

REDEFINING RANDOMNESS

QUANTIS

WHEN RANDOM NUMBERS CANNOT BE LEFT TO CHANCE

TRUE RANDOM NUMBER GENERATOR

Although random numbers are required in many applications, their generation is often overlooked. As computers are deterministic, they are not capable of producing truly random numbers. A physical source of randomness is required and since quantum physics is intrinsically random, it is natural to exploit it for this purpose.

Quantis is a physical random number generator exploiting an elementary quantum optics process. 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.

Quantis random number generators have the advantage over conventional randomness sources of being invulnerable to environmental perturbations and of allowing live status verification. The operation of Quantis is continuously monitored and if a failure is detected the random bit stream is immediately disabled. In addition, Quantis provides full entropy (randomness) instantaneously from the very first photon (bit).

Quantis is available as a USB device and integrates easily in existing applications. It is compatible with the most commonly used operating systems. A library which allows easy access and a demonstration application are provided.

The breadth of application is maximized by the advanced functionalities such as scaling and randomness extraction implemented in the Quantis software package.



APPLICATIONS

- Cryptography
- Lotteries, Online Gaming
- PIN number generation
- Numerical simulations
- Statistical research
- Mobile prepaid system
- Secure printing

MAIN FEATURES

- True quantum randomness
- Most certified quantum RNG
- High bit rate up to 4 Mbits/s
- Randomness extraction capability
- Continuous status check
- Low cost
- Compact and reliable
- Easy integration in applications
- Instantaneous entropy

QUANTIS USB



Quantis-USB-4M

GENERAL SPECIFICATIONS

1: Hardware bit rate prior to randomness extraction

Random bit rate¹	4 Mbit/s \pm 10% (Quantis-USB-4M)
Thermal noise contribution	< 1% (Fraction of random bits arising from thermal noise)
Storage temperature	- 25 to + 85°C
Dimensions	61 mm x 31 mm x 114 mm
USB specification	2.0
Requirement	PC with available USB connector
Power	Via USB port

QUANTIS Certifications

The simplicity of Quantis is also its strength. As the underlying quantum mechanical processes are well understood and easily characterized, it is relatively easy to certify the Quantis products.

Quantis is the most certified true RNG in the market. It has successfully passed the following certifications or government validations:

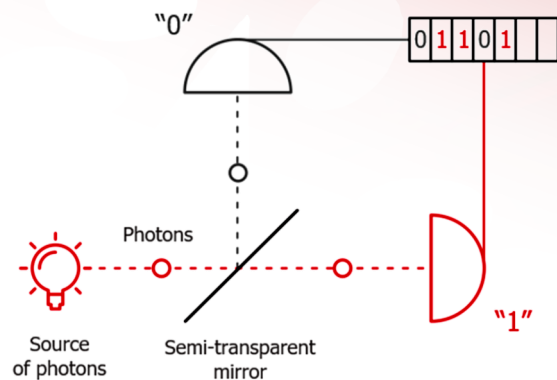
- NIST SP800-22 Test Suite Compliance
- METAS Certification
- CTL Certification
- Several iTech Labs individual Certificates
- Compliance with the BSI's AIS31 standard (dedicated version of Quantis)

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.



QUANTIS Software

SUPPORTED OPERATING SYSTEMS

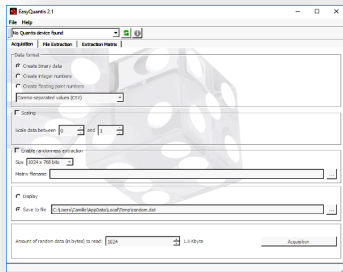
Quantis software (drivers, Quantis library and application) available for the following operating systems :

Supported OS	V18.03.08	V20.2.3
Windows Vista (32-, 64-bit)	✓	✗
Windows Server 2008 (32-, 64-bit)	✓	✗
Windows Server 2012 (32-, 64-bit)	✓	✗
Windows Server 2016 (32-, 64-bit)	✓	✗
Windows 7, 8 (32-, 64-bit)	✓	✗
Windows 10	✗	✓
FreeBSD	✓	✗
Mac OS X*	✓	✗
Solaris / OpenSolaris	✓	✗
Linux 2.6, 3.x, 4x	✓	✗
Ubuntu 18.04	✗	✓
CentOS 7	✗	✓

*Note: MAC OS X only available with Quantis USB

QUANTIS Software

EasyQuantis APPLICATION



Quantis comes with a useful cross operating system application called EasyQuantis allowing to read random numbers, which can be stored in a file or displayed.

Random number can be generated in the following formats :

- Binary
- Integers
- Floating point

The application includes advanced functionalities such as scaling or randomness extraction and can be used to access multiple Quantis generators.

A Command Line Interface can also be used to access Quantis and integrate EasyQuantis in scripts.

QUANTIS LIBRARIES

The Quantis library can be used to access the Quantis QRNG. The library API is identical for the PCIe and USB library and is available on all supported operating systems.

The library enables the production of random binary data, integers and floating point numbers. It can be used to access multiple Quantis generators and includes advanced functionalities such as random data scaling.

The QuantisExtensions library implements a randomness extractor which can be used to postprocess the output of the Quantis QRNG.

LIBRARY WRAPPERS

Wrappers, allowing to access the Quantis library as well as sample source code, are provided for the following programming languages :

- C++
- C#
- Java
- VB.NET

Quantis also supports the standard C++11 random device API.

ORDERING INFORMATION

- Quantis-USB-4M USB device with 1 module generating a random bit stream of 4 Mbits/s

Disclaimer: The information and specifications set forth in this document are subject to change at any time by ID Quantique without prior notice.

Copyright 2006-2022 ID Quantique SA —All rights reserved Quantis USB —Specifications as of August 2022