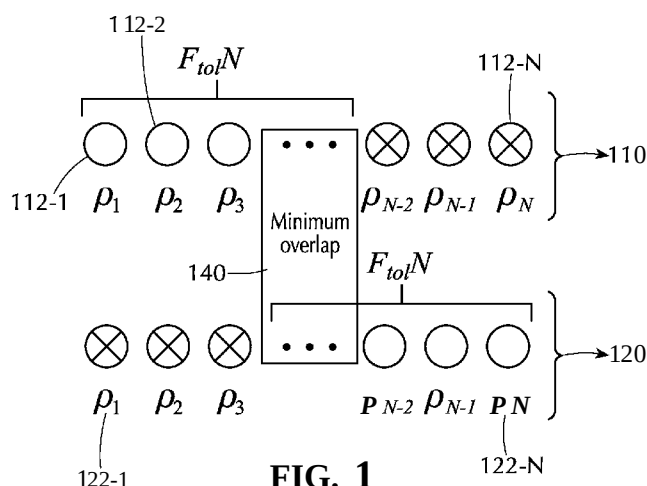




- (51) **International Patent Classification:**
H04L 9/00 (2006.01) *G06Q 40/02* (2012.01)
H04L 9/32 (2006.01)
- (21) **International Application Number:**
PCT/US2012/071564
- (22) **International Filing Date:**
23 December 2012 (23. 12.2012)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
61/579,805 23 December 2011 (23. 12.2011) US
- (71) **Applicant: PRESIDENT AND FELLOWS OF HARVARD COLLEGE** [US/US]; 17 Quincy Street, Cambridge, MA 02138 (US).
- (72) **Inventors: PASTAWSKI, Fernando;** Max-planck-institute Fur Quantenoptik, 85748 Garching (DE). **CIRAC, J., Ignacio;** Max-Planck-Institute Fur Quantenoptik, 85748 Garching (US). **JIANG, Liang;** Institute For Quantum Information, Caltech, Pasadena, CA 91125 (US). **YAO, Norman;** 3 Langdon St. Apt. 44, Cambridge, MA 02138 (US).
- (72) **Inventor (for US only): LUKIN, Mikhail;** Harvard University, Department Of Physics, 60 Garden Street, Cambridge, MA 02138 (US).
- (74) **Agent: KIM, Elizabeth;** Elizabeth Kim Patent Law Offices LLC, 43 Hackensack Road, Chestnut Hill, MA 02467 (US).
- (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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, 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, 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, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, 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, ML, MR, NE, SN, TD, TG).
- Published:**
— with international search report (Art. 21(3))

[Continued on next page]

(54) **Title:** UNFORGEABLE NOISE-TOLERANT QUANTUM TOKENS

(57) **Abstract:** A quantum ticket is defined by a unique serial number; and a set of qubits, each qubit encoding quantum information. The serial number and the set of qubits are distributed only among one or more trusted verifiers who require a tolerance fidelity F_{oi} in order to authenticate the token, where F_{oi} represents a minimum percentage of correct outcomes during authentication of the serial number and the set of qubits. The experimental fidelity F_{exp} for the quantum token is greater than the F_{oi} set by the verifiers, so that an honest user of the quantum ticket who achieves F_{exp} is exponentially likely to be successfully authenticated when seeking authentication by any of the trusted verifiers. The forging fidelity F_{forg} for the quantum token is less than F_{oi} , so that a dishonest user who achieves F_{forg} and attempts forgery of the quantum ticket is exponentially likely to fail to obtain authentication for his forged ticket.

-
- *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

UNFORGEABLE NOISE-TOLERANT QUANTUM TOKENS

[001] CROSS-REFERENCE TO RELATED APPLICATIONS

[002] The present application is based upon, and claims the benefit of priority under 35 U.S.C. § 119, to co-pending United States Provisional Patent Application No. 61/579,805 (the "'805 provisional application"), filed December 23, 2011 and entitled "Unforgeable Noise-Tolerant Quantum Tokens." The content of the '805 provisional application is incorporated herein by reference in its entirety as though fully set forth.

[003] BACKGROUND

[004] The laws of quantum mechanics, in particular the no-cloning theorem, guarantee that any attempt at counterfeiting a credit card, bank note, bill, coin, or other type of payment-related object will fail if the object is embedded with quantum information. However, this security holds only under perfect conditions, whereas in real life quantum information is subject to noise, decoherence, and operational imperfections, all of which provide loopholes that dishonest users can exploit.

[005] Because it is impossible to completely eliminate these imperfections, the development of secure "quantum money" - type protocols that can tolerate some noise and still remain secure is of practical importance.

[006] BRIEF DESCRIPTION OF THE DRAWINGS

[007] The drawings disclose illustrative embodiments. They do not set forth all embodiments. Other embodiments may be used in addition or instead.

[008] FIG. 1 illustrates a qticket (quantum ticket) in accordance with some embodiments of the present invention, and shows how soundness of the qticket can be proved.

[009] FIG. 2 schematically illustrates a quantum retrieval situation for a cv-qticket (classical verification-qticket) in accordance with some embodiments of the present invention.

[010] FIG. 3 is a table showing one example of verification of a single cv-qticket.

[011] FIG. 4 illustrates a possible use of a cv-qticket to implement a quantum-protected credit card.

[012] FIG. 5 illustrates a dishonest user of a quantum credit card who attempts to copy a concert ticket, by assigning an identical serial number, to allow his henchman to enter using an alternate checkpoint gate.

[013] DESCRIPTION

[014] Illustrative embodiments are discussed in this application. It should be understood that the invention is not limited to the particular embodiments described. The terminology used herein is for the purpose of describing particular embodiments only, and is not intended to be limiting, since the scope of the present invention will be limited only by the appended claims.

[015] Unless defined otherwise, all technical and scientific terms used herein have the same meaning as commonly understood by one of ordinary skill in the art to which this invention belongs. Although any methods and systems similar or equivalent to those described herein can also be used in the practice or testing of the present invention, a limited number of the exemplary methods and systems are described herein.

[016] In the present application, the terms "qticket" and "quantum ticket" have the same meaning, and are used interchangeably.

[017] In the present application, the terms "qubit" and "quantum bit" have the same meaning, and are used interchangeably.

[018] In the present application, the terms "quantum token" and "quantum ticket" have the same meaning, and are used interchangeably.

[019] As known by the laws of quantum mechanics, the possession of an object carrying

quantum information does not guarantee that the holder can extract a complete description. The reason is that, while measurements may provide partial access, they do not necessarily allow for a full reconstruction of the original quantum state, since the act of measurement itself may alter or perturb the quantum state per the Heisenberg uncertainty principle.

[020] "Quantum money" protocols, originally developed by Wiesner, are based on the realization that such quantum properties might allow for the design of a quantum "bank note" which is intrinsically and fundamentally immune to counterfeiting. Recent extensions to Wiesner's original "quantum money" protocol, in particular an extended protocol that makes it possible for quantum tokens to be authenticated via classical public communication with a trusted verifier.

[021] These extended protocols all assume that the verification process is noise-free and can occur perfectly. Practically, this is never the case, however. Any verification process has to condone a certain finite fraction of quantum bit (or qubit) failures, in actuality. With the addition of noise, the security itself of previous extended proposals is at issue.

[022] In some embodiments of the present application, quantum tickets are disclosed that ensure security of the protocol, as well as ensuring tolerance to finite errors associated with encoding, storage and coding of individual quantum bits. Each one of these qtickets is issued by a mint, and consists of a unique serial number and N component quantum states, $p = \bigotimes_i p_i$, where each p_i is drawn uniformly at random from an orthogonal set of eigenstates.

[023] As one example, in some embodiments p_i may be drawn from a set Q of polarization eigenstates of the Pauli spin operators. In these embodiments, Q is given by:

[024] $Q = \{|H\rangle, |L\rangle, |+\rangle, |-\rangle, |0\rangle, |1\rangle\}.$

[025] It should be understood that in other embodiments, eigenstates other than the polarization eigenstates of the Pauli spin operators may be used, as long as the eigenstates are orthogonal.

[026] The mint secretly stores a classical description of p , which is distributed only among one or more trusted verifiers. In order to redeem a qticket, the holder physically deposits it with a trusted verifier, who measures the qubits in the relevant basis. This verifier then requires a minimum fraction F_{tol} of correct outcomes, i.e. correct matchings with the previously stored qubits, in order to authenticate the qticket. Following successful authentication or validation, the only information returned by the verifier is whether the qticket has been accepted or rejected.

[027] The soundness of the above-described qticket is the probability that an honest user is successfully verified or authenticated. Such a probability depends crucially on the experimental fidelities associated with single qubit encoding, storage, and decoding. For a given qubit p_j , a map M_j can be defined, which characterizes the overall fidelity, beginning with the mint's encoding and ending with the verifier's validation. The average channel fidelity for each qubit p_j is then given by:

$$[028] \quad F_j = 1 / |\beta| \sum_{\Lambda} \text{Tr}[P_{\Lambda} M_j(\rho_j)].$$

[029] Using the above definition, the verification probability p_h of an honest user is:

$$[030] \quad p_h = \frac{1}{|Q|} \sum_{p \in Q} \text{Tr}[P_{acc} M(p)] \geq 1 - e^{-ND(F_{exp} \| F_{tol})}.$$

[031] In the above mathematical expression for p_h , P_{acc} represents the projector onto the subspace of valid qtickets, $M = \bigotimes_i M_i$, $F_{exp} = 1/N \sum_i F_i$ is the per qubit average experimental fidelity, and the relative entropy D is a measure of distinguishability between two binary probability distributions.

[032] In the above embodiments, as long as the average experimental fidelity F_{exp} associated with single qubit processes is greater than the tolerance fidelity F_{tol} , an honest user is exponentially likely to be verified. In particular, the likelihood of successful verification is exponential in N , the

number of initial qubits.

[033] In the above-described qticket, each qubit is considered to be in one of six possible states. In this case, more than one bit of information may be extracted by measuring the actual state, which is insufficient to recover the original classical description. As explained above, in other embodiments different sets of qubits or possible quantum states may be used or considered.

[034] As further described below, any attempts to forge two copies from a single qticket will lead at least one of the copies to be sufficiently imperfect, ultimately yielding its rejection at the hands of a trusted verifier, both tickets being imperfect.

[035] FIG. 1 illustrates a qticket (quantum ticket) in accordance with some embodiments of the present invention, and schematically shows how soundness of the qticket can be proved. In FIG. 1, an original qticket 110 has N qubits p_i (indicated with reference numerals 111-1, 111-2, ..., 111-N). Likewise, a cloned qticket 120 has N qubits p_j (indicated with reference numerals 122-1, 122-2, ..., 122-N).

[036] For a given tolerance fidelity F_0 , the qticket 110 having N qubits is only successfully authenticated if it contains at least $F_0 N$ valid qubits. However, for two counterfeit qtickets, not all valid qubits must coincide.

[037] To determine a tight security threshold, the counterfeiting of a single qticket 110 is considered, as depicted in FIG. 1. For a given tolerance fidelity F_0 set by the trusted verifiers, a qticket (containing N qubits) is only accepted if at least $F_0 N$ qubits are validated, i.e. the qticket 110 is only successfully authenticated if it contains at least $F_0 N$ valid qubits. However, for two counterfeit qtickets, not all valid qubits must coincide.

[038] In the event that a dishonest user attempts to generate two qtickets from a single valid original, each must contain a minimum of $F_0 N$ valid qubits to be authenticated, as shown in FIG. 1. In order for each counterfeit qticket to contain $F_0 N$ valid qubits, a minimum of $(2F_0 - 1) N$.

qubits must have been perfectly cloned. Thus, for a set tolerance fidelity in order for a dishonest user to succeed, he or she must be able to emulate a qubit cloning fidelity of at least $2F_{\text{tol}} - 1$.

[039] So long as this fidelity is above a fidelity F_{org} achievable for optimal qubit cloning, as allowed by the laws of quantum mechanics, a dishonest user is exponentially unlikely to succeed in getting his/her forged ticket authenticated:

$$p_d = \frac{1}{|Q|} \sum_{\rho \in Q} \text{Tr}[P_{\text{acc}}^{\otimes 2} T(\rho)] \leq e^{-N D(2F_{\text{tol}} - 1 \| 2/3)}.$$

[040]

[041] where T represents any completely positive trace preserving (CPTP) qticket counterfeiting map. To ensure $2F_{\text{tol}} - 1 > 2/3$, the tolerance fidelity F_{tol} must be greater than $5/6$, which is precisely the average fidelity of copies produced by an optimal qubit cloning map.

[042] While in certain situations, an adversary may be able to sequentially engage in multiple verification rounds, the probability of successfully validating counterfeited qtickets grows at most quadratically in the number of such rounds, and hence, the likelihood of successful counterfeiting can remain exponentially small even for polynomially large numbers of verifications.

[043] The qticket 110 in FIG. 1 is a direct transfer qticket which is physically transferable to trusted verifiers, such as concert tickets, by way of example. In many situations, this assumption of physical deposition may either be impossible or undesirable.

[044] It has been shown that it remains possible, even remotely, for a holder to prove the validity of a token by responding to a set of "challenge" questions; these questions can only be successfully answered by measuring an authentic token. Core to this approach is to ensure that the challenge questions reveal no additional information about the quantum state of the token. The holder of a valid token should be capable of answering any single challenge question correctly yet be restricted to an exponentially small probability of satisfactorily answering two of them.

[045] In some embodiments of the present application, classical verification quantum tickets (or "cv-qtickets") that are robust against noise and operational imperfections are implemented. In contrast to the case of bare qtickets, a cv-qticket holder will be expected to answer challenge questions and hence to measure qubits himself, or with a machine at a store. Alternatively, the cv-qticket holder or user may swipe his quantum credit card at a store, and the machine communicates via a classical channel to one or more trusted verifiers and may directly measure or answer the challenge questions.

[046] The possibility of a dishonest holder participating simultaneously in multiple remote verifications is contemplated. This possibility could in principle offer the counterfeiter an additional advantage with respect to the qticket scenario. In particular, certain measurement strategies, which may be chosen posterior to receiving a set of challenge questions, may yield an increased likelihood for multiple successful authentications.

[047] FIG. 2 schematically illustrates a quantum retrieval type situation for a cv-qticket in accordance with some embodiments of the present invention. In the situation illustrated in FIG. 2, two verifiers 220 and 222 ask a holder 210 complementary challenge questions. As further described below, a challenge question consists of requesting the holder 210 to measure each block of qubits along a basis chosen randomly among either X (shown as 231 in FIG. 2) or Z (shown as 232 in FIG. 2). In the illustrated situation, the optimal strategy for the holder 210 is to measure in an intermediate basis 215. Such a strategy saturates the tolerance threshold, which in the illustrated case is given by:

$$p_{tol}^{cv} = \frac{1 + 1/\sqrt{2}}{2}.$$

[048] One example of a cv-qticket framework utilizes as a building block a set of eight possible two-qubit product states, each consisting of two polarization eigenstates (one along X and the other along Z):

$$s = \{|0, 0\rangle, |0, 1\rangle, |1, 0\rangle, |1, 1\rangle, |+, 0\rangle, |+, 1\rangle, |-, 0\rangle, |-, 1\rangle\}.$$

[050] These states constitute a minimal set with the following properties: (1) Only preparation and measurement of qubit states is required; and (2) Each state enables the deterministic answering of either of two complementary challenge questions, for example, a request to measure both X polarizations or both Z polarizations, thereby automatically ensuring soundness in the case of perfect experimental fidelity. When attempting to use the state to answer two complementary challenges from independent verifiers, on average, only $1 + 1/\sqrt{2}$ of replies is correct. Thus, it is possible for a dishonest user to emulate an experimental fidelity (per qubit) of no more than $1/2 + 1/\sqrt{8} \approx 0.85$ with respect to each verifier.

[051] It should be understood that in other embodiments, the number of two-qubit product states can be different from eight, and orthogonal eigenstates other than polarization eigenstates may be used.

[052] In some embodiments, each cv-qticket may be envisioned as consisting of n blocks, each containing r qubit pairs, and thus, a total of $n * r * 2$ qubits. Again, each of the qubit pairs is chosen uniformly at random from the set S . A challenge question consists of requesting the holder to measure each block (of qubits) along a basis chosen randomly among either X or Z.

[053] FIG. 3 is a table showing an example of verification of a single cv (classical verification) - qticket. In the table set forth in FIG. 3, a cv-qticket with $n = 2$ and $r = 4$ is considered, totaling eight qubit pairs and $F_{tol} = 3/4$ (just for illustrative purposes). In FIG. 3, the prepared qubit-pairs are chosen at random, as are the bank's requested measurement bases (for each block). The holder's answer has at most, a single error per block, which according to $F_{tol} = 3/4$ is allowed. As explained above, secure cv-qtickets require $F_{tol}^{cv} > 1/2 + 1/\sqrt{8}$, and a larger number of constituent qubits.

[054] As depicted in the table in FIG. 3, a valid qubit pair (within a block) is one in which the holder correctly answers the orientation for the particular qubit (within the pair) that was prepared along the questioned basis. For a given tolerance threshold F_{tol}^{cv} , an overall answer will only be

deemed correct if at least $F_{\text{tot}}^{\text{cv}} r$ orientations within each of the n blocks are found valid. The motivation for taking blocks of $2r$ qubits is to exponentially suppress the probability that a counterfeiter provides more than $2F_{\text{tot}}^{\text{cv}} r > (1 \pm 1/\sqrt{2})r$ correct answers among two complementary challenge blocks.

[055] In turn, because any two verifiers choose the questions for each block independently and at random, the probability that there exist no complementary blocks scales exponentially with the number of blocks as 2^{-n} . By contrast, if one were to dismiss this block structure, an adversary would be able to emulate a larger average experimental fidelity $(3/4 + 1/\sqrt{32} \approx 0.93)$ by choosing a measurement basis for each pair dependent on whether the corresponding requests are coinciding or complementary.

[056] By analogy to the direct-transfer qticket case described above, honest users of cv-qtickets are exponentially likely to be verified so long as $F_{\text{ext}} > F_{\text{tot}}^{\text{cv}}$. In particular, because there now exist n blocks of qubits, each of which can be thought of as an individual qticket (with r qubits), the probability P_h^{cv} that the honest user will be successfully verified is given by:

$$P_h^{\text{cv}} \geq (1 - e^{-rD(F_{\text{ext}} \| F_{\text{tot}}^{\text{cv}})})^n$$

[057]

[058] Mathematical proofs of cv-qticket security for the above-described cv-qticket based upon a generalized formalism of quantum retrieval games, in combination with a generalized Chernoff-Hoeffding bound, are provided in Exhibit ii (the Supplemental Information section) of the '805 provisional application, the contents of which have been incorporated by reference in their entireties.

[059] So long as $F_{\text{tot}}^{\text{cv}} > 1/2 + 1/\sqrt{8}$, a dishonest user is exponentially unlikely to be authenticated by two independent verifiers. The threshold $1/2 + 1/\sqrt{8}$ corresponds exactly to that achievable by either covariant qubit cloning or by measurement in an intermediate basis (as

illustrated in FIG. 2), suggesting that both such strategies may be optimal.

[060] Likewise, by analogy to the direct-transfer qticket case described in conjunction with FIG. 1, a dishonest user of a cv-qticket is also exponentially likely to fail, with a probability p_d^{cv} given by:

$$[061] \quad p_d^{cv} \leq \binom{v}{2}^2 (1/2 + e^{-rD(F_{in}^{cv} \| 1/2 + 1/\sqrt{8})})^n,$$

[062] where v represents the number of repeated verification attempts.

[063] In the above equation, the factor of $\binom{v}{2}^2$ results from a combinatorial statement accounting for the possibility of choosing which challenge question to answer first and then waiting for feedback from the verifier. Thus, so long as the hierarchy of fidelities is such that:

$1/2 + 1/\sqrt{8} < p_{t_{01}}^{cv} < p_{e_{xp}}$, it is possible to mathematically prove both soundness and security of the cv-qtickets protocol. Further details of such proof is found in Exhibit II of the '805 provisional application, the contents of which are incorporated herein by reference in their entireties.

[064] In some embodiments, the primitives described above may be applied to practically relevant protocols. As one example, one might imagine a composite cv-qticket that allows for multiple verification rounds while also ensuring that the ticket cannot be split into two independently valid subparts. Such a construction may be used to create a quantum-protected credit card.

[065] FIG. 4 illustrates one example of a possible use of the above-described cv-qticket framework to implement a quantum-protected credit card. In the situation illustrated in FIG. 4, a user 420 has been cv-qticket issued by a quantum bank (shown as "Qbank" in FIG. 4) 410, in the form of a QBank card 422. A thief 430 clones two identical copies 432 of the Qbank card 422, and

attempts to use the copies 432 in different stores, shown as store 1, store 2, and store 3.

[066] The classical communication that takes place with the issuer (for example a bank) to verify the cv-qticket, via challenge questions, may be intentionally publicized to a merchant who needs to be convinced of the card's validity. By contrast to modern credit card implementations, such a quantum credit card would be unforgeable and hence immune to fraudulent charges, as illustrated in FIG. 4. Unlike its classical counterpart, the quantum credit card would naturally be unforgeable, preventing thieves from being able to simply copy credit card information and perform remote purchases.

[067] FIG. 5 illustrates a situation where the trusted verifiers may not possess a secure communication channel with each other. In particular, FIG. 5 illustrates a dishonest user 460 who seeks to copy multiple concert tickets 462 and 472, i.e. to create more than one concert ticket with the same serial number. The dishonest user 460 attempts to make it possible for his henchman or friend 470 to enter the concert 450 at an alternate checkpoint gate 456 ("Gate 2"), different from his own checkpoint gate 455 ("Gate 1").

[068] Naively, each verifier (at gates 455 and 456, respectively) would be thought as being able to communicate with one another to prevent such abusive ticket cloning. However, such a safeguard can be overcome in the event that the communication among verifiers is either unsecured, unavailable, or severed (possibly by the dishonest user himself). The qticket is exempt from this type of attack because security is guaranteed even in the case of isolated verifiers.

[069] A classical solution would involve gate verifiers communicating amongst one another to ensure that each ticket serial number is only allowed entry a single time. As shown in FIG. 5, however, such a safeguard can be overcome in the event that communication has been severed. By contrast, a concert ticket based upon the proposed qticket primitive would be automatically secure against such a scenario. Indeed, the security of qtickets is guaranteed even when verifiers are assumed to be isolated. This kind of isolation may be especially useful for applications involving quantum identification tokens, where multiple verifiers may exist who are either unable or

unwilling to communicate with one another.

[070] The above embodiments have described quantum primitives based upon single tokens. Natural extensions to the case of multiple identical quantum tickets open up the possibility of even more novel applications.

[071] In some embodiments of the present application, the above threshold results are extended to the case where c identical copies of the quantum ticket are issued. In this case, to ensure that the production of $c + 1$ valid tokens is exponentially improbable, the required threshold fidelity must be greater than $1 - \frac{1}{(c+1)^{lr+2}}$.

[072] The existence of such multiple identical tokens can provide a certain degree of anonymity for users and could be employed in primitives such as quantum voting.

[073] Rigorous mathematical proofs of the soundness and security of direct-transfer qtickets, described in conjunction with FIG. 1, and of classically verifiable cv-tickets are provided in Exhibit II of the '805 provisional application, the contents of which have been incorporated by reference in their entirety.

[074] In some embodiments, a processing system may be configured and used to implement the methods, systems, and techniques described in the present application. The processing system may include, or may consist of, any type of microprocessor, nanoprocessor, microchip, or nanochip. The processing system may be selectively configured and/or activated by a computer program stored therein. It may include a computer-usable medium in which such a computer program may be stored, to implement the methods and systems described above. The computer-usable medium may have stored therein computer-usable instructions for the processing system. The methods and systems in the present application have not been described with reference to any particular programming language; thus it will be appreciated that a variety of platforms and programming languages may be used to implement the teachings of the present application.

[075] In some embodiments, a computer-usable medium having stored therein computer-readable instructions for a processing system, wherein said instructions when executed by said processing system cause the processing system to measure a set of qubits in a quantum ticket and compare the measured values with stored values, and to authenticate the quantum ticket only if the correct outcomes are greater than a tolerance fidelity F_{t0} .

[076] In sum, a novel class of secure "quantum money"-type primitives capable of tolerating realistic infidelities have been disclosed, and their tolerance to noise has been shown. The protocols proposed in the present application require only the ability to prepare, store, and measure single quantum bit memories, making their experimental realization accessible with current technologies.

[077] Nothing that has been stated or illustrated is intended to cause a dedication of any component, step, feature, object, benefit, advantage, or equivalent to the public. While the specification describes particular embodiments of the present disclosure, those of ordinary skill can devise variations of the present disclosure without departing from the inventive concepts disclosed in the disclosure. While certain embodiments have been described, it is to be understood that the concepts implicit in these embodiments may be used in other embodiments as well. In the present disclosure, reference to an element in the singular is not intended to mean "one and only one" unless specifically so stated, but rather "one or more." All structural and functional equivalents to the elements of the various embodiments described throughout this disclosure, known or later come to be known to those of ordinary skill in the art, are expressly incorporated herein by reference.

What is claimed is:

1. A quantum ticket, comprising

a unique serial number; and

N component quantum qubits $p = \bigotimes_{i=1}^N |p_i\rangle$ ($i = 1, \dots, N$);

wherein the serial number and p are distributed only among one or more trusted verifiers who require a tolerance fidelity F_{tol} in order to authenticate the token, F_{tol} representing a minimum percentage of correct outcomes during authentication of S and p;

wherein an experimental fidelity F_{exp} for the quantum token is greater than F_{tol} ; and

wherein an honest user of the quantum ticket who achieves F_{exp} is exponentially likely to be successfully authenticated when seeking authentication by direct transfer to any of the trusted verifiers.

2. The quantum ticket of claim 1, wherein a forging fidelity F_{forg} for the quantum token is less than F_{tol} , such that a dishonest user who achieves F_{forg} and attempts forgery of the quantum ticket is exponentially unlikely to be successfully authenticated when seeking authentication by direct transfer to any of the trusted verifiers, so that:

$$F_{forg} < F_{tol} < F_{exp}.$$

3. The quantum ticket of claim 1, wherein each one of the qubits are drawn at random from an orthogonal set of eigenstates.

4. The quantum ticket of claim 3, wherein the eigenstates are polarization eigenstates of the Pauli spin operators, and wherein the polarization eigenstates are given by:

$$\{|0\rangle, |1\rangle, |+\rangle, |-\rangle, |+\dot{i}\rangle, |-\dot{i}\rangle\}.$$

5. The quantum ticket of claim 1, wherein the quantum ticket has a soundness corresponding to a probability P_h that the honest user be successfully authenticated when seeking authentication by direct transfer to any of the trusted verifiers, and wherein the probability P_h is given by:

$$p_h = \frac{1}{|Q|} \sum_{\rho \in Q} \text{Tr}[P_{\text{acc}} M(\rho)] \geq 1 - e^{-ND(F_{\text{exp}} \| F_{\text{tgt}})},$$

where $Q = \tilde{Q}^{\otimes N}$;

P_{acc} represents a projector onto the subspace of valid tickets;

$$M = \bigotimes_i M_i;$$

$F_{\text{exp}} = 1/N \sum_i F_i$ is a per qubit average experimental fidelity; and

relative entropy D is a measure of distinguishability between two binary probability distributions.

6. The quantum ticket of claim 2, wherein the quantum ticket has a security corresponding to a probability P_d that a dishonest user fails to have his forged ticket authenticated when seeking authentication by direct transfer to any of the trusted verifiers, and wherein the probability P_d is given by:

$$p_d = \frac{1}{|Q|} \sum_{\rho \in Q} \text{Tr}[P_{\text{acc}} T(\rho)] \leq e^{-ND(2F_{\text{tgt}} - 1)^2/3},$$

7. The quantum ticket of claim 2, wherein for a given F_{tgt} , a minimum forging fidelity F_{forg} that a dishonest user must emulate, in order to have a ticket that he forged successfully authenticated, is given by:

$$F_{\text{forg}} < 2 F_{\text{tgt}} - 1.$$

8. The quantum ticket of claim 2, wherein F_{to} and F_{forg} are defined so that any attempt by any user at forging more than one the quantum ticket leads to both of the copies being sufficiently imperfect so as to be rejected by all the trusted verifiers.

9. The quantum ticket of claim 2, wherein upon issuance of c identical copies of the quantum ticket, a tolerance fidelity F_{tol} that is required in order to exclude the possibility that a $(c + 1)^{\text{th}}$ copy of the quantum ticket be successfully verified, is greater than:

$$1 - \frac{1}{(c+1)(c+2)}.$$

10. The quantum ticket of claim 9, wherein a probability $P_{c \rightarrow c+1}$ that a $(c + 1)^{\text{th}}$ copy of the quantum ticket is successfully verified, after C identical copies of the quantum ticket have been issued, is less than or equal to:

$$e^{-ND((c+1)F_{\text{tol}} - c\| \frac{c+1}{c+2})}.$$

11. A quantum ticket, comprising:

a unique serial number; and

a set containing a plurality N of two-qubit product states, each state allowing for a deterministic answering of either one of two complementary challenge questions, the serial number and the set of two-qubit product states distributed only among one or more trusted verifiers who require a tolerance fidelity $F_{\text{tol}}^{\text{cv}}$ in order to remotely verify the token through a classical channel;

wherein an experimental fidelity F_{exp} for the classically verifiable quantum token is greater than $F_{\text{tol}}^{\text{cv}}$; and

wherein an honest user of the quantum ticket who achieves F_{exp} is exponentially likely to be successfully authenticated when seeking remote verification of the ticket by communication with any of the trusted verifiers over a classical channel.

12. The quantum ticket of claim 11, wherein the quantum ticket has a soundness corresponding to a probability P^{cv}_h that the honest user be successfully authenticated when seeking remote authentication from any of the trusted verifiers through a classical channel, and wherein the probability P^{cv}_h is given by:

$$P^{cv}_h \geq (1 - e^{-rD(F_{cvp} \| F_{old}^{cv})})^n$$

13. The quantum ticket of claim 11, wherein a dishonest user is exponentially unlikely to be authenticated by two independent verifiers, as long as $F_{old}^{cv} > 1/2 + 1/\sqrt{8}$.

14. The quantum ticket of claim 13, wherein the quantum ticket has a security corresponding to a probability P^{cv}_d that a dishonest user fails to obtain authentication for a forged ticket, when seeking remote authentication from any of the trusted verifiers through a classical channel, and wherein the probability P^{cv}_d is given by:

$$P^{cv}_d \leq \binom{v}{2}^2 (1/2 + e^{-rD(F_{old}^{cv} \| 1/2 + 1/\sqrt{8})})^n$$

15. The quantum ticket of claim 11, comprising a quantum credit card.

16. The quantum ticket of claim 11, wherein each one of the plurality N of two-qubit product states comprises two orthogonal eigenstates along mutually perpendicular directions.

17. The quantum ticket of claim 16, wherein $N = 8$, and wherein each one of the two-qubit product states comprises two polarization eigenstates along mutually perpendicular directions; and

wherein the set of polarization eigenstates is given by:

$$\{|0, -\rangle, |0, \rangle, |1, -\rangle, |1, \rangle, |+, 0\rangle, |+, 1\rangle, |-, 0\rangle, |-, 1\rangle\}$$

18. A method comprising:

measuring a set of qubits in a quantum ticket and comparing the measured values with previously stored values, and

authenticating the quantum ticket only if the percentage of correct outcomes are greater than a tolerance fidelity F_{tol} ;

wherein the previously stored values have been distributed only to one or more trusted verifiers.

19. The method of claim 18, wherein the quantum ticket has an experimental fidelity F_{exp} that is greater than F_{tol} , so that an honest user of the quantum ticket who achieves F_{exp} is exponentially likely to be successfully authenticated when seeking authentication from the trusted verifiers.

20. The method of claim 18, wherein the quantum ticket has a forging fidelity F_{forg} that is less than F_{tol} , so that a dishonest user who achieves F_{forg} and attempts forgery of the quantum ticket is exponentially unlikely to be authenticated when seeking authentication from any of the trusted verifiers.

21. The method of claim 20, wherein F_{forg} is a maximum possible fidelity of a forged ticket allowed by quantum mechanics.

22. A computer-usable medium having stored therein computer-readable instructions for a processing system, wherein said instructions when executed by said processing system cause the processing system to measure a set of qubits in a quantum ticket and compare the measured values with stored values, and to authenticate the quantum ticket only if the correct outcomes are greater than a tolerance fidelity F_{tol} .

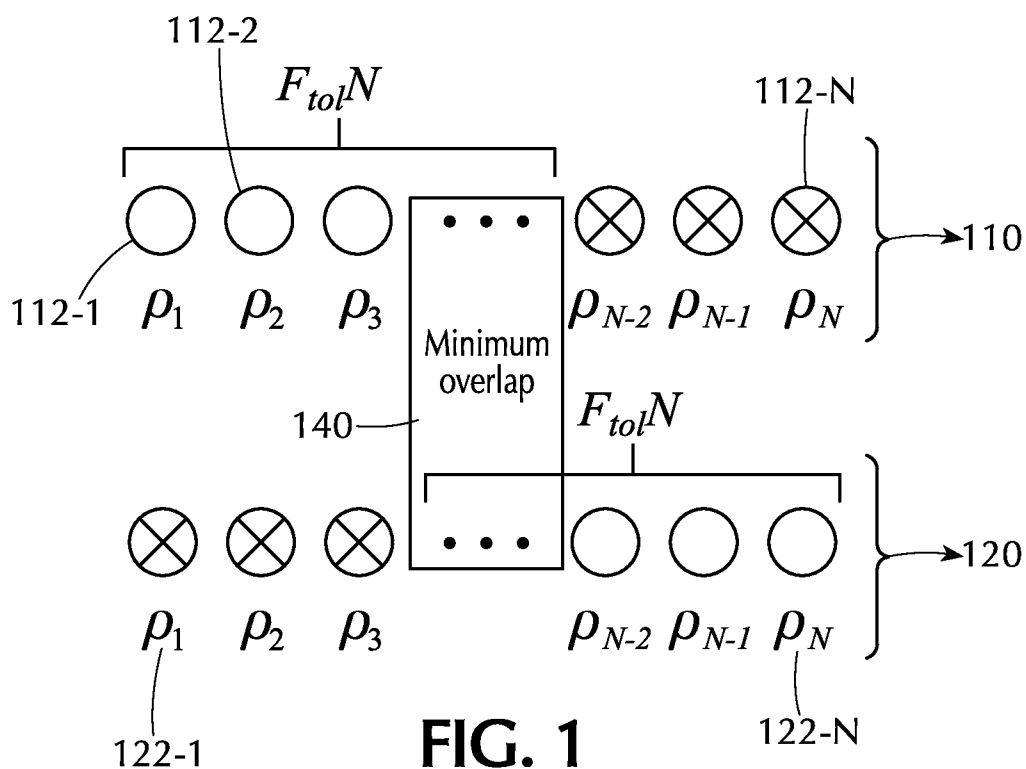


FIG. 1

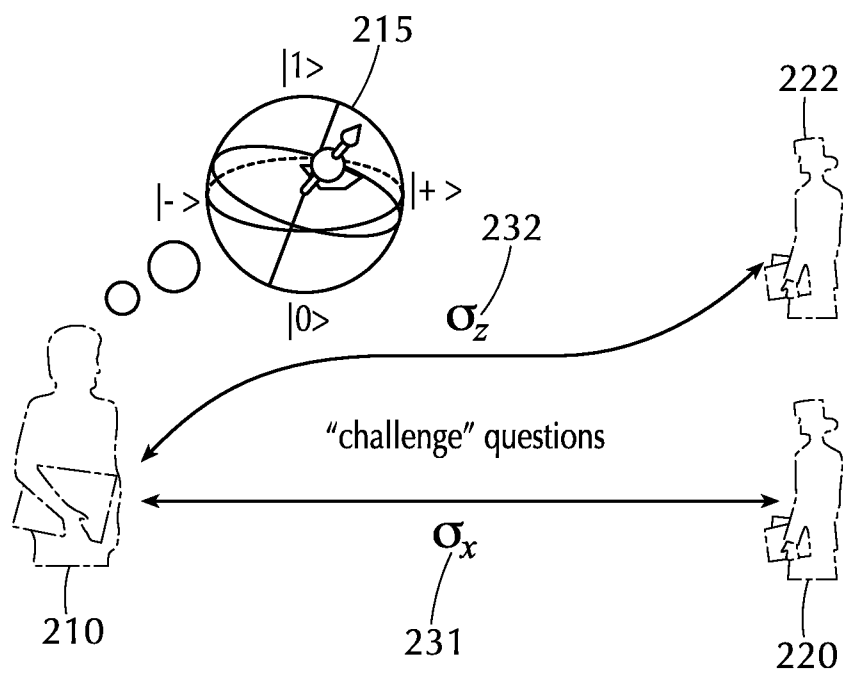


FIG. 2

Table 1

Prepare	$ - , 0 \rangle$	$ 0 , + \rangle$	$ 1 , + \rangle$	$ 0 , + \rangle$	$ 0 , + \rangle$	$ + , 1 \rangle$	$ - , 0 \rangle$	$ 1 , + \rangle$
B:Ask			Z				X	
H:Answer	0,0	0,1	1,1	0,1	$\sim, +$	$+, \sim$	$\sim, +$	$+, \sim$
Correct block	✓	✓	✓	✓	✓	✓	✓	×
B:Result			✓			✓		
				Verified				

FIG. 3

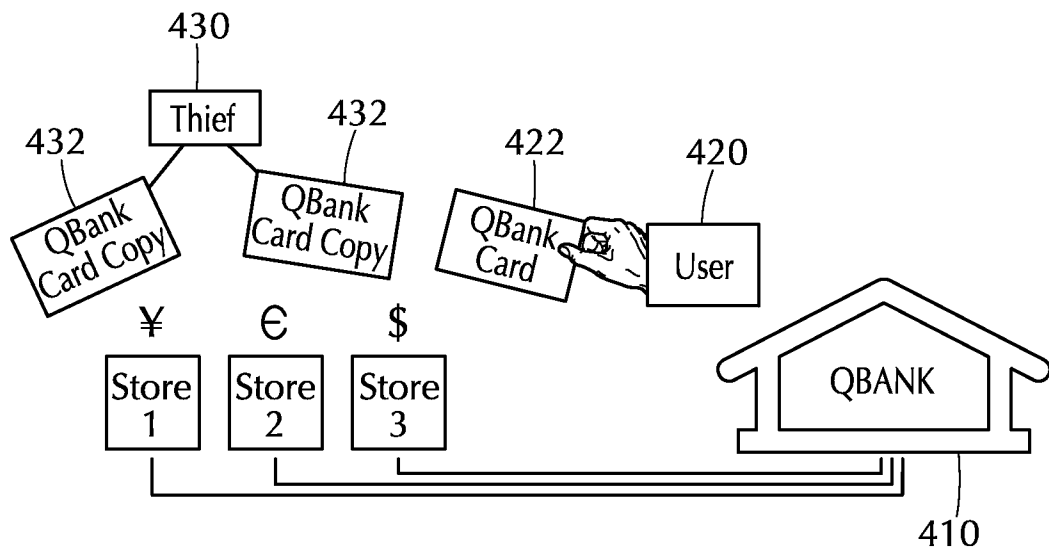


FIG. 4

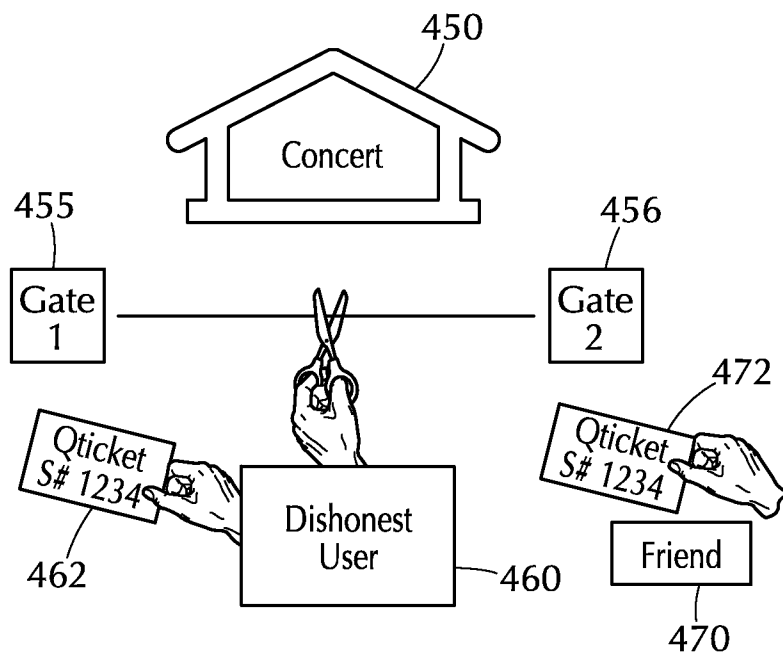


FIG. 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2012/071564**A. CLASSIFICATION OF SUBJECT MATTER****H04L 9/00(2006.01)i, H04L 9/32(2006.01)1, G06Q 40/02(2012.01)1**

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 9/00; H04L 9/32; G06Q 40/00; G06F 21/00

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

Korean utility models and applications for utility models

Japanese utility models and applications for utility models

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

eKOMPASS(KIPO internal) & Keywords: qubit, quantum, token, ticket, fidelity, tolerance, unique serial number, trusted, verify, authenticate

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2005-0249352 Al (CHOI, SORA et al.) 10 November 2005 See paragraphs [16]—[39], [99]; claims 1-5; and figures 1-2.	1-22
A	US 2006-0129486 Al (OHKUMA, KEIJI et al.) 15 June 2006 See paragraphs [117]—[137]; claims 1, 7; and figures 17-19.	1-22
A	US 2010-0212004 Al (FU, YAN) 19 August 2010 See paragraphs [36]—[38], [48]; claims 1-5; and figures 3-5.	1-22
A	US 2005-0157875 Al (NISHIOKA, TSUYOSHI et al.) 21 July 2005 See paragraphs [95]—[120], [146]—[153]; claims 1-3; and figures 1-3.	1-22
A	US 2007-0028113 Al (MOSKOWITZ, SCOTT A.) 1 February 2007 See paragraphs [175]—[179], [240]; claim 1; and figures 1, 3, 9.	1-22

☐ 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 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

03 May 2013 (03.05.2013)

Date of mailing of the international search report

03 May 2013 (03.05.2013)

Name and mailing address of the ISA/KR

Korean Intellectual Property Office
189 Cheongsu-ro, Seo-gu, Daejeon Metropolitan
City, 302-70 1, Republic of Korea

Facsimile No. 82-42-472-7140

Authorized officer

KANG, Hee Gok

Telephone No. 82-42-481-8264



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2012/071564

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2005--0249352 A1	10 . 11 . 2005	KR 10-0596404 B1 KR 10-2005-0 100074 A US 7496203 B2	03 . 07 . 2006 18 . 10 . 2005 24 . 02 . 2009
us 2006--0 129486 A1	15 . 06 . 2006	CN 1820278 A CN 1820278 CO EP 1683 101 A2 JP 2006-048 153 A Wo 2006-01 1679 A2 Wo 2006-01 1679 A3	16 . 08 . 2006 16 . 08 . 2006 26 . 07 . 2006 16 . 02 . 2006 02 . 02 . 2006 30 . 03 . 2006
us 2010--02 12004 A1	19 . 08 . 20 10	None	
us 2005--0 157875 A1	2 1 . 07 . 2005	AU 2002-338042 A1 CN 1589544 A DE 60220083 D1 DE 60220083 T2 EP 1445890 A1 EP 1445890 A4 EP 1445890 B1 JP 04398374 B2 KR 10-0631242 B1 US 7590244 B2 US 7649996 B2 wo 2004-030270 A1	19 . 04 . 2004 02 . 03 . 2005 2 1 . 06 . 2007 10 . 0 1 . 2008 11 . 08 . 2004 26 . 0 1 . 2005 09 . 05 . 2007 30 . 10 . 2009 02 . 10 . 2006 15 . 09 . 2009 19 . 0 1 . 2010 08 . 04 . 2004
us 2007--0028113 A1	0 1 . 02 . 2007	us 2002-00 10684 A1 us 7 159116 B2 us 7475246 B1 wo 0 1- 18628 A2	24 . 0 1 . 2002 02 . 0 1 . 2007 06 . 0 1 . 2009 15 . 03 . 2001