Characterizing the qIND-qCPA (in)security of the CBC, CFB, OFB and CTR modes of operation

Tristan Nemoz[1,2,3], Zoé Amblard[1], and Aurélien Dupin[1]

[1] Thales SIX GTS, Gennevilliers, France
{zoe.amblard,aurelien.dupin}@thalesgroup.com
[2] Télécom Paris, Palaiseau, France
[3] EURECOM, Biot, France
nemoz@eurecom.fr

Abstract. We extend the work performed by Anand, Targhi, Tabia and Unruh (PQCrypto 2016) of studying the post-quantum security of the CBC, CFB, OFB and CTR modes of operation by considering all possible notions of qIND-qCPA security defined by Carstens, Ebrahimi, Tabia and Unruh (TCC 2021).
We show that the results obtained by Anand et al. for the qIND-qCPA-P6 security of these modes carry on to the others IND-qCPA notions, namely the qIND-qCPA-P10 and qIND-qCPA-P11 ones. We also show that CFB, CTR and OFB are insecure according to all of the other notions, regardless of the block cipher they are used with. We provide several results concerning the (in)security of CBC. First of all, we show that it is insecure according to the qIND-qCPA-P9 notion. By distinguishing on the nature of the underlying block cipher, we prove its qIND-qCPA-P5 security when based upon a qPRP and we prove that it can be qIND-qCPA-P13 insecure when based upon a PRP, thus fully characterizing it. We illustrate the later result by using as a counter-example the same block cipher used by Anand et al..

Keywords: Post-quantum cryptography · Block ciphers · Modes of operation · qIND-qCPA security

This paper has been written based on Tristan Nemoz's Master thesis [13].

1 Introduction

1.1 Context and results

While it is now common knowledge that traditional asymmetric cryptography is threatened by quantum computers, notably due to Shor's algorithm [15], the security of the currently used symmetric primitives is still under consideration. Some work in this field includes for instance finding polynomial attacks against symmetric systems using Simon's algorithm [10], evaluating the security of AES

in a quantum world [3,9], defining quantum-aware security notions for cryptosystems [2,4,5,7,8], or performing various security proofs, including that of Fiat–Shamir in the QROM model [6,11].

The security of the CBC, CFB, OFB and CTR modes of operations has been traditionally assessed via the IND-CPA security notion [18]. In this notion, the adversary can issue learning requests and challenge requests. Learning requests are answered by an oracle implementing the encryption function which security is to be assessed. Challenge requests on the other hand are answered by an oracle which nature depends on the "world" the game is taking place in. In the "real" world, the challenge oracle behaves identically to the learning oracle. In the "random" world however, the oracle first applies a permutation chosen at random at the beginning of the game on the adversary's queries. The goal of the adversary is then to find out whether the game takes place in the real world or the random one. A system is said to be IND-CPA secure if the optimal strategy for such an adversary that runs in polynomial time provides low to no advantage when compared to simply guessing at random.

This notion however, requires that both learning and challenge requests are classical. Reasons for considering the security of cryptographic schemes when using superposition queries have previously been given in the literature [1,2,7]. The most sensible one is the fact that quantum communication protocols may arise from the upcoming advent of quantum computers. In such a situation where end-users communicate using quantum states, the question of encryption applied on superposed states and its associated security are to be considered. Another reason is that the security proof of a scheme that is meant to be used classically may use the security against quantum superposition of its internal schemes.

Boneh and Zhandry showed that the immediate, natural translation of the IND-CPA notion in a quantum world was not achievable [2]. Thus, they instead proposed the IND-qCPA notion, where learning queries are quantum, but challenge ones are still classical. In the light of this new notion, Anand et al. proved the IND-qCPA (in)security of the aforementioned modes depending on whether they were used with a standard-secure block cipher or a quantum-secure one.

In the years following Boneh and Zhandry's IND-qCPA definition, some work has been performed to try to define other security notions for a quantum world where both learning and challenge requests are quantum [2,5,7,12]. These notions essentially make use of different quantum oracles and different challenge queries. Eventually, Carstens et al. defined all possible remaining notions and studied the implications between them [4]. This resulted in 14 distinct equivalence classes of qIND-qCPA notions.

In this paper, we extend Anand et al.'s work [1] by studying the security of the CBC, CFB, OFB and CTR modes in all security notions defined by Carstens et al. [4]. Our results are summarized in Table 1.

1.2 Our results

IND-qCPA security We observe that the results found by Anand et al. for the qIND-qCPA-P6 carry on to the two other IND-qCPA notions, namely the qIND-

Table 1. Summary of our results. The ✓ symbol means that all denoted systems are secure in this notion. The ✗ symbol means that no denoted system is secure in this notion. The ◆ symbol means that there is at least one system secure and one insecure in this notion. The superscripts indicate either the article in which this result was first proved, the theorem stating it or the security notion implying it.

	CTR/OFB with PRP/qPRP	CBC with PRP	CBC with qPRP	CFB with PRP	CFB with qPRP
P1	✗ P13	✗ P9	✗ P9	✗ P13	✗ P13
P2	✗ [5]	✗ P12	✗ P12	✗ [5]	✗ [5]
P3	✗ P13	✗ P9	✗ P9	✗ P13	✗ P13
P4	✗ P13	✗ P9	✗ P9	✗ P13	✗ P13
P5	✗ P13	◆ P13	✓ 9	✗ P13	✗ P13
P6	✓ [1]	◆ [1]	✓ [1]	◆ [1]	✓ [1]
P7	✗ P13	◆ P13	✓ P5	✗ P13	✗ P13
P8	✗ P13	✗ P9	✗ P9	✗ P13	✗ P13
P9	✗ P13	✗ 10	✗ 10	✗ P13	✗ P13
P10	✓ 1	◆ P11	✓ 8	◆ P11	✓ 4
P11	✓ P6	◆ 7	✓ P6	◆ 3	✓ P6
P12	✗ [4]	✗ [4]	✗ [4]	✗ [4]	✗ [4]
P13	✗ 2	◆ 6	✓ P5	✗ 5	✗ 5
P14	✓ [1]	✓ [1]	✓ [1]	✓ [1]	✓ [1]

qCPA-P10 and qIND-qCPA-P11 ones. In fact, the proofs in these cases are adapted from the ones written in Anand et al.'s work [1]: simulating a quantum oracle that implements a CTR or OFB mode using classical queries remains possible; we use a variant of the One-way to Hiding Lemma to show the security of CBC and CFB when used with a qPRP and we use the same attack up to an extra step to show that these two modes may be insecure when used with a PRP.

qIND-qCPA-P13 insecurity of CFB, CTR and OFB Furthermore, we see that these are the only security notions verified by the CFB, CTR and OFB modes, since they are qIND-qCPA-P13 insecure, no matter what the underlying block cipher is. Indeed, an adversary in the real world can disentangle the message register from the ciphertext register, while an adversary in the random world can't. This allows them to efficiently distinguish both worlds and thus to win in this game with an high advantage. Since the qIND-qCPA-P13 security notion is implied by all the other notions but the IND-qCPA ones and the IND-CPA one, this fully characterizes the security of these modes.

qIND-qCPA-P5 security of CBC used with a qPRP CBC on the other hand is qIND-qCPA-P5 secure when used with a qPRP. In order to show this, we use a result from Carstens et al. [4] which states that an embedding oracle implementing a random injective function can be replaced by a classical one implementing the same function while only increasing the adversary's advantage by a negligi-

ble amount. We are thus able to replace every challenge query performed by the adversary by a classical one, effectively reducing the qIND-qCPA-P5 security of the system to its IND-CPA security.

qIND-qCPA-P9 insecurity of CBC Moreover, we show that CBC is qIND-qCPA-P9 insecure, no matter what the underlying block cipher is as long as the message to be encrypted is at least two-blocks long. Indeed, with high probability, distinguishing whether a random permutation has been applied in this case is equivalent to distinguishing between the states $|+\rangle$ and $|x\rangle$ for some random x. This distinction is easily done by applying an $\mathbf{H}$ gate on the aforementioned register and then measuring it.

Potential qIND-qCPA-P13 insecurity of CBC used with a PRP Finally, we pull off an attack against CBC used with a PRP in the qIND-qCPA-P13 game by using the same block cipher as Anand et al. in their work [1]. In this game, the adversary is only allowed to perform a single challenge request using an embedding oracle. We show how this challenge request can be used to simulate an access to an embedding oracle implementing the flawed block cipher, allowing the adversary to recover the secret key, which can then be used to differentiate the real world and the random one.

1.3 Previous work

Anand et al. studied in [1] the security of the modes of operation under the qIND-qCPA-P6 security notion and argued that the classical security proofs for these modes still hold for a quantum adversary. Chevalier, Ebrahimi and Vu showed in [5] that the CFB, OFB and CTR modes of operation cannot achieve qIND-qCPA-P2 security. This result was later improved by Carstens et al. who showed that CBC, CFB, OFB and CTR don't satisfy the qIND-qCPA-P12 security notion as long as they use at least two blocks [4].

2 Notations and definitions

2.1 Notations

$[\![a\,;\,b]\!]$ represents the set $[a\,;\,b] \cap \mathbb{N}$. An adversary $\mathcal{A}$ having access to an oracle implementing a function f is denoted $\mathcal{A}^f$. For a given permutation π, we denote $\pi_{a\to b}$ the function which returns the bits of π from a to b inclusive, starting the indexing at 0. The security parameter of a system is denoted λ. Similarly to [1], we define last and droplast as the functions which return respectively the last bit of their input and their input without their last bit. For an arbitrary string a and a bit b, $a \cdot b$ is set to the all-zero string if b is equal to 0 and to a if $b = 1$. Note that if a and b are two bitstrings which have the same size, $a \cdot b$ is defined as the product of a and b as indicated in the definition of the Hadamard gate.

For a given mode of operation mode, we denote E_k the underlying block cipher and by $\mathsf{Enc}^{\mathsf{mode}}_{E_\mathsf{k}}$ the resulting symmetric scheme. If necessary, we denote this resulting scheme $\mathsf{Enc}^{\mathsf{mode}}_{E_\mathsf{k},c_0,\ell}$ to indicate which initialization vector is used and how many blocks the scheme operates on. The advantage of an adversary $\mathcal{A}$ in the experiment Exp using the symmetric scheme $\mathcal{S}$ is defined as, accordingly to the definition given in [12]:

$$\mathsf{Adv}^{\mathrm{exp}}_{\mathcal{A},\mathcal{S}}(\lambda) = \left|\Pr\left[\mathsf{Exp}^0_{\mathcal{S}}(\lambda,\mathcal{A})=1\right] - \Pr\left[\mathsf{Exp}^1_{\mathcal{S}}(\lambda,\mathcal{A})=1\right]\right|$$

where $\Pr\left[\mathsf{Exp}^b_{\mathcal{S}}(\lambda,\mathcal{A})=1\right]$ is the probability that $\mathcal{A}$ returns 1 if the bit they have to guess is set to b. We define the real world to be the one where $b=0$ and the random world to be the one where $b=1$. Note that while the real-or-random notion we use has originally been introduced in [12], it was then named "real or permutation", and the convention for the real and random worlds was the opposite of ours.

We denote BC_k the block cipher introduced by Anand et al. [1], which maps x to:

$$E_{h_1(\mathsf{k})}\left[\mathsf{droplast}\left[x \oplus \left[(\mathsf{k}\|1)\cdot \mathsf{last}(x)\right]\right]\right] \Big\| \left[t_{h_2(\mathsf{k})}\left[x \oplus \left[(\mathsf{k}\|1)\cdot \mathsf{last}(x)\right]\right] \oplus \mathsf{last}(x)\right]$$

with E being a PRP taking as inputs a key of length $\lambda-1$ and a message of length $\lambda-1$ and returns a ciphertext of length $\lambda-1$, t being a PRF taking as input a key of size λ and a message of size λ and returns a single bit and with h_1 and h_2 being two random oracles used to generate appropriate keys for E and t from the master key k. Anand et al. showed that this block cipher is a PRP [1].

If they are unambiguous, we omit both the index in the sums and the normalization constants. As such, we have $|+\rangle = \sum_x |x\rangle$ and $|-\rangle = \sum_x (-1)^x |x\rangle$. We denote $\mathbf{H}$ the Hadamard gate and $\mathbf{X}$ the `NOT` gate. An oracle implementing a function f is denoted $\mathcal{O}_f$. If we want to name a quantum register $|\psi\rangle$, we indicate its name as a subscript, like $|\psi\rangle_{\mathrm{Name}}$.

2.2 Modes of operations

It is to be denoted that a key generation function is supposed to be defined in order to properly define an encryption scheme. For simplicity's sake, we did not include it within the following definitions, since it only consists in randomly choosing a key in $\{0,1\}^\lambda$.

Definition 1 (CBC mode, adapted from [1, Definition 6]). *For a given permutation $E_\mathsf{k}: \{0,1\}^n \to \{0,1\}^n$, we define the CBC scheme with the following encryption and decryption functions:*

$\mathsf{Enc}^{\mathsf{CBC}}_{E_\mathsf{k}}$**:** *For a message $m = m_1 \cdots m_\ell$, choose randomly c_0 and return c_0 along with $c = c_1 \cdots c_\ell$ where, for $i \in [\![1\,;\,\ell]\!]$, $c_i = E_\mathsf{k}(m_i \oplus c_{i-1})$.*

$\mathsf{Dec}^{\mathsf{CBC}}_{E_\mathsf{k}}$**:** *For a ciphertext $c = c_1 \cdots m_\ell$ and being given c_0, return $m = m_1 \cdots m_\ell$ where, for $i \in [\![1\,;\,\ell]\!]$, $m_i = E^{-1}_\mathsf{k}(c_i) \oplus c_{i-1}$.*

Definition 2 (CFB mode, adapted from [1, Definition 7]). *For a given function $E_\mathsf{k} : \{0,1\}^n \to \{0,1\}^n$, we define the CFB scheme with the following encryption and decryption functions:*

$\mathsf{Enc}^{\mathsf{CFB}}_{E_\mathsf{k}}$**:** *For a message $m = m_1 \cdots m_\ell$, choose randomly c_0 and return c_0 along with $c = c_1 \cdots c_\ell$ where, for $i \in [\![1\,;\,\ell]\!]$, $c_i = m_i \oplus E_\mathsf{k}(c_{i-1})$.*

$\mathsf{Dec}^{\mathsf{CFB}}_{E_\mathsf{k}}$**:** *For a ciphertext $c = c_1 \cdots m_\ell$ and being given c_0, return $m = m_1 \cdots m_\ell$ where, for $i \in [\![1\,;\,\ell]\!]$, $m_i = E_\mathsf{k}(c_{i-1}) \oplus c_i$.*

Definition 3 (OFB mode, adapted from [1, Definition 8]). *For a given function $E_\mathsf{k} : \{0,1\}^n \to \{0,1\}^n$, we define the OFB scheme with the following encryption and decryption functions:*

$\mathsf{Enc}^{\mathsf{OFB}}_{E_\mathsf{k}}$**:** *For a message $m = m_1 \cdots m_\ell$, choose randomly c_0 and return c_0 along with $c = c_1 \cdots c_\ell$ where $t_0 = E_\mathsf{k}(c_0)$ and, for $i \in [\![1\,;\,\ell]\!]$, $c_i = t_i \oplus m_i$ and $t_i = E_\mathsf{k}(t_{i-1})$.*

$\mathsf{Dec}^{\mathsf{OFB}}_{E_\mathsf{k}}$**:** *For a ciphertext $c = c_1 \cdots m_\ell$ and being given c_0, computes $t_0 = E_\mathsf{k}(c_0)$ and return $m = m_1 \cdots m_\ell$ where, for $i \in [\![1\,;\,\ell]\!]$, $m_i = t_i \oplus c_i$ and $t_i = E_\mathsf{k}(t_{i-1})$.*

Definition 4 (CTR mode, adapted from [1, Definition 9]). *For a given function $E_\mathsf{k} : \{0,1\}^n \to \{0,1\}^n$, we define the CTR scheme with the following encryption and decryption functions:*

$\mathsf{Enc}^{\mathsf{CTR}}_{E\mathsf{k}}$**:** *For a message $m = m_1 \cdots m_\ell$, choose randomly c_0 and return c_0 along with $c = c_1 \cdots c_\ell$ where, for $i \in [\![1\,;\,\ell]\!]$, $c_i = m_i \oplus E_\mathsf{k}(c_0 \oplus i - 1)$.*

$\mathsf{Dec}^{\mathsf{CTR}}_{E\mathsf{k}}$**:** *For a ciphertext $c = c_1 \cdots m_\ell$ and being given c_0, return $m = m_1 \cdots m_\ell$ where, for $i \in [\![1\,;\,\ell]\!]$, $m_i = c_i \oplus E_\mathsf{k}(c_0 \oplus i - 1)$.*

Some things are to be denoted with these definitions. First of all, in the literature, the initialization vector c_0 is often returned as part of the ciphertext. Since we want to apply these encryption schemes to quantum states, it is completely equivalent to consider that the adversary classically knows c_0 and receives the remaining of the ciphertext as a quantum state.

Furthermore, it is important to note that the maximal ℓ that such a mode of operation accepts is assumed to be polynomial in λ. In all of our proofs, ℓ is assumed to be constant, that is we assume that the oracle only accepts queries of size ℓ, which covers the case where the oracle accepts queries of variable length. Similarly, the block size, denoted n in the definitions, is also assumed to be polynomial in λ. This assumption is justified by the fact that often, $n = \lambda$ holds. The same assumption is made in [1], since the authors claim that CBC and CFB are qIND-qCPA-P6 secure when used with a qPRP by showing that the adversary's advantage is negligible in n.

2.3 Security notions

Pseudorandom permutations

Definition 5 (Standard and quantum-secure pseudorandom permutation, adapted from [19, Definition 3.1]). *A permutation π_k depending on a key k is a standard-secure (respectively quantum-secure) pseudorandom permutation, which we denote PRP (respectively qPRP), if no polynomial quantum adversary $\mathcal{A}$ making classical (respectively quantum) queries to both the permutation and its inverse can distinguish between a truly random permutation and π_k for a randomly chosen k.*

qIND-qCPA notions In [4], Carstens et al. defined 14 different qIND-qCPA notions. A notion is fully characterized by the oracle type on which the adversary performs its learning queries, the one on which they perform their challenge queries, the challenge type, like left-or-right or real-or-random, and the number of challenge queries they are allowed to perform. We quickly define the values these parameters can take and carry on with presenting the security notions we will be working with.

Oracle types Let f be the function implemented by the oracle the adversary has access to. Note that it is sufficient to describe the behavior of an oracle on the basis states to fully describe it. Four types of oracle are considered in Carstens et al.'s work [4]:

Standard oracle: On a basis state $|x, y\rangle$, the oracle returns $|x, y \oplus f(x)\rangle$.
Embedding oracle: This oracle is the same as the standard one, at the exception that the adversary only sends the input register $|x\rangle$. The oracle then prepares a basis state $|0\rangle$ as the output register and acts as a standard oracle, returning $|x, f(x)\rangle$.
Erasing oracle: This oracle requires f to be injective. On a basis state $|x\rangle$, it returns $|f(x)\rangle$.
Classical oracle: This oracle only accepts classical queries.

Challenge type Three challenge types are used in [4]. In this article, we mainly use one of them: the real-or-random one, as defined in [12]. On a challenge query, in the real world, the challenger responds with the encryption of said query. In the random world however, the challenger firstly applies a random permutation π on the input before encrypting it. Note that π is fixed: it is chosen once and for all at the beginning of the game. Note also that this definition allows to use the same definition for classical and quantum queries, since it is possible to define an unitary gate $\boldsymbol{\Pi}$ applying π on a quantum state. Note that in Section 7, we also use the left-or-right return type, as defined by Carstens et al. [4]. When using this return type with an erasing oracle, the adversary sends two quantum states $|\psi_0\rangle$ and $|\psi_1\rangle$ and is given back $|\mathsf{Enc}(\psi_b)\rangle$.

We are now able to define the security notions we'll be working with. We begin by the so-called IND-qCPA notions. Note that for clarity's sake, we don't include the original definition of IND-qCPA as defined in [2] which we mention as qIND-qCPA-P6 but don't use. In all these definitions, a scheme is said to be secure if the adversary only wins with a negligible advantage in λ.

Definition 6 (qIND-qCPA-P10 game, adapted from [4]). *In this notion, the adversary is allowed to perform their learning queries on an erasing oracle and can perform as much challenge queries as they want on a classical oracle.*

Definition 7 (qIND-qCPA-P11 game, adapted from [4]). *In this notion, the adversary is allowed to perform their learning queries on an embedding oracle and can perform as much challenge queries as they want on a classical oracle.*

Both qIND-qCPA-P6 and qIND-qCPA-P10 security notions imply the qIND-qCPA-P11 one. Since Anand et al. showed the (in)security of the modes of operation within the qIND-qCPA-P6 notion, we ought to show the insecurity of these modes in the qIND-qCPA-P11 notion or their security in the qIND-qCPA-P10 one.

We carry on by defining the qIND-qCPA-P13 game.

Definition 8 (qIND-qCPA-P13 game, adapted from [4]). *In this notion, the adversary is allowed to perform their learning queries on a classical oracle and can perform a single challenge query on an embedding oracle.*

The qIND-qCPA-P13 security notion has a very useful property: every qIND-qCPA security notion that is not an IND-qCPA one nor the standard IND-CPA one implies it, as shown in [4]. As such, if we were to show that a scheme is qIND-qCPA-P13 insecure, we would only have to consider its security within the IND-qCPA security notions to fully characterize it. This is the case for the CFB, CTR and OFB modes of operation. CBC requires two more definitions to be fully characterized, which will be introduced at their time of use for clarity's sake, namely the qIND-qCPA-P5 and qIND-qCPA-P9 notions. Similarly, we will only use the qIND-qCPA-P8 notion in section 7, which is why its definition will be given there.

3 Lemmas

In this section, we introduce and prove some lemmas that we use either in our attacks or in our security proofs.

Lemma 1. *We consider a quantum state that can be written as* $\sum_x |x\rangle |f(x)\rangle$ *with* f *being a function from* $\{0,1\}^m$ *to* $\{0,1\}^n$*. Applying an* $\mathbf{H}$ *gate to the first register and then measuring it returns* $|0\rangle$ *with probability* $\frac{1}{2^{2m}} \sum_y \left|f^{-1}(y)\right|^2$*.*

In particular, this method returns $|0\rangle$ *with probability 1 if* f *is constant.*

Proof. We first apply the $\mathbf{H}$ gate on the system, which puts it in the state:

$$\frac{1}{2^m} \sum_x \sum_k (-1)^{x \cdot k} |k\rangle |f(x)\rangle = \frac{1}{2^m} |0\rangle \sum_x |f(x)\rangle + \frac{1}{2^m} \sum_x \sum_{k \neq 0} (-1)^{x \cdot k} |k\rangle |f(x)\rangle . \tag{1}$$

The probability of measuring $|0\rangle$ is thus given by:

$$\Pr[|0\rangle] = \sum_y \Pr[|0, y\rangle] = \sum_y \left(\sum_{x \in f^{-1}(y)} \frac{1}{2^m} \right)^2 = \frac{1}{2^{2m}} \sum_y \left|f^{-1}(y)\right|^2 . \tag{2}$$

□

Lemma 2 (One-way to Hiding). *Let $H : \{0,1\}^n \to \{0,1\}^n$ be a random bijective function and $\mathcal{A}$ be an algorithm making at most q requests to H using either a standard oracle or an erasing one, taking as input two n-bit strings x and y and returning a single bit b. We define an algorithm $\mathcal{B}$ taking inputs similar to those of $\mathcal{A}$ and behaving as follows. $\mathcal{B}$ chooses $i \in [\![1\,;\,q]\!]$ uniformly at random and runs $\mathcal{A}^H(x,y)$ until just before the i-th query to H, at which point it measures the input register in the computational basis and returns the result. If $\mathcal{A}$ makes less than i requests to H, $\mathcal{B}$ returns $\perp \notin \{0,1\}^n$.*

For x being chosen uniformly at random, we define $P^1_{\mathcal{A}}$ to be the expected probability that $\mathcal{A}$ returns 1 if its inputs are x and $H(x)$. For y also being chosen uniformly at random, we define $P^2_{\mathcal{A}}$ to be the expected probability that $\mathcal{A}$ returns 1 if its entries are x and y. Finally, we define $P_{\mathcal{B}}$ to be the expected probability that $\mathcal{B}$ returns x or $H^{-1}(y)$ if its inputs are x and y. Then:

$$\left|P^1_{\mathcal{A}} - P^2_{\mathcal{A}}\right| \leqslant 2q\sqrt{P_{\mathcal{B}}}. \tag{3}$$

This lemma is a variant of the original One-way to Hiding Lemma introduced by Unruh [17], the only differences being the function being bijective, the possibility to use an erasing oracle and the natural redefinition of $P_{\mathcal{B}}$. As such, the proof of this lemma is very similar to the original one, which is why we put it in Appendix A.

Lemma 3 (Simon's algorithm, adapted from [16]). *Let n be the size of the quantum registers we are working with and s a fixed n-bit string. Being given $n-1$ states that can be written as $|x\rangle + |x \oplus s\rangle$, it is possible to recover s in polynomial time with probability at least $\frac{1}{4}$.*

4 qIND-qCPA security of CTR and OFB

In this section, we show that the only security notions that CTR and OFB satisfy are the IND-qCPA ones by using the same argument as Anand et al. for proving their qIND-qCPA-P6 security and by exhibiting an attack against their qIND-qCPA-P13 security.

These proofs only rely on the fact that in order to produce the ciphertext, CTR and OFB perform a XOR between the message and a pseudorandom string s. As such, our proofs can also be applied to stream ciphers, and we will denote $m \oplus s$ an encryption of the message m using such a scheme throughout our proofs.

4.1 IND-qCPA security of CTR and OFB

Since Anand et al. already showed that CTR and OFB are qIND-qCPA-P6 secure, we only have to show that they are also qIND-qCPA-P10 secure to show their full IND-qCPA security. In this security notion, the adversary has access to an

erasing oracle, which cannot be simulated by a standard oracle as used in the qIND-qCPA-P6 notion. Though, we show that Anand et al.'s argument [1] carry on to erasing oracles.

Theorem 1. *A system using a PRP in CTR or OFB mode is qIND-qCPA-P10 secure.*

Proof. We adapt the argument used by Anand et al.: a reduction $\mathcal{R}$ having a classical access to the encryption function can perfectly simulate an erasing oracle.

Indeed, let us assume that the adversary has a state $\sum_{x,y} \alpha_{x,y} |x, y\rangle$ and performs their query using the second register. The reduction queries for the encryption of 0 and receives $s \oplus 0 = s$, since CTR and OFB operate as stream ciphers. $\mathcal{R}$ can then apply $\mathbf{X}$ gates accordingly on the register it received, effectively creating the state $\sum_{x,y} \alpha_{x,y} |x, y \oplus s\rangle$, which is exactly the state the adversary would have received, had they interacted with an erasing oracle.

Thus, the qIND-qCPA-P10 security of CTR and OFB can be reduced to their IND-CPA security, which they satisfy as long as they are used with a PRP. □

4.2 qIND-qCPA-P13 insecurity of CTR and OFB

To fully characterize CTR and OFB, we thus now only have to show that they are qIND-qCPA-P13 insecure.

Theorem 2. *CTR and OFB are qIND-qCPA-P13 insecure, no matter what the underlying block cipher is.*

Proof. $\mathcal{A}$ prepares the state $|+\rangle$ on all their registers and performs their challenge query using it. We can write this state as:

$$\sum_{x_1,\cdots,x_\ell} \bigotimes_{i=1}^{\ell} |x_i\rangle = \sum_x |x\rangle \tag{4}$$

where ℓ is the number of blocks and n their size. If $b = 0$, the adversary receives:

$$\sum_x |x\rangle |x \oplus s\rangle \tag{5}$$

while they will get, if $b = 1$ for a random permutation π:

$$\sum_x |x\rangle |\pi(x) \oplus s\rangle . \tag{6}$$

By performing an $\mathbf{X}$ gate on the second register controlled by the first one, the state becomes, if $b = 0$:

$$\sum_x |x\rangle |s\rangle \tag{7}$$

while it becomes, if $b = 1$:

$$\sum_x |x\rangle |x \oplus \pi(x) \oplus s\rangle . \tag{8}$$

Thus, if $b = 0$, the two registers are not entangled: applying an $\mathbf{H}$ gate on the first register and measuring it yields $|0\rangle$ with certainty. If $b = 1$ however, such a procedure yields $|0\rangle$ with negligible probability. We can apply Lemma 1 with $f = x \mapsto x \oplus \pi(x) \oplus s$ to show this formally. The probability to measure $|0\rangle$ if $b = 1$ is thus given by:

$$\Pr[|0\rangle \mid b = 1] = \frac{1}{2^{2\ell n}} \sum_y \left|f^{-1}(y)\right|^2 . \tag{9}$$

Since the sum is going through all possible y, it is completely equivalent to redefine f to be $x \mapsto x \oplus \pi(x)$. The following is a rewriting of the proof proposed by Iosif Pinelis [14].

We have, for a given y:

$$\left|f^{-1}(y)\right| = \sum_x \mathbb{1}_{\pi(x)=x\oplus y} \tag{10}$$

thus:

$$\left|f^{-1}(y)\right|^2 = \sum_{x_1} \sum_{x_2} \mathbb{1}_{[\pi(x_1)=x_1\oplus y]\cap[\pi(x_2)=x_2\oplus y]} \tag{11}$$

thus:

$$\mathbb{E}\left[\left|f^{-1}(y)\right|^2\right] = \sum_{x_1} \sum_{x_2} \Pr[[\pi(x_1) = x_1 \oplus y] \cap [\pi(x_2) = x_2 \oplus y]] \tag{12a}$$

$$= \sum_{x_1} \Pr[\pi(x_1) = x_1 \oplus y] + \sum_{x_1} \sum_{x_2 \neq x_1} \Pr[[\pi(x_1) = x_1 \oplus y] \cap [\pi(x_2) = x_2 \oplus y]]. \tag{12b}$$

Since π is a random permutation, all the events in $(\pi(x_1) = x_1 \oplus y)_{x_1}$ have the same probability. As such:

$$\mathbb{E}\left[\left|f^{-1}(y)\right|^2\right] = 1 + \frac{1}{2^{\ell n}} \sum_{x_1} \sum_{x_2 \neq x_1} \Pr[\pi(x_2) = x_2 \oplus y \mid \pi(x_1) = x_1 \oplus y]. \tag{12c}$$

Similarly, since π is a random permutation, the events in $(\pi(x_2) = x_2 \oplus y)_{x_2 \neq x_1}$ have all the same probability being given that $\pi(x_1) = x_1 \oplus y$. Thus, we have:

$$\mathbb{E}\left[\left|f^{-1}(y)\right|^2\right] = 2. \tag{12d}$$

Finally, the probability of measuring $|0\rangle$ if $b = 1$ is given by:

$$\Pr[|0\rangle \mid b = 1] = \frac{1}{2^{\ell n - 1}}. \tag{13}$$

All in all, the adversary's advantage is given by:

$$\mathsf{Adv}^{\mathsf{qind\text{-}qcpa\text{-}p13}}_{\mathcal{A},\mathsf{CTR/OFB}}(\lambda) = 1 - \frac{1}{2^{\ell n - 1}}. \tag{14}$$

In particular, it is not negligible with respect to λ. □

5 qIND-qCPA security of CFB

5.1 Potential IND-qCPA insecurity of CFB used with a PRP

We first show that, similarly to Anand et al.'s results [1], there is a PRP which, when used in CFB mode, yields an IND-qCPA insecure scheme. We use the same block cipher as Anand et al. and performs the same attack up to one detail: Anand et al. used the fact that the adversary is allowed to query a uniform superposition on the last qubit so that it is not entangled with the other register. Using an embedding oracle, we cannot use such a trick and are forced to explicitly disentangle this last qubit with the remaining of the state.

Theorem 3. *There is a PRP such that the system using it as a block cipher in CFB mode is qIND-qCPA-P11 insecure.*

Proof. As a recall, in the qIND-qCPA-P11 security notions, the adversary is allowed to perform their learning queries on an embedding oracle, while their challenge queries must be done using a classical one. Our goal is to show that using a specific block cipher, which has been shown to be a PRP by Anand et al. [1], the adversary is able to recover the secret key.

We use the same flawed block cipher BC_k as Anand et al. [1], that is the one which maps a λ-bit string x to:

$$E_{h_1(\mathsf{k})}\left[\mathsf{droplast}\left[x \oplus \left[(\mathsf{k}\|1) \cdot \mathsf{last}(x)\right]\right]\right] \Big\| \left[t_{h_2}(\mathsf{k})\left[x \oplus \left[(\mathsf{k}\|1) \cdot \mathsf{last}(x)\right]\right] \oplus \mathsf{last}(x)\right].$$

We begin by showing that CFB is insecure when accepting only $\ell = 2$ blocks and we will then generalize this result to $\ell \geqslant 2$.

The adversary prepares the following state:

$$\sum_x |x\rangle_{M_1} |0\rangle_{M_2} \tag{15}$$

and performs a learning query using it. They thus receive the following state, where we omitted the M_2 register which is not entangled with the other registers:

$$\sum_x |x\rangle \left|\mathsf{BC}_\mathsf{k}\left(c_0\right) \oplus x\right\rangle_{C_1} \left|\mathsf{droplast}\left(\mathsf{BC}_\mathsf{k}\left(\mathsf{BC}_\mathsf{k}\left(c_0\right) \oplus x\right)\right)\right\rangle_{C_{2,1}} \\ \left|t_{h_2(\mathsf{k})}\left(\mathsf{BC}_\mathsf{k}\left(c_0\right) \oplus x \oplus \left[(\mathsf{k}\|1) \cdot \mathsf{last}\left(\mathsf{BC}_\mathsf{k}\left(c_0\right) \oplus x\right)\right] \oplus \mathsf{last}\left(\mathsf{BC}_\mathsf{k}\left(c_0\right) \oplus x\right)\right)\right\rangle_{C_{2,2}}. \tag{16}$$

$\mathcal{A}$ then measures the $C_{2,1}$ register and gets a value y, disturbing the superposition. Indeed, a message x still present in the superposition must satisfy:

$$y = E_{h_1(\mathsf{k})}\left(\mathsf{droplast}\left(\mathsf{BC}_\mathsf{k}\left(c_0\right) \oplus x \oplus \left[(\mathsf{k}\|1) \cdot \mathsf{last}\left(\mathsf{BC}_\mathsf{k}\left(c_0\right) \oplus x\right)\right]\right)\right) \tag{17a}$$

$$\iff \mathsf{BC}_\mathsf{k}\left(c_0\right) \oplus x \oplus \left[(\mathsf{k}\|1) \cdot \mathsf{last}\left(\mathsf{BC}_\mathsf{k}\left(c_0\right) \oplus x\right)\right] = \begin{vmatrix} E^{-1}_{h_1(\mathsf{k})}(y)\Big\| 0 \\ \text{or} \\ E^{-1}_{h_1(\mathsf{k})}(y)\Big\| 1 \end{vmatrix}. \tag{17b}$$

However, we know that for all x, $\mathsf{last}(x \oplus [(\mathsf{k}\|1) \cdot \mathsf{last}(x)]) = 0$ holds. As such, a valid message x must satisfy:

$$\mathsf{BC}_\mathsf{k}\left(c_0\right) \oplus x \oplus \left[(\mathsf{k}\|1) \cdot \mathsf{last}\left(\mathsf{BC}_\mathsf{k}\left(c_0\right) \oplus x\right)\right] = E^{-1}_{h_1(\mathsf{k})}(y)\Big\| 0. \tag{17c}$$

We also have for any x, y:

$$x \oplus [(\mathsf{k}\|1) \cdot \mathsf{last}(x)] = y \iff \begin{cases} x = y & \text{if } \mathsf{last}(x) = 0 \\ x = y \oplus (\mathsf{k}\|1) & \text{if } \mathsf{last}(x) = 1 \end{cases}. \tag{17d}$$

As such, a message x still present within the superposition must satisfy:

$$\begin{vmatrix} \mathsf{BC}_\mathsf{k}\left(c_0\right) \oplus x = E^{-1}_{h_1(\mathsf{k})}(y)\Big\| 0 \\ \text{or} \\ \mathsf{BC}_\mathsf{k}\left(c_0\right) \oplus x = E^{-1}_{h_1(\mathsf{k})}(y)\Big\| 0 \oplus (\mathsf{k}\|1) \end{vmatrix}. \tag{17e}$$

Thus, the resulting state is, omitting the now measured $C_{2,1}$ register:

$$\begin{aligned} = \; & \left|\mathsf{BC}_\mathsf{k}\left(c_0\right) \oplus E^{-1}_{h_1(\mathsf{k})}(y)\Big\| 0\right\rangle_{M_1} \left|E^{-1}_{h_1(\mathsf{k})}(y)\Big\| 0\right\rangle_{C_1} \left|t_{h_2(\mathsf{k})}\left(E^{-1}_{h_1(\mathsf{k})}(y)\Big\| 0\right)\right\rangle_{C_{2,2}} + \\ & \left|\mathsf{BC}_\mathsf{k}\left(c_0\right) \oplus E^{-1}_{h_1(\mathsf{k})}(y)\Big\| 0 \oplus (\mathsf{k}\|1)\right\rangle_{M_1} \left|E^{-1}_{h_1(\mathsf{k})}(y)\Big\| 0 \oplus (\mathsf{k}\|1)\right\rangle_{C_1} \\ & \left|t_{h_2(\mathsf{k})}\left(E^{-1}_{h_1(\mathsf{k})}(y)\Big\| 0\right) \oplus 1\right\rangle_{C_{2,2}}. \end{aligned} \tag{18}$$

$\mathcal{A}$ now applies an $\mathbf{X}$ gate on M_1 controlled by C_1 in order to disentangle it, since it is now in the basis state $|\mathsf{BC}_\mathsf{k}\left(c_0\right)\rangle$. The state is thus now:

$$\begin{aligned} & \left|E^{-1}_{h_1(\mathsf{k})}(y)\Big\| 0\right\rangle_{C_1} \left|t_{h_2(\mathsf{k})}\left(E^{-1}_{h_1(\mathsf{k})}(y)\Big\| 0\right)\right\rangle_{C_{2,2}} + \\ & \left|E^{-1}_{h_1(\mathsf{k})}(y)\Big\| 0 \oplus (\mathsf{k}\|1)\right\rangle_{C_1} \left|t_{h_2(\mathsf{k})}\left(E^{-1}_{h_1(\mathsf{k})}(y)\Big\| 0\right) \oplus 1\right\rangle_{C_{2,2}}. \end{aligned} \tag{19}$$

Finally, $\mathcal{A}$ can perform an $\mathbf{X}$ gate on $C_{2,2}$ controlled by the last qubit of C_1. This results in the $C_{2,2}$ register now being disentangled from C_1, since it is now in the basis state $\left|t_{h_2(\mathsf{k})}\left(E^{-1}_{h_1(\mathsf{k})}(y)\Big\| 0\right)\right\rangle$. Hence, the state the adversary is left with is:

$$\left|E^{-1}_{h_1(\mathsf{k})}(y)\Big\| 0\right\rangle + \left|E^{-1}_{h_1(\mathsf{k})}(y)\Big\| 0 \oplus (\mathsf{k}\|1)\right\rangle. \tag{20}$$

The adversary is able to create such a state for each of their learning queries. In particular, they can now make use of Lemma 3 to recover $(\mathsf{k}\|1)$ and as such k. They are now able to easily win in the $\mathsf{qIND\text{-}qCPA\text{-}P11}$ game by performing a classical challenge query.

We now consider the case $\ell \geqslant 2$. The adversary can prepare the state:

$$\left(\bigotimes_{i=1}^{\ell-2} |0\rangle\right) \sum_x |x\rangle\,|0\rangle \tag{21}$$

and performs a learning request using it. They will then receive the state:

$$\left(\bigotimes_{i=1}^{\ell-2} |0\rangle\right) \sum_x |x\rangle\,|0\rangle \left(\bigotimes_{i=1}^{\ell-2} \left|\mathsf{BC}_\mathsf{k}^i\left(c_0\right)\right\rangle\right) \left|x \oplus \mathsf{BC}_\mathsf{k}^{\ell-1}\left(c_0\right)\right\rangle \left|\mathsf{BC}_\mathsf{k}\left(x \oplus \mathsf{BC}_\mathsf{k}^{\ell-1}\left(c_0\right)\right)\right\rangle \tag{22}$$

which we can rewrite, by omitting the first $\ell - 2$ messages and ciphertexts registers which are not entangled with the remaining of the state:

$$\sum_x |x\rangle\,|0\rangle \left|x \oplus \mathsf{BC}_\mathsf{k}^{\ell-1}\left(c_0\right)\right\rangle \left|\mathsf{BC}_\mathsf{k}\left(x \oplus \mathsf{BC}_\mathsf{k}^{\ell-1}\left(c_0\right)\right)\right\rangle. \tag{23}$$

This state is actually identical to the one described in Equation 16, excepting that we replaced $\mathsf{BC}_\mathsf{k}\left(c_0\right)$ by $\mathsf{BC}_\mathsf{k}^{\ell-1}\left(c_0\right)$. Since the previous attack worked for any c_0, $\mathcal{A}$ is able to perform the same attack despite the oracle forcing them to use $\ell \geqslant 2$ blocks. □

5.2 IND-qCPA security of CFB used with a qPRP

We show that Anand et al.'s proof for showing that CFB is $\mathsf{qIND\text{-}qCPA\text{-}P6}$ secure when used with a qPRP [1] can be adapted to show that it is also $\mathsf{qIND\text{-}qCPA\text{-}P10}$ secure. Similarly to their work, we also include the proof for the $\mathsf{qIND\text{-}qCPA\text{-}P10}$ security of CBC since they are very similar. We put the differences in brackets.

Theorem 4. *A system using a qPRP in CFB {CBC} mode is qIND-qCPA-P10 secure.*

Proof. We adapt Anand et al.'s proof [1] to the $\mathsf{qIND\text{-}qCPA\text{-}P10}$ security notion. In particular, $\mathcal{A}$ is allowed to perform their learning queries on an erasing oracle.

We begin by showing a very similar lemma to Anand et al.'s Lemma 6.

Lemma 4. *For a random permutation H, we define Enc^i as the function that returns $i+1$ blocks of randomness, including the IV c_0, and then behaves like a standard CFB {CBC} mode to compute the other blocks using H as its underlying block cipher. We stress that for $i = 0$, Enc^i is bijective, and as such can be implemented as an erasing oracle. Let b be a random bit. For every adversary $\mathcal{A}$ performing at most q quantum encryption queries, the following holds:*

$$\begin{aligned}&\left|\Pr\left[\mathcal{A}^{\mathsf{Enc}^0}\left(\mathsf{Enc}^i\left(M_b\right)\right) = b \;\middle|\; M_0, M_1 \leftarrow \mathcal{A}^{\mathsf{Enc}^0}\right] - \right.\\ &\left.\Pr\left[\mathcal{A}^{\mathsf{Enc}^0}\left(\mathsf{Enc}^{i+1}\left(M_b\right)\right) = b \;\middle|\; M_0, M_1 \leftarrow \mathcal{A}^{\mathsf{Enc}^0}\right]\right| \leqslant \mathcal{O}\left(\sqrt{\frac{\ell^3 q^3}{2^n}}\right).\end{aligned} \tag{24}$$

Proof. For simplicity, we denote $\mathsf{Enc} = \mathsf{Enc}^0$. We define:

$$\begin{aligned}\varepsilon(\lambda, n) \stackrel{\text{def}}{=} \big|\Pr\left[\mathcal{A}^{\mathsf{Enc}}\left(\mathsf{Enc}^i\left(M_b\right)\right) = b \;\middle|\; M_0, M_1 \leftarrow \mathcal{A}^{\mathsf{Enc}}\right] - \\ \Pr\left[\mathcal{A}^{\mathsf{Enc}}\left(\mathsf{Enc}^{i+1}\left(M_b\right)\right) = b \;\middle|\; M_0, M_1 \leftarrow \mathcal{A}^{\mathsf{Enc}}\right]\big|.\end{aligned} \tag{25}$$

Similarly to Anand et al.'s proof [1], we also define:

$$\widetilde{\mathsf{Enc}}^i\left(M, c_0, \cdots, c_i\right) = \hat{c}_0 \ldots \hat{c}_\ell \tag{26}$$

where $\hat{c}_j = c_j$ if $j \leqslant i$ and $\hat{c}_j = m_j \oplus H\left(\hat{c}_{j-1}\right)\ \{H\left(m_j \oplus \hat{c}_{j-1}\right)\}$ otherwise. We thus have, for $c_0, \ldots, c_{i+1}$ being uniformly random:

$$\begin{aligned}\varepsilon(\lambda, n) = \Big|\Pr\Big[\mathcal{A}^{\mathsf{Enc}}\left(\widetilde{\mathsf{Enc}}^i\left(M_b, c_0, \ldots, c_i\right)\right) = b \;\Big|\; M_0, M_1 \leftarrow \mathcal{A}^{\mathsf{Enc}}\Big] - \\ \Pr\Big[\mathcal{A}^{\mathsf{Enc}}\left(\widetilde{\mathsf{Enc}}^{i+1}\left(M_b, c_0, \ldots, c_{i+1}\right)\right) = b \;\Big|\; M_0, M_1 \leftarrow \mathcal{A}^{\mathsf{Enc}}\Big]\Big|.\end{aligned} \tag{27}$$

We can then replace c_i and c_{i+1} by respectively $x\ \left\{x \oplus m_b^{i+1}\right\}$ and $y \oplus m_b^{i+1}\ \{y\}$, where x and y are chosen uniformly at random, giving us the following value for $\varepsilon(\lambda, n)$:

$$\begin{aligned}\Big|\Pr\Big[\mathcal{A}^{\mathsf{Enc}}\left(\widetilde{\mathsf{Enc}}^i\left(M_b, c_0, \ldots, c_{i-1}, x\right)\right) = b \;\Big|\; M_0, M_1 \leftarrow \mathcal{A}^{\mathsf{Enc}}\Big] - \\ \Pr\Big[\mathcal{A}^{\mathsf{Enc}}\left(\widetilde{\mathsf{Enc}}^{i+1}\left(M_b, c_0, \ldots, c_{i-1}, x, y \oplus m_b^{i+1}\right)\right) = b \;\Big|\; M_0, M_1 \leftarrow \mathcal{A}^{\mathsf{Enc}}\Big]\Big|.\end{aligned} \tag{28}$$

$$\begin{aligned}\Big\{\Big|\Pr\Big[\mathcal{A}^{\mathsf{Enc}}\left(\widetilde{\mathsf{Enc}}^i\left(M_b, c_0, \ldots, c_{i-1}, x \oplus m_b^{i+1}\right)\right) = b \;\Big|\; M_0, M_1 \leftarrow \mathcal{A}^{\mathsf{Enc}}\Big] - \\ \Pr\Big[\mathcal{A}^{\mathsf{Enc}}\left(\widetilde{\mathsf{Enc}}^{i+1}\left(M_b, c_0, \ldots, c_{i-1}, x \oplus m_b^{i+1}, y\right)\right) = b \;\Big|\; M_0, M_1 \leftarrow \mathcal{A}^{\mathsf{Enc}}\Big]\Big|\Big\}.\end{aligned} \tag{28}$$

By definition of $\widetilde{\mathsf{Enc}}^{i+1}$, this is also equal to:

$$\begin{aligned}\Big|\Pr\Big[\mathcal{A}^{\mathsf{Enc}}\left(\widetilde{\mathsf{Enc}}^{i+1}\left(M_b, c_0, \ldots, c_{i-1}, x, H(x) \oplus m_b^{i+1}\right)\right) = b \;\Big|\; M_0, M_1 \leftarrow \mathcal{A}^{\mathsf{Enc}}\Big] - \\ \Pr\Big[\mathcal{A}^{\mathsf{Enc}}\left(\widetilde{\mathsf{Enc}}^{i+1}\left(M_b, c_0, \ldots, c_{i-1}, x, y \oplus m_b^{i+1}\right)\right) = b \;\Big|\; M_0, M_1 \leftarrow \mathcal{A}^{\mathsf{Enc}}\Big]\Big|.\end{aligned} \tag{29}$$

$$\begin{aligned}\Big\{\Big|\Pr\Big[\mathcal{A}^{\mathsf{Enc}}\left(\widetilde{\mathsf{Enc}}^{i+1}\left(M_b, c_0, \ldots, c_{i-1}, x, H(x)\right)\right) = b \;\Big|\; M_0, M_1 \leftarrow \mathcal{A}^{\mathsf{Enc}}\Big] - \\ \Pr\Big[\mathcal{A}^{\mathsf{Enc}}\left(\widetilde{\mathsf{Enc}}^{i+1}\left(M_b, c_0, \ldots, c_{i-1}, x, y \oplus m_b^{i+1}\right)\right) = b \;\Big|\; M_0, M_1 \leftarrow \mathcal{A}^{\mathsf{Enc}}\Big]\Big|\Big\}.\end{aligned} \tag{29}$$

Thus, similarly to Anand et al.'s proof, we can define the following adversary, which can interact with a standard {erasing} oracle implementing H:

Adversary $\mathcal{A}^{H}_{O2H}(x, y)$

$M_0,\ M_1 \leftarrow \mathcal{A}^{\mathsf{Enc}}$
$b \leftarrow \{0,1\}$
$c_0, \ldots, c_{i-1} \leftarrow \{0,1\}^n$
$c_i \ = \ x \ \left\{x \oplus \ m_b^{i+1}\right\}$
$c_{i+1} \ = \ y \oplus m_b^{i+1} \ \{y\}$
for j **in** $[\![j+2\,;\,\ell]\!]$
  $c_j \ = \ m_b^j \oplus H\left(c_{j-1}\right) \ \left\{H\left(m_b^j \oplus \ c_{j-1}\right)\right\}$
$b' \leftarrow \mathcal{A}^{\mathsf{Enc}}\left(c_0 \cdots \ c_\ell\right)$
return $b = b'$

We now show that $\mathcal{A}_{O2H}$ is able to answer $\mathcal{A}$'s queries, since they are able to implement an erasing oracle implementing H.

$\mathcal{A}_{O2H}$ uses a standard oracle to create c_k from c_{k-1} by simply feeding c_{k-1} and m_k to the standard oracle, which results in leaving the first register unchanged and the second one in the state $|m_k \oplus H\left(c_{k-1}\right)\rangle$, which is c_k by definition.

{$\mathcal{A}_{O2H}$ uses an erasing oracle to create c_k from c_{k-1} by applying an $\mathbf{X}$ gate on m_k controlled by c_{k-1}, and then feeds this register to the erasing oracle, resulting in the state $|H\left(m_k \oplus c_{k-1}\right)\rangle$, which is c_k by definition.}

We denote q_{O2H} the number of queries to H that this adversary performs. For each query that $\mathcal{A}$ performs to compute M_0 and M_1, $\mathcal{A}_{O2H}$ performs ℓ queries to H. They will then perform $\ell - i - 1$ requests to H in order to compute the ciphertext, and finally will answer $\mathcal{A}$'s queries one more time. All in all, $\mathcal{A}_{O2H}$ performs at most $(q+1)\ell - i - 1$ queries to H. Similarly to Anand et al.'s proof [1], we respectively denote q_1, q_2 and q_3 the number of queries performed by $\mathcal{A}_{O2H}$ before, during and after the challenge query. $\varepsilon(\lambda, n)$ is then easily seen to be:

$$\varepsilon(\lambda, n) = \left|\Pr\left[\mathcal{A}^{H}_{O2H}(x, H(x)) = 1\right] - \Pr\left[\mathcal{A}^{H}_{O2H}(x, y) = 1\right]\right| \tag{30}$$

with x and y being chosen uniformly at random. This allows us to use the O2H lemma. We thus consider the adversary $\mathcal{B}$ associated to $\mathcal{A}_{O2H}$ as defined in the lemma and denote the number of the query during which $\mathcal{B}$ measures $\mathcal{A}_{O2H}$'s input register by j and the associated probability by $P^j_{\mathcal{B}}$.

If $j \leqslant q_1$: In this case, the challenge query hasn't yet been performed by $\mathcal{A}$. As such, $\mathcal{A}$ does not know the arguments x and y using which $\mathcal{A}_{O2H}$ has been instantiated. Thus, its queries are independent from those parameters and we have, by denoting $(\mathcal{M} = z)$ the event where $\mathcal{B}$'s measure of $\mathcal{A}_{O2H}$'s

register results in the string z:

$$P_{\mathcal{B}}^{j} = \Pr\left[[\mathcal{B}(x,y) = x] \cup \left[\mathcal{B}(x,y) = H^{-1}(y)\right] \;\middle|\; j \leqslant q_1\right] \tag{31a}$$

$$\leqslant \sum_{x'=0}^{2^n-1} \Pr[\mathcal{M} = x' \mid j \leqslant q_1, x' = x]\frac{1}{2^n} + \sum_{y'=0}^{2^n-1} \Pr\left[\mathcal{M} = y' \;\middle|\; j \leqslant q_1, y' = H^{-1}(y)\right]\frac{1}{2^n} \tag{31b}$$

$$\leqslant \frac{1}{2^{n-1}}. \tag{31c}$$

If $q_1 < j \leqslant q_1 + q_2$: In this case, the previous reasoning still applies to x, we thus have:

$$P_{\mathcal{B}}^{j} \leqslant \frac{1}{2^n} + \frac{1}{2^n}\sum_{y'=0}^{2^n-1} \Pr\left[\mathcal{M} = y' \;\middle|\; q_1 < j \leqslant q_2, y' = H^{-1}(y)\right]. \tag{32}$$

In this case however, $\mathcal{A}_{O2H}$ performs their queries with inputs depending on y. Note that the first query done to H is $y \oplus m_b^{i+1}$. Since $\mathcal{A}$ does not know y when performing their challenge query, y and m_b^{i+1} are independent, which means that $y \oplus m_b^{i+1}$ is uniformly random, since y is uniformly random. Using a similar reasoning, each other query on H can be written as $m_b^k \oplus H\left(c_{k-1}\right)$ $\left\{m_b^k \oplus c_{k-1}\right\}$, with c_{k-1} being uniformly random and independent from m_b^k. Every string has thus the same probability to be measured, even being given that $y' = H^{-1}(y)$. This is thus similar to the previous case and we have:

$$P_{\mathcal{B}}^{j} \leqslant \frac{1}{2^{n-1}}. \tag{33}$$

If $q_1 + q_2 < j$: In this case, the query is performed after $\mathcal{A}$ has received the challenge query. Note that we can use a similar reasoning to Anand et al.'s one to argue that we can consider the queries as being classical. Indeed, as described above, $\mathcal{A}_{O2H}$ only applies permutation matrices on the state they receive from $\mathcal{A}$. We can thus move the measurement performed by $\mathcal{B}$ before the first call to H to answer $\mathcal{A}$'s query, which allows us to consider this query classical.

Like the previous case, the queries performed on H can be written as $m_b^k \oplus H\left(c_{k-1}\right)\left\{m_b^k \oplus c_{k-1}\right\}$. For $k = 1$, it is obvious that this quantity is uniformly random, since c_0 is chosen independently of m_b^1. We thus now only have to show that for c_{k-1} being uniformly random, $m_b^k \oplus H\left(c_{k-1}\right)\left\{m_b^k \oplus c_{k-1}\right\}$ is also uniformly random. It is for this enough to show that $\mathcal{A}$ did not get to know $H\left(c_{k-1}\right)\left\{H\left(m_b^{k-1} \oplus c_{j-2}\right)\right\}$. Since H is a random permutation queried at most q_{O2H} times, $\mathcal{A}$ got to know this value with probability at most $\frac{q_{O2H}}{2^n}$. We can actually do better by arguing that this probability upper-bounds the one that at least one of the queries to H isn't uniformly random. In order to upper-bound $P_{\mathcal{B}}^{j}$, we consider the trivial upper-bound in the case

where $\mathcal{A}$ learned at least one such value, which happens with probability at most $\frac{q_{O2H}}{2^n}$, with 1. The other case is similar to the previous ones, which means that $\mathcal{B}$ will return x or $H^{-1}(y)$ with probability $\frac{1}{2^n}$. We upper-bound the probability of being in this case by the trivial upper-bound, that is 1. All in all, the following holds:

$$P_{\mathcal{B}}^{j} \leqslant \frac{1}{2^n} + \frac{q_{O2H}}{2^n}. \tag{34}$$

Now, we can use the previous upper-bound for every j, which ensures that:

$$P_{\mathcal{B}}^{j} = \sum_{j=1}^{q_{O2H}} P_{\mathcal{B}}^{j} \frac{1}{q_{O2H}} \leqslant \frac{1 + q_{O2H}}{2^n}. \tag{35}$$

Finally, we have, according to the O2H lemma:

$$\varepsilon(\lambda, n) \leqslant 2q_{O2H}\sqrt{\frac{1 + q_{O2H}}{2^n}} = \mathcal{O}\left(\sqrt{\frac{\ell^3 q^3}{2^n}}\right). \tag{36}$$

□

We can now use this lemma to show the $\mathsf{qIND\text{-}qCPA\text{-}P10}$ security of CFB. Since the underlying block cipher is a qPRP, we can replace it with a truly random permutation H while only increasing $\mathcal{A}$'s advantage by a negligible amount. Using triangle inequality and the previous lemma, the following then holds:

$$\begin{aligned}
&\left|\Pr\left[\mathcal{A}^{\mathsf{Enc}}\left(\mathsf{Enc}\left(M_b\right)\right) = b \;\middle|\; M_0, M_1 \leftarrow \mathcal{A}^{\mathsf{Enc}}\right] - \right. \\
&\left.\Pr\left[\mathcal{A}^{\mathsf{Enc}}\left(\mathsf{Enc}^{\ell}\left(M_b\right)\right) = b \;\middle|\; M_0, M_1 \leftarrow \mathcal{A}^{\mathsf{Enc}}\right]\right| && \text{(37a)} \\
&\leqslant \sum_{i=0}^{\ell-1} \left[\left|\Pr\left[\mathcal{A}^{\mathsf{Enc}}\left(\mathsf{Enc}\left(M_b\right)\right) = b \;\middle|\; M_0, M_1 \leftarrow \mathcal{A}^{\mathsf{Enc}}\right] - \right.\right. \\
&\left.\left.\Pr\left[\mathcal{A}^{\mathsf{Enc}}\left(\mathsf{Enc}^{\ell}\left(M_b\right)\right) = b \;\middle|\; M_0, M_1 \leftarrow \mathcal{A}^{\mathsf{Enc}}\right]\right|\right] && \text{(37b)} \\
&\leqslant \mathcal{O}\left(\sqrt{\frac{\ell^5 q^3}{2^n}}\right). && \text{(37c)}
\end{aligned}$$

$\Pr\left[\mathcal{A}^{\mathsf{Enc}}\left(\mathsf{Enc}^{\ell}\left(M_b\right)\right) = b \;\middle|\; M_0, M_1 \leftarrow \mathcal{A}^{\mathsf{Enc}}\right]$ is easily seen to be equal to $\frac{1}{2}$, since in this setup we returned to the adversary a uniformly random string that is independent of their challenge query. This allows us to upper-bound $\mathcal{A}$'s advantage:

$$\mathsf{Adv}^{\mathsf{qind\text{-}qcpa\text{-}p13}}_{\mathcal{A},\mathsf{CFB}}(\lambda) \leqslant \mathcal{O}\left(\sqrt{\frac{\ell^5 q^3}{2^n}}\right) + \mathsf{negl}(\lambda) \tag{38}$$

where $\mathsf{negl}(\lambda)$ is $\mathcal{A}$'s advantage in distinguishing the underlying block cipher from a truly random permutation. ℓ and n being polynomial in λ, this ensures that $\mathcal{A}$'s advantage is negligible with respect to λ. □

5.3 qIND-qCPA-P13 insecurity of CFB

Now that the IND-qCPA security notions have been dealt with, we only have to show that CFB is qIND-qCPA-P13 insecure, even if the underlying block cipher is a qPRP.

Theorem 5. *CFB is qIND-qCPA-P13 insecure, no matter what the underlying block cipher is.*

Proof. $\mathcal{A}$ prepares the following state:

$$\left(\bigotimes_{k=0}^{\ell-1}|0\rangle\right)\sum_{x}|x\rangle \tag{39}$$

and performs their challenge query using it. If $b=0$, the adversary receives:

$$\left(\bigotimes_{k=0}^{\ell-1}|0\rangle\right)\sum_{x}|x\rangle\left(\bigotimes_{i=1}^{\ell-1}\left|E^i\left(c_0\right)\right\rangle\right)\left|x\oplus E_{\mathsf{k}}^{\ell}\left(c_0\right)\right\rangle \tag{40}$$

while they will get, if $b=1$ for a random permutation π:

$$\left(\bigotimes_{k=0}^{\ell-1}|0\rangle\right)\sum_{x}|x\rangle\bigotimes_{i=1}^{\ell}\left|\pi_{(i-1)n\to in-1}(0\|\cdots\|0\|x)\oplus E_{\mathsf{k}}\left(c_{i-1}(x)\right)\right\rangle \tag{41}$$

where c_0 is a random constant function and where we have defined:

$$c_i(x)=\pi_{(i-1)n\to in-1}(0\|\cdots\|0\|x)\oplus E_{\mathsf{k}}\left(c_{i-1}(x)\right). \tag{42}$$

By performing an $\mathbf{X}$ gate on the second register controlled by the first one, the state becomes, if $b=0$:

$$\left(\bigotimes_{k=0}^{\ell-1}|0\rangle\right)\sum_{x}|x\rangle\left(\bigotimes_{i=1}^{\ell-1}\left|E^i\left(c_0\right)\right\rangle\right)\left|E_{\mathsf{k}}^{\ell}\left(c_0\right)\right\rangle \tag{43}$$

while it becomes, if $b=1$:

$$\left(\bigotimes_{k=0}^{\ell-1}|0\rangle\right)\sum_{x}|x\rangle\left|f_{c_0,\pi}(x)\right\rangle \tag{44}$$

with $f_{c_0,\pi}$ being defined as:

$$f_{c_0,\pi}(x)=x\mapsto c_1(x)\|\cdots\|c_{\ell-1}(x)\|(x\oplus c_\ell(x))\,. \tag{45}$$

Thus, if $b=0$, the two registers are not entangled: applying an $\mathbf{H}$ gate on the first register and measuring it yields $|0\rangle$ with certainty. If $b=1$ however, such a procedure yields $|0\rangle$ with negligible probability. We can use for this the Lemma 1. The probability to measure $|0\rangle$ if $b=1$ is thus given by:

$$\Pr[|0\rangle\mid b=1]=\frac{1}{2^{2n}}\sum_{y}\left|f_{c_0,\pi}^{-1}(y)\right|^2. \tag{46}$$

The following is an adaptation of the proof proposed by Iosif Pinelis [14].

We have, for a given y:

$$\left|f_{c_0,\pi}^{-1}(y)\right| = \sum_x \mathbb{1}_{f_{c_0,\pi}(x)=y} \tag{47}$$

thus:

$$\left|f_{c_0,\pi}^{-1}(y)\right|^2 = \sum_{x_1}\sum_{x_2} \mathbb{1}_{[f_{c_0,\pi}(x_1)=y]\cap[f_{c_0,\pi}(x_2)=y]} \tag{48}$$

thus:

$$\begin{aligned}
\mathbb{E}\left[\left|f_{c_0,\pi}^{-1}(y)\right|^2\right] &= \sum_{x_1}\sum_{x_2} \Pr[[f_{c_0,\pi}(x_1)=y]\cap[f_{c_0,\pi}(x_2)=y]] && \text{(49a)}\\
&= \sum_{x_1} \Pr[f_{c_0,\pi}(x_1)=y] + \\
&\quad \sum_{x_1}\sum_{x_2\neq x_1} \Pr[[f_{c_0,\pi}(x_1)=y]\cap[f_{c_0,\pi}(x_2)=y]]. && \text{(49b)}
\end{aligned}$$

Since π is a random permutation, $\pi(x)$ is uniformly random. As such, any bitslice $\pi_{(i-1)n\to(in-1)}(x)$ is also uniformly random. Note also that it is independent from $E_{\mathsf{k}}(c_{i-1}(x))$, thus every $c_i(x)$ is uniformly random. This property does not depend on its input, hence this remains true for $x \oplus c_\ell(x)$. As a consequence, f is uniformly random and we have:

$$\mathbb{E}\left[\left|f_{c_0,\pi}^{-1}(y)\right|^2\right] = \frac{2^n}{2^{\ell n}} + \frac{1}{2^{\ell n}}\sum_{x_1}\sum_{x_2\neq x_1} \Pr[f_{c_0,\pi}(x_2)=y \mid f_{c_0,\pi}(x_1)=y]. \tag{49c}$$

Since the value of $f_{c_o,\pi}(x_1)$ is known, it means that $\pi(x_1)$ has been specified. As such, $\pi(x_2)$ can be equal to any value except $\pi(x_1)$.

Note that the probability that we want to compute is the probability that $c_i(x_1) = c_i(x_2)$ for $i \in [\![1\,;\ell-1]\!]$ and that $c_\ell(x_1)\oplus x_1 = c_i(x_2)\oplus x_2$. Using the definition of c_i, this is equivalent to computing the probability that $\pi(x_1)$ and $\pi(x_2)$ have the same $(\ell-1)n$ first bits and that their last n bits XOR up to $x_1 \oplus x_2$. The probability of the first event is $\frac{2^n-1}{2^{\ell n}}$, since we can freely choose the last n bits of $\pi(x_2)$ as long as they are not equal to those of $\pi(x_1)$, and the probability for the second event being given the first one is $\frac{1}{2^n-1}$ using the same reasoning. All in all, we have:

$$\mathbb{E}\left[\left|f_{c_0,\pi}^{-1}(y)\right|^2\right] = \frac{2^n}{2^{\ell n}} + \frac{1}{2^{\ell n}}\sum_{x_1}\sum_{x_2\neq x_1}\frac{1}{2^{\ell n}-1} = \frac{2^n}{2^{\ell n}} + \frac{2^n(2^n-1)}{2^{\ell n}(2^{\ell n}-1)}. \tag{49d}$$

Thus, the probability of measuring $|0\rangle$ being given that $b=1$ is given by:

$$\Pr[|0\rangle \mid b=1] = \frac{1}{2^{2n}}\sum_y\left(\frac{2^n}{2^{\ell n}} + \frac{2^n(2^n-1)}{2^{\ell n}(2^{\ell n}-1)}\right) = \frac{1}{2^n}\left(1 + \frac{2^n-1}{2^{\ell n}-1}\right). \tag{50}$$

Thus, $\mathcal{A}$'s advantage is given by:

$$\mathsf{Adv}^{\mathsf{qind\text{-}qcpa\text{-}p13}}_{\mathcal{A},\mathsf{CFB}}(\lambda) = 1 - \frac{1}{2^n}\left(1 + \frac{2^n - 1}{2^{\ell n} - 1}\right). \tag{51}$$

In particular, this advantage is not negligible with respect to λ. □

6 qIND-qCPA security of CBC

In this section, we show that when used with a PRP, CBC is potentially insecure with respect to every qIND-qCPA notion except the IND-CPA one. In order to show this, we show that it may be possible to recover the key of the underlying block cipher using a single query to an embedding oracle with high probability. For this, we use the same block cipher as Anand et al.. This allows us to prove that CBC used with a PRP is potentially qIND-qCPA-P11 and qIND-qCPA-P13 insecure. Since every security notion but the IND-CPA one implies either the qIND-qCPA-P11 one or the qIND-qCPA-P13 one [4], this fully characterizes the security of CBC when used with a PRP.

Once done, we show that CBC is qIND-qCPA-P10 and qIND-qCPA-P5 secure when used with a qPRP and qIND-qCPA-P9 insecure, no matter what the underlying block cipher is, which fully characterizes it.

6.1 Potential IND-qCPA and qIND-qCPA-P13 insecurity of CBC used with a PRP

Theorem 6. *There is a PRP such that the system using it as a block cipher in CBC mode is qIND-qCPA-P13 insecure.*

Proof. As a recall, in the qIND-qCPA-P13 security notions, the adversary is allowed to perform their learning queries on a classical oracle, while their single challenge query must be done using an embedding one. Our goal is to show that using a specific block cipher, which has been shown to be a PRP by Anand et al. [1], the adversary is able to recover the secret key using their challenge query. Note that it is important to consider that even if the adversary manages to get the secret key using their challenge request, they also have to use the same challenge request to determine whether they are in the real world or in the random one.

We use the same flawed block cipher BC_k as Anand et al. [1], that is the one which maps a λ-bit string x to:

$$E_{h_1(\mathsf{k})}\left[\mathsf{droplast}\left[x \oplus \left[(\mathsf{k}\|1) \cdot \mathsf{last}(x)\right]\right]\right] \| \left[t_{h_2}(\mathsf{k})\left[x \oplus \left[(\mathsf{k}\|1) \cdot \mathsf{last}(x)\right]\right] \oplus \mathsf{last}(x)\right].$$

We assume that ℓ can be written as $\ell = K(\lambda - 1) + m$ for $K \geqslant 1$. We denote $L = K(\lambda - 1)$. The adversary prepares the following state:

$$\left(\bigotimes_{i=1}^{m} |0\rangle\right) \bigotimes_{k=1}^{L} |+\rangle_{M_k} \tag{52}$$

and performs their challenge query using it. Let us consider the case $b = 0$. In this case, no permutation is applied on $\mathcal{A}$'s input. The adversary measures the m first registers and gets their value C_i for $i \in [\![1\,;\,m]\!]$. Omitting the m first registers which are not entangled with the remaining of the state, the adversary is now left with the state:

$$\sum_{x_1,\cdots,x_L} |x_1\rangle_{M_1} \cdots |x_L\rangle_{M_L} \bigotimes_{k=1}^{L} |\mathsf{droplast}\left(\mathsf{BC_k}\left(C_{m+k-1} \oplus x_k\right)\right)\rangle_{C_{m+k,1}} \\ |\mathsf{last}\left(\mathsf{BC_k}\left(C_{m+k-1} \oplus x_k\right)\right)\rangle_{C_{m+k,2}} \tag{53}$$

where we have defined $C_i = C_{i,1} \| C_{i,2}$. $\mathcal{A}$ now measures all the $C_{k,1}$ registers and gets their respective value y_k, disturbing the superposition. By the principles of quantum mechanics, it is equivalent to consider that $\mathcal{A}$ successively measures each $C_{k,1}$, starting from $k = 1$. We show that the resulting state is:

$$\bigotimes_{k=1}^{L} \left(|x_k\rangle_{M_k} |0\rangle_{C_{m+k,2}} + |x_k \oplus (\mathsf{k}\|1)\rangle_{M_k} |1\rangle_{C_{m+k,2}} \right) \tag{54}$$

for some $(x_k)_{k \in [\![1\,;\,L]\!]}$.

Let us consider the measurement of $C_{m+k,1}$. Note that at this point, since C_{m+k-1} has been measured, the register $C_{m+k,2}$ is only entangled with x_k. The messages x_k still present in the superposition must verify:

$$C_{m+k,1} = E_{h_1(\mathsf{k})}\left(\mathsf{droplast}\left(C_{m+k-1} \oplus x_1 \oplus [(\mathsf{k}\|1) \cdot \mathsf{last}\left(C_{m+k-1} \oplus x_1\right)]\right)\right). \tag{55}$$

This equation is actually the same as the Equation 17a. We can thus apply the same result and state that two messages x_1 are still present within the superposition, with their `XOR` being equal to $\mathsf{k}\|1$. Since $\mathsf{BC_k}$ can be inverted, these two messages cannot be mapped to the same ciphertext. As such, the last bit of the ciphertext, which is present in $C_{m+k,2}$, has to be different, since the $n-1$ other bits are equal. Without loss of generality, we call x_1 the message associated with the last bit 0. Since M_k and $C_{m+k,2}$ are not entangled with any other register, we can apply the same reasoning to any register and write out the result as a tensor product, which is the state described in Equation 54.

The adversary can now apply an $\mathbf{X}$ gate on $C_{m+k,2}$ controlled by the last bit of M_k for every k (which is a polynomial number of operation with respect to λ), effectively disentangling them from the input registers and measures them. The adversary is thus left with the state:

$$\bigotimes_{k=1}^{L} \left(|x_k\rangle_{M_k} + |x_k \oplus (\mathsf{k}\|1)\rangle_{M_k} \right) \tag{56}$$

which can be seen as $L = K(\lambda - 1)$ independent states. $\mathcal{A}$ can thus make use of Lemma 3 to recover k with probability at least $1 - \left(\frac{3}{4}\right)^K$. If they don't manage

to recover it, they return $b = 0$ with probability $\frac{1}{2}$. $\mathcal{A}$ can then check using the key they just got that:

$$\forall i \in [\![1\,;\,m]\!]\,, \mathsf{BC}_{\mathsf{k}}^{i}\left(C_0\right) = C_i \tag{57}$$

and returns $b = 0$ if that's the case and $b = 1$ otherwise. All in all, the probability that $\mathcal{A}$ wins if $b = 0$ is at least $1 - \left(\frac{3}{4}\right)^K + \frac{1}{2}\left(\frac{3}{4}\right)^K$.

We now consider the case $b = 1$. Using the previous strategy, we can make a simpler reasoning to lower-bound the probability of $\mathcal{A}$ winning in that case. The adversary manages to get a key with probability $1 - \left(\frac{3}{4}\right)^K$ and returns $b = 1$ with probability $\frac{1}{2}$ otherwise. If $\mathcal{A}$ managed to get a key k', the probability that $\mathcal{A}$ returns $b = 0$ in that case is equal to the probability that every C_i matches the value it would have had without the application of the random permutation π. That is, we want that $\mathsf{BC}_{\mathsf{k}'}\left(C_i\right) = \mathsf{BC}_{\mathsf{k}}\left(C_i \oplus \pi_{i(n-1)\to in-1}(M)\right)$ for every $i \in [\![0\,;\,m-1]\!]$. We can compute this probability by assuming that $\mathcal{A}$ first checks for the equality for $i = 0$, then for $i = 1$, etc... Let us consider the case $i = 0$ for now. We have that:

$$\mathsf{BC}_{\mathsf{k}'}\left(C_0\right) = \mathsf{BC}_{\mathsf{k}}\left(C_0 \oplus \pi_{0\to n-1}(M)\right) \iff \pi_{0\to n-1}(M) = C_0 \oplus \mathsf{BC}_{\mathsf{k}}^{-1}\left(\mathsf{BC}_{\mathsf{k}'}\left(C_0\right)\right) \tag{58}$$

which, since π is a random permutation, has a probability of happening equal to $\frac{2^{(m-1)n}}{2^{mn}}$, that is $\frac{1}{2^n}$. If we assume this to be true, we can now compute the probability that $\mathsf{BC}_{\mathsf{k}'}\left(C_1\right) = \mathsf{BC}_{\mathsf{k}}\left(C_1 \oplus \pi_{n\to 2n-1}(M)\right)$. Note that the exact same reasoning can be performed here, since C_0 played no role in it. As such, the probability of the adversary returning 0 in this case is equal to $\frac{1}{2^{mn}}$. Note that this probability is independent of whether $\mathcal{A}$ managed to get the right key.

Thus, the probability that $\mathcal{A}$ wins if $b = 1$ is at least $\left[1 - \left(\frac{3}{4}\right)^K\right]\left(1 - \frac{1}{2^{mn}}\right) + \frac{1}{2}\left(\frac{3}{4}\right)^K$.

Hence, the following holds about $\mathcal{A}$'s advantage:

$$\mathsf{Adv}^{\mathsf{qind\text{-}qcpa\text{-}p13}}_{\mathcal{A},\mathsf{CBC}}(\lambda) \geqslant \left[1 - \left(\frac{3}{4}\right)^K\right]\left(1 - \frac{1}{2^{mn}}\right). \tag{59}$$

In particular, this advantage is not negligible with respect to λ. □

The previous proof showed that it is possible to recover the key of this specific PRP when used in CBC mode using a single embedding query. Note that the assumption according to which the number of blocks the oracle accepts has to be greater than or equal to λ is not necessary in a setup where the adversary is allowed to perform several embedding learning queries. As a direct consequence, CBC used with said block cipher is qIND-qCPA-P11 insecure, since this security notion allows the adversary to perform learning queries using such an oracle.

Theorem 7. *There is a PRP such that the system using it as a block cipher in CBC mode is qIND-qCPA-P11 insecure.*

Furthermore, a similar attack can be pulled off against CFB. While we do not write down explicitly the attack for clarity's sake, this can be seen using the similarity of Equations 17a and 55.

6.2 IND-qCPA security of CBC used with a qPRP

The qIND-qCPA-P10 security of CBC used with a qPRP has been shown in Section 5.2.

Theorem 8. *A system using a qPRP in CBC mode is qIND-qCPA-P10 secure.*

6.3 qIND-qCPA-P5 security of CBC used with a qPRP

We now show that CBC used with a qPRP is qIND-qCPA-P5 secure. The definition of the qIND-qCPA-P5 notion is given below.

Definition 9 (qIND-qCPA-P5 game, adapted from [4]). *In this notion, the adversary is allowed to perform their learning queries on a classical oracle and can perform as much challenge queries as they want on an embedding oracle.*

Theorem 9. *A system using a qPRP in CBC mode is qIND-qCPA-P5 secure.*

Proof. We show that we can reduce the qIND-qCPA-P5 security of a qPRP used in CBC mode to its IND-CPA security, in which we know that CBC is secure [1].

The IND-CPA security is identical to the qIND-qCPA-P5 security, with the exception that the challenge queries have to be classical. All in all, our goal is to show that measuring the adversary's input registers during their challenge queries only leads to an increase by a negligible amount of their advantage. By doing so, the challenge queries could be considered classical.

Since E_k is a qPRP, we can replace it with a truly random permutation π while only increasing $\mathcal{A}$'s advantage by a negligible amount, since it is possible to implement $\mathsf{Enc}^{\mathsf{CBC}}_{E_\mathsf{k},c_0,\ell}$ by having a standard oracle access to E_k.

Let us consider a challenge query made by the adversary. The encryption oracle can be described on the basis states as:

$$\mathsf{Enc}^{\mathsf{CBC}}_{\pi,c_0,\ell} \bigotimes_{i=1}^{\ell} \left(|m_i\rangle\,|0\rangle\right) = \bigotimes_{i=1}^{\ell} |m_i\rangle\,|c_i\rangle \tag{60a}$$

with:

$$c_i = \pi\left(m_i \oplus c_{i-1}\right). \tag{60b}$$

Note that for simplicity, we didn't explicitly write the application of a potential random permutation on the input, since our goal is to show that we can define a new encryption oracle that behaves identically to the aforementioned encryption oracle on the basis states, which is a fact independent on the application of such a random permutation beforehand.

We can show that we can decompose this encryption into two steps: encrypting the first block, and encrypting the remaining ones. Hence, we can rewrite the encryption oracle as:

$$\mathsf{Enc}^{\mathsf{CBC}}_{\pi,c_0,\ell} = \left(\mathbf{I}_1 \otimes \mathsf{Enc}^{\mathsf{CBC}}_{\pi,c_1,\ell-1}\right)\left(\boldsymbol{\Pi} \otimes \mathbf{I}_{\ell-1}\right) \tag{61}$$

where $\boldsymbol{\Pi}$ is an embedding oracle implementing the function $x \mapsto \pi(x \oplus c_0)$, $\mathbf{I}_p$ is the identity matrix applied on p input-output blocks and c_1 is the resulting ciphertext register produced by Π. Indeed, on a basis state, we have:

$$(\Pi \otimes \mathbf{I}_{\ell-1}) \bigotimes_{i=1}^{\ell} (|m_i\rangle |0\rangle) = |m_1\rangle |c_1\rangle \bigotimes_{i=2}^{\ell} (|m_i\rangle |0\rangle) \tag{62a}$$

and:

$$\left(\mathbf{I}_1 \otimes \mathsf{Enc}^{\mathsf{CBC}}_{\pi,\ell-1}\right) |m_1\rangle |c_1\rangle \bigotimes_{i=2}^{\ell} (|m_i\rangle |0\rangle) = |m_1\rangle |c_1\rangle \bigotimes_{i=2}^{\ell} (|m_i\rangle |c_i\rangle). \tag{62b}$$

Since they are identical on the basis states, these two oracles are indeed equal. Now, we know that $\boldsymbol{\Pi}$ is an embedding oracle implementing the random injective function $x \mapsto \pi(x \oplus c_0)$. As such, we can use [4, Corollary 11] to apply a measurement on its input while increasing the adversary's advantage by only a negligible quantity in the size of the quantum registers, which is assumed to be polynomial in λ.

Thus, we can consider that the first block to be encrypted is in fact a classical value, since we can apply a measurement onto it before encrypting it. By induction, we can thus apply a measurement on any input block by increasing $\mathcal{A}$'s advantage by only a negligible amount, which effectively reduces the qIND-qCPA-P5 security of the scheme to its IND-CPA security. □

6.4 qIND-qCPA-P9 insecurity of CBC

We now only need to show that CBC is qIND-qCPA-P9 insecure to fully characterize it. The definition of the qIND-qCPA-P9 notion is given below.

Definition 10 (qIND-qCPA-P9 game, adapted from [4]). *In this notion, the adversary is allowed to perform their learning queries on a classical oracle and can perform a single challenge query on an erasing oracle.*

Theorem 10. *CBC is qIND-qCPA-P9 insecure, no matter what the underlying block cipher is.*

Proof. $\mathcal{A}$ prepares the following state:

$$\left(\bigotimes_{i=1}^{\ell-1} |0\rangle\right) \sum_x |x\rangle \tag{63}$$

and performs its challenge query using it. If $b = 0$, the adversary receives:

$$\left(\bigotimes_{i=1}^{\ell-1} \left|E^i_{\mathsf{k}}(c_0)\right\rangle\right) \sum_x \left|E_{\mathsf{k}}\left(x \oplus E^{\ell-1}_{\mathsf{k}}(c_0)\right)\right\rangle \tag{64}$$

while they will get, if $b = 1$ for a random permutation π:

$$\sum_{x} \bigotimes_{i=1}^{\ell} |E_{\mathsf{k}}\left(c_{i-1}(x)\right)\rangle \tag{65}$$

where c_0 is a random constant function and where we have defined:

$$c_i(x) = E_{\mathsf{k}}\left(c_{i-1}(x) \oplus \pi_{(i-1)n \to in-1}(0\| \cdots \|0\|x)\right). \tag{66}$$

$\mathcal{A}$ then measures the $\ell - 1$ first registers, applies an $\mathbf{H}$ gate on the last one and finally measures it. If $b = 0$, the $\ell - 1$ first registers are not entangled with the last one. As such, measuring them won't affect it, and measuring it after having applied an $\mathbf{H}$ gate will yield $|0\rangle$ with probability 1, since the state of the last register is the uniform superposition. This is due to the fact that both functions that are subsequently applied on x, which are $x \mapsto x \oplus E_{\mathsf{k}}^{\ell-1}(c_0)$ and E_{k} are bijective.

Let us now consider the case $b = 1$. Measuring the $\ell - 1$ first registers make the system collapse to a superposition over the possible x. Let us denote c_i the value that the adversary got by measuring the i-th register. For every x still present within the superposition, the following equations must hold:

$$\forall i \in [\![0\,;\,\ell-1]\!]\,, \pi_{in \to (i+1)n-1}(0\| \cdots \|0\|x) = c_i \oplus E_{\mathsf{k}}^{-1}\left(c_{i+1}\right). \tag{67}$$

Since $\pi_{in \to (i+1)n-1}(0\| \cdots \|0\|x)$ is uniformly random, each x has a probability $\frac{1}{2^{\ell n}}$ to still be in the superposition. We denote M the number of such x. Hence, M follows a binomial distribution with parameters 2^n and $\frac{1}{2^{\ell n}}$. As such:

$$\Pr[M = 1 \mid M \geqslant 1] = \frac{2^n \frac{1}{2^{\ell n}} \left(1 - \frac{1}{2^{\ell n}}\right)^{2^n - 1}}{1 - \left(1 - \frac{1}{2^{\ell n}}\right)^{2^n}}. \tag{68}$$

For $\ell \geqslant 2$, the following holds:

$$1 - \left(1 - \frac{1}{2^{\ell n}}\right)^{2^n} = \frac{1}{2^{(\ell-1)n}} - \frac{1}{2^{(2\ell-2)n}} + \mathrm{o}\left(\frac{1}{2^{(2\ell-2)n}}\right) \tag{69}$$

which ensures that:

$$\Pr[M = 1 \mid M \geqslant 1] = 1 - \frac{1}{2^{(\ell-1)n+1}} + \mathrm{o}\left(\frac{1}{2^{(\ell-1)n}}\right). \tag{70}$$

Applying an $\mathbf{H}$ gate on a state containing only a single basis state and measuring it yields $|0\rangle$ with probability $\frac{1}{2^n}$. Thus, the probability that $\mathcal{A}$ wins when $b = 1$ is larger than $\left[1 - \frac{1}{2^{(\ell-1)n+1}} + \mathrm{o}\left(\frac{1}{2^{(\ell-1)n}}\right)\right]\left(1 - \frac{1}{2^n}\right)$.

All in all, $\mathcal{A}$'s advantage satisfies:

$$\mathsf{Adv}^{\mathsf{qind\text{-}qcpa\text{-}p9}}_{\mathcal{A},\mathsf{CBC}}(\lambda) \geqslant 1 - \frac{1}{2^n} - \frac{1}{2^{(\ell-1)n}} + \mathrm{o}\left(\frac{1}{2^{(\ell-1)n}}\right). \tag{71}$$

In particular, this advantage is not negligible with respect to λ. □

7 Discussion

The idea of qIND-qCPA security is intuitively to show that an adversary does not even learn a bit of information by looking at the ciphertext. In a quantum world, such a bit can for instance represent the fact that the plaintext register can be be disentangled with the corresponding ciphertext register, as shown in the Theorems 2, 5 and 10. The fact that such strategies can be applied to security notions gives rise to questioning their relevance. This can be taken to the extreme, as shown by Gagliardoni et al. in [7]. Theorem 11 extends a result of theirs on the qIND-qCPA-P1 notion to the qIND-qCPA-P3 and qIND-qCPA-P8 ones. The definition of the qIND-qCPA-P8 notion is given below, and the qIND-qCPA-P3 one implies it.

Definition 11 (qIND-qCPA-P8 game, adapted from [4]). *In this notion, the adversary is allowed to perform their learning queries on a classical oracle and can perform a single left-or-right challenge query on an erasing oracle.*

Theorem 11. *Let* Enc *be an encryption function from* $\{0,1\}^m$ *to* $\{0,1\}^n$*. There is an adversary which has an advantage of* $\frac{2^m}{2^n}$ *in the qIND-qCPA-P8 security game of* Enc*.*

Proof. In this security notion, $\mathcal{A}$ is allowed to perform a single left-or-right challenge query on an erasing oracle. They prepare the states $|+\rangle$ and $|-\rangle$ and performs their challenge query using them, thus receiving $\sum_x |\mathsf{Enc}(x)\rangle$ or $\sum_x (-1)^x |\mathsf{Enc}(x)\rangle$. Applying an $\mathbf{H}$ gate on the ciphertext and measuring it returns $|0\rangle$ with probability $\frac{2^m}{2^n}$ if $b = 0$ and with probability 0 if $b = 1$. The adversary can thus return $b = 0$ if they measure $|0\rangle$ and $b = 1$ otherwise. □

In particular, this theorem states that any bijective encryption function is qIND-qCPA-P8 insecure. The fact that we can establish the qIND-qCPA-P8 insecurity of any such function without considering any other of its properties makes this notion questionable, along with the qIND-qCPA-P1 one that imply it. This notion originally arose from an equivalent definition of quantum semantic security in [7]. While the authors proposed a way to transform a cipher to circumvent this problem, they did not question the relevance of an encryption system not being secure in this notion. In particular, we can wonder whether the adversary can actually learn any useful information about an insecure scheme according to a notion where challenge requests are quantum. For instance, while it may be possible to recover the secret key of the underlying PRP during the qIND-qCPA-P13 game when used in CBC or CFB mode, it is clear that such an attack cannot also be pulled off against a CTR or OFB mode, since they would otherwise be qIND-qCPA-P6 insecure when used with a PRP.

8 Conclusion

In this paper, we have shown that the modes of operation, whose IND-qCPA security have been studied by Anand et al. [1], are still secure within the gen-

eralized IND-qCPA notions as defined by Carstens et al. [4] when used with a qPRP, and still insecure when used with a PRP.

We have also shown however that CTR, OFB and CFB are qIND-qCPA-P13 insecure, no matter what the underlying block cipher is, essentially by showing that it is possible to disentangle the message register from the ciphertext register in the real world, which can't be done in the random world. Since all the security notions but the IND-qCPA ones and the IND-CPA one impliy the qIND-qCPA-P13 one, this fully characterizes the security of these modes according to each one of these.

Finally, we have shown that, when used with a qPRP, CBC is the only mode to be qIND-qCPA-P5 secure, while still being qIND-qCPA-P9 insecure. This insecurity is once again shown by an attack during which the adversary uses the potential entanglement created by the application of the random permutation on the input register. We furthermore have shown that CBC is qIND-qCPA-P13 insecure by demonstrating that an adversary having an embedding oracle access to such an encryption scheme is able to recover the secret key in a single request.

It is important to consider the subtleties that comes with the notions defined by Carstens et al. [4] when assessing the security of a cryptographic scheme. To know whether a notion truly is useful, it is thus desirable to study the consequences of a scheme not being secure according to this notion, which essentially calls for new quantum semantic security notions.

References

1. Anand, M.V., Targhi, E.E., Tabia, G.N., Unruh, D.: Post-quantum security of the CBC, CFB, OFB, CTR, and XTS modes of operation. In: Takagi, T. (ed.) Post-Quantum Cryptography - 7th International Workshop, PQCrypto 2016. pp. 44–63. Springer, Heidelberg, Germany, Fukuoka, Japan (Feb 24–26 2016). https://doi.org/10.1007/978-3-319-29360-8_4
2. Boneh, D., Zhandry, M.: Secure signatures and chosen ciphertext security in a quantum computing world. In: Canetti, R., Garay, J.A. (eds.) Advances in Cryptology – CRYPTO 2013, Part II. Lecture Notes in Computer Science, vol. 8043, pp. 361–379. Springer, Heidelberg, Germany, Santa Barbara, CA, USA (Aug 18–22, 2013). https://doi.org/10.1007/978-3-642-40084-1_21
3. Bonnetain, X., Naya-Plasencia, M., Schrottenloher, A.: Quantum security analysis of AES. IACR Transactions on Symmetric Cryptology **2019**(2), 55–93 (6 2019). https://doi.org/10.13154/tosc.v2019.i2.55-93, https://tosc.iacr.org/index.php/ToSC/article/view/8314
4. Carstens, T.V., Ebrahimi, E., Tabia, G.N., Unruh, D.: Relationships between quantum IND-CPA notions. In: Nissim, K., Waters, B. (eds.) TCC 2021: 19th Theory of Cryptography Conference, Part I. Lecture Notes in Computer Science, vol. 13042, pp. 273–298. Springer, Heidelberg, Germany, Raleigh, NC, USA (Nov 8–11, 2021). https://doi.org/10.1007/978-3-030-90459-3_9
5. Chevalier, C., Ebrahimi, E., Vu, Q.H.: On security notions for encryption in a quantum world. Cryptology ePrint Archive, Report 2020/237 (2020), https://eprint.iacr.org/2020/237

6. Don, J., Fehr, S., Majenz, C., Schaffner, C.: Security of the Fiat–Shamir transformation in the quantum random-oracle model. In: Boldyreva, A., Micciancio, D. (eds.) Advances in Cryptology – CRYPTO 2019, Part II. Lecture Notes in Computer Science, vol. 11693, pp. 356–383. Springer, Heidelberg, Germany, Santa Barbara, CA, USA (Aug 18–22, 2019). https://doi.org/10.1007/978-3-030-26951-7_13
7. Gagliardoni, T., Hülsing, A., Schaffner, C.: Semantic security and indistinguishability in the quantum world. In: Robshaw, M., Katz, J. (eds.) Advances in Cryptology – CRYPTO 2016, Part III. Lecture Notes in Computer Science, vol. 9816, pp. 60–89. Springer, Heidelberg, Germany, Santa Barbara, CA, USA (Aug 14–18, 2016). https://doi.org/10.1007/978-3-662-53015-3_3
8. Gagliardoni, T., Krämer, J., Struck, P.: Quantum indistinguishability for public key encryption. In: Cheon, J.H., Tillich, J.P. (eds.) Post-Quantum Cryptography - 12th International Conference, PQCrypto 2021. pp. 463–482. Springer, Heidelberg, Germany, Daejeon, South Korea (Jul 20–22 2021). https://doi.org/10.1007/978-3-030-81293-5_24
9. Grassl, M., Langenberg, B., Roetteler, M., Steinwandt, R.: Applying Grover's algorithm to AES: Quantum resource estimates. In: Takagi, T. (ed.) Post-Quantum Cryptography - 7th International Workshop, PQCrypto 2016. pp. 29–43. Springer, Heidelberg, Germany, Fukuoka, Japan (Feb 24–26 2016). https://doi.org/10.1007/978-3-319-29360-8_3
10. Kaplan, M., Leurent, G., Leverrier, A., Naya-Plasencia, M.: Breaking symmetric cryptosystems using quantum period finding. In: Robshaw, M., Katz, J. (eds.) Advances in Cryptology – CRYPTO 2016, Part II. Lecture Notes in Computer Science, vol. 9815, pp. 207–237. Springer, Heidelberg, Germany, Santa Barbara, CA, USA (2016). https://doi.org/10.1007/978-3-662-53008-5_8
11. Liu, Q., Zhandry, M.: Revisiting post-quantum Fiat–Shamir. In: Boldyreva, A., Micciancio, D. (eds.) Advances in Cryptology – CRYPTO 2019, Part II. Lecture Notes in Computer Science, vol. 11693, pp. 236–355. Springer, Heidelberg, Germany, Santa Barbara, CA, USA (Aug 18–22, 2019). https://doi.org/10.1007/978-3-030-26951-7_12
12. Mossayebi, S., Schack, R.: Concrete security against adversaries with quantum superposition access to encryption and decryption oracles (2016)
13. Nemoz, T.: Cryptanalyse quantique d'algorithmes symétriques. Master's thesis, EURECOM (2021)
14. Pinelis, I.: Expectation of the sum of the squares of the cardinal of an inverse function. MathOverflow, https://mathoverflow.net/q/389748
15. Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Computing **26**(5), 1484–1509 (10 1997). https://doi.org/10.1137/s0097539795293172
16. Simon, D.R.: On the power of quantum computation. In: 35th Annual Symposium on Foundations of Computer Science. pp. 116–123. IEEE Computer Society Press, Santa Fe, NM, USA (Nov 20–22, 1994). https://doi.org/10.1109/SFCS.1994.365701
17. Unruh, D.: Revocable quantum timed-release encryption. In: Nguyen, P.Q., Oswald, E. (eds.) Advances in Cryptology – EUROCRYPT 2014. Lecture Notes in Computer Science, vol. 8441, pp. 129–146. Springer, Heidelberg, Germany, Copenhagen, Denmark (May 11–15, 2014). https://doi.org/10.1007/978-3-642-55220-5_8
18. Wooding, M.: New proofs for old modes. Cryptology ePrint Archive, Report 2008/121 (2008), https://eprint.iacr.org/2008/121
19. Zhandry, M.: A note on quantum-secure PRPs. Cryptology ePrint Archive, Report 2016/1076 (2016), https://eprint.iacr.org/2016/1076

A Supplementary Material: Proof of the variant of the One-way to Hiding lemma

Proof. We follow very closely Unruh's proof [17] since this lemma is a variant of the original O2H one.

If $\mathcal{A}$ interacts with a standard oracle, it owns three quantum registers A, K and V, using K as an input register to the oracle and V as an output register. If $\mathcal{A}$ interacts with an erasing oracle, it only owns two quantum registers A and K.

Using the same notations as Unruh [17], $\mathcal{A}$'s state after having performed i queries to an oracle $\mathcal{O}_H$ implementing an arbitrary bijective function H is written as $\left|\Psi^i_{H,x,y}\right\rangle = (\mathbf{U}\mathcal{O}_H)^i \left|\Psi_{x,y}\right\rangle$, where $\mathbf{U}$ is an unitary operation chosen by $\mathcal{A}$ and $|\Psi_{x,y}\rangle$ is $\mathcal{A}$'s initial state, which depends on the classical inputs x and y that $\mathcal{A}$ was called with. When $\mathcal{A}$ measures its final state, it returns a bit b. The probability that $\mathcal{A}$ returns b while being in the state $|\psi\rangle$ is denoted $\Pr_{|\psi\rangle}[\mathcal{A}=1]$. Finally, for a bijective function f, we denote $f_{x,y}$ the function that is equal to f on every input except on x and on $f^{-1}(y)$, where it is defined as $f_{x,y}(x) = y$ and $f_{x,y}\left(f^{-1}(y)\right) = f(x)$. Finally, similarly as Unruh's notation in his proof [17], we define α as $\frac{1}{2^n!2^{2n}}$.

Using these notations, we thus have:

$$P^2_{\mathcal{A}} = \alpha \sum_{H,x,y} \Pr_{\left|\Psi^q_{H,x,y}\right\rangle}[\mathcal{A}=1] \tag{72}$$

and:

$$P^1_{\mathcal{A}} = \frac{1}{2^n!2^n} \sum_{H,x} \Pr_{\left|\Psi^q_{H,x,H(x)}\right\rangle}[\mathcal{A}=1]. \tag{73a}$$

Putting things differently, the situations we are interested in are those when $\mathcal{A}$ interacts with any bijective function H as long as its second input y is equal to $H(x)$, where x is its first input. This allows us to write $P^1_{\mathcal{A}}$ as:

$$P^1_{\mathcal{A}} = \alpha \sum_{H,x,y} \Pr_{\left|\Psi^q_{H_{x,y},x,y}\right\rangle}[\mathcal{A}=1]. \tag{73b}$$

Finally, we can write $P_{\mathcal{B}}$ as:

$$P_{\mathcal{B}} = \alpha \sum_{H,x,y} \Pr\left[\left[\mathcal{B}^H(x,y) = x\right] \cup \left[\mathcal{B}^H(x,y) = H^{-1}(y)\right] \;\middle|\; H,x,y\right] \tag{74a}$$

$$= \alpha \sum_{H,x,y} \left[\Pr\left[\mathcal{B}^H(x,y) = x \;\middle|\; H,x,y\right] + \Pr\left[\mathcal{B}^H(x,y) = x \;\middle|\; H,x,y\right] - \delta_{x,H^{-1}(y)} \Pr\left[\mathcal{B}^H(x,y) = x \;\middle|\; H,x,y\right]\right]. \tag{74b}$$

Now, we define Q_X as the projector on the subspace spanned by X on the $\mathcal{A}$'s K register, similarly to Unruh's proof [17]. This allows us to rewrite $P_{\mathcal{B}}$ as:

$$P_{\mathcal{B}} = \frac{\alpha}{q} \sum_{H,x,y,i} \left[\left(1 - \delta_{x,H^{-1}(y)}\right) \left\| Q_x \left| \Psi^{i-1}_{H,x,y} \right\rangle \right\|^2 + \left\| Q_{H^{-1}(y)} \left| \Psi^{i-1}_{H,x,y} \right\rangle \right\|^2 \right] \tag{74c}$$

$$= \frac{\alpha}{q} \sum_{H,x,y,i} \left\| \left[\left(1 - \delta_{x,H^{-1}(y)}\right) Q_x + Q_{H^{-1}(y)} \right] \left| \Psi^{i-1}_{H,x,y} \right\rangle \right\|^2 \tag{74d}$$

$$= \frac{\alpha}{q} \sum_{H,x,y,i} \left(1 - \frac{\delta_{x,H^{-1}(y)}}{2}\right)^2 \left\| \left(Q_x + Q_{H^{-1}(y)}\right) \left| \Psi^{i-1}_{H,x,y} \right\rangle \right\|^2. \tag{74e}$$

Let us denote T the trace distance and $D_{i,H,x,y}$ the trace distance between $\left|\Psi^i_{H,x,y}\right\rangle$ and $\left|\Psi^i_{H_{x,y},x,y}\right\rangle$. Since the trace distance upper-bounds the probability of distinguishing two quantum states, the following holds:

$$\left| \Pr_{\left|\Psi^q_{H_{x,y},x,y}\right\rangle}[\mathcal{A} = 1] - \Pr_{\left|\Psi^q_{H,x,y}\right\rangle}[\mathcal{A} = 1] \right| \leqslant D_{q,H,x,y} \tag{75}$$

and:

$$D_{i,H,x,y} = T\left(\mathbf{U}\mathcal{O}_H \left| \Psi^{i-1}_{H,x,y} \right\rangle, \mathbf{U}\mathcal{O}_{H_{x,y}} \left| \Psi^{i-1}_{H_{x,y},x,y} \right\rangle \right) \tag{76a}$$

$$= T\left(\mathcal{O}_H \left| \Psi^{i-1}_{H,x,y} \right\rangle, \mathcal{O}_{H_{x,y}} \left| \Psi^{i-1}_{H_{x,y},x,y} \right\rangle \right). \tag{76b}$$

Thus, using triangle inequality:

$$\begin{aligned} D_{i,H,x,y} \leqslant\ & T\left(\mathcal{O}_H \left| \Psi^{i-1}_{H,x,y} \right\rangle, \mathcal{O}_{H_{x,y}} \left| \Psi^{i-1}_{H,x,y} \right\rangle \right) + \\ & T\left(\mathcal{O}_{H_{x,y}} \left| \Psi^{i-1}_{H,x,y} \right\rangle, \mathcal{O}_{H_{x,y}} \left| \Psi^{i-1}_{H_{x,y},x,y} \right\rangle \right) \end{aligned} \tag{77a}$$

$$\leqslant T\left(\mathcal{O}_H \left| \Psi^{i-1}_{H,x,y} \right\rangle, \mathcal{O}_{H_{x,y}} \left| \Psi^{i-1}_{H,x,y} \right\rangle \right) + D_{i-1,H,x,y}. \tag{77b}$$

Thus:

$$D_{q,H,x,y} - D_{0,H,x,y} \leqslant \sum_{i=1}^{q} T\left(\mathcal{O}_H \left| \Psi^{i-1}_{H,x,y} \right\rangle, \mathcal{O}_{H_{x,y}} \left| \Psi^{i-1}_{H,x,y} \right\rangle \right). \tag{78}$$

Note that $D_{0,H,x,y} = 0$, since it is the trace distance between $|\Psi_{x,y}\rangle$ and itself. Now, if $\mathcal{A}$ interacts with a standard oracle, we can check that the following holds by reasoning on the basis states:

$$\begin{aligned} \mathcal{O}_{H_{x,y}} = \mathcal{O}_H \left(\mathbf{I} - Q_x - Q_{H^{-1}(y)} \right) + \sum_{a,v} |a, x, v \oplus y\rangle \langle a, x, v| + \\ \sum_{a,v} \left| a, H^{-1}(y), v \oplus H(x) \right\rangle \left\langle a, H^{-1}(y), v \right| \end{aligned} \tag{79a}$$

while we can write, if $\mathcal{A}$ interacts with an erasing oracle:

$$\mathcal{O}_{H_{x,y}} = \mathcal{O}_H \left(\mathbf{I} - Q_x - Q_{H^{-1}(y)}\right) + \sum_a |a,y\rangle \langle a,x| + \sum_a |a,H(x)\rangle \left\langle a,H^{-1}(y)\right| . \tag{79b}$$

This allows us to write $\mathcal{O}_H \left|\Psi^{i-1}_{H,x,y}\right\rangle$ as:

$$\mathcal{O}_H \left(\mathbf{I} - Q_x - Q_{H^{-1}(y)}\right) \left|\Psi^{i-1}_{H,x,y}\right\rangle + \mathcal{O}_H Q_x \left|\Psi^{i-1}_{H,x,y}\right\rangle + \mathcal{O}_H Q_{H^{-1}(y)} \left|\Psi^{i-1}_{H,x,y}\right\rangle \tag{80}$$

and $\mathcal{O}_{H_{x,y}} \left|\Psi^{i-1}_{H,x,y}\right\rangle$ as, in the case of a standard oracle:

$$\begin{aligned} &\mathcal{O}_H \left(\mathbf{I} - Q_x - Q_{H^{-1}(y)}\right) \left|\Psi^{i-1}_{H,x,y}\right\rangle + \sum_{a,v} |a,x,v\oplus y\rangle \left\langle a,x,v\right|\Psi^{i-1}_{H,x,y}\rangle + \\ &\sum_{a,v} \left|a,H^{-1}(y),v\oplus H(x)\right\rangle \left\langle a,H^{-1}(y),v\right|\Psi^{i-1}_{H,x,y}\rangle \end{aligned} \tag{81a}$$

or, in the case of an erasing oracle:

$$\begin{aligned} &\mathcal{O}_H \left(\mathbf{I} - Q_x - Q_{H^{-1}(y)}\right) \left|\Psi^{i-1}_{H,x,y}\right\rangle + \sum_a |a,y\rangle \left\langle a,x\right|\Psi^{i-1}_{H,x,y}\rangle + \\ &\sum_a |a,H(x)\rangle \left\langle a,H^{-1}(y)\right|\Psi^{i-1}_{H,x,y}\rangle . \end{aligned} \tag{81b}$$

Writing these states like this allows us to use Unruh's Lemma 11 [17], which ensures that $T\left(\mathcal{O}_H \left|\Psi^{i-1}_{H,x,y}\right\rangle, \mathcal{O}_{H_{x,y}} \left|\Psi^{i-1}_{H,x,y}\right\rangle\right)$ is upper-bounded by:

$$2 \left\| \mathcal{O}_H Q_x \left|\Psi^{i-1}_{H,x,y}\right\rangle + \mathcal{O}_H Q_{H^{-1}(y)} \left|\Psi^{i-1}_{H,x,y}\right\rangle \right\| \tag{82a}$$

$$\leqslant 2 \left\| \left(Q_x + Q_{H^{-1}(y)}\right) \left|\Psi^{i-1}_{H,x,y}\right\rangle \right\| \tag{82b}$$

$$\leqslant 2 \left(1 - \delta_{x,H^{-1}(y)}\right) \left\| \left(Q_x + Q_{H^{-1}(y)}\right) \left|\Psi^{i-1}_{H,x,y}\right\rangle \right\| . \tag{82c}$$

Thus, using triangle inequality and Equations 75 and 78:

$$\left|P^1_{\mathcal{A}} - P^2_{\mathcal{A}}\right| \leqslant \alpha \sum_{H,x,y,i} 2 \left(1 - \delta_{x,H^{-1}(y)}\right) \left\| \left(Q_x + Q_{H^{-1}(y)}\right) \left|\Psi^{i-1}_{H,x,y}\right\rangle \right\|^2 \tag{83a}$$

$$\leqslant 2q \sum_{H,x,y,i} \frac{\alpha}{q} \sqrt{\left(1 - \delta_{x,H^{-1}(y)}\right) \left\| \left(Q_x + Q_{H^{-1}(y)}\right) \left|\Psi^{i-1}_{H,x,y}\right\rangle \right\|^2} . \tag{83b}$$

Hence, using Jensen's inequality:

$$\left|P^1_{\mathcal{A}} - P^2_{\mathcal{A}}\right| \leqslant 2q \sqrt{\frac{\alpha}{q} \sum_{H,x,y,i} \left(1 - \delta_{x,H^{-1}(y)}\right) \left\| \left(Q_x + Q_{H^{-1}(y)}\right) \left|\Psi^{i-1}_{H,x,y}\right\rangle \right\|^2} . \tag{84}$$

We can then conclude by noticing that $1 - \delta_{x,H^{-1}(y)} \leqslant \left(1 - \frac{\delta_{x,H^{-1}(y)}}{2}\right)^2$. □