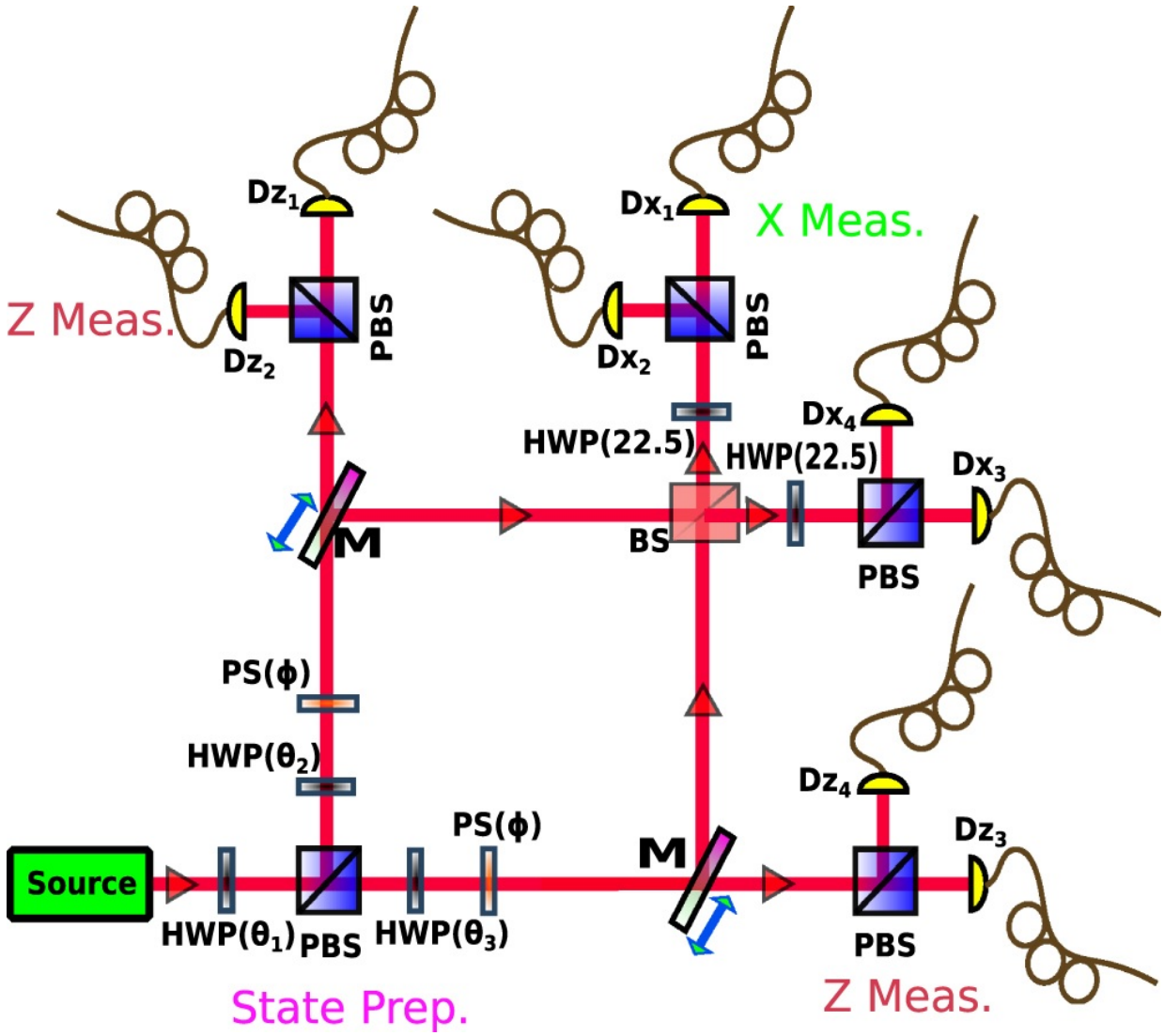
Algorithm ensures that random numbers are truly random

June 24 2016, by Lisa Zyga



Researchers have developed a method to certify more randomness in long sequences of random numbers than other methods can. Credit: Mironowicz et al.

(Phys.org)—Generating a sequence of random numbers may be more difficult than it sounds. Although the numbers may appear random, how do you know for sure that they don't actually follow some complex, underlying pattern? For this reason, finding a way to certify that a sequence of numbers is truly random is often more challenging than generating the sequence in the first place.

In a new study, researchers have developed a new algorithm that increases the amount of certified randomness in a sequence of seemingly random numbers that has been generated experimentally. The researchers, Piotr Mironowicz *et al*., at universities in Poland, Sweden, and Brazil, have published their paper on the new random number certification algorithm in a recent issue of the *New Journal of Physics*.

As the scientists explain, generating long sequences of numbers with certified randomness is critical for ensuring security in computers, cell phones, and other electronic devices.

"Every electronic device needs randomness and needs a lot of it," coauthor Marcin Pawłowski at the University of Gdańsk in Poland told *Phys.org*. "Randomness is necessary whenever you need security. Whenever you want secure communication, a cryptographic key must be generated. It has to be generated randomly so that no adversary can easily guess it. Nowadays, every communication is encrypted that way. Whenever you call someone on your mobile phone or send a text, a sequence of random numbers has to be generated. If someone can predict these numbers (it doesn't have to be perfect—if he or she can guess some of them it's enough), they can listen to your conversation.

"Random numbers are constantly being generated by every machine that can communicate. And even if it does not communicate, every computer needs randomness to allocate programs in the memory. It is trivial to hack a computer which assigns the same place in its memory for the same program every time it's run. Exploiting backdoors or malfunctions in random number generators is one of the most common ways to attack communication or computer systems."

Lots of numbers, no pattern

Although it's relatively easy to generate and certify short sequences of random numbers, cryptographic applications require long sequences of random numbers, and the length is what makes the task much more challenging.

In general, researchers use two main methods to generate long sequences of random numbers. The first method is based on exploiting the randomness inherent in physical systems, such as the optical noise in lasers and radioactive decay in atoms. This randomness can be traced back to these systems' quantum properties. The second method uses computer software that can perform complicated arithmetical procedures. Technically, only the first method produces truly random numbers. The computer-generated numbers are considered "pseudorandom" because knowing how the program develops its computations makes it possible to predict these numbers, which only appear random.

In the new study, the researchers use the first method, by measuring the quantum states of some physical system. However, the physical method has its own problems: How do you know for sure that the measurement devices used to measure the physical system don't have some underlying predictability due to the way they were constructed? To overcome this problem, scientists have developed strict requirements on the devices,

but these "device-independent" protocols are so strict that they are very slow at generating large amounts of random numbers.

As a compromise between security and efficiency, researchers have developed "semi-device-independent" protocols that don't have such strict requirements, but do place limits on the device capacity. These protocols can generate truly random numbers, but they still require a large amount of post-processing computational power to certify that the sequences are random.

More randomness with more computing power

In the new paper, the researchers' main contributions is showing that a tradeoff exists for semi-device-independent protocols. The more computational power that is available to analyze the experimental data and certify its randomness, the less strict the requirements need to be on the measurement devices that generate the random data in the first place.

Based on this tradeoff, the researchers designed a new algorithm that can extract more data from the experiment, and then, using a large amount of computing power, can certify a large amount of randomness—more than any other method developed to date. Even more importantly, it can do so faster and even work in cases where slower methods don't work at all.

"Our method allows to certify more randomness than the standard one," Pawłowski said. "Let's assume that you are using the latter and get 1 bit/second and using ours you get 2 bits/second. It means that the same device certified with our method need half the time to produce the required mount of bits. It's nice.

"But there are cases when our method certifies 1 bit/sec and the standard one 0. Now our method becomes really important because without it we

have a completely useless device. I think this is its biggest advantage—making useless devices useful."

The new method also has the advantage that it doesn't require altering the physical quantum system like other methods do, although it does come at the cost of requiring greater computing power. Nevertheless, the researchers believe that this is a worthwhile tradeoff, and expect that the new approach will guide future research on random number certification.

"We have demonstrated the usefulness of our method in one case, but we have preliminary results and hand-weaving arguments that suggest that our method may be applied for different experimental setups and scenarios (for example, fully device-independent or with one party fully trusted)," Pawłowski said. "We are now trying to prove this and see in which situations it is most useful. Our second goal is to try to reduce the time of computation required for certifying more randomness. We have some preliminary results here too, which suggest it can be done."

More information: Piotr Mironowicz *et al*. "Increased certification of semi-device independent random numbers using many inputs and more post-processing." *New Journal of Physics*. DOI: 10.1088/1367-2630/18/6/065004