entropy

IMPACT FACTOR 2.0

Indexed in: PubMed

CITESCORE 5.2

Article

Quantum Security of Nonce-Based Encryption

Shuping Mao, Peng Wang, Yan Jia, Gang Liu and Bing Liu

MDPI

https://doi.org/10.3390/e27121194

entropy

MDPI

Article

Quantum Security of Nonce-Based Encryption

Shuping Mao [1], Peng Wang [2], Yan Jia [3,4], Gang Liu [5,*] and Bing Liu [1]

[1] Beijing Electronic Science & Technology Institute, Beijing 100070, China; maoshuping19@mails.ucas.ac.cn (S.M.); leoliu76@outlook.com (B.L.)
[2] School of Cryptology, University of Chinese Academy of Sciences, Beijing 100049, China; p-wang@ucas.ac.cn
[3] State Key Laboratory of Cyberspace Security Defense, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100085, China; jiayan22@mails.ucas.ac.cn
[4] School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China
[5] National Key Laboratory of Security Communication, Chengdu 610041, China
* Correspondence: liugang@hnu.edu.cn

Abstract

We investigate the quantum security of nonce-based encryption under the indistinguishability against quantum chosen-plaintext attacks (IND-qCPA). While classical results establish that IV-based modes such as CBC, CFB, OFB, and CTR achieve IND-qCPA security, we demonstrate that simply replacing the random IV with a nonce undermines both classical and quantum security. To address this, we propose a general transformation from R-IND-qCPA security to N-IND-qCPA security and introduce enhanced variants, namely, CBC2, CFB2, OFB2, and CTR2, that are provably secure in the nonce-based quantum setting. We further show that nonce-based stream cipher encryption inherently satisfies N-IND-qCPA security. These results provide a systematic framework for upgrading IV-based constructions to secure nonce-based counterparts, thereby strengthening practical symmetric encryption against quantum adversaries.

Keywords: nonce-based encryption; R-IND-qCPA; N-IND-qCPA

Academic Editor: Osamu Hirota

Received: 3 October 2025
Revised: 17 November 2025
Accepted: 24 November 2025
Published: 24 November 2025

Citation: Mao, S.; Wang, P.; Jia, Y.; Liu, G.; Liu, B. Quantum Security of Nonce-Based Encryption. *Entropy* **2025**, *27*, 1194. https://doi.org/10.3390/e27121194

1. Introduction

A block cipher is a basic building block in modern cryptography, usually modeled as a random permutation on fixed-length inputs. In practice, messages are often much longer than a single block and may vary in length, which requires the use of block cipher modes of operation to extend encryption to arbitrary-length inputs. Modes of operation are generally divided into three categories: encryption modes, authentication modes, and authenticated encryption modes. The earliest encryption modes, such as ECB, CBC, OFB, and CFB, provided confidentiality only. To ensure integrity, authentication modes such as CBC-MAC were developed, and later integrated designs such as CCM, GCM, and OCB were proposed to achieve both confidentiality and integrity.

The progress of quantum algorithms has posed serious challenges to these modes. When adversaries are allowed quantum query access to the underlying primitive, algorithms such as Grover's search [1] and Simon's algorithm [2] can be applied to mount attacks. Under this setting, reduced-round Feistel and Lai–Massey structures, the Even–Mansour cipher, LRW [3–7], authentication modes including CBC-MAC, PMAC, and GMAC [7], and authenticated encryption modes such as OCB and GCM [7–10] have been shown to be insecure.

Against this background, the quantum security of encryption modes has become a central research topic. The natural adaptation of the classical indistinguishability un-

der chosen-plaintext attack (IND-CPA) model to the quantum setting is the IND-qCPA model [11], where challenge queries remain classical, encryption queries may be quantum, and the adversary's distinguishing advantage quantifies security. Because encryption modes aim only at confidentiality, proving IND-qCPA security suffices in the quantum setting. It is important to note that existing quantum security models are probabilistic, in which a random value r is included during the encryption process. Unlike plaintexts and ciphertexts, which may be in quantum superposition, the random value r is always treated as a classical number.

Based on the nature of the random value r, encryption schemes can be categorized into IV-based encryption schemes and nonce-based encryption schemes. Among these, an initialization vector IV is required to be random, whereas a nonce N is required only to be arbitrarily chosen but non-repeating. Compared with random IVs, nonces are easier to generate, avoid reliance on high-quality randomness, and better match practical deployment requirements in modern cryptographic protocols.

The quantum security of encryption schemes varies depending on the type of random value employed. In 2016, Vivekanand et al. [12] demonstrated that encryption modes such as CBC, CFB, OFB, and CTR achieve IND-qCPA security when a random IV is used. In 2021, Bhaumik et al. [8] proposed a new design called QCB, based on OCB, and proved that QCB satisfies IND-qCPA security under the non-adaptive nonce setting. Here, a non-adaptive nonce refers to one that may be arbitrarily chosen but must be selected entirely in advance prior to any encryption queries. In 2025, Lang et al. [13] provided the first formal definition of IND-qCPA security in the adaptive nonce model, although no concrete instantiation has been proposed to date. In addition, there are also studies on the quantum security of block ciphers and their modes of operation [14–17].

We refer to IV-based IND-qCPA as R-IND-qCPA and nonce-based IND-qCPA as N-IND-qCPA. Although CBC, CFB, OFB, and CTR achieve IND-qCPA security when a random IV is used (that is, they are R-IND-qCPA secure), Section 3 demonstrates that replacing the IV with a nonce N not only fails to provide IND-qCPA security but also undermines even IND-CPA security. Enhancing encryption schemes to achieve N-IND-qCPA security constitutes a primary focus of this work.

The main results in the paper are as follows (Table 1):

1. We present a general transformation that converts any R-IND-qCPA secure encryption scheme into an N-IND-qCPA secure scheme.
2. We propose enhanced variants of CBC, CFB, OFB, and CTR, referred to as CBC2, CFB2, OFB2, and CTR2, and provide formal proofs of their security under the N-IND-qCPA definition.
3. We further show that nonce-based stream cipher encryption inherently satisfies N-IND-qCPA security.

Table 1. R-IND-CPA, N-IND-CPA, R-IND-qCPA, N-IND-qCPA security of encryption schemes.

Encryption Schemes	R-IND-CPA	N-IND-CPA	R-IND-qCPA	N-IND-qCPA	Ref.
CBC	yes	no	yes	no	[12], Section 3
CFB	yes	no	yes	no	[12], Section 3
OFB	yes	no	yes	no	[12], Section 3
CTR	yes	no	yes	no	[12], Section 3
CBC2	yes	yes	yes	yes	Section 4
CFB2	yes	yes	yes	yes	Section 5
OFB2	yes	yes	yes	yes	Section 5
CTR2	yes	yes	yes	yes	Section 5

The structure of this paper is organized as follows: Section 2 introduces definitions and notation; Section 3 presents N-IND-CPA attacks against CBC, CFB, OFB, and CTR; Section 4 provides the N-IND-qCPA security proof for CBC2; Section 5 discusses improvements and proofs for other encryption schemes; and Section 6 offers concluding remarks.

2. Preliminaries

2.1. Notations

Block Cipher. A block cipher $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ is a map with key space $\{0,1\}^k$ and message space $\{0,1\}^n$ such that for every key $K \in \{0,1\}^k$, $P \mapsto E(K,P)$ is a permutation on $\{0,1\}^n$. Let E_K denote the map $P \mapsto E(K,P)$.

Let $x \xleftarrow{\$} \{0,1\}^n$ denote selecting an element x from the set $\{0,1\}^n$ uniformly at random. Let $\mathrm{Perm}(n)$ be a set of all permutations on $\{0,1\}^n$. Let $\pi \xleftarrow{\$} \mathrm{Perm}(n)$ be a random permutation on $\{0,1\}^n$. A block cipher keyed by K is a function $E_K \in \mathrm{Perm}(n)$. We call the input and output of E_K as plaintext and ciphertext, respectively. Let $\mathrm{Func}(m,n)$ be the set of all functions from $\{0,1\}^m$ to $\{0,1\}^n$. We write $\mathrm{Func}(n,n)$ as $\mathrm{Func}(n)$.

IV-Based Encryption Scheme. Encryption schemes are typically defined as either probabilistic or stateful. In the context of symmetric cryptography, the randomness or state involved in the encryption process is usually represented explicitly by an initialization vector (IV), meaning that both encryption and decryption can be formalized as deterministic algorithms. The following provides the syntax definition of an IV-based encryption scheme. An IV-based encryption scheme is a pair of algorithms $\Pi = (Enc, Dec)$, where $Enc : \mathsf{Key} \times \mathsf{IV} \times \mathsf{Plaintext} \to \mathsf{Ciphertext}$ and $Dec : \mathsf{Key} \times \mathsf{IV} \times \mathsf{Ciphertext} \to \mathsf{Plaintext}$ are deterministic functions with key space, IV space IV, plaintext space Plaintext, and ciphertext space Ciphertext. We require that $Dec(K, IV, Enc_K(IV, P)) = P$ for any $K \in \mathsf{Key}$ and $IV \in \mathsf{IV}$ and $P \in \mathsf{Plaintext}$. Note that here, for a probabilistic encryption scheme IV is randomly selected from IV.

Nonce-Based Encryption Scheme. If the only requirement on the initialization vector (IV) is that it must not repeat, then even allowing the adversary to choose the IV is acceptable. In this case, the IV is referred to as a nonce, and the corresponding construction is called a nonce-based encryption scheme. Because the syntax of IV-based and nonce-based encryption schemes is identical, the latter simply relaxes the requirements on how the IV is generated. This relaxation greatly facilitates the secure deployment of symmetric encryption, as producing a random IV would otherwise require the additional implementation of a secure random number generator. To highlight the distinction, in the syntax definition the IV space IV is usually replaced by a nonce space Nonce.

2.2. Security Definitions

Let $\mathcal{A}$ be an adversary. Let $\mathcal{A}^{\mathcal{O}} = b$ denote an algorithm that performs queries on the oracle $\mathcal{O}$ and produces the bit of b. In the context of a (keyed) function f, for a classical query X, the response is the value $f(X)$. In contrast, a quantum query is given as a quantum superposition state $\sum \psi_{X,Y}|X\rangle|Y\rangle$, and the response is given by $\sum \psi_{X,Y}|X\rangle|Y \oplus f(X)\rangle$.

For two oracles $\mathcal{O}_1$ and $\mathcal{O}_2$, the classical and quantum distinguishing advantage of $\mathcal{A}$ is defined respectively as follows:

$$\mathrm{Adv}^{\mathrm{dist}}_{\mathcal{O}_1,\mathcal{O}_2}(\mathcal{A}) := |\Pr[\mathcal{A}^{\mathcal{O}_1(\cdot)} = 1] - \Pr[\mathcal{A}^{\mathcal{O}_2(\cdot)} = 1]|,$$
$$\mathrm{Adv}^{\mathrm{qdist}}_{\mathcal{O}_1,\mathcal{O}_2}(\mathcal{A}) := |\Pr[\mathcal{A}^{\mathcal{O}_1(*)} = 1] - \Pr[\mathcal{A}^{\mathcal{O}_2(*)} = 1]|,$$

where we use $\cdot$ to denote a classical query and $\odot$ to denote a quantum query.

Definition 1 (PRF/qPRF). *A (quantum-secure) pseudorandom function ((q)PRF) is an efficiently computable function family $f : \{0,1\}^k \times \{0,1\}^s \to \{0,1\}^n$ for all (quantum) algorithms $\mathcal{A}$,*

$$\left| \Pr_{k \xleftarrow{\$} \{0,1\}^k} \left[\mathcal{A}^{f_k}(*) = 1 \right] - \Pr_{g \xleftarrow{\$} \mathrm{Func}(s,n)} [\mathcal{A}^{g}(*) = 1] \right| \leq \mathrm{negl},$$

where g is a random function from $\{0,1\}^s$ to $\{0,1\}^n$ and where we replace the $*$ symbol by $\cdot$ to denote a classical query or $\odot$ to denote a quantum query).

Definition 2 (PRF/qPRF/PRP/qPRP Advantages). *Let $F : \{0,1\}^k \times \{0,1\}^s \to \{0,1\}^n$ be a function. Let $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher. Let $f \leftarrow \mathrm{Func}(s,n)$ be a random function. Let $p \leftarrow \mathrm{Perm}(n)$ be a random permutation. We assume that all keys are random. The PRF/qPRF/PRP/qPRP advantages are defined as follows:*

$$\begin{aligned} \mathrm{Adv}_F^{PRF}(\mathcal{A}) &= \mathrm{Adv}^{\mathrm{dist}}_{F_K,f}(\mathcal{A}), \\ \mathrm{Adv}_F^{qPRF}(\mathcal{A}) &= \mathrm{Adv}^{\mathrm{qdist}}_{F_K,f}(\mathcal{A}), \\ \mathrm{Adv}_E^{PRP}(\mathcal{A}) &= \mathrm{Adv}^{\mathrm{dist}}_{E_K,\pi}(\mathcal{A}), \\ \mathrm{Adv}_E^{qPRP}(\mathcal{A}) &= \mathrm{Adv}^{\mathrm{qdist}}_{E_K,\pi}(\mathcal{A}). \end{aligned}$$

Definition 3 (Secure Stream Cipher). *A secure stream cipher is an efficiently computable function $SC : \{0,1\}^k \times \{0,1\}^s \to \{0,1\}^L$ that takes a key k and nonce N, then outputs a keystream of length L. For all probabilistic polynomial-time adversaries $\mathcal{A}$, the following advantage is negligible:*

$$\left| \Pr_{K \xleftarrow{\$} \{0,1\}^k} \left[\mathcal{A}^{SC_K(\cdot)} = 1 \right] - \Pr_{g \xleftarrow{\$} \mathrm{Func}(s,L)} [\mathcal{A}^{g}(\cdot) = 1] \right| \leq \mathrm{negl},$$

where g is a random function from $\{0,1\}^s$ to $\{0,1\}^L$.

In the following, we present the definitions of R-IND-CPA and N-IND-CPA.

Definition 4 (R-IND-CPA). *For an encryption scheme $\Pi = (\mathrm{Enc}, \mathrm{Dec})$ and an adversary $\mathcal{A}$, we define the advantage of indistinguishability under a chosen plaintext attack in the random-IV setting (R-IND-CPA) using the following game:*

***Key Generation**: The challenger picks a random key K and a random bit b.*
***Queries**: $\mathcal{A}$ is allowed to make two types of queries:*

> ***Challenge Queries**: $\mathcal{A}$ sends two plaintexts P_0, P_1, to which the challenger chooses randomness R and responds with $C^* = R \| \mathrm{Enc}_K(R, P_b)$.*
> ***Encryption Queries**: For each such query of P, the challenger chooses randomness R and responds with $C = R \| Enc_K(R, P)$.*

***Guess**: $\mathcal{A}$ produces a bit b' and wins if $b = b'$.*

The R-IND-CPA advantage of an adversary $\mathcal{A}$ is defined as

$$\mathrm{Adv}_{\Pi}^{R\text{-}IND\text{-}CPA}(\mathcal{A}) = |2 \Pr[\mathcal{A} \textit{ success }] - 1|.$$

Definition 5 (N-IND-CPA). *For an encryption scheme $\Pi = (\mathrm{Enc}, \mathrm{Dec})$ and an adversary $\mathcal{A}$, we define the advantage of indistinguishability under a chosen plaintext attack in the nonce setting (N-IND-CPA) using the following game:*

***Key Generation**: The challenger picks a random key K and a random bit b.*
***Queries**: $\mathcal{A}$ is allowed to make two types of queries:*

Challenge Queries: *$\mathcal{A}$ sends a nonce N and two plaintexts P_0, P_1, to which the challenger responds with $C^* = \mathrm{Enc}_K(N, P_b)$.*
Encryption Queries: *For each such query of (N, P), the challenger chooses randomness R and responds with $C = R \| Enc_K(N, P)$.*

Guess: *$\mathcal{A}$ produces a bit b', and wins if $b = b'$.*

We stress that the nonce N in the above game never repeats. The N-IND-CPA advantage of an adversary $\mathcal{A}$ is defined as

$$\mathrm{Adv}_{\Pi}^{\textit{N-IND-CPA}}(\mathcal{A}) = |2\Pr[\mathcal{A}\ \textit{success}\ ] - 1|.$$

In the following, we define R-IND-qCPA and N-IND-qCPA.

Definition 6 (R-IND-qCPA)**.** *For an encryption scheme $\Pi = (\mathrm{Enc}, \mathrm{Dec})$ and an adversary $\mathcal{A}$, we define the advantage of indistinguishability under a quantum chosen plaintext attack in the random-IV setting (R-IND-qCPA) using the following game:*

Key Generation: *The challenger picks a random key K and a random bit b.*
Queries: *$\mathcal{A}$ is allowed to make two types of queries:*

Challenge Queries: *$\mathcal{A}$ sends two classical messages P_0, P_1, to which the challenger chooses classical randomness R and responds with classical $C^* = R \| \mathrm{Enc}_K(R, P_b)$.*
Encryption Queries: *For each such query of P, the challenger chooses classical randomness R and encrypts each plaintext in the quantum superposition using R as the randomness:*

$$\sum_{P,C} \psi_{P,C} |P, C\rangle \rightarrow \sum_{P,C} \psi_{P,C} |P, C \oplus (R \| \mathrm{Enc}_K(R, P))\rangle.$$

Guess: *$\mathcal{A}$ produces a bit b' and wins if $b = b'$.*

The R-IND-qCPA advantage of an adversary $\mathcal{A}$ is defined as

$$\mathrm{Adv}_{\Pi}^{\textit{R-IND-qCPA}}(\mathcal{A}) = |2\Pr[\mathcal{A}\ \textit{success}\ ] - 1|.$$

Definition 7 (N-IND-qCPA)**.** *For an encryption scheme $\Pi = (\mathrm{Enc}, \mathrm{Dec})$ and an adversary $\mathcal{A}$, we define the advantage of indistinguishability under a quantum chosen plaintext attack in the nonce setting (N-IND-qCPA) using the following game:*

Key Generation: *The challenger picks a random key K and a random bit b.*
Queries: *$\mathcal{A}$ is allowed to make two types of queries:*

Challenge Queries: *$\mathcal{A}$ sends a classical nonce N and two classical messages P_0, P_1, to which the challenger responds with classical $C^* = \mathrm{Enc}_K(N, P_b)$.*
Encryption Queries: *For each such query of a classical nonce N and a plaintext in the quantum superposition, the challenger encrypts using the following transformation:*

$$\sum_{P,C} \psi_{P,C} |P, C\rangle \rightarrow \sum_{P,C} \psi_{P,C} |P, C \oplus \mathrm{Enc}_K(N, P)\rangle.$$

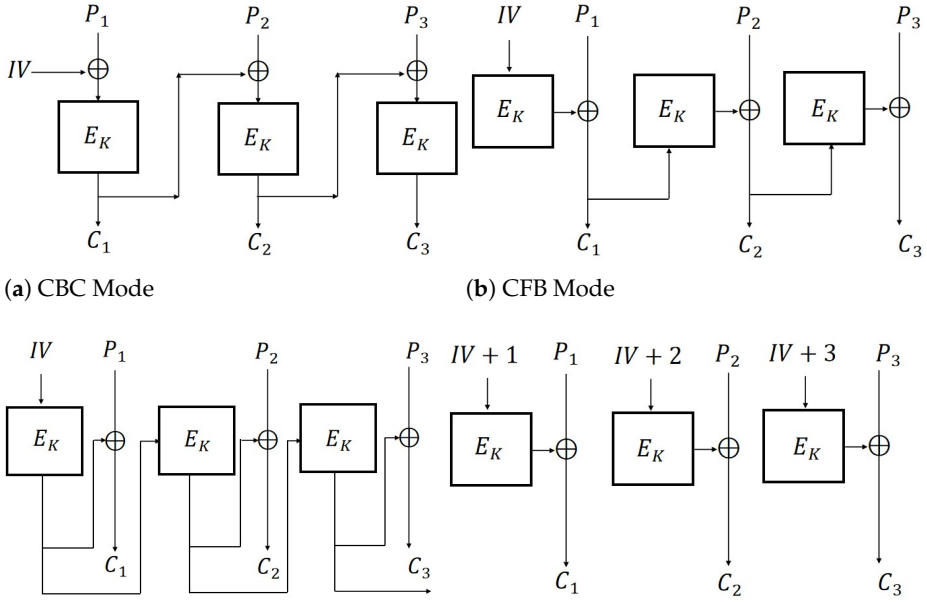
Guess: *$\mathcal{A}$ produces a bit b' and wins if $b = b'$.*

The N-IND-qCPA advantage of an adversary $\mathcal{A}$ is defined as

$$\mathrm{Adv}_{\Pi}^{\textit{N-IND-qCPA}}(\mathcal{A}) = |2\Pr[\mathcal{A}\ \textit{success}\ ] - 1|.$$

2.3. Encryption Modes

The encryption schemes CBC, CFB, OFB, and CTR (Figure 1) are defined as follows:



(**a**) CBC Mode (**b**) CFB Mode

(**c**) OFB Mode (**d**) CTR Mode

Figure 1. Encryption modes ($m = 3$).

Definition 8 (CBC Mode)**.** *Let* $K \in$ Key *and* $IV \in$ IV*. For a given message* $P = P_1P_2 \cdots P_m$*, where* $P_i (i = 1, 2, \cdots, m)$ *is a block of the message, the symmetric encryption scheme CBC is defined as follows:*

Enc: $C_0 = IV$ *and* $C_i = E_K(P_i \oplus C_{i-1})$ *for* $1 \le i \le m$*.* $Enc_K(P) = C_0 \| C_1 \cdots C_m$*.*
Dec: For a given ciphertext $C = C_1 \cdots C_m$ *and* $C_0 = IV$*,* $P_i := E_K^{-1}(C_i) \oplus C_{i-1}$ *for* $1 \le i \le m$*.* $Dec_K(C) = P_1 \cdots P_m$*.*

Definition 9 (CFB Mode)**.** *Let* $K \in$ Key *and* $IV \in$ IV*. For a given message* $P = P_1P_2 \cdots P_m$*, where* $P_i (i = 1, 2, \cdots, m)$ *is a block of the message, the symmetric encryption scheme CFB is defined as follows:*

Enc: $C_0 = IV$ *and* $C_i = E_K(C_{i-1}) \oplus P_i$ *for* $1 \le i \le m$*.* $Enc_K(P) = C_0 \| C_1 \cdots C_m$*.*
Dec: For a given ciphertext $C = C_1 \cdots C_m$ *and* $C_0 = IV$*,* $P_i := E_K(C_{i-1}) \oplus C_i$ *for* $1 \le i \le m$*.* $Dec_K(C) = P_1 \cdots P_m$*.*

Definition 10 (OFB Mode)**.** *Let* $K \in$ Key *and* $IV \in$ IV*. For a given message* $P = P_1P_2 \cdots P_m$*, where* $P_i (i = 1, 2, \cdots, m)$ *is a block of the message, the symmetric encryption scheme OFB is defined as follows:*

Enc: $C_0 = R_0 = IV$*,* $R_i = E_K(R_{i-1})$ *and* $C_i = R_{i-1} \oplus P_i$ *for* $1 \le i \le m$*.* $Enc_K(P) = C_0 \| C_1 \cdots C_m$*.*
Dec: For a given ciphertext $C = C_1 \cdots C_m$ *and* $C_0 = IV$*,* $P_i := E_K(C_{i-1}) \oplus C_i$ *for* $1 \le i \le m$*.* $Dec_K(C) = P_1 \cdots P_m$*.*

Definition 11 (CTR Mode)**.** *Let* $K \in$ Key *and* $IV \in$ IV*. For a given message* $P = P_1P_2 \cdots P_m$*, where* $P_i (i = 1, 2, \cdots, m)$ *is a block of the message, the symmetric encryption scheme CTR is defined as follows:*

1. *Enc:* $C_0 = IV$ *and* $C_i = E_K(C_0 + i) \oplus P_i$ *for* $1 \le i \le m$*.* $Enc_K(P) = C_0 \| C_1 \cdots C_m$*.*
2. *Dec: For a given ciphertext* $C = C_1 \cdots C_m$ *and* $C_0 = IV$*,* $P_i := E_K(C_0 + i) \oplus C_i$ *for* $1 \le i \le m$*.* $Dec_K(C) = P_1 \cdots P_m$*.*

According to [12], CBC, CFB, OFB and CTR are R-IND-qCPA secure, and therefore R-IND-CPA secure.

Theorem 1 (Theorem 3 and Theorem 4 in [12]). *If the function E is a quantum secure PRF, then CBC, CFB, OFB, and CTR are R-IND-qCPA secure.*

However, our research will indicate that none of them are N-IND-CPA secure, and therefore not N-IND-qCPA secure.

3. N-IND-CPA/N-IND-qCPA Attacks With Nonce-Based Encryption Scheme

We noticed that CBC, CFB, OFB, and CTR only maintain the security of Theorem 1 when C_0 is a random IV. If we replace IV with nonce N (which can be selected but not repeated), then CBC, CFB, OFB, and CTR do not even maintain classical security; therefore, they are not N-IND-qCPA secure. For convenience, we define P_i^j as the i-th block in the j-th query. It is easy to argue that the advantage of these attacks is 1.

IND-CPA attack on CBC mode. The IND-CPA attack on CBC is similar to the attack in [18]. The specific process (Figure 2) is as follows :

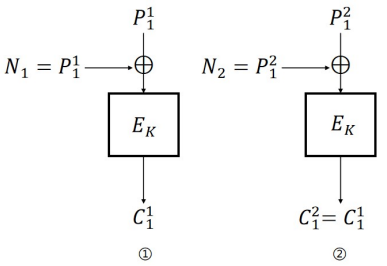


Figure 2. IND-CPA attack on CBC scheme.

1. Encryption query: Let $N_1 = P_1^1$; then, $C_1^1 = E_K(0^n)$.
2. Challenge query: Let $P_0 = P_1^2 \neq P_1^1$, $P_1 \xleftarrow{\$} \{0,1\}^n$, $P_1 \neq P_0$, and $N_2 = P_1^2$; then, $b' = 0$ if $C_1^2 = C_1^1$, otherwise $b' = 1$.

For CBC mode, as long as $N_2 = P_1^2$, there will be $C_1^2 = C_1^1$; thus, the probability of adversary $\mathcal{A}$'s success is 1. The distinguishing advantages are: $\mathrm{Adv}_{CBC}^{\text{N-IND-CPA}}(\mathcal{A}) = 1$. Therefore, $\mathrm{Adv}_{CBC}^{\text{N-IND-qCPA}}(\mathcal{A}) = 1$.

IND-CPA attack on CFB mode. The steps of the IND-CPA attack (Figure 3) against the CFB scheme are as follows:

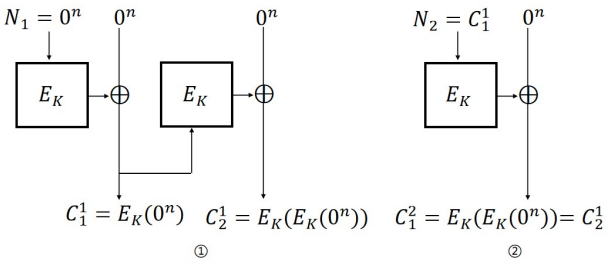


Figure 3. IND-CPA attack on CFB scheme.

1. Encryption query: Let $N_1 = P_1^1 = P_2^1 = 0$; then, $C_1^1 = E_K(0^n)$ and $C_2^1 = E_K(E_K(0^n))$.
2. Challenge query: Let $P_0 = 0^n$, $P_1 \xleftarrow{\$} \{0,1\}^n$, $P_1 \neq P_0$, and $N_2 = C_1^1 = E_K(0^n)$; then, $b' = 0$ if $C_1^2 = C_1^1$, otherwise $b' = 1$.

For CFB mode, the probability of adversary $\mathcal{A}$'s success is 1. The distinguishing advantages are: $\mathrm{Adv}_{CFB}^{\text{N-IND-CPA}}(\mathcal{A}) = 1$. Therefore, $\mathrm{Adv}_{CFB}^{\text{N-IND-qCPA}}(\mathcal{A}) = 1$.

IND-CPA attack on OFB mode. The steps of the IND-CPA attack (Figure 4) against the OFB scheme are as follows:

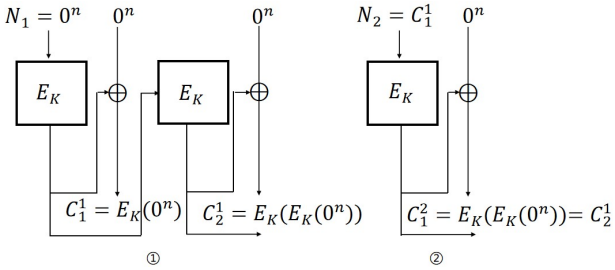


Figure 4. IND-CPA attack on OFB scheme.

1. Encryption query: Let $N_1 = P_1^1 = P_2^1 = 0$; then, $C_1^1 = E_K(0^n)$ and $C_2^1 = E_K(E_K(0^n))$.
2. Challenge query: Let $P_0 = 0^n$, $P_1 \xleftarrow{\$} \{0,1\}^n$, $P_1 \neq P_0$ and $N_2 = C_1^1 = E_K(0^n)$; then, $b' = 0$ if $C_1^2 = C_1^1$, otherwise $b' = 1$.

For OFB mode, the probability of adversary $\mathcal{A}$'s success is 1. The distinguishing advantages are: $\mathrm{Adv}_{OFB}^{\text{N-IND-CPA}}(\mathcal{A}) = 1$. Therefore, $\mathrm{Adv}_{OFB}^{\text{N-IND-qCPA}}(\mathcal{A}) = 1$.

IND-CPA attack on CTR mode. The steps of the IND-CPA attack (Figure 5) against the CTR scheme are as follows:

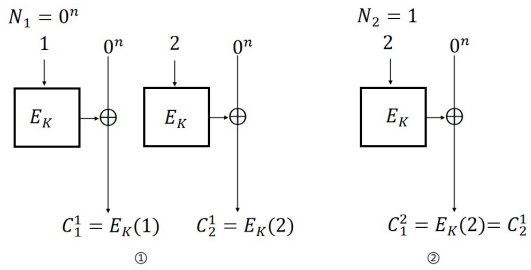


Figure 5. IND-CPA attack on CTR scheme.

1. Encryption query: Let $N_1 = P_1^1 = P_2^1 = 0$; then, $C_1^1 = E_K(1)$ and $C_2^1 = E_K(2)$.
2. Challenge query: Let $P_0 = 0^n$, $P_1 \xleftarrow{\$} \{0,1\}^n$, $P_1 \neq P_0$, and $N_2 = 1$; then, $b' = 0$ if $C_1^2 = C_1^1$, otherwise $b' = 1$.

For CTR mode, the probability of adversary $\mathcal{A}$'s success is 1. The distinguishing advantages are: $\mathrm{Adv}_{CTR}^{\text{N-IND-CPA}}(\mathcal{A}) = 1$. Therefore, $\mathrm{Adv}_{CTR}^{\text{N-IND-qCPA}}(\mathcal{A}) = 1$.

4. CBC2 Mode Is N-IND-qCPA Secure

From Section 3, we know that CBC, CFB, OFB, and CTR are IND-qCPA secure when based on IV, while they are classical insecure when based on nonce. Based on CBC, Rogaway [18] proposed an improved version of CBC2 (Figure 6) which can achieve N-IND-CPA security by adding a key.

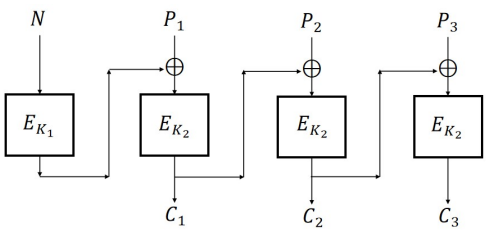


Figure 6. CBC2 scheme ($m = 3$).

Definition 12 (CBC2 Scheme [18]). *Let* $K_1, K_2 \xleftarrow{\$} \{0,1\}^k$. *For a given message* $P = P_1P_2 \cdots P_m$ *and nonce* N, *where* m *is a polynomial in* n, *the symmetric encryption scheme CBC2 is defined as follows:*

Enc: $C_0 = E_{K_1}(N)$ *and* $C_i = E_{K_2}(P_i \oplus C_{i-1})$ *for* $1 \leq i \leq m$. $Enc_{K_1,K_2}(P) = C_1 \cdots C_m$.
Dec: For a given ciphertext $C = C_1 \cdots C_m$ *and* N, $C_0 = E_{K_1}(N)$, $P_i := E_{K_2}^{-1}(C_i) \oplus C_{i-1}$ *for* $1 \leq i \leq m$. $Dec_{K_1,K_2}(C) = P_1 \cdots P_m$.

For CBC2 scheme, the following theorem holds:

Theorem 2 (Theorem 1 in [18]). *If the function* E *is a secure PRP, then CBC2 is N-IND-CPA secure.*

Next, we will demonstrate that CBC2 also satisfies N-IND-qCPA security in quantum environments:

Theorem 3. *If the function* E *is a quantum secure PRF, then CBC2 is N-IND-qCPA secure.*

From Figure 7, it can be seen that in CBC2, the nonce N is first encrypted using E_{K_1} and the output at this time is a random value, which can be essentially understood as transforming the adaptive nonce into a random IV through one encryption.

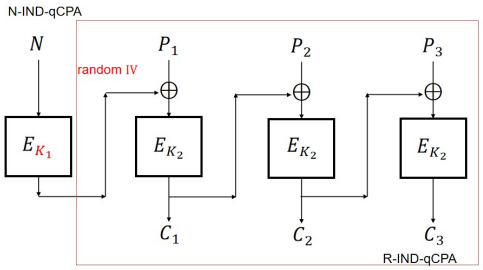


Figure 7. CBC2 scheme and CBC scheme.

The following theorem ensures the validity of Theorem 3:

Theorem 4 (From R-IND-qCPA secure to N-IND-qCPA secure.). *If the function* E *is a quantum secure PRF,* $K_1, K_2 \xleftarrow{\$} \{0,1\}^k$, *then encryption scheme* $Enc_{K_2}(IV, P)$ *is R-IND-qCPA secure with classical random* IV. *Let* $Enc'_{K_1,K_2}(N,P) = Enc_{K_2}(E_{K_1}(N), P)$; *then,* $Enc'_{K_1,K_2}(N,P)$ *is N-IND-qCPA secure with a classical adaptive nonce* N (N *cannot be repeated).*

Proof. We prove this proposition using the game-playing technique. (Table 2).

Table 2. The games G_0, G_1 and G_2.

Game G_0	Game G_1	Game G_2
Initialization	**Initialization**	**Initialization**
$K_1, K_2 \xleftarrow{\$} \{0,1\}^k$	$K_1, K_2 \xleftarrow{\$} \{0,1\}^k$	$K_2 \xleftarrow{\$} \{0,1\}^k$
On query $(N, \sum_P \psi_P \vert P\rangle)$	**On query** $(N, \sum_P \psi_P \vert P\rangle)$	**On query** $(IV, \sum_P \psi_P \vert P\rangle)$
$S_1 = E_{K_1}(N)$	$S_1 = f_{K_1}(N)$	$S_1 = IV$
$\sum_{P,S_2} \psi_{P,S_2} \vert P, S_2\rangle =$	$\sum_{P,S_2} \psi_{P,S_2} \vert P, S_2\rangle =$	$\sum_{P,S_2} \psi_{P,S_2} \vert P, S_2\rangle =$
$\sum_{P,S_2} \psi_{P,S_2} \vert P, S_2 \oplus Enc_{K_2}(S_1, P)\rangle$	$\sum_{P,S_2} \psi_{P,S_2} \vert P, S_2 \oplus Enc_{K_2}(S_1, P)\rangle$	$\sum_{P,S_2} \psi_{P,S_2} \vert P, S_2 \oplus Enc_{K_2}(S_1, P)\rangle$
return $\sum_{S_2} \psi_{S_2} \vert S_2\rangle$	return $\sum_{S_2} \psi_{S_2} \vert S_2\rangle$	return $\sum_{S_2} \psi_{S_2} \vert S_2\rangle$

G_0: The adversary is given oracle access to the quantum oracle of $Enc'_{K_1,K_2}(N,P) = Enc_{K_2}(E_{K_1}(N), P)$.

G_1: We change E to ideal random function f. Let $\mathcal{A}_1$ be adversary run to the quantum oracle of G_0 or G_1. Let $\mathcal{B}_1$ be an adversary run to the classical oracle of E or random function f. Adversary $\mathcal{B}_1$ starts by running $\mathcal{A}_1$ and simulating the games G_0 and G_1 for it. In order to simulate the calls to S_1, $\mathcal{B}_1$ uses its own oracles from the PRF game. Note that N is a classic number, and choosing a non-repeating N is easy. Then, adversary $\mathcal{B}_1$ keeps track of all the sets appearing in the games G_0 or G_1 and enforces the corresponding game rules. In the end, adversary $\mathcal{B}_1$ returns the same bit that $\mathcal{A}_1$ returns. Let $\mathcal{A}_1$ make at most q quantum queries, then let $\mathcal{B}_1$ make at most q quantum queries. It holds that

$$\mathrm{Adv}^{\mathrm{qdist}}_{G_0,G_1}(\mathcal{A}_1) \leq \mathrm{Adv}^{PRF}_{E}(\mathcal{B}_1).$$

G_2: The adversary is given oracle access to the quantum oracle of $Enc_{K_2}(IV, P)$. Let $\mathcal{A}_2$ be an adversary run to the quantum oracle of G_1 or G_2. Let $\mathcal{B}_2$ be an adversary run to the classical oracle of random function f or random IV. $\mathcal{B}_2$ uses its own oracles to simulate S_1. Then, adversary $\mathcal{B}_1$ starts by running $\mathcal{A}_1$ and simulating the games G_1 and G_2 for it. Adversary $\mathcal{B}_1$ keeps track of all the sets appearing in games G_1 or G_2 and enforces the corresponding game rules. In the end, adversary $\mathcal{B}_2$ returns the same bit that $\mathcal{A}_2$ returns. Let $\mathcal{A}_2$ make at most q quantum queries, then let $\mathcal{B}_2$ make at most q quantum queries. It holds that

$$\mathrm{Adv}^{\mathrm{qdist}}_{G_1,G_2}(\mathcal{A}_2) = 0.$$

Thus, we have

$$\mathrm{Adv}^{\mathrm{qdist}}_{G_0,G_2}(\mathcal{A}) \leq \mathrm{Adv}^{\mathrm{qdist}}_{G_0,G_1}(\mathcal{A}_1) + \mathrm{Adv}^{\mathrm{qdist}}_{G_1,G_2}(\mathcal{A}_2) \leq \mathrm{Adv}^{PRF}_{E}(\mathcal{B}_1).$$

□

5. N-IND-qCPA Secure Modification Modes

According to Theorem 4, CFB and OFB can be enhanced to N-IND-qCPA secure versions, which we denote as CFB2 and OFB2, respectively. Additionally, we define the improved CTR version, denoted as CTR2, which is N-IND-qCPA secure.

5.1. CFB2 Mode

We use different keys K_3 and K_2 to encrypt adaptive nonce N and message P, respectively. The improved version of CFB with N-IND-qCPA secure is shown in Figure 8.

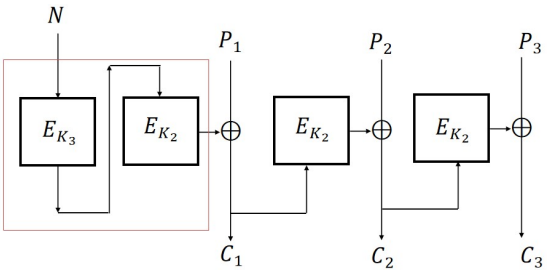


Figure 8. CFB2 scheme (standard construction with $m = 3$).

Let $E_{K_1} \overset{\mathrm{def}}{=} E_{K_2} \circ E_{K_3}$. We can obtain a simplified version of CFB2 (Figure 9) as follows:

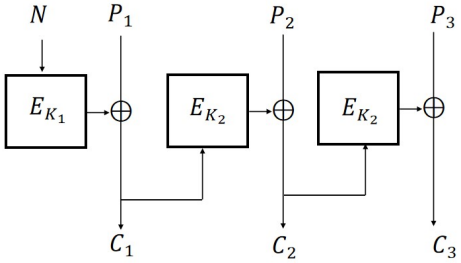


Figure 9. CFB2 scheme (simplified construction with $m = 3$).

Definition 13 (CFB2 Mode). *Let* $K_1, K_2 \xleftarrow{\$} \{0,1\}^k$. *For a given message* $P = P_1P_2 \cdots P_m$ *and nonce* N, *where* m *is a polynomial in* n, *the symmetric encryption scheme CFB2 is defined as follows:*

Enc: $C_1 = E_{K_1}(N) \oplus P_1$ *and* $C_i = E_{K_2}(C_{i-1}) \oplus P_i$ *for* $2 \leq i \leq m$. $Enc_{K_1,K_2}(P) = C_1 \cdots C_m$.
Dec: For a given ciphertext $C = C_1 \cdots C_m$, $P_i := E_{K_2}(C_{i-1}) \oplus C_i$ *for* $2 \leq i \leq m$, $P_1 = E_{K_1}(N) \oplus C_1$. $Dec_{K_1,K_2}(C) = P_1 \cdots P_m$.

Theorem 4 directly implies the following theorem.

Theorem 5. *If the function E is a quantum secure PRF, then CFB2 is N-IND-qCPA secure.*

5.2. OFB2 Mode

Similar to Section 5.1, we define the OFB2 scheme (Figure 10) as follows:

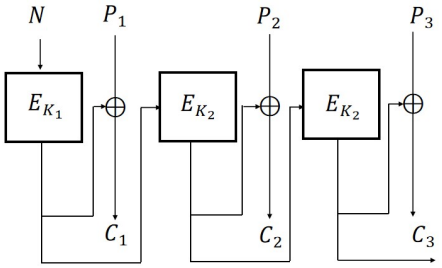


Figure 10. OFB2 scheme ($m = 3$).

Definition 14 (OFB2 Mode). *Let* $K_1, K_2 \xleftarrow{\$} \{0,1\}^k$. *For a given message* $P = P_1P_2 \cdots P_m$ *and nonce* N, *where* m *is a polynomial in* n, *the symmetric encryption scheme OFB2 is defined as follows:*

Enc: $R_0 = E_{K_1}(N)$, $R_i = E_{K_2}(R_{i-1})$ *for* $2 \leq i \leq m$. *Then* $C_i = R_{i-1} \oplus P_i$ *for* $1 \leq i \leq m$. $Enc_{K_1,K_2}(P) = C_1 \cdots C_m$.
Dec: For a given ciphertext $C = C_1 \cdots C_m$, $C_0 = E_{K_1}(N)$, $P_1 = C_0 \oplus C_1$, $P_i := E_{K_2}(C_{i-1}) \oplus C_i$ *for* $2 \leq i \leq m$. $Dec_{K_1,K_2}(C) = P_1 \cdots P_m$.

Theorem 4 directly implies the following theorem.

Theorem 6. *If the function E is a quantum secure PRF, then OFB2 is N-IND-qCPA secure.*

5.3. CTR2 Mode

Because each message block of CTR2 has nonce N as an input, directly referencing the conclusion of Theorem 4 would lead to a significant increase in the number of keys. Therefore, we consider making improvements in terms of the input. We divide the input into two parts, N and $i, i = 1, 2, 3\ldots$, and concatenate them directly. Correspondingly,

the length of the block cipher E_K used at this time is $2n$, and the lengths of P_i and C_i are also $2n$. We define the N-IND-qCPA secure CTR2 scheme (Figure 11) as follows:

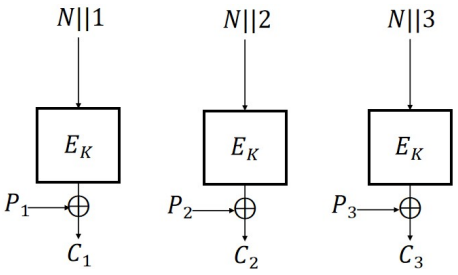


Figure 11. CTR2 scheme ($m = 3$).

Definition 15 (CTR2 Mode). *Let $K \xleftarrow{\$} \{0,1\}^k$. For a given message $P = P_1P_2 \cdots P_m$ and nonce N, where m is a polynomial in n, the symmetric encryption scheme CTR2 is defined as follows:*

Enc: $C_0 = N$ and $C_i = E_K(C_0\|i) \oplus P_i$ for $1 \le i \le m$. $Enc_K(P) = C_1 \cdots C_m$.
Dec: For a given ciphertext $C = C_1 \cdots C_m$ and $C_0 = N$, $P_i := E_K(C_0\|i) \oplus C_i$ for $1 \le i \le m$. $Dec_K(C) = P_1 \cdots P_m$.

For the CTR2 scheme, the following theorem holds:

Theorem 7. *If the function E is a secure PRF, then CTR2 is N-IND-qCPA secure.*

Proof. We prove this proposition using the game-playing technique. (Table 3).

G_0: The adversary is given oracle access to the quantum oracle of $CTR2$.

$G_i, 2 \le i \le m$: We change the ith E to ideal random function f. Let $\mathcal{A}_i$ be an adversary run to the quantum oracle of G_{i-1} or G_i. Let $\mathcal{B}_i$ be an adversary run to the classical oracle of E or random function f. Adversary $\mathcal{B}_i$ starts by running $\mathcal{A}_i$ and simulating the games G_{i-1} and G_i for it. In order to simulate the calls to S_1^i, $\mathcal{B}_i$ uses its own oracles from PRF game. Note that N is a classic number, and choosing a non-repeating N is easy. Then, adversary $\mathcal{B}_i$ keeps track of all the sets appearing in the games G_{i-1} or G_i and enforces the corresponding game rules. In the end, adversary $\mathcal{B}_i$ returns the same bit that $\mathcal{A}_i$ returns. Let $\mathcal{A}_i$ make at most q quantum queries, then let $\mathcal{B}_i$ make at most q quantum queries. It holds that

Table 3. The games $G_0, G_1, \ldots, G_m$.

Game G_0	**Game G_1**	$\cdots$	**Game G_m**
Initialization	**Initialization**	$\cdots$	**Initialization**
$K \xleftarrow{\$} \{0,1\}^k$	$K \xleftarrow{\$} \{0,1\}^k$	$\cdots$	$K \xleftarrow{\$} \{0,1\}^k$
On query $(N, \sum_P \psi_P \vert P\rangle)$	**On query** $(N, \sum_P \psi_P \vert P\rangle)$	$\cdots$	**On query** $(N, \sum_P \psi_P \vert P\rangle)$
	$S_1^1 = f_K(N\|1)$	$\cdots$	
	$\sum_{P_1,S_2^1} \psi_{P_1,S_2^1} \vert P_1, S_2^1\rangle =$		
	$\quad \sum_{P_1,S_2^1} \psi_{P_1,S_2^1} \vert P_1, S_2^1 \oplus S_1^1 \oplus P_1\rangle$		
for $1 \le i \le m$	for $2 \le i \le m$	$\cdots$	for $1 \le i \le m$
$\quad S_1^i = E_K(N\|i)$	$\quad S_1^i = E_K(N\|i)$	$\cdots$	$\quad S_1^i = f_K(N\|i)$
$\quad \sum_{P_i,S_2^i} \psi_{P_i,S_2^i} \vert P_i, S_2^i\rangle =$	$\quad \sum_{P_i,S_2^i} \psi_{P_i,S_2^i} \vert P_i, S_2^i\rangle =$		$\quad \sum_{P_i,S_2^i} \psi_{P_i,S_2^i} \vert P_i, S_2^i\rangle =$
$\quad\quad \sum_{P_i,S_2^i} \psi_{P_i,S_2^i} \vert P_i, S_2^i \oplus S_1^i \oplus P_i\rangle$	$\quad\quad \sum_{P_i,S_2^i} \psi_{P_i,S_2^i} \vert P_i, S_2^i \oplus S_1^i \oplus P_i\rangle$		$\quad\quad \sum_{P_i,S_2} \psi_{P_i,S_2} \vert P_i, S_2 \oplus S_1^i \oplus P_i\rangle$
end for	end for	$\cdots$	end for
return $\sum_{S_2^1,\ldots,S_2^m} \psi_{S_2^1,\ldots,S_2^m} \vert S_2^1, \ldots, S_2^m\rangle$	return $\sum_{S_2^1,\ldots,S_2^m} \psi_{S_2^1,\ldots,S_2^m} \vert S_2^1, \ldots, S_2^m\rangle$	$\cdots$	return $\sum_{S_2^1,\ldots,S_2^m} \psi_{S_2^1,\ldots,S_2^m} \vert S_2^1, \ldots, S_2^m\rangle$

$$\mathrm{Adv}^{\mathrm{qdist}}_{G_{i-1},G_i}(\mathcal{A}_i) \le \mathrm{Adv}^{PRF}_{E}(\mathcal{B}_i).$$

For quantum states P, game G_m returns the XOR value between a quantum message block and a classical random number. Therefore, game G_m returns a random quantum state. It holds that

$$\begin{aligned}\mathrm{Adv}^{\mathrm{qdist}}_{G_0,G_m}(\mathcal{A}_i) &\leq \mathrm{Adv}^{\mathrm{qdist}}_{G_0,G_1}(\mathcal{A}_i) + \mathrm{Adv}^{\mathrm{qdist}}_{G_1,G_2}(\mathcal{A}_i) + \cdots + \mathrm{Adv}^{\mathrm{qdist}}_{G_{m-1},G_m}(\mathcal{A}_i) \\ &\leq \sum_{1\leq i\leq m} \mathrm{Adv}^{PRF}_{E}(\mathcal{B}_i).\end{aligned}$$

□

We note that CTR2 is a stream cipher, and the conclusion and proof of Theorem 7 can be correspondingly extended to stream ciphers.

Theorem 8. *[Nonce-based stream cipher encryption is N-IND-qCPA] Let G be a secure nonce-based stream cipher, $Enc_K(N,P) = G_K(N) \oplus P$; then, $Enc_K(N,P)$ is N-IND-qCPA secure.*

Proof. The proof of this theorem is similar to Theorem 7. We prove this proposition using the game-playing technique. (Table 4).

Table 4. The games G_0, G_1 and G_2.

Game G_0	**Game G_1**	**Game G_2**
Initialization	**Initialization**	**Initialization**
$K \xleftarrow{\$} \{0,1\}^k$	$K \xleftarrow{\$} \{0,1\}^k$	$K \xleftarrow{\$} \{0,1\}^k$
On query $(N, \sum_P \psi_P \vert P\rangle)$	**On query** $(N, \sum_P \psi_P \vert P\rangle)$	**On query** $(N, \sum_P \psi_P \vert P\rangle)$
$S_1 = G_K(N)$	$S_1 = f_K(N)$	$S_1 \xleftarrow{\$} \{0,1\}^{\vert G_K(N)\vert}$
$\sum_{P,S_2} \psi_{P,S_2} \vert P, S_2\rangle =$ $\sum_{P,S_2} \psi_{P,S_2} \vert P, S_2 \oplus S_1 \oplus P\rangle$	$\sum_{P,S_2} \psi_{P,S_2} \vert P, S_2\rangle =$ $\sum_{P,S_2} \psi_{P,S_2} \vert P, S_2 \oplus S_1 \oplus P\rangle$	$\sum_{P,S_2} \psi_{P,S_2} \vert P, S_2\rangle =$ $\sum_{P,S_2} \psi_{P,S_2} \vert P, S_2 \oplus S_1 \oplus P\rangle$
return $\sum_{S_2} \psi_{S_2} \vert S_2\rangle$	return $\sum_{S_2} \psi_{S_2} \vert S_2\rangle$	return $\sum_{S_2} \psi_{S_2} \vert S_2\rangle$

G_0: The adversary is given oracle access to the quantum oracle of $Enc_K(N,P)$.

G_1: We change G to an ideal random function f. Let $\mathcal{A}_1$ be an adversary run to the quantum oracle of G_0 or G_1. Let $\mathcal{B}_1$ be an adversary run to the classical oracle of G or random function f. Similar to the previous proof, we have

$$\mathrm{Adv}^{\mathrm{qdist}}_{G_0,G_1}(\mathcal{A}_1) \leq \mathrm{Adv}^{PRF}_{G}(\mathcal{B}_1).$$

G_2: We change random function f to random $S_1 \xleftarrow{\$} \{0,1\}^{|G_K(N)|}$. Let $\mathcal{A}_2$ be an adversary run to the quantum oracle of G_1 or G_2, and let

$$\mathrm{Adv}^{\mathrm{qdist}}_{G_1,G_2}(\mathcal{A}_2) = 0.$$

Thus, we have

$$\mathrm{Adv}^{\mathrm{qdist}}_{G_0,G_2}(\mathcal{A}) \leq \mathrm{Adv}^{\mathrm{qdist}}_{G_0,G_1}(\mathcal{A}_1) + \mathrm{Adv}^{\mathrm{qdist}}_{G_1,G_2}(\mathcal{A}_2) \leq \mathrm{Adv}^{PRF}_{G}(\mathcal{B}_1).$$

For quantum states P, game G_2 returns the XOR value between a quantum message block and a classical random number. Therefore, game G_2 returns a random quantum state, and $Enc_K(N,P)$ is N-IND-qCPA secure. □

Note that if OFB2 is also a stream cipher, the N-IND-qCPA security of $OFB2$ (Theorem 6) can also be directly derived from Theorem 8.

6. Conclusions

The first contribution of this paper is a general conversion method from R-IND-qCPA to N-IND-qCPA security (Theorem 4). Specifically, if an encryption scheme $Enc_{K_2}(IV, P)$ is R-IND-qCPA secure with random IV, then the construction $Enc_{K_2}(E_{K_1}(N), P)$ achieves N-IND-qCPA security with adaptive but non-repeating nonce N. Conceptually, this transformation encrypts the adaptive nonce once, thereby turning it into a random IV. As a direct application, CBC2 is proven N-IND-qCPA secure. We note, however, that this method generally incurs one additional encryption operation.

In contrast, for CFB and OFB, the situation is more favorable; since these schemes already involve encrypting the IV once, the additional operation can be merged. Thus, the modified variants CFB2 and OFB2 achieve N-IND-qCPA security without extra computational overhead, requiring only distinct keys for the initial block and the subsequent blocks.

Our final result establishes that nonce-based stream ciphers are inherently N-IND-qCPA secure (Theorem 8). If G is a secure nonce-based stream cipher, then $G_K(N) \oplus P$ satisfies N-IND-qCPA security. This can be understood as XORing quantum plaintext states with classical randomness. As a corollary, we derive the N-IND-qCPA secure version CTR2.

When compared to random IVs, nonces that are selectable yet non-repeating offer better alignment with practical deployment requirements. Future research should focus on extending these techniques to further enhance the N-IND-qCPA security of other IV-based encryption schemes. Meanwhile, integrating confidentiality with integrity to develop quantum-secure authenticated encryption schemes represents another important direction for future research.

Author Contributions: Conceptualization, P.W.; methodology, S.M.; writing—original draft, S.M.; writing—review and editing, P.W., Y.J. and G.L.; visualization, S.M. and B.L.; supervision, G.L. and B.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by National Key Laboratory of Security Communication Foundation (2024, 6142103042409) and the Fundamental Research Funds for the Central Universities (Grant Number: 3282025001).

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

IND-CPA	Indistinguishability under Chosen-Plaintext Attack
IND-qCPA	Indistinguishability under quantum Chosen-Plaintext Attack
IV	Initialization Vector
N	Nonce
R-IND-CPA	Indistinguishability under Chosen-Plaintext Attack in the random-IV setting
N-IND-CPA	Indistinguishability under Chosen-Plaintext Attack in the nonce setting
R-IND-qCPA	Indistinguishability under quantum Chosen-Plaintext Attack in the random-IV setting
N-IND-qCPA	Indistinguishability under quantum Chosen-Plaintext Attack in the nonce setting
CBC	Cipher Block Chaining
CFB	Cipher FeedBack Mode
OFB	Output FeedBack Mode
CTR	CounTeR Mode

References

1. Grover, L.K. A Fast Quantum Mechanical Algorithm for Database Search. In Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing, Philadelphia, PA, USA, 22–24 May 1996; pp. 212–219.
2. Simon, D.R. On the Power of Quantum Computation. *SIAM J. Comput.* **1997**, *26*, 1474–1483. [CrossRef]
3. Kuwakado, H.; Morii, M. Quantum distinguisher between the 3-round Feistel cipher and the random permutation. In Proceedings of the IEEE International Symposium on Information Theory, ISIT, Austin, TX, USA, 12–18 June 2010; pp. 2682–2685.
4. Mao, S.; Guo, T.; Wang, P.; Hu, L. Quantum Attacks on Lai-Massey Structure. In Proceedings of the Post-Quantum Cryptography, PQCrypto 2022, Virtual, 28–30 September 2022; Volume 13512, pp. 205–229.
5. Ito, G.; Hosoyamada, A.; Matsumoto, R.; Sasaki, Y.; Iwata, T. Quantum Chosen-Ciphertext Attacks Against Feistel Ciphers. In Proceedings of the Topics in Cryptology—CT-RSA 2019—The Cryptographers' Track at the RSA Conference 2019, San Francisco, CA, USA, 4–8 March 2019; Volume 11405, pp. 391–411.
6. Luo, Y.; Yan, H.; Wang, L.; Hu, H.; Lai, X. Study on block cipher structures against simon's quantum algorithm. *J. Cryptologic Res.* **2019**, *6*, 561–573. (In Chinese)
7. Kaplan, M.; Leurent, G.; Leverrier, A.; Naya-Plasencia, M. Breaking Symmetric Cryptosystems Using Quantum Period Finding. In Proceedings of the Advances in Cryptology—CRYPTO 2016, Santa Barbara, CA, USA, 14–18 August 2016; Volume 9815, pp. 207–237.
8. Bhaumik, R.; Bonnetain, X.; Chailloux, A.; Leurent, G.; Naya-Plasencia, M.; Schrottenloher, A.; Seurin, Y. QCB: Efficient Quantum-Secure Authenticated Encryption. In Proceedings of the Advances in Cryptology—ASIACRYPT 2021, Singapore, 6–10 December 2021; pp. 668–698.
9. Bonnetain, X.; Leurent, G.; Naya-Plasencia, M.; Schrottenloher, A. Quantum Linearization Attacks. In *Proceedings of the Advances in Cryptology—ASIACRYPT 2021—27th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, 6–10 December 2021, Proceedings, Part I*; Tibouchi, M., Wang, H., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2021; Volume 13090, pp. 422–452. [CrossRef]
10. Maram, V.; Masny, D.; Patranabis, S.; Raghuraman, S. On the Quantum Security of OCB. *IACR Trans. Symmetric Cryptol.* **2022**, *2022*, 379–414. [CrossRef]
11. Boneh, D.; Zhandry, M. Secure Signatures and Chosen Ciphertext Security in a Quantum Computing World. In Proceedings of the Advances in Cryptology—CRYPTO 2013, Santa Barbara, CA, USA, 18–22 August 2013; Volume 8043, pp. 361–379.
12. 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 Proceedings of the Post-Quantum Cryptography, PQCrypto 2016, Fukuoka, Japan, 24–26 February 2016; Volume 9606, pp. 44–63.
13. Lang, N.; Leuther, J.; Lucks, S. Generic Composition: From Classical to Quantum Security. Cryptology ePrint Archive, Paper 2025/387, 2025. Available online: https://eprint.iacr.org/2025/387 (accessed on 3 October 2025).
14. Bootsma, S.E.; De Vries, M. A Survey on the Quantum Security of Block Cipher-Based Cryptography. *IEEE Access* **2024**, *12*, 194711–194727. [CrossRef]
15. Mao, S.; Guo, T.; Wang, P.; Xu, R.; Chen, Y.; Hu, L. A quantum-secure partial parallel MAC QPCBC. *Des. Codes Cryptogr.* **2024**, *92*, 4453–4486. [CrossRef]
16. Adomnicai, A.; Minematsu, K.; Shikata, J. Lightweight Yet Nonce-Misuse Secure Authenticated Encryption for Very Short Inputs. *IEEE Internet Things J.* **2025**, *12*, 2807–2824. [CrossRef]
17. Chethana, R.V.; Vrindavanam, J.; Roy, S.; Deshmukh, P.C. A Review of Block Ciphers and Its Post-Quantum Considerations. *IEEE Access* **2025**, *13*, 57834–57846. [CrossRef]
18. Rogaway, P. Nonce-Based Symmetric Encryption. In Proceedings of the Fast Software Encryption, FSE 2004, Graz, Austria, 14–16 February 2004; Volume 3017, pp. 348–359.