Vadim Makarov
IQC Institute for Quantum Computing

Testing quantum crypto

Talk at ETSI 2nd quantum-safe crypto workshop, Ottawa, 6–7 October 2014

Cryptography:	classical	vs.	quantum
Based on...	Unproven mathematical assumptions		Laws of physics
Convenient to implement?	Yes		No
Forward secure?	No		Yes
Authenticate via PKI?	Yes		Yes
Loopholes in implementations?	Yes		

Crypto shocker: four of every 1,000 public keys provide no security (updated)

Almost 27,000 certificates used to protect webmail, e-commerce, and other …

by **Dan Goodin** - Feb 15 2012, 7:00am EDT

An astonishing four out of every 1,000 public keys protecting webmail, online banking, and other sensitive online se
research is the late
prevent eavesdrop

The finding, report
the analysis of son
"modulus" of each
mathematician Eu
Almost 27,000 of t
used to generate t

"The fact is, if thes
one of these event
an independent cr
startling."

HEARTBLEED BUG April 14, 2014 1:30 pm

900 SINs stolen due to Heartbleed bug: Canada Revenue Agency

By Irene Ogrodnik Global News

TORONTO – Roughly 900 Canadians have had their social insurance numbers stolen from the Canada Revenue Agency's systems after the federal agency's online services were hit by the so-called Heartbleed bug.

"CRA has been n
by the Governme
Canada's lead se
agencies of a ma
breach of taxpaye
that occurred ove
six-hour period,"
Revenue Agency
said in a statemer
"Social insurance
numbers (SIN) of

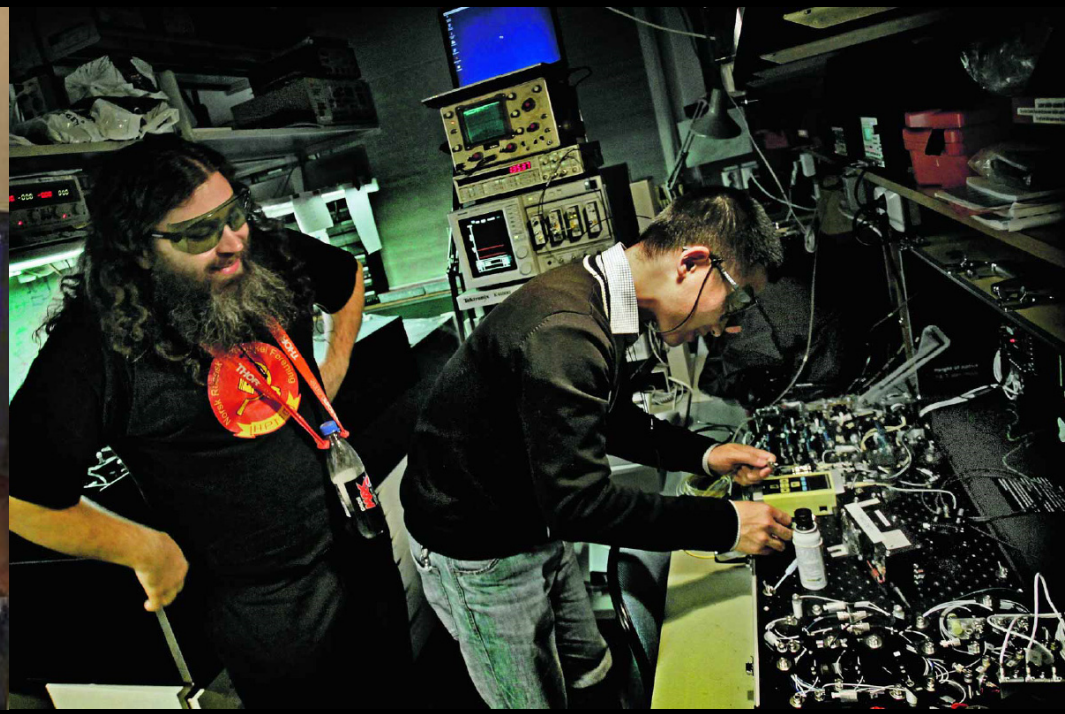
```
Date: Wed, 1 Oct 2014 15:01:20 +0000
From: Matt Cooper <matt.cooper@uwaterloo.ca>
To: "makarov@vad1.com" <makarov@vad1.com>
Subject: [URGENT] Network device compromised

Good morning Vadim,

We have received notice from IST that your NAS has been compromised due to
the ShellShock exploit and it must be removed from the network immediately.

Here is an excerpt from IST Security;

"It looks very much like your NAS qhbackup.iqc.uwaterloo.ca has been
compromised by ShellShock.
Last night (30 Sept) at 2305h we saw a ShellShock-type http request to the
login script for this device, intended to cause it to execute code to
download some scripts and binaries, followed by it actually downloading
same.
```

Cryptography: classical vs. quantum

	Unproven mathematical assumptions	Laws of physics
Based on...		
Convenient to implement?	**Yes**	**No**
Forward secure?	**No**	**Yes**
Authenticate via PKI?	**Yes**	**Yes**
Loopholes in implementations?	**Yes**	**Yes**
Exploitable retroactively?	Sometimes	**No***

* Single exception: A. Lamas-Linares & C. Kurtsiefer, Opt. Express **15**, 9388 (2007)

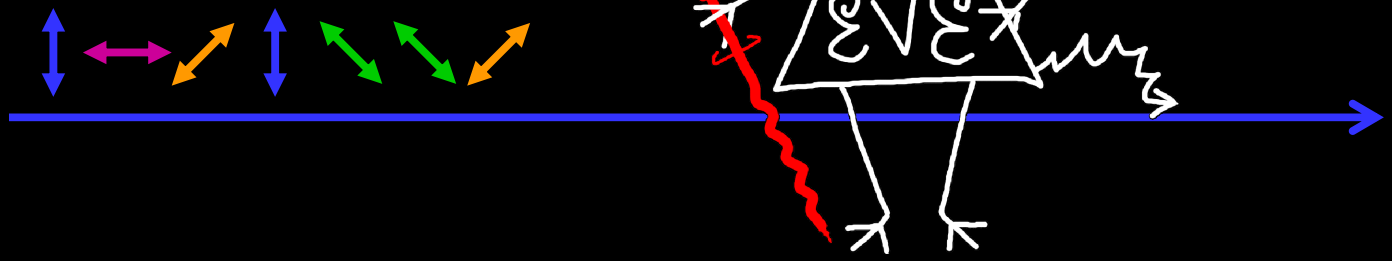
Classical hacking vs. quantum hacking



Often, just a computer
(~$0 equipment)

Optics lab
(≳$0.5M equipment)

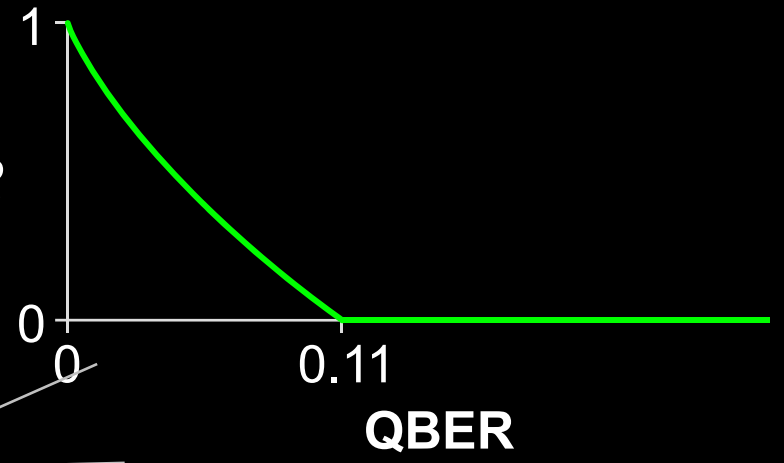
Security model of QKD

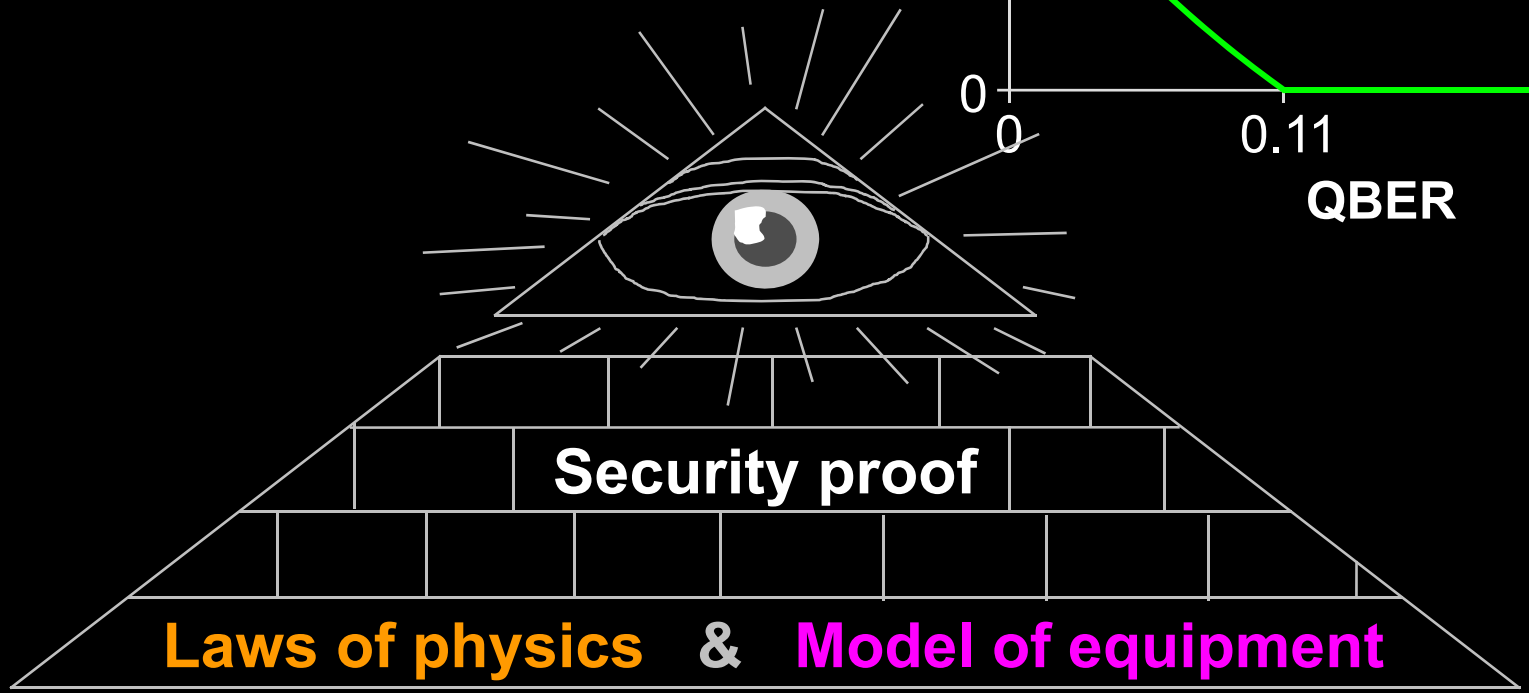


Alice

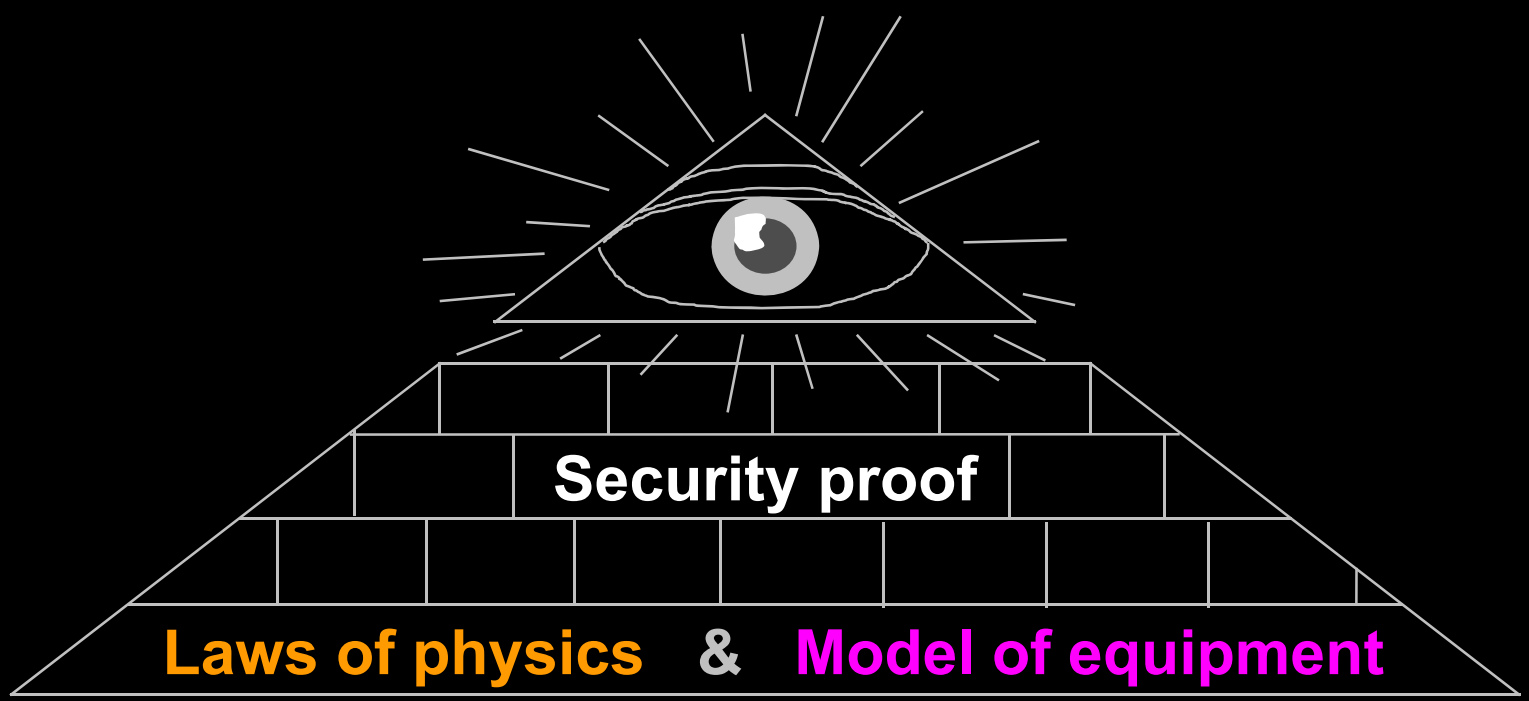
Bob

Secret key rate $R = f(\mathrm{QBER})$





Security model of QKD



Example of vulnerability and countermeasures

Photon-number-splitting attack

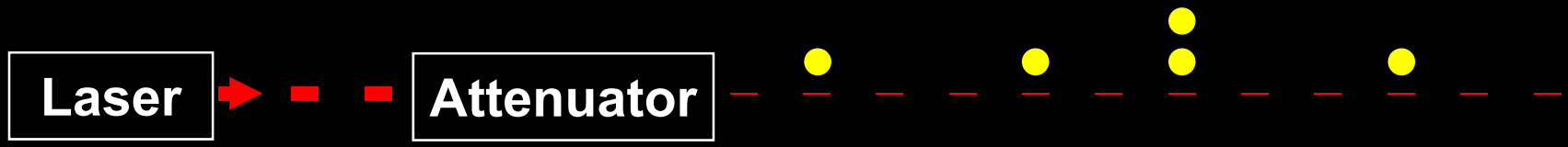
C. Bennett, F. Bessette, G. Brassard, L. Salvail, J. Smolin, J. Cryptology **5**, 3 (1992)

G. Brassard, N. Lütkenhaus, T. Mor, B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000)

N. Lütkenhaus, Phys. Rev. A **61**, 052304 (2000)

S. Félix, N. Gisin, A. Stefanov, H. Zbinden, J. Mod. Opt. **48**, 2009 (2001)

N. Lütkenhaus, M. Jahma, New J. Phys. **4**, 44 (2002)



★ Decoy-state protocol

W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003)

★ SARG04 protocol

V. Scarani, A. Acín, G. Ribordy, N. Gisin, Phys. Rev. Lett. **92**, 057901 (2004)

★ Distributed-phase-reference protocols

K. Inoue, E. Waks, Y. Yamamoto, Phys. Rev. Lett. **89**, 037902 (2002)

K. Inoue, E. Waks, Y. Yamamoto, Phys. Rev. A. **68**, 022317 (2003)

N. Gisin, G. Ribordy, H. Zbinden, D. Stucki, N. Brunner, V. Scarani, arXiv:quant-ph/0411022v1 (2004)

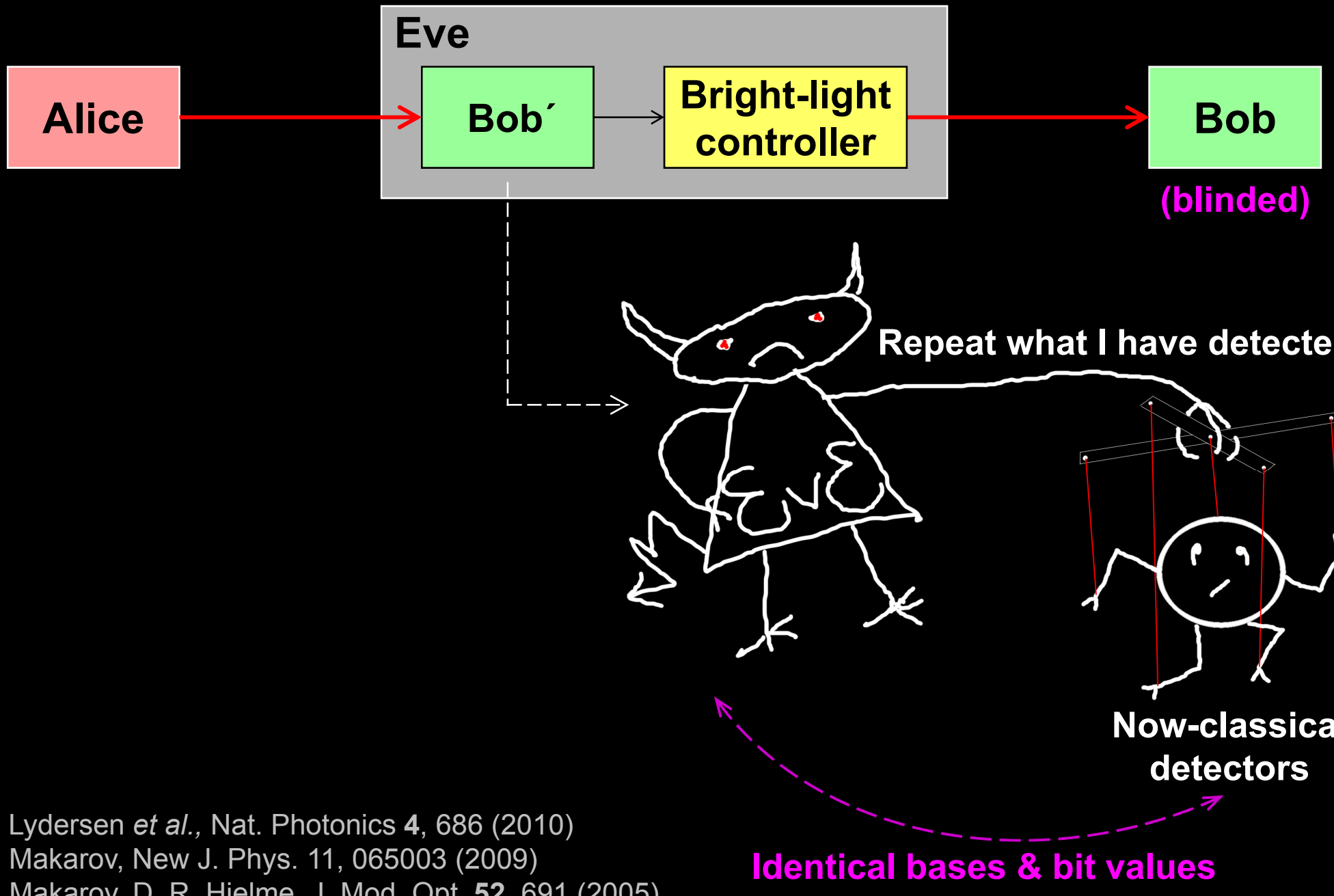
Attack	Target component	Tested system
Pulse energy calibration S. Sajeed *et al.,* presentation at QCrypt (2014)	classical watchdog detector	ID Quantique
Trojan-horse I. Khan *et al.,* presentation at QCrypt (2014)	phase modulator in Alice	SeQureNet
Trojan-horse N. Jain *et al.,* arXiv:1406.5813	phase modulator in Bob	ID Quantique*
Detector saturation H. Qin, R. Kumar, R. Alleaume, presentation at QCrypt (2013)	homodyne detector	SeQureNet
Shot-noise calibration P. Jouguet, S. Kunz-Jacques, E. Diamanti, Phys. Rev. A **87**, 062313 (2013)	classical sync detector	SeQureNet
Wavelength-selected PNS M.-S. Jiang, S.-H. Sun, C.-Y. Li, L.-M. Liang, Phys. Rev. A **86**, 032310 (2012)	intensity modulator	(theory)
Multi-wavelength H.-W. Li *et al.,* Phys. Rev. A **84**, 062308 (2011)	beamsplitter	research syst.
Deadtime H. Weier *et al.,* New J. Phys. **13**, 073024 (2011)	single-photon detector	research syst.
Channel calibration N. Jain *et al.,* Phys. Rev. Lett. **107**, 110501 (2011)	single-photon detector	ID Quantique
Faraday-mirror S.-H. Sun, M.-S. Jiang, L.-M. Liang, Phys. Rev. A **83**, 062331 (2011)	Faraday mirror	(theory)
Detector control I. Gerhardt *et al.,* Nat. Commun. **2**, 349 (2011); L. Lydersen *et al.,* Nat. Photonics **4**, 686 (2010)	single-photon detector	ID Quantique, MagiQ, research syst.
Phase-remapping F. Xu, B. Qi, H.-K. Lo, New J. Phys. **12**, 113026 (2010)	phase modulator in Alice	ID Quantique*
Time-shift Y. Zhao *et al.,* Phys. Rev. A **78**, 042333 (2008)	single-photon detector	ID Quantique

* Attack did not break security of the tested system, but may be applicable to a different implementation.

Attack	Target component	Tested system
Pulse energy calibration S. Sajeed *et al.*, presentation at QCrypt (2014)	classical watchdog detector	ID Quantique
Trojan-horse I. Khan *et al.*, presentation at QCrypt (2014)	phase modulator in Alice	SeQureNet
Trojan-horse N. Jain *et al.*, arXiv:1406.5813	phase modulator in Bob	ID Quantique*
Detector saturation H. Qin, R. Kumar, R. Alleaume, presentation at QCrypt (2013)	homodyne detector	SeQureNet
Shot-noise calibration P. Jouguet, S. Kunz-Jacques, E. Diamanti, Phys. Rev. A **87**, 062313 (2013)	classical sync detector	SeQureNet
Wavelength-selected PNS M.-S. Jiang, S.-H. Sun, C.-Y. Li, L.-M. Liang, Phys. Rev. A **86**, 032310 (2012)	intensity modulator	(theory)
Multi-wavelength H.-W. Li *et al.*, Phys. Rev. A **84**, 062308 (2011)	beamsplitter	research syst.
Deadtime H. Weier *et al.*, New J. Phys. **13**, 073024 (2011)	single-photon detector	research syst.
Channel calibration N. Jain *et al.*, Phys. Rev. Lett. **107**, 110501 (2011)	single-photon detector	ID Quantique
Faraday-mirror S.-H. Sun, M.-S. Jiang, L.-M. Liang, Phys. Rev. A **83**, 062331 (2011)	Faraday mirror	(theory)
Detector control I. Gerhardt *et al.*, Nat. Commun. **2**, 349 (2011); L. Lydersen *et al.*, Nat. Photonics **4**, 686 (2010)	single-photon detector	ID Quantique, MagiQ, research syst.
Phase-remapping F. Xu, B. Qi, H.-K. Lo, New J. Phys. **12**, 113026 (2010)	phase modulator in Alice	ID Quantique*
Time-shift Y. Zhao *et al.*, Phys. Rev. A **78**, 042333 (2008)	single-photon detector	ID Quantique

* Attack did not break security of the tested system, but may be applicable to a different implementation.

Intercept-resend attack with Bob's detector control



L. Lydersen *et al.*, Nat. Photonics **4**, 686 (2010)
V. Makarov, New J. Phys. 11, 065003 (2009)
V. Makarov, D. R. Hjelme, J. Mod. Opt. **52**, 691 (2005)

Countermeasures to detector attacks

Technical

★ **Monitoring extra electrical parameters in detector**

Z. L. Yuan, J. F. Dynes, A. J. Shields, Appl. Phys. Lett. **98**, 231104 (2011)

★ **Randomly varying detector sensitivity**

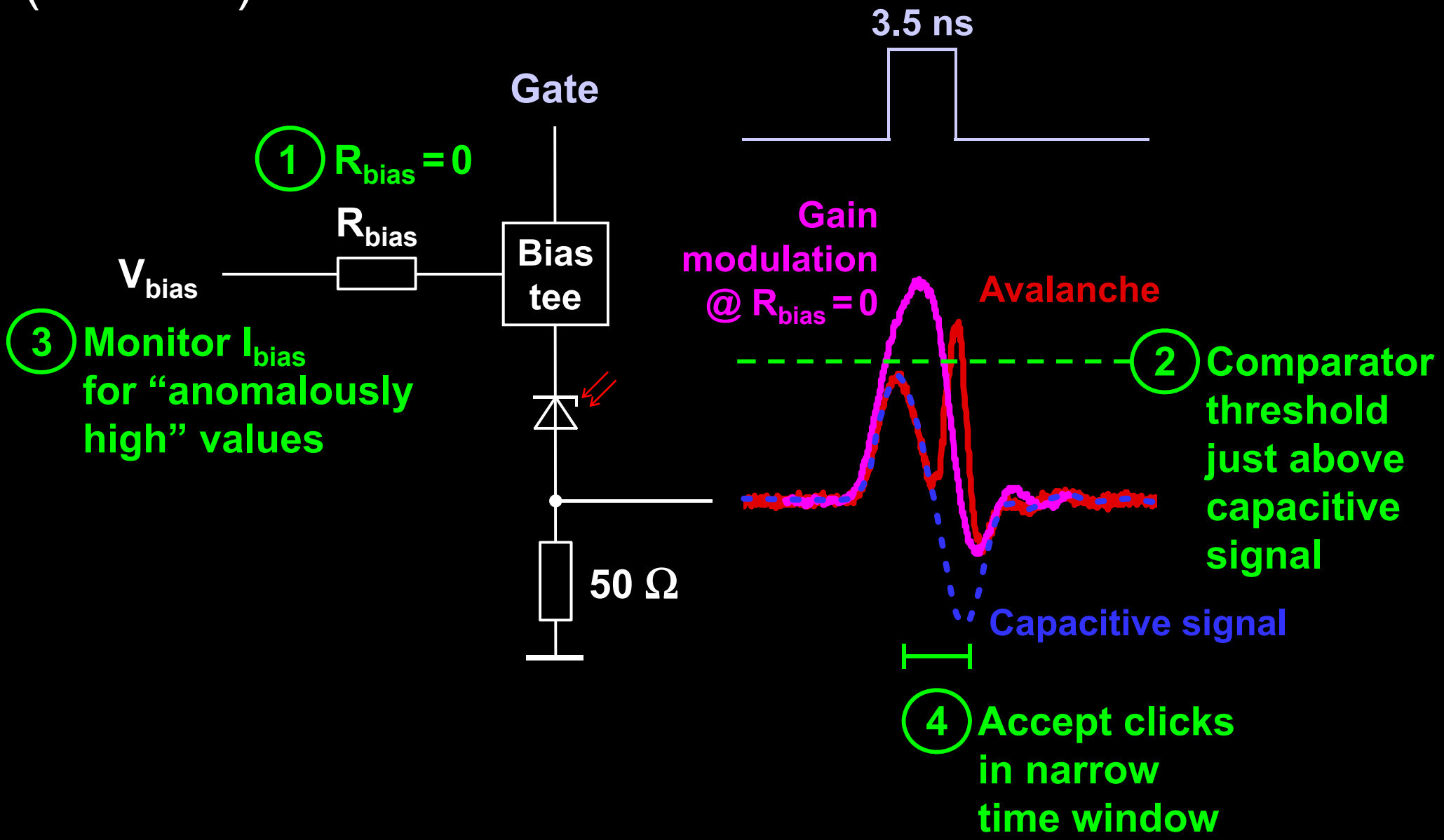
M. Legre, G. Robordy, Intl. patent appl. WO 2012/046135 A2 (filed in 2010)
C. C. W. Lim *et al.,* arXiv:1408.6398

Integrated into security model

★ **Measurement-device-independent QKD**

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

Monitoring extra electrical parameters in detector (Toshiba)



Z. L. Yuan, J. F. Dynes, A. J. Shields, Appl. Phys. Lett. **98**, 231104 (2011);
L. Lydersen, V. Makarov, J. Skaar, Appl. Phys. Lett. **99**, 196101 (2011).
Z. L. Yuan, J. F. Dynes, A. J. Shields, Nat. Photonics **4**, 800 (2010); L. Lydersen *et al., ibid.* 801.

I: Can we test your detector?

Toshiba: No.

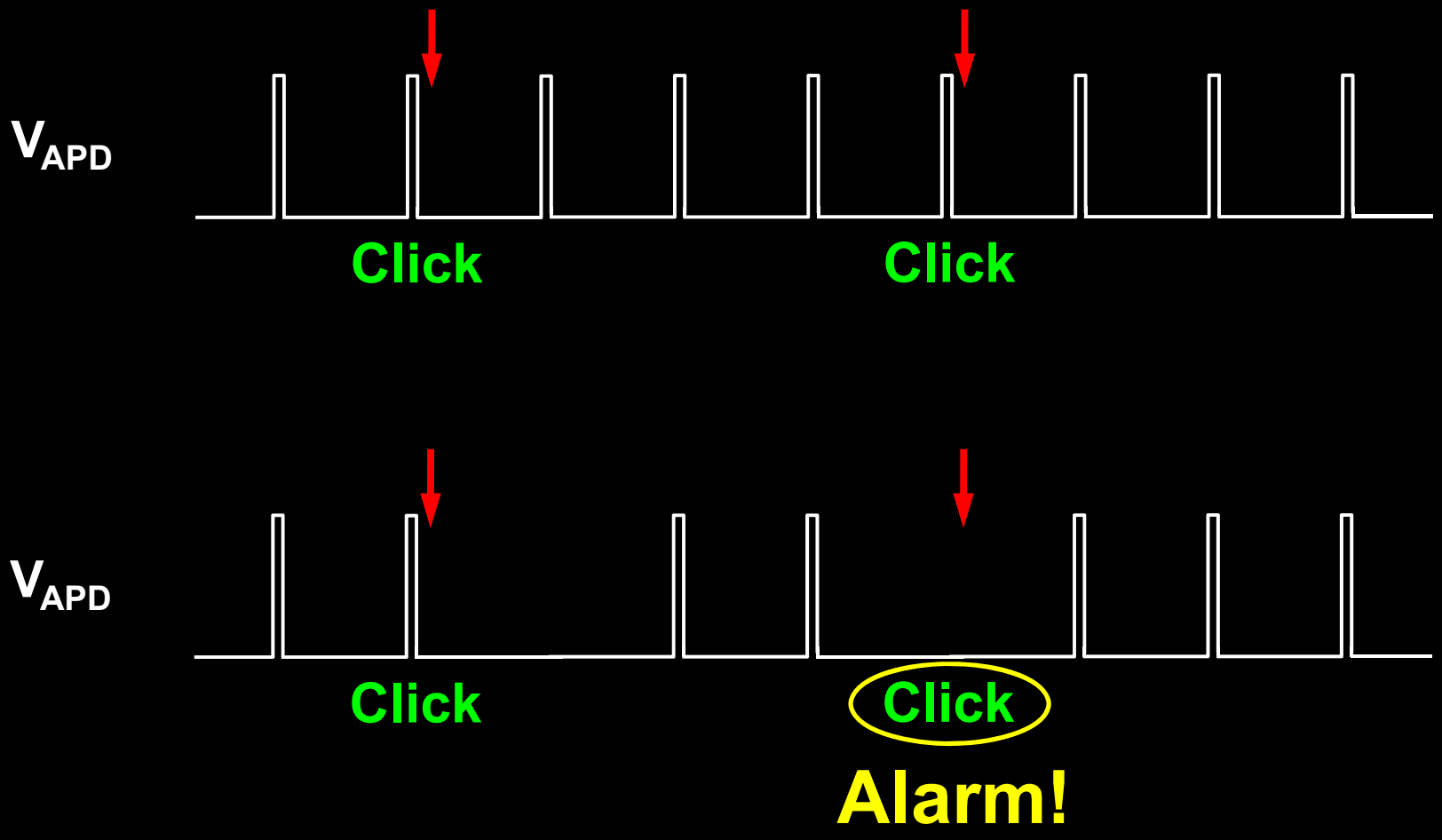
I: Why not?

Toshiba: Still no.

Chinese way: build a copy and hack it.

M.-S. Jiang *et al.,* Phys. Rev. A **88**, 062335 (2013)

Randomly varying detector sensitivity
(ID Quantique)



C. C. W. Lim *et al.*, arXiv:1408.6398
M. Legre, G. Robordy, Intl. patent appl. WO 2012/046135 A2 (filed in 2010)

Countermeasures to detector attacks

Technical

★ **Monitoring extra electrical parameters in detector**

Z. L. Yuan, J. F. Dynes, A. J. Shields, Appl. Phys. Lett. **98**, 231104 (2011)

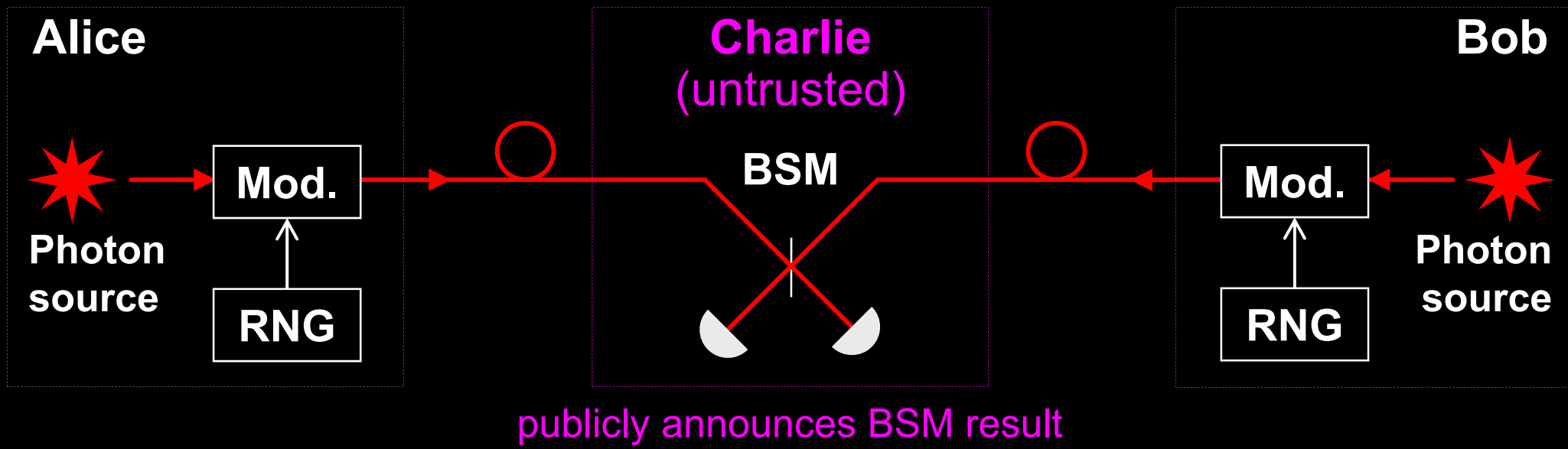
★ **Randomly varying detector sensitivity**

M. Legre, G. Robordy, Intl. patent appl. WO 2012/046135 A2 (filed in 2010)
C. C. W. Lim *et al.,* arXiv:1408.6398

Integrated into security model

★ **Measurement-device-independent QKD**

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



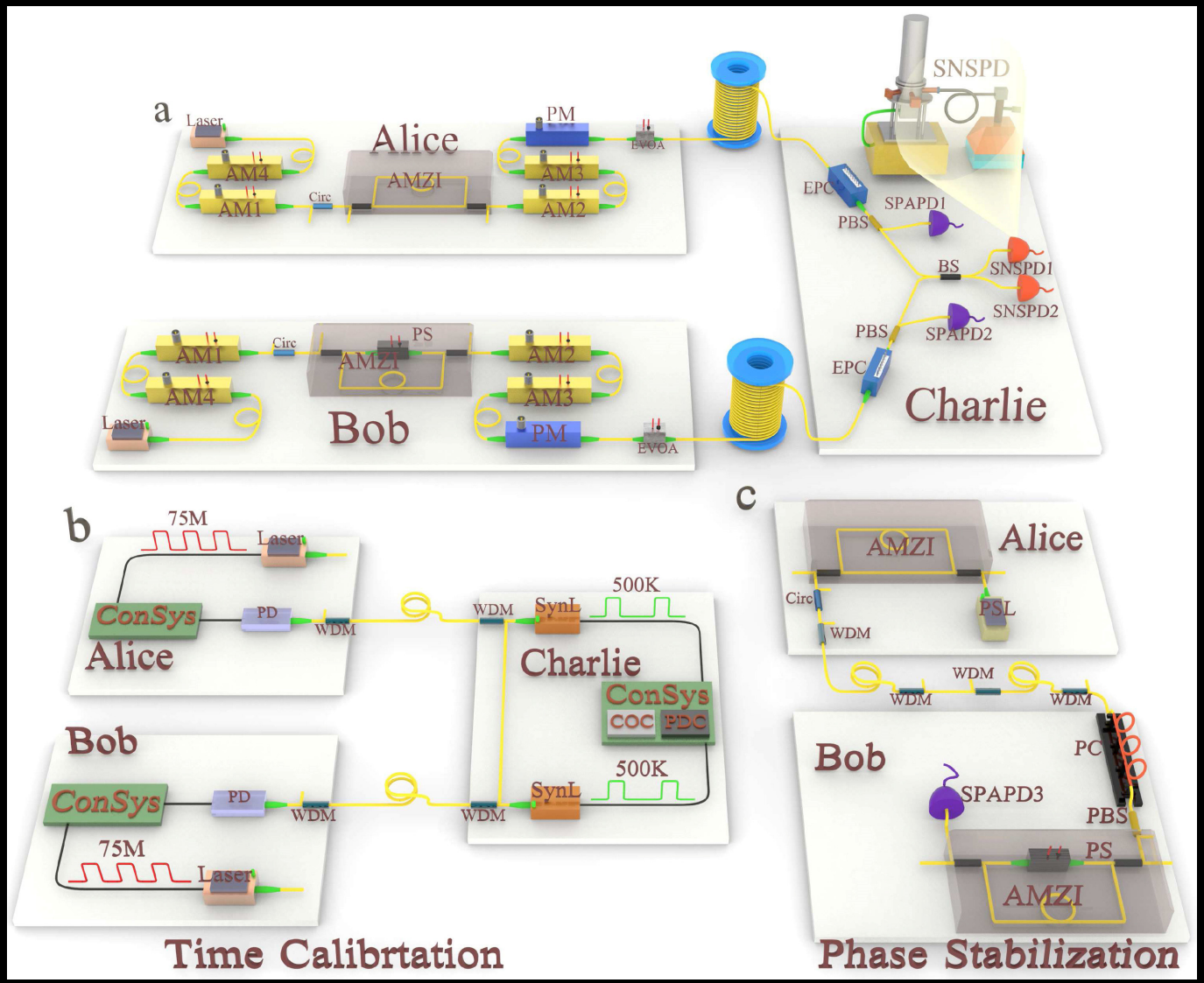
Measurement-device-independent QKD: experiments

Calgary, 28 km
A. Rubenok *et al.*, arXiv:1204.0738v2

Rio de Janeiro, 17 km
T. Ferreira da Silva *et al.*, Phys. Rev. A **88**, 052303 (2013)

Toronto, 10 km
Z. Tang *et al.*, Phys. Rev. Lett. **112**, 190503 (2014)

Hefei, 200 km
Y.-L. Tang *et al.*, arXiv:1407.8012



Responsible disclosure is important

Example: hacking commercial systems

2009

ID Quantique got a detailed vulnerability report

- **reaction: requested time, developed a patch**

M. Legre, G. Ribordy, intl. patent appl. WO 2012/046135 A2 (filed in 2010)

2010

MagiQ Technologies got a detailed vulnerability report

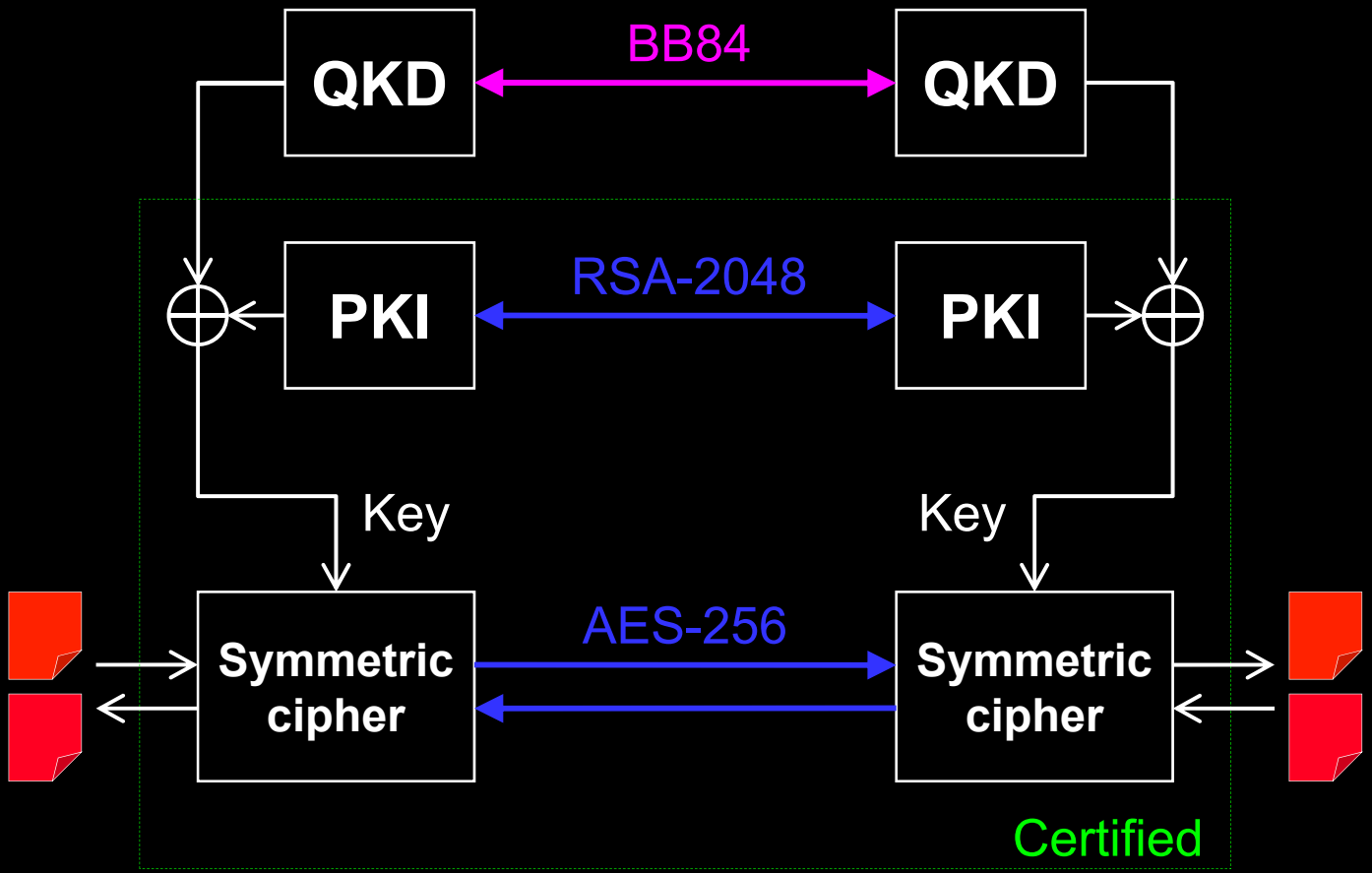
- **reaction: informed us that QPN 5505 is discontinued**

Results presented orally at a scientific conference

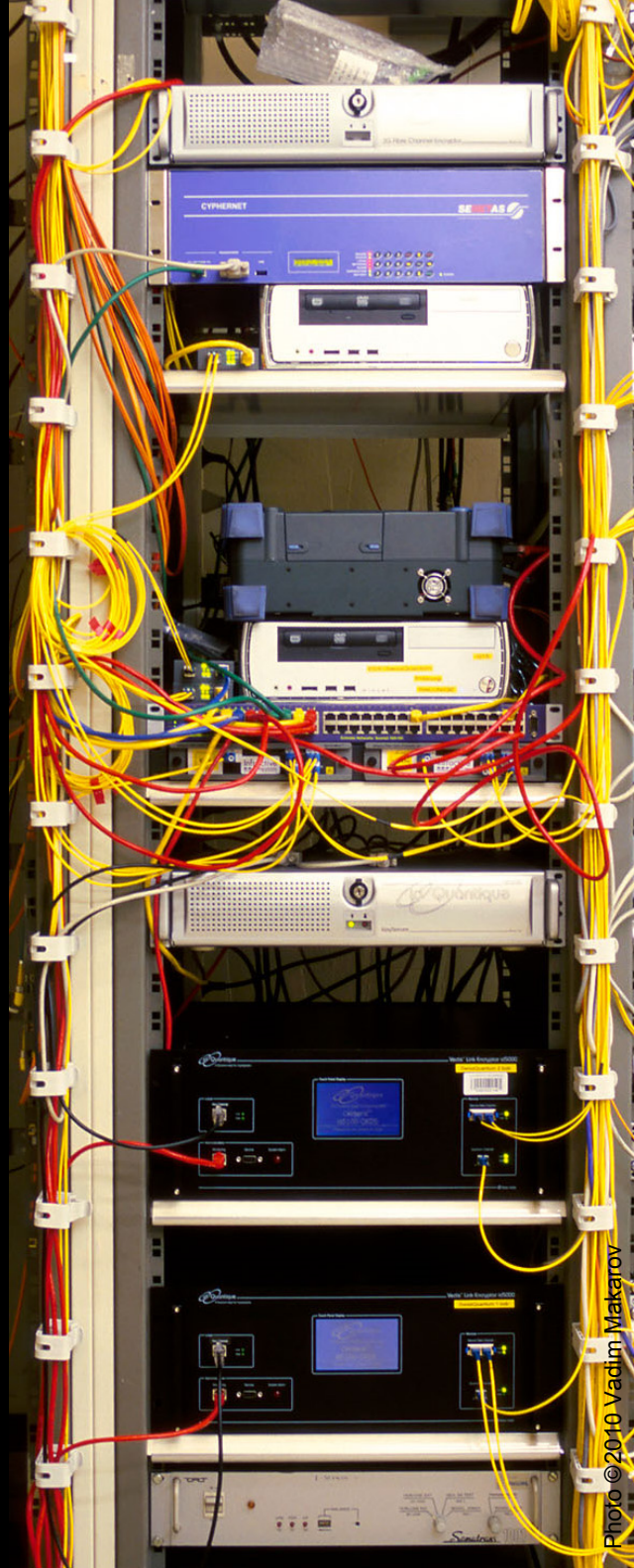
Public disclosure in a journal paper

L. Lydersen *et al.*, Nat. Photonics **4**, 686 (2010)

Dual key agreement



www.swissquantum.com
ID Quantique *Cerberis* system (2010)



www.vad1.com/lab