SUMMARY OF THE INVENTION

The invention is defined in the independent claims, to which reference is now directed. Preferred features are set out in the dependent claims.

In its broadest aspect, the invention provides a scheme that uses quantum information to obtain some of the important advantages of quantum money just outlined, in a way that is technologically feasible today. In particular, the token itself in the present schemes is classical, so that the invention does not rely on the presently problematic long-term storage or transportation of quantum states. In spite of this, embodiments of the invention provide a token that cannot be copied, and which is limited in transmission speed only by the light signalling bound. According to the invention, the future privacy of the token recipient may be respected; and certain embodiments within the scope of the invention may also guarantee past privacy.

According to one aspect of the invention, there is provided a method comprising the steps of: a recipient receiving from an issuing party, at a first space-time point, a plurality of random quantum states, wherein each of the quantum states is chosen from a set of non-orthogonal quantum states and the quantum states represent quantum bits, qubits, or qudits; the recipient applying a sequence of measurements, chosen from a plurality of possible pre-determined measurements, to the quantum states to generate classical measurement outcomes; the recipient generating a token comprising a sequence of classical measurement outcomes by recording the classical measurement outcomes for the sequence of measurements applied to the quantum states; the recipient transmitting to the issuing party data identifying the states for which the measurements were successful; and the recipient presenting to the issuing party, at a second space-time point in the causal future of the first space-time point, the token in return for access to a resource, wherein before applying the sequence of measurements, the recipient having agreed with the issuing party the plurality of possible pre-determined measurements that will generate classical measurement outcomes giving a valid token for the second space-time point; the measurements are chosen by the recipient from the plurality of possible pre-determined measurements in dependence on the space-time point at which the token is to be presented; and the token comprising a sequence of classical measurement outcomes that is valid at a single space-time point.

According to another aspect of the invention, there is provided a method comprising the steps of: an issuing party generating, at a first space-time point, a plurality of random quantum states, each of the quantum states chosen from a set of non-orthogonal quantum states and the quantum states represent quantum bits, qubits, or qudits; the issuing party receiving

from a recipient, at a second space-time point in the causal future of the first space-time point, a token comprising a sequence of classical measurement outcomes, and the issuing party receiving from the recipient data identifying the states for which the measurements were successful, wherein: the token is obtained by the recipient applying a sequence of measurements, chosen from a plurality of possible pre-determined measurements, to the quantum states to generate classical measurement outcomes and recording the classical measurement outcomes for the sequence of measurements applied to the quantum states; the issuing party and recipient agree the plurality of possible pre-determined measurements that will generate measurement outcomes giving a valid token for a second space-time point and the issuing party storing the classical measurement outcomes, and the measurements are chosen from the plurality of possible pre-determined measurements in dependence on the space-time point at which the token is to be presented, and the token comprises a sequence of classical measurement outcomes that is valid at a single space-time point. The method further includes the step of the issuing party verifying whether the token corresponds to a statistically plausible result for the pre-determined measurements applied to the plurality of quantum states, before allowing the recipient access to the resource.

References herein to events or to the performance of method steps 'at' a space-time point are intended to comprise occurrences within an agreed, small (four-dimensional) region around the relevant point. For example, as the skilled person will appreciate the exchange of information generally requires classical and/or quantum data to be sent through agreed channels between two nearby secure sites controlled respectively by either of the parties to the exchange.

Furthermore, the term 'random' is intended throughout to mean perfect or near-perfect randomness. In preferred embodiments of the invention, the states are generated perfectly at random with a view to excluding any possibility that the scheme may successfully be cheated. However, those of skill in the field will appreciate that some deviations from perfect randomness can be tolerated, provided that the bounds on that deviation are known: in particular, slight deviations from perfect randomness do not, materially, compromise security, and are intended to fall within the scope of the claimed invention.

In some embodiments, each of the plurality of qubits may be encoded in a photon of electromagnetic energy or, alternatively, in a weak light pulse with low expected photon number. The invention in these embodiments may advantageously be simple to implement.

BRIEF DESCRIPTION OF THE DRAWINGS

Embodiments of the invention will now be described, by way of illustrative and enabling example only, with reference to the accompanying drawings, in which:

figure 1 is a schematic diagram of two-dimensional space-time, illustrating an exemplary situation in which the present invention finds application;

figure 2 is a flow chart illustrating a method of generating an authentication token in accordance with one aspect of the invention; and

figure 3 is a flow chart illustrating a second method of generating an authentication token in accordance with one aspect of the invention.

DETAILED DESCRIPTION

As outlined above, the light-speed signalling bound is one important motivation for the invention. In view of this, the present schemes will be described in a relativistic context, in which some or all of the space-time points of interest may be space-like separated from one another. This is not essential, however, and the more general application of the invention to non-relativistic settings will be apparent to those of skill in the art.

Figure 1 is a schematic diagram of a simplified, two-dimensional space-time, illustrating an exemplary situation in which the present invention finds application.

CLAIMS

1. A method comprising the steps of:

a recipient receiving from an issuing party, at a first space-time point, a plurality of random quantum states, each of the quantum states chosen from a set of non-orthogonal quantum states and the quantum states represent quantum bits, qubits, or qudits;

the recipient applying a sequence of measurements, chosen from a plurality of possible pre-determined measurements, to the quantum states to generate classical measurement outcomes;

the recipient generating a token comprising a sequence of classical measurement outcomes by recording the classical measurement outcomes for the sequence of measurements applied to the quantum states;

the recipient transmitting to the issuing party data identifying the states for which the measurements were successful; and

the recipient presenting to the issuing party, at a second space-time point in the causal future of the first space time point, the token in return for access to a resource;

wherein:

before applying the sequence of measurements, the recipient having agreed with the issuing party the plurality of possible pre-determined measurements that will generate classical measurement outcomes giving a valid token for the second space-time point;

the measurements are chosen by the recipient from the plurality of possible pre-determined measurements in dependence on the space-time point at which the token is to be presented; and

the token comprising the sequence of classical measurement outcomes is valid at a single space-time point.

2. A method comprising the steps of:

an issuing party generating, at a first space-time point, a plurality of random quantum states, each of the quantum states chosen from a set of non-orthogonal quantum states and the quantum states represent quantum bits, qubits, or qudits;

the issuing party receiving from a recipient, at a second space-time point in the causal future of the first space-time point, a token comprising a sequence of classical measurement outcomes, and the issuing party receiving from the recipient data identifying the states for which the measurements were successful, wherein:

the token is obtained by the recipient applying a sequence of measurements, chosen from a plurality of possible pre-determined measurements, to the quantum states to generate classical

measurement outcomes and recording the classical measurement outcomes for the sequence of measurements applied to the quantum states;

wherein the issuing party and recipient agree the plurality of possible pre-determined measurements that will generate measurement outcomes giving a valid token for a second space-time point and the issuing party storing the classical measurement outcomes, and wherein the measurements are chosen from the plurality of possible pre-determined measurements in dependence on the space-time point at which the token is to be presented, and wherein the token comprises the sequence of classical measurement outcomes is valid at a single space-time point; and

the issuing party verifying whether the token corresponds to a statistically plausible result for the pre-determined measurements applied to the plurality of quantum states, before allowing the recipient access to the resource.

3. The method of any preceding claim, wherein the quantum states are chosen independently at random from among the pure states of a plurality of possible bases for the quantum state space.

4. The method of any of claims 1 to 3, wherein each of the plurality of quantum states comprises a BB84 state for the corresponding two-dimensional qubit space.

5. The method of any of claims 1 to 3, wherein each of the plurality of qubits is encoded in a photon of electromagnetic energy.

6. The method of claim 5, wherein either:

each qubit is encoded as a polarisation state of the corresponding photon; or

each qubit is represented by the polarisation state of a weak light pulse with low expected photon number.

7. The method of any preceding claim, wherein the pre-determined measurement comprises a projection of each of the plurality of quantum states onto one of the possible pure states of the corresponding quantum state space.

8. The method of any preceding claim, wherein the probability that the result of the sequence of measurements gives a valid token for a third space-time point separated from the second space-time point is negligible.

9. The method of any preceding claim, wherein the plurality of quantum states:

are entangled; and/or

comprise at least around 10^3 quantum states.

10. The method of any of claims 1 or 3 to 7 further comprising:

receiving, at a fourth space-time point in the future of the first space-time point and in the past of the second space-time point, a second plurality of quantum states;

applying a second sequence of measurements from the plurality of possible pre-determined measurements to the second plurality of quantum states to obtain a second sequence of classical measurement outcomes;

appending the second sequence of classical measurement outcomes to the token; and

presenting, at the second space-time point, the extended token in return for access to the resource.

11. The method of claim 10, further comprising iterating, at each of a plurality of successive time-like separated space-time points in the future of the first space-time point and in the past of the second space-time point, the steps of:

receiving a further plurality of quantum states;

applying a pre-determined measurement from the plurality of possible pre-determined measurements to the plurality of quantum states to obtain a further sequence of classical measurement outcomes; and

appending the further sequence of classical measurement outcomes to the token, such that the token presented at the second space-time point comprises each of the plurality of sequences of classical measurement outcomes.

12. The method of any of claims 2 to 8, further comprising generating, at a fourth space-time point in the future of the first space-time point and in the past of the second space-time point, a second plurality of quantum states; wherein verifying whether the token corresponds to a statistically plausible result for the pre-determined measurements comprises verifying whether the token includes a statistically plausible result for a first pre-determined measurement on the first plurality of quantum states and a statistically plausible result for a second pre-determined measurement on the second plurality of quantum states.

13. The method of claim 12, further comprising iterating, at each of a plurality of successive time-like separated space-time points in the future of the first space-time point and in the past of the second space-time point, the step of generating a further plurality of quantum states; wherein

receiving the token comprising a sequence of classical measurement outcomes comprises receiving an extended token comprising a plurality of sequences of classical measurement outcomes, and wherein verifying whether the token corresponds to a statistically plausible result for a pre-determined measurement comprises verifying whether the token includes a statistically plausible result for each of a plurality of respective pre-determined measurements on each generated plurality of quantum states.

14. The method of any of claims 1 or 3 to 7, comprising receiving, at the first space-time point, multiple pluralities of random quantum states, each of the quantum states chosen from a respective set of non-orthogonal quantum states; applying a respective pre-determined measurement to the quantum states to obtain an extended token comprising a number of sequences of classical measurement outcomes; and presenting, at the second space-time point, a portion of the extended token in return for access to a resource.

15. The method of any of claims 2 to 8, comprising generating, at the first space-time point, multiple pluralities of random quantum states, each of the quantum states chosen from a respective set of non-orthogonal quantum states; receiving, at a second space-time point in the causal future of the first space-time point, an extended token comprising a number of sequences of classical measurement outcomes; and verifying whether the token corresponds to a statistically plausible result for respective pre-determined measurements on each of the pluralities of quantum states.