Abstract Submitted
for the CUWIP21 Meeting of
The American Physical Society

Generating True Randomness through Quantum Entanglement[1]
ALIZA SIDDIQUI, Department of Physics and Astronomy, Louisiana State University, GAUTAM KAVURI, Department of Physics, 390 UCB University of Colorado, MOHAMMAD ALHEJJI[2], JILA, University of Colorado, 440 UCB, Boulder, CO, YANBAO ZHANG, NTT Basic Research Laboratories and NTT Research Center for Theoretical Quantum Physics, MICHAEL MAZUREK, Associate of the National Institute of Standards and Technology, MARTIN STEVENS, RICHARD MIRIN, SAE WOO NAM, National Institute of Standards and Technology, LYNDEN SHALM, Associate of the National Institute of Standards and Technology — Applications of randomness ranging from cryptography to prevention of gerrymandering require immediate access to certified random bits. Current random number generators (RNGs) output a sequence of binary bits in a random pattern based on a given entropy source such as user activity or radioactive decay. For instance, the National Institute of Standards and Technology (NIST) currently has a public randomness beacon that generates 512 random bits per minute using various hardware and algorithmic entropy sources. In general, a public randomness beacon is a service that emits random bits at a regular interval and is used in several cryptographic applications. However, with regular RNGs, there are three main unsolvable issues: one cannot directly certify the randomness of the output bits, you cannot guarantee the randomness of the underlying process, and you cannot vouch for the security of the system. Recently, NIST has developed a new kind of random number generator that uses quantum entanglement to address the first two issues, and does not need to make detailed assumptions about the underlying device implementation. In this talk I'll discuss how NIST plans to incorporate the random bits generated using entanglement into their next-generation randomness beacon.

[1]Generating True Randomness through Quantum Entanglement
[2]Department of Physics, University of Colorado, Boulder, Colorado, USA

Aliza Siddiqui
Louisiana State University

Date submitted: 04 Jan 2021 Electronic form version 1.4