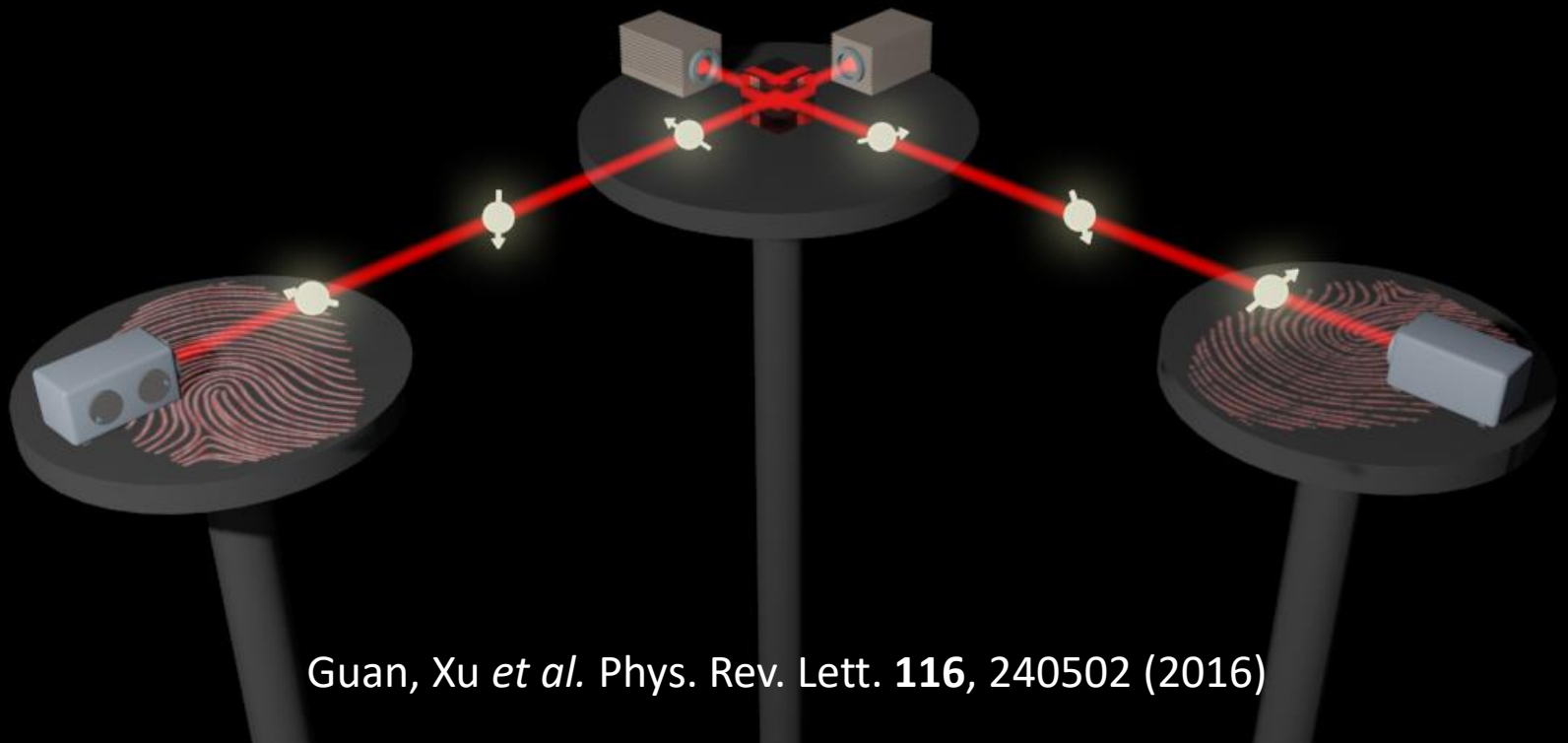
Observation of quantum fingerprinting beating the classical limit

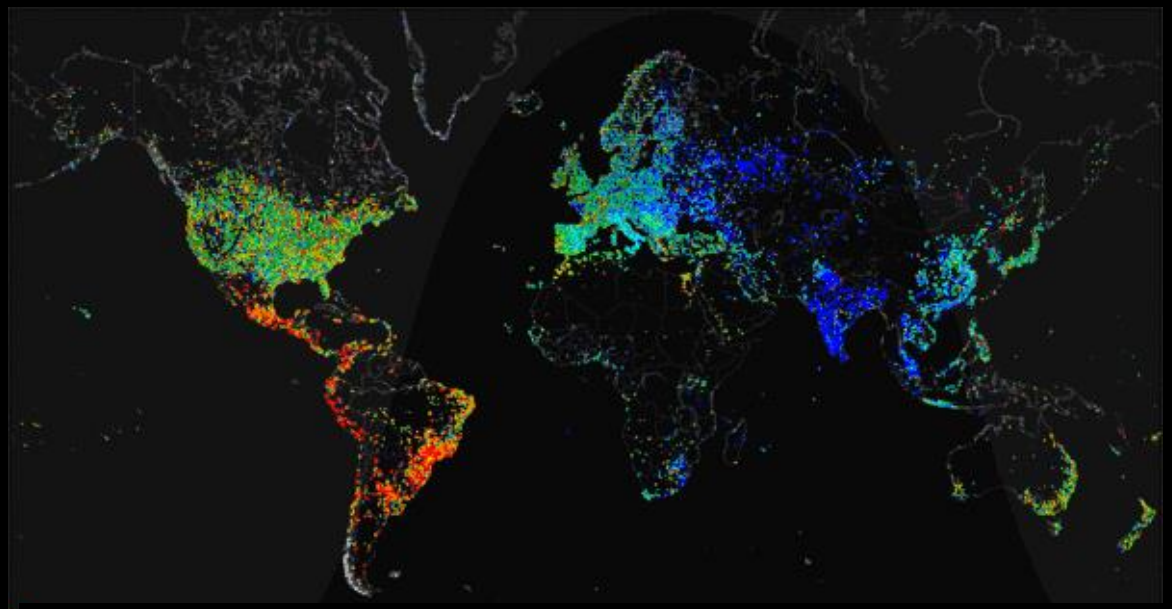
Feihu Xu, *MIT*

Jianyu Guan, Hualei Yin …, Qiang Zhang, Jian-Wei Pan, *USTC*
Lixin You, *CAS*



Guan, Xu *et al.* Phys. Rev. Lett. **116**, 240502 (2016)

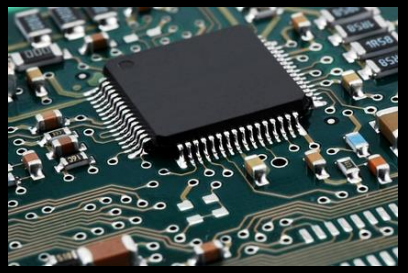
Communication complexity



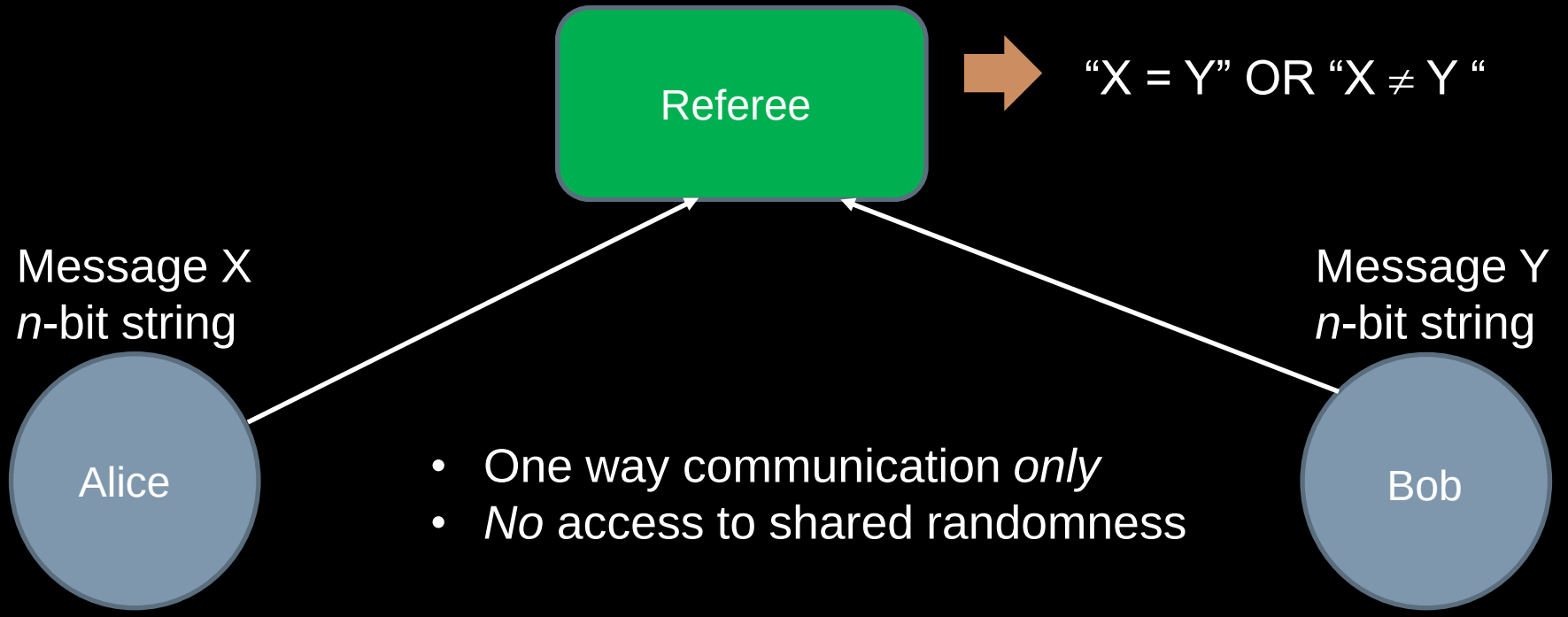
World map of daily utilization of IPv4 addresses

Find the *minimum* amount of communication needed to solve distributed computational tasks.

- Fundamental Physics and CS
- Green communication and networks
- VLSI circuit design
- Data structure design



Fingerprinting model
(simultaneous message passing)



Given two *n*-bit strings, what is the *minimum* amount of information that must be transmitted to the referee?

A. C.-C. Yao, Proc. of the 11th Annual ACM STOC, 209 (1979)

Example: censor illegal movie copy

Send entire file: *n* bits

Send a short **fingerprint** using classical state: $O(\sqrt{n})$ bits*

- ***No*** access to shared randomness

- Each one sends a string to Referee
- Referee compares between strings to find the illegal copy
- **How many bits must be transmitted?**

Send a much shorter fingerprint using **quantum** state: $O(\log_2 n)$ qubits**

* Algorithmica **16**, 298 (1996)

** Phys. Rev. Lett. **87**, 167902 (2001)

Why quantum fingerprinting?

Proven classical bound*:

$$O(\sqrt{n}) \text{ - bits}$$

Proven quantum bound**:

$$O(\log_2 n) \text{ - qubits}$$

An *exponential* saving in communication!

But, it requires $\log_2(n)$ entangled qubits …

* A. Ambainis, Algorithmica **16**, 298 (1996)

** H. Buhrman, *et al.*, Phys. Rev. Lett. **87**, 167902 (2001)

Previous experiments: single-qubit transmission

PRL **95,** 150502 (2005) PHYSICAL REVIEW LETTERS week ending 7 OCTOBER 2005

Single-Qubit Optical Quantum Fingerprinting

Rolf T. Horn,[1] S. A. Babichev,[1,2] Karl-Peter Marzlin,[1] A. I. Lvovsky,[1,2] and Barry C. Sanders[1]
[1]*Institute for Quantum Information Science, University of Calgary, Alberta T2N 1N4, Canada*
[2]*Fachbereich Physik, Universität Konstanz, D-78457 Konstanz, Germany*
(Received 23 September 2004; revised manuscript received 1 December 2004; published 4 October 2005)

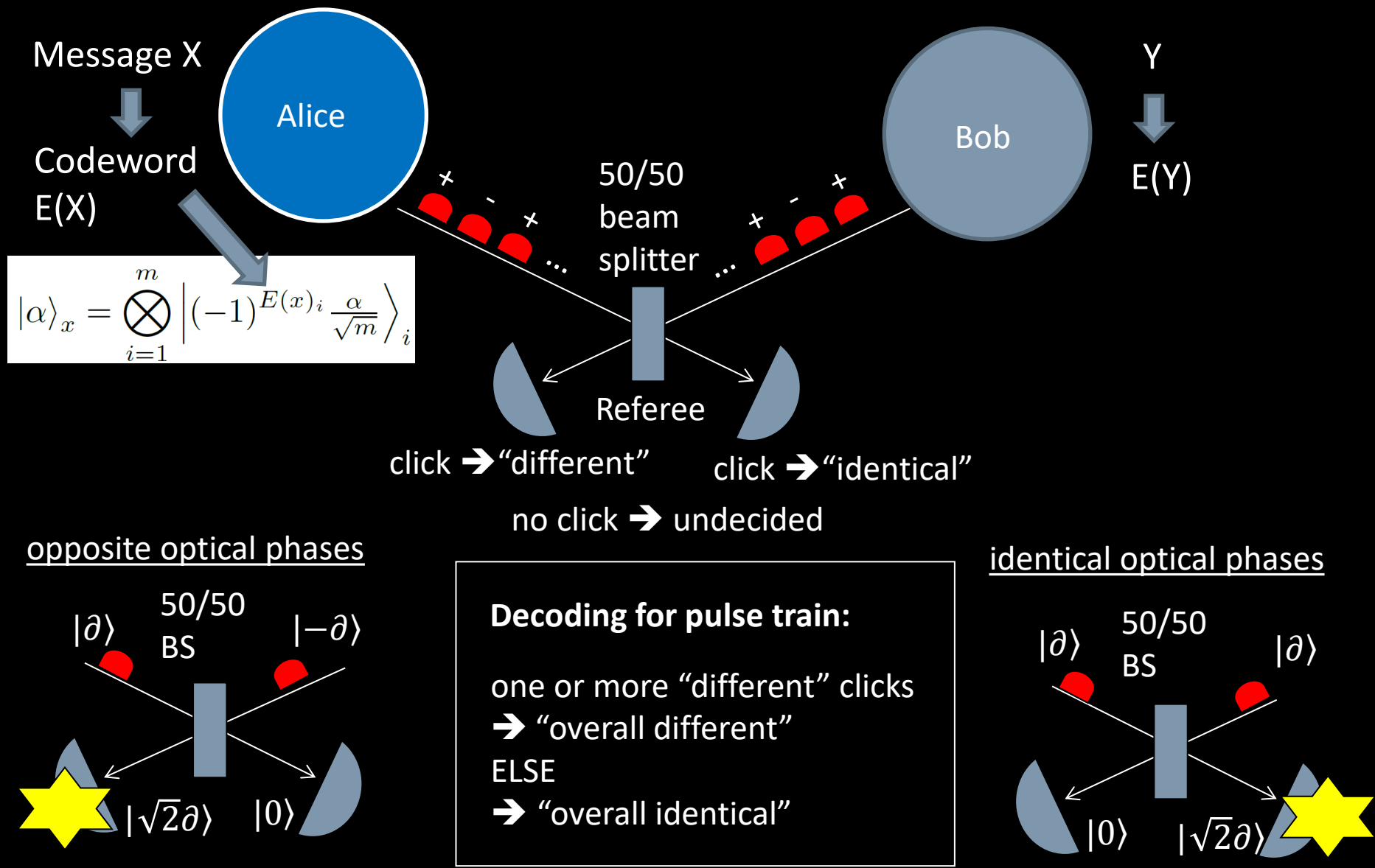
PHYSICAL REVIEW A **72,** 050305(R) (2005)

Experimental quantum communication complexity

Pavel Trojek,[1,2] Christian Schmid,[1,2] Mohamed Bourennane,[3] Časlav Brukner,[4] Marek Żukowski,[5] and Harald Weinfurter[1,2]
[1]*Max-Planck-Institut für Quantenoptik, D-85748 Garching, Germany*
[2]*Sektion Physik, Ludwig-Maximilians-Universität, D-80799 München, Germany*
[3]*Department of Physics, Stockholm University, SE-10691 Stockholm, Sweden*
[4]*Institut für Experimentalphysik, Universität Wien, Boltzmanngasse 5, A-1090, Wien, Austria*
[5]*Instytut Fizyki Teoretycznej i Astrofizyki Uniwersytet Gdański, PL-80-952 Gdańsk, Poland*
(Received 8 June 2004; published 28 November 2005)

- Smaller error probability for *single-qubit* transmission
- *No* reduction in the transmitted information compared with the classical case

A practical coherent-state protocol



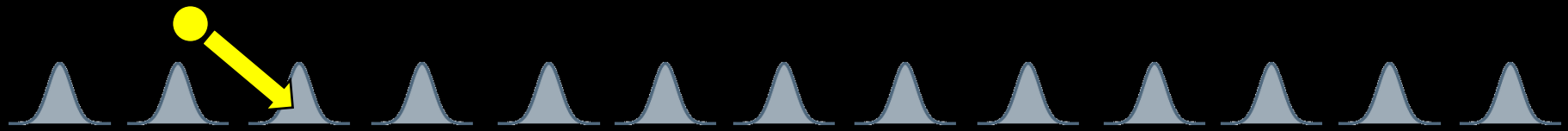
Decoding for pulse train:

one or more "different" clicks
➔ "overall different"
ELSE
➔ "overall identical"

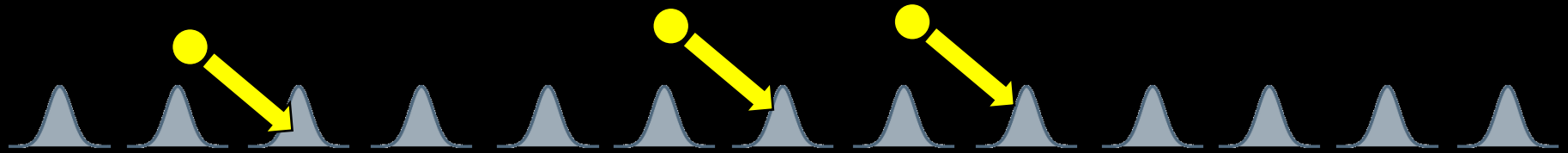
J. Arrazola, N. Lütkenhaus, Phys. Rev. A, **89**, 062305 (2014)

Transmitted Information

States of a single photon across n modes span a Hilbert space of dimension n, which is mathematically equivalent to $\boldsymbol{O(log_2\, n)}$ qubits



A coherent state with total photon number $\mu = |\alpha|^2$ across n modes spans a Hilbert space equivalent to $\boldsymbol{O(\mu\, log_2\, n)}$ qubits

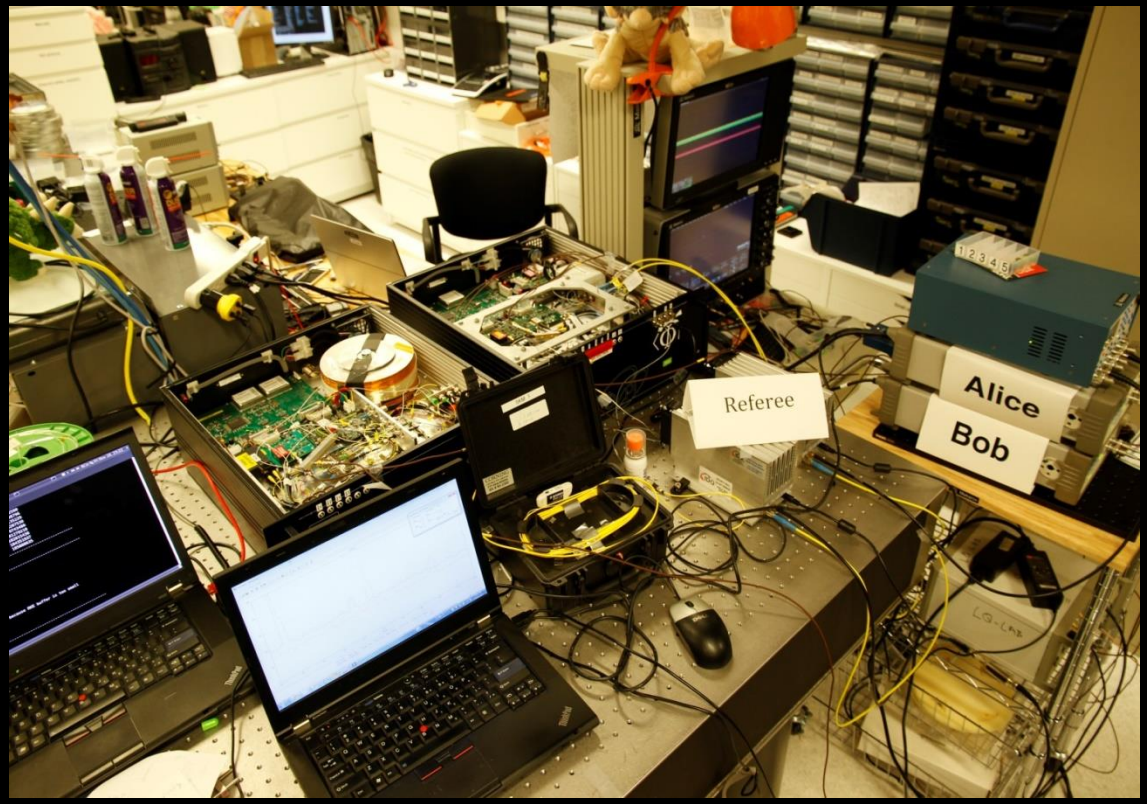


Restrict μ to a **small constant** -> Exponentially small subspace of a larger Hilbert space -> Exponential improvement over classical

Cost: number of modes is linear in the input size

J. Arrazola, N. Lütkenhaus, Phys. Rev. A, **89**, 062305 (2014)

Proof-of-concept implementation



QCrypt2015

- ✓ Constructed a more *efficient* error correcting code
- ✓ Designed an improved decision rule for the referee
- ✓ Built a *modified* plug&play QKD system to perform the experiment

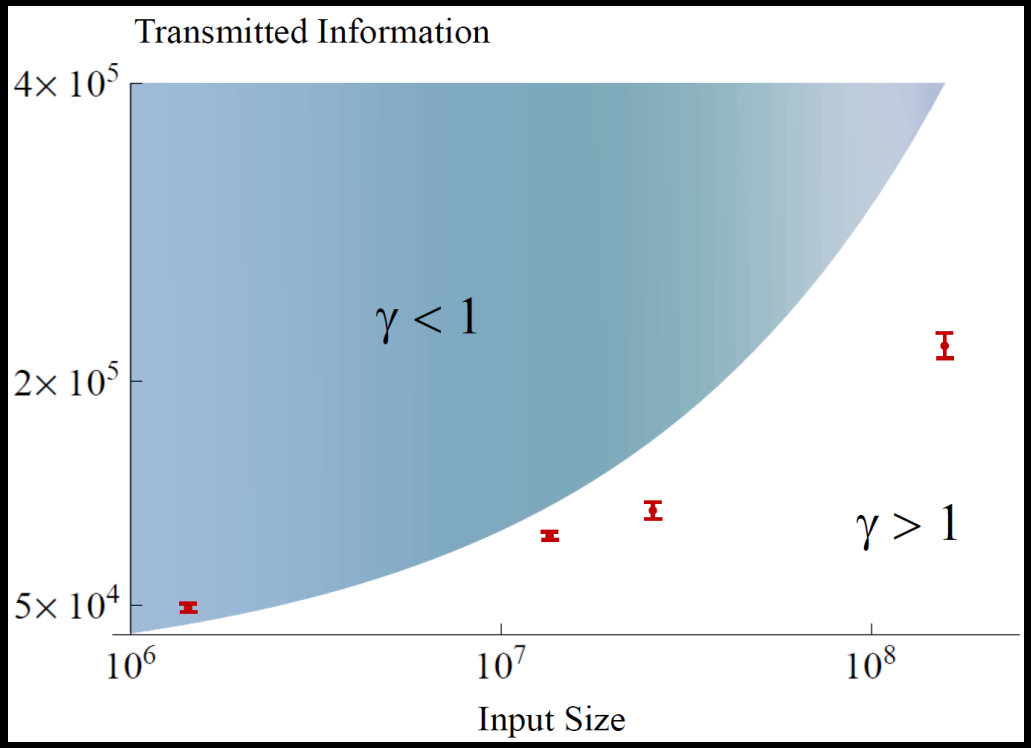
F. Xu, J. Arrazola, …, N. Lütkenhaus, Hoi-Kwong Lo, Nature Commun. **5**, 8735 (2015)

Previous results

best classical protocol

Quantum advantage: $\gamma = \frac{32\sqrt{n}}{Q}$

QCrypt2015



For messages up to 100 Mbits, the information transmitted is 66% lower than the best known classical protocol

F. Xu, J. Arrazola, …, N. Lütkenhaus, Hoi-Kwong Lo, Nature Commun. **5**, 8735 (2015)

Whether quantum fingerprinting can beat the classical theory limit?

Best known classical protocol: $32\sqrt{n}$

Classical theoretical limit: $\frac{\sqrt{n}}{20}$

Three orders of magnitude smaller!

L. Babai, P. G. Kimmel, Proceedings of the 12th Annual IEEE Conference on Computational Complexity, 239–246 (1997)

Our Solution

- ✓ Proved a *tighter* classical theoretical bound
- ✓ Utilized superconducting single-photon detectors with *ultra-low* dark counts
- ✓ Constructed a phase-stabilized Sagnac interferometer

Beating the classical theory limit by 19% over 20 km fiber!

J. Guan, F. Xu *et al.* Phys. Rev. Lett. **116**, 240502 (2016)

Tighten classical bound

Best known classical protocol: $32\sqrt{n}$

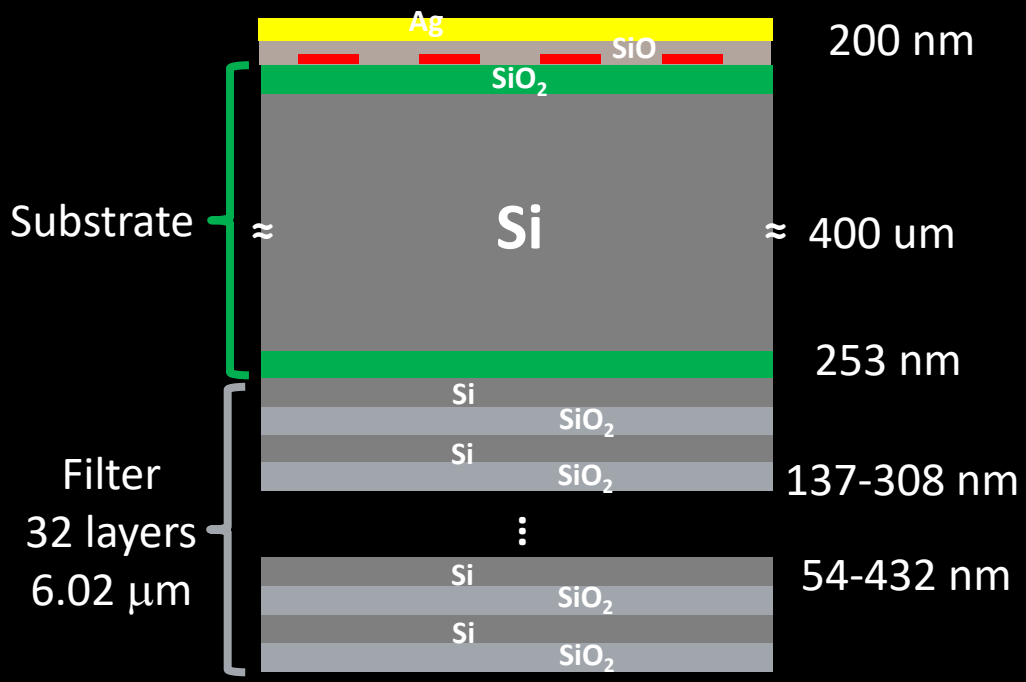
Classical theoretical limit*: $\frac{\sqrt{n}}{20}$

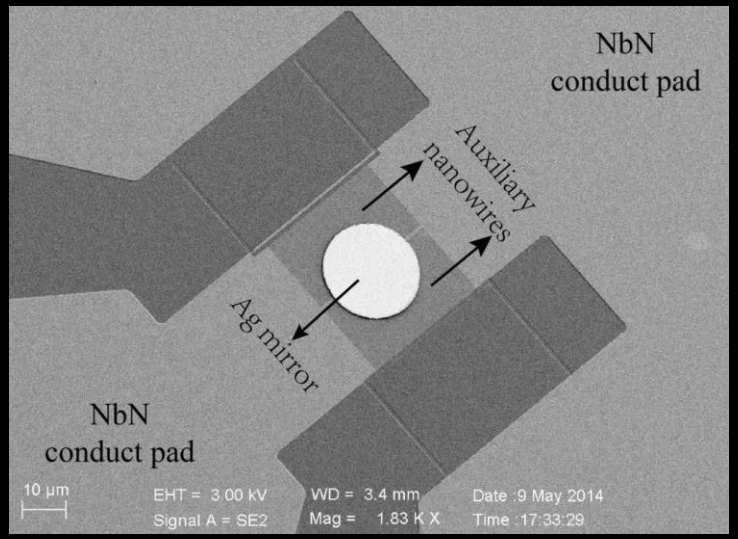
- Optimize the coefficients
- Improve the bound by one order of magnitude

$$C_{\text{limit}} = (1 - 2\sqrt{\epsilon})\sqrt{\frac{n}{2\ln 2}} - 1.$$

*L. Babai, P. G. Kimmel, Proceedings of the 12th Annual IEEE Conference on Computational Complexity, 239–246 (1997)

SNSPD with integrated filter

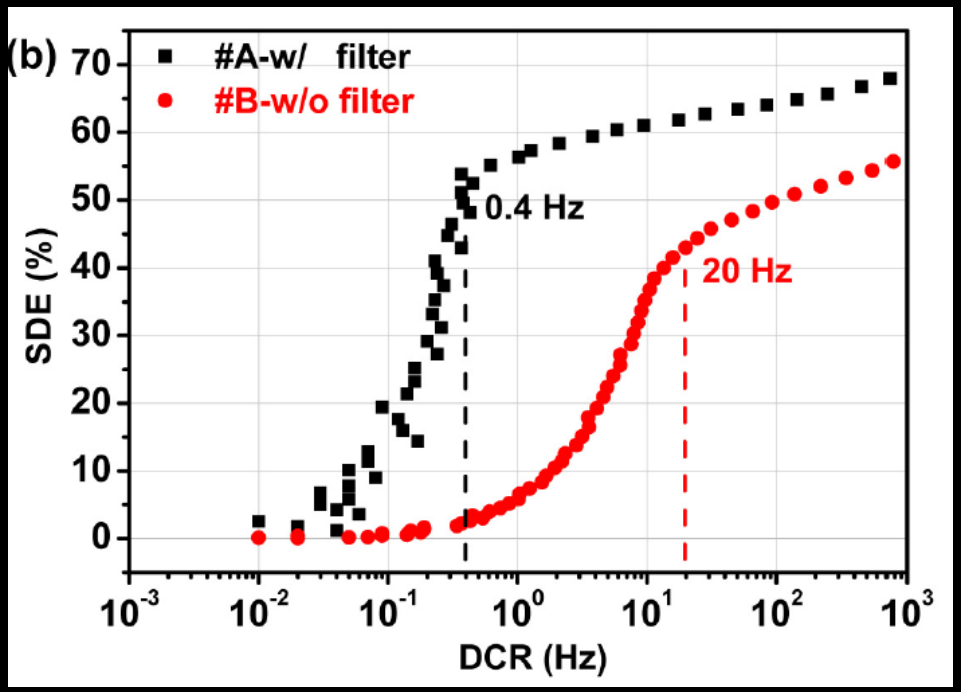




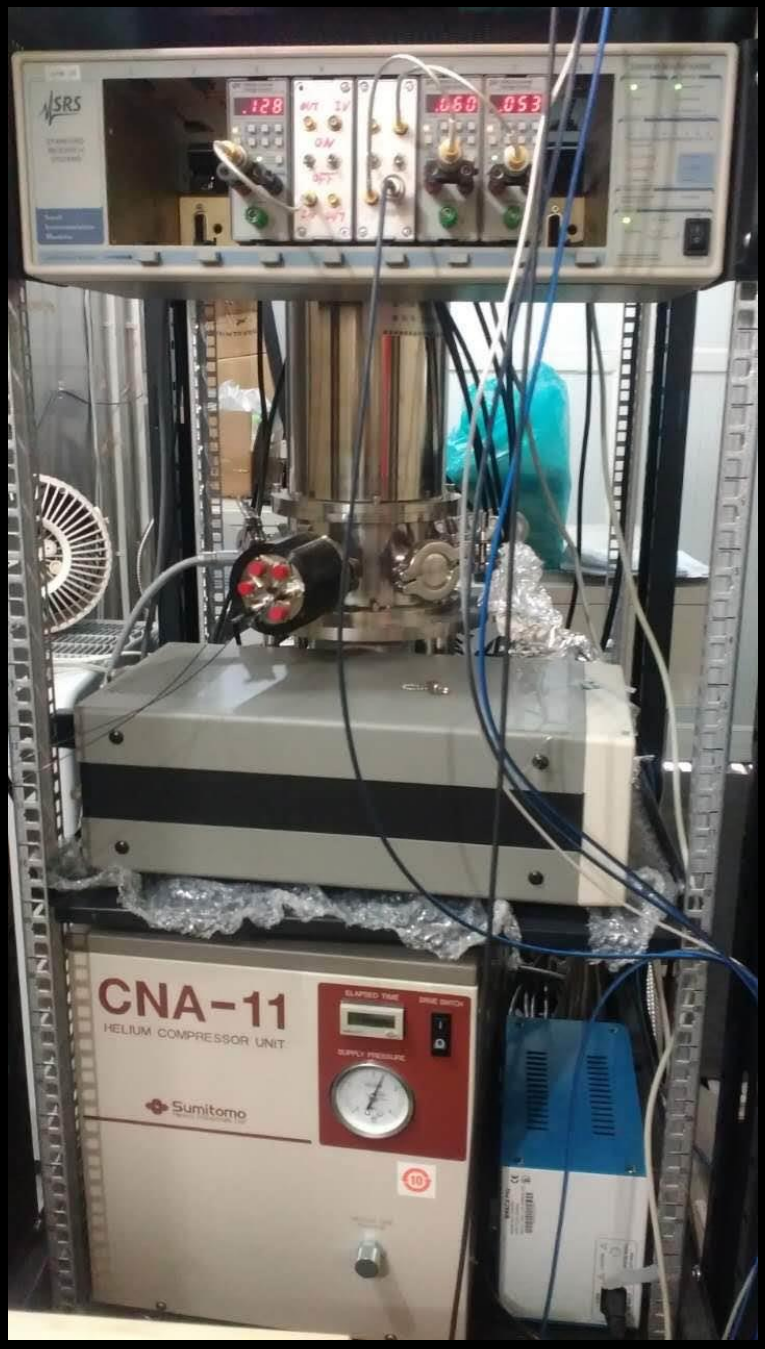
- A multilayer film bandpass filter to suppress the dark counts
- High transmittance over 88%

X. Yang, *et al*. Opt. Express **22**, 16267 (2014)

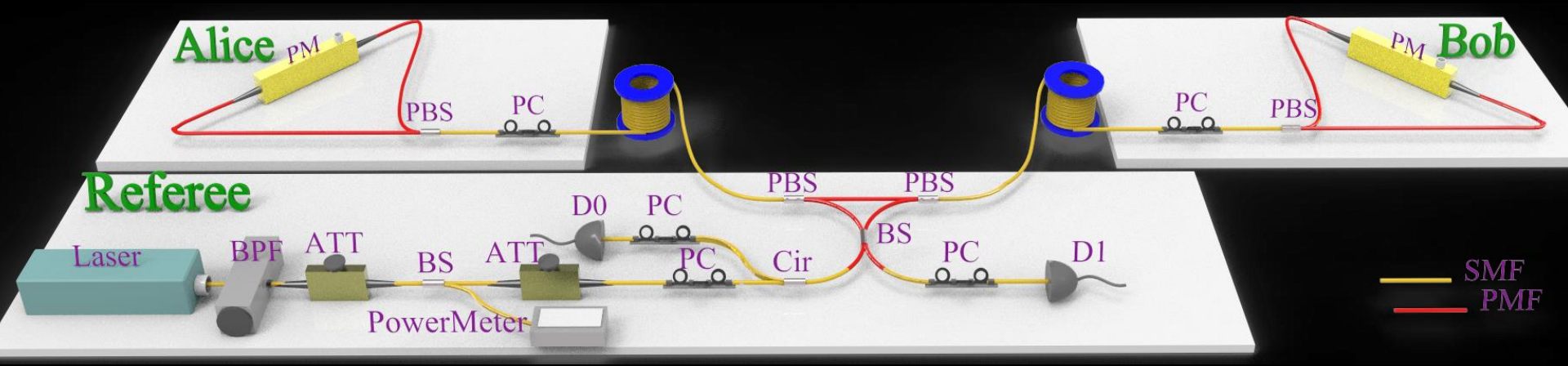
SNSPD



- **Dark count: 0.11 cps**
- Quantum efficiency: 45.6%

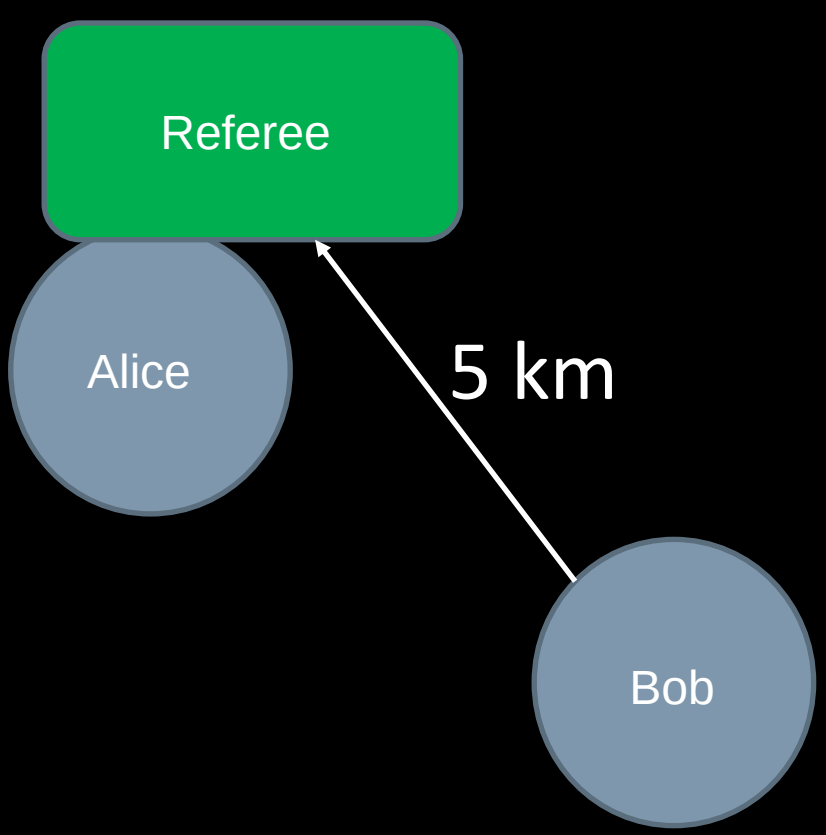


Experimental setup: Sagnac interferometer



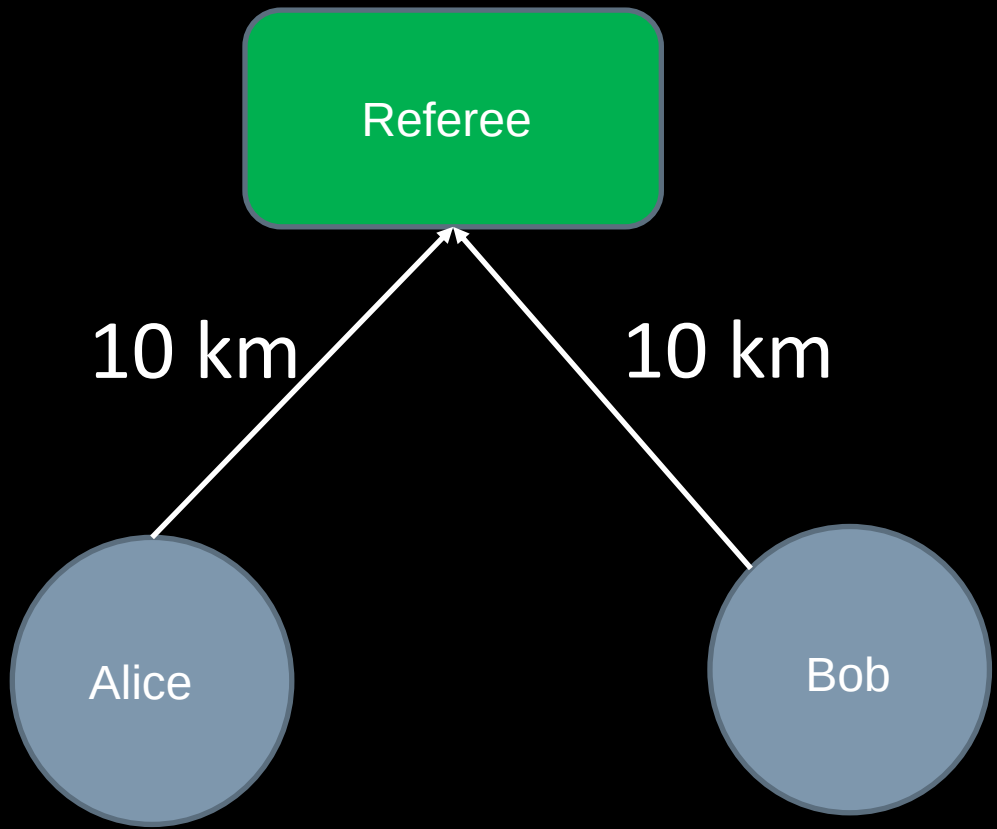
- Automatic compensation of the phase differences between the two pulses
- High interference visibility > 96% over 20 km fiber
- Stable interference up to 24 hours

Comparison between P&P and Sagnac



Plug&Play

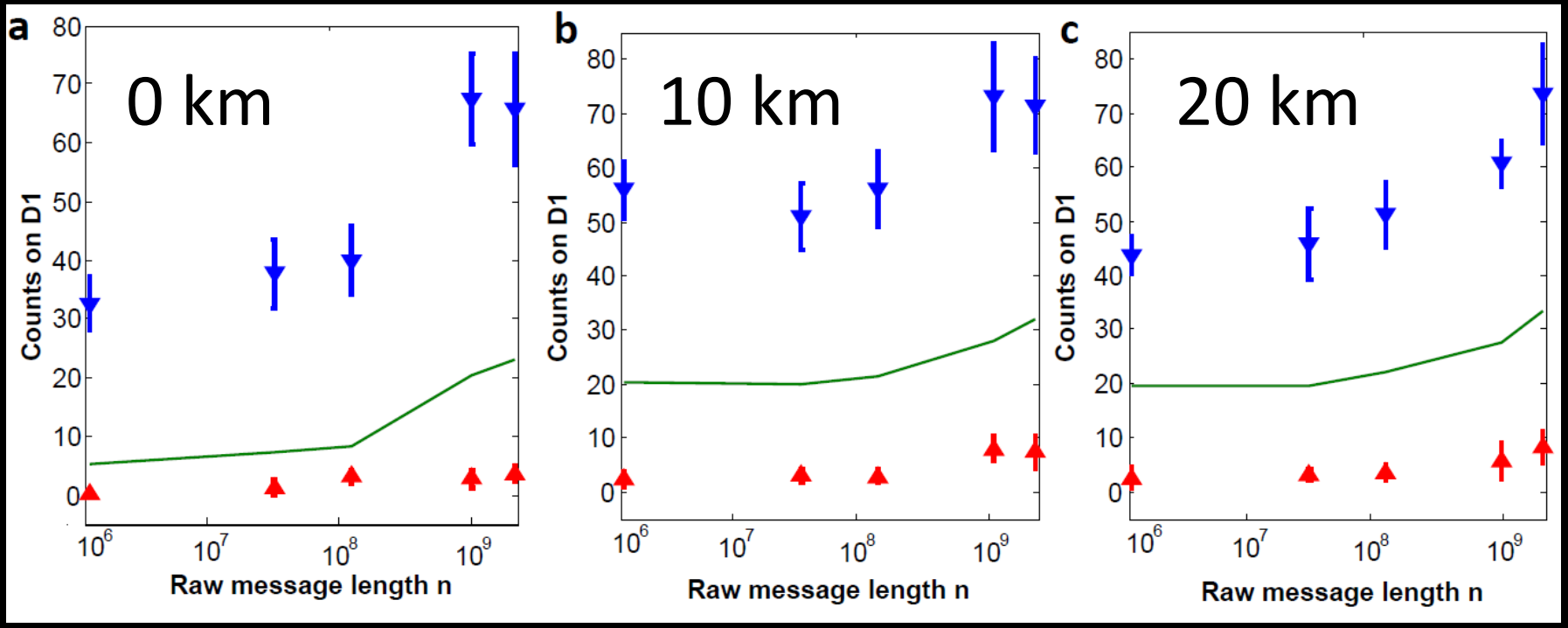
Xu *et al.* Nature Commun. **5**, 8735 (2015)



Sagnac

Guan *et al.* Phys. Rev. Lett. **116**, 240502 (2016)

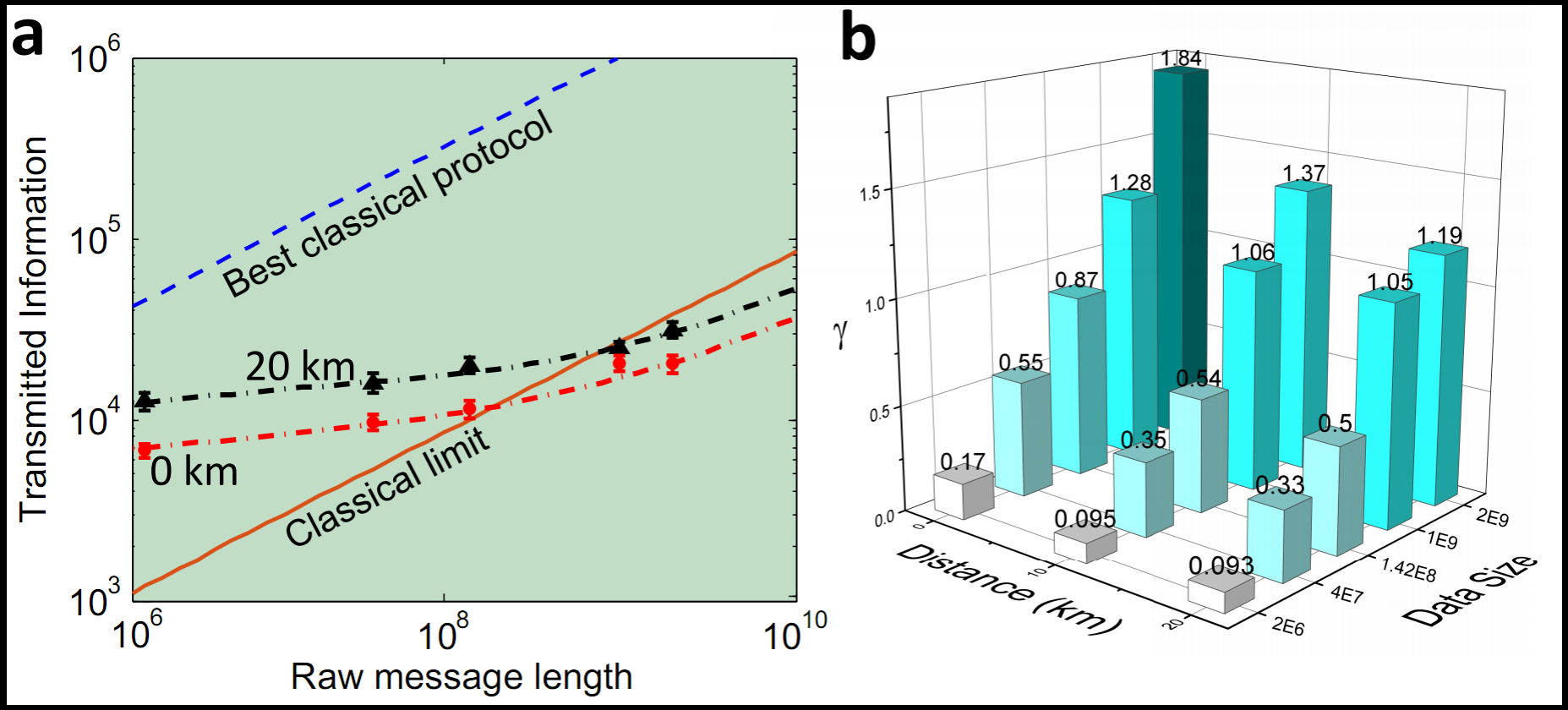
Counts on the ‘different’ detector



- Red: same message
- Blue: different message (code-word distance 0.22)
- Green: pre-determined threshold
- Mean photon per pulse=10^-7

Results

$$\gamma \sim \frac{\sqrt{n/2 \ln 2}}{Q}$$



- 2 orders of magnitude lower than best classical protocol
- Beat the classical limit by 84% (19%) at 0 (20) km

Fingerprint two real videos

TABLE 4: Quantum fingerprinting results for two real videos.

Raw message length (n)	2×10^9
Encoded message length (m)	8.34×10^9
Communication time (s)	333.6
μ_a	656.6 ± 52.5
μ_b	645.7 ± 51.7
Q (both Alice and Bob)	32690.2 ± 2615.22
γ (limitation)	1.14 ± 0.091
γ (best algorithm)	43.8 ± 3.5
$D_{1,th}$	35.9
D_1 when using same video	8.8 ± 3.3
D_1 when using different video	153.5 ± 12.9
ϵ	1.34×10^{-16}

- Beat the classical limit by 14% over 20 km fiber
- Use ~1300 photons only to encode 2 Gbits message!

Discussion

- Limitations
  - Transmit exponentially less information, but at a cost of using quadratically more optical pulses
  - Two-way system: redundant channel uses
  - Local synchronization
- Improvements
  - Multiplexing: WDM
  - Independent lasers + phase locking
  - Distributed synchronization

Summary: Alice and Bob have their quantum fingerprints checked

physicsworld.com

(Mar 23, 2016)

- Demonstrate a quantum fingerprinting system that for the first time beats the ultimate classical limit to transmitted information.

- Our experiment opens the door to other potentially more useful applications, such as better large-scale integrated circuits and more energy-efficient communication.

Feihu Xu: fhxu@mit.edu

F. Xu *et al.* Nature Commun. **5***, 8735* (2015)
J. Guan, F. Xu *et al.* Phys. Rev. Lett. **116**, 240502 (2016)