Independed 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]
MatthiasTroyer [4,5]
Vadim Makarov [1,6,2,7]

Quantis Random Number Generator from ID Quantique

We perform an independent examination of Quantis without access to the manufacturer's internal documentation. We test and analyse Quantis hardware and firmware.

What is inside ?

How it works ?

Is it really quantum ?

Is it random ?

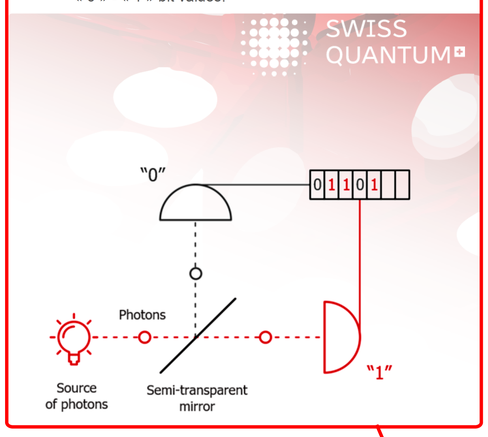
Source of quantumness

Quantis Random Number Generator Broshure (from ID Quantique www.idquantique.com)

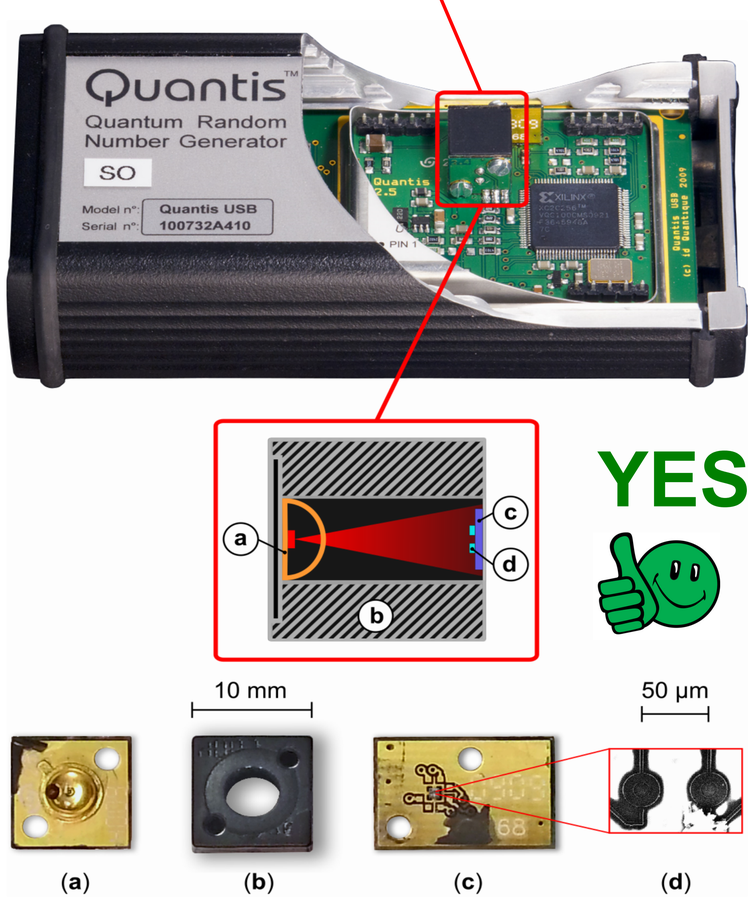
QUANTIS Principle

Based on Quantum Physics :

Photons - light particles - are sent one by one onto a semi-transparent mirror and detected. The exclusive events (reflection - transmission) are associated to « 0 » - « 1 » bit values.



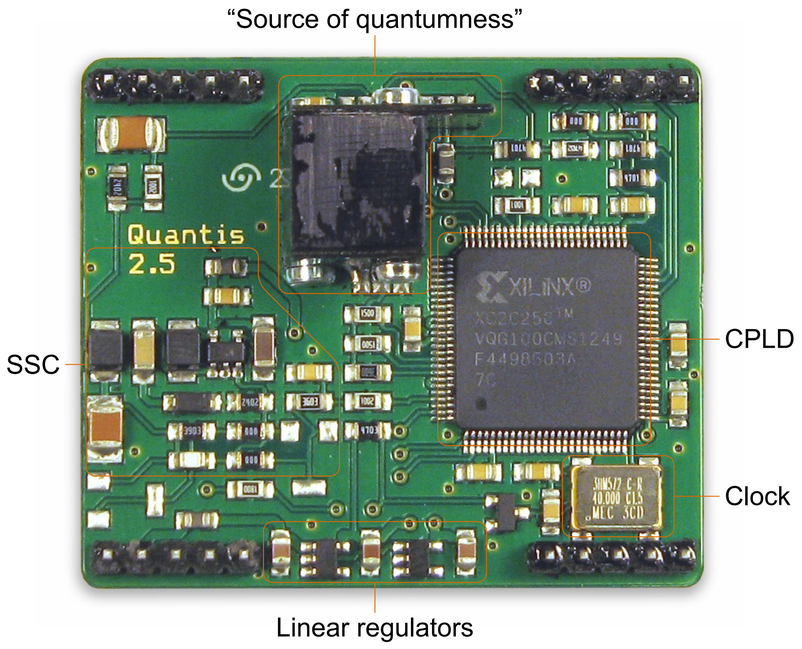
NO !



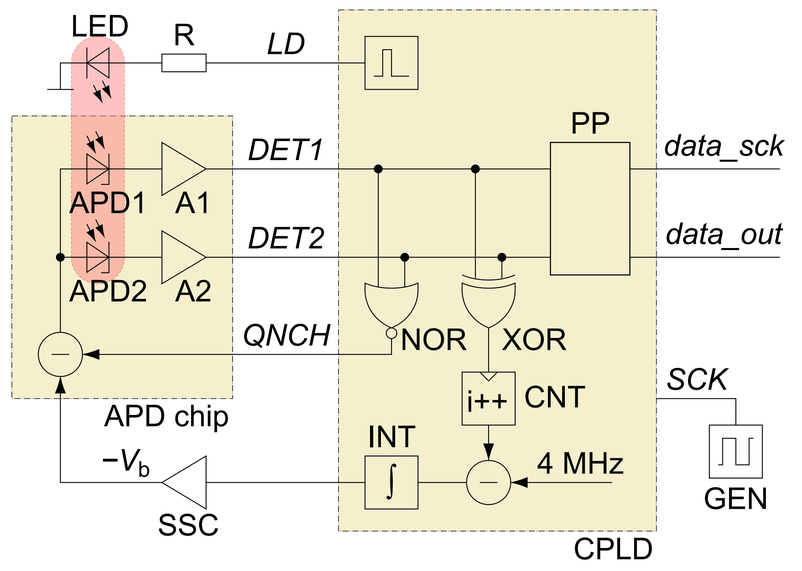
YES !

LED SLEEVE 2 Single-photon detectors

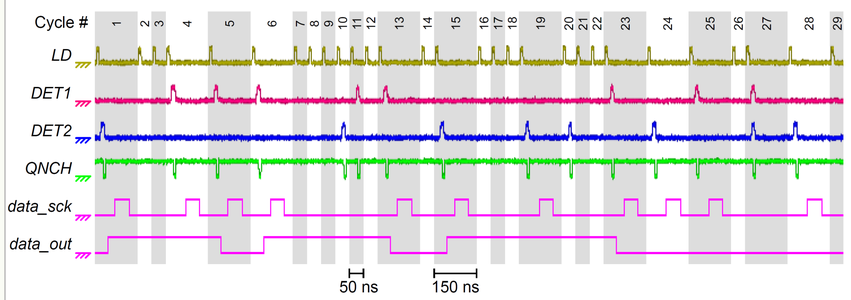
Main printed circuit board



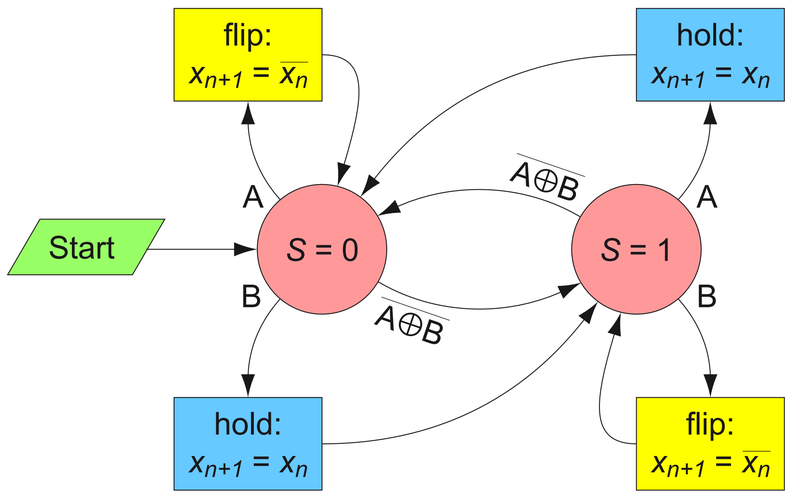
Simplified electrical scheme



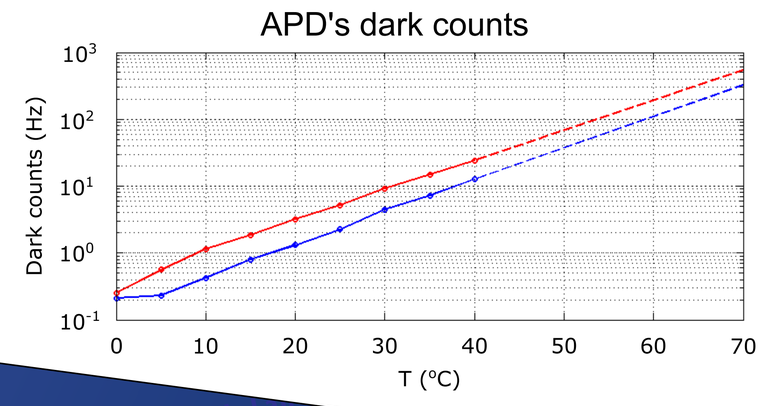
Captured signals

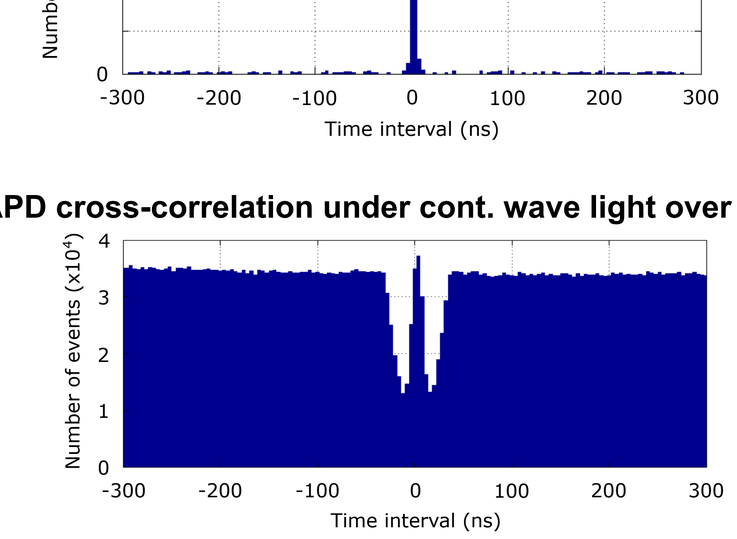


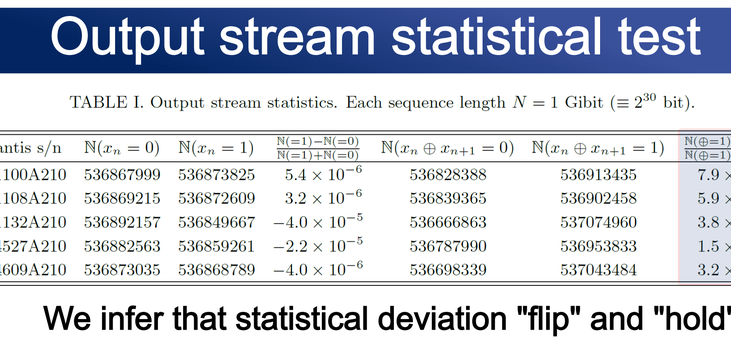
Post processing algorithm

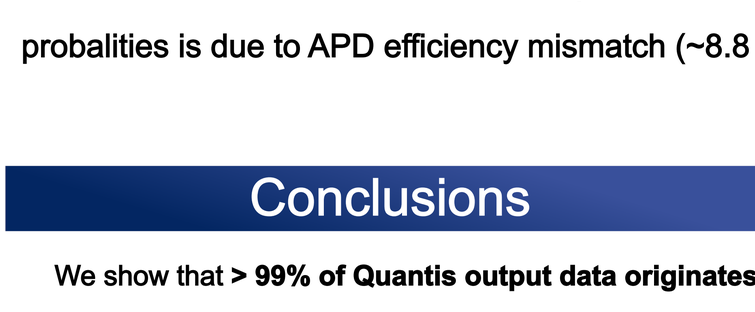


Measurements









Output stream statistical test

TABLE I. Output stream statistics. Each sequence length $N = 1$ Gibit ($\equiv 2^{30}$ bit).

Quantis s/n	$\mathbb{N}(x_n = 0)$	$\mathbb{N}(x_n = 1)$	$\frac{\mathbb{N}(=1)-\mathbb{N}(=0)}{\mathbb{N}(=1)+\mathbb{N}(=0)}$	$\mathbb{N}(x_n \oplus x_{n+1} = 0)$	$\mathbb{N}(x_n \oplus x_{n+1} = 1)$	$\frac{\mathbb{N}(\oplus=1)-\mathbb{N}(\oplus=0)}{\mathbb{N}(\oplus=1)+\mathbb{N}(\oplus=0)}$
0701100A210	536867999	536873825	5.4×10^{-6}	536828388	536913435	7.9×10^{-5}
0701108A210	536869215	536872609	3.2×10^{-6}	536839365	536902458	5.9×10^{-5}
0701132A210	536892157	536849667	-4.0×10^{-5}	536666863	537074960	3.8×10^{-4}
1304527A210	536882563	536859261	-2.2×10^{-5}	536787990	536953833	1.5×10^{-4}
1304609A210	536873035	536868789	-4.0×10^{-6}	536698339	537043484	3.2×10^{-4}

We infer that statistical deviation "flip" and "hold" probalities is due to APD efficiency mismatch (~8.8 %).

Conclusions

We show that **> 99% of Quantis output data originates in physically random processes**: random timing of photon absorption in semiconductor material, and random growth of avalanche owing to impact ionisation. We found minor non random contributions from imperfecton in detector electronics and internal processin algorithm. However all **these effects stay well below specified by ID Quantique 1%.**

Our full results are available in arXiv:2004.04996

* petrov-ma@yandex.ru

[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 Phisics$_6$ ETH Zurich, CH-8093 Zurich, Switzerland
[5] Microsoft Corporation, One Microsoft Way, Redmond, WA 98052, USA
[6] Shanghai Branch, National Laboratory for Phisical 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

Presented at QCrypt, Amsterdam (on-line), 10-14 August 2020