Robustness and device independence of verifiable blind quantum computing

[New J. Phys. 17 (2015) 083040]

Alexandru Gheorghiu, Elham Kashefi, Petros Wallden

1 October

QCrypt 2015, Tokyo

Quantum Verification

Central Question

Can we classically verify the correctness of a computation performed by a quantum device?

Quantum Verification

Central Question

Can we classically verify the correctness of a computation performed by a quantum device?

Theoretical

- $\mathrm{BPP} \overset{?}{\subset} \mathrm{BQP}$, $\mathrm{BQP} \overset{?}{\subset} \mathrm{PH}$
- Quantum and post-quantum cryptography
- Quantum correlations

Quantum Verification

Central Question

Can we classically verify the correctness of a computation performed by a quantum device?

Theoretical

- $\mathrm{BPP} \overset{?}{\subset} \mathrm{BQP}$, $\mathrm{BQP} \overset{?}{\subset} \mathrm{PH}$
- Quantum and post-quantum cryptography
- Quantum correlations

Practical

- Secure delegated (quantum) computations
- Experiments and simulations of quantum mechanics
- Verifying actual quantum computers

Existing approaches

Single server

- Restricted quantum verifier
  [*Aharonov, Ben-Or, Eban '10*], [*Fitzsimons, Kashefi '12*]
- Measurement-only verifier
  [*Morimae '14*], [*Hayashi, Morimae '15*]
- Device independent verifier
  this work, [*Hajdusek, Perez-Delgado, Fitzsimons '15*]
- Classical verifier
  open problem

Non-communicating, entangled servers

- Classical verifier, 2 servers
  [*Reichardt, Unger, Vazirani '12*]
- Classical verifier, multiple servers
  [*McKague '13*]

Verified Universal Blind Quantum Computation (VUBQC)

Important characteristics of [*Fitzsimons, Kashefi '12*] protocol:

- Universal for quantum computations
- Minimal quantum requirements for verifier
- Minimal number of rounds of communication
- Server only learns size of computation (blindness)

Verified Universal Blind Quantum Computation (VUBQC)

Important characteristics of [*Fitzsimons, Kashefi '12*] protocol:

- Universal for quantum computations
- Minimal quantum requirements for verifier
- Minimal number of rounds of communication
- Server only learns size of computation (blindness)

The optimality of this protocol has led to several developments:

- Verification of AKLT states
  [*Morimae, Dunjko, Kashefi '11*]
- Verification with coherent states
  [*Dunjko, Kashefi, Leverrier '12*]
- Experimental implementation
  [*Barz, Fitzsimons, Kashefi, Walther '13*]
- Verification of one-pure-qubit computation
  [*Kapourniotis, Kashefi, Datta '14*]
- Blind quantum computing with decoy states
  [*Xu, Lo '15*]
- Verification with minimal communication
  [*Kapourniotis, Dunjko, Kashefi '15*]

Towards device-independent VUBQC

One-sided device independence

The previous VUBQC protocol assumes a trusted source

Towards device-independent VUBQC

One-sided device independence

The previous VUBQC protocol assumes a trusted source

We remove the assumption of trusted source

$\Longrightarrow$ **device independence**

Towards device-independent VUBQC

One-sided device independence

The previous VUBQC protocol assumes a trusted source

We remove the assumption of trusted source

$\Longrightarrow$ **device independence**

Device independence

Verifier and server share entanglement. Verifier has untrusted single qubit measurement device.

Towards device-independent VUBQC

One-sided device independence

The previous VUBQC protocol assumes a trusted source

We remove the assumption of trusted source
$\Longrightarrow$ **device independence**

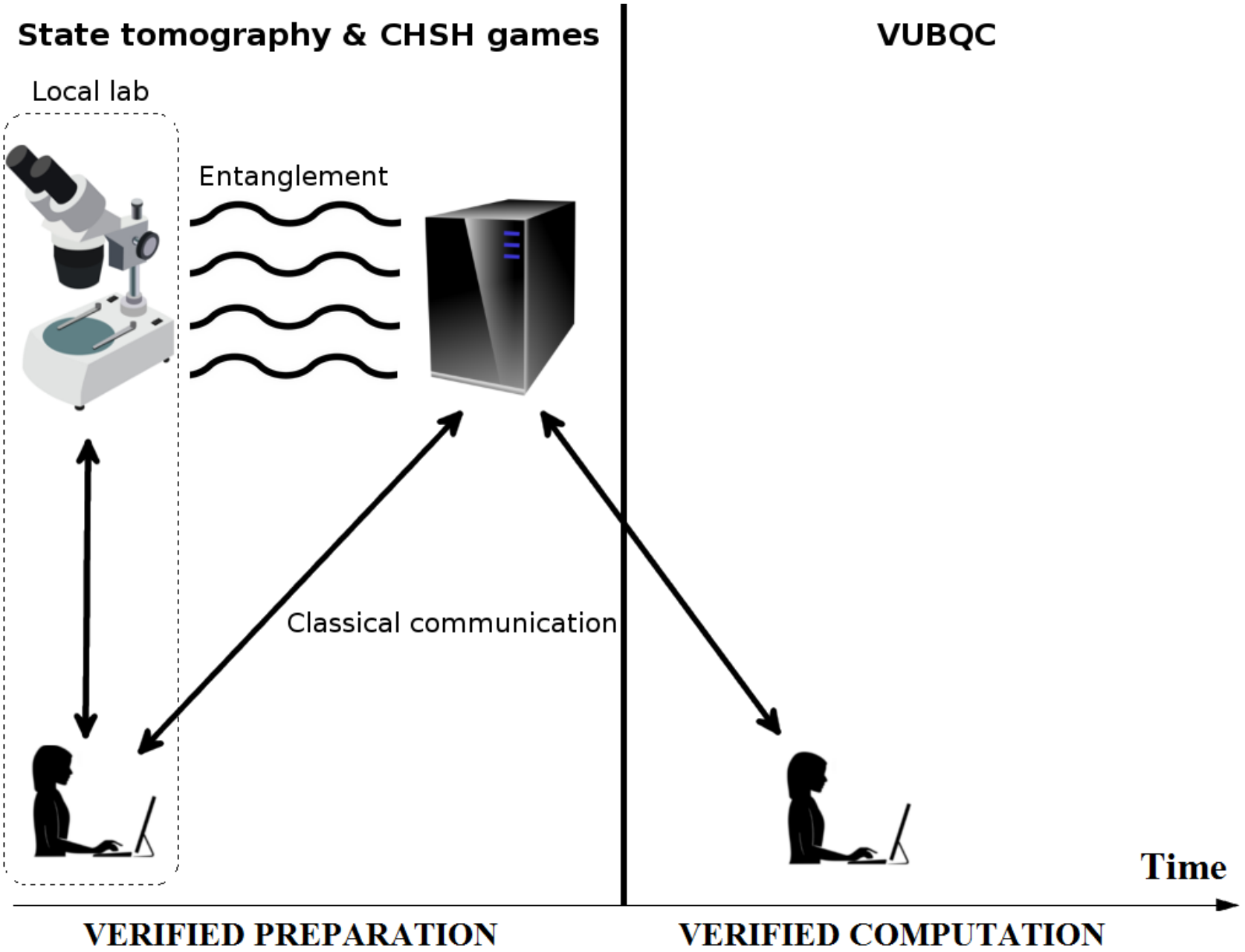
Device independence

Verifier and server share entanglement. Verifier has untrusted single qubit measurement device.

Similar to QKD and QRNG this leads to a trade-off:

- Increased overhead for number of rounds of interaction
- Assumption of no communication between measurement device and server

Device-independent VUBQC



Verified preparation

- Verifier plays CHSH games with measurement device and server
- CHSH measurements performed in different bases
- Verifier uses certain measurements to tomographically verify preparation states of the form ($\theta \in \{0, \pi/4, ...7\pi/4\}$):

$$|+_\theta\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\theta}|1\rangle)$$

- Server cannot distinguish between tomography and CHSH measurements (blindness)
- CHSH games used to test for tensor product of Bell pairs (rigidity)
- Tomography measurements used to test for correct preparation of $|+_\theta\rangle$ states
- Modified state tomography protocol from [*Reichardt, Unger, Vazirani '12*]

Verified preparation

- Verifier plays CHSH games with measurement device and server
- CHSH measurements performed in different bases
- Verifier uses certain measurements to tomographically verify preparation states of the form ($\theta \in \{0, \pi/4, ...7\pi/4\}$):

$$|+_\theta\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\theta}|1\rangle)$$

- Server cannot distinguish between tomography and CHSH measurements (blindness)
- CHSH games used to test for tensor product of Bell pairs (rigidity)
- Tomography measurements used to test for correct preparation of $|+_\theta\rangle$ states
- Modified state tomography protocol from [*Reichardt, Unger, Vazirani '12*]

Verifier certifies that server has correct set of single qubits

Verified computation

- Server entangles single qubits into a UBQC graph state
- Graph state is universal for quantum computation (MBQC computation)
- Preparation angles for $|+_\theta\rangle$ states are unknown to server (blindness)
- Verifier instructs server to measure qubits in graph state
- Server responds with measurement outcomes
- Previous 2 steps repeat until computation has been performed
- Certain qubits measured in the basis of preparation, to test honesty of server (trapification)
- Blindness $\implies$ server cannot distinguish between trap qubits and computation qubits

Verified computation

- Server entangles single qubits into a UBQC graph state
- Graph state is universal for quantum computation (MBQC computation)
- Preparation angles for $|+_\theta\rangle$ states are unknown to server (blindness)
- Verifier instructs server to measure qubits in graph state
- Server responds with measurement outcomes
- Previous 2 steps repeat until computation has been performed
- Certain qubits measured in the basis of preparation, to test honesty of server (trapification)
- Blindness $\Longrightarrow$ server cannot distinguish between trap qubits and computation qubits

Verifier certifies that server has performed the quantum computation correctly

Honest vs dishonest behaviour

In *verified preparation*, verifier accepts if statistics of tomography and CHSH are correct and rejects otherwise

In *verified computation*, verifier accepts if trap measurements are correct and rejects otherwise

Honest devices

Denote as $p(accept|honest)$ as the probability that the verifier accepts outcome of computation, given that the untrusted devices behave honestly.

Dishonest devices

Denote as $p(accept|dishonest)$ as the probability that the verifier accepts outcome of computation, given that the untrusted devices behave dishonestly.

Want: $p(accept|honest) \to 1$, $p(accept|dishonest) \to 0$

Verified computation

For verified computation (VUBQC) with *ideal quantum states*:

$$p(accept|honest) = 1$$

$$p(accept|dishonest) < exp^{-1}(d)$$

Verified computation

For verified computation (VUBQC) with *ideal quantum states*:

$$p(accept|honest) = 1$$
$$p(accept|dishonest) < exp^{-1}(d)$$

Certified approximate state

Verified preparation certifies that, if the verifier accepts, with high probability the state on the server's side is ϵ-close to the ideal state, denoted $|\Psi\rangle = \bigotimes |+_\theta\rangle$ (up to a local isometry).

Verified computation

For verified computation (VUBQC) with *ideal quantum states*:

$$p(accept|honest) = 1$$
$$p(accept|dishonest) < exp^{-1}(d)$$

Certified approximate state

Verified preparation certifies that, if the verifier accepts, with high probability the state on the server's side is ϵ-close to the ideal state, denoted $|\Psi\rangle = \bigotimes |+_\theta\rangle$ (up to a local isometry).

We show that VUBQC protocol is robust to deviations in $|\Psi\rangle$

Robustness of VUBQC

Given a state ρ such that $\|\rho - |\Psi\rangle\langle\Psi|\|_{Tr} \leq \epsilon$, the previously described VUBQC protocol will have: $p(accept|honest) > 1 - O(\epsilon)$ and $p(accept|dishonest) < exp^{-1}(d) + O(\sqrt{\epsilon})$

Verified computation

For verified computation (VUBQC) with *ideal quantum states*:

$$p(accept|honest) = 1$$
$$p(accept|dishonest) < exp^{-1}(d)$$

Certified approximate state

Verified preparation certifies that, if the verifier accepts, with high probability the state on the server's side is ϵ-close to the ideal state, denoted $|\Psi\rangle = \bigotimes |+_\theta\rangle$ (up to a local isometry).

We show that VUBQC protocol is robust to deviations in $|\Psi\rangle$

Robustness of VUBQC

Given a state ρ such that $\|\rho - |\Psi\rangle\langle\Psi|\|_{Tr} \leq \epsilon$, the previously described VUBQC protocol will have: $p(accept|honest) > 1 - O(\epsilon)$ and $p(accept|dishonest) < exp^{-1}(d) + O(\sqrt{\epsilon})$

Deviation is as general as possible

(can include correlation with external adversarial system)

Proof sketch:

Case I: Uncorrelated deviation

$$p(accept|dishonest) = max_j(\, Tr\,(\textstyle\sum_\nu p(\nu) P^{\nu}_{incorrect} B_j(\nu)))$$

$$B_j(\nu) = Tr_S \left(\sum_b |b + c_r\rangle \langle b| \, C_{\nu_C,b} \Omega P \overbrace{((\otimes^S |0\rangle \langle 0|) \otimes \underbrace{\rho^{\nu,b}}_{\text{Input state}})}^{\text{Joint system state } \sigma^{\nu,b}} P^\dagger \Omega^\dagger C^\dagger_{\nu_C,b} \, |b\rangle \langle b + c_r| \right)$$

$\underbrace{}_{\text{Server's qubits}}$

P is the honest run of the protocol. Ω is the server's deviation

$$\rho^{\nu,b} = Tr_E \left(U \left((\otimes^E |0\rangle \langle 0|) \otimes \underbrace{\left|\psi^{\nu,b}\right\rangle \left\langle\psi^{\nu,b}\right|}_{\text{Ideal input}} \right) U^\dagger \right)$$

Robustness of VUBQC

U characterizes the deviation of the input

U and Ω are uncorrelated

Can commute U with P and incorporate input deviation into server's deviation Ω, yielding Ω'

$$B_j(\nu) = Tr_{S+E}\left(\sum_b |b+c_r\rangle\langle b| C_{\nu_C,b}\Omega P U'((\otimes^{S+E}|0\rangle\langle 0|)\otimes|\Psi^{\nu,b}\rangle\langle\Psi^{\nu,b}|)U'^{\dagger}P^{\dagger}\Omega^{\dagger}C^{\dagger}_{\nu_C,b}|b\rangle\langle b+c_r|\right)$$

Becomes

$$B_j(\nu) = Tr_{S+E}\left(\sum_b |b+c_r\rangle\langle b| C_{\nu_C,b}\Omega' P((\otimes^{S+E}|0\rangle\langle 0|)\otimes|\Psi^{\nu,b}\rangle\langle\Psi^{\nu,b}|)P^{\dagger}\Omega'^{\dagger}C^{\dagger}_{\nu_C,b}|b\rangle\langle b+c_r|\right)$$

$\Omega' \propto \Omega$, and we are maximizing over all deviations $\Longrightarrow$ as if we had ideal input

$p(accept|dishonest)$ remains unchanged!

Robustness of VUBQC

$$p(accept|honest) = Tr\left(\sum_\nu p(\nu) P^\nu_{correct} B_0(\nu)\right)$$

$B_0(\nu)$ is the honest action of the server, given $|\Psi\rangle$

Denote $B'_0(\nu)$ as the honest action of the server, given ρ

Want to compute:
$$p'(accept|honest) = Tr\left(\sum_\nu p(\nu) P^\nu_{correct} B'_0(\nu)\right)$$

However:
$$|| \, |\Psi^\nu\rangle \langle\Psi^\nu| - \rho^\nu ||_{Tr} \leq \epsilon$$

By CPTP action and the triangle inequality it follows that:
$$|p(accept|honest) - p'(accept|honest)| \leq 2\epsilon$$

$p(accept|honest)$ changes by at most $O(\epsilon)$!

Case II: Correlated deviation

(can only occur for dishonest server)

Consider a joint (presumably entangled) state ρ_{AB}

Assume $\rho_A = Tr_B(\rho_{AB})$ is state used by VUBQC protocol

We have that $||\rho_A - |\Psi^\nu\rangle\langle\Psi^\nu|\,||_{Tr} \leq \epsilon$

ρ_A is correlated with another system, B

$$\rho_{corr} = \rho_{AB} - \rho_A \otimes \rho_B$$

Evolution of ρ_A under the action of the server:

$$\rho_A \to \mathcal{P}(\rho_A) + \delta\rho_A$$

$\mathcal{P}$ - CPTP map corresponding to uncorrelated action of the server

$\delta\rho_A$ - inhomogeneous term arising from initial correlations

Robustness of VUBQC

$$\rho_A \rightarrow \mathcal{P}(\rho_A) + \delta\rho_A$$

The uncorrelated term in the above expression leaves $p(accept|dishonest)$ unchanged, as previously shown

Therefore, we only need a bound for $\delta\rho_A$

$$\delta\rho_A = Tr_B(U_{AB}\rho_{corr}U_{AB}^{\dagger})$$

Using the gentle measurement lemma, we can show:
$$||\rho_{corr}||_{Tr} = ||\rho_{AB} - \rho_A \otimes \rho_B||_{Tr} \leq 2\sqrt{\epsilon} + 2\epsilon$$

Therefore:
$$||\delta\rho_A||_{Tr} \leq 2\sqrt{\epsilon} + 2\epsilon$$

$p(accept|dishonest)$ changes by at most $O(\sqrt{\epsilon})$!

Consequences

- We have proven security of our protocol for the *most adversarial setting*
- This includes security against *coherent and correlated attacks*
- Used only assumption of *no communication*
- Robustness result shows that VUBQC works with *imperfect input states*
- Previous work, [*Dunjko, Kashefi, Leverrier '12*], showed this only for blindness, not verification

Consequences

- We have proven security of our protocol for the *most adversarial setting*
- This includes security against *coherent and correlated attacks*
- Used only assumption of *no communication*
- Robustness result shows that VUBQC works with *imperfect input states*
- Previous work, [*Dunjko, Kashefi, Leverrier '12*], showed this only for blindness, not verification

We have also shown how to suppress errors in VUBQC using a fault tolerant construction

Fault tolerance

Fault tolerant VUBQC achieved by encoding computation in lattice code of [*Morimae, Fuji '12*] and using sequential repetition, with no asymptotic increase in communication between verifier and server.

Conclusions and future work

Results

- We have developed a device independent verification protocol for quantum device computation
- Our robustness result applies to existing VUBQC protocols
- We have also developed a fault tolerant version of VUBQC

Future directions

- Relativistic quantum verification (true no communication via space-like separation)
- Improving communication complexity and characterising types of correlations useful for verification
- Fully classical verifier verification with computational security

Thank you!

[New J. Phys. 17 (2015) 083040]