IOP Publishing | Astro Ltd
Laser Physics Letters
Laser Phys. Lett. **16** (2019) 019401 (2pp)
https://doi.org/10.1088/1612-202X/aaf22d

Addendum

Comment on 'Inherent security of phase coding quantum key distribution systems against detector blinding attacks' (2018 *Laser Phys. Lett.* 15 095203)

Aleksey Fedorov[1,2,3], Ilja Gerhardt[4,5], Anqi Huang[6], Jonathan Jogenfors[7], Yury Kurochkin[1,2], Antía Lamas-Linares[8], Jan-Åke Larsson[7], Gerd Leuchs[9], Lars Lydersen[10], Vadim Makarov[1,11] and Johannes Skaar[12]

[1] Russian Quantum Center, Skolkovo, Moscow 143025, Russia
[2] QRate, Skolkovo, Moscow 143025, Russia
[3] QApp, Skolkovo, Moscow 143025, Russia
[4] Institute of Physics, University of Stuttgart and Institute for Quantum Science and Technology, Pfaffenwaldring 57, D-70569 Stuttgart, Germany
[5] Max Planck Institute for Solid State Research, Heisenbergstraße 1, D-70569 Stuttgart, Germany
[6] Institute for Quantum Information & State Key Laboratory of High Performance Computing, College of Computer, National University of Defense Technology, Changsha 410073, People's Republic of China
[7] Department of Electrical Engineering, Linköping University, SE-58183 Linköping, Sweden
[8] Texas Advanced Computing Center, The University of Texas at Austin, Austin, Texas, United States of America
[9] Max Planck Institute for the Science of Light and University of Erlangen-Nürnberg, D-91058 Erlangen, Germany
[10] Kringsjåvegen 3E, NO-7032 Trondheim, Norway
[11] National University of Science and Technology MISIS, Moscow 119049, Russia
[12] Department of Technology Systems, University of Oslo, Box 70, NO-2027 Kjeller, Norway

E-mail: makarov@vad1.com

Received 11 September 2018
Accepted for publication 6 November 2018
Published 14 December 2018

In [1], Balygin and his coworkers consider a faked-state attack with detector blinding on Bennett–Brassard 1984 (BB84) quantum key distribution (QKD) protocol. They propose a countermeasure to this attack in a phase-coded system that watches for an abnormally low number of detections in the outer time slots 1 and 3. If the eavesdropper does not pay attention to the outer time slots, the countermeasure will reveal that the attack is being performed (see sections 6, 7 and figure 1(b) in [1]). This approach is conceptually similar to earlier work on non-blinding attacks [2].

However, in the faked-state attack [3] the eavesdropper Eve uses a replica of Bob's setup to detect all quantum states emitted by Alice, then induces her exact detection results in Bob's apparatus. Since Eve is using a replica of Bob's setup, she would register detections in the outer time slots, then induce the same detection results in Bob's apparatus by resending additional bright light pulses centered in the time slots 1 and/or 3. Note that Eve will occasionally register a double click, i.e. simultaneous detection events in both her detectors caused by dark counts or multiphoton pulses from Alice. She may

 © 2018 Astro Ltd Printed in the UK

also in some implementations register multiple clicks in adjacent time slots. She might induce such multiple clicks in Bob using faked states similar to those constructed for distributed-phase-reference protocols [4]. I.e. Eve might even replicate imperfections such as double clicks and dark counts that would exist in Bob's equipment. *This would mean that Bob's detection events are exactly the events measured by a copy of Bob's setup (conditioned on Bob's basis choice), and are therefore indistinguishable from the detection events without the attack. The statistics of these detections at Bob would thus be indistinguishable from the statistics without the attack, and the countermeasure is ineffective.*

Although the search for technical countermeasures against the attacks on detectors continues [5–9], so far the only practical scheme proven to be immune against these attacks is measurement-device-independent QKD [10, 11].

We finally make a minor remark that [1] uses a simplified model of the blinded detector with a single threshold P_{th} at which it begins to make clicks with a non-zero probability. In actuality, the click probability increases gradually at powers higher than that, and there is another threshold $P_{\mathrm{always}} > P_{\mathrm{th}}$ at which it becomes unity [5, 12]. Although this detail is inconsequential for the argument presented in [1], it will have to be heeded when constructing the actual attack.

References

[1] Balygin K A, Klimov A N, Bobrov I B, Kravtsov K S, Kulik S P and Molotkov S N 2018 *Laser Phys. Lett.* **15** 095203

[2] Ferreira da Silva T, Xavier G B, Temporaõ G P and von der Weid J P 2012 *Opt. Express* **20** 18911

[3] Makarov V and Hjelme D R 2005 *J. Mod. Opt.* **52** 691

[4] Lydersen L, Skaar J and Makarov V 2011 *J. Mod. Opt.* **58** 680

[5] Huang A, Sajeed S, Chaiwongkhot P, Soucarros M, Legrè M and Makarov V 2016 *IEEE J. Quantum Electron.* **52** 8000211

[6] Sajeed S, Huang A, Sun S, Xu F, Makarov V and Curty M 2016 *Phys. Rev. Lett.* **117** 250505

[7] Marøy Ø, Makarov V and Skaar J 2017 *Quantum Sci. Technol.* **2** 044013

[8] Koehler-Sidki A, Dynes J F, Lucamarini M, Roberts G L, Sharpe A W, Yuan Z L and Shields A J 2018 *Phys. Rev. Appl.* **9** 044027

[9] Koehler-Sidki A, Lucamarini M, Dynes J F, Roberts G L, Sharpe A W, Yuan Z and Shields A J 2018 *Phys. Rev.* A **98** 022327

[10] Lo H-K, Curty M and Qi B 2012 *Phys. Rev. Lett.* **108** 130503

[11] Tang Y-L *et al* 2016 *Phys. Rev.* X **6** 011024

[12] Lydersen L, Wiechers C, Wittmann C, Elser D, Skaar J and Makarov V 2010 *Nat. Photon.* **4** 686