Quantum Security Evaluation of ASCON

Yujin Oh, Kyungbae Jang, and Hwajeong Seo

Hansung University, Seoul (02876), South Korea

oyj0922@gmail.com, starj1023@gmail.com, hwajeong84@gmail.com

Abstract. Grover's algorithm, which reduces the search complexity of symmetric-key ciphers and hash functions, poses a significant security challenge in cryptography. Recent research has focused on estimating Grover's search complexity and assessing post-quantum security. This paper analyzes a quantum circuit implementation of ASCON, including ASCON-AEAD, hash functions, and ASCON-80pq, in alignment with NIST's lightweight cryptography standardization efforts. We place particular emphasis on circuit depth, which directly impacts execution time, and analyze the quantum resource costs associated with Grover's algorithm-based key recovery and collision attacks. Additionally, we estimate the resources required to assess the quantum-resistant security strength of ASCON, based on security levels and the latest research trends.

Keywords: Post-quantum Security Level · ASCON · Grover's Algorithm · Quantum Collision Attack.

1 Introduction

The advantages of quantum computers can pose potential threats to existing encryption systems, raising the need to reassess the security of cryptography. One of the main challenges in addressing this threat is the development of post-quantum cryptography (PQC), which is being standardized by the National Institute of Standards and Technology (NIST). This need arises from Shor's algorithm [13], which efficiently solves factoring and discrete logarithm problems.

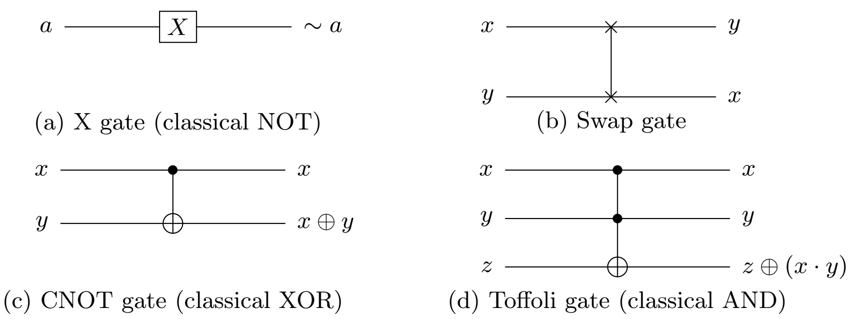
Another important quantum algorithm related to cryptography is Grover's algorithm [6]. Grover's algorithm accelerates data search, reducing the search complexity of symmetric key encryption. While Grover's algorithm can significantly reduce security strength, executing such attacks requires a large-scale quantum circuit. Quantum attacks suggest that the security of cryptographic algorithms can be assessed differently depending on the required quantum circuit size. This aspect is addressed in quantum encryption documents of NIST [10,11], which evaluate post-quantum security strength by considering the quantum cost of potential quantum attacks. NIST estimates the Grover attack costs for AES-128, AES-192, and AES-256, setting the post-quantum security strength, with these costs varying based on the efficiency of quantum circuit implementations for the target cryptographic algorithm.

In this paper, we evaluate the post-quantum security of quantum circuits for all ASCON schemes (ASCON AEAD, hash functions, and ASCON-80pq), which have been selected as NIST's lightweight cryptography standard. To assess ASCON's quantum security, we analyze the quantum circuit implementations required for Grover's algorithm-based key recovery and collision attacks. We estimate the quantum resources needed—including qubit count, gate complexity, and circuit depth—to evaluate the practical feasibility of these attacks, with a particular focus on circuit depth analysis. The depth of a quantum circuit directly impacts its execution time. While Grover's algorithm reduces search complexity by a square root, executing it still incurs substantial quantum circuit costs. As a result, key search using Grover's algorithm remains a time-consuming process, and NIST considers these factors when evaluating security. Consequently, minimizing the depth of symmetric key encryption circuits is an effective strategy for mitigating Grover attack costs. We adopt the ASCON quantum circuit approach from [12] and use it as a basis to estimate the cost of Grover's attack for all parameter. We then evaluate the post-quantum security strength of ASCON according to NIST standards. Compared to existing studies, our research provides a more detailed evaluation of all parameters by considering optimized quantum implementations and practical constraints.

The structure of this paper is as follows. Section 2 explains the background knowledge necessary for ASCON quantum circuits. Section 3 describes the ASCON quantum circuit implementation techniques. Section 4 presents the quantum resource costs. Section 5 estimates Grover attack costs for the ASCON quantum circuit and evaluates the quantum security strength. Finally, Section 6 concludes the paper and discusses future research directions.

2 Background

2.1 Basic Quantum Gates



(a) X gate (classical NOT)

(b) Swap gate

(c) CNOT gate (classical XOR)

(d) Toffoli gate (classical AND)

Fig. 1: Basic quantum gates

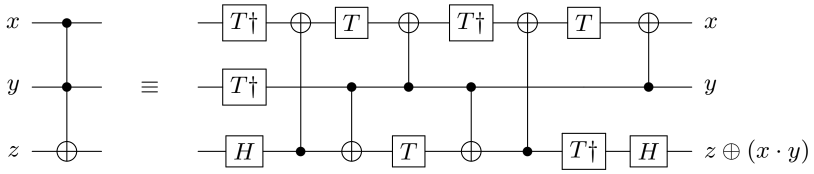
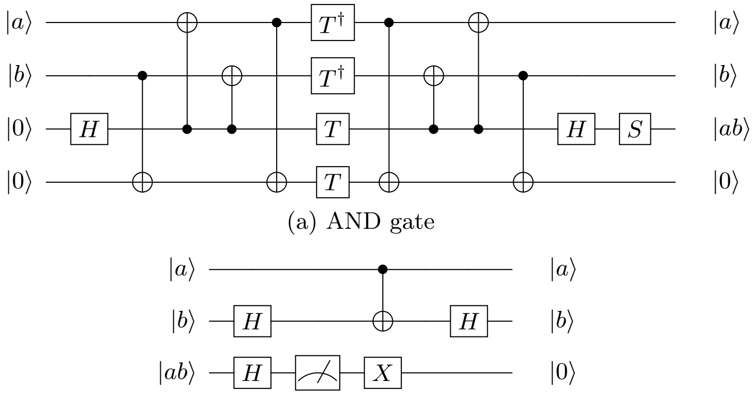


Fig. 2: Toffoli gate decomposition by [1]

This section outlines the quantum gates used in quantum circuit implementations. Figure 1 shows the commonly used gates in quantum circuits, which correspond to classical operations. Among these, the Toffoli gate is the most significant, as it can be decomposed into a combination of gates such as H, CNOT, and T gates. Figure 2 illustrates the decomposition of the Toffoli gate into 8 Clifford gates and 7 T gates, resulting in a T-depth of 4 and a total depth of 8 by [1].

Additionally, the AND gate method proposed by [8] functions similarly to the Toffoli gate but requires the target qubit to be in a clean state (i.e., $|0\rangle$). The AND gate consists of 11 Clifford gates, 4 T gates, and 1 ancilla qubit, achieving a T-depth of 1 and a total depth of 8, as shown in Figure 3a. The ancilla qubits used for the AND gates can be reused. Furthermore, the reverse operation of the AND gate, called AND†, is based on a Measurement gate and consists of 5 Clifford gates and 1 Measurement gate, as shown in Figure 3b. The total depth for this gate is 4, and the T-depth is 0.



(a) AND gate

(b) AND† gate

Fig. 3: Quantum AND and AND† gates

2.2 Grover algorithm

The Grover algorithm efficiently addresses cryptanalysis and search problems. For a cryptographic algorithm using a k-bit key, the search complexity on a classical computer is $O(2^k)$, whereas Grover's algorithm reduces the search complexity to $O(\sqrt{2^k})$. The Grover algorithm consists of three main steps. First, as shown in Equation 1, the Hadamard gate is applied to initialize the k-qubit key into a superposition state. This process ensures that all 2^k keys have equal amplitudes.

$$H^{\otimes k} \left|0\right\rangle^{\otimes k} = \left|\psi\right\rangle = \left(\frac{\left|0\right\rangle + \left|1\right\rangle}{\sqrt{2}}\right) = \frac{1}{2^{k/2}} \sum_{x=0}^{2^k-1} \left|x\right\rangle \tag{1}$$

The next step is the oracle. In the oracle, the cryptographic algorithm uses the superposition state of the key prepared in the previous step to encrypt a known plaintext in a quantum circuit. During this process, ciphertexts for all possible key values are generated. The generated ciphertext (which is actually one of the ciphertexts in the superposition state) is compared to the known ciphertext, and if they match (i.e., if $f(x) = 1$ in Equation 2), the sign of the key value is flipped (i.e., as shown in Equation 3, $(-1)^{f(x)}$). Finally, the implemented quantum circuit undergoes an inversion process for the next iteration, transforming the generated ciphertext back into the known plaintext.

$$f(x) = \begin{cases} 1 \text{ if } ENC_{key}(x) = \text{target output} \\ 0 \text{ if } ENC_{key}(x) \neq \text{target output} \end{cases} \tag{2}$$

$$U_f(\left|\psi\right\rangle \left|-\right\rangle) = \frac{1}{2^{k/2}} \sum_{x=0}^{2^k-1} (-1)^{f(x)} \left|x\right\rangle \left|-\right\rangle \tag{3}$$

After the oracle phase, the diffusion operator amplifies the amplitude of the solution key returned by the oracle. The oracle changes the sign of the solution key. The diffusion operator is easy to implement, and its complexity is negligible compared to the oracle, which is why it is generally ignored in the estimation of Grover attack costs. Grover's algorithm repeats the oracle and diffusion operations multiple times (approximately $\sqrt{2^k}$ times) to amplify the probability of the solution key. This process increases the likelihood of finding the correct key.

2.3 Quantum Collision Attack using Grover algorithm

Grover's search for an n-bit key in block ciphers or a pre-image of an n-bit hash output in hash functions is relatively straightforward, as quantum computing reduces the classical complexity of $O(n)$ to $O(\sqrt{n})$. However, when it comes to quantum collision searches for hash functions, the process is more complex and can be approached using various techniques.

Several quantum collision attack algorithms leveraging Grover's algorithm exist. Among these, the BHT algorithm [3] achieves a query complexity of $O(2^{n/3})$.

However, it requires a substantial quantum memory size of $O(2^{2n/3})$, which makes it impractical. Additionally, Bernstein highlighted in [2] that the BHT algorithm has certain controversial aspects.

Given these limitations, we adopt the CNS algorithm [4], which offers a query complexity of $O(2^{2n/5})$ while requiring significantly $O(2^{n/5})$ in classical memory. Notably, the CNS algorithm is also enable to parallelization, which can further reduce the search complexity. By running 2^s quantum instances in parallel, the search complexity for finding collisions is reduced to $O(2^{2n/5-3s/5})$, where s must satisfy $s \leq n/4$.

In [7], the authors used a parallelization strength of $s = n/6$ to estimate the quantum resource requirements for finding collisions in the SHA-2 and SHA-3 hash functions. Following their methodology, we adopt the same parallelization strength of $s = n/6$ to estimate the quantum resource requirements for finding collisions in the ASCON hash functions.

2.4 Description of ASCON

ASCON [5] is a lightweight cryptographic algorithm selected in the Lightweight Cryptography standardization of NIST. It consists of an authenticated encryption mode with associated data (AEAD), a hash function, and a variant of AEAD designed for resistance against quantum key search attacks, ASCON-80pq. ASCON offers two AEAD modes: ASCON-128 and ASCON-128a. The only difference between them is the number of rounds in the permutation function and the block size. On the other hand, ASCON-80pq shares the same parameters as ASCON-128 except for the key size, with ASCON-80pq using a 160-bit key. The encryption process of ASCON AEAD consists of the Initialization, Associated Data, Plaintext, and Finalization stages, as shown in Figure 4.

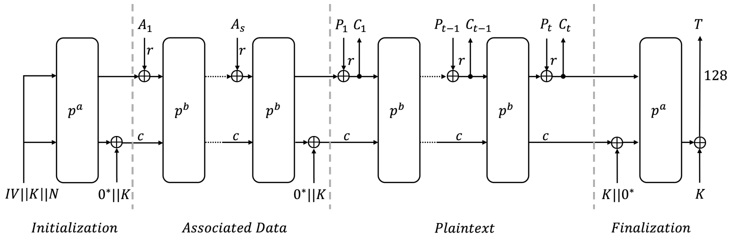


Fig. 4: Encryption of ASCON AEAD

For the hash function, ASCON provides two modes: ASCON-HASH and ASCON-XoF. ASCON-HASH produces a 256-bit hash value, while XoF supports arbitrary-length outputs. The encryption process for the ASCON hash function consists of the Initialization, Absorb Message, and Squeeze Tag stages, as illustrated in Figure 5.

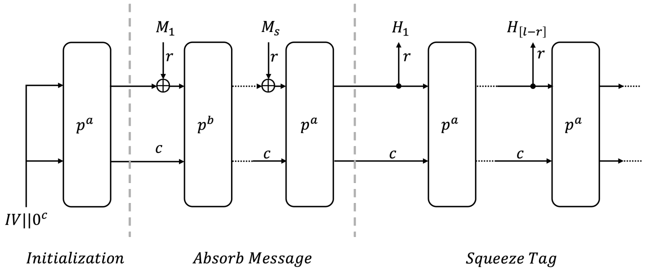


Fig. 5: Encryption of ASCON hash function

The main common components to all ASCON schemes consist of two 320-bit permutations, each configured with different round numbers. For operation, the 320 bits are divided into five 64-bit x_i (S $= x_0||x_1||x_2||x_3||x_4$, where x_0 is the most significant word and x_4 is the least significant word). The permutation function consists of constant addition, a substitution layer using a 5-bit S-box, and a linear layer using a 64-bit diffusion function.

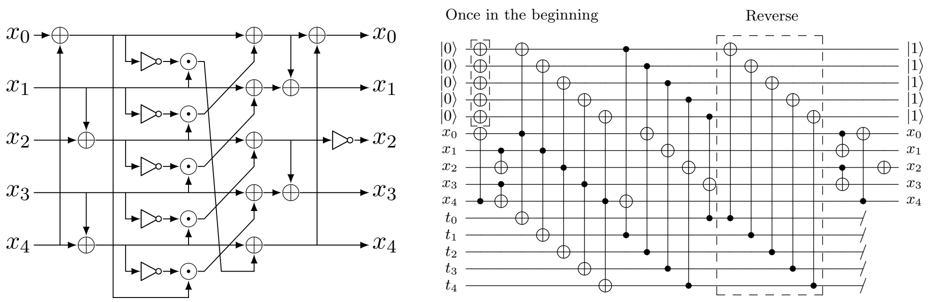
3 Quantum Circuit of ASCON

In this section, we describe our quantum circuit implementation of ASCON. Our primary focus is to strategically optimize the circuit depth, aiming to significantly enhance the efficiency of the Grover's key search. So, we adopt the existing implementation technique of [12], which achieves lowest depth of ASCON, and apply it to all parameters. The technique is as follows:

Substitution Layer with Toffoli Depth 1. As defined in Figure 6a, x_i values are interdependent and undergo both AND and XOR operations ($\odot$ and $\oplus$). This corresponds to the Toffoli gate in quantum, which impacts significantly to circuit depth. To address this, a parallelization method is employed to reduce the overall depth.

In the substitution layer, 64 instances of a 5-bit S-box are used. To process all S-boxes in parallel, two sets of 320 qubits ($= 5 \times 64$) are allocated, resulting in a total of 640 qubits ($= 2 \times 320$). Consequently, all Toffoli gates operate simultaneously, achieving a Toffoli depth of 1 (as shown in Figure 6b).

Qubit Reuse via Reverse operation. To reduce the number of qubits, 320 of them are reused through reverse operation. Since only the CNOT gate is used in the reverse operation, it does not significantly impact the depth. Also, during the reverse process, X gates are omitted, leaving the ancilla qubits in an inverted state (i.e., $|1\rangle$). From subsequent rounds, X gates can be skipped, reducing the total gate count.



(a) 5-bit S-box structure

(b) Quantum circuit of S-box in ASCON [12]

Fig. 6: Implementation of ASCON S-box

AND gate consideration. As described in Section 2.1, the AND gate method [8] can be used to the Toffoli gate. The ancilla qubits used for the AND gates can be reused. Therefore, for parallel processing of the AND gates in the substitution layer, only 320 (= 5 × 64) ancillar qubits are needed initially. However, no additional ancilla qubits need to be allocated, as output qubits (in a clean state) from the linear layer can be borrowed for the AND gates in the substitution layer.

Also, since the reverse operation of the Toffoli gate is not used in this implementation, the resource efficiency benefits provided by the AND† gate are not fully utilized. However, the AND† gate can be utilized in the reverse circuit of the Grover oracle.

Implementation of Linear Layer. The linear layer of ASCON is calculated as follows in Equation 4. To optimize the depth, the out-of-place method is used, with 320 ancilla qubits allocated to store the output. In the end, the implementation utilizes 640 qubits, 960 CNOT gates, and achieves a depth of 3.

$$\begin{aligned}
x_0 &\leftarrow \Sigma_0(x_0) = x_0 \oplus (x_0 \ggg 19) \oplus (x_0 \ggg 28),\\
x_1 &\leftarrow \Sigma_1(x_1) = x_1 \oplus (x_1 \ggg 61) \oplus (x_1 \ggg 39),\\
x_2 &\leftarrow \Sigma_2(x_2) = x_2 \oplus (x_2 \ggg 1) \oplus (x_2 \ggg 6),\\
x_3 &\leftarrow \Sigma_3(x_3) = x_3 \oplus (x_3 \ggg 10) \oplus (x_3 \ggg 17),\\
x_4 &\leftarrow \Sigma_4(x_4) = x_4 \oplus (x_4 \ggg 7) \oplus (x_4 \ggg 41).
\end{aligned} \tag{4}$$

4 Performance

In this section, we estimate the quantum circuit resource costs for all parameters of ASCON. ASCON-AEAD includes ASCON-128, ASCON-128a and ASCON-pq while the ASCON hash functions consist of ASCON-HASH with a 256-bit output and XoF (eXtendable Output Function) with customizable output lengths. For ASCON-AEAD, previous studies have only estimated the resources for ASCON-128. Building upon these approaches, we extend the resource estimation to ASCON-128a and ASCON-pq as well. In the case of ASCON hash function, we build upon the existing implementation [12] but extend the resource estimation beyond 256-bit to include XoF with 384-bit and 512-bit variants.

To implement the quantum circuits, we utilize the quantum programming framework ProjectQ. The accuracy of the implementation is verified using ClassicSimulator library, and the quantum resources are analyzed and evaluated using the ResourceCounter library.

Table 1 presents the resource costs required for implementing ASCON quantum circuits. Additionally, the quantum resources in Table 1 are based on decomposing Toffoli gates into Clifford + T gates (8 Clifford gates + 7 T gates, with a T-depth of 4 and a full depth of 8). For resource estimation, ASCON-AEAD assumes both associated data (AD) and plaintext (P) have a fixed size of 32 bits. For ASCON hash function resource estimation, the input message length is set to be the same as the output length.

Table 1: Quantum resources required for implementations of ASCON.

Cipher		Source	#CNOT	#1qCliff	#T	Toffoli depth (TD)	#Qubit (M)	Full depth (FD)	TD-M	FD-M	TD^2-M	FD^2-M
ASCON-AEAD	ASCON-128	Oh$^+$ [12]	127,200	21,563	67,200	30	20,064	513	$1.15 \cdot 2^{19}$	$1.23 \cdot 2^{23}$	$1.08 \cdot 2^{24}$	$1.23 \cdot 2^{32}$
	ASCON-128a	**Ours**	135,648	22,979	71,680	32	21,344	547	$1.30 \cdot 2^{19}$	$1.39 \cdot 2^{23}$	$1.30 \cdot 2^{24}$	$1.49 \cdot 2^{32}$
	ASCON-80pq	**Ours**	127,264	21,563	67,200	30	20,064	513	$1.15 \cdot 2^{19}$	$1.23 \cdot 2^{23}$	$1.08 \cdot 2^{24}$	$1.23 \cdot 2^{32}$
ASCON hash function	ASCON-HASH (256)	L$^+$ [9]	491,008	208,018	387,072	864	35,136	8,427	$1.81 \cdot 2^{24}$	$1.10 \cdot 2^{28}$	$1.53 \cdot 2^{34}$	$1.13 \cdot 2^{41}$
		Oh$^+$ [12]	406,016	68,435	215,040	96	62,592	1,641	$1.43 \cdot 2^{22}$	$1.53 \cdot 2^{26}$	$1.07 \cdot 2^{29}$	$1.23 \cdot 2^{37}$
	ASCON-XoF (384)	**Ours**	609,024	102,419	322,560	144	93,568	2,461	$1.61 \cdot 2^{23}$	$1.72 \cdot 2^{27}$	$1.81 \cdot 2^{30}$	$1.03 \cdot 2^{39}$
	ASCON-XoF (512)	**Ours**	812,032	136,402	430,080	192	124,544	3,281	$1.43 \cdot 2^{24}$	$1.52 \cdot 2^{28}$	$1.07 \cdot 2^{32}$	$1.22 \cdot 2^{40}$

5 Evaluation of ASCON

Using the estimated quantum resource costs, we estimate Grover's key search and collision search costs for ASCON and evaluate its post-quantum security.

Through the quantum attack cost analysis of cryptographic algorithms, the post-quantum security strength of the cryptosystem can be assessed. In this context, it is important to consider the post-quantum security levels set by NIST. Additionally, according to NIST, this paper estimates the $G-FD$ cost and also evaluates the trade-offs between qubit count and circuit depth by estimating the Td-M, FD-M, Td^2-M, and FD^2-M costs.

5.1 NIST Security Level

NIST provides post-quantum security levels for quantum attacks, and this paper references them during the implementation evaluation [10,11]. NIST defines security levels for the AES and SHA-2/3 families based on the complexity of Grover's key search and collision search, respectively, as shown in Table 2. Security levels 1, 3, and 5 correspond to the complexity of Grover's key search for

AES, while levels 2 and 4 correspond to the complexity of collision search for SHA-2/3. However, for levels 2 and 4, the quantum attack costs have not yet been defined, and only classical attack costs are provided.

Table 2: NIST Security Levels

Level	Cipher	Quantum Cost (Gate count × Full depth)
Level 1	AES-128	$2^{170} \rightarrow 2^{157}$
Level 2	SHA-256/SHA3-256	2^{146} (classical gates)
Level 3	AES-192	$2^{233} \rightarrow 2^{221}$
Level 4	SHA-384/SHA3-384	2^{210} (classical gates)
Level 5	AES-256	$2^{298} \rightarrow 2^{285}$

Grover's algorithm is one of the primary quantum attacks on symmetric-key cryptography, and NIST also considers it. The attack complexity at security levels 1, 3, and 5 depends on the Grover key search cost applied to AES-128, AES-192, and AES-256, respectively. This cost is determined by the total gate count and depth of the Grover key search circuit. NIST estimated the costs for levels 1, 3, and 5 as 2^{170}, 2^{233}, and 2^{298}, respectively, based on the AES quantum circuit implemented by Grassl. However, recent research has been focused on optimizing AES quantum circuits, and in particular, Jaques introduced a depth-optimized AES quantum circuit at Eurocrypt 2020 [8], which reduced the Grover key search cost for AES. As a result, NIST adjusted the Grover key search costs for the AES family based on this research, with the new costs being 2^{157}, 2^{221}, and 2^{285}, respectively.

For security levels 2 and 4, NIST has not yet defined the quantum attack costs for collision attacks on SHA-2 and SHA-3 hash functions. However, in [7], they proposed costs for collision attacks on SHA-2/3 hash functions at levels 2 and 4. Therefore, this paper compares the proposed security levels by Jang et al., as shown in Table 3.

Table 3: The security levels for quantum collision attacks defined by [7].

Level	Cipher	Quantum Cost (Gate count × Full depth)
Level 2	SHA-2/3 (256)	$2^{188}/2^{183}$
Level 4	SHA-2/3 (384)	$2^{266}/2^{260}$
Level 6 (Extension)	SHA-2/3 (512)	$2^{343}/2^{337}$

Additionally, it is important to consider the MAXDEPTH defined by NIST. MAXDEPTH represents the maximum circuit depth that can be executed on a quantum computer. NIST classifies the depth limit for quantum attacks (i.e., MAXDEPTH) within a certain range, such as $2^{40} < 2^{64} < 2^{96}$. This classification reflects the fact that if the circuit depth becomes too large, quantum attacks like Grover's algorithm may become practically infeasible. If the specified depth limit is exceeded, one might consider parallelizing the Grover search.

With the parallelization of Grover's algorithm, the trade-off metrics of the quantum circuit change, with the circuit depth metric being squared. In simple terms, the qubit count× circuit depth metric is replaced by the qubit count×the square of the circuit depth. In this paper, we denote the qubit count, total depth, Toffoli-depth, and T-depth as M, FD, TD, and Td, respectively. Additionally, for quantum circuit evaluation, we estimate FD-M, TD-M, Td-M and also estimate the modified trade-off metrics (FD^2-M, TD^2-M, Td^2-M) for Grover's parallelization.

5.2 Estimating the Grover's attack Costs for ASCON

To estimate the cost of a Grover attack on ASCON, we follow the methodology summarized in Section 2.2 and 2.3. In the oracle, the ASCON quantum circuit and its inverse circuit are executed sequentially. The first step constructs the encryption circuit, while the second step runs the encryption circuit in reverse to return to the pre-encryption state. Thus, the Grover's oracle costs for ASCON are 2 × Table 1, as shown in Table 4.

Furthermore, during this process, the AND gate can be utilized in the reverse circuit. According to the Grover oracle cost estimates summarized in Table 4, the use of AND gates can reduce quantum resource costs without increasing the number of qubits. Additionally, since most quantum resources are used to implement the target cipher in the quantum circuit, the overhead of the diffusion operator is negligible compared to the oracle. For this reason, many studies consider the cost of Grover search in terms of the repetitive cost of the oracle.

The Grover key search attack on ASCON-AEAD requires the sequential repetition of a large number of ASCON quantum circuits. To iteratively recover an k-bit key, the oracle and the diffusion operator set must be repeated $\lfloor \frac{\pi}{4}\sqrt{2^k} \rfloor$ times. For Grover collision attack, in [12], they employed the BHT algorithm. Hoewever, we adopt the CNS approach instead to estimate the collision attack cost for the ASCON hash function. The CNS algorithm has a complexity of $O(2^{2n/5})$. Although it has a higher complexity than the BHT algorithm, we adopt this approach as it does not require quantum memory. Additionally, we also use paralleization which can reduce the serch complexity to $O(2^{2n/5-3s/5})$ ($s \leq \frac{n}{4}$). According to Jang et al. [7], they set $s = \frac{n}{6}$ to define suitable criteria for NIST post-quantum security levels, and we follow that approach.

In summary, the Grover attack costs for ASCON-AEAD and ASCON hash functions are as follows: Table 4 × $\lfloor \frac{\pi}{4}\sqrt{2^k} \rfloor$ (for ASCON-AEAD) and Table 4 × $\lfloor 2^{(2n/5-3s/5)} \rfloor$ (for ASCON hash functions).

Table 4: Decomposed quantum resources for Grover's Oracle on ASCON.

Cipher		Source	#CNOT	#1qCliff	#T	#Measure	T-depth (Td)	#Qubit (M)	Full depth (FD)	Td-M	FD-M	Td^2-M	FD^2-M
ASCON-AEAD	ASCON-128	Oh+ [12]	254,400	43,126	134,440	0	240	20,065	1,026	$1.15 \cdot 2^{22}$	$1.23 \cdot 2^{24}$	$1.08 \cdot 2^{30}$	$1.23 \cdot 2^{34}$
		Oh+-AND [12]	225,600	71,926	38,400	9,600	**30**	20,065	**816**	$\mathbf{1.15 \cdot 2^{19}}$	$\mathbf{1.95 \cdot 2^{23}}$	$\mathbf{1.08 \cdot 2^{24}}$	$\mathbf{1.56 \cdot 2^{33}}$
	ASCON-128a	**Ours**	271,296	45,958	143,360	0	256	21,345	1,094	$1.30 \cdot 2^{22}$	$1.40 \cdot 2^{24}$	$1.30 \cdot 2^{30}$	$1.49 \cdot 2^{34}$
		Ours-AND	240,576	76,678	40,960	10,240	**32**	21,345	**872**	$\mathbf{1.30 \cdot 2^{19}}$	$\mathbf{1.11 \cdot 2^{24}}$	$\mathbf{1.30 \cdot 2^{24}}$	$\mathbf{1.89 \cdot 2^{33}}$
	ASCON-80pq	**Ours**	254,528	43,126	134,440	0	240	20,065	1,026	$1.15 \cdot 2^{22}$	$1.23 \cdot 2^{24}$	$1.08 \cdot 2^{30}$	$1.23 \cdot 2^{34}$
		Ours-AND	225,728	71,926	38,400	9,600	**30**	20,065	**816**	$\mathbf{1.15 \cdot 2^{19}}$	$\mathbf{1.95 \cdot 2^{23}}$	$\mathbf{1.08 \cdot 2^{24}}$	$\mathbf{1.56 \cdot 2^{33}}$
ASCON hash function	ASCON-HASH	L+ [9]	982,016	416,036	774,144	0	6,912	35,137	16,854	$1.81 \cdot 2^{25}$	$1.10 \cdot 2^{29}$	$1.53 \cdot 2^{36}$	$1.13 \cdot 2^{43}$
		Oh+ [12]	812,032	136,870	430,080	0	768	62,593	3,282	$1.43 \cdot 2^{25}$	$1.53 \cdot 2^{27}$	$1.07 \cdot 2^{35}$	$1.23 \cdot 2^{39}$
		Oh+-AND[12]	719,872	229,030	122,880	30,720	**96**	62,593	**2,608**	$\mathbf{1.43 \cdot 2^{22}}$	$\mathbf{1.22 \cdot 2^{27}}$	$\mathbf{1.07 \cdot 2^{29}}$	$\mathbf{1.55 \cdot 2^{38}}$
	ASCON-XoF (384)	**Ours**	1,218,048	204,838	645,120	0	1,152	93,569	4,922	$1.61 \cdot 2^{26}$	$1.72 \cdot 2^{28}$	$1.81 \cdot 2^{36}$	$1.03 \cdot 2^{41}$
		Ours-AND	1,079,808	343,076	184,320	46,0880	**144**	93,569	**3,904**	$\mathbf{1.61 \cdot 2^{23}}$	$\mathbf{1.36 \cdot 2^{28}}$	$\mathbf{1.81 \cdot 2^{30}}$	$\mathbf{1.29 \cdot 2^{40}}$
	ASCON-XoF (512)	**Ours**	1,624,064	272,804	860,160	0	1,536	124,545	6,562	$1.43 \cdot 2^{27}$	$1.52 \cdot 2^{29}$	$1.07 \cdot 2^{38}$	$1.22 \cdot 2^{42}$
		Ours-AND	1,439,744	457,124	245,760	61,440	**192**	124,545	**5,200**	$\mathbf{1.43 \cdot 2^{24}}$	$\mathbf{1.21 \cdot 2^{29}}$	$\mathbf{1.07 \cdot 2^{32}}$	$\mathbf{1.53 \cdot 2^{41}}$

5.3 Comparision with security level

Tables 5 shows the attack costs of ASCON-AEAD. According to the information provided in Table 5, the most optimized quantum attack costs for ASCON-128 and ASCON-128a are 1.26×2^{155} and 1.47×2^{155}, respectively. Therefore, ASCON-128 and ASCON-128a do not achieve post-quantum security level 1, corresponding to the AES-128 (2^{157}) attack cost. In case of ASCON-80pq, it was specifically designed to possess quantum resistance, meaning it was developed with the goal of maintaining security even against attacks carried out using quantum computers. Considering this intended purpose, it is not surprising that the quantum attack cost for ASCON-80pq is calculated to be 1.29×2^{187}, which is a high cost. This cost satisfies the security standards set by NIST for Level 1, and its achievement is an expected outcome.

We apply the CNS algorithm and reduce search complexity through parallelization. In [9], collision algorithm is not applied, so we directly implement CNS in their implementation for comparison. When compared, our results outperform in all metrics except for qubits. Additionally, [12] applies the BHT algorithm. While the results seem superior in the trade-off metric, as mentioned in Section 2.3, there are limitations.

NIST only provides classical costs for SHA2/3-256 and SHA2/3-384, related to levels 2 and 4, and does not provide quantum costs. Thus, the quantum attack costs at levels 2, 4, and 6, as proposed by [7] are used. The quantum collision attack costs for ASCON-HASH (256 bits) and ASCON-XoF (384, 512 bits) are 1.25×2^{184}, 1.19×2^{262}, and 1.89×2^{339}, respectively (as defined in Table 6). When compared to the attack costs for levels 2, 4, and 6 defined by Jang et al. as $2^{188/183}$, $2^{266/260}$, and $2^{343/337}$, the ASCON hash functions satisfy the attack costs associated with SHA3.

6 Conclusion

This paper presents an evaluation of the post-quantum security of the ASCON-AEAD, ASCON hash functions and ASCON-pq. We build upon the approach from [12], applying it to all parameters and estimate the costs associated with key search and quantum collision attacks leveraging Grover's algorithm. First,

Table 5: Costs of the Grover's key search for ASCON-AEAD.

Cipher		Source	#Gate (G)	Full depth (FD)	T-depth (Td)	#Qubit (M)	G-FD	FD-M	Td-M	FD^2-M	Td^2-M
ASCON-AEAD	ASCON-128	Oh+ [12]	$1.31 \cdot 2^{82}$	$1.57 \cdot 2^{73}$	$1.47 \cdot 2^{71}$	$1.22 \cdot 2^{14}$	$1.03 \cdot 2^{156}$	$1.92 \cdot 2^{87}$	$1.79 \cdot 2^{85}$	$1.50 \cdot 2^{161}$	$1.32 \cdot 2^{157}$
		Oh+-AND [12]	$1.01 \cdot 2^{82}$	$1.25 \cdot 2^{73}$	$1.44 \cdot 2^{68}$	$1.22 \cdot 2^{14}$	$1.26 \cdot 2^{155}$	$1.53 \cdot 2^{87}$	$1.76 \cdot 2^{82}$	$1.90 \cdot 2^{160}$	$1.27 \cdot 2^{151}$
	ASCON-128a	**Ours**	$1.39 \cdot 2^{82}$	$1.68 \cdot 2^{73}$	$1.57 \cdot 2^{71}$	$1.30 \cdot 2^{14}$	$\mathbf{1.17 \cdot 2^{156}}$	$1.10 \cdot 2^{88}$	$1.02 \cdot 2^{86}$	$1.83 \cdot 2^{161}$	$1.60 \cdot 2^{157}$
		Ours-AND	$1.10 \cdot 2^{82}$	$1.34 \cdot 2^{73}$	$1.56 \cdot 2^{68}$	$1.30 \cdot 2^{14}$	$\mathbf{1.47 \cdot 2^{155}}$	$1.74 \cdot 2^{87}$	$1.01 \cdot 2^{83}$	$1.17 \cdot 2^{161}$	$1.58 \cdot 2^{151}$
	ASCON-80pq	**Ours**	$1.29 \cdot 2^{98}$	$1.57 \cdot 2^{89}$	$1.47 \cdot 2^{87}$	$1.22 \cdot 2^{14}$	$\mathbf{1.02 \cdot 2^{188}}$	$1.92 \cdot 2^{103}$	$1.79 \cdot 2^{101}$	$1.50 \cdot 2^{193}$	$1.32 \cdot 2^{189}$
		Ours-AND	$1.04 \cdot 2^{98}$	$1.25 \cdot 2^{89}$	$1.44 \cdot 2^{84}$	$1.22 \cdot 2^{14}$	$\mathbf{1.29 \cdot 2^{187}}$	$1.53 \cdot 2^{103}$	$1.76 \cdot 2^{101}$	$1.91 \cdot 2^{192}$	$1.27 \cdot 2^{189}$

Table 6: Costs of the Grover's collision search for ASCON hash function.

Cipher		Source	method	#Gate (G)	Full depth (FD)	T-depth (Td)	#Qubit (M)	G-FD	FD-M	Td-M	FD^2-M	Td^2-M
ASCON hash function	ASCON-HASH	L+ [9]	**CNS**	$1.42 \cdot 2^{97}$	$1.40 \cdot 2^{90}$	$1.15 \cdot 2^{89}$	$1.70 \cdot 2^{57}$	$1.99 \cdot 2^{187}$	$1.19 \cdot 2^{148}$	$1.96 \cdot 2^{146}$	$1.68 \cdot 2^{238}$	$1.13 \cdot 2^{236}$
		Oh+ [12]	BHT	$1.30 \cdot 2^{105}$	$1.58 \cdot 2^{96}$	$1.48 \cdot 2^{94}$	$1.91 \cdot 2^{15}$	$1.03 \cdot 2^{202}$	$1.51 \cdot 2^{112}$	$1.41 \cdot 2^{110}$	$1.20 \cdot 2^{209}$	$1.05 \cdot 2^{205}$
		Oh+-AND [12]	BHT	$1.04 \cdot 2^{105}$	$1.25 \cdot 2^{96}$	$1.47 \cdot 2^{91}$	$1.91 \cdot 2^{15}$	$1.31 \cdot 2^{201}$	$1.20 \cdot 2^{112}$	$1.41 \cdot 2^{107}$	$1.51 \cdot 2^{208}$	$1.04 \cdot 2^{199}$
		Ours	**CNS**	$1.80 \cdot 2^{96}$	$1.09 \cdot 2^{88}$	$1.51 \cdot 2^{86}$	$1.51 \cdot 2^{58}$	$\mathbf{1.96 \cdot 2^{184}}$	$1.66 \cdot 2^{146}$	$1.55 \cdot 2^{144}$	$1.81 \cdot 2^{234}$	$1.59 \cdot 2^{230}$
		Ours-AND	**CNS**	$1.44 \cdot 2^{96}$	$1.74 \cdot 2^{87}$	$1.02 \cdot 2^{83}$	$1.51 \cdot 2^{58}$	$\mathbf{1.25 \cdot 2^{184}}$	$1.25 \cdot 2^{146}$	$1.54 \cdot 2^{141}$	$1.14 \cdot 2^{234}$	$1.57 \cdot 2^{224}$
	ASCON-XoF (384)	**Ours**	**CNS**	$1.78 \cdot 2^{135}$	$1.08 \cdot 2^{127}$	$1.01 \cdot 2^{125}$	$1.42 \cdot 2^{80}$	$\mathbf{1.92 \cdot 2^{262}}$	$1.54 \cdot 2^{207}$	$1.44 \cdot 2^{205}$	$1.67 \cdot 2^{334}$	$1.46 \cdot 2^{330}$
		Ours-AND	**CNS**	$1.42 \cdot 2^{135}$	$1.67 \cdot 2^{126}$	$1.01 \cdot 2^{122}$	$1.42 \cdot 2^{80}$	$\mathbf{1.19 \cdot 2^{262}}$	$1.19 \cdot 2^{207}$	$1.44 \cdot 2^{202}$	$1.00 \cdot 2^{334}$	$1.46 \cdot 2^{324}$
	ASCON-XoF(512)	**Ours**	**CNS**	$1.57 \cdot 2^{174}$	$1.90 \cdot 2^{165}$	$1.78 \cdot 2^{163}$	$1.19 \cdot 2^{102}$	$\mathbf{1.49 \cdot 2^{340}}$	$1.14 \cdot 2^{268}$	$1.06 \cdot 2^{266}$	$1.08 \cdot 2^{434}$	$1.90 \cdot 2^{429}$
		Ours-AND	**CNS**	$1.25 \cdot 2^{174}$	$1.51 \cdot 2^{165}$	$1.77 \cdot 2^{160}$	$1.19 \cdot 2^{102}$	$\mathbf{1.89 \cdot 2^{339}}$	$1.80 \cdot 2^{267}$	$1.06 \cdot 2^{263}$	$1.36 \cdot 2^{433}$	$1.88 \cdot 2^{423}$

when considering MAXDEPTH, key metrics related to circuit depth such as Toffoli-depth, T-depth, and Full depth, and Full depth are critical in assessing quantum circuit performance. In this context, we find that the depth-optimized implementation provides optimal performance across these metrics.

Our analysis reveals that the quantum circuits for ASCON-AEAD (ASCON-128 and ASCON-128a) do not achieve post-quantum security level 1. Therefore, to counter potential quantum computer attacks, the use of ASCON-80pq is recommended. Furthermore, when compared to the quantum collision attack costs defined by [7], the ASCON hash function meets the attack cost requirements similar to those of SHA3. The results offer valuable insights into ASCON's security in a post-quantum environment and contribute to the discussion on the future of lightweight cryptographic standards in the quantum era.

References

1. Amy, M., Maslov, D., Mosca, M., Roetteler, M., Roetteler, M.: A meet-in-the-middle algorithm for fast synthesis of depth-optimal quantum circuits. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems **32**(6), 818–830 (Jun 2013). https://doi.org/10.1109/tcad.2013.2244643, http://dx.doi.org/10.1109/TCAD.2013.2244643 3
2. Bernstein, D.J.: Cost analysis of hash collisions: Will quantum computers make sharcs obsolete. SHARCS **9**, 105 (2009) 5
3. Brassard, G., Hoyer, P., Tapp, A.: Quantum algorithm for the collision problem. arXiv preprint quant-ph/9705002 (1997) 4
4. Chailloux, A., Naya-Plasencia, M., Schrottenloher, A.: An efficient quantum collision search algorithm and implications on symmetric cryptography. In: Advances in Cryptology–ASIACRYPT 2017: 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017, Proceedings, Part II 23. pp. 211–240. Springer (2017) 5

5. Dobraunig, C., Eichlseder, M., Mendel, F., Schläffer, M.: ASCON v1.2. Submission to NIST (2019), https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/round-2/spec-doc-rnd2/ascon-spec-round2.pdf 5
6. Grover, L.K.: A fast quantum mechanical algorithm for database search. In: Proceedings of the twenty-eighth annual ACM symposium on Theory of computing. pp. 212–219 (1996) 1
7. Jang, K., Lim, S., Oh, Y., Kim, H., Baksi, A., Chakraborty, S., Seo, H.: Quantum implementation and analysis of SHA-2 and SHA-3. Cryptology ePrint Archive, Paper 2024/513 (2024), https://eprint.iacr.org/2024/513, https://eprint.iacr.org/2024/513 5, 9, 10, 11, 12
8. Jaques, S., Naehrig, M., Roetteler, M., Virdia, F.: Implementing grover oracles for quantum key search on AES and LowMC. In: Canteaut, A., Ishai, Y. (eds.) Advances in Cryptology - EUROCRYPT 2020 - 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10-14, 2020, Proceedings, Part II. Lecture Notes in Computer Science, vol. 12106, pp. 280–310. Springer (2020). https://doi.org/10.1007/978-3-030-45724-2_10, https://doi.org/10.1007/978-3-030-45724-2_10 3, 7, 9
9. Lee, W.K., Jang, K., Song, G., Kim, H., Hwang, S.O., Seo, H.: Efficient implementation of lightweight hash functions on GPU and quantum computers for iot applications. IEEE Access **10**, 59661–59674 (2022) 8, 11, 12
10. NIST.: Submission requirements and evaluation criteria for the post-quantum cryptography standardization process (2016), https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf 1, 8
11. NIST.: Call for additional digital signature schemes for the post-quantum cryptography standardization process (2022), https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/call-for-proposals-dig-sig-sept-2022.pdf 1, 8
12. Oh, Y., Jang, K., Baksi, A., Seo, H.: Depth-optimized quantum circuits for ASCON: AEAD and HASH. Mathematics **12**(9), 1337 (2024) 2, 6, 7, 8, 10, 11, 12
13. Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM review **41**(2), 303–332 (1999) 1