

# Application of Detection-Loophole-Free Tests of Quantum Nonlocality

B. G. Christensen, K. T. McCusker, J. Altepeter, B. Calkins, T. Gerrits, A. Lita, A. Miller, L. K. Shalm, Y. Zhang, S. W. Nam, N. Brunner, C. C. W. Lim, N. Gisin, P. G. Kwiat

In 1935, Einstein, Podolsky, and Rosen suggested that certain quantum mechanical states must violate one or both of the fundamental classical assumptions of *locality* (sufficiently distant events cannot change the outcome of a nearby measurement) and *realism* (the outcome probabilities of potential measurements depend only on the state of the system). These *nonclassical* two-particle states exhibit multiple-basis correlations, and are referred to as “entangled”. Because locality and realism are so fundamental to classical intuition, a central debate in 20<sup>th</sup> century physics (1) revolved around the following question: could an alternative to quantum mechanics---a local realistic theory---explain entanglement’s seemingly nonclassical correlations? In 1964, John Bell devised a way to in principle answer this question experimentally, by analyzing the limit of allowed correlations between measurements made on an ensemble of any classical system (2). If performed under sufficiently ideal conditions, a violation of Bell’s inequality would *conclusively rule out all possible local realistic theories*. Although entanglement has been experimentally demonstrated and the Bell inequality violated in a myriad of non-ideal experiments, each of these experiments fails to overcome at least one of two critical obstacles, and has required additional assumptions to validate the experiment.

The first obstacle – the “locality loophole” – addresses the possibility that a local realistic theory might rely on some type of signal sent from one entangled particle to its partner (e.g., a signal containing information about the specific measurement carried out on the first particle). The second obstacle – the “detection loophole” – addresses the fact that entangled particles, when measured with low-quantum-efficiency detectors, will produce experimental results that can be explained by a local realistic theory. To avoid this, almost all previous experiments have had to make “fair sampling” assumptions that the collected photons are “typical” of those emitted. Here we report on the first experiment that fully closes the detection loophole with photons.

The high entanglement quality of our source, along with the detection-loophole-free capability, offers interesting possibilities for applications, notably for “device-independent” quantum information processing. Here the goal is to implement a certain protocol, and to guarantee its security, without relying on assumptions about the internal functioning of the devices used in the protocol. Being device-independent, this approach is more robust to device imperfections compared to standard protocols, and is in principle immune to side-channel attacks. By performing local measurements on entangled particles, and observing nonlocal correlations between the outcomes of these measurements, it is possible to certify the presence of genuine randomness in the data in a device-independent way. Device-independent randomness expansion (DIRE) was recently demonstrated in a proof-of-principle experiment using entangled atoms located in two traps separated by one meter (3); however, the resulting 42 random bits required a month of data collection. Here we show that our setup can be used to implement DIRE much more efficiently, where we generate 8700 secure bits of private randomness over 3 hours of data acquisition, achieving rates over 4 orders of magnitude beyond all past experiments.

1. A. Einstein, B. Podolsky, N. Rosen, *Phys. Rev.* **47**, 777-780 (1935).
2. J. Bell, *Physics* **1**, 195 (1964).
3. S. Pironio, *et al.*, *Nature* **464**, 1021-1024 (2010).