

Claims

1. A quantum random number generation (QRNG) system, including:
a single-photon or equivalent single-photon light source;
a beam splitter arranged to direct output from the light source to a first
5 homodyne detector having a first local oscillator and a second homodyne
detector having a second local oscillator; and
a signal control and processing unit configured to:
vary the phases of the first and second local oscillators;
receive, from the first and second homodyne detectors, a plurality of
10 measurements of the output, said plurality of measurements being
dependent on the intensity of the light source and the phases of the first and
second local oscillators;
determine, from the plurality of measurements, whether the CHSH
inequality is satisfied; and
15 output one or more random numbers based on whether the CHSH
inequality is satisfied.
2. A QRNG system according to claim 1, wherein the light source is configured
to generate a plurality of coherent states of varying intensity, and wherein
the system includes an attenuator for attenuating the output to single-
20 photon level.
3. A QRNG system according to claim 1 or claim 2, wherein the signal control
and processing unit is configured to determine a set of single photon
correlation probabilities from said plurality of measurements; and
determine, based on the set of single photon correlation probabilities,
25 whether the CHSH inequality is satisfied.
4. A QRNG system according to any one of claims 1 to 3, wherein the signal
control and processing unit is configured to apply a threshold to respective
measurements prior to determining whether the CHSH inequality is
satisfied.

- 22 -

5. A QRNG system according to any one of claims 1 to 4, wherein the signal control and processing unit is configured to apply a randomness extractor to the one or more random numbers.
6. A QRNG system according to claim 5, wherein the randomness extractor is
5 a universal hashing function.
7. A quantum random number generation (QRNG) method, including:
directing, by a beam splitter, output from a single-photon or equivalent
single-photon light source to a first homodyne detector coupled to a first local
oscillator and a second homodyne detector coupled to a second local oscillator;
10 varying the phases of the first and second local oscillators;
receiving at a signal control and processing unit, from the first and second
homodyne detectors, a plurality of measurements of the output, said plurality
of measurements being dependent on the intensity of the light source and the
phases of the first and second local oscillators;
15 determining, from the plurality of measurements, whether the CHSH
inequality is satisfied; and
outputting one or more random numbers based on whether the CHSH
inequality is satisfied.
8. A QRNG method according to claim 7, wherein the light source is
20 configured to generate a plurality of coherent states of varying intensity;
and wherein the method includes attenuating the output to single-photon
level.
9. A QRNG method according to claim 7 or claim 8, including determining a
set of single photon correlation probabilities from said plurality of
25 measurements; and determining, based on the set of single photon
correlation probabilities, whether the CHSH inequality is satisfied.
10. A QRNG method according to any one of claims 7 to 9, including applying
a threshold to respective measurements prior to determining whether the
CHSH inequality is satisfied.

- 23 -

11. A QRNG method according to any one of claims 7 to 10, including applying a randomness extractor to the one or more random numbers.
12. A QRNG method according to claim 11, wherein the randomness extractor is a universal hashing function.
- 5 13. A photonic chip including a QRNG system according to any one of claims 1 to 6, and/or configured to implement a QRNG method according to any one of claims 7 to 12.