Improving security of a QKD system via an external audit

Vadim 大胡子

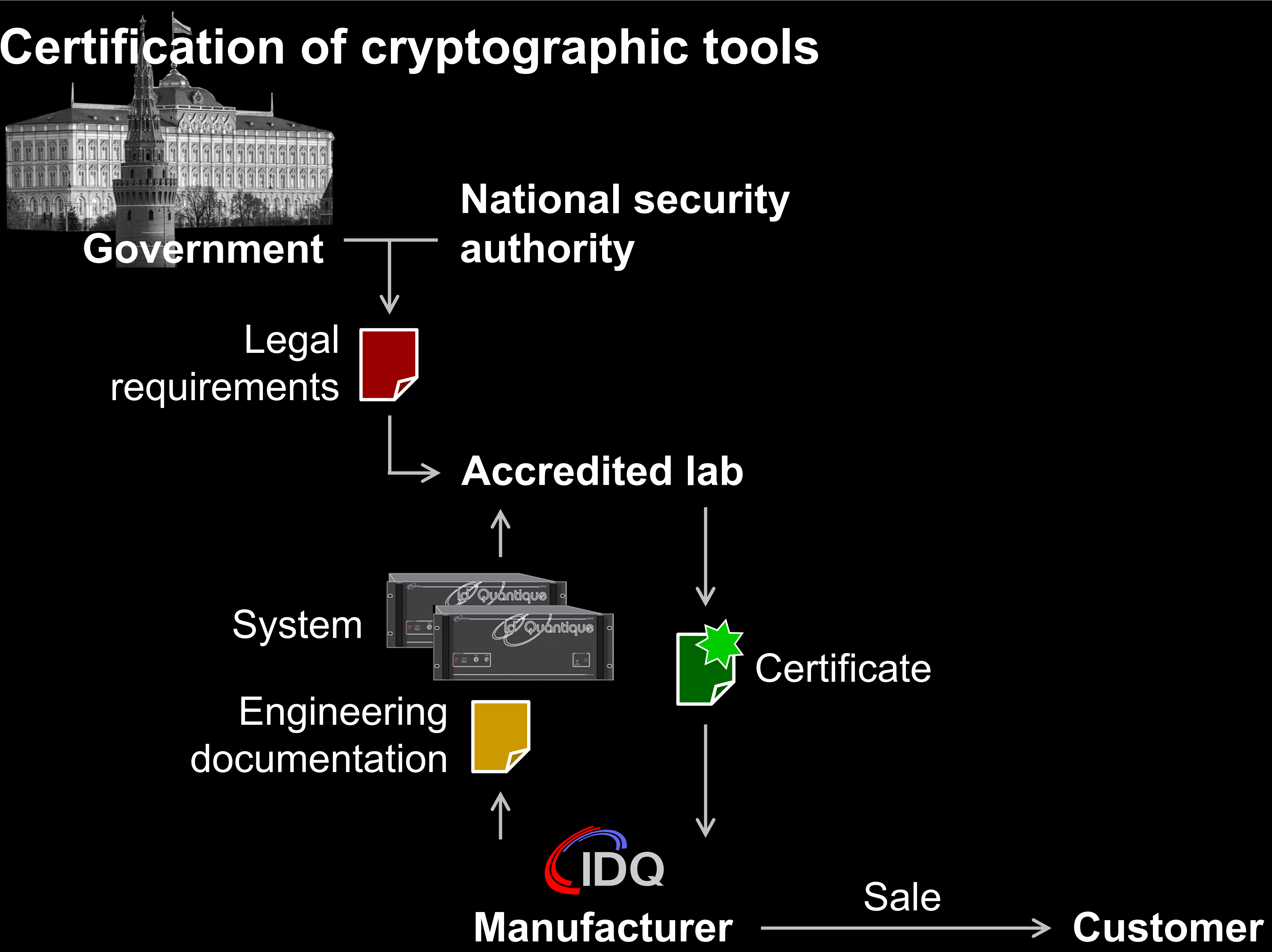
Talk at BQIT online workshop, 27–30 April 2020

Quantum hacking lab

vad1.com/lab

Photo ©2017 Vadim Makarov / ITMO

Certification of cryptographic tools



Government

National security authority

Legal requirements

Accredited lab

System

Engineering documentation

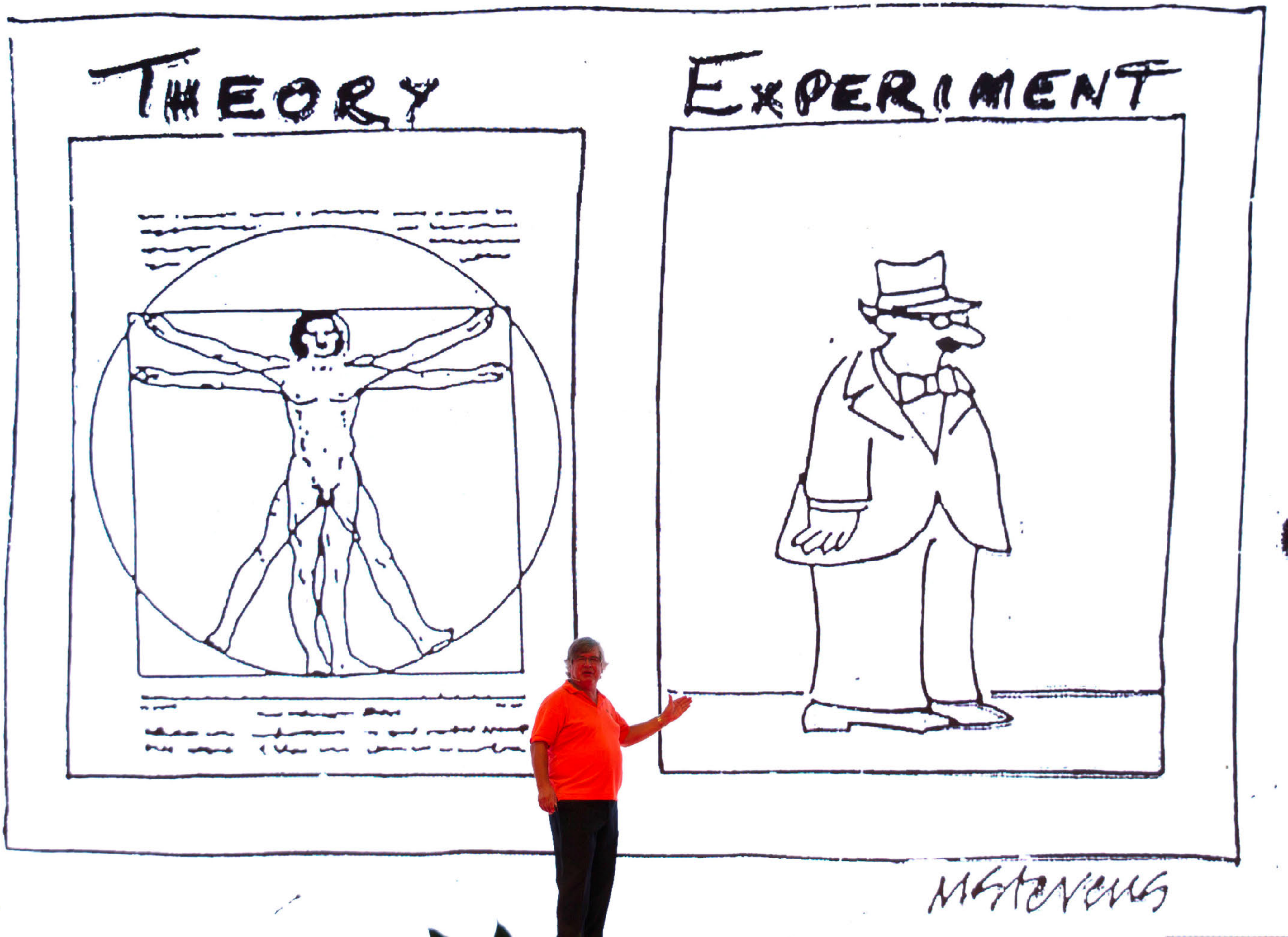
Certificate

IDQ

Manufacturer

Sale

Customer


THEORY
EXPERIMENT
MStevens

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	ongoing
QRATE	New 312.5 MHz system	(2020)	ongoing

S. Sajeed *et al.*, arXiv:1909.07898

Certification standards are being drafted since 2019 in

ETSI Industry standards group in QKD

ISO

Hardness against implementation imperfections

Rating	Description
C3. Solution secure	Imperfection not applicable or in security proof
C2. Solution robust	Protects against known attacks but is not in security proof
C1. Solution only partially effective	Protects adainst one attack but fails to another
C0. Insecure	Loophole confirmed, no countermeasure
CX. Not tested	Loophole suspected

S. Sajeed, P. Chaiwongkhot, A. Huang, H. Qin,
V. Egorov, A. Kozubov, A. Gaidash, V. Chistiakov, A. Vasiliev, A. Gleim, V. Makarov, arXiv:1909.07898

Risk evaluation

Loophole		+	Exploitable with		+	Leaks	
likely	1		today’s	1		major	1
or unlikely	0		or future	0		or minor	0
to exist?			technology?			fraction of key?	

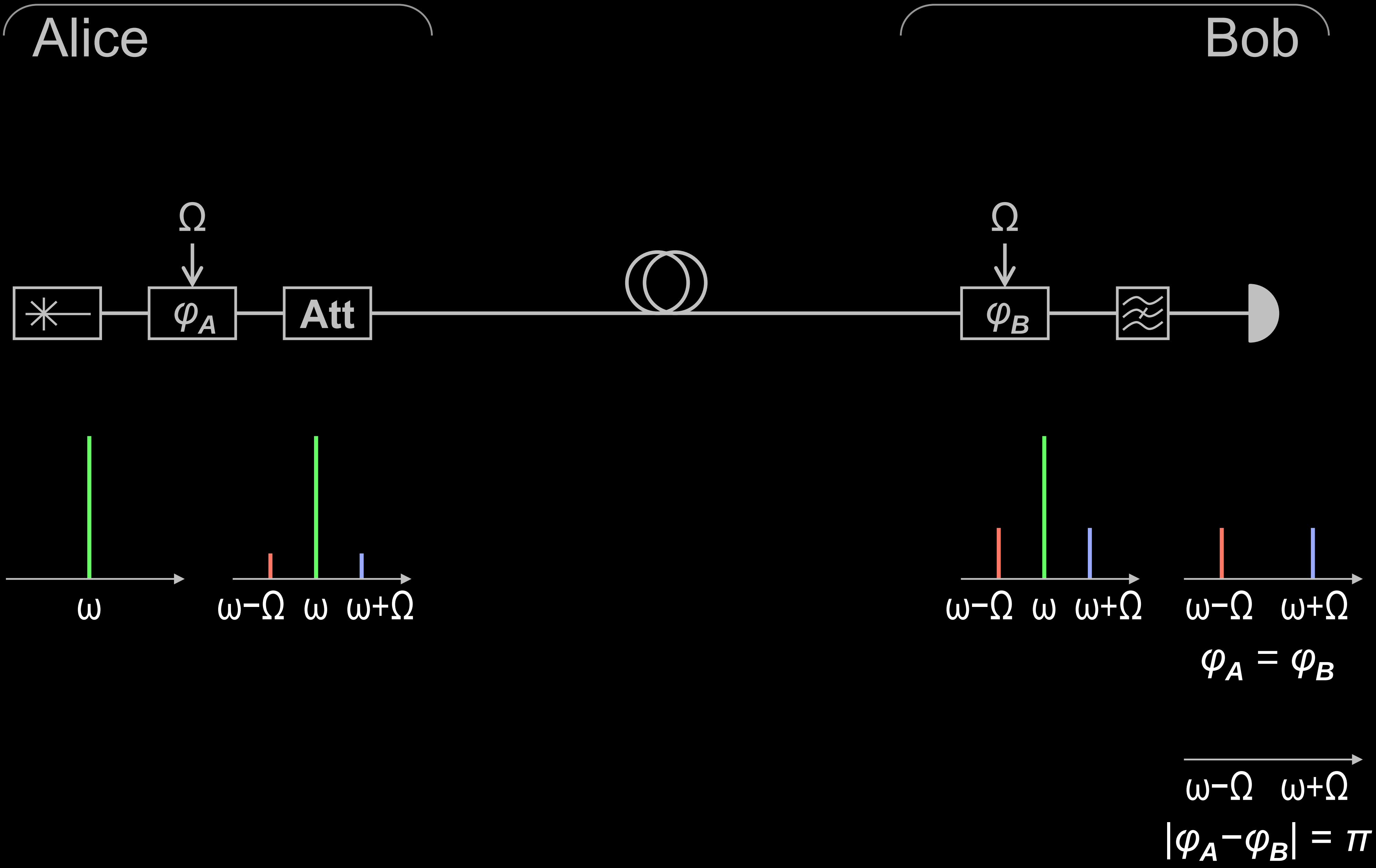
$$= \text{risk} \begin{cases} 3 & \text{Very high} \\ 2 & \text{High} \\ 1 & \text{Medium} \\ 0 & \text{Low} \end{cases}$$

H. Qin, A. Huang, S.-H. Sun, V. Makarov, confidential report for Quantum CTek (2019), unpublished

Potential issue	C_{2017}	Q	Needed lab testing?	Initial risk evaluation	C_{2020}	Status in early 2020
Detector control attack	**CX**	Q1–5,7	Yes	High	**C2**	Loophole experimentally confirmed, countermeasures implemented
Laser damage	**CX**	Q1,3	Yes	High	**C2**	Loophole experimentally confirmed in Alice, countermeasures implemented
Trojan horse	**C2,** **C0**	Q1	Yes	Low (Alice), High (Bob)	**C2,** **C2**	Countermeasure developed, to be implemented
No general security proof	**C0**	Q1,5	No	High	**C3**	Security proofs developed, software updated
Time-shift attack	**CX**	Q1–3,5	Yes	Medium	**CX**	Lower priority, future work
Privacy amplification	**C0**	Q5	No	High	**C3**	Correct processing implemented
Finite-key-size effects	**C0**	Q5	No	Low	**C3**	Security proofs developed, software updated
Non-quantum RNG	**C0**	Q5	No	Low	**C3**	Physical RNG selected, to be implemented
Intersymbol interference	**CX**	Q1–3	Yes	Low	**CX**	Lower priority, future work

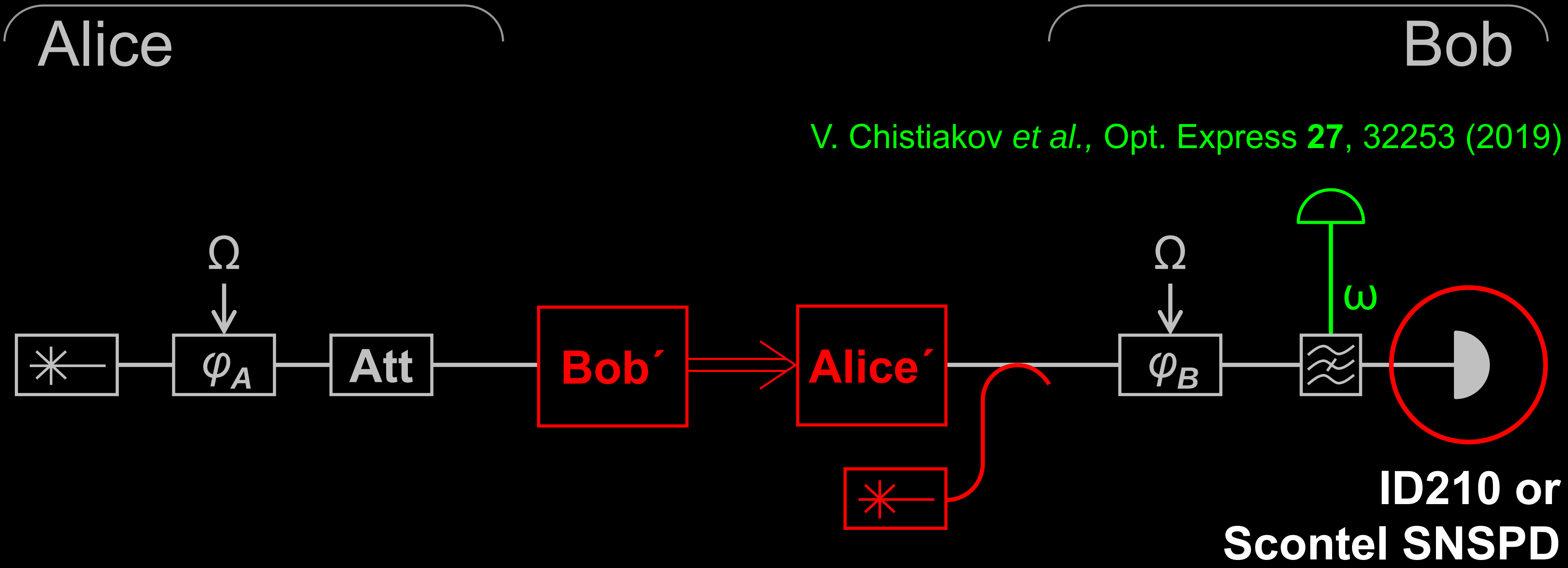
S. Sajeed, P. Chaiwongkhot, A. Huang, H. Qin,
V. Egorov, A. Kozubov, A. Gaidash, V. Chistiakov, A. Vasiliev, A. Gleim, V. Makarov, arXiv:1909.07898

Subcarrier-wave QKD scheme



A. V. Gleim *et al.*, Opt. Express **24**, 2619 (2016)

1. Detector control attack

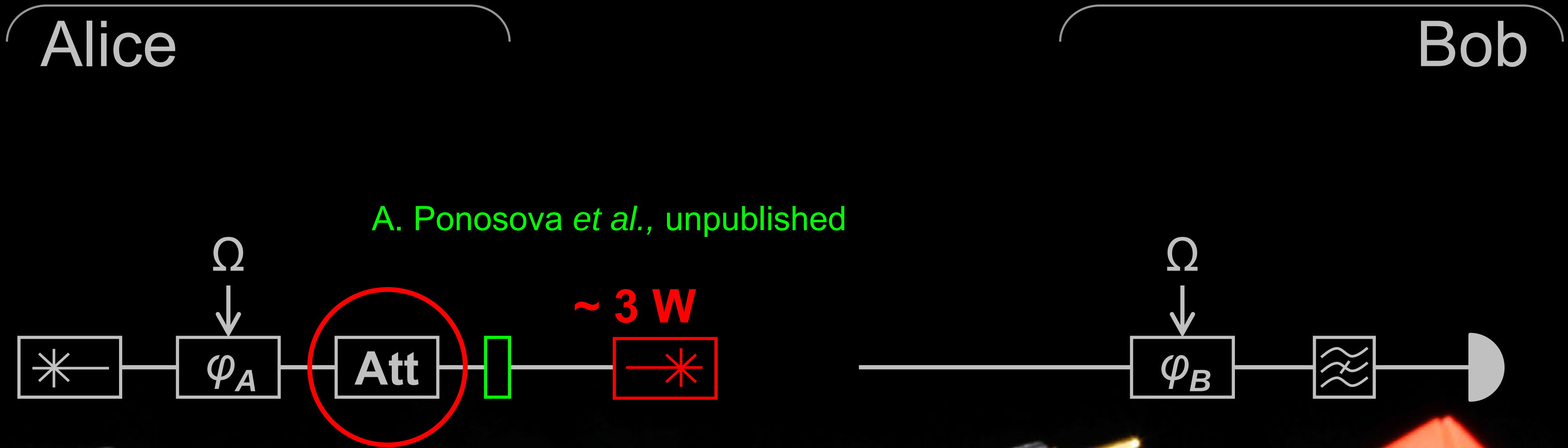


V. Chistiakov *et al.*, Opt. Express **27**, 32253 (2019)

ID210 or Scontel SNSPD

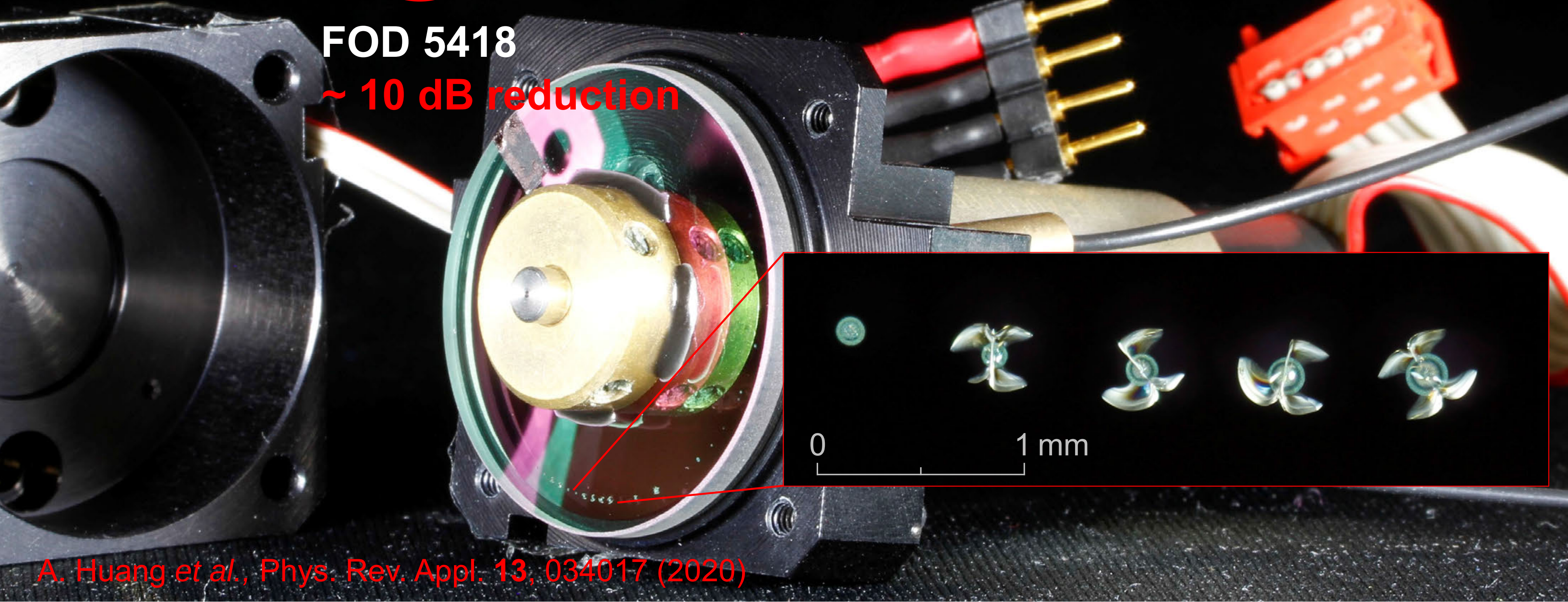
V. Chistiakov *et al.*, Opt. Express **27**, 32253 (2019)
M. Elezov *et al.*, Opt. Express **27**, 30979 (2019)

2. Laser damage



A. Ponosova *et al.*, unpublished

~ 3 W

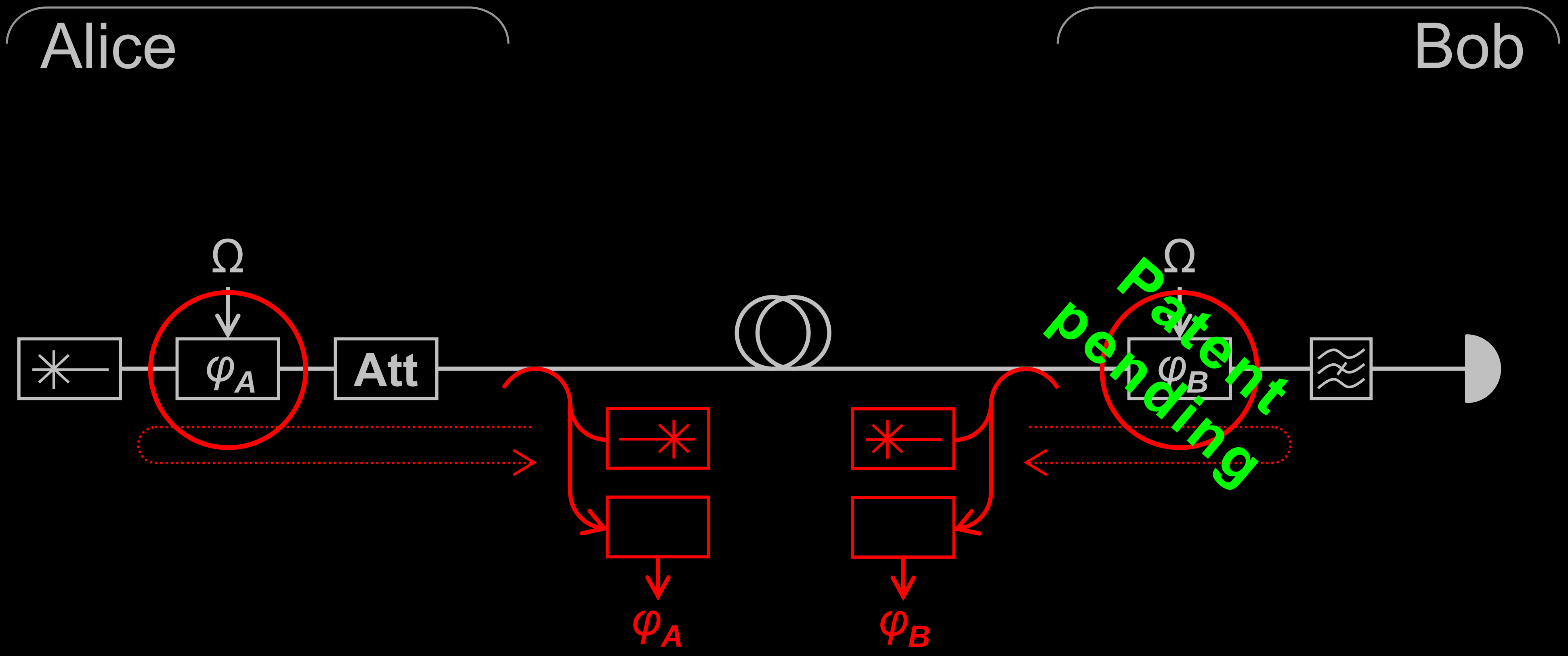


FOD 5418

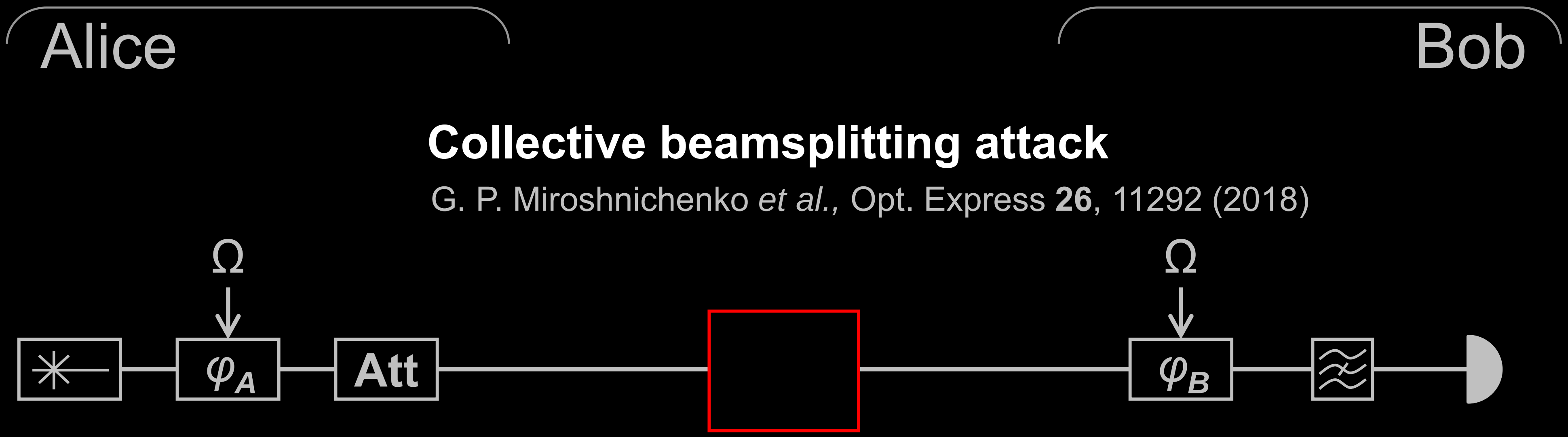
~ 10 dB reduction

A. Huang *et al.*, Phys. Rev. Appl. **13**, 034017 (2020)

3. Trojan horse



4. Lack of general security proof



Collective beamsplitting attack

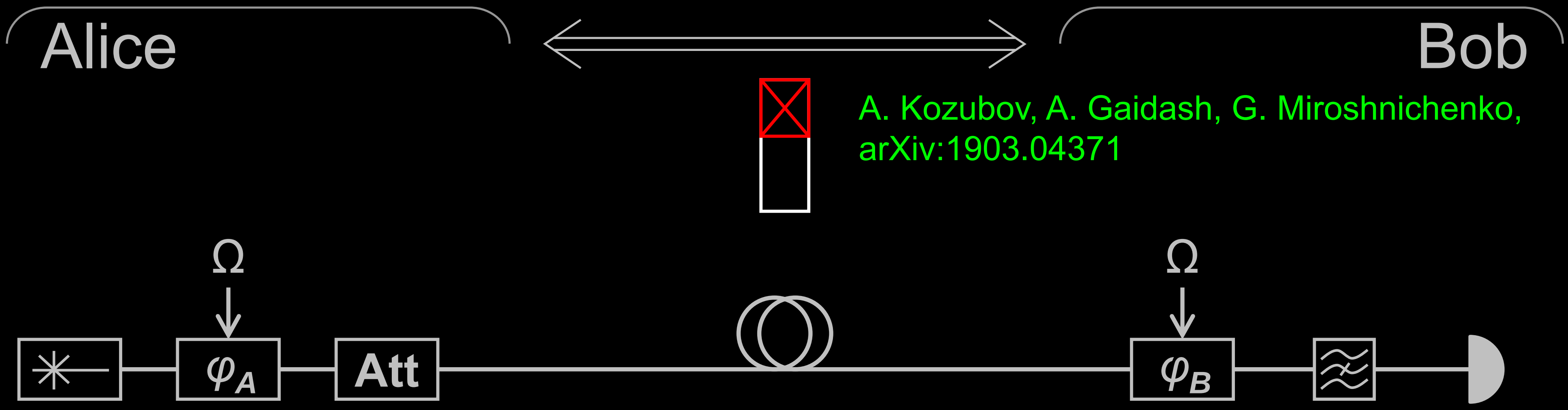
G. P. Miroshnichenko *et al.*, Opt. Express **26**, 11292 (2018)

QND or
manipulating reference ω

General proof

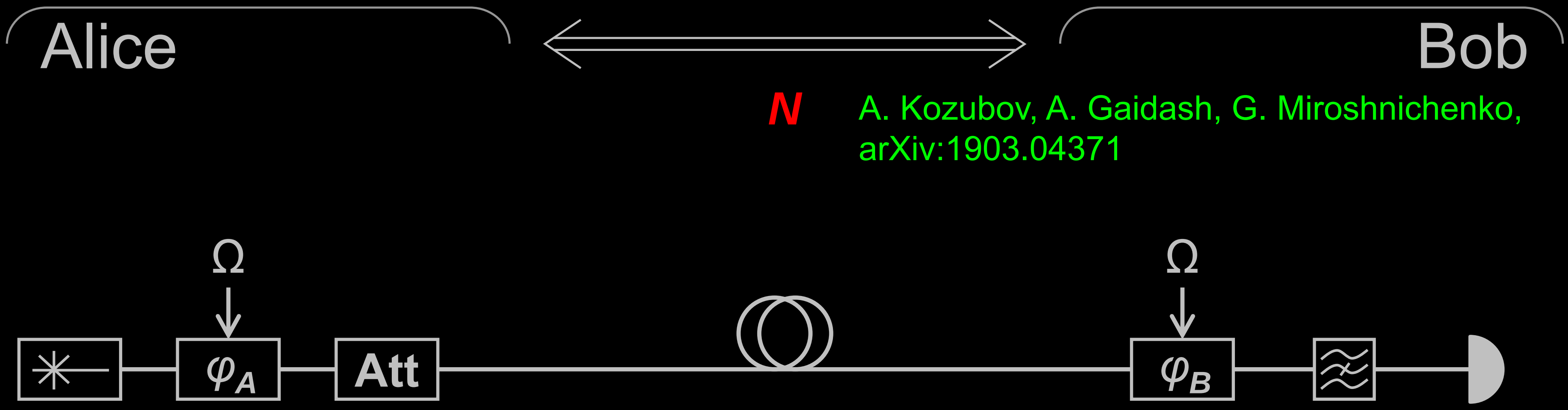
A. Kozubov, A. Gaidash, G. Miroshnichenko, arXiv:1903.04371
A. Gaidash, A. Kozubov, G. Miroshnichenko, J. Opt. Soc. Am. B **36**, B16 (2019)
A. Gaidash, A. Kozubov, G. Miroshnichenko, Physica Scr. (2019)

6. Privacy amplification



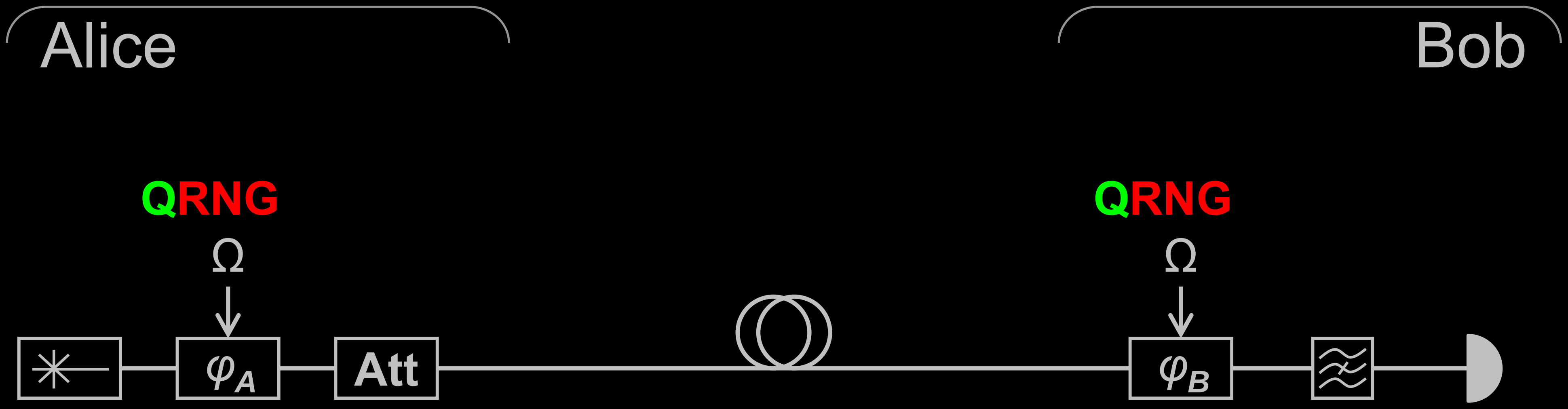
A. Kozubov, A. Gaidash, G. Miroshnichenko,
arXiv:1903.04371

7. Finite-key-size effects



A. Kozubov, A. Gaidash, G. Miroshnichenko, arXiv:1903.04371

8. Non-quantum random number generator



A. Ivanova *et al.*, Nanosyst. Phys. Chem. Math. **8**, 441 (2017)

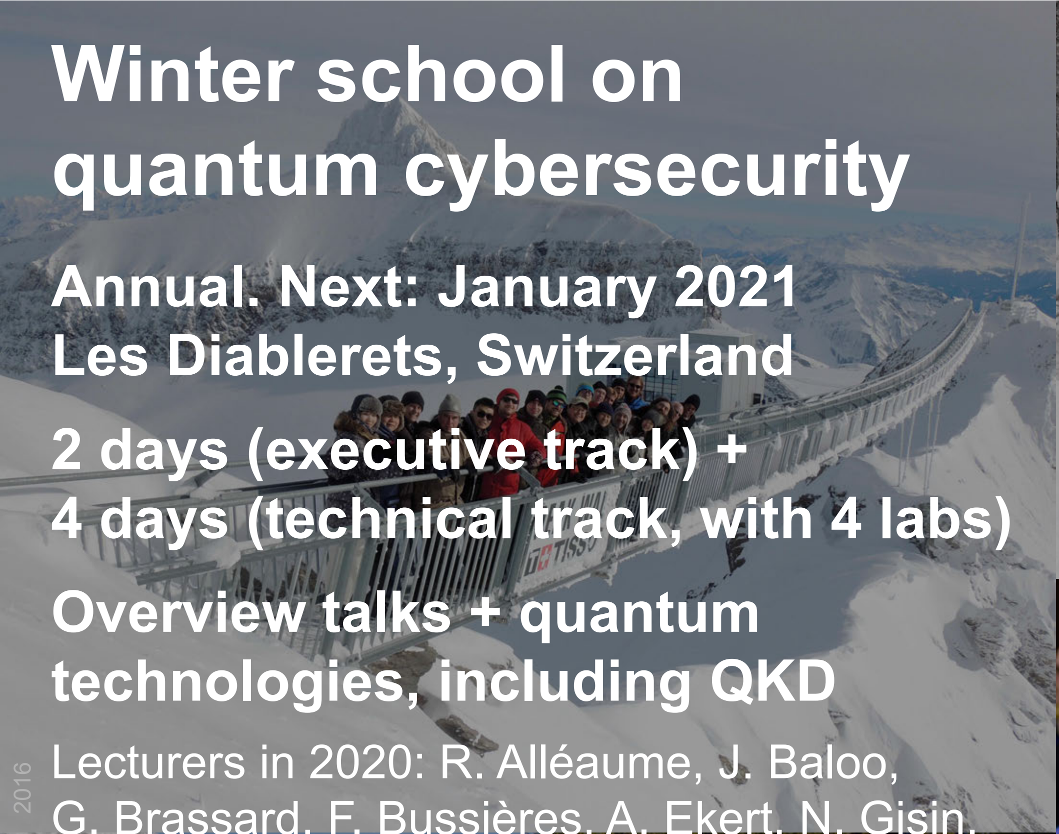
Potential issue	C_{2017}	Q	Needed lab testing?	Initial risk evaluation	C_{2020}	Status in early 2020
Detector control attack	**CX**	Q1–5,7	Yes	High	**C2**	Loophole experimentally confirmed, countermeasures implemented
Laser damage	**CX**	Q1,3	Yes	High	**C2**	Loophole experimentally confirmed in Alice, countermeasures implemented
Trojan horse	**C2,** **C0**	Q1	Yes	Low (Alice), High (Bob)	**C2,** **C2**	Countermeasure developed, to be implemented
No general security proof	**C0**	Q1,5	No	High	**C3**	Security proofs developed, software updated
Time-shift attack	**CX**	Q1–3,5	Yes	Medium	**CX**	Lower priority, future work
Privacy amplification	**C0**	Q5	No	High	**C3**	Correct processing implemented
Finite-key-size effects	**C0**	Q5	No	Low	**C3**	Security proofs developed, software updated
Non-quantum RNG	**C0**	Q5	No	Low	**C3**	Physical RNG selected, to be implemented
Intersymbol interference	**CX**	Q1–3	Yes	Low	**CX**	Lower priority, future work

S. Sajeed, P. Chaiwongkhot, A. Huang, H. Qin,
V. Egorov, A. Kozubov, A. Gaidash, V. Chistiakov, A. Vasiliev, A. Gleim, V. Makarov, arXiv:1909.07898

+ V. Chistiakov, V. Egorov, S. Feng,
A. Gaidash, A. Gleim, S. Kozlov,
A. Kozubov, M. Legre, D. Li,
N. Lütkenhaus, G. Ribordy, S.-H. Sun,
Y. Tang, A. Vasiliev, Y. Zhao

A. Huang S. Sajeed
P. Chaiwongkhot H. Qin

Photo ©2017 Vadim Makarov



Winter school on quantum cybersecurity

Annual. Next: January 2021
Les Diablerets, Switzerland

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

Overview talks + quantum technologies, including QKD

Lecturers in 2020: R. Alléaume, J. Baloo, G. Brassard, F. Bussières, A. Ekert, N. Gisin, V. Makarov, M. Mosca, L. Perret, S. Popescu, R. Pravahan, R. Renner, H. Riel, G. Ribordy, D. Stucki, N. Walenta, E. Wille

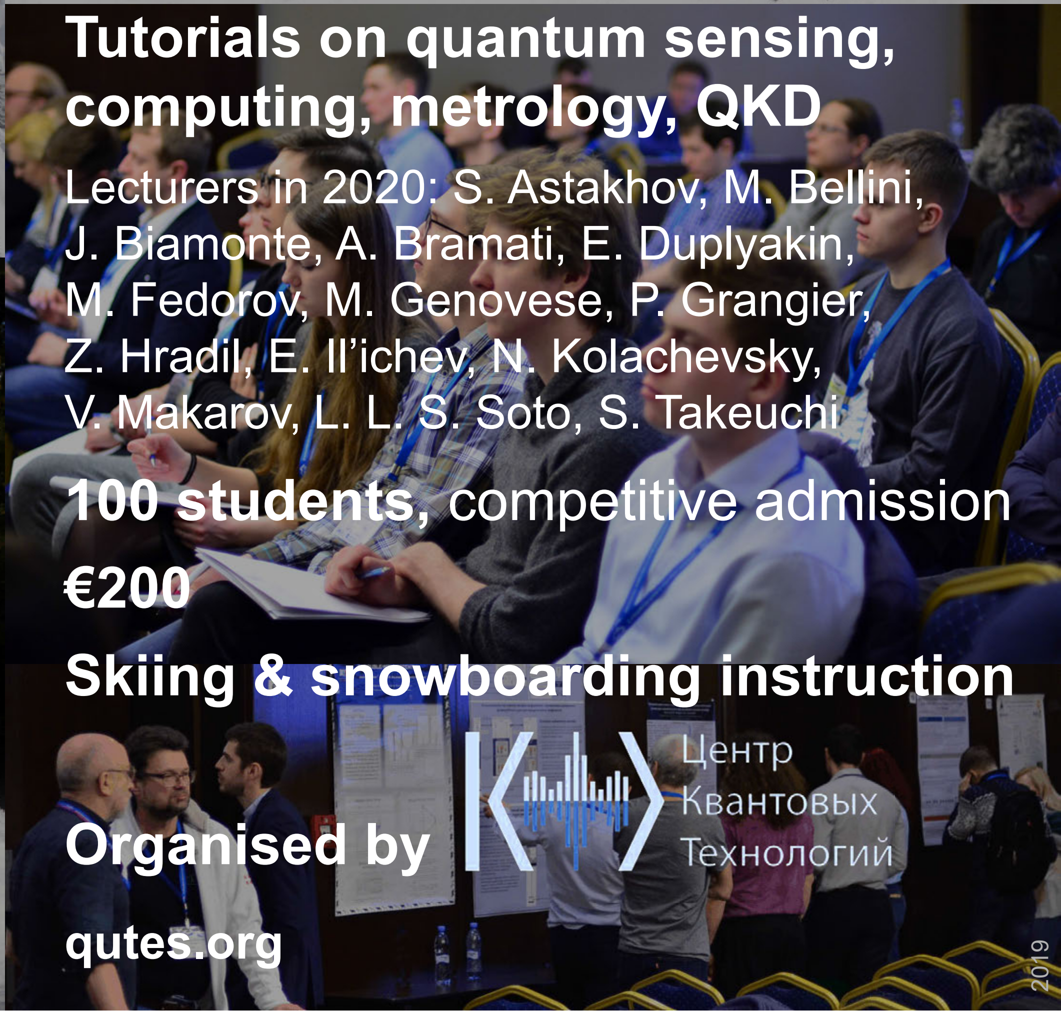
35 students, first-come, sells out

€3200 / €1600 executive track only

Winter sports in breaks

Organised by IDQ

Contact www.idquantique.com for registration



International school on quantum technology

Annual. Next: early March 2021
Roza Khutor, Russia

5 days of lectures and skiing, poster session, industry exhibit

Tutorials on quantum sensing, computing, metrology, QKD

Lecturers in 2020: S. Astakhov, M. Bellini, J. Biamonte, A. Bramati, E. Duplyakin, M. Fedorov, M. Genovese, P. Grangier, Z. Hradil, E. Il'ichev, N. Kolachevsky, V. Makarov, L. L. S. Soto, S. Takeuchi

100 students, competitive admission

€200

Skiing & snowboarding instruction

Organised by Центр Квантовых Технологий

qutes.org