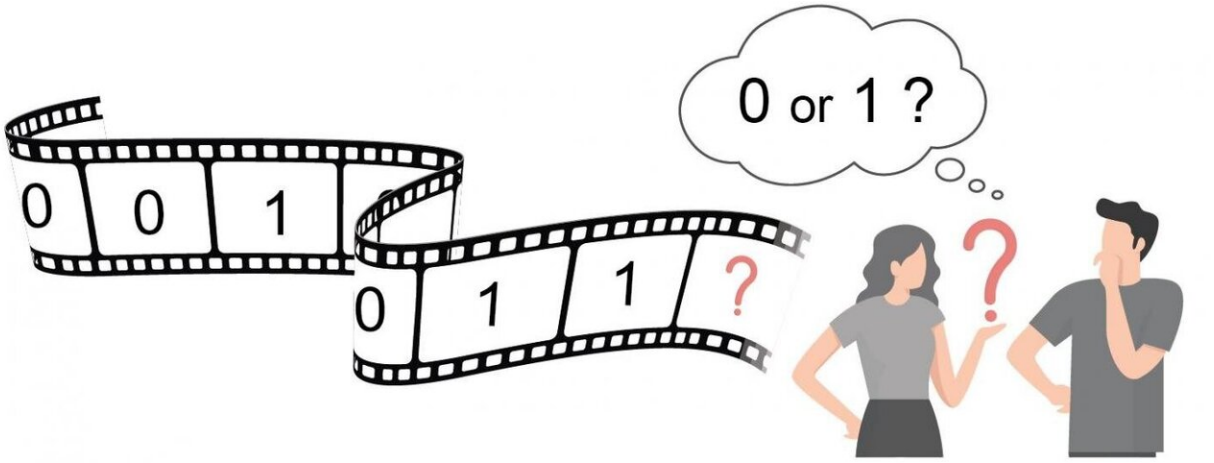
In classical and quantum secure communication practical randomness is incomplete

November 4 2019



Schematic of a random bit sequence, where the next bit has the same probability of being 0 or 1 Credit: Prof. Ido Kanter

Random bit sequences are key ingredients of various tasks in modern life and especially in secure communication. In a new study researchers have determined that generating true random bit sequences, classical or quantum, is an impossible mission. Based on these findings, they have demonstrated a new method of classified secure communication.

The mathematical definition of a random bit sequence is so simple that it

can be summarized in one sentence: A sequence of bits whose next bit is equal to 0 or 1 with equal probability, independent of previous ones. Although the definition is very simple, the practical certification of a process as random is much more complicated but crucial, for example, in secure communication, where information must be scrambled in order to prevent hackers from predicting a bit stream.

In an article to be published on November 5, 2019 in the journal *Europhysics Letters*, researchers at Bar-Ilan University demonstrate that long sequences with certified randomness by the US National Institute of Standard and Technology (NIST) are far from being truly random. Their work demonstrates that a large fraction of non-random bits can be systematically embedded in such bit sequences without negatively affecting their certified randomness. This discovery leads to a new type of classified secure communication between two parties where even the existence of the communication itself is concealed.

"The current scientific and technological viewpoint is that only non-deterministic physical processes can generate truly random bit sequences, which are conclusively verified by hundreds of very comprehensive statistical tests," said the study's lead author, Prof. Ido Kanter, of Bar-Ilan University's Department of Physics and Gonda (Goldschmied) Multidisciplinary Brain Research Center. Kanter's research group includes Shira Sardi, Herut Uzan, Shiri Otmazgin, Dr. Yaara Aviad and Prof. Michael Rosenbluh.

"We propose a reverse strategy, which has never been tested before. Our strategy aims to quantify the maximal amount of information that can be systematically embedded in a certified random bit sequence, without harming its certification," said Ph.D. students Shira Sardi and Herut Uzan, the key contributors to the research.

Using such a strategy, the level of randomness can be quantified beyond

the binary certification. In addition, since the information is systematically embedded in the bit sequence, the approach offers a new cryptosystem, similar to steganography, where the existence of any communication is completely concealed.

"According to the fundamental principles of quantum physics, the randomness of quantum random bit generators is expected to be perfect. In practice, however, this perfect quantum randomness may be diminished by many experimental imperfections, said Prof. Kanter. "Hence, a sequence generated by a quantum number generator ultimately has to be certified by statistical tests which can differentiate between original quantum guaranteed sequences and spurious ones. However, the newly-discovered incompleteness of practical randomness is expected to disrupt even quantum random number generators."

The new viewpoint presented in this work calls for a reevaluation of the quantified definition of measuring classical and quantum randomness, as well as its application to secure communication.

More information: *Europhysics Letters*, DOI: 10.1209/0295-5075/127/60003

Provided by Bar-Ilan University