Experimental QKD with source flaws and tight finite-key analysis

Feihu Xu[1], Shihan Sajeed[2], Sarah Kaiser[2], Zhiyuang Tang[3], Li Qian[1], Vadim Makarov[2], Hoi-Kwong Lo[1,3]

[1]*Dept. of Electrical & Computer Engineering, University of Toronto*
[2]*Institute for Quantum Computing, University of Waterloo*
[3]*Dept. of Physics, University of Toronto*

arXiv: 1408.3667 (2014)

QCrypt 2014, Telecom ParisTech, Sep. 2nd (2014)

Why is QKD under attack?


nature International weekly journal of science

nature news home | news archive | specials | opinion | features | news blog | natu

Take Nature Publishing Group's readership survey for the chance to win a MacBook Air.

comments on this story

Published online 20 May 2010 | Nature | doi:10.1038/news.2010.256

News

Quantum crack in cryptographic armour

A commercial quantum encryption system has been fully hacked for the first time.

Stories by subject

- Physics
- Technology


physicsworld.com
BEST SPECIALIST SITE FOR JOURNALISM 2011

Home | News | Blog | Multimedia | In depth | Jobs | Events

News archive

- 2012
- 2011
  - December 2011
  - November 2011
  - October 2011
  - September 2011
  - August 2011
  - July 2011
  - June 2011
  - May 2011
  - April 2011
  - March 2011
  - February 2011
  - January 2011

Hackers steal quantum code

Jun 17, 2011 5 comments

Bag of quantum tricks

Security proof = Physics + "*Theoretical*" models!

Quantum hacking experiments

Attack	Component	Target
Time-shift Y. Zhao et al., Phys. Rev. A **78**, 042333 (2008)	**Detector**	Measurement
Phase-remapping F. Xu et al., New J. Phys. 12, 113026 (2010)	Phase modulator	Source
Detector blinding L. Lydersen et al., Nat. Photonics 4, 686 (2010)	Detector	Measurement
Channel calibration N. Jain et al., Phys. Rev. Lett. 107, 110501 (2011)	**Detector**	Measurement
Detector deadtime H. Weier et al., New J. Phys. 13, 073024 (2011)	**Detector**	Measurement
Device calibration P. Jouguet et al., Phys. Rev. A **87**, 062313 (2013)	**Local oscilllator**	Measurement
Laser damaging A. Bugge et al., Phys. Rev. Lett. 112, 070503 (2014)	**Detector**	Measurement

MDI-QKD makes QKD Safe Again

29 August 2013 3:00 pm

[See Thur. tutorial for the details on measurement-device-independent QKD]

Science NOW

…. physicists have demonstrated how to *close a technological loophole* that could have left secrets open to eavesdroppers …

What's left for Eve is *only* the source!

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

Outline

1. Source flaws and loss-tolerant protocol
2. Finite-key analysis and decoy-state method
3. Experimental study
4. Summary

Examples on QKD experiments

arXiv.org > quant-ph > arXiv:quant-ph/0607186

arXiv.org > quant-ph > arXiv:quant-ph/0607182

arXiv.org > quant-ph > arXiv:0810.1069

arXiv.org > quant-ph > arXiv:1210.7556

arXiv.org > quant-ph > arXiv:1309.6431

Quantum Physics

A quantum access network

Bernd Fröhlich, James F. Dynes, Marco Lucamarini, Andrew W. Sharpe, Zhiliang Yuan, Andrew J. Shields

(Submitted on 25 Sep 2013)

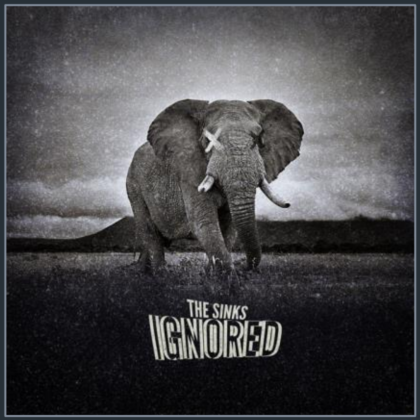
The theoretically proven security of quantum key distribution (QKD) could revolutionise how information exchange is protected in the future. Several field tests of QKD have proven it to be a reliable technology for cryptographic key exchange and have demonstrated nodal networks of point-to-point links. However, so far no convincing answer has been given to the question of how to extend the scope of QKD beyond niche applications in dedicated high security networks. Here we show that adopting simple and cost-effective telecommunication technologies to form a quantum access network can greatly expand the number of users in quantum networks and therefore vastly broaden their appeal. We are able to demonstrate that a high-speed single-photon detector positioned at the network node can be shared between up to 64 users, thereby significantly reducing the hardware requirements for each user added to the network. This shared receiver architecture removes one of the main obstacles restricting the widespread application of QKD. It presents a viable method for realising multi-user QKD networks with resource efficiency and brings QKD closer to becoming the first widespread technology based on quantum physics.

Question: Are there any security problems in the source?

Problem with previous experiments

Previous experiments do *not* consider source flaws.

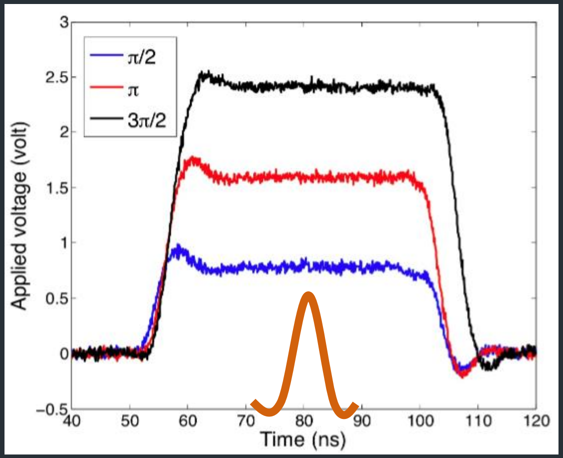
- Perfect phase: $\{0, \pi/2, \pi, 3\pi/2\}$
- Perfect polarization: {H, D, V, A}



But, in experiment, we have…

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

Phase Modulator



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

Our major contributions

1. We implement the *first* QKD experiment that considers source flaws (including modulation flaws).

2. Our decoy implementation achieves tight finite-key security bounds against *general* quantum attacks in the universally composable framework.

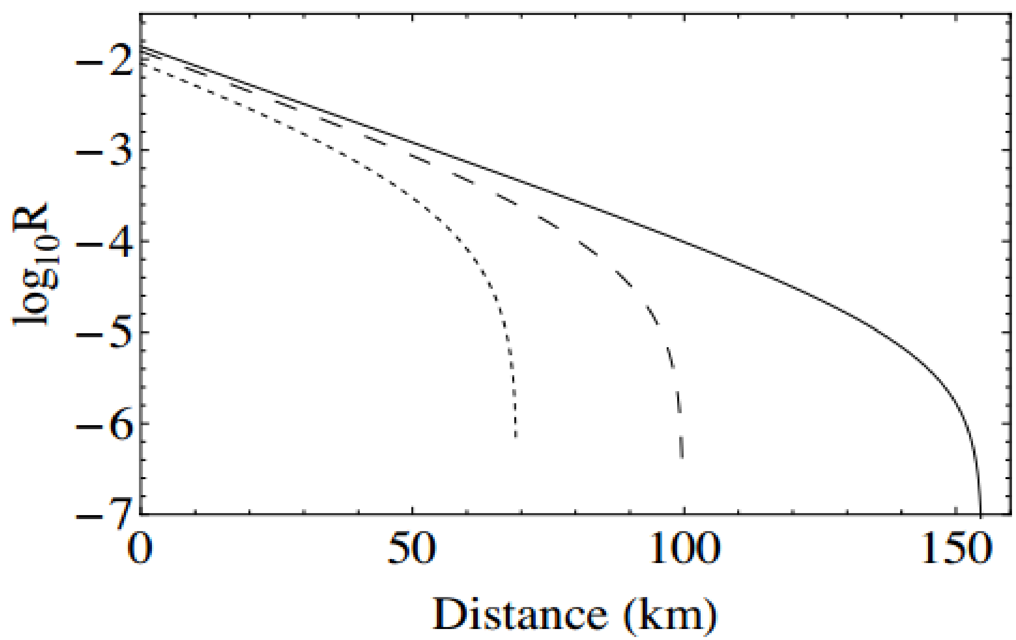
QKD with source flaws

[GLLP proof: Gottesman, Lo, Lütkenhaus, Preskill, *Quant.. Inf. Comput.* 5, 325 (2004)]

Problem: the performance becomes *bad*!

$$K_{\text{rate}} = 1 - h_2(e_{\text{phase}}) - h_2(e_{\text{bit}})$$

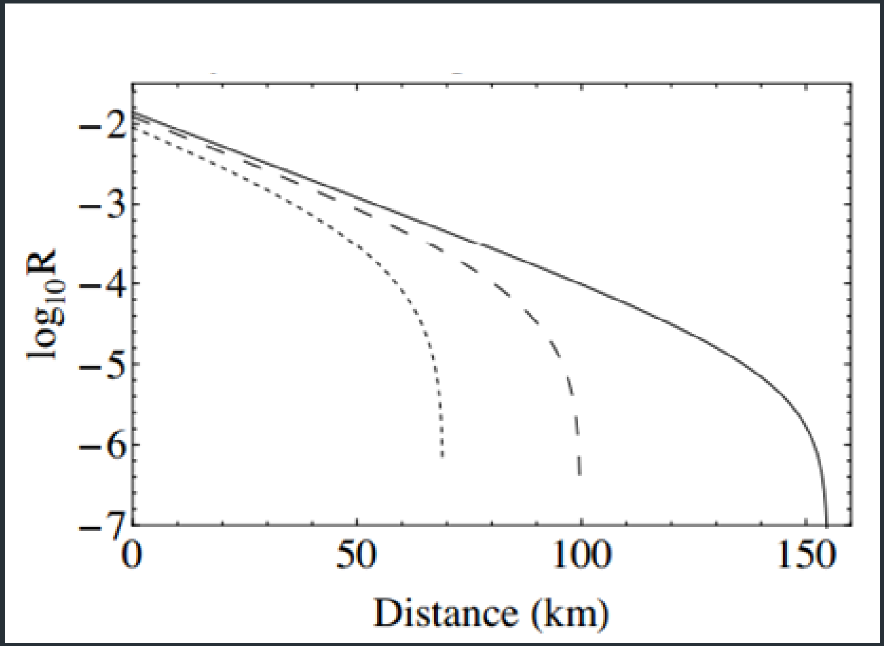
$$e_{\text{phase}} \le e_X + 4\Gamma + 4\sqrt{\Gamma e_X}$$

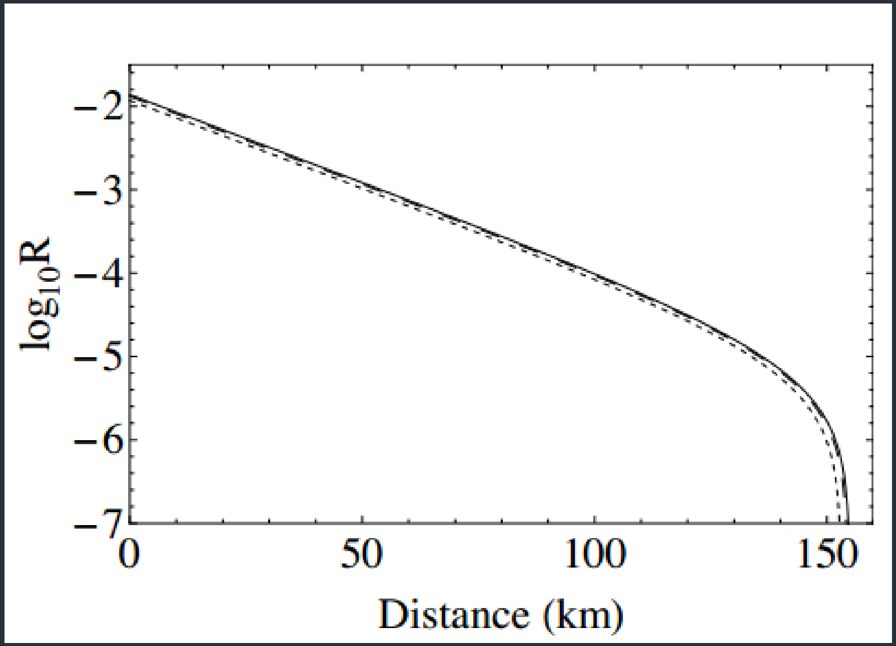


Q1: Does a loss-tolerant protocol exist?

Loss-tolerant protocol

- "qubit assumption": the four BB84 states remain inside two-dimensional Hilbert space.
- Eve cannot attack the system by enhancing source flaws through the channel loss.
- Three states {H, D, V} have the same performance as {H, D, V, A}.





[K. Tamaki, M Curty, G. Kato, H.-K. Lo, K. Azuma, *arXiv: 1312.3514* (2013)]

Questions in practice?

[K. Tamaki *et al.*, *arXiv: 1312.3514* (2013)]

1. The finite-key security analysis?
2. The method with finite-number of decoy states?

3. Quantify the source flaws?
4. Verify the qubit assumption?
5. Implement the protocol in experiment?

A1: Finite-key analysis

Based on [Tomamichel, Lim, Gisin, Renner, Nat. Comm., 3, 634, (2012);
Lim, Curty, Walenta, Xu, Zbinden, *Phys. Rev. A,* **89** 022307 (2014)]

- Tight security bounds against general attacks, obtained by using the entropy uncertainty relations to bound the smooth entropies.

Privacy Amplification

$$\ell \geq s_{z,0}^{L} + s_{z,1}^{L} - s_{z,1}^{L} h\left(e_{x,1}^{U}\right) - \mathrm{leak}_{\mathrm{EC}} - 6\log_2 \frac{21}{\varepsilon_{\mathrm{sec}}} - \log_2 \frac{2}{\varepsilon_{\mathrm{cor}}}$$

Vacuum events

Phase error rate

ε-secret

ε-correct

Single-photon events

Error correction

estimated by using decoy states

measured in experiment

chosen by protocol

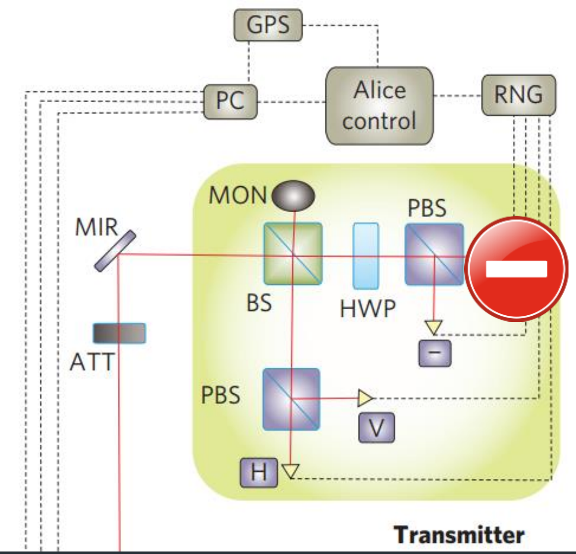
A2: Three-state QKD with decoy states

- Vacuum events and single-photon events are estimated following [Ma, Qi, Zhao, Lo, *Phys. Rev. A*, **72** 012326 (2005)]
- Phase error rate using “rejected data analysis”

[Barnett, Huttner, Phoenix, J. Mod. Opt. 40, 2501-2513 (1993)]

$$e^U_{x,1} = \frac{2P_x s^U_{0_x|z,1} + P_z\left(s^U_{1_x|x,1} - s^L_{0_x|x,1}\right)}{2P_x s^L_{x|z,1}}$$

Basis mismatch counts

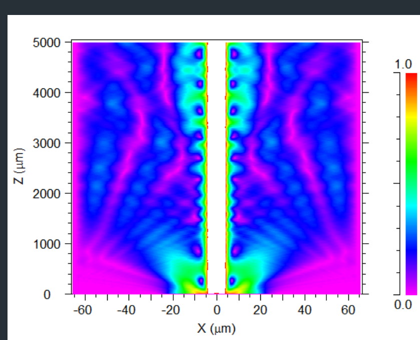


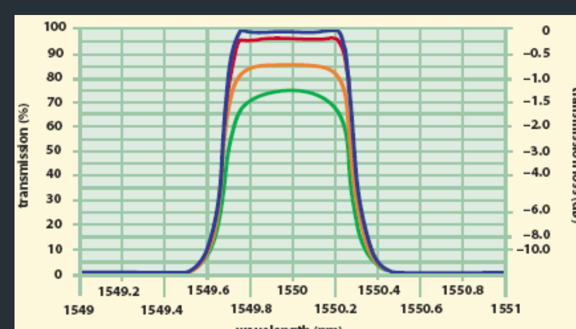
Alice only sends {H, D, V}.

A3: Verify the qubit assumption

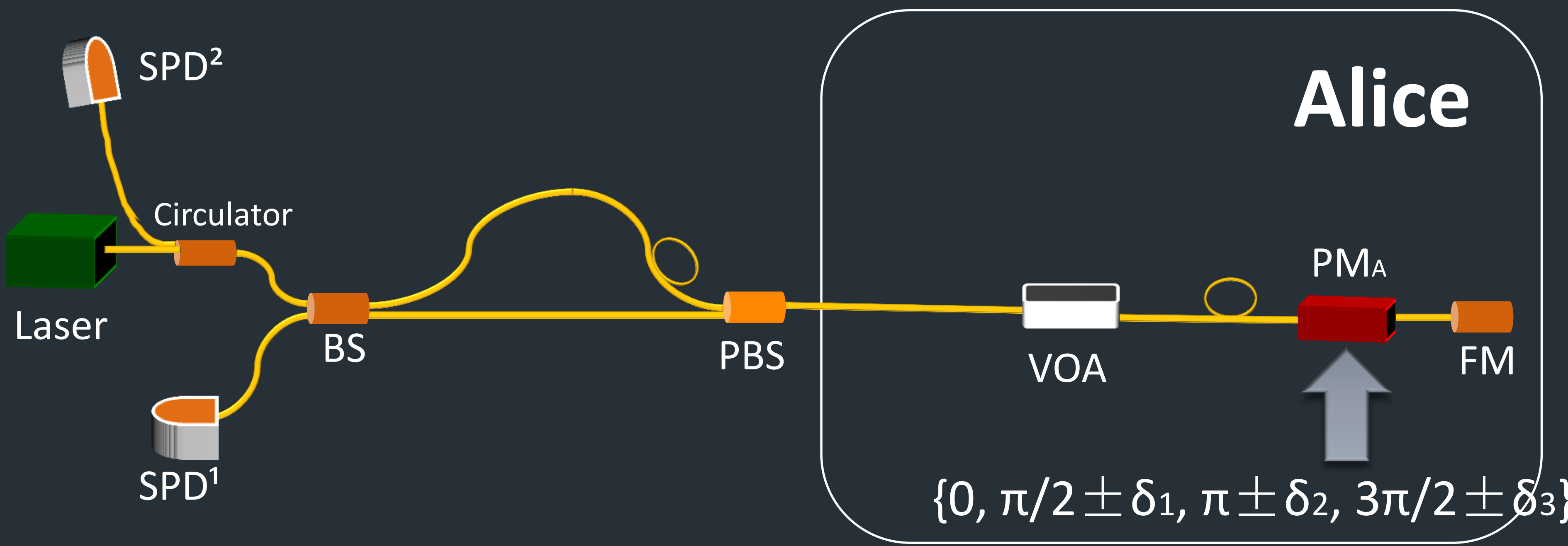
In a phase-encoding system, does Alice prepare a qubit?

Mode	Filter and result
Spatial	Single-mode fiber (core diameter =10 um)
Spectral	Band pass filter (say, 15 GHz for 100ps pulse)
Timing	Synchronization (Fidelity=1-10^{-8})
Polarization	Polarizer/PBS (Fidelity=1-10^{-7})





A4: Quantify the source flaws

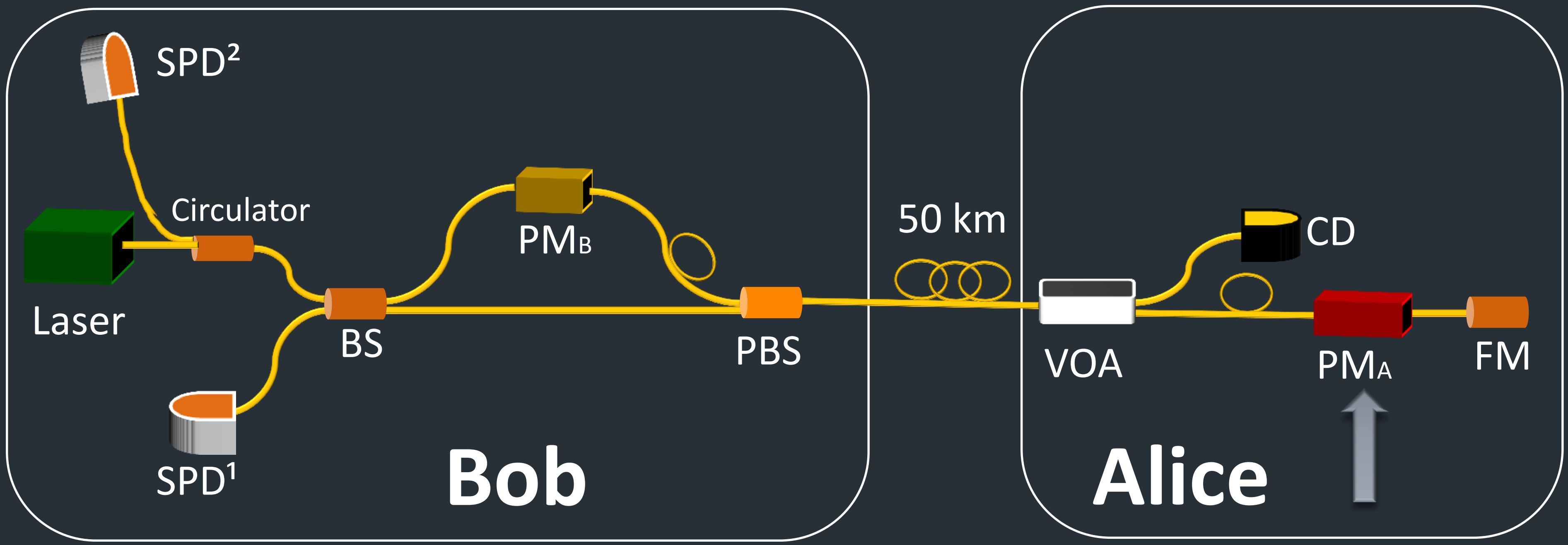


System	θ	$D_{1,\theta}$	$D_{2,\theta}$	$\bar{\delta}_\theta$
ID-500	0	630	867678	-
	$\pi/2$	456735	444336	0.015
	π	856245	3894	0.127
	$3\pi/2$	464160	436962	0.032

Plug&Play system

- ID500: $\delta < 0.127$
- Clavis2: $\delta < 0.147$

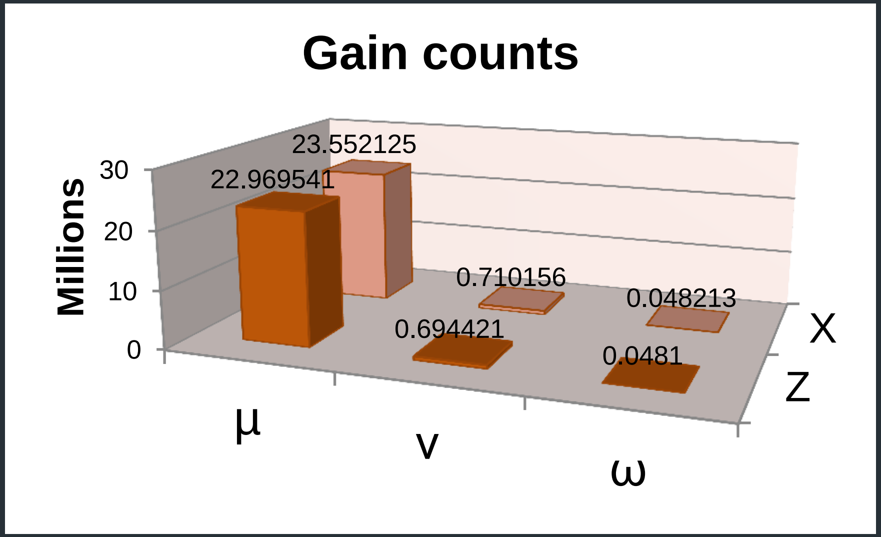
A5: Our implementation

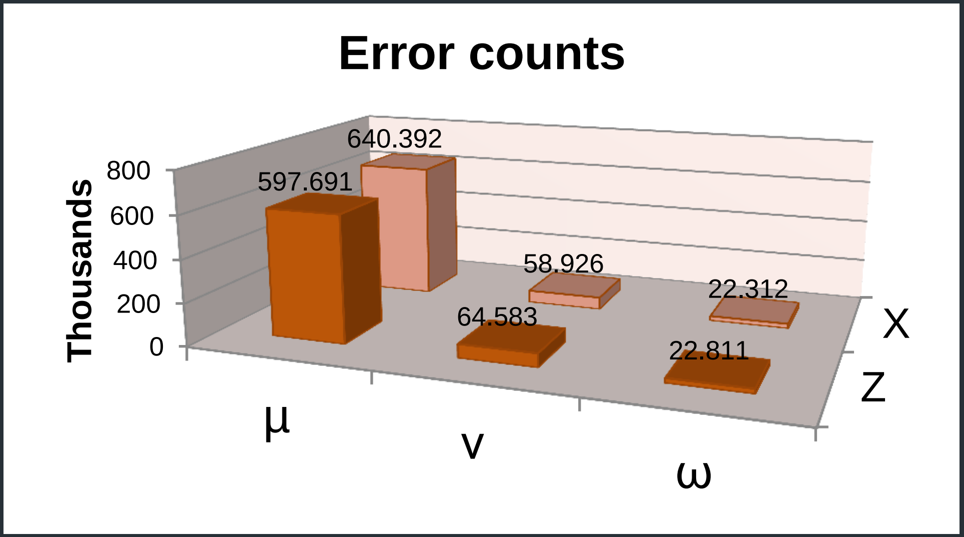


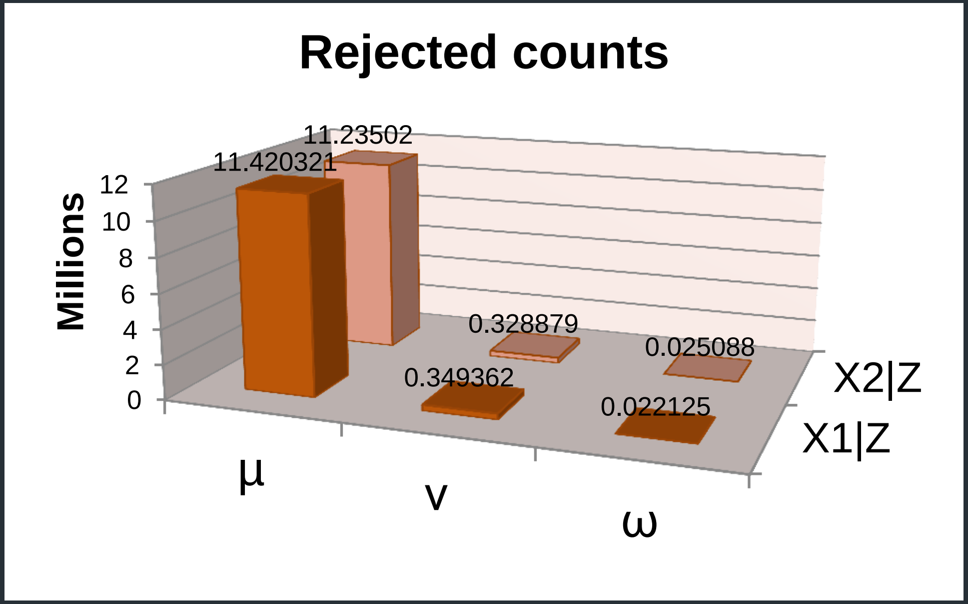
- Commercial plug&play QKD system (ID500).
- Three-state QKD: $PM_A = \{0, \pi/2, \pi\}$.
- Decoy-state BB84: $PM_B = \{0, \pi/2, \pi, 3\pi/2\}$.

http://www.idquantique.com

Raw counts for three-state QKD







- Distance: 50 km telecom fiber
- Total pulses: $N=5X10^{10}$
- Security: $\varepsilon=10^{-10}$

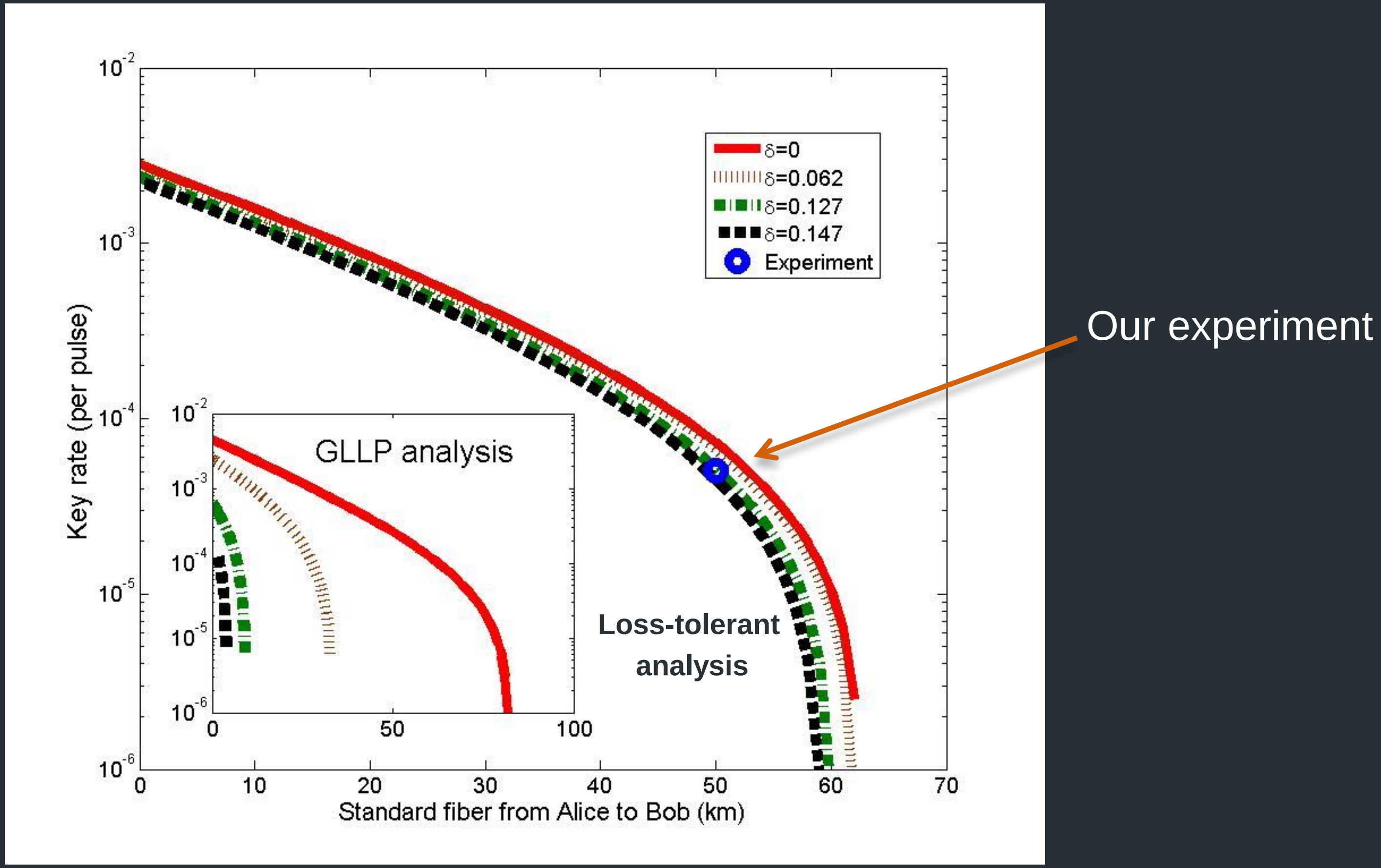
- Measure the counts instead of probabilities (called gains).
- Record the rejected counts!

Results

Parameter	Three-state	BB84
Vacuum events	3.22×10^5	3.21×10^5
Single-photon events	1.30×10^7	1.31×10^5
QBER	2.98%	2.89%
Phase error rate	11.49%	6.01%
Key length	2.60×10^6	7.70×10^6
Key rate (per pulse)	5.21×10^{-5}	1.54×10^{-4}

The security of key generation considers source flaws and it can be against general attacks by Eve.

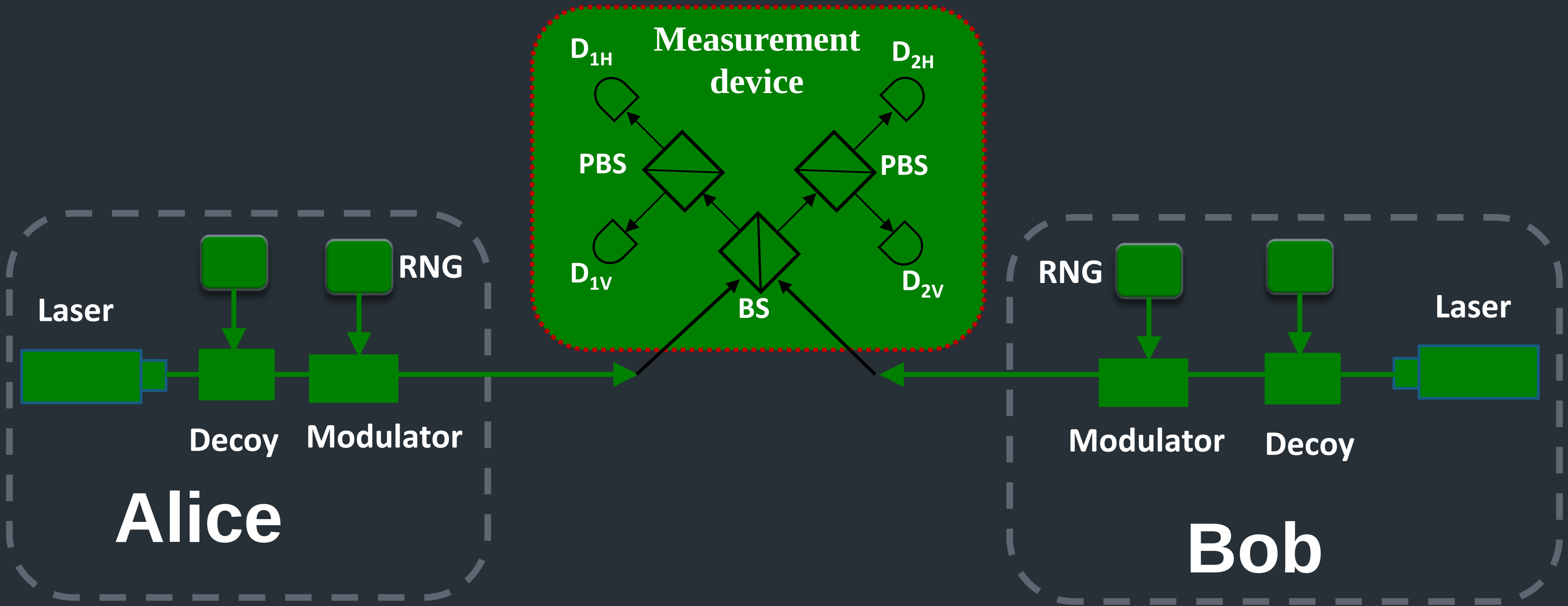
Numerical simulation



Parameters: η=5.05%; P_d= 4×10^{-5}; N=5×10^{10}; $\varepsilon=10^{-10}$

Loss-tolerant to source flaws!

Future directions



- Source flaws in practical MDI-QKD?
- Refined security proof for imperfect fidelity?
- Protect Alice/Bob from leaking unwanted information?
- Source flaws in CV-QKD?
- …

Summary — takeaway message

- A QKD implementation should consider the source flaws and employ a rigorous security analysis.
- Our experiment makes practical QKD loss-tolerant to source flaws over 50 km telecom fiber.
- Three-state QKD is feasible in practice.

Reference:

1. F. Xu, S. Sajeed, S. Kaiser, Z. Tang, L. Qian, V. Makarov, H.-K. Lo, *arXiv: 1408.3667* (2014)
2. K. Tamaki, M Curty, G. Kato, H.-K. Lo, K. Azuma, *arXiv: 1312.3514* (2013)
3. C. Lim, M. Curty, N. Walenta, F. Xu, H. Zbinden, *Phys. Rev. A,* **89** 022307 (2014)

Acknowledgement:
NSERC, Connaught Innovation fund, Industry Canada, CRC program.