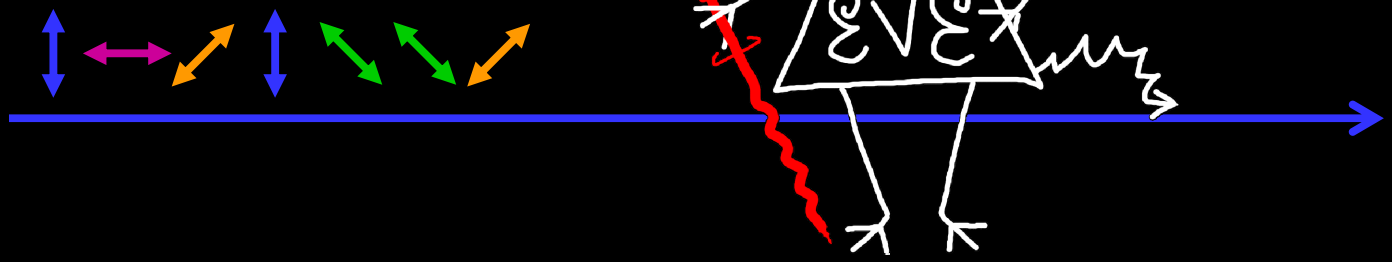

Tutorial at QCrypt, September 12-16, 2016
Challenges to physical security
of
today's quantum technologies
Vadim Makarov
IQC Institute for Quantum Computing
www.vad1.com/lab

A (very) brief history of cryptography

		Broken?
Monoalphabetic cipher	invented ~50 BC (J. Caesar)	~850 (Al-Kindi)
Nomenclators (code books)	~1400 – ~1800	✓
Polyalphabetic (Vigenère)	1553 – ~1900	1863 (F. W. Kasiski)
…		
One-time pad	invented 1918 (G. Vernam)	**impossible** (C. Shannon 1949)
Polyalphabetic electromechanical (Enigma, Purple, etc.)	1920s – 1970s	✓
…		
DES	1977 – 2005	1998: 56 h (EFF)
Public-key crypto (RSA, elliptic-curve)	1977 –	will be once we have q. computer (P. Shor 1994)
AES	2001 –	?
Quantum cryptography	invented 1984, in development	**impossible***
Public-key crypto ('quantum-safe')	in development	?

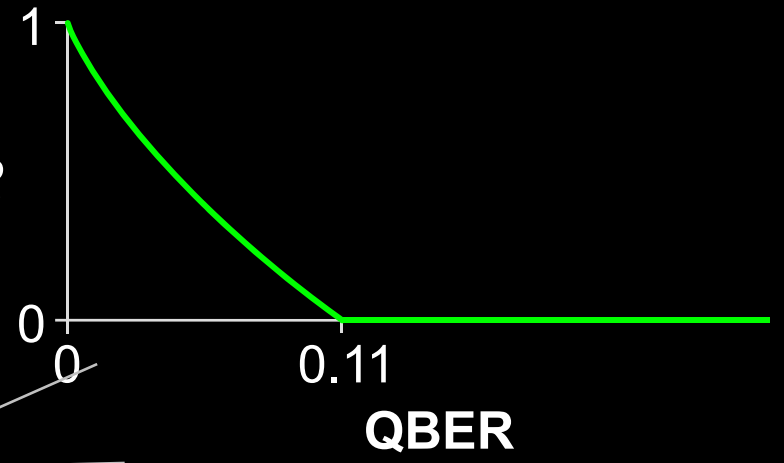
Security model of QKD

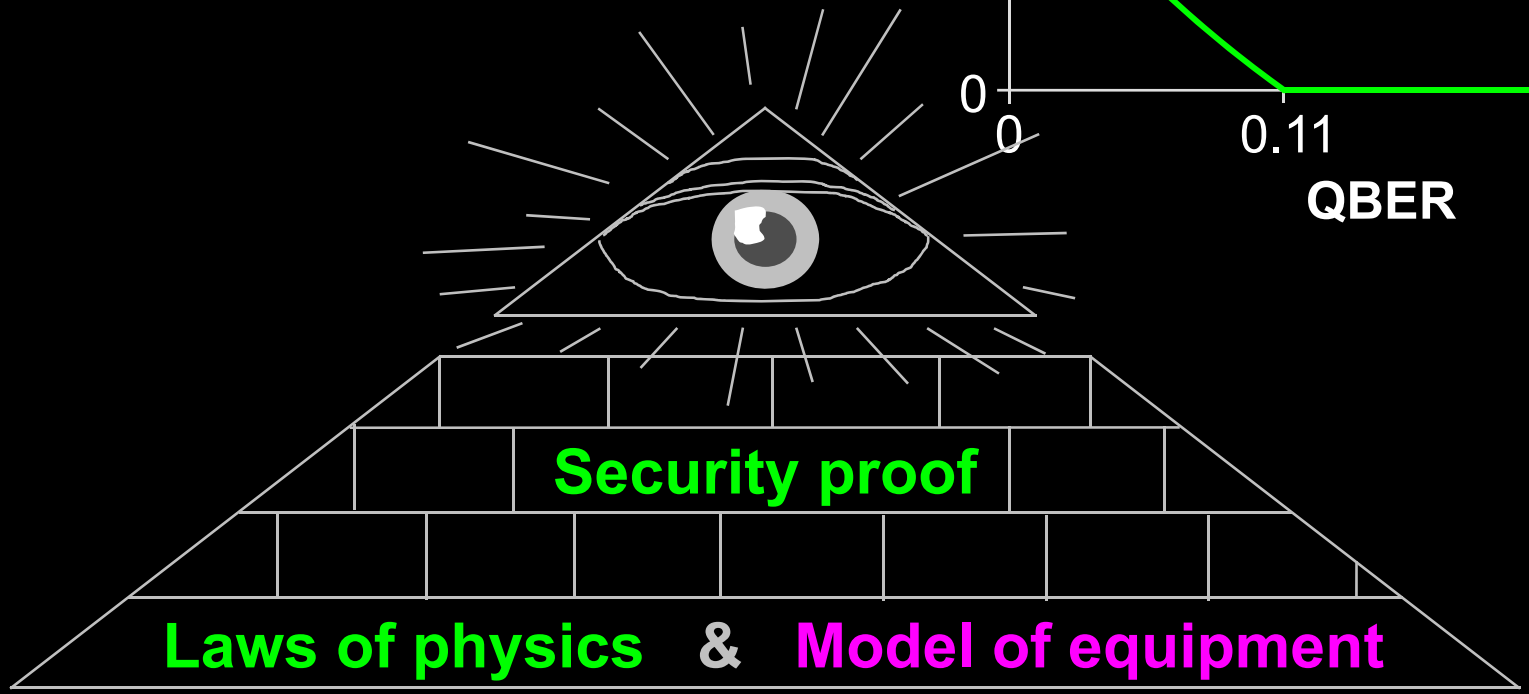


Alice

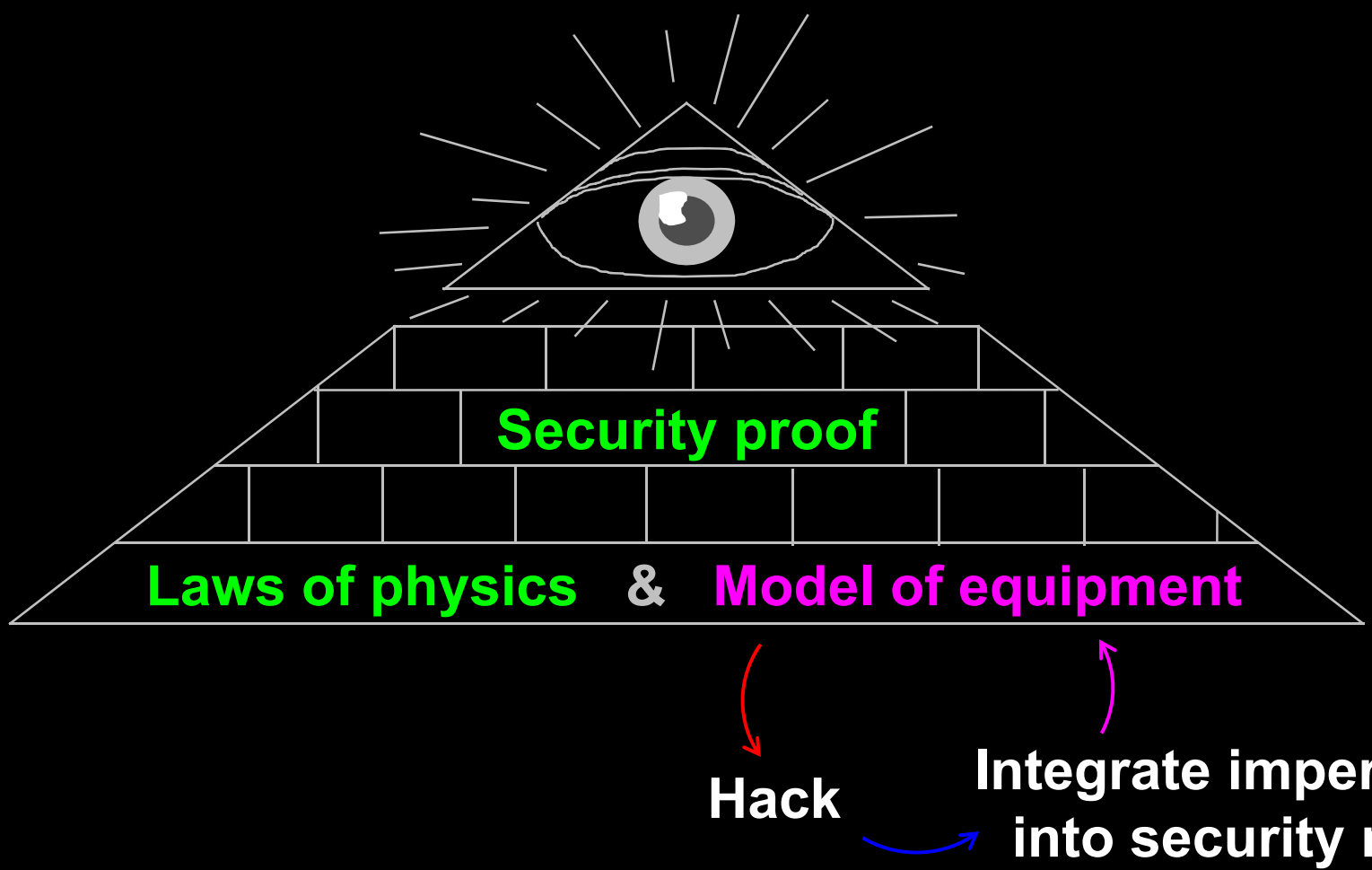
Bob

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





Security model of QKD



Attack	Target component	Tested system
Laser damage V. Makarov *et al.,* arXiv:1510.03148	any	ID Quantique, research system
Spatial efficiency mismatch M Rau *et al.,* IEEE J. Quantum Electron. **21**, 6600905 (2015); S. Sajeed *et al.,* Phys. Rev. A **91**, 062301 (2015)	receiver optics	research system
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)	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 system

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

VII - 26 - X

~~COMINT~~

A HISTORY OF U.S. COMMUNICATIONS SECURITY (U)
(The David G. Boak Lectures)

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND 20755

Revised July 1973

TENTH LECTURE: TEMPEST

In 1962, an officer assigned to a very small intelligence detachment in Japan was performing the routine duty of inspecting the area around his little cryptocenter. As required he was examining a zone 200 ft. in radius to see if there was any "clandestine technical surveillance". Across the street, perhaps a hundred feet away, was a hospital controlled by the Japanese government. He sauntered past a kind of carport jutting out from one side of the building and, up under the eaves, noticed a peculiar thing—a carefully concealed dipole antenna, horizontally polarized, with wires leading through the solid cinderblock wall to which the carport abutted. He moseyed back to his headquarters, then quickly notified the counter-intelligence people and fired off a report of this "find" to Army Security Agency, who, in turn, notified NSA. He was directed to examine this antenna in detail and perhaps recover it, but although the CIC had attempted to keep the carport under surveillance that night, the antenna had mysteriously disappeared when they checked the next day. Up on the roof of the hospital was a forest of Yagi's, TV-antennas, all pointing towards Tokyo in the normal fashion, except *one*. That one was aimed right at the U.S. cryptocenter.

able impact on most of our cryptosystems, and because we view it as the most serious technical security problem we currently face in the COMSEC world.

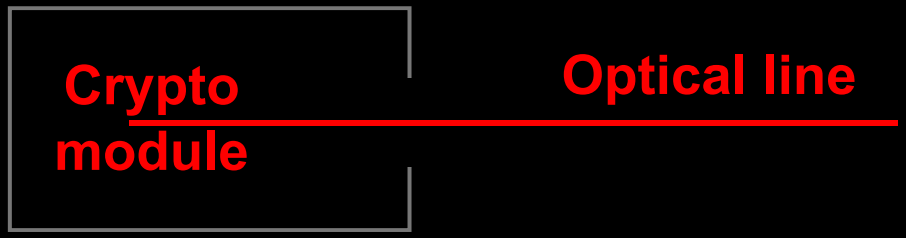
First, let me state the general nature of the problem as briefly as I can, then I will attempt something of a chronology for you. In brief: any time a machine is used to process classified information electrically, the various switches, contacts, relays, and other components in that machine may emit radio frequency or acoustic energy. These emissions, like tiny radio broadcasts, may radiate through free space for considerable distances—a half mile or more in some cases. Or they may be induced on nearby conductors like signal lines, power lines, telephones lines, or water pipes and be conducted along those paths for some distance—and here we may be talking of a mile or more.

When these emissions can be intercepted and recorded, it is frequently possible to analyze them and recover the intelligence that was being processed by the source equipment. The phenomenon affects not only cipher machines but *any* information-processing equipment—teleprinters, duplicating equipment, intercomms, facsimile, computers—you name it. But it has special significance for cryptomachines because it may reveal not only the plain text of individual messages being processed, but also that carefully guarded information about the internal machine processes being governed by those precious keys of ours. Thus, conceivably, the machine could be radiating information which could lead to the reconstruction of our key lists—and that is absolutely the worst thing that can happen to us.

Now, let's go back to the beginning. During WW II, the backbone systems for Army and Navy secure TTY communications were one-time tapes and the primitive rotor key generator then called SIGTOT. Bell Telephone rented and sold the military a mixing device called a 131–B2 and this combined with tape or SIGTOT key with plain text to effect encryption. They had one of these mixers working in one of their laboratories and, quite by accident, noted that each time the machine stepped, a spike would appear on an oscilloscope in a distant part of the lab. They examined these spikes more carefully and found, to their real dismay, that they could read the plain text of the message being enciphered by the machine. Bell Telephone was kind enough to give us some of their records of those days, and the memoranda and reports of conferences that ensued after this discovery are fascinating. They had sold the equipment to the military with the assurance that it was secure, but it wasn't. The only thing they could do was to tell the Signal Corps about it, which they did. There they met the charter members of a club of skeptics (still flourishing!) which could not believe that these tiny pips could really be exploited under practical field conditions. They are alleged to have said something like: "Don't you realize there's a war on? We can't bring our cryptographic operations to a screeching halt based on a dubious and esoteric laboratory phenomenon. If this is really dangerous, prove it." The Bell engineers were placed in a building on Varick Street in New York. Across the street and about 80 feet away was Signal Corps' Varick Street cryptocenter. The Engineers recorded signals for about an hour. Three or four hours later, they produced about 75% of the plain text that was being processed—a fast performance, by the way, that has rarely been equalled. (Although, to get ahead of the story for a moment, in some circumstances now-a-days, either radiated or conducted signals can be picked up, amplified, and used to drive a tele-

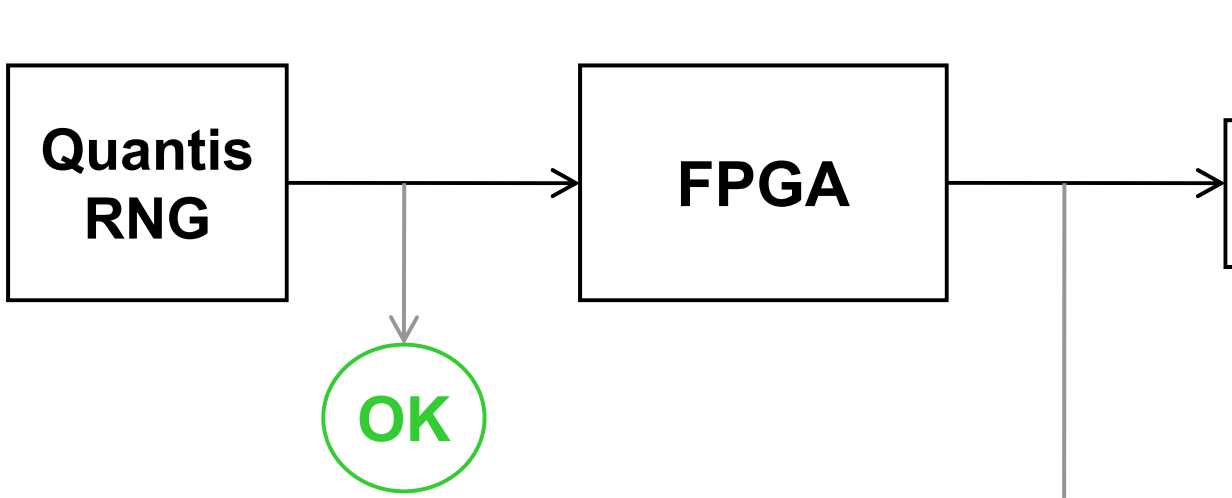
Today's digital

vs. quantum

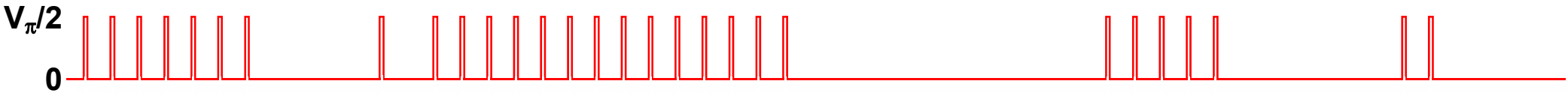


[vs. future quantum]

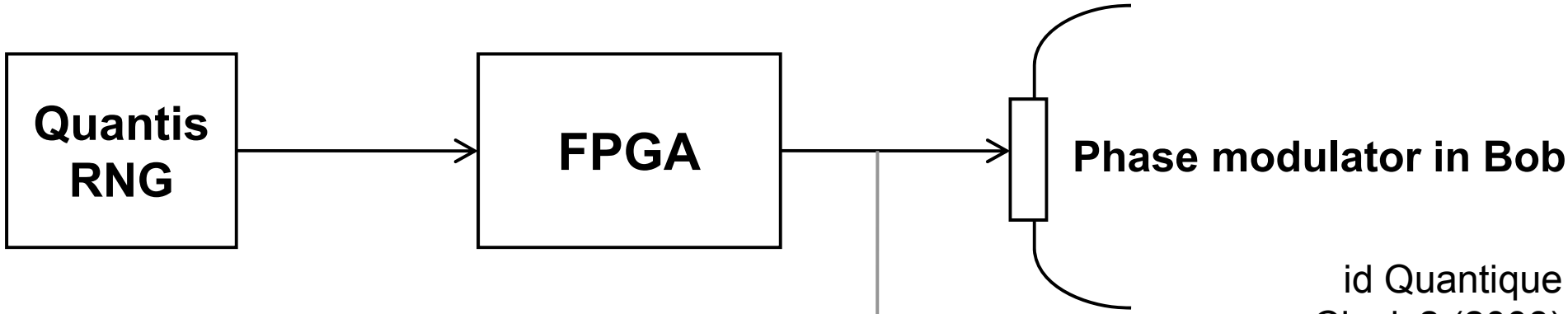
True randomness?



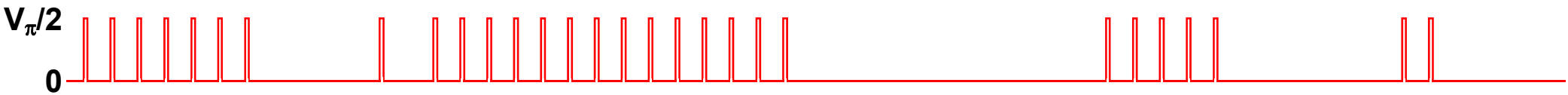
id Quantique
Clavis2 (2008)



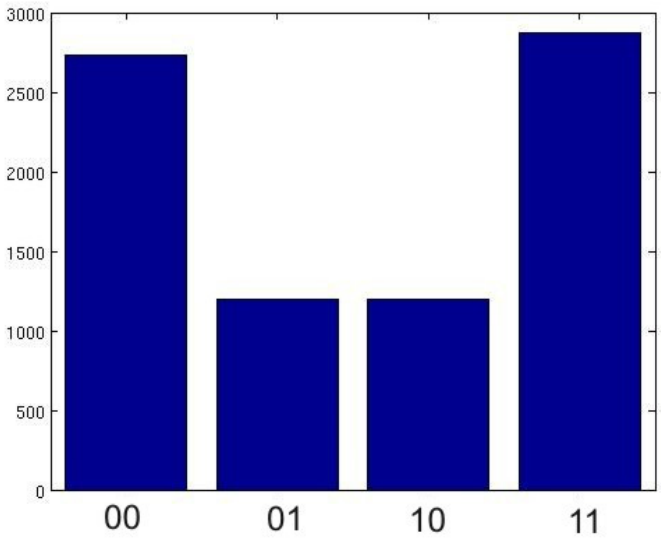
True randomness?



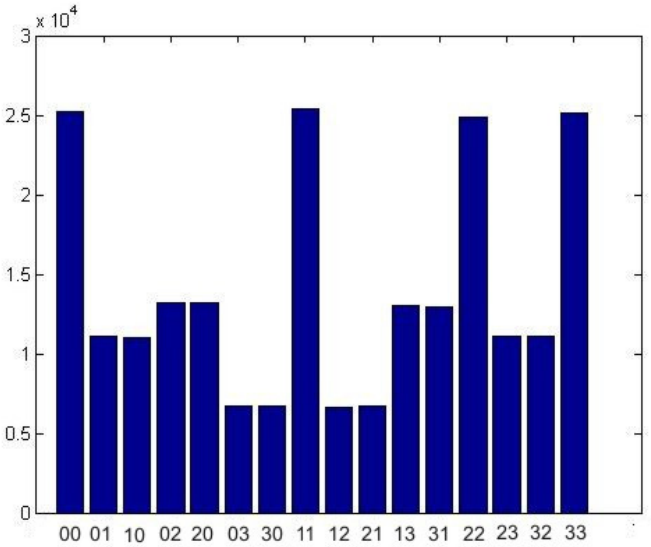
id Quantique
Clavis2 (2008)



Bob:



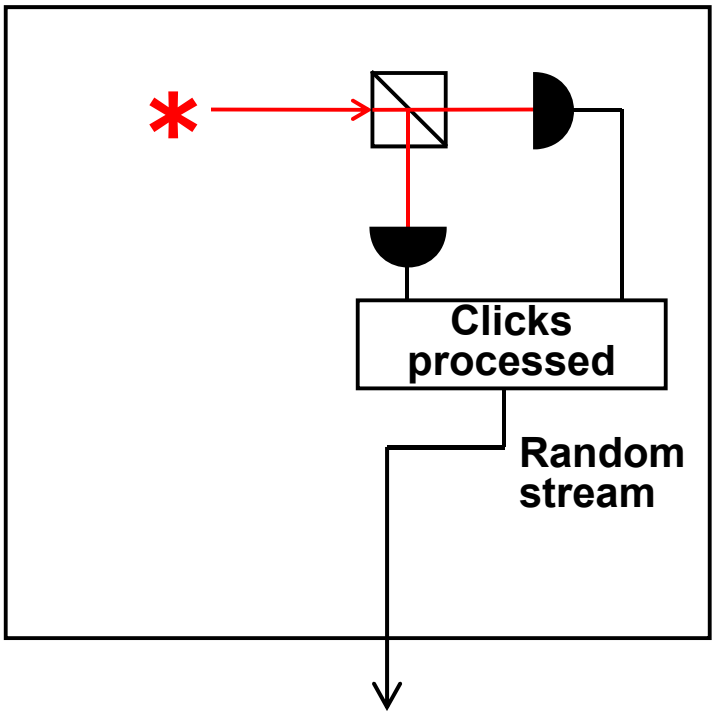
Alice:



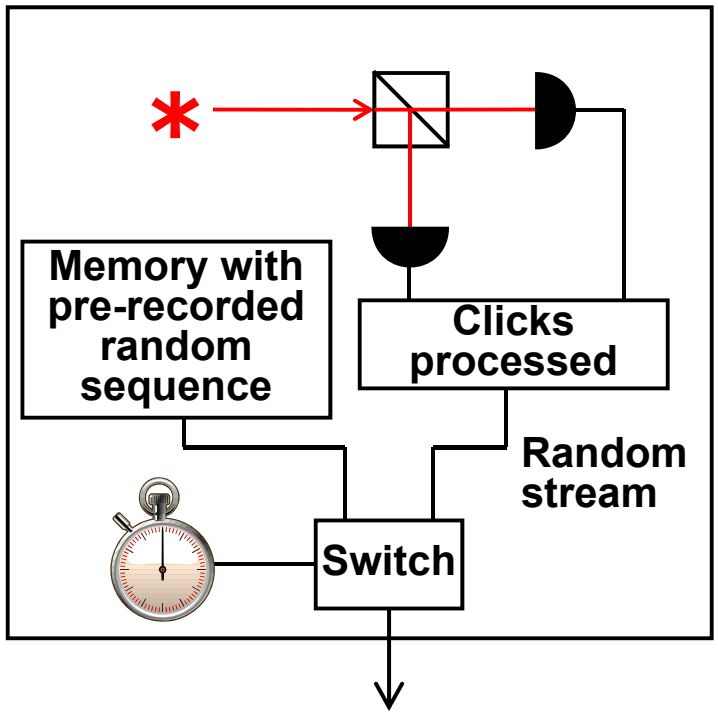
Issue reported patched in 2010

Do we trust the manufacturer?

Quantis RNG



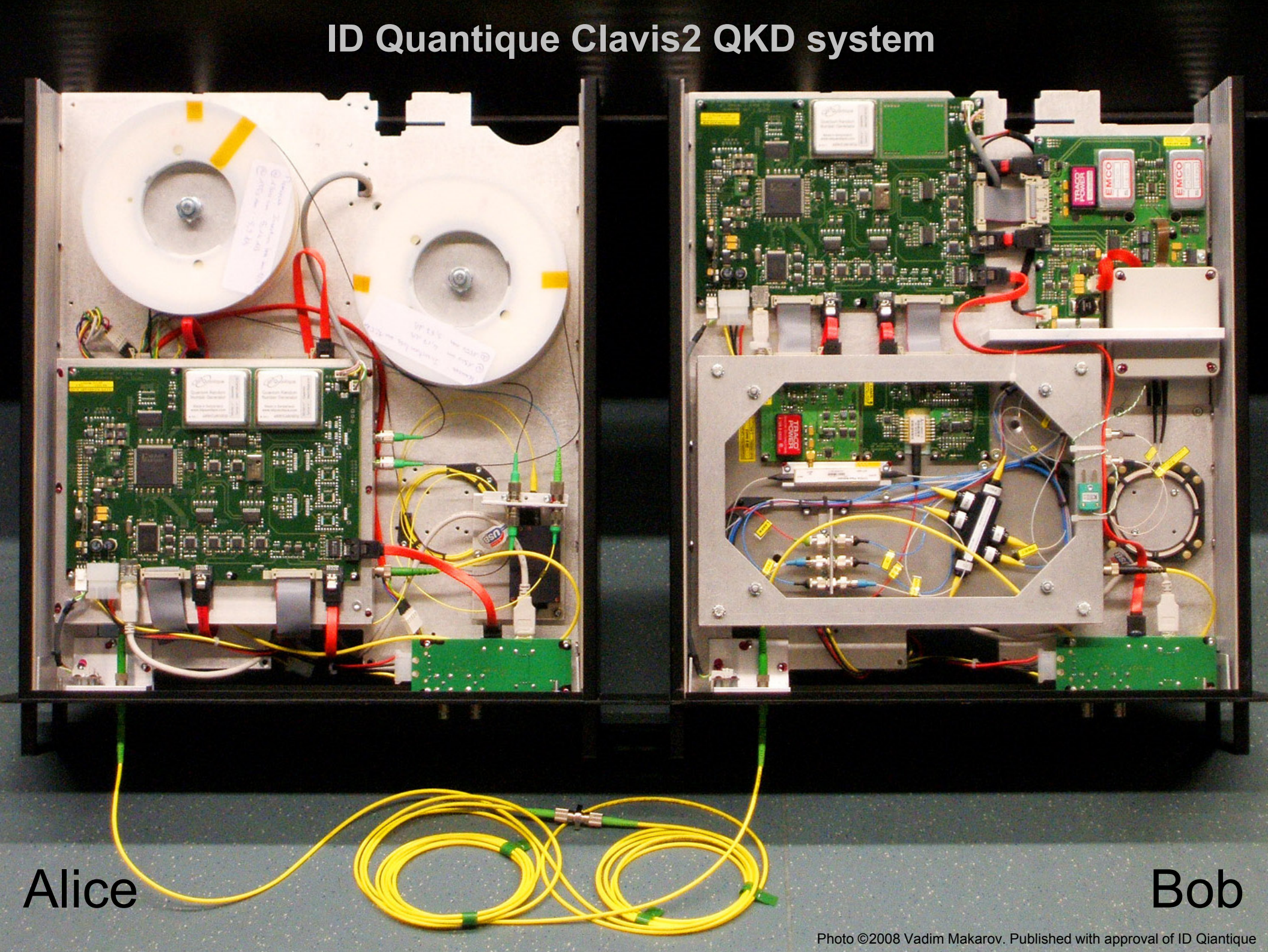
Quantis RNG, Trojan-horsed :)



Many components in QKD system can be Trojan-horsed:

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

ID Quantique Clavis2 QKD system

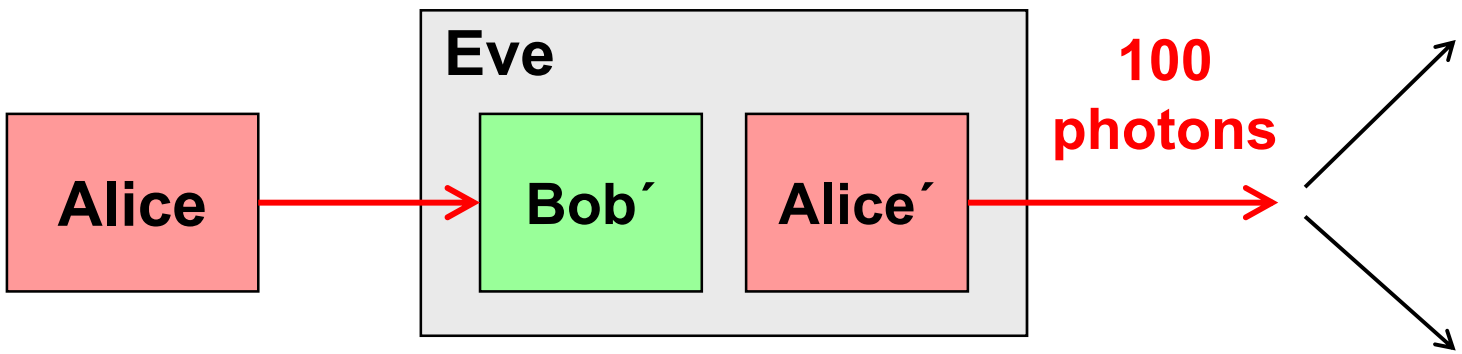


Double clicks

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

Discard them?

Intercept-resend attack... with a twist:



Bob:

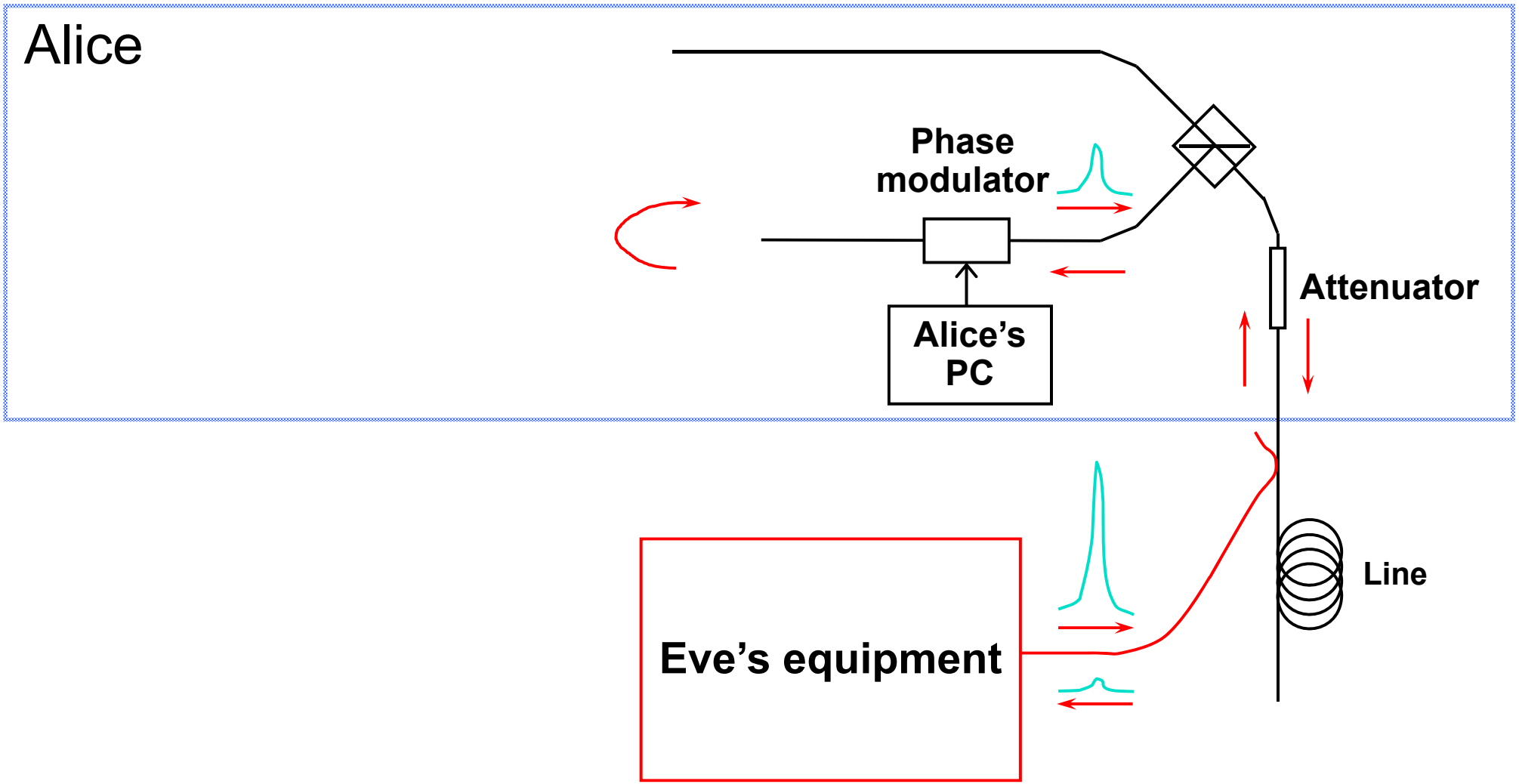
Detects in Eve's basis: single click

Detects in conjugate basis: double click, discarded

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

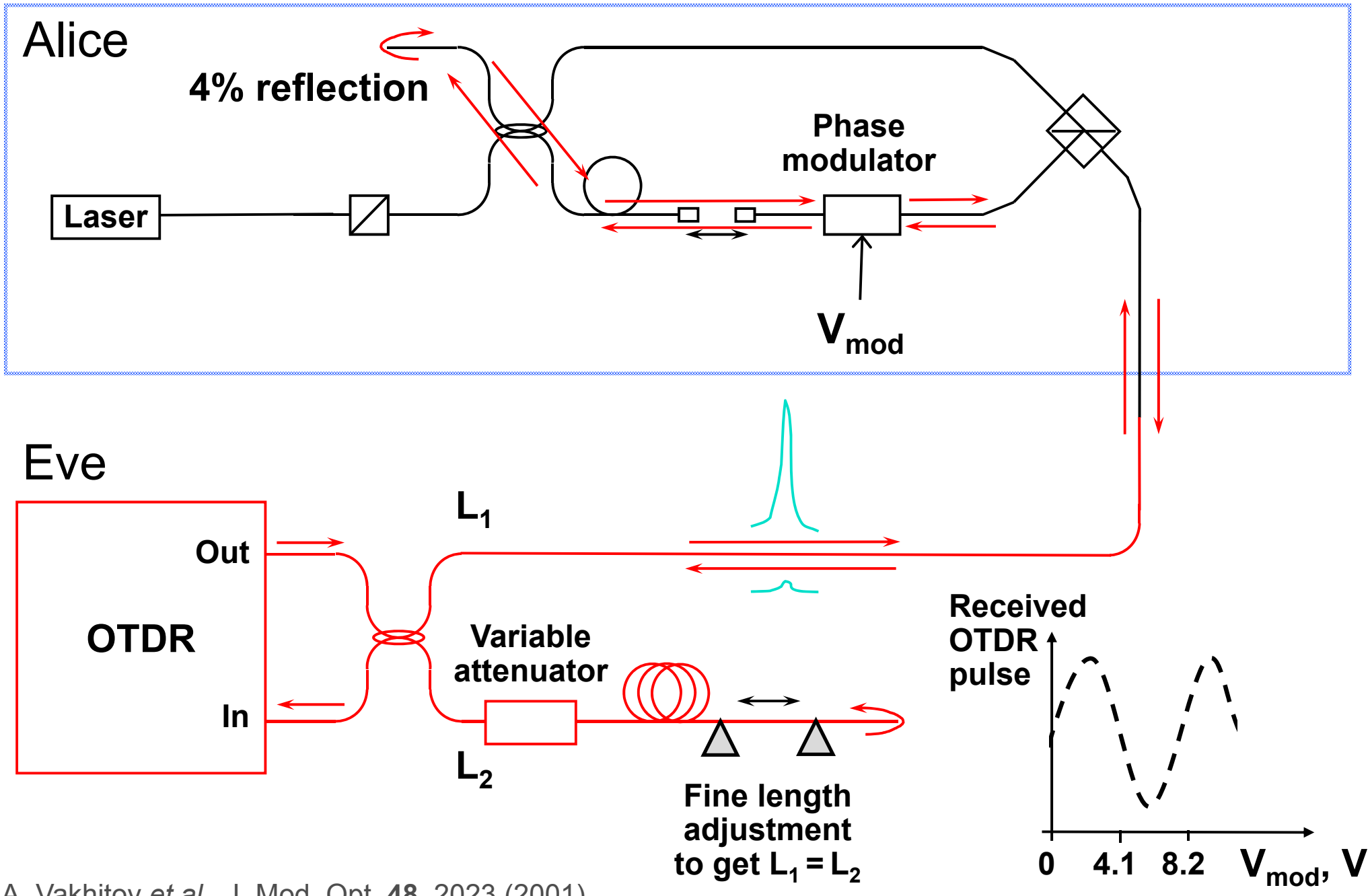
N. Lütkenhaus, Phys. Rev. A **59**, 3301 (1999)
T. Tsurumaru & K. Tamaki, Phys. Rev. A **78**, 032302 (2008)

Trojan-horse attack

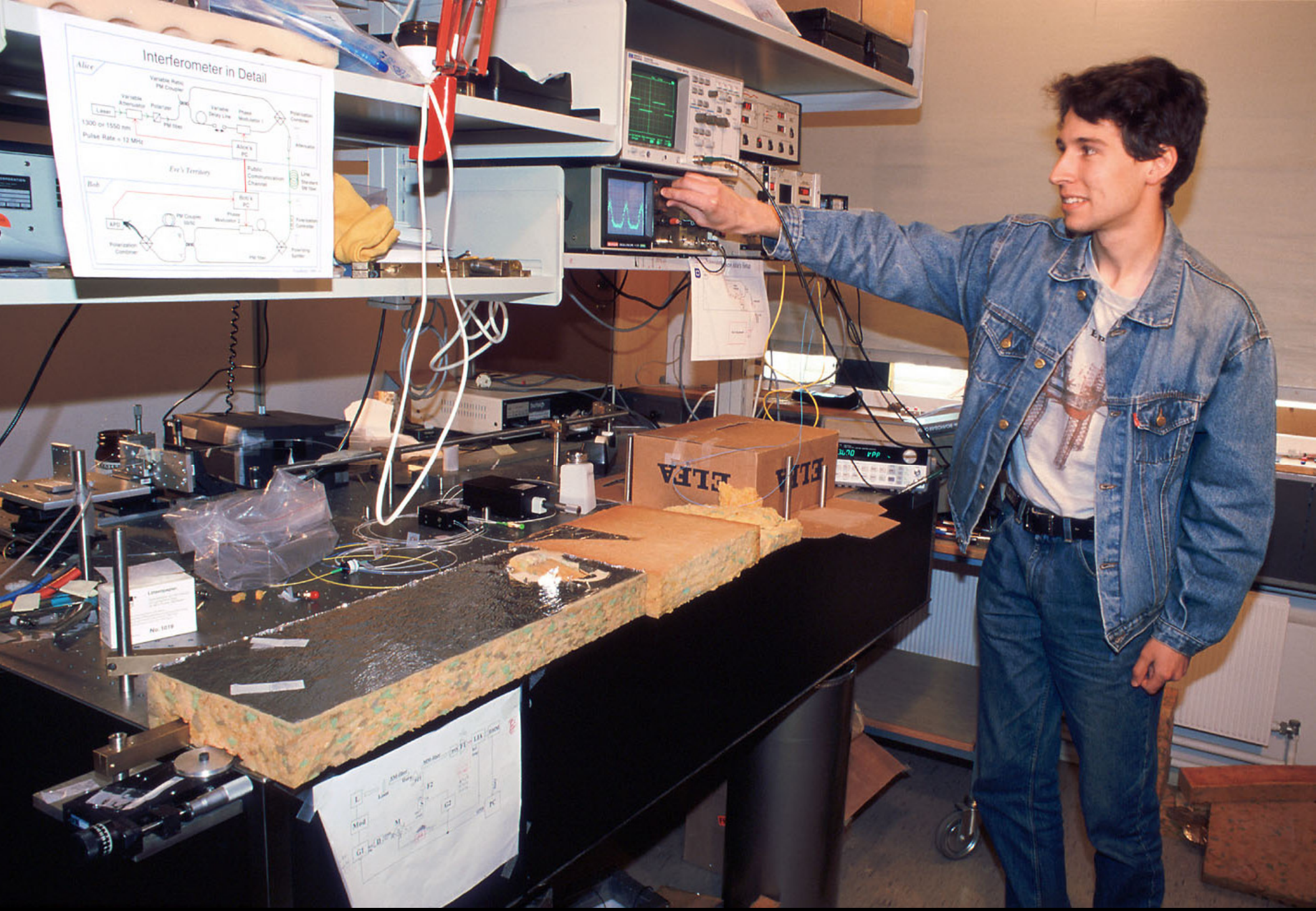


– interrogating Alice's phase modulator with powerful external pulses (can give Eve bit values directly)

Trojan-horse attack experiment

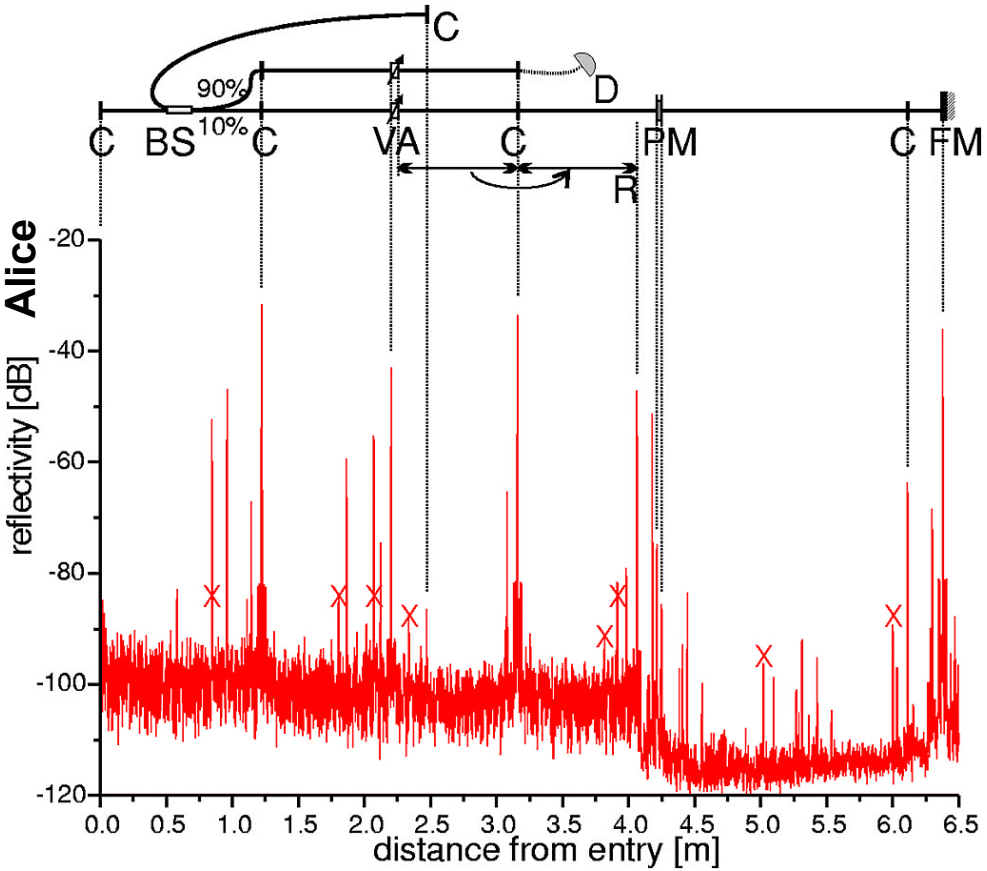


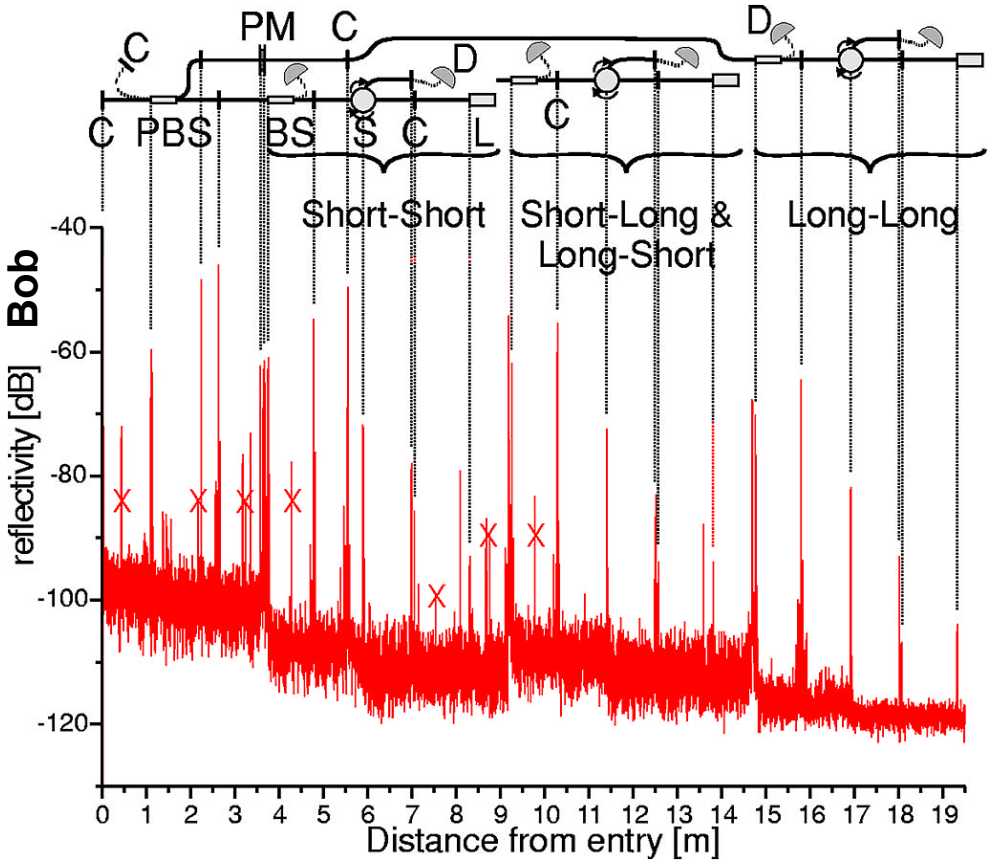
A. Vakhitov *et al.*, J. Mod. Opt. **48**, 2023 (2001)



Artem Vakhitov tunes up Eve's setup

Trojan-horse attack for plug-and-play system

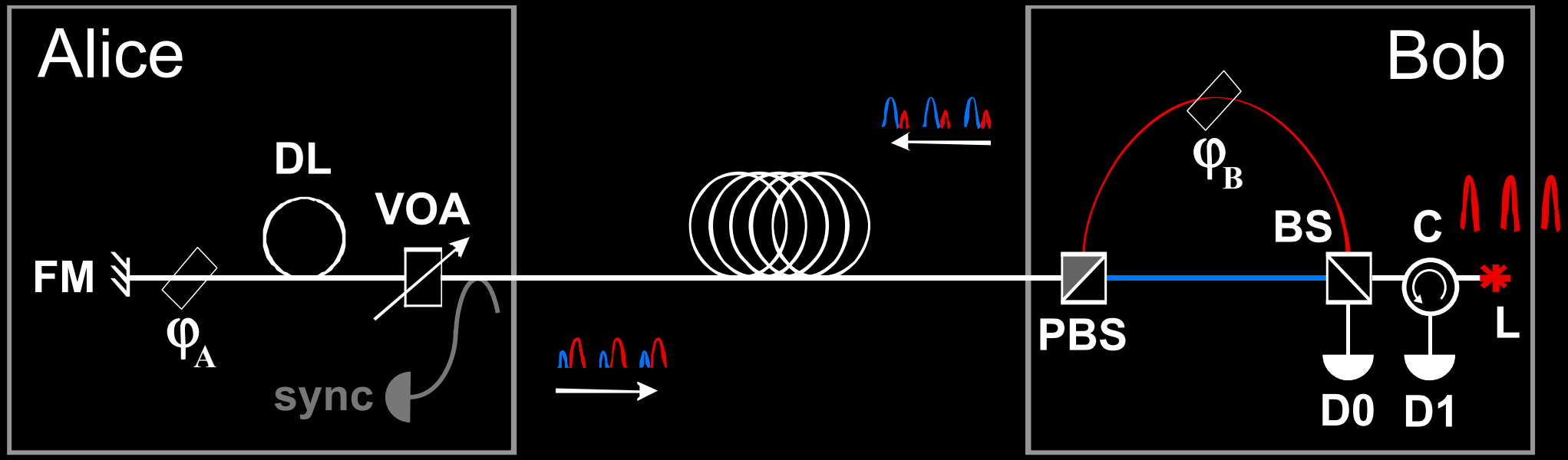




Eve gets back one photon → in principle, extracts 100% information

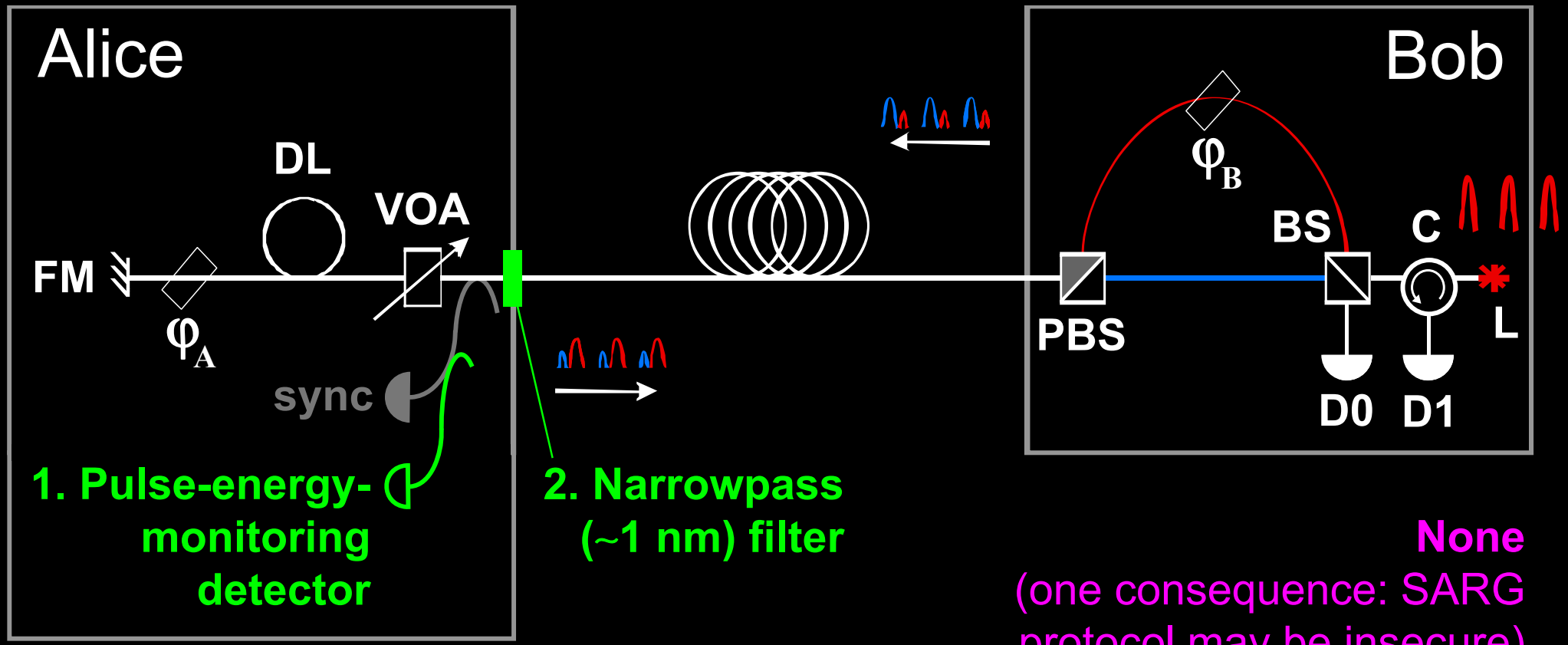
N. Gisin *et al.*, Phys. Rev. A **73**, 022320 (2006)

Countermeasures?



D. Stucki *et al.*, New J. Phys. **4**, 41 (2002)

Countermeasures for plug-and-play system

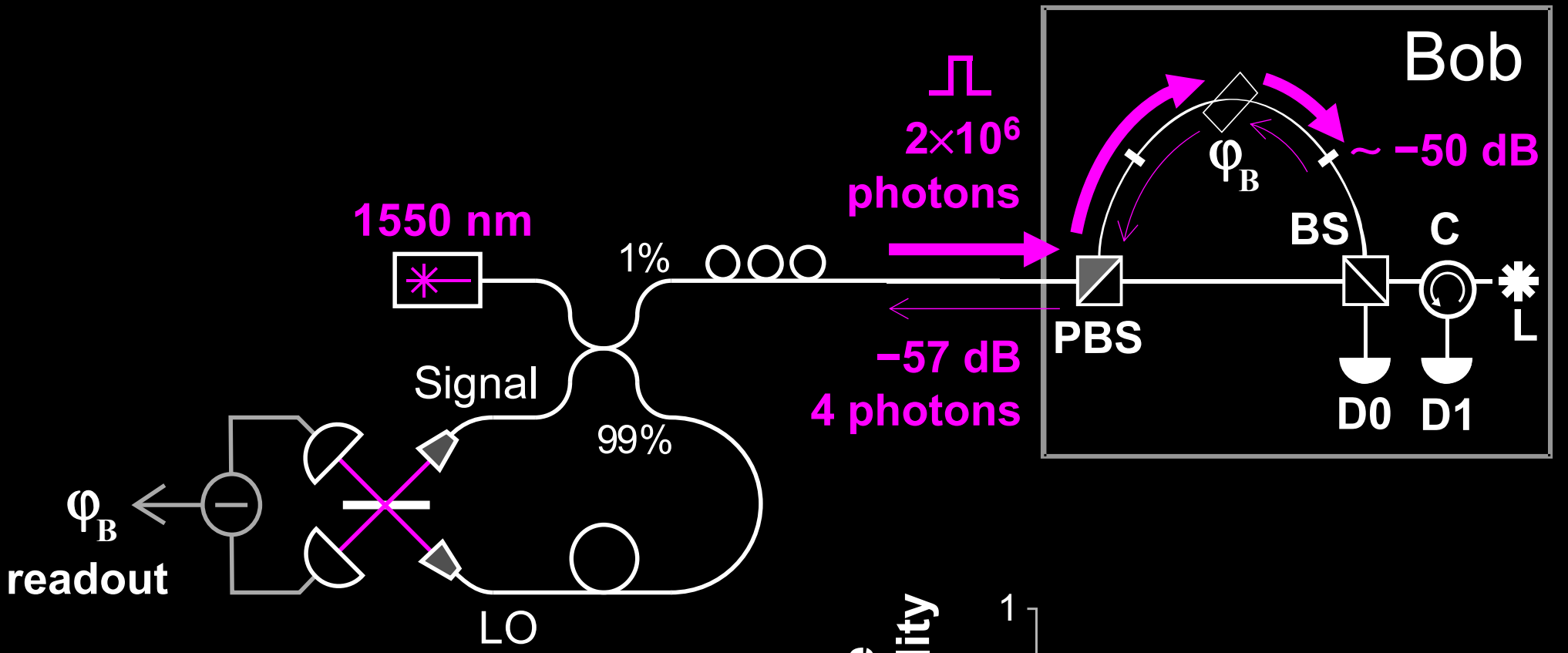


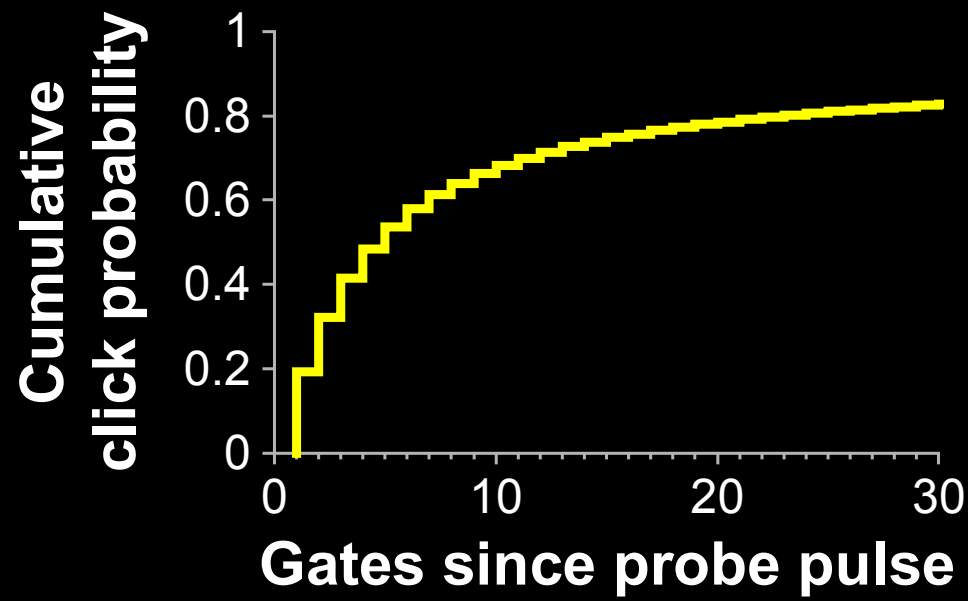
None
(one consequence: SARG protocol may be insecure)

S. Sajeed *et al.*, Phys. Rev. A **91**, 032326 (2015)

N. Jain *et al.*, New J. Phys. **16**, 123030 (2014)

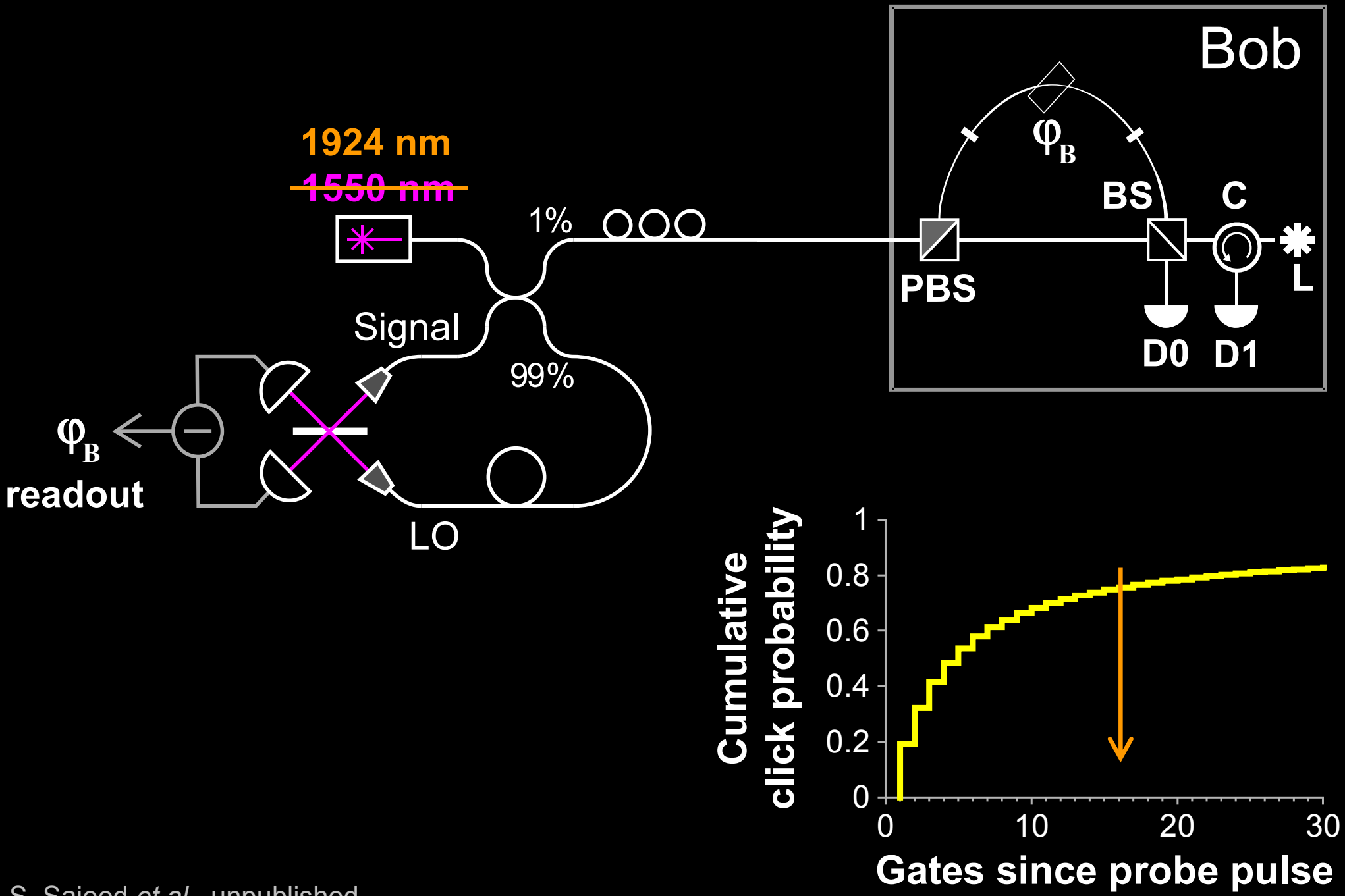
Trojan-horse attack on Bob





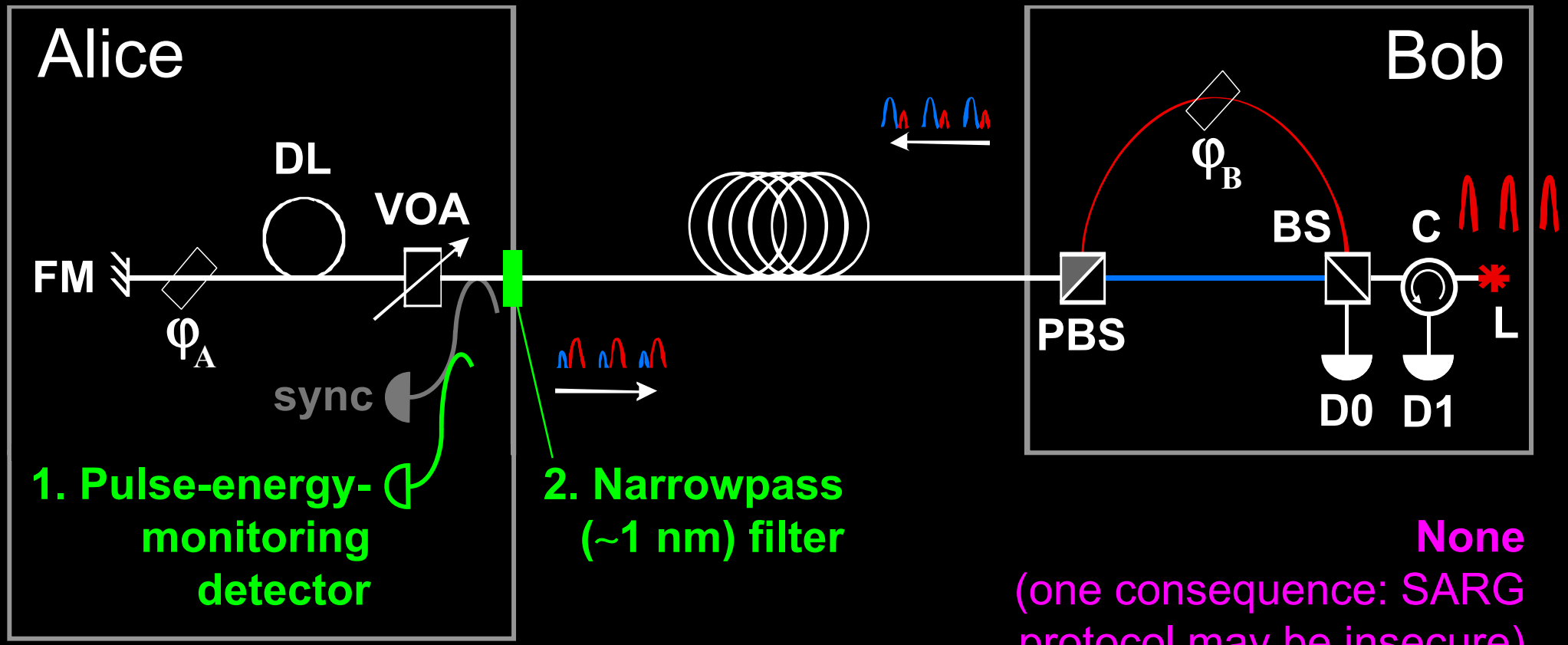
N. Jain *et al.*, New J. Phys. **16**, 123030 (2014)

Trojan-horse attack on Bob



S. Sajeed *et al.*, unpublished

Countermeasures for plug-and-play system

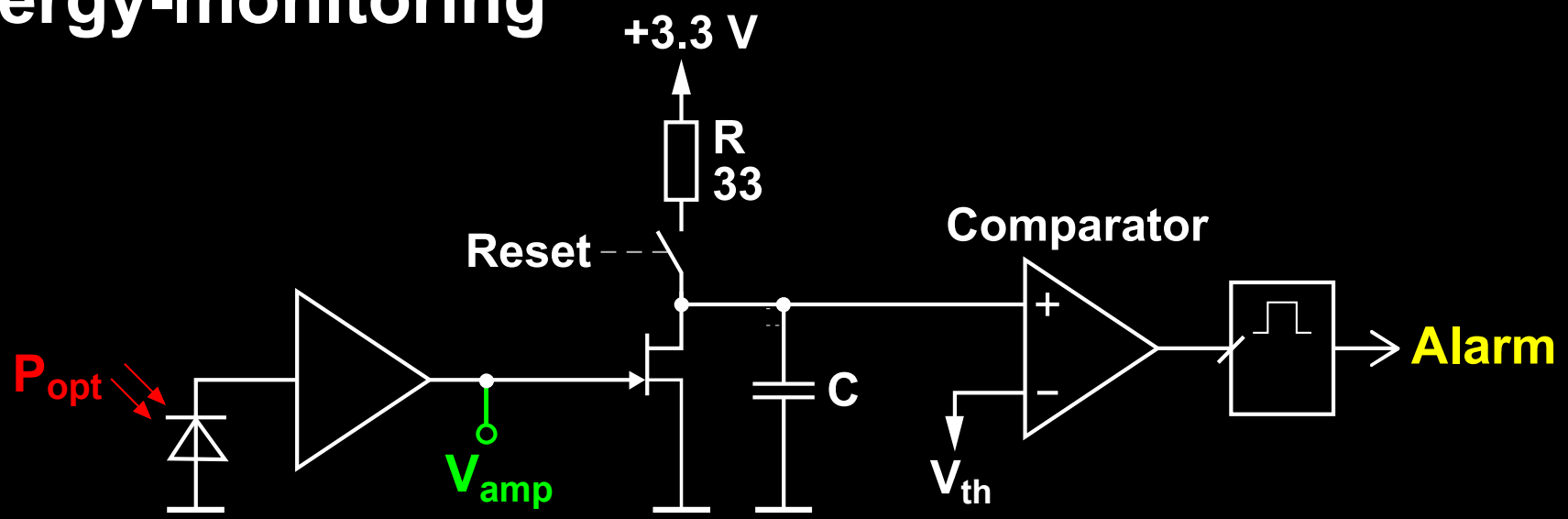


None
(one consequence: SARG protocol may be insecure)

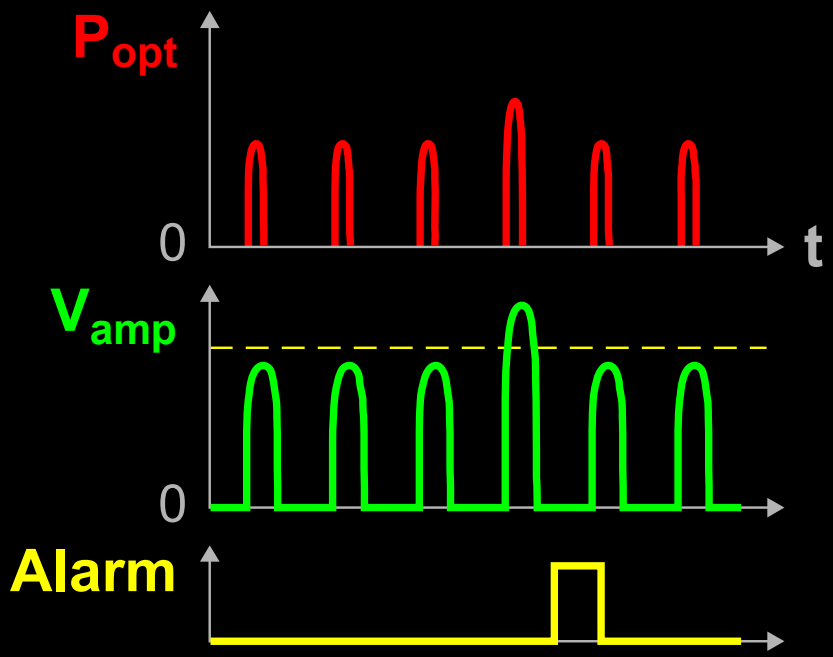
S. Sajeed *et al.*, Phys. Rev. A **91**, 032326 (2015)

N. Jain *et al.*, New J. Phys. **16**, 123030 (2014)

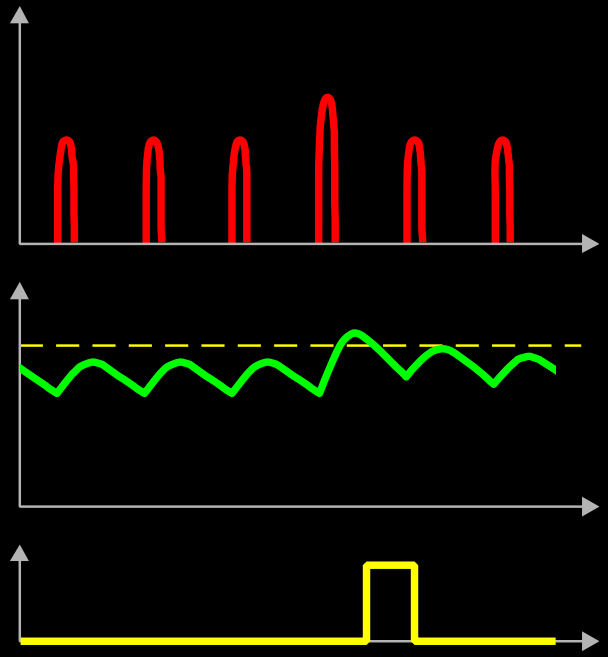
Pulse-energy-monitoring detector



Theory:

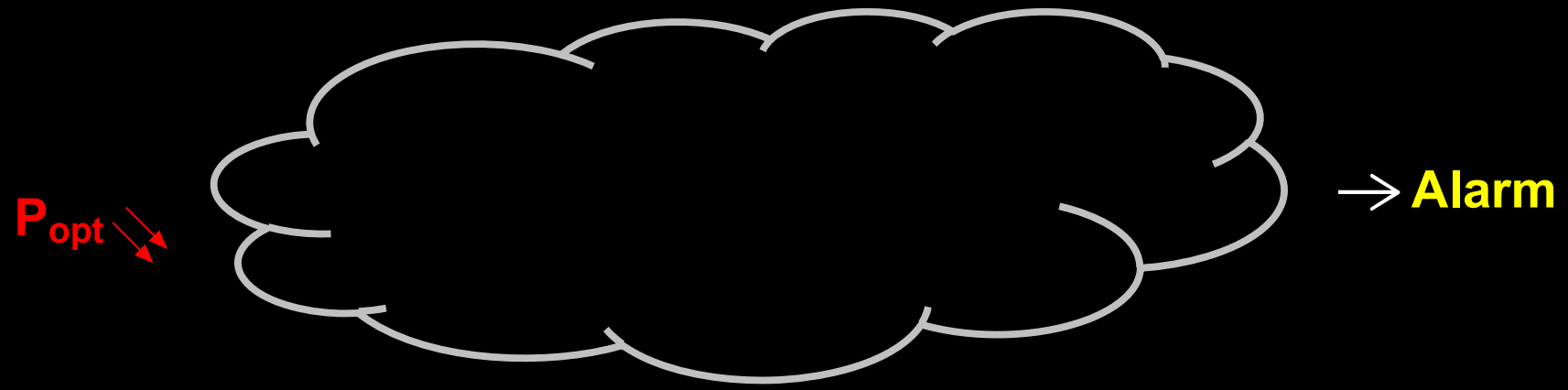


Implementation:

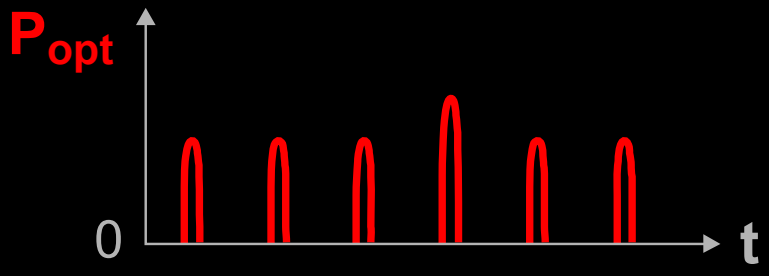


S. Sajeed *et al.*, Phys. Rev. A **91**, 032326 (2015)

Pulse-energy-monitoring detector

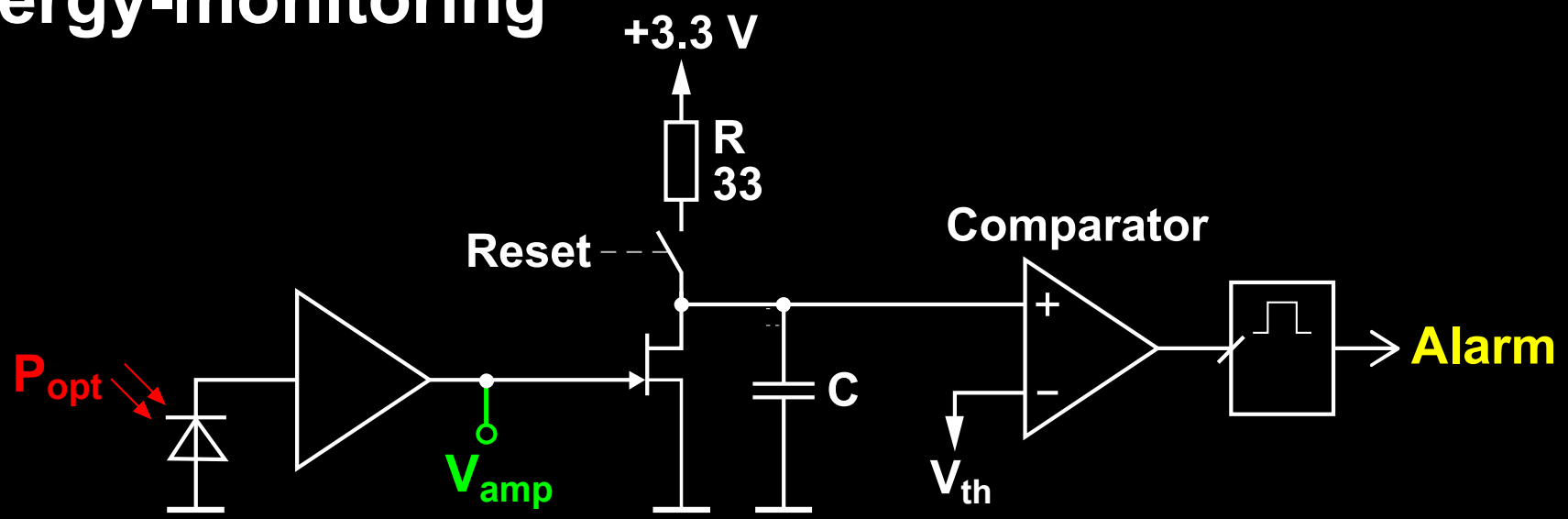


“Certification standard” (internal by ID Quantique):

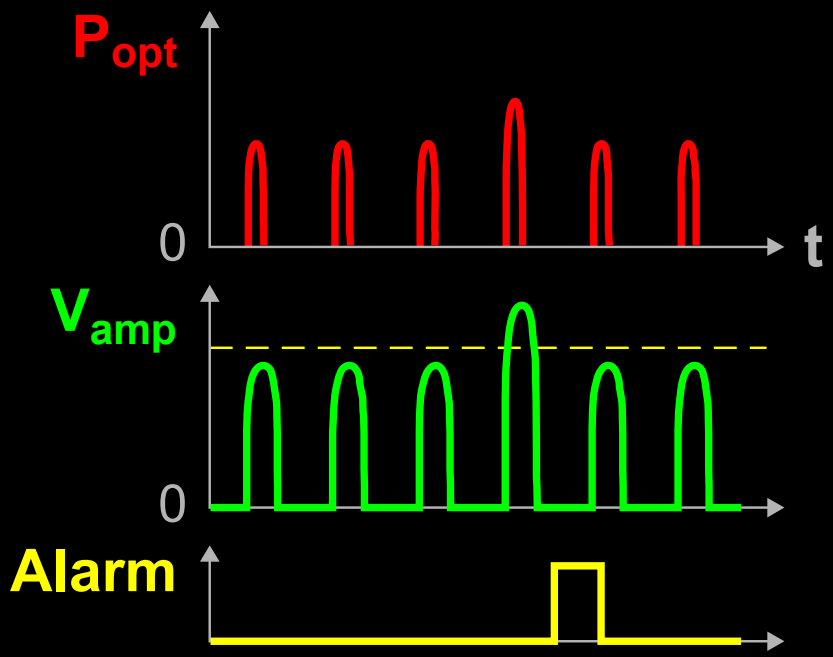


S. Sajeed *et al.*, Phys. Rev. A **91**, 032326 (2015)

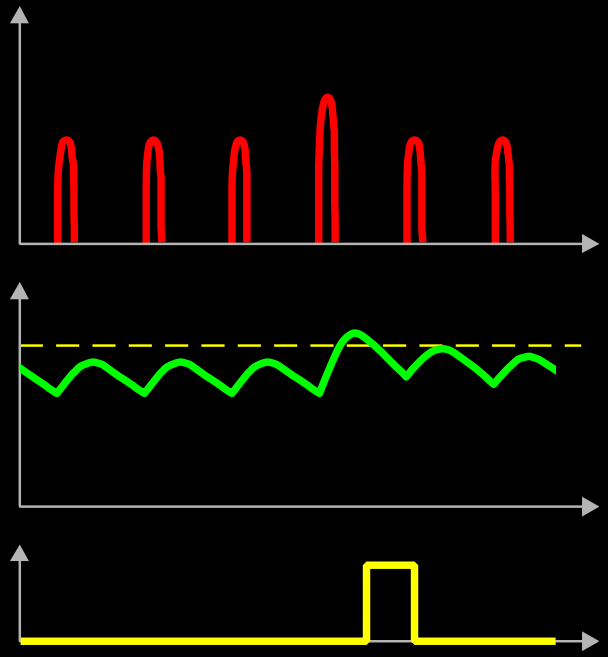
Pulse-energy-monitoring detector



Theory:

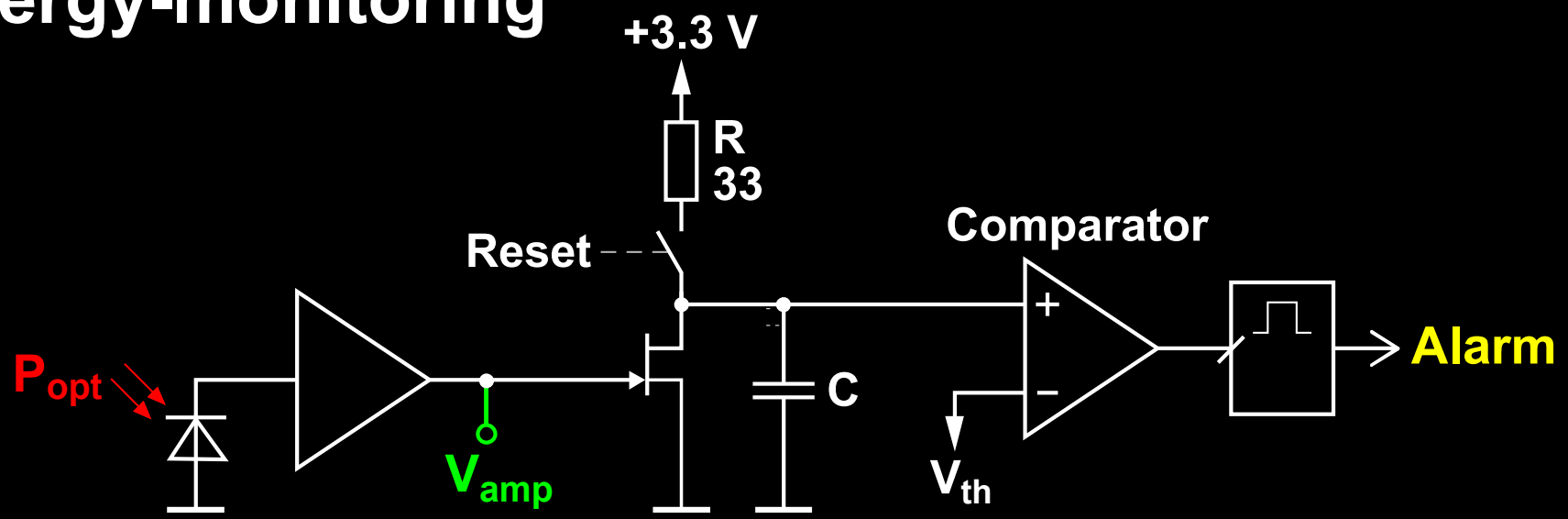


Implementation:

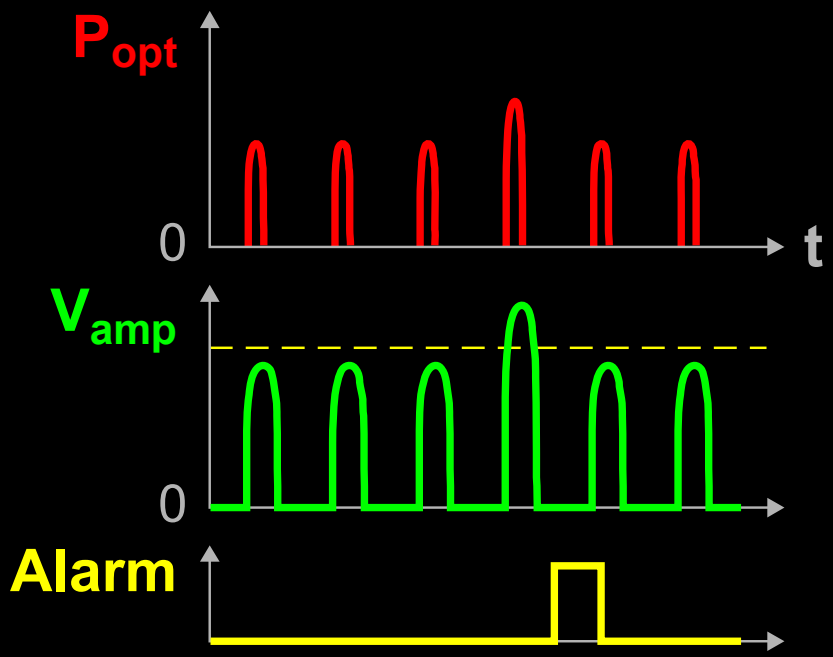


S. Sajeed *et al.*, Phys. Rev. A **91**, 032326 (2015)

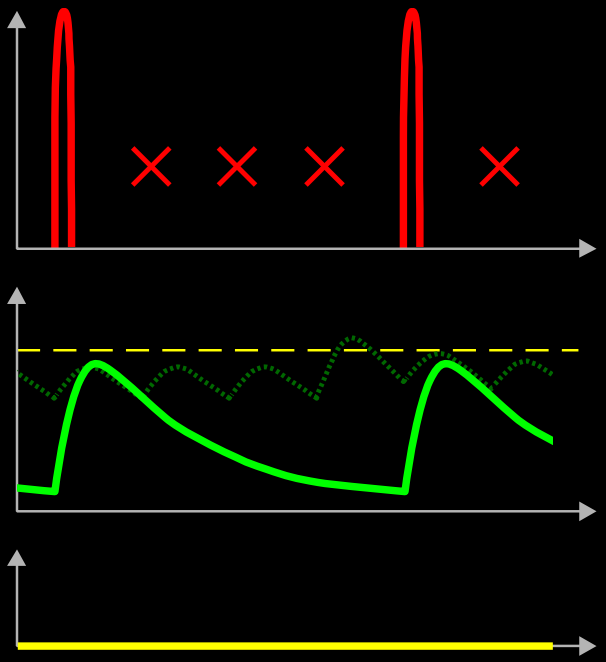
Pulse-energy-monitoring detector



Theory:



Attack:



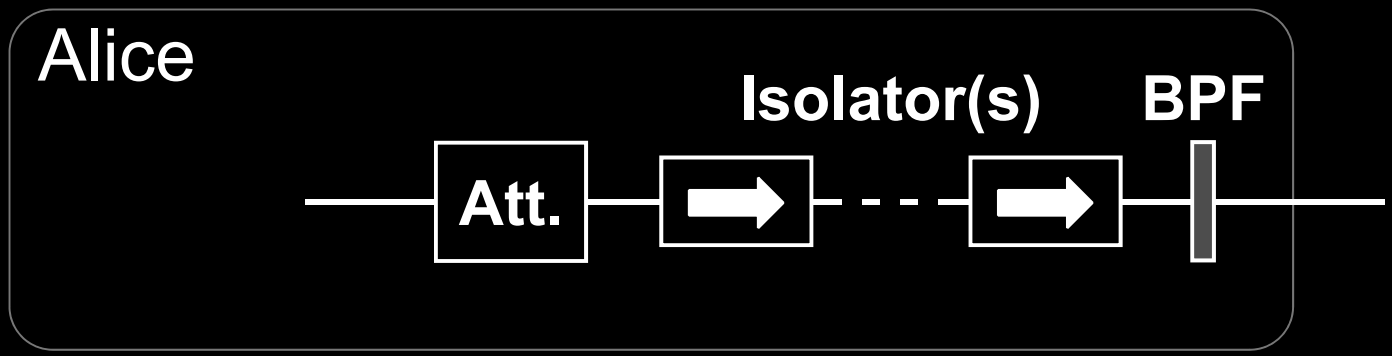
S. Sajeed *et al.*, Phys. Rev. A **91**, 032326 (2015)

Lesson 1. Industry needs implementation standards, certification and testing standards.

ETSI industry specification group for QKD

R. Alléaume *et al.,* Proc. IEEE Globecom Workshop 2014, p. 656

First security standard: Trojan-horse in one-way system



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

Example of vulnerability and countermeasures

Photon-number-splitting attack

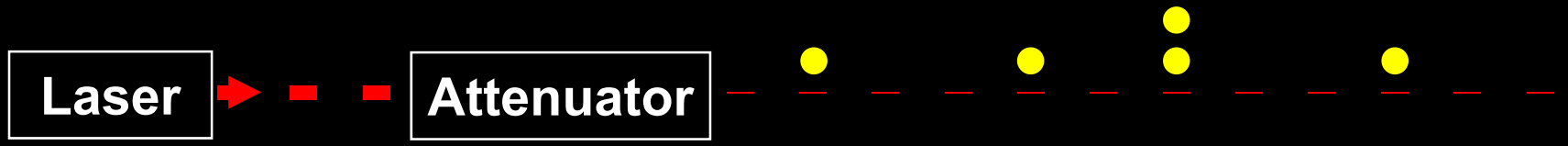
C. Bennett, F. Bessette, G. Brassard, L. Salvail, J. Smolin, J. Cryptology **5**, 3 (1992)

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)

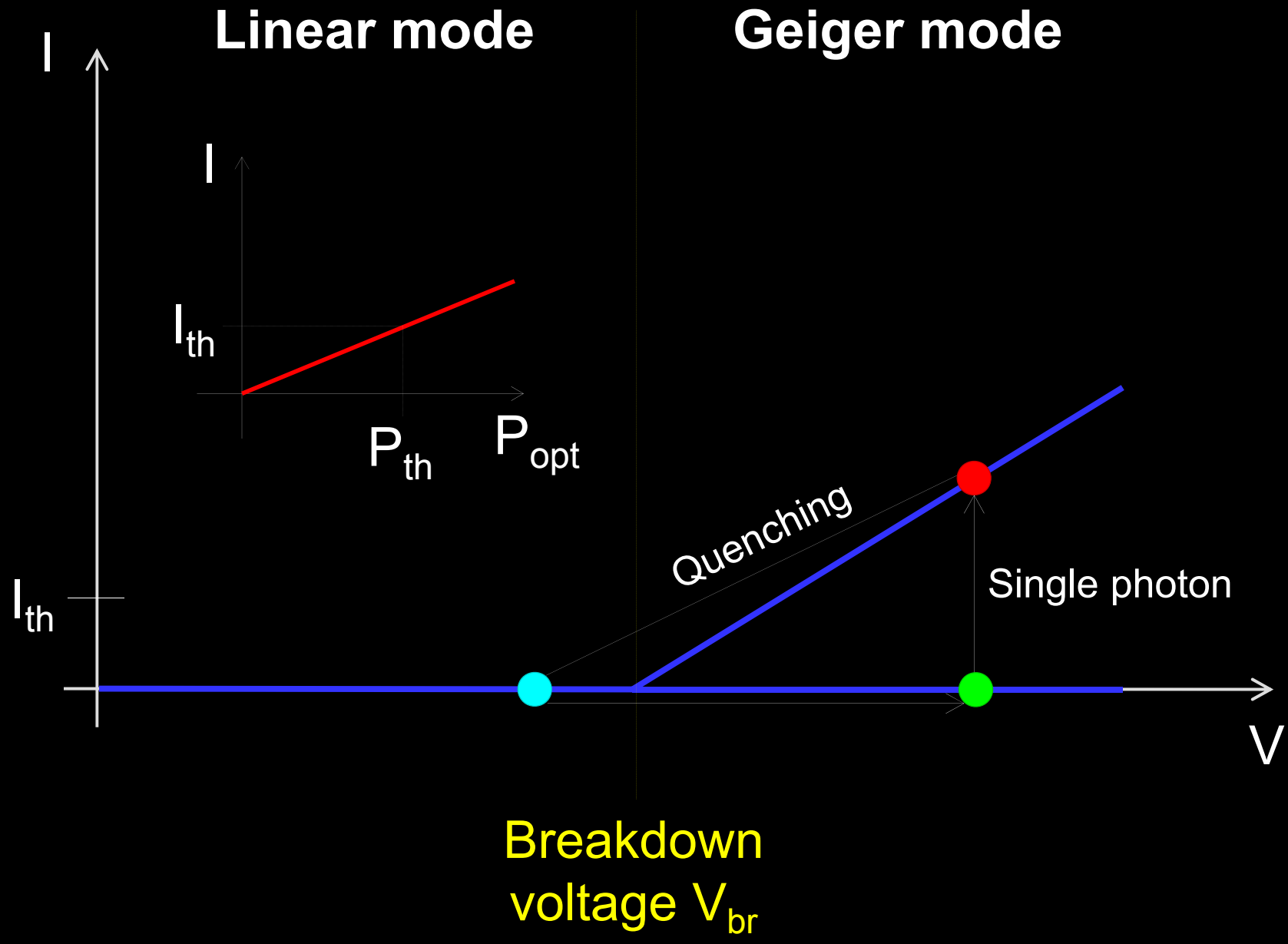
★ Distributed-phase-reference protocols

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

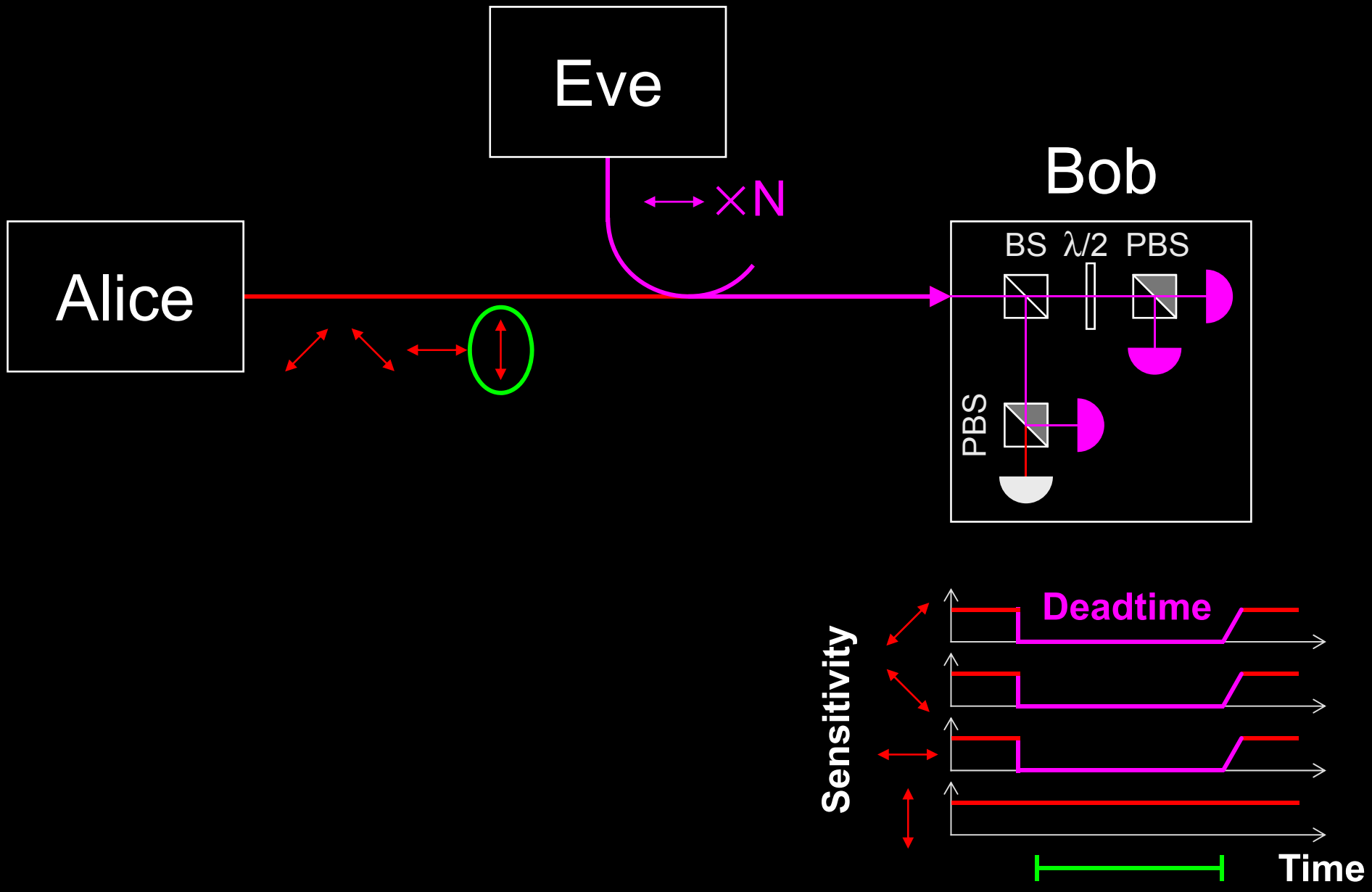
K. Inoue, E. Waks, Y. Yamamoto, Phys. Rev. A. **68**, 022317 (2003)

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

Attack example: avalanche photodetectors (APDs)

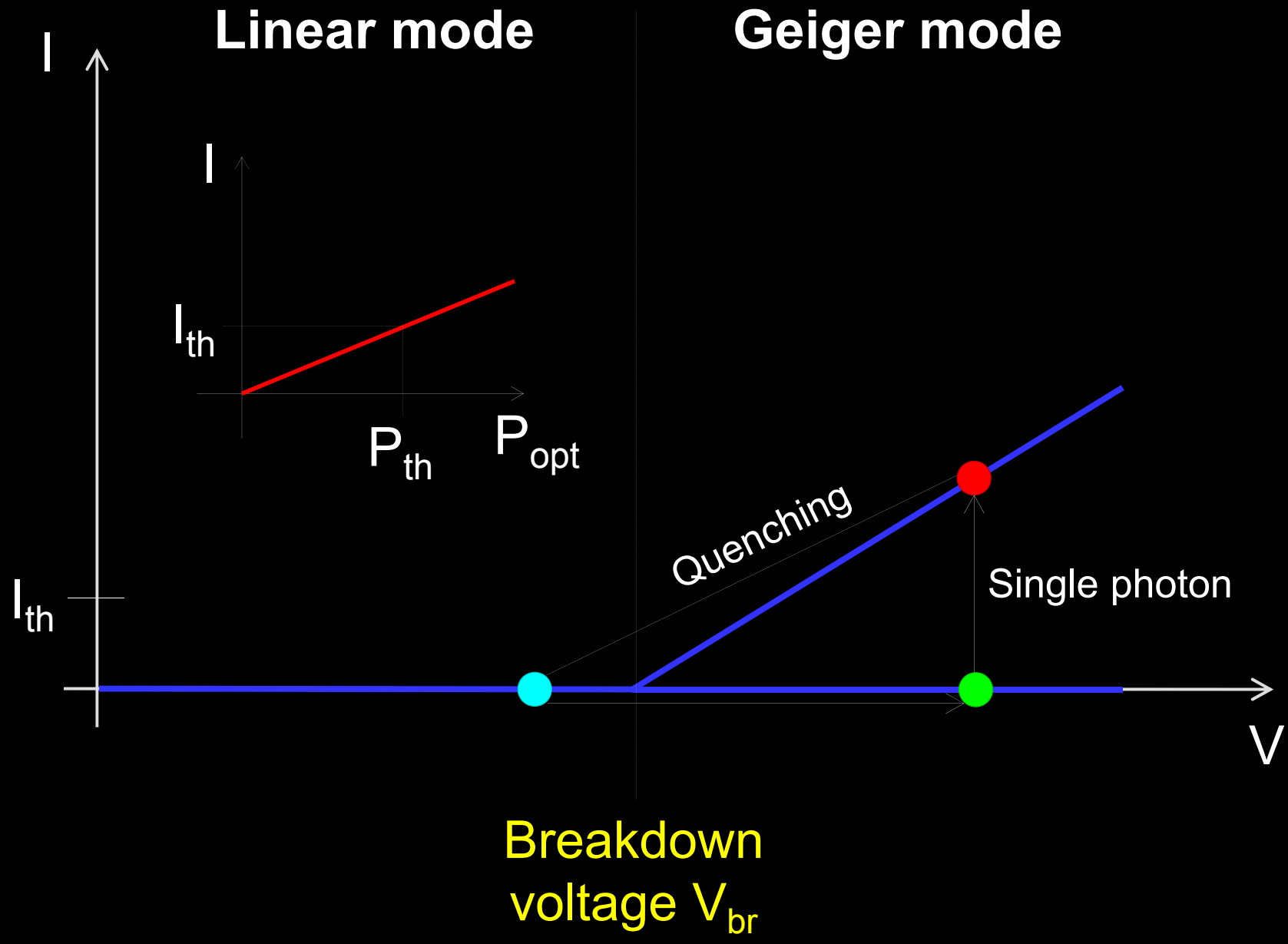


Detector deadtime attack

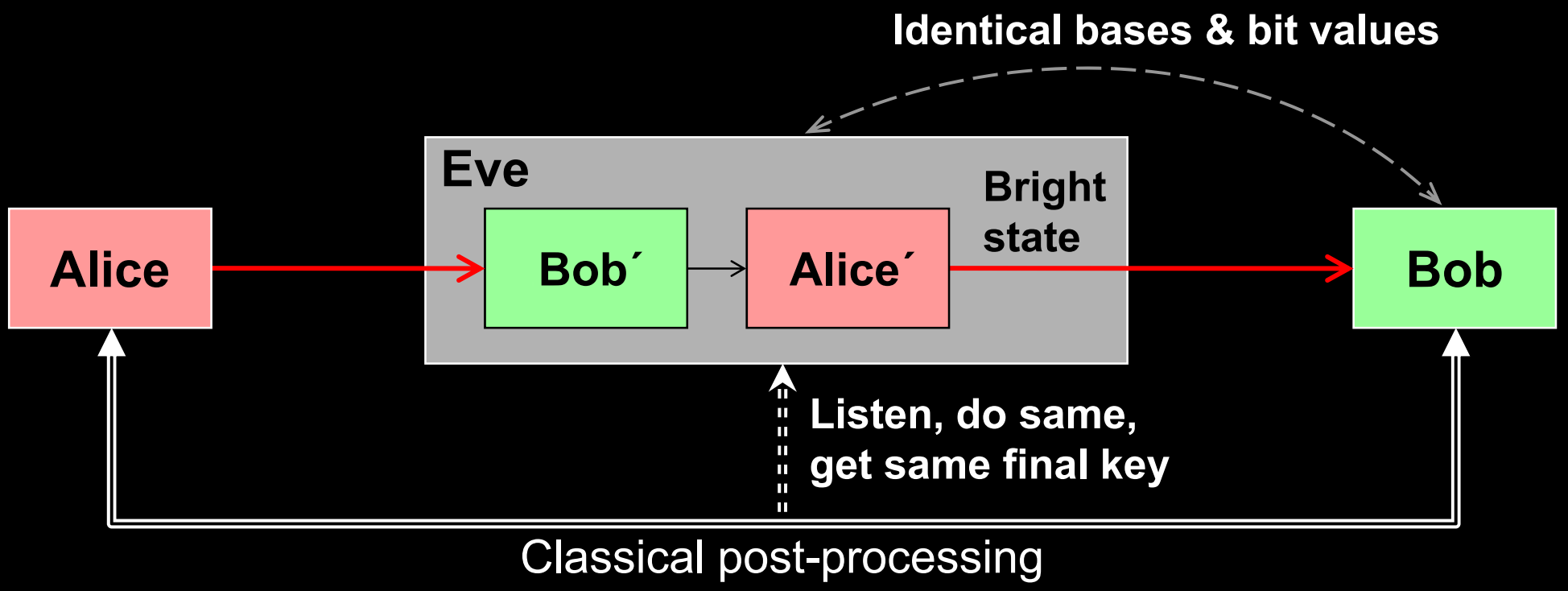


H. Weier *et al.*, New J. Phys. **13**, 073024 (2011)

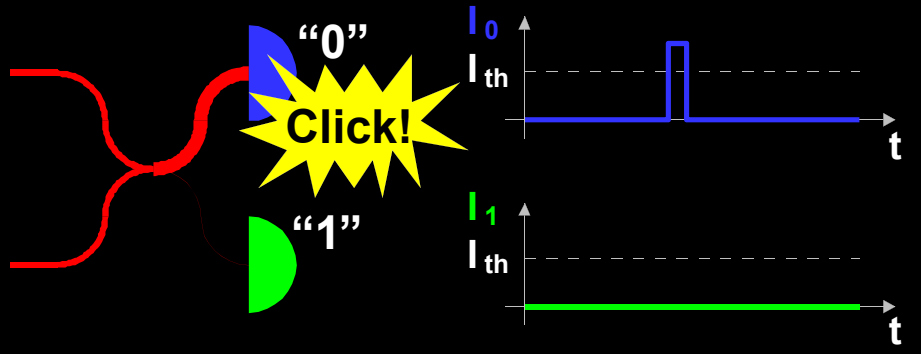
Attack example: avalanche photodetectors (APDs)



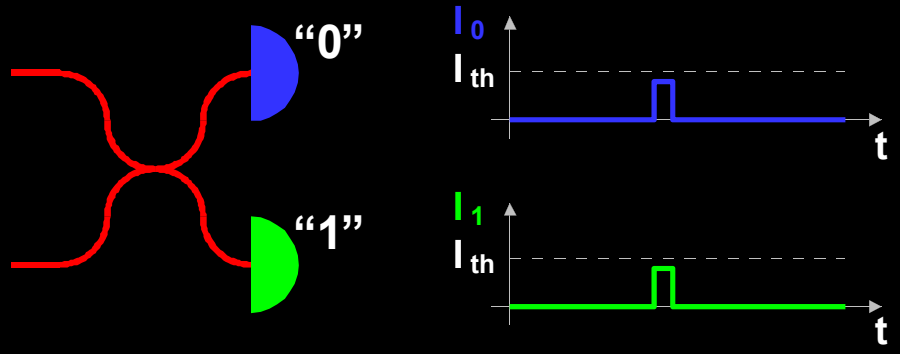
Faked-state attack in APD linear mode



Bob chooses same basis as Eve:

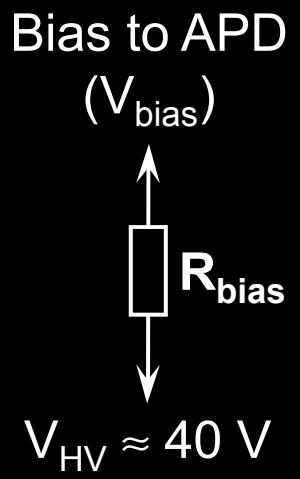


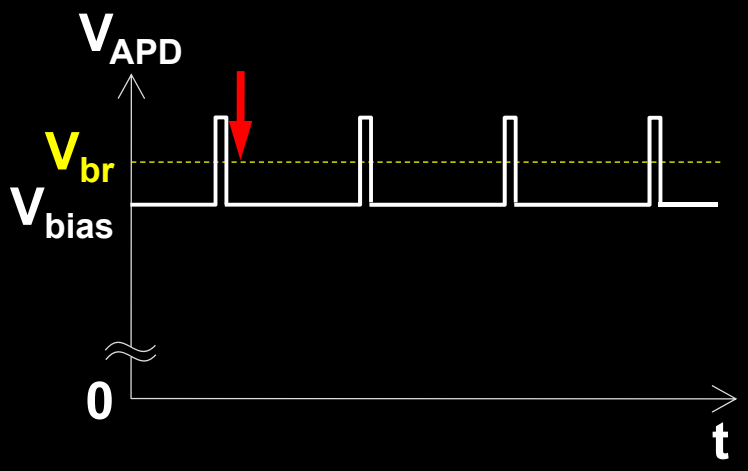
Bob chooses different basis:



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

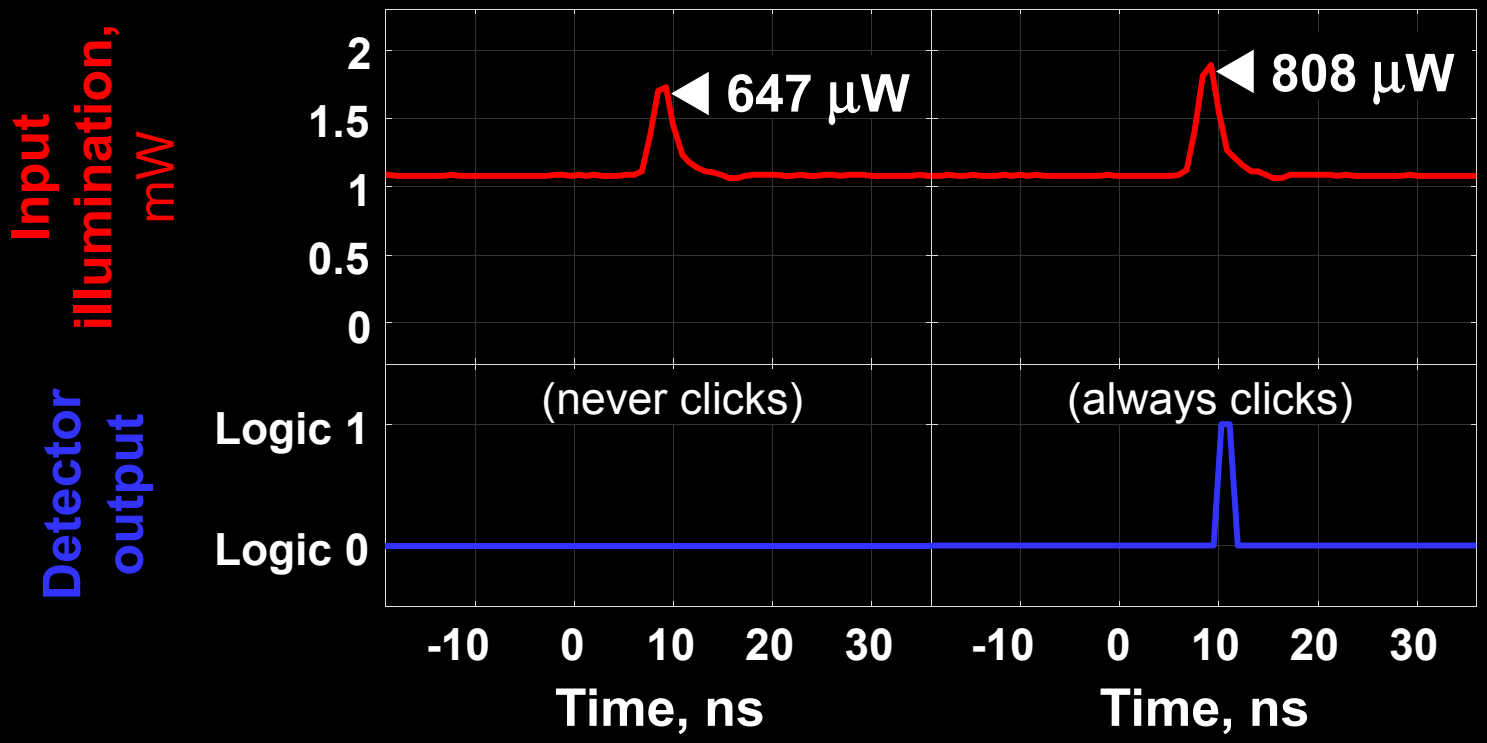
Blinding APD with bright light





Eve applies CW light

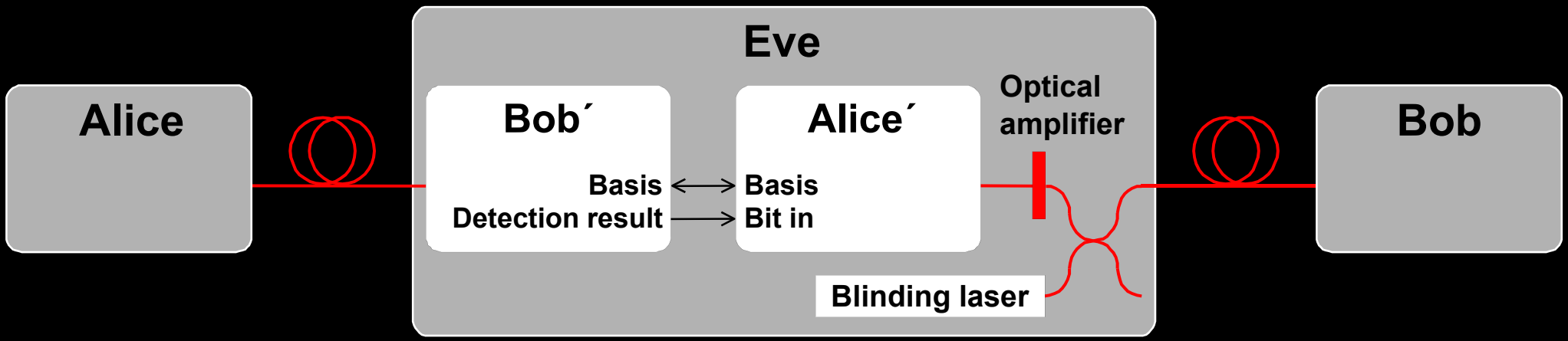
Detector blind!
Zero dark count rate



ID Quantique
Clavis2

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

Proposed full eavesdropper

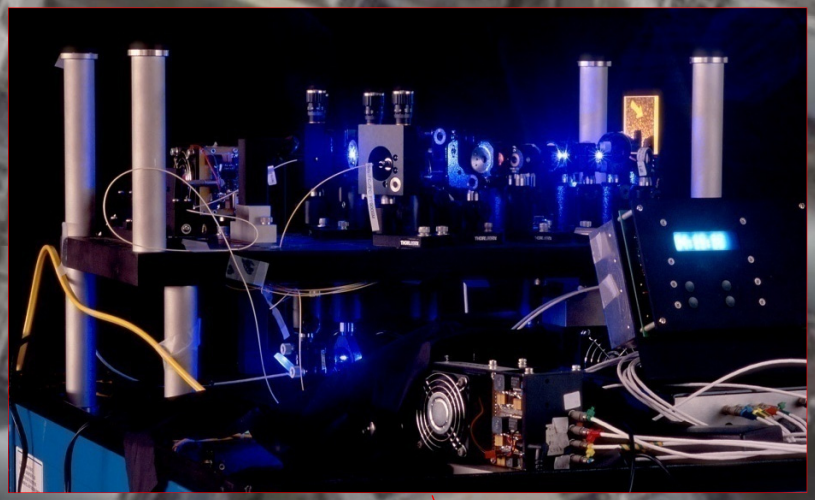


Note: Intercept-resend always breaks QKD security

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



290 m of fiber

Eve

S13

S14

Bob

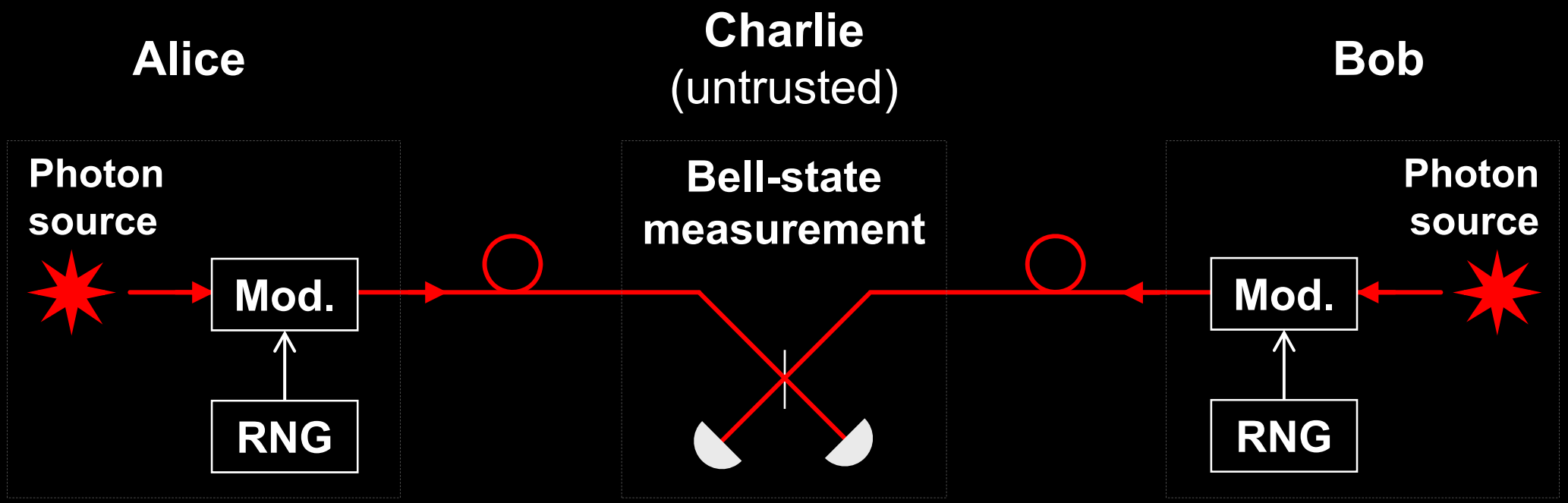
S12

Alice

S15

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

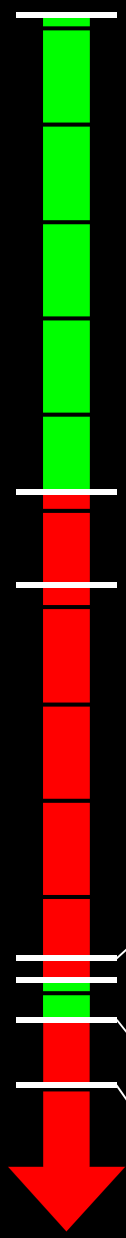
Perfect countermeasure to detector attacks



Measurement-device-independent QKD

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

Industrial countermeasure (ID Quantique)



2005 — First commercial Clavis1 system is shipped to a customer

2010 — Report about detector blinding attack sent to IDQ

2010 — IDQ applies for a patent on randomization of detector efficiency as a countermeasure

2014 — Lim *et al.* upload a preprint about countermeasure arXiv:1408.6398

2014 — ★ Implementation of countermeasure delivered by IDQ to our lab (firmware update for Clavis2)

2016 — Testing report sent to IDQ proposing a modified attack that works

2016 — Testing report sent to IDQ showing full implementation of countermeasure to be unreliable

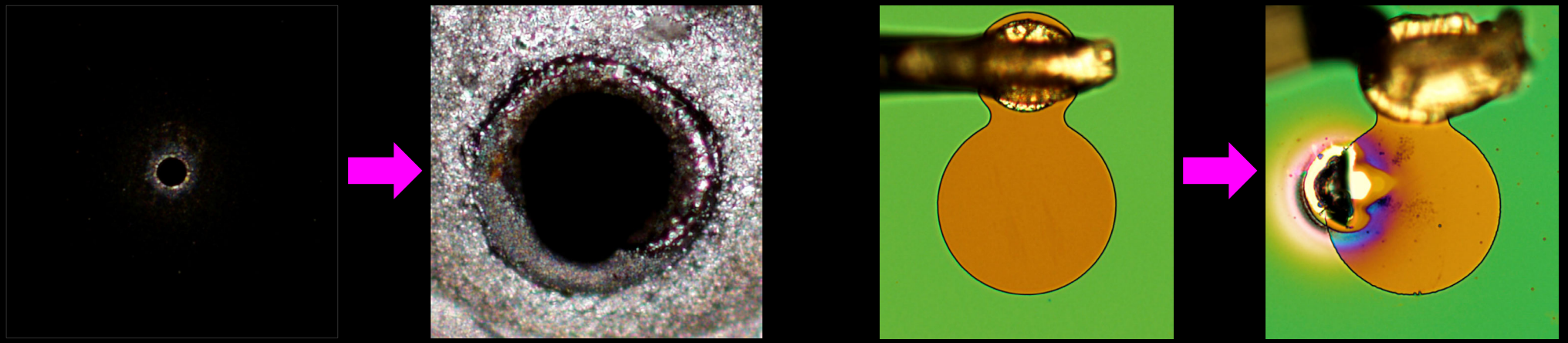
A. Huang *et al.*, arXiv:1601.00993

Once equipment is tested and certified, end of story?

Can Eve modify equipment after installation?

Crypto module — Optical line

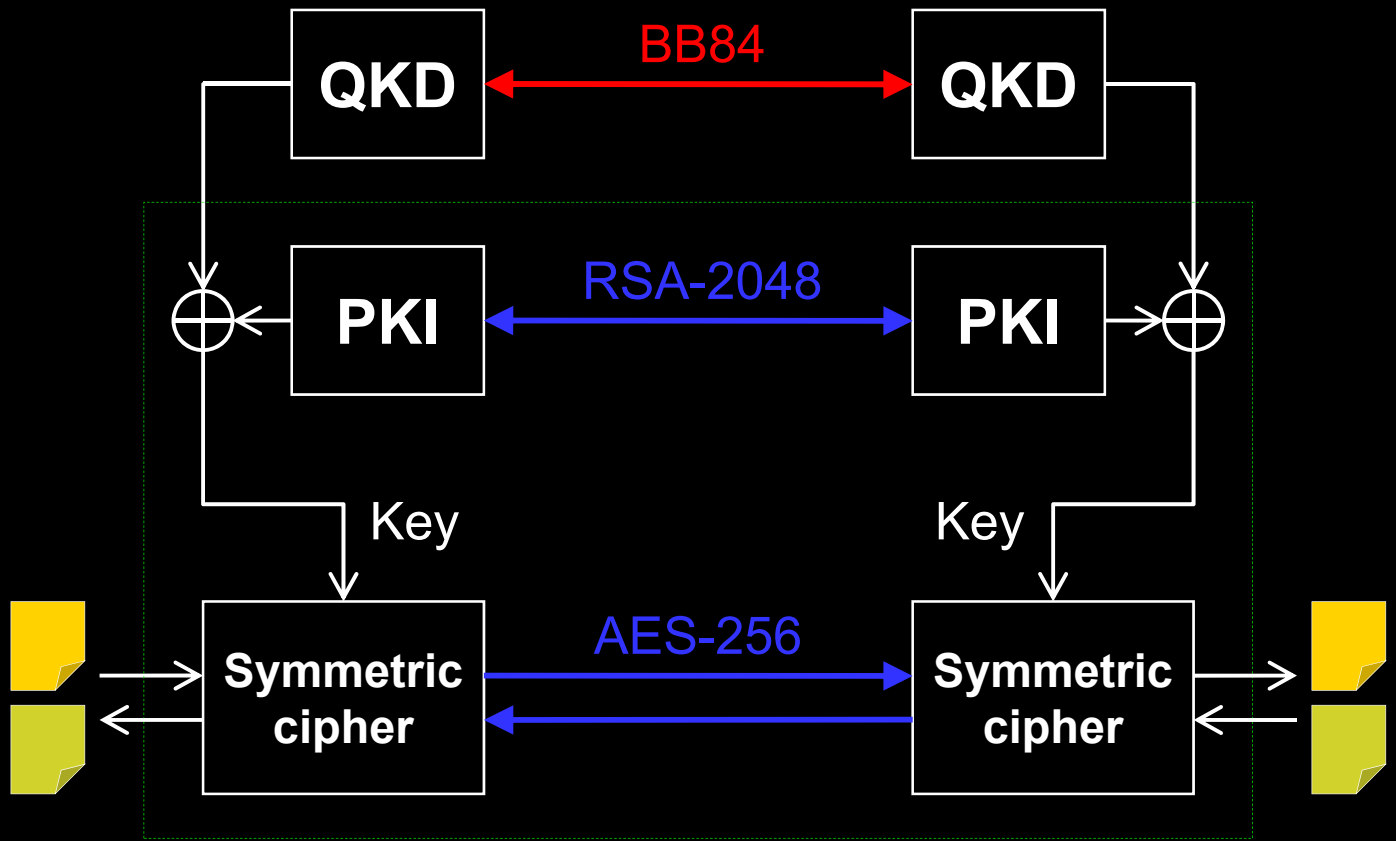
Laser damage

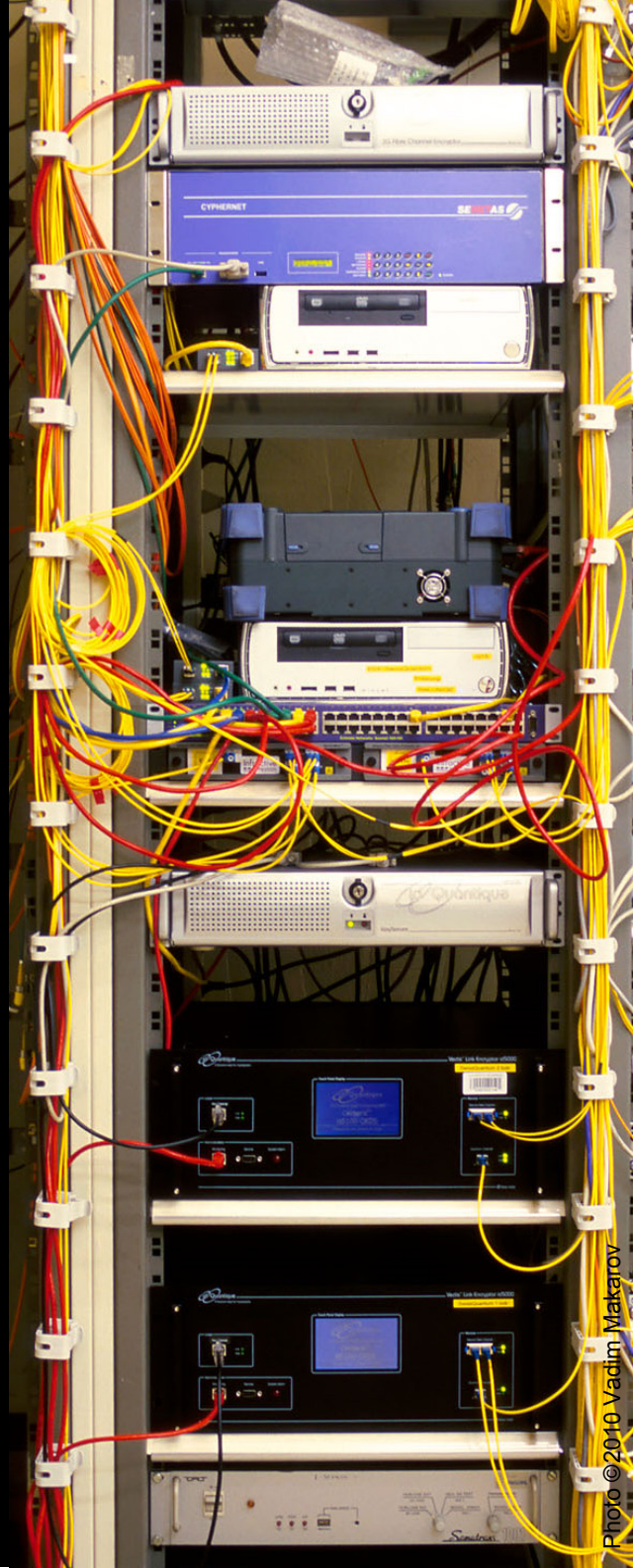


V. Makarov *et al.*, arXiv:1510.03148

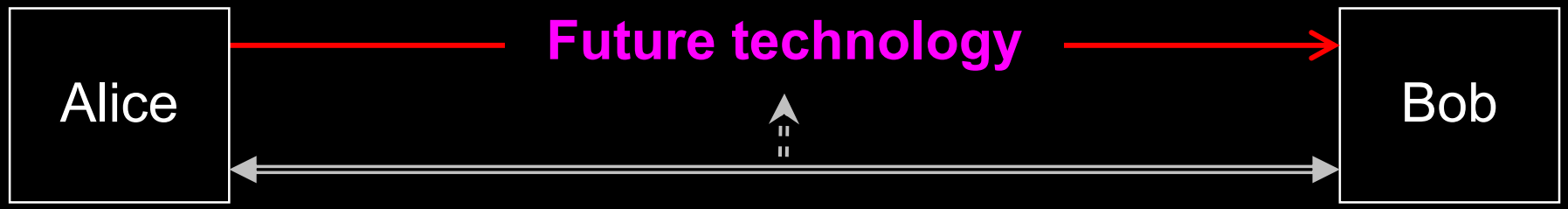
Can we eavesdrop on commercial systems?

ID Quantique's Cerberis:
Dual key agreement





Kerckhoffs' principle



characteristics known **characteristics known**

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

Eavesdropping in real life?

Alice — **Future technology** → Bob

characteristics known — Many papers — **characteristics known**

Alice — **Today's technology (modeled)** → Bob

characteristics measured — Many papers — **characteristics measured**

Alice — **Implemented** → Bob

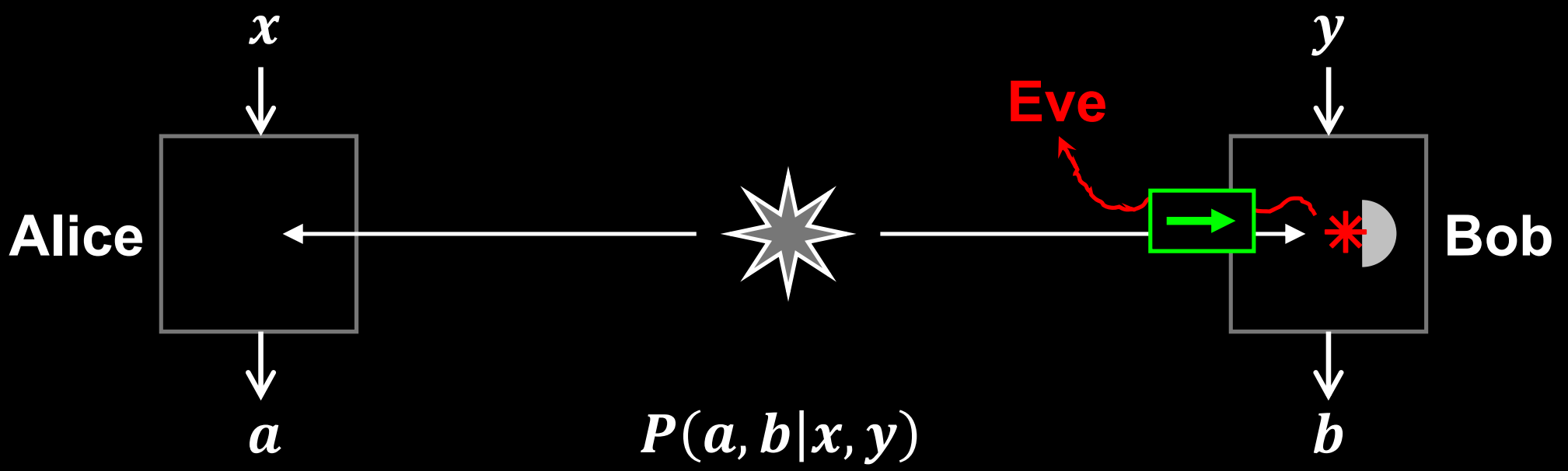
characteristics measured — **characteristics measured**

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

Alice — **Implemented** → Bob

no access — Not yet :) — **no access**

What about device-independent protocols?



Assumptions:

1. No information-leakage channels

2. No memory

J. Barrett, R. Colbeck, A. Kent, Phys. Rev. Lett. **110**, 010503 (2013)
V. Makarov *et al.*, arXiv:1510.03148

Conclusion

Physics promises unbreakable cryptography, but implementing it with our rudimentary quantum technology is a research challenge.

Suggested reading

Introduction to detector attacks and MDI-QKD

H.-K. Lo, M. Curty, K. Tamaki, Nat. Photonics **8**, 595 (2014), 10 pages

Review of more hacking techniques

N. Jain *et al.,* Contemp. Phys. **57**, 366 (2016), 22 pages

Reviews are incomplete. If you are engineering a system, read original literature (or ask for my expert advice).

Informal security evaluation

Only industrial designs

NDA, full access to engineering documentation

Team of experts :)

Identify all known potential vulnerabilities in optics and electronics (Q1–4)

Stage I: **Initial analysis of documentation**

Stage II: **Lab testing**

Security analysis layers in quantum communication

Q7. Installation and maintenance procedures

Q6. Application interface

Q5. Post-processing (e.g., for QKD: sifting, error correction, privacy amplification, authentication)

Q4. Operation cycle (state machine)

Q3. Driver and calibration algorithms

Q2. Analog electronics interface

Q1. Optics

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 it.	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