Physics duo describe a way to guarantee true randomness
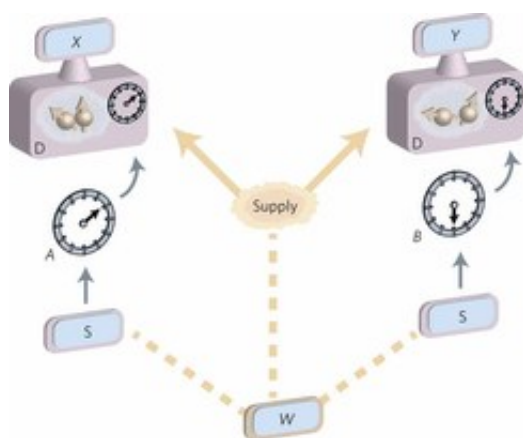
May 8 2012, by Bob Yirka

Illustration of the bipartite set-up. Image (c) *Nature Physics* (2012) doi:10.1038/nphys2300

(Phys.org) -- In the natural world, it seems randomness is all around. Walk through a forest for example and it appears completely random, despite the fact that natural patterns emerge at almost every turn. In the human world, randomness is valued by all manner of people in a variety of circumstances, from testers of systems to ensure that weaknesses show up before products are sold to the public, to cryptologists, to those that run casinos where randomness ensures the house will win far more often than not. Unfortunately, guaranteeing true randomness is not something that comes easy. Take the lowly coin toss for example. A slight difference in weight on the "heads" side may cause the "tales" side to turn up a hundredth of a percentage point more often. Because of this,

new work by a pair of physicists is catching the attention of people across a wide swath of interests.

Roger Colbeck and Renato Renner, as they describe in their paper published in *Nature Physics*, have figured out a way to virtually guarantee randomness in a constant stream of information. They say their technique can also transform a stream of not quite random data, to one that is truly random.

Their work is based on experiments done with quantum entanglement, whereby two particles appear to coexist in separate places. What happens to one, happens to the other at exactly the same time. Scientists don't yet know how it happens, but they are now able to make it happen whenever they want. In looking at studies of quantum entanglement, Colbeck and Renner noted that physicists involved in the study tended to assume that the measurements used to study the phenomenon were originally random.

Because of this, the two calculated what would likely happen if a stream of data that was only partially random was correlated with other variables, thus ensuring that bits of information would not be random. If those bits of information were used to choose measurements on paired particles that were entangled that were caused to go down different paths the outcome would have to be independent of the other variables, which would mean true randomness had been achieved.

The two say that this process could be applied to real world data to create true random data streams that could be used in virtually any application that requires the use of truly random numbers.

 More information: Free randomness can be amplified, *Nature Physics* (2012) doi:10.1038/nphys2300

Abstract

Are there fundamentally random processes in nature? Theoretical predictions, confirmed experimentally, such as the violation of Bell inequalities, point to an affirmative answer. However, these results are based on the assumption that measurement settings can be chosen freely at random, so assume the existence of perfectly free random processes from the outset. Here we consider a scenario in which this assumption is weakened and show that partially free random bits can be amplified to make arbitrarily free ones. More precisely, given a source of random bits whose correlation with other variables is below a certain threshold, we propose a procedure for generating fresh random bits that are virtually uncorrelated with all other variables. We also conjecture that such procedures exist for any non-trivial threshold. Our result is based solely on the no-signalling principle, which is necessary for the existence of free randomness.

via [ScienceNews](#)

Citation: Physics duo describe a way to guarantee true randomness (2012, May 8) retrieved 26 April 2024 from https://phys.org/news/2012-05-physics-duo-true-randomness.html