# 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 fully characterize 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), thus extending the work performed by Anand, Targhi, Tabia and Unruh (PQCrypto 2016).

We show that the results obtained by Anand et al. for the qIND-qCPA-P6 security of these modes carry on to the other IND-qCPA notions, namely the qIND-qCPA-P10 and qIND-qCPA-P11 ones. We also show that all of these modes are insecure according to all of the other notions, regardless of the block cipher they are used with.

We also provide two general results concerning the insecurity of commonly used properties of block ciphers, namely those preserving the length of their input and those using the XOR operation as a way to randomize the encryption. Finally, we use these results to highlight the need for new quantum semantic security notions.

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

## 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 [14], 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] or defining quantum-aware security notions for cryptosystems [2,5,6,7,8].

The security of the CBC, CFB, OFB and CTR modes of operations has been traditionally assessed via the IND-CPA security notion. 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 [2,6,7,11]. 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 [5]. This resulted in 14 distinct equivalence classes of qIND-qCPA notions. However the relevance of these notions is still discussed because of their novelty.

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. [5]. These results are summarized in Table 1. Furthermore, we show two general results about the insecurity of two common practices. Firstly, we show that a scheme preserving the length of its input is not qIND-qCPA-P8 secure, thus generalizing a result from Gagliardoni et al. [7]. We also show that randomizing an encryption using a public function such as the XOR one while giving the associated randomness to the adversary makes the scheme qIND-qCPA-P5-insecure. The way all these are proved questions the relevance of some qIND-qCPA notions and highlights the need for equivalent quantum semantic security notions.

**Table 1.** Summary of our results. The ✓ symbol means that all denoted schemes are secure in this notion. The ✗ symbol means that no denoted scheme is secure in this notion. The ◆ symbol means that there is at least one scheme 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 | ✗ $^{\text{P13}}$ | ✗ $^{\text{P13}}$ | ✗ $^{\text{P13}}$ | ✗ $^{\text{P13}}$ | ✗ $^{\text{P13}}$ |
| P2 | ✗ [6] | ✗ $^{\text{P12}}$ | ✗ $^{\text{P12}}$ | ✗ [6] | ✗ [6] |
| P3 | ✗ $^{\text{P13}}$ | ✗ $^{\text{P13}}$ | ✗ $^{\text{P13}}$ | ✗ $^{\text{P13}}$ | ✗ $^{\text{P13}}$ |
| P4 | ✗ $^{\text{P13}}$ | ✗ $^{\text{P13}}$ | ✗ $^{\text{P13}}$ | ✗ $^{\text{P13}}$ | ✗ $^{\text{P13}}$ |
| P5 | ✗ $^{\text{P13}}$ | ✗ $^{\text{P13}}$ | ✗ $^{\text{P13}}$ | ✗ $^{\text{P13}}$ | ✗ $^{\text{P13}}$ |
| P6 | ✓ [1] | ◆ [1] | ✓ [1] | ◆ [1] | ✓ [1] |
| P7 | ✗ $^{\text{P13}}$ | ✗ $^{\text{P13}}$ | ✗ $^{\text{P13}}$ | ✗ $^{\text{P13}}$ | ✗ $^{\text{P13}}$ |
| P8 | ✗ $^{\text{P13}}$ | ✗ $^{\text{P13}}$ | ✗ $^{\text{P13}}$ | ✗ $^{\text{P13}}$ | ✗ $^{\text{P13}}$ |
| P9 | ✗ $^{\text{P13}}$ | ✗ $^{\text{P13}}$ | ✗ $^{\text{P13}}$ | ✗ $^{\text{P13}}$ | ✗ $^{\text{P13}}$ |
| P10 | ✓ $^{6}$ | ◆ $^{\text{P11}}$ | ✓ $^{9}$ | ◆ $^{\text{P11}}$ | ✓ $^{9}$ |
| P11 | ✓ $^{\text{P6}}$ | ◆ $^{8}$ | ✓ $^{\text{P6}}$ | ◆ $^{7}$ | ✓ $^{\text{P6}}$ |
| P12 | ✗ [5] | ✗ [5] | ✗ [5] | ✗ [5] | ✗ [5] |
| P13 | ✗ $^{1}$ | ✗ $^{3}$ | ✗ $^{3}$ | ✗ $^{2}$ | ✗ $^{2}$ |
| P14 | ✓ [1] | ✓ [1] | ✓ [1] | ✓ [1] | ✓ [1] |

### 1.2 Our contributions

**IND-qCPA security** We observe in appendix A that the results found by Anand et al. for the IND-qCPA using a standard oracle (qIND-qCPA-P6) security notion carry on to the two other IND-qCPA notions, namely the one using an erasing oracle (qIND-qCPA-P10) and the one using an embedding oracle (qIND-qCPA-P11). In these notions, the adversary can perform their learning request on a quantum oracle but is limited to classical challenge queries. 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** Furthermore, we show in subsections 3.1 to 3.3 that these are the only security notions verified by these modes, since they are qIND-qCPA-P13 insecure, no matter what the underlying block cipher is. As shown on Fig. 1, the qIND-qCPA-P13 security notion is the weakest notion in which the challenge request is quantum. Thus, proving the insecurity of these modes with respect to this notion carry on to almost every other notion.

In the qIND-qCPA-P13 security notion, the adversary is allowed classical learning queries and a single real-or-random challenge query performed on an embedding oracle. It means that the adversary's challenge query undergoes the following transformation:

$$\sum_x \alpha_x |x\rangle \to \sum_x \alpha_x |x\rangle \left|\mathsf{Enc}_\mathsf{k}\left(\pi^b(x)\right)\right\rangle$$

with $\pi$ being a random permutation. For the CFB, CTR and OFB modes of operation, we prove this by showing that it is possible for the adversary to disentangle the ciphertext register and the plaintext register in the real world, while it is not possible to do so in the random world. Concerning CBC, we show that for $\ell \geqslant 3$, the adversary is able to separate the registers in two identical states in the real world, which is not possible in the random world with overwhelming probability. They are thus able to distinguish both cases using a SWAP test.

**General results and relevance of the qIND-qCPA notions** We show in subsection 3.4 two general insecurity results.

Firstly, we show that the way the encryption is randomized must be secretly kept in order for it to be qIND-qCPA-P5-secure. In particular, randomizing the encryption by XORing the input with a random string $r$ which is provided to the adversary does not yield a qIND-qCPA-P5-secure scheme.

We then show that in order for a scheme to be qIND-qCPA-P8-secure, the length of the ciphertexts must be higher than that of the plaintexts. In particular, if the randomness is not part of the ciphertext and if the encryption function is bijective, the resulting scheme can not be qIND-qCPA-P8-secure.

We show as an example how the construction provided by Carstens et al. which is secured in all qIND-qCPA notions satisfies both these conditions. We then use these results to exhibit the need for new quantum semantic security notions.

### 1.3 Previous work

Anand et al. studied in [1] the security of the modes of operation under the standard IND-qCPA (qIND-qCPA-P6) security notion. Chevalier, Ebrahimi and Vu showed in [6] 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 are not qIND-qCPA-P12 secure as long as they use at least two blocks [5].

## 2 Prerequisites

### 2.1 Notations and definitions

**Notations** $\llbracket a\,;\,b\rrbracket$ represents the set $[a\,;\,b] \cap \mathbb{N}$. An adversary $\mathcal{A}$ having access to an oracle $\mathcal{O}$ is denoted $\mathcal{A}^{\mathcal{O}}$. For a given permutation $\pi$, we denote $\pi_{a\to b}$ the function which returns the bits of $\pi$ from $a$ to $b$ inclusive, starting the indexing at 0. The security parameter of a system is denoted $\lambda$. 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 $b = 1$.

The advantage of an adversary $\mathcal{A}$ in the experiment $\mathsf{Exp}$ using the symmetric scheme $\mathcal{S}$ is defined as, accordingly to the definition given in [11]:

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

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 [11], it was then named "real or permutation", and the convention for the real and random worlds was the opposite of ours.

We denote $\mathbf{H}$ the Hadamard gate and $\mathbf{X}$ the `NOT` gate. If we want to name a quantum register $|\psi\rangle$, we indicate its name as a subscript, like $|\psi\rangle_{\text{Name}}$.

**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:*

$\mathsf{Enc}^{\mathsf{CBC}}_{E_{\mathsf{k}},\ell}$**:** *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 $i \in [\![1\,;\,\ell]\!]$, $c_i = E_{\mathsf{k}}\left(m_i \oplus c_{i-1}\right)$.*

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

**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:*

$\mathsf{Enc}^{\mathsf{CFB}}_{E_{\mathsf{k}},\ell}$**:** *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 $i \in [\![1\,;\,\ell]\!]$, $c_i = m_i \oplus E_{\mathsf{k}}\left(c_{i-1}\right)$.*

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

**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:*

$\mathsf{Enc}^{\mathsf{OFB}}_{E_{\mathsf{k}},\ell}$**:** *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 $t_0 = E_{\mathsf{k}}\left(c_0\right)$ and, for $i \in [\![1\,;\,\ell]\!]$, $c_i = t_i \oplus m_i$ and $t_i = E_{\mathsf{k}}\left(t_{i-1}\right)$.*

$\mathsf{Dec}^{\mathsf{OFB}}_{E_{\mathsf{k}},\ell}$**:** *For a ciphertext $c = c_1 \cdots c_\ell$ 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:*

$\mathsf{Enc}^{\mathsf{CTR}}_{E_{\mathsf{k}},\ell}$**:** *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 $i \in [\![1\,;\,\ell]\!]$, $c_i = m_i \oplus E_{\mathsf{k}}(c_0 \oplus i - 1)$.*

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

*In these definitions, $c_0 \oplus i - 1$ represents the bitwise XOR between $c_0$ and a fixed $n$-bit representation of $i - 1$.*

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 $\ell$ that such a mode of operation accepts is assumed to be polynomial in $\lambda$. In all of our proofs, $\ell$ is assumed to be constant, that is we assume that the oracle only accepts queries of size $\ell$, 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 $\lambda$. 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 with respect to $n$.

### Security notions

**Definition 5 (Standard and quantum-secure pseudorandom permutation, adapted from [19, Definition 3.1]).** *A permutation $\pi_{\mathsf{k}}$ depending on a key $\mathsf{k}$ 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 $\pi_{\mathsf{k}}$ for a randomly chosen $\mathsf{k}$.*

Since we will consider different types of oracles in the following, we ought to be more precise about what a quantum query is in the previous definition. In particular, since an erasing oracle and a standard oracle can't simulate each other, the precision seems to have to be made. However, Carstens et al. showed that a permutation that is quantum-secure with standard queries are also secure with erasing queries, and reciprocally [5, Lemma 6].

*qIND-qCPA notions* In [5], Carstens et al. defined 14 different equivalence classes for 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.

**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 [5]:

**Standard oracle:** On a basis state $|x, y\rangle$, the oracle returns $|x, y \oplus f(x)\rangle$.

**Embedding oracle:** On a basis state $|x\rangle$, the oracle prepares a 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.

It is important to note that the embedding oracle is the weakest of the three quantum oracles, since it is possible to simulate such an oracle using either one of the two others.

**Challenge type** Three challenge types are used in [5].

**Real-or-random:** On a challenge query, the oracle chooses a random permutation $\pi$ and applies $\pi^b$ to the plaintext register before encrypting it. This means that for a standard or an embedding challenge query, the oracle performs this mapping:

$$|x, y\rangle \to \left|x, y \oplus \mathsf{Enc}_\mathsf{k}\left(\pi^b(x)\right)\right\rangle$$

while it performs this mapping for an erasing oracle:

$$|x\rangle \to \left|\mathsf{Enc}_\mathsf{k}\left(\pi^b(x)\right)\right\rangle .$$

Note that such a permutation is chosen at random for each of the challenge queries the adversary performs.

**Two-ciphertexts** A challenge query is made of two states. On a challenge query on a standard or an embedding oracle, the oracle performs the following mapping:

$$|x_0, y_0\rangle |x_1, y_1\rangle \to |x_0, y_0 \oplus \mathsf{Enc}_\mathsf{k}(x_b)\rangle \left|x_1, y_1 \oplus \mathsf{Enc}_\mathsf{k}\left(x_{\overline{b}}\right)\right\rangle$$

while it performs the following mapping on an erasing oracle:

$$|x_0\rangle |x_1\rangle \to |\mathsf{Enc}_\mathsf{k}(x_b)\rangle \left|\mathsf{Enc}_\mathsf{k}\left(x_{\overline{b}}\right)\right\rangle .$$

**One-ciphertext** A challenge query is made of two states $|\psi_0\rangle$ and $|\psi_1\rangle$. The oracle first measures $\left|\psi_{\overline{b}}\right\rangle$ and throws away the result. It then performs the following mapping on a standard or an erasing oracle:

$$|x_0, y_0\rangle |x_1, y_1\rangle \to |x_b, y_b \oplus \mathsf{Enc}_\mathsf{k}(x_b)\rangle$$

while it performs the following mapping on an erasing oracle:

$$|x_0\rangle |x_1\rangle \to |\mathsf{Enc}_\mathsf{k}(x_b)\rangle .$$

It is immediate to see that the notions using the two-ciphertexts return type implies those with the one-ciphertext one when using the same number of challenge queries and the same learning scheme, since more information is given to the adversary. However, Carstens et al. also showed that it just happens that the same property is true concerning the one-ciphertext return type and the real-or-random one [5]. As such, the real-or-random return type is the weakest among all three.

At the exception of the qIND-qCPA-P13 and IND-qCPA notions, every security notion is used at most once in our work. Thus, for clarity's sake, we define these notions just before their associated proof of (in)security. The IND-qCPA notions are put with the associated proofs in appendix A and we define the qIND-qCPA-P13 security notion here since it is widely used throughout this work.

**Definition 6 (qIND-qCPA-P13 game, adapted from [5]).** *Let $E$ be a cryptographic scheme: $E = (\mathsf{KGen}, \mathsf{Enc}, \mathsf{Dec})$. We denote by $M$ the set of messages $E$ operates on, by $\mathsf{CL}-\mathsf{Enc}$ the classical oracle implementing $\mathsf{Enc}$ and by $\mathsf{EM}-\mathsf{Enc}$ the embedding oracle implementing $\mathsf{Enc}$. We say that $E$ is qIND-qCPA-P13-secure if no polynomial time quantum adversary $\mathcal{A}$ has an advantage larger than $\frac{1}{2}+\varepsilon$ in the following experiment, with $\varepsilon$ being negligible with respect to $\lambda$.*

```
Experiment qIND-qCPA-P13$^b_E(\lambda, \mathcal{A})$
$\mathsf{k} \leftarrow\$\ \mathsf{KGen}\left(1^\lambda\right)$
$\pi \leftarrow\$\ \mathfrak{S}_{|M|}$
$(\mathsf{state}, |\varphi\rangle) \leftarrow\$\ \mathcal{A}^{\mathsf{CL-Enc(k,\cdot)}}()$
$|\psi\rangle \leftarrow\$\ \mathsf{EM}-\mathsf{Enc}\left(\mathsf{k}, \left|\pi^b(\varphi)\right\rangle\right)$
$b' \leftarrow\$\ \mathcal{A}^{\mathsf{CL-Enc(k,\cdot)}}(|\varphi, \psi\rangle, \mathsf{state})$
return $b'$
```

Intuitively, this notion is the weakest one can come up with using a quantum challenge request. Indeed, the classical learning queries greatly limits the power of the adversary, ans they are allowed a single challenge query on the weakest quantum oracle, using the weakest return type. This intuition has been shown by Carstens et al. [5] and is shown on Fig. 1.

Note that the qIND-qCPA-P6 (in)security of the CBC, CFB, OFB and CTR modes of operation is known from [1], and that the IND-CPA security of these modes is also known (see for example [17]). As such, these implications show that in order to completely characterize the security of these modes, proving their qIND-qCPA-P13 insecurity and their qIND-qCPA-P10 security or their qIND-qCPA-P11 insecurity is sufficient.

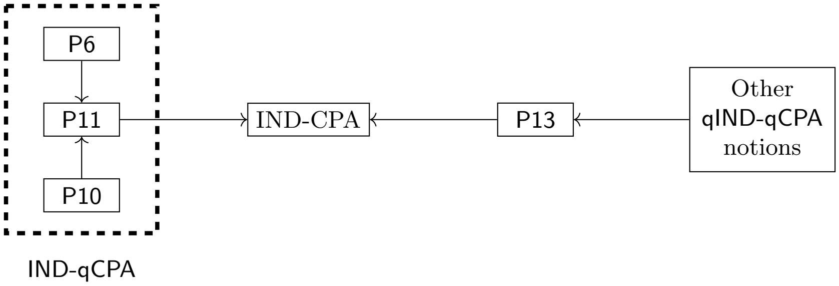

**Fig. 1.** Relationships between qIND-qCPA notions, adapted from [5]. The IND-CPA and qIND-qCPA-P6 (in)security of the CBC, CFB, OFB and CTR modes are known from [1,17]. Thus, proving their qIND-qCPA-P13 insecurity and their qIND-qCPA-P11 insecurity or their qIND-qCPA-P10 security fully characterizes them.

## 2.2 Lemmas

**Lemma 1.** *We consider the quantum state* $\frac{1}{\sqrt{2^m}}\sum_x |x\rangle|f(x)\rangle$ *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* $\frac{1}{2^{2m}}\sum_y \left|f^{-1}(y)\right|^2$*.*

*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:

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

□

## 2.3 IND-qCPA security of CBC, CFB, CTR and OFB

In 2016, Anand et al. characterized the security of the CBC, CFB, CTR and OFB modes of operation [1]. The notion they used is the IND-qCPA notion defined in [2]. As its name suggests, in this notion the adversary is allowed to perform quantum learning queries but is restricted to classical challenge queries. Arguably, the term "IND-qCPA" is now ambiguous, for instance because of the different quantum oracles that can be used to answer the quantum queries.

In this work, IND-qCPA refers to all the notions defined by Carstens et al. that can be identified using the previous description [5]. This includes the qIND-qCPA-P6 notion, which is the one defined in [2], and the qIND-qCPA-P10 and qIND-qCPA-P11 ones. The former uses an erasing oracle to answer learning queries, while the latter uses an embedding one.

While these notions are not equivalent, their similarities allow us to reuse almost identically the proofs performed by Anand et al. to show the (in)security of the CBC, CFB, CTR and OFB modes of operation with respect to the qIND-qCPA-P6 security in the qIND-qCPA-P10 and qIND-qCPA-P11 cases. As such, we put these proofs and the relevant definitions in appendix A.

## 3 Our results

### 3.1 qIND-qCPA-P13 insecurity of CTR and OFB

In this section, we show that, according to Fig. 1, the only security notions that CTR and OFB satisfy are the IND-qCPA ones by exhibiting an attack against their qIND-qCPA-P13 security.

This proof only relies 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 proof can also be applied to stream ciphers, and we will denote $m \oplus s$ an encryption of the message $m$ using such a scheme. Note however that this proof assumes that the ciphertext can be written as $x \oplus s$ entirely. As such, it doesn't carry on to the GCM mode of operation which, though it uses the CTR mode of operation, adds a tag at the end of the ciphertext.

**Theorem 1 (Originally written in [12]).** *CTR and OFB are qIND-qCPA-P13 insecure, no matter what the underlying block cipher is.*

*Proof.* $\mathcal{A}$ prepares the state $|+\rangle$ and performs their challenge query using it. They thus receive:

$$\begin{cases} \sum_x |x\rangle \, |x \oplus s\rangle & \text{if } b = 0 \\ \sum_x |x\rangle \, |\pi(x) \oplus s\rangle & \text{if } b = 1 \end{cases} \tag{3}$$

for a random permutation $\pi$. By performing an $\mathbf{X}$ gate on the second register controlled by the first one, the state becomes:

$$\begin{cases} \sum_x |x\rangle \, |s\rangle & \text{if } b = 0 \\ \sum_x |x\rangle \, |x \oplus \pi(x) \oplus s\rangle & \text{if } b = 1 \end{cases} . \tag{4}$$

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:

$$\Pr[|0\rangle \mid b = 1] = \frac{1}{2^{2\ell n}} \sum_y \left| f^{-1}(y) \right|^2 . \tag{5}$$

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 [13].

We have, for a given $y$:

$$\left|f^{-1}(y)\right| = \sum_{x} \mathbb{1}_{\pi(x)=x\oplus y} \tag{6}$$

thus:

$$\left|f^{-1}(y)\right|^2 = \sum_{x_1}\sum_{x_2} \mathbb{1}_{[\pi(x_1)=x_1\oplus y]\cap[\pi(x_2)=x_2\oplus y]} \tag{7}$$

thus:

$$\begin{aligned}\mathbb{E}\left[\left|f^{-1}(y)\right|^2\right] &= \sum_{x_1}\sum_{x_2} \Pr[[\pi\left(x_1\right) = x_1 \oplus y] \cap [\pi\left(x_2\right) = x_2 \oplus y]] && \text{(8a)}\\ &= \sum_{x_1} \Pr[\pi\left(x_1\right) = x_1 \oplus y] + \\ &\quad \sum_{x_1}\sum_{x_2\neq x_1} \Pr[[\pi\left(x_1\right) = x_1 \oplus y] \cap [\pi\left(x_2\right) = x_2 \oplus y]]. && \text{(8b)}\end{aligned}$$

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

$$\mathbb{E}\left[\left|f^{-1}(y)\right|^2\right] = 1 + \frac{1}{2^{\ell n}} \sum_{x_1}\sum_{x_2\neq x_1} \Pr[\pi\left(x_2\right) = x_2 \oplus y \mid \pi\left(x_1\right) = x_1 \oplus y]. \tag{8c}$$

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

$$\mathbb{E}\left[\left|f^{-1}(y)\right|^2\right] = 2. \tag{8d}$$

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

$$\Pr[|0\rangle \mid b = 1] = \frac{1}{2^{\ell n-1}}. \tag{9}$$

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

$$\mathsf{Adv}^{\mathsf{qind\text{-}qcpa\text{-}p13}}_{\mathcal{A},\mathsf{CTR/OFB}}(\lambda) = 1 - \frac{1}{2^{\ell n-1}}. \tag{10}$$

In particular, it is not negligible with respect to $\lambda$. □

### 3.2 qIND-qCPA-P13 insecurity of CFB

Similarly to the CTR and OFB modes, we show that an adversary can win with non-negligible advantage in the qIND-qCPA-P13 security game of the CFB mode, no matter what the underlying block cipher is. Along with its IND-qCPA (in)security proven in appendix A, this fully characterizes it, according to Fig. 1.

The qIND-qCPA-P13 insecurity of CFB, just like CTR and OFB, comes from the fact that the adversary can disentangle the ciphertext register from the plaintext register, which is not possible in the random world. The same strategy as for these two modes can thus be used to distinguish both worlds.

**Theorem 2 (Originally written in [12]).** *CFB is qIND-qCPA-P13 insecure, no matter what the underlying block cipher is.*

*Proof.* $\mathcal{A}$ prepares the following state, where each register is made of $n$ qubits:

$$\frac{1}{\sqrt{2^n}}\left(\bigotimes_{k=1}^{\ell-1}|0\rangle\right)\sum_x |x\rangle \tag{11}$$

and performs their challenge query using it. They thus receive, ignoring the first $\ell-1$ registers which are not entangled with the others:

$$\begin{cases} \frac{1}{\sqrt{2^n}}\sum\limits_x |x\rangle \left(\bigotimes\limits_{i=1}^{\ell-1}\left|E_{\mathsf{k}}^{i}\left(c_0\right)\right\rangle\right)\left|x\oplus E_{\mathsf{k}}^{\ell}\left(c_0\right)\right\rangle & \text{if } b=0 \\ \frac{1}{\sqrt{2^n}}\sum\limits_x |x\rangle \bigotimes\limits_{i=1}^{\ell}\left|\pi_{(i-1)n\to in-1}(0\parallel\cdots\parallel 0\parallel x)\oplus E_{\mathsf{k}}\left(c_{i-1}(x)\right)\right\rangle & \text{if } b=1 \end{cases} \tag{12}$$

for a random permutation $\pi$, where $c_0$ is a random constant function and where we have defined:

$$c_i(x) \overset{\text{def}}{=} \pi_{(i-1)n\to in-1}(0\parallel\cdots\parallel 0\parallel x)\oplus E_{\mathsf{k}}\left(c_{i-1}(x)\right). \tag{13}$$

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

$$\begin{cases} \frac{1}{\sqrt{2^n}}\sum\limits_x |x\rangle \left(\bigotimes\limits_{i=1}^{\ell-1}\left|E_{\mathsf{k}}^{i}\left(c_0\right)\right\rangle\right)\left|E_{\mathsf{k}}^{\ell}\left(c_0\right)\right\rangle & \text{if } b=0 \\ \frac{1}{\sqrt{2^n}}\sum\limits_x |x\rangle\left|f_{c_0,\pi}(x)\right\rangle & \text{if } b=1 \end{cases} \tag{14}$$

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

$$f_{c_0,\pi}(x) \overset{\text{def}}{=} x\mapsto c_1(x)\parallel\cdots\parallel c_{\ell-1}(x)\parallel\left(x\oplus c_\ell(x)\right). \tag{15}$$

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 Lemma 1 to prove it. The probability to measure $|0\rangle$ if $b=1$ is given by:

$$\Pr[|0\rangle \mid b=1] = \frac{1}{2^{2n}}\sum_y \left|f_{c_0,\pi}^{-1}(y)\right|^2. \tag{16}$$

The following is an adaptation of the proof proposed by Iosif Pinelis [13].

We have, for a given $y$:

$$\left|f_{c_0,\pi}^{-1}(y)\right| = \sum_x \mathbb{1}_{f_{c_0,\pi}(x)=y} \tag{17}$$

thus:

$$\left|f_{c_0,\pi}^{-1}(y)\right|^2 = \sum_{x_1}\sum_{x_2}\mathbb{1}_{\left[f_{c_0,\pi}(x_1)=y\right]\cap\left[f_{c_0,\pi}(x_2)=y\right]} \tag{18}$$

thus:

$$
\begin{aligned}
\mathbb{E}\left[\left|f_{c_0,\pi}^{-1}(y)\right|^2\right] &= \sum_{x_1}\sum_{x_2} \Pr[[f_{c_0,\pi}\left(x_1\right) = y] \cap [f_{c_0,\pi}\left(x_2\right) = y]] && \text{(19a)} \\
&= \sum_{x_1} \Pr[f_{c_0,\pi}\left(x_1\right) = y] + \\
&\quad \sum_{x_1}\sum_{x_2 \neq x_1} \Pr[[f_{c_0,\pi}\left(x_1\right) = y] \cap [f_{c_0,\pi}\left(x_2\right) = y]]. && \text{(19b)}
\end{aligned}
$$

Since $\pi$ 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 $E_{\mathsf{k}}\left(c_{i-1}(x)\right)$, 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, $f_{c_0,\pi}$ is uniformly random and we have:

$$
\mathbb{E}\left[\left|f_{c_0,\pi}^{-1}(y)\right|^2\right] = \frac{2^n}{2^{\ell n}} + \frac{1}{2^{\ell n}} \sum_{x_1}\sum_{x_2 \neq x_1} \Pr[f_{c_0,\pi}\left(x_2\right) = y \mid f_{c_0,\pi}\left(x_1\right) = y]. \tag{19c}
$$

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

Note that the probability that we want to compute is the probability that $c_i\left(x_1\right) = c_i\left(x_2\right)$ for $i \in \llbracket 1\,;\, \ell - 1 \rrbracket$ and that $c_\ell\left(x_1\right) \oplus x_1 = c_i\left(x_2\right) \oplus x_2$. Using the definition of $c_i$, this is equivalent to computing the probability that $\pi\left(x_1\right)$ and $\pi\left(x_2\right)$ 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 $\pi\left(x_2\right)$ as long as they are not equal to those of $\pi\left(x_1\right)$, 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:

$$
\mathbb{E}\left[\left|f_{c_0,\pi}^{-1}(y)\right|^2\right] = \frac{2^n}{2^{\ell n}} + \frac{1}{2^{\ell n}} \sum_{x_1}\sum_{x_2 \neq x_1} \frac{1}{2^{\ell n} - 1} = \frac{2^n}{2^{\ell n}} + \frac{2^n\left(2^n - 1\right)}{2^{\ell n}\left(2^{\ell n} - 1\right)}. \tag{19d}
$$

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

$$
\Pr[|0\rangle \mid b = 1] = \frac{1}{2^{2n}} \sum_{y} \left( \frac{2^n}{2^{\ell n}} + \frac{2^n\left(2^n - 1\right)}{2^{\ell n}\left(2^{\ell n} - 1\right)} \right) = \frac{1}{2^n}\left(1 + \frac{2^n - 1}{2^{\ell n} - 1}\right). \tag{20}
$$

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

$$
\mathsf{Adv}_{\mathcal{A},\mathsf{CFB}}^{\mathsf{qind\text{-}qcpa\text{-}p13}}(\lambda) = 1 - \frac{1}{2^n}\left(1 + \frac{2^n - 1}{2^{\ell n} - 1}\right). \tag{21}
$$

In particular, this advantage is not negligible with respect to $\lambda$. □

### 3.3 qIND-qCPA-P13 insecurity of CBC

Finally, we show that CBC is qIND-qCPA-P13 insecure, no matter what the underlying block cipher is. Contrarily to the three other modes, it is not possible to disentangle the ciphertext register from the plaintext one in this case. However, we show that an adversary is able to separate the answer to its challenge query into two identical registers in the real world, while it isn't possible in the random one. Thus, performing a SWAP test allows to distinguish both cases.

**Theorem 3.** *CBC is qIND-qCPA-P13 insecure if it uses more than 3 blocks, no matter what the underlying block cipher is.*

*Proof.* Let us assume for now that $\ell$ can be written as $\ell = 2L + 1$ with $L \geqslant 1$. $\mathcal{A}$ sends $|+\rangle$ as their unique challenge query. They thus receive, if $b = 0$ :

$$\frac{1}{\sqrt{2^{\ell n}}} \sum_{x_1, \cdots, x_{2L}} |x_1\rangle_{M_1} \cdots |x_{2L}\rangle_{M_{2L}} \left|E_{\mathsf{k}}\left(x_1 \oplus c_0\right)\right\rangle_{C_1} \left|E_{\mathsf{k}}\left(x_2 \oplus E_{\mathsf{k}}\left(x_1 \oplus c_0\right)\right)\right\rangle_{C_2} \cdots \tag{22}$$

Since they know $c_0$, they can apply $\mathbf{X}$ gates accordingly on $M_1$ to `XOR` it with $c_0$, thus creating the following state:

$$\frac{1}{\sqrt{2^{\ell n}}} \sum_{x_1, \cdots, x_{2L}} |x_1\rangle_{M_1} \cdots |x_{2L}\rangle_{M_{2L}} \left|E_{\mathsf{k}}\left(x_1\right)\right\rangle_{C_1} \left|E_{\mathsf{k}}\left(x_2 \oplus E_{\mathsf{k}}\left(x_1\right)\right)\right\rangle_{C_2} \cdots \tag{23}$$

They now measure $C_{L+1}$, thus getting the associated value $c_{L+1}$ and disturbing the superposition. Indeed, the following equation must hold:

$$c_{L+1} = E_{\mathsf{k}}\left(x_{L+1} \oplus E_{\mathsf{k}}\left(x_L \oplus E_{\mathsf{k}}\left(\cdots \oplus E_{\mathsf{k}}\left(x_1\right) \cdots\right)\right)\right) \tag{24a}$$

$$\iff x_{L+1} = E_{\mathsf{k}}^{-1}\left(c_{L+1}\right) \oplus E_{\mathsf{k}}\left(x_L \oplus E_{\mathsf{k}}\left(\cdots \oplus E_{\mathsf{k}}\left(x_1\right) \cdots\right)\right). \tag{24b}$$

This equation shows that the value of the $M_{L+1}$ register is now $E_{\mathsf{k}}^{-1}\left(c_{L+1}\right) \oplus C_L$. Thus, performing an $\mathbf{X}$ gate on $M_{L+1}$ controlled by $C_L$ sets the value of $M_{L+1}$ to $E_{\mathsf{k}}^{-1}\left(c_{L+1}\right)$. As such, it is no longer entangled with the other registers. Furthermore, the ciphertext registers $C_{L+2}, \cdots, C_{2L}$ are only function of $c_{L+1}$ and the plaintext registers $M_{L+2}, \cdots, M_{2L}$. Hence, the state is now separable and can be written as:

$$\begin{gathered}\left(\frac{1}{\sqrt{2^{Ln}}} \sum_{x_1, \cdots, x_L} |x_1, \cdots, x_L\rangle \left|\mathsf{Enc}^{\mathsf{CBC}}_{E_{\mathsf{k}}, L, 0}\left(x_1 \parallel \cdots \parallel x_L\right)\right\rangle\right) \otimes \\ \left(\frac{1}{\sqrt{2^{Ln}}} \sum_{x_{L+2}, \cdots, x_{2L}} |x_{L+2}, \cdots, x_{2L}\rangle \left|\mathsf{Enc}^{\mathsf{CBC}}_{E_{\mathsf{k}}, L, c_{L+1}}\left(x_{L+2} \parallel \cdots \parallel x_{2L}\right)\right\rangle\right)\end{gathered} \tag{25}$$

where $\mathsf{Enc}^{\mathsf{CBC}}_{E_{\mathsf{k}}, L, r}$ is the encryption function using the $\mathsf{CBC}$ mode of operation with $E_{\mathsf{k}}$ as its block cipher, operating on $L$ blocks and using $r$ as its initialization vector. Note that for any message set of messages $\left(x_i\right)_i$, the following holds:

$$\mathsf{Enc}^{\mathsf{CBC}}_{E_{\mathsf{k}}, L, c_{L+1}}\left(x_{L+2} \parallel \cdots \parallel x_{2L}\right) = \mathsf{Enc}^{\mathsf{CBC}}_{E_{\mathsf{k}}, L, 0}\left(\left(x_{L+2} \oplus c_{L+1}\right) \parallel \cdots \parallel x_{2L}\right). \tag{26}$$

Since $\mathcal{A}$ knows $c_{L+1}$ from the measure of $C_{L+1}$, they can apply $\mathbf{X}$ gates on $M_{L+2}$ to `XOR` it with $c_{L+1}$, thus creating the state:

$$\begin{aligned}&\left(\frac{1}{\sqrt{2^{Ln}}}\sum_{x_1,\cdots,x_L}|x_1,\cdots,x_L\rangle\left|\mathsf{Enc}^{\mathsf{CBC}}_{E_{\mathsf{k}},L,0}\left(x_1\parallel\cdots\parallel x_L\right)\right\rangle\right)\otimes\\&\left(\frac{1}{\sqrt{2^{Ln}}}\sum_{x_{L+2},\cdots,x_{2L}}|x_{L+2},\cdots,x_{2L}\rangle\left|\mathsf{Enc}^{\mathsf{CBC}}_{E_{\mathsf{k}},L,0}\left(x_{L+2}\parallel\cdots\parallel x_{2L}\right)\right\rangle\right)\end{aligned}\tag{27}$$

$$=\left(\frac{1}{\sqrt{2^{Ln}}}\sum_{x}|x\rangle\left|\mathsf{Enc}^{\mathsf{CBC}}_{E_{\mathsf{k}},L,0}(x)\right\rangle\right)\otimes\left(\frac{1}{\sqrt{2^{Ln}}}\sum_{x}|x\rangle\left|\mathsf{Enc}^{\mathsf{CBC}}_{E_{\mathsf{k}},L,0}(x)\right\rangle\right).\tag{28}$$

$\mathcal{A}$ now performs a SWAP test [4] on these two states, which is an algorithm that runs in constant time, taking two quantum states $|\varphi\rangle$ and $|\psi\rangle$ and returning $|0\rangle$ with probability $\frac{1}{2}+\frac{1}{2}\left|\langle\varphi|\psi\rangle\right|^2$. Here, since these two states are identical, performing a SWAP test on them will return $|0\rangle$ with probability 1.

Let us consider the case $b=1$ now. The oracle $\mathcal{A}$ interacts with is depicted on Fig. 2.

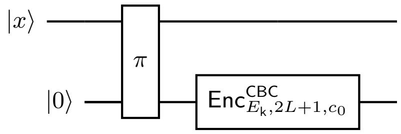

**Fig. 2.** The oracle the adversary interacts with in the random world in the qIND-qCPA-P13 security game of CBC. Note that $\mathsf{Enc}^{\mathsf{CBC}}_{E_{\mathsf{k}},2L+1,c_0}$ can be implemented as an erasing oracle since it is bijective. $\pi$ s a random permutation freshly chosen and implemented as an embedding oracle.

Since $\pi$ is freshly chosen and is implemented as an embedding oracle, we can use [5, Corollary 11] to measure the input register before applying the embedding oracle implementing $\pi$. This Corollary ensures that $\mathcal{A}$ can distinguish the previous oracle from this new one with probability at most $\frac{1+C}{2^{\ell n}}$, with $C$ being an universal constant defined in [18, Theorem 3.1].

Upon measurement, the input register collapses to a random message $x$ and is then passed to the encryption oracle. The resulting state is:

$$|x_1,\cdots,x_{2L}\rangle\,|c_1,\cdots,c_{2L}\rangle\tag{29a}$$

with $c_i$ being defined as:

$$\forall i\in[\![1\,;2L]\!],c_i=E_{\mathsf{k}}\left(\pi_{in\to(i+1)n-1}\left(x_1\parallel x_{2L}\right)\oplus c_{i-1}\right)\tag{29b}$$

and with $c_0$ being chosen uniformly at random. $\mathcal{A}$ firstly measures $c_{L+1}$ and performs a `XOR` operation between $c_0$ and $x_1$ and between $c_{L+1}$ and $x_{L+1}$.

$\mathcal{A}$ will thus perform the SWAP test between $|x_1 \oplus c_0, x_2, \cdots, x_L\rangle|c_1, \cdots, c_L\rangle$ and $|x_{L+2} \oplus c_{L+1}, x_{L+3}, \cdots, x_{2L}\rangle|c_{L+2}, \cdots, c_{2L}\rangle$. Since these two states are basis states, they are either equal or orthogonal. If they are equal, the SWAP test returns $|0\rangle$ with probability 1. If they are orthogonal, it returns $|0\rangle$ with probability $\frac{1}{2}$. Note that the following holds:

$$[\forall i, x_i = x_{L+i+1}] \implies [\forall i, c_i = c_{L+I+1}]\,. \tag{30}$$

Thus, the probability that these two states are equal is the probability that each $x_i$ is equal to $x_{L+i+1}$, which happens with probability $\frac{1}{2^{Ln}}$. All in all, the probability of measuring $|0\rangle$ on average is equal to:

$$\Pr[|0\rangle] = \frac{1}{2^{Ln}} + \frac{1}{2}\left(1 - \frac{1}{2^{LN}}\right) = \frac{1}{2} + \frac{1}{2^{Ln+1}}. \tag{31}$$

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

$$\mathsf{Adv}^{\mathsf{qind\text{-}qcpa\text{-}p13}}_{\mathcal{A},\mathsf{CBC}}(\lambda) \geqslant \frac{1}{2} - \frac{1}{2^{\lfloor\frac{\ell-1}{2}\rfloor n+1}} - \frac{1+C}{2^{\ell n}}. \tag{32}$$

In particular, this advantage is not negligible with respect to $\lambda$. Note that if $\ell$ is odd, the adversary can simply set the first plaintext register to $|0\rangle$. That way, the first ciphertext register will be used as an initialization vector. $\mathcal{A}$ can thus measure it and apply the same strategy as outlined above. □

### 3.4 General results and discussion

The original idea of the IND-CPA security was 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 represent quite abstract information, such as the fact that the plaintext register can be be disentangled with the corresponding ciphertext register, as shown by Theorems 1 and 2. The fact that such strategies can be applied to security notions gives rise to questioning their relevance. This can be taken to the extreme, where commonly used practices kills the potential security of a scheme with respect to some qIND-qCPA notions.

In this section, we prove two general insecurity results about schemes that uses a public function to randomize their encryption (such as the `XOR` one for instance) and those preserving the length of the messages they encrypt. The former concerns the qIND-qCPA-P5 security notion, which we define below.

**Definition 7 (qIND-qCPA-P5 game, adapted from [5]).** *Let $E$ be a cryptographic scheme: $E = (\mathsf{KGen}, \mathsf{Enc}, \mathsf{Dec})$. We denote by $M$ the set of messages $E$ operates on, by $\mathsf{CL}-\mathsf{Enc}$ the classical oracle implementing $\mathsf{Enc}$ and by $\mathsf{EM}-\mathsf{Enc}$ the embedding oracle implementing $\mathsf{Enc}$. We say that $E$ is qIND-qCPA-P5-secure if no polynomial time quantum adversary $\mathcal{A}$ has an advantage larger than $\frac{1}{2}+\varepsilon$ in the following experiment, with $\varepsilon$ being negligible with respect to $\lambda$.*

```
$\textit{Experiment } \textsf{\textit{qIND-qCPA-P5}}_E^b(\lambda, \mathcal{A})$
$\mathsf{k} \leftarrow\!\$\ \mathsf{KGen}\left(1^\lambda\right)$
$\pi \leftarrow\!\$\ \mathfrak{S}_{|M|}$
$b' \leftarrow\!\$\ \mathcal{A}^{\mathsf{CL-Enc(k,\cdot),EM-Enc(k,\cdot,)} \circ \pi^b}()$
$\textbf{return } b'$
```

Intuitively, the qIND-qCPA-P5 security experiment is very similar to the qIND-qCPA-P13 one. In fact, the only difference between these two experiments is that the adversary is allowed to perform multiple challenge queries instead of a single one.

We show that when using a public function to randomize the encryption and providing the adversary with the randomness used, an adversary can manage to get states independent of the said function and randomness in the real world. As such, they can create two identical states and perform a SWAP test on them to measure $|0\rangle$ with probability 1. In the random world however, a fresh permutation is applied on the input register beforehand, making the overlap $\langle\varphi|\psi\rangle$ exponentially small with high probability. The adversary can thus get an advantage close to $\frac{1}{2}$ by exploiting this method, which is what's described in Theorem 4 and its associated proof.

**Theorem 4.** *Let* Enc *be a randomized encryption function from* $\{0,1\}^m \times \{0,1\}^p$ *to* $\{0,1\}^n$*, with* $m$ *being the message length and* $p$ *being the randomness length. If the randomness* $r$ *is given to the adversary and if* Enc *can be written as:*

$$\mathsf{Enc}(x;r) = f(g(x;r))$$

*with* $g$ *being a public, efficient bijective function with respect to* $r$*, then there is an adversary which has an advantage of* $\frac{1}{2} - \frac{1}{2^m}$ *in the qIND-qCPA-P5 security game of* Enc*.*

*Proof.* First of all, let us consider the case $b = 0$. On a challenge request, if $\mathcal{A}$ sends $|+\rangle$, they will receive the following state:

$$\frac{1}{\sqrt{2^m}} \sum_x |x\rangle\, |f(g(x;r))\rangle\,. \tag{33}$$

Since they know $r$, they can apply an erasing oracle implementing $g(\cdot;r)$ on the first register to create the following state:

$$|\psi\rangle = \frac{1}{\sqrt{2^m}} \sum_x |g(x;r)\rangle\, |f(g(x;r))\rangle = \frac{1}{\sqrt{2^m}} \sum_x |x\rangle\, |f(x)\rangle\,. \tag{34}$$

Thus, they are able to create a state which is independent of the randomness that is used. As such, they can perform two challenge request using this method to get $|\psi\rangle \otimes |\psi\rangle$. They can then perform a SWAP test using these two registers, which will return $|0\rangle$ with probability 1.

Let us now consider the case $b = 1$. Using the same method, $\mathcal{A}$ will get the state:

$$\frac{1}{2^m}\left(\sum_{x_0} \left|g\left(x_0; r_0\right)\right\rangle \left|f\left(g\left(\pi_0\left(x_0\right); r_0\right)\right)\right\rangle\right) \otimes \left(\sum_{x_1} \left|g\left(x_1; r_1\right)\right\rangle \left|f\left(g\left(\pi_1\left(x_1\right); r_1\right)\right)\right\rangle\right) \tag{35}$$

and we show that the probability of measuring $|0\rangle$ using the same strategy is close to $\frac{1}{2}$. In order to compute this probability, we need to compute the scalar product of these two states. This scalar product is equal to:

$$\frac{1}{2^m}\sum_{x_0,x_1} \left\langle g\left(x_0; r_0\right), f\left(g\left(\pi_0\left(x_0\right); r_0\right)\right) \middle| g\left(x_1; r_1\right), f\left(g\left(\pi_1\left(x_1\right); r_1\right)\right)\right\rangle \tag{36a}$$

$$= \frac{1}{2^m}\sum_{x_0} \left\langle f\left(g\left(\pi_0\left(x_0\right); r_0\right)\right) \middle| f\left(g\left(\pi_1\left(g^{-1}\left(g\left(x_0; r_0\right); r_1\right)\right); r_1\right)\right)\right\rangle . \tag{36b}$$

This scalar product is thus equal to $\frac{k}{2^m}$, where $k$ is the number of messages $m_0$ such that the following equation is true:

$$f\left(g\left(\pi_0\left(x_0\right); r_0\right)\right) = f\left(g\left(\pi_1\left(g^{-1}\left(g\left(x_0; r_0\right); r_1\right)\right); r_1\right)\right). \tag{37}$$

Since $f$ has to be injective, the previous equation can be rewritten as:

$$g^{-1}\left(g\left(\pi_0\left(x_0\right); r_0\right); r_1\right) = \pi_1\left(g^{-1}\left(g\left(x_0; r_0\right); r_1\right)\right). \tag{38}$$

We now consider $k$ and $\pi_0$ to be fixed and we ought to compute the number of permutations $\pi_1$ such that exactly $k$ of these equations are satisfied.

Note that the number of permutations such that at least $k$ of these equations are satisfied is $\binom{2^m}{k}\left(2^m - k\right)! \sum\limits_{i=0}^{2^m-k} \frac{(-1)^i}{i!}$. Thus, the probability that exactly $k$ of these equations are satisfied is $\frac{1}{k!}\sum\limits_{i=0}^{2^m-k} \frac{(-1)^i}{i!}$. It is thus possible to compute the expected probability of measuring $|0\rangle$:

$$\mathbb{E}\left[\mathbb{P}[|0\rangle]\right] = \frac{1}{2} + \frac{1}{2^{m+1}} \underbrace{\sum_{k=0}^{2^m-1} \frac{k^2}{k!} \sum_{i=0}^{2^m-k} \frac{(-1)^i}{i!}}_{2 \text{ for } m \geqslant 1} = \frac{1}{2} + \frac{1}{2^m}. \tag{39}$$

Thus, $\mathcal{A}$'s advantage is equal to $\frac{1}{2} - \frac{1}{2^m}$. □

We now show an insecurity result with respect to the qIND-qCPA-P8 security notion, which we define below.

**Definition 8 (qIND-qCPA-P8 game, adapted from [5]).** *Let $E$ be a cryptographic scheme: $E = (\mathsf{KGen}, \mathsf{Enc}, \mathsf{Dec})$. We denote by $\mathsf{CL} - \mathsf{Enc}$ the classical oracle implementing $\mathsf{Enc}$, by $\mathsf{ER} - \mathsf{Enc}$ the erasing oracle implementing $\mathsf{Enc}$ and by $\mathcal{M}\,|\psi\rangle$ the measurement in the computational basis of a given register $|\psi\rangle$. We say that $E$ is qIND-qCPA-P8-secure if no polynomial time quantum adversary $\mathcal{A}$ has an advantage larger than $\frac{1}{2} + \varepsilon$ in the following experiment, with $\varepsilon$ being negligible with respect to $\lambda$.*

```
Experiment $\mathit{qIND\text{-}qCPA\text{-}P8}^{b}_{E}(\lambda, \mathcal{A})$
$\mathsf{k} \leftarrow\!\$\ \mathsf{KGen}\left(1^{\lambda}\right)$
$(\mathsf{state}, |\varphi_0\rangle, |\varphi_1\rangle) \leftarrow\!\$\ \mathcal{A}^{\mathsf{CL-Enc}(\mathsf{k},\cdot)}()$
$\mathcal{M}\, |\varphi_{\overline{b}}\rangle$
$|\psi\rangle \leftarrow\!\$\ \mathsf{ER} - \mathsf{Enc}\left(\mathsf{k}, |\varphi_b\rangle\right)$
$b' \leftarrow\!\$\ \mathcal{A}^{\mathsf{CL-Enc}(\mathsf{k},\cdot)}(|\psi\rangle, \mathsf{state})$
return $b'$
```

We show that an adversary can get an advantage of $2^{-d}$ in the qIND-qCPA-P8 security game of a cryptographic scheme, where $d$ is the difference in bitlengths between the ciphertexts and the plaintexts. In particular, an encryption scheme preserving the length of its input can't be qIND-qCPA-P8-secure. This generalizes a result from Gagliardoni et al., who showed this result for the qIND-qCPA-P1 security notion [7], which implies the qIND-qCPA-P8 one.

**Theorem 5 (Originally written in [12]).** *Let* Enc *be a randomized encryption function from* $\{0,1\}^m \times \{0,1\}^p$ *to* $\{0,1\}^n$*, with* $m$ *being the message length and* $p$ *being the randomness length. There is an adversary which has an advantage of* $\frac{2^m}{2^n}$ *in the qIND-qCPA-P8 security game of* Enc*.*

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

$$|+\rangle^m = \frac{1}{\sqrt{2^m}} \sum_x |x\rangle \tag{40a}$$

and

$$|+\rangle^{m-1} |-\rangle = \frac{1}{\sqrt{2^m}} \sum_x (-1)^x |x\rangle \tag{40b}$$

and performs their challenge query using them. They thus receive:

$$\frac{1}{\sqrt{2^m}} \sum_x (-1)^{b \cdot x} |\mathsf{Enc}(x, r_0)\rangle \tag{41}$$

They now apply an $\mathbf{H}$ gate on this state, which results in the following state:

$$\frac{1}{\sqrt{2^{m+n}}} \sum_x (-1)^{b \cdot x} \sum_y (-1)^{y \cdot \mathsf{Enc}(x, r_0)} |y\rangle \tag{42a}$$

$$= \frac{1}{\sqrt{2^{m+n}}} \sum_x (-1)^{b \cdot x} |0\rangle + \frac{1}{\sqrt{2^{m+n}}} \sum_x (-1)^{b \cdot x} \sum_{y \neq 0} (-1)^{y \cdot \mathsf{Enc}(x, r_0)} |y\rangle \tag{42b}$$

$\mathcal{A}$ now measures this state. Note that the probability of measuring $|0\rangle$ is :

$$\left( \frac{1}{\sqrt{2^{m+n}}} \sum_x (-1)^{b \cdot x} \right)^2 = \begin{cases} \frac{2^m}{2^n} & \text{if } b = 0 \\ 0 & \text{otherwise} \end{cases}. \tag{43}$$

The adversary can thus return $b = 0$ if they measure $|0\rangle$ and $b = 1$ otherwise. □

Thus, these two theorems give two necessary conditions for a scheme to be qIND-qCPA-P1 and qIND-qCPA-P2-secure, since both these notions imply the qIND-qCPA-P5 one. Additionally, they give another necessary condition to be qIND-qCPA-P1-secure, since this notion implies the qIND-qCPA-P8 one. The security with respect to these two notions is important, since Carstens et al. proved that being secure with respect to these two notions implied the security with respect to any qIND-qCPA notion [5].

For instance, Carstens et al. showed that the following construction is both qIND-qCPA-P1 and qIND-qCPA-P2-secure:

$$\mathsf{Enc}_{\mathsf{k}}\left(m; r; r'\right) = \mathsf{qPRP}_{r}\left(r' \parallel m\right) \parallel \mathsf{PRP}_{\mathsf{k}}(r).$$

Note that we can consider the second part of the ciphertext to be classically given to the adversary. As such, the ciphertext is $p$ bits longer than the plaintext, with $p$ being the bitlength of the randomness $r'$, which lower-bounds the advantage of an adversary in the qIND-qCPA-P8 security game by $\frac{1}{2^p}$, using Theorem 5. Furthermore, it is to be noted that the randomization of the encryption is not done using a public function, which prevents Theorem 4 from breaking its qIND-qCPA-P5, and as such qIND-qCPA-P1 and qIND-qCPA-P2 security.

It is however important to consider what these results actually mean regarding the security of the studied encryption scheme. For instance, one could argue that in Theorems 1, 2 and 5, the adversary is able to win in the associated security game without learning anything whatsoever about the encryption scheme, which questions the relevance of the associated notions. While this adversary did manage to win in these security games, it is not yet clear what does that imply concerning the confidentiality of the ciphertexts for instance.

In the classical setting, this problem is solved by the semantic security notion, which is equivalent to the IND-CPA one. The intuition behind this notion is that there is low to no difference for an algorithm to be provided with a ciphertext or to be provided with no ciphertext at all. In the quantum setting however, a single quantum semantic security notion has been defined, which is equivalent to the qIND-qCPA-P1 security notion [7]. In order to fully understand what the insecurity with respect to the qIND-qCPA-P5, qIND-qCPA-P8 or qIND-qCPA-P13 security notions means, it is necessary to define the equivalent quantum semantic security notions. Such a task will not only provide a better understanding of these notions and of their relations, but will also help in defining what standard should be adopted to evaluate the quantum security of an encryption scheme.

## 4 Conclusion

In this paper, we have shown that the standard IND-qCPA security results proven by Anand et al. [1] carry on to the erasing and embedding IND-qCPA notions defined by Carstens et al. [5].

We have also shown however that CBC, CTR, OFB, CFB are qIND-qCPA-P13 insecure, no matter what the underlying block cipher is. Since all the security notions but the IND-qCPA ones and the IND-CPA one imply the qIND-qCPA-P13 one, this fully characterizes the security of these modes.

Finally, we gave two general insecurity results on the schemes using a public function to randomize their encryption and on those preserving the length of their input. These two results give necessary conditions for a scheme to be secure with respect to all qIND-qCPA notions and we used these to highlight the need 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 (2019). https://doi.org/10.13154/tosc.v2019.i2.55-93
4. Buhrman, H., Cleve, R., Watrous, J., de Wolf, R.: Quantum fingerprinting. Physical Review Letters **87**(16) (sep 2001). https://doi.org/10.1103/physrevlett.87.167902
5. 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
6. 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
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. Mossayebi, S., Schack, R.: Concrete security against adversaries with quantum superposition access to encryption and decryption oracles (2016)
12. Nemoz, T.: Cryptanalyse quantique d'algorithmes symétriques. Master's thesis, EURECOM (2021)
13. Pinelis, I.: Expectation of the sum of the squares of the cardinal of an inverse function. MathOverflow, https://mathoverflow.net/q/389748
14. 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
15. 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
16. 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
17. Wooding, M.: New proofs for old modes. Cryptology ePrint Archive, Report 2008/121 (2008), https://eprint.iacr.org/2008/121
18. Zhandry, M.: A note on the quantum collision and set equality problems. Quantum Inf. Comput. **15**(7&8), 557–567 (2015). https://doi.org/10.26421/QIC15.7-8-2
19. Zhandry, M.: A note on quantum-secure PRPs. Cryptology ePrint Archive, Report 2016/1076 (2016), https://eprint.iacr.org/2016/1076

# A Adapting Anand et al.'s work to the more general IND-qCPA notions

## A.1 Definitions

Similarly to [1], we define $\mathsf{last}$ and $\mathsf{droplast}$ as the functions which return respectively the last bit of their input and their input without their last bit.

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

$$\begin{cases} E_{h_1(\mathsf{k})}\left[\mathsf{droplast}\,(x)\right] \parallel t_{h_2(\mathsf{k})}(x) & \text{if } \mathsf{last}(x) = 0 \\ E_{h_1(\mathsf{k})}\left[\mathsf{droplast}\,[x \oplus (\mathsf{k} \parallel 1)]\right] \parallel \left[t_{h_2(\mathsf{k})}\,[x \oplus (\mathsf{k} \parallel 1)] \oplus 1\right] & \text{if } \mathsf{last}(x) = 1 \end{cases} \tag{44}$$

with $E$ being a $\mathsf{PRP}$ 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 $\mathsf{PRF}$ taking as input a key of size $\lambda$ and a message of size $\lambda$ 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 $\mathsf{k}$. Anand et al. showed that this block cipher is a $\mathsf{PRP}$ [1].

We also define the relevant security notions.

**Definition 9 (qIND-qCPA-P10 game, adapted from [5]).** *Let $E$ be a cryptographic scheme: $E = (\mathsf{KGen}, \mathsf{Enc}, \mathsf{Dec})$. We denote by $M$ the set of messages $E$ operates on, by $\mathsf{CL} - 1ct - b - \mathsf{Enc}$ the classical oracle implementing $\mathsf{Enc}$ in its 1-ciphertext version: it takes two inputs $m_0$ and $m_1$ and returns the encryption of $m_b$. We also denote $\mathsf{ER} - \mathsf{Enc}$ the erasing oracle implementing $\mathsf{Enc}$. We say that $E$ is qIND-qCPA-P10-secure if no polynomial time quantum adversary $\mathcal{A}$ has an advantage larger than $\frac{1}{2} + \varepsilon$ in the following experiment, with $\varepsilon$ being negligible with respect to $\lambda$.*

```
Experiment $\mathsf{qIND\text{-}qCPA\text{-}P10}^b_E(\lambda, \mathcal{A})$
$\mathsf{k} \leftarrow\!\$\ \mathsf{KGen}\left(1^\lambda\right)$
$\pi \leftarrow\!\$\ \mathfrak{S}_{|M|}$
$b' \leftarrow\!\$\ \mathcal{A}^{\mathsf{ER}-\mathsf{Enc}(\mathsf{k},\cdot),\mathsf{CL}-1ct-b-\mathsf{Enc}(\mathsf{k},\cdot)}()$
return $b'$
```

**Definition 10 (qIND-qCPA-P11 game, adapted from [5]).** *Let $E$ be a cryptographic scheme: $E = (\mathsf{KGen}, \mathsf{Enc}, \mathsf{Dec})$. We denote by $M$ the set of messages $E$ operates on, by $\mathsf{CL} - 1ct - b - \mathsf{Enc}$ the classical oracle implementing $\mathsf{Enc}$ in its 1-ciphertext version: it takes two inputs $m_0$ and $m_1$ and returns the encryption of $m_b$. We also denote $\mathsf{EM} - \mathsf{Enc}$ the embedding oracle implementing $\mathsf{Enc}$. We say that $E$ is qIND-qCPA-P11-secure if no polynomial time quantum adversary $\mathcal{A}$ has an advantage larger than $\frac{1}{2} + \varepsilon$ in the following experiment, with $\varepsilon$ being negligible with respect to $\lambda$.*

```
Experiment $\mathsf{qIND\text{-}qCPA\text{-}P11}^b_E(\lambda, \mathcal{A})$
$\mathsf{k} \leftarrow\!\$\ \mathsf{KGen}\left(1^\lambda\right)$
$\pi \leftarrow\!\$\ \mathfrak{S}_{|M|}$
$b' \leftarrow\!\$\ \mathcal{A}^{\mathsf{EM}-\mathsf{Enc}(\mathsf{k},\cdot),\mathsf{CL}-1ct-b-\mathsf{Enc}(\mathsf{k},\cdot)}()$
return $b'$
```

These notions simply mean that in the qIND-qCPA-P10 game, the adversary is allowed to perform erasing queries on the encryption function, while it is only permitted embedded query in the qIND-qCPA-P11 one.

According to Fig. 1, we ought to show the insecurity of the CBC, CFB, OFB and CTR modes in the qIND-qCPA-P11 notion or their security in the qIND-qCPA-P10 one to fully characterize them.

### A.2 Lemmas

**Lemma 2 (Simon's algorithm, adapted from [15]).** *Let $s$ be 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 $\frac{1}{4}$.*

**Lemma 3 (One-way to Hiding Lemma, originally written in [12]).**

*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:*

$$\left|P^1_{\mathcal{A}} - P^2_{\mathcal{A}}\right| \leqslant 2q\sqrt{P_{\mathcal{B}}}. \tag{45}$$

This lemma is a variant of the original One-way to Hiding Lemma introduced by Unruh [16], 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, Unruh's original proof can almost be reused unmodified. Interested readers can find the proof in appendix B.

### A.3 IND-qCPA security of CTR and OFB

In this section, we show that Anand et al.'s argument [1] to prove the qIND-qCPA-P6 security of CTR and OFB can also be applied to prove its qIND-qCPA-P10 security.

**Theorem 6 (Originally written in [12]).** *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, without loss of generality, let us assume that the adversary has an ancilla register and a query register, so that the sent state could be written as $\sum_{x,y} \alpha_{x,y} |x, y\rangle$. 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. □

### A.4 Potential IND-qCPA insecurity of CFB used with a PRP

We now 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 7 (Originally written in [12]).** *There is a PRP such that the system using it as a block cipher in CFB mode is qIND-qCPA-P11 insecure.*

*Proof.* We use the same block cipher $\mathsf{BC_k}$ as Anand et al. [1], as described in Equation 44. The adversary can prepare the state:

$$\left(\bigotimes_{i=1}^{\ell-2} |0\rangle\right) \sum_x |x\rangle\, |0\rangle \tag{46}$$

and performs a learning request using it, thus receiving the state, omitting the registers that are not entangled with the others:

$$\sum_x |x\rangle_M \left|\mathsf{BC_k^{\ell-1}}\left(c_0\right) \oplus x\right\rangle_{C_1} \left|\mathsf{BC_k}\left(\mathsf{BC_k^{\ell-1}}\left(c_0\right) \oplus x\right)\right\rangle_{C_2}. \tag{47}$$

The adversary then performs an $\mathbf{X}$ gate on $M$ controlled by $C_1$, thus putting it in the basis state $\left|\mathsf{BC_k^{\ell-1}}\left(c_0\right)\right\rangle$, which disentangles it from the other registers. Hence, the state can now be written as:

$$\sum_x \left|\mathsf{BC_k^{\ell-1}}\left(c_0\right) \oplus x\right\rangle_{C_1} \left|\mathsf{BC_k}\left(\mathsf{BC_k^{\ell-1}}\left(c_0\right) \oplus x\right)\right\rangle_{C_2} \tag{48a}$$

$$= \sum_x |x\rangle_{C_1} \left|\mathsf{BC_k}\left(x\right)\right\rangle_{C_2} \tag{48b}$$

$$= \sum_x |x\rangle_{C_1} \left|\mathsf{droplast}\left(\mathsf{BC_k}(x)\right)\right\rangle_{C_{2,2}} \left|\mathsf{last}\left(\mathsf{BC_k}(x)\right)\right\rangle_{C_{2,2}}. \tag{48c}$$

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

$$z = E_{h_1(\mathsf{k})}\left(\mathsf{droplast}\left(x \oplus [(\mathsf{k} \parallel 1) \cdot \mathsf{last}(x)]\right)\right) \tag{49a}$$

$$\iff x \oplus [(\mathsf{k} \parallel 1) \cdot \mathsf{last}(x)] = \begin{cases} E^{-1}_{h_1(\mathsf{k})}(z) \parallel 0 \\ E^{-1}_{h_1(\mathsf{k})}(z) \parallel 1 \end{cases}. \tag{49b}$$

However, we know that for all $Y$, $\mathsf{last}(Y \oplus [(\mathsf{k} \parallel 1) \cdot \mathsf{last}(Y)]) = 0$ holds. As such, a valid message $x$ must satisfy, denoting $Z = E^{-1}_{h_1(\mathsf{k})}(z) \parallel 0$ for conciseness' sake:

$$x \oplus [(\mathsf{k} \parallel 1) \cdot \mathsf{last}\left(x\right)] = Z \tag{49c}$$

$$\iff x = \begin{cases} Z \\ Z \oplus (\mathsf{k} \parallel 1) \end{cases}. \tag{49d}$$

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

$$|Z\rangle_{C_1} \left|t_{h_2(\mathsf{k})}(Z)\right\rangle_{C_{2,2}} + |Z \oplus (\mathsf{k} \parallel 1)\rangle_{C_1} \left|t_{h_2(\mathsf{k})}(Z) \oplus 1\right\rangle_{C_{2,2}} . \tag{50}$$

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 $\left|t_{h_2(\mathsf{k})}(Z)\right\rangle$. Hence, the state the adversary is left with is:

$$|Z\rangle + |Z \oplus (\mathsf{k} \parallel 1)\rangle . \tag{51}$$

The adversary is able to create such a state for each of their learning queries. In particular, they can now make use of Lemma 2 to recover $(\mathsf{k} \parallel 1)$ and as such $\mathsf{k}$. They are now able to easily win in the qIND-qCPA-P11 game by performing a classical challenge query. □

### A.5 Potential IND-qCPA insecurity of CBC used with a PRP

We now show a similar attack on the qIND-qCPA-P13 security of CBC used with a PRP to the one used for CFB.

**Theorem 8.** *There is a PRP such that the system using it as a block cipher in CBC mode is qIND-qCPA-P11 insecure.*

*Proof.* We use the same block cipher $\mathsf{BC}_\mathsf{k}$ as Anand et al. [1], as described in Equation 44. The adversary can prepare the state:

$$\left(\bigotimes_{i=1}^{\ell-1} |0\rangle\right) \sum_x |x\rangle \tag{52}$$

and performs a learning request using it, thus receiving the state, omitting the registers that are not entangled with the others:

$$\sum_x |x\rangle_M \left|\mathsf{BC}_\mathsf{k}\left(\mathsf{BC}_\mathsf{k}^{\ell-1}(c_0) \oplus x\right)\right\rangle_C . \tag{53}$$

Note that $\mathcal{A}$ gets to know the value of $\mathsf{BC}_\mathsf{k}^{\ell-1}(c_0)$ using the previous ciphertext register, which is not entangled with the others. Thus, $\mathcal{A}$ can apply $\mathbf{X}$ gates on $M$ to XOR it with this value, thus creating the state written in Equation 48b. From there, they can apply the same method to recover $\mathsf{k}$ and win in the qIND-qCPA-P11 security game. □

### A.6 IND-qCPA security of CBC and CFB used with a qPRP

We show that Anand et al.'s proof for showing that CBC and CFB are qIND-qCPA-P6 secure when used with a qPRP [1] can be adapted to show that they are also qIND-qCPA-P10 secure. Similarly to their work, we perform the proof for the qIND-qCPA-P10 security of CFB and point out the differences with the one for CBC in brackets.

**Theorem 9 (Originally written in [12]).** *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 qIND-qCPA-P10 security notion. In particular, $\mathcal{A}$ is allowed to perform their learning queries on an erasing oracle. We first show a very similar lemma to Anand et al.'s Lemma 6.

**Lemma 4 (Originally written in [12]).** *For a random permutation $H$, we define $\mathsf{Enc}^i$ 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 $i = 0$, $\mathsf{Enc}^i$ 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:*

$$\begin{aligned}&\Big|\Pr\Big[\mathcal{A}^{\mathsf{Enc}^0}\left(\mathsf{Enc}^i\left(M_b\right)\right) = b \;\Big|\; M_0, M_1 \leftarrow \mathcal{A}^{\mathsf{Enc}^0}\Big] \; - \\ &\quad \Pr\Big[\mathcal{A}^{\mathsf{Enc}^0}\left(\mathsf{Enc}^{i+1}\left(M_b\right)\right) = b \;\Big|\; M_0, M_1 \leftarrow \mathcal{A}^{\mathsf{Enc}^0}\Big]\Big| \leqslant \mathcal{O}\left(\sqrt{\frac{\ell^3 q^3}{2^n}}\right).\end{aligned} \tag{54}$$

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

$$\begin{aligned}\varepsilon(\lambda, n) \overset{\text{def}}{=} \;&\big|\Pr\big[\mathcal{A}^{\mathsf{Enc}}\left(\mathsf{Enc}^i\left(M_b\right)\right) = b \;\big|\; M_0, M_1 \leftarrow \mathcal{A}^{\mathsf{Enc}}\big] \; - \\ &\quad \Pr\big[\mathcal{A}^{\mathsf{Enc}}\left(\mathsf{Enc}^{i+1}\left(M_b\right)\right) = b \;\big|\; M_0, M_1 \leftarrow \mathcal{A}^{\mathsf{Enc}}\big]\big| \,.\end{aligned} \tag{55}$$

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

$$\widetilde{\mathsf{Enc}}^i\left(M, c_0, \cdots, c_i\right) = \hat{c}_0 \dots \hat{c}_\ell \tag{56}$$

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 $c_0, \dots, c_{i+1}$ being uniformly random:

$$\begin{aligned}\varepsilon(\lambda, n) = \;&\Big|\Pr\Big[\mathcal{A}^{\mathsf{Enc}}\Big(\widetilde{\mathsf{Enc}}^i\left(M_b, c_0, \dots, c_i\right)\Big) = b \;\Big|\; M_0, M_1 \leftarrow \mathcal{A}^{\mathsf{Enc}}\Big] \; - \\ &\quad \Pr\Big[\mathcal{A}^{\mathsf{Enc}}\Big(\widetilde{\mathsf{Enc}}^{i+1}\left(M_b, c_0, \dots, c_{i+1}\right)\Big) = b \;\Big|\; M_0, M_1 \leftarrow \mathcal{A}^{\mathsf{Enc}}\Big]\Big| \,.\end{aligned} \tag{57}$$

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 $\varepsilon(\lambda, n)$:

$$\begin{aligned}&\Big|\Pr\Big[\mathcal{A}^{\mathsf{Enc}}\Big(\widetilde{\mathsf{Enc}}^i\left(M_b, c_0, \dots, c_{i-1}, x\right)\Big) = b \;\Big|\; M_0, M_1 \leftarrow \mathcal{A}^{\mathsf{Enc}}\Big] \; - \\ &\quad \Pr\Big[\mathcal{A}^{\mathsf{Enc}}\Big(\widetilde{\mathsf{Enc}}^{i+1}\left(M_b, c_0, \dots, c_{i-1}, x, y \oplus m_b^{i+1}\right)\Big) = b \;\Big|\; M_0, M_1 \leftarrow \mathcal{A}^{\mathsf{Enc}}\Big]\Big| \,.\end{aligned} \tag{58}$$

$$\begin{aligned}&\Big\{\Big|\Pr\Big[\mathcal{A}^{\mathsf{Enc}}\Big(\widetilde{\mathsf{Enc}}^i\left(M_b, c_0, \dots, c_{i-1}, x \oplus m_b^{i+1}\right)\Big) = b \;\Big|\; M_0, M_1 \leftarrow \mathcal{A}^{\mathsf{Enc}}\Big] \; - \\ &\quad \Pr\Big[\mathcal{A}^{\mathsf{Enc}}\Big(\widetilde{\mathsf{Enc}}^{i+1}\left(M_b, c_0, \dots, c_{i-1}, x \oplus m_b^{i+1}, y\right)\Big) = b \;\Big|\; M_0, M_1 \leftarrow \mathcal{A}^{\mathsf{Enc}}\Big]\Big|\Big\} \,.\end{aligned} \tag{58}$$

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

$$\Big|\Pr\Big[\mathcal{A}^{\mathsf{Enc}}\Big(\widetilde{\mathsf{Enc}}^{i+1}\big(M_b, c_0, \ldots, c_{i-1}, x, H(x) \oplus m_b^{i+1}\big)\Big) = b \;\Big|\; M_0, M_1 \leftarrow \mathcal{A}^{\mathsf{Enc}}\Big] - \Pr\Big[\mathcal{A}^{\mathsf{Enc}}\Big(\widetilde{\mathsf{Enc}}^{i+1}\big(M_b, c_0, \ldots, c_{i-1}, x, y \oplus m_b^{i+1}\big)\Big) = b \;\Big|\; M_0, M_1 \leftarrow \mathcal{A}^{\mathsf{Enc}}\Big]\Big|. \tag{59}$$

$$\Big\{\Big|\Pr\Big[\mathcal{A}^{\mathsf{Enc}}\Big(\widetilde{\mathsf{Enc}}^{i+1}\left(M_b, c_0, \ldots, c_{i-1}, x, H(x)\right)\Big) = b \;\Big|\; M_0, M_1 \leftarrow \mathcal{A}^{\mathsf{Enc}}\Big] - \Pr\Big[\mathcal{A}^{\mathsf{Enc}}\Big(\widetilde{\mathsf{Enc}}^{i+1}\big(M_b, c_0, \ldots, c_{i-1}, x, y \oplus m_b^{i+1}\big)\Big) = b \;\Big|\; M_0, M_1 \leftarrow \mathcal{A}^{\mathsf{Enc}}\Big]\Big|\Big\}. \tag{59}$$

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 $\ell$ 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:

$$\varepsilon(\lambda, n) = \left|\Pr\left[\mathcal{A}^H_{O2H}(x, H(x)) = 1\right] - \Pr\left[\mathcal{A}^H_{O2H}(x, y) = 1\right]\right| \tag{60}$$

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 $P_{\mathcal{B}}^{j}$.

**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 $z$:

$$\begin{aligned}
P_{\mathcal{B}}^{j} &= \Pr\big[[\mathcal{B}(x,y) = x] \cup \big[\mathcal{B}(x,y) = H^{-1}(y)\big] \;\big|\; j \leqslant q_1\big] \qquad (61a) \\
&\leqslant \sum_{x'=0}^{2^n-1} \Pr[\mathcal{M} = x' \mid j \leqslant q_1, x' = x]\frac{1}{2^n} + \\
&\quad \sum_{y'=0}^{2^n-1} \Pr\big[\mathcal{M} = y' \;\big|\; j \leqslant q_1, y' = H^{-1}(y)\big]\frac{1}{2^n} \qquad (61b) \\
&\leqslant \frac{1}{2^{n-1}}. \qquad (61c)
\end{aligned}$$

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

$$P_{\mathcal{B}}^{j} \leqslant \frac{1}{2^n} + \frac{1}{2^n}\sum_{y'=0}^{2^n-1} \Pr\big[\mathcal{M} = y' \;\big|\; q_1 < j \leqslant q_2, y' = H^{-1}(y)\big]. \tag{62}$$

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:

$$P_{\mathcal{B}}^{j} \leqslant \frac{1}{2^{n-1}}. \tag{63}$$

**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:

$$P_{\mathcal{B}}^j \leqslant \frac{1}{2^n} + \frac{q_{O2H}}{2^n}. \tag{64}$$

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

$$P_{\mathcal{B}}^j = \sum_{j=1}^{q_{O2H}} P_{\mathcal{B}}^j \frac{1}{q_{O2H}} \leqslant \frac{1 + q_{O2H}}{2^n}. \tag{65}$$

Finally, we have, according to the O2H lemma:

$$\varepsilon(\lambda, n) \leqslant 2q_{O2H}\sqrt{\frac{1 + q_{O2H}}{2^n}} = \mathcal{O}\left(\sqrt{\frac{\ell^3 q^3}{2^n}}\right). \tag{66}$$

□

We can now use this lemma to show the qIND-qCPA-P10 security of CFB {CBC }. 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:

$$\begin{aligned}
&\Big|\Pr\left[\mathcal{A}^{\mathsf{Enc}}\left(\mathsf{Enc}\left(M_b\right)\right) = b \,\middle|\, M_0, M_1 \leftarrow \mathcal{A}^{\mathsf{Enc}}\right] - \\
&\quad \Pr\left[\mathcal{A}^{\mathsf{Enc}}\left(\mathsf{Enc}^{\ell}\left(M_b\right)\right) = b \,\middle|\, M_0, M_1 \leftarrow \mathcal{A}^{\mathsf{Enc}}\right]\Big| && \text{(67a)}\\
&\leqslant \sum_{i=0}^{\ell-1} \Big[\Big|\Pr\left[\mathcal{A}^{\mathsf{Enc}}\left(\mathsf{Enc}\left(M_b\right)\right) = b \,\middle|\, M_0, M_1 \leftarrow \mathcal{A}^{\mathsf{Enc}}\right] - \\
&\quad \Pr\left[\mathcal{A}^{\mathsf{Enc}}\left(\mathsf{Enc}^{\ell}\left(M_b\right)\right) = b \,\middle|\, M_0, M_1 \leftarrow \mathcal{A}^{\mathsf{Enc}}\right]\Big|\Big] && \text{(67b)}\\
&\leqslant \mathcal{O}\left(\sqrt{\frac{\ell^5 q^3}{2^n}}\right). && \text{(67c)}
\end{aligned}$$

$\Pr\left[\mathcal{A}^{\mathsf{Enc}}\left(\mathsf{Enc}^{\ell}\left(M_b\right)\right) = b \,\middle|\, M_0, M_1 \leftarrow \mathcal{A}^{\mathsf{Enc}}\right]$ 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:

$$\mathsf{Adv}^{\mathsf{qind\text{-}qcpa\text{-}p13}}_{\mathcal{A},\mathsf{CFB}}(\lambda) \leqslant \mathcal{O}\left(\sqrt{\frac{\ell^5 q^3}{2^n}}\right) + \mathsf{negl}(\lambda) \tag{68}$$

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

## B Proof of the variant of the One-way to Hiding lemma

*Proof.* We follow very closely Unruh's proof [16] 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 [16], $\mathcal{A}$'s state after having performed $i$ queries to an oracle $\mathcal{O}_H$ implementing an arbitrary bijective function $H$ is written as $\left|\Psi^i_{H,x,y}\right\rangle = \left(\mathbf{U}\mathcal{O}_H\right)^i \left|\Psi_{x,y}\right\rangle$, where $\mathbf{U}$ is an unitary operation chosen by $\mathcal{A}$ and $\left|\Psi_{x,y}\right\rangle$ 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 [16], we define $\alpha$ as $\frac{1}{2^n!2^{2n}}$.

Using these notations, we thus have:

$$P^2_{\mathcal{A}} = \alpha \sum_{H,x,y} \Pr_{\left|\Psi^q_{H,x,y}\right\rangle}[\mathcal{A} = 1] \tag{69}$$

and:

$$P^1_{\mathcal{A}} = \frac{1}{2^n!2^n} \sum_{H,x} \Pr_{\left|\Psi^q_{H,x,H(x)}\right\rangle}[\mathcal{A} = 1]. \tag{70a}$$

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:

$$P^1_{\mathcal{A}} = \alpha \sum_{H,x,y} \Pr_{\left|\Psi^q_{H_{x,y},x,y}\right\rangle}[\mathcal{A} = 1]. \tag{70b}$$

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

$$\begin{aligned} P_{\mathcal{B}} &= \alpha \sum_{H,x,y} \Pr\big[\big[\mathcal{B}^H(x,y) = x\big] \cup \big[\mathcal{B}^H(x,y) = H^{-1}(y)\big] \bigm| H,x,y\big] && (71a) \\ &= \alpha \sum_{H,x,y} \big[\Pr\big[\mathcal{B}^H(x,y) = x \bigm| H,x,y\big] + \Pr\big[\mathcal{B}^H(x,y) = x \bigm| H,x,y\big] \; - \\ &\qquad \delta_{x,H^{-1}(y)} \Pr\big[\mathcal{B}^H(x,y) = x \bigm| H,x,y\big]\big] \,. && (71b) \end{aligned}$$

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 [16]. This allows us to rewrite $P_{\mathcal{B}}$ as:

$$\begin{aligned} P_{\mathcal{B}} &= \frac{\alpha}{q} \sum_{H,x,y,i} \left[\left(1 - \delta_{x,H^{-1}(y)}\right) \left\| Q_x \left|\Psi^{i-1}_{H,x,y}\right\rangle\right\|^2 + \left\| Q_{H^{-1}(y)} \left|\Psi^{i-1}_{H,x,y}\right\rangle\right\|^2\right] && (71c) \\ &= \frac{\alpha}{q} \sum_{H,x,y,i} \left\| \left[\left(1 - \delta_{x,H^{-1}(y)}\right) Q_x + Q_{H^{-1}(y)}\right] \left|\Psi^{i-1}_{H,x,y}\right\rangle\right\|^2 && (71d) \\ &= \frac{\alpha}{q} \sum_{H,x,y,i} \left(1 - \frac{\delta_{x,H^{-1}(y)}}{2}\right)^2 \left\| \left(Q_x + Q_{H^{-1}(y)}\right) \left|\Psi^{i-1}_{H,x,y}\right\rangle\right\|^2 . && (71e) \end{aligned}$$

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:

$$\left| \Pr_{\left|\Psi^q_{H_{x,y},x,y}\right\rangle}[\mathcal{A} = 1] - \Pr_{\left|\Psi^q_{H,x,y}\right\rangle}[\mathcal{A} = 1] \right| \leqslant D_{q,H,x,y} \qquad (72)$$

and:

$$\begin{aligned} D_{i,H,x,y} &= T\left(\mathbf{U}\mathcal{O}_H \left|\Psi^{i-1}_{H,x,y}\right\rangle, \mathbf{U}\mathcal{O}_{H_{x,y}} \left|\Psi^{i-1}_{H_{x,y},x,y}\right\rangle\right) && (73a) \\ &= T\left(\mathcal{O}_H \left|\Psi^{i-1}_{H,x,y}\right\rangle, \mathcal{O}_{H_{x,y}} \left|\Psi^{i-1}_{H_{x,y},x,y}\right\rangle\right) . && (73b) \end{aligned}$$

Thus, using triangle inequality:

$$\begin{aligned} D_{i,H,x,y} &\leqslant T\left(\mathcal{O}_H \left|\Psi^{i-1}_{H,x,y}\right\rangle, \mathcal{O}_{H_{x,y}} \left|\Psi^{i-1}_{H,x,y}\right\rangle\right) + \\ &\qquad T\left(\mathcal{O}_{H_{x,y}} \left|\Psi^{i-1}_{H,x,y}\right\rangle, \mathcal{O}_{H_{x,y}} \left|\Psi^{i-1}_{H_{x,y},x,y}\right\rangle\right) && (74a) \\ &\leqslant T\left(\mathcal{O}_H \left|\Psi^{i-1}_{H,x,y}\right\rangle, \mathcal{O}_{H_{x,y}} \left|\Psi^{i-1}_{H,x,y}\right\rangle\right) + D_{i-1,H,x,y}. && (74b) \end{aligned}$$

Thus:

$$D_{q,H,x,y} - D_{0,H,x,y} \leqslant \sum_{i=1}^{q} T\left(\mathcal{O}_H \left|\Psi^{i-1}_{H,x,y}\right\rangle, \mathcal{O}_{H_{x,y}} \left|\Psi^{i-1}_{H,x,y}\right\rangle\right) . \qquad (75)$$

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

$$\begin{aligned}\mathcal{O}_{H_{x,y}} = \mathcal{O}_H \left(\mathbf{I} - Q_x - Q_{H^{-1}(y)}\right) + \sum_{a,v} |a, x, v \oplus y\rangle \langle a, x, v| + \\ \sum_{a,v} \left|a, H^{-1}(y), v \oplus H(x)\right\rangle \left\langle a, H^{-1}(y), v\right|\end{aligned} \tag{76a}$$

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

$$\mathcal{O}_{H_{x,y}} = \mathcal{O}_H \left(\mathbf{I} - Q_x - Q_{H^{-1}(y)}\right) + \sum_a |a, y\rangle \langle a, x| + \sum_a |a, H(x)\rangle \left\langle a, H^{-1}(y)\right| . \tag{76b}$$

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

$$\mathcal{O}_H \left(\mathbf{I} - Q_x - Q_{H^{-1}(y)}\right) \left|\varPsi^{i-1}_{H,x,y}\right\rangle + \mathcal{O}_H Q_x \left|\varPsi^{i-1}_{H,x,y}\right\rangle + \mathcal{O}_H Q_{H^{-1}(y)} \left|\varPsi^{i-1}_{H,x,y}\right\rangle \tag{77}$$

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

$$\begin{aligned}\mathcal{O}_H \left(\mathbf{I} - Q_x - Q_{H^{-1}(y)}\right) \left|\varPsi^{i-1}_{H,x,y}\right\rangle + \sum_{a,v} |a, x, v \oplus y\rangle \left\langle a, x, v\middle|\varPsi^{i-1}_{H,x,y}\right\rangle + \\ \sum_{a,v} \left|a, H^{-1}(y), v \oplus H(x)\right\rangle \left\langle a, H^{-1}(y), v\middle|\varPsi^{i-1}_{H,x,y}\right\rangle\end{aligned} \tag{78a}$$

or, in the case of an erasing oracle:

$$\begin{aligned}\mathcal{O}_H \left(\mathbf{I} - Q_x - Q_{H^{-1}(y)}\right) \left|\varPsi^{i-1}_{H,x,y}\right\rangle + \sum_a |a, y\rangle \left\langle a, x\middle|\varPsi^{i-1}_{H,x,y}\right\rangle + \\ \sum_a |a, H(x)\rangle \left\langle a, H^{-1}(y)\middle|\varPsi^{i-1}_{H,x,y}\right\rangle .\end{aligned} \tag{78b}$$

Writing these states like this allows us to use Unruh's Lemma 11 [16], which ensures that $T\left(\mathcal{O}_H \left|\varPsi^{i-1}_{H,x,y}\right\rangle, \mathcal{O}_{H_{x,y}} \left|\varPsi^{i-1}_{H,x,y}\right\rangle\right)$ is upper-bounded by:

$$2 \left\|\mathcal{O}_H Q_x \left|\varPsi^{i-1}_{H,x,y}\right\rangle + \mathcal{O}_H Q_{H^{-1}(y)} \left|\varPsi^{i-1}_{H,x,y}\right\rangle\right\| \tag{79a}$$

$$\leqslant 2 \left\|\left(Q_x + Q_{H^{-1}(y)}\right) \left|\varPsi^{i-1}_{H,x,y}\right\rangle\right\| \tag{79b}$$

$$\leqslant 2 \left(1 - \delta_{x,H^{-1}(y)}\right) \left\|\left(Q_x + Q_{H^{-1}(y)}\right) \left|\varPsi^{i-1}_{H,x,y}\right\rangle\right\| . \tag{79c}$$

Thus, using triangle inequality and Equations 72 and 75:

$$\left|P^1_{\mathcal{A}} - P^2_{\mathcal{A}}\right| \leqslant \alpha \sum_{H,x,y,i} 2 \left(1 - \delta_{x,H^{-1}(y)}\right) \left\|\left(Q_x + Q_{H^{-1}(y)}\right) \left|\varPsi^{i-1}_{H,x,y}\right\rangle\right\|^2 \tag{80a}$$

$$\leqslant 2q \sum_{H,x,y,i} \frac{\alpha}{q} \sqrt{\left(1 - \delta_{x,H^{-1}(y)}\right) \left\|\left(Q_x + Q_{H^{-1}(y)}\right) \left|\varPsi^{i-1}_{H,x,y}\right\rangle\right\|^2}. \tag{80b}$$

Hence, using Jensen's inequality:

$$\left|P_{\mathcal{A}}^{1}-P_{\mathcal{A}}^{2}\right| \leqslant 2q\sqrt{\frac{\alpha}{q}\sum_{H,x,y,i}\left(1-\delta_{x,H^{-1}(y)}\right)\left\|\left(Q_x+Q_{H^{-1}(y)}\right)\left|\Psi_{H,x,y}^{i-1}\right\rangle\right\|^2}. \quad (81)$$

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