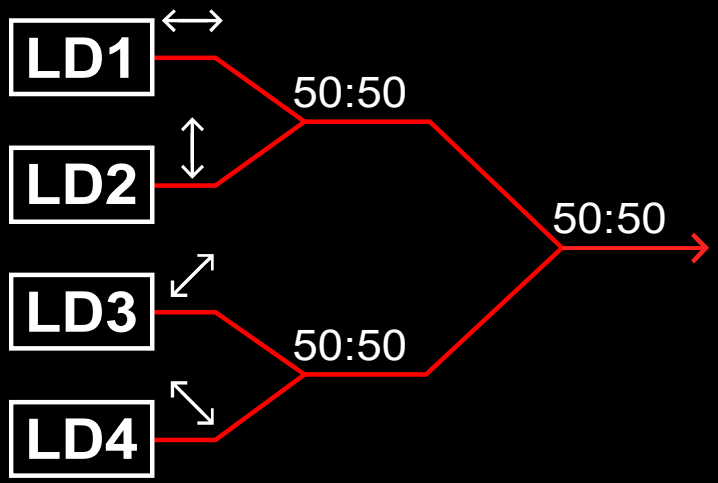
Source distinguishability; Certification and audit

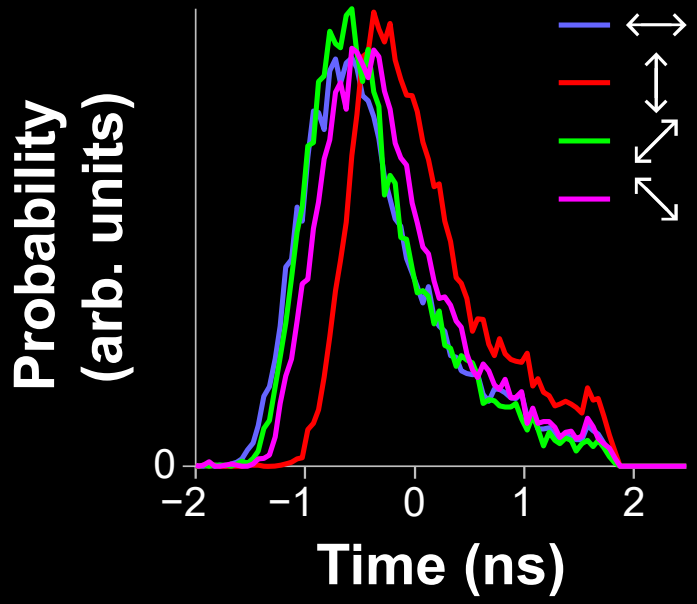
Attack	Target component	Tested system
Distinguishability of decoy states A. Huang *et al.,* Phys. Rev. A **98**, 012330 (2018)	laser in Alice	3 research systems
Intersymbol interference K. Yoshino *et al.,* poster at QCrypt (2016)	intensity modulator in Alice	research system
Laser damage V. Makarov *et 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

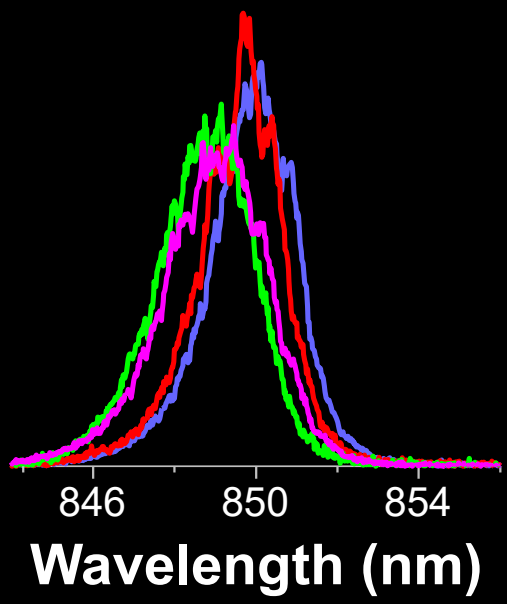
3 ways to deal with an imperfection

- ★ 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

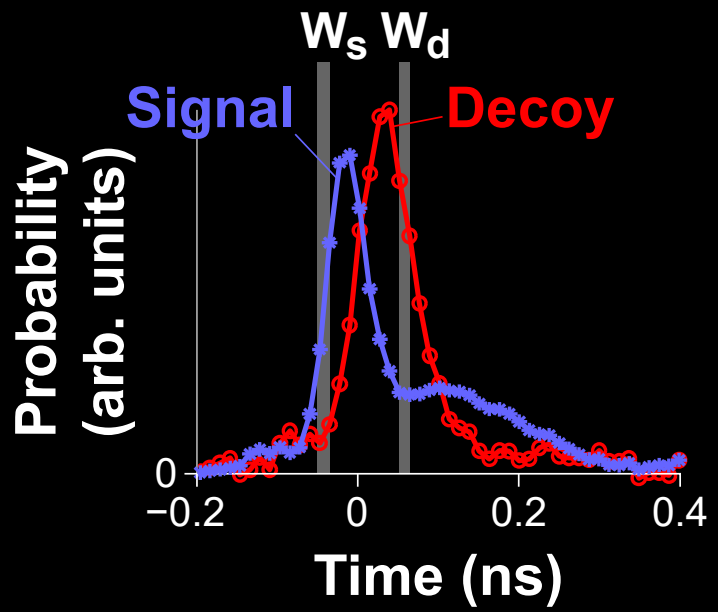
Distinguishability of source states





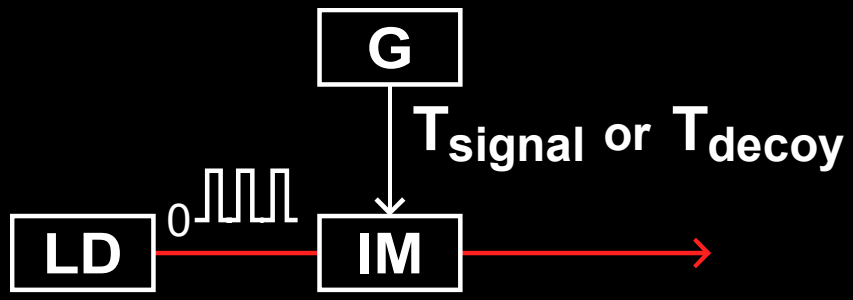


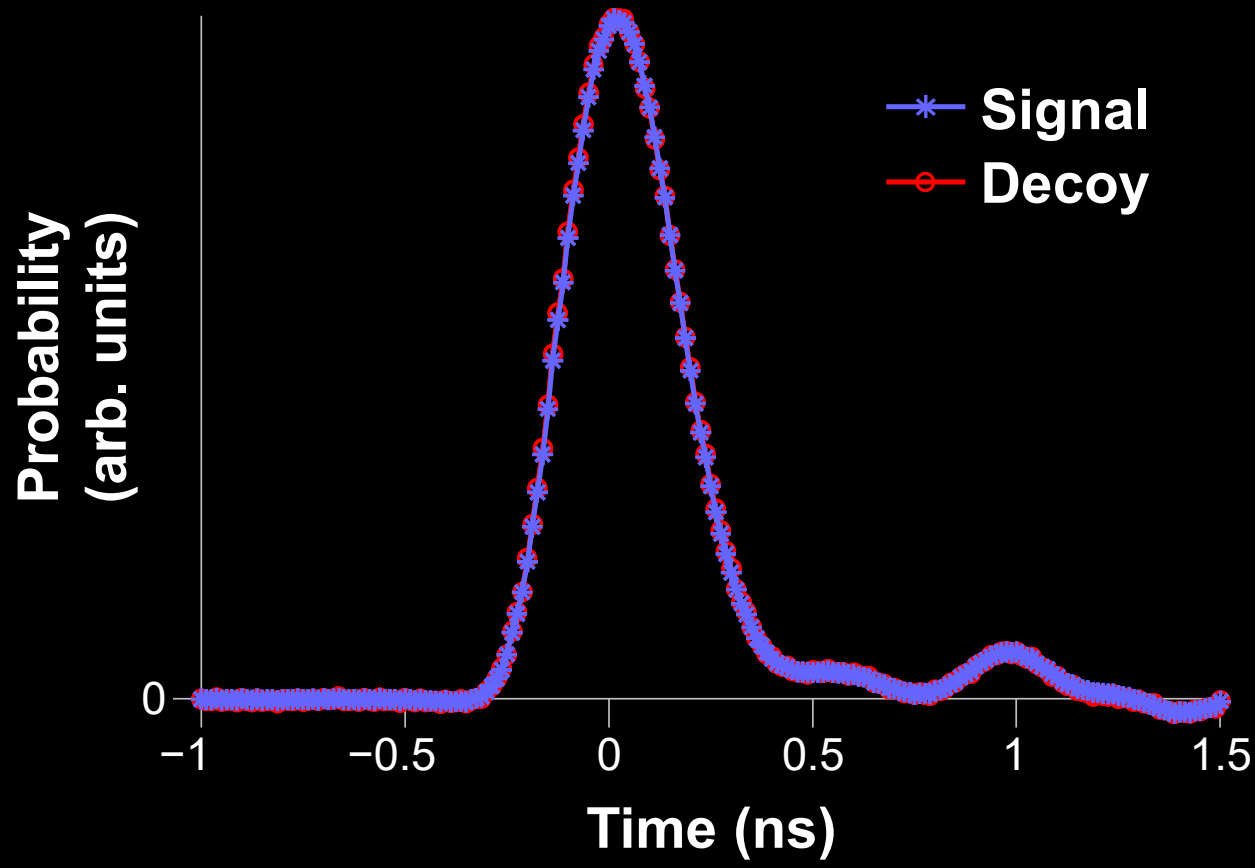
S. Nauerth *et al.*, New J. Phys. **11**, 065001 (2009)



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

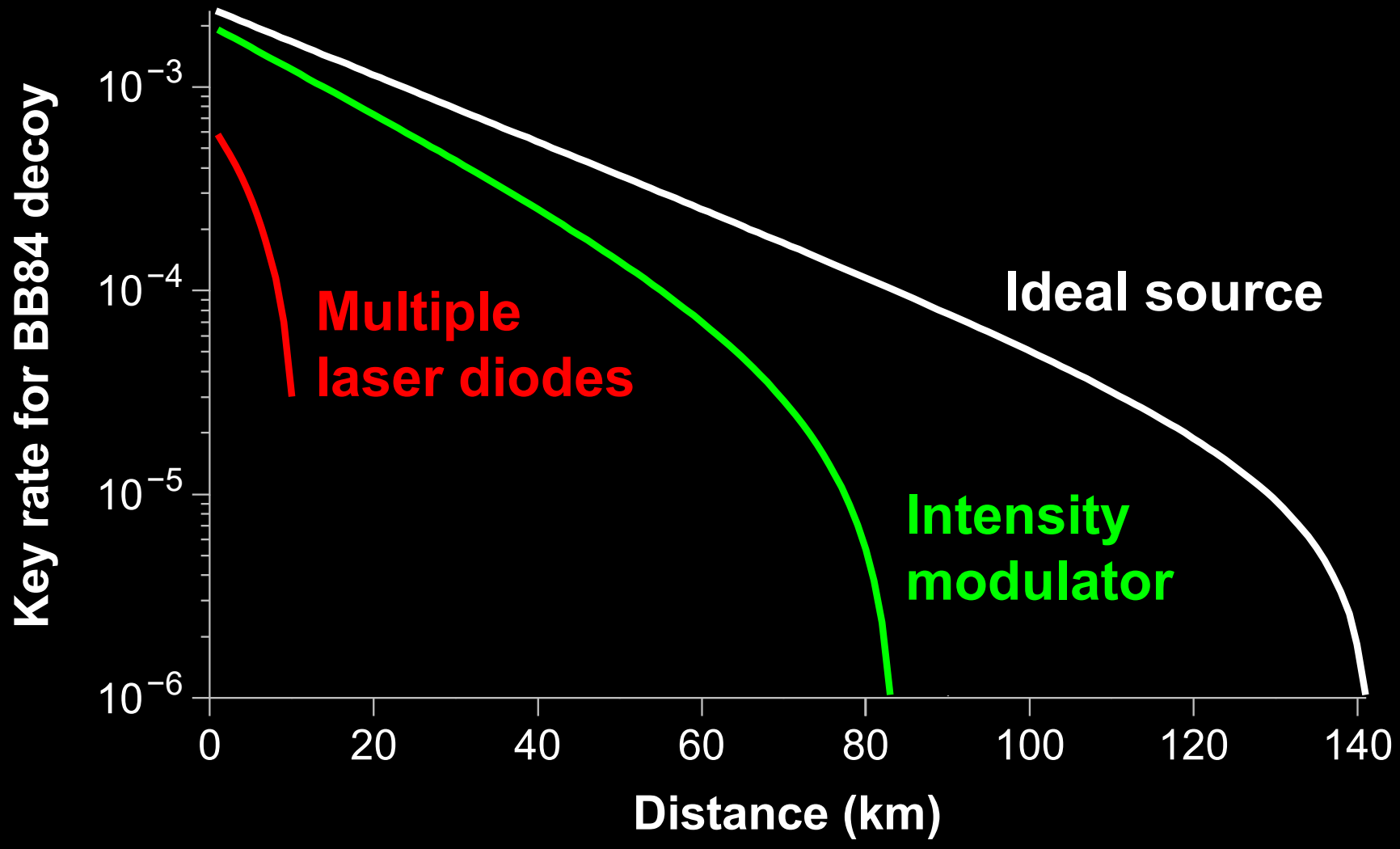
Distinguishability of source states





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

Government

National security agency

Legal requirements

Approval

Accredited lab

System

Certificate

Engineering documentation

IDQ

Manufacturer

Sale

Customer

Certification of cryptographic tools

Government

National security agency

Legal requirements

Approval

Accredited lab

Russia: optional for commercial uses

System

Certificate

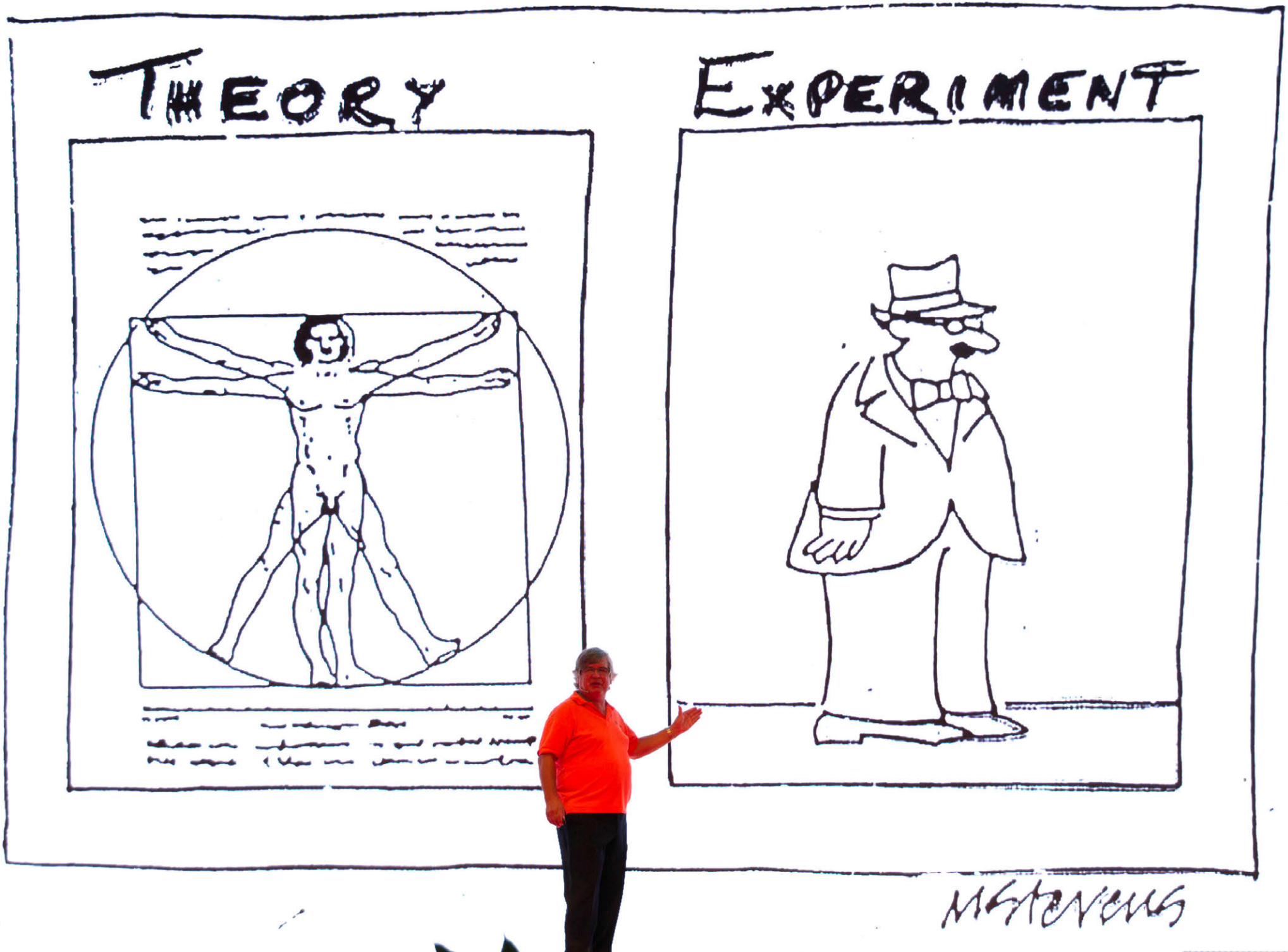
Engineering documentation

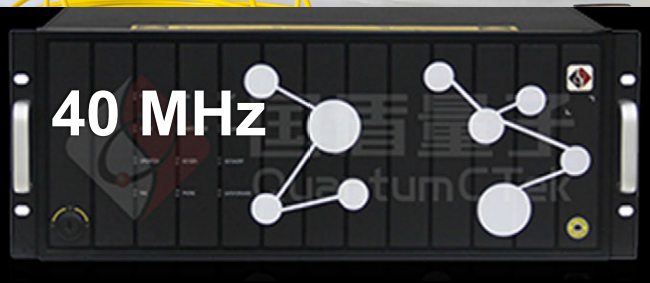
IDQ

Manufacturer

Sale

Customer


THEORY
EXPERIMENT
M STEVENS

Security audit	System	Report	Tests
IDQ	 Clavis3	2016	–2018 incomplete
国盾量子 QuantumCTek	 40 MHz	2016, 2018–19	ongoing
ITMO UNIVERSITY (ООО Квантовые коммуникации)	Subcarrier scheme	2018	ongoing
		S. Sajeed *et al.*, arXiv:1909.07898	
QRATE	New 1 GHz system	(2020)	to do

International certification standards are being developed

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 for [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

VII - 26 - X

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.

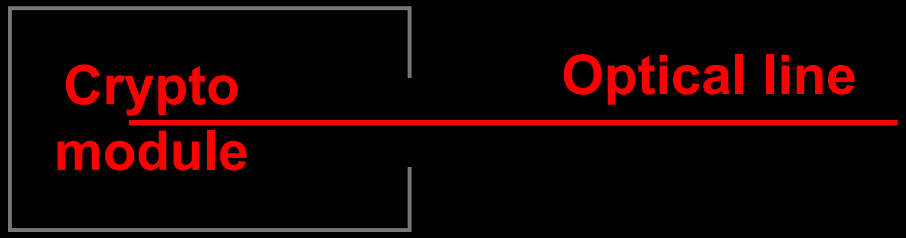
First, let me state the general nature of the problem as briefly as I can, then I will attempt something of a chronology for you. In brief: any time a machine is used to process classified information electrically, the various switches, contacts, relays, and other components in that machine may emit 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]

UNIVERSITY OF WATERLOO

Quantum hacking lab

vad1.com/lab