IN BRIEF 18 April 2018

Encrypt your data with random quantum weirdness

NO RANDOM number generator has been proved to be truly random – except this one.

Thanks to a quirk of quantum mechanics, a single photon – a particle of light – can be in two states at once, like a coin mid-flip. The coin is just as likely to land on heads or tails. The same goes for the photon, which is polarised at two angles at once, until it settles into one when measured. This rule is the basis of a device built by Peter Bierhorst at the US National Institute of Standards and Technology in Boulder, Colorado.

He and his colleagues produced pairs of entangled photons with a laser, which shoots them at two detectors, each fitted with a filter that allows only photons of a particular polarisation through.

The detectors were 187 metres apart, and one of two filters for each was chosen just before the photons hit. This ensures that the final state of each photon is not affected by outside forces, since no information has time to pass between the detectors. Also, if the photons stay entangled, it is proof they haven't been tampered with.

Each photon has a 50 per cent chance of going through a filter, depending on which state it collapses into. A photon that makes it through the filter is a 1, and one that doesn't is a 0. These random 1s and 0s can be strung together and converted into integers to be used in encryption.

The experiment's success rate was low – just 1024 usable random bits were produced by 55 million photon pairs, (*Nature*, doi.org/cm94). That's enough to confirm the randomness of the output, but not enough to be useful.

This article appeared in print under the headline "Quantum trick produces truly random numbers"

Want more? Read the extended version of

this article.

Magazine issue 3174, published 21 April 2018