Battling with quantum hackers

Hoi-Kwong Lo

Center for Quantum Information and Quantum Control (CQIQC)
Department of Electrical & Computer Engineering
and Department of Physics

University of Toronto

hklo@comm.utoronto.ca
http://www.comm.utoronto.ca/~hklo/

H.-K. Lo, M. Curty and K. Tamaki, (Invited Review)
Nature Photonics, 8, 595–604 (2014).
H.-K. Lo, M. Curty and B. Qi, PRL 108, 130503 (2012).
Z. Tang et al., Phys. Rev. A 93, 042308 (2016).

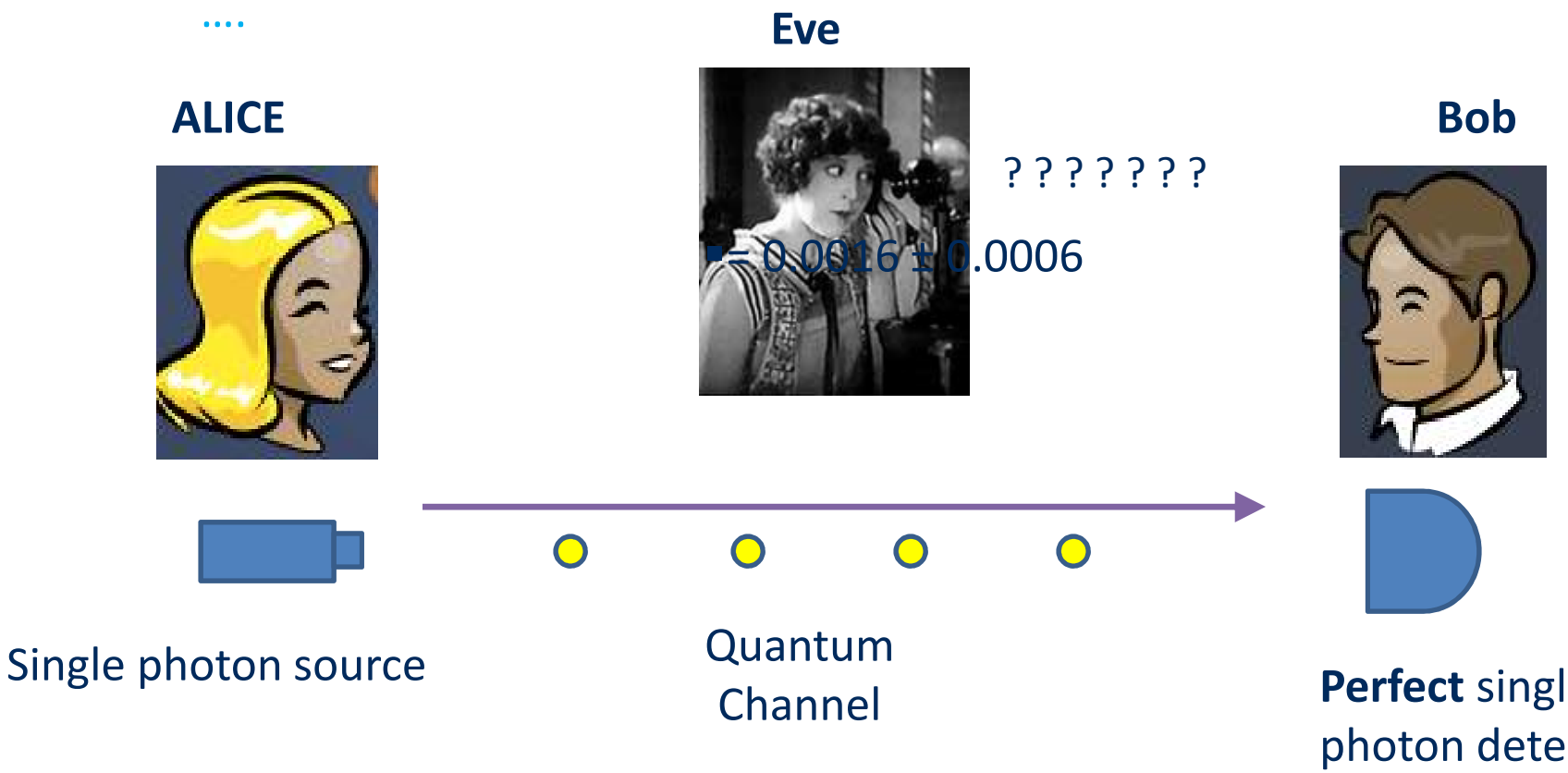
Qcrypt 2016. 15 Sept., 2016

Outline

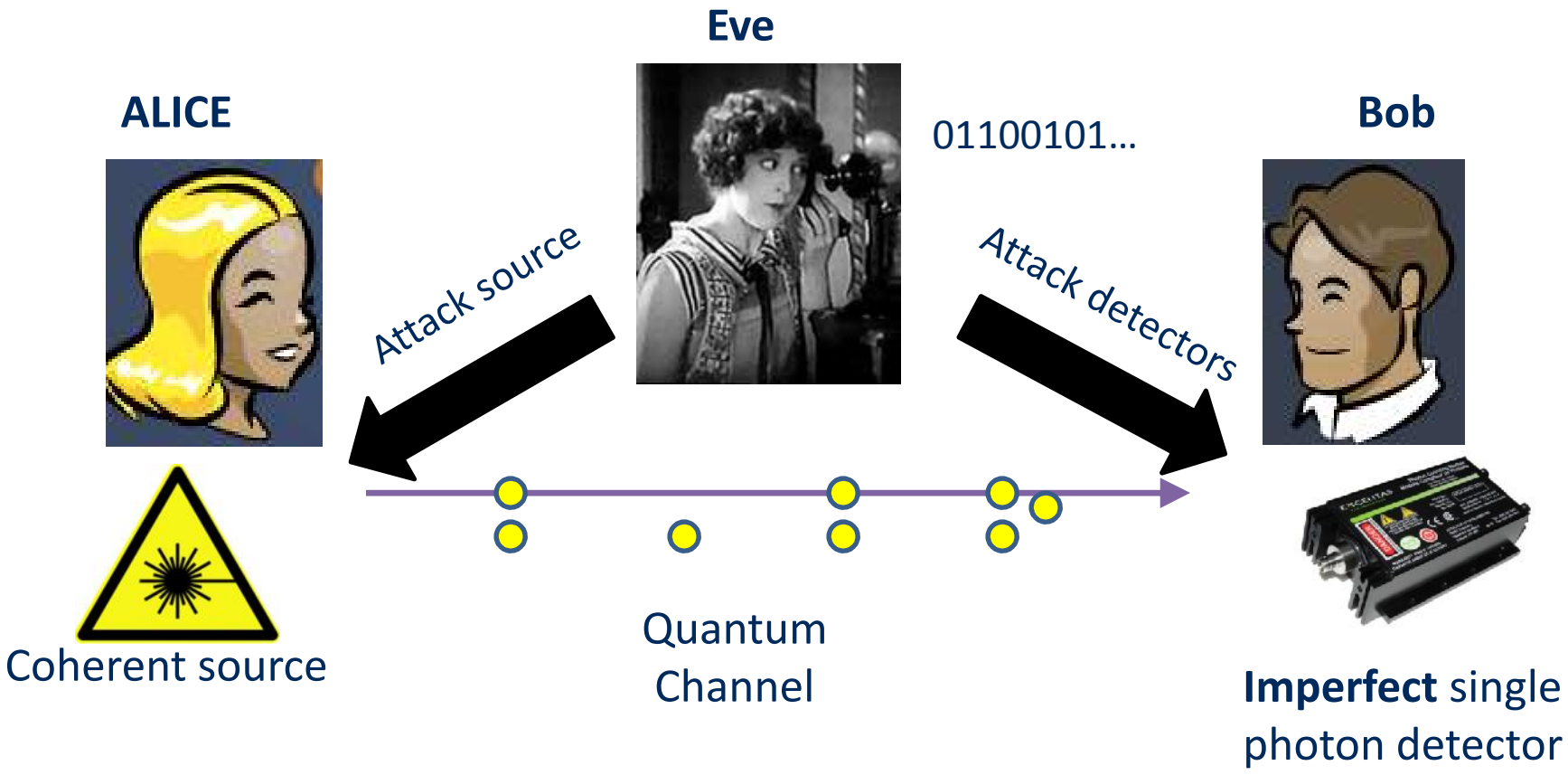
1. Introduction: security of practical QKD
2. Detection security: measurement-device-independent QKD
3. Source security: QKD with source flaws
4. Summary

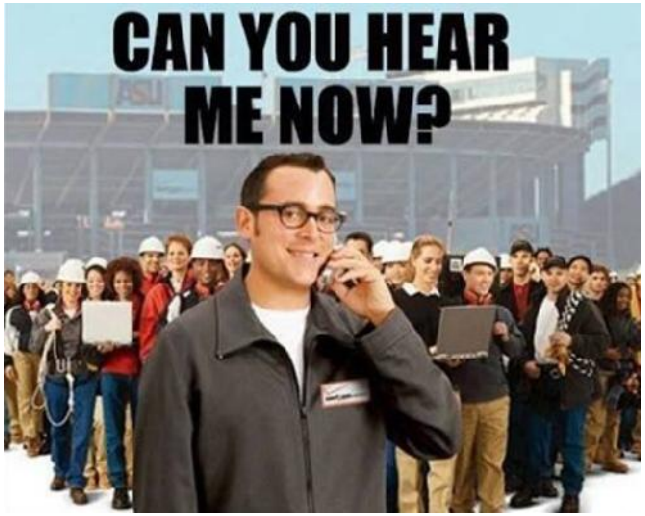
In theory , QKD (e.g. BB84 protocol) is secure…

D. Mayers, J. of ACM 48, 351 (2001).
H.-K. Lo and H. F. Chau, Science 283, 2050 (1999).
P. W. Shor and J. Preskill, PRL 85, 441 (2000).
….



In practice …


Eve
ALICE
Bob
01100101…
Attack source
Attack detectors
Coherent source
Quantum
Channel
Imperfect single
photon detector



National Security Agency (NSA)

Users

Can NSA
break QKD?

Security loopholes in practical QKD

Cf.
Vadim Makarov's talk yesterday.

Photon number splitting attack Brassard *et al.*, Phys. Rev. Lett. **85** 1330 (2000).	Attacks on sources
Phase remapping attack Xu *et al.*, New J. Phys. **12**, 113026 (2010).	
Source tampering attacks Y. Tang *et al.*, Phys. Rev. A **88** 022308 (2013) S. Sun *et al.*, Phys. Rev. A **92** 022304 (2015)	
Time-shift attack Qi *et al.*, Quant. Inf. Comput. **7**, 073 (2007); Zhao *et al.*, Phys. Rev. A **78**, 042333 (2008).	Attacks on detectors
Bright illumination attack Markarov, New J. Phys. **12**, 113026 (2009); Lydersen *et al.*, Nat. Photon. **4**, 686 (2010); Lydersen *et al.*, Opt. Express **18**, 27938 (2010); Lydersen *et al.*, Phys. Rev. A **84**, 032320 (2011); Wiechers *et al.*, New. J. Phys. **13**, 013043 (2011).	
Device calibration attack Jain *et al.*, Phys. Rev. Lett. **197**, 110501 (2011).	
Attack by exploiting the dead time of SPD Weier *et al.*, New. J. Phys. **13**, 073024 (2011).	
Laser damage attack A. Bugge *et al.*, Phys. Rev. Lett., **112**, 070503 (2014).	

Countermeasures

- Security patches
  - Ad hoc. Cannot close other potential loopholes.

  Z. Yuan et al., Nature Photonics 4, 800 (2010)
  L. Lydersen et al., Nature Photonics 4, 801 (2010)
- Better models to understand imperfections in practical QKD systems
  - Hard to close all the security loopholes

  T.F. da Silva et al., Opt. Express 20, 18911 (2012)
- Device Independent QKD
  - Based on loophole-free Bell test (Cf. this morning's sessions)

  Requires detectors with near-unity quantum efficiency.
  Overall link loss has to be small or efficient heralding is needed.
  - Very low key generation rate (~10^{-10} per pulse) at practical distance with a parametric down conversion source.

  e.g. D. Mayers and A. Yao, FOCS '98, p. 503 ; A. Acin et al., PRL 98, 230501 (2007) ; Gisin et al., Phys. Rev. Lett. 105, 070501 (2010); Vazirani and T. Vidick, PRL 113, 140501 (2014); R. Arnon-Friedman, R. Renner, T. Vidick, http://arxiv.org/abs/1607.01797 , etc.
  - Vulnerable to memory attack (covert channels).

  J. Barrett, R. Colbeck & A. Kent, PRL 010503 (2013).

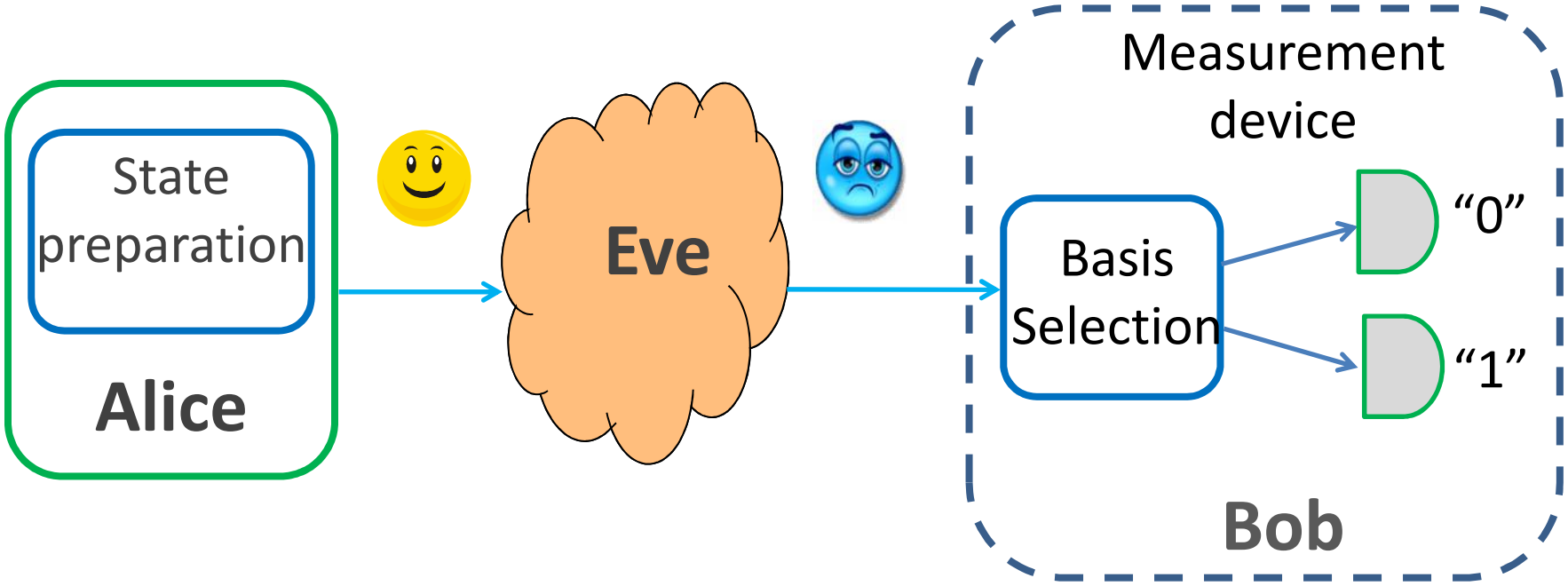
Outline

1. Introduction: security of practical QKD
2. **Detection security: measurement-device-independent QKD**
3. Source security: QKD with source flaws
4. Summary

Automatically immune to **all** (known or yet to be discovered) detection attacks!

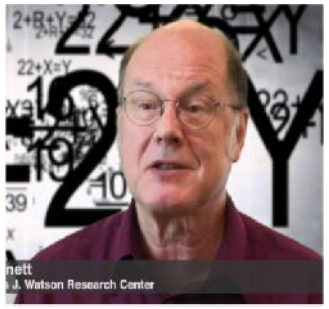
H.-K. Lo, M. Curty and B. Qi, *Phys. Rev. Lett*. **108**, 130503 (2012).
[See also E. Biham, B. Huttner, and T. Mor, Phys. Rev. A, 54(4):2651 (1996)
H. Inamori, Algorithmica 34, pp. 340-365 (2002).
See also, S. L. Braunstein and S. Pirandola, PRL 108, 130502 (2012).]

Achilles' heel for QKD



The weakest link in a QKD system is the measurement device.

"Photon detectors have turned out to be an Achilles' heel for quantum key distribution (QKD),… "
---Charles Bennett



Security loopholes in practical QKD

Photon number splitting attack
Brassard *et al.*, Phys. Rev. Lett. **85** 1330 (2000).

Phase remapping attack
Xu *et al.*, New J. Phys. **12**, 113026 (2010).

Source tampering attacks
Y. Tang *et al.*, Phys. Rev. A **88** 022308 (2013)
S. Sun *et al.*, Phys. Rev. A **92** 022304 (2015)

Attacks on sources

Time-shift attack
Qi *et al.*, Quant. Inf. Comput. **7**, 073 (2007);
Zhao *et al.*, Phys. Rev. A **78**, 042333 (2008).

Bright illumination attack
Markarov, New J. Phys. **12**, 113026 (2009);
Lydersen *et al.*, Nat. Photon. **4**, 686 (2010);
Lydersen *et al.*, Opt. Express **18**, 27938 (2010);
Lydersen *et al.*, Phys. Rev. A **84**, 032320 (2011);
Wiechers *et al.*, New. J. Phys. **13**, 013043 (2011).

Device calibration attack
Jain *et al.*, Phys. Rev. Lett. **197**, 110501 (2011).

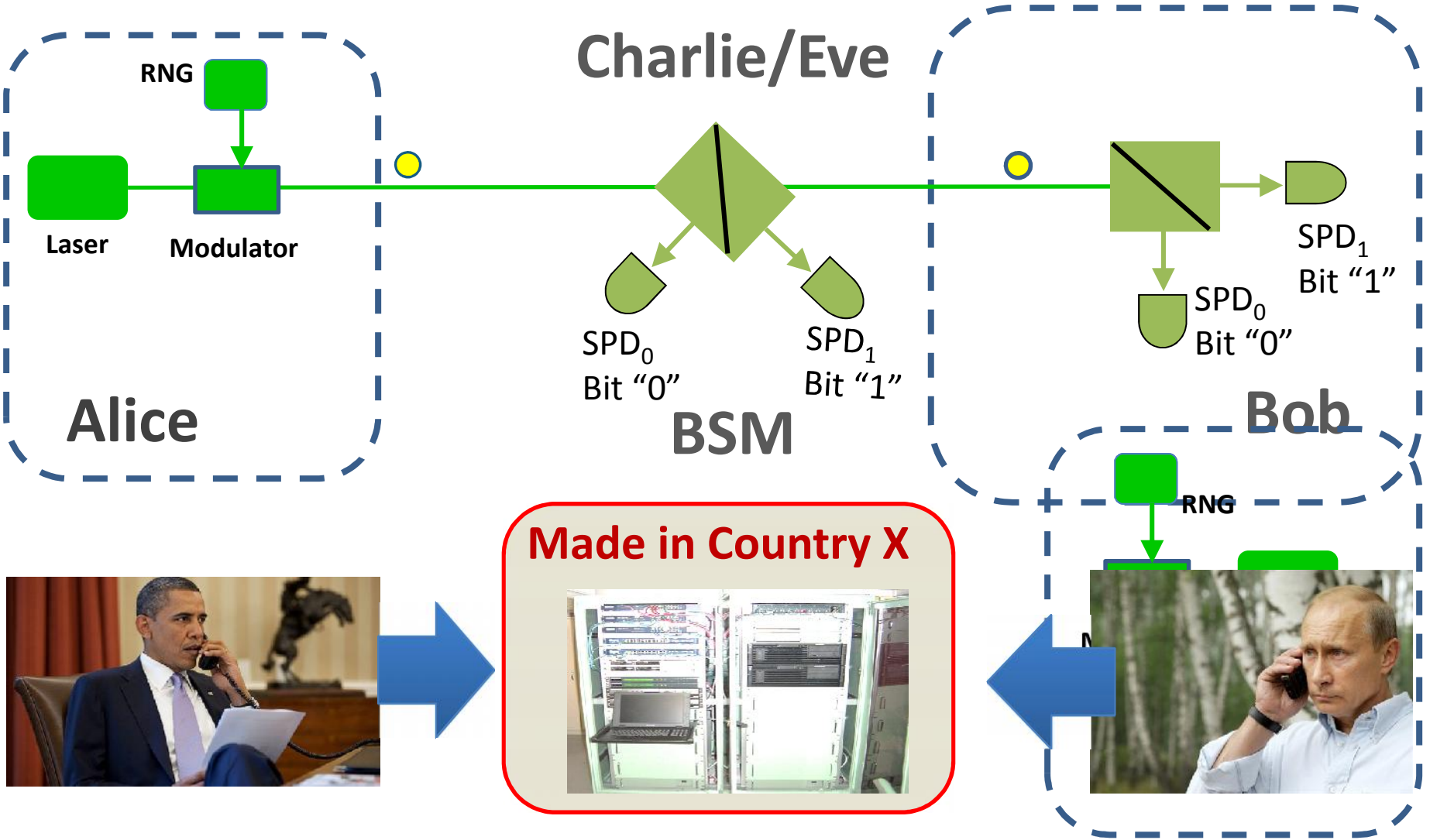
Attack by exploiting the dead time of SPD
Weier *et al.*, New. J. Phys. **13**, 073024 (2011).

Laser damage attack
A. Bugge *et al.*, Phys. Rev. Lett., **112**, 070503 (2014).

Attacks on detectors

Cf.
Vadim Makarov's talk yesterday.

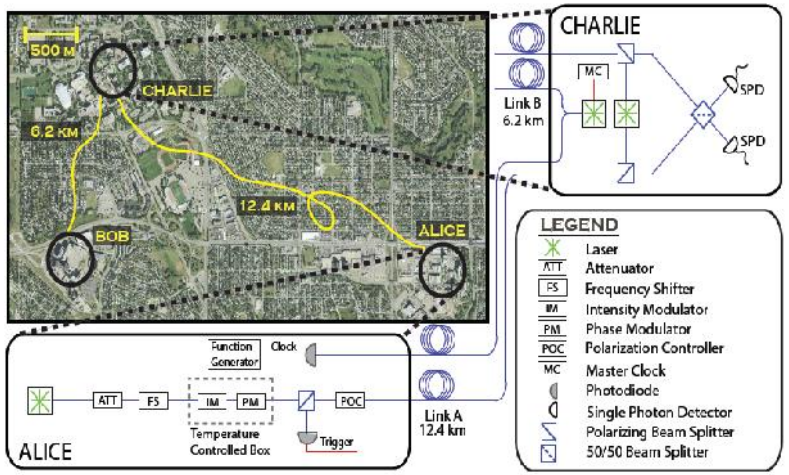
Measurement-device-independent QKD



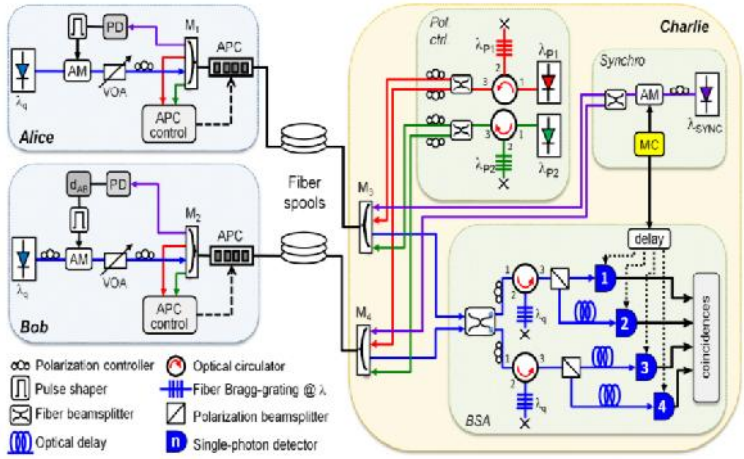
Secure QKD with ***untrusted*** relay!

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

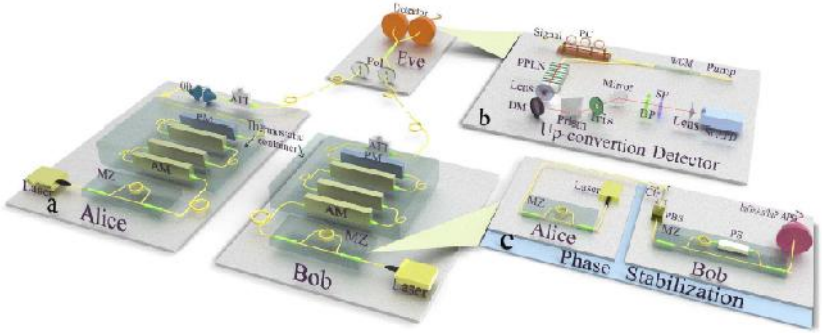
Initial MDI-QKD demonstrations



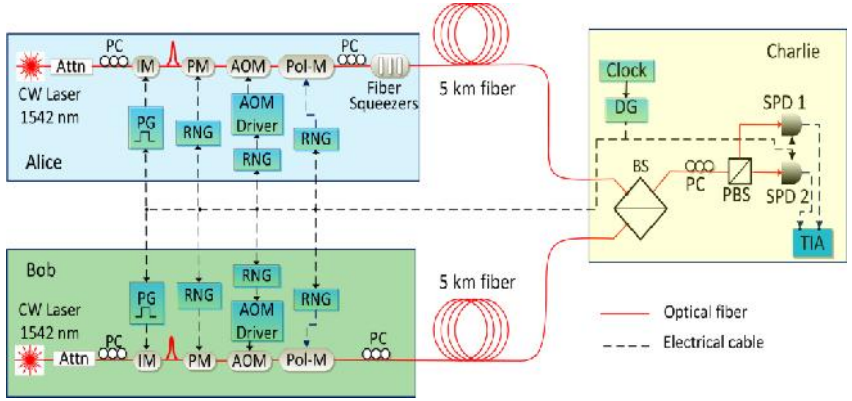
A. Rubenok *et al.*, *PRL* 111, 130501 (2013)



T. Silva *et al.*, *PRA*, 88 052303 (2013)



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



Z. Tang *et al*. *PRL* 112, 19050 (2014)

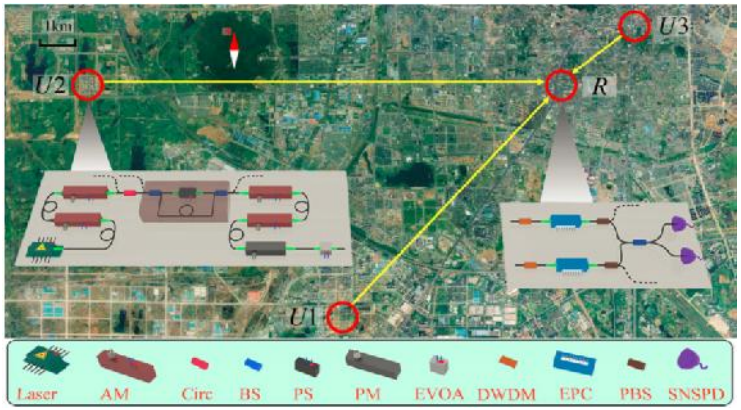
Four initial Experiments

	Calgary PRL 111, 130501 (2013)	Brazil PRA, 88 052303 (2013)	China PRL 111, 130502 (2013)	Toronto PRL 112, 19050 (2014)
Encoding	Time-bin	Polarization (active stabilization)	Time-bin (active stabilization)	Polarization (passive stabilization)
Practicality	Field test (Proof-of-Principle)	Lab system (Proof-of-Principle)	Lab system (Custom components)	Lab system (All commercial components)
Asymptotic key rate	~ 10^{-6} (~ 10 km)	1×10^{-6} (17 km)	Not reported	6.6×10^{-6} (10 km)
Finite-key rate (per pulse)	Not reported	Not reported	$1x10^{-7}$ (50 km)	$1x10^{-8}$ (10 km)
Parameter optimization	No	No	No	Yes

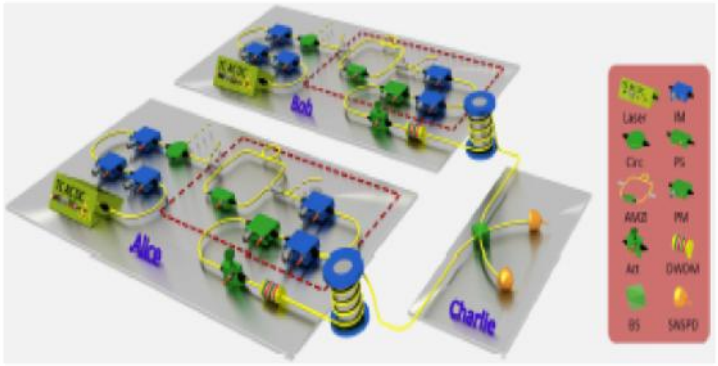
Four Published Experimental Demonstrations of MDI-QKD:

Two proof-of-principle. Two with random switching of bits and bases.

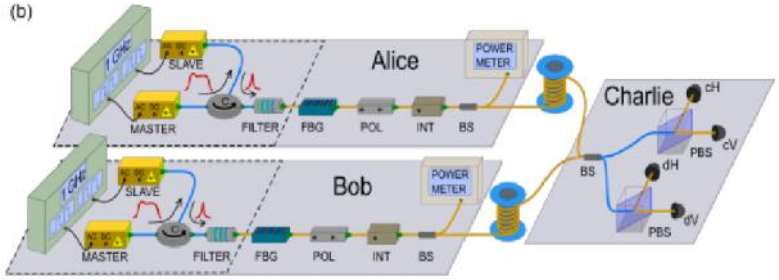
Recent MDI-QKD Experiments



MDI-QKD over untrustful metropolitan network Y.L. Tang et al., PRX 6, 011024 (2016).



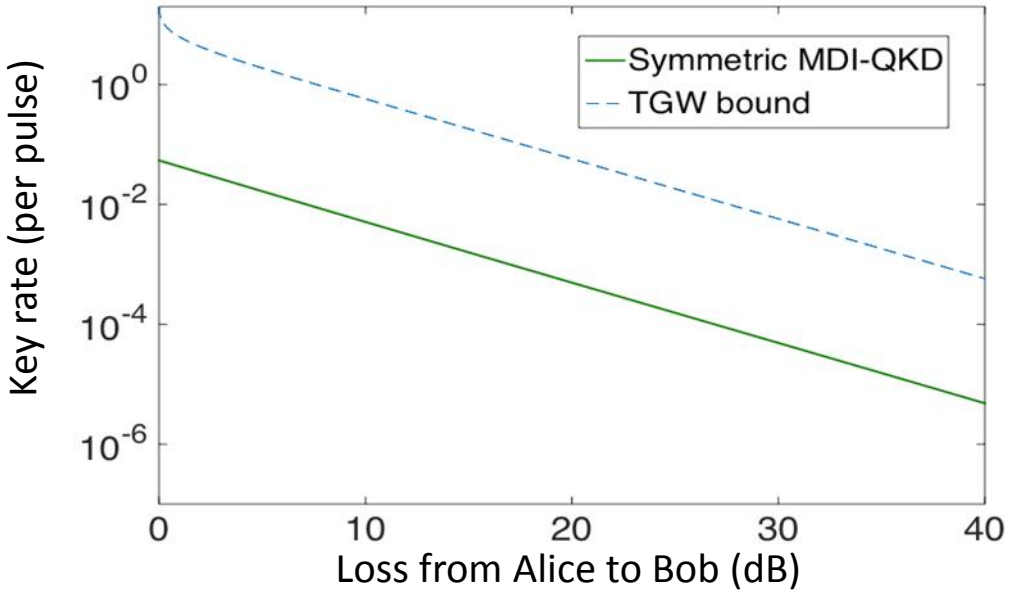
MDI-QKD with 404km: H.-L. Yin et al., http://arxiv.org/abs/1606.06821



MDI-QKD with > 1 Mbps key rate: L. C. Comandar et al., Nature Photonics, 10 312 (2016).

MDI-QKD vs TGW bound

Assuming state-of-the-art high-efficiency SPDs with η=93%, and QBER=0.25% (which corresponds to =0.1 in theoretical model).

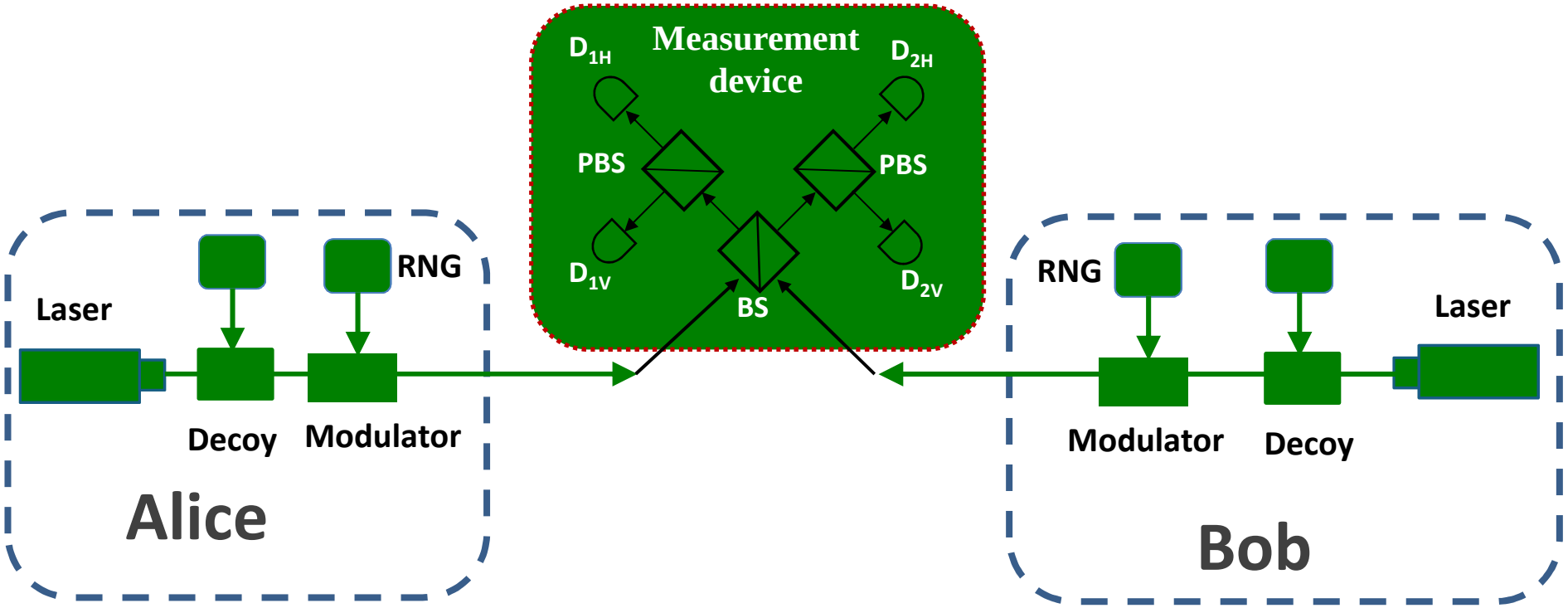


MDI-QKD is only about two orders of magnitude away from the fundamental limit at metropolitan distance (e.g from20km)!

[Recall loss at telecom fiber is about 0.2dB/km.]

M. Takeoka, S. Guha, M. M. Wilde, *Nat. Comm.*, **5**, 5235 (2014)
F. Xu, M. Curty, B. Qi, L. Qian, H.-K- Lo, *Nature Photonics* 9, 772–773 (2015)

Towards **experimental** side-channel-free QKD



How to address ***both*** source and detector flaws?

Outline

1. Introduction: security of practical QKD
2. Detection security: measurement-device-independent QKD
3. **Source security: QKD with source flaws**
4. Summary

Security loopholes in practical QKD

Photon number splitting attack
Brassard *et al.*, Phys. Rev. Lett. **85** 1330 (2000).

Phase remapping attack
Xu *et al.*, New J. Phys. **12**, 113026 (2010).

Source tampering attacks
Y. Tang *et al.*, Phys. Rev. A **88** 022308 (2013)
S. Sun *et al.*, Phys. Rev. A **92** 022304 (2015)

Attacks on sources

Time-shift attack
Qi *et al.*, Quant. Inf. Comput. **7**, 073 (2007);
Zhao *et al.*, Phys. Rev. A **78**, 042333 (2008).

Bright illumination attack
Markarov, New J. Phys. **12**, 113026 (2009);
Lydersen *et al.*, Nat. Photon. **4**, 686 (2010);
Lydersen *et al.*, Opt. Express **18**, 27938 (2010);
Lydersen *et al.*, Phys. Rev. A **84**, 032320 (2011);
Wiechers *et al.*, New J. Phys. **13**, 013043 (2011).

Protected by MDI-QKD

Device calibration attack
Jain *et al.*, Phys. Rev. Lett. **197**, 110501 (2011).

Attack by exploiting the dead time of SPD
Weier *et al.*, New. J. Phys. **13**, 073024 (2011).

Laser damage attack
A. Bugge *et al.*, Phys. Rev. Lett., **112**, 070503 (2014).

Attacks on detectors

Assumptions at source

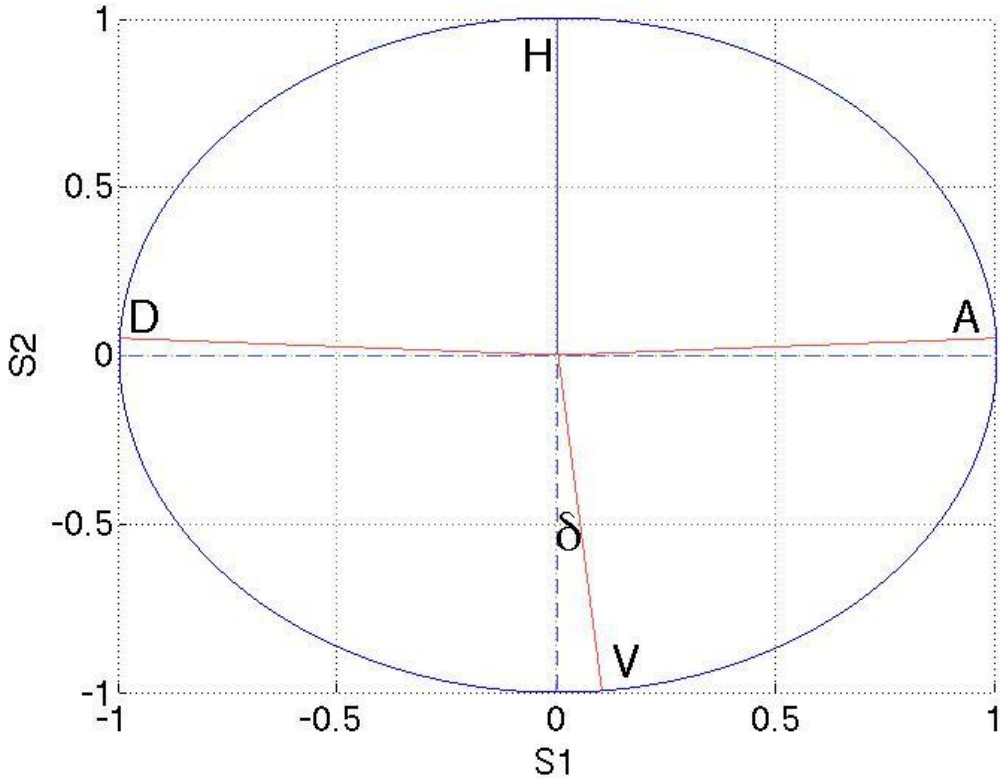
1. Perfect encoding
2. No side channel
3. Perfect quantum random number generation
4. Perfect phase randomization
5. Perfect intensity control

MDI-QKD with source flaws

- Assumption in MDI-QKD:
  - Sources must be TRUSTED
  - Not verified in previous demonstrations
- Sources are not perfect
  - Multi-photon components
    - Decoy state method gives a good solution

    W.-Y. Hwang, PRL 91, 057901 (2003); H.-K. Lo, X. Ma, and K. Chen, PRL 94 , 230504 (2005); X.-B. Wang, PRL 94, 230503 (2005).
  - **State preparation flaws**
    - **Actual states are not exact BB84 states**
  - and others …(No side channel, perfect quantum random number generation, perfect phase randomization, perfect intensity control).

State preparation flaws



State preparation flaws

- Expected: $0, \frac{p}{4}, \frac{p}{2}, \frac{3p}{4}$
- Actual: $0, \frac{p}{4}(1+\frac{d}{p}), \frac{p}{2}(1+\frac{d}{p}), \frac{3p}{4}(1+\frac{d}{p})$

MDI-QKD with state preparation flaws - GLLP

- GLLP can be applied.

Gottesman, Lo, Lütkenhaus, and Preskill, QIC 5, 325 (2004).

- State imperfection characterized by

$$\Delta_{ini} = \frac{1}{2}(1 - F_A(\mathrm{r}_A^X, \mathrm{r}_A^Z) F_B(\mathrm{r}_B^X, \mathrm{r}_B^Z))$$

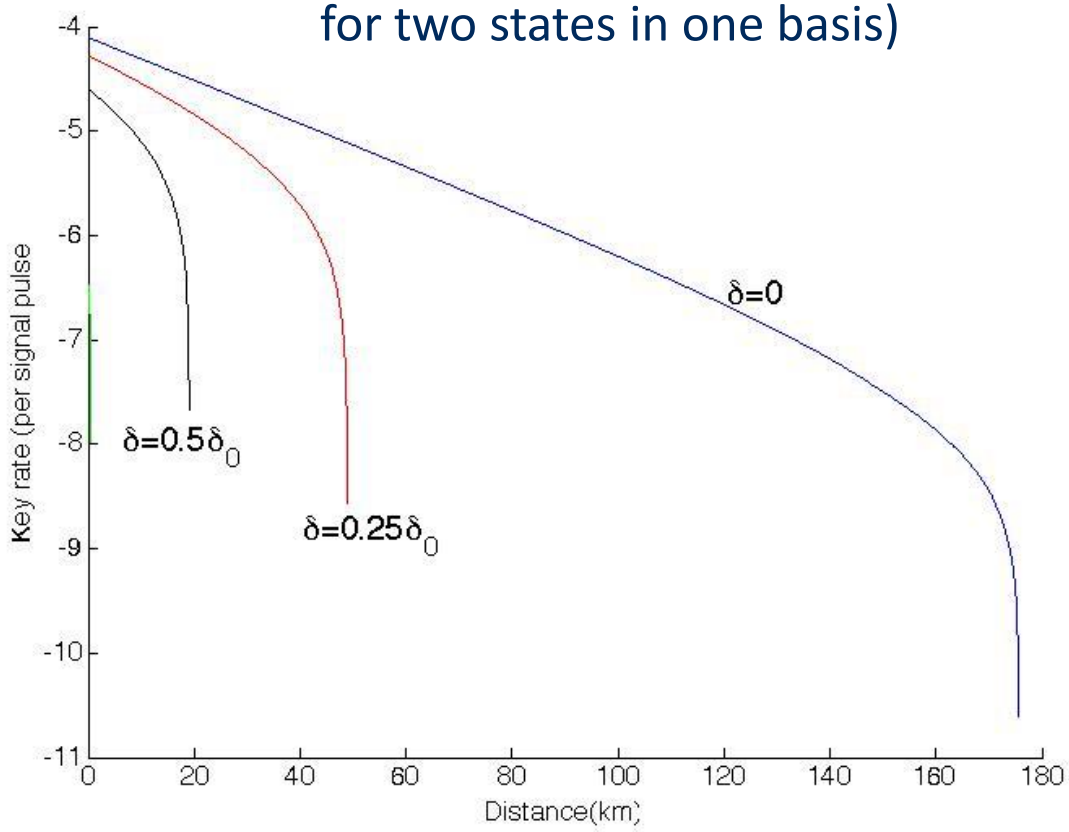
- Pessimistic assumption: Eve can **enhance** the flaws of single photon part by exploiting the loss

$$\Delta \le \frac{\Delta_{ini}}{Y_{11}}$$

  - Y_{11}: Gain of single photon
- Poor performance, not loss tolerant

MDI-QKD with state preparation flaws - GLLP

- δ/π ~ relative encoding errors
- δ_0 = 0.063 rad (corresponding to 30 dB extinction ratio for two states in one basis)



With prior security proof, GLLP, the key rate decays quickly for even small δ. This is bad!

Loss tolerant protocol with source flaws

- Built on the work **loss tolerant** QKD
  - K. Tamaki et al., Phys. Rev. A, **90**, 052314 (2014)
- Three state protocol: $\{|0_Z\rangle, |1_Z\rangle, |0_X\rangle\}$ ("qubit assumption")
- Estimate e_x using rejected data analysis (events where Alice and Bob use different bases)
- Distill secret key from where both Alice and Bob use Z basis
- Loss tolerant BB84 demonstrated on commercial QKD systems (ID Quantique ID-500 & Clavis 2)
  - F. Xu *et al*., Phys. Rev. A, **92**, 032305 (2015).

  (Feihu Xu won Best Student Paper Prize, Qcrypt 2014).

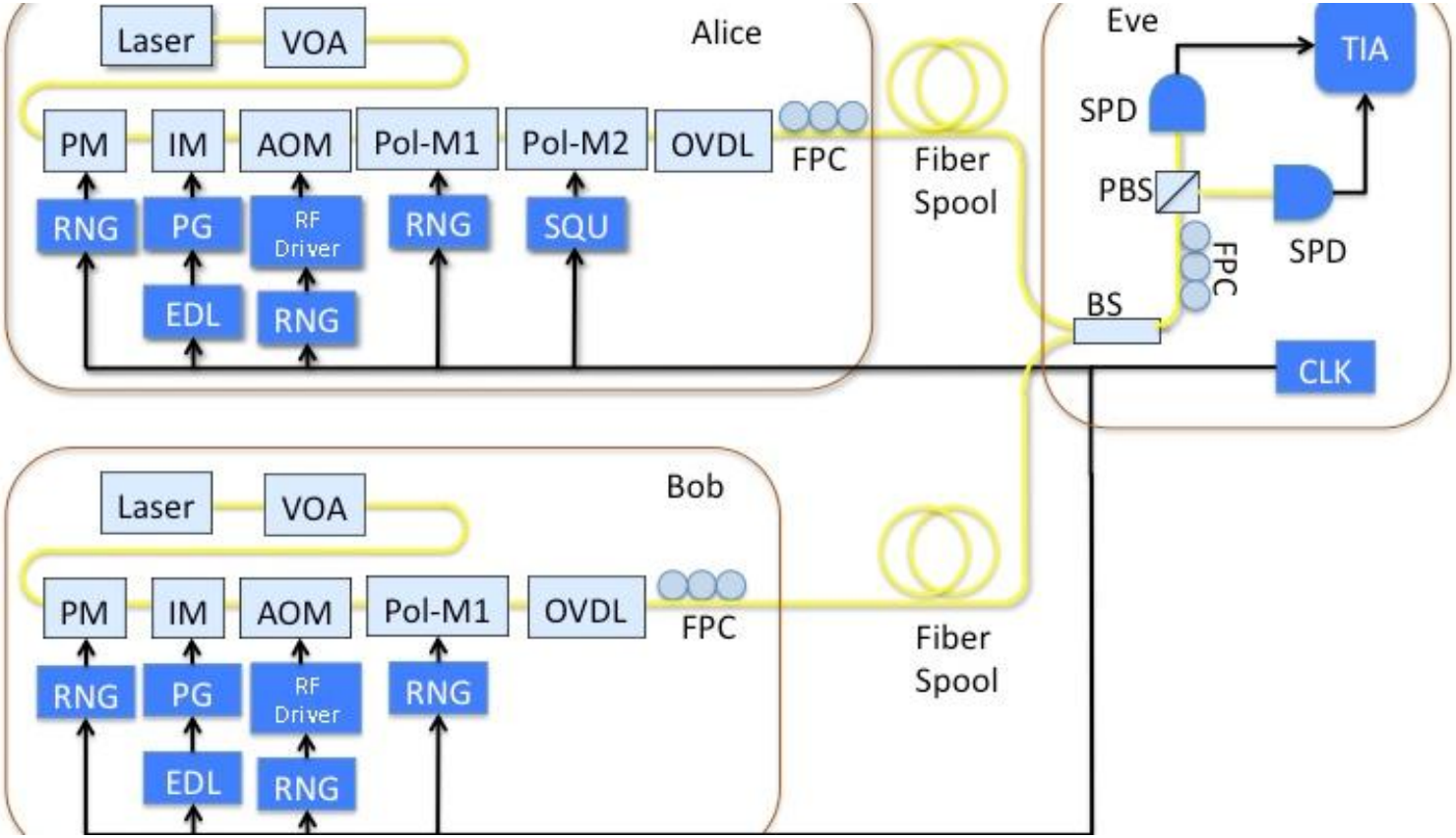
Challenge: To combine loss tolerant protocol with MDI-QKD in order to address **both** source and detector flaws.

Experiment realization with MDI-QKD

- Implement loss tolerant MDI-QKD with source flaws
- Polarization encoding
- Polarization states characterized by quantum state tomography
- Distance: 10 km and 40 km (SMF-28 optical fiber)
- Repetition rate: 10 MHz

Z. Tang et al., PRA 93, 042308 (2016).

Experimental setup



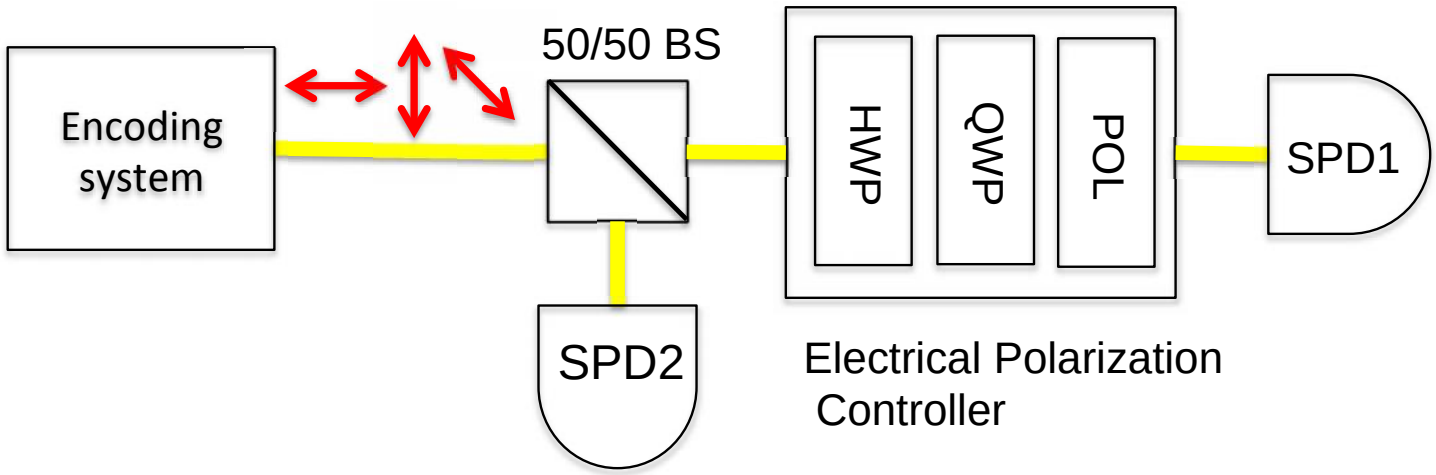
Clock cycle: 500kHz → 10MHz

Detector Efficiency: 10% → 20%.

Z. Tang, *et al.*, Phys. Rev. A, **93,** 042308 (2016)

Z. Tang et al., PRA 93, 042308 (2016).

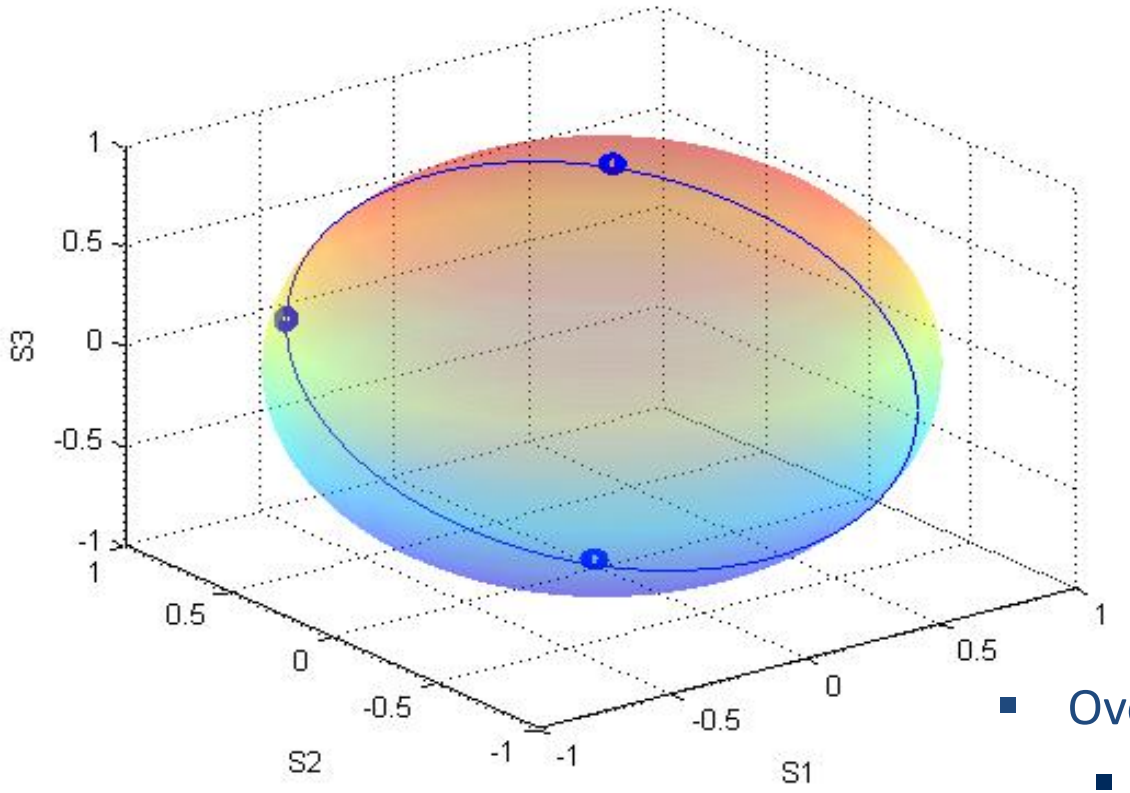
Quantum State Tomography
- quantifying state preparation errors



		Projected states			
		$\|H\rangle$	$\|V\rangle$	$\|D\rangle$	$\|R\rangle$
Alice's states	$\rho_{E,0_Z}$	201311	583	112867	114043
	$\rho_{E,1_Z}$	982	203500	122028	110687
	$\rho_{E,0_X}$	114815	117459	35646	38239
Bob's states	$\rho_{E',0_Z}$	201366	660	113259	117803
	$\rho_{E',1_Z}$	791	201763	109106	116062
	$\rho_{E',0_X}$	118648	110962	18923	57935

Z. Tang et al., PRA 93, 042308 (2016).

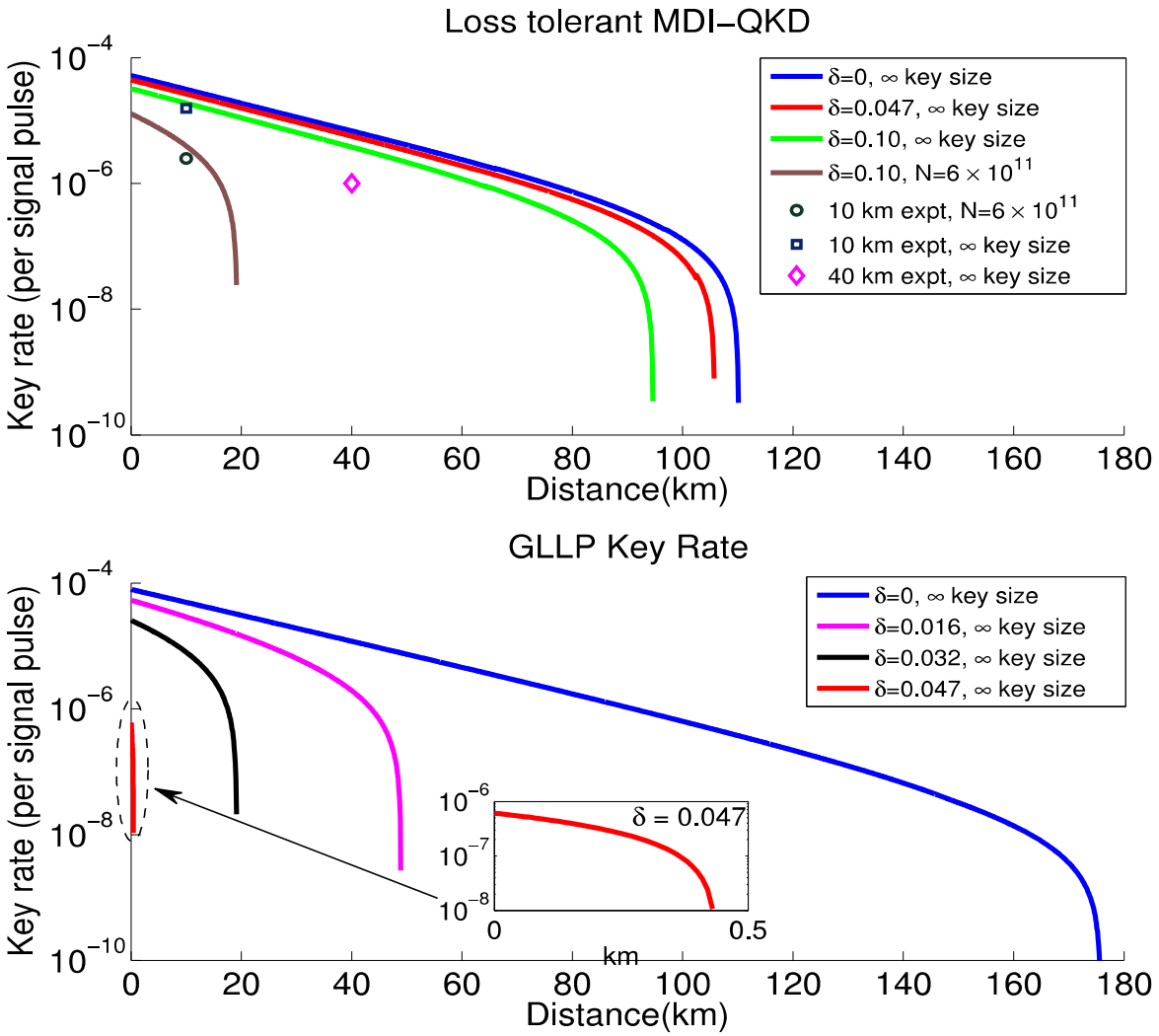
Quantum State Tomography
- quantifying state preparation errors



- Overlap between H, V, and D
  - $F(H, V)^2 = 0.0024 \pm 0.0006$
  - $F(H, D)^2 = 0.4994 \pm 0.0030$
  - $F(V, D)^2 = 0.4963 \pm 0.0028$

Z. Tang et al., PRA 93, 042308 (2016).

Result



With loss-tolerant protocol, the key rate remains quite high for reasonable δ. Great news!

Z. Tang et al., PRA 93, 042308 (2016).

Results

- GLLP gives a pessimistic treatment to combine source preparation errors into key rate estimation
  - Key rate decreases drastically with state preparation errors
- Loss tolerant MDI-QKD
  - Robust against source flaws
- Demonstrated the feasibility to generate secure key even with source flaws in MDI-QKD

Z. Tang et al., PRA 93, 042308 (2016).

Relaxing assumptions at source

1. Perfect encoding – loss-tolerant protocol K. Tamaki et al., Phys. Rev. A, **90**, 052314 (2014).
2. No side channel – verify qubit assumption plus leaky source.

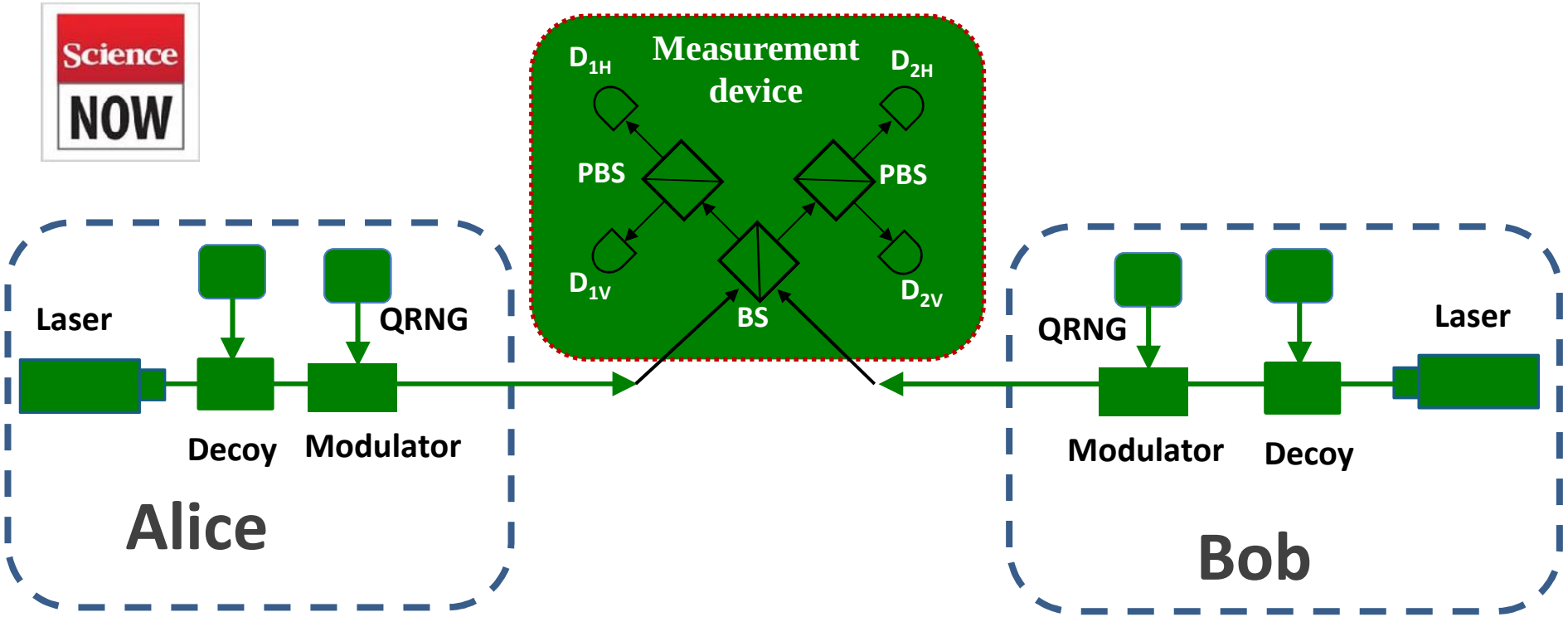
   K. Tamaki, M. Curty and M. Lucamarini, New J. Phys. 18, 065008 (2016).
3. Perfect random numbers – quantum random number generator plus extractor functions See e.g. F. Xu, B. Qi, X. Ma, H. Xu, H. Zheng, and H.-K. Lo, *Opt. Express*, 20, 12366, (2012).
4. Perfect phase randomization – discrete phase randomization

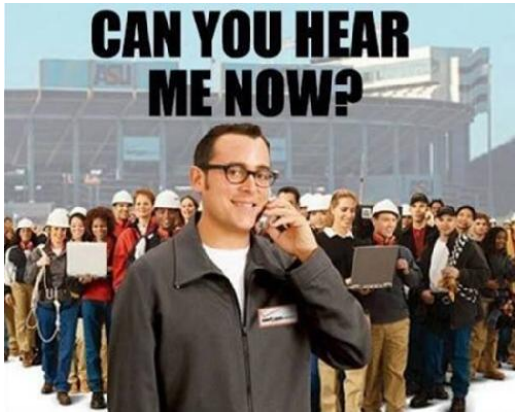
   Z. Cao, Z. Zhang, H.-K. Lo, X. Ma, New J. Phys. 17 053014 (2015).
5. Perfect intensity control – intensity fluctuations allowed

   See e.g. Akihiro Mizutani's talk on Monday.

Is QKD safe again?

http://news.sciencemag.org/physics/2013/08/quantum-cryptography-safe-again





Better dream: Quantum Internet

R. Hughes et al.,
arXiv: 1305.0305

Low cost devices

Janet

Low cost devices

David

Expensive devices in
Untrusted relays/repeaters

Low cost devices

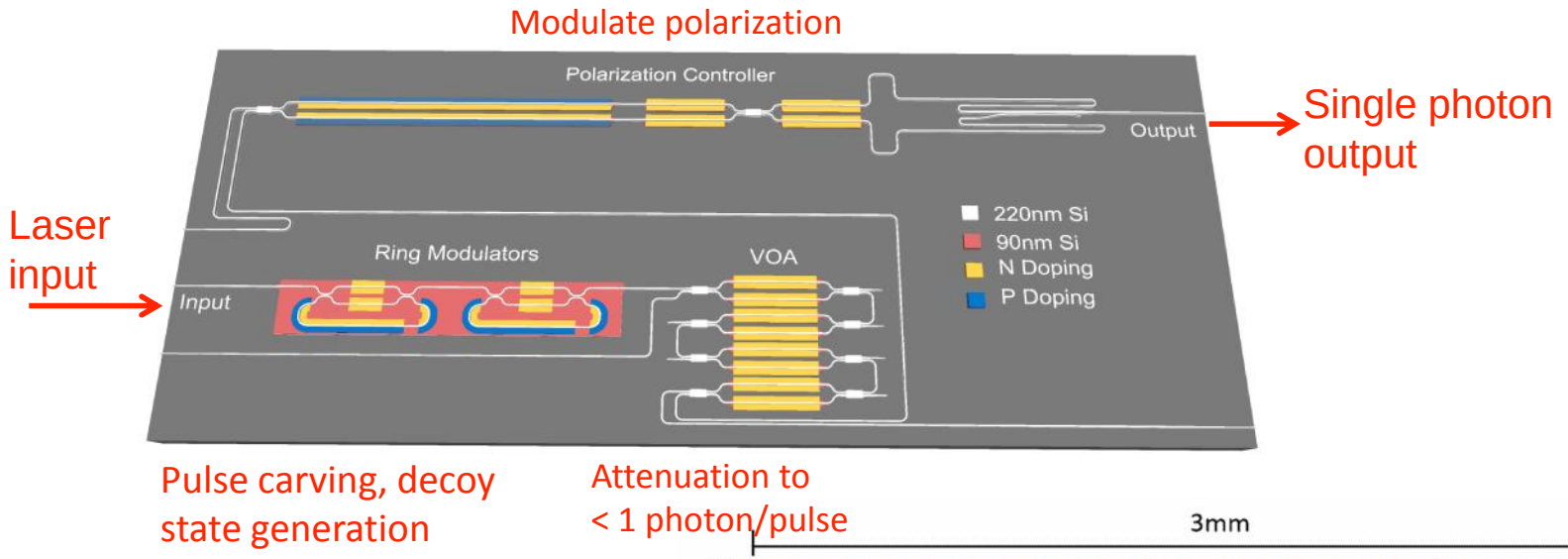
Alice

Low cost devices

Bob

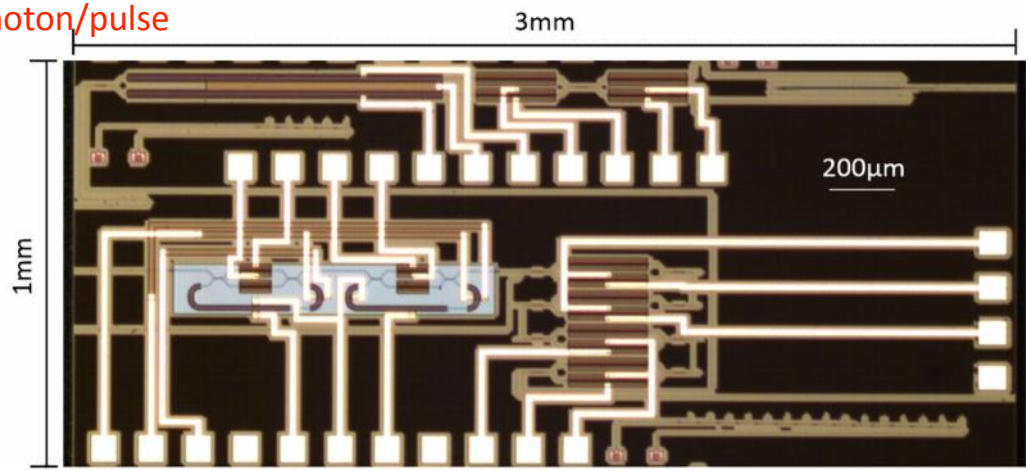
MDI-QKD
Quantum repeaters
Quantum teleportation
Quantum cloud computing
...

Si photonic QKD transmitter
Decoy state, polarization encoded, BB84



First Si integrated photonic QKD transmitter

Fabricated in IME baseline Si photonic process



C. Ma et al., http://arxiv.org/abs/1606.04407 (Collaboration between Lo's group and Joyce Poon's group).

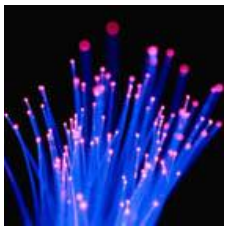
Quantum repeaters may be more difficult than a quantum computer,
if we follow the dogma of the necessity of matter quantum memories.

However, today, we show a new quantum repeater scheme, which is much simpler than a quantum computer and is the ultimate of all optical network.

All-photonic quantum repeaters

Koji Azuma, K. Tamaki & H.-K. Lo, Nat. Commun. **6**, 6787 (2015).

Quantum repeaters → distance



Photon via fiber

See Qcrypt 2015 talk by Koji Azuma for details.

People in my Group

- **Principal Investigator**
  - Hoi-Kwong Lo
- **Grad Students**
  - Olinka Bedroya
  - (Mike) Wenyuan Wang
  - Ilan Tzitrin
  - Chenyang Li
  - (Xiaoqing Zhong
- **Postdoc** Dr. Keith Lee
- **Collaborators**
  - Prof. Li Qian (U. of T.)
  - Prof. Joyce Poon (U. of T.)
  - Prof. V. Makarov (Waterloo)
  - Prof. N. Lutkenhaus (Waterloo)
  - Dr. Feihu Xu (MIT)
  - Dr. Bing Qi (Oak Ridge, US)
  - Prof. M. Curty (U. of Vigo, Spain
  - Dr. K. Tamaki (NTT, Japan)
  - Dr. K. Azuma (NTT, Japan)
  - Prof. X. Ma (Tsinghua U)
  - …

Thank numerous collaborators including e.g. Zhiyuan Tang, Feihu Xu, Bing Qi & Marcos Curty for slide preparation!

Thank You !

- Secure quantum key distribution

  H.-K. Lo, M. Curty and K. Tamaki, *Nature Photonics* **8**, 595–604 (2014).
- MDI-QKD

  H.-K. Lo, M. Curty and B. Qi, *Phys. Rev. Lett*. **108**, 130503 (2012).
- Experimental MDI-QKD with encoding flaws

  Z. Tang et al., *PRA* **93**, 042308 (2016).

See also

- MDI-QKD: F. Xu, M. Curty, B. Qi, L. Qian, H.-K- Lo, *Nature Photonics* **9**, 772–773 (2015) .
- Si chip-based QKD: (collaboration with Prof. Joyce Poon, http://arxiv.org/abs/1606.04407)
- All photonics quantum repeaters: K. Azuma, K. Tamaki, H.-K. Lo, *Nature Commun.* 6, 6787 (2015).

MaRS
INNOVATION.CA
CANADA FOUNDATION FOR INNOVATION | FONDATION CANADIENNE POUR L'INNOVATION
Office of Naval Research ONR Science & Technology
Ontario Research Fund
NSERC CRSNG

Collaborators

Prof. Li Qian
(ECE, U of T.)

Prof. Joyce Poon
(ECE, U. of T.)

Prof. Vadim Makarov
(IQC, Waterloo)

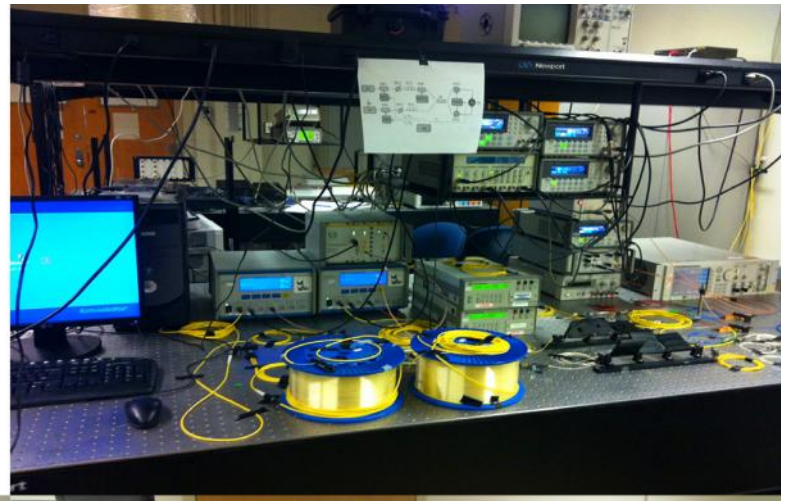
Prof. Norbert Lutkenhaus
(IQC, Waterloo)

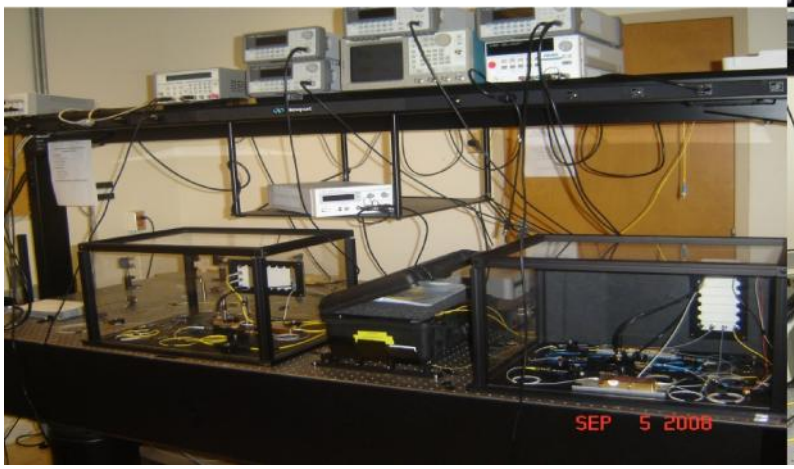
Dr. Kiyoshi Tamaki
(NTT, Japan)

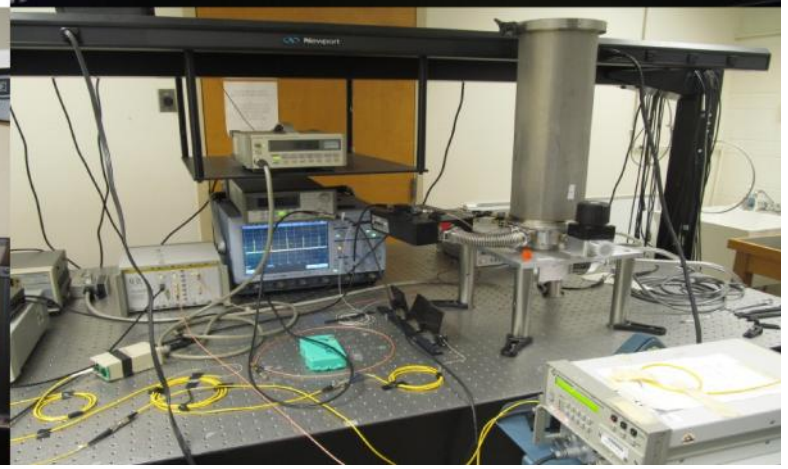
Dr. Koji Azuma
(NTT, Japan)

Prof. Marcos Curty
(U. Of Vigo, Spain)

Our laboratory

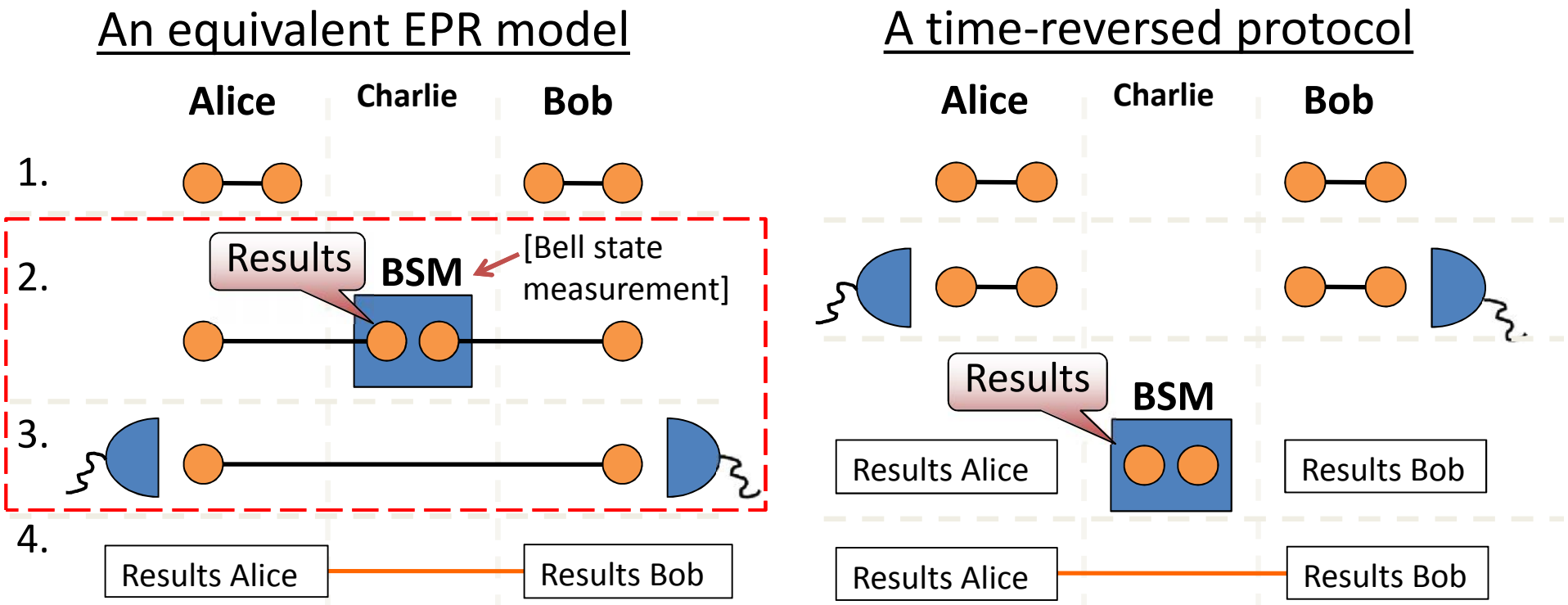






http://www.comm.utoronto.ca/~hklo/index.html

MDI-QKD with single photons



The result of BSM only reveals *correlation* between Alice and Bob but not the value of the individual bits!

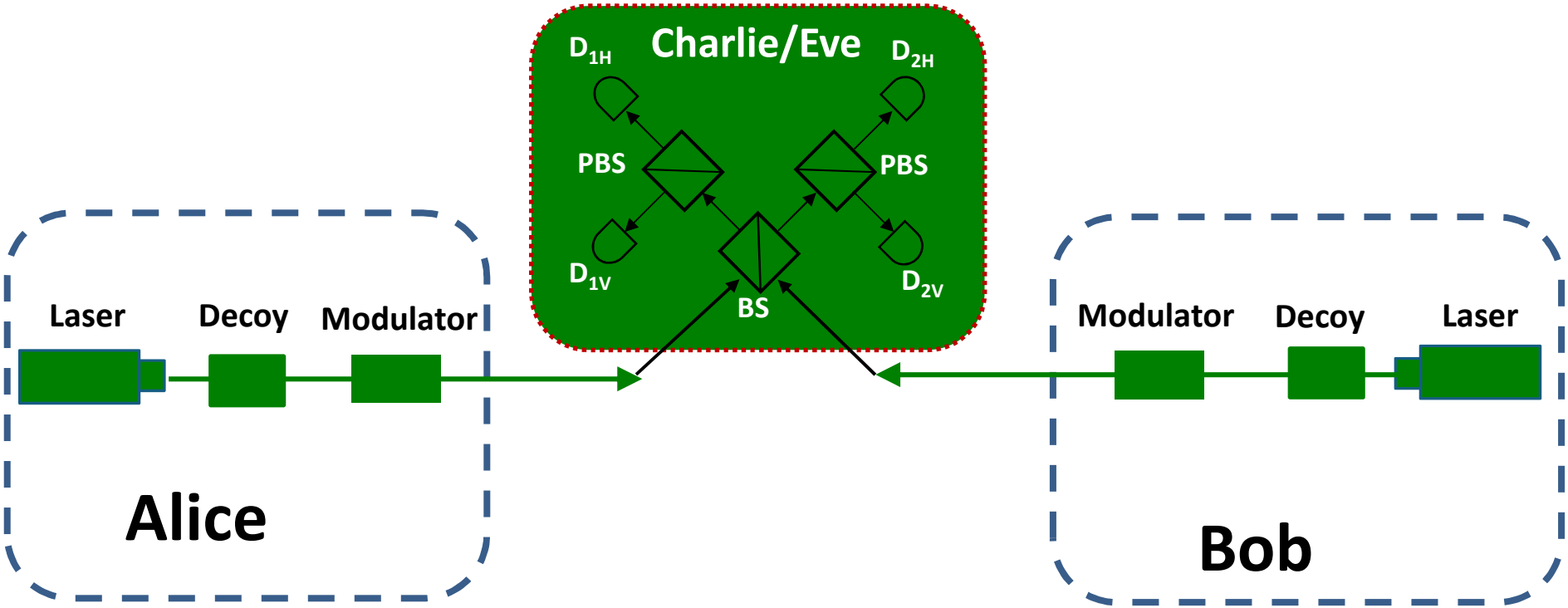
Time-reversed EPR QKD

E. Biham, B. Huttner, and T. Mor, Phys. Rev. A, 54(4):2651 (1996)

H. Inamori, Algorithmica 34, pp. 340-365 (2002).

See also, S. L. Braunstein and S. Pirandola, PRL 108, 130502 (2012).

MDI-QKD with Decoy States



Assumption: Alice and Bob trust their state preparation.

Great Advantage: Charlie can be totally untrusted. No need to certify detectors!

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

Results

- Key Rate Estimation

$$R = q\{Q_{11}^{rect}[1 - H_2(e_{11}^{diag})] - Q_{\mu\mu}^{rect} f(E_{\mu\mu}^{rect}) H_2(E_{\mu\mu}^{rect})\}$$

Privacy amplification

Error correction

- q : fraction of pulses used for key generation
  Both Alice and Bob send signal states in rectilinear basis
- Q_{11}^{rect} : Gain of single photon component
- e_{11}^{diag} : Quantum bit error rate of single photon component
- $Q_{\mu\mu}^{rect}$: Gain of signal states
- $E_{\mu\mu}^{rect}$: Quantum bit error rate of signal states

- Measured from experiment
  Gain $Q_{\mu\mu}^{rect}$, Error Rate $E_{\mu\mu}^{rect}$
- Estimated gain and error rate of single photon pulses using two decoy-state method
  Gain Q_{11}^{rect} , Error Rate e_{11}^{diag}

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

Other research directions in MDI-QKD

- Phase encoding MDI-QKD (without qubit assumption).

  K. Tamaki, H.-K. Lo, C.-H. F. Fung and B. Qi., Phys. Rev. A 85, 042307 (2012).

- Entanglement witness for MDI-QKD

  C. Branciard, D. Rosset, Y.-C. Liang, and N. Gisin, Phys. Rev. Lett. 110, 060405 (2013); P. Xu et al., Phys. Rev. Lett. 112, 140506 (2014).

- Square root improvement of the key rate for MDI-QKD

  Memory-Assisted: C. Panayi, M. Razavi, X. Ma and N. Lütkenhaus, New J. Phys. 16, 043005 (2014); S. Abruzzo, H. Kampermann, and D. Bruß, Phys. Rev. A 89, 012301 (2014).

  Without memory: K. Azuma, K. Tamaki, W. J. Munro, Nat. Comm. 6, 10171 (2015)

- MDI-QKD with entangled source

  F. Xu, B. Qi, Z. Liao, H.-K. Lo, Appl. Phys. Lett., 103, 061101 (2013).

- Continuous variable (CV)-MDI-QKD

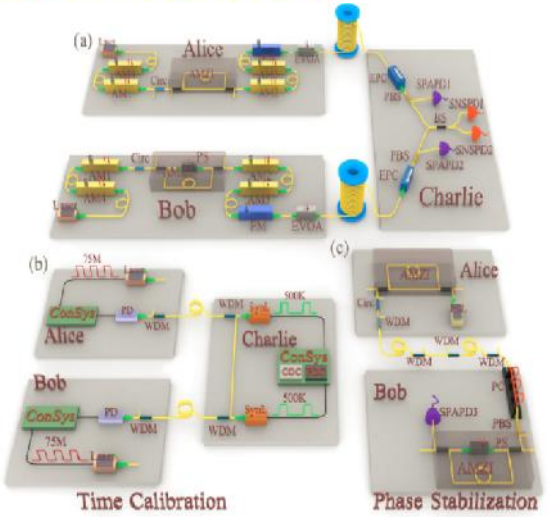
  e.g. Z. Li et al., PRA 89, 052301 (2014); X.C. Ma et al, PRA 89, 042335 (2014); S. Pirandola et al., Nature Photonics 9, 397–402 (2015). C. Ottavinai et al., Phys. Rev. A 91, 022320 (2015), S. Pirandola et al., Nature Photonics 9, 773-775 (2015), N. Hosseinidehaj and R. Malaney, https://arxiv.org/abs/1605.05445

Long distance MDI-QKD experiment

Measurement-device-independent quantum key distribution over 200 km

Yan-Lin Tang, Hua-Lei Yin, Si-Jing Chen, Yang Liu, Wei-Jun Zhang, Xiao Jiang, Lu Zhang, Jian Wang, Li-Xing You, Jian-Yu Guan, Dong-Xu Yang, Zhen Wang, Hao Liang, Zhen Zhang, Nan Zhou, Xiongfeng Ma, Teng-Yun Chen, Qiang Zhang, Jian-Wei Pan

(Submitted on 30 Jul 2014)



- Repetition rate: 75 MHz
- **Superconducting nanowire single-photon detectors (SNSPD): 40% efficiency**
- Key rate: 100 bits/s over 50km fiber
- Distance: up to 200 km
- Y.-L. Tang et al., Phys. Rev. Lett. 113, 190501 (2014).
- Also, for a field test, see Y.-L. Tang et al., IEEE J. Sel. T. Quantum Electron. 21, 6600407 (2014).

Results

$$R \geq Q_{11}^{Z}[1-H_2(e_{11}^{X})]-Q_{\mu\mu}^{Z} f(E_{\mu\mu}^{Z}) H_2(E_{\mu\mu}^{Z})$$

	Data size	Security bound	Q_{11}^{z}	e_{11}^{x}	$Q_{\mu\mu}^{Z}$	$E_{\mu\mu}^{Z}$	R (per signal)
10 km	6×10^{11}	10^{-3}	3.96×10^{-5}	0.189	6.31×10^{-5}	0.0178	2.48×10^{-6}
10 km	∞	n/a	4.17×10^{-5}	0.079	6.31×10^{-5}	0.0178	1.57×10^{-5}
40 km	∞	n/a	1.88×10^{-5}	0.122	2.94×10^{-5}	0.0368	1.00×10^{-6}

Z. Tang et al., PRA 93, 042308 (2016).

Table 7.1: Summary of reported MDI-QKD demonstrations

	Our work [49]	Ref. [67]	Ref. [66]	Ref. [68]	Ref. [69]	Ref. [70]	Our work [53]
Encoding scheme	polarization	time bin	time bin	polarization	time bin	time bin	polarization
Environment	fiber spool	fiber spool	field test	fiber spool	fiber spool	field test	fiber spool
Clock rate	500 kHz	1 MHz	2 MHz	1 MHz	75 MHz	75 MHz	10 MHz
Distance	10 km	50 km	18.6 km	17 km	200 km	30 km	10 km
Random key bit & intensity switching?	Yes	Yes	No	No	Yes	Yes	Yes
Real time random number generation?	No	Yes	No	No	Yes	Yes	No
Considering encoding flaws?	No	No	No	No	No	No	Yes
Verification of pulse intensity?	No	No	No	No	No	No	No
Key rate (finite-key correction)	0.005 bps (bits per second)	0.1 bps	not reported	not reported	0.02 bps	17 bps	0.5 bps
Key rate (no finite-key correction)	3 bps	not reported	2 bps	1 bps	not reported	not reported	157 bps

More recent experiments.

- MDI-QKD network, Y.L. Tang et al., PRX 6, 011024 (2016).
- MDI-QKD with > 1 Mbps key rate. L. C. Comandar et al., Nature Photonics, 10 312 (2016).
- MDI-QKD with 404km, H.-L. Yin et al., http://arxiv.org/abs/1606.06821

Also, CV-MDI-QKD: e.g. S. Pirandola et al., Nature Photonics 9, 397–402 (2015).

Parameters used in simulation

Detector efficiency [1]	Channel misalignment [2]	Dark count rate [1]	ECC inefficiency [3]
93%	0.1%	10	1.16

All based on real experimental parameters.

[1] F. Marsili et al., *Nature Photonics* **7**, 210-214 (2013).
[2] Y.-L., Tang et al., *Phys. Rev. Lett.* **113**, 190501 (2014).
[3] G. Brassard and L. Savail, *Lect. Notes. Comp. Sci.* **765**, 410-423 (1994).

MDI-QKD has high key rate and is highly suitable for both metropolitan distance and long-distance communications.

See also R. Valivarthi *et al.*, http://arxiv.org/abs/1501.07307
(Published on-line in Journal of Modern Optics)

Decoy state QKD with a leaky source

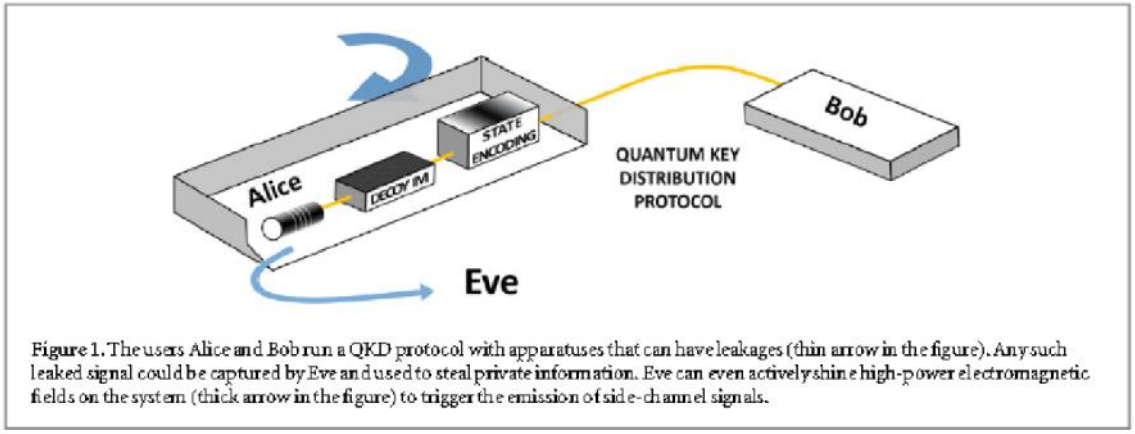
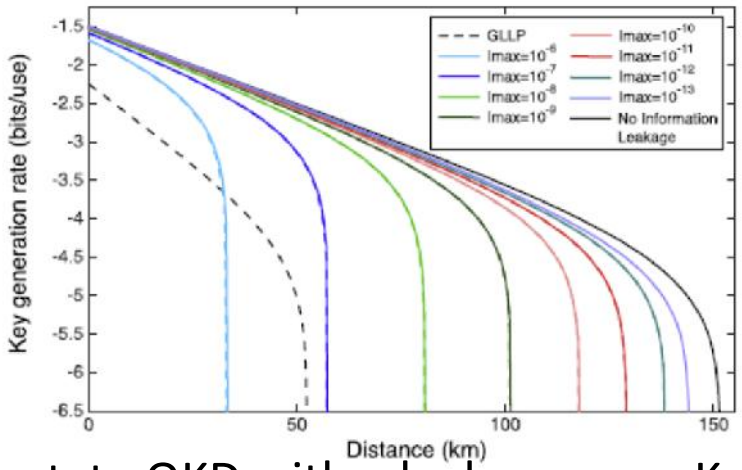


Figure 1. The users Alice and Bob run a QKD protocol with apparatuses that can have leakages (thin arrow in the figure). Any such leaked signal could be captured by Eve and used to steal private information. Eve can even actively shine high-power electromagnetic fields on the system (thick arrow in the figure) to trigger the emission of side-channel signals.



Decoy state QKD with a leaky source, K. Tamaki, M. Curty and M. Lucamarini, New J. Phys. 18, 065008 (2016).

High-speed quantum random number generator (QRNG) prototype

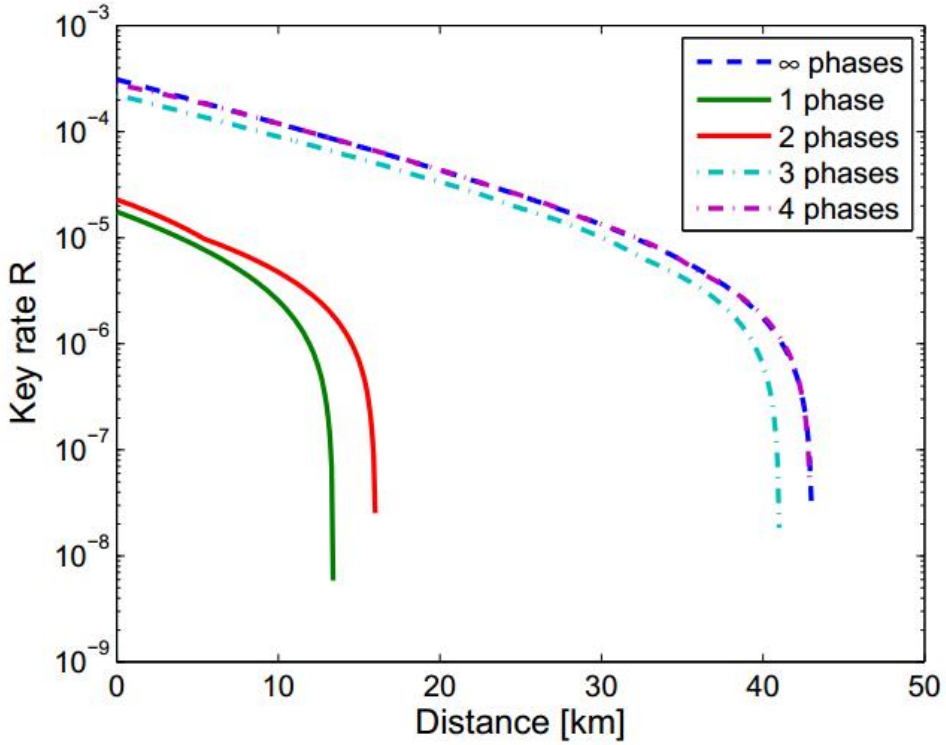
Many different proposals for QRNGs from many groups. For example: using Phase Noises of a laser operating slightly above threshold.

http://www.comm.utoronto.ca/~hklo/QRNG/Quantoss.html

F. Xu, B. Qi, X. Ma, H. Xu, H. Zheng, and H.-K. Lo, *Opt. Express*, 20, 12366, (2012); US Patent # 8,554,814 (2013) by B. Qi, H.-K. Lo, and L. Qian.

Discrete phase randomization

- Previously, decoy state BB84 required *perfect* phase randomization (assumption 4), which requires ***infinite*** bits of random numbers.
- We show how to achieve secure decoy state BB84 with only a ***few*** bits per signal pulse.



Z. Cao, Z. Zhang, H.-K. Lo, X. Ma, New J. Phys. 17 053014 (2015).

Intensity fluctuations

- Assume that the intensity of the emitted light lies in a certain interval except for small probability ε .
- Assume also that the phase modulation lies in a certain interval except for a small probability ε .
- Use tagging idea in GLLP to prove security for a decoy state QKD protocol.

Towards secure QKD with testable assumptions on modulation devices. See A. Mizutani's talk.

K. Azuma, K. Tamaki and HKL, Nat. Commun. **6**, 6787 (2015).

All-photonic quantum repeaters

This protocol uses only

- Linear optical elements
- Single-photon sources
- Photon detectors
- Fast active feedforward techniques

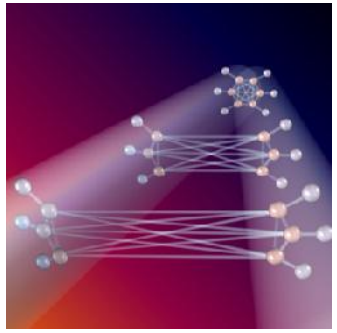


Image from the web site of Nature Commun. [http://www.nature.com/ncomms/archive/date/2015/04/index.html]

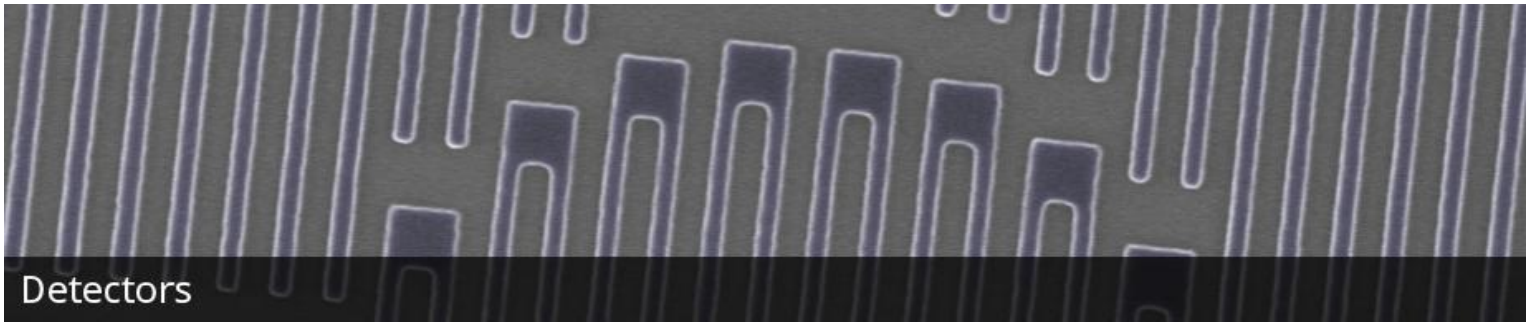
Distinguished advantages:

- Repetition rate of this protocol could be increased as high as one wants.
- Coherent frequency converters for photons could be unnecessary.
- All the elemental components are simpler than matter quantum memories.
- It could work at room temperature.
- It is proved to be much simpler than the KLM quantum computer.

The main idea:

"Time reversal" of DLCZ-type quantum repeaters.

Commercial high-efficiency single-photon detectors

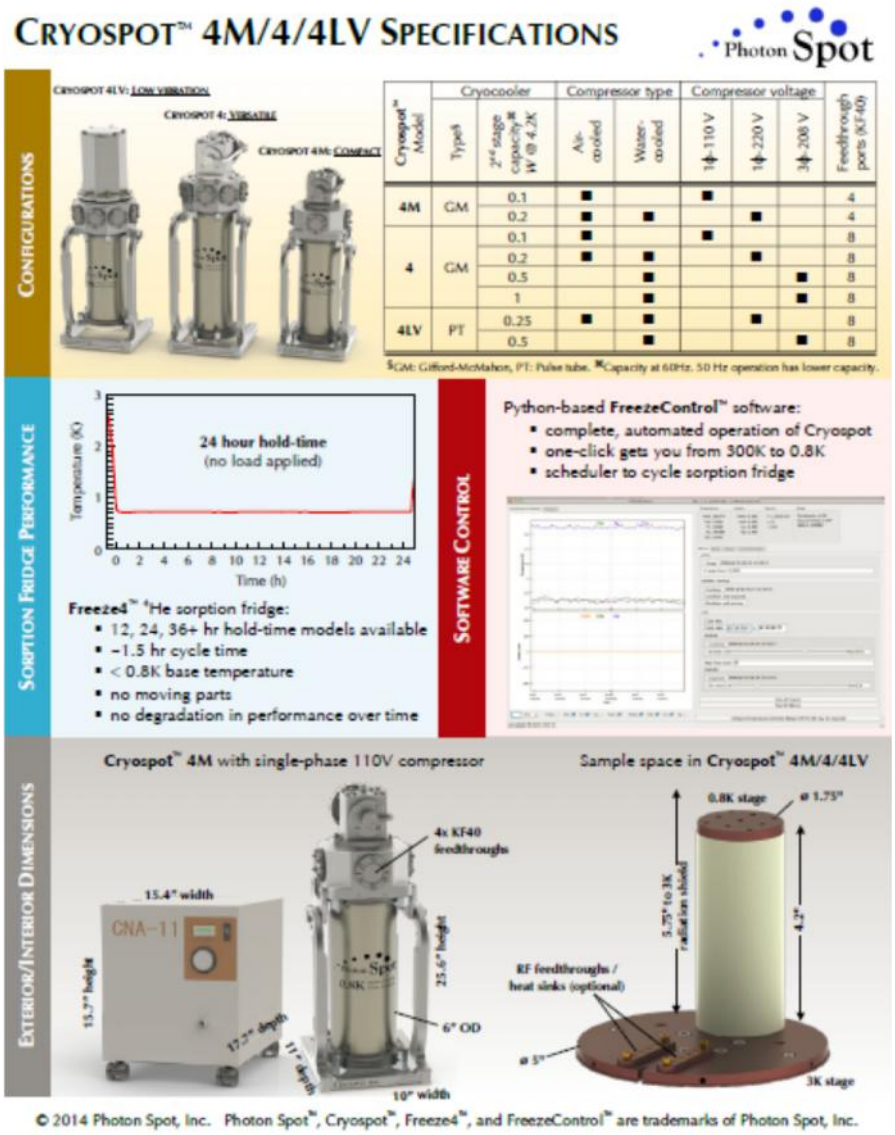


Some firms (e.g. Photon Spot) offer commercial

superconducting nanowire single photon detectors (SNSPDs).

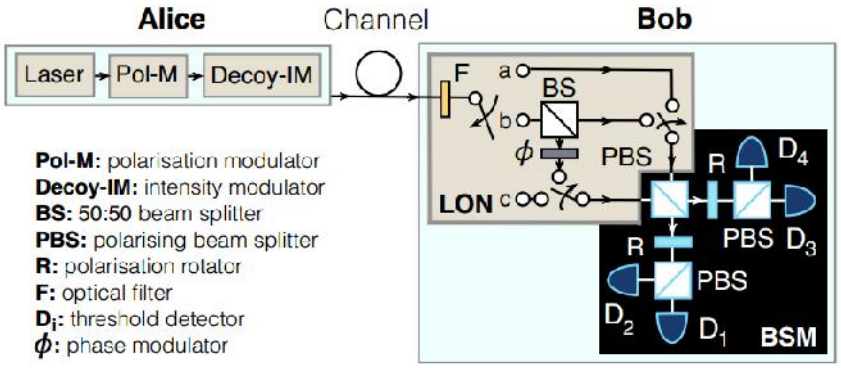
- Extremely low dark counts
- 30-50 picosecond timing jitter
- **>90% quantum efficiency near 1550nm**
- Reset times of 3 - 30 nanoseconds
- Ability to distinguish multi-photon events.

See e.g. http://www.photonspot.com/detectors

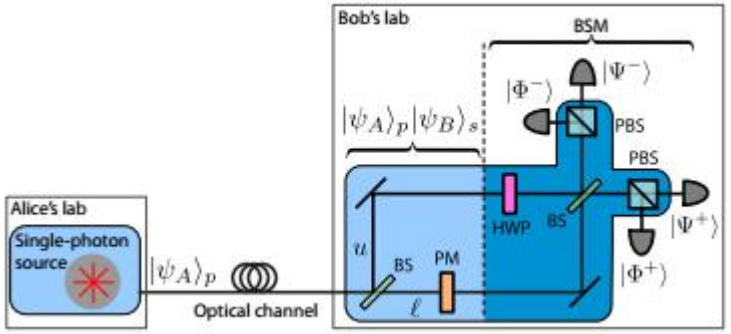


It claims that “one-click gets you from 300K to 0.8K.”

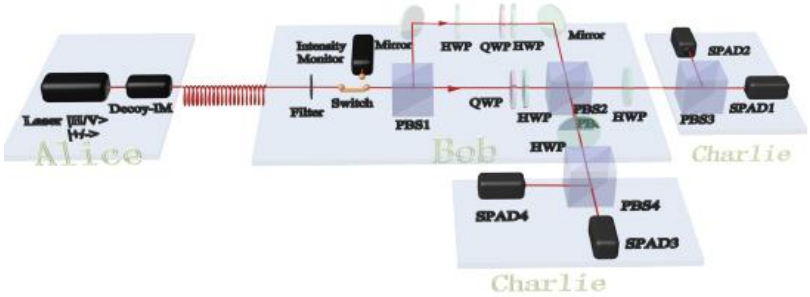
Recent protocols inspired by MDI-QKD



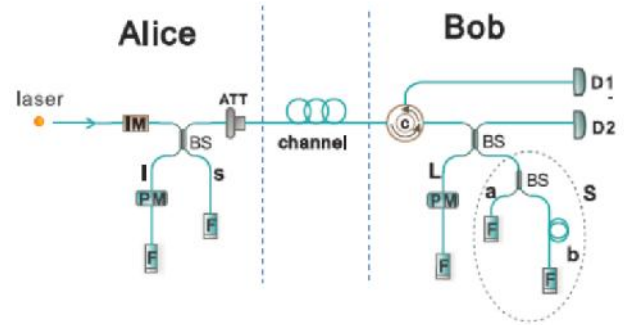
P. Gonzalez *et al.*, *arXiv* 1410.1422 (2014)



C. C. W. Lim *et al.*, Appl. Phys. Lett. 105, 221112 (2014).



W. Cao *et al.*, *arXiv* 1410, 2928 (2014)



W.-Y. Liang *et al.*, *arXiv* 1505.00897 (2015)

Are single-photon Bell-state QKD protocols secure?

Security loophole where Eve, in principle, sends Bob multi-photon signals (in a Trojan Horse attack) and replaces detection system with faulty components.

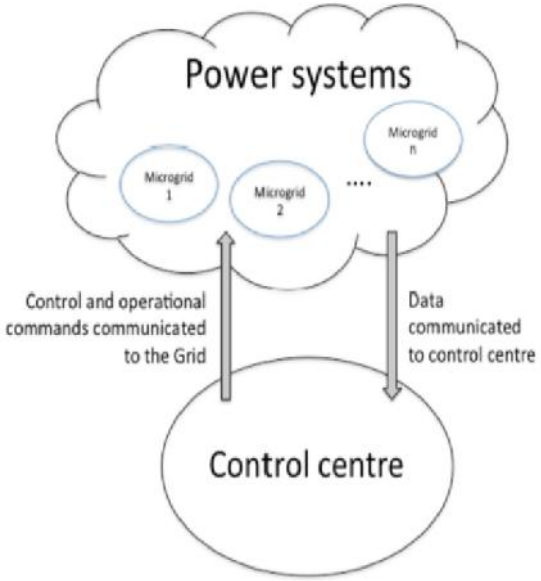
B. Qi, Phys. Rev. A 91, 020303 (R) (2015)

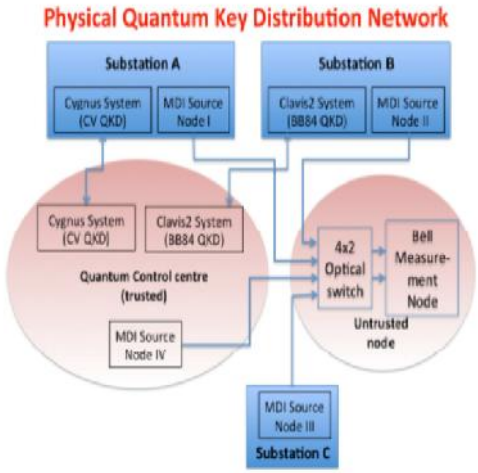
Insecurity of detector-device-independent quantum key distribution

Shihan Sajeed, Anqi Huang, Shihai Sun, Feihu Xu, Vadim Makarov, Marcos Curty, http://arxiv.org/abs/1607.05814

See Friday afternoon's talk by Anqi Huang.

Smart Grid: Cyber-Physical Operation, Security and Quantum Technology





At U. of T., an interdisciplinary team consisting of

- Prof. Deepa Kundur (Communication Security)
- Prof. Reza Iravani (Energy Systems),
- Prof. Li Qian (Photonics)
- Prof. Hoi-Kwong Lo (Quantum Communication)

has been formed to study smart grid and quantum technologies.

Deepa Kundur

Reza Iravani

Hackers caused power cut in western Ukraine - US

BBC News, 12 January 2016

“The attack caused a blackout for 80,000 customers of western Ukraine's Prykarpattyaoblenergo utility.”

“DHS said the "BlackEnergy Malware" used in the attack appears to have infected Ukraine's systems via a corrupted Microsoft Word attachment.”

Outline

1. Introduction: security of practical QKD
2. **Source security: QKD with source flaws**
3. Detection security: measurement-device-independent QKD
4. Summary

Assumptions at source

1. Perfect Encoding
2. No side channel
3. Perfect random numbers
4. Perfect Phase Randomization

See also M. Lucamarini et al., Practical security bounds against the Trojan-horse attack in quantum key distribution, http://arxiv.org/abs/1506.01989

Relaxing assumptions at source

1. Perfect Encoding – loss-tolerant protocol
2. No side channel – verify qubit assumption
3. Perfect random numbers – quantum random number generator plus extractor functions
4. Perfect Phase Randomization – discrete phase randomization

Problem with previous BB84 experiments

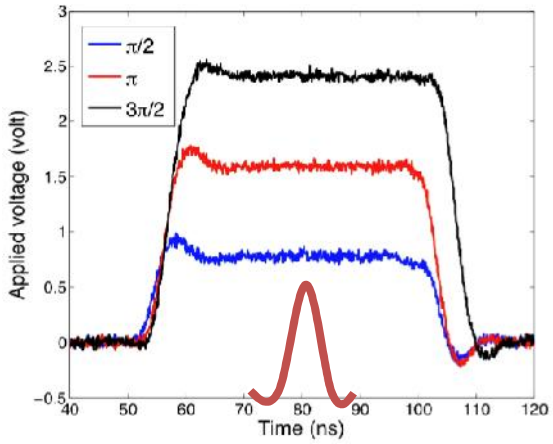
Previous experiments do ***not*** consider source flaws.

- Perfect phase: {0, π/2, π, 3π/2}
- Perfect polarization: {H, D, V, A}

But, in experiment, phase modulators are inaccurate:

- $\{0 \pm \delta_0, \pi/2 \pm \delta_1, \pi \pm \delta_2, 3\pi/2 \pm \delta_3\}$
- $\{H \pm \delta'_0, D \pm \delta'_1, V \pm \delta'_2, A \pm \delta'_3\}$

Phase Modulator

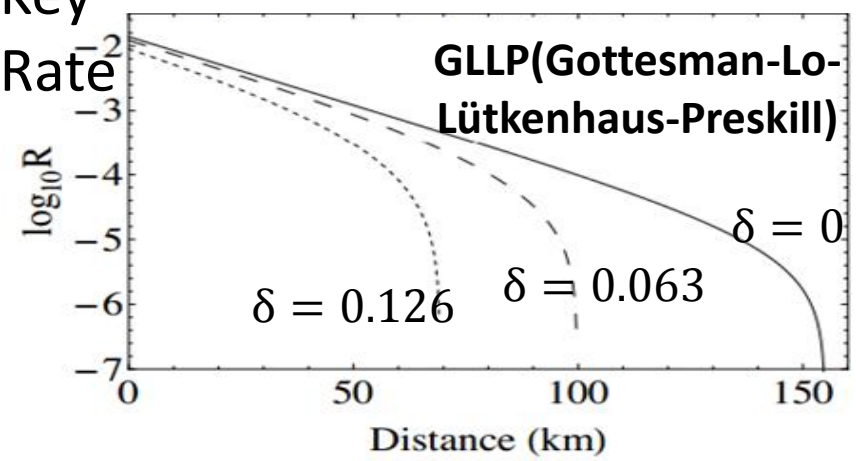


Owing to source flaws, key may ***not*** be proven secure!

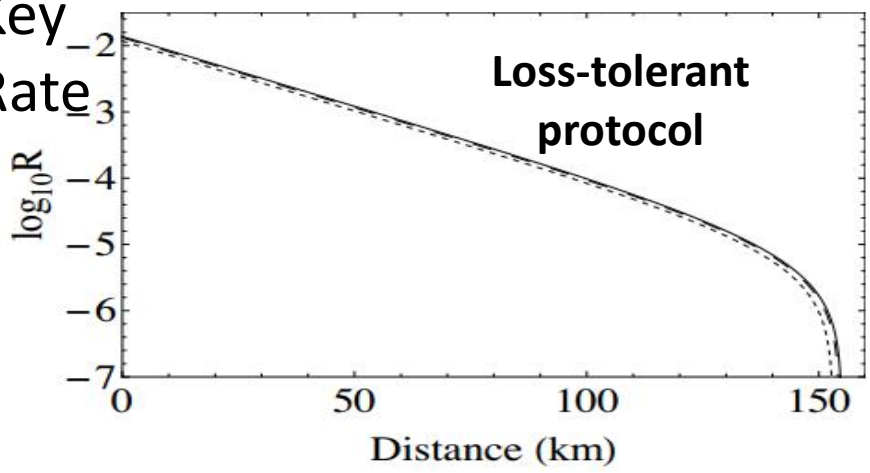
Solution: Loss-tolerant protocol

- "qubit assumption": the four BB84 states remain inside two-dimensional Hilbert space.
- USD (unambiguous state discrimination) attack **impossible**.
- Eve **cannot** enhance source flaws via the channel loss.
- Three states {H, D, V} have the same performance as {H, D, V, A}.
- Uses basis mismatch events to achieve high performance.

Key Rate



Key Rate



K. Tamaki *et al*., PRA 90, 052314 (2014). See also Z.-Q. Ying *et al.,* PRA 90, 052319 (2014);

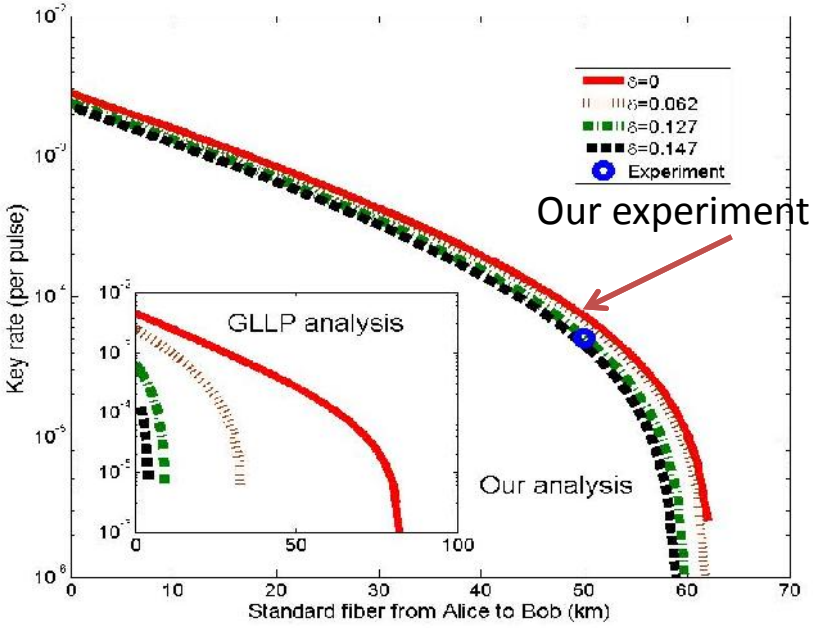
A. Mizutani *et al*., http://arxiv.org/abs/1504.08151

GLLP: Gottesman, Lo, Lütkenhaus and Preskill, QIC 5, 325 (2004).

Experimental loss-tolerant QKD

- Performed experiment to characterize encoding flaws in two commercial systems. Encoding error: $\delta < 0.127$ for ID-500 system with confidence level $\varepsilon = 10$
- Verified the qubit assumption with high accuracy.
- Experimental QKD with source flaws over 50km fiber on ID-500: QBER=2.89%, Key rate=260 bit/s.

Mode	Filter and Estimated result
Spatial	Single-mode fiber
Spectral	Band pass filter
Timing	Synchronization ($1- F=10^{-8}$)
Polarization	Polarizer ($1- F=10^{-7}$)



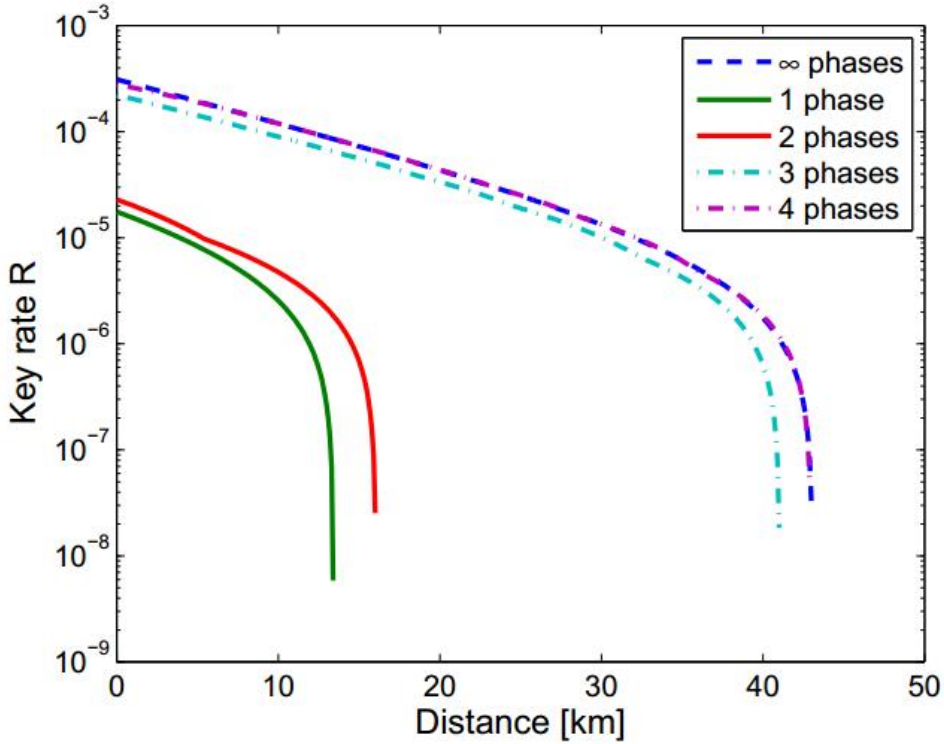
F. Xu, S. Sajeed, S. Kaiser, Z. Tang, L. Qian, V. Makarov, H.-K. Lo, Phys. Rev. A 92, 032305 (2015)

Discrete phase randomization

- Previously, decoy state BB84 required *perfect* phase randomization (assumption 4), which requires ***infinite*** bits of random numbers.
- We show how to achieve secure decoy state BB84 with only a ***few*** bits per signal pulse.

$$|\alpha e^{i\theta}\rangle$$

$$\{\theta_k = \frac{2\pi k}{N} | k = 0, 1, \ldots, N-1\}.$$



Z. Cao, Z. Zhang, H.-K. Lo, X. Ma, *New J. Phys.* **17**, 053014 (2015).

Parameters used in simulation

Detector efficiency [1]	Channel misalignment [2]	Dark count rate [1]	ECC inefficiency [3]
93%	0.1%	10	1.16

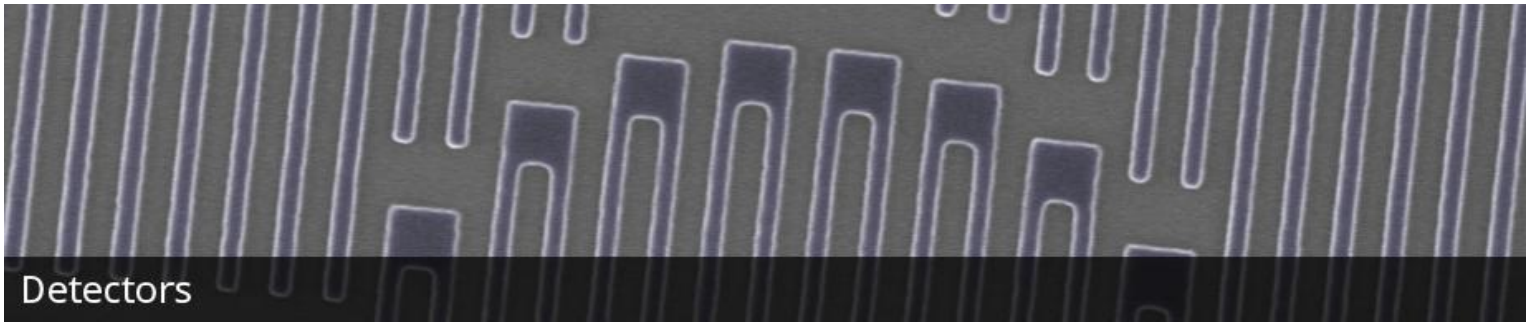
All based on real experimental parameters.

[1] F. Marsili et al., *Nature Photonics* **7**, 210-214 (2013).
[2] Y.-L., Tang et al., *Phys. Rev. Lett.* **113**, 190501 (2014).
[3] G. Brassard and L. Savail, *Lect. Notes. Comp. Sci.* **765**, 410-423 (1994).

MDI-QKD has high key rate and is highly suitable for both metropolitan distance and long-distance communications.

See also R. Valivarthi *et al.*, http://arxiv.org/abs/1501.07307
(Published on-line in Journal of Modern Optics)

Commercial high-efficiency single-photon detectors

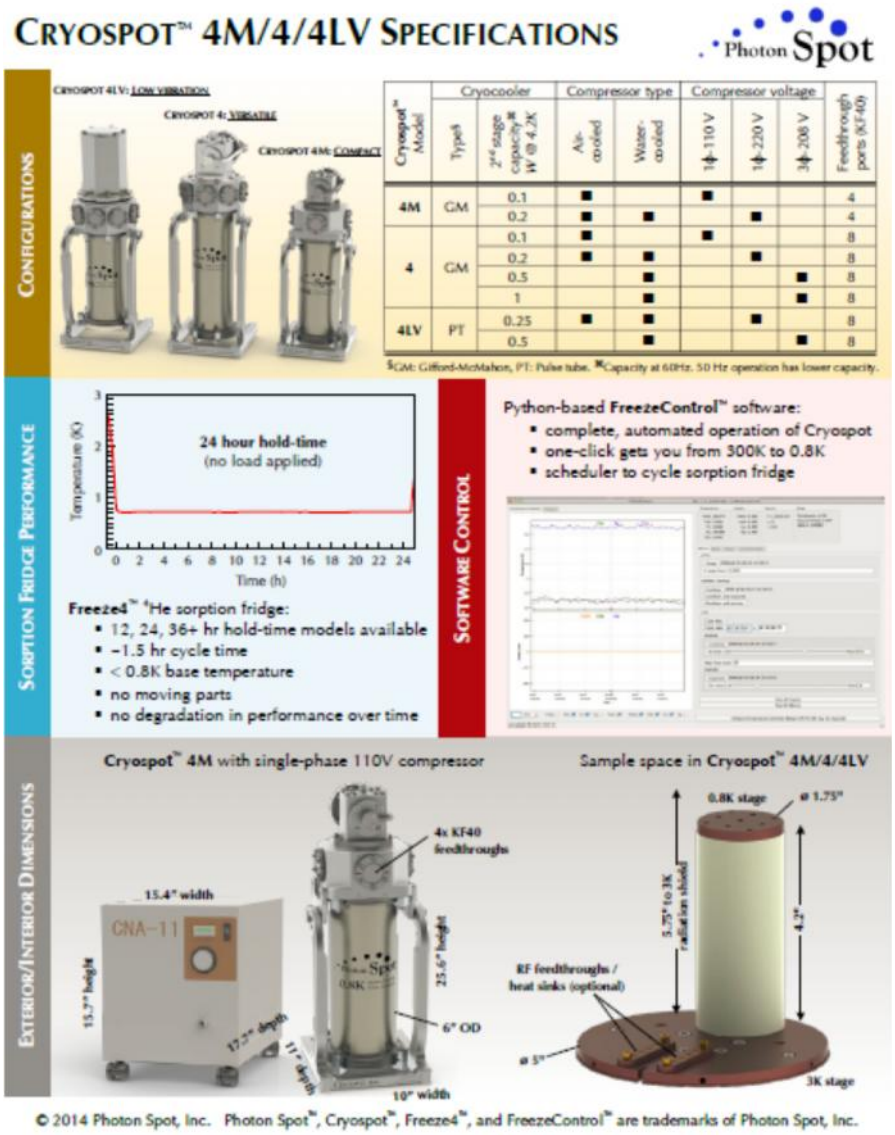


Some firms (e.g. Photon Spot) offer commercial

superconducting nanowire single photon detectors (SNSPDs).

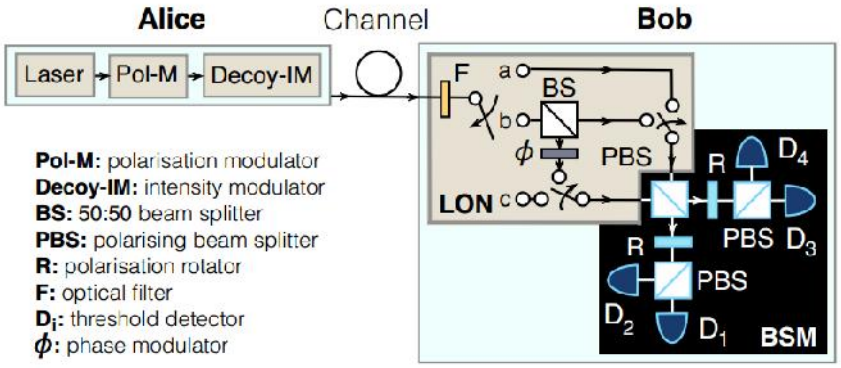
- Extremely low dark counts
- 30-50 picosecond timing jitter
- **>90% quantum efficiency near 1550nm**
- Reset times of 3 - 30 nanoseconds
- Ability to distinguish multi-photon events.

See e.g. http://www.photonspot.com/detectors

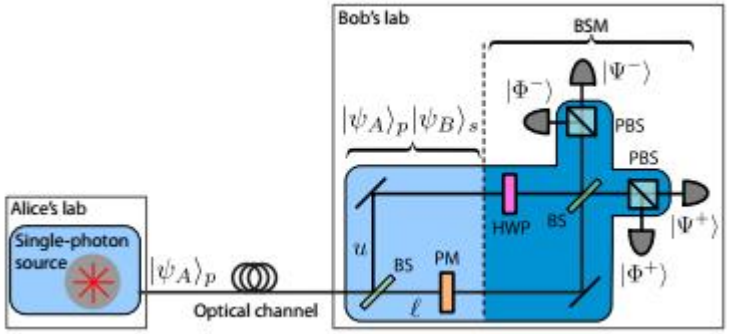


It claims that “one-click gets you from 300K to 0.8K.”

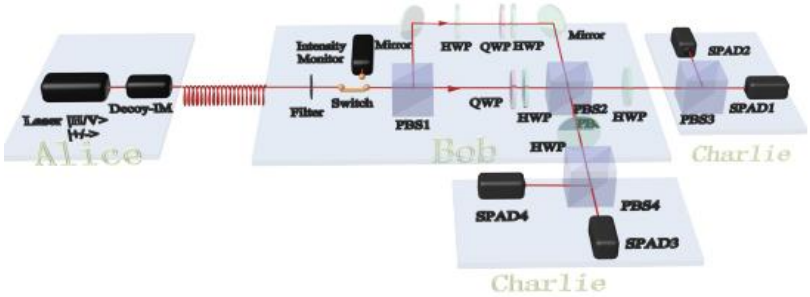
Recent protocols inspired by MDI-QKD



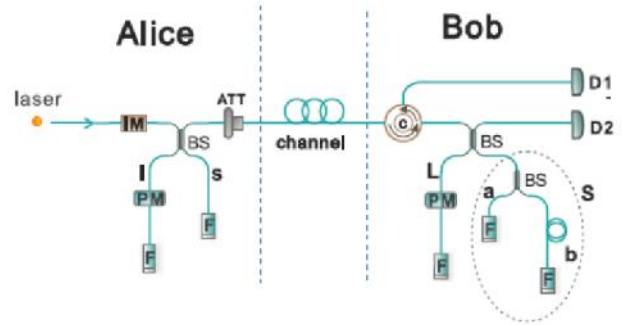
P. Gonzalez *et al.*, *arXiv* 1410.1422 (2014)



C. C. W. Lim *et al.*, Appl. Phys. Lett. 105, 221112 (2014).



W. Cao *et al.*, *arXiv* 1410, 2928 (2014)



W.-Y. Liang *et al.*, *arXiv* 1505.00897 (2015)

Are single-photon Bell-state QKD protocols secure?

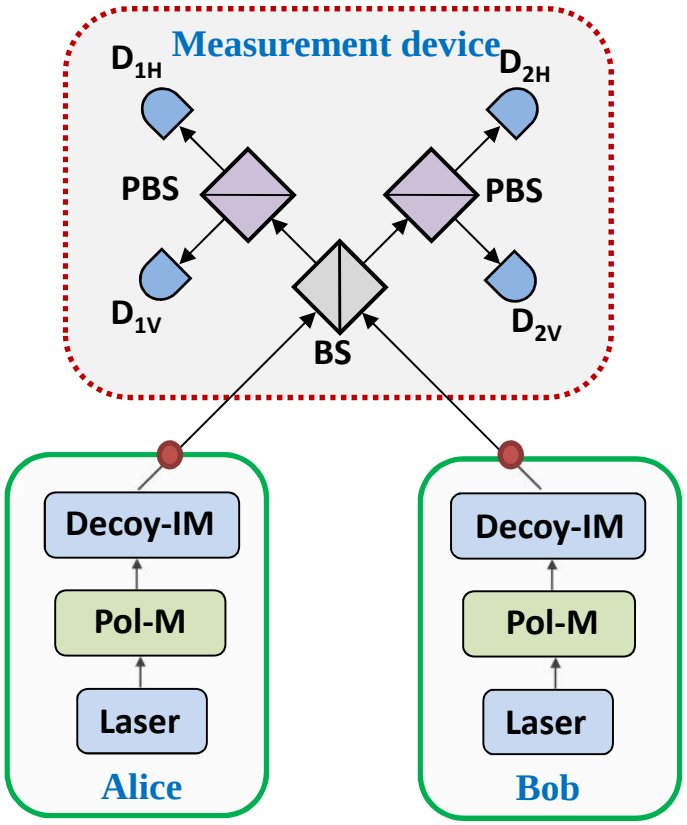
Security loophole where Eve, in principle, sends Bob multi-photon signals (in a Trojan Horse attack) and replaces detection system with faulty components.

B. Qi, Phys. Rev. A 91, 020303 (R) (2015)

List of major practical issues

1. Decoy-state estimation for laser source
   - How many decoy states for a tight estimation?
2. Finite-key analysis
   - Composable security analysis in a practical setting?
3. Parameter optimization
   - Ignored in all previous theories and experiments
4. Practical implementation
   - A real demonstration with off-the-shelf components?

Practical decoy-state method



Secure key rate

$$R \geq P_Z^{1,1} Y_Z^{1,1} \left[1 - H_2\left(e_X^{1,1}\right)\right] - Q_Z f_e(E_Z) H_2(E_Z)$$

- **Goal:** estimate a lower bound of the yield $Y_{Z,L}^{1,1}$ and an upper bound of the error rate $e_{X,U}^{1,1}$.

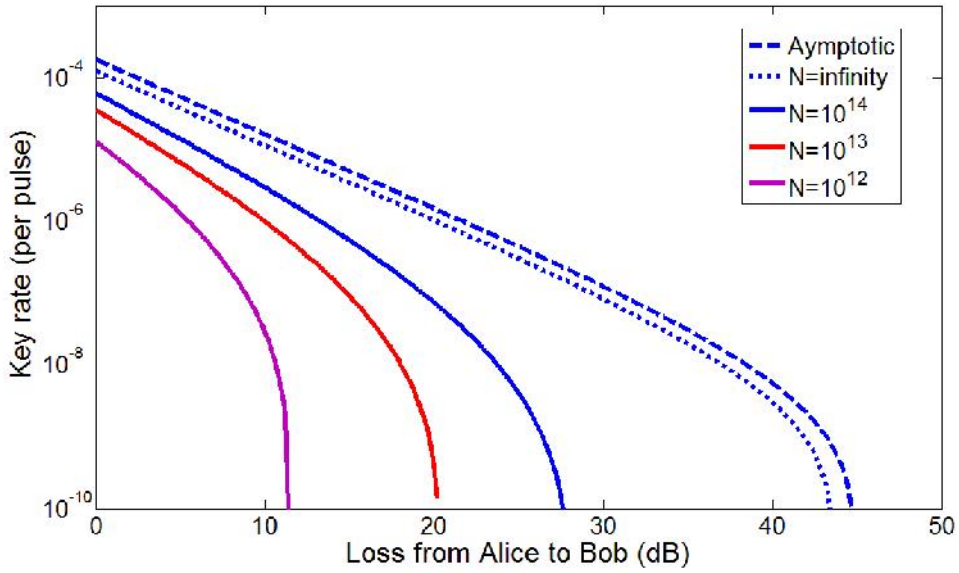
- Finite decoy-state method:
  - Modulate two Lasers by different intensities.
  - Measure corresponding Gains and QBERs.
  - Estimate single-photon using post-selections.

Two decoy states are enough to provide a tight estimation!

F. Xu, M. Curty, B. Qi, H.-K. Lo, *New J. Phys.*, **15**, 113007, 2013
See also, e.g., X. Ma, C.-H. F. Fung and M. Razavi, Phys. Rev. A 86, 052305 (2012);
X. B. Wang, Phys. Rev. A, 87, 012320 (2013).

Finite-key analysis

A finite-key security bound using smooth entropies and a novel parameter estimation using a new modified Chernoff bound.



- For a 1 GHz system and 15% detector, Alice and Bob can distribute a 1 Mb key over a 75 km fibre within 3 hours.

MDI-QKD is feasible within a reasonable time-frame!

M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, H.-K. Lo, *Nat. Comm.*, **5**, 3732 (2014);
Also, T. T. Song, Q.-Y. Wen, F.-Z. Guo, and X.-Q. Tan, Phys. Rev. A 86, 022332 (2012).