Independent security analysis of a commercial quantum random number generator Quantis from ID Quantique

Mikhail Petrov,[1, 2, *] Igor Radchenko,[3] Damian Steiger,[4, 5]
Renato Renner,[4] Matthias Troyer,[4, 5] and Vadim Makarov[1, 6, 2, 7]

[1] *Russian Quantum Center, Skolkovo, Moscow 121205, Russia*
[2] *NTI Center for Quantum Communications, National University of Science and Technology MISiS, Moscow 119049, Russia*
[3] *Moscow State University, Moscow, 119991 Russia*
[4] *Institute for Theoretical Physics, ETH Zurich, CH-8093 Zurich, Switzerland*
[5] *Microsoft Corporation, One Microsoft Way, Redmond, WA 98052, USA*
[6] *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 201315, People's Republic of China*
[7] *Department of Physics and Astronomy, University of Waterloo, Waterloo, ON, N2L 3G1 Canada*

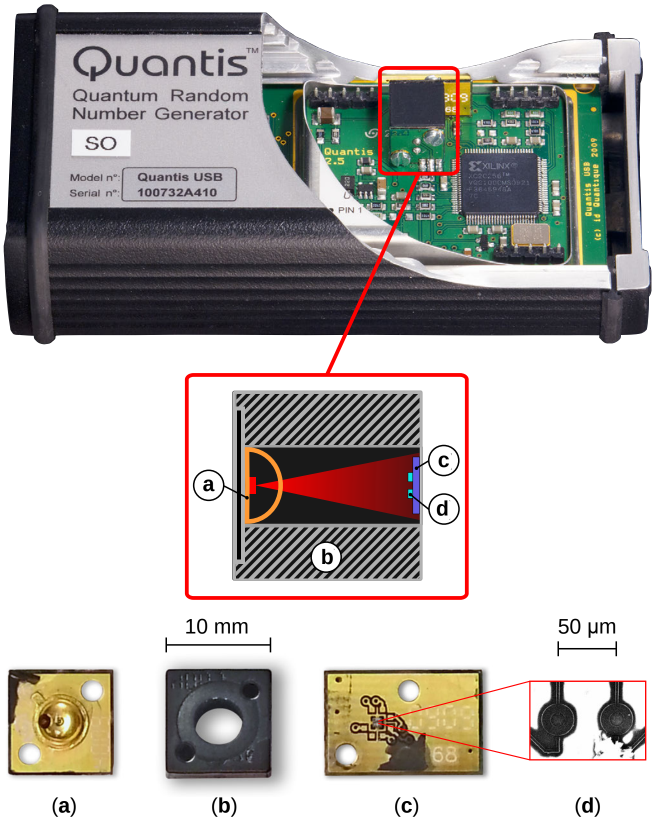

FIG. 1. "Source of quantumness" taken apart. (a) Light-emitting-diode light source. (b) Anodized aluminum sleeve. (c) Pair of single-photon detectors. (d) Photosensitive areas of the single-photon detectors (electron-microscope image).

We reverse-engineer, test and analyse hardware and firmware of the commercial quantum-optical random number generator Quantis from ID Quantique. We show that > 99% of its output data originates in physically random processes: random timing of photon absorption in a semiconductor material, and random growth of avalanche owing to impact ionisation. We have also found minor non-random contributions from imperfections in detector electronics and an internal processing algorithm. Our work shows that the design quality of a commercial quantum-optical randomness source can be verified without cooperation of the manufacturer and without access to the engineering documentation.

While no optical beamsplitter element has been found in the Quantis device, it nevertheless contains two sources of randomness—two Geiger-mode APDs (Fig. 1). Within them, the relevant quantum processes are photoexcitation and impact ionisation. Basically, either APD may be regarded as an independent source of randomness, however the presence of two of them increases the bit rate.

We have performed several measurements to test for potential imperfections in Quantis that could have an impact on the randomness in the output bit stream. Most interestingly, we have found a correlation between adjacent output bits owing to the click rate mismatch of the APDs. However this and other effects stay well below the specified "thermal noise contribution" of less than 1% [1], and could be eliminated by the use of randomness extractors [2]. Our preliminary conclusion is that Quantis conforms to its published specification of the physical randomness content in the output bit stream.

Our full results are available in **arXiv:2004.04996.**

[1] ID Quantique, Quantis random number generator, `https://www.idquantique.com/random-number-generation/products/quantis-random-number-generator/`, visited 7 Dec 2019.

[2] M. Troyer and R. Renner, "ID Quantique techical paper on randomness extractor," version 1.0 (Sep 2012), available on request from `https://www.idquantique.com/resource-library/random-number-generation/`.

[*] m.petrov@rqc.ru