Abstract Submitted
for the MAR15 Meeting of
The American Physical Society

Certifying Unpredictable Randomness from Quantum Nonlocality PETER BIERHORST, Tulane University — A device-independent quantum randomness protocol takes an initial random seed as input and then expands it in to a longer random string. It has been proven that if the initial random seed is trusted to be unpredictable, then the longer output string can also be certified to be unpredictable by an experimental violation of Bell's inequality. It has furthermore been argued that the initial random seed may not need to be truly unpredictable, but only uncorrelated to specific parts of the Bell experiment. In this work, we demonstrate rigorously that this is indeed true, under assumptions related to "no superdeterminism/no conspiracy" concepts along with the no-signaling assumption. So if we assume that superluminal signaling is impossible, then a loophole-free test of Bell's inequality would be able to generate provably unpredictable randomness from an input source of (potentially predictable) classical randomness.

Peter Bierhorst
Tulane University

Date submitted: 14 Nov 2014 Electronic form version 1.4