IDQ
FROM VISION TO TECHNOLOGY

REDEFINING RANDOMNESS

QUANTIS COMPONENT

WHEN RANDOM NUMBERS CANNOT BE LEFT TO CHANCE

TRUE RANDOM NUMBER GENERATOR BASED ON QUANTUM PHYSICS

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.

The Quantis-OEM component has been designed for mounting as a true random number generator on a printed circuit board.

Quantis-OEM

METAS

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

APPLICATIONS

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

MAIN FEATURES

- True quantum randomness
- Certified by Swiss National Laboratory
- Passes NIST and Diehard randomness tests
- High bit rate of 4 Mbits/s
- Low cost
- Compact and reliable
- Continuous status check
- Easy integration on custom circuits

ID Quantique SA
Chemin de la Marbrerie 3

1227 Carouge/Geneva
Switzerland

T +41 22 301 83 71
F +41 22 301 83 79

info@idquantique.com
www.idquantique.com

REDEFINING RANDOMNESS

QUANTIS-OEM COMPONENT

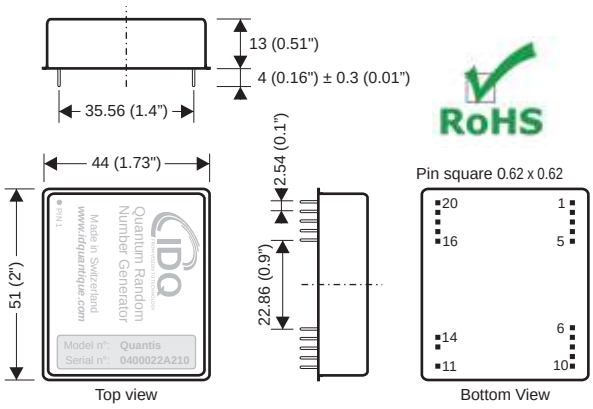
FUNCTIONAL DESCRIPTION

Quantis-OEM is a component that can be mounted on a printed circuit board (PCB). A detailed application note can be downloaded from IDQ´s 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 also present on output pin DATA_STROBE every eighth DATA_CLK pulses. It allows one 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.

OUTLINE DIMENSION mm (inches)



PIN LAYOUT

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

ORDERING INFORMATION

Quantis-OEM-4M	OEM component generating a random bit stream of 4 Mbits/s

RELATED PRODUCTS

Quantis-PCIe-4M	PCI Express card with 1 module generating a random bit stream of 4 Mbits/s
Quantis-USB-4M	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

ID Quantique SA
Chemin de la Marbrerie 3
1227 Carouge/Geneva
Switzerland
T +41 22 301 83 71
F +41 22 301 83 79
info@idquantique.com
www.idquantique.com