Quantum Communication with coherent states: Realizing communication and information complexity advantages of quantum communication

Juan Miguel Arrazola, Markos Karasamanis,
Dave Touchette, Ben Lovitz,
Norbert Lütkenhaus

Institute for Quantum Computing

University of Waterloo

CryptoWorks21 NSERC CRSNG ARL Industry Canada Industrie Canada Canada

Quantum Communication

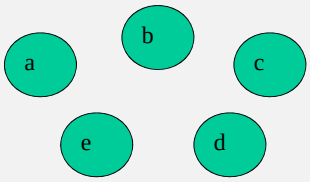
using quantum effects in quantum communication

- qualitative advantage
  measurement back-reaction on signal
  ➔ quantum key distribution (cannot be achieved classically)

- quantitative advantage
  use fewer resources to accomplish a goal
  leak less information to participants (towards secure multi-party computation)

Information & Communication complexity Complexity

multi-party computation



- given input: a,b,c,d,e …
- evaluate z= f(a,b,c,d,e …)

Communication Complexity:
How much information (bits, qubits) needs to be exchanged to evaluate function?

Information Complexity: (secure multi-party computation, information leakage)
How much does each party learn about the input of the others?

Quantum Communication can offer better performance than classical communication

Why would one care about secure multi-party computation?

Talking to non-quantum cryptographers:

- there are algorithms to do secure multi-party computations
  (Note: ➔ they are based on computational assumptions!)
- they are hardly used, as they are computational intensive, and may require lots of two-way communication (latency!)

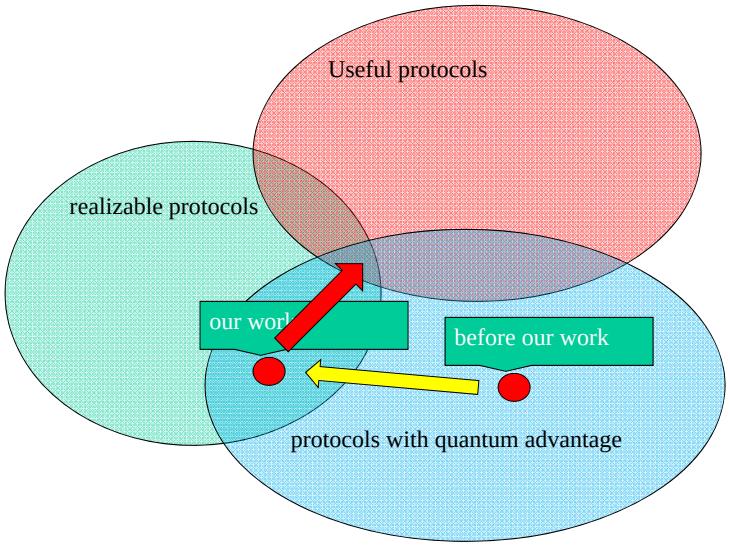
Anecdotally:
Google and Amazon use it to evaluate correlation between clicking and spending
➔ not time critical

Use case:

privacy issues: ***(Privacy by Design)***
air lines (passenger list) ←➔ government (no-fly lists)

reduced exposure risk
decision making at central node based on distributed input
(financial, military), so that breach
of central node does can not leak knowledge of contributing nodes

Expectation Management



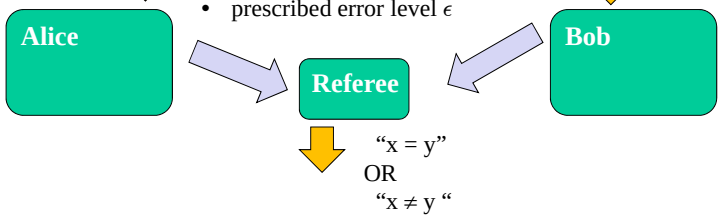
[Buhrman, Cleve, Watrous, de Wolf, PRL 87, 167902 (2001)]

Task Description: Finger Printing

(simultaneous message passing)

$\mathbf{x} \in \{0,1\}^n$ $\qquad$ $\mathbf{y} \in \{0,1\}^n$

- one way communication only
- no shared source of randomness
- prescribed error level ϵ



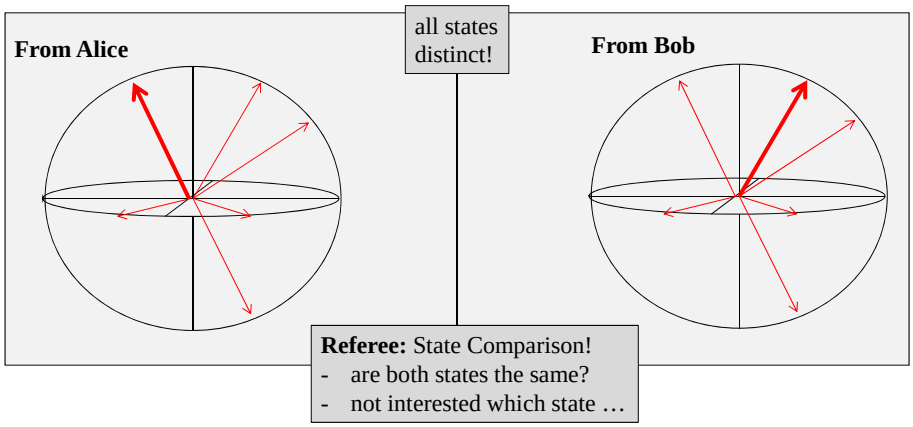
"x = y"
OR
"x ≠ y "

Two **different** question:
- how much information need to be transmitted to solve the task? (Communication complexity)
- how much does the referee learn about the input? (information complexity)

Exponential Gap between classical and quantum
classical $O(\sqrt{n})$
quantum $O(\log_2 n)$

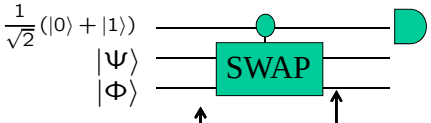
Mechanism for Quantum Finger Printing

protocol encodes 2^n states in a n dimensional Hilbert space!
➔ highly non-orthogonal states!



C-SWAP Test

Tool to give information about two states being in the same state or not …



measurement in basis $\frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$

$$Prob(" + ") = \frac{1}{2}\left(1 + |\langle\Phi|\Psi\rangle|^2\right)$$

$$Prob(" - ") = \frac{1}{2}\left(1 - |\langle\Phi|\Psi\rangle|^2\right)$$

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\ |\Psi\rangle\,|\Phi\rangle$$

$$\frac{1}{\sqrt{2}}(|0\rangle\ |\Psi\rangle\,|\Phi\rangle + |1\rangle\ |\Phi\rangle\ |\Psi\rangle)$$

	Equal input	Unequal input
'same' (+)	1	$\left[\frac{1}{2}\left(1 + \lvert\langle\Phi\lvert\Psi\rangle\rvert^2\right)\right]^n$
'different' (-)	0	$1 - \left[\frac{1}{2}\left(1 + \lvert\langle\Phi\lvert\Psi\rangle\rvert^2\right)\right]^n$

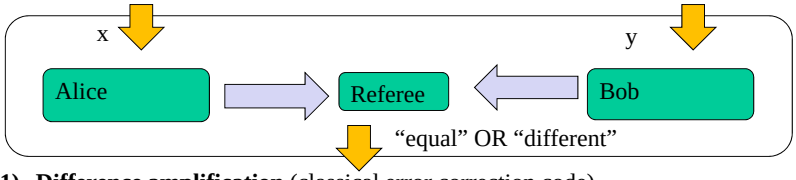
➔ 0 for $n \to \infty$

If n repetitions allowed
➔ can quickly reduce

➔ 1for $n \to \infty$

Quantum Finger Printing Protocol

[Buhrman, Cleve, Watrous, de Wolf, PRL 87, 167902 (2001)]



1) Difference amplification (classical error correction code)

x → E(x)

n bits → m > n bits

Hamming weight d(E(x), E(x')) > (1-δ) m

(we will later on use m = 3 n and δ = 0.92)

→ one bit difference

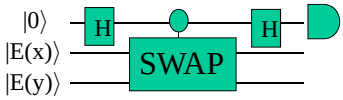
→ 8% error difference

2) Alice, Bob: **Quantum encoding**

$$E(x) \to |E(x)\rangle := \frac{1}{\sqrt{m}} \sum_{i=1}^{m} (-1)^{E(x)_i} |i\rangle$$

 # qubits: log m

3) Referee: **Conditional-SWAP test**



	Equal input	Unequal input
'same'	1	< ½(1+δ^2)
'different'	0	> ½(1-δ^2)

4) k-fold repetition to reduce errors < ϵ [require repetition: k = O(log 1/ϵ)]

Optical encodings

protocol states:

$$x \to |E(x)\rangle := \frac{1}{\sqrt{m}} \sum_{i=1}^{m} (-1)^{E(x)_i} |i\rangle$$

1) Qubits |i⟩: representation as state of log(

Polarization encoding

each qubit corresponds to a single p

→ need to generate log(m) highly e

First optical implementation:

[Horn et al, PRL 95, 150502 (2005)]

[Trojek et al, PRA 72 050305 (R)(2005)]

- aims at reducing error, not at reducin communication
- not scalable to large input

2) Qudits |i⟩: representation one out of m levels of a single quantum system

a) Orbital Angular Momentum of Light

b) multi-rail encoding

each quantum system represented by single photon in on out of m optical modes (e.g time bin, spatial modes …)

3) Optical Modes:

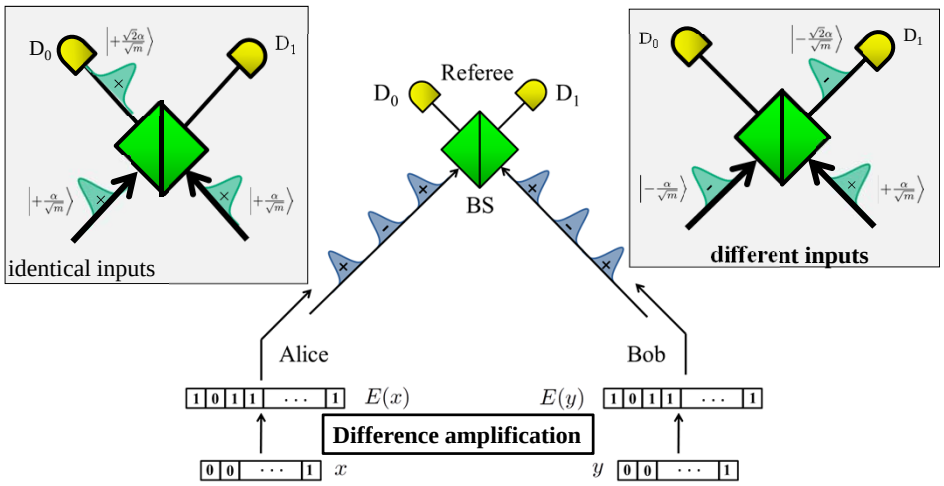
choose laser pulses (coherent states)

$$|\alpha\rangle_x = \bigotimes_{i=1}^{m} \left| (-1)^{E(x)_i} \frac{\alpha}{\sqrt{m}} \right\rangle_i$$

[S. Massar, Phys. Rev. A 71, 012310 (2005) laser pulses as single-photon approximation]

Coherent-state Protocol

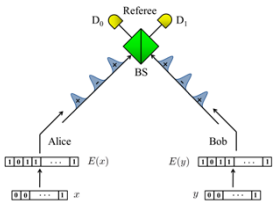
[Arrazola and Lütkenhaus, Phys. Rev A 89, 062305 (2014)]



overall identical inputs: only detector D_0 clicks
some differences: some D_0 clicks, some D_1 clicks

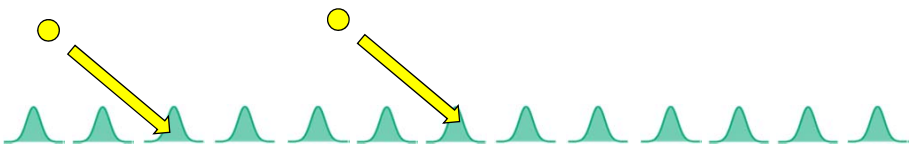
occurrence of D_1 detector clicks
➔ "overall different"
➔ else: "overall identical"

Resource counting



overall mean photon number $|\alpha|^2$
➔ sufficiently large
such that at least one click if difference exists
➔ sufficiently low
so that utilized Hilbert space is small

<u>Observation for ideal devices:</u>
total number of photons N independent of length m!



1 photon in m modes ➔ dimension Hilbert space m, ➔ ***log m*** qubits
N photons in m modes ➔ dim is $\binom{N+m-1}{m-1} \approx m^N$ ➔ ***O(N log m)*** qubits

Communication and Information Complexity Performance

Communication Complexity **[JMA, NL, Phys. Rev A 90, 042335 (2014)]**

classical:

best known protocol $\sim 32\sqrt{n}$

[Ambainis, Algorithmica 16, 298 (1996)]

bound on performance: $\sim 1.4\sqrt{n}$

[Guan, Zhang, Pan et al, Phys. Rev. Lett. 116, 240502 (2016)]

Our quantum implementation: number of pulses: n
Dimension: $O(\log_2 n)$

number of photons in the channel dramatically decreased

- reduced cross-talk in fiber
- fewer detection clicks expected

➔ faster clock rates???

does not require time resolution in detector!
Accumulation of photons would just be fine
➔ allows higher clock rate

Information Complexity **[Arrazola, Touchette, arXiv:1607.07516]**

classical:

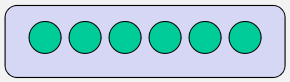
bound on performance: $\sim 0.2\sqrt{n}$

Our quantum implementation: $O(\log_2 n)$

Trade-off entanglement vs. #signals

- **original quantum finger printing protocol:**

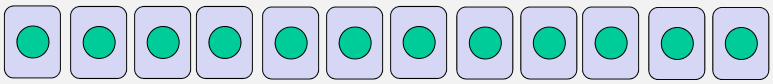
O(log n) highly entangled qubits



one signal of dim n
(plus repetition)

- **our optical protocol:**

equivalent to n separable qubits (two coherent states span a qubit!)



n signals of dimension 2, highly non-orthogonal

➔ same scaling of effective Hilbert space dimension and information leakage!
➔ non-orthogonality is a powerful tool

Experimental realities

loss between sources and referee?

- ➔ simply increase mean photon number to compensate loss
- ➔ does not affect scaling of resources!

dark count in detectors?

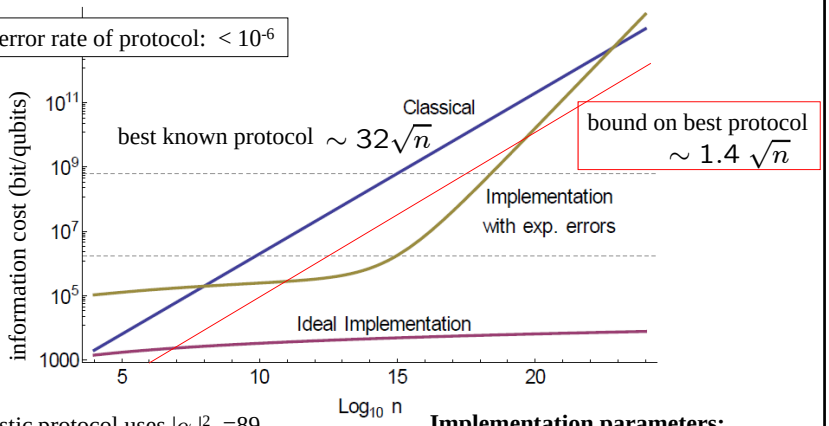
- ➔ set optimal threshold scheme to decide 'overall identical' or 'overall different'
- ➔ will affect scaling for larger input size states:need to maintain signal/noise ratio

mode matching on beam splitter?

- ➔ uses again optimal threshold scheme to discriminate 'identical/different'
- ➔ does not affect scaling, as errors are proportional to signal

Communication complexity: Simulation optical system example of combined effects

target error rate of protocol: $< 10^{-6}$



- ➔ idealistic protocol uses $|\alpha|^2$ =89
- ➔ realistic protocol uses $|\alpha|^2$ = 6651
  - ➔ starting at n = 10^{13} one needs to increase $|\alpha|^2$ to balance increasing dark count effects

Implementation parameters:

error amplification δ = 0.92 [m = 3 n]

η = 0.1 ➔ **90% loss!!**

dark count probability $d_B = 4 \times 10^{-9}$

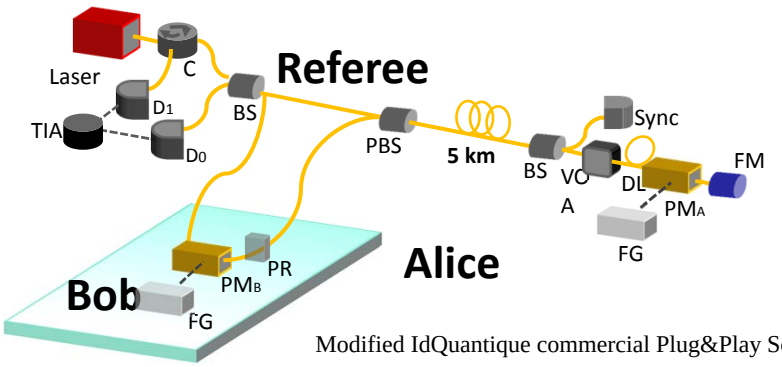
visibility v = 0.98

Implementation

Experimental Quantum Fingerprinting

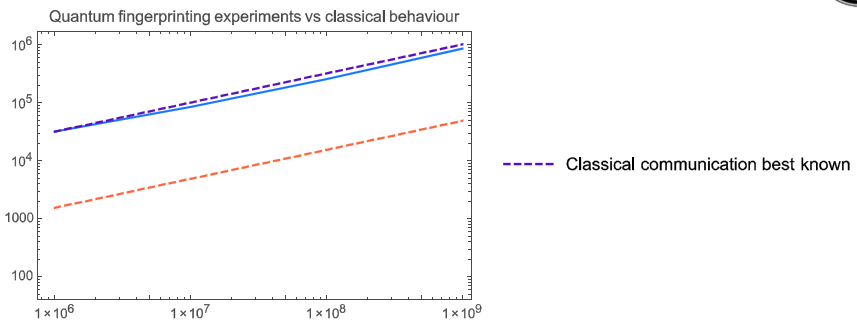
Feihu Xu,[1,2,*] Juan Miguel Arrazola,[3,*] Kejin Wei,[1,4] Wenyuan Wang,[1,5] Pablo Palacios-Avila,[3,6] Chen Feng,[7] Shihan Sajeed,[8] Norbert Lütkenhaus,[3,†] and Hoi-Kwong Lo[1,‡]

[Xu et al, Nature Communications 6, 8735 (2015)]



Modified IdQuantique commercial Plug&Play Scheme

Experimental Results

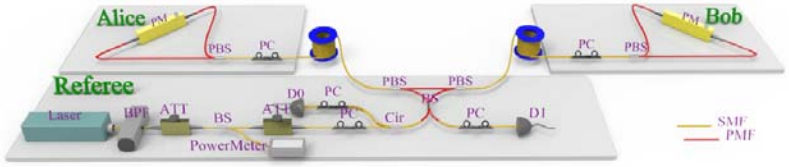


d_{det}= 3.5 x 10^{-6}
η_{det} = 20%
clockrate 5 MHz
5km distance Alice/Referee to Bob

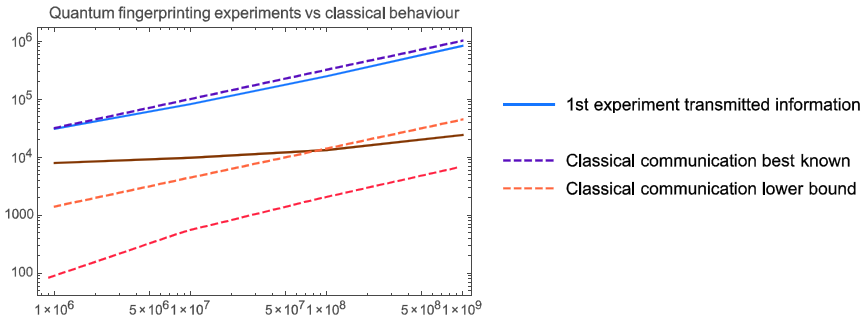
Note: We use roughly 7,000 photons for input size of 10^8!

Another experimental realization …

[Guan, Zhang, Pan et al, Phys. Rev. Lett. 116, 240502 (2016)]



beats not only best known classical protocol, but also best known bound on any classical protocol



Other protocols

Translation mechanism

$$f_\alpha\left(\sum_{i=1}^{n}\lambda_i\,|i\rangle\right)=\bigotimes_{i=1}^{n}|\lambda_i\alpha\rangle_i$$

projection onto $|i\rangle$ ⟷ Threshold Photon Counting in mode i

Coherent Pulse Encoding scheme

- can be translated to other communication complexity protocols maintaining quantum advantage **[J.M. Arrazola, N. L, Phys. Rev. A 90, 042335 (2015)]]**
- can be used by other quantum protocols (quantum retrieval games)
  [Arrazola, Karasamanis, NL, Phys. Rev. A 93, 062311 (2016)]
- Extension to d-dimensional systems, QAM modulation [Lovitz et al, in preparation]

Concrete examples:

- Euclidean distance of real vectors, **[Kumar, Diamanti, Kerenidis, PRA 95, 032337 (2017)]**
- Quantum Money **[Amiri, Arrazola, PRA 95, 062334 (2017), Bozzio et al, arXiv:1705.01428, Guan et al, arxiv:1709.05882]**
- Closed Group Digital Signatures **[E. Andersson]**
- appointment scheduling …

Scheduling Problem

Alice $x \in \{0,1\}^n$: 0, 1, 0, 0, 0, 0, 1

Bob $y \in \{0,1\}^n$: 1, 0, 0, 0, 0, 0, 1

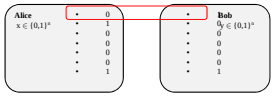
Task:

Find common open time slot ("1")
- with minimum number of communications
- OR
- with minimum leakage of information to each other

	Classical	Quantum
Communication Cost	$O(n)$	$O(\sqrt{n}\log_2 n)$
Information Cost	$O(n)$	$O(\sqrt{n}\log_2 n)$

Quantum Protocols: Distributed Grover Search **[Buhrman, Cleve Widgerson, STOC 1998]**

Optical Protocol: Individual AND protocol



Protocol Π_{AND}

Repeat until conclusive result

Protocol $\tilde{\Pi}_{AND}$

• a • b

Initialize:

$|\alpha\rangle\,|0\rangle$ → **Alice**:
a=0: Identity
a= 1: Beam splitter rotation π/r

→ Bob:
b=0: Replace by $|\alpha\rangle\,|0\rangle$
b=1: Identity Operation

repeat r times

last or r return

(0,0), (0,1), (1,0) — $|\alpha\rangle\,|0\rangle$

(1,1) — $|0\rangle\,|\alpha\rangle$

photon counting:
Click for first mode ➔ AND(a,b)=0
Click in second mode ➔ AND(a,b)=1
No click: inconclusive, Prob = $\exp(-|\alpha|^2)$

Full Protocol

Protocol Π_D

Step 1: classical sampling (open up set of size s, compare bits to look for coincidence)
Step 2: If no coincidence found, run protocol Π_{AND} until coincidence found

Information leakage:

$$\begin{aligned}\mathrm{QIC}(\Pi_D) \leq & s + \log s + 1 \\ & + \frac{n}{1-\exp(-|\alpha|^2)}\left[\frac{2(2r+3)}{n} + h\left(\frac{1}{2}(1-F(r,\alpha))\right)\right. \\ & \left. + 2(2r+3)\, h\left(\frac{2\ln n}{s} + \frac{1}{n}\right)\right],\end{aligned}$$

in which

$$F(r,\alpha) = \exp\left[-r\,|\alpha|^2\left[1-\cos\left(\frac{\pi}{2r}\right)\right]\right].$$

s = $n^{2/3}$, r = $n^{1/3}$, fixed α ➔QIC(Π_D) = O($n^{2/3}$)

Ideal setting

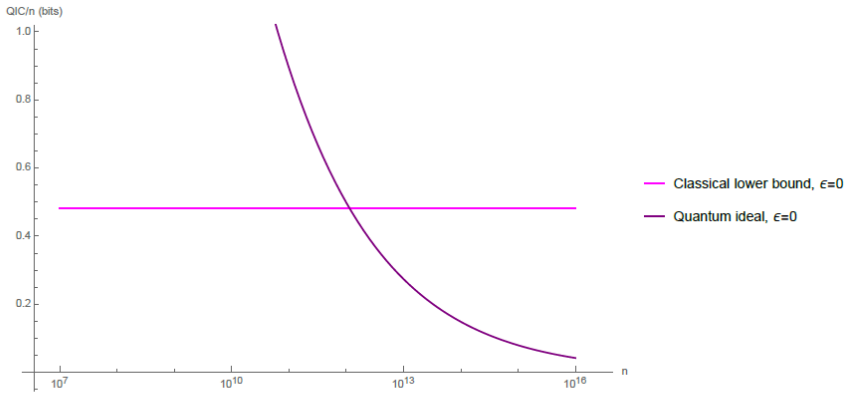
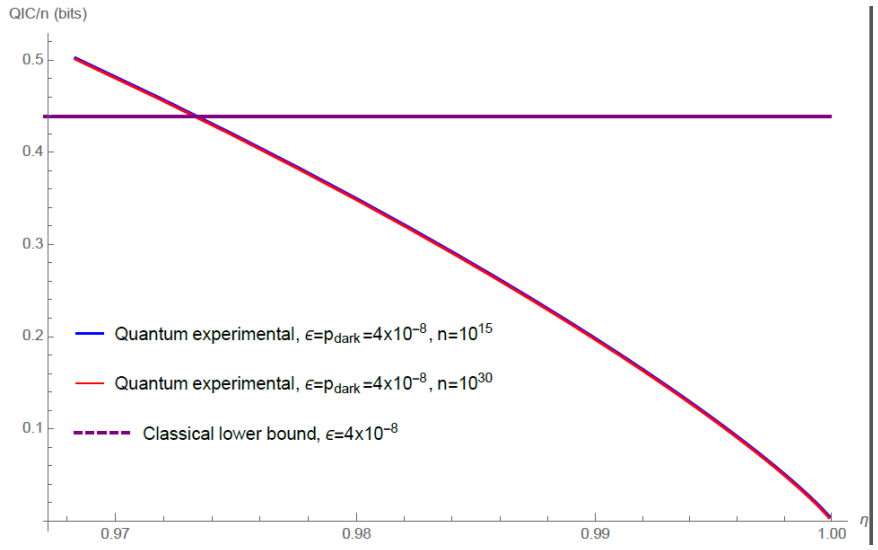


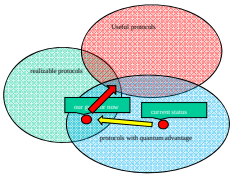
Figure 1: This figure shows the $\mathcal{O}(n^{2/3})$ limiting behaviour of our quantum protocol in comparison with the $\Omega(n)$ classical lower bound in the ideal setting for zero-error. We have chosen the number of rounds $r = n^{1/3}$, the coherent state amplitude $\alpha = 1$ and subsample size $s = n^{2/3}$. The information leakage (QIC) measured in bits divided by the input size n is plotted on the y-axis, and the input size n on the x-axis.

Loss behaviour



Summary

- There is a path to implement **scalable quantum communication complexity protocols!**
  ➔ think about other useful protocols



- advantage in use of **Hilbert space dimensions**, **number of photons** used

- entry into world **information complexity protocols**
  (direction of secure multi-party computations)