

(51) International Patent Classification:
H04L 9/08 (2006.01)(21) International Application Number:
PCT/GB2018/050008(22) International Filing Date:
03 January 2018 (03.01.2018)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
1700085.2 04 January 2017 (04.01.2017) GB(71) Applicant: **CAMBRIDGE ENTERPRISE LTD**
[GB/GB]; The Old Schools, Trinity Lane, Cambridge Cam-
bridgeshire CB2 1TN (GB).(72) Inventor: **KENT, Adrian**; University of Cambridge, Cen-
tre for Mathematical Studies, Wilberforce Road, Cambridge
Cambridgeshire CB3 0WA (GB).(74) Agent: **REDDIE & GROSE LLP**; The White Chapel
Building, 10 Whitechapel High Street, London, Greater
London E1 8QS (GB).(81) Designated States (*unless otherwise indicated, for every
kind of national protection available*): AE, AG, AL, AM,
AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ,
CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO,
DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN,
HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP,
KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME,
MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ,
OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA,
SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN,
TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.(84) Designated States (*unless otherwise indicated, for every
kind of regional protection available*): ARIPO (BW, GH,
GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ,
UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ,
TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK,

(54) Title: FUTURE POSITION COMMITMENT

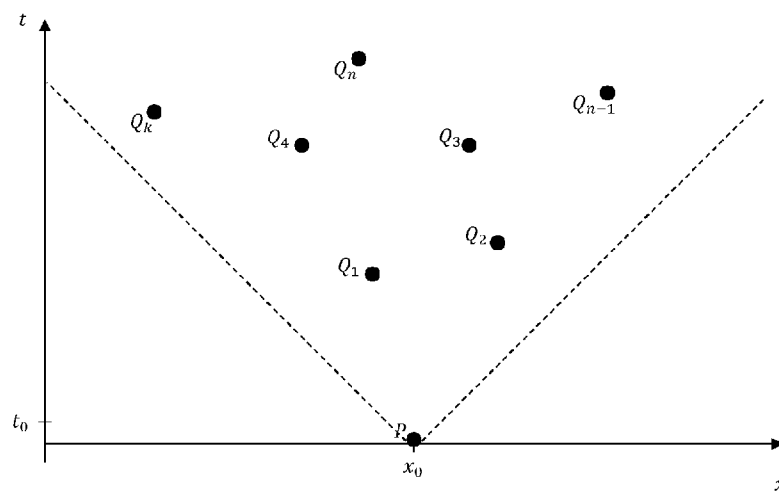


FIGURE 1

(57) **Abstract:** A cryptographic system enables a user securely to access a resource from an issuer at a first space-time point selected by the user, but not at a second (or other) space-time point. The parties (the issuer and the user) pre-agree representations of the future space-time points, which may include any number of future space-time points. The system then comprises a commitment device for use in a commitment protocol between the user and the issuer in which the user makes a secure commitment to the issuer, the commitment comprising the agreed representation of the space-time point selected by the user. The commitment device is configured to generate commitment data at a first output associated with the user and validation data at a second output associated with the issuer. Respective redemption devices at each of the space-time points each have an input for receiving a token presented by the user, the token being derived from the commitment data. Each redemption device is configured to validate the token if, and only if, the token is presented at the space-time point selected by the user and represented in the commitment.



EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV,
MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM,
TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW,
KM, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

FUTURE POSITION COMMITMENT

FIELD OF THE INVENTION

The present invention relates to secure authentication. More particularly, the invention provides an authentication token that cannot be forged, and can be transmitted by
5 electromagnetic waves and/or other standard means of communication; as well as methods for issuing and validating the token.

BACKGROUND TO THE INVENTION AND PRIOR ART

The redemption of tokens of various descriptions in exchange for goods and services, access to resources and other capabilities is a commonplace part of life today. For
10 example, money and other forms of credit may be exchanged for physical or virtual goods; passwords may be used to gain access to certain networks or data. However, in a world in which a token-issuing party does not or cannot have implicit trust in the party receiving the token for future validation, there can be an underlying desire to ensure that the token cannot be exploited unfairly. For instance, the token issuer may require assurance that the
15 token cannot be copied and used many times, thereby giving access to more resources than it is intended to allow. That imperative (and indeed the motivation for the token recipient to forge the token) can and often does scale with the inherent value of the resource in question.

Accordingly, the provision of a secure authentication token is a known problem in the field
20 of cryptography.

Various classical token-issuing schemes exist. Everyday currency is the most immediate example. However, as is known, no standard banknote is impossible to copy: forgery is a real world problem. Further, where a transaction is characterised by an overriding urgency or otherwise short timescales, familiar, tangible banknotes and coins are of limited use
25 insofar as the speed with which they can be transferred from one place to another is fundamentally restricted. This property makes material money an asset of limited value in many situations, such as modern financial trading networks.

Turning, then, to virtual tokens, one solution commonly adopted is to issue a password at a first point, P , in space and time (for example, in return for a payment) that can be used by
30 the recipient as an authentication token at any one of a finite number of future points Q_i ($i = 1, \dots, n$) in space-time. However, an immediate drawback of such an approach is

that there can be no *a priori* prohibition on the receiving party redeeming the token at a plurality of those future points: once the password is known, it simply needs to be recalled and repeated in order to gain access to multiple resources consecutively or even simultaneously. Because of this risk, the token issuing party may feel obliged to check, when the password is returned at a given point Q_k by the recipient in exchange for access to the relevant resource, that the same password has not been used at any point either in the causal past of or space-like separated from Q_k . This can be cumbersome and can incur unacceptable delay, particularly if any number of the points Q_i are not causally related to one another.

10 In some instances, the issuing party may choose to determine a unique password $password_i$ for use at each of the points Q_i ; ask, at point P , the receiving party at which future point they intend to use the password; and issue the relevant password accordingly. However, this approach may be appropriate only in a limited number of circumstances. For example, the token recipient may not know, when receiving the token at P , at which of the
15 Q_i she will choose to redeem it. Furthermore, even if she does know, she may wish to keep this information private: for instance, if the token is to be used to place a stock trade at some point Q_k on a global financial network, the trader may not wish to give the market advance warning of the time or place of her intended trade.

Since the introduction of Wiesner's 'quantum money' in 1983 (see Wiesner, S. Conjugate coding. *Sigact News* **15**, 78-88 (1983)), attempts have been made to exploit the properties of quantum mechanical systems to create an unforgeable authentication token. In the simplest version of the quantum money approach, a token takes the form of a stored quantum state, the classical description of which is not known to the recipient. The laws of quantum mechanics dictate that such a state cannot be copied without destroying the
20 original; it follows that these solutions are unconditionally or information-theoretically secure. The terms 'unconditional security' and 'information-theoretic security' are used interchangeably in this document to refer to security that can be proven relying only on the laws of physics, provided the protocol is followed faithfully (there is no cheating). In other words, the relevant proofs do not rely on the presumed practical intractability of a
25 computational problem that can, in principle, be solved.
30

Since quantum states can be encoded in photons of electromagnetic radiation, with sufficiently good technology quantum money tokens have the further advantage of being susceptible to transmission at light speed: they do not suffer the drawback mentioned above of classical, physical tokens such as banknotes. Moreover, known techniques such as

quantum teleportation and quantum secret sharing in principle allow quantum states to be transmitted in a way that affords more flexibility in response to incoming data than would be possible by sending a token along a single, definable path through space-time at speeds up to and including light speed. Some examples of the advantages to be gained by exploiting these techniques are discussed in Kent, A. Quantum tasks in Minkowski space. *Classical and Quantum Gravity* **29**, 224013 (2012); in Hayden, P. *et al.* preprint 1210.0913 [quant-ph] (2012), published as J. Phys. A: Math. Theor. **49** (2016) 175304; and in Adlam, E. and Kent, A. preprint 1509.04226 [quant-ph] (2015), published as Phys. Rev. A **93**, 062327 (2016).

Quantum money solutions have the additional advantage of providing both perfect 'future privacy' and perfect 'past privacy', innate to many classical approaches. By future privacy here is meant that the party issuing the token at point P cannot obtain any information about when or where it will be presented for redemption until that event takes place, beyond the constraints implied by physical bounds on signalling speeds. Thus, the token recipient need not divulge details of his future movements in order to have access to the token. Similarly, past privacy refers to the ability of the recipient to redeem the token at a chosen point – say, Q_k – without unavoidably revealing any information about the token's whereabouts between P and Q_k : so long as they are stored and transmitted securely, quantum tokens carry no record of their past locations. Future privacy and past privacy can be desirable or even imperative for certain individuals but also, for example, in the context of financial trading, where a record of past locations of the token implies a record of past locations where a trade could have been made. Such a record can encode valuable, exploitable information about trading strategies.

However, as is known to those of skill in the field, quantum money solutions are not, to date, technically feasible: at present, the art lacks adequate solutions for long-term, interference-free storage of the sorts of systems in which quantum states can be encoded. Reliable transmission, particularly at or near light speed, is also not always straightforward. Progress towards a truly operational realisation of a quantum token authentication scheme is likely to be slow, and it is probable that the technology once available will at least initially be cumbersome and/or prohibitively expensive. Indeed, it is not implausible that the storage and communication of classical data will always be significantly easier (and/or less costly) than the storage and transmission of information encoded in quantum states.

The inventor has appreciated that it is advantageous to provide an information-theoretically secure authentication scheme that does not rely on lengthy storage or transmission of

quantum states. An earlier, unpublished patent application in the name of the inventor, GB patent application no. 1511652.8, discloses a scheme in which two parties may derive a classical, unforgeable authentication token, for use by one of them in exchange for a resource from the other, through a short series of interactions with one another and with certain quantum states. The approach provides some of the advantages of quantum money without relying on the presently problematic long-term storage of quantum states; it is therefore technologically feasible using state of the art technology available today. However, the methods disclosed in GB '652.8 are restrictive in that they require a token-issuing party (or issuer) to be equipped with sources that enable him to generate quantum states and transmit them to the token recipient (or user).

The present invention improves upon the earlier approach just described, principally by introducing greater flexibility in terms of the technological capabilities required of the parties. In particular, one problem that this invention addresses is to provide classical, secure authentication tokens for use by a recipient in exchange for a resource, in a scenario in which the party issuing the token does not have ready access to any means for generating and/or transmitting quantum states, and/or the party requesting and using the token does not have ready access to any means for receiving and/or measuring quantum states. A further problem that may be addressed by the invention is where the user and issuer may have classical technologies that allow secure implementation but they may not (or not both) have quantum technologies available. Or they may only have available quantum technologies that are more costly, cumbersome or unreliable than their classical technologies. They may also (now or in future) have sufficient confidence that specific classical cryptographic commitment schemes are computationally secure (against both classical and quantum computers) and wish to implement token schemes that rely on this computational security and require fewer and shorter data exchanges and/or require less other resources than other token schemes described.

SUMMARY OF THE INVENTION

The invention is defined in the independent claims, to which reference should be made. Preferred features are set out in the dependent claims.

In one aspect, in general, the invention relates to a cryptographic system for enabling a user securely to access a resource from an issuer at a first future point in space-time selected by the user and unknown to the issuer, but not at a second, different future space-time point.

The parties (the issuer and the user) pre-agree representations of the future space-time points, and the cryptographic system comprises a commitment device for use in a bipartite commitment protocol between them, in which the user makes a secure commitment to the issuer that comprises the agreed representation of the point in space-time selected by the user. In other words, she commits to the fact that she will present the token at that chosen point, and not at the other point. The commitment device is configured to generate commitment data at a first output associated with the user, and to generate validation data at a second output associated with the issuer.

The cryptographic system further includes at least two redemption devices, one corresponding to each of the first and the second points in space-time. The redemption devices each have an input for receiving a token that may be presented by the user to the issuer (or directly to the device) at the respective point in space-time, the token being derived from the commitment data generated in the secure commitment. Each redemption device is configured to validate such a token if, and only if, it is presented at the point in space-time selected by the user and represented in the commitment; that is, if (and only if) the token is derived from commitment data generated in a commitment representing the selected point in space-time to which the respective redemption device corresponds.

In view of the motivations discussed above, the invention is conceived particularly for application to scenarios in which the token is to be valid at a single, unique future point – it may resemble familiar, physical money in this way and this is one of its principal advantages. However, the invention is not intended to be limited to such applications, nor should it be construed as such; in its broadest sense, the invention provides a token that, when presented to the issuer at one point, guarantees him that it has not been presented at one or more alternative points.

As one especial advantage, embodiments of the invention may enable the user to access the resource at her chosen time and location without requiring any transfer of information between the first point, at which it is valid, and the second, at which it is not.

The first and second points in space-time may be two of a larger plurality of space-time points, each in the future of the point at which the commitment is made. The user and/or the issuer may each be represented by a plurality of agents, one corresponding to each at of the future space-time points (as well as one corresponding to the issuance point).

At least two of the points (or the first and second points, where there are only two) may be space-like separated from one another. Though more generally applicable, the invention may be particularly advantageous in such scenarios, in that the ability conferred on the agent to whom the token is presented to know with certainty whether or not it has been presented at any point with an earlier (or equal) time co-ordinate, without reliance on data received from those earlier, perhaps space-like, points becomes relevant. In other words, on receiving the token and performing his prescribed checks, the agent may instantaneously be certain as to its validity: he need not wait the finite time necessary to receive information from agents at points outside his past light cone. (It is also true that in preferred embodiments no information from within the past light cone is required; this may also prove advantageous in terms of a lighter burden on the respective agents to prepare and send data.)

In preferred embodiments, the secure commitment made by the user of the resource using the commitment device is information-theoretically (synonymously, unconditionally) secure.

In some realisations, the commitment may be at least computationally secure. By 'computational security' here is meant security that is guaranteed unless at least one party can solve some computational problem that is believed to be hard to solve in timescales over which security is a relevant concern. In yet further embodiments, the commitment may be at least technologically secure; *viz.*, secure unless at least one party has technology that is believed to be impractical at the time in which the protocol takes place.

The token presented to the issuer by the user in exchange for the resource may consist exclusively of classical data. The token may simply be the commitment data generated in the secure commitment, or may be derived from or representative of those data in some way.

Embodiments conferring unconditional security using a purely classical token are preferred, in that they may provide one of the principal advantages of quantum money whilst avoiding the problematic need for long-term storage and/or long-distance transmission of quantum information that is characteristic of quantum money solutions.

In another aspect, in general, the invention relates to a commitment device usable within such a cryptographic system, for enabling a user of a resource to make a secure commitment to the issuer of that resource. The commitment device is configured to output commitment data generated in the secure commitment, from which the user's authentication token may be derived. The commitment device is also configured to output

validation data generated in the secure commitment, which the issuer may use to verify that the token is valid at the space-time point at which it is presented to the issuer by the user.

The token may be transmitted to agents of the user at one or more of the future space-time points; and the validation data may be transmitted to agents of the issuer at both (or all) of the future space-time points. Since the issuer is ignorant of the specific future space-time point selected by the user until the moment at which the token is presented, the presence of agents at all possible token redemption points will ensure that he is able to validate the token wherever she should present it.

10 In some embodiments, the agreed representation of the space-time point selected by the user corresponds to a binary word of suitable length and agreed to represent, or code for, that point. In that case, the secure commitment comprises a series of bit commitments: one to each bit of the word. A commitment protocol that is based on bit commitments may be advantageously straightforward for the parties to carry out, though in principle other
15 alphabets could be used to compose representations of the various space-time points and such representations are not excluded from the scope of the appended claims.

In a quantum commitment scheme, the commitment device may comprise suitable functionality for generating and measuring quantum information, for example under the control of a suitably-programmed computer or processor. In a classical commitment
20 scheme, in one embodiment it may be possible for the commitment device to comprise a suitably programmed computer or processor.

In yet another aspect, in general, the invention relates to a redemption device usable within a cryptographic system, for enabling an issuer of a resource to validate a token presented to him by a user of the resource. The redemption device includes an input for receiving the
25 token, and is configured to validate the token if and only if the token is ascertained to be derived from commitment data generated in a commitment to the space-time point at (or corresponding to) which the token is presented.

In a further aspect, in general, the invention relates to a method for enabling a user securely to access a resource from an issuer at a first future point in space-time selected
30 by the user, but not at a second, different future space-time point. The method preferably comprises the step of the user and the issuer implementing a bipartite commitment protocol, in which the user makes a secure commitment to the issuer. The commitment

comprises a representation agreed by the parties to represent the user's selected future space-time point. The commitment phase generates commitment data for use by the user and validation data for use by the issuer.

5 The method further includes the step of the issuer (or an agent of the issuer) receiving, at one or both of the space-time points, a token presented by the user (or an agent of the user). The token is derived from the commitment data generated in the secure commitment. On receiving the token, the issuer validates it if, and only if, the token is presented at the point in space-time selected by the user and represented in the commitment; that is, if (and only if) the token is derived from commitment data generated in
10 a commitment representing the point in space-time at (or corresponding to) which the token is presented.

Further aspects of the invention reside in the method steps performed by the user as part of the commitment protocol and, separately, in the method steps performed by the issuer as part of the commitment protocol.

15 In some embodiments of the present systems and methods as described herein, the commitment device of the cryptographic system is a quantum device, and the commitment made by the user to the issuer is a quantum commitment.

A quantum commitment device in accordance with these embodiments may enable the user to generate a sequence of quantum states, and to transmit those states to the issuer.
20 Thus the commitment data here comprise the quantum information encoded in the sequence; and the token may comprise a classical description (or representation) of the overall quantum state of the sequence. The quantum commitment device in these examples may also include means enabling the issuer to receive the quantum states from the user, to apply a randomly chosen measurement to each of the quantum states received
25 and to record (classically) the outcomes of those measurements. The validation data in this case may be derived from those measurement results.

In one example of a quantum commitment protocol that enables the user to commit to a binary representation of her chosen space-time point, the user may commit to each bit of the appropriate binary word by generating a particular sub-sequence of her overall
30 sequence of quantum states in a particular way. That is, she may commit to a first value of a bit (say, '0') by generating a sub-sequence of quantum states chosen randomly from among a first set of quantum states, pre-agreed with the issuer, and to a second value of a

bit (say, '1') by generating a sub-sequence of quantum states chosen randomly from among a second set, also pre-agreed with the issuer.

Preferably for good security, each sub-sequence used to encode a single bit of the binary word in these embodiments includes at least around fifty quantum states, for example at
5 least 30 or 40 or 50.

In one particularly simple implementation, the first and second sets of quantum states may be the pure states of respective bases of the Hilbert space of the relevant quantum systems, used to encode the quantum states.

Preferably, each quantum state generated by the user corresponds to a bit of quantum
10 information, a qubit. In some embodiments, each qubit may be encoded as a photon of electromagnetic energy or, realistically, as a weak light pulse with low expected photon number. As one possibility, each qubit in this case may be realised as a polarisation state of the corresponding photon (or of the corresponding weak light pulse).

In other embodiments of the present systems and methods as described herein, the
15 commitment device of the cryptographic system is a classical device, and the commitment made by the user to the issuer is a classical commitment.

A classical commitment device in accordance with these embodiments, which may enable the user to commit to a representation, such as a binary representation, of her chosen space-time point may enable the issuer and the user independently to generate a
20 respective string of random numbers, and to transmit data derived from at least one of those random numbers to the user or the issuer, respectively. In some examples of such a protocol, the data transmitted may be derived from (or a function of) the respective party's random numbers as well as data received from the other party.

In some cases, the user may realise each of her bit commitments as a plurality of
25 elementary bit commitments. In these examples, the classical commitment device may enable the issuer to transmit a first pair of random numbers to the user, wherein each of the random numbers corresponds to a respective bit value. It may further enable the user to make an elementary bit commitment by adding, to the one of the random numbers received from the issuer that corresponds to the bit value to which she wishes to commit,
30 one of her (independently-generated) random numbers; and to transmit the result of the

addition to the issuer. The token here may include the random number generated by the user and used in the addition.

Alternative embodiments discussed herein may provide a commitment protocol of less-than-unconditional security by enabling the user to return instead a number that is the result of a different function performed on the two numbers received from the issuer. Schemes according to such embodiments may be at least computationally secure. In some cases, they may be unconditionally secure.

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 each of the parties to the exchange. Such an exchange may be said to occur at a point in space-time, the point defined as the geographical region occupied by the two sites and the space in between them taken together with the finite time required for the data to be transmitted.

Furthermore, the term 'random' is intended throughout to connote perfect or near-perfect randomness. In preferred embodiments of the invention, the states are generated perfectly at random with a view to precluding any possibility that the scheme may successfully be cheated. However, those of skill in the art 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.

BRIEF DESCRIPTION OF THE DRAWINGS

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

figure 1 is a schematic diagram of a 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;

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

figure 4 is a flow-chart illustrating a method of generating a portion of an authentication token in accordance with another aspect of the invention.

DETAILED DESCRIPTION OF SOME EMBODIMENTS

As outlined above, the light speed signalling bound is one important motivation for this 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. As already mentioned, this is not essential, 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 and will be used to illustrate an exemplary situation in which the present invention finds application.

A first party, a recipient A, wishes to receive from a second party, an issuer B, at a point $P = (x_0, t_0)$ in space and time a token that she can return to him, in exchange for an asset, at some point in the future of P . As discussed further below, the exact point at which A wishes to trade in the token may or may not be known to her at P : the invention in its generality embraces both possibilities. The token may be a voucher, password or other encoding of information of any of the sorts discussed above for allowing access to a particular resource. For example, in some embodiments of the invention the token acts as physical money, exchangeable for goods and/or services. In other embodiments, the token is a password for gaining access to a given network and may be presented in digital form. In yet further examples, it may represent virtual credit for use in trading on a financial network, for instance taking the form of a signed document stating that A owns some number of shares of a given corporation.

Importantly, in view of the motivations discussed above embodiments of the present invention make no reliance on any level of trust existing between the parties A and B. It is assumed that A may try to cheat B by, for example, presenting her token more than once, or by attempting to forge it. Equally, it is presumed that B may attempt to violate A's privacy, both past and future. As will be discussed further below, schemes embodying the invention may be secure from B's perspective, and may also protect A's future privacy. They may also protect A's past privacy to some extent. For example, if she chooses not to use her token, then B may be prevented from obtaining certain information pertaining to A's past movements that is encoded in the token.

The following discussions assume that the token issuer B is more generally an 'agency', with agents as introduced in the Summary above distributed across a network of points at which A may choose to trade in her token (as well as at point *P*). Equally, the token user A may in some embodiments be a similar agency with a similar network of agents, though this is not in general essential. For instance, A and B could be financial institutions participating in a global financial network, with trading systems controlled by human agents and/or computers at many locations around the globe. In other embodiments, A may be represented by a private individual (or a small group of individuals) who may only visit some of the potential redemption points and who wishes to keep her (or who wish to keep their) movements, and in particular the token's location, secret insofar as possible.

In any event, suppose that B's agents operate with complete trust in one another and are able to share secret (classical) information securely between themselves at or near light speed. Similarly, A's agents (where they exist) also co-operate with complete mutual trust and may also be able to share secret classical information securely between themselves at or near light speed. If light speed or near-light speed transmission of information is not feasible for A's agents, then the scheme is still useful but the mobility of her token is restricted. The protocols discussed below give A security based on the assumption that any sharing of information between her agents is done securely, and using separate communications channels to those used by B and his agents.

In communicating amongst themselves, either group of agents could use any standard cryptographically secure communications scheme and any standard communications system. Some embodiments may make use of one-time pads to encrypt and decrypt the communications, in accordance with Vernam G. S. Cipher printing telegraph systems for secret wire and radio telegraphic communications. *Journal American Institute of Electrical Engineers XLV*, 109-115 (1926), so as to ensure theoretically perfect security. These pads could be generated ahead of time and/or during the protocol, for example by using standard quantum key distribution schemes implemented by commercially available quantum cryptography apparatus. As the skilled reader will appreciate, many such quantum key distribution schemes exist and are known. A recent review is given, for example, in Lo, H.-K. *et al.* Secure quantum key distribution. *Nature photonics* **8**, 595-604 (2014).

As one further overriding presumption, the present discussion assumes that both parties and their agents (if any) have access to suitably programmed classical computing devices

for carrying out the appropriate calculations and storing the resulting data and that the calculations and storage can be carried out securely.

As mentioned above, the invention encompasses both schemes in which a token is generated through use of quantum systems generated by the user to complete a quantum commitment from her to the issuer that she will redeem the token at a given point, as well as wholly classical schemes for making a similar commitment in which no quantum technology is required. The remaining discussions of this document present one example of a scheme involving quantum commitments and two example schemes involving classical commitments, and are organised as follows.

First, embodiments of the exemplary quantum scheme will be described. We begin with a discussion of the scheme in its most straightforward application, as a scheme for providing the user A with a token that she can redeem at a chosen later point in the event that the token issuer B cannot generate random quantum states (which, as discussed above, is a fundamental assumption of the earlier scheme described in GB '652.8). Various possibilities for a modified scheme, in which the token user may have more flexibility in choosing when and where to redeem her token, will then be introduced.

A second section of the disclosure presents an exemplary commitment scheme within the scope of the invention that is purely classical in nature. A third section presents a further exemplary commitment scheme within the scope of the invention that is again purely classical in nature and which relies on a computational hardness assumption for its security and is, as such, computationally secure modulo the stated assumption. The scheme is information-theoretically secure against the issuer. Schemes with the reverse property (that is, which are information-theoretically secure against the user and computationally secure against the issuer) are also possible.

A. Quantum commitment schemes

A.1 A single-round scheme

Though not essential to the invention in its generality, a first realisation of the quantum scheme discussed here presupposes for ease of illustration that the token recipient A has, on initiating the scheme at P , a fixed intention to redeem the token at a particular point $Q_k = (x_k, t_k)$, chosen from among a set of n pre-agreed, discrete points $\{Q_i = (x_i, t_i)\}_{i=1}^n$ in the future of P (refer to figure 1, in which the broken lines denote the light cone originating

at P). Here $n < \infty \in \mathbb{N}$ and may, for example, be on the order of 10^3 , though depending upon the application of interest it may be many orders of magnitude larger or as small as 2.

The token issuer B is represented by a network of agents, one located at P and one at each of the points Q_i at which the parties have agreed that A may trade in her token.

5 These agents (or in this particular embodiment, at least the agent at P) each possess apparatus suitable for receiving and measuring quantum states sent over short distances, as well as for transmitting and receiving classical data securely to and from each other as discussed above. The user A of the eventual token, on the other hand (or, where she too is represented by a plurality of agents, her agent at P), holds means for generating
10 quantum states, and for transmitting them over at least short distances. For example, she may be equipped with a credit card-sized device resembling a mobile phone, designed to receive classical data or use securely stored classical data in a way that allows it to generate and transmit in a narrow beam quantum states for the implementation of protocols for quantum key distribution and related cryptographic tasks. Such a device
15 could transmit quantum states to a similarly-sized device operated by the issuer B, which is able to receive classical data in a way that allows it to make appropriate measurements for the implementation of quantum key distribution and related cryptographic tasks and securely to record the results. The transmission could, for example, be of quantum states encoded in photon polarisation states as discussed further below, transmitted over a short
20 distance through free space (with the two devices appropriately aligned) or, alternatively, through an optical fibre connecting the devices.

(For simplicity of exposition, the present discussion refers throughout to A as an individual, on a path through space-time that begins at P . However, as has been mentioned above, A as a party may also be represented as a number of agents, distributed across the network
25 of possible trade points Q_i , at which tokens may be presented, as well as at P .)

Figure 2 illustrates schematically a quantum token-generation protocol 20 according to the invention that is designed to be applicable in the scenario just outlined. In the following, the various steps of the protocol will be introduced concretely in the context of one specific embodiment. Several variations on certain details of that example that are envisaged will
30 then be discussed.

Suppose first of all that the parties choose to work with qubits of information. Further, let those qubits be realised as polarisation states of single photons (or, realistically, as weak light pulses with average photon number below 1). (The generation and transmission of

photons is a well-known technique, details of which can be found, for example, in Lo, H.-K. *et al.* Secure quantum key distribution. *Nature photonics* **8**, 595 (2014) (and the references cited therein) and in Lunghi, T. *et al.* Experimental bit commitment based on quantum communication and special relativity. *Phys. Rev. Lett.* **111**, 180504 (2013).)

- 5 Before engaging in the exchange 20, A and B agree – in addition to the points Q_i themselves at which A may redeem her token – a coding for those points, designating each with a unique binary code word of suitable length. As an arbitrary example, a first point Q_1 may be labelled as a string of ‘0’s; a second Q_2 as a string of ‘0’s with a final ‘1’; and so on. They then also agree that A will ‘commit’ at P to a trade at the point Q_k of her choosing,
- 10 unknown to B, by generating and sending to B’s agent at P a sequence of quantum states that ‘spell’ the relevant code word in some suitable way. For instance, she can commit to a ‘0’ bit by generating a string of M pure states chosen at random from the two basis states $|0\rangle$ and $|1\rangle$ of the computational basis for the two-dimensional photonic Hilbert space, where $|0\rangle$ corresponds to a photon polarised in the vertical direction and $|1\rangle$ to a photon
- 15 polarised in the horizontal direction. For minimal levels of security, M here is on the order of 10; preferably, the user A would use at least 50 photons to represent each bit of the word. To commit to a ‘1’ bit, she can generate a similar sequence of states, chosen this time at random from the two basis states $|\pm\rangle := \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ of the so-called Hadamard basis for the same Hilbert space, the relevant photon polarisation states being the two
- 20 directions at 45° to the vertical.

- Note that, as mentioned above, the scheme does not rely for its security on the user A’s ability to generate states perfectly randomly from the relevant bases. Further and additionally, security may also be guaranteed notwithstanding a less-than-perfect independence of the probabilities of generating each of the two possible states for any one
- 25 given qubit from the corresponding probabilities associated with any other (for example, if the generation of a photon in the $|0\rangle$ state were to imply a higher-than-average probability that the subsequent photon to be generated would also be in the $|0\rangle$ state).

With the premises of their scheme thus defined, the parties then engage in the exchange 20 of figure 2.

- 30 In a first step 22, the token user A generates a sequence of N quantum states that codes for her chosen trading point Q_k in the sense just described. For good security, N here is preferably on the order of $M \log n$ or larger. Thus, she generates a composite state of the

form $|\psi\rangle = |\varphi_1\rangle_1 \dots |\varphi_N\rangle_N$, where tensor products between the individual states, omitted for simplicity of notation, are implied. For instance, suppose she wishes to redeem her token at a point assigned the code word 0010 (n in this simplified example being equal to $16 = 2^4$). Then, again simplifying for illustration so that $M = 3$, the state $|\psi\rangle$ might look

5 something like $(|0\rangle_1|1\rangle_2|1\rangle_3)(|0\rangle_4|1\rangle_5|0\rangle_6)(|+\rangle_7|-\rangle_8|-\rangle_9)(|1\rangle_{10}|1\rangle_{11}|1\rangle_{12})$. The quantum information encoded in that sequence represents commitment data, by means of which A commits to B that she will trade at Q_k . She records a classical description (such as this) of the sequence generated, which she will carry with her to Q_k to act, in effect, as her authentication token.

- 10 In step 24, A transmits her sequence of states to B's agent at P . In this example, since the individual qubit states are encoded as single photons, they may be sent through optical fibre or free space using standard, commercially available quantum key distribution sending and receiving apparatus. They might use the setup described in Lunghi, T. *et al.* Experimental bit commitment based on quantum communication and special relativity. *Phys. Rev. Lett.* **111**, 180504 (2013), for instance. To give a concrete example, A may
- 15 transmit her string of states to B's agent in an agreed time sequence that constitutes a short transmission burst (such as 1000 states every microsecond within an agreed millisecond, for example).

- On receiving the composite state $|\psi\rangle$, B's agent at P proceeds to carry out a sequence of
- 20 measurements on them at step 26. Specifically, for each state that he receives, he makes a random choice to measure the photon's polarisation either in the computational basis or in the Hadamard basis. Concretely: he might measure the state of the qubit in the computational basis by arranging a vertical polarisation filter before a photodetector. Since a vertically polarised photon is guaranteed to pass through such a filter, while a horizontally
- 25 polarised one is guaranteed not to pass, registration of a photon at the detector will correspond to a measurement of that photon as being in the $|0\rangle$ state, while failure to make any reading will correspond to a measurement of the photon as being in the $|1\rangle$ state. A similar arrangement with a filter arranged at 45° might be used to realise a measurement in the Hadamard basis. Alternative measurement arrangements are of course familiar to
- 30 those of skill in the art. For instance, in place of the polarising filters, B's agent at P may use birefringent crystals or polarising beam splitters to allow both polarisation types in the relevant basis to pass, but in beams that emerge from different points or have different spatial directions.

The collection of all apparatus used by the token recipient A in generating and transmitting her sequence, and in recording the overall state $|\psi\rangle$, together with that used by the token issuer B's agent at P in receiving and measuring the sequence and recording his results, is referred to herein as a 'commitment device'. The commitment device may be a single
 5 apparatus at the same location as the relevant agents of A and B, or it may comprise two portions, one held by the agent of A and one by the agent of B, linked by a suitable communications channel. The commitment device may comprise apparatus for generating and measuring the quantum states, controlled by a suitably-programmed processor or computer, and may comprise inputs and outputs for receiving data or information from and
 10 outputting data or information to the agents of A and B.

B's agent at P records, at step 28, the measurements performed and their outcomes, classically (by writing them down, for instance; or by inputting them to a computer memory; or by utilising a suitably-programmed processor or computer that automatically generates signals corresponding to the measurement results from detection devices and transfers
 15 them directly to a computer memory); and sends that information as validation data securely to all other agents of B, each of which is prepared to be presented with A's token at one of the Q_i .

To access her desired resource, A reveals to B's agent at Q_k the classical description of the sequence of states that she generated at P : she presents her token. To validate the token,
 20 he verifies whether the results of the measurements on the sequence of states actually received at P could (statistically plausibly) have been obtained by performing those same measurements on the sequence that A now claims to have sent. Again, the collection of all physical apparatus employed by the parties at Q_k is referred to herein as a 'redemption device'. The redemption device may be a single apparatus at the same location as the
 25 relevant agents of A and B, or it may comprise two portions, one held by the agent of A and one by the agent of B, which may be linked by a suitable communications channel. The commitment device may comprise inputs and outputs for receiving data or information from and outputting data or information to the agents of A and B.

By statistically plausible here is meant that the measurement results obtained could with
 30 significant probability have arisen given the states represented in the token that A presents. Briefly: under the conditions and assumptions of the present discussion, one in two of the measurements performed by B's agent at P will have been a measurement in the same basis as A claims to have chosen the corresponding quantum state from. In these cases,

following the laws of quantum mechanics, the measurement result should equal the claimed state of the relevant qubit. Allowing for some total level of error x accumulated between A's preparation of the states, the transmission and B's measurements, the results will realistically match a high proportion – namely, $1-x$ – of the time. If the results are equal
 5 for a significantly lower proportion of the relevant states, then B's agent at Q_k would reject the token. (The second half of the measurements will have been performed in the opposite basis to one from which the corresponding state is purported to be taken. Those measurements should give equi-probable, random results, and as such do not convey much by way of useful information. These results may therefore be ignored by B's agent at
 10 Q_k in his validation of the token.)

Future privacy for A follows, because she does not need to communicate to B the sequence that she chose to generate – and thus, the binary encoding of her choice of Q_k – until she returns the token. Additionally, where party A is represented by a number of agents as discussed above, light-speed transmission of the token between them is possible
 15 since it amounts to nothing more than a string of classical information, which can be sent by radio waves or any other known means.

Variations

In the scenario of figure 2, the short-distance communication at step 24 is the only point of the scheme at which transportation of quantum information is required. The skilled reader
 20 will appreciate that, although some errors, noise and losses may be incurred at this step, errors up to a threshold value can be allowed for by taking the number N of states to be sufficiently large to compensate for the associated error probability and by standard statistical tests.

Additionally on the point of transmission losses and inaccuracies, those of skill in the art will
 25 appreciate that B's agent at P may in reality succeed in measuring only a subset of the N states prepared and sent by A's agent at P . In some realisations, B's agent may in this case provide feedback to A's in real- or near-real-time about which qubit states produced a measurement outcome, based on the timings of the positive measurement results. Thus, for example, he may communicate that he obtained results for states 2, 5, 18, 23, and so
 30 on, in the sequence. Accordingly, the token in this case can be made up simply as a redacted version of A's classical description of the state $|\psi\rangle$; and B's agents at the various Q_i need only be made aware of the successful measurement outcomes. (As will be clear to the skilled reader, in situations in which losses are high the number of states generated

and sent by A should be sufficiently high to ensure a final token of adequate length for security, in accordance with the discussion above. It should also be of adequate length to guarantee that final token remains uniquely valid at the user's chosen redemption point. To do this, the parties should ensure that each sub-sequence sent from the user to the issuer at P as an encoding of a single bit includes sufficiently many states that at least M of them are guaranteed, or at least highly likely, to be measured successfully.)

In the specific example above, B's agent at P carries out the measurement step 26 immediately on receiving A's sequence of states at P . Though this may be preferred by parties not wishing to incur unnecessary experimental burdens, costs or risks, it is not an essential feature of the invention. In other words, should the relevant agent of B have the technological capabilities to store and/or transmit quantum states reliably, the measurement may instead be carried out at a later time, at a different point in space or even by another agent (provided, of course, that the measurement takes place at a space-time point that is in the causal past of the earliest point Q_1 at which A may appear and present her token for verification.)

The exemplary set of four possible states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ for A's qubits given above (referred to herein as the 'BB84 states') is given by way of example only, and in other embodiments the states generated by A may be chosen instead from any number of (complete or incomplete) bases.

A sufficient condition on the states, and on the issuer B's possible measurements, is that each pair that the user might have sent according to the protocol can be statistically distinguished by one of the measurements that the issuer may choose to apply according to the protocol. By 'statistically distinguished' here is meant that the probabilities of the relevant outcomes when a measurement is performed are different for the two states in the pair. In the example of the BB84 states given above, measurement of photon polarisation in the vertical/horizontal directions gives certain outcomes with probability 1 when the measured states are prepared as pure states of the computational basis, but this degree of distinction is not an essential feature of the invention. In general, whatever coding scheme the parties adopt should stipulate that the states from which the user may choose when encoding one of the bit values must all differ from the states from which she may choose when encoding the other of the bit values.

A necessary condition is that the possible qubit states are not mutually orthogonal. In preferred embodiments, the states are quite far from mutually orthogonal, such as the BB84 states.

Thus far, the invention has been illustrated as a commitment scheme in which the parties agree a binary encoding of the points at which the token user may elect to trade. Other possibilities are envisaged: with a suitable choice of sets of quantum states corresponding to the various letters, the alphabet used for the encoding may alternatively include three or more letters. As one example, the six states of the protocol described in Bruß, D. Optimal eavesdropping in quantum cryptography with six states. *Phys. Rev. Lett.* **81**, 3018 (1998), grouped into three bases, might form a suitable set of states to realise the scheme with a three-letter coding.

Indeed, though the above discussion illustrates the inventive scheme with reference to photonic qubits, other embodiments may instead make use of alternative two-level quantum mechanical systems such as electrons to encode bits of quantum information in a suitable known manner. Again, those qubits may encode any suitable states of choice. Furthermore, though qubit implementations are presently preferred for reasons of simplicity both of exposition and of implementation, the skilled reader will appreciate that the invention is not limited to the use of two-level quantum systems, and still further embodiments may implement the present methods using d -level quantum systems such as trapped ions to encode so-called qudit quantum states.

In all cases, the states with which the parties deal need be neither pure states of the relevant Hilbert space, nor independent of one another. Indeed, in practice experimental noise will ensure that the states are not perfectly pure. As those of skill in the art will recognise, the identification of acceptable levels of noise and errors and the adjustment of protocol parameters and statistical tests to deal with noise, errors and losses up to these levels, in ways appropriate to the particular coding scheme being employed, are routine.

A.2 An extending scheme

One can easily imagine situations in which A might not know, or may prefer not to decide, at P when and where she will want to redeem her token. For example, if the token represents credit for a trade, then A may want to keep open the option of making the trade somewhere in a global trading network at time t_1 , or of waiting until a later time t_2 , or a third time t_3 that is later still, and so on. Her chosen location may also be time-dependent, and

this sequence may not be known to her in advance. For instance, trading conditions at her first chosen point (say, London at t_1) may determine both whether she should trade then and there and, if not, where she should consider next.

Embodiments of this invention foresee several adaptations of the scheme discussed in
5 section A.1 above to this set of circumstances.

The following discussion assumes for simplicity that A may wish to cash in her token at one of a first set $\{Q_{i_1}^{(1)}\}$ of space-time points in the causal future of P or, alternatively, to defer redemption to one of a number of further sets $\{Q_{i_2}^{(2)}\}$, $\{Q_{i_3}^{(3)}\}$, and so on, where all of the points in each set $\{Q_{i_m}^{(m)}\}$ are in the causal future of all of the points in the preceding set
10 $\{Q_{i_{m-1}}^{(m-1)}\}$. The application of these embodiments also extends to more general configurations, not limited by causal relations in this way, and the assumption is made merely for ease of illustration. Note also that the number $n^{(m)}$ of points in one (the m^{th}) set need not necessarily be the same as the number of points in any other of the sets.

First, assume that A (or her agents) is (or are) at all points able to generate and transmit
15 quantum states; and that all of B's agents are able to receive and measure states that may be sent to them, in the appropriate bases, as well as to send and receive classical data amongst themselves.

One protocol 30 that may be useful in that case is outlined in figure 3.

In a first stage 32 of the method according to this embodiment, A and B proceed as
20 described above with reference to figure 2. Thus, at space-time point P , A generates at step 322 a sequence of qubits (or qudits) that code for a first point $Q_{k_1}^{(1)}$ at which she has decided she may wish to trade; she records the classical description $|\psi^{(0)}\rangle$ of the overall sequence, and passes the quantum states to B's agent at P along a suitable channel at step 324. At step 326, B's agent carries out a sequence of random measurements on the
25 states he has received; records the outcomes as before; and sends those data securely to his agents at all points $Q_{i_1}^{(1)}$. A, meanwhile, either sends her classical description of her sequence (*viz.*, her token) securely to an agent at $Q_{k_1}^{(1)}$, or else carries it with her on her space-time path to that point.

On reaching $Q_{k_1}^{(1)}$ at step 34, A makes a decision whether or not to redeem the token generated at P . If not, she returns to step 322. Thus, she chooses from among the next agreed set $\{Q_{i_2}^{(2)}\}$, a new candidate point $Q_{k_2}^{(2)}$ at which she may prefer to trade, and generates a second sequence of quantum states $|\psi^{(1)}\rangle$ that code for that point in the sense described above. She again makes a record of the states produced, which can be
 5 appended to her original token to define a new token $|\psi^{(0)}\rangle \otimes |\psi^{(1)}\rangle$ that will be valid at $Q_{k_2}^{(2)}$; and transmits the states to B's respective agent, thus committing to the new (potential) trading point $Q_{k_2}^{(2)}$.

On receiving the fresh sequence of states, B's agent at $Q_{k_1}^{(1)}$ measures them randomly as
 10 before and records his findings. He too appends the measurement data to those obtained by B's agent at P , and sends the cumulative data via secure channels to his colleagues at all points $Q_{i_2}^{(2)}$. (As before, that B's agent acts immediately upon receiving the states from A is not a requisite of the scheme: should he happen to be able to store quantum systems reliably for an extended period of time, and/or send them to another point in space-time, he
 15 may prefer to measure them later on and/or at another location on the globe, with the proviso noted previously; viz., that the measurement takes place at a point in space-time that is in the causal past of the earliest point Q_1 on the network at which A may appear and present her token for verification. Again as before, B's agent at $Q_{k_1}^{(1)}$ may optionally report to A which qubit states gave a positive measurement outcome, so that between them they
 20 may adapt the token to exclude the information encoded in the redundant or 'lost' qubits.)

In order to implement this embodiment of the invention, as the skilled person will appreciate it is necessary for the agents of A and B at $Q_{k_1}^{(1)}$ to have access to a suitably-programmed commitment device which may, for example, be similar to the commitment device located at P . For example, apparatus having both the functionality of a commitment device and a
 25 redemption device may be present.

Note that, at the agents' mutual choice (and in dependence, for instance, on the numbers of space-time points in the respective sets $\{Q_{i_1}^{(1)}\}$ and $\{Q_{i_2}^{(2)}\}$), the number $N^{(1)}$ of states in the new sequence $|\psi^{(1)}\rangle$ may be the same as or different to the number $N^{(0)}$ of states in $|\psi^{(0)}\rangle$. Indeed, the invention in principle does not exclude the possibility that the states
 30 generated at $Q_{k_1}^{(1)}$ embody the coding of the points $\{Q_{i_2}^{(2)}\}$ in a manner different from that

adopted at P . For instance, the parties at $Q_{k_1}^{(1)}$ may exchange photons in states other than the BB84 states introduced above, or may even work with alternative quantum systems (such as electrons, for example), should that prove more convenient for whatever reason.

Note also that in this scenario, A may prefer to be represented by a plurality of agents, (one at each point $Q_{i_1}^{(1)}$, for example), each tasked with generating and sending a fresh sequence of states to a respective agent of B. In this way, B cannot learn anything about A's initial choice of trading point $Q_{k_1}^{(1)}$ – and thus, her trading strategy and its development over time – should she decide to postpone her trade to an alternative point later in time. Optionally, A's agents at many of the $Q_{i_1}^{(1)}$ may prepare and send to the corresponding agents of B 'dummy' states, not intended to play any role in generating the token but which may prevent B from inferring the initial choice of trading point $Q_{k_1}^{(1)}$. Such dummy states should ideally take the form of a set of states that would be a valid continuation of the token, if the original sequence $|\psi^{(0)}\rangle$ had in fact represented a commitment to the respective point (at which the relevant agent is located). When sending them, A's agents should ideally follow the other communications prescribed by the protocol, as though the states might genuinely be used for a token continuation. By way of example: if B's nearby agent sends to an agent of A states for which measurement outcomes were obtained, as above, she accepts this list and follows any further rules prescribed by the protocol. She also sends secure messages to A's other agents, of suitable lengths, so that they are indistinguishable by signal traffic analysis from the secure messages that would contain data continuing the token.

Extension: third and subsequent stages

The immediate possibility for repeated extension of the scheme in this way will be apparent. If, on reaching $Q_{k_2}^{(2)}$, A again decides that she is not yet ready to redeem her token, the process just described can be iterated until she does. The token grows linearly in length at each stage. In particular, in embodiments in which the numbers of states produced at each stage are of the same order of magnitude (say, $\sim N$), for instance, then the length of the token generated at stage $m - 1$ for presentation to an agent of B at some point $Q_{k_m}^{(m)}$ will be on the order of mN .

The scheme may be iterated for any number of rounds, limited only by technological constraints.

Alternative

In the extension of the scheme through time as just described, it was assumed that A (or her agents) at all points would hold means for generating and transmitting quantum systems in states suitable for encoding a position commitment; and that B's agents at all points would be capable of receiving those states and of performing suitable measurements on them. Those conditions are not in fact required for successful application of an 'extending token' scheme in accordance with the invention. For example, the protocol of figure 2 may be combined with that of my earlier patent application GB '652.8 to accommodate parties having at their disposal technologies other than those assumed in the discussion of figure 3 above, as follows.

Assume now that an initial token is generated at P , and either sent or carried through time and space to $Q_{k_1}^{(1)}$, at which point A decides to postpone her trade – her redemption of the token. Assume also that there is no physical apparatus available to A at $Q_{k_1}^{(1)}$ that allows her to generate and send quantum states, but that she can receive and measure such states; and that B's corresponding agent is now able to generate and send states to A. In overview, the parties may then extend the original token by engaging in a position commitment protocol according to the earlier scheme disclosed in GB '652.8, the contents of which are incorporated herein in their totality by reference. The extended, 'hybrid' token will take the form of a classical description of the sequence of states sent to B's agent at P by A, followed by a series of (classical) measurement results obtained by A at $Q_{k_1}^{(1)}$ by measuring a second sequence of states received by her from B's agent there.

The steps of the earlier position commitment protocol will now be reviewed briefly, with reference to figure 4, for completeness of disclosure. Again, a specific implementation that uses photon polarisations to encode the necessary quantum information is given, for concreteness and to aid understanding. The variations discussed above in terms of the specific quantum systems and states with which the parties work are equally applicable to the following discussion.

Imagine that A at $Q_{k_1}^{(1)}$ wishes to obtain a token segment that can be appended to her description of the state $|\psi^{(0)}\rangle$ that she generated at P , to give a token that will allow her to trade at a next chosen point $Q_{k_2}^{(2)}$. B's agent, at step 42, now generates a sequence of photons of suitable length $N^{(1)}$, chosen this time independently at random from among the

BB84 states. He records the states generated, classically, as his validation data; and transmits the photons to A at step 44. Thus A may receive an overall state of the form $|\psi^{(1)}\rangle = |0\rangle_1|+\rangle_2|-\rangle_3 \dots |0\rangle_j \dots |1\rangle_{N(1)}$, for instance. In this case, A commits to her next chosen space-time point $Q_{k_2}^{(2)}$, bit by bit, by means of the particular measurements that she proceeds to carry out on the photons making up that state at step 46.

To give a concrete example: assume again that the point $Q_{k_2}^{(2)}$ is agreed by the parties to be represented by a particular binary word, including some suitable number of bits. At step 46, the user may then commit to the first bit of that word by measuring a first sub-sequence of M of the states received from the issuer's agent at $Q_{k_1}^{(1)}$ in the appropriate one of two bases for the photonic Hilbert space. For instance, mirroring the discussion in section A.1 above, she may commit to a '0' bit by measuring the first M states in the computational basis, and to a '1' bit by measuring those states in the Hadamard basis. She records the results of her measurements as her commitment data for this round of the scheme which, in this instance, also represent her new token segment.

15 B. Classical commitment scheme

An exemplary commitment scheme in accordance with the invention that requires no interaction with quantum systems will now be described. For simplicity, the scheme will be described as a single-round scheme, similarly to that of section A.1 above. Again for simplicity, the following discussion again assumes that the parties A and B agree to represent space-time points, at which A may present an authentication token to B, as unique binary words; that is, that A's commitment to her chosen point is made up as a series of bit commitments. The possible classical realisations of the invention are not limited in any of these respects, and the disclosure should not be construed as implying any such limitations.

The classical commitment scheme of this example may be realised by two pairs of agents representing each party A, B located at each point P, Q_i in the network. Each 'point' here is now taken to be a region in space-time (for example, the spatial extension of the region could be defined by a city, or a building or a room; and the temporal extension by some small time interval); a first agent of each of the issuer and the user are taken to be relatively close together at one point within that region; and a second agent of each are also taken to be relatively close together at a second point within the region, where the first and second

points are space-like separated from one another with significantly greater spatial separation than between the first pair of agents or the second pair of agents.

All agents of the issuer B pre-agree, and privately share, a string of random numbers, defined modulo R , where R is a large integer defining a security parameter. As an illustrative example, R might be taken to be 50, although it could be significantly smaller or larger, such as between 10 and 200 or between 25 and 100. They also agree that particular pairs of random numbers in the string are to be used by particular agents at particular times in the protocol. The pairings are again chosen at random, subject only to the constraint that the two numbers in any given pair are different. All agents of the user A also pre-agree, and privately share, their own string of random numbers, again defined modulo R ; and assign particular ones of those random numbers to be used by particular agents at particular times in the protocol.

Using a suitable commitment device, the agents of the token recipient at P then proceed to commit to each bit of the appropriate binary word, by completing a set of $2S$ elementary bit commitments, where S is a second agreed large integer defining a further security parameter. As an illustrative example, S might be taken to be 20, although it could be significantly smaller or larger, such as between 10 and 200 or between 25 and 100.. Each of the elementary bit commitments is implemented as follows.

First, the first of A's two agents at P requests to the first of B's two agents at P that the protocol commences; and B's agent responds by sending to A's agent the pair of random numbers (n_0, n_1) assigned to that particular point in space-time. The agent of A initiating the protocol responds by swiftly returning the single number $n_b + r_1$ (evaluated modulo R), where b is the value of the bit to which she wishes to commit and r_1 is the one of her pre-distributed random numbers assigned to be used in this exchange.

The $2S$ bits thus committed are arranged in pairs $(b_{\{10\}}, b_{\{11\}}), \dots, (b_{\{S0\}}, b_{\{S1\}})$, and are chosen randomly by A's initiating agent (or chosen randomly by A and pre-agreed in advance in coordination with her agents) subject to the constraints $b_{\{10\}} \oplus b_{\{11\}} = b_{\{20\}} \oplus b_{\{21\}} = \dots = b_{\{S0\}} \oplus b_{\{S1\}} = b'$, where b' is the bit value to which A wishes to commit.

With the $2S$ elementary bit commitments thus completed, at any point space-like separated from P A is effectively separately committed to the bit value b by each of the S pairs of individual bit commitments. An agent of hers at one of those points can prove her commitment by returning the random numbers $r_{\{10\}}, r_{\{11\}}, \dots, r_{\{S1\}}$ to an agent of B's.

However, at points time-like separated from P , A is no longer committed unless her and B's agents choose to continue the commitment. The commitment to b' can be continued by similar exchanges, involving new random numbers and the unveiling of specified subsets of the elementary bit commitments, between the second agents of each of A and B, as

5 described in Kent, A. Secure Classical Bit Commitment using Fixed Capacity Communication Channels. J.Cryptolog. 18, 313-335 (2005), the contents of which are incorporated herein in their entirety by reference.

The commitment can be further continued by similar exchanges, which alternately take place between the first agents of A and B and the second agents of A and B, again as
10 described in Kent, A. Secure Classical Bit Commitment using Fixed Capacity Communication Channels. J.Cryptolog. 18, 313-335 (2005). By the combination of techniques described in that paper, a bit commitment can thus be sustained, in principle indefinitely, by continuing exchanges.

It will thus be seen that these pairs of agents can sustain a string of bit commitments that
15 code for some space-time point on the network in the causal future of the initiation point. This point, the initial token redemption point, is chosen by A (through her local agents), and is kept secret from B by the bit commitment protocols unless and until A chooses to reveal it.

In this protocol the issuer's validation data comprise the totality of all pairs of random
20 numbers previously sent (i.e. sent in rounds of the protocol prior to the unveiling) to either agent of the user, together with all numbers received from either agent in these rounds. The user's commitment data comprise the totality of all the pre-distributed shared random numbers used by the user's agents in the commitment exchanges previously sent to generate numbers sent to the issuer's agents. Although commitment and validation data
25 thus continue to be generated at each round of the protocol, the user's commitment to their original choice of committed data is guaranteed secure against all known attacks, as shown in the cited reference (Kent, 2005).

To reveal it and redeem the token, an agent of A's located at the chosen point in space sends to a nearby agent of B's, for input to a redemption device, all the random data used
30 by the two agents of A in the relevant bit commitment protocols, from the initiation round onwards, including data used in at least one round that is spacelike separated from the point in space-time where the nearby agent of B's will receive this communication. This spacelike separation guarantees to B's agent that the commitments are being validly

unveiled, and hence that the token is being validly presented. To check this guarantee, B's agent at the redemption point needs to wait to receive from the agents of B at the initiation point the data they received in the final spacelike separated round. (He also needs the data from earlier rounds, but this may already have been sent to and reached him, so it per se requires no further delay.)

Extension

It will be appreciated that the scheme just described may be extended in a manner similar to the extension of the quantum scheme outlined in section A.2, in the event that the token user A on reaching the point committed to decides to postpone her trade. Rather than unveiling the token at the original token redemption point, A's agents at that point may initiate a second set of commitments defining a valid continuation of the token. If the possibility exists that the token will be continued in this fashion, A's and B's agents at P continue to sustain the original commitments, defining the original token, until they learn that the token has been redeemed. It will also be appreciated that the classical commitment scheme just outlined, as a scheme for committing to one particular point in space-time, may be combined with either of the quantum schemes described in section 1 to produce a hybrid token that is derived from two or three types of commitment data. Specifically, A's hybrid token, which she may eventually choose to redeem at some final $Q_{k_f}^{(f)} \in \{Q_{i_f}^{(f)}\}$, may comprise any number of quantum state descriptions $|\psi^{(m)}\rangle$, any number of sets $\{M^{(m)}\}$ of measurement outcomes and any number of sets of random numbers $\{r_m\}$ used by her agents in a classical commitment scheme as just described.

Thus, schemes for generating and extending a secure authentication token according to this invention may find application in a more varied set of circumstances than those disclosed previously. In particular, this invention accommodates situations in which the token user A (or her agents) and agents of the token issuer B at a given, m^{th} stage of the scheme may possess either means for generating and sending quantum states; or means for receiving and measuring them; or neither. In other words, the parties may choose, stage by stage (including at P), to follow the protocol of figure 2, that of figure 4 or that of this section, a choice dictated by their respective technological capabilities at that point in space and time.

C. Classical commitment scheme based on computational security assumptions

Another exemplary commitment scheme in accordance with the invention that requires no interaction with quantum systems will now be described. For simplicity, the protocol will first be introduced as a single-round scheme, similarly to that of section A.1 above. Also
 5 for simplicity, the following discussion assumes that the parties A and B agree to represent the n space-time points, at which A may present an authentication token to B, as n distinct unique numbers m lying in the range $[1, 2, \dots, p]$, where p is the prime parameter in which the scheme below is defined. For definiteness, the coding scheme defining these representations is chosen by B, using a randomly chosen set of n numbers with these
 10 properties. The prime parameter p is required to be much larger than n . The bit commitment scheme described in this example derives from T. P. Pedersen Non-interactive and information theoretic secure verifiable secret sharing in Proceedings on Advances in Cryptology – CRYPTO, LNCS 576, Springer, 1992, pp. 129-140, the entire contents of which are incorporated herein by reference. The possible classical realisations
 15 of the invention are not limited in any of these respects, and the disclosure should not be construed as implying any such limitations.

The classical commitment scheme of this example may be realised by single agents representing each party A, B located at each point P, Q_i in the network; that is, each party may have one agent located at each network point. Each 'point' here is again taken to be a
 20 small region in space-time (for example, the spatial extension of the region could be defined as a city, or a building, or a room, and the temporal extension by some small time interval). The commitment device may be implemented as a suitably-programmed processor or computer, having suitable inputs and outputs for receiving and transmitting data or information from and to the agents of A and B.

25 A and B agree a large prime number p , sufficiently large that B is willing to accept security based on the assumption that A cannot solve random instances of the discrete logarithm problem modulo p with any technology, including any algorithm she may run on any classical or quantum computer, during any time interval over which a token may be defined and sustained.

30 All agents of the issuer B pre-agree, and privately share, a string of random numbers, defined modulo p . They also agree that particular pairs of random numbers in the string are to be used by particular agents at particular times in the protocol. The pairings are again chosen at random, subject only to the constraint that the two numbers in any given

pair are different. All agents of the user A also pre-agree, and privately share, their own string of random numbers, again defined modulo p ; and assign particular ones of those random numbers to be used by particular agents at particular times in the protocol.

The agent of the token recipient A at P then proceeds to commit to the valid redemption point as follows.

First, A's agent at P requests to B's agent at P that the protocol commences; B's agent responds by sending to A's agent the pair of random numbers (g_1, g_2) assigned to that particular point in space-time. The agent of A initiating the protocol responds by swiftly returning the single number $c = (g_1)^r (g_2)^t$, (modulo p). Here t is the code representing her chosen space-time point $Q_{k_1}^{(1)}$, as described above, and r is the one of her pre-distributed random numbers assigned to be used in this exchange.

To reveal A's commitment and redeem the token, an agent of A's located at the chosen point $Q_{k_1}^{(1)}$ in space-time sends to a nearby agent of B's the numbers (r, t) (modulo p). The agent of B, by using a suitable redemption device, verifies that indeed t is the code for $Q_{k_1}^{(1)}$, and that $c = (g_1)^r (g_2)^t$ (modulo p). If so, he accepts the token as valid; if not, he rejects it.

Extension

It will be appreciated that the scheme just described may be extended in a manner similar to the extension of the quantum scheme outlined in section A.2, in the event that the token user A on reaching the point committed to decides to postpone her trade. Rather than unveiling the token at the originally-chosen redemption point, A's agent there may use a suitable commitment device at that location to initiate a second commitment defining a valid continuation of the token. It will also be appreciated that the classical commitment scheme just outlined, as a scheme for committing to one particular point in space-time, may be combined with either of the quantum schemes described in section A or with the classical commitment scheme previously outlined in section B to produce a hybrid token that is derived from two, three or four types of commitment data. Specifically, A's hybrid token, which she may eventually choose to redeem at some final $Q_{k_f}^{(f)} \in \{Q_{i_f}^{(f)}\}$, may comprise any number of quantum state descriptions $|\psi^{(m)}\rangle$, any number of sets $\{M^{(m)}\}$ of measurement outcomes and any number of sets of random numbers $\{r_m\}$ used by her agents in the

appropriate manner in either or both of the two classical commitment schemes just described,

Thus, schemes for generating and extending a secure authentication token according to this invention may find application in a more varied set of circumstances than those disclosed previously. In particular, this invention accommodates situations in which, depending on the commitment device functionality available at each point, the token user A (or her agents) and agents of the token issuer B at a given, m^{th} stage of the scheme may possess either means for generating and sending quantum states; or means for receiving and measuring them; or neither. In other words, the parties may choose, stage by stage (including at P), to follow the protocol of figure 2, that of figure 4 or that of this section, a choice dictated by their respective technological capabilities at that point in space and time.

CLAIMS

1. A cryptographic system for enabling a user securely to access a resource from an issuer at a first space-time point selected by the user, but not at a second space-time point, the system comprising:

- 5 a commitment device for use in a commitment protocol between the user and the issuer in which the user makes a secure commitment to the issuer, the commitment comprising an agreed representation of the space-time point selected by the user, the commitment device configured to generate commitment data at a first output associated with the user and further configured to generate validation data at a second output
10 associated with the issuer; and
 respective redemption devices at the first and second space-time points, each of the redemption devices having an input for receiving a token presented by the user, the token being derived from the commitment data, each redemption device being configured to validate the token if, and only if, the token is presented at the space-time point selected
15 by the user and represented in the commitment.

2. A cryptographic system according to claim 1, in which the first and second space-time points are two of a larger plurality of space-time points.

3. A cryptographic system according to claim 1 or claim 2, in which the first and second, or the first and at least one other, space-time points are space-like separated from one
20 another.

4. A cryptographic system according to any of claims 1 to 3, in which the secure commitment is information-theoretically secure.

5. A cryptographic system according to any of claims 1 to 3, in which the secure commitment is at least computationally secure.

- 25 6. A cryptographic system according to any of claims 1 to 3, in which the secure commitment is at least technologically secure.

7. A cryptographic system according to any preceding claim, in which the token consists of classical data.

8. A cryptographic system according to any preceding claim, in which the token comprises
30 the commitment data.

9. A cryptographic system according to any preceding claim, in which the token is output for transmission to respective agents of the user at one or more of the space-time points.

10. A cryptographic system according to any preceding claim, in which the validation data are output for transmission to respective agents of the issuer at the first and second, or the first and all other, space-time points.

11. A cryptographic system according to any preceding claim, in which the agreed representation of the selected space-time point corresponds to an agreed binary word representative of the selected space-time point, the commitment comprising a series of bit commitments, each bit commitment comprising a commitment to a successive letter of the agreed binary word.

12. A cryptographic system according to any preceding claim, for enabling the user securely to access a resource at a third space-time point selected by the user, but not at a fourth space-time point, the cryptographic system comprising:

a further commitment device at the first space-time point selected by the user, for use in a further commitment protocol between the user and the issuer in which the user makes a further secure commitment to the issuer, the further commitment comprising an agreed representation of the third space-time point selected by the user, the further commitment device configured to generate further commitment data and further validation data; and

respective further redemption devices at the third and fourth space-time points, for receiving a further token presented by the user, the further token being derived from the commitment data and the further commitment data, each redemption device being configured to validate the further token if, and only if, the further token is presented at the space-time point selected by the user and represented in the further commitment.

13. A cryptographic system according to any preceding claim, in which the commitment device and/or the further commitment device comprises a quantum commitment device.

14. A cryptographic system according to claim 13, in which the quantum commitment device and/or the further commitment device comprises:

means enabling the user to generate a sequence of quantum states, the sequence being representative of the selected space-time point, the commitment data and/or the further commitment data comprising the quantum information encoded in the sequence of quantum states, and to transmit the quantum states to the issuer; and

means enabling the issuer to receive the quantum states from the user and to apply a randomly chosen measurement to each of the quantum states received, the validation data and/or the further validation data being derived from the results of the measurements.

15. A cryptographic system according to claim 14, in which the token comprises a
5 classical description of the sequence of quantum states generated.

16. A cryptographic system according to claim 14 or claim 15 when dependent on claim 11 or claim 12, in which the quantum commitment device and/or the further quantum commitment device enables the user to commit to a first value of a bit by generating a sub-sequence of quantum states chosen randomly from among a first agreed set of quantum
10 states, and to commit to a second value of a bit by generating a sub-sequence of quantum states chosen randomly from among a second agreed set of quantum states.

17. A cryptographic system according to claim 16, in which the first agreed set of quantum states comprises the pure states of a first basis, and the second agreed set of quantum states comprises the pure states of a second basis.

15 18. A cryptographic system according to claim 16 or 17, in which each sub-sequence of quantum states comprises around fifty quantum states.

19. A cryptographic system according to any of claims 14 to 18, in which the quantum commitment device and/or the further quantum commitment device further comprises means for enabling the issuer to communicate to the user the quantum states, of the
20 quantum states transmitted from the user to the issuer, for which a positive measurement result is obtained.

20. A cryptographic system according to any of claims 14 to 19, in which each quantum state of the sequence of quantum states corresponds to a bit of quantum information, qubit.

21. A cryptographic system according to claim 20, in which each of the sequence of qubits
25 comprises a BB84 state for the corresponding two-dimensional Hilbert space.

22. A cryptographic system according to claim 20 or claim 21, in which each qubit of the sequence of qubits is encoded as a photon of electromagnetic energy.

23. A cryptographic system according to claim 20 or claim 21, in which each qubit of the sequence of qubits is encoded as a weak pulse of electromagnetic energy with low expected photon number.

24. A cryptographic system according to claim 22 or claim 23, in which each qubit of the sequence of qubits is realised as a polarisation state of the corresponding photon or of the corresponding weak light pulse.

25. A cryptographic system according to any of claims 14 to 24, in which each redemption device and/or each further redemption device comprises means enabling the issuer to verify that the validation data and/or the further validation data could statistically plausibly have been obtained by applying the randomly chosen measurements to the sequence of quantum states represented by the token or the further token presented by the user.

26. A cryptographic system according to any of claims 1 to 12, in which the commitment device and/or the further commitment device comprises a classical commitment device.

27. A cryptographic system according to claim 26 when dependent on claim 11 or claim 12, in which the classical commitment device and/or the further classical commitment device comprises means enabling the issuer and the user independently to generate a respective string of random numbers, and to transmit data derived from at least one of the generated random numbers to the user or the issuer, respectively.

28. A cryptographic system according to claim 27, in which each bit commitment comprises a plurality of elementary bit commitments.

29. A cryptographic system according to claim 28, in which the classical commitment device and/or the further classical commitment device comprises:

means enabling the issuer to transmit to the user a first of the random numbers generated by the issuer, the first random number corresponding to a first value of a bit, and a second of the random numbers generated by the issuer, the second random number corresponding to a second value of the bit; and

means enabling the user to make an elementary bit commitment by adding, to the one of the random numbers received from the issuer that corresponds to the bit value being committed to, one of the random numbers generated by the user, and to transmit the result of the addition to the issuer.

30. A cryptographic system according to claim 28, in which the token and/or the further token comprises the random number generated by the user and used in the addition.

31. A method for enabling a user securely to access a resource from an issuer at a first space-time point selected by the user, but not at a second space-time point, the method comprising:

the user and the issuer completing a commitment protocol in which the user makes a secure commitment to the issuer, the commitment comprising an agreed representation of the space-time point selected by the user, wherein making the commitment includes the user generating commitment data and the issuer generating validation data; and

the issuer receiving, at one or both of the space-time points, a token presented by the user, the token being derived from the commitment data, and validating the token if, and only if, the token is presented at the space-time point selected by the user and represented in the commitment.

32. A method according to claim 31, in which the first and second space-time points are two of a larger plurality of space-time points.

33. A method according to claim 31 or claim 32, in which the first and second, or the first and at least one other, space-time points are space-like separated from one another.

34. A method according to any of claims 31 to 33, in which the secure commitment is information-theoretically secure.

35. A method according to any of claims 31 to 33, in which the secure commitment is at least computationally secure.

36. A method according to any of claims 31 to 33, in which the secure commitment is at least technologically secure.

37. A method according to any of claims 31 to 36, in which the token consists of classical data.

38. A method according to any of claims 31 to 37, in which the token comprises the commitment data.

39. A method according to any of claims 31 to 38, further comprising the user transmitting the token to respective agents at one or more of the space-time points.

40. A method according to any of claims 31 to 39, further comprising the issuer transmitting the validation data to respective agents at the first and second, or the first and all other, space-time points.

5 41. A method according to any of claims 31 to 40, in which the agreed representation of the selected space-time point corresponds to an agreed binary word representative of the selected space-time point, the commitment comprising a series of bit commitments, each bit commitment comprising a commitment to a successive letter of the agreed binary word.

42. A method according to any of claims 31 to 41, for enabling the user securely to access a resource at a third space-time point selected by the user, but not at a fourth space-time point, the method comprising:

10 the user and the issuer completing a further commitment protocol at the first space-time point, in which the user makes a further secure commitment to the issuer, the further commitment comprising an agreed representation of the third space-time point selected by the user, wherein making the further commitment includes the user generating further commitment data and the issuer generating further validation data; and

15 the issuer receiving, at one or both of the third and fourth space-time points, a further token presented by the user, the further token being derived from the commitment data and the further commitment data, and validating the token if, and only if, the further token is presented at the third space-time point selected by the user and represented in the further commitment.

43. A method according to any of claims 31 to 42, in which the secure commitment and/or the further secure commitment made by the user is a quantum commitment.

44. A method according to claim 43, in which making the secure commitment, and/or making the further secure commitment, comprises:

25 the user generating a sequence of quantum states, the sequence being representative of the selected space-time point, the commitment data and/or the further commitment data comprising the quantum information encoded in the sequence of quantum states, and transmitting the quantum states to the issuer; and

30 the issuer receiving the quantum states from the user and applying a randomly chosen measurement to each of the quantum states received, the validation data and/or the further validation data being derived from the results of the measurements.

45. A method according to claim 44, in which the token and/or the further token comprises a classical description of the sequence of quantum states generated.

46. A method according to claim 44 or claim 45 when dependent on claim 41 or claim 42, in which making the commitment comprises, and/or making the further commitment
5 comprises, the user committing to a first value of a bit by generating a sub-sequence of quantum states chosen randomly from among a first agreed set of quantum states, and/or committing to a second value of a bit by generating a sub-sequence of quantum states chosen randomly from among a second agreed set of quantum states.

47. A method according to claim 46, in which the first agreed set of quantum states
10 comprises the pure states of a first basis, and the second agreed set of quantum states comprises the pure states of a second basis.

48. A method according to claim 46 or 47, in which each sub-sequence of quantum states comprises around fifty quantum states.

49. A method according to any of claims 44 to 48, in which making the secure
15 commitment, and/or making the further secure commitment, further comprises the issuer communicating to the user the quantum states, of the quantum states transmitted from the user to the issuer, for which a positive measurement result is obtained.

50. A method according to any of claims 44 to 49, in which each quantum state of the sequence of quantum states corresponds to a bit of quantum information, a qubit.

20 51. A method according to claim 50, in which each of the sequence of qubits comprises a BB84 state for the corresponding two-dimensional Hilbert space.

52. A method according to claim 50 or claim 51, in which each qubit of the sequence of qubits is encoded as a photon of electromagnetic energy.

25 53. A method according to claim 50 or claim 51, in which each qubit of the sequence of qubits is encoded as a weak pulse of electromagnetic energy with low expected photon number.

54. A method according to claim 52 or claim 53, in which each qubit of the sequence of qubits is realised as a polarisation state of the corresponding photon or of the corresponding weak light pulse.

55. A method according to any of claims 44 to 54, in which validating the token, and/or validating the further token, comprises verifying that the validation data and/or the further validation data could statistically plausibly have been obtained by applying the randomly chosen measurements to the sequence of quantum states represented by the token and/or the further token presented by the user.

56. A method according to any of claims 31 to 42, in which the secure commitment and/or the further secure commitment made by the user is a classical commitment.

57. A method according to claim 56 when dependent on claim 41 or claim 42, in which making the commitment, and/or making the further commitment, comprises the issuer and the user independently generating a respective string of random numbers, and transmitting data derived from at least one of the generated random numbers to the user or the issuer, respectively.

58. A method according to claim 57, in which each bit commitment comprises a plurality of elementary bit commitments.

59. A method according to claim 58, in which making the secure commitment, and/or making the further secure commitment, comprises:

the issuer transmitting to the user a first of the random numbers generated by the issuer, the first random number corresponding to a first value of a bit, and a second of the random numbers generated by the issuer, the second random number corresponding to a second value of the bit; and

the user making an elementary bit commitment by adding, to the one of the random numbers received from the issuer that corresponds to the bit value being committed to, a random number of the random numbers generated by the user, and transmitting the result of the addition to the issuer.

60. A method according to claim 59, in which the token and/or the further comprises the random number generated by the user and used in the addition.

61. A commitment device for use in a commitment protocol between a user and an issuer of a resource in which the user makes a secure commitment to the issuer, the commitment comprising an agreed representation of a space-time point selected by the user, the commitment device configured to generate commitment data at a first output associated

with the user and further configured to generate validation data at a second output associated with the issuer, in accordance with any of claims 1 to 30.

62. A redemption device usable by an issuer of a resource, the redemption device having an input for receiving the token presented by a user of the resource, the token being
5 derived from commitment data generated in a secure commitment made by the user to the issuer, the commitment comprising an agreed representation of a space-time point selected by the user, the redemption device being configured to validate the token if, and only if, the token is presented at the space-time point selected by the user and represented in the commitment, in accordance with any of claims 1 to 30.

10 63. A commitment method comprising making a secure commitment to an issuer of a resource, the commitment comprising an agreed representation of a selected space-time point, in which making the commitment comprises generating commitment data, in accordance with any of claims 31 to 60.

15 64. A redemption method comprising receiving a token presented by a user of a resource, the token being derived from commitment data generated in a secure commitment made by the user to the issuer, the commitment comprising an agreed representation of a space-time point selected by the user, and validating the token if, and only if, the token is presented at the space-time point selected by the user and represented in the commitment, in accordance with any of claims 31 to 60.

20 65. A non-transitory computer storage medium carrying a program for programming a commitment device as defined in any of claims 1 to 30 or 61.

66. A non-transitory computer storage medium carrying a program for programming a redemption device as defined in any of claims 1 to 31 or 62.

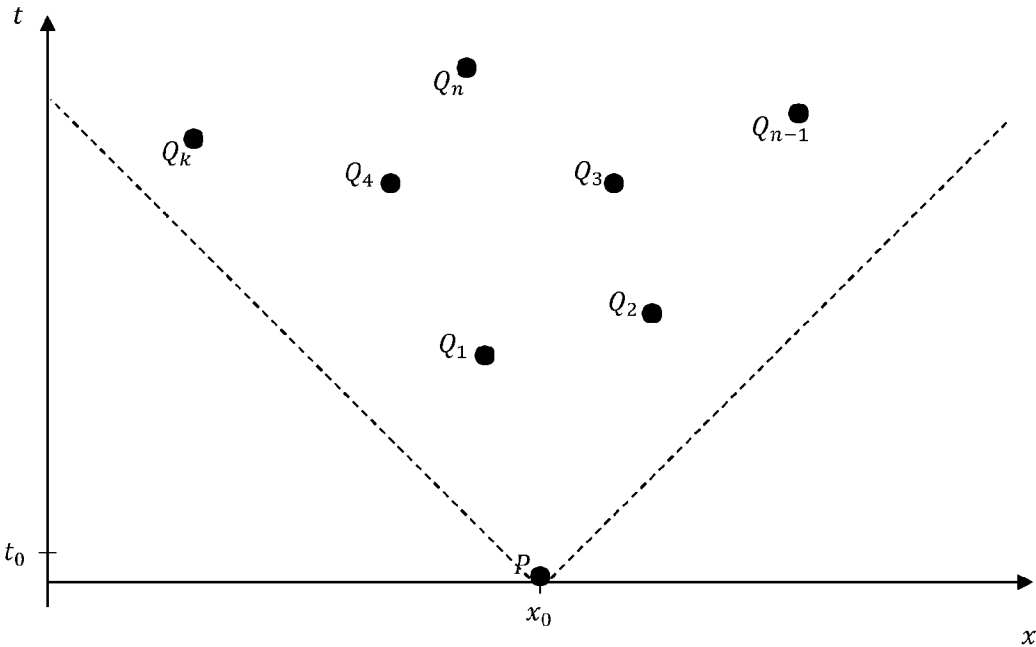


FIGURE 1

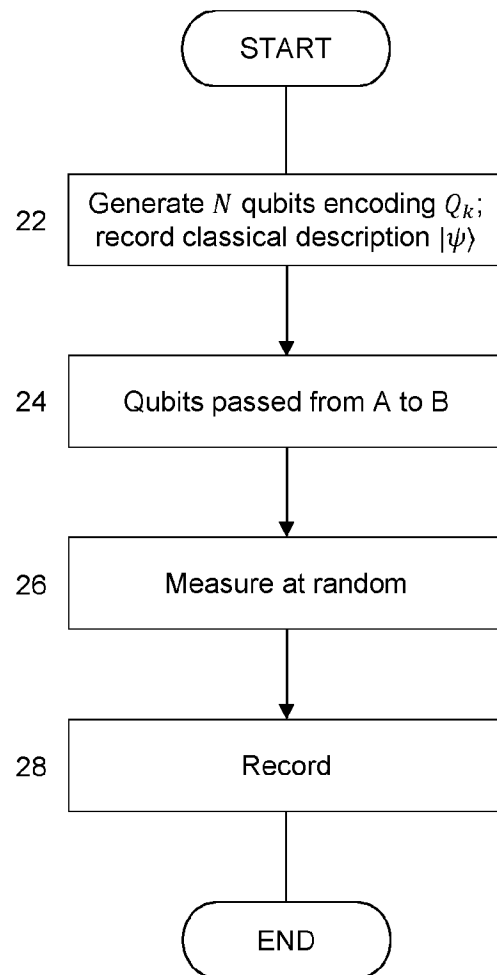
20

FIGURE 2

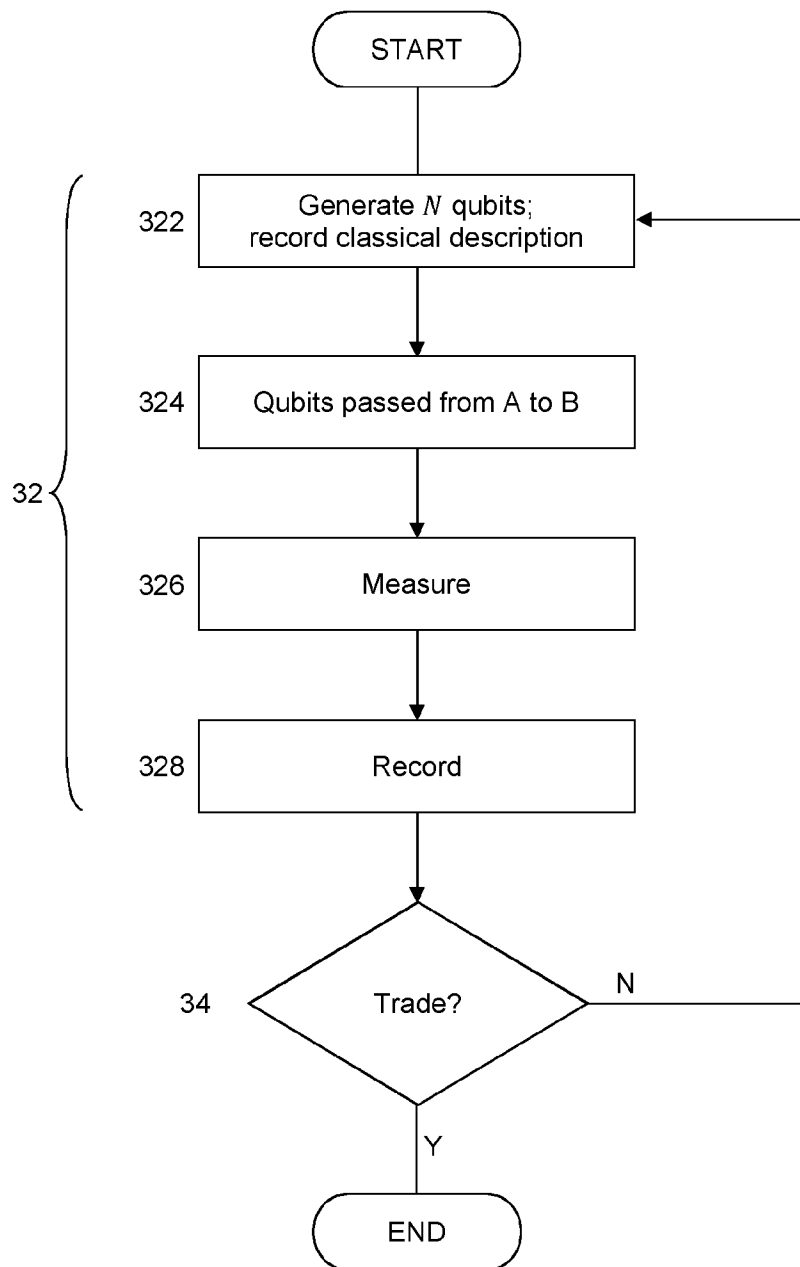
30

FIGURE 3

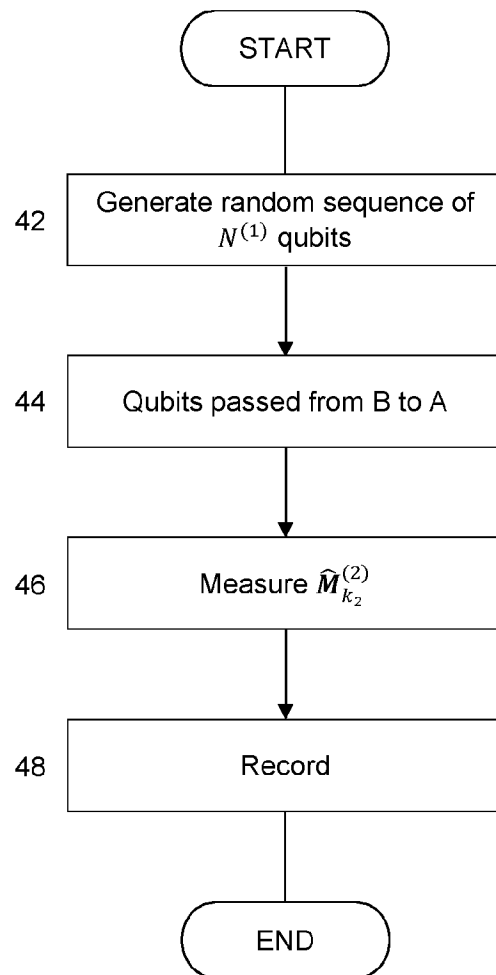
40

FIGURE 4

INTERNATIONAL SEARCH REPORT

International application No
PCT/GB2018/050008

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/08
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2007/011935 A1 (HONEYWELL INT INC [US]; GHOST SUBHAS SKG [IN]) 25 January 2007 (2007-01-25) paragraph [0020] - paragraph [0037]; figure 5 paragraph [0044] - paragraph [0051] ----- -/-	1-66



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

5 March 2018

Date of mailing of the international search report

12/03/2018

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Tenbieg, Christoph

INTERNATIONAL SEARCH REPORT

International application No
PCT/GB2018/050008

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	GHOSH S K ET AL: "A plan-commit-prove protocol for secure verification of traversal path", NETWORKS, 2004. (ICON 2004). PROCEEDINGS. 12TH IEEE INTERNATIONAL CONFERENCE ON SINGAPORE 16-19 NOV. 2004, PISCATAWAY, NJ, USA, IEEE, US, vol. 2, 16 November 2004 (2004-11-16), pages 458-462, XP010778590, DOI: 10.1109/ICON.2004.1409208 ISBN: 978-0-7803-8783-6 Ch. I, II, III -----	1-66
A	ROBERT A MALANEY: "Location-Dependent Communications using Quantum Entanglement", ARXIV.ORG, CORNELL UNIVERSITY LIBRARY, 201 OLIN LIBRARY CORNELL UNIVERSITY ITHACA, NY 14853, 4 March 2010 (2010-03-04), XP080394291, DOI: 10.1103/PHYSREVA.81.042319 page 1 - page 7 -----	1-66
A	US 2006/022832 A1 (KENT ADRIAN P [GB] ET AL) 2 February 2006 (2006-02-02) paragraph [0026] - paragraph [0043] paragraph [0059] - paragraph [0068] -----	1-66

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/GB2018/050008

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2007011935 A1	25-01-2007	US 2007014411 A1 WO 2007011935 A1	18-01-2007 25-01-2007
US 2006022832 A1	02-02-2006	NONE	