick arXiv:1610.03574 2016
- (KW2017) Kashefi, Wallden J. Phys. A 2017
- (GWK2017) Gheorghiu, Wallden, Kashefi NJP 2017
- Gheorghiu, Kashefi, Unruh, Wallden in preparation 2017


**Thanks for your attention!!**