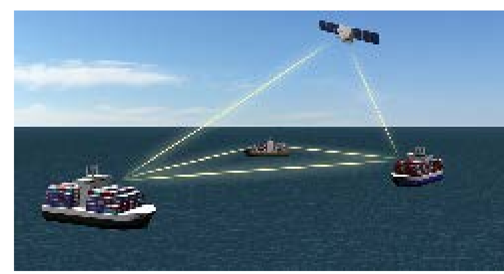
Quantum-secured communications over an optical network

George Siopsis

University of Tennessee



Army Science & Technology Symposium & Showcase, Washington, DC
August 2018

Collaborators

Raphael Pooser
U of Tennessee / ORNL

Bing Qi
U of Tennessee / ORNL

Radhakrishnan Balu
Army Research Laboratory

Hoi-Kwong Lo
U of Toronto

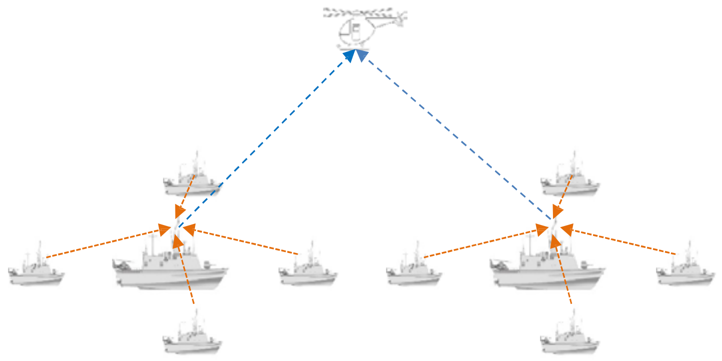
Eric Lukosi
U of Tennessee

Mark Wilde
Louisiana State U

Eric Chitambar
Southern Illinois U

- Several students trained in the course of the program in the collaborating Universities/Institutions in the US and Canada

Quantum secured network

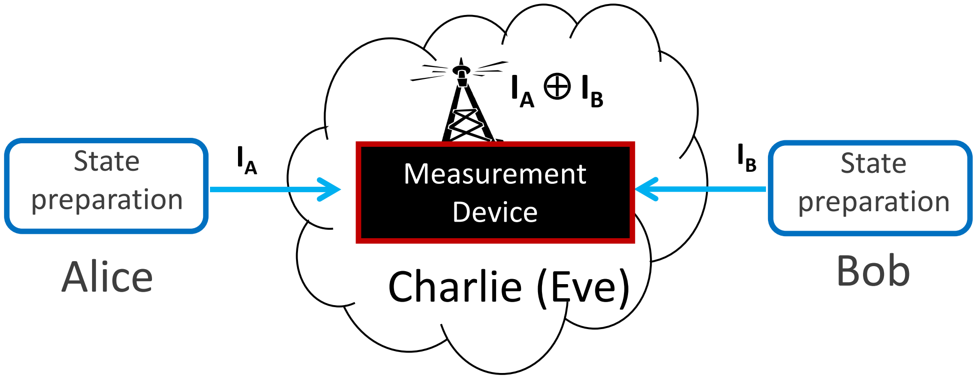


GOAL: To develop a highly reconfigurable network enabling quantum secure communications, both wired and wireless, that can adapt to unpredictable changes in the environment using existing technology.

- Theoretical/Computational/Experimental Program.
- Study quantitatively limits on the resilience of quantum secure communications, quantum key distribution (QKD), quantum position verification (QPV), and scalable quantum networks where nodes can be added and deleted over time.
- Tolerate the high channel loss and unpredictable changes of the free space optical links due to turbulence.
- Quickly respond to environmental changes.
- Built-in quantum authentication.

MDI-QKD network

- **Unprecedented security**
  - Automatically immune to all detector side channel attacks;
  - The network relays can be untrusted.

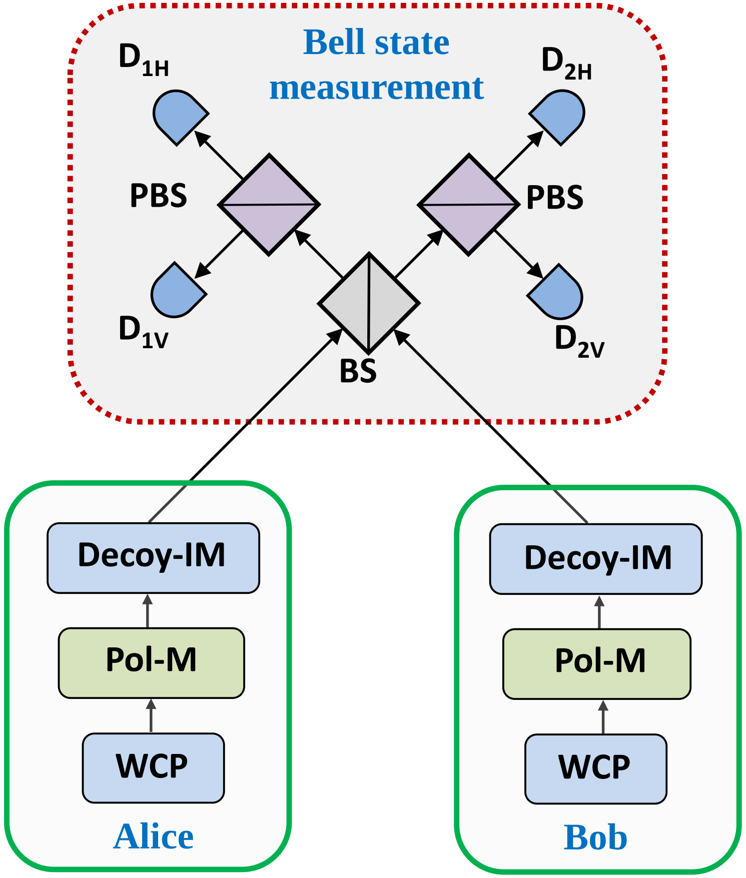


H.-K. Lo, M. Curty, and B. Qi, *Phys. Rev. Lett*. **108**, 130503 (2012).

- **Longest point-to-point QKD**
  - World record: MDI QKD over 404 km optical fiber.

H.-L. Yin, *et al*., "Measurement device independent quantum key distribution over 404 km optical fibre," *Phys. Rev. Lett*. **117**, 190501 (2016).

MDI QKD is practical



Detection Pattern	Bell State
$\{D_{1H}$ & $D_{2V}\}$ or $\{D_{1V}$ & $D_{2H}\}$	$\lvert\psi^-\rangle = \frac{1}{\sqrt{2}}(\lvert HV\rangle - \lvert VH\rangle)$
$\{D_{1H}$ & $D_{1V}\}$ or $\{D_{2H}$ & $D_{2V}\}$	$\lvert\psi^+\rangle = \frac{1}{\sqrt{2}}(\lvert HV\rangle + \lvert VH\rangle)$
Others	Fail

Bases	$\lvert\psi^-\rangle$	$\lvert\psi^+\rangle$
Rectilinear	Bit flip	Bit flip
Diagonal	Bit flip	No bit flip

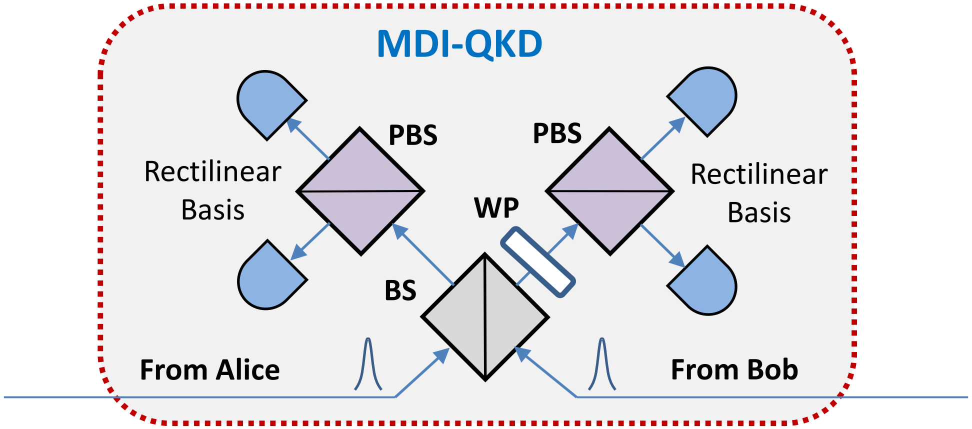
H.-K. Lo, M. Curty, and B. Qi, *Phys. Rev. Lett.* **108**, 130503 (2012).

Reconfigurable QKD network

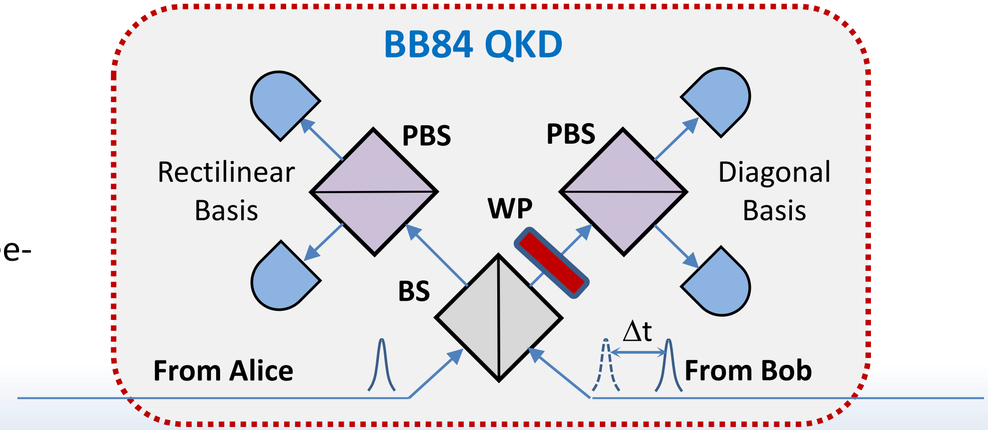
Features

- Can be operated at either highly secure MDI-QKD mode or highly efficient decoy state BB84 QKD mode;
- To switch between two modes, the network center simply rotates one measurement basis.

B. Qi, H.-K. Lo, C. C. W. Lim, G. Siopsis, E. A. Chitambar, R. Pooser, P. G. Evans, and W. Grice, "Free-space reconfigurable quantum key distribution network," 2015 IEEE International Conference on Space Optical Systems and Applications (ICSOS), pp. 1-6. IEEE (2015).

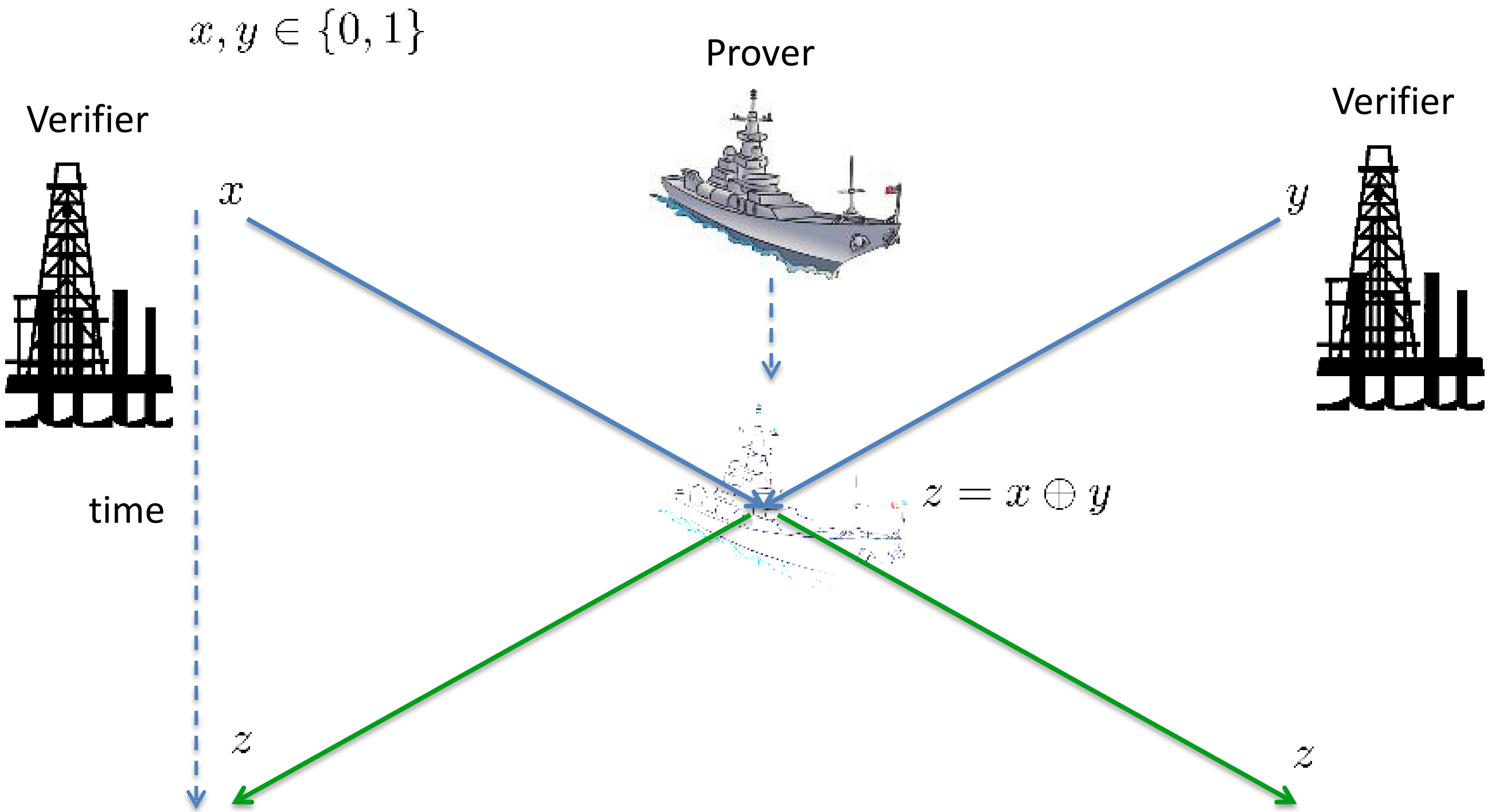


(a) MDI-QKD with untrusted relay



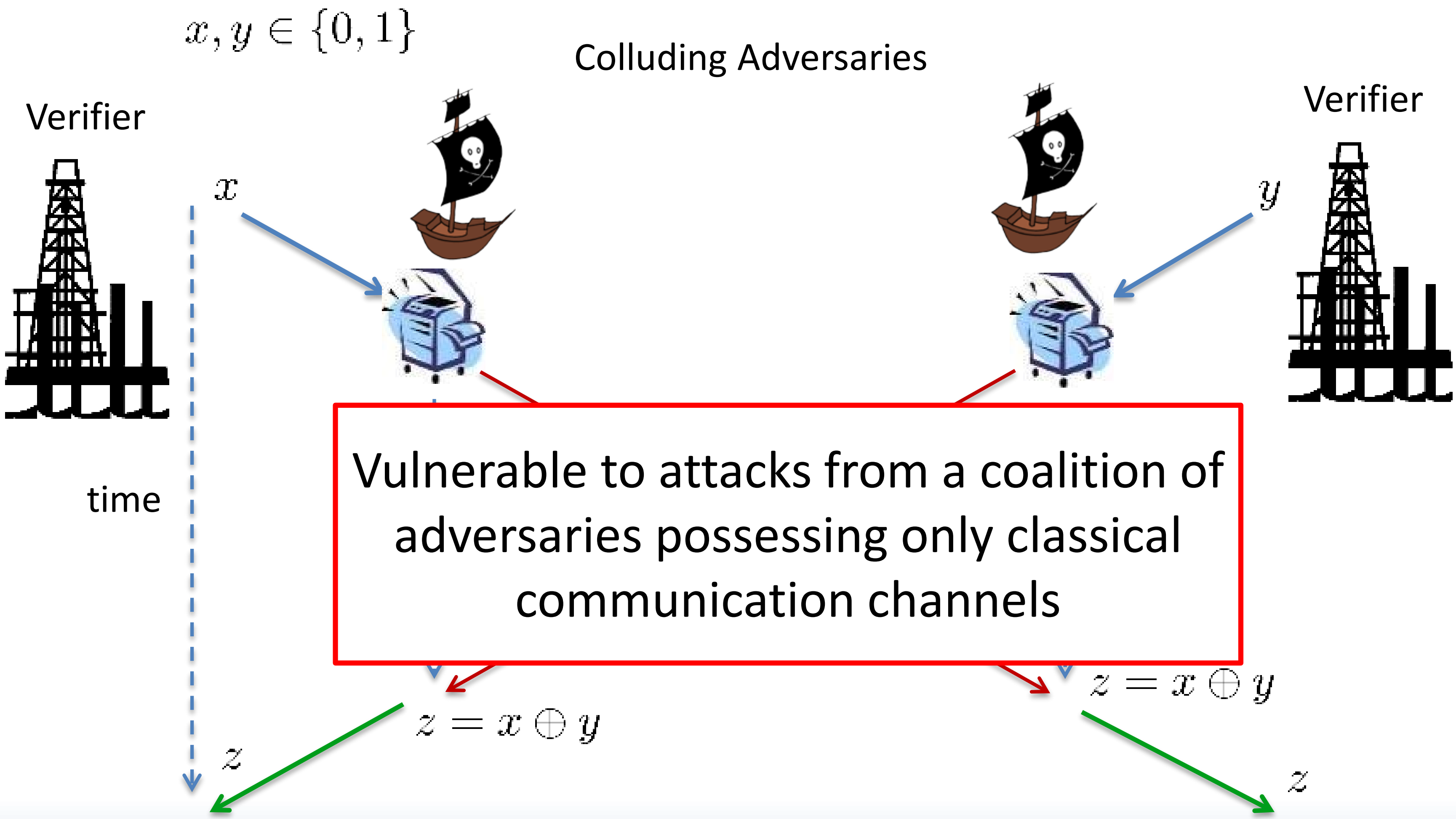
(b) Decoy state BB84 QKD with trusted relay

Position based cryptography (PBC)



Chandran, *et al.*, *Lect. Notes Comput. Sci.* **5677**, 391 (2009).

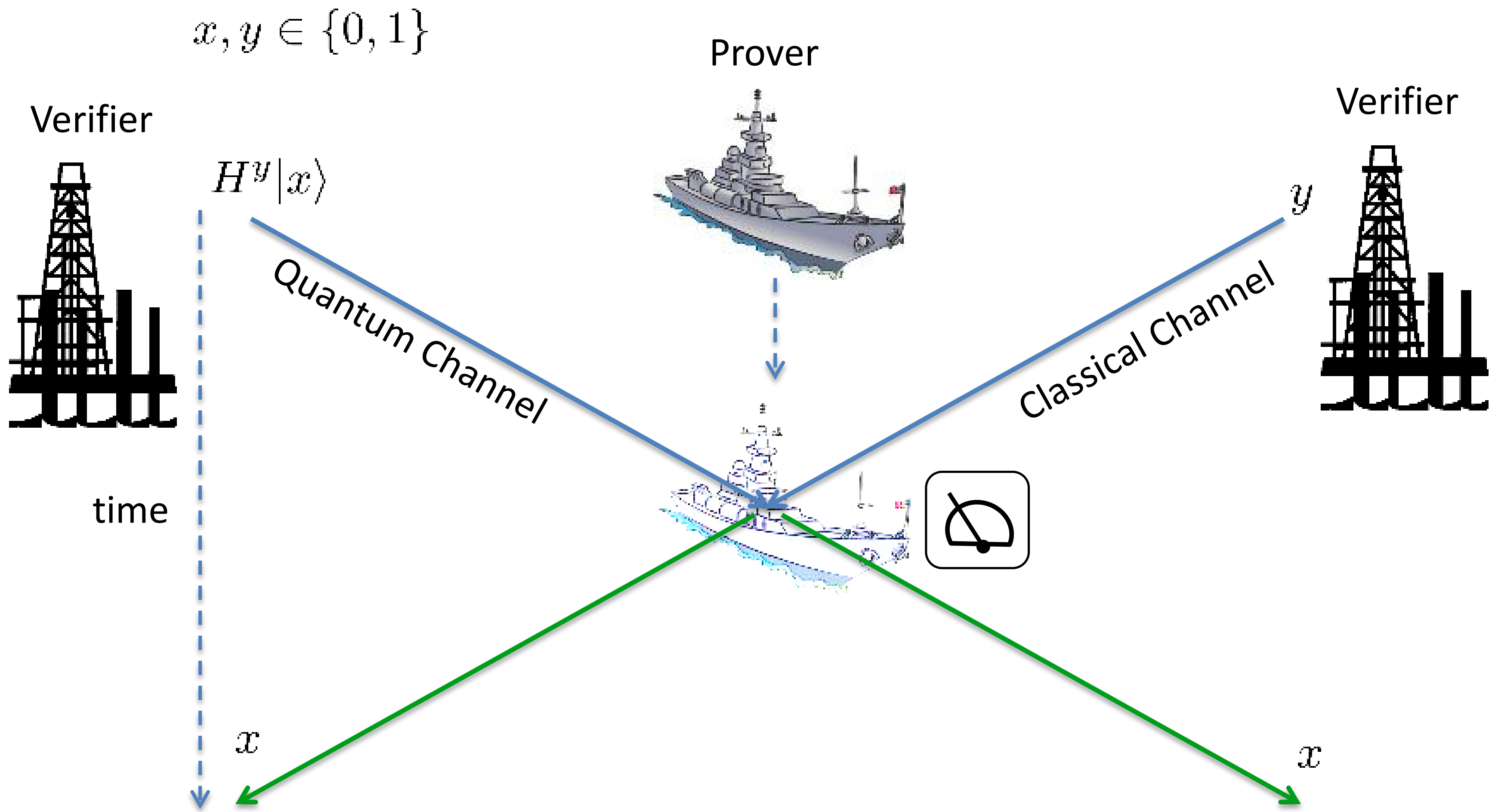
Position based cryptography (PBC)



Vulnerable to attacks from a coalition of adversaries possessing only classical communication channels

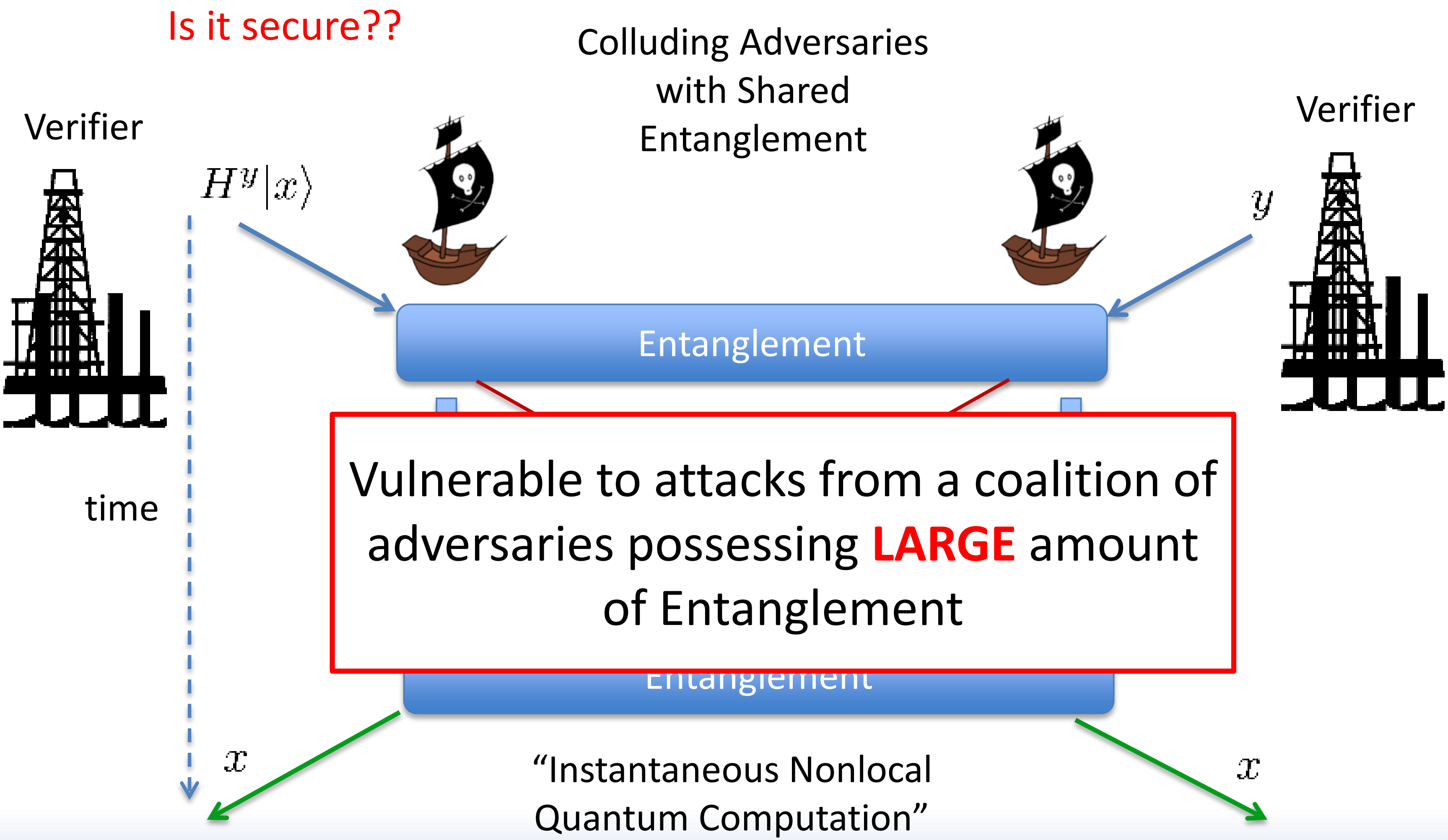
Chandran, *et al.*, *Lect. Notes Comput. Sci.* **5677**, 391 (2009).

Position based quantum cryptography (PBQC)



Chandran, *et al.*, *Lect. Notes Comput. Sci.* **391**, 5677 (2009).
Kent, *et al.*, *PRA* **84**, 012326 (2011).

Position based quantum cryptography (PBQC)



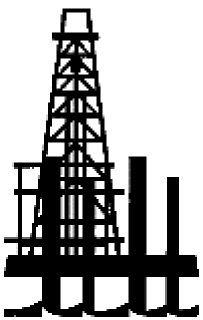
Buhrman, *et al.*, *SIAM J. Comput.* **43**, 150 (2014).

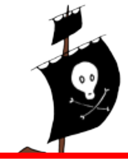
Position based quantum cryptography (PBQC)

What if the adversaries don't share entanglement??

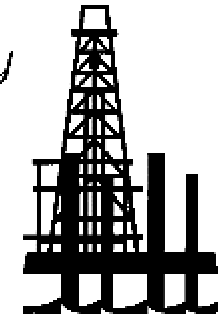
Noiseless Quantum Channel:

Verifier





Verifier



- This scenario is provably secure.
- In noiseless PBQC,

  Unentangled Adversaries => Secure

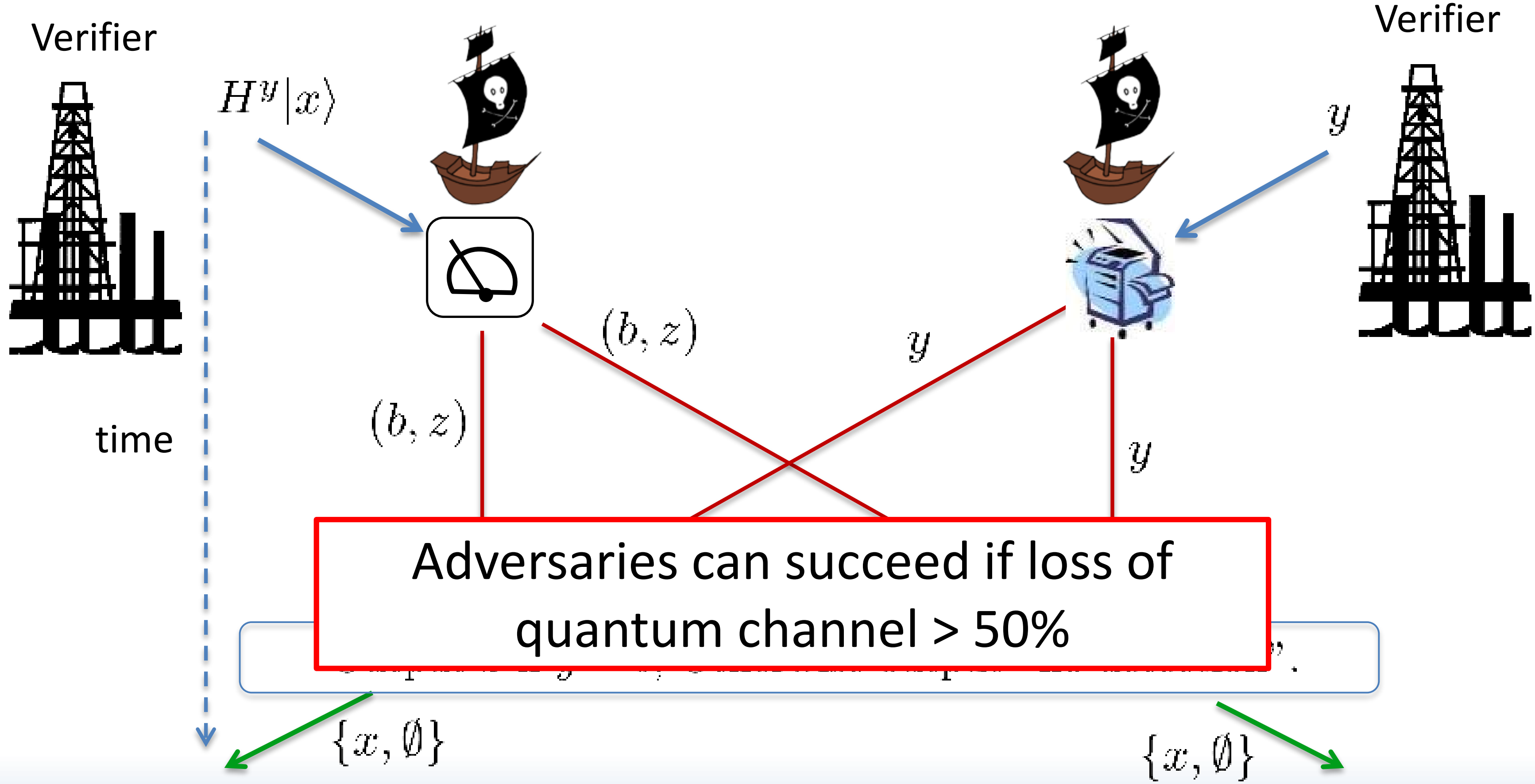
  Entangled Adversaries => Insecure
- Fundamental Question:

  How much entanglement is needed to break PBQC?

Position based quantum cryptography (PBQC)

What if the adversaries don't share entanglement??

Noisy Quantum Channel:



Adversaries can succeed if loss of quantum channel > 50%

Qi and Siopsis, *PRA* **91**, 042337 (2015).

Measurement-Device-Independent (MDI) PBQC

PHYSICAL REVIEW A **94**, 032315 (2016)

Loss-tolerant quantum secure positioning with weak laser sources

Charles Ci Wen Lim,[1,*] Feihu Xu,[2] George Siopsis,[3] Eric Chitambar,[4] Philip G. Evans,[1] and Bing Qi[1,3]

- PBQC based on the concept of measurement-device-independent QKD
- Provides a new fundamental lower bound on the entanglement needed to break PBQC:

  For ideal sources and arbitrary channel loss,

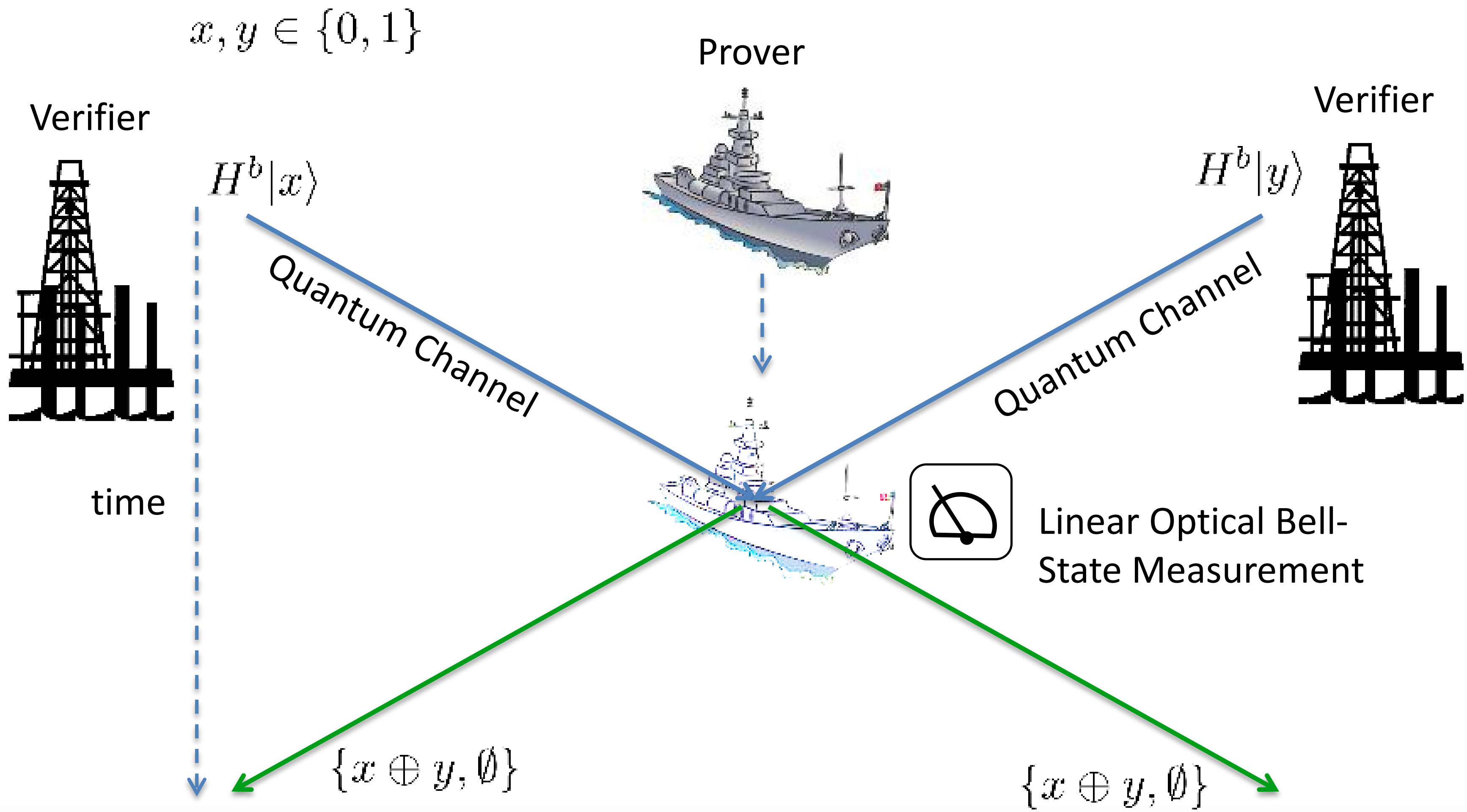
  protocol is secure against *PPT adversaries*.

  Adversaries can share arbitrary PPT entanglement.

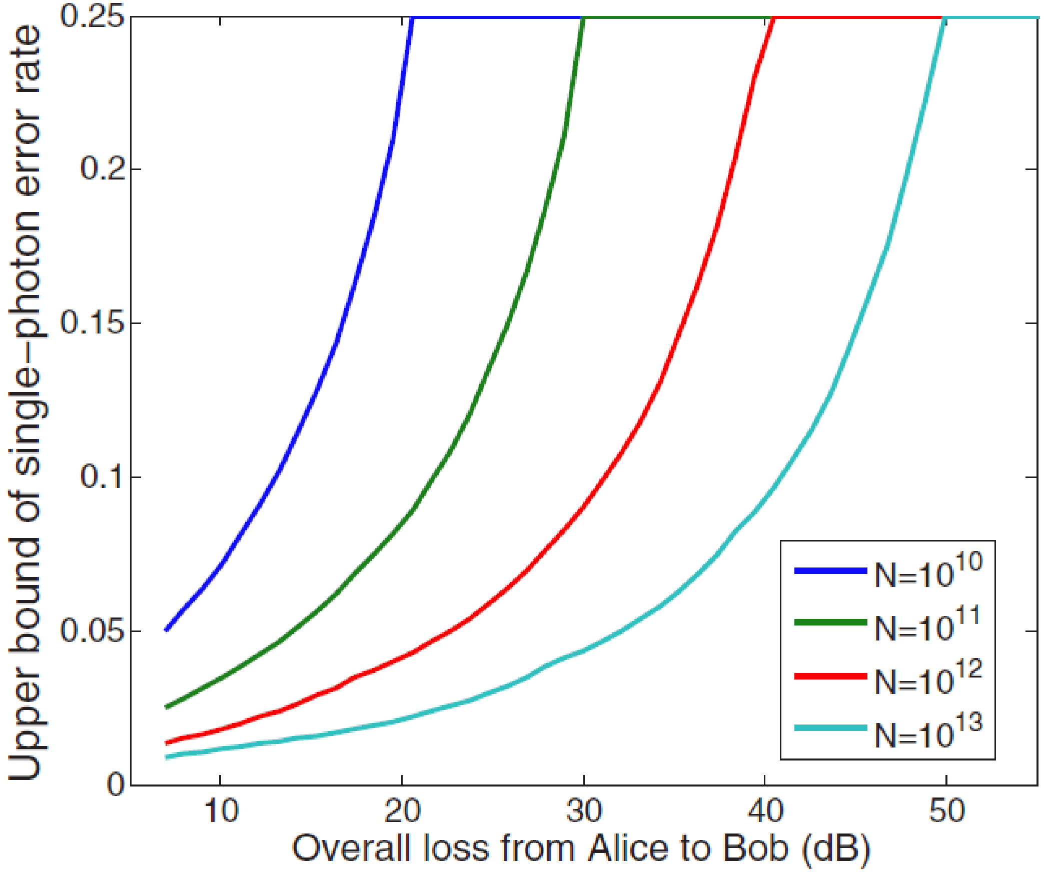
- For realistic sources, the protocol incorporates weak laser sources and the decoy-state method to become loss-tolerant.

Lo, Curty, and Qi, *Phys. Rev. Lett.* **108**, 130503 (2012).

Measurement-Device-Independent (MDI) PBQC



Measurement-Device-Independent (MDI) PBQC

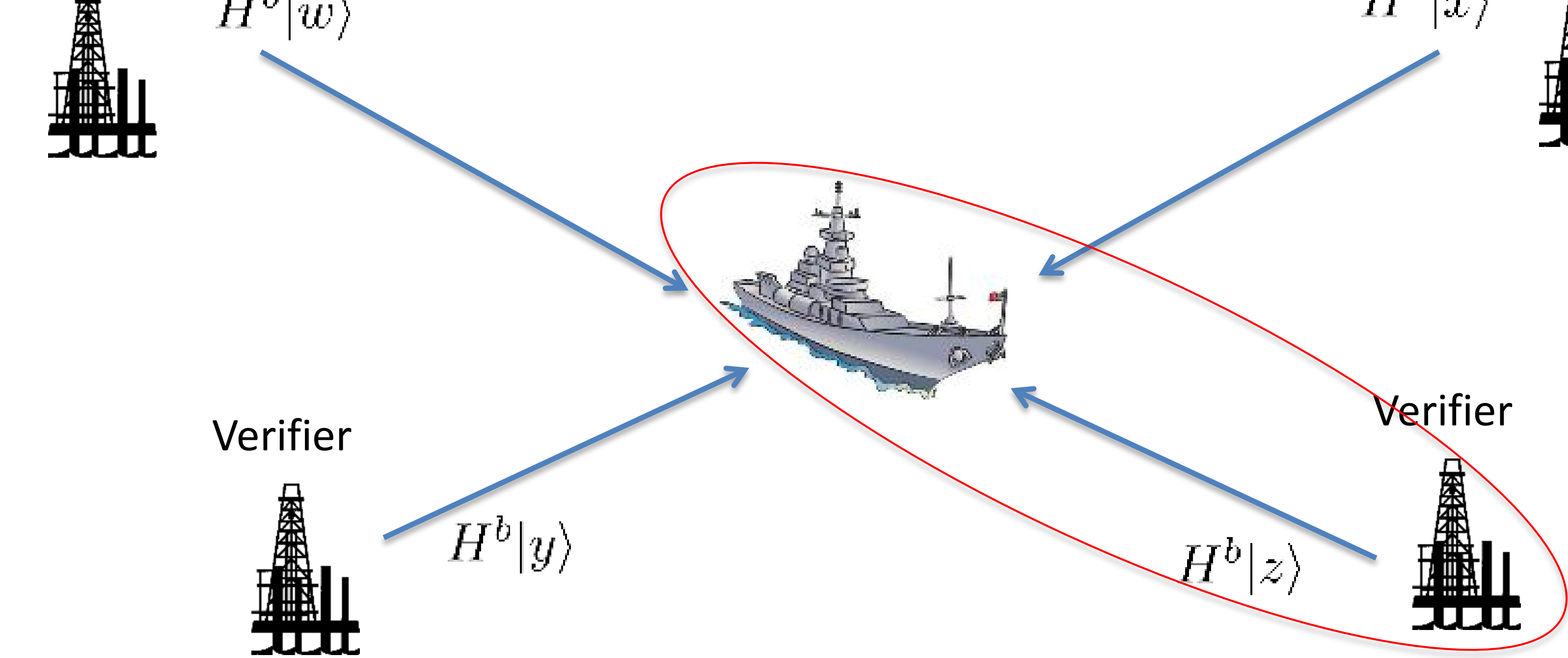


Protocol becomes insecure when error rate > .25

- Simulation with baseline QBER of .1%, detector efficiency of 64%, and a dark count rate of 2.5 x 10^{-6}.
- MDI PBQC can tolerate a 47 dB channel loss.

PBQC: Current and Future Work

- MDI PBQC with multiple verifiers
  How does the entanglement cost needed to break PBQC scale with the number of verifiers?

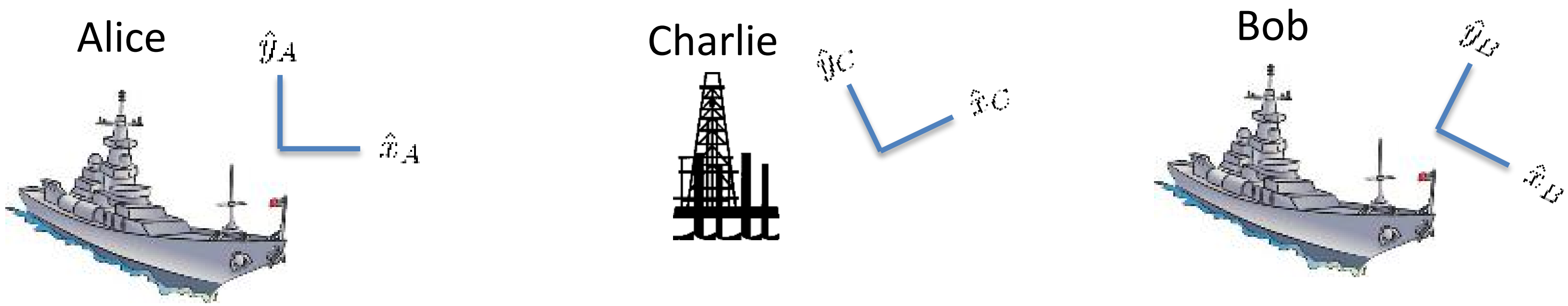


- What if the prover already shares a private channel with one of the verifiers?

A. Kent, *Phys. Rev. A* **84**, 022335 (2011).

PBQC: Current and Future Work

- Reference-Frame Independent QKD and PBQC



- What if Alice, Bob, Charlie, … etc. do not possess a share reference frame, such as alignment of polarization states?
- How does this affect their ability for QKD and/or PBQC?
- Can interactive classical communication help overcome some of the misalignment?
- Can connections be made to the "resource theory of shared reference frames"?

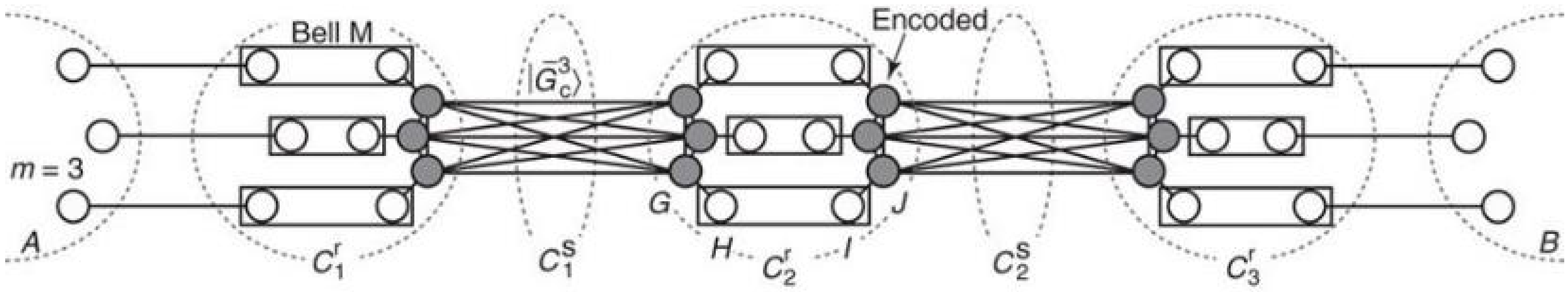
A. Laing, V. Scarani, J. G. Rarity, and J. L. O'Brien, *Phys. Rev. A* **82**, 012304 (2010).
C. Wang, X.-T. Song, Z.-Q. Yin, S. Wang, W. Chen, C.-M. Zhang, G.-C. Guo, and Z.-F. Han, *Phys. Rev. Lett.* ***115***, 160502 (2015).
S. D. Bartlett, T. Rudolph, and R. W. Spekkens, *Phys. Rev. Lett.* **91**, 027901 (2003).
G. Gour and R. W. Spekkens, *New J. Phys.* **10**, 033023 (2008).

Scalable MDI QKD Network

- Joint theoretical/experimental effort.

GOAL: Build highly scalable quantum network, incl. quantum repeaters based on protocol by Lo, *et al*., that would enable high-rate MDI QKD in a general quantum network with channels of asymmetric losses where nodes can be dynamically added or deleted over time.

- Untrusted relays.
- All-photonic quantum repeaters that do not require matter quantum memory and can be implemented with existing technology.



W. Wang, F. Xu, and H.-K. Lo, arXiv:1807.03466 (2018).
K. Azuma, K. Tamaki, and H.-K. Lo, *Nature Communications* **6**, 6787 (2015).

Modeling of Optical Quantum Networks

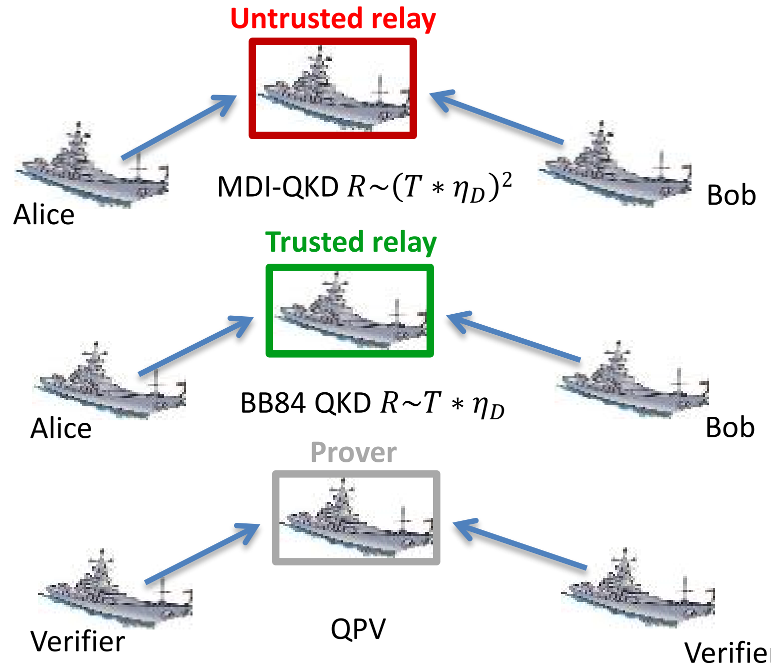
➢ In collaboration with R. Balu (ARL)

GOAL: Build computational models based on the QNET framework. It is a versatile tool for the simulation of quantum optics networks and describes open quantum systems at the microscopic level in terms of quantum stochastic differential equations (QSDEs).

- Implemented on DoD HPC infrastructure.
- Symbolic manipulation to derive the SLH parameters of the system and numerically solves the resulting QSDEs using the QuTip tool.
- Scalable approach to the derivation of master equations for systems of interconnected optical and mechanical components.
- We use this tool to model protocols and circuits and determine the optimal parameters of operation.

J. Gough and M. R. James, *Comm. Math. Phys*. **287**, 1109 (2009).
N. Tezak, A. Niederberger, D. S. Pavlichin, G. Sarma, and H. Mabuchi, *Philosophical Transactions A* **370**, 5270 (2012).
C. W. Gardiner and M. J. Collett, *Phys. Rev. A* **31**, 3761 (1985).
J. R. Johansson, P. D. Nation, and F. Nori, *Comp. Phys. Comm*. **184**, 1234 (2013).

Free-space MDI-QKD system design



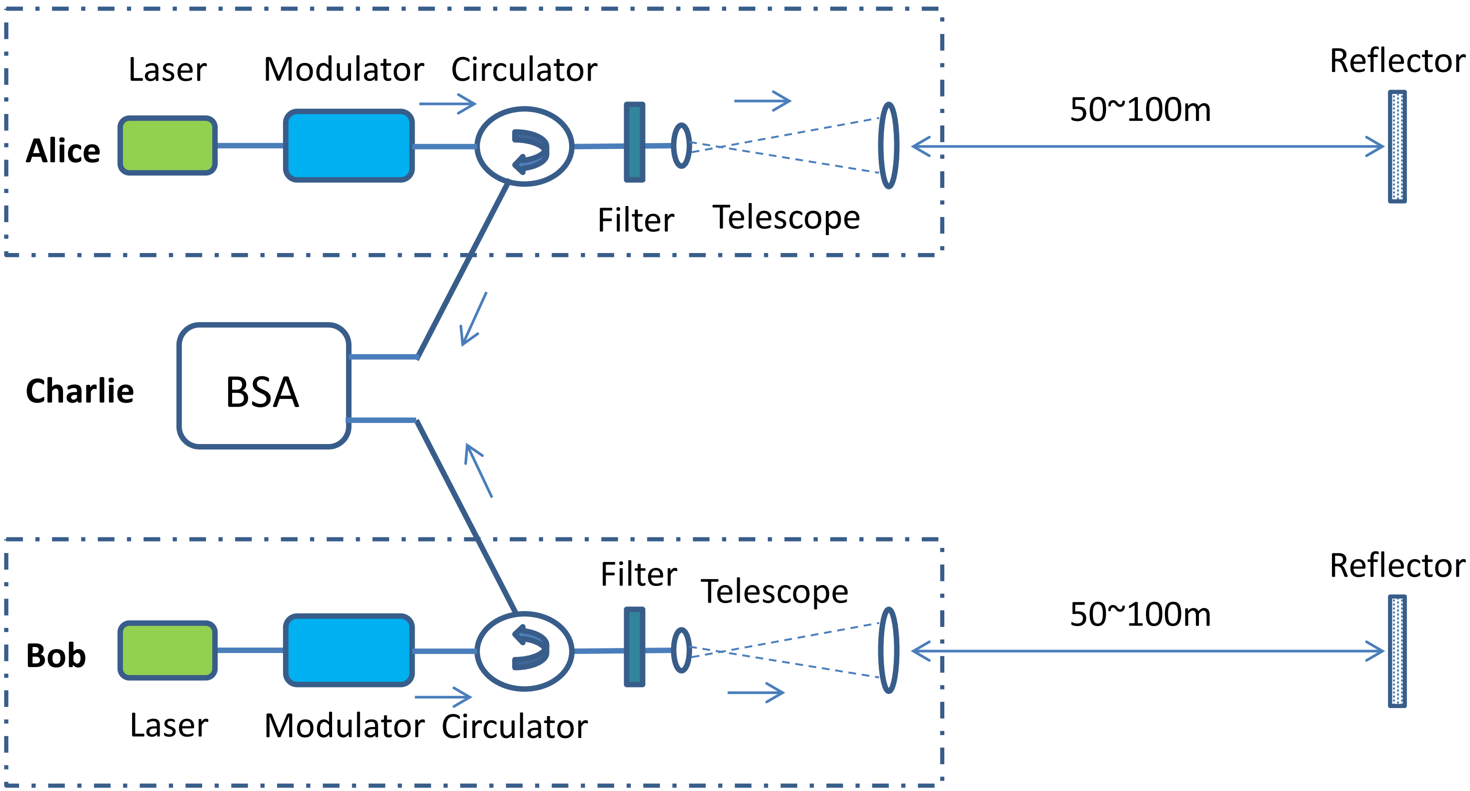
One system→ three protocols

- ❑ MDI-QKD protocol
  - Highly secure over untrusted relay
  - Could be the first free-space MDI-QKD demonstration
- ❑ Decoy state BB84 QKD over trusted relay protocol
  - Highly efficient over trusted relay
- ❑ Quantum position verification protocol
  - Authentication scheme to initialize QKD process

Polarization coding *vs* time-bin coding

- ❑ BB84 QKD
  - Optical fiber: time-bin coding (birefringence of optical fiber)
  - Free space: polarization coding (no need of interferometer phase stabilization)
- ❑ Free space MDI QKD
  - Polarization coding—polarization alignment among 3 parties; Time-bin coding—polarization alignment between 2 parties
  - Time-bin coding—interferometer phase stabilization and/or laser frequency stability
- ❑ We chose polarization coding scheme for reconfigurable QKD scheme

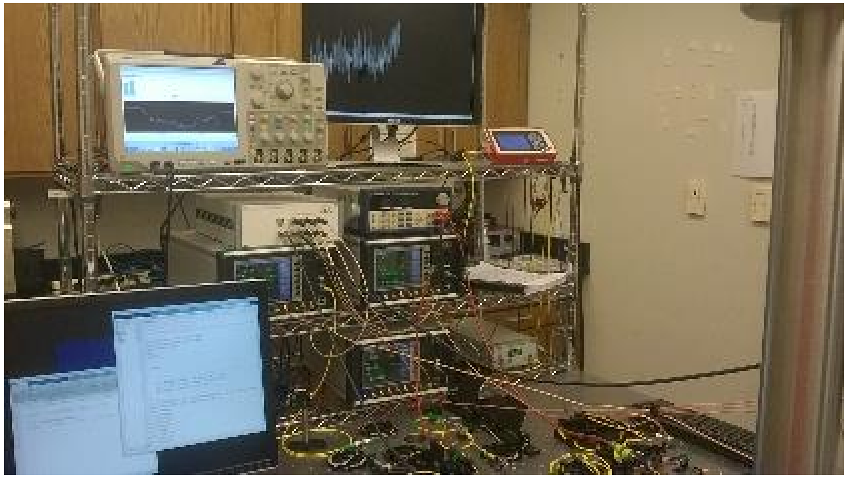
Experimental design



Features

- Two independent free-space quantum channels—addresses the main challenge in free-space MDI-QKD.
- Two QKD users and the measurement device at the same physical location—significantly reduce the required resources.

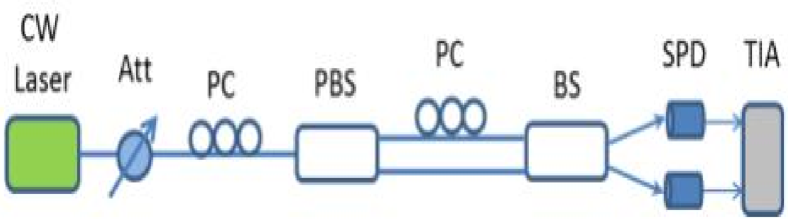
Our lab at the University of Tennessee

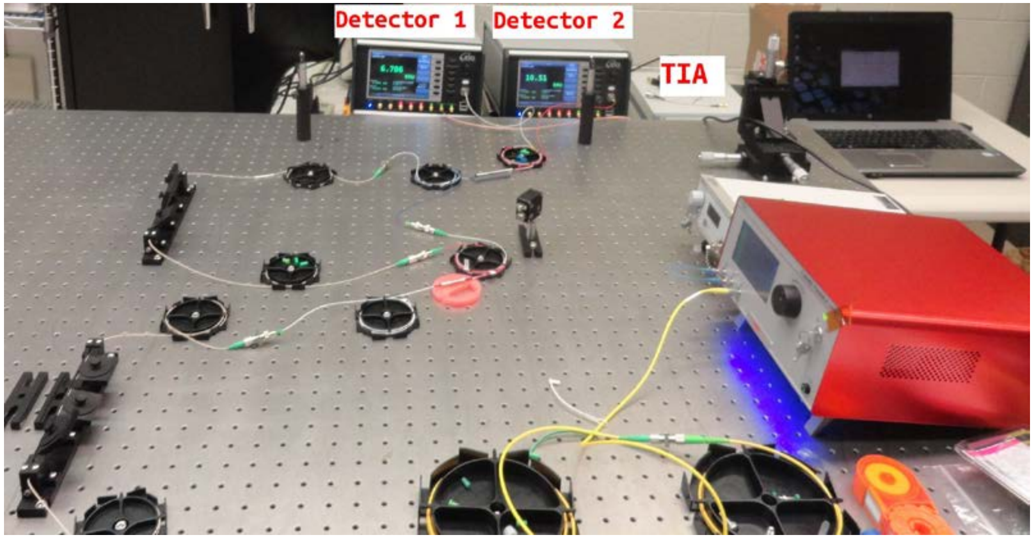


- Funded by ONR.

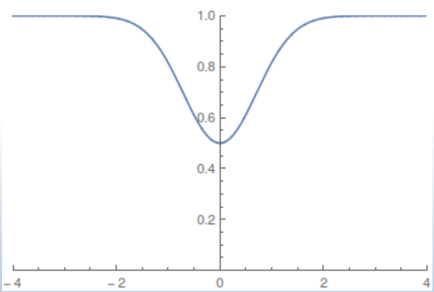
HOM Interference

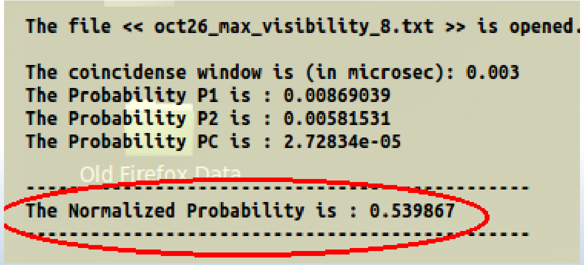
Experimental Setup





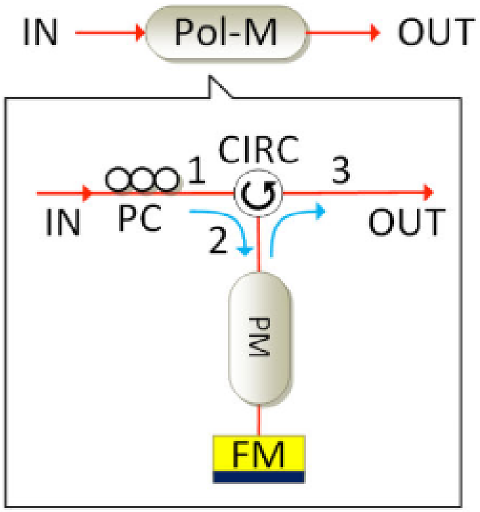
- TIA records detection events in a .txt file
- Our code compares the time tags and records coincidence events
- Calculate P1, P2, and Pc: Probabilities of detection at SPD1, SPD2 and coincidence probability.
- Calculate P = Pc/(P1*P2), HOM predicts P=0.5 (HOM dip)



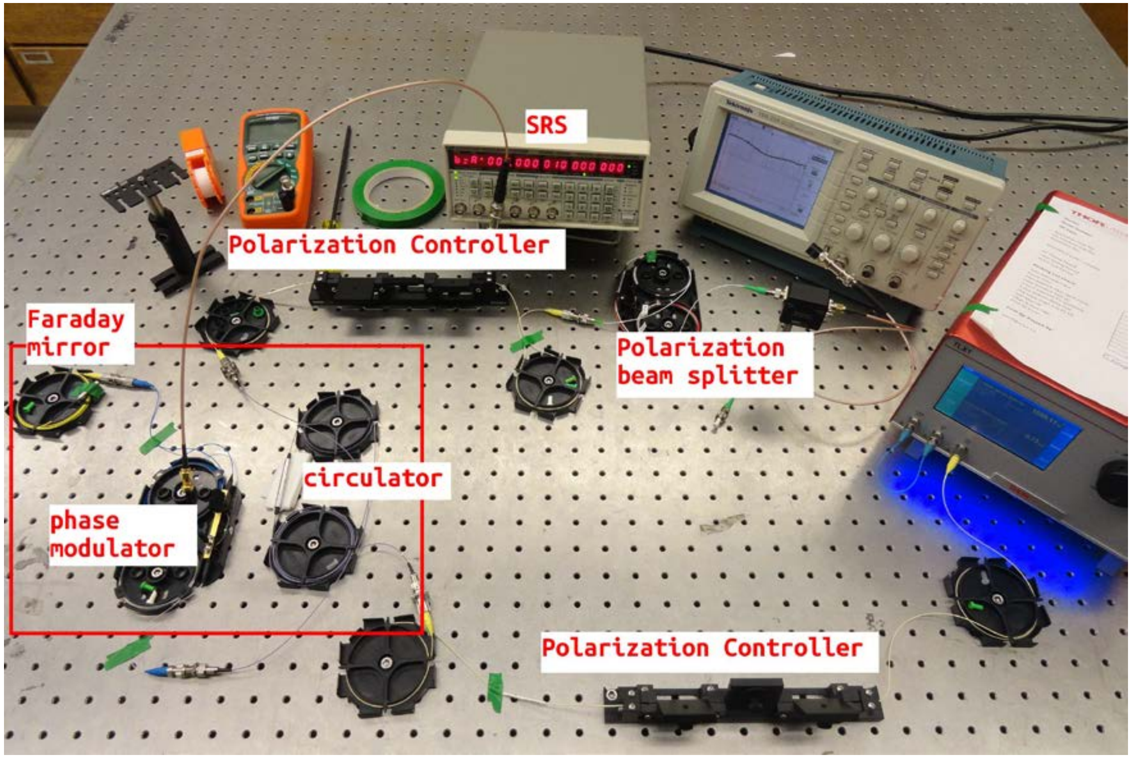


We have observed dips down to 0.54

Polarization Modulation Implementation

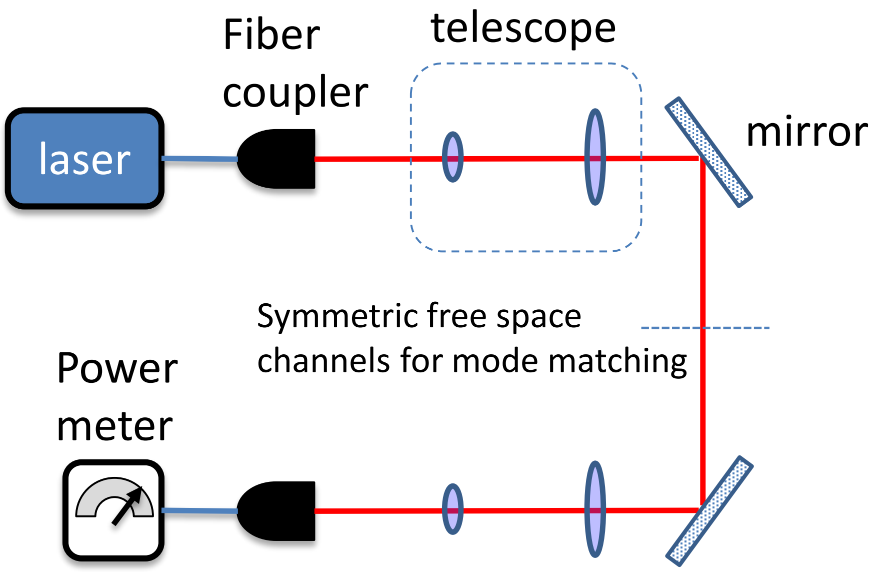


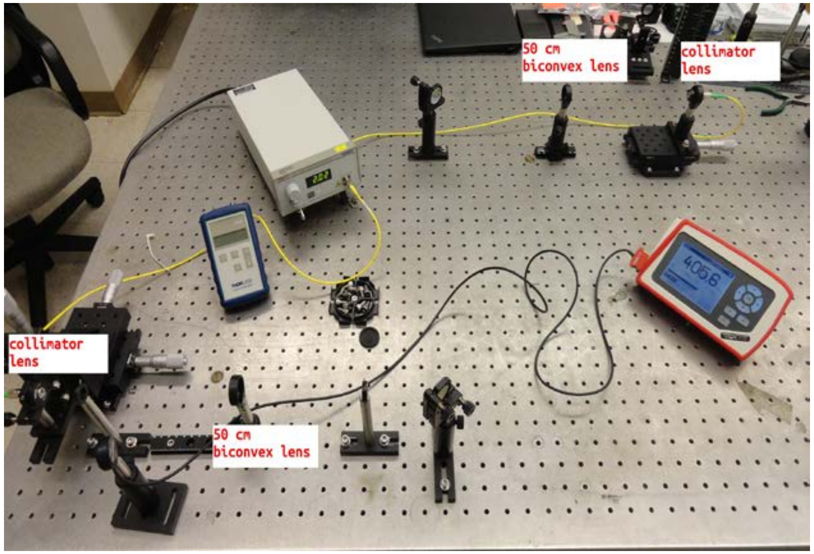
Z. Tang, Z. Liao, F. Xu, B. Qi, L. Qian, and H.K. Lo, Phys. Rev. Lett. **112**, 190503 (2014).



- The SRS provides the driving voltage for the phase modulator. The provided voltage determines the phase introduced between the TE and TM components of the input light.
- The phase modulator introduces polarization mode dispersion. It is compensated by reflecting on a Faraday mirror and passing through the PM a second time.
- The polarization beam splitter sets the measurement basis. The two polarization controllers allow the alignment of the $|\,TE\,\rangle + \exp(i\phi)\,|\,TM\,\rangle$ with the measurement basis.

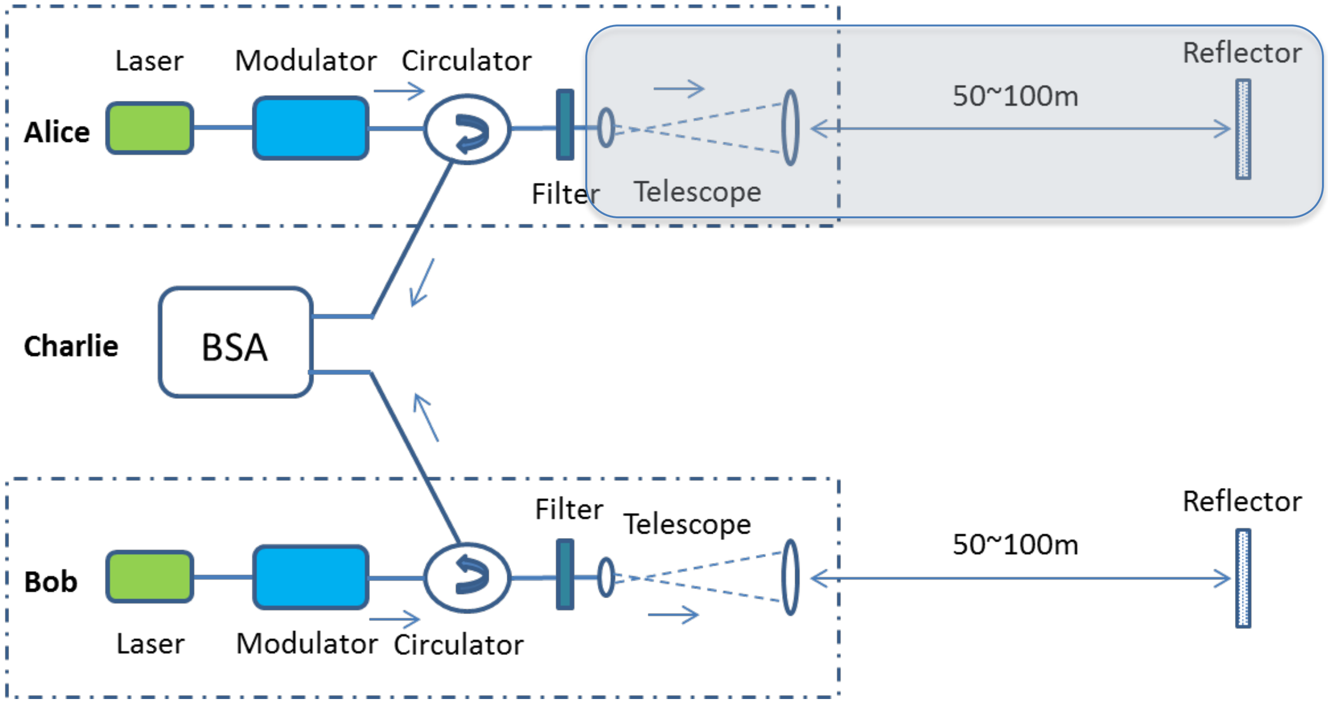
Free-space optics





1) Free space optics (lenses, mirrors) and fiber collimators procured.
2) Fiber-to-fiber coupling experiment built in order to ascertain coupling efficiency and losses.
3) 75% table top coupling efficiency achieved at short distances.
4) Next step is to increase distance to 50 m (25 m from each fiber coupler to beam waist).

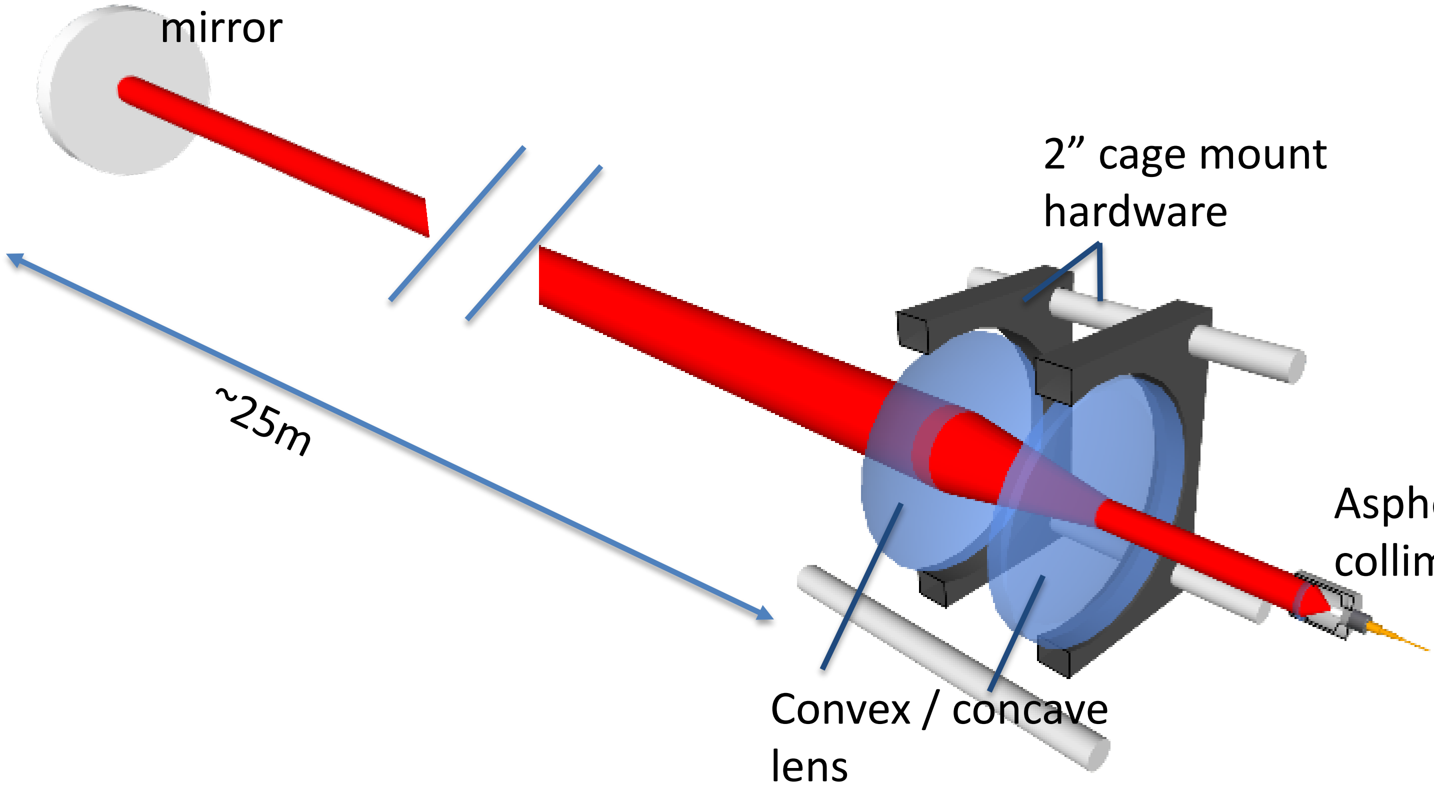
Free space optical design



Transmissive telescope design

- Short distance for proof of principle allows minimal Fresnel losses and diffraction

Free space optical design



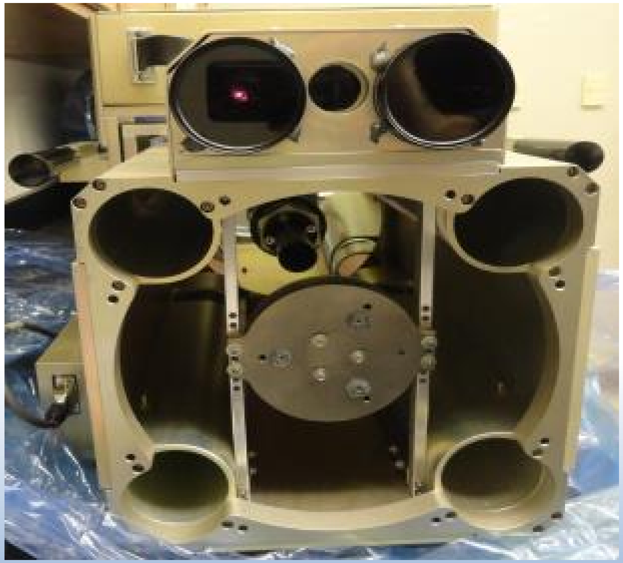
Transmissive telescope design

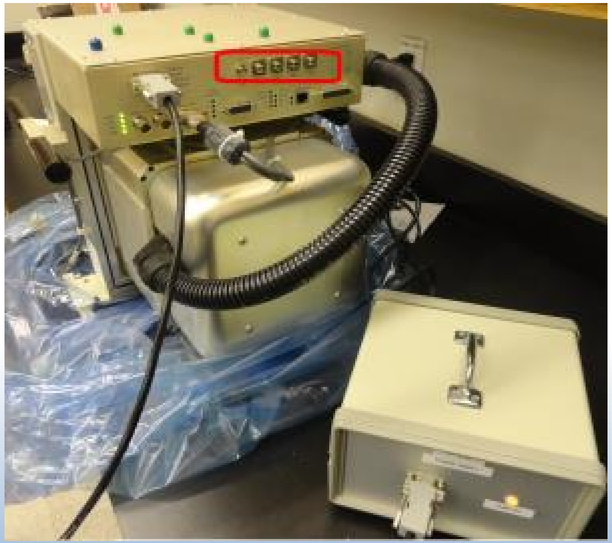
- No active stabilization in first gen short range design

Free-space optics

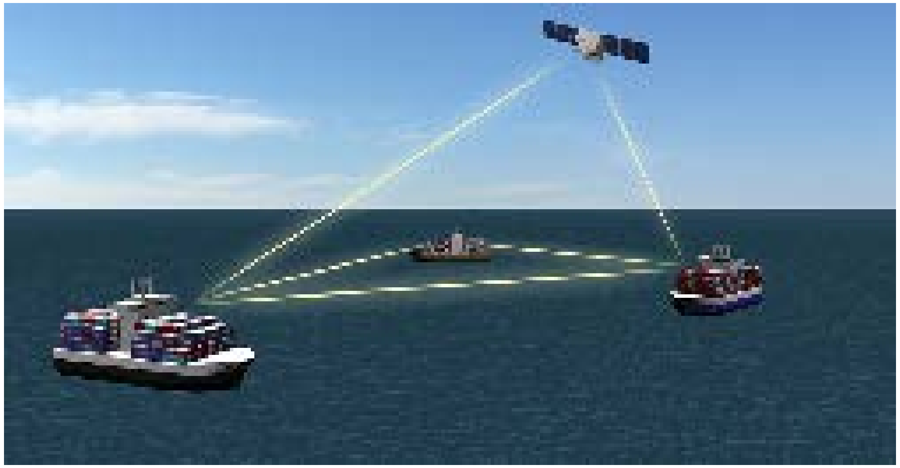
Joshua Bienfang
NIST

In collaboration with NIST, we are testing commercial telescopic systems for potential long distance experiment.





Conclusion



US/CANADA Multi-institution

Theoretical/Computational/Experimental Program

- To develop a highly reconfigurable network enabling quantum secure communications, both wired and wireless, that can adapt to unpredictable changes in the environment using existing technology.

Thank You !