Researchers roll Einstein's dice: Developing a quantum random number generator

November 30 2011

(PhysOrg.com) -- Quantum mechanics implies that uncertainty in experimental measurements are an inherent part of nature – an idea that Albert Einstein disparagingly characterized as “rolling dice”. This true quantum randomness, for which Einstein was concerned, contrasts with a conventional gaming die, whose motion follows the laws of classical mechanics and is therefore pseudo-random. With the right physical information about initial conditions, the outcome of a dice roll can be accurately predicted.

Now, reporting in the online issue of *Optics Express*, a National Research Council (NRC) team led by Dr. Benjamin Sussman has successfully used quantum mechanical fluctuations to create a physical analogue of truly a

random die. More importantly, their die can be rolled extremely quickly and can be easily measured providing the potential to transform the security of future high-speed information networks – from encrypting military communications, to securing individual online purchases, to generating random numbers for lotteries, or in high performance computing applications.

Devices that depend on sequences of random numbers for their security are everywhere and sequences are used as cryptographic keys in numerous protocols. Yet fast and reliable generation of truly random number sequences continues to be a challenge. Most current technologies depend on number sequences generated by computational algorithms that are actually deterministic – only giving the appearance of being random. As technologies depending upon random number sequences proliferate, the fact that the numbers are not really random becomes increasingly problematic.

Dr. Sussman and his team have developed a novel solution. The researchers used stimulated Raman scattering to amplify quantum vacuum fluctuations of the electromagnetic field to macroscopic intensities. The high intensity allows them to measure the optical phase of the generated light pulses using convenient, macroscopic devices like PIN diodes – devices that are low-cost and high-speed. Team member, Dr. Philip Bustard explains, “Because the vacuum fluctuations are random, so too are the phases of the generated optical pulses. The phase measurements can then be converted into binary, generating the required random bit sequences.”

As modern security infrastructure and the digital economy put the secrets of governments, businesses, and individuals into cyberspace, it increases the vulnerability of this information to attacks. Dr. Sussman notes that, “While the rolling of dice has been essential to games of chance throughout the ages, the importance of random numbers has

never been more apparent. Aside from its application in generating random numbers for reliable lotteries and gaming platforms, a truly random number generator will provide impenetrable encryption for communications – be they military transmissions, secure banking, or online purchasing – that underpin the modern connected world."

More information: www.opticsinfobase.org/oe/abst … m?URI=oe-19-25-25173

Provided by National Research Council of Canada