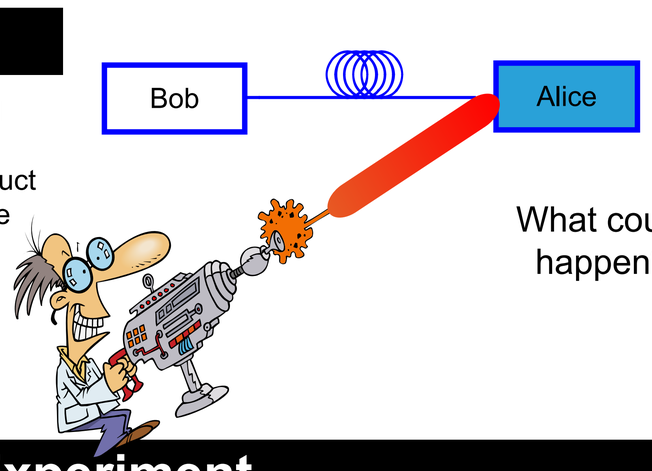
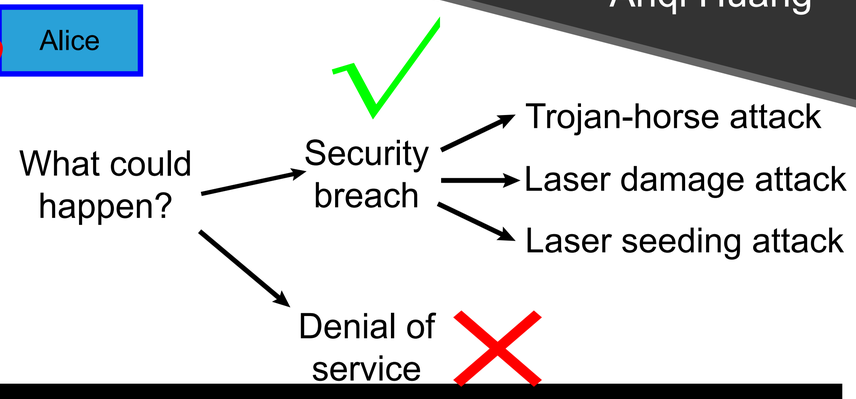
Protecting QKD sources against light-injection attacks

Daria Ruzhitskaya [*,1,2]
Anastasiya Ponosova [1,2]
Friederike Jöhlinger [3,4]
Poompong Chaiwongkhot [5,6]
Vladimir Egorov [7]
Djeylan Aktas [3]
John Rarity [3]
Chris Erven [3,8]
Vadim Makarov [1,2,9]
Anqi Huang [10]

Introduction

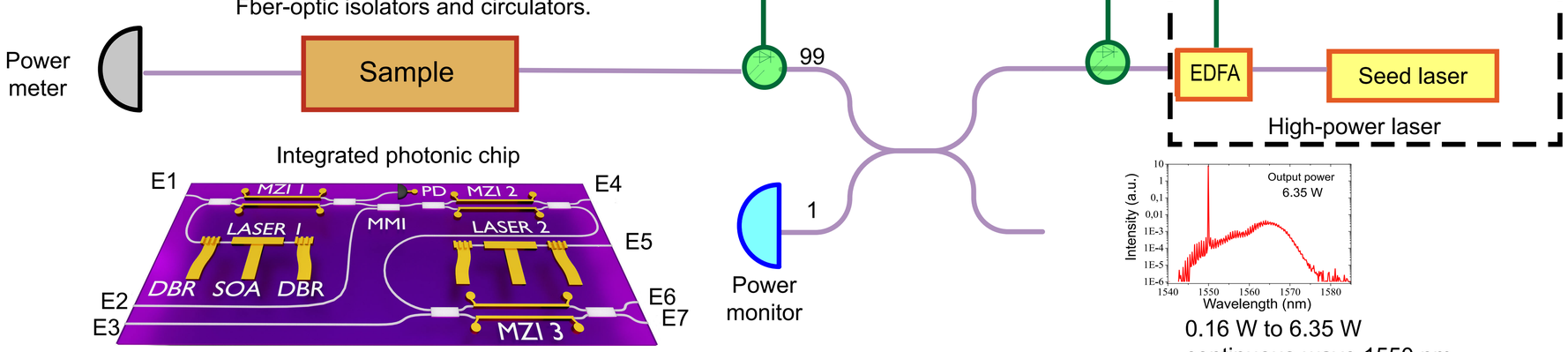
In the age of measurement-device-independent quantum key distribution (MDI QKD) and twin-field QKD (TF QKD), the source units of these QKD schemes may become a new “Achilles' heel” of the whole system because an adversary, Eve, can inject lasers to conduct various attacks on the sources, i.e., the laser damage attack, Trojan-horse attack, and the laser seeding attack [1-6]. To protect laser injection attacks, we investigate the effectiveness of several possible countermeasures, which includes isolators, circulators and integrated components in the chip.





Experiment

Fber-optic isolators and circulators.



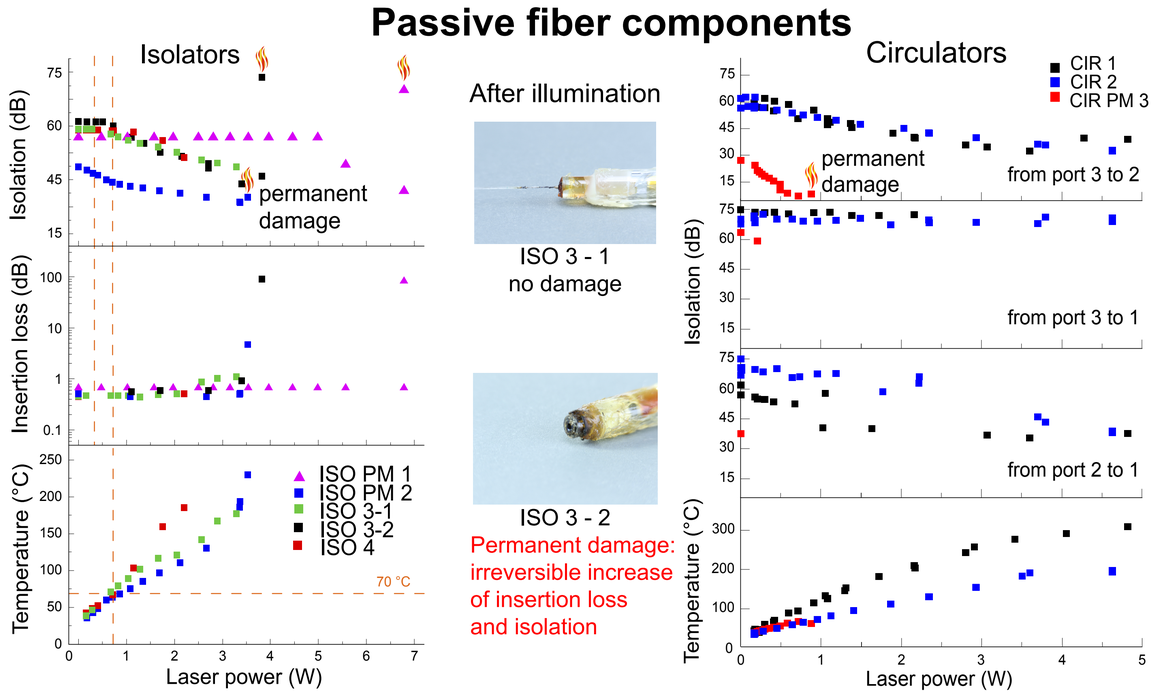
0.16 W to 6.35 W continuous-wave 1550 nm SMF-28

Chip details in: *P. Sibson, C. Erven, M. Godfrey, S. Miki, T. Yamashita, M. Fujiwara, M. Sasaki, H. Terai, M. G. Tanner, C. M. Natarajan, R. H. Hadfield, J. L. O'Brien, M. G. Thompson.,* Chip-based quantum key distribution., *Nat. Commun. 13984 (2017)*

Details of testing setup: *A. Huang, R. Li, V. Egorov, S. Tchouragoulov, K. Kumar, V. Makarov.* Laser damage attack against optical attenuators in quantum key distribution., Phys.., Rev. 8Appl. 13, 034017 (2020).

Results

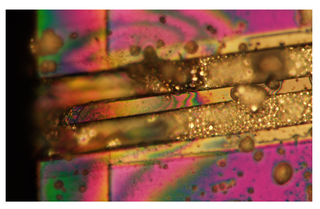
Passive fiber components



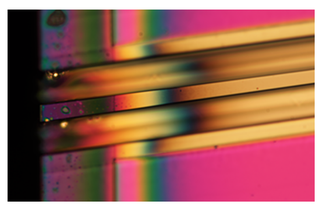
Testing outcomes	Polarization sensitivity	Samples	Minimum isolation, dB	Maximum decrease of isolation, dB
Isolators	sensitive	2	21.8	31.9
	insensitive	3	27.6	34.5
Circulators	sensitive	1	6.4	20.6
	insensitive	2	32	33.7

InP QKD transmitter chip

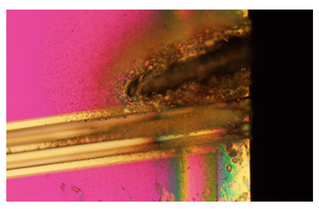
Destroyed coupling ports under test



SSC E1, P_{HPL} = 2.0 W



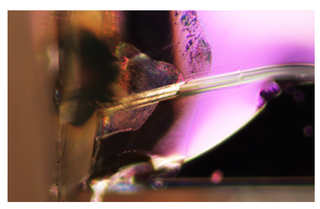
SSC E2
no damage



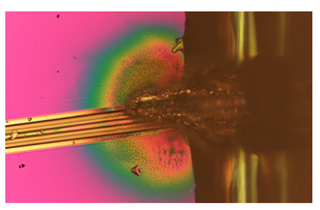
SSC E4, P_{HPL} = 2.5 W

Glued pigtails

SSC E1, P_{HPL} = 5.2 W (max)



SSC E3, P_{HPL} = 1.6 W



SSC E4, P_{HPL} = 5.2 W

Conclusion

The experimental results show that the tested components may be a good passive countermeasure against all the known attacks that rely on light injection into the QKD source (laser-damage, Trojan-horse, and laser-seeding). However, we caution that these good candidates should be further tested in a pulsed regime and at different wavelengths, to ensure their reliability as the protection. The possibility for Eve to affect the internal components in the photonics chip in these other regimes should also be checked.

References

[1] *N. Jain, E. Anisimova, I. Khan, V. Makarov, C. Marquardt, G. Leuchs*, New J. Phys. 16, 123030 (2014).
[2] *S.-H. Sun, F. Xu, M.-S. Jiang, X.-C. Ma, H.-K. Lo, L.-M. Liang*, Phys. Rev. A 92, 022304 (2015).
[3] *V. Makarov, J.-P.Bourgoin, P. Chaiwongkhot, M. Gagné T. Jennewein, S. Kaiser, R. Kashyap, M.Legré, C. Minshull, S. Sajeed*, Phys. Rev. A 94, 030302 (2016).
[4] *A. Huang, R. Li, V. Egorov, S. Tchouragoulov, K. Kumar, V. Makarov*, Phys. Rev. Appl. 13, 034017 (2020).
[5] *A. Huang, Á. Navarrete, S.-H. Sun, P. Chaiwongkhot, M. Curty, V. Makarov*, Phys. Rev. Appl. 12, 064043 (2019).
[6] *X.-L. Pang, A.-L. Yang, C.-N. Zhang, J.-P. Dou, H. Li, J. Gao, X.-M. Jin*, Phys. Rev. Appl. 13, 034008 (2020).

* dariaruzh@yandex.ru

[1] Russian Quantum Center, Skolkovo, Moscow, Russia
NTI Center for Quantum Communications, National University of Science and Technology MISiS, Moscow, Russia
[2] Quantum Engineering Technology Labs, H. H. Wills Physics Laboratory & Department of Electrical and Electronic Engineering, University of Bristol, Bristol, United Kingdom
[4] Quantum Engineering Centre for Doctoral Training, H. H. Wills Physics Laboratory and Department of Electrical and Electronic Engineering, University of Bristol, Bristol, United Kingdom
[5] Institute for Quantum Computing, University of Waterloo, Waterloo, ON, N2L 3G1 Canada
[6] Department of Physics and Astronomy, University of Waterloo, Waterloo, ON, N2L 3G1 Canada
Faculty of Photonics and Optical Information, ITMO University, Kadetskaya line 3b, 199034 St. Petersburg, Russia
[8] KETS Quantum Security Ltd, Unit DX, Bristol, United Kingdom
[9] Shanghai Branch, National Laboratory for Physical Sciences at Microscale and CAS Center for Excellence in Quantum Information, University of Science and Technology of China, Shanghai, People's Republic of China
[10] Institute for Quantum Information & State Key Laboratory of High Performance Computing, College of Computer, National University of Defense Technology, Changsha, People's Republic of China

Presented at online QCrypt 2020, August 10 – 14