Title: Higher-Order Blind Quantum Computation

Speakers: Thomas Vinet

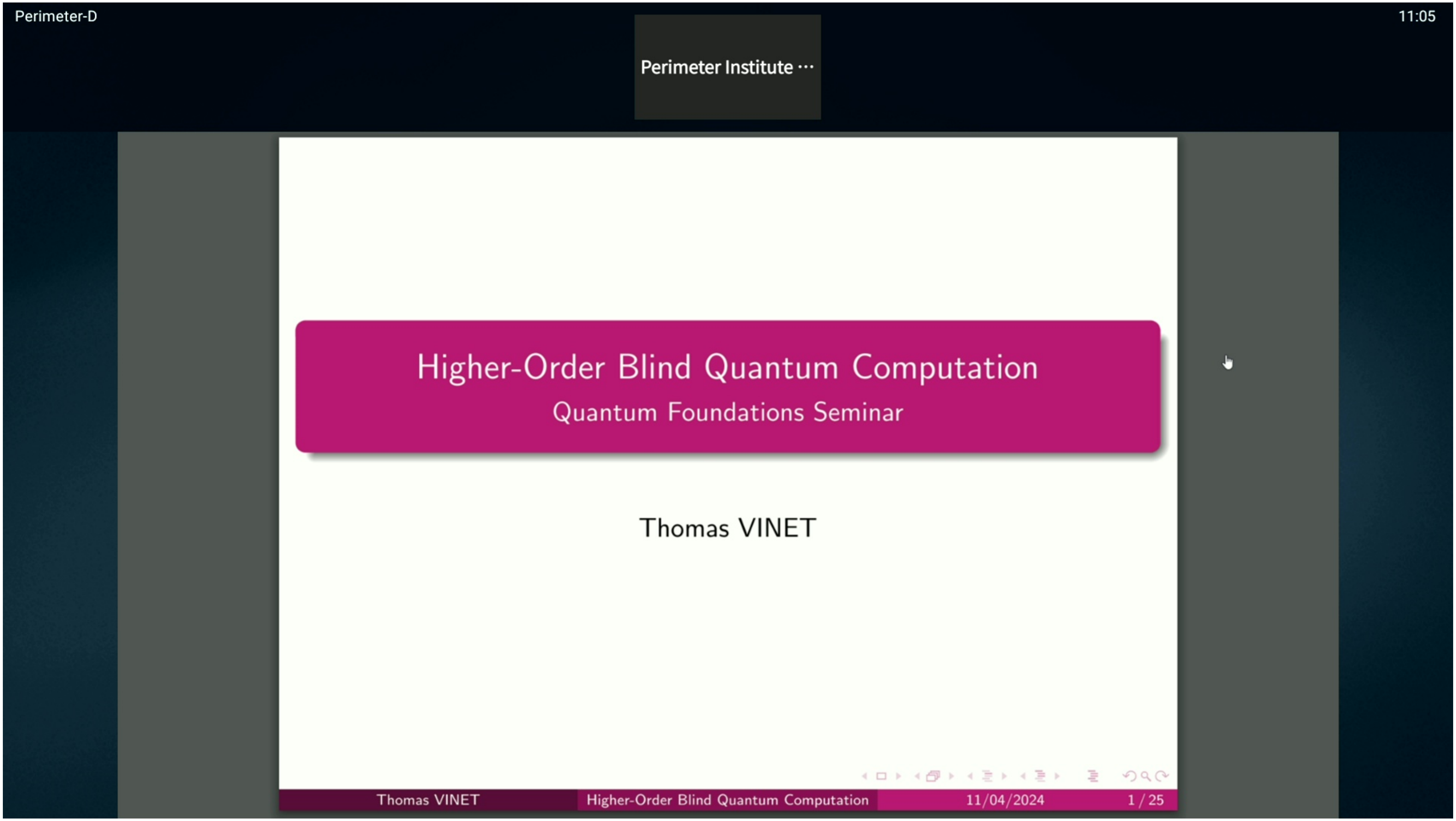
Series: Quantum Foundations

Date: April 11, 2024 - 11:00 AM

URL: https://pirsa.org/24040083

Abstract: In the near future, where only a small number of companies and institutions will have access to large-scale quantum computers, it is essential that clients are able to delegate their computations in a secure way, without their data being accessible by the server. The field of blind quantum computation has emerged in recent years to address this issue, however, the majority of work on this topic has so far been restricted to the secure computation of sequences of quantum gates acting on a quantum state. Yet, a client capable of performing quantum subroutines may want to conceal not only their quantum states but also the subroutines they perform themselves. In this work, we introduce a framework of higher-order blind quantum computation, where a client performs a quantum subroutine (for example a unitary gate), which is transformed in a functional way by a server with more powerful quantum capabilities (described by a higher-order transformation), without the server learning about the details of the subroutine performed. As an example, we show how the DQC1 algorithm for estimating the trace of a unitary gate can be implemented securely by a server given only an (extended) black-box description of the unitary gate. Finally, we extend the framework to the case where the details of the server's algorithm are also concealed from the client.

Zoom link


Perimeter-D
11:05
Perimeter Institute ···
Higher-Order Blind Quantum Computation
Quantum Foundations Seminar
Thomas VINET
Thomas VINET
Higher-Order Blind Quantum Computation
11/04/2024
1 / 25

Perimeter-D 11:05

Perimeter Institute ···

Table of contents

1. Introduction
2. Blind Quantum Computation
   - One Time Pad
   - Secure Assisted Quantum Computation
   - Universal Blind Quantum Computation
3. Higher-Order Blind Quantum Computation
   - Situation 1: Client's knowledge
   - Situation 2: Server's knowledge
     - Commuting matrices with unitaries
     - OTP - Depolarizing Channels
     - Protocol

Perimeter-D 11:06

Perimeter Institute ···

Introduction

- In the future: few people will be able to do big computations
- Framework to help client gain advantage of this power
- Security of data

Perimeter Instit

Table of contents

1. Introduction
2. Blind Quantum Computation
   - One Time Pad
   - Secure Assisted Quantum Computation
   - Universal Blind Quantum Computation
3. Higher-Order Blind Quantum Computation
   - Situation 1: Client's knowledge
   - Situation 2: Server's knowledge
     - Commuting matrices with unitaries
     - OTP - Depolarizing Channels
     - Protocol

Perimeter-D 11:09

Perimeter Institute ···

One Time Pad

Blind Quantum Computation

- Encode data, completely random for the attacker
- Classical one time pad: $x, y : x \oplus y$
- Quantum OTP: quantum state ρ, applies either $\mathbb{1}, X, Y, Z$
- $\frac{1}{4}(\rho + X\rho X + Y\rho Y + Z\rho Z) = \frac{\mathbb{1}}{2}$: maximally mixed state
- Complete depolarizing channel

Perimeter-D 11:10

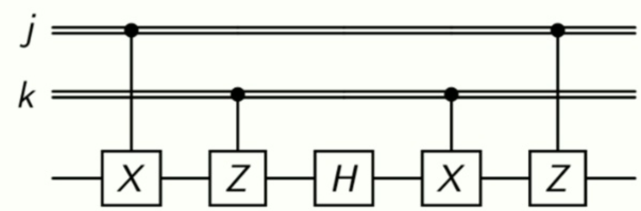
Perimeter Institute ···

Secure Assisted Quantum Computation

Blind Quantum Computation

- Gate is known, decomposition in the universal set of gates $\{H, T, CNOT\}$[1]
- Alice sends her qubits while applying first X, Z gates randomly

Figure: Example for H



[1] Childs,

Perimeter-D 11:13

Perimeter Institute ···

Universal Blind Quantum Computation

Blind Quantum Computation

- UBQC[2]: Gates also secure
- Use of Measurement Based Quantum Computation
- Graph state
- Alice prepares qubits, sends them to Bob
- Measurement angles are randomized
- One Time Pad on inputs: in the processus

[2] Broadbent, Fitzsimons, and Kashefi, "Universal Blind Quantum Computation".

Perimeter-D 11:14

Perimeter Institute ···

Blind Quantum Computation

- Papers written few years ago
- All assume a low compute power from the client
- Can we give the client more power to do more transformations ?

Table of contents

1 Introduction

2 Blind Quantum Computation
- One Time Pad
- Secure Assisted Quantum Computation
- Universal Blind Quantum Computation

3 Higher-Order Blind Quantum Computation
- Situation 1: Client's knowledge
- Situation 2: Server's knowledge
  - Commuting matrices with unitaries
  - OTP - Depolarizing Channels
  - Protocol

Higher-Order Blind Quantum Computation

- Alice has a quantum description of $|\psi\rangle$ and U
- Can compute simple and known gates on n qubits
- Wants to have access to a higher-order transformation on more qubits
- Example: $C(U)$ for DQC1

Situation 1: Client's knowledge

Higher-Order Blind Quantum Computation

- Alice has knowledge of the supermap decomposition

Situation 1: Client's knowledge

Higher-Order Blind Quantum Computation

- Alice has knowledge of the supermap decomposition
- Knows the unitaries V, W
- Use of a server that can compute unitaries (UBQC, Childs)
- Multiple rounds of communication
- Security kept with one-time pads

Perimeter Institute ···

Situation 2: Server's knowledge

Higher-Order Blind Quantum Computation

- Alice wants to compute some non-linear map $f(U)$
- Alice has a classical description of this map
- Bob has a supermap description $S(U, U, ...) = f(U)$
- Alice wants to keep her state and gate private
- Bob wants to leak as less information as possible about his implementation of S

Perimeter-D 11:26

Perimeter Institute ···

Situation 2: Server's knowledge

Higher-Order Blind Quantum Computation

- No information on Bob's implementation
- Still multiple communication rounds
- Idea: find OTPs for Alice that commute with the unitaries, while keeping Bob's security

Perimeter-D 11:28

Perimeter Institute ···

Commuting matrices with unitaries

Situation 2: Server's knowledge - Higher-Order Blind Quantum Computation

- $U = P^\dagger DP$, we want to find unitaries M such that $UM = MU$
- $[U, M] = 0 \iff [D, PMP^\dagger] = 0$
- $D = \mathrm{diag}(\lambda_i)$, then $DM = MD \iff \forall i, j, \lambda_i = \lambda_j$ or $m_{ij} = 0$
- In the basis P, M is block diagonal
- Size of blocks: mutiplicities of eigenvalues
- Pseudo commuting matrices: $UM = \alpha MU, \alpha \in \mathbb{U}$
- Stronger conditions, and still a block matrix at the end

Commuting matrices with unitaries

Situation 2: Server's knowledge - Higher-Order Blind Quantum Computation

- M commuting with U, then $PMP^\dagger$ is block diagonal
- If all eigenvalues of U are of multiplicity 1, then $M = P^\dagger D' P$
- On a OTP point of view: Alice has M, can find P
- We need multiplicities to be at least 2: we can randomize the basis $P(\bigoplus N_i)$

Perimeter-D 11:30

Perimeter Institute ···

Commuting matrices with unitaries

Situation 2: Server's knowledge - Higher-Order Blind Quantum Computation

Lemma (4x4 decomposition)

Let D a 4×4 diagonal matrix with non-zero determinant. We denote diagonal matrices as $D = \text{diag}(\alpha, \beta, \gamma, \delta)$. Then we can find $a, b, c, d, e, f \in \mathbb{C}$ such that:

$$D = \mathrm{diag}(a, a, b, b)\mathrm{diag}(c, d, c, d)\mathrm{diag}(e, f, f, e).$$

We denote those matrices $\Lambda^{(i)}(D), i \in 1, 2, 3$.

Perimeter-D 11:33

Perimeter Institute ···

Commuting matrices with unitaries

Situation 2: Server's knowledge - Higher-Order Blind Quantum Computation

Proposition

Let U be a unitary matrix of size $4n$, and its diagonal decomposition $U = P^\dagger DP$. We can therefore write $D = \oplus_{i=1}^{n} D_i$. Then we can write $U = U^{(1)}U^{(2)}U^{(3)}$, with $U^{(j)} = P^\dagger(\oplus_{i=1}^{n}\Lambda^{(j)}(D_i))P$.

Proposition

Let U be a unitary of size $n, n \geq 4$. Then we can find $n-1$ matrices $U_{i1\leq i<n}$ all diagonal in the same basis as U with 2 eigenvalues of multiplicity at least 2 such that $U = \prod_i^{n-1} U_i$

OTP - Depolarizing Channels

Situation 2: Server's knowledge - Higher-Order Blind Quantum Computation

- Global form of commuting matrices
- Alice chooses one randomly from a set of commuting matrices
- Need to form a depolarizing channel

OTP - Depolarizing Channels

Situation 2: Server's knowledge - Higher-Order Blind Quantum Computation

- Kraus operators for a depolarizing channel on qudits: $K_{ij} = \frac{1}{\sqrt{d}} |i\rangle\langle j|$
- We want Kraus operators that are unitaries
- Relation between Kraus operators represented by an unitary
- Need d^2 unitaries that are two-by-two orthogonal under Frobenius norm
- Sylvester's generalized matrices: $\sigma_{kj} = \sum_{m=0}^{d-1} \omega^{jm} |m+j\rangle\langle m| , \omega = e^{\frac{2i\pi}{d}}$
- $K^d = \{\sigma_{kj}^{\dagger} | k, j \in 0, ..., d-1\}$
- CPTP map: we need another thing to have a mixed state
- Quasi-Depolarizing Channel: $I_{n,m} = \mathrm{diag}(\underbrace{\frac{1}{2n}, ..., \frac{1}{2n}}_{n}, \underbrace{\frac{1}{2m}, ..., \frac{1}{2m}}_{m})$

Perimeter-D 11:39

Perimeter Institute ···

OTP - Depolarizing Channels

Situation 2: Server's knowledge - Higher-Order Blind Quantum Computation

Proposition

Let D be a diagonal matrix of size $m+n$, with 2 eigenvalues of multiplicity m and n. Let $\rho = \begin{pmatrix} AB \\ CD \end{pmatrix}$ a density matrix of size $m+n$. We denote $x = Tr(A)$. Then $K_{x,i,j} = U_{x,n}K_i^n \oplus U_{-x,m}K_j^m$ are Kraus Operators of the quasi depolarizing channel of size $n+m$, with $K_j^m, K_i^n \in K^n, K_m^j \in K^m$, and $U_{a,b} = \mathrm{diag}(e^{i\pi a}, 1, ..., 1)$ a diagonal matrix of size b

Perimeter Institute ···

OTP - Depolarizing Channels

Situation 2: Server's knowledge - Higher-Order Blind Quantum Computation

- From a different point of view than Alice's :

$$\Phi_{n,m}(\rho) = \int_{x=0}^{1} \frac{1}{n^2 m^2} \sum_{K_i \in K^n, K_j \in K^m} (U_{x,n} K_i^n \oplus U_{-x,m} K_j^m) \rho (U_{x,n} K_i^n \oplus U_{-x,m} K_j^m)$$

- Diagonal blocks: Depolarizing channel of size n and m
- Off-diagonal blocks:

$$\sum_{K_i \in K^n} K_i = \begin{pmatrix} 1 \dots 1 \\ 0 \dots 0 \\ \vdots \quad \vdots \\ 0 \dots 0 \end{pmatrix}, \int_{x=0}^{1} e^{2i\pi x} dx = 0$$

Protocol

Situation 2: Server's knowledge - Higher-Order Blind Quantum Computation

- Bob has a gate $U = P^\dagger D P$ of size n
- $U = \prod_{i=1}^{n-1} U_i$, where $U_i = P^\dagger D_i P$, $D_i = \lambda_i I_{k_i} \oplus \gamma_i I_{n-k_i}$
- Alice has a state ρ
- For each round $i \in 1, ..., n-1$:
  - Bob chooses two random unitaries N, M of size k_i and $n - k_i$ and sends to Alice through a classical channel $\mathcal{B} = P(N \oplus M)$
  - Alice randomly picks a gate A $\in K^{k_i}$ and B $\in K^{n-k_i}$. She computes $x = Tr_{k_i}(\rho)$ as the trace of the upper block of size $k_i \times k_i$ of ρ. She then applies $E_i = \mathcal{B}^\dagger(U_{x,k_i} A \oplus U_{-x,n-k_i} B)\mathcal{B}$, with the help of a third party (BQC) and sends her qubits to Bob
  - Bob applies U_i and sends back the qubits
  - Alice applies E^{-1}

Perimeter-D 11:44

Perimeter Institute ···

Conclusion

- Framework with quasi optimal security of both parties
- Need a protocol to ensure Alice is following the protocol
- Better decomposition of Kraus operators ?
- Security in more sophisticated transformations (use of multiple copies)

Perimeter-D 11:46

Perimeter Institute ···

Conclusion

Thanks for your attention !