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 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;