Laser Physics Letters

Astro Ltd.

ADDENDUM

Response to Comment on ‘Inherent security of phase coding quantum key distribution systems against detector blinding attacks’

To cite this article: K A Balygin *et al* 2019 *Laser Phys. Lett.* **16** 019402

IOP Publishing | Astro Ltd
Laser Physics Letters
Laser Phys. Lett. **16** (2019) 019402 (2pp)
https://doi.org/10.1088/1612-202X/aaf22c

Addendum

Response to Comment on 'Inherent security of phase coding quantum key distribution systems against detector blinding attacks'

K A Balygin[1,3], A N Klimov[1,2,3], I B Bobrov[1,3], K S Kravtsov[1,2,3], S P Kulik[1,3] and S N Molotkov[3,4,5,6]

[1] Faculty of Physics, Moscow State University, Moscow, 119991, Russia
[2] Prokhorov General Physics Institute, Russian Academy of Sciences, Moscow, 119991, Russia
[3] Quantum Technology Centre of Moscow State University, Moscow, 119991, Russia
[4] Academy of Cryptography of the Russian Federation, Moscow, 121552, Russia
[5] Institute of Solid State Physics, Russian Academy of Sciences, Chernogolovka, Moscow region, 142432, Russia
[6] Faculty of Computational Mathematics and Cybernetics, Moscow State University, Moscow, 119991, Russia

E-mail: sergei.molotkov@gmail.com

Received 29 October 2018
Accepted for publication 6 November 2018
Published 14 December 2018

In the received comment [1] to our paper [2] the authors expressed doubts about the results we presented, in particular, they claim that an attacker can completely emulate the normal operation of Bob's system using fake pulses even in the case of phase coding systems. This claim is ill-founded due to the presence of a delay interferometer in Bob's system: any transmitted fake pulse will be split into two in the adjacent time slots and will produce either two 'detector clicks' or none. Moreover, preservation of detection statistics in the outer time slots in our understanding means not only leaving the probabilities themselves untouched, but also keeping the conditional probabilities of having the outer detector pulse given there is a detection in the central time window. As a result, due to the complexity of the system as well as the ability of legitimate users to monitor various statistics, including the conditional probabilities, the vague description given by the authors cannot be considered as a specific attack.

Cryptography, including quantum cryptography, is an exact science. Therefore, any quantum cryptography protocol, as well as an attack on it, must be clearly and concisely presented. To perform an attack Eve makes specific measurements, obtains their results, prepares her own states in a certain way, and sends them to Bob. For an attack to be sound, it must be shown, in exact mathematical expressions that it does not change the monitored statistics of photocounts.

The main statement of our work was that the detector blinding attack as it appears in the cited papers is detectable in systems with phase coding. Detectability directly follows from the presence of the delay interferometer and the conservation of energy in a distributed interference. If the authors really claim that a particular new attack with detector blinding for phase coding systems allows Eve to remain undetected, they need to provide a succinct description of the attack as well as the underlying math.

Overall, we find that one of our goals was to show a significant structural difference between the polarization coding

and phase coding systems. A consequence of such a difference results in the inability of blunt application of a well known attack to phase coding systems. The same strategy just does not work because of significantly broader monitoring abilities existing in phase coding systems.

Besides that, if new attacks that threatens the security of phase coding systems via detector blinding or other means show up, we will be interested in discussing them and inventing effective protection.

References

[1] Fedorov A *et al* Comment on 'Inherent security of phase coding quantum key distribution systems against detector blinding attacks' (2018 Laser Phys. Lett. 15 095203) *Laser. Phys. Lett.*

[2] Balygin K A, Klimov A N, Bobrov I B, Kravtsov K S, Kulik S P and Molotkov S N 2018 Inherent security of phase coding quantum key distribution systems against detector blinding attacks *Laser Phys. Lett.* **15** 095203