PROOF-OF-PRINCIPLE QUANTUM KEY DISTRIBUTION IMMUNE TO DETECTOR ATTACKS

Allison Rubenok, Joshua A. Slater, Philip Chan,
Itzel Lucio-Martinez & Wolfgang Tittel

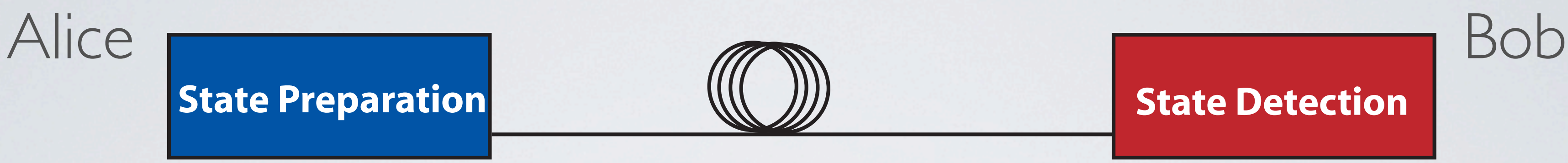
Institute for Quantum Information Science
University of Calgary, Canada

Institute for Quantum Information Science at the University of Calgary

UNIVERSITY OF CALGARY

QCrypt 2012 - Sept 10 2012

Quantum Key Distribution



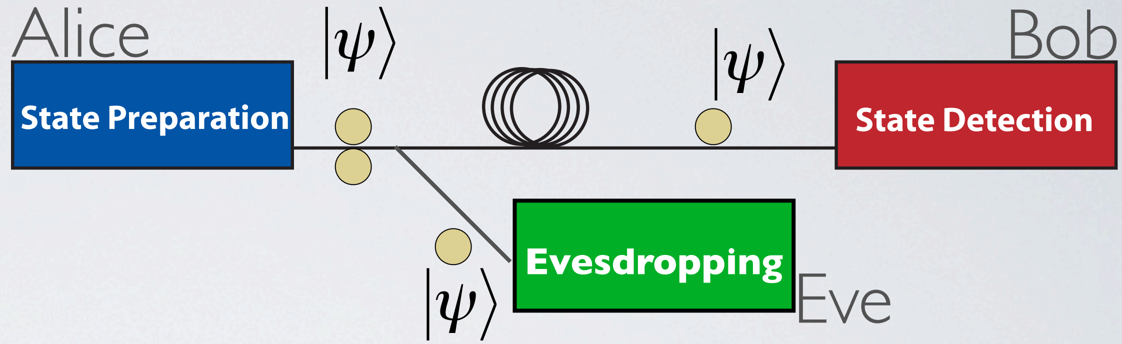
- Experimental (level 2):
  - 100s of km of optical fibre
  - 100 km through free space
  - Trusted node networks: Tokyo, Swiss, SECOQC, DARPA
  - Commercial Products: idQuantique, MagiQ

Side-Channel Attacks

Photon Number Splitting

Counter:

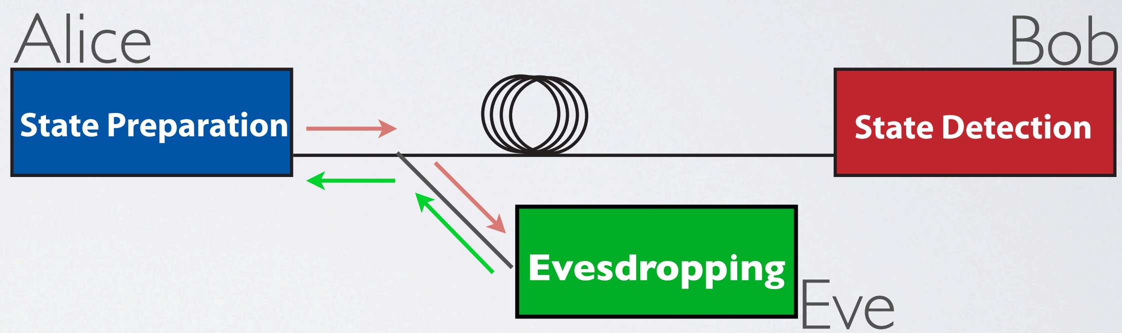
Decoy Analysis



Trojan Horse

Counter:

Optical Isolators



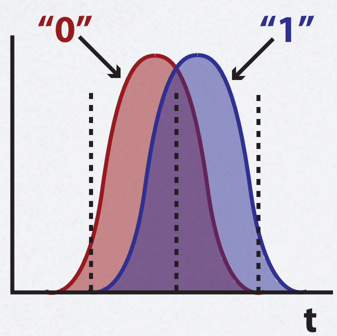
Detector Weaknesses

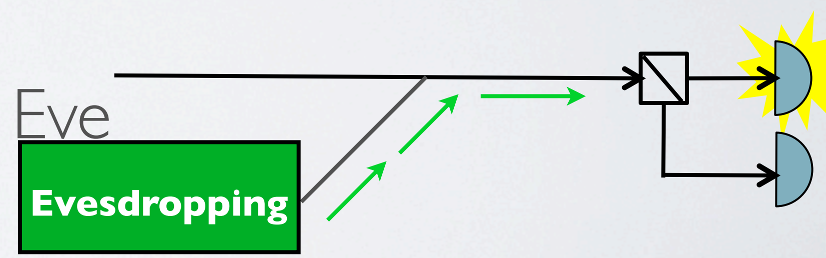
i.e. time-shift attack

or blinding & faked states

Counter:

Robust Detectors





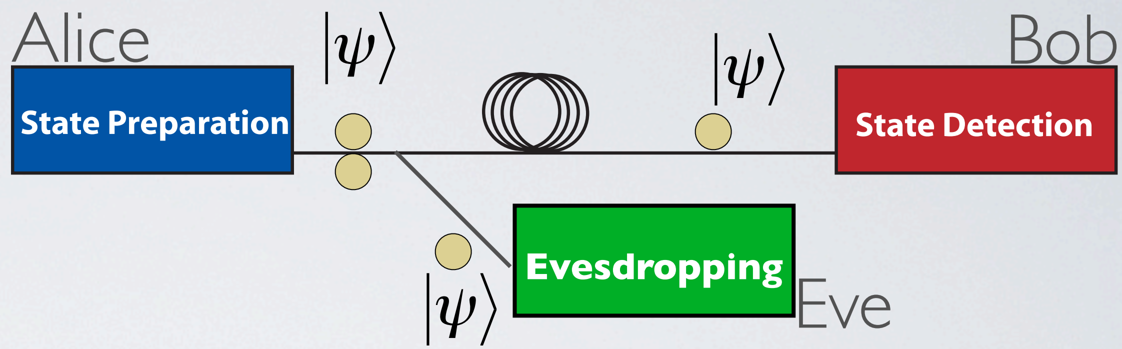
Brassard *et al*, PRL 85, 11330 (2002), Gisin *et al*, PRA, 022320 (2006), Zhao, PRA 78, 042333 (2008), Lydersen *et al*, Nat. Phot 4, 686689 (2010)

SIDE-CHANNEL ATTACKS

Photon Number Splitting

Counter:

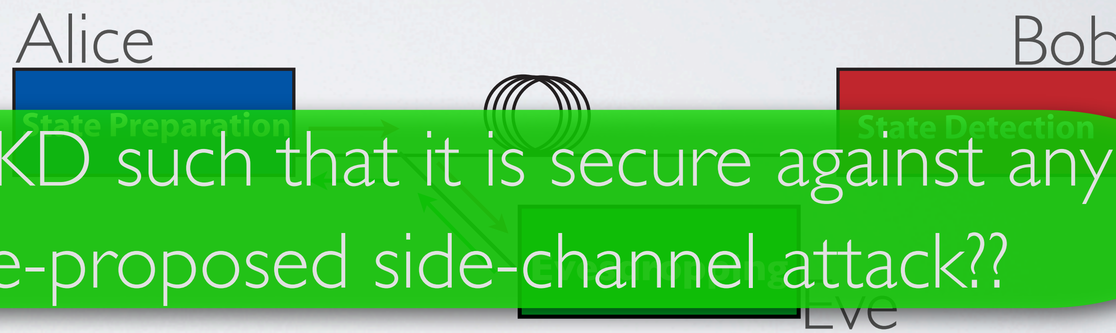
Decoy Analysis



Trojan Horse

Counter:

Optical Isolators



Can we implement QKD such that it is secure against any known or yet-to-be-proposed side-channel attack??

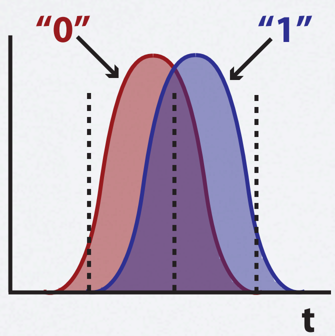
Detector Weaknesses

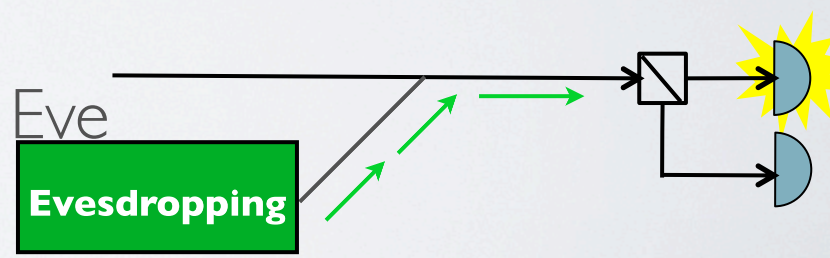
i.e. time-shift attack

or blinding & faked states

Counter:

Robust Detectors



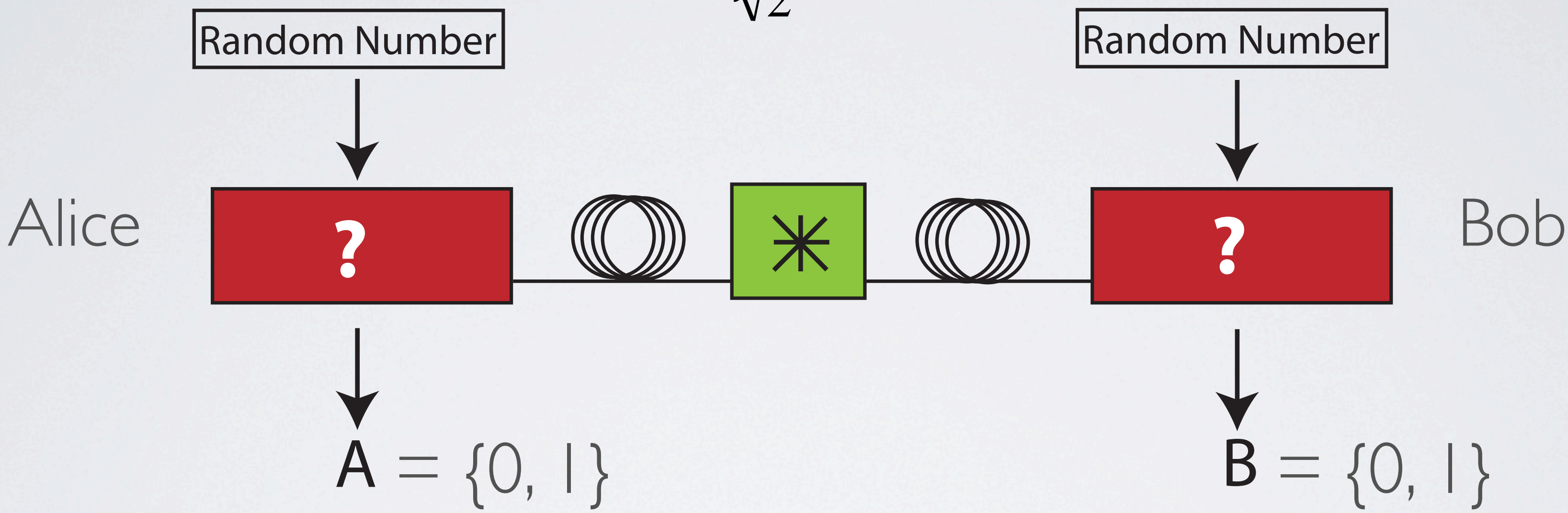


Brassard *et al*, PRL 85, 11330 (2002), Gisin *et al*, PRA, 022320 (2006), Zhao, PRA 78, 042333 (2008), Lydersen *et al*, Nat. Phot 4, 686689 (2010)

Device-Independent QKD

Protection against side-channel attacks:

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right)$$



Requires:

- qubit projection measurements, entanglement source
- loophole-free Bell Test

To produce secret key:

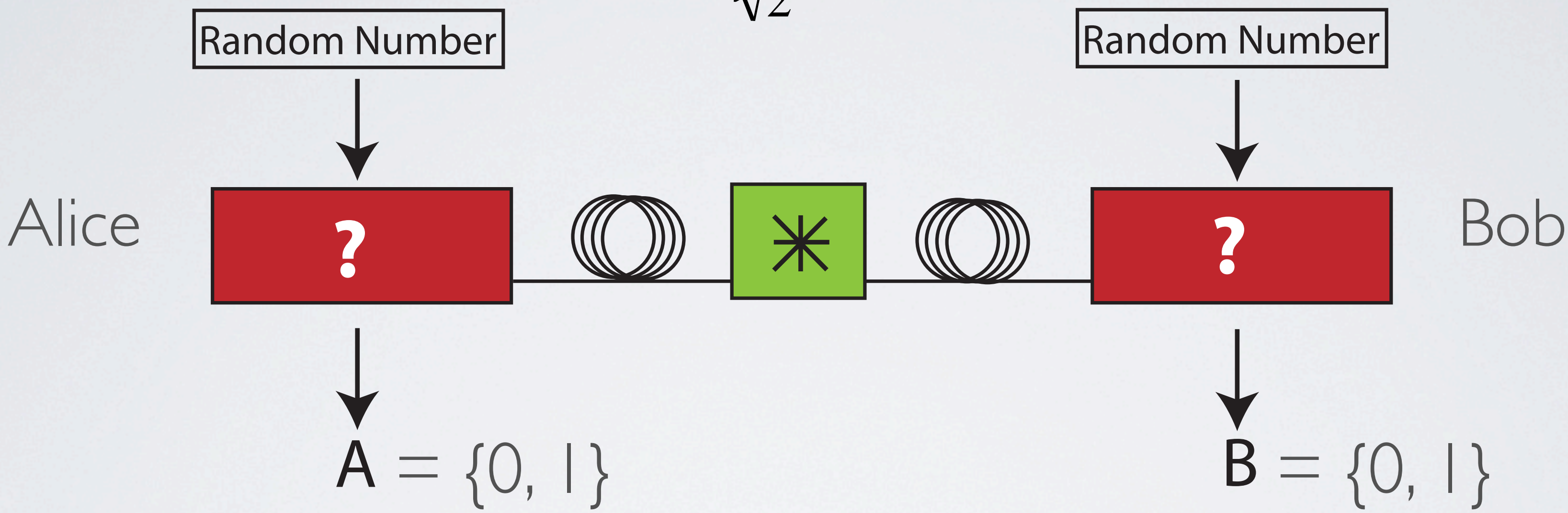
- sifting, error correction & privacy amplification

Acin, Brunner, Gisin, Masenes, Pironio, Scarani PRL 98, 230501 (2007), Masanes, Pironio, Acin, Nat. Comm. 2, 238 (2011).

Device-Independent QKD

Protection against side-channel attacks:

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right)$$



Requires:

- qubit projection measurements, entanglement source
- loophole-free Bell Test

Currently Infeasible: Detection Loophole

To produce secret key:

- sifting, error correction & privacy amplification

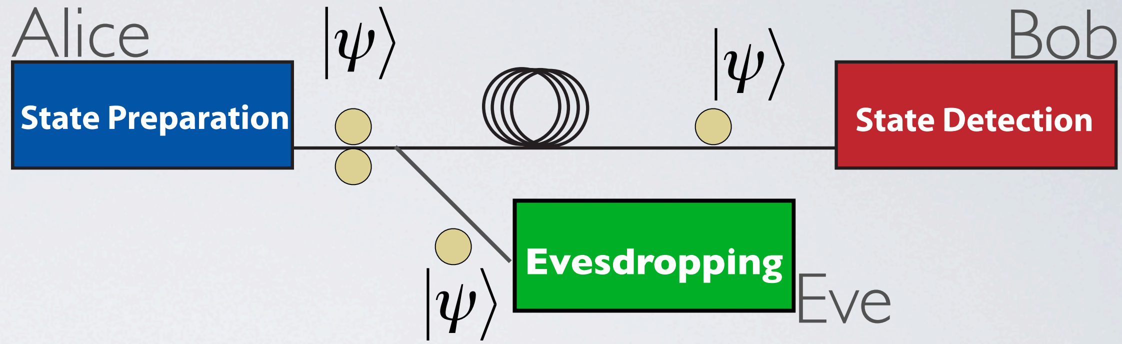
Acin, Brunner, Gisin, Masenes, Pironio, Scarani PRL 98, 230501 (2007), Masanes, Pironio, Acin, Nat. Comm. 2, 238 (2011).

Side-Channel Attacks

Photon Number Splitting

Counter:

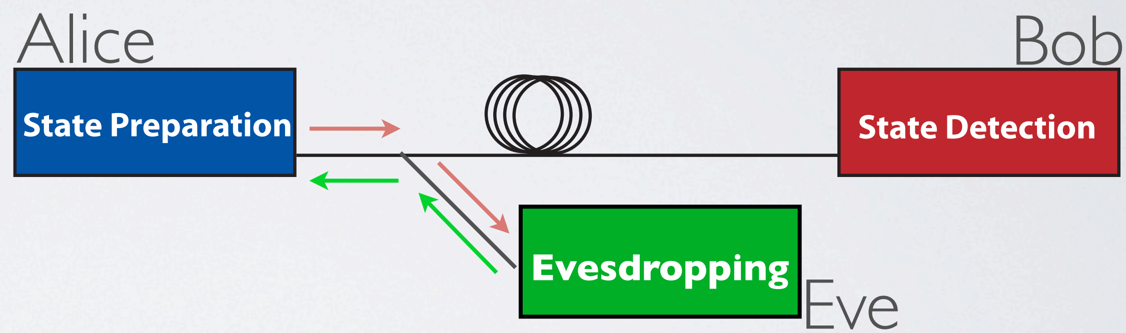
Decoy Analysis



Trojan Horse

Counter:

Optical Isolators



Detector Weaknesses

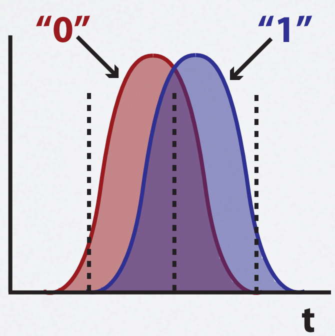
i.e. time-shift attack

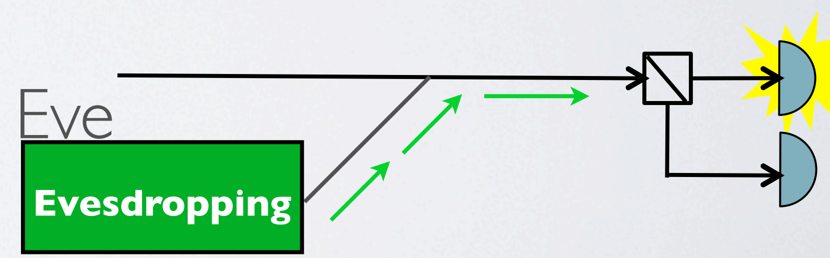
or blinding & faked states

Counter:

Robust Detectors?

Or New Protocols?

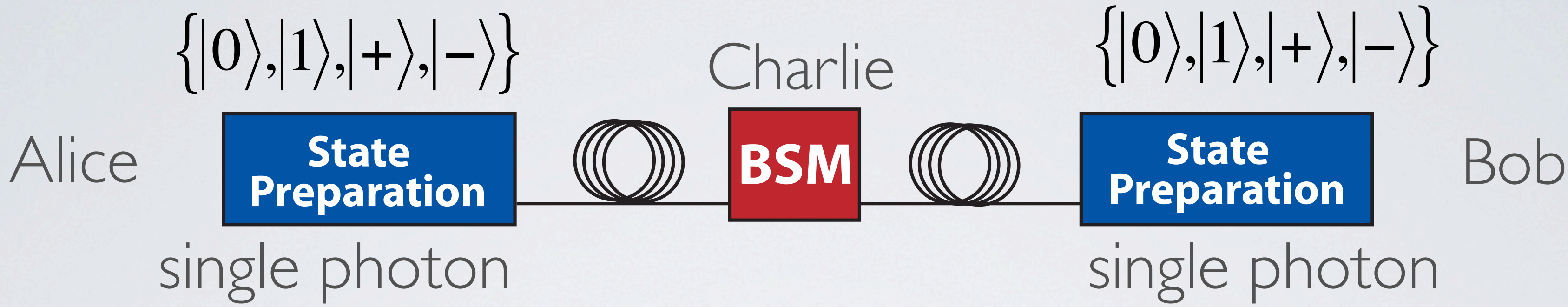




Brassard *et al*, PRL 85, 11330 (2002), Gisin *et al*, PRA, 022320 (2006), Zhao, PRA 78, 042333 (2008), Lydersen *et al*, Nat. Phot 4, 686689 (2010)

Table of Contents

New QKD Protocol: Time-Reversed QKD



$$|\psi^-\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right) = \frac{1}{\sqrt{2}}\left(|+-\rangle - |-+\rangle\right)$$

Requires:

- Bell-state measurements
- single photon source

To produce secret key:

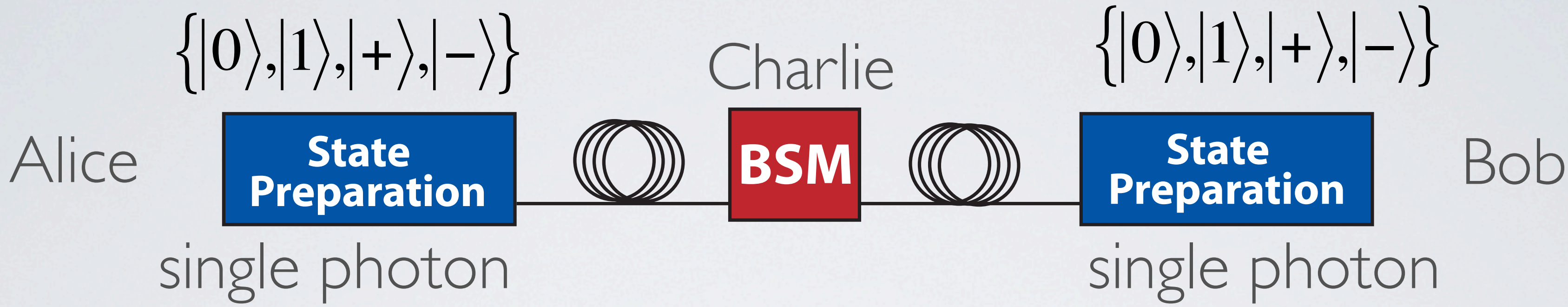
- Psi- projection & same bases implies different key bits
- sifting, Bob flip bits, error correction & privacy amplification

De-correlates detector response from secret key bits

➡ Immune to detector attacks

Inamori, Algorithmica 34, 340 (2002)

New QKD Protocol: Time-Reversed QKD



$$|\psi^-\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right) = \frac{1}{\sqrt{2}}\left(|+-\rangle - |-+\rangle\right)$$

Requires:

- Bell-state measurements
- single photon source ← Currently Difficult

To produce secret key:

- Psi- projection & same bases implies different key bits
- sifting, Bob flip bits, error correction & privacy amplification

De-correlates detector response from secret key bits

➡ Immune to detector attacks

Inamori, Algorithmica 34, 340 (2002)

Measurement Device Independent QKD (MDI-QKD)

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right) = \frac{1}{\sqrt{2}}\left(|+-\rangle - |-+\rangle\right)$$

Requires:

- Bell-state measurements
- random μ variation (signal & decoy states) to avoid PNS

Decoy Analysis to assess: $Q_{11}^{Z}, Q_{11}^{X}, e_{11}^{Z}, e_{11}^{X}$

To produce secret key:

- z-basis for key, x-basis for eavesdropping detection

$$S = Q_{11}^{z}\left(1 - h_2\left(e_{11}^{x}\right)\right) - Q_{\mu\mu}^{z} f h_2\left(e_{\mu\mu}^{z}\right)$$

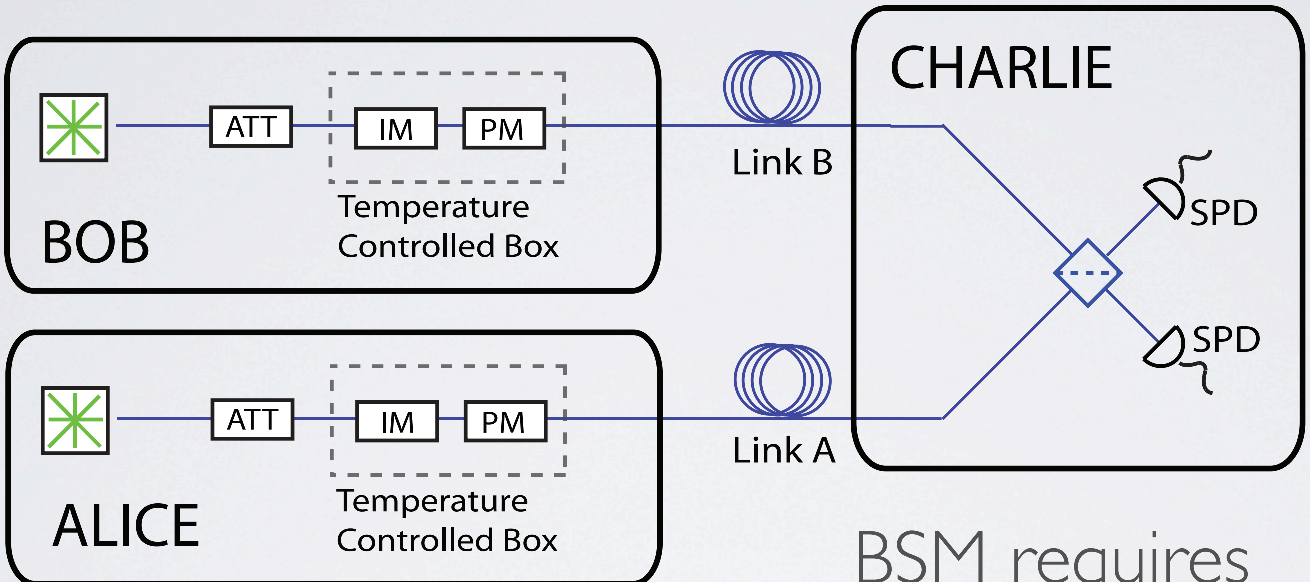
Lo *et al*, PRL 108, 130503 (2012) (see also Braunstein *et al*, PRL 108, 130502 (2012))

TABLE OF CONTENTS

- New Protocol: Measurement Device Independent QKD
- **Experimental Demonstration**
    - Setup
    - Results
- Conclusions

Experiment

Achievable with present technology



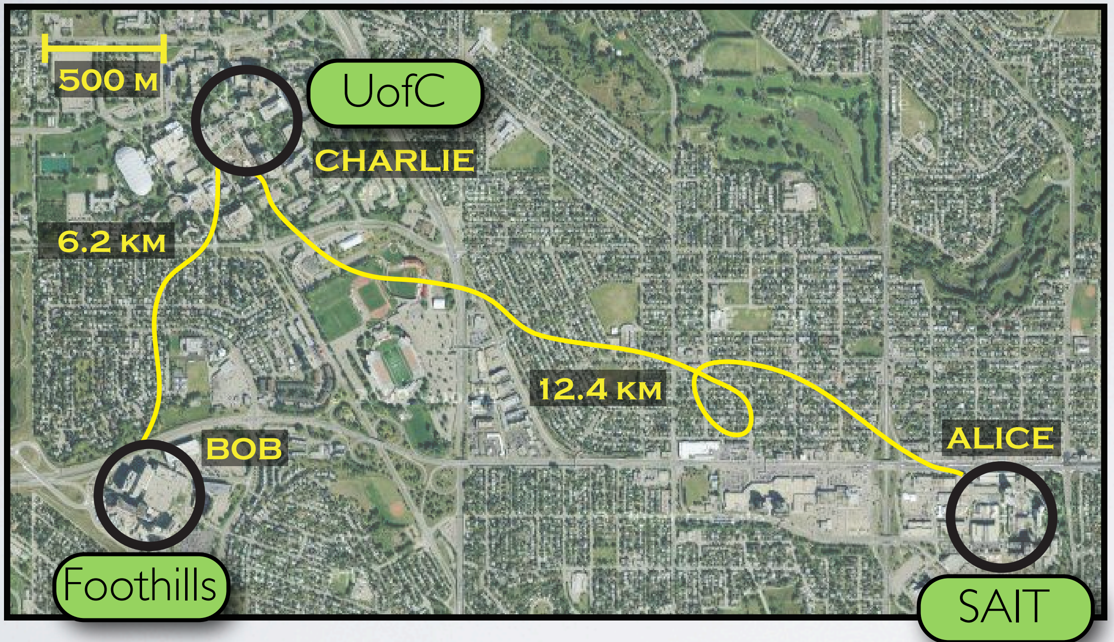
1550 nm time-bin qubits

- 500 ps FWHM, 1.4 ns time separation
- standard off-the-shelf telecommunication components
- pm fibre components (non-pm links)

BSM requires indistinguishable photons:

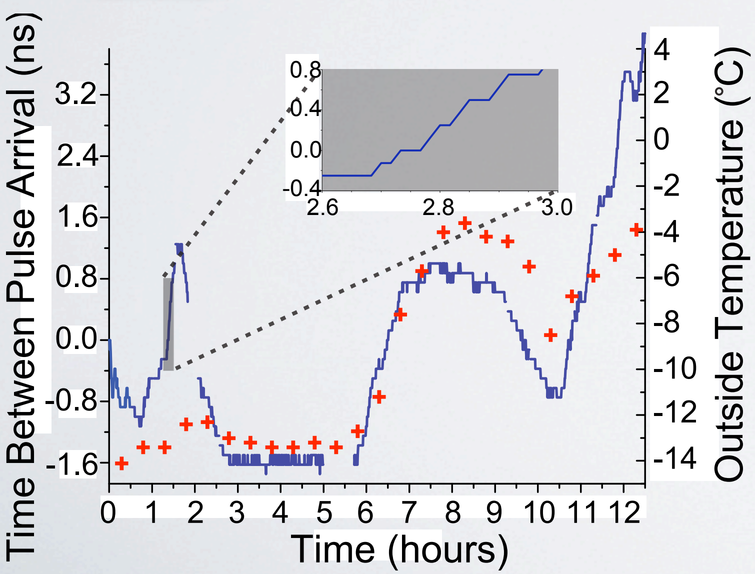
- temporal overlap
- polarization overlap
- spectral overlap
- spatial overlap

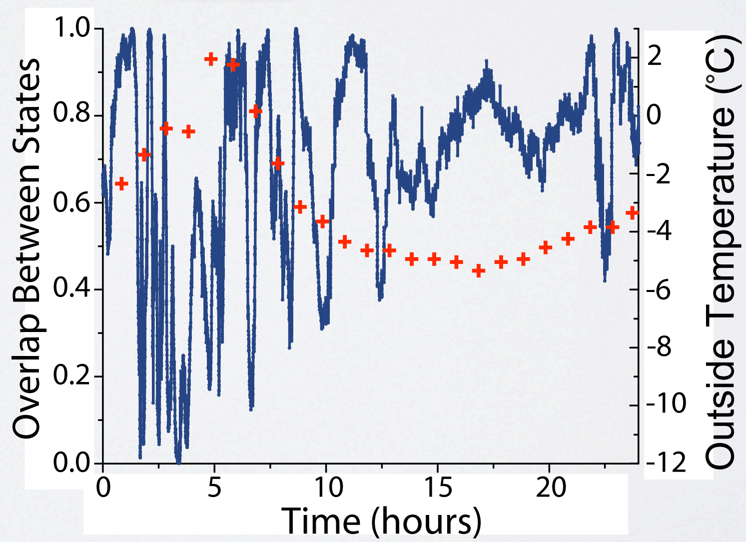
Experiment



BSM requires indistinguishable photons:

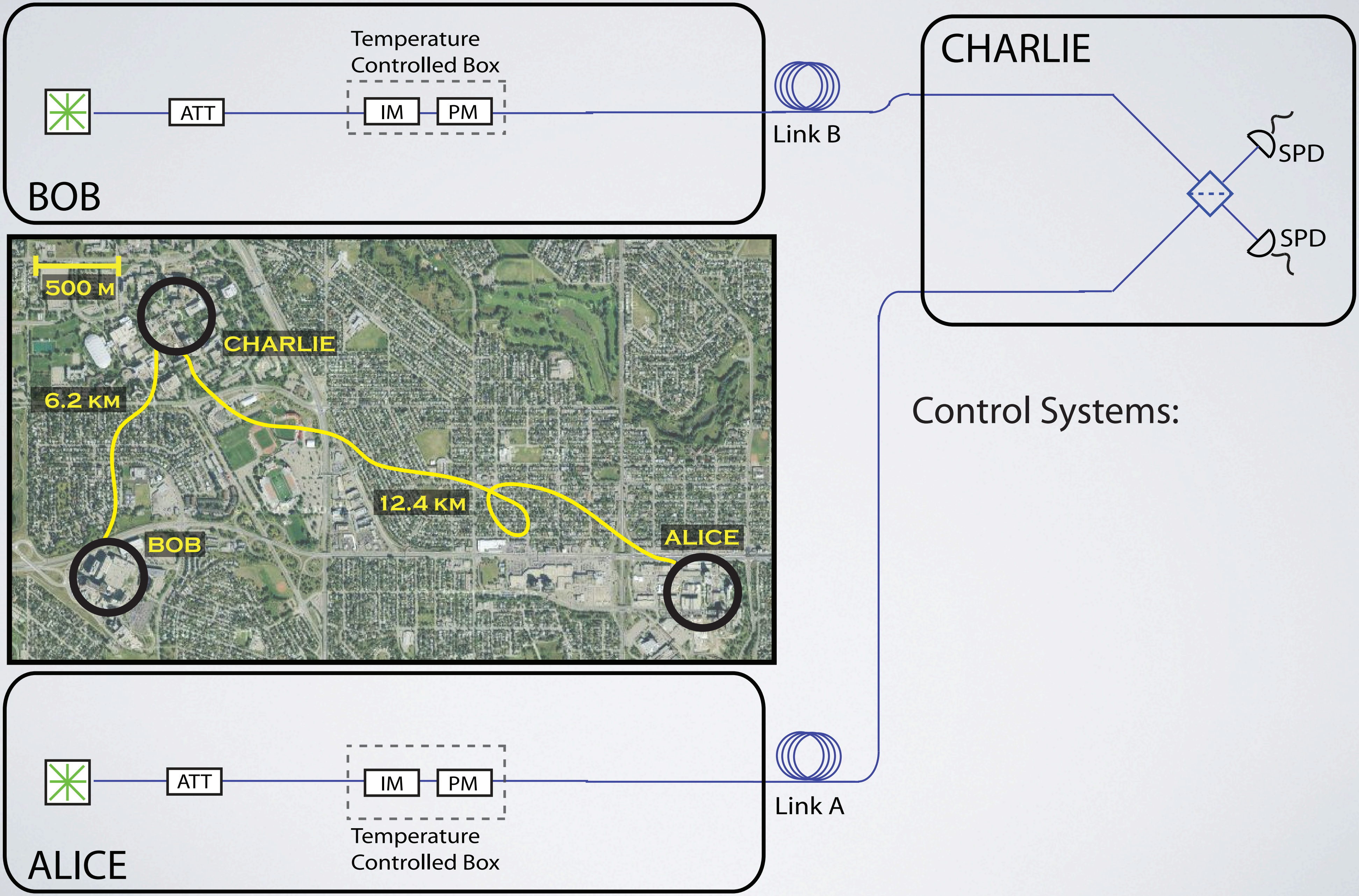
- temporal overlap
- polarization overlap
- spectral overlap
- spatial overlap





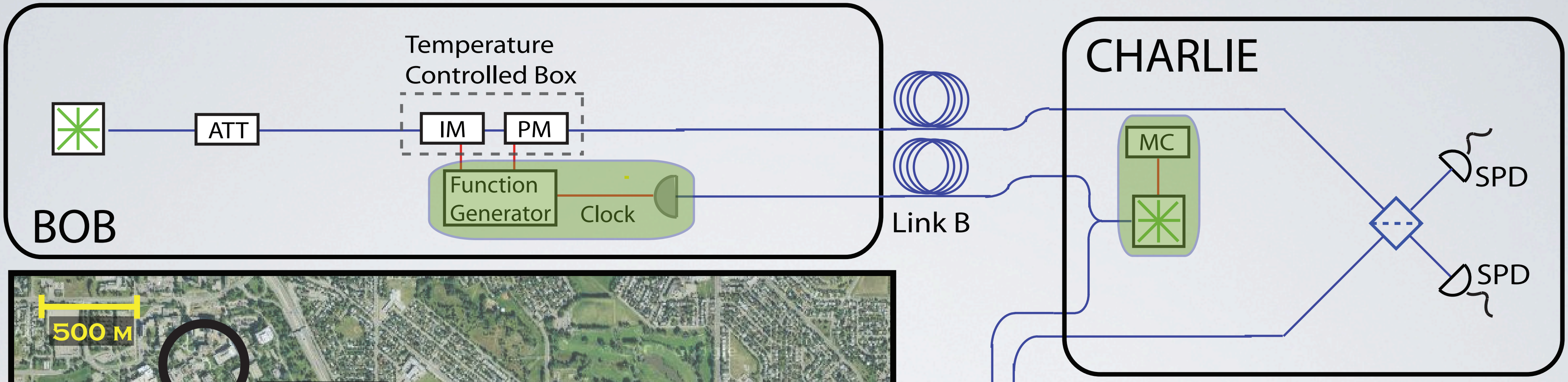
Also, relative frequency drift of 20 MHz/h

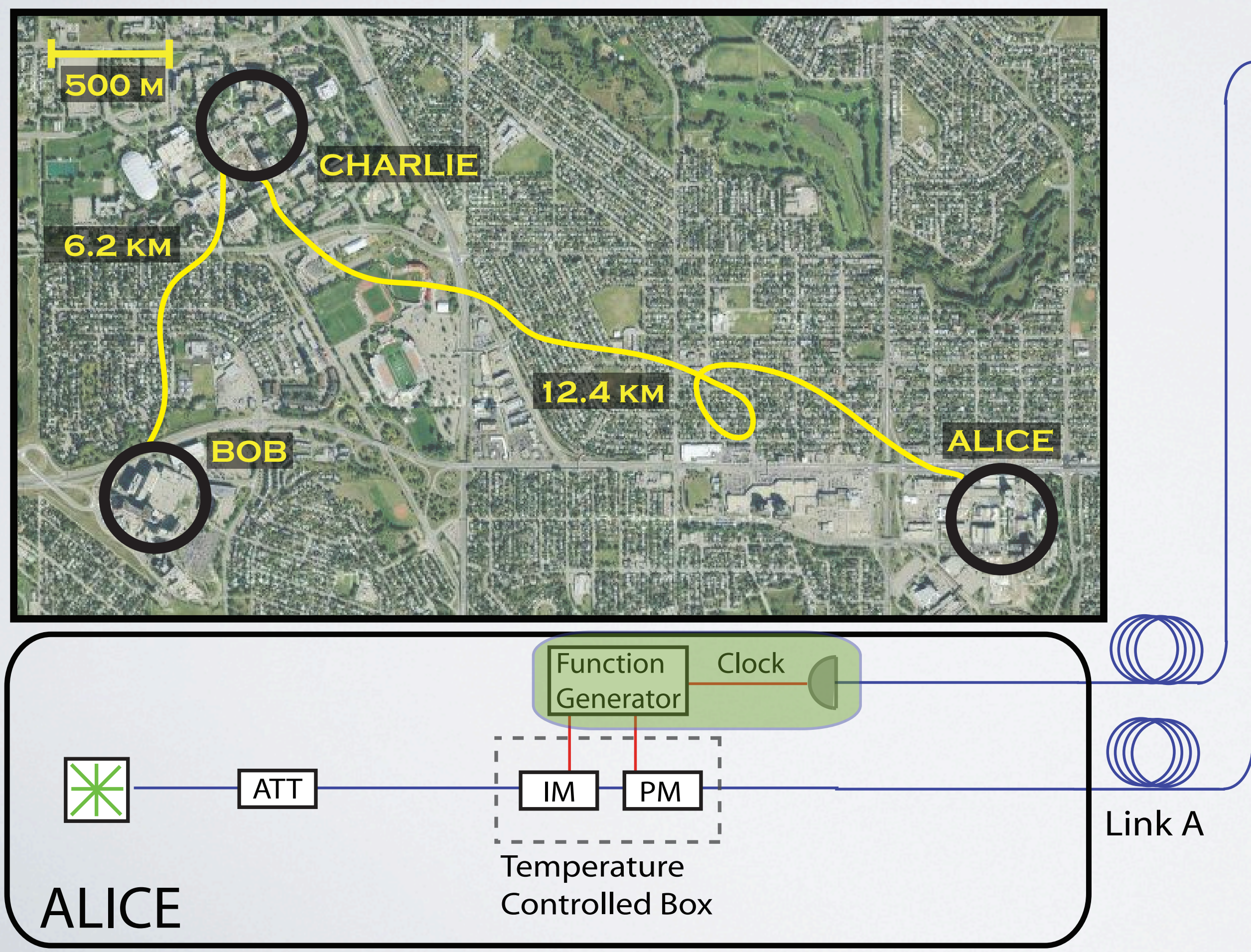
EXPERIMENT



Control Systems:

Experiment



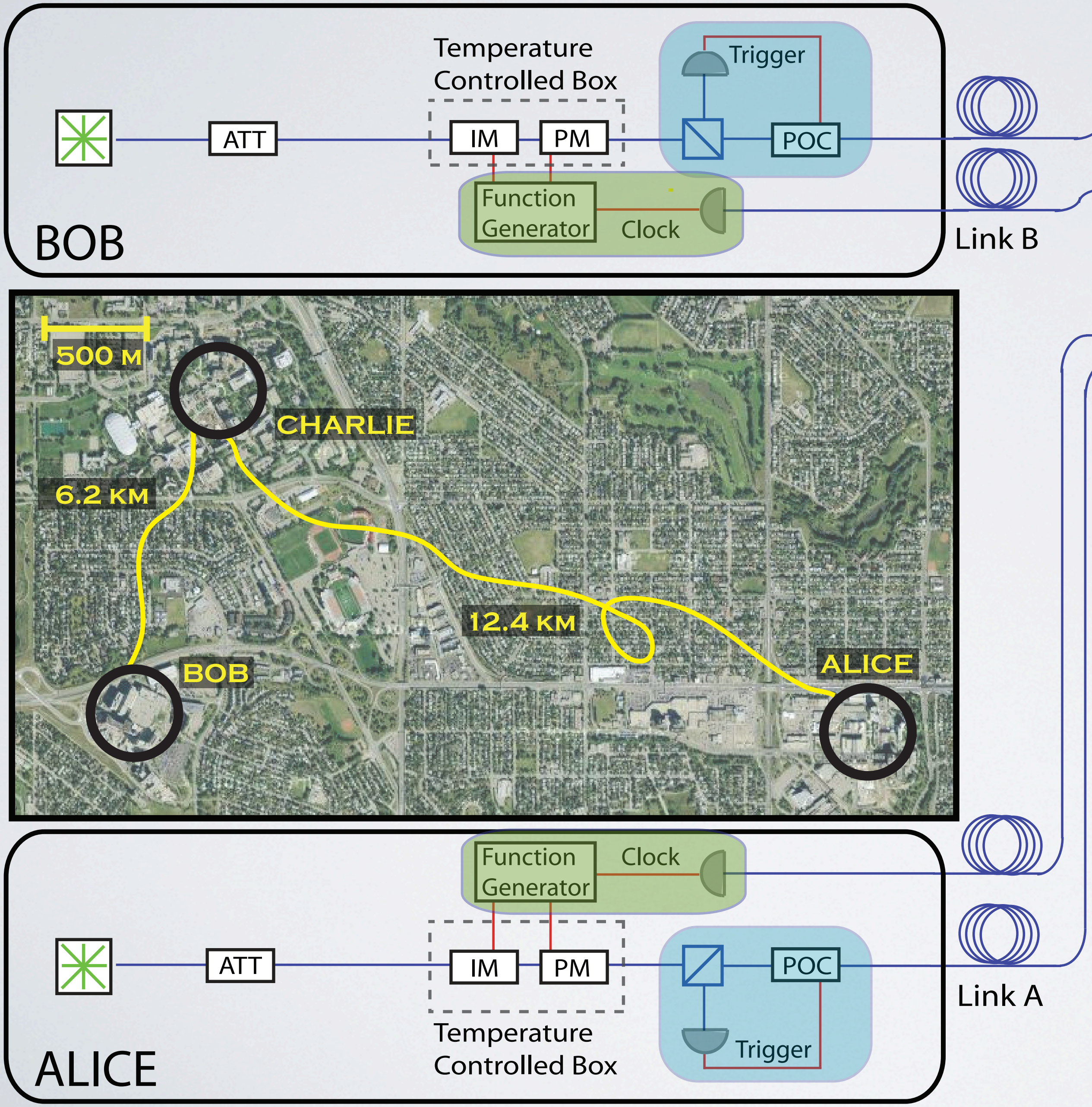


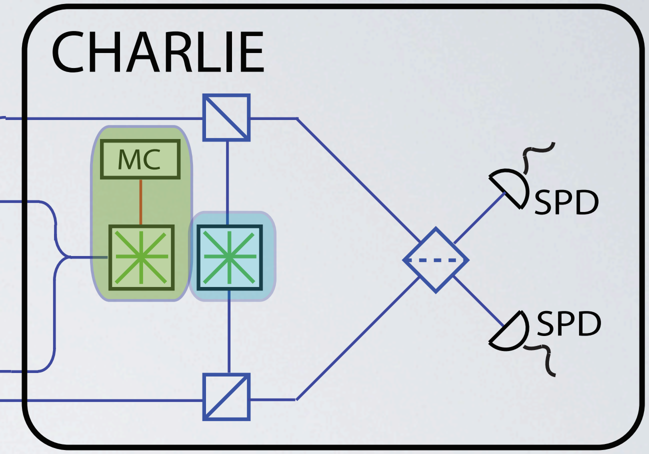
Control Systems:

- Timing Feedback

Charlie measured every 30 s & sent correction to A&B
Maintained:
< 50 ps difference

Experiment



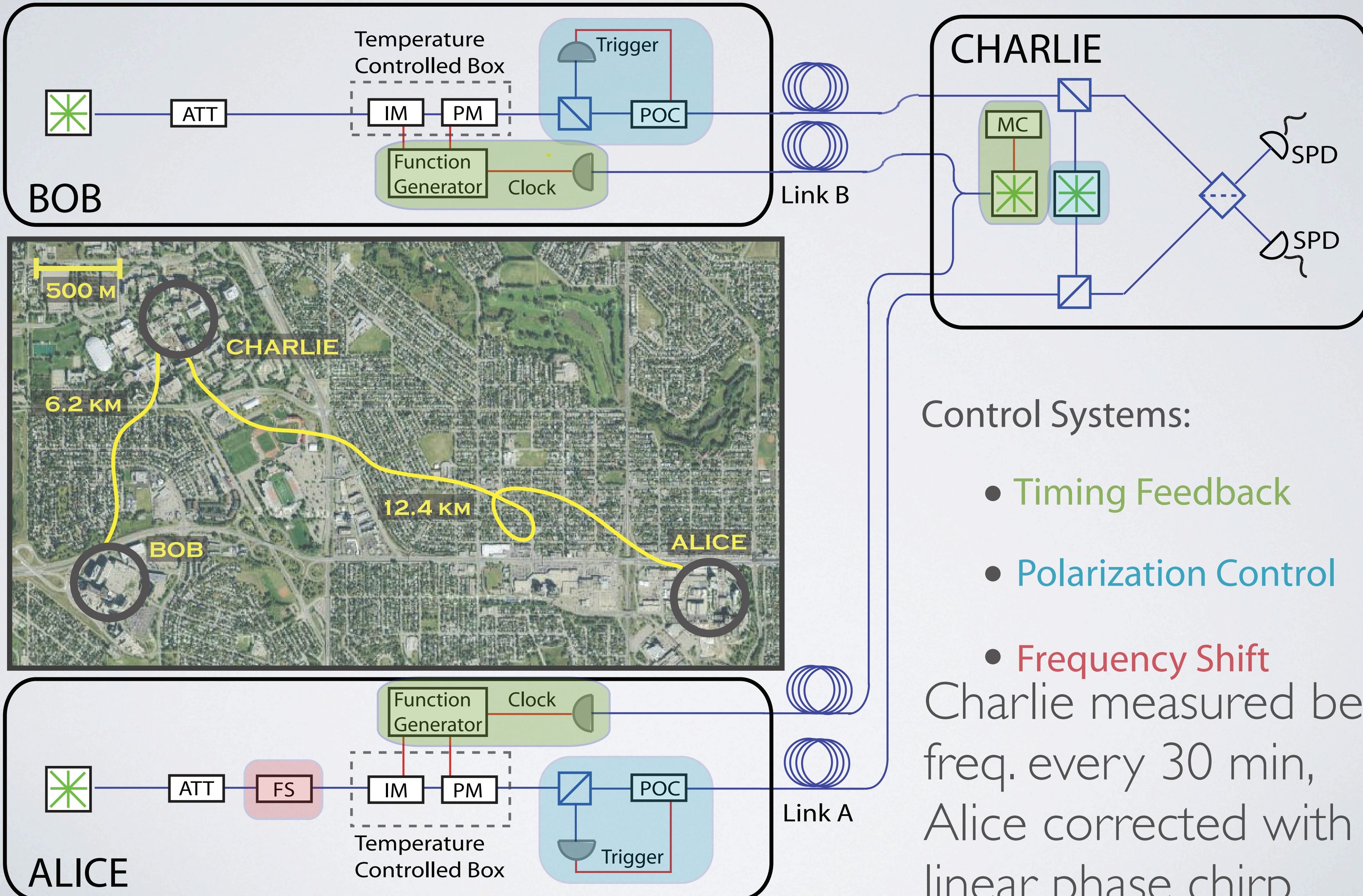


Control Systems:

- Timing Feedback
- Polarization Control

Charlie sent ortho. polarized light every 10 s (250 ms) A&B transform their photons

EXPERIMENT

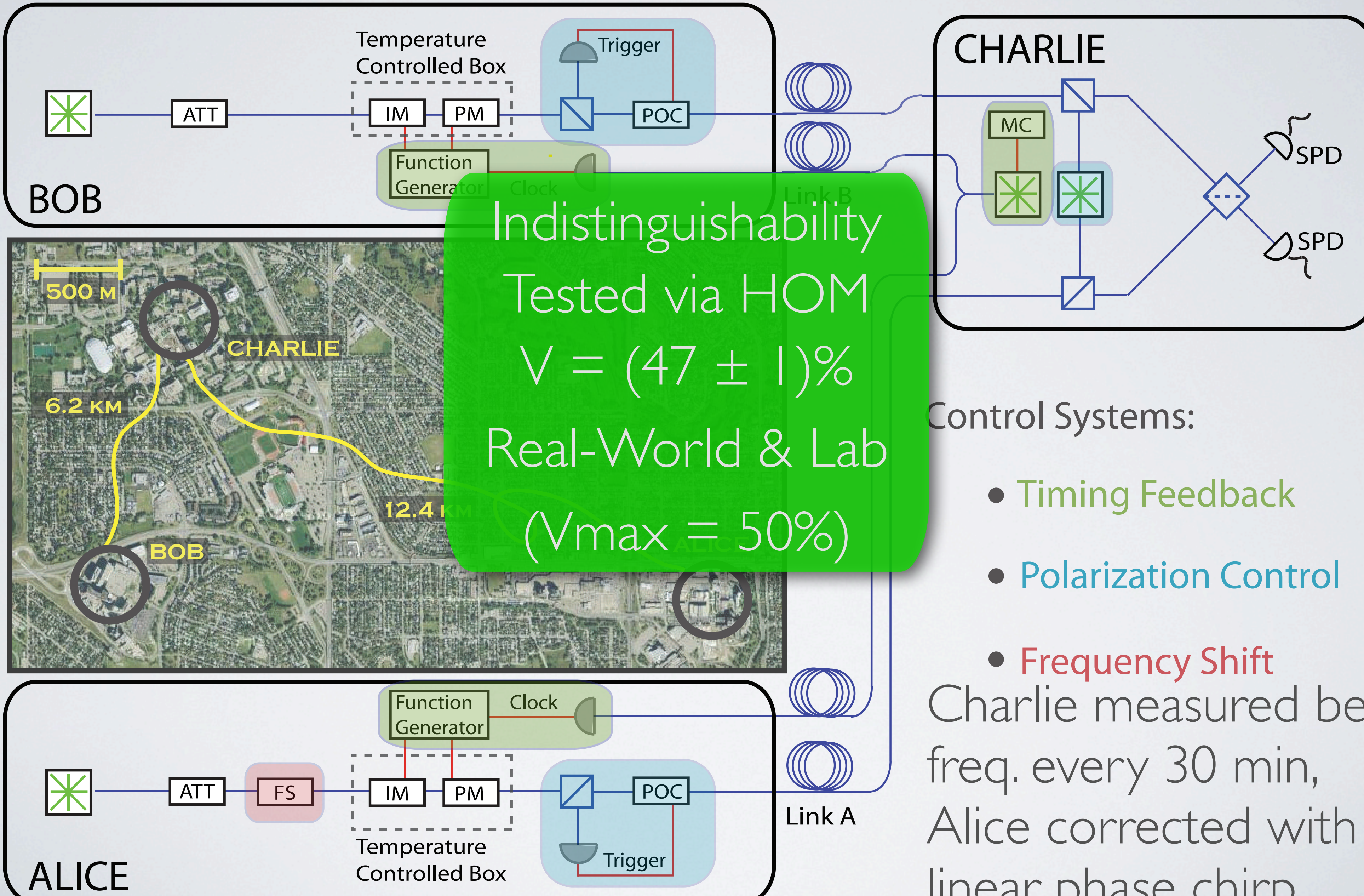


Control Systems:

- Timing Feedback
- Polarization Control
- Frequency Shift

Charlie measured beat freq. every 30 min, Alice corrected with linear phase chirp

Experiment



Indistinguishability Tested via HOM
V = (47 ± 1)%
Real-World & Lab
(Vmax = 50%)

Control Systems:

- Timing Feedback
- Polarization Control
- Frequency Shift

Charlie measured beat freq. every 30 min, Alice corrected with linear phase chirp

RESULTS: MDI-QKD

Measured Error Rates & Gains (Alice/Bob sending same basis):

$$Q_{\mu\mu}^{Z}, Q_{\mu\mu}^{X}, e_{\mu\mu}^{Z}, e_{\mu\mu}^{X}$$

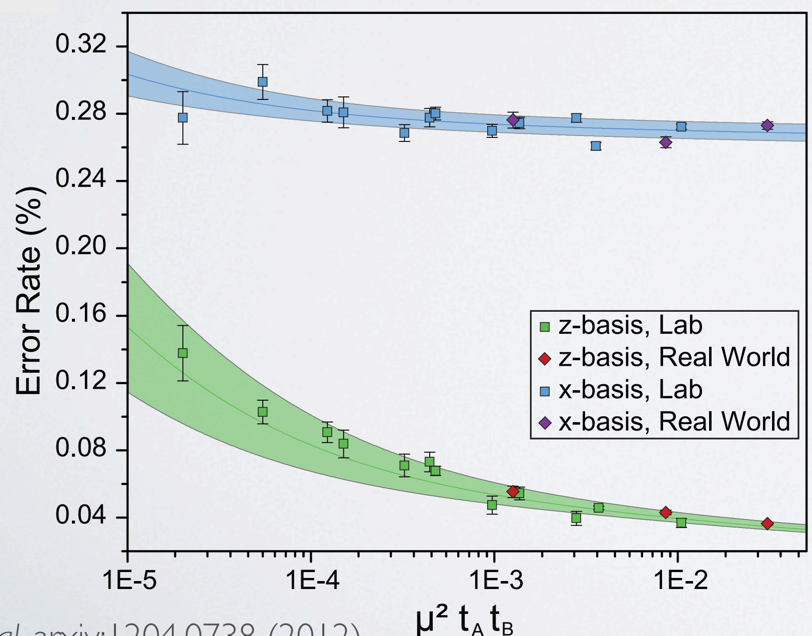
Repeated for:

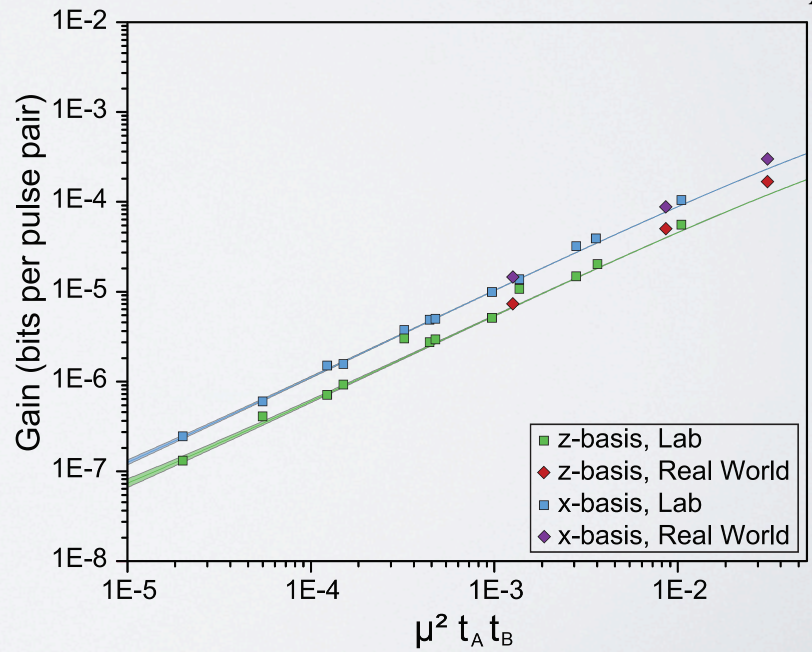
- different distances:
- different $\mu_A = \mu_B$:

$$\mu_{A,B} = \{0.1, 0.25, 0.5\}$$

l_A [km]	l_A [dB]	l_B [km]	l_B [dB]	l_{TOTAL} [dB]	
30.98	6.8	11.75	6.8	13.6	Lab
40.80	9.1	40.77	9.1	18.2	Lab
51.43	11.3	32.19	11.3	22.7	Lab
61.15	13.7	42.80	13.6	27.2	Lab
12.40	4.5	6.20	4.5	9.0	Real-world

$l_A = l_B$





Rubenok *et al*, arxiv:1204.0738 (2012).

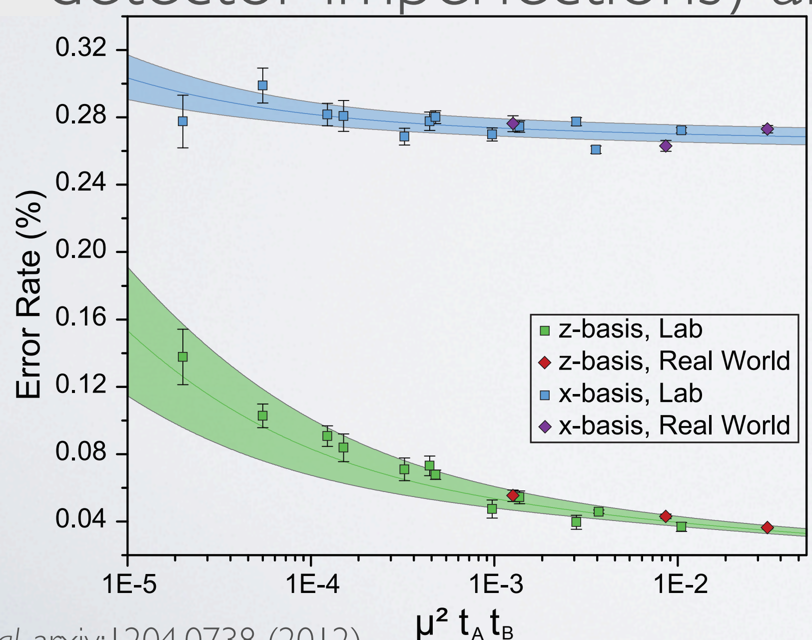
RESULTS: MDI-QKD

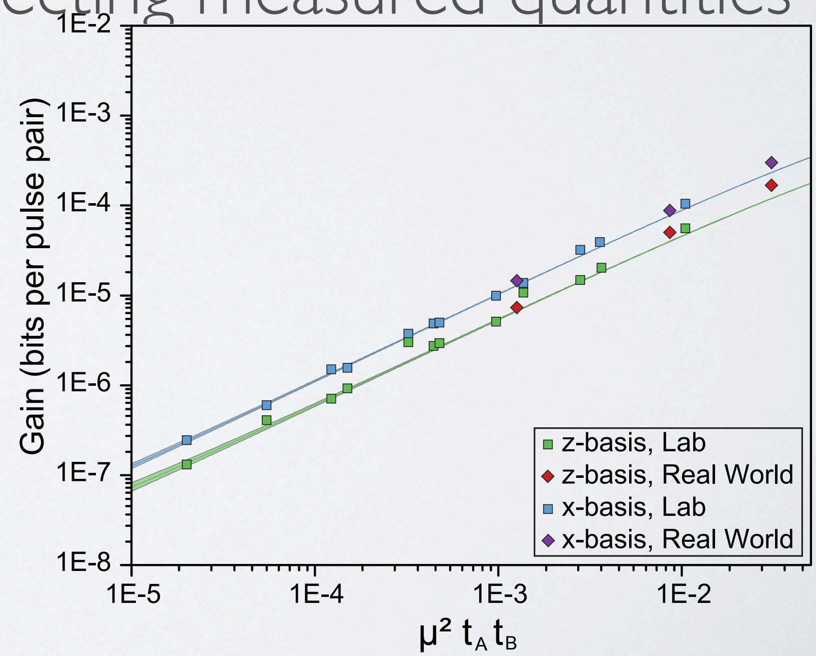
Measured Error Rates & Gains (Alice/Bob sending same basis):

$Q^Z_{\mu\mu}, Q^X_{\mu\mu}, e^Z_{\mu\mu}, e^X_{\mu\mu}$

Simulations using independently measured parameters

- ➡ agree with experimental measured quantities
- ➡ we understand imperfections (i.e. state generation & detector imperfections) affecting measured quantities





Rubenok *et al*, arxiv:1204.0738 (2012).

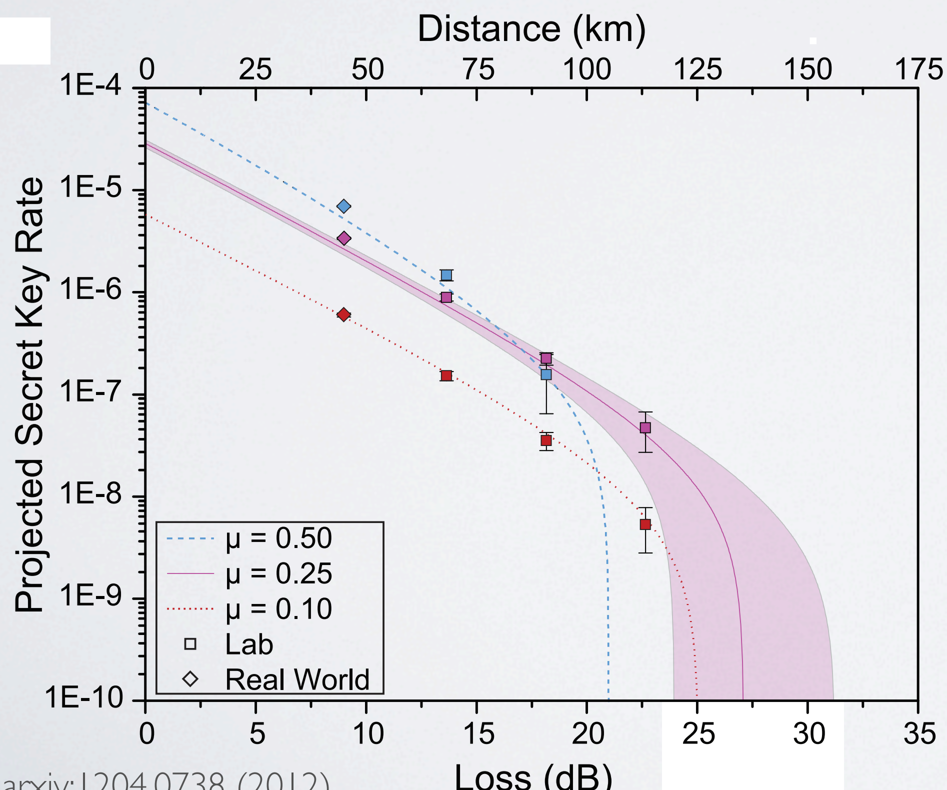
RESULTS

Estimate Secret Key Rate: $S = Q_{11}^{z}\left(1 - h_2\left(e_{11}^{x}\right)\right) - Q_{\mu\mu}^{z} f h_2\left(e_{\mu\mu}^{z}\right)$

With Alice/Bob sending same basis:

Measured Error Rates & Gains: $Q_{\mu\mu}^{Z}, Q_{\mu\mu}^{X}, e_{\mu\mu}^{Z}, e_{\mu\mu}^{X}$

Use simulation to estimate: $Q_{11}^{Z}, Q_{11}^{X}, e_{11}^{Z}, e_{11}^{X}$



Secret key possible up to 27 dB (127 km), (but, assuming efficient decoy analysis)

Rubenok *et al*, arxiv:1204.0738 (2012).

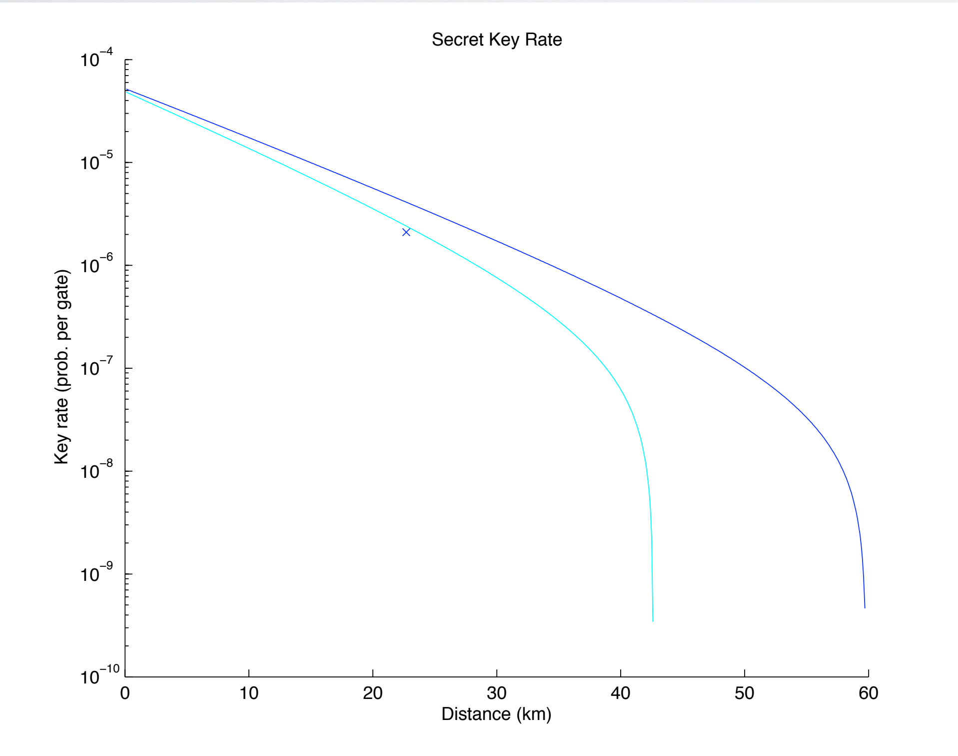
NEW RESULTS

Recently proposed Decoy analysis for MDI-QKD:

- random modulation between 3 μ: vacuum, decoy & signal
- lower bounds Q_{11}^{Z} & upper bounds e_{11}^{X}
    - But how tight?

$$S = Q_{11}^{z}\left(1 - h_2\left(e_{11}^{x}\right)\right) - Q_{\mu\mu}^{z} f h_2\left(e_{\mu\mu}^{z}\right)$$

Optimized μ (signal & decoy) to maximize secret key rate



Simulation (100% efficient):
S = 4.2e-6

Simulation of Decoy Analysis:
S = 2.4e-6
Efficiency: 57%

Experiment: S = 2.2e-6

Wang, arxiv:1207.0392 (2012), see also T. Ferreira da Silva et al., arXiv:1207.6345 (2012)

CONCLUSIONS

MDI-QKD removes side-channel detector attacks

Technology sufficiently developed to implement MDI-QKD

Straight-forward work required to build complete system

Efficiency of decoy analysis likely can be improved

Real-world, controlled Bell-State Measurements demonstrated, also a requirement for quantum repeaters, quantum networks, LOQC...