IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 8 November 2024, accepted 7 December 2024, date of publication 19 December 2024, date of current version 30 December 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3520364

SURVEY

A Survey on the Quantum Security of Block Cipher-Based Cryptography

S. E. BOOTSMA AND M. DE VRIES
TNO, Applied Cryptography and Quantum Algorithms, 2595 DA The Hague, The Netherlands
Corresponding author: M. De Vries (manon.devries@tno.nl)

This work was supported in part by the Ministry of Defence Netherlands under the V21.04 Project, and in part by the Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek (TNO) Early Research Program "Next Generation Cryptography."

ABSTRACT The development of quantum computers represents an important advancement in computing, using quantum mechanics to address problems that were previously difficult to solve. This technological advancement poses a challenge for cryptographic systems. While some methods are known to be vulnerable, the impact of quantum computing on symmetric cryptography has received less research attention, largely because the common advice is to simply double the key size. This paper explores how quantum computing affects symmetric cryptography, focusing on block cipher-based cryptography. It surveys existing literature on the quantum resilience of symmetric cryptographic primitives based on block ciphers and their security in various scenarios. Not all symmetric cryptographic functionalities are quantum-secure, and their security depends on the specific *adversary model* being considered. We provide an overview of the research conducted and pinpoint areas where further investigation is needed.

INDEX TERMS Symmetric cryptography, block ciphers, modes of operation, quantum security, quantum computing, survey of knowledge.

I. INTRODUCTION

Among the cryptographic methods we rely on today, it is the asymmetric algorithms that are the most vulnerable to the attacks enabled by a *cryptographically relevant quantum computer*. Cryptographic research has therefore mostly been on the replacement of asymmetric primitives and their embedding in existing protocols. However, symmetric cryptography, including block ciphers, stream ciphers and hashing, does not emerge unscathed either. Some, like the Even-Mansour cipher [1], can be broken in a quantum setting, although the impact of quantum computing on symmetric cryptography is generally less severe. This paper provides a detailed survey of the impact of quantum computing on symmetric cryptography, with a specific focus on block cipher-based cryptography.

Our contribution:

- We summarize the most common formal security notions found in the literature for proving the quantum security of modes of operation: IND-1CPA, PO1, IND-qCPA, and EUF-qCMA (also referred to as qPO).
- We explain the two main adversary models used in quantum attacks on symmetric cryptography: Q1 (quantum computer access) and Q2 (quantum computer access with superposition query capabilities), and discuss their relevance.
- We survey relevant quantum algorithms for attacking block ciphers and their modes of operation: Simon's, Kuperberg's, Grover's, Deutsch-Jozsa's, Bernstein-Vazirani's and Shor's algorithm.
- We provide an overview of block ciphers and various construction methods that are not quantum-secure, including Even-Mansour, the FX-construction, PRINCE, AEZv5, COPA, and CLOC.
- We review the formal quantum security of encryption modes (ECB, CBC, CFB, XTS, OFB, CTR), authentication modes (CBC-MAC, CMAC), authenticated encryption modes (OCB, CCM, GCM, CWC, EAX, SIV, (AES-)OTR) and KDF modes (assuming the underlying block cipher is a *(quantum) pseudorandom function*).

The associate editor coordinating the review of this manuscript and approving it for publication was Shuangqing Wei.

- We examine the quantum security of AES and the formal security of its associated modes of operation.
- Lastly we make some observations, address unanswered questions and suggest areas for further research.

A. STRUCTURE AND SCOPE

The structure of this paper is as follows. Section II introduces quantum computation, formal security notions, adversary models, attack complexity, and explores quantum algorithms and their implications for symmetric cryptography. In Section III, we discuss the relevance of two specific adversary models, Q1 and Q2. Section IV reviews the security of block cipher primitives, identifies broken block ciphers, and discusses various attacks. In Section V different modes of operation are covered, including encryption modes, authentication modes, authenticated encryption modes and key derivation modes. Section VI offers a detailed review of AES, comparing its classical and quantum security, evaluating its security margins, and examining the security of its modes of operation. We conclude by discussing some observations, addressing unanswered questions, and suggesting areas for further research.

Summary of Findings: The security of an encryption scheme depends on both the security of its block cipher primitive and its mode of operation. This survey reveals that while few block ciphers are *currently* broken in a quantum context, many modes of operation either lack formal quantum security guarantees or are known to be insecure. If the underlying block cipher is a quantum pseudorandom function, only the encryption modes CBC, CFB, XTS, OFB, and CTR are IND-qCPA secure. Among these, only OFB and CTR are IND-qCPA secure when the block cipher is a classical pseudorandom function. None of the authentication modes of operation considered are formally secure in the Q2 model, regardless of the block cipher's quantum security.

While some classical security notions like IND-CPA (see Section II-B) have been successfully adapted to the quantum realm for encryption (IND-qCPA), defining quantum counterparts for authentication is still an ongoing process, leading to varied outcomes for authentication and authenticated encryption modes. Many known efficient attacks on block cipher constructions and modes of operation appear in the Q2 model. However, some attacks have been adapted to the Q1 model, albeit with reduced efficiency (e.g. the *offline Simon attack*). The AES block cipher appears resilient against these attacks, which is promising; however, the underlying reasons for this resilience remain unclear.

Research in this area has mostly occurred over the past five years, gaining increasing recognition, highlighting its ongoing importance. The focus has been primarily on widely adopted primitives involved in competitions such as Lightweight and CAESAR, as well as well-known modes of operation. However, there has been limited exploration of older or lesser-known primitives and their applications. Moreover, many modes and primitives are assumed to be secure in the Q1 model due to the absence of attacks, without formal proof of their security. This poses challenges, particularly for components expected to play critical roles in future quantum-safe protocols, such as block cipher modes of operation and key derivation functions (KDFs) used in hybrid protocols.

II. PRELIMINARIES

A. QUANTUM COMPUTATION

We provide a brief overview of quantum computation, originating from [2]. A quantum system is a complex Hilbert space $\mathcal{H}$ together with an inner product $\langle\cdot|\cdot\rangle$. The state of a quantum system is given by a vector $|\psi\rangle$, where $\langle\psi|\psi\rangle = 1$. For quantum systems $\mathcal{H}_1$ and $\mathcal{H}_2$, their joint quantum system is given by the tensor product $\mathcal{H}_1 \otimes \mathcal{H}_2$. Given $|\psi_1\rangle \in \mathcal{H}_1$ and $|\psi_2\rangle \in \mathcal{H}_2$, the product state is represented by $|\psi_1\rangle|\psi_2\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2$.

Consider a quantum state $|\psi\rangle$ and an orthonormal basis $\mathcal{B} = \{|b_0\rangle, \ldots, |b_{d-1}\rangle\}$ for $\mathcal{H}$, a measurement of $|\psi\rangle$ in basis $\mathcal{B}$ yields the value i with probability $|\langle b_i|\psi\rangle|^2$, after which the quantum state collapses to the basis vector $|b_i\rangle$. If $|\psi\rangle$ is part of a joint system $\mathcal{H} \otimes \mathcal{H}'$, then it can be expressed as

$$|\psi\rangle = \sum_{i=0}^{d-1} \alpha_i |b_i\rangle|\psi_i'\rangle$$

for some complex coefficients α_i and states $|\psi_i'\rangle$ over $\mathcal{H}'$. In this case, a measurement on $\mathcal{H}$ yields the outcome i with probability $|\alpha_i|^2$, and the resulting quantum state becomes $|b_i\rangle|\psi_i'\rangle$.

A unitary transformation over a d-dimensional Hilbert space $\mathcal{H}$ is a $d \times d$ matrix $\mathbf{U}$ such that $\mathbf{U}\mathbf{U}^\dagger = \mathbf{I}_d$, where $\mathbf{U}^\dagger$ denotes the conjugate transpose. A quantum algorithm operates on a product space $\mathcal{H}_{\text{in}} \otimes \mathcal{H}_{\text{out}} \otimes \mathcal{H}_{\text{work}}$ and consists of n unitary transformations $\mathbf{U}_1, \ldots, \mathbf{U}_n$ within this space. Here, $\mathcal{H}_{\text{in}}$ denotes the input space, $\mathcal{H}_{\text{out}}$ the output space, and $\mathcal{H}_{\text{work}}$ the workspace. A classical input x to the quantum algorithm is transformed into the quantum state $|x, 0, 0\rangle$. The unitary transformations are applied sequentially, producing the final state

$$|\psi_x\rangle = \mathbf{U}_n \ldots \mathbf{U}_1 |x, 0, 0\rangle.$$

Upon measurement, the state $|\psi_x\rangle$ collapses to the tuple (a, b, c) with probability $|\langle a, b, c|\psi_x\rangle|^2$, and the algorithm's output is b.

Definition 1 (Quantum-Accessible Oracle): An oracle $O : X \to Y$ is implemented by a unitary transformation $\mathbf{O}$ where

$$\mathbf{O}|x, y, z\rangle := |x, y + O(x), z\rangle$$

and $+ : X \times X \to X$ is a group operation defined on X.

B. FORMAL SECURITY NOTIONS

In cryptography, the security of schemes is proven formally. Understanding these formalities is necessary in order to give a comprehensive overview of the literature. We start with some definitions.

Definition 2 (Symmetric Encryption Scheme): A symmetric encryption scheme is defined as a triple

$$\Pi = (\text{Key}, \text{Enc}, \text{Dec}),$$

where:

- Key *is the key generation algorithm, which takes as input* 1^n *(the security parameter in unary) and outputs a key* k.
- Enc *is the encryption algorithm, which takes as input a key* k *and a plaintext* $m \in \{0,1\}^*$*, and outputs ciphertext* c.
- Dec *is the decryption algorithm, which takes as input a key* k *and ciphertext* c*, and outputs a message* m *or an error.*

Definition 3 (Symmetric Authentication Scheme): A symmetric authentication scheme (or MAC scheme) is defined as a triple

$$\Sigma = (\text{Key}, \text{Sign}, \text{Verify}),$$

where:

- Key *is the key generation algorithm, which takes as input* 1^λ *(the security parameter in unary) and outputs a key* k.
- Sign *is the signing algorithm, which takes as input the key* k *and a message* $m \in \{0,1\}^*$*, and outputs a tag* σ.
- Verify *is the verification algorithm, which takes as input the key* k*, a message* m*, and a tag* σ*, and outputs either* `accept` *(if the tag is valid) or* `reject` *(if the tag is invalid).*

Security games are used to prove or disprove the security of these schemes. One of these games is the IND-CPA security game [3]. In this game we give the adversary $\mathcal{A}$ access to an *encryption oracle*, that encrypts messages of $\mathcal{A}$'s choice using a key k unknown to $\mathcal{A}$. The adversary is allowed to interact with the oracle adaptively, as many times as it likes.

Consider now the following experiment called $\text{SymK}^{\text{CPA}}_{\mathcal{A},\Pi}(n)$:

Definition 4 (The IND-CPA experiment $SymK^{CPA}_{\mathcal{A},\Pi}(n)$*): Let* Π *be an encryption scheme,* $\mathcal{A}$ *the adversary and* n *the security parameter. The experiment* $SymK^{CPA}_{\mathcal{A},\Pi}(n)$ *is defined by the following process*:

1) *A key* k *is generated by running* $\text{Key}(1^n)$.
2) *The adversary* $\mathcal{A}$ *is given input* 1^n *and oracle access to* $\text{Enc}_k(\cdot)$*, and outputs a pair of messages* m_0, m_1 *of the same length.*
3) *A bit* $b \in \{0,1\}$ *is chosen uniformly at random, and then a ciphertext* $c \leftarrow \text{Enc}_k(m_b)$ *is computed and given to* $\mathcal{A}$.
4) *The adversary* $\mathcal{A}$ *continues to have oracle access to* $\text{Enc}_k(\cdot)$*, and outputs a bit* b'.
5) *The output of the experiment is defined to be 1 if* $b' = b$*, and 0 otherwise. In the former case, we say that* A ***succeeds***.

This leads to the next definition.

Definition 5 (IND-CPA security): A symmetric-key encryption scheme $\Pi = (\text{Key}, \text{Enc}, \text{Dec})$ *is IND-CPA secure, if for all probabilistic polynomial-time adversaries* $\mathcal{A}$*, there is a negligible function* negl *such that*

$$\mathbb{P}\left[SymK^{CPA}_{A,\Pi}(n) = 1\right] \leq \frac{1}{2} + \text{negl}(n),$$

where the probability is taken over the randomness used by $\mathcal{A}$*, as well as the randomness used in the experiment.*

Intuitively, IND-CPA security implies that the adversary cannot guess which message was encrypted with a probability higher than 1/2.

IND-CPA is among several classical security definitions, including IND-CCA and EUF-CMA (for authentication schemes). Translating these definitions to the quantum setting is nontrivial, and ongoing research aims to ensure their correct adaptation (cf. Remark 1). Our focus is on the most common quantum notions: IND-1CPA and IND-qCPA for encryption, and PO1 and EUF-qCMA for authentication. We provide brief descriptions for each. For a comprehensive overview, refer to [4], [5], [6], and [7].

- **IND-1CPA:** IND-CPA where the adversary $\mathcal{A}$ has access to a quantum computer.
- **IND-qCPA:** An extension of IND-1CPA where the adversary can send queries to the encryption oracle in superposition and receive a superposition of ciphertexts in return. See Definition 7 for a formal definition.
- **PO1:** Here the adversary has oracle access to the signing algorithm of the authentication part of the scheme and a quantum computer, but queries are classical. An authentication scheme is PO1 secure if after q queries to the oracle the adversary cannot produce $q+1$ valid message-tag pairs (see [5]).
- **EUF-qCMA (also referred to as qPO):** These terms are used interchangeably in the literature, but we use EUF-qCMA exclusively. This notion extends PO1 by allowing the adversary to make superposition queries to the oracle, representing the quantum analogue of classical existential forgery (cf. Definition 8).

Remark 1: We focus only on IND-CPA security in the quantum setting due to the unresolved inconsistencies in defining correct IND-CCA security in this context. Translating classical IND-CCA security to the quantum setting is challenging because handling decryption queries after quantum challenge queries is problematic. Storing quantum ciphertexts is non-trivial due to quantum properties like no-cloning and destructive measurements, leaving this issue unresolved [4].

For completeness we state here the formal definition of IND-qCPA ([2, Def. 4.5]) and EUF-qCMA ([8, Section 2.2]) security.

Definition 6 (Quantum Encryption Oracle): Let Π *be an encryption scheme. We define the quantum encryption oracle (cf. Definition 1)* U_{Enc_k} *associated with* Π *and initialized with key* k *as a family of unitary operators defined by*:

$$\mathbf{U}_{\text{Enc}_\mathbf{k}} : \sum_{x,y,z} \alpha_{x,y,z}|x,y,z\rangle \rightarrow \sum_{x,y,z} \alpha_{x,y,z}|x, y \oplus \text{Enc}_k(x;r), z\rangle,$$

where the same randomness[1] *r is used in superposition in all the executions of* $\mathrm{Enc}_k(x)$ *within one query. For each new query, a fresh independent r is used.*

Definition 7 (IND-qCPA Security): A symmetric key encryption scheme Π is indistinguishable under a quantum chosen message attack (IND-qCPA secure) if no efficient adversary $\mathcal{A}$ can win in the following game, except with probability at most $\frac{1}{2} + \mathsf{negl}(n)$:

1) *A key k is generated by running* $\mathrm{Key}(1^n)$ *and a bit $b \in \{0, 1\}$ is chosen uniformly at random.*
2) *The adversary $\mathcal{A}$ is allowed to make two types of oracle queries:*
   a) ***Challenge Queries:*** *$\mathcal{A}$ sends two messages m_0, m_1, to which the oracle responds with $c = \mathrm{Enc}_k(m_b)$.*
   b) ***Encryption Queries:*** *For each such query, the oracle chooses randomness r and encrypts each message in the superposition using r as randomness*:

$$\sum_{m,c,z} \psi_{m,c,z} |m, c, z\rangle \longrightarrow \sum_{m,c,z} \psi_{m,c,z} |m, c \oplus \mathrm{Enc}_k(m; r), z\rangle.$$

3) *The adversary $\mathcal{A}$ produces a bit b', and wins if $b = b'$.*

Definition 8 Existentially Unforgeable Under Quantum Chosen Message Attack (EUF-qCMA): Quantum chosen message queries allow the adversary to maintain its own quantum state and issue quantum queries to the signing oracle. Let $\sum_{m,x,y} \psi_{m,x,y} |m, x, y\rangle$ be the adversary's state just prior to issuing a signing query. The MAC signing oracle transforms this state as follows:

1) It chooses a random string r to be used by the MAC signing algorithm.
2) It signs each "slot" in the given superposition by running $\mathrm{Sign}_k(m; r)$, where Sign is the signing algorithm with randomness r. More precisely, the signing oracle performs the following transformation:

$$\sum_{m,x,y} \psi_{m,x,y} |m, x, y\rangle \rightarrow \sum_{m,x,y} \psi_{m,x,y} |m, x \oplus \mathrm{Sign}_k(m; r), y\rangle.$$

After issuing q quantum chosen message queries, the adversary wins the game if it can generate $q + 1$ valid classical message-tag pairs.

C. ADVERSARY MODELS

There have been many quantum attacks published on cryptographic algorithms, including symmetric algorithms. Before outlining the attacks, it is important to distinguish the different adversary models. Most literature uses the Q1 and Q2 terminology, which we extend to include Q0 (*the classical model*) and the *related-key attack* model.

- **Q0:** The classical attack model. The adversary uses classical devices and can make classical encryption or decryption queries to its oracles. The adversary does not have access to a quantum computer. Security notions like IND-CPA, IND-CCA and EUF-CMA belong[2] in this category.
- **Q1:** The adversary possesses a quantum computer in addition to classical resources (Q0). The adversary has access to a quantum computer, but is limited to making classical encryption or decryption queries to an oracle [9]. This corresponds to a classical chosen-plaintext or chosen-ciphertext attack, with the addition of quantum computing power. Security notions that belong here are for example PO1 and IND-1CPA.
- **Q2:** The adversary possesses Q1 resources *and* has the capability to perform superposition encryption or decryption queries to its oracles, of which the adversary obtains a superposition of outputs. This is a strong, yet simple model and its relevance will be discussed in Section III. Security notions that fall inside this category include IND-qCPA and EUF-qCMA (cf. Definition 7 and Definition 8).
- **(Quantum) related-key attack model:** A particularly strong additional model is the *related-key attack* model, which has both a classical and a quantum version. In the classical variant we allow the adversary to perform so-called related-key attacks. Related-key attacks become feasible when there exists a connection between different keys, meaning that they are not independently or randomly chosen, and this relationship is either known to the adversary, or can be manipulated by it [10]. In such attacks, the adversary observes encryptions performed with various keys and exploits these relationships to recover (a part of) a key. It is important to note that if a related-key attack is possible, it represents a threat in both classical and quantum contexts. However, they rely on the assumption that keys exhibit some form of interrelation, which is typically not the case in many practical applications, although such cases do exist.[3]
  The quantum related-key attack model is an extension of the Q2 model. It has Q2 capabilities, and the adversary is allowed to query both the quantum encryption and decryption oracles with superpositions of keys. Quantum related-key attacks are incredibly strong, but unlikely to be feasible for a typical implementation. Rötteler and Steinwandt demonstrated that, under certain assumptions, the key of any block cipher can be efficiently recovered in polynomial time if a quantum related-key attack is possible [12].

[1] To ensure non-deterministic encryption.

[2] Security notions are modelled in an adversary model.

[3] A notable exception illustrating this attack occurred with WEP (Wi-Fi encryption), which used the RC4 cipher. The key consisted of a variable 24-bit Initialization Vector (IV) combined with a frequently unchanging WEP key [11].

The relevance of the adversary models above will be discussed in Section III. For reference we state the definition of a (quantum) pseudorandom function (see [13] and [14]).

Definition 9 (Pseudorandom function): A family of functions $F_s : \{0,1\}^k \to \{0,1\}^\ell$, indexed by a key $s \in \{0,1\}^n$, is said to be pseudorandom if it satisfies the following two properties:

- ***Efficient to evaluate:*** *The value $F_s(x)$ is efficiently computable given s and x.*
- ***Pseudorandomness:*** *The function F_s cannot be efficiently distinguished from a uniformly random function $R : \{0,1\}^k \to \{0,1\}^\ell$, given access to pairs $(x_i, F_s(x_i))$, where the x_i's can be adaptively chosen by the Q0 adversary.*

More informally, a function f is called a pseudorandom function (PRF) if it can generate output from a random seed[4] and a data variable, such that the output is computationally indistinguishable from truly random output.

Definition 10 (Quantum pseudorandom function): A family of functions $F_s : \{0,1\}^k \to \{0,1\}^\ell$, indexed by a key $s \in \{0,1\}^n$, is called a quantum pseudorandom function (qPRF) if it satisfies the following properties:

- ***Efficient to evaluate:*** *The value $F_s(x)$ is efficiently computable given s and x.*
- ***Quantum pseudorandomness:*** *The function F_s cannot be efficiently distinguished from a uniformly random function $R : \{0,1\}^k \to \{0,1\}^\ell$, even by an adversary in the Q2 model.*

More informally, a function f is called a quantum pseudorandom function (qPRF) if it can generate output from a random seed and a data variable, such that the output is computationally indistinguishable from truly random output, even by an adversary with quantum superposition capabilities.

D. ATTACK COMPLEXITY

Classical attack complexity is consistently presented by specifying computational workload, memory demands, and the number of oracle queries or plaintext-ciphertext pairs required. This allows for meaningful comparisons between different attack methods. Quantum complexity, outlined below, differs slightly [15].

- **Quantum time complexity:** Represents the number of elementary quantum gates applied to a qubit or qubit register. This is important because the gates used in a quantum computer are typically not physical components; instead, they are processes of manipulation, often implemented using lasers.
- **Quantum query complexity:** many quantum algorithm complexity bounds and algorithms in literature rely heavily on query complexity, assessing the number of times an oracle is invoked. Calls in superposition to an oracle imply a Q2 adversary model.
- **Quantum memory complexity:** denotes the quantity of qubits within the circuit, allowing for more parallel operations and reducing time complexity.

Insight 1 (Quantum Random Access Memory (QRAM)): QRAM is a specialized form of quantum memory, which stands out for its ability to access data (quantum or classical) based on memory addresses which are in a quantum state themselves [16]. This unique feature offers potential advantages, facilitating the acceleration of specific algorithms [17] (and potentially, attacks [18]). Some of the research discussed here assumes the existence of QRAM. However, practical implementation of QRAM has numerous challenges, including significant gate overhead in hardware realization [16]. The debate over the future viability of QRAM remains ongoing. While acknowledging its importance in certain attacks and algorithms, we opted to focus primarily on evaluating the time complexity of these attacks.

E. QUANTUM ALGORITHMS AND SYMMETRIC CRYPTOGRAPHY

In this section we discuss quantum algorithms that are relevant in symmetric cryptography. We outline the algorithms, their complexity and their usage in attacks.

1) GROVER'S ALGORITHM AND ITS GENERALIZATIONS

Grover's algorithm [19] presents a quadratic speed-up for the unstructured search problem compared to classical methods. While classical approaches require on average $N/2$ queries to find a marked item in an unsorted database of N items, Grover's algorithm achieves this with a time complexity of $\mathcal{O}(N^{1/2})$. The algorithm is asymptotically optimal, meaning that for large inputs, it performs slightly worse (by a constant factor) than the best possible algorithm for the problem.

Example 1 (Ideal Cipher): When E is an ideal cipher, the best attack is brute force search for the key. If n is the bit length of the key, classical complexity for brute force is $\mathcal{O}(2^n)$, while Grover's algorithm reduces quantum complexity to $\mathcal{O}(2^{n/2})$.

One should remark that there are several generalizations of Grover's algorithm. For example there is a version that searches for elements in databases with repeated elements [19] and a version called *quantum partial search* [20], where one is only interested in the first few bits of an address.

2) COLLISION FINDING ALGORITHMS

Collision finding algorithms can be used to attack hash functions and block ciphers. Let H be a hash function and denote the size of the digest by n. The classical time complexity for finding collisions with a brute force attack is $\mathcal{O}(2^{n/2})$ due to the birthday attack [21, section 11]. In the Q1 model, it can be accomplished with a slight increase in speed. In [15] a new quantum collision finding algorithm is presented with a time complexity of $\tilde{\mathcal{O}}(2^{2n/5})$ (equal to the query complexity) and quantum memory of $\mathcal{O}(n)$. This is a significant improvement regarding the quantum memory of the algorithm presented

[4]For a block cipher, the random seed is the key.

in [22]. The algorithm presented there has time complexity $\tilde{\mathcal{O}}(2^{n/3})$, but requires $\tilde{\mathcal{O}}(2^{n/3})$ quantum memory.

The algorithms discussed above primarily address single-target preimage search for hash functions. However, there is also interest in finding at least one preimage for a set of hash values, known as multi-target preimage search: given access to a random permutation $H : \{0,1\}^n \to \{0,1\}^n$ and a set $T = \{y_1, \ldots, y_{2^t}\}$, find the preimage of one of the y_i by H, i.e., find $i \in \{1, \ldots, 2^t\}$ and $x \in \{0,1\}^n$ such that $H(x) = y_i$.

The best classical algorithm finds one out of 2^t targets with an exhaustive search in $\Omega(2^{n-t})$. When $t \leq 3n/7$ its quantum time complexity is $\tilde{\mathcal{O}}(2^{n/2-t/6})$, with quantum memory requirements of $\mathcal{O}(n)$. This approach in the $Q1$ setting can be utilized to detect collisions and multi-target preimages in hash functions. However, when using the algorithm to attack encryption modes, it needs to operate in the Q2 setting, as discussed in [15].

3) SIMON'S ALGORITHM

Simon's algorithm [23] is a quantum algorithm designed to solve the following problem: Given a function $f : \{0,1\}^n \to \{0,1\}^n$ such that there exists $c \in \{0,1\}^n$ satisfying the property that for all $x, y \in \{0,1\}^n, f(x) = f(y)$ if and only if $y = x \oplus c$ or $x = y$, where $\oplus$ denotes bitwise XOR. The objective is to find c.

We can extend this algorithm to determine whether two functions f and g satisfy $g(x) = f(x \oplus s)$ for all x and some s. Classically this requires $\Omega(2^{n/2})$ queries to the function f, as per the birthday problem. In the quantum setting, using Simon's algorithm, this requires only $\mathcal{O}(n)$ queries, implying an exponential speed-up. However, this algorithm requires highly structured components, which makes it only suitable in very specific cases.

This algorithm has been used in many attacks on modes of operation and cryptographic constructions (see for example [1] and [24]). Moreover, Simon's algorithm was applied to break established MAC and authenticated encryption modes, along with conducting quantum slide attacks. These attacks are generally very efficient [25] and the precise impact on commonly used symmetric cryptography algorithms will be explored in Section IV.

The offline Simon attack: The aforementioned attacks using Simon's algorithm are in the Q2 model, where one requires superposition queries to a quantum oracle. However, this is not always of much practical use (see Section III). In [26] a variant of Simon's algorithm is proposed that can be used in the Q1 model. They use it to attack the Even-Mansour construction in quantum time $\tilde{\mathcal{O}}(2^{n/3})$ with $\mathcal{O}(2^{n/3})$ classical queries and $\mathcal{O}(n^2)$ qubits (where n is the security parameter). To the best of our knowledge Simon's algorithm does not offer any significant advantages in attacking AES.

4) KUPERBERG'S ALGORITHM

Kuperberg's algorithm solves a relatively similar problem as Simon's algorithm. It solves the hidden shift problem (HSP). Let f, g be two injective functions, $(G, \cdot)$ a group. Given the promise that there exists $s \in G$ such that, for all x, $f(x) = g(x \cdot s)$, retrieve s. The first sub-exponential (in quantum query, and both quantum- and classical time) algorithms are presented in [27]. They have a time and space complexity of $2^{\mathcal{O}(n^{1/2})}$ for a group size of 2^n. Combination algorithms such as Kuperberg+Simon have been developed, followed by improvements to the initial algorithms (for both see [28]).

Attack in the Q2 Model

The paper [28] introduces a quantum attack on the Poly1305 message authentication code (MAC), which is used in protocols such as TLS 1.3. The MAC is designed to provide a security level of 128 bits. The quantum attack has a time and query complexity of 2^{38}, which raises concerns about its quantum security, even though the attack is in the Q2 adversary model.

5) DEUTSCH-JOZSA ALGORITHM

The Deutsch-Jozsa algorithm [29], together with Bernstein-Vazirani and Shor's algorithm are algorithms used in the quantum variant of the classical linearization attacks, the latter first introduced in [30]. These attacks target nonlinear terms in a block cipher and replace them with linear terms in order to obtain the secret key.

The Deutsch-Jozsa algorithm is a deterministic quantum algorithm that offers an exponential speed-up over any deterministic classical algorithm when solving the Deutsch-Jozsa problem. This problem is as follows: suppose we have access to a black-box quantum oracle that implements a function $f : \{0,1\}^n \to \{0,1\}$. We are given the assurance that this function is either constant (where it consistently produces the same output) or balanced (meaning half the inputs map to 0 and the other half to 1). The task is to determine, by using the oracle, whether f is a constant or balanced function. In the classical world we would, in the worst case, have to check $2^{n-1} + 1$ function values. The Deutsch-Jozsa algorithm does it within 1 query.

The Deutsch algorithm [31] is a special case of the Deutsch-Jozsa algorithm for $n = 1$. It solves the problem with 1 query instead of the 2 needed queries in the classical case. This might seem like a negligible speed-up, but it is crucial when the same function cannot be queried more than once.

In [32, Section 3.1] two attacks utilizing Deutsch-Jozsa on symmetric cryptography are given.

Attacks in the Q2 Model

Attack on ΘCB: ΘCB is an advanced mode of operation that offers a higher-level abstraction compared to OCB3, which is itself extension of OCB. In ΘCB, the block cipher is replaced by a tweakable block cipher (see [33] for the meaning of tweakable). Notably, [32] successfully executed a forgery attack, creating legitimate messages without prior knowledge of the encryption key. This attack can be avoided by choosing the initial value (IV) in a clever way [34].

XOR MACs: A XOR MAC (message authentication code) [35] is a method for verifying the authenticity and integrity of transmitted messages. They are considered classically secure, if their underlying finite pseudorandom function (cf. Definition 9) family is secure. Using Deutsch's algorithm forgery attacks can be made.

Bernstein-Vazirani [36]: The Bernstein-Vazirani (BV) algorithm solves the Bernstein-Vazirani problem: given access to an oracle for a function $f : \{0,1\}^n \to \{0,1\}$, that satisfies $f(x) = s \cdot x$ for unknown $s \in \{0,1\}^n$ and $\cdot$ being the dot product in $\mathbb{F}_2$, find s. Classically, this can be solved with n queries to the oracle. In the quantum setting this can be done within 1 query.

Attacks in the Q2 Model

Partial key recovery Even-Mansour: An attack on the Even-Mansour construction, which relies on two keys denoted as k_1 and k_2, is discussed in [37]. In this work, an algorithm based on BV's algorithm is introduced, allowing for the recovery of one of the keys with an overwhelming probability. This is achieved using n^2 queries (with n the bit size of both k_1 and k_2), an exponential improvement over the classically required $2^{n/2}$ queries.

Quantum distinguisher on 3-round Feistel scheme: A Feistel scheme is a classical construction for creating block ciphers. Specifically, a 3-round Feistel scheme is constructed using three random functions denoted as P_1, P_2, and P_3. It has been established that a 3-round Feistel scheme remains a secure pseudorandom permutation (a bijective PRF), provided that the internal functions are pseudorandom [38]. However, in a study by Xie et al. [37], a quantum-based distinguisher is developed using the BV algorithm, enabling the differentiation between the 3-round Feistel scheme and a truly random permutation.

Forgery attack: The attack on ΘCB with Deutsch's algorithm can be generalised to also work with BV's algorithm [32].

Grover meets BV: In [39] both Grover's algorithm and BV's algorithm are employed to perform attacks on several round Feistel contructions. We have not seen any successful attacks that break current block cipher implementations based on Feistel structures (e.g., Camellia [40]).

Shor's algorithm [41]: Surprisingly, Shor's algorithm finds its place in this list. Initially, Shor introduced his algorithm for period finding, from which factoring and solving the discrete logarithm problem are specific applications. Today, we commonly refer to the factoring algorithm as Shor's algorithm. The factoring algorithm has a significant impact on public-key cryptography but not as much on symmetric cryptography. However, the period finding algorithm can be used to attack symmetric cryptographic primitives. This algorithm solves the following problem. Let $(G, +)$ be a finite abelian group of size 2^n, X an arbitrary set. Given access to a function $f : G \to X$ that is either injective, or periodic, determine the case and/or find the period.

Classically, this requires subsequent queries to the function until the output repeats, i.e., this takes $\mathcal{O}(2^n)$ queries to the function. Using Shor's algorithm this can be reduced to $\mathcal{O}(\text{poly}(\log(2^n))$.

Attack in the Q2 Model

Poly1305: We have already talked about Poly1305 (a MAC to provide 128 bits of security) when investigating Kuperberg's algorithm, but Shor's algorithm can also be used. Kuperberg's algorithm required explicitly 2^{38} quantum gates and the same number of queries to an oracle. In contrast, the attack in [32] using Shor's algorithm only needs 32 superposition queries, while still requiring the same number of quantum gates. This represents a significant reduction in superposition queries.

We have discussed several algorithms that are used to investigate the quantum security of symmetric cryptography, but this list is by no means exhaustive. Various combinations of the aforementioned attacks have led to intriguing discoveries (see for example [42] for Grover+Simon, and [28] for Simon+Kuperberg). Additionally, some attacks originally designed using the Q2 model have been adapted to the Q1 adversary model (e.g. the *offline Simon attack*), albeit at a reduced efficiency.

Quantum adaptations of classical attacks: The boomerang attack [43] is a differential attack that exploits the structure in block cipher designs to recover the key. A quantum variant (the *quantum boomerang attack*) was explored in [44]. Although faster than its classical counterpart, the attack was shown not to exceed the quadratic speed-up of Grover's attack.

Similar conclusions were drawn in [45], where quantum adaptations of linear and differential cryptanalysis were explored. These adaptations achieved quadratic speed-ups but did not exceed Grover's results for keys that are the same size as the block size. Interestingly, however, they found that the speed-up of these attacks increases when the key size exceeds the block size.

III. RELEVANCE OF THE ADVERSARY MODELS Q1 AND Q2

Most of the improvements regarding time complexity and memory demands are happening in the Q2 adversary model. In this section we investigate the relevance of this model and compare it with the Q1 model. Recall the different attacking models: Q0, Q1 and Q2 in the realm of symmetric cryptography (see Section II-C).

A. Q1 MODEL AND ITS RELEVANCE

In the Q1 model, we consider classical infrastructure with adversaries possessing quantum computers. This makes the model extremely relevant due to store now, decrypt later attacks. Moreover, there are many relevant attacks appearing within the Q1 model, highlighting its significance, particularly in the realm of asymmetric cryptography. For instance, RSA's security relies on the difficulty of factoring large integers, a problem efficiently solvable by Shor's algorithm on a

quantum computer, without the need for superposition queries. In symmetric cryptography, we have encountered a few Q1 attacks, such as the *offline Simon attack*, *collision finding algorithms*, and *brute force attacks*. The last one uses Grover's algorithm and gives at most a quadratic speed-up. Additionally, the threat of *store now, decrypt later* is only relevant in this model and not in the Q2 model.[5]

B. Q2 MODEL AND ITS RELEVANCE

In the Q1 model, we have focused on cryptography running on classical infrastructures with an adversary possessing a quantum computer. This is extremely relevant due to store now, decrypt later attacks. However, in the distant future, one might envision a world where everyone has quantum computers, a scenario that can be thought of as the Q2 model. This naturally grants the adversary more power. Take, for instance, the Even-Mansour block cipher (discussed in Section II-E). This cipher is considered classically computationally secure.[6] However, when examined in the Q2 model, it is completely broken. In [1], an algorithm is presented that can break the Even-Mansour cipher with a complexity of $\mathcal{O}(n)$ (with n the security parameter), a huge improvement compared to the classical approach with a complexity of $\mathcal{O}(2^{n/4})$. This is a big result, implying that some algorithms that are considered classically secure will not remain secure once we can make superposition queries to an oracle.

As mentioned earlier, the Q2 model becomes relevant when cryptographic algorithms operate on a quantum computer, enabling superposition queries. In practice, one approach to prevent adversaries from making such queries is to measure the final state of an encryption process, ensuring all outcomes are classical. This approach relies on a physical hardware assumption, specifically the accurate implementation of this final *classicalization* step, which can effectively protect against quantum superposition attacks. Therefore, with accurate physical implementation, it is feasible to achieve Q2-secure schemes.

However, despite the potential effectiveness of such a mitigation strategy, it is important to recognize the practical scenarios where the Q2 model becomes relevant. For instance, consider a future scenario described in [46], where an adversary targets a classical encryption chip, and by manipulating the chip's physical environment, induces quantum behavior, enabling him to query the device on a superposition of plaintexts. It is not unreasonable to assume that ongoing innovations like extreme miniaturization and optical electronics will make it possible to induce quantum behavior in future electronics.

While these situations seem unlikely, history regarding cryptography shows it is wise to consider the worst-case scenario, in this case where the adversary can query the target device in superposition. Here are several more reasons why this model should be considered:

1) **Natural next step**: The model assumes the adversary has access to a quantum computer for computations. It is reasonable to assume that when quantum computers are strong enough to run algorithms to break cryptography, we might also see situations where cryptography is run on a quantum computer. Also, as illustrated above, the cryptography targeted can run on a classical device and might be manipulated to behave in a quantum manner.
2) **General security**: Security in the Q2 model implies security in any other scenario, except for related-key attacks.
3) **Non-triviality**: This model does not immediately break all cryptography. There are several proposed primitives that remain secure in this model [2].
4) **Potential Q1 attacks**: Attacks in the Q2 model could lead to the discovery of attacks in the Q1 model (e.g., the offline Simon attack as seen in Section II-E).
5) **Practical scenarios**: Situations may arise where messages are encrypted in superposition, either by accident or intention. For instance, an encryption scheme integral to a quantum protocol using quantum communication differs from a standard protocol resilient to quantum adversaries [47].
6) **Inherently immune systems**: Creating systems inherently immune to superposition attacks eliminates the need for hardware designers to worry about the quantum security aspects of its cryptographic implementations [2].

C. OVERHEAD

A key question to consider is the overhead introduced when aiming for security in the Q2 model. This overhead can be addressed through either hardware implementations or cryptographic adjustments, such as consistently using Q2-secure schemes. Hardware-based approaches remain speculative, as quantum computers have not yet advanced to that level. On the cryptographic side, it varies. It is feasible to choose a block cipher and mode of operation that are both Q2-secure, since not all have been broken in the Q2 model (see Section IV and Section V). In theory, one could use a Q2-secure mode of operation like OFB or CTR (cf. Table 3) and add Q2-secure authentication on top. However, this approach is often error-prone, and authenticated encryption (AE) is generally preferred in situations that require both authentication and confidentiality. Most widely used AE schemes are not Q2-secure (cf. Section V-C), but there are promising proposals like QCB. Nonetheless, its practical performance remains unknown.

IV. SECURITY OF BLOCK CIPHER PRIMITIVES

In previous sections, we have discussed adversary models, both classical and quantum, as well as important quantum

[5]The Q2 model requires an oracle, which it can send *superposition* queries. It cannot use harvested data, since this data was not a result of superposition queries.

[6]Under existential forgery attacks and standard decryption attacks.

algorithms relevant to the security of block cipher-based cryptography. We now outline some security concepts, discuss which block ciphers have been broken, and look into specific quantum attacks on block ciphers.

A. SECURITY NOTIONS

Classical and quantum generic attacks: By *generic attack*, we mean brute-forcing the key. If an attack demonstrates greater efficiency[7] than a brute force attack, it suggests the block cipher is broken. In the realm of quantum computing, Grover's algorithm can be used for brute force attacks, and is considered the *generic attack*. It provides a quadratic speed-up compared to classical brute force. For future reference, we define the security of a block cipher.

Definition 11 ((Quantum) Security of Block Ciphers): A block cipher E is considered broken if an attack is known that is markedly more efficient than the generic attack: classically, a brute force search for the key, and in the quantum setting, a Grover's search for the key.

Remark 2: The notions of a block cipher being *broken* and being *secure* are distinct. To deem a block cipher secure, it must not be broken, **and** the brute force attack must be computationally infeasible. This typically means that the brute force attack requires an average of 2^{128} operations to perform (cf. level 1 [48, p.16]).

Security margin: Many block cipher primitives utilize internal *rounds*, which involve a repetition of the same steps. Each round contributes to the security[8] of the cipher. The *security margin* is defined as *the highest number of rounds for which an attack has been found to be more efficient than the best generic attack* [9].

Impact of Grover's algorithm: In classical cryptography, brute force attacks have a complexity of $\mathcal{O}(2^n)$, where n denotes the security parameter (often equal to the key length). In the quantum realm, Grover's algorithm stands as the best generic attack, characterized by a complexity of $\mathcal{O}(2^{n/2})$.

B. BROKEN BLOCK CIPHERS

We investigate which block ciphers are susceptible to attacks more efficient than Grover's search akin to Definition 11. Given the immense number of ciphers out there, we only focus on well-known algorithms or those that have excelled in recent cryptographic competitions. Noteworthy competitions include the NIST Lightweight Cryptography Competition (Lightweight) and the CAESAR competition (CAESAR). Thus far, no attacks have been found against the AES block cipher that are asymptotically more efficient than a Grover search for the key (see Section VI for details on the security of AES).

[7]Determining efficiency can be ambiguous. If the (asymptotic) complexity of the attack is the same, a cipher may not be considered broken, as shown with the Biclique attacks on AES in Section VI.

[8]This only holds up to a certain bound due to slide attacks [49].

1) EVEN-MANSOUR

Introduced in 1997 [50], the Even-Mansour cipher is defined as

$$\mathrm{EM}^{\mathcal{F}}_{K_1,K_2}(x) = \mathcal{F}(x \oplus K_1) \oplus K_2,$$

where $\mathcal{F}$ is a publicly known permutation over n-bit strings, and K_1 and K_2 are n-bit keys. The cipher aims to have a formal proof of security while maintaining simplicity [51].

Its classical security proof shows that the best attack has a time complexity of $\mathcal{O}(2^n)$ for a key of length $2n$. In [1] an attack is presented, using Simon's algorithm (see Section II-E) which breaks the Even-Mansour cipher in the Q2 adversary model. The main insight behind this attack is that the n-bit secret key K_1 acts as the period of the function $\mathrm{EM}^{\mathcal{F}}_{K_1,K_2}(x) \oplus \mathcal{F}(x)$. This allows the use of Simon's algorithm, as quantum queries to $\mathrm{EM}^{\mathcal{F}}_{K_1,K_2}(x)$ are permitted. The exponential speedup compared to classical attacks comes from leveraging the algebraic structure of $\mathrm{EM}^{\mathcal{F}}_{K_1,K_2}(x)$ and its hidden period using Simon's algorithm. The follow-up paper [26], translated the Q2 attacks into Q1 attacks. This was the first time it was shown that Q2 attacks can, under certain circumstances, be translated to Q1 attacks.

We remark that there is a variant of Even-Mansour, called Tweakable Even-Mansour, which can be proven secure in the Q1 model [52].

2) THE FX-CONSTRUCTION

Although the FX-construction [53] is not a block cipher itself, it provides a straightforward approach to increase the key length of a block cipher by combining a generic cipher with the Even-Mansour cipher. As a result, it's not surprising that Simon's algorithm is relevant in this context. This construction is, for instance, applied in the PRINCE block cipher, which is used to encrypt memory in certain types of micro-controllers (see [54] and [55]).

Simon's algorithm-based attacks, described in [42], effectively break the FX-construction in the Q2 adversary model. Similarly as in Section IV-B1, the follow-up paper [26] translated these Q2 attacks into Q1 attacks. Although these Q1 attacks (on Even-Mansour and the FX-construction) are less effective, they still outperform generic attacks, indicating that the FX-construction is also compromised in the Q1 model.

3) SUMMARY OF EVEN-MANSOUR AND THE FX-CONSTRUCTION

To summarize the complexities of quantum attacks (Q1 & Q2) on the Even-Mansour and FX constructions, we present Table 1:

4) PRINCE AND PRINCEV2

In [54], the attack from [26] on the FX-construction was implemented to target the PRINCE cipher [57], which is a 64-bit block cipher with a 128-bit key. The classical security of PRINCE is characterized by a data-time trade-off of $D \cdot T \geq 2^{126}$, where D represents the amount of plaintext-ciphertext

TABLE 1. Summary of the complexity of quantum attacks (Q1 & Q2) on Even-Mansour and the FX-construction for an n-bit block cipher with an m-bit key [26].

Target (model)	Queries	Time	Q-memory†	C-memory‡	Ref.
EM (Q2)	$\mathcal{O}(n)$	$\mathcal{O}(n^3)$	$\mathcal{O}(n)$	$\mathcal{O}(n^2)$	[1]
EM (Q1)	$\mathcal{O}(2^{n/3})$	$\mathcal{O}(2^{n/3})$	$\mathcal{O}(2^{n/3})$	$\mathcal{O}(2^{n/3})$	[1]
EM (Q1)	$\mathcal{O}(2^{3n/7})$	$\mathcal{O}(2^{3n/7})$	$\mathcal{O}(n)$	$\mathcal{O}(2^{n/7})$	[56]
EM (Q1)	$\mathcal{O}(2^{n/3})$	$\mathcal{O}(n^3 2^{n/3})$	$\mathcal{O}(n^2)$	$\mathcal{O}(n)$	[26]
FX (Q2)	$\mathcal{O}(n2^{m/2})$	$\mathcal{O}(n^3 2^{m/2})$	$\mathcal{O}(n^2)$	0	[42]
FX (Q2)	$\mathcal{O}(n)$	$\mathcal{O}(n^3 2^{m/2})$	$\mathcal{O}(n^2)$	$\mathcal{O}(n)$	[26]
FX (Q1)	$\mathcal{O}(2^{3(m+n)/7})$	$\mathcal{O}(2^{3(m+n)/7})$	$\mathcal{O}(n)$	$\mathcal{O}(2^{(m+n)/7})$	[56]
FX (Q1)	$\mathcal{O}(2^{(m+n)/3})$	$\mathcal{O}(n^3 2^{(m+n)/3})$	$\mathcal{O}(n^2)$	$\mathcal{O}(n)$	[26]

† Quantum memory.
‡ Classical memory.

TABLE 2. Precise quantum resources required to perform a key recovery attack using the offline Simon attack on the PRINCE cipher [54].

Target	Offline Queries	Operations	Circuit Depth	Qubits	Remarks
PRINCE	2^{48}	$2^{65.0}$	$2^{54.9}$	$2^{14.0}$	With query limit
PRINCE	2^{50}	$2^{64.4}$	$2^{54.9}$	$2^{14.0}$	Without query limit
PRINCE	3	$2^{80.1}$	$2^{75.7}$	$2^{8.0}$	Grover's key search

pairs gathered by the adversary. In Table 2 we outline the precise resources needed.

In the Q1 setting, the offline Simon attack proves more efficient compared to the general attack (Grover's key search), thus technically rendering PRINCE broken.

In 2020, an updated version of the PRINCE cipher, known as PRINCEv2, was introduced [58]. It features a different key schedule and no longer employs the FX construction, making it immune to the attack previously mentioned. To date, no quantum attacks exploiting weaknesses in PRINCEv2 have been discovered.

5) AEZV5, COPA, AND CLOC

AEZv5 features a key size of 384 bits and was a third-round candidate in the CAESAR competition, which aimed to identify new authenticated encryption schemes. The cipher incorporates several internal functions that, when combined, enable Simon's algorithm to discover periods. It is vulnerable to a key recovery attack in the Q2 model, as outlined in [59]. The attack, employing Simon's algorithm, demonstrated a time complexity of only $2^{11.1}$. In [25], successful Q2 forgery attacks using Simon's algorithm are detailed against several CAESAR candidates, including the third-round candidates COPA and CLOC. CLOC is compromised due to its use of the CBC-MAC mode, which is vulnerable to period-finding attacks. A similar vulnerability affects COPA.

C. ASCON

So far, we have discussed several ciphers featured in the CAESAR lightweight cryptography competition. As an honorable mention, we want to highlight Ascon, a lightweight cryptographic cipher designed for resource-constrained environments such as IoT devices and embedded systems. It provides authenticated encryption with associated data (AEAD) and is optimized for efficiency. Ascon was selected as a winner in of the CAESAR competition and is recognized for its strong security against both classical and quantum attacks. To date, the only known quantum attack uses Grover's algorithm [60], requiring $1.26 \cdot 2^{155}$ operations to retrieve the key for ASCON-128 (128-bit key).

D. COLLISION RESISTANCE

Collision finding algorithms (Section II-E) aim to identify pairs of inputs to a function that yield identical outputs. The security of hash functions relies heavily on their ability to resist collision finding attacks. However, collision finding algorithms can also pose threats to the security of block ciphers. For instance, in 2016, the *SWEET32 attack* targeted 64-bit block ciphers such as TDES, in combination with common modes of operation [61]. This attack heavily relied on collision finding algorithms. The complexity of a collision attack in this context depends on the block size, not the key size.

In classical settings, the complexity of naive collision search is $\mathcal{O}(2^{n/2})$, due to the birthday attack. In the quantum setting, the time complexity of naive collision search is $\tilde{\mathcal{O}}(2^{2n/5})$ (see Section II-E), requiring only $\mathcal{O}(n)$ quantum memory [15][9]. This implies that naive quantum collision search is somewhat more efficient ($\tilde{\mathcal{O}}(2^{0.4n})$ instead of $\mathcal{O}(2^{0.5n})$) for single-target collision search) compared to the naive classical case, but there is no quadratic speed-up like Grover's attack. No literature has been found that explicitly demonstrates weaknesses in block ciphers through the use of quantum collision algorithms.

V. MODES OF OPERATION

Block cipher primitives are limited to encrypting or decrypting a fixed-size block, and require additional techniques to handle arbitrary message lengths. A *mode of operation* (or *mode of use*) is used to chain multiple blocks together to support larger messages and a padding scheme is used to pad the messages in order to fit the block size. Modes of operation can also be used to construct KDFs (*key derivation functions*) from block cipher primitives, or to provide message authentication and integrity guarantees.

We will examine common modes of operation (see Section I-A), dividing them into *encryption*, *authentication*, *authenticated encryption* and *KDF* modes. In Section VI-E, we discuss these modes of operation when the AES algorithm is used as the underlying block cipher.

[9] Quantum attacks with a time complexity of $\tilde{\mathcal{O}}(2^{n/3})$ also exist [22], but these attacks involve a memory complexity of $\tilde{\mathcal{O}}(2^{n/3})$, resulting in a higher product (of time- and memory complexity) of $\tilde{\mathcal{O}}(2^{2n/3})$ than the classical attack, which has product of time- and memory complexity $\mathcal{O}(2^{n/2})$.

TABLE 3. Security of encryption modes of operation in quantum settings, according to [47], with added information on XTS from [62].

Mode	IND-1CPA (Q1)	IND-qCPA (Q2) (with PRF)	IND-qCPA (Q2) (with qPRF)
ECB	No	No	No
CBC	Yes	No	Yes
CFB	Yes	No	Yes
XTS	Unknown	No (in spirit)†	Yes‡
OFB	Yes	Yes	Yes
CTR	Yes	Yes	Yes

† A quantum adversary can recover part of the key and plaintext. However, the security notion IND-qCPA is not formally broken.
‡ Given some extra assumptions (next to the block cipher being a qPRF) like the sector addresses being uniformly random [62].

TABLE 4. Security of authentication modes of operation in quantum settings.

Mode	Q1 model	Q2 model	Source
CBC-MAC	No literature	EUF-qCMA insecure†	[25]
HMAC	No literature	EUF-qCMA secure‡	[65]
CMAC	No literature	EUF-qCMA insecure	[25]

† It is EUF-qCMA secure if both a nonce prefix variant and a qPRF are used [5].
‡ Under the standard assumption that the underlying compression function is a qPRF.

A. ENCRYPTION MODES

Table 3 provides an overview of the security of various encryption modes of operation, assuming the underlying block ciphers are at least classical *pseudorandom functions* (see Definition 9). Given the numerous security notions, we focus on the most common: IND-1CPA (in Q1) and IND-qCPA (in Q2), as detailed in Section II-B. Note that we do not include any quantum CCA (chosen ciphertext attack) notions, as these have not yet been properly adapted to the quantum setting.

Remark 3: The last two columns require further explanation. The **with PRF** column assumes the underlying block cipher functions as a classical PRF (cf. Definition 9), while the **with qPRF** column assumes it behaves as a quantum PRF (cf. Definition 10).

The ECB (Electronic Codebook) mode is insecure in all scenarios and is not recommended for current applications due to the amount of information it leaks [63]. Both CBC and CFB modes are vulnerable in the Q2 model when the underlying block cipher functions solely as a PRF and not as a qPRF. In the case of XTS mode, commonly used for disk encryption, a Q2 quantum adversary can recover parts of both the key and the plaintext if the block cipher is not a qPRF. The CBC, CFB, and XTS modes are all susceptible to attacks using period finding through Simon's algorithm. Conversely, the OFB and CTR modes can achieve IND-qCPA even when the block cipher is only a classical PRF. For more details on the CBC, CFB, OFB, and CTR modes, refer to [64].

B. AUTHENTICATION MODES

Instead of encryption, a block cipher can also be used for authentication. We explore two block cipher modes: CBC-MAC and CMAC, and include the *hash-based* HMAC for comparison. Table 4 outlines the quantum security for each of these authentication modes (see [5], [25] and [65]).

Unlike encryption, where IND-1CPA is the most commonly used notion in Q1, and IND-qCPA is the most commonly used notion in Q2, there is still ongoing debate about which quantum security notions to use for authentication. Providing a complete overview of all the notions would be overly complex, so we only discuss the most frequently occurring: *EUF-qCMA* and *1PO* (see Section II-B).

As in Section V-A, we assume that the underlying block cipher or hash function is at least a PRF. It should be noted that CBC-MAC and CMAC are EUF-qCMA insecure, regardless of the type of underlying block cipher [25].

Once again, these insecurities come from the clever use of period finding with Simon's algorithm.

Remark 4: In the quantum realm, after approximately $\tilde{\mathcal{O}}(2^{2n/5})$ MAC'ed messages (see Section IV-D), using an n-bit MAC, there is a significant likelihood of encountering two distinct messages M_1 and M_2 such that

$$\mathrm{MAC}_k(M_1) = \mathrm{MAC}_k(M_2).$$

Consequently, finding collisions for both CMAC and CBC-MAC using a block cipher with a 128-bit block size requires, on average, 2^{51} operations. This scenario assumes that the adversary can obtain enough signed messages. Moreover, this poses a problem only if knowledge of two messages with the same MAC enables the creation of the MAC for a new message. The latter is a known vulnerability for CBC-MAC with variable length messages, we do not know whether this affects CMAC.

C. AUTHENTICATED ENCRYPTION MODES

The modes of operation mentioned above offer either encryption or authentication, but not both. However, there are modes that provide both functionalities, known as authenticated encryption (AE) modes. The security of these modes is typically modeled by separately considering their encryption and authentication components. Therefore, we use the same quantum security notions as discussed in Section V-A and Section V-B. Table 5 gives an overview of the results found.

We observe that for OCB, GCM, EAX, SIV, and (AES)-OTR, their security remains unaffected regardless of whether the underlying block cipher is a PRF or a qPRF.

Remark 5: Regarding SIV, it has numerous variants, but our examination focused on the most generic variant [67].

TABLE 5. Security of authenticated encryption modes in quantum settings.

Mode of Operation	Q1 model	Q2 model
OCB†	No literature	IND-qCPA insecure [62], EUF-qCMA insecure [25]
CCM	No literature	No literature‡
GCM	No literature	IND-qCPA insecure⋆ [5], EUF-qCMA insecure [25]
CWC	No literature	No literature
EAX	No literature	IND-qCPA insecure, EUF-qCMA insecure [5]
SIV	No literature	IND-qCPA insecure, EUF-qCMA insecure [5]
(AES-)OTR	No literature	IND-qCPA insecure [66], EUF-qCMA insecure [25]

† OCB has 3 variants. OCB2 is **not** classically secure. We only look at OCB1 and OCB3 here.
‡ [25] mentions that the attacks he found (based on Simon's algorithm in Q2) do not apply to CCM, because of its nonce use, which might give a positive indication towards its quantum security.
⋆ GCM can be IND-qCPA secure if a specific nonce length is used [5], but this does not counter the EUF-qCMA insecurity found by Kaplan [25].

Observing the table above, it is clear that many modes of operation are insecure in the Q2 model, and none have been proven secure in Q2. Some attacks compromise both the authentication and encryption aspects, as seen in the cases of OCB and GCM. Despite this, much remains unknown about these AE modes, particularly regarding their security in the Q1 model. Ongoing research investigates Q2-safe authenticated encryption, with promising proposals like QCB (see [34], [68] and [69]).

Remark 6: All of these attacks can be executed using Simon's algorithm in some capacity, either through period finding or linearization [32]. With the exception of the attacks on OCB3 authentication, which can be carried out using Deutsch's algorithm (cf. Section II-E).

D. KEY DERIVATION FUNCTIONS

Key derivation involves generating one or more cryptographic keys from a secret using a PRF. This process is typically carried out by *key derivation functions* (KDFs). These functions are commonly employed to enhance the entropy of low-entropy inputs, such as human-generated passwords, or inputs that do not possess the required characteristics. For example, TLS 1.3 and the Signal double ratchet protocol use HKDF [70], a KDF based on HMAC, for this purpose [71]. While most KDFs are based on hash functions, some utilize block ciphers, as shown in NIST SP 800-108 Rev. 1 [13].

KDFs will play a crucial role in *hybrid post-quantum protocols*, which involve utilizing two key exchange algorithms—one quantum-safe and one that is not, such as x25519+ML-KEM [72]. The outputs of both algorithms must be combined into a single secret key. Proposals for these *key combiners* suggest the use of KDFs [73]. Specifically for this purpose, the chosen KDF should act as a *dual-PRF*, functioning as a PRF with two input keys and remaining secure even if one of the inputs is compromised or malicious.

- **Security:** The security of a key derivation function is evaluated based on the extent to which we can distinguish its output from a genuinely uniformly distributed bit string of the same length [70].
- **Quantum:** No quantum attacks targeting KDFs (either block cipher or hash based) have been found in the literature.

The quantum security of key combiners and quantum dual-PRFs has only recently gained attention, as highlighted in [71] and [74]. The theoretical understanding in this area is still developing, and much research is needed before definitive security claims can be made. For instance, there is no proof that the KDF used in the quantum-safe standard [73], which incorporates KMAC-128, KMAC-256, SHA3-256, and SHA3-512, functions as a quantum dual-PRF. Additionally, [75] proposes a hybrid scheme that simply concatenates both outputs and uses HKDF, the standard KDF in TLS 1.3. However, HKDF is only proven to be a quantum PRF, not a dual-PRF [71]. Although these methods are based on hash functions and fall outside the scope of this paper, we emphasize the lack of proofs as a significant issue.

E. QUANTUM SIDE-CHANNEL ATTACKS

The focus in this paper has been on the *cryptographic* security of block ciphers. We have not looked at potential benefits of quantum computing to side-channel attacks. Very little is known in the case that a potential quantum adversary has more information due to potential side-channel leakage. In [76] a side channel attack is shown which gives another quadratic speed-up on top of Grover's algorithm. However, we could not find more literature regarding this topic.

VI. SECURITY OF AES AND ITS MODES OF OPERATION

In this section, we delve into the most prevalent symmetric cryptographic cornerstone of today' the Advanced Encryption Standard (AES). We review its classical security, compare it with known quantum attacks and aim to give a thorough overview on the quantum security of AES.

A. THE CLASSICAL SECURITY OF AES

AES comes in three versions: AES-128, AES-192, and AES-256, each defined by a unique key size. These different key sizes make brute force attacks infeasible, requiring approximately 2^{128}, 2^{192}, or 2^{256} operations, respectively. Up until the time of writing no classical attacks have been found that drastically decrease the number of operations needed to break AES. The only attack on full[10] AES is the Biclique attack [77] reducing the complexity by a factor of 4. Table 6 gives the precise numbers.

[10]Full AES means the version of AES as intended, so not the reduced round version.

TABLE 6. Classical key recovery attacks on AES.

AES version	Biclique complexity	Brute force complexity	Data complexity
AES-128	$2^{126.1}$ operations	2^{128} operations	2^{88} plaintext-ciphertext pairs
AES-192	$2^{189.7}$ operations	2^{192} operations	2^{80} plaintext-ciphertext pairs
AES-256	$2^{254.4}$ operations	2^{256} operations	2^{40} plaintext-ciphertext pairs

TABLE 7. Quantum resource estimates for Grover's algorithm to attack AES-*k*, where $k \in \{128, 192, 256\}$ [80]. Two types of gates, T and Clifford, were used to construct the circuits.

	#gates		depth†		#qubits
k	T	Clifford	T	overall	
128	$1.19 \cdot 2^{86}$	$1.55 \cdot 2^{86}$	$1.06 \cdot 2^{80}$	$1.16 \cdot 2^{81}$	2953
192	$1.81 \cdot 2^{118}$	$1.17 \cdot 2^{119}$	$1.21 \cdot 2^{112}$	$1.33 \cdot 2^{113}$	4449
256	$1.41 \cdot 2^{151}$	$1.83 \cdot 2^{151}$	$1.44 \cdot 2^{144}$	$1.57 \cdot 2^{145}$	6681

† The longest path in the circuit.

The speed-up from the Biclique attack is so little and the amount of data needed is so huge that most literature omits the attack and still says that AES is secure.

B. THE QUANTUM SECURITY OF AES

It is often recommended to double the key size as a precaution against Grover's attack, a principle that applies to AES as well. However, doubling the AES key size to counter Grover's algorithm is considered conservative due to several factors. Quantum computing hardware will likely be more costly to build and operate than classical hardware. Moreover, Zalka demonstrated [78] that achieving the full quadratic speed-up of Grover's algorithm requires all steps to be performed sequentially. While brute-force attacks are typically parallelized in practice to reduce the time required to break a key, parallelizing Grover's algorithm is inefficient and significantly reduces its advantage.

Several authors have delved into the precise evaluation of the quantum resources involved in Grover's attack on AES, with a comprehensive overview provided in [79]. There are three main practical resources needed for a key recovery attack on AES using Grover's algorithm. The number of qubits, the number of quantum gates and the number of plaintext-ciphertext pairs needed. In Table 7 we outline some of the resources needed to attack AES with a brute force search as found in [80].

Due to the overhead associated with implementing AES as a quantum circuit in Grover's algorithm, the costs are significantly higher than 2^{64}. Additionally, these implementations require a substantial number of Clifford gates, which are notoriously expensive to execute. In the 2017 NIST call for post-quantum cryptography (PQC), 2^{96} gates were defined as the approximate number that atomic-scale qubits could perform in a millennium, constrained by the speed of light [48, p. 17]. This comparison illustrates that the 2^{86} Clifford gates needed to attack AES-128 is substantial. Given that Grover's algorithm does not parallelize well, the practical implications suggest that doubling your key size when using AES-128 may not be necessary.

Quantum attacks on AES

Our discussion has focused on Grover-based brute force attacks against AES, as there are currently no other known quantum Q1 or Q2 attacks that offer greater efficiency. Nevertheless, there are quantum attacks identified on reduced-round AES, which will be explored in more detail in Section VI-D.

C. CLASSICAL SECURITY MARGIN OF AES

The algorithm AES consists of a number of transformation rounds: 10, 12 and 14 rounds for AES-128, AES-192, AES-256 respectively. The security margin of AES is the **number of rounds** for which an attack exists with a time complexity lower than 2^{128} (or 2^{196} or 2^{256}). If this margin is lower than the total chosen number of rounds in the complete cipher, it is considered secure.

For instance, in AES-128, one of the most potent classical attacks is the *impossible differential attack* [81], which can target up to 7 rounds with a time complexity of approximately 2^{105} and memory complexity of 2^{72}. Given that AES-128 consists of a total of 10 rounds, it remains secure in the classical context. On the other hand, for AES-256, the leading attack[11] is the Demirci-Selçuk Meet-in-the-middle attack (DS MITM) [82], which can address up to 8 rounds with a time complexity of approximately 2^{200}. As the primitive employs 14 rounds, it remains secure in the classical domain.

Remark 7: There are more powerful attacks than the above attacks. For example there are related-key attacks on AES-256 that target 10 rounds with a time complexity of 2^{45} [83]. However, in these attacks the adversary needs information about the interrelation between different keys (see Section II-C), hence there relevance could be subject to debate.

D. QUANTUM SECURITY MARGIN OF AES

For reduced-round AES-128 and AES-192, the most effective known quantum attacks that outperform a straightforward Grover search are quantum square attacks, which target 6 rounds for AES-128 and 7 rounds for AES-192, respectively. These attacks, as detailed in [9, Appendix A], still rely on Grover's algorithm but are more efficient than generic attacks on AES with the specified number of rounds.

The most effective quantum attack at the moment of writing for AES-256 is the quantum Demirci-Selçuk meet-in-the-middle attack (qDS-MITM) [9]. While using Grover's algorithm quantum DS-MITM outperforms Grover's generic key search for up to 8 rounds (if applied to 9 rounds, Grover key search becomes more efficient). Given that the primitive uses 14 rounds, it remains secure in the context of a quantum adversary model. In Table 8 we summarize these results.

[11] Excluding related-key attacks.

TABLE 8. Quantum security margin of AES (with classical margin to compare).

Version	Rounds reached† (classically)	Rounds reached† (quantum)	Rounds used in AES	Best quantum attack	Source
AES-128	7	6	10	Quantum square attacks (Q1)	[9]
AES-192	8	7	12	Quantum square attacks (Q1)	[9]
AES-256	9	8	14	qDS-MITM (Q1)	[9]

† **Important:** Note that for the classical case, the comparison is made against classical brute force search, while for the quantum case, the comparison is made against Grover's search.

The above attacks on reduced round AES takes place in the Q1 model. No attacks in the Q2 model have been found yet. For now it seems that the only classical attacks that have been accelerated more than quadratically are so-called slide attacks (first described in [49]) using Simon's algorithm (see Section II-E). However, AES seems to be immune to these attacks. While there exists a potential acceleration of the classical impossible differential attack within the Q2 model, the speed-up is less than quadratic. Notably, it appears that AES demonstrates a resistance to the exponential accelerations commonly encountered in the Q2 model, as discussed in [9].

E. SECURITY OF MODES OF OPERATION WITH AES

As discussed in Section V, it is evident that not all modes of operation are secure in a quantum setting, particularly in the Q2 model. For some modes, security within the Q2 model depends on whether the employed block cipher functions like a qPRF (see Section V-A).

AES is designed to function as a pseudorandom function in classical settings, generating output that is indistinguishable from a truly random function. This property is crucial when assessing the IND-qCPA security of cryptographic constructions such as CBC, CFB, OFB, and CTR. Currently, no Q1 nor Q2 attacks on AES are more efficient than Grover's attack. Due to this lack of attacks, AES-256[12] is widely recognized as a qPRF, ensuring security in its encryption/authentication modes (see Table 3 and Table 4). However, for authenticated encryption, both GCM and OCB are insecure in the Q2 model, regardless of the properties of AES.

[12]Only AES-256 is considered a qPRF (see Definition 10). Due to Grover's attack, the probability of distinguishing the output of AES-128 and AES-192 from a truly random function becomes non-negligible, violating the definition of a qPRF.

VII. SOME OBSERVATIONS AND UNANSWERED QUESTIONS

- Almost all current quantum attacks are based on Simon's algorithm in the Q2 model, which is important to keep in mind when designing new block ciphers and block cipher-based constructions.
- AES-256 is currently considered to be a quantum pseudorandom function, which means that, when used with an appropriate mode of operation, it is quantum-secure.
- There are very few provably secure authenticated encryption modes in the quantum setting. Research is needed to develop such modes, with a promising start made with QCB (see [34]).
- Some attacks ([17] and [18]) rely on QRAM (cf. Insight 1). However, the feasibility of QRAM in the near future is debated [16]. The relevance of these attacks depends on the development of QRAM, making it an important research area to monitor.
- The debate on quantum versions of security definitions in both the Q1 and Q2 model for authentication and authenticated encryption has not been fully concluded yet, making it difficult to draw conclusions.
- The quantum security of KDFs and key combiners is often assumed when the underlying block cipher is secure, but explicit proof is missing.
- The Q1 security model is the most relevant in the short term, yet most research has focused on the Q2 model. More investigation is needed into the Q1 security of authentication and authenticated encryption modes of operation. Ideally, proofs within the Q1 model should be provided, if possible.
- In practice, the high cost of implementing Grover's algorithm on AES reduces the urgency or necessity to double the key size.

ACKNOWLEDGMENT

The authors would like to thank Thomas Attema and Thijs Veugen, for their thorough review and insightful suggestions, which have significantly improved the quality of this article.

REFERENCES

[1] H. Kuwakado and M. Morii, "Security on the quantum-type Even–Mansour cipher," in *Proc. Int. Symp. Inf. Theory Its Appl. (ISITA)*, Honolulu, HI, USA, Oct. 2012, pp. 312–316. [Online]. Available: https://ieeexplore.ieee.org/document/6400943/

[2] D. Boneh and M. Zhandry, "Secure signatures and chosen ciphertext security in a quantum computing world," in *Proc. 33rd Annu. Cryptol. Conf.*, in Lecture Notes in Computer Science, vol. 8043, Santa Barbara, CA, USA. Springer, Jan. 2013, pp. 361–379, doi: 10.1007/978-3-642-40084-1_21.

[3] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*, 2nd ed., Boca Raton, FL, USA: CRC Press, 2014. [Online]. Available: https://www.crcpress.com/Introduction-to-Modern-Cryptography-Second-Edition/Katz-Lindell/p/book/9781466570269

[4] C. Chevalier, E. Ebrahimi, and Q.-H. Vu, "On security notions for encryption in a quantum world," in *Proc. 23rd Int. Conf. Cryptol. India*, in Lecture Notes in Computer Science, vol. 13774, Kolkata, India. Cham, Switzerland: Springer, Jan. 2022, pp. 592–613, doi: 10.1007/978-3-031-22912-1_26.

[5] N. D. Lang and S. Lucks, "On the post-quantum security of classical authenticated encryption schemes," in *Proc. 14th Int. Conf. Cryptol. Afr.*, in Lecture Notes in Computer Science, vol. 14064, Sousse, Tunisia. Cham, Switzerland: Springer, Jul. 2023, pp. 79–104, doi: 10.1007/978-3-031-37679-5_4.

[6] T. V. Carstens, E. Ebrahimi, G. N. Tabia, and D. Unruh, "Relationships between quantum IND-CPA notions," in *Proc. 19th Theory Cryptogr. Conf.*, in Lecture Notes in Computer Science, vol. 13042, Raleigh, NC, USA. Cham, Switzerland: Springer, Nov. 2021, pp. 240–272, doi: 10.1007/978-3-030-90459-3_9.

[7] G. Alagic, C. Majenz, A. Russell, and F. Song, "Quantum-access-secure message authentication via blind-unforgeability," in *Proc. 39th Annu. Int. Conf. Theory Appl. Cryptograph. Techn.*, in Lecture Notes in Computer Science, vol. 12107, Zagreb, Croatia. Cham, Switzerland: Springer, May 2020, pp. 788–817, doi: 10.1007/978-3-030-45727-3_27.

[8] D. Boneh and M. Zhandry, "Quantum-secure message authentication codes," in *Proc. 32nd Annu. Int. Conf. Theory Appl. Cryptograph. Techn.*, in Lecture Notes in Computer Science, vol. 7881, Athens, Greece. Cham, Switzerland: Springer, May 2013, pp. 592–608, doi: 10.1007/978-3-642-38348-9_35.

[9] X. Bonnetain, M. Naya-Plasencia, and A. Schrottenloher, "Quantum security analysis of AES," *IACR Trans. Symmetric Cryptol.*, vol. 2019, no. 2, pp. 55–93, Jun. 2019, doi: 10.46586/tosc.v2019.i2.55-93.

[10] A. Biryukov and D. Khovratovich, "Related-key cryptanalysis of the full AES-192 and AES-256," in *Proc. 15th Int. Conf. Theory Appl. Cryptol. Inf. Secur.*, in Lecture Notes in Computer Science, vol. 5912, Tokyo, Japan. Cham, Switzerland: Springer, Dec. 2009, pp. 1–18, doi: 10.1007/978-3-642-10366-7_1.

[11] S. Fluhrer, I. Mantin, and A. Shamir, "Weaknesses in the key scheduling algorithm of RC4," in *Proc. 8th Int. Workshop Sel. Areas in Cryptogr.*, in Lecture Notes in Computer Science, vol. 2259, Toronto, ON, Canada. Cham, Switzerland: Springer, Aug. 2001, pp. 1–24, doi: 10.1007/3-540-45537-x_1.

[12] M. Röetteler and R. Steinwandt, "A note on quantum related-key attacks," *Inf. Process. Lett.*, vol. 115, no. 1, pp. 40–44, Jan. 2015, doi: 10.1016/j.ipl.2014.08.009.

[13] L. Chen, "Recommendation for key derivation using pseudorandom functions," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. 800-108, 2024. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/108/r1/upd1/final

[14] M. Zhandry, "How to construct quantum random functions," *J. ACM*, vol. 68, no. 5, pp. 1–43, Oct. 2021, doi: 10.1145/3450745.

[15] A. Chailloux, M. Naya-Plasencia, and A. Schrottenloher, "An efficient quantum collision search algorithm and implications on symmetric cryptography," in *Proc. 23rd Int. Conf. Theory Appl. Cryptol. Inf. Secur.*, in Lecture Notes in Computer Science, vol. 10625, Hong Kong. Cham, Switzerland: Springer, Dec. 2017, pp. 211–240, doi: 10.1007/978-3-319-70697-9_8.

[16] S. Jaques and A. G. Rattew, "QRAM: A survey and critique," 2023, *arXiv:2305.10310*.

[17] A. Schrottenloher, "Improved quantum algorithms for the k-XOR problem," in *Proc. 28th Int. Conf. Sel. Areas Cryptogr.*, in Lecture Notes in Computer Science. Cham, Switzerland: Springer, Jan. 2022, pp. 311–331, doi: 10.1007/978-3-030-99277-4_15.

[18] A. Hosoyamada and Y. Sasaki, "Quantum collision attacks on reduced SHA-256 and SHA-512," in *Proc. 41st Annu. Int. Cryptol. Conf.*, in Lecture Notes in Computer Science, vol. 12825. Cham, Switzerland: Springer, Jan. 2021, pp. 616–646, doi: 10.1007/978-3-030-84242-0_22.

[19] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proc. 28th Annu. ACM Symp. Theory Comput.*, Philadelphia, PA, USA, May 1996, pp. 212–219, doi: 10.1145/237814.237866.

[20] L. K. Grover and J. Radhakrishnan, "Is partial quantum search of a database any easier?" in *Proc. 17th Annu. ACM Symp. Parallelism Algorithms Archit.*, Las Vegas, NV, USA, Jul. 2005, pp. 186–194, doi: 10.1145/1073970.1073997.

[21] C. Paar and J. Pelzl, *Understanding Cryptography: A Textbook for Students and Practitioners*. Cham, Switzerland: Springer, 2010, doi: 10.1007/978-3-642-04101-3.

[22] G. Brassard, P. Høyer, and A. Tapp, "Quantum cryptanalysis of hash and claw-free functions," *ACM SIGACT News*, vol. 28, no. 2, pp. 14–19, Jun. 1997, doi: 10.1145/261342.261346.

[23] D. R. Simon, "On the power of quantum computation," *SIAM J. Comput.*, vol. 26, no. 5, pp. 1474–1483, Oct. 1997, doi: 10.1137/s0097539796298637.

[24] H. Kuwakado and M. Morii, "Quantum distinguisher between the 3-round Feistel cipher and the random permutation," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2010, pp. 2682–2685.

[25] M. Kaplan, G. Leurent, A. Leverrier, and M. Naya-Plasencia, "Breaking symmetric cryptosystems using quantum period finding," in *Proc. 36th Annu. Int. Cryptol. Conf.*, in Lecture Notes in Computer Science, vol. 9815, Santa Barbara, CA, USA. Cham, Switzerland: Springer, Aug. 2016, pp. 207–237, doi: 10.1007/978-3-662-53008-5_8.

[26] X. Bonnetain, A. Hosoyamada, M. Naya-Plasencia, Y. Sasaki, and A. Schrottenloher, "Quantum attacks without superposition queries: The offline Simon's algorithm," in *Proc. 25th Int. Conf. Theory Appl. Cryptol. Inf. Secur.*, in Lecture Notes in Computer Science, vol. 11921, Kobe, Japan. Cham, Switzerland: Springer, Dec. 2019, pp. 552–583, doi: 10.1007/978-3-030-34578-5_20.

[27] G. Kuperberg, "A subexponential-time quantum algorithm for the dihedral hidden subgroup problem," *SIAM J. Comput.*, vol. 35, no. 1, pp. 170–188, Jan. 2005.

[28] X. Bonnetain and M. Naya-Plasencia, "Hidden shift quantum cryptanalysis and implications," in *Proc. 24th Int. Conf. Theory Appl. Cryptol. Inf. Secur.*, vol. 11272, Brisbane, QLD, Australia. Cham, Switzerland: Springer, Jan. 2018, pp. 560–592, doi: 10.1007/978-3-030-03326-2.

[29] D. Deutsch and R. Jozsa, "Rapid solution of problems by quantum computation," *Proc. Roy. Soc. London A, Math. Phys. Sci.*, vol. 439, no. 1907, pp. 553–558, Dec. 1992. doi: 10.1098/rspa.1992.0167.

[30] A. Kipnis and A. Shamir, "Cryptanalysis of the HFE public key cryptosystem by relinearization," in *Proc. 19th Annu. Int. Cryptol. Conf.*, in Lecture Notes in Computer Science, vol. 1666, Santa Barbara, CA, USA. Cham, Switzerland: Springer, Jan. 1999, pp. 19–30, doi: 10.1007/3-540-48405-1_2.

[31] D. Deutsch, "Quantum theory, the Church–Turing principle and the universal quantum computer," *Proc. Roy. Soc. London. A. Math. Phys. Sci.*, vol. 400, no. 1818, pp. 97–117, 1985, doi: 10.1098/rspa.1985.0070.

[32] X. Bonnetain, G. Leurent, M. Naya-Plasencia, and A. Schrottenloher, "Quantum linearization attacks," in *Proc. 27th Int. Conf. Theory Appl. Cryptol. Inf. Secur.*, in Lecture Notes in Computer Science, Singapore. Cham, Switzerland: Springer, Jan. 2021, pp. 422–452, doi: 10.1007/978-3-030-92062-3_15.

[33] M. Liskov, R. L. Rivest, and D. Wagner, "Tweakable block ciphers," in *Proc. 22nd Annu. Int. Cryptol. Conf.*, in Lecture Notes in Computer Science, Santa Barbara, CA, USA. Cham, Switzerland: Springer, Jan. 2002, pp. 31–46, doi: 10.1007/3-540-45708-9_3.

[34] R. Bhaumik, X. Bonnetain, A. Chailloux, G. Leurent, M. Naya-Plasencia, A. Schrottenloher, and Y. Seurin, "QCB: Efficient quantum-secure authenticated encryption," in *Proc. 27th Int. Conf. Theory Appl. Cryptol. Inf. Secur.*, in Lecture Notes in Computer Science, vol. 13090, Singapore. Cham, Switzerland: Springer, Jan. 2021, pp. 668–698, doi: 10.1007/978-3-030-92062-3_23.

[35] M. Bellare, R. Guérin, and P. Rogaway, "XOR MACs: New methods for message authentication using finite pseudorandom functions," in *Proc. 15th Annu. Int. Cryptol. Conf.*, in Lecture Notes in Computer Science, vol. 963, Santa Barbara, CA, USA. Cham, Switzerland: Springer, Jan. 1995, pp. 15–28, doi: 10.1007/3-540-44750-4_2.

[36] E. Bernstein and U. Vazirani, "Quantum complexity theory," in *Proc. 25th Annu. ACM Symp. Theory Comput.*, San Diego, CA, USA, May 1993, pp. 11–20, doi: 10.1145/167088.167097.

[37] H. Xie and L. Yang, "Using Bernstein–Vazirani algorithm to attack block ciphers," *Des., Codes Cryptogr.*, vol. 87, no. 5, pp. 1161–1182, May 2019, doi: 10.1007/s10623-018-0510-5.

[38] M. Luby and C. Rackoff, "How to construct pseudorandom permutations from pseudorandom functions," *SIAM J. Comput.*, vol. 17, no. 2, pp. 373–386, Apr. 1988, doi: 10.1137/0217022.

[39] B.-M. Zhou and Z. Yuan, "Quantum key-recovery attack on Feistel constructions: Bernstein–Vazirani meet Grover algorithm," *Quantum Inf. Process.*, vol. 20, no. 10, p. 330, Oct. 2021, doi: 10.1007/s11128-021-03256-0.

[40] K. Aoki, T. Ichikawa, M. Kanda, M. Matsui, S. Moriai, J. Nakajima, and T. Tokita, "Specification of Camellia—A 128-bit block cipher," Specification Version 2.0, 2001.

[41] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proc. 35th Annu. Symp. Found. Comput. Sci.*, Santa Fe, NM, USA, Nov. 1994, pp. 124–134, doi: 10.1109/SFCS.1994.365700.

[42] G. Leander and A. May, "Grover meets Simon—Quantumly attacking the FX-construction," in *Proc. 23rd Int. Conf. Theory Appl. Cryptol. Inf. Secur.*, in Lecture Notes in Computer Science, vol. 5, Hong Kong. Cham, Switzerland: Springer, Jan. 2017, pp. 161–178, doi: 10.1007/978-3-319-70697-9_6.

[43] D. Wagner, "The boomerang attack," in *Proc. 6th Int. Workshop Fast Softw. Encryption*, in Lecture Notes in Computer Science, vol. 1636, Rome, Italy. Cham, Switzerland: Springer, Jan. 1999, pp. 156–170, doi: 10.1007/3-540-48519-8_12.

[44] P. Frixons, M. Naya-Plasencia, and A. Schrottenloher, "Quantum boomerang attacks and some applications," in *Proc. Int. Conf. Select. Areas Cryptogr.*, in Lecture Notes in Computer Science, vol. 13203. Cham, Switzerland: Springer, Jan. 2022, pp. 332–352, doi: 10.1007/978-3-030-99277-4_16.

[45] M. Kaplan, G. Leurent, A. Leverrier, and M. Naya-Plasencia, "Quantum differential and linear cryptanalysis," *IACR Trans. Symmetric Cryptol.*, vol. 2016, no. 1, pp. 71–94, Dec. 2016, doi: 10.13154/tosc.v2016.i1.71-94.

[46] T. Gagliardoni, A. Hülsing, and C. Schaffner, "Semantic security and indistinguishability in the quantum world," in *Proc. Annu. Int. Cryptol. Conf.*, in Lecture Notes in Computer Science, vol. 9816, Santa Barbara, CA, USA. Cham, Switzerland: Springer, Jan. 2016, pp. 60–89, doi: 10.1007/978-3-662-53015-3_3.

[47] M. V. Anand, E. Ebrahimi, G. N. M. Tabia, and D. Unruh, "Post-quantum security of the CBC, CFB, OFB, CTR, and XTS modes of operation," in *Proc. Post-Quantum Cryptogr.*, in Lecture Notes in Computer Science, Fukuoka, Japan. Cham, Switzerland: Springer, Jan. 2016, pp. 44–63, doi: 10.1007/978-3-319-29360-8_4.

[48] Nat. Inst. Standards Technol. (Dec. 2016). *Post-Quantum Cryptography Standardization—Call for Proposals*. Accessed: Jun. 20, 2024. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf

[49] A. Biryukov and D. Wagner, "Slide attacks," in *Proc. Int. Workshop Fast Softw. Encryption*, in Lecture Notes in Computer Science, vol. 1636, Rome, Italy. Cham, Switzerland: Springer, Jan. 1999, pp. 245–259, doi: 10.1007/3-540-48519-8_18.

[50] S. Even and Y. Mansour, "A construction of a cipher from a single pseudorandom permutation," *J. Cryptol.*, vol. 10, no. 3, pp. 151–161, Jun. 1997, doi: 10.1007/s001459900025.

[51] O. Dunkelman, N. Keller, and A. Shamir, "Minimalism in cryptography: The Even–Mansour scheme revisited," in *Proc. 31st Annu. Int. Conf. Theory Appl. Cryptograph. Techn.*, in Lecture Notes in Computer Science, vol. 7237, Cambridge, U.K. Cham, Switzerland: Springer, Jan. 2012, pp. 336–354, doi: 10.1007/978-3-642-29011-4_21.

[52] G. Alagic, C. Bai, J. Katz, C. Majenz, and P. Struck, "Post-quantum security of tweakable Even–Mansour, and applications," in *Proc. 43rd Annu. Int. Conf. Theory Appl. Cryptograph. Techn.*, in Lecture Notes in Computer Science, vol. 14651, Zurich, Switzerland. Cham, Switzerland: Springer, Jan. 2024, pp. 310–338, doi: /10.1007/978-3-031-58716-0_11.

[53] J. Kilian and P. Rogaway, "How to protect DES against exhaustive key search (an analysis of DESX)," *J. Cryptol.*, vol. 14, no. 1, pp. 17–35, Jan. 2001, doi: 10.1007/s001450010015.

[54] X. Bonnetain and S. Jaques, "Quantum period finding against symmetric primitives in practice," *IACR Trans. Cryptograph. Hardw. Embedded Syst.*, vol. 2022, no. 1, pp. 1–27, Nov. 2021.

[55] "Security solutions for IoT," NXP Semiconductors, Bengaluru, Karnataka, Application Note AN12278, 2020. [Online]. Available: https://www.nxp.com/docs/en/application-note/AN12278.pdf

[56] A. Hosoyamada and Y. Sasaki, "Cryptanalysis against symmetric-key schemes with online classical queries and offline quantum computations," in *Proc. Cryptographers' Track RSA Conf.*, in Lecture Notes in Computer Science, vol. 10808, San Francisco, CA, USA. Cham, Switzerland: Springer, Jan. 2018, pp. 198–218, doi: 10.1007/978-3-319-76953-0_11.

[57] J. Borghoff, A. Canteaut, T. Güneysu, E. B. Kavun, M. Knezevic, L. R. Knudsen, G. Leander, V. Nikov, C. Paar, C. Rechberger, P. Rombouts, S. S. Thomsen, and T. Yalçin, "PRINCE—A low-latency block cipher for pervasive computing applications-extended abstract," in *Proc. 18th Int. Conf. Theory Appl. Cryptol. Inf. Secur.*, in Lecture Notes in Computer Science, vol. 7658, Beijing, China. Cham, Switzerland: Springer, 2012, pp. 208–225, doi: 10.1007/978-3-642-34961-4_14.

[58] D. Božilov, M. Eichlseder, M. Knežević, B. Lambin, G. Leander, T. Moos, V. Nikov, S. Rasoolzadeh, Y. Todo, and F. Wiemer, "PRINCEv2—More security for (almost) no overhead," in *Proc. SAC*, in Lecture Notes in Computer Science, vol. 12804. Cham, Switzerland: Springer, Jan. 2020, p. 1269.

[59] X. Bonnetain, "Quantum key-recovery on full AEZ," in *Proc. 24th Int. Conf. Sel. Areas Cryptogr.*, in Lecture Notes in Computer Science, vol. 10719, Ottawa, ON, Canada. Cham, Switzerland: Springer, Dec. 2017, pp. 394–406, doi: 10.1007/978-3-319-72565-9_20.

[60] Y. Oh, K. Jang, A. Baksi, and H. Seo, "Depth-optimized quantum circuits for ASCON: AEAD and HASH," *Mathematics*, vol. 12, no. 9, p. 1337, Apr. 2024. [Online]. Available: https://www.mdpi.com/2227-7390/12/9/1337

[61] K. Bhargavan and G. Leurent, "On the practical (in-)security of 64-bit block ciphers: Collision attacks on HTTP over TLS and OpenVPN," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Vienna, Austria, Oct. 2016, pp. 456–467, doi: 10.1145/2976749.2978423.

[62] V. Maram, D. Masny, S. Patranabis, and S. Raghuraman, "On the quantum security of OCB," *IACR Trans. Symmetric Cryptol.*, vol. 2022, no. 2, pp. 379–414, Jun. 2022, doi: 10.46586/tosc.v2022.i2.379-414.

[63] Eur. Union Agency for Cybersecurity (ENISA). (2014). *Algorithms, Key Size and Parameters Report*. [Online]. Available: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014

[64] T. Nemoz, Z. Amblard, and A. Dupin, "Characterizing the qIND-qCPA (in)security of the CBC, CFB, OFB and CTR modes of operation," in *Proc. 14th Int. Conf. Post-Quantum Cryptogr.*, in Lecture Notes in Computer Science, College Park, MD, USA. Cham, Switzerland: Springer, Jan. 2023, pp. 445–475, doi: 10.1007/978-3-031-40003-2_17.

[65] A. Hosoyamada and T. Iwata, "On tight quantum security of HMAC and NMAC in the quantum random Oracle model," in *Proc. 41st Annu. Int. Cryptol. Conf.*, in Lecture Notes in Computer Science, vol. 5. Cham, Switzerland: Springer, Jan. 2021, pp. 585–615, doi: 10.1007/978-3-030-84242-0_21.

[66] M. Jauch and V. Maram, "Quantum cryptanalysis of OTR and OPP: Attacks on confidentiality, and key-recovery," in *Proc. 30th Int. Conf. Sel. Areas Cryptogr.*, in Lecture Notes in Computer Science, Fredericton, NB, Canada. Cham, Switzerland: Springer, Jan. 2024, pp. 275–296, doi: 10.1007/978-3-031-53368-6_14.

[67] P. Rogaway and T. Shrimpton, "A provable-security treatment of the key-wrap problem," in *Proc. 25th Annu. Int. Conf. Theory Appl. Cryptograph. Techn.*, in Lecture Notes in Computer Science, vol. 4004, Saint Petersburg, Russia. Cham, Switzerland: Springer, Jan. 2006, pp. 373–390, doi: 10.1007/11761679_23.

[68] J. Leuther and S. Lucks, "QCB is blindly unforgeable," in *Proc. 4th Int. Conf. Codes, Cryptol., Inf. Secur.*, in Lecture Notes in Computer Science, vol. 13874, Rabat, Morocco. Cham, Switzerland: Springer, Jan. 2023, pp. 91–108, doi: 10.1007/978-3-031-33017-9_6.

[69] C. Janson and P. Struck, "Sponge-based authenticated encryption: Security against quantum attackers," in *Proc. 13th Int. Conf. Post-Quantum Cryptogr.*, in Lecture Notes in Computer Science, vol. 13512. Cham, Switzerland: Springer, Jan. 2022, pp. 230–259, doi: 10.1007/978-3-031-17234-2_12.

[70] H. Krawczyk, "Cryptographic extraction and key derivation: The HKDF scheme," in *Proc. 30th Annu. Cryptol. Conf.*, in Lecture Notes in Computer Science, Santa Barbara, CA, USA. Cham, Switzerland: Springer, Jan. 2010, pp. 631–648, doi: 10.1007/978-3-642-14623-7_34.

[71] N. Aviram, B. Dowling, I. Komargodski, K. G. Paterson, E. Ronen, and E. Yogev, "Practical (post-quantum) key combiners from one-wayness and applications to TLS," Cryptol. ePrint Arch., Tech. Paper 2022/065, 2022. [Online]. Available: https://eprint.iacr.org/2022/065

[72] M. Barbosa, D. Connolly, J. D. Duarte, A. Kaiser, P. Schwabe, K. Varner, and B. Westerbaan, "X-wing: The hybrid KEM you've been looking for," *IACR Cryptol. ePrint Arch.*, vol. 1, no. 1, pp. 1–22, 2024. [Online]. Available: https://cic.iacr.org/p/1/1/21

[73] M. Ounsworth, A. Wussler, and S. Kousidis. (Jul. 2023). *Combiner Function for Hybrid Key Encapsulation Mechanisms (Hybrid KEMs)*. Internet Eng. Task Force. [Online]. Available: https://datatracker.ietf.org/doc/draft-ounsworth-cfrg-kem-combiners/04/

[74] F. Giacon, F. Heuer, and B. Poettering, "KEM combiners," in *Proc. 21st IACR Int. Workshop Public Key Cryptogr.*, in Lecture Notes in Computer Science, vol. 10769, Rio de Janeiro, Brazil. Cham, Switzerland: Springer, Jan. 2018, pp. 190–218, doi: 10.1007/978-3-319-76578-5_7.

[75] D. Stebila, S. Fluhrer, and S. Gueron. (Sep. 2023). *Hybrid Key Exchange in TLS 1.3*. Internet Eng. Task Force. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-tls-hybrid-design/09/

[76] D. P. Martin, A. Montanaro, E. Oswald, and D. Shepherd, "Quantum key search with side channel advice," in *Proc. 24th Int. Conf. Sel. Areas Cryptogr.*, in Lecture Notes in Computer Science, vol. 10719, Ottawa, ON, Canada. Cham, Switzerland: Springer, Dec. 2017, pp. 407–422, doi: 10.1007/978-3-319-72565-9_21.

[77] A. Bogdanov, D. Khovratovich, and C. Rechberger, "Biclique cryptanalysis of the full AES," in *Proc. 17th Int. Conf. Theory Appl. Cryptol. Inf. Secur.*, in Lecture Notes in Computer Science, vol. 7073, Seoul, South Korea. Cham, Switzerland: Springer, Jan. 2011, pp. 344–371, doi: c10.1007/978-3-642-25385-0_19.
[78] C. Zalka, "Grover's quantum searching algorithm is optimal," *Phys. Rev. A*, vol. 60, no. 4, p. 2746, 1999.
[79] S. Jaques, M. Naehrig, M. Roetteler, and F. Virdia, "Implementing Grover oracles for quantum key search on AES and LowMC," in *Proc. 39th Annu. Int. Conf. Theory Appl. Cryptograph. Techn.*, in Lecture Notes in Computer Science, vol. 6, Zagreb, Croatia. Cham, Switzerland: Springer, Oct. 2019, pp. 280–310, doi: 10.1007/978-3-030-45724-2_10.
[80] M. Grassl, B. Langenberg, M. Roetteler, and R. Steinwandt, "Applying Grover's algorithm to AES: Quantum resource estimates," in *Proc. 7th Post-Quantum Cryptogr.*, in Lecture Notes in Computer Science, vol. 9606, Fukuoka, Japan. Cham, Switzerland: Springer, 2016, pp. 29–43, doi: 10.1007/978-3-319-29360-8_3.
[81] G. Leurent and C. Pernot, "New representations of the AES key schedule," in *Proc. 40th Annu. Int. Conf. Theory Appl. Cryptograph. Techn.*, in Lecture Notes in Computer Science, vol. 12696, Zagreb, Croatia. Cham, Switzerland: Springer, Jan. 2021, pp. 54–84, doi: 10.1007/978-3-030-77870-5_3.
[82] H. Demirci and A. A. Selçuk, "A meet-in-the-middle attack on 8-round AES," in *Proc. 15th Int. Workshop Fast Softw. Encryption*, in Lecture Notes in Computer Science, vol. 5086, Lausanne, Switzerland. Cham, Switzerland: Springer, Jul. 2008, pp. 116–126, doi: 10.1007/978-3-540-71039-4_7.
[83] A. Biryukov, O. Dunkelman, N. Keller, D. Khovratovich, and A. Shamir, "Key recovery attacks of practical complexity on AES-256 variants with up to 10 rounds," in *Proc. 29th Annu. Int. Conf. Theory Appl. Cryptograph. Techn.*, in Lecture Notes in Computer Science, vol. 6001, French Riviera, France. Cham, Switzerland: Springer, Jan. 2010, pp. 299–319, doi: 10.1007/978-3-642-13190-5_15.

S. E. BOOTSMA received the B.Sc. and M.Sc. degrees in mathematics from the University of Groningen, in 2023.

Since 2023, he has been a Researcher with TNO working on applied cryptography and quantum algorithms. His research interests include (applied) cryptography, quantum algorithms, and elliptic curves.

M. DE VRIES received the B.Sc. degree in artificial intelligence from the University of Groningen, in 2012, and the M.Sc. degree in computer science from the Technical University of Eindhoven, in 2017. Since 2013, she has been in various roles in information security. Since 2023, she has been a Researcher with TNO, with a focus on applied cryptography.