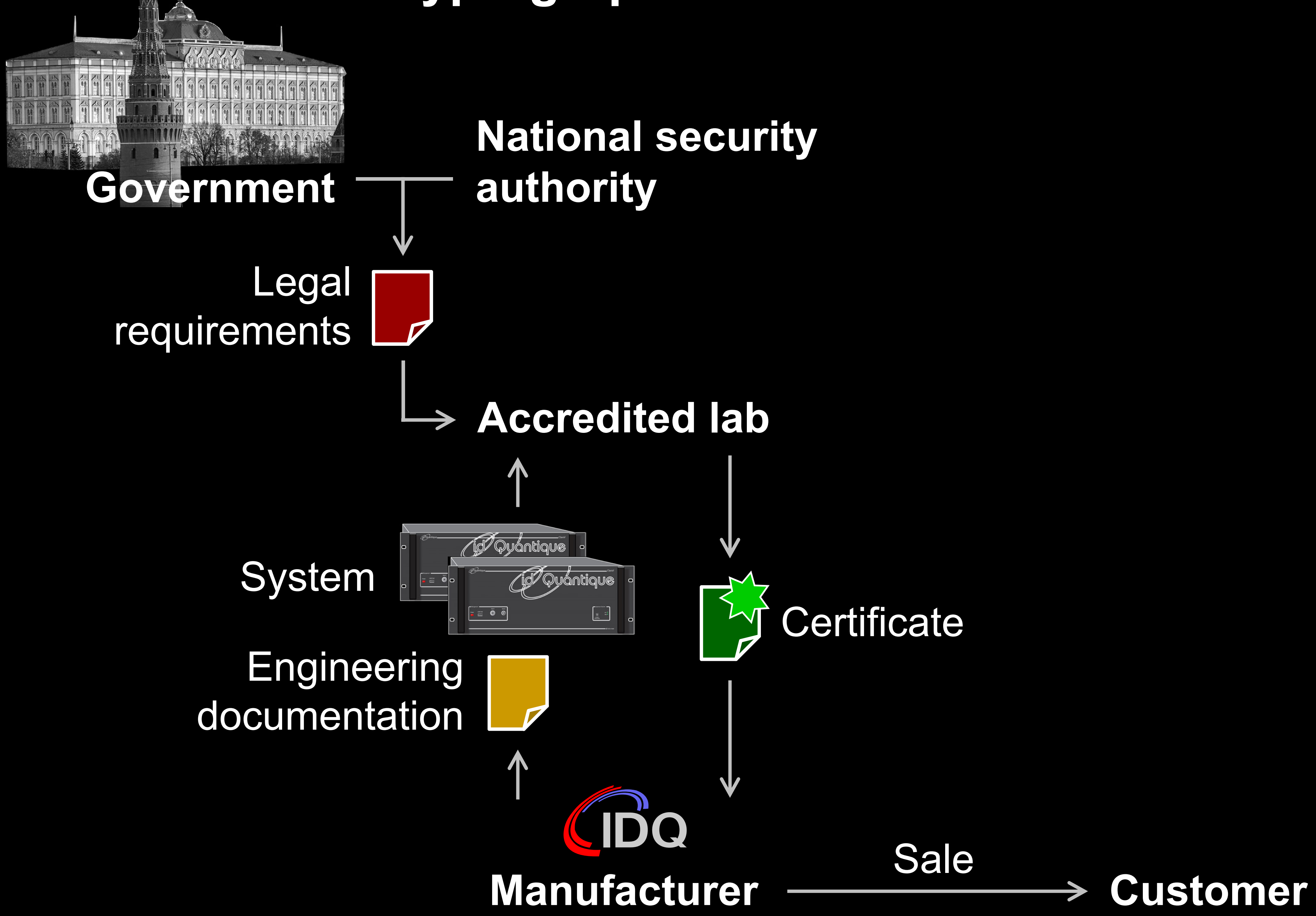
Certification of cryptographic tools



Government

National security authority

Legal requirements

Accredited lab

System

Engineering documentation

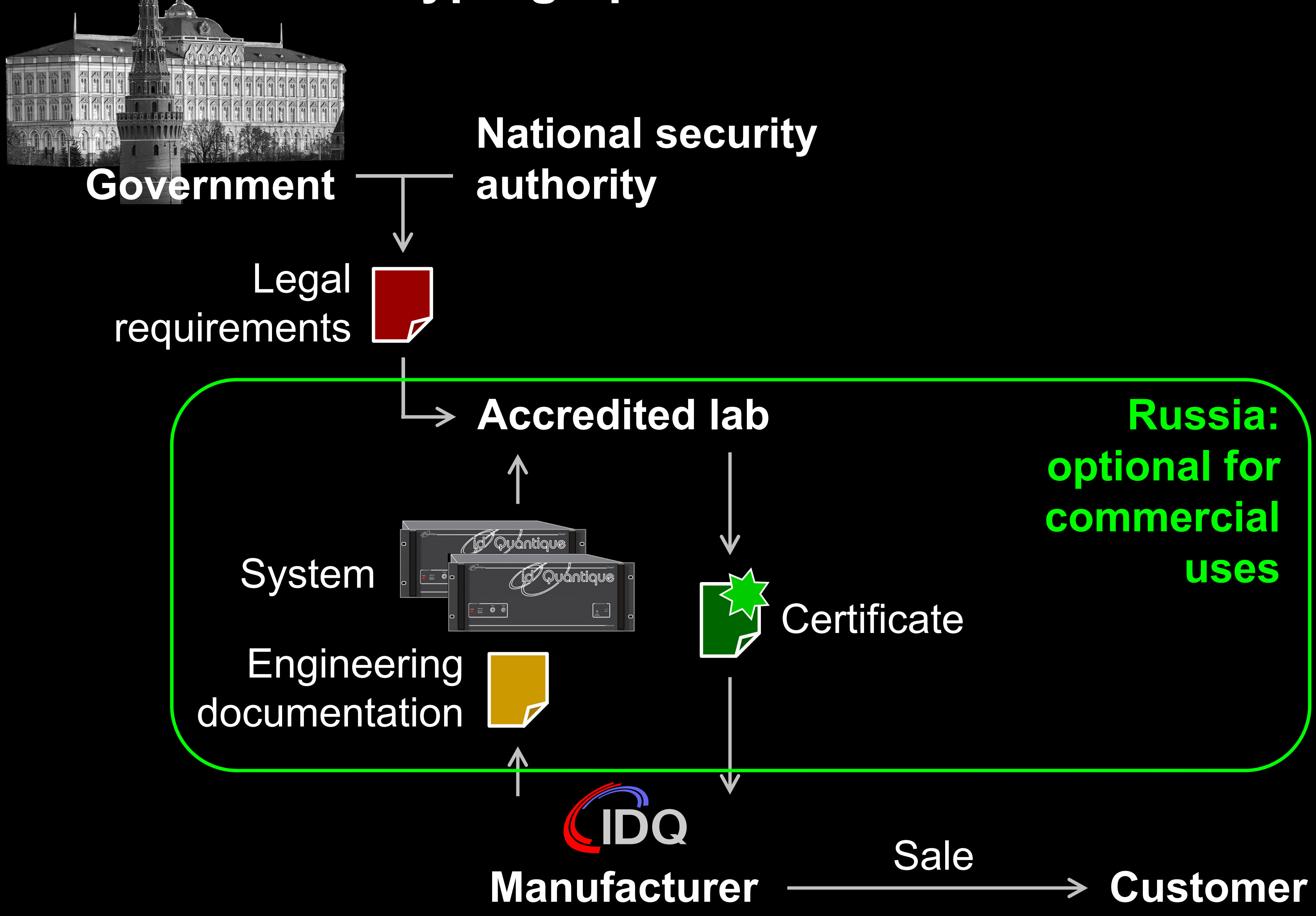
Certificate

Manufacturer

Sale

Customer

Certification of cryptographic tools



Government

National security authority

Legal requirements

Accredited lab

Russia: optional for commercial uses

System

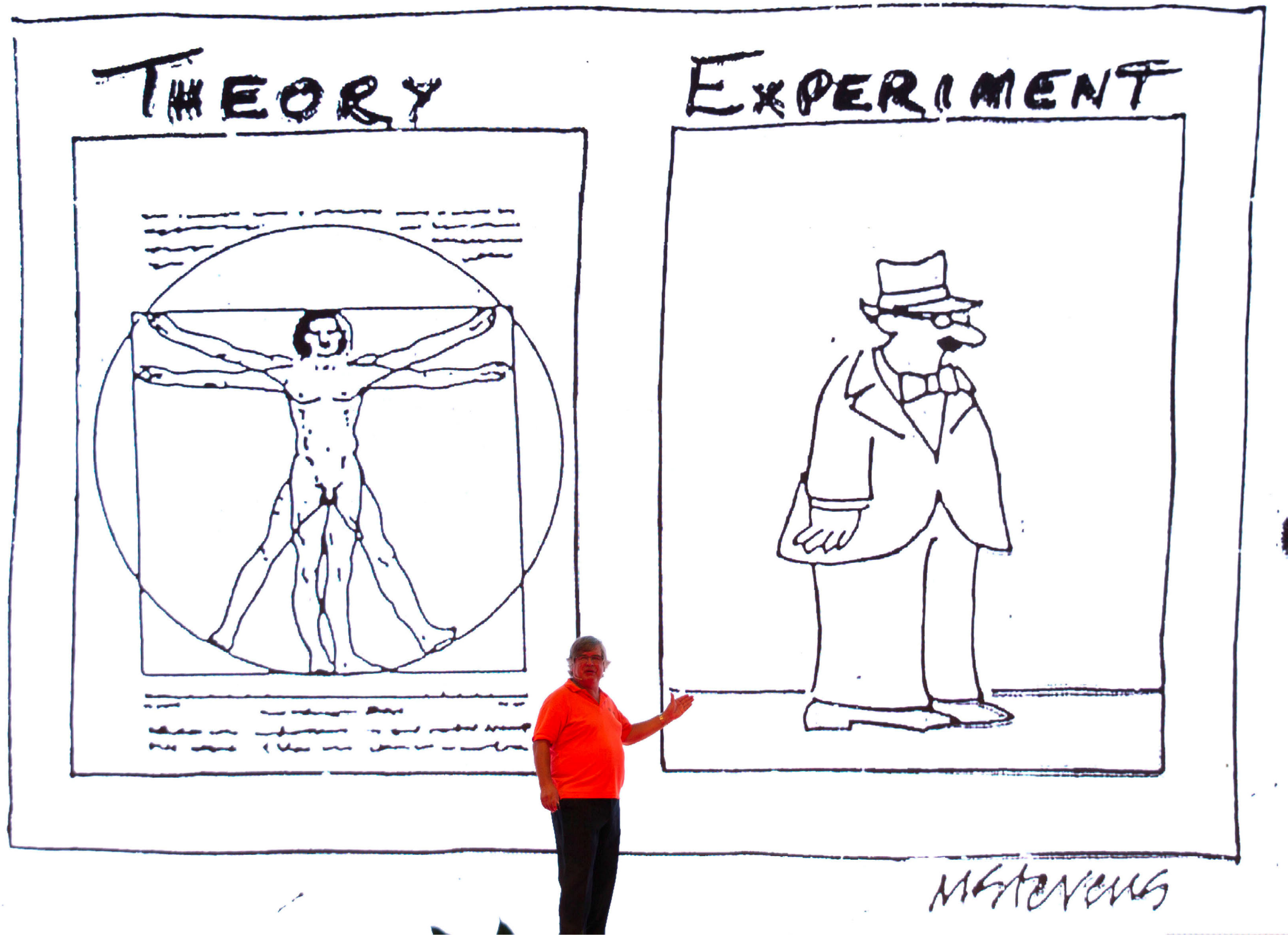
Certificate

Engineering documentation

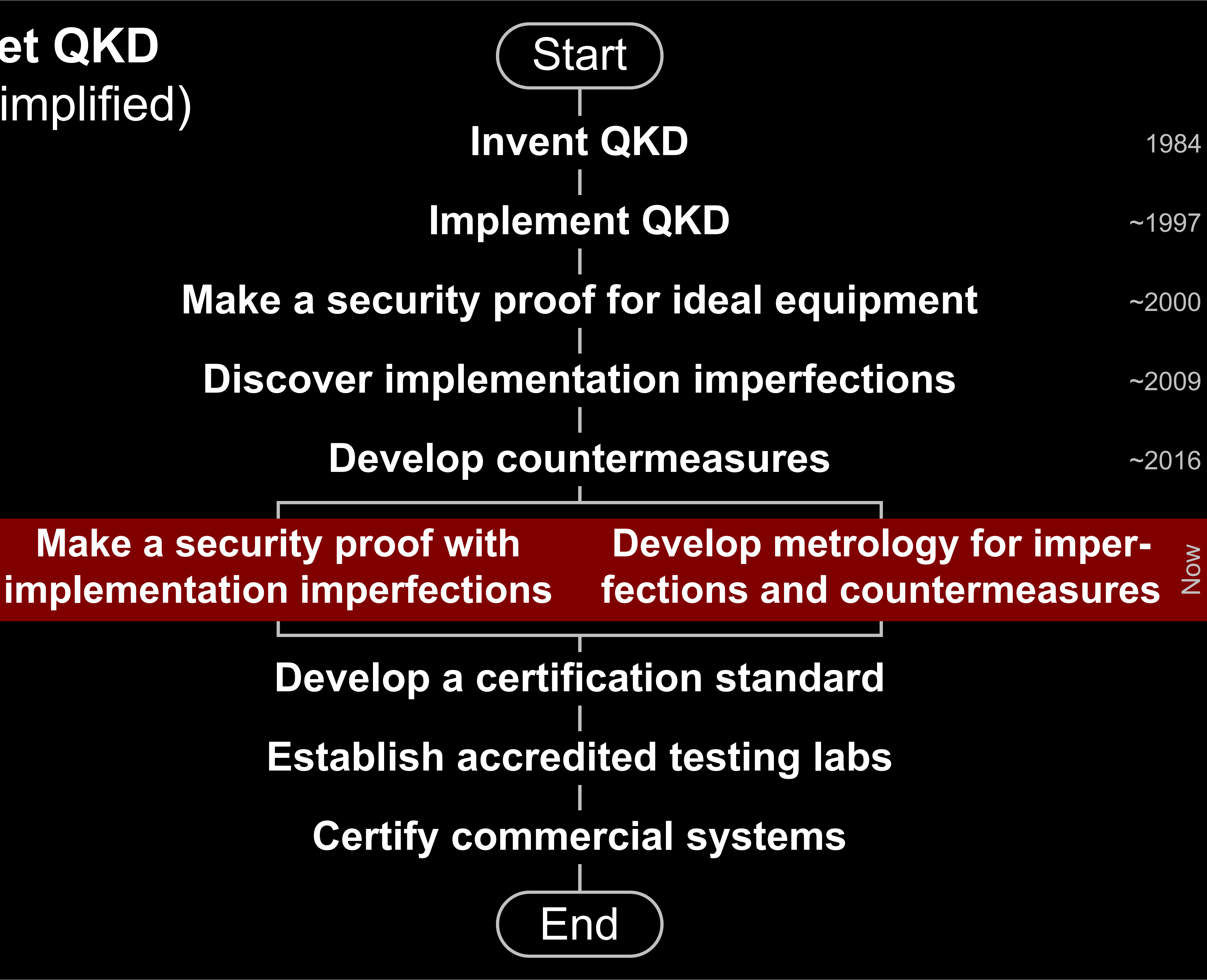
Manufacturer

Sale

Customer


THEORY
EXPERIMENT
MStevens

Get QKD
(simplified)



Start

Invent QKD — 1984

Implement QKD — ~1997

Make a security proof for ideal equipment — ~2000

Discover implementation imperfections — ~2009

Develop countermeasures — ~2016

Make a security proof with implementation imperfections

Develop metrology for imperfections and countermeasures

Now

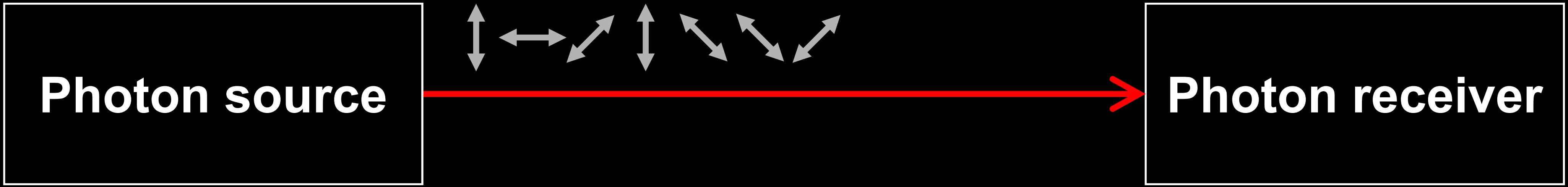
Develop a certification standard

Establish accredited testing labs

Certify commercial systems

End

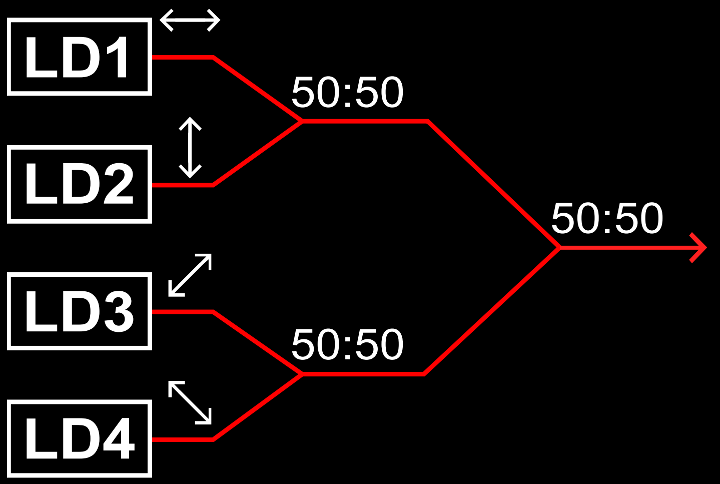
Attack	Target component	Tested system
Distinguishability of decoy states A. Huang *et al.*, Phys. Rev. A **98**, 012330 (2018)	laser in Alice	3 research systems
Intersymbol interference K. Yoshino *et al.*, poster at QCrypt (2016)	intensity modulator in Alice	research system
Laser damage V. Makarov *et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

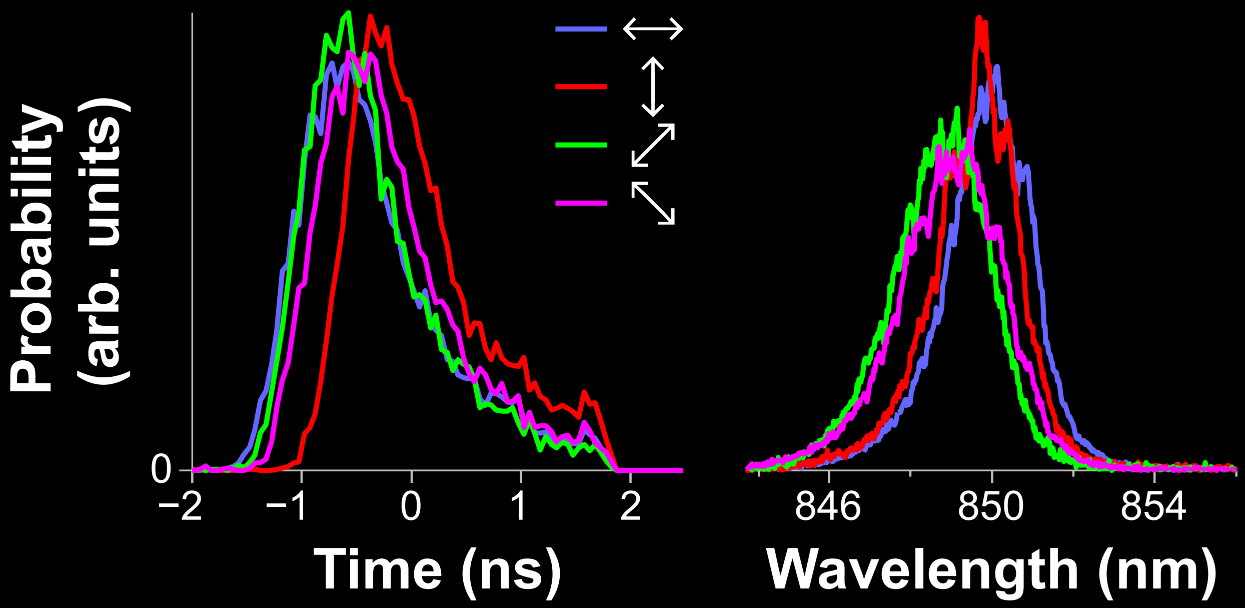


Photon source

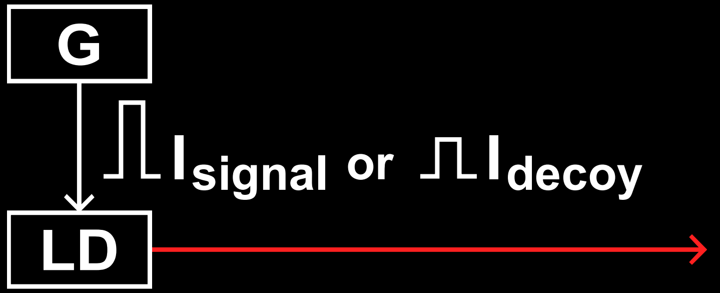
Photon receiver

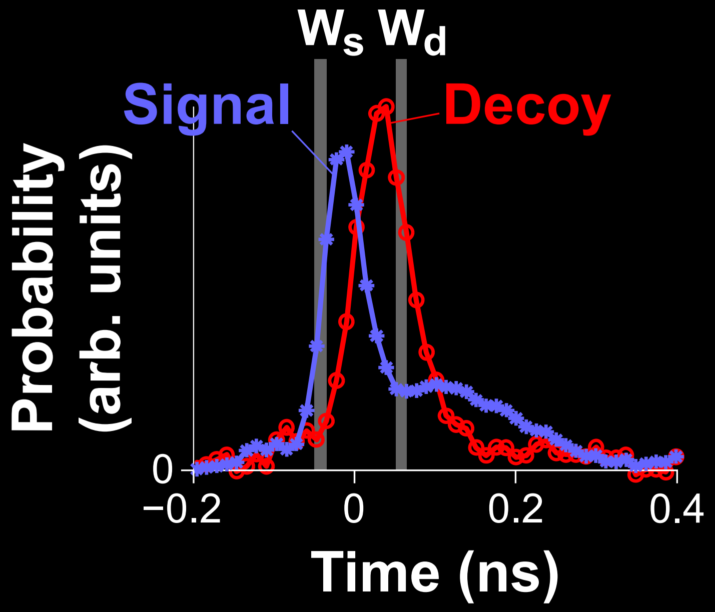
Distinguishability of source states





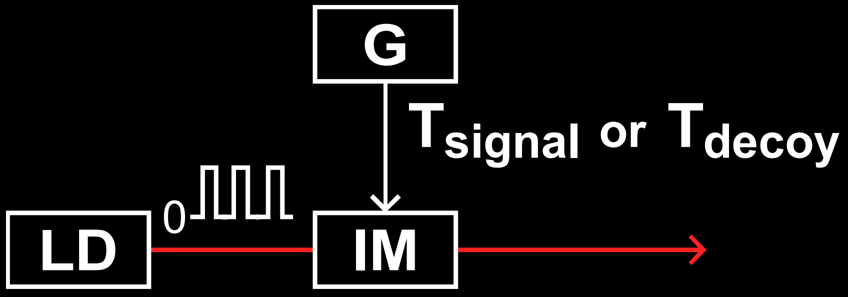
S. Nauerth *et al.*, New J. Phys. **11**, 065001 (2009)

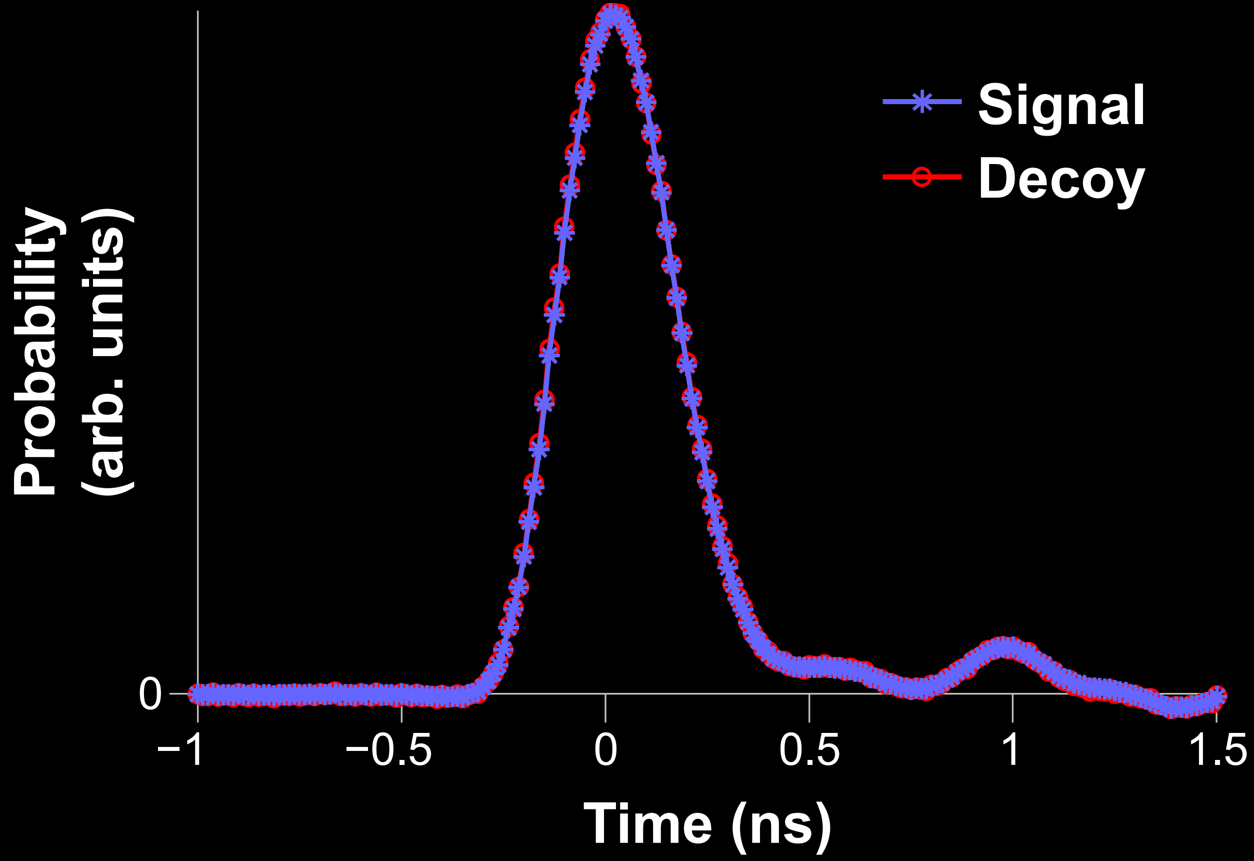




A. Huang, S.-H. Sun, Z. Liu, V. Makarov, Phys. Rev. A **98**, 012330 (2018)

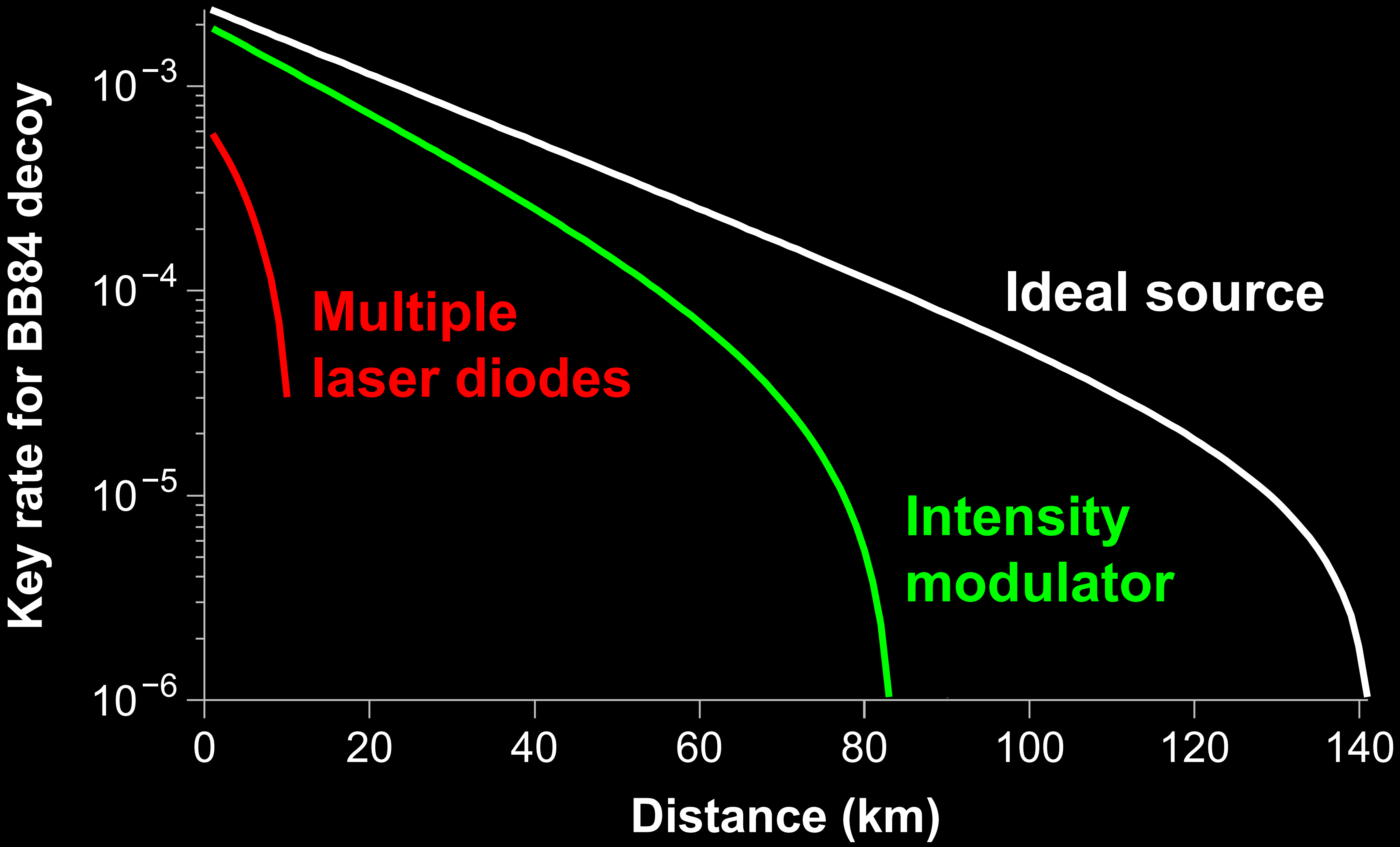
Distinguishability of source states





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)

Security audit	System	Report	Tests
IDQ	Clavis3	2016	–2018 incomplete
国盾量子 QuantumCTek	(undisclosed)	2016	ongoing
ITMO UNIVERSITY (ООО Квантовые коммуникации)	Subcarrier scheme (A. Gleim)	2018	ongoing
QRATE	New 1 GHz system	(2019)	to do

S. Sajeed *et al.*, unpublished

International certification standards are being developed

ETSI

Industry standards
group in QKD

ISO

Example of initial analysis report

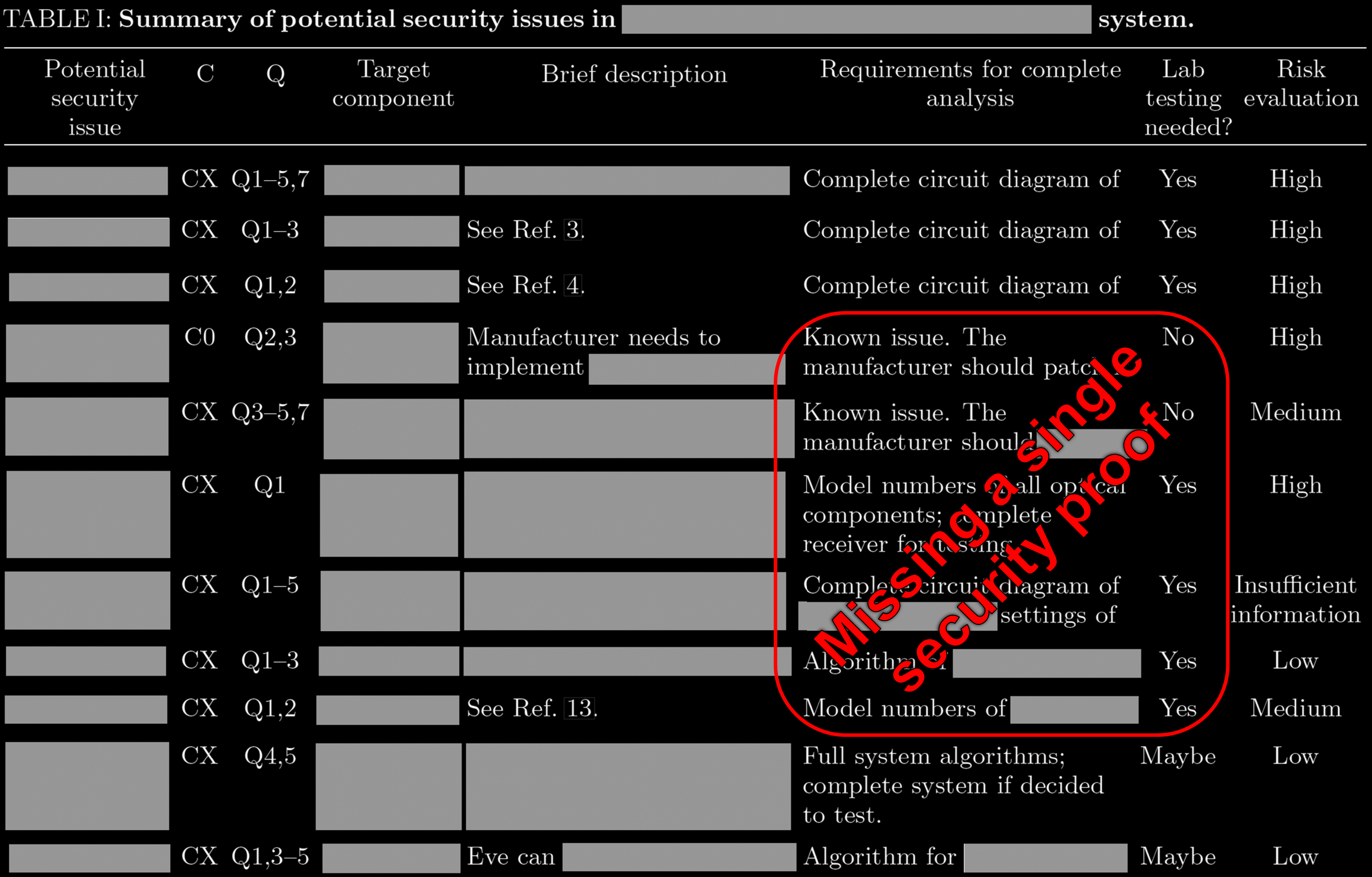
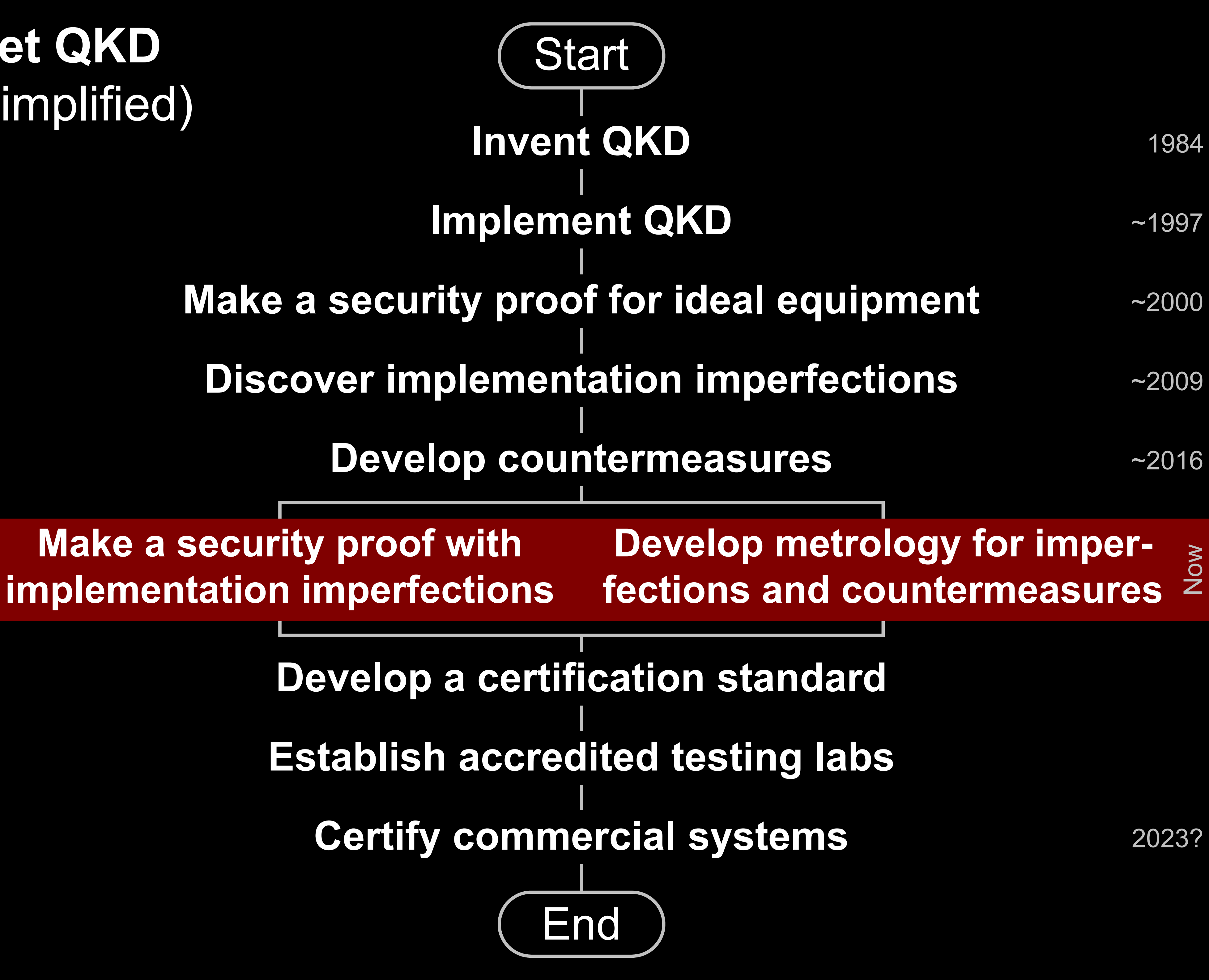


TABLE I: **Summary of potential security issues in [redacted] system.**

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 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

Missing a single security proof

Get QKD
(simplified)



Start

Invent QKD 1984

Implement QKD ~1997

Make a security proof for ideal equipment ~2000

Discover implementation imperfections ~2009

Develop countermeasures ~2016

Make a security proof with implementation imperfections

Develop metrology for imperfections and countermeasures

Now

Develop a certification standard

Establish accredited testing labs

Certify commercial systems 2023?

End

Photo ©2017 Vadim Makarov, Scott McManus / IQC

UNIVERSITY OF WATERLOO

Quantum hacking lab

vad1.com/lab

Photo ©2018 Vadim Makarov

2016

2018

Winter school on quantum cybersecurity

Annual. Next: 25–31 January 2020
Les Diablerets, Switzerland

2 days (executive track) +
4 days (technical track, with 4 labs)

Overview talks + quantum technologies, including QKD

Lecturers in 2019: J. Baloo, C. Bennett, G. Brassard, E. Diamanti, R. Floeter, N. Gisin, J. Hart, B. Huttner, E. Hodges, V. Makarov, M. Mosca, S. Popescu, R. Renner, F. Ruess, G. Ribordy, V. Scarani, D. Stucki, C. Williams

30 students

€3200 / €1600 executive track only

Winter sports in breaks

Organised by IDQ

www.idquantique.com/winter-school-2018

2019

International school on quantum technology

Annual. Next: early March 2020
Roza Khutor, Russia

4 days of lectures and skiing, poster session

Tutorials on quantum sensing, computing, metrology, QKD

Lecturers in 2019: A. Akimov, V. Balykin, M. Chekhova, V. Eliseev, A. Fedyanin, A. Korolkov, L. Krivitsky, V. Makarov, A. Odinokov, O. Snigirev, S. Straupe, A. Urivsky, S. Vyatchanin, F. Zhelezko

100 students

€80 academic / €300 other (TBC)

4 h of pro skiing instruction

Organised by Центр Квантовых Технологий

qutes.org