perform a test on the first random bit string received from the quantum device to confirm quantum behaviour by the quantum device in generating the received random bit string;

on condition that the test provides a confirmation of quantum behaviour, generate one or more cryptographic keys using the first random bit string;

encrypt the one or more cryptographic keys; and

transmit the encrypted one or more cryptographic keys via the client interface to the client in response to receiving the request from the client.

Also disclosed is a system for providing a random bit string for use in one or more cryptographic applications, the system comprising:

an electronic processor that executes specific computer-executable instructions stored in a non-transitory memory to provide a two-source randomness extractor and a seeded randomness extractor, wherein the specific computer-executable instructions when executed cause the electronic processor to at least:

receive, by the two-source randomness extractor, from a first source of randomness a first input comprising a first random bit string having an input length, represented by n, a first min-entropy, and a first min-entropy rate;

receive, by the two-source randomness extractor, from a second source of randomness a second input comprising a second random bit string having a second min-entropy and a second min-entropy rate;

generate and output, by the two-source randomness extractor, a third random bit string derived from the first and second random bit strings, the third random bit string having a third min-entropy rate which has been amplified to be greater than at least the first min-entropy rate;

receive, by the seeded randomness extractor, from the second source of randomness, a fourth random bit string having a fourth min-entropy, wherein the fourth min-entropy is less than a third min-entropy of the third random bit string;

receive, by the seeded randomness extractor, the third random bit string as a seed; and

generate, by the seeded randomness extractor, a fifth random bit string using the third and fourth random bit strings;

wherein a length of the third random bit string, represented by m, is asymptotically proportional to a sum of the first and second min-entropies minus

the input length (n); and wherein the two-source randomness extractor has a complexity of order equal to or less than $n \times \log(n)$; and

a key generation system that receives the fifth random bit string and uses the fifth random bit string to generate a cryptographic key used in encryption or decryption of data.

Also disclosed is a cryptographic system comprising a secure user environment including:

a store containing one or more seeds, each seed comprising or generated from a first random bit string which is certified as produced by quantum behaviour within a quantum device;

a first private source of randomness configured to generate and output a second random bit string; and

a seeded randomness extractor configured to receive a first input comprising a seed from the store and a second input comprising the second random bit string, wherein the randomness extractor is further configured to generate and output a third random bit string in response to a user request, the third random bit string being usable for forming a cryptographic key, wherein the third random bit string has amplified entropy compared to the second random bit string.

Also disclosed is a system for generating a random bit string, the system comprising:

at least one weak source of randomness configured to generate a first bit string and a second bit string;

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

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

a two-source randomness extractor configured to receive the first bit string and the third bit string and to generate a fourth random bit string.

Also disclosed is a method of generating a random bit string, the method comprising:

providing a weak source of randomness;

providing a quantum apparatus configured to generate plurality of quantum particles in an entangled quantum state;

measuring each of the plurality of particles in 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 using a two-source randomness extractor.

Also disclosed is a method of operating a system for providing a random bit string for use in one or more cryptographic applications, wherein the method comprises:

configuring a test system to receive a first random bit string having a first entropy and to perform a test using the first random bit string to confirm quantum behaviour in the generation of the first random bit string; and

configuring a two-source randomness extractor to:

receive a first input comprising the first random bit string for which the test has confirmed quantum behaviour in the generation of the first random bit string;

receive a second input comprising a second random bit string having a second entropy; and

generate and output a third random bit string derived from the first and second random bit strings, the third random bit string having a third entropy which has been amplified to be greater than both the first entropy and the second entropy.

Also disclosed is a method of operating a cryptographic software-as-a-service system for providing cryptographic keys to client users, wherein the method comprises:

configuring a client interface to receive a request from a client for a cryptographic key;

configuring a service interface to request and receive a first random bit string from a quantum device; and

configuring at least one processing component to:

perform a test on the first random bit string received from the quantum device to confirm quantum behaviour by the quantum device in generating the received random bit string;

on condition that the test provides a confirmation of quantum behaviour, generate one or more cryptographic keys using the first random bit string;

encrypt the one or more cryptographic keys; and

transmit the encrypted one or more cryptographic keys via the client interface to the client in response to receiving the request from the client.

Also disclosed is a method of operating a cryptographic system comprising a secure user, wherein the method includes:

configuring a store containing one or more seeds, wherein each seed comprises or is generated from a first random bit string which is certified as produced by quantum behaviour within a quantum device;

configuring a first private source of randomness to generate and output a second random bit string; and

configuring a seeded randomness extractor to receive a first input comprising a seed from the store and a second input comprising the second random bit string, wherein the randomness extractor is further configured to generate and output a third random bit string in response to a user request, the third random bit string being usable for forming a cryptographic key, wherein the third random bit string has amplified entropy compared to the second random bit string.

Also disclosed and defined in the claims of this patent specification are various methods and apparatus using non-deterministic random number generation and randomness verification, such as for use in cryptographic systems and applications.

Description of the drawings

The present invention will be better understood from the following detailed description, with reference to the accompanying drawings in which:

FIG. 1 is a schematic diagram of an example of an apparatus for certifying that a number has been produced by a quantum apparatus and of an example of a randomness extractor configured to generate a random number for use in a variety of downstream applications;

Claims

1. A system for providing a random bit string for use in one or more cryptographic applications, the system comprising:

an electronic processor that executes specific computer-executable instructions stored in a non-transitory memory to provide a two-source randomness extractor and a seeded randomness extractor, wherein the specific computer-executable instructions when executed cause the electronic processor to at least:

receive, by the two-source randomness extractor, from a first source of randomness a first input comprising a first random bit string having an input length, represented by *n*, a first min-entropy, and a first min-entropy rate;

receive, by the two-source randomness extractor, from a second source of randomness a second input comprising a second random bit string having a second min-entropy and a second min-entropy rate;

generate and output, by the two-source randomness extractor, a third random bit string derived from the first and second random bit strings, the third random bit string having a third min-entropy rate which has been amplified to be greater than at least the first min-entropy rate;

receive, by the seeded randomness extractor, from the second source of randomness, a fourth random bit string having a fourth min-entropy, wherein the fourth min-entropy is less than a third min-entropy of the third random bit string;

receive, by the seeded randomness extractor, the third random bit string as a seed; and

generate, by the seeded randomness extractor, a fifth random bit string using the third and fourth random bit strings;

wherein a length of the third random bit string, represented by *m*, is asymptotically proportional to a sum of the first and second min-entropies minus the input length (*n*); and wherein the two-source randomness extractor has a complexity of order equal to or less than *n x log(n)*; and

a key generation system that receives the fifth random bit string and uses the fifth random bit string to generate a cryptographic key used in encryption or decryption of data.

2. The system of claim 1, wherein the system is configured to receive the first random bit string over a public network from a source which is remote from the system, optionally wherein the system is configured to authenticate communications including the first random bit string received from the source over the public network.

3. The system of claim 1 or claim 2 wherein the test is a Bell test to confirm the presence of quantum entanglement as part of the generation of the first random bit string, optionally wherein the Bell test is evaluated against the Mermin inequality.

4. The system of any preceding claim, wherein the test system is configured to determine the level of entropy in the first random bit string, and optionally wherein the two-source randomness extractor is configured to use this determined entropy to generate the third random bit string having perfect entropy.

5. The system of any preceding claim, wherein the first random bit string is derived from measurement of states prepared by a quantum device.

6. The system of claim 5, wherein each of the states to be measured comprises 3 qubits, optionally wherein each of the states to be measured is a Greenberger-Home-Zeilinger state.

7. The system of claim 5 or 6, wherein the test system is configured to provide a measurement basis to the quantum device for making each state measurement, each measurement basis being taken from a set of multiple possible measurement bases, and wherein the test system uses the measurement bases and outcomes of the respective measurements of the states prepared by the quantum device to confirm quantum behaviour in the generation of the first random bit string.

8. The system of any of claims 5 to 7, wherein the test system is configured to perform multiple rounds of measurement of the state of the quantum device, optionally wherein the number of rounds is at least 10^5, 10^6, 10^7 or 10^8.

9. The system of any preceding claim, wherein the test system is configured to run a set of quantum circuits on a quantum computer, and optionally wherein the quantum circuits are customized to run on a given quantum computer.

10. The system of claim 9, wherein each quantum circuit is configured to: (i) prepare a state involving multiple qubits; (ii) perform a measurement on the prepared state, the measurement being taken from a set of multiple possible measurements; and (iii) output the measured state of the qubits at the end of the circuit as the measurement result.

11. The system of any preceding claim, wherein the two-source randomness extractor is configured to receive n1 bits of the first random bit string and n2 bits of the second random bit string and to output m bits of the third random bit string, wherein $m \leq n1+n2$.

12. The system of any preceding claim, wherein the two-source randomness extractor is a strong extractor, such that the output of the strong two-source randomness extractor, namely the third random bit string, is independent of any one of the two inputs thereto, namely the first and second random bit strings, such that either the first random bit string or the second random bit string could be made public without compromising secrecy of the third random bit string.

13. The system of claim 11 or 12, wherein the two-source randomness extractor is configured such that providing the first and second random bit strings have a combined min entropy rate of > 1, the third random bit string will have perfect entropy.

14. The system of claim 13, wherein the perfect entropy of the third random bit string is subject to a protocol error which reflects the probability that an adversary could distinguish the output from something that is perfectly uniformly distributed, wherein the probability is less than 2^{-32}, less than 2^{-64}, less than 2^{-128} or less than 2^{-256}.

15. The system of any preceding claim, wherein multiple fourth random bit strings can be used in succession with the same seed to produce multiple respective fifth random bit strings.

16. The system of claim 15, wherein the seeded randomness extractor is a strong extractor, such that the output of the strong seeded randomness extractor, namely the fifth random bit string, is independent of any one of the two inputs thereto, namely the third and fourth random bit strings, such that multiple fifth random bit strings can be produced from the same seed in combination with multiple respective fourth random bits strings without compromising secrecy of the seed, and optionally wherein the number of fifth random bits strings that can be produced from the same seed is limited by a security parameter.

17. The system of claim 16, wherein the seed has perfect entropy, and optionally wherein the perfect entropy of the seed is subject to a protocol error which reflects the probability that an adversary could distinguish the output from something that is perfectly uniformly distributed, wherein the probability is less than 2^{-32}, less than 2^{-64}, less than 2^{-128} or less than 2^{-256}.

18. The system of any of claims 15 to 17, wherein the system is configured to save the multiple fifth random bit strings into a database for use in creating cryptographic keys, optionally where the database is included in said system.

19. The system of any preceding claim, wherein at least one of the two-source randomness extractor and the seeded randomness extractor is implemented with complexity $\leq O(n \log(n))$, optionally using a number theoretic transform.

20. The system of any preceding claim, wherein at least one of the two-source randomness extractor and the seeded randomness extractor is implemented as a Dodis extractor.

21. The system of any preceding claim, wherein the two-source randomness extractor is the same as or shares an implementation with the seeded randomness extractor

22. The system of any preceding claim, wherein the system further comprises a first private random number generator configured to produce the second random bit string and to output the second random bit string to the two-source randomness extractor.

23. The system of claim 15 or any claim dependent thereon, wherein the system further comprises a second private random number generator configured to produce the fourth random bit string and to output the fourth random bit string to the seeded randomness extractor, wherein the second private random number generator optionally is the same as or shares an implementation with the first private random number generator.

24. The system of claim 22 or 23, wherein at least one of the first and second private random number generators comprises at least one of: a weak source of randomness; a source of imperfect randomness; a deterministic source of random numbers; a source of pseudo-random numbers; a source of random numbers that does not exhibit quantum behaviour; or any combination of the above.

25. The system of any of claims 22 to 24, wherein at least one of the second random bit string and further random bit string is produced by a block min-entropy source, wherein each block, comprising a fixed number of bits in the string, has a certain amount of min-entropy, even when conditioned on an adversary knowing all previous blocks and having a complete model of operation of the block min-entropy source,.

26. The system of any preceding claim, wherein the system is implemented within at least one of a trusted execution environment and a separate hardware module or separate chip of a computer.

27. A method of operating a system for providing a random bit string for use in one or more cryptographic applications, wherein the method comprises, by an electronic processor that executes specific computer-readable instructions stored in a non-transitory memory:

configuring a two-source randomness extractor to at least:

receive a first input comprising a first random bit string having an input length, represented by *n*, and first min-entropy and first min-entropy rate;

receive a second input comprising a second random bit string having a second min-entropy and second min-entropy rate;

generate and output a third random bit string derived from the first and second random bit strings, the third random bit string having a third min-entropy rate which has been amplified to be greater than both the first min-entropy rate and the second min-entropy rate;

receive a fourth random bit string; and

generate a fifth random bit string using the third random bit string and the fourth random bit string; and

configuring a key generation system to at least:

receive the fifth random bit string; and

use the fifth random bit string to generate a cryptographic key used in encryption or decryption of data;

wherein a length of the third random bit string, represented by *m*, is asymptotically proportional to a sum of the first min-entropy and the second min-entropy, minus the input length (*n*); and

wherein the two-source randomness extractor has a complexity of order equal or less than *n log(n)*.

28. The method of claim 27, further comprising configuring a test system to receive the first random bit string to perform a test to confirm quantum behavior in generation of the generation of the first random bit string.

29. The method of claim 28, wherein the two-source randomness extractor is a strong two-source randomness extractor, such that output of the strong two-source randomness extractor, namely the third random bit string, is independent of any one of the first and second random bit strings, such that either the first random bit string or the second random bit string could be made public without compromising secrecy of the third random bit string.

30. The method of claim 29, wherein the third random bit string has near-perfect entropy.

31. The method of claim 27, further comprising configuring a seeded randomness extractor to:

receive as a seed a first input comprising the third random bit string output by the two-source randomness extractor;

receive a second input comprising the fourth random bit string having a fourth min-entropy, wherein the fourth min-entropy is less than a third min-entropy of the third random bit string; and

generate and output the fifth random bit string derived from the third and fourth random bit strings, wherein multiple fourth random bit strings are used in succession with the seed to produce multiple respective fifth random bit strings.

32. The method of claim 31, wherein the seeded randomness extractor is a strong extractor, such that secrecy of the fifth random bit string, is independent of any one of the third and fourth random bit strings, such that multiple fifth random bit strings are produced from the seed in combination with multiple respective fourth random bits strings without compromising secrecy of the seed, and wherein a number of fifth random bits strings that are produced from the seed is limited by a security parameter.

33. The method of claim 27, the two-source randomness extractor generates the third random bit string at a rate larger than 10 Mbits/sec.

34. The method of claim 27, wherein the two-source randomness extractor uses circulant matrices to compute and output the third random bit string.

35. The method of claim 27, wherein configuring the two-source randomness extractor comprises implementing the two-source randomness extractor using a number theoretic transform (NTT).

36. The method of claim 31, wherein configuring the seeded randomness extractor comprises implementing the seeded randomness extractor using a number theoretic transform (NTT) that has a complexity of an order equal or less than n log(n).

37. The method of claim 27, wherein the first input is received from a first source of randomness having a guessing probability, represented by p1, the second input is received from a second source of randomness having a guessing probability, represented by p2, and the third random bit string has a security parameter (εSEC) greater than zero, and m is substantially equal to:

$$\frac{1}{5}[-log(p1 \times p2) - log\varepsilon_{sec}^{-8} + 10 - 4log3] - \frac{n}{5}.$$

38. The system of claim 1, wherein the first source of randomness has a guessing probability, represented by p1, the second source of randomness has a guessing probability represented by p2, the third random bit string has a security parameter (εSEC) greater than zero, and m is substantially equal to:

$$\frac{1}{5}[-log(p1 \times p2) - log\varepsilon_{sec}^{-8} + 10 - 4log3] - \frac{n}{5}.$$

39. The system of claim 1, wherein m is asymptotically proportional to the sum of the first and second min-entropies minus the input length (n) as n increases.

40. The method of claim 27, wherein m is asymptotically proportional to the sum of the first and second min-entropies minus the input length (n) as n increases.

41. The system of claim 4, wherein the test system is further configured to determine a level of entropy in the first random bit string; and wherein the two-source randomness extractor is configured to use the determined level of entropy to generate the third random bit string having near-perfect entropy.

42. The system of claim 25, and wherein the block min-entropy source is a Santha-Vazirani source.