Unclonable Functional Encryption

Arthur Mehta[3] and Anne Müller[1,2]

[1] CISPA Helmholtz Center for Information Security, Saarbrücken, Germany
anne.mueller@cispa.de
[2] Graduate School of Computer Science, Saarland University, Germany
[3] Department of Mathematics and Statistics, University of Ottawa, Ottawa, Canada
amehta2@uottawa.ca

Abstract. In a functional encryption (FE) scheme, a user that holds a ciphertext and a function-key can learn the result of applying the function to the plaintext message. Security requires that the user does not learn anything beyond the function evaluation. We extend this notion to the quantum setting by providing definitions and a construction for a quantum functional encryption (QFE) scheme which allows for the evaluation of polynomialy-sized circuits on arbitrary quantum messages. Our construction is built upon quantum garbled circuits [BY22].

We also investigate the relationship of QFE to the seemingly unrelated notion of unclonable encryption (UE) and find that any QFE scheme *universally* achieves the property of unclonable functional encryption (UFE). In particular we assume the existence of an unclonable encryption scheme with quantum decryption keys which was recently constructed by [AKY24]. Our UFE guarantees that two parties cannot simultaneously recover the correct function outputs using two independently sampled function secret keys. As an application we give the first construction for public-key UE with variable decryption keys.

Lastly, we establish a connection between quantum indistinguishability obfuscation (qiO) and quantum functional encryption (QFE); Showing that any multi-input indistinguishability-secure quantum functional encryption scheme unconditionally implies the existence of qiO.

Table of Contents

1 Introduction

The development of Functional Encryption (FE) marks a significant evolution in cryptography, enabling a more nuanced and controlled access to encrypted data [O'N10; BSW11]. Traditional public-key encryption allows either full decryption or none at all, a model insufficient for many modern applications, such as cloud services, where selective access to data is essential. FE addresses this by allowing decryption keys to reveal only specific functions of the encrypted data.

In more detail, an FE scheme for a family of functions $\mathcal{F}$ enables a specialized form of decryption that takes as input both a ciphertext ct and a function key sk_f and outputs the evaluation $f(\mathsf{m})$ on the plain text m. The security of the scheme ensures that an adversary in possession of $(\mathsf{ct}, \mathsf{sk}_f)$ cannot recover additional information beyond $f(\mathsf{m})$.

A broad goal within quantum cryptography aims to generalize various cryptographic tools into the quantum setting. This includes works studying verifiable delegation [RUV13; Gri19], randomized encodings and garbled circuits [BY22], and quantum indistinguishablity obfuscation (qiO) [BK21]. Another approach explores new functionalities uniquely achievable in the quantum setting, such as unclonable encryption (UE) [BL20], where an adversary is unable to create two ciphertexts that both decrypt to the same message as the original ciphertext.

While the works mentioned above demonstrate the tremendous progress made in the field, there remain significant open challenges. Prior to this work, a formal treatment and secure construction of quantum functional encryption (QFE) had not been provided. Instead, [BY22] suggests QFE as a potential application of quantum garbled circuits. Additionally, although there has been some progress, a complete construction for either qiO or UE remains an open problem. We explore how QFE can advance these topics.

Summary of Results. Our results on the topics of QFE, UE, and qiO are as follows:

1. We give the first formal definitions of QFE, covering both simulation and indistinguishability-based security. Our treatment spans adaptive and non-adaptive models, as well as multi-message, multi-query, and multi-input scenarios, addressing all key variants of functional encryption.
2. We use quantum garbled circuits to give the first construction of single-query, adaptively simulation-secure QFE.
3. We present a universal construction for unclonable QFE, showing that any QFE scheme can be made unclonably secure, assuming the existence of UE. As a corollary, we use this to obtain the first indistinguishable-uncloneable secure public-key encryption scheme with variable decryption keys.
4. Laslty, we establish a connection between quantum indistinguishability obfuscation (qiO) and QFE; Showing that any multi-input indistinguishability-secure quantum functional encryption scheme unconditionally implies the existence of qiO.

1.1 Quantum Functional Encryption

In this work, we formally define Functional Encryption in the quantum setting, referred to as Quantum Functional Encryption (QFE). At a high level, a QFE scheme for a class of circuits $\mathcal{C}$ allows for selective decryption with respect to function keys sk_C, which must satisfy two key properties: *correctness* and *security*. The correctness property ensures that decryption returns $C(\rho_{\mathsf{m}})$ for all $C \in \mathcal{C}$ and states ρ_{m}, and the security property guarantees that no additional information is revealed beyond $C(\rho_{\mathsf{m}})$.

While correctness in QFE is relatively straightforward, defining security requires more nuanced attention. Security can be analyzed through two primary frameworks: simulation-based security

(SIM-security) and the generally weaker indistinguishability-based security (IND-security). Both approaches have further distinctions between adaptive and non-adaptive versions, whether an adversary has a single or multiple challenge ciphertexts, and depending on whether the adversary obtains one or more function keys. The formal definitions and detailed treatments are presented in Section 3 and Appendix A.1. Below we provide the basic structure of QFE and outline notions of correctness as well as SIM-security and IND-security.

QFE.(Setup, KeyGen, Enc, Dec) $\mathsf{Setup}(1^\lambda)$, takes as input the security parameter λ, and outputs a master public key mpk, and a master secret key msk. Given msk and a circuit $C \in \mathcal{C}$, the key generation algorithm, $\mathsf{KeyGen}(\mathsf{msk}, C)$, produces a secret function key sk_C. Encryption, $\mathsf{Enc}(\mathsf{mpk}, \rho_\mathsf{m})$, uses mpk and outputs a ciphertext ρ_ct. Finally, the decryption algorithm, $\mathsf{Dec}(\mathsf{sk}_C, \rho_\mathsf{ct})$, takes a function key sk_C and the ciphertext ρ_ct, and outputs a quantum state.

Correctness. Correctness requires that for all messages ρ_m, circuits $C \in \mathcal{C}$ and random coins used by Enc and Setup it holds that

$$C(\rho_\mathsf{m}) = \mathsf{Dec}(\mathsf{sk}_C, \rho_\mathsf{ct}).$$

As outlined in Section 3 we additionally require correctness to respect correlation with possible side information.

Simulation Security. Simulation security is formalized by comparing the output of two experiments: in the real experiment, the adversary interacts with the actual encryption scheme to produce an encryption of a chosen message, and choice of function key(s) sk_C. In the ideal experiment, a simulator is given access to the function key sk_C and the image state $C(\rho_\mathsf{m})$, and produces a ciphertext without access to the underlying message. The scheme is called simulation secure, abbreviated as SIM-secure, if the outputs of these two experiments are computationally indistinguishable. A QFE scheme is further said to be *adaptively* simulation secure if the adversary can either choose the message first and then the function secret key or the other way around.

The formal definition of simulation security in the restricted setting, where the adversary holds only a single ciphertext and single function key, is provided in Definition 23.

Indistinguishability Security. In the classical setting, IND-security is defined with respect to *admissible queries*. Specifically, an adversary holding a function key sk_f for some function f cannot distinguish between encryptions of two admissible queries, meaning that $f(\mathsf{m}_0) = f(\mathsf{m}_1)$. Adapting IND-security to the quantum setting introduces some challenges, particularly in defining admissible queries. A first naive approach would be to require the trace distance of outputs states $C(\rho_{\mathsf{m}_1})$ and $C(\rho_{\mathsf{m}_1})$ to be suitably close in order for them to be admissible. However, as we discuss in Section 3.2 this approach is insufficient to prevent attacks based on quantum side information.

An alternative, approach would be to take into account the internal state of an adversary and thereby restricting quantum side information. Although such an approach may be be useful in some applications, such as when the messages are are not chosen by the adversary, it remains too restrictive for many use cases. Instead, in Definition 25 we introduce a notion of admissible queries which allows an adversary to be entangled with part of the message. As in the case in the classical setting our notion of sim-security is generally stronger and, we show that it implies IND-security.

Multi-message Security. More generally we also consider the notion of SIM-security and IND-security in the context where an adversary has access to numerous ciphertexts. In Appendix A.1 we provide an extension of the SIM-security from Definition 23 to the multi-message setting. As in the classical case, we show in Lemma 6 that any non-adaptive single-query simulation-secure scheme with classical secret keys is also multi-message simulation-secure.

Multi-query/Collusion Security In the classical setting, functional encryption schemes often require security to hold even in the presence of colluding key holders. A malicious user should not be able to combine several function keys to extract unauthorized information. More formally, a group of users holding secret keys $\mathsf{sk}_{C_1}, \ldots, \mathsf{sk}_{C_q}$, along with an encryption of m, should only be able to learn $C_1(\mathsf{m}), \ldots, C_q(\mathsf{m})$, and nothing more about m. This scenario is often referred to as "collusion resistance." In our work, we refer to this property as *multi-query security*. We note, however, that classical simulation-secure FE is not achievable against an adversary who may possesses an unbounded number of function keys, a scenario sometimes referred to as unbounded collusion [Agr+13].[4]

In the quantum setting, the no-cloning theorem makes it unclear to what extent collusion is possible and presents challenges to formalising multi-querry security. In particular, without several copies of the underlying ciphertext it may not be possible to obtain several evaluations. In Section 6, we introduce a more general form of QFE called *quantum multi-input functional encryption* (QMIFE). This framework extends our treatment of both simulation-based security and indistinguishability-based security, encompassing multi-query security as a special case. Below, in Section 1.4, we provide an overview of QMIFE and discuss how IND-security and SIM-security can be adapted to QMIFE.

1.2 QFE for Poly-sized Circuits

In the classical setting, it is known that a *non-succinct* form of FE can be constructed using a cryptographic primitive known as randomized encodings (RE). Specifically, [SS10; GVW12] show that any RE scheme which possess the additional property of being *decomposable*, can be used to construct an FE scheme for the class of polynomial-sized circuits. Here the constructed FE scheme is considered non-succinct as the size of the ciphertext must be at least as large as the size of allowable circuits.

Randomized Encodings A randomized encoding (RE) of a function f is a probabilistic function $\hat{f}$ such that, for any input x, the value of $f(x)$ can be recovered from $\hat{f}(x)$, but no additional information about f or x is revealed. An RE scheme is called *decomposable* if a function f and a sequence of inputs $(x_1, \ldots, x_n)$ can be encoded in two parts: an *offline* part $\hat{f}_{\text{off}}$, which depends only on f and some randomness r, and an *online* part $\hat{f}_i$, which depends on each input x_i and the same randomness r. We write DRE for RE schemes which satisfy this proprety.

In [BY22] Brakerski and Yuen both define and give a construction for decomposable RE in the quantum setting called the *Quantum Garbled circuit* (QGC) scheme. Our first main result presents a constuction for QFE based on QGC.

Theorem 1 (Informal). *Given a QGC scheme with perfect correctness and a public key encryption scheme there exists a single-query adaptive SIM-secure QFE scheme for the class of polynomial-sized circuits.*

The formal statement and construction of our QFE scheme is given in Section 4.2. Similar to the classical constructions given in [SS10; GVW12], our scheme is not succinct. While succinct FE is needed for many applications, such as delegated computation, we show that the our QFE scheme can be used to obtain the first public-key unclonable encryption scheme with variable decryption keys. This in turn provides several applications such as private-key quantum money. Details on our applications to unclonable cryptography are discussed in Section 1.3. Below we outline our construction for QFE and highlight the specific challenges which present in the quantum setting.

[4] Assuming the existence of a family of weak pseudo-random functions.

Outline of QFE Construction The basic observation that enables the construction of FE from garbled circuits is their decomposability. It allows one to decouple the circuit and input by viewing both as inputs to a universal circuit. Here a universal circuit U takes as input a circuit description C and state ρ_{m} and outputs $C(\rho_{\mathsf{m}})$. Due to the decomposability property the encoding of the classical circuit description and the encoding of the quantum input can be handled separately. In this way, using a decomposable RE scheme for a universal circuit, combined with a restricted form of functional encryption for pairs of circuits, enables functional encryption for all polynomial-sized circuits.

While the above construction is fairly straightforward to translate into the quantum setting using the QGC, more difficulty arises when creating adaptive security. In the adaptive security setting the adversary can first request a ciphertext and then a secret key for an arbitrary function. Since the simulator is not allowed learn the message which the adversary selected, the simulator only obtains the output of the circuit evaluation during the second stage. Therefore the simulator needs to first create an 'empty' ciphertext and later provide a secret key that opens the ciphertext to the correct value. Techniques for handling the classical part adaptively are well known but they cannot be applied to the quantum part. To resolve this we employ a 'trick' inspired by the concept of computation trough teleportation.

We describe the classical and quantum techniques to achieve this for a single bit or qubit repectively. For a classical message an 'empty' ciphertext can be created by encrypting the bit 0 and the bit 1 in two separate slots of the ciphertext and later revealing the key for only one slot. Clearly in the quantum setting we cannot enumerate all possible values a single qubit can take. Instead the uniquely quantum phenomenon of teleportation can help us achieve such a construction. The simulator encrypts one qubit of an EPR pair $\sigma^{AB} = \frac{1}{\sqrt{2}}(|0\rangle^A|0\rangle^B + |1\rangle^A|1\rangle^B)$ pair using the quantum one time pad: $|\mathsf{ct}\rangle = X^a Z^b \sigma^A$.

Later when the simulator learns the output state ρ it teleports the state into the ciphertext. This results into a randomization of the ciphertext since now the state $X^{a'} Z^{b'} \rho$ is contained resulting in the ciphertext $X^a Z^b X^{a'} Z^{b'} \rho = X^{a \oplus a'} Z^{b \oplus b'} \rho$ where (a', b') are the teleportation correction keys. We can then use a classical ciphertext as described above to reveal the keys $(a \oplus a', b \oplus b')$.

1.3 Unclonable QFE

As an application of our QFE scheme we obtain a novel form of unclonable encryption (UE), which we call *unclonable functional encryption*.

Unclonable Encryption Unclonable encryption, first introduced by Broadbent and Lord [BL20], is an encryption scheme that leverages the no-cloning theorem to achieve a novel cryptographic functionality. Specifically, it guarantees that an adversary in possession of a ciphertext ρ_{ct} cannot generate two states, ρ_B and ρ_C, that both correctly decrypt to the same message m. This is formalised in the following security game with a tripartite adversary $\mathcal{A} = (A, B, C)$. In the first phase A receives a ciphertext ρ_{ct} that enrcypts a message m and has to produce a state ρ_{BC} by applying an arbitrary quantum channel. In the second phase B and C are activated, they receive the state ρ_B and ρ_C respectively and each get a copy of the decryption key. They win the experiment if both B and C correctly guess the message m. The strongest security notion for unclonable encryption is unclonable-indistinguishability security which allows A to choose two messages $\mathsf{m}_0, \mathsf{m}_1$. To win the game B and C have to both guess correctly which of these message was encrypted. A second weaker notion, often simply referred to as unclonable security, weakens the win condition of the security game to requiring B and C to simultaneously recover a random message in it's entirety. In our work all definitions are with respect to the stronger notion of unclonable-indistinguishable security.

Vairable-key UE While currently there is no provably secure construction for the strongest notion of UE there do exists several weaker variants which have allowed for more progress. Kundu and Tan consider one such variant called unclonable encryption with variable keys [KT22]. Their modified version of UE allows a ciphertext to be decrypted using multiple decryption keys, with each adversary in a cloning attack receiving an independently generated key. In the device-independent setting [KT22] give a construction for secret-key unclonable encryption with variable keys. While this scheme enjoys device indepedence it only obtains the weaker notion unclonable security.

Kundi and Tan also further outline that although weaker than UE such a scheme is still useful for known applications of UE such as quantum money. A private-key quantum money scheme can be constructed from unclonable encryption as follows: A banknote is created by creating a ciphertext of a random message. The bank holds a deryption key and can verify the message by decrypting it. In the case of unclonable encryption with variable decryption keys each bank that needs to verify the banknote independently samples a decryption key.

Unclonable QFE In this work, we introduce a novel cryptographic primitive called *Unclonable Functional Encryption* (Unclonable QFE), which combines the security properties of QFE with the unclonable security characteristics of UE. The formal definition of Unclonable QFE is provided in Definition 26, where we extend the security requirements of a QFE scheme to include unclonable security. Our approach builds on the familiar security game from UE with some key modifications. In the first phase, the underlying message is encrypted using a QFE scheme. After an adversarial splitting channel is applied, in the second phase, two adversaries, B and C, each receive independently generated function secret keys for some circuit. Our new security notion ensures that both B and C cannot simultaneously guess which of the two challenge messages was encrypted, thus preserving unclonability in the functional encryption setting. Notably, we allow for the encryption of quantum messages. While UE is usually concerned with the protection of classical messages we maintain the properties of functional encryption for quantum messages while at the same time achieving unclonability for any message, classical or quantum. In Theorem 7 we prove that such a scheme can be constructed from any QFE scheme, such as our construction from Section 4.2, assuming the existence of an unclonable encryption scheme which allows for quantum decryption keys, such as that given by [AKY24].

Theorem 2 (Informal). *Any single-query QFE scheme for n-qubit messages is an unclonable-indistinguishable secure functional encryption scheme with variable decryption keys assuming an unclonable-indistinguishable secure encryption scheme with quantum decryption keys for single bit messages.*

When the function secret keys are fixed to be the identity circuit this implies a public-key unclonable-indisintguishable secure encryption scheme with variable decryption keys. In contrast to the standard definition of unclonable encryption here the KeyGen algorithm is run twice to produce independently sampled secret keys. We assume that the randomness can be chosen in such a way that the same encryption key is produced with different decryption keys.

Corollary 1 (Informal). *There exists a public-key unclonable-indistinguishable secure encryption scheme with variable decryption keys for n-bit messages assuming a single-query QFE scheme and an unclonable-indistinguishable secure encryption scheme with quantum decryption keys for single bit messages.*

Outline of the Unclonable QFE Construction The construction is inspired by Hiroka et al. [Hir+23] and the universal construction of Waters and Wichs [WW23]. In [Hir+23] they show a universal plaintext expansion result for unclonable encryption: A construction based solely on

quantum randomized encodings is a mulit-bit unclonable encryption scheme if there exists a single bit unclonable-indistinguishable secure encryption scheme. Unfortunately, the existence of such a scheme is not yet known in the plain model. Therefore we instead rely on an unclonable encryption scheme with quantum decryption keys which was recently constructed by Ananth, Kaleoglu, and Yuen [AKY24].

The idea of our construction is that the ciphertext has two modes indicated by a flag bit in the plaintext. In the first mode ($f = 0$), which is the mode the real encryption procedure uses, the plaintext is simply encrypted under the QFE scheme and padded to a certain length:

$$\rho_{\mathsf{ct}_0} = \mathsf{QFE.Enc}(\rho_{\mathsf{m}} \otimes |0\rangle\langle 0|^{O(\lambda)} \otimes |f = 0\rangle\langle f = 0|)$$

To prove security we want to reduce to the unclonable encryption scheme with quantum secret keys UEQ. Therefore we show that, due to the security of the QFE scheme, the first ciphertext is indistinguishable to the following ciphertext which makes use of the UEQ scheme. Let $\mathsf{ek}, |\mathsf{dk}\rangle$ be the encryption and decryption keys of the UEQ scheme and let $\rho_{UE} \leftarrow \mathsf{UEQ.Enc}(1^\lambda, b)$ be an unclonable encryption of a bit $b \leftarrow \{0, 1\}$. Define $\rho_{\mathsf{m}_b} = \rho_{\mathsf{m}}$ and $\rho_{\mathsf{m}_{1-b}}$ an arbitrary n-qubit state. Then a ciphertext in the second mode is created as follows:

$$\rho_{\mathsf{ct}_1} = \mathsf{QFE.Enc}(\rho_{\mathsf{m}_0} \otimes \rho_{\mathsf{m}_1} \otimes |\mathsf{dk}\rangle\langle\mathsf{dk}| \otimes \rho_{UE} \otimes |f = 1\rangle\langle f = 1|)$$

Now we can define a class of circuits $U(C, \cdot)$ that checks the last bit of the message and in the case of $f = 0$ outputs the message $C(\rho_{\mathsf{m}})$. In case of $f = 1$ the circuit decrypts the ρ_{UE} ciphertext to get b, selects the message m_b and outputs $C(\rho_{\mathsf{m}_b})$. Indistinguishability of the ciphertexts ρ_{ct_0} and ρ_{ct_1} follows from the security of the QFE scheme.

During the reduction we encounter the issue that we have to create the QFE ciphertext before we learned the decryption key $|\mathsf{dk}\rangle$ for the single-bit unclonable encryption scheme. Only in the second phase of the experiment is this key revealed. At this point we have to reveal the decryption key to the adversary who is attacking the QFE construction.

This part of the proof is reminiscent of the transformation given in [AK21] who also use the mode change via a flag bit trick. They use classical functional encryption to transform secret-key unclonable encryption into public-key unclonable encryption.[5]

In their construction it is possible to hardcode the classical decryption key of an unclonable encryption scheme into the circuit description and then create a function secret key for this circuit to complete the proof. Unfortunately we cannot directly apply same technique as [AK21]. In our case the decryption key is a quantum state and our QFE scheme does not support hardcoding quantum states into the circuit description.

To solve this issue we create 2n EPR pairs and put one qubit of each EPR pair in the ciphertext. Later we can teleport the quantum decryption keys into the ciphertext and hardcode the correction keys of the teleportation into the function secret key. The circuit applies the correction keys to the decryption key and can then use it to decrypt the ρ_{UE} ciphertext. Hardcoding the teleportation keys into the circuit introduces a randomization of the function secret key which is why we do not achieve fully fledged unclonable encryption but only a version with variable decryption keys. Furthermore we have to make sure that each part of the reduction B and C who each obtain a quantum decryption key $|\mathsf{dk}\rangle$ can create a valid decryption key for their part of the reduction. Since the EPR pairs for the teleportation procedure cannot be held by both B and C at the same time we need to provide two teleportation slots. Then B and C each individually teleport the decryption key into the ciphertext and create a function secret key based on their teleportation keys. The teleportation keys (a, b) are uniformly random bits, so the function secret keys that

[5] They also explain very well why a normal public-key encryption scheme is not sufficient but a functional encryption scheme is.

depend on them are indistinguishable from regular function secret keys that were created with freshly sampled bits.

In the second step of the proof we construct a ciphertext with the the flag bit set to 1 to reduce multi-bit security of our unclonable functional encryption scheme to the single bit security of the unclonable encryption scheme of [AKY24].

1.4 QMIFE and Applications to Quantum Indistinguishability Obfuscation

In the classical setting much research has focused on improving on the trade-off inherent between the size of allowable circuits and the length of the ciphertext. Recall the schemes constructed in [SS10; GVW12], as well as our scheme given in Section 3, are considered non-succinct as the size of the ciphertext must be at least as large as the circuit description of allowable circuits. In [Gol+14], a stronger variant on FE, known as multi-input functional encryption (MIFE) is introduced. In [Gol+14] it is shown that MIFE enables applications towards indistinguishability obfuscation without the requirement of succinctness.

MIFE Multi-Input Functional Encryption (MIFE) extends traditional functional encryption to handle functions over multiple ciphertexts, potentially encrypted under different keys. This general framework allows for the computation of aggregate information from various data sources, going beyond single-input functional encryption. In MIFE, the owner of a master secret key (MSK) can derive special function keys that enable the evaluation of an n-ary function $f(x_1, \ldots, x_n)$ on ciphertexts corresponding to different messages, even when encrypted by different parties. Such multi-input functionality has been shown to allow for many powerful applications such as multi-party delegated computation, and construction of indistinguishability obfuscation (iO) and virtual black-box obfuscation (VBBO).

QMIFE Analogously, a quantum multi-input functional encryption (QMIFE) scheme is a QFE scheme that can evaluate a function on multiple, individually encrypted quantum inputs. In our definition of QMIFE we switch to the secret-key version of functional encryption. Therefore the ciphertexts cannot be encrypted by anyone but only by the holder of encryption secret keys. Additionally the scheme is tagged with an encryption limit k which indicates how many ciphertexts per encryption key can be obtained.

The IND-definition for QMIFE readily generalizes using methods from the IND-security definition for QFE: For any combination of inputs and circuit queries the restriction of admissible queries has to be fulfilled. In the SIM-security definition a new uniquely quantum challenge arises. Informally we want to give the simulator exactly the information that we want to allow a participant in the QMIFE scheme to learn. In the classical setting this corresponds to the output of the quantum circuit for any combination of challenge inputs. In the quantum setting we have the problem that different combinations of inputs are possible but the quantum ciphertexts are not necessarily reusable. If we give the simulator access to all possible circuit outputs we are giving him too much information since obtaining all outputs might not be a physical process. On the other hand, allowing the simulator to obtain only one output is too little information.

For instance, an adversary could attempt to run decryption $\mathsf{Dec}(\mathsf{sk}_C, \rho_{\mathsf{ct}_1}, \rho_{\mathsf{ct}_2})$ on two ciphertext registers, measure one register, uncompute the decryption, and then swap the first register with a new state. We solve this issue by giving the simulator access to a trusted party that holds the input messages. The simulator can query the trusted party by defining a circuit and indices to select the input messages. Then the trusted party carries out the circuit evaluation, moves the output into a new register by applying a CNOT gate to every qubit and uncomputes the circuit on the input registers. The trusted party returns the output to the adversary and proceeds in the same manner for additional queries. Now the state that is obtained by the simulator is entangled with

the trusted party and any measurements that might be performed by the simulator disturb the state and influence future circuit evaluations. This simulates the information we expect a recipient of a number of ciphertexts and function keys to be able to compute without breaking the security of the QMIFE scheme.

Our formal presentation of QMIFE, including both IND-security and SIM-security definitions, is given in Section 6. Additionally, our treatment of QMIFE covers multi-query QFE as a special case. Our main application is given in Theorem 8 and Theorem 9 which provide the following quantum analogue of the celebrated reductions to iO and VBBO given in [Gol+14].

Theorem 3 (Informal). *Any single-query non-adaptive IND-secure QMIFE unconditionally implies qiO.*

Theorem 4 (Informal). *Any single-query non-adaptive SIM-secure QMIFE scheme unconditionally implies virtual black box quantum obfuscation.*

1.5 Additional Related Work

Functional Encryption While we are the first to consider functional encryption for quantum circuits there has been a series of works enhancing classical functional encryption using quantum techniques. By adding the possibility to certifiably delete the ciphertext of the FE scheme [Hir+24] construct certified everlasting functional encryption. [KN22] define and create functional encryption with secure key leasing from any secret-key FE and they construct FE with single decryptor against bounded collusions assuming sub-exponentially secure indistinguishability obfuscation and the sub-exponential hardness of the learning with errors (LWE) problem. Using different techniques Çakan and Goyal [ÇG23] construct functional encryption with copy protected secret keys against unbounded collusions from sub-exponentially secure indistinguishability obfuscation, one-way functions and LWE.

Unclonable Encryption The notion of unclonable encryption was formally defined by [BL20], previously a similar notion was introduced by [Got03]. Since then the gold standard of indistinguishable-unclonable secure encryption with negligible adversarial advantage has only been achieved in the quantum random oracle model by [Ana+22] and a construction in the plain model remains an open question. Various alternative notions of unclonable encryption have been achieved such as device-independent unclonable encryption with variable secret keys [KT22], unclonable encryption with interaction [BC23], unclonable encryption with quantum decryption keys [AKY24]. The encryption procedure of [KT22] is defined as an interactive process, although the interaction can be removed in the trusted device setting. The relationship of unclonable encryption to other primitives that require a form of unclonability such as quantum money [Wie83; AC12] and copy protected programs [Aar09; AK21; Bro+21; Ana+22; CMP24; CG24] has also been studied.

We note that the [KT22] scheme is only proven to achieve the weaker notion of unclonable security, where a successful attack requires both parties to guess the entire message. In our work all security notions obey the stronger uncloneable-indisinguishability. For brevity we often simply refer to this as unclonable security in the text.

Quantum Obfuscation Alagic and Fefferman [AF16] provide a quantum analouge of the classical impossibility result for virtual black box obfuscation (VBB), showing that the notion of quantum virtual black box obfuscation (QVBB) is also impossible to achieve. Furthermore, [Ala+21] show that a quantum scheme cannot achieve VBB for classical circuits either. The first feasability result for qiO was obtained by Broadbent and Kazmi [BK21] for circuits with log-many non-clifford gates relying on classical iO. Since then several works have put forth candidate constructions using a wide

variety of techniques. Bartusek and Malavolta [BM22] construct qiO for null circuits[6] assuming classical VBB. [Bar+23] construct QVBB for pseudo-deterministic circuits[7] with a classical description assuming classical VBB. [BBV24] improve upon this result by constructing ideal QVBB[8] for pseudo-deterministic circuits with a quantum description assuming classical VBB. Since classical VBB is known to be impossible these constructions are only candidates for qiO meaning we can hope that if the classical VBB is instantiated with classical iO the constructions can be proven secure with new ideas.

1.6 Open Questions

An important open question is the construction of quantum indistinguishability obfuscation. In this work we make a step towards exploring the relationship of quantum functional encryption to qiO via multi-input quantum functional encryption. It is an interesting open question if QMIFE can be constructed by for example leveraging classical multi-input functional encryption which can be constructed from classical iO, a reasonable assumption in the construction of qiO.

Another open question that this work raises are enhanced versions of quantum functional encryption. A QFE scheme with succinct ciphertext would have interesting applications such as delegated computation [Gol+13] and can potentially provide another route towards qiO. In the classical setting techniques to transform succinct FE to iO haven been explored extensively [BV15; AJS15; Gar+16; AJ15] and might be applicable in the quantum setting to.

Lastly we only construct QFE for a single key query and leave it as an open problem to construct QFE secure against multiple key queries.

Acknowledgements We would like to thank Henry Yuen for helpful discussions. Arthur Mehta is supported by NSERC Alliance Consortia Quantum grants, reference number: ALLRP 578455 - 22 and the NSERC Discovery Grants Program.

2 Preliminaries

For an integer $n \in \mathbb{N}$ we write $[n] = \{1, \ldots, n\}$. Let $p(\cdot)$ denote a polynomial. Let $negl(\cdot)$ denote a negligible function f, i.e. for every constant $c \in \mathbb{N}$ there exists a positive integer n_0 such that for all $n > n_0$, $f(n) < n^{-c}$.

Let $\mathcal{H}_n$ denote a finite dimensional Hilbert space of dimension 2^n and let a pure quantum state be denoted by a vector $|\psi\rangle \in \mathcal{H}$. Let a mixed quantum state be denoted as $\rho \in D(\mathcal{H}_n)$ where $D(\mathcal{H}_n)$ is the set of density operators on $\mathcal{H}_n$ which are positive semidefinite and have trace equal to 1. A general quantum operation is a completely positive trace preserving (CPTP) map $\Phi : D(\mathcal{H}_n) \to D(\mathcal{H}_m)$.

For a classical string $x \in \{0,1\}^n$ we let $|x| = n$ denote the length of the string and for a quantum state $\rho \in D(\mathcal{H}_n)$ we let $|\rho| = n$ denote the size, i.e. the number of qubits.

Let Tr denote the trace operator. Let the partial trace be denoted as $\mathrm{Tr}_{(b)}[\rho_{ab}] = \rho_a = \mathrm{Tr}(\rho_b)\rho_a$. We write ρ_{x_i} to denote taking the partial trace of everything but the i-th qubit $\mathrm{Tr}_{(\bar{i})}(\rho_x) = \rho_{x_i}$. We write ρ^A to denote that the qubits in ρ are conceptually grouped together in a register A.

A family of quantum circuits $\{C_\lambda\}_{\lambda\in\mathbb{N}}$ is called uniform if there exists a deterministic Turing machine running in time $\mathrm{poly}(\lambda)$ such that on input 1^λ it outputs a description of C_λ. A quantum polynomial time (QPT) algorithm is a polynomial-time uniform family of quantum circuits.

[6] Null quantum circuits are circuits that reject on every input with overwhelming probability.

[7] A pseudo-deterministic circuit takes as input a classical string and outputs a deterministic bit with overwhelming probability taken over the randomness introduced by the quantum circuit.

[8] Ideal QVBB is very similar but slightly stronger than QVBB.

A universal gate set for quantum circuits is the Clifford group consisting of the controlled-not gate CNOT, phase gate P and Hadamard gate H with additionally the T-gate T. Let X and Z be the following gates

$$\mathsf{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \mathsf{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

2.1 Indistinguishability of Quantum States

The *trace distance* between two quantum states $\rho, \sigma \in \mathcal{D}(\mathcal{H}_n)$ is defined as

$$\mathrm{TD}(\rho, \sigma) = \frac{1}{2}\mathrm{Tr}\left(\sqrt{(\rho - \sigma)^\dagger (\rho - \sigma)}\right)$$

.

Let $\mathcal{R} = \{\rho_n\}_{n\in\mathbb{N}}$ and $\mathcal{S} = \{\sigma_n\}_{s\in\mathbb{N}}$ be two ensembles of quantum states such that ρ_n and σ_n are n-qubit states. $\mathcal{R}$ and $\mathcal{S}$ are called *perfectly indistinguishable* if for all n: $\rho_n = \sigma_n$.

$\mathcal{R}$ and $\mathcal{S}$ are called *satistically indistinguishable* if there exits a negligible function negl such that for all sufficiently large n:

$$\mathrm{TD}(\rho_n, \sigma_n) \leq negl(n)$$

.

$\mathcal{R}$ and $\mathcal{S}$ are called *computationally indistinguishable* if there exits a negligible function negl such that for all QPT distinguisher $\mathcal{D}$ and all states $\rho_n \in \mathcal{R}$ and $\sigma_n \in \mathcal{S}$:

$$|\Pr[\mathcal{D}(\rho_n) = 1] - \Pr[\mathcal{D}(\sigma_n) = 1]| \leq negl(n)$$

.

The diamond norm for two quantum channels Φ and Ψ mapping a n-qubit quantum state to a m-qubit quantum state is defined as follows:

$$||\Phi - \Psi||_\diamond = \max_{\rho \in D(\mathcal{H}^{2n})} \mathrm{TD}((\Phi \otimes I)\rho - (\Psi \otimes I)\rho)$$

2.2 Quantum Randomized Encodings

We recall the following definitions from [BY22].

Classical Description of Quantum Circuits A quantum circuit is a tuple $(\mathcal{P}, \mathcal{G})$ where $\mathcal{P}$ is the topology of the circuit and $\mathcal{G}$ is a set of unitaries. The topology of a quantum circuit is a tuple $(\mathcal{B}, \mathcal{I}, \mathcal{O}, \mathcal{W}, \texttt{inwire}, \texttt{outwire}, \mathcal{Z}, \mathcal{T})$.

1. $\mathcal{I}$ is an ordered set of input terminals.
2. $\mathcal{Z}$ is a subset of $\mathcal{O}$ which indicates ancilla qubits that are to be initialised to the state $|0\rangle$.
3. $\mathcal{O}$ is an ordered set of output terminals.
4. $\mathcal{T}$ is the set of output terminals to be traced out.
5. $\mathcal{W}$ is the set of wires.
6. $\mathcal{B}$ are placeholder gates. For every $g \in \mathcal{B}$ `inwire(g)` describes an ordering of input wires $w \in \mathcal{W}$ and `outwire(g)` describes an ordering of output wires $w \in \mathcal{W}$. For every $g \in \mathcal{B}$ the number of input and output wires is equal.
7. The disjoint sets $\mathcal{I}, \mathcal{O}, \mathcal{B}$ form the nodes of the circuit. Together with the set $\mathcal{W}$ as edges they define a directed acyclic graph.

The gate set $\mathcal{G}$ defines a unitary of the appropriate size for every node in $\mathcal{B}$. The evaluation of a circuit $C = (\mathcal{P}, \mathcal{G})$ on state ρ of size $|\mathcal{I}|$ is defined as $C(\rho, |0\rangle^{\otimes|\tilde{\mathcal{Z}}|}) = \sigma$ where σ resulted from applying the gates in $\mathcal{G}$ according to the topology and tracing out the qubits specified by $\mathcal{T}$. The size of a quantum circuit is the number of wires in $\mathcal{W}$. The descritpion of quantum operations by a quantum circuit describes a CPTP map.

Definition 1. *Quantum Randomized Encodings (QRE)*
Let $(\mathsf{Encode}, \mathsf{Decode}, \mathsf{Sim})$ *be QPT algorithms. Let* C *denote a class of general quantum circuits.*

$\mathsf{Encode}(F, \rho_x, r, \rho_e) \to \hat{F}(\rho_x, r)$*: Encode* (F, ρ_x, r, ρ_e) *takes a function* $F \in C$*, quantum input* ρ_x*, classical randomness* r *and a set of EPR pairs* ρ_e *and outputs a quantum randomized encoding* $\hat{F}(\rho_x, r)$*.*
$\mathsf{Decode}(\hat{F}(\rho_x, r), T) \to F(\rho_x)$*: Decode takes as input a quantum randomized encoding* $\hat{F}(\rho_x, r)$ *and the topology* T *of the function* F *and outputs* $F(\rho_x)$*.*
$\mathsf{Sim}(F(\rho_x), T)$*: Sim takes as input the value* $F(\rho_x)$ *and the topology of* F *and simulates a quantum randomized encoding.*

A QRE scheme fulfills the following properties:

- ***Correctness*** *For all quantum states* (ρ_x, ρ_z) *and randomness* r *it holds that*

$$(\mathsf{Decode}(\hat{F}(\rho_x, r), T), \rho_z) = (F(\rho_x), \rho_z)$$

.

- ***(t,ϵ)-Privacy*** *For all quantum states* (ρ_x, ρ_z) *and distinguishers of size* t *it holds that*

$$(\mathsf{Sim}(F(\rho_x)), \rho_z) \approx_\epsilon (\hat{F}(\rho_x, r), \rho_z)$$

.

A QRE can additionally fulfill the following property:

Definition 2. *Decomposability*

- ***Decomposability:*** *The encoding* $\hat{F}$ *is decomposable if there exists an operation* $\hat{F}_{off}$ *(called the offline part of the encoding) and a collection of input encoding operations* $\hat{F}_1, \ldots, \hat{F}_n$ *such that for all inputs* $\rho_x = (\rho_{x_1}, \ldots, \rho_{x_n})$*,* $\hat{F}(\rho_x, r) = (\hat{F}_{off}, \hat{F}_1, \ldots, \hat{F}_n)(r\rho_x, r, \rho_e)$ *where the functions* $\hat{F}_{off}, \hat{F}_1, \ldots, \hat{F}_n$ *act on disjoint subsets of qubits from* ρ_e*,* ρ_x *(but can depend on all bits of* r*), each* $\hat{F}_i$ *acts on a single qubit* ρ_{x_i}*, and* $\hat{F}$ *does not act on any of the qubits of* ρ_x*.*
- ***Classical Encoding of Classical Inputs:*** *If an input qubit* x_i *is classical, then the input encoding operation* $\hat{F}_i$ *is computable by a classical circuit.*

Definition 3. *Quantum Garbled Circuits (QGC)*
Quantum Garbled Circuits are an instantiation of QRE that fulfill the Decomposability property with classical encodings of classical inputs. For a quantum circuit of size s *the randomized encoding can be computed by a circuit of size* $poly(\lambda, s)$ *and fulfills computational security, that is for every polynomial* $t(\lambda)$ *there exists a negligible function* $\varepsilon = negl(\lambda)$ *such that the scheme is* $(t', \epsilon') - private$*, where* $t'(\lambda) = t(\lambda) - poly(\lambda, s)$ *and* $\epsilon'(\lambda) = \epsilon(\lambda) \cdot s$*. The decoding and simulation procedures are computable in time* $poly(\lambda) \cdot s$*.*

Additional preliminaries regarding classical functional encryption, quantum obfuscation and unclonable encryption can be found in Section 2.2.

2.3 The Quantum One Time Pad

The Quantum One Time Pad (QOTP) [Amb+00] is the quantum analogue to the classical One Time Pad.

Definition 4. *(Quantum One Time Pad)*

$\mathsf{Enc}(\mathsf{sk}, |\phi\rangle \in \mathcal{H}_1) \to |\mathsf{ct}\rangle$ *Given a secret key* $\mathsf{sk} = (a, b)$ *and a quantum message* $|\psi\rangle$ *apply the following operation to the state to obtain the ciphertext:*

$$|\mathsf{ct}\rangle = \mathsf{X}^a\mathsf{Z}^b|\phi\rangle$$

$\mathsf{Dec}(\mathsf{sk}, |\mathsf{ct}\rangle) \to |\phi\rangle$ *Given a secret key* $\mathsf{sk} = (a, b)$ *and a ciphertext apply the following operation to obtain the message:*

$$|\phi\rangle = \mathsf{X}^a\mathsf{Z}^b|\mathsf{ct}\rangle$$

When the key $\mathsf{sk} = (a, b)$ is chosen uniformly at random from $\{0, 1\}^2$, the QOTP information theoretically hides the state. The technique generalises to mulit-qubit states by encrypting qubit by qubit.

2.4 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 [Ben+93]. 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 and obtains the correction keys (a, b). The keys (a, b) are send to B who applies an X gate to the state if $a = 1$ and a Z gate to the state if $b = 1$. Now Bob holds the state ρ. The technique generalises to mulit-qubit states by teleporting qubit by qubit.

2.5 Classical Functional Encryption

Definition 5. *(Functional Encryption) Let* $\lambda \in \mathbb{N}$ *be the security parameter. Let* $\mathcal{F} = \{\mathcal{F}_\lambda\}_{\lambda\in\mathbb{N}}$ *be a class of circuits with input space* $\mathcal{X} = \{\mathcal{X}_\lambda\}_{\lambda\in\mathbb{N}}$ *and output space* $\mathcal{Y} = \{\mathcal{Y}_\lambda\}_{\lambda\in\mathbb{N}}$*. A functional encryption scheme is defined by the PPT algorithms* $\mathsf{FE} = (\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$.

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

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

Definition 6. *(Correctness) Let* $(\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^\lambda)$, $\mathsf{sk}_f \leftarrow \mathsf{KeyGen}(\mathsf{msk}, f), \mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{mpk}, \mathsf{m})$. *Then the FE is correct, if for all* $f \in \mathcal{F}$ *and* $\mathsf{m} \in \mathcal{X}$ *it holds that* $f(\mathsf{m}) = \mathsf{Dec}(\mathsf{sk}_f, \mathsf{ct})$.

Definition 7. *(Single-Query IND-Security for Classical Functional Encryption) Let* $\lambda \in \mathbb{N}$ *be the security parameter and let* $\mathcal{A}$ *be a QPT adversary. Consider the experiment* $\exp^{\mathsf{FE}}_{\mathcal{A},b}(1^\lambda)$*:*

1. $\mathsf{FE.Setup}(1^\lambda) \to (\mathsf{mpk}, \mathsf{msk})$
2. $(\mathsf{m}_0, \mathsf{m}_1, \mathsf{st}) \leftarrow \mathcal{A}^{\mathsf{sk}_f \leftarrow \mathsf{KeyGen}(\mathsf{msk}, \cdot)}(1^\lambda, \mathsf{mpk})$ *where* $\mathsf{m}_0, \mathsf{m}_1$ *have to be admissible queries for a function* f *that* $\mathcal{A}$ *queries, they fulfil* $f(\mathsf{m}_0) = f(\mathsf{m}_1)$.
3. *Sample* $b \leftarrow \{0, 1\}$

4. $\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{mpk}, \mathsf{m}_b)$.
5. $b' \leftarrow \mathcal{A}^{O(\cdot)}(1^\lambda, \mathsf{ct}, \mathsf{st})$.
6. *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 IND-security if for all QPT adversaries $\mathcal{A}$*, there exists a negligible function negl such that for all* $\lambda \in \mathbb{N}$*:*

$$\left|\Pr\left[1 \leftarrow \mathsf{Exp}^{Ind}_{\mathcal{A},b=0}\right] - \Pr\left[1 \leftarrow \mathsf{Exp}^{Ind}_{\mathcal{A},b=1}\right]\right| \leq negl(\lambda)$$

where the random coins are taken over the randomnes of $\mathcal{A}$*,* Setup, KeyGen *and* Enc.

Adaptive vs. Non-adaptive security

- *The scheme is called non-adaptively secure if the the adversary only queries the* KeyGen *oracle before receiving a ciphertext. Then the oracle* $O(\cdot)$ *is the empty oracle.*
- *The scheme is called adaptively secure if the adversary can either query the* KeyGen *oracle before or after receiving the ciphertext. Then the oracle* $O(\cdot)$ *is the function* $\mathsf{KeyGen}(\mathsf{msk}, \cdot)$.

Definition 8. *(Single-Query SIM-security) Let* λ *be the security parameter and let* $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ *be a QPT adversary and let* Sim *be a QPT simulator.*

$\mathsf{Exp}^{Real}_{\mathcal{A}}(1^\lambda)$	$\mathsf{Exp}^{Ideal}_{\mathcal{A}}(1^\lambda)$
$(\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^\lambda)$	$(\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^\lambda)$
$(\mathsf{m}, \mathsf{st}) \leftarrow \mathcal{A}_1^{O_1(\cdot)}(1^\lambda, \mathsf{mpk})$	$(\mathsf{m}, \mathsf{st}) \leftarrow \mathcal{A}_1^{O_1(\cdot)}(1^\lambda, \mathsf{mpk})$
$\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{mpk}, \mathsf{m})$	$ct \leftarrow \mathsf{Sim}(1^\lambda, \mathsf{mpk}, \mathcal{V})$ where $\mathcal{V} = (C, \mathsf{sk}_C, C(\mathsf{m}), 1^{\lvert\mathsf{m}\rvert})$ if $\mathcal{A}$ queried O_1 on C and $\mathcal{V} = \emptyset$ otherwise.
$\alpha \leftarrow \mathcal{A}_2^{O_2(\cdot)}(\mathsf{ct}, \mathsf{st})$	$\alpha \leftarrow \mathcal{A}_2^{O'_2(\cdot)}(\mathsf{ct}, \mathsf{st})$
The experiment outputs the state α	The experiment outputs the state α

The FE scheme is single-query simulation-secure if for any adversary $\mathcal{A}$ *and all messages* m *there exists a simulator* Sim *such that the real and ideal distributions are computationally indistinguishable:*

$$\{\mathsf{Exp}^{Real}_{\mathcal{A}}(1^\lambda)\}_{\lambda\in\mathbb{N}} \approx_c \{\mathsf{Exp}^{Ideal}_{\mathcal{A}}(1^\lambda)\}_{\lambda\in\mathbb{N}}$$

.

Adaptive vs Non-adaptive security:

1. *Non-adaptive: the adversary* $\mathcal{A}_1$ *is allowed to make one key query to* $O_1(\cdot)$ *where the oracle* $O_1(\cdot)$ *is* $\mathsf{KeyGen}(\mathsf{msk}, C) \rightarrow sk_C$.
2. *Adaptive: the adversary is allowed to make one key query either to* $O_1(\cdot)$ *or* $O_2(\cdot)$ *(*$O'_2(\cdot)$ *in the ideal world) where* $O_1(\cdot)$ *and* $O_2(\cdot)$ *are* $\mathsf{KeyGen}(\mathsf{msk}, C) \rightarrow sk_C$ *and* $O'_2(\cdot)$ *is a* KeyGen *oracle controlled by the simulator* $\mathsf{sk}_C \leftarrow \mathsf{Sim}(1^\lambda, \mathsf{msk}, C, C(\mathsf{m}), 1^{\lvert\mathsf{m}\rvert})$. *The simulator is stateful, in this invocation* Sim *has access to the state of the simulator from it's first invocation where it produced the ciphertext.*

In this work we only require a very simple functional encryption schemes: We require a single-query adaptively SIM-secure FE scheme for the identity circuit and we require a single-query adaptively SIM-secure FE scheme for a family of two cicruits. Such schemes are constructed in [GVW12].

2.6 Classical Multi-input Functional Encryption

We recall the syntax and security definition of a classical multi-input functional encryption scheme (MIFE) [Gol+14]. We only consider the case where all encryption keys are secret.

Let $\mathcal{X} = \{\mathcal{X}_\lambda\}_{\lambda\in\mathbb{N}}$ and $\mathcal{Y} = \{\mathcal{Y}_\lambda\}_{\lambda\in\mathbb{N}}$ be ensembles where each $\mathcal{X}_\lambda$ and $\mathcal{Y}_\lambda$ is a finite set. Let $\mathcal{F} = \{\mathcal{F}_\lambda\}_{\lambda\in\mathbb{N}}$ be an ensemble where each $\mathcal{F}_\lambda$ is a finite collection of n-ary functions. Each function $f \in \mathcal{F}_\lambda$ takes as input n strings $x_1, \ldots, x_n$, where each $x_i \in \mathcal{X}_\lambda$ and outputs $f(x_1, \ldots, x_n) \in \mathcal{Y}_\lambda$. A multi-input functional encryption scheme is additionally parametrized by a parameter k which denotes how many ciphertexts can be produced for one encryption key ek.

A multi-input functional encryption scheme MIFE for $\mathcal{F}$ consists of four algorithms $(\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ as described below.

- **Setup** $\mathsf{Setup}(1^\lambda, n) \to (\mathsf{msk}, \mathsf{ek}_1, \ldots, \mathsf{ek}_n)$ is a PPT algorithm that takes as input the security parameter λ and the function arity n. It outputs n encryption keys $\mathsf{ek}_1, \ldots, \mathsf{ek}_n$ and a master secret key msk.
- **KeyGen** $\mathsf{KeyGen}(\mathsf{msk},\mathrm{f}) \to \mathsf{sk}_f$ is a PPT algorithm that takes as input the master secret key msk and an n-ary function $f \in \mathcal{F}_\lambda$ and outputs a corresponding secret key sk_f.
- **Enc** $\mathsf{Enc}(\mathsf{ek}, x) \to \mathsf{ct}$ is a PPT algorithm that takes as input an encryption key $\mathsf{ek}_i \in (\mathsf{ek}_1, \ldots, \mathsf{ek}_n)$ and an input message $x \in \mathcal{X}_\lambda$ and outputs a ciphertext ct. In the case where all of the encryption keys ek_i are the same, we assume that each ciphertext ct has an associated label i to denote that the encrypted plaintext constitutes an i'th input to a function $f \in \mathcal{F}_\lambda$. For convenience of notation, we omit the labels from the explicit description of the ciphertexts. In particular, note that when ek_i's are distinct, the index of the encryption key ek_i used to compute ct implicitly denotes that the plaintext encrypted in ct constitutes an i'th input to f, and thus no explicit label is necessary.
- **Dec** $\mathsf{Dec}(\mathsf{sk}_f, \mathsf{ct}_1, \ldots, \mathsf{ct}_n) \to y$ is a deterministic algorithm that takes as input a secret key sk_f and n ciphertexts $\mathsf{ct}_1, \ldots, \mathsf{ct}_n$ and outputs a string $y \in \mathcal{Y}_\lambda$.

Definition 9. *(Correctness) A multi-input functional encryption scheme $\mathcal{FE}$ for $\mathcal{F}$ is correct if for all $f \in \mathcal{F}_\lambda$ and all $(x_1, \ldots, x_n) \in \mathcal{X}_\lambda^n$:*

$$\Pr\left[\begin{array}{l}\mathsf{Dec}(\mathsf{sk}_f, \mathsf{Enc}(\mathsf{ek}_1, x_1), \ldots, \mathsf{Enc}(\mathsf{ek}_n, x_n)) = f(x_1, \ldots, x_n) : \\ (\mathsf{msk}, \mathsf{ek}_1, \ldots, \mathsf{ek}_n) \leftarrow \mathsf{Setup}(1^\lambda, n), \mathsf{sk}_f \leftarrow \mathsf{KeyGen}(\mathsf{msk}, f)\end{array}\right] = 1 - negl(\lambda)$$

where the probability is taken over the coins of $\mathsf{KeyGen}, \mathsf{Setup}, \mathsf{Enc}$.

Definition 10. *(Compatibility of function and message queries)*

Let $\{f\}$ be any set of n-ary functions $f \in \mathcal{F}_\lambda$. Let X^0, X^1 a pair of input vectors where $X^b = \{x^b_{1,j}, \ldots, x^b_{n,j}\}_{j\in[k]}$. We say (X^0, X^1) and $\{f\}$ are compatible if they satisfy the following property:

For every $f \in \{f\}$ and every $j_1, \ldots, j_n \in [k]$

$$f(x^0_{1,j_1}, \ldots, x^0_{n,j_n}) = f(x^1_{1,j_1}, \ldots, x^1_{n,j_n})$$

Definition 11. *(Classical MIFE selective IND-Security)*

A multi-input functional encryption scheme MIFE for n-ary functions $\mathcal{F}$ is k-IND-secure if for every PPT adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$, the advantage of $\mathcal{A}$ defined as

$$\mathrm{Adv}^{\mathsf{MIFE},\mathrm{IND}}_{\mathcal{A}}(1^\lambda) = \left|\Pr\left[\mathsf{Exp}^{\mathrm{IND}-\mathsf{MIFE}}_{\mathcal{A}}(1^\lambda) = 1\right] - \frac{1}{2}\right| \leq negl(\lambda)$$

where:

$$\begin{aligned}
&\mathsf{Exp}_{\mathcal{A}}^{\mathrm{IND-MIFE}}(1^\lambda):\\
&(\boldsymbol{X}^0,\boldsymbol{X}^1,\mathsf{st}_1)\leftarrow\mathcal{A}_1(1^\lambda,n)\ \textit{where}\ \boldsymbol{X}^\ell=\{x^\ell_{1,j},\ldots,x^\ell_{n,j}\}_{j\in[k]}\\
&(\{\mathsf{ek}_i\}_{i\in[n]},\mathsf{msk})\leftarrow\mathsf{Setup}(1^\lambda,n)\\
&b\leftarrow\{0,1\}\\
&\mathsf{ct}_{i,j}\leftarrow\mathsf{Enc}(\mathrm{ek}_i,x^b_{i,j})\quad\forall i\in[n],j\in[k]\\
&b'\leftarrow\mathcal{A}_2^{\mathsf{KeyGen}(\mathsf{msk},\cdot)}(\mathsf{st}_1,\{\mathsf{ct}_{i,j}\}_{i\in[n],j\in[k]})\\
&\textit{Output: }(b=b')
\end{aligned}$$

Let $\{f\}$ denote the entire set of key queries made by $\mathcal{A}$ at any point dirung the game. Then, the challenge message vectors $\boldsymbol{X}_0$ and $\boldsymbol{X}_1$ chosen by $\mathcal{A}$ must be compatible with $\{f\}$ (Definition 10).

Lemma 1. *[Gol+14] Let $k=k(\lambda)$ be a fixed poly(λ). Then, assuming indistinguishability obfuscation for all polynomial-time computable classical circuits and one-way functions, there exists a $k-$ MIFE scheme that is selectively IND-secure.*

Definition 12. *(Classical MIFE Sim-Security) A multi-input functional encryption scheme for n-ary functions is k-SIM-secure if for every QPT adversary $\mathcal{A}=(\mathcal{A}_1,\mathcal{A}_2)$ there exists a stateful simulator* Sim *such that the outputs of the following experiments are computationally indistinguishable:*

$\mathsf{Exp}_{\mathcal{A}}^{Real}(1^\lambda)$	$\mathsf{Exp}_{\mathcal{A}}^{Ideal}(1^\lambda)$
$(\{\mathsf{ek}_i\}_{i\in[n]},\mathsf{msk})\leftarrow\mathsf{Setup}(1^\lambda,n)$	
$(X,\mathsf{st})\leftarrow\mathcal{A}_1^{\mathsf{KeyGen}(\mathsf{msk},\cdot)}(1^\lambda,n)$	$(X,\mathsf{st})\leftarrow\mathcal{A}_1^{O_1(\cdot)}(1^\lambda)$
where $X=\{\mathsf{m}_{1,j},\ldots,\mathsf{m}_{n,j}\}_{j\in[k]}$	where $X=\{\mathsf{m}_{1,j},\ldots,\mathsf{m}_{n,j}\}_{j\in[k]}$
$\mathsf{ct}_{i,j}\leftarrow\mathsf{Enc}(\mathsf{ek}_i,\mathsf{m}_{i,j})\quad\forall i\in[n],j\in[k]$	$\{\mathsf{ct}_{i,j}\}_{i\in[n],j\in[k]}\leftarrow\mathsf{Sim}^{\mathsf{TP}(\cdot)}(1^\lambda,1^{\lvert m_{i,j}\rvert})$
$\alpha\leftarrow\mathcal{A}_2^{\mathsf{KeyGen}(\mathsf{msk},\cdot)}(\{\mathsf{ct}_{i,j}\}_{i\in[n],j\in[k]},\mathsf{st})$	$\alpha\leftarrow\mathcal{A}_2^{O_2(\cdot)}(\{\mathsf{ct}_{i,j}\}_{i\in[n],j\in[k]},\mathsf{st})$
The experiment outputs α	The experiment outputs α

where the oracle $\mathsf{TP}(\cdot)$ *denotes the ideal world trusted party.* TP *accepts queries of the form $(g,(j_1,\ldots,j_n))$ and outputs $g(\mathsf{m}_{1,j_1},\ldots,\mathsf{m}_{n,j_n})$.*

$O_1(\cdot)$ is a KeyGen *oracle controlled by the simulator and $O_2(\cdot)$ is a* KeyGen *oracle controlled by the simulator with access to* TP*. We say* Sim *is admissible if* Sim *only queries* TP *on functions that $\mathcal{A}$ queried to its oracle.*

In a single-query secure scheme $\mathcal{A}$ (in the real world) can only make a single query to the KeyGen *oracle or (in the ideal world) a single query to either $O_1(\cdot)$ or $O_2(\cdot)$.*

2.7 Quantum Obfuscation

Definition 13. *Let $\{\mathcal{C}_\lambda\}_{\lambda\in\mathbb{N}}$ be a family of circuits and let $\mathcal{X}_\lambda$ be the input space and let $\mathcal{Y}_\lambda$ be the output space of the circuit family. A quantum obfuscator consists of two QPT algorithms* $(\mathsf{Obf},\mathsf{Eval})$ *with the following syntax:*

- $\mathsf{Obf}(1^\lambda,C)\to\tilde{C}$ *The obfuscator takes as input the security parameter λ and a classical description of a quantum circuit $C\in\{\mathcal{C}_\lambda\}_{\lambda\in\mathbb{N}}$ and outputs an obfuscation of C which can be classical or quantum.*
- $\mathsf{Eval}(\tilde{C},\rho_x)\to\rho_y$ *The evaluation takes as input the obfuscated program $\tilde{C}$ and an input $\rho_x\in\mathcal{X}$ and outputs $\rho_y\in\mathcal{Y}$.*

Quantum Indistinguishability Obfuscation Several definitions for qiO have come up in the literature. We closely follow the definition of [BK21].[9]

Definition 14. *(Quantum Indistinguishability Obfuscation)*
The following three properties are required of a quantum indistinguishability obfuscator:

1. *Correctness: The obfuscation scheme is correct if for any circuit $C \in \{\mathcal{C}_\lambda\}_{\lambda\in\mathbb{N}}$ there existat a negligible functions $negl(\lambda)$ such that*

$$||\mathsf{Eval}(\tilde{C},\cdot) - C(\cdot)||_\diamond \leq 1 - negl(\lambda)$$

   where $\tilde{C} \leftarrow \mathsf{Obf}(1^\lambda, C)$.
2. *Efficiency: There exists a polynomial $p(\lambda)$ such that for any $C \in \{\mathcal{C}_\lambda\}_{\lambda\in\mathbb{N}}$ the size of the obfuscated circuit is only larger by a factor of $p(|C|)$:*

$$|\mathsf{Obf}(C)| \leq p(|C|)$$

3. *Security: For any two circuits $C_1, C_2 \in \{\mathcal{C}_\lambda\}_{\lambda\in\mathbb{N}}$ that are perfectly equivalent*

$$||C_1 - C_2||_\diamond = 0$$

   no QPT distinguisher can distinguish their obfuscation with more than negligible probability:

$$|\Pr[\mathcal{D}(\mathsf{Obf}(C_1)) = 1] - \Pr[\mathcal{D}(\mathsf{Obf}(C_2)) = 1]| \leq negl(\lambda)$$

Quantum Virtual Black Box Obfuscation

Definition 15. *(Quantum Virtual Black Box Obfuscation) The following properties are required of a QVBB obfuscator:*

1. *Correctness: The obfuscation scheme is correct if for any circuit $C \in \{\mathcal{C}_\lambda\}_{\lambda\in\mathbb{N}}$ there existat a negligible functions $negl(\lambda)$ such that*

$$||\mathsf{Eval}(\tilde{C},\cdot) - C(\cdot)||_\diamond \leq 1 - negl(\lambda)$$

   where $\tilde{C} \leftarrow \mathsf{Obf}(1^\lambda, C)$.
2. *Efficiency: There exists a polynomial $p(\lambda)$ such that for any $C \in \{\mathcal{C}_\lambda\}_{\lambda\in\mathbb{N}}$ the size of the obfuscated circuit is only larger by a factor of $p(|C|)$:*

$$|\mathsf{Obf}(C)| \leq p(|C|)$$

3. *Security: For every QPT adversary $\mathcal{A}$, there exists a QPT simulator Sim with superposition access to its oracle such that for all circuits $C \in \{C_\lambda\}_{\lambda\in\mathbb{N}}$,*

$$\left|\Pr[\mathcal{A}(\tilde{C}) = 1] - \Pr[\mathsf{Sim}^{C(\cdot)}(1^\lambda, 1^{|C|}) = 1]\right| \leq negl(\lambda)$$

   where $\tilde{C} \leftarrow \mathsf{Obf}(1^\lambda, C)$.

[9] The qiO definition from the earlier work of [AF16] differs in that they require a weaker notion of functional equivalence for C_1, C_2 in item 3. The circuits are required to have a negligible diamond norm but we (following [BK21]) require a diamond norm of 0. In fact [AF16] show that qiO is impossible to achieve under their definition.

2.8 Unclonable Encryption

Definition 16. *(Unclonable Encryption) A unclonable encryption scheme consists of three QPT algorithms* $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$

$\mathbf{KeyGen}(1^\lambda) \to (\mathbf{ek}, \mathbf{dk})$ KeyGen *takes as input the security parameter and outputs an encryption key* ek *and a decryption key* dk.

$\mathbf{Enc}(\mathbf{ek}, \mathbf{m}) \to |\mathbf{ct}\rangle$ Enc *takes as input the encryption key and a message and outputs a quantum ciphertext.*

$\mathbf{Dec}(\mathbf{dk}, |\mathbf{ct}\rangle) \to \mathbf{m}$ Dec *takes as input the decryption key and the quantum ciphertext and outputs a message*

Definition 17. *(Correctness)*

$$\Pr[\mathsf{m} = \mathsf{Dec}(\mathsf{dk}, |\mathsf{ct}\rangle) : |\mathsf{ct}\rangle \leftarrow \mathsf{Enc}(\mathsf{ek}, \mathsf{m}), (\mathsf{ek}, \mathsf{dk}) \leftarrow \mathsf{KeyGen}(1^\lambda)] \geq 1 - negl(\lambda)$$

There are various flavours of unclonable encryption such as secret-key unclonable encryption with quantum decryption keys where ek is a private classical key and $|\mathsf{dk}\rangle$ is a quantum state (see Definition 18) or public-key unclonable encryption where ek is a classical public key and dk is a classical decryption key.

Definition 18. *(Unclonable Encryption with Quantum Decryption Keys) An unclonable encryption scheme with quantum decryption keys is defined as in Definition 16 where* KeyGen *produces a secret key pair such that the decryption key is a quantum state* $|\mathsf{dk}\rangle$ *and the encryption key is a classical key. The algorithm* KeyGen *is pseudodeterministic such that it can produce several copies of the same decryption key.*

Definition 19. *(Unclonable-indistinguishable Security for Secret Key UE) Let* $\mathcal{A} = (A, B, C)$ *be a QPT adversary and let* $\lambda \in \mathbb{N}$ *be the security parameter.*

$\mathsf{Exp}_{\mathcal{A}}^{IND-UEQ}(1^\lambda)$

$(\mathsf{m}_0, \mathsf{m}_1, st) \leftarrow A(1^\lambda) where |\mathsf{m}_0| = |\mathsf{m}_1| = 1$

$(\mathsf{ek}, |\mathsf{dk}\rangle^{\otimes 2}) \leftarrow \mathsf{KeyGen}(1^\lambda)$

$b \leftarrow \{0, 1\}$

$|\mathsf{ct}\rangle \leftarrow \mathsf{Enc}(\mathsf{ek}, \mathsf{m}_b)$

$\rho^{BC} \leftarrow A(|\mathsf{ct}\rangle, st)$

$b_B \leftarrow B(\rho^B, |\mathsf{dk}\rangle)$ *and* $b_C \leftarrow C(\rho^C, |\mathsf{dk}\rangle)$ *where* B *and* C *are not allowed to communicate.*

Output $b_B = b_C = b$

An unclonable encryption scheme is called one-time unclonable-indisintguishable secure if for all (A, B, C) *if there exists a negligible function negl such that for all* $\lambda \in \mathbb{N}$*:*

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

Such a scheme is presented in [AKY24], where the authors additionally define a security notion of t-unclonability which allows the adversary to get t copies of the secret key.

Lemma 2. *[AKY24] There is a one-time unclonable encryption scheme with quantum decrpytion keys for single bit messages.*

Definition 20. *(Unclonable-Indistinguishable Security for Public Key Unclonable Encryption with Variable Decryption Keys)*

Let $\mathcal{A} = (A, B, C)$ be a QPT adversary and let λ be the security parameter.

$\mathsf{Exp}_{\mathcal{A}}^{UE-VDK}(1^\lambda)$
$(\mathsf{ek}, \mathsf{dk}_0) \leftarrow \mathsf{KeyGen}(1^\lambda, r_0), (\mathsf{ek}, \mathsf{dk}_1) \leftarrow \mathsf{KeyGen}(1^\lambda, r_1)$, *where* $r_0 = (r, r_0')$,
$r_1 = (r, r_1'), r_0', r_1' \leftarrow \{0,1\}^{l(\lambda)}, r \leftarrow \{0,1\}^{k(\lambda)}$
$(\mathsf{m}_0, \mathsf{m}_1, \rho_{\mathsf{st}}) \leftarrow A(1^\lambda, \mathsf{ek})$ *where* $|\mathsf{m}_0| = |\mathsf{m}_1| = n$
$b \leftarrow \{0,1\}$
$|\mathsf{ct}\rangle \leftarrow \mathsf{Enc}(\mathsf{ek}, \mathsf{m}_b)$
$\rho^{BC} \leftarrow A(|\mathsf{ct}\rangle, \rho_{\mathsf{st}})$
$b_B \leftarrow B(\rho^B, \mathsf{dk}_0)$ *and* $b_C \leftarrow C(\rho^C, \mathsf{dk}_1)$ *where B and C are not allowed to communicate.*
Output $b_B = b_C = b$

An unclonable encryption scheme is called unclonable-indisintguishable secure if for all (A, B, C) there exists a negligible function negl such that for all $\lambda \in \mathbb{N}$:

$$\Pr\left[\mathsf{Exp}_{\mathcal{A}}^{UE-VDK}(1^\lambda) = 1\right] \leq \frac{1}{2} + negl(\lambda)$$

3 Definition: Quantum Functional Encryption

In this section we adapt the definition of Functional Encryption to the Quantum setting. First, we give a defintion for simulation security and then for indistinguishability security. We show that simulation security implies our definition of indistinguishability security.

Definition 21. *Quantum Functional Encryption Let λ be the security parameter and let* (Setup, KeyGen, Enc, Dec) *be QPT algorithms.*

- $\mathsf{Setup}(1^\lambda) \rightarrow (\mathsf{mpk}, \mathsf{msk})$ *Given the security parameter λ output a master public key* mpk *and a master secret key* msk*.*
- $\mathsf{KeyGen}(\mathsf{msk}, C) \rightarrow \mathsf{sk}_C$ *Given the master secret key and a quantum circuit C output a secret key sk_C.*
- $\mathsf{Enc}(\mathsf{mpk}, \rho_{\mathsf{m}}) \rightarrow \rho_{\mathsf{ct}}$ *Given the public key* mpk *and a message ρ_{m} output a ciphertext ρ_{ct}.*
- $\mathsf{Dec}(\mathsf{sk}_C, \rho_{\mathsf{ct}}) \rightarrow C(\rho_{\mathsf{m}})$ *Given a function secret key sk_C and ciphertext ρ_{ct} which is an encryption of ρ_{m} output the value $C(\rho_{\mathsf{m}})$.*

Definition 22 (Correctness of a functional encryption scheme). *For all messages $\rho_{\mathsf{m}z}$, circuits C and random coins used by* Enc *and* Setup *it holds that*

$$(C(\rho_{\mathsf{m}}), \rho_z) = (\mathsf{Dec}(\mathsf{sk}_C, \rho_{\mathsf{ct}}), \rho_z)$$

where $\mathsf{sk}_C \leftarrow \mathsf{KeyGen}(\mathsf{msk}, C), \rho_{\mathsf{ct}} \leftarrow \mathsf{Enc}(\mathsf{mpk}, \rho_{\mathsf{m}})$ *and* $(\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathsf{Setup}(\lambda)$

3.1 Simulation Based Security Definition

Definition 23 (Single-query Sim-Security for QFE). *Let λ be the security parameter and let $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ be a QPT adversary and let* Sim *be a QPT simulator.*

$\mathsf{Exp}^{Real}_{\mathcal{A}}(1^\lambda)$	$\mathsf{Exp}^{Ideal}_{\mathcal{A}}(1^\lambda)$
$(\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^\lambda)$	$(\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^\lambda)$
$(\rho_{\mathsf{m}}, \rho_{\mathsf{st}}) \leftarrow \mathcal{A}_1^{O_1(\cdot)}(\mathsf{mpk})$	$(\rho_{\mathsf{m}}, \rho_{\mathsf{st}}) \leftarrow \mathcal{A}_1^{O_1(\cdot)}(\mathsf{mpk})$
$\rho_{\mathsf{ct}} \leftarrow \mathsf{Enc}(\mathsf{mpk}, \rho_{\mathsf{m}})$	$\rho_{ct} \leftarrow \mathsf{Sim}(1^\lambda, \mathsf{mpk}, \mathcal{V})$ where $\mathcal{V} = (C, \mathsf{sk}_C, C(\rho_{\mathsf{m}}), 1^{\lvert\rho_{\mathsf{m}}\rvert})$ if $\mathcal{A}$ queried O_1 on C and $\mathcal{V} = \emptyset$ otherwise.
$\alpha \leftarrow \mathcal{A}_2^{O_2(\cdot)}(\rho_{\mathsf{ct}}, \rho_{\mathsf{st}})$	$\alpha \leftarrow \mathcal{A}_2^{O'_2(\cdot)}(\rho_{\mathsf{ct}}, \rho_{\mathsf{st}})$
The experiment outputs the state α	The experiment outputs the state α

The QFE scheme is single-query simulation-secure if for any adversary $\mathcal{A}$ and all messages ρ_{m} there exists a simulator Sim *such that the real and ideal distributions are computationally indistinguishable:*

$$\{\mathsf{Exp}^{Real}_{\mathcal{A}}(1^\lambda)\}_{\lambda\in\mathbb{N}} \approx_c \{\mathsf{Exp}^{Ideal}_{\mathcal{A}}(1^\lambda)\}_{\lambda\in\mathbb{N}}$$

.

Adaptive vs Non-adaptive security:

1. *Non-adaptive: the adversary $\mathcal{A}_1$ is allowed to make one key query to $O_1(\cdot)$ where the oracle $O_1(\cdot)$ is $\mathsf{KeyGen}(\mathsf{msk}, C) \to sk_C$.*
2. *Adaptive: the adversary is allowed to make one key query either to $O_1(\cdot)$ or $O_2(\cdot)$ ($O'_2(\cdot)$ in the ideal world) where $O_1(\cdot)$ and $O_2(\cdot)$ are $\mathsf{KeyGen}(\mathsf{msk}, C) \to sk_C$ and $O'_2(\cdot)$ is a* KeyGen *oracle controlled by the simulator $\mathsf{sk}_C \leftarrow \mathsf{Sim}(1^\lambda, \mathsf{msk}, C, C(\rho_{\mathsf{m}}), 1^{\lvert\rho_{\mathsf{m}}\rvert})$. The simulator is stateful, in this invocation* Sim *has access to the state of the simulator from it's first invocation where it produced the ciphertext.*

3.2 Indistinguishability Based Security Definition

In this section we comment on potential issues when trying to find an appropriate indistinguishability-based definintion of functional encryption for the quantum setting. The simulation-based definition is generally preferred as indistinguishability-based security does not capture a meaningful security notion for some functions [O'N10; BSW11]. Nevertheless indistinguishability-based security can be easier to achieve and still has many important applications as we can see in the extension to the multi-input setting in Section 6.

First we give the definition for the IND-security experiment and then we discuss the notion of admissible queries in depth.

Definition 24 (Single-Query IND-Security for QFE).
Let λ be the security parameter and let $\mathcal{A} = (\mathcal{A}_0, \mathcal{A}_1)$ be a QPT adversary.

$\mathsf{Exp}^{IND}_{\mathcal{A},b}(1^\lambda)$

$(\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^\lambda)$

$(\rho_{\mathsf{m}_0}, \rho_{\mathsf{m}_1}, \rho_{\mathsf{st}}) \leftarrow \mathcal{A}_0^{\mathsf{sk}_C \leftarrow \mathsf{KeyGen}(\mathsf{msk},\cdot)}(\mathsf{mpk})$, *where ρ_{m_0} and ρ_{m_1} are admissible queries for the circuit C that $\mathcal{A}$ queries.*

$\rho_{\mathsf{ct}} \leftarrow \mathsf{Enc}(\mathsf{mpk}, \rho_{\mathsf{m}_b})$

$b' \leftarrow \mathcal{A}_1^{O(\cdot)}(\mathsf{mpk}, \rho_{\mathsf{ct}}, \rho_{\mathsf{st}})$

The FE scheme is called secure if for any adversary $\mathcal{A}$ that makes admissible queries (Definition 25) it holds that

$$\left|\Pr\left[1 \leftarrow \mathsf{Exp}^{Ind}_{\mathcal{A},b=0}\right] - \Pr\left[1 \leftarrow \mathsf{Exp}^{Ind}_{\mathcal{A},b=1}\right]\right| \leq negl(\lambda)$$

where the random coins are taken over the randomnes of $\mathcal{A}$, Setup, KeyGen *and* Enc.

Adaptive vs. Non-adaptive security

- *The scheme is called non-adaptively secure if the the adversary only queries the* KeyGen *oracle before receiving a ciphertext. Then the oracle $O(\cdot)$ is the empty oracle.*
- *The scheme is called adaptively secure if the adversary can either query the* KeyGen *oracle before or after receiving the ciphertext. Then the oracle $O(\cdot)$ is the function* $\mathsf{KeyGen}(\mathsf{msk}, \cdot)$.

In the classical setting admissible queries are defined as $C(\mathsf{m}_0) = C(\mathsf{m}_1)$. To adjust this definition to the quantum setting we have to redefine the condition that the quantum circuit has the same output on the inputs ρ_{m_0} and ρ_{m_1}. A natural first attempt to define admissible queries $\rho_{\mathsf{m}_0}, \rho_{\mathsf{m}_1}$ is to use the trace distance of the output states since the trace distance bounds the adversaries probability of distinguishing two quantum states

$$\mathrm{TD}(C(\rho_{\mathsf{m}_0}), C(\rho_{\mathsf{m}_1})) \leq negl(\lambda)$$

This definition is not sufficient as can be seen in the following scenario: $\mathcal{A}$ creates the states $\rho = |EPR\rangle\langle EPR|$ and $\sigma = |EPR\rangle\langle EPR|$ and gives one qubit each to the experiment $\rho_{\mathsf{m}_0} = \rho_1$ and $\rho_{\mathsf{m}_1} = \sigma_1$. $\mathcal{A}$ queries the identity circuit and receives ρ_{ct}. The states ρ_{m_0} and ρ_{m_1} have trace distance 0 since they are both the maximally mixed state. $\mathcal{A}$ can decrypt ρ_{ct} using the function secret key and check with non-negl probability which quibt it is by applying a coherent measurement on the qubit remaining in it's internal state and the received qubit.

The above attack is not applicable in the simulation-based setting. The scheme that we proved secure under Sim-security allows an adversary to stay entangled with the challenge message. This entanglement is maintained by the encryption procedure or the simulator respectively.

An alternative approach to defining IND-security would be to take the adversaries internal state into account. The messages $\rho_{\mathsf{m}_0} = \sum_i p_i \rho_{\mathsf{m}_{0,i}}, \rho_{\mathsf{m}_1} = \sum_i q_i \rho_{\mathsf{m}_{1,i}}$ are admissible queries if

$$\mathrm{TD}\left(\sum_i p_i C(\rho_{\mathsf{m}_{0,i}}) \otimes \rho_{A_i}, \sum_i q_i C(\rho_{\mathsf{m}_{1,i}}) \otimes \rho_{A_i}\right) \leq negl(\lambda). \tag{1}$$

where ρ_A is the adversary's internal state.

For many functionalities this would enforce the adversary to stay unentangled with the challenge message queries. The definition might still be useful in some applications, as for example messages that are not chosen by the adversary fall into this category.

To allow the adversary more freedom and in particular to enable the adversary to stay entangled with a part of the challenge message we can allow the following way of querying messages.

Definition 25. *(Admissible queries) For a challenge message $\rho^{EU}_{\mathsf{m}_b}$ the adversary specifies a register E that is encrypted and a register U that will be returned unencrypted to the adversary. The message $\rho^{EU}_{\mathsf{m}_{1-b}}$ which is not used as the challenge is not returned to the adversary. Then the challenge queries have to fulfill:*

$$TD\left(\sum_i p_i C(\rho^E_{\mathsf{m}_{0,i}}) \otimes \rho^U_{\mathsf{m}_{0,i}} \otimes \rho_{A_i}, \sum_i q_i C(\rho^E_{\mathsf{m}_{1,i}}) \otimes \rho^U_{\mathsf{m}_{1,i}} \otimes \rho_{A_i}\right) \leq negl(\lambda) \tag{2}$$

where ρ_A is the adversary's internal state and C is the circuit that the adversary queries.

In practice this allows for any entanglement to be moved into the challenge query such that the state of the adversary is unentangled with the message queries and the state can be written as $\rho_{\mathsf{m}_0^{EU}} \otimes \rho_{\mathsf{m}_1^{EU}} \otimes \rho_{\mathcal{A}}$. This simplifies the check if the query is admissible to

$$\begin{aligned}&\mathrm{TD}\left(\sum_i p_i C(\rho^E_{\mathsf{m}_{0,i}}) \otimes \rho^U_{\mathsf{m}_{0,i}} \otimes \rho_A, \sum_i q_i C(\rho^E_{\mathsf{m}_{1,i}}) \otimes \rho^U_{\mathsf{m}_{1,i}} \otimes \rho_A\right)\\ &= \mathrm{TD}\left(\sum_i p_i C(\rho^E_{\mathsf{m}_{0,i}}) \otimes \rho^U_{\mathsf{m}_{0,i}}, \sum_i q_i C(\rho^E_{\mathsf{m}_{1,i}}) \otimes \rho^U_{\mathsf{m}_{1,i}}\right) \leq negl(\lambda).\end{aligned}$$

Useful special cases of Definition 25 are

1. Classical messages. For classical messages the definition reduces to the classical definition of admissibility since
$$\mathrm{TD}(C(\mathsf{m}_0) \otimes \rho_A, C(\mathsf{m}_1) \otimes \rho_A) = 0.$$
exactly when $C(\mathsf{m}_0) = C(\mathsf{m}_1)$.
2. Defining both ρ_{m_0} and ρ_{m_1} with respect to a single quantum state σ. In the IND-security game the adversary might hold a single copy of a special quantum state σ which he would like to use for defining both messages ρ_{m_0} and ρ_{m_1}. Since the experiment only creates a single ciphertext and discards the other message we can allow the adversary to only provide a single copy of σ and define ρ_{m_0} and ρ_{m_1} to each contain the state σ.

This definition of IND-security is implied by simulation secure quantum functional encryption.

Lemma 3. *A QFE scheme that is single-query (non)-adaptively SIM-secure (Definition 23) is also single-query (non)-adaptively IND-secure (Definition 24).*

The proof can be found in Appendix B.

4 Construction: Quantum Functional Encryption

We construct a single-query adaptively secure functional encryption scheme for quantum circuits. We start by constructing a simple functional encryption scheme for a single circuit where the circuit has to be fixed ahead of time. Then we use this construction to achieve single-query adaptively secure functional encryption for polynomial sized circuits. Our construction follows the ideas used by [SS10; GVW12] in the classical setting. They show how to leverage classical randomized encodings to achieve classical functional encryption. Similarly, quantum randomized encodings can be used to achieve quantum functional encryption.

4.1 QFE for a Single Circuit

First we construct a quantum functional encryption scheme that only allows to evaluate a circuit family consisting of one circuit $\mathcal{C} = \{C_\lambda\}_{\lambda in \mathbb{N}}$ with fixed input size $n = poly(\lambda)$ and output size $d = poly(\lambda)$. To achieve this construction we make use of the Quantum One Time Pad and a classical FE scheme that allows functional encryption for the identity circuit $\mathsf{IdFE} = (\mathsf{IdFE.Setup}, \mathsf{IdFE.KeyGen}, \mathsf{IdFE.Enc}, \mathsf{IdFE.Dec})$. Such a scheme is constructed in [GVW12]. Let $D(\mathcal{H}_n)$ be the input space, let $D(\mathcal{H}_d)$ be the output space and let the circuit be denoted as C.

Setup(1^λ) $\rightarrow$ (mpk, msk) Run the classical IdFE scheme to obtain the keys $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{IdFE.Setup}(1^\lambda)$. Output $(\mathsf{mpk} = \mathsf{pk}, \mathsf{msk} = \mathsf{sk})$.

Enc(mpk, ρ_m) $\rightarrow$ ct Sample a pair of keys for the QOTP (a, b), where $a, b \in \{0,1\}^d$. Compute

$$\rho_{\mathsf{ct}_0} = \mathsf{X}^a\mathsf{Z}^b C(\rho_\mathsf{m})$$

Encrypt the QOTP keys using the classical FE scheme

$$\mathsf{ct}_1 = \mathsf{IdFE.Enc}(\mathsf{mpk}, (a, b))$$

Output $\mathsf{ct} = (\rho_{\mathsf{ct}_0}, \mathsf{ct}_1)$.

KeyGen(msk) $\rightarrow$ sk* Run the IdFE scheme to obtain the secret key $\mathsf{sk}^* = \mathsf{IdFE.KeyGen}(\mathsf{msk})$.

Dec(sk*, ct) $\rightarrow$ ρ_m Given $\mathsf{ct} = (\rho_{\mathsf{ct}_0}, \mathsf{ct}_1)$ use the key sk^* to obtain the QOPT keys $(a, b) = \mathsf{IdFE.Dec}(\mathsf{sk}^*, \mathsf{ct}_1)$ and then decrypt the quantum state

$$\rho_\mathsf{m} = \mathsf{X}^a\mathsf{Z}^b\rho_{\mathsf{ct}_0}$$

Theorem 5. *Given a classical FE scheme for the identity circuit that fulfills adaptive sim-security, there exists an adaptively sim-secure QFE scheme for a single circuit.*

Proof.

Correctness Due to the correctness of the classical FE scheme and the correctness of the QOTP the scheme is correct.

Security We define a simulator Sim for the scheme. The adversary can either query the key first and then obtain the ciphertext or obtain the ciphertext first and then the key. We distinguish the simulator's behaviour in these two cases.

1. The adversary queries non-adaptively, i.e. it queries the key first. That means the simulator obtains $C(\rho_\mathsf{m})$. The simulator creates the ciphertext as the honest encryption algorithm would.
2. The adversary queries adaptively, i.e. it queries the ciphertext first. The simulator needs to create a ciphertext without knowledge of the value it should later decrypt to. The simulator creates d EPR pairs and sends one qubit of each EPR pair to the adversary and keeps the other qubit of each EPR pair. The classical ciphertext is simulated via the simulator of the classical FE scheme:
$$\mathsf{ct} = \mathsf{IdFE.Sim}(\mathsf{mpk}, |x| = 2d)$$
When the adversary queries the key, the simulator learns $C(\rho_\mathsf{m})$ and performs the teleportation circuit using $C(\rho_\mathsf{m})$ and the halves of the EPR pairs which he holds. Sim obtains the correction keys $(a, b) \in \{0,1\}^d$ and creates the key using the simulator for the classical IdFE-scheme:
$$sk^* = \mathsf{IdFE.Sim}(\mathsf{sk}, (a, b))$$
. The simulator outputs sk^*.

In the case of a non-adaptive query the simulator behaves as the experiment in the real world. Therefore real and ideal experiments are indistinguishable. For the case of an adaptive query we establish security via a series of hybrids:

Hybrid 0: This is the real world, where the ciphertext is created by the Encryption algorithm

Hybrid 1: In this Hybrid we use the simulator of the classical IdFE-scheme to simulate the ciphertext in case of an adaptive query. The quantum state part of the ciphertext is created honestly and the corresponding encryption keys are used to answer the key query using the simulator of the IdFE-scheme.

Claim. Hybrid 0 and Hybrid 1 are computationally indistinguishable.

Proof. Due to the adaptive security of the IdFE-scheme this change is not noticeable to the adversary. An adversary that can distinguish between Hybrid 0 and Hybrid 1 could distinguish between the real and simulated experiment of the IdFE scheme. □

Hybrid 2: This is the Ideal world where the simulator Sim runs as defined above.

Claim. Hybrid 1 and Hybrid 2 are perfectly indistinguishable.

Proof. The simulator creates d EPR pairs and sends one qubit each as a ciphertext ρ_{ct_0}. Upon receiving $(\rho_{\mathsf{ct}_0}, \mathsf{ct}_1)$ the adversary cannot distinguish ρ_{ct_0} in Hybrid 1 from the state in Hybrid 2 since 1 qubit of an EPR pair appears as a maximally mixed state, the same as a state encrypted under the QOTP. Since ct_1 is a ciphertext simulated by IdFE as in the previous Hybrid it contains no information about the QOTP keys. Upon receiving the key query the simulator obtains $C(\rho_{\mathsf{m}})$ and teleports the state through the corresponding EPR pairs and obtains the correction keys (a, b). The teleported state the adversary now holds is $X^a Z^b C(\rho_{\mathsf{m}})$ which is equivalent to a QOTP encrypted state with the key (a, b). The keys are revealed using the IdFE simulator. □

□

4.2 QFE for a poly-sized family of circuits

In this section we construct a QFE scheme for circuits of polynomial size. We need the following building blocks:

Let $\mathsf{OneQFE} = (\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ be the single circuit QFE scheme from the previous section. Let $\mathsf{TwoFE} = (\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ be a classical FE scheme for a family of two circuits [GVW12]. Let $\mathsf{QRE} = (\mathsf{Encode}, \mathsf{Decode})$ be a quantum randomized encoding scheme that is also decomposable. In particular we will use the quantum garbled circuits construction of [BY22] which has the special property that if there is a classical part of the input the encoding procedure is classical.

Let U be a universal quantum circuit, that is on inputs ρ_{m} and C it evaluates to $U(C, \rho_{\mathsf{m}}) = C(\rho_{\mathsf{m}})$. Let the decription of C have length l and ρ_{m} be a quantum state of dimension n. Then we can create a randomized encoding of $U(C, \rho_{\mathsf{m}})$ where due to the decomposability the randomized encoding can be created in independent pieces where each piece only depends on one bit of the input. Let R denote classical randomness and e denote a set of EPR pairs, then the randomized encoding $\tilde{U}$ can be written as

$$\begin{aligned}\mathsf{Encode}(U, C, \rho_{\mathsf{m}}, R, e) &= \tilde{U}(C, \rho_{\mathsf{m}}, R, e) \\ &= (\tilde{U}_1(C[1], R, e_1), \ldots, \tilde{U}_l(C[l], R, e_1), \tilde{U}_x(\rho_{\mathsf{m}}, R, e_2), \tilde{U}_{off}(R, e_3))\end{aligned}$$

where e_1, e_2, e_3 are disjoint subsets of the qubits contained in the set of EPR pairs e.

To construct FE for a poly sized family of circuits we use l instances of the classical TwoFE scheme for the family of two circuits $\{f_{C[i]=0}, f_{C[i]=1}\}$:

$$\begin{aligned}f_{C[i]=0}(R, t) &= \tilde{U}_i(0, R, t) \\ f_{C[i]=1}(R, t) &= \tilde{U}_i(1, R, t)\end{aligned}$$

where t is a classical bit that can be obtained from measuring the EPR pairs from the set e_1.

During encryption we create l classical ciphertexts that can later be opened to the description of the circuit using the KeyGen algorithm of TwoFE. Given a description of C the $i'th$ ciphertext is opened such that it decrypts to $\tilde{U}_i(C[i], R, t)$, the randomized encoding of the $i'th$ bit of the description of C.

Additionally we use two instances of the quantum OneQFE scheme for the circuits:

$$f_{in}(\rho_{\mathsf{m}}, e, R) = \tilde{U}_{in}(\rho_{\mathsf{m}}, R, e)$$

$$f_{off}(e, R) = \tilde{U}_{off}(R, e)$$

Putting everything together we can see that our encryption procedure produces the individual pieces of the decomposable randomized encoding scheme by relying on simpler functional encryption primitives. The final output $C(\rho_{\mathsf{m}})$ can be obtained by decrypting the individual parts of the ciphertext and then the result can be decoded.

Let $\lambda \in \mathbb{N}$ be the security parameter and let $\mathcal{M} = D(\mathcal{H}_s)$ where $s = poly(\lambda)$ be the message space. Let $\mathcal{C} = \{C_\lambda\}_\lambda$ be a family of quantum circuits with inputs of size s, outputs of size $t = poly(\lambda)$ and classical description of size $l = poly(\lambda)$.

$\mathsf{Setup}(1^\lambda) \to (\mathsf{mpk}, \mathsf{msk})$ Create l keys for the TwoFE-scheme:

$$(\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow \mathsf{TwoFE.KeyGen}(1^\lambda) \quad for\ i \in 1, \ldots, l$$

where the i-th keypair is associated with the circuit family $\{f_{C[i]=0}, f_{C[i]=1}\}$.
Run the OneQFE scheme twice, once for the circuit f_{in} and once for the circuit f_{off}.

$$(\mathsf{pk}_{in}, \mathsf{sk}_{in}) \leftarrow \mathsf{OneQFE.KeyGen}(1^\lambda)$$
$$(\mathsf{pk}_{off}, \mathsf{sk}_{off}) \leftarrow \mathsf{OneQFE.KeyGen}(1^\lambda)$$

Output $(\mathsf{mpk} = (\mathsf{pk}_1, \ldots, \mathsf{pk}_l, \mathsf{pk}_{in}, \mathsf{pk}_{off}), \mathsf{msk} = (\mathsf{sk}_1, \ldots, \mathsf{sk}_l, \mathsf{sk}_{in}, \mathsf{sk}_{off}))$.

$\mathsf{Enc}(\mathsf{mpk}, \rho_{\mathsf{m}} \in \mathcal{M}) \to \rho_{\mathsf{ct}}$ Sample $R \leftarrow \mathcal{R}$ and sample $l+n+k$ EPR pairs. The EPR pairs are split into 3 groups $E^l = \{(e^l_{i,1}, e^l_{i,2})\}_{i\in[l]}$, $E^n = \{(e^n_{i,1}, e^n_{i,2})\}_{i\in[n]}$ and $E^k = \{(e^k_{i,1}, e^k_{i,2})\}_{i\in[k]}$. For $i \in 1, \ldots, l$ take the first qubit of each EPR pair in the group E^l and measure it in the computational basis to obtain t_i, then compute

$$ct_i \leftarrow \mathsf{TwoFE.Enc}(\mathsf{pk}_i, R, t_i)$$

Use the quantum OneQFE scheme to compute the ciphertext

$$\rho_{ct_{in}} \leftarrow \mathsf{OneQFE.Enc}(\mathsf{pk}_{in}, \rho_{\mathsf{m}}, R, \{e^n_{i,1}\}_{i\in[n]})$$

and compute the ciphertext

$$\rho_{ct_{off}} \leftarrow \mathsf{OneQFE.Enc}(\mathsf{pk}_{off}, R, \{e^n_{i,2}\}_{i\in[n]}, \{e^l_{i,2}\}_{i\in[l]}, E^k)$$

Output $\rho_{\mathsf{ct}} = (\{\mathsf{ct}_i\}_{i\in[l]}, \rho_{\mathsf{ct}_{in}}, \rho_{\mathsf{ct}_{off}})$.

$\mathsf{KeyGen}(\mathsf{msk}, C \in \mathcal{C}) \to \mathsf{sk}^*_C$ For $i \in 1, \ldots, l$ create

$$sk^*_i = \mathsf{TwoFE.KeyGen}(\mathsf{sk}_i, f_{C[i]})$$

and create

$$sk^*_{in} \leftarrow \mathsf{OneQFE.KeyGen}(\mathsf{sk}_{in}, f_{in})$$
$$sk^*_{off} \leftarrow \mathsf{OneQFE.KeyGen}(\mathsf{sk}_{off}, f_{off})$$

Output $sk^*_C = (\mathsf{sk}^*_1, \ldots, \mathsf{sk}^*_l, \mathsf{sk}^*_{in}, \mathsf{sk}^*_{off})$.

$\mathbf{Dec}(\mathsf{sk}^*_C, \boldsymbol{\rho}_{\mathsf{ct}}) \to \boldsymbol{\rho}_{\mathsf{m}}$ For $i \in 1, \cdots, l$ decrypt

$$\tilde{U}(C[i], R, t_i) = \mathsf{TwoFE.Dec}(\mathsf{sk}^*_i, ct_i)$$

and create

$$\tilde{U}(\rho_{\mathsf{m}}, R, e) \leftarrow \mathsf{OneQFE.Dec}(\mathsf{sk}^*_{in}, \rho_{ct_{in}})$$
$$\tilde{U}(R, e) \leftarrow \mathsf{OneQFE.Dec}(\mathsf{sk}^*_{off}, \rho_{ct_{off}})$$

Output $y = \mathsf{Decode}(\tilde{U}(C[1], R, t_1), \ldots, \tilde{U}(C[l], R, t_l), \tilde{U}(\rho_{\mathsf{m}}, R, e), \tilde{U}(R, e))$.

Theorem 6. *Given an adaptively sim-secure classical FE scheme for a family of two circuits, an adaptively sim-secure QFE scheme for a single circuit and a QGC scheme, there exists an adaptively sim-secure QFE scheme for poly sized circuits.*

Proof.

Correctness

$$\begin{aligned}
&\mathsf{Dec}(\mathsf{sk}_C, \mathsf{Enc}(\mathsf{msk}, \rho_{\mathsf{m}})) = \mathsf{Dec}(\mathsf{sk}^*_C, ct_1, \ldots ct_l, \rho_{ct_{in}}, \rho_{ct_{off}}) \\
&= \mathsf{Decode}(\mathsf{TwoFE.Dec}(\mathsf{sk}^*_1, ct_1), \ldots, \mathsf{TwoFE.Dec}(\mathsf{sk}^*_l, ct_l), \mathsf{OneQFE.Dec}(\mathsf{sk}^*_{in}, \rho_{ct_{in}}), \\
&\quad \mathsf{OneQFE.Dec}(\mathsf{sk}^*_{off}, \rho_{ct_{off}})) \\
&= \mathsf{Decode}(\tilde{U}(C[1], R, t_1), \ldots, \tilde{U}(C[l], R, t_l), \tilde{U}(\rho_{\mathsf{m}}, R, e), \tilde{U}(R, e)) \\
&= \mathsf{Decode}(\mathsf{Encode}(U, C, \rho_{\mathsf{m}}, R, e)) \\
&= C(\rho_{\mathsf{m}})
\end{aligned}$$

Security We define a simulator Sim for the scheme. We distinguish whether the adversary makes an adaptive or non-adaptive query.

1. The adversary queries non-adaptively. The simulator obtains $C, C(\rho_{\mathsf{m}})$ and creates the ciphertext as follows:
   (a) Create the randomized encoding using the simulator of the QRE scheme.
   $$(\hat{U}(C[1], R, t_1), \ldots, \hat{U}(C[l], R, t_l), \hat{U}(\rho_{\mathsf{m}}, R, e), \hat{U}(R, e)) \leftarrow \mathsf{QRE.Sim}(C(\rho_{\mathsf{m}}), \mathcal{T}_C)$$
   where $\mathcal{T}_C$ is the topology of the circuit $U(\cdot)$.
   (b) Create the ciphertexts using the simulator of the classical TwoFE scheme and the quantum OneQFE scheme for the non-adaptive case to create ciphertexts:
   $$\begin{aligned}
   ct_i &\leftarrow \mathsf{TwoFE.Sim}(\mathsf{pk}_i, \hat{U}(C[i], R, t_1)) \quad for\ i \in [l] \\
   \rho_{ct_{in}} &\leftarrow \mathsf{OneQFE.Sim}(\mathsf{pk}_{in}, \hat{U}(\rho_{\mathsf{m}}, R, e)) \\
   \rho_{ct_{off}} &\leftarrow \mathsf{OneQFE.Sim}(\mathsf{pk}_{off}, \hat{U}(R, e))
   \end{aligned}$$
2. The adversary queries adaptively. The simulator has to create a ciphertext without knowing the evaluation result.
   (a) Use the simulator of the classical TwoFE scheme and the quantum OneQFE scheme for the adaptive case to create ciphertexts:
   $$\begin{aligned}
   (ct_i, st_i) &\leftarrow \mathsf{TwoFE.Sim}(\mathsf{pk}_i, 1^{|C[i]|+|R|+|t_i|}) \quad for\ i \in [l] \\
   (\rho_{ct_{in}}, st_{in}) &\leftarrow \mathsf{OneQFE.Sim}(\mathsf{pk}_{in}, 1^{|\mathsf{m}|+|R|+|e|}) \\
   (\rho_{ct_{off}}, st_{off}) &\leftarrow \mathsf{OneQFE.Sim}(\mathsf{pk}_{off}, 1^{|R|+|e|})
   \end{aligned}$$

(b) Upon receiving a key query Sim obtains $C(\rho_{\mathsf{m}})$ and can create the randomized encoding.

$$(\hat{U}(C[1], R, t_1), \cdots, \hat{U}(C[l], R, t_l), \hat{U}(\rho_{\mathsf{m}}, R, e), \hat{U}(R, e)) \leftarrow \mathsf{QRE.Sim}(C(\rho_{\mathsf{m}}))$$

(c) Then Sim creates the key by using the simulator of the underlying FE schemes.

$$\mathsf{sk}_i^* \leftarrow \mathsf{TwoFE.Sim}(\mathsf{sk}_i, \hat{U}(C[i], st_i, R, t_i)) \quad for\ i \in [l]$$
$$\mathsf{sk}_{in}^* \leftarrow \mathsf{OneQFE.Sim}(\mathsf{sk}_{in}, st_{in}, \hat{U}(\rho_{\mathsf{m}}, R, e))$$
$$\mathsf{sk}_{off}^* \leftarrow \mathsf{OneQFE.Sim}(\mathsf{sk}_{off}, st_{off}, \hat{U}(R, e))$$

Hybrid 0 This is the real world.

Hybrid i For $i \in \{1, \ldots, l\}$. Sample R and E^l, E^n, E^k as in Enc.

For $1 \leq j < l$ let the ciphertexts be created honestly:

$$ct_j \leftarrow \mathsf{TwoFE.Enc}(pk_j, R, t_j)$$

In the non-adaptive case:

For $i \leq j \leq l$ create the partial randomized encoding and simulate the ciphertext using the simulator of the underlying scheme:

$$ct_j \leftarrow \mathsf{TwoFE.Sim}(\tilde{U}(C[i], R, t_i))$$

In the adaptive case:

For $i \leq j \leq l$ simulate the ciphertext using the simulator of the underlying scheme:

$$ct_j \leftarrow \mathsf{TwoFE.Sim}(\mathsf{pk}_i, 1^{|C[i]|+|R|+|e_i|})$$

Create $\rho_{ct_{in}}, \rho_{ct_{off}}$ honestly.

Claim. Hybrids 0 to l are indistinguishable up to negligible probability.

Proof. To show indistinguishability of each pair of games we can invoke the security of the TwoFE scheme. A distinguisher between the Hybrids can break the security of the TwoFE scheme. □

Hybrid l+1, Hybrid l+2 For ciphertexts $\rho_{ct_{in}}$ and $\rho_{ct_{off}}$ use the simulator to create the ciphertexts in Hybrid l+1 and Hybrid l+2 respectively.

In the non-adaptive case:

$$\rho_{ct_{in}} \leftarrow \mathsf{OneQFE.Sim}(\mathsf{pk}_{in}, \tilde{U}(\rho_{\mathsf{m}}, R, E^n))$$
$$\rho_{ct_{off}} \leftarrow \mathsf{OneQFE.Sim}(\mathsf{pk}_{off}, \tilde{U}(R, E^k))$$

In the adaptive case:

$$\rho_{ct_{in}} \leftarrow \mathsf{OneQFE.Sim}(\mathsf{pk}_{in}, 1^{|\mathsf{m}|+|R|+|E^n|})$$
$$\rho_{ct_{off}} \leftarrow \mathsf{OneQFE.Sim}(\mathsf{pk}_{off}, 1^{|R|+|E^k|})$$

Claim. Hybrids l and l+1 are indistinguishable as well as Hybrids l+1 and l+2 up to negligible probability.

Proof. To show indistinguishability of each pair of games we can invoke the security of the OneQFE scheme. A distinguisher between the Hybrids can break the security of the OneQFE scheme. □

Hybrid l+3 In the non-adaptive case: Upon receiving the key query $C, C(\rho_{\mathsf{m}})$ use the simulator of the randomized encoding to create $\hat{U}(C(\rho_{\mathsf{m}}), \mathcal{T}_C) \leftarrow \mathsf{Sim}$ and use the simulated randomized encoding to create the ciphertext instead of the real randomized encoding.

In the adaptive case: Upon receiving the key query $C, C(\rho_{\mathsf{m}})$ use the simulator of the randomized encoding to create $\hat{U}(C(\rho_{\mathsf{m}}), \mathcal{T}_C) \leftarrow \mathsf{Sim}$ and use the simulated randomized encoding to answer the secret key query.

This is the ideal world.

Claim. Hybrids l+2 and l+3 are indistinguishable up to negligible probability.

Proof. Due to the indistinguishability of the simulated randomized encoding from the real randomized encoding the Hybrids are indistinguishable. □

□

5 Unclonable Functional Encryption

In this section we define and construct an unclonable functional encryption scheme. Security requires that two participants who try to copy a ciphertext can obtain independently generated function secret keys for any circuit and cannot both guess which messages out of two challenge messages was encrypted. When the function secret keys are fixed to be the identity circuit this implies a public-key unclonable encryption scheme with variable decryption keys (Definition 20).

5.1 Definition

An unclonable functional encryption scheme is defined by the syntax and correctness properties of a QFE scheme, see Definition 21 and Definition 22.

Definition 26. *(Non-adaptive Unclonable-Indistinguishable Functional Encryption)*

Let λ be the security parameter, let $\mathcal{A} = (A, B, C)$ be a QPT adversary and let $\mathcal{C}_\lambda$ be a family of circuits.

$\mathsf{Exp}_{\mathcal{A}}^{QFE-UE-IND}(1^\lambda)$

$(\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^\lambda)$

$(\rho_{\mathsf{m}_0}, \rho_{\mathsf{m}_1}, \rho_{\mathsf{st}}, C_B, C_C) \leftarrow A(1^\lambda, \mathsf{mpk})$

$b \leftarrow \{0,1\}$ $\qquad\qquad$ $\rho_{\mathsf{ct}} \leftarrow \mathsf{Enc}(\mathsf{mpk}, \rho_{\mathsf{m}_b})$

$\mathsf{sk}_{C_B} \leftarrow \mathsf{KeyGen}(\mathsf{msk}, C_B), \mathsf{sk}_{C_C} \leftarrow \mathsf{KeyGen}(\mathsf{msk}, C_C)$

$\rho_{BC} \leftarrow A(\rho_{\mathsf{ct}}, \rho_{\mathsf{st}})$

$b_B \leftarrow B(\mathsf{mpk}, \rho_{\mathsf{ct}}, \rho_{\mathsf{st}_B}, \mathsf{sk}_{C_B})$

$b_C \leftarrow C(\mathsf{mpk}, \rho_{\mathsf{ct}}, \rho_{\mathsf{st}_C}, \mathsf{sk}_{C_C})$

$Output b_B = b_C = b$

The FE scheme is called unclonable-indistinguishably secure if for any adversary $\mathcal{A} = (A, B, C)$ and any $C_B, C_C \in \mathcal{C}_\lambda$

$$\Pr\left[\mathsf{Exp}_{\mathcal{A}}^{QFE-UE-IND}(1^\lambda) = 1\right] \leq \frac{1}{2} + negl(\lambda)$$

where the random coins are taken over the randomness of $\mathcal{A}$, $\mathsf{Setup}, \mathsf{KeyGen}$ and Enc.

For brevity we often refer to this definition as unclonable functional encryption.

Remark 1. An adaptive security notion of unclonable functional encryption can be defined by giving each B and C oracle access to the KeyGen functionality instead of $\mathcal{A}$ outputting a description of the circuits for which secret keys should be produced.

5.2 Construction

We need the following components:

- Let $\mathsf{QFE} = (\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ be a non-adaptive IND-secure QFE scheme.
- Let $\mathsf{UEQ} = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ be a one-time unclonable-indistinguishable encryption scheme for single bit messages with quantum decryption keys of size $l(\lambda)$ and ciphertext size $t(\lambda)$ and let $s(\lambda)$ be an upper bound on the description of the decrpytion circuit.

We highlight that the construction is solely based on the QFE scheme and the UEQ scheme is not explicitly used, we only require the existence of a UEQ scheme. The unclonable QFE scheme is universal which means that the unclonable security property holds as long as any UEQ scheme with the mentioned properties is secure, such as [AKY24].

The construction relies on a QFE scheme for the family of circuits $\mathcal{U}_\lambda = \{U_{p(\lambda),l(\lambda),s(\lambda),n(\lambda)}\}_{\lambda\in\mathbb{N}}$ which has the following structure:

$U_{(C,a,b)}(\rho_{\mathsf{m}_0}, \rho_{\mathsf{m}_1}, |\mathsf{dk}_0\rangle, |\mathsf{dk}_1\rangle, \rho_{UE}, C_{Dec}, f) =$
- if $f = 0$ output $C(\rho_{\mathsf{m}_0})$
- if $f = 1$ do:
  - Compute $|\mathsf{dk}'_0\rangle = X^a Z^b |\mathsf{dk}_0\rangle$ and $|\mathsf{dk}'_1\rangle = X^a Z^b |\mathsf{dk}_1\rangle$
  - Measure the first λ bits of $|\mathsf{dk}'_0\rangle$ in the computational basis,
  - if they are all 0 remove them and set $|\mathsf{dk}^*\rangle = |\mathsf{dk}'_0\rangle$
    - else measure the first λ bits of $|\mathsf{dk}'_1\rangle$ in the computational basis,
    - if they are all 0 remove them and set $|\mathsf{dk}^*\rangle = |\mathsf{dk}'_1\rangle$
    - else if both checks fail output $\perp$
  - Interpret C_{Dec} as the description of a circuit for decryption: $U(C_{Dec}, |\mathsf{dk}^*\rangle, \rho_{UE}) = b$
  - Output $C(\rho_{\mathsf{m}_b})$

Then the following is an unclonable functional encryption scheme for a family of quantum circuits $\mathcal{C} = \{C_\lambda\}_{\lambda\in\mathbb{N}}$ with classical description of size $p(\lambda)$ inputs in $\mathcal{X} = \mathcal{D}(\mathcal{H}_n)$.

$\mathsf{Setup}(1^\lambda, r) \to (\mathsf{mpk}, \mathsf{msk})$ Run $(\mathsf{mpk}, \mathsf{msk}) = \mathsf{QFE.Setup}(1^\lambda, r)$.
Output $(\mathsf{mpk}, \mathsf{msk})$.

$\mathsf{KeyGen}(1^\lambda, C \in \mathcal{C}_\lambda, r') \to \mathsf{sk}_C$ Sample random strings $a, b \leftarrow \{0,1\}^{l(\lambda)+s(\lambda)}$ using randomness r'.
Run $\mathsf{sk}_C \leftarrow \mathsf{QFE.KeyGen}(\mathsf{msk}, U_{(C,a,b)})$.
Output sk_C.

$\mathsf{Enc}(\mathsf{mpk}, \rho_{\mathsf{m}} \in \mathcal{X}) \to \rho_{\mathsf{ct}}$
Compute $\rho_{\mathsf{ct}} \leftarrow \mathsf{QFE.Enc}(\mathsf{mpk}, (\rho_{\mathsf{m}} \otimes |0\rangle\langle 0|^{\otimes(n+2l+t+s)} \otimes |0\rangle\langle 0|))$
Output ρ_{ct}.

$\mathsf{Dec}(\mathsf{sk}_C, \rho_{\mathsf{ct}}) \to \rho_{\mathsf{m}}$ Run $\mathsf{QFE.Dec}(\mathsf{sk}_C, \rho_{\mathsf{ct}}) = \rho_{\mathsf{m}}$ and output ρ_{m}.

Theorem 7. *Any single-query QFE scheme for n-qubit messages and universal circuits (Definition 24) is a single-query unclonable-indistinguishable functional encryption scheme (Definition 26) if there exists an unclonable-indistinguishable encryption scheme with quantum decryption keys for single bit messages (Definition 18).*

Proof.

Correctness The scheme is correct based on the correctness of the underlying functional encryption scheme.

We show security by a series of Hybrids:

Hybrid 0: This is the unclonable functional encrpytion experiment $\mathsf{Exp}_{\mathcal{A}}^{QFE-UE-IND}$.

Hybrid 1: In this Hybrid we change how the challenge ciphertext is created, in particular we change the flag bit f to 1 such that the circuit executes the second case of it's description.

$\mathsf{Enc}^*(\mathsf{mpk}, \rho_{\mathsf{m}_0}, \rho_{\mathsf{m}_1})$:

1. Run $\mathsf{UEQ.KeyGen}(1^\lambda, r^*) = (\mathsf{ek}, |\mathsf{dk}_0\rangle)$. Produce another copy of the decryption key by using the same randomness $\mathsf{UEQ.KeyGen}(1^\lambda, r^*) = (\mathsf{ek}, |\mathsf{dk}_1\rangle)$.
2. Sample 2 sets of $l(\lambda)$ EPR pairs σ_0^{AB} and σ_1^{AB}. Let σ_0^A, σ_1^A denote registers containing the first qubit of each EPR pair and σ_0^B,σ_1^B denote registers containing the second qubit of each EPR pair respectively.
3. Sample $b \leftarrow \{0,1\}$.
4. Run $\rho_{UE} \leftarrow \mathsf{UEQ.Enc}(1^\lambda, b)$.
5. Create the ciphertext

$$\rho_{\mathsf{ct}} = \mathsf{QFE.Enc}(\mathsf{mpk}, (\rho_{\mathsf{m}_0} \otimes \rho_{\mathsf{m}_1} \otimes \sigma_0^A \otimes \sigma_0^B \otimes \rho_{UE} \otimes C_{Dec} \otimes |1\rangle\langle 1|))$$

6. Teleport the key $(0^\lambda \otimes |\mathsf{dk}_0\rangle)$,$(0^\lambda \otimes |\mathsf{dk}_1\rangle)$ through the EPR pairs σ_0^B, σ_1^B respectively and obtain the teleportation keys $(a'_0, b'_0), (a'_1, b'_1)$. Output $(\rho_{\mathsf{ct}}, (a'_0, b'_0), (a'_1, b'_1))$.

Claim. $|p_0 - p_1| \leq negl(\lambda)$ where p_0 is the winning probability of the adversary in Hybrid 0 and p_1 is the winning probability in Hybrid 1.

Proof. We show that an adversary $\mathcal{A} = (A, B, C)$ that can win in Hybrid 0 with a higher probability than in Hybrid 1 can be used to break IND-security of the underlying QFE scheme.

During the reduction both parties B and C will need to obtain independently sampled secret keys for the functional encryption scheme. Since our QFE scheme is only single-query secure we cannot allow the adversary to sample two secret keys. Instead we reduce to the notion of 2-player single-query IND-security which we define in Definition 30. This security notion allows two recipients of a ciphertext that don't further communicate to each receive a functional secret key from the single-query secure QFE scheme. We also show that this security notion is implied by single-query IND-secure QFE.

Let $\mathcal{A}^* = (A^*, B^*, C^*)$ be the adversary in the 2-player single-query non-adaptive IND-security game against the quantum functional encryption scheme. A^* receives the public key mpk from the experiment and runs A on input $(1^\lambda, \mathsf{mpk})$ until A outputs messages $\rho_{\mathsf{m}_0}, \rho_{\mathsf{m}_1}$. Sample $b \leftarrow \{0,1\}$.

To create the first challenge message $\rho_{\mathsf{m}_0^*}$ A^* performs the steps of the honest Enc algorithm without the creation of the QFE ciphertext. Then A^* sets

$$\rho_{\mathsf{m}_0^*} = (\rho_{\mathsf{m}_b} \otimes |0\rangle\langle 0|^{n(\lambda)} \otimes |0\rangle\langle 0|^{\otimes 2l(\lambda)+t(\lambda)+s(\lambda)} \otimes |0\rangle\langle 0|)$$

To create the challenge message $\rho_{\mathsf{m}_0^*}$ A^* performs encryption as defined in Enc^* without the creation of the ciphertext (step 5) but with the teleportation (step 6) to obtain teleportation keys $(a_0, b_0), (a_1, b_1)$. In step 4 use the bit b that was already sampled. Then the message $\rho_{\mathsf{m}_1^*}$ is defined as

$$\rho_{\mathsf{m}_1^*} = (\rho_{\mathsf{m}_0} \otimes \rho_{\mathsf{m}_1} \otimes \sigma_0^A \otimes \sigma_0^B \otimes \rho_{UE} \otimes C_{Dec} \otimes |1\rangle\langle 1|)$$

Note that $\mathcal{A}$ is not required to copy the messages ρ_{m_0} and ρ_{m_1} to define the challenge messages. According to the IND-security experiment $\mathcal{A}^*$ can define both messages by referring to a single

quantum state, this is a special case of Definition 25. $\mathcal{A}^*$ declares the messages $\rho_{\mathsf{m}_0^*}, \rho_{\mathsf{m}_1^*}$ and additionally outputs the circuit descriptions $\mathsf{sk}_{C_B} = U_{(C,a_0,b_0)}$ and $\mathsf{sk}_{C_C} = U_{(C,a_1,b_1)}$.

Both sk_{C_B} and sk_{C_C} are admissible function queries since

$$U_{(C,a_0,b_0)}(\rho_{\mathsf{m}_0^*}) = \rho_{\mathsf{m}_b} = U_{(C,a_0,b_0)}(\rho_{\mathsf{m}_1^*})$$

and

$$U_{(C,a_1,b_1)}(\rho_{\mathsf{m}_0^*}) = \rho_{\mathsf{m}_b} = U_{(C,a_1,b_1)}(\rho_{\mathsf{m}_1^*})$$

and $\mathcal{A}^*$ is no longer entangled with the input messages.

$\mathcal{A}^*$ receives the ciphertext ρ_{ct} and runs $\mathcal{A}$ to obtain ρ_{BC}.

Then B^* and C^* are activated with the state $(\rho_B, \mathsf{sk}_{C_B}, b)$ and $(\rho_C, \mathsf{sk}_{C_C}, b)$ respectively and each run B and C on input $(\rho_B, \mathsf{sk}_{C_B})$ and $(\rho_C, \mathsf{sk}_{C_C})$ respectively until they output a bit b_B, b_C.

A^*, B^*, C^* simulate Hybrid 0 if $\rho^*_{\mathsf{m}_0}$ is picked as challenge and they simulate Hybrid 1 if $\rho^*_{\mathsf{m}_1}$ is picked. Let $b^* \in \{0,1\}$ denote the choice of the challenge message.

B^* outputs $b^*_B = 0$ if $b_B = b$ otherwise B^* outputs $b^*_B = 1$, similarly C^* outputs $b^*_C = 0$ if $b_C = b$ and otherwise outputs $b^*_C = 1$.

This means that if $b_B = b_C = b$ we have $b^*_B = b^*_C = 0$. For Hybrid 1 we show in Lemma 4 that $b_B = b_C = b$ only occurs with negligible advantage.

The winning probability of $\mathcal{A}^*$ is

$$\begin{aligned}
&\frac{1}{2}(\Pr[b^*_B = b^*_C = 0 | b^* = 0] + \Pr[b^*_B = b^*_C = 1 | b^* = 1]) \\
&= \frac{1}{2}(\Pr[b_B = b_C = b | b, b^* = 0] + (\Pr[b_B \neq b \vee b_C \neq b | b, b^* = 1])) \\
&= \frac{1}{2}(\underbrace{\Pr[b_B = b_C = b | b, b^* = 0]}_{p_0} + (1 - \underbrace{\Pr[b_B = b_C = b | b, b^* = 1]}_{1/2 + negl(\lambda)})) \\
&= \frac{1}{2}(p_0 + 1/2 - negl(\lambda))
\end{aligned}$$

Therefore, if the advantage of $\mathcal{A}$ in Hybrid 0 is non-negligible $p_0 = \frac{1}{2} + non - negl(\lambda)$, $\mathcal{A}^*$ can break the 2-player IND-security of QFE with non-negligible advantage.

□

Lemma 4. *In Hybrid 1 the advantage of $\mathcal{A} = (A, B, C)$ is negligible if UEQ is secure.*

Proof. We show that an adversary that breaks the security of the unclonable functional encryption scheme breaks uncloneability of the underlying UEQ encryption scheme with quantum decryption keys with the same advantage.

Let $\mathcal{A} = (A, B, C)$ be an adversary that breaks the security of the unclonable functional encryption scheme. Then we can build an adversary $\mathcal{A}^* = (A^*, B^*, C^*)$ that breaks the security of the UEQ scheme. In the role of A^* send challenge messages $b_0 = 0, b_1 = 1$ to the experiment and obtain ρ_{UE}.

Create the setup for unclonable functional encryption $(\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^\lambda)$ and run A on input $(1^\lambda, \mathsf{mpk})$. Receive the challenge messages $\rho_{\mathsf{m}_0}, \rho_{\mathsf{m}_1}$ from A.

Build the ciphertext as in Hybrid 2: Sample 2 sets of n EPR pairs σ_0^{AB} and σ_1^{AB}. Let σ_0^A, σ_1^A denote registers containing the first qubit of each EPR pair and σ_0^B,σ_0^B denote registers containing the second qubit of each EPR pair respectively.

Create the ciphertext $\rho_{\mathsf{ct}} = \mathsf{QFE.Enc}(\mathsf{mpk}, (\rho_{\mathsf{m}_0} \otimes \rho_{\mathsf{m}_1} \otimes \sigma_0^A \otimes \sigma_0^B \otimes \rho_{UE} \otimes C_{Dec} \otimes |1\rangle\langle 1|))$ and send ρ_{ct} to A. If ρ_{UE} is an encryption of $b = 0$ then ρ_{ct} is an encryption of ρ_{m_0}, if ρ_{UE} is an encryption of $b = 1$ then ρ_{ct} is an encryption of ρ_{m_1}.

Additionally $\mathcal{A}$ outputs $\rho_{\mathsf{st}_B} = (\mathsf{msk}, \sigma_0^B)$ and $\rho_{\mathsf{st}_C} = (\mathsf{msk}, \sigma_1^B)$.

A performs the splitting channel and outputs a state ρ^{BC} which is also the state that A^* defines as it's result of the splitting channel. Now B^* and C^* are activated. They take as input the states $\rho^B, \rho_{\mathsf{st}_B}$ and $\rho^C, \rho_{\mathsf{st}_C}$ respectively and each receive a copy of the secret key $|\mathsf{dk}\rangle$ from the experiment.

B^* teleports the state $0^\lambda \otimes |\mathsf{dk}\rangle$ trough the EPR pairs σ_0^B and obtains the teleportation correction keys a_0, b_0.

He produces the secret key $\mathsf{dk}_B = \mathsf{QFE.KeyGen}(\mathsf{msk}, U_{(C,a_0,b_0)})$ where C is the identity circuit. He runs the adversary B on input ρ^B and the secret key dk_B and outputs whatever B^* outputs.

C^* does the same actions as B^* on his respective EPR pairs. He teleports the state $0^\lambda \otimes |\mathsf{dk}\rangle$ trough the EPR pairs σ_1^B and obtains the teleportation correction keys a_1, b_1.

He produces the secret key $\mathsf{dk}_C = \mathsf{QFE.KeyGen}(\mathsf{msk}, U_{(C,a_1,b_1)})$ where C is the identity circuit. He runs the adversary C on input ρ^C and the secret key dk_C and outputs whatever C^* outputs.

(A^*, B^*, C^*) wins with the same probability as (A, B, C). □

□

Lemma 5. *Any non-adaptive unclonable-indistinguishable functional encryption scheme is a public key unclonable-indistinguishable encryption scheme with variable decryption keys (Definition 20).*

Proof. Note that the key queries in the unclonable functional encryption experiment do not have to be admissible queries. In particular B and C can both obtain a secret key for the circuit that computes the identity even if $\rho_{\mathsf{m}_0}, \rho_{\mathsf{m}_1}$ are different messages. This defines decryption keys for an unclonable public-key encryption scheme. Security and correctness follow as a special case of the security and correctness of the unclonable functional encryption scheme. □

Corollary 2. *There exists a universal public-key unclonable-indisinguishable encryption scheme with variable decrpytion keys (Definition 20) for n-bit messages assuming a single-query QFE scheme (Definition 26) and assuming the existance of an unclonable-indistinguishable encryption scheme with quantum decryption keys for single bit messages (Definition 18).*

Remark 2. The techniques given in this section can be applied more generally. Assuming the existence of UE with a given level of security, any QFE scheme can be modified to achieve unclonable security at the same level, without explicitly using the original UE scheme. For example, instead of reducing to the security of UE with variable decryption keys we could reduce to an ideal UE scheme, i.e. an unclonable-indistinguishable encryption scheme with standard classical decryption keys and then also achieve this ideal security notion for the unclonable QFE scheme.

6 From Quantum Multi-input Functional Encryption to Quantum Indistinguishability Obfuscation

In this section we first define multi-input functional encryption in the quantum setting. Then, we show that multi-input quantum functional encryption implies quantum indistinguishability obfuscation. In the classical setting it is known that IND-secure multi-input functional encryption and qiO are equivalent, one notion can be constructed from the other [Gol+14]. An interesting open question that we do not address in this work is from what assumptions IND-secure quantum multi-input functional encryption could be constructed.

6.1 Definitions

In this section we are switching to a secret-key flavor of functional encryption. The adversary cannot create ciphertexts on its own but has to query the Enc functionality for this. First we establish the syntax of a quantum multi-input functional encryption scheme.

A quantum multi-input functional encryption scheme QMIFE for a family of circuits $\{\mathcal{C}_\lambda\}_{\lambda\in\mathbb{N}}$ with input space $\mathcal{X}_\lambda$ and output space $\mathcal{Y}_\lambda$ consists of four algorithms $(\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ as described below.

- **Setup** $\mathsf{Setup}(1^\lambda, n) \to (\mathsf{msk}, \mathsf{ek}_1, \ldots, \mathsf{ek}_n)$ is a QPT algorithm that takes as input the security parameter $\lambda \in \mathbb{N}$ and the number of input qubits $n \in \mathbb{N}$. It outputs n encryption keys $\mathsf{ek}_1, \ldots, \mathsf{ek}_n$ and a master secret key msk.
- **KeyGen** $\mathsf{KeyGen}(\mathsf{msk}, C) \to \mathsf{sk}_C$ is a QPT algorithm that takes as input the master secret key msk and a circuit $C \in \mathcal{C}_\lambda$ and outputs a corresponding secret key sk_C.
- **Enc** $\mathsf{Enc}(\mathsf{ek}, \rho_x) \to \rho_{\mathsf{ct}}$ is a QPT algorithm that takes as input an encryption key $\mathsf{ek}_i \in (\mathsf{ek}_1, \ldots, \mathsf{ek}_n)$ and an input message $\rho_x \in \mathcal{X}$ and outputs a ciphertext ρ_{ct}. In the case where all of the encryption keys ek_i are the same, we assume that each ciphertext ρ_{ct} has an associated label i to denote that the encrypted plaintext constitutes an i'th input the circuit $C \in \mathcal{C}_\lambda$. For convenience of notation, we omit the labels from the explicit description of the ciphertexts. It might also be useful to distinguish between classical and quantum input. Since any classical input can be embedded in a quantum state we do not explicitly differentiate between these two types of inputs here.
- **Dec** $\mathsf{Dec}(\mathsf{sk}_C, \rho_{\mathsf{ct}_1}, \ldots, \rho_{\mathsf{ct}_n}) \to \rho_y$ is a QPT algorithm that takes as input a secret key sk_C and n ciphertexts $\rho_{\mathsf{ct}_1}, \ldots, \rho_{\mathsf{ct}_n}$ and outputs a state $\rho_y \in \mathcal{Y}_\lambda$.

In the description of this syntax we only declared inputs, outputs and ciphertexts explicitly as quantum states but other parts of the scheme such as keys could also contain quantum data in a specific instantiation.

Indistinguishability Based Security The scheme is parameterized by k which denotes the number of ciphertexts the adversary is allowed to learn per secret key.

Admissible challenge messages are defined using the same concept as in Section 3.2 for the IND-security of simple functional encryption. We additionally have to take into account that the adversary can choose between different combinations of input ciphertexts to evaluate the circuit.

Definition 27. *(Admissible queries for QMIFE) Let Q be a set of circuits containing circuits $C \in \{C_\lambda\}_{\lambda\in\mathbb{N}}$ with input size n. The adversary in $\mathsf{Exp}_{\mathcal{A}}^{\mathrm{IND}-\mathsf{QMIFE}}$ specifies a challenge query by states ρ_{m^0}, ρ_{m^1} with the following structure: A state $\rho_{m^b_{h,j}}$ is defined by taking the partial trace of ρ_{m^b} indexed by $h \in [n], j \in [k]$:*

$$\rho_{m^b_{h,j}} = Tr_{(\bar{h},\bar{j})}[\rho_{m^b}]$$

The messages are grouped in vectors X^0, X^1 where $X^b = \{\rho^{EU}_{m^b_{1,j}}, \cdots, \rho^{EU}_{m^b_{n,j}}\}_{j\in[k]}$. For each challenge message indexed by $h \in [n], j \in [k], b \in \{0,1\}$ the adversary can specify a register E that will be used for encryption and a register U that will be returned unencrypted. The challenge messages corresponding to $1-b$ are not returned to the adversary.

Let $\rho^U_{m^b_{j^*}}$ be a state that groups together the registers not used for encryption, the state contains $\rho^U_{m^b_{h,j^*}}$ for all $h \in [n]$ and a specific choice of $j^* = (j_1, \ldots, j_n)$ with each $j_i \in [k]$.

We say (X^0, X^1) and Q are compatible if the following property is satisfied for all $C \in Q$ and for all choices of j^*:

$$TD\left(\sum_i p_i C(\rho^E_{\mathsf{m}^0_{1,j_1,i}},\cdots,\rho^E_{\mathsf{m}^0_{n,j_n,i}})\otimes\rho^U_{m^b_{j^*,i}}\otimes\rho_{A_i},\sum_i q_i C(\rho^E_{\mathsf{m}^1_{1,j_1,i}},\cdots,\rho^E_{\mathsf{m}^1_{n,j_n,i}})\otimes\rho^U_{m^b_{j^*,i}}\otimes\rho_{A_i}\right)\leq negl(\lambda)$$

where ρ_A is the local state of the adversary.

Definition 28. *(Quantum MIFE IND-Security)*
Let $\mathsf{QMIFE}=(\mathsf{Setup},\mathsf{KeyGen},\mathsf{Enc},\mathsf{Dec})$ *be a quantum multi-input functional encrpytion scheme for a circuit family* $\{C_\lambda\}_{\lambda\in\mathbb{N}}$ *and let* $\mathcal{A}=(\mathcal{A}_1,\mathcal{A}_2)$ *be a QPT adversary.*

$$\begin{aligned}
&\mathsf{Exp}^{\mathrm{IND}-\mathsf{QMIFE}}_{\mathcal{A}}(1^\lambda):\\
&(\mathsf{ek},\mathsf{msk})\leftarrow\mathsf{Setup}(1^\lambda,n)\\
&(\boldsymbol{X}^0,\boldsymbol{X}^1,\rho_{\mathsf{st}_1})\leftarrow\mathcal{A}_1^{\mathsf{KeyGen}(\mathsf{msk},\cdot)}(1^\lambda,n)\ \text{ where }\boldsymbol{X}^\ell=\left\{\rho^\ell_{\mathsf{m}_{1,j}},\ldots,\rho^\ell_{\mathsf{m}_{n,j}}\right\}_{j\in[k]}\\
&b\leftarrow\{0,1\}\\
&\mathsf{ct}_{i,j}\leftarrow\mathsf{Enc}\left(\mathrm{ek}_i,\rho^b_{\mathsf{m}_{i,j}}\right)\forall i\in[n],j\in[k]\\
&b'\leftarrow\mathcal{A}_2^{O(\cdot)}\left(\rho_{\mathsf{st}_1},\{\rho_{\mathsf{ct}_{i,j}}\}_{i\in[n],j\in[k]}\right)\\
&\textit{Output: }(b=b')
\end{aligned}$$

Let Q denote the entire set of key queries made by $\mathcal{A}$. Then, the challenge message vectors $\boldsymbol{X}_0$ and $\boldsymbol{X}_1$ chosen by $\mathcal{A}_1$ must be compatible with Q (Definition 27). The scheme is k-IND-secure if for every QPT adversary $\mathcal{A}=(\mathcal{A}_1,\mathcal{A}_2)$, the advantage of $\mathcal{A}$ defined as

$$\mathrm{Adv}^{\mathsf{QMIFE},\mathrm{IND}}_{\mathcal{A}}(1^\lambda)=\left|\Pr\left[\mathsf{Exp}^{\mathrm{IND}-\mathsf{QMIFE}}_{\mathcal{A}}(1^\lambda)=1\right]-\frac{1}{2}\right|\leq negl(\lambda)$$

Adaptive vs. Non-adaptive security

- *The scheme is called non-adaptively secure if the the adversary only queries the* KeyGen *oracle before receiving a ciphertext. Then the oracle $O(\cdot)$ is the empty oracle.*
- *The scheme is called adaptively secure if the adversary can either query the KeyGen oracle before or after receiving the ciphertext. Then the oracle $O(\cdot)$ is the function* $\mathsf{KeyGen}(\mathsf{msk},\cdot)$.

Simulation Security In the simulation security setting we need to give the simulator access to the output of the circuit evaluated on any combination of inputs. In the classical setting this is simple: There is a trusted part which holds the input messages $\boldsymbol{X}=\{\mathsf{m}_{1,j},\ldots,\mathsf{m}_{n,j}\}_{j\in[k]}$ and the simulator can specify a queries of the form $(g,j_1,\ldots,j_n)$ where g is a function and j_1 to j_n are indices selecting the input for the function. The simulator can make multiple queries using an arbitrary combination of indices and any function that the adversary requested keys for.

In the quantum setting we run into the issue that the inputs which are quantum states cannot be reused arbitrarily. On the other hand for some functionalities it might be possible or even desired that after obtaining one output the state of the input ciphertext can be restored by uncomputing the decryption unitary. Then the inputs can be reused to evaluate the same or a different functionality on a combination of input ciphertexts.

In the quantum setting a standard way of modelling quantum access to a oracle is the following. The user specifies a query $|\phi\rangle=\sum_i\alpha_i|x_i\rangle|u_i\rangle$ and the oracle answers with the state $|\phi'\rangle=\sum_i\alpha_i|x_i\rangle|u_i\oplus f(x_i)\rangle$. This state is computed by first applying f to the x register, xoring

the result to the u register and uncomputing the function on the x register. We can use the same concept to define how the trusted party answers queries with the difference that the trusted party already holds the input register. This allows the trusted party to reuse the input messages and answer multiple queries of the form $(g, \sum \alpha_l |j_{1,l} \otimes \ldots \otimes j_{n,l}\rangle)$. It is to be noted though that this causes the answer register to be entangled with the input register. Therefore a measurement by the simulator will also collapse the input state and multiple evaluations are not guaranteed to work correctly.

Definition 29. *(Quantum MIFE SIM-Security) A multi-input functional encryption scheme for a circuit family $\{C_\lambda\}_{\lambda\in\mathbb{N}}$ is k-SIM-secure if for every QPT adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ there exists a stateful simulator Sim such that the outputs of the following experiments are computationally indistinguishable:*

$\mathsf{Exp}^{Real}_{\mathcal{A}}(1^\lambda)$	$\mathsf{Exp}^{Ideal}_{\mathcal{A}}(1^\lambda)$
$(\{\mathsf{ek}_i\}_{i\in[n]}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^\lambda, n)$	
$(X, \mathsf{st}) \leftarrow \mathcal{A}_1^{\mathsf{KeyGen}(\cdot)}(1^\lambda, n)$	$(X, \mathsf{st}) \leftarrow \mathcal{A}_1^{O_1(\cdot)}(1^\lambda, n)$
where $X = \{\rho_{\mathsf{m}_{1,j}}, \ldots, \rho_{\mathsf{m}_{n,j}}\}_{j\in[k]}$	where $X = \{\rho_{\mathsf{m}_{1,j}}, \ldots, \rho_{\mathsf{m}_{n,j}}\}_{j\in[k]}$
$\rho_{\mathsf{ct}_{i,j}} \leftarrow \mathsf{Enc}(\mathsf{ek}_i, \rho_{\mathsf{m}_{i,j}}) \forall i \in [n], j \in [k]$	$\{\rho_{\mathsf{ct}_{i,j}}\}_{i,j} \leftarrow \mathsf{Sim}^{\mathsf{TP}(\cdot)}(1^\lambda, 1^{\lvert C\rvert}, \{1^{\lvert\rho_{\mathsf{m}_{i,j}}\rvert}\}_{i\in[n],j\in[k]})$
$\alpha \leftarrow \mathcal{A}_2^{O'_2(\cdot)}(\{\rho_{\mathsf{ct}_{i,j}}\}_{i\in[n],j\in[k]}, \mathsf{st})$	$\alpha \leftarrow \mathcal{A}_2^{O_2(\cdot)}(\{\rho_{\mathsf{ct}_{i,j}}\}_{i\in[n],j\in[k]}, \mathsf{st})$
The experiment outputs α	The experiment outputs α

where the oracle $\mathsf{TP}(\cdot)$ denotes the ideal world trusted party. It accepts queries of the form $(g, \sum \alpha_l |j_{1,l} \otimes \ldots \otimes j_{n,l}\rangle)$ and computes

$$\sum \alpha_l |j_{1,l}, \cdots, j_{n,l}\rangle \otimes \rho_{\mathsf{m}} \otimes g(\rho_{\mathsf{m}_{1,j_{1,l}}}, \ldots, \rho_{\mathsf{m}_{n,j_{n,l}}})$$

The message register ρ_{m} is kept by TP and used for future queries, the rest is returned to the simulator.

The oracle $O_1(\cdot)$ is a KeyGen oracle controlled by the simulator and the oracle $O_2(\cdot)$ is a KeyGen oracle controlled by the simulator with access to the trusted party TP. A simulator is admissible if it only queries the trusted party on functionalities that $\mathcal{A}$ queried to its oracle.

Remark 3. In this definition we have for the first time in this work considered the case of multiple function queries. We remark that defining a multi-query QFE scheme for only a single ciphertext runs into the same issues we described above. Given multiple function keys a single ciphertext has the possibility to be evaluated to different outputs but physically not all these evaluations might be possible. Therefore a solution as presented here for the multi-input case is necessary and a definition for a multi-query simulation secure QFE scheme can be derived from this definition by restricting the input to a single message $n = 1$.

6.2 IND-secure QMIFE implies qiO

Theorem 8. *A QMIFE scheme that fullfills non-adaptive single-query 2-IND-security unconditionally implies quantum indistinguishability obfuscation.*

Proof. Let QMIFE be a quantum multi input functional encryption scheme. We define an obfuscation scheme $(\mathsf{Obf}, \mathsf{Eval})$ for a familiy of circuits $\{C_\lambda\}_{\lambda\in\mathbb{N}}$ that take as input n qubits and are described by a classical string of length l.

$\mathsf{Obf}(C)$:

- Run $\mathsf{QMIFE.Setup}(1^\lambda, n') \to (\mathsf{msk}, \mathsf{ek}_1, \ldots, \mathsf{ek}_{n'})$ where $n' = 3n + l$
- Run $\mathsf{QMIFE.KeyGen}(U, \mathsf{msk}) \to sk_U$ where U is a variant of a universal circuit that computes $U(C, \rho_1, \cdots, \rho_n, a_1, b_1, \ldots, a_n, b_n) = C(X^{a_1} Z^{b_1} \rho_1, \cdots, X^{a_n} Z^{a_n} \rho_n)$
- Create n ciphertexts that encrypt the bit $b = 0$ and n ciphertexts that encrypt $b = 1$:

$$\forall i \in [2n], b \in \{0, 1\} : \mathsf{ct}_i^b \leftarrow \mathsf{QMIFE.Enc}(\mathsf{ek}_i, b)$$

- Create n EPR pairs and take the first qubit of each EPR pair $\rho_e = (\rho_{e_1}, \rho_{e_2})$ and encrypt it:

$$\forall i \in [n] : \rho_{ct_{2n+i}} \leftarrow \mathsf{QMIFE.Enc}(\mathsf{ek}_{2n+i}, \rho_{e_{i,1}})$$

.

- Encrypt the circuit C:

$$\mathsf{ct}_C \leftarrow \mathsf{QMIFE.Enc}(\mathsf{ek}_{3n+1}, C)$$

- Output $\tilde{C} = (\mathsf{sk}_U, \mathsf{ct}_C, \{\mathsf{ct}_i^b\}_{i \in [n], b \in \{0,1\}}, \{\rho_{\mathsf{ct}_i}\}_{i \in [n]}, \{\rho_{e_{i,2}}\}_{i \in [n]})$

$\mathsf{Eval}(\tilde{C}, \rho_x)$

- Teleport the state ρ_x which is of size n trough the EPR pairs $\rho_{e_{1,2}} \otimes \cdots \otimes \rho_{e_{n,2}}$ and obtain $((a_1, b_1), \cdots, (a_n, b_n))$ as teleportation keys.
- Select the remaining ciphertexts such that they are encryptions of (a_i, b_i): $\forall i \in [n]$ select $\mathsf{ct}_i^{a_i}$ and $\mathsf{ct}_{i+1}^{b_i}$.
- Run $\mathsf{QMIFE.Dec}(\mathsf{sk}_U, \mathsf{ct}_C, \rho_{\mathsf{ct}_1}, \ldots, \rho_{\mathsf{ct}_n}, \mathsf{ct}_1^{a_1}, \mathsf{ct}_2^{b_1}, \cdots, \mathsf{ct}_{2n-1}^{a_n}, \mathsf{ct}_{2n}^{b_n}) = \rho_y$

First we analyse the correctness of the scheme. By correctness of the QMIFE scheme and correctness of the teleportation gadgets the scheme outputs the correct evaluation.

$$\begin{aligned}
&\mathsf{QMIFE.Dec}(\mathsf{sk}_U, \mathsf{ct}_C, \rho_{\mathsf{ct}_1}, \ldots, \rho_{\mathsf{ct}_n}, \mathsf{ct}_1^{a_1}, \mathsf{ct}_2^{b_1}, \cdots, \mathsf{ct}_{2n-1}^{a_n}, \mathsf{ct}_{2n}^{b_n}) \\
&= U(C, \rho_1, \cdots, \rho_n, a_1, b_1, \ldots, a_n, b_n) \\
&= C(X^{a_1} Z^{b_1} \rho_1, \cdots, X^{a_n} Z^{a_n} \rho_n) \\
&= C(\rho_{x_1}, \ldots, \rho_{x_n})
\end{aligned}$$

We note that a honest user will only be guaranteed one use of the obfuscated program since the teleportation ciphertexts are consumed during this operation. If the quantum circuit belongs to a class of circuits that only take classical inputs we can avoid the use of the teleportation helper state and the scheme can be redefined to let the user select it's classical inputs in the same manner as the bits (a_i, b_i) are selected here. This will still not guarantee a reusable qiO scheme since the obfuscated circuit itself might be a quantum state that collapses during evaluation.

No we show that the security of the qiO scheme can be reduced to the security of the underlying QMIFE scheme. Let $\mathcal{A}$ be an adversary that wins the qiO experiment with non-negligible advantage. Then we can construct an adversary $\mathcal{B}$ that wins the QMIFE IND-security experiment with non-negligible advantage.

$\mathcal{B}$ receives 1^λ and runs $\mathcal{A}$ on input 1^λ until $\mathcal{A}$ outputs (C_0, C_1). $\mathcal{B}$ queries the KeyGen oracle on the function U as defined above and receives the secret key sk_U.

$\mathcal{B}$ constructs it's challenge vectors as follows: Sample n EPR pairs $\rho_{e_i} = \frac{1}{\sqrt{2}}(|0\rangle^1|0\rangle^2 \otimes |1\rangle^1|1\rangle^2) = (\rho_{e_{i,1}}, \rho_{e_{i,2}})$ and put the first qubit each in the challenge vector X^0 and put the second qubit each in the 'do not encrypt' part of the challenge query. $X^0 = (C_0, \rho_{e_{1,1}^0}, \cdots, \rho_{e_{n,1}^0}, \{a_{i,1} = 0, a_{i,2} = 1, b_{i,1} = 0, b_{i,2} = 1\}_{i \in [n]})$ Sample n additional EPR pairs and put the first qubit each in the challenge vector X^1 and put the second qubit each in the 'do not encrypt' part of the challenge query.

$X^1 = (C_1, \rho_{e^1_{1,1}}, \cdots, \rho_{e^1_{n,1}}, \{a_{i,1} = 0, a_{i,2} = 1, b_{i,1} = 0, b_{i,2} = 1\}_{i\in[n]})$. Let $\rho^U_{X^b} = \rho_{e^b_{1,2}} \otimes \cdots \otimes \rho_{e^b_{n,2}}$ for each $b \in \{0, 1\}$.

The experiment sends $(\mathsf{ct}_C, \{\rho_{\mathsf{ct}_i}\}_{i\in[n]}, \{\mathsf{ct}^d_i\}_{i\in[n],d\in\{0,1\}}, \{\rho_{e_{i,2}}\}_{i\in[n]})$ where ct_C is the encryption of C_b, $\{\rho_{\mathsf{ct}_i}\}_{i\in[n]}$ are the encryptions of the EPR pair halves, $\{\mathsf{ct}^d_i\}_{i\in[2n],d\in\{a,b\}}$ are the encryptions of a_i, b_i and the unencrypted second halves of the EPR pairs $\{\rho_{e_{i,2}}\}_{i\in[n]}$ to $\mathcal{B}$.

No we need to verify that the query (U, X^0, X^1) forms an admissible query for the QMIFE IND-experiment according to Definition 27. The challenge vectors X^1, X^0 only differ in the first component which contains C_b. Let the state $\rho_{X^0,ab}$ and $\rho_{X^1,ab}$ denote the state containing the classical bit queries of each challenge vector. Then for the inputs to $U(C_0, \cdot), U(C_1, \cdot)$ it holds that

$$\mathrm{TD}\left(\underbrace{\rho_{e^0_{1,1}} \otimes \cdots \otimes \rho_{e^0_{n,1}}}_{\rho_{X^0,e}} \otimes \rho_{X^0,ab}, \underbrace{\rho_{e^1_{1,1}} \otimes \cdots \otimes \rho_{e^1_{n,1}}}_{\rho_{X^1,e}} \otimes \rho_{X^1,ab}\right) = 0$$

$\mathcal{B}$ does not need to keep any information other than the secret key in it's local state ρ_B, in particular $\mathcal{B}$ is not entangled with any part of the challenge query (the remaining halves of the EPR pairs of the challenge query are given away to the experiment and returned without encryption per the definition of admissible queries). Let these qubits be contained in the registers $\rho^U_{X^0}$ and $\rho^U_{X^1}$ respectively.

$$\mathrm{TD}\left(\sum_i \rho_{X^0,e,i} \otimes \rho_{X^0,ab} \otimes \rho^U_{X^0,i} \otimes \rho_B, \sum_i \rho_{X^1,e,i} \otimes \rho_{X^1,ab} \otimes \rho^U_{X^1,i} \otimes \rho_B\right) = 0$$

By the requirement of the qiO IND-experiment the circuits C_0, C_1 are perfectly functionally equivalent. The circuits $U(C_0, \cdot), U(C_1, \cdot)$ inherit this property.

Then,

$$\mathrm{TD}\left(\sum_i U(C_0, \rho_{X^0,e,i}, \rho_{X^0,ab}) \otimes \rho^U_{X^0,i} \otimes \rho_B, \sum_i U(C_1, \rho_{X^1,e,i}, \rho_{X^1,ab}) \otimes \rho^U_{X^1,i}, \rho_B\right) = 0$$

which means the query (U, X^0, X^1) forms an admissible query for the QMIFE IND-experiment.

$\mathcal{B}$ sends the obfuscated circuit $\tilde{C}_b = (\mathsf{sk}_U, \mathsf{ct}_C, \{\mathsf{ct}^d_i\}_{i\in[2n],d\in\{a,b\}}, \{\rho_{\mathsf{ct}_i}\}_{i\in[n]}, \{\rho_{e_{i,2}}\}_{i\in[n]})$ to $\mathcal{A}$. $\mathcal{B}$ outputs whatever $\mathcal{A}$ outputs. If the QMIFE IND-experiment selected X^0 as a challenge it perfectly simulates an obfuscation of C_0 if the QMIFE IND-experiment selected X^1 as a challenge it perfectly simulates an obfuscation of C_1. Therefore $\mathcal{B}$ wins with the same probability as $\mathcal{A}$.

□

6.3 SIM-secure QMIFE implies QVBB

In this section we show that a simulation-secure QMIFE implies QVBB, even if we cannot hope to achieve such a construction. It is known that quantum virtual black box obfuscation is impossible to achieve for general circuits [AF16], therefore, impossibility of QMIFE immediately follows.

Theorem 9. *A QMIFE scheme that fulfills non-adaptive single-query 2-SIM-security unconditionally implies virtual black box quantum obfuscation.*

Proof. The same construction as in the previous proof of Theorem 8 implies QVBB if the QMIFE scheme is 2-SIM secure.

For any adversary $\mathcal{A}(1^\lambda)$ we define a simulator $\mathsf{Sim}(1^\lambda)$ for the scheme as follows. Let $\widetilde{\mathsf{Sim}}(1^\lambda)$ be the simulator for the QMIFE scheme. Then Sim creates n EPR pairs as required by the construction and runs the simulator $\widetilde{\mathsf{Sim}}$ to create the remaining parts of the obfuscated circuit, i.e.

the ciphertexts and the key for the universal circuit pairs as defined in Theorem 8. Upon receiving a query from $\widetilde{\mathsf{Sim}}$ the simulator forwards the query to its own oracle. Indistinguishability follows from the security of the QMIFE scheme. □

References

[Aar09] S. Aaronson. "Quantum Copy-Protection and Quantum Money". In: *2009 24th Annual IEEE Conference on Computational Complexity* (2009).

[AC12] S. Aaronson and P. Christiano. "Quantum money from hidden subspaces". In: *44th Annual ACM Symposium on Theory of Computing*. DOI: 10.1145/2213977.2213983.

[AF16] G. Alagic and B. Fefferman. "On quantum obfuscation". In: *arXiv preprint arXiv:1602.01771* (2016).

[Agr+13] S. Agrawal, S. Gorbunov, V. Vaikuntanathan, and H. Wee. "Functional Encryption: New Perspectives and Lower Bounds". In: *Advances in Cryptology – CRYPTO 2013*.

[AJ15] P. Ananth and A. Jain. "Indistinguishability Obfuscation from Compact Functional Encryption". In: *Advances in Cryptology – CRYPTO 2015, Part I*. DOI: 10.1007/978-3-662-47989-6_15.

[AJS15] P. Ananth, A. Jain, and A. Sahai. "Indistinguishability obfuscation from functional encryption for simple functions". In: *Cryptology ePrint Archive* (2015).

[AK21] P. Ananth and F. Kaleoglu. "Unclonable Encryption, Revisited". In: *TCC 2021: 19th Theory of Cryptography Conference, Part I*. DOI: 10.1007/978-3-030-90459-3_11.

[AKY24] P. Ananth, F. Kaleoglu, and H. Yuen. "Simultaneous Haar Indistinguishability with Applications to Unclonable Cryptography". In: *arXiv preprint arXiv:2405.10274* (2024).

[Ala+21] G. Alagic, Z. Brakerski, Y. Dulek, and C. Schaffner. "Impossibility of Quantum Virtual Black-Box Obfuscation of Classical Circuits". In: *Advances in Cryptology – CRYPTO 2021, Part I*. DOI: 10.1007/978-3-030-84242-0_18.

[Amb+00] A. Ambainis, M. Mosca, A. Tapp, and R. Wolf. "Private Quantum Channels." In: DOI: 10.1109/SFCS.2000.892142.

[Ana+22] P. Ananth, F. Kaleoglu, X. Li, Q. Liu, and M. Zhandry. "On the Feasibility of Unclonable Encryption, and More". In: *Advances in Cryptology – CRYPTO 2022, Part II*. DOI: 10.1007/978-3-031-15979-4_8.

[Bar+23] J. Bartusek, F. Kitagawa, R. Nishimaki, and T. Yamakawa. "Obfuscation of Pseudo-Deterministic Quantum Circuits". In: *55th Annual ACM Symposium on Theory of Computing*. DOI: 10.1145/3564246.3585179.

[BBV24] J. Bartusek, Z. Brakerski, and V. Vaikuntanathan. "Quantum State Obfuscation from Classical Oracles". In: *Proceedings of the 56th Annual ACM Symposium on Theory of Computing*. DOI: 10.1145/3618260.3649673.

[BC23] A. Broadbent and E. Culf. *Uncloneable Cryptographic Primitives with Interaction*. In: (2023). arXiv: 2303.00048 [quant-ph].

[Ben+93] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters. "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels". In: *Phys. Rev. Lett.* 70 (13 1993). DOI: 10.1103/PhysRevLett.70.1895.

[BK21] A. Broadbent and R. A. Kazmi. "Constructions for Quantum Indistinguishability Obfuscation". In: *Progress in Cryptology - LATINCRYPT 2021: 7th International Conference on Cryptology and Information Security in Latin America*. DOI: 10.1007/978-3-030-88238-9_2.

[BL20] A. Broadbent and S. Lord. "Uncloneable Quantum Encryption via Oracles". In: *tqc2020*. DOI: 10.4230/LIPIcs.TQC.2020.4.

[BM22] J. Bartusek and G. Malavolta. "Indistinguishability Obfuscation of Null Quantum Circuits and Applications". In: *13th Innovations in Theoretical Computer Science Conference (ITCS 2022)*. DOI: 10.4230/LIPIcs.ITCS.2022.15.

[Bro+21] A. Broadbent, S. Jeffery, S. Lord, S. Podder, and A. Sundaram. "Secure Software Leasing Without Assumptions". In: *TCC 2021: 19th Theory of Cryptography Conference, Part I*. DOI: 10.1007/978-3-030-90459-3_4.

[BSW11] D. Boneh, A. Sahai, and B. Waters. "Functional Encryption: Definitions and Challenges". In: *TCC 2011: 8th Theory of Cryptography Conference*. DOI: 10.1007/978-3-642-19571-6_16.

[BV15] N. Bitansky and V. Vaikuntanathan. "Indistinguishability Obfuscation from Functional Encryption". In: *56th Annual Symposium on Foundations of Computer Science*. DOI: 10.1109/FOCS.2015.20.

[BY22] Z. Brakerski and H. Yuen. "Quantum garbled circuits". In: *Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing*.

[ÇG23] A. Çakan and V. Goyal. "Unclonable cryptography with unbounded collusions". In: *Cryptology ePrint Archive* (2023).

[CG24] A. Coladangelo and S. Gunn. "How to Use Quantum Indistinguishability Obfuscation". In: *Proceedings of the 56th Annual ACM Symposium on Theory of Computing*. DOI: 10.1145/3618260.3649779.

[CMP24] A. Coladangelo, C. Majenz, and A. Poremba. "Quantum copy-protection of compute-and-compare programs in the quantum random oracle model". In: *Quantum* 8 (2024). DOI: 10.22331/q-2024-05-02-1330.

[Gar+16] S. Garg, C. Gentry, S. Halevi, M. Raykova, A. Sahai, and B. Waters. "Candidate indistinguishability obfuscation and functional encryption for all circuits". In: *SIAM Journal on Computing* 45.3 (2016).

[Gol+13] S. Goldwasser, Y. T. Kalai, R. A. Popa, V. Vaikuntanathan, and N. Zeldovich. "Reusable garbled circuits and succinct functional encryption". In: *45th Annual ACM Symposium on Theory of Computing*. DOI: 10.1145/2488608.2488678.

[Gol+14] S. Goldwasser et al. "Multi-input Functional Encryption". In: *Advances in Cryptology – EUROCRYPT 2014* (2014).

[Got03] D. Gottesman. "Uncloneable encryption". In: *Quantum Info. Comput.* 3.6 (2003).

[Gri19] A. B. Grilo. "A Simple Protocol for Verifiable Delegation of Quantum Computation in One Round". In: *icalp2019*. DOI: 10.4230/LIPIcs.ICALP.2019.28.

[GVW12] S. Gorbunov, V. Vaikuntanathan, and H. Wee. "Functional Encryption with Bounded Collusions via Multi-party Computation". In: *Advances in Cryptology – CRYPTO 2012*. DOI: 10.1007/978-3-642-32009-5_11.

[Hir+23] T. Hiroka, F. Kitagawa, R. Nishimaki, and T. Yamakawa. "Robust Combiners and Universal Constructions for Quantum Cryptography". In: (2023). arXiv: 2311.09487 [quant-ph].

[Hir+24] T. Hiroka, F. Kitagawa, T. Morimae, R. Nishimaki, T. Pal, and T. Yamakawa. "Certified Everlasting Secure Collusion-Resistant Functional Encryption, and More". In: *Advances in Cryptology – EUROCRYPT 2024*.

[KN22] F. Kitagawa and R. Nishimaki. "Functional Encryption with Secure Key Leasing". In: *Advances in Cryptology – ASIACRYPT 2022, Part IV*. DOI: 10.1007/978-3-031-22972-5_20.

[KT22] S. Kundu and E. Y.-Z. Tan. "Device-independent uncloneable encryption". In: *arXiv preprint arXiv:2210.01058* (2022).

[O'N10] A. O'Neill. "Definitional Issues in Functional Encryption." In: *IACR Cryptology ePrint Archive* 2010 (2010).

[RUV13] B. W. Reichardt, F. Unger, and U. Vazirani. "Classical command of quantum systems". In: 496 (2013). DOI: 10.1038/nature12035.

[SS10] A. Sahai and H. Seyalioglu. "Worry-free encryption: functional encryption with public keys". In: *ACM CCS 2010: 17th Conference on Computer and Communications Security*. DOI: 10.1145/1866307.1866359.

[Wie83] S. Wiesner. "Conjugate Coding". In: *SIGACT News* 15.1 (1983). DOI: 10.1145/1008908.1008920.

[WW23] B. Waters and D. Wichs. "Universal Amplification of KDM Security: From 1-Key Circular to Multi-Key KDM". In: *Advances in Cryptology – CRYPTO 2023, Part II*. DOI: 10.1007/978-3-031-38545-2_22.

A Additional Definitions and their Relations

A.1 Multi-Message Simulation-Secure QFE

In Definition 23 the adversary only chooses a single message. We can adjust the experiment to allow the adversary to choose multiple messages, where each message is a quantum state of dimension d. In the Real world the experiment is adjusted as follows:

$$\begin{aligned}&(\rho_{\mathsf{m}_1},\dots,\rho_{\mathsf{m}_n},st)\leftarrow\mathcal{A}^{O_1(\cdot)}(\mathsf{mpk})\\&(\rho_{\mathsf{ct}_i})\leftarrow\mathsf{Enc}(\mathsf{mpk},\rho_{\mathsf{m}_i})\quad\text{for all } i\in[n]\end{aligned}$$

In the Ideal world the experiment is adjusted as follows:

$$\begin{aligned}&(\rho_{\mathsf{m}_1},\dots,\rho_{\mathsf{m}_n},st)\leftarrow\mathcal{A}^{O_1(\cdot)}(\mathsf{mpk})\\&(\rho_{\mathsf{ct}_1},\dots,\rho_{\mathsf{ct}_n})\leftarrow\mathsf{Sim}(1^\lambda,\mathsf{mpk},\mathcal{V})\quad\text{for all } i\in[n]\\&\quad\text{where } \mathcal{V}=(C_f,\mathsf{sk}_f,C_f(\rho_{\mathsf{m}_1}),\dots,C_f(\rho_{\mathsf{m}_n}),1^d)\end{aligned}$$

In the classical world it is known that a non-adaptive single-message secure scheme is also secure for multiple messages. In the adaptive setting this is not the case [GVW12]. We show that the implication from single-message schemes to multi-message schemes in the non-adaptive setting also holds for QFE schemes. To show this we need the function secret key of the QFE scheme to be classical which is true for our scheme but might not be a requirement for every realisation of QFE.

Lemma 6. *A non-adaptive single-query simulation-secure QFE scheme with classical secret keys is also a non-adaptive single-query multi-message simulation secure QFE scheme.*

Proof. Let $(\mathsf{Setup},\mathsf{KeyGen},\mathsf{Enc},\mathsf{Dec})$ be a non-adaptive single-query simulation-secure QFE scheme with simulator Sim. Then we can construct the following simulator Sim^* for the multi-message scheme:

1. Obtain $\mathcal{V}=(C_f,\mathsf{sk}_f,C_f(\rho_{\mathsf{m}_1}),\dots,C_f(\rho_{\mathsf{m}_n}),1^{|\rho_{\mathsf{m}_n}|})$ from the experiment.
2. For every $i\in[n]$ invoke the single message simulator:

$$\rho_{\mathsf{ct}_i}\leftarrow\mathsf{Sim}(1^\lambda,\mathsf{mpk},\{C_f,sk_f,C_f(\rho_{\mathsf{m}_i})\})$$

3. output $(\rho_{\mathsf{ct}_1},\cdots,\rho_{\mathsf{ct}_n})$

Let $\mathcal{A}$ be an adversary that succeeds in distinguishing the Real and Ideal world in the multi-message experiment. Then there is an adversary $\mathcal{A}^*$ that can distinguish Real and Ideal world of the single-message experiment. In the following way a Hybrid experiment is defined for each $i \in [n]$. $\mathcal{A}^*$ receives mpk and forwards it to $\mathcal{A}$. When $\mathcal{A}$ makes a key query C_f $\mathcal{A}^*$ forwards the query to it's KeyGen oracle and receives sk_f which it forwards to $\mathcal{A}$. When $\mathcal{A}$ outputs $(\rho_{\mathsf{m}_1}, \ldots, \rho_{\mathsf{m}_n})$ $\mathcal{A}^*$ encrypts messages 1 to $i-1$ honestly and forwards ρ_{m_i} to it's own experiment and receives ρ_{ct_i}. Messages $i+1$ to n are encrypted using the simulator Sim. $\mathcal{A}^*$ send $(\rho_{\mathsf{ct}_1}, \ldots, \rho_{\mathsf{ct}_n})$ to $\mathcal{A}$ and outputs whatever $\mathcal{A}$ outputs. Indistinguishability between Hybrids i and $i+1$ follows from the security of the single-message QFE scheme. □

Corollary 3. *The schemes in Section 4.1 and Section 4.2 are non-adaptive single-query multi-message simulation-secure QFE schemes.*

A.2 2-Player Security of QFE

In this Lemma we show that a single-query secure QFE scheme is still secure if two non-communicating parties each obtain a function secret key. In this definition we consider that a single ciphertext must be split between the two non-communicating parties. A slightly different notion of security where both B and C obtain their own copy of the ciphertext would also be implied by a QFE scheme.

Definition 30 (Non-Adaptive 2-player Single-Query IND-Security for QFE).
Let λ be the security parameter and let $\mathcal{A} = (A, B, C)$ be a QPT adversary.

$$
\begin{aligned}
&\mathsf{Exp}^{2P-IND}_{\mathcal{A},b}(1^\lambda)\\
&(\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^\lambda)\\
&(\rho_{\mathsf{m}_0}, \rho_{\mathsf{m}_1}, \rho_{\mathsf{st}_A}, \rho_{\mathsf{st}_B}, \rho_{\mathsf{st}_C}, C_B, C_C) \leftarrow A(\mathsf{mpk})\\
&\rho_{\mathsf{ct}} \leftarrow \mathsf{Enc}(\mathsf{mpk}, \rho_{\mathsf{m}_b})\\
&\rho_{BC} \leftarrow A(\rho_{\mathsf{st}_A}, \rho_{\mathsf{ct}})\\
&\mathsf{sk}_{C_B} \leftarrow \mathsf{KeyGen}(\mathsf{msk}, C_B), \mathsf{sk}_{C_C} \leftarrow \mathsf{KeyGen}(\mathsf{msk}, C_C)\\
&b_B \leftarrow B(\mathsf{mpk}, \rho_{\mathsf{ct}}, \rho_{\mathsf{st}_B}, \mathsf{sk}_{C_B})\\
&b_C \leftarrow C(\mathsf{mpk}, \rho_{\mathsf{ct}}, \rho_{\mathsf{st}_C}, \mathsf{sk}_{C_C})
\end{aligned}
$$

The FE scheme is called secure if for any adversary $\mathcal{A} = (A, B, C)$ where $(\rho_{\mathsf{m}_0}, \rho_{\mathsf{m}_1}, C_B, \rho_{\mathsf{st}_B})$ and $(\rho_{\mathsf{m}_0}, \rho_{\mathsf{m}_1}, C_C, \rho_{\mathsf{st}_C})$ are each admissible queries (Definition 25) it holds that

$$\Pr[b_B = b_C = b] \leq \frac{1}{2} + negl(\lambda)$$

where the random coins are taken over the randomness of $\mathcal{A}$, $\mathsf{Setup}, \mathsf{KeyGen}$ and Enc.

Remark 4. One could obtain an adaptive security notion by allowing B and C to make adaptive function secret key queries themselves.

Difference to Unclonable Functional Encryption Experiment. The experiments for 2-player single-query IND-Security for QFE and the experiment for unclonable functional encryption look very similar. Note that in this experiment the function secret keys that are obtained are restricted to be admissible queries. In the unclonable functional encryption experiment the function queries are not subject to any admissibility constraint which is a much stronger notion.

Lemma 7. *Any non-adaptively IND-secure single-query QFE scheme (Definition 24) is also a 2-player single-query IND-secure QFE scheme (Definition 30).*

Proof. An adversary $\tilde{A}$ in the single-query QFE IND-experiment can execute an adversary (A, B, C) that wins the 2-player IND-experiment by only executing A and B and by only making a single key query C_B. Since to break security in the 2-player IND-security experiment both players B and C need to guess the correct bit b, $\tilde{A}$ can win the IND-security experiment with the same probability as (A, B, C) by outputting the guess B outputs. □

B Proof: Sim-security implies IND-security

Here we provide the proof of Lemma 3. We restate the Lemma for convenience.

Lemma 8. *A QFE scheme that is single-query (non)-adaptively SIM-secure (Definition 23) is also single-query (non)-adaptively IND-secure (Definition 24).*

Proof. Let $\mathcal{A}$ be an adversary that wins $\mathsf{Exp}^{IND}_{\mathcal{A},b}$ with non-negligible probability. Then we can define an adversary $\mathcal{A}^*$ that wins the SIM-security experiment with non-negligible probability. Upon receiving mpk $\mathcal{A}^*$ runs $\mathcal{A}$ on input mpk until $\mathcal{A}$ outputs $(\rho^{EU}_{\mathsf{m}_0}, \rho^{EU}_{\mathsf{m}_1}, \rho_{\mathsf{st}})$. A key-query of $\mathcal{A}$ is forwarded by $\mathcal{A}^*$ to it's own key oracle. Then $\mathcal{A}^*$ samples a random bit b and sends $\rho^E_{\mathsf{m}_b}$ as it's challenge message and receives ρ_{ct}. $\mathcal{A}^*$ runs $\mathcal{A}$ on input $(\rho_{\mathsf{ct}}, \rho^U_{\mathsf{m}_b}, \rho_{\mathsf{st}})$ until it outputs a guess b'.

$\mathcal{A}^*$ outputs the state (b', b). If $\mathcal{A}^*$ interacted in the ideal world the probability that $b = b'$ is $\frac{1}{2} + negl(\lambda)$. In the ideal world the simulator receives the state $C(\rho^U_{\mathsf{m}_b})$ without any information on the bit b. Let Φ be a completely positive trace preserving (CPTP) map that describes the action of the simulator in the ideal experiment and Φ' be a CPTP map that applies Φ on the corresponding subsystem and the identity everywhere else. After receiving the ciphertext the adversary holds the state $\sum_i \Phi(C(\rho^E_{\mathsf{m}_{b,i}})) \otimes \rho^U_{\mathsf{m}_{b,i}} \otimes \rho_{A_i}$.

$$
\begin{aligned}
&\mathrm{TD}(\sum_i \Phi(C(\rho^E_{\mathsf{m}_{0,i}})) \otimes \rho^U_{\mathsf{m}_{0,i}} \otimes \rho_{A_i}, \sum_i \Phi(C(\rho^E_{\mathsf{m}_{1,i}})) \otimes \rho^U_{\mathsf{m}_{1,i}} \otimes \rho_{A_i}) \\
&= \mathrm{TD}(\sum_i \Phi'(C(\rho^E_{\mathsf{m}_{0,i}}) \otimes \rho^U_{\mathsf{m}_{0,i}} \otimes \rho_{A_i}), \sum_i \Phi'(C(\rho^E_{\mathsf{m}_{1,i}}) \otimes \rho^U_{\mathsf{m}_{1,i}} \otimes \rho_{A_i})) \\
&= \mathrm{TD}(\Phi'(\sum_i C(\rho^E_{\mathsf{m}_{0,i}}) \otimes \rho^U_{\mathsf{m}_{0,i}} \otimes \rho_{A_i}), \Phi'(\sum_i C(\rho^E_{\mathsf{m}_{1,i}}) \otimes \rho^U_{\mathsf{m}_{1,i}} \otimes \rho_{A_i})) \\
&\leq \mathrm{TD}(\sum_i C(\rho^E_{\mathsf{m}_{0,i}}) \otimes \rho^U_{\mathsf{m}_{0,i}} \otimes \rho_{A_i}, \sum_i C(\rho^E_{\mathsf{m}_{1,i}}) \otimes \rho^U_{\mathsf{m}_{1,i}} \otimes \rho_{A_i}) \\
&\leq negl(\lambda)
\end{aligned}
$$

The second to last step follows from the fact that the trace distance cannot be increased by applying a CPTP map. By definition of the trace distance $\mathcal{A}$ cannot distinguish the two states with more than negligible probability in the ideal world.

By assumption $\mathcal{A}$ wins the IND-experiment with non-negligible advantage, therefore in the case of the real world $b = b'$ with $\frac{1}{2} + \varepsilon$ where ε is non-negligible probability and we can distinguish the real and ideal cases with advantage $\varepsilon/2$. □