

Abstract

AMPLIFYING, GENERATING, OR CERTIFYING RANDOMNESS

A security test logic system can include a non-transitory memory configured to store measurements from a measurement apparatus, the measurement outputs comprising indications of presence or absence of coincidences where particles are detected at more than one detector at substantially the same time, the detectors being at the end of different channels from a particle source and having substantially the same length. The system can include a processor configured to compute a test statistic from the stored measurements. The test statistic may express a Bell inequality, and the system can compare the test statistic with a threshold. The processor can be configured to generate and output a certificate certifying that the measurements are from a quantum system if the value of the computed test statistic passes the threshold.

Figure 1