Abstract Submitted
for the MAR17 Meeting of
The American Physical Society

Experimentally Generated Random Numbers Certified by the Impossibility of Superluminal Signaling PETER BIERHORST, LYNDEN K. SHALM, NIST - Boulder, ALAN MINK, STEPHEN JORDAN, YI-KAI LIU, NIST - Gaithersburg, ANDREA ROMMAL, Muhlenberg College, SCOTT GLANCY, NIST - Boulder, BRADLEY CHRISTENSEN, University of Wisconsin-Madison, SAE WOO NAM, EMANUEL KNILL, NIST - Boulder — Random numbers are an important resource for applications such as numerical simulation and secure communication. However, it is difficult to certify whether a physical random number generator is truly unpredictable. Here, we exploit the phenomenon of quantum nonlocality in a loophole-free photonic Bell test experiment to obtain data containing randomness that cannot be predicted by any theory that does not also allow the sending of signals faster than the speed of light. To certify and quantify the randomness, we develop a new protocol that performs well in an experimental regime characterized by low violation of Bell inequalities. Applying an extractor function to our data, we obtain 256 new random bits, uniform to within $10^{-}3$.

Peter Bierhorst
NIST - Boulder

Date submitted: 07 Nov 2016 Electronic form version 1.4