MEASUREMENT-DEVICE-INDEPENDENT QUANTUM KEY DISTRIBUTION

Joshua A. Slater

Vienna Centre for Quantum Science & Technology
University of Vienna, Austria

Institute for Quantum Science & Technology
University of Calgary, Canada

MEASUREMENT-DEVICE-INDEPENDENT QUANTUM KEY DISTRIBUTION

Joshua A. Slater

|Vienna Centre for Quantum Science & Technology
University of Vienna, Austria⟩ + |Institute for Quantum Science & Technology
University of Calgary, Canada⟩

VCQ

Institute for QUANTUM SCIENCE AND TECHNOLOGY at the University of Calgary

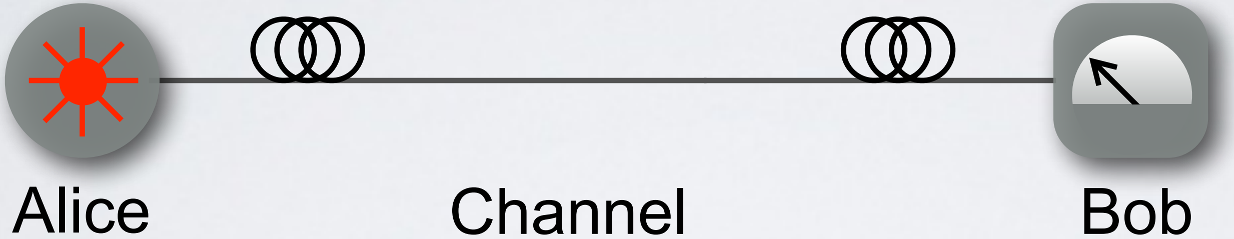
UNIVERSITY OF CALGARY

OUTLINE

- Side-Channel Attacks
- Measurement-Device-Independent QKD
- Experimental Challenges
- Experiments (part 1) - First Generation
- Theoretical Studies
- Alternative Protocols
- Experiments (part II) - Most Recent

QKD SECURITY

QKD protects the channel from Eve's tampering



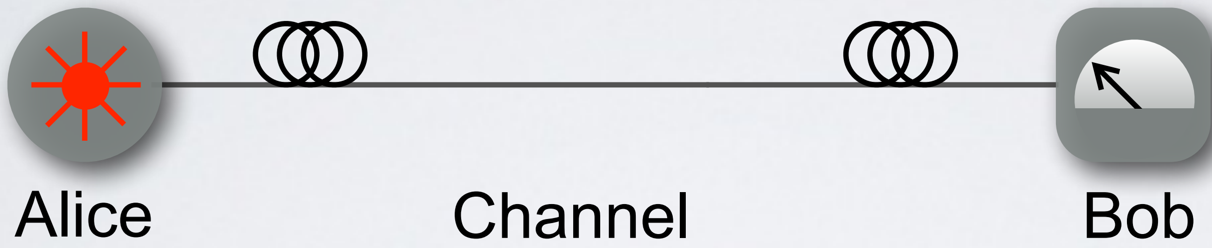
Prepare-and-Measure QKD

Channel secured by correlations

Sources & Measurements assumed secure

QKD SECURITY

QKD protects the channel from Eve's tampering



Prepare-a

Ch

So ... ure

Table 1. Summary of various quantum hacking attacks against certain commercial and research QKD set-ups.

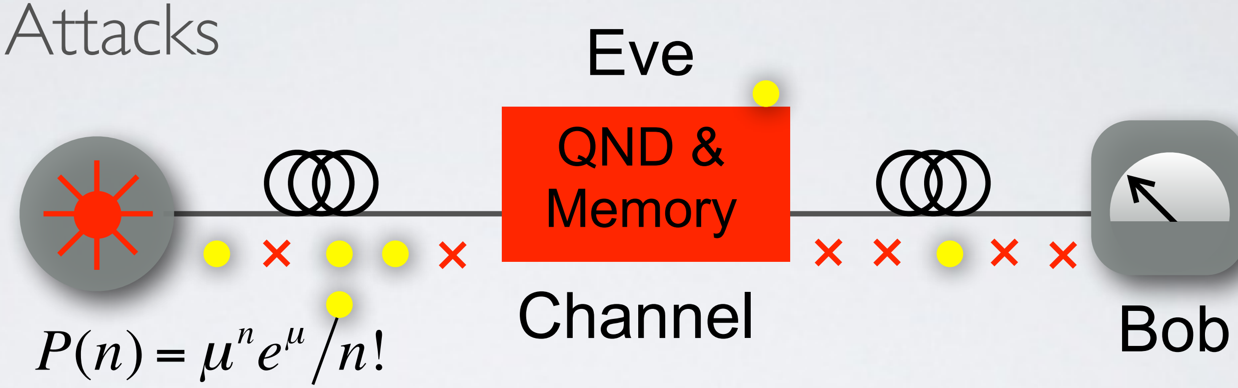
Attack	Target component	Tested system
Time shift[75–78]	Detector	Commercial system
Time information[79]	Detector	Research system
Detector control[80–82]	Detector	Commercial system
Detector control[83]	Detector	Research system
Detector dead time[84]	Detector	Research system
Channel calibration[85]	Detector	Commercial system
Phase remapping[86]	Phase modulator	Commercial system
Faraday mirror[87]	Faraday mirror	Theory
Wavelength[88]	Beamsplitter	Theory
Phase information[89]	Source	Research system
Device calibration[90]	Local oscillator	Research system

Lo, Curty, Tamaki, Nat. Photon (2014)

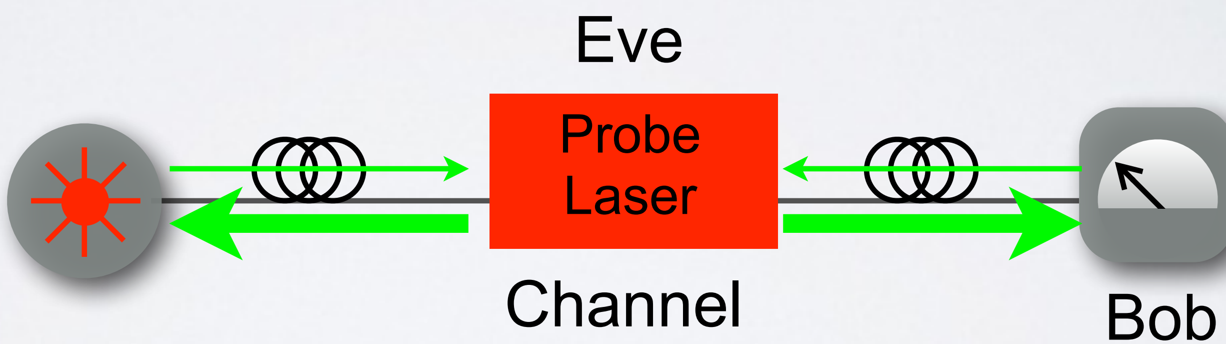
QKD SECURITY

(Some) Source Attacks

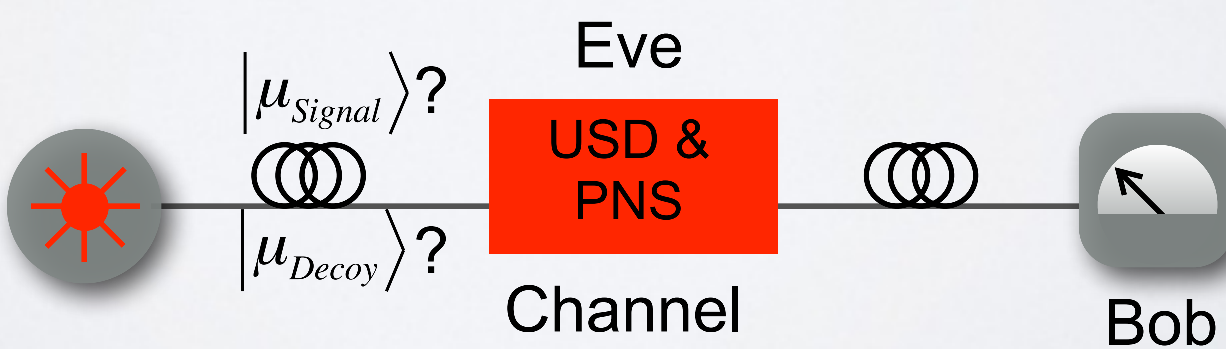
Photon-Number Splitting (PNS)



Trojan Horse



Phase Information



G. Brassard et al, PRA (2000), N. Gisin et al, PRA (2006), Y.-L. Tang et al, PRA (2013)

QKD SECURITY

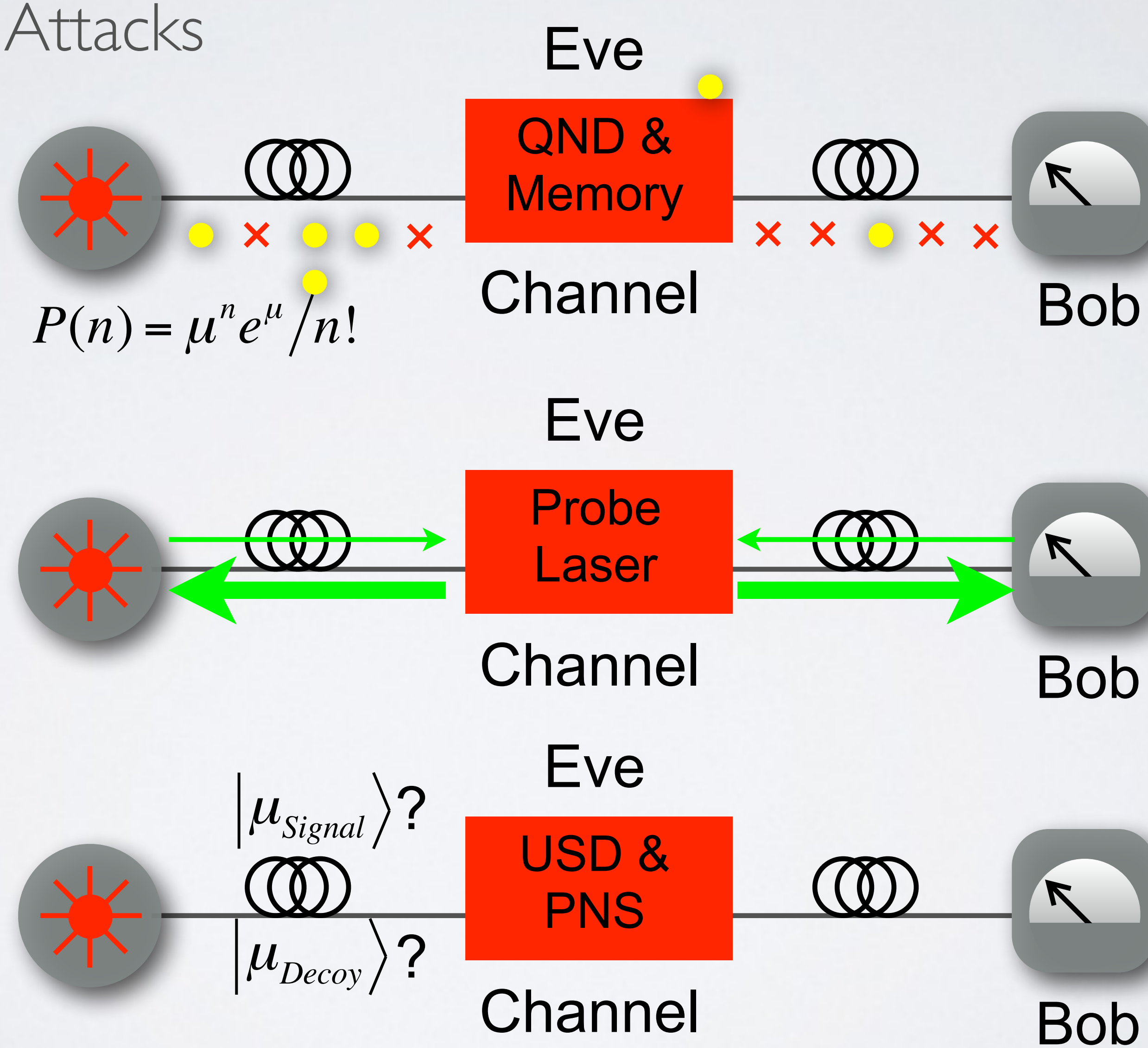
(Some) Source Attacks

Counters:

Photon-Number Splitting (PNS) — Decoy States

Trojan Horse — Isolators

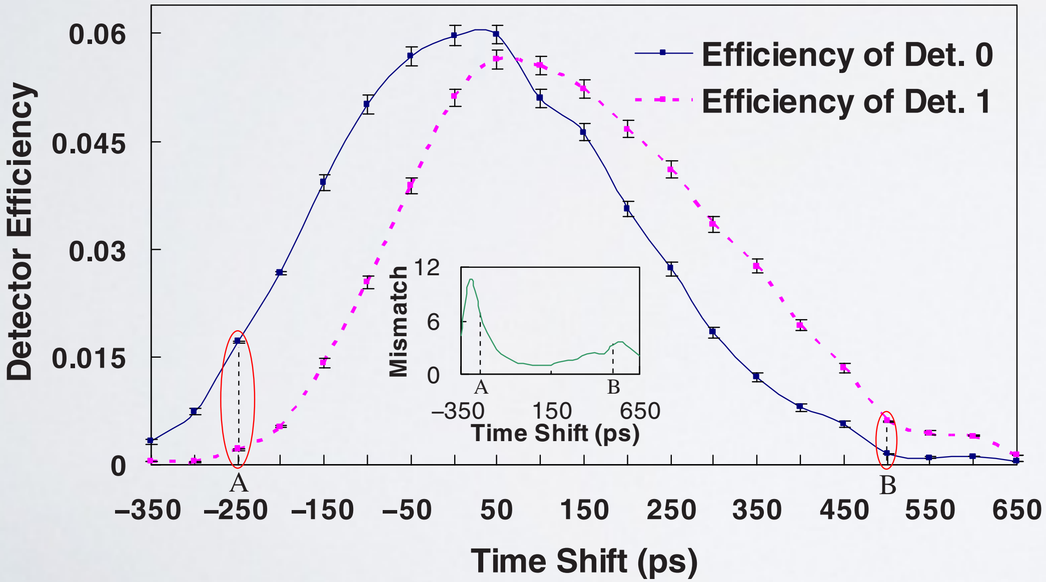
Phase Information — Random Phase



G. Brassard et al, PRA (2000), N. Gisin et al, PRA (2006), Y.-L. Tang et al, PRA (2013)

QKD SECURITY

Time-Shift attack

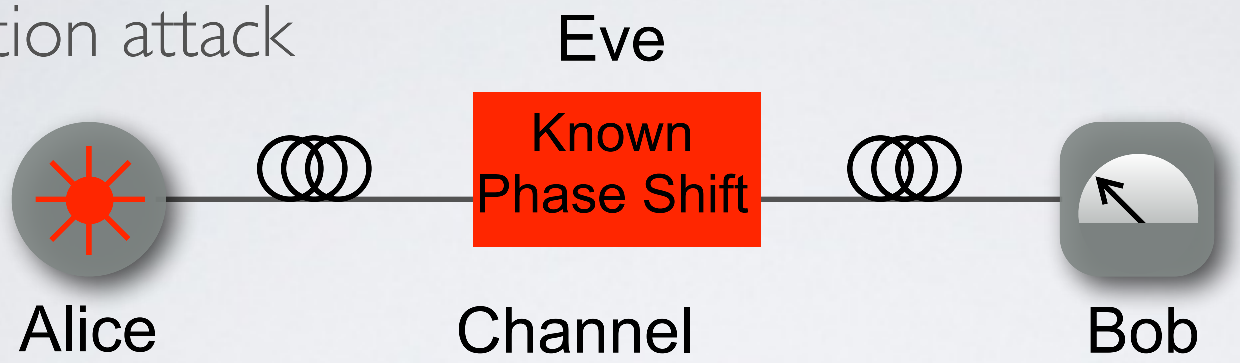


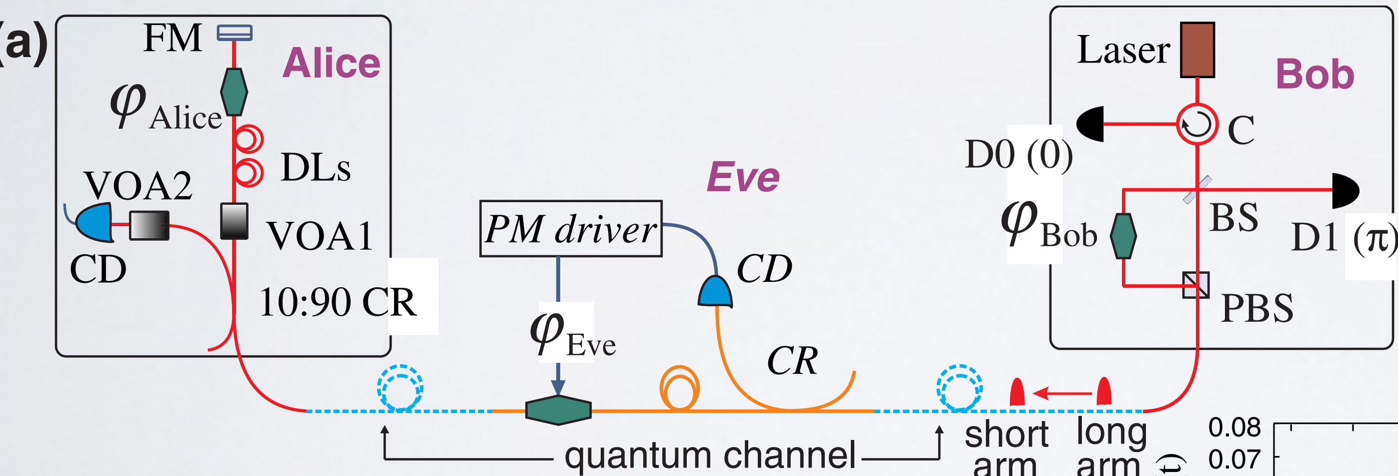
Shifting arrival time of photon to increase knowledge of bit upon detection

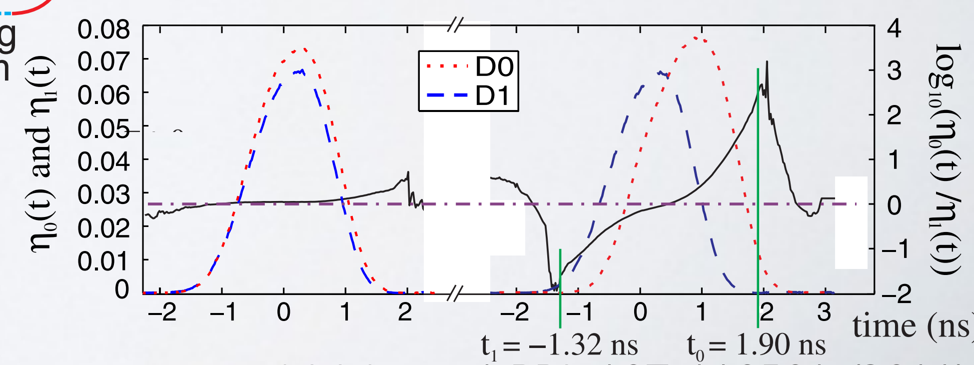
V. Makarov et al PRA 74, 022313 (2006), Y. Zhan et al PRA 78, 042333 (2008),

QKD SECURITY

Calibration attack







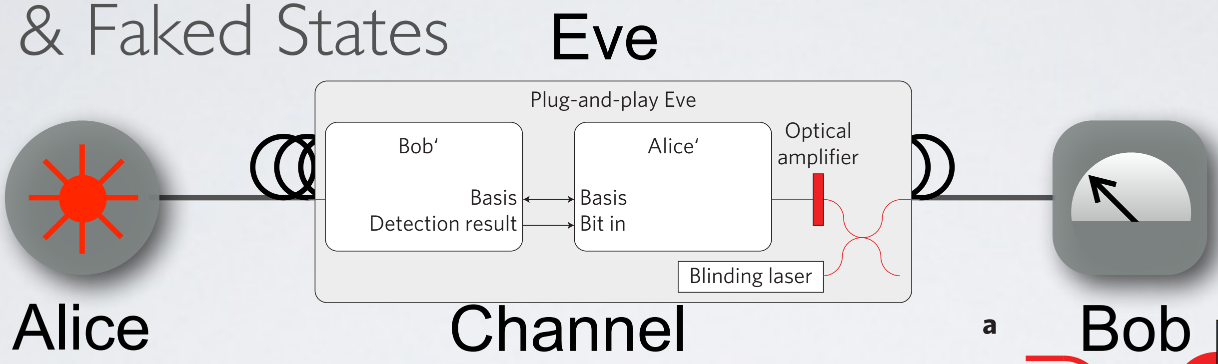
Eve introduces a delay, to create a efficiency mismatch

N. Jain et al, PRL 107, 110501 (2011)

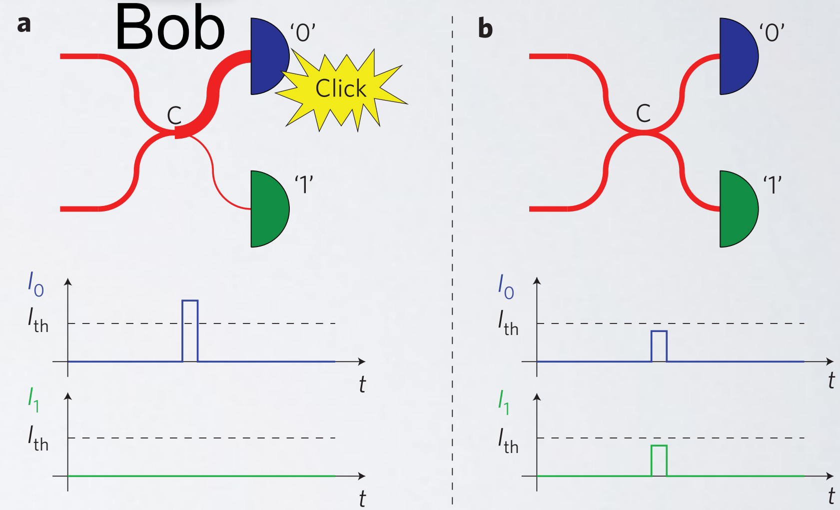
APD Operation:

QKD SECURITY

Blinding & Faked States



Bob's Detectors only 'click' when Eve wants



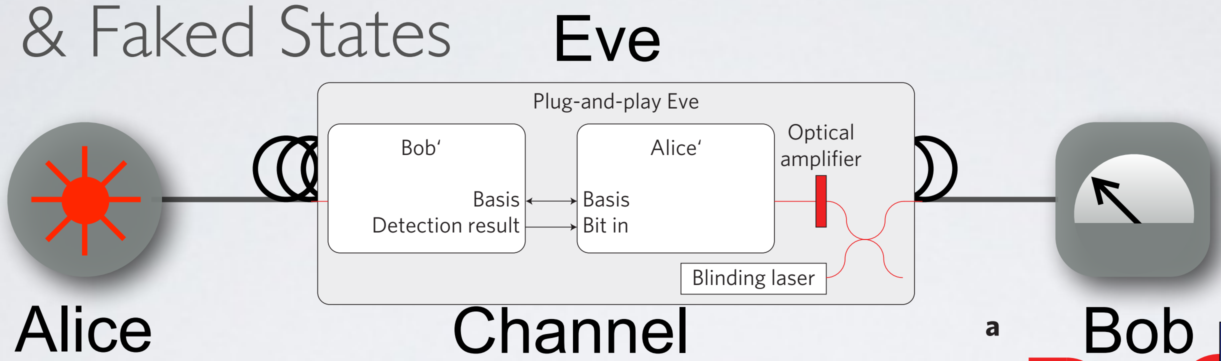
Faked states sent by Eve		Clicks at Bob			
		V	**−45°**	***H***	**+45°**
1,702,067	***V***	1,693,799 99.51%	0	0	0
2,055,059	**−45°**	0	2,048,072 99.66%	0	0
2,620,099	***H***	0	0	2,614,918 99.80%	0
2,359,494	**+45°**	0	0	0	2,358,418 99.95%

L. Lydersen et al, Nat. Photon. 4, 686 (2010), I. Gerhardt et al Nat. Comm. 2, 349 (2011)

APD Operation:

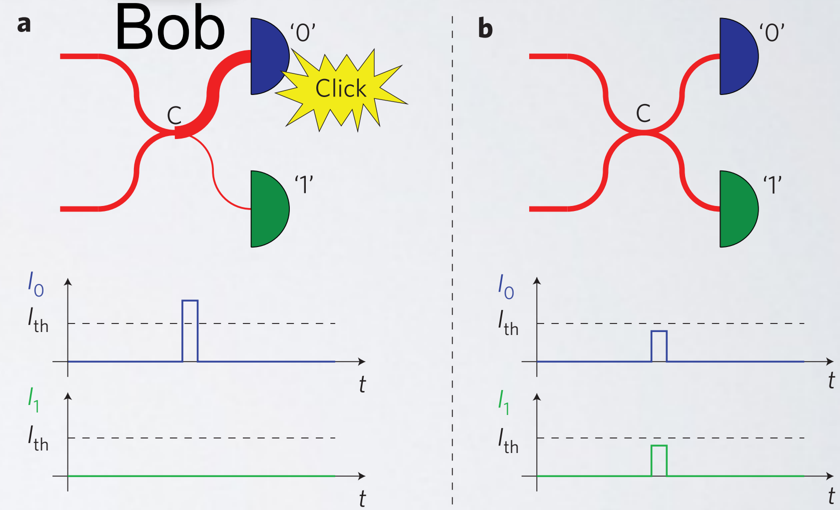
QKD SECURITY

Blinding & Faked States



Other Examples
- Thermal Blinding, Lydersen et al., Opt Exp (2010)
- Without Inception, Weier et al., NJP (2011)

- Controlling SN-SPD, Lydersen et al., NJP (2011)
- Controlling SN-SPD, Tanner et al., Opt Exp (2014)
- Blinding SD-SPD, Jiang et al., PRA (2013)



		V	**−45°**	***H***	**+45°**
1,702,067	***V***	1,693,799 99.51%	0	0	0
2,055,059	**−45°**	0	2,048,072 99.66%	0	0
2,620,099	***H***	0	0	2,614,918 99.80%	0
2,359,494	**+45°**	0	0	0	2,358,418 99.95%

L. Lydersen et al, Nat. Photon. 4, 686 (2010), I. Gerhardt et al Nat. Comm. 2, 349 (2011)

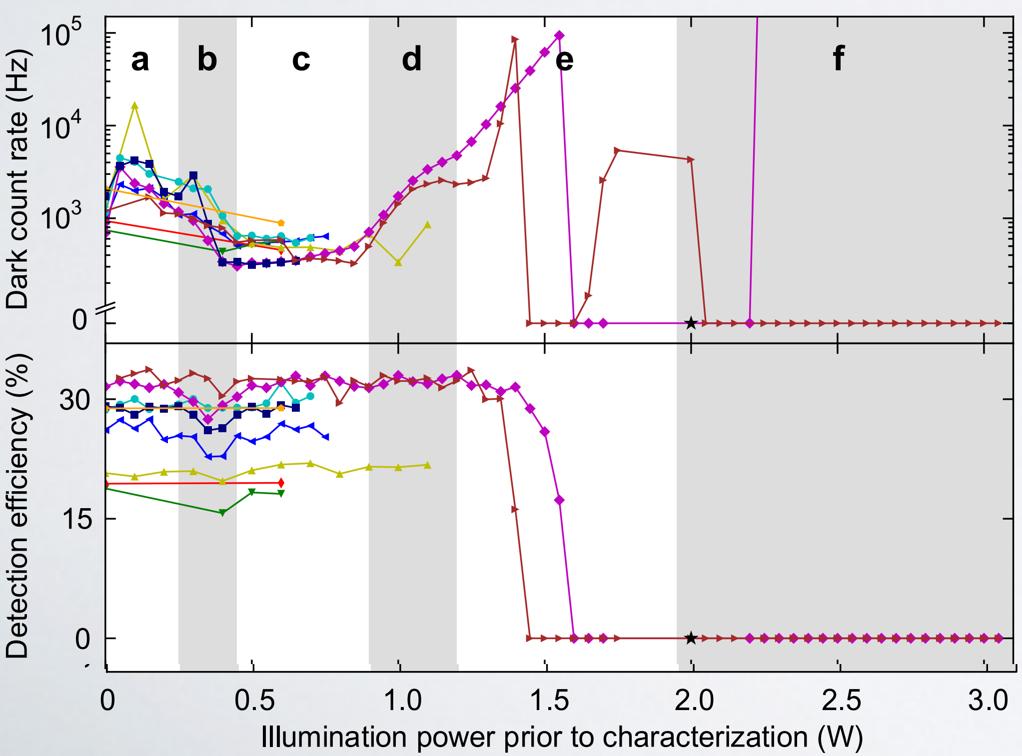
QKD SECURITY

Blinding

PRL **112,** 070503 (2014) PHYSICAL REVIEW LETTERS week ending 21 FEBRUARY 2014

Laser Damage Helps the Eavesdropper in Quantum Cryptography

Audun Nystad Bugge,[1] Sebastien Sauge,[2] Aina Mardhiyah M. Ghazali,[3] Johannes Skaar,[1] Lars Lydersen,[1] and Vadim Makarov[4,*]



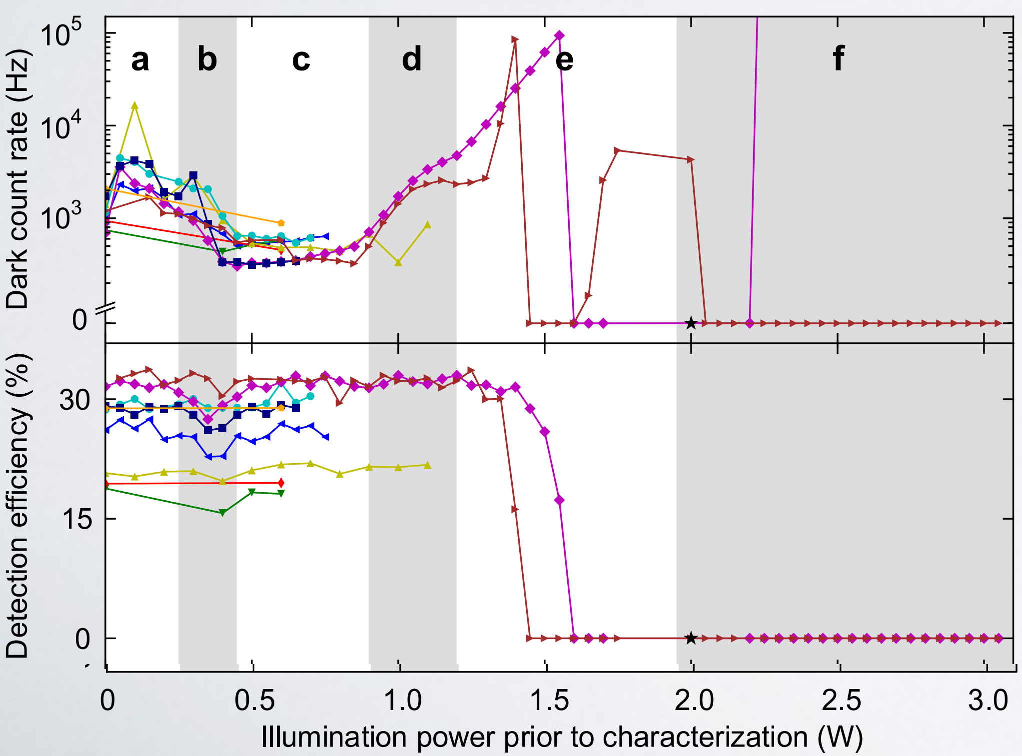
QKD SECURITY

Blinding

PRL **112,** 070503 (2014) PHYSICAL REVIEW LETTERS week ending 21 FEBRUARY 2014

Laser Damage Helps the Eavesdropper in Quantum Cryptography

Audun Nystad Bugge,[1] Sebastien Sauge,[2] Aina Mardhiyah M. Ghazali,[3] Johannes Skaar,[1] Lars Lydersen,[1] and Vadim Makarov[4,*]



“f. Catastrophic structure damage takes place ..... the bonding wires melted off ..... completely lost all photosensitivity, with the device becoming a resistor.....

Later states of damage result in visible changes to the APD ..... In the last stage of damage, the laser beam produces a hole”

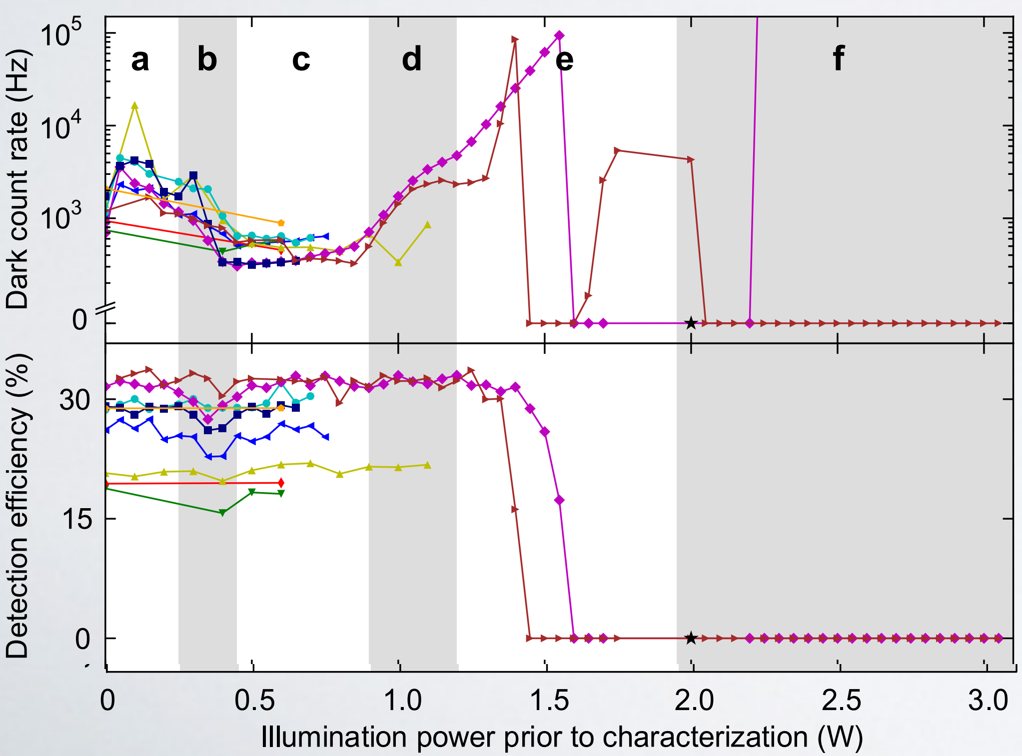
QKD SECURITY

Blinding


PRL **112,** 070503 (2014) PHYSICAL REVIEW LETTERS week ending 21 FEBRUARY 2014

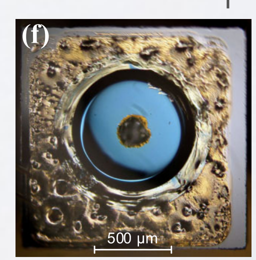
Laser Damage Helps the Eavesdropper in Quantum Cryptography

Audun Nystad Bugge,[1] Sebastien Sauge,[2] Aina Mardhiyah M. Ghazali,[3] Johannes Skaar,[1] Lars Lydersen,[1] and Vadim Makarov[4,*]



"f. Catastrophic structure damage takes place ..... the bonding wires melted off ..... completely lost all photosensitivity, with the device becoming a resistor.....

Later states of damage result in visible changes to the APD ..... In the last stage of damage, the laser beam produces a hole"



OPTIONS?

OPTIONS?

1) Better Security Proofs? ... to deal with our imperfections?

Random Variation of Detector Efficiency: A Secure Countermeasure against Detector Blinding Attacks for Quantum Key Distribution

Charles Ci Wen Lim, Nino Walenta, Matthieu Legré, Nicolas Gisin and Hugo Zbinden

Quant-ph:1408.6398

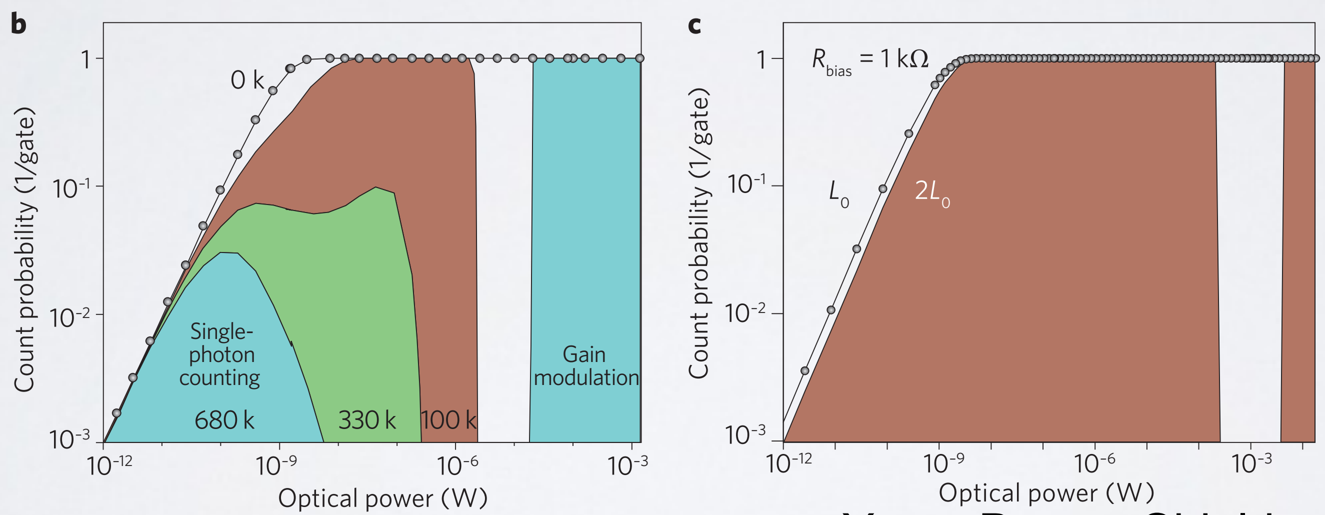
If $F(y_e, y)$ & not η,

then Eve can be caught!

OPTIONS?

1) Better Security Proofs? ... to deal with our imperfections?

2) Better Devices? ... that can't be hacked?



Yuan, Dynes, Shields, Nat. Photon. (2010)

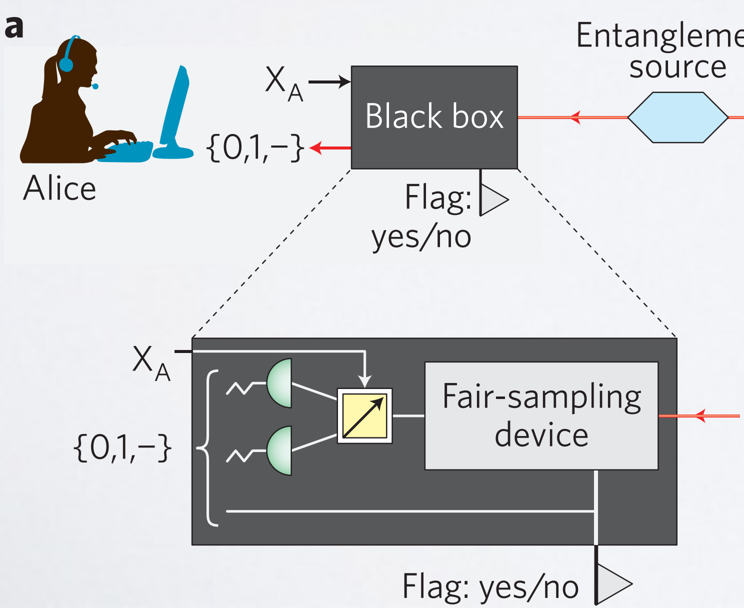
OPTIONS?

1) Better Security Proofs? ... to deal with our imperfections?

2) Better Devices? ... that can't be hacked?

3) Better Protocols? ... immune to hacking?

Device-Independent (DI) QKD?



Efficiencies of 80%

10^{-10} bits/pulse

OPTIONS?

1) Better Security Proofs? ... to deal with our imperfections?

2) Better Devices? ... that can't be hacked?

3) Better Protocols? ... immune to hacking?

Device-Independent (MDI) QKD?

.... immune to large class of hacks?

Measurement Device-Independent (MDI) QKD?

OUTLINE

- Side-Channel Attacks
- **Measurement-Device-Independent QKD**
- Experimental Challenges
- Experiments (part 1) - First Generation
- Theoretical Studies
- Alternative Protocols
- Experiments (part II) - Most Recent

OLD IDEA

PHYSICAL REVIEW A VOLUME 54, NUMBER 4 OCTOBER 1996

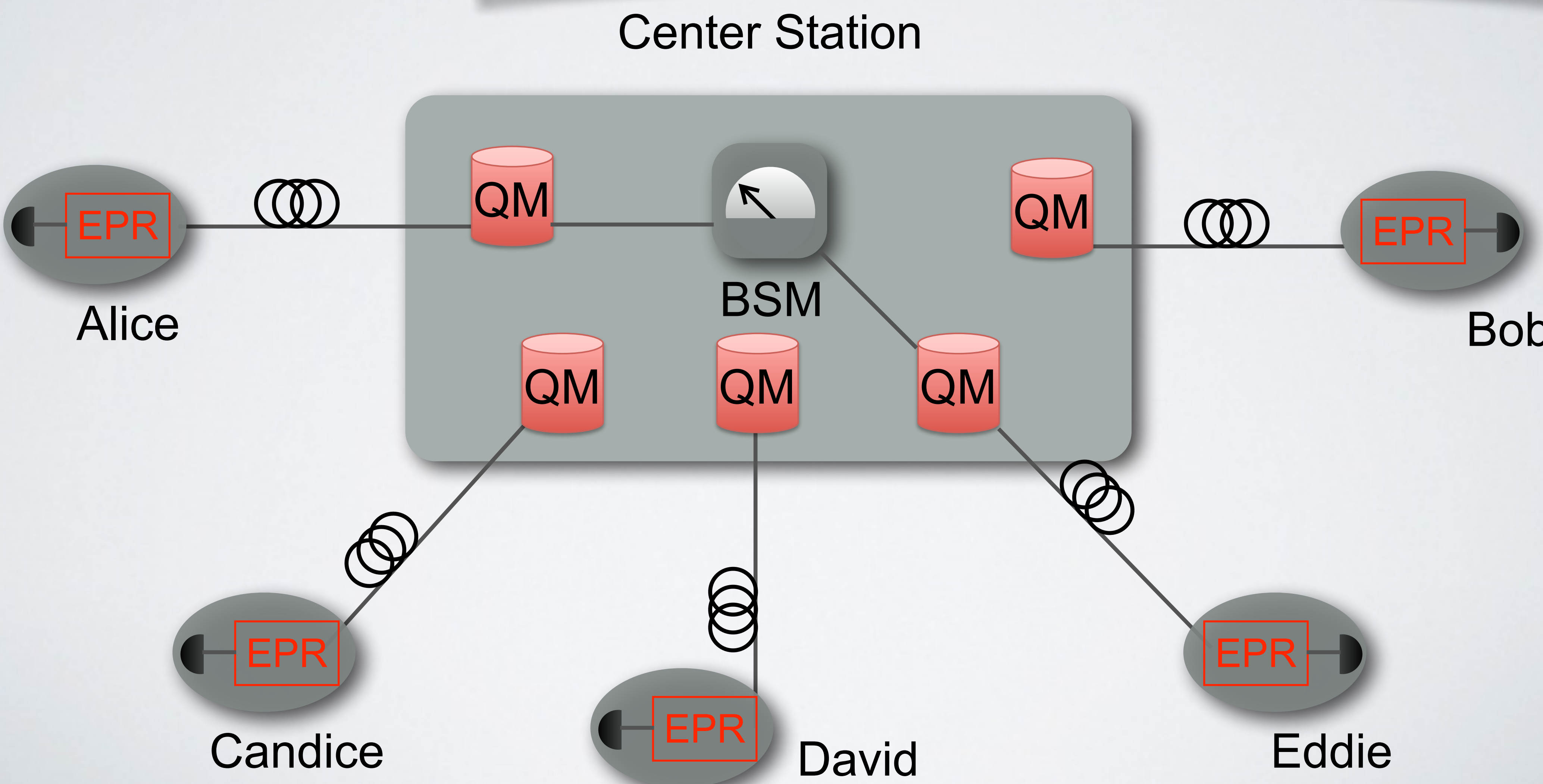
Quantum cryptographic network based on quantum memories

Eli Biham
Computer Science Department, Technion, Haifa 32000, Israel

Bruno Huttner
Group of Applied Physics, University of Geneva, CH-1211, Geneva 4, Switzerland

Tal Mor
Department of Physics, Technion, Haifa 32000, Israel

(Received 4 March 1996)



OLD IDEA

Time-Reversed EPR QKD (Biham, Hattner, Tor, PRA 1996)

Security proved (H. Inamori Algorithmica 2002)

NEW IMPORTANCE!

Side-Channel-Free QKD (Braunstein & Pirandola, PRL 130502 (2012))

Private Spaces, Remote State Preparation & Virtual channels

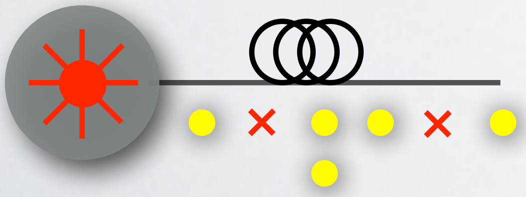
NEW IMPORTANCE!

Measurement-Device-Independent QKD (Lo, Curdy, Qi, PRL 130503 (2012))

1. Detector Side Channels all removed

known & yet to be discovered!

2. PNS attack avoidable with Decoy States



$P(n) = \mu^n e^{\mu} / n!$

NEW IMPORTANCE!

Measurement-Device-Independent QKD (Lo, Curdy, Qi, PRL 130503 (2012))

1. Distribution (Alice & Bob)

   Attenuated Laser, Random intensity, Random BB84: $\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}$

   Charlie:

   Project each pair onto a Bell-State: $|\psi-\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right)$

2. Reconciliation

   Charlie announces BSMs ➔ Alice & Bob announce bases

   Keep bits when BSM successful & bases equal ➔ bit flip

3. Parameter Estimation
4. Privacy Amplification

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

MDI-QKD

Why?

1. Detector Side Channels all removed

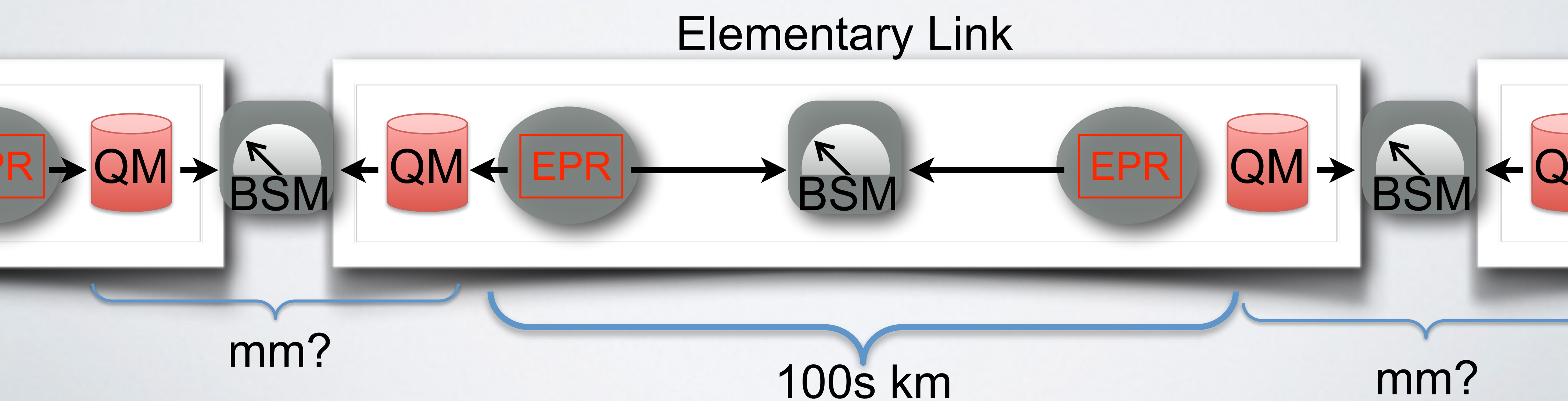
2. Does not require high-efficiency detection

3. Doubles the Distance (as with EPR-QKD)

MDI-QKD

Why?

4. A step towards Quantum Repeaters



MDI-QKD

Why?

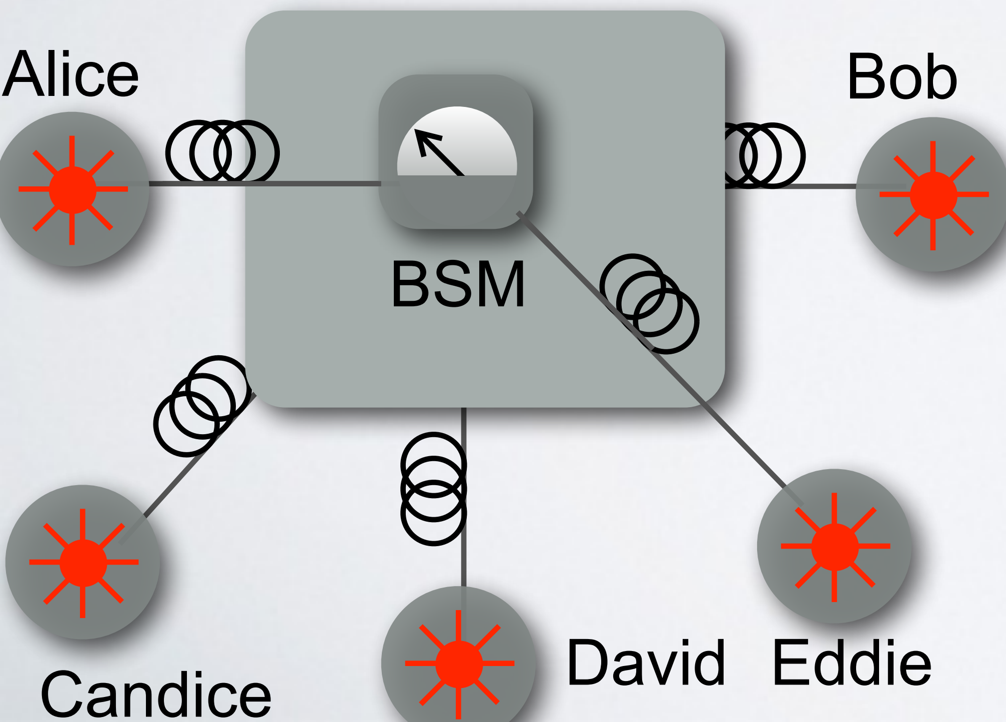
LETTER

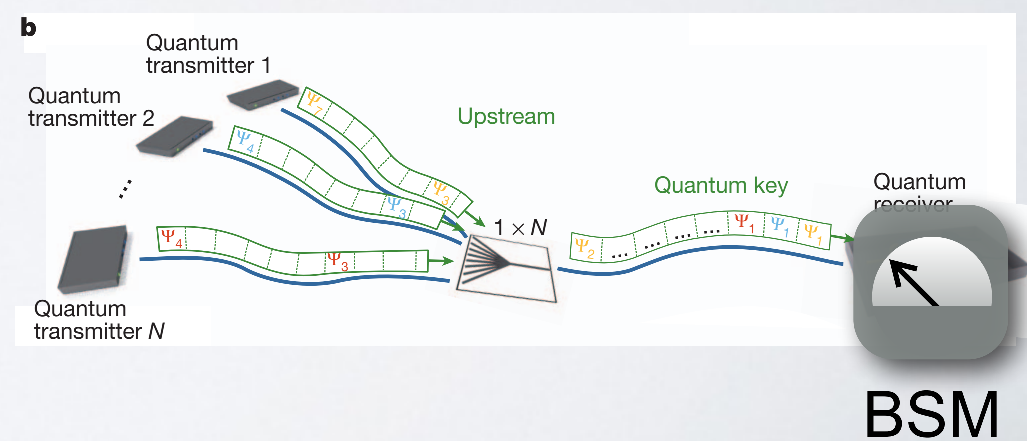
doi:10.1038/nature12493

A quantum access network

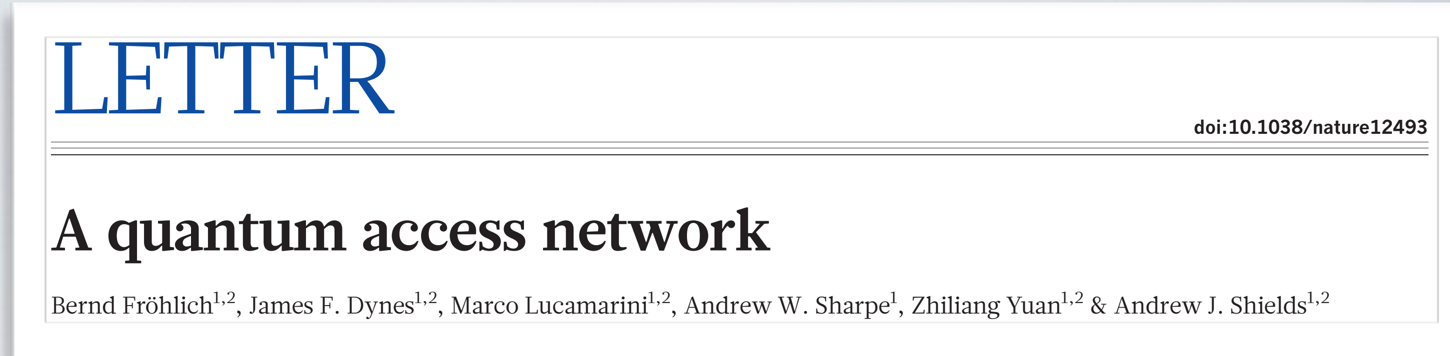
Bernd Fröhlich[1,2], James F. Dynes[1,2], Marco Lucamarini[1,2], Andrew W. Sharpe[1], Zhiliang Yuan[1,2] & Andrew J. Shields[1,2]

5. Networks





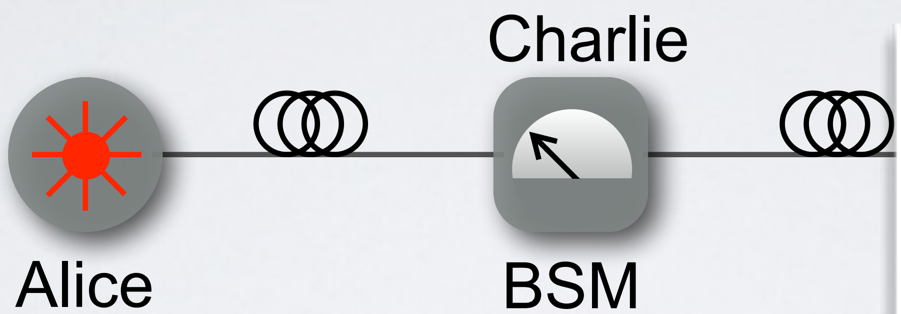
MDI-QKD

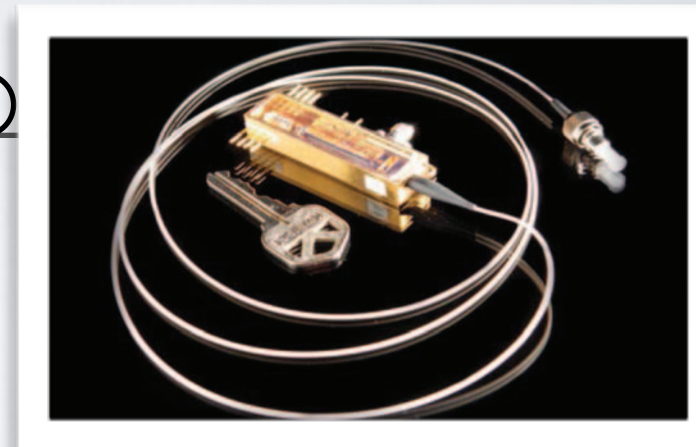

LETTER
doi:10.1038/nature12493

A quantum access network

Bernd Fröhlich[1,2], James F. Dynes[1,2], Marco Lucamarini[1,2], Andrew W. Sharpe[1], Zhiliang Yuan[1,2] & Andrew J. Shields[1,2]

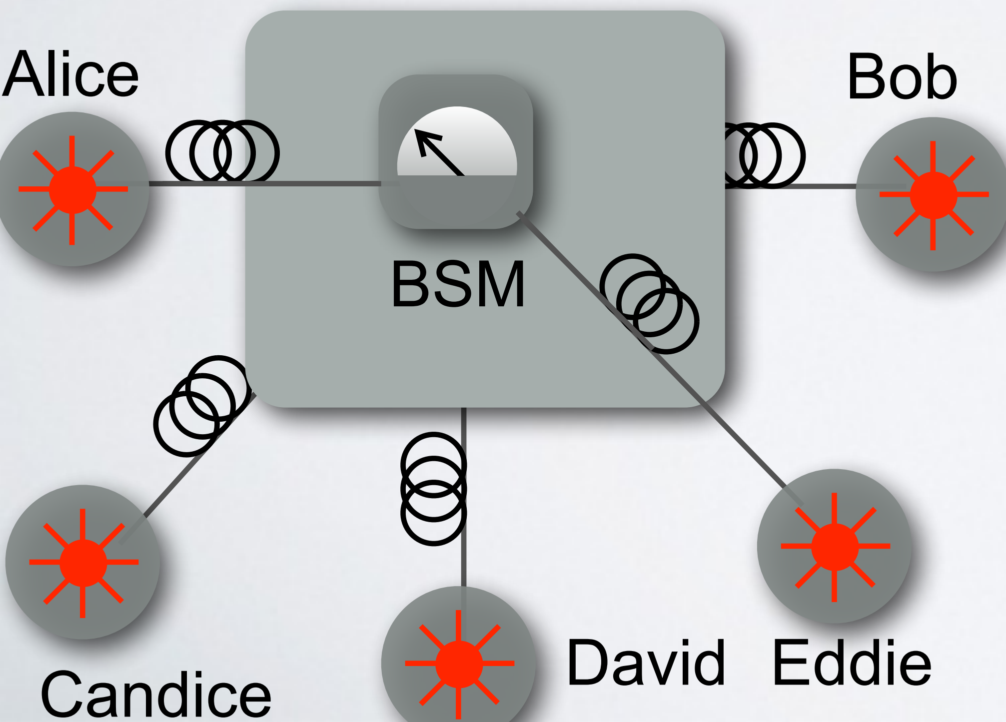
Why?

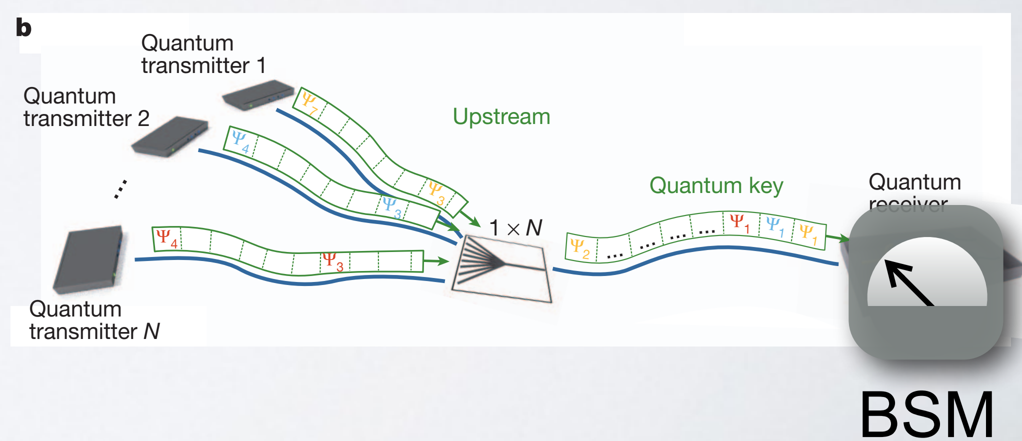




Hughes, 1305.0305

5. Networks





MDI-QKD

Why?

1. Detector Side Channels all removed

2. Does not require high-efficiency detection

3. Potential for Long Distance (as with EPR-QKD)

4. A step towards Quantum Repeaters

5. Untrusted, Quantum Access, Networking

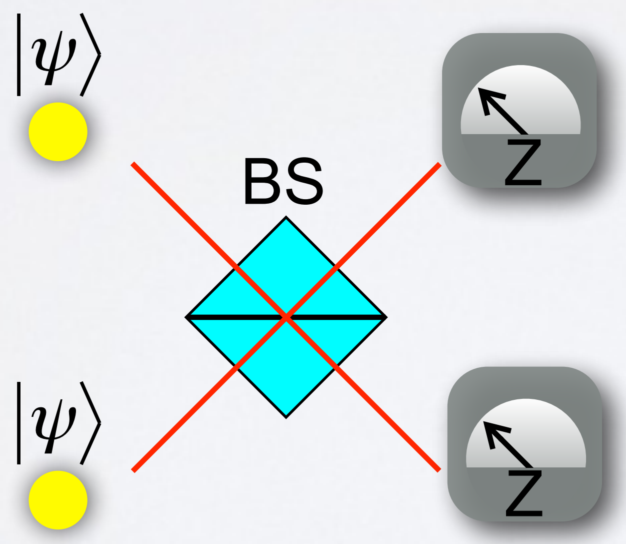
OUTLINE

- Side-Channel Attacks
- Measurement-Device-Independent QKD
- **Experimental Challenges**
- Experiments (part I) - First Generation
- Theoretical Studies
- Alternative Protocols
- Experiments (part II) - Most Recent

CHALLENGES

Bell-State Measurement

with Linear Optics, 50%:



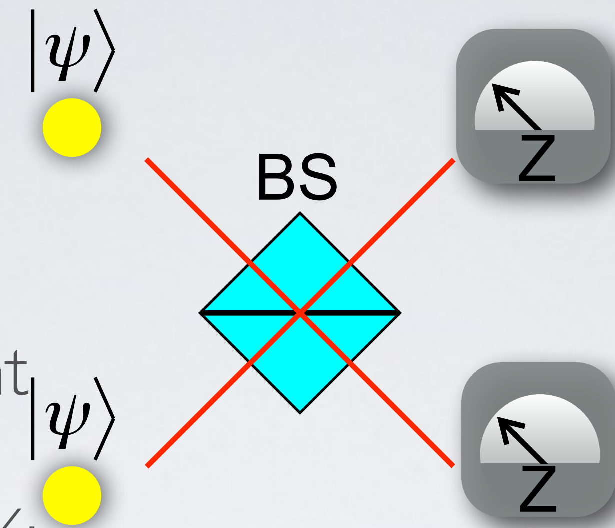
Different Z values:

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

CHALLENGES

Bell-State Measurement

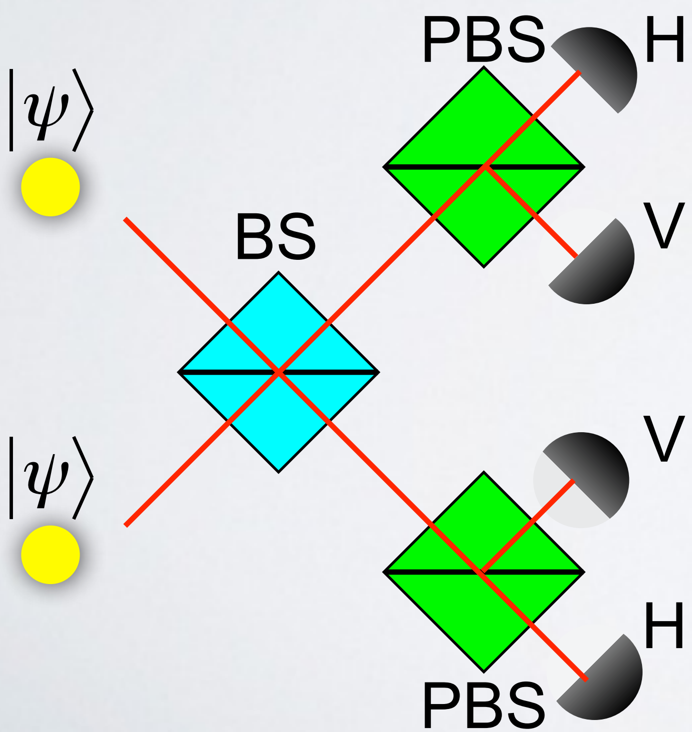
with Linear Optics, 50%:



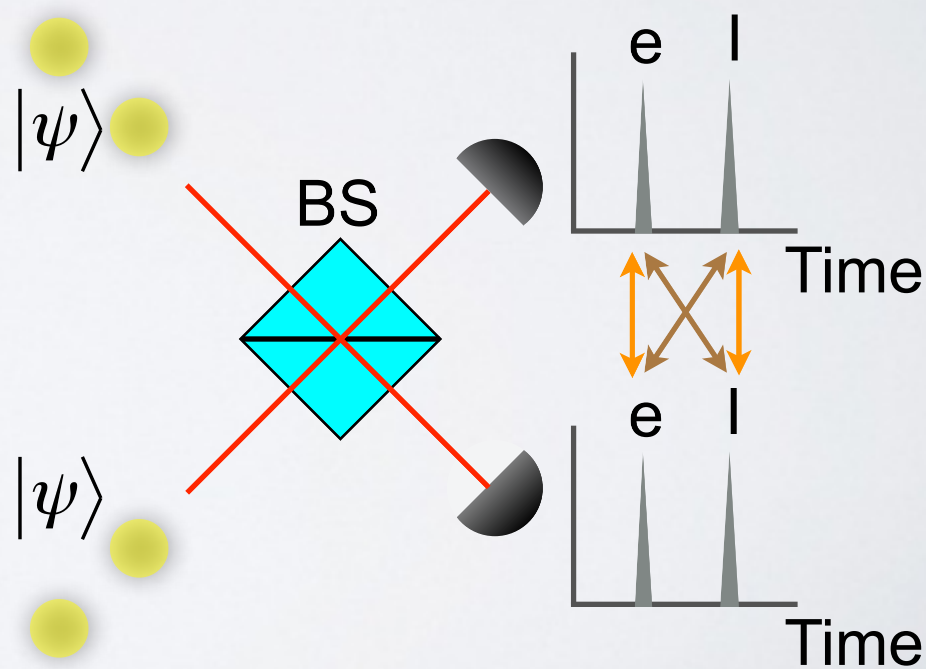
Different Z values:

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

Polarization:



Time-Bin:



H/V Basis - Z Basis

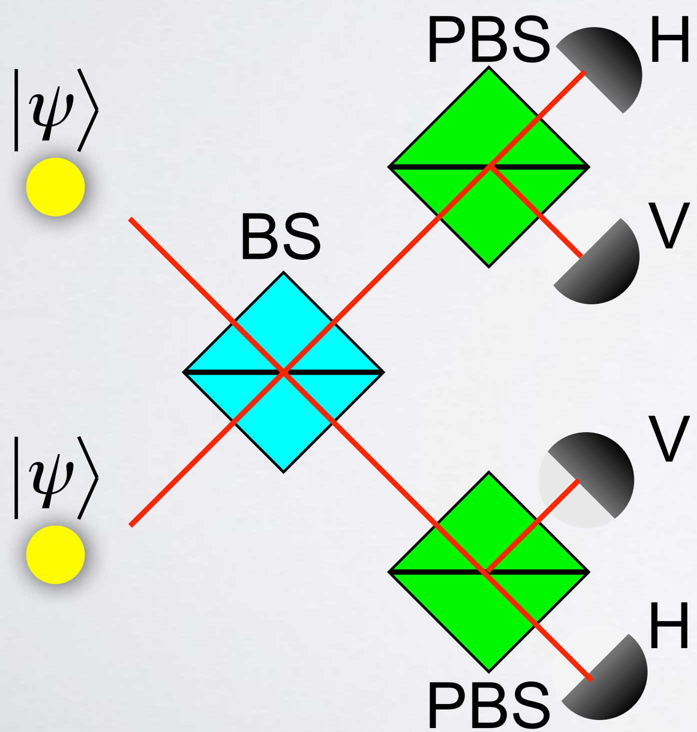
Alice n	State	Bob n	State	P(BSM)

CHALLENGES

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

Poissonian statistics:

$$P(n) = \mu^{n} e^{\mu} / n!$$



H/V Basis - Z Basis

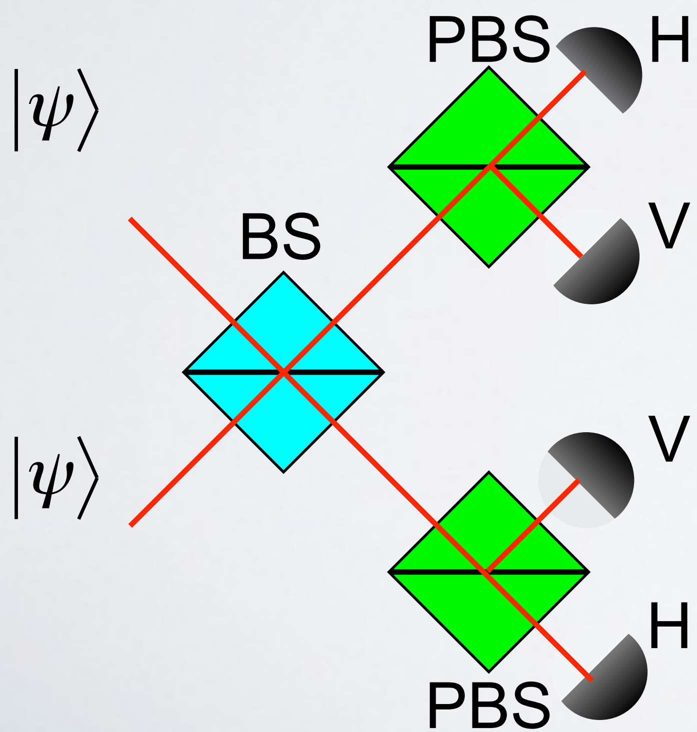
Alice n	State	Bob n	State	P(BSM)
0	—	0	—	0

CHALLENGES

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

Poissonian statistics:

$$P(n) = \mu^n e^{\mu} / n!$$



H/V Basis - Z Basis

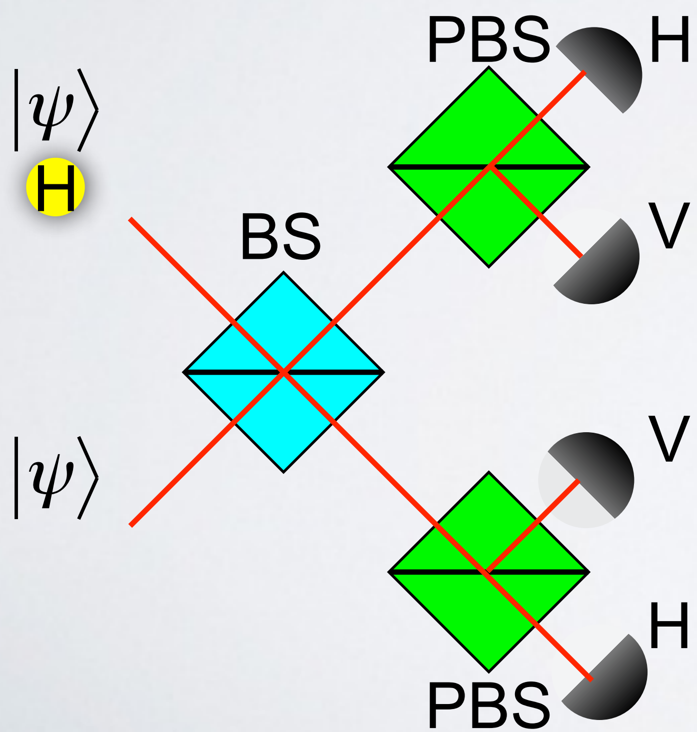
Alice n	State	Bob n	State	P(BSM)
0	—	0	—	0
1	H	0	—	0

CHALLENGES

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

Poissonian statistics:

$$P(n) = \mu^n e^{\mu} / n!$$



CHALLENGES

H/V Basis - Z Basis

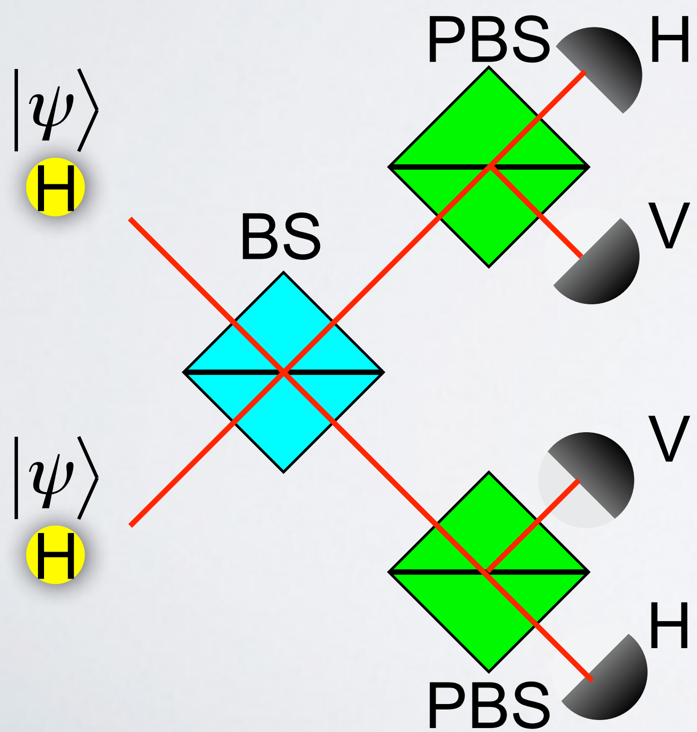
Alice n	State	Bob n	State	P(BSM)
0	—	0	—	0
1	H	0	—	0
1	H	1	H	0

Interference! → (row: 1, H, 1, H, 0)

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

Poissonian statistics:

$$P(n) = \mu^n e^{\mu} / n!$$



H/V Basis - Z Basis

Alice n	State	Bob n	State	P(BSM)
0	—	0	—	0
1	H	0	—	0
1	H	1	H	0
1	H	1	V	1/2

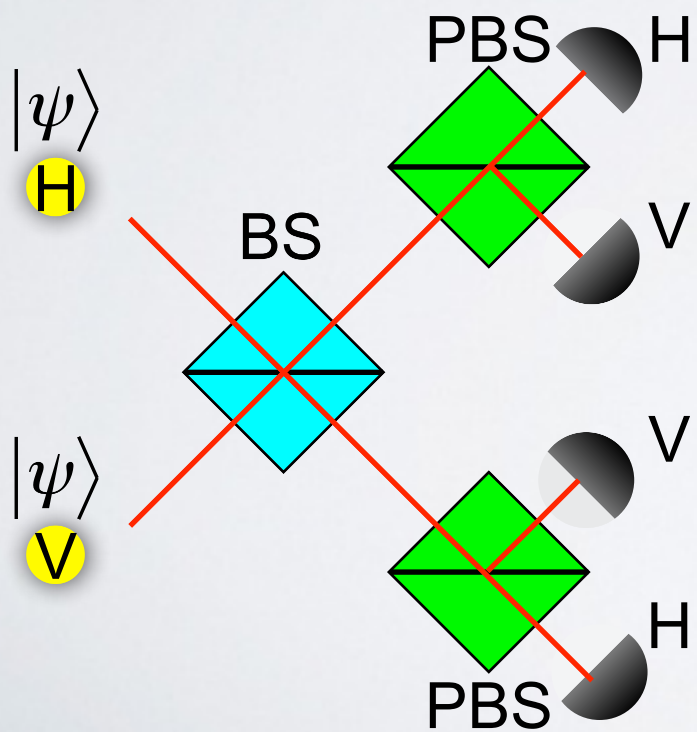
Interference! → (row: 1, H, 1, H)

CHALLENGES

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

Poissonian statistics:

$$P(n) = \mu^n e^{\mu} / n!$$



H/V Basis - Z Basis

Alice n	State	Bob n	State	P(BSM)
0	—	0	—	0
1	H	0	—	0
1	H	1	H	0
1	H	1	V	1/2
2	H	0	—	0

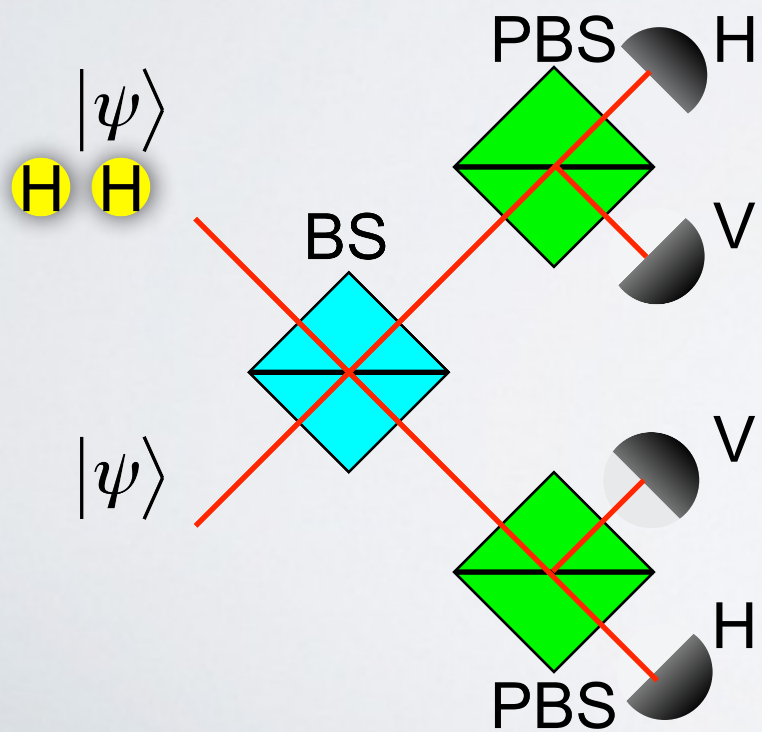
CHALLENGES

Interference! → (row: Alice n = 1, H; Bob n = 1, H)

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

Poissonian statistics:

$$P(n) = \mu^n e^{\mu} / n!$$



CHALLENGES

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

Poissonian statistics:

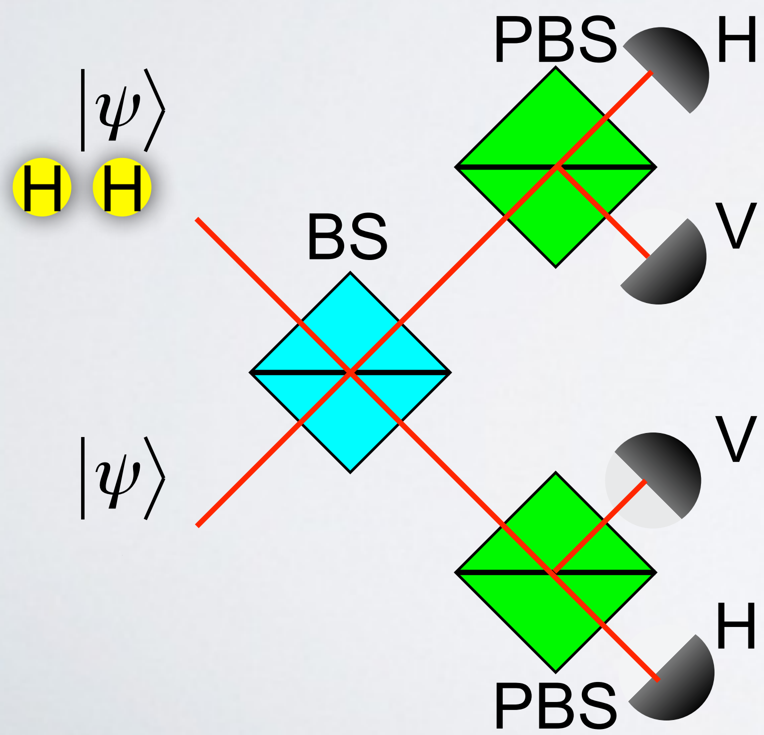
$$P(n) = \mu^n e^{\mu} / n!$$

H/V Basis - Z Basis

Alice n	State	Bob n	State	P(BSM)
0	—	0	—	0
1	H	0	—	0
1	H	1	H	0
1	H	1	V	1/2
2	H	0	—	0

Interference! → (row: 1, H, 1, H, 0)

$$e^Z = 0\%$$

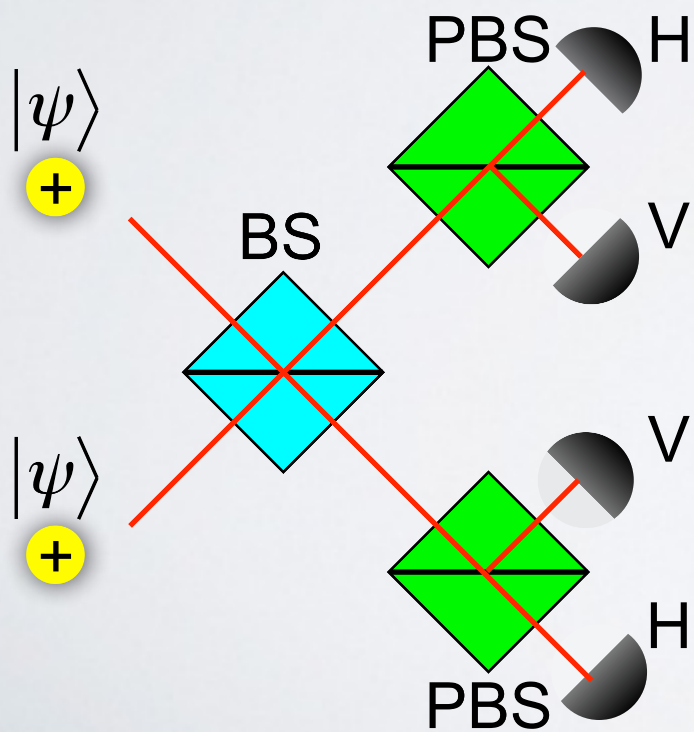


CHALLENGES

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

Poissonian statistics:

$$P(n) = \mu^n e^\mu / n!$$



H/V Basis - Z Basis

Interference! → (row 1, H, 1, H)

Alice n	State	Bob n	State	P(BSM)
0	—	0	—	0
1	H	0	—	0
1	H	1	H	0
1	H	1	V	1/2
2	H	0	—	0

$$e^Z = 0\%$$

+/- Basis - X Basis

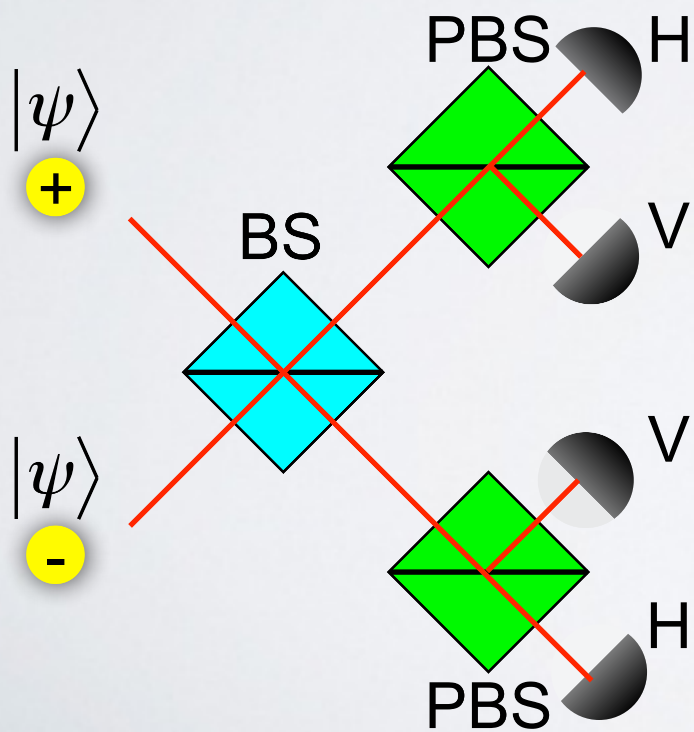
Alice n	State	Bob n	State	P(BSM)
1	Plus	1	Plus	0

CHALLENGES

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

Poissonian statistics:

$$P(n) = \mu^n e^\mu / n!$$



H/V Basis - Z Basis

Alice n	State	Bob n	State	P(BSM)
0	—	0	—	0
1	H	0	—	0
1	H	1	H	0
1	H	1	V	1/2
2	H	0	—	0

Interference! → (row: 1, H, 1, H, 0)

$$e^Z = 0\%$$

+/- Basis - X Basis

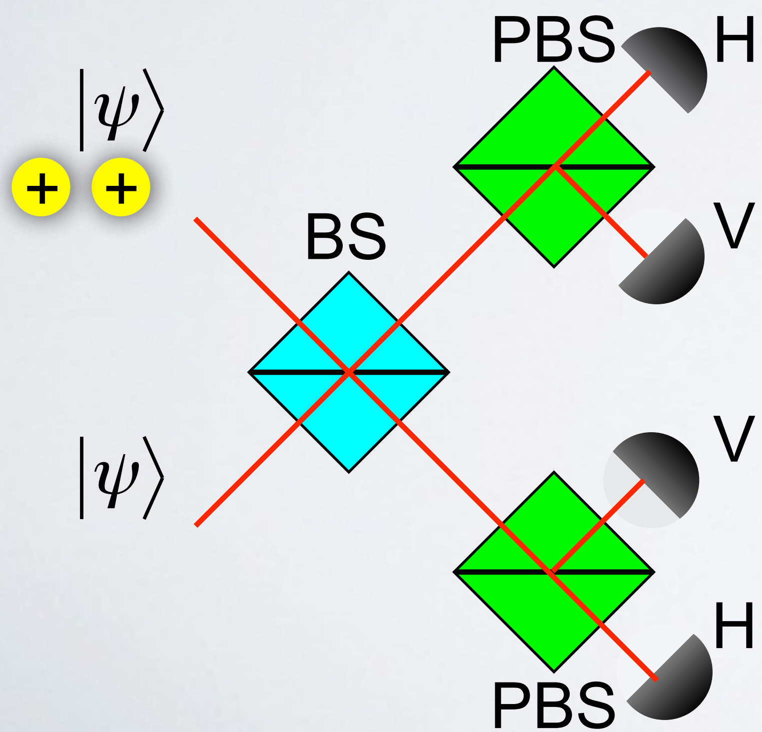
Alice n	State	Bob n	State	P(BSM)
1	Plus	1	Plus	0
1	Plus	1	minus	1/2

CHALLENGES

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

Poissonian statistics:

$$P(n) = \mu^n e^\mu / n!$$



H/V Basis - Z Basis

Interference! → (row 1, H, 1, H)

Alice n	State	Bob n	State	P(BSM)
0	—	0	—	0
1	H	0	—	0
1	H	1	H	0
1	H	1	V	1/2
2	H	0	—	0

$$e^Z = 0\%$$

+/- Basis - X Basis

Alice n	State	Bob n	State	P(BSM)
1	Plus	1	Plus	0
1	Plus	1	minus	1/2
2	Plus	0	—	1/4

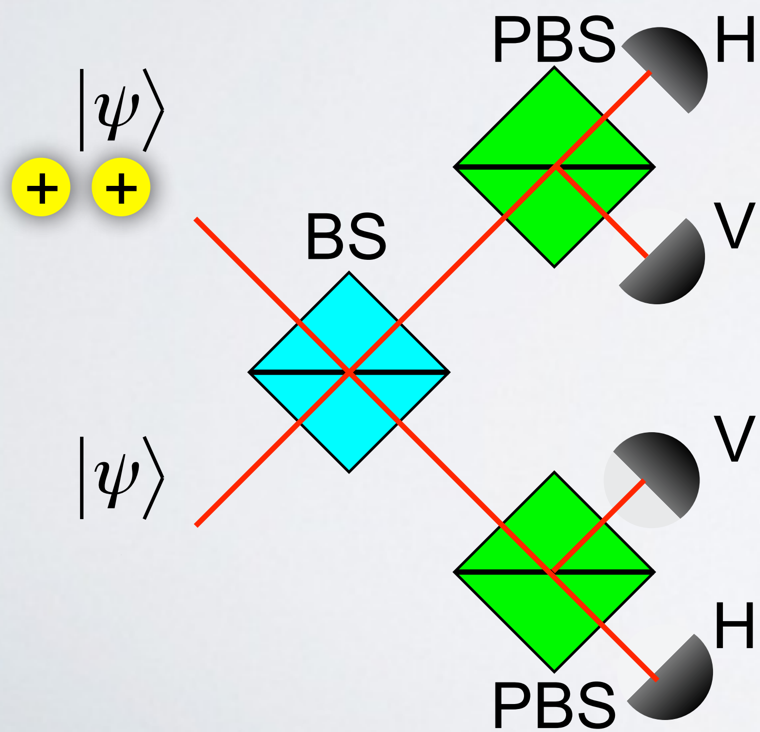
CHALLENGES

Interference! →

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

Poissonian statistics:

$$P(n) = \mu^n e^{\mu} / n!$$



H/V Basis - Z Basis

Alice n	State	Bob n	State	P(BSM)
0	—	0	—	0
1	H	0	—	0
1	H	1	H	0
1	H	1	V	1/2
2	H	0	—	0

$$e^Z = 0\%$$

+/- Basis - X Basis

Alice n	State	Bob n	State	P(BSM)
1	Plus	1	Plus	0
1	Plus	1	minus	1/2
2	Plus	0	—	1/4

$$e^X = 25\%$$

$$e^X_{11} = 0\%$$

$$Q^X = 2Q^Z$$

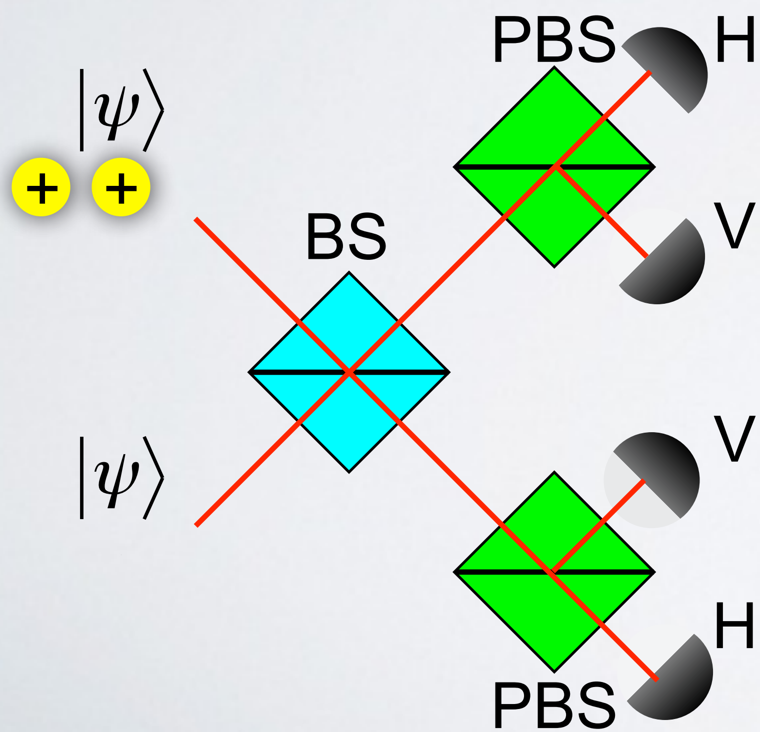
CHALLENGES

Interference! →

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

Poissonian statistics:

$$P(n) = \mu^n e^\mu / n!$$



H/V Basis - Z Basis

Alice n	State	Bob n	State	P(BSM)
0	—	0	—	0
1	H	0	—	0
1	H	1	H	0
1	H	1	V	1/2
2	H	0	—	0

$$e^Z = 0\%$$

+/- Basis - X Basis

Alice n	State	Bob n	State	P(BSM)
1	Plus	1	Plus	0
1	Plus	1	minus	1/2
2	Plus	0	—	1/4

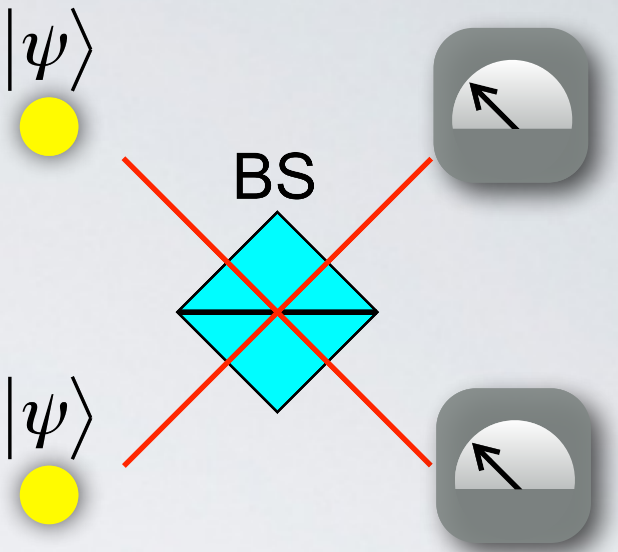
$$e^X = 25\%$$

$$e^X_{11} = 0\%$$

$$Q^X = 2Q^Z$$

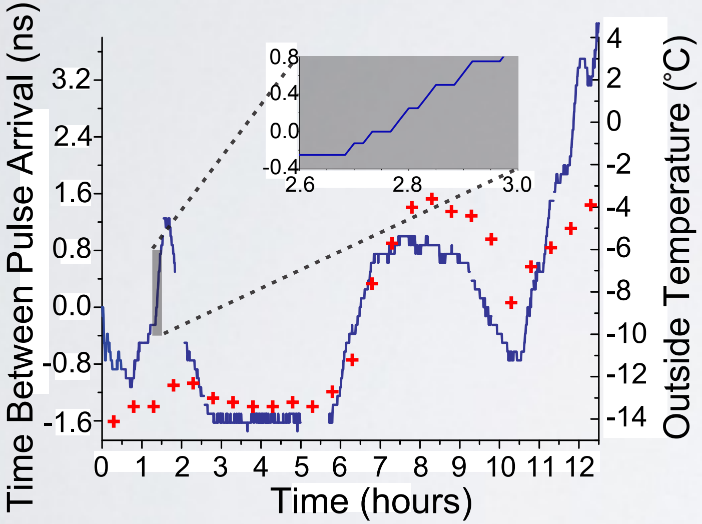
$$S = Q^Z_{11}\left(1 - h_2\left(e^X_{11}\right)\right) - Q^Z_{\mu\mu} f h_2\left(e^Z_{\mu\mu}\right)$$

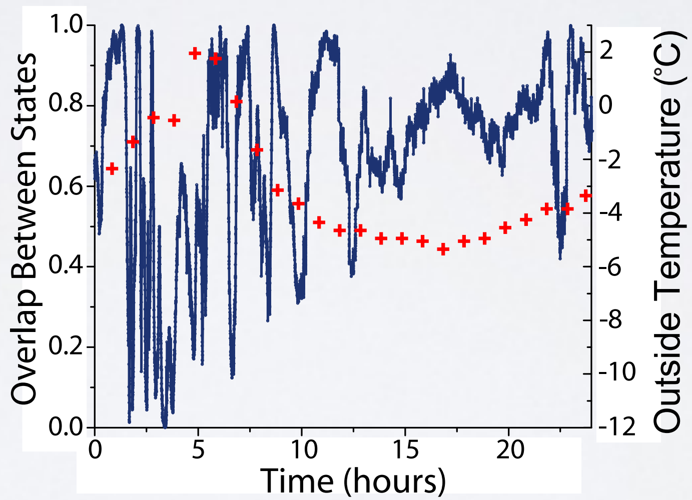
CHALLENGES

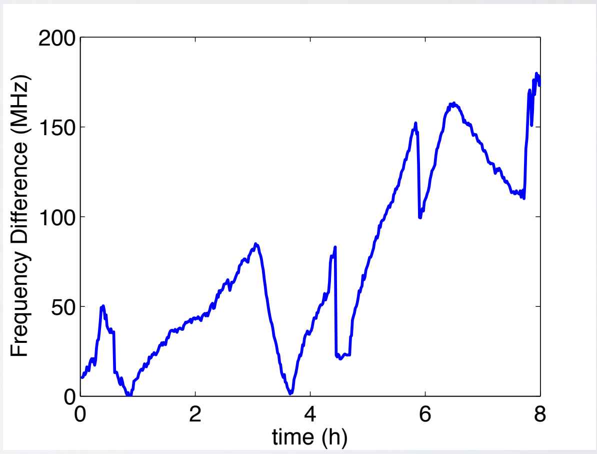


Bell-State Measurement

Maintaining Indistinguishability - Time, Polarization, Frequency

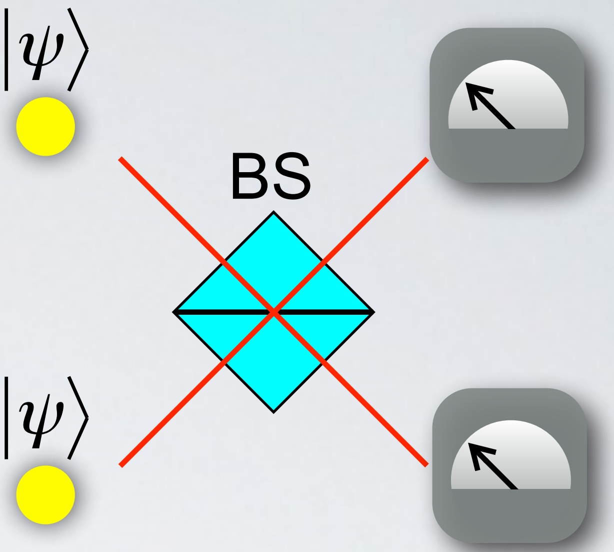






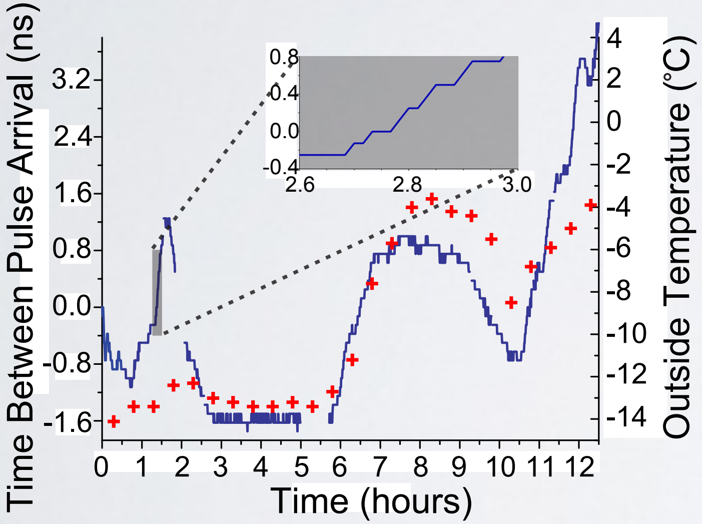
Also, qubit mode: extra polarization, or phase (interferometer)

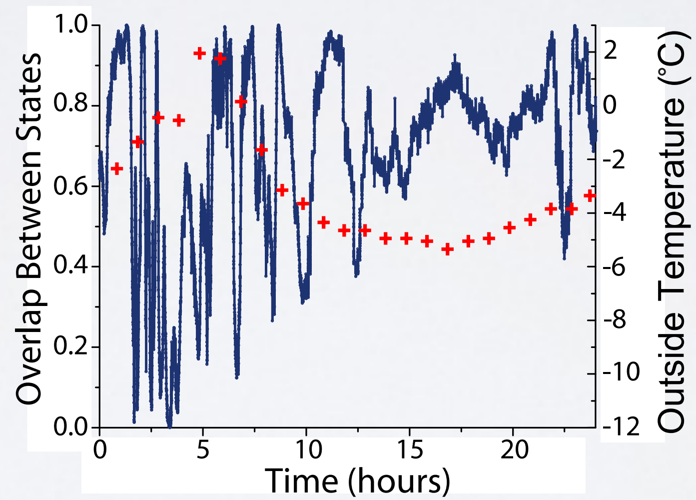
CHALLENGES

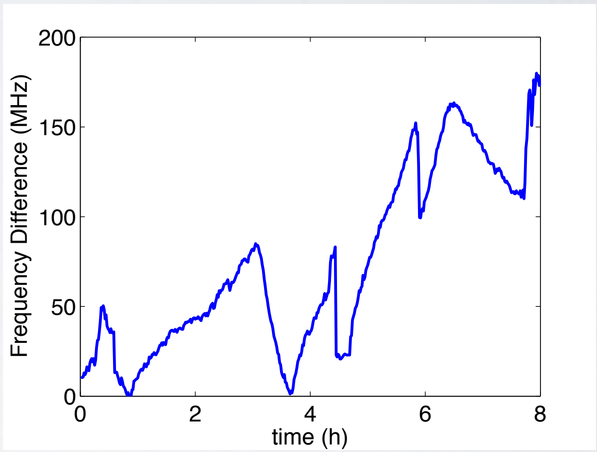


Bell-State Measurement

Maintaining Indistinguishability - Time, Polarization, Frequency







Also, qubit mode: extra polarization, or phase (interferometer)

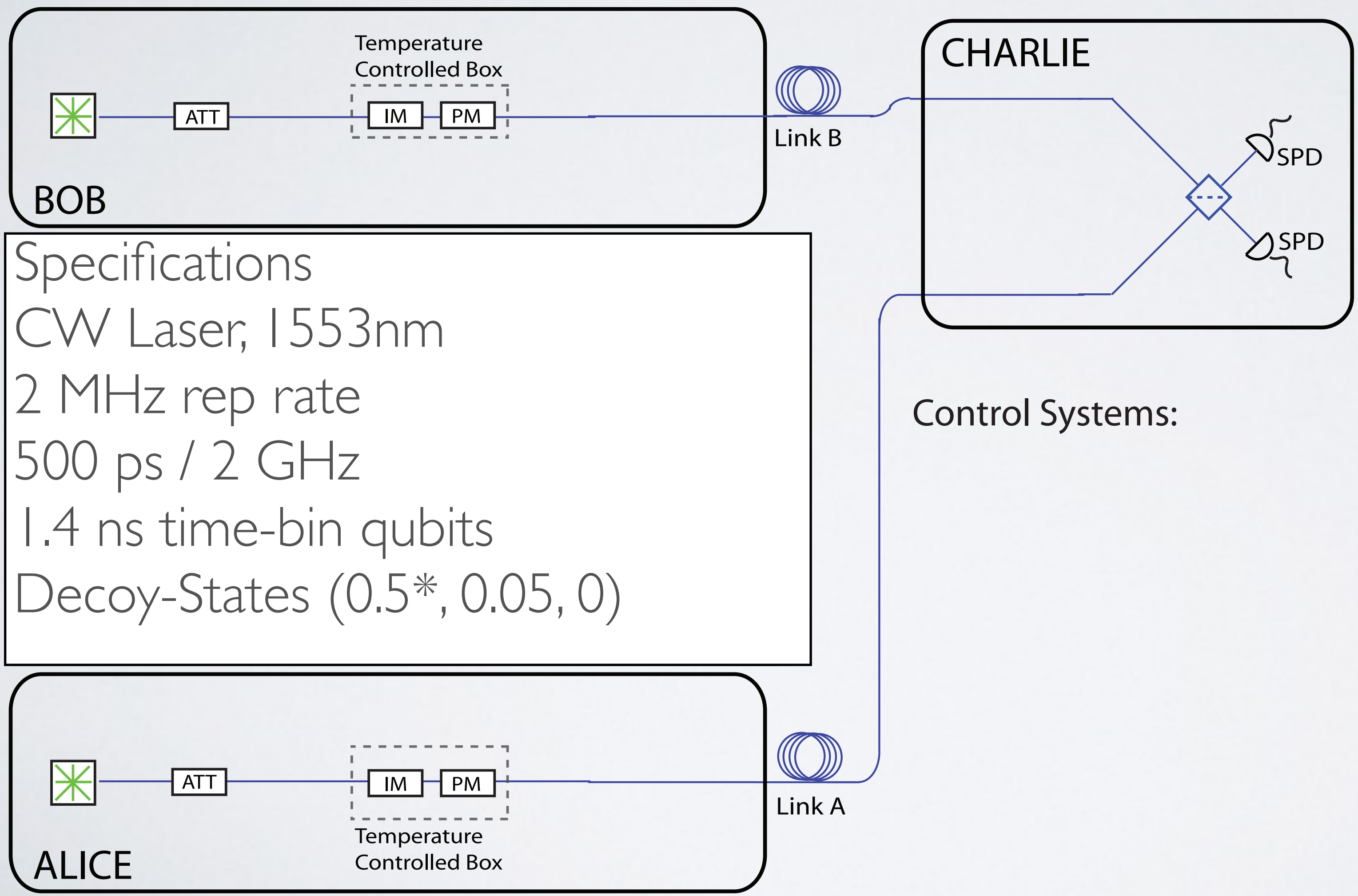
BSM not demonstrated outside the lab (before MDI-QKD)

OUTLINE

- Side-Channel Attacks
- Measurement-Device-Independent QKD
- Experimental Challenges
- **Experiments (part I) - First Generation**
- Theoretical Studies
- Alternative Protocols
- Experiments (part II) - Most Recent

EXPERIMENTS

Calgary, Canada (A. Rubenok, JAS, et al. PRL 111, 130501 (2013))

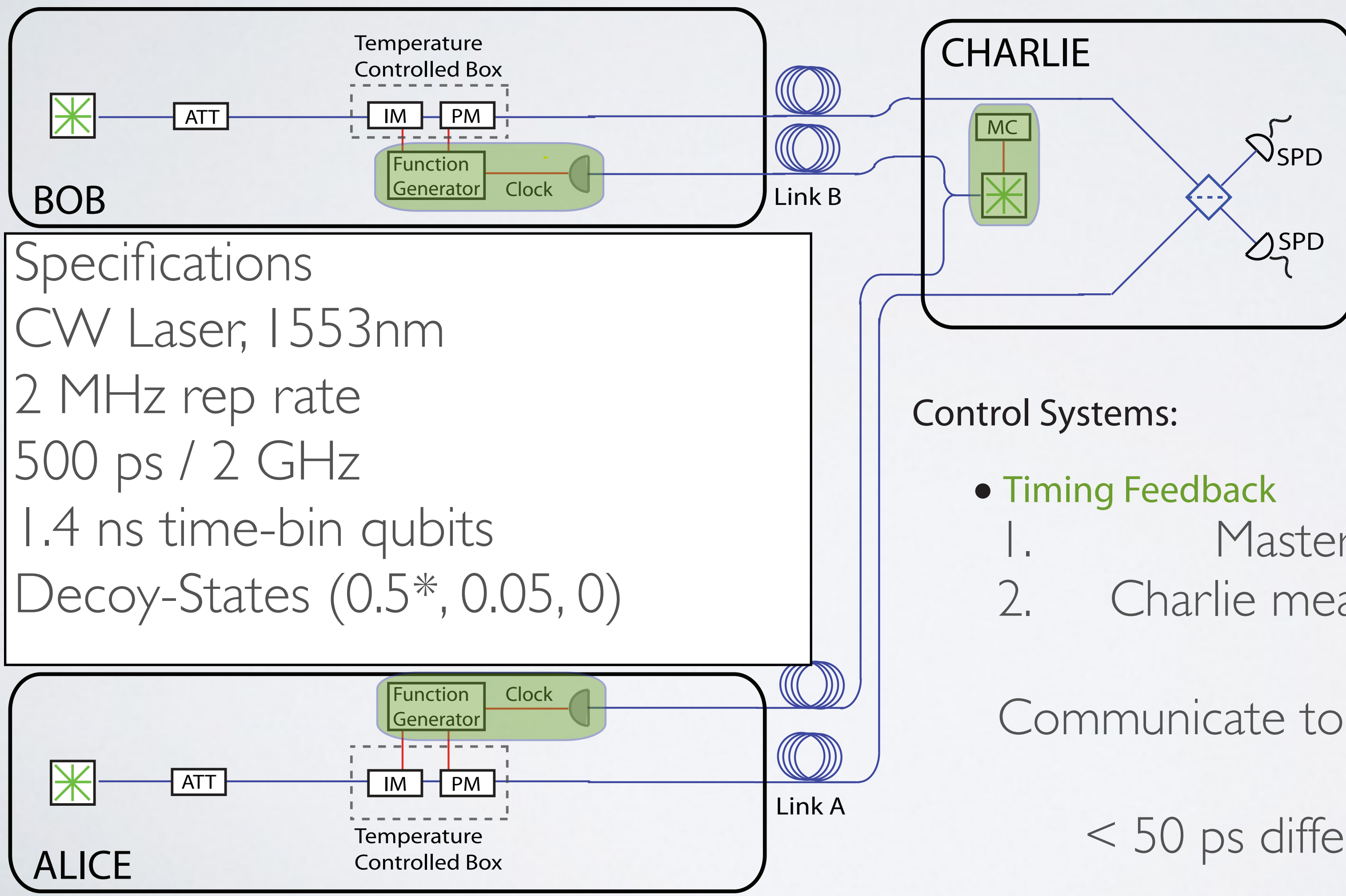


Specifications
CW Laser, 1553nm
2 MHz rep rate
500 ps / 2 GHz
1.4 ns time-bin qubits
Decoy-States (0.5*, 0.05, 0)

Control Systems:

EXPERIMENTS

Calgary, Canada (A. Rubenok, JAS, et al. PRL 111, 130501 (2013))



Specifications
CW Laser, 1553nm
2 MHz rep rate
500 ps / 2 GHz
1.4 ns time-bin qubits
Decoy-States (0.5*, 0.05, 0)

Control Systems:

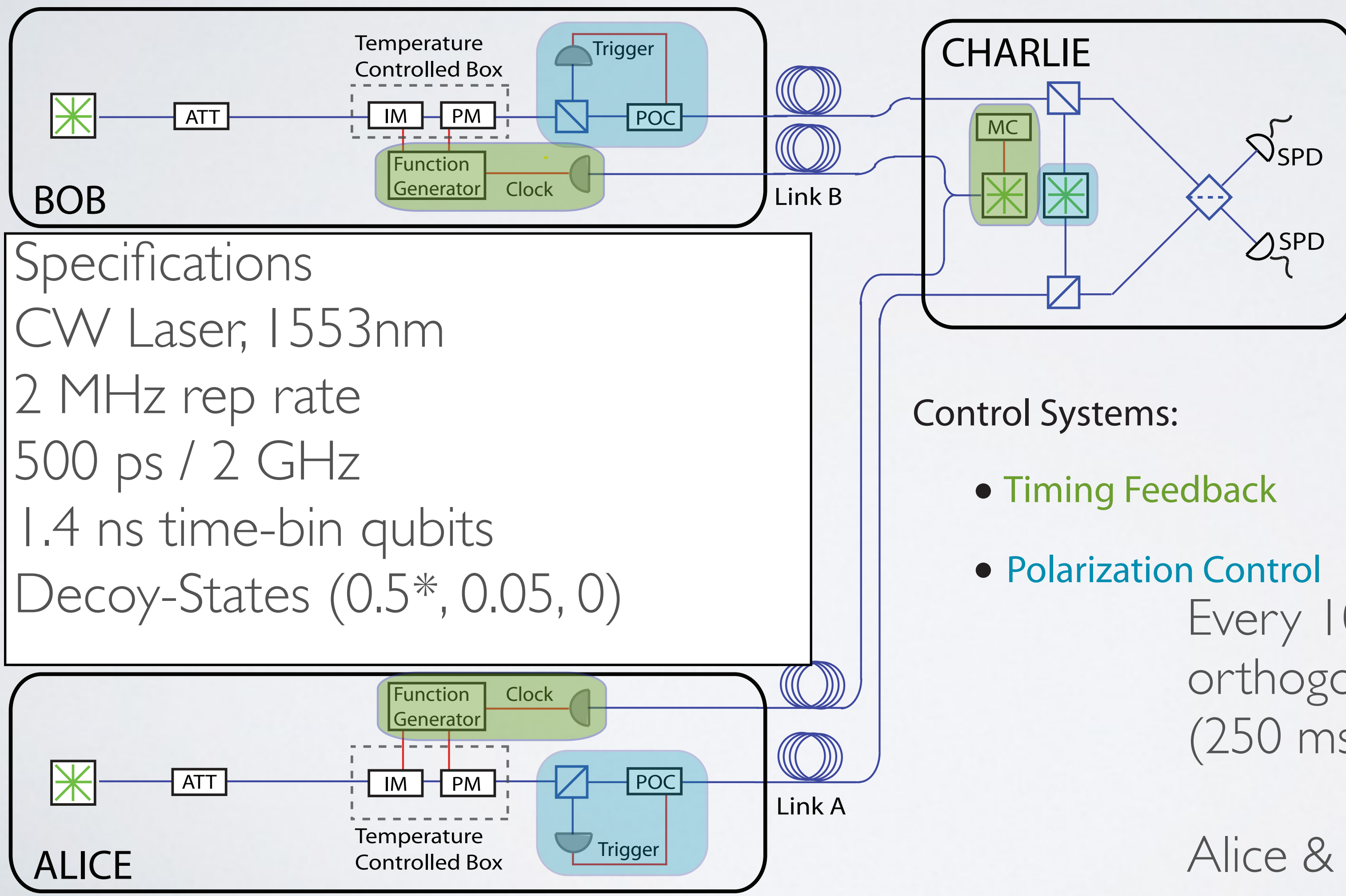
- Timing Feedback
  1. Master Clock
  2. Charlie measured (30s)

Communicate to Alice & Bob

< 50 ps difference

EXPERIMENTS

Calgary, Canada (A. Rubenok, JAS, et al. PRL 111, 130501 (2013))



Specifications
CW Laser, 1553nm
2 MHz rep rate
500 ps / 2 GHz
1.4 ns time-bin qubits
Decoy-States (0.5*, 0.05, 0)

Control Systems:

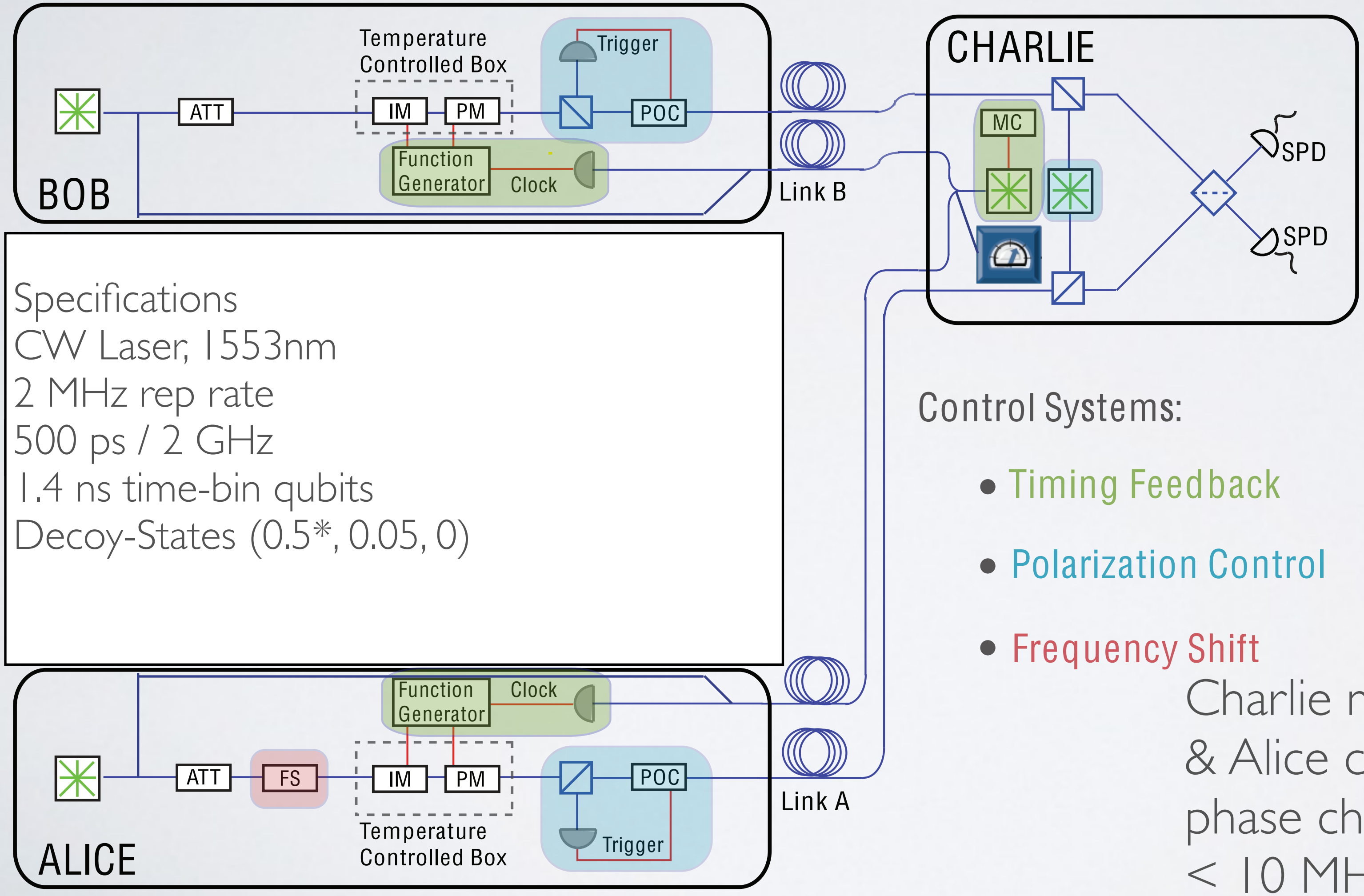
- Timing Feedback
- Polarization Control

Every 10 s, Charlie sends orthogonally polarized light (250 ms)

Alice & Bob compensate

EXPERIMENTS

Calgary, Canada (A. Rubenok, JAS, et al. PRL 111, 130501 (2013))



Specifications
CW Laser, 1553nm
2 MHz rep rate
500 ps / 2 GHz
1.4 ns time-bin qubits
Decoy-States (0.5*, 0.05, 0)

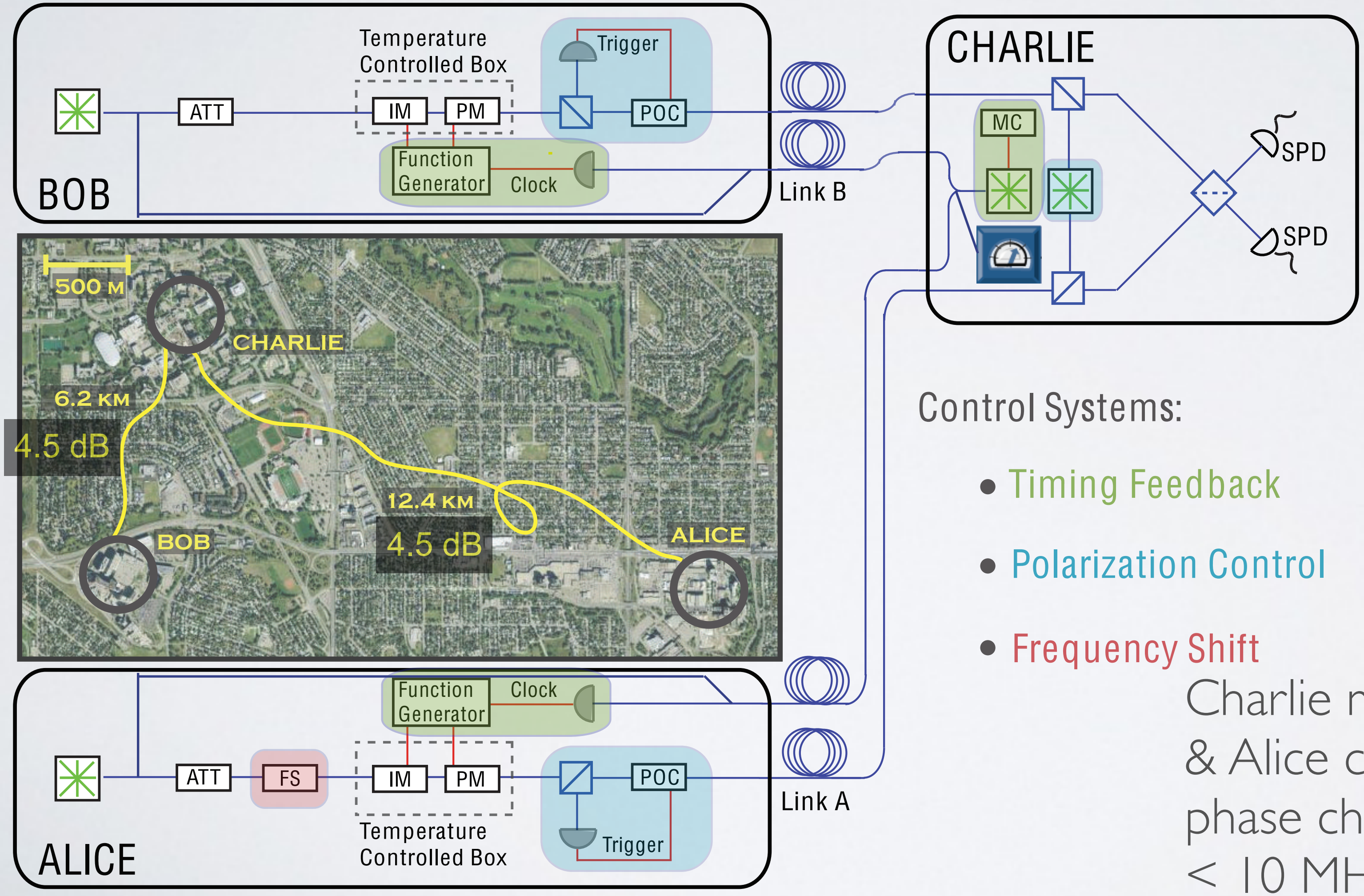
Control Systems:

- Timing Feedback
- Polarization Control
- Frequency Shift

Charlie measured
& Alice corrected with linear phase chirp
< 10 MHz difference

EXPERIMENTS

Calgary, Canada (A. Rubenok, JAS, et al. PRL 111, 130501 (2013))



Control Systems:

- Timing Feedback
- Polarization Control
- Frequency Shift

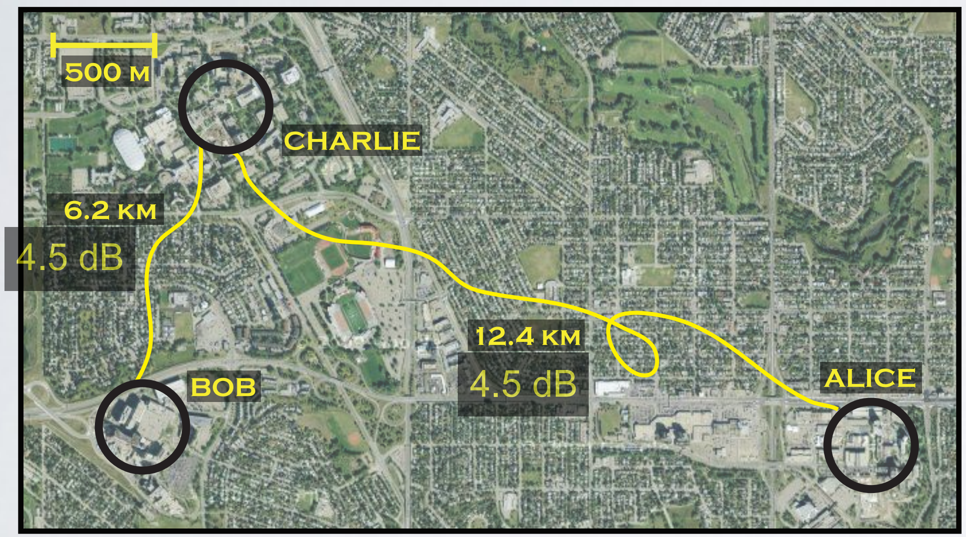
Charlie measured
& Alice corrected with linear phase chirp
< 10 MHz difference

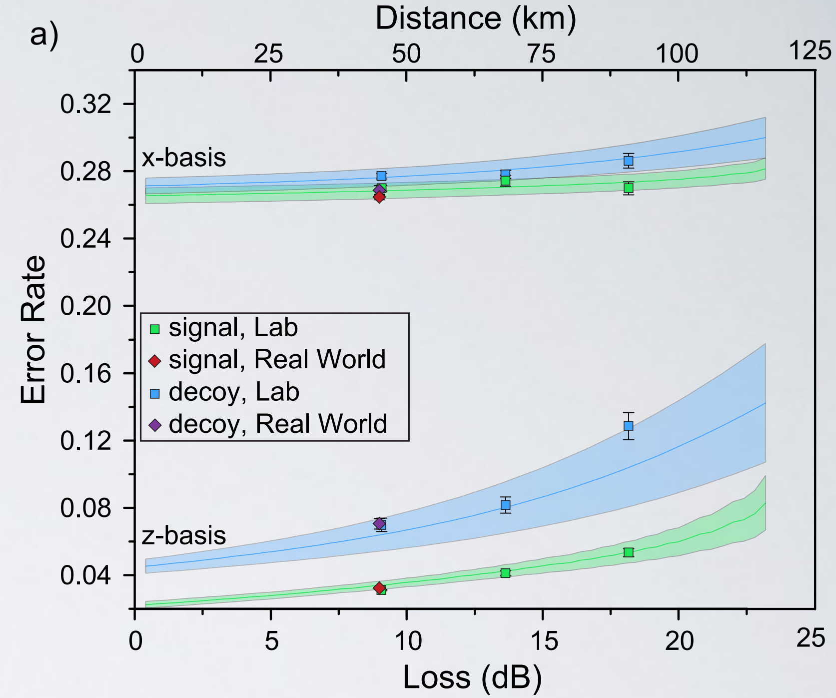
EXPERIMENTS

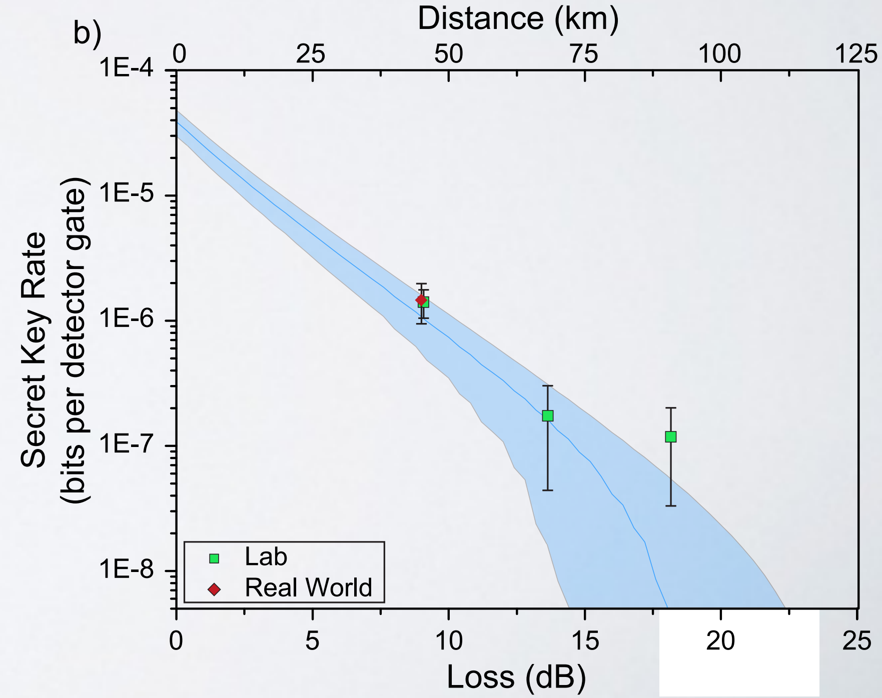
Calgary, Canada

A. Rubenok, JAS, et al. PRL 111, 130501 (2013)

P. Chan, JAS, *et al.* Opt Exp 22, 12716 (2014)





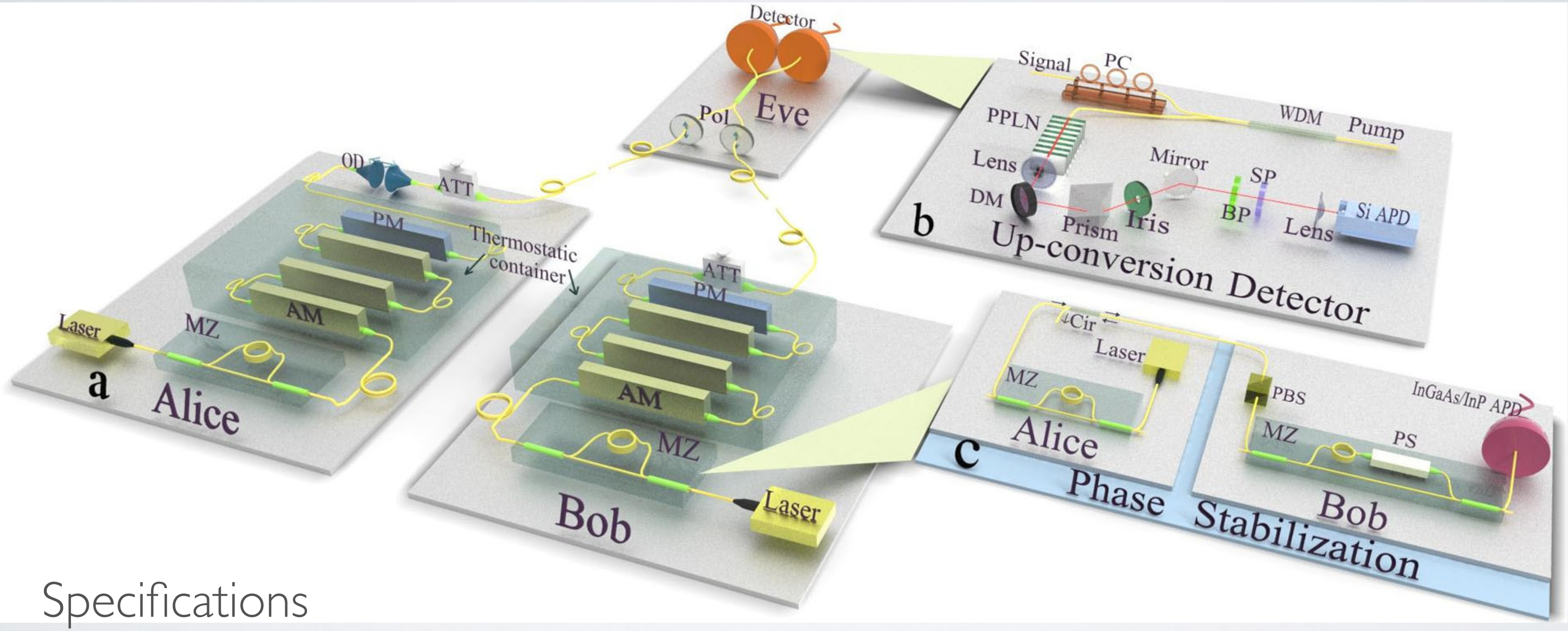


Parameter	Alice's value	Bob's value
$b^{z=0} = b^{z=1}$	$(7.12 \pm 0.98) \times 10^{-3}$	$(1.14 \pm 0.49) \times 10^{-3}$
$b^{x=-} = b^{x=+}$	$(5.45 \pm 0.37) \times 10^{-3}$	$(1.14 \pm 0.49) \times 10^{-3}$
$m^{z=0}$	0.9944 ± 0.0018	0.9967 ± 0.0008
$m^{z=1}$	0	0
$m^{x=+} = m^{x=-}$	0.4972 ± 0.011	0.5018 ± 0.0080
$\phi^{z=0} = \phi^{z=1} = \phi^{x=+}$ [rad]	0	0
$\phi^{x=-}$ [rad]	$\pi + (0.075 \pm 0.015)$	$\pi - (0.075 \pm 0.015)$

$$|\psi\rangle = \sqrt{m^{Z,X} + b^{Z,X}}\,|0\rangle + e^{i\phi_{Z,X}}\sqrt{1 - m^{Z,X} + b^{Z,X}}\,|1\rangle$$

EXPERIMENTS

Hefei, China (Y. Liu, et al. PRL 111, 130502 (2013))



Specifications

Pulsed, 1550 nm

2 ns / 10 pm

85 ns time-bin qubits

Decoy-States (0.5, 0.2, 0.1,0)

0.1 pm frequency precision

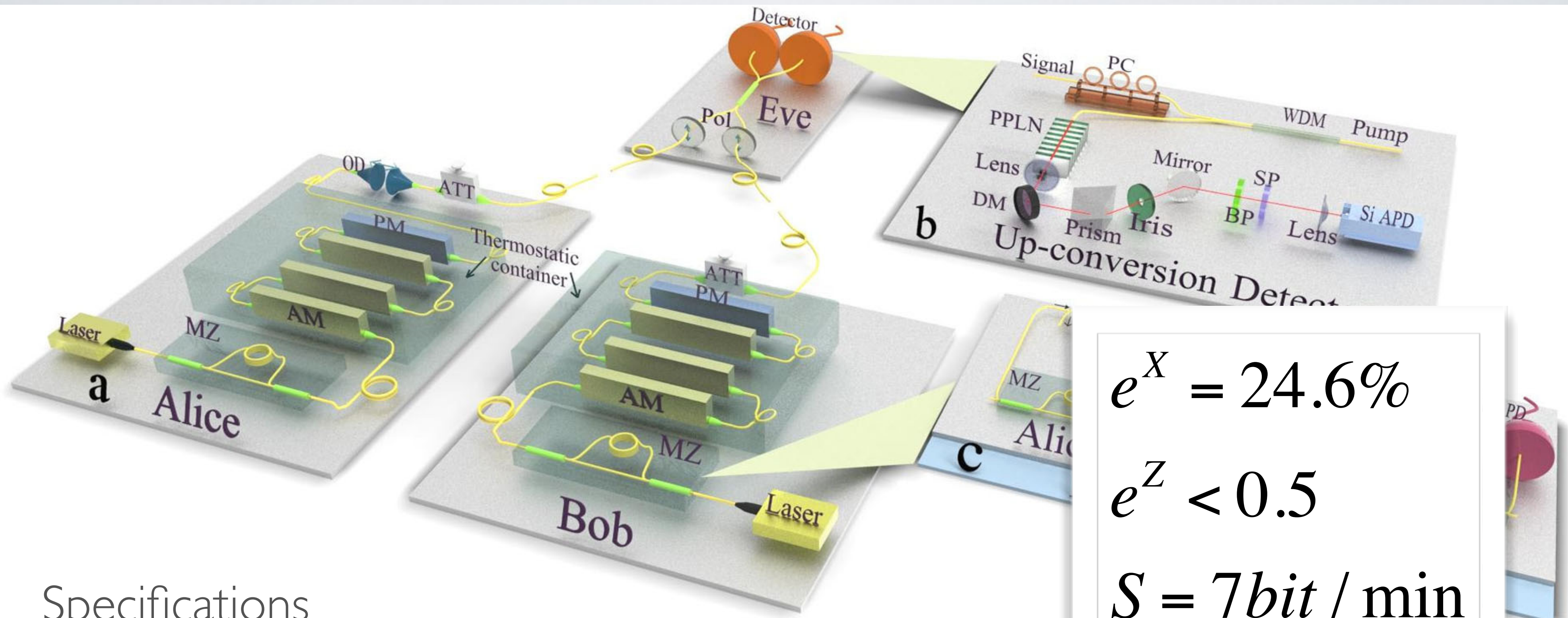
10 ps time precision

Random modulations

Phase-stabilized interferometers

EXPERIMENTS

Hefei, China (Y. Liu, et al. PRL 111, 130502 (2013))



$$e^X = 24.6\%$$
$$e^Z < 0.5$$
$$S = 7bit / \min$$

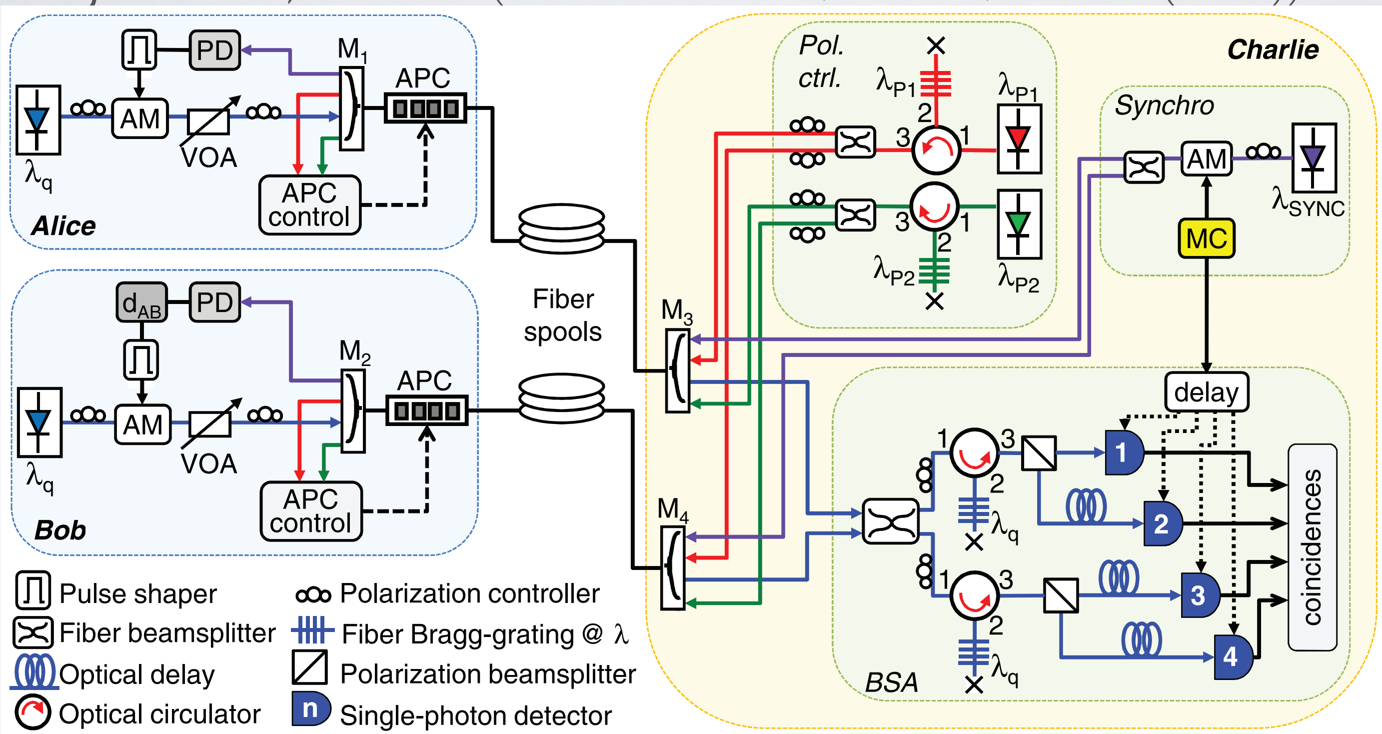
Specifications

Pulsed, 1550 nm
2 ns / 10 pm
85 ns time-bin qubits
Decoy-States (0.5, 0.2, 0.1,0)

0.1 pm frequency precision
10 ps time precision
Random modulations
Phase-stabilized interferometers

EXPERIMENTS

Rio de Janeiro, Brazil (T. F. da Silva et al., PRA 88, 052303 (2013))



Extracted data

$$Q_r^{11} = 6.88\times10^{-6}$$
$$E_d^{11} = 0.018$$
$$Q_{\text{rect}} = 1.36\times10^{-5}$$
$$E_{\text{rect}} = 0.057$$
$$R = 1.04\times10^{-6}$$

Specifications

cw laser, 1546 nm

1.5 ns / 650 MHz

Polarization qubits

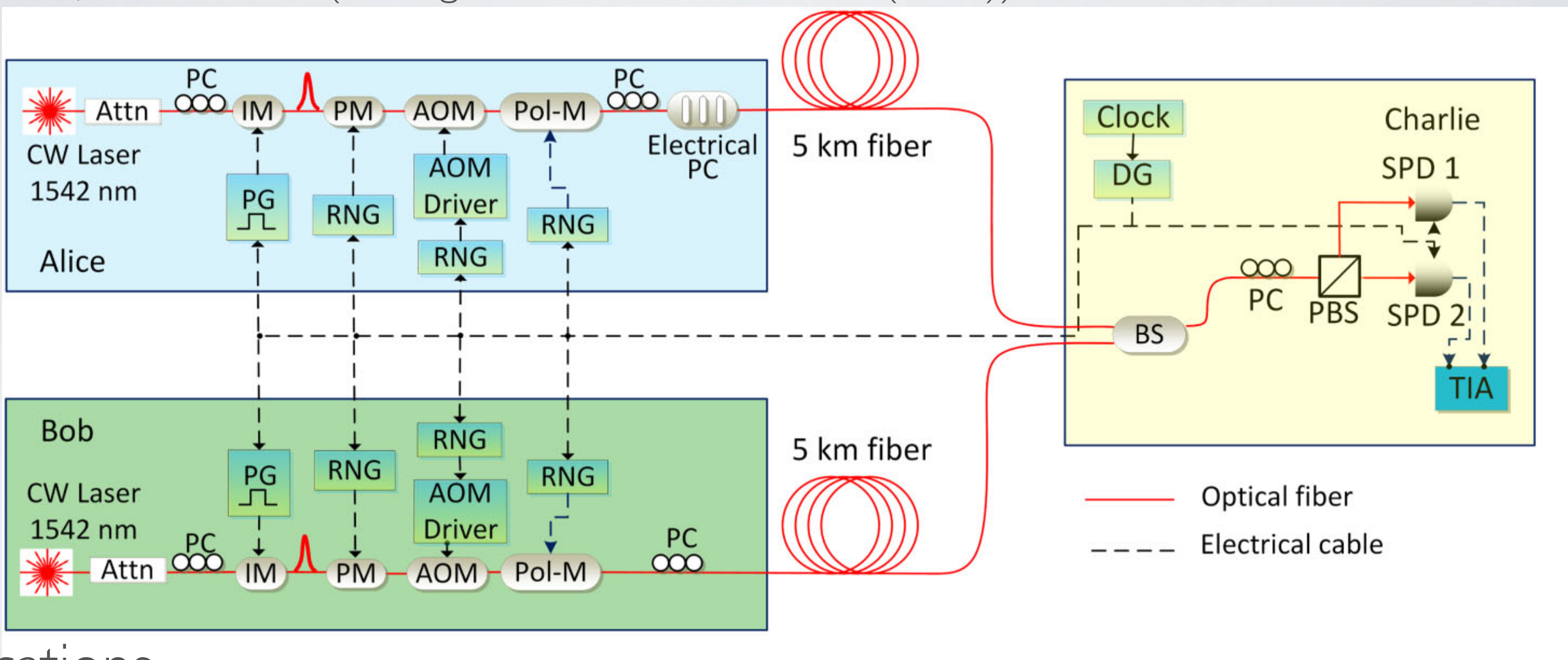
Decoy-States (0.5, 0.1,0)

Rep 1 MHz

Multiplexed - time / polarization sync

EXPERIMENTS

Toronto, Canada (Z. Tang et al., PRL 112, 190503 (2014))



Specifications

cw laser, 1542 nm

Phase randomized states

1.5 ns / 650 MHz

Polarization qubits

Decoy-States (0.3, 0.1,0.01)

$$e^X = 26.2\%$$

$$e^Z = 1.8$$

$$S = 1e^{-8}$$

EXPERIMENTS

	Qubit	Features
Calgary, Canada (A. Rubenok, JAS, et al. PRL 111, 130501 (2013))	time-bin	- real-world deployment - ‘active’ stabilization - optimized intensities
Hefei, China (Y. Liu, et al. PRL 111, 130502 (2013))	time-bin	- random modulation - finite key analysis
Rio de Janeiro, Brazil (T. F. da Silva et al., PRA 88, 052303 (2013))	Polarization	- WDM multiplexed fiber
Toronto, Canada (Z. Tang et al., PRL 112, 190503 (2014))	Polarization	- pre-set random modulation - phase-randomized source - finite key analysis - optimized intensities

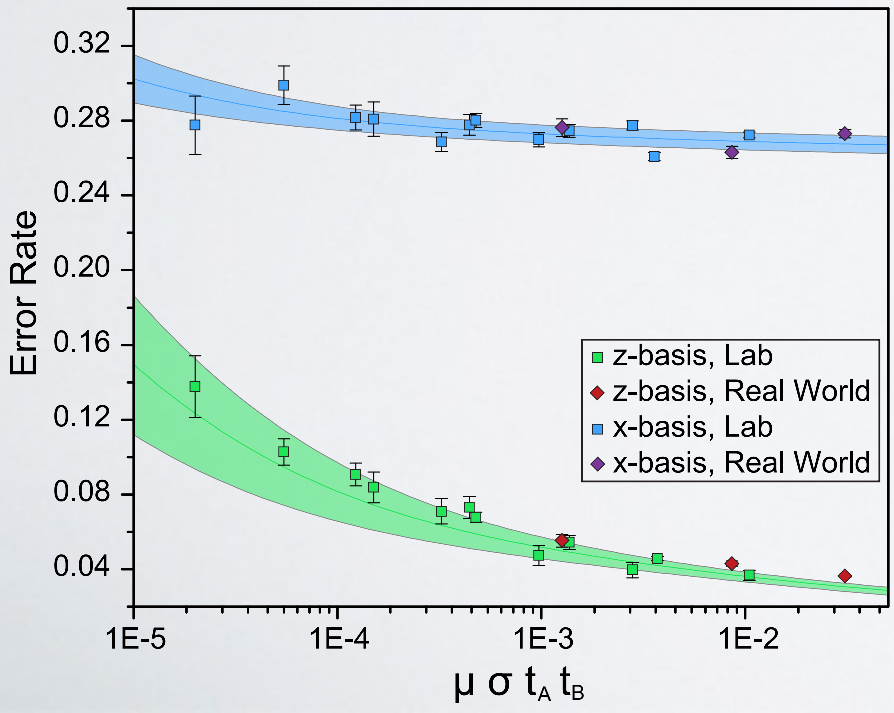
OUTLINE

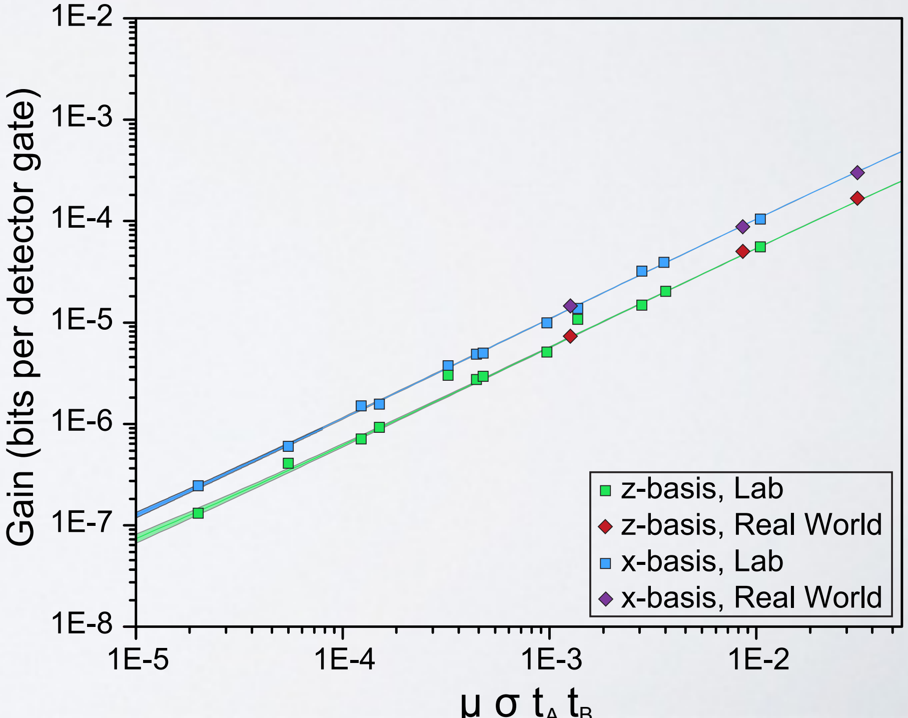
- Side-Channel Attacks
- Measurement-Device-Independent QKD
- Experimental Challenges
- Experiments (part 1) - First Generation
- **Theoretical Studies**
- Alternative Protocols
- Experiments (part II) - Most Recent

THEORETICAL STUDIES OF MDI-QKD

1) Adapted to Experimental Systems (P. Chan, JAS, *et al.* Opt Exp 22, 12716)

$$|\psi\rangle = \sqrt{m^{Z,X} + b^{Z,X}}\,|0\rangle + e^{i\phi_{Z,X}}\sqrt{1 - m^{Z,X} + b^{Z,X}}\,|1\rangle$$

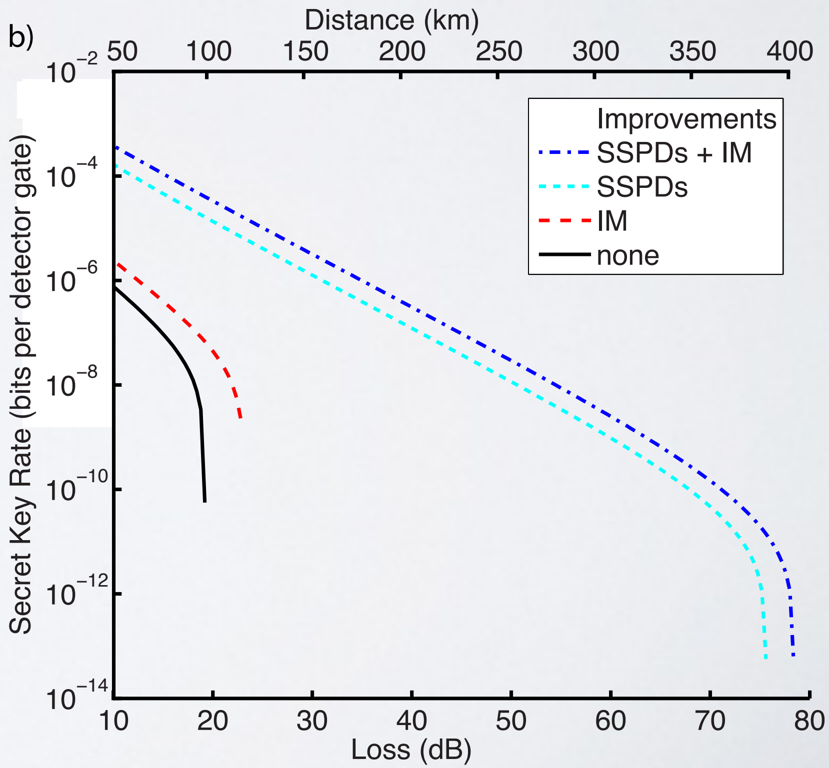




THEORETICAL STUDIES OF MDI-QKD

1) Adapted to Experimental Systems (P. Chan, JAS, *et al.* Opt Exp 22, 12716)

$$|\psi\rangle = \sqrt{m^{Z,X} + b^{Z,X}}\,|0\rangle + e^{i\phi_{Z,X}}\sqrt{1 - m^{Z,X} + b^{Z,X}}\,|1\rangle$$



Examination of "rate-limiting components"

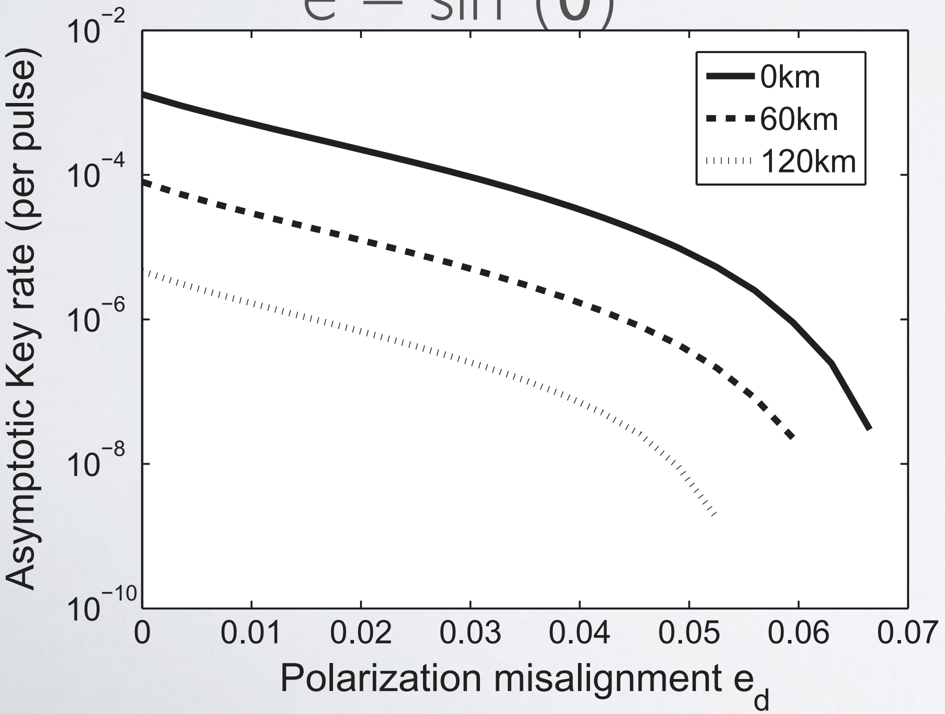
Lab-Standard vrs. State-of-the-Art

THEORETICAL STUDIES OF MDI-QKD

2) Examination of Imperfections Impact (F. Xu *et al.* NJP 15, 113007)

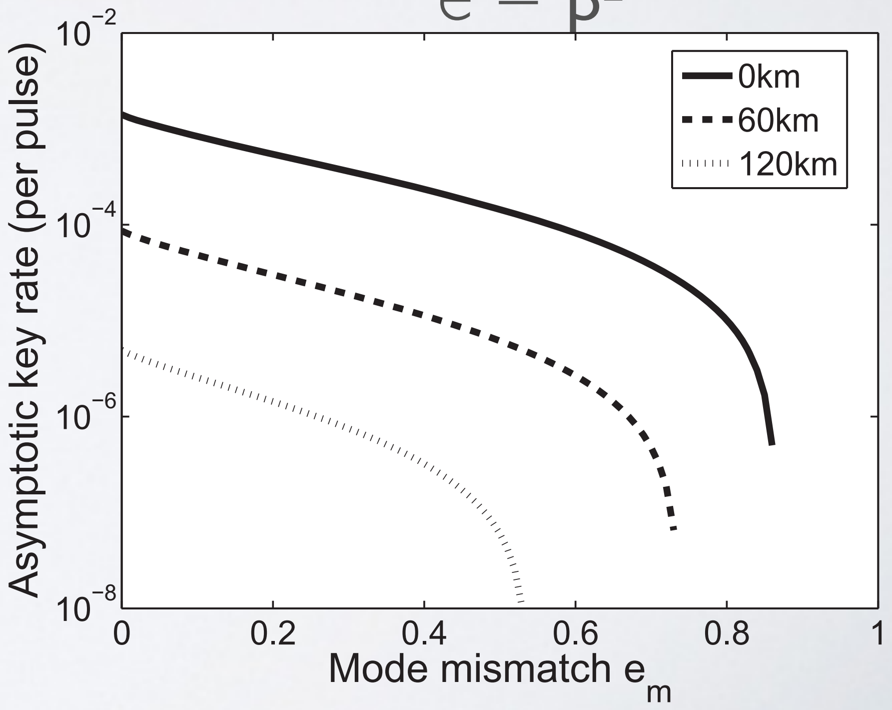
State mis-alignment

$e = \sin^2(\theta)$



Mode mis-alignment

$e = \beta^2$



THEORETICAL STUDIES OF MDI-QKD

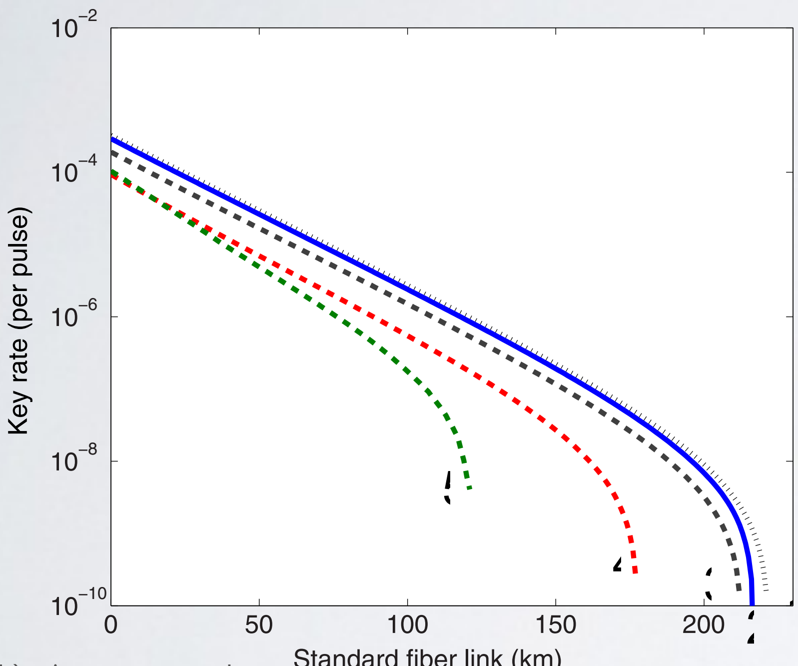
1) Examination of Rate-Limiting Devices (P. Chan, JAS, *et al.* Opt Exp 22, 12716)
2) Examination of Imperfections Impact (F. Xu *et al.* NJP 15, 113007)
3) Examination of Photon Number Distribution (Wang & Wang Sci. Rep. 04612)

Major Impact:
Efficient Detection

Other Minor Impacts
State preparation
Favourable number distributions

THEORETICAL STUDIES OF MDI-QKD

Decoy-State Analyses & Finite-Key



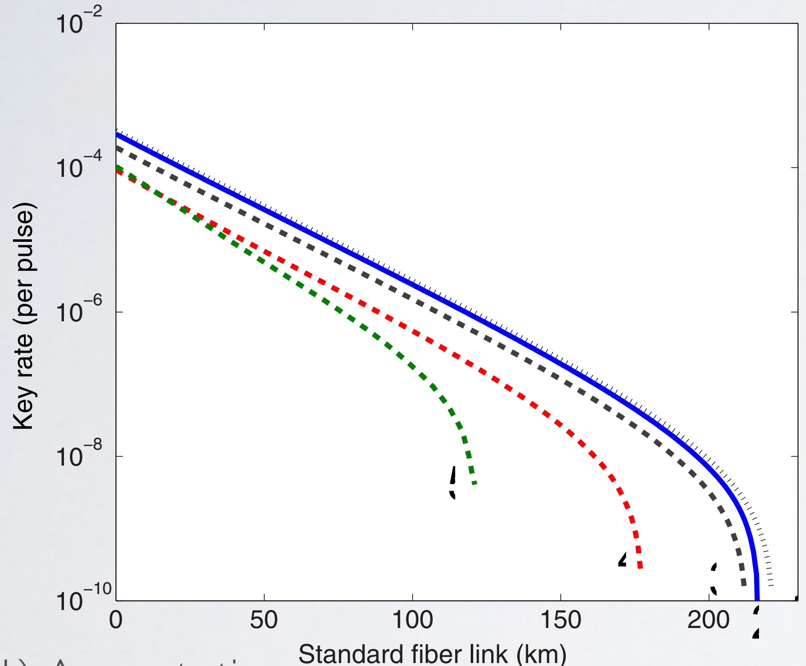
1) Asymptotic
2) F. Xu et al, PRA 052333 (2014), optimized
3) S.-H. Sun et al, PRA 052329 (2013), optimized
4) Z.-W. Yu et al, arxiv:1309:5886,
5) X. Ma et al, PRA 052305 (2012), numeric
6) P. Chan, JAS, et al, Opt Exp (2014), optimization of Wang PRA 012320 (2012)

Optimization:

Step 1 - intensities:
2 (blue) - 2 decoys
(0.0005, 0.01, 0.25)
@ 50 km

THEORETICAL STUDIES OF MDI-QKD

Decoy-State Analyses & Finite-Key



1) Asymptotic
2) F. Xu et al, PRA 052333 (2014), optimized
3) S.-H. Sun et al, PRA 052329 (2013), optimized
4) Z.-W. Yu et al, arxiv:1309:5886,
5) X. Ma et al, PRA 052305 (2012), numeric
6) P. Chan, JAS, et al, Opt Exp (2014), optimization of Wang PRA 012320 (2012)

Optimization:

Step 1 - intensities:
2 (blue) - 2 decoys
(0.0005, 0.01, 0.25)
@ 50 km

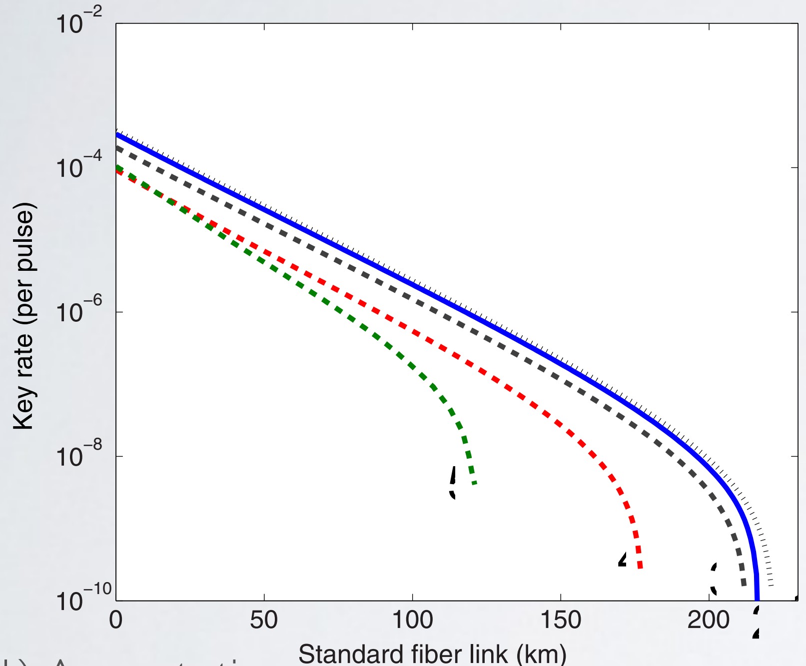
Step 2 - Ratios:

$P_{signal} = 0.58$
$P_{decoy} = 0.30$
$P_{vacuum} = 0.12$

$P_{X|signal} = 0.03$
$P_{X|decoy} = 0.71$
$P_{X|vaccum} = 0.83$

THEORETICAL STUDIES OF MDI-QKD

Decoy-State Analyses & Finite-Key



1) Asymptotic
2) F. Xu et al, PRA 052333 (2014), optimized
3) S.-H. Sun et al, PRA 052329 (2013), optimized
4) Z.-W. Yu et al, arxiv:1309:5886,
5) X. Ma et al, PRA 052305 (2012), numeric
6) P. Chan, JAS, et al, Opt Exp (2014), optimization of Wang PRA 012320 (2012)

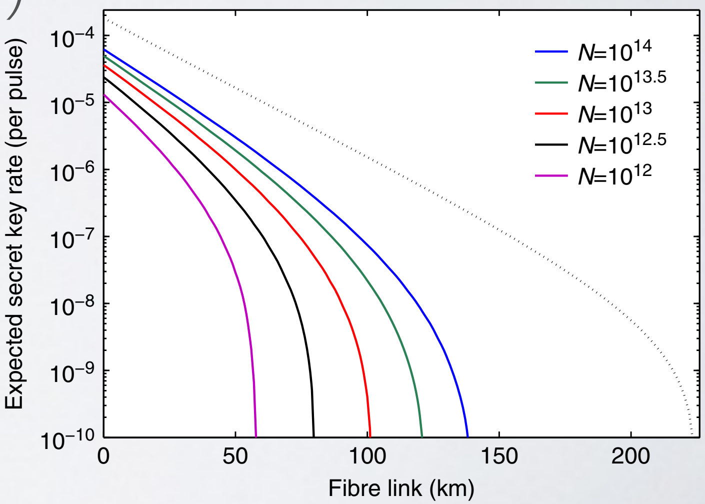
Optimization:

Step 1 - intensities:
2 (blue) - 2 decoys
(0.0005, 0.01, 0.25)
@ 50 km

Step 2 - Ratios:

$P_{signal} = 0.58$
$P_{decoy} = 0.30$
$P_{vacuum} = 0.12$

$P_{X|signal} = 0.03$
$P_{X|decoy} = 0.71$
$P_{X|vaccum} = 0.83$



M. Curty et al Nat. Comm. 5, 3732 (2014)

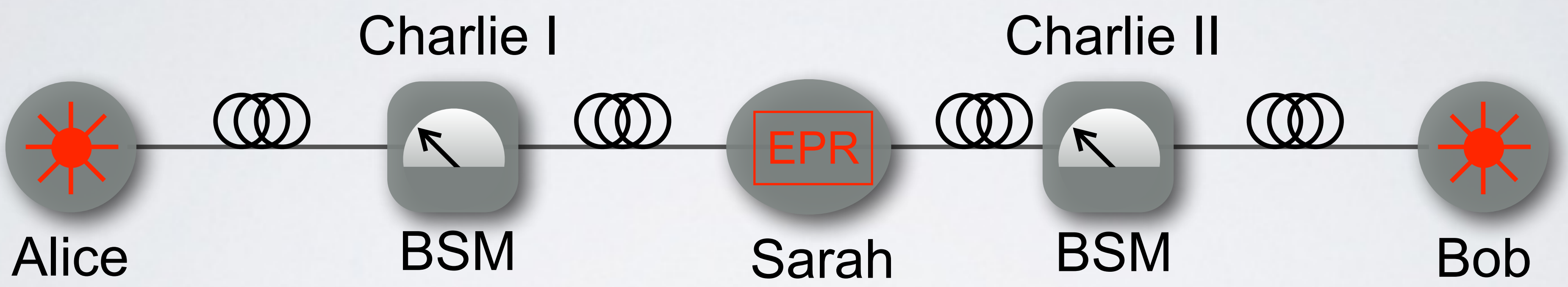
OUTLINE

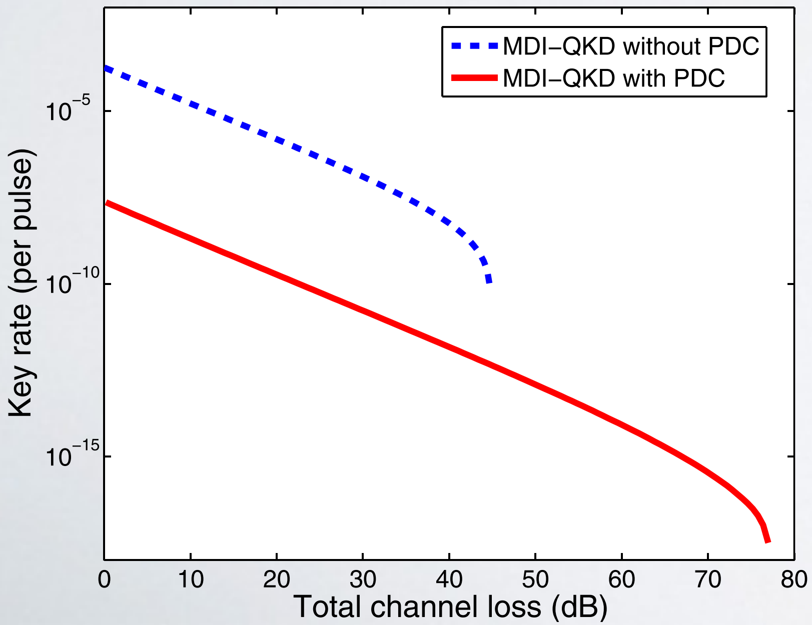
- Side-Channel Attacks
- Measurement-Device-Independent QKD
- Experimental Challenges
- Experiments (part 1) - First Generation
- Theoretical Studies
- **Alternative Protocols**
- Experiments (part II) - Most Recent

VARIATIONS OF MDI-QKD

Combined with Quantum Entanglement / Relay

(F. Xu et al AIP 103, 061101 (2013))

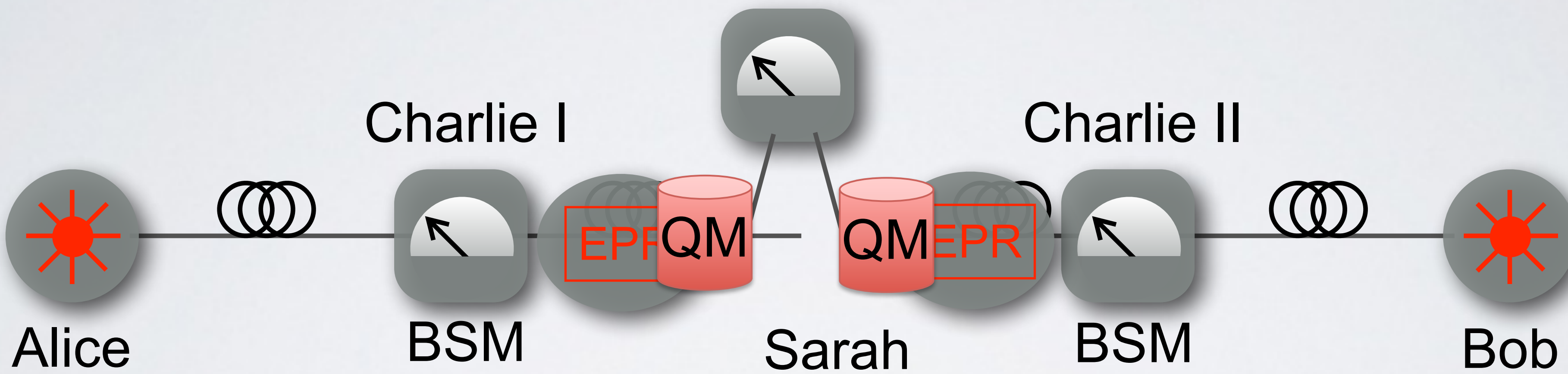


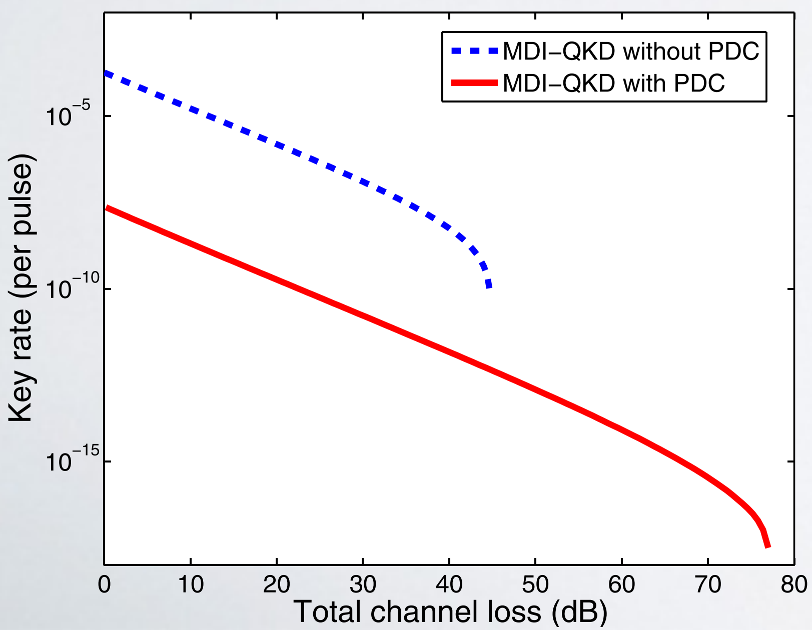


VARIATIONS OF MDI-QKD

Combined with Quantum Entanglement / Relay

(F. Xu et al AIP 103, 061101 (2013))





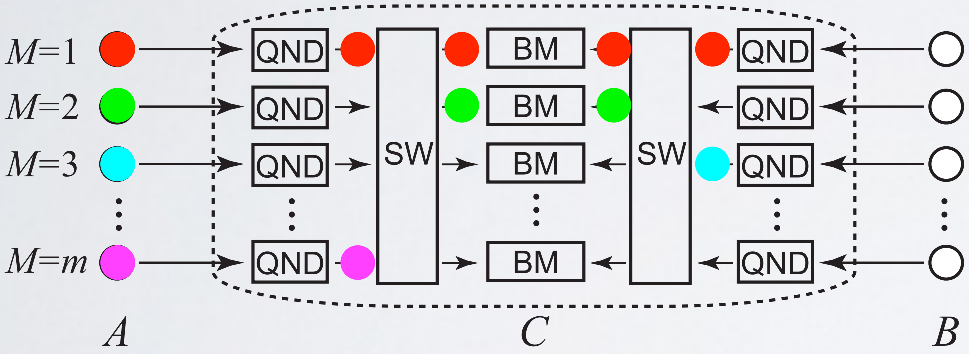
With quantum Memories
Friday, 11:00am

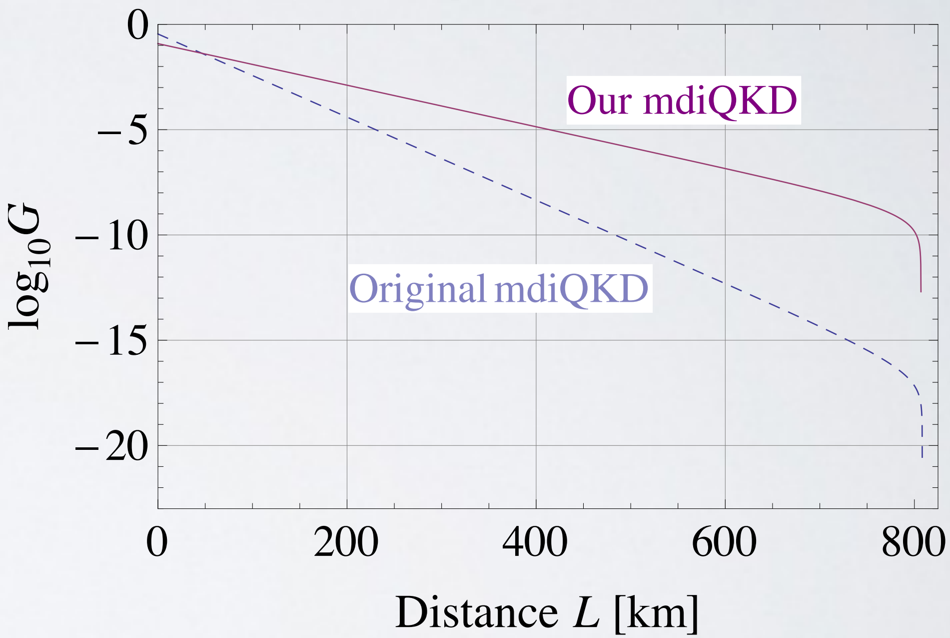
VARIATIONS OF MDI-QKD

Adaptive-BSM-MDI-QKD

(K. Azuma, et al. arxiv:1408.2884 (2014))

Multiplexing in Frequency





Poster on frequency multiplexed quantum memories for QKD

(H. Krovi QCrypt 2014)

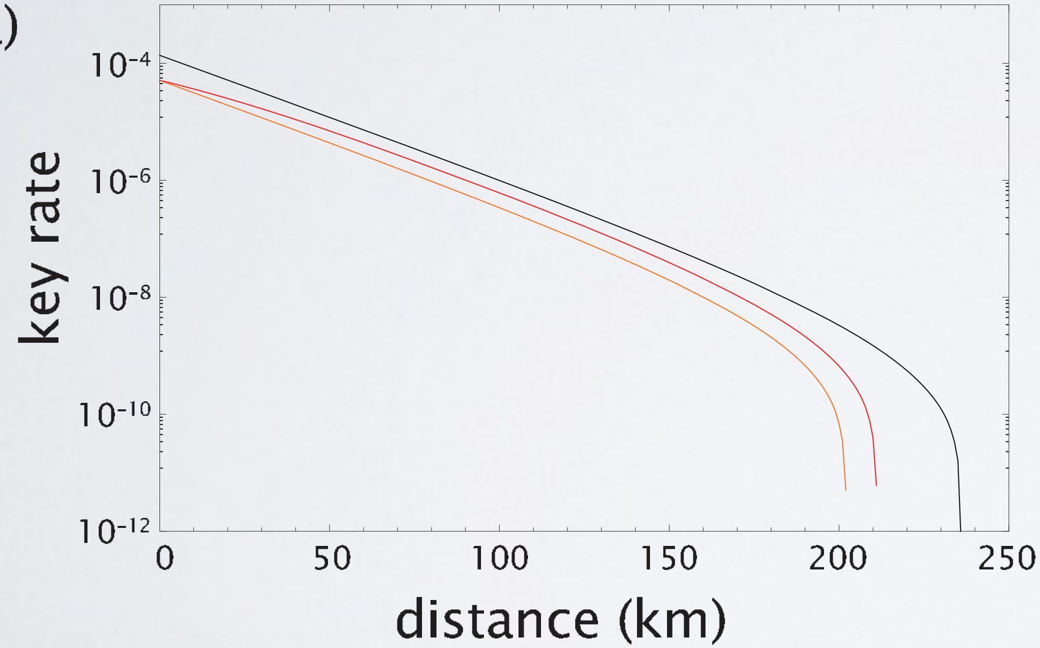
VARIATIONS OF MDI-QKD

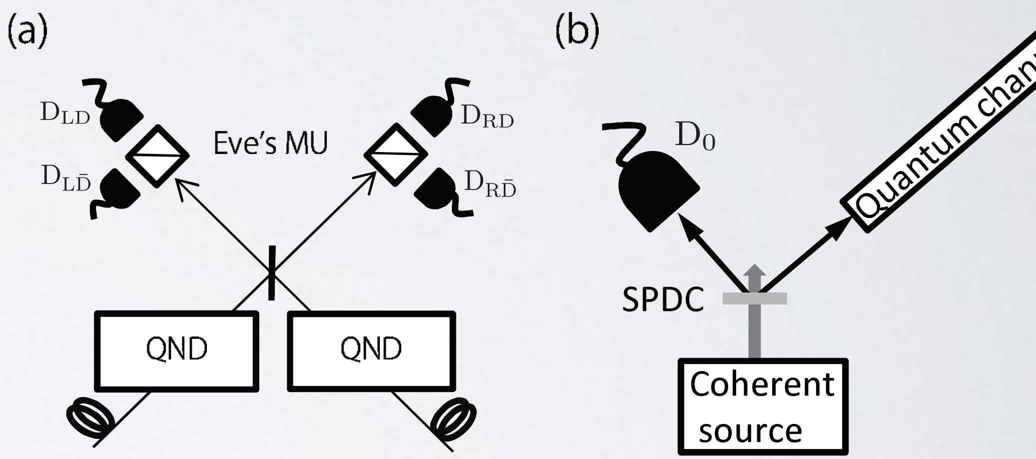
SARG-MDI-QKD

(A. Mitzutani, et al. Sci Reports 05236 (2014))

Some multi-photon emissions secure

(a)





But poissonian statistics very bad

VARIATIONS OF MDI-QKD

CHSH-MDI-QKD

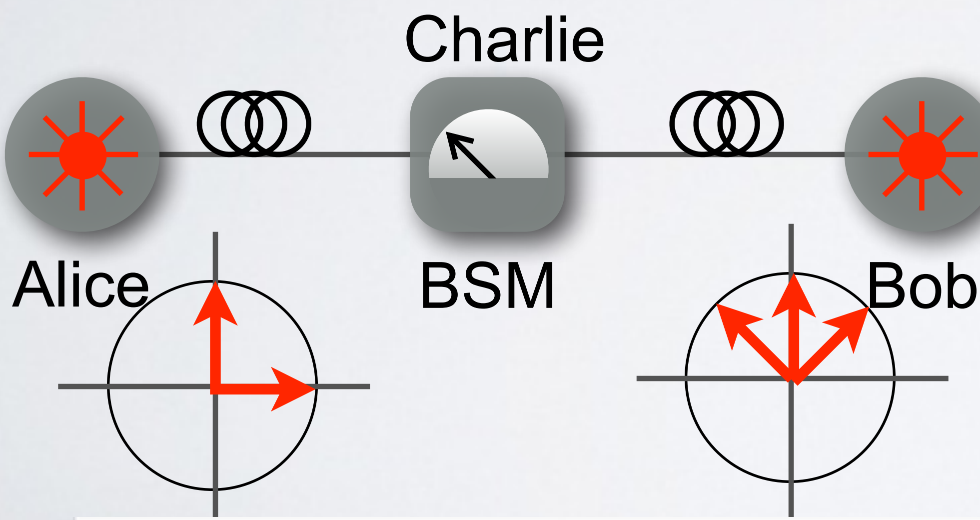
(K. Azuma, et al. arxiv:1408.2884 (2014))

Use CHSH to Bound Eve's knowledge

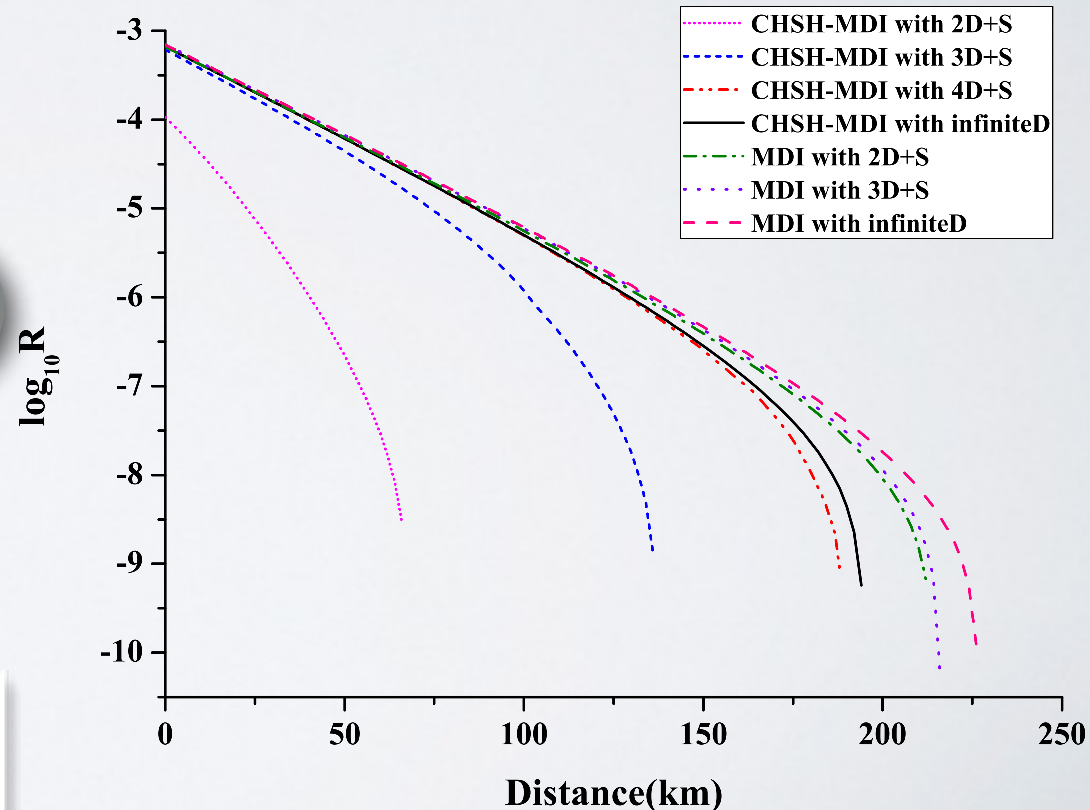
Assumption: dimension of state is 2

(H.W. Li et al, PRA 89, 032302 (2014))

(C.-M. Zhang et al, 1408.0592)



$$S = Q_{11}^{Z}\left(1-\log_2\left(1+\sqrt{2-\frac{S_{1,1}^{CHSH}}{4}}\right)\right)+Q_{\mu\mu}^{Z} f h_2\left(e_{\mu\mu}^{Z}\right)$$

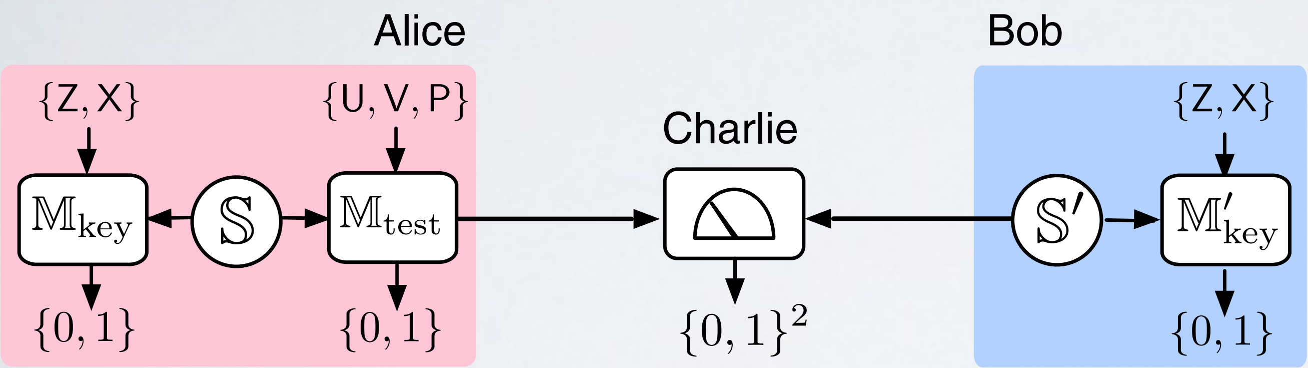


Decoy & Finite Key analysis

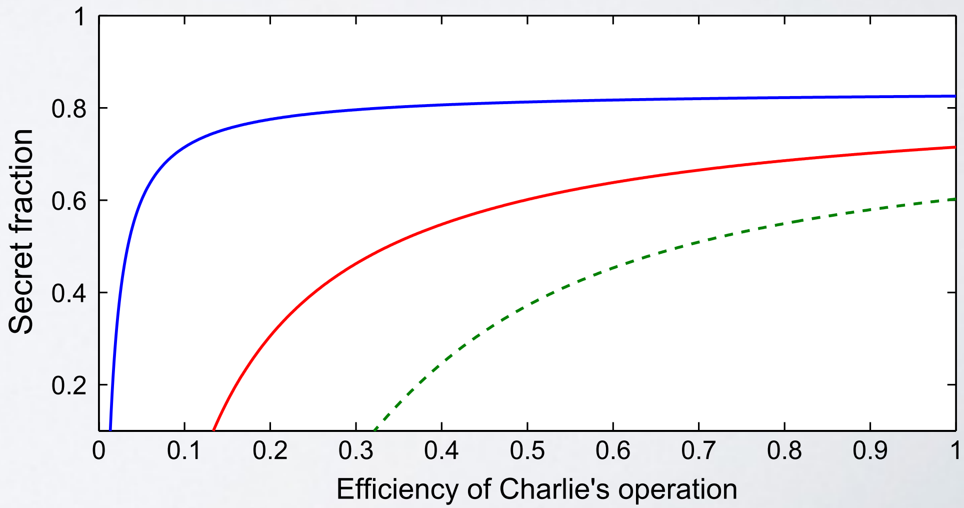
VARIATIONS OF MDI-QKD

DI-QKD with Local Bell Tests

C. C. W. Lim, et al PRX 3, 031006 (2013)



$$S = 1 - \log_2\left(1 + \frac{S}{4\eta}\sqrt{8 - S^2}\right) - 2h_2(e)$$



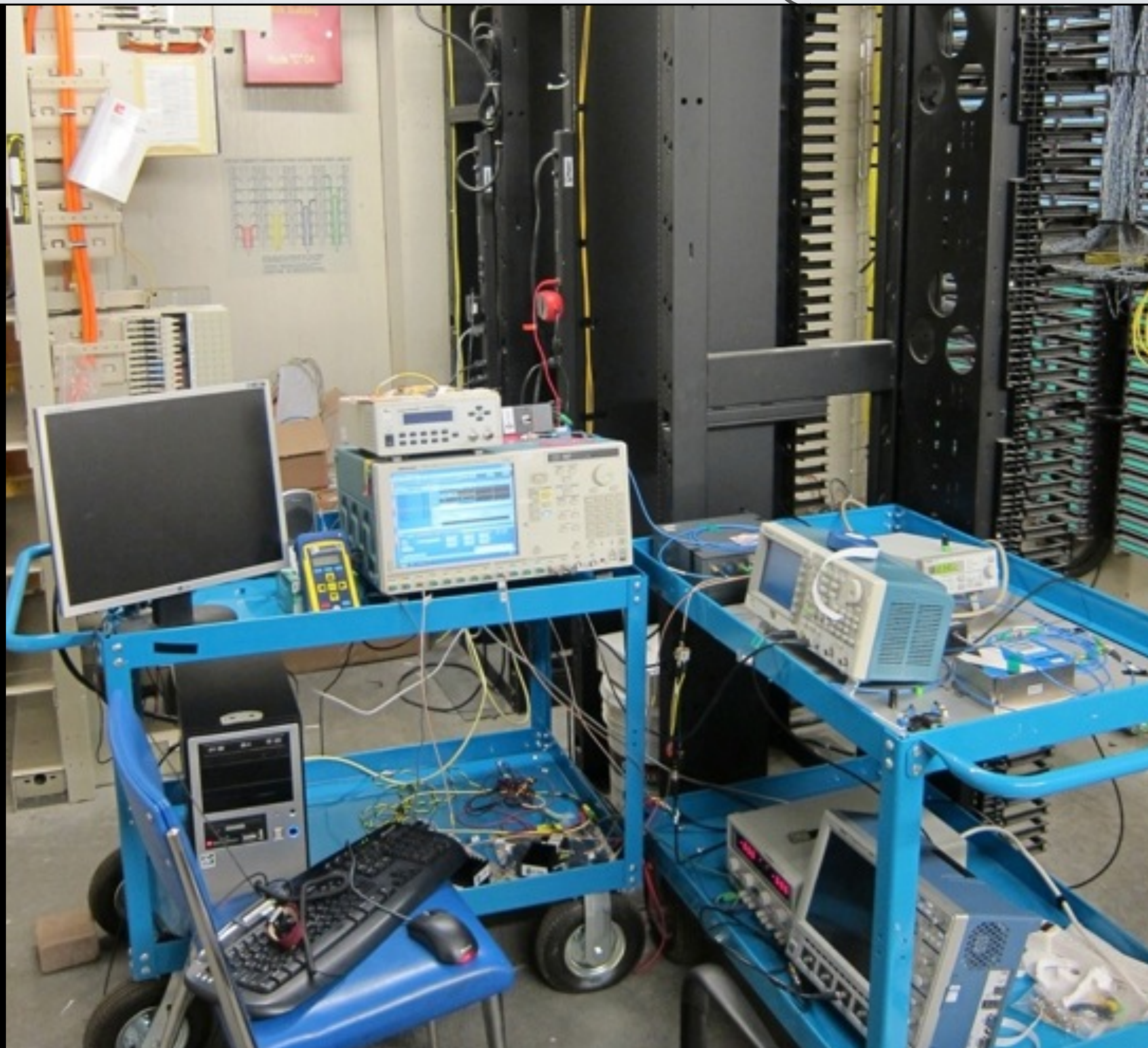
Note: Dependence on Loss

Finite Key version available

OUTLINE

- Side-Channel Attacks
- Measurement-Device-Independent QKD
- Experimental Challenges
- Experiments (part 1) - First Generation
- Theoretical Studies
- Alternative Protocols
- **Experiments (part II) - Most Recent**

THE CUTTING-EDGE OF MDI-QKD



THE CUTTING-EDGE OF MDI-QKD

Towards Full Automation:
Calgary, Canada (QCrypt 2013)

Alice

Exciting Graphs!

Charlie

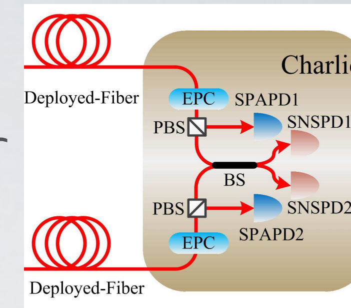
TCP/IP communication.
Automatic time / polarization
Continuous frequency monitor

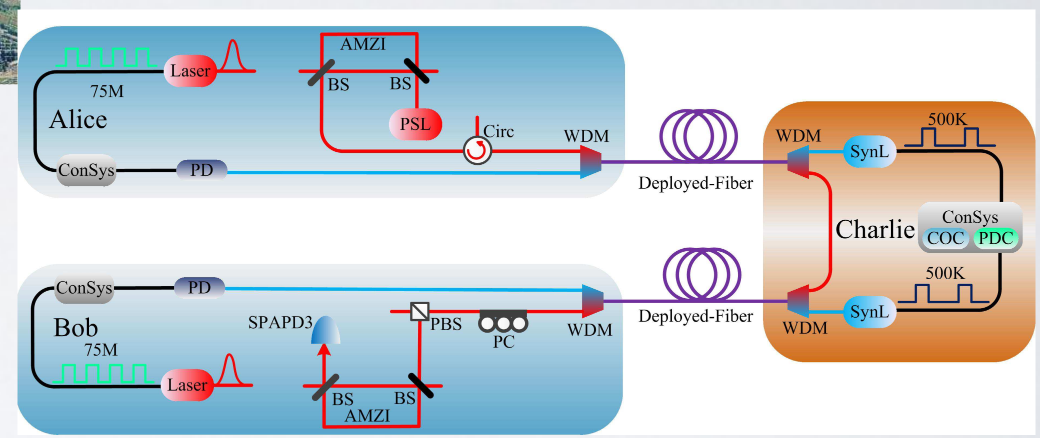
THE CUTTING-EDGE OF MDI-QKD

Full Automation:

Hefei, China (Y.-L. Tang et al arxiv:1408.2330)

Field stabilization of indistinguishability





75 MHz rep rate

18.2 hours

7 bits/s

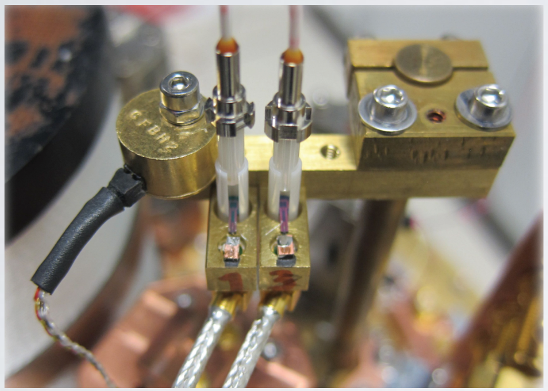
THE CUTTING-EDGE OF MDI-QKD

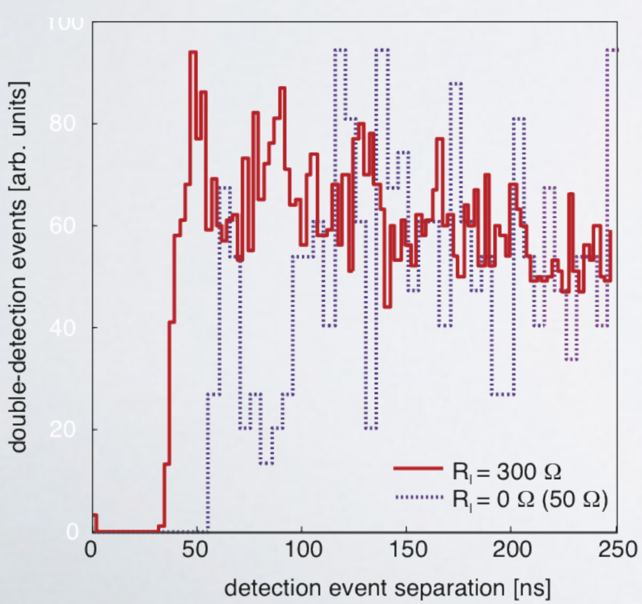
Efficient Bell-State Measurements

Calgary, Canada (R. Valivarthi, JAS, et al., submitted)

NIST

JPL Jet Propulsion Laboratory California Institute of Technology





50% System efficiency

< 40 ns recovery time

Limits Rep-Rate
10 MHz

Theory: $e^Z = 0\%$

Experiment: $e^Z(\psi^+) = 0.32 \pm 0.02\%$

$e^Z(\psi^-) = 0.32 \pm 0.02\%$

Theory: $e^X = 25\%$

Experiment: $e^X(\psi^+) = 26.92 \pm 0.11\%$

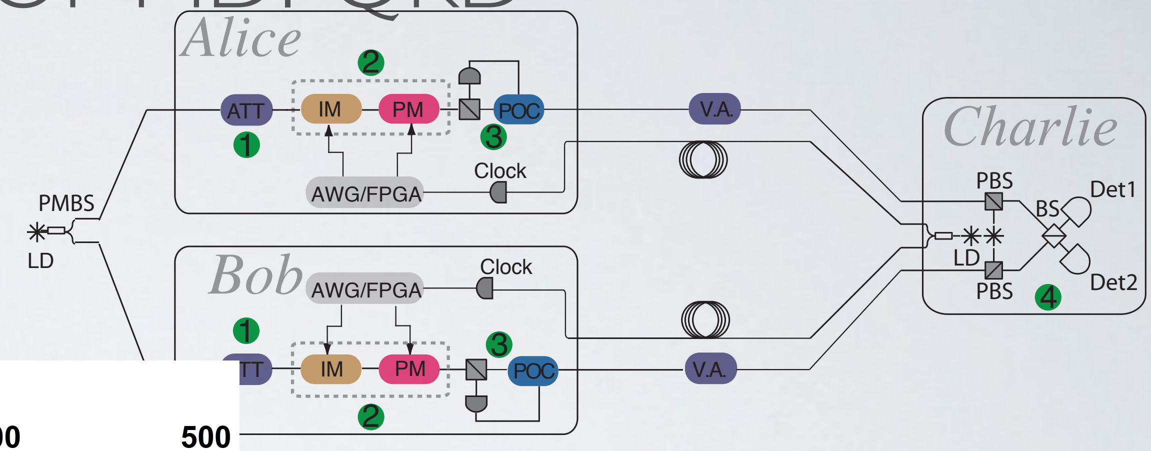
$e^X(\psi^+) = 26.64 \pm 0.10\%$

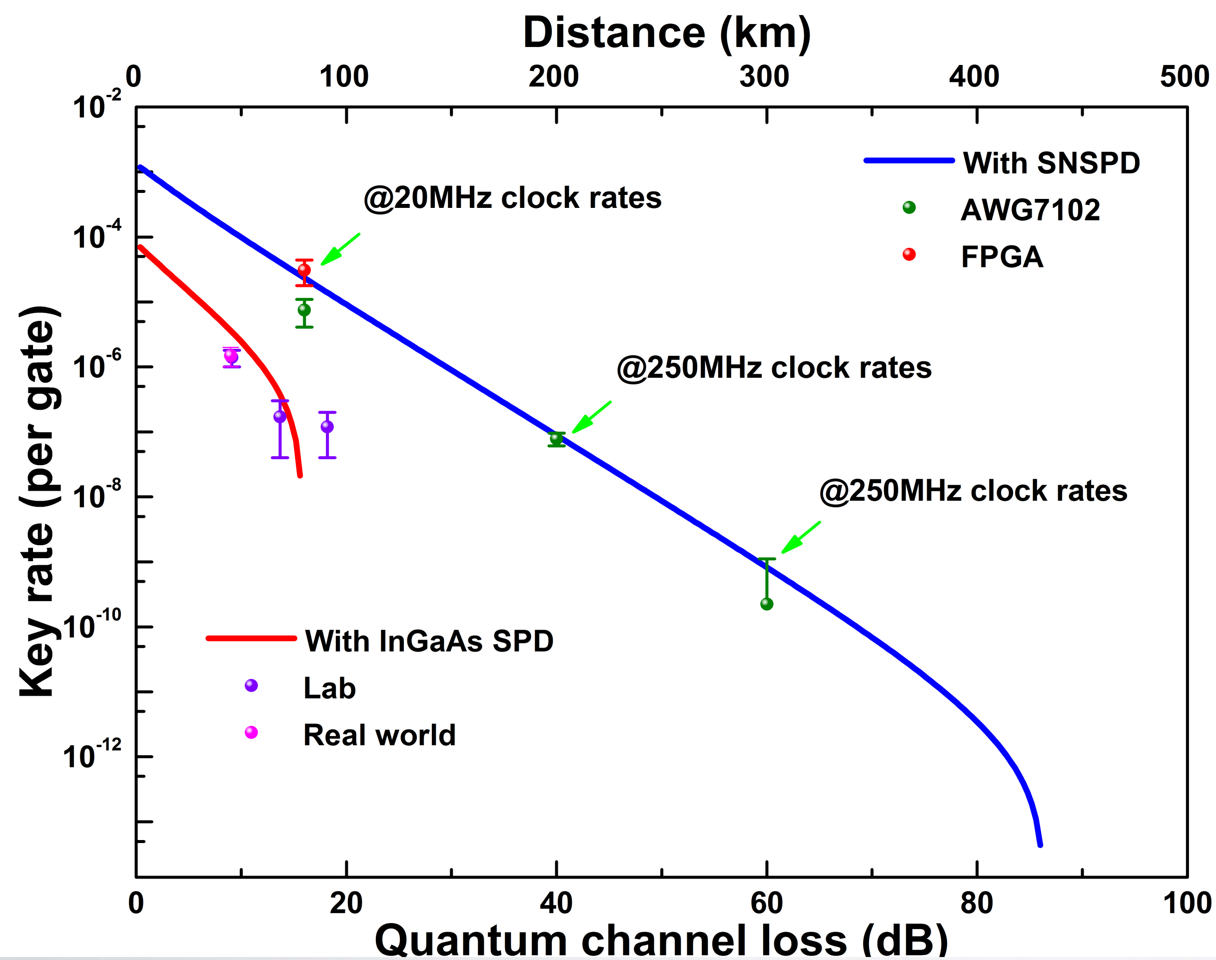
THE CUTTING-EDGE OF MDI-QKD

Long Distance / High Loss

Calgary, Canada

(R. Valivarthi, JAS, et al., QCrypt Poster)





250 MHz,

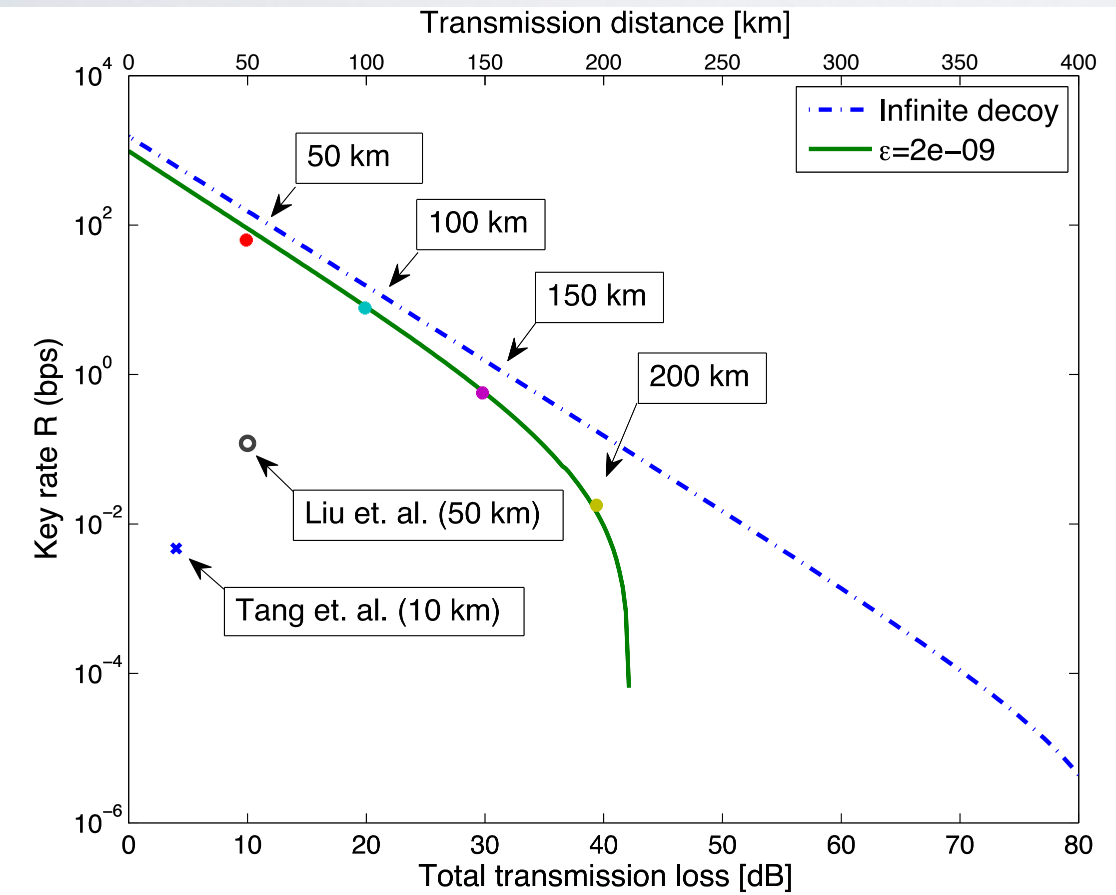
$2.23e^{-10}$ bits/pulse @ 60 dB

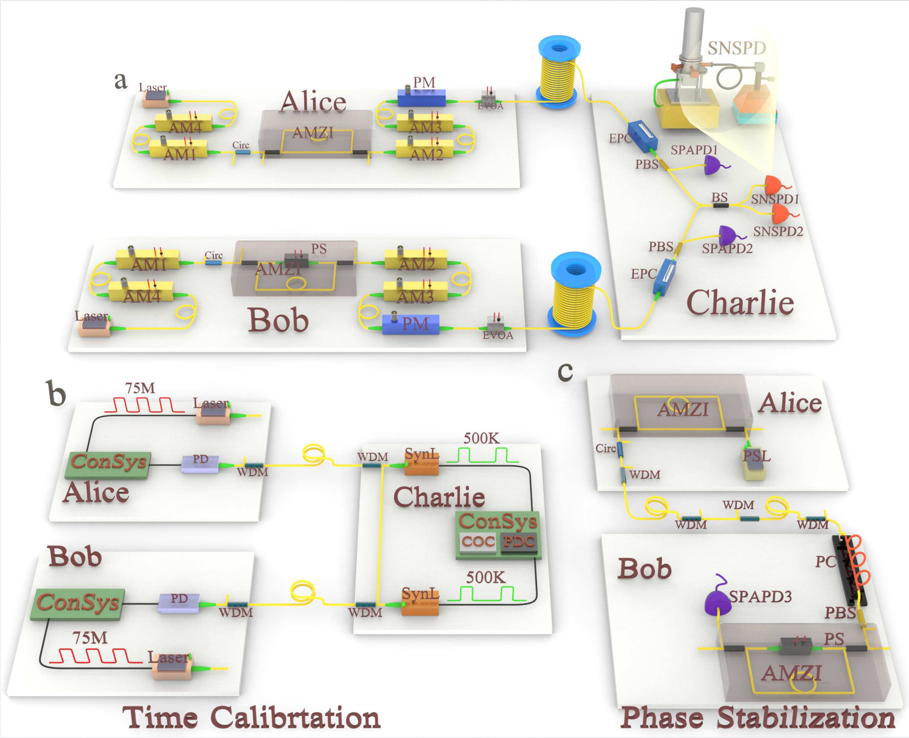
3.3 bit/min

THE CUTTING-EDGE OF MDI-QKD

Long Distance / High Loss
Hefei, China

(Y.-L. Tang et al., arxiv:1407.8012)





75 MHz Rep-Rate

@ 200 km, 0.009 b/sec

THE CUTTING-EDGE OF MDI-QKD

Long Distance / High Loss	Distance	Loss	Key
Hefei, China (Y.-L. Tang et al., arxiv:1407.8012)	200 km	40 dB	0.54 bit/min ε
Calgary, Canada (R. Valivarthi et al., QCrypt 2014)	1 km	60 dB	3.3 bit/min asymptotic
Geneva, Switzerland (B. Korzh et al., arxiv:1407.7427)	307 km	52 dB	191 bit/min ε

MEASUREMENT-DEVICE-INDEPENDENT QUANTUM KEY DISTRIBUTION

Removes all detector side-channel attacks

Experimental demonstrations (real-world / lab, different encodings)

Potential for untrusted Quantum Access Networks

Potential for long-distance

Lots of theoretical & experimental work happening!

Thank you!