

# Quantis

# True randomness upon request



**Quantis-OEM  
(4 Mbits/sec)**

## QUANTIS APPLICATION NOTE

**id Quantique**

Ch. de la Marbrerie, 3 1227 Carouge Switzerland  
Tel: +41 (0)22 301 83 71 Fax: +41 (0)22 301 83 79  
sales@idquantique.com  
www.idquantique.com

Patents pending

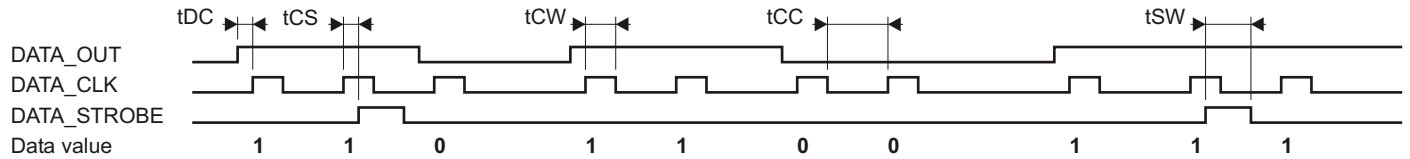
**id Quantique**  
A Quantum Leap for Cryptography

## Functional description

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 eighth DATA\_CLK pulses. It allows to latch an external shift register (see below). 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 output 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.

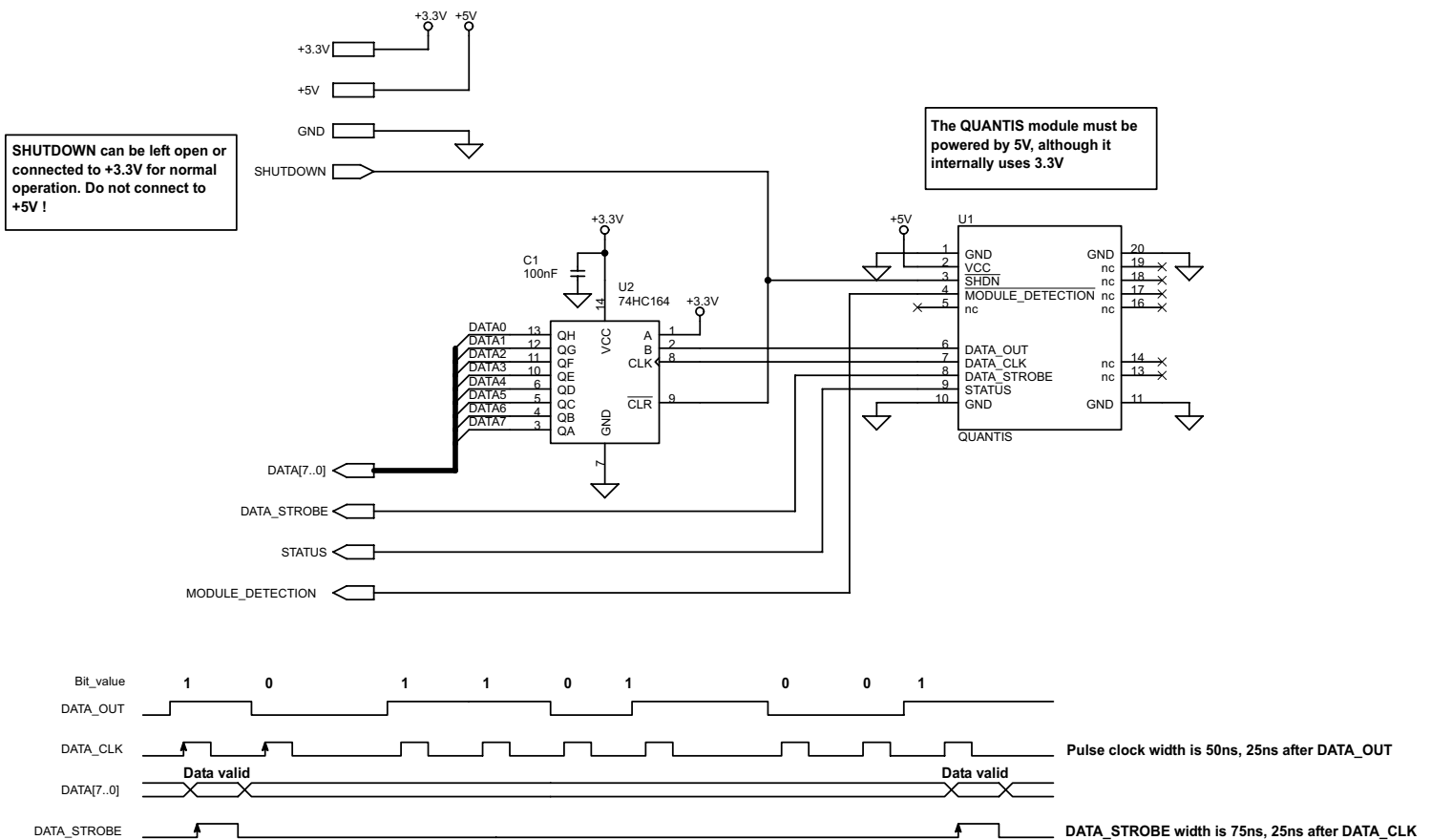
## Switching characteristics

|     |       |  |
|-----|-------|--|
| 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                  |



## Read-out example

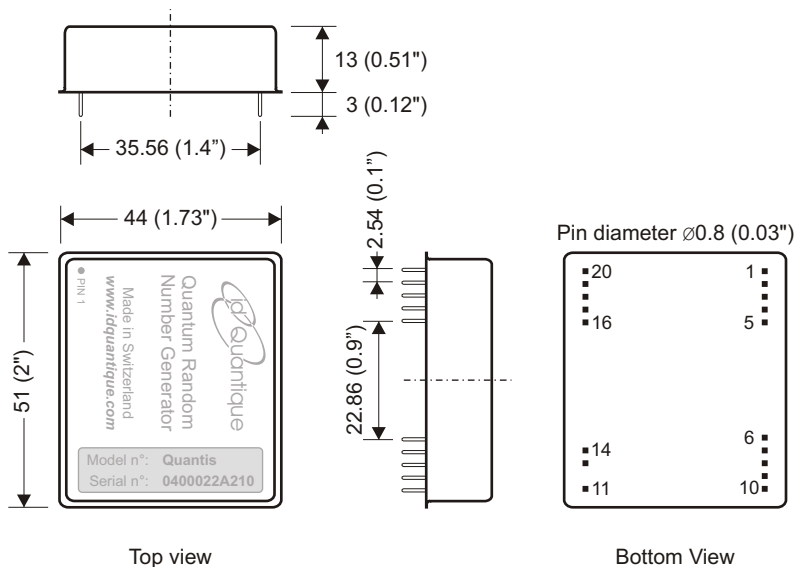
The schematic below shows a simple way to access the random bit stream generated by the Quantis module. A Quantis module is connected to an 8-bit Serial-In, Parallel-Out Shift Register. Shutdown can be left open or can be connected to +3.3V.



## General specifications

|                                      |   |
|--------------------------------------|---|
| Random bit rate                      | 4 Mbit/s $\pm$ 10%  |
| Thermal noise contribution           | < 1% (Fraction of random bits arising from thermal noise) |
| Input and output                     | LVTTTL max. 3.3V  |
| Operating temperature                | 0 to +70°C  |
| Storage temperature                  | -25 to +85°C  |
| Weight                               | 30g   |
| Case                                 | Metallic and shielded                                     |
| Power supply (VCC)                   | +5V 10%   |
| Power supply                         | < 40mA  |
| Power supply (SHDN connected to GND) | < 500 A   |

## Outline dimensions in 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 and sales contact

|                |  |
|----------------|--|
| Quantis-OEM:   | OEM 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 |

For further information on this or other products, please contact *id Quantique* by phone: +41 (0)22 301 83 71, fax: +41 (0)22 301 83 79, or email: [sales@idquantique.com](mailto:sales@idquantique.com).

## Disclaimer

The information and specification set forth above are subject to change at any time by *id Quantique* without prior notice. Copyright *id Quantique SA* 2004.

