Unforgeable noise-tolerant quantum tokens

Fernando Pastawski[a,1], Norman Y. Yao[b], Liang Jiang[c], Mikhail D. Lukin[b], and J. Ignacio Cirac[a]

[a]Max-Planck-Institut für Quantenoptik, 85748 Garching, Germany; [b]Physics Department, Harvard University, Cambridge, MA 02138; and [c]Institute for Quantum Information, California Institute of Technology, Pasadena, CA 91125

Edited by Peter W. Shor, Massachusetts Institute of Technology, Cambridge, MA, and approved August 23, 2012 (received for review February 29, 2012)

The realization of devices that harness the laws of quantum mechanics represents an exciting challenge at the interface of modern technology and fundamental science. An exemplary paragon of the power of such quantum primitives is the concept of "quantum money" [Wiesner S (1983) ACM SIGACT News 15:78–88]. A dishonest holder of a quantum bank note will invariably fail in any counterfeiting attempts; indeed, under assumptions of ideal measurements and decoherence-free memories such security is guaranteed by the no-cloning theorem. In any practical situation, however, noise, decoherence, and operational imperfections abound. Thus, the development of secure "quantum money"-type primitives capable of tolerating realistic infidelities is of both practical and fundamental importance. Here, we propose a novel class of such protocols and demonstrate their tolerance to noise; moreover, we prove their rigorous security by determining tight fidelity thresholds. Our proposed protocols require only the ability to prepare, store, and measure single quantum bit memories, making their experimental realization accessible with current technologies.

Contrary to classical intuition, possession of an object carrying quantum information does not guarantee that the holder can extract a complete description. Although measurements may provide partial access, they do not necessarily allow for a full reconstruction of the original quantum state. Wiesner realized that such quantum properties might enable the design of a quantum "bank note," which is fundamentally immune to counterfeiting. Recent extensions to Wiesner's original "quantum money" protocol (1) have garnered significant interest (2–7). One particular extension enables the authentication of quantum tokens via classical public communication with a trusted verifier (8). However, to tolerate noise, the verification process must condone a certain finite fraction of quantum bit (qubit failures); naturally, such a relaxation of the verification process enhances the ability for a dishonest user to forge quantum tokens. It is exactly this interplay that we, here, seek to address, by focusing on a class of "quantum token"-protocols that involve either direct physical or classical-communication verification of qubit memories.

Analysis

Quantum Ticket (Qticket). Our approach to quantum tokens extends the original quantum money primitive (1) by ensuring tolerance to finite errors associated with encoding, storage and decoding of individual quantum bits (qubits). We denote the tokens within our first primitive as quantum tickets (qtickets); each qticket is issued by the mint and consists of a unique serial number and N component quantum states, $\rho = \bigotimes_i \rho_i$, where each ρ_i is drawn uniformly at random from the set, $Q = \{|+\rangle, |-\rangle, |+i\rangle, |-i\rangle, |0\rangle, |1\rangle\}$, of polarization eigenstates of the Pauli spin operators. The mint secretly stores a classical description of ρ, distributed only among 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 in order to authenticate the qticket; following validation, the only information returned by the verifier is whether the qticket has been accepted or rejected.

The soundness of a qticket, i.e., the probability that an honest user is successfully verified, depends crucially on the experimental fidelities associated with single qubit encoding, storage, and decoding. Thus, for a given qubit ρ_i, we define the map, M_i, which characterizes the overall fidelity, beginning with the mint's encoding and ending with the verifier's validation; the average channel fidelity (9) is then given by, $F_i = 1/|\tilde{Q}| \sum_{\rho_i} \text{Tr}[\rho_i M_i(\rho_i)]$. With this definition, the verification probability of an honest user is

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

where $Q = \tilde{Q}^{\otimes N}$, P_{acc} represents the projector onto the subspace of valid qtickets, $M = \bigotimes_i M_i$, $F_{\text{exp}} = 1/N \sum_i F_i$ is the per qubit average experimental fidelity, and the relative entropy D is a measure of distinguishability between two binary probability distributions. Crucially, so long as the average experimental fidelity associated with single qubit processes is greater than the tolerance fidelity, an honest user is exponentially likely to be verified.

We consider each qubit in a qticket to be in one of six possible states; no more than one bit of information may be extracted by measuring the actual state, which is insufficient to recover the original classical description (10). Producing counterfeits without going through a classical description provides a more powerful approach. However, optimal cloning results, which represent a quantitative formulation of the celebrated no-cloning theorem (11) provide tight restrictions on the quality of such "duplicates" (12). Our security proof can be seen as an extension of these results; in particular, we demonstrate that 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.

To determine a tight security threshold, we consider the counterfeiting of a single qticket. For a given tolerance fidelity (F_{tol}) set by the verifiers, a qticket is only accepted if at least $F_{\text{tol}}N$ qubits are validated. In the event that a dishonest user attempts to generate two qtickets from a single valid original, each must contain a minimum of $F_{\text{tol}}N$ valid qubits to be authenticated. As depicted in Fig. 1*A*, in order for each counterfeit qticket to contain $F_{\text{tol}}N$ valid qubits, a minimum of $(2F_{\text{tol}} - 1)N$ 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 $2F_{\text{tol}} - 1$. Crucially, so long as this fidelity is above that achievable for optimal qubit cloning (2/3) (12), a dishonest user is exponentially unlikely to succeed:

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

Author contributions: F.P., N.Y.Y., L.J., M.D.L., and J.I.C. performed research and wrote the paper.

The authors declare no conflict of interest.

This article is a PNAS Direct Submission.

[1]To whom correspondence should be addressed. E-mail: fernando.pastawski@mpq.mpg.de.

This article contains supporting information online at www.pnas.org/lookup/suppl/doi:10.1073/pnas.1203552109/-/DCSupplemental.

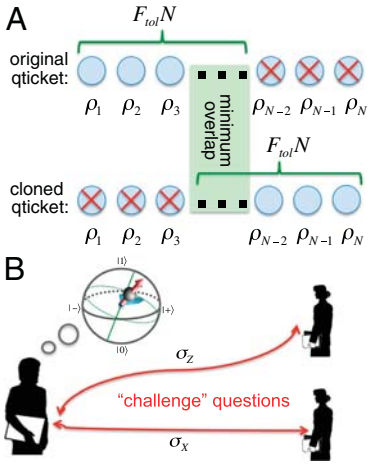

Fig. 1. (*A*) Depicts the pigeonhole type argument that is utilized in the proof of qticket soundness. For a tolerance fidelity F_{tol}, a qticket is only successfully authenticated if it contains at least $F_{\text{tol}}N$ valid qubits. However, for two counterfeit qtickets, not all valid qubits must coincide. The minimum number of perfectly cloned qubits enabling both qtickets to be accepted is $(2F_{\text{tol}} - 1)N$. (*B*) Depicts the quantum retrieval type situation envisioned for cv-qtickets. For two verifiers asking complementary "challenge" questions, the optimal strategy is for the user to measure in an intermediate basis. Such a strategy saturates the tolerance threshold, $F_{\text{tol}}^{\text{cv}} = \frac{1+1/\sqrt{2}}{2}$.

where T represents any completely positive trace preserving (CPTP) qticket counterfeiting map. To ensure $2F_{\text{tol}} - 1 > 2/3$, the tolerance fidelity must be greater than $5/6$, which is precisely the average fidelity of copies produced by an optimal qubit cloning map (12). In certain cases, an adversary may be able to sequentially engage in multiple verification rounds; however, 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. Rigorous statement and proofs of these claims are published as *SI Text* available online.

Classic Verification Qticket (CV-Qticket). Our previous discussion of qtickets assumed that such tokens are physically transferable to trusted verifiers (e.g., concert tickets); however, in many situations, this assumption of physical deposition may either be impossible or undesirable. Recently, it has been shown (8) 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.

We now discuss a specific realization of such an approach, the classical verification quantum ticket (cv-qticket), and demonstrate its robustness against noise and operational imperfections. 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. Our treatment will contemplate the possibility of a dishonest holder participating simultaneously in multiple remote verifications, which 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.

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):

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

These states constitute a minimal set with the following properties: (1) Only preparation and measurement of qubit states is required. (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), thus, automatically ensuring soundness in the case of perfect experimental fidelity. (3) 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 allowing 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.

We then envision each cv-qticket to consist of n blocks, each containing r qubit pairs, and thus, a total of $n \times r \times 2$ qubits; as before, each of the qubit pairs is chosen uniformly at random from 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; naturally, as depicted in Table 1, 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 $F_{\text{tol}}^{\text{cv}}$, an overall answer will only be deemed correct if at least $F_{\text{tol}}^{\text{cv}} r$ 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 $2F_{\text{tol}}^{\text{cv}} r > (1 + 1/\sqrt{2})r$ correct answers among two complementary challenge blocks. 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.

By analogy to the qticket case, honest users are exponentially likely to be verified so long as $F_{\text{exp}} > F_{\text{tol}}^{\text{cv}}$; in particular, because

Table 1. Verification of a single cv-qticket. Here, we consider a cv-qticket with $n = 2$ and $r = 4$, totaling eight qubit pairs and $F_{\text{tol}} = 3/4$ (for illustrative purposes only). 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 $F_{\text{tol}} = 3/4$ is allowed. Secure cv-qtickets require $F_{\text{tol}} > 1/2 + 1/\sqrt{8}$ and a larger number of constituent qubits

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	−,+	+,−	−,+	+,−
Correct block	✓	✓	✓	✓	✓	✓	✓	×
B:Result		✓				✓		
				Verified				

there now exist n blocks of qubits, each of which can be thought of as an individual qticket (with r qubits),

$$p_h^{\mathrm{cv}} \geq (1 - e^{-rD(F_{\mathrm{exp}} \| F_{\mathrm{tol}}^{\mathrm{cv}})})^n. \quad [3]$$

The proof of cv-qticket security is based upon a generalized formalism of quantum retrieval games (8, 13), in combination with a generalized Chernoff–Hoeffding bound (14) (details in *SI Text*). So long as $F_{\mathrm{tol}}^{\mathrm{cv}} > 1/2 + 1/\sqrt{8}$, a dishonest user is exponentially unlikely to be authenticated by two independent verifiers. Interestingly, the threshold $1/2 + 1/\sqrt{8}$ corresponds exactly to that achievable by either covariant qubit cloning (15) or by measurement in an intermediate basis (Fig. 1*B*), suggesting that both such strategies may be optimal (16). Similar to the qticket case, one finds that a dishonest user is exponentially likely to fail:

$$p_d^{\mathrm{cv}} \leq \binom{\nu}{2}^2 (1/2 + e^{-rD(F_{\mathrm{tol}}^{\mathrm{cv}} \| 1/2 + 1/\sqrt{8})})^n, \quad [4]$$

where ν represents the number of repeated verification attempts. We note that the factor of $\binom{\nu}{2}^2$ 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 $1/2 + 1/\sqrt{8} < F_{\mathrm{tol}}^{\mathrm{cv}} < F_{\mathrm{exp}}$, it is possible to prove both soundness and security of the cv-qtickets protocol (see *SI Text* for rigorous statement and proofs).

Applications. Next, we consider applications of the above primitives to practically relevant protocols. For instance, one might imagine a composite cv-qticket that allows for multiple verification rounds while also ensuring that the token cannot be split into two independently valid subparts (8). Such a construction may be used to create a quantum-protected credit card. Indeed, the classical communication that takes place with the issuer (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 (Fig. 2*A*).

An alternate advantage offered by the qticket framework is evinced in the case where verifiers may not possess a secure communication channel with each other. Consider, for example, a dishonest user who seeks to copy multiple concert tickets, enabling his henchmen to enter at different checkpoint gates. 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; however, as shown in Fig. 2*B*, 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. Such 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.

Discussion

Although quantum primitives have been the subject of tremendous theoretical interest, their practical realization demands robustness in the face of realistic imperfections. Our above analysis demonstrates that such noise tolerance can be achieved for certain classes of unforgeable quantum tokens. Moreover, the derived tolerance thresholds are remarkably mild and suggest that proof of principle experiments are currently accessible in systems ranging from trapped ions (17, 18) and superconducting devices (19, 20) to solid-state spins (21–25). In particular, recent advances on single nuclear spins situated in a compact room-temperature solid have demonstrated that ultralong storage times can be attained in combination with high fidelity initialization and readout (24); such advances suggest that quantum devices based upon single qubit quantum memories may be both practical and realistically feasible.

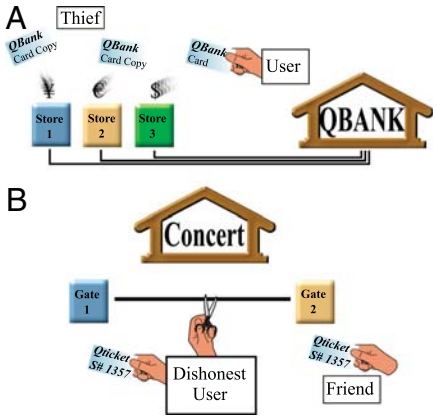

Fig. 2. (*A*) Depicts the possibility of using the cv-qticket framework to implement a quantum-protected credit card. Unlike its classical counterpart, the quantum credit card would naturally be unforgeable, preventing thieves from being able to simply copy credit card information and perform remote purchases. (*B*) Depicts a dishonest user who attempts to copy a concert qticket (e.g., same serial number), enabling his friend to enter at an alternate checkpoint gate. Naively, each verifier can 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.

Although our analysis has focused on describing a primitive based upon single tokens, natural extensions to the case of multiple identical quantum tokens open up the possibility of even more novel applications. In particular, as detailed in the *SI Text*, it is possible to extend our threshold results to the case where c identical copies of the quantum token 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 $1 - \frac{1}{(c+1)(c+2)}$. 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. A crucial question that remains is whether a rigorous proof of anonymity can be obtained in a noisy environment. Furthermore, our proposed quantum tokens can also be seen as a basic noise tolerant building block for implementing more advanced application schemes; such schemes can range from novel implementations of quantum key distribution (16, 26,–28) based upon physical qubit transport to complex one-time-entry identification cards. Beyond these specific applications, a number of scientific avenues can be explored, including for example, understanding whether an interplay between computational assumptions and quantum memories can yield fundamentally new approaches to encryption.

Appendix

We now outline the proof for the security of the qticket protocol that is fully developed in the online *SI Text*. First, the claim in Eq. **2** is restated in terms of an equivalent one, which averages over the set of all pure product states instead of over Q. This reformulation is achieved by invoking the three-design property for the set $\bar{Q}$, i.e., the fact that degree three polynomials in the state may equivalently be averaged over $\bar{Q}$ or over all possible pure qubit states. An explicit expression for P_{acc} is used to show that the security statement has degree three in each component. We then bound the average cloning probability for the set of k-qubit pure product states by $(2/3)^k$, following the lines of

the original proof of optimal cloning by Werner (12). This bound can be seen as limiting the possibility of positively correlating the successful cloning of different components. From this hypothesis, a generalized Chernoff bound (14) applicable to (possibly) dependent random variables allows us to infer the validity of Eq. **2**. Finally, the security with respect to v consecutive verification attempts, allowing for an adaptive counterfeiting strategy, is bound in terms of the situation of Eq. **2**, where a map on a single qticket produces two counterfeits. In particular, we sum over the possible verification outcomes containing at least two positive replies and grouping these into $\binom{v}{2}$ disjoint scenarios. In turn, by fixing the initial verifier replies of each scenario, the adaptive counterfeiting strategy can be reinterpreted as a counterfeiting map.

We now sketch the security proof for cv-qtickets. Abstractly, cv-qtickets consist of a set of randomly produced states and requested challenge questions on these states. The formalism of quantum retrieval games (QRGs) specifically models this scenario (8, 13), allowing one to bound the probability with which optimal strategies can provide correct answers. This framework is presented in a largely self-contained manner because its generality and potential make it of independent interest. Using only the basic definitions for QRGs and some simple properties, we prove that, on average, given a state randomly chosen from S, and the two complementary challenge questions no more than $1 + 1/\sqrt{2}$ of them may be answered satisfactorily. Generalized Chernoff bounds (14) are then applied to bound the likelihood of succeeding at threshold games, i.e., composite games where the correctness of an answer corresponds to correctly providing a certain fraction of the answer components. Full cv-qtickets are then modelled as QRG for scenarios in which the holder of a cv-qticket wishes to simultaneously answer questions from two independent verifiers without any additional aid. Finally, a combinatorial argument, similar to the one used for qtickets, is used to provide a polynomial upper bound on how the double verification probability may increase with the number v of verification attempts.

ACKNOWLEDGMENTS. We thank Y. Chu, C. R. Laumann, and S. D. Bennett for insights and discussions. This work was supported in part by Deutsche Forschungsgemeinschaft (DFG) (SFB 631 and Nanosystem Initiative München NIM), Quantun Computing, Control and Communication (QCCC) elite network Bayern, the European Union project MALICIA, Catalunya Caixa, the National Basic Research Program of China (NBRPC) (973 program), the National Science Foundation (NSF), the Center for Ultracold Atoms (CUA), the Department of Energy (FG0297ER25308), the Defense Advanced Research Projects Agency (DARPA) quantum entanglement science and technology (QuEST), Multi University Research Initiative (MURI), Packard Foundation and the Sherman Fairchild Foundation.

1. Wiesner S (1983) Conjugate coding. *ACM SIGACT News* 15:78–88.
2. Aaronson S (2009) *Quantum Copy-Protection and Quantum Money* (IEEE, Los Alamitos, CA), pp 229–242.
3. Lutomirski A, et al. (2009) Breaking and making quantum money: Toward a new quantum cryptographic protocol. arXiv:0912.3825.
4. Mosca M, Stebila D (2010) Quantum coins. Error-correcting codes, finite geometries and cryptography. *Proc Am Math Soc* 523:35–47.
5. Farhi E, et al. (2010) Quantum state restoration and single-copy tomography for ground states of Hamiltonians. *Phys Rev Lett* 105:190503–190506.
6. Farhi E, Gosset D, Hassidim A, Lutomirski A, Shor P (2010) Quantum money from knots. arXiv:1004.5127.
7. Lutomirski A (2011) Component mixers and a hardness result for counterfeiting quantum money. arXiv:1107.0321.
8. Gavinsky D (2011) Quantum money with classical verification. *Proceedings of the 2012 IEEE Conference on Computational Complexity (CCC)* (IEEE Porto, Portugal), pp 42–52.
9. Nielsen MA (2002) A simple formula for the average gate fidelity of a quantum dynamical operation. *Phys Lett A* 303:249–252.
10. Holevo A (1973) Statistical problems in quantum physics. *Proceedings of the Second Japan-USSR Symposium on Probability Theory. LNM*, eds G Maruyama and Y Prokhorov (Springer, Berlin, Heidelberg), Vol. 330, pp 104–119.
11. Wootters WK, Zurek WH (1982) A single quantum cannot be cloned. *Nature* 299:802–803.
12. Werner RF (1998) Optimal cloning of pure states. *Phys Rev A* 58:1827–1832.
13. Gutoski G, Watrous J (2007) *Toward a general theory of quantum games, STOC 2007* (ACM, New York, NY), pp 565–574.
14. Impagliazzo R, Kabanets V (2010) Constructive proofs of concentration bounds. *Lecture Notes in Computer Science*, (APROX 2010)/(RANDOM 2010), eds M Serna, R Shaltiel, K Jansen, and J Rolim (Springer, Berlin, Heidelberg), Vol. 6302, pp 617–631.
15. Bruss D, Cinchetti M, Mauro D'Ariano G, Macchiavello C (2000) Phase-covariant quantum cloning. *Phys Rev A* 62:012302–012308.
16. Gisin N, Ribordy G, Tittel W, Zbinden H (2002) Quantum cryptography. *Rev Mod Phys* 74:145–195.
17. Hume DB, Rosenband T, Wineland DJ (2007) High-fidelity adaptive qubit detection through repetitive quantum non-demolition measurements. *Phys Rev Lett* 99:120502–120505.
18. Langer C, et al. (2005) Long-lived qubit memory using atomic ions. *Phys Rev Lett* 95:060502.
19. Wendin G (2003) Scalable solid-state qubits: Challenging decoherence and read-out. *Phil Trans R Soc A* 361:1323–1338.
20. Gladchenko S, et al. (2009) Superconducting nanocircuits for topologically protected qubits. *Nat Phys* 5:48–53.
21. Dutt MVG, et al. (2007) Quantum register based on individual electronic and nuclear spin qubits in diamond. *Science* 316:1312–1316.
22. Morton JJL, et al. (2008) Solid-state quantum memory using the 31P nuclear spin. *Nature* 455:1085–1088.
23. Balasubramanian G, et al. (2009) Ultralong spin coherence time in isotopically engineered diamond. *Nat Mater* 8:383–387.
24. Maurer PC, et al. (2012) Room-temperature quantum bit memory exceeding one second. *Science* 336:1283–1286.
25. Steger M, et al. (2012) Quantum information storage for over 180 s using donor spins in a 28Si "semiconductor vacuum". *Science* 336:1280–1283.
26. Bennet CH, Brassard G (1984) Quantum cryptography: Public key distribution and coin tossing. *Proceedings of IEEE International Conference on Computers Systems and Signal Processing* pp 175–179.
27. Gottesman D, Lo H (2003) Proof of security of quantum key distribution with two-way classical communications. *IEEE Trans Inf Theory* 49:457–475.
28. Scarani V, Renner R (2008) Quantum cryptography with finite resources: Unconditional security bound for discrete-variable protocols with one-way postprocessing. *Phys Rev Lett* 100:200501.

Supporting Information

Pastawski et al. 10.1073/pnas.1203552109

SI Text

Notation and External Results. The following definitions and external results will be used extensively throughout the proofs and are included here to provide a self-contained presentation.

Definition 1: A quantum state t-design is a probability distribution over pure quantum states $(p_i, |\psi_i\rangle)$ (or $(p_i, |\psi_i\rangle\langle\psi_i|)$) such that

$$\sum_i p_i (|\psi_i\rangle\langle\psi_i|)^{\otimes t} = \int_{\text{Haar}} (|\psi\rangle\langle\psi|)^{\otimes t} d\psi. \qquad \text{[S1]}$$

In other words, a quantum state t-design duplicates the properties of the unique unitarily invariant Haar measure over quantum states for all polynomials up to degree t. Alternatively, the discrete average and continuous measure of definition 1 may be taken over pure density matrices given that they are insensitive to phases. The equality of the $2t$ leg tensors expressed in definition 1 is actually exploited by contracting each sides of the equality with a tensor that is independent of ψ. By contracting a pair of legs of the resulting tensor with an identity operator, one may verify that a $(t+1)$-design is always a t-design. Indeed, any polynomial expression in $|\psi\rangle\langle\psi|$ with degree at most t can be expressed by the contraction of $(|\psi\rangle\langle\psi|)^{\otimes t}$ with a tensor. This is indeed where the property of t-designs is used in practice for specific polynomials in $|\psi\rangle\langle\psi|$.

Claim 1. (3-design over $\mathscr{H}_2$) The set of pure states

$$\tilde{Q} = \{|0\rangle, |1\rangle, |+\rangle, |-\rangle, |+i\rangle, |-i\rangle\} \qquad \text{[S2]}$$

with equal weights $p_i = 1/6$ constitutes a quantum state 3-design over $\mathscr{H}_2$ (1). By abuse of notation, we will also use $\tilde{Q}$ to denote the associated set of normalized pure density matrices.

The average fidelity for a channel quantifies how well the channel preserves quantum states.

Definition 2: The average fidelity of a map M is defined as

$$F(M) = \int_{\text{Haar}} \langle\psi|M(|\psi\rangle\langle\psi|)|\psi\rangle d\psi = \frac{1}{6}\sum_{|\psi\rangle\in\tilde{Q}} \langle\psi|M(|\psi\rangle\langle\psi|)|\psi\rangle. \qquad \text{[S3]}$$

The last expression is not part of the definition but is derived from the fact that the average fidelity can be expressed as a a Haar average of a degree 2 polynomial in $|\psi\rangle\langle\psi|$ and that $\tilde{Q}$ is a 3-design (and hence also a two-design).

Throughout the text, boolean values $\mathscr{B} = \{\text{True}, \text{False}\}$ will be represented as True $:=1$, False $:=0$ and the negation $\bar{b} := 1-b$. We will also use the variable $\vec{b}$ to denote boolean strings (i.e., ordered sequences of values in $\{0,1\}$) with $\text{len}(\vec{b})$ denoting the length or number of components of a sequence and $tl(\vec{b})$ denoting the string obtained from removing the last element from $\vec{b}$. We will denote by $\mathbf{Pr}[e]$ the probability of an event e and $\mathbf{Exp}[v]$ the expectation value of an expression v. Note that according to our convention, if the expression is a boolean formula they may be used interchangeably.

The relative entropy is a distinguishability measure between two probability distributions. It will be used extensively (particularly among binary or Bernoulli distributions) and appears in the definition of auxiliary results. Let $0 \le p, q \le 1$, by abuse of notation, we take $D(p\|q) = p\ln\frac{p}{q} + (1-p)\ln\frac{1-p}{1-q}$, the relative entropy between two Bernoulli probability distributions with respective parameters p and q. Note that this definition satisfies $D(p\|q) \ge 2(p-q)^2$.

The following generalization of the Chernof–Hoeffding bound derived by Panconesi and Srinivasan (2) provides the same thesis as a standard Chernoff bound while relaxing the hypothesis to allow dependent random variables.

Theorem 1. *(Generalized Chernof–Hoeffding bound) Let $X_1, \ldots, X_n$ be Boolean $\{0,1\}$ random variables, such that for some δ_i and every $S \subseteq \{1,\ldots,n\}$, it holds that $\mathbf{Pr}[\bigwedge_{i\in S} X_i] \le \prod_{i\in S}\delta_i$. Then for any $\gamma \in [\delta, 1]$ we have that $\mathbf{Pr}[\sum_{i=1}^n X_i \ge \gamma n] \le e^{-nD(\gamma\|\delta)}$, with $\delta := n^{-1}\sum_{i=1}^n \delta_i$.*

A further generalization to real valued random variables will also be required. This is adapted to our purpose from theorem 3.3 of Impagliazzo and Kabanets (3).

Theorem 2. *Let $X_1, \ldots, X_n$ be real valued random variables, with each $X_i \in [0,1]$. Suppose that there is a $0 \le \delta \le 1$ s.t., for every set $S \subseteq \{1,\ldots,n\}$, $\mathbf{Exp}[\prod_{i\in S} X_i] \le \delta^{|S|}$ and γ s.t. $\delta \le \gamma \le 1$ and $\gamma n \in \mathbb{N}$. Then we have that $\mathbf{Pr}[\sum_{i=1}^n X_i \ge \gamma n] \le 2e^{-nD(\gamma\|\delta)}$.*

Quantum Tickets (Qtickets). We first provide a rigorous definition of qtickets and how they are verified. We then proceed to our claims and the soundness, security, and tightness of our security bound (accompanied with respective proofs). Namely, we show that qtickets may be successfully redeemed by an honest holder achieving a sufficiently good storage fidelity. We then show that a dishonest holder will have a negligible chance of producing two qtickets that are accepted by verifiers from a single valid qticket, even after repeated verification attempts. Finally we show how a simple counterfeiting strategy has a high probability of producing two such qtickets if the verification tolerance is set below the threshold value. As an extension, we consider how our results generalize to producing multiple identical qtickets.

Definition of qtickets. Each qticket consists of a serial number s and an N component pure product state $\rho^{(s)} = \bigotimes_{i=1}^N \rho_i^{(s)}$. For each serial number s, qticket components $\rho_i^{(s)}$ are chosen uniformly at random from $\tilde{Q}$ (the set of pure density matrices of the 3-design presented in definition 1). This means qtickets $\rho^{(s)}$ are taken uniformly at random from the set $Q = \tilde{Q}^{\otimes N}$ (where by abuse of notation, the elements of Q are density matrices corresponding to the N component pure product states in $\mathscr{H}_Q = \mathscr{H}_2^{\otimes N}$, with components taken from $\tilde{Q}$). The verifiers store a database containing, for each s, a classical description of $\rho^{(s)}$ kept secret from ticket holders and the general public. In order to simplify notation, the serial number s associated to individual qtickets will be omitted from now on.

In order to use qtickets, they are transferred to a verification authority who can either accept or reject them. In both cases, however, the qticket is not returned, only the binary outcome of verification. The qticket protocol is additionally parameterized

by the fraction F_{tol} of quantum bits (qubits) that a verification authority requires to be correct in order for verification to succeed. In order to verify a submitted qticket $\tilde{\rho}$, a full measurement will be performed in the product basis associated to the original qticket ρ and the number of correct outcomes is then counted. If more than at least $F_{\text{tol}}N$ are correct, the (possibly noisy) submitted qticket $\tilde{\rho}$ is accepted; otherwise, it is rejected.

For any pure product state $\rho = \bigotimes_{i=1}^{N} \rho_i$ we define a projector $P_{\text{acc}}^{\rho} \in \mathscr{L}(\mathscr{H}_Q)$ associated to the subspace of states that would be accepted if ρ were a qticket (i.e., states coinciding with ρ in at least a fraction F_{tol} of the qubits). The projector P_{acc}^{ρ} offers a more abstract interpretation and may be rigorously defined as follows.

Definition 3: (Acceptance Projector) Given a pure N qubit product state $\rho = \bigotimes_{i=1}^{N} \rho_i$ and a security parameter $0 \leq F_{\text{tol}} \leq 1$, we define the acceptance projector

$$P_{\text{acc}}^{\rho} = \sum_{\vec{b}\,:\,\sum b_i \geq F_{\text{tol}} N} \bigotimes_{i=1}^{N} (b_i \rho_i + \bar{b}_i \rho_i^{\perp}),$$

where $\vec{b} \in \{0,1\}^N$ is a boolean string.

By abuse of notation, ρ_i and its orthogonal complement $\rho_i^{\perp} \coloneqq 1_2 - \rho_i$ are used as rank 1 projectors in $\mathscr{L}(\mathscr{H}_2)$.

Soundness. The soundness result states that even under imperfect storage and readout fidelity, legitimate qtickets work well as long as the fidelity loss is not too severe. The completely positive trace preserving (CPTP) maps M_i will be assumed to represent the encoding, storage and readout of the i-th qubit component of the qticket. In this sense, the soundness statement takes place at the level of single qubits. This is necessarily the case because legitimate qtickets are ruined if a significant fraction of the qubits fail in a correlated way. Given $F_i = F(M_i)$, the average fidelity of the qubit map M_i, we define $F_{\text{exp}} \coloneqq N^{-1} \sum F_i$ to be the average qubit fidelity of the full map $M = \bigotimes_i M_i$ over all components. The probability that the "noisy" qticket resulting from this map is accepted as valid is given by $p_h(M) = \frac{1}{|Q|} \sum_{\rho \in Q} \text{Tr}[P_{\text{acc}}^{\rho} M(\rho)]$.

Theorem 3. (Soundness of qtickets) *As long as $F_{\text{exp}} > F_{\text{tol}}$, an honest holder can successfully redeem qtickets with a probability*

$$p_h(M) \geq 1 - e^{-ND(F_{\text{tol}} \| F_{\text{exp}})}.$$

Proof: Consider the boolean random variables $\vec{X} = (X_1, \ldots, X_N)$ with joint distribution given by

$$\mathbf{Pr}[\vec{X} = \vec{b}] = \frac{1}{|Q|} \sum_{\rho \in Q} \text{Tr}\left[M(\rho) \bigotimes_{i=1}^{N} (b_i \rho_i + \bar{b}_i \rho_i^{\perp}) \right]. \qquad \textbf{[S4]}$$

Because $M = \bigotimes_i M_i$, we may recast Eq. **S2** as

$$\mathbf{Pr}[\vec{X} = \vec{b}] = \prod_{i=1}^{N} \frac{1}{6} \sum_{\rho_i \in \tilde{Q}} \text{Tr}\left[M_i(\rho_i)(b_i \rho_i + \bar{b}_i \rho_i^{\perp}) \right] \qquad \textbf{[S5]}$$

Because $\tilde{Q}$ is a quantum state two-design over qubit space, each factor coincides with the definition of the average fidelity F_i of M_i if $b_i = 1$ and with $1 - F_i$ if $b_i = 0$. Hence the X_i are independent boolean random variables with probability $\mathbf{Pr}[X_i] = F_i$. Moreover, according to definition 3, we have $\frac{1}{|Q|} \sum_{\rho \in Q} \text{Tr}[P_{\text{acc}}^{\rho} M(\rho)] = \mathbf{Pr}[\sum_{i=1}^{N} X_i \geq F_{\text{tol}} N]$. Because the X_i are independent, a standard Chernof–Hoeffding bound allows us to conclude.

Security. Consider the probability of producing two tokens, both passing verification by means of the most general possible transformation, a CPTP map T, applied on a single genuine qticket.

Definition 4: (Counterfeiting fidelity) We define the average counterfeiting fidelity of a map $T \in \mathscr{H}_Q \to \mathscr{H}_Q^{\otimes 2}$ as

$$p_d(T) = \frac{1}{|Q|} \sum_{\rho \in Q} \text{Tr}[(P_{\text{acc}}^{\rho})^{\otimes 2} T(\rho)] \qquad \textbf{[S6]}$$

Note that definition 4 can also be thought of as N nested averages over the qubit state 3-design $\tilde{Q}$ of each tensor factor ρ_i of ρ.

One of our main results states that as long as the verification threshold F_{tol} is set sufficiently high (>5/6), a counterfeiter will have negligible (exponentially small in N) chances of producing two verified tokens from a single genuine original.

Theorem 4. (Security of qtickets) *For $F_{\text{tol}} > 5/6$ and for any CPTP map $T \in \mathscr{H}_Q \to \mathscr{H}_Q^{\otimes 2}$ we have that*

$$p_d(T) \leq e^{-ND(2F_{\text{tol}} - 1 \| 2/3)}. \qquad \textbf{[S7]}$$

Most of the work for proving this theorem goes into excluding the possibility that a nonproduct counterfeiting strategy could perform significantly better than any product strategy such as performing optimal cloning on each individual qubit. That is, we take into account the fact that the map T need not factorize with respect to the different components of the qticket. Note also that $D(2F_{\text{tol}} - 1 \| 2/3) = 0$ precisely for $F_{\text{tol}} = 5/6$ and is positive otherwise. Finally, we prove that even if the holder of a qticket attempts to perform v succesive verification attempts (each time possibly using information learned from the acceptance/rejection of previous attempts) the chances of having two or more submitted qtickets accepted grows by no more than a factor of $\binom{v}{2}$.

Theorem 5. (Security of qtickets with learning) *If the holder of a valid qticket submits v tokens for verification, the probability of having two or more accepted is upper bounded by*

$$p_{d,v} = \binom{v}{2} e^{-ND(2F_{\text{tol}} - 1 \| 2/3)}.$$

Note that because $\binom{v}{2}$ is a polynomial of degree 2 in v, this bound still allows for an exponentially large number (in N) of qticket submissions v, while preserving exponentially good security.

Proof Outline. We now outline the proof for theorems 4 and 5. First, the claim in theorem 4 is equated to an equivalent one, which averages over the set of all pure product states instead of Q. We then bound the average cloning probability by $(2/3)^N$ for the set of pure product states following the lines of R. F. Werner (4) for the optimal cloning of pure states. From there, the generalized Chernoff bound from theorem 1 for dependent random variables allows us to derive the desired result. The result of theorem 5 is obtained from a counting argument relating the security

of multiple verification attempts with the static counterfeiting fidelity bound of theorem 4.

Equivalence with Continuous Statement. For the qticket protocol, drawing each component from a discrete set of states is required in order to provide an efficient classical description. However, certain statements are simpler to analyze over the full set of pure product states. This is the case for the counterfeiting fidelity, which can also be expressed as a uniform average over all pure product states.

Lemma 1. (Counterfeiting fidelity) *The average counterfeiting fidelity of a map T can be expressed as*

$$p_d(T) = \int d\vec{\rho}\ \mathrm{Tr}[(P_{\mathrm{acc}}^{\vec{\rho}})^{\otimes 2} T(\vec{\rho})] \qquad \textbf{[S8]}$$

where $\int d\vec{\rho}$ represents N nested integrations on the Haar measure of qubit components $\int d\rho_1 \cdots \int d\rho_N$ and $\vec{\rho} = \rho_1 \otimes \cdots \otimes \rho_N$ is the resulting product state.

Proof: Definition 4 and lemma 1 express $p_d(T)$ as the average of the same expression over a discrete (respectively continuous) set of product states. Our claim is that the nested continuous averages of lemma 1 can be transformed one by one into nested discrete averages over the 3-design $\tilde{Q}$, eventually coinciding with definition 4. To prove this claim using the definition of 3-designs, we must ensure that, as a function of any tensor factor ρ_i of $\vec{\rho}$, the expression $\mathrm{Tr}[(P_{\mathrm{acc}}^{\vec{\rho}})^{\otimes 2} T(\vec{\rho})]$ can be expressed as a polynomial of degree at most 3.

Definition 3 may seem unnecessarily cumbersome, yet it serves to make explicit that the projector P_{acc}^{ρ} can be expressed as a multivariable polynomial with total degree N but degree 1 in each of the tensor factors ρ_i of the qticket ρ. Inspection of definition 3 allows us to ascertain that the set of monomials summing to P_{acc}^{ρ} is statically defined by F_{tol} and each monomials has degree at most 1 in each of the tensor components ρ_i of ρ. Furthermore, note that regardless of what the multiqubit map T is, its application $T(\rho)$ has degree 1 on ρ and hence on every tensor factor ρ_i of a product state ρ. Hence, the integrand of lemma 1 is a polynomial of degree at most 3 in each of the qubit components ρ_i of $\vec{\rho}$. We may hence replace the nested integrals one by one by averages over $\tilde{Q}$ reaching the expression of definition 4 after N steps.

Optimal Cloning for Pure Product States. R. F. Werner (4) obtained a tight upper bound for the average probability of a CPTP map T producing m clones from n copies of an unknown pure quantum state $|\psi\rangle$. Our statement is that if one attempts to clone an N component pure product state, the optimal cloning probability is achieved by independently cloning each of the components; neither generating entanglement nor correlations may help with the cloning. We present this statement for the case of cloning two copies from a qubit product state, but the derivation is fully generalizable.

Lemma 2. (Optimal cloning of pure product states) *The average cloning fidelity over N qubit component pure product states of a CPTP map T is bounded by*

$$\int d\vec{\rho}\,\mathrm{Tr}[\vec{\rho}^{\otimes 2} T(\vec{\rho})] \leq (2/3)^N.$$

Proof: One possible derivation of this lemma is by following the lines of the original proof for optimal cloning of pure states (4). First one shows that if there is a CPTP map T achieving average cloning fidelity $F^\star$ then there is a covariant CPTP map $T^\star$ achieving the same average cloning fidelity. This map can be explicitly constructed as

$$T^\star(\vec{\rho}) = \int d\vec{g}\ \vec{g}^{\dagger\otimes 2} T(\vec{g}\,\vec{\rho}\,\vec{g}^{\dagger}) \vec{g}^{\otimes 2}, \qquad \textbf{[S9]}$$

where the integral $\int d\vec{g}$ averages over all possible local rotations $\vec{g}$ on N subsystems. This covariant map achieves exactly the same cloning fidelity for any initial pure product state because all pure product states are equivalent up to local unitaries.

Finally, we observe

$$0 \leq \mathrm{Tr}[\vec{\rho}^{\otimes 2} T^\star(1_{2^N} - \vec{\rho})] \qquad \textbf{[S10]}$$

because $1_{2^N} - \vec{\rho}$ is positive and $T^\star$ positivity preserving. We then obtain

$$F^\star \leq \mathrm{Tr}[\vec{\rho}^{\otimes 2} T^\star(1_{2^N})] \qquad \textbf{[S11]}$$

and may now average this inequality over $\vec{\rho}$ and use

$$\int d\vec{\rho}\ \vec{\rho}^{\otimes 2} = \frac{(S_2)^{\otimes N}}{3^N}, \qquad \textbf{[S12]}$$

where S_2 is the rank 3 projector onto the symmetric space of two qubits. The operator norm of this expression is $1/3^N$ whereas $\mathrm{Tr}[T^\star(1_{2^N})] \leq 2^N$ leading to $F^\star \leq (\frac{2}{3})^N$, as desired.

Pigeonhole Argument and Chernoff Bound. We are now ready to prove the first no-counterfeiting result for qtickets.

Proof of Theorem 4: Consider the boolean random variables $\vec{E} = (E_1, \ldots, E_N)$ with joint distribution given by

$$\mathbf{Pr}[\vec{E} = \vec{b}] = \int d\vec{\rho}\,\mathrm{Tr}\left[T(\vec{\rho}) \bigotimes_{i=1}^{N} (b_i \rho_i^{\otimes 2} + \bar{b}_i (1_4 - \rho_i^{\otimes 2}))\right]. \qquad \textbf{[S13]}$$

Intuitively, the variable E_i represents the event of measuring the i-th component to be correctly cloned.

In order for the two qtickets to be accepted, there must be a total of at least $F_{\mathrm{tol}} N$ components yielding the correct measured outcome in each qticket. By the pigeonhole principle, there are at least $2F_{\mathrm{tol}}N - N$ components that were measured correctly on both submitted qtickets,

$$p_d(T) \leq \mathbf{Pr}\left[\sum_{i=1}^{N} E_i \geq (2F_{\mathrm{tol}} - 1)N\right]. \qquad \textbf{[S14]}$$

For arbitrarily chosen T, the E_i may be dependent variables. However, according to lemma 2, for any subset S of qubit components, we may bound

$$\mathbf{Pr}[\forall_{i \in S} E_i] \leq \left(\frac{2}{3}\right)^{|S|}. \qquad \textbf{[S15]}$$

Theorem 1 is now invoked to provide an upper bound on the RHS of Eq. **S14**, yielding the thesis of theorem 4.

Combinatorial Bound on Learning. The bound on counterfeiting that we have provided assumes that two (possibly entangled) counterfeits are produced by applying a CPTP map on a single original copy. In contrast, a sequential strategy temporally orders the sub-

mitted qtickets where the production strategy (CPTP map) for the later submissions can depend on whether previous submissions where accepted or not. The counterfeiter may learn valuable information about how to construct valid qtickets from the feedback provided by the verifiers. The content of theorem 5 is that even with a valid qticket and the information learned from v repeated submissions it is very unlikely for a counterfeiter to produce more than one accepted qticket.

Proof of Theorem 5: According to theorem 4, the probability $p_d(T)$ for any CP map T to produce two valid counterfeit copies from a single one is upper bounded by $B = e^{-ND(2F_{\text{tol}}-1\|2/3)}$. We bound the counterfeiting probability of an interactive strategy S submitting v tokens for verification by the sum of the counterfeiting fidelity of $\binom{v}{2}$ CP maps $T_{k,l}$. Each of these maps corresponds to the case in which a specific pair $\{k, l\}$ of the v submitted tokens are the first to be accepted by the verifiers.

Without loss of generality, we assume that in an interactive strategy the holder waits for the outcome of the j-th verification in order to decide how to continue and produce the $j+1$-th submission. We model a v step interactive strategy S as a collection of CPTP maps $\{S_{\vec{b}}\}$ with $\vec{b}$ a boolean string of length between 0 and $v-1$ representing what the counterfeiter does after receiving the first $\text{len}(\vec{b})$ verification outcomes.

Each $S_{\vec{b}}$ is a CPTP map from $\mathcal{H}_H$ to $\mathcal{H}_Q \otimes \mathcal{H}_H$, where $\mathcal{H}_Q$ is a Hilbert space accommodating qtickets and $\mathcal{H}_H$ is a larger space representing the memory of the holder. Fig. S1 illustrates information flow as understood for both the interactive and non-interactive scenarios.

For any partial verification result $\vec{b}$ we may write the CPTP map which produces the $\text{len}(\vec{b})$ submissions as $\tilde{S}_{tl(\vec{b})}$, which is composed of successively applying $S_{\vec{b}'}$ for all initial substrings $\vec{b}'$ of $\vec{b}$. That is

$$\tilde{S}_{\varnothing} \coloneqq S_{\varnothing} \qquad \tilde{S}_{\vec{b}} \coloneqq (\text{id}_Q^{\otimes \text{len}(\vec{b})} \otimes S_{\vec{b}}) \circ \tilde{S}_{tl(\vec{b})}. \qquad \textbf{[S16]}$$

For an interactive strategy S the probability that the first $\text{len}(\vec{b})$ verification outcomes are given by $\vec{b}$ is expressed as

$$p_{\vec{b}}(S) = \frac{1}{|Q|} \sum_{\rho \in Q} \text{Tr}\left[\tilde{S}_{tl(\vec{b})}(\rho) \bigotimes_{j=1}^{\text{len}(\vec{b})} (b_j P^{\rho}_{\text{acc}} + \bar{b}_j P^{\rho}_{\text{rej}}) \otimes 1_H\right], \qquad \textbf{[S17]}$$

where $P^{\rho}_{\text{rej}} \coloneqq 1_Q - P^{\rho}_{\text{acc}}$. The probability for the interactive strategy S to succeed at counterfeiting in v steps can be described as the sum of these probabilities over all possible full verification outcomes, including at least two acceptances:

$$p_{d,v}(S) = \sum_{\vec{b} \,:\, \sum_{\text{len}(\vec{b})=v} b_i \geq 2} p_{\vec{b}}(S). \qquad \textbf{[S18]}$$

The key idea now is to use $p_{\vec{b}}(S) = p_{\vec{b}0}(S) + p_{\vec{b}1}(S)$ to provide an alternate expression for this sum. Namely, we combine verification outcomes starting in the same way into a single summand while avoiding the inclusion of failed counterfeiting attempts. Each full verification outcome containing two or more successful verifications has a unique shortest initial substring containing exactly two successful verifications. That a given substring is the shortest can be guaranteed by taking the last verification of the substring to be one of the two accepted.

$$p_{d,v}(S) = \sum_{\vec{b} \,:\, \sum_{b_{\text{len}}(\vec{b})=1} b_i = 2} p_{\vec{b}}(S). \qquad \textbf{[S19]}$$

Each of the $\binom{v}{2}$ summands on the RHS of Eq. **S19**, may be characterized by two indices k, l s.t.

$$\vec{b} = \overbrace{0\ldots0}^{k-1}1\overbrace{0\ldots0}^{l-k-1}1 \quad \text{for some } k < l \leq v. \qquad \textbf{[S20]}$$

For each one of these summands, we construct a static strategy $T_{k,l}(\rho) = \text{Tr}_{\setminus k,l}[\tilde{S}_{tl(\vec{b})}(\rho)]$ that takes as input a single valid qticket ρ and submits exactly two tokens. The counterfeiting probability of this map on ρ is

$$\begin{aligned}\text{Tr}[(P^{\rho}_{\text{acc}})^{\otimes 2} T_{k,l}(\rho)] &= \text{Tr}[(P^{\rho}_{\text{acc}})^{\otimes 2} \text{Tr}_{\setminus k,l}[\tilde{S}_{tl(\vec{b})}(\rho)]] \\ &= \text{Tr}\left[\tilde{S}_{tl(\vec{b})}(\rho) \bigotimes_{j=1}^{\text{len}(\vec{b})} (b_j P^{\rho}_{\text{acc}} + \bar{b}_j 1_Q) \otimes 1_H\right] \\ &\geq \text{Tr}\left[\tilde{S}_{tl(\vec{b})}(\rho) \bigotimes_{j=1}^{\text{len}(\vec{b})} (b_j P^{\rho}_{\text{acc}} + \bar{b}_j P^{\rho}_{\text{rej}}) \otimes 1_H\right]. \end{aligned} \qquad \textbf{[S21]}$$

By averaging over $\rho \in Q$ we obtain $p_{\vec{b}}(S) \leq p_d(T_{k,l}) \leq B$ and invoking Eq. **S19** we obtain $p_{d,v}(S) \leq \binom{v}{2} B$.

Tightness. For $F_{\text{tol}} < 5/6$ applying an optimal qubit cloning map (4) $\Lambda(\rho) = \frac{1}{3}\rho \otimes \rho + \frac{1}{6}\rho \otimes 1 + \frac{1}{6} 1 \otimes \rho$ on each of the individual qubits of the qticket provides a good counterfeiting probability. The plot in Fig. S2 illustrates the probability of counterfeiter to actually get two qtickets accepted when taking this approach. For each of the two counterfeited qtickets, the probability of failing verification is the cumulant of a binomial distribution $B(N, 5/6)$ up to $F_{\text{tol}}N$ and rejection probability may be upper bounded by $\frac{1}{2}\exp(-2N(5/6 - F_{\text{tol}})^2)$ using Hoeffding's inequality. Even when failure of the two qtickets is anticorrelated, the probability of either of them failing verification cannot exceed the sum. Hence, the scheme cannot be made secure for $F_{\text{tol}} < 5/6$. Although such a scheme provides optimal forging probability when $(F_{\text{tol}} = 1)$, other schemes could in principle outperform it in terms of counterfeiting capability. However, our security result shows that asymptotically in N, no other strategy may work for $F_{\text{tol}} > 5/6$.

Extension: Issuing multiple identical qtickets. Our results admit generalization to a scenario where the c identical copies of each qticket are issued and successful verification of $c+1$ is to be excluded. To obtain an analog of lemma 1 requires the individual qubits composing a qticket to be drawn at random from a state t-design with $t = c + (c+1)$ (for example, $t = 5$ would already be needed if two identical copies are issued). The optimal $c \to c+1$ cloning probability for N component product states is in this case bounded by $(\frac{c+1}{c+2})^N$. The threshold fidelity required to guarantee security is then given by $F_{\text{tol}} > 1 - \frac{1}{(c+1)(c+2)}$ For such an F_{tol}, the analogous result to theorem 4 one obtained is

$$p_{c\to c+1}(T) \leq e^{-ND((c+1)F_{\text{tol}} - c\|\frac{c+1}{c+2})}. \qquad \textbf{[S22]}$$

Finally, if $v > c+1$ verification attempts are allowed, the probability of counterfeiting can be proven not to grow faster than $\binom{v}{c+1}$. The proofs of these claims completely follow the lines that have been presented. Striving for legibility, we have limited the proof presented to $c = 1$, thus avoiding the notational burden imposed by the extra indices required.

CV-Qtickets. In this section we provide a proof that cv-qtickets are secure, not only against counterfeiting but also against any other possible double usage. We first present definitions for cv-qtickets and their verification. We then state the associated soundness and security guarantees and outline the security proof. Only the proof

of the security statement is provided because proving soundness for cv-qtickets requires no additional techniques as compared to soundness of qtickets.

Definition of CV-qticket. Each cv-qticket is composed of $n \times r$ qubit pairs. Each qubit pair is prepared by choosing a state from

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

uniformly at random.

A full verification question for the cv-qticket will consist of n randomly chosen axes from $\{X, Z\}$ each corresponding to a specific block of r qubit pairs. In principle, the holder of the cv-qticket then measures the polarization of every qubit component along the corresponding requested axis and communicates the measurement outcomes to the verifier. The criteria to consider an answer correct is the following; within each of the n blocks, at least $F_{\text{tol}}r$ of the reported outcomes corresponding to qubits prepared in a polarization eigenstate of the inquired axis should be given correctly.

Soundness. The soundness result states that even under imperfect storage and readout fidelity, legitimate cv-qtickets work well as long as the fidelity loss is not too severe. Again, the CPTP maps M_j will be assumed to represent the encoding, storage, and readout of the j-th qubit component of the cv-qticket, with the full map over all components given by $M = \bigotimes_{j\in\{1,\ldots,2r\times n\}} M_j$. In the case of cv-qtickets, sufficiently many $(F_{\text{tol}}r)$ correct answers should be provided within each block, demanding that a sufficiently good average fidelity be implemented for every single block. A random remapping of the Cartesian axes for each qubit component of a cv-qticket is also necessary and can be achieved via a random unitary (possibly from a unitary 2-design). This is required, for example, in the case where an actual physical polarization, say X, is lost faster than other components. In this case asking for the stored X polarization for all qubits in a block may yield a large failure probability even though the average storage fidelity among the qubits is sufficiently high. A random unitary remapping solves this problem and allows to connect with the average qubit storage fidelity, even in the case where only two nominal axes are used.

Given $F_j = F(M_j)$, the average fidelity of the qubit map M_j, we define $F_{\text{exp},b} \coloneqq N^{-1}\sum_j : \lceil \frac{j}{2r} \rceil = b F_j$ to be the average qubit fidelity within block $b \in \{1, \ldots, n\}$. Furthermore, to simplify the final expression, let us define $F_{\text{exp}} = \min_b F_{\text{exp},b}$.

Theorem 6. (Soundness of cv-qtickets) *As long as $F_{\text{exp}} > F_{\text{tol}}$, an honest holder implementing a map M can successfully redeem cv-qtickets with a probability*

$$p_{\text{h}}^{\text{cv}}(M) \geq \left(1 - e^{-rD(F_{\text{exp}}\|F_{\text{tol}})}\right)^n.$$

Observe that one may reduce this statement to n independent statements within each block that are completely analogous to the soundness for qtickets theorem 3.

Security. A naive security statement expresses that the holder of a single cv-qticket is unable to produce two copies from it, each with the potential of passing a verification. Because the verification of cv-qtickets is achieved by sending a classical message to a verifier, a stronger security statement is needed for cv-qtickets; it states that even with simultaneous access to two randomly chosen verification questions, the holder of a cv-qticket is exponentially unlikely to provide satisfactory answers to both. We further extend our security claim, to an even more adverse scenario; the holder of a cv-qticket has simultaneous access to v independent verification questions and may proceed to answer them in any chosen order. Moreover failing in verification attempts does not forbid the holder from further attempts that may possibly be performed relying on the information accumulated from previous verification outcomes.

Let S be a mathematical object denoting the counterfeiting strategy taken by the holder of a valid cv-qticket. We will denote by $p_{d,v}^{\text{cv}}(S)$, the probability that strategy S leads to two or more successful verifications when engaging in v verification attempts with possibly independent verifiers. The probability is taken over the random generation of cv-qtickets, of verification questions and of measurement outcomes (Born's rule). The security statement is then as follows.

Theorem 7. (Security of cv-qtickets) *For any counterfeiting strategy S and tolerance parameter $F_{\text{tol}} > \frac{1+1/\sqrt{2}}{2}$ we have*

$$p_{d,v}^{cv}(S) \leq \binom{v}{2}^2 \left(1/2 + e^{-rD(F_{\text{tol}}\|\frac{1+1/\sqrt{2}}{2})}\right)^n.$$

The proof of this statement goes as follows. Because abstractly cv-qtickets consist of a set of randomly produced states and questions requested on these states the formalism of quantum retrieval games (QRGs) provides adequate modelling. This framework is presented in a largely self-contained manner because its generality and potential make it of independent interest. We first provide basic definitions for QRGs and derive some simple results. Then we present possible ways of composing QRGs together with associated quantitative bounds. The first results are then applied to the qubit pair constituents of cv-qtickets to bound the holders potential to provide answers to complementary question. Cv-qtickets are then modelled by a QRG for scenarios in which the holder of a cv-qticket wishes to simultaneously answer questions from two independent verifiers without any additional aid. Finally, a combinatorial bound, similar to the one used for qtickets, is used to provide an upper limit on how the double verification probability may increase with the number v of verification attempts.

Quantum retrieval games. Quantum retrieval games (QRGs), recently defined by Gavinsky (5) provide a framework to analyze protocols in which information is to be extracted from a state produced according to a classical probability distribution. We will here present a definition of QRGs following Gavinsky as well as some additional results derived that may be of independent interest.

Alice prepares a normalized state $\rho_s = \varrho(s)/p_s$ according to the probability $p_s \coloneqq \text{Tr}[\varrho_s]$ and transfers it to Bob. Whereas Alice remembers the index s of the generated state, Bob is only provided with ρ_s and a full description of the distribution from which it was generated. Alice then asks Bob a question about s that Bob attempts to answer as best as possible. A simple possibility is for Alice to directly ask Bob the value of s. In general, however, the set of possible answers A need not coincide with the set of indexes S over the possible prepared states. If each answer a is either correct or incorrect the question may be modeled as $\sigma \in S \times A \to \{0, 1\}$. That is, $\sigma(s, a) = 1$ iff the answer a is correct for state index s and $\sigma(s, a) = 0$ otherwise. Such a definition for σ faithfully represents Gavinsky's QRGs. We extend this notion to weighted quantum retrieval games (WQRGs) to model situations where some answers are "more correct" than others. Here for each prepared state s and possible answer a the game will assign a nonnegative real value $\sigma(s, a)$ associated to the utility function of answer a given input s (i.e., $\sigma \in S \times A \to \mathbb{R}_+$).

Bob needs to choose an answer $a \in A$ and may use his copy of state ρ_s to do so. The most general strategy that Bob can take according to the laws of quantum mechanics is to perform a positive operator valued measurement (POVM). We will consider post-selected POVMs, as opposed to a physical POVM, as those that may fail to produce a measurement outcome. That is, whereas a physical POVM always produces an outcome from the expected set, for post-selected POVM some "invalid" outcomes are discarded and excluded from statistics.

In order to express the random preparation of states by Alice we first define the notion of an indexed ensemble.

Definition 5: (Indexed Ensemble) We will say that ϱ is an ensemble on $\mathcal{H}$ indexed over S iff $\forall s \in S : \varrho(s)$ is a positive operator on $\mathcal{H}$ and $\sum_{s\in S} \mathrm{Tr}[\varrho(s)] = 1$.

Note that if ϱ is an indexed ensemble, then $\rho = \sum_s \varrho(s)$ is a normalized density matrix. Although Alice gives a specific state $\varrho(s)/\mathrm{Tr}[\varrho(s)]$ to Bob, because Bob does not know s, he does not know which one has been received. The state $\rho = \mathrm{Tr}_{\mathrm{Alice}}[\sum_{s\in S} s \otimes \varrho(s)]$ will be called the reduced density matrix of ϱ because it corresponds to tracing out Alice's classically correlated subsystem containing the index s. Without loss of generality, ρ can be assumed to be full rank on $\mathcal{H}$.

In other words, a physical/selective projection $\mathcal{P}$ indexed over A is simply a physical/post-selected POVM equipped with an interpretation for each possible measurement outcome in terms of possible answers in $a \in A$.

Definition 6: (Selective and Physical Projections) We will say that $\mathcal{P}$ is a selective projection indexed over A iff $\forall a \in A$, $\mathcal{P}(a)$ are bounded positive semidefinite operators on $\mathcal{H}$. It will also be a physical projection iff $\sum_a \mathcal{P}(a) = 1$.

Note that no normalization has been imposed for selective projections because induced probability distributions are normalized a posteriori. An indexed ensemble and a projection on the same Hilbert space induce a joint probability distribution over the indexes $S \times A$ of prepared states and provided answers.

Definition 7: (Induced Probability Distribution) Let ϱ be an ensemble on $\mathcal{H}$ indexed over S and let $\mathcal{P}$ be a projection on $\mathcal{H}$ indexed over A. Then

$$p(s_0, a_0) = \frac{\mathrm{Tr}[\mathcal{P}(a_0)\varrho(s_0)]}{\sum_{s,a} \mathrm{Tr}[\mathcal{P}(a)\varrho(s)]}. \qquad \textbf{[S23]}$$

is a probability distribution over $S \times A$ that will be denoted by $p = \langle \varrho, \mathcal{P} \rangle$ and is undefined unless $\sum_{s,a} \mathrm{Tr}[\mathcal{P}(a)\varrho(s)] > 0$.

Furthermore, note that for physical projections the denominator in Eq. **S23** is 1 and the marginal of the resulting distribution over S is $p(s) = \sum_a p(s, a) = \mathrm{Tr}[\varrho(s)]$, which is independent of $\mathcal{P}$.

Definition 8: (Weighted Quantum Retrieval Games) Let ϱ be an ensemble on $\mathcal{H}$ indexed over S. Consider a utility function $\sigma \in S \times A \to \mathbb{R}_+$. Then the pair $\mathcal{G} = (\varrho, \sigma)$ is a weighted quantum retrieval game. A WQRG is also a QRG when $\sigma \in S \times A \to \{0, 1\}$.

The value of a game $\mathcal{G}$ w.r.t. a projection $\mathcal{P}$ is the average utility obtained by Bob by using a certain measurement strategy $\mathcal{P}$. This value is given by the expectancy of the utility function σ over the joint distribution of prepared states and measurement outcomes.

Definition 9: The value of game $\mathcal{G} = (\varrho, \sigma)$ w.r.t. projection $\mathcal{P}$ is defined as

$$\mathrm{Val}(\mathcal{G}, \mathcal{P}) \coloneqq \sum_{s,a} p(s, a)\sigma(s, a) \qquad \textbf{[S24]}$$

where $p = \langle \varrho, \mathcal{P} \rangle$ is the induced probability distribution.

We now define the optimum value achievable by Bob for two distinct conditions depending on whether selective or physical projections are allowed.

Definition 10: The selective (respectively physical) value of a game $\mathcal{G}$ are defined as

$$\mathrm{Sel}(\mathcal{G}) \coloneqq \sup_{\mathcal{P}\in \text{Selective projections}} \mathrm{Val}(\mathcal{G}, \mathcal{P}) \qquad \textbf{[S25]}$$

$$\mathrm{Phys}(\mathcal{G}) \coloneqq \sup_{\mathcal{P}\in \text{Physical projections}} \mathrm{Val}(\mathcal{G}, \mathcal{P}). \qquad \textbf{[S26]}$$

Note that according to this definition $\mathrm{Sel}(\mathcal{G}) \geq \mathrm{Phys}(\mathcal{G})$ because the supremum is taken over a larger set. However, for certain tailored games, the selective and physical values will coincide. The advantage of selective values is that they may be straightforwardly computed and are more amenable to compositional results. If Bob is forced to provide an answer, he can only achieve the physical value of a game. If Bob is allowed to abort the game after measuring his state ρ_s and aborted games are not considered when calculating his expected utility then he will be able to achieve the selective value.

The following result provides an explicit formula to calculate the selective value of a game. In this sense, it is a generalization of lemma 4.3 in (5).

Theorem 8. (Selective Value of a Game) *Let $\mathcal{G} = (\varrho, \sigma)$ be a WQRG with $\sum_s \varrho(s) = \rho$. Define $O(a) \coloneqq \sum_s \sigma(s, a)\rho^{-1/2}\varrho(s)\rho^{-1/2}$. Then the selective value of $\mathcal{G}$ may be calculated as $\mathrm{Sel}(\mathcal{G}) = \max_a \|O(a)\|$, where $\|\cdot\|$ denotes the operator norm.*

Proof: We first use the definition of the value of a game $\mathcal{G}$ w.r.t. $\mathcal{P}$, expand the induced probability distribution and move the sum over s inside the trace

$$\mathrm{Val}(\mathcal{G}, \mathcal{P}) = \frac{\sum_a \mathrm{Tr}[\mathcal{P}(a) \sum_s \sigma(s, a)\varrho(s)]}{\sum_a \mathrm{Tr}[\mathcal{P}(a) \sum_s \varrho(s)]}. \qquad \textbf{[S27]}$$

We define $\tilde{\mathcal{P}}$ such that $\tilde{\mathcal{P}}(a) = \rho^{1/2}\mathcal{P}(a)\rho^{1/2}$. Using this definition and that of ρ and O_a we may rewrite

$$\mathrm{Val}(\mathcal{G}, \mathcal{P}) = \frac{\sum_a \mathrm{Tr}[\tilde{\mathcal{P}}(a)O(a)]}{\sum_a \mathrm{Tr}[\tilde{\mathcal{P}}(a)]} \leq \max_a \frac{\mathrm{Tr}[\tilde{\mathcal{P}}(a)O(a)]}{\mathrm{Tr}[\tilde{\mathcal{P}}(a)]}$$
$$\leq \max_a \|O(a)\|. \qquad \textbf{[S28]}$$

The first inequality uses the positivity of all summands. For the second inequality we note that $\tilde{\mathcal{P}}(a)$ must be positive semidefinite and the variational definition of operator norm of the positive semidefinite operator $O(a)$. Equality can be achieved by taking $\tilde{\mathcal{P}}(a_0)$ to be a projector onto the highest eigenvalue subspace of $O(a_0)$ if $\|O(a_0)\| = \max_a \|O(a)\|$ and taking $\tilde{\mathcal{P}}(a_0) = 0$ otherwise.

The theorem provides an explicit construction of a projection achieving the selective value of a game. Furthermore, the proof allows us to derive a necessary and sufficient condition under which the selective and physical values of a game coincide.

Corollary 9. *Given a retrieval game $\mathcal{G}$, we have that* $\mathrm{Sel}(\mathcal{G}) = \mathrm{Phys}(\mathcal{G})$ *iff there exist positive* $\tilde{\mathcal{P}}(a)$ *such that*

$$O(a)\tilde{\mathcal{P}}(a) = \mathrm{Sel}(\mathcal{G})\tilde{\mathcal{P}}(a) \quad \text{and} \quad \sum_a \tilde{\mathcal{P}}(a) = \rho \qquad \text{[S29]}$$

We now turn to the systematic composition of retrieval games in the form of product and threshold games. Composition provides a way to construct more elaborate retrieval games together with bounds on their associated values. A natural definition of tensor product may be given for indexed ensembles, projections, and utility functions.

$$(\varrho_1 \otimes \varrho_2)(s_1, s_2) = \varrho_1(s_1) \otimes \varrho_2(s_2) \qquad \text{[S30]}$$

$$(\mathcal{P}_1 \otimes \mathcal{P}_2)(a_1, a_2) = \mathcal{P}_1(a_1) \otimes \mathcal{P}_2(a_2) \qquad \text{[S31]}$$

$$(\sigma_1 \otimes \sigma_2)((s_1, s_2), (a_1, a_2)) = \sigma_1(s_1, a_1)\sigma_2(s_2, a_2) \qquad \text{[S32]}$$

These definitions have the property that the tensor product of physical projections is a physical projection and that the induced probability distribution of two tensor product is the tensor product of the individual induced probability distributions:

$$\langle(\varrho_1 \otimes \varrho_2), (\mathcal{P}_1 \otimes \mathcal{P}_2)\rangle = \langle\varrho_1, \mathcal{P}_1\rangle \otimes \langle\varrho_2, \mathcal{P}_2\rangle.$$

Definition 11: (Tensor Product WQRG) Let $\mathcal{G}_1 = (\varrho_1, \sigma_1)$ and $\mathcal{G}_2 = (\varrho_2, \sigma_2)$. We define the tensor product WQRG $\mathcal{G}_1 \otimes \mathcal{G}_2$ as

$$\mathcal{G}_1 \otimes \mathcal{G}_2 = (\varrho_1 \otimes \varrho_2, \sigma_1 \otimes \sigma_2).$$

Proposition 10. (Tensor Product Selective Value) *The selective value of a tensor product game is the product of the selective value of the independent games.*

$$\mathrm{Sel}(\mathcal{G}_1 \otimes \mathcal{G}_2) = \mathrm{Sel}(\mathcal{G}_1)\mathrm{Sel}(\mathcal{G}_2)$$

Proof: By using the definition of $O(a)$ in theorem 8 with respect to the WQRG involved we obtain

$$\|O(a_1, a_2)\| = \|O_1(a_1) \otimes O_2(a_2)\| = \|O_1(a_1)\|\|O_2(a_2)\|.$$

Maximizing over a_1 and a_2 on both sides theorem 8 provides the desired equality.

The selective value of the product game is attained by the tensor product of projections, each achieving the respective selective values.

Corollary 11. (Tensor Product Physical Value) *If* $\mathrm{Phys}(\mathcal{G}_1) = \mathrm{Sel}(\mathcal{G}_1)$ *and* $\mathrm{Phys}(\mathcal{G}_2) = \mathrm{Sel}(\mathcal{G}_2)$ *then* $\mathrm{Phys}(\mathcal{G}_1 \otimes \mathcal{G}_2) = \mathrm{Sel}(\mathcal{G}_1 \otimes \mathcal{G}_2)$.

Given a direct product game and a projection for it one may consider the inverse procedure of defining a projection on one of the subcomponents of the game.

Definition 12: (Restriction of a Projection) Let $\mathcal{P}$ be a projection on $\mathcal{H}_1 \otimes \mathcal{H}_2$ indexed over $A_1 \times A_2$. Furthermore, let ρ_2 be a normalized density matrix on $\mathcal{H}_2$. We define the restriction $\mathcal{P}_{|1}$ with respect to ρ_2 and A_2 as

$$\mathcal{P}_{|1}(a_1) = \sum_{a_2} \mathrm{Tr}_2(\mathcal{P}(a_1, a_2)1 \otimes \rho_2).$$

By abuse of notation, if $\rho = \rho_1 \otimes \rho_2$ is a normalized product state in $\mathcal{H}_1 \otimes \mathcal{H}_2$ we may define the restriction of $\mathcal{P}$ with respect to the normalized tensor factors of ρ. This is the case for the reduced density matrix of product indexed ensembles. By restricting a projection one obtains a new projection that induces the same reduced probability distribution.

Lemma 3. (Restriction of a Projection) *Let $\mathcal{P}_{|1}$ be the restriction of $\mathcal{P}$ with respect to ρ_2 and A_2, where ρ_2 is the reduced density matrix of ϱ_2. Then*

$$\langle\varrho_1, \mathcal{P}_{|1}\rangle(s_1, a_1) = \sum_{s_2, a_2} \langle\varrho_1 \otimes \varrho_2, \mathcal{P}\rangle(s_1 s_2, a_1 a_2).$$

Theorem 12. (Selective Value of Threshold QRG) *Let $\mathcal{G}_j = (\varrho_j, \sigma_j)$ be WQRGs s.t. $\sigma_j \in (S_j, A_j) \to [0, 1]$ and $\mathrm{Sel}(\mathcal{G}_j) = \delta_j$ for all $j \in \{1, \ldots, n\}$. Furthermore take $\delta = n^{-1}\sum_{j=1}^n \delta_j$ and $\delta \le \gamma \le 1$. Define the QRG $\mathcal{G}_\gamma = (\bigotimes_j \varrho_j), \sigma_\gamma)$ with a tensor product ensemble distribution and boolean utility function*

$$\sigma_\gamma(\vec{s}, \vec{a}) = \left(\sum_{j=1}^n \sigma_j(s_j, a_j) \ge \gamma n\right).$$

Then we have $\mathrm{Sel}(\mathcal{G}_\gamma) \le 2e^{-nD(\gamma\|\delta)}$.

Proof: The direct product indexed ensemble $\varrho = \bigotimes_j \varrho_j$ and projection $\mathcal{P}$ induce a normalized probability distribution over $\vec{S} \times \vec{A}$ given by

$$p(\vec{s}, \vec{a}) = \frac{\mathrm{Tr}[\mathcal{P}(\vec{a})\varrho(\vec{s})]}{\sum_{\vec{s}\vec{a}} \mathrm{Tr}[\mathcal{P}(\vec{a})\varrho(\vec{s})]}.$$

Define the dependent random variable X_j to be $\sigma_j(s_j, a_j)$ where s_j and a_j are taken according to this probability distribution. For any $S \subseteq \{1, \ldots, n\}$, we may define $\mathcal{P}_{|S}$ as the restriction of the projection $\mathcal{P}$ to the subsystems specified by S with respect to $(\rho_{\vec{s}})$. By proposition 10 we have that

$$\mathbf{Exp}\left[\prod_{j\in S} X_j\right] = \mathrm{Val}\left(\bigotimes_{j\in S} \mathcal{G}_j, \mathcal{P}_{|S}\right) \le \prod_{j\in S} \delta_j. \qquad \text{[S33]}$$

Using theorem 1 and definition 9 we obtain

$$\mathrm{Val}(\mathcal{G}_\gamma, \mathcal{P}) = \mathbf{Pr}\left[\sum_j X_j \ge \gamma n\right] \le 2e^{-nD(\gamma\|\delta)}. \qquad \text{[S34]}$$

Because this is true for arbitrary $\mathcal{P}$ we conclude that $\mathrm{Sel}(\mathcal{G}_\gamma) \le 2e^{-nD(\gamma\|\delta)}$.

CV-qticket qubit pair building block. Consider a game in which Alice transfers to Bob one of the following states chosen at random

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

each with probability 1/8. Alice then asks Bob for the Z polarization of both qubits, possible answers being $A = \{00, 01, 10, 11\}$. An answer is correct iff it coincides in the polarization of the qubit prepared in a Z eigenstate. Bob can always answer the question correctly by measuring both qubits in the Z basis.

The quantum retrieval game formalism applies to this problem although one must admit that it is like cracking a nut with a sledgehammer. We call this game $\mathcal{G}_Z = (\varrho, \sigma_Z)$ where we have $\sum_s \varrho(s) = \rho = 1_4/4$, and $\mathrm{Tr}(\varrho(s)) = 1/8$ for all $s \in S$. A formal definition of the utility function σ_Z can be given as $\sigma_Z(s, a) = (s_1 \equiv a_1 \text{ or } s_2 \equiv a_2)$. We first define the operators $O(a)$ from theorem 8. Due to symmetry we may restrict to considering one such operator

$$O(00) = 4(\varrho(0, +) + \varrho(0, -) + \varrho(+, 0) + \varrho(-, 0)) \qquad \textbf{[S35]}$$

and find that $\|O(00)\| = 1$ that is a nondegenerate eigenvalue for all $O(a)$. The fact that the four corresponding eigenspaces are orthogonal confirms that 1 is also the physical value of the game.

The same trivial value of 1 can be achieved for the game in which Alice requests the X direction polarization of the states. We will call this game $\mathcal{G}_X = (\varrho, \sigma_X)$. The problem becomes interesting if Bob is requested provide a guess for both complementary polarizations. There are two relevant possibilities, both of which will require Bob to give an answer twice as long as before. The first scenario describes the best case probability of Bob answering both questions correctly and may be modeled by a QRG with utility function

$$\mathcal{G}_\wedge = (\varrho, \sigma_\wedge) \qquad \sigma_\wedge(s, a_X a_Z) = \sigma_X(s, a_X) \wedge \sigma_Z(s, a_Z).$$

In the second scenario we are interested in the average number of questions answered correctly when two complementary questions are posed and may be modeled by the WQRG with utility function

$$\mathcal{G}_{\mathrm{avg}} = (\varrho, \sigma_{\mathrm{avg}}) \qquad \sigma_{\mathrm{avg}}(s, a_X a_Z) = \frac{\sigma_X(s, a_X) + \sigma_Z(s, a_Z)}{2}.$$

Thanks to symmetries one need only calculate a single $\|O(a)\|$ and for concreteness we choose $O(++00)$. For the conjunction QRG we obtain

$$O(++00) = 4(\varrho(0, +) + \varrho(+, 0)) \quad \text{and} \quad \|O_{++00}\| = 3/4.$$

For the average WQRG we obtain

$$O(++00) = 2[2\varrho(0, +) + 2\varrho(+, 0) + \varrho(0, -) + \varrho(-, 0) + \varrho(+, 1) + \varrho(1, +)] \qquad \textbf{[S36]}$$

and $\|O_{++00}\| = 1/2 + 1/\sqrt{8} \approx 0.8536$, precisely the optimal fidelity for covariant qubit cloning (i.e., cloning of equatorial qubits). On the other hand, if Bob is asked the same question twice instead of complementary questions it is clear that he will be able to repeat two correct answers. All in all, if Bob is asked complementary question half of the time and coinciding questions half of the time he will be able to emulate an average fidelity of $3/4 + \sqrt{2}/8 \approx 0.927$.

Indeed, once we have defined a concrete WQRG, calculating its selective value becomes an exercise thanks to theorem 8. Furthermore, if the game has sufficient symmetry it will be possible to prove a coinciding physical values for the game.

CV-qticket. We will first bound the probability of answering two of these randomly chosen questions by bounding the selective value of the corresponding retrieval game. As an auxiliary initial step, we bound the value of a game where r complementary questions are asked on r qubit pairs (corresponding to the case in which the two random questions in a block are complementary).

$$\sigma^{(X)}_{F_{\mathrm{tol}}}(\vec{s}, \vec{a}^{(X)}) = \left(\sum_{j=1}^{r} \sigma_j^{(X)}(s_j, a_j^{(X)}) \geq F_{\mathrm{tol}} r\right)$$

$$\sigma^{(Z)}_{F_{\mathrm{tol}}}(\vec{s}, \vec{a}^{(Z)}) = \left(\sum_{j=1}^{r} \sigma_j^{(Z)}(s_j, a_j^{(Z)}) \geq F_{\mathrm{tol}} r\right)$$

$$\sigma^{\wedge}_{F_{\mathrm{tol}}}(\vec{s}, (\vec{a}^{(X)}, \vec{a}^{(Z)})) = \sigma^{(X)}_{F_{\mathrm{tol}}}(\vec{s}, \vec{a}^{(X)}) \wedge \sigma^{(Z)}_{F_{\mathrm{tol}}}(\vec{s}, \vec{a}^{(Z)}) \qquad \textbf{[S37]}$$

We will not calculate the selective value exactly but give a bound in terms of theorem 12. In order for the two block answers to be correct, among the two, at least $2F_{\mathrm{tol}}r$ answers should have been provided correctly for individual qubit pairs. Such a condition is weaker because it only imposes that the sum among the two block answers be sufficiently large, not necessarily implying that they are both above threshold.

$$\sigma^{\wedge}_{F_{\mathrm{tol}}}(\vec{s}, (\vec{a}^{(X)}, \vec{a}^{(Z)})) \leq \left(\sum_{j=1}^{r} \sigma_j^{\mathrm{avg}}(s_j, (a_j^{(X)}, a_j^{(Z)})) \geq F_{\mathrm{tol}} r\right) \qquad \textbf{[S38]}$$

The description on the right hand side has precisely the form required for theorem 12. We conclude that the selective value and hence the probability within any strategy of providing valid answers to two complementary questions for the same block is upper bounded by $2\exp[-rD(F_{\mathrm{tol}}\|1/2 + 1/\sqrt{8})]$ (for $F_{\mathrm{tol}} > 1/2 + 1/\sqrt{8}$).

Given two randomly chosen questions for a block there is a probability of 1/2 that they will coincide and a probability 1/2 that they will be complementary. Taking this into account, the probability for a dishonest holder to correctly answer two such randomly chosen block questions is upper bounded by $1/2 + \exp[-rD(F_{\mathrm{tol}}\|1/2 + 1/\sqrt{8})]$. By taking r sufficiently large, this value can be guaranteed to be smaller then 1. Hence, the probability of correctly answering n such randomly chosen threshold question pairs will be upper bounded by $B := (1/2 + \exp[-rD(F_{\mathrm{tol}}, 1/2 + 1/\sqrt{8})])^n$, which can be made exponentially close to 1 in n.

Combinatorial bound on choosing and learning. The formulation presented adequately models a scenario in which the holder of a cv-qticket does not receive any feedback from the verifiers. However, if the holder of a cv-qticket can engage in several verification protocols, new possibilities arise that should be taken into account.

Firstly, by simultaneously engaging in several (v) verification protocols with different verifiers, the holder may simultaneously have access to v challenge questions. The holder may then, for instance, choose the most similar questions and attempt to answer these. Furthermore, by successively participating in v verification protocols the holder can choose to perform verifications sequentially and wait for the outcome of the k-th before choosing which question to answer as the $k + 1$-th and providing an answer for it.

In general, if the holder engages in v verification attempts, he will receive v random questions providing no additional information on the cv-qticket. There are $\binom{v}{2}$ possible question pairs among these, each of which can be seen as randomly chosen. Thus if no feedback is used the probability of answering at least one of these pairs correctly is upper bounded by $\binom{v}{2}B$. An example scenario where this bound is relatively tight is when r is very large and n is relatively small. In this case, the probability of answering two randomly chosen questions is well approximated by the collision probability 2^{-n} (i.e., the probability that two ques-

tions coincide) that grows precisely as $\binom{v}{2}$ if the holder has access to v independently drawn questions and may choose to answer any pair.

Suppose, now, that the answers to the verifiers are provided sequentially so that the decision of which answer to produce for each verifier may be made dependent on the outcome of previous verifications. We can safely assume that the answers to challenge questions are then provided sequentially, each after receiving the acceptance or rejection of the previous ones. We can then apply a similar argument to the one exposed for the proof of theorem 5, which yields an additional factor of $\binom{v}{2}$ corresponding to the possible feedback scenarios up to the point of the second accepted answer, each of which can be simulated statically (i.e., by assuming the given feedback and fixing a corresponding POVM to generate answer up to that point). Hence, the total probability for an interactive strategy with v verification attempts of producing two or more accepted answers is upper bounded by $\binom{v}{2}^2 B$.

It may seem artificial for verifiers to select a random question each time. Randomness is important in order to avoid revealing information about the issued cv-qticket. However, the verifier may choose a random question once and for all and ask it until it is answered correctly. Once it has been answered correctly, the verifier knows that the cv-qticket has already been redeemed and can thus reject all subsequent verification attempts. Such a scheme resembles existing protocols for prepaid telephone cards. However, the quantum case provides an advantage because one may have multiple verifiers that do not communicate. In a simple example with two verifiers, two composite questions may be chosen such that they are complementary on every qubit pair (i.e., one question is chosen at random and uniquely determines the other).

Applications. Our quantum information application attempts to reduce quantum requirements to a minimum. However, even prepare and measure qubit memories remain technologically challenging. For problems admitting a classical solution, such an approach is likely to be technologically less demanding. In other words, relevant applications for prepare and measure quantum memories will be those solving problems for which no classical solutions are known. In this section we discuss some problems with classical solutions and propose refinement of such problems for which no classical solution is possible.

Enforcing single usage with a single verifier. For some applications, the no cloning of quantum information is only an apparent advantage. Our qticket and cv-qticket constructions can guarantee an exponentially small double usage probability. However, such a guarantee may be trivially enforced classically for scenarios where there is a single verifier or if the verifiers have access to realtime communication with a centralized database. In this case, a randomly chosen classical ticket has equally good properties. After a ticket is successfully redeemed once, it can be removed from the central database, making it invalid for any successive verification attempt. In fact this classical strategy is widely used for crediting prepaid phone lines with a client calling a toll free number and typing the purchased ticket number in order to credit a telephone account. Thus in such scenarios, the quantum strategy does not provide additional protection with respect to a classical solution.

Multiple noncommunicating verifiers. In scenarios with multiple noncommunicating verifiers, (cv-)qtickets provide a solution to a problem where all classical approaches fail. We describe a witness protection program as an example of how such a scenario might look.

In a witness protection program, a governmental institution decides to give asylum to a key eyewitness to whom an unforgeable quantum token is issued. This token can be used by the witness (holder) to claim asylum in any of a set of participating hotels (verifiers). The issuer also provides all hotels with the necessary information to verify the tokens. When using the token, neither the eyewitness nor the chosen hotel wish to divulge the locale where the witness is hosted, thus protecting both from being targets of an attack. In particular, communication is suspended between participating hotels as well as with the issuing authority. Any classical solution cannot prevent a sufficiently resourceful holder from making copies of the received token, thus hotels are forced to communicate in order to avoid its double use. In this case, a quantum solution based on unforgeable tokens is the sole possibility to satisfy these unique constraints. A protocol satisfying such constraints is illustrated in Fig. S3.

Reduced availability under sporadic verification. In principle, a centralized database may guarantee that classical ticket is only redeemed once. However, there are situations where the ticket should be available only to one holder at a time and the nonclonable nature of a qticket allows enforcing this. One such example is the sporadic control of tickets required for a given service. For concreteness, imagine a qticket that is valid for making use of a public transportation network. Commuters are sporadically controlled, at which point if they are found to have an invalid qticket they are charged an important fine, whereas if they are found to hold a valid qticket, they are provided with a fresh substitute. If the transportation tickets are classical, sporadic control cannot avoid counterfeited copies in the hands of colluding commuters from circulating simultaneously. The deceiving commuters need only communicate classically among each other before and after they are controlled, effectively sharing a single classical ticket to make use of the service multiple times*. In contrast the unavailability of long distance quantum communication would disallow their sharing a qticket in such a way (i.e., each valid qticket may only be at one place at a time).

The quantum credit card. Having developed a single verification, noise tolerant, nonforgeable token, such as the cv-qticket, it is now possible to examine generalizations to interesting composite protocols. For instance, Gavinsky's proposal (5) allows for multiple verification rounds to be performed on a single token, while also ensuring that the token cannot be split into two independently valid subparts. Such a construction may be seen as a quantum credit card. Indeed, the classical communication that takes place with the issuer (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. An alternate possibility is to follow the original interpretation as a quantum cash token where verification is performed by the receiver each time the "money" changes hands.

Excluding eeavesdroppers. Although qtickets do not provide additional advantage against dishonest holder in the scenario of a single verifier quantumness may provide an advantage against eavesdropping and untrusted communication. In order to make online banking more secure, Banks routinely use TANs (transaction authentication numbers) as an additional security measure. The bank sends its client a list of TANs via postal service in addition to an online password that is set up via another channel. Each time a bank transaction is requested online by the client, the bank requests a TAN from the list to guarantee the authenticity of the transaction. An impostor then needs to know both a secret password used by the user and some TANs, thus increasing the difficulty to succesfully impersonate a transaction with respect to any single security measure. However, because TANs are classical objects it is conceivable that an eavesdropper may learn them while remaining undetected (imagine an eavesdrop-

*If the classical ticket is not renewed upon control even communication is unnecesary.

per taking X-ray pictures of the correspondence). As a result, the additional security measure becomes ineffective with some effort of the eavesdropper.

This problem can be straightforwardly resolved by using quantum prepare and measure memories. Even if a cv-qticket is sent via an untrusted optical fiber or postal service, the receiver may openly communicate with the issuer and sacrifice some of the received qubits in order to obtain a bound on how much information could have leaked to eavesdropers. Quantum key distribution (QKD) takes precisely such an approach to obtain a statistical bound on the information that has leaked out. Gavinsky's @ scheme, allowing multiple verification rounds may be reinterpreted as quantum TAN lists. The holder of a quantum TAN list may verify its validity and perform a transaction by publicly communicating with the bank. If the quantum TAN list is verified to be legitimate, then the probability of an eavesdropper getting verified by using the leaked information will be negligible (exponentially small). In turn, the cv-qtickets described in the main text and appendix may be used as basic building blocks for such a scheme in the presence of noise.

1. Zhu H, Englert B, (2011) Quantum state tomography with fully symmetric measurements and product measurements. *Phys Rev A* 84:022327.
2. Panconesi A, Srinivasan A, (1997) Randomized distributed edge coloring via an extension of the Chernoff-Hoeffding bounds. *SIAM J Comput* 26:350–368.
3.
3. Impagliazzo R, Kabanets V (2010) Constructive proofs of concentration bounds. *Lecture Notes in Computer Science*, (APROX 2010)/(RANDOM 2010), eds M Serna, R Shaltiel, K Jansen and J Rolim (Springer, Berlin, Heidelberg) Vol. 6302, pp 617–631.
4. Werner RF, (1998) Optimal cloning of pure states. *Phys Rev A* 58:1827–1832.
5. Gavinsky D, (2011) Quantum money with classical verification. *Proceedings of the 2012 IEEE Conference on Computational Complexity (CCC)* (IEEE Porto, Portugal), pp 42–52.

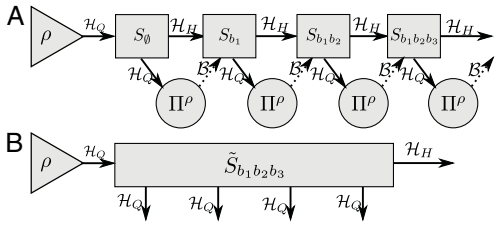

Fig. S1. (*A*) We schematically illustrate how a dynamical strategy *S* works. Each step of a strategy (gray rectangles) is a CPTP map $S_{\vec{b}}$ that depends on the classical outcome $\vec{b}$ of previous verifications. The first map $S_\varnothing$ takes an original qticket ρ as input, whereas subsequent steps rely on an internal memory state of the holder. The content of internal memory could range from no information at all to a full original qticket and a detailed register of previous submissions. The verifiers have a fixed strategy Π^ρ that consists of applying the measurement $\{P^\rho_{\text{acc}}, P^\rho_{\text{rej}}\}$ and only returning the classical boolean measurement outcome. (*B*) By fixing the classical input $\vec{b}$ to the strategy, a CPTP map $\tilde{S}_{\vec{b}} \in \mathscr{H}_Q \to \mathscr{H}_Q^{\otimes \text{len}}(\vec{b})+1 \otimes \mathscr{H}_H$ is constructed, corresponding to one possible partial application of the strategy *S*. This CPTP map produces $\text{len}(\vec{b})+1$ possibly entangled outputs in $\mathscr{H}_Q$ from a single input qticket.

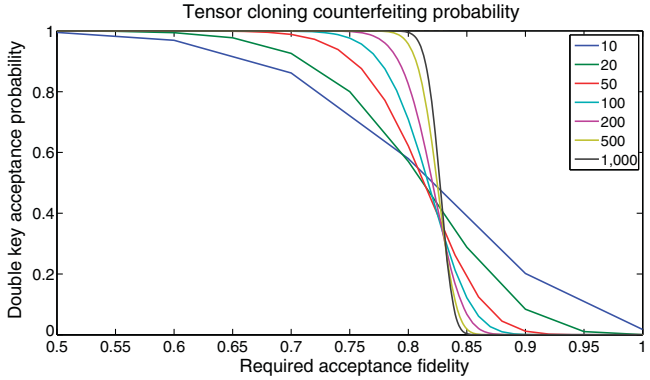

Fig. S2. We numerically calculate the probability of accepting two copies of a qticket when the adversary strategy is assumed to be independently cloning each of the *N* qubits using an optimal cloning map. We see that the probability of producing two accepted qtickets approaches a step function at 5/6 with *N*.

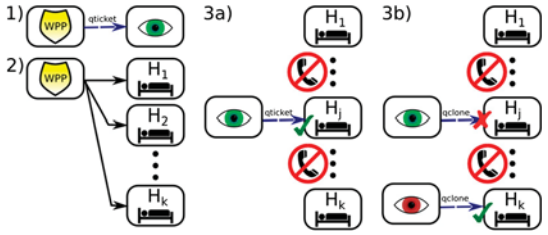

Fig. S3. 1) The issuing entity hands a qticket to the key witness. 2) It provides the hotels with the secret classical description that will be used to verify it. 3a) An honest witness chooses a hotel and physically transfers the qticket for verification. It will be accepted as long as the level of accumulated noise is below threshold. 3b) A dishonest witness will fail to counterfeit his/her qticker to provide accommodation for an additional guest. However, there is no way of avoiding a valid qticket from changing hands.