# Revocable quantum timed-release encryption

Dominique Unruh
University of Tartu

October 23, 2019

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

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

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

**1 Introduction** **2**
1.1 Example applications . . . . . 2
1.2 Our contribution . . . . . 4
1.3 Related work . . . . . 6
1.4 Organization . . . . . 6
1.5 Preliminaries . . . . . 7

**2 Defining revocable TREs** **7**

**3 Constructing revocably one-way TREs** **10**

**4 CSS codes – recap and properties** **14**

**5 Revocably hiding TREs** **16**
5.1 Relation to quantum authentication codes and uncloneable encryption . . . . . 21

**6 TREs in the random oracle model** **22**
6.1 One-way to hiding . . . . . 22
6.2 Precomputation . . . . . 26
6.3 Iterated hashing . . . . . 28

**7 Unknown recipient encryption** **30**

**A Auxiliary lemmas** **38**

**B Full proof: revocably one-way timed-release encryptions** **40**

**C Full proofs: CSS codes** **47**
C.1 Proof of Lemma 1 . . . . . 47
C.2 Proof of Lemma 2 . . . . . 48
C.3 Proof of Lemma 3 . . . . . 48
C.4 Proof of Lemma 4 . . . . . 49

**D Full proofs: revocably hiding timed-release encryptions** **51**

**E Full proofs: one-way to hiding** **63**

**F Full proofs: precomputation** **65**

**G Full proofs: iterated hashing** **67**

**Symbol index** **70**

**Keyword index** **71**

**References** **72**

# 1 Introduction

We present and construct revocable timed-release encryption schemes (based on quantum cryptography).[1] 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] published 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;[2] exchange of 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]; etc.

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

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 for the TRE to be returned. 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 a 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.

(Note: the use of the word "revocable" here has nothing to do with "revocability" of, say, signature keys. In the present setting, we mean that the recipient of the ciphertext can *voluntarily* give back the encryption. That is, he can "revoke"/"undo" the fact that he received the ciphertext.)

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

[1] Our constructions rely on the existence of non-revocable (i.e., normal) timed-release encryption. In the quantum setting, only one *practical* candidate for non-revocable timed-release encryption is currently known, "iterated hashing". See Section 1.2 below.

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

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 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.[3]

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. [SSS+13] reports on quantum memory with a coherence time of 39 minutes at room temperature and three hours at low temperatures. This does not immediately imply quantum TREs of the same magnitude (because the error rate needs to be taken into account), but it shows that current technology has the potential for achieving them.

**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 3). 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.[4]

**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 not more than one recipient can decrypt it (until a certain timeout $T'$). 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. 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

[3]One challenge: The client needs to convince the dealer that the TRE indeed contains a signature on a transaction. I.e., we need a way to prove that a TRE $V$ contains a given value (and the running time of this proof should not depend on $T$). At least for our constructions (see below), this could be achieved as follows: The client produces a commitment $c$ on the content of the classical inner TRE $V_0$ and proves that $c$ contains the right content (using a SNARK [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 $P$.

We leave a proof of the security of this construction for future work. Note also that this construction does not work if $V$ is a TRE in the random oracle model because a SNARK cannot prove any statements involving the random oracle. However, once we instantiate the random oracle with a hash function (or if we use the constructions without random oracles, based on the assumption that iterated hashing is hard), then SNARKs can be applied.

[4]Note: this only works if the goal of data retention is the prosecution, not the prevention of crime, since the data will be available only after a relatively long delay (after solving a TRE). To partially circumvent this limitation, each database entry can be stored multiple times using revocable TREs with different time-parameters $T_i$ (each being revoked before the time $T_i$ has passed). Then, when a database entry is accessed early on, it will still be contained in a TRE with small $T_i$. Later on, TREs with larger $T_i$ will need to be solved.

in Section 7.) 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.

Note that URE is not strictly speaking an application of revocable TREs because our construction of UREs does not work based on arbitrary TREs. However, UREs are an application of the specific construction given in this paper, and of the methods introduced here.

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.)

**Digital goods.** A vendor wants to sell certain digital goods (say, a movie) in such a way that they can be used after a certain point in time only (e.g., at the official release date of the movie). However, the vendor also wants to make it possible to return the goods for a refund, but obviously only before they have been consumed. A timed-release encryption achieves this task.

### 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 $B$.[5] Then $B$ is encrypted in a (non-revocable) $T$-hiding TRE $V_0$. The resulting TRE $(|\Psi\rangle, V_0)$ is sent to the recipient. Revocation is straightforward: the recipient sends $|\Psi\rangle$ back to the sender, who checks that $|\Psi\rangle$ still encodes $m$ in basis $B$. Intuitively, $|\Psi\rangle$ cannot be reliably copied without knowledge of basis $B$, hence before time $T$ the recipient cannot copy $|\Psi\rangle$ and thus looses access to $|\Psi\rangle$ and thus to $m$ upon revocation.

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

The resulting scheme even enjoys everlasting security (cf., e.g., [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 (Section 3) 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. Perhaps quantum-money? (See [AC12] and the references therein.)

**Revocably hiding TREs.** The next step is to construct revocably *hiding* TREs (Section 5). 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 5 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

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

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 one, 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 6.1). This gives a simpler and more efficient alternative to the complex construction for revocably hiding TREs described above, though at the cost of using the random-oracle model and loosing everlasting security. The second transformation allows us to assume without loss of generality that the adversary performs no oracle queries before receiving the TRE, simplifying other security proofs (Section 6.2).

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.[6] 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 6.3). (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.) Another construction is given by [BGJ+15], based on obfuscation. (The rough idea there is that a Turing machine is constructed that idles for $T$ steps and then output a message $m$. The TRE consists of the obfuscated Turing machine. Due to the obfuscation one cannot recover $m$ faster than running the $T$ idle steps.) Their construction is shown secure under the assumption that indistinguishability obfuscation, one-way functions, and "non-parallelizing languages" exist.[7] Their security proof does not directly apply in the quantum setting,[8] but it might be adaptable with some modifications to the definition of "non-parallelizing languages". However, their scheme has a large gap between the time-bound $T$ and the honest decryption time. (The paper has no precise analysis of the gap, but the gap would be at least the gap between the execution time of the Turing machine and the execution time of the obfuscated Turing machine.)

[6] Iterated hashing has the downside that producing the TRE takes as long as decrypting it. However, this long computation can be moved into a precomputation phase that is independent of the message $m$, making this TRE suitable at least for some applications. [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.

[7] They also have constructions that do not need indistinguishability obfuscation. However, there the size of the TRE seems to be proportional to $T$. If we assume that sending is not instantaneous, this means that sending the TRE may take longer than solving it. Hence, in a model where transmission is modeled as a sequential process, it is unclear whether such a TRE has an advantage over the trivial one where we send $0^T \| m$ – here you can only read $m$ after waiting $T$ steps till the 0's have been transmitted.

[8] For example, the proof that BPP/*poly* $\subseteq$ P/*poly* holds does not have a direct quantum equivalent.

We leave it as an open problem to identify more practical candidates for TREs, perhaps following the ideas of [RSW96] but not based on RSA or other quantum-easy problems. We also sketch (without security analysis) a variant of iterated hashing that greatly reduces the amortized computational costs of the sender.

**Unknown recipient encryption.** In Section 7, 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 TRE construction, that we prove to be secure (even with everlasting security).

### 1.3 Related work

The possibility of timed-release encryption was first conceived by [May93]. The first protocol was given by [RSW96], their protocol is insecure against quantum computers, though. [DN93, DNW05, MMV11] present alternatives based on hashing, but those are not suitable as timed-release encryption, only for proving that the recipient performed a certain amount of work (as the sender cannot predict the result of the computation of the recipient). [MMV11] also shows that in the classical random oracle model (when not using other assumptions), the sender's computation in a TRE has to be at least as computationally expensive as the recipient's (like for our iterated hashing); however, they do not exclude that encryption can be parallelized while decryption needs to be sequential. [BGJ$^+$15] presents a classical construction of TREs based on indistinguishability obfuscation; however the construction does not seem practical at this point (see Section 1.2).

The idea of using CSS codes to perform privacy amplification (we use it in the construction of revocably hiding TREs) was introduced by [SP00] in the context of quantum key distribution.

Uncloneable encryption [Got03] is a very similar primitive to revocable TRE. It is an encryption scheme where without the key, one cannot make a copy of the ciphertext. (See Section 5.1 for more discussion.) There could also be a connection between revocable TREs and quantum authentication codes [BCG$^+$02] (the codes we use look similar to those in [BGS13]), see Section 5.1 as well.

Our unknown recipient encryption seems, at the first glance, related to anonymous quantum communication [BBF$^+$07]. However, anonymous quantum communication serves the task of transmitting a quantum state from a sender to a recipient so that only the sender knows who the recipient is, and no-one knows who the sender is. This is a task that can be achieved for classical messages without using quantum communication [BT07], the achievement of [BBF$^+$07] was to make it possible to transfer a quantum message. In contrast, URE is a task that is impossible without quantum communication. Also, the sender is not kept secret (quite to the contrary: the sender authenticates his message). And the recipient is not necessarily secret either. In fact, URE provides no provisions to transfer the ciphertext to the recipient, secret or otherwise, this is outside the protocol. URE only guarantees that if the ciphertext arrives at a recipient, he can verify that no one else got the plaintext. (The "unknown" in "unknown recipient encryption" means that it is not necessary to know the recipient beforehand, not that the recipient will be kept secret.)

### 1.4 Organization

In Section 2 we give formal definitions of TRE and revocable TRE. In Section 3 we construct revocably one-way TREs from normal (non-revocable) TREs. In Section 4 we review the definition and some properties of CSS codes, needed for Section 5. In Section 5 we show how to construct revocably *hiding* TREs in the standard model, using CSS codes. In Section 6, we study constructions in the random oracle model. More precisely, in Section 6.1 we show how to transform revocably one-way TREs into revocably hiding TREs, in Section 6.2 we give a transformation that allows us to disregard precomputation by the adversary (this simplifies

other constructions), and in Section 6.3 we give a construction of a non-revocable TRE (which can then be combined with the results from earlier sections to get a revocably hiding TRE). In Section 7 we define and construct unknown recipient encryption. The appendices contain proofs that were deferred for better readability. Before the references, a symbol index and a keyword index can be found.

### 1.5 Preliminaries

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

Let $\operatorname{im} M$ denote the image of an operator/a function $M$. 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 $\mathrm{GF}(2)^n$). Given a linear code $C$, let $C^\perp$ be the dual code ($C^\perp := \{x : \forall y \in C.\ x, y \text{ orthogonal}\}$).

Let $X, Y, Z$ denote the Pauli operators. Let $|\beta_{ij}\rangle$ denote the four Bell states, namely $|\beta_{00}\rangle := \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$ and $|\beta_{fe}\rangle = (Z^f X^e \otimes I)|\beta_{00}\rangle = (I \otimes X^e Z^f)|\beta_{00}\rangle$. 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 $A^{x_1} \otimes \cdots \otimes A^{x_n}$. E.g., $X^x|y\rangle = |x \oplus y\rangle$, and $H^B|x\rangle = |x\rangle_B$.

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

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

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

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

## 2 Defining revocable TREs

**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. Throughout this paper, we will consider *quantum* adversaries. All definitions can be easily adapted to classical adversaries. However, since revocable TREs are easily seen to be impossible without quantum communication, considering classical adversaries does not seem useful.

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 $X_1$ and $X_2$ takes time at most $T_1 + T_2$. (This should be satisfied by most reasonable timing models such as circuit size, circuit depth, execution steps of a quantum 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 quantum circuit that is output by a probabilistic polynomial-time Turing machine (the Turing machine may run in polynomial-time in the size of both the classical and the quantum input). To understand why we need the notion of sequential polynomial time, consider the following example TRE: $\mathrm{TRE}(m) := (k, enc(H^T(k), m))$ 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 $enc(H^T(k), m)$ using $2^\eta$ *parallel* decryptions. Thus this TRE is not hiding if we consider $T$-time adversaries. Of course, such an attack is not practical since it needs an exponential number of parallel processes. Hence we additionally require that the total number of steps performed by the adversary is polynomial. That is, this TRE seems to be hiding with respect to an adversary that is simultaneously $T$-time and sequential-polynomial-time (we did not prove this, since this is just an illustrative example). 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 that 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.[9] 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 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 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 $m_0, m_1$, $\mathrm{TRE}(m_0)$ and $\mathrm{TRE}(m_1)$ are indistinguishable for a $T$-time, sequential-polynomial-time adversary $A_1$. (See the discussion above why we additionally need 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.

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

**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-time*[10] *and $T$-time we have that*

$$\big|\Pr[b'=1 : (m_0,m_1) \leftarrow A_0(), V \leftarrow \mathrm{TRE}(m_0), b' \leftarrow A_1(V)] - \Pr[b'=1 : (m_0,m_1) \leftarrow A_0(), V \leftarrow \mathrm{TRE}(m_1), b' \leftarrow A_1(V)]\big|$$

*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.*[11]*)*

We remind the reader that all algorithms are assumed to be quantum throughout the paper (see the discussion on timing models, page 7). Thus Definition 2 formalizes security against efficient quantum adversaries. Similarly for all following definitions.

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*

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

*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 $V \leftarrow \mathrm{TRE}(m)$. 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 $m$ contained in the TRE. When formalizing this, we have to be careful. A definition like: *"conditioned on revocation succeeding, $p_0 := \Pr[$adversary outputs 1 given $\mathrm{TRE}(m_0)]$ and $p_1 := \Pr[$adversary outputs 1 given $\mathrm{TRE}(m_1)]$ are close ($|p_0 - p_1|$ is negligible)"* does not work: if Pr[revocation succeeds] is very small, $|p_0 - p_1|$ can become large even if the adversary rarely succeeds in distinguishing. (Consider, e.g., an adversary that intentionally fails revocation except in the very rare case that he guesses an encryption key that allows to decrypt the TRE immediately.) Also, a definition like *"$|p_0 - p_1| \cdot \Pr[$revocation succeeds$]$ is negligible"* is problematic: Does Pr[revocation succeeds] refer to an execution with $\mathrm{TRE}(m_0)$ or $\mathrm{TRE}(m_1)$? Instead, we will require *"$|p_0 - p_1|$ is negligible with*

[10] We 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 $T$.

[11] If $M$ 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.

$p_i := \Pr[$*adversary outputs* 1 *and revocation succeeds given* $\mathrm{TRE}(m_i)]$". This definition avoids the complications of a conditional probability and additionally implies as side effect that also $\Pr[$revocation succeeds given $\mathrm{TRE}(m_0)]$ and $\Pr[$revocation succeeds given $\mathrm{TRE}(m_1)]$ are close.

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 $b \in \{0, 1\}$:*

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

*A timed-release encryption* TRE *with message space $M$ is $T$-*revocably hiding*, if for any adversary $(A_0, A_1, A_2)$ where $A_1$ is sequential-polynomial-time and $T$-time and $A_0, A_2$ are sequential-polynomial-time, we have that the advantage*

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

*is negligible.*

Note that although revocably hiding seems to be a stronger property than hiding, we we do not know whether 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 also 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 we do not know whether revocable one-wayness implies 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* $V \leftarrow \mathrm{TRE}(m)$.
- *Run the revocation protocol of* TRE*, where the sender is honest, and the recipient is $A_1(V)$. Let $ok$ be the output of the sender (i.e., $ok = 1$ if the sender accepts).*
- $m' \leftarrow A_2()$.

*A timed-release encryption* TRE *with message space $M$ is $T$-*revocably one-way*, if for any quantum adversary $(A_0, A_1, A_2)$ where $A_1$ is sequential-polynomial-time and $T$-time and $A_0, A_2$ are sequential-polynomial-time, we have that*

$$\Pr[m = m' \wedge ok = 1 : G]$$

*is negligible.*

## 3 Constructing revocably one-way TREs

In this section, we present our construction $\mathrm{RTRE}_{ow}$ 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 5), and also as a building block in our random-oracle based construction (Section 6.1).

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 it because it makes the protocol (non-revocably) hiding at little extra cost (Theorem 2).

**Definition 7 (Revocably one-way TRE $\mathrm{RTRE}_{ow}$)**

- *Let $n$ be an integer.*
- *Let $\mathrm{TRE}_0$ be a $T$-hiding TRE with message space $\{0,1\}^{2n}$.*

*We construct a revocable TRE $\mathrm{RTRE}_{ow}$ 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 7.)*
- *Compute $V_0 \leftarrow \mathrm{TRE}_0(B, p)$.*
- *Send $V_0$ and $|\Psi\rangle$.*

***Decryption:***

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

***Revocation:***

- *The recipient sends $|\Psi\rangle$ back to the sender.*
- *The sender measures $|\Psi\rangle$ in basis $B$; call the outcome $\gamma$.*
- *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.[12] We also know that until time $T$, the adversary does not know anything about $B$ (since $\mathrm{TRE}_0$ 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 $\mathrm{TRE}_0$ were implemented using a trusted third party (i.e., if $B$ is sent to the adversary after time $T$).[13] However, the adversary has access to $V_0 = \mathrm{TRE}_0(B)$ when trying to clone $|\Psi\rangle$. From the information-theoretical point of view, this is the same as having access to $B$. Thus the no-cloning theorem and its variants cannot be applied because they rely on the fact that $B$ is *information-theoretically* hidden.

One might want to save the argument in the following way: Although $V_0 = \mathrm{TRE}_0(B)$ information-theoretically contains $B$, it is indistinguishable from $\hat{V}_0 = \mathrm{TRE}_0(\hat{B})$ which does not contain $B$ but an independently chosen $\hat{B}$. And if the adversary is given $\hat{V}_0$ instead of $V_0$, we can use information-theoretical arguments to show that he cannot learn $m$. But although this argument would work if $\mathrm{TRE}_0$ were hiding against polynomial-time adversaries (e.g., if $\mathrm{TRE}_0$ were a commitment scheme). But $\mathrm{TRE}_0$ 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

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

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

revocation, the adversary provably cannot ever learn $m$, it might be possible that with $V_0$, he can learn $m$ right after time $T$ has passed.

Indeed, it is not obvious how to exclude that there is some "encrypted-cloning" procedure that, given $|\Psi\rangle = |m\rangle_B$ and $\mathrm{TRE}_0(B)$, without disturbing $|\Psi\rangle$, produces a state $|\Psi'\rangle$ that for a $T$-time distinguisher looks like a random state, but still $|\Psi'\rangle$ can be transformed into $|\Psi\rangle$ in time $\gg T$. Such an "encrypted-cloning" would be sufficient for breaking $\mathrm{RTRE}_{ow}$. (Of course, it is a direct corollary from our security proof that such encrypted-cloning is impossible.)[14]

**Proof idea.** As we have seen in the preceding discussion, we can prove that the property "the adversary cannot learn $m$ ever" holds when sending $\hat{V}_0 = \mathrm{TRE}_0(\hat{B})$ for an independent $\hat{B}$ instead of $V_0 = \mathrm{TRE}_0(B)$. But we cannot prove that this property carries over to the $V_0$-setting because it cannot be tested in time $T$. Examples for properties that do carry over would be "the adversary cannot learn $m$ in time $T$" or "revocation succeeds" or "when measured in basis $B$, the adversary's revocation-message does not yield outcome $m$". But we would like to have a property like "the min-entropy of $m$ is large (or revocation fails)".[15] 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 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 can be 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, see Lemma 15) we have that this property implies "the min-entropy of $m$ is large (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 ($\mathrm{RTRE}_{ow}$ is revocably one-way)** *Let $\delta_T^{ow}$ 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 13 below), a measurement whether two $n$-qubit registers are in an EPR state up to $t := \sqrt{n}$ phase flips and $t$ bit flips (defined as $P_t^{EPR}$ on page 13 below), and one NOT- and one AND-gate.*

*Assume that the protocol parameter $n$ is superlogarithmic.*

*The protocol $\mathrm{RTRE}_{ow}$ 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 46.*

[14] To illustrate that "encrypted-cloning" is not a far fetched idea, consider the following quite similar revocable TRE: Let $E_K(|\Psi\rangle)$ denote the quantum one-time pad encryption of $|\Psi\rangle \in \mathbb{C}^{2^n}$ using key $K \in \{0,1\}^{2n}$, i.e., $E_K(|\Psi\rangle) = Z^{K_1} X^{K_2} |\Psi\rangle$ with $K = K_1 \| K_2$ [AMTW00]. $\mathrm{RTRE}(m) := (E_K(|m\rangle_B), B, \mathrm{TRE}_0(K))$. For revocation, the sender sends $E_K(|m\rangle_B)$ back, and the recipient checks if it is the right state. Again, if $K$ is unknown, it is not possible to clone $E_K(|m\rangle_B)$ as it is effectively a random state even given $B$. But we can break RTRE as follows:

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

[15] For the reader unfamiliar with min-entropy [Ren05]: A random variable has min-entropy $\geqslant k$ iff it cannot be guessed with probability better than $2^{-k}$. Thus "high min-entropy" basically means "hard to guess".

**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 $\mathrm{RTRE}_{ow}$ inlined), it thus suffices to show that $\Pr[m = m' \wedge ok = 1 : \mathit{Game}\ 1]$ is negligible. We highlight changes between games in blue.

**Game 1 (Original game)**

- *Run* $A_0()$. $m \xleftarrow{\$} \{0,1\}^n$, $p \xleftarrow{\$} \{0,1\}^n$, $B \xleftarrow{\$} \{0,1\}^n$. $V_0 \leftarrow \mathrm{TRE}_0(B,p)$. $X \leftarrow |m \oplus p\rangle_B$.
- *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* $\gamma$. *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* $A_0()$. $m \xleftarrow{\$} \{0,1\}^n$, $p \xleftarrow{\$} \{0,1\}^n$, $B \xleftarrow{\$} \{0,1\}^n$. $V_0 \leftarrow \mathrm{TRE}_0(B,p)$. $X \leftarrow |m\rangle_B$.
- *Run* $A_1(X, V_0)$. *Measure* $X$ *in basis* $B$*; outcome* $\gamma$. *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* $A_0()$. ~~$m \xleftarrow{\$} \{0,1\}^n$~~, $p \xleftarrow{\$} \{0,1\}^n$, $B \xleftarrow{\$} \{0,1\}^n$. $V_0 \leftarrow \mathrm{TRE}_0(B,p)$. *Initialize* $XY$ *as* $|\widetilde{0^n 0^n}\rangle$.
- *Run* $A_1(X, V_0)$. *Measure* $X$ *in basis* $B$*; outcome* $\gamma$.
- *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 $P_B^= := \sum_{x \in \{0,1\}^n} |x,x\rangle_B\langle x,x|_B$. We show that again $\Pr[m = m' \wedge ok = 1]$ does not change.

**Game 4 (Changed revocation test)**

- *Run* $A_0()$. $p \xleftarrow{\$} \{0,1\}^n$, $B \xleftarrow{\$} \{0,1\}^n$. $V_0 \leftarrow \mathrm{TRE}_0(B,p)$. *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* $\gamma$.~~
- *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 $\mathrm{TRE}_0(B,p)$ and one where we use $\mathrm{TRE}_0(\hat{B},p)$. 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 $P_t^{EPR} := \sum_{f,e} |\widetilde{fe}\rangle\langle\widetilde{fe}|$ where the sum ranges over all $f, e \in \{0,1\}^n$ with $\omega(f), \omega(e) \leqslant t$. (Remember that $|\widetilde{fe}\rangle$ stands for an EPR state with phase flips $f$ and bit flips $e$, see page 7.) Here $t$ is an arbitrary integer, to get a negligible bound on the adversary's advantage we choose

$t := \sqrt{n}$.[16] That is, $P_t^{EPR}$ tests whether two $n$-qubit registers form an EPR state (with at most $t$ 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* $A_0()$. $p \xleftarrow{\$} \{0,1\}^n$, $B \xleftarrow{\$} \{0,1\}^n$. $V_0 \leftarrow \mathrm{TRE}_0(B,p)$. *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

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

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 $\mathrm{TRE}(B,p)$ by $\mathrm{TRE}(\hat{B},p)$ 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* $A_0()$. $p \xleftarrow{\$} \{0,1\}^n$, ~~$B \xleftarrow{\$} \{0,1\}^n$.~~ $\hat{B} \leftarrow \{0,1\}^n$. $V_0 \leftarrow \mathrm{TRE}_0(\hat{B},p)$. *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 $\Pr[isEPR = 0 \wedge ok = 1] \leqslant 2^{-t-1}$ which is negligible. This proves the revocable onewayness of $\mathrm{RTRE}_{ow}$. □

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 ($\mathrm{RTRE}_{ow}$ is hiding)** *The protocol* $\mathrm{RTRE}_{ow}$ *from Definition 7 is* $T$*-hiding. (A concrete security bound is given in Appendix B, page 47.)*

The full proof is given in Appendix B, page 47.

# 4 CSS codes – recap and properties

In this section, 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].

This section is only needed for understanding Section 5 (revocably hiding TREs). A reader who is only interested in the random oracle based constructions may skip this section.

[16] This is not necessarily optimal. To get optimal security bounds, one needs to choose $t$ to minimize the concrete security bound given at the end of the proof in Appendix B, page 46.

The proofs of the lemmas in this section are given in Appendix C.

A *CSS code* with parameters $n, k_1, k_2, t$ consists of two classical linear binary codes, namely an $[n, k_1]$ code $C_1$[17] 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 1 (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 $\sum_{y \in \{0,1\}^n/C^\perp} (-1)^{x \cdot y} = 0$.*

**Lemma 2 (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 $\mathbb{C}^{2^n}$.*

**Lemma 3 (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 7.)*

**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 isometry[18] describing error correction and decoding for the CSS 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 $\omega(f), \omega(e) \leqslant t$ 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 $X^{e_1} \otimes \cdots \otimes X^{e_n}$ 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 CSS 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 $\operatorname{span}\{|\xi_{xuv}\rangle : x \in C_1/C_2\}$, there is a $|\Psi\rangle$ such that $U_{uv}^{dec} |\xi\rangle = |\perp\rangle \otimes |\Psi\rangle$.

**Lemma 4 (Decoding and error correcting)** *Polynomial-time operations $U_{uv}^{dec}$ and $U_{uv}^{EC}$ with the properties above exist.*

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

[18] I.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 $\dim_{out} := |C_1/C_2 \cup \{\perp\}| \cdot \dim_\Psi$ where $\dim_\Psi$ 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.

# 5 Revocably hiding TREs

We now turn to the problem of constructing revocably hiding TREs. The construction from the previous section is revocably one-way, but it is certainly not revocably hiding because the adversary might be lucky enough to guess a few bits of the basis $B$, measure the corresponding bits of the message $m$ without modifying the state, and successfully pass revocation. So some bits of $m$ will necessarily leak. The most natural approach for dealing with partial leakage (at least in the case of QKD) is to use privacy amplification. That is, we pick a function $F$ from a suitable family of functions (say, universal hash functions with suitable parameters), and then to send $m$, we encrypt a random $x$ using the revocably one-way TRE, and additionally transmit $F(x) \oplus m$. If $x$ has sufficiently high min-entropy, $F(x)$ will look random, and thus $F(x) \oplus m$ will not leak anything about $m$. Additionally, we need to transmit $F$ to the recipient, in a way that the adversary does not have access to it when measuring the quantum state. Thus, we have to include $F$ in the classical TRE. So, altogether, we would send $(m \oplus F(x), \mathrm{TRE}_0(B, F))$ and $|m\rangle_B$. In fact, this scheme might be secure, we do not have an attack. Yet, when it comes to proving its security, we face difficulties: In the proof of $\mathrm{RTRE}_{ow}$, to use the hiding property of $\mathrm{TRE}_0$, we identified a property that can be checked in time $T$, and that guarantees that $m$ cannot be guessed. (Namely, we used that the registers $XY$ contain EPR pairs up to some errors which implies that the adversary cannot predict the outcome $m$ of measuring $Y$.) In the present case, we would need more. We need a property $P$ that guarantees that $F(x)$ is indistinguishable from random given the adversary's state when $x$ is the outcome of measuring $Y$. Note that here it is not sufficient to just use that $x$ has high min-entropy and that $F$ is a strong randomness extractor; at the point when we test the property $P$, $F$ is already fixed and thus not random. Instead, we have to find a measurable property $P'$ that guarantees: For the particular value $F$ chosen in the game, $F(x)$ is indistinguishable from randomness. (And additionally, we need that $P'$ holds with overwhelming probability when $\mathrm{TRE}_0(B, f)$ is replaced by a fake TRE not containing $B, f$.) We were not able to identify such a property.[19]

**Using CSS codes.** The above 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 $|\widetilde{fe}\rangle$ with $\omega(f), \omega(e) \leqslant t$. Then they use the fact that, roughly speaking, $|\widetilde{0^n 0^n}\rangle$ is an encoding of $|\widetilde{0^\ell 0^\ell}\rangle$ for some $\ell < n$ using a random CSS code correcting $t$ bit/phase error. (See Section 4 for a short recap of CSS codes.) So if Alice and Bob apply error correction and decoding to $|\widetilde{fe}\rangle$, they get the state $|\widetilde{0^\ell 0^\ell}\rangle$. Then, if Alice and Bob measure that state, they get identical and uniformly distributed keys, and the adversary has no information. Furthermore, the resulting protocol can be seen to be equivalent to one that does not need quantum codes (and thus quantum computers) but only

[19] To illustrate the difficulty of identifying such a property: Call a function $F$ $s$-good if $F(x)$ is uniformly random if all bits $x_i$ with $s_i = 0$ are uniformly random (and independent). In other words, $F$ tolerates leakage of the bits with $s_i = 1$. For suitable families of functions $F$, and for $s$ with low Hamming weight, a random $F$ will be $s$-good with high probability. Furthermore, when using a fake $\mathrm{TRE}_0$, $XY$ is in state $|\widetilde{fe}\rangle$ with $s := (f \vee e)$ of low Hamming weight with overwhelming probability after successful revocation (this we showed in the security proof for $\mathrm{RTRE}_{ow}$). In this case, all bits of $Y$ with $s_i = 0$ will be "untampered" and we expect that $F(x)$ is uniformly random for $s$-good $F$ (when $x$ is the outcome of measuring $Y$). So we are tempted to choose $P'$ as: "$XY$ is in a superposition of states $|\widetilde{fe}\rangle$ such that the chosen $F$ is $(f \vee e)$-good". This property holds with overwhelming property using a fake $\mathrm{TRE}_0$. 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.

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

Note that this simplified protocol is a "randomized" TRE which does not allow us to encrypt an arbitrary message, but instead chooses the message $x$. The obvious approach to transform it to a normal TRE for encrypting a given message $m$ is to send $m \oplus x$ in addition to the TRE. This is indeed what we do, but there are some additional 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 $\mathrm{RTRE}'_{hid}$)**
*(a) The game is parametric in $b \in \{0,1\}$.*
*(b) $(m_0, m_1) \leftarrow A_0()$. Pick $B$, $Q$. Initialize $XY$ as $|0^{\widetilde{q+n}}0^{q+n}\rangle$.*
*(c) Measure from $Y$ the parameters $u, v$ of the CSS code $C_{u,v}$.*
*(d) $V_0 \xleftarrow{\$} \mathrm{TRE}_0(Q)$. 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 $\mu := \big|\Pr[b' = 1 \wedge ok = 1 : \mathit{Game}\ 4(0)] - \Pr[b' = 1 \wedge ok = 1 : \mathit{Game}\ 4(1)]\big|$ is negligible. Here $\mathit{Game}\ 4(0)$ denotes Game 4 with parameter $b := 0$ and analogously for $b := 1$.

As in the security proof for $\mathrm{RTRE}_{ow}$, 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 $\mu$ 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 $|\widetilde{0^\ell 0^\ell}\rangle$."

**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* $|\widetilde{0^{q+n}0^{q+n}}\rangle$.
*(c) Measure from $Y$ the parameters $u, v$ of the CSS code $C_{u,v}$.*
*(d)* $V_0 \xleftarrow{\$} \mathrm{TRE}_0(Q)$. *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 $|\widetilde{0^\ell 0^\ell}\rangle$. 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).

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

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 $|\widetilde{0^\ell 0^\ell}\rangle$. 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 $|\widetilde{0^\ell 0^\ell}\rangle$ 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 $\mathrm{TRE}_0$ 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 $\mathrm{TRE}_0(Q)$ 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 $V_0 \leftarrow \mathrm{TRE}_0(\hat{Q})$ with independent $\hat{Q}$.*

Finally, we show that $\Pr[ok = 1 \wedge isEPR = 0 : \mathit{Game}\ 7]$ 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 $\omega(f), \omega(e) \leqslant t$. Since $|\widetilde{fe}\rangle = (Z^f X^e \otimes I)|\widetilde{0^{n+q}0^{n+q}}\rangle$, and $|\widetilde{0^{n+q}0^{n+q}}\rangle$ is an encoding of $|\widetilde{0^\ell 0^\ell}\rangle$, error correction on $X$ removes the effect of $Z^f X^e$, and then decoding leads to the state $|\widetilde{0^\ell 0^\ell}\rangle$. That is, $isEPR = 1$ holds with overwhelming probability when revocation succeeds ($ok = 1$). Thus $\Pr[ok = 1 \wedge isEPR = 0 : \mathit{Game}\ 7]$ is negligible.

Combining all results, we have that $\mu$ is negligible. This shows the security of $\mathrm{RTRE}'_{hid}$. □

**Entanglement-free protocol.** The protocol $\mathrm{RTRE}'_{hid}$ 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 $\mathrm{RTRE}_{ow}$). 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 of games (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 $A_1$ as a natural definition of randomized TREs would do. (We call this *late key revelation*) The effect of this is that $\mathrm{RTRE}'_{hid}$ 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 $\mathrm{TRE}_0$ with security exponential in $\ell$. (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 $\mathrm{RTRE}_{ow}$, 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 Section 4.)*
- *Let $q$ be an integer.*
- *Let $\mathrm{TRE}_0$ 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 7. $C_1/C_2$ denotes the quotient of codes.)*

*We construct a revocable TRE $\mathrm{RTRE}_{hid}$ 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 $\{1,\dots,q+n\}\backslash Q =: \{b_1,\dots,b_n\}$; the relative order of the $a_i$ and of the $b_i$ does not matter.)*[20]*
- *Compute $V_0 \leftarrow \mathrm{TRE}_0(B, Q, r, p)$.*
- *The TRE consists of $(V_0, u, m \oplus x \oplus p)$ and $|\Psi\rangle$.*

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

***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 $\gamma$.*[21]
- *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 $r'$.*[22]
- *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 Section 7, the inclusion of $B, r$ will turn out to be useful.

**Theorem 3 (**$\mathrm{RTRE}_{hid}$ **is revocably hiding)** *Let $\delta_T^{hid}$ be the time to compute the following things: $q$ controlled Hadamard gates, applying an already computed permutation to $n+q$ qubits, a $q$-qubit measurement in the computational basis (called $M_R$ in the proof), a comparison of two $q$-qubit strings, the error-correction/decoding operations $U_{uv}^{EC}$, $U_{uv}^{dec}$ that exist by Lemma 4, 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* $\mathrm{TRE}_0$ *is $T$-hiding with $(2^{-2(k_1-k_2)} \cdot negligible)$-security.*[23] *Assume that $tq/(q+n) - 4(k_1-k_2)\ln 2$ is superlogarithmic.*

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

*A concrete security bound is given at the end of the proof, page 62, equation* (25).

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 $\mathrm{TRE}_0$ is only $T$-hiding with negligible-security, then we have to choose $\ell$ to be logarithmic.

If $\mathrm{TRE}_0$ is $T$-hiding with exponential security, by rescaling the security parameter we can get $(2^{-2\ell} \cdot negligible)$-security for any message length $\ell$. Note that for given $\ell$, the codes $C_1, C_2$ can always be chosen to match the other constraints: First, fix some $t \geqslant 8\ell \ln 2 + \gamma$ where $\gamma$ 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 $k_1' - k_2 \geqslant \ell$ (i.e., it must correct at least $t$ errors and encode words of length $\ell$; 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 $k_1' \geqslant \ell + k_2$. 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

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

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

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

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 (25) 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.

### 5.1 Relation to quantum authentication codes and uncloneable encryption

There are some parallels between our construction of revocably hiding TREs and quantum authentication codes [BCG+02]. In quantum authentication codes, a message is authenticated and encrypted by a quantum error detecting code (randomly chosen from a given family of codes). Since the adversary does not know the code, he cannot modify the message without high probability of creating an invalid code word. Curiously, in the quantum setting, authentication also implies secrecy: any quantum authentication scheme is also an encryption scheme. This strong connection between authentication and encryption might be at the core of our revocably hiding TRE, too: during revocation, we check the authenticity of the TRE, and this implies that the adversary will not be able to learn anything about the content of the TRE. We do not know whether this connection is merely superficial, or whether there is a deeper relation between quantum authentication codes and revocably hiding TRE. Or, more concretely: is the following construction already a revocably hiding TRE?

**Construction 1** *To encrypt $m$, encode $m$ with a quantum authentication code with random key $k$. Let $|\Psi\rangle$ be the resulting state. Encrypt $k$ using a classical hiding TRE. Send the TRE and $|\Psi\rangle$ to the recipient.*

We leave it as a question for future work whether this gives rise to a revocably hiding TRE.

Note also that the code we used in our construction (i.e., a CSS code with interspersed check bits at locations $Q$) resembles the "trap codes" from [BGS13]. In the trap code, a code word is authenticated by interspersing it with check qubits and then encrypting it with a quantum one-time pad. Again, we do not know whether there are deeper reasons for this connection. (They motivate their choice with the fact that it is possible to perform computations on the data in trap codes without decoding, a fact that has no relevance for our setting.)

Another strongly related primitive (both to revocable TRE and quantum authentication codes) is uncloneable encryption [Got03]. Uncloneable encryption is an encryption scheme with the property that it is not possible to copy (clone) a ciphertext without knowledge of the key (even if the key is only computationally hidden). More precisely, after the adversary correctly returned a ciphertext, the state of the adversary will be independent from the message (up to small trace distance). This is very similar to a revocably hiding TRE (except for the temporal aspect). [Got03] shows that any quantum authentication scheme gives rise to an uncloneable encryption scheme. We leave it to future research to explore the formal connection between revocably hiding TRE and uncloneable encryption, in particular whether Construction 1 is a revocably hiding TRE when instantiated with an uncloneable encryption scheme.

At the first glance, the proof technique employed in the constructions from [Got03] seems quite different from ours. They show that the adversary cannot clone a ciphertext by reducing the uncloneability to the authentication property of an underlying quantum authentication scheme. However, there is one strong parallel between our proof and theirs: In our proof, we identify a certain efficiently testable property (namely, whether the returned TRE together with the state of the sender forms an EPR pair with few errors), and show that this property implies a non-testable, but desired property (namely, that the recipient's state is nearly independent of the message). And the efficiently testable property is then preserved from game to game. A similar approach is found implicitly in the proofs of [Got03] (for the computational case): the efficiently

testable property is whether a given state would pass the verification of the authentication scheme. The non-testable property is, like in our case, the independence of the adversary's state from the encrypted message. And the proof makes use of the fact that if the testable property is satisfied for uniformly random keys, then it is satisfied for pseudorandom keys.

# 6 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.[24] More formally, if the oracle is $H$, the adversary can query $H(x_1), \ldots, H(x_q)$ for arbitrarily large $q$ and arbitrary $x_1, \ldots, x_q$ 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.

## 6.1 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 which 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 (revocable) TRE, and use $H(k)$ as a one-time-pad to encrypt the message:

**Theorem 5 (Hiding timed-release encryptions)** *Let $H : \{0,1\}^n \to \{0,1\}^m$ 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 $k \xleftarrow{\$} \{0,1\}^n$, $V' \leftarrow$* 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*.*

*Then we have*

*(i) If* TRE *is $T$-oneway and $T$-revocably one-way then* TRE′ *is $T$-revocably hiding.*

*(ii) If* TRE *is $T$-oneway then* TRE′ *is $T$-hiding.*

*(iii) If* TRE *is $T$-oneway without offline-queries and $T$-revocably one-way without offline-queries then* TRE′ *is $T$-revocably hiding without offline-queries.*

*(iv) If* TRE *is $T$-oneway 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.*[25]

[24] In [MMV11], this is called "$T$ levels of adaptivity".

[25] For other timing models, the reduction described in the proof may incur an overhead, leading to a smaller $T$ for TRE′.

Notice that we assume that TRE does not access $H$. Otherwise simple counterexamples can be constructed. (E.g., 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 5 (One-way to hiding)** *Let $H : \{0,1\}^n \to \{0,1\}^m$ 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 $i \xleftarrow{\$} \{1,\dots,q\}$ 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 measurement outcome. (When $A$ makes less than $i$ queries, $B$ outputs $\perp \notin \{0,1\}^n$.)*

*Let*

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

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

Before we prove this lemma, we explain why such a lemma is useful for proofs in the quantum random oracle model. Consider a situation where a protocol uses a value $H(x)$, and we want to show that $H(x)$ is indistinguishable from a uniformly random $y$. In the classical setting, we can do the following: The probability that an adversary distinguishes $H(x)$ and $y$ is upper bounded by the probability $P'_B$ that the adversary performs an $H$-query with input $x$. Formally, $|P_A^1 - P_A^2| \leqslant P'_B$ when $P_A^1$ and $P_A^2$ are the probability that the adversary outputs 1 given $H(x)$ and $y$, respectively. So, in order to show the indistinguishability of $H(x)$ and $y$, we just need to show that $P'_B$ is negligible. That is, we have reduced an indistinguishability to the hardness of guessing $x$. Note that this even holds when the adversary gets $x$ as an input. We may still get non-trivial bounds on the probability $P'_B$ if we can show that $A$ does not query $x$ from $H$. This is useful, for example, when we try to show that $H(x)$ and $y$ are indistinguishable to an adversary $C$ that gets $f(x)$ where $f$ is a one-way function: We construct an adversary $A(x,y)$ that calls $C(f(x),y)$, and prove that $A(x,y)$ queries $x$ with negligible probability, which follows immediately from the one-wayness of $f$ and the construction of $A$.

If we try to apply the same technique in the quantum setting, we run into a problem. We would like to say that the probability of distinguishing $H(x)$ and $y$ is bounded by the probability that $A$ queries $x$ from $H$. However, since $H$ can be queried in superposition, it is not even clear what that means. E.g., if $A$ queries $\sum_{x\in X}|x\rangle$ with $X$ being the domain of $H$, should we say that $A$ queried $x$ or not? Also, we cannot, after the execution, talk about the inputs of past queries (such as "all the queries made contain $x$ only with small amplitude"), because to speak about them afterwards would mean to measure or copy them during the execution. And that would disturb the execution of the adversary. The situation is further complicated by the possibility that the queries are entangled with the adversary's state. To circumvent these difficulties, we do not execute the adversary $A$ directly, but instead define a new adversary $B$ who runs $A$, but at some random query stops and measures the input to the query. The probability $P_B$ that this adversary $B$ measures $x$ is the quantum analogue to the probability $P'_B$ that a classical $A$ queries $x$ in some query. (For classical $A$, we have $P_B = P'_B/q$ where $q$ is the number of queries.) If we can upper-bound $|P_A^1 - P_A^2|$ in terms of $P_B$, we can relate the probability of distinguishing

$H(x)$ and $y$ to that of guessing $x$ in a slightly modified game. For example, if we wish to show that an adversary $C$ does not distinguish $H(x)$ and $y$ given $f(x)$, we do the following: $A(x,y)$ calls $C(f(x),y)$. To show indistinguishability, we then need to show that $P_B$ is negligible. $P_B$ is the probability that we measure $x$ if we run $C(f(x),y)$, stop at a randomly chosen $H$-query, and measure the query argument. From the one-wayness of $f$, we get that $P_B$ is negligible. Hence $H(x)$ and $y$ are indistinguishable given $f(x)$.

Summarizing, to show the indistinguishability of $H(x)$ and $y$ in various setting involving a quantum random oracle $H$, we need to upper-bound $|P_A^1 - P_A^2|$ in terms of $P_B$. And this is exactly what Lemma 5 does.

The name of the lemma derives from the fact that it is useful for reducing a hiding (i.e., indistinguishability) property to a guessing (i.e., one-wayness) property.

The usefulness of this lemma is not limited to the present setting, it has since been generalized and used to analyze quantum position verification protocols [Unr14] and non-interactive quantum zero-knowledge arguments of knowledge [Unr15].

*Proof of Lemma 5.* 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 $|\Psi^i_{Hxy}\rangle := (UO_H)^i|\Psi_{xy}\rangle$. Then

$$P_A^2 = \sum_{Hxy} \alpha \underbrace{\Pr[M \text{ outputs 1 on state } |\Psi^q_{Hxy}\rangle]}_{=:b_{Hxy}}. \tag{2}$$

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

Furthermore, we see that

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

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

$$P_A^1 = \sum_{Hxy} \alpha b_{H_{xy}xy}. \tag{3}$$

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

$$P_B = \sum_{Hxyi} \tfrac{\alpha}{q} \|Q_x|\Psi^{i-1}_{Hxy}\rangle\|^2 \tag{4}$$

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

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

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

Hence

$$|b_{Hxy} - b_{H_{xy}xy}| \leqslant D_q \leqslant \sum_{i=1}^{q} \mathrm{TD}(O_H|\Psi^{i-1}_{Hxy}\rangle, O_{H_{xy}}|\Psi^{i-1}_{Hxy}\rangle). \tag{5}$$

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

$$\begin{aligned}
&\mathrm{TD}(O_H|\Psi^{i-1}_{Hxy}\rangle, O_{H_{xy}}|\Psi^{i-1}_{Hxy}\rangle)\\
&= \mathrm{TD}(O_H(1-Q_x)|\Psi^{i-1}_{Hxy}\rangle + O_HQ_x|\Psi^{i-1}_{Hxy}\rangle,\\
&\qquad O_H(1-Q_x)|\Psi^{i-1}_{Hxy}\rangle + V_yQ_x|\Psi^{i-1}_{Hxy}\rangle)\\
&\overset{(*)}{\leqslant} 2\|O_HQ_x|\Psi^{i-1}_{Hxy}\rangle\| = 2\|Q_x|\Psi^{i-1}_{Hxy}\rangle\|. \qquad (6)
\end{aligned}$$

Here $(*)$ uses Lemma 11 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

$$\begin{aligned}
|P^1_A - P^2_A| &\overset{(2,3)}{\leqslant} \sum_{Hxy} \alpha\,|b_{Hxy} - b_{Hxyxy}| \overset{(5)}{\leqslant} \sum_{Hxyi} \alpha\,\mathrm{TD}(O_H|\Psi^{i-1}_{Hxy}\rangle, O_{H_{xy}}|\Psi^{i-1}_{Hxy}\rangle)\\
&\overset{(6)}{\leqslant} \sum_{Hxyi} \alpha\,2\|Q_x|\Psi^{i-1}_{Hxy}\rangle\| \overset{(*)}{\leqslant} 2q\sqrt{\sum_{Hxyi} \tfrac{\alpha}{q}\,\|Q_x|\Psi^{i-1}_{Hxy}\rangle\|^2} \overset{(4)}{=} 2q\cdot\sqrt{P_B}.
\end{aligned}$$

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

To show Theorem 5 using this Lemma 5, we assume an adversary $(A_0, A_1, A_2)$ against the revocable 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)* $H \xleftarrow{\$} (\{0,1\}^n \to \{0,1\}^m)$. $k \xleftarrow{\$} \{0,1\}^n$.

*(b)* $(m_0, m_1) \leftarrow A^H_0()$. $V' \leftarrow \mathrm{TRE}(k)$. $m := m_b \oplus H(k)$. *Run the revocation protocol of* TRE, *with* $A^H_1(V', m)$ *as recipient. Let ok be the honest sender's output. If* $ok = 1$, $b' \leftarrow A^H_2()$, *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 $P^1_A$ from Lemma 5 is the probability of $b' = 1 \wedge ok = 1$ in Game 1. And $P^2_A$ is independent of $b$ since $m_b \oplus h$ hides $b$ for random $h$. Thus, to show that $P^1_A$ is almost independent of $b$ (and thus TRE′ revocably hiding), it is sufficient to show that $|P^1_A - P^2_A|$ is negligible. By Lemma 5, 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)* $H \xleftarrow{\$} (\{0,1\}^n \to \{0,1\}^m)$. $k \xleftarrow{\$} \{0,1\}^n$. $(m_0, m_1) \leftarrow A^H_0()$. $V' \leftarrow \mathrm{TRE}(k)$.

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

*(c) Run the revocation protocol with* $A^H_1(V', m)$, *outcome ok. If* $ok = 1$, *run* $A^H_2()$ *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 $|P^1_A - P^2_A|$ is negligible, and thus TRE′ is revocably hiding.

The full proof of Theorem 5 is given in Appendix E.

## 6.2 Precomputation

We will now develop a second transformation for TREs in the random oracle model. In contrast to Section 6.1, we assume a TRE that already uses a random oracle, and we change the way the random oracle is queried. 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 6.3 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 (Timed-release encryptions with offline-queries)** *Let $\ell, n, m$ be integers (dependent on the security parameter), assume that $\ell$ is superlogarithmic, and let $H : \{0,1\}^{\ell+n} \to \{0,1\}^m$ be a random oracle. Let* TRE *be a revocable timed-release encryption in the random oracle model using an oracle $G : \{0,1\}^n \to \{0,1\}^m$.*

*Let* TRE$'$ *be the following timed-release encryption:*

- ***Encryption:*** TRE$'(m)$ *picks $a \xleftarrow{\$} \{0,1\}^\ell$. Then* TRE$'(m)$ *runs $V \leftarrow$* TRE$(m)$*, except that any oracle query $G(x)$ by* 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.*[26]

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 6 (Removing offline oracle queries)** *Let $H : \{0,1\}^{\ell+n} \to \{0,1\}^m$ and $G : \{0,1\}^n \to \{0,1\}^m$ 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 $\tilde{a} = a$.*[27]

*Consider the following two games:*

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

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

[27] Formally, 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 B:* $a \xleftarrow{\$} \{0,1\}^\ell$, $H \xleftarrow{\$} (\{0,1\}^{\ell+n} \to \{0,1\}^m)$, $G \xleftarrow{\$} (\{0,1\}^n \to \{0,1\}^m)$, $A^H()$, $b' \leftarrow \tilde{B}^{G,H}(a)$.

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

We give the proof in Appendix F.

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 6 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 6 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).

In more detail:

*Proof of Theorem 6.* 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

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

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

Let $\tilde{B}^{G,H}(a)$ run $V \leftarrow \mathrm{TRE}^G(m_b), b' \leftarrow \tilde{A}_1^{G,H}(a, V)$ where $\tilde{A}_1$ is the result of applying the transformation described in Lemma 6 (that transforms $B$ into $\tilde{B}$ there) to $A_1$. Note that our $\tilde{B}$ results from $B$ when applying the transformation from Lemma 6.

(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 $H \xleftarrow{\$} (\{0,1\}^{\ell+n} \to \{0,1\}^m)$, $(m_0, m_1) \leftarrow A_0^H(a, V)$. 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

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

Here $(*)$ uses Lemma 6 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 $\left|p_0^* - p_1^*\right|$ is negligible. Since $p_b^* \approx p_b$ for any $b \in \{0,1\}$, it follows that $\left|p_0 - p_1\right|$. Thus TRE′ is $T$-hiding. □

### 6.3 Iterated hashing

In all constructions so far we assumed that we already have a (non-revocable) TRE. In the classical setting, only three constructions of TREs are known. The one from [RSW96] can be broken by factoring, the one from [BGJ+15] does not seem to be practical due to its strong assumptions and large gap, this leaves only repeated hashing as a practical candidate for the quantum setting. We prove that the following construction to be one-way without offline queries:

**Definition 10 (Iterated hashing)** *Let $n$ and $T$ be polynomially-bounded integers (depending on the security parameter), and assume that $n$ is superlogarithmic. Let $H : \{0,1\}^n \to \{0,1\}^n$ denote the random oracle.*

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

- *Encryption: $\mathrm{TRE}_{ih}(m)$ 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 $\mathrm{TRE}_{ih}$ 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 $\mathrm{TRE}_{ih}$ is one-way without offline-queries, so we can later use the transformation from Appendix F to remove this restriction.

Yet, using the random-oracle transformations from Theorems 5 and 6, we can transform it into a hiding TRE. This is plugged into $\mathrm{RTRE}_{ow}$, 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 Definition 11 below.)

An alternative construction is to plug $\mathrm{TRE}_{ih}$ (after transforming it using Theorems 5 and 6) into $\mathrm{RTRE}_{hid}$. This results in a more complex yet everlastingly secure scheme.

And finally, if we wish to avoid the random oracle model altogether, we can take as our basic assumption that a suitable variant of iterated hashing is a hiding TRE,[28] and get a revocably hiding, everlastingly secure TRE by plugging it into $\mathrm{RTRE}_{hid}$.

[28] E.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.

**Theorem 7 (Iterated hashing is one-way without offline-queries)** $\mathrm{TRE}_{ih}$ *from Definition 10 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 70,* (30)*).*

The proof is given in Appendix G.

As mentioned above, by combining our results so far, we get the following revocably hiding TRE in the random oracle model:

**Definition 11 (Hash-based revocable timed-release encryption)** *Let $\ell$ be an integer and $\eta$ the security parameter. Assume three random oracles $G : \{0,1\}^\eta \to \{0,1\}^\ell$ and $H : \{0,1\}^{2\eta} \to \{0,1\}^\eta$ and $L : \{0,1\}^{2\eta} \to \{0,1\}^{2\eta}$. We construct a revocable timed-release encryption $\mathrm{RTRE}_{hash}$ 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 $|\Psi\rangle := |k \oplus p\rangle_B$.*
- *$h_1 := H_a^{T+1}(0^n) \oplus k^*$ 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 $(B\|p) := h_2 \oplus L\big(a\|(h_1 \oplus H_a^{T+1}(0^n))\big)$.*
- *Measure $|\Psi\rangle$ in basis $B$; call the outcome $\gamma$.*
- *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 $\gamma$.*
- *If $\gamma = k \oplus p$, revocation succeeds (sender outputs 1).*

**Theorem 8 ($\mathrm{RTRE}_{hash}$ is revocably hiding)** *The timed-release encryption $\mathrm{RTRE}_{hash}$ from Definition 11 is $T$-revocably hiding and $T$-hiding in the random oracle model, assuming the parallel oracle-query timing model.*

*Proof.* The timed-release encryption $\mathrm{TRE}_{ih}$ from Definition 10 (with $n := \eta$ and using an oracle $H : \{0,1\}^\eta \to \{0,1\}^\eta$) is $T$-one-way without offline-queries by Theorem 7 and has message space $\{0,1\}^\eta$. Applying the transformation from Theorem 5 (with $n = m = \eta$ and using an oracle $L : \{0,1\}^\eta \to \{0,1\}^{2\eta}$), we get a timed-release encryption with message space $\{0,1\}^{2\eta}$ that is $T$-hiding without offline-queries and uses oracles $H : \{0,1\}^\eta \to \{0,1\}^\eta$ and $L : \{0,1\}^\eta \to \{0,1\}^{2\eta}$. Applying the transformation from Theorem 6 (with $\ell := \eta$), we get a timed-release encryption with message space $\{0,1\}^{2\eta}$ that is $T$-hiding and uses oracles $H : \{0,1\}^{2\eta} \to \{0,1\}^\eta$ and $L : \{0,1\}^{2\eta} \to \{0,1\}^{2\eta}$. (To apply Theorem 6, we can assume that the oracles $H, L$ are encoded into a single oracle.) By using this timed-release encryption as $\mathrm{TRE}_0$ 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 $\delta_T^{ow} = 0$ 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 5 (with oracle $G : \{0,1\}^\eta \to \{0,1\}^\ell$), this leads to the timed-release encryption $\mathrm{RTRE}_{hash}$ from Definition 11. By Theorem 5, $\mathrm{RTRE}_{hash}$ is $T$-hiding and $T$-revocably hiding. □

**Precomputation of iterated hashing.** The main drawback of the iterated hashing construction used in $\mathrm{RTRE}_{hash}$ is the fact that the encryption of a message takes as long as the decryption. In both cases, the hash function $H$ needs to be applied $T+1$ times (to compute $H_a^{T+1}(0^n)$ in $\mathrm{RTRE}_{hash}$). If we want to construct a TRE that takes a week to decrypt, we will need to compute for a week to construct it. However, the value $H_a^{T+1}(0^n)$ is independent of the message $m$ to be encrypted. Thus $H_a^{T+1}(0^n)$ can be precomputed and stored, to be used when we know which message $m$ we want to encrypt. The rest of the encryption is fast.

This approach makes iterated hashing already much more practical, but it still has the drawback that a lot of computational resources are wasted on the sender's side: the sender needs to produce a fresh precomputed iterated hash value for each TRE he wants to send. The following approach could mitigate that problem (but a formal analysis is out of the scope of this work):

The sender (i.e., any party who wishes to send TREs) will have a continuously running iterated hash computation with a random starting value $x$. I.e., at any time $t$, the sender will compute $H^t(x)$. Furthermore, assume some fixed parameter $\Delta$. $\Delta$ indicates the maximum time parameter for any TRE that the sender may wish to produce. Then, if the sender wishes to send a TRE at time $t$ with time parameter $T$, he sends $\mathrm{TRE}(m) := (H^{t-\Delta}(x), H(r \| H^{t-\Delta+T}(x)) \oplus m, r)$. (Here $r$ is a random bitstring.) That is, he makes $H^{t-\Delta}(x)$ public and uses it as the starting point of an iterated hash chain of length $T$. Note that whenever a new TRE is published, no element of the hash chain beyond $H^{t-\Delta}(x)$ has been revealed, so the recipient will have to perform $T$ iterations of $H$ to compute $H^{t-\Delta+T}(x)$.

If we wish to save space, it is sufficient if the sender does not save all computed values $H^t(x)$, but only the values at certain intervals (say every second or every minute). Also values older than $\Delta$ can be discarded.

There is still one problem with this construction: Given one TRE at time $t_0$, the recipient can start constructing the chain $H^{t_0-\Delta+t}(x)$ for values $t \geqslant 0$. Initially, the recipient is $\Delta$ hashes behind the sender. If the recipient's computational power is just slightly larger than the sender's, this gap will become smaller, and after a while the recipient will know $H^{t-\Delta+u}(x)$ at time $t$ for some large $u$. Now if the sender sends a TRE at time $t_1$, the recipient needs to compute $H^{t_1-\Delta+T}(x)$. But to compute this, he can start from $H^{t_1-\Delta+u}(x)$, which needs only $T-u$ hashes as opposed to $T$ hashes. To avoid this problem, the continuously running hash chain will have to be periodically restarted with a new initial value.

A full analysis of this scheme will take into account many factors, in particular the interaction between different TREs arising from the same hash chain (compositionality problems). This analysis is out of scope of this paper, we leave it to future work. (Both as a stand-alone quantum-secure TRE and as part of a construction of a revocable TRE.)

# 7 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 not more than one recipient can decrypt it (until a certain timeout $T'$). 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 URE-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 encryption $\text{RTRE}_{hid}$, he needs to know the bases $B$, the indices $Q$, and the bits $r$. Fortunately, in the construction of $\text{RTRE}_{hid}$, 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.[29]

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.

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.

**Definition 12 (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 $keygen_1()$ produces a classical key pair $(pk, sk)$, $enc_1(sk, id, m)$ returns a (quantum) ciphertext $C$ with plaintext $m$ with unique id $id$,*[30] *$dec_1(pk, C)$ returns a pair $(m, id)$.*

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

$$Pr[m = m' \wedge id = id' : (pk, sk) \leftarrow keygen_1, (m, id) \leftarrow A(pk), \\ C \leftarrow enc_1(sk, id, m), (m', id') \leftarrow dec_1(pk, C)]$$

*where $dec_1(pk, C)$ is invoked at most time $T'$ after $enc_1(sk, id, m)$.*

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. Note further that, in contrast to normal public-key encryption,

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

[30] The id could also be picked by $enc_1$ itself, e.g., at random or sequentially. Then the security definition (Definition 13) has to be changed in a straightforward way so that the adversary does not pick the id himself but gets it from $enc_1$.

URE uses the secret key for encryption ($enc_1(sk, id, m)$), and the public key for decryption ($dec_1(pk, C)$). This is necessary since anyone should be able to decrypt.

**On the necessity of the time parameter.** Our definition of UREs includes a time parameter $T'$, and the definition of correctness only requires successful decryption if the message is delivered within time $T'$. Our construction makes use of this time parameter to instantiate the underlying TRE. Is such a time parameter necessary in general? The answer is yes, and in fact $T' \in O(T_{dec})$ where $T_{dec}$ is the honest decryption time. Consider the following attack: A URE $C$ containing a message $m$ is created and given to the adversary. The adversary constructs a (unitary) quantum circuit $D$ that applies a purified version of the honest decryption algorithm $dec_1(pk, \cdot)$. Let $M$ denote the output register that contains the decryption. The adversary applies $D$ to $C$. Due to the correctness of the URE, $M$ contains $|m\rangle$ (or a state very close to $|m\rangle$). Then the adversary measures $m$. Since the state of $M$ is $|m\rangle$, this measurement will not disturb the state. Now the adversary applies $D^\dagger$. This restores the original URE $C$. The time for these operations is $O(T_{dec})$. The adversary now has $m$, and he can send the unmodified $C$ on to the honest recipient. If the honest recipient does not have a timeout for accepting UREs, he will decrypt $C$ successfully, in violation of the security of UREs.

**Security of UREs.** 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 13 (Security of UREs)** *We call an URE* $(keygen_1, enc_1, dec_1)$ secure *iff for any sequential-polynomial-time adversary $A$ (that may share state between invocations), the following is negligible*

$$\Big|\Pr[b' = b_{id^*} : (pk, sk) \leftarrow keygen_1(), b_\perp \xleftarrow{\$} \{0,1\}, \\ C \leftarrow A^E(pk), (m, id^*) \leftarrow dec_1(pk, C), b' \leftarrow A^E(pk, id^*)] - \tfrac{1}{2}\Big|.$$

*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 $m$.

**Constructing URE.** We can now proceed to formalize our URE construction (that was sketched above). Our construction is based specifically on the timed-release encryption $\mathrm{RTRE}_{hid}$ from Section 5.

**Definition 14 (URE from timed-release encryptions)** *Let $(sigkeygen, sign, verify)$ be an existentially quantum-unforgeable signature scheme. Let $\mathrm{TRE}_0$ be a timed-release encryption. Let $\mathrm{RTRE}_{sk,t_0,id}$ be defined like $\mathrm{RTRE}_{hid}$ (Definition 9), except that $V_0 \leftarrow \mathrm{TRE}_0(B, Q, r, p)$ is replaced by $\sigma := sign(sk, (B, Q, r, t_0, id)), V_0 \leftarrow \mathrm{TRE}_0(B, Q, r, p, \sigma)$. We define an unknown recipient encryption scheme $\mathrm{URE}(T')$ (parametric in a time duration $T'$) as follows:*

- ***Key generation:*** *$keygen_1() := sigkeygen()$.*

- ***Encryption:*** *$\mathrm{enc}_1(sk, id, m)$ does: Let $t_0$ be the current time (more precisely, any time not later than the time when $\mathrm{enc}_1$ returns). Let $V := \mathrm{RTRE}_{sk,t_0,id}(m)$. Return $C := (t_0, id, V)$.*
- ***Decryption:*** *$\mathrm{dec}_1(pk, (t_0, id, V))$ does: Let $t_1$ be the current time. Decrypt the timed-release encryption $V_0$ contained in $V$ to get $B, Q, r, p, \sigma$. Run the revocation test of $\mathrm{RTRE}_{sk,t_0,id}$ using those values $B, Q, r$. Run $\mathrm{verify}(pk, \sigma, (B, Q, r, t_0, id))$. Check if $t_1 \leqslant t_0 + T'$. If all three checks succeed, decrypt $V$ (as specified in the definition of $\mathrm{RTRE}_{hid}$) to get $m$ and return $(m, id)$. If one of the three checks fails, return $(\bot, \bot)$.*

Finally, we can show security.

**Theorem 9** *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 $T'$.*[31]

*Assume the conditions of Theorem 3 are satisfied. Let $\delta_T^{hid}, \ell$ be as in Theorem 3. Let $T' := T - \delta_T^{hid}$. Then $\mathrm{URE}(T')$ 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 $\mathrm{dec}_1$ in Definition 13 (i.e., we have everlasting security).*

*Proof.* We prove this with a sequence of games. The first game is the game from Definition 13.

**Game 1 (Original game)**
*(a)* $(pk, sk) \leftarrow \mathit{keygen}_1()$.
*(b)* $b_\bot \xleftarrow{\$} \{0,1\}$.
*(c)* $C \leftarrow A^E(pk)$.
*(d)* $(m, id^*) \leftarrow \mathit{dec}_1(pk, C)$.
*(e)* $b' \leftarrow A^E(pk, id^*)$.

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

We now unfold the definition of $\mathit{dec}_1$. For convenience, for a timed-release encryption $V$ returned by $\mathrm{RTRE}_{sk,t_0,id}$, let $\mathit{getV}_0(V)$ return the contained timed-release encryption $V_0$ contained in $V$. Let $\mathit{decTRE}_0(V)$ denote the decryption of $\mathit{getV}_0(V)$ (using the decryption algorithm of $\mathrm{TRE}_0$). Let $\mathit{revocRTRE}(V, B, Q, r)$ denote the revocation test of $\mathrm{RTRE}_{sk,t_0,id}$ on timed-release encryption $V$ using values $B, Q, r$.

Note that in the following game, we omitted the computation of $m$ (by $\mathit{dec}_1$) because $m$ is never used anyway.

**Game 2 (Unfolding $\mathit{dec}_1$)**
*(a)* $(pk, sk) \leftarrow \mathit{keygen}_1()$.
*(b)* $b_\bot \xleftarrow{\$} \{0,1\}$.
*(c)* $(t_0, id, V) \leftarrow A^E(pk)$.
*(d)* ~~$(m, id^*) \leftarrow \mathit{dec}_1(pk, V)$~~
*(e)* $t_1 \leftarrow \mathit{currentTime}()$
*(f)* $(B, Q, r, p, \sigma) = \mathit{decTRE}_0(\mathit{getV}_0(V))$.
*(g)* $ok \leftarrow \mathit{revocRTRE}(V, B, Q, r)$.
*(h)* $sigOk \leftarrow \mathit{verify}(pk, \sigma, (B, Q, r, t_0, id))$
*(i)* $timeOk \leftarrow (t_1 \leqslant t_0 + T')$
*(j)* $allOk := ok \wedge sigOk \wedge timeOk$.
*(k)* *If* $allOk = 1$, $id^* := id$. *Else* $id^* := \bot$.
*(l)* $b' \leftarrow A^E(pk, id^*)$

[31] Parallel 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.

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

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 $\mathrm{RTRE}_{sk,t_0,id}$ 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)* $j \xleftarrow{\$} \{1,\ldots,\#E\}$.
*(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* $\nexists j.id = id_j$, *then* $id := id_1$.
*(g)* $(B, Q, r, p, \sigma) = decTRE_0(getV_0(V))$.
*(h)* $ok \leftarrow revocRTRE(V, B_{id}, Q_{id}, r_{id})$.
*(i)* $sigOk \leftarrow verify(pk, \sigma, (B, Q, r, t_0, id))$.
*(j)* $timeOk \leftarrow (t_1 \leqslant t_{0,id} + T')$.
*(k)* $allOk := ok \wedge sigOk \wedge timeOk$.
*(l)* *If* $allOk = 1$, $id^* := id$. *Else* $id^* := \perp$.
*(m)* $b' \leftarrow A^E(pk, id^*)$.

Games 2 and 3 only differ when $\big((B, Q, r, t_0) \neq (B_{id}, Q_{id}, r_{id}, t_{0,id}) \vee \nexists j.id = id_j\big) \wedge sigOk = 1$ in Game 2. But $(B, Q, r, t_0) \neq (B_{id}, Q_{id}, r_{id}, t_{0,id}) \vee \nexists j.id = id_j$ 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 $sigOk = 1$ implies that $\sigma$ 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 $\Pr[\big((B, Q, r, t_0) \neq (B_{id}, Q_{id}, r_{id}, t_{0,id}) \vee \nexists j.id = id_j\big) \wedge sigOk = 1 : Game\ 2] \leqslant \mu_1$ for some negligible $\mu_1$ and hence $\big|\Pr[b' = b_{id^*} : Game\ 2] - \Pr[b' = b_{id^*} : Game\ 3]\big| \leqslant \mu_1$.

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 $allOk := 0$ which means that $A$ then has probability exactly $\frac{1}{2}$ of guessing $b_{id^*} = b_\perp$.)

**Game 4 (Guessing the session)**

*(a)* $j \xleftarrow{\$} \{1,\ldots,\#E\}$.
*(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* $\nexists j.id = id_j$, *then* $id := id_1$.
*(g)* $(B, Q, r, p, \sigma) = decTRE_0(getV_0(V))$.
*(h)* $ok \leftarrow revocRTRE(V, B_{id}, Q_{id}, r_{id})$.
*(i)* $sigOk \leftarrow verify(pk, \sigma, (B, Q, r, t_0, id))$.

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

First, observe that due to step (f), $id = id_j$ holds for some $j \in \{1, \ldots, \#E\}$. 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 $id^* = \bot$ and hence $b' = b_{id^*}$ with probability exactly $\frac{1}{2}$. Thus

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

Thus so far we have

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

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)* $j \xleftarrow{\$} \{1, \ldots, \#E\}$.
*(b)* $(pk, sk) \leftarrow keygen_1()$.
*(c)* $b_\bot \xleftarrow{\$} \{0, 1\}$.
*(d)* $(t_0, id, V) \leftarrow A^E(pk)$.
*(e)* $t_1 \leftarrow currentTime()$
*(f)* *If* $\nexists j.id = id_j$, *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)* $timeOk \leftarrow (t_1 \leqslant t_{0,id} + T')$.
*(k)* $allOk := ok \wedge sigOk \wedge timeOk \wedge id = id_j$.
*(l)* *If* $allOk = 1$, $id^* := id$. *Else* $id^* := \bot$.
*(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 $b' = b_{id^*} = b_\bot$ with probability $\frac{1}{2}$, no matter which inputs are given to *revocRTRE*. Hence $\Pr[b' = b_{id^*} : Game\ 5] = \Pr[b' = b_{id^*} : Game\ 4]$.

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)* $j \xleftarrow{\$} \{1, \ldots, \#E\}$.
*(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) $b \xleftarrow{\$} \{0,1\}$. $b_{id'} := b$. $t_0^* \leftarrow currentTime()$. $V^* \leftarrow \mathrm{RTRE}_{sk,t_0^*,id'}(m_b)$.
(g) *Denote the values* $B, Q, r$ *chosen by* $\mathrm{RTRE}_{sk,t_0^*,id'}$ *with* $B^*, Q^*, r^*$.
(h) $(t_0, id, V) \leftarrow (A_1')^E((t_0^*, id', V^*))$.
(i) $t_1 \leftarrow currentTime()$
(j) *If* $\nexists j.id = id_j$, *then* $id := id_1$.
(k) $(B, Q, r, p, \sigma) = decTRE_0(getV_0(V))$.
(l) $ok \leftarrow revocRTRE(V, B^*, Q^*, r^*)$.
(m) $sigOk \leftarrow verify(pk, \sigma, (B, Q, r, t_0, id))$.
(n) $timeOk \leftarrow (t_1 \leqslant t_0^* + T')$.
(o) $allOk := ok \wedge sigOk \wedge timeOk \wedge id = id'$.
(p) *If* $allOk = 1$, $id^* := id$. *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 $\Pr[b' = b_{id^*} : Game\ 6] = \Pr[b' = b_{id^*} : Game\ 5]$.

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) $j \xleftarrow{\$} \{1, \ldots, \#E\}$.
(b) $(pk, sk) \leftarrow keygen_1()$.
(c) $b_\perp \xleftarrow{\$} \{0,1\}$.
(d) $(m_0, m_1, id') \leftarrow A_0^E(pk, j)$.
(e) $b \xleftarrow{\$} \{0,1\}$. $b_{id'} := b$. $t_0^* \leftarrow currentTime()$. $V^* \leftarrow \mathrm{RTRE}_{sk,t_0^*,id'}(m_b)$.
(f) *Denote the values* $B, Q, r$ *chosen by* $\mathrm{RTRE}_{sk,t_0^*,id'}$ *with* $B^*, Q^*, r^*$.
(g) $(t_0, id, V) \leftarrow A_1^E((t_0^*, id', V^*))$.
(h) $t_1 \leftarrow currentTime()$
(i) *If* $\nexists j.id = id_j$, *then* $id := id_1$.
(j) $(B, Q, r, p, \sigma) = decTRE_0(getV_0(V))$.
(k) $ok \leftarrow revocRTRE(V, B^*, Q^*, r^*)$.
(l) $sigOk \leftarrow verify(pk, \sigma, (B, Q, r, t_0, id))$.
(m) $timeOk \leftarrow (t_1 \leqslant t_0^* + T')$.
(n) $allOk := ok \wedge sigOk \wedge timeOk \wedge id = id'$.
(o) *If* $allOk = 1$, $id^* := id$. *Else* $id^* := \perp$.
(p) $b' \leftarrow A_2^E(pk, id^*)$.

If $A_1'$ runs more than $T'$ steps, we will have $t_1 > t_0^* + T'$ and thus $timeOk = 0$, 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 $\Pr[b' = b_{id^*} : Game\ 7] = \Pr[b' = b_{id^*} : Game\ 6]$.

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

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

Thus so far we have

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

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 (h)–(j) and steps (l)–(p) and return $(b' \wedge allOk)$. 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 $revocRTRE(V)$, we mean an execution of the revocation test of $\mathrm{RTRE}_{sk,t_0^*,id'}$. (I.e., $revocRTRE(V)$ is the same as $revocRTRE(V, B, Q, r)$ using the values $B, Q, r$ chosen by the earlier call $\mathrm{RTRE}_{sk,t_0^*,id'}$.)

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)* $V^* \leftarrow \mathrm{RTRE}_{sk,t_0^*,id'}(m_b)$.
*(d)* $V \leftarrow B_1(V^*)$.
*(e)* $ok \leftarrow revocRTRE(V)$.
*(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

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

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

Then we have

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

For the next step, we will need the security of $\mathrm{RTRE}_{sk,t_0^*,id'}$. Theorem 3 states that $\mathrm{RTRE}_{hid}$ is $T'$-revocably hiding, but $\mathrm{RTRE}_{sk,t_0^*,id'}$ differs from $\mathrm{RTRE}_{hid}$ by additionally including $\sigma := sign(sk, (B, Q, r, t_0^*, id'))$. However, the proof of Theorem 3 still goes through for this modified scheme. (In fact, $\sigma$ is a function of public parameters $sk, t_0^*, id'$, and of data $B, Q, r$ that is contained contained in $V_0$ anyway. So it is not surprising that the inclusion of $\sigma$ does not reduce security.) Thus $\mathrm{RTRE}_{sk,t_0^*,id'}$ 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 $\mathrm{RTRE}_{sk,t_0^*,id'}$ is $T'$-revocably hiding with everlasting security, $\mu_2$ is negligible.

So altogether we have

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

which is negligible. Hence $\mathrm{URE}(T')$ is secure. □

**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 13) 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.

**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, the Cluster of Excellence "Multimodal Computing and Intereaction". We thank Sébastien Gambs for the suggesting the data retention application. We thank the anonymous reviewers for many helpful suggestions, in particular the digital goods application.

# A Auxiliary lemmas

**Lemma 7 (Detecting bit errors)** *Fix integers $t, q, n \geqslant 1$. Let $x^0, x^1 \in \{0,1\}^{q+n}$ such that $\omega(x^0) \geqslant t+1$ or $\omega(x^1) \geqslant t+1$. Consider the following process: Select uniformly $Q = \{Q_1, \ldots, Q_q\} \in [q+n]_q$. (Recall, $[q+n]_q$ refers to q-size subsets of $\{1, \ldots, q+n\}$, see page 7.) Select uniformly $B = B_1 \ldots B_q \in \{0,1\}^q$. Let $P(x) := \Pr[\nexists i \in \{1, \ldots, q\} : x_{Q_i}^{B_i} = 1]$.*

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

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

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 $P(x) = \Pr[\nexists j \in I : C_j = 1 \wedge j \in Q]$.

Let $R_1, \ldots, R_{q+n}$ 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 $P(x) = \Pr[\nexists j \in I : C_j = 1 \wedge j \in R \,\big|\, |R| = q] = \Pr[\forall j \in I : Z_j = 0 \,\big|\, |R| = q]$.

We proceed to lower bound $\Pr[|R| = q]$. The Stirling 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

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

Thus

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

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

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

**Lemma 8 (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 7.)*

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

$$\begin{aligned}\langle x,y|(A\otimes I)|\widetilde{0^n0^n}\rangle &= \sum_z \frac{1}{\sqrt{N}}\langle x,y|(A\otimes I)|z,z\rangle = \sum_z \frac{1}{\sqrt{N}}A_{xz}\delta_{yz}\\ &= \frac{1}{\sqrt{N}}A_{xy} = \frac{1}{\sqrt{N}}A^T_{yx} = \sum_z \frac{1}{\sqrt{N}}\delta_{xz}A^T_{yz} = \sum_z \frac{1}{\sqrt{N}}\langle x,y|(I\otimes A^T)|z,z\rangle\\ &= \langle x,y|(I\otimes A^T)|\widetilde{0^n0^n}\rangle.\end{aligned}$$

Since $|x,y\rangle$ form an orthonormal basis, this implies that $(A\otimes I)|\widetilde{0^n0^n}\rangle = (I\otimes A^T)|\widetilde{0^n0^n}\rangle$. □

**Lemma 9 (Cauchy-Schwarz inequality, vector based)** *Let $\alpha_i$ be complex numbers and $|\Psi_i\rangle$ finite-dimensional vectors. Then*

$$\big\|\sum_i \alpha_i|\Psi_i\rangle\big\|^2 \leqslant \Big(\sum_i |\alpha_i|^2\Big)\cdot\Big(\sum_i \||\Psi_i\rangle\|^2\Big).$$

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

$$\begin{aligned}\big\|\sum_i \alpha_i|\Psi_i\rangle\big\|^2 = \sum_j\big|\sum_i \alpha_i x_{ij}\big|^2 &\overset{(*)}{\leqslant} \sum_j\Big(\sum_i|\alpha_i|^2\cdot\sum_i|x_{ij}|^2\Big)\\ &= \sum_i|\alpha_i|^2\cdot\sum_i\sum_j|x_{ij}|^2 = \sum_i|\alpha_i|^2\cdot\sum_i\||\Psi_i\rangle\|^2.\end{aligned}$$

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

**Lemma 10 (Closeness to ideal states)** *Let $\rho$ be a mixed state, and let $P$ be a projector. Let $1-\varepsilon := \operatorname{tr} P\rho$. (I.e., $\varepsilon$ is the probability that measuring $\rho$ with $P$ fails.)*

*Then there exists a mixed state $\rho^{ideal}$ such that*

- $\mathrm{TD}(\rho,\rho^{ideal}) \leqslant \sqrt{\varepsilon}$.
- *$\rho^{ideal}$ is a mixture over $\operatorname{im} P$. (I.e., $\rho = \sum_i p_i|\Psi_i\rangle\langle\Psi_i|$ for quantum states $|\Psi_i\rangle \in \operatorname{im} P$ and $p_i \geqslant 0$ 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., $\rho$ 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

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

Then we have

$$\mathrm{TD}(\rho,\rho^{ideal}) \overset{(*)}{\leqslant} \sqrt{1-F(\rho,\rho^{ideal})^2} = \sqrt{\varepsilon}.$$

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

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

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

$$\mathrm{TD}(\rho,\rho^{ideal}) = \mathrm{TD}\big(\sum p_i\rho_i, \sum p_i\rho_i^{ideal}\big) \overset{(*)}{\leqslant} \sum p_i\mathrm{TD}(\rho_i,\rho_i^{ideal}) \leqslant \sum p_i\sqrt{\varepsilon_i} \overset{(**)}{\leqslant} \sqrt{\sum p_i\varepsilon_i} = \sqrt{\varepsilon}.$$

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

**Lemma 11** *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* $\mathrm{TD}(|\Psi_1\rangle, |\Psi_2\rangle) \leqslant 2\||\Psi_1^*\rangle\|$.

*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 $\||\Psi_2^*\rangle\| = \alpha$. 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

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

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

$$\mathrm{TD}(|\Psi_1\rangle, |\Psi_2\rangle) \overset{(*)}{\leqslant} \sqrt{1 - (1 - 2\alpha^2)^2} = \sqrt{4\alpha^2(1 - \alpha^2)} = \sqrt{4\alpha^2\beta^2} = 2\alpha\beta \leqslant 2\alpha.$$

$(*)$ only holds if $1 - 2\alpha^2 \geqslant 0$.[32] However, if this does not hold, then $\alpha \geqslant \frac{1}{\sqrt{2}}$ and thus $\mathrm{TD}(|\Psi_1\rangle, |\Psi_2\rangle) \leqslant 1 \leqslant 2\alpha$. □

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

In this appendix, we give the full security proof for the protocol $\mathrm{RTRE}_{ow}$ from Section 3, Definition 7. We first start with the proof that $\mathrm{RTRE}_{ow}$ is revocably one-way. And below (page 46) we show that it is (non-revocably) hiding.

We restate Theorem 1

**Theorem 10 (**$\mathrm{RTRE}_{ow}$ **is revocably one-way)** *Let $\delta_T^{ow}$ 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 40 below), a measurement whether two $n$-qubit registers are in a $|\widetilde{0^n 0^n}\rangle$ state with at most $t$ phase flips and $t$ bit flips (for a given $t$; formally defined as $P_t^{EPR}$ on page 40 below), and one NOT- and one AND-gate.*

*Assume that the protocol parameter $n$ is superlogarithmic.*

*The protocol* $\mathrm{RTRE}_{ow}$ *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 46.*

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 10, 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 7):

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

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,

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

[32] Thanks to Espen Auseth Nielsen for pointing this out.

**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)* $V_0 \leftarrow \mathrm{TRE}_0(B,p)$.
*(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* $\gamma$.
*(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 $\mathrm{RTRE}_{ow}$ inlined), it suffices to show that $\Pr[m = m' \wedge ok = 1 : \mathit{Game}\ 1]$ 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)* $V_0 \leftarrow \mathrm{TRE}_0(B,p)$.
*(d)* $X \leftarrow |m\rangle_B$.
*(e)* *Run* $A_1(X, V_0)$.
*(f)* *Measure* $X$ *in basis* $B$*; outcome* $\gamma$.
*(g)* *If* $m = \gamma$, $ok := 1$. *Else* $ok := 0$.
*(h)* $m' \leftarrow A_2() \oplus p$.

**Lemma 12 (Game 1 vs. Game 2)** $\Pr[m' = m \wedge ok = 1 : \mathit{Game}\ 1] = \Pr[m' = m \wedge ok = 1 : \mathit{Game}\ 2]$.

*Proof.* Consider first an intermediate game $G$ which is like Game 2, except that the last step is still "$m' \leftarrow A_2()$". 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 $\Pr[m' = m \wedge ok = 1 : \mathit{Game}\ 1] = \Pr[m' = m \oplus p \wedge ok = 1 : G]$.

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

**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)* $V_0 \leftarrow \mathrm{TRE}_0(B,p)$.
*(d)* *Initialize* $XY$ *as* $|\widetilde{0^n 0^n}\rangle$.
*(e)* *Run* $A_1(X, V_0)$.
*(f)* *Measure* $X$ *in basis* $B$*; outcome* $\gamma$.
*(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 13 (Game 2 vs. Game 3)** $\Pr[m' = m \wedge ok = 1 : Game\ 2] = \Pr[m' = m \wedge ok = 1 : Game\ 3]$.

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

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

Here $(*)$ uses Lemma 8 and the fact that $H$ is symmetric.

Hence the probability of measuring $m$ is $\||\Psi_m\rangle\|^2 = 2^{-n}$ 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. □

**Game 4 (Changed revocation test)**
*(a) Run* $A_0()$.
*(b)* $p \xleftarrow{\$} \{0,1\}^n$, $B \xleftarrow{\$} \{0,1\}^n$.
*(c)* $V_0 \leftarrow \mathrm{TRE}_0(B,p)$.
*(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* $\gamma$.~~
*(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 14 (Game 3 vs. Game 4)** $\Pr[m' = m \wedge ok = 1 : Game\ 3] = \Pr[m' = m \wedge ok = 1 : Game\ 4]$.

*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 $\Pr[m' = m \wedge ok = 1 : Game\ 4] = \Pr[m' = m \wedge ok = 1 : G]$.

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 $\Pr[m' = m \wedge ok = 1 : G'] = \Pr[m' = m \wedge ok = 1 : Game\ 3]$. □

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

**Game 5 (Testing the state)**

*(a) Run* $A_0()$.
*(b)* $p \xleftarrow{\$} \{0,1\}^n$, $B \xleftarrow{\$} \{0,1\}^n$.
*(c)* $V_0 \leftarrow \mathrm{TRE}_0(B,p)$.
*(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 isEPR.*
*(h)* ~~*Measure* $Y$ *in basis* $B$*, outcome* $m$*.*~~
*(i)* ~~$m' \leftarrow A_2() \oplus p$.~~

**Lemma 15 (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* $\Pr[m = m'] \leqslant 2^{-n}(n+1)^{2t}$*. (In other words, the min-entropy of* $m$ *given* $Z$ *is at least* $n - 2t\log(n+1)$*.)*

*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 $T := \{fe : \omega(f), \omega(e) \leqslant t\}$. 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

$$\begin{aligned}
\Pr[m = m'] &= \sum_m \big\| \left(I_n \otimes H^B |m\rangle\langle m| H^B \otimes P_m\right) |\Psi\rangle \big\|^2 \\
&= \sum_m \Big\| \sum_{fe\in T} \alpha_{fe} (I_n \otimes H^B |m\rangle\langle m| H^B) |\widetilde{fe}\rangle \otimes P_m |\Psi_{fe}\rangle \Big\|^2 \\
&\overset{(*)}{\leqslant} \sum_m \Big( \sum_{fe\in T} |\alpha_{fe}|^2 \cdot \sum_{fe\in T} \|((I_n \otimes H^B |m\rangle\langle m| H^B) |\widetilde{fe}\rangle \otimes P_m |\Psi_{fe}\rangle\|^2 \Big) \\
&= \sum_m \Big( \underbrace{\sum_{fe\in T} |\alpha_{fe}|^2}_{=1} \cdot \sum_{fe\in T} \underbrace{\|(I_n \otimes H^B |m\rangle\langle m| H^B) |\widetilde{fe}\rangle\|^2}_{=2^{-n} \quad (**)} \cdot \|P_m |\Psi_{fe}\rangle\|^2 \Big) \\
&= 2^{-n} \sum_{fe\in T} \underbrace{\sum_m \|P_m |\Psi_{fe}\rangle\|^2}_{=1} = 2^{-n}|T|. \qquad (7)
\end{aligned}$$

Here $(*)$ uses Lemma 9 (vector-based variant of the Cauchy-Schwarz-inequality).

And $(**)$ uses

$$\begin{aligned}
&\big\|(I_n \otimes H^B |m\rangle\langle m| H^B) |\widetilde{fe}\rangle\big\| = \big\|(Z^f X^e \otimes H^B |m\rangle\langle m| H^B) |\widetilde{0^n 0^n}\rangle\big\| \\
&\overset{\text{Lemma 8}}{=} \big\|(Z^f X^e H^B \otimes H^B |m\rangle\langle m|) |\widetilde{0^n 0^n}\rangle\big\| = \big\|(Z^f X^e H^B \otimes H^B) \cdot 2^{-n/2} |m\rangle |m\rangle\big\| = 2^{-n/2}.
\end{aligned}$$

We now bound $|T|$. Notice that any $e$ with $\omega(e) \leqslant t$ can be specified by giving $t$ indices $i \in \{0, \ldots, n\}$ 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 $|T| \leqslant (n+1)^{2t}$.

Summarizing, we have

$$\Pr[m = m'] \overset{(7)}{\leqslant} 2^{-n}|T| \leqslant 2^{-n}(n+1)^{2t}. \qquad \square$$

**Lemma 16 (Game 4 vs. Game 5)** $\Pr[m' = m \wedge ok = 1 : Game\ 4] \leqslant \sqrt{\Pr[isEPR = 0 \wedge ok = 1 : Game\ 5]} + 2^{-n}(n+1)^{2t}$.

*Proof.* For $b \in \{0,1\}^n$, let $\rho_b$ 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

$$\Pr[isEPR = 1 \wedge ok = 1 : Game\ 5] = \sum_b \operatorname{tr} P_t^{EPR} \rho_b \cdot \Pr[B = b \wedge ok = 1 : Game\ 5]. \quad (8)$$

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 10 there is a state $\rho'_b$ such that $\mathrm{TD}(\rho_b, \rho'_b) \leqslant \sqrt{1 - \operatorname{tr}(P_t^{EPR}\rho_b)}$ 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 15 implies that $\Pr[m = m' : Game\ 4'] \leqslant \varepsilon := 2^{-n}(n+1)^{2t}$. Here *Game* $4'$ is the following game: "Initialize $XYZ$ with $\rho'_b$. Measure $Y$ in basis $b$, outcome $m$. $m' \leftarrow A_2(Z)$. ($Z$ stands for the quantum register holding the adversary's state.)"

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

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

$$\begin{aligned}
&\Pr[m = m' \wedge ok = 1 : Game\ 4] \\
&= \sum_b q_b \Pr[m = m' \mid B = b \wedge ok = 1 : Game\ 4] \\
&\leqslant \sum_b q_b \Big(\varepsilon + \sqrt{1 - \operatorname{tr}(P_t^{EPR}\rho_b)}\Big) \\
&\leqslant \big(\textstyle\sum_b q_b\big) \cdot \left(\varepsilon + \sqrt{1 - \dfrac{\sum_b q_b \operatorname{tr}(P_t^{EPR}\rho_b)}{\sum_b q_b}}\ \right) && \text{(Jensen's inequality)} \\
&= \big(\textstyle\sum_b q_b\big)\varepsilon + \sqrt{\big(\sum_b q_b\big) \cdot \Big(\big(\sum_b q_b\big) - \big(\sum_b q_b \operatorname{tr}(P_t^{EPR}\rho_b)\big)\Big)} \\
&\leqslant \varepsilon + \sqrt{\Pr[ok = 1 : Game\ 5] - \textstyle\sum_b q_b \operatorname{tr}(P_t^{EPR}\rho_b)} && \text{(using } \textstyle\sum_b q_b = \Pr[ok = 1 : Game\ 5] \leqslant 1\text{)} \\
&\overset{(8)}{=} \varepsilon + \sqrt{\Pr[ok = 1 : Game\ 5] - \Pr[isEPR = 1 \wedge ok = 1 : Game\ 5]} \\
&= \varepsilon + \sqrt{\Pr[isEPR = 0 \wedge ok = 1 : Game\ 5]}.
\end{aligned}$$

□

**Game 6 (Using fake timed-release encryption)**
*(a)* *Run* $A_0()$.
*(b)* $p \xleftarrow{\$} \{0,1\}^n$, ~~$B \xleftarrow{\$} \{0,1\}^n$.~~
*(c)* $\hat{B} \leftarrow \{0,1\}^n$. $V_0 \leftarrow \mathrm{TRE}_0(\hat{B}, p)$.
*(d)* *Initialize* $XY$ *as* $|\widetilde{0^n 0^n}\rangle$.
*(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 17 (Game 5 vs. Game 6)** $\Pr[\mathit{isEPR} = 0 \wedge \mathit{ok} = 1 : \mathit{Game}\ 5] \leqslant \Pr[\mathit{isEPR} = 0 \wedge \mathit{ok} = 1 : \mathit{Game}\ 6] + \mu$ *for some negligible* $\mu$.

*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 $V_0 \leftarrow \mathrm{TRE}_0(B, p)$.

Then we immediately see that $\Pr[\mathit{isEPR} = 0 \wedge \mathit{ok} = 1 : G] = \Pr[\mathit{isEPR} = 0 \wedge \mathit{ok} = 1 : \mathit{Game}\ 5]$ and $\Pr[\mathit{isEPR} = 0 \wedge \mathit{ok} = 1 : G'] = \Pr[\mathit{isEPR} = 0 \wedge \mathit{ok} = 1 : \mathit{Game}\ 6]$ 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 $\mathit{isEPR} = 0 \wedge \mathit{ok} = 1$). Together, these steps take time at most $T$ (by definition of $\delta_T^{ow}$). Furthermore, all steps before and after $V_0 \xleftarrow{\$} \mathrm{TRE}_0(B, p)$ run in sequential-polynomial-time.

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

Hence $\Pr[\mathit{isEPR} = 0 \wedge \mathit{ok} = 1 : G] \leqslant \Pr[\mathit{isEPR} = 0 \wedge \mathit{ok} = 1 : G'] + \mu$ for some negligible $\mu$. □

**Lemma 18 (Equality measurements on Bell-basis states)** $P_B^=|\widetilde{fe}\rangle = |\widetilde{fe}\rangle$ *iff for all* $i$ *we have* $(B_i = 0 \wedge f_i = 0) \vee (B_i = 1 \wedge e_i = 0)$. *And* $P_B^=|\widetilde{fe}\rangle = 0$ *otherwise.*

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

| $B$ | $e$ | $f$ | $P_B^=\|\widetilde{fe}\rangle$ | $B$ | $e$ | $f$ | $P_B^=\|\widetilde{fe}\rangle$ |
|---|---|---|---|---|---|---|---|
| 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 $|\widetilde{fe}\rangle = |\widetilde{e_1 f_1}\rangle \otimes \cdots \otimes |\widetilde{e_n f_n}\rangle$ (up to reordering of qubits). □

**Lemma 19 (Game 6 is secure)** $\Pr[\mathit{isEPR} = 0 \wedge \mathit{ok} = 1 : \mathit{Game}\ 6] \leqslant 2^{-t-1}$.

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

Before bounding $\sum_B 2^{-n} \operatorname{tr} \overline{P_t^{EPR}} P_B^= \rho$, we show for any $f, e \in \{0,1\}^n$ that $p_{fe} := \sum_B 2^{-n} \operatorname{tr} \overline{P_t^{EPR}} P_B^= |\widetilde{fe}\rangle\langle\widetilde{fe}| \leqslant 2^{-t-1}$. We distinguish two cases: $\omega(e), \omega(f) \leqslant t$ and $\max(\omega(f), \omega(e)) \geqslant t + 1$. If $\omega(f), \omega(e) \leqslant t$, by Lemma 18, for any $B$ either $P_B^=|\widetilde{fe}\rangle = 0$ or $P_B^=|\widetilde{fe}\rangle = |\widetilde{fe}\rangle$ depending on $B$. Since $P_t^{EPR}|\widetilde{fe}\rangle = |\widetilde{fe}\rangle$, it follows that $\overline{P_t^{EPR}} P_B |\widetilde{fe}\rangle = 0$ and hence $p_{fe} = 0$. If $\max(\omega(f), \omega(e)) \geqslant t + 1$, then by Lemma 18 there are at most $q := 2^n / 2^{t+1}$ different values of $B$ such that $P_B^=|\widetilde{fe}\rangle \neq 0$ (this bound is tight iff $e = 0^n$ and $\omega(f) = t + 1$ or vice versa). Hence $p_{fe} \leqslant q \cdot 2^{-n} = 2^{-t-1}$. Thus, in all cases, $p_{fe} \leqslant 2^{-t-1}$.

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

$$\begin{aligned}
&\Pr[isEPR = 0 \wedge ok = 1 : Game\ 6] \\
&= \sum_B 2^{-n} \operatorname{tr} \overline{P_t^{EPR}} P_B^{=} \rho \\
&\overset{(*)}{=} \sum_B 2^{-n} \operatorname{tr}\Big( \big(\textstyle\sum_{fe} P_{fe}\big) \overline{P_t^{EPR}} P_B^{=} \rho \Big) \\
&= \sum_{Bef} 2^{-n} \operatorname{tr} P_{fe} \overline{P_t^{EPR}} P_B^{=} \rho \\
&\overset{(**)}{=} \sum_{Bef} 2^{-n} \operatorname{tr} P_{fe} \overline{P_t^{EPR}} P_B^{=} \rho P_{fe} \\
&\overset{(***)}{=} \sum_{Bef} 2^{-n} \operatorname{tr} \overline{P_t^{EPR}} P_B^{=} (P_{fe} \rho P_{fe}) \\
&= \sum_{fe} \Big( \alpha_{fe} \sum_B 2^{-n} \operatorname{tr} \overline{P_t^{EPR}} P_B^{=} |\widetilde{fe}\rangle\langle\widetilde{fe}| \Big) \\
&= \sum_{fe} \alpha_{fe} p_{fe} \leqslant \sum_{fe} \alpha_{fe} 2^{-t-1} = \operatorname{tr} \rho \cdot 2^{-t-1} = 2^{-t-1}.
\end{aligned}$$

Here $(*)$ uses that $\sum_{fe} P_{fe} = 1$ since $|\widetilde{fe}\rangle$ 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 18.) □

We can now finally prove the revocable onewayness of $\mathrm{RTRE}_{ow}$:

*Proof of Theorem 10.* We have

$$\begin{aligned}
&\Pr[m' = m \wedge ok = 1 : Game\ 1] \\
&= \Pr[m' = m \wedge ok = 1 : Game\ 4] && \text{(Lemmas 12, 13, and 14)} \\
&\leqslant \sqrt{\Pr[isEPR = 0 \wedge ok = 1 : Game\ 5]} + 2^{-n}(n+1)^{2t} && \text{(Lemma 16)} \\
&\leqslant \sqrt{\Pr[isEPR = 0 \wedge ok = 1 : Game\ 6] + \mu} + 2^{-n}(n+1)^{2t} && \text{(Lemma 17; } \mu \text{ negligible)} \\
&\leqslant \sqrt{2^{-t-1} + \mu} + 2^{-n}(n+1)^{2t} =: \nu && \text{(Lemma 19)} \qquad (9)
\end{aligned}$$

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 $\nu$ is negligible.

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

Thus $\mathrm{RTRE}_{ow}$ is revocably one-way.

Note that (9) also tells us the concrete security of $\mathrm{RTRE}_{ow}$. Namely, when $\mu$ is the advantage of an adversary against $\mathrm{TRE}_0$ (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 $\mathrm{RTRE}_{ow}$. □

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

**Theorem 11 ($\mathrm{RTRE}_{ow}$ is hiding)** *The protocol $\mathrm{RTRE}_{ow}$ 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 $\left|\Pr[b' = 1 : \mathit{Game}\ 1(0)] - \Pr[b' = 1 : \mathit{Game}\ 1(1)]\right|$ is negligible. Here $\mathit{Game}\ 1(b)$ denotes $\mathit{Game}\ 1$ 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)* $V_0 \leftarrow \mathrm{TRE}_0(B, p)$.
*(e)* $X \leftarrow |m_b \oplus p\rangle_B$.
*(f)* $b' \leftarrow A_1(X, V_0)$.

Since $\mathrm{TRE}_0$ is $T$-hiding, and $A_1$ is $T$-time, and $A_0, A_1$ are sequential-polynomial-time, we can replace the arguments of $\mathrm{TRE}_0$ 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)* $V_0 \leftarrow \mathrm{TRE}_0(B, \tilde{p})$.
*(e)* $X \leftarrow |m_b \oplus p\rangle_B$.
*(f)* $b' \leftarrow A(X, V_0)$.

We then have that $\left|\Pr[b' = 1 : \mathit{Game}\ 1(b)] - \Pr[b' = 1 : \mathit{Game}\ 2(b)]\right|$ 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)* $V_0 \leftarrow \mathrm{TRE}_0(B, \tilde{p})$.
*(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 $p \xleftarrow{\$} \{0,1\}^n$, both $p$ and $p \oplus m_b$ have the same distribution. Hence $\Pr[b' = 1 : \mathit{Game}\ 2(b)] = \Pr[b' = 1 : \mathit{Game}\ 3(b)]$ for $b \in \{0,1\}$.

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

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

Note that this also tells us the concrete security of $\mathrm{RTRE}_{ow}$. Namely, when $\mu$ is the advantage of an adversary against $\mathrm{TRE}_0$ (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 $\mu$ also bounds the advantage against $\mathrm{RTRE}_{ow}$. □

# C Full proofs: CSS codes

## C.1 Proof of Lemma 1

*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 $C' := \operatorname{span}\{y_2, \dots, y_k\}$. 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

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

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 $\sum_{y\in\{0,1\}^n/C^\perp}(-1)^{x\cdot y} = 0$. □

## C.2 Proof of Lemma 2

*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 1 (a), $\langle\xi_{xuv}|\xi_{x'u'v'}\rangle = 0$. □

## C.3 Proof of Lemma 3

*Proof.*

$$\begin{aligned}
&2^{-n/2}\sum_{x,u,v}|\xi_{xuv}\rangle\otimes|\xi_{xuv}\rangle \\
&= 2^{-n/2}|C_2|^{-1}\sum_{x,u,v}\sum_{w_1,w_2\in C_2}(-1)^{v\cdot(w_1\oplus w_2)}|x\oplus w_1\oplus u\rangle\otimes|x\oplus w_2\oplus u\rangle \\
&= 2^{-n/2}|C_2|^{-1}\sum_{x,u,w_1,w_2}\underbrace{\sum_{v\in\{0,1\}^n/C_2^\perp}(-1)^{v\cdot(w_1\oplus w_2)}}_{\substack{=0 \text{ if } w_1\neq w_2,\ =|C_2| \text{ if } w_1=w_2 \\ \text{by Lemma 1 (b)}}}|x\oplus w_1\oplus u\rangle\otimes|x\oplus w_2\oplus u\rangle \\
&= 2^{-n/2}\sum_{x,u,w}|x\oplus w\oplus u\rangle\otimes|x\oplus w\oplus u\rangle \\
&= 2^{-n/2}\sum_{j\in\{0,1\}^n}|j\rangle\otimes|j\rangle \\
&= |\widetilde{0^n0^n}\rangle
\end{aligned}$$

□

## C.4 Proof of Lemma 4

*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 $\omega(f), \omega(e) \leqslant t$. In the following calculation, we will apply a number of polynomial-time 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 $\omega(f), \omega(e) \leqslant t$ 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 \big(2^{-k_2/2} \sum_{w \in C_2} (-1)^{v\cdot w} |x \oplus w \oplus u\rangle\big) \\
&= X^e \_ \big(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\big) \\
&= 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 \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 \_\, 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 \_\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)} \Big(2^{-n/2} \sum_z (-1)^{z\cdot(x\oplus w)} |z\rangle\Big) |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 1 (a) (using } w \in C_2, |C_2| = 2^{k_2}) \\
&\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_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' \_\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}
\end{aligned}
$$

$$\mapsto 2^{k_2/2-n/2} \sum_{z'\in C_2^\perp} (-1)^{f\cdot u\oplus(z'\oplus v)\cdot x} \Big(\sum_y 2^{-n/2}(-1)^{y\cdot z'}|y\rangle\Big)|H_2 f\rangle|H_1 e\rangle \text{ using } H^{\otimes n}$$

$$= 2^{k_2/2-n} \sum_y \sum_{z'\in C_2^\perp} (-1)^{z'\cdot(y\oplus x)}(-1)^{f\cdot u\oplus v\cdot x}|y\rangle|H_2 f\rangle|H_1 e\rangle$$

$$= 2^{k_2/2-n} \sum_{y'} \sum_{z'\in C_2^\perp} (-1)^{z'\cdot y'}(-1)^{f\cdot u\oplus v\cdot x}|y'\oplus x\rangle|H_2 f\rangle|H_1 e\rangle \qquad \text{with } y' := y\oplus x$$

$$= 2^{k_2/2-n} \sum_{y'\in C_2} 2^{n-k_2}(-1)^{f\cdot u\oplus v\cdot x}|y'\oplus x\rangle|H_2 f\rangle|H_1 e\rangle \qquad \text{by Lemma 1 (a) (using } |C_2^\perp| = 2^{n-k_2},$$
$$(C_2^\perp)^\perp = C_2)$$

$$\mapsto 2^{-k_2/2} \sum_{y'\in C_2} \_\, (-1)^{f\cdot u\oplus v\cdot x}|x\rangle|y'\oplus x\rangle|H_2 f\rangle|H_1 e\rangle \qquad \text{using } U_5 : |z\rangle \mapsto |z \bmod C_2\rangle|z\rangle$$

$$\mapsto 2^{-k_2/2} \sum_{y'\in C_2} (-1)^{f\cdot u\oplus v\cdot x}|x\rangle|y'\,\_\rangle|H_2 f\rangle|H_1 e\rangle \qquad \text{using } U_6 : |z_1\rangle|z_2\rangle \mapsto |z_1\rangle|z_2\oplus z_1\rangle$$

$$= (-1)^{v\cdot x}|x\rangle|\Psi\rangle \qquad \text{with } |\Psi\rangle := 2^{-k_2/2}(-1)^{f\cdot u} \sum_{y'\in C_2} |y'\rangle|H_2 f\rangle|H_1 e\rangle$$

$$\mapsto \_\,|x\rangle|\Psi\rangle \qquad \text{using } Z^v$$

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 $\omega(z\oplus z') \leqslant t$ 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 $\omega(e) \leqslant t$, 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 $\omega(e) \leqslant t$ as needed in the above calculation. $U_{ec2}$ is constructed analogously with respect to $C_2^\perp$ 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 $|x\oplus w\rangle \mapsto |x\oplus w\rangle|0^n\rangle \overset{(*)}{\mapsto} |x\oplus w\rangle|w\rangle \mapsto |x\rangle|w\rangle$ where $(*)$ uses a unitary $|z\rangle|z'\rangle \mapsto |z\rangle|z'\oplus(z \bmod C_2)\rangle$.)
- $Z^v := Z^{v_1}\otimes\cdots\otimes Z^{v_n}$ 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 $|0^n\rangle|0^{n-k_2}\rangle \overset{H^{\otimes n-k_2}}{\mapsto} \frac{1}{\sqrt{|C_2|}}\sum_{z\in\{0,1\}^{n-k_2}}|0^n\rangle|z\rangle \overset{(*)}{\mapsto} \frac{1}{\sqrt{|C_2|}}\sum_{z\in\{0,1\}^{n-k_2}}|Gz\rangle|z\rangle \overset{(**)}{\mapsto} \frac{1}{\sqrt{|C_2|}}\sum_{z\in\{0,1\}^{n-k_2}}|Gz\rangle|0^{n-k_2}\rangle$. 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 $U_{check} : |x\rangle|z\rangle \mapsto |\bot\rangle|0^n\rangle|x\rangle$ 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 $\mathrm{span}\{|\xi_{xuv}\rangle : x\in C_1/C_2\}$, there is a $|\Psi\rangle$ such that $U_{uv}^{dec}|\xi_{xuv}\rangle = |\perp\rangle\otimes|\Psi\rangle$.

This shows the existence of $U_{uv}^{dec}$. □

# 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: $B\in\{0,1\}^q$, $Q\in[q+n]_q$, $r\in\{0,1\}^q$, $x\in C_1/C_2$, $u\in\{0,1\}^n/C_1$, $v\in\{0,1\}^n/C_2^\perp$. 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 2).

Also recall the definition of $P_t^{EPR}$ (page 40). 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* $\mathrm{RTRE}_{hid}$*.)*
*(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)* $V_0 \leftarrow \mathrm{TRE}_0(B, Q, r, p)$.
*(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 $\mathrm{RTRE}_{hid}$ inlined), it suffices to show that $\left|\Pr[b' = 1 \wedge ok = 1 : Game\ 1(0)] - \Pr[b' = 1 \wedge ok = 1 : Game\ 1(1)]\right|$ 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)* $V_0 \leftarrow \mathrm{TRE}_0(B, Q, r, p)$.
*(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)** *For* $b \in \{0,1\}$ *we have*

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

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

$$\begin{aligned}
&\Pr[b' = 1 \wedge ok = 1 \mid (x, \hat{x}, m_0, m_1) = (\underline{x}, \underline{\hat{x}}, \underline{m}_0, \underline{m}_1) : Game\ 2(b)] \\
&\quad = \begin{cases} \Pr[b' = 1 \wedge ok = 1 \mid (x, m_0, m_1) = (\underline{x}, \underline{m}_0, \underline{m}_1) : Game\ 1(b)] & \text{if } \underline{m}_b \oplus \underline{x} = \underline{\hat{x}} \\ 0 & \text{if } \underline{m}_b \oplus \underline{x} \neq \underline{\hat{x}}. \end{cases} \qquad (10)
\end{aligned}$$

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

Thus

$$\begin{aligned}
&|C_1/C_2| \Pr[b' = 1 \wedge ok = 1 : Game\ 2(b)] \\
&= \sum_{\substack{\underline{x}, \underline{\hat{x}}, \\ \underline{m}_0, \underline{m}_1}} \frac{1}{|C_1/C_2|} \Pr[b' = 1 \wedge ok = 1 \mid (x, \hat{x}, m_0, m_1) = (\underline{x}, \underline{\hat{x}}, \underline{m}_0, \underline{m}_1) : Game\ 2(b)] \\
&\qquad \cdot \Pr[(m_0, m_1) = (\underline{m}_0, \underline{m}_1) : Game\ 2(b)] \\
&\overset{(10)}{=} \sum_{\underline{x}, \underline{m}_0, \underline{m}_1} \frac{1}{|C_1/C_2|} \Pr[b' = 1 \wedge ok = 1 \mid (x, m_0, m_1) = (\underline{x}, \underline{m}_0, \underline{m}_1) : Game\ 1(b)] \\
&\qquad \cdot \Pr[(m_0, m_1) = (\underline{m}_0, \underline{m}_1) : Game\ 1(b)] \\
&= \Pr[b' = 1 \wedge ok = 1 : Game\ 1(b)].
\end{aligned}$$

□

**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)* $V_0 \leftarrow \mathrm{TRE}_0(B, Q, r, p)$.
*(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*

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

*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:

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

Here $(*)$ uses the definition of $|\xi_{xuv}\rangle$, and $(**)$ uses Lemma 1 (b) with $C := C_2$ and $x := w_1 \oplus w_2$.
Thus $\rho_1^{xu} = \rho_2^{xu}$ and the lemma follows. □

**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 51.)*
*(k) Measure $Y$ using $M_X^{uv}$, outcome $x$.*
*(l) Measure $Y$ using $M_R$, outcome $r$.*
*(m)* $V_0 \leftarrow \mathrm{TRE}_0(B, Q, r, p)$.
*(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* $\Pr[b' = 1 \wedge ok = 1 : \mathit{Game}\ 3(b)] = \Pr[b' = 1 \wedge ok = 1 : \mathit{Game}\ 4(b)]$.

*Proof.* To show this lemma, it is sufficient to show two things: When initializing $XY$ with $|\widetilde{0^{q+n}0^{q+n}}\rangle$, 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 $C_1/C_2 \cup \{\bot\}$). 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 $|\Psi_{xruv}\rangle := (I_{q+n} \otimes P_r P_x^{uv} P_{uv}(H^B \otimes I_n)U_Q)|\widetilde{0^{q+n}0^{q+n}}\rangle$. (Reminder: $P_r, P_{uv}, P_x^{uv}$ are defined on page 51.) Then the probability of getting outcomes $x, r, u, v$ is $\||\Psi_{xruv}\rangle\|^2$, and the post-measurement-state is $|\Psi_{xruv}\rangle / \||\Psi_{xruv}\rangle\|$.

We have

$$|\Psi_{xruv}\rangle = (I_{q+n} \otimes P_r P_x^{uv} P_{uv})(I_{q+n} \otimes (H^B \otimes I_n)U_Q)|\widetilde{0^{q+n}0^{q+n}}\rangle \tag{11}$$

$$\overset{(*)}{=} (I_{q+n} \otimes P_r P_x^{uv} P_{uv})(U_Q^\dagger(H^B \otimes I_n) \otimes I_{q+n})|\widetilde{0^{q+n}0^{q+n}}\rangle \tag{12}$$

$$= (U_Q^\dagger(H^B \otimes I_n) \otimes I_{q+n})(I_{q+n} \otimes P_r P_x^{uv} P_{uv})|\widetilde{0^{q+n}0^{q+n}}\rangle \tag{13}$$

$$\overset{(**)}{=} (U_Q^\dagger(H^B \otimes I_n) \otimes I_{q+n})(P_r P_x^{uv} P_{uv} \otimes I_{q+n})|\widetilde{0^{q+n}0^{q+n}}\rangle \tag{14}$$

$$\overset{(***)}{=} (U_Q^\dagger(H^B \otimes I_n) \otimes I_{q+n})(P_r P_x^{uv} P_{uv} \otimes I_{q+n})2^{-q/2-n/2} \sum_{r,x,u,v} |r\rangle|\xi_{xuv}\rangle|r\rangle|\xi_{xuv}\rangle \tag{15}$$

$$\overset{(****)}{=} 2^{-q/2-n/2} U_Q^\dagger(H^B \otimes I_n)|r\rangle|\xi_{xuv}\rangle \otimes |r\rangle|\xi_{xuv}\rangle. \tag{16}$$

Here $(*)$ uses Lemma 8 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 8 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 3.

And $(****)$ uses that the $|r\rangle|\xi_{xuv}\rangle$ are orthogonal (Lemma 2), and that thus $P_r P_x^{uv} P_{uv}$ is a projector onto $|r\rangle|\xi_{xuv}\rangle$.

Hence the probability $\||\Psi_{xruv}\rangle\|^2$ 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. □

**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) $B \xleftarrow{\$} \{0,1\}^q$. $Q \xleftarrow{\$} [q+n]_q$. $p \xleftarrow{\$} C_1/C_2$.*
*(d) Initialize $XY$ as $|\widetilde{0^{q+n}0^{q+n}}\rangle$.*
*(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) $V_0 \leftarrow \mathrm{TRE}_0(B, Q, r, p)$.*
*(j) $\hat{x} \xleftarrow{\$} C_1/C_2$. 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)** $\Pr[b' = 1 \wedge ok = 1 : \mathit{Game}\ 4(b)] = \Pr[b' = 1 \wedge ok = 1 : \mathit{Game}\ 5(b)]$ *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 $Y$. □

**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)* $B \xleftarrow{\$} \{0,1\}^q$. $Q \xleftarrow{\$} [q+n]_q$. $p \xleftarrow{\$} C_1/C_2$.
*(d) Initialize $XY$ as* $|0^{\widetilde{q+n}}0^{q+n}\rangle$.
*(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)* $V_0 \leftarrow \mathrm{TRE}_0(B, Q, r, p)$.
*(i)* $\hat{x} \xleftarrow{\$} C_1/C_2$. *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 isEPR.*
*(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* $\varepsilon := \Pr[ok = 1 \wedge isEPR = 0 : \mathit{Game}\ 6]$. *Then we have* $\left|\Pr[b' = 1 \wedge ok = 1 : \mathit{Game}\ 5(0)] - \Pr[b' = 1 \wedge ok = 1 : \mathit{Game}\ 5(1)]\right| \leqslant \sqrt{\varepsilon}$.

*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 $b \in \{0,1\}$:

$$\begin{aligned}&\Pr[b' = 1 \wedge ok = 1 : \mathit{Game}\ 5(b)]\\ &= \sum_{\hat{x},u,v} \Pr_{\hat{x}uv} \cdot \Pr[b' = 1 : \text{start with } \rho_{\hat{x}uv}, x \leftarrow \text{measure } Y \text{ with } M_X^{uv}, b' \leftarrow B(x \oplus m_b \oplus \hat{x})]\end{aligned} \tag{17}$$

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 $\mathrm{span}\{|r\rangle|x\rangle|\Psi\rangle : r \in \{0,1\}^q, |\Psi\rangle \text{ arbitrary}\}$, and let $M_X$ be the corresponding measurement $M_X = \{P_x\}_{x \in C_1/C_2 \cup \{\bot\}}$. (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 $|\Psi\rangle$):

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

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 $x \in C_1/C_2 \cup \{\bot\}$. 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 (17):

$$\begin{aligned}&\Pr[b' = 1 \wedge ok = 1 : Game\ 5(b)]\\ &= \sum_{\hat{x},u,v} \Pr_{\hat{x}uv} \underbrace{\Pr[b' = 1 : \text{start with } \rho_{\hat{x}uv}^*, x \leftarrow \text{measure } Y \text{ with } M_X, b' \leftarrow B(x \oplus m_b \oplus \hat{x})]}_{=:\mathrm{Succ}_{\hat{x}uv}^b} \qquad (18)\end{aligned}$$

Furthermore, we have

$$\varepsilon = \Pr[ok = 1 \wedge isEPR = 0 : Game\ 6] = \sum_{\hat{x},u,v} \Pr_{\hat{x}uv} \underbrace{\mathrm{tr}((1 - P_{C_1/C_2}^{EPR}) \otimes I)\rho_{\hat{x}uv}^*}_{=:\varepsilon_{\hat{x}uv}}. \qquad (19)$$

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

Since $\mathrm{tr}(P_{C_1/C_2}^{EPR} \otimes I)\rho_{\hat{x}uv}^* = 1 - \varepsilon_{\hat{x}uv}$ by definition of $\varepsilon_{\hat{x}uv}$, Lemma 10 implies existence of a state $\rho_{\hat{x}uv}^{ideal}$ such that

$$\mathrm{TD}(\rho_{\hat{x}uv}^*, \rho_{\hat{x}uv}^{ideal}) \leqslant \sqrt{\varepsilon_{\hat{x}uv}} \qquad (20)$$

and

$$\rho_{\hat{x}uv}^{ideal} \text{ is a mixture over } \mathrm{im}(P_{C_1/C_2}^{EPR} \otimes I) \qquad (21)$$

Equation (21) implies that $\rho_{\hat{x}uv}^{ideal}$ is of the form $\left(\sum_x \frac{1}{|C_1/C_2|}|x\rangle\langle x| \otimes |x\rangle\langle x|\right) \otimes \rho_{rest}$. 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 $\rho_{rest}$. 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 (20), it follows that

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

Or using abbreviations from above: $\left|\mathrm{Succ}_{\hat{x}uv}^0 - \mathrm{Succ}_{\hat{x}uv}^1\right| \leqslant \sqrt{\varepsilon_{\hat{x}uv}}$.

Thus

$$\begin{aligned}&\big|\Pr[b' = 1 \wedge ok = 1 : Game\ 5(0)] - \Pr[b' = 1 \wedge ok = 1 : Game\ 5(1)]\big|\\ &\overset{(18)}{\leqslant} \sum_{\hat{x},u,v} \Pr_{\hat{x}uv} |\mathrm{Succ}_{\hat{x}uv}^0 - \mathrm{Succ}_{\hat{x}uv}^1| \leqslant \sum_{\hat{x},u,v} \Pr_{\hat{x}uv} \sqrt{\varepsilon_{\hat{x}uv}} \overset{(*)}{\leqslant} \sqrt{\sum_{\hat{x},u,v} \Pr_{\hat{x}uv} \varepsilon_{\hat{x}uv}} \overset{(19)}{=} \sqrt{\varepsilon}.\end{aligned}$$

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

**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* $|0^{\widetilde{q+n}}0^{q+n}\rangle$.
*(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)* $\hat{B} \xleftarrow{\$} \{0,1\}^q$. $\hat{Q} \xleftarrow{\$} [q+n]_q$. $\hat{r} \xleftarrow{\$} \{0,1\}^q$. $V_0 \leftarrow \mathrm{TRE}_0(\hat{B}, \hat{Q}, \hat{r}, p)$.
*(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* $P^{EPR}_{C_1/C_2}$, *outcome* *isEPR*.

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

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

*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 $\Pr[ok = 1 : G \wedge isEPR = 0 : G] = \Pr[ok = 1 \wedge isEPR = 0 : \textit{Game } 6]$ and $\Pr[ok = 1 \wedge isEPR = 0 : G'] = \Pr[ok = 1 \wedge isEPR = 0 : \textit{Game } 7]$ 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 $\sum_{x \in C_1/C_2} |x\rangle|x\rangle$ $(P^{EPR}_{C_1/C_2})$, 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 $\delta_T^{hid}$ and our additivity assumptions on timing models, page 7).

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

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

**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* $|0^{\widetilde{q+n}}0^{q+n}\rangle$.
*(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)* $\hat{B} \xleftarrow{\$} \{0,1\}^q$. $\hat{Q} \xleftarrow{\$} [q+n]_q$. $\hat{r} \xleftarrow{\$} \{0,1\}^q$. $V_0 \leftarrow \mathrm{TRE}_0(\hat{B}, \hat{Q}, \hat{r}, p)$.
*(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)** $\Pr[ok = 1 \text{ and } isEPR = 0 : Game\ 7] = \Pr[ok = 1 \text{ and } isEPR = 0 : Game\ 8]$.

*Proof.* The difference between the two games 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 $M_R, M_{UV}$. □

**Game 9 (Measure $t$-error state)**
(a) $(m_0, m_1) \leftarrow A_0()$.
(b) $p \xleftarrow{\$} C_1/C_2$.
(c) *Initialize $XY$ as* $|0^{\widetilde{q+n}0^{q+n}}\rangle$.
(d) $\hat{B} \xleftarrow{\$} \{0,1\}^q$. $\hat{Q} \xleftarrow{\$} [q+n]_q$. $\hat{r} \xleftarrow{\$} \{0,1\}^q$. $V_0 \leftarrow \mathrm{TRE}_0(\hat{B}, \hat{Q}, \hat{r}, p)$.
(e) $\hat{x} \xleftarrow{\$} C_1/C_2$. *Run* $A_1(X, V_0, u, \hat{x} \oplus p)$.
(f) $B \xleftarrow{\$} \{0,1\}^q$. $Q \xleftarrow{\$} [q+n]_q$.
(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 isEPR.*~~
(m) *Measure $X'Y'$ using $P_t^{EPR}$, outcome isEPR.*

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

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

*we have $pr_1 \leqslant pr_2$. (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 if $X, Y$ 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 $\rho$, 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 $\mathrm{tr}_H(U|\psi\rangle|0^m\rangle)(\langle\psi|\langle 0^m|U^\dagger)$ where $H$ refers to some auxiliary system of dimension $m$.

We then have that

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

$P_1$ and $P_2$ are orthogonal projectors, thus to show $pr_1 \leqslant pr_2$, it is sufficient to show $\operatorname{im} P_1 \subseteq \operatorname{im} P_2$. By definition of $P_t^{EPR}$ we have $\operatorname{im} P_t^{EPR} = \operatorname{span}\{|\widetilde{fe}\rangle : \omega(f), \omega(e) \leqslant t\}$ (where $f, e$ are $n$-bit strings). We thus have that $\operatorname{im} P_1 = \operatorname{span}\{|\widetilde{fe}\rangle|0^m\rangle : \omega(f), \omega(e) \leqslant t\}$. Thus to show $\operatorname{im} P_1 \subseteq \operatorname{im} P_2$, it is sufficient to show that $|\widetilde{fe}\rangle|0^m\rangle \in \operatorname{im} P_2$ for $\omega(f), \omega(e) \leqslant t$. 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 $|\widetilde{fe}\rangle = (Z^f X^e \otimes I_n)|\widetilde{0^n 0^n}\rangle$.

And by Lemma 3, we have that $2^{-n/2} \sum_{x,u,v} |\xi_{xuv}\rangle \otimes |\xi_{xuv}\rangle = |\widetilde{0^n 0^n}\rangle$. Hence $|\widetilde{fe}\rangle = 2^{-n/2} \sum_{x,u,v} Z^f X^e |\xi_{xuv}\rangle \otimes |\xi_{xuv}\rangle$. Since all $|\xi_{xuv}\rangle$ are orthogonal (Lemma 2), we have for any $u, v$ that the unnormalized post-measurement state after measuring $|\widetilde{fe}\rangle$ using $I_n \otimes M_{UV}$ with outcome $(u, v)$ is $|\Psi_{uv}\rangle := (I_n \otimes P_{uv})|\widetilde{fe}\rangle = 2^{-n/2} \sum_x Z^f X^e |\xi_{xuv}\rangle \otimes |\xi_{xuv}\rangle$.

Since $f, e$ have Hamming weight $\leqslant t$, 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

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

Let $\rho'$ 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 $|\widetilde{fe}\rangle\langle\widetilde{fe}|$. Then $\rho' = \sum_{uv} |\Psi'_{uv}\rangle\langle\Psi'_{uv}|$. Thus

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

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

We have thus shown that $\operatorname{im} P_1 \subseteq \operatorname{im} P_2$, and as discussed above, this implies $pr_1 \leqslant pr_2$. □

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

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

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

Here $(*)$ uses that $pr_1 \leqslant pr_2$ 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 $\rho$ is also the state in Game 9 right before the measurement of $u, v$, conditioned on $ok = 1$. □

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

*Consider the following game: Pick $B \xleftarrow{\$} \{0,1\}^q, Q \xleftarrow{\$} [q+n]_q$. 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* $\Pr[ok = 1 \wedge isEPR = 0] \leqslant 3\sqrt{q}\,(1 - \frac{q}{2(q+n)})^{t+1}$.

*Proof.* We first consider the case that $\rho = |\widetilde{fe}\rangle\langle\widetilde{fe}|$ 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 $Q = \{Q_1, \ldots, Q_q\}$ and $B = B_1 \ldots B_n$, 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 $X, Y$, if 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 7, 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

$$\Pr[ok = 1 \wedge isEPR = 0] \leqslant \Pr[ok = 1] \leqslant P(x) \overset{(*)}{\leqslant} 3\sqrt{q}\,(1 - \tfrac{q}{2(q+n)})^{t+1} =: \gamma \quad \text{if } \rho = |\widetilde{fe}\rangle\langle\widetilde{fe}| \text{ with } \omega(f) > t \text{ or } \omega(e) > t. \tag{22}$$

Here $(*)$ uses Lemma 7.

Now we consider the case that $\rho = |\widetilde{fe}\rangle\langle\widetilde{fe}|$ with $\omega(f), \omega(e) \leqslant t$. 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 $\omega(e') \leqslant \omega(e) \leqslant t$ and $\omega(f') \leqslant \omega(f) \leqslant t$. Thus the measurement $P_t^{EPR}$ will succeed with probability 1, hence

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

Together with (22), we have

$$\Pr[ok = 1 \wedge isEPR = 0] \leqslant \gamma \qquad \text{if } \rho = |\widetilde{fe}\rangle\langle\widetilde{fe}| \text{ for some } f, e \in \{0,1\}^{q+n} \tag{23}$$

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

$$\Pr[ok = 1 \wedge isEPR = 0] = \sum \alpha_i \Pr[ok = 1 \wedge isEPR = 0 : \text{using } \rho := |\widetilde{e_i f_i}\rangle\langle\widetilde{e_i f_i}|] \overset{(23)}{\leqslant} \sum \alpha_i \gamma = \gamma \quad \text{if } \rho = \sum_i \alpha_i |\widetilde{e_i f_i}\rangle\langle\widetilde{e_i f_i}| \tag{24}$$

Now consider the general case of an arbitrary density operator $\rho$. 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 $P^1_{eq} := |00\rangle\langle 00| + |11\rangle\langle 11|$ and identities. Furthermore, one can check that $P^1_{eq} = |\beta_{00}\rangle\langle\beta_{00}| + |\beta_{10}\rangle\langle\beta_{10}|$. 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 $\rho^*$ be the state we get when measuring $\rho$ using $M_{Bell}$ and discarding the outcome. Then $\rho^* = \sum_i \alpha_i |\widetilde{f_i e_i}\rangle\langle\widetilde{f_i e_i}|$ for some $\alpha_i, f_i, e_i$ with $\alpha_i \geqslant 0$, $\sum \alpha_i = 1$.

We then have

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

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 (24) and the fact that $\rho^*$ is of the form $\sum_i \alpha_i |\widetilde{e_i f_i}\rangle\langle\widetilde{e_i f_i}|$.

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. □

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

*Proof.* To show this claim, let $\rho$ 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

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

We can now finally prove the security of $\mathrm{RTRE}_{hid}$:

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

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

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

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

By Lemmas 21, 22, and 23 it follows that

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

By Lemma 24 we have

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

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

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

By Lemmas 26 and 28,

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

and by Lemma 30, we have

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

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

$$\mu \leqslant \sqrt{\underbrace{2^{2(k_1-k_2)} \cdot 3\sqrt{q}\,(1 - \tfrac{q}{2(q+n)})^{t+1}}_{=:\mu_2} + 2^{2(k_1-k_2)}\mu_1}. \tag{25}$$

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

To show that $\mu_2$ is negligible, let $\ell := k_1 - k_2$ and observe that

$$\begin{aligned}\mu_2/(3\sqrt{q}) &\leqslant 2^{2\ell}\,(1 - \tfrac{q}{2(q+n)})^t = 2^{2\ell}\Big(\underbrace{(1 - \tfrac{q}{2(q+n)})^{2(q+n)/q}}_{\leqslant 1/e \quad (*)}\Big)^{tq/(2(q+n))} \\ &\leqslant 2^{2\ell}e^{-tq/(2(q+n))} = e^{-\frac{1}{2}(tq/(q+n) - 4\ell\ln 2)}\end{aligned}$$

Here $(*)$ uses the fact that $(1-1/x)^x$ is increasing for $x \geqslant 1$ 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, $\mu_2$ is negligible.

Thus both summands below the square root in (25) are negligible, hence $\mu$ is negligible. Thus $\mathrm{RTRE}_{hid}$ is $(T - \delta_T^{hid})$-revocably hiding.

Note that (25) also tells us the concrete security of $\mathrm{RTRE}_{hid}$. Namely, when $\mu_1$ is the advantage of an adversary against $\mathrm{TRE}_0$ (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 (25) bounds the advantage of $(A_0, A_1, A_2)$ against $\mathrm{RTRE}_{hid}$. □

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

**Theorem 12 ($\mathrm{RTRE}_{hid}$ is hiding)** *The protocol $\mathrm{RTRE}_{hid}$ from Definition 9 is $T$-hiding.*

The proof is completely analogous to that of Theorem 11.

# E Full proofs: one-way to hiding

*Proof of Theorem 5.* 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 $(\{0,1\}^n \to \{0,1\}^m)$ as *Fun*. By definition of revocably hiding (Definition 5) and of TRE$'$, we have to show that $\mu$ is negligible where

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

with the following game:

**Game 1 (Original game)**
*(a) In this game, $b \in \{0,1\}$ is a parameter of the game.*
*(b) $H \xleftarrow{\$} \mathit{Fun}$.*
*(c) $k \xleftarrow{\$} \{0,1\}^n$.*
*(d) $(m_0, m_1) \leftarrow A_0^H()$.*
*(e) $V' \leftarrow \mathrm{TRE}(k)$.*
*(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

$$\begin{aligned}\varepsilon_b := \big|&\Pr[b'' = 1 : H \xleftarrow{\$} \mathit{Fun}, k \xleftarrow{\$} \{0,1\}^n, b'' \leftarrow A(b, k, H(k))] \\ &- \Pr[b'' = 1 : H \xleftarrow{\$} \mathit{Fun}, k \xleftarrow{\$} \{0,1\}^n, y \xleftarrow{\$} \{0,1\}^m, b'' \leftarrow A(b, k, y)]\big|.\end{aligned}$$

We then have

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

where $\overset{\varepsilon_0}{\approx}$ denotes a difference of $\varepsilon_0$ ($\overset{\varepsilon_1}{\approx}$ 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 $\mu \leqslant \varepsilon_0 + \varepsilon_1$.

We will now show that $\varepsilon_b$ 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 $i \xleftarrow{\$} \{1,\ldots,q_0+q_1+q_2\}$ and $h \xleftarrow{\$} \{0,1\}^m$, and then runs $A^H(b,k,h)$ until the $i$-th query and measure the argument $k'$ of that query (cf. Lemma 5). $B$ then returns $k'$ (or $\bot \notin \{0,1\}^n$ if there was no $i$-th query).

Then by Lemma 5,

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

Consider the following games:

**Game 2 (Measure in phase 0)**
*(a)* $H \xleftarrow{\$} Fun$.
*(b)* $k \xleftarrow{\$} \{0,1\}^n$.
*(c)* $i \xleftarrow{\$} \{1,\ldots,q_0\}$.
*(d)* $h \xleftarrow{\$} \{0,1\}^m$.
*(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)* $H \xleftarrow{\$} Fun$.
*(b)* $k \xleftarrow{\$} \{0,1\}^n$.
*(c)* $i \xleftarrow{\$} \{1,\ldots,q_1\}$.
*(d)* $h \xleftarrow{\$} \{0,1\}^m$.
*(e)* $(m_0,m_1) \leftarrow A_0^H()$.
*(f)* $V' \leftarrow \mathrm{TRE}(k)$.
*(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)* $H \xleftarrow{\$} Fun$.
*(b)* $k \xleftarrow{\$} \{0,1\}^n$.
*(c)* $i \xleftarrow{\$} \{1,\ldots,q_2\}$.
*(d)* $h \xleftarrow{\$} \{0,1\}^m$.
*(e)* $(m_0,m_1) \leftarrow A_0^H()$.
*(f)* $V' \leftarrow \mathrm{TRE}(k)$.
*(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* $k' := \bot$.

We have that $p_0 := \Pr[k = k' : Game\ 2]$ is negligible because $k$ is never used. We have that $p_1 := \Pr[k = k' : Game\ 3]$ 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 $\Pr[k = k' \wedge ok = 1 : Game\ 4]$ is negligible because TRE is $T$-revocably one-way and $A_1^H$ runs in time $T$. Since $k' = \bot \neq k$ when $ok \neq 1$, we have $p_2 := \Pr[k = k' : Game\ 4] = \Pr[k = k' \wedge ok = 1 : Game\ 4]$.

Furthermore, by construction of $B$, we have:

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

Thus $\varepsilon_b \overset{(26)}{\leqslant} 2(q_0+q_1+q_2)\sqrt{\sum_i \frac{q_i}{q_0+q_1+q_2} p_i}$ Since $p_1, p_2, p_3$ are negligible and $q_0, q_1, q_2$ polynomially bounded, $\varepsilon_b$ is negligible, and hence $\mu \leqslant \varepsilon_0 + \varepsilon_1$ 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 $p_0, p_1, p_2$ loose 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 $q_0 = 0$. □

# F Full proofs: precomputation

*Proof of Lemma 6.* We describe a sequence of games, the first being identical to Game A from Lemma 6, and the last being identical to Game B from Lemma 6.

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

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

**Game 2 (Changing $A$'s oracle)**
$a \xleftarrow{\$} \{0,1\}^\ell$, $H \xleftarrow{\$} (\{0,1\}^{\ell+n} \to \{0,1\}^m)$, $G_1 \xleftarrow{\$} (\{0,1\}^n \to \{0,1\}^m)$, $A^{H \wr_a G_1}()$, $b' \leftarrow B^H(a)$.

We claim that

$$\left|\Pr[b' = 1 : Game\ 1] - \Pr[b' = 1 : Game\ 2]\right| \leqslant q 2^{-\ell/2+1} \tag{27}$$

To show (27) it is sufficient to show that for fixed $H, G_1$, we have that $\mathrm{TD}(\rho_1, \rho_2) \leqslant q 2^{-\ell/2+1}$ where $\rho_1$ is the state after executing $a \xleftarrow{\$} \{0,1\}^\ell, A^H()$ and $\rho_2$ is the state after executing $a \xleftarrow{\$} \{0,1\}^\ell, A^{H \wr_a G_1}()$. ($\rho_1, \rho_2$ 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 $A^{H \wr_a G_1}$ is $|\Psi_q^a\rangle := (UO_{H \wr_a G_1})^q|\Psi_0\rangle$ with the same $|\Psi_0\rangle$ and the same $U$. With this notation,

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

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

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

We claim that $D_i \leqslant 4i^2$ 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 $D_{i+1} \leqslant 4(i+1)^2$ assuming $D_i \leqslant 4i^2$.

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 $O_H = O_{H^{l_a}G_1} + O_H P_a - O_{G_1} P_a$ where $O_{G_1}|(\tilde{a}\|x), v\rangle := |(\tilde{a}\|x), v \oplus G_1(x)\rangle$. Then

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

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

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

Thus

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

This finishes the proof by induction that $D_i \leqslant 4i^2$.[33]

We are now ready to bound $\mathrm{TD}(\rho_1, \rho_2)$. 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 $\mathrm{TD}(|\Psi_q\rangle, |\Psi_q^a\rangle) = \sqrt{1 - F_a^2}$. And

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

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

$$\begin{aligned}
\mathrm{TD}(\rho_1, \rho_2) &= \mathrm{TD}\Big(\sum_a 2^{-\ell}|a\rangle\langle a| \otimes |\Psi_q\rangle\langle\Psi_q|, \sum_a 2^{-\ell}|a\rangle\langle a| \otimes |\Psi_q^a\rangle\langle\Psi_q^a|\Big) \\
&= \sum_a 2^{-\ell}\mathrm{TD}(|\Psi_q\rangle, |\Psi_q^a\rangle) = \sum_a 2^{-\ell}\sqrt{1 - F_a^2} \\
&\leqslant \sum_a 2^{-\ell}\sqrt{1 - (1 - \tfrac{1}{2}\Delta_a)^2} = \sum_a 2^{-\ell}\sqrt{\Delta_a - \tfrac{1}{4}\Delta_a^2} \\
&\leqslant \sum_a 2^{-\ell}\sqrt{\Delta_a} \overset{(*)}{\leqslant} \sqrt{\sum_a 2^{-\ell}\Delta_a} \\
&= \sqrt{2^{-\ell} D_q} \leqslant \sqrt{2^{-\ell} 4q^2} = q2^{-\ell/2+1}.
\end{aligned}$$

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

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

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

**Game 3 (Decomposing $H$)**
$a \xleftarrow{\$} \{0,1\}^\ell$, $H_1 \xleftarrow{\$} (\{0,1\}^{\ell+n} \to \{0,1\}^m)$, $G \xleftarrow{\$} (\{0,1\}^n \to \{0,1\}^m)$, $H := H_1 \wr_a G$,
$G_1 \xleftarrow{\$} (\{0,1\}^n \to \{0,1\}^m)$, $A^{H \wr_a G_1}()$, $b' \leftarrow B^H(a)$.

Since $H_1 \wr_a G$ 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 $\Pr[b' = 1 : \mathit{Game}\ 2] = \Pr[b' = 1 : \mathit{Game}\ 3]$.

**Game 4 (Substituting equal oracles)**
$a \xleftarrow{\$} \{0,1\}^\ell$, $H_1 \xleftarrow{\$} (\{0,1\}^{\ell+n} \to \{0,1\}^m)$, $G \xleftarrow{\$} (\{0,1\}^n \to \{0,1\}^m)$, ~~$H := H_1 \wr_a G$,~~
$G_1 \xleftarrow{\$} (\{0,1\}^n \to \{0,1\}^m)$, $A^{H_1 \wr_a G_1}()$, $b' \leftarrow B^{(H_1 \wr_a G_1) \wr_a G}(a)$.

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

**Game 5 (Introducing $\tilde{B}$)**
$a \xleftarrow{\$} \{0,1\}^\ell$, $H_1 \xleftarrow{\$} (\{0,1\}^{\ell+n} \to \{0,1\}^m)$, $G \xleftarrow{\$} (\{0,1\}^n \to \{0,1\}^m)$,
$G_1 \xleftarrow{\$} (\{0,1\}^n \to \{0,1\}^m)$, $H := H_1 \wr_a G_1$, $A^H()$, $b' \leftarrow \tilde{B}^{H,G}(a)$.

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

**Game 6 (Game B)**
$a \xleftarrow{\$} \{0,1\}^\ell$, ~~$H_1 \xleftarrow{\$} (\{0,1\}^{\ell+n} \to \{0,1\}^m)$,~~ $G \xleftarrow{\$} (\{0,1\}^n \to \{0,1\}^m)$,
~~$G_1 \xleftarrow{\$} (\{0,1\}^n \to \{0,1\}^m)$,~~ $H \xleftarrow{\$} (\{0,1\}^{\ell+n} \to \{0,1\}^m)$, $A^H()$, $b' \leftarrow \tilde{B}^{H,G}(a)$.

Since $H_1 \wr_a G_1$ 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 $H := H_1 \wr_a G_1$ by a uniformly chosen $H$ and have $\Pr[b' = 1 : \mathit{Game}\ 5] = \Pr[b' = 1 : \mathit{Game}\ 6]$.

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

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

# G Full proofs: iterated hashing

*Proof of Theorem 7.* 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 $\mathrm{TRE}_{ih}$ is $T$-one-way without offline-queries it is therefore sufficient to show the following: For any $T$-time algorithm $A$, $A^H()$ 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, $O_H : |a, (k_1, \dots, k_q), (v_1, \dots, v_q)\rangle \to |a, (k_1, \dots, k_q), (v_1 \oplus H(k_1), \dots, v_q \oplus H(k_q))\rangle$ 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 $H : \{0,1\}^n \to \{0,1\}^n$, and a tuple $\mathbf{x} = (x_1, \ldots, x_{T+1})$, we define $H_{\mathbf{x}}$ to be the function resulting from $H$ by setting $H(x_{i-1}) := x_i$ for $i = 1, \ldots, s$ 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 $0 \leqslant j < s$) or $s = T + 1$ if no duplicates occur in $0, x_1, \ldots, x_{T+1}$.

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 $(x_1, \ldots, x_i) = (x'_1, \ldots, x'_i)$ 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 $x_{i+1}, \ldots, x_{T+1}$.

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 $\sum_{H,\mathbf{x}} \frac{1}{N} \mathrm{TD}(|\Psi^{H,\mathbf{x}}\rangle, |\Phi^{H,\mathbf{x}}\rangle)$. 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 $0 \leqslant i < j \leqslant T + 1$. Fix a measurement $M$. Fix an $i$-good family $\{|\Psi^{H,\mathbf{x}}\rangle\}_{H,\mathbf{x}}$. Then $\sum_{H,\mathbf{x}} \frac{1}{N} \Pr[$measuring $|\Psi^{H,\mathbf{x}}\rangle$ using $M$ 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 $(x_1, \ldots, x_{j-1}, x_j \oplus p, x_{j+1}, \ldots, x_T)$. Since $\mathbf{x} \oplus p$ ranges over the same tuples as $\mathbf{x}$, we have for any $p \in \{0,1\}^n$:

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

and thus

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

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 $i \leqslant T$, 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 $H : \{0,1\}^n \to \{0,1\}^n$ and $\mathbf{x} \in (\{0,1\}^n)^{T+1}$ and also some $y \in \{0,1\}^n$. Let $\mathbf{x}_y := (x_1, \ldots, x_{i+1}, y, \ldots, y)$.

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

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

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

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 11 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 $H : \{0,1\}^n \to \{0,1\}^n$ and $\mathbf{x} \in (\{0,1\}^n)^{T+1}$ and $y \in \{0,1\}^n$,

$$\mathrm{TD}\big(O_{H_{\mathbf{x}}}|\Psi^{H\mathbf{x}}\rangle, O_{H_{\mathbf{x}_y}}|\Psi^{H\mathbf{x}_y}\rangle\big) \leqslant 2\|O_{H_{\mathbf{x}}} P^*_{x_{i+1}\dots x_{T+1}y}|\Psi^{H\mathbf{x}}\rangle\|. \tag{29}$$

We abbreviate "given state $|\Psi\rangle$, measuring $K_1, \dots, K_q$ in the computational basis yields $(z_1, \dots, z_q)$ with $\{z_1, \dots, z_q\} \cap \{a, b, c, d, \dots\} \neq \varnothing$" 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 $\delta_y$ 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

$$\begin{aligned}
\sum_{y\in\{0,1\}^n} 2^{-n}\delta_y &= \sum_y 2^{-n} \sum_{H,\mathbf{x}} \frac{1}{N} \mathrm{TD}(O_{H_{\mathbf{x}}}|\Psi^{H\mathbf{x}}\rangle, O_{H_{\mathbf{x}_y}}|\Psi^{H\mathbf{x}_y}\rangle) \\
&\overset{(29)}{\leqslant} \sum_{H,\mathbf{x},y} \frac{1}{N2^n} 2\|O_{H_{\mathbf{x}}} P^*_{x_{i+1}\dots x_{T+1}y}|\Psi^{H\mathbf{x}}\rangle\| = \sum_{H,\mathbf{x},y} \frac{1}{N2^n} 2\|P^*_{x_{i+1}\dots x_{T+1}y}|\Psi^{H\mathbf{x}}\rangle\| \\
&= \sum_{H,\mathbf{x},y} \frac{1}{N2^n} 2\sqrt{\Pr[|\Psi^{H,\mathbf{x}}\rangle \mapsto x_{i+1}\dots x_{T+1}y]} \\
&\overset{(*)}{\leqslant} 2\sqrt{\sum_{H,\mathbf{x},y} \frac{1}{N2^n} \Pr[|\Psi^{H,\mathbf{x}}\rangle \mapsto x_{i+1}\dots x_{T+1}y]} \\
&\leqslant 2\sqrt{\sum_{i=1}^{q} \underbrace{\sum_{H,\mathbf{x},y} \frac{1}{N2^n}}_{=1} \sum_{j=i+1}^{T+1} \underbrace{\Pr[|\Psi^{H,\mathbf{x}}\rangle \mapsto_i x_j]}_{=2^{-n}\ (\text{Claim 1})} + \sum_{i=1}^{q} \underbrace{\sum_{H,\mathbf{x}} \frac{1}{N2^n}}_{=2^{-n}} \underbrace{\sum_y \Pr[|\Psi^{H,\mathbf{x}}\rangle \mapsto_i y]}_{=1}} \\
&= 2\sqrt{q(T-i+1)2^{-n} + q2^{-n}} = 2^{-n/2+1}\sqrt{q(T-i+2)} =: \varepsilon.
\end{aligned}$$

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

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

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 $\delta_{y_0} \leqslant \varepsilon = 2^{-n/2+1}\sqrt{q(T-i+2)}$. 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:

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

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

$$\begin{aligned}&\Pr[x' = x_{T+1} : H \xleftarrow{\$} (\{0,1\}^n \to \{0,1\}^n), x_1, \ldots, x_{T+1} \xleftarrow{\$} \{0,1\}^n, x' \leftarrow A^{H_\mathbf{x}}()]\\ &\qquad\leqslant 2^{-n/2}\sqrt{2q}(T+2)^{3/2} + 2^{-n}.\end{aligned}$$

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

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

Notice that for $H$ and $x_1, \ldots, x_n$ 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

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

The latter probability is the probability of $A$ breaking the timed-release encryption $\mathrm{TRE}_{ih}$. 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), $\mathrm{TRE}_{ih}$ is $T$-one-way.

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

# Symbol index


| | | |
|---|---|---|
| $sigkeygen()$ | Key generation for signature scheme | 32 |
| $sign(sk, m)$ | Signing algorithm (signature scheme) | 32 |
| $verify(pk, \sigma, m)$ | Verification algorithm (signature scheme) | 32 |
| $\mathrm{RTRE}_{sk,t_0,id}$ | Variant of revocable timed-release encryption $\mathrm{RTRE}_{hid}$, used in URE scheme | 32 |
| $\mathrm{RTRE}_{hash}$ | Revocably hiding timed-release encryption from Definition 11 | 29 |
| $enc_1$ | Unknown recipient encryption | 31 |
| $dec_1$ | Unknown recipient decryption | 31 |

| | | |
|---|---|---|
| $keygen_1$ | Unknown recipient encryption key generation | 31 |
| $\mathrm{URE}(T')$ | Unknown recipient encryption scheme | 32 |
| $P_t^{EPR}$ | EPR states with max. $t$ phase and $t$ bit flips | 40 |
| $\mathrm{TRE}_{ih}$ | Timed-release encryption by iterated hashing Definition 10 | 28 |
| $\omega(x)$ | Hamming weight of $x$ | 7 |
| $\oplus$ | Bitwise XOR | 7 |
| $[q+n]_q$ | Set of all subsets of $\{1,\ldots,q+n\}$ of size $q$ | 7 |
| $\lvert\beta_{fe}\rangle$ | Bell state | 7 |
| $C^\perp$ | Dual code | 7 |
| $\lvert\widetilde{xy}\rangle$ | EPR state with phase flips $f$ and bit flips $e$ | 7 |
| $\lvert m\rangle_B$ | $m$ encoded in basis $B$ | 7 |
| $\lvert\!\lvert\!\lvert A\rvert\!\rvert\!\rvert$ | Operator norm of $A$ | 7 |
| $\lVert x\rVert$ | Euclidean norm of $x$ | 7 |
| $P_{C_1/C_2}^{EPR}$ | EPR state in $\mathbb{C}^{C_1/C_2}\otimes\mathbb{C}^{C_1/C_2}$ | 51 |
| $P_x^{uv}$ | Projector of measurement $M_X^{uv}$ for outcome $x$ | 51 |
| $\mathrm{RTRE}_{ow}$ | Revocably one-way timed-release encryption from Definition 7 | 11 |
| $\mathrm{TD}(\rho_1,\rho_2)$ | Trace distance between $\rho_1$ and $\rho_2$. | 7 |
| $\delta_T^{hid}$ | Time loss in revocably hiding timed-release encryption | 20 |
| $\mathrm{RTRE}_{hid}$ | Revocably hiding timed-release encryption from Definition 9 | 19 |
| $C/D$ | Quotient of codes $C$ and $D$ | 15 |
| $\delta_T^{ow}$ | Time loss in revocably one-way timed-release encryption | 40 |
| $\lvert\xi_{xuv}\rangle$ | Codewords in CSS code | 15 |
| $x \mod C$ | Projection into quotient code $D/C$ | 15 |
| $U_{uv}^{dec}$ | Decoding for the CSS code $\{\lvert\xi_{xuv}\rangle\}_x$ | 15 |
| $U_{uv}^{EC}$ | Error correction and decoding for the CSS code $\{\lvert\xi_{xuv}\rangle\}_x$ | 15 |
| $isEPR$ | Boolean indicating whether checking for $t$-error EPR state succeeded. | 43 |
| $P_B^=$ | Measures if two registers are equal in basis $B$ | 40 |
| $M_X^{uv}$ | Measure $x$ in a state $\lvert r\rangle\lvert\xi_{xuv}\rangle$, given $u,v$ | 51 |
| $P_{uv}$ | Projector of measurement $M_{UV}$ for outcome $u,v$ | 51 |
| $M_{UV}$ | Measures $u,v$ in a state $\lvert r\rangle\lvert\xi_{xuv}\rangle$ | 51 |
| $P_r$ | Projector of measurement $M_R$ for outcome $r$ | 51 |
| $M_R$ | Measures first $q$ bits | 51 |
| $\operatorname{im} M$ | Image of operator/function $M$ | 7 |

# Keyword index


Calderbank-Shor-Steane code, *see* CSS code
clock
  global, 31
correctness
  unknown recipient encryption, 31
CSS code, 15

early key revelation, 19
encryption
  timed-release, 8
  unknown recipient, 31
EPR pair, 7
EPR state, 7

global clock, 31

hiding, 9
  revocably, 10
  revocably, without offline-queries, 26
  without offline-queries, 26

key revelation
  early, 19
  late, 19

late key revelation, 19

offline-queries
  hiding without, 26
  one-way without, 26
  revocably hiding without, 26

one-way
revocably, 9, 10
without offline-queries, 26
oracle-query timing model
parallel, 22
sequential, 22

parallel oracle-query timing model, 22
polynomial time
sequential, 8
protocol
revocation, 9

revocably hiding, 10
without offline-queries, 26
revocably one-way, 9, 10
revocation protocol, 9

secure (unknown recipient encryption), 32
sequential oracle-query timing model, 22
sequential polynomial time, 8

time
sequential polynomial, 8
timed-release encryption, 8
timing model, 7
parallel oracle-query, 22
sequential oracle-query, 22
TRE, *see* timed-release encryption

unknown recipient encryption, 31
security, 32
URE, *see* unknown recipient encryption

## References

[ABB+07] Romain Alleaume, 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 Riguidel, Louis Salvail, Andrew Shields, Harald Weinfurter, and Anton Zeilinger. Secoqc white paper on quantum key distribution and cryptography. arXiv:quant-ph/0701168v1, 2007.

[AC12] Scott Aaronson and Paul Christiano. Quantum money from hidden subspaces. In *STOC '12*, pages 41–60. ACM, 2012.

[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. *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.

[BBF+07] Gilles Brassard, Anne Broadbent, Joseph Fitzsimons, Sébastien Gambs, and Alain Tapp. Anonymous quantum communication. In Kaoru Kurosawa, editor, *Asiacrypt 2007*, volume 4833 of *LNCS*, pages 460–473. Springer, 2007.

[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.

[BCG+02] Howard Barnum, Claude Crépeau, Daniel Gottesman, Adam Smith, and Alain Tapp. Authentication of quantum messages. In *FOCS 2002*, pages 449–458. IEEE, 2002.

[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.

[BGJ+15] Nir Bitansky, Shafi Goldwasser, Abhishek Jain, Omer Paneth, Vinod Vaikuntanathan, and Brent Waters. Time-lock puzzles from randomized encodings. IACR ePrint 2015/514, v. 20150529:075432, May 2015.

[BGS13] Anne Broadbent, Gus Gutoski, and Douglas Stebila. Quantum one-time programs. In Ran Canetti and JuanA. Garay, editors, *Crypto 2013*, volume 8043 of *LNCS*, pages 344–360. Springer, 2013.

[BN00] Dan Boneh and Moni Naor. Timed commitments. In *Crypto 2000*, pages 236–254. Springer, 2000.

[BT07] Anne Broadbent and Alain Tapp. Information-theoretic security without an honest majority. In Kaoru Kurosawa, editor, *Asiacrypt 2007*, volume 4833 of *LNCS*, pages 410–426. Springer, 2007.

[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. Robert Calderbank and Peter 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. IEEE, 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] Cynthia Dwork and Moni 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.

[DNW05] Cynthia Dwork, Moni Naor, and Hoeteck Wee. Pebbling and proofs of work. In Victor Shoup, editor, *Advances in Cryptology, Proceedings of CRYPTO '05*, volume 3621 of *Lecture Notes in Computer Science*, pages 37–54. Springer-Verlag, 2005. Online available at `http://www.wisdom.weizmann.ac.il/~naor/PAPERS/peb_abs.html`.

[EPR35] Albert Einstein, Boris Podolsky, and Nathan 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`.

[Got03] Daniel Gottesman. Uncloneable encryption. *Quantum Information & Computation*, 3(6):581–602, 2003.

[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.

[May93] Timothy C. May. Timed-release crypto. Cypherpunks mailing list, February 1993. archived at `http://cypherpunks.venona.com/date/1993/02/msg00129.html`, re-archived at `http://www.webcitation.org/6JhMIlgIF`.

[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] Michael A. Nielsen and Isaac L. 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/`.

[Ren05] Renato Renner. *Security of Quantum Key Distribution*. PhD thesis, ETH Zurich, September 2005. Available at `http://arxiv.org/abs/quant-ph/0512258v2`.

[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.

[SSS+13] Kamyar Saeedi, Stephanie Simmons, Jeff Z. Salvail, Phillip Dluhy, Helge Riemann, Nikolai V. Abrosimov, Peter Becker, Hans-Joachim Pohl, John J. L. Morton, and Mike L. W. Thewalt. Room-temperature quantum bit storage exceeding 39 minutes using ionized donors in silicon-28. *Science*, 342(6160):830–833, 2013.

[Ste96] Andrew 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`.

[Unr14] Dominique Unruh. Quantum position verification in the random oracle model. In *Crypto 2014*, volume 8617 of *LNCS*, pages 1–18. Springer, August 2014. Preprint on IACR ePrint 2014/118.

[Unr15] Dominique Unruh. Non-interactive zero-knowledge proofs in the quantum random oracle model. In *Eurocrypt 2015*, volume 9057, pages 755–784. Springer, 2015. Full version is IACR ePrint 2014/587.

[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.