CLAIMS

1. A system for generating a random bit string, the system comprising:

a weak source of randomness configured to repeatedly generate a first bit string and a second bit string, the first bit string and the second bit string generated in one instance not necessarily having the same values as the first bit string and the second bit string generated in another instance;

a quantum apparatus configured to receive one or more of the second bit strings and, for each of one or more of the second bit strings the quantum apparatus receives, to output an associated third bit string, wherein the quantum apparatus comprises a plurality of quantum systems;

a security test logic system configured to compute a test statistic, for each of such one or more of the second bit strings the quantum apparatus receives, using the second bit string and the associated third bit string;

the security test logic system configured to determine whether to accept or reject the associated third bit string based at least in part on the computed test statistic, and to determine whether the plurality of quantum systems are approximately non-signaling; and

a two-source extractor configured to receive, if the security test logic system accepts the associated third bit string, a bit string based on one or more of the first bit strings and a bit string based on one or more of the third bit strings and to generate the random bit string.

2. The system of claim 1, wherein the quantum apparatus comprise a photonics device.
3. The system of claim 1, wherein the plurality of quantum systems comprise 2 or 4 quantum systems, each of the 2 or 4 quantum systems comprising a qubit.
4. The system of claim 3, wherein each of the plurality of quantum systems comprises a measurement device configured to perform a measurement on the qubit and to output a bit that comprises a result of the measurement.
5. The system of claim 1, wherein the security test logic system is further configured to:

compute a first test in which a violation of a Bell inequality is measured;

compute a second test to determine whether the plurality of quantum systems are approximately non-signaling; and

accept the associated third bit string in response to the violation of the Bell inequality and determining that the plurality of quantum systems are approximately non-signaling.

6. The system of claim 1, wherein the weak source of randomness comprises at least a first weak source of randomness to generate the first bit string and a second weak source of randomness to generate the second bit string.
7. The system of claim 1, wherein the associated third bit string is generated based at least in part on a plurality of measurement settings selected using the one or more of the second bit strings.
8. The system of claim 4, wherein the plurality of quantum systems comprises a detection system comprising the measurement device in each of the plurality of quantum systems, wherein the detection system comprises a plurality of detectors, wherein each measurement device comprises at least one of the plurality of detectors, and wherein the test statistic is computed based at least in part on indications of presence or absence of coincidences associated with particles being detected by the plurality of detectors in the detection system at substantially the same time.
9. The system of claim 1, wherein the security test logic system is further configured to:

select a plurality of measurement settings;

perform a first plurality of measurements using the plurality of selected measurement settings;

generate baseline histograms from the first plurality of measurements;

perform a second plurality of measurements using the plurality of selected measurement settings;

generate test histograms from the second plurality of measurements; and

determine that the plurality of quantum systems are approximately non-signaling based at least in part on a comparison between the baseline histograms and the test histograms.

10. The system of claim 1, wherein the security test logic system is further configured to compute a second test statistic and determine whether to accept or reject the associated third bit string based at least in part on the computed second test statistic.

11. The system of claim 1, wherein each of the plurality of quantum systems comprises a state expander configured to produce a qubit.

12. The system of claim 4, wherein the security test logic system comprises:

a non-transitory memory configured to store the result of the measurement, and

a processor configured to compute the test statistic based at least in part on the stored result.

13. A system for generating a random bit string, the system comprising:

a weak source of randomness configured to repeatedly generate a first bit string and a second bit string, the first bit string and the second bit string generated in one instance not necessarily having the same values as the first bit string and the second bit string generated in another instance;

a quantum apparatus configured to receive one or more of the second bit strings and to output an associated third bit string, wherein the quantum apparatus comprises a plurality of quantum systems;

a security test logic system configured to perform:

a first security test configured to compute a test statistic, for each of such one or more of the second bit strings the quantum apparatus receives, using the second bit string and the associated third bit string; and

a second security test configured to:

select a plurality of measurement settings;

perform a first plurality of measurements using the plurality of selected measurement settings;

generate baseline histograms from the first plurality of measurements;

perform a second plurality of measurements using the plurality of selected measurement settings;

generate test histograms from the second plurality of measurements; and

determine that the plurality of quantum systems are approximately non-signaling based at least in part on a comparison between the baseline histograms and the test histograms;

wherein the security test logic system is further configured to determine whether to accept or reject the associated third bit string based at least in part on the first security test and the second security test; and

a two-source extractor configured:

to receive, if the security test logic system accepts the associated third bit string, a bit string based on one or more of the first bit strings and a bit string based on one or more of the third bit strings; and

to generate the random bit string.

14. The system of claim 13, wherein the quantum apparatus comprises a photonics device.
15. The system of claim 13, wherein the plurality of quantum systems comprise 2 or 4 quantum systems, wherein each quantum system generates a qubit.
16. The system of claim 15 wherein each of the plurality of quantum systems comprises a measurement device configured to perform a measurement on the qubit and to output a bit that comprises a result of the measurement.
17. The system of claim 13, wherein the weak source of randomness comprises at least a first weak source of randomness to generate the first bit string and a second weak source of randomness to generate the second bit string.
18. The system of claim 13, wherein the associated third bit string is generated based at least in part on a second plurality of measurement settings selected using the one or more of the second bit strings.
19. The system of claim 16, wherein the plurality of quantum systems comprises a detection system comprising the measurement device in each of the plurality of quantum systems, wherein the detection system comprises a plurality of detectors, wherein each measurement device comprises at least one of the plurality of detectors, and wherein the test statistic is computed based at least in part on indications of presence or absence of coincidences associated with particles being detected by the plurality of detectors in the detection system at substantially the same time.
20. The system of claim 16, wherein the security test logic system comprises:

a non-transitory memory configured to store the result of the measurement, and

a processor configured to compute the test statistic based at least in part on the stored result.

21. The system of claim 13, wherein the test statistic comprises determining a level of violation of a Bell inequality.
22. The system of claim 21, wherein the Bell inequality comprises a CHSH (Clauser Horne Shimony Holt) inequality.
23. The system of claim 13, wherein each of the plurality of quantum systems comprises a state expander configured to produce a qubit.
24. The system of claim 13, wherein the security test logic system is further configured to compute a second test statistic and determine whether to accept or reject the associated third bit string based at least in part on the computed second test statistic.