Revocable Quantum Timed-Release Encryption

Dominique Unruh

University of Tartu, Estonia

Abstract. Timed-release encryption is a kind of encryption scheme that a recipient can decrypt only after a specified amount of time T (assuming that we have a moderately precise estimate of his computing power). A *revocable* timed-release encryption is one where, before the time T is over, the sender can "give back" the timed-release encryption, provably loosing all access to the data. We show that revocable timed-release encryption without trusted parties is possible using quantum cryptography (while trivially impossible classically).

Along the way, we develop two proof techniques in the quantum random oracle model that we believe may have applications also for other protocols.

Finally, we also develop another new primitive, *unknown recipient encryption*, which allows us to send a message to an unknown/unspecified recipient over an insecure network in such a way that at most one recipient will get the message.

1 Introduction

We present and construct revocable timed-release encryption schemes (based on quantum cryptography). To explain what revocable timed-release encryption is, we first recall the notion of timed-release encryption (also known as a time-lock puzzle); we only consider the setting without trusted parties in this paper. A timed-release encryption (TRE) for time T is an algorithm that takes a message m and "encrypts" it in such a way that the message cannot be decrypted in time T but can be decrypted in time $T' > T$. (Here T' should be as close as possible to T, preferably off by only an additive offset.)

The crucial point here is that the recipient can open the encryption without any interaction with the sender. (E.g., [21] publishes a secret message that is supposed not to be openable before 2034.) Example use cases could be: messages for posterity [22]; data that should be provided to a recipient at a given time, even if the sender goes offline; A sells some information to B that should be revealed only later, but B wants to be sure that A cannot withdraw this information any more;[1] exchange of secrets where none of the parties should be able to abort depending on the data received by the other; fair contract signing [6]; electronic auctions [6]; mortgage payments [22]; concurrent zero-knowledge protocols [6]; etc.

Physically, one can imagine TRE as follows: The message m is put in a strongbox with a timer that opens automatically after time T'. The recipient cannot get the message in time T because the strongbox will not be open by then.

[1] In this case, zero-knowledge proofs could be used to show that the TRE indeed contains the right plaintext.

P.Q. Nguyen and E. Oswald (Eds.): EUROCRYPT 2014, LNCS 8441, pp. 129–146, 2014.

It turns out, however, that a physical TRE is more powerful than a digital one. Consider the following example setting: Person P goes to a meeting with a criminal organization. As a safe guard, he leaves compromising information m with his friend F, to be released if P does not resurface after one day. (WikiLeaks/Assange seems to have done something similar [19].) As P assumes F to be curious, P puts m in a physical TRE, to be opened only after one day. If P returns before the day is over, P asks the TRE back. If F hands the TRE over to P, P will be sure that F did not and will not read m. (Of course, F may refuse to hand back the TRE, but F cannot get m without P noticing.)

This works fine with physical TRE, but as soon as P uses a digital TRE, F can cheat. F just copies the TRE before handing it back and continues decrypting. After one day, F will have m, without P noticing.

So physical TREs are "revocable". The recipient can give back the encryption before the time T has passed. And the sender can check that this revocation was performed honestly. In the latter case, the sender will be sure that the recipient does not learn anything. Obviously, a digital TRE can never have that property, because it can be copied before revocation.

However, if we use quantum information in our TRE, things are different. Quantum information cannot, in general, be copied. So it is conceivable that a quantum TRE is revocable.

1.1 Example Applications

We sketch a few more possible applications of revocable TREs. Some of them are far beyond the reach of current technology (because they need reliable storage of quantum states for a long time). In some cases, however, TREs with very short time T are used, this might be within the reach of current technology. The applications are not worked out in detail (some are just first ideas), and we do not claim that they are necessarily the best options in their respective setting, but they illustrate that revocable TREs could be a versatile tool worth investigating further.

Deposits. A client has to provide a deposit for some service (e.g., car rental). The dealer should be able to cash in the deposit if the client does not return. Solution: The client produces a T-revocable TRE containing a signed transaction that empowers the dealer to withdraw the deposit. When the client returns the car within time T, the client can make sure the dealer did not keep the deposit.[2]

[2] One challenge: The client needs to convince the dealer that the TRE indeed contains a signature on a transaction. I.e., we need a way to prove that a TRE V contains a given value (and the running time of this proof should not depend on T). At least for our constructions (see below), this could be achieved as follows: The client produces a commitment c on the content of the classical inner TRE V_0 and proves that c contains the right content (using a SNARK [4] so that the verification time does not depend on T). Then client and dealer perform a quantum two-party computation [12] with inputs c, V, and opening information for c, and with dealer outputs V and b where b is a bit indicating whether the message in V satisfies P.

Such deposits might also be part of a cryptographic protocol where deposits are revoked or redeemed automatically depending on whether a party is caught cheating (to produce an incentive against cheating). In this case, the time T might well be in the range of seconds or minutes, which could be within the reach of near future quantum memory [15].

Data Retention with Verifiable Deletion. Various countries have laws requiring the retention of telecommunication data, but mandate the deletion of the data after a certain period (e.g., [14]). Using revocable TREs, clients could provide their data within revocable TREs (together with a proof of correctness, cf. footnote 2). At the end of the prescribed period, the TRE is revoked, unless it is needed for law-enforcement. This way, the clients can verify that their data is indeed erased from the storage.

Unknown Recipient Encryption. An extension of revocable TREs is "unknown recipient encryption" (URE) which allows a sender to encrypt a message m in such a way that any recipient but at most one recipient can decrypt it. That is, the sender can send a message to an unknown recipient, and that recipient can, after decrypting, be sure that only he got the message, even if the ciphertext was transferred over an insecure channel. Think, e.g., of a client connecting to a server in an anonymous fashion, e.g., through (a quantum variant of) TOR [11], and receiving some data m. Since the connection is anonymous and the client has thus no credentials to authenticate with the server, we cannot avoid that the data gets "stolen" by someone else. However, with unknown recipient encryption, it is possible to make sure that the client will detect if someone else got his data. This application shows that revocable TREs can be the basis for other unexpected cryptographic primitives. Again, the time T may be small in some applications, thus in the reach of the near future. We stress that URE is non-interactive, so this works even if no bidirectional communication is possible. It could be used for a cryptographic dead letter box where a "spy" deposits secret information, and the recipient can verify that no-one found it. Unknown recipient encryption is formalized in the full version [27].

A variant of this is "one-shot" quantum key distribution: Only a single message is sent from Alice to Bob, and as long as Bob receives that message within time T, he can be sure no-one else got the key. (This is easily implemented by encrypting the key with a URE.)

1.2 Our Contribution

Definitions. We give formal definitions of TREs and revocable TREs (Section 2). These definitions come in two flavors: T-hiding (no information is leaked before time T) and T-one-way (before time T, the plaintext cannot be guessed completely).)

One-Way Revocable TREs. Then we construct one-way revocable TREs (Section 3). Although one-wayness is too weak a property for almost all purposes, the construction and its proof are useful as a warm-up for the hiding

construction, and also useful on their own for the random oracle based constructions (see below). The construction itself is very simple: To encrypt a message m, a quantum state $|\Psi\rangle$ is constructed that encodes m in a random BB84 basis B.[3] Then B is encrypted in a (non-revocable) T-hiding TRE V_0. The resulting TRE $(|\Psi\rangle, V_0)$ is sent to the recipient. Revocation is straightforward: the recipient sends $|\Psi\rangle$ back to the sender, who checks that $|\Psi\rangle$ still encodes m in basis B. Intuitively, $|\Psi\rangle$ cannot be reliably copied without knowledge of basis B, hence before time T the recipient cannot copy $|\Psi\rangle$ and thus looses access to $|\Psi\rangle$ and thus to m upon revocation.

The proof of this fact is not as easy as one might think at the first glance ("use the fact that B is unknown before time T, and then use that a state $|\Psi\rangle$ cannot be cloned without knowledge of the basis") because information-theoretical and complexity-theoretic reasoning need to be mixed carefully.

The resulting scheme even enjoys everlasting security (cf., e.g., [17,10,1,7,20]): after successful revocation, the adversary cannot break the TRE even given unlimited computation.

We hope that the ideas in the proof benefit not only the construction of revocable TREs, but might also be useful in other contexts where it is necessary to prove uncloneability of quantum-data based on cryptographic and not information-theoretical secrecy (quantum-money perhaps?).

Revocably Hiding TREs. The next step is to construct revocably *hiding* TREs (Section 4). The construction described before is not hiding, because if the adversary guesses a few bits of B correctly, he will learn some bits of m while still passing revocation. A natural idea would be to use privacy amplification: the sender picks a universal hash function F and includes it in the TRE V_0. The actual plaintext is XORed with $F(m)$ and transmitted. Surprisingly, we cannot prove this construction secure, see the beginning of Section 4 for a discussion. Instead, we prove a construction that is based on CSS codes. The resulting scheme uses the same technological assumptions as the one-way revocable one: sending and measuring of individual qubits, quantum memory. Unfortunately, the reduction in this case is not very efficient; as a consequence the underlying non-revocable TRE needs to be exponentially hard, at least if we want to encrypt messages of superlogarithmic length. Notice that the random oracle based solutions described below do not have this drawback.

Like the previous scheme, this scheme enjoys everlasting security.

Random Oracle Transformations. We develop two transformations of TREs in the quantum random oracle model. The first transformation takes a revocably one-way TRE and transforms it into a revocably hiding one (by sending $m \oplus H(k)$ and putting k into the revocably one-way TRE; Section 5.1). This gives a simpler and more efficient alternative to the complex construction for revocably hiding TREs described above, though at the cost of using the random-oracle model and loosing everlasting security. The second transformation allows us to assume

[3] I.e., each bit of m is randomly encoded either in the computational or the diagonal basis.

without loss of generality that the adversary performs no oracle queries before receiving the TRE, simplifying other security proof (Section 5.2).

For both transformations we prove general lemmas that allow us to use analogous transformations also on schemes unrelated to TREs (e.g., to make an encryption scheme semantically secure). We believe these to be of independent interest, because the quantum random oracle model is notoriously difficult to use, and many existing classical constructions are not known to work in the quantum case.

Classical TREs. Unfortunately, only very few constructions of classical TRE are known. Rivest, Shamir, and Wagner [22] present a construction based on RSA; it is obviously not secure in the quantum setting [23]. Other constructions are iterated hashing (to send m, we send $H(H(H(\dots(r)\dots)))\oplus m$) and preimage search (to decrypt, one needs to invert $H(k)$ where $k\in\{1,\dots,T\}$); with suitable amplification this becomes a TRE [26]). Preimage search is not a good TRE because it breaks down if the adversary can compute in parallel. This leaves iterated hashing.[4] We prove that (a slight variation of) iterated hashing is hiding even against quantum adversaries and thus suitable for plugging into our constructions of revocable TREs (Section 5.3). (Note, however, that the hardness of iterated hashing could also be used as a very reasonable assumption on its own. The random oracle model is thus not strictly necessary here, it just provides additional justification for that assumption.)

We leave it as an open problem to identify more practical candidates for iterated hashing, perhaps following the ideas of [22] but not based on RSA or other quantum-easy problems.

For space reasons, details and full proofs are deferred to the full version [27] of this paper.

1.3 Preliminaries

For the necessary background in quantum computing, see, e.g., [18].

Let $\omega(x)$ denote the Hamming weight of x. By $\binom{[q+n]}{q}$ we denote the set of all size-q subsets of $\{1,\dots,q+n\}$. I.e., $S\in\binom{[q+n]}{q}$ iff $S\subseteq\{1,\dots,q+n\}$ and $|S|=q$. By $\oplus$ we mean bitwise XOR (or equivalently, addition in $\mathrm{GF}(2)^n$). Given a linear code C, let $C^\perp$ be the dual code ($C^\perp := \{x : \forall y\in C.\ x,y \text{ orthogonal}\}$).

Let X,Y,Z denote the Pauli operators. Let $|\beta_{ij}\rangle$ denote the four Bell states, namely $|\beta_{00}\rangle := \frac{1}{\sqrt{2}}|00\rangle+\frac{1}{\sqrt{2}}|11\rangle$ and $|\beta_{fe}\rangle = (Z^fX^e\otimes I)|\beta_{00}\rangle = (I\otimes X^eZ^f)|\beta_{00}\rangle$. In slight abuse of notation, we call $|\beta_{00}\rangle$ an *EPR pair* (originally, [13] used

[4] Iterated hashing has the downside that producing the TRE takes as long as decrypting it. However, this long computation can be moved into a precomputation phase that is independent of the message m, making this TRE suitable at least for some applications. [16] present a sophisticated variant of iterated hashing that circumvents this problem; their construction, however, does not allow the sender to predict the recipient's output and is thus not suitable for sending a message into the future.

$|\beta_{11}\rangle$). And a state consisting of EPR pairs we call an *EPR state*. H denotes the Hadamard gate, and I_n the identity on $\mathbb{C}^{2^n}$ (short I if n is clear from the context). Let $|m\rangle_B$ denote $m \in \{0,1\}^n$ encoded in basis $B \in \{0,1\}^n$, where 0 stands for the computational and 1 for the diagonal basis.

Given an operator A and a bitstring $x \in \{0,1\}^n$, we write A^x for $A^{x_1} \otimes \cdots \otimes A^{x_n}$. E.g., $X^x|y\rangle = |x \oplus y\rangle$, and $H^B|x\rangle = |x\rangle_B$.

Given $f, e \in \{0,1\}^n$, we write $|\widetilde{fe}\rangle$ for $|\beta_{f_1 e_1}\rangle \otimes \cdots \otimes |\beta_{f_n e_n}\rangle$, except for the order of qubits: the first qubits of all EPR pairs, followed by the last qubits of all EPR pairs. In other words, $|\widetilde{0^n 0^n}\rangle = \sum_{x\in\{0,1\}^n} |w\rangle|w\rangle$ and $|\widetilde{fe}\rangle = (Z^f X^e \otimes I)|\widetilde{0^n 0^n}\rangle$.

Let $\|\cdot\|$ be the Euclidean norm (i.e., $\||\Psi\rangle\|^2 = |\langle\Psi|\Psi\rangle|$) and let $|||\cdot|||$ denote the corresponding operator norm (i.e., $|||A||| := \sup_{x\neq 0}\|Ax\|/\|x\|$).

By $\mathrm{TD}(\rho_1, \rho_2)$ we denote the trace distance between density operators ρ_1, ρ_2. We write short $\mathrm{TD}(|\Psi_1\rangle, |\Psi_2\rangle)$ for $\mathrm{TD}(|\Psi_1\rangle\langle\Psi_1|, |\Psi_2\rangle\langle\Psi_2|)$.

Whenever we speak about algorithms, we mean quantum algorithms. (In particular, adversaries are always assumed to be quantum.)

2 Defining Revocable TREs

A timed-release encryption (TRE) consists of: An encryption algorithm $\mathrm{TRE}(m)$ that returns a (possibly quantum) ciphertext V containing m. A decryption algorithm that computes m from V (without using any key). Possibly: a revocation algorithm in which the recipient gives back V to the sender and the sender performs some check on V. We have two basic security properties for TREs: T-hiding means that within time T, an adversary cannot learn anything about m, and T-one-way means that within time T, an adversary cannot guess m. (These basic security properties do not refer to the revocation algorithm.) For formal definitions of these basic properties, and a discussion on timing-models and definitions in related work, see the full version [27].

We now define the *revocable* hiding property. A TRE is revocably T-hiding if an adversary cannot both successfully pass the revocation protocol within time T and learn something about the message m contained in the TRE. When formalizing this, we have to be careful. A definition like: "conditioned on revocation succeeding, $p_0 :=$ Pr[adversary outputs 1 given $\mathrm{TRE}(m_0)$] and $p_1 :=$ Pr[adversary outputs 1 given $\mathrm{TRE}(m_1)$] are close ($|p_0 - p_1|$ is negligible)" does not work: if Pr[revocation succeeds] is very small, $|p_0 - p_1|$ can become large even if the adversary rarely succeeds in distinguishing. (Consider, e.g., an adversary that intentionally fails revocation except in the very rare case that he guesses an encryption key that allows to decrypt the TRE immediately.) Also, a definition like "$|p_0 - p_1| \cdot$ Pr[revocation succeeds]" is problematic: Does Pr[revocation succeeds] refer to an execution with $\mathrm{TRE}(m_0)$ or $\mathrm{TRE}(m_1)$?. Instead, we will require "$|p_0 - p_1|$ is negligible with $p_i :=$ Pr[adversary outputs 1 and revocation succeeds given $\mathrm{TRE}(m_i)$]". This definition avoids the complications of a conditional probability and additionally implies as side effect that also Pr[revocation succeeds given $\mathrm{TRE}(m_0)$] and Pr[revocation succeeds given $\mathrm{TRE}(m_1)$] are close.

Definition 1 (Revocably hiding timed-release encryption). *Given a revocable timed-release encryption* TRE *with message space M, and an adversary (A_0, A_1, A_2) (that is assumed to be able to keep state between activations of A_0, A_1, A_2) consider the following game $G(b)$ for $b \in \{0,1\}$:*

- $(m_0, m_1) \leftarrow A_0()$.
- $V \leftarrow \mathrm{TRE}(m_b)$.
- *Run the revocation protocol of* TRE*, where the sender is honest, and the recipient is $A_1(V)$. Let ok be the output of the sender (i.e., $ok = 1$ if the sender accepts).*
- $b' \leftarrow A_2()$.

A timed-release encryption TRE *with message space M is T-*revocably hiding*, if for any adversary (A_0, A_1, A_2) where A_1 is sequential-polynomial-time and T-time and A_0, A_2 are sequential-polynomial-time, $\left|\Pr[b' = 1 \wedge ok = 1 : G(0)] - \Pr[b' = 1 \wedge ok = 1 : G(1)]\right|$ is negligible.*

Note that although revocably hiding seems to be a stronger property than hiding, we are not aware of any proof that a T-revocably hiding TRE is also T-hiding. (It might be that it is possible to extract the message m in time $\ll T$, but only at the cost of making a later revocation impossible. This would contradict T-hiding but not T-revocably hiding.) Therefore we always need to show that our revocable TREs are both T-hiding and T-revocably hiding.

Again, we define the weaker property of revocable one-wayness which only requires the adversary to guess the message m. We need this weaker property for intermediate constructions. Like for hiding, we stress that revocable one-wayness does not seem to imply one-wayness.

Definition 2 (Revocably one-way TRE). *Given a revocable timed-release encryption* TRE *with message space M, and an adversary (A_0, A_1, A_2) (that is assumed to be able to keep state between activations of A_0, A_1, A_2) consider the following game G:*

- *Run $A_0()$.*
- *Pick $m \xleftarrow{\$} M$, run $V \leftarrow \mathrm{TRE}(m)$.*
- *Run the revocation protocol of* TRE*, where the sender is honest, and the recipient is $A_1(V)$. Let ok be the output of the sender (i.e., $ok = 1$ if the sender accepts).*
- $m' \leftarrow A_2()$.

A timed-release encryption TRE *with message space M is T-*revocably one-way*, if for any quantum adversary (A_0, A_1, A_2) where A_1 is sequential-polynomial-time and T-time and A_0, A_2 are sequential-polynomial-time, we have that $\Pr[m = m' \wedge ok = 1 : G]$ is negligible.*

3 Constructing Revocably One-Way TREs

In this section, we present our construction RTRE_{ow} for revocably one-way TREs. Although one-wayness is too weak a property, this serves as a warm-up

for our considerably more involved revocably hiding TREs (Section 4), and also as a building block in our random-oracle based construction (Section 5.1).

The following protocol is like we sketched in the introduction, except that we added a one-time pad p. That one-time pad has no effect on the revocable one-wayness, but we introduce because it makes the protocol (non-revocably) hiding at little extra cost.

Definition 3 (Revocably one-way TRE RTRE_{ow})
- *Let n be an integer.*
- *Let TRE_0 be a T-hiding TRE with message space $\{0,1\}^{2n}$.*

We construct a revocable TRE RTRE_{ow} with message space $\{0,1\}^n$.

***Encryption** of $m \in \{0,1\}^n$:*
- *Pick $p, B \xleftarrow{\$} \{0,1\}^n$.*
- *Construct the state $|\Psi\rangle := |m \oplus p\rangle_B$. (Recall that $|x\rangle_B$ is x encoded in basis B, see page 134.)*
- *Compute $V_0 \leftarrow \mathrm{TRE}_0(B, p)$.*
- *Send V_0 and $|\Psi\rangle$.*

Decryption:
- *Decrypt V_0.*
- *Measure $|\Psi\rangle$ in basis B; call the outcome γ.*
- *Return $m := \gamma \oplus p$.*

Revocation:
- *The recipient sends $|\Psi\rangle$ back to the sender.*
- *The sender measures $|\Psi\rangle$ in basis B; call the outcome γ.*
- *If $\gamma = m \oplus p$, revocation succeeds (sender outputs 1).*

Naive Proof Approach. (In the following discussions, for clarity we omit all occurrences of the one-time pad p.) At a first glance, it seems the security of this protocol should be straightforward to prove: We know that without knowledge of the basis B, one cannot clone the state $|\Psi\rangle$, not even approximately.[5] We also know that until time T, the adversary does not know anything about B (since TRE_0 is T-hiding). Hence the adversary cannot reliably clone $|\Psi\rangle$ before time T. But the adversary would need to do so to pass revocation and still keep a state that allows him to measure m later (when he learns B).

Unfortunately, this argument is not sound. It would be correct if TRE_0 were implemented using a trusted third party (i.e., if B is sent to the adversary after time T).[6] However, the adversary has access to $V_0 = \mathrm{TRE}_0(B)$ when trying to clone $|\Psi\rangle$. From the information-theoretical point of view, this is the same as having access to B. Thus the no-cloning theorem and its variants cannot be applied because they rely on the fact that B is *information-theoretically* hidden.

[5] This fact also underlies the security of BB84-style QKD protocols [3].

[6] Again, this is implicit in proofs for BB84-style QKD protocols: there the adversary gets a state $|\Psi\rangle = |m\rangle_B$ from Alice (key m encoded in a secret base B), which he has to give back to Bob unchanged (because otherwise Alice and Bob will detect tampering). And he wishes to, at the same time, keep information to later be able to compute the key m when given B.

One might want to save the argument in the following way: Although $V_0 = \mathrm{TRE}_0(B)$ information-theoretically contains B, it is indistinguishable from $\hat{V}_0 = \mathrm{TRE}_0(\hat{B})$ which does not contain B but an independently chosen $\hat{B}$. And if the adversary is given $\hat{V}_0$ instead of V_0, we can use information-theoretical arguments to show that he cannot learn m. But although this argument would work if TRE_0 were hiding against polynomial-time adversaries (e.g., if TRE_0 were a commitment scheme). But TRE_0 is only hiding for T-time adversaries! This only guarantees that all observable events that happen with V_0 *before time* T also happen with $\hat{V}_0$ *before time* T and vice versa. In particular, since with $\hat{V}_0$, the adversary cannot learn m before time T, he cannot learn m before time T with V_0. But although with $\hat{V}_0$, after successful revocation, the adversary provably cannot ever learn m, it might be possible that with V_0, he can learn m right after time T has passed.

Indeed, it is not obvious how to exclude that there is some "encrypted-cloning" procedure that, given $|\Psi\rangle = |m\rangle_B$ and $\mathrm{TRE}_0(B)$, without disturbing $|\Psi\rangle$, produces a state $|\Psi'\rangle$ that for a T-time distinguisher looks like a random state, but still $|\Psi'\rangle$ can be transformed into $|\Psi\rangle$ in time $\gg T$. Such an "encrypted-cloning" would be sufficient for breaking RTRE_{ow}. (Of course, it is a direct corollary from our security proof that such encrypted-cloning is impossible.)[7]

Proof Idea. As we have seen in the preceding discussion, we can prove that the property "the adversary cannot learn m ever" holds when sending $\hat{V}_0 = \mathrm{TRE}_0(\hat{B})$ for an independent $\hat{B}$ instead of $V_0 = \mathrm{TRE}_0(B)$. But we cannot prove that this property carries over to the V_0-setting because it cannot be tested in time T. Examples for properties that do carry over would be "the adversary cannot learn m in time T" or "revocation succeeds" or "when measured in basis B, the adversary's revocation-message does not yield outcome m". But we would like to have a property like "the entropy of m is large (or revocation fails)". That property cannot be tested in time T, so it does not carry over. Yet, we can use a trick to still guarantee that this property holds in the V_0-setting.

For this, we first modify the protocol in an (information-theoretically) indistinguishable way: Normally, we would pick m at random and send $|\Psi\rangle := |m\rangle_B$

[7] To illustrate that "encrypted-cloning" is not a far fetched idea, consider the following quite similar revocable TRE: Let $E_K(|\Psi\rangle)$ denote the quantum one-time pad encryption of $|\Psi\rangle \in \mathbb{C}^{2^n}$ using key $K \in \{0,1\}^{2n}$, i.e., $E_K(|\Psi\rangle) = Z^{K_1}X^{K_2}|\Psi\rangle$ with $K = K_1 \| K_2$ [2]. $\mathrm{RTRE}(m) := (E_K(|m\rangle_B), B, \mathrm{TRE}_0(K))$. For revocation, the sender sends $E_K(|m\rangle_B)$ back, and the recipient checks if it is the right state. Again, if K is unknown, it is not possible to clone $E_K(|m\rangle_B)$ as it is effectively a random state even given B. But we can break RTRE as follows:

The recipient measures $|\Phi\rangle := E_K(|m\rangle_B)$ in basis B. Using $XH = HZ$ and $ZH = HX$, we have $|\Phi\rangle = Z^{K_1}X^{K_2}H^B|m\rangle = H^B X^{K_1 * B} Z^{K_1 * \bar{B}} Z^{K_2 * B} X^{K_2 * \bar{B}}|m\rangle = \pm|m \oplus (K_2 * \bar{B}) \oplus (K_1 * B)\rangle_B$ where $*$ is the bit-wise product and $\bar{B}$ the complement of B. Thus the measurement of $|\Phi\rangle$ in basis B does not disturb $|\Phi\rangle$, and the recipient learns $m \oplus (K_1 * B) \oplus (K_2 * \bar{B})$. He can then send back the undisturbed state $|\Phi\rangle$ and pass revocation. After decrypting $\mathrm{TRE}_0(K)$, he can compute m, and reconstruct the state $|\Phi\rangle = E_K(|m\rangle_B)$ using known K, m, B. Thus he performed an "encrypted cloning" of $|\Phi\rangle$ *before* decrypting $\mathrm{TRE}_0(K)$.

to the adversary. Instead, we initialize two n-bit quantum registers X, Y with EPR pairs and send X to the adversary. The value m is computed by measuring Y in basis B. Now we can formulate a new property: "after revocation but before measuring m, XY are still EPR pairs (up to some errors) or revocation fails". This property can be shown to hold in the $\hat{V}_0$-setting using standard information-theoretical tools. And the property tested in time T, all we have to do is a measurement in the Bell basis. Thus the property also holds in the V_0-setting. And finally, due to the monogamy of entanglement ([9]; but we need a custom variant of it) we have that this property implies "the entropy of m is high (or revocation fails)".

We have still to be careful in the details, of course. E.g., the revocation check itself contains a measurement in basis B which would destroy the EPR state XY; this can be fixed by only measuring whether the revocation check would succeeds, without actually measuring m.

Theorem 1 (RTRE_{ow} is revocably one-way). *Let δ_T^{ow} be the time to compute the following things: a measurement whether two n-qubit registers are equal in a given basis B, a measurement whether two n-qubit registers are in an EPR state up to $t := \sqrt{n}$ phase flips and t bit flips, and one NOT- and one AND-gate.*

Assume that the protocol parameter n is superlogarithmic.

The protocol RTRE_{ow} from Definition 3 is $(T - \delta_T^{ow})$-revocably one-way, even if adversary A_2 is unlimited (i.e., after revocation, security holds information-theoretically).

A concrete security bound is derived in the full version [27].

Since revocable one-wayness does not imply (non-revocable) one-wayness, we additionally show the hiding property of RTRE_{ow}. Due to the presence of the one-time pad p, the proof is unsurprising.

4 Revocably Hiding TREs

We now turn to the problem of constructing revocably hiding TREs. The construction from the previous section is revocably one-way, but it is certainly not revocably hiding because the adversary might be lucky enough to guess a few bits of the basis B, measure the corresponding bits of the message m without modifying the state, and successfully pass revocation. So some bits of m will necessarily leak. The most natural approach for dealing with partial leakage (at least in the case of QKD) is to use privacy amplification. That is, we pick a function F from a suitable family of functions (say, universal hash functions with suitable parameters), and then to send m, we encrypt a random x using the revocably one-way TRE, and additionally transmit $F(x) \oplus m$. If x has sufficiently high min-entropy, $F(x)$ will look random, and thus $F(x) \oplus m$ will not leak anything about m. Additionally, we need to transmit F to the recipient, in a way that the adversary does not have access to it when measuring the quantum state. Thus, we have to include F in the classical TRE. So, altogether, we would send $(m \oplus F(x), \mathrm{TRE}_0(B, f))$ and $|m\rangle_B$. In fact, this scheme might be secure,

we do not have an attack. Yet, when it comes to proving its security, we face difficulties: In the proof of RTRE_{ow}, to use the hiding property of TRE_0, we identified a property that can be checked in time T, and that guarantees that m cannot be guessed. (Namely, we used that the registers XY contain EPR pairs up to some errors which implies that the adversary cannot predict the outcome m of measuring Y.) In the present case, we would need more. We need a property P that guarantees that $F(x)$ is indistinguishable from random given the adversary's state when x is the outcome of measuring Y. Note that here it is not sufficient to just use that x has high min-entropy and that F is a strong randomness extractor; at the point when we test the property P, F is already fixed and thus not random. Instead, we have to find a measurable property P' that guarantees: For the particular value F chosen in the game, $F(x)$ is indistinguishable from randomness. (And additionally, we need that P' holds with overwhelming probability when $\mathrm{TRE}_0(B, f)$ is replaced by a fake TRE not containing B, f.) We were not able to identify such a property.[8]

Using CSS Codes. This discussion shows that, when we try to use privacy amplification, we encounter the challenge how to transmit the hash function F. Yet, in the context of QKD, there is a second approach for ensuring that the final key does not leak any information: Instead of first exchanging a raw key and then applying privacy amplification to it, Shor and Preskill [24] present a protocol where Alice and Bob first create shared EPR pairs with a low number of errors. In our language: Alice and Bob share a superposition of states $|\widetilde{fe}\rangle$ with $\omega(f), \omega(e) \leqslant t$. Then they use the fact that, roughly speaking, $|\widetilde{0^n 0^n}\rangle$ is an encoding of $|\widetilde{0^\ell 0^\ell}\rangle$ for some $\ell < n$ using a random CSS code correcting t bit/phase error. (Calderbank-Shor-Steane codes [8,25].) So if Alice and Bob apply error correction and decoding to $|\widetilde{fe}\rangle$, they get the state $|\widetilde{0^\ell 0^\ell}\rangle$. Then, if Alice and Bob measure that state, they get identical and uniformly distributed keys, and the adversary has no information. Furthermore, the resulting protocol can be seen to be equivalent to one that does not need quantum codes (and

[8] To illustrate the difficulty of identifying such a property: Call a function F s-good if $F(x)$ is uniformly random if all bits x_i with $s_i = 0$ are uniformly random (and independent). In other words, F tolerates leakage of the bits with $s_i = 1$. For suitable families of functions F, and for s with low Hamming weight, a random F will be s-good with high probability. Furthermore, when using a fake TRE_0, XY is in state $|\widetilde{fe}\rangle$ with $s := (f \vee e)$ of low Hamming weight with overwhelming probability after successful revocation (this we showed in the security proof for RTRE_{ow}). In this case, all bits of Y with $s_i = 0$ will be "untampered" and we expect that $F(x)$ is uniformly random for s-good F (when x is the outcome of measuring Y). So we are tempted to choose P' as: "XY is in a superposition of states $|\widetilde{fe}\rangle$ such that the chosen F is $(f \vee e)$-good". This property holds with overwhelming property using a fake TRE_0. But unfortunately, this fails to guarantee that $f(x)$ is random. E.g., if $F(ab) = a \oplus b$, then F is 10-good and 01-good. Thus a superposition of $|\widetilde{10\,00}\rangle$ and $|\widetilde{01\,00}\rangle$ satisfies property P' for that F. But $\frac{1}{\sqrt{2}}|\widetilde{10\,00}\rangle + \frac{1}{\sqrt{2}}|\widetilde{01\,00}\rangle = \frac{1}{\sqrt{2}}|0000\rangle - \frac{1}{\sqrt{2}}|1111\rangle$, so $x \in \{00, 11\}$ with probability 1 and thus $F(x) = 0$ always. So P' fails to guarantee that $F(x)$ is random.

thus quantum computers) but only transmits and measures individual qubits (BB84-style). It turns out that we can apply the same basic idea to revocably hiding TREs.

For understanding the following proof sketch, it is not necessary to understand details of CSS codes. It is only important to know that for any CSS code C, there is a family of disjoint codes $C_{u,v}$ such that $\bigcup_{u,v} C_{u,v}$ forms an orthonormal basis of $\mathbb{C}^{\{0,1\}^n}$.

Consider the following protocol (simplified):

Definition 4 (Simplified protocol RTRE'_{hid}). *Let C be a CSS code on $\{0,1\}^n$ that encodes plaintexts from a set $\{0,1\}^m$ and that corrects t phase and bit flips. Let q be a parameter.*

- ***Encryption:*** *Create $q+n$ EPR pairs in registers X, Y. Pick a set $Q = \{i_1, \dots, i_q\} \in [q+n]_q$ of qubit pair indices and a basis $B \in \{0,1\}^q$, and designate the qubit pairs in XY selected by Q as "test bits" in basis B. (The remaining pairs in XY will be considered as an encoding of EPR pairs using C.) Send X together with the description of C and a hiding TRE $\mathrm{TRE}_0(Q)$ to the recipient.*
  The plaintext contained in the TRE is x where x results from: Consider the bits of Y that are not in Q as a codeword from one of the codes $C_{u,v}$. Measure what u, v are (this is possible since the $C_{u,v}$ are orthogonal). Decode the code word. Measure the result in the computational basis.
- ***Decryption:*** *Decrypt $\mathrm{TRE}_0(Q)$. Considering the bits of X that are not in Q as a codeword from $C_{u,v}$ and decode and measure as in the encryption.*
- ***Revocation:*** *Send back X. The sender measures the bit pairs from XY selected by Q using bases B, yielding r, r'. If $r = r'$, revocation succeeds.*

Note that this simplified protocol is a "randomized" TRE which does not allow us to encrypt an arbitrary message, but instead chooses the message x. The obvious approach to transform it to a normal TRE for encrypting a given message m is to send $m \oplus x$ in addition to the TRE. This is indeed what we do, but there are some difficulties that we discuss below.

Entanglement-Free Protocol. The protocol RTRE'_{hid} requires Alice to prepare EPR pairs and apply the decoding operation of CSS codes. While our protocol may not be feasible with current technology anyway due to the required quantum memory, we wish to reduce the technological requirements as much as possible. Fortunately, CSS codes have the nice property that decoding with subsequent measurement in the computational basis is equivalent to a sequence of individual qubit measurements. Using these properties, we can rewrite Alice so that she only sends and measures individual qubits in BB84 bases, and Bob stores and measures individual qubits in BB84 bases (i.e., like in RTRE_{ow}). See the final protocol description (Definition 5) below for details. In the full proof, this change means that we have to add further games in front of the sequence of games to rewrite the entanglement-free operations into EPR-pair based ones.

Early Key Revelation. One big problem remains: the security definition used for proving security of Definition 4 gives $m_b \oplus x$ to A_2, and not to A_1 as a natural

definition of randomized TREs would do. (We call this *late key revelation*) The effect of this is that RTRE'_{hid} is only secure if the plaintext x is not used before time T. This limitation, of course, contradicts the purpose of TREs and needs to be removed. We need *early key revelation* where the adversary A_1 is given $m_b \oplus x$. As our proof needs the fact that x is picked only after A_1 runs, our solution is to reduce security with early key revelation to security with late key revelation. This is done by guessing what x will be when invoking A_1. If that guess turns out incorrect in the end, we abort the game. Unfortunately, this reduction multiplies the advantage of the adversary by a factor of $2^{|x|} = 2^\ell$; the effect is that our final protocol will need an underlying scheme TRE_0 with security exponential in ℓ.

We can now present the precise protocol and its security:

Definition 5 (The protocol)

- *Let C_1, C_2 be a CSS code with parameters n, k_1, k_2, t. (n is the bit length of the codes, k_1, k_2 refer to the parameters of the codes C_1, C_2, and t to the number of corrected errors.)*
- *Let q be an integer.*
- *Let TRE_0 be a TRE with message space $\{0,1\}^q \times [q+n]_q \times C_1/C_2$. (Recall, $[q+n]_q$ refers to q-size subsets of $\{1,\ldots,q+n\}$, see page 133. C_1/C_2 denotes the quotient of codes.)*

We construct a revocable TRE RTRE_{hid} with message space C_1/C_2 (isomorphic to $\{0,1\}^\ell$ with $\ell := k_1 - k_2$).

*We **encrypt** a message $m \in C_1/C_2$ as follows:*

- *Pick uniformly $B \in \{0,1\}^q$, $Q \in [q+n]_q$, $p \in C_1/C_2$. $u \in \{0,1\}^n/C_1$, $r \in \{0,1\}^q$, $x \in C_1/C_2$, $w \in C_2$.*
- *Construct the state $|\Psi\rangle := U_Q^\dagger(H^B \otimes I_n)(|r\rangle \otimes |x \oplus w \oplus u\rangle)$. Here U_Q denotes the unitary that permutes the qubits in Q into the first half of the system. (I.e., $U_Q|x_1 \ldots x_{q+n}\rangle = |x_{a_1} \ldots x_{a_q}\, x_{b_1} \ldots x_{b_n}\rangle$ with $Q =: \{a_1,\ldots,a_q\}$ and $\{1,\ldots,q+n\}\backslash Q =: \{b_1,\ldots,b_n\}$; the relative order of the a_i and of the b_i does not matter.)*[9]
- *Compute $V_0 \leftarrow \mathrm{TRE}_0(B, Q, r, p)$.*
- *The TRE consists of $(V_0, u, m \oplus x \oplus p)$ and $|\Psi\rangle$.*

***Decryption** is performed as follows:*

- *Decrypt V_0, this gives B, Q, r, p.*
- *Apply U_Q to $|\Psi\rangle$ and measure the last n qubits in the computational basis; call the outcome γ.*[10]
- *Return $m := (\gamma \oplus u) \bmod C_2$.*

*The **revocation** protocol is the following:*

- *The recipient sends $|\Psi\rangle$ back to the sender.*

[9] Notice that, since $U_Q^\dagger$ is just a reordering of qubits, and H^B is a sequence of Hadamards applied to a known basis state, the state $|\Psi\rangle$ can also directly be produced by encoding individual qubits in the computational or diagonal basis, which is technologically simpler.

[10] Since U_Q is just a reordering of qubits, this just corresponds to measuring a subset of the qubits in the computational basis.

- *The sender applies* $(H^B \otimes I_n)U_Q$ *to* $|\Psi\rangle$ *and measures the first* q *qubits, call the outcome* r'.[11]
- *If* $r = r'$*, revocation succeeds (sender outputs* 1*).*

Notice that in this protocol (and in contrast to the simplified description above), we have included B, r in the TRE V_0, even though they are not needed by the recipient. In fact, the protocol would still work (and be secure with almost unmodified proof) if we did not include these values. However, when constructing unknown recipient encryption, the inclusion of B, r will turn out to be useful.

Theorem 2 (RTRE_{hid} **is revocably hiding).** *Let* δ_T^{hid} *be the time to compute the following things: q controlled Hadamard gates, applying an already computed permutation to* $n + q$ *qubits, a q-qubit measurement in the computational basis (called* M_R *in the proof), a comparison of two q-qubit strings, the error-correction/decoding operations* U_{uv}^{EC}, U_{uv}^{dec} *of the CSS code, a measurement whether two n-qubit registers are in the state* $\sum_{x\in C_1/C_2}|x\rangle|x\rangle$ *(called* P_{C_1/C_2}^{EPR} *in the proof), one AND-gate, and one NOT-gate.*

Assume that TRE_0 *is* T*-hiding with* $(2^{-2(k_1-k_2)}\cdot negligible)$*-security.*[12] *Assume that* $tq/(q+n) - 4(k_1 - k_2)\ln 2$ *is superlogarithmic.*

Then the TRE from Definition 5 is $(T - \delta_T^{hid})$*-revocably hiding even if* A_2 *is unlimited (i.e., after revocation, security holds information-theoretically).*

A concrete security bound is derived in the full version [27].

Those parameters can always be instantiated [27], leading to a revocable TRE for logarithmic length messages, and a TRE for arbitrary length messages if TRE_0 has exponential security. Furthermore, RTRE_{hid} is also T-hiding.

5 TREs in the Random Oracle Model

We present constructions and transformations of TREs in the random oracle model. (We use the quantum random oracle that can be accessed in superposition, cf. [5].)

The results in this section will be formulated with respect to two different timing models. In the *sequential oracle-query timing model*, one oracle query is one time step. I.e., if we say an adversary runs in time T, this means he performs at most T random oracle queries. In the *parallel oracle-query timing model*, an arbitrary number of parallel oracle-queries can be performed in one time step. However, in time T, at most T oracle queries that depend on each other may be performed.[13] More formally, if the oracle is H, the adversary can query $H(x_1), \ldots, H(x_q)$ for arbitrarily large q and arbitrary $x_1, \ldots, x_n$ in each

[11] Since U_Q is just a reordering of the qubits, this is equivalent to measuring a subset of the qubits in the bases specified by B.

[12] I.e., in Definition 1, we require that the advantage is not only negligible, but actually $\leqslant 2^{-2(k_1-k_2)}\mu$ for some negligible μ.

[13] In [16], this is called "T levels of adaptivity".

time step. (Of course, if the adversary is additionally sequential-polynomial-time, then q will be polynomially bounded.)

Security in those timing models implies security in timing models that count actual (sequential/parallel) computation steps because in each step, at most one oracle call can be made.

5.1 One-Way to Hiding

In the previous section, we have seen how to construct revocably hiding TREs. However, the construction was relatively complex and came with an exponential security loss in the reduction. As an alternative, we present a transformation takes a TRE that is (revocably) one-way and transforms it into one that is (revocably) hiding in the random oracle model. The basic idea is straightforward: we encrypt a key k in a one-way TRE, and use $H(k)$ as a one-time-pad to encrypt the message:

Theorem 3 (Hiding TREs). *Let H be a random oracle and let* TRE *be a (revocable or non-revocable) TRE (not using H).*

Then the TRE TRE′ *encrypts m as follows: Run $k \xleftarrow{\$} \{0,1\}^n$, $V' \leftarrow \mathrm{TRE}(k)$, and then return $V := (V', m \oplus H(k))$. (Decryption is analogous, and revocation is unchanged from* TRE.*)*

Then, if TRE *is T-oneway and T-revocably one-way then* TRE′ *is T-revocably hiding. And if* TRE *is T-oneway then* TRE′ *is T-hiding. (The same holds "without offline-queries"; see Section 5.2 below.)*

This holds both for the parallel and the sequential oracle-query timing model.[14]

Notice that we assume that TRE does not access H. Otherwise simple counterexamples can be constructed. (E.g., $\mathrm{TRE}(k)$ could include $H(k)$ in the TRE V'.) However, TRE may access another random oracle, say G, and TRE′ then uses both G and H.

In a classical setting, this theorem would be straightforward to prove (using lazy sampling of the random oracle). Yet, in the quantum setting, we need a new technique for dealing with this. We present a generic lemma for reducing hiding-style properties (semantic security) to a one-wayness-style properties (unpredictability) from which we can derive Theorem 3.

5.2 Precomputation

We will now develop a second transformation for TREs in the random oracle model. The security definition for TREs permit the adversary to run an arbitrary (sequential-polynomial-time) computation before receiving the TRE. In particular, we do not have a good upper bound on the number of oracle queries performed in this precomputation phase ("offline queries"). This can make proofs harder because even if the adversary runs in time T, this does not allow us to conclude that only T oracle queries will be performed. Our transformation will allow us to transform a TRE that is only secure when the adversary makes no

offline queries (such as the one presented in Section 5.3 below) into a TRE that is secure without this restriction.

We call a TRE *T-hiding without offline-queries* if the hiding property holds for adversaries were A_0 makes no random oracle queries. Analogously we define *T-revocably hiding without offline-queries* and *T-one-way without offline-queries*.

To transform a TRE that is secure without offline-queries into a fully secure one, the idea is to make sure that the offline-queries are useless for the adversary. We do this by using only a part $H(a\|\cdot)$ of the random oracle where a is chosen randomly with the TRE. Intuitively, since during the offline-phase, the adversary does not know a, none of his offline-queries will be of the form $H(a\|\cdot)$, thus they are useless.

Theorem 4 (TREs with offline-queries). *Let G and H be random oracles and ℓ superlogarithmic. Let* TRE *be a revocable TRE using G. Let* TRE$'$ *be the result of replacing in* TRE *all oracle queries $G(x)$ by queries $H(a\|x)$, where a is chosen by the encryption algorithm of* TRE$'$ *and is included in the message send to the recipient.*

If TRE *is T-revocably hiding without offline-queries then* TRE$'$ *is T-revocably hiding (and analogously for T-hiding). This holds both for the parallel and the sequential oracle-query timing model.*[14]

To prove this, we develop a general lemma for this kind of transformations. (In the classical setting this is simple using the lazy sampling proof technique, but that is not available in the quantum setting.)

5.3 Iterated Hashing

In all constructions so far we assumed that we already have a (non-revocable) TRE. In the classical setting, only two constructions of TREs are known. The one from [22] can be broken by factoring, this leaves only repeated hashing as a candidate for the quantum setting. We prove that the following construction to be one-way without offline queries:

Definition 6 (Iterated hashing). *Let n and T be polynomially-bounded integers (depending on the security parameter), and assume that n is superlogarithmic. Let $H : \{0,1\}^n \to \{0,1\}^n$ denote the random oracle. The timed-release encryption* TRE_{ih} *with message space $\{0,1\}^n$ encrypts m as $V := H^{T+1}(0^n) \oplus m$.*

We can prove that TRE_{ih} is T-one-way *without* offline queries. TRE_{ih} is obviously not one-way *with* offline queries, the adversary can precompute $H^{T+1}(0^n)$. Yet, using the random-oracle transformations from Theorems 3 and 4, we can transform it into a hiding TRE. This is plugged into RTRE_{ow}, to get a revocably one-way TRE, and using Theorem 3 again, we get a revocably hiding TRE in the random oracle model. (The resulting protocol is spelled out in the full version [27].)

[14] For other timing models, the reduction described in the proof may incur a overhead, leading to a smaller T for TRE$'$.

An alternative construction is to plug TRE_{ih} (after transforming it using Theorems 3 and 4) into RTRE_{hid}. This results in a more complex yet everlastingly secure scheme.

And finally, if we wish to avoid the random oracle model altogether, we can take as our basic assumption that a suitable variant of iterated hashing[15] is a hiding TRE, and get a revocably hiding, everlastingly secure TRE by plugging it into RTRE_{hid}.

Acknowledgements. Dominique Unruh was supported by the Estonian ICT program 2011-2015 (3.2.1201.13-0022), the European Union through the European Regional Development Fund through the sub-measure "Supporting the development of R&D of info and communication technology", by the European Social Fund's Doctoral Studies and Internationalisation Programme DoRa, by the Estonian Centre of Excellence in Computer Science, EXCS. We thank Sébastien Gambs for the suggesting the data retention application.

References

1. Alleaume, R., Bouda, J., Branciard, C., Debuisschert, T., Dianati, M., Gisin, N., Godfrey, M., Grangier, P., Langer, T., Leverrier, A., Lutkenhaus, N., Painchault, P., Peev, M., Poppe, A., Pornin, T., Rarity, J., Renner, R., Ribordy, G., Riguidel, M., Salvail, L., Shields, A., Weinfurter, H., Zeilinger, A.: Secoqc white paper on quantum key distribution and cryptography. arXiv:quant-ph/0701168v1 (2007)
2. Ambainis, A., Mosca, M., Tapp, A., Wolf, R.: Private quantum channels. In: FOCS 2000, pp. 547–553. IEEE (2000)
3. Bennett, C.H., Brassard, G.: Quantum cryptography: Public-key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computers, Systems and Signal Processing 1984, pp. 175–179. IEEE Computer Society (1984)
4. Bitansky, N., Canetti, R., Chiesa, A., Tromer, E.: From extractable collision resistance to succinct non-interactive arguments of knowledge, and back again. In: ITCS 2012, pp. 326–349. ACM, New York (2012)
5. Boneh, D., Dagdelen, Ö., Fischlin, M., Lehmann, A., Schaffner, C., Zhandry, M.: Random oracles in a quantum world. In: Lee, D.H., Wang, X. (eds.) ASIACRYPT 2011. LNCS, vol. 7073, pp. 41–69. Springer, Heidelberg (2011)
6. Boneh, D., Naor, M.: Timed commitments. In: Bellare, M. (ed.) CRYPTO 2000. LNCS, vol. 1880, pp. 236–254. Springer, Heidelberg (2000)
7. Cachin, C., Maurer, U.: Unconditional security against memory-bounded adversaries. In: Kaliski Jr., B.S. (ed.) CRYPTO 1997. LNCS, vol. 1294, pp. 292–306. Springer, Heidelberg (1997)
8. Calderbank, A.R., Shor, P.W.: Good quantum error-correcting codes exist. Phys. Rev. A 54, 1098 (1996), `http://arxiv.org/abs/quant-ph/9512032v2`
9. Coffman, V., Kundu, J., Wootters, W.K.: Distributed entanglement. Phys. Rev. A 61, 052306 (2000)

[15] E.g., $(a, H^{T+2}(a) \oplus m)$ for random a. Or the protocol resulting from applying Theorems 3 and 4 to Definition 6. That this is a realistic assumption for suitable hash functions is confirmed by our analysis in the random oracle model.

10. Damgård, I., Fehr, S., Salvail, L., Schaffner, C.: Cryptography in the bounded quantum-storage model. In: FOCS 2005, pp. 449–458 (2005), Full version is arXiv:quant-ph/0508222v2
11. Dingledine, R., Mathewson, N., Syverson, P.: Tor: the second-generation onion router. In: USENIX 2004, SSYM 2004, p. 21. USENIX Association, Berkeley (2004)
12. Dupuis, F., Nielsen, J.B., Salvail, L.: Actively secure two-party evaluation of any quantum operation. In: Safavi-Naini, R., Canetti, R. (eds.) CRYPTO 2012. LNCS, vol. 7417, pp. 794–811. Springer, Heidelberg (2012)
13. Einstein, A., Podolsky, B., Rosen, N.: Can quantum-mechanical description of physical reality be considered complete? Phys. Rev. 47, 777–780 (1935)
14. European Parliament & Council. Directive 2006/24/ec, directive on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks. Official Journal of the European Union L 105, 54–63 (2006), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF
15. Khodjasteh, K., Sastrawan, J., Hayes, D., Green, T.J., Biercuk, M.J., Viola, L.: Designing a practical high-fidelity long-time quantum memory. Nature Communications 4 (2013)
16. Mahmoody, M., Moran, T., Vadhan, S.: Time-lock puzzles in the random oracle model. In: Rogaway, P. (ed.) CRYPTO 2011. LNCS, vol. 6841, pp. 39–50. Springer, Heidelberg (2011)
17. Müller-Quade, J., Unruh, D. (January 2007), http://eprint.iacr.org/2006/422
18. Nielsen, M., Chuang, I.: Quantum Computation and Quantum Information, 10th anniversary edn. Cambridge University Press, Cambridge (2010)
19. Palmer, E.: Wikileaks backup plan could drop diplomatic bomb. CBS News (December 2010), http://www.cbsnews.com/stories/2010/12/02/eveningnews/main7111845.shtml
20. Rabin, M.O.: Hyper-encryption by virtual satellite. Science Center Research Lecture Series (December 2003), http://athome.harvard.edu/programs/hvs/
21. Rivest, R.: Description of the LCS35 time capsule crypto-puzzle (April 1999), http://people.csail.mit.edu/rivest/lcs35-puzzle-description.txt
22. Rivest, R.L., Shamir, A., Wagner, D.A.: Time-lock puzzles and timed-release crypto. Technical Report MIT/LCS/TR-684, Massachusetts Institute of Technology (February 1996), http://theory.lcs.mit.edu/~rivest/RivestShamirWagner-timelock.ps
23. Shor, P.W.: Algorithms for quantum computation: Discrete logarithms and factoring. In: 35th Annual Symposium on Foundations of Computer Science, Proceedings of FOCS 1994, pp. 124–134. IEEE Computer Society (1994)
24. Shor, P.W., Preskill, J.: Simple proof of security of the BB84 quantum key distribution protocol. Phys. Rev. Lett. 85, 441–444 (2000)
25. Steane, A.M.: Multiple particle interference and quantum error correction. Proc. R. Soc. London A 452, 2551–2576 (1996)
26. Unruh, D.: Protokollkomposition und Komplexität (Protocol Composition and Complexity). PhD thesis, Universität Karlsruhe (TH), Berlin (2006), http://www.cs.ut.ee/~unruh/publications/unruh07protokollkomposition.html (in German)
27. Unruh, D.: Revocable quantum timed-release encryption. IACR ePrint 2013/606 (2013) (full version of this paper)