Optical Quantum Communication with Quantitative Advantage

Juan Miguel Arrazola
Benjamin Lovitz
Ashutosh Marwah
Dave Touchette

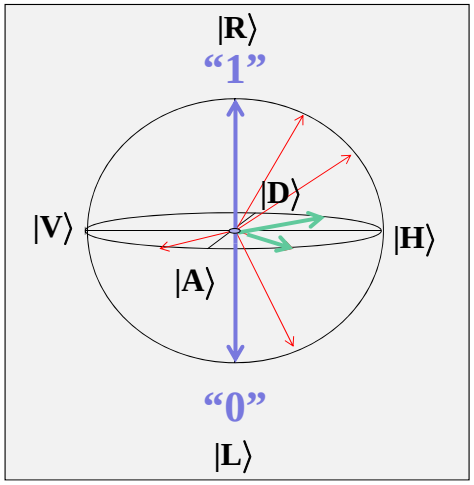
Norbert Lütkenhaus
Institute for Quantum Computing
& Department of Physics and Astronomy
University of Waterloo

CryptoWorks21

NSERC CRSNG

Industry Canada Industrie Canada
Canada

Quantum Communication



Bits ➔ Qubits

Optical Realisation of Qubits:

single photon & polarization
➔ Bloch Sphere

coherent states (laser pulses)
with field amplitude α or β
➔ overlap

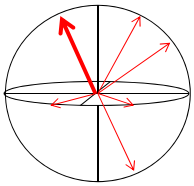
$$\langle \alpha | -\alpha \rangle = \exp\left[-2|\alpha|^2\right]$$

can be tuned to any value:

0 non-orthogonal (quantum) 1

orthogonal (classical) identical

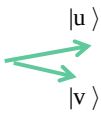
Communication with quantum states



channel

higher throughput?

discriminating two non-orthogonal states:
(single shot)



- Can we with certainty discriminate which of the two states was sent?
  ➔ No!

$$Prob(error) \geq \frac{1}{2}\left(1 - \sqrt{1 - |\langle u|v\rangle|^2}\right)$$

- can we duplicate the signal (cloning)?
  ➔ No!

Consequence:
using an n-dimensional signal
➔ can transmit only n clearly distinct messages
➔ can transmit $\log_2$ n bits of information
➔ cannot increase **general purpose** throughput of channel!

Quantum Communication

Privacy
➔ Quantum Key Distribution
➔ Secure Multi-Party Computation
  ➔ data comparison
  ➔ scheduling algorithm

Efficiency
➔ Quantum Communication Complexity
  ➔ efficient comparison of data
  ➔ scheduling algorithms

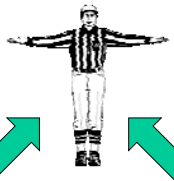
[Buhrman, Cleve, Watrous, de Wolf, PRL 87, 167902 (2001)]

Quantum Fingerprinting

file size: n bits (2^n possibilities)

classical communication:
$O(\sqrt{n})$ bits

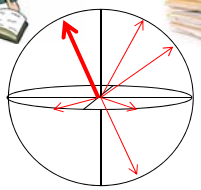
quantum communication:
O(log n) qubits

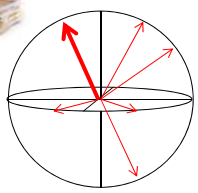


are the data equal or not?

footnotes:
- one-way communication
- no shared randomness
- allow for ϵ -error

It is easier to decide whether two states are equal , than to find out what the individual states are!





2^n different states in n-dim vector space

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

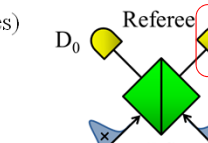
[Arrazola and Lütkenhaus, Phys. Rev A 89, 062305 (2014)]

Quantum Fingerprinting

file size: n bits (2^n possibilities)

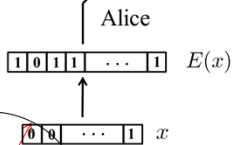
classical communication:
$O(\sqrt{n})$ bits

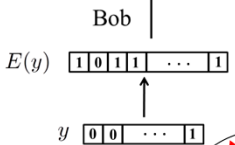
quantum communication:
O(log n) qubits

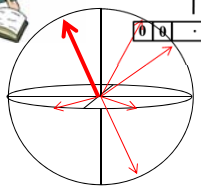


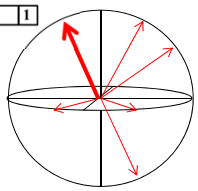
difference detection:
➔ dark port monitoring

footnotes:
- one-way communication
- no shared randomness
- allow for ϵ -error







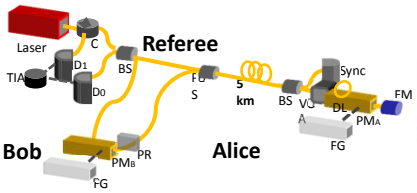


the amplitudes for each pulse will be small
➔ highly non-orthogonal states
➔ deep in the quantum domain

2^n different states in n-dim vector space

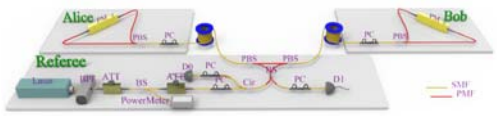
Experimental Realizations

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

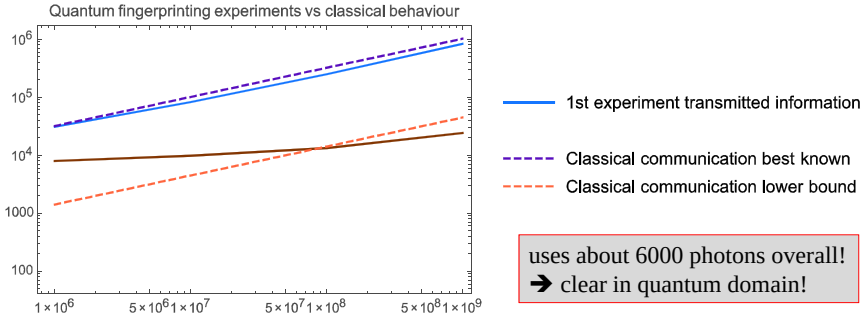


commercial QKD device (IDQuantique)

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



Sagnac interferometer



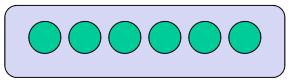
uses about 6000 photons overall!
➔ clear in quantum domain!

Trade-off signal dimensions vs. #signals

[Lovitz, NL, Phys. Rev. A 97, 032340 (2018)]

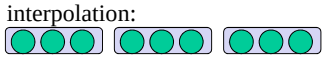
Abstract Considerations:

- **original quantum finger printing protocol:**



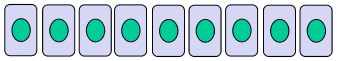
1 block of log n qubits

- interpolation:



n/k blocks of log k qubits

- **our optical protocol:**

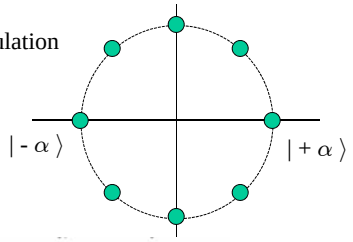


n blocks of single qubits

all variations have effective log n qubit dimensional Hilbert space!

Optical Implementation

PSK modulation



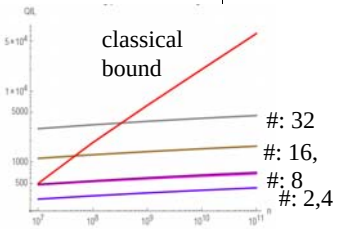
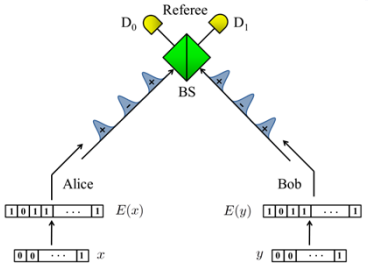
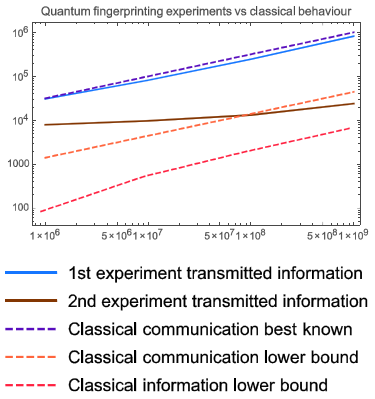


FIG. 2: Quantum information leakage (QIL), measured in bits, as a function of the input size n for our ring protocols to attain error probability $\varepsilon = 0.01$ in the ideal setting.

Privacy aspects:





in quantum fingerprinting referee learns at most O (log n) bits

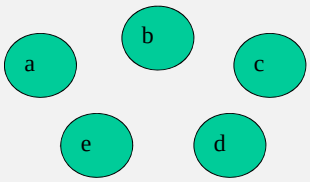
Information Complexity **[Arrazola, Touchette, arXiv:1607.07516]**

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

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

Secure Multi-Party computation

secure multi-party computation



- given input: a,b,c,d,e …
- evaluate z= f(a,b,c,d,e …)
- parties learn only result z, but not other inputs

Examples:
- compare the inputs (Equality function)
- scheduling (find next available common free time slot) (AND function)

Application Examples:

- **Privacy:** compare names on
  - no fly list
  - passenger list
- **Protect commercial information:** evaluate combination of commercial database:
  - one contains people'sweb-searches
  - one that contains people's online purchases

Pairwise secret keys enable this!

for t> n/2 honest participants (with broadcast)

for t>2n/3 honest participants (without broadcast)

➔ **Secret key (QKD!) is useful not only for encryption per se!**

But for two parties secret key is useless, and we cannot achieve honest majority!

Optical Appointment Scheduling

[Lovitz, Touchette, Lütkenhaus, Phys. Rev. A 97, 042320 (2018)]

Alice's x Bob's y

Scheduling Problem Definition:

- find common free slot in calendar of length n!
- reveal as little as possible about each calendar

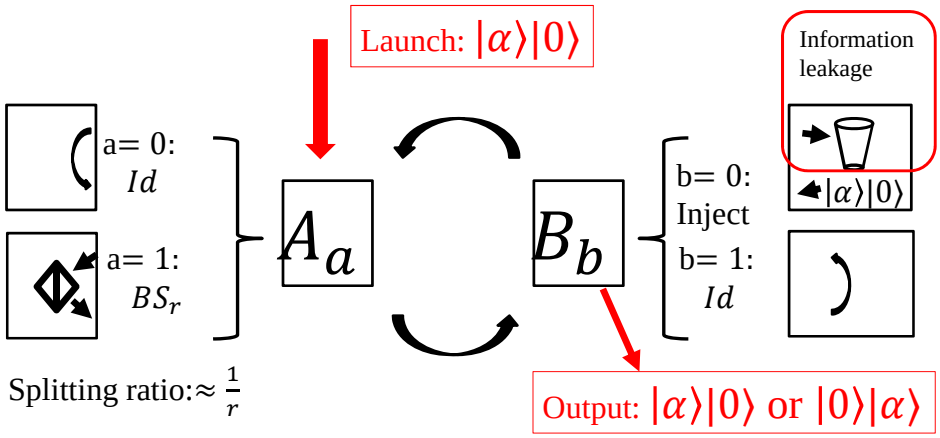
Information Cost:

- Classical: leakage $\geq 0.48\, n$
- Quantum **Advantage**: quantum leakage$\leq \tilde{O}(\sqrt{n})$
  ➔Can be achieved with coherent state distributed Grover
- Need **Interaction**: for r messages, can only achieve $\tilde{O}(\frac{n}{r})$

Here we do not worry about *amount of communication*, but only about *information leakage*

➔ simplification possible:
test the calendar entries one by one

Optical Bit-Wise AND



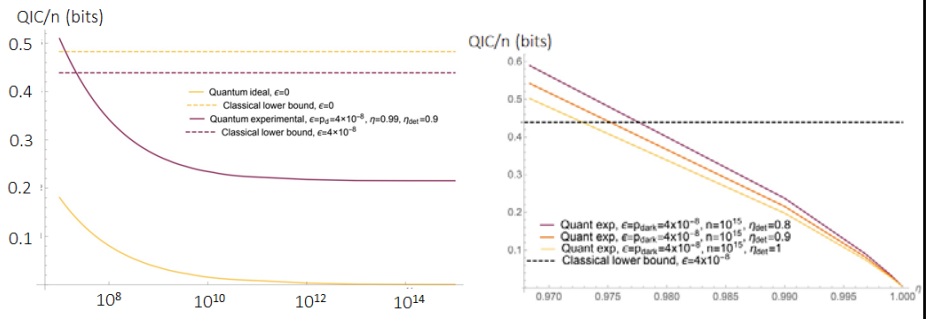
➔ protocol enables determining AND(a,b)
(probabilistically, but can repeat)

➔ honest-but-curious model:
(protocol leaks information to Bob)

a	b
0	0
0	1
1	0

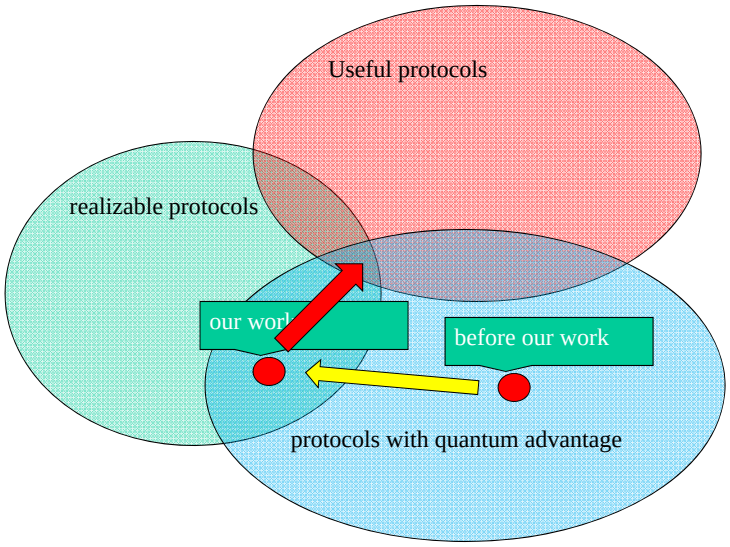
a	b
1	1

Optical Appointment Scheduling: Simulation



➔ can be implemented using laser pulses
➔ requires high one-way efficiency (97.5%)

Road map



Summary

- **Optics is the natural implementation** medium for quantum communication
- Modern **optical communication tools** including Phase-Shift Keying open the path to exploit the quantum effects
- Quantum Effects do not increase the general purpose information throughput through channels, but can give **enhancement for individual full protocols!**
- **Secret key (QKD) enables more than just secret communication:**
  for example: secure multi-party computation
- Optical solutions to exploit **privacy** and **efficiency** enhancing quantum effects
  - **data comparison** (efficiency improvement demonstrated, privacy enhancement under way)
  - **privacy enhanced scheduling algorithm** proposed