

# How Random is Quantum Randomness?

Cristian S. Calude  
University of Auckland

Asian Logic Conference, Wellington, December 2011

## What is quantum randomness?

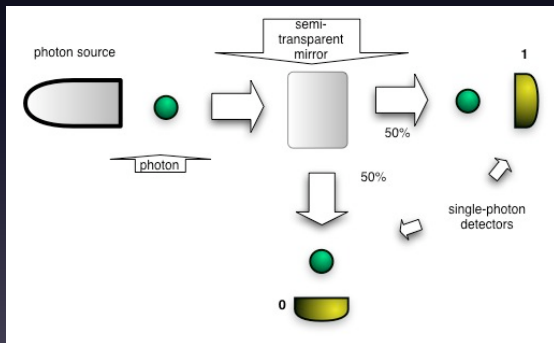
Quantum randomness appears in two different scenarios:

(i) the complete impossibility to predict or explain the occurrence of certain *single* events and measurement outcomes from any kind of operational causal connection, and

(ii) the concatenation of such single quantum random events forms sequences of random bits with the least correlations, as the occurrence of a particular bit value in a binary expansion does not depend on previous or future bits of that expansion.

## Optical quantum randomness

A photon generated by a source beamed to a semi-transparent mirror is reflected or transmitted with 50 per cent chance; measuring, we get a quantum random bit.



- has been confirmed by theoretical and experimental research,
- passes all reasonable statistical properties of randomness.

But, where is it coming from?

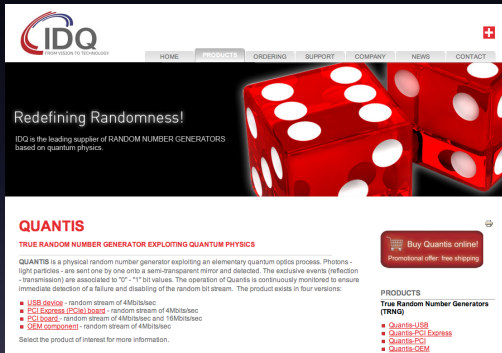
## True randomness?

In spite of mathematics—there is no true randomness—generators of **true random bits** proliferate.

*Nature's* claim (doi:10.1038/news.2010.181, 14 April 2010):



Truly random numbers have been generated at last.



The screenshot shows the IDQ website with a navigation bar (HOME, PRODUCTS, ORDERING, SUPPORT, COMPANY, NEWS, CONTACT) and a main banner with the text "Redefining Randomness!" and "IDQ is the leading supplier of RANDOM NUMBER GENERATORS based on quantum physics." Below the banner, the "QUANTIS" product is described as a "TRUE RANDOM NUMBER GENERATOR EXPLOITING QUANTUM PHYSICS". A list of product variants is provided: USB device, PCI Express (PCIe) board, PCI board, and QCM component. A "Buy Quantis online!" button with a shopping cart icon and a "Promotional offer: free shipping" message is also visible. A "PRODUCTS" section lists "True Random Number Generators (TRNG)" with sub-items: Quantis-USB, Quantis-PCI Express, Quantis-PCI, and Quantis-QCM.

**IDQ**  
INTEGRATED DEVICE QUANTUM

HOME PRODUCTS ORDERING SUPPORT COMPANY NEWS CONTACT

**Redefining Randomness!**  
IDQ is the leading supplier of RANDOM NUMBER GENERATORS based on quantum physics.

**QUANTIS**  
TRUE RANDOM NUMBER GENERATOR EXPLOITING QUANTUM PHYSICS

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 to ensure immediate detection of a failure and disabling of the random bit stream. The product exists in four versions:

- **USB device** - random stream of 4Mbits/sec
- **PCI Express (PCIe) board** - random stream of 4Mbits/sec
- **PCI board** - random stream of 4Mbits/sec and 16Mbits/sec
- **QCM component** - random stream of 4Mbits/sec

Select the product of interest for more information.

Buy Quantis online!  
Promotional offer: free shipping

**PRODUCTS**  
**True Random Number Generators (TRNG)**

- Quantis-USB
- Quantis-PCI Express
- Quantis-PCI
- Quantis-QCM

Quantis: quantum mechanical random number generator produced and sold by *id Quantique* of the University of Geneva

Born's 1926 decision to “give up determinism in the world of atoms” has become a core part of our understanding of quantum mechanics.

No-go theorems (such as the Kochen-Specker theorem ▶ NGT) are stronger: if we assume non-contextuality, then there can, in general, be no pre-existing definite values (value indefiniteness) prescribable to certain sets of measurement outcomes in dimension three or greater Hilbert space.

Quantum randomness is not due to ignorance of the system being measured; indeed, since there are in general **no definite values** associated with the measured observable it is surprising there is an outcome at all.



### Assume

- a standard picture of quantum mechanics, i.e. a Copenhagen-like interpretation in which measurement irreversibly alters the quantum state,
- measurements are non-contextual,
- and the experimenter has freedom in the choice of measurement basis (the “free-will assumption”).

Under the above assumptions, a quantum random experiment certified by value indefiniteness and performed under ideal conditions generates an infinite (strongly) incomputable sequence of bits:

*every Turing machine can reproduce exactly only finitely many scattered digits of such an infinite sequence, i.e. the sequence is bi-immune.*

Data consisting of  $2^{32}$ -bit strings:

- 1 10 quantum random strings generated by the *Vienna IQOQI* group
- 2 10 quantum random strings generated with the *Quantis* device
- 3 10 strings from the binary expansion of  $\pi$  obtained from the University of Tokyo's supercomputing center
- 4 10 pseudo-random strings produced by *Mathematica 6*
- 5 10 pseudo-random strings produced by *Maple 11*

## Normality test

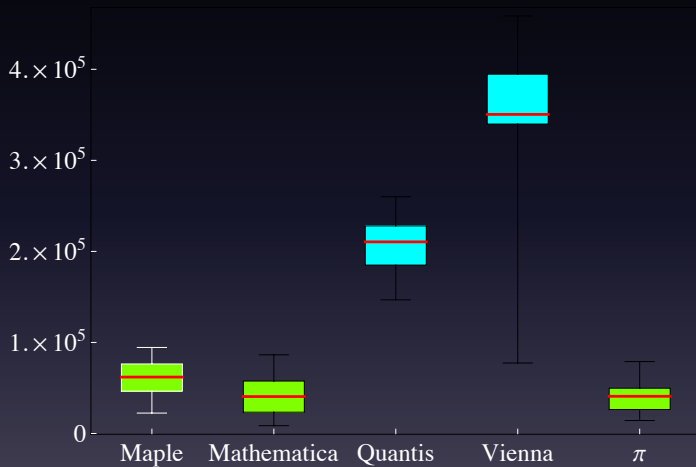
For any fixed integer  $m > 1$ ,  $B_m = \{0, 1\}^m$ , and for every  $1 \leq i \leq 2^m$  denote by  $N_i^m$  the number of occurrences of the lexicographical  $i$ th binary string of length  $m$  in the string  $x$  over  $B_m$ . By  $|x|_m$  we denote the length of  $x$

A string  $x$  is normal if for every natural  $1 \leq m \leq \log_2 \log_2 |x|$ ,

$$\left| \frac{N_j^m(x)}{|x|_m} - 2^{-m} \right| \leq \sqrt{\frac{\log_2 |x|}{|x|}},$$

for every  $1 \leq j \leq 2^m$ .

## Box-and-whisker plot



# Statistical significance

Table: Kolmogorov-Smirnov test for normality tests.

Kolmogorov-Smirnov test $p$ -values	Mathematica	Quantis	Vienna	$\pi$
Maple	0.4175	$< 10^{-4}$	<b>0.0002</b>	0.1678
Mathematica		$< 10^{-4}$	<b>0.0002</b>	0.9945
Quantis			<b>0.0002</b>	$< 10^{-4}$
Vienna				<b>0.0002</b>

- Find other principles certifying quantum randomness.
- Is quantum randomness certified by Kochen-Specker theorem Kurtz random? (A real which is contained in every c.e. open set  $U$  of measure one is called Kurtz random.)
- Are all forms of quantum randomness equal in quality?

A. A. Abbott, C. S. Calude, K. Svozil. Incomputability of quantum randomness, in preparation, 2011.

C. S. Calude, K. Svozil. Quantum randomness and value indefiniteness, *Advanced Science Letters* 1 (2008), 165–168.

C. S. Calude, M. J. Dinneen, M. Dumitrescu, K. Svozil. Experimental evidence of quantum randomness incomputability, *Physical Review A*, 82, 022102 (2010), 1–8.



A no-go theorem is a theorem that states that a particular situation is not physically possible.

Bell's theorem: No physical theory of local hidden variables can reproduce all QM predictions.

In QM, VD + NC is contradictory:

VD: All observables defined for a QM system have definite values at all times.

NC: If a QM system possesses a property (value of an observable), then it does so independently of how that value is eventually measured.

► QIndet