



# Interactive Proofs For Quantum Computations

Dorit Aharonov, Michael Ben-Or, Elad Eban

School of Computer Science and Engineering  
The Hebrew University of Jerusalem

## 1 The Strength of Quantum Mechanics is (also) a Weakness

According to the modern Church-Turing thesis any reasonable physical system can be simulated efficiently by a probabilistic Turing machine

In Physics predictions and experimental results are compared

Theory Experiment

$$F=ma \iff \text{Image of a person pushing a cart}$$

$$E=mc^2 \iff \text{Image of a glowing light bulb}$$

$$|\phi\rangle = \sum_{m=0}^{\infty} U_m |0\dots 0\rangle \iff \text{Image of a quantum circuit diagram}$$

Quantum Computation is interesting since we think it violates the modern Church Turing thesis because we believe BPP=BQP, and that BQP can be realized physically.

Following these beliefs, it is impossible to compute predictions for quantum experiments!

## 2 Motivating Questions

- Testing the Borders of Quantum Mechanics: Karl Popper: a scientific physical theory must be falsifiable. Is QM a falsifiable theory? [Vazirani'07]. Is it possible to test QM "outside of BPP"?
- The Experimental Aspect: How can one verify that a physical system is indeed a quantum computer?
- Cryptographic-Commercial: Is it possible to trust the outcome of a company that sells quantum CPU time? How can we check that a system we want to buy is indeed a quantum computer?

## 4 Using Interaction

### Interactive proofs (GMR85)

A protocol between a BPP verifier (V) and a computationally unbounded prover (P) such that:

- For all  $x \in L$ :  $\Pr(V \text{ accepts}) > 2/3$
- For all  $x \notin L$ :  $\Pr(V \text{ rejects}) > 2/3$

### Interactive View of Shor's Algorithm

For  $N=xy, x \leq y$  decide whether  $x_1=1$

- P sends  $x, y: x \leq y \ \& \ xy=N$ .
- V accepts if  $xy=N \ \& \ x_1=1$

### Quantum Prover Interactive Proof (QPIP)

- In QPIP:
- The prover (P) is computationally restricted to BQP.
  - The verifier (V) is a hybrid quantum-classical machine: A BPP machine + O(1) qubits.
  - Quantum and classical communication channels.

## 7 A Simple Quantum Authentication Scheme

Intuitively, in error detection codes we want to detect a given set of errors (say, all errors on  $\leq d$  qubits), with certainty. In contrast, in QAS we would like to detect any error with high probability

### The Clifford QAS

Alice prepares  $|\phi\rangle(0^{\otimes d})$ , and applies a random  $U \in C_{m+d}$ . The Clifford group on  $m+d$  qubits. Bob applies  $U^{-1}$  and measures the last  $d$  qubits. Declares the state valid only if they are all  $|0\rangle$ . Abort otherwise.

### Proof Idea

Eve's operator  $O$  is translated by the random Clifford to the following operator:

$$\rho \rightarrow s\rho + (1-s) \sum_{P \in I} P\rho P^{-1}$$

a uniform mixture of Paulis. Bob detects an error unless  $P$  is the identity on the last  $d$  qubits. The probability for this bad event is  $2^{-d}$

## 10 Signed Quantum Reed-Solomon Error Detection Codes

### A) [BCGHS'06] introduced the signed quantum RS code $C_k$

$$|S_k^{\pm}\rangle = \frac{1}{\sqrt{q}} \sum_{f \in \mathbb{F}_q[x]} |k, f(\alpha_1), \dots, k, f(\alpha_m)\rangle$$

$k_i \in \{-1, +1\}$

When  $m=2d+1$ , it detects  $d$  errors.

### B) Logical operations

$$\bar{X} = X^{\otimes d} \otimes X^{\otimes d} \otimes X^{\otimes d}$$
$$\bar{Z} = Z^{\otimes d} \otimes Z^{\otimes d} \otimes Z^{\otimes d}$$

C-NOT, Fourier and measurement in the computational basis, are performed transversally, independently of  $k$ .

### C) The Signed RS QAS

Alice Picks a random  $k$ , encodes the message using  $C_k$ , and then applies a random Pauli  $P$  to the resulting state. Bob applies  $P^{-1}$  and checks whether the message is in  $C_k$ .

### D) Proof sketch

The random Pauli transforms any attack by Eve to a (not necessarily uniform) mixture of Pauli operators. Pauli operators are detected with high probability over  $k$ .

## 5 Results

### Theorems:

- There exists a QPIP for Q-CIRCUIT.  $\rightarrow$  BQP=QPIP.
- Q-CIRCUIT has a fault tolerant QPIP protocol: computation and communication are subject to noise.
- Q-CIRCUIT has a blind QPIP protocol.

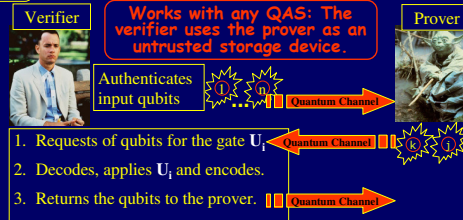
### Q-CIRCUIT:

Input: a quantum circuit gates:  $U=U_T \dots U_1$

Output: distinguish between:

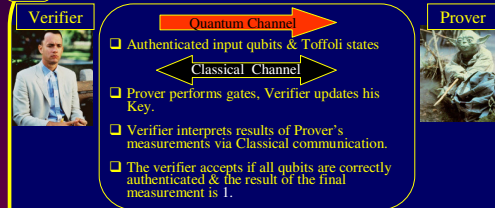
A blind protocols is one where the prover gains no information about the function being computed or the input.

## 8 Simple QPIP Protocol



The verifier accepts if all qubits are correctly authenticated & the result of the final measurement is 1. Making the protocol blind: Verifier asks for all pairs of qubits.

## 11 Polynomial Based QPIP Protocol



Fault tolerance: we adapt standard techniques to the QPIP protocol. Care is due since the verifier needs to prepare authenticated states sequentially, due to lack of space.

Making the computation of  $U|x\rangle$  blind: we use a universal circuit  $Q$ , which on input  $|U^{-1}|x\rangle$  outputs  $|U^{-1}U|x\rangle$

## 3 Shor's Answer is Not Sufficient

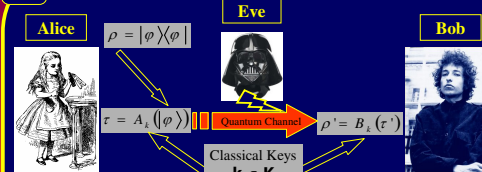
### The Answer

- Shor's algorithm can be run on a large number  $N$ , the answer can be easily verified.
- Verification rather than prediction.
- Assuming factoring is intractable this is the first test of QM outside of BPP.
- This works for any problem in NP/BQP

### The Problems

- Probably BQP  $\not\subseteq$  NP. So this reasoning will not work for all problems in BQP.
- Probably factorization is not BQP complete (log depth quantum circuit). Can we verify the evaluation of Jones poly?
- 100 bit numbers can be factorized on a PC  $\rightarrow$  Shor's algorithm cannot be used to test a 100 qubit quantum computer.

## 6 Quantum Authentication (QAS)



A QAS is a pair of quantum algorithms  $A$  and  $B$  together with a set of classical keys  $K$  such that:  $A$  encodes an input in the message space  $A_k: H \rightarrow M$ .  $B$  decodes and checks validity  $B_k: M \rightarrow H \otimes V$

A QAS is  $\epsilon$  secure if  $\forall |\phi\rangle$ :  
 Completeness:  $\forall k \in K$ :  
 $B_k A_k(\rho) = |\phi\rangle\langle\phi| \otimes |\text{VAL}\rangle\langle\text{VAL}|$   
 Soundness: For any adversary operator  $O$ , set:  $\rho' = |k\rangle\langle k| \sum_{B, O A_k(\rho)}$   
 Then:  
 $\text{Tr}(|(I - |\phi\rangle\langle\phi|) \otimes |\text{VAL}\rangle\langle\text{VAL}| \rho') \leq \epsilon$

## 9 Fault Tolerant QPIP

- To be physically realizable, the QPIP must work in the presence of noise.
- Fault tolerant quantum computation schemes encode each qubit by a poly-log number of qubits. If we allow the verifier a quantum memory of poly-log qubits, we can add fault tolerant techniques to the simple QPIP protocol.
- However, when keeping the verifier's quantum memory constant, we do not know how to make the scheme fault tolerant.

### Motivation for a new QPIP protocol

- Handle noise with a constant quantum size verifier.
- Reduce quantum communication.
- Transfer the bulk of quantum computation to the prover.

We need the prover to be able to apply gates, without knowing the authentication code!

## 12 Open Questions

- Can we achieve this with a completely classical verifier? (Find a protocol or prove impossibility result)
- And what if we allow two provers? (Preliminary results [Broadbent et al.] show this with entangled provers.)

## 13 Related Work

- Secure assisted quantum computation. A.M. Childs [Chi01]. Large quantum memory, blind, not secure against malicious server.
- Blind quantum computation. P. Arrighi and L. Salvai [AS06]. Publicly verifiable function, secure against individual attacks.
- Independently: Universal blind quantum computation. A. Broadbent, J. Fitzsimons, E. Kashefi [BFK08]. Similar results motivated by blind computation. Verifier's memory is of one qubit!