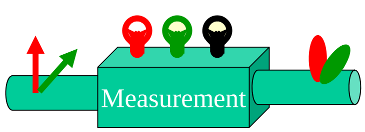
Quantum Communication: How quantum signals help to maintain privacy and speed things up

Juan Miguel Arrazola, Markos Karasamanis,
Dave Touchette, Ben Lovitz,
Norbert Lütkenhaus
Institute for Quantum Computing
University of Waterloo

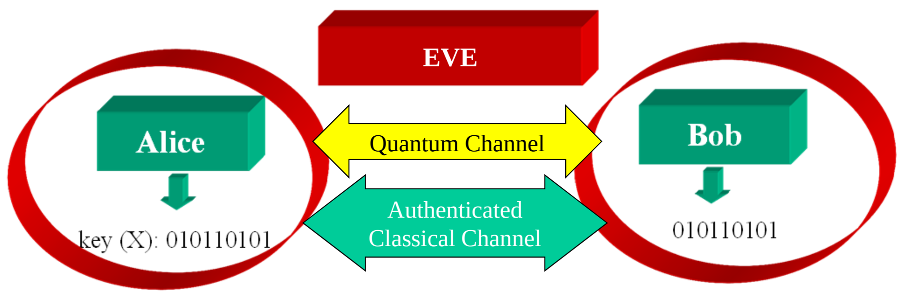
Principles of QKD in physics terms

quantum signals allow for testing of eavesdropping activity:
- Heisenberg Uncertainty principle
- back-reaction of measurement onto quantum system



eavesdroppers introduce errors
errors observed → protocol aborts
- no protection against denial-of-service attack

Quantum Key Distribution Primitive



Alice/Bob devices:

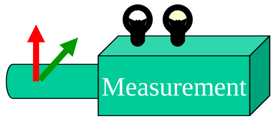
- trusted (cannot be manipulated by Eve)
- characterized (QM description known, QM believed to hold)
- secure perimeter (Eve cannot read internal status of devices)

Quantum Communication

using quantum effects in quantum communication

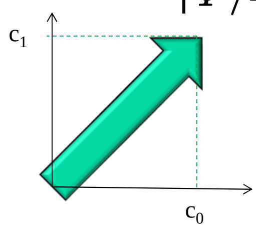
- qualitative advantage
  measurement back-reaction on signal
  ➔ quantum key distribution (cannot be achieved classically)
- quantitative advantage
  use fewer resources to accomplish a goal
  leak less information to participants (towards secure multi-party computation)

Quantum Mechanics



quantum mechanics predicts probabilities of events to happen …

$$|\Psi\rangle = \sum_i c_i |u_i\rangle$$



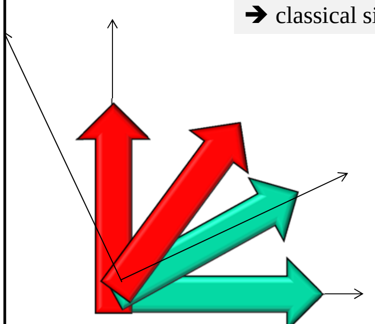
the **state of the system** is described by a
- complex unit vector $|\Psi\rangle$

The **measurement** is described by
- an orthonomal basis $\{ |u_i\rangle \}$

$$\Pr(\text{"i"}) = |c_i|^2$$

classical communication embedded in quantum mechanics

orthogonal states can be perfectly discriminated
➔ classical signals are embedded into quantum mechanical formalism



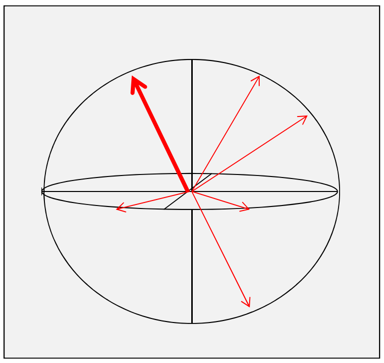
Non-orthogonal states cannot be perfectly discriminated!

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

but there are measurements that can unambiguously discriminate the two signals with some probability!

$$Prob(success) \leq 1 - |\langle u|v\rangle|$$

How much information can be read out of QM systems?

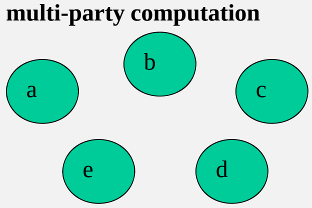


we can prepare a quantum system in an arbitrary number of different internal states!

BUT: if used in a communication context, we can recover at most $\mathbf{\log_2 d}$ number of bits about the input states

Information & Communication complexity Complexity

multi-party computation



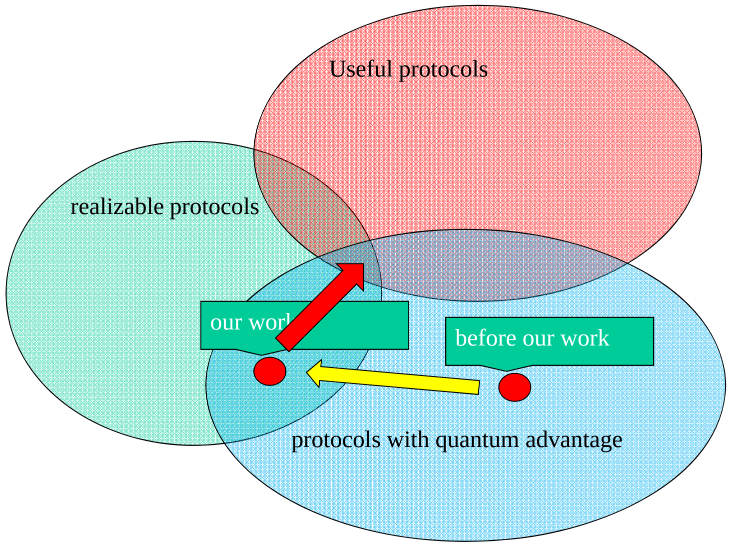
- given input: a,b,c,d,e …
- evaluate z= f(a,b,c,d,e …)

Communication Complexity:
How many signals need to be exchanged to evaluate function?

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

Quantum Communication can offer better performance than classical communication

Expectation Management



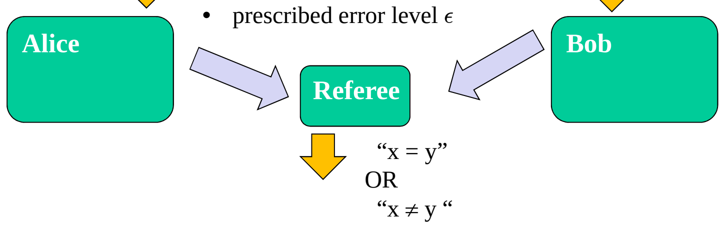
Task Description: Finger Printing

(simultaneous message passing)

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

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

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



Exponential Gap between classical and quantum

classical $O(\sqrt{n})$ **[Ambainis, Algorithmica 16, 298 (1996)]**

quantum $O(\log_2 n)$

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

note: If we were to give access to either

- two-way classical communication, or
- access to share randomness

➔ would also give $O(\log_2 n)$ in classical communication

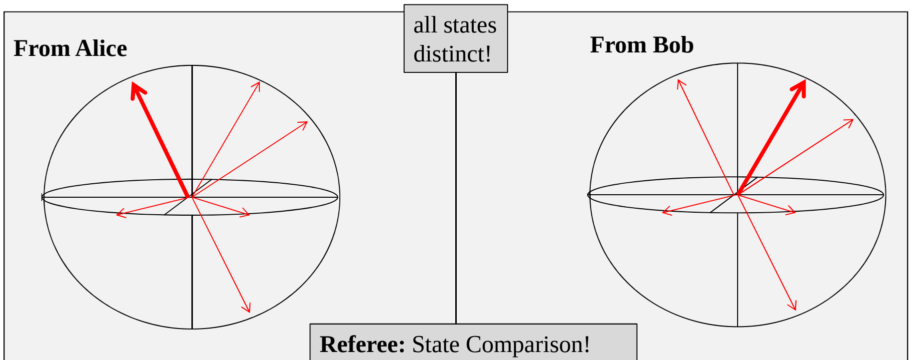
Two **different** question:

- **how many signals need to be transmitted to solve the task?**
- how much does the referee learn about the input?

Mechanism for Quantum Finger Printing

protocol encodes $\mathbf{2^n}$ states in a n dimensional Hilbert space!

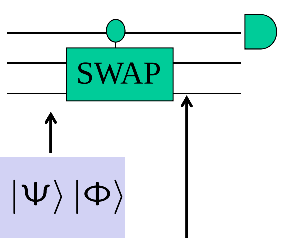
➔ highly non-orthogonal states!



Referee: State Comparison!
- are both states the same?
- not interested which state …

C-SWAP Test

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



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

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	$\left[\frac{1}{2}\left(1 + |\langle\Phi|\Psi\rangle|^2\right)\right]^n$
'different' (-)	0	$1 - \left[\frac{1}{2}\left(1 + |\langle\Phi|\Psi\rangle|^2\right)\right]^n$

➔ 0 for n $\to \infty$

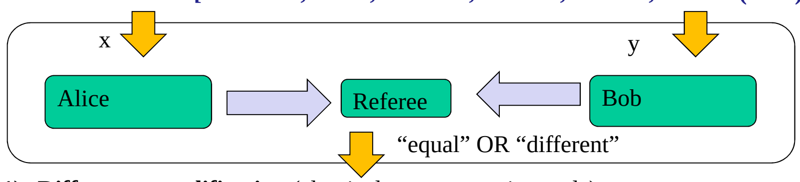
➔ 1for n $\to \infty$

If n repetitions allowed
➔ can quickly reduce

Waterloo IQC Institute for Quantum Computing

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)

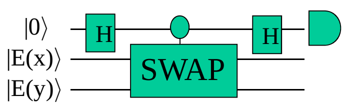
→ **one bit difference**
→ **8% error difference**

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

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

 # qubits: log m

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



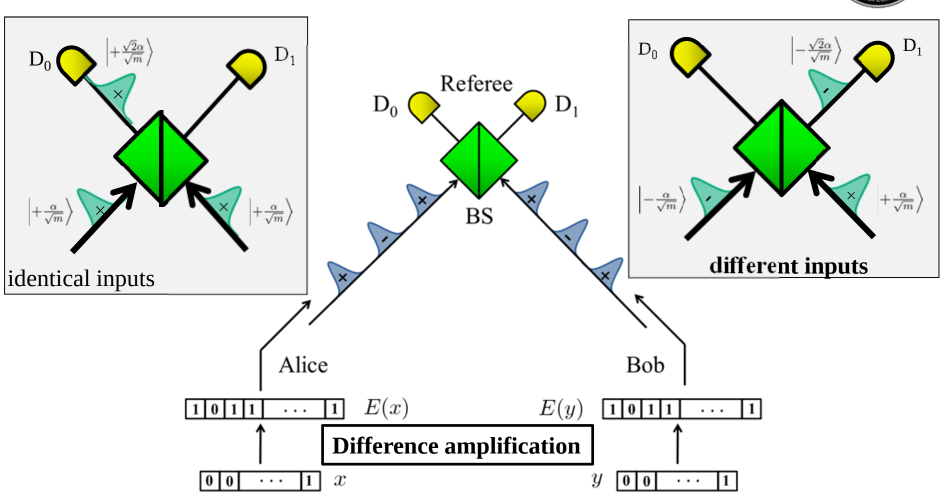
	Equal input	Unequal input
'same'	1	< ½(1+δ^2)
'different'	0	> ½(1-δ^2)

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

Waterloo IQC Institute for Quantum Computing

Coherent-state Protocol

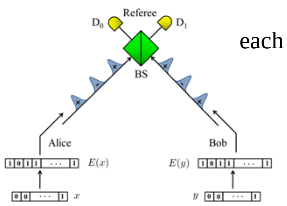
[Arrazola and Lütkenhaus, Phys. Rev A 89, 062305 (2014)]



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"

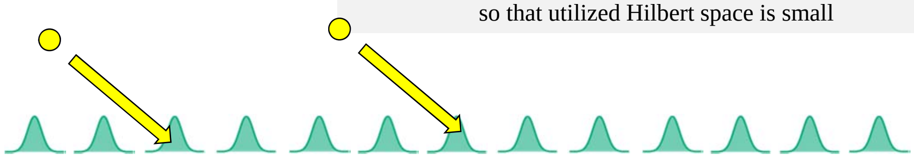
Resource counting



each pulse $\left|+\frac{\alpha}{\sqrt{m}}\right\rangle$

➔ $\Pr(\text{click}) = 1 - e^{-2\frac{|\alpha^2|}{m}} \approx 2\frac{|\alpha^2|}{m}$

make 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



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

Experimental realities

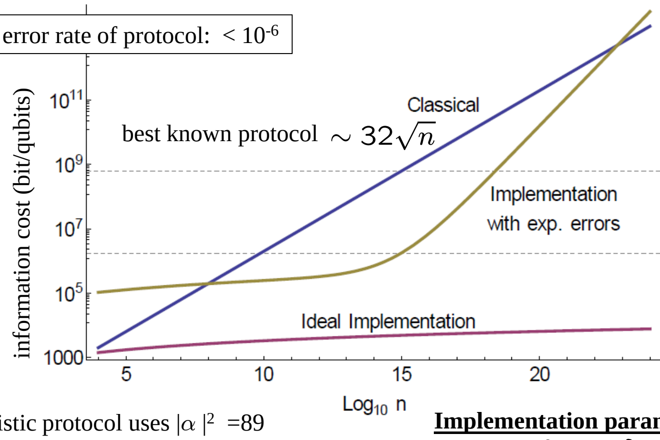
loss between sources and referee?
➔ simply increase mean photon number to compensate loss
➔ does not affect scaling of resources!

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

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 $\delta = 0.92$ [m = 3 n]

$\eta = 0.1$ ➔ **90% loss!!**

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

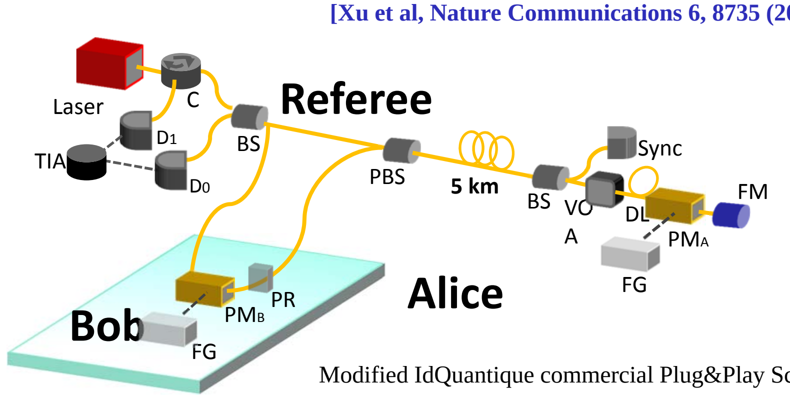
visibility v = 0.98

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,‡]

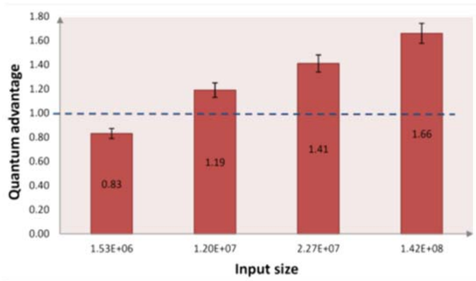
[Xu et al, Nature Communications 6, 8735 (2015)]



Modified IdQuantique commercial Plug&Play Scheme

Experimental Results

Quantum advantage: $\gamma = \frac{C}{Q}$

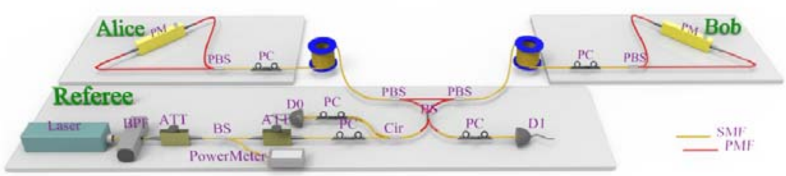


d_{det}= 3.5 x 10^{-6}
η_{det} = 20%
clockrate 5 MHz
5km distance Alice/Referee to Bob

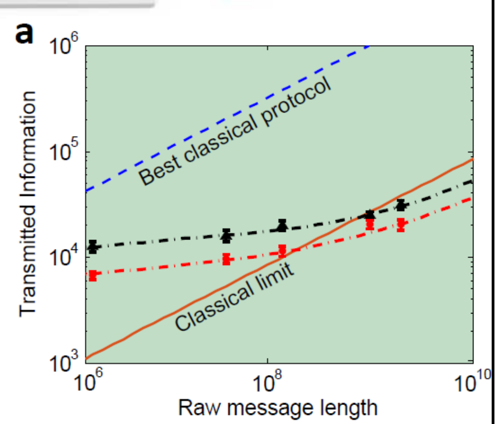
Note: We use roughly 7,000 photons for input size of 10^8!

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



Will this convince an optical communication engineer?

[Phys. Rev A 90, 042335 (2014)]

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

Our quantum implementation: number of pulses: n
Dimension: log n

BUT:

encoding has constant energy (photon number)

➔ number of photons in the channel dramatically decreased

- reduced cross-talk in fiber
- fewer detection clicks expected ➔ faster clock rates???

ALSO

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

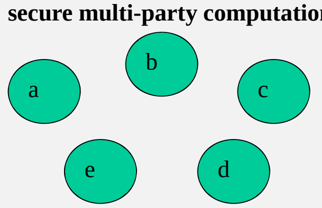
AND

leaks only O(log n) bits about strings x, y to referee
➔ Information Complexity
see our paper **[Arrazola, Touchette, arXiv:1607.07516]**

Information Complexity

How much does each party learn about the input of the others?

secure multi-party computation



- given input: a,b,c,d,e …
- evaluate z= f(a,b,c,d,e …)
- so that all parties know z and their own input
- but nothing else

cannot be achieved exactly
[Buhrman, Christandl, Schaffner, | Phys. Rev. Lett. 109, 160501 (2012)]

For Quantum Fingerprinting:

- equality function
- communication constraints: one-way, no shared randomness
- Bound on classical protocol: $O(\sqrt{n})$
  (exact expression known!)

[Arrazola, Touchette, arXiv:1607.07516]

➔ our quantum optical protocol can beat that!

The story continues …

Encoding scheme can be used to address

- hidden matching protocol

  (needs programmable mode switching)

- 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)]

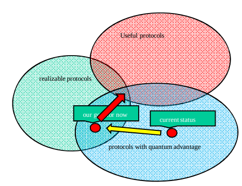
appointment scheduling problem

- has quadratic quantum advantage
- has an optical implementation shuttling laser pulses for and back
- is still very susceptible to coupling losses

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)