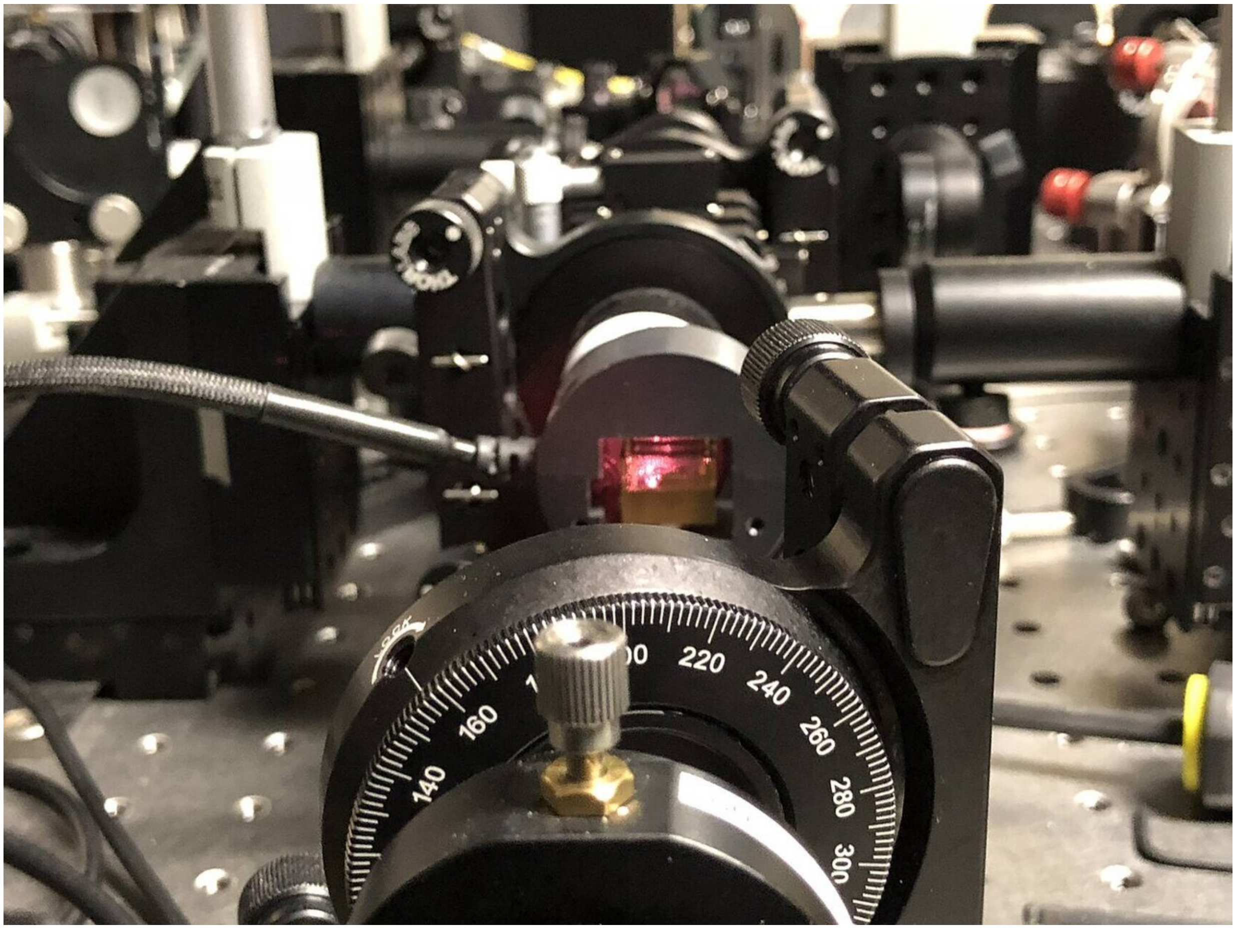
PHYS.ORG

A device-independent protocol for more efficient random number generation

March 9 2021, by Ingrid Fadelli



Using powerful laser pulses focused into a small crystal, entangled pairs of photons are created. These entangled photons are then sent to remote stations where measurements on them lead to random bits being created. Credit: Krister Shalm.

Recent advancements in the development of experimental Bell tests have enabled the implementation of a new type of device-independent random number generator. Remarkably, this new type of random number generators can be realized with malicious quantum devices, without requiring detailed models of the quantum devices used.

Researchers at the University of Colorado/NIST Boulder (CU/NIST Boulder) and the NTT Corporation in Japan have recently developed a protocol for random number generation that can be implemented on a variety of quantum systems. This protocol, presented in a paper published in *Nature Physics*, could pave the way towards the development of safer and more effective random number generators.

"We have been interested in trying to understand how to use quantum entanglement to build an entirely new class of random number generators that are, in some sense, the most secure sources of randomness that nature allows, as far as we know," Lynden Krister Shalm, one of the researchers who carried out the study, told Phys.org.

In their previous studies, Shalm and his colleagues tried to leverage the non-local properties of quantum entanglement to generate random bits certified in a device-independent way. The security of their system depended primarily on the fact that hackers cannot send information faster than the speed of light.

"Our system differs from regular random number generators, which rely on either a physical process (e.g., radioactive decay) or mathematical algorithms," Shalm said.

In contrast with the system devised by Shalm and his colleagues, random number generators that are based on physical processes or mathematical algorithms need a number of extra assumptions to be met. To produce highly secure and certified random bits using entanglement, however, the system devised by Shalm and his colleagues must consume a great deal of randomness, which significantly impairs their system's efficiency.

"When I visited CU/NIST Boulder at the beginning of 2017, I was excited to learn that the experimental group led by Krister already had the ability to demonstrate device-independent randomness generation," Yanbao Zhang, another researcher involved in the study, told Phys.org. "As such an experiment consumes many random bits while generating only a small number of high-quality certified random bits, it is desirable to achieve device-independent randomness expansion, where more certified output bits are generated than the consumed input bits."

Shalm, Zhang and their colleagues devised a method that utilizes a small amount of seed randomness to generate more quantum-based certified random bits than those consumed by the random number generator. This is one of the primary features that sets their system apart from other random number generators.

"It is a bit like how a seed crystal can be used to grow a much larger structure," Shalm said. "We are able to output 24% more random bits than we input into the system."

In principle, the system devised by Shalm and his colleagues could be run in a way that would allow researchers to infinitely expand the input seed randomness. To achieve randomness expansion, the team at CU/NIST Boulder and NTT had to push their experimental systems to their current limits, as their technical requirements are incredibly demanding.

To expand the input seed randomness into more random bits certified in a device-independent way, the researchers had to make a clever use of these seed bits. Systems typically achieve this by running a special test on entangled particles, known as a 'loophole-free Bell test.'

"Instead of running this test, which consumes randomness, on all of the entangled photons we produce, we 'spot-check' some of the photons at random to make sure the system is behaving as expected," Shalm said. "It is similar to how a food inspector might select only a small but random sample of tomatoes for testing rather than testing every tomato in an incoming shipment. Our spot-checking protocol performs in a similar manner, but we have to take great care to make sure that the system to be spot-checked isn't being cheated."

In the context of the 'tomato' analogy provided by Shalm, if tomatoes were piled into boxes containing 2^k tomatoes each, other spot-checking protocols developed in the past would require each tomato in a box to be selected randomly with a small probability. On the other hand, the protocol devised by Shalm, Zhang and their colleagues would only require one tomato in a box to be selected uniformly at random.

"To check a box of tomatoes, the usual protocol thus consumes 2^k biased random bits while our protocol consumes only k uniformly random bits," Zhang said. "In practice, uniformly random bits rather than biased random bits are easily accessible from sources such as the NIST randomness beacon. Hence, our spot-checking protocol is experimentally more friendly."

The recent study by Shalm, Zhang and their colleagues could ultimately enable the experimental realization of infinite device-independent randomness expansion. Moreover, this study could aid the current understanding of the randomness of quantum mechanics and some of its fundamental limits.

"From a more practical point-of-view, our experiment is an example of proto-quantum networks where entangled particles are exchanged and operated on under stringent conditions to accomplish tasks not possible by any other classical (or local quantum) system," Shalm said. "These non-local quantum networks are fascinating from both a foundational and practical viewpoint."

In the future, the system developed by Shalm, Zhang and their colleagues could be used to develop compact and highly secure random number generators. Currently, device-independent generators are too complex to be implemented on compact devices or smart phones. To overcome this limitation, the researchers are currently trying to integrate their device-independent random number generator into public randomness beacons that output random bits at periodic intervals.

"This use of our system could serve any application that requires a random sample of various resources," Shalm said. "In this context, our random number generator could be used to select people for jury duty, for helping to randomly audit election systems, or even to help draw up congressional districts in a fair and non-partisan manner to combat gerrymandering. Using our system, we could also let quantum mechanics draw up our voting districts instead of politicians."

Shalm, Zhang and their colleagues were among the first to realize device-independent randomness expansion, a strong type of randomness expansion that classical systems cannot achieve. In the future, their work could inspire other teams to create similar protocols for regular quantum random number generators.

"We now are working to turn our random number generator into a fully-fledged service," Shalm said. "It is amazing to me that we can take something that has its origins in some of the earliest debates about the philosophical nature of quantum theory and turn it into a secure public service."

The experiment carried out by Shalm, Zhang and their colleagues spanned over the course of two weeks. In these two weeks, the researchers collected approximately 110 hours-worth of data. In their next studies, they would like to improve their system's efficiency, allowing it to realize device-independent randomness expansion within a few hours of experimental runtime.

"In addition, our current security analysis works in the presence of a classical hacker who holds arbitrary classical side information of the output randomness but does not share any entanglement with the quantum devices used," Zhang said. "In the future, we would like to enhance the security of the output random bits against the more powerful quantum hacker that is fully entangled with our quantum devices."

More information: Device-independent randomness expansion with entangled photons. *Nature Physics*(2021). DOI: 10.1038/s41567-020-01153-4.

Citation: A device-independent protocol for more efficient random number generation (2021, March 9) retrieved 25 April 2024 from https://phys.org/news/2021-03-device-independent-protocol-efficient-random.html