
mathsinside
RANDOM

THE RANDOM REVOLUTION

From cybercrime to gaming with the help of mathematics

High profile cases of cybercrime often make the headlines and cause a constant headache for businesses and individuals. What few people realise is that a lot of cyber security relies on being able to generate lists of random numbers. Unfortunately, generating genuinely random numbers is harder than you may think.

If you ask a person to pick a number at random, many will pick the number 7 – which is not very random at all. Computers generate random numbers via a set of rules, but this too can be vulnerable to hackers who might be able to work out what rules the computer is using.

$$\underbrace{\frac{-h^2}{2\mu}\nabla^2\psi}_{①} + \underbrace{V\psi}_{②} = \underbrace{E\psi}_{③}$$

The Schrödinger Equation – one of the most important equations in quantum mechanics. Although it may look daunting, it is analogous to a simple classical equation for the conservation of energy; term 1 represents kinetic energy, term 2 potential energy and term 3 the total energy.

Researchers at Lancaster University and Quantum Base have applied the strange laws of quantum mechanics to develop a low-cost solution for generating genuinely random numbers. Quantum mechanics is mainly used to describe how tiny particles such as electrons behave at very small scales.

With quantum mechanics you cannot predict precisely the position of an electron, instead you are given probabilities which describe how likely it is that the particle is located at a particular location. At the heart of quantum mechanics is the Schrödinger Equation which contains the probability function ψ. The position of an electron is no longer predicted with certainty – it is now a matter of probabilities.

Researchers at Lancaster University use quantum diodes in which electrons are given the option of passing along two different paths, one with a high energy and the other a low energy. The probabilistic nature of quantum mechanics means that they have been able to design it so that the electrons pass through the different paths with a 50:50 probability. The two different paths are assigned values of 0 and 1, meaning that the choices of the electrons result in a random number which is governed not by a computer algorithm, but by the laws of quantum mechanics. The result is a small low-cost diode which can produce an endless stream of truly random numbers.

The possible applications for this technology are extensive, and encompass any type of encryption which relies on random numbers such as buying goods over the internet with a credit card. Other less obvious applications include the generation of codes on gift cards, randomly generated lottery numbers, cryptocurrencies, verification of passports and pharmaceutical security codes.

quantumbase.com/sse

LONDON MATHEMATICAL SOCIETY EST. 1865
Quantum Base
Lancaster University
Appleyard Lees
mathsinside