Entrapping Nature

Elham Kashefi

University of Edinburgh
UK Networked Quantum Information Technologies Hub
CNRS, Pierre and Marie Curie University
Paris Centre for Quantum Computing
Profile of a Quantum Person
Profile of a Quantum Person

Mathematics
Profile of a Quantum Person

Mathematics

Computer Science

Track A

Track B
Profile of a Quantum Person

Mathematics

Physics

Computer Science

Track A

Track B
Profile of a Quantum Person

Mathematics

Physics

Computer Science

Experiment

Track A

Track B
Profile of a Quantum Person

Mathematics

Physics

Industry

Computer Science

Experiment

Track A

Track B
Profile of a Quantum Person

Mathematics

Physics

Industry

Computer Science

Experiment

Engineering

Chemistry

Philosophy

Track A

Track B
Quantum Computing as the technology for simulating quantum systems
Quantum Computing as the technology for simulating quantum systems

Spectacular Progress

from complexity theory to cryptography
from simulation to sampling
from tomography to implementation
from foundation to interpretation
QSoft Vision of Quantum Technology

Hardware

Communication Network

Computing Device
QSoft Vision of Quantum Technology
QSoft Vision of Quantum Technology

Application

Secrecy

Speed

Interface

Verification/Benchmarking

Abstraction/Modeling/Encoding

Hardware

Communication Network

Computing Device
National Investments

Europe 1bn€
UK 270M £
Netherlands 80M $
China Billions !
US, Singapore, Canada

Quantum Era

Quantum Machines

Private Investments

Google, IBM, Intel, ATOS, Alibaba
Big VC founds
Startups Companies
Quantum Era

National Investments

Europe 1bn €
UK 270M £
Netherlands 80M $
China Billions !
US, Singapore, Canada

Private Investments
Google, IBM, Intel, ATOS, Alibaba
Big VC founds
Startups Companies
Quantum Era

National Investments

Europe 1bn €
UK 270M £
Netherlands 80M $
China Billions !
US, Singapore, Canada

Private Investments

Google, IBM, Intel, ATOS, Alibaba
Big VC founds
Startups Companies

Target: > 50 qubits Device
Quantum Era

National Investments

Europe 1bn €
UK 270M £
Netherlands 80M $
China Billions $

US, Singapore, Canada

Quantum Era

Private Investments

Google, IBM, Intel, ATOS, Alibaba
Big VC founds
Startups Companies

Target: > 50 qubits Device

Feature: Not simulatable classically
Quantum Era

National Investments

Europe 1bn €
UK 270M £
Netherlands 80M $
China Billions !
US, Singapore, Canada

Private Investments
Google, IBM, Intel, ATOS, Alibaba
Big VC founds
Startups Companies

Target: > 50 qubits Device
Feature: Not Simulatable Classically
Problem: Testing, Validation, BenchMarking, Certification, Verification …
Quantum Era

National Investments

- Europe 1bn €
- UK 270M £
- Netherlands 80M $
- China Billions !
- US, Singapore, Canada

Private Investments

- Google, IBM, Intel, ATOS, Alibaba
- Big VC founds Startups Companies

Moore's Law for Quantum Computers

**Target:** > 50 qubits Device

**Feature:** Not Simulatable Classically

**Problem:** Testing, Validation, BenchMarking, Certification, Verification …

Can we BOOTSTRAP a smaller quantum device to test a bigger one?
Quantum Verification

Efficient verification methods for realistic quantum devices
Quantum Verification

Efficient verification methods for realistic quantum devices

- Correctness of the outcome
- Operation monitoring
- Quantum property testing
Quantum Verification

- Efficient verification methods for realistic quantum devices
  - Correctness of the outcome
  - Operation monitoring
  - Quantum property testing
  - Architectural constraints
  - Experimental imperfections
Quantum Verification

Efficient verification methods for realistic quantum devices

- Correctness of the outcome
- Operation monitoring
- Quantum property testing

- Architectural constraints
- Experimental imperfections

Non-universal:
- D-Wave machine
- Quantum Simulator
- Current Q2020 architecture
Quantum Verification

Efficient verification methods for realistic quantum devices

- Correctness of the outcome
- Operation monitoring
- Quantum property testing

- Architectural constraints
- Experimental imperfections

Non-universal:
- D-Wave machine
- Quantum Simulator
- Current Q2020 architecture

Goal

Criteria to test emerging quantum devices
What is Verification
What is Verification

A mechanism that when witness is accepted the outcome is good
What is Verification

A mechanism that when witness is accepted the outcome is good

A mechanism that when witness is accepted the outcome is not bad
What is Verification

A mechanism that when witness is accepted the outcome is good.

A mechanism that when witness is accepted the outcome is **not bad**.

A mechanism that probability of witness is accepted and the outcome is **bad is bounded**.
What is Verification

A mechanism that prob of witness is acc and outcome is bad is bounded
A \textbf{mechanism} that the probability of witness is accurate and outcome is bad is bounded.
What is Verification

A mechanism that prob of witness is acc and outcome is bad is bounded random parameters.

Verifier \( \nu \) \[ \text{random parameters} \]

Prover/Device/Eve/Noise
What is Verification

A mechanism that prob of witness is acc and outcome is bad is bounded

Verifier \[\nu\]  Prover/Device/Eve/Noise

random parameters

\[B(\nu)\]

density operator of classical and quantum output
A **mechanism** that prob of witness is acc and outcome is bad is bounded.
What is Verification

 verifier  prover
 ν  ------------->  ∈  ←-  B(ν)

A mechanism that prob of witness is acc and outcome is bad is bounded
A mechanism that prob of \textbf{witness is acc and outcome is bad} is bounded

\[
P^\nu_{\text{incorrect}} := P_\bot \otimes |\text{acc}\rangle\langle\text{acc}| \]
A mechanism that prob of witness is acc and outcome is bad is bounded.
A mechanism that prob of witness is acc and outcome is bad is bounded

\[ \sum_{\nu} p(\nu) \text{Tr} (P_{\text{incorrect}}^\nu B(\nu)) \leq \epsilon \]
What is the challenge

A mechanism that prob of witness is acc and outcome is bad is bounded

\[ P_{\text{incorrect}}^\nu := P_\perp \otimes |\text{acc}\rangle \langle \text{acc}| \]

\[ \sum_\nu p(\nu) \text{Tr} (P_{\text{incorrect}}^\nu B(\nu)) \leq \epsilon \]
What is the challenge

A mechanism that **prob** of witness is acc and outcome is bad is **bounded**

\[
P^\nu_{\text{incorrect}} := P_{\perp} \otimes \ket{\text{acc}}\bra{\text{acc}}
\]

\[
\sum_{\nu} p(\nu) \Tr(P^\nu_{\text{incorrect}} B(\nu)) \leq \epsilon
\]
What is the challenge

A mechanism that **prob** of witness is acc and outcome is bad is bounded

\[
\sum_\nu p(\nu) \operatorname{Tr} \left( P^\nu_{\text{incorrect}} \otimes B(\nu) \right) \leq \epsilon
\]
How to deal with deviation

\[ \sum_{\nu} p(\nu) \text{Tr} (P_{\text{incorrect}}^\nu B(\nu)) \leq \epsilon \]
How to deal with deviation

\[ \sum_{\nu} p(\nu) \text{Tr} (P_{\text{incorrect}}^{\nu} B(\nu)) \leq \epsilon \]

Different toolkits / Different tasks / Different witness / Different properties / Different assumptions / …..
How to deal with deviation

\[
\sum_{\nu} p(\nu) \text{Tr} (P_{\text{incorrect}}^{\nu} B(\nu)) \leq \epsilon
\]

Different toolkits / Different tasks / Different witness / Different properties / Different assumptions / …..
Most General Deviation

\[ \Omega_{Eve,\text{system}} \]

Quantum Hiding
Most General Deviation

\[ \Omega_{\text{Eve,system}} \]

Quantum Hiding

\[ \sigma_{\text{testsubspace}} \]
Most General Deviation

$\Omega_{Eve,system}$

Quantum Hiding

$\sigma_{testsubspace}$

Practical Protocols with No assumptions whatsoever
Most General Deviation

\[ \Omega_{Eve,system} \]

Quantum Hiding

\[ \sigma_{test\text{subspace}} \]

Classically Impossible

Practical Protocols with No assumptions whatsoever
Entrapping Nature

Untrusted Quantum Theory

Falsifiable via

Trusted Quantum Measurement
Entrapping Nature

Untrusted Relativistic Quantum Theory

Falsifiable via

Trusted Wave Packet
Global Directions on Verification
Global Directions on Verification

via **Hiding**: Cloud-based     Crypto App     Distributed Network
Global Directions on Verification

via Hiding: Cloud-based Crypto App Distributed Network

FIG. 4: Schematic of a quantum computation with verification sub-routines.

Whereas the laws of physics have been tested in various limits—small or large scales, high or low energies—the boundary of high computational complexity is mostly unexplored. So, it is even imaginable that quantum mechanics might break down at some scale of complexity [22].

On the experimental side, current quantum computers [23] are limited to the processing of a few qubits, which does not allow yet to solve problems which are intractable using classical computers. In the future when large-scale quantum computers might be available [24–27], the verification of quantum computations and quantum simulations will be a crucial task [28].

Thus, our demonstration might have implications for new quantum computing experiments as well as on the foundations of quantum physics.

Add Caslav’s statement: In our implementation, we assume the correctness of quantum mechanics for the verification of quantum resources. Without this assumption, a full demonstration would require the two entangled photons to be sent far apart from each other in two distant laboratories of the prover where only in the very last instant of the computation the verifier gives the measurement instructions to the prover. By this means, no classical computers could mimic the output of the computation.

ACKNOWLEDGEMENTS

The authors are grateful to D. Aharonov and S. Aaronson for discussions. We acknowledge support from...
Global Directions on Verification

via Hiding: Cloud-based Crypto App Distributed Network

FIG. 4: Schematic of a quantum computation with verification sub-routines.

Whereas the laws of physics have been tested in various limits—small or large scales, high or low energies—the boundary of high computational complexity is mostly unexplored. So, it is even imaginable that quantum mechanics might break down at some scale of complexity [22].

On the experimental side, current quantum computers [23] are limited to the processing of a few qubits, which does not allow yet to solve problems which are intractable using classical computers. In the future when large-scale quantum computers might be available [24–27], the verification of quantum computations and quantum simulations will be a crucial task [28].

Thus, our demonstration might have implications for new quantum computing experiments as well as on the foundations of quantum physics.

Add Caslav's statement: In our implementation, we assume the correctness of quantum mechanics for the verification of quantum resources. Without this assumption, a full demonstration would require the two entangled photons to be sent far apart from each other in two distant laboratories of the prover where only in the very last instant of the computation the verifier gives the measurement instructions to the prover. By this means, no classical computers could mimic the output of the computation.

ACKNOWLEDGEMENTS

Please add Acknowledgements

The authors are grateful to D. Aharonov and S. Aaronson for discussions. We acknowledge support from...

AUTHOR CONTRIBUTION

S.B. designed and performed the experiments, acquired the experimental data, carried out theoretical calculations and the data analysis, and wrote the manuscript. E.K. and J.F. carried out theoretical calculations, contributed the proofs, and edited the manuscript. C.B. provided theoretical analysis and wrote the manuscript. P.W. edited the manuscript and supervised the project.


Global Directions on Verification

via Hiding: Cloud-based Crypto App Distributed Network
Global Directions on Verification

via **Hiding** : Cloud-based Crypto App Distributed Network

via **Proof System** : Quantum Simulation
Global Directions on Verification

via **Hiding** : Cloud-based Crypto App Distributed Network

via **Proof System** : Quantum Simulation

via **Hypothesis Testing** : Bench Marking Quantum Supremacy
Global Directions on Verification

via **Hiding** : Cloud-based Crypto App Distributed Network

- EPSRC UK
- NRF Singapore
- USAirforce
- EU QFlagship

via **Proof System** : Quantum Simulation

via **Hypothesis Testing** : Bench Marking Quantum Supremacy
Global Directions on Verification

via **Hiding**: Cloud-based Crypto App Distributed Network

- EPSRC UK
- NRF Singapore
- USAirforce
- EU QFlagship

via **Proof System**: Quantum Simulation

- Number Crunching
- Noise Handling
- Architecture Adaptation
- New Methods Development

via **Hypothesis Testing**: Bench Marking Quantum Supremacy
Verification Status
Verification Status

- It exists
- It is expanding

Trust Worthy Quantum Information TyQi17 Paris
Verification Status

- It exists
- It is expanding

Trust Worthy Quantum Information TyQi17 Paris

- The overhead depends on the level of trust

<table>
<thead>
<tr>
<th>Entanglement</th>
<th>Measurements</th>
<th>Trusted</th>
<th>Semi-trusted (i.i.d.)</th>
<th>Untrusted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trusted</td>
<td>$O(N)$</td>
<td>$O(N^4 \log N)$</td>
<td>$O(N^{13} \log(N))$</td>
<td></td>
</tr>
<tr>
<td>Untrusted</td>
<td>$O(N^4 \log N)$</td>
<td>$O(N^4 \log N)$</td>
<td>$O(N^{64})$</td>
<td></td>
</tr>
</tbody>
</table>
Verification Status

- It exists
- It is expanding

arXiv:1709.06984

Verification of quantum computation:
An overview of existing approaches

Alexandru Gheorghiu, Theodoros Kapourniotis, Elham Kashefi

<table>
<thead>
<tr>
<th>Entanglement</th>
<th>Measurements</th>
<th>Trusted</th>
<th>Semi-trusted (i.i.d.)</th>
<th>Untrusted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trusted</td>
<td>O(N)</td>
<td>O(N^4 logN)</td>
<td>O(N^{13} log(N))</td>
<td></td>
</tr>
<tr>
<td>Untrusted</td>
<td>O(N^4 logN)</td>
<td>O(N^4 logN)</td>
<td>O(N^{64})</td>
<td></td>
</tr>
</tbody>
</table>
Verification Challenge
Verfication Challenge

- uniform platform versus tailored made

Standardisation ??? Given the unknown nature of the emerging devices
Verification Challenge

- uniform platform versus tailored made

**Standardisation**

??? Given the unknown nature of the emerging devices

- Academic versus Industry’s need

??? Objective improvements
Quantum Era

Target: > 50 qubits Device

Feature: Noisy Qubits

Problem: What are they useful for

Do we need to wait till error correcting codes became feasible
Classical - Quantum Collaboration Landscape

Efficient Certification

Cyber Security

Quantum Tech

Enhanced-Security
Protocols for hybrid classical-quantum communication network

- Electronic voting
- Fingerprinting
- Digital currency
- Secure cloud
- Blockchain
- Secure multi-party computing
Protocols for hybrid classical-quantum communication network

- Electronic voting
- Fingerprinting
- Digital currency
- Secure cloud
- Blockchain
- Secure multi-party computing

- Practical Security Analysis
Quantum Cryptography

Protocols for hybrid classical-quantum communication network

- Electronic voting
- Fingerprinting
- Digital currency
- Secure cloud
- Blockchain
- Secure multi-party computing

- Standard telecom technology
- Long distance
- Long term stability
- Silicon-integrated
- Small scale devices

- Practical Security Analysis
Quantum Crypto Status
Quantum Crypto Status

- It exists
- It is expanding

Quantum Cryptography QCrypt17 Cambridge
Quantum Crypto Status

- It exists
- It is expanding

Quantum Cryptography QCrypt17 Cambridge

- Quantum Protocols for Quantum Webs
  - Q Fingerprinting
  - Q Money
  - Q Secure cloud
  - Q Byzantine Agreement
  - Q Secure multi-party computing
Quantum Crypto Status

- It exists
- It is expanding

Quantum Cryptography QCrypt17 Cambridge

- Quantum Protocols for Quantum Webs
  - Q Fingerprinting
  - Q Money
  - Q Secure cloud
  - Q Byzantine Agreement
  - Q Secure multi-party computing

They need few qubits …. works with noisy one too
Quantum Crypto Challenge
Quantum Crypto Challenge

How to exploit them for Classical Web?
Quantum Crypto Challenge

How to exploit them for Classical Web?

- Academic versus Industry’s need

Objective improvements
Quantum Crypto Challenge

How to exploit them for Classical Web?

- Academic versus Industry’s need

Objective improvements

Performances / Cost / Added values
First large-scale practical experiment with SMPC to implement a secure auction.

Recently: Efficient (low communication) computational SMPC

Computation represented by a series of additions and multiplications of elements in $F_p$.

Linear Verifiable Secret Sharing
Other collaborators

**Theory**
- Damian Markham (LIP6)
- Joe Fitzsimons (SUTD)
- Anna Pappa (UCL)
- Anne Broadbent (Ottawa)
- Vedran Dunjko (Innsbruck)
- Anthony Leverrier (INREA)
- Animesh Datta (Warwick)
- Theodoros Kapourniotis (Warwick)

**Experiment**
- Stefanie Barz (Vienna, Oxford)
- Philip Walther (Vienna)
- Ian Walmsley (Oxford)
Other collaborators

**Theory**
- Damian Markham (LIP6)
- Joe Fitzsimons (SUTD)
- Anna Pappa (UCL)
- Anne Broadbent (Ottawa)
- Vedran Dunjko (Innsbruck)
- Anthony Leverrier (INREA)
- Animesh Datta (Warwick)
- Theodoros Kapourniotis (Warwick)

**Experiment**
- Stefanie Barz (Vienna, Oxford)
- Philip Walther (Vienna)
- Ian Walmsley (Oxford)
A girl simple dream
A girl simple dream

Quantum Devices
The base unit of MUSIQC is a collection of $N$ trapped atomic ion qubits, where $N$ registers are coupled to photonic quantum channels, and through a reconfigurable optical crossconnect. This architecture features two elements: (a) The elementary logic unit (ELU) consists of a register of $N$ elementary logic units (ELU) with local interactions, called the Elementary Logic Unit (ELU). Quantum logic operations within the ELU are ideally fast and deterministic, with error rates sufficiently small that fault-tolerant error correction is possible. Fault-tolerant error correction even in the face of probabilistic interconnects, and how such a quantum network can support fault-tolerant error correction within an ELU is possible. While we focus our discussions on quantum registers and quantum processors regardless of their relative location. Finally, we prove that this architecture is applicable to other qubit platforms that feature strong optical transitions, such as quantum dots, neutral atoms, or nitrogen-vacancy (NV) color centers in diamond. There are many known protocols for phonon-based gates between trapped atomic ion qubits, and here we summarize the main points relevant to the quantum harmonic motion. Such phonons can be used to entangle quantum logic gates mediated through the collective phonon mode, and then onto other qubits for dependent optical or microwave dipole forces. There is the Lamb Dicke parameter, where entangling operations with characteristic speed and dependent forces on one or more ions, affecting entangling quantum logic gates between qubits, is the Lamb Dicke parameter, $\lambda = \frac{\hbar}{m \omega}$, where $m$ is the mass of the ion, $\omega$ is the frequency of harmonic oscillation of the ions, and $\hbar$ is Planck’s constant. In this way, qubits can be mapped onto phonon states and then onto other qubits for dependent forces on one or more ions, affecting entangling quantum logic gates between qubits.
A girl simple dream

Global Verifiable Secure Quantum Web