The Quantum Decoherence Model: Everlasting Composable Secure Computation and More

Nico Döttling[1]*, Alexander Koch[4]**, Sven Maier***, Jeremias Mechler[3]***, Anne Müller[1,2], Jörn Müller-Quade[3]***, and Marcel Tiepelt[5]***

[1] CISPA Helmholtz Center for Information Security, Saarbrücken, Germany
{doettling,anne.mueller}@cispa.de
[2] Saarbrücken Graduate School of Computer Science, Saarland University Saarbrücken, Germany
[3] KASTEL Security Research Labs, Karlsruhe Institute of Technology (KIT), Karlsruhe, Germany
{jeremias.mechler,joern.mueller-quade}@kit.edu
[4] Secorvo Security Consulting GmbH, Karlsruhe, Germany
[5] NTT Social Informatics Laboratories, Tokyo, Japan
rsrch.mtiepelt@mailbox.org

Abstract. Quantum cryptography allows to achieve security goals which are unobtainable using classical cryptography alone: it offers the promise of everlasting privacy. That is, an adversary trying to attack a protocol must succeed during the run of the protocol. After the protocol has terminated, security holds unconditionally.

In this work, we initiate the study of a new model which we call the *quantum decoherence model* (QDM). In a nutshell, this model captures adversaries that are computationally bounded during the run of a protocol (and some time after), but become computationally unbounded long after the protocol terminates. Importantly, once the adversary becomes computationally unbounded, he can only remember a bounded number of qubits from before the computational bound was lifted.

We provide a variant of the Universal Composability framework which captures the new notion of quantum decoherence and augment it with quantum random oracles. As our main contribution, we construct a non-interactive commitment scheme achieving unconditional and statistical security against malicious senders and everlasting security against malicious receivers under our new security notion. Such commitments imply general secure multiparty computation with everlasting security.

* Funded by the European Union (ERC, LACONIC, 101041207). Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Research Council. Neither the European Union nor the granting authority can be held responsible for them.

** Work done while at KASTEL Security Research Labs, KIT and CNRS, IRIF, Université Paris Cité, France

*** This work was funded by the Topic Engineering Secure Systems of the Helmholtz Association (HGF) and supported by KASTEL Security Research Labs, Karlsruhe.

Finally, we show that our core technique can be applied to a broader spectrum of problems. We show that it gives rise to everlasting public key encryption and OT in the QDM. Finally, we also consider the weaker notion of incompressible encryption in the setting of quantum decoherence, and show that post-quantum IND-CPA secure public key encryption is sufficient to realize this notion without resorting to random oracles.
At the technical core of our constructions is a new, conceptually simple yet powerful *reverse entropic uncertainty relation*.

Keywords: Everlasting Security · Commitments · Quantum Random Oracle · In-compressible Encryption

1 Introduction

A Threat in the Long-Term Future. Almost all of classical cryptography suffers from a fundamental problem: Computational privacy is susceptible to be broken *after the fact* once an adversary becomes sufficiently powerful in the future. In fact, it is well known that counter-intelligence efforts such as VENONA [60] pursued a *store now, decrypt later* approach: large quantities of ciphertext data are stored speculating on a break of the underlying encryption schemes at a later point in time. Classical incompressible encryption schemes [36, 17, 37] inflate the costs of such an approach and hence penalize a mass surveillance adversary. However, this does not protect *individual* ciphertexts from being decrypted at a later point in time.

Everlasting Privacy. Quantum cryptography offers the intriguing promise of basing security of cryptographic protocols on some of the most fundamental laws of nature. The seminal work of Bennett and Brassard [10] showed that a quantum communication channel, together with a classical *authenticated channel*, is sufficient to establish unconditionally secure keys. The intervention of an eavesdropping adversary trying to learn the key is detectable, hence if no interference has been detected the protocol parties can trust that a key thus established is secure. One of the most desirable features of quantum cryptography is boosting "short term" computational security guarantees into *everlasting privacy*. Specifically, if the classical authenticated channel in the BB84 protocol is implemented using, say, digital signatures, then an adversary trying to attack this protocol has to break security of the signature scheme *during the run of the protocol*, hence pretty much instantaneously. Once the protocol has terminated and the honest parties have established a key, this key will be information-theoretically hidden from the adversary. Any effort to break the security of the underlying computationally secure signature scheme *after the fact* will be futile. Hence, even if the adversary becomes computationally unbounded after the termination of the protocol, this will not allow him to compromise the key.

A very recent line of work achieves everlasting privacy for more advanced primitives in the so-called *certified deletion model* [21, 43, 42, 41, 7, 40, 8, 45].

Protocols with certified deletion allow a receiver of (say) a quantum ciphertext to destroy this ciphertext by measuring it in a certain basis. Moreover, this measurement yields a certificate by which the receiver can convince the issuer of the ciphertext that the ciphertext has been destroyed. Conditioned on this certificate being valid, the encrypted message enjoys everlasting privacy, *i.e.*, even if the receiver becomes computationally unbounded at a later point in time, he will not be able to learn anything about the encrypted message after the fact. Consequently, this model hinges on *limited cooperation* by the receiver in order to achieve everlasting privacy; there is no intrinsic mechanism in place through which the issuer could enforce deletion of the ciphertext.[6]

Bounded Storage Models. The *bounded quantum storage model* (BQSM) [29] offers an alternative route to everlasting privacy. The BQSM imposes a bound on the number of qubits the adversary can store *at any time*. Damgård et al. [29] construct a statistically hiding and statistically binding quantum bit commitment in the BQSM. Their construction only needs one message, but somewhat unconventionally the committer is the receiver of the message. Hence, this protocol is not *non-interactive* in the standard sense where only communication from the sender to the receiver is allowed.

Koenig et al. [46] introduce the noisy storage model, which assumes *quantum noise* to model a *gradual* decay of quantum states. In particular, this model makes it necessary for honest parties to *wait* until information held by the adversary has decayed. Furthermore, they construct unconditionally secure randomized string commitments in the noisy storage model [46].

Both the bounded quantum storage model and the noisy storage model impose *stringent* assumptions on the adversary's ability to store quantum information *during the run of a protocol*. In particular, a bound on this ability must be known to the protocol designer, and the efficiency of such protocols generally degrades for more conservative bounds, as protocols in this model achieve security by overwhelming the adversary's ability to store quantum information. On the other hand, computationally secure protocols can become a liability long after the protocol has terminated, as information that *should have been kept private indefinitely* may be exposed in the far future.

1.1 Our Contribution

Quantum Decoherence. In this work, we strike a new balance between computational and unconditional security. We consider a new model, which we call the *quantum decoherence model (QDM)*. We argue that this model factors in realistic technological capabilities and limitations. The premise of this model is that an adversary might store quantum information for a long time *but not long enough until he is able to break computational hardness assumptions*. More formally, in the QDM protocols are modeled as having two distinct *stages*. In the

[6] On the other hand, deletion could be tied to an external reward. One may, *e.g.* consider a setting where the certificate of deletion facilitates decryption of a payment encrypted under a witness encryption scheme [33].

first stage, called *online stage*, which encompasses the entire run of a protocol, the adversary is computationally bounded but can otherwise perform arbitrary QPT computations. Critically, the adversary has access to a reliable quantum memory of arbitrary polynomial size. Specifically, the size of the memory is not known to the protocol designer and it is chosen adversarially depending on the protocol under attack. In the second stage, which we call the *everlasting stage*, we lift the computational bound on the adversary, but in turn only allow him to *remember* an a-priori bounded number of qubits from the online stage, in addition to an *unbounded number of classical bits*.

The quantum decoherence model can be seen as a restriction of the *everlasting security* framework [66], in that we additionally require that a quantum memory bound is imposed on the adversary before he becomes unbounded.

The quantum decoherence model is distinctly different from the bounded storage model and the noisy storage model, in that the two latter models assume a bound on the adversary's ability to store quantum information once or multiple times [35] *during* the run of the protocol. In the QDM, we make a different trade-off: The underlying assumption is that the adversary cannot store a sufficiently large amount of qubits for long enough until he is capable of breaking the computationally secure components of the protocol. Therefore, at no point in our protocols do we need to incur waiting times to make sure that the storage bound applies, the storage bound only needs to apply at a point in the future which might be long after the protocol terminates. We note that Damgård et al. [29] do provide a characterization of the QBSM which is similar to the QDM. However, none of their protocols leverage the fact that the adversary is computationally bounded during the online stage, and in fact none of their protocols use computationally secure components. In particular, a careful look at the model and the commitment protocol given in [29] shows that the storage bound on the parties needs to be enforced right at the end of the commitment phase, rather than at some point in the far future after all protocols in whose "context" of the commitment protocol is running have terminated.

We will consider two flavors of the quantum decoherence model. Specifically, we will consider the QDM both in the standard model and in the quantum random oracle model (QROM). In the quantum random oracle model, we require the adversary to make at most a polynomial number of superposition queries to the QRO during the online stage. This polynomial bound is adversarially chosen and may depend on the protocol under attack. In the everlasting stage, we lift the query bound from the adversary, *i.e.*, the adversary may now query the QRO an unbounded number of times. This is equivalent to providing the entire truth table of the QRO to the adversary.

In the second flavor of the quantum decoherence model, the adversary does not become computationally unbounded in the second stage, but instead obtains the secrets of the honest parties. This models the setting of *forward security* [25] and can be seen as a quantum analogue of the (purely classical) *incompressible cryptography* (IC) framework [36]. In the IC framework, the adversary may only remember a bounded number of classical bits about (say) a challenge ciphertext

before he obtains the honest party's secret keys. From a technological perspective, a severe bound on the ability to store classical information is much harder to justify than a quantum storage bound; storing large amounts of classical information is a nuisance, but does not pose potentially insurmountable technological challenges. The IC model is motivated by driving up the costs for mass surveillance adversaries by forcing them to commit large amounts of classical storage for a long time. The same rationale holds for the quantum decoherence model, but with a vengeance: Even if we live in a world in which it becomes feasibly to store quantum information over long time periods, the QDM forces adversaries to commit large amounts of (potentially very expensive) quantum storage for a long time.

Universal Composability with Decoherence. Unruh [66] defines a quantum version of the universal composability framework [22]. We introduce a new flavor of the framework which incorporates our quantum decoherence, a formal version of which can be found in Section 5.1. Specifically, in this model the environment can decide to undergo a *state transition*, which imposes a (parametrized) bound on the quantum storage of the environment but grants it unbounded computational power. A somewhat subtle aspect of this model concerns quantum random oracles. In order to properly model the environment becoming unbounded, it will obtain the entire truth table of the random oracle in the everlasting stage.

Composable Quantum Commitments in the QDM. Our first contribution is the construction of *non-interactive* composable string commitments in the QDM. The protocol (cf. Construction 1) is proven secure in the everlasting quantum UC framework with quantum decoherence, which we detail in Section 5.1. The construction relies on a post-quantum public-key encryption scheme and a classical non-interactive statistically binding commitment scheme, the latter of which we instantiate with a quantum random oracle to prove security. The resulting quantum string commitment scheme is composable, statistically binding and satisfies everlasting hiding in the QDM.

Theorem 1 (Informal version of Theorem 8). *Assume there exists a post-quantum IND-CPA-secure public-key encryption scheme. Then, there exists a quantum string commitment protocol in the QROM with everlasting quantum UC with decoherence security.*

Due to the compatibility of our security notion in the QDM with the everlasting quantum UC notion of Unruh [65], we obtain a protocol for composable general multi-party computation with everlasting security as a corollary of our commitment protocol.

Theorem 2 (Informal version of Proposition 5). *Assume there exists a post-quantum IND-CPA-secure public-key encryption scheme. Then, for every PPT functionality $\mathcal{F}$, there exists a protocol π_F that realizes $\mathcal{F}$ in the QROM with everlasting quantum UC with decoherence security.*

Everlasting Public-Key Encryption and OT in the QDM. Next, we show that our techniques also give rise to everlasting public-key encryption (cf. Construction 2). We define everlasting secure public-key encryption in the natural way; namely we require IND-CPA security against QDM adversaries who are computationally bounded in the first stage, but are subject to a quantum storage bound when transitioning to the second stage, in which they are computationally unbounded.

Theorem 3 (Informal version of Theorem 9). *Assume there exists a post-quantum IND-CPA-secure public-key encryption scheme. Then, there exists a public-key encryption scheme which achieves everlasting IND-CPA security in the QDM and the QROM.*

Finally, we show that our techniques allow to construct a semi-honest two message Oblivious Transfer (OT) protocol (cf. Construction 3). Security is achieved in the everlasting quantum UC framework in the QDM and QROM.

Theorem 4 (Informal version of Theorem 10). *Assume there exists a two-message OT protocol with statistical security against malicious senders and computational post-quantum security against semi-honest receivers. Then, there exists an OT protocol which is statistically secure against malicious senders and achieves everlasting security against semi-honest receivers in the QDM and QROM.*

We remark that we can also obtain OT by plugging our commitment into the compilers of Unruh [65] or Bartusek et al. [5], but using our techniques, we achieve a more direct and round-optimal construction.

An Instantiation Barrier. The security of the protocols given in Theorems 1, 3 and 4 relies on an idealized primitive, namely a statistically binding commitment instantiated using as a quantum random oracle.

This raises the question whether this commitment scheme can also be instantiated in the standard model. As a complementary result, we demonstrate in Section 10 that in general, computationally hiding commitment schemes are insufficient to instantiate this construction. We establish this by providing a commitment scheme which is statistically binding under the standard LWE assumption [58], yet when using it to instantiate the classical commitment scheme used in the quantum commitment protocol, Construction 1 becomes insecure.

Quantum Incompressible Encryption. We further extend our techniques to the setting of quantum incompressible encryption. Specifically, we show (cf. Construction 5) that any post-quantum public-key encryption scheme implies a quantum incompressible encryption scheme *without quantum random oracles.*

Theorem 5 (Informal version of Theorem 12). *Assuming the existence of a post-quantum IND-CPA-secure public-key encryption scheme, there exists a quantum incompressible encryption scheme. In this scheme, honest users need only prepare, transmit and measure single qubit states.*

Prepare-and-Measure Protocols. An appealing feature of our protocols is that honest participants do not need any quantum storage, but only the ability to prepare, transmit and measure single qubits. That is, the states can be sent immediately after creation and measured immediately upon reception. Such protocols, called "prepare-and-measure" protocols, are realizable with current technology.

2 Technical Outline

In the following, we will discuss our techniques with respect to the commitment protocol given in Section 6, which can also be applied to our public-key construction in Section 7 and our oblivious transfer protocol from Section 8.

Encoding in Conjugate Bases. At the heart of our constructions is a technique called *encoding in conjugate bases*, originally proposed by Wiesner [68] and Benett and Brassard [10]. This technique takes a bitstring $\mathbf{x} \in \{0,1\}^n$ and encodes each bit of $\mathbf{x}$ in one of two bases, chosen uniformly at random. These two bases are chosen to be the eigenbases of two anti-commuting operators, typically the computational basis $\mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, and the Hadamard basis $\mathbf{H} = \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, which are the eigenbases of the Pauli $\mathbf{Z}$ and Pauli $\mathbf{X}$ operator, respectively.

In other words, the encoder chooses a random bitstring $\boldsymbol{\theta} \in \{0,1\}^n$ and encodes $\mathbf{x}$ into a state

$$|\phi_{\mathbf{x},\boldsymbol{\theta}}\rangle = \bigotimes_{i=1}^{n} (\mathbf{H}^{\theta_i} |x_i\rangle).$$

The computational basis is typically denoted as $+$ and the Hadamard basis as $\times$. Throughout the document, we will identify $+ = 0$ and $\times = 1$ according to the representation above. The state $|\phi_{\mathbf{x},\boldsymbol{\theta}}\rangle$ can be seen as a "weak" commitment to $\mathbf{x}$; without knowledge of the bitstring $\boldsymbol{\theta}$ it does not "fully reveal" $\mathbf{x}$, but at the same time it binds to $\mathbf{x}$, in the sense that opening $|\phi_{\mathbf{x},\boldsymbol{\theta}}\rangle$ to any value different from $\mathbf{x}$ is detectable with substantial probability. Wiesner's original application for this technique was quantum money [68], but it is also at the core of quantum key distribution protocols [10] and more recent concepts such as certifiable deletion [20, 6].

Entropic Uncertainty. The process of measuring an arbitrary n-qubit quantum state in randomly chosen bases has strong entropic uncertainty guarantees. Specifically, fix an arbitrary (adversarially prepared, potentially mixed) n-qubit quantum state ρ and assume a collection of bases $\boldsymbol{\theta} \in \{+,\times\}^n$ are chosen uniformly at random.

Then, measuring each qubit of the state ρ with the corresponding basis in $\boldsymbol{\theta}$ produces a high entropy outcome, even given $\boldsymbol{\theta}$. Specifically, let $\mathbf{x}$ denote the measurement outcome. It can be shown [28] that the conditional min-entropy of $\mathbf{x}$ given $\boldsymbol{\theta}$ is at least $-n \cdot \log(1/2 + 1/4 \cdot \sqrt{2})$. If we switch to the somewhat

relaxed setting of *smooth min-entropy*[7] we can obtain an even stronger bound. Specifically, in [29] it was shown that the conditional smooth min-entropy of X given $\boldsymbol{\theta}$ approaches $n/2$ for a sufficiently large n, where X corresponds to the random variable associated with measurement outcomes $\mathbf{x}$.

It is instructive to think of this scenario as a guessing game: An adversary prepares a state ρ, sends it to the experimenter that measures ρ using random bases $\boldsymbol{\theta} \in_R \{+,\times\}^n$, obtaining an outcome X. The adversary is then told the choice of basis $\boldsymbol{\theta}$ and needs to guess the outcome X, and wins if his guess is correct. The min-entropy of X given $\boldsymbol{\theta}$ is the logarithm of the success probability of the best-possible adversary in this experiment.

The above uncertainty relations assume that a state ρ is prepared adversarially and then measured in randomly chosen bases $\boldsymbol{\theta} \in_R \{+,\times\}^n$. In our setting though, the situation is reversed: An honest sender prepares a state $|\phi_{\mathbf{x},\boldsymbol{\theta}}\rangle = \bigotimes_{i=1}^n (\mathbf{H}^{\theta_i}|x_i\rangle)$, which is then measured via an arbitrary, adversarially chosen POVM M. Given the outcome of this measurement and the basis choices $\boldsymbol{\theta}$, the task of the adversary is to guess the string $\mathbf{x}$ which was encoded in $|\phi_{\mathbf{x},\boldsymbol{\theta}}\rangle$. For the purpose of this outline it is instructive to think of M as a POVM which measures the entire state $|\phi_{\mathbf{x},\boldsymbol{\theta}}\rangle$, *i.e.*, after the measurement the state collapses into a classical state. In Section 4 we will consider partial measurements, where the adversary retains a residual quantum state after the measurement.

Assume for now that $\mathbf{x}$ is chosen uniformly random as well, *i.e.*, it has maximal entropy. We will show that in this setting, preparing a uniformly random state $|\phi_{\mathbf{x},\boldsymbol{\theta}}\rangle$ and measuring a given state with a uniform choice of bases, results in the same distribution for the random variable, *i.e.*, we can resort to the above uncertainty relations to bound the min-entropy of $\mathbf{x}$ given $\boldsymbol{\theta}$ and the result of the measurement in the "reversed" experiment.

Specifically, consider an alternative state preparation procedure for $|\phi_{\mathbf{x},\boldsymbol{\theta}}\rangle$. The sender prepares a tensor product of n EPR pairs and splits them into two systems, σ_E and σ_A. He then chooses a uniformly random basis $\boldsymbol{\theta} \in_R \{+,\times\}^n$ and measures each qubit in σ_A in basis θ_i. Since the joint system σ_{EA} is a tensor product of EPR pairs, it suffices to consider the effect on a single EPR pair

$$\mathsf{epr} = |0\rangle|0\rangle + |1\rangle|1\rangle = (\mathbf{H}|0\rangle)(\mathbf{H}|0\rangle) + (\mathbf{H}|1\rangle)(\mathbf{H}|1\rangle).$$

If the first qubit is measured in basis $+$, we obtain a uniformly random bit x and the residual state collapses to $|x\rangle$. On the other hand, measuring the first qubit in basis $\times$ is equivalent to first performing a Hadamard transform on the first qubit and then measuring the first qubit in the computational basis $+$, as

$$(\mathbf{H} \otimes \mathbf{I}) \cdot \mathsf{epr} = |0\rangle(\mathbf{H}|0\rangle) + |1\rangle(\mathbf{H}|1\rangle),$$

we obtain a random bit x and the residual state collapses to $\mathbf{H}|x\rangle$. In effect, measuring σ_E using a basis $\mathbf{H}^\theta$ corresponding to bit θ yields a bit x, and the system σ_A collapses to $\mathbf{H}^\theta|x\rangle$.

[7] A random variable X has δ-smooth min-entropy k, if it is δ-close in statistical distance to a random variable $\tilde{X}$ which has *true min-entropy* k.

Going one step further, we can think of an experiment where the measurement in basis θ is delayed. That is, the experiment prepares σ_{EA} and sends the system σ_A *without* measuring σ_E in basis θ. Due to non-locality, in the view of the adversary this is identically distributed to the last experiment. This is now equivalent to an experiment where the EPR pairs have been *pre-shared*, where the experiment and the adversary perform their measurements on their respective sub-systems independently. Using the same reasoning again, we can argue that this is identically distributed to an experiment where the adversary locally prepares a tensor product of EPR pairs σ_{EA}, measures the sub-system σ_A with the POVM M, and sends the residual state σ_E to the experiment which measures σ_E using basis θ. But this is just a special case of an experiment where the adversary prepares some state ρ, sends ρ to the experiment that measures ρ using basis θ and obtains an output $\mathbf{x}$.

Hence, the same min-entropy bounds as above apply. That is, the smooth min-entropy of a uniform $\mathbf{x}$ given the choice of $\boldsymbol{\theta}$ and given the outcome of a POVM M on $|\phi_{\mathbf{x},\boldsymbol{\theta}}\rangle$ approaches $n/2$ for sufficiently large n.

Our proof follows the general outline of transforming a security game based on conjugate coding into a security game using EPR pairs. The technique was introduced in the security analysis of quantum key distribution [62, 48] and later also found application in the work of Broadbent and Islam [21], who used it to prove security of their certified deletion scheme. While the techniques seem similar at first, the required uncertainty relations and corresponding security games are quite different.

In the security game of a certified deletion experiment, the adversary needs to make a prediction for a deletion certificate which corresponds to the measurement outcome of a quantum state in the Hadamard basis. The uncertainty relation guarantees that the adversary cannot predict the measurement outcome in the computational basis later. This type of uncertainty relation bears resemblance to proofs in the area of quantum key distribution. Our uncertainty relation on the other hand is related to bounds known from the area of the Quantum Bounded Storage Model. In the security game for protocols in the QDM, the adversary does not need to publish a measurement outcome but a measurement is enforced by the decoherence bound. Furthermore, we generically adapt the uncertainty relation to allow for only a partial measurement and remaining quantum memory.

Bartusek and Khurana [6] construct advanced primitives with certified deletion by extending the work of [21]. While their proof technique does not rely on uncertainty relations but on a cut-and-choose technique, they still make use of conjugate coding and a transformation to EPR pairs in order to prove security.

2.1 Quantum String Commitments

The entropic uncertainty relation discussed previously is the starting point for our non-interactive commitment scheme COM, cf. Section 6. As additional ingredients we use a seeded randomness extractor Ext, a parity-check matrix $\mathbf{PC}$

of a moderately high-rate $\mathbb{F}_2$-linear error-correcting code $\mathtt{C}$ of minimum distance $d \in \mathcal{O}(\kappa)$, and a classical statistically binding non-interactive commitment scheme com. (See Definition 7 for formal definitions of these terms.) The scheme COM proceeds as follows.

- On input of a message μ, the sender chooses uniformly random $\mathbf{x}, \boldsymbol{\theta} \in \{0,1\}^N$ and an appropriate extractor seed s, as well as uniformly random coins $r \in_R \{0,1\}^\kappa$. He computes $\sigma = \mathsf{Ext}(s, \mathbf{x}) \oplus \mu$, a syndrome $\mathbf{c} = \mathbf{PC} \cdot \mathbf{x}$ and a commitment $h = \mathsf{com}((\boldsymbol{\theta}, s, \sigma, \mathbf{c}); r)$. He finally prepares a state $|\phi_{\mathbf{x},\boldsymbol{\theta}}\rangle = \bigotimes_{i=1}^N (\mathbf{H}^{\theta_i} |x_i\rangle)$ and sends h and $|\phi_{\mathbf{x},\boldsymbol{\theta}}\rangle$ to the receiver.
- When receiving h and $|\phi_{\mathbf{x},\boldsymbol{\theta}}\rangle$, the (honest) receiver chooses $\boldsymbol{\theta}' \in_R \{0,1\}^N$ uniformly at random and measures $|\phi_{\mathbf{x},\boldsymbol{\theta}}\rangle$ in the bases given by $\boldsymbol{\theta}'$, and stores the measurement outcome $\mathbf{x}'$ together with h.
- To unveil a commitment, the sender provides $\mathbf{x}$, $(\boldsymbol{\theta}, s, \sigma, \mathbf{c})$ and r to the receiver. The receiver first checks whether $\mathbf{c} = \mathbf{PC} \cdot \mathbf{x}$, $h = \mathsf{com}((\boldsymbol{\theta}, s, \sigma, \mathbf{c}); r)$ and whether $\mathbf{x}$ and $\mathbf{x}'$ agree at the indices i for which $\theta_i = \theta'_i$. If so he outputs $\mu' = \sigma \oplus \mathsf{Ext}(s, x)$, and $\perp$ otherwise.

The statistical binding property of the scheme COM is established along the following lines. As the commitment scheme com is statistically binding, h must open to the unique triple $(\boldsymbol{\theta}, s, \sigma, \mathbf{c})$ with overwhelming probability.

If the sender tries to unveil two different $\mu \neq \mu'$ using two different $\mathbf{x}_1 \neq \mathbf{x}_2$, then $\mathbf{x}_1$ and $\mathbf{x}_2$ must have Hamming distance at least d, as they are different and have the same syndrome $\mathbf{c}$. That is, $\mathbf{x}_1$ and $\mathbf{x}_2$ differ in at least d coordinates. In the security reduction, we may assume that the receiver's measurement in bases $\boldsymbol{\theta}'$ is postponed until after the malicious sender announces $\mathbf{x}_1$ and $\mathbf{x}_2$ and opens h to $(\boldsymbol{\theta}, s, \sigma, \mathbf{c})$, as $\boldsymbol{\theta}'$ is hidden from the sender's view. Thus, for each index i at which $\mathbf{x}_1$ and $\mathbf{x}_2$ differ, the receiver will pick a θ'_i for which $\theta'_i = \theta_i$ with probability $1/2$. But if this happens, either $\mathbf{x}_1$ or $\mathbf{x}_2$ will be inconsistent with the receiver's measurement and will be rejected. As $\mathbf{x}_1$ and $\mathbf{x}_2$ differ in d coordinates, the probability that no inconsistency is detected is 2^{-d}. Consequently, the receiver rejects one of $\mathbf{x}_1$, $\mathbf{x}_2$, except with negligible probability 2^{-d}. (In the formal proof, we will use a more refined argument to show that this commitment scheme is extractable.)

Establishing the (everlasting) hiding property of COM is more challenging. Our proof strategy is to use the entropic uncertainty relation discussed above, together with the randomness extraction property of Ext. In order to do so, we must first remove $\boldsymbol{\theta}$ and s information-theoretically from the view of a malicious receiver. The issue here is that the statistically binding commitment $h = \mathsf{com}((\boldsymbol{\theta}, s, \sigma, \mathbf{c}); r)$ fully determines $\boldsymbol{\theta}$ and s.

In order to "decouple" the commitment h from $\boldsymbol{\theta}$ and s, we consider an idealized commitment scheme com and implement this via a random oracle H. Let com' be a post-quantum-secure extractable commitment scheme which we instantiate by a public-key encryption scheme and a CRS. We set $\mathsf{com}(y; r) = (\mathsf{com}'(r), \mathsf{H}(r) \oplus y)$, where we model H as a quantum random oracle, *i.e.*, the adversary can query H on superpositions. First note that this commitment scheme is classically extractable; an extractor can first extract r from

$\mathsf{com}'(r)$, and then recover y from the second part of the commitment using r. Extractability could alternatively be achieved by extracting directly from the QROM. Known QROM extraction techniques [31] do not directly allow an extraction in our setting since the adversary becomes computationally unbounded with access to the RO in the everlasting phase of our protocol. While this technique could possibly be extended to our setting, we decided to extract from the extractable commitment com' to show that extractability does not hinge on the random oracle and is preserved if H is instantiated.

Next, we argue that an adversary that is capable of constructing a random oracle query with non-negligible weight on r can break the hiding property of the commitment scheme com'. Therefore, we can choose h' uniformly at random and program $\mathsf{H}(r)$ to be h' *after the adversary has sent all his queries*. Consequently, $\mathsf{H}(r) \oplus (\boldsymbol{\theta}, s, \sigma, \mathbf{c})$ statistically hides the committed value $(\boldsymbol{\theta}, s, \sigma, \mathbf{c})$ during the online stage.

As the view of the adversary in the online stage is independent of $\boldsymbol{\theta}$, s, σ and $\mathbf{c}$, we can now leverage the entropic uncertainty relation to establish that $\mathbf{x}$ has high smooth conditional min-entropy after the online stage, *i.e.*, when the adversary's view is measured or collapsed. We need to additionally consider that the syndrome $\mathbf{c} = \mathbf{PC} \cdot \mathbf{x}$ leaks a few bits of information about $\mathbf{x}$, but this can be routinely handled via the min-entropy chain rule [30, 59]. We can then argue that $\mathsf{Ext}(s, \mathbf{x})$ is statistically close to uniform from the adversary's view, and hence $\sigma = \mathsf{Ext}(s, \mathbf{x}) \oplus \mathbf{m}$ statistically hides $\mathbf{m}$.

The same technical blueprint can be leveraged to construct everlasting public-key encryption and oblivious transfer. We provide these constructions in Sections 7 and 8.

Everlasting vs. Statistical Hiding. Given that commitment schemes with the (stronger) statistical hiding property can be constructed from one-way functions [39], it is a natural question why the (weaker) everlasting hiding property is pursued. To this end, we remark that we require our commitment scheme to be not only hiding, but to be *composable* as well. In this setting, the statistical hiding property is subject to strong impossibility results in the classical [56, 12] and quantum [66] setting. While using the QROM could, in principle, allow us to circumvent these, we have intentionally chosen not to do so: When instantiating the QROM in real life, the extractability property necessary for composability would be lost immediately. Instead, by relying on a CRS and PKE for extractability, extractability is *not* lost when instantiating the QROM. Thus, in our construction, we mainly use the QROM to achieve correlation intractability, whose importance is illustrated in Section 2.3.

2.2 Everlasting Public-Key Encryption

The construction of the everlasting commitment scheme also gives rise to an everlasting public-key encryption scheme. Briefly speaking, the query to the random oracle is encrypted using a classical, post-quantum IND-CPA secure encryption scheme, which can be broken by the unbounded adversary only, which happens

only after the quantum state collapsed. We provide the detailed construction and security in Section 7.

2.3 An Instantiation Barrier

At first glance it may be reasonable to conjecture that the commitment scheme discussed in Section 2.1 is secure for any statistically binding, post-quantum computationally hiding non-interactive commitment scheme instead of a random oracle.

However, we will now sketch that the computationally hiding property is insufficient to instantiate this construction. The full argument is given in Section 10. Specifically, we will provide a statistically binding commitment scheme which is post-quantum hiding under the Learning with Errors (LWE) assumption, for which the above commitment scheme is insecure in the everlasting setting.

The basic idea is to construct a classical commitment scheme com which has strong quantum malleability properties. A natural starting point to construct such a scheme is the notion of *quantum fully homomorphic encryption* (QFHE) [50, 16]. A QFHE scheme allows encrypting quantum information, and further allows arbitrary (efficient) quantum computations on encrypted data, without knowledge of the secret key. In terms of security, we require standard (quantum) IND-CPA security, whereas in terms of correctness we require homomorphic evaluation and decryption to yield the same outcome as performing the same quantum computation on the plaintexts. Mahadev [50] constructed a leveled QFHE scheme based on the post-quantum hardness of the LWE problem with super-polynomial modulus-to-noise ratio. This was later improved by Brakerski [16], who constructed a leveled QFHE scheme from the post-quantum hardness of LWE with polynomial modulus-to-noise ratio.

Let $\mathsf{QFHE} = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{Eval})$ be a QFHE scheme with the mild additional property that ciphertexts statistically bind to the plaintext they encrypt, *i.e.*, it is not possible to open a ciphertext c to two different plaintexts m_1 and m_2 in a convincing way; this property is satisfied *e.g.* by the scheme given in [16] which is based on the *primal Regev encryption scheme* [58]. We will construct a commitment scheme $\mathsf{com}_{\mathsf{QFHE}}$ from QFHE in the straightforward way: We will have a common reference string that consists of a public key pk of QFHE generated via $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\kappa)$. To commit to a message μ, we choose random coins r and encrypt μ to $h = \mathsf{Enc}(\mathsf{pk}, \mu; r)$ using randomness r. The commitment scheme is statistically binding due to the additional extra requirement we imposed above, and hiding due to the IND-CPA security of QFHE.

To see that instantiating the commitment scheme com with $\mathsf{com}_{\mathsf{QFHE}}$ in the construction COM discussed in the previous paragraph renders COM insecure, note the following. Consider the following adversary strategy against the hiding property of COM in the decoherence model. Let $|\phi\rangle = |\phi_{\mathbf{x},\boldsymbol{\theta}}\rangle$.

Online Stage: – Given the common reference string $\mathsf{crs} = \mathsf{pk}$ and the commitment $h = \mathsf{Enc}(\mathsf{pk}, \boldsymbol{\theta}, s, \sigma, \mathbf{c}; r)$, as well as $|\phi\rangle$, the adversary first encrypts $|\phi\rangle$ to a quantum ciphertext $h_{|\phi\rangle}$.

– Consider the following quantum circuit $C(\boldsymbol{\theta}, s, \sigma, |\phi\rangle)$, which takes basis choices $\boldsymbol{\theta} \in \{0,1\}^N$, and extractor seed s, a string σ and a quantum state $|\phi\rangle$. It computes $|\phi'\rangle = (\bigotimes_{i=1}^{N} \mathbf{H}^{\theta_i}) \cdot |\phi\rangle$ and measures $|\phi'\rangle$ in the computational basis, obtaining an $\mathbf{x}' \in \{0,1\}^N$. Next, it computes and outputs $\mu' = \sigma \oplus \mathsf{Ext}(s, \mathbf{x}')$.
– The adversary now homomorphically evaluates C on the ciphertexts h and $h_{|\phi\rangle}$, obtaining a *classical* ciphertext d. The public key pk and the ciphertext d are then forwarded to the second stage of the adversary.

Everlasting Stage:
– Given pk and d, the adversary will now brute-force a secret key sk corresponding to pk, *e.g.* by enumerating all random coins of the KeyGen algorithm.
– Given sk, it can now decrypt d to $\mu' = \mathsf{Dec}(\mathsf{sk}, d)$ and output μ'.

Correctness of this attack follows routinely from the homomorphic correctness of QFHE. Specifically, μ' follows the same distribution as if we had evaluated C on $\boldsymbol{\theta}$, s, σ and $|\phi\rangle$ in the plain. As $|\phi\rangle = (\bigotimes_{i=1}^{N} \mathbf{H}^{\theta_i}) \cdot |\mathbf{x}\rangle$ and $\sigma = \mathsf{Ext}(s, \mathbf{x})$, it follows readily that $\mu' = \mu$. That is, this attack always recovers the message μ.

Interestingly, this attack does not rely on the compactness property of QFHE, that is it still works even if the size of the (classical) ciphertext d scales with the size of the circuit C.

2.4 Quantum Incompressible Encryption

The discussion in the last section seems to suggest that non-standard components such as random oracles are necessary to achieve any meaningful notion of security in the decoherence setting. However, as discussed above, we may settle on a version of the decoherence model where we provide somewhat more restricted abilities to the adversary in the everlasting stage. Specifically, rather than granting the adversary unbounded computational power, we can *e.g.* make the secret keys of the honest parties available. This would, under normal circumstances, be sufficient to break any long-term privacy guarantee. As discussed above, in analogy to the incompressibility framework proposed in [36] we call this setting the *quantum incompressibility model*.

Taking a careful look at the proof for the hiding property of the commitment scheme COM above, in order to rely on the entropic uncertainty relation, the critical ability of the security reduction is to postpone the basis choice $\boldsymbol{\theta}$ (as well as the extractor seed s). In the proof above, we relied on a weak programmability property of the quantum random oracle to achieve this. However, this property can also be achieved using primitives in the standard model. Specifically, *non-committing encryption* [23] allows to issue *dummy ciphertexts* which are indistinguishable from regular ciphertexts, but can later be opened to an arbitrary message m together with a corresponding secret key sk. Intuitively, this is possible as such schemes allow the message to be *programmed* into the secret key sk in an indistinguishable way.

Now, given a suitable post-quantum non-committing encryption scheme, we can instantiate the blueprint of protocol COM with a non-committing encryption

scheme NCE instead of the post-quantum commitment com to obtain a quantum incompressible encryption scheme. The construction is provided in Section 9.

2.5 Additional Related Work

The area of incompressible encryption originated in a purely classical setting, where the classical memory of the adversary is restricted. The first work in the area constructed secret-key incompressible encryption [32]. Guan, Wichs, and Zhandry [36] construct incompressible signatures and public-key incompressible encryption schemes. They give two constructions for the public-key setting, where one scheme relies on public-key encryption and has low rate and the second construction has optimal rate but uses the strong assumption of indistinguishability obfuscation. This was improved upon by [17], who construct rate-1 public-key incompressible encryption from standard assumptions. The notion of incompressible encryption has also been extended to the notions of incompressible attribute-based encryption and incompressible functional encryption [34]. Furthermore, [13] have constructed a public-key encryption scheme that achieves both incompressibility and leakage resilience at the same time. The notion of leakage resilience models that an adversary obtains the full ciphertext but only a few bits of leakage obtained from a leakage function applied to the secret-key. In [47] incompressible encryption constructions are improved to attain key-dependent message security and anonymity. In a recent work Yogev and Ben-David [69] show that any classical public-key encryption scheme with subexponential security is an incompressible encryption scheme and also achieves the notion of everlasting security in the classical bounded storage model.

Müller-Quade and Unruh [54] show an impossibility result for everlasting commitments given a coin toss or common reference string (CRS). The impossibility arises since these functionalities are long-term revealing, that is, any secrets between two parties can eventually be computed by the (unbounded) adversary. They give constructions for everlasting hiding and computationally binding commitments from PKE and zero-knowledge proofs. Our construction, on the other hand, targets everlasting hiding and statistically binding commitments made possible by the additional assumptions on the quantum memory.

In a concurrent and independent work Champion *et al.* [27] construct untelegraphable encryption. This notion requires that from a quantum ciphertext one cannot create a classical representation that can be decrypted given the secret key. They construct an information-theoretically secure secret-key untelegraphable encryption scheme and show that it can be used to construct an everlasting secure encryption scheme in the QROM. By extending their result to the public-key setting one can achieve an equivalent result to our everlasting secure public-key encryption scheme in Section 7 when setting the decoherence bound $q = 0$. In both our and their work it is noticed that the QROM cannot be instantiated in the construction. Due to this issue, our work explores the security notion of incompressible encryption. In the work of Champion *et al.* [27] an additional impossibility result is provided. They show that there cannot be a black-box construction of everlasting public-key untelegraphable encryption from

any falsifiable assumption assuming the sub-exponential hardness of one-way functions. Furthermore, they show that the notion of collusion-resistant untelegraphable encryption implies the impossibility of hyper-efficient shadow tomography [1, 44]. Additionally, they show that weakly-efficient shadow tomography, a new notion of shadow tomography which they define, is impossible assuming everlasting untelegraphable encryption. Broadbent, Culf, and Rochette [19] extend their work by constructing information-theoretic untelegraphable encryption with additional properties such as multi-ciphertext and bounded-collusion security. Their construction uses Haar-random unitaries as a key and when instantiated with pseudorandom unitaries they obtain a scheme with everlasting security.

Barhoush and Salvail [3] have combined the BQSM with computational assumptions to construct efficient one-time programs. Information-theoretically secure one-time programs in the BQSM have previously been constructed in [4]. From one-time programs they construct k-program broadcast which is a primitive that allows any receiver to learn at most k evaluations of the program. This primitive in turn allows the contruction of a plethora of primitives in the BQSM such as CCA1-secure asymmetric key encryption, signatures, signature tokens, and encryption tokens. In the work of [4] the k-program is made more efficient by using the assumption of one-way functions and a construction inspired by quantum garbled circuits. Then they construct functional encryption in the computational BQSM which bypasses classical impossibilities result known for functional encryption [15, 2].

Table of Contents

1 Introduction . . . 2
1.1 Our Contribution . . . 3
2 Technical Outline . . . 7
2.1 Quantum String Commitments . . . 9
2.2 Everlasting Public-Key Encryption . . . 11
2.3 An Instantiation Barrier . . . 12
2.4 Quantum Incompressible Encryption . . . 13
2.5 Additional Related Work . . . 14
3 Preliminaries . . . 17
3.1 Quantum Information . . . 17
3.2 The Quantum Decoherence Model (QDM) . . . 18
3.3 Randomness Extractors . . . 19
3.4 Linear Codes . . . 19
3.5 Public Key Encryption . . . 20
3.6 Functional Encryption . . . 21
3.7 Secret Key Encryption . . . 21
3.8 Commitments . . . 22
3.9 Oblivious Transfer . . . 23
3.10 Quantum State Teleportation . . . 24
3.11 The Quantum Random Oracle (QROM) . . . 24
3.12 Compressed Oracles . . . 24
3.13 Reprogramming . . . 26
4 Conditional Min-Entropy for Wiesner Coding . . . 27
4.1 Min-Entropy Given Quantum Memory . . . 32
5 Quantum Universal Composability with Decoherence . . . 33
5.1 Introduction to the Model . . . 33
5.2 Changes to the Execution . . . 37
5.3 Ideal Functionalities . . . 38
6 Composable Everlasting Commitment Scheme . . . 41
6.1 Applications . . . 49
7 Everlasting Public-Key Encryption . . . 50
8 Oblivious Transfer with Everlasting Semi-Honest Security . . . 54
9 Quantum Incompressible Encryption . . . 60
9.1 Construction . . . 61
9.2 Hybrid Incompressible Encryption . . . 64
10 On the Necessity of the Random Oracle . . . 65
11 Conclusion . . . 66
A Wiesner Coding Extraction . . . 73
B Proofs of the Properties of the UC-Notion . . . 74

3 Preliminaries

Notation. We denote by $[n]$ for $n \in \mathbb{N}$ the set $\{1, \ldots, n\}$. The security parameter will be κ. Bold lowercase Roman letters, *e.g.* $\mathbf{b}$, represent bit vectors. For any vector or bit string $\mathbf{x}$, the ith position will be expressed as x_i. Vectors are denoted in bold lower case letters and matrices are denoted in bold upper case letters. Given two bit vectors, $\oplus$ defines their bitwise *XOR* operation and $\|$ the concatenation of the strings. For any set S, $X \xleftarrow{\$} S$ denotes uniformly sampling from the set. We denote $\exp(x)$ the exponential function e^x.

We say a function $f(\kappa)$ is negligible in the security parameter κ, written $f \in \mathit{negl}(\kappa)$, if for every positive integer c there exists some integer n_0 such that for all $\kappa > n_0$ it holds that $f(\kappa) < \frac{1}{\kappa^c}$, thus it asymptotically decreases faster then any polynomial. A function f is overwhelming if $1 - f$ is negligible.

3.1 Quantum Information

Each qubit is represented as an element in a two-dimensional Hilbert space $\mathcal{H}^2$. To discriminate quantum states from classical values we use the canonical *Dirac notation*, *e.g.* the state vector $|\psi\rangle$ and its dual $\langle\psi|$. The inner product is written as $\langle\psi|\psi\rangle$. A quantum state $|\psi\rangle^P$ denotes that $|\psi\rangle$ is in possession of or associated with a party P. If not otherwise stated, the state is represented in the computational basis, which we denote as "+", consisting of the orthogonal vectors $|0\rangle = \left(\begin{smallmatrix}1\\0\end{smallmatrix}\right)$ and $|1\rangle = \left(\begin{smallmatrix}0\\1\end{smallmatrix}\right)$ for a two dimensional Hilbert space. Additionally we use the Hadamard (or *diagonal*) basis $|+\rangle = 1/\sqrt{2}\left(\begin{smallmatrix}1\\1\end{smallmatrix}\right)$ and $|-\rangle = 1/\sqrt{2}\left(\begin{smallmatrix}1\\-1\end{smallmatrix}\right)$, which we denote as "×", to encode quantum states. The gate that transforms a state from the computational to the diagonal basis is the Hadamard gate denoted H. We denote H^b for a bit $b \in \{0, 1\}$ to denote that the gate is applied if $b = 1$ and not otherwise. By θ, we denote a string of the above bases. We denote the measurement operator with respect to the basis θ as M_θ. An equivalent description of a quantum state is given by the density operator or matrix $\rho \equiv \sum_i p_i |\psi_i\rangle\langle\psi_i|$, which omits the information about a particular basis. It may be noted that two states that admit the same density matrix cannot be distinguished by any measurement. The trace distance for two density matrices ρ, σ is defined as $\mathrm{TD}(\rho, \sigma) = \frac{1}{2}\,\mathrm{tr}(\sqrt{(\rho - \sigma)^\dagger(\rho - \sigma)})$, where tr denotes the trace of a matrix.

A measurement is a collection of operators $\{M_m\}$ where m indicates the measurement outcome. A projective measurement needs to satisfy $\sum M_m^\dagger M_m = I$ and the operators need to be orthogonal. The probability for outcome m when a state ρ is measured is given by $p_m(\rho) = \mathrm{tr}\,(M_m^\dagger M_m \rho)$. A POVM is a collection of operators $\{E_m\}$ such that $\sum E_m = I$.

The statistical distance, or total variational distance, of two distributions X and Y over a domain S is defined as $\Delta(X, Y) = \frac{1}{2}\sum_{a \in S} |\mathsf{Pr}[X = a] - \mathsf{Pr}[Y = a]|)$.

Entropy. The min-entropy captures the maximum probability of guessing a string X, possibly conditioned on some event Y, *i.e.*, $H_{\min}(X) = -\log(\max_x P_X(x))$ and $H_{\min}(X|Y) = -\log\big(\sum_Y P_Y(y) \max_x P_{X|Y}(x|Y = y)\big)$.

We also consider the smooth min-entropy which introduces a small error parameter ε, $H^{\varepsilon}_{\min}(X|Y) = \max_{(X',Y')} H_{\min}(X'|Y')$, where the maximum is taken over all distributions $(X', Y') : \Delta((X', Y'), (X, Y)) \leq \varepsilon$.

Similarly the quantum smooth min-entropy is defined as $H^{\epsilon}_{\min}(A|B)_{\rho} = \sup_{\rho'} H_{\min}(A|B)_{\rho'}$ where sup ranges over density operators $\rho'_{AB} \in \mathcal{D}(\mathcal{H}_{AB})$ which are ϵ-close to ρ_{AB}. A state is ϵ-close if $||\rho - \rho'||_1 \leq \mathrm{tr}(\rho) \cdot \epsilon$. When the state is classical, the quantum min-entropy coincides with the classical min-entropy. The max-entropy of a quantum state given by the density matrix ρ is $H_{\max}(\rho) = \log(\mathrm{rank}\,\rho)$.

Conjugate Coding. We describe the basic idea behind conjugate coding [68] (or Wiesner encoding) to encode classical information into a quantum state $|\psi\rangle$. Let $\mathit{encode}_{\theta} \colon \{0,1\}^N \to \mathcal{H}^N$ be a function mapping strings to quantum states, $X \mapsto |\phi\rangle$. The function uniformly samples a string θ of basis vectors $\{+, \times\}$ for each qubit and encodes the input X of bits b to a quantum string, *i.e.*, for each bit position i it performs the following operation: If $\theta = +$ it encodes 0 as $|0\rangle$ and 1 as $|1\rangle$, and if $\theta = \times$ it encodes 0 as $|+\rangle$ and 1 as $|-\rangle$.

Additional preliminaries regarding cryptographic protocols can be found in Section 3.6 and preliminaries regarding the QROM can be found in Section 3.11.

3.2 The Quantum Decoherence Model (QDM)

Everlasting Security in the Quantum Decoherence Model. Everlasting or *Long-Term* Security [55] allows to consider technological progress by assuming that computational problems might be broken in the future. The model splits the security experiment into two phases: A polynomially bounded phase against an adversary $\mathcal{A}_1$, and an unbounded phase against adversary $\mathcal{A}_2$, where the adversary may extract information from the view of the former. The framework has previously been considered in the quantum setting by Unruh [66], *i.e.*, with quantum adversaries, but in the setting of Universal Composability (UC) [22]; resulting in everlasting UC security.

Additionally, we assume that the quantum state of the adversary undergoes a decoherence process. In this model the adversary has the additional restriction that during a certain phase in the protocol the quantum storage is limited to a fixed number of qubits. For example, Damgård et al. [29] consider a similar situation: the Bounded Quantum Storage Model (BQSM). In the BQSM a computationally unbounded adversary has a bounded quantum storage after receiving a quantum state. After a part of the state has been measured information about the original state is irrevocably lost. The security of the BQSM directly relies on the limited quantum storage.

We propose the Quantum Decoherence Model (QDM). This model serves as a technique to upgrade the security of schemes against adversaries that become more powerful after the execution of the protocol *i.e.*, they become computationally unbounded or gain information such as the leakage of secret keys. Let $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ be an adversary in the QDM. In the first phase $\mathcal{A}_1$ is a QPT adversary. Before transitioning to the second phase $\mathcal{A}_1$'s state is restricted to q

qubits. In the second phase, $\mathcal{A}_2$ has access to the state of $\mathcal{A}_1$ and may be computationally unbounded or otherwise defined according to the security model of the protocol. The adversary has unlimited classical storage at all times. If it turns out that an adversary has more than q bits of quantum storage, the security of the protocol falls back to its computational security guarantees. Therefore, our model provides a best-of-both-worlds guarantee: computational security and everlasting security if the storage bound applies at some point after the run of the protocol. Note that this is not achievable via *e.g.* robust combiners, as bounded storage that only applies at some future point after the protocol is insufficient to get any meaningful security.

3.3 Randomness Extractors.

We make use of a randomness extractor which, given a seed and a min-entropy input, outputs a string that is statistically close to a uniformly random string even if the seed is published.

Definition 1. *A function* $\mathsf{Ext} : \{0,1\}^l \times \{0,1\}^n \to \{0,1\}^d$ *is called a* (w,ε)*-strong randomness extractor if for all* $x \in \{0,1\}^n$ *with* $H_{min}(x) \geq w$*, it holds that*

$$\{(\mathsf{Ext}(s,x),s)\colon s \xleftarrow{\$} U_l\} \approx_\varepsilon \{(r,s)\colon r \xleftarrow{\$} U_d, s \xleftarrow{\$} U_l\}\,,$$

where U_l *and* U_d *are independent uniform distributions over* $\{0,1\}^l$*,* $\{0,1\}^d$*.*

The following Lemma shows that we can apply a randomness extractor to an input for which we have a smooth min-entropy guarantee instead of a min-entropy guarantee.

Lemma 1. *A* (w,ε)*-strong randomness extractor* $\mathsf{Ext} : \{0,1\}^l \times \{0,1\}^n \to \{0,1\}^d$ *for all* X *distributed over* $\{0,1\}^n$ *with* $H_{min}(X) \geq w$ *is a* $(w,\varepsilon+\varepsilon')$*-strong randomness extractor for all* X' *distributed over* $\{0,1\}^n$ *with* $H^{\varepsilon'}_{min}(X') \geq w$*.*

Proof. Let X have smooth min-entropy $H^{\varepsilon'}_{\min}(X) \geq w$. Then there exists a distribution X' such that $H_{\min}(X) \geq w$ and $\Delta(X,X') \leq \varepsilon'$. Let S be an independent uniform seed over $\{0,1\}^l$. Since statistical distance cannot increase under applying a deterministic function, it must hold that $\mathsf{Ext}(X,S) \approx_{\varepsilon'} \mathsf{Ext}(X',S)$. Since it holds that $\mathsf{Ext}(X',S) \approx_\varepsilon U_d$ it follows that $\mathsf{Ext}(X,S) \approx_{\varepsilon+\varepsilon'} U_d$. □

3.4 Linear Codes

Definition 2. *A binary* $[N,K,D]$*-linear code encodes words in* $\{0,1\}^K$ *to codewords in* $\{0,1\}^N$*. The code is defined by a generator matrix* G *which maps a word to a codeword or a parity check matrix* PC *which maps a codeword to* 0 *or produces an error syndrome.* D *is the minimum distance of the code and is defined as the Hamming distance between two code words. There are efficient encoding and decoding algorithms such that for all* $m \in \{0,1\}^K$*,* $\mathsf{Decode}(\mathsf{Encode}(m)) = m$*.*

Theorem 6. *(Theorem 22, [63]) For all integers $k \geq 2$ and all ϵ such that $1 - kH(\epsilon) > 0$, where H is the binary entropy, there exists a polynomial-time constructible family of binary linear codes with rate $1-kH(\epsilon)$ and minimum relative distance arbitrarily close to $\epsilon^{1+1/(k-1)}$ for which a circuit of size $O(nlog(n))$ and logarithmic depth will decode some $\Omega(\epsilon^{1+1/(k-1)})$ fraction of errors.*

In our protocol, we will make use of Sipser Spielman expander codes [63] for parameter $k = 2$ and a small constant ϵ. Fixing the codeword length N this yields a code with message length $K = (1-\gamma)N$ for $\gamma = 2H(\epsilon)$, distance $D = \epsilon^2$ and decoding radius αN for $\alpha = \Omega(\epsilon^2)$. Hence the length of a syndrome of this code is $N - K = \gamma N$. As $H(\epsilon) \to 0$ for $\epsilon \to 0$, we can make $\gamma = 2H(\epsilon) > 0$ an arbitrarily small constant by choosing ϵ to be a suitably small constant.

3.5 Public Key Encryption

A public key encryption scheme consists of three algorithms $\mathsf{PKE} = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ with the following functionalities:

$\mathsf{KeyGen}(1^\kappa) \to (\mathsf{pk}, \mathsf{sk})$**:** Given the security parameter KeyGen as unary input, KeyGen outputs a public key and a private key.

$\mathsf{Enc}(\mathsf{pk}, \mathsf{m}) \to \mathsf{ct}$**:** Given the public key and a message, Enc is a probabilistic polynomial-time algorithm that computes a ciphertext.

$\mathsf{Dec}(\mathsf{sk}, \mathsf{ct}) \to \mathsf{m}$**:** Given a ciphertext and the secret key, Dec outputs a message.

A PKE scheme is called *perfectly correct* if for all $\kappa \in \mathbb{N}$ and all m in the message space, it holds that $\mathsf{Pr}[\mathsf{Dec}(\mathsf{sk}, \mathsf{Enc}(\mathsf{pk}, \mathsf{m})) = \mathsf{m} \mid (\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\kappa)] = 1$, where the probability is taken over the random coins of Enc and KeyGen.

Definition 3 (IND-CPA Security for PKE Schemes). *Let $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ be a PKE scheme and let κ be the security parameter. Let $\mathcal{A}$ be a quantum polynomial-time adversary and let the experiment $\mathsf{Exp}_{\mathcal{A}}^{\mathsf{IND\text{-}CPA}}(\kappa)$ be defined as follows:*

1. $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\kappa)$
2. $(m_0, m_1, st) \leftarrow \mathcal{A}(1^\kappa, \mathsf{pk})$
3. $\mathsf{ct} \leftarrow \mathsf{Enc}(m_b)$ *where* $b \xleftarrow{\$} \{0, 1\}$
4. $b' \leftarrow \mathcal{A}(st, \mathsf{ct})$
5. *if* $b = b'$ *the experiment outputs 1, otherwise the experiment outputs 0*

The PKE scheme is IND-CPA-secure if for every QPT adversary A *that sends challenges of equal length and eventually outputs a bit, there exists a negligible function negl such that for every $\kappa \in \mathbb{N}$, it holds that*

$$\mathsf{Pr}[\mathsf{Exp}_{\mathcal{A}}^{\mathsf{IND\text{-}CPA}}(\kappa) = 1] \leq \frac{1}{2} + negl(\kappa)$$

3.6 Functional Encryption

A functional encryption (FE) scheme [15] is a classical public key encryption scheme that allows to create keys in the context of a specific circuit. The decryption algorithm outputs the result of applying this function to the message and not the original message itself.

Definition 4. *(Functional Encryption) Let 1^κ be the security parameter. Let $\{\mathsf{C}_{1^\kappa}\}$ be a class of circuits with input space $\mathcal{X}_{1^\kappa}$ and output space $\mathcal{Y}_{1^\kappa}$. A functional encryption scheme is defined by the PPT algorithms* $\mathsf{FE} = (\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$.

Setup$(1^\kappa) \to (\mathsf{mpk}, \mathsf{msk})$**:** *given the security parameter 1^κ outputs the master public key* mpk *and the master secret key* msk.
KeyGen$(\mathsf{msk}, \mathsf{C}) \to \mathsf{sk}_\mathsf{C}$**:** *given the master secret key* msk *and a circuit* C *and outputs a function key* sk_C.
Enc$(\mathsf{mpk}, m) \to \mathsf{ct}$**:** *given* mpk *and a message $m \in \mathcal{X}$*
Dec$(\mathsf{sk}_\mathsf{C}, \mathsf{ct}) \to y$**:** *given a ciphertext* ct *and* sk_C *output a value $y \in \mathcal{Y}$.*

The scheme has to fulfill the following correctness and security properties:

Correctness. Let $(\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^\kappa)$, $\mathsf{sk}_\mathsf{C} \leftarrow \mathsf{KeyGen}(\mathsf{msk}, \mathsf{C}), \mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{mpk}, m)$. Then the FE is correct, if for all $\mathsf{C} \in \{\mathsf{C}_{1^\kappa}\}$ and $m \in \mathcal{X}$ it holds that $\mathsf{Pr}[\mathsf{C}(m) = \mathsf{Dec}(\mathsf{sk}_\mathsf{C}, \mathsf{ct})] \geq 1 - negl(1^\kappa)$.

Definition 5. *(Single-Key Semi-Adaptive Security) Consider the experiment* $\mathrm{Dist}^{\mathsf{FE}}_{\mathcal{A}}(1^\kappa)$*:*

1. *Run* $\mathsf{FE.Setup}(1^\kappa) \to (\mathsf{mpk}, \mathsf{msk})$ *and sample a random bit $b \leftarrow \{0, 1\}$.*
2. *On input 1^κ and* mpk *the adversary $\mathcal{A}$ outputs to plaintext messages m_0, m_1 and receives the ciphertext* $\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{mpk}, m_b)$.
3. *$\mathcal{A}$ submits a circuit* C *such that* $\mathsf{C}(m_0) = \mathsf{C}(m_1)$*, and receives* $\mathsf{sk}_\mathsf{C} \leftarrow \mathsf{KeyGen}(\mathsf{msk}, \mathsf{C})$.
4. *The adversary $\mathcal{A}$ outputs a guess b'. If $b' = b$ the adversary wins and the experiment outputs 1. Otherwise, the experiment outputs 0.*

A functional encryption scheme is said to have single-key semi-adaptive security if for all QPT adversaries $\mathcal{A}$, there exists a negligible function negl such that for all $\kappa \in \mathbb{N}$:

$$\mathsf{Pr}[\mathrm{Dist}^{\mathsf{FE}}_{\mathcal{A}}(1^\kappa) = 1] \leq \frac{1}{2} + negl(1^\kappa).$$

3.7 Secret Key Encryption

A secret key encryption scheme consists of three algorithms $\mathsf{SKE} = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ with the following functionalities:

$\mathsf{KeyGen}(1^\kappa) \to \mathsf{sk}$**:** Given the security parameter KeyGen outputs a secret key.
$\mathsf{Enc}(\mathsf{sk}, \mathsf{m}) \to \mathsf{ct}$**:** Given the key and a message Enc is a probabilistic algorithm that computes a ciphertext.

$\mathsf{Dec}(\mathsf{sk}, \mathsf{ct}) \to \mathsf{m}$**:** Given a ciphertext and the secret key Dec outputs a message.

A SKE scheme is called *perfectly correct* if for all $\kappa \in \mathbb{N}$ and all messages m in the message space, it holds that $\mathsf{Pr}[\mathsf{Dec}(\mathsf{sk}, \mathsf{Enc}(\mathsf{sk}, \mathsf{m})) = \mathsf{m} \mid \mathsf{sk} \leftarrow \mathsf{KeyGen}(1^\kappa)] = 1$, where the probability is taken over the random coins of Enc and KeyGen.

Definition 6. *(IND-CPA Security for SKE schemes) Let* $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ *be a SKE scheme and let* κ *be the security parameter. Let* $\mathcal{A}$ *be a quantum polynomial-time adversary and let the experiment* $\mathsf{Exp}_{\mathcal{A}}^{\mathsf{IND\text{-}CPA}}(\kappa)$ *be defined as follows:*

1. $\mathsf{sk} \leftarrow \mathsf{KeyGen}(1^\kappa)$
2. $(\mathsf{m}_0, \mathsf{m}_1, st) \leftarrow \mathcal{A}(1^\kappa)^{\mathcal{O}_{\mathsf{Enc}(\mathsf{sk}, \cdot)}}$
3. $\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{m}_b)$ *where* $b \xleftarrow{\$} \{0,1\}$
4. $b' \leftarrow \mathcal{A}(1^\kappa, st)^{\mathcal{O}_{\mathsf{Enc}(\mathsf{sk}, \cdot)}}$
5. *if* $b = b'$ *the experiment outputs 1, otherwise the experiment outputs 0*

The PKE scheme is IND-CPA-secure if for every QPT adversary A *that sends equal-length messages* m_0 *and* m_1 *as challenge and eventually outputs a bit, there exists a negligible function negl such that for all* $\kappa \in \mathbb{N}$*, it holds that*

$$\mathsf{Pr}[\mathsf{Exp}_{\mathcal{A}}^{\mathsf{IND\text{-}CPA}}(\kappa) = 1] \leq \frac{1}{2} + negl(\kappa).$$

3.8 Commitments

We briefly recall the general definition of a commitment protocol between the sender S and the receiver R in Definition 7,

Definition 7 (Commitment scheme). *A non-interactive commitment scheme* $\mathsf{COM} = (\mathsf{COM.Com}, \mathsf{COM.Unv}, \mathsf{COM.Vrf})$ *is an efficient two-stage protocol, comprising the commit method* Com*, the unveil method* Unv *and the verification method* Vrf *and describes the interaction between two parties, the sender and the receiver.*

$\mathsf{Com}(1^\kappa, \mu)$ *Given a string* $\mu \in \{0,1\}^n$ *and the security parameter* 1^κ*, the sender computes a commitment message* com *and an internal state* st*. She sends the commitment* com *to the receiver.*

$\mathsf{Unv}(1^\kappa, st) \to \mathsf{op}$ *The sender computes an opening* op *and sends the message to the receiver.*

$\mathsf{Vrf}(1^\kappa, \mathsf{com}, \mathsf{op}) \to \mu/\perp$ *The receiver runs the verification algorithm and outputs the message* μ *if the verification succeeded. Otherwise he rejects the unveil.*

A commitment protocol is correct *if an honest commitment gets rejected only with negligible probability, where the probability is over the random coins used by* Com*,* i.e.*, if for all* $\kappa \in \mathbb{N}$ *and all* $\mu \in \{0,1\}^n$*, it holds that*

$$\Pr\left[\mathsf{Vrf}(1^\kappa, \mathsf{com}, \mathsf{op}) = \mu : \begin{matrix}(st, \mathsf{com}) \leftarrow \mathsf{Com}(1^\kappa, \mu) \\ \mathsf{op} \leftarrow \mathsf{Unv}(1^\kappa, st, \mathsf{com})\end{matrix}\right] = 1$$

Definition 8. *(Hiding) A commitment scheme is computationally hiding if for any QPT adversary $\mathcal{A}$ it holds for any messages μ_0, μ_1 that:*

$$|\Pr[\mathcal{A}(1^\kappa, \mathsf{com}) = 1 : \mathsf{com} \leftarrow \mathsf{Com}(1^\kappa, \mu_0)] - \Pr[\mathcal{A}(1^\kappa, \mathsf{com}) = 1 : \mathsf{com} \leftarrow \mathsf{Com}(1^\kappa, \mu_1)]| = negl(\kappa)$$

We require statistically binding commitments and additionally we require the stronger notion of extractability.

Definition 9. *(Extractability) A commitment scheme is called extractable if for any unbounded adversary $\mathcal{A}$ there exists an unbounded extractor Ext such that for any unbounded distinguisher D it holds that*

$$|\Pr\left[D(1^\kappa, st_2, out) = 1 : \begin{array}{c}(st_1, \mathsf{com}) \leftarrow \mathcal{A}(1^\kappa) \\ (st_2, \mathsf{op}) \leftarrow \mathcal{A}(1^\kappa, st_1) \\ out \leftarrow \mathsf{Vrf}(\mathsf{com}, \mathsf{op})\end{array}\right] - \Pr\left[D(1^\kappa, st_2, out) = 1 : \begin{array}{c}(st_1, \mathsf{com}) \leftarrow \mathcal{A}(1^\kappa) \\ \mu \leftarrow \mathsf{Ext}(\mathsf{com}) \\ (st_2, \mathsf{op}) \leftarrow \mathcal{A}(1^\kappa, st_1) \\ out \leftarrow \mathsf{Vrf}(\mathsf{com}, \mathsf{op}) \\ out := \texttt{Fail}\ if\ out \notin (\mu, \bot)\end{array}\right]| = negl(\kappa)$$

3.9 Oblivious Transfer

Oblivious transfer is a protocol between a sender and a receiver where the sender selects two messages and the receiver obtains only one of those messages based on a selection bit b. The receiver learns nothing about the other message and the sender learns nothing about the bit b. Let κ be the security parameter and let q be the storage parameter.

Definition 10. *A protocol $\mathsf{OT} = (\mathsf{OT.Setup}, \mathsf{OT.R1}, \mathsf{OT.S1}, \mathsf{OT.R2})$ consists of four PPT algorithms that are defined as follows:*

- $\mathsf{Setup}(1^\kappa) \to crs$ *takes as input the security parameter and outputs a common reference string.*
- $\mathsf{R1}(1^\kappa, crs, b) \to (ot_1, st)$ *takes as input the security parameter, the crs, and a bit b and outputs the first message ot_1 and a state st.*
- $\mathsf{S1}(1^\kappa, crs, \mu_0, \mu_1, ot_1) \to ot_2$ *takes as input the security parameter, the crs, the first OT message and two messages $\mu_0, \mu_1 \in \{0,1\}^\kappa$ and outputs a message ot_2.*
- $\mathsf{R2}(1^\kappa, crs, st, ot_2) \to \mu_b$ *takes as input the security parameter, the crs, a state st, the second OT message and outputs the message ot_2.*

Correctness. An OT protocol is *correct* if for every κ, any pair of messages $\mu_0, \mu_1 \in \{0,1\}^\kappa$ and any bit $b \in \{0,1\}$, it holds that $\mathsf{Pr}[\mu_b = \mu'_b \leftarrow \mathsf{R2}(1^\kappa, crs, st, ot_2) : (ot_2 \leftarrow \mathsf{S1}(1^\kappa, crs, \mu_0, \mu_1, ot_1), (ot_1, st) \leftarrow \mathsf{R1}(1^\kappa, crs, b)), crs \leftarrow \mathsf{Setup}(1^\kappa)] = 1$, where the probability is over the random coins of the respective probabilistic algorithms.

In this work make use of the classical OT protocol by Peikert et al. [57], which realizes the ideal functionality $\mathcal{F}_{\mathsf{OT}}$ in the UC framework. We refer the reader to [57] for details on the security properties.

3.10 Quantum State Teleportation

Two spatially separated parties A and B can teleport a quantum state from one person to the other by using shared entanglement and classical communication [11]. A holds the state ρ and one qubit of an EPR pair, B holds the other qubit of the EPR pair. A performs a Bell measurement on the two states, which is equivalent to a CNOT gate followed by a Hadamard gate on ρ and a computational basis measurement on each qubit, and obtains the correction keys (a, b). Now Bob holds the state $X^a Z^b \rho (X^a Z^b)^\dagger$ from which he can recover the original state after obtaining the teleportation keys (a, b).

3.11 The Quantum Random Oracle (QROM)

The QROM [14] extends the classical Random Oracle Model [9]; it models an *ideal hash function*, but takes into account that the adversary $\mathcal{A}$ could implement the function on a quantum computer thus allowing oracle queries in superposition. This invalidates various classical techniques such as reprogrammability of the random oracle or the recording of queries made by the adversary. Therefore several techniques, such as Unruh's "One-way to Hiding" Lemma [64] or Zhandry's compressed oracles [70], have been developed to improve the usability of the QROM in proofs. Lemma 2 is one such result.

Lemma 2. *([70]) After making t quantum queries to a quantum random oracle $\mathcal{H} : \{0,1\}^n \to \{0,1\}^n$, the probability of finding a preimage x of $y = \mathcal{H}(x)$ is at most $O(t^2/2^n)$.*

One technique to simulate the QROM is to fix a random function, given by its truth table, and answer queries by evaluating the function in superposition. This technique neither records the queries of the adversary nor is it efficient. Other techniques employ a quantum secure PRF but in the context of everlasting security the adversary will eventually become computationally unbounded and could then distinguish the PRF from a truly random function. The technique of compressed random oracles fits our needs.

3.12 Compressed Oracles

The main idea of compressed oracles [70] that separates them from previous approaches [71] is that instead of responding according to a fixed random function,

which we refer to as the fixed standard oracle (FStO) from here on, this approach stores a superposition over all functions $H = \sum_h |h\rangle$. Upon receiving a query the oracle creates the following state: $\sum_{x,u} |x,u\rangle \to \sum_{x,u} \sum_h |x, u \oplus h(x)\rangle \otimes |h\rangle$. While this initially contains each function h with equal amplitudes, any query *entangles* the adversary's state with the oracle and any measurement outcome of the adversary *fixes* the QRO such that the superposition is only over mappings that respect the adversary's previous measurements. Due to the entanglement with the adversary this technique allows to record queries made by the adversary.

Lemma 3. *[70, Lemma 2] The standard oracle and the fixed standard oracle are perfectly indistinguishable.*

$$\mathsf{Pr}[\mathcal{A}^{FStO}() = 1] = \mathsf{Pr}[\mathcal{A}^{StO}() = 1]$$

Zhandry [70] provides a way to efficiently simulate the oracle using a compression mechanism. We will not delve into the specifics of the compressed oracle and only treat it as a black box with the following interface.

Definition 11. *The compressed oracle consists of three efficient algorithms* Init, Update *and* End.

Init *takes no input and outputs the empty database D.*
Update$(|\phi\rangle, D) \to (|\phi'\rangle, D')$ *takes as input a quantum query $|\phi\rangle$ and answers the query according to the compressed oracle mechanism.*
End(D) *Collapse the database by measuring and outputing the values.*

The whole oracle requires qubits in the order of t, the number of queries, and provides a QPT circuit to respond to oracle queries. The uncompressed version is usually referred to as the standard oracle (StO) and the compressed version as the compressed standard oracle (CStO).

Lemma 4. *[70, Lemma 4] The standard oracle and the compressed standard oracle are perfectly indistinguishable.*

$$\mathsf{Pr}[\mathcal{A}^{StO}() = 1] = \mathsf{Pr}[\mathcal{A}^{CStO}() = 1]$$

In the everlasting setting we simulate the RO using the compressed random oracle in the first phase and then we need to provide the adversary with the truth table of the complete random oracle in the second phase. In the following Lemma we show that finish the simulation of the random oracle using the End functionality and providing a truth table that is consistent with the obtained values is indistinguishable from an interaction with the random oracle.

Exp_1**:** The queries are answered by the random oracle. After the end of the simulation the truth table is provided.
Exp_2**:** The queries are answered using the compressed oracle. After the simulation the compressed oracle is measured. Since the database only contains polynomially many values the remaining values are inserted from a random function.

Lemma 5. Exp_1 *and* Exp_2 *are perfectly indistinguishable.*

Proof.

H_0. Hybrid 0 is Exp_1

H_1. In Hybrid 1 we simulate the random oracle using the uncompressed StO. The standard oracle starts in a superposition over all functions. When collapsing a random function is selected consistent with any queries that might have previously collapsed the state partly. Since the StO uses the whole function table for the simulation we get the complete function table of a uniformly random function which is equivalent to the random oracle. Therefore $H_0 = H_1$.

H_2. Hybrid 2 is Exp_2 Here we switch to simulating using the compressed oracle. Based on Lemma 4 the compressed oracle and the standard oracle are indistinguishable. The values that were not queried by the adversary are uniformly random to him. Therefore $H_1 = H_2$. □

3.13 Reprogramming

Often a proof requires to reprogram the output of a specific value. Therefore we provide the following lemma (cf. Lemma 6) which shows that a value that was queried with low probability can be reprogrammed to a new output.

We add a new functionality to the compressed oracle simulation which allows to reprogram.

Definition 12. *The function* $\mathsf{Reprogram}(|\phi\rangle, D, x^*, h) \to (|\phi'\rangle, D')$ *takes as input a query* $|\phi\rangle$*, a special input* x^* *and the database* D *of a compressed random oracle and proceeds as follows: If the input* x^* *is queried, the value* h *is returned, if any other value is queried the answer is defined by the* Update *functionality.*

The Reprogram functionality is implemented by quantumly comparing the inputs to x^*, *i.e.*, storing 1 if $x \neq x^*$ and storing 0 if $x = x^*$ into a separate register. The state of the query after computing this function in superposition is $|\phi'\rangle = \sum_{x,u} \alpha_{x,u}|x,u\rangle|1\rangle + \alpha^*|x^*,u^*\rangle|0\rangle$. Depending on the last register a controlled query is issued to the compressed random oracle, such that the Update functionality is applied to the state if the control bit is 1 and the value y is used if the bit is 0. The controlled operation is implemented by turning every gate in the circuit into a controlled gate. This answers all queries other than x^* as before and is indistinguishable to $\mathcal{A}$.

We consider two simulations of the oracle corresponding to interactions with the adversary $\mathcal{A}$ who is allowed to make t queries in total:

Exp_1: The queries are answered as defined above by the compressed oracle. This perfectly simulates the random oracle.

Exp_2: We split the adversary's queries into two sets of t_1 and t_2 queries such that $t = t_1 + t_2$. During the first t_1 queries, the value x^* is not known to $\mathcal{A}$, during the remaining t_2 queries, the value may be known to $\mathcal{A}$. After t_1 queries, we reprogram the random oracle at value x^* to the output of a uniformly random value $y = \mathcal{H}(x^*)$.

Lemma 6. *Let $\mathcal{A}$ be an adversary that makes t queries to the random oracle $\mathcal{H} : \{0,1\}^n \to \{0,1\}^m$. Then,*

$$\mathsf{Pr}[1 \leftarrow \mathcal{A}^{\mathsf{Exp1}}] - \mathsf{Pr}[1 \leftarrow \mathcal{A}^{\mathsf{Exp2}}] \leq O\left(\sqrt{\frac{t^2}{2^n}}\right).$$

Proof. During the remaining t_2 queries, the value of x^* is reprogrammed by applying the Reprogram function. After the reprogramming step the distribution of the random oracle is the same since the new value is also a uniformly random value, the adversary can only tell a difference if the query x^* also appeared within the first t_1 queries.

At the i-th query we have the query state $|\phi'_i\rangle = \sum_{x,u} \alpha_{i,x,u}|x\rangle|u\rangle|0\rangle + \alpha_{i,x^*}|x^*\rangle|u\rangle|1\rangle$. The combined amplitude of a^* over all t_1 queries cannot be larger than $\sqrt{t_1^2/2^n}$. Otherwise we have an adversary that can find a preimage x^* with probability higher than $t_1^2/2^n$ contradicting Lemma 2.

The Euclidean distance between the states of all t queries combined $|\phi_t\rangle$ and $|\phi'_t\rangle$ is $|\alpha_t^*| \leq \sqrt{t^2/2^n}$. Then, the advantage in distinguishing $|\phi_t\rangle$ from $|\phi'_t\rangle$ is $\mathrm{TD}(|\phi_t\rangle\langle\phi_t|, |\phi'_t\rangle\langle\phi'_t|) \leq |\alpha_t^*|$ [70, Lemma 1]. □

4 Conditional Min-Entropy for Wiesner Coding

In this section we prove several lemmas regarding the min-entropy of a classical string under a Wiesner encoding, *i.e.*, each bit gets randomly encoded in either the computational or the diagonal (Hadamard) basis.

Lemma 7. *Let $|\psi\rangle$ be a quantum state that encodes $x \xleftarrow{\$} \{0,1\}^n$ using Wiesner coding. Let Θ be a random variable denoting the basis choice that is uniformly distributed over $\{+,\times\}^n$ and let X be a random variable denoting the choice of the string x. An arbitrary measurement is performed on the state. Let the outcome of the measurement be denoted as $Y_{x,\theta}$. After the measurement is applied the basis choice Θ is revealed. Then the min-entropy of x conditioned on the measurement outcome and the basis choice is:*

$$H^{\varepsilon}_{min}(X|Y_{x,\theta}, \Theta) \geq n\left(\frac{1}{2} - 2\lambda\right)$$

where $\varepsilon = exp\left(-\frac{\lambda^2 n}{32(2-\log(\lambda))^2}\right)$ and $0 < \lambda < \frac{1}{2}$.

To prove Lemma 7 we need the following uncertainty relation.

Lemma 8 ([29]). *Let $\rho \in \mathcal{D}(\mathcal{H}_2^{\otimes n})$ be an arbitrary quantum state and let Θ be uniformly distributed over $\{+,\times\}^n$. Denote the measurement outcome of ρ in the basis Θ as X. Then for any $0 < \lambda < \frac{1}{2}$, $H^{\varepsilon}_{min}(X|\Theta) \geq n\left(\frac{1}{2} - 2\lambda\right)$, where $\varepsilon = exp\left(-\frac{\lambda^2 n}{32(2-\log(\lambda))^2}\right)$.*

Note that in Lemma 8 the uncertainty comes from the measurement in the orthogonal bases $\{+,\times\}$ while in Lemma 7 the uncertainty comes from creating the states in these bases.

We will use the following corollary of Lemma 8.

Lemma 9. *Let Y be a probability distribution supported on a finite domain $\mathcal{Y}$, and for any $y \in \mathcal{Y}$ let $\rho_y \in \mathcal{D}(\mathcal{H}_2^{\otimes n})$ be an arbitrary quantum state depending on y, and let Θ be uniformly distributed over $\{+,\times\}^n$. Denote the measurement outcome of ρ_y in the basis Θ as X_y. Then it holds for any $0 < \lambda < \frac{1}{2}$ that*

$$H^{\varepsilon}_{min}(X_Y|\Theta,Y) \geq n\left(\frac{1}{2} - 2\lambda\right).$$

where $\varepsilon = exp\left(-\frac{\lambda^2 n}{32(2-\log(\lambda))^2}\right)$.

Proof. Fix any $y \in \mathcal{Y}$. Lemma 8 yields that $H^{\varepsilon}_{\min}(X_y|\Theta) \geq n\left(\frac{1}{2} - 2\lambda\right)$. Now let (X'_y, Θ'_y) be a (correlated) pair of random variables that is ε-close to (X_y, Θ) in statistical distance such that $H_{\min}(X'_y|\Theta'_y) \geq n\left(\frac{1}{2} - 2\lambda\right)$ (such a pair (X'_y, Θ') exists by the definition of smooth min-entropy). In other words, for every $y \in \mathcal{Y}$ we have a pair of random variables (X'_y, Θ'_y) which is ε-close to (X_y, Θ) and has min-entropy $H_{\min}(X'_y|\Theta'_y) \geq n\left(\frac{1}{2} - 2\lambda\right)$. Hence it holds that

$$\begin{aligned}
H_{\min}(X'_Y|\Theta'_Y, Y) &= -\log\Big(\sum_{y\in\mathcal{Y}} \mathsf{Pr}[Y=y] \cdot 2^{-H_{\min}(X'_y|\Theta'_y)}\Big) \\
&\geq -\log\Big(\sum_{y\in\mathcal{Y}} \mathsf{Pr}[Y=y] \cdot 2^{-n\left(\frac{1}{2}-2\lambda\right)}\Big) \\
&= -\log\Big(2^{-n\left(\frac{1}{2}-2\lambda\right)} \cdot \sum_{y\in\mathcal{Y}} \mathsf{Pr}[Y=y]\Big) \\
&= n\left(\frac{1}{2} - 2\lambda\right).
\end{aligned}$$

We will now show that (X_Y, Θ, Y) and (X'_Y, Θ'_Y, Y) have statistical distance ε. It holds that

$$\begin{aligned}
\Delta((X_Y,\Theta,Y),(X'_Y,\Theta'_Y,Y)) &= \max_P |\mathsf{Pr}[P(X_Y,\Theta,Y)=1] - \mathsf{Pr}[P(X'_Y,\Theta'_Y,Y)=1]| \\
&= \max_P \sum_y \mathsf{Pr}[Y=y] \cdot |\mathsf{Pr}[P(X_y,\Theta,y)=1] - \mathsf{Pr}[P(X'_y,\Theta'_y,y)=1]| \\
&\leq \sum_y \mathsf{Pr}[Y=y] \cdot \max_P |\mathsf{Pr}[P(X_y,\Theta,y)=1] - \mathsf{Pr}[P(X'_y,\Theta'_y,y)=1]| \\
&\leq \sum_y \mathsf{Pr}[Y=y] \cdot \epsilon \\
&= \epsilon \sum_y \mathsf{Pr}[Y=y] \\
&= \epsilon.
\end{aligned}$$

Hence, it follows that

$$H_{\min}^{\varepsilon}(X_Y|\Theta, Y) \geq n\left(\frac{1}{2} - 2\lambda\right).$$

□

We will use this corollary in the following way. Assume that ρ is some quantum state, and by performing a partial measurement on ρ we obtain a measurement outcome Y (that follows a classical distribution depending on ρ and the measurement operator) and a residual state ρ_Y. Then we can equivalently first sample Y and then prepare the state ρ_Y depending on Y. Hence, we can treat Y in Lemma 9 as the outcome of a partial measurement of a state ρ, and X as the measurement of the residual state ρ_Y in basis Θ.

Experiment 1 *Let C be the challenger and let $\mathcal{A}$ be a computationally unbounded quantum adversary with the restriction that the quantum memory has to be completely measured in the transition from step 2 to step 3. They play the following experiment $\mathsf{Exp}_1(\mathcal{A})$:*

1. *C samples $\mathbf{x} \in \{0,1\}^n, \boldsymbol{\theta} \in \{0,1\}^n$ and creates the state $|\phi\rangle = H^{\otimes_i \theta_i}|\mathbf{x}\rangle$. The state $|\phi\rangle$ is sent to $\mathcal{A}$.*
2. *$\mathcal{A}$ measures the state $|\phi\rangle$.*
3. *C sends the basis choice $\boldsymbol{\theta}$ to $\mathcal{A}$.*
4. *$\mathcal{A}$ outputs a classical string y.*
5. *Output (x, y, θ).*

Experiment 2 *Let C be the challenger and let $\mathcal{B}$ be a computationally unbounded quantum adversary with the restriction that the quantum memory has to be completely measured in the transition from step 1 to step 2. They play the following experiment $\mathsf{Exp}_2(\mathcal{B})$:*

1. *$\mathcal{B}$ generates an n-qubit quantum state and sends it to C. $\mathcal{B}$ may only retain classical memory.*
2. *C samples $\boldsymbol{\theta} \in \{0,1\}^n$. If $\theta_i = 0$, C measures the i-th qubit in the computational basis, if $\theta_i = 1$, C measures in the Hadamard basis. Let $\mathbf{x}$ be the measurement outcome.*
3. *C sends the basis choice $\boldsymbol{\theta}$ to $\mathcal{B}$.*
4. *$\mathcal{B}$ outputs a classical string y.*
5. *Output (x, y, θ).*

Lemma 10. *Let $\mathcal{A}$ be an adversary in Experiment 1, then there exists an adversary $\mathcal{B}$ such that*

$$\mathsf{Exp}_1(\mathcal{A}) \equiv \mathsf{Exp}_2(\mathcal{B})$$

Proof. To show Lemma 10 we introduce two intermediate hybrids.

Hybrid 0. Let Hybrid 0 be Experiment 1.

Hybrid 1. In this hybrid the challenger creates n EPR pairs instead of Wiesner states. $\mathsf{Hyb1}(\mathcal{A})$:

1. C generates n EPR pairs and sends one half of each to $\mathcal{A}$.
2. C samples $\boldsymbol{\theta} \in \{0,1\}^n$. If $\theta_i = 0$, C measures the remaining half in the computational basis, if $\theta_i = 1$, C measures in the Hadamard basis. Let $\mathbf{x}$ be the measurement outcome.
3. $\mathcal{A}$ has to measure his state.
4. C sends the basis choice $\boldsymbol{\theta}$ to $\mathcal{A}$.
5. $\mathcal{A}$ outputs a classical string y.
6. Output (x, y, θ).

Claim. $\mathsf{Exp}_1(\mathcal{A}) \equiv \mathsf{Hyb1}(\mathcal{A})$

Proof. First note that the measurement of one bit of an EPR pair in both the computational or Hadamard basis gives $x_i = 0$ or $x_i = 1$ with probability $\frac{1}{2}$ each. Each qubit is measured separately, therefore the distribution of $\mathbf{x}$ is equivalent to choosing $\mathbf{x} \in \{0,1\}^n$ uniformly at random.

Secondly, $\mathcal{A}$ cannot distinguish between receiving one qubit of an EPR pair, where the other half measured in the basis $\boldsymbol{\theta}$, or a random Wiesner state created with basis choice $\boldsymbol{\theta}$ since the partial density matrices are the same.

Let

$$\rho_W = \sum_{\substack{\boldsymbol{\theta} \in \{0,1\}^n \\ x \in \{0,1\}^n}} p_x p_\theta \bigotimes_{i \in [n]} \mathbf{H}^{\theta_i} |x_i\rangle\langle x_i| \mathbf{H}^{\theta_i}$$

denote the state that C sends in Hybrid 0 where the choice over $\mathbf{x}$ and $\boldsymbol{\theta}$ is uniformly random and $p_x = \frac{1}{2^n}, p_\theta = \frac{1}{2^n}$.

Let $\rho_{EPR} = \bigotimes_{i \in [n]} |\phi^+\rangle\langle\phi^+|$ where $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ is an EPR pair. The challenger keeps the first qubit of each EPR pair and applies a measurement in the basis $\boldsymbol{\theta'} \in \{0,1\}^n$ on this qubit. Let $M_x^{\boldsymbol{\theta'}}$ denote a measurement in the basis specified by $\boldsymbol{\theta'}$ and M_x a measurement in the computational basis. Let $p_x = \frac{1}{2^n}, p_{\theta'} = \frac{1}{2^n}$.

Let ρ_C be the density matrix resulting from tracing out the first qubit of each EPR pair and applying the measurement.

$$
\begin{aligned}
\rho_C &= tr_C(\sum_{\substack{\boldsymbol{\theta'}\in\{0,1\}^n \\ x\in\{0,1\}^n}} p_{\theta'}(M_{x_i}^{\boldsymbol{\theta'}}\otimes\mathbf{I})\rho_{EPR}(M_{x_i}^{\boldsymbol{\theta'}}\otimes\mathbf{I})^\dagger) \\
&= tr_C(\sum_{\substack{\boldsymbol{\theta'}\in\{0,1\}^n \\ x\in\{0,1\}^n}} p_{\theta'}\bigotimes_{i\in[n]}(M_{x_i}^{\boldsymbol{\theta'}}\otimes\mathbf{I})\frac{1}{2}(|0\rangle|0\rangle+|1\rangle|1\rangle)(\langle 0|\langle 0|+\langle 1|\langle 1|)(M_{x_i}^{\boldsymbol{\theta'}_i}\otimes\mathbf{I})^\dagger) \\
&= tr_C(\sum_{\substack{\boldsymbol{\theta'}\in\{0,1\}^n \\ x\in\{0,1\}^n}} p_{\theta'}\bigotimes_{i\in[n]}(M_{x_i}\otimes\mathbf{I})\frac{1}{2}(\mathbf{H}^{\boldsymbol{\theta'}_i}|0\rangle|0\rangle+\mathbf{H}^{\boldsymbol{\theta'}_i}|1\rangle|1\rangle)(\langle 0|\mathbf{H}^{\boldsymbol{\theta'}_i}\langle 0|+\langle 1|\mathbf{H}^{\boldsymbol{\theta'}_i}\langle 1|)(M_{x_i}\otimes\mathbf{I})^\dagger) \\
&= tr_C(\sum_{\substack{\boldsymbol{\theta'}\in\{0,1\}^n \\ x\in\{0,1\}^n}} p_{\theta'}\bigotimes_{i\in[n]}(M_{x_i}\otimes\mathbf{I})\frac{1}{2}(|0\rangle\mathbf{H}^{\boldsymbol{\theta'}_i}|0\rangle+|1\rangle\mathbf{H}^{\boldsymbol{\theta'}_i}|1\rangle)(\langle 0|\langle 0|\mathbf{H}^{\boldsymbol{\theta'}_i}+\langle 1|\langle 1|\mathbf{H}^{\boldsymbol{\theta'}_i})(M_{x_i}\otimes\mathbf{I})^\dagger) \\
&= tr_C(\sum_{\substack{\boldsymbol{\theta'}\in\{0,1\}^n \\ x\in\{0,1\}^n}} p_{\theta'}\bigotimes_{i\in[n]}\frac{1}{2}|x_i\rangle\langle x_i|\otimes\mathbf{H}^{\boldsymbol{\theta'}_i}|x_i\rangle\langle x_i|\mathbf{H}^{\boldsymbol{\theta'}_i}) \\
&= \sum_{\substack{\boldsymbol{\theta'}\in\{0,1\}^n \\ x\in\{0,1\}^n}} p_{\theta'}p_x\bigotimes_{i\in[n]}\frac{1}{2}\mathbf{H}^{\boldsymbol{\theta'}_i}|x_i\rangle\langle x_i|\mathbf{H}^{\boldsymbol{\theta'}_i}
\end{aligned}
$$

Therefore the states ρ_W and ρ_C are the same and consequently the distribution of the measurement outcome on $\mathcal{A}$'s side has the same distribution.

To conclude, $(X_0, Y_0, \Theta_0) = (X_1, Y_1, \Theta_1)$ where (X_0, Y_0, Θ_0) is the output distribution of Hybrid 0 and (X_1, Y_1, Θ_1) is the output distribution of Hybrid 1. □

Hybrid 2. In Hybrid 2 we define an adversary $\mathcal{B}$ that creates the EPR pairs and uses $\mathcal{A}$ as a subroutine. $\mathsf{Hyb2}(\mathcal{B})$:

1. $\mathcal{B}$ honestly generates n EPR pairs and sends one half of each to C. He gives the remaining state to $\mathcal{A}$.
2. $\mathcal{A}$ has to measure the remaining state.
3. C samples $\boldsymbol{\theta} \in \{0,1\}^n$. If $\theta_i = 0$, C measures in the computational basis, if $\theta_i = 1$, C measures in the Hadamard basis. Let $\mathbf{x}$ be the measurement outcome.
4. C sends the basis choice $\boldsymbol{\theta}$ to $\mathcal{B}$ which he forwards to $\mathcal{A}$.
5. $\mathcal{A}$ outputs a classical string y which $\mathcal{B}$ outputs.
6. Output (x, y, θ).

Claim. Let $\mathcal{B}$ be the adversary in Hybrid 2, then $\mathsf{Hyb2}(\mathcal{B}) \equiv \mathsf{Hyb1}(\mathcal{A})$

Proof. The state shared between $\mathcal{A}$ and C in Hybrid 2 is the same as the state in Hybrid 1. $\mathcal{B}$ simulates Hybrid 1 to $\mathcal{A}$ up to the fact that it is not the challenger that creates the EPR pairs. Due to the symmetry of an EPR pair it does not

matter which party creates the EPR pairs. Therefore, it follows that C outputs a x, θ and $\mathcal{A}$ outputs a y which follow the same distribution as in Hybrid 1.

To conclude, $(X_1, Y_1, \Theta_1) = (X_2, Y_2, \Theta_2)$ where (X_1, Y_1, Θ_1) is the output distribution of Hybrid 1 and (X_2, Y_2, Θ_2) is the output distribution of Hybrid 2.

Furthermore, Hybrid 2 is a special case of Experiment 2. Therefore, we have shown that there exists for every $\mathcal{A}$ an adversary $\mathcal{B}$ such that $\mathsf{Exp}_1(\mathcal{A}) \equiv \mathsf{Exp}_2(\mathcal{B})$. □

□

Now we can prove Lemma 7 by combining the previous results.

Proof. Let (X, Y, Θ) be defined as in Lemma 7 and let $\mathcal{A}$ be an adversary in Experiment 1. The distribution of Experiment 1 corresponds to the task described in Lemma 7.

Due to Lemma 10 we know there exists an adversary $\mathcal{B}$ in Experiment 2 which induces a distribution (X', Y', Θ') such that

$$(X, Y, \Theta) = (X', Y', \Theta')$$

Now, given a smooth min-entropy bound for X' conditioned on Y', Θ' we know that it must also hold for X conditioned on Y, Θ since the distributions are the same.

We can apply the smooth min-entropy bound of Lemma 9. Since the Lemma holds for an adversary creating an arbitrary quantum state, it also holds for the adversary $\mathcal{B}$.

$$\begin{aligned} H_{\min}^{\varepsilon}(X|Y, \Theta) &= H_{\min}^{\varepsilon}(X'|Y', \Theta') \\ &\geq n\left(\frac{1}{2} - 2\lambda\right) \end{aligned}$$

□

4.1 Min-Entropy Given Quantum Memory

In this section we analyse Experiment 1 (cf. Experiment 1) in the case, that the adversary can keep a quantum state in his memory. The memory is bounded in the number of qubits that can be stored. We state a simplified version of the chain rule for smooth min-entropy from [59]. The derivation of this corollary appears in [61, Corollary 2.25].

Corollary 1. *(Chain rule for smooth min-entropy [59]) Let X and Y be classical random variables and let Q be a quantum register.*

$$H_{min}^{\varepsilon}(X|Y, Q) \geq H_{min}^{\varepsilon}(X|Y) - H_{max}(Q)$$

Lemma 11. *Let $|\psi\rangle$ be a quantum state that encodes $x \xleftarrow{\$} \{0,1\}^n$ using Wiesner coding. Let Θ be a random variable denoting the basis choice and let X be a random variable denoting the choice of the string x. An arbitrary measurement is performed on $n-q$ bits of the state, where $0 \leq q \leq n$. Let Q be the remaining quantum state and let the outcome of the measurement be denoted as $Y_{x,\theta}$. After the measurement is applied the basis choice Θ is revealed. Then the min-entropy of x conditioned on the measurement outcome, the basis choice and the remaining quantum state Q is:*

$$H^{\varepsilon}_{min}(X|Y_{x,\theta},\Theta,Q) \geq n\left(\frac{1}{2}-2\lambda\right)-q$$

where $\varepsilon = exp\left(-\frac{\lambda^2 n}{32(2-\log(\lambda))^2}\right)$ and $0<\lambda<\frac{1}{2}$.

Proof. First we apply the chain rule (Corollary 1) and then we apply Lemma 7 to obtain

$$\begin{aligned} H^{\varepsilon}_{\min}(X|Y_{x,\theta},\Theta,Q) &\geq H^{\varepsilon}_{\min}(X|Y_{x,\theta},\Theta) - H_{\max}(Q) \\ &= H^{\varepsilon}_{\min}(X|Y_{x,\theta},\Theta) - q \\ &\geq n\left(\frac{1}{2}-2\lambda\right)-q\,, \end{aligned}$$

where we have used that the max-entropy of a q-qubit state is bounded by q. □

5 Quantum Universal Composability with Decoherence

In this section, we introduce the notion of everlasting quantum UC security with decoherence as well as its properties. Then, we construct a composable commitment scheme in the $\mathcal{F}_{\mathsf{CRS}}$- and (programmable) quantum random oracle-hybrid model that is secure under our notion. Using this commitment scheme, we construct protocols for oblivious transfer as well as general MPC with (composable) long-term security.

5.1 Introduction to the Model

Security Notion and Framework. To capture (quantum) composable everlasting security, *i.e.* security a setting where the adversary is first computationally bounded, but becomes unbounded after the execution has finished, Unruh [66] has proposed the *everlasting quantum UC* framework and notion. The general idea is as follows: In an online phase, all entities like the environment, the adversary as well as the protocol parties are efficient, just like with standard UC security. After the execution has finished, the environment's state is traced out. This state may contain all information about the execution that the environment has seen, for example the parties' inputs and outputs as well as all communication

observed by the adversary. For a protocol π to everlasting-quantum-UC-emulate a protocol ϕ, we require that the trace distance between the environment's state in the execution with π and the adversary and the environment's state in the execution with ϕ and the simulator is negligible. In particular, this implies that the security (after the online phase) does not and cannot rely on *any* hard problem.

To capture security in our setting, we need to adjust the notion of everlasting quantum UC.

Incorporating Random Oracles. The standard notion of (quantum) long-term or everlasting composable security [66, 56] only considers the environment's final view or state. However, it does not, for example, include internal state of ideal functionalities that the environment has not (indirectly) observed. Depending on the used ideal functionalities, such a security notion may not meaningfully capture long-term security [49] because important information is hidden by the model. Consequently, a variant of long-term security has been proposed by Magri et al. [49] that extends the (non-quantum) UC machine model to include an additional *long-term output tape*. The execution experiment is modified such that after the execution has stopped, the adversary is activated once again on all long-term output tapes as input. Subsequently, it outputs a string a. The experiment's output is modified to include a. Via this mechanism, security even with knowledge of internal state of *e.g.* ideal functionalities can be meaningfully captured, resulting in a strengthened notion of long-term security.

The approach of Magri et al. [49] is not directly applicable to our setting, as they consider long-term output tapes with content of polynomial length only. In contrast, the value table of a random oracle with super-polynomial domain and co-domain cannot be efficiently represented. Thus, we take a slightly different approach, tailored to the case of (programmable) quantum random oracles. To this end, we extend the experiment to incorporate a special entity $\mathcal{RO}$, which captures multiple (inefficient) random oracles. At the end of the execution, the (still efficient) adversary may program the random oracles at a polynomial number of positions. Finally, the (possibly super-polynomial) value tables of $\mathcal{RO}$ are included in the execution's output. This ensures that all entities except the experiment remain efficient.

Modeling Decoherence. Apart from capturing (programmable) random oracles, we also want to model the setting of *quantum decoherence*. To this end, we consider an efficient quantum environment in the online phase like with standard everlasting quantum UC security. To model the decoherence after the execution, we restrict the class of admissible environments to environments that, at the end of the execution, hold a quantum state of at most size q, where q is a parameter. This final quantum state can be chosen arbitrarily by the environment.

We closely follow the Everlasting Quantum UC framework due to Unruh [66] as well as the established notion of everlasting quantum UC security. We remark that the notation in [66] is different from the standard UC one [22]. We refer the interested reader to [66] for an introduction to Everlasting Quantum UC.

Changes to the Network Execution. Starting with the network execution introduced in [66], we introduce an additional (inefficient) machine $\mathcal{RO}$ that captures a polynomial number of (quantum) random oracles that can be accessed by protocol parties as well as the adversary. We use $\mathcal{RO}(\mathsf{id}, (X, Y), |\phi\rangle)$ to denote that $\mathcal{RO}$ is queried for ID id, domain X and codomain Y with quantum state $|\phi\rangle$. If $|\phi\rangle$ encodes a single classical value x, we will also write x instead of $|\phi\rangle$.

At the end of the execution, the adversary is activated once again and may provide (without further communication with the environment) lists containing an ID id^* as well as a list of tuples (x_i, y_i). If a random oracle with ID id^* exists, is then evaluated on its domain, resulting in its full value table, which is then programmed to contain the values (x_i, y_i) provided by the adversary. The value tables are then stored in the register $\mathcal{H}^{class}$ of $\mathcal{RO}$, which later on becomes part of the experiment's output.

We stress that allowing the adversary to program the random oracle at the end of the execution does not negatively affect the security of honest parties during the online phase, where the random oracle behaves completely honest. Intuitively, properties such as the soundness of a proof scheme or the binding property of a commitment scheme, which may in principle be affected by the programming, are meaningless after the execution has finished.

We call the framework resulting from the above changes the *Everlasting Quantum UC with Decoherence* framework.

With the above changes of the execution experiment at hand, we define a random variable capturing the environment's state at the end of the execution as well as the value table of the random oracle (for the specified session).

Definition 13 (LTState**).** *Let N be a network. Let* $\mathrm{LTState}_N(\kappa, a) = \mathcal{H}^{state}_{\mathtt{environment}} \otimes \mathcal{H}^{class}_{\mathcal{RO}}$ *be the density operator consisting of the traced-out systems* $\mathcal{H}^{state}_{\mathtt{environment}}$ *(*i.e. *the environment's state) and* $\mathcal{H}^{class}_{\mathcal{RO}}$ *from s in the network N. Here, s denotes the final state of the execution of N on input* $(1^\kappa, a)$ *according to Definition 17.*

In contrast to the definition of [66], we are interested in environments whose quantum state's size is bounded by some parameter $q \in \mathbb{N}$ at the end of the execution, capturing the setting of quantum decoherence. To this end, we define q-quantum-bounded environments.

Definition 14 (q-Quantum-Bounded Environment). *Let $q \in \mathbb{N}$. We say that an environment $\mathcal{Z}$ is q-quantum-bounded if, before returning* $(\mathtt{environment}, \varepsilon, out)$*, $\mathcal{Z}$ measures all but the first q qubits of* $\mathcal{H}^{state}_{\mathtt{environment}}$ *in the computational basis.*

Protocol Emulation. Based on the above definitions, we define the notion of *q-Everlasting Quantum-UC Security with Decoherence*. This notion accounts for q-quantum bounded environments as well as additional information in the experiment's output.

Definition 15 (q-Everlasting Quantum-UC Security with Decoherence). *Let protocols π and ϕ be given. We say that π q-Everlasting Quantum-UC-emulates ϕ with Decoherence (short q-eqUC-D-emulates) iff for every set $C \subseteq parties_\pi$ and for every quantum-polynomial-time adversary $\mathcal{A}$, there is a quantum-polynomial-time simulator $\mathcal{S}$ such that for every q-quantum-bounded quantum-polynomial-time environment $\mathcal{Z}$, there exists a negligible function negl such that for all $\kappa \in \mathbb{N}$ and all $a \in \{0,1\}^*$, it holds that $TD(\text{LTState}_N(\kappa, a), \text{LTState}_{N'}(\kappa, a)) \leq negl(\kappa)$ where $N = \pi^C \cup \{\mathcal{Z}, \mathcal{A}\}$ and $N' = \phi^C \cup \{\mathcal{Z}, \mathcal{S}\}$.*

We now establish useful properties of our notion. In particular, we prove that it is reflexive, transitive, features completeness of the dummy adversary and is closed under general concurrent (*i.e.* universal) composition.

Proposition 1 (Reflexivity, Transitivity). *q-everlasting quantum-UC security with decoherence is reflexive and transitive.*

For the proof, see Appendix B.

In Definition 17, we change the execution experiment with the introduction of a special entity $\mathcal{RO}$ as well as a final phase where the adversary is activated once again. In its register $\mathcal{H}^{class}$, it may find a list of tuples prefixed by an ID as well as values (x_i, y_i), which are provided by the environment. The adversary may arbitrarily modify its register, but not communicate with the environment anymore. Based on the register's content, the experiment will program the random oracles using the provided values. In the following, we specify the behavior of the dummy adversary in this experiment, which simply leaves $\mathcal{H}^{class}$ unchanged.

Definition 16 (Dummy Adversary). *In the online phase,* i.e. *before the last activation of the environment, the dummy adversary $\mathcal{D}$ behaves as defined in [66], except that it also forwards messages between the environment and $\mathcal{RO}$. On its last activation, it simply does nothing.*

In particular, if there is a message written in the register $\mathcal{H}^{class}$ of the dummy adversary, this message will be forwarded to $\mathcal{H}^{class}$ of $\mathcal{RO}$ as per Definition 17.

Like with standard UC security and everlasting quantum UC security, the dummy adversary is complete for our new notion.

Proposition 2 (Completeness of the Dummy Adversary). *Let $\mathcal{D}$ be the dummy adversary. Let π and ϕ be protocols. If π q-eqUC-D-emulates ϕ for $\mathcal{D}$, then π q-eqUC-D-emulates ϕ for every QPT adversary $\mathcal{A}$.*

For the proof, see Appendix B.

Theorem 7 (Composition Theorem). *Let π, ϕ and ρ be quantum-polynomial-time protocols. Assume that π q-eqUC-D-emulates ϕ. Then, ρ^π q-eqUC-D-emulates ρ^ϕ.*

In Theorem 7, ρ^ϕ denotes the protocol ρ that makes subroutine calls to the protocol ϕ. In ρ^π, these subroutine calls to ρ are replaced by calls to ϕ.[8] For the proof, see Appendix B. It is easy to see that protocols that are statistically quantum UC-secure [66] remain secure under our notion.

Proposition 3 (Compatibility with Everlasting Quantum UC Security). *Let π and ϕ be protocols such that π statistically quantum-UC-emulates ϕ. Then, π q-eqUC-D-emulates ϕ for any q.*

For the proof, see Appendix B.

5.2 Changes to the Execution

We give a formal definition of our changes to the execution. In particular, we extend the execution to include an entity $\mathcal{RO}$ that models multiple random oracles, each identified by an ID id, a domain X and a codomain Y. Special care has to be taken that $\mathcal{RO}(\mathsf{id},\cdot)$ is only used by exactly *one* protocol session, similar to the *subroutine respecting* property of standard UC security. To this end, we associate each random oracle with the session it was first called from. Calls from other sessions will be ignored. Looking ahead, this will be crucial to establish the composition theorem, as it allows to uniquely determine which simulator is responsible for each random oracle.

Definition 17 (Everlasting Quantum UC with Decoherence Execution). *The execution in our framework is defined as in [66], except with the following changes to the experiment:*

- *We introduce an additional (inefficient) machine $\mathcal{RO}$ with identity $\mathcal{RO}$ and Hilbert spaces $\mathcal{H}^{state}$, $\mathcal{H}^{class}$ and $\mathcal{H}^{quant}$.*
- *Initially, $\mathcal{H}^{class}$ contains an empty list $\mathcal{L}=\emptyset$.*
- *Protocol parties with session ID sid and the adversary may communicate with $\mathcal{RO}$ through the usual mechanism. Encoded in the receiver ID id_{rcpt} are an ID id as well as an* efficiently samplable *and* efficiently recognizable *domain X and codomain Y.*
- *For a message to $\mathcal{RO}$ with receiver ID $id_{rcpt}=(\mathsf{id},X,Y)$ and $\mathcal{H}^{quant}=|\phi\rangle$, we write $(\mathcal{RO}(\mathsf{id},(X,Y),|\phi\rangle)$.*
- *Messages $(\mathsf{id},(X,Y),|\phi\rangle)$ to $\mathcal{RO}$ are handled as follows:*
  - *Let id_{snd} be the sender's ID. If $id_{snd}\neq\mathcal{A}$: Let s denote the sender's (non-extended) session. If $\mathcal{RO}(\mathsf{id},\cdot)$ has been previously queried from a session $s'\neq s$, ignore this message. Otherwise, set s as the session of $\mathcal{RO}(\mathsf{id},\cdot)$ and continue. Else, if $id_{snd}=\mathcal{A}$, we assume that the adversary includes a session s in id_{rcpt}. If $\mathcal{RO}(\mathsf{id},\cdot)$ has been previously queried from a session $s'\neq s$, ignore the message.*

[8] The notion of protocol composition in [66] is much simpler than the current definition of the composition operator in standard UC [22], which addresses many important subtleties. Nevertheless, we have chosen to adhere to the notion of [66] because we consider the task of adapting [66] to the latest changes of Universal Composability out of scope for this paper. However, we stress that our notion is universally composable according to the most recent definition.

- *Let* id *be the ID resp.* X *and* Y *be domain and codomain encoded in* id_{rcpt} *(which is classical). If* $(\mathsf{id}, (X', Y')) \in \mathcal{L}$*, but* $X' \neq X$ *or* $Y \neq Y$*, ignore the message. Otherwise, sample a function* $f_{\mathsf{id},(X,Y)}$ *uniformly at random from the family of functions with the specified domain and codomain and add* $(\mathsf{id}, (X, Y))$ *to* $\mathcal{L}$*.*
- *If* $(\mathsf{id}, (X, Y)) \in \mathcal{L}$*, compute the answer* $|\phi\rangle = \sum_{x,u} \alpha_{x,u}|x, u\rangle$ *as* $\sum_{x,u} \alpha_{x,u}|x, u \oplus f_{\mathsf{id},(X,Y)}(x)\rangle$*.*

– *At the end of the experiment, the adversary is activated once again on a message with sender ID* `final` *and classical part* m*, which is defined as follows:*
- *Let* m' *be the (measured) content of* $\mathcal{H}^{class}$ *of the environment. If* m' *specifies a list consisting of tuples* $(\mathsf{id}_j, (x_1^j, y_1^j), \ldots, (x_n^j, y_n^j))$*, where* $x_i^j \neq x_k^j$ *for all* $i \neq k$*, then* $m = m'$*.*
- *Otherwise,* m *is set as the empty word* ε*.*

– *Let* o' *be the (measured) content of* $\mathcal{H}^{class}$ *of the adversary. Copy* o' *to* $\mathcal{H}^{class}$ *of* $\mathcal{RO}$ *and activate* $\mathcal{RO}$*.*

– *On its last activation,* $\mathcal{RO}$ *evaluates all* $f_{\mathsf{id}^*,(X^*,Y^*)}$ *for* $(\mathsf{id}^*, (X^*, Y^*)) \in \mathcal{L}$ *on their respective domains, obtaining their (classical) value tables. Then,* $\mathcal{RO}$ *reads its register* $\mathcal{H}^{class}$ *tries to interprets its content as a polynomial number of tuples* $(\mathsf{id}_j, (x_1^j, y_1^j), \ldots, (x_n^j, y_n^j))$*. For each tuple* (x_i, y_i)*, the value table for ID* id_j *(if existing in* $\mathcal{L}$*) is programmed to the value* y_i *at position* x_i *if* $x_i \in X$ *and* $y_i \in Y$*. Finally,* $\mathcal{H}^{class}$ *is adjusted to contain all value tables of all random oracles in* $\mathcal{L}$*, lexicographically sorted by their IDs.*

In order to simplify the notation, we use $\mathcal{RO}(\mathsf{id}, (X, Y), |\phi\rangle)$ to denote that $\mathcal{RO}$ is queried for ID id, domain X and codomain Y with quantum state $|\phi\rangle$. If $|\phi\rangle$ encodes a single classical value x, we will also write x instead of $|\phi\rangle$.

5.3 Ideal Functionalities

We state important ideal functionalities used in this paper. In line with [66], we assume classical input-output behavior.

We start with a definition of the functionality for commitments $\mathcal{F}_{\text{COM}}$. We state a variant of $\mathcal{F}_{\text{COM}}$ for bit commitments. The definition for string commitments is totally analogous.

The ideal functionality $\mathcal{F}_{\mathsf{CRS}}$ models a common reference string that is accessible by all parties.

The ideal functionality for zero-knowledge $\mathcal{F}_{\mathsf{ZK}}$ allows a prover P to prove the validity of a statement x to a verifier V relative to a relation R, ensuring that the prover knows an appropriate witness.

Functionality $\mathcal{F}_{\text{COM}}$

$\mathcal{F}_{\text{COM}}$ proceeds as follows, parameterized with a security parameter κ, running with a committer C and a receiver Rec and an adversary $\mathcal{S}$.

1. Upon receiving an input $(\texttt{commit}, sid, b)$ from C, where $b \in \{0,1\}$, record the value b and generate a public delayed output $(\texttt{committed}, sid)$ to Rec. Ignore subsequent `commit` inputs.
2. Upon receiving an input $(\texttt{unveil}, sid)$ from C, generate a public delayed output $(\texttt{unveil}, sid, b)$ to Rec if there has been a previously delivered `committed` output. Otherwise, ignore this input. Ignore subsequent `unveil` inputs.

Fig. 1: The ideal functionality for commitments $\mathcal{F}_{\text{COM}}$, adapted from [24].

Functionality $\mathcal{F}_{\mathsf{CRS}}$

$\mathcal{F}_{\mathsf{CRS}}$ proceeds as follows, parameterized with a security parameter κ, a family of efficiently samplable distributions $\{D_\kappa\}_{\kappa\in\mathbb{N}}$ and an adversary $\mathcal{S}$.

1. When activated for the first time on input $(\texttt{value}, sid \,\|\, \texttt{crs})$ by a party P, sample a value $d \leftarrow D_\kappa$ and generate a public delayed output $(\texttt{value}, sid, d)$ to P. Answer subsequent $(\texttt{value}, sid \,\|\, \texttt{crs})$ inputs from parties P' by generating a public delayed output $(\texttt{value}, sid, d)$ to P'.

Fig. 2: The ideal functionality for a common reference string $\mathcal{F}_{\mathsf{CRS}}$, adapted from [24].

Functionality $\mathcal{F}_{\mathsf{OT}}$

$\mathcal{F}_{\mathsf{OT}}$ proceeds as follows, parametrized by a security parameter κ, a sender P_A, a receiver P_B and an adversary $\mathcal{S}$.

1. When receiving a message $(\texttt{send}, sid, (\mu_0, \mu_1))$ from the sender P_B where $(\mu_0, \mu_1) \in \{0,1\}^l$ store (μ_0, μ_1).
2. When receiving a message $(\texttt{receive}, sid, b)$ from the receiver P_B, if (μ_0, μ_1) were already send, deliver output (sid, μ_b) to the receiver, otherwise send nothing.

Fig. 3: The ideal functionality for Oblivious Transfer $\mathcal{F}_{\mathsf{OT}}$, adapted from [26].

Functionality $\mathcal{F}_{\mathsf{ZK}}$

$\mathcal{F}_{\mathsf{ZK}}$ proceeds as follows, parameterized with a security parameter κ, a relation R, running with a prover P, a verifier V and an adversary $\mathcal{S}$.

1. Upon receiving input $(\texttt{ZK-prover}, sid, x, w)$ from P, do: If $R(x, w) = 1$, generate a public delayed output $(\texttt{ZK-proof}, sid, x)$ to V and halt. Otherwise, halt without output.

Fig. 4: The ideal functionality for zero-knowledge $\mathcal{F}_{\mathsf{ZK}}$, adapted from [26].

6 Composable Everlasting Commitment Scheme

In this section, we present a commitment scheme that is secure according to our notion of everlasting quantum-UC-security with decoherence. Our protocol extends the work from Brassard et al. [18], which claimed the statistical binding *and* statistical hiding property, a claim that we now know is impossible to achieve [53]. The unconditional binding property was shown to be false by Mayers [52]. We recall the protocol and attack:

Commitment protocol of BCJL'93 [18]. The protocol makes use of a linear $[N, K, D]$-code $\mathcal{C}$. To commit to a bit $\boldsymbol{\mu}$, the sender chooses a random value $\mathbf{r}$ and a codeword $\mathbf{c}$ such that the inner product $\langle \mathbf{r}|\mathbf{c}\rangle = \boldsymbol{\mu}$. She then chooses a random basis vector $\boldsymbol{\theta} \in \{0,1\}^n$ and creates the state $|\phi\rangle = \bigotimes_i H^{\boldsymbol{\theta}_i}|c_i\rangle$. She sends the state $|\phi\rangle$ along with $\mathbf{r}$. The receiver measures the state $|\phi\rangle$ in a randomly chosen basis $\boldsymbol{\theta}' \in \{0,1\}^n$ and obtains y.

In the unveil phase, the committer sends $(\boldsymbol{\theta}, \mathbf{c}, \boldsymbol{\mu})$. The receiver checks for positions where $\theta_i = \theta'_i$ if $c_i = y_i$ and that $\mathbf{c}$ is a codeword and that $\langle \mathbf{r}|\mathbf{c}\rangle = \boldsymbol{\mu}$.

Intuitively, the scheme is statistically hiding based on the uncertainty relations for Wiesner coding: The receiver has no way of extracting the bits of $\mathbf{c}$ without knowing the basis in which they were encoded. Brassard *et al.* argued the statistical binding property on grounds of the following two statements which are by themselves not wrong. However, they do not include every possible cheating strategy for the committer.

1. In the unveil phase, $\mathbf{c}'$ has to pass the check that it is a codeword. Any codewords differ in at least d bits.
2. If the sender has to lie about at least d positions of $(\boldsymbol{\theta}, \mathbf{c})$ to unveil a *different* message, the receiver is very likely to catch this in the consistency check.

It was not taken into account that the sender could actually stay entangled with $|\phi\rangle$ and delay the measurement of this subsystem and thereby the choice of $\boldsymbol{\theta}$ until the unveil phase. Therefore, unveiling to either $\boldsymbol{\mu} = 0$ or $\boldsymbol{\mu} = 1$ is still possible in the unveil phase.

Our protocol. To circumvent the issue with the BCJL'93 [18] protocol, we require the committer to additionally commit to the basis $\boldsymbol{\theta}$. We instantiate the commitment using a random oracle. Since we prove security in the UC model, we additionally need to show extractability. Therefore, we encrypt the random oracle query using a PKE scheme and extract the value from the PKE. The public key of the PKE scheme is part of the common reference string.

Now, if the receiver were unbounded, he could extract the value $\boldsymbol{\theta}$ from the message. Hence, we require the receiver to be initially computationally bounded. After the quantum storage bound applies, the receiver may become computationally unbounded. If the receiver could hold on to the quantum state until he becomes computationally unbounded (allowing them to learn the basis vectors $\boldsymbol{\theta}$), the hiding property of the commitment scheme would be trivial to break.

Construction 1 (Commitment Scheme $\pi_{\mathrm{COM}} = \pi_{\mathrm{COM}}(q)$). *Let $\kappa \in \mathbb{N}$ be a security parameter and let $q \in \mathbb{N}$ be a quantum storage bound. Let C be an linear $[N, (1-\gamma)N]$-code with parity check matrix $\mathbf{PC}$ which can efficiently decode from αN of errors (for some small constants $\gamma, \alpha > 0$). Assume that $N \geq \mathsf{poly}(\kappa) + q$. Let PKE be a perfectly correct public key encryption scheme with (efficiently checkable) message space $\mathcal{M} = \{0,1\}^{N+l+d+(N-K)+z}$ and (efficiently checkable) randomness space $\mathcal{R}$. The message space of the commitment scheme is $\{0,1\}^d$. Let $\mathsf{Ext} : \{0,1\}^l \times \{0,1\}^N \to \{0,1\}^d$ be a strong (w, ε)-randomness extractor with $w \leq N\left(\frac{1}{2} - 2\lambda - \gamma\right) - q$. Let $X = \{0,1\}^{N+l+d+(N-K)+z}$ and $Y = \{0,1\}^m$, where $m \geq N + l + d + (N - K)$.*

Commit Phase.

1. C*: On input* $(\mathtt{commit}, sid, \mu)$*,* $\mu \in \{0,1\}^d$*, send* $(\mathtt{value}, sid \,\|\, \mathtt{crs})$ *to* $\mathcal{F}_{\mathsf{CRS}}$ *parameterized with the distribution* $\{\mathsf{pk}\}_{(\mathsf{pk},\mathsf{sk}) \leftarrow \mathsf{PKE.Gen}(1^\kappa)}$ *to obtain* pk*.*
2. C*: Sample* $\boldsymbol{\theta} \xleftarrow{\$} \{0,1\}^N, \mathbf{x} \xleftarrow{\$} \{0,1\}^N$ *uniformly at random, set* $\mathsf{ct}_0 = \mathbf{PC} \cdot \mathbf{x}$ *and compute the quantum state* $|\phi\rangle = \bigotimes_{i=1}^N H^{\theta_i} |x_i\rangle$*. Sample* $r \xleftarrow{\$} \{0,1\}^{N+l+d+(N-K)+z}$*,* $s \xleftarrow{\$} \{0,1\}^l$ *uniformly at random and compute* $\boldsymbol{\sigma} = \mathsf{Ext}(s, \mathbf{x}) \oplus \mu$ *and* $h = \mathcal{RO}(sid, (X, Y), r) \oplus (\boldsymbol{\theta} \,\|\, s \,\|\, \boldsymbol{\sigma} \,\|\, \mathsf{ct}_0)$ *and* $\mathsf{ct}_1 \leftarrow \mathsf{PKE.Enc}(\mathsf{pk}, r)$*. Let r' denote the randomness used to generate the ciphertext. Send* $(\mathtt{commit}, sid, |\phi\rangle, h, \mathsf{ct}_1)$ *to the receiver* Rec*.*
3. Rec*: Receive* $(\mathtt{commit}, sid, |\phi\rangle, h, \mathsf{ct}_1)$ *from* C*. Sample* $\boldsymbol{\theta}' \xleftarrow{\$} \{0,1\}^N$ *uniformly at random and measure* $|\phi_i\rangle$ *in the computational basis if* $\theta'_i = 0$ *and in the Hadamard basis if* $\theta'_i = 1$*. Let* $\mathbf{y} \in \{0,1\}^N$ *denote the result. Output* $(\mathtt{committed}, sid)$*.*

Unveil Phase.

1. C*: On input* $(\mathtt{unveil}, sid)$*, send* $(\mathtt{unveil}, sid, \boldsymbol{\theta}, s, r, \mathbf{x}, \mu, r')$ *to the receiver.*
2. Rec*: Receive* $(\mathtt{unveil}, sid, \boldsymbol{\theta}, s, r, \mathbf{x}, \mu, r')$ *from* C*.*
3. Rec*: Send* $(\mathtt{value}, sid \,\|\, \mathtt{crs})$ *to* $\mathcal{F}_{\mathsf{CRS}}$ *parameterized with the distribution* $\{\mathsf{pk}\}_{(\mathsf{pk},\mathsf{sk}) \leftarrow \mathsf{PKE.Gen}(1^\kappa)}$ *to obtain* pk*. If* $r \notin \mathcal{M}$ *or* $r' \notin \mathcal{R}$ *or* $\mathsf{PKE.Enc}(\mathsf{pk}, r; r') \neq \mathsf{ct}_1$*, halt.*
4. Rec*: For* $i = 1, \ldots, N$*: If* $\theta_i = \theta'_i$*, assert that* $x_i = y_i$*. Assert that* $\mathsf{ct}_0 = \mathbf{PC} \cdot \mathbf{x}$*,* $h = \mathcal{RO}(sid, (X, Y), r) \oplus (\boldsymbol{\theta} \,\|\, s \,\|\, \boldsymbol{\sigma} \,\|\, \mathsf{ct}_0)$ *and* $\boldsymbol{\sigma} = \mathsf{Ext}(s, \mathbf{x}) \oplus \mu$*. If any check fails, halt. Otherwise, output* $(\mathtt{unveil}, sid, \mu)$*.*

In the above protocol, $\mathcal{RO}$ is an interface of the execution experiment that provides random oracles (see Section 5.1).

Theorem 8. *If* PKE *is perfectly correct and IND-CPA-secure against quantum polynomial-time adversaries, then* $\pi_{\mathrm{COM}}(q)$ *in Construction 1 q-eqUC-D-realizes* $\mathcal{F}_{\mathrm{COM}}$ *under static malicious corruptions in the QROM.*

Proof. In order to prove Theorem 8, we state a simulator for the dummy adversary, which is complete (Proposition 2). For the sake of better readability, we state different simulators for each possible corruption. These individual simulators can be easily combined to a common one.

Corrupted Committer, Honest Receiver. First, note that the secret μ of the commitment is completely defined by $\boldsymbol{\sigma}$, s and $\mathbf{x}$. In order to extract the commitment, it thus suffices to obtain these values. To this end, we first decrypt the ciphertext ct_1, which allows us to unmask σ, s, ct_0 as well as (presumptive) bases used to encode $\mathbf{x}$ in the quantum state $|\phi\rangle$. By measuring $|\phi\rangle$ in the extracted bases, we obtain $\mathbf{x}$, perform an error correction step and can reconstruct μ.

Definition 18 (Simulator, Corrupted Committer, Honest Receiver). *Initially, set extfail* $= \texttt{false}$.

1. *Generate* $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{PKE.Gen}(1^\kappa)$. *Simulate* $\mathcal{F}_{\mathsf{CRS}}$ *by returning* pk *on input* $(\texttt{value}, sid \,\|\, \texttt{crs})$ *after confirmation by the environment for the delayed output.*
2. *Forward queries from and to* $\mathcal{RO}$ *like the dummy adversary.*
3. *Receive* $(\texttt{commit}, sid, |\phi\rangle, h, \mathsf{ct}_1)$ *from the environment as message to the honest receiver.*
4. *Let* $r^* = \mathsf{PKE.Dec}(\mathsf{sk}, \mathsf{ct}_1)$ *and parse* $h \oplus \mathcal{RO}(sid, (X, Y), r^*)$ *as* $(\boldsymbol{\theta}' \,\|\, s' \,\|\, \boldsymbol{\sigma}' \,\|\, \mathsf{ct}_0)$ *according to the protocol description.*
5. *If the decryption or the subsequent parsing fails, set extfail* $= \texttt{true}$*, sample* $\boldsymbol{\theta}' \xleftarrow{\$} \{0,1\}^N$ *uniformly at random and measure* $|\phi_i\rangle$ *in the computational basis if* $\theta'_i = 0$ *and in the Hadamard basis if* $\theta'_i = 1$. *Let* $\mathbf{x}^* \in \{0,1\}^N$ *denote the result. Send* $(\texttt{commit}, sid, 0)$ *to* $\mathcal{F}_{\mathrm{COM}}$ *as input of the corrupted committer and allow the public delayed output of* $\mathcal{F}_{\mathrm{COM}}$ *for the receiver. Continue with item 10.*
6. *Otherwise, measure the state* $|\phi\rangle$ *in the basis* $\boldsymbol{\theta}'$ *to obtain* $\mathbf{x}^*$. *If* $\mathbf{x}^*$ *has a syndrome* $\mathsf{ct}_0^* := \mathbf{PC}\mathbf{x}^*$ *that differs from* ct_0*, we compute an alternative* $\mathbf{x}'$ *and save* $\mathbf{x}^*$ *for inclusion in a later check. Use the efficient error correction procedure of the linear error correcting code to compute* $\mathbf{x}'$ *such that* $ct_0 = \mathbf{PC}\mathbf{x}'$. *In case the error correction procedure outputs* $\perp$*, the simulator sets extfail* $= \texttt{true}$.
7. *Recompute a state* $|\psi\rangle = \otimes_i H^{\theta'_i}|x_i^*\rangle$ *and run the honest receiver's check using* $\mathbf{x}'$*: measure* $|\psi\rangle$ *in a random basis* $\tilde{\boldsymbol{\theta}}$ *to obtain* $\tilde{x}$ *and check for every* i *where* $\theta'_i = \tilde{\theta}_i$ *if* $x'_i = \tilde{x}_i$. *If the honest receiver would reject the state, set extfail* $= \texttt{true}$.
8. *Compute* $\mathsf{Ext}(s', \mathbf{x}') \oplus \boldsymbol{\sigma}' = \mu^*$.
9. *Send* $(\texttt{commit}, sid, \mu^*)$ *to* $\mathcal{F}_{\mathrm{COM}}$ *as input of the corrupted committer and allow the public delayed output of* $\mathcal{F}_{\mathrm{COM}}$ *for the receiver.*
10. *Receive* $(\texttt{unveil}, sid, \boldsymbol{\theta}, s, r, \mathsf{ct}_0, \mathbf{x}, \mu, r')$ *from the environment as unveil message.*
11. *For each* θ_i*, decide with probability* $1/2$ *to add it to a set* I *or to forget it.*
12. *Perform the following checks:*
    - *Check if* $\mathsf{ct}_0 = \mathbf{PC}\mathbf{x}$.
    - *Check if* $\mathbf{x} = \mathbf{x}'$
    - *Check if* $r \in \mathcal{M}$, $r' \in \mathcal{R}$ *and* $\mathsf{ct}_1 = \mathsf{PKE.Enc}(\mathsf{pk}, r; r')$.
    - *Check for every* $\theta_i \in I$ *if* $x_i^* = x_i$.

- *Check if* $h = \mathcal{RO}(sid, (X, Y), r) \oplus (\boldsymbol{\theta} \,\|\, s \,\|\, \boldsymbol{\sigma} \,\|\, \mathsf{ct}_0)$.
- *Check if* $\boldsymbol{\sigma} = \mathsf{Ext}(s, \mathbf{x}) \oplus \mu$.

13. *If extfail* $= \mathtt{true}$ *and the receiver would accept or if any of the checks fail, output a special error symbol* $\perp$*. Otherwise, send* $(\mathtt{unveil}, sid)$ *to* $\mathcal{F}_{\mathrm{COM}}$ *as input of the committer and allow the public delayed output of* $\mathcal{F}_{\mathrm{COM}}$ *for the receiver.*
14. *On its last activation,* $\mathcal{S}$ *behaves like the dummy adversary.*

Lemma 12. *If* PKE *is perfectly correct and* C *is a linear* $[N, K, D]$*-code that fulfills the properties of Definition 2, then* $\pi_{\mathrm{COM}}(q)$ *q-eqUC-D-realizes* $\mathcal{F}_{\mathrm{COM}}$ *for a corrupted committer under static malicious corruptions.*

Proof. In order to prove Lemma 12, we define the following hybrids.

- H_0: The (real) execution with $\pi_{\mathrm{COM}}(q)$ and the dummy adversary $\mathcal{D}$.
- H_1: The execution with an ideal functionality $\mathcal{F}_1$ that provides all inputs to the adversary and lets it determine all outputs. The simulator $\mathcal{S}_1$ performs the protocol on behalf of the honest receiver, making its output through $\mathcal{F}_1$. With respect to $\mathcal{RO}$, $\mathcal{S}_1$ behaves like the dummy adversary.
- H_2: The execution with $\mathcal{F}_2 = \mathcal{F}_1$ and a simulator $\mathcal{S}_2$. $\mathcal{S}_2$ is identical to $\mathcal{S}_1$, except that it decrypts the ciphertext ct_1. If the decryption fails or results in a different plaintext in the message space from the one the receiver would accept, it outputs a special error symbol $\perp_2$.
- H_3: The execution with $\mathcal{F}_3 = \mathcal{F}_2$ and a simulator $\mathcal{S}_3$. $\mathcal{S}_3$ is identical to $\mathcal{S}_2$, except that it also performs the measurement of item 6 to extract $\mathbf{x}^*$ and that it checks if the extracted string $\mathbf{x}^*$ can be corrected to a valid codeword $\mathbf{x}'$ (for syndrome ct_0) and tests if the honest receiver would accept as in item 7. If this check fails but the error syndrome consistency check is successful, it outputs a special error symbol $\perp_3$.
- H_4: The execution with $\mathcal{F}_4 = \mathcal{F}_3$ and a simulator $\mathcal{S}_4$. $\mathcal{S}_4$ is identical to $\mathcal{S}_3$, except that and additional check is added to the checks an honest receiver would perform as in item 12: it also checks if $\mathbf{x} = \mathbf{x}'$, where $\mathbf{x}$ is received from the corrupted committer and $\mathbf{x}'$ is the corrected codeword. If this check fails, it outputs a special error symbol $\perp_4$.
- H_5: The execution with $\mathcal{F}_5 = \mathcal{F}_4$ and a simulator $\mathcal{S}_5$. $\mathcal{S}_5$ is identical to $\mathcal{S}_4$, except that it extracts the committed value in item 8 and outputs a special error symbol $\perp_5$ if the receiver would accept a different value than the extracted one.
- H_6: The (ideal) execution with $\mathcal{F}_{\mathrm{COM}}$ and the simulator $\mathcal{S}$.

Let out_i denote the output of H_i, *i.e.* $\mathcal{H}^{state}_{\mathtt{environment}} \otimes \mathcal{H}^{class}_{\mathcal{RO}}$ in analogy to Definitions 13 and 17.

For each adjacent pair of hybrids H_i, H_{i+1}, we will prove that for every q-bounded efficient quantum environment, the trace distance of out_i and out_{i+1} is zero or negligible.

Claim. $\mathrm{TD}(\mathrm{out}_0, \mathrm{out}_1) = 0$.

Proof. The changes between H_0 and H_1 are only syntactical and do not affect the output distribution of the execution. □

Claim. If PKE is perfectly correct, then $\mathrm{TD}(\mathrm{out}_1, \mathrm{out}_2) = 0$.

Proof. out_1 and out_2 are identically distributed unless the simulator outputs $\perp_2$. Let $\mathrm{E}_\perp$ denote this event. By definition of the simulator in H_2, $\mathrm{E}_\perp$ only occurs if the decryption of ct_1 fails, but $\mathsf{ct}_1 = \mathsf{PKE.Enc}(\mathsf{pk}, r; r')$ and $r \in \mathcal{M}$ and $r' \in \mathcal{R}$ (relative to the values r, r' sent by the corrupted committer in the commit phase) or ct_1 decrypts to $m' \in \mathcal{M}$, but $\mathsf{ct}_1 = \mathsf{PKE.Enc}(\mathsf{pk}, r, r')$ and $r \neq m'$. As PKE is perfectly correct, it holds for all $\kappa \in \mathbb{N}$, all $m \in \mathcal{M}$ and all $r \in \mathcal{R}$ that $\mathsf{Pr}[m \neq \mathsf{PKE.Dec}(\mathsf{sk}, \mathsf{PKE.Enc}(\mathsf{pk}, m; r)) \mid (\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{PKE.Gen}(1^r)] = 0$. This implies that $\Pr[\mathrm{E}_\perp] = 0$ and the claim follows. □

Claim. If C is a linear $[N, (1-\gamma)N]$-code that fulfills the properties of Theorem 6, $\mathrm{TD}(\mathrm{out}_2, \mathrm{out}_3) \leq \mathit{negl}(\kappa)$.

Proof. $\mathcal{S}_3$ extracts the value $\mathbf{x}^*$ by measuring in the extracted basis and checks if $\mathbf{x}^*$ is a valid codeword for the given error syndrome. If the extracted value $\mathbf{x}^*$ fulfills the syndrome check, no abort occurs and the outputs of out_2 and out_3 are trace-indistinguishable.

If the extracted value $\mathbf{x}^*$ does not fulfill the syndrome check, we cannot immediately abort the simulation. The sender could create a quantum state where a few qubits differ from the later revealed $\mathbf{x}$ (which has to fulfill the consistency check regarding the error syndrome) and not be detected due to the measurement of the receiver in a random basis.

We first adjust $\mathbf{x}^*$ to a codeword with valid error syndrome: Decode $\mathbf{x}^*$ to obtain an m. If the decoding was successful, encode it freshly to obtain $\tilde{\mathbf{x}}$. Then, use ct_0 to introduce errors to $\tilde{\mathbf{x}}$ to obtain $\mathbf{x}'$ with $\mathbf{P}\mathbf{C}\mathbf{x}' = \mathsf{ct}_0$.

Since the honest receiver measures only approximately half of the qubits in the correct basis, the consistency check between $\mathbf{x}^*$ and $\mathbf{x}'$ can only be applied to a subset. To simulate the honest receiver's measurement, we recreate the quantum state. According to the extraction property of Wiesner codings Lemma 34, this is indistinguishable to directly forwarding the state. Therefore, the check $\mathbf{x}' = \mathbf{x}$ passes and no additional abort is introduced in this step.

If the decoding was unsuccessful, there was no $\mathbf{x}'$ within the decoding radius radius of αN of x^*. That means any value the adversary reveals in the commitment that fulfills the error syndrome consistency check must have Hamming distance at least αN from x^* and will be rejected by the honest adversary, except with probability $(\frac{1}{2})^{\alpha N}$ which is negligible for $N \in \Theta(\kappa), 0 < \alpha < 1$. Therefore $\mathcal{S}_3$ can output $\perp_3$.

□

Claim. If C is a linear $[N, (1-\gamma)N]$-code that fulfills the properties of Theorem 6, then, $\mathrm{TD}(\mathrm{out}_3, \mathrm{out}_4) \leq \mathit{negl}(\kappa)$.

Proof. Let $\mathrm{E}_\perp$ denote the event that $\mathcal{S}_4$ outputs $\perp_4$. Then, $\mathrm{TD}(\mathrm{out}_3, \mathrm{out}_4) = \Pr[\mathrm{E}_\perp]$.

By definition, $\mathcal{S}_4$ outputs $\perp_4$ if and only if the simulated honest receiver would accept the decommitment (relative to the measurements performed for extraction), but the bitstring $\mathbf{x}$ sent by the corrupted committer (which is a correct codeword relative to ct_0) is unequal to $\mathbf{x}'$, *i.e.* the extracted and possibly corrected codeword. In this case, we have $\delta(\mathbf{x}, \mathbf{x}') = D$ (as both $\mathbf{x}$ and $\mathbf{x}'$ are correct codewords) and $\delta(\mathbf{x}', \mathbf{x}^*) \leq \alpha N \leq D/2 - 1$, as the extracted codeword $\mathbf{x}^*$ could be corrected to $\mathbf{x}'$. Thus, from the triangle inequality, it follows that $\delta(\mathbf{x}, \mathbf{x}^*) \geq D/2$. However, such a value $\mathbf{x}$ is rejected, except with negligible probability of at most $(\frac{1}{2})^{D/2}$ with $D \in \Theta(\kappa)$. Thus, $\Pr[\mathrm{E}_\perp]$ is also negligible and the claim follows. □

Claim. $\mathrm{TD}(\mathrm{out}_4, \mathrm{out}_5) = 0$.

Proof. Since we have established in the previous hybrids that we abort if $\mathbf{x} \neq \mathbf{x}'$ or $\sigma \neq, \sigma', s \neq s'$, we conclude that in the case of no abort we extract the correct value: $\mathsf{Ext}(s', x') \oplus \sigma' = \mu^* = \mu = \mathsf{Ext}(s, x) \oplus \sigma$. □

Claim. $\mathrm{TD}(\mathrm{out}_5, \mathrm{out}_6) \leq \mathit{negl}(\kappa)$.

Proof. out_5 and out_6 are identically distributed unless there is an output $\perp$ in H_6 or an output $\perp_2, \perp_4, \perp_5$ in H_5. As proven before (and using the union bound), the probability of the latter is negligible. By definition of $\mathcal{S}_6$, an output of $\perp$ would have resulted in an output of $\perp_2, \perp_4$, or $\perp_5$ in one of the previous hybrids. Thus, using the union bound, this probability is also negligible, resulting in a negligible probability in total. □

□

Corrupted Receiver, Honest Committer.

Definition 19 (Simulator, Corrupted Receiver, Honest Committer). *Let* $\mathcal{S}' = (\mathcal{S}'.\mathsf{Init}, \mathcal{S}'.\mathsf{Update}, \mathcal{S}'.\mathsf{End})$ *be a compressed oracle simulator (*cf. *Definition 11).*

1. *Initially, sample* $r \xleftarrow{\$} \{0,1\}^{N+l+d+(N-K)+z}$ *and query* $\mathcal{RO}(sid, (X, Y), 0^{N+l+d+(N-K)+z})$ *to "register" the random oracle.*[9]
2. *Initialize the compressed oracle database* $D \leftarrow \mathcal{S}'.\mathsf{Init}$. *For queries to* $\mathcal{RO}(sid, (X, Y), \cdot)$*, use* $(|\phi'\rangle, D') \leftarrow \mathcal{S}'.\mathsf{Update}(\cdot, D)$ *to answer the queries with* $|\phi'\rangle$*, where* D *is kept as an internal state and set to* D' *after the query. Otherwise, forward queries from and to* $\mathcal{RO}$ *like the dummy adversary.*
3. *Generate* $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{PKE.Gen}(1^\kappa)$. *Simulate* $\mathcal{F}_{\mathsf{CRS}}$ *by returning* pk *on input* $(\mathtt{value}, sid \,\|\, \mathtt{crs})$ *after confirmation by the environment for the delayed output of* $\mathcal{F}_{\mathsf{CRS}}$.

[9] Without loss of generality, we assume that this session is the first session to query $\mathcal{RO}(sid, \cdot)$.

4. *On input* $(\texttt{committed}, sid)$ *from* $\mathcal{F}_{\mathrm{COM}}$*, sample* $\boldsymbol{\theta} \xleftarrow{\$} \{0,1\}^N, \mathbf{x} \xleftarrow{\$} \{0,1\}^N$ *uniformly at random, set* $\mathsf{ct}_0 = \mathbf{PCx}$ *and compute the quantum state* $|\phi\rangle = \bigotimes_{i=1}^{N} H^{\theta_i}|x_i\rangle$*. Sample* $s \xleftarrow{\$} \{0,1\}^l, \boldsymbol{\sigma} \xleftarrow{\$} \{0,1\}^d, r \xleftarrow{\$} \{0,1\}^{N+l+d+(N-K)+z}$ *uniformly at random ane let* $r'' = \mathcal{RO}(sid, (X,Y), r)$ *and* $h = r'' \oplus (\boldsymbol{\theta} \,\|\, s \,\|\, \boldsymbol{\sigma} \,\|\, \mathsf{ct}_0)$*. Compute* $\mathsf{ct}_1 \leftarrow \mathsf{PKE.Enc}(\mathsf{pk}, r)$*. Let* r' *denote the randomness used to generate the ciphertext. Report* $(\texttt{commit}, sid, |\phi\rangle, h, \mathsf{ct}_1)$ *as message from the honest committer and deliver it upon confirmation by the environment.*
5. *On input* $(\texttt{unveil}, sid, \mu)$ *from* $\mathcal{F}_{\mathrm{COM}}$*, sample a random* $s' \in \{0,1\}^l$ *and set* $\boldsymbol{\sigma}' = \mathsf{Ext}(s', \mathbf{x}) \oplus \mu$*. Program the internally simulated random oracle such that it evaluates to* $r'' = h \oplus (\boldsymbol{\theta} \,\|\, s' \,\|\, \boldsymbol{\sigma}' \,\|\, \mathsf{ct}_0)$ *at position* r*.*
6. *Report* $(\texttt{unveil}, sid, \boldsymbol{\theta}, s', r, \mathbf{x}, \mu, r')$ *as message from the committer to the receiver and deliver it upon confirmation by the environment.*
7. *On the last activation, read* l *from* $\mathcal{H}^{class}$*. Run* $\mathcal{S}'.\mathsf{End}(D)$ *to obtain a value table* $\mathcal{L}$ *for the internally simulated compressed oracle.*
   - *If* l *contains a list starts with the current session ID* sid *and contains a list* $\mathcal{L}'$ *of tuples* (x_i, y_i)*, create a new list* $\mathcal{L}''$ *as follows. If there is no element* $(r, \star) \in \mathcal{L}'$*, add* (r, r'') *to* $\mathcal{L}''$*. Otherwise, leave* $\mathcal{L}'$ *as is. Then, adjust* l *to contain* $\mathcal{L}''$ *and copy the adjusted* l *to* $\mathcal{H}^{class}$*.*
   - *If* l *contains no list starting with* sid*, modify* $\mathcal{H}^{class}$ *to include a list for* sid *with* $\mathcal{L} \cup \{(r, r'')\}$*.*

Lemma 13. *If* PKE *is an IND-CPA-secure PKE scheme against quantum polynomial-time adversaries,* $\mathtt{C}$ *is a linear* $[N, (1-\gamma)N)]$*-code that fulfills the properties of Definition 2 and* Ext *is a* (w, ε)*-strong randomness extractor s.t.* $t \leq N\left(\frac{1}{2} - 2\lambda - \gamma\right) - q$*, then* $\pi_{\mathrm{COM}}(q)$ *q-eqUC-D-realizes* $\mathcal{F}_{\mathrm{COM}}$ *for a corrupted receiver.*

Proof. To prove Lemma 13, we establish the following hybrids:

- H_0: The (real) execution of $\pi_{\mathrm{COM}}(q)$ and the dummy adversary $\mathcal{D}$.
- H_1: The execution with an ideal functionality $\mathcal{F}_1$ that provides all inputs to the adversary and lets it determine all outputs. The simulator $\mathcal{S}_1$ performs the protocol on behalf of the honest sender, making its output through $\mathcal{F}_1$. For $\mathcal{RO}$, $\mathcal{S}_1$ behaves like the dummy adversary.
- H_2: The execution with $\mathcal{F}_2 = \mathcal{F}_1$. $\mathcal{S}_2$ is identical to $\mathcal{S}_1$, except that simulates $\mathcal{RO}(sid, (X,Y), \cdot)$ with a compressed oracle. On its last activation, it proceeds like in item 7, with the exception that it does not program at position r (unless r is part of the value table of the compressed oracle).
- H_3: The execution with $\mathcal{F}_3 = \mathcal{F}_2$ and a simulator $\mathcal{S}_3$. $\mathcal{S}_3$ is identical to $\mathcal{S}_2$, except that it initially samples r like in item 1, samples $r^* \xleftarrow{\$} \{0,1\}^{N+l+d+(N-K)+z}$ and uses r^* instead of $\mathcal{RO}(sid, (X,Y), r)$ in item 4. It handles the unveil phase like in items 6 and 7, programming the random oracle to r^* at position r.
- H_4: The (ideal) execution with $\mathcal{F}_{\mathrm{COM}}$ and $\mathcal{S}$.

Claim. $\mathrm{TD}(\mathrm{out}_0, \mathrm{out}_1) = 0$.

Proof. The changes between H_0 and H_1 are only syntactical and do not affect the output distribution of the execution. □

Claim. $\mathrm{TD}(\mathrm{out}_1, \mathrm{out}_2) = 0$.

Proof. Compressed oracles perfectly simulate the random oracle. Upon termination of the simulation, the value table is consistent with any input-output pairs the adversary might have observed, according to Lemma 5. □

Claim. If PKE is IND-CPA-secure against quantum polynomial-time adversaries, then $\mathrm{TD}(\mathrm{out}_2, \mathrm{out}_3) \leq \mathit{negl}(\kappa)$.

Proof. In Hybrid 3, we possibly reprogram the random oracle. According to Lemma 6, this is not observable by the adversary if the reprogrammed position is not known to the adversary, except with negligible probability. Since the adversary additionally has information on the position r due to receiving an encryption of r, we first establish that the probability of querying the random oracle at r is still negligible.

To this end, we reduce to the IND-CPA security of PKE using the efficient quantum adversary $\mathcal{B}$ which is defined as follows:

1. On input $(1^\kappa, a)$, obtain a public key pk from the IND-CPA experiment for PKE.
2. Sample $r_0, r_1 \xleftarrow{\$} \{0,1\}^{N+l+d+(N-K)+z}$.
3. Send r_0, r_1 as challenges to the IND-CPA experiment, receiving a ciphertext ct.
4. Internally emulate H_3 up to the unveil phase, except with the following changes:
   - Emulate $\mathcal{RO}$ using distinct compressed oracles for each pair $(\mathit{sid}, (X', Y'))$.
   - Embed the public key pk provided by the experiment into the common reference string.
   - Use ct instead of ct_1.
5. At the beginning of the unveil phase, use $\mathcal{S}'.\mathsf{End}$ to obtain a list $\mathcal{L}$ of queries to $\mathcal{RO}(\mathit{sid}, (X, Y), \cdot)$ (simulated by a compressed oracle). If $r_0 \in \mathcal{L}$, send 0 to the IND-CPA experiment. Otherwise, send 1 to the IND-CPA experiment

Let b' denote the challenge bit used in the IND-CPA experiment. Then, we have for $\mathcal{B}$'s advantage in the IND-CPA experiment:

$$
\begin{aligned}
&|\frac{1}{2} \cdot \Pr[\mathrm{out}_{\mathcal{B}} = 0 \mid b' = 0] + \frac{1}{2} \cdot \Pr[\mathrm{out}_{\mathcal{B}} = 1 \mid b' = 1]| \\
=&|\frac{1}{2} \cdot \Pr[r_0 \in \mathcal{L} \mid b' = 0] + \frac{1}{2} \cdot \Pr[r_0 \notin \mathcal{L} \mid b' = 1]| \\
=&|\frac{1}{2} \cdot \Pr[r_0 \in \mathcal{L} \mid b' = 0] + \frac{1}{2} \cdot (1 - \Pr[r_0 \in \mathcal{L} \mid b' = 1])| \\
\leq&|\frac{1}{2} \cdot \Pr[r_0 \in \mathcal{L} \mid b' = 0] + \frac{1}{2} \cdot (1 - \mathit{negl}(\kappa))| \\
\leq&\frac{1}{2} + |\Pr[r_0 \in \mathcal{L} \mid b' = 0] - \frac{1}{2} \cdot \mathit{negl}(\kappa))|
\end{aligned}
$$

Let $p_0 = \Pr[r_0 \in \mathcal{L}]$. As PKE is IND-CPA-secure by assumption, it follows that p_0 is negligible and the claim follows.

Let p_1 be the probability that the adversary distinguishes the reprogrammed value on an unknown value. p_1 is negligible due to Lemma 6. Then, we can establish that $\mathrm{TD}(\mathrm{out}_2, \mathrm{out}_3)$ is bounded by $p_0 + p_1$, which is negligible. □

Claim. If C is a linear $[N, (1-\gamma)N]$-code that fulfills the properties of Theorem 6 and Ext is a (w, ε)-strong randomness extractor s.t. $w \leq N\left(\frac{1}{2} - 2\lambda - \gamma\right) - q$ and ε is negligible in κ, then $\mathrm{TD}(\mathrm{out}_3, \mathrm{out}_4) \leq \mathit{negl}(\kappa)$.

Proof. The information that the adversary has on the string $\mathbf{x}$ depends the state $|\phi\rangle$. The value of h is uniformly random and therefore independent of $\mathbf{x}$ and $|\phi\rangle$. After the execution has finished, the memory bound applies to the environment and its state can be split into a quantum part Q where $|Q| = q$ and a classical part Y, where Y includes any information obtained from measuring the state $|\phi\rangle$. Let the random variable $X = \mathbf{x}$.

After the value table of $\mathcal{RO}$ is returned in the experiment's output, $\boldsymbol{\theta}$ is well-defined and can be reconstructed. During the everlasting phase the adversary can additionally obtain information that was previously hidden under computational assumptions such as the syndrome ct_0 which is of length $N - K = \gamma N$. At this point, the min-entropy of $\mathbf{x}$ is given by

$$
\begin{aligned}
H_{\min}^{\varepsilon'}(X|Y, Q, \boldsymbol{\theta}, ct_0) &\geq H_{\min}^{\varepsilon'}(X|Y, Q, \boldsymbol{\theta}) - \gamma N && (1)\\
&\geq N\left(\frac{1}{2} - 2\lambda\right) - \gamma N - q && (2)\\
&\geq w && (3)
\end{aligned}
$$

where we have first applied the chain rule for min-entropy and then applied the uncertainty relation of Lemma 11. Thus, the trace distance between out_3 and out_4 is bounded by $\varepsilon + \varepsilon'$, which is negligible in κ, since the randomness extractor produces an output that is ε close to a uniform output and incurs an error ε' since we are given an X with a smooth min-entropy bound instead of min-entropy, see Lemma 1.

We now consider the second case where the commitment is opened. In this case, output is distributed as in H_3 and the claim follows. □

□

Both Parties Honest. The simulation can be handled in analogy to the case of a corrupted receiver and we omit it. □

6.1 Applications

Using our commitment scheme π_{COM}, we can easily construct a protocol for composable zero-knowledge that is q-eqUC-D-secure.

Proposition 4. *Under the assumption of perfectly correct post-quantum-IND-CPA-secure public-key encryption, there exists a protocol* $\pi_{\mathrm{ZK}} = \pi_{\mathrm{ZK}}(q)$ *that* q*-eqUC-D-realizes the ideal functionality for zero-knowledge* $\mathcal{F}_{\mathsf{ZK}}$*.*

Proof. As statistically UC-secure protocols are also statistically quantum-UC-secure [66], we can use Proposition 3 to import the statistically UC-secure protocol for zero-knowledge of Canetti and Fischlin [24] in the $\mathcal{F}_{\mathrm{COM}}$-hybrid model into our framework. Using the composition theorem, we can replace its instances of $\mathcal{F}_{\mathrm{COM}}$ with instances of $\pi_{\mathrm{COM}}(q)$. As q-eqUC-D security is transitive, the composed protocol eqUC-D-realizes $\mathcal{F}_{\mathsf{ZK}}$ in the $\mathcal{F}_{\mathsf{CRS}}$-hybrid model. □

Furthermore, we can construct a q-eqUC-D-secure multi-party-computation (MPC) protocol without additional assumptions.

Proposition 5. *Let* $\mathcal{F}$ *be a classical probabilistic-polynomial-time functionality. Given a perfectly correct post-quantum-IND-CPA-secure public-key encryption scheme, there exists a protocol* $\pi_{\mathcal{F}}(q)$ *that* q*-eqUC-D-realizes* $\mathcal{F}$ *with the restriction that the number of protocol parties does not depend on the security parameter.*

Proof. Unruh [67] shows that there exists a protocol π in the $\mathcal{F}_{\mathrm{COM}}$-hybrid model that statistically quantum-UC-realizes $\mathcal{F}$. For two protocols π and ρ, if π statistically quantum-UC-emulates ρ, then π also emulates ρ under everlasting quantum UC security [65]. From Proposition 3, it follows that a protocol π that eqUC-emulates a protocol ϕ also q-eqUC-D-emulates ϕ for any q. Using the composition theorem and the transitivity of our notion, we can replace instances of $\mathcal{F}_{\mathrm{COM}}$ by our protocol $\pi_{\mathrm{COM}}(q)$ such that we get a protocol $\pi_{\mathcal{F}}(q)$ that q-eqUC-D-realizes $\mathcal{F}$ in the $\mathcal{F}_{\mathsf{CRS}}$-hybrid model. □

We remark that we could also obtain MPC by using the compiler of Bartusek et al. [5]. Since the compiler of Unruh [67] is already in the everlasting framework we can immediately obtain composable MPC.

7 Everlasting Public-Key Encryption

In this section, we present an everlasting secure public-key encryption scheme. We prove its security in the QROM under the assumption of the Quantum Decoherence Model.

Similarly to the construction of the commitment scheme in the previous section, we create a quantum state using random Wiesner states $|\phi\rangle = \bigotimes_{i=1}^{n} H^{\theta_i}|x_i\rangle$. The basis choice is masked by the output of the random oracle and the query to the random oracle is encrypted using a classical IND-CPA secure encryption scheme. The message is encrypted by xoring the message to the output of the randomness extractor applied to x. To decrypt a message one can decrypt the classical ciphertext to obtain the basis choice, measure the quantum state accordingly and unmask the message.

An adversary that intercepts the message can break the classical encryption scheme once he becomes unbounded and obtains the basis choice, but due to the decoherence assumption, the quantum state must have collapsed already.

Definition 20 ($\mathsf{Exp}_{\mathcal{A}}^{\mathsf{Ever\text{-}IND\text{-}CPA}}(\kappa, q)$ **Everlasting IND-CPA Security).** *Let* $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ *be a PKE scheme. Let* $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ *be an adversary where* $\mathcal{A}_1$ *is a QPT adversary that has restricted quantum memory of* q *bits after step 4 and where* $\mathcal{A}_2$ *is unbounded. Let* κ *be the security parameter and the experiment* $\mathsf{Exp}_{\mathcal{A}}^{\mathsf{Ever\text{-}IND\text{-}CPA}}(\kappa, q)$ *be defined as follows.*

1. $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\kappa, 1^q)$
2. $(m_0, m_1, st) \leftarrow \mathcal{A}_1(1^\kappa, 1^q, \mathsf{pk})$
3. $\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{pk}, m_b)$ *where* $b \xleftarrow{\$} \{0,1\}$
4. $(st_q, st_c) \leftarrow \mathcal{A}_1(\mathsf{ct}, st)$ *where* st_q *is a quantum state of size* q *and* st_c *is a classical state of arbitrary size.*
5. $b' \leftarrow \mathcal{A}_2(st_q, st_c)$
6. *if* $b = b'$ *the experiment outputs 1, otherwise the experiment outputs 0*

The PKE scheme is everlasting IND-CPA-secure *if for every adversary* $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$*, where* $\mathcal{A}_1$ *is QPT, there exists a negligible function* $negl$ *such that for all* $\kappa \in \mathbb{N}$ *and all* $q \in \mathbb{N}$*, it holds that*

$$\mathsf{Pr}[\mathsf{Exp}_{\mathcal{A}}^{\mathsf{Ever\text{-}IND\text{-}CPA}}(\kappa, q) = 1] \leq \frac{1}{2} + negl(\kappa)$$

Construction 2. *The algorithms* $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ *are defined below. Let* κ *be the security parameter and* q *the storage bound.*

- *Let* $(\mathsf{PKE.KeyGen}, \mathsf{PKE.Enc}, \mathsf{PKE.Dec})$ *be a classical PKE scheme.*
- *Let* $\mathcal{RO} : \{0,1\}^z \to \{0,1\}^{N+l+d}$ *be a pseudorandom generator, implemented by a random oracle. Let* $z, d, s, N \in poly(\kappa)$*.*
- *Let* $\mathsf{Ext} : \{0,1\}^l \times \{0,1\}^N \to \{0,1\}^d$ *be a* (w, ε)*-strong randomness extractor s.t.* $w \leq N\left(\frac{1}{2} - 2\lambda\right) - q$*.*

$\mathsf{KeyGen}(1^\kappa) \to (\mathsf{pk}, \mathsf{sk})$: $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{PKE.KeyGen}(1^\kappa)$

$\mathsf{Enc}(\mathsf{pk}, \mathsf{m}) \to \mathsf{ct}$: *Choose* $r \in \{0,1\}^z$ *and encrypt* $\mathsf{ct}_0 \leftarrow \mathsf{PKE.Enc}(\mathsf{pk}, r)$*. Choose* $\boldsymbol{\theta} \in \{0,1\}^N$*,* $\mathbf{x} \in \{0,1\}^N$ *and compute the quantum state* $|\phi\rangle = \bigotimes_{i=1}^n H^{\theta_i} |x_i\rangle$*. Choose* $s \in \{0,1\}^l$ *and compute* $\boldsymbol{\sigma} = \mathsf{Ext}(s, \mathbf{x}) \oplus \mathsf{m}$ *and* $\mathsf{ct}_1 = \mathcal{RO}(r) \oplus (\boldsymbol{\theta} \,\|\, s \,\|\, \boldsymbol{\sigma})$*. Output the ciphertext* $\mathsf{ct} = (|\phi\rangle, \mathsf{ct}_1, \mathsf{ct}_0)$*.*

$\mathsf{Dec}(\mathsf{sk}, \mathsf{ct}) \to \mathsf{m}$: *Decrypt the classical ciphertext* $r = \mathsf{PKE.Dec}(\mathsf{sk}, \mathsf{ct}_0)$*, compute* $(\boldsymbol{\theta} \,\|\, s \,\|\, \boldsymbol{\sigma}) = \mathcal{RO}(r) \oplus \mathsf{ct}_1$ *and measure the quantum state in basis* $\boldsymbol{\theta}$ *to obtain* $\mathbf{x}$*. Compute* $\mathsf{m} = \boldsymbol{\sigma} \oplus \mathsf{Ext}(s, \mathbf{x})$*.*

Theorem 9. *Let* κ *be the security parameter and let* q *be the storage parameter. Given a classical IND-CPA-secure PKE scheme and a* $(poly(\kappa), negl(\kappa))$*-randomness extractor, the PKE scheme* $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ *from Construction 2 is everlasting IND-CPA-secure in the QROM against an adversary* $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ *in the Quantum Decoherence Model, where* $\mathcal{A}_2$ *receives the random oracle's full value table as input.*

Correctness follows from the correctness of the classical PKE scheme.

Proof. To show that an adversary $\mathcal{A}$ cannot win the $\mathsf{Exp}_{\mathcal{A}}^{\mathsf{Ever\text{-}IND\text{-}CPA}}(\kappa, q)$ experiment with more than neglible advantage, we show that he cannot distinguish encryptions of m_0 from encryptions of m_1 with more than negligible advantage. Recall that the adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ is split into two phases, where $\mathcal{A}_1$ is quantum-computationally bounded and $\mathcal{A}_2$ is unbounded. $\mathcal{A}_2$ receives a quantum state of at most size q and an polynomial classical state from $\mathcal{A}_1$. $\mathcal{A}_1$ may make a polynomially-bounded number of queries t to the random oracle. To simulate the random oracle, we use the compressed oracles technique. After the adversary becomes unbounded, we reveal the value table of the random oracle.

Hybrid 0. The first hybrid is $\mathsf{Exp}_{\mathcal{A}}^{\mathsf{Ever\text{-}IND\text{-}CPA}}(\kappa, q)$, where message m_b is honestly encrypted.

Hybrid 1. In hybrid 1, we change the encryption of r to a new uniformly sampled r' such that $\mathsf{ct}_0 \leftarrow \mathsf{PKE.Enc}(\mathsf{pk}, r')$.

Lemma 14. *$|p_0 - p_1| \leq negl(\kappa)$, where p_0 is the probability that the experiment outputs 1 in hybrid 0 and p_1 is the probability that the experiment outputs 1 in hybrid 1.*

Proof. If an adversary $\mathcal{A}'$ can distinguish hybrid 0 from hybrid 1, then we can use this adversary to break the IND-CPA security of the underlying PKE scheme.

In hybrid 0, the adversary is given $(\mathsf{PKE.Enc}(\mathsf{pk}, r), \mathcal{RO}(r) \oplus (\theta||s||\sigma), |\phi\rangle)$. In hybrid 1, the adversary is given $(\mathsf{PKE.Enc}(\mathsf{pk}, r'), \mathcal{RO}(r) \oplus (\theta||s||\sigma), |\phi\rangle)$.

The difference between hybrid 0 and hybrid 1 is whether $\mathsf{PKE.Enc}(\mathsf{pk}, r)$ and $\mathcal{RO}(r)$ or $\mathsf{PKE.Enc}(\mathsf{pk}, r')$ and $\mathcal{RO}(r)$ are given during phase 1. Since the value $\mathcal{RO}(r)$ is masked by $(\theta||s||\sigma)$, which are not known to the adversary, a unbounded phase 2 adversary that extracted r^* cannot check if this value was used in $\mathcal{RO}(r) \oplus (\theta||s||\sigma)$.

Let $\mathcal{A}$ be the adversary against the underlying encryption scheme. He samples r and r' and sends them as challenge to the IND-CPA experiment and receives a challenge ciphertext ct. $\mathcal{A}$ samples a random function $\mathcal{RO}$ and computes $\mathcal{RO}(r) = y$.

He sends y and ct to $\mathcal{A}'$ and answers any queries to the random oracle by simulating the random oracle using compressed random oracles $\mathcal{A}'$ answers a query $t = \sum_i \alpha_i |x_i\rangle|u_i\rangle$ with $\sum_i \alpha_i |x_i\rangle|u_i \oplus \mathcal{RO}(x_i)\rangle$. For a random query t_i the adversary measures the query and checks if $x = r$. If this is the case then $\mathcal{A}$ guesses the message r in the IND-CPA experiment, if $\mathcal{A}'$ does not guess r then $\mathcal{A}$ guesses r' in the experiment. If $\mathcal{A}'$ queries the value r with non-negligible probability p in a query then $\mathcal{A}$ answers r with probability $\frac{p}{t}$ where t is the number of queries and wins the experiment with non-negligible advantage.

□

Hybrid 2. In hybrid 2, we replace $\mathcal{RO}(r)$ by a uniformly random value h in the encryption algorithm. We set the output of the random oracle to be h at input r.

Lemma 15. *$|p_1 - p_2| \leq O\left(\sqrt{\frac{t^2}{2^z}}\right)$ where p_1 is the probability that the experiment outputs 1 in hybrid 1 and p_2 is the probability that the experiment outputs 1 in hybrid 2.*

Proof. Since $\mathsf{ct}_1 = \mathcal{RO}(r) \oplus (\boldsymbol{\theta} \,\|\, s \,\|\, \boldsymbol{\sigma})$ is the only value in the adversary's view that depends on r we can use Lemma 6 to bound the probability that the reprogramming is detected by $O\left(\sqrt{\frac{t^2}{2^z}}\right)$ where t is the number of queries that are made to the random oracle. □

Hybrid 3. In hybrid 3, we replace the output of the randomness extractor by a uniformly random value $\mathbf{u}$. This changes $\boldsymbol{\sigma} = \mathsf{Ext}(s, \mathbf{x}) \oplus \mathsf{m}_b$ to $\boldsymbol{\sigma} = \mathbf{u}$.

Lemma 16. *$|p_2 - p_3| \leq \varepsilon + \varepsilon'$, where p_2 is the probability that the experiment outputs 1 in hybrid 2 and p_3 is the probability that the experiment outputs 1 in hybrid 3 and ε and ε' are the errors incurred by the randomness extractor and the smooth min-entropy.*

Proof. Based on the definition of a (w, ε)-extractor (cf. Definition 1) replacing the output by a uniformly random value cannot be detected by the adversary $\mathcal{A}$ with probability larger than ε. For this statement to be applicable we need to show that the smooth min-entropy of $\mathbf{x}$ is at least w. The entropy of $\mathbf{x}$ depends on $|\phi\rangle$ which depends on $\boldsymbol{\theta}$. Since the value h is uniformly random the value $\mathsf{ct}_1 = h \oplus (\boldsymbol{\theta}||s||\boldsymbol{\sigma})$ does not reveal anything about $\boldsymbol{\theta}$ to $\mathcal{A}_1$. At this point the memory bound applies to $\mathcal{A}_1$ and a quantum state Q of maximum size q and an arbitrary classical state Y remains. The classical state may contain $\mathsf{ct}_0, \mathsf{ct}_1$ and any information obtained by measuring the quantum state $|\phi\rangle$. Let X denote the classical random variable describing $\mathbf{x}$. $\mathcal{A}_2$ can later learn the value $\boldsymbol{\theta}$. Therefore the min-entropy of $\mathbf{x}$ is given by

$$H_{\min}^{\varepsilon'}(X|Y, \boldsymbol{\theta}) \geq N(\frac{1}{2} - 2\lambda) - q$$

where we have applied the uncertainty relation for Wiesner Coding (Lemma 11) and incur an additional error of ε' since we are working with smooth min-entropy, see Lemma 1. Both ϵ and ε' are negligible. □

In hybrid 3 the encryption is independent of the bit b. Therefore the adversary's probability of guessing the correct bit is $\frac{1}{2}$. Since all hybrids are indistinguishable up to negligible probability the adversary's advantage of winning the $\mathsf{Exp}_{\mathcal{A}}^{\mathsf{Ever\text{-}IND\text{-}CPA}}(\kappa, q)$ experiment is negligible. □

8 Oblivious Transfer with Everlasting Semi-Honest Security

In this section, we construct a composable OT protocol that provides everlasting security against semi-honest adversaries in the quantum decoherence model. Moreover, it provides statistical receiver security even against malicious senders.

The general idea is as follows, resembling our construction of a composable commitment scheme with everlasting security: The sender prepares two quantum states using Wiesner coding. Then, the bases for each state are masked using hashes a random oracle. The preimages are transmitted via a classical OT, ensuring that the receiver can only obtain the information about one of the basis choices. The corresponding state can be measured in the correct basis and one of the messages is obtained.

Due to the decoherence assumption, one of the quantum states has to be measured *without* knowing the correct basis. Encoding the messages μ_0 and μ_1 using the output of a randomness extractor ensures that no partial information about the message can be recovered.

We can instantiate the classical OT by the 2-round OT of Peikert et al. [57]. They provide a construction for either statistical receiver and computational (post-quantum) sender security or the reverse: statistical sender and computational (post-quantum) receiver security. For our protocol we need the statistically receiver secure and computationally sender secure construction which also provides an extractor for the sender message.

We consider a *semi-honest adversary* for our notion of q-everlasting quantum UC security with decoherence. Contrary to a malicious adversary that corrupts a party and subsequently completely controls it, the semi-honest adversary will only get access to the internal state of the corrupted party which continues to follow the protocol honestly. In the context of the QDM, we consider environments that eventually have to reduce their quantum state to a limited number of qubits. Since the honest receiver of a quantum state in our protocol immediately measures the state, the additional restriction of quantum decoherence becomes obsolete. Taking a closer look, our protocol fulfills a stronger notion of semi-honest security where the quantum states received by the corrupted party may be measured differently (or not at all). In this setting, quantum decoherence is, as we will see, important again. Letting the adversary take control of the party when it receives the quantum state does not disturb the protocol execution since the receiving party does not send any further messages after receiving the quantum state in the case of our protocol.

Comparison to [65]. Unruh also considers the notion of semi-honest or passive adversaries and solves this problem by defining an execution with a passive adversary as follows: The protocol participants have to be unitary machines. That means their behaviour can be described by a unitary, thus they are not allowed to make measurements and the quantum state (has it not been transmitted to another party) can be given to the adversary at the end of the execution.

Our definition is a simplified version of Unruh's definition specifically tailored to our OT protocol. Since the receiver gets the quantum message at the end and does not send anything further its receiving action described as a unitary can be undone by the adversary after obtaining the state by applying the inverse unitary. Therefore we can say w.l.o.g. that the adversary immediately takes control of the state. Since the first message of the receiver is classical we simply consider the adversary to obtain a copy of it.

We now present our construction.

Construction 3. *Let κ be the security parameter and q the storage bound.*

- *Let* $(\mathsf{COT.Setup}, \mathsf{COT.R1}, \mathsf{COT.S1}, \mathsf{COT.R2})$ *be a classical OT protocol.*
- *Let* $\mathsf{Ext} : \{0,1\}^l \times \{0,1\}^N \to \{0,1\}^d$ *be a* (w, ε)*-strong randomness extractor s.t.* $w \leq N\left(\frac{1}{2} - 2\lambda\right) - q$ *and* $N, l, d \in poly(\kappa)$.
- *Let* $X = \{0,1\}^m$ *and* $Y = \{0,1\}^{N+l+d}$*, where* $m \in poly(\kappa)$.

Receiver

1. *On input* $(\mathtt{receive}, sid, b)$*, query the* $\mathcal{F}_{\mathsf{CRS}}$ *functionality using* $(\mathtt{value}, sid \,\|\, crs)$ *parameterized with distribution* $\{crs\}_{crs \leftarrow \mathsf{COT.Setup}(1^\kappa)}$ *to obtain* crs.
2. *Compute* $ot_1 \leftarrow \mathsf{COT.R1}(1^\kappa, crs, b)$ *and send* ot_1 *to the sender.*

Sender

1. *On input* $(\mathtt{send}, sid, (\mu_0, \mu_1))$*, query the* $\mathcal{F}_{\mathsf{CRS}}$ *functionality using* $(\mathtt{value}, sid \,\|\, crs)$ *parameterized with distribution* $\{crs\}_{crs \leftarrow \mathsf{COT.Setup}(1^\kappa)}$ *to obtain* crs *and wait for the message* ot_1.
2. *Upon reception, sample* $\boldsymbol{\theta}_0, \boldsymbol{\theta}_1 \in \{0,1\}^N$ *and* $x_0, x_1 \leftarrow \{0,1\}^N$*. Create the states* $|\phi_0\rangle = H^{\boldsymbol{\theta}_0}|x_0\rangle$ *and* $|\phi_1\rangle = H^{\boldsymbol{\theta}_1}|x_1\rangle$.
3. *Sample* $s \leftarrow \{0,1\}^l$ *and compute* $\boldsymbol{\sigma}_0 = \mathsf{Ext}(x_0, s) \oplus \boldsymbol{\mu}_0$ *and* $\boldsymbol{\sigma}_1 = \mathsf{Ext}(x_1, s) \oplus \boldsymbol{\mu}_1$.
4. *Sample* $r_0, r_1 \leftarrow \{0,1\}^z$ *and let* $h_0 = \mathcal{RO}(sid \,\|\, 0, (X, Y), r_0) \oplus (\boldsymbol{\theta}_0 \,\|\, \boldsymbol{\sigma}_0 \,\|\, s)$ *and* $h_1 = \mathcal{RO}(sid \,\|\, 1, (X, Y), r_1) \oplus (\boldsymbol{\theta}_1 \,\|\, \boldsymbol{\sigma}_1 \,\|\, s)$.
5. *Compute* $ot_2 \leftarrow \mathsf{COT.S1}(1^\kappa, crs, ot_1, r_0, r_1)$.
6. *Send* $(\mathtt{send}, sid, (h_0, h_1, |\phi_0\rangle, |\phi_1\rangle, ot_2))$ *to the receiver.*

Receiver

1. *Receive* $(\mathtt{send}, sid, (h_0, h_1, |\phi_0\rangle, |\phi_1\rangle), ot_2)$ *from the sender.*
2. *Compute* $r_b \leftarrow \mathsf{COT.R2}(1^\kappa, crs, ot_2)$.
3. *Compute* $\mathcal{RO}(sid \,\|\, b, (X, Y), r_b) \oplus h_b = (\boldsymbol{\theta}_b, \boldsymbol{\sigma}_b, s)$ *and measure the state* $|\phi_b\rangle$ *in basis* $\boldsymbol{\theta}_b$ *to obtain* x_b.
4. *Compute* $\boldsymbol{\sigma}_b \oplus \mathsf{Ext}(x_b, s) = \boldsymbol{\mu}_b$ *and output* μ_b.

Theorem 10. *Let κ be the security parameter and let q be the storage parameter. Given a* $(poly(\kappa), negl(\kappa))$*-randomness extractor and a classical OT protocol* COT *that simultaneously*

– *statistically UC-realizes* $\mathcal{F}_{\mathsf{OT}}$ *for malicious senders and honest receivers as well as*
– *computationally quantum-UC-realizes* $\mathcal{F}_{\mathsf{OT}}$ *for semi-honest receivers and honest senders,*

the OT protocol from Construction 3 q-eqUC-D-realizes $\mathcal{F}_{\mathsf{OT}}$ *under static malicious corruption of the sender and static semi-honest corruptions of the receiver.*

Proof.

Semi-honest Everlasting Sender Security.

Lemma 17. *Given a* $(poly(\kappa), negl(\kappa))$*-randomness extractor and a classical OT protocol with computational quantum-UC-security against semi-honest receivers, the OT protocol from Construction 3 q-eqUC-D-realizes* $\mathcal{F}_{\mathsf{OT}}$ *under static semi-honest corruptions of the receiver.*

Proof. We define a simulator $\mathcal{S}$ for the dummy adversary as follows:

1. Generate $crs \leftarrow \mathsf{COT.Setup}(1^\kappa)$. Simulate $\mathcal{F}_{\mathsf{CRS}}$ by returning crs on input $(\mathtt{value}, sid \,\|\, crs)$ after confirmation by the environment for the delayed output of $\mathcal{F}_{\mathsf{CRS}}$.
2. Query $\mathcal{RO}(sid||0,(X,Y),0)$, $\mathcal{RO}(sid||1,(X,Y),0)$ to "register" both random oracles for this session.[10]
3. Initialize two compressed oracle databases $D_b \leftarrow \mathcal{S}'.\mathsf{Init}$. For queries to $\mathcal{RO}(sid \,\|\, b,(X,Y),\cdot)$, use $(|\phi'\rangle, D_b') \leftarrow \mathcal{S}'.\mathsf{Update}(\cdot, D_b)$ to answer the queries with $|\phi'\rangle$, where D_b is kept as an internal state and set to D_b' after the query.
4. Let ot_1 be the OT receiver's first message and b its input.
5. Send $(\mathtt{receive}, sid, b)$ to to $\mathcal{F}_{\mathsf{OT}}$ and obtain μ_b.
6. Set $\mu_{1-b} \leftarrow \{0,1\}^N$ to a uniformly random value. Prepare the ot_2 message according to the protocol specification of the sender message and send it on behalf of the sender.
7. On the last activation, read l from $\mathcal{H}^{class}$. Run $\mathcal{S}'.\mathsf{End}(D_b)$ for both random oracles to obtain a value table $\mathcal{L}_b$ for the internally simulated compressed oracle. If l contains a list l_b that starts with ID $sid||b$ for $b \in \{0,1\}$, add the values of $\mathcal{L}_b$ to l_b without overwriting existing values. Otherwise, simply add $\mathcal{L}_b$ to l.

We show that the real and the ideal executions are trace-indistinguishable by starting with the real-world execution and transforming it into the ideal-world execution.

Hybrid 0. This is the real execution with the dummy adversary.

[10] Without loss of generality, we assume that this session is the first session to query $\mathcal{RO}(sid||0,\cdot)$ and $\mathcal{RO}(sid||1,\cdot)$.

Hybrid 1. The execution with an ideal functionality $\mathcal{F}_1$ that provides all inputs to the adversary and lets it determine all outputs. The simulator $\mathcal{S}_1$ performs the protocol on behalf of the honest sender, making its output through $\mathcal{F}_1$.

Lemma 18. *$TD(out_0, out_1) = 0$, where out_i is the output of hybrid i.*

Proof. This change is purely syntactical. □

Hybrid 2. The simulator $\mathcal{S}$ simulates the random oracle using the compressed oracle technique. At the end of the first phase, it collapses the random oracle and writes their value tables to its register $\mathcal{H}^{class}$ like the simulator.

Lemma 19. *$TD(out_1, out_2) = 0$.*

Proof. This change is not noticeable due to the indistinguishability of the compressed oracle to the standard random oracle, see Lemma 4. □

Hybrid 3. After ending the compressed oracle simulation, check whether the query $\mathcal{RO}(sid \,\|\, 1-b, (X, Y), r_{1-b})$ occurred. If so, output a special error symbol $\perp$.

Lemma 20. *If* COT *is quantum-UC-secure against semi-honest receivers, then* $TD(\text{out}_2, \text{out}_3) \leq negl(\kappa)$.

Proof. out_2 and out_3 are trace-indistinguishabe unless a query to the random oracle of the form $\mathcal{RO}(sid \,\|\, 1-b, (X, Y), r_{1-b})$ occurs. We show that an adversary that queries r_{1-b} can be used to distinguish between a simulated and real execution of the the classical OT protocol.

Let $\mathcal{Z}$ be an environment that queries $\mathcal{RO}(sid \,\|\, 1-b, \cdot)$ on r_{1-b} with non-negligible probability. Then, we can construct an environment $\mathcal{Z}^*$ that can distinguish between a real execution of COT and a simulated execution of COT as follows:

1. $\mathcal{Z}^*$ acts as environment in a quantum UC execution and internally emulates H_3. Let (r_0, r_1) be the input of the internally emulated environment for the OT sender and let b be its input for the OT receiver.
2. Instead of simulating the execution of COT, $\mathcal{Z}^*$ performs this execution with the quantum UC experiment, where it semi-honestly corrupts the receiver. It provides (r_0, r_1) as input for the sender and b as input for the receiver as provided by $\mathcal{Z}$. All COT messages in H_3 are used from the quantum UC execution.
3. When the OT protocol execution has ended, $\mathcal{Z}^*$ measures the random oracles. If $\mathcal{Z}$ has queried the random oracle on $\mathcal{RO}(sid \,\|\, 1-b, (X, Y), r_{1-b})$, $\mathcal{Z}^*$ guesses that it was in the real execution. Otherwise, it guesses that it was in the ideal execution.

Observe that if $\mathcal{Z}^*$ interacts with the ideal execution, the probability that $\mathcal{Z}$ queries $\mathcal{RO}(sid \,\|\, 1-b, \cdot)$ on r_{1-b} is negligible, as the execution is independent of r_{1-b}, where b is the choice bit.

Let $b' = 0$ denote that $\mathcal{Z}^*$ interacts with the ideal execution for COT and $b' = 1$ denote that $\mathcal{Z}^*$ interacts with the real execution for COT.

Therefore $\mathcal{Z}^*$ has the following advantage:

$$\begin{aligned}
&|1/2 \cdot \mathsf{Pr}[out = 0 \mid b' = 0] + 1/2 \cdot \mathsf{Pr}[out = 1 \mid b' = 1]| \\
=&|1/2 \cdot \mathsf{Pr}[\mathcal{Z} \text{ queries } \mathcal{RO}(sid \,\|\, 1-b, \cdot) \text{ at } r_{1-b} \mid b' = 0] \\
&\quad + 1/2 \cdot \mathsf{Pr}[\mathcal{Z} \text{ does not query } \mathcal{RO}(sid \,\|\, 1-b, \cdot) \text{ at } r_{1-b} \mid b' = 1]| \\
\leq&|1/2 \cdot \mathsf{Pr}[\mathcal{Z} \text{ queries } \mathcal{RO}(sid \,\|\, 1-b, \cdot) \text{ at } r_{1-b} \mid b' = 0] + 1/2 + negl(\kappa)|
\end{aligned}$$

As the advantage of $\mathcal{Z}^*$ is bounded by $\frac{1}{2} + negl$ by assumption, it follows that the probability that $\mathcal{Z}$ queries $\mathcal{RO}(sid \,\|\, 1-b, \cdot)$ on r_{1-b} negligible. □

Hybrid 4. This is the ideal experiment with the ideal functionality $\mathcal{F}_{\mathsf{OT}}$ and the simulator as defined above up to the additional abort condition introduced in the previous hybrid.

Lemma 21. *If* Ext *is a* (w, ϵ)*-strong randomness extractor, where* $w \leq N(1/2 - 2\lambda) - q)$ *and* ϵ *is negligible, then* $TD(\text{out}_3, \text{out}_4) \leq negl(\kappa)$.

Proof. In this hybrid, the simulator sends b to the ideal functionality to obtain μ_b and creates an ot_2 message which contains the message μ_b and a randomly sampled message $\mu^*_{1-b} \leftarrow \{0,1\}^N$ according to the protocol specifications for the sender: $(|\phi_b\rangle, |\phi_{1-b}\rangle, h_b, h_{1-b}, ot_1)$

We now show that out_3 and out_4 are trace-indistinguishable.

In the previous hybrid, we have established that the internally emulated adversary did not query the random oracle at r_{1-b}, except with negligible probability. Therefore, it does not learn the basis $\boldsymbol{\theta}_{1-b}$, except with negligible probability. Eventually, the environment has to reduce its quantum state given by $H^{\boldsymbol{\theta}_b}|x_b\rangle$ and $H^{\boldsymbol{\theta}_{1-b}}|x_{1-b}\rangle$ to at most q qubits.

We consider the entropy of the value x_{1-b}. Let X be a classical random variable describing x_{1-b}, let Y be a classical random variable describing the state st_c that the environment holds and let Q describe the state st_q that the environment holds.

Then based on Lemma 11 the min-entropy of x_{1-b} is

$$H^{\varepsilon'}_{\min}(X|Y, Q, \theta_{1-b}) \geq N\left(\frac{1}{2} - 2\lambda\right) - q$$

Therefore the output of the randomness extractor applied to x_{1-b} is not distinguishable from uniformly random with more than negligible probability and the output of the randomness extractor cannot be distinguished from a uniformly random value. Therefore the message μ_{1-b} in Hybrid 2 and the message μ^*_{1-b} in Hybrid 3 respectively appear uniformly random since they are XOR-ed to the output of the randomness extractor.

It thus follows that the trace distance between out_2 and out_3 can be bounded by $\varepsilon + \varepsilon' = negl(\kappa)$, where ε and ε' are the advantages related to the randomness extractor and the smooth min-entropy respectively. □

Hybrid 5. We remove the additional abort condition.

Lemma 22. *If* COT *is semi-honest sender-secure, then* $TD(\text{out}_4, \text{out}_5) \leq negl(\kappa)$.

Proof. By the same argument as for Lemma 20, out_4 and out_5 are trace-indistinguishable. □

□

Statistical Receiver Security.

Lemma 23. *Given a* $(poly(\kappa), negl(\kappa))$*-randomness extractor and a classical OT protocol that statistically UC-realizes* $\mathcal{F}_{\mathsf{OT}}$ *for malicious senders and honest receivers, the OT protocol from Construction 3 q-eqUC-D-realizes* $\mathcal{F}_{\mathsf{OT}}$ *under static malicious corruption of the sender.*

Proof. In order to prove the statistical receiver security, we state the following simulator for the dummy adversary.

Definition 21 (Simulator).

1. *Execute the UC simulator for* COT *to obtain the CRS crs and return it as output of* $\mathcal{F}_{\mathsf{CRS}}$.
2. *Forward queries from and to* $\mathcal{RO}$ *like the dummy adversary.*
3. *Obtain the message* $(\texttt{send}, sid, (h_0, h_1, |\phi_0\rangle, |\phi_1\rangle, ot_2'))$ *from the environment.*
4. *Use the UC simulator for* COT *to extract* ot_2' *to obtain messages* (r_0, r_1). *If the extraction fails, output a special error symbol* $\perp$.
5. *Use* r_0 *and* r_1 *to obtain* μ_0, μ_1 *by performing the computations of the honest receiver for both messages.*
6. *Send* $(\texttt{send}, sid, (\mu_0, \mu_1))$ *to* $\mathcal{F}_{\mathsf{OT}}$.
7. *On its last activation* $\mathcal{S}$*, behaves like the dummy adversary.*

We show that the ideal execution with the simulator is indistinguishable from the real execution with the adversary.

Hybrid 0. This is the real execution between the environment, the dummy adversary and the honest receiver.

Hybrid 1. Instead of running the honest receiver, the simulator runs the UC simulator for the OT protocol.

Lemma 24. *If* COT *is statistically UC-secure against malicious senders, then* $TD(\text{out}_0, \text{out}_1) \leq negl$.

Proof. As the reduction is straight-forward, we omit it. □

Hybrid 2. After receiving the $(\texttt{send}, sid, (h_0, h_1, |\phi_0\rangle, |\phi_1\rangle, ot_2'))$ message from the environment the simulator extracts (μ_0', μ_1') as in Step 4 and 5. After the honest receiver outputs (b, μ_b) check if $\mu_b = \mu_b'$. If the check fails abort the simulation, if the check succeeds send (μ_0', μ_1') to the ideal functionality $\mathcal{F}_{\mathsf{OT}}$.

Lemma 25. *$TD(out_1, out_2) \leq negl(\kappa)$.*

Proof. In the first step, the simulator uses the UC simulator for COT to extract (r_0, r_1).

In the second step the simulator will compute $\boldsymbol{\theta}_0$ and $\boldsymbol{\theta}_1$ as the honest receiver would for each b and measure the states $|\phi_0\rangle$ and $|\phi_1\rangle$ in the respective basis to obtain x_0 and x_1. Then μ_0 and μ_1 can be computed. Using $\boldsymbol{\theta}_0, \boldsymbol{\theta}_1, x_0, x_1$ the simulator recreates the quantum state $|\phi_0'\rangle, |\phi_1'\rangle$ and creates $eot_2'' = (\texttt{send}, sid, (h_0, h_1, |\phi_0'\rangle, |\phi_1'\rangle, ot_2''))$. Due to the extraction properties of Wiesner Coding, Lemma 34, the message is identically distributed.

Based on the extraction of the message, the receiver will obtain the same message whether he obtains it from computing the UC OT simulator or from querying the ideal functionality. □

Hybrid 3. This is the ideal execution with the simulator as defined above.

Lemma 26. *If COT is statistically UC-secure against malicious senders, then $TD(\text{out}_2, \text{out}_3) \leq negl(\kappa)$.*

Proof. The changes between H_2 and H_3 are only syntactic and oblivious for the environment, with the exception of the abort criterion. As the probability of a wrong extraction is negligible, the claim follows. □

□

Both parties honest. This case is similar to the simulator for the corrupted receiver so we omit the details here. □

9 Quantum Incompressible Encryption

In the classical setting, the notion of *incompressible encryption* was first introduced by Guan et al. [36] as an extension of *disappearing* encryption [38], which in itself is an extension of the bounded storage model [51]. There, the key idea is to make a scheme *secure* against key leaks as long as not the entire ciphertext was stored. This is modeled similar to the classical IND-security games, with the difference that after receiving the challenge ciphertext, the adversary gets to create a state of size S which is *smaller than the ciphertext* (this storage bound can be adversarially chosen before the KeyGen algorithm is run). A second adversary *with access to the secret key*, both challenge messages but only the *compressed* state has to guess which of the two messages was encrypted.

The transfer of this experiment to the quantum setting is quite straightforward and can be seen below; we replace the bound for the classical storage with an q-qubit quantum state st_q, yet allow for an arbitrary *classical* state st_c to be transferred.

Definition 22. ($\mathsf{Exp}^{\mathsf{QIE}}_{\mathcal{A}}(\kappa)$) *Let* $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ *be a quantum polynomial time adversary. Let* $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ *be an encryption scheme.*

1. $1^q \leftarrow \mathcal{A}_1(1^\kappa)$
2. $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\kappa, 1^q)$
3. $b \leftarrow \{0,1\}$
4. $(m_0, m_1) \leftarrow \mathcal{A}_1(\mathsf{pk})$
5. $\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{pk}, m_b)$
6. $(st_q, st_c) \leftarrow \mathcal{A}_1(\mathsf{pk}, \mathsf{ct})$ *where* st_q *is a quantum state of size at most* q *and* st_c *is a classical state of arbitrary size*
7. $b' \leftarrow A_2(\mathsf{pk}, \mathsf{sk}, st_q, st_c)$
8. *the adversary wins if* $b = b'$ *and the experiment outputs 1, otherwise the experiment outputs 0*

The encryption scheme is a quantum incompressible encryption scheme if the advantage of an adversary to win $\mathsf{Exp}^{\mathsf{QIE}}_{\mathcal{A}}(\kappa)$ *is negligible:*

$$\mathsf{Pr}[\mathsf{Exp}^{\mathsf{QIE}}_{\mathcal{A}}(\kappa) = 1] \leq \frac{1}{2} + negl(\kappa).$$

Definition 23. *(correctness) An incompressible encryption scheme has to fulfill the usual correctness property. For all messages* m *and all keys generated by* $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\kappa)$ *the following holds:*

$$\mathsf{Pr}[\mathsf{Dec}(\mathsf{sk}, \mathsf{Enc}(\mathsf{pk}, m)) = m] \geq 1 - negl(\kappa).$$

9.1 Construction

The construction and security proof of our scheme follows the classical incompressible encryption scheme of Guan et al. [36]. The key generation algorithm is completely classical, but the ciphertext has a quantum part. Note that the quantum state can be stream encoded and decoded. That means that the honest parties only need to have one qubit at a time in their storage. It falls into the category of *prepare-and-measure* protocols which are realizable with today's quantum technology. Our construction uses a non-compact single key functional encryption scheme, the definition of which can be found in Section 3.6.

Construction 4. *Let* $\mathsf{FE} = (\mathsf{FE.Setup}, \mathsf{FE.KeyGen}, \mathsf{FE.Enc}, \mathsf{FE.Dec})$ *be a single-key selectively secure functional encryption scheme. Let* $\mathsf{Ext} : \{0,1\}^l \times \{0,1\}^d \to \{0,1\}^n$ *be a* (t, ϵ)*-randomness extractor with* $l = q + poly(\kappa)$ *where* q *is the quantum memory bound and* $d = poly(\kappa)$*. The quantum incompressible encryption scheme is made up of the algorithms* $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ *which are defined below:*

$\mathsf{KeyGen}(1^\kappa, 1^q)$: *Run* $\mathsf{FE.Setup}(1^\kappa) \to (\mathsf{FE.mpk}, \mathsf{FE.msk})$*. Then generate the secret key for the following function* f_v *parametrized by a hardcoded* $v \in \{0,1\}^{d+n+l}$*:*

$$f_v(s' = (s, z, \boldsymbol{\theta}), \text{flag}) = \begin{cases} s' & \text{if flag} = 0 \\ s' \oplus v & \text{if flag} = 1 \end{cases}$$

Generate $\mathsf{sk} = \mathsf{FE.sk}_{f_v} \leftarrow \mathsf{FE.KeyGen}(\mathsf{FE.msk}, f_v)$ *and output* $\mathsf{pk} = \mathsf{FE.mpk}$ *and* sk.

Enc($\mathsf{pk}, m \in \{0,1\}^n$): *Sample* $s \in \{0,1\}^d$ *as a seed for the randomness extractor. Sample* $\mathbf{x} \in \{0,1\}^l$ *and compute* $z = \mathsf{Ext}(x,s) \oplus m$. *Sample* $\boldsymbol{\theta}$ *and encode* $\mathbf{x}$ *into the quantum state* $|\phi\rangle = \bigotimes_i H^{\boldsymbol{\theta}_i}|x_i\rangle$. *Compute* $\mathsf{FE.ct} = \mathsf{FE.Enc}(\mathsf{FE.mpk}, ((s \,\|\, z \,\|\, \boldsymbol{\theta}), 0))$. *Output the ciphertext* $\mathsf{ct} = (\mathsf{FE.ct}, |\phi\rangle)$.

Dec($\mathsf{sk}, \mathsf{ct} = (\mathsf{FE.ct}, |\phi\rangle)$): *Decrypt the FE ciphertext using the functional secret key:* $(s \,\|\, z \,\|\, \boldsymbol{\theta}) \leftarrow \mathsf{FE.Dec}(\mathsf{sk}, \mathsf{FE.ct})$. *Measure the state* $|\phi\rangle$ *in the basis* $\boldsymbol{\theta}$ *and compute* $m = \mathsf{Ext}(x,s) \oplus z$.

Guan et al. [36] give an instantiation of the functional encryption scheme from any CPA-secure public key encryption scheme for the specific functionality f_v that is needed in the construction.

Theorem 11. *Given a single-key selectively secure FE scheme and a* $(poly(\kappa), negl(\kappa))$ *min-entropy extractor the scheme from Construction 4 is a quantum incompressible encryption scheme.*

Proof. We prove the property by a series of hybrids.

Hybrid 0. The first hybrid is the $\mathsf{Exp}^{\mathsf{QIE}}_{\mathcal{A}}(\kappa)$ experiment where $b = 0$.

Hybrid 1. We change the flag bit from 0 to 1 and encrypt $s' \oplus v$ instead of s'. Therefore $\mathsf{FE.ct} \leftarrow \mathsf{FE.Enc}(\mathsf{FE.mpk}, (s' \oplus v, 1))$.

Lemma 27. $|p_0 - p_1| \leq negl(\kappa)$, *if* FE *is a single key selective functional encryption scheme.*

Proof. Note that the decryption algorithm outputs the same value as before $f_v(s', 0) = s' = f_v(s' \oplus v, 1)$. An adversary that is able to distinguish between Hybrid 0 and Hybrid 1 can break the single-key selective security property of the underlying functional encryption scheme. Let $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ be the adversary that distinguishes the hybrids. Then we can build an adversary $\mathcal{A}'$ that breaks the FE scheme:

1. Send 1^κ to $\mathcal{A}_1$ and receive 1^q.
2. Receive $\mathsf{FE.mpk}$ and send it to $\mathcal{A}_1$.
3. Receive the challenge ciphertexts m_0 and m_1.
4. As in the honest encryption algorithm sample $s, \mathbf{x}$ and compute $\mathsf{Ext}(\mathbf{x}, s) \oplus m_0 = z$. Sample $\boldsymbol{\theta}$ and encode the quantum state $|\phi\rangle = \bigotimes_i H^{\boldsymbol{\theta}_i}|x_i\rangle$. Sample uniformly random v and set $s' = (s \,\|\, z \,\|\, \boldsymbol{\theta})$. Send $FE.m_0 = (s', 0)$ and $\mathsf{FE}.m_1 = (s' \oplus v, 1)$ to the FE challenger.
5. Query f_v to the challenger and receive $\mathsf{FE.sk}_{f_v}$ in response.
6. Receive $\mathsf{FE.ct}$ in response and forward $(\mathsf{FE.ct}, |\phi\rangle)$ to $\mathcal{A}_1$
7. Forward $\mathsf{FE.sk}_{f_v}$ to $\mathcal{A}_2$.
8. If $\mathcal{A}_2$ says Hybrid 0 output 0, if $\mathcal{A}_2$ says Hybrid 1 output 1.

If $\mathsf{FE.ct}$ was an encryption of m_0 the adversary receives the ciphertext as in Hybrid 0, if m_1 the adversary receives the ciphertext as in Hybrid 1. Therefore an adversary that can distinguish Hybrid 0 from Hybrid 1 with more than negligible probability can break the security property of the functional encryption scheme with more than negligible probability. □

Hybrid 2. During KeyGen only compute $(\mathsf{FE.mpk}, \mathsf{FE.msk}) \leftarrow \mathsf{FE.Setup}(\kappa)$. Upon receiving the challenge messages, sample $u \in \{0,1\}^{n+d+l}$. Compute $\mathsf{FE.ct} = \mathsf{FE.Enc}(\mathsf{FE.mpk}, (u, 1))$. Sample $\boldsymbol{\theta}, \mathbf{x} \in \{0,1\}^n$ and compute $|\phi\rangle = \bigotimes_i H^{\boldsymbol{\theta}_i}|x_i\rangle$. Send $(\mathsf{FE.ct}, |\phi\rangle)$ to $\mathcal{A}_1$. Then sample s and compute $z = \mathsf{Ext}(\mathbf{x}, s) \oplus m_0$. Set $s' = (s \,\|\, z \,\|\, \boldsymbol{\theta})$ and let $v = s' \oplus u$ and compute the secret key for v: $\mathsf{sk} = \mathsf{FE.sk}_{f_v} \leftarrow \mathsf{FE.KeyGen}(\mathsf{FE.msk}, f_v)$.

Lemma 28. $p_1 = p_2$

Proof. In Hybrid 2 we delay the computation of the secret key until the second phase of the experiment. We encrypt uniform u and compute $v = s' \oplus u$. In Hybrid 1 we sample uniform v and encrypt $u = s' \oplus v$. These distribution are indistinguishable. □

Hybrid 3:. Replace the output of the randomness extractor by a uniformly random value $r \in \{0,1\}^n$.

Lemma 29. $|p_2 - p_3| \leq negl(\kappa)$, *if* Ext *is a* (w, ε)*-Extractor.*

Proof. The elements $\mathsf{FE.ct}$ and $|\phi\rangle$ are independent of each other. Later the basis of the state $|\phi\rangle$ is revealed. Based on the definition of a (w, ε)-Extractor replacing the output by a uniformly random value cannot be detected by the adversary with probability larger than ε which is negligible. For this statement to be applicable we need to show that the min-entropy of x is at least w. Let the random variable $X = x$ and let Y describe any classical information that the adversary holds and let Q be a random variable describing any quantum information of at most size q that the adversary holds. Let Θ be the basis choice that is revealed later. Then we can apply Lemma 11:

$$H_{\min}^{\varepsilon'}(X|YQ\Theta) \geq n\left(\frac{1}{2} - 2\lambda\right) - q$$

We can choose an appropriate randomness extractor such that $n\left(\frac{1}{2} - 2\lambda\right) - q > w$ and we incur an additional error ε' since we are given an X with a smooth min-entropy bound instead of min-entropy, see Lemma 1. Since ε and ε' are negligible the Lemma is shown. □

Hybrid 4. Set the bit b to be 1 instead of 0.

Lemma 30. $p_3 = p_4$

Proof. Since the message m_b gets XORed to a uniformly random value, the change is not noticable for the adversary. □

Hybrid 5. Instead of the uniformly random value r we go back to using the extractor output.

Lemma 31. $|p_4 - p_5| \leq negl(\kappa)$

Proof. The lemma holds by a similar argument as Lemma 29. □

Hybrid 6. Switch back to creating the secret key immediately and encrypting the value $s' \oplus v$ instead of a random value.

Lemma 32. $|p_5 - p_6| \leq negl(\kappa)$

Proof. The Lemma holds by a similar argument as Lemma 28. □

Hybrid 7. Switch back to creating the real ciphertext $\mathsf{FE.ct} = \mathsf{FE.Enc}(\mathsf{FE.mpk}, (s', 0))$. This is the $\mathsf{Exp}^{\mathsf{QIE}}_{\mathcal{A}}(\kappa)$ experiment where $b = 1$.

Lemma 33. $|p_6 - p_7| \leq negl(\kappa)$

Proof. The Lemma holds by a similar argument as Lemma 27. □

This concludes the proof of Theorem 11. □

9.2 Hybrid Incompressible Encryption

In the QIE scheme from the previous section the quantum part of the ciphertext grows with the length of the message. Using a hybrid encryption approach we can construct a quantum incompressible encryption scheme as follows: take a QIE scheme and encrypt the secret key of a symmetric encryption scheme. Then use the symmetric encryption scheme to encrypt arbitrarily long messages. The quantum part of the ciphertext only depends on the length of the key of the symmetric scheme.

Construction 5. *Let* $\mathsf{QI.PKE} = (\mathsf{QI.KeyGen}, \mathsf{QI.Enc}, \mathsf{QI.Dec})$ *be a quantum incompressible encryption scheme. Let* $\mathsf{SK} = (\mathsf{SK.KeyGen}, \mathsf{SK.Enc}, \mathsf{SK.Dec})$ *be a classical symmetric key encryption scheme. Then a quantum incompressible encryption scheme* $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ *can be constructed as follows:*

$\mathsf{KeyGen}(1^\kappa, 1^q)$: *Run* $\mathsf{QI.KeyGen}(1^\kappa, 1^q) \to (\mathsf{QI.pk}, \mathsf{QI.sk})$. *Output* $(\mathsf{pk}, \mathsf{sk}) = (\mathsf{QI.pk}, \mathsf{QI.sk})$.

$\mathsf{Enc}(\mathsf{pk}, \mathsf{m} \in \{0,1\}^n)$: *Generate a secret key from the symmetric key encryption scheme:* $\mathsf{SK.KeyGen}(1^\kappa) = \mathsf{SK.sk}$. *Encrypt the secret key using the* QI.PKE *scheme:* $\mathsf{QI.Enc}(\mathsf{pk}, \mathsf{SK.sk}) = \mathsf{ct}_0$ *and encrypt the message using the classical symmetric key scheme:* $\mathsf{SK.Enc}(\mathsf{SK.sk}, \mathsf{m}) = \mathsf{ct}_1$.

$\mathsf{Dec}(\mathsf{sk}, \mathsf{ct} = (\mathsf{ct}_0, \mathsf{ct}_1))$: *Decrypt the quantum ciphertext:* $\mathsf{QI.Dec}(\mathsf{sk}, \mathsf{ct}_0) \to \mathsf{SK.sk}$ *and use the obtained secret key to decrypt the message* $\mathsf{SK.Dec}(\mathsf{SK.sk}, \mathsf{ct}_1) = \mathsf{m}$.

Correctness. Based on the correctness of the underlying quantum incompressible encryption scheme and the underlying symmetric key encryption scheme the scheme from Construction 5 is correct.

Theorem 12. *Given a IND-CPA-secure symmetric encryption scheme and a quantum incompressible encryption scheme, the hybrid scheme Construction 5 is a quantum incompressible encryption scheme in the quantum decoherence model.*

Proof (sketch). We start with an encryption to m_0. We can replace the secret key of the symmetric key encryption scheme by relying on the security of the quantum incompressible encryption scheme. Then we can switch the message from m_0 to m_1 by relying on the security of the symmetric key encryption scheme. □

10 On the Necessity of the Random Oracle

We show how to construct an everlasting hiding and unconditionally binding quantum bit commitment from a linear $[N, K, D]$-code and from a non-interactive, statistical binding commitment $\mathcal{H}$, if the later was modeled as a random oracle. The commitment $\mathcal{H}$ allows the sender to commit to the uniform random bases θ, the extraction seed s, the extractor message σ and a random string r, while hiding the same from the receiver during execution of the protocol. In this section we want to demonstrate the significance of the random oracle for the classical commitment by presenting an alternative construction in the plain model. Specifically, we show that a statistical binding commitment instantiated with quantum fully homomorphic encryption (QFHE) is not sufficient to achieve everlasting security due to to the possibility to perform a measurement relative to the classical committed values.

A quantum fully homomorphic encryption scheme (cf. [16, §3.2], [50]) is a quadruple of algorithms QHE.KeyGen, QHE.Enc, QHE.Dec and QHE.Eval that allows to homomorphically evaluate a quantum circuit U on a quantum state $|\psi\rangle$. Let QHE.KeyGen output a classical pair of keys pk, sk such that the public key pk is contained in the common reference string of the commitment scheme. Let QHE.Enc encrypt a quantum state, performing the map $|\psi\rangle \mapsto \mathsf{Enc}(|\psi\rangle)$, and QHE.Dec decrypt a quantum state, performing the map $\mathsf{Enc}(|\psi\rangle) \mapsto |\psi\rangle$. Finally, let QHE.Eval apply a quantum circuit U to a quantum ciphertext $\mathsf{Enc}(|\psi\rangle)$, *i.e.*, $\mathsf{Enc}(|\psi\rangle) \mapsto \mathsf{Enc}(U|\psi\rangle)$. Note that if the circuit U contains a measurement, then the resulting ciphertext is classical in a quantum register and can still be decrypted correctly (cf. [16, §2.1]), if the secret key of the QFHE scheme is known. We can now instantiate the non-interactive, statistically binding commitment scheme of the quantum bit commitment using the encryption of the QFHE, *i.e.*, $\mathsf{com}\mu = (\text{QHE.Enc}(\mathsf{pk}, (\theta \,\|\, s \,\|\, \sigma \,\|\, r), |\phi\rangle, c)$, where $|\phi\rangle = \bigotimes_i H^{\theta_i}|x_i\rangle$, $c = \text{PC}x$ and $\sigma = \mathsf{Ext}(x, s) \oplus \mu$ are constructed as before. Indeed, if the public key of the QFHE scheme is contained in the common reference string and QFHE is perfectly correct, then the encryption is statistically binding. If the underlying fully homomorphic encryption is q-IND-CPA, then the commitment is quantum-computationally hiding.

Consider an everlasting adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ where $\mathcal{A}_1$ receives the quantum bit commitment $(|\phi\rangle, h, \mathbf{c})$ with $h := \text{QHE.}\textsc{Enc}(\mathsf{pk}, (\theta \,\|\, s \,\|\, \sigma \,\|\, r))$. First, define a quantum circuit that unmasks the quantum bit commitment: Let U_{break} be a quantum circuit that takes as input the values θ, s, σ and $|\phi\rangle$. The circuit first measures $|\phi\rangle$ with respect to bases θ resulting in a codeword $\mathbf{x}$, then computes $\mathsf{Ext}(\mathbf{x}, s)$, and finally outputs $\mu \leftarrow \mathsf{Ext}(\mathbf{x}, s) \oplus \sigma$. Without loss of generality we can assume that the measurement is moved to the end of the circuit.

Given the quantum state $|\phi\rangle$ and the commitment to the bases $\text{QHE.}\textsc{Enc}(\mathsf{pk}, (\theta \,\|\, s \,\|\, \sigma \,\|\, r))$, the adversary $\mathcal{A}_1$ can first encrypt the quantum state resulting in $\mathsf{Enc}(|\phi\rangle)$ and then homomorphically evaluate the circuit using $\text{QHE.}\textsc{Eval}$. This results in a classical ciphertext $\mathsf{Enc}(U_{\text{break}}|\phi\rangle) = \mathsf{Enc}(\mu)$. The resulting string is a q-IND-CPA secure encryption, and thus the the polynomial bounded adversary cannot decrypt the output.

However, after the adversary is computationally unbounded, $\mathcal{A}_2$ can break the QFHE scheme, acquiring the secret key sk and decrypt $\mathsf{Enc}(\mu)$, receiving the output of the quantum circuit in plain. If the QFHE scheme is correct, this is exactly the committed to message of the sender, and thus the quantum commitment instantiated with QFHE does not achieve everlasting security. It is therefore conceivable that additional *new* properties are required to achieve everlasting security for (quantum) bit commitments, which were fulfilled by the quantum random oracle, but are not by *any* statistical binding commitment in the plain model.

11 Conclusion

We introduced quantum decoherence as a new cryptographic assumption that reflects the major challenge of keeping quantum states coherent for a long period of time.

Under this assumption, we constructed a composable commitment scheme in the $\mathcal{F}_{\mathsf{CRS}}$-hybrid and QROM model, which enables composable general MPC with everlasting security. To model and prove the security of our protocols, we proposed a variant of everlasting quantum UC security. We justify the use of the random oracle by considering a variant of our commitment scheme where the everlasting security is surprisingly lost if the random oracle is replaced with a certain statistically binding commitment scheme based on quantum fully-homomorphic encryption.

Additional results in the quantum decoherence model include everlasting public-key encryption, round-efficient composable oblivious transfer with semi-honest everlasting security against corrupted receivers and statistical security against corrupted senders as well as quantum incompressible encryption.

Acknowledgments. Parts of this work were supported by funding from the topic Methods for Engineering Secure Systems (No. 46.23.01) of the Helmholtz Association (HGF) and by KASTEL Security Research Labs. Alexander Koch acknowledges the support of the French Agence Nationale de la Recherche

(ANR), under the France 2030 ANR Project ANR-22-PECY-003 SecureCompute. The authors would like to thank Willi Geiselmann for fruitful discussions regarding codes, and Roland Gröll and Wasilij Beskorovajnov for discussions related to Section 10. Additionally, we would like to thank the anonymous reviewers for helpful comments.

References

1. Aaronson, S.: Shadow Tomography of Quantum States. SIAM Journal on Computing **49**(5), STOC18–368–STOC18–394 (2020). https://doi.org/10.1137/18M120275X. eprint: https://doi.org/10.1137/18M120275X
2. Agrawal, S., Gorbunov, S., Vaikuntanathan, V., Wee, H.: Functional Encryption: New Perspectives and Lower Bounds. In: Canetti, R., Garay, J.A. (eds.) Advances in Cryptology – CRYPTO 2013, Part II. Lecture Notes in Computer Science, pp. 500–518. Springer, Heidelberg, Germany, Santa Barbara, CA, USA (2013). https://doi.org/10.1007/978-3-642-40084-1_28
3. Barhoush, M., Salvail, L.: Functional encryption in the bounded storage models. arXiv preprint arXiv:2309.06702 (2023)
4. Barhoush, M., Salvail, L.: Powerful Primitives in the Bounded Quantum Storage Model. arXiv preprint arXiv:2302.05724 (2023)
5. Bartusek, J., Coladangelo, A., Khurana, D., Ma, F.: One-Way Functions Imply Secure Computation in a Quantum World. In: Annual International Cryptology Conference, pp. 467–496 (2021)
6. Bartusek, J., Khurana, D.: Cryptography with Certified Deletion. In: Handschuh, H., Lysyanskaya, A. (eds.) Advances in Cryptology – CRYPTO 2023, Part V. Lecture Notes in Computer Science, pp. 192–223. Springer, Heidelberg, Germany, Santa Barbara, CA, USA (2023). https://doi.org/10.1007/978-3-031-38554-4_7
7. Bartusek, J., Khurana, D., Poremba, A.: Publicly-Verifiable Deletion via Target-Collapsing Functions. In: CRYPTO (5). Lecture Notes in Computer Science, pp. 99–128. Springer (2023)
8. Bartusek, J. *et al.*: Obfuscation and Outsourced Computation with Certified Deletion. IACR Cryptol. ePrint Arch. (2023)
9. Bellare, M., Rogaway, P.: Random Oracles are Practical: A Paradigm for Designing Efficient Protocols. In: Denning, D.E., Pyle, R., Ganesan, R., Sandhu, R.S., Ashby, V. (eds.) ACM CCS 93: 1st Conference on Computer and Communications Security, pp. 62–73. ACM Press, Fairfax, Virginia, USA (1993). https://doi.org/10.1145/168588.168596
10. Bennett, C.H., Brassard, G.: Quantum cryptography: Public key distribution and coin tossing. Theoretical computer science **560**, 7–11 (2014)
11. Bennett, C.H., Brassard, G., Crépeau, C., Jozsa, R., Peres, A., Wootters, W.K.: Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. Phys. Rev. Lett. **70**, 1895–1899 (1993). https://doi.org/10.1103/PhysRevLett.70.1895
12. Berger, R. *et al.*: Composable Long-Term Security with Rewinding. In: Rothblum, G.N., Wee, H. (eds.) Theory of Cryptography - 21st International Conference, TCC 2023, Taipei, Taiwan, November 29 - December 2, 2023, Proceedings, Part IV. Lecture Notes in Computer Science, pp. 510–541. Springer (2023). https://doi.org/10.1007/978-3-031-48624-1_19

13. Bhushan, K., Goyal, R., Koppula, V., Narayanan, V., Prabhakaran, M., Rajasree, M.S.: Leakage-Resilient Incompressible Cryptography: Constructions and Barriers. In: Chung, K.-M., Sasaki, Y. (eds.) Advances in Cryptology – ASIACRYPT 2024, pp. 201–234. Springer Nature Singapore, Singapore (2025)
14. Boneh, D., Dagdelen, Ö., Fischlin, M., Lehmann, A., Schaffner, C., Zhandry, M.: Random Oracles in a Quantum World. In: Lee, D.H., Wang, X. (eds.) Advances in Cryptology – ASIACRYPT 2011. Lecture Notes in Computer Science, pp. 41–69. Springer, Heidelberg, Germany, Seoul, South Korea (2011). https://doi.org/10.1007/978-3-642-25385-0_3
15. Boneh, D., Sahai, A., Waters, B.: Functional Encryption: Definitions and Challenges. In: Ishai, Y. (ed.) TCC 2011: 8th Theory of Cryptography Conference. Lecture Notes in Computer Science, pp. 253–273. Springer, Heidelberg, Germany, Providence, RI, USA (2011). https://doi.org/10.1007/978-3-642-19571-6_16
16. Brakerski, Z.: Quantum FHE (Almost) As Secure As Classical. In: Shacham, H., Boldyreva, A. (eds.) Advances in Cryptology – CRYPTO 2018, Part III. Lecture Notes in Computer Science, pp. 67–95. Springer, Heidelberg, Germany, Santa Barbara, CA, USA (2018). https://doi.org/10.1007/978-3-319-96878-0_3
17. Branco, P., Döttling, N., Dujmovic, J.: Rate-1 Incompressible Encryption from Standard Assumptions. In: TCC (2). Lecture Notes in Computer Science, pp. 33–69. Springer (2022)
18. Brassard, G., Crépeau, C., Jozsa, R., Langlois, D.: A Quantum Bit Commitment Scheme Provably Unbreakable by both Parties. In: 34th Annual Symposium on Foundations of Computer Science, pp. 362–371. IEEE Computer Society Press, Palo Alto, CA, USA (1993). https://doi.org/10.1109/SFCS.1993.366851
19. Broadbent, A., Culf, E., Rochette, D.: Optimal Untelegraphable Encryption and Implications for Uncloneable Encryption. (2025). arXiv: 2510.00903 [quant-ph]
20. Broadbent, A., Islam, R.: Quantum encryption with certified deletion. In: Theory of Cryptography: 18th International Conference, TCC 2020, Durham, NC, USA, November 16–19, 2020, Proceedings, Part III 18, pp. 92–122 (2020)
21. Broadbent, A., Islam, R.: Quantum Encryption with Certified Deletion. In: Pass, R., Pietrzak, K. (eds.) TCC 2020: 18th Theory of Cryptography Conference, Part III. Lecture Notes in Computer Science, pp. 92–122. Springer, Heidelberg, Germany, Durham, NC, USA (2020). https://doi.org/10.1007/978-3-030-64381-2_4
22. Canetti, R.: Universally Composable Security: A New Paradigm for Cryptographic Protocols. In: 42nd Annual Symposium on Foundations of Computer Science, pp. 136–145. IEEE Computer Society Press, Las Vegas, NV, USA (2001). https://doi.org/10.1109/SFCS.2001.959888
23. Canetti, R., Feige, U., Goldreich, O., Naor, M.: Adaptively secure multi-party computation. In: Proceedings of the twenty-eighth annual ACM symposium on Theory of computing, pp. 639–648 (1996)
24. Canetti, R., Fischlin, M.: Universally Composable Commitments. In: Kilian, J. (ed.) Advances in Cryptology – CRYPTO 2001. Lecture Notes in Computer Science, pp. 19–40. Springer, Heidelberg, Germany, Santa Barbara, CA, USA (2001). https://doi.org/10.1007/3-540-44647-8_2
25. Canetti, R., Halevi, S., Katz, J.: A Forward-Secure Public-Key Encryption Scheme. In: Biham, E. (ed.) Advances in Cryptology – EUROCRYPT 2003. Lecture Notes in Computer Science, pp. 255–271. Springer, Heidelberg, Germany, Warsaw, Poland (2003). https://doi.org/10.1007/3-540-39200-9_16

26. Canetti, R., Lindell, Y., Ostrovsky, R., Sahai, A.: Universally composable two-party and multi-party secure computation. In: 34th Annual ACM Symposium on Theory of Computing, pp. 494–503. ACM Press, Montréal, Québec, Canada (2002). https://doi.org/10.1145/509907.509980
27. Champion, J., Kitagawa, F., Nishimaki, R., Yamakawa, T.: Untelegraphable Encryption and its Applications. To appear in TCC 2025 (2025). arXiv: 2410.24189 [quant-ph]
28. Coles, P.J., Berta, M., Tomamichel, M., Wehner, S.: Entropic uncertainty relations and their applications. Reviews of Modern Physics **89**(1), 015002 (2017)
29. Damgård, I., Fehr, S., Renner, R., Salvail, L., Schaffner, C.: A Tight High-Order Entropic Quantum Uncertainty Relation with Applications. In: Menezes, A. (ed.) Advances in Cryptology – CRYPTO 2007. Lecture Notes in Computer Science, pp. 360–378. Springer, Heidelberg, Germany, Santa Barbara, CA, USA (2007). https://doi.org/10.1007/978-3-540-74143-5_20
30. Dodis, Y., Reyzin, L., Smith, A.: Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. In: International conference on the theory and applications of cryptographic techniques, pp. 523–540 (2004)
31. Don, J., Fehr, S., Majenz, C., Schaffner, C.: Online-Extractability in the Quantum Random-Oracle Model. In: Dunkelman, O., Dziembowski, S. (eds.) Advances in Cryptology – EUROCRYPT 2022, Part III. Lecture Notes in Computer Science, pp. 677–706. Springer, Heidelberg, Germany, Trondheim, Norway (2022). https://doi.org/10.1007/978-3-031-07082-2_24
32. Dziembowski, S.: On Forward-Secure Storage (Extended Abstract). In: Dwork, C. (ed.) Advances in Cryptology – CRYPTO 2006. Lecture Notes in Computer Science, pp. 251–270. Springer, Heidelberg, Germany, Santa Barbara, CA, USA (2006). https://doi.org/10.1007/11818175_15
33. Garg, S., Gentry, C., Sahai, A., Waters, B.: Witness encryption and its applications. In: Boneh, D., Roughgarden, T., Feigenbaum, J. (eds.) 45th Annual ACM Symposium on Theory of Computing, pp. 467–476. ACM Press, Palo Alto, CA, USA (2013). https://doi.org/10.1145/2488608.2488667
34. Goyal, R., Koppula, V., Rajasree, M.S., Verma, A.: Incompressible Functional Encryption. (2024)
35. Grilo, A.B., Lamontagne, P.: The Round Complexity of Proofs in the Bounded Quantum Storage Model. arXiv preprint arXiv:2405.18275 (2024)
36. Guan, J., Wichs, D., Zhandry, M.: Incompressible Cryptography. In: Dunkelman, O., Dziembowski, S. (eds.) Advances in Cryptology – EUROCRYPT 2022, Part I. Lecture Notes in Computer Science, pp. 700–730. Springer, Heidelberg, Germany, Trondheim, Norway (2022). https://doi.org/10.1007/978-3-031-06944-4_24
37. Guan, J., Wichs, D., Zhandry, M.: Multi-instance Randomness Extraction and Security Against Bounded-Storage Mass Surveillance. In: TCC (3). Lecture Notes in Computer Science, pp. 93–122. Springer (2023)
38. Guan, J., Zhandry, M.: Disappearing Cryptography in the Bounded Storage Model. In: Nissim, K., Waters, B. (eds.) TCC 2021: 19th Theory of Cryptography Conference, Part II. Lecture Notes in Computer Science, pp. 365–396. Springer, Heidelberg, Germany, Raleigh, NC, USA (2021). https://doi.org/10.1007/978-3-030-90453-1_13
39. Haitner, I., Reingold, O.: Statistically-hiding commitment from any one-way function. In: Johnson, D.S., Feige, U. (eds.) 39th Annual ACM Symposium on Theory of Computing, pp. 1–10. ACM Press, San Diego, CA, USA (2007). https://doi.org/10.1145/1250790.1250792

40. Hiroka, T., Kitagawa, F., Morimae, T., Nishimaki, R., Pal, T., Yamakawa, T.: Certified Everlasting Secure Collusion-Resistant Functional Encryption, and More. IACR Cryptol. ePrint Arch. (2023)
41. Hiroka, T., Morimae, T., Nishimaki, R., Yamakawa, T.: Certified Everlasting Functional Encryption. IACR Cryptol. ePrint Arch. (2022)
42. Hiroka, T., Morimae, T., Nishimaki, R., Yamakawa, T.: Certified Everlasting Zero-Knowledge Proof for QMA. In: CRYPTO (1). Lecture Notes in Computer Science, pp. 239–268. Springer (2022)
43. Hiroka, T., Morimae, T., Nishimaki, R., Yamakawa, T.: Quantum Encryption with Certified Deletion, Revisited: Public Key, Attribute-Based, and Classical Communication. In: ASIACRYPT (1). Lecture Notes in Computer Science, pp. 606–636. Springer (2021)
44. Huang, H.-Y., Kueng, R., Preskill, J.: Predicting many properties of a quantum system from very few measurements. Nature Physics **16**(10), 1050–1057 (2020). https://doi.org/10.1038/s41567-020-0932-7
45. Kitagawa, F., Nishimaki, R., Yamakawa, T.: Publicly Verifiable Deletion from Minimal Assumptions. In: TCC (4). Lecture Notes in Computer Science, pp. 228–245. Springer (2023)
46. Koenig, R., Wehner, S., Wullschleger, J.: Unconditional Security From Noisy Quantum Storage. IEEE Trans. Information Theory **58**(3), 1962–1984 (2012). https://doi.org/10.1109/TIT.2011.2177772
47. Koppula, V., Kumar, A., Rajasree, M.S., Swaminathan, H.: Incompressible Encryption Beyond CPA/CCA Security. IACR Communications in Cryptology **2**(2) (2025). https://doi.org/10.62056/ayfhbnja5
48. Lo, H.-K., Chau, H.F.: Unconditional security of quantum key distribution over arbitrarily long distances. science **283**(5410), 2050–2056 (1999)
49. Magri, B., Malavolta, G., Schröder, D., Unruh, D.: Everlasting UC Commitments from Fully Malicious PUFs. Journal of Cryptology **35**(3), 20 (2022). https://doi.org/10.1007/s00145-022-09432-4
50. Mahadev, U.: Classical Homomorphic Encryption for Quantum Circuits. In: 2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS), pp. 332–338 (2018). https://doi.org/10.1109/FOCS.2018.00039
51. Maurer, U.M.: Conditionally-Perfect Secrecy and a Provably-Secure Randomized Cipher. Journal of Cryptology **5**(1), 53–66 (1992). https://doi.org/10.1007/BF00191321
52. Mayers, D.: The Trouble with Quantum Bit Commitment. (1996). arXiv: quant-ph/9603015
53. Mayers, D.: Unconditionally Secure Quantum Bit Commitment is Impossible. Phys. Rev. Lett. **78**, 3414–3417 (1997). https://doi.org/10.1103/PhysRevLett.78.3414
54. Müller-Quade, J., Unruh, D.: Long-Term Security and Universal Composability. In: Vadhan, S.P. (ed.) TCC 2007. Lecture Notes in Computer Science, pp. 41–60. Springer (2007). https://doi.org/10.1007/978-3-540-70936-7_3
55. Müller-Quade, J., Unruh, D.: Long-Term Security and Universal Composability. In: Vadhan, S.P. (ed.) TCC 2007: 4th Theory of Cryptography Conference. Lecture Notes in Computer Science, pp. 41–60. Springer, Heidelberg, Germany, Amsterdam, The Netherlands (2007). https://doi.org/10.1007/978-3-540-70936-7_3
56. Müller-Quade, J., Unruh, D.: Long-Term Security and Universal Composability. Journal of Cryptology **23**(4), 594–671 (2010). https://doi.org/10.1007/s00145-010-9068-8

57. Peikert, C., Vaikuntanathan, V., Waters, B.: A Framework for Efficient and Composable Oblivious Transfer. In: Wagner, D. (ed.) Advances in Cryptology – CRYPTO 2008. Lecture Notes in Computer Science, pp. 554–571. Springer, Heidelberg, Germany, Santa Barbara, CA, USA (2008). https://doi.org/10.1007/978-3-540-85174-5_31
58. Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. In: Gabow, H.N., Fagin, R. (eds.) 37th Annual ACM Symposium on Theory of Computing, pp. 84–93. ACM Press, Baltimore, MA, USA (2005). https://doi.org/10.1145/1060590.1060603
59. Renner, R.: Security of quantum key distribution. International Journal of Quantum Information **6**(01), 1–127 (2005)
60. Romerstein, H., Breindel, E.: The Venona Secrets: Exposing Soviet Espionage and America's Traitors. Simon and Schuster (2001)
61. Schaffner, C.: Cryptography in the bounded-quantum-storage model. arXiv preprint arXiv:0709.0289 (2007)
62. Shor, P.W., Preskill, J.: Simple proof of security of the BB84 quantum key distribution protocol. Physical review letters **85**(2), 441 (2000)
63. Sipser, M., Spielman, D.: Expander codes. IEEE Transactions on Information Theory **42**(6), 1710–1722 (1996). https://doi.org/10.1109/18.556667
64. Unruh, D.: Collapse-Binding Quantum Commitments Without Random Oracles. In: Cheon, J.H., Takagi, T. (eds.) Advances in Cryptology – ASIACRYPT 2016, Part II. Lecture Notes in Computer Science, pp. 166–195. Springer, Heidelberg, Germany, Hanoi, Vietnam (2016). https://doi.org/10.1007/978-3-662-53890-6_6
65. Unruh, D.: Everlasting Multi-party Computation. In: Canetti, R., Garay, J.A. (eds.) Advances in Cryptology – CRYPTO 2013, Part II. Lecture Notes in Computer Science, pp. 380–397. Springer, Heidelberg, Germany, Santa Barbara, CA, USA (2013). https://doi.org/10.1007/978-3-642-40084-1_22
66. Unruh, D.: Everlasting Multi-party Computation. Journal of Cryptology **31**(4), 965–1011 (2018). https://doi.org/10.1007/s00145-018-9278-z
67. Unruh, D.: Universally Composable Quantum Multi-party Computation. In: Gilbert, H. (ed.) Advances in Cryptology – EUROCRYPT 2010. Lecture Notes in Computer Science, pp. 486–505. Springer, Heidelberg, Germany, French Riviera (2010). https://doi.org/10.1007/978-3-642-13190-5_25
68. Wiesner, S.: Conjugate Coding. SIGACT News **15**(1), 78–88 (1983). https://doi.org/10.1145/1008908.1008920
69. Yogev, E., Ben-David, S.: Incompressible Encryption with Everlasting Security. To appear in TCC 2025 (2025). eprint: https://eprint.iacr.org/2025/975
70. Zhandry, M.: How to Record Quantum Queries, and Applications to Quantum Indifferentiability. In: Boldyreva, A., Micciancio, D. (eds.) Advances in Cryptology – CRYPTO 2019, Part II. Lecture Notes in Computer Science, pp. 239–268. Springer, Heidelberg, Germany, Santa Barbara, CA, USA (2019). https://doi.org/10.1007/978-3-030-26951-7_9
71. Zhandry, M.: Secure Identity-Based Encryption in the Quantum Random Oracle Model. In: Safavi-Naini, R., Canetti, R. (eds.) Advances in Cryptology – CRYPTO 2012. Lecture Notes in Computer Science, pp. 758–775. Springer, Heidelberg, Germany, Santa Barbara, CA, USA (2012). https://doi.org/10.1007/978-3-642-32009-5_44

Supplementary Material

A Wiesner Coding Extraction

In the following lemma, we show that upon receiving a quantum state an extractor can measure and recreate the state such that the honest receiver obtains the same output for the positions where the state is measured in the same basis.

Exp_1	Exp_2
$\mathcal{A}$: Choose $\theta, \theta^* \in \{0,1\}^n$ and create $\|\phi\rangle$.	$\mathcal{A}$: Choose $\theta, \theta^* \in \{0,1\}^n$ and create $\|\phi\rangle$.
	$\mathsf{Ext}(\|\phi\rangle, \theta, \theta^*)$: measure the state $\|\phi\rangle$ in basis θ and obtain x'. Create the new state $\|\phi'\rangle = \bigotimes_i H^{\theta_i} x'_i$. Forward $\|\phi'\rangle$ and θ^* to Rec_1.
$\mathsf{Rec}_1(\|\phi\rangle, \theta^*)$: measure $\|\phi\rangle$ in basis θ^* to obtain x^*.	$\mathsf{Rec}_1(\|\phi'\rangle, \theta^*)$: measure $\|\phi'\rangle$ in basis θ^* to obtain x^*.
$\mathsf{Rec}_2(x^*, \theta)$: for $\theta_i = \theta_i^*$ output x_i^*.	$\mathsf{Rec}_2(x^*, \theta)$: for $\theta_i = \theta_i^*$ output x_i^*.

Lemma 34. *The outputs of* Exp_1 *and* Exp_2 *are identically distributed.*

Proof. By computing the partial density matrix of each experiment, we can see that the output is the same.

Let $M_x^{\theta^*} = M_x^{\theta_1^*} \otimes \cdots \otimes M_x^{\theta_n^*}$ be the measurement operator that Rec_1 applies to the state $\rho = |\phi\rangle\langle\phi|$. The post measurement state is $\rho' = \sum_x M_x \rho M_x^\dagger$. We split the state into subsystem A and B such that all qubits at position i where $\theta_i = \theta_i^*$ are in subsystem A, the rest are in subsystem B.

$$\begin{aligned} tr_B(\rho') &= tr_B\left(\sum_x M_x^{\theta_1^*} \otimes \dots M_x^{\theta_n^*} \ \rho \ (M_x^{\theta_1^*} \otimes \dots M_x^{\theta_n^*})^\dagger\right) \\ &= \sum_x tr_B(\bigotimes_{i=1\dots n} M_x^{\theta_i^*} \ tr_{\bar{i}}(\rho) \ M_x^{\theta_i^*\,\dagger}) \\ &= \sum_x \bigotimes_{i \in A} M_x^{\theta_i^*} \ tr_{\bar{i}}(\rho) \ M_x^{\theta_i^*\,\dagger} \end{aligned}$$

In Exp_2 the receiver applies the same measurement operator as in the first experiment, but the extractor first applies his own measurement $E_x^\theta = E_x^{\theta_1} \otimes \cdots \otimes E_x^{\theta_n}$. Let $\rho'' = \sum_x M_x (\sum_{x'} E_{x'} \ \rho \ E_{x'}^\dagger) M_x^\dagger$ be the post measurement state. We define subsystems A and B as above.

$$
\begin{aligned}
tr_B(\rho'') &= tr_B(\sum_x M_x(\sum_{x'} E_{x'}\ \rho\ E_{x'}^\dagger)M_x^\dagger) \\
&= \sum_x \sum_{x'} tr_B(M_x^{\theta_1^*} \otimes \dots M_x^{\theta_n^*} E_x^{\theta_1} \otimes \dots E_{x'}^{\theta_n}\ \rho\ (E_{x'}^{\theta_1} \otimes \dots E_x^{\theta_n})^\dagger (M_x^{\theta_1^*} \otimes \dots M_x^{\theta_n^*})^\dagger) \\
&= \sum_x \sum_{x'} tr_B(\bigotimes_{i=1\dots n} E_{x'}^{\theta_i} M_x^{\theta_i^*}\ tr_{\bar{i}}(\rho)\ {E_{x'}^{\theta_i}}^\dagger {M_x^{\theta_i^*}}^\dagger) \\
&= \sum_x \sum_{x'} \bigotimes_{i\in A} E_{x'}^{\theta_i} M_x^{\theta_i^*}\ tr_{\bar{i}}(\rho)\ {E_{x'}^{\theta_i}}^\dagger {M_x^{\theta_i^*}}^\dagger \\
&= \sum_x \bigotimes_{i\in A} M_x^{\theta_i^*}\ tr_{\bar{i}}(\rho)\ {M_x^{\theta_i^*}}^\dagger
\end{aligned}
$$

In the subset A we are restricted to elements E^{θ_i} and $M^{\theta_i^*}$ where $\theta_i = \theta_i^*$ therefore $E_{x'}^i$ and M_x^i are measurements in the same basis. If a state is measured in a certain basis and then measured again in the same basis we know that only the same output $x = x'$ is possible.

□

B Proofs of the Properties of the UC-Notion

In the following, we re-state the properties of our notion and give the proofs.

Proposition 6 (Reflexivity, Transitivity). *q-everlasting quantum-UC security with decoherence is reflexive and transitive.*

Proof. The proof is very similar to the one in [66].

Reflexivity. For $\mathcal{S} = \mathcal{A}$ and $N = \pi \cup \{\mathcal{Z}, \mathcal{A}\}$ resp. $N' = \pi \cup \{\mathcal{Z}, \mathcal{S}\}$, it follows that $\text{LTState}_N(\kappa, a)$ and $\text{LTState}_{N'}(\kappa, a)$ are identical and their trace distance is zero.

Transitivity. Let π, ϕ, σ be protocols such that π q-eqUC-D-emulates ϕ and ϕ q-eqUC-D-emulates σ. To prove the transitivity, it suffices to use the triangle inequality of the trace distance and the fact that the simulator $\mathcal{S}_1$ for π is an adversary for ϕ. □

Like with standard UC security and everlasting quantum UC security, the dummy adversary is complete for our new notion.

Proposition 7 (Completeness of the Dummy Adversary). *Let $\mathcal{D}$ be the dummy adversary. Let π and ϕ be protocols. If π q-eqUC-D-emulates ϕ for $\mathcal{D}$, then π q-eqUC-D-emulates ϕ for every QPT adversary $\mathcal{A}$.*

Proof. Let $\mathcal{S}_\mathcal{D}$ be the simulator for the dummy adversary. We construct an adversary $\mathcal{S}_\mathcal{A}$ for a quantum-polynomial-time adversary $\mathcal{A}$ as follows:

1. In the online phase, forward messages between $\mathcal{A}$, $\mathcal{S}_\mathcal{D}$, the environment and the protocol as in [66].
2. On its last activation, $\mathcal{S}_\mathcal{A}$ copies the contents of its register $\mathcal{H}^{class}$ to $\mathcal{H}^{class}$ of its internal emulation of $\mathcal{A}$ and activates $\mathcal{A}$.
3. Then, it copies the contents of $\mathcal{H}^{class}$ of its internal emulation of $\mathcal{A}$ to $\mathcal{H}^{class}$ of its internal emulation of $\mathcal{S}_\mathcal{D}$ and activates $\mathcal{S}_\mathcal{D}$.
4. Finally, it copies $\mathcal{H}^{class}$ of its internal emulation of $\mathcal{S}_\mathcal{D}$ to its own register $\mathcal{H}^{class}$.

It follows from the definition of $\mathcal{S}_\mathcal{A}$ and the triangle inequality of the trace distance that the trace distance between $\mathrm{LTState}_N(\kappa, a)$ and $\mathrm{LTState}_{N'}(\kappa, a)$ with $N = \pi \cup \{\mathcal{Z}, \mathcal{A}\}$ resp. $N' = \phi \cup \{\mathcal{Z}, \mathcal{S}_\mathcal{A}\}$ is negligible. □

Theorem 13 (Composition Theorem). *Let π, ϕ and ρ be quantum-polynomial-time protocols. Assume that π q-eqUC-D-emulates ϕ. Then, ρ^π q-eqUC-D-emulates ρ^ϕ.*

In Theorem 7, ρ^ϕ denotes the protocol ρ that makes subroutine calls to the protocol ϕ. In ρ^π, these subroutine calls to ρ are replaced by calls to ϕ.[11]

Again, our proof closely follows the original proof in [66].

Proof. Our goal is to prove that under the assumptions of Theorem 7, ρ^π q-eqUC-D-emulates ρ^ϕ. Since ρ is quantum-polynomial-time, ρ invokes at most a polynomial number n of instances of its subprotocol π or ϕ. Since π q-eqUC-D-emulates ϕ, there is a quantum-polynomial-time simulator $\mathcal{S}$ such that for all q-quantum-bounded quantum-polynomial-time environments $\mathcal{Z}$ we have that $\mathrm{LTState}_N(\kappa, a)$ and $\mathrm{LTState}_{N'}(\kappa, a)$ with $N = \pi \cup \{\mathcal{Z}, \mathcal{D}\}$ resp. $N' = \phi \cup \{\mathcal{Z}, \mathcal{S}\}$ are trace-indistinguishable. In the following, we call $\mathcal{S}$ the *dummy simulator*.

Let a quantum-polynomial-time adversary $\mathcal{A}'$ be given (that is supposed to attack ρ^π). We construct a simulator $\mathcal{S}'$ that internally simulates the adversary $\mathcal{A}'$ and n instances $\mathcal{S}_1, \ldots, \mathcal{S}_n$ of $\mathcal{S}$ for sessions with session IDs $sid_1, \ldots, sid_n$. The simulated adversary $\mathcal{A}'$ is connected to the environment and to the protocol ρ (via the external dummy adversary), but all messages between $\mathcal{A}'$ and the i-th instance π_i of π are routed through the dummy simulator instance $\mathcal{S}_i$ (which is then supposed to transform these messages into a form suitable for instances of ϕ).

Calls $\mathcal{RO}(\mathsf{id}, (X, Y), \cdot)$ are handled as follows by $\mathcal{S}'$:

– If it originates from some (internally emulated) $\mathcal{S}_j$ for session s:
  - If it is the first message to $\mathcal{RO}(\mathsf{id}, \cdot)$, then $\mathcal{S}_j$ is marked responsible for ID id.

[11] The notion of protocol composition in [66] is much simpler than the current definition of the composition operator in standard UC [22], which addresses many important subtleties. Nevertheless, we have chosen to adhere to the notion of [66] because we consider the task of adapting [66] to the latest changes of Universal Composability out of scope for this paper. However, we stress that our notion is universally composable according to the most recent definition.

  - If $\mathcal{S}_j$ is not responsible for ID id, the message is ignored.
  - Otherwise, the query is forwared to $\mathcal{RO}$ via the external adversary.
- If it originates from $\mathcal{A}'$ for session s:
  - If the session s is simulated by some $\mathcal{S}_j$, then forward the query to $\mathcal{S}_j$.
  - If the session s is not simulated by some $\mathcal{S}_j$:
    * If this is the first message to $\mathcal{RO}(\mathsf{id}, \cdot)$, then $\mathcal{A}'$ is marked responsible for ID id.
    * If $\mathcal{A}$ is not responsible for ID id, the message is ignored.
- If it originates from the environment, forward it to $\mathcal{A}'$.

Answers from $\mathcal{RO}$ (via the external adversary) are forwarded to the querying entity, which appropriately handles it.

On its last activation, $\mathcal{S}'$ reads the contents of its register $\mathcal{H}^{class}$ and copies it to $\mathcal{H}^{class}$ of $\mathcal{A}'$, which is then activated. Subsequently, it parses $\mathcal{H}^{class}$ of $\mathcal{A}'$ as a list of tuples, each beginning with an ID id^*. If id^* is associated with some $\mathcal{S}_j$, then the list with ID id^* is appended to $\mathcal{H}^{class}$ (which is initially empty) of $\mathcal{S}_j$. If $\mathcal{A}'$ is marked responsible for ID id, then appended the list to $\mathcal{H}^{class}$ of $\mathcal{S}'$. After all tuples have been processed, all $\mathcal{S}_j$ are activated. For $j = 1, \ldots, n$, read $\mathcal{H}^{class}$ of $\mathcal{S}_j$ and parse it as a list of tuples, each beginning with an ID id^*. If $\mathcal{S}_j$ is marked responsible for ID id^*, then copy the list to $\mathcal{H}^{class}$ of $\mathcal{S}'$.

We have to show that for any quantum-polynomial-time environment $\mathcal{Z}$, we have that $\mathrm{LTState}_N(\kappa, a)$ and $\mathrm{LTState}_{N'}(\kappa, a)$ with $N = \rho^\pi \cup \{\mathcal{Z}, \mathcal{A}'\}$ resp. $N' = \rho^\phi \cup \{\mathcal{Z}, \mathcal{S}'\}$ are trace-indistinguishable.

The Hybrid Environment. For this, we construct a hybrid environment $\mathcal{Z}_{\rho,i}$. This environment internally simulates the machines $\mathcal{Z}$, $\mathcal{A}'$, the protocol ρ, instances $\pi_1, \ldots, \pi_{i-1}$ of the real protocol π, and instances $\mathcal{S}_{i+1}, \ldots, \mathcal{S}_n$ and $\phi_{i+1}, \ldots, \phi_n$ of the dummy simulator $\mathcal{S}$ and the protocol ϕ, respectively. For $j = 1, \ldots, i-1$, let sid_j denote the session ID of π_j, for $i = j$, let sid_j denote the session ID of the challenge session and for $j > i$, let sid_j denote the session ID of ϕ_j.

The communication between $\mathcal{Z}$, $\mathcal{A}'$, and ρ is directly forwarded by $\mathcal{Z}_{\rho,i}$.

Communication between $\mathcal{A}'$ and the j-th protocol instance of π resp. ϕ is forwarded as follows: If $j < i$, the communication is simply forwarded to π_j. If $j > i$, the communication is routed through the corresponding dummy simulator $\mathcal{S}_j$ (which is then supposed to transform these messages into a form suitable for ϕ_j). And finally, if $j = i$, the communication is passed to the external adversary.

Calls to $\mathcal{RO}$ are handled similarly as above.

When the internally emulated environment $\mathcal{Z}$ has finished its execution, $\mathcal{Z}_{\rho,i}$ performs the following steps:

- It reads the contents of $\mathcal{Z}$'s register $\mathcal{H}^{class}$ and handles them as above. The final lists are copied to $\mathcal{H}^{class}$ of $\mathcal{Z}_{\rho,i}$.
- Before halting, $\mathcal{Z}_{\rho,i}$ overwrites its state register with $\mathcal{H}^{state}_{\texttt{environment}}$ of the internally emulated environment $\mathcal{Z}$.

Clearly, if $\mathcal{Z}$ is q-bounded, so is $\mathcal{Z}_{\rho,i}$.

We show that there is a negligible function $negl$ such that $\mathrm{TD}(\mathrm{LTState}_{N_i}(\kappa, a), \mathrm{LTState}_{N_i'}(\kappa, a)) \leq negl(\kappa)$ for any $i = 1, \ldots, n$ with $N_i = \pi \cup \{\mathcal{Z}_{\rho,i}, \mathcal{D}\}$ resp. $N_i' = \phi \cup \{\mathcal{Z}_{\rho,i}, \mathcal{S}\}$.

The Distinguishing Environment. For this, we construct an environment $\mathcal{Z}_\rho$ which expects as its initial input a pair (i, z), and then runs $\mathcal{Z}_{\rho,i}$ with input z. The final message for the adversary is handled analogously.

By assumption, for all quantum-polynomial-time environments $\mathcal{Z}$, there exists a negligible function *negl* such that $\mathrm{TD}(\mathrm{LTState}_N(\kappa, a), \mathrm{LTState}_{N'}(\kappa, a)) \leq \mathit{negl}(\kappa)$ with $N = \pi \cup \{\mathcal{Z}, \mathcal{D}\}$ resp. $N' = \phi \cup \{\mathcal{Z}, \mathcal{S}\}$. Thus, it holds that $\mathrm{LTState}_{N_i}(\kappa, a) = \mathrm{LTState}_N(\kappa, (a, i))$ with $N_i = \pi \cup \{\mathcal{Z}_{\rho,i}, \mathcal{D}\}$ and $N = \pi \cup \{\mathcal{Z}_\rho, \mathcal{D}\}$ and $\mathrm{LTState}_{N'_i}(\kappa, a) = \mathrm{LTState}_{N'}(\kappa, (a, i))$ with $N'_i = \phi \cup \{\mathcal{Z}_{\rho,i}, \mathcal{S}\}$ and $N' = \phi \cup \{\mathcal{Z}_\rho, \mathcal{S}\}$ and their trace distance is negligible for all i, z. Moreover, it holds by definition that the trace distance of $\mathrm{LTState}_{N_i}(\kappa, a)$ and $\mathrm{LTState}_{N'_{i+1}}(\kappa, a)$ with $N_i = \pi \cup \{\mathcal{Z}_{\rho,i}, \mathcal{D}\}$ and $N'_i = \phi \cup \{\mathcal{Z}_{\rho,i+1}, \mathcal{S}\}$ is zero.

Using the triangle inequality for the trace distance, it follows that $\mathrm{TD}(\mathrm{LTState}_{N_n}(\kappa, a), \mathrm{LTState}_{N'_1}(\kappa, a))$ with $N_n = \pi \cup \{\mathcal{Z}_{\rho,n}, \mathcal{D}\}$ and $N'_1 = \phi \cup \{\mathcal{Z}_{\rho,1}, \mathcal{S}\}$ is bounded by $n \cdot \mathit{negl}(\kappa)$, which is negligible.

Additionally, $\mathrm{LTState}_{N_n}(\kappa, a)$ and $\mathrm{LTState}_N(\kappa, a)$ with $N_n = \pi \cup \{\mathcal{Z}_{\rho,n}, \mathcal{D}\}$ and $N = \pi^\phi \cup \{\mathcal{Z}, \mathcal{A}'\}$ resp. $\mathrm{LTState}_{N'_1}(\kappa, a)$ and $\mathrm{LTState}_{N'}(\kappa, a)$ with $N'_1 = \phi \cup \{\mathcal{Z}_{\rho,1}, \mathcal{S}\}$ and $N' = \rho^\phi \cup \{\mathcal{Z}, \mathcal{S}'\}$ are identical. Since $\mathcal{A}$ and $\mathcal{S}$ are QPT, so is $\mathcal{S}'$ and the claim follows. □

It is easy to see that protocols that are statistically quantum UC-secure [66] remain secure under our notion.

Proposition 8 (Compatibility with Everlasting Quantum UC Security). *Let π and ϕ be protocols such that π statistically quantum-UC-emulates ϕ. Then, π q-eqUC-D-emulates ϕ for any q.*

Proof (Sketch). As π statistically quantum-emulates ϕ, there exists a simulator $\mathcal{S}_\mathcal{D}$ for the dummy adversary (under statistical quantum UC security) that is efficient in the runtime of the environment. In particular, for efficient environments, $\mathcal{S}_\mathcal{D}$ is efficient, too. $\mathcal{S}_\mathcal{D}$ can be easily extended to a simulator $\mathcal{S}'_\mathcal{D}$ for the dummy adversary (under q-eqUC-D security) appropriately handling the last activation. To this end, $\mathcal{S}'_\mathcal{D}$ does nothing, just like the dummy adversary.

Now, suppose that $\mathcal{S}'_\mathcal{D}$ is not a valid simulator for the dummy adversary under q-eqUC-D security. Then, we can prove that $\mathcal{S}_\mathcal{D}$ is not a valid simulator for the dummy adversary under statistical quantum UC security. To this end, we construct a distinguishing quantum UC environment $\mathcal{Z}$ that internally executes a distinguishing q-eqUC-D environment $\mathcal{Z}'$ as well as $\mathcal{S}'_\mathcal{D}$. As $\mathcal{Z}$ is unbounded, it can simply internally emulate $\mathcal{RO}$.

Finally, $\mathcal{Z}$ performs the final steps of Definition 17 to program $\mathcal{RO}$. To produce its final output, $\mathcal{Z}$ moves $\mathcal{H}^{state}_{\mathcal{Z}'} \otimes \mathcal{H}^{class}_{\mathcal{RO}}$ to its own register $\mathcal{H}^{state}_{\mathtt{environment}}$ and halts.

By definition, the output of $\mathcal{Z}$ in the quantum UC execution is identical to the output of the (presumptive) execution of $\mathcal{Z}'$ in the everlasting quantum UC with decoherence execution and the claim follows. □