# Building one-time memories from isolated qubits (full version posted at http://arxiv.org/abs/1304.5007)

Yi-Kai Liu *

April 19, 2013

**Abstract**

One-time memories (OTM's) are a simple type of tamper-resistant cryptographic hardware, which can be used to implement many forms of secure computation, such as one-time programs. Here we investigate the possibility of building OTM's using *isolated qubits* — qubits that can only be accessed using local operations and classical communication (LOCC). Isolated qubits can be implemented using current technologies, such as nitrogen vacancy centers in diamond.

We construct OTM's that are information-theoretically secure against one-pass LOCC adversaries using 2-outcome measurements. (Also, these OTM's can be prepared and accessed by honest parties using only LOCC operations.) This result is somewhat surprising, as OTM's cannot exist in a fully-quantum world or in a fully-classical world; yet they can be built from the combination of a quantum resource (single-qubit measurements) with a classical restriction (on communication between qubits).

Our construction resembles Wiesner's original idea of quantum conjugate coding, implemented using random error-correcting codes; our proof of security uses entropy chaining to bound the supremum of a suitable empirical process. In addition, we conjecture that our random codes can be replaced by some class of efficiently-decodable codes, to get computationally-efficient OTM's that are secure against computationally-bounded LOCC adversaries.

In addition, we construct data-hiding states, which allow an LOCC sender to encode an $(n-O(1))$-bit messsage into $n$ qubits, such that at most half of the message can be extracted by a one-pass LOCC receiver, but the whole message can be extracted by a general quantum receiver.

## 1 Introduction

One-time memories (OTM's) are a simple type of tamper-resistant cryptographic hardware [1]. An OTM device behaves as follows: one party (Alice) can write two messages $s, t \in \{0,1\}^k$ into the device, and then give the device to another party (Bob); after receiving the device, Bob can then choose to read either $s$ or $t$, but not both. An OTM is far simpler than a general-purpose processor, but it can be used to implement sophisticated forms of secure computation, such as one-time programs[1] [1] (and, more recently, quantum one-time programs [2]). The remarkable fact about these constructions is that the OTM is the *only* piece of hardware that has to be tamper-resistant; everything else consists of cryptographic software running on untrusted general-purpose processors.

*Applied and Computational Mathematics Division, National Institute of Standards and Technology, Gaithersburg, MD, USA. Email: yi-kai.liu@nist.gov

[1] A one-time program is a package of hardware and software that is prepared by Alice and given to Bob. It can compute a function $f$ (chosen by Alice when she prepares the package) on a single input $x$ provided by Bob (when he runs the package). During its execution, the one-time program behaves like a black box, i.e., Bob learns nothing about its internal functioning. After running once, the one-time program "self-destructs," i.e., it stops functioning, and no more information can be extracted from it.

Intuitively, it seems much easier to build an OTM, rather than a general-purpose tamper-proof processor. In particular, one may ask whether it is possible to build *provably-secure* OTM's based on some clear *physical principle*. Unfortunately, OTM's cannot exist in a fully classical world, because information can always be copied without destroying it; and OTM's cannot exist in a fully quantum world, for more subtle reasons, which are expressed in the no-go theorems for quantum oblivious transfer, bit commitment, and other kinds of two-party secure computation.

One way around these no-go theorems is to try to construct protocols that are secure against a restricted class of quantum adversaries. Here we consider a model with *isolated qubits*, where all parties (both honest and dishonest) are only allowed to perform local quantum operations (on each qubit) and classical communication (between qubits). This class of operations is known as *$n$-partite LOCC*, where $n$ is the number of qubits. This model is motivated by recent experimental work on nitrogen vacancy centers in diamond.

We will construct an OTM that consists of $n$ isolated qubits. When Alice prepares the device, she can perform $n$-partite LOCC operations on the qubits, and likewise, when Bob reads the device, he can perform $n$-partite LOCC operations on the qubits. However, there is no communication or interaction between Alice and Bob, apart from the step where Alice gives the device (containing the $n$ qubits) to Bob. [2]

Our results can be compared to those of Salvail [3], who showed a protocol for bit commitment that is secure against adversaries who can only perform $k$-local measurements, where $k = O(1)$. However, Salvail's protocol is interactive, and does not imply an OTM, which is required to be non-interactive; and the proof techniques needed for a non-interactive OTM are quite different.

We remark that there is some general intuition that relates to our "isolated qubits" model, as well as the bounded / noisy storage model [4, 5, 6, 7]. When building a quantum computer, or more precisely a quantum memory, there are two conflicting requirements: first, to protect the qubits from unwanted interactions with the environment (i.e., noise and decoherence); and second, to provide strong interactions between the qubits and some kind of external probe (in order to read and write from the memory). The bounded / noisy storage model assumes that there is no way to build a quantum memory that meets both of these requirements, and can "read in" quantum information encoded in photons (for example). Our "isolated qubits" model assumes that one can build qubits with a particular trade-off between these two requirements, namely strong protection from noise and decoherence, and only classical (not entangling) gates and measurements.

Our first main result is a construction for data hiding states (see Section 2). These states are simpler to analyze than our one-time memories, and they demonstrate the basic point that a sender can use LOCC operations to "hide" information from a LOCC receiver. We consider a system of $n$ isolated qubits, and we construct a set of $2^{\tilde{n}}$ states, where $\tilde{n} := n - \Theta(1)$, by sampling independently at random from the set $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}^{\otimes n}$. These states are all tensor products of single-qubit pure states, hence they can be prepared using only LOCC operations.

First, we show that these states can be distinguished almost perfectly using a general quantum measurement (the "pretty good measurement," see Section 2.1). Then we consider "one-pass" LOCC measurement strategies, i.e., measurement strategies that measure each qubit at most once. (For comparison, a general LOCC measurement strategy may perform many weak measurements on the same qubit. Note that bounding the power of general LOCC measurement strategies is a difficult open problem.) We show that a one-pass LOCC measurement strategy using 2-outcome measurements can extract at most $\approx n/2$ bits of information about which state was prepared (see Sections 2.2 and 2.3). Note that there exists a trivial LOCC measurement strategy that can extract $n/2$ bits of information, by measuring each qubit in the $\{|0\rangle, |1\rangle\}$ basis, for instance; hence the above bound is tight. In addition, we show that a one-pass LOCC measurement strategy using $q$-outcome measurements (for any constant $q$) can extract at most $\approx (0.7067)n$ bits of information (see Section 2.4).

The main point of this data-hiding result is to pave the way for our construction of one-time

[2] Note that this is a different scenario from most previous work on the power of LOCC operations [8], where Alice and Bob share some *bipartite* quantum system, and a "local operation" refers to an arbitrary operation on either Alice's subsystem or Bob's subsystem, and "classical communication" refers to communication between Alice and Bob.

memories, which will use a similar idea of sampling random states from the set $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}^{\otimes n}$, but will restrict access to the data in a more subtle way.

Our data-hiding states differ from previous work in some significant ways. Most previous constructions of data-hiding states [8, 9, 10, 11] are secure against a much stronger class of LOCC adversaries (with infinite LOCC rather than one-pass LOCC). On the other hand, almost all of those constructions use entangled states, which cannot be realized in our isolated qubits model. (An exception is [9], which uses separable Werner states. This approach too is quite different from ours.)

Our proof techniques are probabilistic, taking advantage of the random construction of our data-hiding states. We develop two different approaches. The first approach is "entropy chaining," aka Dudley's inequality for empirical processes. This is similar to a union bound over the set of all one-pass adaptive LOCC measurement strategies, but it takes advantage of the positive correlations between the performance of strategies that are similar. This approach gives a tight bound for adversaries that use 2-outcome measurements, but it performs poorly when applied to adversaries that use $q$-outcome measurements for large $q$. The second approach involves calculating the "collision entropy" of the unknown message, conditioned on every possible sequence of measurement outcomes. This approach does not give a tight bound, but it works fairly well for all values of $q$.

We now describe our construction for one-time memories (see Section 3). We consider a system of $n$ isolated qubits, and we pick two random error-correcting codes, $C : \{0,1\}^k \to \{0,1\}^n$ and $D : \{0,1\}^k \to \{0,1\}^n$. (That is, each codeword is chosen independently and uniformly at random in $\{0,1\}^n$.) Given two messages $s$ and $t$ in $\{0,1\}^k$, we prepare each qubit $i$ (for $i = 1, 2, \ldots, n$) as follows. Let $C(s)_i$ and $D(t)_i$ denote the $i$'th bit in the strings $C(s)$ and $D(t)$, respectively. We prepare the $i$'th qubit in a pure state that has the following properties: first, if the qubit is measured in the $\{|0\rangle, |1\rangle\}$ basis, the outcome is more likely to be $|0\rangle$ if $C(s)_i = 0$, and $|1\rangle$ if $C(s)_i = 1$; and second, if the qubit is measured in the $\{|+\rangle, |-\rangle\}$ basis, the outcome is more likely to be $|+\rangle$ if $D(t)_i = 0$, and $|-\rangle$ if $D(t)_i = 1$. This is similar to Wiesner's idea of quantum conjugate coding [12]. We refer to these states as one-time memory (OTM) states.

It is straightforward to check that these OTM states can be prepared using only LOCC operations, and that an honest party can recover either $s$ or $t$ using only LOCC operations (see Section 3.1). We prove that no one-pass LOCC adversary using 2-outcome measurements can learn both $s$ and $t$ simultaneously; in particular, no such adversary can extract more than $\approx (1.9189)k < 2k$ bits of information about $(s, t)$ (see Section 3.2). This bound is surely not optimal, but at least it demonstrates that our OTM construction "leaks" at most a constant fraction (bounded below 1) of the bits of $s$ and $t$.

We remark that our OTM states do in fact leak some information. For instance, there is a one-pass LOCC strategy that can extract $n/2 \approx (1.2528)k$ bits of information about $s$ and $t$. Moreover, an adversary can always obtain partial information about both $s$ and $t$. We conjecture that such "leaky" OTM's are still sufficient for applications such as one-time programs, thanks to techniques such as leak-resistant encryption [13].

The proof that these OTM states are secure uses similar techniques to our first result on data-hiding states, but there are some additional challenges, as the OTM states are correlated, rather than being chosen independently. To address this issue, our proof uses large-deviation bounds for locally dependent random variables, and applies both of our previous techniques (bounding the "collision entropy," and "entropy chaining") in sequence.

We think it is an interesting challenge to develop our OTM construction into a useful primitive for secure computation. In this paper we have taken a first step, by constructing OTM's based on isolated qubits, and analyzing their security in a simple information-theoretic framework (e.g., using random codes in the OTM's, and describing the adversary's knowledge in terms of mutual information). The next step is to make our OTM's efficient, and prove a stronger security guarantee that allows composition of OTM's to implement more sophisticated functions. Finally, it is an open problem to better understand the power of general LOCC strategies (going beyond the one-pass LOCC strategies considered here).

# References


[1] S. Goldwasser, Y.T. Kalai and G.N. Rothblum, "One-Time Programs," *CRYPTO 2008*, pp.39-56.

[2] A. Broadbent, G. Gutoski and D. Stebila, "Quantum one-time programs," arXiv:1211.1080.

[3] L. Salvail, "Quantum Bit Commitment from a Physical Assumption," *CRYPTO 1998*, pp.338-353.

[4] I. Damgaard, S. Fehr, L. Salvail and C. Schaffner, "Cryptography In the Bounded Quantum-Storage Model," *FOCS 2005*, pp.449-458.

[5] R. Koenig and B.M. Terhal, "The Bounded Storage Model in the Presence of a Quantum Adversary," *IEEE Trans. Inf. Th.*, vol. 54, no. 2 (2008).

[6] I. Damgaard, S. Fehr, L. Salvail and C. Schaffner, "Secure Identification and QKD in the Bounded-Quantum-Storage Model," *CRYPTO 2007*, pp.342-359.

[7] S. Wehner, C. Schaffner and B. Terhal, "Cryptography from Noisy Storage," *Phys. Rev. Lett.* 100, 220502 (2008).

[8] D.P. DiVincenzo, D.W. Leung and B.M. Terhal, "Quantum Data Hiding," *IEEE Trans. Inf. Theory*, Vol. 48, No. 3, pp.580-599 (2002).

[9] T. Eggeling and R. F. Werner, "Hiding Classical Data in Multipartite Quantum States," *Phys. Rev. Lett.* 89, 097905 (2002).

[10] D.P. DiVincenzo, P. Hayden and B.M. Terhal, "Hiding Quantum Data," *Found. Phys.* 33(11), pp.1629-1647, 2003.

[11] P. Hayden, D. Leung and G. Smith, "Multiparty data hiding of quantum information," *Phys. Rev. A* 71, 062339 (2005).

[12] S. Wiesner, "Conjugate coding," *ACM SIGACT News*, Volume 15, Issue 1, 1983, pp.78-88.

[13] A. Akavia, S. Goldwasser and V. Vaikuntanathan, "Simultaneous Hardcore Bits and Cryptography against Memory Attacks," *TCC 2009*, pp.474-495.