

Quantis
True randomness upon request



METAS

New

Tested and certified by **METAS**
Swiss Federal Office of Metrology

Quantum Random Number Generator



(PCI)



(USB)



(OEM)

When random numbers cannot be left to chance!

Although random numbers are required in many applications, their generation is often overlooked.

Being deterministic, computers are not capable of producing random numbers. A physical source of randomness is necessary. Quantum physics being intrinsically random, it is natural to exploit a quantum process for such a source. Quantum random number generators have the advantage over conventional randomness sources of being invulnerable to environmental perturbations and of allowing live status verification.

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.

The operation of Quantis is continuously monitored. If a failure is detected the random bit stream is immediately disabled.

Quantis is available as a PCI card, an USB device and a component for mounting on a printed circuit board (see Quantis-OEM). Quantis is easily integrated in existing applications.

Main features

- ▶ True quantum randomness
- ▶ Passes NIST and Diehard randomness tests
- ▶ High bit rate up to 16 Mbits/s
- ▶ Low cost
- ▶ Compact and reliable
- ▶ Continuous status check
- ▶ Easy integration in existing applications

Applications

- ▶ Cryptography
- ▶ Gambling, lotteries
- ▶ Secure printing
- ▶ PIN number generation
- ▶ Mobile prepaid system
- ▶ Statistical research
- ▶ Numerical simulations

Quantis PCI card

Functional description

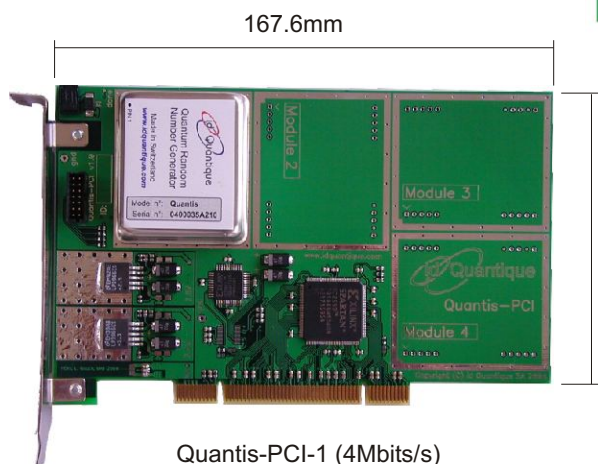
The Quantis-PCI cards provide a random bit stream at an average rate of 4Mbit/s (Quantis-PCI-1) and 16Mbits/s (Quantis-PCI-4). To guarantee a high level of integrity, all internal functions are continuously monitored. In case of a system failure the bit stream is automatically inhibited.

Drivers are provided to interface the PCI card with Windows (2000, XP), Linux (2.4, 2.6), FreeBSD (4, 5, 6) and Solaris (8, 9, 10 for SPARC, x86 and x64) Operating Systems. A Quantis library can be used to access the Quantis-PCI card. The library works under all four OS families. Under Windows use of this library is mandatory, whereas under Linux, FreeBSD and Solaris, one has direct access to the random bit stream generated by the PCI card through the file: /dev/qrandom access .

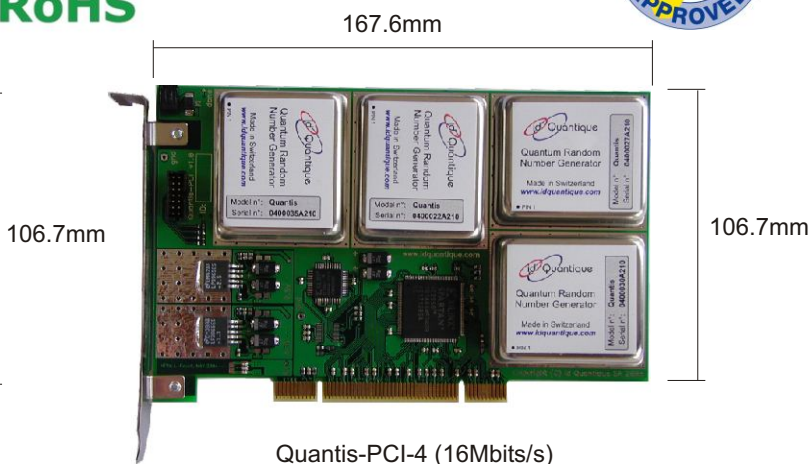
A simple application is supplied that does the acquisition of the random bit stream. A Labview Virtual Instrument is also provided.

General specifications

Random bit rate	4 Mbit/s \pm 10% for Quantis-PCI-1 16 Mbit/s \pm 10% for Quantis-PCI-4
Thermal noise contribution	< 1% (Fraction of random bits arising from thermal noise)
Storage temperature	-25 to +85°C
Dimensions	167.6 mm x 106.7 mm
PCI local bus specification	2.2
Drivers	Windows 2000, XP (Plug and Play compatible) Linux 2.4, 2.6 FreeBSD 4, 5, 6 Solaris 8, 9, 10 for SPARC, x86 and x64
Requirements	IBM-compatible PC Available PCI slot



Quantis-PCI-1 (4Mbits/s)



Quantis-PCI-4 (16Mbits/s)

Quantis USB device

Functional description

The Quantis-USB device provides a random bit stream at an average rate of 4Mbit/s. To guarantee a high level of integrity, all internal functions are continuously monitored. In case of a system failure the bit stream is automatically inhibited.

Drivers are provided to interface the USB device with Windows (2000, XP) and Linux (2.4, 2.6) Operating Systems. A Quantis library can be used to access the USB device. The library works under both OS families. Under Linux one has also direct access to the random bit stream generated by the USB device through the file: /dev/usb/random.

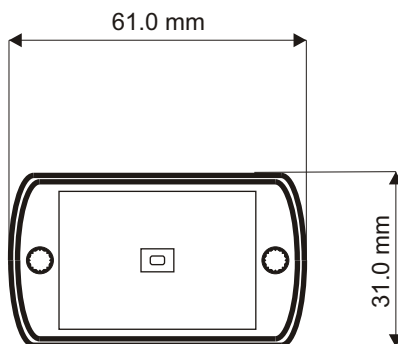
A simple application is supplied that does the acquisition of the random bit stream. A Labview Virtual Instrument is also provided.

General specifications

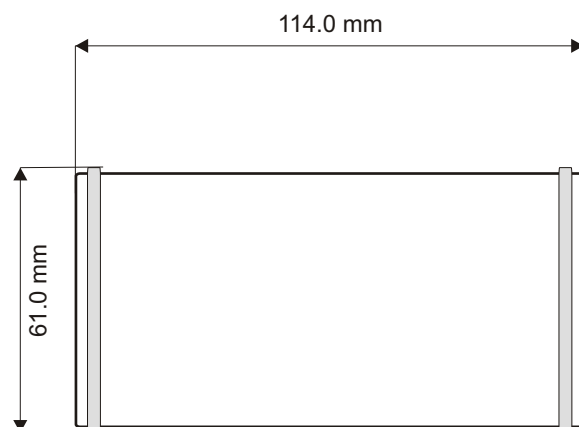
Random bit rate	4 Mbit/s \pm 10%
Thermal noise contribution	< 1% (Fraction of random bits arising from thermal noise)
Storage temperature	-25 to +85°C
Dimensions	61mm x 31mm x 114mm
USB specification	2.0
Drivers	Windows 2000, XP (Plug and Play compatible) Linux 2.4, 2.6
Requirements	IBM-compatible PC Available USB connector via USB port
Power	



Quantis USB Front view



Quantis USB Top view



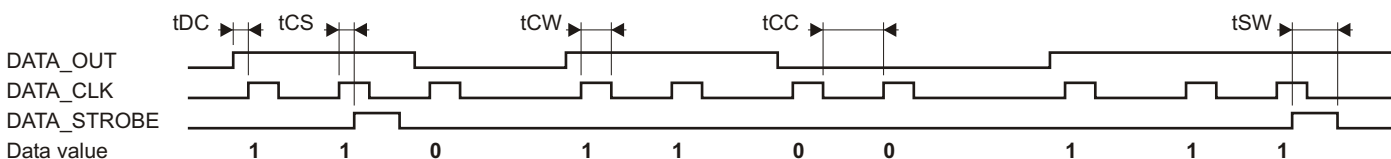
Quantis OEM module

Functional description

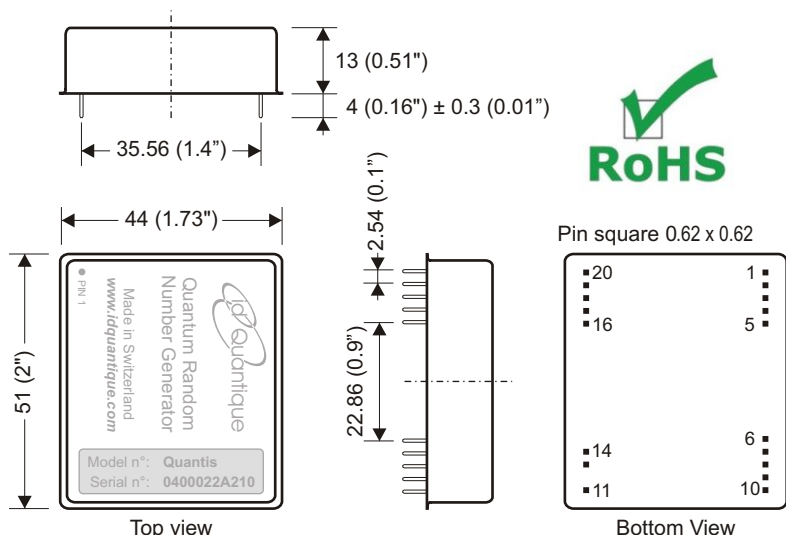
Quantis OEM module is a device to be mounted on a (PCB) printed circuit board. A complete application note is available on the website. The output pin DATA_OUT provides a random bit stream at an average rate of 4Mbit/s. The output pin DATA_CLK indicates a valid bit on DATA_OUT. A pulse is inserted on output pin DATA_STROBE every eight DATA_CLK pulses. It allows to latch an external shift register (see application note). The output pin STATUS is at logical high level under normal operation. In case of system failure, it goes to low level and the bit stream is inhibited. When input pin SHDN (shutdown) is at low level, the module is stopped and power consumption is reduced. SHDN is also used to reinitialize the module if STATUS is at low level. SHDN should be left open if not in use. MODULE_DETECTION is always at low level. It can be used to detect the presence of a module when several modules are used in a circuit.

Switching characteristics

tDC	25ns	DATA_OUT before DATA_CLK
tCS	25ns	DATA_CLK before DATA_STROBE
tCW	50ns	DATA_CLK pulse width
tCC	100ns	Minimum time between two DATA_CLK pulses
tSW	75ns	DATA_STROBE pulse width



Outline dimension mm (inches)



Pin lay-out

1	GND	20	GND
2	VCC	19	NC (Reserved)
3	SHDN	18	NC (Reserved)
4	Module_Detection	17	NC (Reserved)
5	NC (Reserved)	16	NC (Reserved)
6	DATA_OUT	15	NO PIN
7	DATA_CLK	14	NC
8	DATA_STROBE	13	NC
9	STATUS	12	NO PIN
10	GND	11	GND

NC: No connection - Do not connect.

Ordering information

Quantis - OEM	OEM Module generating a random bit stream of 4 Mbits/s
Quantis - USB	USB device with 1 module generating a random bit stream of 4 Mbits/s
Quantis - PCI-1	PCI card with 1 module generating a random bit stream of 4 Mbits/s
Quantis - PCI-4	PCI card with 4 modules generating a random bit stream of 16 Mbits/s