Towards a complexity theory for non-local quantum computation

Andreas Bluhm— Univ. Grenoble Alpes, CNRS, Grenoble INP, LIG

Joint work with Simon Höfer, Alex May, Mikka Stasiuk, Philip Verduyn Lunel, and Henry Yuen

Aachen, July 10, 2025

Motivation: Quantum position-verification

Introduction

CNN World

World / Asia

Finance worker pays out $25 million after video call with deepfake ‘chief financial officer’

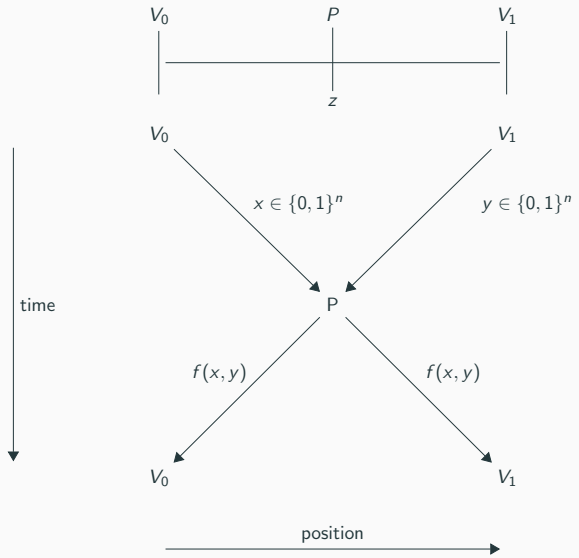
By Heather Chen and Kathleen Magramo, CNN

2 minute read · Published 2:31 AM EST, Sun February 4, 2024

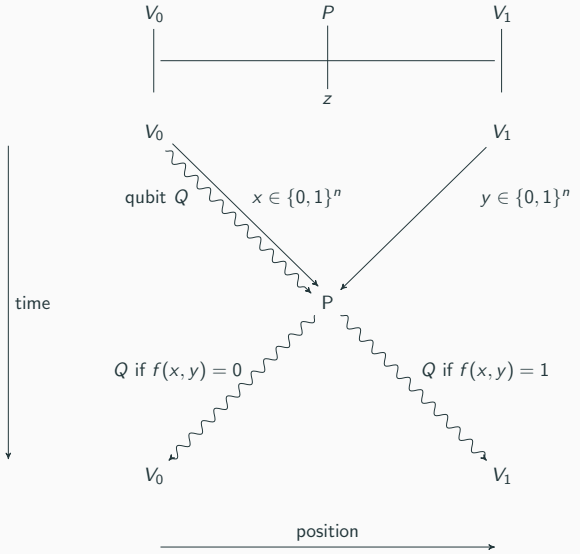
- How can such scams be foiled?
- Idea: Verify the location of the alleged chief financial officer!
- Position-based cryptography: Use position as credential

Classical protocols

- Special relativity: Information cannot travel faster than the speed of light
- Distance bounding: Send questions, accept if answers arrive fast enough
- Collaborating attackers can copy questions to break any classical protocol $\Longrightarrow$ need for quantum protocols

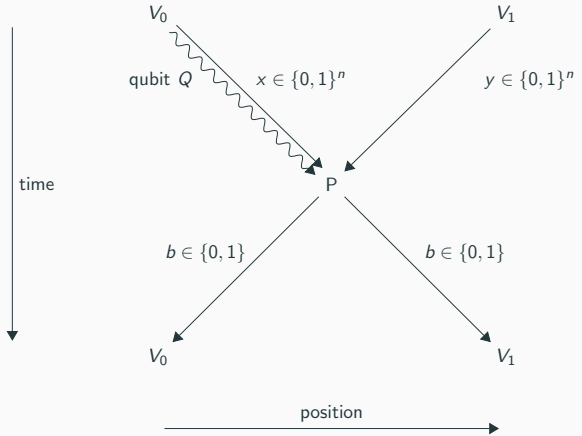


f-route protocol



- Protocol goes back to *Kent et al.* [KMS11]
- Verifiers prepare entangled pair $|\Omega\rangle$
- Send one qubit Q of it and keep the other
- At the end of the protocol: Bell measurement

f-measure protocol



- Protocol resembles [BK11]
- Verifiers prepare Q randomly as $|0\rangle$ or $|1\rangle$, apply Hadamard gate if $f(x, y) = 1$
- Prover measures in basis specified by $f(x, y)$, sends back outcome b
- Verifiers check consistency of b with the Q they sent

Comparing the two protocols

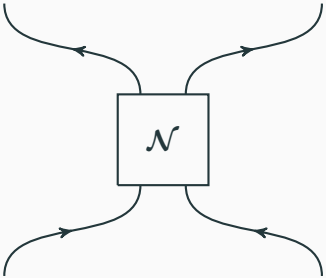
- Both protocols use a classical Boolean function f and a single qubit
- For both protocols, it can be proven that attackers need to control $\Omega(n)$ qubits to attack successfully [BCS22]
- The proofs are very similar in both cases
- [ABMSVL24] proves upper bounds of $O(2^{\sqrt{n \log n}})$ EPR pairs on f-route, but not on f-measure (teleportation attack in [BK11] gives upper bound of $O(2^n)$)
- f-measure is still secure if quantum information travels slowly and thus fits current technology better (qubits transmitted using fiber optics)

Are f-measure and f-route equally secure?

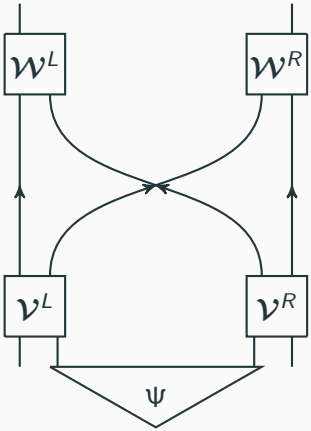
Tasks in non-local quantum computation

Non-local quantum computation

What we would like to implement:



What we can implement:



$\mathcal{N}$, $\mathcal{V}^L$, $\mathcal{V}^R$, $\mathcal{W}^L$, $\mathcal{W}^R$ are quantum channels and Ψ is the resource state.

Coherent NLQC tasks

f-route and f-measure are incoherent in the sense that x and y must be classical.

What about coherent versions? Some examples:

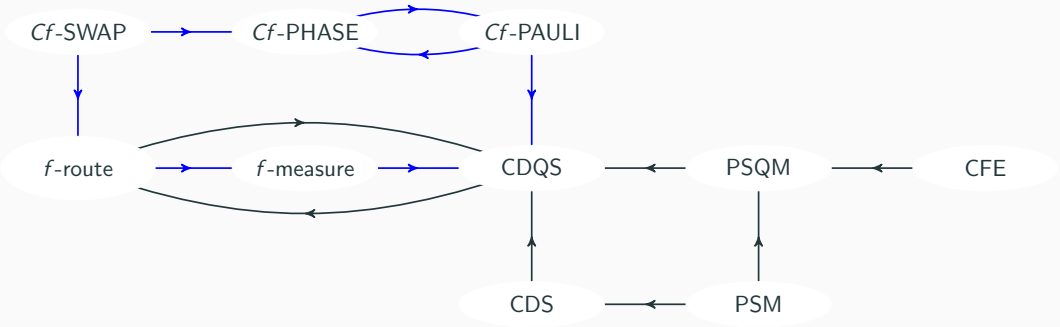
$$Cf\text{-SWAP}_{AA'BB'} = \sum_{x,y} \text{SWAP}_{A'B'}^{f(x,y)} \otimes |x\rangle\langle x|_A \otimes |y\rangle\langle y|_B$$

$$Cf\text{-PHASE}_{AA'BB'} = \sum_{x,y} (-1)^{f(x,y)} \; |x\rangle\langle x|_A \otimes |y\rangle\langle y|_B$$

$$Cf\text{-}\mathbf{Z}_{AA'BB'} = \sum_{x,y} \mathbf{Z}_{A'}^{f(x,y)} \otimes |x\rangle\langle x|_A \otimes |y\rangle\langle y|_B \, .$$

In particular, if you can do $Cf\text{-SWAP}_{AA'BB'}$, then you can do f-route.

Old and new reductions



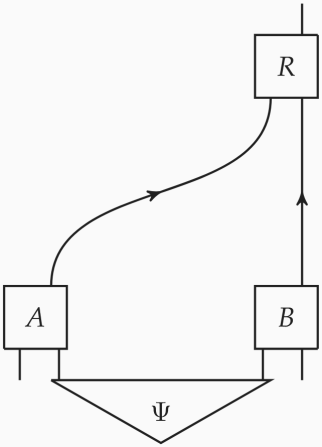
CD(Q)S: Conditional disclosure of (quantum) secrets

PS(Q)M: Private simultaneous (quantum) message passing

CFE: Coherent function evaluation

Blue arrows are new, black ones are from [ABMSVL24].

Conditional disclosure of quantum secrets



A and B share a resource state Ψ and send quantum messages to a referee R.

- A and B receive n-bit strings x, y, respectively
- A has an additional classical bit s, the secret
- A and B cannot communicate with each other, only send messages to the referee
- R should learn s if and only if $f(x, y) = 1$

f-measure to CDQS (1/2): Hiding information

- Consider a purified version of f-measure in which the verifiers do not produce $H^{f(x,y)}|b\rangle$ for a random bit b, but prepare an EPR pair $|\Omega\rangle_{QR}$, keep half of it, and measure it in the $H^{f(x,y)}$-basis in the end. Let W be the classical random variable after measuring R
- The aim of the verifiers is to guess the outcome of this measurement
- Let $\rho_{RAB}^{(x,y)}$ the state after the attackers have send their messages. To answer successfully, the state must fulfill $H(W|A)_{\rho_{WAB}^{(x,y)}} \leq \varepsilon$
- Using an entropic uncertainty relation, with $\sigma_{WAB}^{(x,y)}$ arising from $\rho_{RAB}^{(x,y)}$ by measuring in the $(f \oplus 1)(x,y)$-basis:

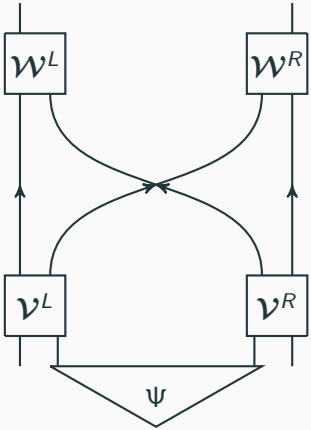
$$H(W|A)_{\rho_{WAB}^{(x,y)}} + H(W|B)_{\sigma_{WAB}^{(x,y)}} \geq 1$$

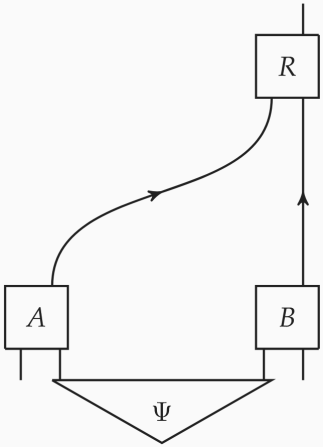
- Thus, to successfully attack, in the first round the attackers must have already destroyed the information necessary to win the protocol for $f \oplus 1$

f-measure to CDQS (2/2): Constructing an NLQC protocol

- Aim: We want to convert a strategy for f-measure into one for CDQS
- Prepare a uniformly random bit r and prepare $|\varphi\rangle = H|r\rangle$
- Run the first round of f-measure and
  1. have Alice send to the referee the system she would usually send to Bob
  2. have Bob send to the referee the system he would usually keep

Pictorial representation





f-measure to CDQS (2/2): Constructing an NLQC protocol

- Aim: We want to convert a strategy for f-measure into one for CDQS
- Prepare a uniformly random bit r and prepare $|\varphi\rangle = H|r\rangle$
- Run the first round of f-measure and
  1. have Alice send to the referee the system she would usually send to Bob
  2. have Bob send to the referee the system he would usually keep
- Alice sends $s \oplus r$ as well
- The honest referee performs the actions Bob would perform in the second round for f-measure
- If $f(x, y) = 1$, the referee can recover r (and thus s) since we are playing a valid strategy for f-measure
- If $f(x, y) = 0$, the actions of Alice and Bob before sending to the referee have destroyed the information needed to recover r and s stays hidden from the referee

Why "a complexity theory for NLQC"?

What's the bigger plan?

- Entanglement cost in certain NLQC tasks can be upper bounded by complexity measures $\implies$ lower bounds on entanglement imply lower bounds on complexity, notoriously hard
- Lower bounds on entanglement cost for f-route give lower bounds on memory size and span program size to compute f. For functions in P, even super-linear lower bounds are open
- Alternative question: *When is one computation harder to do non-locally than another?*
- Strategy like for complexity classes and reductions among computational problems
- Goal: Identify the hardest NLQCs, which are useful candidates for position-based cryptography

Summary

- f-measure and f-route are important protocols for QPV
- We have shown that they are equally hard
- First subexponential upper bounds for f-measure
- More reductions between NLQC tasks, also coherent ones

Some open questions:

- Show impossibility of reductions, for example from incoherent to coherent tasks
- Are all incoherent tasks equally hard?
- Find more links to other areas of quantum information and (quantum) cryptography

References

[ABMSVL24]: R. Allerstorfer, H. Buhrman, A. May, F. Speelman, P. Verduyn Lunel. Relating non-local quantum computation to information theoretic cryptography. *Quantum* 8:1387, 2024.

[BCS22]: AB, M. Christandl, and F. Speelman. A single-qubit position verification protocol that is secure against multi-qubit attacks. *Nature Physics*, 18(6):623–626, 2022.

[BK11]: S. Beigi and R. König. Simplified instantaneous non-local quantum computation with applications to position-based cryptography. *New Journal of Physics*, 13(9):093036, 2011.

Our paper: