Quantum hacking

Vadim Makarov

RQC MISIS

vad1.com/lab

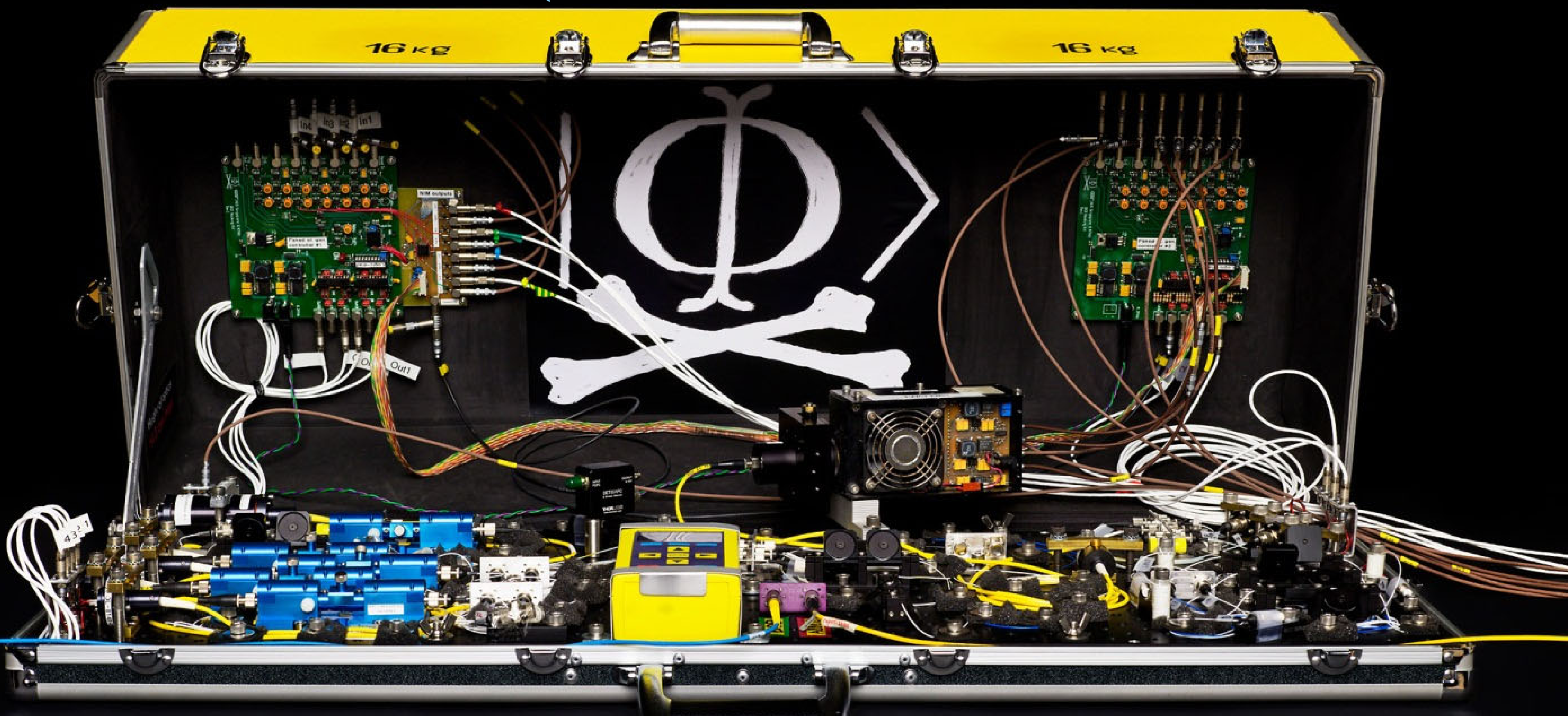
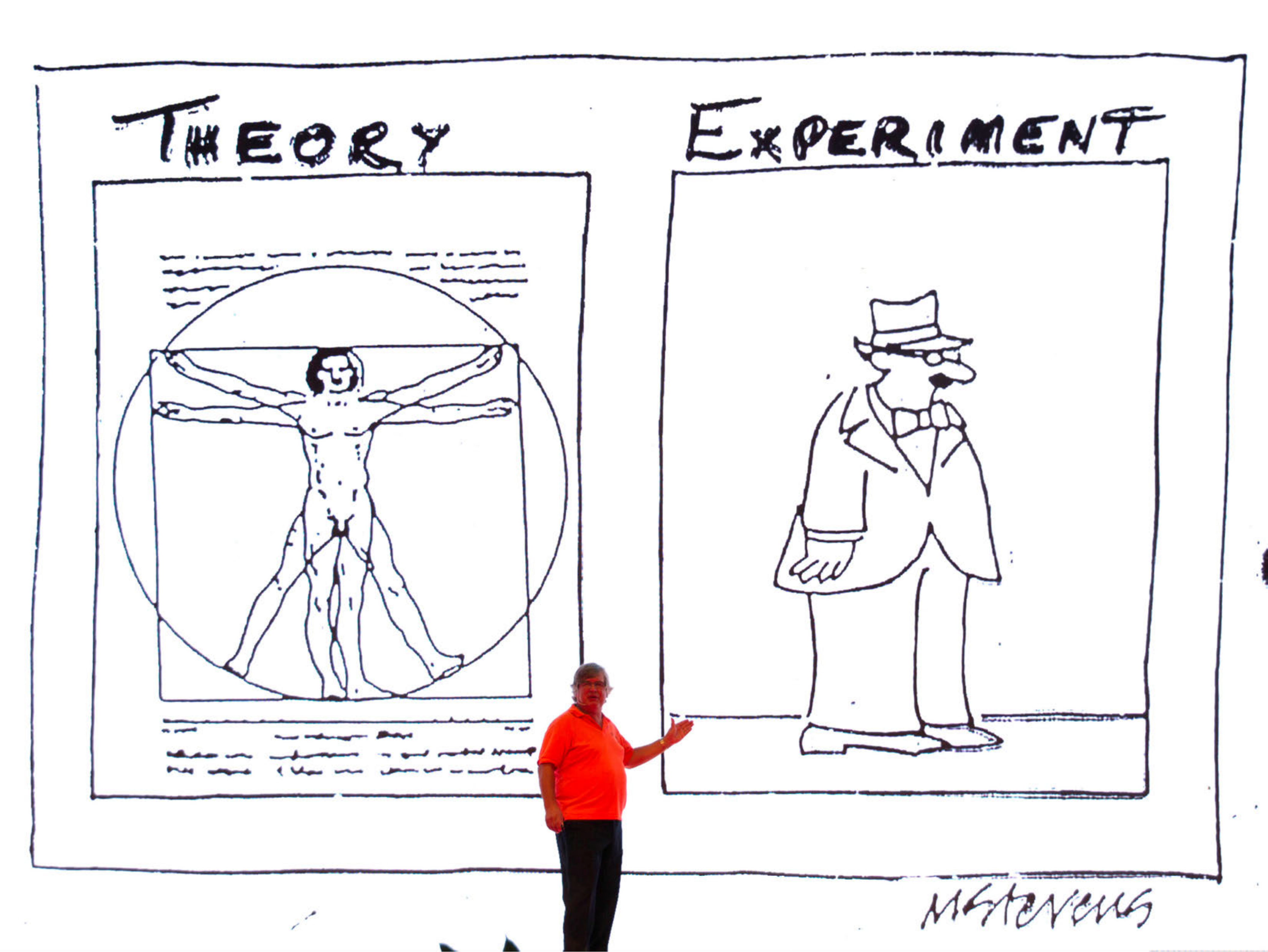
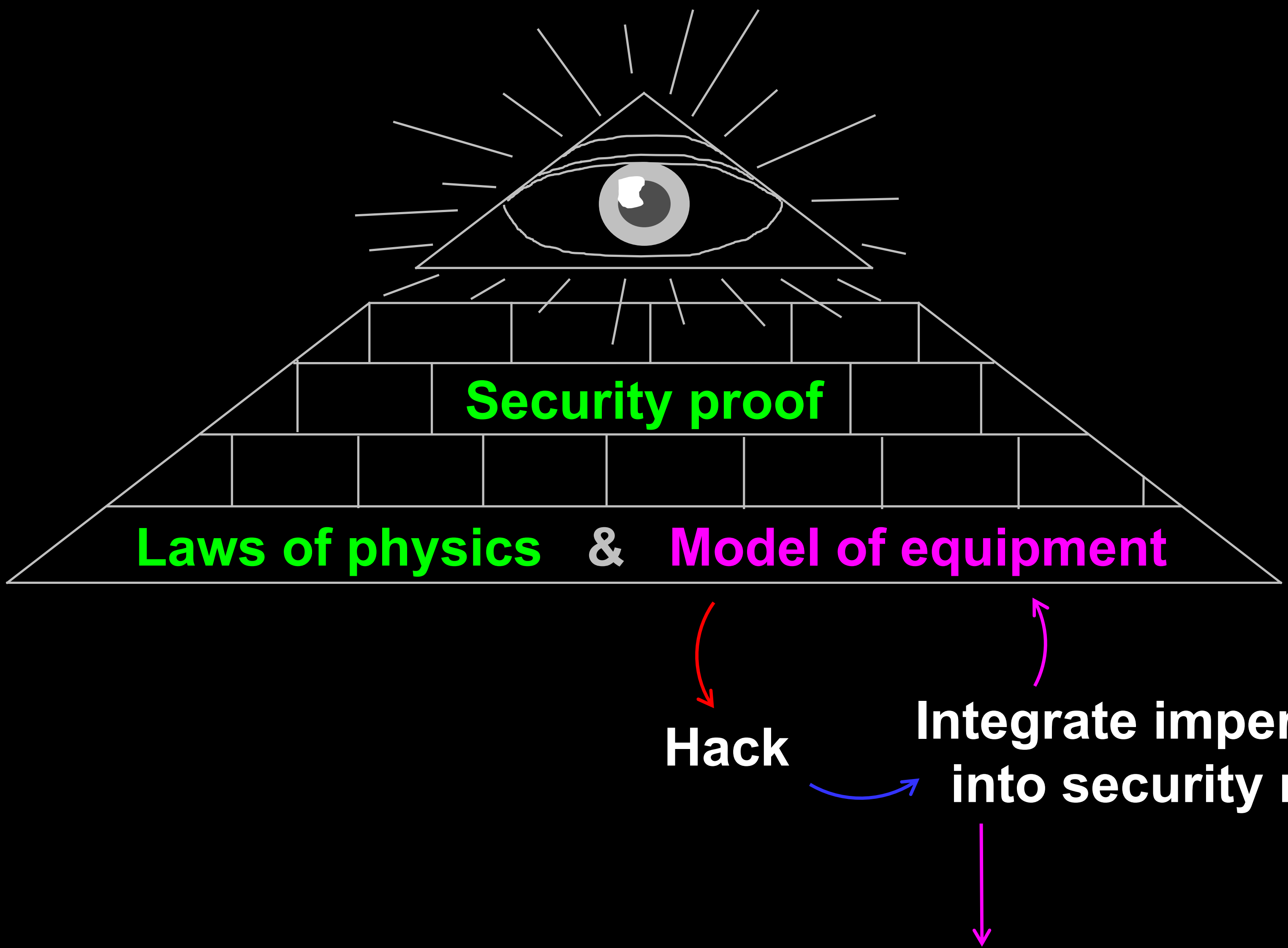


Photo ©2010 NTNU Info / Geir Mogen

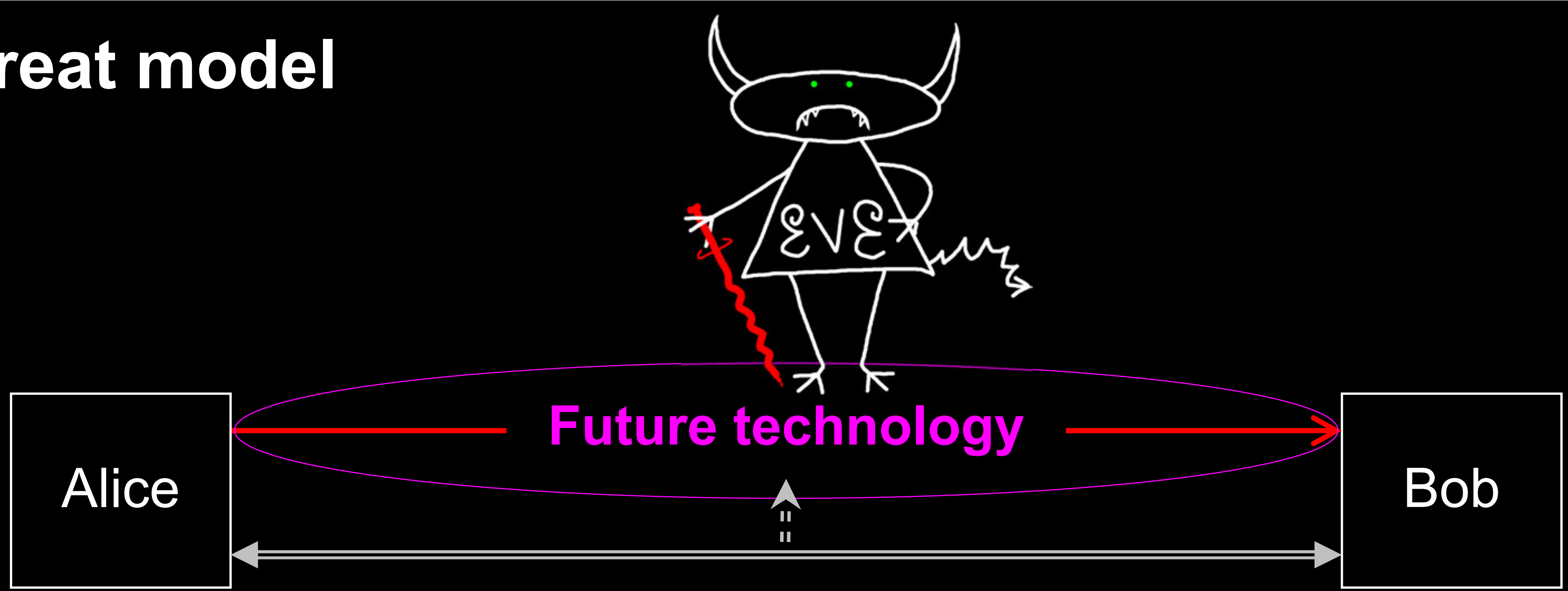

THEORY
EXPERIMENT
MStevens

Implementation security of quantum communications



Formal certification: we need standards and labs ecosystem

Threat model



physically secure, **characteristics known**

physically secure, **characteristics known**

Kerckhoffs' principle:

Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi

A. Kerckhoffs, J. des Sciences Militaires **9**, 5 (1883)

Everything about the system that is not explicitly secret is known to the enemy

Attack	Target component	Tested system
Distinguishability of decoy states A. Huang *et al.*, Phys. Rev. A **98**, 012330 (2018)	laser in Alice	3 research systems
Intersymbol interference K. Yoshino *et al.*, poster at QCrypt (2016)	intensity modulator in Alice	research system
Laser damage V. Makarov *et al.*, Phys. Rev. A **94**, 030302 (2016); A. Huang *et al.*, poster at QCrypt (2018)	any	5 commercial & 1 research systems
Spatial efficiency mismatch M. Rau *et al.*, IEEE J. Sel. Top. Quantum Electron. **21**, 6600905 (2015); S. Sajeed *et al.*, Phys. Rev. A **91**, 062301 (2015)	receiver optics	2 research systems
Pulse energy calibration S. Sajeed *et al.*, Phys. Rev. A **91**, 032326 (2015)	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.*, New J. Phys. **16**, 123030 (2014); S. Sajeed *et al.*, Sci. Rep. **7**, 8403 (2017)	phase modulator in Bob	ID Quantique
Detector saturation H. Qin, R. Kumar, R. Alleaume, Proc. SPIE 88990N (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 system
Deadtime H. Weier *et al.*, New J. Phys. **13**, 073024 (2011)	single-photon detector	research system
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 systems

Example of vulnerability and countermeasures

Photon-number-splitting attack

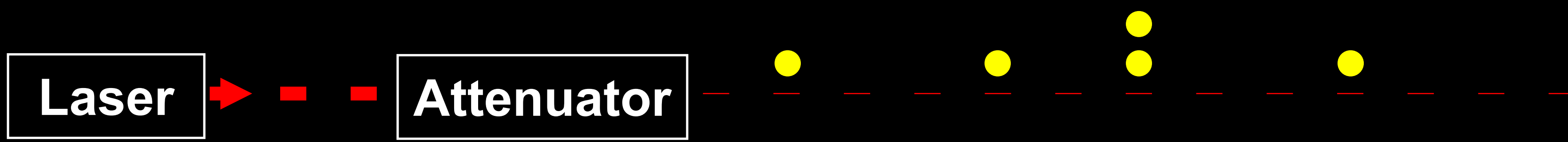
C. Bennett, F. Bessette, G. Brassard, L. Salvail, J. Smolin, J. Cryptology **5**, 3 (1992)

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)

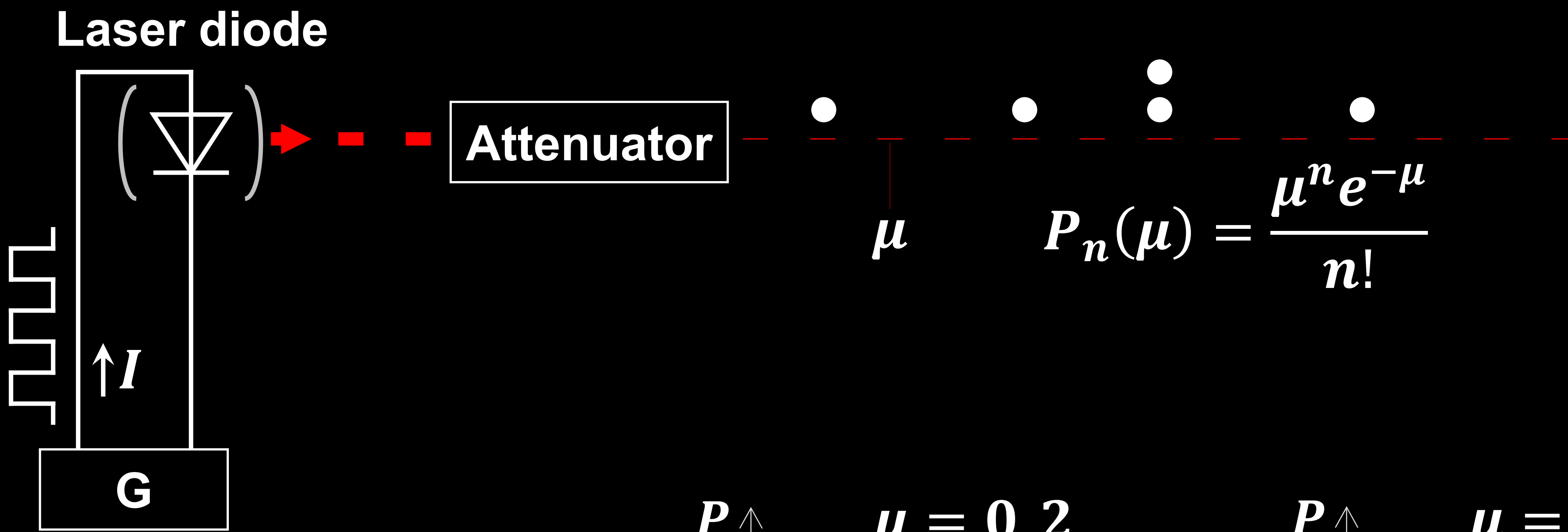
Distributed-phase-reference protocols

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

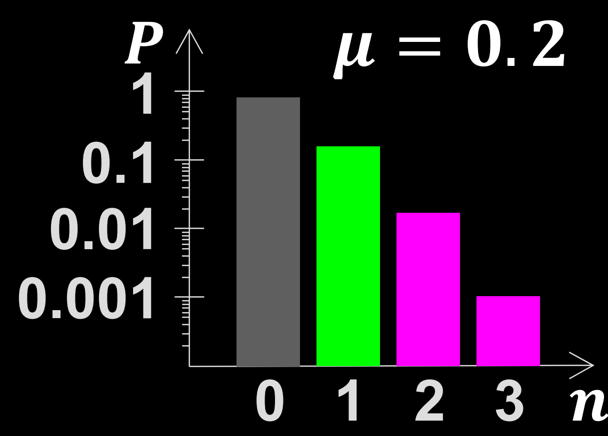
K. Inoue, E. Waks, Y. Yamamoto, Phys. Rev. A. **68**, 022317 (2003)

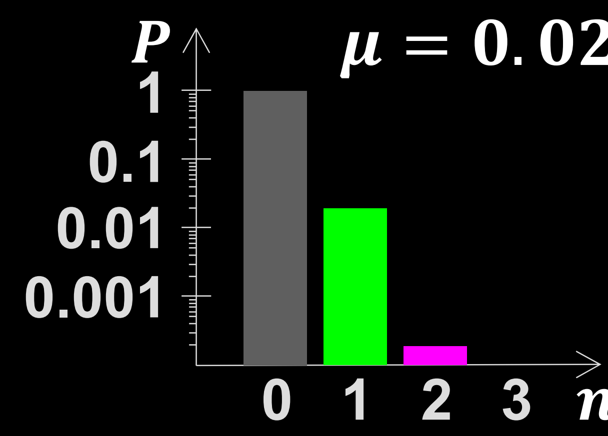
N. Gisin, G. Ribordy, H. Zbinden, D. Stucki, N. Brunner, V. Scarani, arXiv:quant-ph/0411022v1 (2004)

Attenuated laser source



$$P_n(\mu) = \frac{\mu^n e^{-\mu}}{n!}$$





S. J. van Enk, C. A. Fuchs, arXiv:quant-ph/0111157

Commercial QKD

1st generation (circa 2008)
ID Quantique *Cerberis* system

Classical encryptors:

L2, 2 Gbit/s
L2, 10 Gbit/s
L3 VPN, 100 Mbit/s

WDMs

Key manager

QKD to another node (4 km)

QKD to another node (14 km)

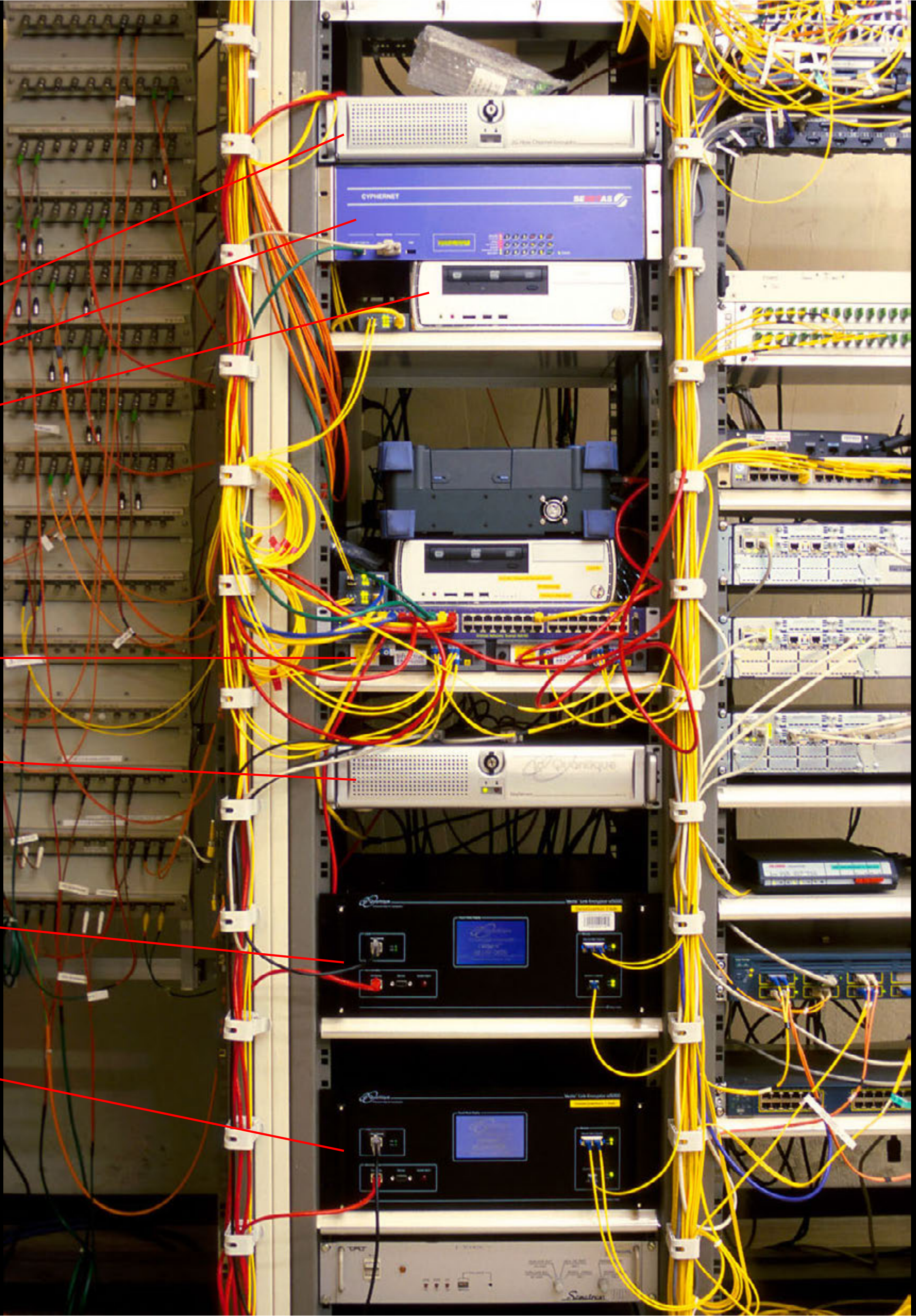
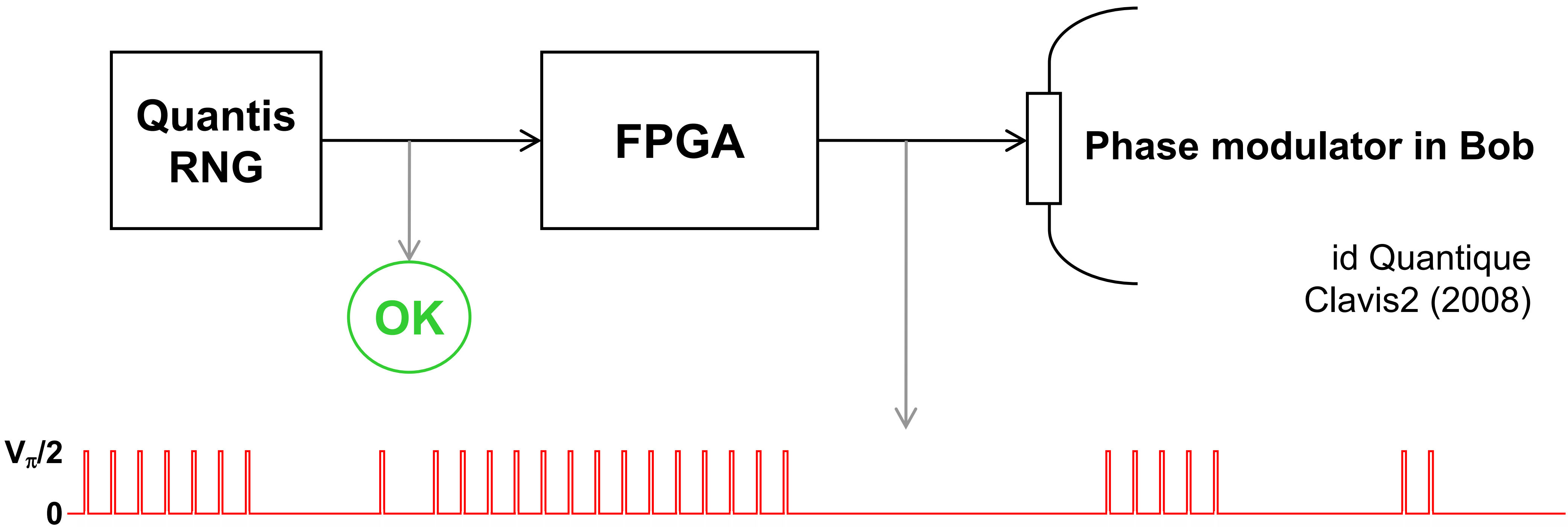


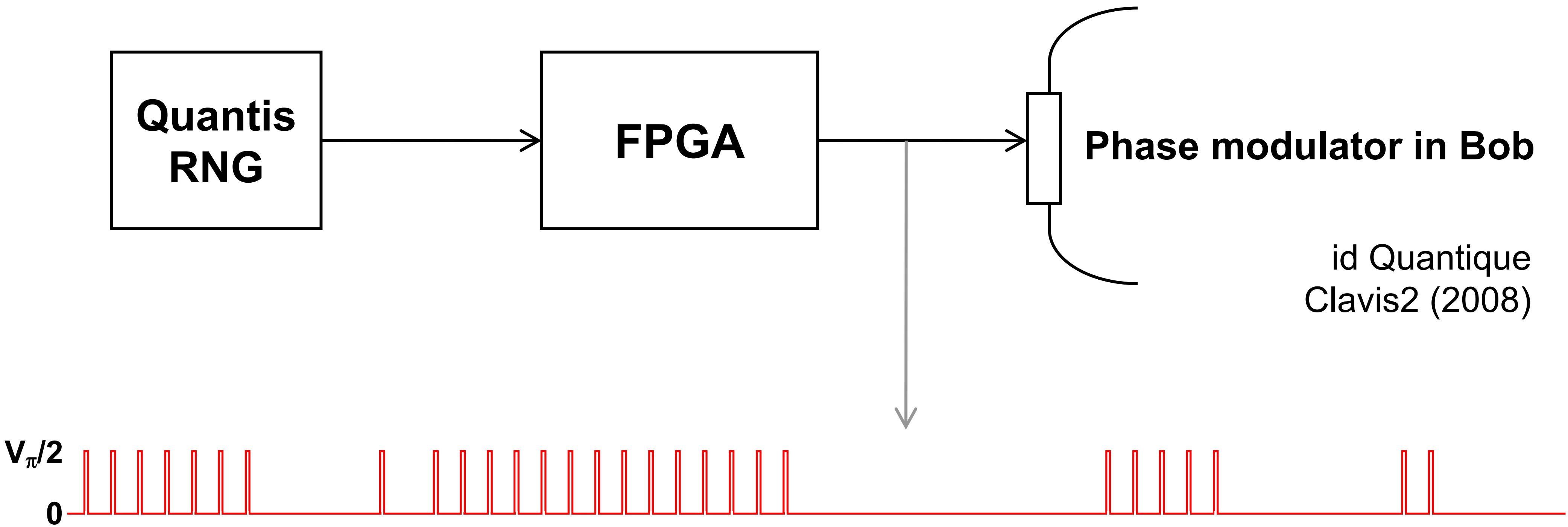
Photo ©2010 Vadim Makarov

www.swissquantum.com

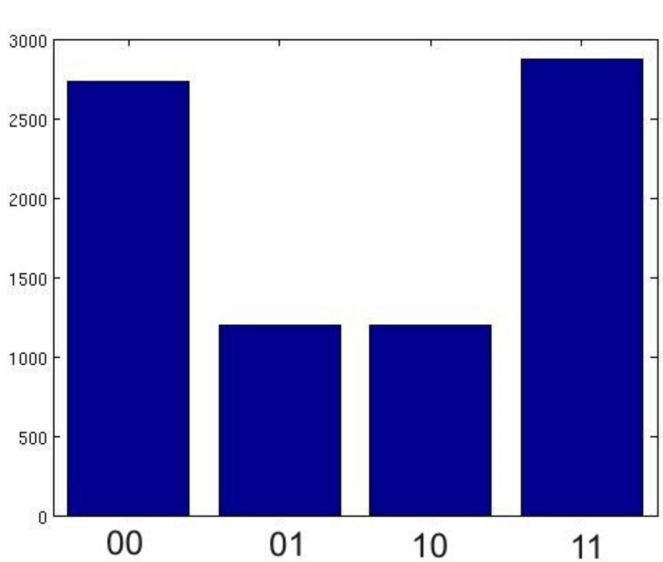
True randomness?



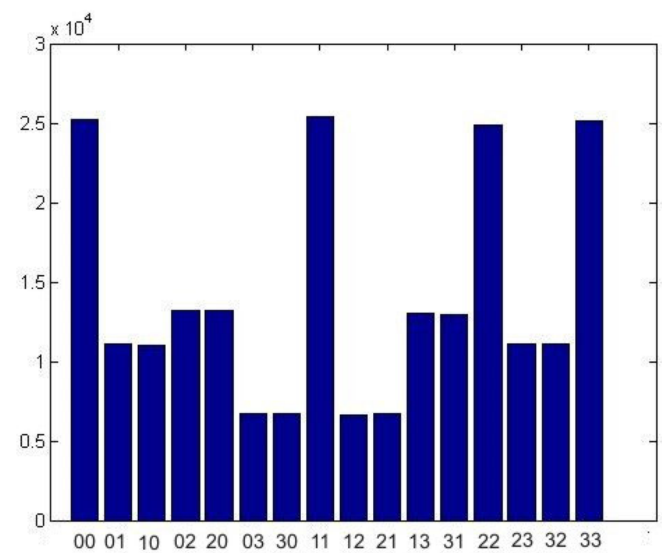
True randomness?



Bob:

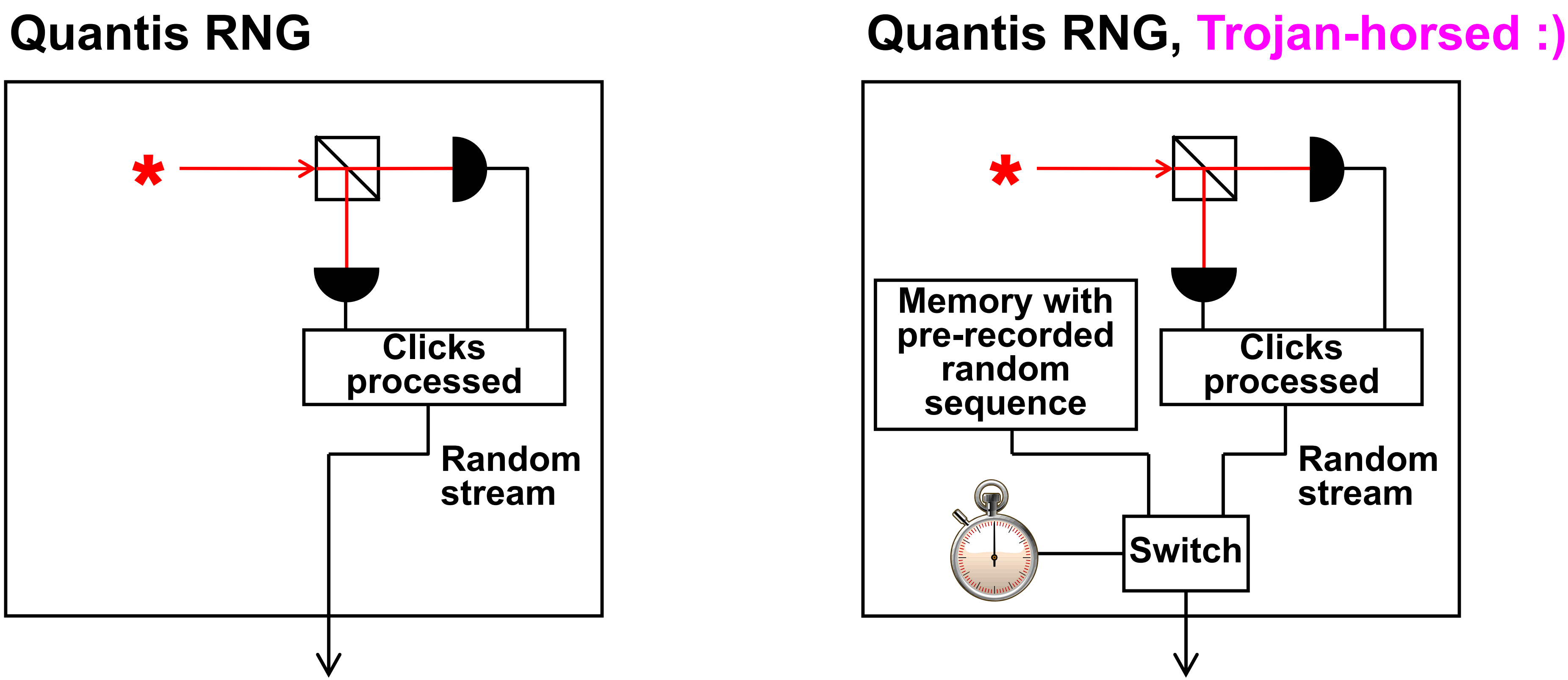


Alice:



Issue reported patched in 2010

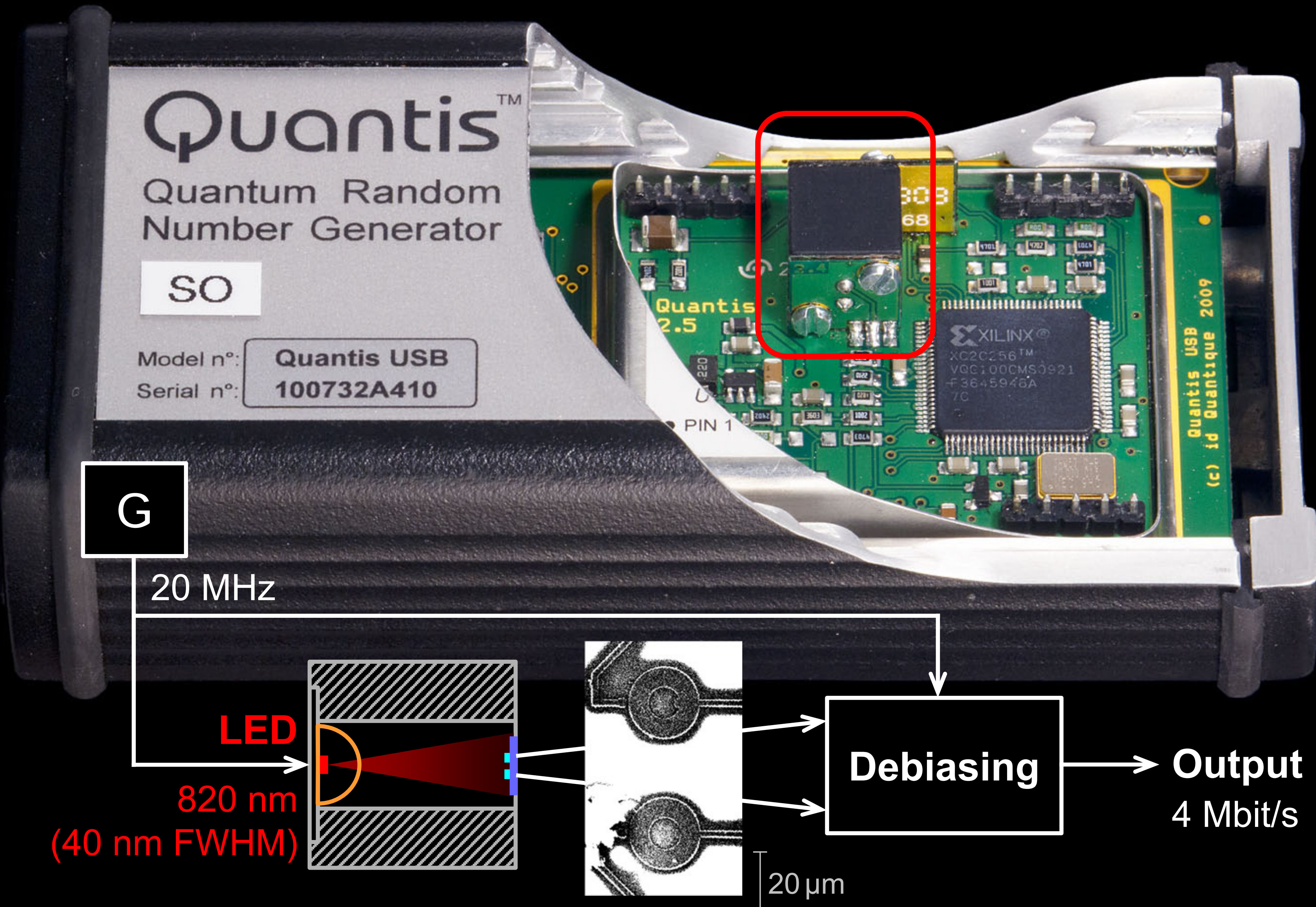
Do we trust the manufacturer?



Many components in QKD system can be Trojan-horsed:

– access to secret information
– electrical power
– way to communicate outside or compromise security

Quantis RNG: what's inside?



G. Ribordy, O. Guinnard, US patent appl. US 2007/0127718 A1 (filed in 2006)
M. Petrov, I. Radchenko *et al.*, EPJ Quantum Technol. **9**, 17 (2022)

ID Quantique Clavis2 QKD system

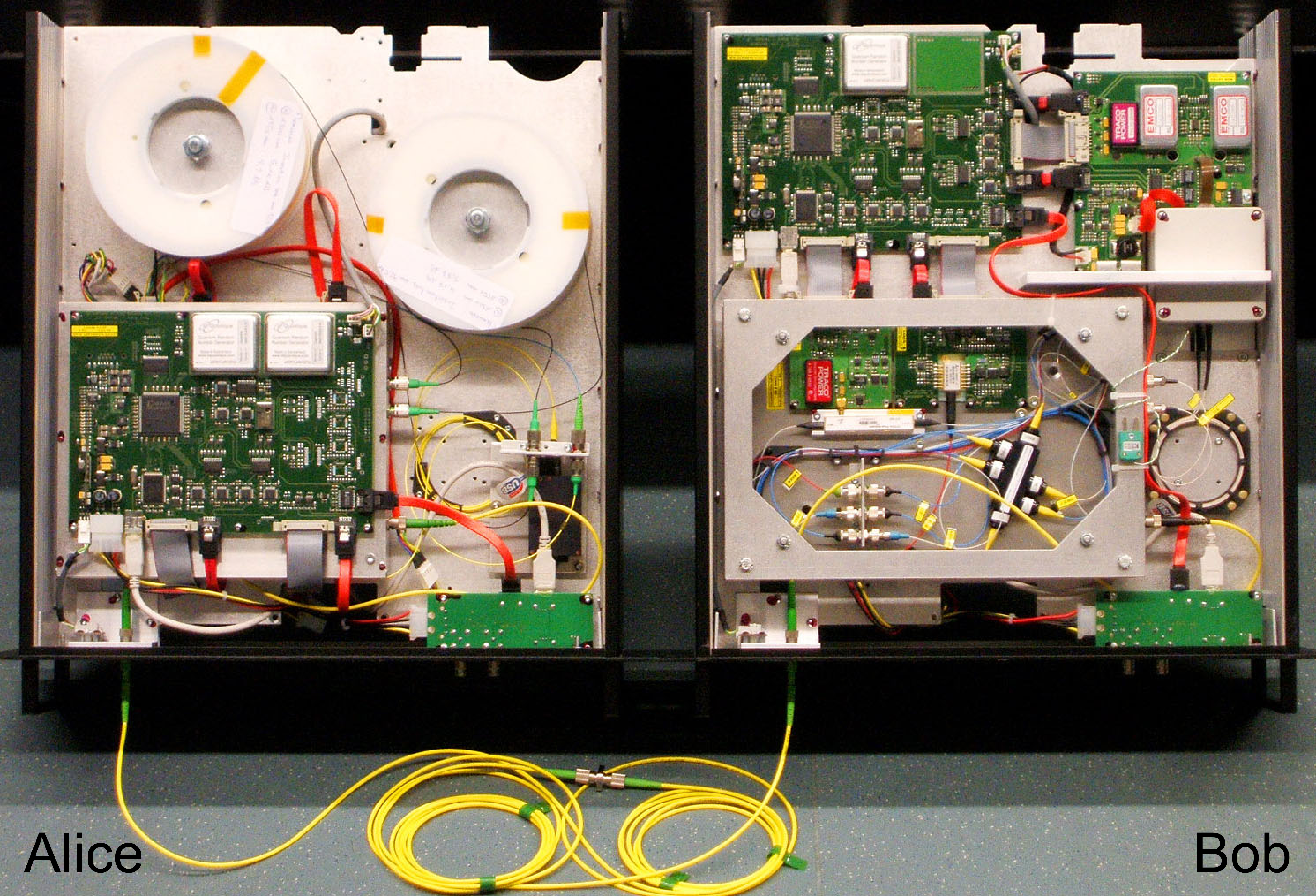


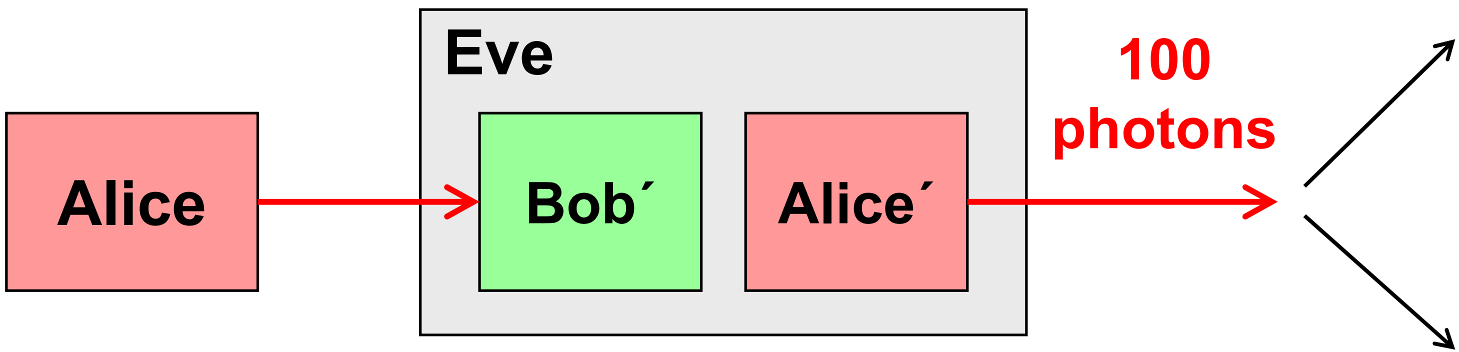
Photo ©2008 Vadim Makarov. Published with approval of ID Qiantique

Double clicks

– occur naturally because of detector dark counts, multi-photon pulses...

Discard them?

Intercept-resend attack... with a twist:



Bob:

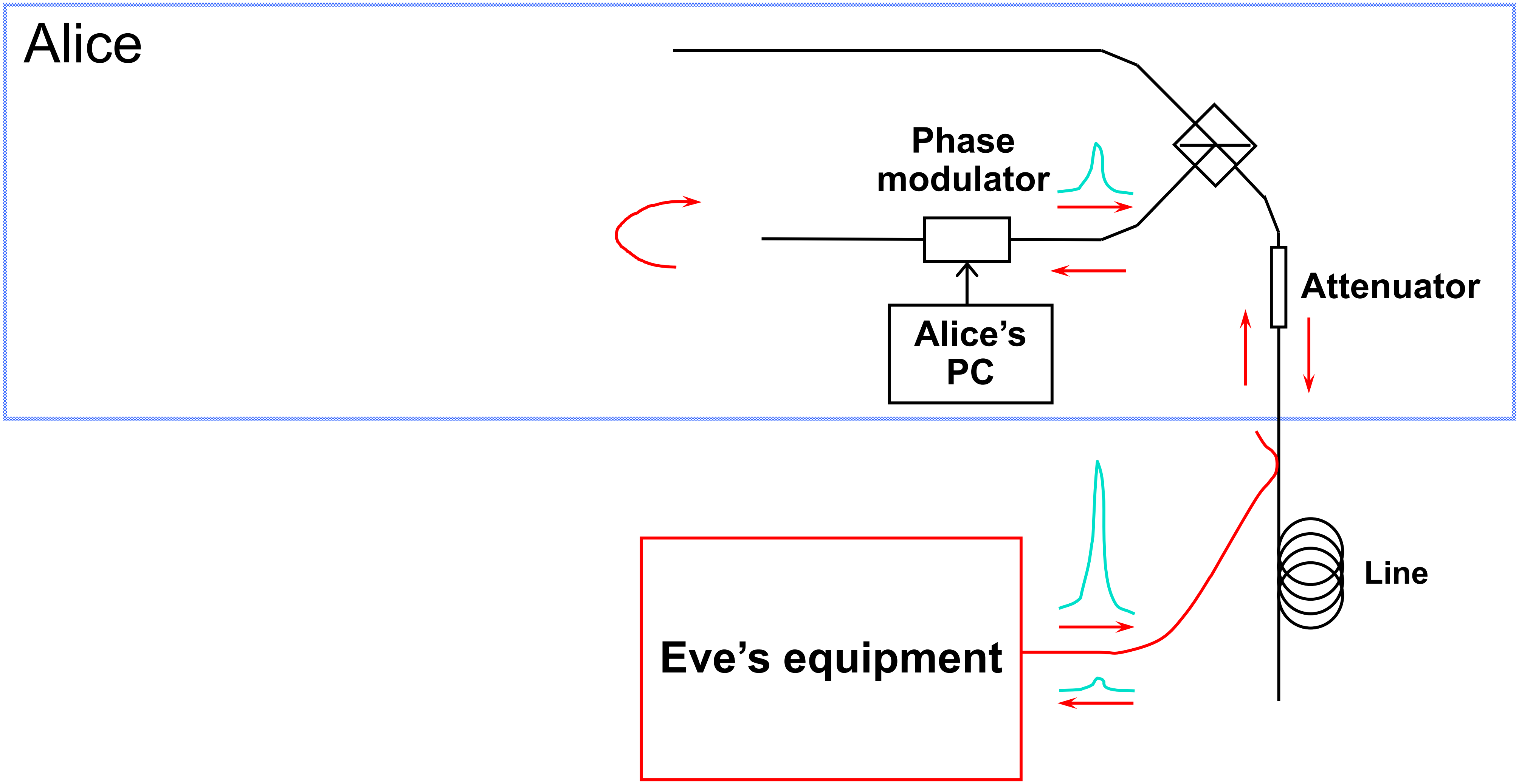
Detects in Eve's basis: single click

Detects in conjugate basis: double click, discarded

Proper treatment for double clicks: assign a random bit value.

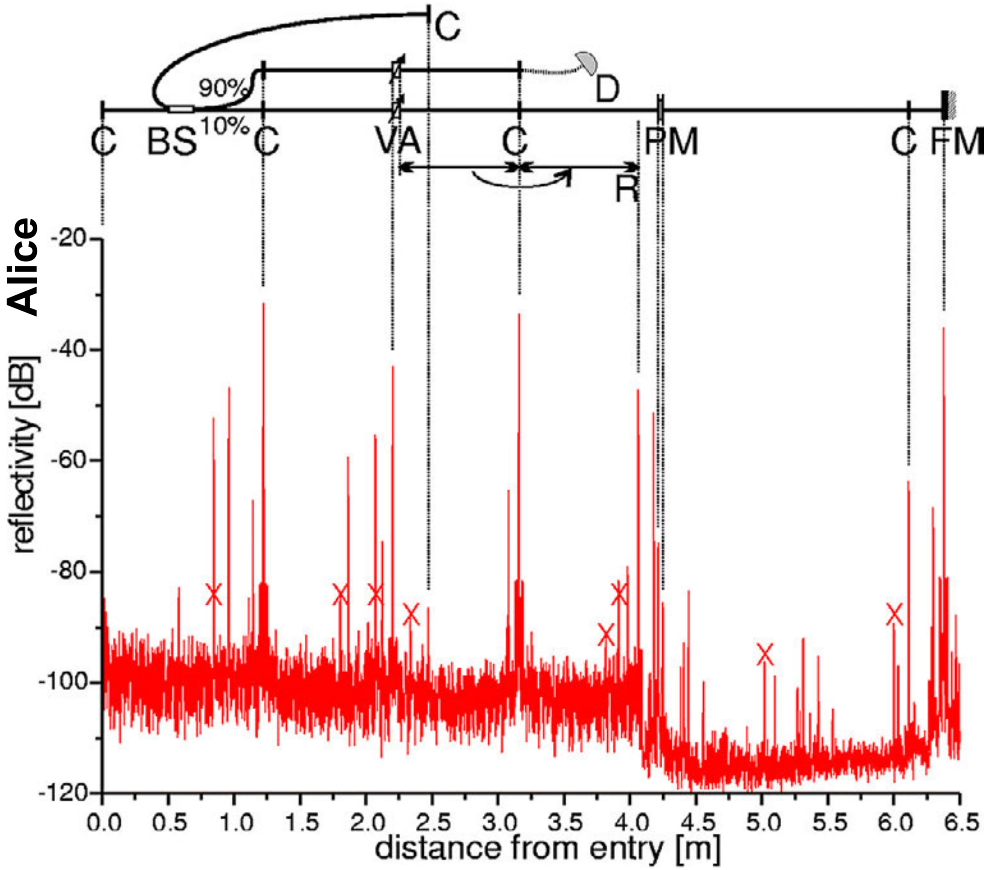
N. Lütkenhaus, Phys. Rev. A **59**, 3301 (1999)
T. Tsurumaru & K. Tamaki, Phys. Rev. A **78**, 032302 (2008)

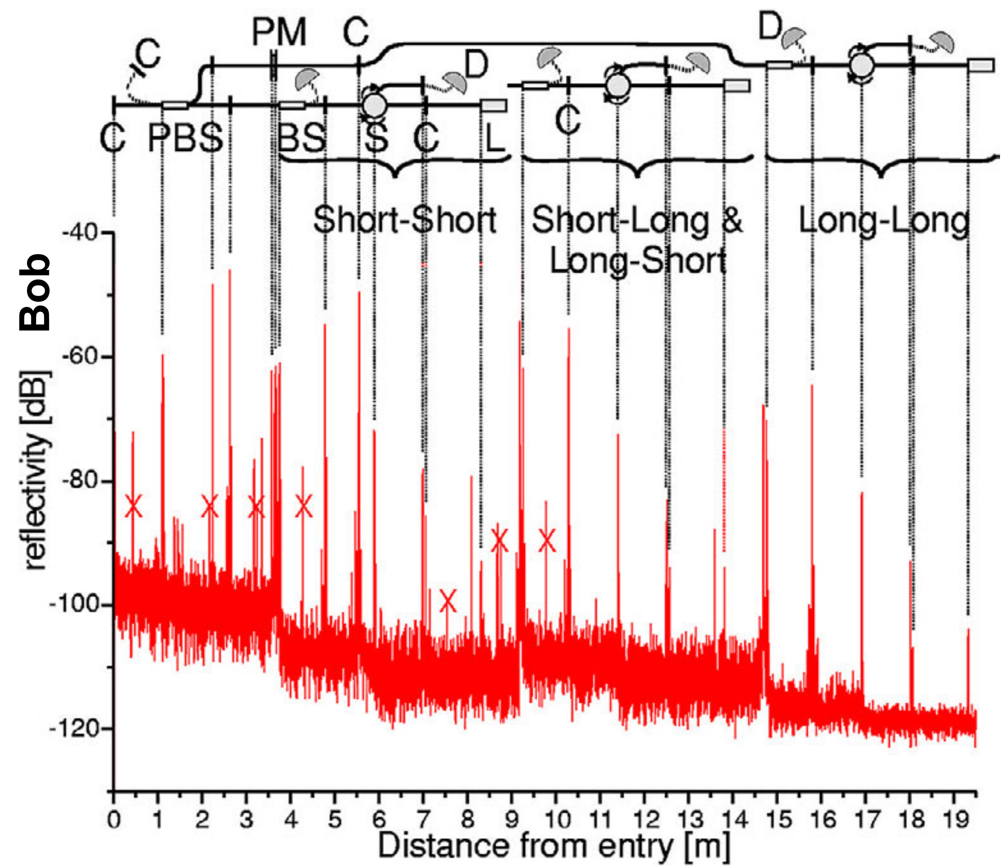
Trojan-horse attack



– interrogating Alice's phase modulator with powerful external pulses (can give Eve bit values directly)

Trojan-horse attack for plug-and-play system

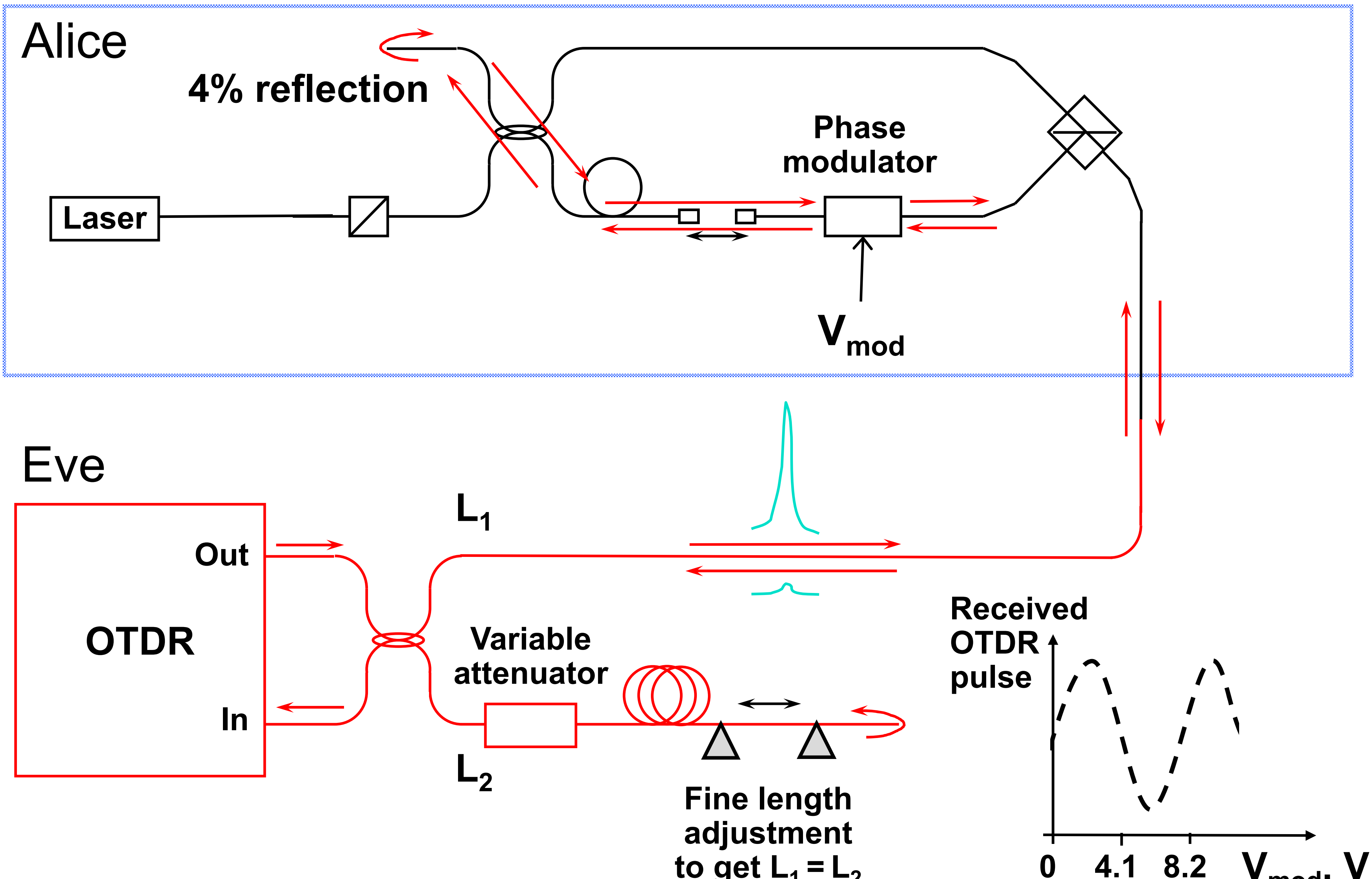




Eve gets back one photon $\rightarrow$ in principle, extracts 100% information

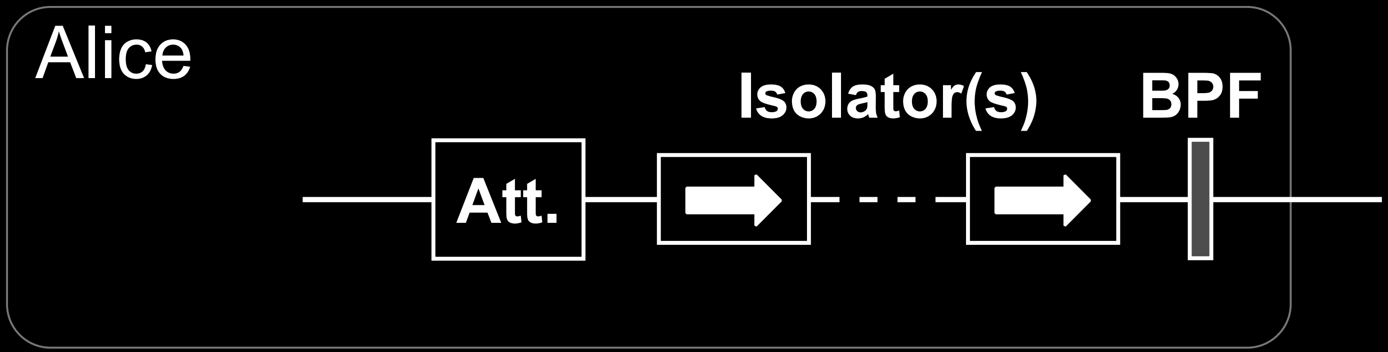
N. Gisin *et al.*, Phys. Rev. A **73**, 022320 (2006)

Trojan-horse attack experiment



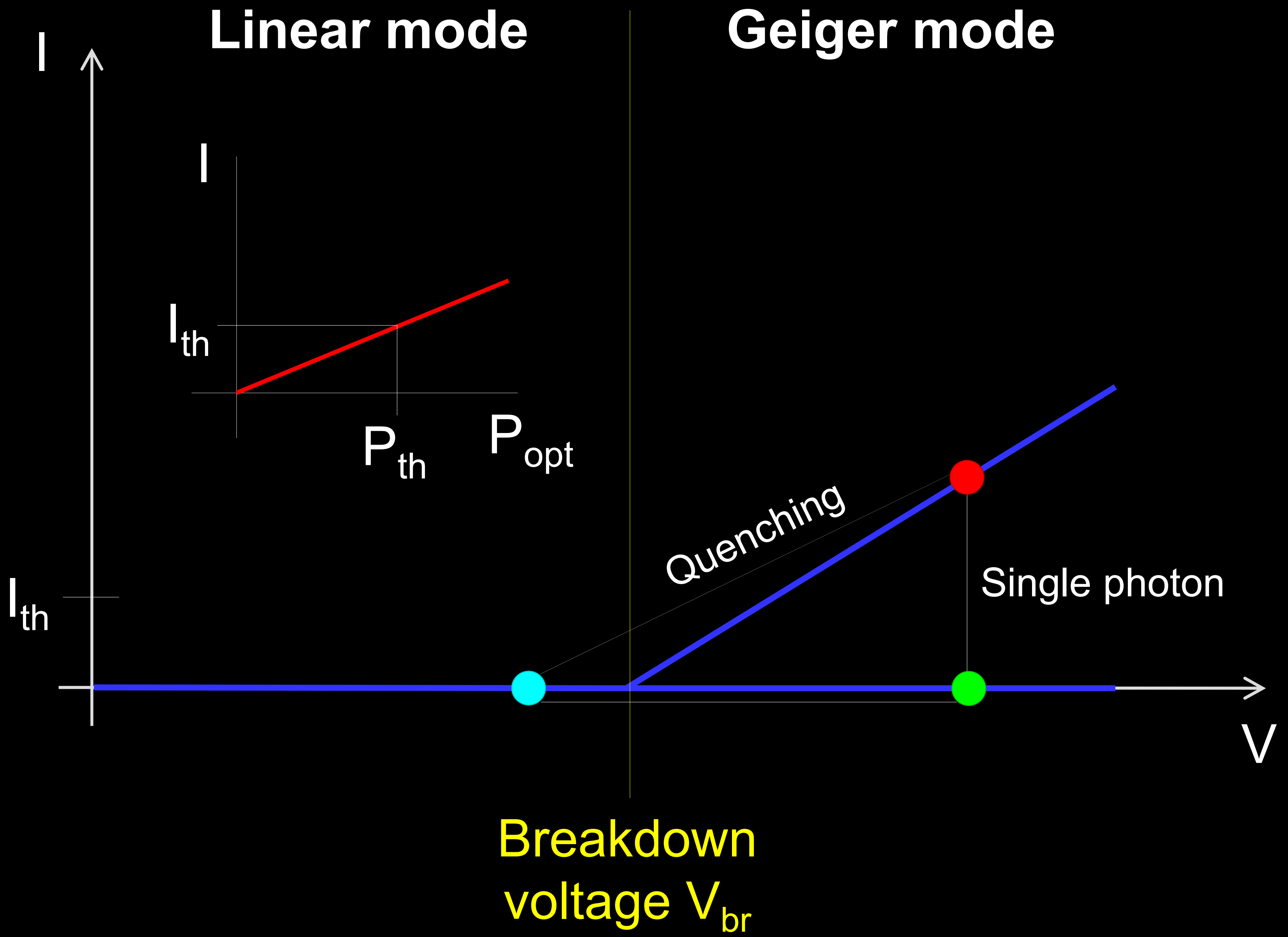
A. Vakhitov *et al.*, J. Mod. Opt. **48**, 2023 (2001)

Draft security standard @ ETSI: Trojan-horse in one-way system

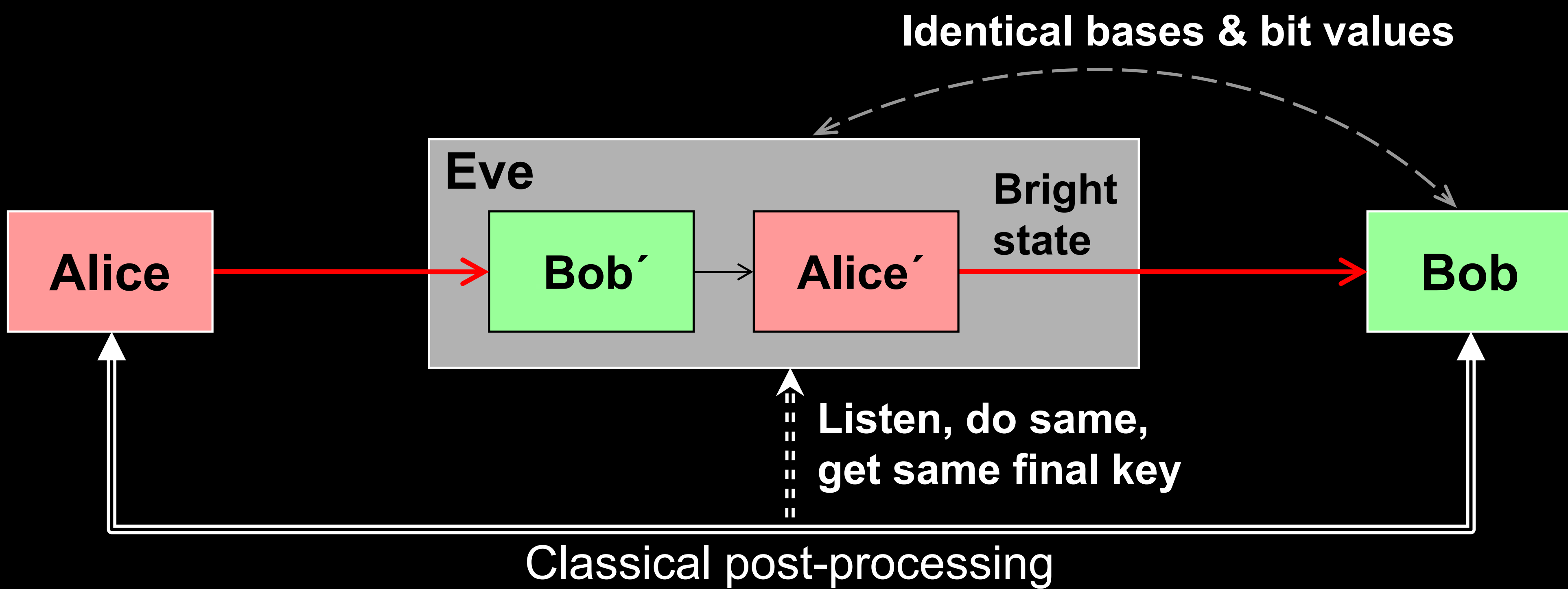


M. Lucamarini *et al.*, Phys. Rev. X **5**, 031030 (2015)

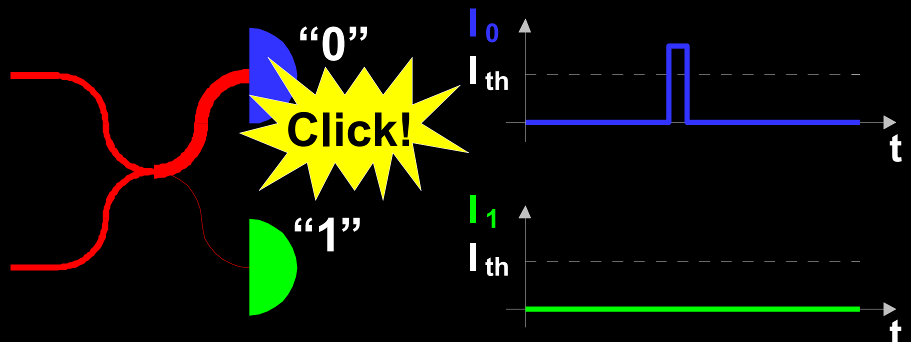
Attack example: avalanche photodetectors (APDs)



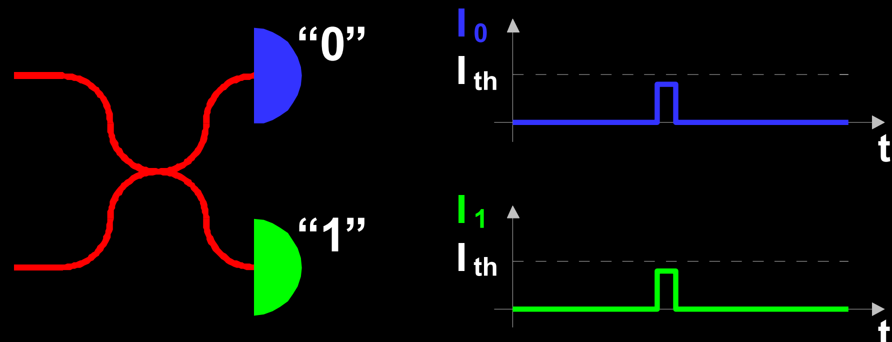
Faked-state attack in APD linear mode



Bob chooses same basis as Eve:

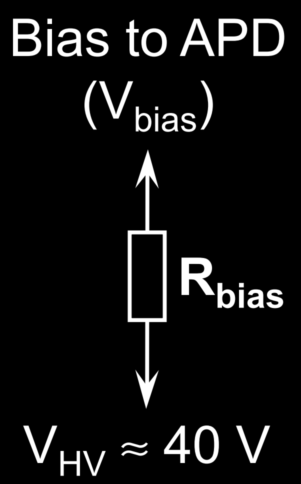


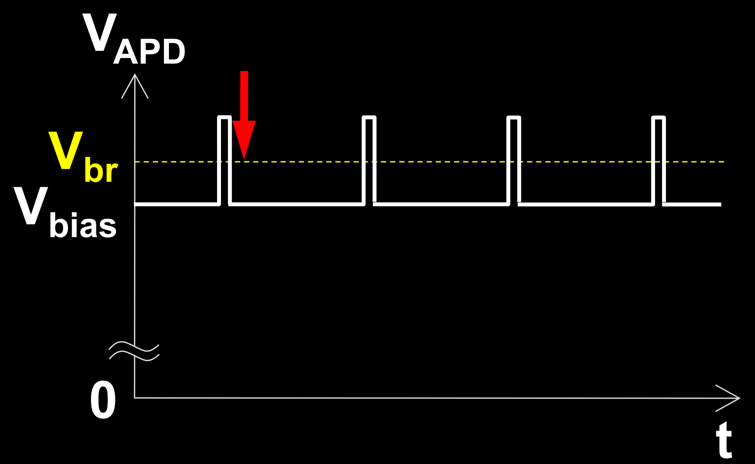
Bob chooses different basis:



L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, V. Makarov, Nat. Photonics **4**, 686 (2010)

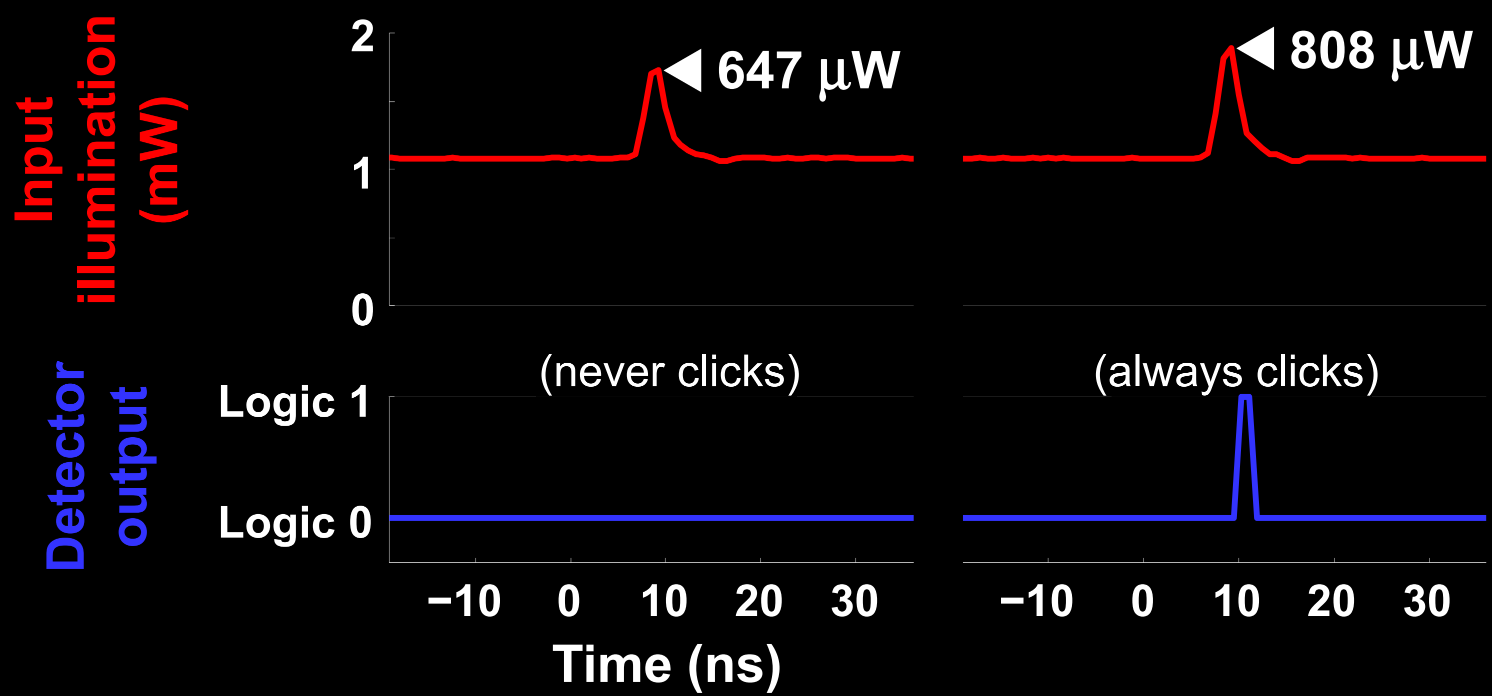
Blinding APD with bright light





Eve applies CW light

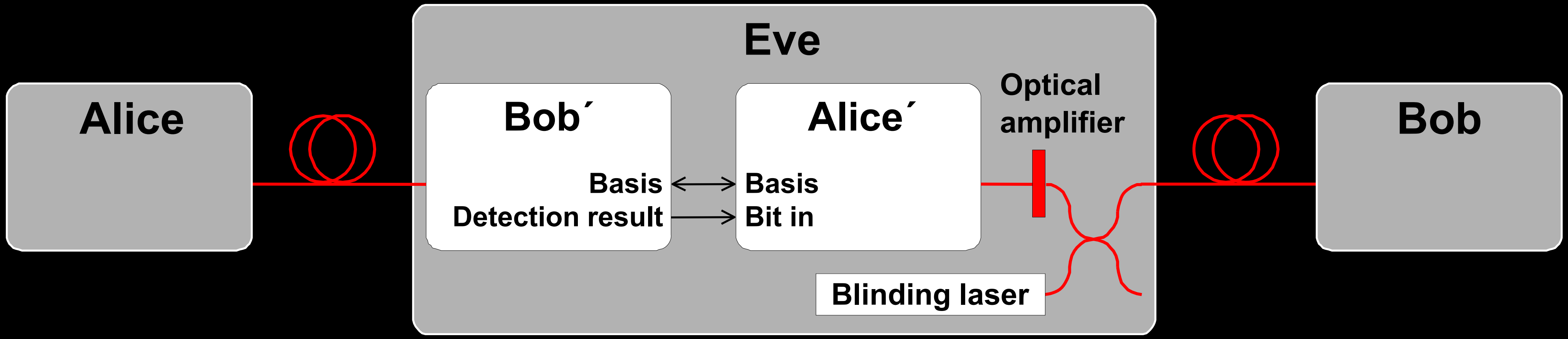
⇨ **Detector blind!**
Zero dark count rate



ID Quantique Clavis2

L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, V. Makarov, Nat. Photonics **4**, 686 (2010)

Proposed full eavesdropper

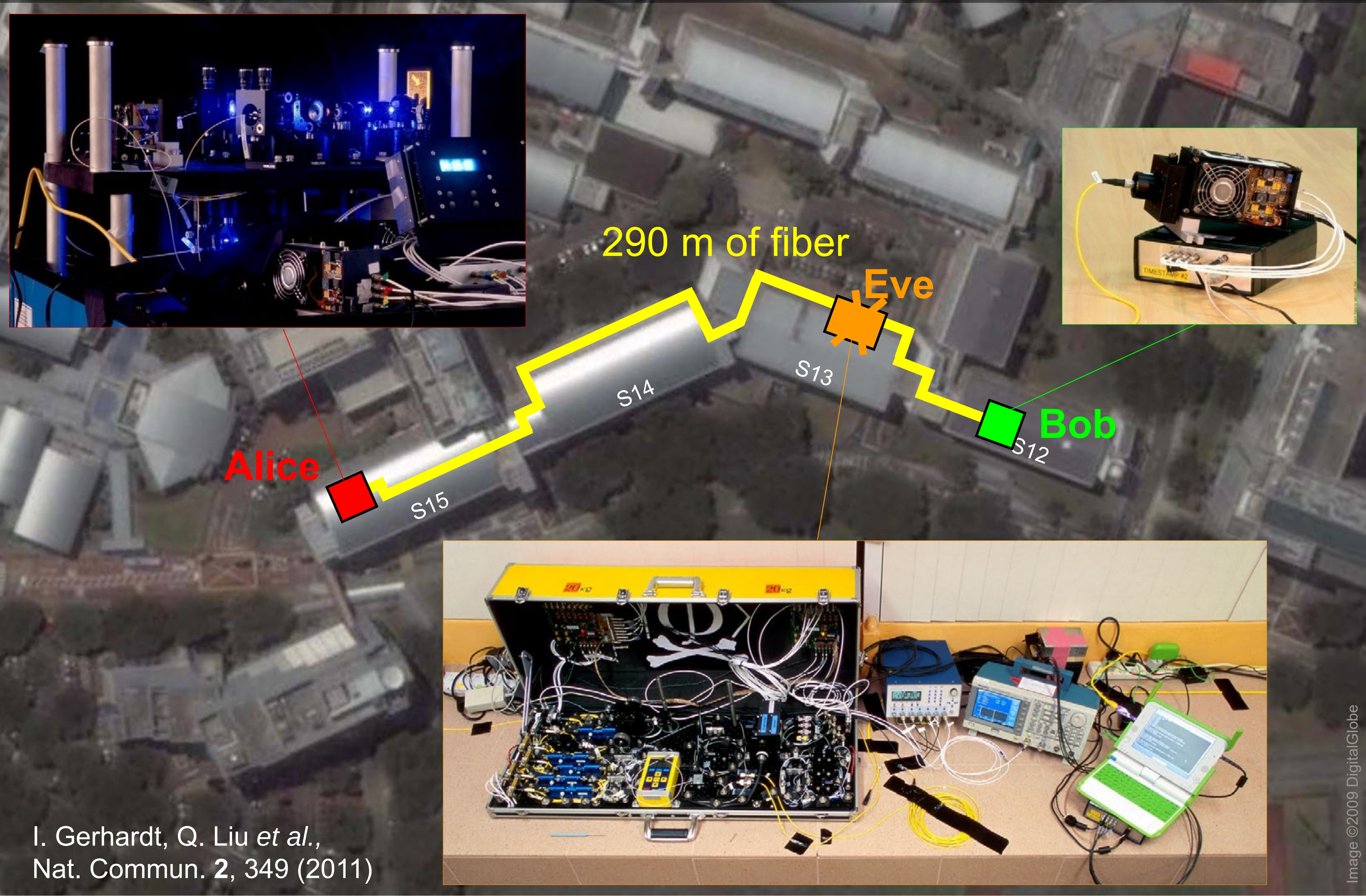


Note: Intercept-resend always breaks QKD security

M. Curty, M. Lewenstein, N. Lütkenhaus, Phys. Rev. Lett. **92**, 217903 (2004)

Eavesdropping 100% key on installed QKD line

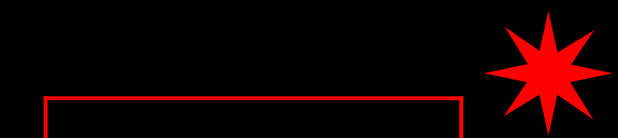
on campus of the National University of Singapore, July 4–5, 2009



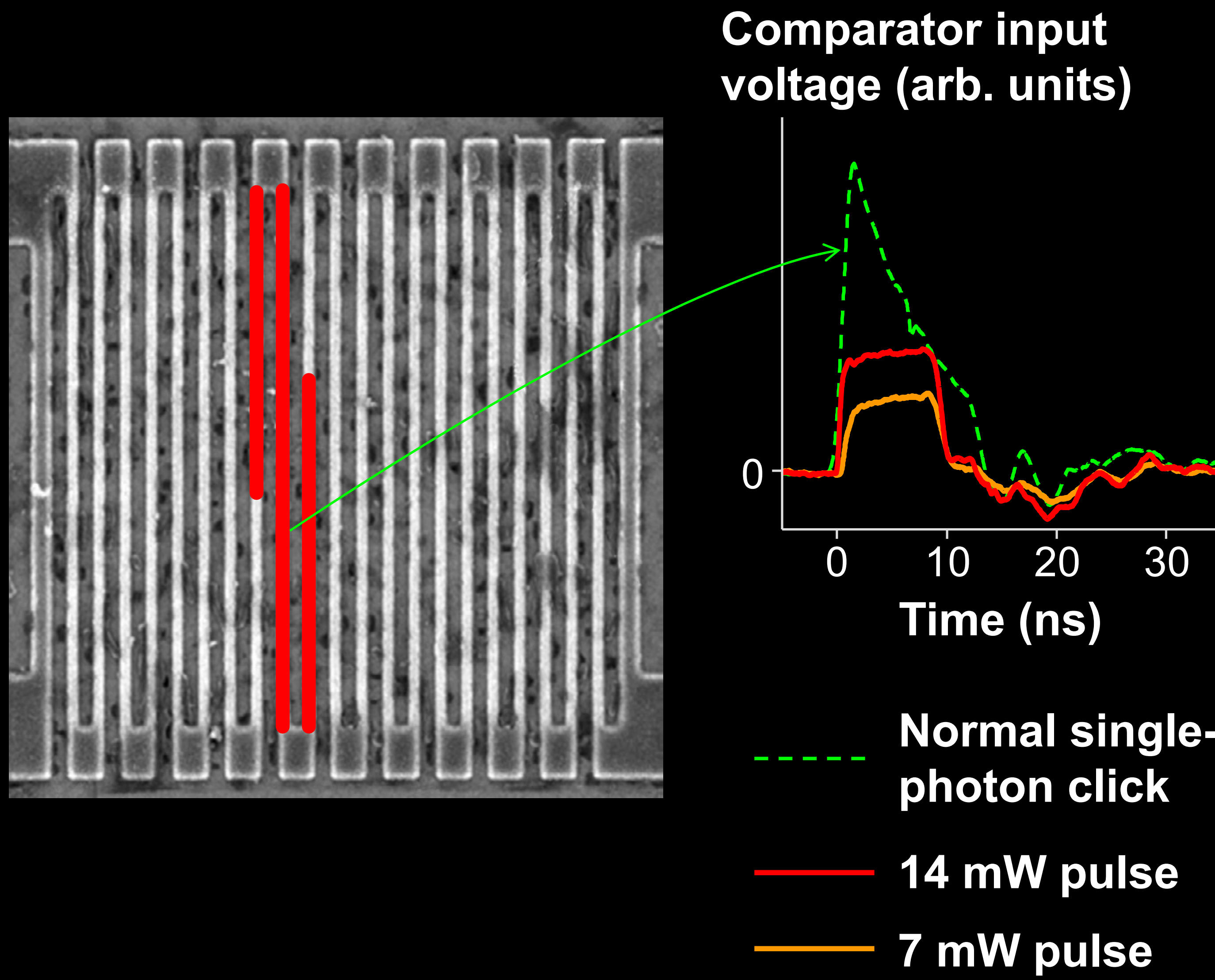
I. Gerhardt, Q. Liu *et al.*,
Nat. Commun. **2**, 349 (2011)

Controlling superconducting nanowire single-photon detectors

1. Blind (latch)

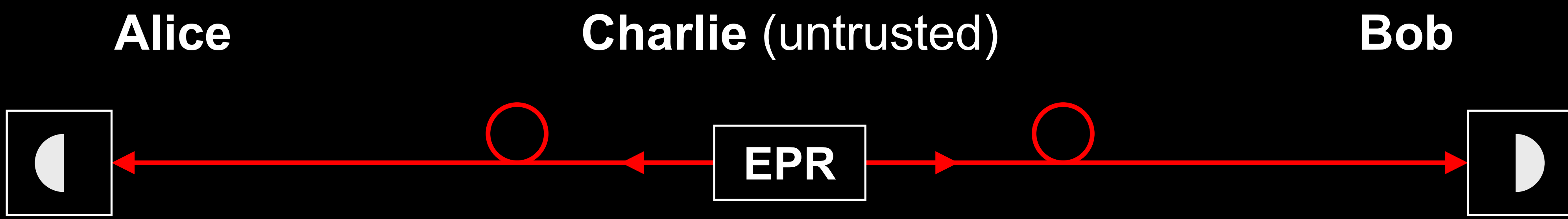


2. Control

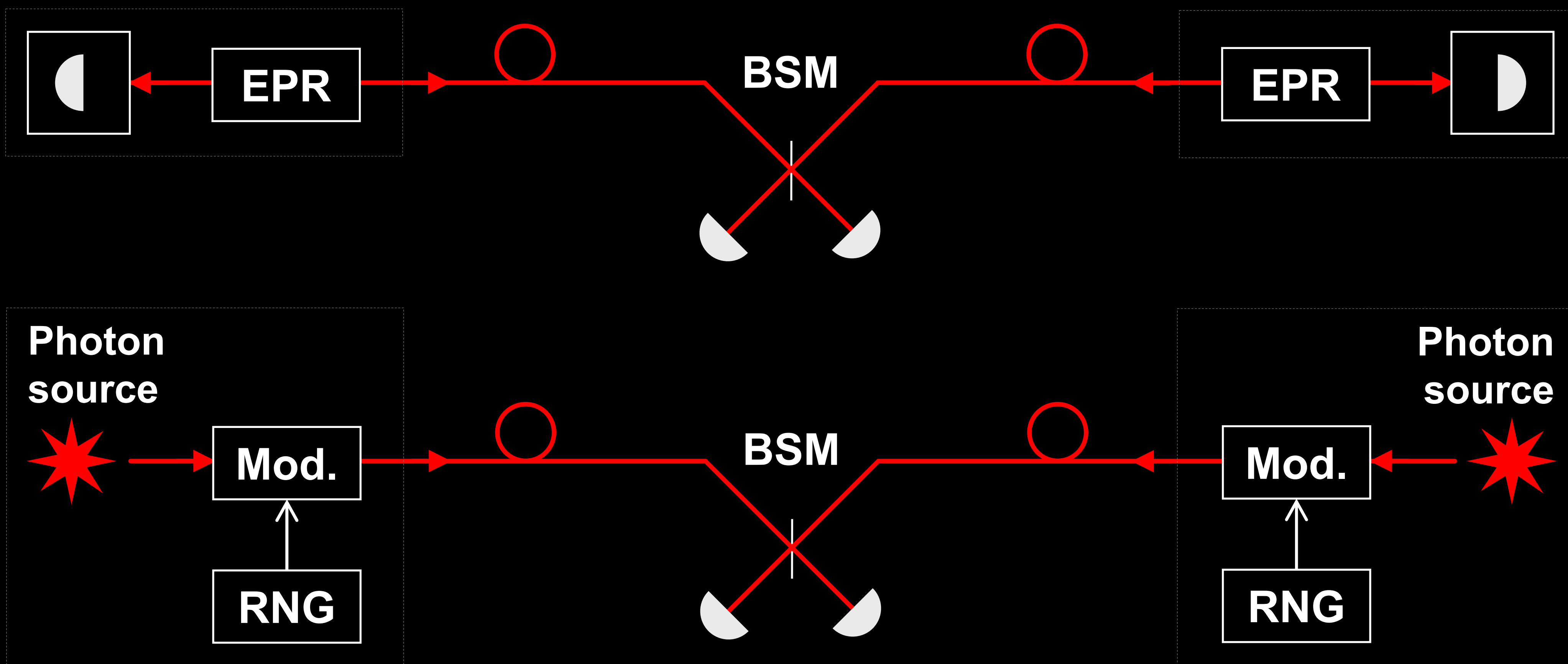


L. Lydersen, M. K. Akhlaghi, A. H. Majedi, J. Skaar, V. Makarov, New J. Phys. **13**, 113042 (2011)
M. G. Tanner, V. Makarov, R. H. Hadfield, Opt. Express **22**, 6734 (2014)

Countermeasures to detector attacks?



A. Ekert, Phys. Rev. Lett. **67**, 661 (1991); C. H. Bennett *et al.*, Phys. Rev. Lett. **68**, 557 (1992)



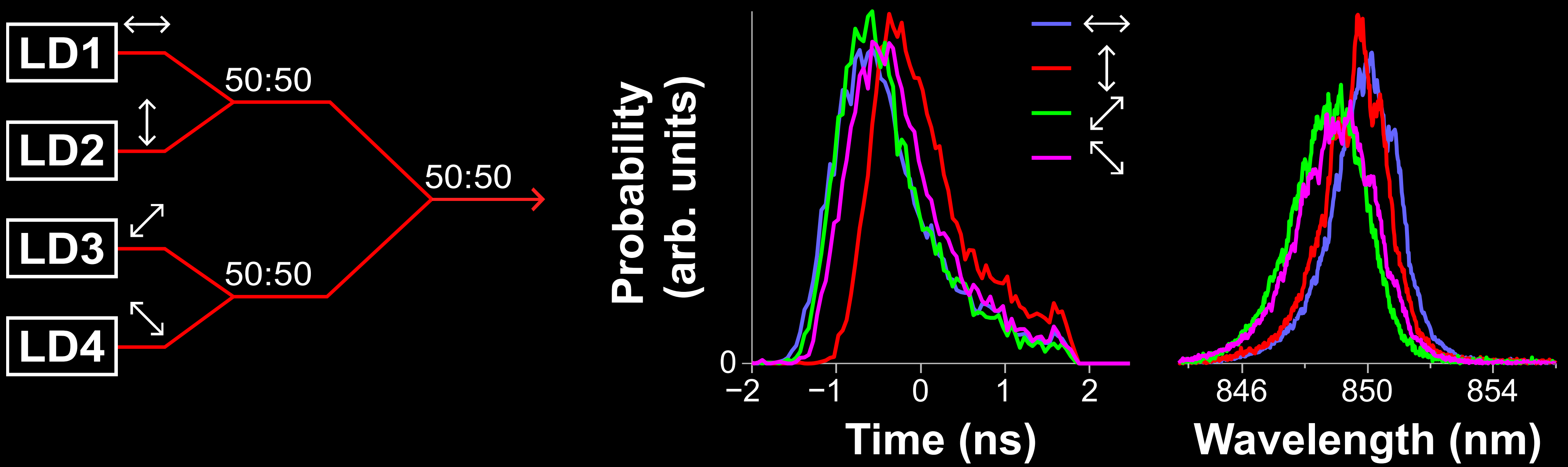
Measurement-device-independent QKD

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

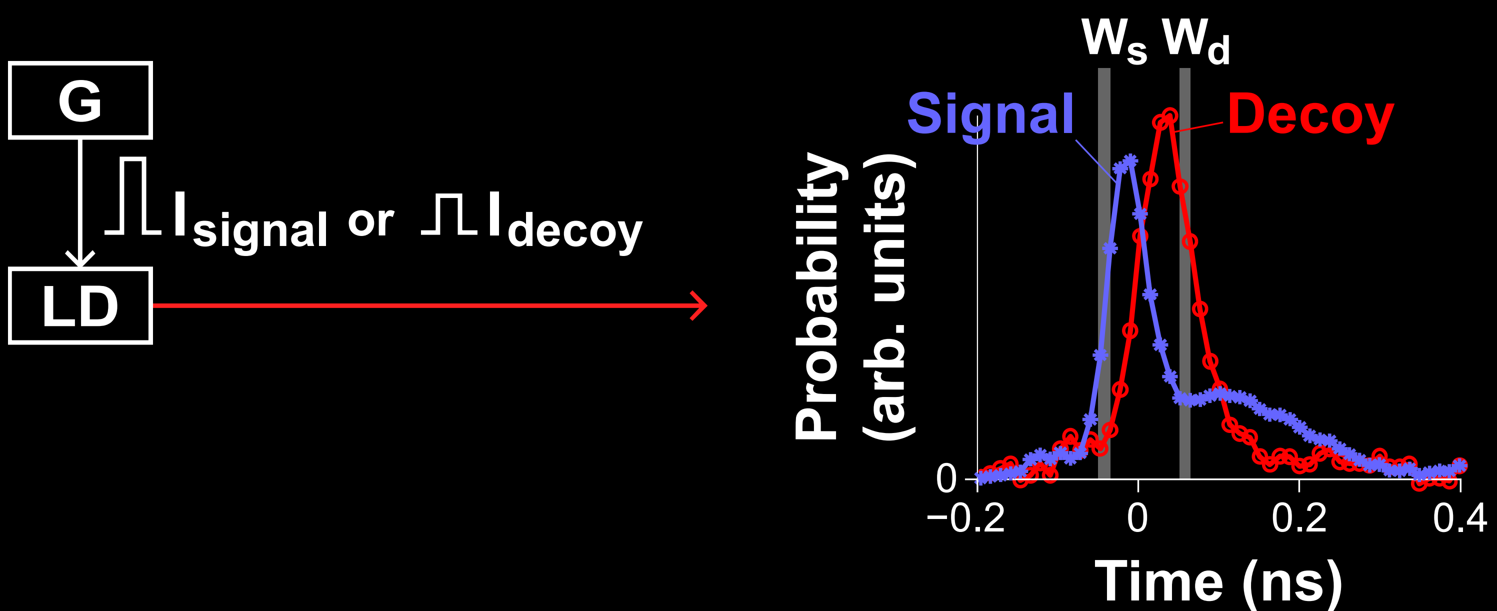
3 ways to deal with an imperfection

- Technical countermeasure that attempts to stop the attack
- Make a scheme intrinsically insensitive to imperfection
- Characterise imperfection, upper-bound *partial* information leakage, eliminate it by privacy amplification

Distinguishability of source states

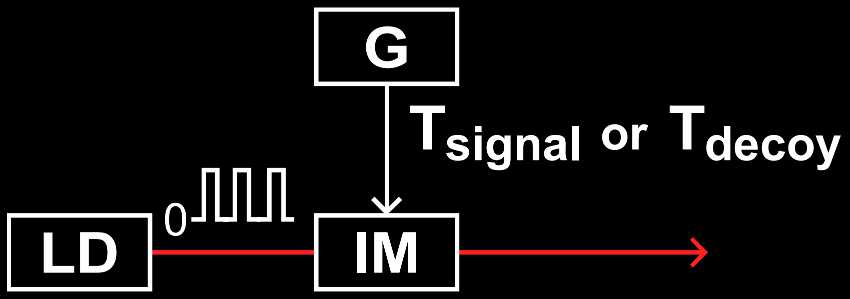


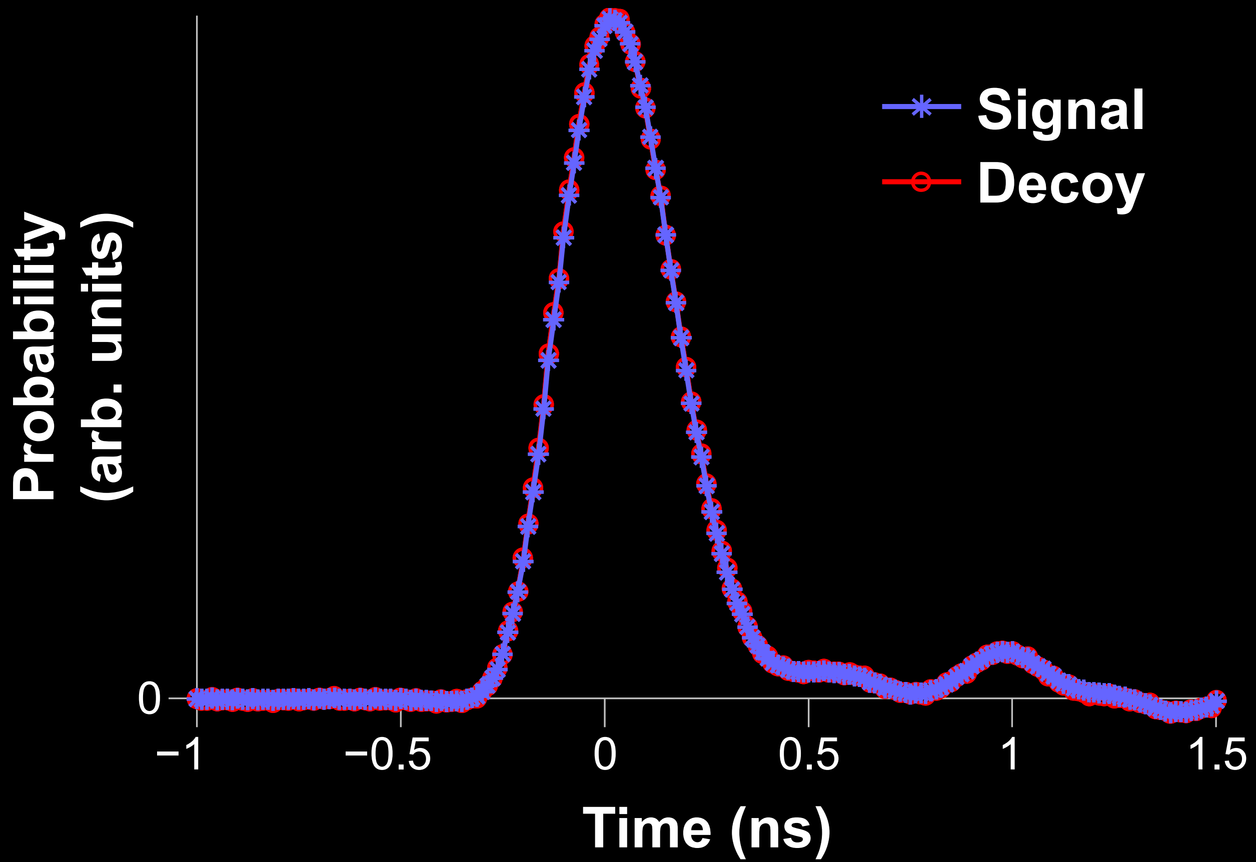
S. Nauerth *et al.*, New J. Phys. **11**, 065001 (2009)



A. Huang, S.-H. Sun, Z. Liu, V. Makarov, Phys. Rev. A **98**, 012330 (2018)

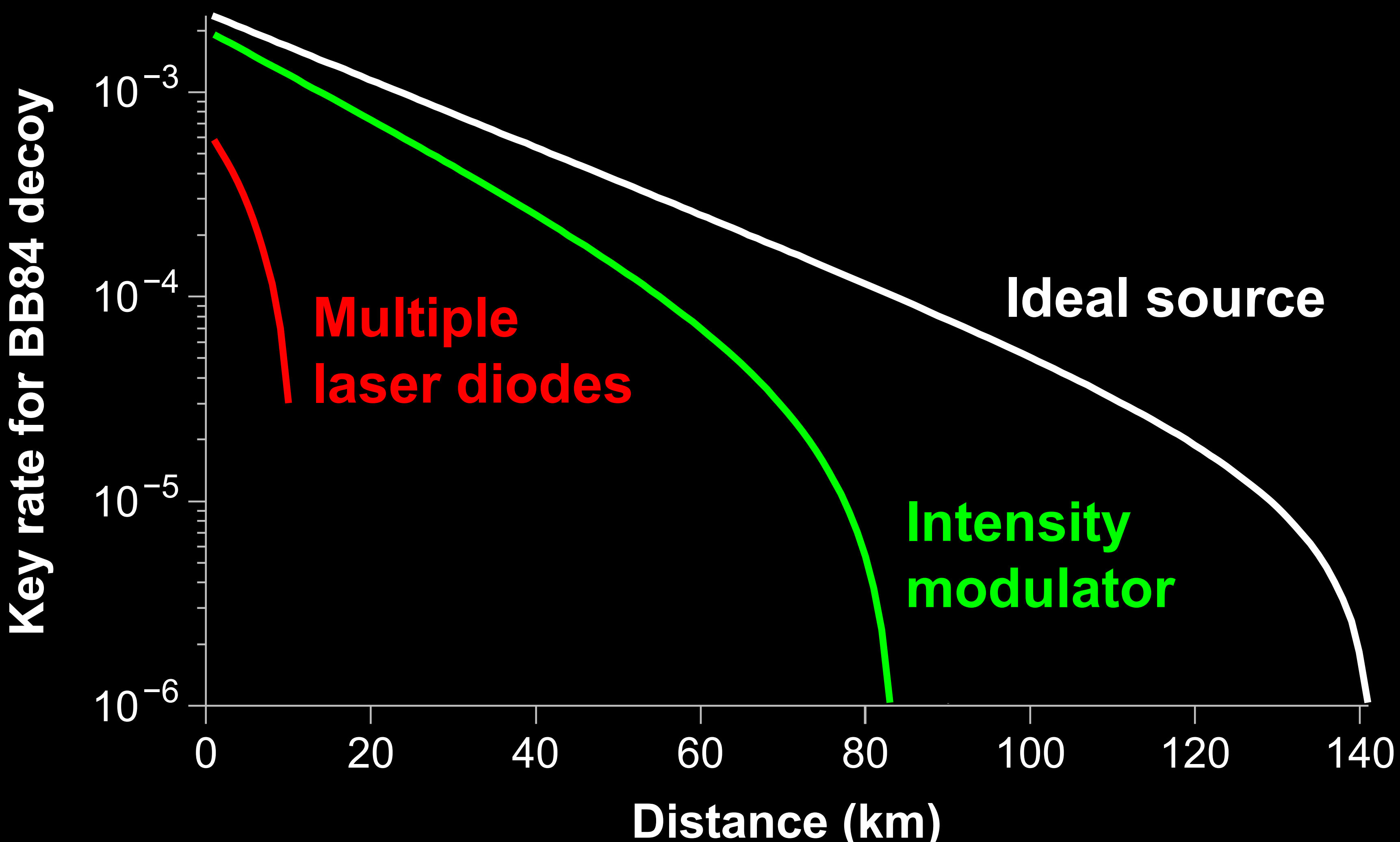
Distinguishability of source states





A. Huang, S.-H. Sun, Z. Liu, V. Makarov, Phys. Rev. A **98**, 012330 (2018)

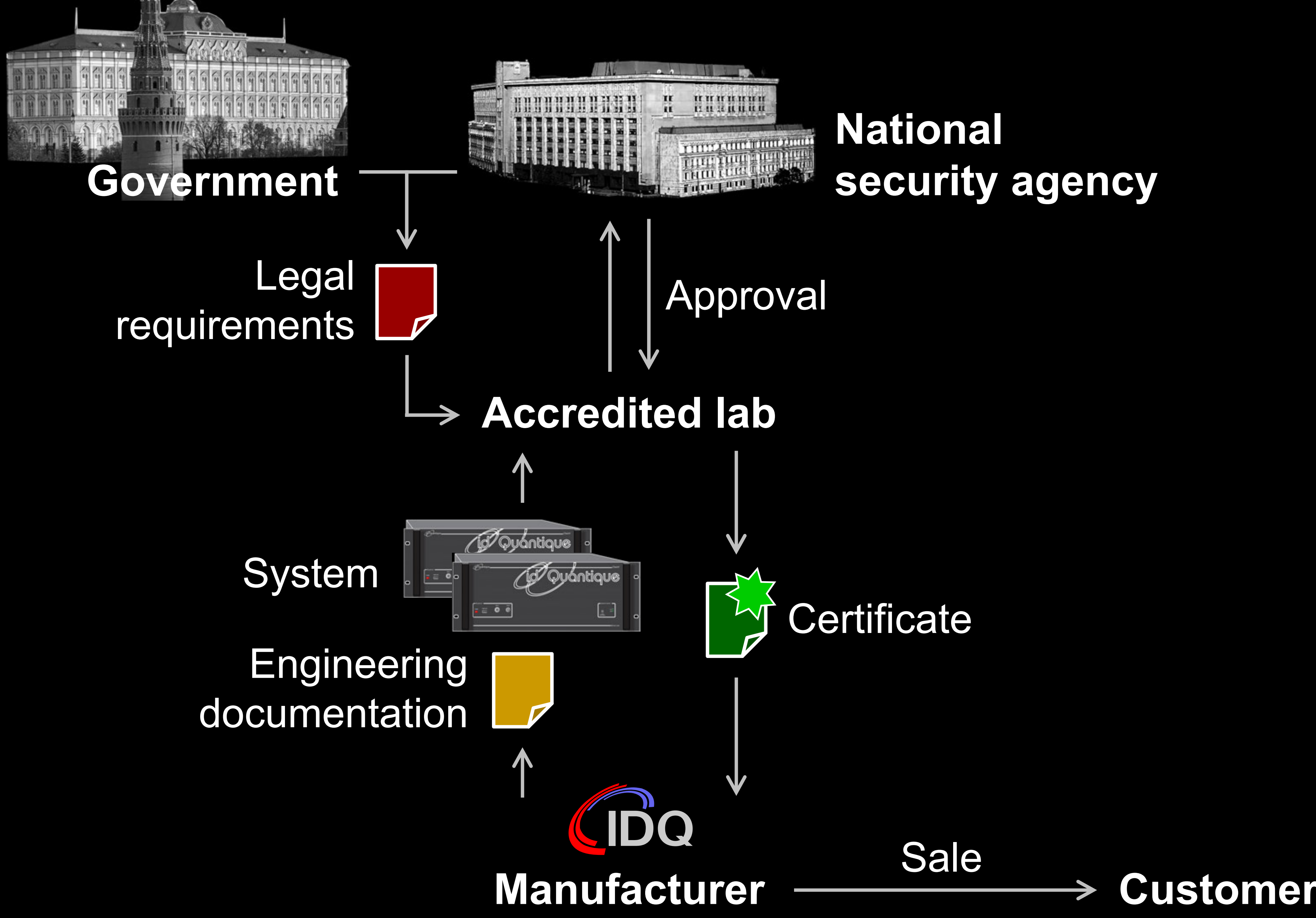
Distinguishability of source states

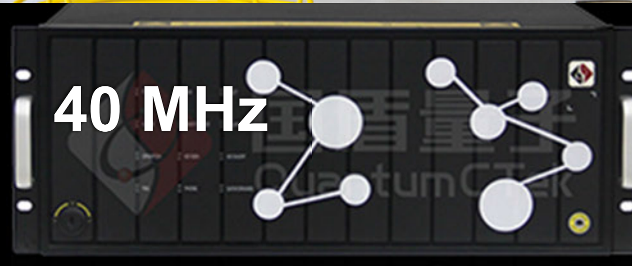


Pump-current modulation: zero key rate

A. Huang, S.-H. Sun, Z. Liu, V. Makarov, Phys. Rev. A **98**, 012330 (2018)

Certification of cryptographic tools



Security audit	System	Report	Tests
IDQ	 Clavis3	2016	–2018 interrupted
国盾量子 QuantumCTek	 40 MHz	2016, 2018–19	ongoing
ITMO UNIVERSITY (ООО Квантовые коммуникации)	Subcarrier scheme	2018	–2021
QRATE	312.5 MHz	2022	ongoing

S. Sajeed *et al.*, Sci. Rep. **11**, 5110 (2021)

Certification standards are being drafted since 2019 in

ETSI **Industry standards group in QKD**

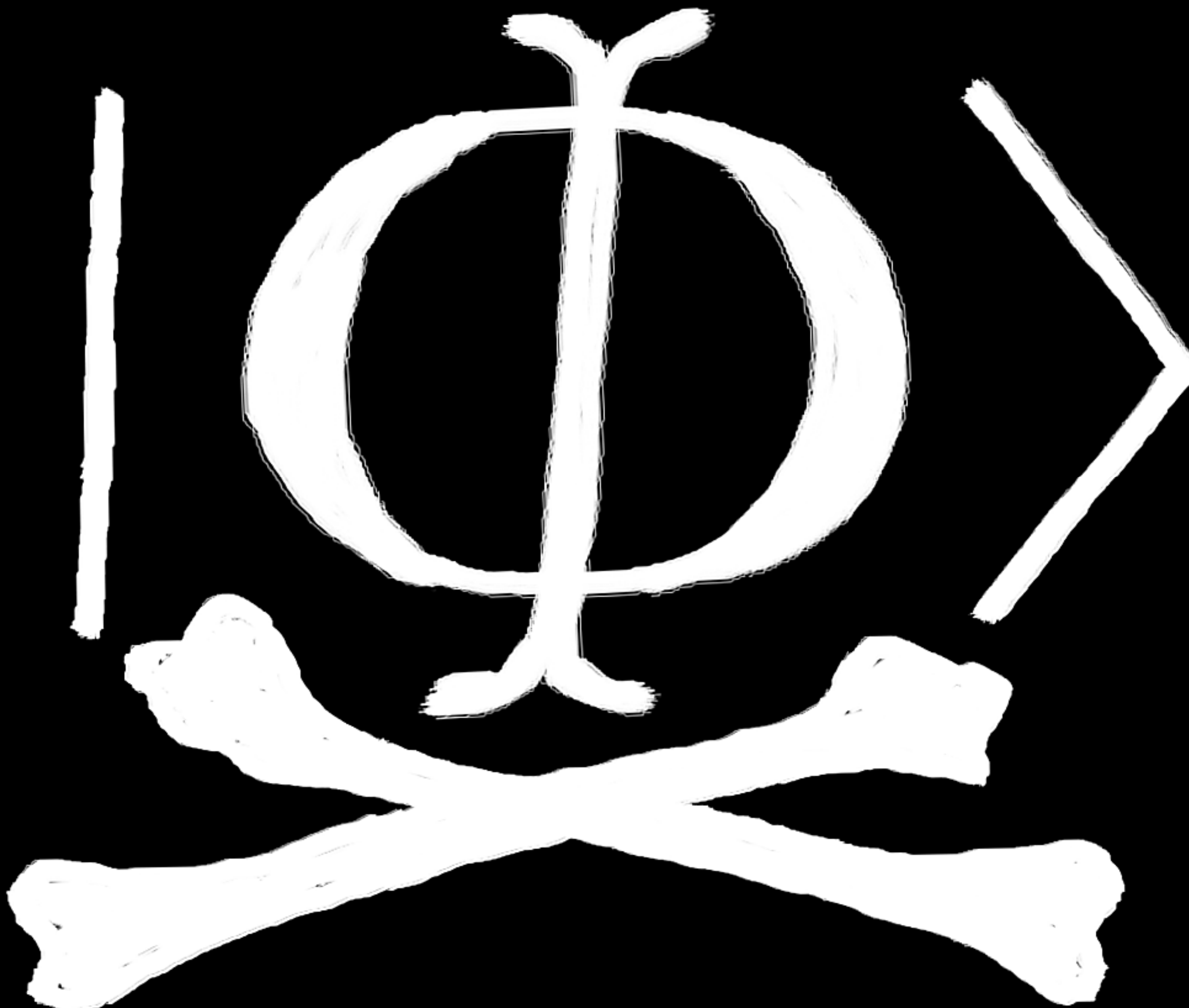
ISO

Example of initial analysis report

TABLE I: **Summary of potential security issues in [redacted] system.**

Potential security issue	C	Q	Target component	Brief description	Requirements for complete analysis	Lab testing needed?	Risk evaluation
[redacted]	CX	Q1–5,7	[redacted]	[redacted]	Complete circuit diagram of	Yes	High
[redacted]	CX	Q1–3	[redacted]	See Ref. 3.	Complete circuit diagram of	Yes	High
[redacted]	CX	Q1,2	[redacted]	See Ref. 4.	Complete circuit diagram of	Yes	High
[redacted]	C0	Q2,3	[redacted]	Manufacturer needs to implement [redacted]	Known issue. The manufacturer should patch.	No	High
[redacted]	CX	Q3–5,7	[redacted]	[redacted]	Known issue. The manufacturer should [redacted]	No	Medium
[redacted]	CX	Q1	[redacted]	[redacted]	Model numbers of all optical components; complete receiver for testing.	Yes	High
[redacted]	CX	Q1–5	[redacted]	[redacted]	Complete circuit diagram of [redacted] settings of	Yes	Insufficient information
[redacted]	CX	Q1–3	[redacted]	[redacted]	Algorithm of [redacted]	Yes	Low
[redacted]	CX	Q1,2	[redacted]	See Ref. 13.	Model numbers of [redacted]	Yes	Medium
[redacted]	CX	Q4,5	[redacted]	[redacted]	Full system algorithms; complete system if decided to test.	Maybe	Low
[redacted]	CX	Q1,3–5	[redacted]	Eve can [redacted]	Algorithm for [redacted]	Maybe	Low

Missing a single security proof



RQC MISIS Quantum hacking lab vad1.com/lab