CLAIMS

1. A method of generating a random bit string, the method comprising:

providing a weak source of randomness;

providing a quantum device configured to entangle a plurality of quantum particles in a quantum state;

measuring each of the plurality of particles in two different bases;

determining a level of violation of a Bell inequality;

determining whether to accept or abort based at least partly on the determined level of violation; and

extracting the random bit string via a two-source extractor.

2. The method of claim 1, wherein the Bell inequality comprises the CHSH (Clauser Horne Shimony Holt) inequality.

3. The method of claim 1, wherein the plurality of quantum particles is 2 or 4.

4. The method of claim 1, wherein determining whether to accept or abort comprises determining whether the quantum device satisfies a non-signaling criterion.

5. The method of claim 4, wherein the non-signaling criterion comprises a criterion for approximate non-signaling.

6. 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 second bit string generated in one instance not necessarily having the same values as the first bit string and 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 at least in part based 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 output of the quantum apparatus, 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.

7. The system of claim 6, wherein the quantum apparatus comprises a photonics device.

8. The system of claim 6, wherein the quantum apparatus comprises 2 or 4 quantum systems, each quantum system comprising a qubit.

9. The system of claim 6, wherein the quantum system comprises a measurement device configured to perform a measurement on the qubit and to output a bit that comprises a result of the measurement.

10. The system of claim 8, wherein the security test logic system is configured to compute:

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

a second test to determine whether two or more quantum systems are approximately non-signaling.

11. A system configured to output a random bit, the system comprising:

a quantum generator configured to generate an entangled pair of particles, a and a';

a first state expansion device configured to generate an entangled state comprising a and b;

a second state expansion device configured to generate an entangled state comprising a' and b';

a first measurement device configured to perform a coincidence measurement relating to a two-fold coincidence of ab or $a'b$ or ab' or $a'b'$;

a second measurement device configured to measure violation of a Bell inequality and to determine whether the entangled states are non-signaling; and

a two-source extractor configured to receive input from the second measurement device and to output a random bit.

12. A security test system comprising:

a non-transitory memory configured to store measurement outputs 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; and

a processor configured to:

compute a test statistic from the stored measurement outputs, the test statistic expressing a Bell inequality;

compare the test statistic with a threshold; and

generate a certificate certifying that the measurement outputs are from a quantum system if the value of the computed test statistic is below the threshold.

13. The security test system of claim 12 wherein the processor is configured to compute the test statistic by multiplying the reciprocal of a number of rounds of measurements by the sum, over the set of the rounds of measurements, of binary-valued array entries corresponding to the rounds of measurements, the corresponding entries determined according to values of measurement settings of detectors used in the measurement apparatus when individual ones of the rounds of measurements were made.

14. The security test system of claim 13 wherein the array acts to assess the coincidences as being evidence for or against quantum effects having generated individual ones of the measurements.

15. The security test system of claim 12 wherein the channels carry qubits which are in either of the following quantum states: a quantum state equal to the reciprocal of the square root of two times the sum of the quantum states of two pairs of qubits, where the

quantum states of the pairs of qubits are entangled and in superposition; or a quantum state equal to one half of the sum, over i from 0 to 3, of the tensor product of a qubit on an i^{th} channel with the same qubit.

16. The security test system of claim 12 wherein the processor is further configured to test for interaction between the individual measurement devices within the measurement apparatus, by creating a baseline histogram from the measurements and comparing the baseline histogram with one or more test histograms of measurements obtained from the measurement apparatus.

17. The security test system of claim 12 wherein the processor is further configured to compute a second test statistic and take the second test statistic into account before deciding whether to generate the certificate.

18. An apparatus for creating a quantum superposition of a photon, the apparatus comprising:

at least one pair of waveguides, each waveguide comprising a plurality of blocks of light-displacing material interspersed with a plurality of polarization modifiers; and

an input to receive a pair of entangled photons, the photons having mutually orthogonal polarizations, the input connected to the pair of waveguides such that each waveguide receives one of the pair of entangled photons and guides the entangled photon within the waveguide through the blocks of light-displacing material and the polarization modifiers to create a quantum superposition of the photon whereby there are a plurality of possible paths the photon follows within the waveguide along which polarization is changed;

wherein each waveguide is sized and shaped such that, for each entangled photon a length of a path travelled by the photon through the waveguide is substantially the same irrespective of the mutually orthogonal polarizations of the entangled photons.

19. The apparatus of claim 18 comprising, for each waveguide, a pair of output optical fibres, each output optical fibre of a pair being configured to accept light which is

polarized in one of the mutually orthogonal polarizations and to discard light which is polarized in the other mutually orthogonal polarization.

20. The apparatus of claim 18 wherein the plurality of blocks of light-displacing material comprise at least one block formed of a material that displaces light in a first direction, and at least one block formed from material that displaces light in a second direction different from the first direction.

21. The apparatus of claim 20 wherein the at least one block that displaces light in a first direction is made from an up-air crystal, and the at least one block that displaces light in the second direction is made from a down-air crystal.

22. The apparatus of claim 18 wherein the plurality of blocks of light-displacing material are made of the same material.

23. The apparatus of claim 18 wherein the blocks of light-displacing material are made from one or more of: calcite, lithium niobate.

24. The apparatus of claim 18, wherein the apparatus comprises six blocks of light-displacing material.

25. The apparatus of claim 24 wherein the six blocks of light-displacing material are made from up-air crystal and down-air crystal arranged in the following sequence from an output end of the waveguide to an input end of the waveguide: down-air crystal, up-air crystal, up-air crystal, down-air crystal, down-air crystal, up-air crystal.

26. The apparatus of claim 25 wherein the polarization modifiers are placed in the sequence of blocks of light-displacing material in the following order from an output end of the waveguide to an input end of the waveguide and with or without the following air gaps: polarization modifier, air gap, down-air crystal, polarization modifier, up-air crystal, air gap,

polarization modifier, air gap, up-air crystal, polarization modifier, down-air crystal, air gap, polarization modifier, air gap, down-air crystal, polarization modifier, up-air crystal.

27. The apparatus of claim 18 wherein the polarization modifiers are half wave plates.

28. The apparatus of claim 18 wherein a plurality of the polarization modifiers are separated from adjacent ones of the blocks of light-displacing material by air gaps.

29. The apparatus of claim 28 wherein a second plurality of the polarization modifiers are in contact with adjacent ones of the blocks of light-displacing material.

30. The apparatus of claim 18 wherein at least one of the polarization modifiers comprises a region through which light passes without modification of polarization.

31. The apparatus of claim 18 further comprising a casing holding the apparatus, the casing being formed from material that reduces one or more of: the influence of atmospheric pressure, vibration, humidity on the waveguides.

32. The apparatus of claim 18 further comprising a cooling chamber holding the waveguides and configured to reduce the temperature of the waveguides to around negative twenty degrees Celsius.

33. A method for creating superposition of states, the method comprising:

receiving from a generator a pair of entangled photons, the photons having mutually orthogonal polarizations; and

inputting the pair of entangled photons to a pair of waveguides, such that each waveguide receives one of the pair of entangled photons and guides the entangled photon within the waveguide along its length to create a quantum superposition of the entangled photon whereby there are a plurality of possible paths the entangled photon follows within the waveguide along which polarization is changed;

wherein each waveguide is sized and shaped such that, for each entangled photon, a length of a path travelled by the entangled photon through the waveguide is substantially the same irrespective of the mutually orthogonal polarizations of the entangled photons in the pair of entangled photons.

34. An apparatus for detecting entangled photon pairs that are in superposition in a stream of photons comprising both entangled photon pairs and classical photons, the apparatus comprising:

at least one pair of measuring devices, each measuring device comprising:

a plurality of detectors, each detector arranged to detect single photons;

detector configuration apparatus, to automatically configure according to values of control parameters, for each detector, a measurement basis of the detector;

a photon input having two photon paths, one path for each of two possible mutually orthogonal photon polarizations, each photon path travelling to a different one of the detectors and wherein the photon paths within a single measuring device are substantially the same length;

wherein the photon paths of the measuring devices in the pair are substantially the same length.

35. The apparatus of claim 34 comprising one or more processors configured to assess the occurrence of coincidences, where a coincidence comprises photons detected at more than one of the detectors within a time interval of about 15 nanoseconds or shorter, and where the one or more processors check whether a detector in a first one of a pair of the measuring devices detects a photon at a first time and a detector in the other one of the pair of the measuring devices detects a photon within the time interval relative to the first time, wherein occurrence of a coincidence indicates a likelihood that the detectors detected an entangled photon in superposition.

36. The apparatus of claim 35 wherein the one or more processors check coincidences at which photons are detected at the detectors within a single measuring device, such that if a detector in the single measuring device detects a photon at a first time and another detector in the single measuring device detects a photon within a specified time of the first time, there is a likelihood that the detected photon is a classical photon.

37. The apparatus of claim 34 wherein each of the measuring devices comprises four detectors comprising a first pair of detectors for each of two mutually orthogonal polarizations,

and a second pair of detectors for each of two mutually orthogonal polarizations, where the first pair of detectors operates for a first optical mode and the second pair of detectors operates for a second optical mode.

38. The apparatus of claim 34 wherein the detector configuration apparatus comprises an apparatus to change a number of radians of a phase shift between two orthogonal values, and to change a first polarization to a second polarization, for use by individual ones of the detectors.

39. The apparatus of claim 34 wherein the detector configuration apparatus is configured to receive the values of the control parameters from a first weak source of randomness.

40. The apparatus of claim 34 wherein the detector configuration apparatus is configured to receive the values of the control parameters as four bits.

41. The apparatus of claim 34 wherein an output of the apparatus comprises, for each measurement device, two bits, each bit representing whether a photon was detected or not in a given measurement basis.