# Source distinguishability; Certification and audit

RQC

MISIS

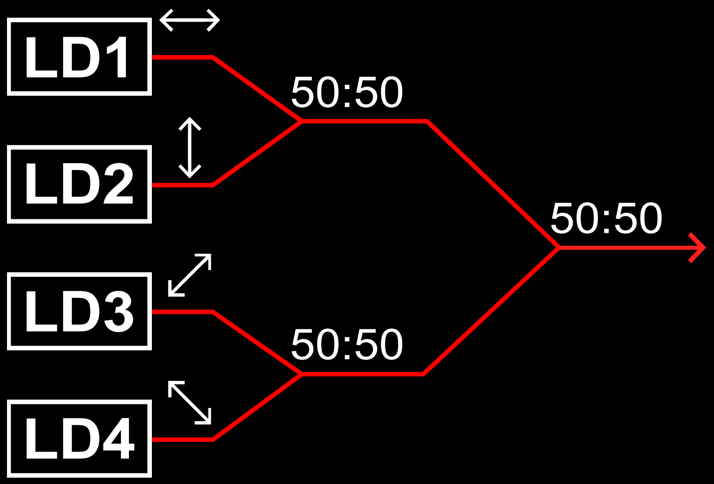
Quantum hacking lab
vad1.com/lab

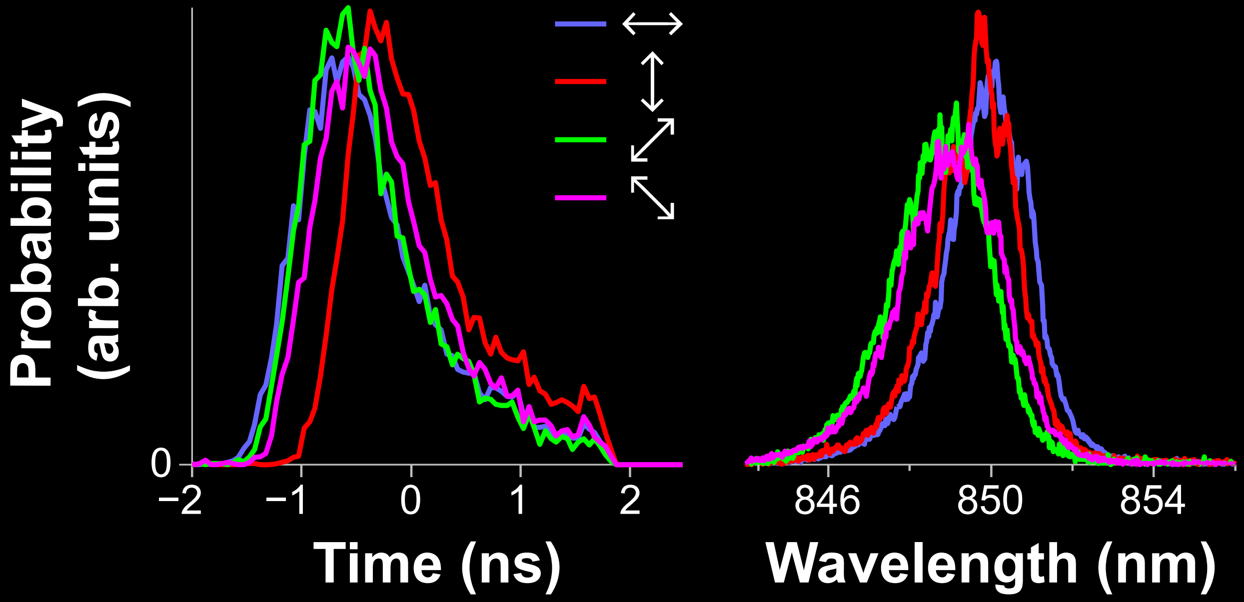
Lecture 13 in Quantum communications course,
19 Nov 2023

# 3 ways to deal with an imperfection

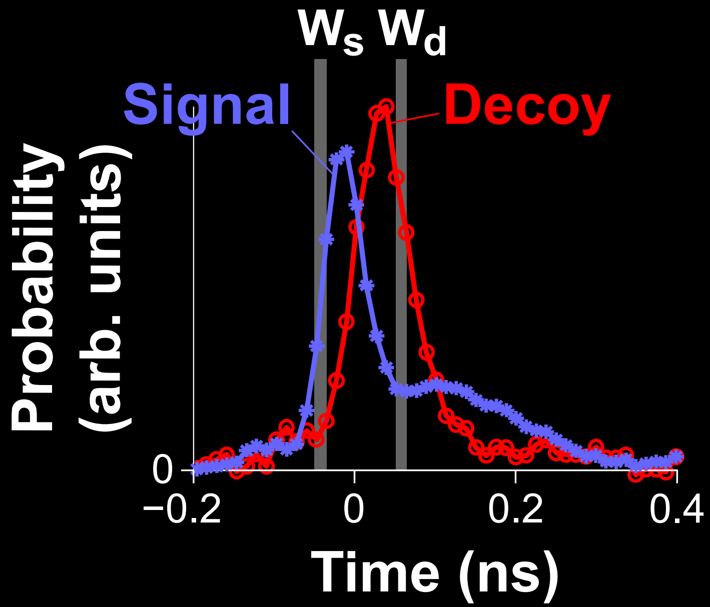
- ★ Technical countermeasure that attempts to stop the attack
- ★ Make a scheme intrinsically insensitive to imperfection
- ★ Characterise imperfection, upper-bound *partial* information leakage, eliminate it by privacy amplification

# Distinguishability of source states



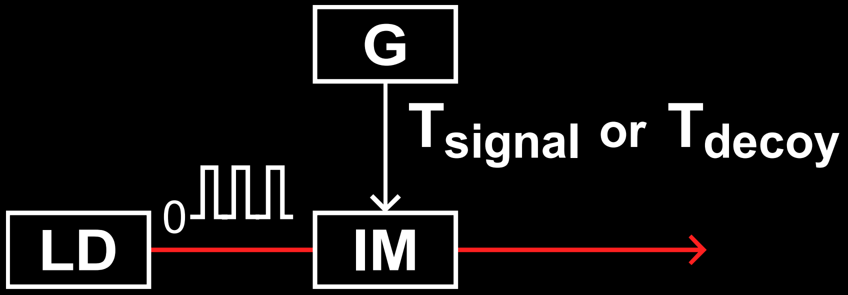


S. Nauerth *et al.*, New J. Phys. **11**, 065001 (2009)



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

# Distinguishability of source states



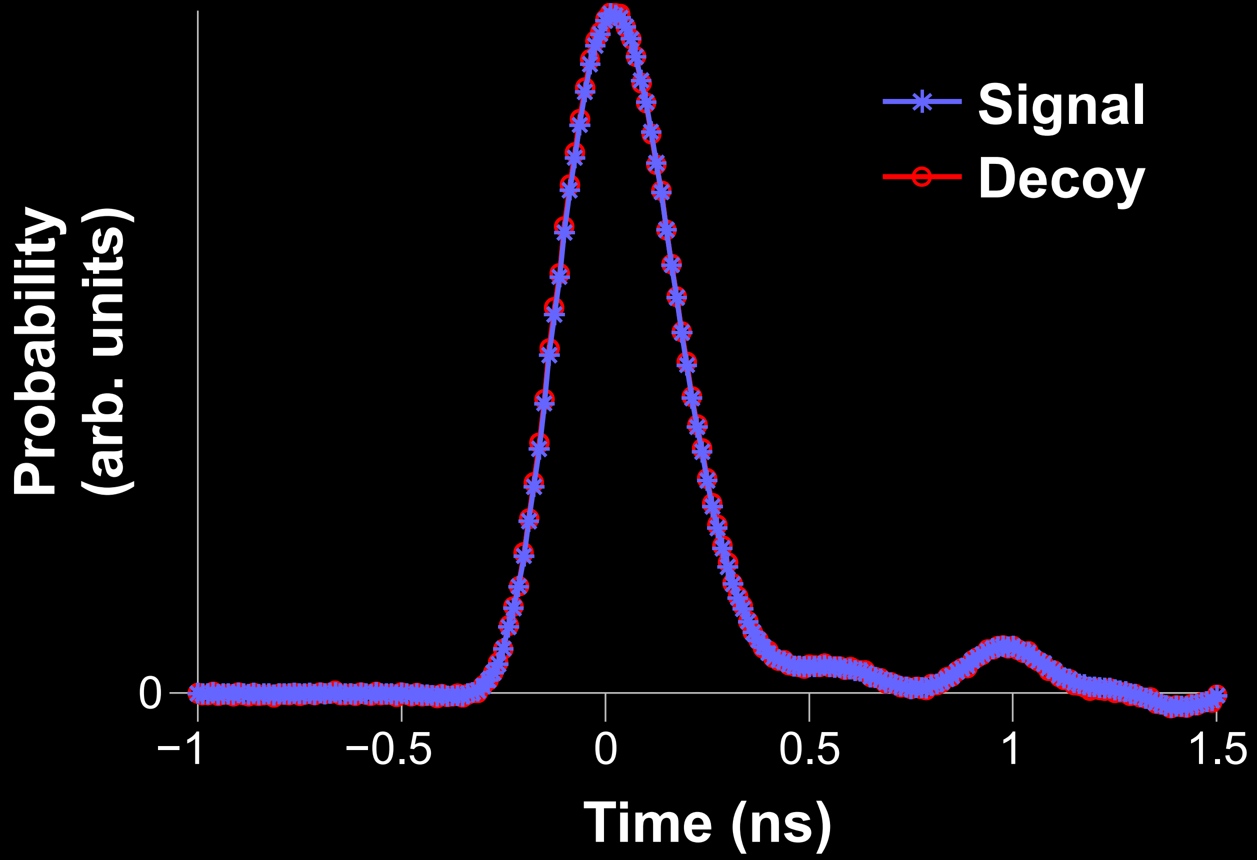
G

$T_{\text{signal}}$ or $T_{\text{decoy}}$

0

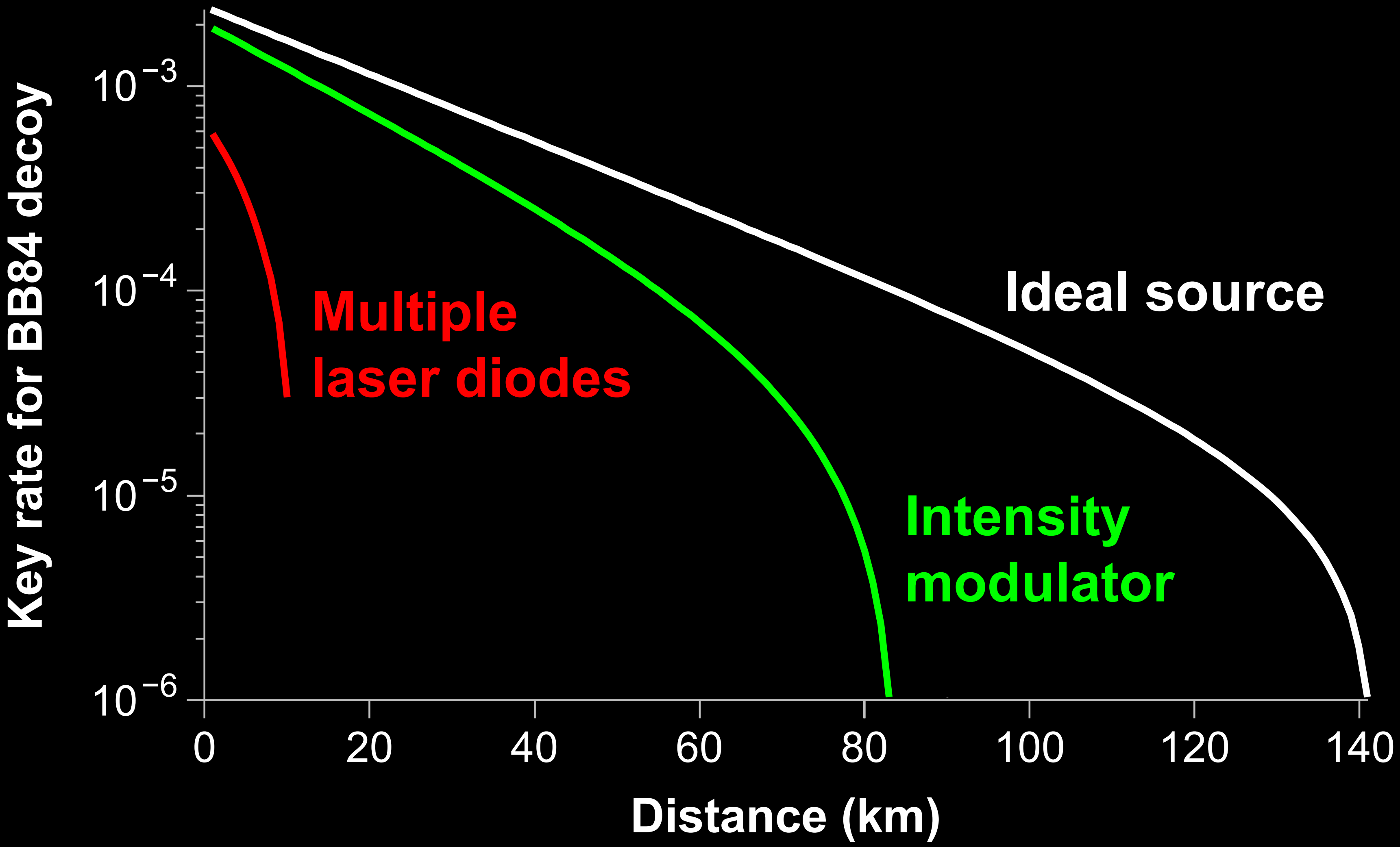
LD

IM



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

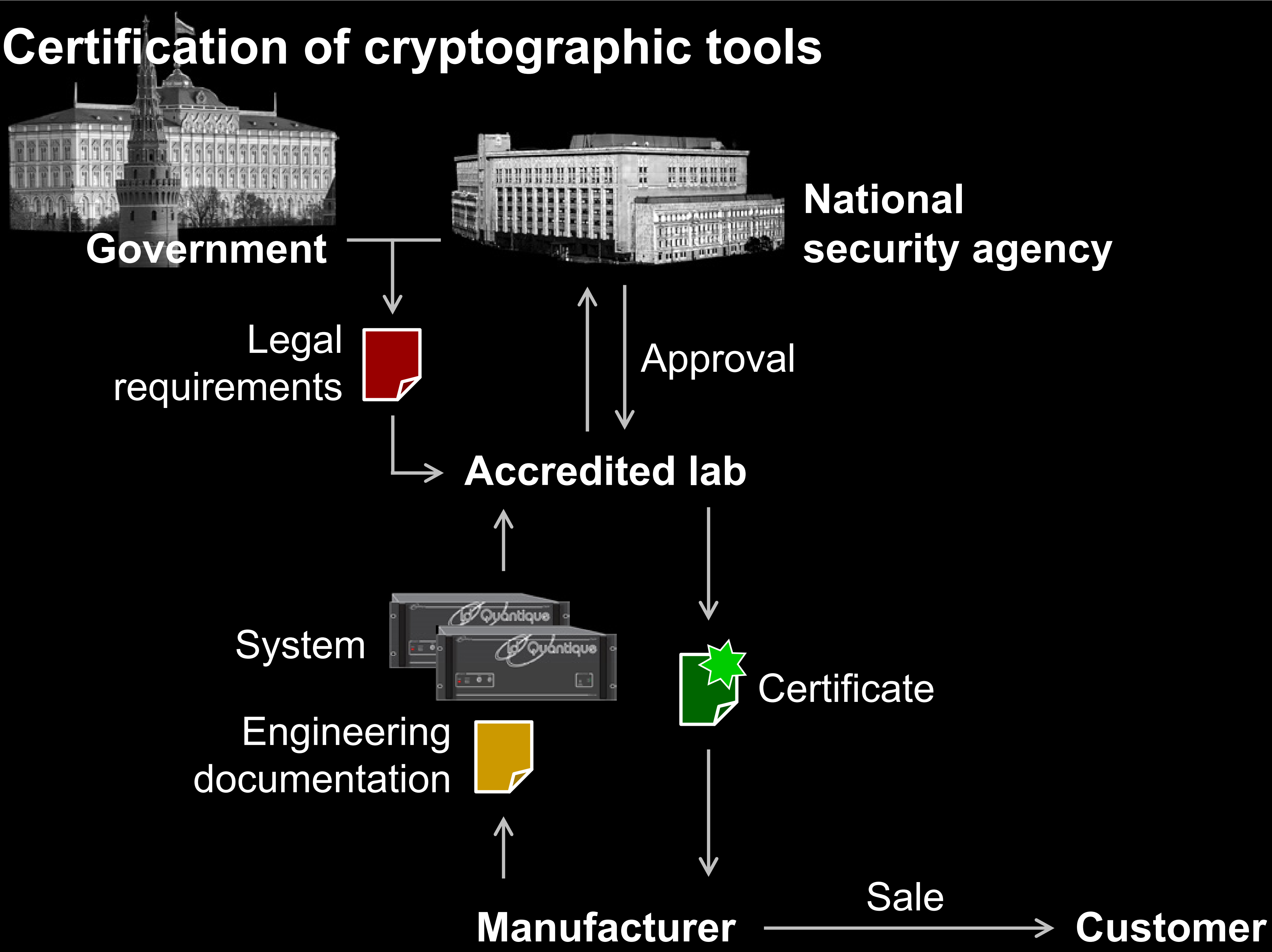
# Distinguishability of source states



**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

Engineering documentation

Certificate

**Manufacturer**

Sale

**Customer**

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

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

V. Makarov *et al.*, Phys. Rev. Appl. **22**, 044076 (2024)

**Certification standards are being drafted since 2019 in**

ETSI **Industry standards group in QKD** ISO

# Example of initial analysis report

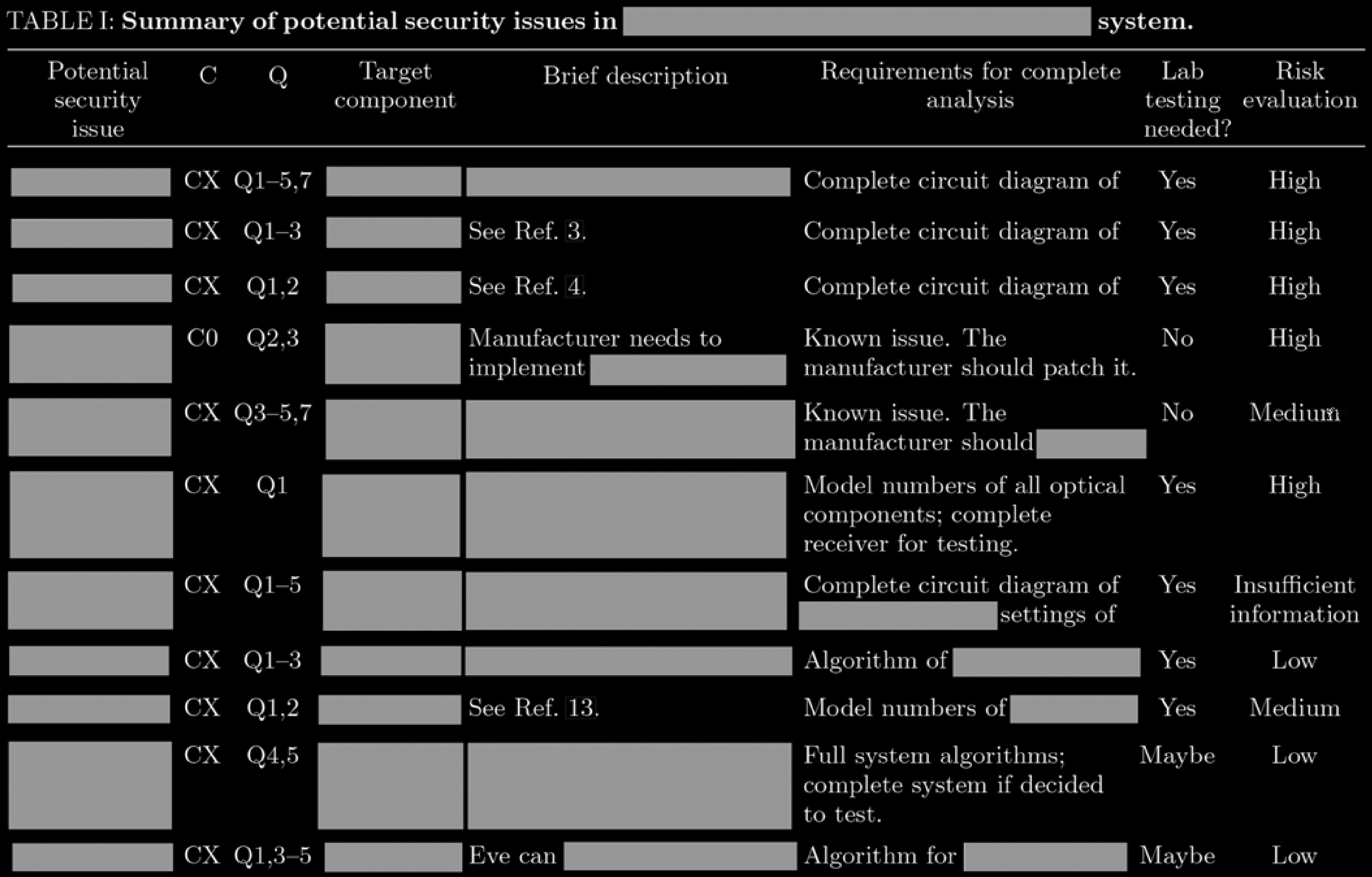


TABLE I: **Summary of potential security issues in [redacted] system.**

| 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 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 |

# ISO/IEC 23837: Security requirements, test and evaluation methods for quantum key distribution

7 Supplementary activities for the evaluation of quantum optical components in the transmitter module
- 7.1 General
- 7.2 Evaluation activity to test the photon-number distribution of optical pulses
- 7.3 Evaluation activity to test the mean photon number and stability of optical pulses
- 7.4 Evaluation activity to test the independence of the intensities of optical pulses
- 7.5 Evaluation activity to test the accuracy of state encoding
- 7.6 Evaluation activity to test the indistinguishability of encoded states from the perspective of non-encoding degrees of freedom
- 7.7 Evaluation activity to test the uniform distribution of the global phase of optical pulses
- 7.8 Evaluation activity to test the degree of optical isolation of the TX module
- 7.9 Evaluation activity to test the sensitivity of the injected light monitor in the TX module
- 7.10 Evaluation activity to test the robustness of the TX module against laser injection

8 Supplementary activities for the evaluation of quantum optical components in the receiver module
- 8.1 General
- 8.2 Evaluation activity to test the consistency of detection probability in the RX module
- 8.3 Evaluation activity to test if back-flashes from the RX module can leak information
- 8.4 Evaluation activity to test the degree of optical isolation of the RX module
- 8.5 Evaluation activity to test the sensitivity of the injected light monitor in the RX module
- 8.6 Evaluation activity to test the robustness of the RX module against bright light blinding
- 8.7 Evaluation activity to test the appropriateness of dead time settings of single-photon detectors
- 8.8 Evaluation activity to test the temporal profile of the detection efficiency for single-photon detectors
- 8.9 Evaluation activity to test the robustness of the RX module against laser injection
- 8.10 Evaluation activity to test the detection limits of homodyne detectors in the RX module
- 8.11 Evaluation activity to test the appropriateness of double-click events handling

https://www.iso.org/obp/ui/en/#iso:std:iso-iec:23837:-2:ed-1:v1:en

# ISO/IEC 23837: Security requirements, test and evaluation methods for quantum key distribution

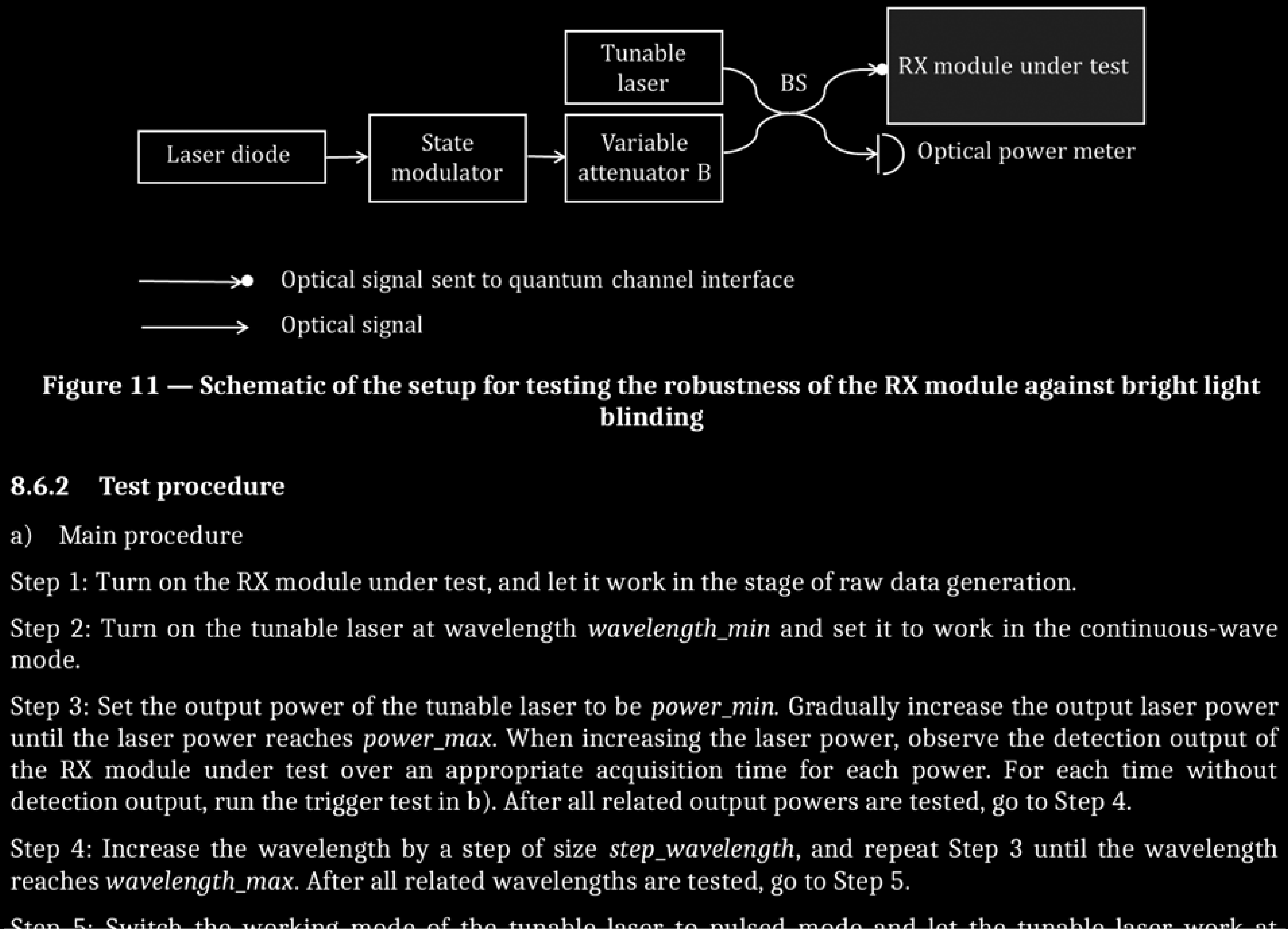


**Figure 11 — Schematic of the setup for testing the robustness of the RX module against bright light blinding**

### 8.6.2 Test procedure

a) Main procedure

Step 1: Turn on the RX module under test, and let it work in the stage of raw data generation.

Step 2: Turn on the tunable laser at wavelength *wavelength_min* and set it to work in the continuous-wave mode.

Step 3: Set the output power of the tunable laser to be *power_min*. Gradually increase the output laser power until the laser power reaches *power_max*. When increasing the laser power, observe the detection output of the RX module under test over an appropriate acquisition time for each power. For each time without detection output, run the trigger test in b). After all related output powers are tested, go to Step 4.

Step 4: Increase the wavelength by a step of size *step_wavelength*, and repeat Step 3 until the wavelength reaches *wavelength_max*. After all related wavelengths are tested, go to Step 5.

Step 5: Switch the working mode of the tunable laser to pulsed mode and let the tunable laser work at

~~COMINT~~

Declassified and approved for release by NSA on 12-10-2008 pursuant to E.O. 12958, as amended. MDR 54498

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.

[redacted]

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 een equalled. (Although, to get ahead of the story for a moment, in some circumstances now-a-ays, either radiated or conducted signals can be picked up, amplified, and used to drive a tele-

# Today's digital

Crypto module - Bus - Memory - Software - Bus - Signal proc. - DAC - Amplifier

# vs. quantum

Crypto module

Optical line

# [vs. future quantum]

Crypto module

Quantum bus, computer, memory...