Progress towards quantum-based random-number generation using entangled photons

Krister Shalm, Evan Meyer-Scott, Bradley G. Christensen, Peter Bierhorst, Michael A. Wayne, Martin J. Stevens, Thomas Gerrits, Scott Glancy, Michael S. Allman, Kevin J. Coakley, Shellee D. Dyer, Carson Hodge, Adriana E. Lita, Varun B. Verma, Camilla Lambrocco, Edward Tortorici, Alan Migdall, Yanbao Zhang, Joshua C. Bienfang, Richard P. Mirin, Emanuel Knill, and Sae Woo Nam, Andrea Rommal, Stephen Jordan, Alan Mink, Yi-Kai Liu, Paulina Kuo, Xiao Tang, Rene Peralta, … others

NIST 05-02-2016

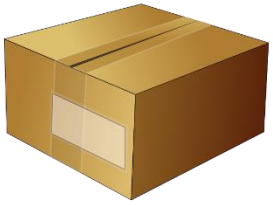
NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Outline

- Contrast classical and quantum descriptions
- Einstein's objection to quantum mechanics
- Bell inequalities
- Loophole-free Bell Inequality
- Our experiment
- Random bits from a loophole-free Bell test

Classical vs. Quantum

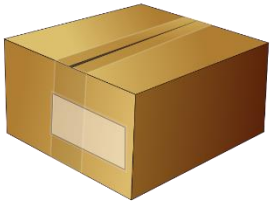
Classical world: Objects have physical properties that are independent of observation; measurement only *reveals* them.



or

Color of the object is set before we open the box.

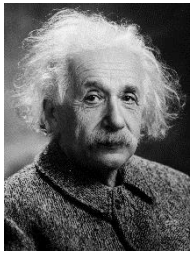
Quantum world: An object's physical properties are specified *by* the act of measurement; objects are described by states that specify the probabilities of possible measurement outcomes;



$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|\blacksquare\rangle + |\blacksquare\rangle)$$

Color is indeterminate until we open the box.

Notable physicists took a dim view of this picture.



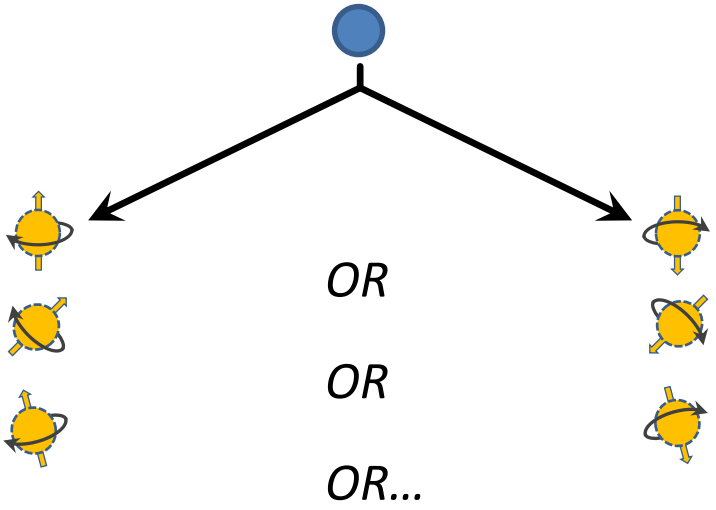
Einstein's criticism: entanglement

Quantum mechanics allows for states with well-defined properties to be composed of multiple particles. Quantum mechanics need not specify *how* the properties of the constituent particles comprise the total state.

Example: Spontaneous decay

Parent: zero angular momentum

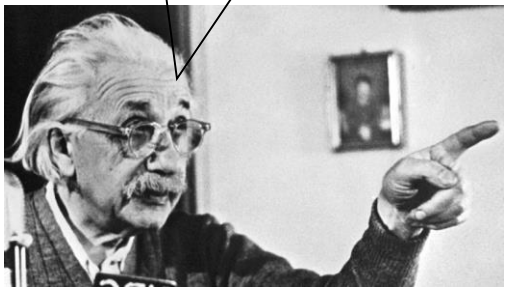
Daughters: *net* zero angular momentum



QM only specifies the property of the total state of the two particles.

The angular momentum of one particle can depend on how you choose to observe the other particle.

spukhafte Fernwirkungen



"No reasonable definition of reality could be expected to permit this."

Alpha Centauri

Elements of reality → predicatbility

MAY 15, 1935 PHYSICAL REVIEW VOLUME 47

Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?

A. EINSTEIN, B. PODOLSKY AND N. ROSEN, *Institute for Advanced Study, Princeton, New Jersey*

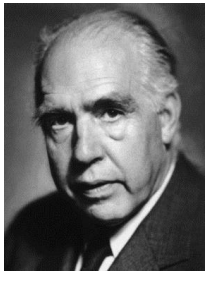
(Received March 25, 1935)

In a complete theory there is an element corresponding to each element of reality. A sufficient condition for the reality of a physical quantity is the possibility of predicting it with certainty, without disturbing the system. In quantum mechanics in the case of two physical quantities described by non-commuting operators, the knowledge of one precludes the knowledge of the other. Then either (1) the description of reality given by the wave function in quantum mechanics is not complete or (2) these two quantities cannot have simultaneous reality. Consideration of the problem of making predictions concerning a system on the basis of measurements made on another system that had previously interacted with it leads to the result that if (1) is false then (2) is also false. One is thus led to conclude that the description of reality as given by a wave function is not complete.

"While we have thus shown that the wave function does not provide a complete description of the physical reality, we left open the question of whether or not such a description exists. We believe, however, that such a theory is possible."

➔ Hidden variables

Other notable physicists took a dim view of this picture.



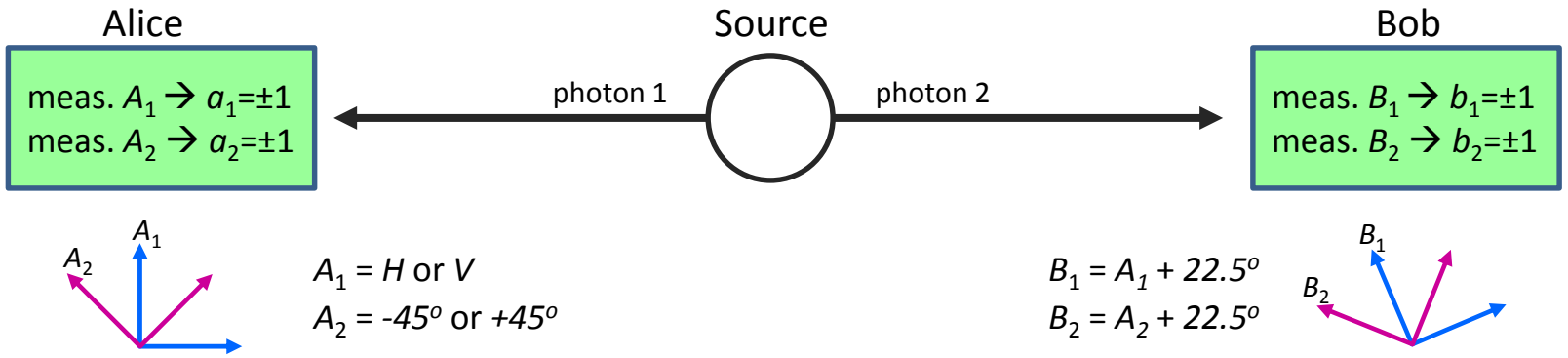
The Bell Inequalities

1964 John S. Bell proposed an experiment that, with sufficient statistics, distinguishes between systems with “real” (but perhaps hidden) pre-existing values and non-local entangled systems as described by quantum mechanics; a test of “local-realism”.

For our purpose, a violation of a Bell inequality certifies that the measurement outcomes could not have been predicted by any amount of prior knowledge.

The CHSH Bell Inequality

A Bell test well suited to polarization entangled photons



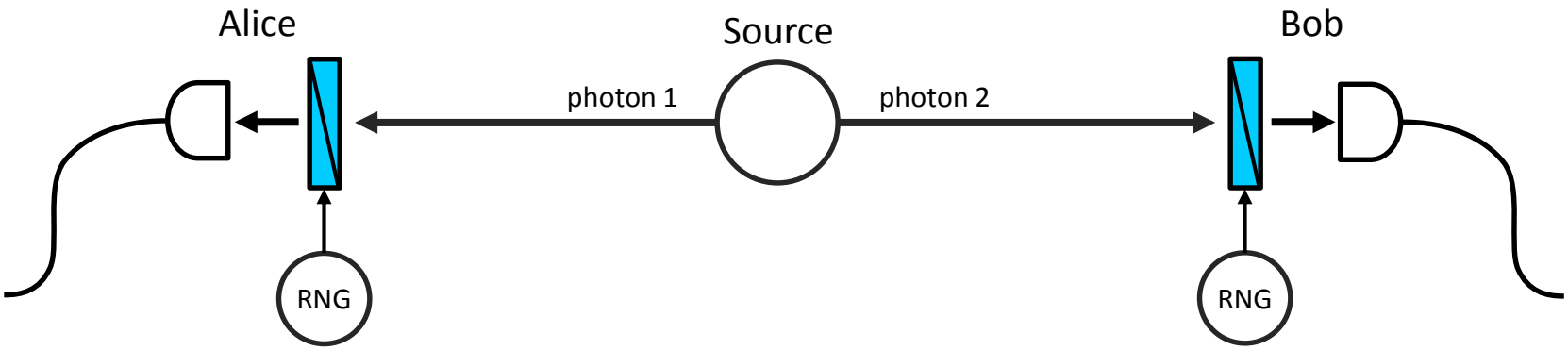
1. Photons are prepared and sent simultaneously to Alice and Bob for independent measurement.
2. Each randomly choose one of two measurements, A_i, B_j.
3. Alice and Bob measure their photon's polarizations and record results a_i, $b_j \in \{1, -1\}$.
4. Repeat to build statistics → calculate expectation values

Analyzed with "classical" inputs: $|E(A_1B_1) + E(A_2B_1) + E(A_2B_2) - E(A_1B_2)| \leq 2$

Analyzed with an input entangled state such as: $|\psi\rangle = \frac{1}{\sqrt{2}}(|VH\rangle - |HV\rangle)$ ← anti-symmetric

$$|E(A_1B_1) + E(A_2B_1) + E(A_2B_2) - E(A_1B_2)| \leq 2\sqrt{2}$$

Assumptions Lead to Loopholes



Some of the main loopholes:

Locality Loophole: The photons must not be able to send signals to one another so as to collude
→ Space-like separated

Freedom of Choice Loophole: Alice and Bob must be free to make measurement decisions independently → High-quality, low-latency RNGs

Fair Sampling/Detection Loophole: Must collect and detect enough of the pairs from the source to
→ Advances in optics and single-photon detectors

Difficult to close *all* loopholes simultaneously. Many experimental tests since 1972.

Delft
B. Hensen, H. Bernien, A. E. Dreau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellan, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau, and R. Hanson, Nature 526, 682.

– Published 29 October 2015.

NIST
Lynden K. Shalm et al., Phys. Rev. Lett. 115, 250402

– Published 16 December 2015

Vienna
Marissa Giustina, Marijn A. M. Versteegh, Sören Wengerowsky, Johannes Handsteiner, Armin Hochrainer, Kevin Phelan, Fabian Steinlechner, Johannes Kofler, Jan-Åke Larsson, Carlos Abellán, Waldimar Amaya, Valerio Pruneri, Morgan W. Mitchell, Jörn Beyer, Thomas Gerrits, Adriana E. Lita, Lynden K. Shalm, Sae Woo Nam, Thomas Scheidl, Rupert Ursin, Bernhard Wittmann, and Anton Zeilinger, Phys. Rev. Lett. 115, 250401

– Published 16 December 2015

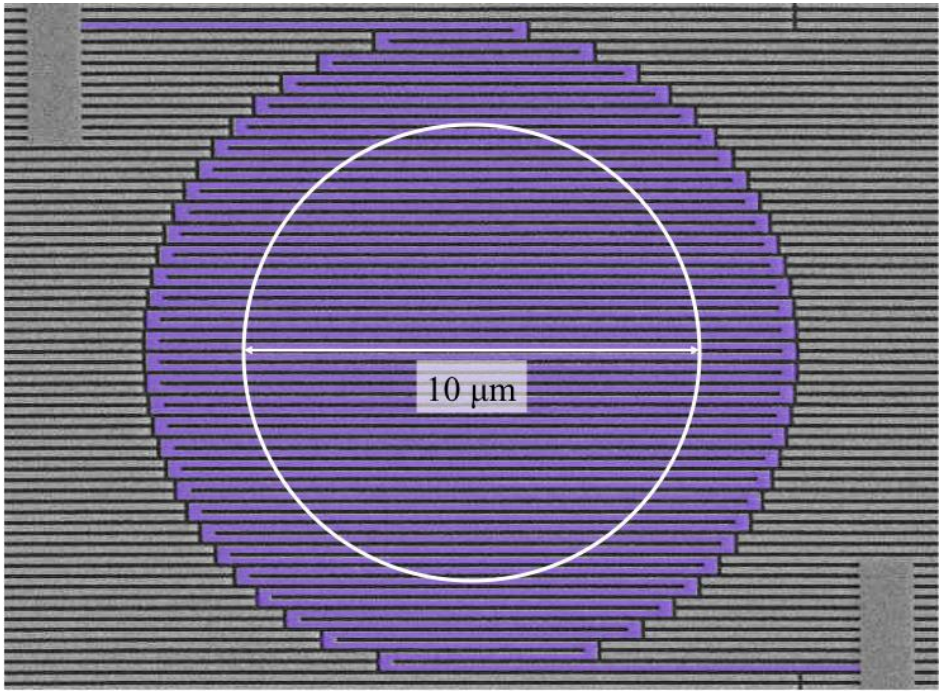
Photons: Detection Loophole

NIST has developed high efficiency, high-speed single-photon detectors based on superconducting nanowires

Efficiency > 90 %

Timing jitter < 160 ps

Operates < 3 K

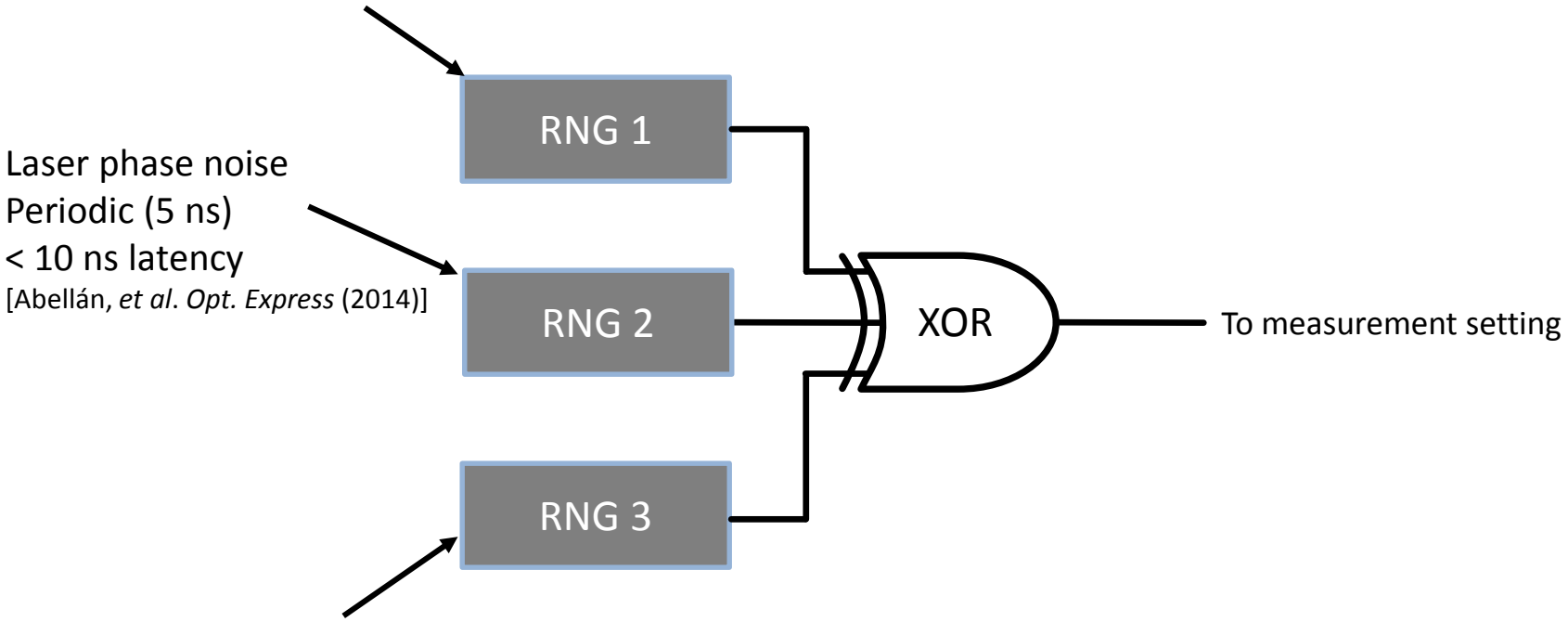


Marsili *et al.* Nature Photonics, **7**, 210 (2013).

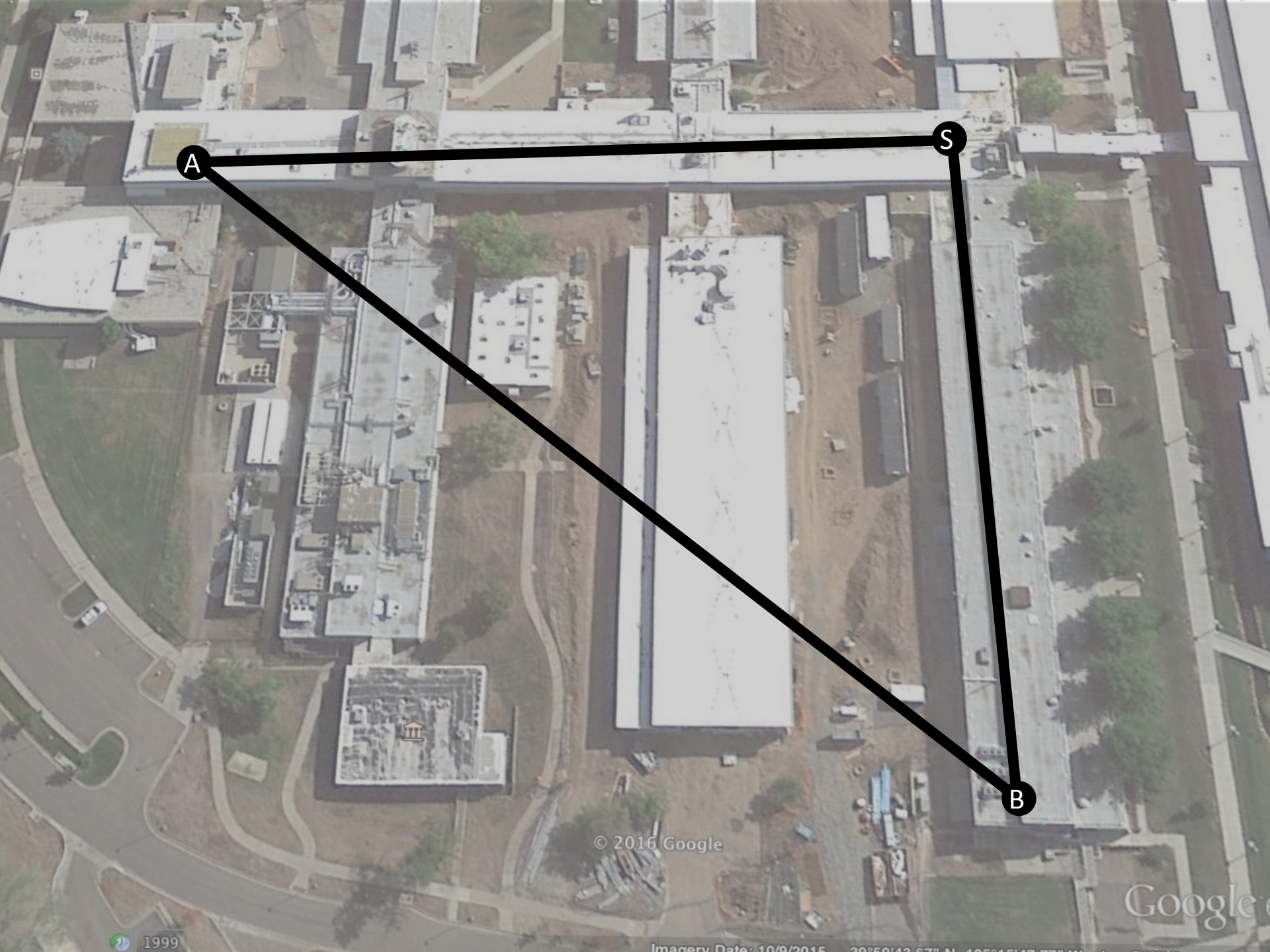
Freedom of Choice Loophole

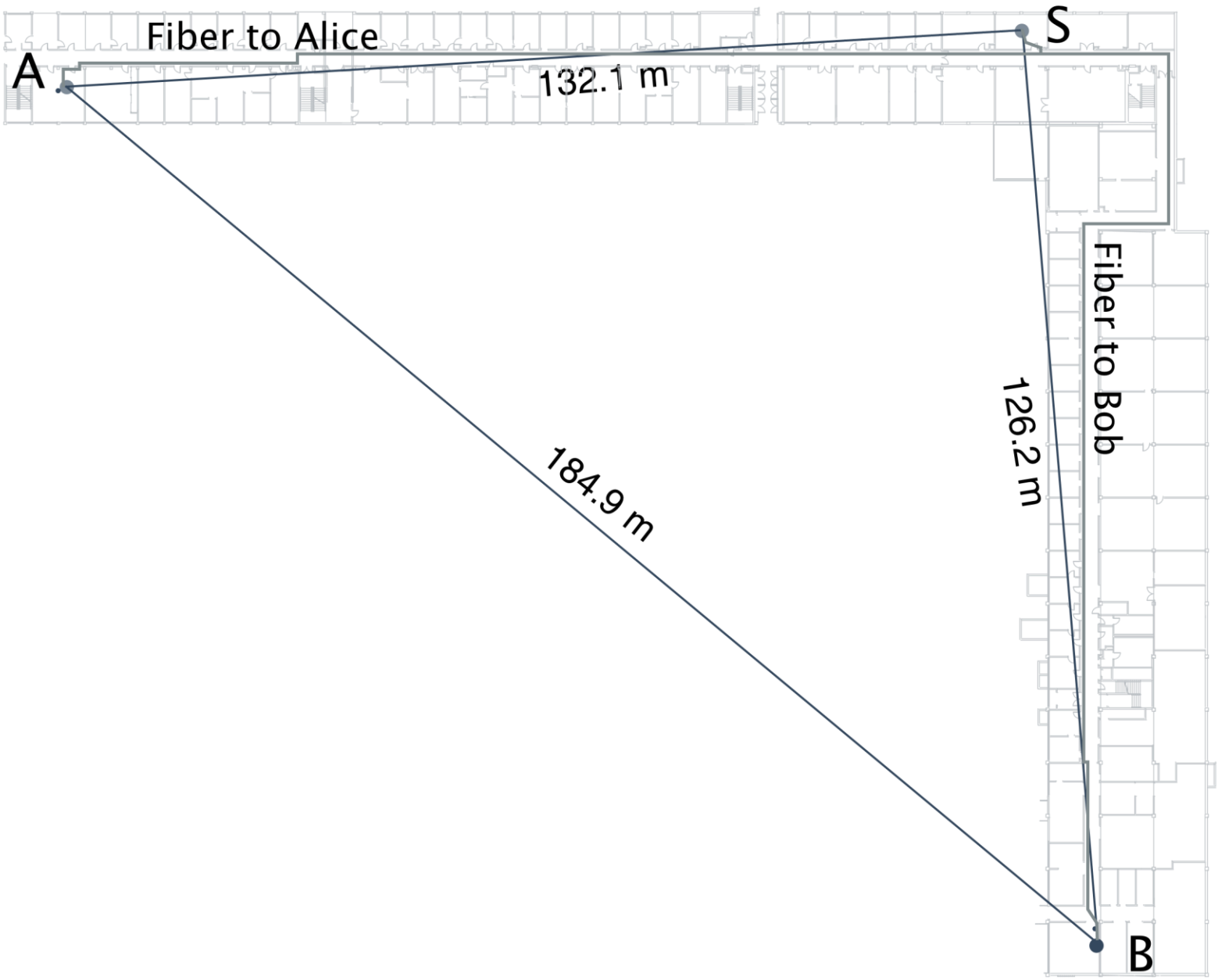
Photon sampling
Asynchronous (triggered)
< 3 ns latency
[M. Wayne, *et al., To be submitted*]

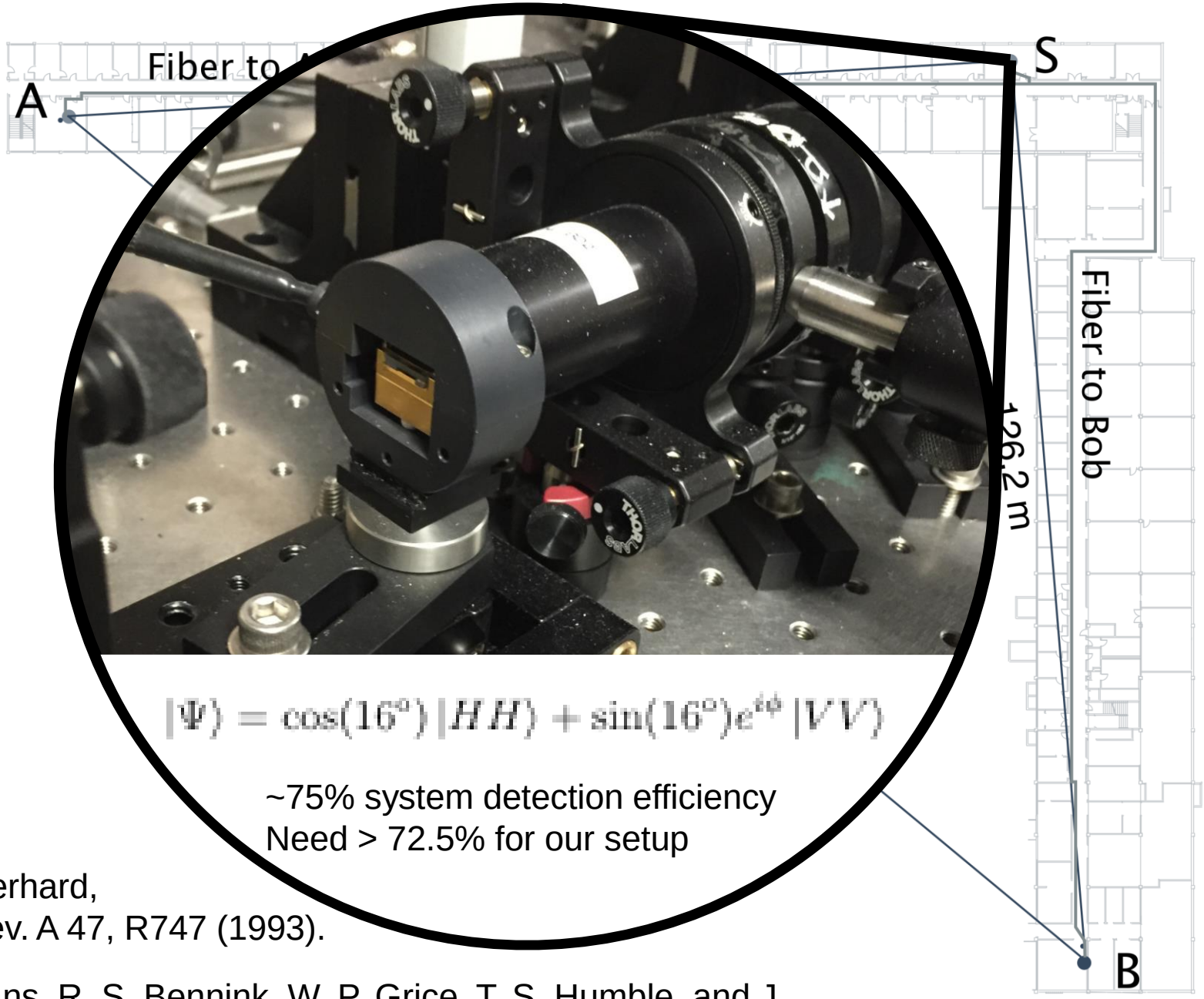
Laser phase noise
Periodic (5 ns)
< 10 ns latency
[Abellán, *et al*. *Opt. Express* (2014)]



Hashed pre-determined data

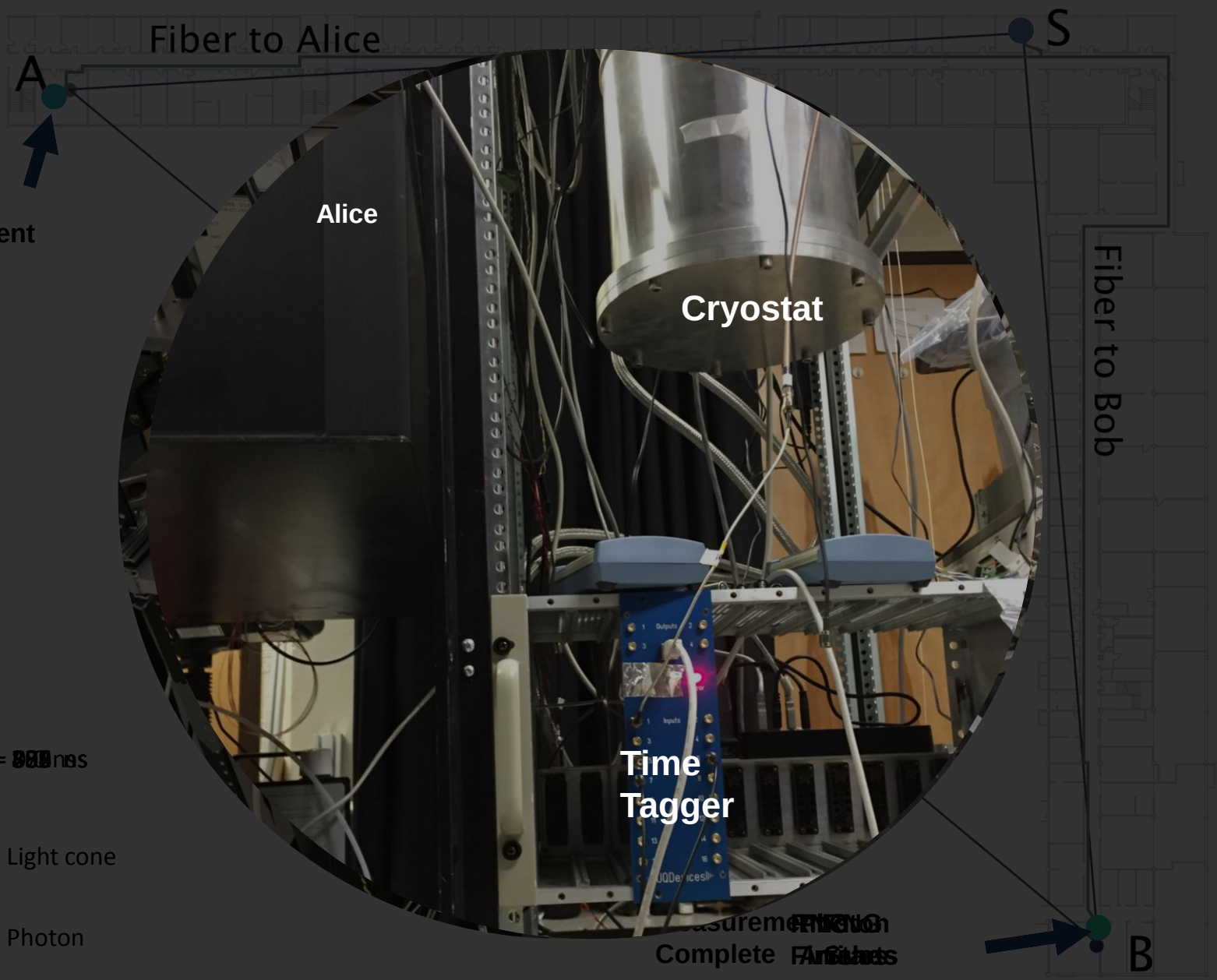

A
S
B
© 2016 Google
1999
Imagery Date: 10/9/2015
Google


Fiber to Alice
A
S
132.1 m
Fiber to Bob
126.2 m
184.9 m
B



P. H. Eberhard,
Phys. Rev. A 47, R747 (1993).

P. G. Evans, R. S. Bennink, W. P. Grice, T. S. Humble, and J. Schaake, Phys. Rev. Lett. 105, 253601 (2010).


Fiber to Alice
A
S
Alice
Cryostat
Fiber to Bob
Time
Tagger
Light cone
Photon
B

Hypothesis testing

The violation observed in a Bell test can be quantified by an observed p-value (*the probability that a local realistic system could have produced violation at least as high*)

Prediction-based-ratio (PBR) method [1, 2] to calculate p-values

- does not make assumptions about Bell test distribution (e.g. std. dev.)
- asymptotically optimal in the rate at which confidence in p-values is gained
- based on Markov inequality

First Bell test run in September 2015.

- trial rate ≈ 100 kHz
- run lengths 30 minutes to few hours
- p-values as small as 5.9×10^{-9}

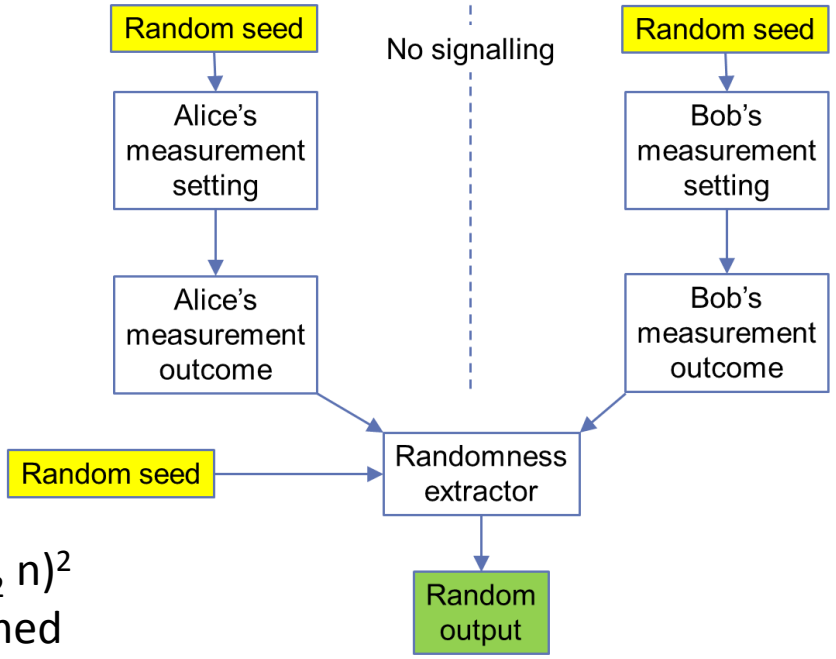
We're working on quantifying min-entropy of the output, which will then be used in the Trevisan extractor

[1] Yanbao Zhang et. al, Phys. Rev. A 84, 062118 (2011)

[2] P. Bierhorst, J. Phys. A 48, 195302 (2015)

Trevisan Randomness Extractor

Input: a weakly random string with a bounded min-entropy
Input: a uniformly distributed seed smaller than input string
Output: and generates an ε-close uniformly distributed random string not exceeding the input entropy.



<u>Advantages</u>

- Seed d is smaller than input string n: $d \sim O(\log_2 n)^2$
- Strong extractor; seed randomness not consumed

<u>Characteristics</u>

- Each output bit is independent, thus Trevisan is parallelizable
- Uses 2 hashes to produce each output bit from the string and the seed
  - Polynomial (Reed Solomon) and Parity (Hadamard)

Conclusion

Fundamental tests of quantum mechanics as a source of certifiable uncertainty
- reduces (minimizes?) the options for an attacker

First-pass experiment has been completed
- expect to scale to 1 MHz this year

New terrain for randomness extraction
- working on connecting to data analysis methods

Suitable for the NIST randomness beacon

Thanks!