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.

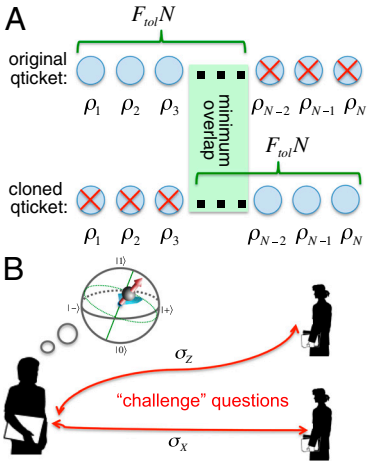

Fig. 1. (*A*) Depicts the pigeonhole type argument that is utilized in the proof of qticket soundness. For a tolerance fidelity F_{tol}, a qticket is only successfully authenticated if it contains at least $F_{\text{tol}}N$ valid qubits. However, for two counterfeit qtickets, not all valid qubits must 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:

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

where v represents the number of repeated verification attempts. We note that the factor of $\binom{v}{2}^2$ results from a combinatorial statement accounting for the possibility of choosing which challenge question to answer first and then waiting for feedback from the verifier. Thus, so long as the hierarchy of fidelities is such that $1/2 + 1/\sqrt{8} < F_{\mathrm{tol}}^{\mathrm{cv}} < F_{\mathrm{exp}}$, 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.

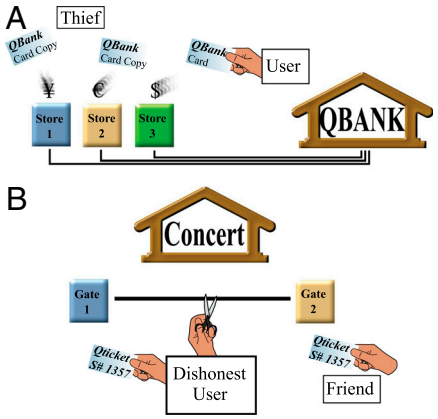

Fig. 2. (*A*) Depicts the possibility of using the cv-qticket framework to implement a quantum-protected credit card. Unlike its classical counterpart, the quantum credit card would naturally be unforgeable, preventing thieves from being able to simply copy credit card information and perform remote 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 $\tilde{Q}$, i.e., the fact that degree three polynomials in the state may equivalently be averaged over $\tilde{Q}$ 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.