Bar-Ilan University
אוניברסיטת בר-אילן
BIU
Center for Research in Applied Cryptography and Cyber Security

The 11th BIU Winter School on Cryptography in a Quantum World

February 14-17, 2021

Thomas Vidick
California Institute of Technology

Delegation of quantum computations

Thomas Vidick, Caltech

Part I: *Delegation with a quantum verifier*

Problem statement: Delegated Quantum Computation (DQC)

Outline

1. Information-theoretic delegation with a small quantum verifier
   (a) Blindness: the quantum one-time pad
   (b) Verifiability: Clifford authentication

2. Information-theoretic delegation with two provers
   (a) Testing entanglement
   (b) Two-prover delegation in the circuit model
   (c) Two-prover delegation in the Hamiltonian model

3. Computationally secure delegation with a classical verifier
   (a) Classically committing to a qubit
   (b) The Mahadev protocol

Definition (Blindness)**.** *A DQC protocol $\mathcal{P}_{AB}$ provides* ε-blindness *if for all adversarial behaviors $\{\mathcal{F}_i\}$ there exists a CPTP map $\mathcal{F} : \mathcal{L}(\mathcal{H}_B) \to \mathcal{L}(\mathcal{H}_B)$ such that*

$$\mathrm{Tr}_A \circ \mathcal{P}_{AB} \approx_\varepsilon \mathcal{F} \circ \mathrm{Tr}_A \ .$$

The Childs protocol for blind DQC

Transversal gates

Definition (Clifford)**.** *A one- or two-qubit gate C is* Clifford *if for every Pauli P, there is a Pauli P' such that $CP = P'C$.*

The T gate $\quad T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$

Definition (Verifiability)**.** *A DQC protocol* $\mathcal{P}_{AB}$ *provides* ε-verifiability *if for all adversarial behaviors* $\{\mathcal{F}_i\}$ *and all initial states* $\psi_{AR_1} \otimes \psi_{R_2B}$ *there is a* $0 \leq p_\psi \leq 1$ *such that*

$$\rho^{\psi}_{AR_1} \approx_\varepsilon p_\psi (\mathcal{U} \otimes \mathrm{Id}_{R_1})(\psi_{AR_1}) + (1 - p_\psi)|err\rangle\langle err| \otimes \psi_{R_1} .$$

Authentication

Definition (Authentication scheme)**.** *A quantum authentication scheme (QAS) from ℓ to $m = \ell + e$ qubits with security ε is specified by two families of unitaries $\mathcal{E} = \{E_k\}$ and $\mathcal{D} = \{D_k\}$ together with a set of classical keys $\mathcal{K}$ such that:*

1. *(Completeness:) For all $k \in \mathcal{K}$ and all $|\psi\rangle$,*

$$D_k\big(E_k\big(|\psi\rangle\langle\psi| \otimes |0^e\rangle\langle 0^e|\big)E_k^\dagger\big)D_k^\dagger \;=\; |\psi\rangle\langle\psi| \otimes |0^e\rangle\langle 0^e| \;.$$

2. *(Soundness:) For any $|\psi\rangle$ let*

$$\Pi \;=\; |\psi\rangle\langle\psi| \otimes \mathrm{Id} + (\mathrm{Id} - |\psi\rangle\langle\psi|) \otimes (\mathrm{Id} - |0^e\rangle\langle 0^e|) \;.$$

Then for any CPTP map $\mathcal{F}$, if

$$\sigma \;=\; \frac{1}{|\mathcal{K}|}\sum_k D_k\big(\mathcal{F}\big(\,E_k(|\psi\rangle\langle\psi| \otimes |0^e\rangle\langle 0^e|)E_k^\dagger\,\big)\big)D_k^\dagger$$

then

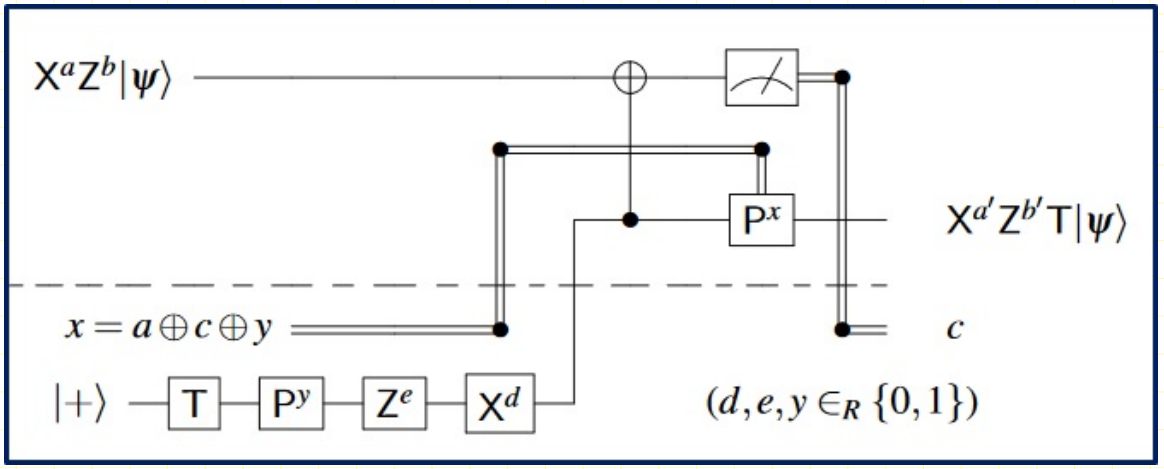
$$\mathrm{Tr}\big(\Pi\,\sigma\big) \;\geq\; 1 - \varepsilon \;.$$

Verifiable delegation

- Childs protocol can be modified by adding authentication.
  Provides verifiability at the cost of $O(\log(1/\varepsilon))$-qubit (Clifford) quantum computer for verifier.

- Clifford authentication allows transversal application of Pauli gates.
  Polynomial-code authentication allows transversal application of Clifford gates.

- Non-Clifford gates require magic states + classical communication.



- [ABOE'08,ABOEM'18] ε-blind and verifiable protocol with $O(\log(1/\varepsilon))$-qubit verifier, one-way quantum communication and two-way classical communication.

- [BFK'09,FK'16] $O(1)$-qubit verifier, measurement-based model of quantum computing.

The Clifford authentication scheme

- Key k species Clifford circuit E_k on $(e+1)$ qubits.
- $D_k = E_k$: $|\psi\rangle|0^e\rangle \mapsto E_k(|\psi\rangle|0^e\rangle)$.

Lemma (Pauli twirl)**.** *For any m-qubit $P \neq P'$, and density ρ on $m+m'$ qubits,*

$$\frac{1}{4^m} \sum_{Q \in \mathcal{P}_m} \left(Q^\dagger P' Q \otimes \mathrm{Id}\right) \rho \left(Q^\dagger P Q \otimes \mathrm{Id}\right) = 0 \,.$$

Lemma (Pauli twirl)**.** *For any m-qubit $P \neq P'$, and density ρ on $m + m'$ qubits,*

$$\frac{1}{4^m} \sum_{Q \in \mathcal{P}_m} \left(Q^\dagger P' Q \otimes \mathrm{Id}\right) \rho \left(Q^\dagger P Q \otimes \mathrm{Id}\right) = 0 \,.$$

Let $\mathcal{F}(\cdot) = U \cdot U^\dagger$, for some $U = \sum_P \alpha_P P$

The Pauli twirl reduces any attack to a *non-uniform* mixture of Pauli attacks.

Lemma (Clifford decoherence)**.** *Let ρ be a density on $m + m'$ qubits. Let $U = \sum_{P \in \mathcal{P}_m} P \otimes U_P$ be arbitrary. Then*

$$\frac{1}{|\mathcal{C}_m|} \sum_{C \in \mathcal{C}_m} \left((C \otimes \mathrm{Id})^\dagger U (C \otimes \mathrm{Id})\right) \rho \left((C \otimes \mathrm{Id})^\dagger U^\dagger (C \otimes \mathrm{Id})\right)$$

$$= (I \otimes U_I)\, \rho\, (I \otimes U_I)^\dagger + \frac{1}{4^m - 1} \sum_{P,Q \in \mathcal{P}_m \setminus \{\mathrm{Id}\}} (P \otimes U_Q)\, \rho\, (P \otimes U_Q)\,.$$

Summary

- Computation on encrypted data.

  No code allows universal transversal gate set: magic states and communication.

- Perfect information-theoretic blindness.

  ε-verifiability with $O(\log(1/\varepsilon))$ blow-up in computation size/communication.

- Additional models: measurement-based, post-hoc.

Open questions

- Fault-tolerance: can errors at the verifier side be exploited by the prover?

- Protocols for sub-universal classes of circuits, e.g. IQP circuits.

- Verification for sampling problems?

- Reduce classical communication/computation of the verifier.

200
180
160
140
120
100
80
60
40
mm
40
60
80
100
120
140
160
180
200
220
240
260