

Revocable quantum timed-release encryption

Dominique Unruh

September 19, 2013

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 losing 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	1	C	CSS codes – recap and properties	26
1.1	Example applications	2	D	Full proofs: revocably hiding timed-release encryptions	30
1.2	Our contribution	3	E	Full proofs: one-way to hiding	40
1.3	Preliminaries	4	F	Full proofs: precomputation	43
2	Defining revocable TREs	5	G	Full proofs: iterated hashing	47
3	Constructing revocably one-way TREs	7	H	Hash-based revocable timed-release encryptions	50
4	Revocably hiding TREs	10	I	Unknown recipient encryption	50
5	TREs in the random oracle model	15		References	56
5.1	One-way to hiding	15		Symbol index	58
5.2	Precomputation	16		Keyword index	59
5.3	Iterated hashing	17			
A	Auxiliary lemmas	17			
B	Full proof: revocably one-way timed-release encryptions	19			

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., [Riv99] publishes a secret message that is supposed not to be openable before 2034.) Example use cases could be: messages for posterity [RSW96]; 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

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

secrets where none of the parties should be able to abort depending on the data received by the other; fair contract signing [BN00]; electronic auctions [BN00]; mortgage payments [RSW96]; concurrent zero-knowledge protocols [BN00]; ...

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.

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 [Pal10].) 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

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 [KSH⁺13].

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., [Eur06]). 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.,

²One 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 [BCCT12] so that the verification time does not depend on T). Then client and dealer perform a quantum two-party computation [DNS12] 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 .

through (a quantum variant of) TOR [DMS04], 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. (More details in Appendix I.) 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.

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 loses 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., [MQU07, DFSS05, ABB⁺07, CM97, Rab03]): 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 losing everlasting security.

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

The second transformation allows us to assume 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 [RSW96] present a construction based on RSA; it is obviously not secure in the quantum setting [Sho94]. 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 [Unr06]). 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 [RSW96] but not based on RSA or other quantum-easy problems.

Unknown recipient encryption. In Appendix I, we formalize the notion and security of unknown recipient encryption (URE, see Section 1.1 above) and give a construction based on our revocably hiding time-vault construction, that we prove to be secure (even with everlasting security).

1.3 Preliminaries

For the necessary background in quantum computing, see, e.g., [NC10].

Let $\omega(x)$ denote the Hamming weight of x . By $[q+n]_q$ we denote the set of all size- q subsets of $\{1, \dots, q+n\}$. I.e., $S \in [q+n]_q$ iff $S \subseteq \{1, \dots, q+n\}$ and $|S| = q$. By \oplus we mean bitwise XOR (or equivalently, addition in $\text{GF}(2)^n$). 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 $|\beta_{fe}\rangle = (Z^f X^e \otimes I)|\beta_{00}\rangle = (I \otimes X^e Z^f)|\beta_{00}\rangle$. In slight abuse of notation, we call $|\beta_{00}\rangle$ an *EPR pair* (originally, [EPR35] used $|\beta_{11}\rangle$). 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 $A^{x_1} \otimes \dots \otimes A^{x_n}$. 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 $|\beta_{f_1 e_1}\rangle \otimes \dots \otimes |\beta_{f_n e_n}\rangle$, 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., $\|\Psi\|^2 = \langle \Psi | \Psi \rangle$) and let $\|\cdot\|$ denote the corresponding operator norm (i.e., $\|A\| := \sup_{x \neq 0} \|Ax\|/\|x\|$).

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

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

⁴Iterated 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. [MMV11] 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.

2 Defining revocable TREs

Timing models. Before we can define the security of TREs, we need to discuss the *timing model* we use to measure the adversary’s complexity. In most situations, we wish that an adversary cannot gain any advantage by parallelizing. This is because if we wish to construct a TRE that should not be decrypted before 1 day has passed, we need to know how much computation time may pass in that time. While it is reasonable to assume some upper bounds on the sequential speed of the hardware available to the attacker, we may not know how many parallel instances of this hardware the attacker uses. Thus our timing model should preferably count parallel, not sequential time. (“Solving the puzzle should be like having a baby: two women can’t have a baby in 4.5 months.” [RSW96])

Instead of fixing a concrete timing model, we will keep our definitions and results generic in the timing model that is used (except when stated explicitly). We will only sometimes assume that if performing operations X_1 takes time T_1 and operations X_2 take time T_2 , then performing T_1 and T_2 takes time at most $X_1 + X_2$. (This should be satisfied by most reasonable timing models such as circuit size, circuit depth, execution steps of a RAM machine, etc.)

We will also need the notion of *sequential polynomial time*. This is the notion of polynomial time usually employed in cryptography that counts all executions steps, no matter whether they are in parallel or sequential. We will not need a more fine grained notion such as “in sequential time T ” for some concrete T . Thus sequential polynomial time is more or less independent of the machine model, but for concreteness we specify that an algorithm is sequential-polynomial-time if it can be implemented by a probabilistic polynomial-time Turing machine. To understand why we need the notion of sequential polynomial time, consider the following example TRE: $\text{TRE}(m) := (k, \text{enc}(H^T(k), m))$ with $k \xleftarrow{\$} \{0, 1\}^\eta$. One might assume that m cannot be learned by T -time adversaries (with respect to parallel time), because $H^T(k)$ can only be computed by T sequential applications of H . But this is not correct: using brute-force, we can compute m from $\text{enc}(H^T(k), m)$ using 2^η parallel decryptions. Of course, such an attack is not practical. Indeed, TRE seems hiding with respect to T -(parallel)-time adversaries that are at the same time sequential-polynomial-time. So the right notion of an adversary against a TRE is one that is both T -time and sequential-polynomial-time.

Non-revocable TREs. First, we define the security properties a normal (non-revocable) TRE should have. We are not aware of a suitable formal definition in the literature.

Hofheinz and Unruh [HU05] formally define what they call time-lock puzzles, but those are intended for proofs of computational power and not for encrypting messages and thus do not formalize anything resembling our hiding property. Also, their definition can only express asymptotic hardness of the puzzle and does not take into account parallel time. Mahmoody, Moran, and Vadhan [MMV11] also define time-lock puzzles. They take into account parallel execution time and can express time in a more fine-grained way. However, their definition is not suitable for encrypting messages. Also, they do not exclude adversaries that use exponential parallelism; this excludes many sensible puzzles, for example those that use encryption as a building block.⁵ Dwork and Naor [DN93] give an informal definition of “proofs of work”, but again this does not deal with encryption of messages, and parallel time is (intentionally) not considered. Note that all the above definitions are well-suited for the applications they were specified for, which was not the sending of messages into the future.

We first define what a TRE (secure or not) is:

Definition 1 (Timed-release encryption) A timed-release encryption (TRE) with message space M consists of two algorithms:

- Encryption. A probabilistic sequential polynomial-time algorithm TRE that takes as input a message $m \in M$ (and the security parameter which in the following will be left implicit) and outputs V (the TRE itself).
- Decryption. A probabilistic sequential-polynomial-time algorithm that, upon input V (as constructed by TRE), outputs m with overwhelming probability.

Roughly speaking, a timed-release encryption TRE is T -hiding if within time T , one cannot learn anything about the message, i.e., for any m_0, m_1 , $\text{TRE}(m_0)$ and $\text{TRE}(m_1)$ are indistinguishable for a T -time, sequential-polynomial-time adversary A_1 . (See the discussion above why we additionally need

⁵E.g., the timed-release encryption TRE from the discussion of sequential-polynomial-time above would not be secure according to their definition.

sequential-polynomial-time.) Furthermore, we allow the adversary an arbitrary (sequential-polynomial-time) precomputation A_0 before he receives the TRE, this accounts for the fact that we cannot well bound the amount of time the adversary has invested before we produced the TRE.

Definition 2 (Hiding timed-release encryption) *A timed-release encryption TRE with message space M is T -hiding if for algorithms A_0, A_1 such that A_0 is sequential-polynomial-time and A_1 is sequential-polynomial-time⁶ and T -time we have that*

$$\begin{aligned} & | \Pr[b' = 1 : (m_0, m_1) \leftarrow A_0(), V \leftarrow \text{TRE}(m_0), b' \leftarrow A_1(V)] \\ & - \Pr[b' = 1 : (m_0, m_1) \leftarrow A_0(), V \leftarrow \text{TRE}(m_1), b' \leftarrow A_1(V)] | \end{aligned}$$

is negligible. (We assume that A_0 always outputs $m_0, m_1 \in M$, and we allow A_0, A_1 to keep state between activations.⁷)

We also define one-wayness of TREs. T -one-wayness only requires that in time T , the adversary cannot guess the uniformly random message m completely. This is quite a weak property, but we need it for intermediate results in some constructions.

Definition 3 (One-way TRE) *A timed-release encryption TRE with message space M is T -one-way, if for any quantum adversary (A_0, A_1) where A_1 is sequential-polynomial-time and T -time and A_0 is sequential-polynomial-time, we have that*

$$\Pr[m = m' : A_0(), m \xleftarrow{\$} M, V \leftarrow \text{TRE}(m), m' \leftarrow A_1(V)]$$

is negligible. (We allow A_0, A_1 to keep state between activations.)

Revocable TREs. We now define what revocable TREs are. A revocable TRE differs from a TRE only by the additional revocation protocol that is supposed to convince the sender that the recipient cannot decrypt the TRE any more.

Definition 4 (Revocable TREs) *A revocable timed-release encryption consists of a timed-release encryption TRE and a two-party sequential-polynomial-time protocol, the revocation protocol, between sender and recipient of the TRE. (The sender may keep state during the computation of the TRE that is used in the revocation protocol.)*

For any $m \in M$ (where m may depend on the security parameter), it holds:

- *Let $V \leftarrow \text{TRE}(m)$. Run the revocation protocol where the recipient gets V as input. Then, with overwhelming probability, the sender accepts the revocation (i.e., outputs 1).*

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 contain in the TRE. When formalizing this, we have to be careful. A definition like: “conditioned on revocation succeeding, $p_0 := \Pr[\text{adversary outputs 1 given TRE}(m_0)]$ and $p_1 := \Pr[\text{adversary outputs 1 given TRE}(m_1)]$ are close ($|p_0 - p_1|$ is negligible)” does not work: if $\Pr[\text{revocation succeeds}]$ 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 “ $|p_0 - p_1| \cdot \Pr[\text{revocation succeeds}]$ ” is problematic: Does $\Pr[\text{revocation succeeds}]$ refer to an execution with $\text{TRE}(m_0)$ or $\text{TRE}(m_1)$?. Instead, we will require “ $|p_0 - p_1|$ is negligible with $p_i := \Pr[\text{adversary outputs 1 and revocation succeeds given TRE}(m_i)]$ ”. This definition avoids the complications of a conditional probability and additionally has implies as side effect that also $\Pr[\text{revocation succeeds given TRE}(m_0)]$ and $\Pr[\text{revocation succeeds given TRE}(m_1)]$ are close.

Furthermore, the discussion concerning sequential-polynomial-time and precomputation from Definition 2 applies here as well.

Definition 5 (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 $b \in \{0, 1\}$:*

⁶We add sequential-polynomial-time here, because with respect to some time-measures, T -time might not imply sequential-polynomial-time. E.g., if T -time refers to parallel time, then NP is easy even for relatively small T .

⁷If M is infinite, we might also wish to add the condition that $|m_0| = |m_1|$, otherwise constructing hiding TRE for such M is trivially impossible.

- $(m_0, m_1) \leftarrow A_0()$.
- $V \leftarrow \text{TRE}(m_b)$.
- 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 we have that the advantage

$$|\Pr[b' = 1 \wedge ok = 1 : G(0)] - \Pr[b' = 1 \wedge ok = 1 : G(1)]|$$

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 6 (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 $V \leftarrow \text{TRE}(m)$.
- 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 (Theorem 2).

Definition 7 (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 4.)
- Compute $V_0 \leftarrow \text{TRE}_0(B, p)$.
- Send V_0 and $|\Psi\rangle$.

Decryption is performed as follows:

- Decrypt V_0 , this gives B, p .
- Measure $|\Psi\rangle$ in basis B ; call the outcome γ .

- Return $m := \gamma \oplus p$.

The **revocation** protocol is the following:

- 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.⁸ 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).⁹ However, the adversary has access to $V_0 = \text{TRE}_0(B)$ 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.

One might want to save the argument in the following way: Although $V_0 = \text{TRE}_0(B)$ information-theoretically contains B , it is indistinguishable from $\hat{V}_0 = \text{TRE}_0(\hat{B})$ 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 is 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 $\text{TRE}_0(B)$, 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 $|\Psi\rangle$ by 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.)¹⁰

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 $\hat{V}_0 = \text{TRE}_0(\hat{B})$ for an independent \hat{B} instead of $V_0 = \text{TRE}_0(B)$. 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 $|\Psi\rangle := |m\rangle_B$ 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

⁸This fact also underlies the security of BB84-style QKD protocols [BB84].

⁹Again, 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 .

¹⁰To 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 $K \in \{0, 1\}^{2^n}$, i.e., $E_K(|\Psi\rangle) = Z^{K_1} X^{K_2} |\Psi\rangle$ with $K = K_1 \| K_2$ [AMTW00]. $\text{RTRE}(m) := (E_K(|m\rangle_B), B, \text{TRE}_0(K))$. 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 $|\Phi\rangle = Z^{K_1} X^{K_2} H^B |m\rangle = H^B X^{K_1 * \bar{B}} Z^{K_1 * \bar{B}} Z^{K_2 * \bar{B}} X^{K_2 * \bar{B}} |m\rangle = \pm |m \oplus (K_2 * \bar{B}) \oplus (K_1 * B)\rangle_B$ where $*$ is the bit-wise product and \bar{B} the complement of B . Thus the measurement of $|\Phi\rangle$ 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 $\text{TRE}_0(K)$, 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 $\text{TRE}_0(K)$.

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 ([CKW00]; 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 succeed, 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 (defined as P_B^- on page 9 below), a measurement whether two n -qubit registers are in an EPR state up to t phase flips and t bit flips (for a given t ; defined as P_t^{EPR} on page 10 below), and one NOT- and one AND-gate.*

Assume that the protocol parameter n is superlogarithmic.

The protocol RTRE_{ow} from Definition 7 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 given at the end of the proof in Appendix B, page 25.

Proof sketch. We now proceed to a more detailed proof sketch. The full proof is given in Appendix B.

Our proof proceeds as a sequence of games. Game 1 is the game from Definition 6 (with the definition of RTRE_{ow} inlined), it thus suffices to show that $\Pr[m = m' \wedge ok = 1 : \text{Game 1}]$ is negligible. We highlight changes between games in blue.

Game 1 (Original game)

- Run $A_0()$. $m \xleftarrow{\$} \{0, 1\}^n$, $p \xleftarrow{\$} \{0, 1\}^n$, $B \xleftarrow{\$} \{0, 1\}^n$. $V_0 \leftarrow \text{TRE}_0(B, p)$. $X \leftarrow |m \oplus p\rangle_B$.
- Run $A_1(X, V_0)$. (We pass the quantum register X to A_1 which means that A_1 has read-write access to it.)
- Measure X in basis B ; outcome γ . If $m \oplus p = \gamma$, $ok := 1$, else $ok := 0$. $m' \leftarrow A_2()$.

First, we use the laws of \oplus to get rid of the one-time-pad p which is irrelevant for the revocable one-wayness and only a hindrance in the present proof. The probability $\Pr[m = m' \wedge ok = 1]$ does not change.

Game 2 (One-time-pad removed)

- Run $A_0()$. $m \xleftarrow{\$} \{0, 1\}^n$, $p \xleftarrow{\$} \{0, 1\}^n$, $B \xleftarrow{\$} \{0, 1\}^n$. $V_0 \leftarrow \text{TRE}_0(B, p)$. $X \leftarrow |m\rangle_B$.
- Run $A_1(X, V_0)$. Measure X in basis B ; outcome γ . If $m = \gamma$, $ok := 1$, else $ok := 0$. $m' \leftarrow A_2() \oplus p$.

Now we introduce EPR pairs into the protocol as explained in the proof idea. Producing EPR pairs XY and measuring Y in basis B with outcome m is equivalent to picking m at random and initializing X with $|m\rangle_B$. Hence the new game is equivalent and $\Pr[m = m' \wedge ok = 1]$ does not change.

Game 3 (Using EPR pairs)

- Run $A_0()$. ~~$m \xleftarrow{\$} \{0, 1\}^n$~~ , $p \xleftarrow{\$} \{0, 1\}^n$, $B \xleftarrow{\$} \{0, 1\}^n$. $V_0 \leftarrow \text{TRE}_0(B, p)$.
- Initialize XY as $|\widetilde{0^n 0^n}\rangle$. Run $A_1(X, V_0)$. Measure X in basis B ; outcome γ .
- Measure Y in basis B , outcome m . If $m = \gamma$, $ok := 1$, else $ok := 0$. $m' \leftarrow A_2() \oplus p$.

Unfortunately, we cannot yet argue that the state of XY after a successful revocation is still an EPR state: Since we measure X and Y in basis B in order to perform the revocation check, XY will never contain an EPR state after that measurement. So we replace those measurements and the test $m = \gamma$ with a direct measurement whether X and Y would give the same outcome when both measured in basis B . I.e., apply the measurement operator $P_B^- := \sum_{x \in \{0, 1\}^n} |x\rangle_B \langle x, x|_B$. We show that again $\Pr[m = m' \wedge ok = 1]$ does not change.

Game 4 (Changed revocation test)

- Run $A_0()$. $p \xleftarrow{\$} \{0, 1\}^n$, $B \xleftarrow{\$} \{0, 1\}^n$. $V_0 \leftarrow \text{TRE}_0(B, p)$. Initialize XY as $|\widetilde{0^n 0^n}\rangle$.
- Run $A_1(X, V_0)$. Measure XY using P_B^- ; outcome ok . ~~Measure X in basis B ; outcome γ .~~
- Measure Y in basis B , outcome m . ~~If $m = \gamma$, $ok := 1$. Else $ok := 0$.~~ $m' \leftarrow A_2() \oplus p$.

Now we come to the crucial step of our proof. As explained in the proof idea, the property $P :=$ “the adversary cannot learn m ever (unless revocation fails)” (formally: “not $(m = m' \wedge ok = 1)$ ”) does not carry over between a setting where we use $\text{TRE}_0(B, p)$ and one where we use $\text{TRE}_0(\hat{B}, p)$. Instead, we want to use the property “after revocation but before measuring m , XY are still EPR pairs (up to some errors) or revocation fails”. We model this using a measurement operator $P_t^{\text{EPR}} := \sum_{f,e} |\widetilde{fe}\rangle\langle\widetilde{fe}|$ where the sum ranges over all $f, e \in \{0, 1\}^n$ with $\omega(f), \omega(e) \leq t$. (Remember that $|\widetilde{fe}\rangle$ stands for an EPR state with phase flips f and bit flips e , see page 4.) Here t is an arbitrary integer, but for best results we choose $t := \sqrt{n}$. That is, P_t^{EPR} tests whether two n -qubit registers form an EPR state (up to t phase flips and t bit flips). If we measure XY using P_t^{EPR} and call the outcome $isEPR$, property P can be written “not $(isEPR = 0 \wedge ok = 1)$ ”. This is reflected in the following game:

Game 5 (Testing the state)

- Run $A_0()$. $p \xleftarrow{\$} \{0, 1\}^n$, $B \xleftarrow{\$} \{0, 1\}^n$. $V_0 \leftarrow \text{TRE}_0(B, p)$. Initialize XY as $|\widetilde{0^n 0^n}\rangle$.
- Run $A_1(X, V_0)$. Measure XY using P_B^- ; outcome ok .
- Measure XY using P_t^{EPR} ; outcome $isEPR$.
- Measure Y in basis B , outcome m . $m' \leftarrow A_2() \oplus p$.

It is well-known that if XY form an EPR state, then the adversary’s state cannot contain any information about the outcome of measuring X (monogamy of entanglement). In the present case the situation is made more complicated because of the possibility of errors in the EPR state, because we do not know whether the state is really a t -error EPR state or whether the measurement P_t^{EPR} just got lucky on a somewhat different state, and because of the additional condition $ok = 1$. Still, we can prove

$$\Pr[m' = m \wedge ok = 1 : \text{Game 4}] \leq \sqrt{\Pr[isEPR = 0 \wedge ok = 1 : \text{Game 5}]} + 2^{-n}(n + 1)^{2t}.$$

In particular it is now sufficient to show that $\Pr[isEPR = 0 \wedge ok = 1]$ is negligible in Game 5.

Game 5 runs in time T . Thus, we can replace $\text{TRE}(B, p)$ by $\text{TRE}(\hat{B}, p)$ for random B without changing more than negligibly any property computed during the game. In particular, $\Pr[isEPR = 0 \wedge ok = 1]$ changes only by a negligible amount.

Game 6 (Using fake TRE)

- Run $A_0()$. $p \xleftarrow{\$} \{0, 1\}^n$, $B \xleftarrow{\$} \{0, 1\}^n$. $\hat{B} \leftarrow \{0, 1\}^n$. $V_0 \leftarrow \text{TRE}_0(\hat{B}, p)$.
- Initialize XY as $|\widetilde{0^n 0^n}\rangle$. Run $A_1(X, V_0)$. $B \xleftarrow{\$} \{0, 1\}^n$.
- Measure XY using P_B^- ; outcome ok . Measure XY using P_t^{EPR} ; outcome $isEPR$.

Finally, we can show that it is not possible to create a state that passes the equality test P_B^- for random B without already being close to an EPR state (with t bit/phase flips). That is, we show that $\Pr[isEPR = 0 \wedge ok = 1] \leq 2^{-t-1}$ which is negligible. This proves the revocable onewayness of RTRE_{ow} . \square

Since revocable one-wayness does not imply (non-revocable) one-wayness, we show the hiding property in an additional theorem. Due to the presence of the one-time pad p , the proof is unsurprising.

Theorem 2 (RTRE_{ow} is hiding) *The protocol RTRE_{ow} from Definition 7 is T -hiding. (A concrete security bound is given in Appendix B, page 26.)*

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 be 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 $(m \oplus F(x), \text{TRE}_0(B, f))$ 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 $\text{TRE}_0(B, f)$ is replaced by a fake TRE not containing B, f .) We were not able to identify such a property.¹¹

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 [SP00] 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 $|\widetilde{f}e\rangle$ with $\omega(f), \omega(e) \leq t$. 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 [CS96, Ste96], see Appendix C.) So if Alice and Bob apply error correction and decoding to $|\widetilde{f}e\rangle$, 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 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 8 (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 $\text{TRE}_0(Q)$ 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 $\text{TRE}_0(Q)$. 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, 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

¹¹To 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 $|\widetilde{f}e\rangle$ 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 $|\widetilde{f}e\rangle$ such that the chosen F is $(f \vee e)$ -good”. This property holds with overwhelming probability 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.

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.

In the revocation, why do we not simply measure whether XY consists of EPR pairs instead of comparing in a random basis? If we do that, our protocol cannot be transformed into a protocol without entanglement (paragraph “entanglement-free protocol” below). And why do we test only a subset Q of the qubit pairs? Otherwise our proof would break down: we use in the analysis of Game 7 that the parts of XY that contain the codeword from $C_{u,v}$ form EPR pairs. This would not hold if we would measure those parts in basis B .

Proof sketch. Now we can prove that this protocol is revocably hiding. Again, we use a sequence of games (the numbering is chosen to match the numbering in the full proof for the unsimplified protocol in Appendix D). The first game represents the definition of revocably hiding.

Game 4 (Revocable hiding property of RTRE'_{hid})

- (a) *The game is parametric in $b \in \{0, 1\}$.*
- (b) $(m_0, m_1) \leftarrow A_0()$. Pick B, Q . Initialize XY as $|0^{q+n}0^{q+n}\rangle$.
- (c) Measure from Y the parameters u, v of the CSS code $C_{u,v}$.
- (d) $V_0 \stackrel{\$}{\leftarrow} \text{TRE}_0(B)$. Run $A_1(X, V_0, u, v)$. (We pass the quantum register X to A_1 which means that A_1 has read-write access to it.)
- (e) Measure the Q -parts of X and Y in basis B ; if the outcomes are equal, $ok := 1$.
- (f) Measure the result of decoding the non- Q -part of Y ; outcome x .
- (g) $b' \leftarrow A_2(x \oplus m_b)$.

Note that since we analyze a “randomized” TRE, we did not encrypt the message m_b chosen by the adversary, but instead gave $x \oplus m_b$ to the adversary after getting the random plaintext x of the TRE. Notice also that we give $x \oplus m_b$ to the adversary A_2 and not to A_1 as would be more natural. We discuss reasons and solutions for this in the paragraph “early key revelation” below.

We need to show that $\mu := |\Pr[b' = 1 \wedge ok = 1 : \text{Game 4}(0)] - \Pr[b' = 1 \wedge ok = 1 : \text{Game 4}(1)]|$ is negligible. Here $\text{Game 4}(0)$ denotes Game 4 with parameter $b := 0$ and analogously for $b := 1$.

As in the security proof for RTRE_{ow} , we then transform the game into one where we test a property that will imply that the adversary does not learn anything about x after revocation, i.e., that μ is negligible. Since the plaintext x is the result of decoding Y using code $C_{u,v}$, a suitable property is: “When decoding Y using code $C_{u,v}$ and error correcting and decoding X using code $C_{u,v}$, then we get the state $|0^\ell 0^\ell\rangle$.”

Game 6 (Testing the state)

- (a) ~~The game is parametric in $b \in \{0, 1\}$.~~
- (b) $(m_0, m_1) \leftarrow A_0()$. Pick B, Q . Initialize XY as $|0^{q+n}0^{q+n}\rangle$.
- (c) Measure from Y the parameters u, v of the CSS code $C_{u,v}$.
- (d) $V_0 \stackrel{\$}{\leftarrow} \text{TRE}_0(B)$. Run $A_1(X, V_0, u, v)$.
- (e) Measure the Q -parts of X and Y in basis B ; if the outcomes are equal, $ok := 1$.
- (f) ~~Decode Y and error-correct and decode X (bits not in Q only), measure if the resulting state of XY (excluding Q -bits) is $|0^\ell 0^\ell\rangle$. If so, $isEPR := 1$.~~
- (g) ~~Measure the result of decoding the non- Q part of Y ; outcome x .~~
- (h) ~~$b' \leftarrow A_2(x \oplus m_b)$.~~

We can now prove the following bound (Lemma 24 in Appendix D).

$$\mu \leq \sqrt{\varepsilon} \quad \text{for} \quad \varepsilon := \Pr[ok = 1 \wedge isEPR = 0 : \text{Game 6}] \tag{1}$$

The proof of this bound is roughly the following (we ignore the condition $ok = 1$): A state that passes the test in step (f) with probability $1 - \varepsilon$ will have trace distance $\sqrt{\varepsilon}$ from a state that, when decoded and error corrected, is $|0^\ell 0^\ell\rangle$. Notice that before step (f), the state in Game 4 and Game 6 is the same. This means that if in Game 4, before step (f), we were to additionally error correct and decode X , we would have $|0^\ell 0^\ell\rangle$ in XY at that point (up to trace distance $\sqrt{\varepsilon}$). Thus by monogamy of entanglement, the adversary cannot have any information about the outcome x of measuring Y (except with probability $\sqrt{\varepsilon}$). Since applying error correction and decoding to X has no effect (X is not used any more afterwards), the same holds for the unmodified Game 4. Equation (1) follows.

Now, in Game 6, the steps after computing TRE_0 take time T because we removed A_2 from the game. (We ignore the additive overhead from decoding and error correction in this proof sketch.) Thus we can replace $\text{TRE}_0(Q)$ by a fake TRE without changing the probability of $\Pr[ok = 1 \wedge isEPR = 0]$ by more than a negligible amount.

Game 7 (Using fake TRE) Like Game 6, but using $V_0 \leftarrow \text{TRE}_0(\hat{Q})$ with independent \hat{Q} .

Finally, we show that $\Pr[ok = 1 \wedge isEPR = 0 : \text{Game 7}]$ is negligible as follows: B and Q are not used before step (e). That is, in step (e), we measure a random subset of the qubit pairs in XY in a random basis. Except with negligible probability, the only states that pass this test are EPR states with up to t bit/phase flips. I.e., after throwing away the test bits, we have a superposition of states $|\widetilde{fe}\rangle$ with $\omega(f), \omega(e) \leq t$. Since $|\widetilde{fe}\rangle = (Z^f X^e \otimes I)|0^{n+q}0^{n+q}\rangle$, and $|0^{n+q}0^{n+q}\rangle$ is an encoding of $|0^\ell 0^\ell\rangle$, error correction on X removes the effect of $Z^f X^e$, and then decoding leads to the state $|0^\ell 0^\ell\rangle$. That is, $isEPR = 1$ holds with overwhelming probability when revocation succeeds ($ok = 1$). Thus $\Pr[ok = 1 \wedge isEPR = 0 : \text{Game 7}]$ is negligible.

Combining all results, we have that μ is negligible. This shows the security of RTRE'_{hid} . \square

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 9) below for details. In the full proof, this change means that we have to add further games in front of the sequence (Games 2 and 3) to rewrite the entanglement-free operations into EPR-pair based ones.

Early key revelation. One big problem remains: the security definition used in Game 4 gives $m_b \oplus x$ to A_2 , and not to A_1 (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 $m_b \oplus x$. The problem is that when A_1 is executed, we do not know x yet. If we were to measure x earlier, the measurement of $isEPR$ in Game 6 would fail since measuring x would destroy the EPR pairs in XY . 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 . (In the full proof, this reduction is performed in the step between Games 1 and 2.)

Non-revocable hiding. Finally, we also need to show that the protocol is hiding (not just revocably hiding). As in the case of RTRE_{ow} , we do this by simply adding a one-time-pad p to the protocol.

The final protocol. We can now state the precise protocol and its security:

Definition 9 (The protocol)

- Let C_1, C_2 be a CSS code with parameters n, k_1, k_2, t . (See Appendix C.)
- 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 $\{1, \dots, q+n\}$, see page 4. 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., $U_Q|x_1 \dots x_{q+n}\rangle = |x_{a_1} \dots x_{a_q} x_{b_1} \dots x_{b_n}\rangle$ with $Q =: \{a_1, \dots, a_q\}$ and $\{1, \dots, q+n\} \setminus Q =: \{b_1, \dots, b_n\}$; the relative order of the a_i and of the b_i does not matter.)¹²

- Compute $V_0 \leftarrow \text{TRE}_0(B, Q, r, p)$.
- 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 .¹³
- Return $m := (\gamma \oplus u) \bmod C_2$.

The **revocation** protocol is the following:

- The recipient sends $|\Psi\rangle$ back to the sender.
- The sender applies $(H^B \otimes I_n)U_Q$ to $|\Psi\rangle$ and measures the first q qubits, call the outcome r' .¹⁴
- 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 in Appendix I, the inclusion of B, r will turn out to be useful.

Theorem 3 (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 $U_{uv}^{EC}, U_{uv}^{\text{dec}}$ from Appendix C, 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 $(2^{-2(k_1 - k_2)} \cdot \text{negligible})$ -security.¹⁵ Assume that $tq/(q + n) - 4(k_1 - k_2) \ln 2$ is superlogarithmic.

Then the TRE from Definition 9 is $(T - \delta_T^{\text{hid}})$ -revocably hiding even if A_2 is unlimited (i.e., after revocation, security holds information-theoretically).

A concrete security bound is given at the end of the proof, page 39, equation (20).

The full proof is given in Appendix D.

On the parameter choice. Concerning the choice of parameters in this theorem: we would like $\ell := k_1 - k_2$ to be as large as possible because it is the bitlength of the messages of this TRE. But if TRE_0 is only T -hiding with negligible-security, then we have to choose ℓ to be logarithmic.

If TRE_0 is T -hiding with exponential security, by rescaling the security parameter we can get $(2^{-2\ell} \cdot \text{negligible})$ -security for any message length ℓ . Note that for given ℓ , the codes C_1, C_2 can always be chosen to match the other constraints: First, fix some $t \geq 8\ell \ln 2 + \gamma$ where γ is superlogarithmic. Then fix an efficiently correctable CSS code C'_1, C_2 with parameters n, k'_1, k_2, t under the only constraint that $k'_1 - k_2 \geq \ell$ (i.e., it must correct at least t errors and encode words of length ℓ ; notice that we are free in our choice of n, k'_1, k_2 here). Then pick an arbitrary code C_1 with $C'_1 \supseteq C_1 \supseteq C_2$ and $|C_1| = 2^{\ell + k_2}$. This is possible since $k'_1 \geq \ell + k_2$. Note that C_1 still efficiently corrects t errors since it is a subset of C'_1 . So C_1, C_2 is a CSS code with parameters n, k_1, k_2, t such that $\ell = k_1 - k_2$. Then we set $q := n$ and have that $tq/(q + n) - 4(k_1 - k_2) \ln 2 = \gamma/2$ is superlogarithmic. (Of course, this way of choosing parameters is not optimal, it just shows that choosing suitable C_1, C_2 is always possible. For really fine tuning the parameters, one best uses the precise bounds from (20) in the proof.)

Theorem 4 (RTRE_{hid} is hiding) The protocol RTRE_{hid} from Definition 9 is T -hiding.

The proof is completely analogous to that of Theorem 2.

¹²Notice 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.

¹³Since U_Q is just a reordering of qubits, this just corresponds to measuring a subset of the qubits in the computational basis.

¹⁴Since 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 .

¹⁵I.e., in Definition 5, we require that the advantage is not only negligible, but actually $\leq 2^{-2(k_1 - k_2)}\mu$ for some negligible μ .

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. [BDF⁺11].)

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.¹⁶ More formally, if the oracle is H , the adversary can query $H(x_1), \dots, H(x_q)$ for arbitrarily large q and arbitrary x_1, \dots, x_n in each 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 that 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 5 (Hiding TREs (details in Theorem 10)) *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 $k \xleftarrow{\$} \{0, 1\}^n$, $V' \leftarrow \text{TRE}(k)$, and then return $V := (V', m \oplus H(k))$. (Decryption is analogous, and revocation is unchanged from TRE.)

Then, if TRE is T -one-way and T -revocably one-way then TRE' is T -revocably hiding. And if TRE is T -one-way 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.¹⁷

Notice that we assume that TRE does not access H . Otherwise simple counterexamples can be constructed. (E.g., $\text{TRE}(k)$ 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. The following lemma allows us to prove the security of TRE', but it is not restricted to TREs. Instead, it gives a generic reduction from a hiding-style property (semantic security) to a one-wayness-style property (unpredictability) that should be applicable to many other protocols, too.

Lemma 1 (One-way to hiding (details in Lemma 31)) *Let $H : \{0, 1\}^n \rightarrow \{0, 1\}^m$ be a random oracle. Consider an algorithm A that makes at most q oracle queries. Let $B^H(x)$ do the following: pick $i \xleftarrow{\$} \{1, \dots, q\}$ and $y \xleftarrow{\$} \{0, 1\}^m$, run $A^H(x, y)$ until (just before) the i -th query, measure the argument of the query in the computational basis, output the outcome. Let*

$$\begin{aligned} P_A^1 &:= \Pr[b' = 1 : x \leftarrow \{0, 1\}^n, b' \leftarrow A^H(x, H(x))] \\ P_A^2 &:= \Pr[b' = 1 : x \leftarrow \{0, 1\}^n, y \xleftarrow{\$} \{0, 1\}^m, b' \leftarrow A^H(x, y)] \\ P_B &:= \Pr[x = x' : x \leftarrow \{0, 1\}^n, x' \leftarrow B^H(x)] \end{aligned}$$

Then $|P_A^1 - P_A^2| \leq 2q\sqrt{P_B}$.

To show Theorem 5 using this lemma, we assume an adversary (A_0, A_1, A_2) against the revocably hiding property of TRE', and we have to show that $\Pr[b' = 1 \wedge ok = 1]$ is almost independent of the parameter b in the following game:

Game 1 (Revocably hiding of TRE')

(a) $H \xleftarrow{\$} (\{0, 1\}^n \rightarrow \{0, 1\}^m)$. $k \xleftarrow{\$} \{0, 1\}^n$.

¹⁶In [MMV11], this is called “ T levels of adaptivity”.

(b) $(m_0, m_1) \leftarrow A_0^H(\cdot)$. $V' \leftarrow \text{TRE}(k)$. $m := m_b \oplus H(k)$. Run the revocation protocol of TRE, with $A_1^H(V', m)$ as recipient. Let ok be the honest sender's output. If $ok = 1$, $b' \leftarrow A_2^H(\cdot)$, else $b' := 0$.

Let A be the algorithm that on input (k, h) performs step (b) from this game, but using h instead of $H(k)$ in $m := m_b \oplus H(k)$. Then P_A^1 from Lemma 1 is the probability of $b' = 1 \wedge ok = 1$ in Game 1. And P_A^2 is independent of b since $m_b \oplus h$ hides b for random h . Thus, to show that P_A^1 is almost independent of b (and thus TRE' revocably hiding), it is sufficient to show that $|P_A^1 - P_A^2|$ is negligible. By Lemma 1, it is in turn sufficient to show that P_B is negligible. Also, by construction of B , P_B is $\Pr[k' = k \wedge ok = 1]$ in the following game (in this proof sketch, we ignore the possibility that B aborts already during the execution of A_0 or A_1 , these cases are handled similarly):

Game 2 (Measure query)

(a) $H \xleftarrow{\$} (\{0, 1\}^n \rightarrow \{0, 1\}^m)$. $k \xleftarrow{\$} \{0, 1\}^n$. $(m_0, m_1) \leftarrow A_0^H(\cdot)$. $V' \leftarrow \text{TRE}(k)$.

(b) $i \xleftarrow{\$} \{1, \dots, \#queries\}$. $h \xleftarrow{\$} \{0, 1\}^m$. $m := m_b \oplus h$.

(c) Run the revocation protocol with $A_1^H(V', m)$, outcome ok . If $ok = 1$, run $A_2^H(\cdot)$ until the i -th query and measure the argument k' to that query. Otherwise set $k' := \perp$.

Notice that this is the revocable one-wayness game for TRE (where step (b) is part of the adversary). Thus $\Pr[k' = k \wedge ok = 1]$ is negligible, so P_B and hence $|P_A^1 - P_A^2|$ is negligible, and thus TRE' is revocably hiding.

Full proofs of Lemma 1 and Theorem 5 are given in Appendix E.

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 Definition 2 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 6 (TREs with offline-queries (details in Theorem 11)) *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.¹⁷

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.)

Lemma 2 (Removing offline queries (details in Lemma 32)) *Let $H : \{0, 1\}^{\ell+n} \rightarrow \{0, 1\}^m$ and $G : \{0, 1\}^n \rightarrow \{0, 1\}^m$ be random oracles. Let A, B be oracle algorithms (which can share state), and assume that A makes at most q oracle queries to H , while B makes an arbitrary number of queries to H .*

Let $\tilde{B}(a)$ be the algorithm that results from $B(a)$ by the following change: Whenever B makes an oracle query $H(\tilde{a}\|x)$, \tilde{B} instead queries $H(\tilde{a}\|x)$ if $\tilde{a} \neq a$ and $G(x)$ if $\tilde{a} = a$.

Consider the following two games:

Game A: $a \xleftarrow{\$} \{0, 1\}^\ell$, $H \xleftarrow{\$} (\{0, 1\}^{\ell+n} \rightarrow \{0, 1\}^m)$, $A^H(\cdot)$, $b' \leftarrow B^H(a)$.

¹⁷For other timing models, the reduction described in the proof may incur a overhead, leading to a smaller T for TRE'.

Game B: $a \xleftarrow{\$} \{0, 1\}^\ell$, $H \xleftarrow{\$} (\{0, 1\}^{\ell+n} \rightarrow \{0, 1\}^m)$, $G \xleftarrow{\$} (\{0, 1\}^n \rightarrow \{0, 1\}^m)$,
 $A^H(\cdot)$, $b' \leftarrow \tilde{B}^{G,H}(a)$.

Then $|\Pr[b' = 1 : \text{Game A}] - \Pr[b' = 1 : \text{Game B}]| \leq q2^{-\ell/2+1}$.

This lemma can now immediately be used to show: If a cryptographic scheme \tilde{S} using a random oracle G is secure assuming the adversary never queries G during precomputation, then S , which queries $H(a\|x)$ instead of $G(x)$ for some random a , is secure even if the adversary queries H even during precomputation. Namely, if we let A^H encode the adversary's precomputation, and $B^H(a)$ the actual security game for S , then Game A encodes the security of S . And Game B encodes the security of \tilde{S} because in $\tilde{B}^{G,H}$, all queries that S makes to H are replaced by queries to G , i.e., we have effectively replaced S by \tilde{S} . Thus Lemma 2 allows to reduce the security of S to that of \tilde{S} .

Applying this generic proof plan to TREs, we get Theorem 6. But we stress that Lemma 2 is not limited to TREs, it can be used whenever we wish to exclude queries during an offline-phase (e.g., to get tighter bounds in a reduction).

Full proofs are given in Appendix F.

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 [RSW96] 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 10 (Iterated hashing (details in Definition 11)) *Let n and T be polynomially-bounded integers (depending on the security parameter), and assume that n is superlogarithmic. Let $H : \{0, 1\}^n \rightarrow \{0, 1\}^n$ 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 prove in Appendix G (Theorem 12) 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 5 and 6, we can transform it into a hiding TRE. This is plugged into RTRE_{ow} , to get a revocably one-way TRE, and using Theorem 5 again, we get a revocably hiding TRE in the random oracle model. (The resulting protocol is spelled out in Appendix H.)

An alternative construction is to plug TRE_{ih} (after transforming it using Theorems 5 and 6) 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 hashing¹⁸ 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 S ebastien Gambs for the suggesting the data retention application.

A Auxiliary lemmas

Lemma 3 (Detecting bit errors) *Fix integers $t, q, n \geq 1$. Let $x^0, x^1 \in \{0, 1\}^{q+n}$ such that $\omega(x^0) \geq t + 1$ or $\omega(x^1) \geq t + 1$. Consider the following process: Select uniformly $Q = \{Q_1, \dots, Q_q\} \in [q+n]_q$. (Recall, $[q+n]_q$ refers to q -size subsets of $\{1, \dots, q+n\}$, see page 4.) Select uniformly $B = B_1 \dots B_q \in \{0, 1\}^q$. Let $P(x) := \Pr[\nexists i \in \{1, \dots, q\} : x_{Q_i}^{B_i} = 1]$.*

Then $P(x) \leq 3\sqrt{q}(1 - \frac{q}{2(q+n)})^{t+1}$.

¹⁸E.g., $(a, H^{T+2}(a) \oplus m)$ for random a . Or the protocol resulting from applying Theorems 5 and 6 to Definition 10. That this is a realistic assumption for suitable hash functions is confirmed by our analysis in the random oracle model.

Proof. Obviously, $P(x)$ is maximized if $(\omega(x^0), \omega(x^1)) = (t+1, 0)$ or $(\omega(x^0), \omega(x^1)) = (0, t+1)$. Without loss of generality we assume $\omega(x^0) = 0$ and $\omega(x^1) = t+1$.

Let $C_1, \dots, C_{q+n} \in \{0, 1\}$ be independently uniformly distributed. Then $P(x) = \Pr[\#i : x_{Q_i}^{C_{Q_i}} = 1]$. (Because (Q, B_1, \dots, B_q) has the same distribution as $(Q, C_{Q_1}, \dots, C_{Q_n})$.)

Let $I := \{i : x_i^1 = 1\}$. Then, $\exists i : x_{Q_i}^{C_{Q_i}} = 1$ iff $\exists j \in I : C_j = 1 \wedge j \in Q$. Hence $P(x) = \Pr[\#j \in I : C_j = 1 \wedge j \in Q]$.

Let R_1, \dots, R_{q+n} be independently Bernoulli-distributed with $\Pr[R_i = 1] = q/(q+n)$. Let $R := \{j : R_j = 1\}$. (I.e., each j is in R with probability $q/(q+n)$.) Let $Z_j := C_j R_j$. Note that conditioned on $|R| = q$, R has the same distribution as Q . Hence $P(x) = \Pr[\#j \in I : C_j = 1 \wedge j \in R \mid |R| = q] = \Pr[\forall j \in I : Z_j = 0 \mid |R| = q]$.

We proceed to lower bound $\Pr[|R| = q]$. The Sterling formula [AS72, 6.1.38, p.257] states $\sqrt{2\pi}x^{x+1/2}e^{-x} < x! < \sqrt{2\pi}x^{x+1/2}e^{-x}e^{1/(12x)}$ for $x > 0$. Hence

$$\binom{q+n}{q} = \frac{(q+n)!}{n!q!} \geq \frac{\sqrt{2\pi}(q+n)^{q+n+1/2}e^{-q-n}}{\sqrt{2\pi}n^{n+1/2}e^{-n}e^{1/(12n)}\sqrt{2\pi}q^{q+1/2}e^{-q}e^{1/(12q)}} = \frac{(q+n)^{q+n+1/2}}{\sqrt{2\pi}n^{n+1/2}q^{q+1/2}e^{1/(12q)}e^{1/(12n)}}$$

Thus

$$\begin{aligned} \Pr[|R| = q] &= \binom{q+n}{q} \left(\frac{q}{q+n}\right)^q \left(1 - \frac{q}{q+n}\right)^n = \frac{(q+n)^{q+n+1/2}}{\sqrt{2\pi}n^{n+1/2}q^{q+1/2}e^{1/(12q)}e^{1/(12n)}} \frac{q^q}{(q+n)^q} \frac{n^n}{(q+n)^n} \\ &= \frac{(q+n)^{1/2}}{\sqrt{2\pi}n^{1/2}q^{1/2}e^{1/(12q)}e^{1/(12n)}} \geq \frac{1}{\sqrt{2\pi}q^{1/2}e^{1/12}e^{1/12}} \geq \frac{1}{3\sqrt{q}}. \end{aligned}$$

Hence $P(x) = \Pr[\forall j \in I : Z_j = 0 \wedge |R| = q] / \Pr[|R| = q] \leq 3\sqrt{q} \Pr[\forall j \in I : Z_j = 0]$.

Since the Z_j are independently Bernoulli-distributed with $\Pr[Z_j = 1] = q/2(q+n)$, we have $\Pr[\forall j \in I : Z_j = 0] = (1 - \frac{q}{2(q+n)})^{|I|}$. Thus $P(x) \leq 3\sqrt{q}(1 - \frac{q}{2(q+n)})^{t+1}$. \square

Lemma 4 (Operating on EPR pair halves) *For any A , we have $(A \otimes I_n)|\widetilde{0^n 0^n}\rangle = (I_n \otimes A^T)|\widetilde{0^n 0^n}\rangle$. (Here A^T denotes the transpose of A , not the Hermitean transpose A^\dagger . And recall that $|\widetilde{0^n 0^n}\rangle$ denotes n EPR pairs, see page 4.)*

Proof. Let $N := 2^n$ and $I := I_n$. $\delta_{xy} := I$ iff $x = y$ and 0 otherwise. For any x, y , we have

$$\begin{aligned} \langle x, y | (A \otimes I) |\widetilde{0^n 0^n}\rangle &= \sum_z \frac{1}{\sqrt{N}} \langle x, y | (A \otimes I) |z, z\rangle = \sum_z \frac{1}{\sqrt{N}} A_{xz} \delta_{yz} \\ &= \frac{1}{\sqrt{N}} A_{xy} = \frac{1}{\sqrt{N}} A_{yx}^T = \sum_z \frac{1}{\sqrt{N}} \delta_{xz} A_{yz}^T = \sum_z \frac{1}{\sqrt{N}} \langle x, y | (I \otimes A^T) |z, z\rangle \\ &= \langle x, y | (I \otimes A^T) |\widetilde{0^n 0^n}\rangle. \end{aligned}$$

Since $|x, y\rangle$ form an orthonormal basis, this implies that $(A \otimes I)|\widetilde{0^n 0^n}\rangle = (I \otimes A^T)|\widetilde{0^n 0^n}\rangle$. \square

Lemma 5 (Cauchy-Schwarz inequality, vector based) *Let α_i be complex numbers and $|\Psi_i\rangle$ finite-dimensional vectors. Then*

$$\left\| \sum_i \alpha_i |\Psi_i\rangle \right\|^2 \leq \left(\sum_i |\alpha_i|^2 \right) \cdot \left(\sum_i \|\Psi_i\|^2 \right).$$

Proof. Let x_{ij} denote the j -th component of $|\Psi_i\rangle$. Then

$$\begin{aligned} \left\| \sum_i \alpha_i |\Psi_i\rangle \right\|^2 &= \sum_j \left| \sum_i \alpha_i x_{ij} \right|^2 \stackrel{(*)}{\leq} \sum_j \left(\sum_i |\alpha_i|^2 \cdot \sum_i |x_{ij}|^2 \right) \\ &= \sum_i |\alpha_i|^2 \cdot \sum_i \sum_j |x_{ij}|^2 = \sum_i |\alpha_i|^2 \cdot \sum_i \|\Psi_i\|^2. \end{aligned}$$

Here $(*)$ uses the (usual) Cauchy-Schwarz-inequality. \square

Lemma 6 (Closeness to ideal states) *Let ρ be a mixed state, and let P be a projector. Let $1 - \varepsilon := \text{tr } P\rho$. (I.e., ε is the probability that measuring ρ with P fails.)*

Then there exists a mixed state ρ^{ideal} such that

- $\text{TD}(\rho, \rho^{ideal}) \leq \sqrt{\varepsilon}$.
- ρ^{ideal} is a mixture over $\text{im } P$. (I.e., $\rho = \sum_i p_i |\Psi_i\rangle\langle\Psi_i|$ for quantum states $|\Psi_i\rangle \in \text{im } P$ and $p_i \geq 0$ and $\sum p_i = 1$.)

Proof. We first consider the special case where $\rho = |\Psi\rangle\langle\Psi|$ for some quantum state $|\Psi\rangle$. (I.e., ρ is pure.) Let $F(\cdot, \cdot)$ denote the Fidelity between two quantum states. Let $\rho^{ideal} := |\Phi\rangle\langle\Phi|$ with $|\Phi\rangle := P|\Psi\rangle/\|P|\Psi\rangle\|$. Then

$$F(\rho, \rho^{ideal})^2 = |\langle\Psi|\Phi\rangle|^2 = \frac{|\langle\Psi|P|\Psi\rangle|^2}{\|P\Psi\|^2} = \frac{|\langle\Psi|P|\Psi\rangle|^2}{|\langle\Psi|P|\Psi\rangle|^2} = |\langle\Psi|P|\Psi\rangle| = \|P\Psi\|^2 = \text{tr } P\rho = 1 - \varepsilon.$$

Then we have

$$\text{TD}(\rho, \rho^{ideal}) \stackrel{(*)}{\leq} \sqrt{1 - F(\rho, \rho^{ideal})^2} = \sqrt{\varepsilon}.$$

Here $(*)$ uses that the trace distance is bounded in terms of the fidelity (e.g., [NC10, (9.101)]). Also, by construction, ρ^{ideal} is a mixture over $\text{im } P$. Thus the lemma holds for pure ρ .

Now consider the general case. Then $\rho = \sum_i p_i \rho_i$ for some pure mixed states ρ_i and for $\sum p_i = 1$, $p_i \geq 0$. Let $\varepsilon_i := 1 - \text{tr } P\rho_i$. Then $\varepsilon = 1 - \text{tr } \sum_i p_i P\rho_i = \sum_i p_i (1 - \text{tr } P\rho_i) = \sum_i p_i \varepsilon_i$. Since the lemma holds for pure states, we can apply it to get states ρ_i^{ideal} that are mixtures over $\text{im } P$ and such that $\text{TD}(\rho_i, \rho_i^{ideal}) \leq \sqrt{\varepsilon_i}$.

Let $\rho^{ideal} := \sum p_i \rho_i^{ideal}$. Then ρ^{ideal} is a mixture over $\text{im } P$ and we have

$$\text{TD}(\rho, \rho^{ideal}) = \text{TD}\left(\sum p_i \rho_i, \sum p_i \rho_i^{ideal}\right) \stackrel{(*)}{\leq} \sum p_i \text{TD}(\rho_i, \rho_i^{ideal}) \leq \sum p_i \sqrt{\varepsilon_i} \stackrel{(**)}{\leq} \sqrt{\sum p_i \varepsilon_i} = \sqrt{\varepsilon}.$$

Here $(*)$ follows from the convexity of the trace distance (e.g., [NC10, (9.50)]). And $(**)$ uses Jensen's inequality. \square

Lemma 7 Let $|\Psi_1\rangle, |\Psi_2\rangle$ be quantum states that can be written as $|\Psi_i\rangle = |\Psi_i^*\rangle + |\Phi^*\rangle$ where both $|\Psi_i^*\rangle$ are orthogonal to $|\Phi^*\rangle$.

Then $\text{TD}(|\Psi_1\rangle, |\Psi_2\rangle) \leq 2\| |\Psi_1^*\rangle \|$.

Proof. Let $\alpha := \| |\Psi_1^*\rangle \|$ and $\beta = \| |\Phi^*\rangle \|$. Since $|\Phi^*\rangle$ is orthogonal to $|\Psi_1^*\rangle$ and $|\Psi_1\rangle$ is a quantum state, $\alpha^2 + \beta^2 = \| |\Psi_1\rangle \|^2 = 1$. And since $|\Phi^*\rangle$ is orthogonal to $|\Psi_2^*\rangle$ and $|\Psi_2\rangle$ is a quantum state, $\| |\Psi_2^*\rangle \|^2 + \beta^2 = \| |\Psi_2\rangle \|^2 = 1$, hence $\| |\Psi_2^*\rangle \|^2 = \alpha$. Let F denote the fidelity between quantum states. Then $F(|\Psi_1\rangle, |\Psi_2\rangle) = |\langle\Psi_1|\Psi_2\rangle|$ by definition and we have

$$F(|\Psi_1\rangle, |\Psi_2\rangle) = |\langle\Psi_1^*|\Psi_2^*\rangle + \langle\Phi^*|\Phi^*\rangle| = |\langle\Psi_1^*|\Psi_2^*\rangle + \beta^2| \geq \beta^2 - |\langle\Psi_1^*|\Psi_2^*\rangle| \geq \beta^2 - \alpha^2 = 1 - 2\alpha^2.$$

By [NC10, Section 9.2.3, (9.97)], we have $\text{TD}(|\Psi_1\rangle, |\Psi_2\rangle) = \sqrt{1 - F(|\Psi_1\rangle, |\Psi_2\rangle)^2}$. Hence

$$\text{TD}(|\Psi_1\rangle, |\Psi_2\rangle) \leq \sqrt{1 - (1 - 2\alpha^2)^2} = \sqrt{4\alpha^2(1 - \alpha^2)} = \sqrt{4\alpha^2\beta^2} = 2\alpha\beta \leq 2\alpha.$$

(Notice that this is almost tight for $\beta = \| |\Phi^*\rangle \| \approx 1$. If $|\Psi_1^*\rangle = |\Psi_1\rangle$, all inequalities except the last one ($2\alpha\beta \leq 2\alpha$) are equalities.) \square

B Full proof: revocably one-way timed-release encryptions

In this appendix, we give the full security proof for the protocol RTRE_{ow} from Section 3, Definition 7. We first start with the proof that RTRE_{ow} is revocably one-way. And below (page 10) we show that it is (non-revocably) hiding.

We restate Theorem 1

Theorem 7 (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 (formally defined as P_B^- on page 20 below), a measurement whether two n -qubit registers are in a $|0^n 0^n\rangle$ state up to t phase flips and t bit flips (for a given t ; formally defined as P_t^{EPR} on page 20 below), and one NOT- and one AND-gate.

Assume that the protocol parameter n is superlogarithmic.

The protocol RTRE_{ow} from Definition 7 is $(T - \delta_T^{ow})$ -revocably one-way, even if A_2 is unlimited (i.e., after revocation, security holds information-theoretically).

A concrete security bound is given at the end of the proof, page 25.

The rest of this section will be devoted to proving this theorem.

For the rest of this section, assume an adversary (A_1, A_2) where A_1 is sequential-polynomial-time and $(T - \delta_T^{ow})$ -time and A_2 is sequential-polynomial-time. To show Theorem 7, we need to show that the probability of the adversary winning the game from Definition 6 is negligible.

Some measurements. We first define two measurement operators that will be used in this proof:

The projector P_t^{EPR} measures whether a $2n$ -qubit state is an EPR state with at most t phase and at most t bit flips. Formally (recall the Bell-basis notation $|\widetilde{fe}\rangle$ from page 4):

$$P_t^{EPR} := \sum_{\substack{f, e \in \{0,1\}^n \\ \omega(f), \omega(e) \leq t}} |\widetilde{fe}\rangle\langle\widetilde{fe}|.$$

Given a basis $B \in \{0,1\}^n$, the projector P_B^- measures whether two n -qubit systems would give the same outcome when measured in basis B . Formally,

$$P_B^- := \sum_{x \in \{0,1\}^n} |x, x\rangle_B \langle x, x|_B.$$

Sequence of games. We now proceed to define a number of games and to show the relation between the attack probabilities in these games. From this we finally deduce the security of our protocol. X and Y refer to n -bit quantum registers.

Game 1 (Original game)

- (a) Run $A_0()$.
- (b) $m \xleftarrow{\$} \{0,1\}^n$, $p \xleftarrow{\$} \{0,1\}^n$, $B \xleftarrow{\$} \{0,1\}^n$.
- (c) $V_0 \leftarrow \text{TRE}_0(B, p)$.
- (d) $X \leftarrow |m \oplus p\rangle_B$.
- (e) Run $A_1(X, V_0)$. (We pass the quantum register X to A_1 which means that A_1 has read-write access to it.)
- (f) Measure X in basis B ; outcome γ .
- (g) If $m \oplus p = \gamma$, $ok := 1$. Else $ok := 0$.
- (h) $m' \leftarrow A_2()$.

Since Game 1 is the game from Definition 6 (with the definition of RTRE_{ow} inlined), it suffices to show that $\Pr[m = m' \wedge ok = 1 : \text{Game 1}]$ is negligible.

The first game removes p from some steps, this is more of a cosmetic change that makes notation easier later.

Game 2 (One-time-pad removed)

- (a) Run $A_0()$.
- (b) $m \xleftarrow{\$} \{0,1\}^n$, $p \xleftarrow{\$} \{0,1\}^n$, $B \xleftarrow{\$} \{0,1\}^n$.
- (c) $V_0 \leftarrow \text{TRE}_0(B, p)$.
- (d) $X \leftarrow |m\rangle_B$.
- (e) Run $A_1(X, V_0)$.
- (f) Measure X in basis B ; outcome γ .
- (g) If $m = \gamma$, $ok := 1$. Else $ok := 0$.
- (h) $m' \leftarrow A_2() \oplus p$.

Lemma 8 (Game 1 vs. Game 2) $\Pr[m' = m \wedge ok = 1 : \text{Game 1}] = \Pr[m' = m \wedge ok = 1 : \text{Game 2}]$.

Proof. Consider first an intermediate game G which is like Game 2, except that the last step is still “ $m' \xleftarrow{\$} A_2()$ ”. The difference between G and Game 1 is then that m is consistently replaced by $m \oplus p$. Since $m \oplus p$ has the same distribution as m for $m \xleftarrow{\$} \{0,1\}^n$, it follows that $\Pr[m' = m \wedge ok = 1 : \text{Game 1}] = \Pr[m' = m \oplus p \wedge ok = 1 : G]$.

Furthermore, G differs from Game 2 only in the fact that we add p to m' in the last step. Hence $\Pr[m' = m \oplus p \wedge ok = 1 : G] = \Pr[m' \oplus p = m \oplus p \wedge ok = 1 : \text{Game 2}] = \Pr[m' = m \wedge ok = 1 : \text{Game 2}]$.

□

Game 3 (Using EPR states)

- (a) Run $A_0()$.
- (b) $m \xleftarrow{\$} \{0,1\}^n$, $p \xleftarrow{\$} \{0,1\}^n$, $B \xleftarrow{\$} \{0,1\}^n$.
- (c) $V_0 \leftarrow \text{TRE}_0(B,p)$.
- (d) Initialize XY as $|\widetilde{0^n 0^n}\rangle$.
- (e) Run $A_1(X, V_0)$.
- (f) Measure X in basis B ; outcome γ .
- (g) Measure Y in basis B , outcome m .
- (h) If $m = \gamma$, $ok := 1$. Else $ok := 0$.
- (i) $m' \leftarrow A_2() \oplus p$.

Lemma 9 (Game 2 vs. Game 3) $\Pr[m' = m \wedge ok = 1 : \text{Game 2}] = \Pr[m' = m \wedge ok = 1 : \text{Game 3}]$.

Proof. It is sufficient to show that for any basis B , “ $m \xleftarrow{\$} \{0,1\}^n; X \leftarrow |m\rangle_B$ ” and “ $XY \leftarrow |\widetilde{0^n 0^n}\rangle$; measure Y in basis B , outcome m ” are equivalent. I.e., we need to show that in the second case, m is uniformly distributed, and the state in X is $|m\rangle_B$.

The probability of measuring m is $\|\Psi_m\|^2$ and the state of XY after measuring m is $|\Psi_m\rangle/\|\Psi_m\|$ where $|\Psi_m\rangle := (H^B|m\rangle\langle m|H^B \otimes I_n)|\widetilde{0^n 0^n}\rangle$. We have

$$\begin{aligned}
|\Psi_m\rangle &= (H^B|m\rangle\langle m|H^B \otimes I_n)|\widetilde{0^n 0^n}\rangle \\
&= (H^B \otimes I_n)(|m\rangle\langle m| \otimes I_n)(H^B \otimes I_n)|\widetilde{0^n 0^n}\rangle \\
&\stackrel{(*)}{=} \|(H^B \otimes I_n)(|m\rangle\langle m| \otimes I_n)(I_n \otimes H^B)|\widetilde{0^n 0^n}\rangle\| \\
&= \sum_{\tilde{m}} 2^{-n/2} (H^B|m\rangle\langle m|\tilde{m}\rangle) \otimes (H^B|\tilde{m}\rangle) \\
&= 2^{-n/2} (H^B|m\rangle) \otimes (H^B|m\rangle) = 2^{-n/2} |m\rangle_B \otimes |m\rangle_B.
\end{aligned}$$

Here (*) uses Lemma 4 and the fact that H is symmetric.

Hence the probability of measuring m is $\|\Psi_m\|^2 = 2^{-n}$ and the state of XY is then $|m\rangle_B \otimes |m\rangle_B$. Thus, after tracing out Y , we have $|m\rangle_B$ in X . The two games are therefore equivalent. \square

Game 4 (Changed revocation test)

- (a) Run $A_0()$.
- (b) $p \xleftarrow{\$} \{0,1\}^n$, $B \xleftarrow{\$} \{0,1\}^n$.
- (c) $V_0 \leftarrow \text{TRE}_0(B,p)$.
- (d) Initialize XY as $|\widetilde{0^n 0^n}\rangle$.
- (e) Run $A_1(X, V_0)$.
- (f) Measure XY using $P_B^\#$; outcome ok .
- (g) ~~Measure X in basis B ; outcome γ .~~
- (h) Measure Y in basis B , outcome m .
- (i) ~~If $m = \gamma$, $ok := 1$. Else $ok := 0$.~~
- (j) $m' \leftarrow A_2() \oplus p$.

Lemma 10 (Game 3 vs. Game 4) $\Pr[m' = m \wedge ok = 1 : \text{Game 3}] = \Pr[m' = m \wedge ok = 1 : \text{Game 4}]$.

Proof. Consider first an intermediate game G , which is like Game 4, except that line (g) is not removed. Since X is not used after (g), we have $\Pr[m' = m \wedge ok = 1 : \text{Game 4}] = \Pr[m' = m \wedge ok = 1 : G]$.

Consider further a game G' which is like G , except that (f) is moved after (h). Then $\Pr[m' = m \wedge ok = 1 : G] = \Pr[m' = m \wedge ok = 1 : G']$ because $P_B^\#$ and measurements in basis B commute (they are diagonal in the same basis).

Finally, after the measurements of X, Y in basis B , we have that X, Y are in state $|\gamma\rangle|m\rangle$. Thus $ok = 1$ iff $m = \gamma$. Hence, if we replace the measurement using $P_B^\#$ with “if $m = \gamma$, $ok := 1$, else $ok := 0$ ”, we get Game 3 and have $\Pr[m' = m \wedge ok = 1 : G'] = \Pr[m' = m \wedge ok = 1 : \text{Game 3}]$. \square

In the following, let t be an arbitrary integer with $0 \leq t \leq n$. (In the end, we will fix $t := \sqrt{n}$.)

Game 5 (Testing the state)

- (a) Run $A_0()$.

- (b) $p \stackrel{s}{\leftarrow} \{0, 1\}^n, B \stackrel{s}{\leftarrow} \{0, 1\}^n$.
- (c) $V_0 \leftarrow \text{TRE}_0(B, p)$.
- (d) Initialize XY as $|\widetilde{0^n 0^n}\rangle$.
- (e) Run $A_1(X, V_0)$.
- (f) Measure XY using P_B^- ; outcome ok .
- (g) Measure XY using P_t^{EPR} ; outcome is $isEPR$.
- (h) Measure Y in basis B ; outcome m .
- (i) $m' \leftarrow A_2(\cdot) \oplus p$.

Lemma 11 (Uncertainty relation for t -error EPR states) Let X, Y be n -bit quantum registers and Z a quantum register. Let M be a projective measurement on Z . Let $B \in \{0, 1\}^n$. Let $|\Psi\rangle$ be a state of XYZ that is in the image of $P_t^{EPR} \otimes I_Z$ (here I_Z is the identity on Z). Let m be the outcome of measuring Y in basis B . Let m' be the outcome of applying M to Z . Then $\Pr[m = m'] \leq 2^{-n}(n+1)^{2t}$.

Proof. Since the states $|\widetilde{fe}\rangle$ form a basis for the state space of XY , we can write $|\Psi\rangle = \sum_{fe} \alpha_{fe} |\widetilde{fe}\rangle \otimes |\Psi_{fe}\rangle$ for some quantum states $|\Psi_{fe}\rangle$ living in Z . Let $T := \{fe : \omega(f), \omega(e) \leq t\}$. Since $|\Psi\rangle = P_t^{EPR} |\Psi\rangle$, we have $\alpha_{fe} = 0$ for $fe \notin T$. Thus $|\Psi\rangle = \sum_{fe \in T} \alpha_{fe} |\widetilde{fe}\rangle \otimes |\Psi_{fe}\rangle$ with $\sum_{fe \in T} |\alpha_{fe}|^2 = 1$.

For any m' , let $P_{m'}$ be the projector for outcome m' in the measurement M . Thus m, m' is the result of applying the measurement $\{I_n \otimes H^B |m\rangle\langle m| H^B \otimes P_{m'}\}_{mm'}$ to $|\Psi\rangle$. Hence

$$\begin{aligned}
\Pr[m = m'] &= \sum_m \|(I_n \otimes H^B |m\rangle\langle m| H^B \otimes P_m) |\Psi\rangle\|^2 \\
&= \sum_m \left\| \sum_{fe \in T} \alpha_{fe} (I_n \otimes H^B |m\rangle\langle m| H^B) |\widetilde{fe}\rangle \otimes P_m |\Psi_{fe}\rangle \right\|^2 \\
&\stackrel{(*)}{\leq} \sum_m \left(\sum_{fe \in T} |\alpha_{fe}|^2 \cdot \sum_{fe \in T} \|(I_n \otimes H^B |m\rangle\langle m| H^B) |\widetilde{fe}\rangle \otimes P_m |\Psi_{fe}\rangle\|^2 \right) \\
&= \sum_m \left(\underbrace{\sum_{fe \in T} |\alpha_{fe}|^2}_{=1} \cdot \sum_{fe \in T} \underbrace{\|(I_n \otimes H^B |m\rangle\langle m| H^B) |\widetilde{fe}\rangle\|^2}_{=2^{-n}} \cdot \|P_m |\Psi_{fe}\rangle\|^2 \right) \\
&= 2^{-n} \sum_{fe \in T} \underbrace{\sum_m \|P_m |\Psi_{fe}\rangle\|^2}_{=1} = 2^{-n} |T|. \tag{2}
\end{aligned}$$

Here $(*)$ uses Lemma 5 (vector-based variant of the Cauchy-Schwarz-inequality).

And $(**)$ uses

$$\begin{aligned}
\|(I_n \otimes H^B |m\rangle\langle m| H^B) |\widetilde{fe}\rangle\| &= \|(Z^f X^e \otimes H^B |m\rangle\langle m| H^B) |\widetilde{0^n 0^n}\rangle\| \\
&\stackrel{\text{Lemma 4}}{=} \|(Z^f X^e H^B \otimes H^B |m\rangle\langle m|) |\widetilde{0^n 0^n}\rangle\| = \|(Z^f X^e H^B \otimes H^B) \cdot 2^{-n/2} |m\rangle\langle m|\| = 2^{-n/2}.
\end{aligned}$$

We now bound $|T|$. Notice that any e with $\omega(e) \leq t$ can be specified by giving t indices $i \in \{0, \dots, n\}$ with $e_i = 1$ (where $i = 0$ for unused indices when $\omega(e) < t$). Thus there are at most $(n+1)^t$ such e . Hence $|T| \leq (n+1)^{2t}$.

Summarizing, we have

$$\Pr[m = m'] \stackrel{(2)}{\leq} 2^{-n} |T| \leq 2^{-n} (n+1)^{2t}. \quad \square$$

Lemma 12 (Game 4 vs. Game 5) $\Pr[m' = m \wedge ok = 1 : \text{Game 4}] \leq \sqrt{\Pr[isEPR = 0 \wedge ok = 1 : \text{Game 5}] + 2^{-n}(n+1)^{2t}}$.

Proof. For $b \in \{0, 1\}^n$, let ρ_b denote the state of the system after measuring $ok = 1$ in the case that $B = b$ in Game 5. (I.e., the post-measurement-state conditioned on having chosen $B = b$ and on outcome $ok = 1$.) Then

$$\Pr[isEPR = 1 \wedge ok = 1 : \text{Game 5}] = \sum_b \text{tr} P_t^{EPR} \rho_b \cdot \Pr[B = b \wedge ok = 1 : \text{Game 5}]. \tag{3}$$

Let $\hat{\rho}_b$ be the state of the system after measuring $ok = 1$ in the case $B = b$ in Game 4. Since Games 4 and 5 are identical up to this point, $\rho_b = \hat{\rho}_b$.

By Lemma 6 there is a state ρ'_b such that $\text{TD}(\rho_b, \rho'_b) \leq \sqrt{1 - \text{tr}(P_t^{\text{EPR}} \rho_b)}$ and such that $\rho'_b = \sum_i p_i |\Psi_i\rangle\langle\Psi_i|$ where each $|\Psi_i\rangle$ is in the image of P_t^{EPR} .

In the special case $\rho'_b = |\Psi_i\rangle\langle\Psi_i|$ for some such $|\Psi_i\rangle$, Lemma 11 implies that $\Pr[m = m' : \text{Game 4}] \leq \varepsilon := 2^{-n}(n+1)^{2t}$. Here *Game 4'* is the following game: “Initialize XYZ with ρ'_b . Measure Y in basis b , outcome m . $m' \leftarrow A_2(Z)$. (Z stands for the quantum register holding the adversary’s state.)”

Since ρ'_b is a mixture of such states $|\Psi_i\rangle\langle\Psi_i|$, $\Pr[m = m' : \text{Game 4}] \leq \varepsilon$ follows also in the general case by averaging. Since $\text{TD}(\hat{\rho}_b, \rho'_b) \leq \sqrt{1 - \text{tr}(P_t^{\text{EPR}} \rho_b)}$, it follows that $\Pr[m = m' | B = b \wedge ok = 1 : \text{Game 4}] \leq \varepsilon + \sqrt{1 - \text{tr}(P_t^{\text{EPR}} \rho_b)}$.

We abbreviate $q_b := \Pr[B = b \wedge ok = 1 : \text{Game 4}] = \Pr[B = b \wedge ok = 1 : \text{Game 5}]$ (equality holds because the two games are identical up to the measurement of ok). Then

$$\begin{aligned}
& \Pr[m = m' \wedge ok = 1 : \text{Game 4}] \\
&= \sum_b q_b \Pr[m = m' | B = b \wedge ok = 1 : \text{Game 4}] \\
&\leq \sum_b q_b \left(\varepsilon + \sqrt{1 - \text{tr}(P_t^{\text{EPR}} \rho_b)} \right) \\
&\leq \left(\sum_b q_b \right) \cdot \left(\varepsilon + \sqrt{1 - \frac{\sum_b q_b \text{tr}(P_t^{\text{EPR}} \rho_b)}{\sum_b q_b}} \right) \quad (\text{Jensen's inequality}) \\
&= \left(\sum_b q_b \right) \varepsilon + \sqrt{\left(\sum_b q_b \right) \cdot \left(\left(\sum_b q_b \right) - \left(\sum_b q_b \text{tr}(P_t^{\text{EPR}} \rho_b) \right) \right)} \\
&\leq \varepsilon + \sqrt{\Pr[ok = 1 : \text{Game 5}] - \sum_b q_b \text{tr}(P_t^{\text{EPR}} \rho_b)} \quad (\text{using } \sum_b q_b = \Pr[ok = 1 : \text{Game 5}] \leq 1) \\
&\stackrel{(3)}{=} \varepsilon + \sqrt{\Pr[ok = 1 : \text{Game 5}] - \Pr[isEPR = 1 \wedge ok = 1 : \text{Game 5}]} \\
&= \varepsilon + \sqrt{\Pr[isEPR = 0 \wedge ok = 1 : \text{Game 5}]} \quad \square
\end{aligned}$$

Game 6 (Using fake timed-release encryption)

- (a) Run $A_0()$.
- (b) $p \xleftarrow{\$} \{0, 1\}^n$, $B \xleftarrow{\$} \{0, 1\}^n$.
- (c) $\hat{B} \leftarrow \{0, 1\}^n$. $V_0 \leftarrow \text{TRE}_0(\hat{B}, p)$.
- (d) Initialize XY as $|\widehat{0^n 0^n}\rangle$.
- (e) Run $A_1(X, V_0)$.
- (f) $B \xleftarrow{\$} \{0, 1\}^n$.
- (g) Measure XY using P_B^- ; outcome ok .
- (h) Measure XY using P_t^{EPR} ; outcome $isEPR$.

Lemma 13 (Game 5 vs. Game 6) $\Pr[isEPR = 0 \wedge ok = 1 : \text{Game 5}] \leq \Pr[isEPR = 0 \wedge ok = 1 : \text{Game 6}] + \mu$ for some negligible μ .

Proof. First, consider an intermediate game G' defined like Game 6, except that B is chosen and XY initialized before the computation of V_0 . Let G be the same game, except that V_0 is chosen as $V_0 \leftarrow \text{TRE}_0(B, p)$.

Then we immediately see that $\Pr[isEPR = 0 \wedge ok = 1 : G] = \Pr[isEPR = 0 \wedge ok = 1 : \text{Game 5}]$ and $\Pr[isEPR = 0 \wedge ok = 1 : G'] = \Pr[isEPR = 0 \wedge ok = 1 : \text{Game 6}]$ because only operations that operate on distinct variables/quantum registers are moved around.

Furthermore, in game G , after computing V_0 , we have a measurement using P_B^- , a measurement using P_t^{EPR} , an invocation of the $(T - \delta_T^{ow})$ -time adversary A_1 , and a NOT- and an AND-gate (for evaluating $isEPR = 0 \wedge ok = 1$). Together, these steps take time at most T (by definition of δ_T^{ow}). Furthermore, all steps before and after $V_0 \xleftarrow{\$} \text{TRE}_0(B, p)$ run in sequential-polynomial-time.

Since TRE_0 is T -hiding, replacing $\text{TRE}_0(B, p)$ by $\text{TRE}_0(\hat{B}, p)$ thus only negligibly changes $\Pr[isEPR = 0 \wedge ok = 1]$.

Hence $\Pr[isEPR = 0 \wedge ok = 1 : G] \leq \Pr[isEPR = 0 \wedge ok = 1 : G'] + \mu$ for some negligible μ . \square

Lemma 14 (Equality measurements on Bell-basis states) $P_B^-|\widetilde{f}e\rangle = |\widetilde{f}e\rangle$ iff for all i we have $(B_i = 0 \wedge f_i = 0) \vee (B_i = 1 \wedge e_i = 0)$. And $P_B^-|\widetilde{f}e\rangle = 0$ otherwise.

Proof. For the case that $|e| = |f| = 1$, it follows from the following case distinction:

B	e	f	$P_B^- \widetilde{f}e\rangle$	B	e	f	$P_B^- \widetilde{f}e\rangle$
0 (comp. basis)	0	0	$ \widetilde{00}\rangle$	1 (diag. basis)	0	0	$ \widetilde{00}\rangle$
0	0	1	0	1	0	1	$ \widetilde{01}\rangle$
0	1	0	$ \widetilde{10}\rangle$	1	1	0	0
0	1	1	0	1	1	1	0

For checking the four cases with $B = 1$, it is convenient to use that $|\widetilde{0f}\rangle = \frac{1}{\sqrt{2}}(|++\rangle \pm |--\rangle)$ and $|\widetilde{1f}\rangle = \frac{1}{\sqrt{2}}(|-+\rangle \pm |+-\rangle)$ for $f = 0, 1$.

The general case follows from the fact that $P_B^- = P_{B_1}^- \otimes \cdots \otimes P_{B_n}^-$ and $|\widetilde{f}e\rangle = |e_1 f_1\rangle \otimes \cdots \otimes |e_n f_n\rangle$ (up to reordering of qubits). \square

Lemma 15 (Game 6 is secure) $\Pr[isEPR = 0 \wedge ok = 1 : \text{Game 6}] \leq 2^{-t-1}$.

Proof. Observe that $\Pr[isEPR = 0 \wedge ok = 1 : \text{Game 6}] = \sum_B 2^{-n} \text{tr} \overline{P_t^{EPR}} P_B^- \rho$ where ρ is the state after the invocation of A_1 , and $\overline{P_t^{EPR}} := 1 - P_t^{EPR}$.

Before bounding $\sum_B 2^{-n} \text{tr} \overline{P_t^{EPR}} P_B^- \rho$, we show for any $f, e \in \{0, 1\}^n$ that $p_{fe} := \sum_B 2^{-n} \text{tr} \overline{P_t^{EPR}} P_B^- |\widetilde{f}e\rangle \langle \widetilde{f}e| \leq 2^{-t-1}$. We distinguish two cases: $\omega(e), \omega(f) \leq t$ and $\max(\omega(f), \omega(e)) \geq t + 1$. If $\omega(f), \omega(e) \leq t$, by Lemma 14, for any B either $P_B^-|\widetilde{f}e\rangle = 0$ or $P_B^-|\widetilde{f}e\rangle = |\widetilde{f}e\rangle$ depending on B . Since $P_t^{EPR}|\widetilde{f}e\rangle = |\widetilde{f}e\rangle$, it follows that $\overline{P_t^{EPR}} P_B^-|\widetilde{f}e\rangle = 0$ and hence $p_{fe} = 0$. If $\max(\omega(f), \omega(e)) \geq t + 1$, then by Lemma 14 there are at most $q := 2^n/2^{t+1}$ different values of B such that $P_B^-|\widetilde{f}e\rangle \neq 0$ (this bound is tight iff $e = 0^n$ and $\omega(f) = t + 1$ or vice versa). Hence $p_{fe} \leq q \cdot 2^{-n} = 2^{-t-1}$. Thus, in all cases, $p_{fe} \leq 2^{-t-1}$.

We abbreviate $P_{fe} := |\widetilde{f}e\rangle \langle \widetilde{f}e|$ and $\alpha_{fe} := \langle \widetilde{f}e | \rho | \widetilde{f}e \rangle$. We proceed:

$$\begin{aligned}
& \Pr[isEPR = 0 \wedge ok = 1 : \text{Game 6}] \\
&= \sum_B 2^{-n} \text{tr} \overline{P_t^{EPR}} P_B^- \rho \\
&\stackrel{(*)}{=} \sum_B 2^{-n} \text{tr} \left(\left(\sum_{fe} P_{fe} \right) \overline{P_t^{EPR}} P_B^- \rho \right) \\
&= \sum_{Bef} 2^{-n} \text{tr} P_{fe} \overline{P_t^{EPR}} P_B^- \rho \\
&\stackrel{(**)}{=} \sum_{Bef} 2^{-n} \text{tr} P_{fe} \overline{P_t^{EPR}} P_B^- \rho P_{fe} \\
&\stackrel{(***)}{=} \sum_{Bef} 2^{-n} \text{tr} \overline{P_t^{EPR}} P_B^- (P_{fe} \rho P_{fe}) \\
&= \sum_{fe} \left(\alpha_{fe} \sum_B 2^{-n} \text{tr} \overline{P_t^{EPR}} P_B^- |\widetilde{f}e\rangle \langle \widetilde{f}e| \right) \\
&= \sum_{fe} \alpha_{fe} p_{fe} \leq \sum_{fe} \alpha_{fe} 2^{-t-1} = \text{tr} \rho \cdot 2^{-t-1} = 2^{-t-1}.
\end{aligned}$$

Here (*) uses that $\sum_{fe} P_{fe} = 1$ since $|\widetilde{f}e\rangle$ form a basis.

And (**) uses that $P_{fe} = P_{fe} \cdot P_{fe}$ and the circularity of the trace.

And (***) uses that P_t^{EPR} , P_B^- , and P_{fe} commute because they are all diagonal in the Bell basis. (This is immediate from the definition for P_t^{EPR} and P_{fe} , and for P_B^- it follows from Lemma 14.) \square

We can now finally prove the revocable onewayness of RTRE_{ow} :

Proof of Theorem 7. We have

$$\begin{aligned}
& \Pr[m' = m \wedge ok = 1 : \text{Game 1}] \\
&= \Pr[m' = m \wedge ok = 1 : \text{Game 4}] && \text{(Lemmas 8, 9, and 10)} \\
&\leq \sqrt{\Pr[isEPR = 0 \wedge ok = 1 : \text{Game 5}]} + 2^{-n}(n+1)^{2t} && \text{(Lemma 12)} \\
&\leq \sqrt{\Pr[isEPR = 0 \wedge ok = 1 : \text{Game 6}]} + \mu + 2^{-n}(n+1)^{2t} && \text{(Lemma 13; } \mu \text{ negligible)} \\
&\leq \sqrt{2^{-t-1} + \mu} + 2^{-n}(n+1)^{2t} =: \nu && \text{(Lemma 15)} \tag{4}
\end{aligned}$$

So far, our calculation was for arbitrary t . If we fix $t := \sqrt{n}$, then 2^{-t-1} and $2^{-n}(n+1)^{2t}$ are negligible, and hence ν is negligible.

Furthermore, the lemmas above hold for any adversary sequential-polynomial-time adversary (A_1, A_2) with A_1 being $(T - \delta_T^{ow})$ -time. And $\Pr[m' = m \wedge ok = 1 : \text{Game 1}]$ is the probability that (A_1, A_2) wins the game from Definition 6 (revocable one-wayness).

Thus RTRE_{ow} is revocably one-way.

Note that (4) also tells us the concrete security of RTRE_{ow} . Namely, when μ is the advantage of an adversary against TRE_0 (that runs only a small additive amount longer than the original adversary (A_0, A_1, A_2)); it consists of the code in Game 6), then $\max_t(\sqrt{2^{-t-1} + \mu} + 2^{-n}(n+1)^{2t})$ bounds the advantage of (A_0, A_1, A_2) against RTRE_{ow} . \square

Hiding. Note that revocable one-wayness does not immediately imply one-wayness or hiding. However, due to the one-time-pad p used in RTRE_{ow} , it is easy to show that RTRE_{ow} is hiding:

Theorem 8 (RTRE_{ow} is hiding) *The protocol RTRE_{ow} from Definition 7 is T-hiding. (A concrete security bound is given at the end of the proof.)*

Proof. We need to show that for an adversary (A_0, A_1) such that A_0 is sequential-polynomial-time and A_1 is sequential-polynomial-time and T -time, we have that $|\Pr[b' = 1 : \text{Game 1}(0)] - \Pr[b' = 1 : \text{Game 1}(1)]|$ is negligible. Here $\text{Game 1}(b)$ denotes Game 1 running with parameter b , and Game 1 is defined as follows:

Game 1 (Original protocol)

- (a) In this game, $b \in \{0, 1\}$ is a parameter of the game.
- (b) $(m_0, m_1) \leftarrow A_0()$.
- (c) $p \xleftarrow{\$} \{0, 1\}^n$, $B \xleftarrow{\$} \{0, 1\}^n$.
- (d) $V_0 \leftarrow \text{TRE}_0(B, p)$.
- (e) $X \leftarrow |m_b \oplus p\rangle_B$.
- (f) $b' \leftarrow A_1(X, V_0)$.

Since TRE_0 is T -hiding, and A_1 is T -time, and A_0, A_1 are sequential-polynomial-time, we can replace the arguments of TRE_0 by different ones.

Game 2 (Fake timed-release encryption)

- (a) In this game, $b \in \{0, 1\}$ is a parameter of the game.
- (b) $(m_0, m_1) \leftarrow A_0()$.
- (c) $p \xleftarrow{\$} \{0, 1\}^n$, $\tilde{p} \xleftarrow{\$} \{0, 1\}^n$, $B \xleftarrow{\$} \{0, 1\}^n$.
- (d) $V_0 \leftarrow \text{TRE}_0(B, \tilde{p})$.
- (e) $X \leftarrow |m_b \oplus p\rangle_B$.
- (f) $b' \leftarrow A(X, V_0)$.

We then have that $|\Pr[b' = 1 : \text{Game 1}(b)] - \Pr[b' = 1 : \text{Game 2}(b)]|$ is negligible for $b \in \{0, 1\}$.

Game 3 (Removing m)

- (a) In this game, $b \in \{0, 1\}$ is a parameter of the game.
- (b) $(m_0, m_1) \leftarrow A_0()$.
- (c) $p \xleftarrow{\$} \{0, 1\}^n$, $\tilde{p} \xleftarrow{\$} \{0, 1\}^n$, $B \xleftarrow{\$} \{0, 1\}^n$.
- (d) $V_0 \leftarrow \text{TRE}_0(B, \tilde{p})$.

- (e) $X \leftarrow |p\rangle_B$.
(f) $b' \leftarrow A(X, V_0)$.

In this game, we have substituted p by $p \oplus m_b$. For $p \stackrel{\$}{\leftarrow} \{0, 1\}^n$, both p and $p \oplus m_b$ have the same distribution. Hence $\Pr[b' = 1 : \text{Game } 2(b)] = \Pr[b' = 1 : \text{Game } 3(b)]$ for $b \in \{0, 1\}$.

Finally, since b is never used in Game 3, we have $\Pr[b' = 1 : \text{Game } 3(0)] = \Pr[b' = 1 : \text{Game } 3(1)]$.

Combining all equations, we get that $|\Pr[b' = 1 : \text{Game } 1(0)] - \Pr[b' = 1 : \text{Game } 1(1)]|$ is negligible.

Note that this also tells us the concrete security of RTRE_{ow} . Namely, when μ is the advantage of an adversary against TRE_0 (that runs only a small additive amount longer than the original adversary (A_0, A_1) ; it consists of the code in Game 2), then μ also bounds the advantage against RTRE_{ow} . \square

C CSS codes – recap and properties

We recall the definition of CSS codes and prove some properties that we will need in the following. For more information, see [CS96, Ste96] or the textbook [NC10, Section 10.4.2].

A CSS code with parameters n, k_1, k_2, t consists of two classical linear binary codes, namely an $[n, k_1]$ code C_1 ¹⁹ and an $[n, k_2]$ code C_2 such that $C_2 \subseteq C_1$ and both C_1 and C_2^\perp can correct up to t errors. We require that the parity check matrices of C_1, C_2 are computable in polynomial time, and that error correction can be performed in polynomial time. (Here we assume an asymptotic setting in which C_1, C_2 are defined for every security parameter.)

Given two binary codes $C \subseteq D$, with slight abuse of notation, D/C denotes a representative system of the quotient D/C . More precisely, we assume an idempotent linear polynomial-time computable operation “mod C ” on $\{0, 1\}^n$ such that we have that $x \bmod C = x' \bmod C$ iff $x - x' \in C$ and for all codes $D \supseteq C$ that $x \in D \implies x \bmod C \in D$ and that $x \bmod D \bmod C = x \bmod D$. (Such an operation can always be found, e.g., $x \bmod C := H^T(HH^T)^{-1}Hx$ if H is the parity check matrix of C and H^T its transpose. Note that HH^T is invertible because we can assume H to be of full rank.) We then let $D/C := \{x \bmod C : x \in D\}$.

Let $|\xi_{xuv}\rangle := \frac{1}{\sqrt{|C_2|}} \sum_{w \in C_2} (-1)^{v \cdot w} |x \oplus w \oplus u\rangle \in \mathbb{C}^{2^n}$. For any $u \in \{0, 1\}^n/C_1$ and $v \in \{0, 1\}^n/C_2^\perp$, the set of states $\{|\xi_{xuv}\rangle\}_{x \in C_1/C_2}$ define a different quantum code (with similar properties) where $|\xi_{xuv}\rangle$ is the encoding of a word $x \in C_1/C_2$.

Lemma 16 (Characters sums)

- (a) For a linear binary code C , if $x \in C^\perp$ then $\sum_{y \in C} (-1)^{x \cdot y} = |C|$, and if $x \notin C^\perp$, then $\sum_{y \in C} (-1)^{x \cdot y} = 0$.
(b) For a linear binary code C and $x \in C$, if $x = 0$ then $\sum_{y \in \{0, 1\}^n/C^\perp} (-1)^{x \cdot y} = |C|$, and if $x \neq 0$, then $\sum_{y \in \{0, 1\}^n/C^\perp} (-1)^{x \cdot y} = 0$.

Proof. We prove (a) first.

The first part of (a) follows since for $x \in C^\perp$, we have $(-1)^{x \cdot y} = (-1)^0 = 1$ for all $y \in C$. For the second part, notice that $x \notin C^\perp$ implies that there is a $y_1 \in C$ such that $x \cdot y_1 = 1$. Fix a basis $\{y_1, \dots, y_k\}$ of C (using that particular y_1). Let $C' := \text{span}\{y_2, \dots, y_k\}$. Then $\sum_{y \in C} (-1)^{x \cdot y} = \sum_{y \in C'} (-1)^{x \cdot y} + (-1)^{x \cdot (y \oplus y_1)} = \sum_{y \in C'} (-1)^{x \cdot y} + (-1)^{x \cdot y} (-1)^{x \cdot y_1} = \sum_{y \in C'} (-1)^{x \cdot y} + (-1)^{x \cdot y} (-1) = 0$.

We now prove (b).

The first part of (b) follows since $(-1)^{x \cdot y} = 1$ and $|\{0, 1\}^n/C^\perp| = 2^n/(2^{n-\dim C}) = 2^{\dim C} = |C|$. For the second part, we have

$$0 \stackrel{(*)}{=} \sum_{y \in \{0, 1\}^n} (-1)^{x \cdot y} = \sum_{\substack{y \in \{0, 1\}^n/C^\perp \\ z \in C^\perp}} (-1)^{x \cdot (y \oplus z)} \stackrel{(**)}{=} \sum_{\substack{y \in \{0, 1\}^n/C^\perp \\ z \in C^\perp}} (-1)^{x \cdot y} = |C^\perp| \cdot \sum_{y \in \{0, 1\}^n/C^\perp} (-1)^{x \cdot y}$$

Here $(*)$ is by (a) (with $C := \{0, 1\}^n$ and $x \notin C^\perp = \{0\}$). And $(**)$ uses that $x \cdot z = 0$ for $x \in C$ and $z \in C^\perp$. So $|C^\perp| \sum_{y \in \{0, 1\}^n/C^\perp} (-1)^{x \cdot y} = 0$, and hence $\sum_{y \in \{0, 1\}^n/C^\perp} (-1)^{x \cdot y} = 0$. \square

Lemma 17 (CSS codes form a basis) $\{|\xi_{xuv}\rangle\}_{x \in C_1/C_2, u \in \{0, 1\}^n/C_1, v \in \{0, 1\}^n/C_2^\perp}$ is an orthonormal basis of \mathbb{C}^{2^n} .

¹⁹A $[n, k]$ -code is a code consisting of 2^k codewords, each of length n . That is, a k -dimensional subspace of $\{0, 1\}^n = \text{GF}(2)^n$.

Proof. We easily verify that $\|\xi_{xuv}\rangle\| = 1$. Furthermore, the number of tuples (x, u, v) is $|C_1/C_2| \cdot |\{0, 1\}^n/C_1| \cdot |\{0, 1\}^n/C_2^\perp| = (2^{k_1}/2^{k_2}) \cdot (2^n/2^{k_1}) \cdot (2^n/2^{n-k_2}) = 2^n$. Thus $\{\xi_{xuv}\rangle\}_{x,u,v}$ forms a basis if the $\xi_{xuv}\rangle$ are linearly independent. Thus, to show that $\{\xi_{xuv}\rangle\}_{x,u,v}$ is an orthonormal basis, it is thus sufficient to show that the $\xi_{xuv}\rangle$ are orthogonal (and thus also linearly independent).

To show this, fix $x, x' \in C_1/C_2$, $u, u' \in \{0, 1\}^n/C_1$, $v, v' \in \{0, 1\}^n/C_2^\perp$ with $(x, u, v) \neq (x', u', v')$. We will show that $\langle \xi_{xuv} | \xi_{x'u'v'} \rangle = 0$.

We have $\langle \xi_{xuv} | \xi_{x'u'v'} \rangle = \frac{1}{|C_2|} \sum_{w, w' \in C_2} (-1)^{v \cdot w \oplus v' \cdot w'} \langle x \oplus u \oplus w | x' \oplus u' \oplus w' \rangle$. If $(x, u) \neq (x', u')$, then $x \oplus u \neq x' \oplus u'$ and $x \oplus u, x' \oplus u' \in \{0, 1\}^n/C_2$ since $x, x' \in C_1/C_2$ and $u, u' \in \{0, 1\}^n/C_1$. Thus $(x \oplus u) - (x' \oplus u') \notin C_2$ and thus $x \oplus u \oplus w \neq x' \oplus u' \oplus w'$ for any $w, w' \in C_2$. Hence $\langle \xi_{xuv} | \xi_{x'u'v'} \rangle = 0$ if $(x, u) \neq (x', u')$. If $(x, u) = (x', u')$, then $v \neq v'$. Also, the scalar product $\langle x \oplus u \oplus w | x' \oplus u' \oplus w' \rangle$ vanishes for $w \neq w'$. Thus we have $\langle \xi_{xuv} | \xi_{x'u'v'} \rangle = \frac{1}{|C_2|} \sum_{w \in C_2} (-1)^{(v \oplus v') \cdot w}$. Since $v, v' \in \{0, 1\}^n/C_2^\perp$ and $v \neq v'$, we have that $v - v' \notin C_2^\perp$. Thus by Lemma 16 (a), $\langle \xi_{xuv} | \xi_{x'u'v'} \rangle = 0$. \square

Lemma 18 (EPR states as CSS code superpositions) $2^{-n/2} \sum_{x,u,v} |\xi_{xuv}\rangle \otimes |\xi_{xuv}\rangle = |\widetilde{0^n 0^n}\rangle$ with $x \in C_1/C_2, u \in \{0, 1\}^n/C_1, v \in \{0, 1\}^n/C_2^\perp$. (Recall that $|\widetilde{0^n 0^n}\rangle$ denotes n EPR pairs, see page 4.)

Proof.

$$\begin{aligned}
& 2^{-n/2} \sum_{x,u,v} |\xi_{xuv}\rangle \otimes |\xi_{xuv}\rangle \\
&= 2^{-n/2} |C_2|^{-1} \sum_{x,u,v} \sum_{w_1, w_2 \in C_2} (-1)^{v \cdot (w_1 \oplus w_2)} |x \oplus w_1 \oplus u\rangle \otimes |x \oplus w_2 \oplus u\rangle \\
&= 2^{-n/2} |C_2|^{-1} \sum_{x,u, w_1, w_2} \underbrace{\sum_{v \in \{0, 1\}^n/C_2^\perp} (-1)^{v \cdot (w_1 \oplus w_2)} |x \oplus w_1 \oplus u\rangle \otimes |x \oplus w_2 \oplus u\rangle}_{=0 \text{ if } w_1 \neq w_2, =|C_2| \text{ if } w_1 = w_2 \text{ by Lemma 16 (b)}} \\
&= 2^{-n/2} \sum_{x,u,w} |x \oplus w \oplus u\rangle \otimes |x \oplus w \oplus u\rangle \\
&= 2^{-n/2} \sum_{j \in \{0, 1\}^n} |j\rangle \otimes |j\rangle \\
&= |\widetilde{0^n 0^n}\rangle \quad \square
\end{aligned}$$

Error-correction and decoding operations. We proceed to define some operations related to CSS codes that are needed for subsequent proofs:

For $u \in \{0, 1\}^n/C_1, v \in \{0, 1\}^n/C_2^\perp$, let U_{uv}^{EC} be an isometry²⁰ describing error correction and decoding for the CCS code $\{|\xi_{xuv}\rangle\}_x$. More precisely, we require that for any u, v and any $f \in \{0, 1\}^n, e \in \{0, 1\}^n$ with $\omega(f), \omega(e) \leq t$ there is a state $|\Psi\rangle$ such that for all x we have $U_{uv}^{EC} X^e Z^f |\xi_{xuv}\rangle = |x\rangle \otimes |\Psi\rangle$. Here X^e stands for $X^{e_1} \otimes \dots \otimes X^{e_n}$ and Z^f analogously where X, Z are the Pauli gates.

Let U_{uv}^{dec} be an isometry describing decoding (without error correction) for the CCS code $\{|\xi_{xuv}\rangle\}_x$. More precisely, we require that for any $u \in \{0, 1\}^n/C_1, v \in \{0, 1\}^n/C_2^\perp$ there is a state $|\Psi\rangle$ such that for all $x \in C_1/C_2$ we have $U_{uv}^{dec} |\xi_{xuv}\rangle = |x\rangle \otimes |\Psi\rangle$. And for any $u \in \{0, 1\}^n/C_1, v \in \{0, 1\}^n/C_2^\perp$ and any $|\xi\rangle$ orthogonal to $\text{span}\{|\xi_{xuv}\rangle : x \in C_1/C_2\}$, there is a $|\Psi\rangle$ such that $U_{uv}^{dec} |\xi\rangle = |\perp\rangle \otimes |\Psi\rangle$.

Lemma 19 (Decoding and error correcting) *Polynomial-time operations U_{uv}^{dec} and U_{uv}^{EC} with the properties above exist.*

Proof. We first construct U_{uv}^{EC} . Fix $x \in C_1/C_2, u \in \{0, 1\}^n/C_1, v \in \{0, 1\}^n/C_2^\perp$ as well as $f \in \{0, 1\}^n, e \in \{0, 1\}^n$ with $\omega(f), \omega(e) \leq t$. In the following calculation, we will apply a number of polynomial-time

²⁰I.e., a pure quantum operation that may add auxiliary qubits. This is slightly less demanding than requiring a unitary. (Which in turns can lead to a smaller circuit for U_{uv}^{EC} and thus to a more efficient reduction in our construction of revocably-hiding timed-release encryptions below.) Notice that the conditions for U_{uv}^{dec} below cannot even be satisfied by a unitary operation: the dimension of the input space of U_{uv}^{dec} is $\dim_{in} := 2^n$, and the dimension of the output space is $\dim_{out} := |C_1/C_2| \cdot \dim_{\Psi}$ where \dim_{Ψ} is the dimension of $|\Psi\rangle$. Since $|C_1/C_2|$ is not a power of two, $\dim_{in} = \dim_{out}$ is impossible, so U_{uv}^{dec} cannot be unitary.

isometries to $X^e Z^f |\xi_{xuv}\rangle$ to reach a state of the form $|x\rangle \otimes |\Psi\rangle$. The isometries will depend only on u, v , and $|\Psi\rangle$ will depend only on u, v, f, e . Thus, by taking the product of these isometries, we get U_{uv}^{EC} such that for any u, v and any $f \in \{0, 1\}^n, e \in \{0, 1\}^n$ with $\omega(f), \omega(e) \leq t$ there is a state $|\Psi\rangle$ such that for all x we have $U_{uv}^{EC} X^e Z^f |\xi_{xuv}\rangle = |x\rangle \otimes |\Psi\rangle$, as required by the definition of U_{uv}^{EC} . All sum-indices range over $\{0, 1\}^n$ unless specified otherwise.

(The following calculation loosely follows [NC10, Section 10.4.2].)

To increase readability, we highlight differences between the lines of the calculation in blue, with an underscore () denoting an omitted piece of formula.

$$\begin{aligned}
& X^e Z^f |\xi_{xuv}\rangle \\
&= X^e Z^f \left(2^{-k_2/2} \sum_{w \in C_2} (-1)^{v \cdot w} |x \oplus w \oplus u\rangle \right) \\
&= X^e \underline{\quad} \left(2^{-k_2/2} \sum_{w \in C_2} (-1)^{v \cdot w \oplus f \cdot (x \oplus w \oplus u)} |x \oplus w \oplus u\rangle \right) \\
&= 2^{-k_2/2} \underline{\quad} \sum_{w \in C_2} (-1)^{v \cdot w \oplus f \cdot (x \oplus w \oplus u)} |x \oplus w \oplus u \oplus e\rangle \\
&\mapsto 2^{-k_2/2} \sum_{w \in C_2} (-1)^{v \cdot w \oplus f \cdot (x \oplus w \oplus u)} |x \oplus w \oplus \underline{\quad} e\rangle && \text{using } U_1 : |z\rangle \mapsto |z \oplus u\rangle \\
&\mapsto 2^{-k_2/2} \sum_{w \in C_2} (-1)^{v \cdot w \oplus f \cdot (x \oplus w \oplus u)} |x \oplus w \oplus e\rangle |H_1(x \oplus w \oplus e)\rangle && \text{using } U_2 : |z\rangle \mapsto |z\rangle |H_1 z\rangle \\
& && \text{with } H_1 \text{ parity check matrix of } C_1 \\
&= 2^{-k_2/2} \sum_{w \in C_2} (-1)^{v \cdot w \oplus f \cdot (x \oplus w \oplus u)} |x \oplus w \oplus e\rangle |H_1 e\rangle && \text{since } x \oplus w \in C_1 = \ker H_1 \\
&\mapsto 2^{-k_2/2} \sum_{w \in C_2} (-1)^{v \cdot w \oplus f \cdot (x \oplus w \oplus u)} |x \oplus w \underline{\quad}\rangle |H_1 e\rangle && \text{using } U_{ec1} : |z_1\rangle |H_1 e\rangle \mapsto |z_1 \oplus e\rangle |H_1 e\rangle, \\
& && \text{see below} \\
&\mapsto 2^{-k_2/2} \sum_{w \in C_2} (-1)^{v \cdot w \oplus f \cdot (x \oplus w \oplus u)} \left(2^{-n/2} \sum_z (-1)^{z \cdot (x \oplus w)} |z\rangle \right) |H_1 e\rangle && \text{using } H^{\otimes n} \\
&= 2^{-k_2/2 - n/2} \sum_z \sum_{w \in C_2} (-1)^{w \cdot (z \oplus f \oplus v)} (-1)^{f \cdot (x \oplus u) \oplus z \cdot x} |z\rangle |H_1 e\rangle \\
&= 2^{-k_2/2 - n/2} \sum_{z'} \sum_{w \in C_2} (-1)^{w \cdot z'} (-1)^{f \cdot u \oplus (z' \oplus v) \cdot x} |z' \oplus f \oplus v\rangle |H_1 e\rangle && \text{with } z' := z \oplus f \oplus v \\
&= 2^{-k_2/2 - n/2} \sum_{z' \in C_2^\perp} 2^{k_2} (-1)^{f \cdot u \oplus (z' \oplus v) \cdot x} |z' \oplus f \oplus v\rangle |H_1 e\rangle && \text{by Lemma 16 (a) (using } w \in C_2, |C_2| = 2^{k_2}) \\
&\mapsto 2^{k_2/2 - n/2} \sum_{z' \in C_2^\perp} \underline{\quad} (-1)^{f \cdot u \oplus (z' \oplus v) \cdot x} |z' \oplus f \underline{\quad}\rangle |H_1 e\rangle && \text{using } U_3 : |z\rangle \mapsto |z \oplus v\rangle \\
&\mapsto 2^{k_2/2 - n/2} \sum_{z' \in C_2^\perp} (-1)^{f \cdot u \oplus (z' \oplus v) \cdot x} |z' \oplus f\rangle |H_2(z' \oplus f)\rangle |H_1 e\rangle && \text{using } U_4 : |z\rangle \mapsto |z\rangle |H_2 z\rangle \\
& && \text{with } H_2 \text{ parity check matrix of } C_2^\perp \\
&= 2^{k_2/2 - n/2} \sum_{z' \in C_2^\perp} (-1)^{f \cdot u \oplus (z' \oplus v) \cdot x} |z' \oplus f\rangle |H_2 f\rangle |H_1 e\rangle && \text{since } z' \in C_2^\perp = \ker H_1 \\
&\mapsto 2^{k_2/2 - n/2} \sum_{z' \in C_2^\perp} (-1)^{f \cdot u \oplus (z' \oplus v) \cdot x} |z' \underline{\quad}\rangle |H_2 f\rangle |H_1 e\rangle && \text{using } U_{ec2} : |z_1\rangle |H_2 f\rangle \mapsto |z_1 \oplus f\rangle |H_2 f\rangle \\
& && \text{see below} \\
&\mapsto 2^{k_2/2 - n/2} \sum_{z' \in C_2^\perp} (-1)^{f \cdot u \oplus (z' \oplus v) \cdot x} \left(\sum_y 2^{-n/2} (-1)^{y \cdot z'} |y\rangle \right) |H_2 f\rangle |H_1 e\rangle && \text{using } H^{\otimes n} \\
&= 2^{k_2/2 - n} \sum_y \sum_{z' \in C_2^\perp} (-1)^{z' \cdot (y \oplus x)} (-1)^{f \cdot u \oplus v \cdot x} |y\rangle |H_2 f\rangle |H_1 e\rangle \\
&= 2^{k_2/2 - n} \sum_{y'} \sum_{z' \in C_2^\perp} (-1)^{z' \cdot y'} (-1)^{f \cdot u \oplus v \cdot x} |y' \oplus x\rangle |H_2 f\rangle |H_1 e\rangle && \text{with } y' := y \oplus x \\
&= 2^{k_2/2 - n} \sum_{y' \in C_2} 2^{n - k_2} (-1)^{f \cdot u \oplus v \cdot x} |y' \oplus x\rangle |H_2 f\rangle |H_1 e\rangle && \text{by Lemma 16 (a) (using } |C_2^\perp| = 2^{n - k_2}, \\
& && (C_2^\perp)^\perp = C_2)
\end{aligned}$$

$$\begin{aligned}
&\mapsto 2^{-k_2/2} \sum_{y' \in C_2} \underline{-} (-1)^{f \cdot u \oplus v \cdot x} |x\rangle |y' \oplus x\rangle |H_2 f\rangle |H_1 e\rangle && \text{using } U_5 : |z\rangle \mapsto |z \bmod C_2\rangle |z\rangle \\
&\mapsto 2^{-k_2/2} \sum_{y' \in C_2} (-1)^{f \cdot u \oplus v \cdot x} |x\rangle |y' \underline{-}\rangle |H_2 f\rangle |H_1 e\rangle && \text{using } U_6 : |z_1\rangle |z_2\rangle \mapsto |z_1\rangle |z_2 \oplus z_1\rangle \\
&= (-1)^{v \cdot x} |x\rangle |\Psi\rangle && \text{with } |\Psi\rangle := 2^{-k_2/2} (-1)^{f \cdot u} \\
& && \sum_{y' \in C_2} |y'\rangle |H_2 f\rangle |H_1 e\rangle \\
&\mapsto \underline{-} |x\rangle |\Psi\rangle && \text{using } Z^v
\end{aligned}$$

In the above calculation, we used the unitaries U_{ec1} and U_{ec2} . We describe U_{ec1} : Let $ec1$ be a polynomial-error error correction function for C_1 , i.e., $ec1(z) = z'$ if $\omega(z \oplus z') \leq t$ and $z' \in C_1$. Let H_1 be the parity check matrix of C_1 . Let $H_1^{-1}(z)$ denote a polynomial-time function that returns some preimage of z under H_1 if such exists and is defined arbitrarily elsewhere. For $y \in \{0, 1\}^n$, let $ec1'(y) := ec1(H_1^{-1}(y)) \oplus H_1^{-1}(y)$. Then for $\omega(e) \leq t$, we have that $H_1^{-1}(H_1 e) \oplus e \in \ker H_1 = C_1$ because both e and $H_1^{-1}(H_1 e)$ are preimages of $H_1 e$ under H_1 . Hence $ec1(H_1^{-1}(H_1 e)) = H_1^{-1}(H_1 e) \oplus e$, and thus $ec1'(H_1 e) = e$. Let $U_{ec1} : |z_1\rangle |z_2\rangle \mapsto |z_1 \oplus ec1'(z_2)\rangle |z_2\rangle$. Then $U_{ec1} : |z_1\rangle |H_1 e\rangle \mapsto |z_1 \oplus e\rangle |H_1 e\rangle$ for $\omega(e) \leq t$ as needed in the above calculation. U_{ec2} is constructed analogously with respect to C_2^1 instead of C_1 .

As discussed in the beginning of the proof, U_{uv}^{EC} is then the product of the isometries applied in the above calculation.

We now construct U_{uv}^{dec} . We define the following unitaries and isometries:

- $U_{\oplus u} : |z\rangle \mapsto |z \oplus u\rangle$ for $z \in \{0, 1\}^n$.
- $U_{split} : |x \oplus w\rangle \mapsto |x\rangle |w\rangle$ for $x \in C_1/C_2$ and $w \in C_2$. (This can be implemented by $|x \oplus w\rangle \mapsto |x \oplus w\rangle |0^n\rangle \xrightarrow{(*)} |x \oplus w\rangle |w\rangle \mapsto |x\rangle |w\rangle$ where $(*)$ uses a unitary $|z\rangle |z'\rangle \mapsto |z\rangle |z' \oplus (z \bmod C_2)\rangle$.)
- $Z^v := Z^{v_1} \otimes \dots \otimes Z^{v_n}$ where Z is the Pauli matrix Z .
- $U_G : |0^n\rangle \mapsto \frac{1}{\sqrt{|C_2|}} \sum_{w \in C_2} |w\rangle$. (This can be implemented using $n - k_2$ auxiliaries as $|0^n\rangle |0^{n-k_2}\rangle \xrightarrow{H^{\otimes n-k_2}} \frac{1}{\sqrt{|C_2|}} \sum_{z \in \{0,1\}^{n-k_2}} |0^n\rangle |z\rangle \xrightarrow{(*)} \frac{1}{\sqrt{|C_2|}} \sum_{z \in \{0,1\}^{n-k_2}} |Gz\rangle |z\rangle \xrightarrow{(**)} \frac{1}{\sqrt{|C_2|}} \sum_{z \in \{0,1\}^{n-k_2}} |Gz\rangle |0^{n-k_2}\rangle$. Here G is the generator matrix of C_2 . And $G^{-1}(z)$ computes the unique preimage of z under G where $G^{-1}(z)$ is arbitrary if this preimage does not exist. And $(*)$ uses a unitary $|z\rangle |z'\rangle \mapsto |z \oplus Gz'\rangle |z'\rangle$. And $(**)$ uses a unitary $|z\rangle |z'\rangle \mapsto |z\rangle |z' \oplus G^{-1}(z)\rangle$.)
- $U_{check} : |x\rangle |0^n\rangle \mapsto |x\rangle |0^n\rangle |0^n\rangle$ for $x \in C_1/C_2$ and $U_{check} : |x\rangle |z\rangle \mapsto |\perp\rangle |0^n\rangle |x\rangle$ for $x \notin C_1/C_2$ or $z \neq 0^n$.

Notice that all these operations can be implemented in polynomial time.

If we start with a state $|\xi_{xuv}\rangle$ with $x \in C_1/C_2$ and apply the following operations sequentially, we get the following states:

- After $U_{\oplus u}$: $\frac{1}{\sqrt{|C_2|}} \sum_{w \in C_2} (-1)^{v \cdot w} |x \oplus w\rangle$.
- After U_{split} : $\frac{1}{\sqrt{|C_2|}} \sum_{w \in C_2} (-1)^{v \cdot w} |x\rangle |w\rangle$.
- After $I_n \otimes Z^v$: $|x\rangle \otimes \frac{1}{\sqrt{|C_2|}} \sum_{w \in C_2} |w\rangle$.
- After $I_n \otimes U_G^\dagger$: $|x\rangle \otimes |0^n\rangle$. (This holds because $U_G |0^n\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{w \in C_2} |w\rangle$.)
- After U_{check} : $|x\rangle \otimes |0^n\rangle |0^n\rangle$.

Let U_{uv}^{dec} be the operation resulting from applying all these operations sequentially.

Thus, with $|\Psi\rangle := |0^n\rangle |0^n\rangle$ we have: For any u, v there is a state $|\Psi\rangle$ such that for all x we have $U_{uv}^{dec} |\xi_{xuv}\rangle = |x\rangle \otimes |\Psi\rangle$.

Furthermore, for fixed u, v , if we apply the same sequence of operations to a state $|\xi\rangle$ that is orthogonal to all $|\xi_{xuv}\rangle$ ($x \in C_1/C_2$), then after $I_n \otimes U_G^\dagger$ we get a state $|\Phi\rangle$ that is orthogonal to all $|x\rangle |0^n\rangle$ ($x \in C_1/C_2$), i.e., $|\Phi\rangle$ is spanned by vectors $|x\rangle |z\rangle$ with $x \notin C_1/C_2$ or $z \neq 0^n$. Thus $U_{uv}^{dec} |\xi\rangle = U_{check} |\Phi\rangle = |\perp\rangle \otimes |\Psi\rangle$ for some $|\Psi\rangle$.

Hence for any u, v and any $|\xi\rangle$ is orthogonal to $\text{span}\{|\xi_{xuv}\rangle : x \in C_1/C_2\}$, there is a $|\Psi\rangle$ such that $U_{uv}^{dec} |\xi_{xuv}\rangle = |\perp\rangle \otimes |\Psi\rangle$.

This shows the existence of U_{uv}^{dec} . \square

D Full proofs: revocably hiding timed-release encryptions

This section is devoted to proving Theorem 3.

Let (A_0, A_1, A_2) be an adversary such that A_0 is sequential-polynomial-time and A_1 is sequential-polynomial-time and $(T - \delta_T^{hid})$ -time. (No restrictions on A_2 .)

Variable conventions. In the following, the variables B, Q, r, x, u, v always range over the following sets unless explicitly specified otherwise: $B \in \{0, 1\}^q$, $Q \in [q + n]_q$, $B \in \{0, 1\}^q$, $r \in \{0, 1\}^q$, $x \in C_1/C_2$, $u \in \{0, 1\}^n/C_1$, $v \in \{0, 1\}^n/C_2^\perp$. The same holds for derived variable names such as r_1 or r' .

Some measurements. We first define a number of projective measurements that will be used in this proof:

The measurement M_R measures the first q qubits of an $q + n$ qubit register in the computational basis. Formally, $M_R = \{P_r\}_{r \in \{0, 1\}^q}$ with $P_r := |r\rangle\langle r| \otimes I_n$.

The measurement M_{UV} measures the values u, v in an $q + n$ qubit state of the form $|r\rangle \otimes |\xi_{xuv}\rangle$. Formally, let $P_{uv} = \sum_x I_q \otimes |\xi_{xuv}\rangle\langle \xi_{xuv}|$ and $M_{UV} := \{P_{uv}\}_{u, v}$.

The measurement M_X^{uv} , parametric in u, v , measures the value x in an $q + n$ qubit state of the form $|r\rangle \otimes |\xi_{xuv}\rangle$. (If the parameters u, v do not match, the outcome is \perp .) Formally, let $P_x^{uv} = I_q \otimes |\xi_{xuv}\rangle\langle \xi_{xuv}|$ and $P_\perp^{uv} = 1 - \sum_x P_x^{uv}$ and $M_X^{uv} = \{P_x^{uv}\}_{x \in C_1/C_2 \cup \{\perp\}}$.

That the measurements M_{UV} and M_X^{uv} are indeed projective measurements follows from the fact that the $|\xi_{xuv}\rangle$ form an orthonormal basis (Lemma 17).

Also recall the definition of P_t^{EPR} (page 20). Similarly, we define $P_{C_1/C_2}^{EPR} := \sum_{x \in C_1/C_2} |x\rangle\langle x| \otimes |x\rangle\langle x|$, i.e., P_{C_1/C_2}^{EPR} is the analogue of P_{C_1/C_2}^{EPR} for basis $\{|x\rangle\}_{x \in C_1/C_2}$.

Sequence of games. We now proceed to define a number of games and to show the relation between the attack probability in these games. From this we finally deduce the security of our protocol. X and Y refer to n -bit quantum registers.

Game 1 (Original game)

- (a) In this game, $b \in \{0, 1\}$ is a parameter of the game.
- (b) $(m_0, m_1) \leftarrow A_0()$. ($m_0, m_1 \in C_1/C_2$ since that is the message space of RTRE_{hid} .)
- (c) $B \xleftarrow{\$} \{0, 1\}^q$. $Q \xleftarrow{\$} [q + n]_q$. $p \xleftarrow{\$} C_1/C_2$.
- (d) $u \xleftarrow{\$} \{0, 1\}^n/C_1$. $r \xleftarrow{\$} \{0, 1\}^q$.
- (e) $x \xleftarrow{\$} C_1/C_2$.
- (f) $w \xleftarrow{\$} C_2$.
- (g) $X \leftarrow U_Q^\dagger (H^B \otimes I_n) (|r\rangle \otimes |x \oplus w \oplus u\rangle)$.
- (h) $V_0 \leftarrow \text{TRE}_0(B, Q, r, p)$.
- (i) Run $A_1(X, V_0, u, m_b \oplus x \oplus p)$. (We pass the quantum register X to A_1 which means that A_1 has read-write access to it.)
- (j) Apply $(H^B \otimes I_n)U_Q$ to X .
- (k) Measure X using M_R , outcome r' . If $r = r'$, $ok := 1$, else $ok := 0$.
- (l) Run $b' \leftarrow A_2()$.

Since Game 1 is the game from Definition 5 (with the definition of RTRE_{hid} inlined), it suffices to show that $|\Pr[b' = 1 \wedge ok = 1 : \text{Game 1}(0)] - \Pr[b' = 1 \wedge ok = 1 : \text{Game 1}(1)]|$ is negligible.

Game 2 (Late key revelation)

- (a) In this game, $b \in \{0, 1\}$ is a parameter of the game.
- (b) $(m_0, m_1) \leftarrow A_0()$.
- (c) $B \xleftarrow{\$} \{0, 1\}^q$. $Q \xleftarrow{\$} [q + n]_q$. $p \xleftarrow{\$} C_1/C_2$.
- (d) $u \xleftarrow{\$} \{0, 1\}^n/C_1$. $r \xleftarrow{\$} \{0, 1\}^q$.
- (e) $x \xleftarrow{\$} C_1/C_2$. $\hat{x} \xleftarrow{\$} C_1/C_2$
- (f) $w \xleftarrow{\$} C_2$.
- (g) $X \leftarrow U_Q^\dagger (H^B \otimes I_n) (|r\rangle \otimes |x \oplus w \oplus u\rangle)$.
- (h) $V_0 \leftarrow \text{TRE}_0(B, Q, r, p)$.
- (i) Run $A_1(X, V_0, u, \hat{x} \oplus p)$.
- (j) Apply $(H^B \otimes I_n)U_Q$ to X .

- (k) Measure X using M_R , outcome r' . If $r = r'$, $ok := 1$, else $ok := 0$.
(l) If $m_b \oplus x = \hat{x}$, run $b' \leftarrow A_2()$. Else let $b' := 0$.

Lemma 20 (Game 1 vs. Game 2) Then for $b \in \{0, 1\}$ we have

$$\Pr[b' = 1 \wedge ok = 1 : \text{Game 1}(b)] = |C_1/C_2| \Pr[b' = 1 \wedge ok = 1 : \text{Game 2}(b)]$$

Proof. Note that for all $\underline{x}, \hat{x}, \underline{m}_0, \underline{m}_1$, we have

$$\begin{aligned} \Pr[b' = 1 \wedge ok = 1 \mid (x, \hat{x}, m_0, m_1) = (\underline{x}, \hat{x}, \underline{m}_0, \underline{m}_1) : \text{Game 2}(b)] \\ = \begin{cases} \Pr[b' = 1 \wedge ok = 1 \mid (x, m_0, m_1) = (\underline{x}, \underline{m}_0, \underline{m}_1) : \text{Game 1}(b)] & \text{if } \underline{m}_b \oplus \underline{x} = \hat{x} \\ 0 & \text{if } \underline{m}_b \oplus \underline{x} \neq \hat{x}. \end{cases} \end{aligned} \quad (5)$$

And since up to and including the invocation of A_0 , the games are identical, we have $\Pr[(m_0, m_1) = (\underline{m}_0, \underline{m}_1) : \text{Game 2}(b)] = \Pr[(m_0, m_1) = (\underline{m}_0, \underline{m}_1) : \text{Game 1}(b)]$.

Thus

$$\begin{aligned} & |C_1/C_2| \Pr[b' = 1 \wedge ok = 1 : \text{Game 2}(b)] \\ &= \sum_{\substack{\underline{x}, \hat{x}, \\ \underline{m}_0, \underline{m}_1}} \frac{1}{|C_1/C_2|} \Pr[b' = 1 \wedge ok = 1 \mid (x, \hat{x}, m_0, m_1) = (\underline{x}, \hat{x}, \underline{m}_0, \underline{m}_1) : \text{Game 2}(b)] \\ & \quad \cdot \Pr[(m_0, m_1) = (\underline{m}_0, \underline{m}_1) : \text{Game 2}(b)] \\ &\stackrel{(5)}{=} \sum_{\underline{x}, \underline{m}_0, \underline{m}_1} \frac{1}{|C_1/C_2|} \Pr[b' = 1 \wedge ok = 1 \mid (x, m_0, m_1) = (\underline{x}, \underline{m}_0, \underline{m}_1) : \text{Game 1}(b)] \\ & \quad \cdot \Pr[(m_0, m_1) = (\underline{m}_0, \underline{m}_1) : \text{Game 1}(b)] \\ &= \Pr[b' = 1 \wedge ok = 1 : \text{Game 1}(b)]. \quad \square \end{aligned}$$

Game 3 (Using CSS codes)

- (a) In this game, $b \in \{0, 1\}$ is a parameter of the game.
(b) $(m_0, m_1) \leftarrow A_0()$.
(c) $B \xleftarrow{\$} \{0, 1\}^q$. $Q \xleftarrow{\$} [q+n]_q$. $p \xleftarrow{\$} C_1/C_2$.
(d) $u \xleftarrow{\$} \{0, 1\}^n/C_1$. $r \xleftarrow{\$} \{0, 1\}^q$.
(e) $x \xleftarrow{\$} C_1/C_2$. $\hat{x} \xleftarrow{\$} C_1/C_2$.
(f) ~~$w \xleftarrow{\$} C_2$~~ $v \xleftarrow{\$} \{0, 1\}^n/C_2^\perp$
(g) $X \leftarrow U_Q^\dagger (H^B \otimes I_n) (|r\rangle \otimes |\xi_{xuv}\rangle)$.
(h) $V_0 \leftarrow \text{TRE}_0(B, Q, r, p)$.
(i) Run $A_1(X, V_0, u, \hat{x} \oplus p)$.
(j) Apply $(H^B \otimes I_n) U_Q$ to X .
(k) Measure X using M_R , outcome r' . If $r = r'$, $ok := 1$, else $ok := 0$.
(l) If $m_b \oplus x = \hat{x}$, run $b' \leftarrow A_2()$. Else let $b' := 0$.

Lemma 21 (Game 2 vs. Game 3) For $b \in \{0, 1\}$ we have

$$\Pr[b' = 1 \wedge ok = 1 : \text{Game 2}(b)] = \Pr[b' = 1 \wedge ok = 1 : \text{Game 3}(b)]$$

Proof. In Games 2 and 3, w and v are never used except in the construction of the state $|x \oplus w \oplus u\rangle$ and $|\xi_{xuv}\rangle$, respectively. Thus to show Lemma 21, it is sufficient to show that for all x and u , $|x \oplus w \oplus u\rangle$ and $|\xi_{xuv}\rangle$ are indistinguishable by any quantum circuit for random v, w , i.e., that $\rho_1^{xu} = \rho_2^{xu}$ for $\rho_1^{xu} := \sum_w \frac{1}{|C_2|} |x \oplus w \oplus u\rangle \langle x \oplus w \oplus u|$ and $\rho_2^{xu} := \sum_v \frac{1}{|\{0, 1\}^n/C_2^\perp|} |\xi_{x,u,v}\rangle \langle \xi_{x,u,v}|$. This equality is shown by the following calculation:

$$\begin{aligned} \rho_2^{xu} &\stackrel{(*)}{=} \sum_{w_1, w_2} \frac{1}{|C_2|} \left(\sum_v \frac{1}{|\{0, 1\}^n/C_2^\perp|} (-1)^{v \cdot (w_1 \oplus w_2)} \right) |x \oplus w_1 \oplus u\rangle \langle x \oplus w_2 \oplus u| \\ &\stackrel{(**)}{=} \sum_w \frac{1}{|C_2|} |x \oplus w \oplus u\rangle \langle x \oplus w \oplus u| = \rho_1^{xu}. \end{aligned}$$

Here $(*)$ uses the definition of $|\xi_{xuv}\rangle$, and $(**)$ uses Lemma 16 (b) with $C := C_2$ and $x := w_1 \oplus w_2$.

Thus $\rho_1^{xu} = \rho_2^{xu}$ and the lemma follows. \square

Game 4 (Using EPR pairs)

- (a) In this game, $b \in \{0, 1\}$ is a parameter of the game.
(b) $(m_0, m_1) \leftarrow A_0()$.
(c) $B \xleftarrow{\$} \{0, 1\}^q$. $Q \xleftarrow{\$} [q+n]_q$. $p \xleftarrow{\$} C_1/C_2$.
(d) $u \xleftarrow{\$} \{0, 1\}^n/C_1$. $r \xleftarrow{\$} \{0, 1\}^q$.
(e) $x \xleftarrow{\$} C_1/C_2$. $\hat{x} \xleftarrow{\$} C_1/C_2$.
(f) $v \xleftarrow{\$} \{0, 1\}^n/C_2^\perp$.
(g) $X \leftarrow U_Q^\dagger(H^B \otimes I_n)(|r\rangle \otimes |\xi_{xuv}\rangle)$.
(h) Initialize XY as $|0^{q+n}0^{q+n}\rangle$.
(i) Apply $(H^B \otimes I_n)U_Q$ to Y .
(j) Measure Y using M_{UV} , outcome u, v . (Reminder: M_{UV}, M_X^{uv}, M_R are defined on page 30.)
(k) Measure Y using M_X^{uv} , outcome x .
(l) Measure Y using M_R , outcome r .
(m) $V_0 \leftarrow \text{TRE}_0(B, Q, r, p)$.
(n) $\hat{x} \xleftarrow{\$} C_1/C_2$. Run $A_1(X, V_0, u, \hat{x} \oplus p)$.
(o) Apply $(H^B \otimes I_n)U_Q$ to X .
(p) Measure X using M_R , outcome r' . If $r = r'$, $ok := 1$, else $ok := 0$.
(q) If $m_b \oplus x = \hat{x}$, run $b' \leftarrow A_2()$. Else let $b' := 0$.

Lemma 22 (Game 3 vs. Game 4) For $b \in \{0, 1\}$, we have $\Pr[b' = 1 \wedge ok = 1 : \text{Game 3(b)}] = \Pr[b' = 1 \wedge ok = 1 : \text{Game 4(b)}]$.

Proof. To show this lemma, it is sufficient to show two things: When initializing XY with $|0^{q+n}0^{q+n}\rangle$, applying $(H^B \otimes I_n)U_Q$ on Y , and performing the measurements M_{UV} , M_X^{uv} , and M_R on Y , then the outcomes u, v, x, r will be uniformly distributed over their respective domains (note: x has to be uniformly distributed over C_1/C_2 , not over $C_1/C_2 \cup \{\perp\}$). And the post-measurement-state in X in this case is $U_Q^\dagger(H^B \otimes I_n)(|r\rangle \otimes |\xi_{xuv}\rangle)$.

Let $|\Psi_{xruv}\rangle := (I_{q+n} \otimes P_r P_x^{uv} P_{uv})(H^B \otimes I_n)U_Q|0^{q+n}0^{q+n}\rangle$. (Reminder: P_r, P_{uv}, P_x^{uv} are defined on page 30.) Then the probability of getting outcomes x, r, u, v is $\|\Psi_{xruv}\|^2$, and the post-measurement-state is $|\Psi_{xruv}\rangle / \|\Psi_{xruv}\|$.

We have

$$|\Psi_{xruv}\rangle = (I_{q+n} \otimes P_r P_x^{uv} P_{uv})(I_{q+n} \otimes (H^B \otimes I_n)U_Q)|0^{q+n}0^{q+n}\rangle \quad (6)$$

$$\stackrel{(*)}{=} (I_{q+n} \otimes P_r P_x^{uv} P_{uv})(U_Q^\dagger(H^B \otimes I_n) \otimes I_{q+n})|0^{q+n}0^{q+n}\rangle \quad (7)$$

$$= (U_Q^\dagger(H^B \otimes I_n) \otimes I_{q+n})(I_{q+n} \otimes P_r P_x^{uv} P_{uv})|0^{q+n}0^{q+n}\rangle \quad (8)$$

$$\stackrel{(**)}{=} (U_Q^\dagger(H^B \otimes I_n) \otimes I_{q+n})(P_r P_x^{uv} P_{uv} \otimes I_{q+n})|0^{q+n}0^{q+n}\rangle \quad (9)$$

$$\stackrel{(***)}{=} (U_Q^\dagger(H^B \otimes I_n) \otimes I_{q+n})(P_r P_x^{uv} P_{uv} \otimes I_{q+n})2^{-q/2-n/2} \sum_{r,x,u,v} |r\rangle|\xi_{xuv}\rangle|r\rangle|\xi_{xuv}\rangle \quad (10)$$

$$\stackrel{(***)}{=} 2^{-q/2-n/2} U_Q^\dagger(H^B \otimes I_n)|r\rangle|\xi_{xuv}\rangle \otimes |r\rangle|\xi_{xuv}\rangle. \quad (11)$$

Here (*) uses Lemma 4 with $A := (H^B \otimes I_n)U_Q$ and with $A^T = U_Q^T(H^B \otimes I_n)^T = U_Q^\dagger(H^B \otimes I_n)$ where we use that H is symmetric and U_Q is real-valued and thus $U_Q^\dagger = U_Q^T$.

And (**) uses Lemma 4 with $A := P_r P_x^{uv} P_{uv}$ and $A^T = P_{uv}^T (P_x^{uv})^T P_r^T = P_{uv} P_x^{uv} P_r$ where we use that $P_{uv}^T = P_{uv}^\dagger = P_{uv}$ because P_{uv} is real-valued and Hermitean, and analogously for P_x^{uv}, P_r .

And (***) uses Lemma 18.

And (****) uses that the $|r\rangle|\xi_{xuv}\rangle$ are orthogonal (Lemma 17), and that thus $P_r P_x^{uv} P_{uv}$ is a projector onto $|r\rangle|\xi_{xuv}\rangle$.

Hence the probability $\|\Psi_{xruv}\|^2$ of measuring x, r, u, v is 2^{-n-q} , thus x, r, u, v are uniformly distributed. And the post measurement state is $U_Q^\dagger(H^B \otimes I_n)|r\rangle|\xi_{xuv}\rangle \otimes |r\rangle|\xi_{xuv}\rangle$ in XY , thus the post measurement state in X is $U_Q^\dagger(H^B \otimes I_n)|r\rangle|\xi_{xuv}\rangle$.

This shows the lemma. \square

Game 5 (Delay measuring x)

- (a) In this game, $b \in \{0, 1\}$ is a parameter of the game.

- (b) $(m_0, m_1) \leftarrow A_0()$.
- (c) $B \stackrel{s}{\leftarrow} \{0, 1\}^q$. $Q \stackrel{s}{\leftarrow} [q+n]_q$. $p \stackrel{s}{\leftarrow} C_1/C_2$.
- (d) Initialize XY as $|0^{q+n}0^{q+n}\rangle$.
- (e) Apply $(H^B \otimes I_n)U_Q$ to Y .
- (f) Measure Y using M_{UV} , outcome u, v .
- (g) ~~Measure Y using M_X^{uv} , outcome x .~~
- (h) Measure Y using M_R , outcome r .
- (i) $V_0 \leftarrow \text{TRE}_0(B, Q, r, p)$.
- (j) $\hat{x} \stackrel{s}{\leftarrow} C_1/C_2$. Run $A_1(X, V_0, u, \hat{x} \oplus p)$.
- (k) Apply $(H^B \otimes I_n)U_Q$ to X .
- (l) Measure X using M_R , outcome r' . If $r = r'$, $ok := 1$, else $ok := 0$.
- (m) ~~Measure Y using M_X^{uv} , outcome x .~~
- (n) If $m_b \oplus x = \hat{x}$, run $b' \leftarrow A_2()$. Else let $b' := 0$.

Lemma 23 (Game 4 vs. Game 5) $\Pr[b' = 1 \wedge ok = 1 : \text{Game 4}(b)] = \Pr[b' = 1 \wedge ok = 1 : \text{Game 5}(b)]$ for $b \in \{0, 1\}$.

Proof. The measurement M_X^{uv} on Y that is moved in Game 5 commutes with M_R because it operates on a different part of the register Y . And it commutes with steps (i)–(l) because the latter do not operate on Y . \square

Game 6 (Testing the state)

- (a) ~~In this game, $b \in \{0, 1\}$ is a parameter of the game.~~
- (b) $(m_0, m_1) \leftarrow A_0()$.
- (c) $B \stackrel{s}{\leftarrow} \{0, 1\}^q$. $Q \stackrel{s}{\leftarrow} [q+n]_q$. $p \stackrel{s}{\leftarrow} C_1/C_2$.
- (d) Initialize XY as $|0^{q+n}0^{q+n}\rangle$.
- (e) Apply $(H^B \otimes I_n)U_Q$ to Y .
- (f) Measure Y using M_{UV} , outcome u, v .
- (g) Measure Y using M_R , outcome r .
- (h) $V_0 \leftarrow \text{TRE}_0(B, Q, r, p)$.
- (i) $\hat{x} \stackrel{s}{\leftarrow} C_1/C_2$. Run $A_1(X, V_0, u, \hat{x} \oplus p)$.
- (j) Apply $(H^B \otimes I_n)U_Q$ to X .
- (k) Measure X using M_R , outcome r' . If $r = r'$, $ok := 1$, else $ok := 0$.
- (l) Apply $I_q \otimes U_{uv}^{EC}$ to X and $I_q \otimes U_{uv}^{dec}$ to Y . Measure XY using P_{C_1/C_2}^{EPR} , outcome is EPR .
- (m) ~~Measure Y using M_X^{uv} , outcome x .~~
- (n) ~~If $m_b \oplus x = \hat{x}$, run $b' \leftarrow A_2()$. Else let $b' := 0$.~~

Lemma 24 (Game 5 vs. Game 6) Let $\varepsilon := \Pr[ok = 1 \wedge isEPR = 0 : \text{Game 6}]$. Then we have $|\Pr[b' = 1 \wedge ok = 1 : \text{Game 5}(0)] - \Pr[b' = 1 \wedge ok = 1 : \text{Game 5}(1)]| \leq \sqrt{\varepsilon}$.

Proof. For any \hat{x}, u, v , let $\rho_{\hat{x}uv}$ be the state in Game 6 after step (k), conditioned on the variables \hat{x}, u, v, ok in the game taking the values $\hat{x}, u, v, 1$. Let $\Pr_{\hat{x}uv}$ be the probability of \hat{x}, u, v, ok in the game taking the values $\hat{x}, u, v, 1$.

Note that until step (k), Game 5 and Game 6 are identical, hence $\rho_{\hat{x}uv}$ and $\Pr_{\hat{x}uv}$ also refer to Game 5. Thus we have for $b \in \{0, 1\}$:

$$\begin{aligned} & \Pr[b' = 1 \wedge ok = 1 : \text{Game 5}(b)] \\ &= \sum_{\hat{x}, u, v} \Pr_{\hat{x}uv} \cdot \Pr[b' = 1 : \text{start with } \rho_{\hat{x}uv}, x \leftarrow \text{measure } Y \text{ with } M_X^{uv}, b' \leftarrow B(x \oplus m_b \oplus \hat{x})] \end{aligned} \quad (12)$$

where $B(x')$ runs “If $x' = 0$, run $b' \leftarrow A_2()$. Else let $b' := 0$. Return b' ”.

Let P_x be the projector upon $\text{span}\{|r\rangle|x\rangle|\Psi\rangle : r \in \{0, 1\}^q, |\Psi\rangle \text{ arbitrary}\}$, and let M_X be the corresponding measurement $M_X = \{P_x\}_{x \in C_1/C_2 \cup \{\perp\}}$. (I.e., M_X measures the result of decoding with U_{uv}^{dec} in the computational basis.)

One easily verifies for all r, x, u, v, x', u', v' (and suitable $|\Psi\rangle$):

$$\begin{aligned}
P_x(I_q \otimes U_{uv}^{dec})|r\rangle|\xi_{xuv}\rangle &= |r\rangle|x\rangle \otimes |\Psi\rangle = (I_q \otimes U_{uv}^{dec})|r\rangle|\xi_{xuv}\rangle = (I_q \otimes U_{uv}^{dec})P_x^{uv}|r\rangle|\xi_{xuv}\rangle \\
P_x(I_q \otimes U_{uv}^{dec})|r\rangle|\xi_{x'u'v'}\rangle &= 0 = (I_q \otimes U_{uv}^{dec})P_x^{uv}|r\rangle|\xi_{x'u'v'}\rangle && \text{if } (x, u, v) \neq (x', u', v') \\
P_\perp(I_q \otimes U_{uv}^{dec})|r\rangle|\xi_{xuv}\rangle &= 0 = (I_q \otimes U_{uv}^{dec})P_\perp^{uv}|r\rangle|\xi_{xuv}\rangle \\
P_\perp(I_q \otimes U_{uv}^{dec})|r\rangle|\xi_{x'u'v'}\rangle &= |r\rangle|\perp\rangle \otimes |\Psi\rangle = (I_q \otimes U_{uv}^{dec})P_\perp^{uv}|r\rangle|\xi_{x'u'v'}\rangle && \text{if } (u, v) \neq (u', v')
\end{aligned}$$

Since the $|\xi_{xuv}\rangle$ form a basis, this implies that $P_x(I_q \otimes U_{uv}^{dec}) = (I_q \otimes U_{uv}^{dec})P_x^{uv}$ for any u, v and $x \in C_1/C_2 \cup \{\perp\}$. Hence applying $I_q \otimes U_{uv}^{dec}$ and then measuring with M_X is equivalent to measuring with M_X^{uv} and then applying $I_n \otimes U_{uv}^{dec}$. Thus the following four games have the same probability of $b' = 1$:

- Start with $\rho_{\hat{x}uv}$, $x \leftarrow$ measure Y with M_X^{uv} , $b' \leftarrow B(x \oplus m_i \oplus \hat{x})$.
- Start with $\rho_{\hat{x}uv}$, **apply $I_q \otimes U_{uv}^{EC}$ to X** , $x \leftarrow$ measure Y with M_X^{uv} , **apply $I_q \otimes U_{uv}^{dec}$ to Y** , $b' \leftarrow B(x \oplus m_i \oplus \hat{x})$. (Uses that $B(\dots)$ does not access X, Y .)
- Start with $\rho_{\hat{x}uv}$, **apply $I_q \otimes U_{uv}^{EC}$ to X** , **apply $I_q \otimes U_{uv}^{dec}$ to Y** , $x \leftarrow$ measure Y with M_X , $b' \leftarrow B(x \oplus m_i \oplus \hat{x})$. (Uses that $I_q \otimes U_{uv}^{dec}, M_X$ is equivalent to $M_X^{uv}, I_q \otimes U_{uv}^{dec}$.)
- Start with $\rho_{\hat{x}uv}^*$, **apply $I_q \otimes U_{uv}^{EC}$ to X** , **apply $I_q \otimes U_{uv}^{dec}$ to Y** , $x \leftarrow$ measure Y with M_X , $b' \leftarrow B(x \oplus m_i \oplus \hat{x})$. (Using the definition of $\rho_{\hat{x}uv}^*$, see below.)

Here we define $\rho_{\hat{x}uv}^*$ to be the state resulting from applying $I_q \otimes U_{uv}^{EC} \otimes I_q \otimes U_{uv}^{dec}$ to XY in $\rho_{\hat{x}uv}$.

Thus we can continue the computation from (12):

$$\begin{aligned}
&\Pr[b' = 1 \wedge ok = 1 : \text{Game 5}(b)] \\
&= \sum_{\hat{x}, u, v} \Pr_{\hat{x}uv} \underbrace{\Pr[b' = 1 : \text{start with } \rho_{\hat{x}uv}^*, x \leftarrow \text{measure } Y \text{ with } M_X, b' \leftarrow B(x \oplus m_b \oplus \hat{x})]}_{=: \text{Succ}_{\hat{x}uv}^b} \quad (13)
\end{aligned}$$

Furthermore, we have

$$\varepsilon = \Pr[ok = 1 \wedge isEPR = 0 : \text{Game 6}] = \sum_{\hat{x}, u, v} \Pr_{\hat{x}uv} \underbrace{\text{tr}((1 - P_{C_1/C_2}^{EPR}) \otimes I) \rho_{\hat{x}uv}^*}_{=: \varepsilon_{\hat{x}uv}}. \quad (14)$$

(Here I is the identity on all registers except X, Y .)

Since $\text{tr}(P_{C_1/C_2}^{EPR} \otimes I) \rho_{\hat{x}uv}^* = 1 - \varepsilon_{\hat{x}uv}$ by definition of $\varepsilon_{\hat{x}uv}$, Lemma 6 implies existence of a state $\rho_{\hat{x}uv}^{ideal}$ such that

$$\text{TD}(\rho_{\hat{x}uv}^*, \rho_{\hat{x}uv}^{ideal}) \leq \sqrt{\varepsilon_{\hat{x}uv}} \quad (15)$$

and

$$\rho_{\hat{x}uv}^{ideal} \text{ is a mixture over } \text{im}(P_{C_1/C_2}^{EPR} \otimes I) \quad (16)$$

Equation (16) implies that $\rho_{\hat{x}uv}^{ideal}$ is of the form $(\sum_x \frac{1}{|C_1/C_2|} |x\rangle\langle x| \otimes |x\rangle\langle x|) \otimes \rho_{rest}$. Note also that in the game “start with $\rho_{\hat{x}uv}^{ideal}$, $x \leftarrow$ measure Y with M_X , $b' \leftarrow B(x \oplus m_b \oplus \hat{x})$ ”, the adversary $B(x \oplus m_b \oplus \hat{x})$ operates only on ρ_{rest} . Thus x is uniformly distributed on C_1/C_2 and independent of the initial state of $B(x \oplus m_b \oplus \hat{x})$. Thus the return value of b' of $B(x \oplus m_b \oplus \hat{x})$ is independent of m_i , hence:

$$\begin{aligned}
&\Pr[b' = 1 : \text{start with } \rho_{\hat{x}uv}^{ideal}, x \leftarrow \text{measure } Y \text{ with } M_X, b' \leftarrow B(x \oplus m_0 \oplus \hat{x})] \\
&= \Pr[b' = 1 : \text{start with } \rho_{\hat{x}uv}^{ideal}, x \leftarrow \text{measure } Y \text{ with } M_X, b' \leftarrow B(x \oplus m_1 \oplus \hat{x})].
\end{aligned}$$

By (15), it follows that

$$\begin{aligned}
&|\Pr[b' = 1 : \text{start with } \rho_{\hat{x}uv}^*, x \leftarrow \text{measure } Y \text{ with } M_X, b' \leftarrow B(x \oplus m_0 \oplus \hat{x})] \\
&\quad - \Pr[b' = 1 : \text{start with } \rho_{\hat{x}uv}^*, x \leftarrow \text{measure } Y \text{ with } M_X, b' \leftarrow B(x \oplus m_1 \oplus \hat{x})]| \leq \sqrt{\varepsilon_{\hat{x}uv}}.
\end{aligned}$$

Or using abbreviations from above: $|\text{Succ}_{\hat{x}uv}^0 - \text{Succ}_{\hat{x}uv}^1| \leq \sqrt{\varepsilon_{\hat{x}uv}}$.

Thus

$$\begin{aligned}
&|\Pr[b' = 1 \wedge ok = 1 : \text{Game 5}(0)] - \Pr[b' = 1 \wedge ok = 1 : \text{Game 5}(1)]| \\
&\stackrel{(13)}{\leq} \sum_{\hat{x}, u, v} \Pr_{\hat{x}uv} |\text{Succ}_{\hat{x}uv}^0 - \text{Succ}_{\hat{x}uv}^1| \leq \sum_{\hat{x}, u, v} \Pr_{\hat{x}uv} \sqrt{\varepsilon_{\hat{x}uv}} \stackrel{(*)}{\leq} \sqrt{\sum_{\hat{x}, u, v} \Pr_{\hat{x}uv} \varepsilon_{\hat{x}uv}} \stackrel{(14)}{=} \sqrt{\varepsilon}.
\end{aligned}$$

Here $(*)$ uses Jensen’s inequality and the fact that $\sum_{\hat{x}, u, v} \Pr_{\hat{x}uv} \leq 1$. \square

Game 7 (Using fake timed-release encryption)

- (a) $(m_0, m_1) \leftarrow A_0()$.
- (b) $B \xleftarrow{\$} \{0, 1\}^q$. $Q \xleftarrow{\$} [q+n]_q$. $p \xleftarrow{\$} C_1/C_2$.
- (c) Initialize XY as $|0^{q+n}0^{q+n}\rangle$.
- (d) Apply $(H^B \otimes I_n)U_Q$ to Y .
- (e) Measure Y using M_{UV} , outcome u, v .
- (f) Measure Y using M_R , outcome r .
- (g) $\hat{B} \xleftarrow{\$} \{0, 1\}^q$. $\hat{Q} \xleftarrow{\$} [q+n]_q$. $\hat{r} \xleftarrow{\$} \{0, 1\}^q$. $V_0 \leftarrow \text{TRE}_0(\hat{B}, \hat{Q}, \hat{r}, p)$.
- (h) $\hat{x} \xleftarrow{\$} C_1/C_2$. Run $A_1(X, V_0, u, \hat{x} \oplus p)$.
- (i) Apply $(H^B \otimes I_n)U_Q$ to X .
- (j) Measure X using M_R , outcome r' . If $r = r'$, $ok := 1$, else $ok := 0$.
- (k) Apply $I_q \otimes U_{uv}^{EC}$ to X and $I_q \otimes U_{uv}^{dec}$ to Y . Measure XY using P_{C_1/C_2}^{EPR} , outcome $isEPR$.

Lemma 25 (Game 6 vs. Game 7) For some $\mu \in (2^{-2(k_1-k_2)} \cdot \text{negligible})$ we have

$$\Pr[ok = 1 \text{ and } isEPR = 0 : \text{Game 6}] \leq \Pr[ok = 1 \text{ and } isEPR = 0 : \text{Game 7}] + \mu.$$

Proof. First, consider an intermediate game G defined like Game 6, except that the following steps are performed *before* V_0 is computed: choosing $\hat{x} \xleftarrow{\$} C_1/C_2$, computing the argument $\hat{x} \oplus p$ of A_1 , measuring Y using M_R . Analogously G' is defined like Game 7, with the same modifications.

Then we immediately see that $\Pr[ok = 1 : G \wedge isEPR = 0 : G] = \Pr[ok = 1 \wedge isEPR = 0 : \text{Game 6}]$ and $\Pr[ok = 1 \wedge isEPR = 0 : G'] = \Pr[ok = 1 \wedge isEPR = 0 : \text{Game 7}]$ because only operations that operate on distinct variables/quantum registers are moved around.

Furthermore, in game G , after computing V_0 , we have an invocation of the $(T - \delta_T^{hid})$ -time adversary A_1 , q controlled Hadamard gates (H^B), an application of an already computed permutation on $q+n$ qubits (U_Q^\dagger), a q -qubit measurement in the computational basis (M_R on X), an n -bit equality test, the operations U_{uv}^{EC} , U_{uv}^{dec} , a measurement whether two n -qubit registers are in the state $\sum_{x \in C_1/C_2} |x\rangle|x\rangle$ (P_{C_1/C_2}^{EPR}), and a NOT- and an AND-gate (for evaluating $isEPR = 0 \wedge ok = 1$). Together, these steps take time at most T (by definition of δ_T^{hid} and our additivity assumptions on timing models, page 5).

Since TRE_0 is T -hiding with $(2^{-2(k_1-k_2)} \cdot \text{negligible})$ -security, replacing $\text{TRE}_0(B, Q, r, p)$ by $\text{TRE}_0(\hat{B}, \hat{Q}, \hat{r}, p)$ thus only changes $\Pr[isEPR = 0 \wedge ok = 1]$ by some $\mu \in (2^{-2(k_1-k_2)} \cdot \text{negligible})$.

Hence $\Pr[isEPR = 0 \wedge ok = 1 : G] \leq \Pr[isEPR = 0 \wedge ok = 1 : G'] + \mu$. \square

Game 8 (Delay basis choices)

- (a) $(m_0, m_1) \leftarrow A_0()$.
- (b) ~~$B \xleftarrow{\$} \{0, 1\}^q$. $Q \xleftarrow{\$} [q+n]_q$. $p \xleftarrow{\$} C_1/C_2$.~~
- (c) Initialize XY as $|0^{q+n}0^{q+n}\rangle$.
- (d) ~~Apply $(H^B \otimes I_n)U_Q$ to Y .~~
- (e) ~~Measure Y using M_{UV} , outcome u, v .~~
- (f) ~~Measure Y using M_R , outcome r .~~
- (g) $\hat{B} \xleftarrow{\$} \{0, 1\}^q$. $\hat{Q} \xleftarrow{\$} [q+n]_q$. $\hat{r} \xleftarrow{\$} \{0, 1\}^q$. $V_0 \leftarrow \text{TRE}_0(\hat{B}, \hat{Q}, \hat{r}, p)$.
- (h) $\hat{x} \xleftarrow{\$} C_1/C_2$. Run $A_1(X, V_0, u, \hat{x} \oplus p)$.
- (i) ~~$B \xleftarrow{\$} \{0, 1\}^q$. $Q \xleftarrow{\$} [q+n]_q$.~~
- (j) ~~Apply $(H^B \otimes I_n)U_Q$ to Y .~~
- (k) ~~Apply $(H^B \otimes I_n)U_Q$ to X .~~
- (l) ~~Measure Y using M_R , outcome r .~~
- (m) Measure X using M_R , outcome r' . If $r = r'$, $ok := 1$, else $ok := 0$.
- (n) ~~Measure Y using M_{UV} , outcome u, v .~~
- (o) Apply $I_q \otimes U_{uv}^{EC}$ to X and $I_q \otimes U_{uv}^{dec}$ to Y . Measure $X'Y'$ using P_{C_1/C_2}^{EPR} , outcome $isEPR$. (Here X', Y' refer to the last n qubits of X, Y , respectively.)

Lemma 26 (Game 7 vs. Game 8) $\Pr[ok = 1 \text{ and } isEPR = 0 : \text{Game 7}] = \Pr[ok = 1 \text{ and } isEPR = 0 : \text{Game 8}]$.

Proof. The difference between the two lemmas is simple swapping of lines of code. All involved quantum operations and measurements are on different registers X, Y , except for the measurements M_R and M_{UV} on Y which commute by definition of M_R, M_{UV} . \square

Game 9 (Measure t -error state)

- (a) $(m_0, m_1) \leftarrow A_0()$.
- (b) $p \stackrel{s}{\leftarrow} C_1/C_2$.
- (c) Initialize XY as $|0^{q+n}0^{q+n}\rangle$.
- (d) $\hat{B} \stackrel{s}{\leftarrow} \{0, 1\}^q$. $\hat{Q} \stackrel{s}{\leftarrow} [q+n]_q$. $\hat{r} \stackrel{s}{\leftarrow} \{0, 1\}^q$. $V_0 \leftarrow \text{TRE}_0(\hat{B}, \hat{Q}, \hat{r}, p)$.
- (e) $\hat{x} \stackrel{s}{\leftarrow} C_1/C_2$. Run $A_1(X, V_0, u, \hat{x} \oplus p)$.
- (f) $B \stackrel{s}{\leftarrow} \{0, 1\}^q$. $Q \stackrel{s}{\leftarrow} [q+n]_q$.
- (g) Apply $(H^B \otimes I_n)U_Q$ to Y .
- (h) Apply $(H^B \otimes I_n)U_Q$ to X .
- (i) Measure Y using M_R , outcome r .
- (j) Measure X using M_R , outcome r' . If $r = r'$, $ok := 1$, else $ok := 0$.
- (k) ~~Measure Y using M_{UV} , outcome u, v .~~
- (l) ~~Apply $I_q \otimes U_{uv}^{EC}$ to X and $I_q \otimes U_{uv}^{dec}$ to Y . Measure $X'Y'$ using P_{C_1/C_2}^{EPR} , outcome is EPR .~~
- (m) Measure $X'Y'$ using P_t^{EPR} , outcome is EPR .

Lemma 27 (Decoding tested EPR states) For any state ρ of $X'Y'$ and with

$$\begin{aligned} pr_1 &:= \Pr[\text{isEPR} = 1 : \text{start with } \rho, \text{isEPR} \leftarrow \text{measure using } P_t^{EPR}] \\ pr_2 &:= \Pr[\text{isEPR} = 1 : \text{start with } \rho, (u, v) \leftarrow \text{measure using } I_n \otimes M_{UV}, \\ &\quad \text{apply } U_{uv}^{EC} \otimes U_{uv}^{dec}, \text{isEPR} \leftarrow \text{measure using } P_{C_1/C_2}^{EPR}] \end{aligned}$$

we have $pr_1 \leq pr_2$. (Here we write in slight abuse of notation M_{UV} for the restriction of M_{UV} to $X'Y'$. Since M_{UV} ignores the first q qubits of X, Y anyway, this restriction is well-defined. And by ‘‘measure using P_{C_1/C_2}^{EPR} ’’, we mean applying P_{C_1/C_2}^{EPR} to the first n qubits of the outputs of U_{uv}^{EC} and U_{uv}^{dec} .)

Proof. It is sufficient to show the inequality for pure states ρ , all other density operators are convex combinations of pure states and the probabilities pr_1, pr_2 are then the corresponding convex combinations of the probabilities for the pure states. We thus assume $\rho = |\Psi\rangle\langle\Psi|$.

Let U be the purification of the steps ‘‘ $(u, v) \leftarrow$ measure using $I_n \otimes M_{UV}$, apply $U_{uv}^{EC} \otimes U_{uv}^{dec}$ ’’. I.e., the result of applying these steps to an initial state $|\psi\rangle\langle\psi|$ is $\text{tr}_H(U|\psi\rangle\langle\psi|0^m)\langle\langle\psi|0^m|U^\dagger)$ where H refers to some auxiliary system of dimension m .

We then have that

$$\begin{aligned} pr_1 &= \left\| \overbrace{(P_t^{EPR} \otimes |0^m\rangle\langle 0^m|)|\Psi\rangle\langle\Psi|0^m}^{=:P_1} \right\|^2 \\ pr_2 &= \left\| \overbrace{(P_{C_1/C_2}^{EPR} \otimes I_m)U|\Psi\rangle\langle\Psi|0^m}^{=:P_2} \right\|^2 = \left\| U^\dagger(P_{C_1/C_2}^{EPR} \otimes I_m)U|\Psi\rangle\langle\Psi|0^m \right\|^2 \end{aligned}$$

P_1 and P_2 are orthogonal projectors, thus to show $pr_1 \leq pr_2$, it is sufficient to show $\text{im } P_1 \subseteq \text{im } P_2$. By definition of P_t^{EPR} we have $\text{im } P_t^{EPR} = \text{span}\{|\tilde{f}e\rangle : \omega(f), \omega(e) \leq t\}$ (where f, e are n -bit strings). We thus have that $\text{im } P_1 = \text{span}\{|\tilde{f}e\rangle|0^m\rangle : \omega(f), \omega(e) \leq t\}$. Thus to show $\text{im } P_1 \subseteq \text{im } P_2$, it is sufficient to show that $|\tilde{f}e\rangle|0^m\rangle \in \text{im } P_2$ for $\omega(f), \omega(e) \leq t$. For the rest of the proof, fix such f, e .

Since $|\beta_{ij}\rangle = (Z^i X^j \otimes I_1)|\beta_{00}\rangle$, it follows that $|\tilde{f}e\rangle = (Z^f X^e \otimes I_n)|0^n 0^n\rangle$.

And by Lemma 18, we have that $2^{-n/2} \sum_{x,u,v} |\xi_{xuv}\rangle \otimes |\xi_{xuv}\rangle = |\widetilde{0^n 0^n}\rangle$. Hence $|\tilde{f}e\rangle = 2^{-n/2} \sum_{x,u,v} Z^f X^e |\xi_{xuv}\rangle \otimes |\xi_{xuv}\rangle$. Since all $|\xi_{xuv}\rangle$ are orthogonal (Lemma 17), we have for any u, v that the unnormalized post-measurement state after measuring $|\tilde{f}e\rangle$ using $I_n \otimes M_{UV}$ with outcome (u, v) is $|\Psi_{uv}\rangle := (I_n \otimes P_{uv})|\tilde{f}e\rangle = 2^{-n/2} \sum_x Z^f X^e |\xi_{xuv}\rangle \otimes |\xi_{xuv}\rangle$.

Since f, e have Hamming weight $\leq t$, by definition of U_{uv}^{EC} and U_{uv}^{dec} we have $U_{uv}^{EC} Z^f X^e |\xi_{xuv}\rangle = \pm U_{uv}^{EC} X^e Z^f |\xi_{xuv}\rangle = \pm |x\rangle \otimes |\Phi_{uvfe}\rangle$ and $U_{uv}^{dec} |\xi_{xuv}\rangle = |x\rangle \otimes |\Phi'_{uvfe}\rangle$ for some quantum states $|\Phi_{uvfe}\rangle, |\Phi'_{uvfe}\rangle$. Thus the unnormalized state after additionally applying $(U_{uv}^{EC} \otimes U_{uv}^{dec})$ to $|\Psi_{uv}\rangle$ is

$$|\Psi'_{uv}\rangle := (U_{uv}^{EC} \otimes U_{uv}^{dec})|\Psi_{uv}\rangle = 2^{-n/2} \sum_x \pm |x\rangle \otimes |\Phi_{uvfe}\rangle \otimes |x\rangle \otimes |\Phi'_{uvfe}\rangle \in \text{im } P_{C_1/C_2}^{EPR}.$$

Let ρ' denote the state after applying the steps ‘‘ $(u, v) \leftarrow$ measure using $I_n \otimes M_{UV}$, apply $U_{uv}^{EC} \otimes U_{uv}^{dec}$ ’’ to the initial state $|\tilde{f}e\rangle\langle\tilde{f}e|$. Then $\rho' = \sum_{uv} |\Psi'_{uv}\rangle\langle\Psi'_{uv}|$. Thus

$$\text{tr } P_{C_1/C_2}^{EPR} \rho' = \sum_{uv} \text{tr } P_{C_1/C_2}^{EPR} |\Psi'_{uv}\rangle\langle\Psi'_{uv}| = \sum_{uv} \text{tr } |\Psi'_{uv}\rangle\langle\Psi'_{uv}| = 1$$

By definition of U , we have that $\text{tr}_H(U|\widetilde{f}e\rangle|0^m\rangle)(\langle\widetilde{f}e|0^m|U^\dagger) = \rho'$. Hence $\text{tr}(P_{C_1/C_2}^{EPR} \otimes I_m)(U|\widetilde{f}e\rangle|0^m\rangle)(\langle\widetilde{f}e|0^m|U^\dagger) = 1$. Thus $U|\widetilde{f}e\rangle|0^m\rangle \in \text{im}(P_{C_1/C_2}^{EPR} \otimes I_m)$. And thus finally $|\widetilde{f}e\rangle|0^m\rangle \in \text{im}U^\dagger(P_{C_1/C_2}^{EPR} \otimes I)U = \text{im}P_2$.

We have thus shown that $\text{im}P_1 \subseteq \text{im}P_2$, and as discussed above, this implies $pr_1 \leq pr_2$. \square

Lemma 28 (Game 8 vs. Game 9) $\Pr[ok = 1 \text{ and } isEPR = 0 : \text{Game 8}] \leq \Pr[ok = 1 \text{ and } isEPR = 0 : \text{Game 9}]$.

Proof. To show this claim, let ρ' denote the state in Game 8 right before step (n) (i.e. before measuring u, v), conditioned on $ok = 1$. And let ρ denote the result of tracing out in ρ' all but the last n qubits of X and Y . (I.e., ρ describes the last n qubits of X and Y conditioned on $ok = 1$ before step (n).)

Then with pr_1, pr_2 as in Lemma 27, we have

$$\begin{aligned} & \Pr[ok = 1 \text{ and } isEPR = 0 : \text{Game 8}] \\ &= \Pr[isEPR = 0 | ok = 1 : \text{Game 8}] \cdot \Pr[ok = 1 : \text{Game 8}] \\ &\leq \Pr[isEPR = 0 | ok = 1 : \text{Game 8}] \\ &= (1 - pr_2) \Pr[ok = 1 : \text{Game 8}] \stackrel{(*)}{\leq} (1 - pr_1) \Pr[ok = 1 : \text{Game 9}] \\ &\stackrel{(**)}{=} \Pr[isEPR = 0 | ok = 1 : \text{Game 9}] \cdot \Pr[ok = 1 : \text{Game 9}] \\ &= \Pr[ok = 1 \text{ and } isEPR = 0 : \text{Game 9}]. \end{aligned}$$

Here $(*)$ uses that $pr_1 \leq pr_2$ by Lemma 27, and that $\Pr[ok = 1]$ is identical in Game 8 and Game 9 because up to the measurement of ok , these games are identical.

And $(**)$ uses the fact that ρ is also the state in Game 9 right before the measurement of u, v , conditioned on $ok = 1$. \square

Lemma 29 (ok implies $isEPR$) *Let ρ be the initial state of a bipartite system XY where X and Y are $q + n$ -qubits each.*

Consider the following game: Pick $B \stackrel{s}{\leftarrow} \{0, 1\}^q, Q \stackrel{s}{\leftarrow} [q + n]_q$. Apply $(H^B \otimes I_n)U_Q$ to X and to Y . Then measure X and Y with M_R , outcomes r', r . Let $ok := 1$ iff $r = r'$. Then measure $X'Y'$ using P_t^{EPR} , outcome $isEPR$. (Recall: $X'Y'$ are the last n qubit pairs of XY .)

Then $\Pr[ok = 1 \wedge isEPR = 0] \leq 3\sqrt{q}(1 - \frac{q}{2(q+n)})^{t+1}$.

Proof. We first consider the case that $\rho = |\widetilde{f}e\rangle\langle\widetilde{f}e|$ with $\omega(f) > t$ or $\omega(e) > t$.

Note that when measuring both qubits of $|\beta_{01}\rangle$ or $|\beta_{11}\rangle$ in the computational basis, the outcomes will be different with probability 1. Furthermore, note that $(H \otimes H)|\beta_{10}\rangle = |\beta_{01}\rangle$ and $(H \otimes H)|\beta_{11}\rangle = -|\beta_{11}\rangle$.

For a given $Q = \{Q_1, \dots, Q_q\}$ and $B = B_1 \dots B_n$, we have for all i :

- If $f_{Q_i} = 1$ and $B_i = 1$, then $r_i \neq r'_i$ with probability 1. (Because in this case the i -th qubit pair of XY after applying U_Q to X, Y is $|\beta_{f_{Q_i}e_{Q_i}}\rangle \in \{|\beta_{10}\rangle, |\beta_{11}\rangle\}$, and after additionally applying $(H^B \otimes I_n)$ to X, Y , it the i -th qubit pair is $(H \otimes H)|\beta_{f_{Q_i}e_{Q_i}}\rangle \in \{|\beta_{01}\rangle, -|\beta_{11}\rangle\}$. And r_i, r'_i are the outcomes of measuring this qubit pair in the computational basis. Hence $r_i \neq r'_i$.)
- If $e_{Q_i} = 1$ and $B_i = 0$, then $r_i \neq r'_i$ with probability 1. (Because in this case the i -th qubit pair of XY after applying U_Q to X, Y is $|\beta_{f_{Q_i}e_{Q_i}}\rangle \in \{|\beta_{01}\rangle, |\beta_{11}\rangle\}$, and after additionally applying $(H^B \otimes I_n)$ to X, Y , it the i -th qubit pair is $(H^0 \otimes H^0)|\beta_{f_{Q_i}e_{Q_i}}\rangle \in \{|\beta_{01}\rangle, |\beta_{11}\rangle\}$. And r_i, r'_i are the outcomes of measuring this qubit pair in the computational basis. Hence $r_i \neq r'_i$.)

In the notation of Lemma 3, the probability that there is no i such that Q, B satisfying one of these cases is written $P(x)$, where $x^0 := e$ and $x^1 := f$. Thus

$$\begin{aligned} \Pr[ok = 1 \wedge isEPR = 0] &\leq \Pr[ok = 1] \leq P(x) \stackrel{(*)}{\leq} 3\sqrt{q}(1 - \frac{q}{2(q+n)})^{t+1} =: \gamma \\ &\text{if } \rho = |\widetilde{f}e\rangle\langle\widetilde{f}e| \text{ with } \omega(f) > t \text{ or } \omega(e) > t. \end{aligned} \quad (17)$$

Here $(*)$ uses Lemma 3.

Now we consider the case that $\rho = |\widetilde{f}e\rangle\langle\widetilde{f}e|$ with $\omega(f), \omega(e) \leq t$. In this case, after applying $(H^B \otimes I_n)U_Q$ to both X and Y and after measuring the first q qubits in X and Y (measurement M_R), the state of the last n qubit pairs of XY is $|\widetilde{f}'e'\rangle$ where f' is a subsequence of f and e' a subsequence of e .

In particular $\omega(e') \leq \omega(e) \leq t$ and $\omega(f') \leq \omega(f) \leq t$. Thus the measurement P_t^{EPR} will succeed with probability 1, hence

$$\Pr[ok = 1 \wedge isEPR = 0] \leq \Pr[isEPR = 0] = 0 \leq \gamma \quad \text{if } \rho = |\widetilde{fe}\rangle\langle\widetilde{fe}| \text{ with } \omega(f), \omega(e) \leq t.$$

Together with (17), we have

$$\Pr[ok = 1 \wedge isEPR = 0] \leq \gamma \quad \text{if } \rho = |\widetilde{fe}\rangle\langle\widetilde{fe}| \text{ for some } f, e \in \{0, 1\}^{q+n} \quad (18)$$

Now we consider the case that $\rho = \sum_i \alpha_i |e_i \widetilde{f_i}\rangle\langle e_i \widetilde{f_i}|$ for some $f_i, e_i \in \{0, 1\}^{q+n}$ and $\alpha_i \geq 0$, $\sum \alpha_i = 1$. Then

$$\begin{aligned} \Pr[ok = 1 \wedge isEPR = 0] \\ = \sum \alpha_i \Pr[ok = 1 \wedge isEPR = 0 : \text{using } \rho := |e_i \widetilde{f_i}\rangle\langle e_i \widetilde{f_i}|] &\stackrel{(18)}{\leq} \sum \alpha_i \gamma = \gamma \\ &\text{if } \rho = \sum_i \alpha_i |e_i \widetilde{f_i}\rangle\langle e_i \widetilde{f_i}| \quad (19) \end{aligned}$$

Now consider the general case of an arbitrary density operator ρ . Let P_{eq} be the projector that measures whether the first q qubit pairs have the same value in the computational basis. I.e., $P_{eq} := \sum_{x, y_1, y_2} |xy_1\rangle\langle xy_1| \otimes |xy_2\rangle\langle xy_2|$ with $x \in \{0, 1\}^q$, $y_1, y_2 \in \{0, 1\}^n$.

Note that P_{eq} is a tensor product of projectors $P_{eq}^1 := |00\rangle\langle 00| + |11\rangle\langle 11|$ and identities. Furthermore, one can check that $P_{eq}^1 = |\beta_{00}\rangle\langle\beta_{00}| + |\beta_{10}\rangle\langle\beta_{10}|$. Thus P_{eq} is diagonal in the Bell basis.

And P_t^{EPR} is diagonal in the Bell basis by definition.

Let M_{Bell} be a complete measurement in the Bell basis. I.e., $M_{Bell} := \{|\widetilde{fe}\rangle\langle\widetilde{fe}|\}_{f, e \in \{0, 1\}^{q+n}}$. Since M_{Bell} is diagonal in the Bell basis, it commutes with P_{eq} and P_t^{EPR} .

Furthermore, since $U_Q \otimes U_Q$ only reorders the qubit pairs, M_{Bell} and $(U_Q \otimes U_Q)$ commute if we discard the result of M_{Bell} . (Otherwise, the outcome of M_{Bell} would have to be additionally permuted.)

And since $(H \otimes H)|\beta_{ij}\rangle = \pm|\beta_{ji}\rangle$, we have that $(H^B \otimes I_n \otimes H^B \otimes I_n)$ commutes with M_{Bell} if we discard the outcome of M_{Bell} . (Otherwise, the bit pairs with $B_i = 1$ in the outcome of M_{Bell} would need to be swapped.)

Thus M_{Bell} commutes with applying $(H^B \otimes I_n)U_Q$ to both X and Y .

Let ρ^* be the state we get when measuring ρ using M_{Bell} and discarding the outcome. Then $\rho^* = \sum_i \alpha_i |f_i e_i\rangle\langle f_i e_i|$ for some α_i, f_i, e_i with $\alpha_i \geq 0$, $\sum \alpha_i = 1$.

We then have

$$\begin{aligned} \Pr[ok = 1 \wedge isEPR = 0 : B \stackrel{\$}{\leftarrow} \{0, 1\}^q, Q \stackrel{\$}{\leftarrow} [q+n]_q, \text{ apply } (H^B \otimes I_n)U_Q \text{ to } X, Y, \\ r, r' \leftarrow \text{measure } X, Y \text{ with } M_R, ok := (r = r'), isEPR \leftarrow \text{measure } X'Y' \text{ with } P_t^{EPR}] \\ \stackrel{(*)}{=} \Pr[ok = 1 \wedge isEPR = 0 : B \stackrel{\$}{\leftarrow} \{0, 1\}^q, Q \stackrel{\$}{\leftarrow} [q+n]_q, \text{ apply } (H^B \otimes I_n)U_Q \text{ to } X, Y, \\ ok \leftarrow \text{measure } XY \text{ with } P_{eq}, isEPR \leftarrow \text{measure } X'Y' \text{ with } P_t^{EPR}] \\ = \Pr[ok = 1 \wedge isEPR = 0 : B \stackrel{\$}{\leftarrow} \{0, 1\}^q, Q \stackrel{\$}{\leftarrow} [q+n]_q, \text{ apply } (H^B \otimes I_n)U_Q \text{ to } X, Y, \\ ok \leftarrow \text{measure } XY \text{ with } P_{eq}, isEPR \leftarrow \text{measure } X'Y' \text{ with } P_t^{EPR}, \text{ measure } XY \text{ with } M_{Bell}] \\ \stackrel{(**)}{=} \Pr[ok = 1 \wedge isEPR = 0 : \text{measure } XY \text{ with } M_{Bell}, B \stackrel{\$}{\leftarrow} \{0, 1\}^q, Q \stackrel{\$}{\leftarrow} [q+n]_q, \text{ apply } (H^B \otimes I_n)U_Q \text{ to } X, Y, \\ ok \leftarrow \text{measure } XY \text{ with } P_{eq}, isEPR \leftarrow \text{measure } X'Y' \text{ with } P_t^{EPR}, \text{ measure } XY \text{ with } M_{Bell}] \\ = \Pr[ok = 1 \wedge isEPR = 0 : \text{use } \rho^* \text{ instead of } \rho, B \stackrel{\$}{\leftarrow} \{0, 1\}^q, Q \stackrel{\$}{\leftarrow} [q+n]_q, \text{ apply } (H^B \otimes I_n)U_Q \text{ to } X, Y, \\ ok \leftarrow \text{measure } XY \text{ with } P_{eq}, isEPR \leftarrow \text{measure } X'Y' \text{ with } P_t^{EPR}] \\ \stackrel{(***)}{\leq} \gamma. \end{aligned}$$

Here (*) uses that P_{eq} and M_R only operate on the first q qubit pairs, and thus do not touch $X'Y'$.

And (**) uses that M_{Bell} commutes with applying $(H^B \otimes I_n)U_Q$, with P_t^{EPR} , and with P_{eq} as discussed above.

And (***) uses Equation 19 and the fact that ρ^* is of the form $\sum_i \alpha_i |e_i \widetilde{f_i}\rangle\langle e_i \widetilde{f_i}|$.

Since the left hand side of the preceding calculation is the probability $\Pr[ok = 1 \wedge isEPR = 0]$ from the statement of the lemma, the lemma follows. \square

Lemma 30 (*ok implies isEPR in Game 9*) $\Pr[ok = 1 \text{ and } isEPR = 0 : \text{Game 9}] \leq 3\sqrt{q} \left(1 - \frac{q}{2(q+n)}\right)^{t+1}$.

Proof. To show this claim, let ρ denote the state in Game 9 right before choosing B, Q (step (f)). Then the game in Lemma 29 is identical to Game 9. Thus by Lemma 29, we have

$$\Pr[ok = 1 \wedge isEPR = 0 : \text{Game 9}] \leq 3\sqrt{q} \left(1 - \frac{q}{2(q+n)}\right)^{t+1}. \quad \square$$

We can now finally prove the security of RTRE_{hid} :

Proof of Theorem 3. Game 1 describes the game played by the adversary according to Definition 5. We thus need to show that

$$\mu := |\Pr[b' = 1 \wedge ok = 1 : \text{Game 1}(0)] - \Pr[b' = 1 \wedge ok = 1 : \text{Game 1}(1)]|$$

is negligible. Note that $|C_1/C_2| = 2^{k_1-k_2}$. By Lemma 20, we get

$$\mu = 2^{k_1-k_2} |\Pr[b' = 1 \wedge ok = 1 : \text{Game 2}(0)] - \Pr[b' = 1 \wedge ok = 1 : \text{Game 2}(1)]|.$$

By Lemmas 21, 22, and 23 it follows that

$$\mu = 2^{k_1-k_2} |\Pr[b' = 1 \wedge ok = 1 : \text{Game 5}(0)] - \Pr[b' = 1 \wedge ok = 1 : \text{Game 5}(1)]|.$$

By Lemma 24 we have

$$\mu \leq 2^{k_1-k_2} \sqrt{\varepsilon} \quad \text{with} \quad \varepsilon := \Pr[ok = 1 \wedge isEPR = 0 : \text{Game 6}].$$

By Lemma 25 we have for some $\mu_1 \in (2^{-2(k_1-k_2)} \cdot \text{negligible})$:

$$\varepsilon \leq \Pr[ok = 1 \wedge isEPR = 0 : \text{Game 7}] + \mu_1.$$

By Lemmas 26 and 28,

$$\varepsilon \leq \Pr[ok = 1 \wedge isEPR = 0 : \text{Game 9}] + \mu_1$$

and by Lemma 30, we have

$$\varepsilon \leq 3\sqrt{q} \left(1 - \frac{q}{2(q+n)}\right)^{t+1} + \mu_1$$

where n, t, q are parameters of the protocol. So altogether,

$$\mu \leq \sqrt{\underbrace{2^{2(k_1-k_2)} \cdot 3\sqrt{q} \left(1 - \frac{q}{2(q+n)}\right)^{t+1} + 2^{2(k_1-k_2)} \mu_1}_{=: \mu_2}}. \quad (20)$$

We have that $2^{2(k_1-k_2)} \mu_1$ is negligible by choice of μ_1 .

To show that μ_2 is negligible, let $\ell := k_1 - k_2$ and observe that

$$\begin{aligned} \mu_2 / (3\sqrt{q}) &\leq 2^{2\ell} \left(1 - \frac{q}{2(q+n)}\right)^t = 2^{2\ell} \underbrace{\left(1 - \frac{q}{2(q+n)}\right)^{2(q+n)/q}}_{\leq 1/e \text{ (*)}}^{tq/(2(q+n))} \\ &\leq 2^{2\ell} e^{-tq/(2(q+n))} = e^{-\frac{1}{2}(tq/(q+n) - 4\ell \ln 2)} \end{aligned}$$

Here (*) uses the fact that $(1 - 1/x)^x$ is increasing for $x \geq 1$ and tends to $1/e$. Since $tq/(q+n) - 4\ell \ln 2$ is superlogarithmic (condition in the statement of Theorem 3), $\mu_2/(3\sqrt{q})$ is negligible. Since q is polynomially bounded, μ_2 is negligible.

Thus both summands below the square root in (20) are negligible, hence μ is negligible. Thus RTRE_{hid} is $(T - \delta_T^{hid})$ -revocably hiding.

Note that (20) also tells us the concrete security of RTRE_{hid} . Namely, when μ_1 is the advantage of an adversary against TRE_0 (that runs only a small additive amount longer than the original adversary (A_0, A_1, A_2) ; it consists of the code in Game 7), then the right hand side of (20) bounds the advantage of (A_0, A_1, A_2) against RTRE_{hid} . \square

Hiding. Note that revocable hiding does not immediately imply hiding. However, due to the one-time-pad p used in RTRE_{hid} , it is easy to show that RTRE_{hid} is hiding:

Theorem 9 (RTRE_{hid} is hiding) *The protocol RTRE_{hid} from Definition 9 is T -hiding.*

The proof is completely analogous to that of Theorem 8.

E Full proofs: one-way to hiding

Lemma 31 (One-way to hiding) *Let $H : \{0, 1\}^n \rightarrow \{0, 1\}^m$ be a random oracle. Consider an oracle algorithm A that makes at most q queries to H . Let B be an oracle algorithm that on input x does the following: pick $i \stackrel{\$}{\leftarrow} \{1, \dots, q\}$ and $y \stackrel{\$}{\leftarrow} \{0, 1\}^m$, run $A^H(x, y)$ until (just before) the i -th query, measure the argument of the query in the computational basis, output the measurement outcome. (When A makes less than i queries, B outputs $\perp \notin \{0, 1\}^n$.)*

Let

$$\begin{aligned} P_A^1 &:= \Pr[b' = 1 : H \stackrel{\$}{\leftarrow} (\{0, 1\}^n \rightarrow \{0, 1\}^m), x \leftarrow \{0, 1\}^n, b' \leftarrow A^H(x, H(x))] \\ P_A^2 &:= \Pr[b' = 1 : H \stackrel{\$}{\leftarrow} (\{0, 1\}^n \rightarrow \{0, 1\}^m), x \leftarrow \{0, 1\}^n, y \stackrel{\$}{\leftarrow} \{0, 1\}^m, b' \leftarrow A^H(x, y)] \\ P_B &:= \Pr[x = x' : H \stackrel{\$}{\leftarrow} (\{0, 1\}^n \rightarrow \{0, 1\}^m), x \leftarrow \{0, 1\}^n, x' \leftarrow B^H(x)] \end{aligned}$$

Then $|P_A^1 - P_A^2| \leq 2q\sqrt{P_B}$.

Proof. We assume that the state of A is composed of three quantum systems A, K, V . Then an execution of A leads to the final state $(UO_H)^q |\Psi_{xy}\rangle$ where $|\Psi_{xy}\rangle$ is an input dependent initial state, $O_H : |a, k, v\rangle \mapsto |a, k, v \oplus H(k)\rangle$ is an oracle query, and U is A 's state transition operation. A 's output is produced by applying a measurement M to A 's final state.

We define $|\Psi_{Hxy}^i\rangle := (UO_H)^i |\Psi_{xy}\rangle$. Then

$$P_A^2 = \sum_{Hxy} \alpha \underbrace{\Pr[M \text{ outputs } 1 \text{ on state } |\Psi_{Hxy}^q\rangle]}_{=: b_{Hxy}}. \quad (21)$$

where $\alpha := 2^{-m2^n - n - m}$ (i.e., the probability of each particular triple Hxy).

Furthermore, we see that

$$P_A^1 = \Pr[b' = 1 : H \stackrel{\$}{\leftarrow} (\{0, 1\}^n \rightarrow \{0, 1\}^m), x \stackrel{\$}{\leftarrow} \{0, 1\}^n, y \stackrel{\$}{\leftarrow} \{0, 1\}^m, b' \leftarrow A^{H_{xy}}(x, y)]$$

where H_{xy} denotes the function with $H_{xy}(x) = y$ and $H_{xy} = H$ everywhere else. Thus

$$P_A^1 = \sum_{Hxy} \alpha b_{H_{xy}xy}. \quad (22)$$

And in our notation, we can describe B as follows: $B^H(x)$ picks $i \stackrel{\$}{\leftarrow} \{1, \dots, q\}$ and $y \stackrel{\$}{\leftarrow} Y$, measures the quantum system K of the state $|\Psi_{Hxy}^i\rangle$, and outputs the result. Thus

$$P_B = \sum_{Hxyi} \frac{\alpha}{q} \|Q_x |\Psi_{Hxy}^i\rangle\|^2 \quad (23)$$

where Q_x is the orthogonal projector projecting K onto $|x\rangle$. (I.e., $\|Q_x |\Psi_{Hxy}^i\rangle\|^2$ is the probability of measuring x in K in $|\Psi_{Hxy}^i\rangle$.)

For fixed H, x, y , let $D_i := \text{TD}(|\Psi_{Hxy}^i\rangle, |\Psi_{H_{xy}xy}^i\rangle)$. Since the trace distance bounds how well a measurement can distinguish between two states, $|b_{Hxy} - b_{H_{xy}xy}| \leq D_q$. And $D_0 = \text{TD}(|\Psi_{xy}\rangle, |\Psi_{xy}\rangle) = 0$ and

$$\begin{aligned} D_i &= \text{TD}(UO_H |\Psi_{Hxy}^{i-1}\rangle, UO_{H_{xy}} |\Psi_{H_{xy}xy}^{i-1}\rangle) \\ &\leq \text{TD}(UO_H |\Psi_{Hxy}^{i-1}\rangle, UO_{H_{xy}} |\Psi_{Hxy}^{i-1}\rangle) + \text{TD}(UO_{H_{xy}} |\Psi_{Hxy}^{i-1}\rangle, UO_{H_{xy}} |\Psi_{H_{xy}xy}^{i-1}\rangle) \\ &= \text{TD}(O_H |\Psi_{Hxy}^{i-1}\rangle, O_{H_{xy}} |\Psi_{Hxy}^{i-1}\rangle) + D_{i+1}. \end{aligned}$$

Hence

$$|b_{Hxy} - b_{Hxyxy}| \leq D_q \leq \sum_{i=1}^q \text{TD}(O_H|\Psi_{Hxy}^{i-1}\rangle, O_{Hxy}|\Psi_{Hxy}^{i-1}\rangle). \quad (24)$$

Let $V_y|a, k, v\rangle := |a, k, v \oplus y\rangle$. Then $O_{Hxy} = O_H(1 - Q_x) + V_yQ_x$. (This can be verified by checking the equation for all basis states $|a, k, v\rangle$.) From this we get

$$\begin{aligned} & \text{TD}(O_H|\Psi_{Hxy}^{i-1}\rangle, O_{Hxy}|\Psi_{Hxy}^{i-1}\rangle) \\ &= \text{TD}(O_H(1 - Q_x)|\Psi_{Hxy}^{i-1}\rangle + O_HQ_x|\Psi_{Hxy}^{i-1}\rangle, \\ & \quad O_H(1 - Q_x)|\Psi_{Hxy}^{i-1}\rangle + V_yQ_x|\Psi_{Hxy}^{i-1}\rangle) \\ & \stackrel{(*)}{\leq} 2\|O_HQ_x|\Psi_{Hxy}^{i-1}\rangle\| = 2\|Q_x|\Psi_{Hxy}^{i-1}\rangle\|. \end{aligned} \quad (25)$$

Here (*) uses Lemma 7 and the fact that the left summands in the second trace distance (which are in the image of $(1 - Q_x)$) are orthogonal to the right summands (which are in the image of Q_x).

Thus

$$\begin{aligned} |P_A^1 - P_A^2| & \stackrel{(21,22)}{\leq} \sum_{Hxy} \alpha |b_{Hxy} - b_{Hxyxy}| \stackrel{(24)}{\leq} \sum_{Hxyi} \alpha \text{TD}(O_H|\Psi_{Hxy}^{i-1}\rangle, O_{Hxy}|\Psi_{Hxy}^{i-1}\rangle) \\ & \stackrel{(25)}{\leq} \sum_{Hxyi} \alpha 2\|Q_x|\Psi_{Hxy}^{i-1}\rangle\| \stackrel{(*)}{\leq} 2 \sum_i \sqrt{\sum_{Hxy} \alpha \|Q_x|\Psi_{Hxy}^{i-1}\rangle\|^2} \stackrel{(23)}{=} 2q \cdot \sqrt{P_B}. \end{aligned}$$

Here (*) uses Jensen's inequality. \square

Theorem 10 (Hiding timed-release encryptions) *Let $H : \{0, 1\}^n \rightarrow \{0, 1\}^m$ be a random oracle. Let TRE be a (revocable or non-revocable) timed-release encryption with message space $\{0, 1\}^n$ (not using H).*

Let TRE' be the following timed-release encryption (with message space $\{0, 1\}^m$):

- **Encryption:** TRE'(m) runs $k \xleftarrow{\$} \{0, 1\}^n$, $V' \leftarrow \text{TRE}(k)$, and then returns $V := (V', m \oplus H(k))$.
- **Decryption:** Given $V = (V', c)$, run the decryption of TRE on V' , resulting in k . Then return $c \oplus H(k)$.
- **Revocation (if TRE is revocable):** Identical to the revocation protocol of TRE.

The we have

- (i) *If TRE is T-one-way and T-revocably one-way then TRE' is T-revocably hiding.*
- (ii) *If TRE is T-one-way then TRE' is T-hiding.*
- (iii) *If TRE is T-one-way without offline-queries and T-revocably one-way without offline-queries then TRE' is T-revocably hiding without offline-queries.*
- (iv) *If TRE is T-one-way without offline-queries then TRE' is T-hiding without offline-queries.*

Both statements hold both for the parallel and the sequential oracle-query timing model.²¹

Proof. We first show (i): if TRE is T-one-way and T-revocably one-way, then TRE' is T-revocably hiding.

Fix an adversary (A_0, A_1, A_2) against the T-revocably hiding property of TRE'. Since A_0, A_1, A_2 all run in sequential-polynomial-time, there are polynomially bounded q_0, q_1, q_2 such that q_i bounds the number of oracle calls performed by A_i . Without loss of generality, we assume that A_i makes exactly q_i queries. We abbreviate the set of functions $(\{0, 1\}^n \rightarrow \{0, 1\}^m)$ as *Fun*. By definition of revocably hiding (Definition 5) and of TRE', we have to show that μ is negligible where

$$\mu := |\Pr[b' = 1 \wedge ok = 1 : \text{Game 1}(0)] - \Pr[b' = 1 \wedge ok = 1 : \text{Game 1}(1)]|$$

with the following game:

Game 1 (Original game)

- (a) *In this game, $b \in \{0, 1\}$ is a parameter of the game.*
- (b) $H \xleftarrow{\$} \text{Fun}$.
- (c) $k \xleftarrow{\$} \{0, 1\}^n$.
- (d) $(m_0, m_1) \leftarrow A_0^H()$.

²¹For other timing models, the reduction described in the proof may incur an overhead, leading to a smaller T for TRE'.

- (e) $V' \leftarrow \text{TRE}(k)$.
- (f) $m := m_b \oplus H(k)$.
- (g) Run the revocation protocol of TRE, with $A_1^H(V', m)$ as recipient. Let ok be the honest sender's output.
- (h) If $ok = 1$, $b' \leftarrow A_2^H()$, else $b' := 0$.

Note that this game somewhat differs from that from Definition 5: if $ok = 0$, we do not run A_2 . However, this does not change the probability that $b' = 1 \wedge ok = 1$.

Let A be the algorithm that on input (b, k, h) and with oracle access to H performs steps (d)-(h) from Game 1(b) but using h instead of $H(k)$ in (f). A then outputs 1 iff $b' = 1 \wedge ok = 1$.

Let

$$\varepsilon_b := |\Pr[b'' = 1 : H \stackrel{\$}{\leftarrow} \text{Fun}, k \stackrel{\$}{\leftarrow} \{0, 1\}^n, b'' \leftarrow A(b, k, H(k))] \\ - \Pr[b'' = 1 : H \stackrel{\$}{\leftarrow} \text{Fun}, k \stackrel{\$}{\leftarrow} \{0, 1\}^n, y \stackrel{\$}{\leftarrow} \{0, 1\}^m, b'' \leftarrow A(b, k, y)]|.$$

We then have

$$\begin{aligned} & \Pr[b' = 1 \wedge ok = 1 : \text{Game 1}(0)] \\ & \stackrel{(*)}{=} \Pr[b'' = 1 : H \stackrel{\$}{\leftarrow} \text{Fun}, k \stackrel{\$}{\leftarrow} \{0, 1\}^n, b'' \leftarrow A(0, k, H(k))] \\ & \stackrel{\varepsilon_0}{\approx} \Pr[b'' = 1 : H \stackrel{\$}{\leftarrow} \text{Fun}, k \stackrel{\$}{\leftarrow} \{0, 1\}^n, h \stackrel{\$}{\leftarrow} \{0, 1\}^m, b'' \leftarrow A(0, k, h)] \\ & \stackrel{(**)}{=} \Pr[b'' = 1 : H \stackrel{\$}{\leftarrow} \text{Fun}, k \stackrel{\$}{\leftarrow} \{0, 1\}^n, h \stackrel{\$}{\leftarrow} \{0, 1\}^m, b'' \leftarrow A(1, k, h)] \\ & \stackrel{\varepsilon_1}{\approx} \Pr[b'' = 1 : H \stackrel{\$}{\leftarrow} \text{Fun}, k \stackrel{\$}{\leftarrow} \{0, 1\}^n, b'' \leftarrow A(1, k, H(k))] \\ & \stackrel{(*)}{=} \Pr[b' = 1 \wedge ok = 1 : \text{Game 1}(1)] \end{aligned}$$

where $\stackrel{\varepsilon_0}{\approx}$ denotes a difference of ε_0 ($\stackrel{\varepsilon_1}{\approx}$ analogous). Here $(*)$ is by definition of A . And $(**)$ uses that A uses b only in the computation “ $m := m_b \oplus h$ ”, so for uniform h , A 's output is independent of b .

Thus $\mu \leq \varepsilon_0 + \varepsilon_1$.

We will now show that ε_b is negligible for $b \in \{0, 1\}$. This then concludes the proof. For the remainder of the proof, fix some $b \in \{0, 1\}$.

Let B be the oracle algorithm that on input k picks $i \stackrel{\$}{\leftarrow} \{1, \dots, q_0 + q_1 + q_2\}$ and $h \stackrel{\$}{\leftarrow} \{0, 1\}^m$, and then runs $A^H(b, k, h)$ until the i -th query and measure the argument k' of that query (cf. Lemma 31). B then returns k' (or $\perp \notin \{0, 1\}^n$ if there was no i -th query).

Then by Lemma 31,

$$\varepsilon_b \leq 2(q_0 + q_1 + q_2) \sqrt{\Pr[k = k' : H \stackrel{\$}{\leftarrow} \text{Fun}, k \stackrel{\$}{\leftarrow} \{0, 1\}^n, k' \leftarrow B^H(k)]} \quad (26)$$

Consider the following games:

Game 2 (Measure in phase 0)

- (a) $H \stackrel{\$}{\leftarrow} \text{Fun}$.
- (b) $k \stackrel{\$}{\leftarrow} \{0, 1\}^n$.
- (c) $i \stackrel{\$}{\leftarrow} \{1, \dots, q_0\}$.
- (d) $h \stackrel{\$}{\leftarrow} \{0, 1\}^m$.
- (e) Run $A_0^H()$ until the i -th query and measure the argument k' to that query.

Game 3 (Measure in phase 1)

- (a) $H \stackrel{\$}{\leftarrow} \text{Fun}$.
- (b) $k \stackrel{\$}{\leftarrow} \{0, 1\}^n$.
- (c) $i \stackrel{\$}{\leftarrow} \{1, \dots, q_1\}$.
- (d) $h \stackrel{\$}{\leftarrow} \{0, 1\}^m$.
- (e) $(m_0, m_1) \leftarrow A_0^H()$.
- (f) $V' \leftarrow \text{TRE}(k)$.
- (g) $m := m_b \oplus h$.
- (h) Run the revocation protocol with $A_1^H(V', m)$ until the i -th query and measure the argument k' to that query.

Game 4 (Measure in phase 2)

- (a) $H \stackrel{\$}{\leftarrow} \text{Fun}$.
- (b) $k \stackrel{\$}{\leftarrow} \{0, 1\}^n$.
- (c) $i \stackrel{\$}{\leftarrow} \{1, \dots, q_2\}$.
- (d) $h \stackrel{\$}{\leftarrow} \{0, 1\}^m$.
- (e) $(m_0, m_1) \leftarrow A_0^H()$.
- (f) $V' \leftarrow \text{TRE}(k)$.
- (g) $m := m_b \oplus h$.
- (h) Run the revocation protocol with $A_1^H(V', m)$, outcome ok .
- (i) If $ok = 1$, run $A_2^H()$ until the i -th query and measure the argument k' to that query. Otherwise set $k' := \perp$.

We have that $p_0 := \Pr[k = k' : \text{Game 2}]$ is negligible because k is never used. We have that $p_1 := \Pr[k = k' : \text{Game 3}]$ is negligible because TRE is T -one-way and A_1^H runs in time T and no oracle queries are performed in the game excepts those by A_1^H . And we have that $\Pr[k = k' \wedge ok = 1 : \text{Game 4}]$ is negligible because TRE is T -revocably one-way and A_1^H runs in time T . Since $k' = \perp \neq k$ when $ok \neq 1$, we have $p_2 := \Pr[k = k' : \text{Game 4}] = \Pr[k = k' \wedge ok = 1 : \text{Game 4}]$.

Furthermore, by construction of B , we have:

$$\Pr[k = k' : H \stackrel{\$}{\leftarrow} \text{Fun}, k \leftarrow \{0, 1\}^n, k' \leftarrow B^H(x)] = \sum_{i=0,1,2} \frac{q_i}{q_0 + q_1 + q_2} p_i$$

Thus $\varepsilon_b \stackrel{(26)}{\leq} 2(q_0 + q_1 + q_2) \sqrt{\sum_i \frac{q_i}{q_0 + q_1 + q_2} p_i}$. Since p_1, p_2, p_3 are negligible and q_0, q_1, q_2 polynomially bounded, ε_b is negligible, and hence $\mu \leq \varepsilon_0 + \varepsilon_1$ is negligible, too.

To prove (ii), we can use a very similar proof. We only list the changes that need to be made: In Game 1, the steps (g)–(h) are replaced by “ $b' \leftarrow A_1^H(V', m)$ ”. Any occurrence of “ $b' = 1 \wedge ok = 1$ ” is replaced by “ $b' = 1$ ”. In Game 3, (h) is replaced by “Run $A_1^H()$ until the i -th query and measure the argument k' to that query.” Game 4 is removed. All sums involving q_0, q_1, q_2 or p_0, p_1, p_2 lose the terms with q_2 or p_2 .

Parts (iii) and (iv) of the theorem are proven like parts (i) and (ii), except that we have $q_0 = 0$. \square

F Full proofs: precomputation

Lemma 32 (Removing offline oracle queries) *Let $H : \{0, 1\}^{\ell+n} \rightarrow \{0, 1\}^m$ and $G : \{0, 1\}^n \rightarrow \{0, 1\}^m$ be random oracles. Let A, B be oracle algorithms (which can share state), and assume that A makes at most q oracle queries to H , and that B makes an arbitrary number of queries to H .*

Let $\tilde{B}(a)$ be the algorithm that results from $B(a)$ by the following change: Whenever B makes an oracle query $H(\tilde{a}||x)$, \tilde{B} instead makes an oracle query $H(\tilde{a}||x)$ if $\tilde{a} \neq a$ and $G(x)$ if $\tilde{a} = a$.²²

Consider the following two games:

Game A: $a \stackrel{\$}{\leftarrow} \{0, 1\}^\ell$, $H \stackrel{\$}{\leftarrow} (\{0, 1\}^{\ell+n} \rightarrow \{0, 1\}^m)$, $A^H()$, $b' \leftarrow B^H(a)$.

Game B: $a \stackrel{\$}{\leftarrow} \{0, 1\}^\ell$, $H \stackrel{\$}{\leftarrow} (\{0, 1\}^{\ell+n} \rightarrow \{0, 1\}^m)$, $G \stackrel{\$}{\leftarrow} (\{0, 1\}^n \rightarrow \{0, 1\}^m)$, $A^H()$, $b' \leftarrow \tilde{B}^{G,H}(a)$.

Then $|\Pr[b' = 1 : \text{Game A}] - \Pr[b' = 1 : \text{Game B}]| \leq q2^{-\ell/2+1}$.

Proof of Lemma 32. We describe a sequence of games, the first being identical to Game A from Lemma 32, and the last being identical to Game B from Lemma 32.

Game 1 (Game A)

$a \stackrel{\$}{\leftarrow} \{0, 1\}^\ell$, $H \stackrel{\$}{\leftarrow} (\{0, 1\}^{\ell+n} \rightarrow \{0, 1\}^m)$, $A^H()$, $b' \leftarrow B^H(a)$.

In the following, for an oracle $H : \{0, 1\}^{\ell+n} \rightarrow \{0, 1\}^m$ and an oracle $G : \{0, 1\}^n \rightarrow \{0, 1\}^m$ and a value $a \in \{0, 1\}^\ell$, let $H \lambda_a G : \{0, 1\}^{\ell+n} \rightarrow \{0, 1\}^m$ denote the oracle with $(H \lambda_a G)(\tilde{a}||x) := H(\tilde{a}||x)$ for $\tilde{a} \neq a$ and $(H \lambda_a G)(a||x) := G(x)$.

²²Formally, we replace the unitary operation $|k, v\rangle \mapsto |k, v \oplus H(k)\rangle$ by the unitary $|(\tilde{a}||x), v\rangle \mapsto |(\tilde{a}||x), v \oplus H(\tilde{a}||x)\rangle$ ($\tilde{a} \neq a$), $|(a||x), v\rangle \mapsto |(a||x), v \oplus G(x)\rangle$.

Game 2 (Changing A 's oracle)

$a \xleftarrow{\$} \{0,1\}^\ell$, $H \xleftarrow{\$} (\{0,1\}^{\ell+n} \rightarrow \{0,1\}^m)$, $G_1 \xleftarrow{\$} (\{0,1\}^n \rightarrow \{0,1\}^m)$, $A^{H \circ G_1}()$, $b' \leftarrow B^H(a)$.

We claim that

$$|\Pr[b' = 1 : \text{Game 1}] - \Pr[b' = 1 : \text{Game 2}]| \leq q2^{-\ell/2+1} \quad (27)$$

To show (27) it is sufficient to show that for fixed H, G_1 , we have that $\text{TD}(\rho_1, \rho_2) \leq q2^{-\ell/2+1}$ where ρ_1 is the state after executing $a \xleftarrow{\$} \{0,1\}^\ell$, $A^H()$ and ρ_2 is the state after executing $a \xleftarrow{\$} \{0,1\}^\ell$, $A^{H \circ G_1}()$. (ρ_1, ρ_2 describe states of a system with two registers, one for the value of a , and one for the state of A .)

Without loss of generality we can assume that A only performs unitary operations. Then the evolution of A can be described by a unitary operation U that operates on a tripartite system S, K, V where S contains A 's internal state, K is the input register for the random oracle, and V is the output register. The state of SKV before the first oracle query we call $|\Psi_0\rangle$. Then the final state of $A^H()$ is $|\Psi_q\rangle := (UO_H)^q|\Psi_0\rangle$ where $O_H : |k, v\rangle \mapsto O_H : |k, v \oplus H(v)\rangle$. Analogously, we get that the final state of $A^{H \circ G_1}$ is $|\Psi_q^a\rangle := (UO_{H \circ G_1})^q|\Psi_0\rangle$ with the same $|\Psi_0\rangle$ and the same U . With this notation,

$$\rho_1 = \sum_{a \in \{0,1\}^\ell} 2^{-\ell} |a\rangle\langle a| \otimes |\Psi_q\rangle\langle \Psi_q| \quad \text{and} \quad \rho_2 = \sum_{a \in \{0,1\}^\ell} 2^{-\ell} |a\rangle\langle a| \otimes |\Psi_q^a\rangle\langle \Psi_q^a|.$$

In order to bound $\text{TD}(\rho_1, \rho_2)$, we first bound D_i where

$$D_i := \sum_{a \in \{0,1\}^\ell} \|\Psi_i\rangle - |\Psi_i^a\rangle\|^2 \quad \text{and} \quad |\Psi_i\rangle := (UO_H)^i|\Psi_0\rangle \quad \text{and} \quad |\Psi_i^a\rangle := (UO_{H \circ G_1})^i|\Psi_0\rangle.$$

We claim that $D_i \leq 4i^2$ and show this by induction on i . For $i = 0$, we have that $D_i = \sum_a \|\Psi_0\rangle - |\Psi_0\rangle\|^2 = 0$. We now show $D_{i+1} \leq 4(i+1)^2$ assuming $D_i \leq 4i^2$.

Let $P_a|s, k, v\rangle := |s, k, v\rangle$ if $k = (a||\cdot)$ and $P_a|s, k, v\rangle := 0$ otherwise. Note that $O_H = O_{H \circ G_1} + O_H P_a - O_{G_1} P_a$ where $O_{G_1}|(\tilde{a}||x), v\rangle := |(\tilde{a}||x), v \oplus G_1(x)\rangle$. Then

$$\begin{aligned} D_{i+1} &= \sum_a \|\Psi_{i+1}^a\rangle - |\Psi_{i+1}\rangle\|^2 = \sum_a \|UO_{H \circ G_1}|\Psi_i^a\rangle - UO_H|\Psi_i\rangle\|^2 = \sum_a \|O_{H \circ G_1}|\Psi_i^a\rangle - O_H|\Psi_i\rangle\|^2 \\ &= \sum_a \|(O_{H \circ G_1}|\Psi_i^a\rangle - O_{H \circ G_1}|\Psi_i\rangle) + (O_{G_1}P_a|\Psi_i\rangle - O_H P_a|\Psi_i\rangle)\|^2 \\ &\hspace{15em} (\text{using } O_H = O_{H \circ G_1} + O_H P_a - O_{G_1} P_a) \\ &\leq \sum_a d_a^2 + 2d_a t_a + t_a^2 \end{aligned}$$

where $d_a := \|O_H^b|\Psi_i^a\rangle - O_H^b|\Psi_i\rangle\|$ and $t_a := \|O_{G_1}P_a|\Psi_i\rangle - O_H P_a|\Psi_i\rangle\|$.

Since $O_{H \circ G_1}$ is unitary, we have $d_a = \|\Psi_i^a\rangle - |\Psi_i\rangle\|$ and thus $D_i = \sum_a d_a^2$.

Furthermore, $t_a := \|(O_{G_1} - O_H)P_a|\Psi_i\rangle\| \leq \|O_{G_1} - O_H\| \cdot \|P_a|\Psi_i\rangle\| \leq (\|O_{G_1}\| + \|O_H\|) \cdot \|P_a|\Psi_i\rangle\| = 2\|P_a|\Psi_i\rangle\|$. (Remember that $\|x+y\|^2 \leq \|x\|^2 + 2\|x\|\|y\| + \|y\|^2$.) Hence $\sum_a t_a^2 \leq 4 \sum_a \|P_a|\Psi_i\rangle\|^2 \leq 4$ since the projectors P_a are orthogonal. The Cauchy-Schwarz-Inequality implies $\sum_a d_a t_a \leq \sqrt{\sum_a d_a^2} \cdot \sqrt{\sum_a t_a^2} \leq \sqrt{D_i} \cdot 2$.

Thus

$$D_{i+1} \leq \sum_a d_a^2 + 2d_a t_a + t_a^2 \leq D_i + 4\sqrt{D_i} + 4 \leq 4i^2 + 8i + 4 = 4(i+1)^2.$$

This finishes the proof by induction that $D_i \leq 4i^2$.²³

We are now ready to bound $\text{TD}(\rho_1, \rho_2)$. Let $F_a := |\langle \Psi_q | \Psi_q^a \rangle|$ denote the fidelity between $|\Psi_q\rangle$ and $|\Psi_q^a\rangle$. By [NC10, Section 9.2.3, (9.97)], we have $\text{TD}(|\Psi_q\rangle, |\Psi_q^a\rangle) = \sqrt{1 - F_a^2}$. And

$$\begin{aligned} \Delta_a &:= \|\Psi_q\rangle - |\Psi_q^a\rangle\|^2 \\ &= \langle \Psi_q | \Psi_q \rangle - \langle \Psi_q | \Psi_q^a \rangle - \langle \Psi_q^a | \Psi_q \rangle + \langle \Psi_q^a | \Psi_q^a \rangle \\ &= 1 - 2\Re(\langle \Psi_q | \Psi_q^a \rangle) + 1 \\ &\geq 1 - 2|\langle \Psi_q | \Psi_q^a \rangle| + 1 \\ &= 2(1 - F_a) \end{aligned}$$

²³This calculation of the bound for D_i follows roughly the corresponding calculation from [NC10, Section 6.6].

where $\Re(x)$ denotes the real part of x . Hence $F_a \geq 1 - \frac{1}{2}\Delta_a$ and thus

$$\begin{aligned}
\text{TD}(\rho_1, \rho_2) &= \text{TD}\left(\sum_a 2^{-\ell} |a\rangle\langle a| \otimes |\Psi_q\rangle\langle\Psi_q|, \sum_a 2^{-\ell} |a\rangle\langle a| \otimes |\Psi_q^a\rangle\langle\Psi_q^a|\right) \\
&= \sum_a 2^{-\ell} \text{TD}(|\Psi_q\rangle, |\Psi_q^a\rangle) = \sum_a 2^{-\ell} \sqrt{1 - F_a^2} \\
&\leq \sum_a 2^{-\ell} \sqrt{1 - (1 - \frac{1}{2}\Delta_a)^2} = \sum_a 2^{-\ell} \sqrt{\Delta_a - \frac{1}{4}\Delta_a^2} \\
&\leq \sum_a 2^{-\ell} \sqrt{\Delta_a} \stackrel{(*)}{\leq} \sqrt{\sum_a 2^{-\ell} \Delta_a} \\
&= \sqrt{2^{-\ell} D_q} \leq \sqrt{2^{-\ell} 4q^2} = q2^{-\ell/2+1}.
\end{aligned}$$

Here $(*)$ uses Jensen's inequality.

As discussed above, $\text{TD}(\rho_1, \rho_2) \leq q2^{-\ell/2+1}$ proves (27).

Game 3 (Decomposing H)

$$\begin{aligned}
a &\stackrel{\$}{\leftarrow} \{0, 1\}^\ell, H_1 \stackrel{\$}{\leftarrow} (\{0, 1\}^{\ell+n} \rightarrow \{0, 1\}^m), G \stackrel{\$}{\leftarrow} (\{0, 1\}^n \rightarrow \{0, 1\}^m), H := H_1 \lambda_a G, \\
G_1 &\stackrel{\$}{\leftarrow} (\{0, 1\}^n \rightarrow \{0, 1\}^m), A^{H \lambda_a G_1}(), b' \leftarrow B^H(a).
\end{aligned}$$

Since $H_1 \lambda_a G$ is a uniformly distributed function for uniformly distributed H_1, G (and since H_1, G are not used except in the construction of H), we have $\Pr[b' = 1 : \text{Game 2}] = \Pr[b' = 1 : \text{Game 3}]$.

Game 4 (Substituting equal oracles)

$$\begin{aligned}
a &\stackrel{\$}{\leftarrow} \{0, 1\}^\ell, H_1 \stackrel{\$}{\leftarrow} (\{0, 1\}^{\ell+n} \rightarrow \{0, 1\}^m), G \stackrel{\$}{\leftarrow} (\{0, 1\}^n \rightarrow \{0, 1\}^m), \underline{H := H_1 \lambda_a G}, \\
G_1 &\stackrel{\$}{\leftarrow} (\{0, 1\}^n \rightarrow \{0, 1\}^m), A^{H_1 \lambda_a G_1}(), b' \leftarrow B^{(H_1 \lambda_a G_1) \lambda_a G}(a).
\end{aligned}$$

The oracle supplied to A in the two games is the same since $H \lambda_a G_1 = (H_1 \lambda_a G) \lambda_a G_1 = H_1 \lambda_a G_1$ by definition of λ_a . The oracle supplied to B is the same since $H = H_1 \lambda_a G = (H_1 \lambda_a G_1) \lambda_a G$. Furthermore, we can drop the definition of H from Game 4 since H is not used any more. Hence $\Pr[b' = 1 : \text{Game 3}] = \Pr[b' = 1 : \text{Game 4}]$.

Game 5 (Introducing \tilde{B})

$$\begin{aligned}
a &\stackrel{\$}{\leftarrow} \{0, 1\}^\ell, H_1 \stackrel{\$}{\leftarrow} (\{0, 1\}^{\ell+n} \rightarrow \{0, 1\}^m), G \stackrel{\$}{\leftarrow} (\{0, 1\}^n \rightarrow \{0, 1\}^m), \\
G_1 &\stackrel{\$}{\leftarrow} (\{0, 1\}^n \rightarrow \{0, 1\}^m), \underline{H := H_1 \lambda_a G_1}, A^H(), b' \leftarrow \tilde{B}^{H, G}(a).
\end{aligned}$$

By definition of \tilde{B} , we have that $\tilde{B}^{H, G} = B^{H \lambda_a G}$ for any oracles H, G . Thus (and using that $H = H_1 \lambda_a G_1$) we have $\Pr[b' = 1 : \text{Game 4}] = \Pr[b' = 1 : \text{Game 5}]$.

Game 6 (Game B)

$$\begin{aligned}
a &\stackrel{\$}{\leftarrow} \{0, 1\}^\ell, \underline{H_1 \leftarrow (\{0, 1\}^{\ell+n} \rightarrow \{0, 1\}^m)}, G \stackrel{\$}{\leftarrow} (\{0, 1\}^n \rightarrow \{0, 1\}^m), \\
\underline{G_1 \leftarrow (\{0, 1\}^n \rightarrow \{0, 1\}^m)}, H &\stackrel{\$}{\leftarrow} (\{0, 1\}^{\ell+n} \rightarrow \{0, 1\}^m), A^H(), b' \leftarrow \tilde{B}^{H, G}(a).
\end{aligned}$$

Since $H_1 \lambda_a G_1$ is uniformly distributed for uniform H_1, G_1 (and since H_1, G_1 are not used except in the construction of H), we can replace $H := H_1 \lambda_a G_1$ by a uniformly chosen H and have $\Pr[b' = 1 : \text{Game 5}] = \Pr[b' = 1 : \text{Game 6}]$.

Summarizing, we have that $\Pr[b' = 1 : \text{Game 2}] = \Pr[b' = 1 : \text{Game 6}]$. Furthermore Game 1 is identical to Game A from Lemma 32 and Game 6 is identical to Game B from Lemma 32. Hence (27) implies that

$$|\Pr[b' = 1 : \text{Game A}] - \Pr[b' = 1 : \text{Game B}]| \leq q2^{-\ell/2+1}. \quad \square$$

We can use Lemma 32 to transform a timed-release encryption that is (revocably) hiding without offline-queries into one that is (revocably) hiding:

Theorem 11 (timed-release encryptions with offline-queries) *Let ℓ, n, m be integers (dependent on the security parameter), assume that ℓ is superlogarithmic, and let $H : \{0, 1\}^{\ell+n} \rightarrow \{0, 1\}^m$ be a random oracle. Let TRE be a revocable timed-release encryption in the random oracle model using an oracle $G : \{0, 1\}^n \rightarrow \{0, 1\}^m$.*

Let TRE' be the following timed-release encryption:

- **Encryption:** $\text{TRE}'(m)$ picks $a \xleftarrow{\$} \{0, 1\}^\ell$. Then $\text{TRE}'(m)$ runs $V \leftarrow \text{TRE}(m)$, except that any oracle query $G(x)$ by $\text{TRE}(m)$ is replaced by an oracle query $H(a\|x)$. TRE' returns (a, V) .
- **Decryption:** Given (a, V) , run the decryption of TRE on V , except that any oracle query $G(x)$ is replaced by an oracle query $H(a\|x)$.
- **Revocation:** Run the revocation protocol of TRE , except that any oracle query $G(x)$ is replaced by an oracle query $H(a\|x)$.

If TRE is T -revocably hiding without offline-queries then TRE' is T -revocably hiding.

If TRE is T -hiding without offline-queries then TRE' is T -hiding.

Both statements hold both for the parallel and the sequential oracle-query timing model.²⁴

Proof. We show that if TRE is T -hiding without offline-queries then TRE' is T -hiding. The T -revocably hiding property is proven analogously.

By Definition 2, we need to show that $|p_0 - p_1|$ is negligible where

$$p_b := \Pr[b' = 1 : H \xleftarrow{\$} (\{0, 1\}^{\ell+n} \rightarrow \{0, 1\}^m), (m_0, m_1) \leftarrow A_0^H(), (a, V) \leftarrow (\text{TRE}')^H(m_b), b' \leftarrow A_1^H(a, V)]$$

and A_0 is sequential-polynomial-time and A_1 is sequential-polynomial-time and T -time.

Fix $b \in \{0, 1\}$. Let $B^H(a)$ run $V \leftarrow \text{TRE}_a^H(m_b), b' \leftarrow A_1^H(a, V)$ where TRE_a^H is like TRE^G , except that all $G(x)$ queries are replaced by $H(a\|x)$ queries. (Note that with this notation $(\text{TRE}')^H(m)$ runs $a \xleftarrow{\$} \{0, 1\}^\ell, V \leftarrow \text{TRE}_a^H(m)$. Note also that A and B share state because B accesses m_0, m_1 .)

Let $\tilde{B}^{G,H}(a)$ run $V \leftarrow \text{TRE}^G(m_b), b' \leftarrow \tilde{A}_1^{G,H}(a, V)$ where \tilde{A}_1 is the result of applying the transformation described in Lemma 32 (that transforms B into \tilde{B} there) to A_1 . Note that our \tilde{B} results from B when applying the transformation from Lemma 32.

(In the proof for the T -revocably hiding property we let B^H and $\tilde{B}^{G,H}$ additionally run the revocation protocol and $A_2^H/\tilde{A}_2^{G,H}$.)

Let $A_0^*(V)$ run $H \xleftarrow{\$} (\{0, 1\}^{\ell+n} \rightarrow \{0, 1\}^m), (m_0, m_1) \leftarrow A_0^H(a, V)$. Let $(A_1^*)^G(V)$ run $a \xleftarrow{\$} \{0, 1\}^\ell, b' \leftarrow \tilde{A}_1^{G,H}(a, V)$. (Where A_1^* uses the H picked by A_0^* .)

(In the proof for the T -revocably hiding property we additionally construct A_2^* analogously to A_1^* .)

Note that (A_0^*, A_1^*) described in this way is not sequential-polynomial-time any more because it picks an exponentially large function H . However, [Zha12] shows that (A_0^*, A_1^*) can be simulated in sequential-polynomial-time (by replacing H by a $2q'$ -wise independent function where q' is the number of queries of $(\tilde{A}_0, \tilde{A}_1)$). The construction from [Zha12] does not increase the number of G -queries, hence A_1^* is still T -time (this holds both for the parallel and the sequential oracle-query timing model).

Let q be an upper bound on the number of oracle queries performed by A_0 . We can choose q to be polynomially bounded since A_0 is sequential-polynomial-time.

By $p \approx p'$ we mean that $|p - p'|$ is negligible.

We have then

$$\begin{aligned} p_b &= \Pr[b' = 1 : a \xleftarrow{\$} \{0, 1\}^\ell, H \xleftarrow{\$} (\{0, 1\}^{\ell+n} \rightarrow \{0, 1\}^m), (m_0, m_1) \leftarrow A_0^H(), b' \leftarrow B^H(a)] \\ &\stackrel{(*)}{\approx} \Pr[b' = 1 : a \xleftarrow{\$} \{0, 1\}^\ell, H \xleftarrow{\$} (\{0, 1\}^{\ell+n} \rightarrow \{0, 1\}^m), G \xleftarrow{\$} (\{0, 1\}^n \rightarrow \{0, 1\}^m), \\ &\quad (m_0, m_1) \leftarrow A_0^H(), b' \leftarrow \tilde{B}^{G,H}(a)] \\ &= \Pr[b' = 1 : a \xleftarrow{\$} \{0, 1\}^\ell, H \xleftarrow{\$} (\{0, 1\}^{\ell+n} \rightarrow \{0, 1\}^m), G \xleftarrow{\$} (\{0, 1\}^n \rightarrow \{0, 1\}^m), \\ &\quad (m_0, m_1) \leftarrow A_0^H(), V \leftarrow \text{TRE}^G(m_b), b' \leftarrow \tilde{A}_1^{G,H}(a, V)] \\ &= \Pr[b' = 1 : \cancel{a \xleftarrow{\$} \{0, 1\}^\ell}, \cancel{H \xleftarrow{\$} (\{0, 1\}^{\ell+n} \rightarrow \{0, 1\}^m)}, G \xleftarrow{\$} (\{0, 1\}^n \rightarrow \{0, 1\}^m), \\ &\quad (m_0, m_1) \leftarrow A_0^*(V), V \leftarrow \text{TRE}^G(m_b), b' \leftarrow (A_1^*)^G(V)] =: p_b^* \end{aligned}$$

Here $(*)$ uses Lemma 32 and the fact that $q2^{-\ell/2-1}$ is negligible.

Notice that p_b^* is the game from Definition 2 for the timed-release encryption TRE and adversary (A_0^*, A_1^*) . Since A_0^* is sequential-polynomial-time and does not access G and A_1^* is sequential-polynomial-time and T -time, and since TRE is T -hiding without offline-queries, we have that $|p_0^* - p_1^*|$ is negligible. Since $p_b^* \approx p_b$ for any $b \in \{0, 1\}$, it follows that $|p_0 - p_1|$. Thus TRE' is T -hiding. \square

²⁴For other timing models, the reduction described in the proof may incur an overhead, leading to a smaller T .

G Full proofs: iterated hashing

Definition 11 (Iterated hashing) Let n and T be polynomially-bounded integers (depending on the security parameter), and assume that n is superlogarithmic. Let $H : \{0, 1\}^n \rightarrow \{0, 1\}^n$ denote the random oracle.

We define a timed-release encryption TRE_{ih} with message space $\{0, 1\}^n$ in the random oracle model as follows:

- *Encryption:* $\text{TRE}_{ih}(m)$ returns the timed-release encryption $V := H^{T+1}(0^n) \oplus m$.
- *Decryption:* Given V , return $H^{T+1}(0^n) \oplus V$.

Note that this timed-release encryption cannot be one-way: Since TRE_{ih} is not randomized, the adversary can compute $H^{T+1}(0^n)$ during the precomputation (i.e., before getting the timed-release encryption), and then recover m quickly later. But TRE_{ih} is one-way without offline-queries, so we can later use the transformation from Appendix F to remove this restriction.

Theorem 12 (Iterated hashing is one-way without offline-queries) TRE_{ih} from Definition 11 is T -one-way without offline-queries. (Assuming the parallel oracle-query timing model.)

A concrete security bound can be found at the end of the proof (page 49, (30)).

Proof. The adversary (A_0, A_1) against T -one-wayness without offline-queries has to output $V \oplus H^{T+1}(0^n)$ given V within time T . (This includes A_0 , because we consider the case without offline-queries and thus A_0 runs in time T with respect to oracle-query timing.) To show that TRE_{ih} is T -one-way without offline-queries it is therefore sufficient to show the following: For any T -time algorithm A , $A^H(\cdot)$ outputs $H^{T+1}(0^n)$ with negligible probability.

We assume that the state of A is composed of three quantum systems A , $K = (K_1, \dots, K_q)$, $V = (V_1, \dots, V_q)$. Then an execution of A leads to the final state $(UO_H)^{T-1}|\Psi\rangle$ where $|\Psi\rangle$ is the initial state, $O_H : |a, (k_1, \dots, k_q), (v_1, \dots, v_q)\rangle \rightarrow |a, (k_1, \dots, k_q), (v_1 \oplus H(k_1), \dots, v_q \oplus H(k_q))\rangle$ is an oracle query (on q inputs), and U is A 's state transition operation. A 's output is produced by applying a measurement M to A 's final state.

Given a function $H : \{0, 1\}^n \rightarrow \{0, 1\}^n$, and a tuple $\mathbf{x} = (x_1, \dots, x_{T+1})$, we define $H_{\mathbf{x}}$ to be the function resulting from H by setting $H(x_{i-1}) := x_i$ for $i = 1, \dots, s$ with $x_0 := 0^n$ where s is the largest index such that x_s did not already occur (formally, the largest s such that $x_s \neq x_j$ for all $0 \leq j < s$) or $s = T + 1$ if no duplicates occur in $0, x_1, \dots, x_{T+1}$.

Let $|\Psi_i^{H, \mathbf{x}}\rangle$ be the result of running the adversary i steps on oracle $H_{\mathbf{x}}$. I.e., $|\Psi_i^{H, \mathbf{x}}\rangle = (UO_{H_{\mathbf{x}}})^i|\Psi\rangle$.

A family of states $\{|\Psi^{H, \mathbf{x}}\rangle\}_{H, \mathbf{x}}$ we call i -good if for any \mathbf{x} and \mathbf{x}' with $(x_1, \dots, x_i) = (x'_1, \dots, x'_i)$ we have that $|\Psi^{H, \mathbf{x}}\rangle = |\Psi^{H, \mathbf{x}'}\rangle$. I.e., a family of states is i -good if it does not depend on x_{i+1}, \dots, x_{T+1} .

Given two families $\{|\Psi^{H, \mathbf{x}}\rangle\}_{H, \mathbf{x}}$ and $\{|\Phi^{H, \mathbf{x}}\rangle\}_{H, \mathbf{x}}$, their distance is defined as $\sum_{H, \mathbf{x}} \frac{1}{N} \text{TD}(|\Psi^{H, \mathbf{x}}\rangle, |\Phi^{H, \mathbf{x}}\rangle)$, where $N := (2^n)^{2^n} (2^n)^{T+1}$ is the number of values H, \mathbf{x} . Notice that the distance satisfies the triangle inequality, and is invariant under the application of unitary transformations $U_{H, \mathbf{x}}$ (that may depend on H, \mathbf{x}) to the states.

Claim 1 Fix $0 \leq i < j \leq T + 1$. Fix a measurement M . Fix an i -good family $\{|\Psi^{H, \mathbf{x}}\rangle\}_{H, \mathbf{x}}$. Then $\sum_{H, \mathbf{x}} \frac{1}{N} \Pr[\text{measuring } |\Psi^{H, \mathbf{x}}\rangle \text{ using } M \text{ yields } x_j] = 2^{-n}$.

We show this claim. Let “ $|\Psi^{H, \mathbf{x}}\rangle \mapsto x_j$ ” abbreviate “measuring $|\Psi^{H, \mathbf{x}}\rangle$ using M yields x_j ”. Let $\mathbf{x} \oplus p$ be short for $(x_1, \dots, x_{j-1}, x_j \oplus p, x_{j+1}, \dots, x_T)$. Since $\mathbf{x} \oplus p$ ranges over the same tuples as \mathbf{x} , we have for any $p \in \{0, 1\}^n$:

$$\sum_{H, \mathbf{x}} \frac{1}{N} \Pr[|\Psi^{H, \mathbf{x}}\rangle \mapsto x_j] = \sum_{H, \mathbf{x}} \frac{1}{N} \Pr[|\Psi^{H, \mathbf{x} \oplus p}\rangle \mapsto x_j \oplus p]. \quad (28)$$

and thus

$$\begin{aligned}
& \sum_{H, \mathbf{x}} \frac{1}{N} \Pr[|\Psi^{H, \mathbf{x}}\rangle \mapsto x_j] \\
& \stackrel{(28)}{=} \sum_p 2^{-n} \sum_{H, \mathbf{x}} \frac{1}{N} \Pr[|\Psi^{H, \mathbf{x} \oplus p}\rangle \mapsto x_j \oplus p] \\
& \stackrel{(*)}{=} \sum_p 2^{-n} \sum_{H, \mathbf{x}} \frac{1}{N} \Pr[|\Psi^{H, \mathbf{x}}\rangle \mapsto x_j \oplus p] \\
& \stackrel{(**)}{=} 2^{-n} \underbrace{\sum_{H, \mathbf{x}} \frac{1}{N}}_{=1} \underbrace{\sum_{p'} \Pr[|\Psi^{H, \mathbf{x}}\rangle \mapsto p']}_{\leq 1} = 2^{-n}.
\end{aligned}$$

Here (*) holds because for i -good families, $|\Psi^{H, \mathbf{x} \oplus p}\rangle = |\Psi^{H, \mathbf{x}}\rangle$. And (**) substitutes $p' := x_j \oplus p$. The claim follows.

Claim 2 For $i \leq T$, if $\{|\Psi^{H, \mathbf{x}}\rangle\}_{H, \mathbf{x}}$ is i -good, then $\{O_{H, \mathbf{x}}|\Psi^{H, \mathbf{x}}\rangle\}_{H, \mathbf{x}}$ has distance at most $2^{-n/2+1}\sqrt{q(T-i+2)}$ from an $(i+1)$ -good family of states.

To prove this claim, we first fix $H : \{0, 1\}^n \rightarrow \{0, 1\}^n$ and $\mathbf{x} \in (\{0, 1\}^n)^{T+1}$ and also some $y \in \{0, 1\}^n$. Let $\mathbf{x}_y := (x_1, \dots, x_{i+1}, y, \dots, y)$.

For a set of values $W \subseteq \{0, 1\}^n$, we define a projector P_W^* on K as $P_W^* := \sum |x_1, \dots, x_q\rangle\langle x_1, \dots, x_q|$ where the sum ranges over all $x_1, \dots, x_q \in \{0, 1\}^n$ with $\{x_1, \dots, x_q\} \cap W \neq \emptyset$. That is, P_W^* measures (in the computational basis) whether at least one K_i contains a value in W . We write short $P_{abc\dots}^*$ for $P_{\{a, b, c, \dots\}}^*$.

In the following calculation, let \approx denote trace distance at most $2\|O_{H, \mathbf{x}} P_{x_{i+1} \dots x_{T+1} y}^* |\Psi^{H, \mathbf{x}}\rangle\|$.

$$\begin{aligned}
O_{H, \mathbf{x}} |\Psi^{H, \mathbf{x}}\rangle &= O_{H, \mathbf{x}} P_{x_{i+1} \dots x_{T+1} y}^* |\Psi^{H, \mathbf{x}}\rangle + O_{H, \mathbf{x}} (1 - P_{x_{i+1} \dots x_{T+1} y}^*) |\Psi^{H, \mathbf{x}}\rangle \\
&\stackrel{(*)}{=} O_{H, \mathbf{x}} P_{x_{i+1} \dots x_{T+1} y}^* |\Psi^{H, \mathbf{x}}\rangle + O_{H, \mathbf{x}_y} (1 - P_{x_{i+1} \dots x_{T+1} y}^*) |\Psi^{H, \mathbf{x}}\rangle \\
&\stackrel{(**)}{\approx} O_{H, \mathbf{x}_y} P_{x_{i+1} \dots x_{T+1} y}^* |\Psi^{H, \mathbf{x}}\rangle + O_{H, \mathbf{x}_y} (1 - P_{x_{i+1} \dots x_{T+1} y}^*) |\Psi^{H, \mathbf{x}}\rangle \\
&= O_{H, \mathbf{x}_y} |\Psi^{H, \mathbf{x}}\rangle \stackrel{(***)}{=} O_{H, \mathbf{x}_y} |\Psi^{H, \mathbf{x}_y}\rangle.
\end{aligned}$$

Here (*) uses that the responses $H_{\mathbf{x}}$ and $H_{\mathbf{x}_y}$ differ only on inputs x_{i+1}, \dots, x_T, y . And (**) uses Lemma 7 and the fact that $|\Phi^*\rangle := O_{H, \mathbf{x}_y} (1 - P_{x_{i+1} \dots x_{T+1} y}^*) |\Psi^{H, \mathbf{x}}\rangle = O_{H, \mathbf{x}} (1 - P_{x_{i+1} \dots x_{T+1} y}^*) |\Psi^{H, \mathbf{x}}\rangle$ is orthogonal to both $|\Psi_1^*\rangle := O_{H, \mathbf{x}} P_{x_{i+1} \dots x_{T+1} y}^* |\Psi^{H, \mathbf{x}}\rangle$ and $|\Psi_2^*\rangle := O_{H, \mathbf{x}_y} P_{x_{i+1} \dots x_{T+1} y}^* |\Psi^{H, \mathbf{x}}\rangle$. And (***) uses that $\{|\Psi^{H, \mathbf{x}}\rangle\}_{H, \mathbf{x}}$ is i -good by assumption and thus $|\Psi^{H, \mathbf{x}}\rangle = |\Psi^{H, \mathbf{x}_y}\rangle$.

Thus we have that for any $H : \{0, 1\}^n \rightarrow \{0, 1\}^n$ and $\mathbf{x} \in (\{0, 1\}^n)^{T+1}$ and $y \in \{0, 1\}^n$,

$$\text{TD}(O_{H, \mathbf{x}} |\Psi^{H, \mathbf{x}}\rangle, O_{H, \mathbf{x}_y} |\Psi^{H, \mathbf{x}_y}\rangle) \leq 2\|O_{H, \mathbf{x}} P_{x_{i+1} \dots x_{T+1} y}^* |\Psi^{H, \mathbf{x}}\rangle\|. \quad (29)$$

We abbreviate “given state $|\Psi\rangle$, measuring K_1, \dots, K_q in the computational basis yields (z_1, \dots, z_q) with $\{z_1, \dots, z_q\} \cap \{a, b, c, d, \dots\} \neq \emptyset$ ” with “ $|\Psi\rangle \mapsto abcd\dots$ ”. And “given state $|\Psi\rangle$, measuring K_i in the computational basis yields $z \in \{a, b, c, d, \dots\}$ ” with “ $|\Psi\rangle \mapsto_i abcd\dots$ ”.

Let δ_y be the distance between $\{O_{H, \mathbf{x}} |\Psi^{H, \mathbf{x}}\rangle\}_{H, \mathbf{x}}$ and $\{O_{H, \mathbf{x}_y} |\Psi^{H, \mathbf{x}_y}\rangle\}_{H, \mathbf{x}}$. We then have

$$\begin{aligned}
\sum_{y \in \{0, 1\}^n} 2^{-n} \delta_y &= \sum_y 2^{-n} \sum_{H, \mathbf{x}} \frac{1}{N} \text{TD}(O_{H, \mathbf{x}} |\Psi^{H, \mathbf{x}}\rangle, O_{H, \mathbf{x}_y} |\Psi^{H, \mathbf{x}_y}\rangle) \\
&\stackrel{(29)}{\leq} \sum_{H, \mathbf{x}, y} \frac{1}{N 2^n} 2\|O_{H, \mathbf{x}} P_{x_{i+1} \dots x_{T+1} y}^* |\Psi^{H, \mathbf{x}}\rangle\| = \sum_{H, \mathbf{x}, y} \frac{1}{N 2^n} 2\|P_{x_{i+1} \dots x_{T+1} y}^* |\Psi^{H, \mathbf{x}}\rangle\| \\
&= \sum_{H, \mathbf{x}, y} \frac{1}{N 2^n} 2\sqrt{\Pr[|\Psi^{H, \mathbf{x}}\rangle \mapsto_{x_{i+1} \dots x_{T+1} y}]} \\
&\stackrel{(*)}{\leq} 2\sqrt{\sum_{H, \mathbf{x}, y} \frac{1}{N 2^n} \Pr[|\Psi^{H, \mathbf{x}}\rangle \mapsto_{x_{i+1} \dots x_{T+1} y}]}
\end{aligned}$$

$$\begin{aligned}
&\leq 2 \sqrt{\sum_{i=1}^q \sum_{H, \mathbf{x}, y} \frac{1}{N2^n} \sum_{j=i+1}^{T+1} \underbrace{\Pr[|\Psi^{H, \mathbf{x}}\rangle \mapsto_i x_j]}_{=2^{-n} \text{ (Claim 1)}} + \sum_{i=1}^q \sum_{H, \mathbf{x}} \frac{1}{N2^n} \sum_y \underbrace{\Pr[|\Psi^{H, \mathbf{x}}\rangle \mapsto_i y]}_{=1}} \\
&= 2\sqrt{q(T-i+1)2^{-n} + q2^{-n}} = 2^{-n/2+1}\sqrt{q(T-i+2)} =: \varepsilon.
\end{aligned}$$

Here (*) uses Jensen's inequality.

Since $\sum_{y \in \{0,1\}^n} 2^{-n} \delta_y \leq \varepsilon$, there is a y_0 with $\delta_{y_0} \leq \varepsilon$.

Thus $\{O_{H, \mathbf{x}} |\Psi^{H, \mathbf{x}}\rangle\}_{H, \mathbf{x}}$ and $\{O_{H, \mathbf{x}_{y_0}} |\Psi^{H, \mathbf{x}_{y_0}}\rangle\}_{H, \mathbf{x}}$ have distance at most $\delta_{y_0} \leq \varepsilon = 2^{-n/2+1}\sqrt{q(T-i+2)}$. And $\{O_{H, \mathbf{x}_{y_0}} |\Psi^{H, \mathbf{x}_{y_0}}\rangle\}_{H, \mathbf{x}}$ is $(i+1)$ -good by construction (since $\mathbf{x}_{y_0} = (x_1, \dots, x_{i+1}, y_0, \dots, y_0)$ is independent of x_{i+2}, \dots, x_{T+1}). Claim 2 follows.

Claim 3 *If $\{|\Psi^{H, \mathbf{x}}\rangle\}_{H, \mathbf{x}}$ is i -good and U is unitary, then $\{U|\Psi^{H, \mathbf{x}}\rangle\}_{H, \mathbf{x}}$ is i -good.*

This follows immediately from the definition of i -good.

Claim 4 *$\{|\Psi_i^{H, \mathbf{x}}\rangle\}_{H, \mathbf{x}}$ has distance $\sum_{i=0}^{i-1} 2^{-n/2+1}\sqrt{q(T-i+2)}$ from an i -good family of states.*

To show this claim, first note that $|\Psi_0^{H, \mathbf{x}}\rangle = |\Psi\rangle$ is independent of x_1, \dots, x_{T+1} , hence $\{|\Psi_0^{H, \mathbf{x}}\rangle\}_{H, \mathbf{x}}$ is 0-good. By induction over i and using Claim 2 and Claim 3 and the fact that the distance between families is invariant under unitaries U and satisfies the triangle inequality, we get that $\{|\Psi_i^{H, \mathbf{x}}\rangle\}_{H, \mathbf{x}}$ has distance $\sum_{i=0}^{i-1} 2^{-n/2+1}\sqrt{q(T-i+2)}$ from an i -good family, showing the claim.

The final state of the adversary running with oracle $H_{\mathbf{x}}$ is $|\Psi_T^{H, \mathbf{x}}\rangle$. Thus the probability that the adversary outputs x_{T+1} with oracle $H_{\mathbf{x}}$ is $p_{H, \mathbf{x}} := \Pr[\text{measuring } |\Psi_T^{H, \mathbf{x}}\rangle \text{ yields } x_{T+1}]$. By Claim 1, $\sum_{H, \mathbf{x}} \frac{1}{N} \Pr[\text{measuring } |\Phi^{H, \mathbf{x}}\rangle \text{ yields } x_{T+1}] = 2^{-n}$ for $(T+1)$ -good $\{|\Phi^{H, \mathbf{x}}\rangle\}_{H, \mathbf{x}}$. By Claim 4, $\{|\Psi_T^{H, \mathbf{x}}\rangle\}_{H, \mathbf{x}}$ has the following distance from a $(T+1)$ -good family:

$$\begin{aligned}
2^{-n/2+1}\sqrt{q} \sum_{i=0}^T 1 \cdot \sqrt{T-i+2} &\stackrel{(*)}{\leq} 2^{-n/2+1}\sqrt{q} \sqrt{(T+1) \cdot \sum_{i=0}^T T-i+2} \\
&= 2^{-n/2+1}\sqrt{q} \sqrt{(T+1) \cdot \left((T+1)(T+2) - \frac{T(T+1)}{2} \right)} \\
&\leq 2^{-n/2+1}\sqrt{q} \sqrt{(T+2)^3/2} = 2^{-n/2}\sqrt{2q}(T+2)^{3/2}.
\end{aligned}$$

Here (*) uses the Cauchy-Schwarz-Inequality. Hence $\sum_{H, \mathbf{x}} \frac{1}{N} p_{H, \mathbf{x}} \leq 2^{-n/2}\sqrt{2q}(T+2)^{3/2} + 2^{-n}$. Thus

$$\Pr[x' = x_{T+1} : H \stackrel{\$}{\leftarrow} (\{0,1\}^n \rightarrow \{0,1\}^n), x_1, \dots, x_{T+1} \stackrel{\$}{\leftarrow} \{0,1\}^n, x' \leftarrow A^{H_{\mathbf{x}}}] \leq 2^{-n/2}\sqrt{2q}(T+2)^{3/2} + 2^{-n}.$$

Observe that, if $0, x_1, \dots, x_{T+1}$ does not contain duplicates, $x_{T+1} = (H_{\mathbf{x}})^{T+1}(0^n)$. The probability of $0^n, x_1, \dots, x_{T+1}$ containing duplicates is at most $\frac{(T+1)(T+2)}{2} 2^{-n}$. Hence

$$\begin{aligned}
&\Pr[x' = (H_{\mathbf{x}})^{T+1}(0^n) : H \stackrel{\$}{\leftarrow} (\{0,1\}^n \rightarrow \{0,1\}^n), x_1, \dots, x_n \stackrel{\$}{\leftarrow} \{0,1\}^n, x' \leftarrow A^{H_{\mathbf{x}}}] \\
&\leq 2^{-n/2}\sqrt{2q}(T+2)^{3/2} + 2^{-n} + \frac{(T+1)(T+2)}{2} 2^{-n} \leq 2^{-n/2}\sqrt{2q}(T+2)^{3/2} + 2^{-n-1}(T+2)^2
\end{aligned}$$

Notice that for H and x_1, \dots, x_n chosen uniformly at random, $H_{\mathbf{x}}$ is uniformly distributed. Hence we can replace $H_{\mathbf{x}}$ by H in the above probability and get

$$\begin{aligned}
&\Pr[x' = H^{T+1}(0^n) : H \stackrel{\$}{\leftarrow} (\{0,1\}^n \rightarrow \{0,1\}^n), x' \leftarrow A^H()] \\
&\leq 2^{-n/2}\sqrt{2q}(T+2)^{3/2} + 2^{-n-1}(T+2)^2 \quad (30)
\end{aligned}$$

The latter probability is the probability of A breaking the timed-release encryption TRE_{ih} . Since $2^{-n/2}\sqrt{2q}(T+2)^{3/2} + 2^{-n-1}(T+2)^2$ is negligible for polynomially-bounded T (number of queries) and q (number of inputs per query), TRE_{ih} is T -one-way.

We can also directly derive the concrete security for the *sequential* oracle-query timing model by setting $q := 1$. \square

H Hash-based revocable timed-release encryptions

We can now combine our results on timed-release encryptions in the random oracle model with the construction of a revocably one-way timed-release encryption (Section 3) to get the following revocably hiding timed-release encryption in the random oracle model.

Definition 12 (Hash-based revocable timed-release encryption) *Let ℓ be an integer and η the security parameter. Assume three random oracles $G : \{0, 1\}^\eta \rightarrow \{0, 1\}^\ell$ and $H : \{0, 1\}^{2\eta} \rightarrow \{0, 1\}^\eta$ and $L : \{0, 1\}^{2\eta} \rightarrow \{0, 1\}^{2\eta}$. We construct a revocable timed-release encryption $\text{RTRE}_{\text{hash}}$ with message space $\{0, 1\}^\ell$.*

Encryption of a message $m \in \{0, 1\}^\ell$:

- Pick $k, k^*, p, B, a \xleftarrow{\$} \{0, 1\}^\eta$.
- Construct the state $|\Psi\rangle := |k \oplus p\rangle_B$.
- $h_1 := H_a^{T+1}(0^\eta) \oplus k^*$ where $H_a(x) := H(a\|x)$.
- $h_2 := L(a\|k^*) \oplus (B\|p)$.
- $c := G(k) \oplus m$.
- The timed-release encryption consists of $V := (h_1, h_2, a, c)$ and $|\Psi\rangle$.

Decryption is performed as follows:

- Given $V = (h_1, h_2, a, c)$, compute $(B\|p) := h_2 \oplus L(a\|(h_1 \oplus H_a^{T+1}(0^\eta)))$.
- Measure $|\Psi\rangle$ in basis B ; call the outcome γ .
- Return $m := G(\gamma \oplus p) \oplus c$.

The **revocation** protocol is the following:

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

Theorem 13 ($\text{RTRE}_{\text{hash}}$ is revocably hiding) *The timed-release encryption $\text{RTRE}_{\text{hash}}$ from Definition 12 is T -revocably hiding and T -hiding in the random oracle model, assuming the parallel oracle-query timing model.*

Proof. The timed-release encryption TRE_{ih} from Definition 11 (with $n := \eta$ and using an oracle $H : \{0, 1\}^\eta \rightarrow \{0, 1\}^\eta$) is T -one-way without offline-queries by Theorem 12 and has message space $\{0, 1\}^\eta$. Applying the transformation from Theorem 10 (with $n = m = \eta$ and using an oracle $L : \{0, 1\}^\eta \rightarrow \{0, 1\}^{2\eta}$), we get a timed-release encryption with message space $\{0, 1\}^{2\eta}$ that is T -hiding without offline-queries and uses oracles $H : \{0, 1\}^\eta \rightarrow \{0, 1\}^\eta$ and $L : \{0, 1\}^\eta \rightarrow \{0, 1\}^{2\eta}$. Applying the transformation from Theorem 11 (with $\ell := \eta$), we get a timed-release encryption with message space $\{0, 1\}^{2\eta}$ that is T -hiding and uses oracles $H : \{0, 1\}^{2\eta} \rightarrow \{0, 1\}^\eta$ and $L : \{0, 1\}^{2\eta} \rightarrow \{0, 1\}^{2\eta}$. (To apply Theorem 11, we can assume that the oracles H, L are encoded into a single oracle.) By using this timed-release encryption as TRE_0 in the construction from Definition 7 (with $n := \eta$), we get a revocable timed-release encryption with message space $\{0, 1\}^\eta$ that is T -revocably one-way by Theorem 1. (Note for this that $\delta_T^{\text{ow}} = 0$ if we measure time in oracle queries because none of the operations listed in Theorem 1 query the oracle.) And it is T -hiding by Theorem 2 and thus, since its message space has superpolynomial size, also T -one-way. We then apply the transformation from Theorem 10 (with oracle $G : \{0, 1\}^\eta \rightarrow \{0, 1\}^\ell$), this leads to the timed-release encryption $\text{RTRE}_{\text{hash}}$ from Definition 12. By Theorem 10, $\text{RTRE}_{\text{hash}}$ is T -hiding and T -revocably hiding. \square

I Unknown recipient encryption

We describe an application of revocable timed-release encryptions: *unknown recipient encryption* (URE). Unknown recipient encryption 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 [DMS04], 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. We stress that URE is non-interactive, so this works even if no bidirectional communication is possible.

How does this work? Basically, unknown recipient encryption consists of a T -revocably hiding timed-release encryption V containing the message m . Then the sender sends V over the network to the recipient, and the recipient runs the revocation protocol to test whether V is unopened (we assume revocation to be non-interactive here). If revocation succeeds and the recipient got V within time T after sending, the T -revocable hiding property guarantees that no-one else could learn m . (From the point of view of the revocable timed-release encryption, the network channel becomes the timed-release encryption-recipient, and the network channel then gives the timed-release encryption back, but not to the URE-sender, but to the URE-recipient.)

There are several reasons why the above does not work with arbitrary timed-release encryptions. First, the revocation protocol might be destructive, i.e., after revocation, the recipient cannot decrypt the message any more. Fortunately, the timed-release encryptions described in this work do not have this problem.

Second, how does the recipient know how to perform the revocation test? For example, in the timed-release encryptions RTRE_{hid} , he needs to know the bases B , the indices Q , and the bits r . Fortunately, in the construction of RTRE_{hid} , anticipating this section, we included the values B, Q, r inside the inner timed-release encryption V_0 , even though only Q was needed for decrypting the timed-release encryption.²⁵

Third, to be able to refuse a URE that arrives more than time T after sending (and thus might have been copied), we need to let the recipient know the time t_0 of sending *in a secure way*. Similarly, we need to make sure that the values B, Q, r used for revocation are not modified by the attacker. To solve this problem, we assume a public key infrastructure, but we use it the other way around than is usual with encryption: the sender signs the values B, Q, r, t_0 , and the recipient can then check these using the sender's public key. (We need to be careful here: transmitting the signature in clear would be problematic since it might leak data about B, Q, r which could be used to cheat in the revocation. Instead, we include the signature inside the inner timed-release encryption V_0 .)

We now proceed to describe URE in more detail.

Definition 13 (Unknown recipient encryption) *An unknown recipient encryption (URE) scheme with message space M consists of a time parameter T , of a key generation algorithm keygen_1 , an encryption algorithm enc_1 and a decryption algorithm dec_1 . Here $\text{keygen}_1()$ produces a classical key pair (pk, sk) , $\text{enc}_1(sk, id, m)$ returns a (quantum) ciphertext C with plaintext m with unique id id ,²⁶ $\text{dec}_1(sk, C)$ returns a pair (m, id) .*

Unknown recipient encryption is assumed to have correctness: for any adversary A , the following probability is overwhelming:

$$\Pr[m = m' \wedge id = id' : (pk, sk) \leftarrow \text{keygen}_1, (m, id) \leftarrow A(pk), \\ C \leftarrow \text{enc}_1(sk, id, m), (m', id') \leftarrow \text{dec}_1(pk, C)].$$

Note that we have included a message id id in the definition of UREs. It will be assumed that no two messages are sent using the same id. The use of message ids greatly simplifies the definition of security below.

We assume a *global clock* available to all parties. When a computation takes time T (with respect to the timing model underlying the timed-release encryptions used below) then the global clock advances by *at least* T between start and end of that computation.

We now proceed to define security of UREs. Since we wish to use the same secret key for several encryptions, we need to model a security definition in which a number of messages can be encrypted. Basically, a URE guarantees is that any message that is successfully decrypted will be semantically secure. We model this by a game in which the adversary can produce a number of message pairs (m_0, m_1) to be encrypted with different ids id . For each id , it is randomly chosen which message to encrypt. If one of these messages is successfully decrypted by the recipient, then the adversary should be unable to tell which of the two message were encrypted for that id .

Definition 14 (Security of UREs) *We call an URE ($\text{keygen}_1, \text{enc}_1, \text{dec}_1$) secure iff for any sequential-polynomial-time adversary A (that may share state between invocations), the following is negligible*

$$\left| \Pr[b' = b_{id^*} : (pk, sk) \leftarrow \text{keygen}_1(), b_1 \xleftarrow{\$} \{0, 1\}, C \leftarrow A^E(pk), (m, id^*) \leftarrow \text{dec}_1(pk, C), b' \leftarrow A^E(pk, id^*) \right] - \frac{1}{2} \right|.$$

²⁵Note that in the case of RTRE_{ow} , we cannot include the necessary information in V_0 because the revocation protocol of RTRE_{ow} uses, besides other information, the message m itself. Including m in V_0 would make RTRE_{ow} non-revocable. Instead, we would have to change the revocation test of RTRE_{ow} to test only a subset of the bits, as done in RTRE_{hid} .

²⁶The id could also be picked by enc_1 itself, e.g., at random or sequentially. Then the security definition (Definition 14) has to be changed in a straightforward way so that the adversary does not pick the id himself but gets it from enc_1 .

Here E is an oracle that upon invocation $E(m_0, m_1, id)$ does: If E was already called with that id , return \perp . Else pick $b_{id} \xleftarrow{\$} \{0, 1\}$ and return $enc_1(sk, id, m_{b_{id}})$.

Notice that our security definition does not guarantee any flavor of integrity or non-malleability. However, such could be easily added to an existing URE: Instead of encrypting m , encrypt a signed message m .

We can now proceed to formalize our URE construction (that was sketched above). Our construction is based specifically on the timed-release encryption $RTRE_{hid}$ from Section 4.

Definition 15 (URE from timed-release encryptions) Let $(sigkeygen, sign, verify)$ be an existentially quantum-unforgeable signature scheme. Let TRE_0 be a revocable timed-release encryption. Let $RTRE_{sk,t_0,id}$ be defined like $RTRE_{hid}$ (Definition 9), except that $V_0 \leftarrow TRE_0(B, Q, r, p)$ is replaced by $\sigma := sign(sk, (B, Q, r, t_0, id))$, $V_0 \leftarrow TRE_0(B, Q, r, p, \sigma)$. We define an unknown recipient encryption scheme $URE(T')$ (parametric in a time duration T') as follows:

- **Key generation:** $keygen_1() := sigkeygen()$.
- **Encryption:** $enc_1(sk, id, m)$ does: Let t_0 be the current time (more precisely, any time not later than the time when enc_1 returns). Let $V := RTRE_{sk,t_0,id}(m)$. Return $C := (t_0, id, V)$.
- **Decryption:** $dec_1(pk, (t_0, id, V))$ does: Let t_1 be the current time. Decrypt the timed-release encryption V_0 contained in V to get B, Q, r, p, σ . Run the revocation test of $RTRE_{sk,t_0,id}$ using those values B, Q, r . Run $verify(pk, \sigma, (B, Q, r, t_0, id))$. Check if $t_1 \leq t_0 + T'$. If all three checks succeed, decrypt V (as specified in the definition of $RTRE_{hid}$) to get m and return (m, id) . If one of the three checks fails, return (\perp, \perp) .

Finally, we can show security.

Theorem 14 Assume that the timing model satisfies the following condition: For any algorithm A' , the following algorithm can be implemented in time T' : Run algorithm A' and abort if A' runs more than time T' .²⁷

Assume the conditions of Theorem 3 are satisfied. Let δ_T^{hid}, ℓ be as in Theorem 3. Let $T' := T - \delta_T^{hid}$. Then $URE(T')$ is a secure URE with message space $\{0, 1\}^\ell$.

This even holds if we allow the adversary A to be computationally unlimited after the invocation of dec_1 in Definition 14 (i.e., we have everlasting security).

Proof. We prove this with a sequence of games. The first game is the game from Definition 14.

Game 1 (Original game)

- $(pk, sk) \leftarrow keygen_1()$.
- $b_\perp \xleftarrow{\$} \{0, 1\}$.
- $C \leftarrow A^E(pk)$.
- $(m, id^*) \leftarrow dec_1(pk, C)$.
- $b' \leftarrow A^E(pk, id^*)$.

We need to show that $|\Pr[b' = b_{id^*} : \text{Game 1}] - \frac{1}{2}|$ is negligible.

We now unfold the definition of dec_1 . For convenience, for a timed-release encryption V returned by $RTRE_{sk,t_0,id}$, let $getV_0(V)$ return the contained timed-release encryption V_0 contained in V . Let $decTRE_0(V)$ denote the decryption of $getV_0(V)$ (using the decryption algorithm of TRE_0). Let $revocRTRE(V, B, Q, r)$ denote the revocation test of $RTRE_{sk,t_0,id}$ on timed-release encryption V using values B, Q, r .

Note that in the following game, we omitted the computation of m (by dec_1) because m is never used anyway.

Game 2 (Unfolding dec_1)

- $(pk, sk) \leftarrow keygen_1()$.
- $b_\perp \xleftarrow{\$} \{0, 1\}$.
- $(t_0, id, V) \leftarrow A^E(pk)$.
- ~~$(m, id^*) \leftarrow dec_1(pk, V)$~~
- $t_1 \leftarrow currentTime()$

²⁷Parallel and sequential oracle-query timing-models satisfy this. Also “real life” satisfies this (at least approximately) because one can just use a timer to abort after T' steps.

- (f) $(B, Q, r, p, \sigma) = \text{decTRE}_0(\text{getV}_0(V))$.
- (g) $ok \leftarrow \text{revocRTRE}(V, B, Q, r)$.
- (h) $\text{sigOk} \leftarrow \text{verify}(pk, \sigma, (B, Q, r, t_0, id))$
- (i) $\text{timeOk} \leftarrow (t_1 \leq t_0 + T')$
- (j) $\text{allOk} := ok \wedge \text{sigOk} \wedge \text{timeOk}$.
- (k) If $\text{allOk} = 1$, $id^* := id$. Else $id^* := \perp$.
- (l) $b' \leftarrow A^E(pk, id^*)$

We then immediately have $\Pr[b' = b_{id^*} : \text{Game 1}] = \Pr[b' = b_{id^*} : \text{Game 2}]$

During the first invocation of A (step (c)), A makes a number of queries $E(\cdot, \cdot, id)$. Invocations $E(\cdot, \cdot, id)$ with an id that was not used before we call *fresh*. Let id_j denote the id used in the j -th fresh query.

Let B_{id}, Q_{id}, r_{id} denote the values chosen by $\text{RTRE}_{sk, t_0, id}$ during the fresh oracle query $E(\cdot, \cdot, id)$, and let $t_{0, id}$ denote the value t_0 chosen in that query.

We now change the revocation test in the previous game such that instead of using B, Q, r as extracted from V , we use the original values $B_{id}, Q_{id}, r_{id}, t_{0, id}$ used in the creation of the timed-release encryption. Additionally, we assign a default value for the session id output by A if it is not an existing session, and finally we guess the session which the adversary attacks (but that guess j is not used anywhere yet). Let $\#E$ denote a polynomial upper bound on the number of oracle queries performed by A during its first invocation.

Game 3 (Using B_{id}, Q_{id}, r_{id})

- (a) $j \xleftarrow{\$} \{1, \dots, \#E\}$.
- (b) $(pk, sk) \leftarrow \text{keygen}_1()$.
- (c) $b_\perp \xleftarrow{\$} \{0, 1\}$.
- (d) $(t_0, id, V) \leftarrow A^E(pk)$.
- (e) $t_1 \leftarrow \text{currentTime}()$
- (f) If $\exists j. id = id_j$, then $id := id_1$.
- (g) $(B, Q, r, p, \sigma) = \text{decTRE}_0(\text{getV}_0(V))$.
- (h) $ok \leftarrow \text{revocRTRE}(V, B_{id}, Q_{id}, r_{id})$.
- (i) $\text{sigOk} \leftarrow \text{verify}(pk, \sigma, (B, Q, r, t_0, id))$.
- (j) $\text{timeOk} \leftarrow (t_1 \leq t_{0, id} + T')$.
- (k) $\text{allOk} := ok \wedge \text{sigOk} \wedge \text{timeOk}$.
- (l) If $\text{allOk} = 1$, $id^* := id$. Else $id^* := \perp$.
- (m) $b' \leftarrow A^E(pk, id^*)$.

Games 2 and 3 only differ when $((B, Q, r, t_0) \neq (B_{id}, Q_{id}, r_{id}, t_{0, id}) \vee \exists j. id = id_j) \wedge \text{sigOk} = 1$ in Game 2. But $(B, Q, r, t_0) \neq (B_{id}, Q_{id}, r_{id}, t_{0, id}) \vee \exists j. id = id_j$ implies that E did not sign (B, Q, r, t_0, id) before step (i) (by construction of enc_1 and the fact that each invocation of E uses a different id). In this case $\text{sigOk} = 1$ implies that σ is a forgery, which happens only with negligible probability since sign is existentially quantum-unforgeable. (In the statement of the lemma, we have allowed A to be computationally unlimited after invoking dec_1 . However, this impacts only step (m), all other steps remain polynomial-time, hence we can apply unforgeability here.) So $\Pr[((B, Q, r, t_0) \neq (B_{id}, Q_{id}, r_{id}, t_{0, id}) \vee \exists j. id = id_j) \wedge \text{sigOk} = 1 : \text{Game 2}] \leq \mu_1$ for some negligible μ_1 and hence $|\Pr[b' = b_{id^*} : \text{Game 2}] - \Pr[b' = b_{id^*} : \text{Game 3}]| \leq \mu_1$.

Now we will only allow A to make its final guess when we guess correctly which session A will attack. (More precisely, if the guess is wrong, we set $\text{allOk} := 0$ which means that A then has probability exactly $\frac{1}{2}$ of guessing $b_{id^*} = b_\perp$.)

Game 4 (Guessing the session)

- (a) $j \xleftarrow{\$} \{1, \dots, \#E\}$.
- (b) $(pk, sk) \leftarrow \text{keygen}_1()$.
- (c) $b_\perp \xleftarrow{\$} \{0, 1\}$.
- (d) $(t_0, id, V) \leftarrow A^E(pk)$.
- (e) $t_1 \leftarrow \text{currentTime}()$
- (f) If $\exists j. id = id_j$, then $id := id_1$.
- (g) $(B, Q, r, p, \sigma) = \text{decTRE}_0(\text{getV}_0(V))$.
- (h) $ok \leftarrow \text{revocRTRE}(V, B_{id}, Q_{id}, r_{id})$.
- (i) $\text{sigOk} \leftarrow \text{verify}(pk, \sigma, (B, Q, r, t_0, id))$.

- (j) $timeOk \leftarrow (t_1 \leq t_{0,id} + T')$.
- (k) $allOk := ok \wedge sigOk \wedge timeOk \wedge id = id_j$.
- (l) If $allOk = 1$, $id^* := id$. Else $id^* := \perp$.
- (m) $b' \leftarrow A^E(pk, id^*)$.

First, observe that due to step (f), $id = id_j$ holds for some $j \in \{1, \dots, \#E\}$. Thus $id = id_j$ holds with probability $1/\#E$ and whether it holds is independent of the state of A and of all other random variables before step (k). Furthermore, if $id \neq id_j$, then in (m) we have $id^* = \perp$ and hence $b' = b_{id^*}$ with probability exactly $\frac{1}{2}$. Thus

$$\begin{aligned} |\Pr[b' = b_{id^*} : \text{Game 4}] - \frac{1}{2}| &= \left| \overbrace{\left(\Pr[b' = b_{id^*} | id \neq id_j : \text{Game 4}] - \frac{1}{2} \right)}^{=\frac{1}{2}} \Pr[id \neq id_j : \text{Game 4}] \right. \\ &\quad \left. + \overbrace{\left(\Pr[b' = b_{id^*} | id = id_j : \text{Game 4}] - \frac{1}{2} \right)}_{=\Pr[b'=b_{id^*}:\text{Game 3}]} \Pr[id = id_j : \text{Game 4}] \right| \\ &= \frac{1}{\#E} |\Pr[b' = b_{id^*} : \text{Game 3}] - \frac{1}{2}|. \end{aligned}$$

Thus so far we have

$$|\Pr[b' = b_{id^*} : \text{Game 1}] - \frac{1}{2}| \leq \mu_1 + \#E \cdot |\Pr[b' = b_{id^*} : \text{Game 4}] - \frac{1}{2}|.$$

We now change the game such that in the revocation test, we always use B, Q, r from session j .

Game 5 (Revocation from session j)

- (a) $j \xleftarrow{\$} \{1, \dots, \#E\}$.
- (b) $(pk, sk) \leftarrow keygen_1()$.
- (c) $b_\perp \xleftarrow{\$} \{0, 1\}$.
- (d) $(t_0, id, V) \leftarrow A^E(pk)$.
- (e) $t_1 \leftarrow currentTime()$
- (f) If $\#j.id = id_j$, then $id := id_1$.
- (g) $(B, Q, r, p, \sigma) = decTRE_0(getV_0(V))$.
- (h) $ok \leftarrow revocRTRE(V, B_{id_j}, Q_{id_j}, r_{id_j})$.
- (i) $sigOk \leftarrow verify(pk, \sigma, (B, Q, r, t_0, id))$.
- (j) $timeOk \leftarrow (t_1 \leq t_{0,id} + T')$.
- (k) $allOk := ok \wedge sigOk \wedge timeOk \wedge id = id_j$.
- (l) If $allOk = 1$, $id^* := id$. Else $id^* := \perp$.
- (m) $b' \leftarrow A^E(pk, id^*)$.

If $id = id_j$, then $B_{id_j}, Q_{id_j}, r_{id_j} = B_{id}, Q_{id}, r_{id}$, and if $id \neq id_j$, then $b' = b_{id^*} = b_\perp$ with probability $\frac{1}{2}$, no matter which inputs are given to $revocRTRE$. Hence $\Pr[b' = b_{id^*} : \text{Game 5}] = \Pr[b' = b_{id^*} : \text{Game 4}]$.

Now we split the adversary: The first invocation of A is split into two parts: $A_0(pk, j)$ performs all steps before the j -th fresh query to E and outputs E 's input (m_0, m_1, id') . And A'_1 takes as input the reply to the j -th fresh query and continues with the computation. Furthermore, we rename the second invocation of A to be A_2 . Also, we unfold the definitions of E and enc_1 for the j -th query. (And the values B, Q, r, t_0, id from that query are now called $B^*, Q^*, r^*, t_0^*, id'$ instead of $B_{id_j}, Q_{id_j}, r_{id_j}, t_{0,id_j}, id_j$.)

Game 6 (Splitting A)

- (a) $j \xleftarrow{\$} \{1, \dots, \#E\}$.
- (b) $(pk, sk) \leftarrow keygen_1()$.
- (c) $b_\perp \xleftarrow{\$} \{0, 1\}$.
- (d) ~~$(t_0, id, V) \leftarrow A^E(pk)$~~ .
- (e) $(m_0, m_1, id') \leftarrow A_0^E(pk, j)$.
- (f) $b \xleftarrow{\$} \{0, 1\}$. $b_{id'} := b$. $t_0^* \leftarrow currentTime()$. $V^* \leftarrow RTRE_{sk, t_0^*, id'}(m_b)$.
- (g) Denote the values B, Q, r chosen by $RTRE_{sk, t_0^*, id'}$ with B^*, Q^*, r^* .
- (h) $(t_0, id, V) \leftarrow (A'_1)^E((t_0^*, id', V^*))$.
- (i) $t_1 \leftarrow currentTime()$
- (j) If $\#j.id = id_j$, then $id := id_1$.
- (k) $(B, Q, r, p, \sigma) = decTRE_0(getV_0(V))$.

- (l) $ok \leftarrow \text{revocRTRE}(V, B^*, Q^*, r^*)$.
- (m) $\text{sigOk} \leftarrow \text{verify}(pk, \sigma, (B, Q, r, t_0, id))$.
- (n) $\text{timeOk} \leftarrow (t_1 \leq t_0^* + T')$.
- (o) $\text{allOk} := ok \wedge \text{sigOk} \wedge \text{timeOk} \wedge id = id'$.
- (p) If $\text{allOk} = 1$, $id^* := id$. Else $id^* := \perp$.
- (q) $b' \leftarrow A_2^E(pk, id^*)$.

We have only split the adversary and unfolded the definitions of E and enc_1 , all computations stay the same. Hence $\Pr[b' = b_{id^*} : \text{Game 6}] = \Pr[b' = b_{id^*} : \text{Game 5}]$.

Now we constrain A'_1 to run at most time T' . That is, let A_1 be like A'_1 , except that it aborts after time T' (including the time spent by the oracle E).

Game 7 (A_1 runs time T')

- (a) $j \xleftarrow{\$} \{1, \dots, \#E\}$.
- (b) $(pk, sk) \leftarrow \text{keygen}_1()$.
- (c) $b_\perp \xleftarrow{\$} \{0, 1\}$.
- (d) $(m_0, m_1, id') \leftarrow A_0^E(pk, j)$.
- (e) $b \xleftarrow{\$} \{0, 1\}$. $b_{id'} := b$. $t_0^* \leftarrow \text{currentTime}()$.
- (f) $V^* \leftarrow \text{RTRE}_{sk, t_0^*, id'}(m_b)$.
- (g) Denote the values B, Q, r chosen by $\text{RTRE}_{sk, t_0^*, id'}$ with B^*, Q^*, r^* .
- (h) $(t_0, id, V) \leftarrow A_1^E((t_0^*, id', V^*))$.
- (i) $t_1 \leftarrow \text{currentTime}()$.
- (j) If $\nexists j.id = id_j$, then $id := id_1$.
- (k) $(B, Q, r, p, \sigma) = \text{decTRE}_0(\text{getV}_0(V))$.
- (l) $ok \leftarrow \text{revocRTRE}(V, B^*, Q^*, r^*)$.
- (m) $\text{sigOk} \leftarrow \text{verify}(pk, \sigma, (B, Q, r, t_0, id))$.
- (n) $\text{timeOk} \leftarrow (t_1 \leq t_0^* + T')$.
- (o) $\text{allOk} := ok \wedge \text{sigOk} \wedge \text{timeOk} \wedge id = id'$.
- (p) If $\text{allOk} = 1$, $id^* := id$. Else $id^* := \perp$.
- (q) $b' \leftarrow A_2^E(pk, id^*)$.

If A'_1 runs more than T' steps, we will have $t_1 > t_0^* + T'$ and thus $\text{timeOk} = 0$, and then the adversary guesses $b_{id^*} = b_\perp$ with probability exactly $\frac{1}{2}$, independent of whether A'_1 continues to run or not. Thus $\Pr[b' = b_{id^*} : \text{Game 7}] = \Pr[b' = b_{id^*} : \text{Game 6}]$.

Furthermore, if $\text{allOk} = 0$, then $id^* = \perp$ and hence b' equals $b_{id^*} = b_\perp$ with probability $\frac{1}{2}$. Similarly, $(b' \wedge \text{allOk}) = 0$ equals $b_{id^*} = b_\perp$ with probability $\frac{1}{2}$. And if $\text{allOk} = 1$, then $b' = (b' \wedge \text{allOk})$. Thus $\Pr[b' = b_{id^*} : \text{Game 6}] = \Pr[(b' \wedge \text{allOk}) = b_{id^*} : \text{Game 6}]$.

Moreover, if $\text{allOk} = 1$, then $b_{id^*} = b$. And if $\text{allOk} = 0$, then $(b' \wedge \text{allOk}) = 0$ has the same probability of being $b_{id^*} = b_\perp$ and of being b (namely $\frac{1}{2}$). Thus $\Pr[(b' \wedge \text{allOk}) = b_{id^*} : \text{Game 6}] = \Pr[(b' \wedge \text{allOk}) = b : \text{Game 6}]$.

Thus so far we have

$$|\Pr[b' = b_{id^*} : \text{Game 1}] - \frac{1}{2}| \leq \mu_1 + \#E \cdot |\Pr[(b' \wedge \text{allOk}) = b : \text{Game 7}] - \frac{1}{2}|.$$

Let $B_0()$ run steps (a)–(e), except for picking b and $b_{id'}$, and let B_0 return $(m_0, m_1, sk, t_0^*, id')$. Let $B_1(V^*)$ run $(t_0, id, V) \leftarrow A_1((t_0^*, id', V^*))$ (here id', V^* are known to B_1 because they were chosen by B_0) and return V . Let $B_2(ok)$ run steps (i)–(k) and steps (m)–(q) and return $(b' \wedge \text{allOk})$. All of B_0, B_1, B_2 also simulate the oracle E themselves, this is possible since sk is known to B_0, B_1, B_2 . When writing $\text{revocRTRE}(V)$, we mean an execution of the revocation test of $\text{RTRE}_{sk, t_0^*, id'}$. (I.e., $\text{revocRTRE}(V)$ is the same as $\text{revocRTRE}(V, B, Q, r)$ using the values B, Q, r chosen by the earlier call $\text{RTRE}_{sk, t_0^*, id'}$.)

Then we can rewrite Game 7 as follows:

Game 8 (Using B)

- (a) $b \xleftarrow{\$} \{0, 1\}$.
- (b) $(m_0, m_1, sk, t_0^*, id') \leftarrow B_0()$.
- (c) $V^* \leftarrow \text{RTRE}_{sk, t_0^*, id'}(m_b)$.
- (d) $V \leftarrow B_1(V^*)$.
- (e) $ok \leftarrow \text{revocRTRE}(V)$.

(f) $b'' = B_2(ok)$.

And we get $\Pr[(b' \wedge allOk) = b : \text{Game 7}] = \Pr[b'' = b : \text{Game 8}]$.

Thus so far we have

$$\left| \Pr[b' = b_{id^*} : \text{Game 1}] - \frac{1}{2} \right| \leq \mu_1 + \#E \cdot \left| \Pr[b'' = b : \text{Game 8}] - \frac{1}{2} \right|.$$

Let Game 8(0) denote Game 8 with $b := 0$ fixed, and analogously Game 8(1).

Then we have

$$\begin{aligned} \left| \Pr[b'' = b : \text{Game 8}] - \frac{1}{2} \right| &= \left| \frac{1}{2} \Pr[b'' = 1 : \text{Game 8(1)}] + \frac{1}{2} (1 - \Pr[b'' = 1 : \text{Game 8(0)}]) - \frac{1}{2} \right| \\ &= \frac{1}{2} \left| \Pr[b'' = 1 : \text{Game 8(1)}] - \Pr[b'' = 1 : \text{Game 8(0)}] \right| =: \mu_2. \end{aligned}$$

For the next step, we will need the security of $\text{RTRE}_{sk, t_0^*, id'}$. Theorem 3 states that RTRE_{hid} is T' -revocably hiding, but $\text{RTRE}_{sk, t_0^*, id'}$ differs from RTRE_{hid} by additionally including $\sigma := \text{sign}(sk, (B, Q, r, t_0^*, id'))$. However, the proof of Theorem 3 still goes through for this modified scheme. (In fact, σ is a function of public parameters sk, t_0^*, id' , and of data B, Q, r that is contained in V_0 anyway. So it is not surprising that the inclusion of σ does not reduce security.) Thus $\text{RTRE}_{sk, t_0^*, id'}$ is $T' = (T - \delta_T^{hid})$ -revocably hiding even when we allow the adversary to be computationally unlimited in its last invocation (everlasting security).

Furthermore, B_0 and B_1 are sequential-polynomial-time, and B_1 runs in time T' (since B_1 just invokes A_1 which aborts after time T' by definition). (B_2 can be unlimited because in the statement of the lemma, A is allowed to be computationally unlimited after invoking dec_1 .) Thus, since $\text{RTRE}_{sk, t_0^*, id'}$ is T' -revocably hiding with everlasting security, μ_2 is negligible.

So altogether we have

$$\left| \Pr[b' = b_{id^*} : \text{Game 1}] - \frac{1}{2} \right| \leq \mu_1 + \#E \cdot \mu_2.$$

which is negligible. Hence $\text{URE}(T')$ is secure. \square

UREs without public key infrastructure. Our construction of UREs requires the sender to sign part of his messages. Without a public key infrastructure, our security definition (Definition 14) is clearly unsatisfiable: the adversary could intercept a ciphertext C , decrypt it to get m , reencrypt it, and send it on (using a fresh time-stamp t_0). However, even if we drop the signature from our construction, some flavor of security seems still to be guaranteed. Roughly: “an encrypted message m that is successfully decrypted within time T cannot be known to others”. This could still be useful if the message m itself carries some proof about its creation time (e.g., if it depends on public data that was produced only recently). We leave it as an open question what security can be achieved with UREs that do not use a public key infrastructure.

References

- [ABB⁺07] Romain Allaume, Jan Bouda, Cyril Branciard, Thierry Debuisschert, Mehrdad Dianati, Nicolas Gisin, Mark Godfrey, Philippe Grangier, Thomas Langer, Anthony Leverrier, Norbert Lutkenhaus, Philippe Painchault, Momtchil Peev, Andreas Poppe, Thomas Pornin, John Rarity, Renato Renner, Gregoire Ribordy, Michel Riguide, Louis Salvail, Andrew Shields, Harald Weinfurter, and Anton Zeilinger. Secoqc white paper on quantum key distribution and cryptography. arXiv:quant-ph/0701168v1, 2007.
- [AMTW00] Andris Ambainis, Michele Mosca, Alain Tapp, and Ronald de Wolf. Private quantum channels. In *FOCS 2000*, pages 547–553. IEEE, 2000.
- [AS72] Milton Abramowitz and Irene A. Stegun, editors. *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables*. U.S. Department of Commerce, 10th printing edition, 1972. Online available at <http://www.math.hkbu.edu.hk/support/aands/toc.htm>.
- [BB84] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public-key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing 1984*, pages 175–179. IEEE Computer Society, 1984.

- [BCCT12] Nir Bitansky, Ran Canetti, Alessandro Chiesa, and Eran Tromer. From extractable collision resistance to succinct non-interactive arguments of knowledge, and back again. In *ITCS '12*, pages 326–349, New York, NY, USA, 2012. ACM.
- [BDF⁺11] Dan Boneh, Özgür Dagdelen, Marc Fischlin, Anja Lehmann, Christian Schaffner, and Mark Zhandry. Random oracles in a quantum world. In *ASIACRYPT 2011*, pages 41–69, Berlin, Heidelberg, 2011. Springer-Verlag.
- [BN00] Dan Boneh and Moni Naor. Timed commitments. In *Crypto 2000*, pages 236–254. Springer, 2000.
- [CKW00] Valerie Coffman, Joydip Kundu, and William K. Wootters. Distributed entanglement. *Phys. Rev. A*, 61:052306, Apr 2000.
- [CM97] Christian Cachin and Ueli Maurer. Unconditional security against memory-bounded adversaries. In Burton S. Kaliski Jr., editor, *Advances in Cryptology, Proceedings of CRYPTO '97*, volume 1294 of *LNCS*, pages 292–306. Springer, 1997.
- [CS96] A. R. Calderbank and P. W. Shor. Good quantum error-correcting codes exist. *Phys. Rev. A*, 54:1098, 1996. arXiv:quant-ph/9512032v2.
- [DFSS05] Ivan Damgård, Serge Fehr, Louis Salvail, and Christian Schaffner. Cryptography in the bounded quantum-storage model. In *FOCS 2005*, pages 449–458, 2005. Full version is arXiv:quant-ph/0508222v2.
- [DMS04] Roger Dingledine, Nick Mathewson, and Paul Syverson. Tor: the second-generation onion router. In *USENIX 2004, SSYM'04*, pages 21–21, Berkeley, CA, USA, 2004. USENIX Association.
- [DN93] C. Dwork and M. Naor. Pricing via processing, or, combatting junk mail. In Ernest F. Brickell, editor, *Advances in Cryptology, Proceedings of CRYPTO '92*, volume 740 of *Lecture Notes in Computer Science*, pages 139–147. Springer-Verlag, 1993.
- [DNS12] Frédéric Dupuis, Jesper Buus Nielsen, and Louis Salvail. Actively secure two-party evaluation of any quantum operation. In Reihaneh Safavi-Naini and Ran Canetti, editors, *Crypto 2012*, volume 7417 of *LNCS*, pages 794–811. Springer, 2012.
- [EPR35] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47:777–780, May 1935.
- [Eur06] 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. Online available <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF>.
- [HU05] Dennis Hofheinz and Dominique Unruh. Comparing two notions of simulatability. In *Theory of Cryptography, Proceedings of TCC 2005*, Lecture Notes in Computer Science, pages 89–103. Springer-Verlag, February 2005.
- [KSH⁺13] Kaveh Khodjasteh, Jarrah Sastrawan, David Hayes, Todd J. Green, Michael J. Biercuk, and Lorenza Viola. Designing a practical high-fidelity long-time quantum memory. *Nature Communications*, 4:–, 2013.
- [MMV11] Mohammad Mahmoody, Tal Moran, and Salil Vadhan. Time-lock puzzles in the random oracle model. In Phillip Rogaway, editor, *Crypto 2011*, volume 6841 of *LNCS*, pages 39–50. Springer, 2011.
- [MQU07] Jörn Müller-Quade and Dominique Unruh. <http://eprint.iacr.org/2006/422>, January 2007.
- [NC10] M. Nielsen and I. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, 10th anniversary edition, 2010.

- [Pal10] Elizabeth Palmer. Wikileaks backup plan could drop diplomatic bomb. *CBS News*, December 2010. <http://www.cbsnews.com/stories/2010/12/02/eveningnews/main7111845.shtml>.
- [Rab03] Michael O. Rabin. Hyper-encryption by virtual satellite. Science Center Research Lecture Series, December 2003. Online available at <http://athome.harvard.edu/programs/hvs/>.
- [Riv99] Ron Rivest. Description of the lcs35 time capsule crypto-puzzle. <http://people.csail.mit.edu/rivest/lcs35-puzzle-description.txt>, April 1999.
- [RSW96] Ronald L. Rivest, Adi Shamir, and David A. Wagner. Time-lock puzzles and timed-release crypto. Technical Report MIT/LCS/TR-684, Massachusetts Institute of Technology, February 1996. Online available at <http://theory.lcs.mit.edu/~rivest/RivestShamirWagner-timelock.ps>.
- [Sho94] Peter W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *35th Annual Symposium on Foundations of Computer Science, Proceedings of FOCS 1994*, pages 124–134. IEEE Computer Society, 1994.
- [SP00] Peter W. Shor and John Preskill. Simple proof of security of the bb84 quantum key distribution protocol. *Phys. Rev. Lett.*, 85:441–444, Jul 2000.
- [Ste96] A. M. Steane. Multiple particle interference and quantum error correction. *Proc. R. Soc. London A*, 452:2551–76, 1996.
- [Unr06] Dominique Unruh. *Protokollkomposition und Komplexität (Protocol Composition and Complexity)*. PhD thesis, Universität Karlsruhe (TH), Berlin, 2006. In German, online available at <http://www.cs.ut.ee/~unruh/publications/unruh07protokollkomposition.html>.
- [Zha12] Mark Zhandry. Secure identity-based encryption in the quantum random oracle model. In *Crypto 2012*, volume 7417 of *LNCS*, pages 758–775. Springer, 2012.

Symbol index

$\text{sigkeygen}()$	Key generation for signature scheme	52
$\text{sign}(sk, m)$	Signing algorithm (signature scheme)	52
$\text{verify}(pk, \sigma, m)$	Verification algorithm (signature scheme)	52
$\text{RTRE}_{sk, t_0, id}$	Variant of revocable timed-release encryption RTRE_{hid} , used in URE scheme	52
RTRE_{hash}	Revocably hiding timed-release encryption from Definition 12	50
enc_1	Unknown recipient encryption	51
dec_1	Unknown recipient decryption	51
keygen_1	Unknown recipient encryption key generation	51
$\text{URE}(T')$	Unknown recipient encryption scheme	52
P_t^{EPR}	EPR states with max. t phase and t bit flips	20
TRE_{ih}	Timed-release encryption by iterated hashing Definition 11	47
$\omega(x)$	Hamming weight of x	4
\oplus	Bitwise XOR	4
$[q + n]_q$	Set of all subsets of $\{1, \dots, q + n\}$ of size q	4
$ \beta_{fe}\rangle$	Bell state	4
C^\perp	Dual code	4
$ \widetilde{xy}\rangle$	EPR state with phase flips f and bit flips e	4
$ m\rangle_B$	m encoded in basis B	4
$\ A\ $	Operator norm of A	4
$\ x\ $	Euclidean norm of x	4
P_{C_1/C_2}^{EPR}	EPR state in $\mathbb{C}^{C_1/C_2} \otimes \mathbb{C}^{C_1/C_2}$	30
P_x^{uv}	Projector of measurement M_X^{uv} for outcome x	30
RTRE_{ow}	Revocably one-way timed-release encryption from Definition 7	7
$\text{TD}(\rho_1, \rho_2)$	Trace distance between ρ_1 and ρ_2 .	4
δ_T^{hid}	Time loss in revocably hiding timed-release encryption	14

RTRE_{hid}	Revocably hiding timed-release encryption from Definition 9	13
C/D	Quotient of codes C and D	26
δ_T^{ow}	Time loss in revocably one-way timed-release encryption	19
$ \xi_{xuv}\rangle$	Codewords in CCS code	26
$x \bmod C$	Projection into quotient code D/C	26
U_{uv}^{dec}	Decoding for the CCS code $\{ \xi_{xuv}\rangle\}_x$	27
U_{uv}^{EC}	Error correction and decoding for the CCS code $\{ \xi_{xuv}\rangle\}_x$	27
$isEPR$	Boolean indicating whether checking for t -error EPR state succeeded.	22
P_B^-	Measures if two registers are equal in basis B	20
M_X^{uv}	Measure x in a state $ r\rangle \xi_{xuv}\rangle$, given u, v	30
P_{uv}	Projector of measurement M_{UV} for outcome u, v	30
M_{UV}	Measures u, v in a state $ r\rangle \xi_{xuv}\rangle$	30
P_r	Projector of measurement M_R for outcome r	30
M_R	Measures first q bits	30
$\text{im } M$	Image of operator/function M	

Keyword index

clock	without offline-queries, 16
global, 51	oracle-query timing model
correctness	parallel, 15
unknown recipient encryption, 51	sequential, 15
early key revelation, 13	parallel oracle-query timing model, 15
encryption	polynomial time
timed-release, 5	sequential, 5
unknown recipient, 51	protocol
EPR pair, 4	revocation, 6
EPR state, 4	revocably hiding, 7
global clock, 51	without offline-queries, 16
hiding, 6	revocably one-way, 6, 7
revocably, 7	revocation protocol, 6
revocably, without offline-queries, 16	secure (unknown recipient encryption), 51
without offline-queries, 16	sequential oracle-query timing model, 15
key revelation	sequential polynomial time, 5
early, 13	time
late, 13	sequential polynomial, 5
late key revelation, 13	timed-release encryption, 5
offline-queries	timing model, 5
hiding without, 16	parallel oracle-query, 15
one-way without, 16	sequential oracle-query, 15
revocably hiding without, 16	TRE, <i>see</i> timed-release encryption
one-way	unknown recipient encryption, 51
revocably, 6, 7	security, 51
	URE, <i>see</i> unknown recipient encryption