Title: Protocols and Implementations of Quantum Position Verification

Speakers: Eric Chitambar, Paul Kwiat

Collection: QPV 2023: Advances in quantum position verification

Date: September 20, 2023 - 9:30 AM

URL: https://pirsa.org/23090017

Protocols and Implementations of Quantum Position Verification

Eric Chitambar

Paul Kwiat

Ian George

Andrew Conrad

QPV 2023: Advances in quantum position verification

NSF

UNIVERSITY OF ILLINOIS URBANA-CHAMPAIGN

Q-NEXT

Protocols and Implementations of Quantum Position Verification

and Some Related Work on Relativistic QKD

Eric Chitambar **Paul Kwiat**

Ian George **Andrew Conrad**

QPV 2023: Advances in quantum position verification

NSF

UNIVERSITY OF ILLINOIS URBANA-CHAMPAIGN

Q-NEXT

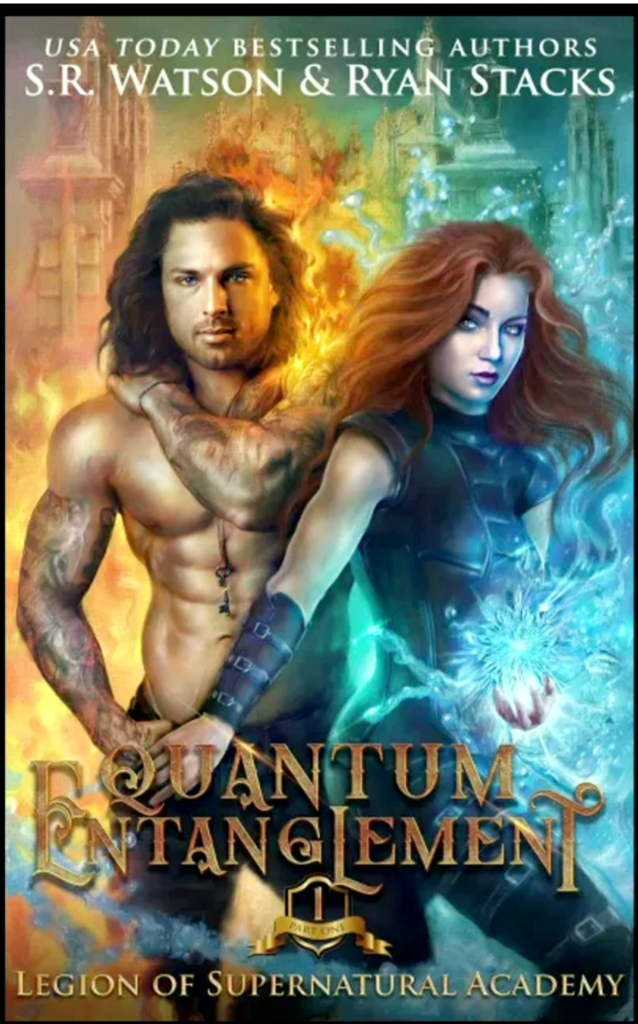
Outline

Principles and tools for QPV

1. Relativistic QKD
2. QPV and state discrimination

Drone-based QPV protocol

3. An entanglement-distribution QPV protocol
4. Experimental implementation

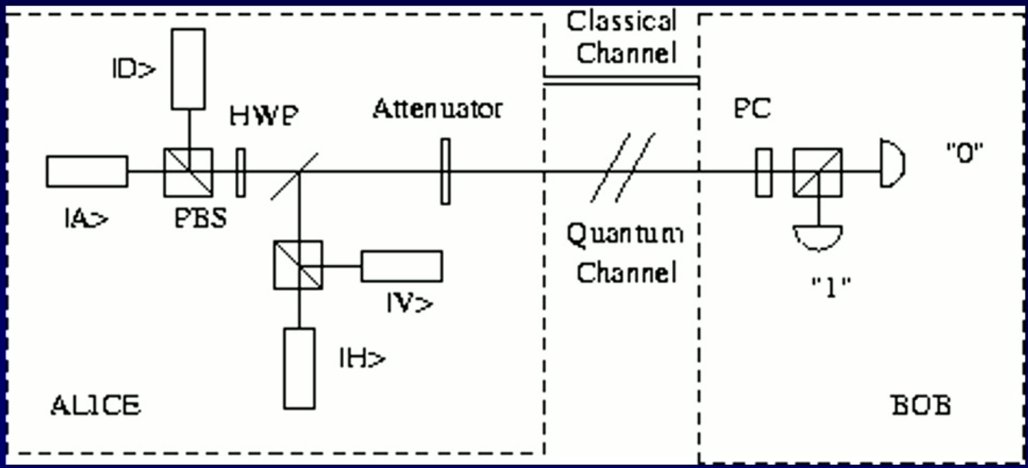


Release Date: October 3, 2019
Genre: Paranormal Romance

Genesis and Elysian are quantum entangled for a singular purpose. Their recruitment to the Legion of Supernatural Academy is unexpected but vital to the future of humanity. This unique series takes the world of supernatural academies to new heights with twisted tales, suspense-driven fantasy, and self-discovery.

Part I: Relativistic QKD

BB84 (Six-state) Protocol



Alice transmits a photon in one of **four** (six) states.

Bob measures the photon in one of **two** (three) bases.

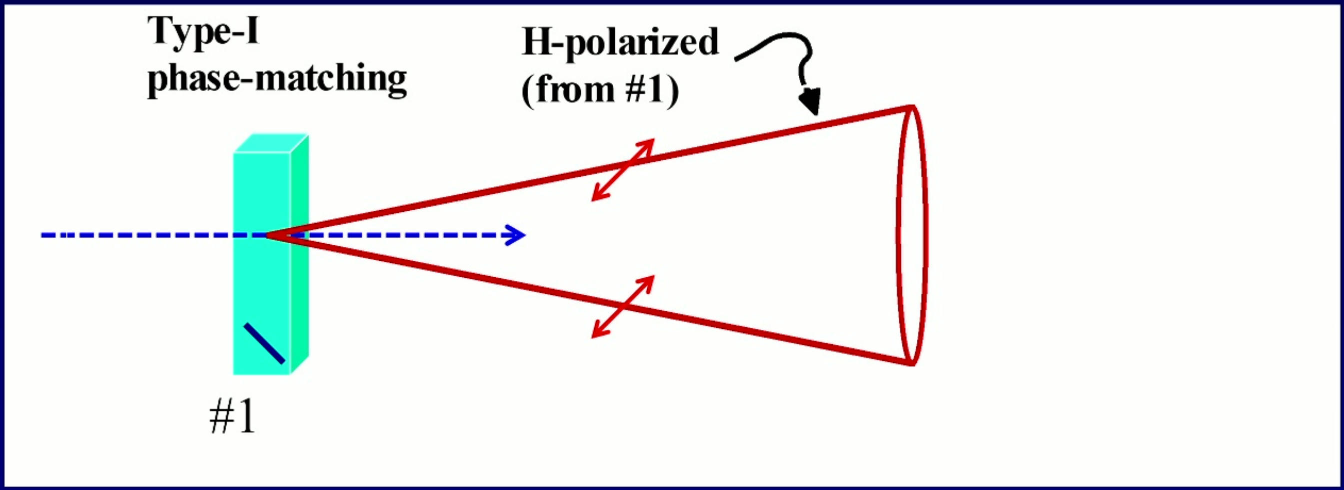
Alice and Bob sift out the trials -50% (33%) where they used same basis.

The sifted keys have “perfect” correlation.

An intrusive eavesdropper induces errors up to 25% (33%).

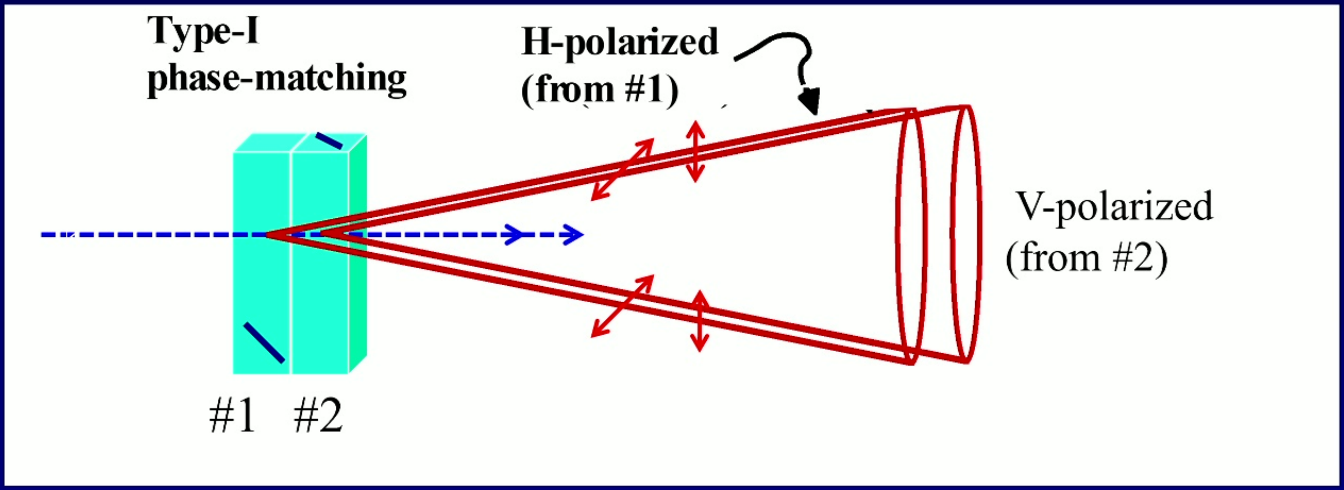
How We Make Entanglement

"Spontaneous DownConversion": high-energy parent photon can split into two daughter photons (with same polarization)



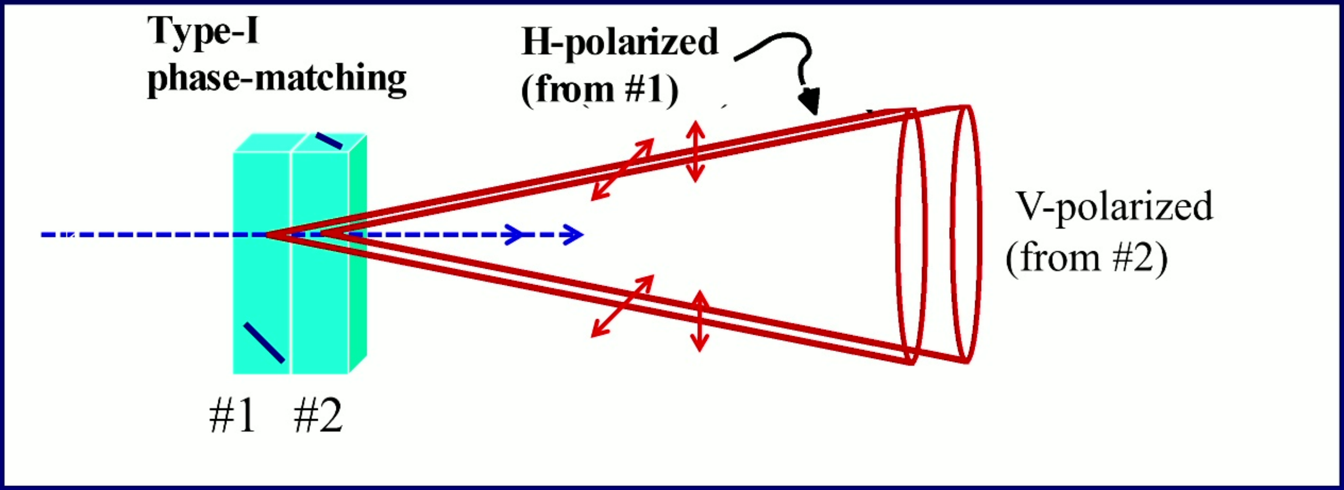
How We Make Entanglement

"Spontaneous DownConversion": high-energy parent photon can split into two daughter photons (with same polarization)



How We Make Entanglement

"Spontaneous DownConversion": high-energy parent photon can split into two daughter photons (with same polarization)

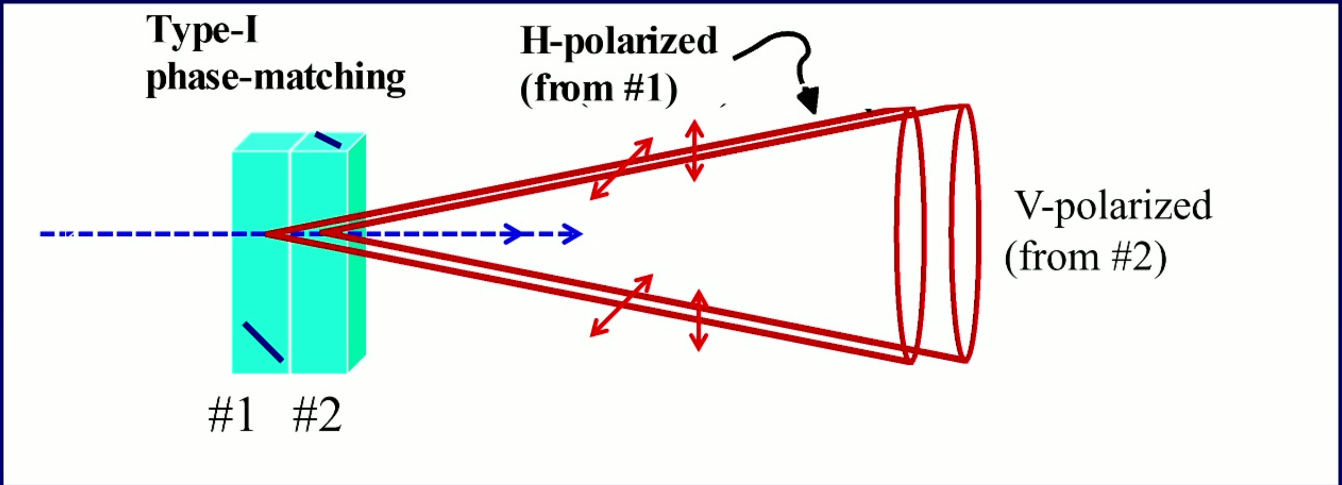


We don't know WHICH crystal created the pair of photons, but we know they both came from the same crystal

→ they MUST have the same polarization: $|\psi\rangle = |H\rangle|H\rangle + |V\rangle|V\rangle$

How We Make Entanglement

"Spontaneous DownConversion": high-energy parent photon can split into two daughter photons (with same polarization)

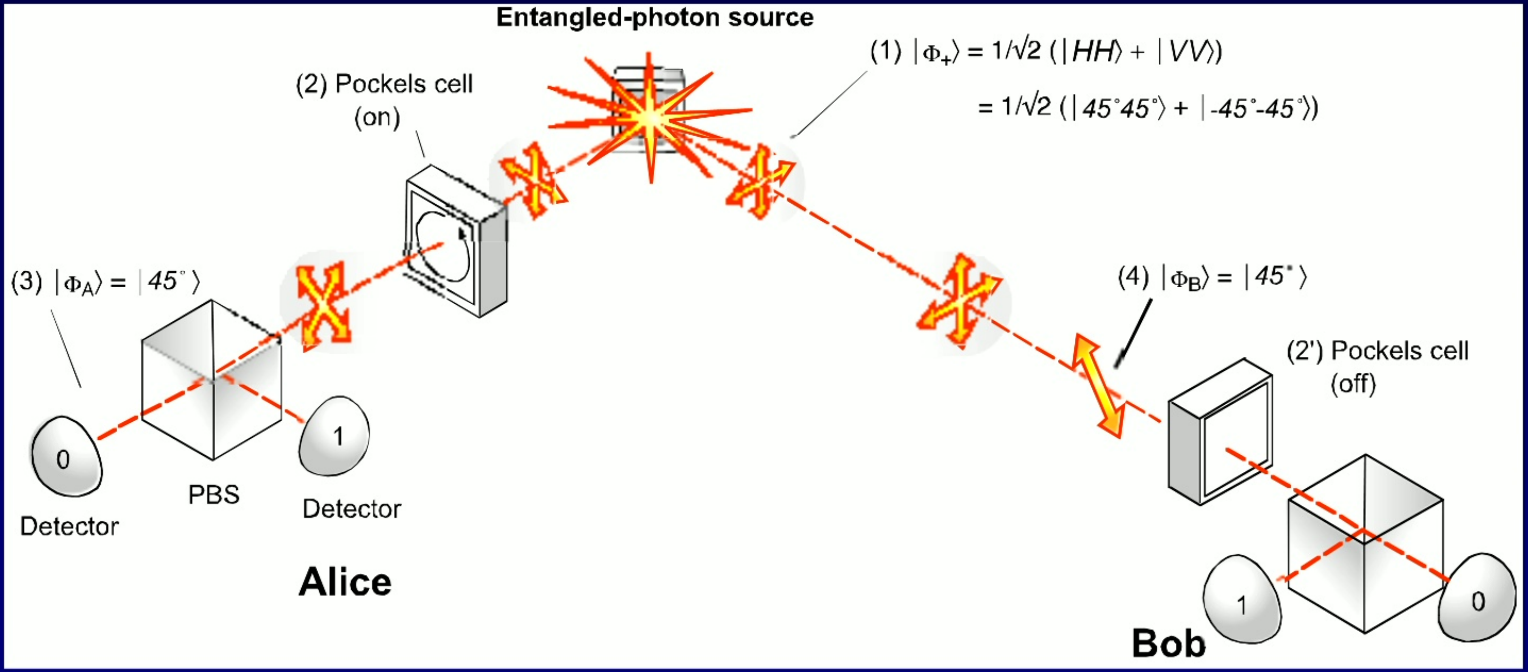


Foreshadowing: Changing the pump polarization → alters which/how much entanglement

We don't know WHICH crystal created the pair of photons, but we know they both came from the same crystal

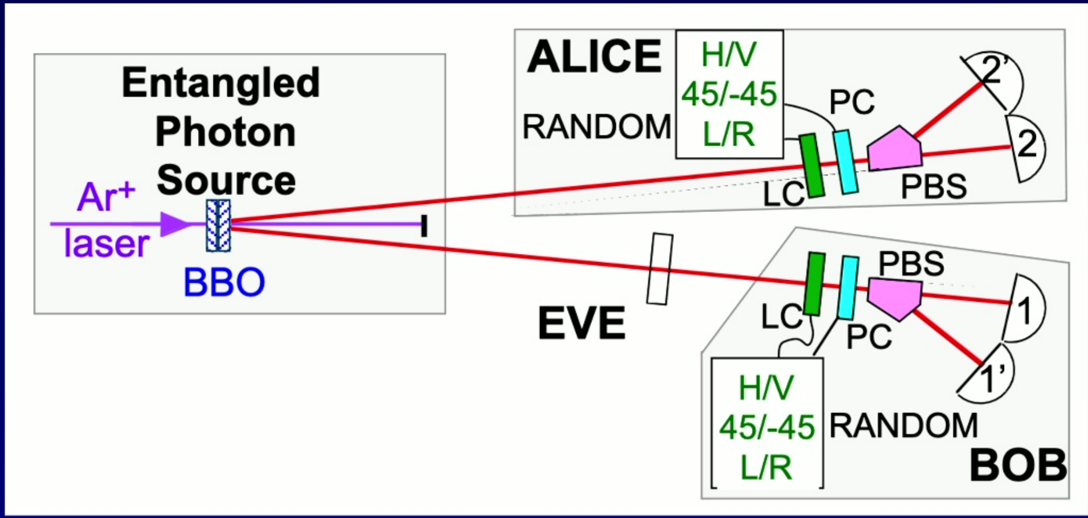
→ they MUST have the same polarization: $|\psi\rangle = |H\rangle|H\rangle + |V\rangle|V\rangle$

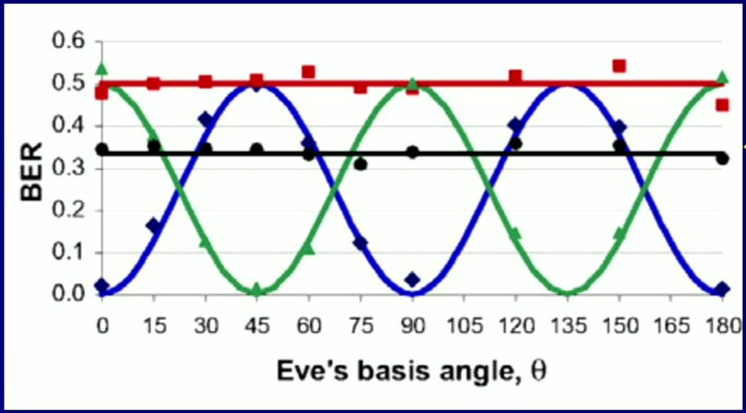
Entangled-Photon Quantum Cryptography



- Alice & Bob randomly measure polarization in the (H/V) or the (+45/-45) basis.
- Discuss via a "public channel" which bases they used, *but not the results*.
- Discard cases (50%) where they used different bases → uncorrelated results.
- Keep cases where they used the same basis → *perfectly correlated results!*
- Define H ≡ "0" ≡ 45, V ≡ "1" ≡ –45. **They now share a secret key.**

Experimental Realization of Six-State QKD Protocol
{D. Enzer, PGK et al., New Journal Physics 4, 45.1 (2002)}

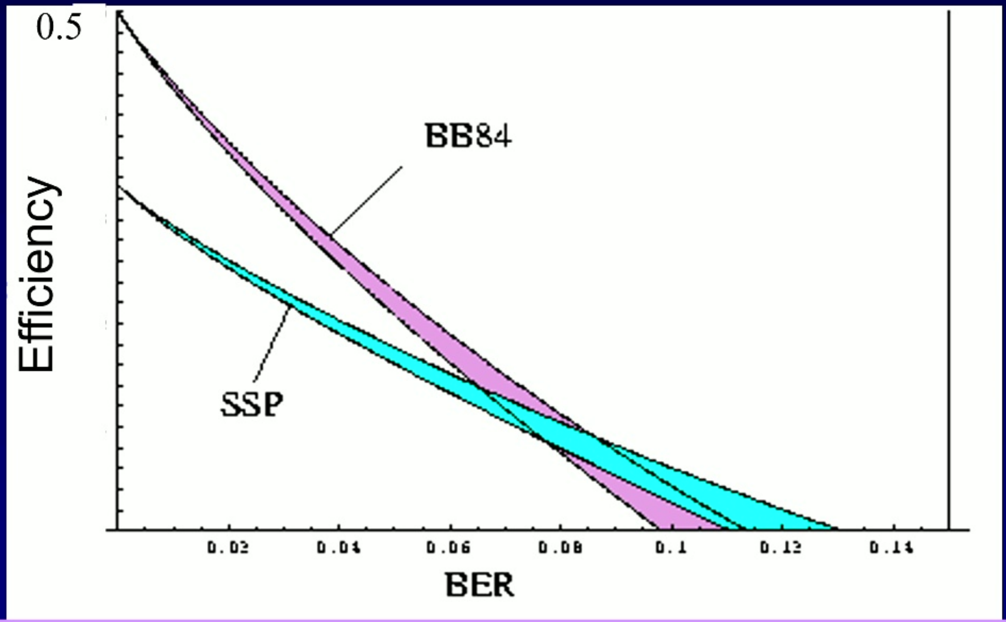




Total BER is 33%, independent of attack strategy

(cf. to 25% BER in BB84 4-state protocol)

The Trouble with Sifting



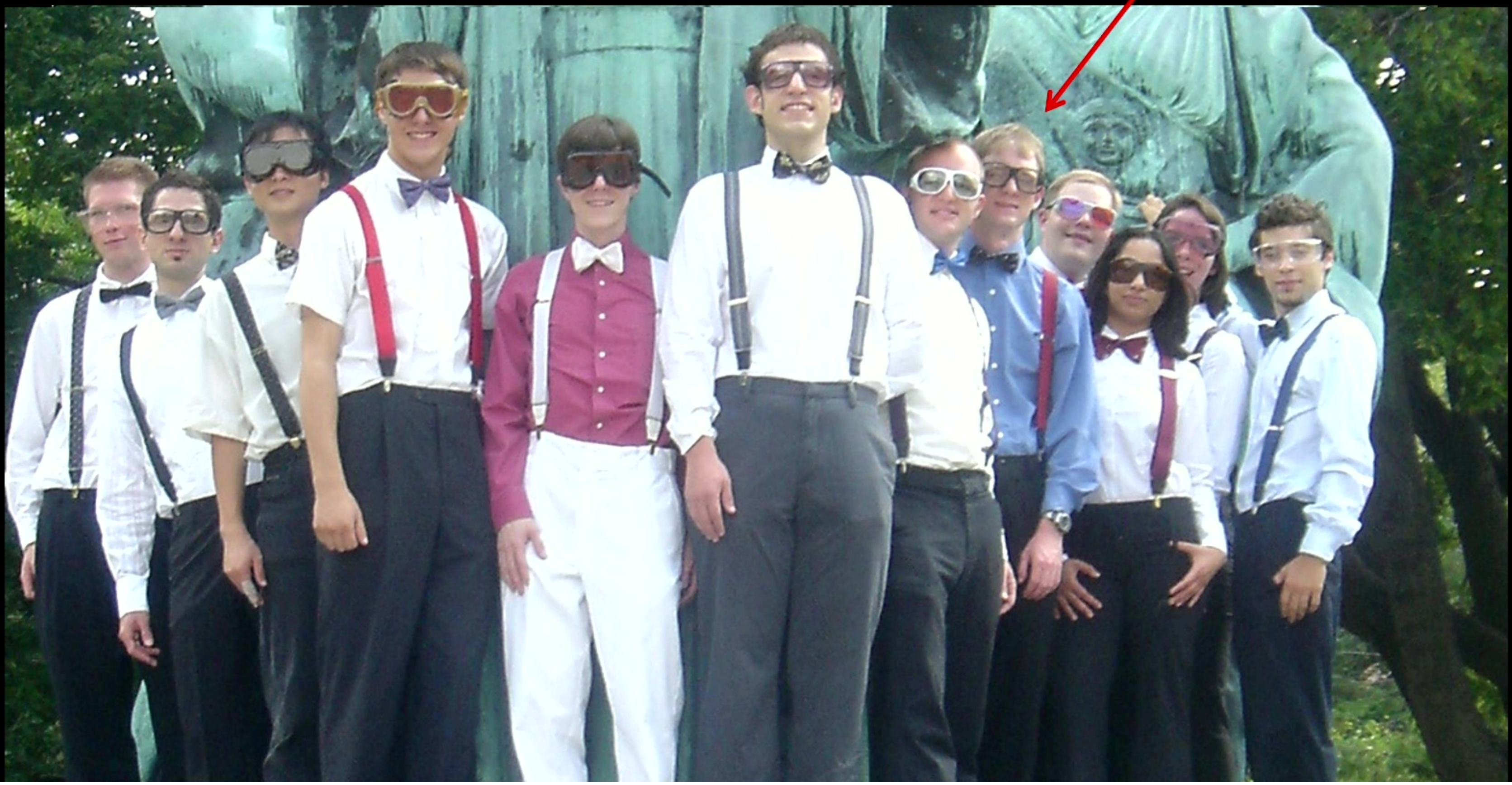
BB84: sifting ⇒ 50% inefficiency
Six-State Protocol: sifting ⇒ 66% inefficiency

PGK Group, Circa 2006

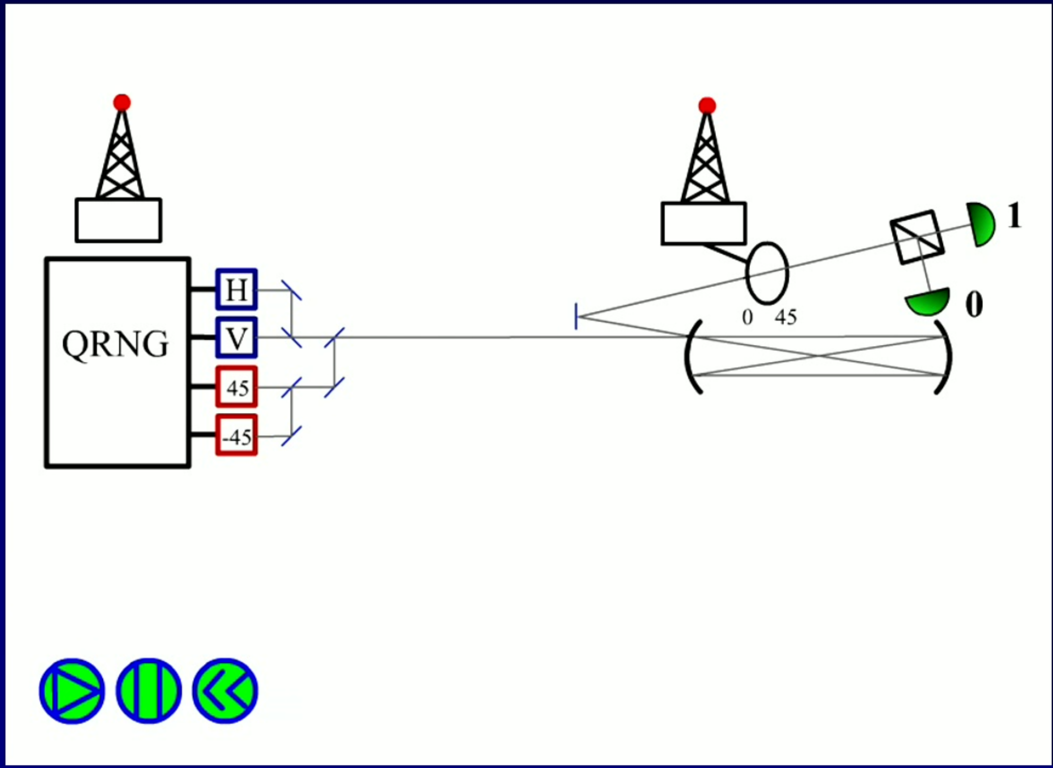
Graduate Students: Joe Altepeter, Julio Barreirro, Onur Hosten, **Evan Jeffrey**, Nicholas Peters, Radhika Rangarajan, Aaron VanDevender, Joseph Yasi

Undergraduates: Kyle Arnold, Gleb Akselrod, Rachel Hillmer, Kevin Uskali

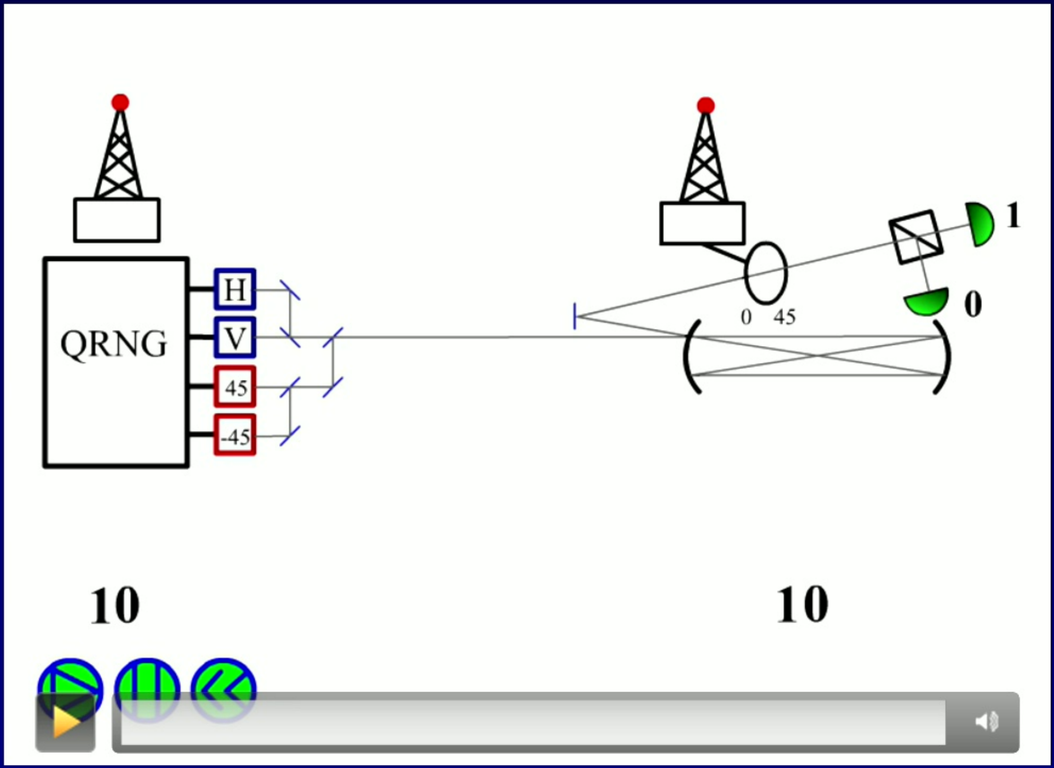
Associated Theory Post-Doc: Tzu-Cheih Wei



"Relativistic" Quantum Cryptography

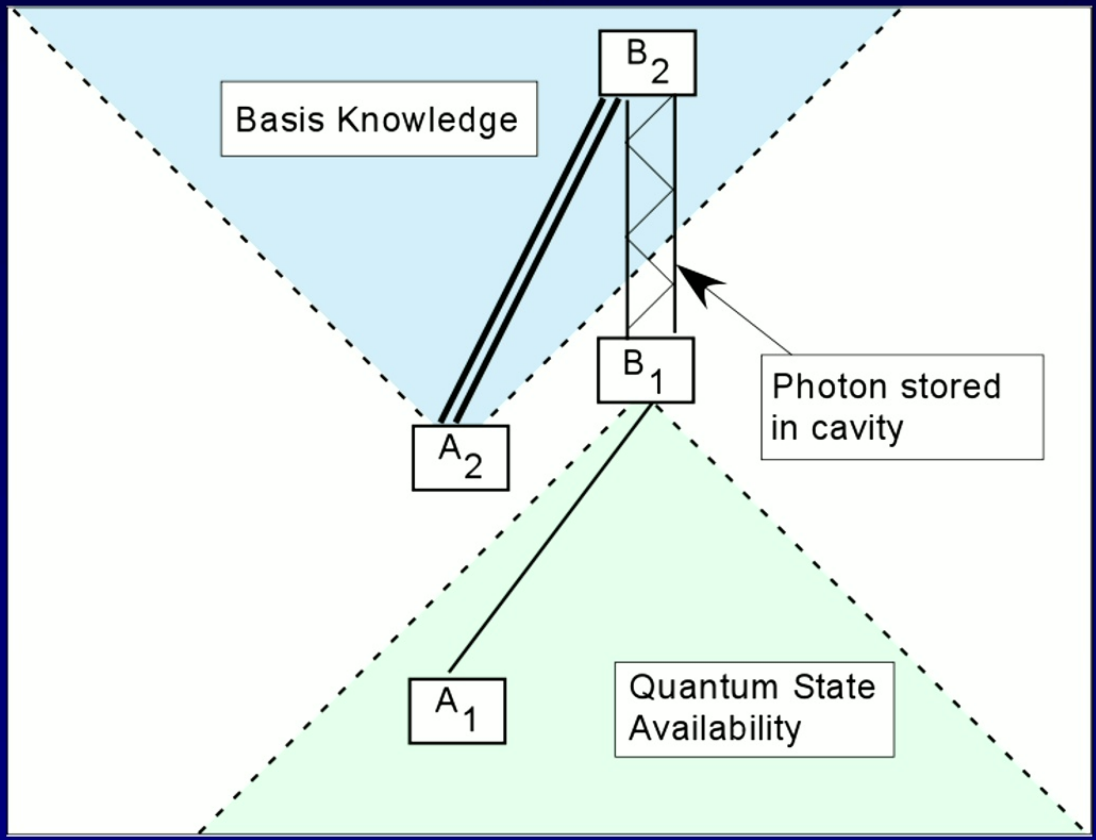


"Relativistic" Quantum Cryptography



Bob stores each photon until Alice tells him which basis to use
→ net efficiency is increased to 100% (in principle)
→ same security as BB84 (Eve's ρ cannot depend on Bob)

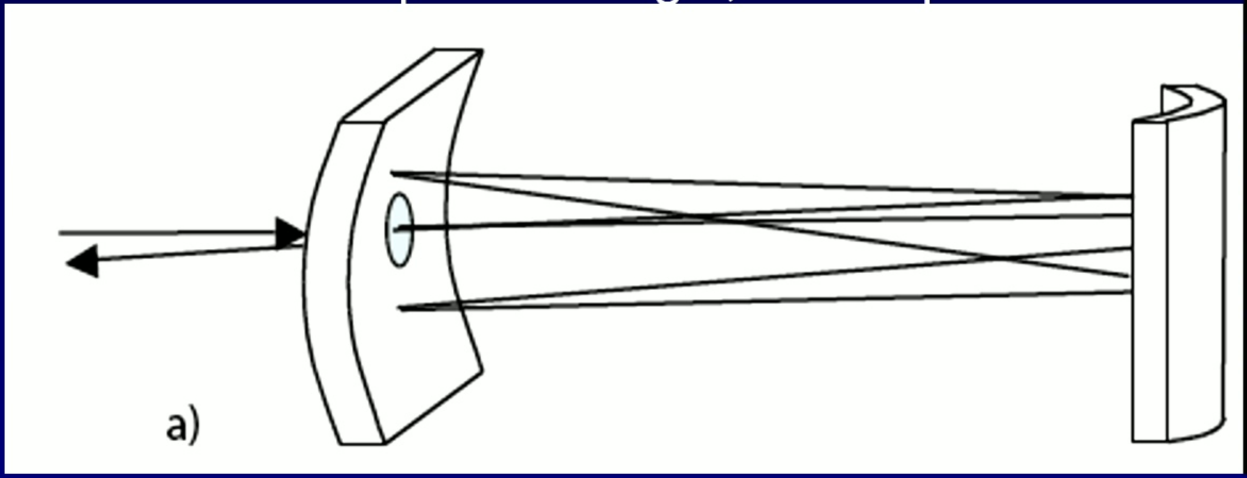
QKD and Special Relativity

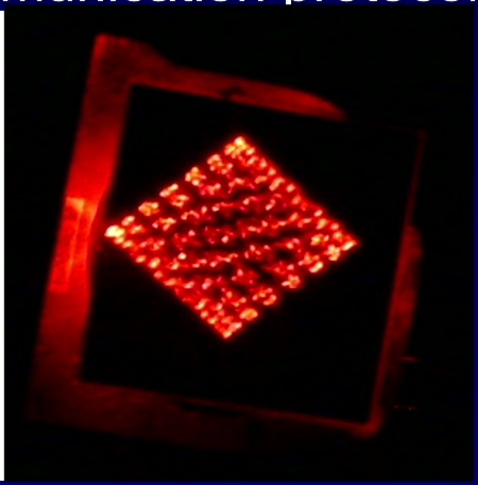


- These two light cones must not overlap
- A_2 may be before B_1 in some reference frames
- *Alice and Bob must know their space-time coordinates*

Quantum Memory: low-loss optical delay line

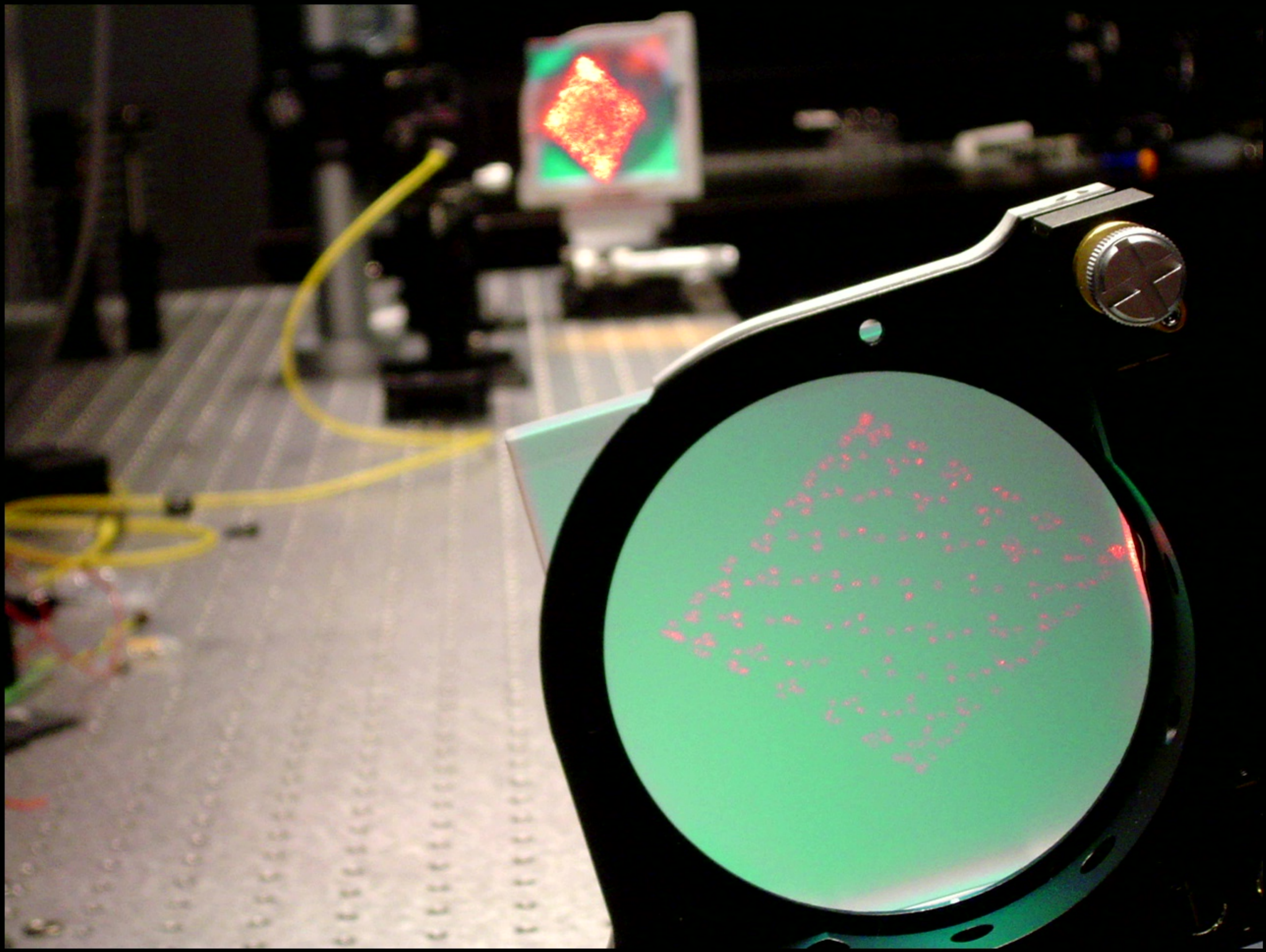
Applications to quantum cryptography, quantum “repeaters”, scalable quantum logic, novel quantum communication protocols

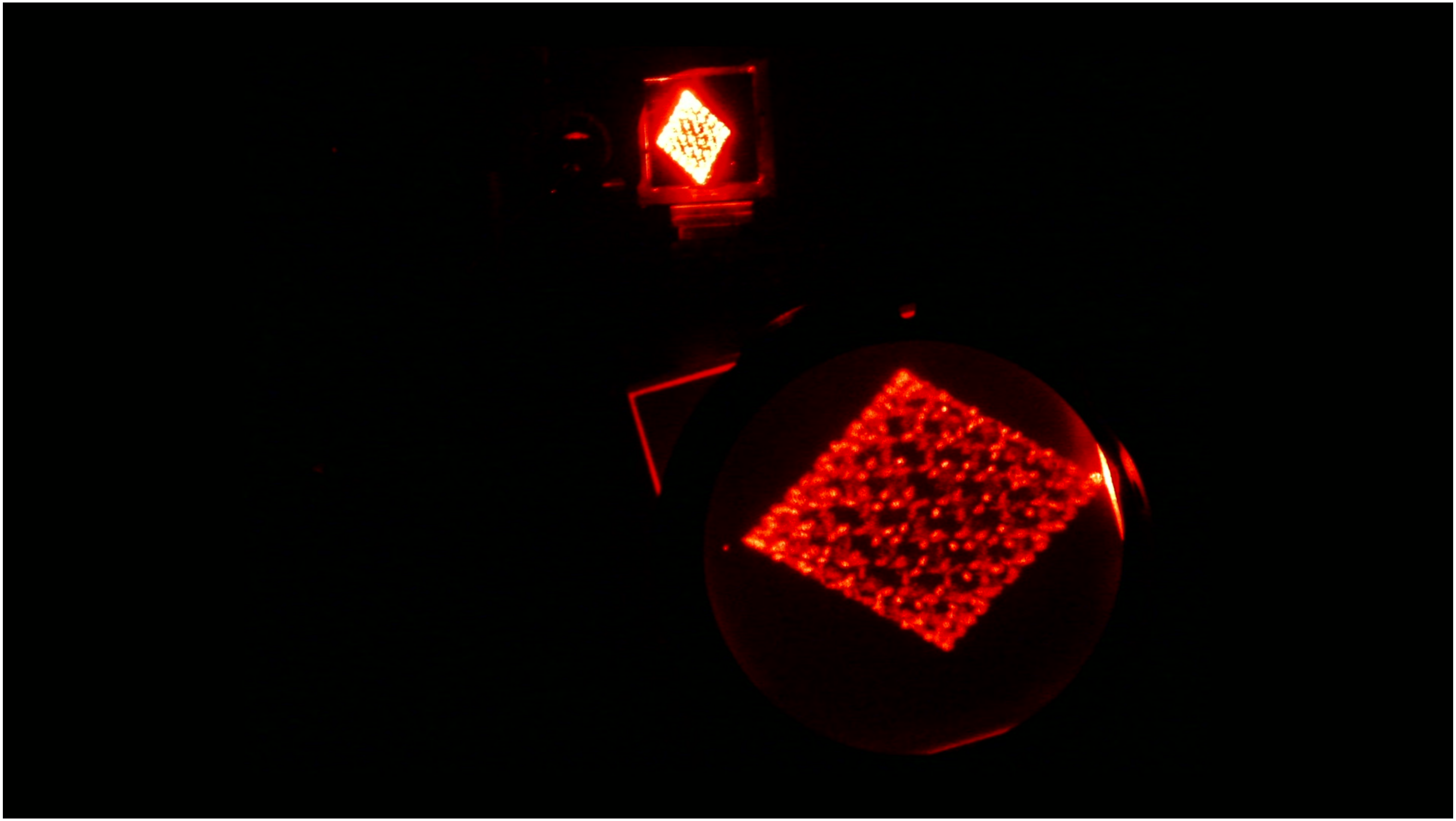




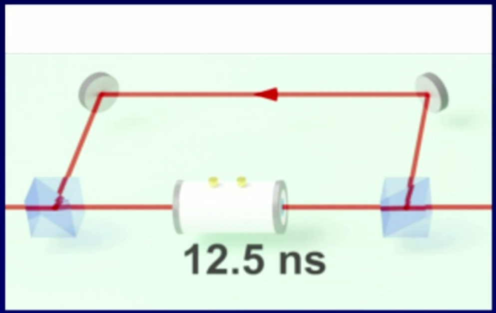
Advantages

- High bandwidth (~10 nm)
- Polarization insensitive
- Adjustable time delay (10 ns – 10μs)
- Low loss (custom mirror coatings)
- Store multiple k-vectors, spatial modes

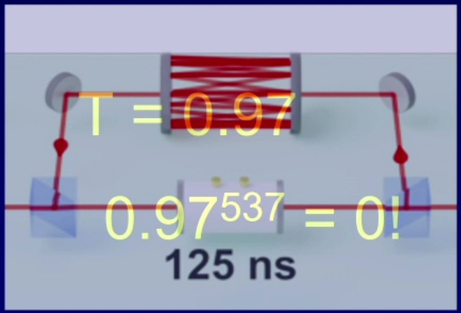




FYI: Adjustable Quantum Memory

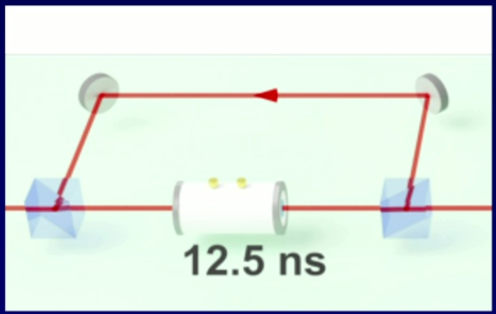


Flat-mirror cavity

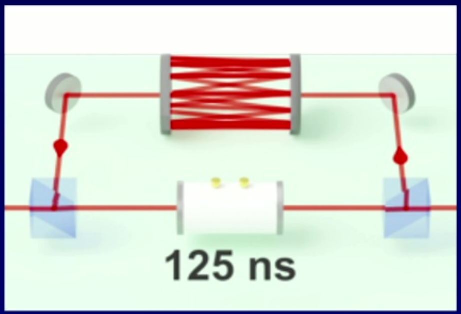


Herriott cell cavity

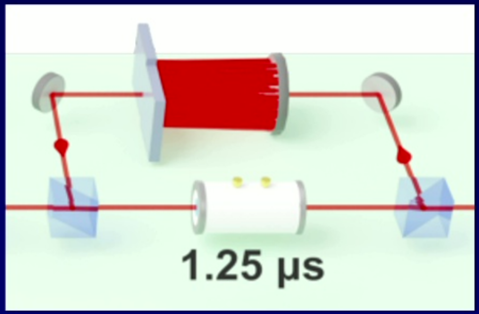
FYI: Adjustable Quantum Memory



Flat-mirror cavity



Herriott cell cavity



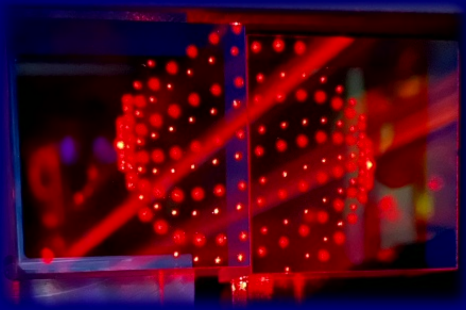
Modified Herriott cell cavity

Number of bounces limited by mirror area

E.g., 1.1-m spacing

→ 339 reflections

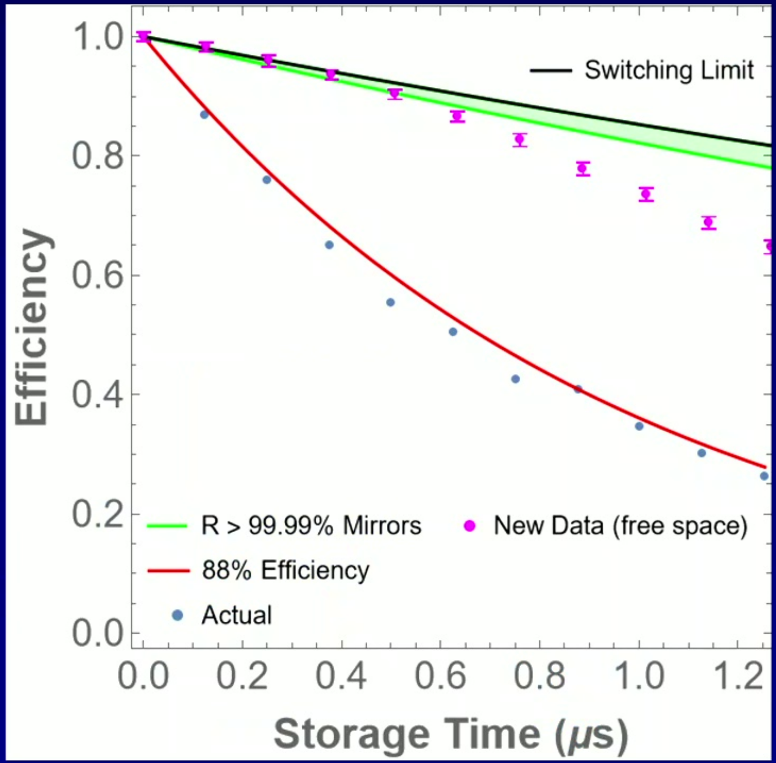
→ 1.25-µs delay

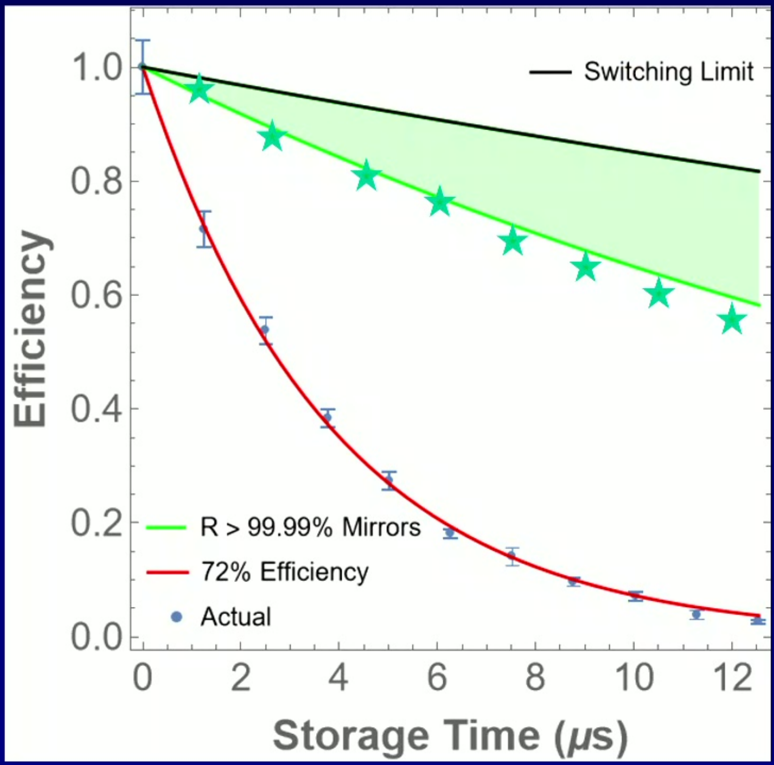


Memory performance limited by mirror reflectivity and polarization-switching efficiency

While fiber-based memories must deal with fundamental dispersion and loss limitations, mirror coatings and active-switching technologies are continuously improving

125-ns loop end-to-end efficiency



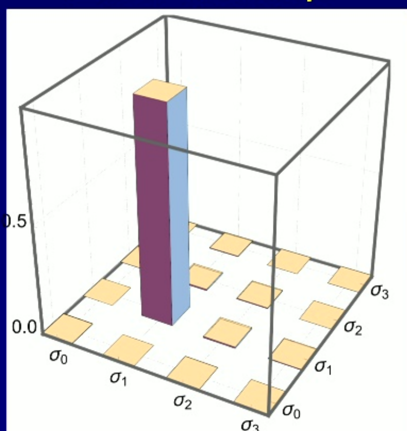


1.25-μs loop end-to-end efficiency

Memory preserves quantum state encoded onto photons

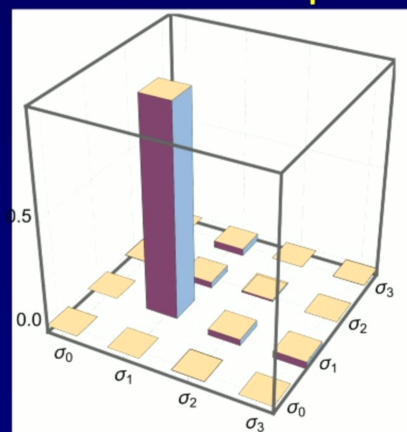
Propagating in free space and reflecting at mostly ~0° angle of incidence prevents changes to the polarization state of the qubits being stored in the memory

12.5-ns loop



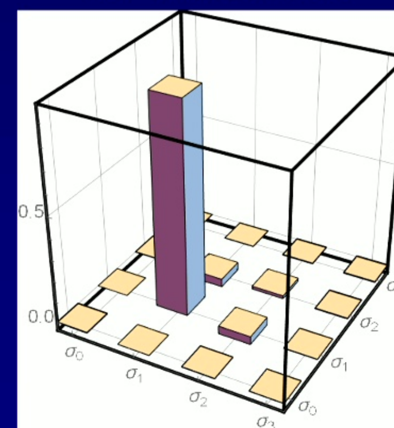
99.4(3)% χ-fidelity

125-ns loop



99.0(1)% χ-fidelity

1.25-μs loop

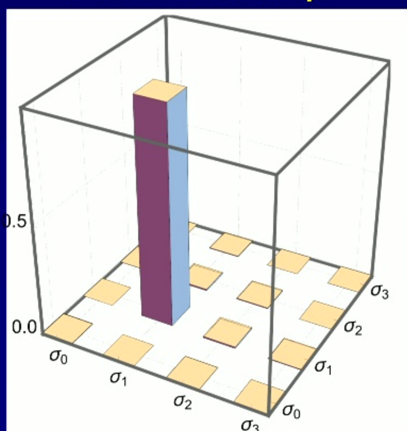


97.8(2)% χ-fidelity

Memory preserves quantum state encoded onto photons

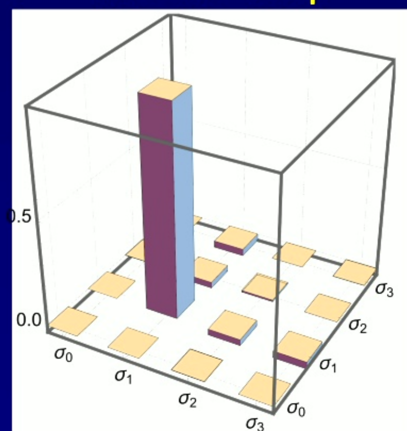
Propagating in free space and reflecting at mostly ~0° angle of incidence prevents changes to the polarization state of the qubits being stored in the memory

12.5-ns loop



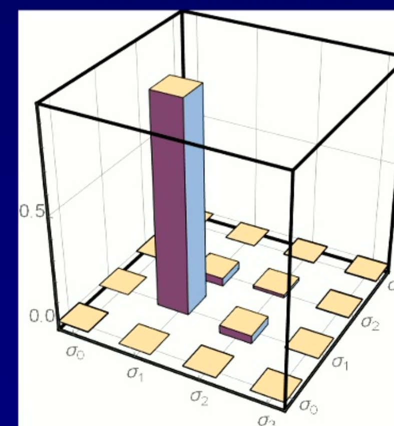
99.4(3)% χ-fidelity

125-ns loop



99.0(1)% χ-fidelity

1.25-μs loop

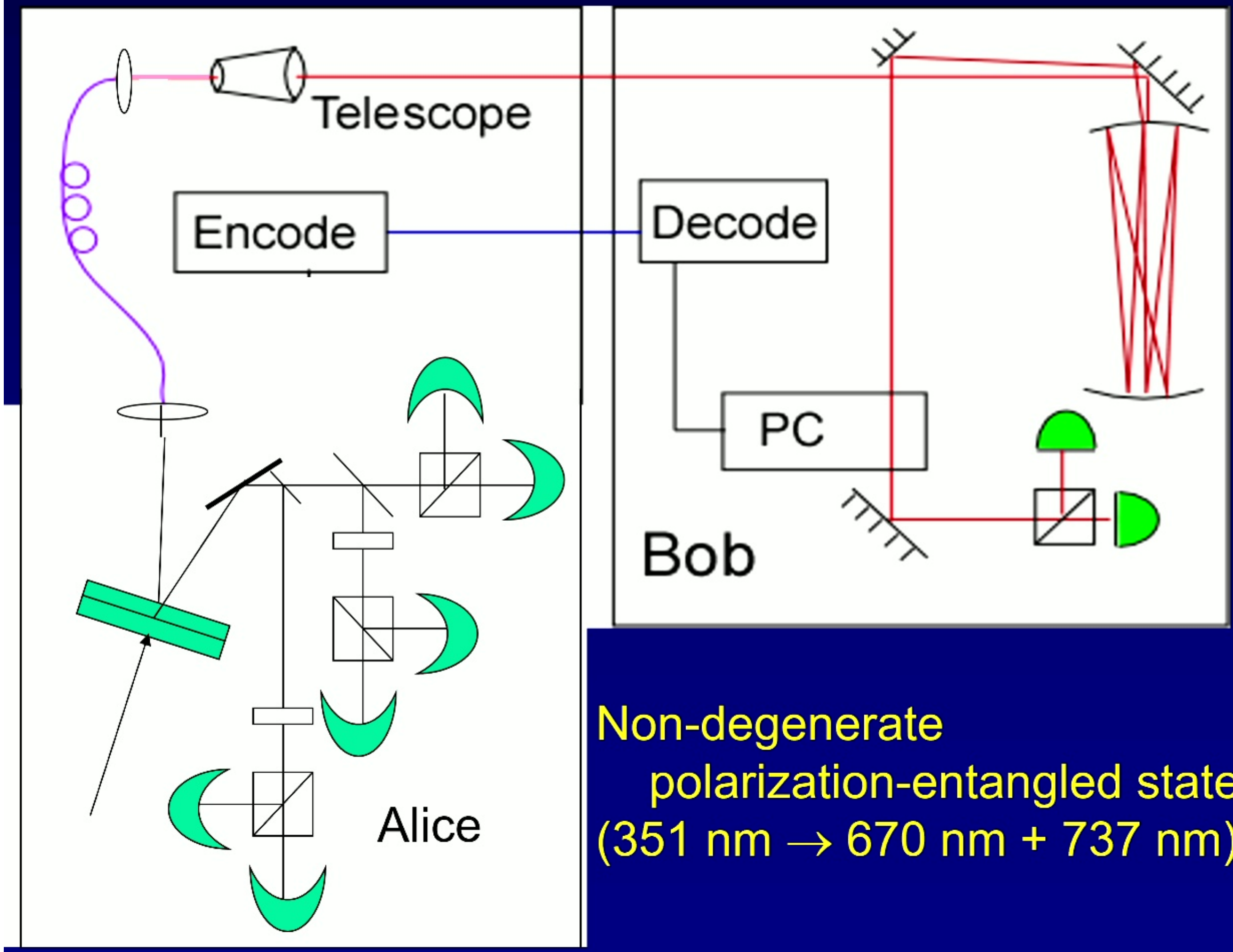


97.8(2)% χ-fidelity

Bandwidth: 1.5 THz

Time-Bandwidth: 6x10^6

Incorporate *entangled* photon source

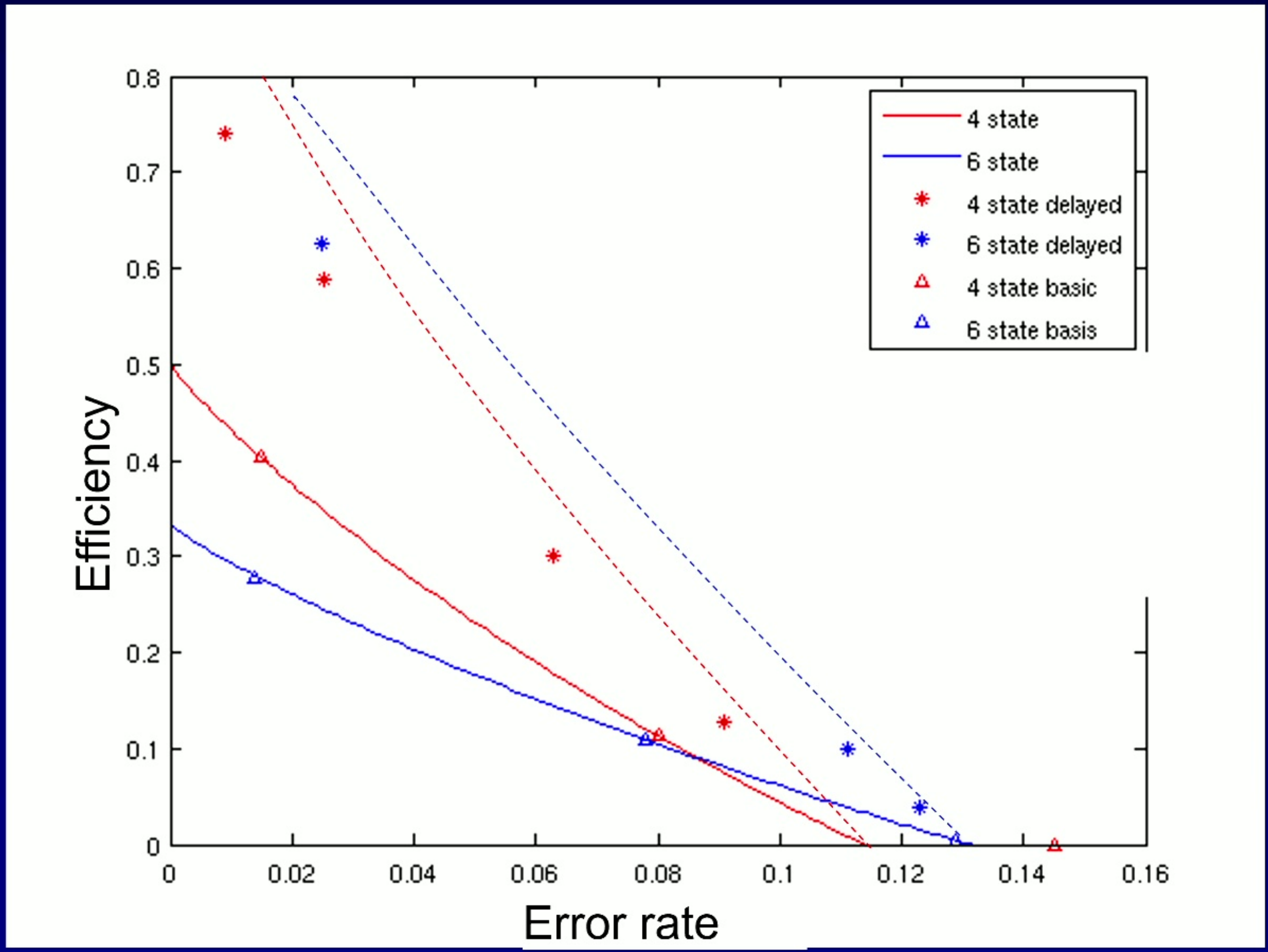


Non-degenerate polarization-entangled state (351 nm → 670 nm + 737 nm)

BB84, 30 mW pump power
94 sifted bits/second
2.5% error rate
→ 65.5 secret bits/second

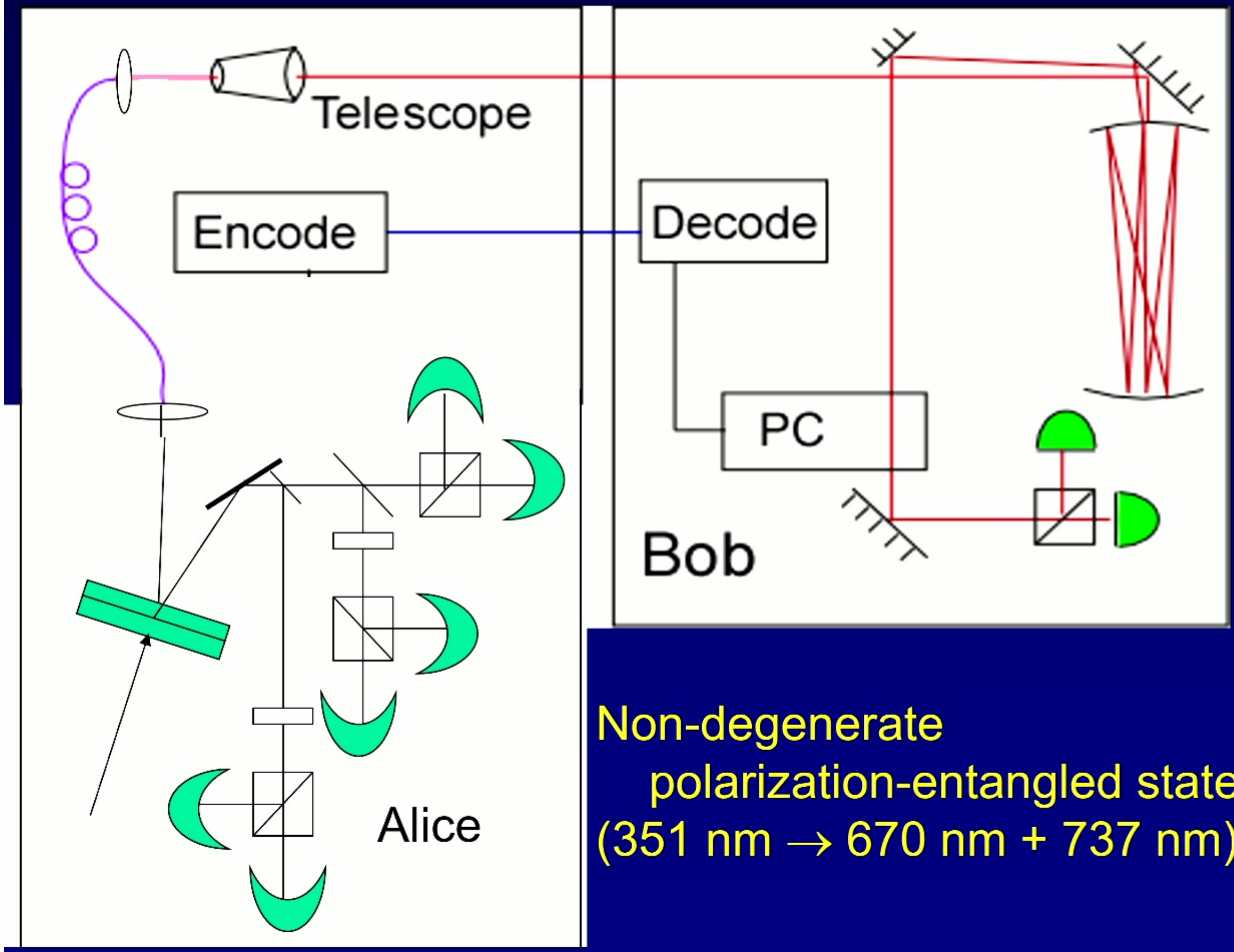
BB84, 90 mW pump power
214 bits/second
3.1% error rate
→ 136 secret bits/second
→ **yield enhancement = 1.3**

SSP, 90 mW pump power
371 bits/second
2.7% error rate
→ 251 bits/second
→ **yield enhancement = 2.1**



Efficiency
Error rate
4 state
6 state
4 state delayed
6 state delayed
4 state basic
6 state basis
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
0.02
0.04
0.06
0.08
0.1
0.12
0.14
0.16

Incorporate *entangled* photon source



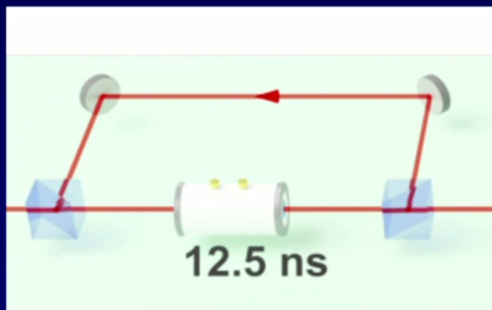
Non-degenerate polarization-entangled state (351 nm → 670 nm + 737 nm)

BB84, 30 mW pump power
94 sifted bits/second
2.5% error rate
→ 65.5 secret bits/second

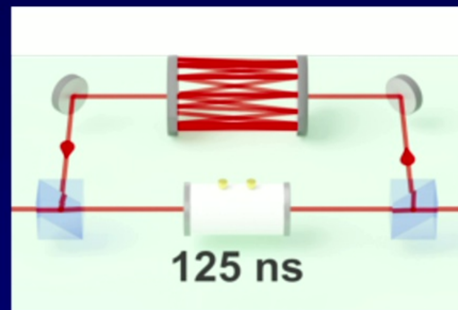
BB84, 90 mW pump power
214 bits/second
3.1% error rate
→ 136 secret bits/second
→ **yield enhancement = 1.3**

SSP, 90 mW pump power
371 bits/second
2.7% error rate
→ 251 bits/second
→ **yield enhancement = 2.1**

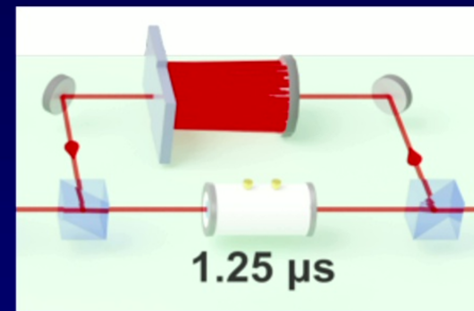
FYI: Adjustable Quantum Memory



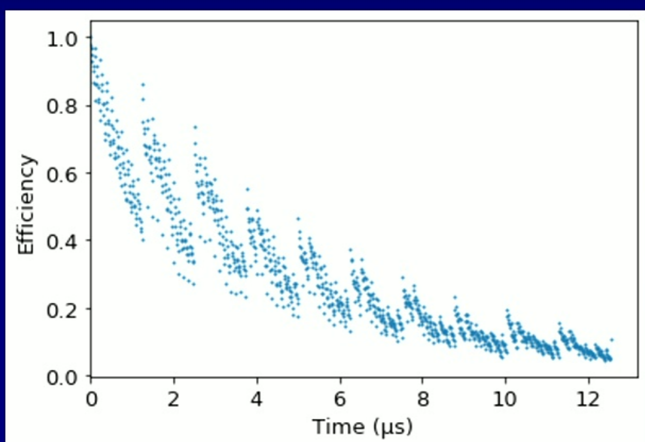
Flat-mirror cavity



Herriott cell cavity



Modified Herriott cell cavity

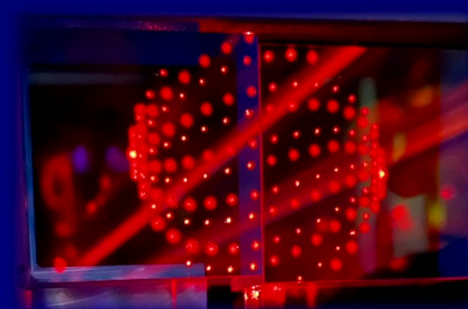


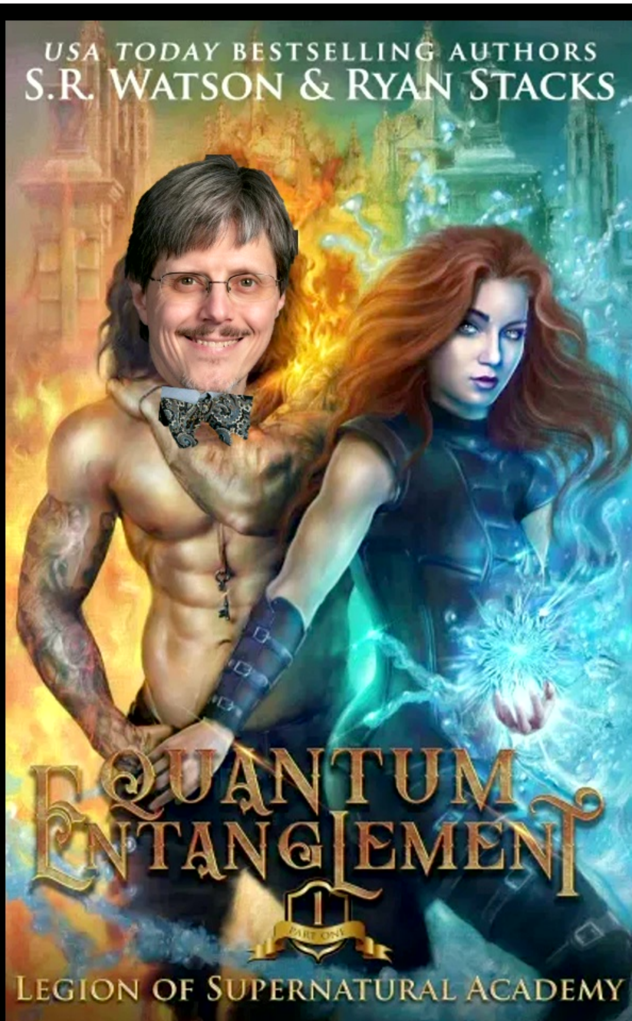
Number of bounces limited by mirror area

E.g., 1.1-m spacing

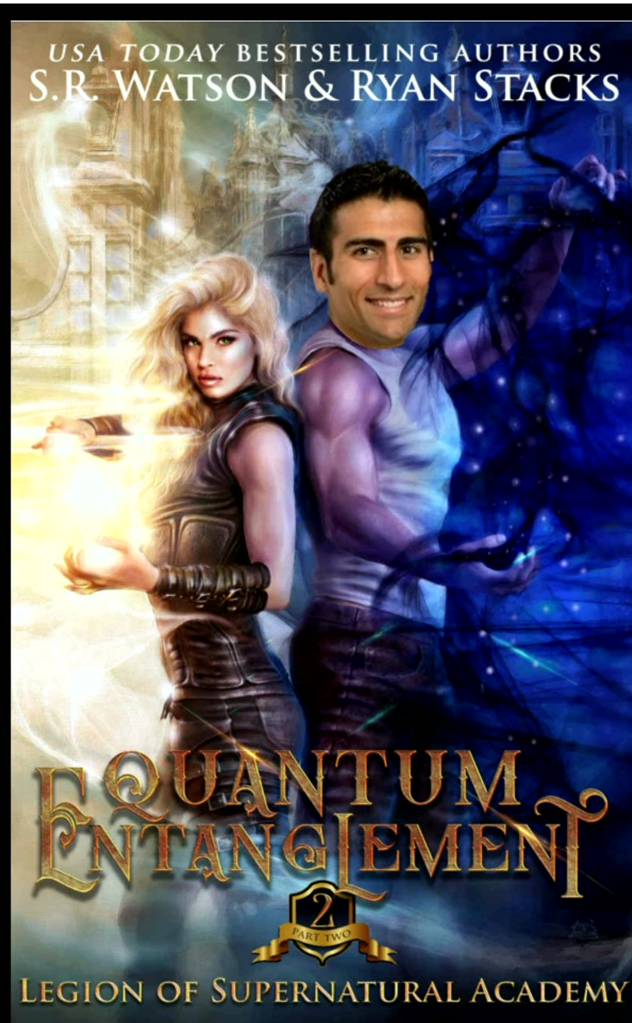
→ 339 reflections

→ 1.25-μs delay




USA TODAY BESTSELLING AUTHORS
S.R. WATSON & RYAN STACKS
QUANTUM ENTANGLEMENT
1
PART ONE
LEGION OF SUPERNATURAL ACADEMY


USA TODAY BESTSELLING AUTHORS
S.R. WATSON & RYAN STACKS
QUANTUM ENTANGLEMENT
2
PART TWO
LEGION OF SUPERNATURAL ACADEMY



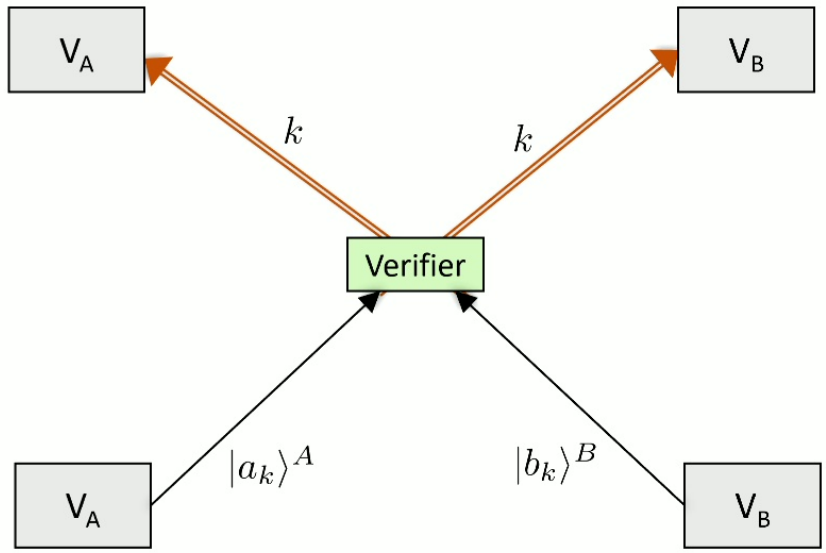
Quantum Position Verification

QPV and State Discrimination

- Many QPV protocols can be understood as a state discrimination problem.

A family of orthogonal states

$$\begin{cases} |\psi_1\rangle^{AB} = |0\rangle^A \otimes |0\rangle^B \\ |\psi_2\rangle^{AB} = |1\rangle^A \otimes |0\rangle^B \\ |\psi_3\rangle^{AB} = |+\rangle^A \otimes |1\rangle^B \\ |\psi_4\rangle^{AB} = |-\rangle^A \otimes |1\rangle^B \end{cases}$$



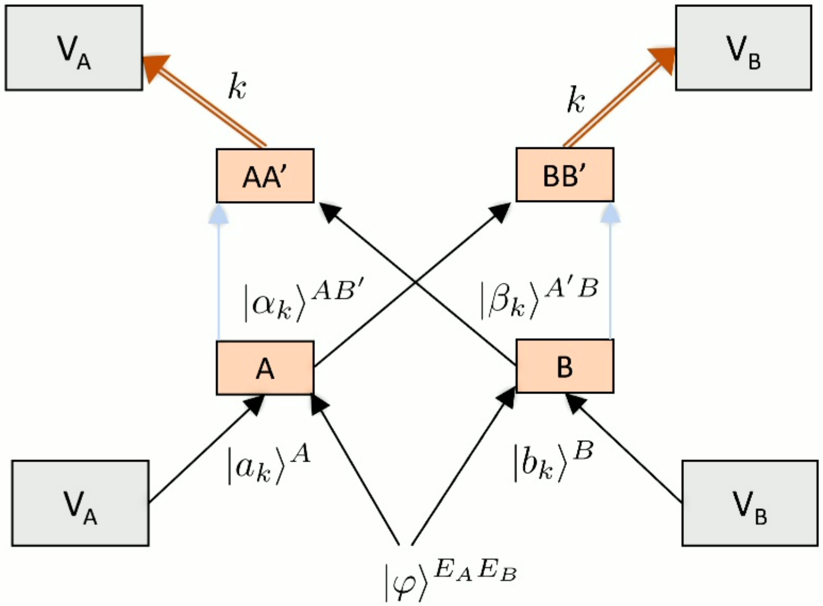
- The prover needs to identify which bipartite state $|\psi_k\rangle^{AB}$ was sent by the verifiers.

QPV and State Discrimination

- In order to be secure, the orthogonality of the encoded states $|\psi_k\rangle$ must be sufficiently nonlocal.

- They should not be distinguishable by *local operations* and *simultaneous communication.*

- Different adversarial models to consider:
  - Local operations and simultaneous quantum communication (**LOSQC**)
  - Entanglement-assisted local operations and simultaneous quantum communication (**eLOSQC**)

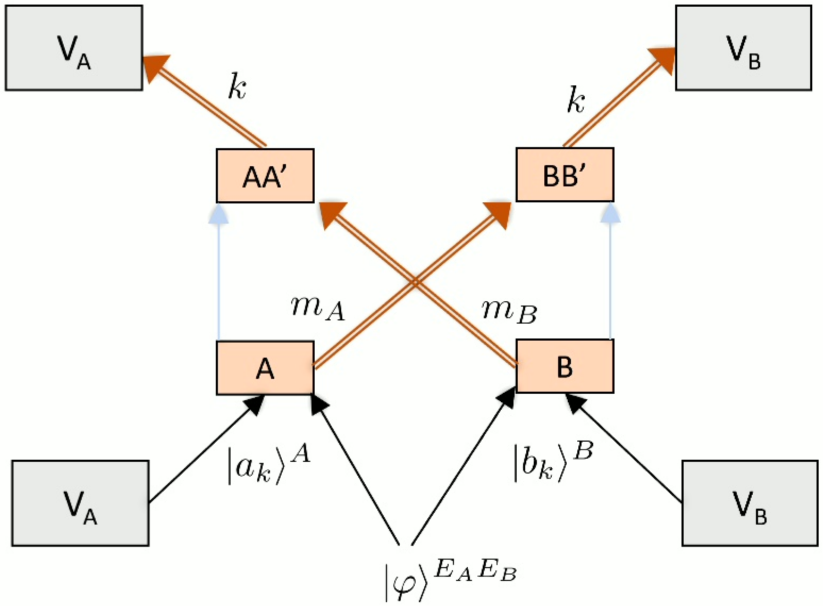


QPV and State Discrimination

- In order to be secure, the orthogonality of the encoded states $|\psi_k\rangle$ must be sufficiently nonlocal.

- They should not be distinguishable by *local operations* and *simultaneous communication.*

- Different adversarial models to consider:
  - Local operations and simultaneous classical communication (**LOSCC**)
  - Entanglement-assisted local operations and simultaneous classical communication (**eLOSCC**)

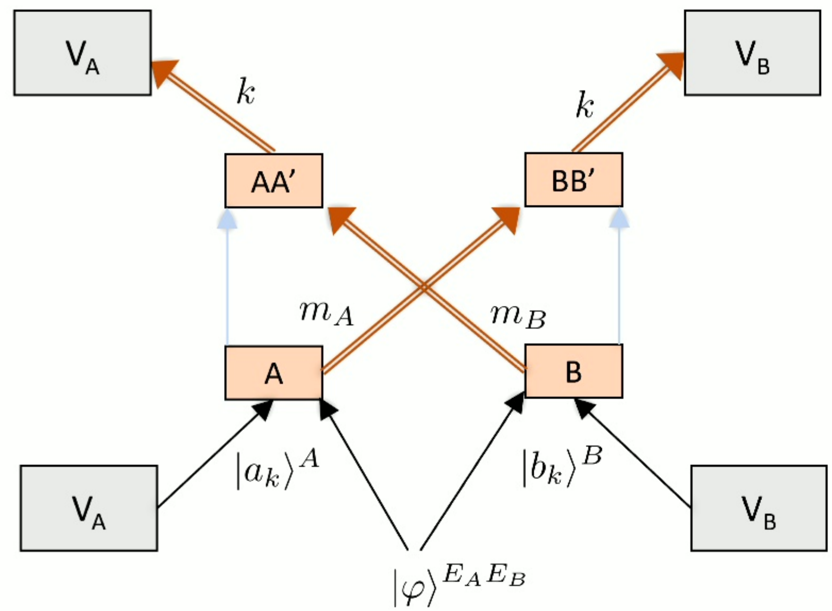


QPV and State Discrimination

- In order to be secure, the orthogonality of the encoded states $|\psi_k\rangle$ must be sufficiently nonlocal.

- They should not be distinguishable by *local operations* and *simultaneous communication.*

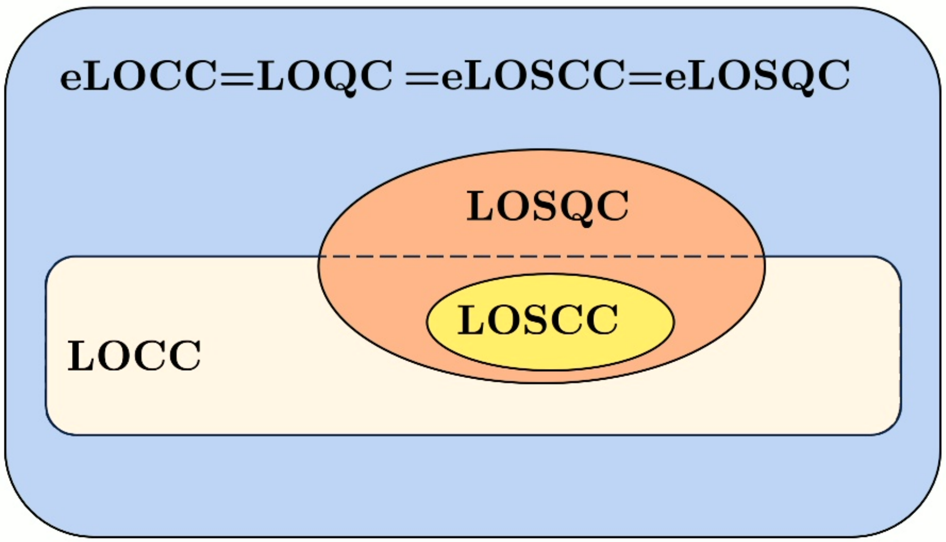
- Different adversarial models to consider:
  - Local operations and simultaneous classical communication (**LOSCC**)
  - Entanglement-assisted local operations and simultaneous classical communication (**eLOSCC**)



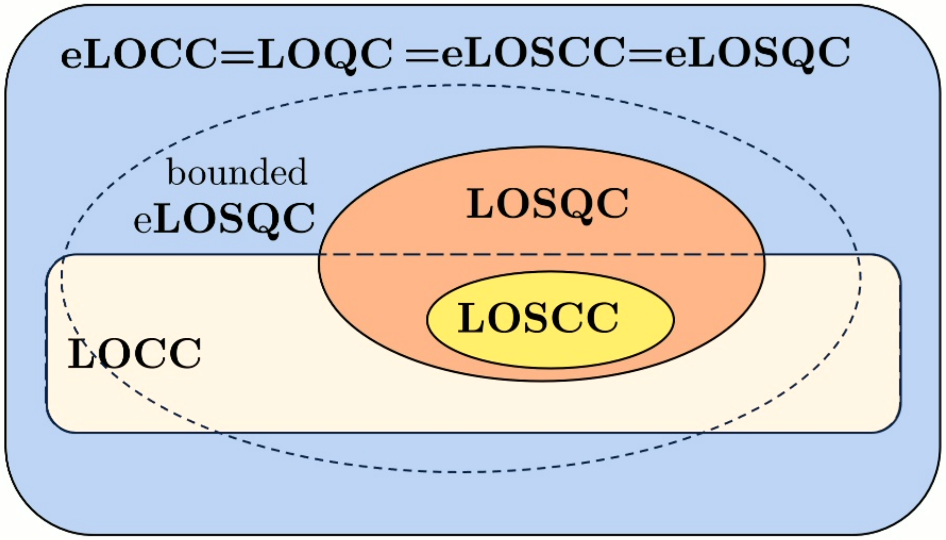
Different Operational Classes

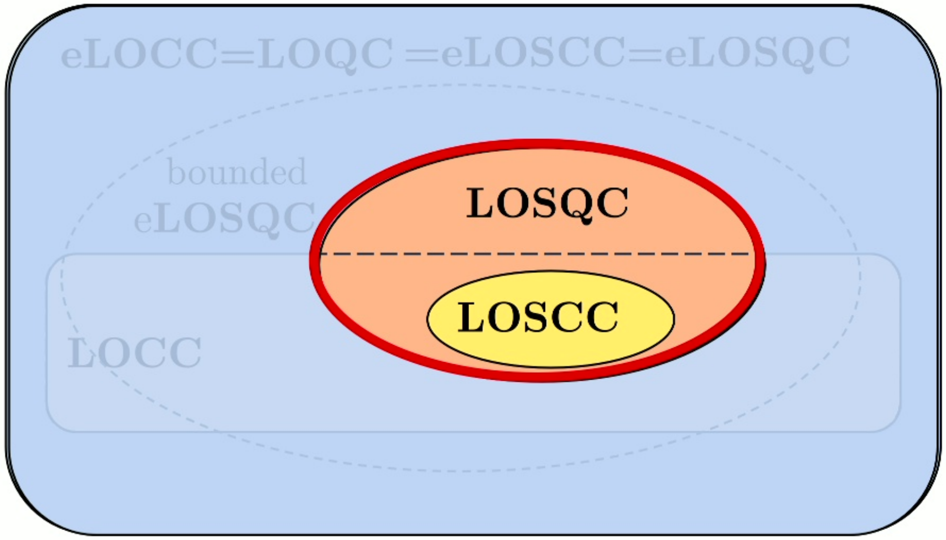
- These should be compared to standard:
  - Local operations and classical communication (**LOCC**)
  - Entanglement-assisted local operations and classical communication (**eLOCC**)
  - Local operations and quantum communication (**LOQC**)

Unrestricted classical communication



Different Operational Classes



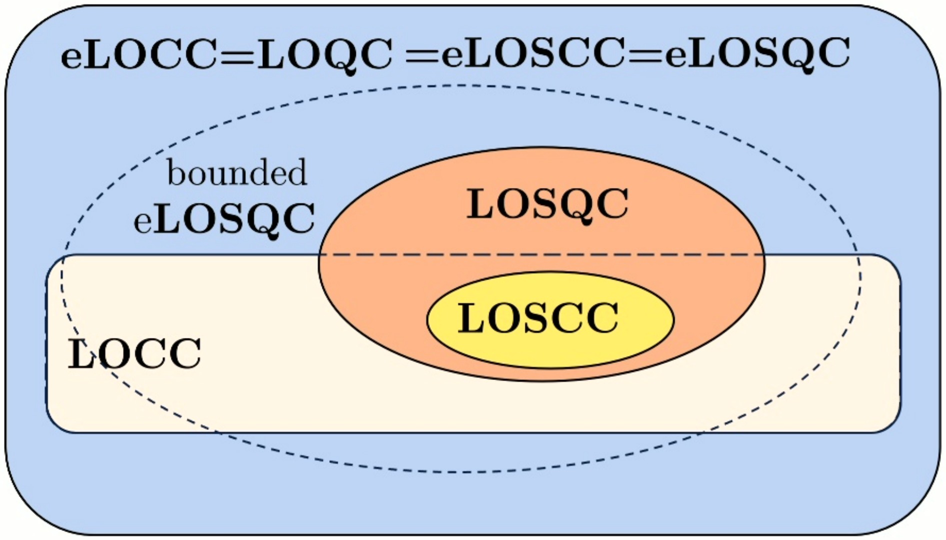


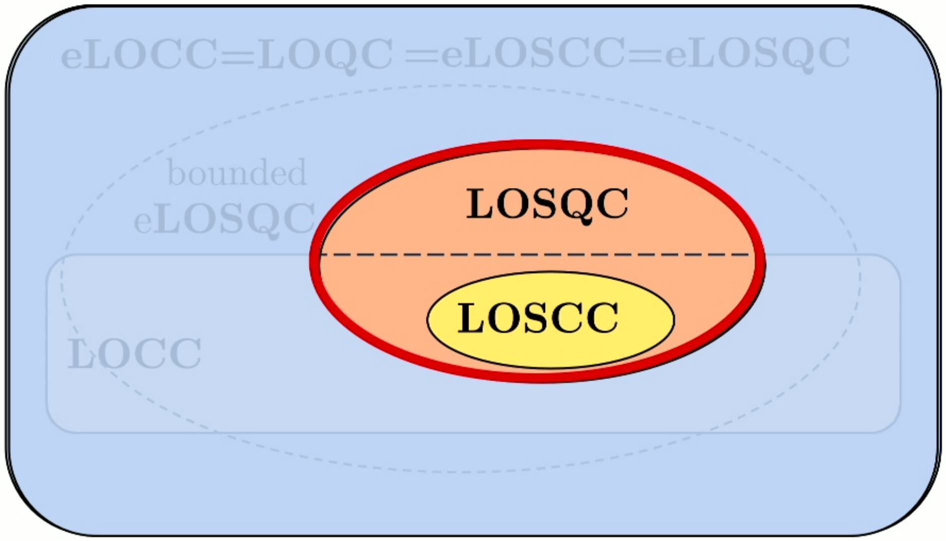
- The intermediate regime of **bounded entanglement** is where most QPV analysis sits.

- Every family of orthogonal $\{|\psi_k\rangle\}_k$ that is difficult to discriminate using a class of operations constitutes a good QPV scheme under attacks from that class.

- The **no pre-shared entanglement** model is the simplest to analyze, but even in this scenario relatively little is known.

Different Operational Classes

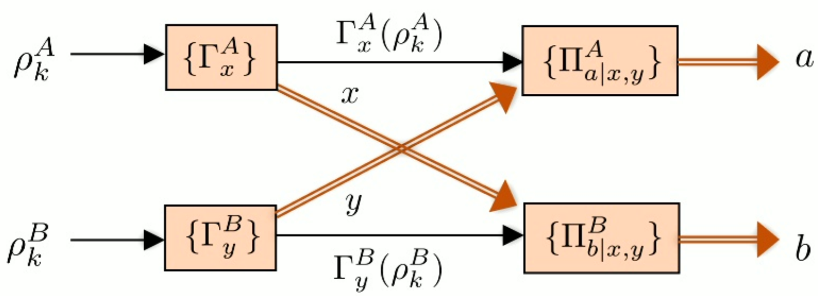




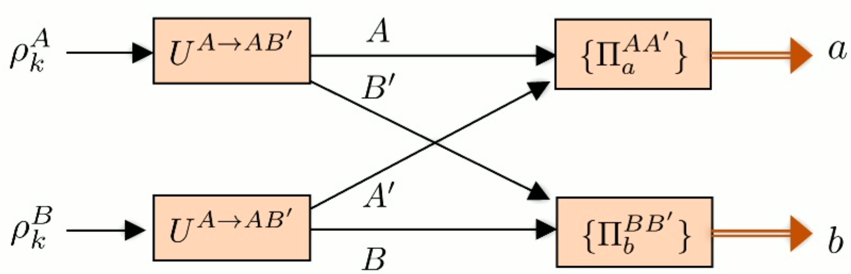
- The intermediate regime of **bounded entanglement** is where most QPV analysis sits.
- Every family of orthogonal $\{|\psi_k\rangle\}_k$ that is difficult to discriminate using a class of operations constitutes a good QPV scheme under attacks from that class.
- The **no pre-shared entanglement** model is the simplest to analyze, but even in this scenario relatively little is known.
- Simplify the problem even further:
  How well can a family of orthogonal **product states**
  $$\{|\psi_k\rangle = |a_k\rangle^A |b_k\rangle^A\}_k$$
  be distinguished by LOSCC and LOSQC?

The structure of LOSCC and LOSQC protocols

- The structure of LOSCC protocols:



- The structure of LOSQC protocols:



- Does the quantum communication help?

Yes!

Consider two copies of each Bell state

$$|\psi_1\rangle = |\Phi^+\rangle^{AB'} \otimes |\Phi^+\rangle^{BA'}$$
$$|\psi_2\rangle = |\Phi^-\rangle^{AB'} \otimes |\Phi^-\rangle^{BA'}$$
$$|\psi_3\rangle = |\Psi^+\rangle^{AB'} \otimes |\Psi^+\rangle^{BA'}$$
$$|\psi_4\rangle = |\Psi^-\rangle^{AB'} \otimes |\Psi^-\rangle^{BA'}$$

- Perfectly distinguishable by LOSQC but not LOSCC.

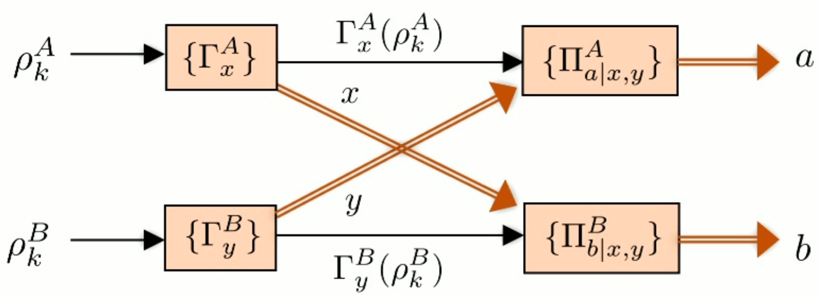
Yu, Duan, Ying, **PRL** 109, 020506 (2012).

- Also true if coarse-grained.

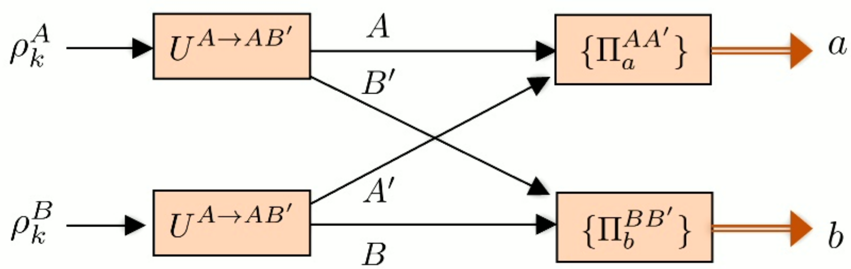
Allerstorfer, Buhrman, Speelman, Lunel, arXiv:2208.04341.

The structure of LOSCC and LOSQC protocols

- The structure of LOSCC protocols:



- The structure of LOSQC protocols:



- Does the quantum communication help?

Yes!

Consider two copies of each Bell state

$$|\psi_1\rangle = |\Phi^+\rangle^{AB'} \otimes |\Phi^+\rangle^{BA'}$$
$$|\psi_2\rangle = |\Phi^-\rangle^{AB'} \otimes |\Phi^-\rangle^{BA'}$$
$$|\psi_3\rangle = |\Psi^+\rangle^{AB'} \otimes |\Psi^+\rangle^{BA'}$$
$$|\psi_4\rangle = |\Psi^-\rangle^{AB'} \otimes |\Psi^-\rangle^{BA'}$$

- Perfectly distinguishable by LOSQC but not LOSCC.

Yu, Duan, Ying, **PRL** 109, 020506 (2012).

- Also true if coarse-grained.

Allerstorfer, Buhrman, Speelman, Lunel, arXiv:2208.04341.

- But these involve distinguishing entangled states.
What about for product states?

Distinguishing orthogonal product states

- This problem has a rich history in quantum information theory.
  - Any $2 \otimes 2$ family of orthogonal product states can be perfectly distinguished by LOCC.

$$\begin{cases} |\psi_1\rangle = |0\rangle \otimes |\theta\rangle & |\psi_3\rangle = |1\rangle \otimes |\phi\rangle \\ |\psi_2\rangle = |0\rangle \otimes |\theta^\perp\rangle & |\psi_4\rangle = |1\rangle \otimes |\phi^\perp\rangle \end{cases}$$

Walgate and Hardy, **PRL** 89, 147901 (2002).

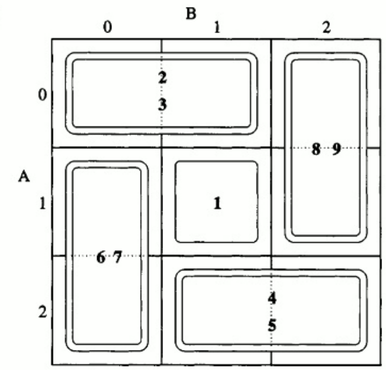
  - Any $2 \otimes n$ family of orthogonal product states can be perfectly distinguished by LOCC.

Bennett, DiVincenzo, Mor, Shor, Smolin, Terhal, **PRL** 82, 5385 (1999).

  - There exists orthogonal product state that cannot be distinguished by LOCC

"Nonlocality without entanglement"

$$\begin{cases} |\psi_1\rangle = |1\rangle \otimes |1\rangle & |\psi_4\rangle = |2\rangle \otimes |1+2\rangle & |\psi_7\rangle = |1-2\rangle \otimes |0\rangle \\ |\psi_2\rangle = |0\rangle \otimes |0+1\rangle & |\psi_5\rangle = |2\rangle \otimes |1-2\rangle & |\psi_8\rangle = |0+1\rangle \otimes |2\rangle \\ |\psi_3\rangle = |0\rangle \otimes |0-1\rangle & |\psi_6\rangle = |1+2\rangle \otimes |0\rangle & |\psi_8\rangle = |0-1\rangle \otimes |2\rangle \end{cases}$$



Bennett, DiVincenzo, Fuchs, Mor, Rains, Shor, Smolin, Wootters, **PRA** 59, 1070 (1999).

Distinguishing orthogonal product states

Proposition [I.George, R. Allerstorfer, P. Lunel, E.C.]:

- For perfect discrimination of $2 \otimes 2$ orthogonal product states, LOSQC=LOSCC and the states must have the form:

$$\begin{cases} |\psi_1\rangle = |0\rangle \otimes |0\rangle & |\psi_3\rangle = |1\rangle \otimes |0\rangle \\ |\psi_2\rangle = |0\rangle \otimes |1\rangle & |\psi_4\rangle = |1\rangle \otimes |1\rangle \end{cases}$$

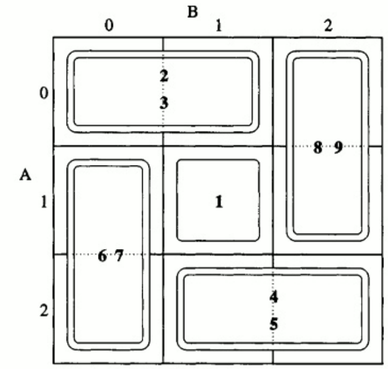
- A $2 \otimes n$ family of orthogonal product states can be perfectly distinguished by LOSC iff it has the form:

$$\begin{cases} \left.\begin{array}{l} |0\rangle^A \otimes |j\rangle^B \\ |1\rangle^A \otimes (x_j|j\rangle + y_j|j+1\rangle)^B \end{array}\right\} \text{ for } \quad j \in \{0, 2, 4, ..., 2m\} \\ |g_i\rangle^A \otimes |i\rangle^B \quad \text{for} \quad i > 2m+1 \end{cases}$$

Distinguishing orthogonal product states

- But what about the sausage states?

$$\begin{cases} |\psi_1\rangle = |1\rangle \otimes |1\rangle & |\psi_4\rangle = |2\rangle \otimes |1+2\rangle & |\psi_7\rangle = |1-2\rangle \otimes |0\rangle \\ |\psi_2\rangle = |0\rangle \otimes |0+1\rangle & |\psi_5\rangle = |2\rangle \otimes |1-2\rangle & |\psi_8\rangle = |0+1\rangle \otimes |2\rangle \\ |\psi_3\rangle = |0\rangle \otimes |0-1\rangle & |\psi_6\rangle = |1+2\rangle \otimes |0\rangle & |\psi_8\rangle = |0-1\rangle \otimes |2\rangle \end{cases}$$



- These states cannot be distinguished by LOSCC.

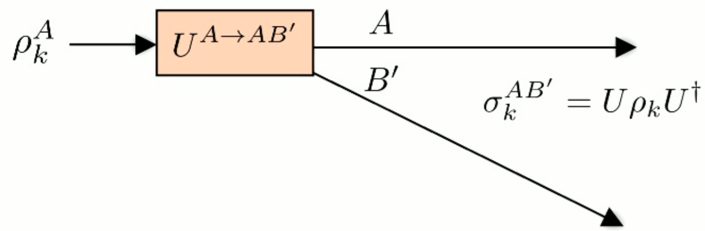
- They also cannot be distinguished by LOSQC (see theorem below).

- What about two copies of the states: $\{|\psi_k\rangle^{\otimes 2} = |a_k\rangle^{\otimes 2} \otimes |b_k\rangle^{\otimes 2}\}$? $\Rightarrow$
  - Distinguishable by LOSQC
  - Distinguishable by LOSCC

Conjecture:

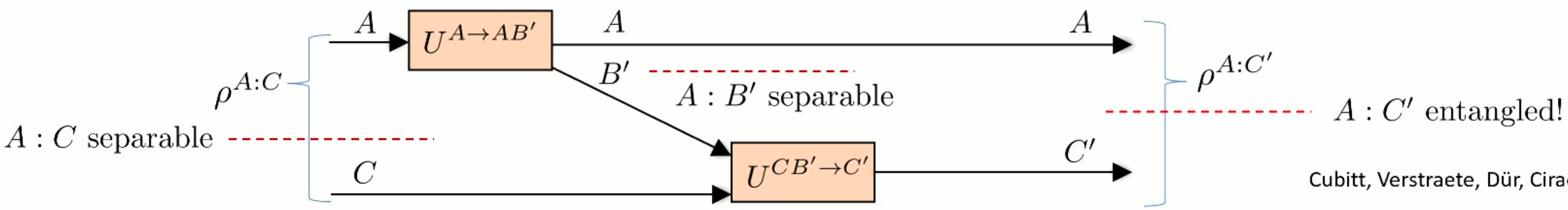
Two copies of any set of orthogonal product states is sufficient for LOSCC discrimination (or at least the ensemble must have a large number of states).

LOSQC is more powerful than LOSCC



- Distinguish between two types of quantum communication:
  - **Separable communication**, i.e. $\sigma_k^{AB'}$ is separable for all k.
  - **Entangled communication**, i.e. $\sigma_k^{AB'}$ is entangled for some k.

- Separable communication can be used to perform non-classical tasks, like entanglement distribution.



Cubitt, Verstraete, Dür, Cirac, **PRL** 91, 037902 (2003).

Theorem [I.George, R. Allerstorfer, P. Lunel, E.C.]:

The four states can be perfectly distinguished by LOSQC only if entangled communication is used:

$$|\psi_1\rangle = |0\rangle \otimes |0+1\rangle \qquad |\psi_3\rangle = |1\rangle \otimes |0+2\rangle$$
$$|\psi_2\rangle = |0\rangle \otimes |0-1\rangle \qquad |\psi_4\rangle = |1\rangle \otimes |0-2\rangle$$

LOSQC state discrimination with error

- Perfect state discrimination is interesting from a fundamental persective, but not for practical QPV.
- **QPV question:**

  Given an ensemble $\{|\psi_k\rangle\}_k$, what is the smallest error probability in state discrimination using LOSQC?

Theorem [I.George, R. Allerstorfer, P. Lunel, E.C.]:

Let $\{|\psi_k\rangle^{AB} = |a_k\rangle^A|b_k\rangle^B\}_k$ be an ensemble of product states that contains four states of the form

$$\begin{aligned}
|\psi_0\rangle^{AB} &= |a_0\rangle^A|b_0\rangle^B, \\
|\psi_1\rangle^{AB} &= |a_1\rangle^A|b_1\rangle^B, \\
|\psi_2\rangle^{AB} &= |a_2\rangle^A(\cos\theta|b_0\rangle + e^{i\phi}\sin\theta|b_1\rangle)^B \\
|\psi_3\rangle^{AB} &= |a_3\rangle^A(\cos\theta|b_0\rangle - e^{i\phi}\sin\theta|b_1\rangle)^B,
\end{aligned}$$

with $\langle a_0|a_1\rangle \neq 0$. Suppose Alice and Bob can identify each state with at least probability $1-\epsilon$ using some LOBQC protocol. Then

$$2\epsilon + \frac{4\sqrt{\epsilon(1-\epsilon)}}{|\langle a_0|a_1\rangle|^2} + \sqrt{1-|\langle a_2|a_3\rangle|^2} > 1.$$

LOSQC state discrimination with error

Example: Generalized BB84 states:

$$\begin{aligned}
|\psi_0\rangle^{AB} &= |0\rangle^A \otimes |0\rangle^B, \\
|\psi_1\rangle^{AB} &= |0\rangle^A \otimes |1\rangle^B, \\
|\psi_2\rangle^{AB} &= |1\rangle^A \otimes (\cos\theta|0\rangle + e^{i\phi}\sin\theta|1\rangle)^B \\
|\psi_3\rangle^{AB} &= |1\rangle^A \otimes (\cos\theta|0\rangle - e^{i\phi}\sin\theta|1\rangle)^B
\end{aligned}$$

The LOSQC error probability P_{err} is lower bounded as: $$P_{err} > \frac{1}{4}\left(\frac{1}{2} - \frac{1}{\sqrt{5}}\right) \approx 1.3\%.$$

LOSQC state discrimination with error

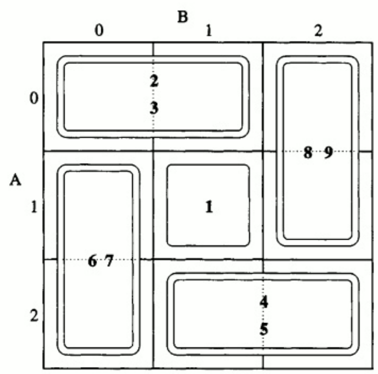
Example: Generalized BB84 states:

$$|\psi_0\rangle^{AB} = |0\rangle^A \otimes |0\rangle^B,$$
$$|\psi_1\rangle^{AB} = |0\rangle^A \otimes |1\rangle^B,$$
$$|\psi_2\rangle^{AB} = |1\rangle^A \otimes (\cos\theta|0\rangle + e^{i\phi}\sin\theta|1\rangle)^B$$
$$|\psi_3\rangle^{AB} = |1\rangle^A \otimes (\cos\theta|0\rangle - e^{i\phi}\sin\theta|1\rangle)^B$$

The LOSQC error probability P_{err} is lower bounded as: $P_{err} > \frac{1}{4}\left(\frac{1}{2} - \frac{1}{\sqrt{5}}\right) \approx 1.3\%.$

- But what about the sausage states?

Example:



The LOSQC error probability P_{err} is lower bounded as:

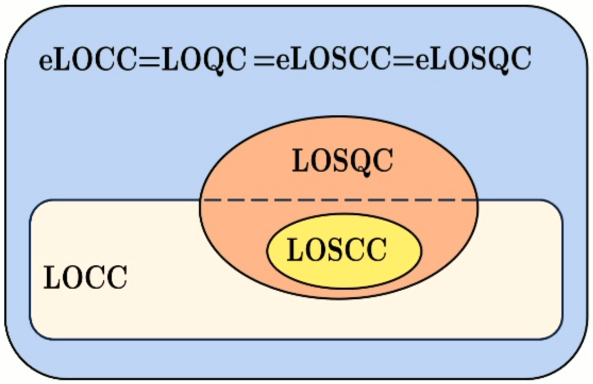
$$P_{err} > \frac{1}{9}\left(\frac{1}{2} - \frac{2}{\sqrt{17}}\right) \approx .16\%.$$

Open problems and future directions

- What are the necessary and sufficient conditions for product state discrimination under LOSCC and LOSQC?

- **Copy complexity**: How many copies of an ensemble state do Alice and Bob need before they can perfectly discriminate by LOSCC?

$$\{|\psi_k\rangle^{\otimes n} = |a_k\rangle^{\otimes n} \otimes |b_k\rangle^{\otimes n}\}$$



- What families of states are distinguishable by LOSQC but not LOCC?

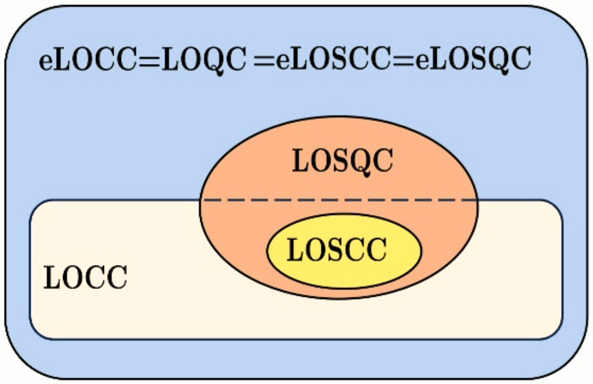
- **Most important question for QPV**:
  What are the entanglement costs for state discrimination under eLOSCC and eLOSQC?

Open problems and future directions

- What are the necessary and sufficient conditions for product state discrimination under LOSCC and LOSQC?

- **Copy complexity**: How many copies of an ensemble state do Alice and Bob need before they can perfectly discriminate by LOSCC?

$$\{|\psi_k\rangle^{\otimes n} = |a_k\rangle^{\otimes n} \otimes |b_k\rangle^{\otimes n}\}$$



- What families of states are distinguishable by LOSQC but not LOCC?

- **Most important question for QPV**:
  What are the entanglement costs for state discrimination under eLOSCC and eLOSQC?

- **Example: BB84 states**:

$$\begin{cases} |\psi_1\rangle^{AB} = |0\rangle^A \otimes |0\rangle^B & |\psi_3\rangle^{AB} = |+\rangle^A \otimes |1\rangle^B \\ |\psi_2\rangle^{AB} = |1\rangle^A \otimes |0\rangle^B & |\psi_4\rangle^{AB} = |-\rangle^A \otimes |1\rangle^B \end{cases}$$

One ebit suffices for perfect discrimination

Lo and Lau **PRA** 83, 012322 (2011).

LOSQC state discrimination with error

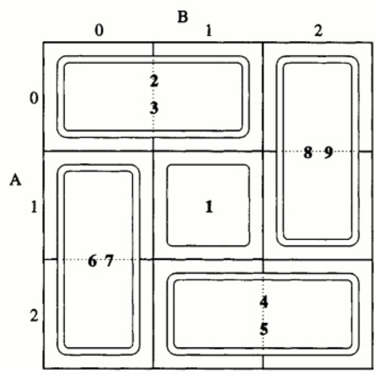
Example: Generalized BB84 states:

$$|\psi_0\rangle^{AB} = |0\rangle^A \otimes |0\rangle^B,$$
$$|\psi_1\rangle^{AB} = |0\rangle^A \otimes |1\rangle^B,$$
$$|\psi_2\rangle^{AB} = |1\rangle^A \otimes (\cos\theta|0\rangle + e^{i\phi}\sin\theta|1\rangle)^B$$
$$|\psi_3\rangle^{AB} = |1\rangle^A \otimes (\cos\theta|0\rangle - e^{i\phi}\sin\theta|1\rangle)^B$$

The LOSQC error probability P_{err} is lower bounded as: $P_{err} > \frac{1}{4}\left(\frac{1}{2} - \frac{1}{\sqrt{5}}\right) \approx 1.3\%.$

- But what about the sausage states?

Example:



The LOSQC error probability P_{err} is lower bounded as:

$$P_{err} > \frac{1}{9}\left(\frac{1}{2} - \frac{2}{\sqrt{17}}\right) \approx .16\%.$$

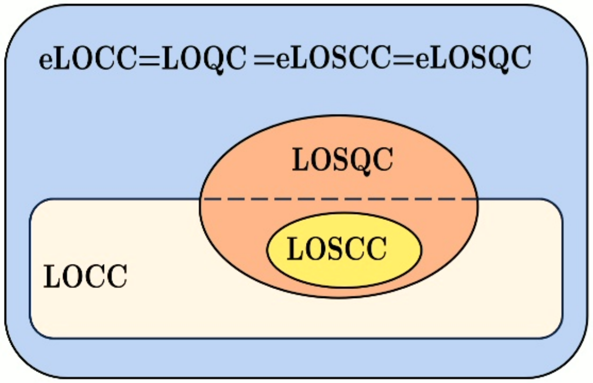
Open problems and future directions

Open problems and future directions

- What are the necessary and sufficient conditions for product state discrimination under LOSCC and LOSQC?

- **Copy complexity**: How many copies of an ensemble state do Alice and Bob need before they can perfectly discriminate by LOSCC?

$$\{|\psi_k\rangle^{\otimes n} = |a_k\rangle^{\otimes n} \otimes |b_k\rangle^{\otimes n}\}$$



- What families of states are distinguishable by LOSQC but not LOCC?

- **Most important question for QPV**: What are the entanglement costs for state discrimination under eLOSCC and eLOSQC?

- **Example: BB84 states**:

$$\begin{cases} |\psi_1\rangle^{AB} = |0\rangle^A \otimes |0\rangle^B & |\psi_3\rangle^{AB} = |+\rangle^A \otimes |1\rangle^B \\ |\psi_2\rangle^{AB} = |1\rangle^A \otimes |0\rangle^B & |\psi_4\rangle^{AB} = |-\rangle^A \otimes |1\rangle^B \end{cases}$$

One ebit suffices for perfect discrimination

Lo and Lau **PRA** 83, 012322 (2011).

LOSQC state discrimination with error

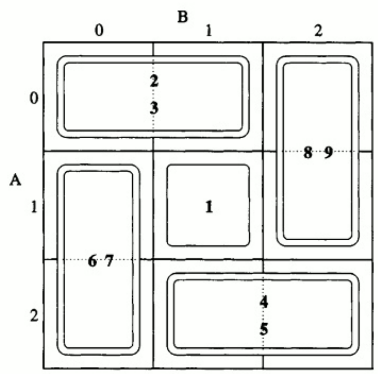
Example: Generalized BB84 states:

$$|\psi_0\rangle^{AB} = |0\rangle^A \otimes |0\rangle^B,$$
$$|\psi_1\rangle^{AB} = |0\rangle^A \otimes |1\rangle^B,$$
$$|\psi_2\rangle^{AB} = |1\rangle^A \otimes (\cos\theta|0\rangle + e^{i\phi}\sin\theta|1\rangle)^B$$
$$|\psi_3\rangle^{AB} = |1\rangle^A \otimes (\cos\theta|0\rangle - e^{i\phi}\sin\theta|1\rangle)^B$$

The LOSQC error probability P_{err} is lower bounded as: $$P_{err} > \frac{1}{4}\left(\frac{1}{2} - \frac{1}{\sqrt{5}}\right) \approx 1.3\%.$$

- But what about the sausage states?

Example:



The LOSQC error probability P_{err} is lower bounded as:

$$P_{err} > \frac{1}{9}\left(\frac{1}{2} - \frac{2}{\sqrt{17}}\right) \approx .16\%.$$

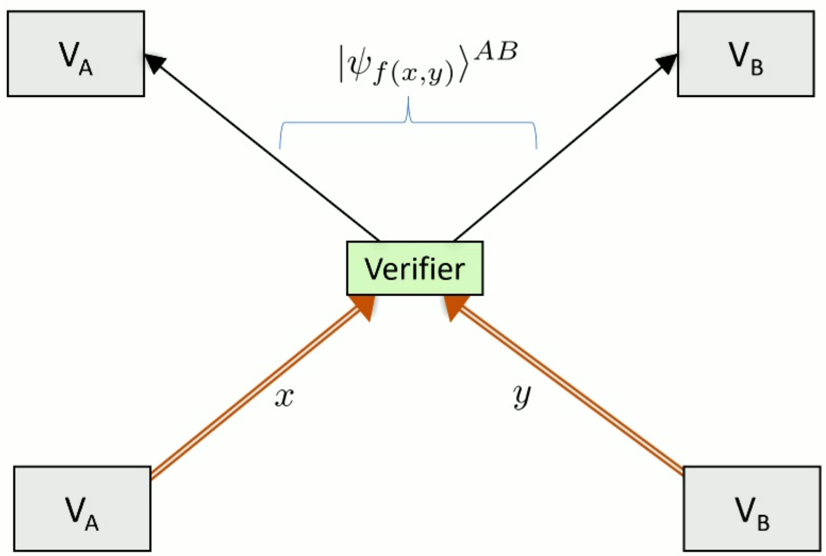
Near-term realization of QPV

- How to implement QPV using today's (or tomorrow's) technology?
- There will generally be a trade-off between the feasibility of implementation and the security guarantees.
- Suggested heuristic benchmark for first-generation QPV implementations:

  The scheme should be secure assuming the adversaries have the same capabilities as the honest prover (in terms of quantum memory, measurements, gates, **channel loss** etc.).

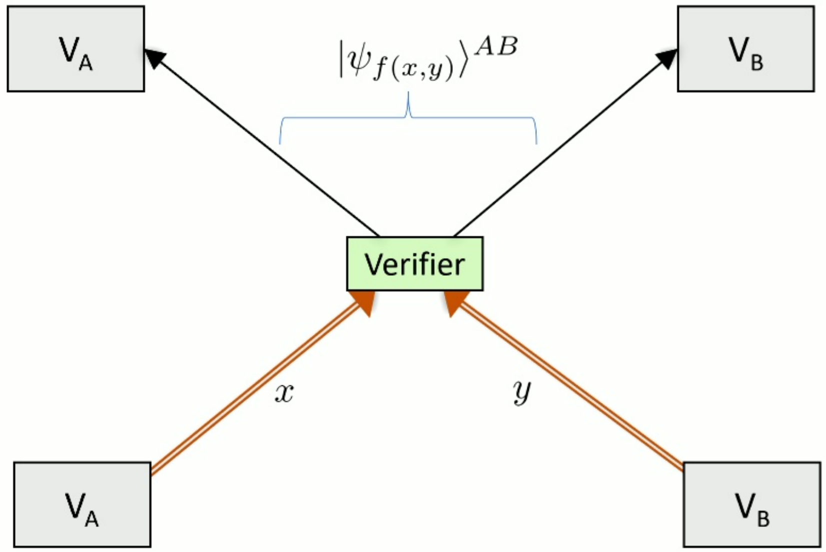
- This allows for greater flexibility in protocol designs.

Entanglement preparation as a QPV task



- **Idea**: Force the honest prover to prepare different entangled states.

Entanglement preparation as a QPV task



- **Idea**: Force the honest prover to prepare different entangled states.

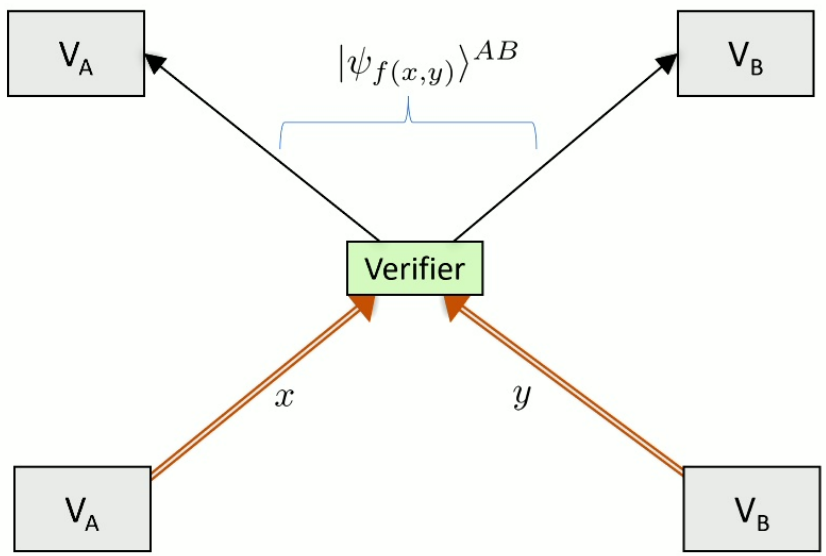
- **Advantage**: No quantum measurement required for the prover; only an entanglement source.

Suitable for deployment on a drone!

- **Intuition for why this works**:
  - Entanglement *preparation* is impossible in the **LOSCC** model.

    Entangled quantum communication is required!

Entanglement preparation as a QPV task



- **Idea**: Force the honest prover to prepare different entangled states.
- **Advantage**: No quantum measurement required for the prover; only an entanglement source.

Suitable for deployment on a drone!

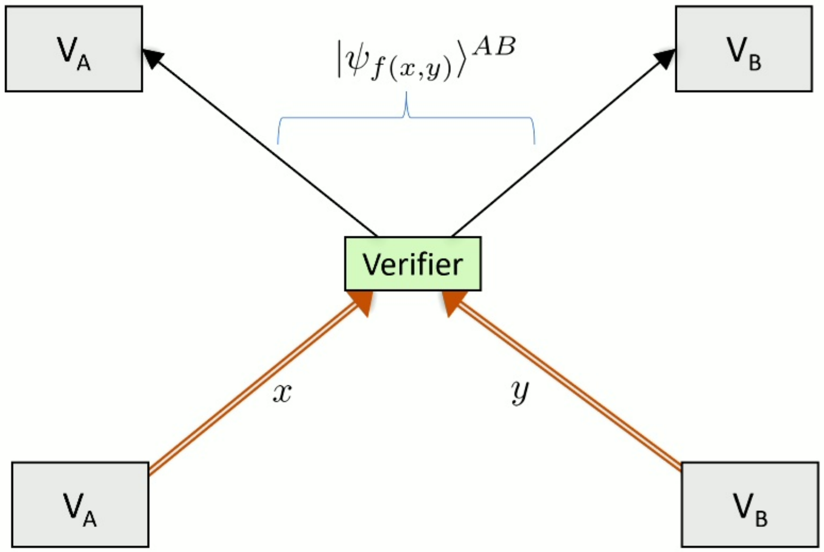
- **Intuition for why this works**:
  - Entanglement *preparation* is impossible in the **LOSCC** model.

    Entangled quantum communication is required!

Theorem [I. George, A. Conrad, E.C., P.K.]:

If the adversaries are not allowed quantum memory, then there is a secure entanglement distribution QPV protocol that tolerates **any rate of loss** and error rate $\delta \leq 3.34\%$.

Entanglement preparation as a QPV task



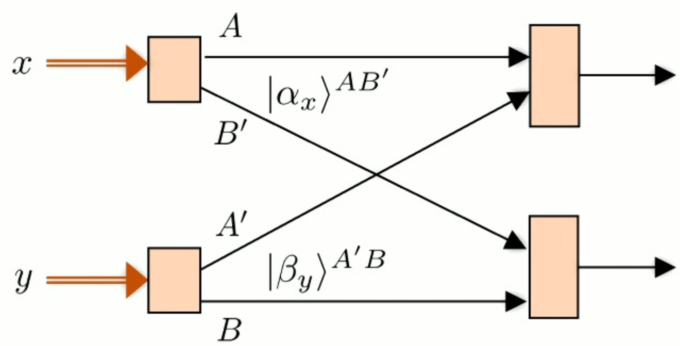
- **Idea**: Force the honest prover to prepare different entangled states.
- **Advantage**: No quantum measurement required for the prover; only an entanglement source.

Suitable for deployment on a drone!

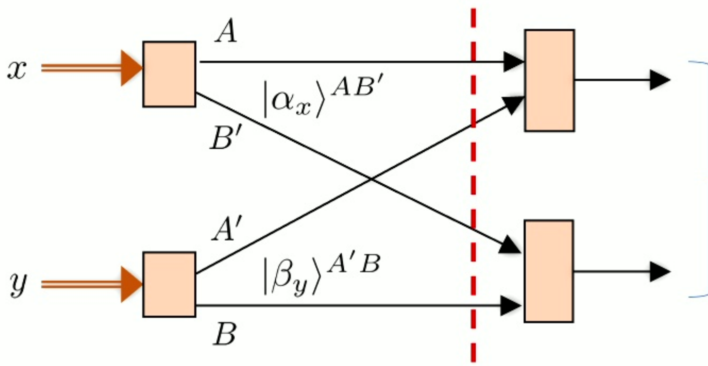
- **Intuition for why this works**:
  - Entanglement *manipulation* is difficult in the **LOSQC** model; i.e. transforming $|\psi_{f(x,y)}\rangle \mapsto |\psi_{f(x',y')}\rangle$

- Choose $|\psi_{f(x,y)}\rangle = \cos[f(x,y)]|00\rangle + \sin[f(x,y)]|11\rangle$

LOSQC entanglement distribution



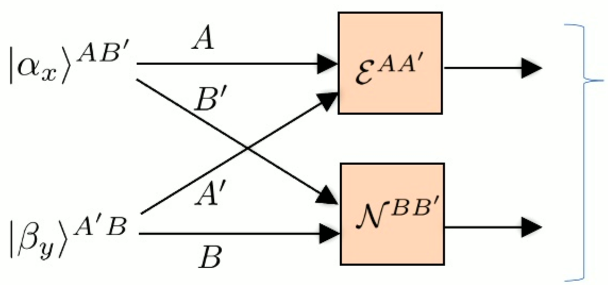
LOSQC entanglement distribution



$$|\psi_{f(x,y)}\rangle = \cos[f(x,y)]|00\rangle + \sin[f(x,y)]|11\rangle$$

Under what conditions for $|\alpha_x\rangle$ and $|\beta_y\rangle$ is this possible?

At this point in time no more communication is allowed.



$$\mathcal{E}^{AA'} \otimes \mathcal{N}^{BB'} \left(|\alpha_x\rangle\langle\alpha_x|^{AB'} \otimes |\beta_y\rangle\langle\beta_y|^{A'B} \right) \approx |\psi_{f(x,y)}\rangle\langle\psi_{f(x,y)}|$$

- One attack is just to prepare all possible entangled states:

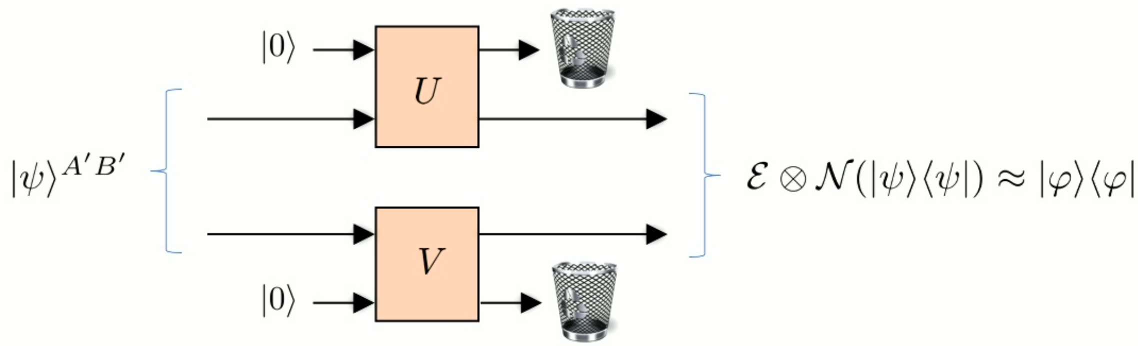
$$|\alpha_x\rangle = \bigotimes_y |\psi_{f(x,y)}\rangle$$

Entanglement manipulation with no communication

General problem statement:

Given two bipartite entangled states $|\psi\rangle^{A'B'}$ and $|\varphi\rangle^{AB}$ how well can Alice and Bob transform $|\psi\rangle \mapsto |\varphi\rangle$ by local operations (and shared randomness)?

$$F_{\mathrm{LO}}(|\psi\rangle \to |\varphi\rangle) := \max_{\mathcal{E},\mathcal{N}} \langle\varphi|\mathcal{E}\otimes\mathcal{N}(|\psi\rangle\langle\psi|)|\varphi\rangle$$

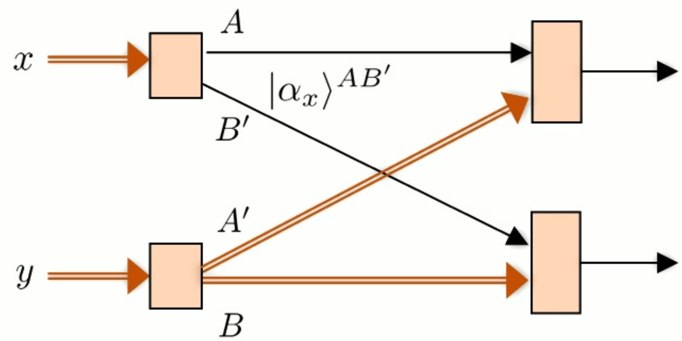


Theorem [I. George, E.C.]:

$$F_{\mathrm{LO}}(|\psi\rangle \to |\varphi\rangle) = \max_{P'} F((P\otimes P')^{\downarrow}, Q^{\downarrow})$$

where $P^{\downarrow}$ and $Q^{\downarrow}$ are the ordered squared-Schmidt coefficients of $|\psi\rangle$ and $|\varphi\rangle$, and $|P'| \leq |P||Q|$.

Security against single ebit attacks



Adversarial power is equal to the honest prover's power.

- Consider a class of attacks in which the adversaries can exchange just a single ebit.

Theorem [I. George, A. Conrad, E.C., P.K.]:

There is an entanglement distribution QPV protocol with transmission rate η and loss rate δ that is secure against one-ebit attacks provided

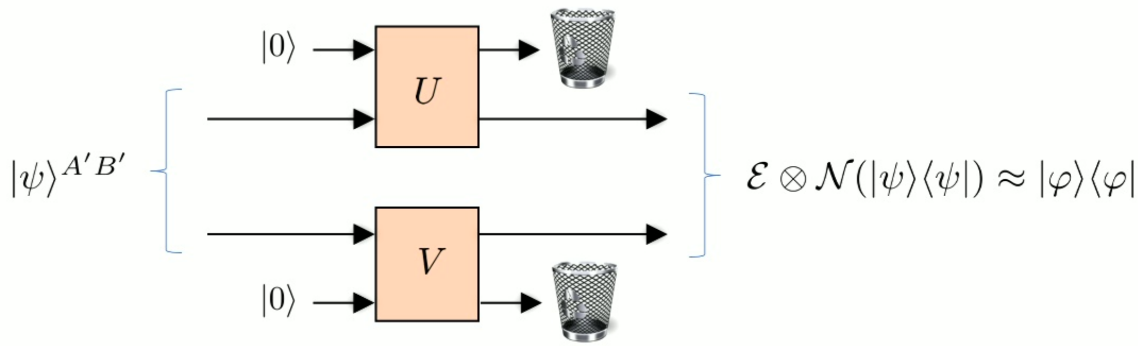
$$\delta(\eta) \leq \min_{p\in[\frac{1}{2},1]} \max_{\theta_{x,y}} \frac{1}{4}(1-\sin(2\theta_{x,y}))\left(\eta - \cos(\theta_{x,y})\sqrt{p} + \sin(\theta_{x,y})\sqrt{1-p})^2\right).$$

Entanglement manipulation with no communication

General problem statement:

Given two bipartite entangled states $|\psi\rangle^{A'B'}$ and $|\varphi\rangle^{AB}$ how well can Alice and Bob transform $|\psi\rangle \mapsto |\varphi\rangle$ by local operations (and shared randomness)?

$$F_{\mathrm{LO}}(|\psi\rangle \to |\varphi\rangle) := \max_{\mathcal{E},\mathcal{N}} \langle\varphi|\mathcal{E}\otimes\mathcal{N}(|\psi\rangle\langle\psi|)|\varphi\rangle$$

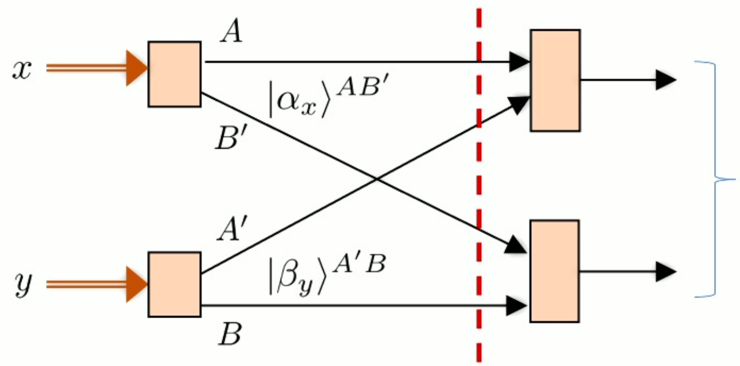


Theorem [I. George, E.C.]:

$$F_{\mathrm{LO}}(|\psi\rangle \to |\varphi\rangle) = \max_{P'} F((P\otimes P')^{\downarrow}, Q^{\downarrow})$$

where $P^{\downarrow}$ and $Q^{\downarrow}$ are the ordered squared-Schmidt coefficients of $|\psi\rangle$ and $|\varphi\rangle$, and $|P'| \leq |P||Q|$.

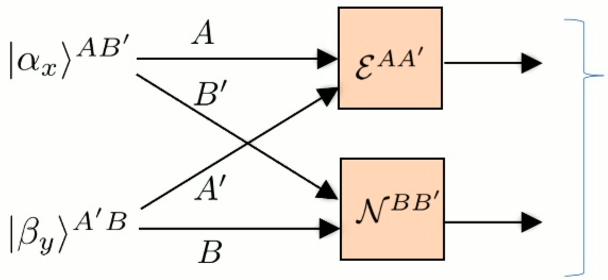
LOSQC entanglement distribution



$$|\psi_{f(x,y)}\rangle = \cos[f(x,y)]|00\rangle + \sin[f(x,y)]|11\rangle$$

At this point in time no more communication is allowed.

Under what conditions for $|\alpha_x\rangle$ and $|\beta_y\rangle$ is this possible?



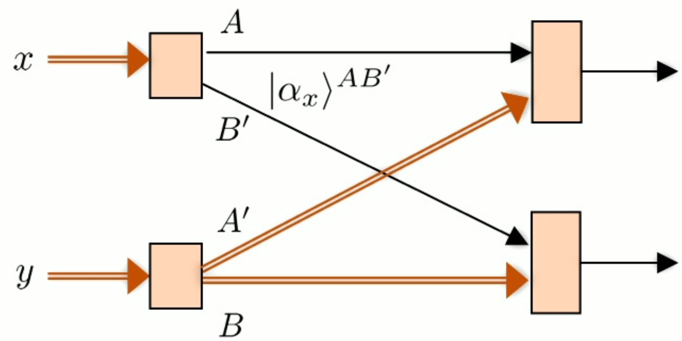
$$\mathcal{E}^{AA'} \otimes \mathcal{N}^{BB'} \left(|\alpha_x\rangle\langle\alpha_x|^{AB'} \otimes |\beta_y\rangle\langle\beta_y|^{A'B} \right) \approx |\psi_{f(x,y)}\rangle\langle\psi_{f(x,y)}|$$

- One attack is just to prepare all possible entangled states:

$$|\alpha_x\rangle = \bigotimes_y |\psi_{f(x,y)}\rangle$$

- But this requires large entanglement. Is it optimal?

Security against single ebit attacks



Adversarial power is equal to the honest prover's power.

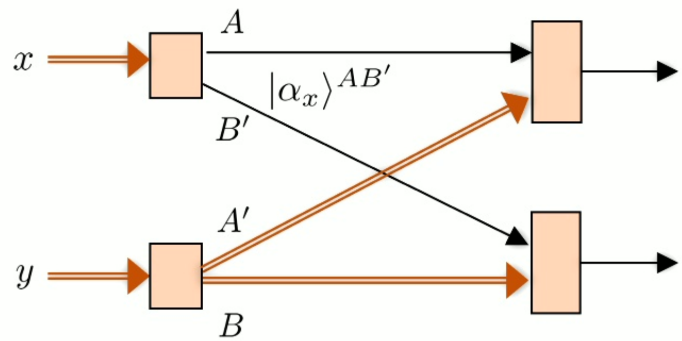
- Consider a class of attacks in which the adversaries can exchange just a single ebit.

Theorem [I. George, A. Conrad, E.C., P.K.]:

There is an entanglement distribution QPV protocol with transmission rate η and loss rate δ that is secure against one-ebit attacks provided

$$\delta(\eta) \leq \min_{p\in[\frac{1}{2},1]} \max_{\theta_{x,y}} \frac{1}{4}(1-\sin(2\theta_{x,y}))\left(\eta - \cos(\theta_{x,y})\sqrt{p} + \sin(\theta_{x,y})\sqrt{1-p})^2\right).$$

Security against single ebit attacks



Adversarial power is equal to the honest prover's power.

- Consider a class of attacks in which the adversaries can exchange just a single ebit.

Theorem [I. George, A. Conrad, E.C., P.K.]:

There is an entanglement distribution QPV protocol with transmission rate η and loss rate δ that is secure against one-ebit attacks provided

$$\delta(\eta) \leq \min_{p\in[\frac{1}{2},1]} \max_{\theta_{x,y}} \frac{1}{4}(1-\sin(2\theta_{x,y}))\left(\eta - \cos(\theta_{x,y})\sqrt{p} + \sin(\theta_{x,y})\sqrt{1-p})^2\right).$$

In particular, we can tolerate an error rate of 0.2% and loss of 3%.

- This is stronger than the original BB84 protocol, which is completely insecure under single ebit attacks.

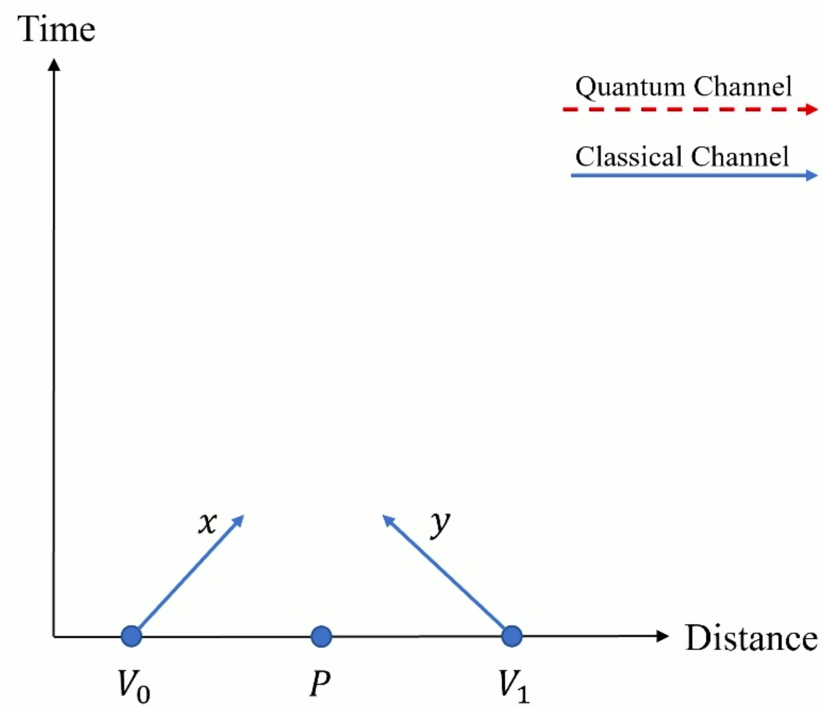

USA TODAY BESTSELLING AUTHORS
S.R. WATSON & RYAN STACKS
QUANTUM ENTANGLEMENT
1
PART ONE
LEGION OF SUPERNATURAL ACADEMY
USA TODAY BESTSELLING AUTHORS
S.R. WATSON & RYAN STACKS
QUANTUM ENTANGLEMENT
2
PART TWO
LEGION OF SUPERNATURAL ACADEMY

Part IV: Experimental Implementation

Our Approach

Our Protocol

1. Verifiers V_0, V_1 send classical random bit strings x, y, respectively
   - Where $x \cdot y = \theta \in (0, \frac{\pi}{4})$



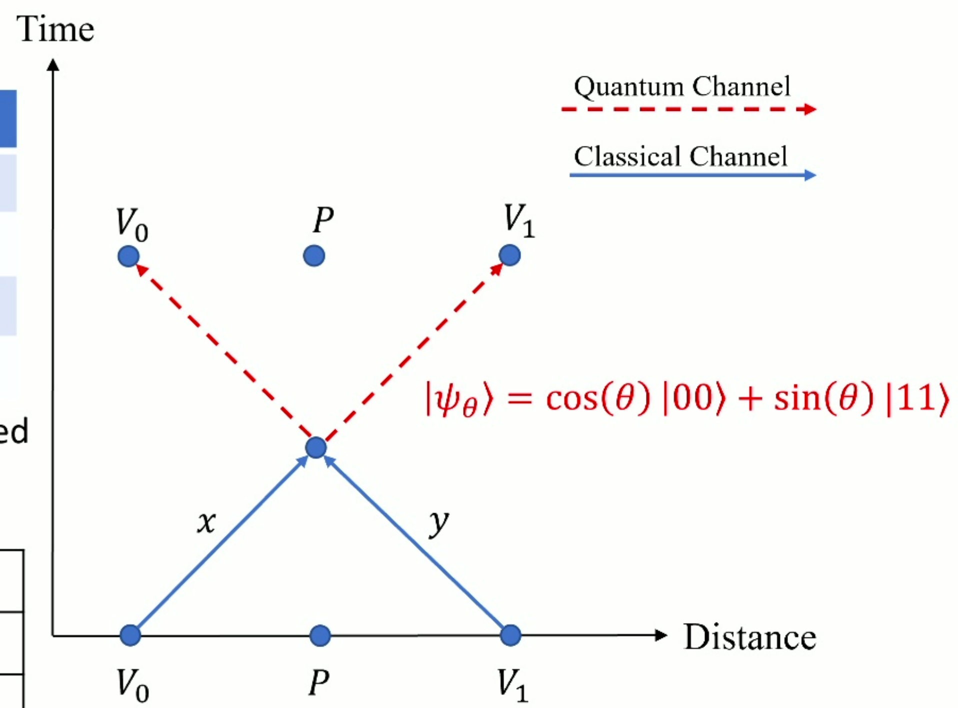
Our Approach

Verifiers select random measurement basis:

Case	V_0	V_1
1	$\|+\rangle\langle+\|, \|-\rangle\langle-\|$	$\|\theta\rangle\langle\theta\|, \|\theta^\perp\rangle\langle\theta^\perp\|$
2	$\|+\rangle\langle+\|, \|-\rangle\langle-\|$	$\|-\theta\rangle\langle-\theta\|, \|-\theta^\perp\rangle\langle-\theta^\perp\|$
3	$\|\theta\rangle\langle\theta\|, \|\theta^\perp\rangle\langle\theta^\perp\|$	$\|+\rangle\langle+\|, \|-\rangle\langle-\|$
4	$\|-\theta\rangle\langle-\theta\|, \|-\theta^\perp\rangle\langle-\theta^\perp\|$	$\|+\rangle\langle+\|, \|-\rangle\langle-\|$

Note: If the target modulated entanglement state is produced $|\psi_\theta\rangle$ by an honest prover, then the following measurement outcomes are not possible

Bad Outcome	V_0	V_1
1	$\|+\rangle\langle+\|$	$\|\theta^\perp\rangle\langle\theta^\perp\|$
2	$\|-\rangle\langle-\|$	$\|-\theta^\perp\rangle\langle-\theta^\perp\|$
3	$\|\theta^\perp\rangle\langle\theta^\perp\|$	$\|+\rangle\langle+\|$
4	$\|-\theta^\perp\rangle\langle-\theta^\perp\|$	$\|-\rangle\langle-\|$



If a Bad Outcome is measured → Cheating is detected

56

Attacks: 1 e-bit + Quantum Memory

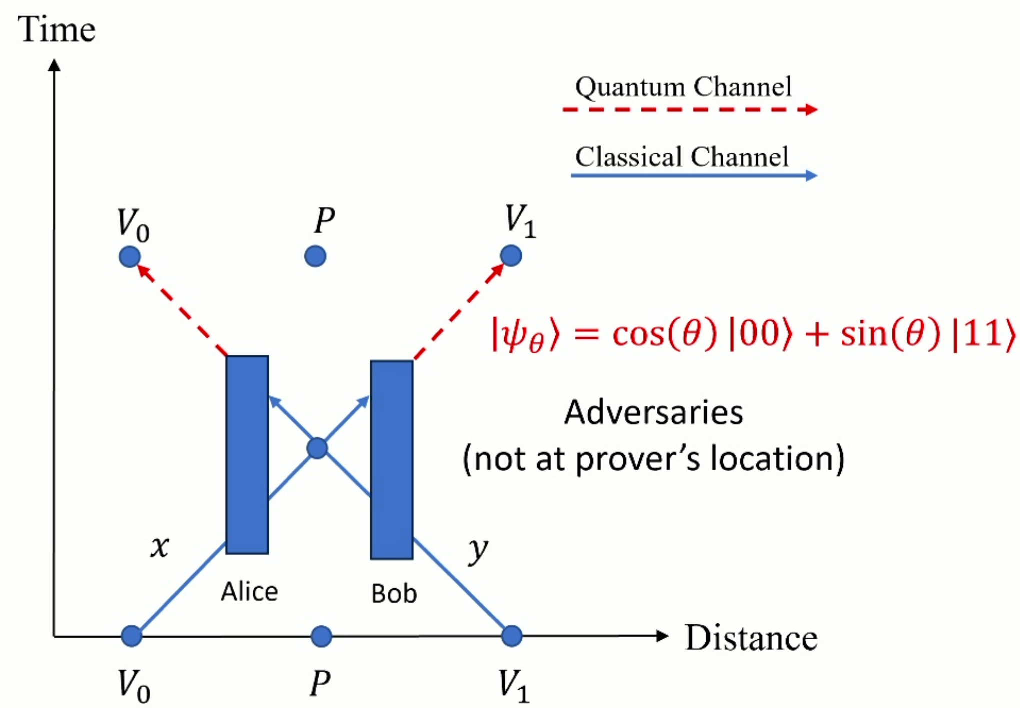
Attackers

- If attackers have ***1 entangled bit*** (e-bit) and a ***quantum memory:***
  - Attackers can attenuate an EPR state to the target state

Start: EPR Pair $|\Phi^+\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$

Local Attenuation: Attenuate Attenuate

Output: $|\psi_\theta\rangle = \cos(\theta)\,|00\rangle + \sin(\theta)\,|11\rangle$



Attackers produce $|\psi_\theta\rangle$ with 50% success probability

If channel loss > 50%, then attackers win

→ Loss intolerance

Attacks: No Quantum Memory

Attackers

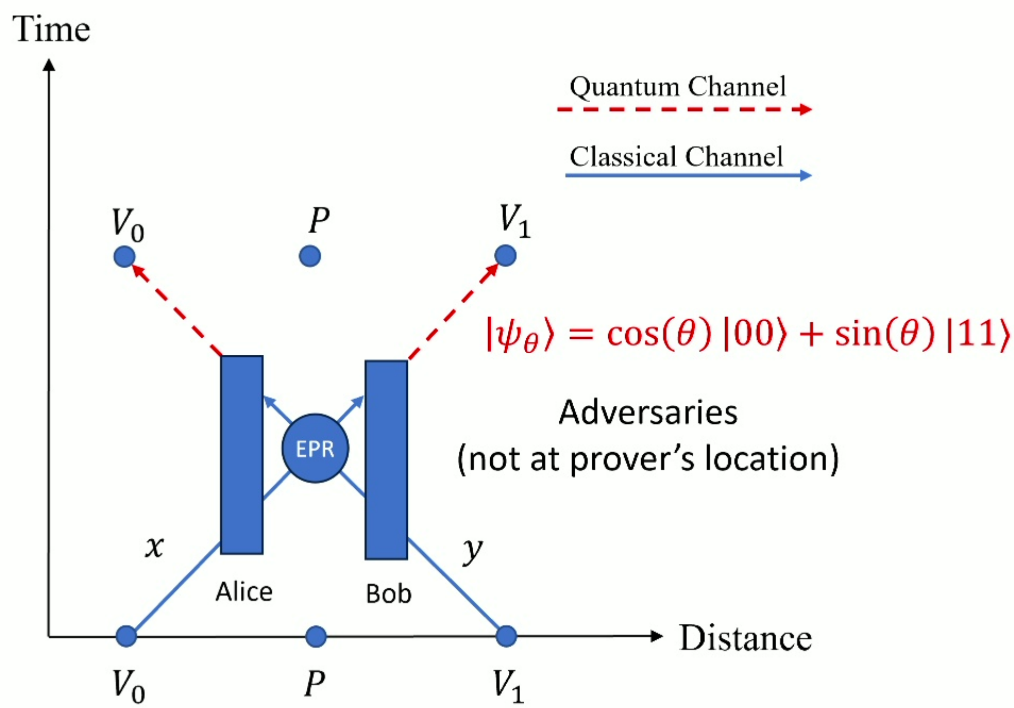
- If attackers have ***1 entangled bit*** (e-bit) and ***no quantum memory:***
  - Attackers can attenuate an EPR state to the target state, but the EPR pair must originate at the prover's location, thus the verifiers win

Start: EPR Pair $|\Phi^+\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$

Local Attenuation: Attenuate | Attenuate

Output: $|\psi_\theta\rangle = \cos(\theta)\,|00\rangle + \sin(\theta)\,|11\rangle$

Attackers produce $|\psi_\theta\rangle$ with 50% success probability



If the attackers lack a quantum memory, then our modulated entanglement protocol achieves complete loss tolerance

Attacks: No Quantum Memory

Attackers

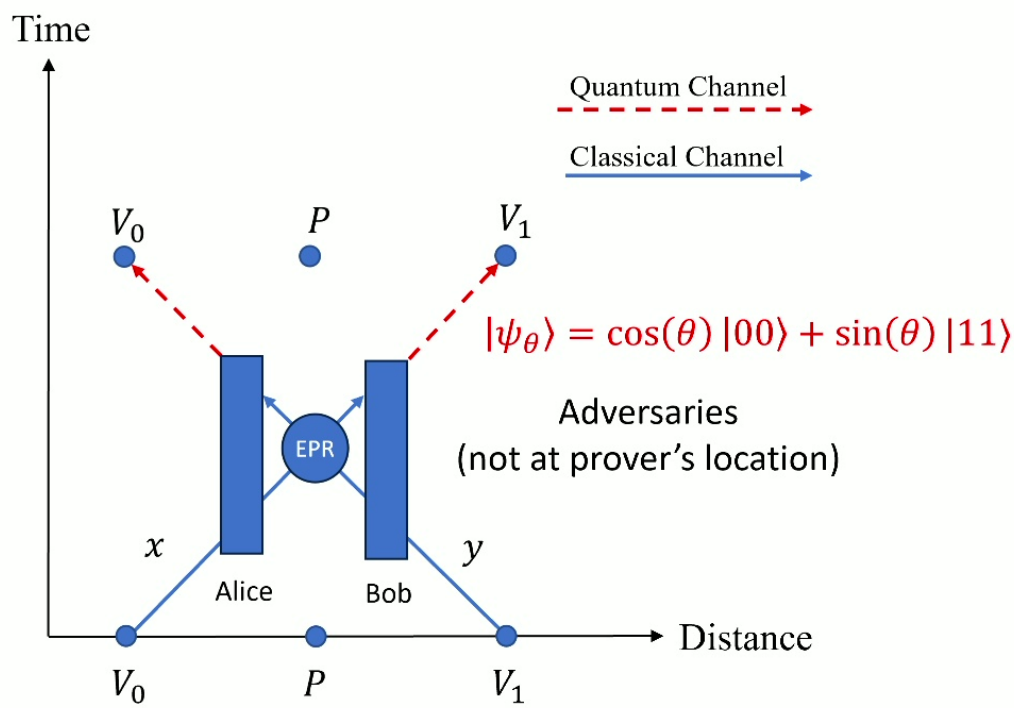
- If attackers have ***1 entangled bit*** (e-bit) and ***no quantum memory:***
  - Attackers can attenuate an EPR state to the target state, but the EPR pair must originate at the prover's location, thus the verifiers win

Start: EPR Pair $|\Phi^+\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$

Local Attenuation: Attenuate Attenuate

Output: $|\psi_\theta\rangle = \cos(\theta)\,|00\rangle + \sin(\theta)\,|11\rangle$

Attackers produce $|\psi_\theta\rangle$ with 50% success probability



If the attackers lack a quantum memory, then our modulated entanglement protocol achieves complete loss tolerance

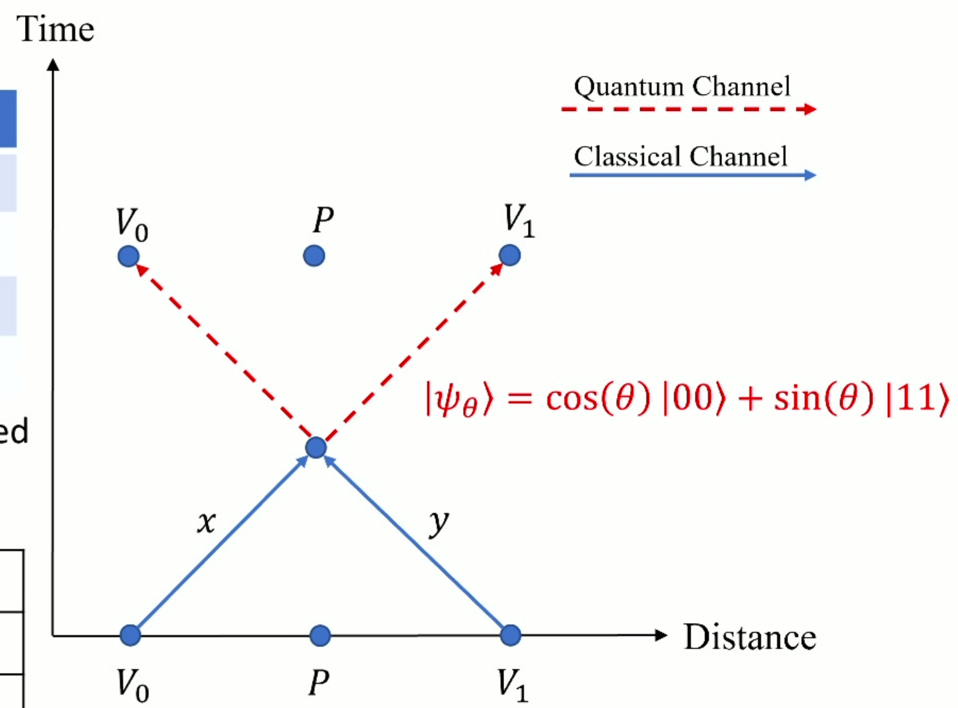
Our Approach

Verifiers select random measurement basis:

Case	V_0	V_1
1	$\vert+\rangle\langle+\vert, \vert-\rangle\langle-\vert$	$\vert\theta\rangle\langle\theta\vert, \vert\theta^\perp\rangle\langle\theta^\perp\vert$
2	$\vert+\rangle\langle+\vert, \vert-\rangle\langle-\vert$	$\vert-\theta\rangle\langle-\theta\vert, \vert-\theta^\perp\rangle\langle-\theta^\perp\vert$
3	$\vert\theta\rangle\langle\theta\vert, \vert\theta^\perp\rangle\langle\theta^\perp\vert$	$\vert+\rangle\langle+\vert, \vert-\rangle\langle-\vert$
4	$\vert-\theta\rangle\langle-\theta\vert, \vert-\theta^\perp\rangle\langle-\theta^\perp\vert$	$\vert+\rangle\langle+\vert, \vert-\rangle\langle-\vert$

Note: If the target modulated entanglement state is produced $|\psi_\theta\rangle$ by an honest prover, then the following measurement outcomes are not possible

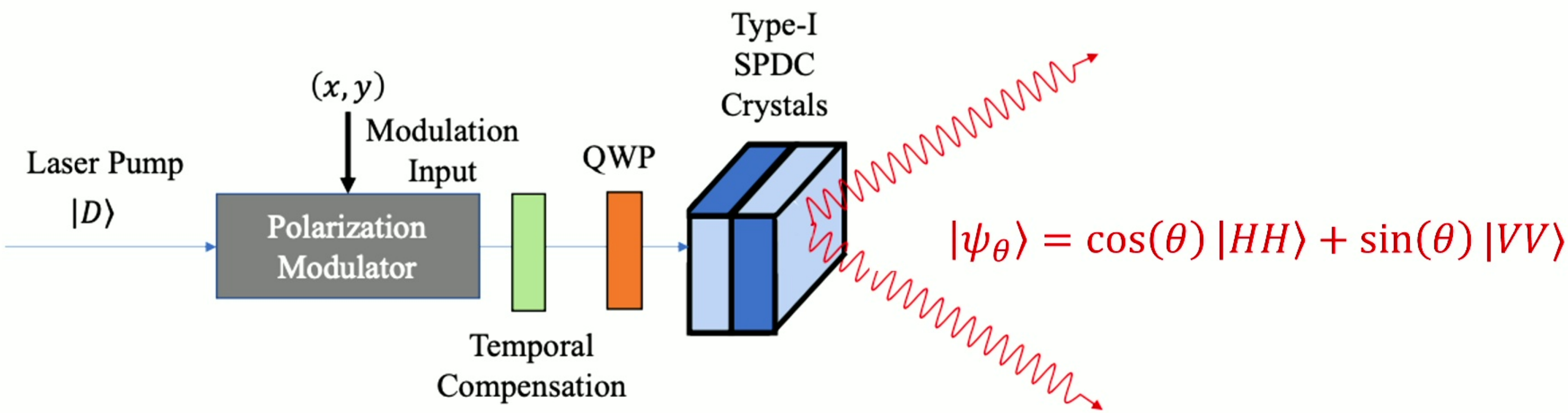
Bad Outcome	V_0	V_1
1	$\vert+\rangle\langle+\vert$	$\vert\theta^\perp\rangle\langle\theta^\perp\vert$
2	$\vert-\rangle\langle-\vert$	$\vert-\theta^\perp\rangle\langle-\theta^\perp\vert$
3	$\vert\theta^\perp\rangle\langle\theta^\perp\vert$	$\vert+\rangle\langle+\vert$
4	$\vert-\theta^\perp\rangle\langle-\theta^\perp\vert$	$\vert-\rangle\langle-\vert$



If a Bad Outcome is measured → Cheating is detected

56

Hardware Implementation



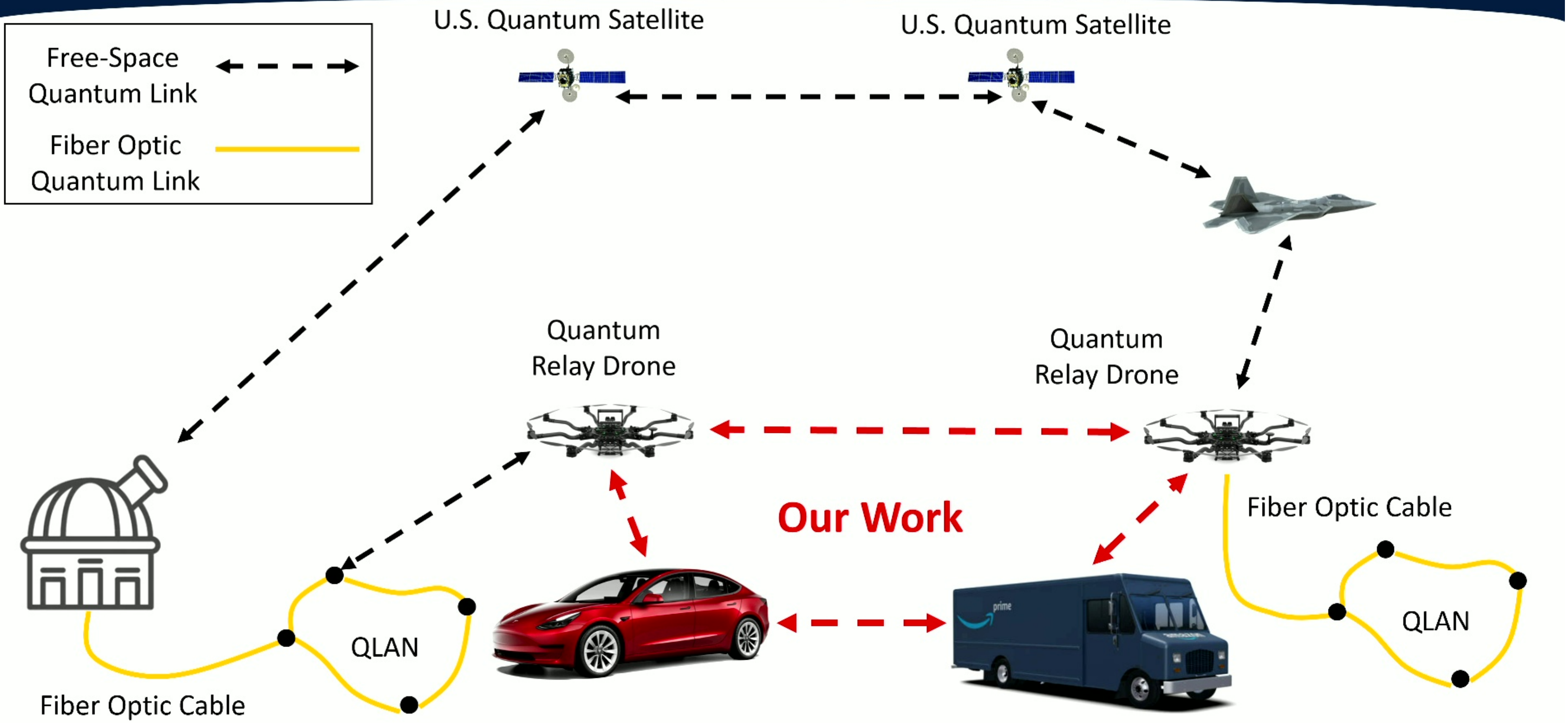
Changing the pump polarization
→ alters how much entanglement

Building upon previous work

Andrew Conrad[1], Samantha Isaac[2], Roderick Cochran[3],
Daniel Sanchez-Rosales[3], Timur Javid[1], Shuen Wu[1,2],
Prof. Daniel Gauthier[3], Prof. Paul Kwiat[1,2]

[1]Department of Electrical Engineering, University of Illinois Urbana-Champaign (UIUC), Urbana, IL
[2]Department of Physics, Illinois Quantum Information Science & Technology Center (IQUIST)
University of Illinois Urbana-Champaign (UIUC), Urbana, IL
[3]Department of Physics, The Ohio State University, Columbus, OH

Free-Space Quantum Network



System Design

System Overview:

- Quantum Transmitter (Alice)
  - Quantum Key Distribution (QKD) source:
    - Resonant cavity LED
    - Decoy state
    - Polarization encoded
  - Custom optics benches
- Quantum Receiver (Bob)
  - Single-Photon Detectors (SPCM-AQ4C)
  - FPGA-based Time-Tagger
  - Qubit-based Time Synchronization (Post-processing)
- Pointing, Acquisition, and Tracking (PAT) system
- Mobile Platforms:
  - Drone
  - Car

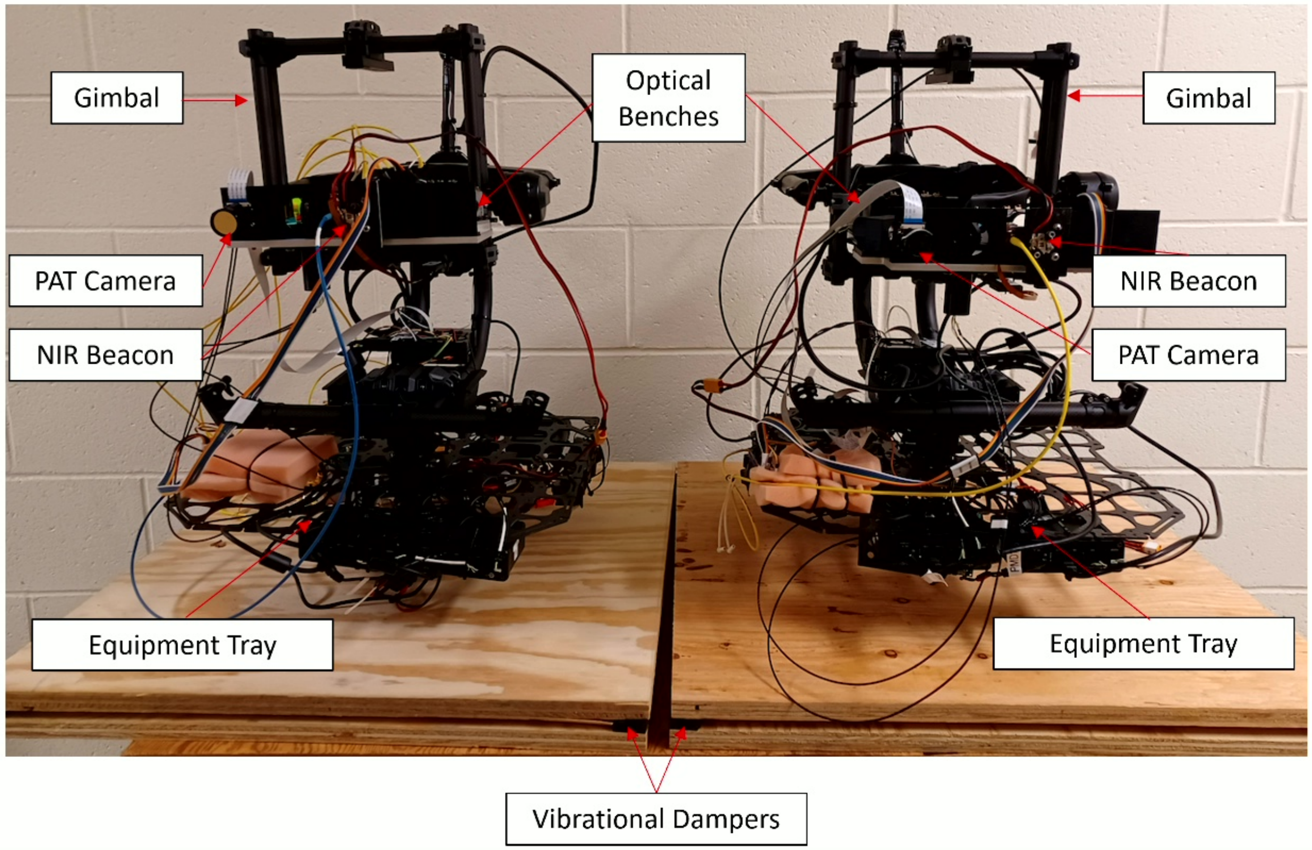
Image Courtesy Timur Javid

Modular Design

Modular Design:

- Our QKD system shares no resources with host mobile platform
  - Power
  - Control
  - Communication
- Single quick-release connection with drone
  → Place QKD transmitter (receiver) on other platforms (*e.g.*, vehicle) with no required hardware changes

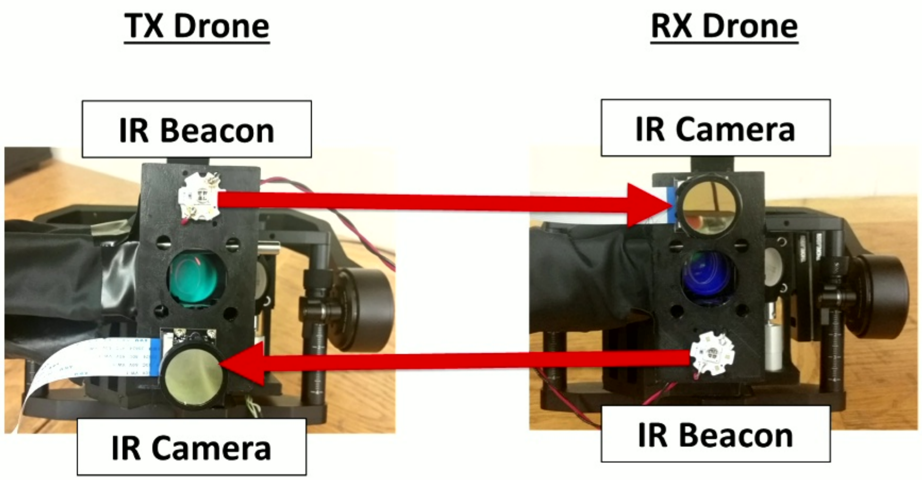
QKD Transmitter (Alice) **QKD Receiver (Bob)**

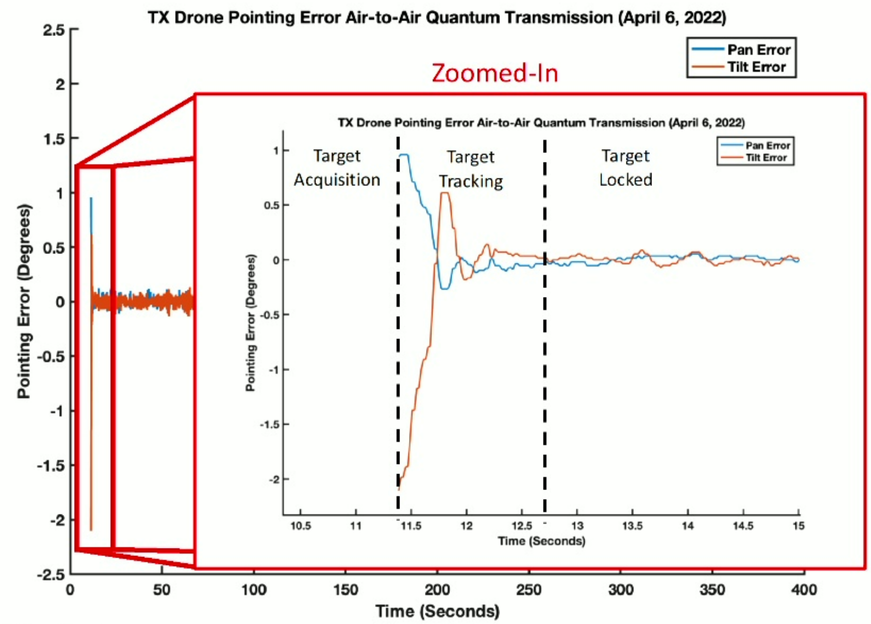


PAT Subsystem (Course Adjustment)

Outer-Control Loop Calibration

- Initial Pointing, acquisition, and course pointing
- IR Beacon/IR Camera
- Image processing to identify location in camera's reference frame
- Feedback Control





Gimbal (Movi Pro)

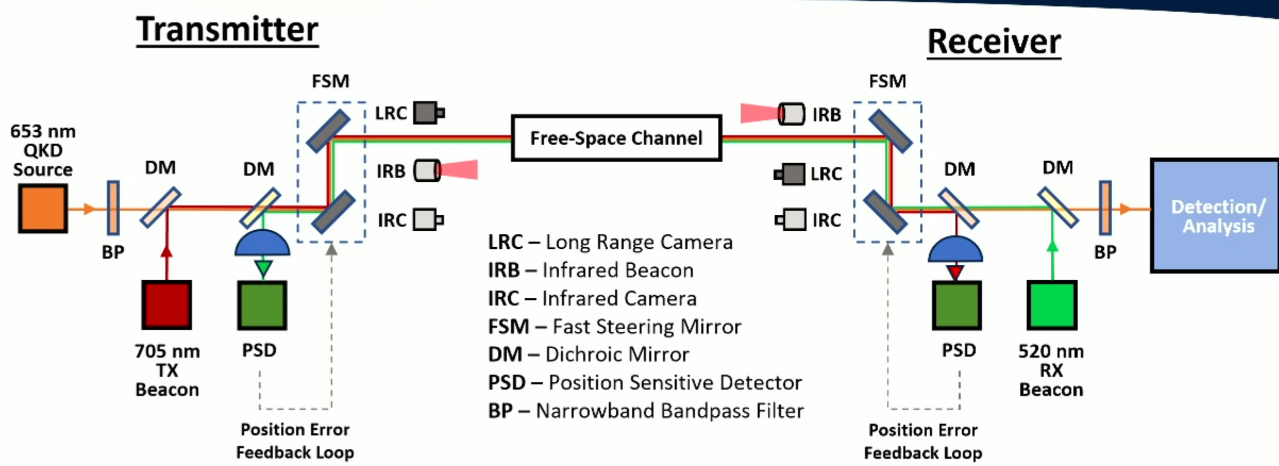
- Tracking Performance:
  - Pan RMS Error = 0.0230°
  - Tilt RMS Error = 0.0263°

Gimbal Jitter Specification = 0.02°

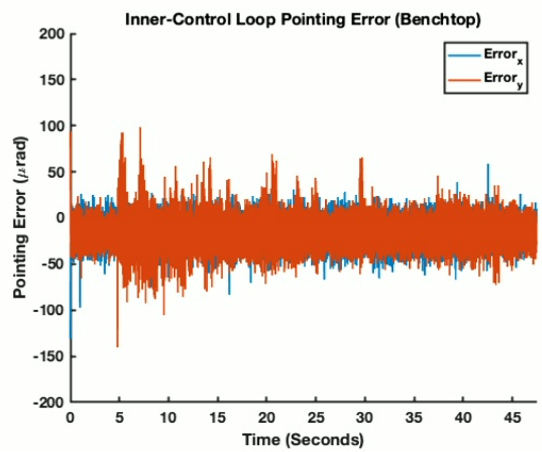
PAT Subsystem (Fine Adjustment)

PAT Subsystem (Fine Adjustment)

- Co-propagating laser beacons
  - Transmitter: 705-nm beacon
  - Receiver: 520-nm beacon
- Fast Steering Mirrors + Position Sensitive Diode (PSD)
- Senses incoming beacon beam Angle of Arrival (AoA)
- Raspberry Pi single-board computer
- Local (no PAT communication between drones)



Fast Steering Mirrors (Model LR-17)



Pointing Error_x = 21.1 μrad
Pointing Error_y = 22.9 μrad

Air-to-Air Classical Locking

Drone Platform

- Alta 8 Pro Drone
- 20 lbs payload capacity
- Two 10,000 mA-hr Lithium Polymer Batteries

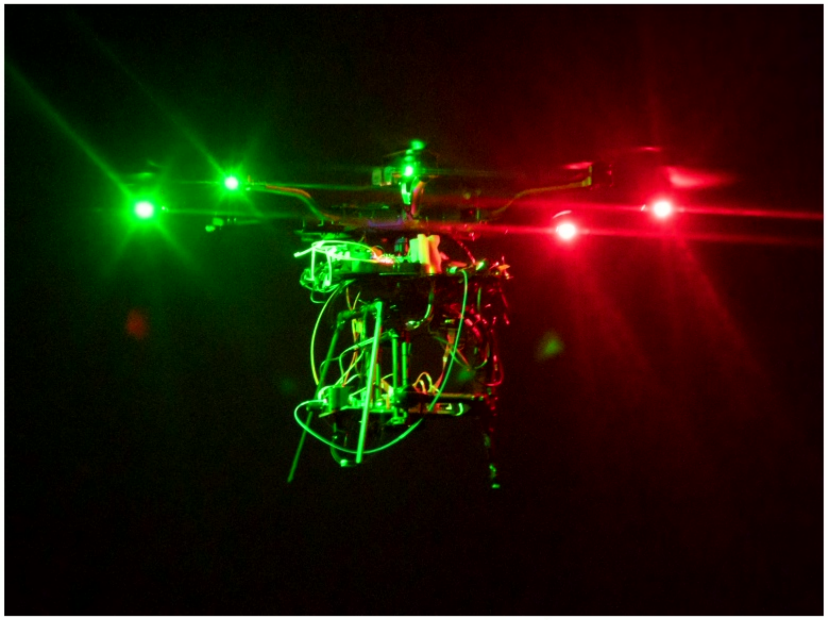
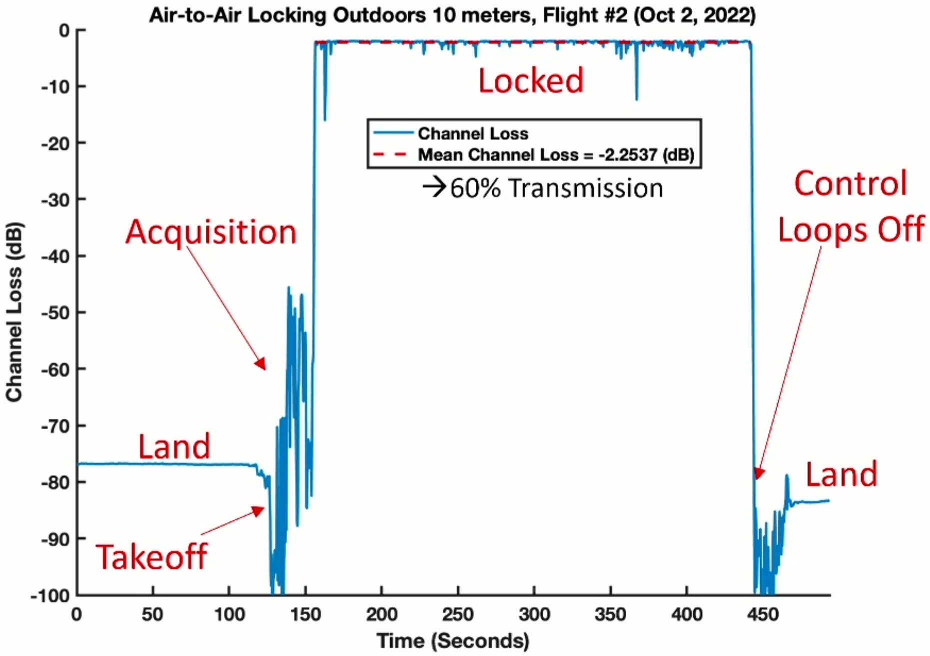


Image Courtesy Timur Javid

System Characterization

- Classical Air-to-Air Locking into multimode fiber
- Average 2.25 dB Channel Loss (60% transmission)
- 10-meter distance



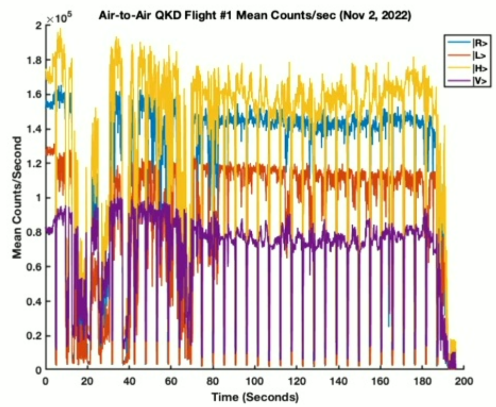
Drone Air-to-Air QKD Flights (Nov 2nd, 2022)

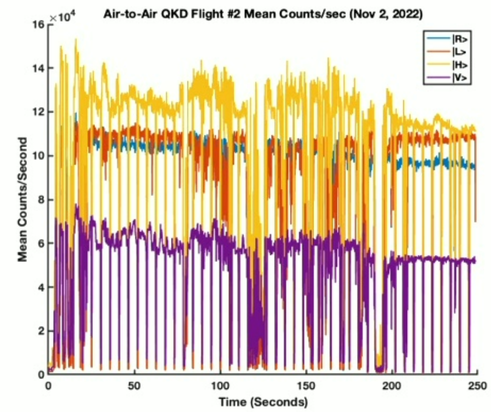
Air-to-Air QKD Setup
- Both drones hovering
- 10-meter distance between drones
- Altitude ~5 meters above ground

Quantum Transmission
- Average QBER =2.9% (R/L Basis), 3.0% (H/V Basis)
- 1st demonstration of drone-to-drone QKD
- Collaborating with Lütkenhaus group to develop tailor-made finite key analysis

UNIVERSITY OF WATERLOO

Image Courtesy Timur Javid





	Flight #1	Flight #2	Flight #3
QBER (R/L)	2.0%	1.8%	5.0%
QBER (H/V)	3.6%	3.1%	2.4%
Mean Photon Number μ	0.78	0.78	0.73

70 mph Vehicle-to-Vehicle Quantum Transmission

Car-to-Car Quantum Setup

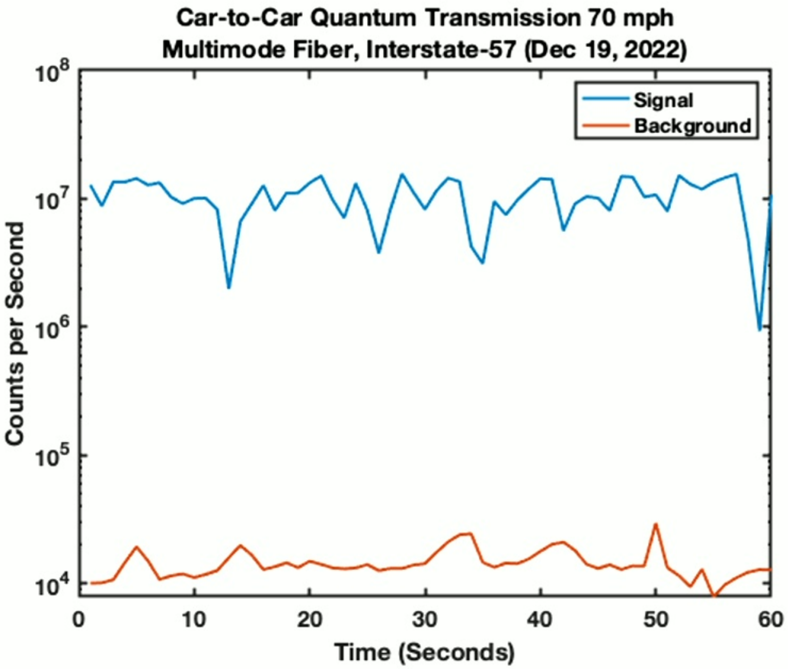
- 70 mph
- Interstate Highway (I-57)
- Outer-Control Loop only (Near-IR Beacon)
- No alignment lasers
- Attenuated laser quantum source
- Coupled into multi-mode and single-mode fiber
- Achieved 70 mph 28.6 dB SNR into multimode fiber and 17.4 dB SNR into single-mode fiber
- **We believe this is the first demonstration of a car-to-car quantum link on public highway**

Image Courtesy Google Earth

70 mph Car-to-Car into Multimode Fiber

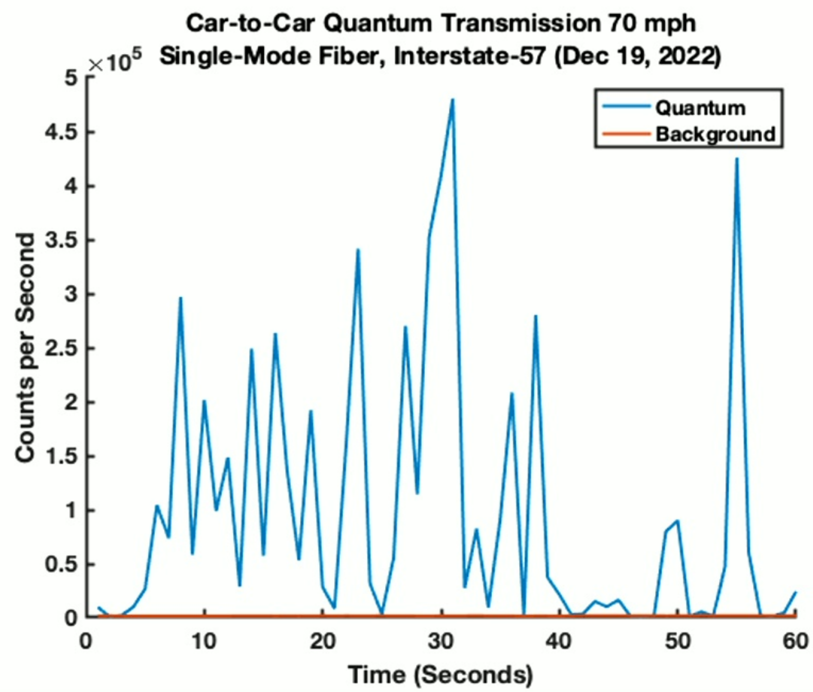
Multimode Fiber

- Mean Signal = 10,465,380 counts/sec
- Mean Background = 14,440 counts/sec
- Mean Signal-to-Noise (SNR) = 28.6 dB



Single-Mode Fiber (SMF)

- SMF needed for quantum teleportation, entanglement swapping, etc.
- Mean Signal = 97,080 counts/sec
- Mean Background = 1,730 counts/sec
- Mean Signal-to-Noise (SNR) = 17.4 dB



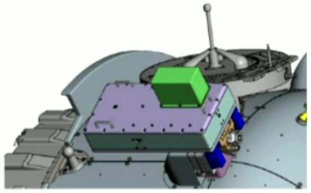
SEAQUE: Space Entanglement Annealing QUantum Experiment

ILLINOIS

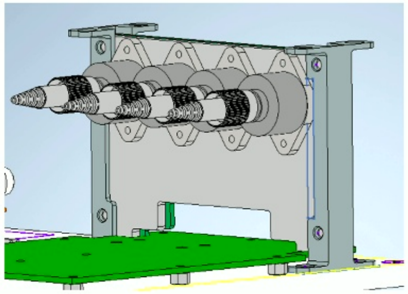
Project Lead
Optical Payload
Control Board

JPL
Funding and Program Management

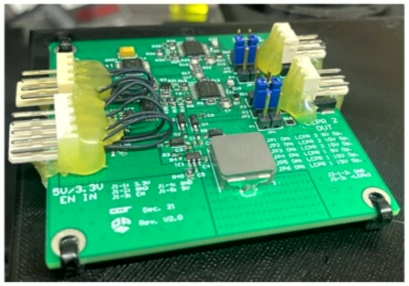
Laboratory for Advanced Space Systems at Illinois
Electrical Platform and Interface with Nanoracks



University of Waterloo
Detector Module



National University of Singapore
Liquid Crystal Electronics



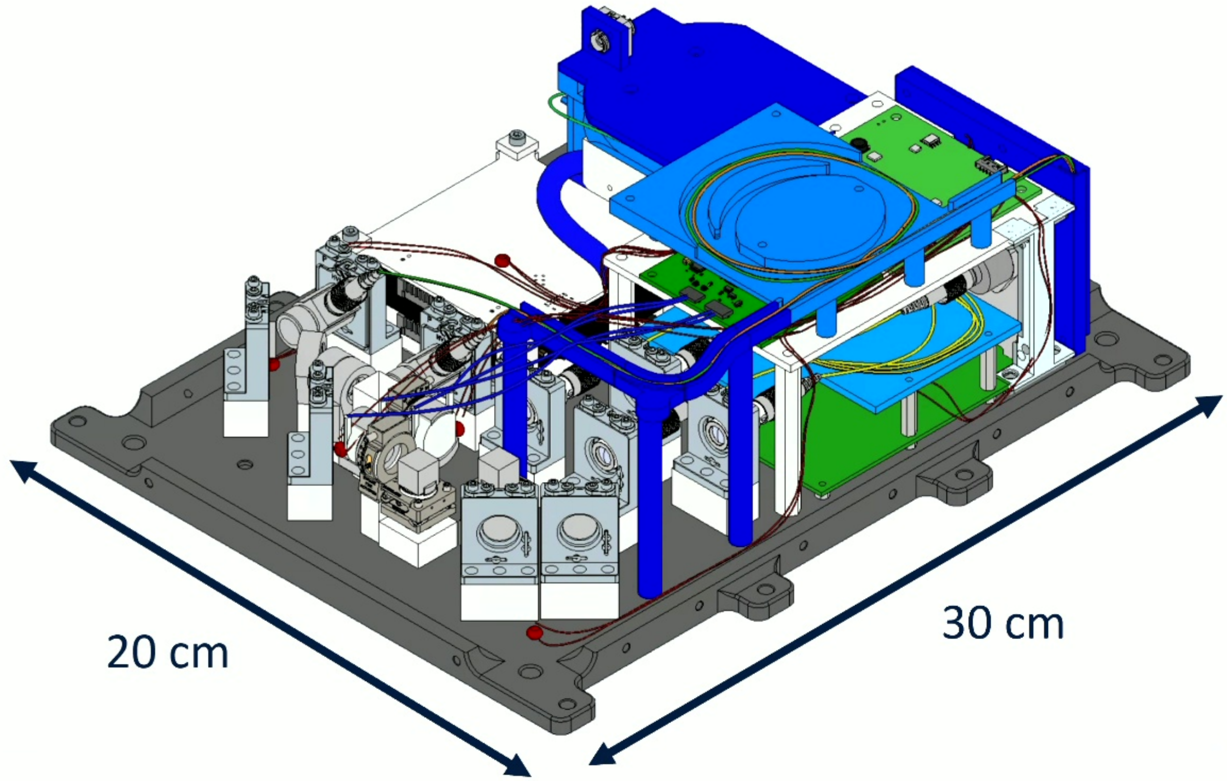
AdVR
SPDC waveguide

Goals

Goal 1

Demonstrate capabilities of quantum light systems in space

- Create and verify entanglement
- Integrated optics



Goals

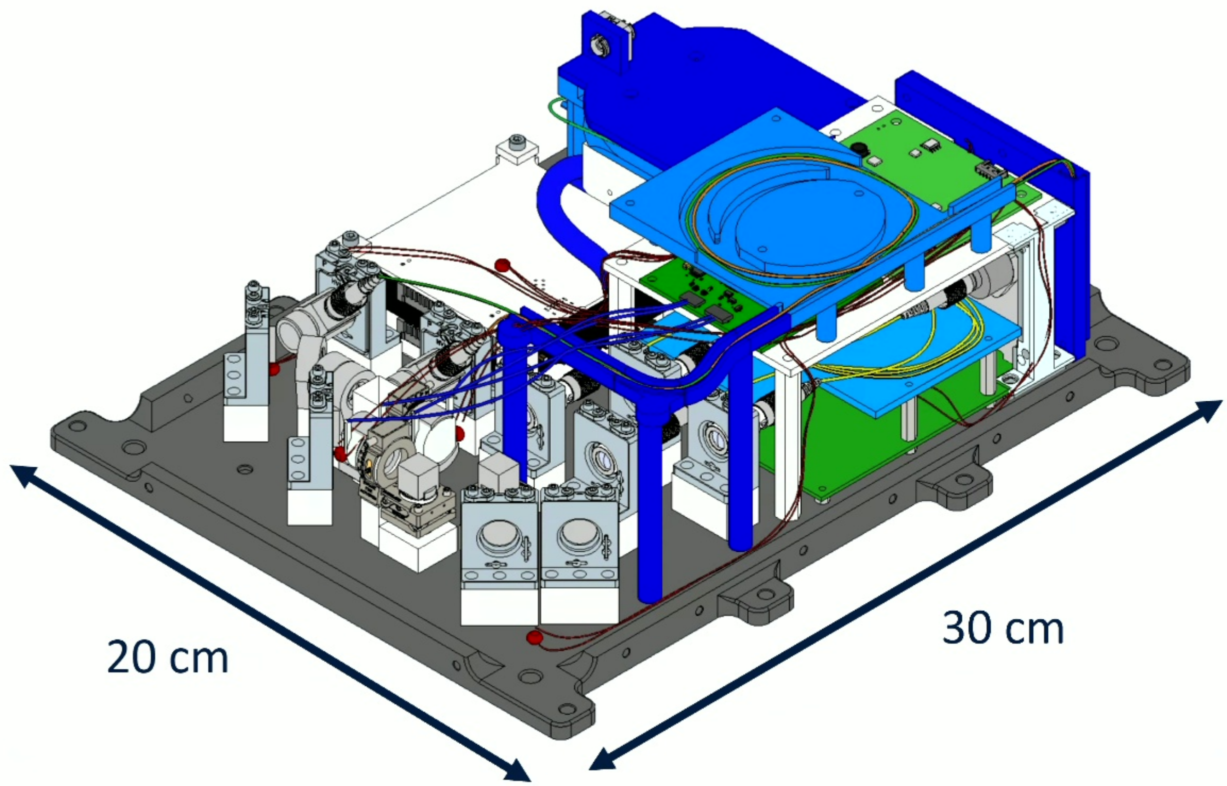
Goal 1

Demonstrate capabilities of quantum light systems in space

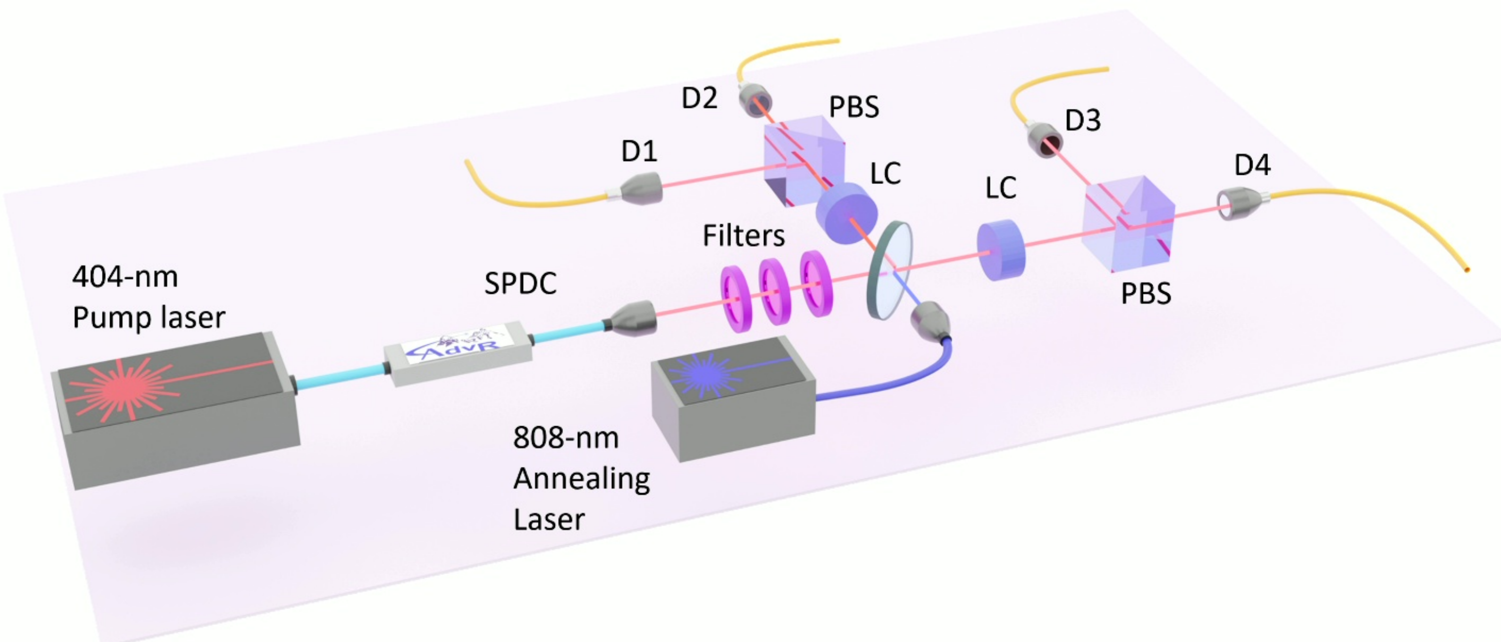
- Create and verify entanglement
- Integrated optics

Goal 2

Perform detector "self-healing" through laser annealing

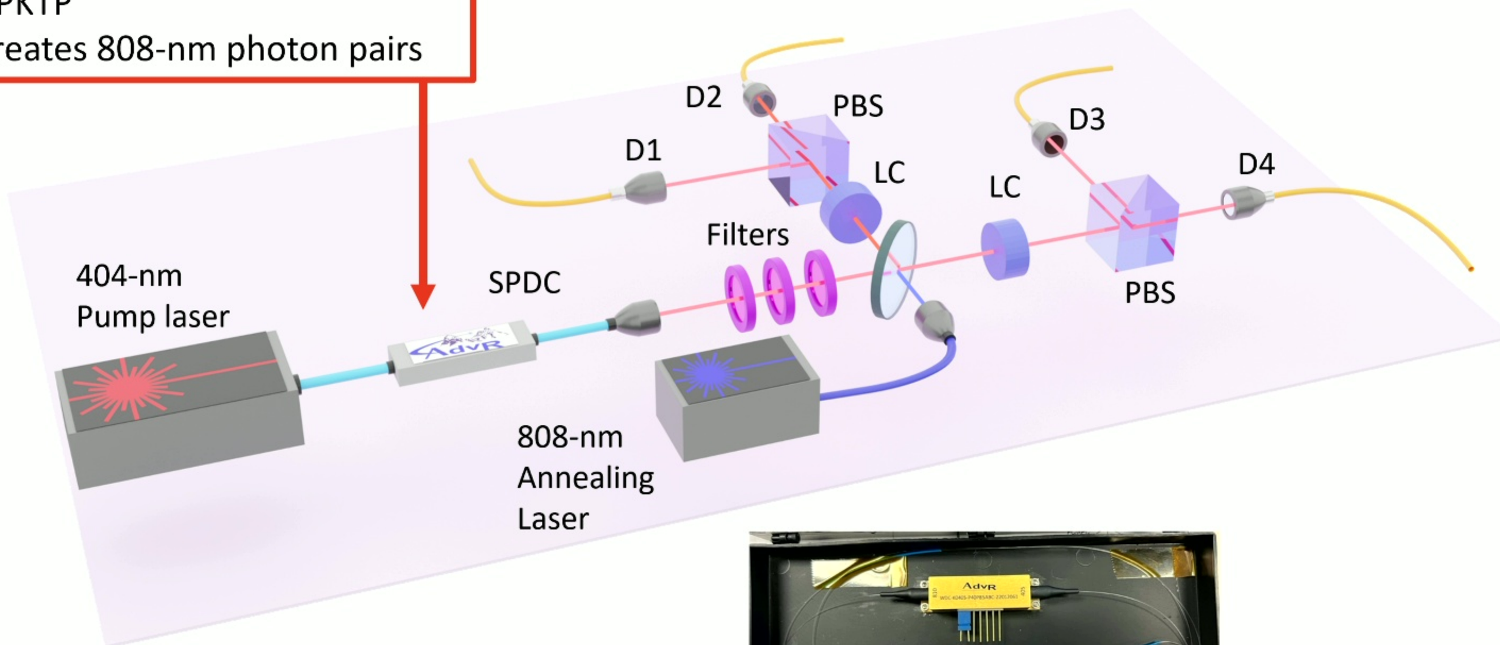


Entanglement Source

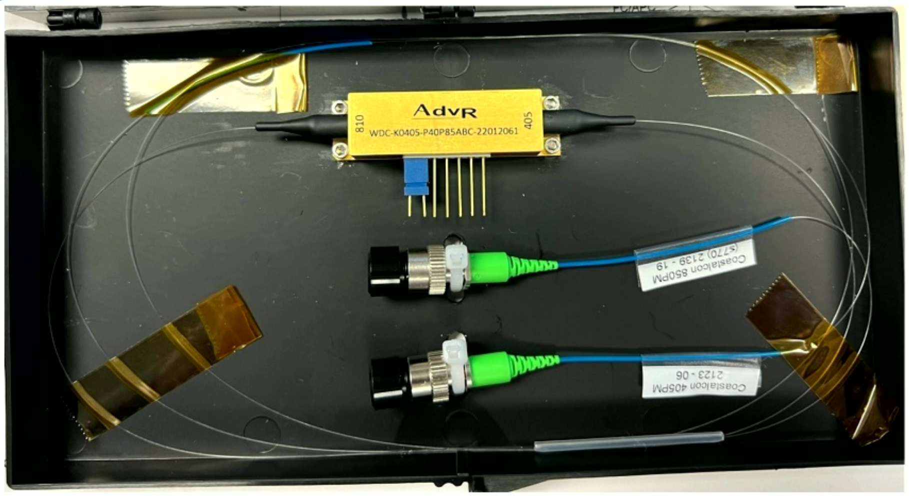


Entanglement Source

Waveguide:
- PPKTP
- creates 808-nm photon pairs

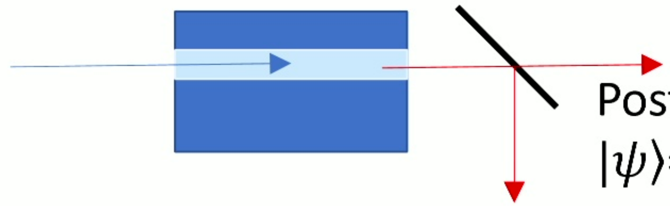


SEAQUE Entanglement Source



PPKTP waveguide, Type II

405nm → 810 nm (H) + 810 nm (V)



Postselected state:

$|\psi\rangle = |H\rangle|V\rangle + |V\rangle|H\rangle$

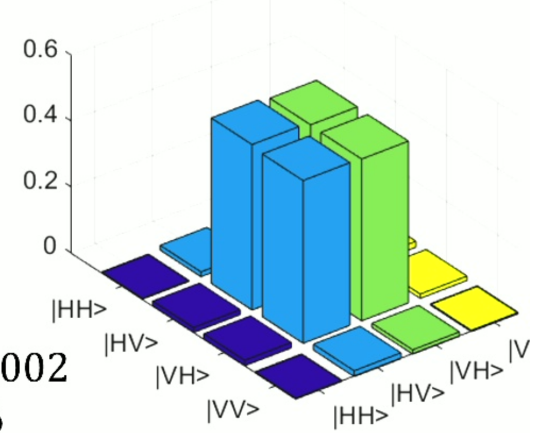
Fiber-In/Fiber-Out Timing Compensated SPDC Module

WDC-K0405-P40P85ABC

SN: 22012061

Optical Characterization

Pump Wavelength	404.88 nm
Pair Rate	25 MHz/mW (power in input fiber)
2-Photon Visibility	95% with 3 nm filter
Module Degeneracy Temperature	45.1°C



Fidelity: 0.991 ± 0.001

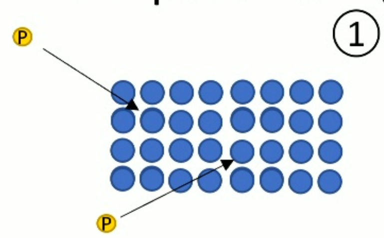
Concurrence: 0.984 ± 0.002

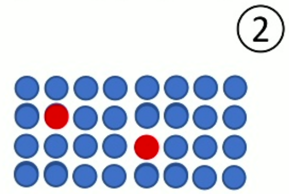
Bell Test: 2.758 ± 0.006

AdvR

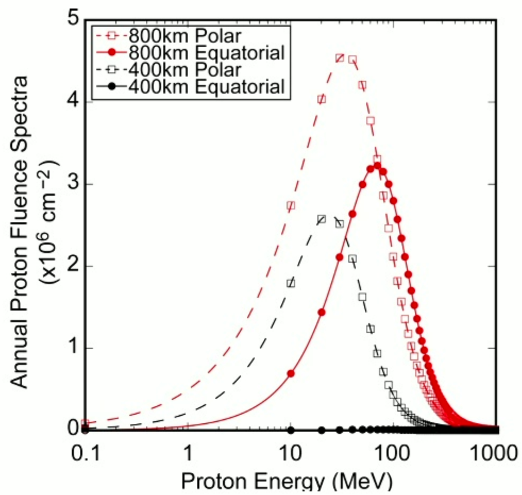
Radiation & Single-Photon Detectors

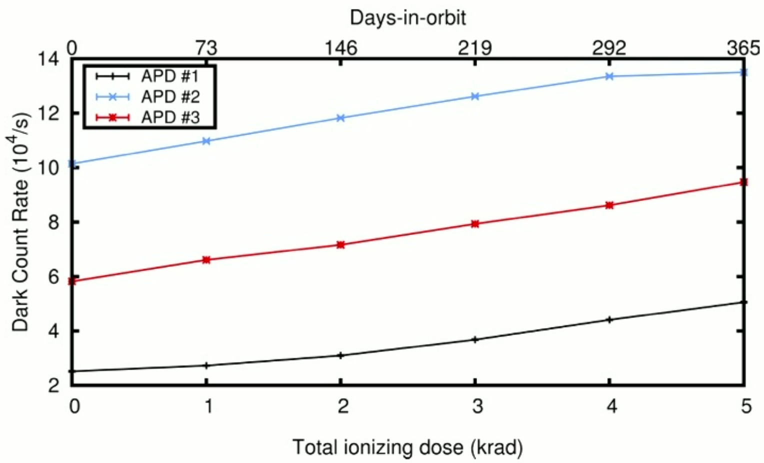
Si Avalanche PhotoDiode single-photon detectors accumulate damage while exposed to high energy protons in low-earth orbit.





Protons ionize and displace atoms in the semiconductor crystal, raising the number of detector **dark counts** (erroneous detection events).





Tan, Chandrasekara, Cheng, & Ling, “Silicon avalanche photodiode operation and lifetime analysis for small satellites,” Opt. Expr. **21,** 16946 (2013)

Healing through Annealing

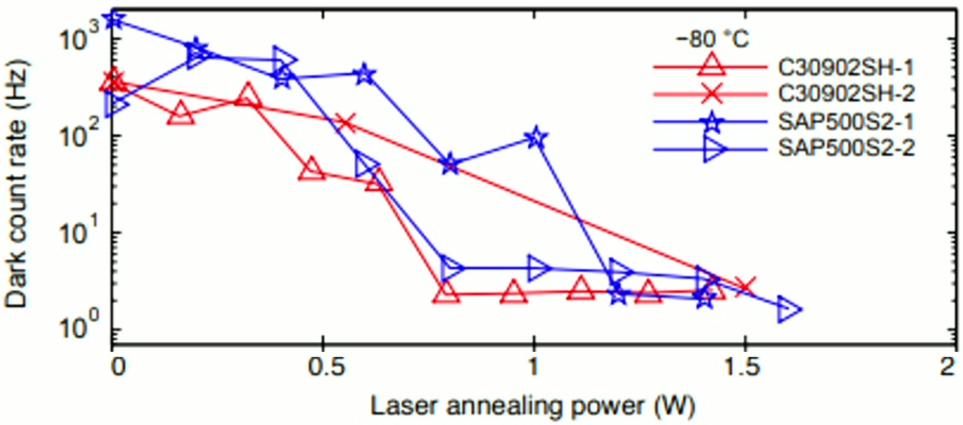
Radiation damage on single photon detectors can be **reduced** through annealing.

Thermal Annealing:

- Entire detector is heated.
- Found to reduce dark count rate by ~6.6 times

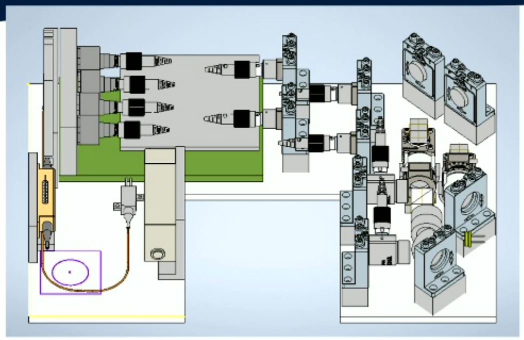
Laser Annealing:

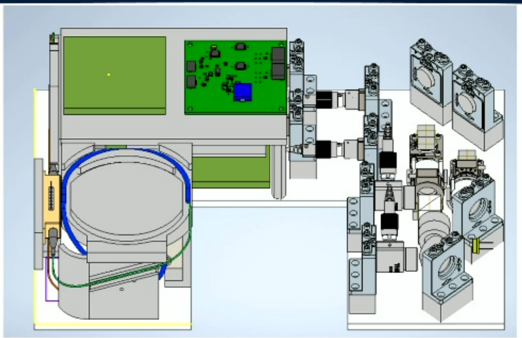
- A high power (~0.5-2 Watts) laser sined onto the detector (provides a focused heating)
- Found to reduce dark count rate by 5.5-758 times (near -80℃)

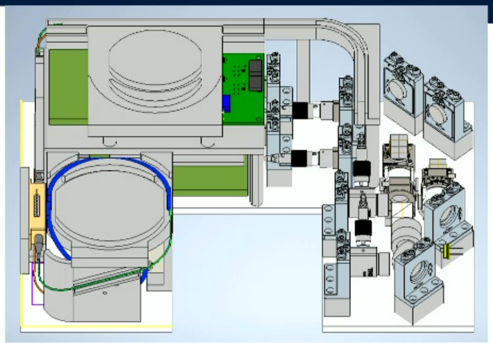


Lim, *et al.* "Laser annealing heals radiation damage in avalanche photodiodes", *EPJ Quantum Technol.* **4,** 11 (2017)

Layout design and Assembly Order



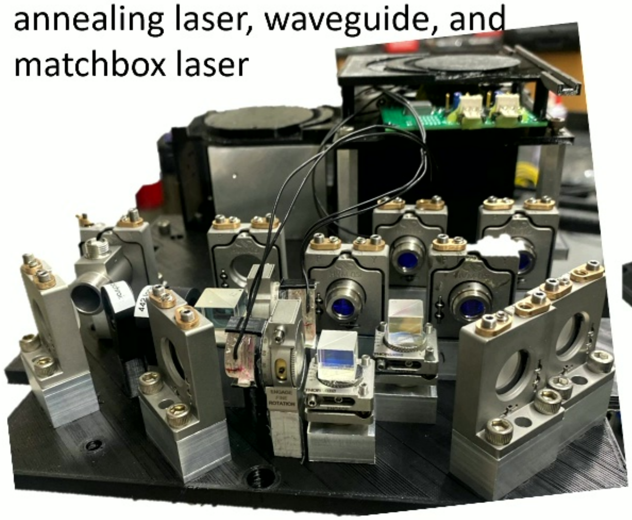


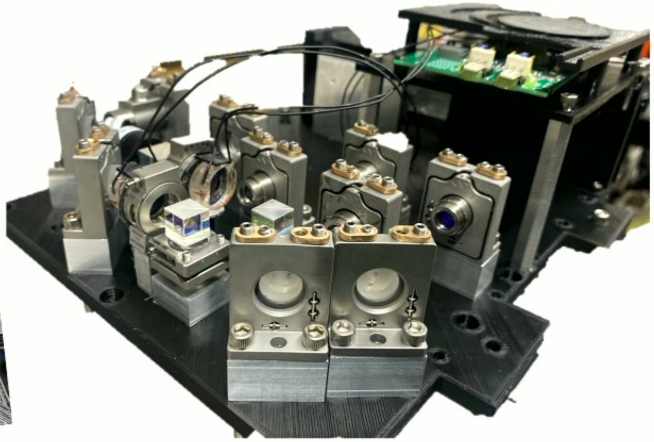


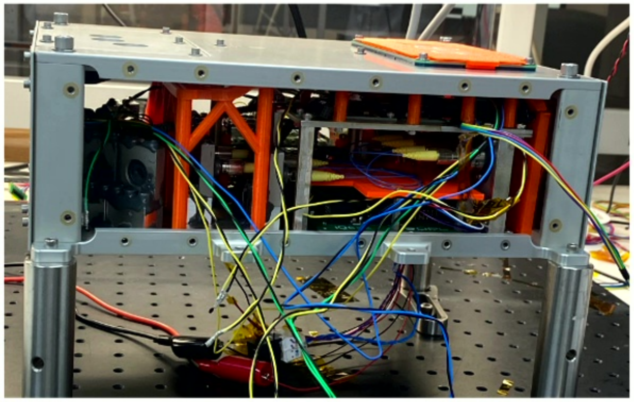
Step 1: mount optics, detector board, annealing laser, waveguide, and matchbox laser

Step 2: mount electronics and fiber supports

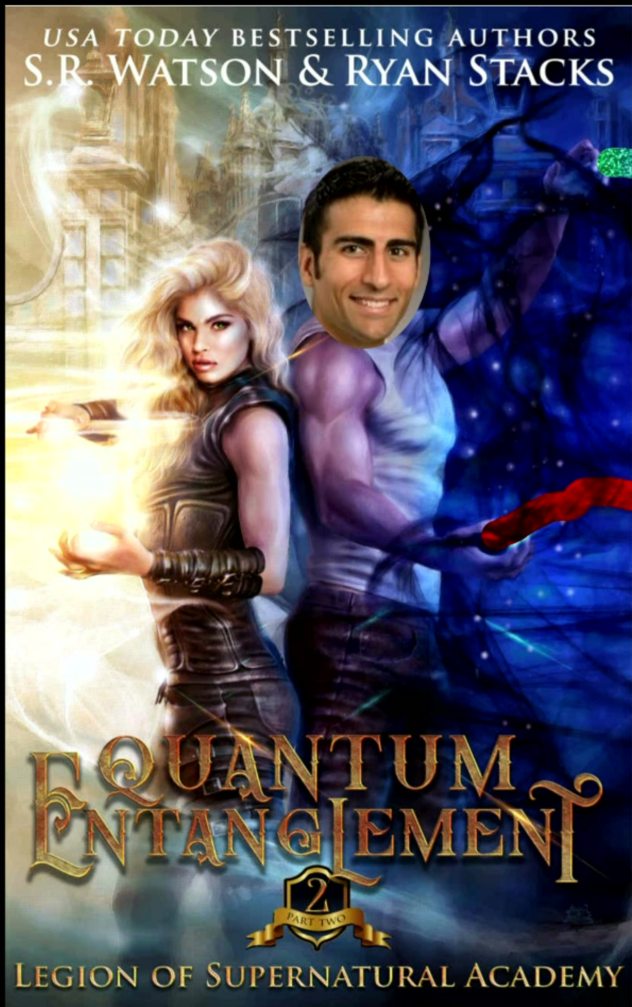
Step 3: mount final fiber supports over electronics board







KQC: Kwiat's Quantum Consortium (Cohort, Clan, Collective, Comrades, ...)


USA TODAY BESTSELLING AUTHORS
S.R. WATSON & RYAN STACKS
QUANTUM ENTANGLEMENT
2
PART TWO
LEGION OF SUPERNATURAL ACADEMY

Questions?


USA TODAY BESTSELLING AUTHORS
S.R. WATSON & RYAN STACKS
QUANTUM ENTANGLEMENT
3
PART THREE
LEGION OF SUPERNATURAL ACADEMY