Provable and Practical: Establishing Post-Quantum Security Bounds for Ascon

Suprita TALNIKAR[1,2] Anandarup ROY[1,3] Kouichi SAKURAI[1]

Abstract: The selection of Ascon as the winner of the NIST Lightweight Cryptography (LWC) standardisation process positions it for long-term deployment in constrained environments. This report undertakes a comprehensive comparative analysis of two complementary pillars of post-quantum security evaluation as applied to the Ascon family of algorithms: concrete resource estimation and theoretical provable security. By synthesising the "bottom-up" circuit costing analysis of Oh et al. with the "top-down" formal proofs of Lang et al., we establish a robust "security bracket" for each Ascon variant. Our findings confirm that while Ascon-128/128a offer approximately 64 bits of post-quantum security, falling short of NIST's Level 1, the Ascon-80pq variant provides a robust 80 bits of security, making it a suitable choice for new post-quantum systems. The analysis also reveals critical flaws in proposed large-key variants, highlighting that for sponge-based schemes, capacity is a co-equal driver of post-quantum security with key size. We conclude with strategic recommendations for implementers, standards bodies, and future cryptographic research.

Keywords: Post-Quantum Security, Ascon, Semi-Classical O2H, Q2 Attack

1. Introduction

The selection of Ascon as the winner of the National Institute of Standards and Technology (NIST) Lightweight Cryptography (LWC) standardisation process marks a significant milestone in symmetric cryptography [1], [2]. The multi-year public competition, which began with 57 candidates and was narrowed to 10 finalists, concluded with Ascon being chosen as a "good all-around choice" for its security, performance, and flexibility in constrained environments [1]. Designed for long-term deployment in the Internet of Things (IoT), embedded systems, and other resource-limited devices, Ascon is poised for widespread adoption [3], [4].

This long-term horizon, however, necessitates a rigorous evaluation of its security posture not just against contemporary classical computers, but against the looming threat of large-scale, fault-tolerant quantum computers. The advent of quantum computing introduces fundamentally new attack vectors against established cryptographic systems. While much of the public focus has been on Shor's algorithm, which catastrophically breaks public-key cryptography, Grover's algorithm presents a more subtle but equally significant threat [5]. Grover's search algorithm offers a quadratic speedup for unstructured search problems, effectively reducing the security of a cipher with a k-bit key from 2^k classical operations to approximately $2^{k/2}$ quantum operations [6]. This reduction necessitates a complete reassessment of key lengths and security levels for algorithms intended for use in a post-quantum world. Consequently, understanding the precise cost and practical feasibility of Grover-based attacks against Ascon is not an academic exercise but a critical requirement for ensuring the longevity and trustworthiness of this new standard [7].

2. Foundations of Analysis: Costing Circuits vs. Proving Bounds

To appreciate the nuances of the comparative analysis, it is essential to first understand the distinct technical foundations upon which each paper is built. This section deconstructs the core methodologies, key metrics, and central theoretical tools employed by Oh et al. [8] and Lang et al. [7], respectively.

2.1 The Concrete Costing Approach

The work of Oh et al. is rooted in the practicalities of quantum computation [8]. Its primary goal is not to prove an abstract security level but to estimate the tangible quantum resources required to mount a successful key recovery or collision attack against all variants of Ascon. This approach is driven by the understanding that the theoretical speedup of Grover's algorithm is only one part of the story; the true threat is determined by the cost and feasibility of building and running the quantum circuit that implements the attack [5].

[1] Department of Advanced Informatics, Kyushu University, Fukuoka, Japan
[2] Applied Statistics Unit, Indian Statistical Institute, Kolkata, India
[3] Dr. ROY is supported by the National Institute of Information and Communications Technology(NICT), Japan, under the NICT International Invitational Program.

2.1.1 Primary Goal: Practical Feasibility and Depth Optimisation

A central theme of the Oh et al. paper is the critical importance of *circuit depth* [8]. In a quantum computer, qubits are fragile and susceptible to decoherence—the loss of their quantum state due to interaction with the environment. The longer a computation runs (i.e., the deeper the circuit), the more likely it is that decoherence will corrupt the result. This physical limitation is captured by the NIST concept of `MAXDEPTH`, which posits a maximum circuit depth (e.g., within ranges like 2^{40}, 2^{64}, or 2^{96}) that a quantum computer can execute reliably [5]. An attack, no matter how theoretically efficient in terms of query count, becomes practically infeasible if its required circuit depth exceeds this threshold. Therefore, the paper's focus is not just on implementing Ascon, but on implementing it with the lowest possible depth, as this directly corresponds to the most threatening version of a quantum attack. Minimising depth is presented as the most effective strategy for an attacker aiming to reduce the cost of a Grover-based attack [8]. This reframes the optimisation problem: for practical quantum attacks, circuit depth is arguably a more critical target than qubit count. A high oracle depth makes a sequential attack infeasible, forcing an adversary into costly parallelisation schemes where the overall cost scales with the square of the oracle depth. This makes minimising depth the single most effective strategy for a quantum attacker and thus the most important metric for a defender to analyse.

2.1.2 Quantum Circuit Implementation Strategy

To achieve its goal of a low-depth implementation, the paper adopts and extends a set of optimisation techniques, applying them across the full suite of Ascon parameters [8]. The strategies target the most computationally intensive layers of the Ascon permutation:

- **Parallel S-box Implementation:** The Ascon substitution layer applies 64 instances of a 5-bit S-box in parallel. The S-box logic involves both XOR and AND operations. In a quantum circuit, the AND operation is typically implemented using a Toffoli gate, a major contributor to circuit depth. To minimise this, the paper employs a space-for-time tradeoff. It allocates two sets of 320 qubits, allowing all 64 S-boxes to be computed simultaneously. This parallelisation reduces the Toffoli depth of the entire substitution layer to just 1, a significant optimisation that comes at the cost of an increased qubit count [8].
- **Out-of-Place Linear Layer:** The linear layer involves a series of bitwise rotations and XORs. To optimise the depth of this layer, an "out-of-place" computation method is used, which involves allocating an additional 320 ancilla qubits to store the output. This again trades qubit resources for a reduction in depth, achieving a very low depth of 3 for the entire linear layer computation [8].
- **Toffoli and AND Gate Decomposition:** The choice of how to implement the logical AND operation is critical. The standard Toffoli gate can be decomposed into a sequence of more fundamental Clifford and T gates, resulting in a T-depth of 4 and a full depth of 8. An alternative, the "AND gate" proposed by Jaques et al. [5], offers a superior T-depth of just 1. However, this gate requires its target qubit to be in a "clean" (zero) state. The Oh et al. paper notes that while this makes it less useful for the forward encryption circuit, it is an ideal optimisation for the reverse (uncomputation) circuit within the Grover oracle, as the ancilla qubits can be prepared in a clean state. This use of the AND gate is a subtle but important optimisation to reduce the overall oracle cost [8].

2.1.3 Key Metrics for Cost Analysis

The output of this concrete analysis is a detailed accounting of quantum resources. The key metrics are [5], [8]:

- **Physical Resources (Qubits, M):** The total number of qubits required, measuring the *size* of the quantum computer.
- **Gate Counts (CNOT, T-gate):** The total number of each gate type. The T-gate count is particularly important due to its high cost in fault-tolerant quantum error correction.
- **Circuit Depth (Td, TD, FD):** Measures of the circuit's execution time, including T-depth (Td), Toffoli-depth (TD), and Full Depth (FD).
- **Composite Metrics:** Single-figure estimates of attack cost, such as Gate count × Full depth (G-FD), and trade-off metrics like FD-M. For parallelised attacks, the dependence on depth becomes quadratic, leading to metrics like $FD^2 - M$.

2.2 The Provable Security Approach

In contrast to the "bottom-up" approach, the work of Lang et al. takes a "top-down" approach grounded in formal mathematical proof [7]. The goal is to establish a security guarantee for the Ascon authenticated encryption (AE) mode against a broad, generic class of quantum adversaries.

2.2.1 The Q1 Security Model

The analysis is situated in the *Q1 security model*, which captures a realistic near-future scenario where cryptographic operations on user devices are classical, but a powerful adversary possesses a quantum computer. In this model, the adversary has:

- **Classical access** to the full cryptographic construction (e.g., making classical encryption/decryption queries to Ascon AEAD).
- **Quantum access** to the underlying primitive (e.g., querying the unkeyed 320-bit permutation P and its inverse P^{-1} in superposition).

This is the standard model for assessing the post-quantum security of symmetric-key constructions [9], [10].

2.2.2 The Semi-Classical O2H Lemma

The central mathematical tool used by Lang et al. is the *semi-classical One-way to Hiding (O2H) lemma*, introduced by Ambainis, Hamburg, and Unruh [10]. The O2H

lemma is a powerful technique that allows a proof to "reprogram" a random oracle (in this case, the random permutation P) on a small set of inputs and then bound the probability that a quantum adversary can detect this change. The lemma considers two random functions, G and H, identical everywhere except on a small, randomly chosen *puncture set*, S. It states that the adversary's advantage in distinguishing G from H is bounded by a function of the adversary's query depth and the probability of "finding" an element in the puncture set.

2.2.3 Game-Based Proof Structure

The security proof uses a sequence of "games," a standard cryptographic technique. Starting from the real world (Game 0), it transitions through slightly altered intermediate games to an ideal world (Game 4), where the adversary interacts with a perfect random oracle. By summing the small probability gaps between each game, the paper bounds the adversary's advantage in distinguishing real Ascon from an ideal oracle.

2.3 Synthesis: Establishing Lower and Upper Security Bounds

Though methodologically distinct, the two approaches are complementary. Together, they define a "security bracket" that tightly bounds Ascon's true post-quantum security level.

The concrete analysis of Oh et al. provides a practical *upper bound* on security. By constructing a specific, optimised attack and calculating its cost, it demonstrates that the security of Ascon is *at most* this high [8]. For example, its finding that a key search on Ascon-128a has a G-FD cost of 1.47×2^{155} establishes a hard ceiling on its security level. The theoretical analysis of Lang et al. provides a formal *lower bound* on security against generic attacks. By proving that *any* generic quantum adversary in the Q1 model needs at least $\min\{2^{k/2}, 2^{c/3}\}$ operations to break the AEAD security of Ascon, it establishes a guaranteed floor [7]. The security is *at least* this high.

The convergence of these two bounds provides the strongest possible form of security validation. When the upper bound from the best-known concrete attack is close to the lower bound from the formal proof, it creates a narrow bracket within which the true security level must lie. This triangulation provides a much higher degree of confidence than either paper could offer in isolation.

3. A Comparative Dissection of Quantum Attacks

This section compares how each paper analyzes key quantum threats to Ascon, focusing on key search, collision attacks, and state recovery.By juxtaposing their treatment of key search, collision attacks, and state recovery, we can illuminate the unique contributions and limitations of each approach.

Table 1 A high-level comparison of the analytical frameworks used by Oh et al. and Lang et al.

Feature	Oh et al. [8]	Lang et al. [7]
Primary Goal	Estimate concrete resource costs of specific attacks.	Prove asymptotic security bounds against generic attacks.
Analytical Model	Quantum Circuit Model.	Q1 Random Permutation Model.
Core Technique	Circuit synthesis and cost accounting.	Game-based proofs using the O2H Lemma.
Key Metrics	Qubits (M), Gate Counts, Circuit Depth (FD, Td), G-FD.	Adversarial Advantage, Query Complexity (q_c, q_p), Data Complexity (σ).
Output	Concrete cost tables.	Asymptotic security formulas.

3.1 Grover's Key Search: From Asymptotic Bound to Concrete Cost

Grover's algorithm poses a direct quantum threat to symmetric ciphers [6]. Both papers examine this attack from distinct angles.

Lang et al. [7] provide a theoretical analysis: an adversary uses Grover's algorithm to search a 2^k key space with $O(2^{k/2})$ queries, yielding bounds like $\min 2^{k/2}, 2^{c/3}$.

Oh et al. [8] translate this into concrete cost. For Ascon-128, Grover requires $\approx 2^{63}$ iterations. Each oracle call involves one forward and one reverse Ascon encryption. Their depth-optimized implementation yields a Full Depth (FD) of 1.30×2^{10} and gate count of 1.04×2^{18}, resulting in a total cost of 1.47×2^{155} in the G-FD metric.

Lang et al. also explore a more advanced vulnerability in a large-key variant. In the *nonce-masking* version of Ascon-128a, a second key K' is XORed into the nonce to simulate 256-bit security. They describe a time-data trade-off attack: collecting D ciphertexts and using Grover to search for any of the D initial states reduces complexity to $\sqrt{2^{256}/D}$, yielding $T^2 \cdot D \approx 2^{256}$. The optimal point is $D = T \approx 2^{85.3}$, revealing the scheme offers only 85 bits of post-quantum security [7]. This underscores the value of theoretical analysis in uncovering multi-query vulnerabilities beyond single-instance costing.

This attack exploits the sponge structure to recover a full internal state. It is a data-time trade-off attack: the adversary collects encryptions of a chosen message under 2^ζ different nonces, then uses Grover's algorithm to search for one of the 2^ζ corresponding internal states. The optimal complexity is achieved when the data and time complexities are balanced, which occurs at a cost of approximately $O(2^{n/3})$, where $n = r + c = 320$ is the state size of Ascon. This analysis leads to one of the most critical insights: the paramount importance of the *capacity parameter* c for the post-quantum security of the AEAD mode. The theoretical analysis by Lang et al. explicitly shows that the security of Ascon AEAD against a block-wise adaptive adversary is

bounded by $\min\{2^{k/2}, 2^{c/3}\}$ [7]. The $2^{c/3}$ term arises directly from these state recovery attacks. This means that even if the key size k is very large, a small capacity c can become a fatal bottleneck. The paper powerfully demonstrates this by analysing the proposed *LK-Ascon-256b* variant, which has a 256-bit key but a capacity of only 128 bits ($k = 256, c = 128$). A naive analysis focusing only on key recovery would suggest a security level of $2^{256/2} = 128$ bits. However, the theoretical bound from Lang et al. correctly identifies the weak capacity as the limiting factor, yielding a true security level of only $2^{128/3} \approx 43$ bits. This is a "much worse" result, rendering the scheme far less secure than even the standard Ascon-128. The theoretical work thus provides a vital strategic insight that a more narrowly-focused concrete analysis might miss: for sponge-based authenticated encryption, capacity is a co-equal partner with key size in determining post-quantum security.

3.2 Practical Feasibility and the MAXDEPTH Constraint

Theoretical complexity provides a measure of an attack's cost in an idealised model, but the concrete analysis of Oh et al. introduces a crucial "feasibility filter": the `MAXDEPTH` constraint [8]. An attack may have an acceptable total gate cost, but if its sequential depth is too great, it will be defeated by quantum decoherence. Consider the standard Grover key search on Ascon-128a. As calculated previously, this requires approximately 2^{63} sequential iterations of the Grover oracle. The depth-optimised oracle from Oh et al. has a Full Depth (FD) of 1.30×2^{10} [8]. Therefore, the total depth of the sequential attack is approximately $2^{63} \times 1.30 \times 2^{10} \approx 1.30 \times 2^{73}$. This value significantly exceeds the 2^{64} `MAXDEPTH` threshold suggested by NIST as a plausible near-term limit for reliable quantum computation [5]. This implies that a simple, sequential Grover search is likely to be practically infeasible. An adversary would be forced to resort to *parallelising Grover's algorithm*. While this allows the attack to be completed within the `MAXDEPTH` limit, it comes at a steep cost. As noted by Oh et al., parallelisation squares the dependence on depth in the composite cost metrics (e.g., the cost scales with $FD^2 - M$ instead of FD-M) [8]. The concrete depth analysis acts as a vital reality check on the theoretical attack complexities, demonstrating that an attack which appears potent in terms of query count might be practically unrealisable due to its execution time.

4. The Security Landscape of the Ascon Family: A Unified View

By integrating the concrete cost estimates of Oh et al. with the theoretical security proofs of Lang et al., we can construct a comprehensive and unified security landscape for the entire Ascon family. This section provides a consolidated assessment for each variant, culminating in **Table ??** which serves as a definitive guide to their post-quantum posture.

4.1 Standard NIST Variants

For the official variants standardised or considered by NIST, the two papers provide converging lines of evidence, leading to high-confidence conclusions.

4.1.1 Ascon-128 and Ascon-128a

These are the primary variants for lightweight use cases.

- **Concrete Analysis (Oh et al.):** The G-FD cost for a Grover key search on Ascon-128a is calculated as 1.47×2^{155}. This value is critically compared against the benchmark for NIST Post-Quantum Security Level 1, which is set at 2^{157} (based on the cost of a Grover attack on AES-128). Since the attack cost on Ascon-128a is lower than this threshold, the paper's explicit conclusion is that Ascon-128 and Ascon-128a "do not achieve post-quantum security level 1" [8].
- **Theoretical Analysis (Lang et al.):** The analysis provides a security bound of $\min\{k/2, c/3\}$ bits. For Ascon-128a ($k = 128, c = 192$), the security is $\min\{128/2, 192/3\} = \min\{64, 64\} = 64$ bits. For Ascon-128 ($k = 128, c = 256$), the security is $\min\{128/2, 256/3\} = \min\{64, 85.3\} = 64$ bits. In both cases, the security is bottlenecked by the 128-bit key size [7].
- **Unified Assessment:** Both papers, approaching from opposite directions, conclude that Ascon-128 and Ascon-128a offer a consistent and well-understood post-quantum security level of approximately 64 bits. This is insufficient for applications requiring NIST Level 1 compliance.

4.1.2 Ascon-80pq

This variant was specifically designed with post-quantum key search attacks in mind.

- **Concrete Analysis (Oh et al.):** The Grover key search attack on Ascon-80pq, with its 160-bit key, has a concrete G-FD cost of 1.29×2^{187}. The paper describes this as a "high cost" and explicitly states that it "satisfies the security standards set by NIST for Level 1" [8].
- **Theoretical Analysis (Lang et al.):** Applying the $\min\{k/2, c/3\}$ bound to Ascon-80pq ($k = 160, c = 256$) yields a security level of $\min\{160/2, 256/3\} = \min\{80, 85.3\} = 80$ bits [7].
- **Unified Assessment:** The two analyses are in strong agreement. Ascon-80pq is a robust and suitable choice for applications that require a post-quantum security level equivalent to or exceeding that of AES-128.

4.1.3 Ascon-HASH and Ascon-XOF

The security of the hash function modes is analysed only by Oh et al. [8].

- **Concrete Analysis (Oh et al.):** The analysis focuses on quantum collision resistance. Using the parallelised CNS algorithm, the cost to find a collision in the 256-bit Ascon-HASH is 1.25×2^{184} G-FD. The paper concludes that the Ascon hash functions meet the security requirements comparable to SHA-3.
- **Unified Assessment:** Based on the available evi-

dence, the Ascon hash and XOF functions appear robustly secure against known quantum collision-finding attacks.

5. Synthesis of Findings on the Ascon Family

Based on the synthesised evidence, the following definitive security verdicts can be rendered:

- **Ascon-128 / Ascon-128a:** These variants offer approximately 64 bits of post-quantum security. While secure against classical attacks, this level is insufficient for long-term security in an era of quantum computers and does not meet NIST's Post-Quantum Security Level 1. Their use in new systems requiring post-quantum resilience is not recommended.
- **Ascon-80pq:** This variant offers a well-supported security level of 80 bits. It comfortably meets the requirements for NIST Level 1 and represents a robust and suitable choice for lightweight applications that must maintain security against quantum adversaries.
- **Ascon-HASH / Ascon-XOF:** The available evidence indicates that the Ascon hash functions are robustly secure, with quantum collision resistance comparable to that of the SHA-3 standard. They are suitable for use in post-quantum applications.
- **Large-Key Proposals (LK-Ascon, Nonce Masking):** These proposals should be avoided. Their security is deceptively low and does not match their large key sizes. They serve as a powerful case study in why post-quantum security analysis must look beyond key size alone.

5.1 Recommendations for Implementers and Standards Bodies

The conclusions of this analysis lead to several actionable recommendations:

When developing new systems that require lightweight cryptography with long-term, post-quantum security, the use of **Ascon-80pq** is strongly recommended over Ascon-128 or Ascon-128a. The marginal performance difference is a small price to pay for the significant increase in quantum resilience.

The findings from this comparative analysis offer crucial lessons for the design and standardisation of future algorithms.

(1) *Capacity is Co-Equal to Key Size:* For sponge-based constructions, the capacity c is not a secondary parameter but a co-equal driver of post-quantum security alongside the key size k. The security against state recovery attacks is fundamentally limited by capacity.

(2) *Beware of Complex Keying Schedules:* Proposals that aim to increase security by adding complexity to the keying or initialisation process must be scrutinised for their susceptibility to sophisticated trade-off attacks. A simple increase in the raw number of secret bits does not guarantee an increase in effective security.

This body of work illuminates areas for further investigation. The Lang et al. paper notes that its proof technique for message-wise adaptive adversaries does not yield a tighter security bound than for the more powerful block-wise adaptive case, leaving the precise security of Ascon in this standard model as an open problem [7]. Additionally, a concrete resource estimation of the state recovery attacks on the AEAD modes could provide valuable data points to complement the existing theoretical analysis.

6. Constructing a Theoretical Simon's Attack on Ascon

Applying the Kaplan et al. framework to Ascon requires a careful examination of its duplex mode to identify a structural feature that can be moulded into a periodic function. The iterative nature of the sponge construction, with its clear separation of rate and capacity, provides just such a feature.

6.1 Identifying an Attack Vector in the Duplex Mode

The core operation in Ascon's absorbing phase involves taking the current state $S = (S_r, S_c)$, XORing an r-bit message block M into the rate part, and applying the permutation p to the entire state to produce the next state: $S' = p((S_r \oplus M) \parallel S_c)$. The key observation is that the permutation p is a fixed, public, and unkeyed function. Its output depends solely on its b-bit input.

This structure suggests a powerful attack vector: if an adversary can force the input to the permutation p to be identical for two different computational paths, the entire subsequent evolution of the state will also be identical. Let's consider two different message histories, H_0 and H_1, which after being processed by Ascon, result in two different internal states, $S_0 = (S_{r0}, S_{c0})$ and $S_1 = (S_{r1}, S_{c1})$. If an adversary could somehow ensure that the capacity parts of these states were identical (i.e., $S_{c0} = S_{c1}$), it would gain significant control. Suppose such a "capacity collision" has been found. The states are $S_0 = (S_{r0}, S_c)$ and $S_1 = (S_{r1}, S_c)$. Now, consider processing a subsequent message block M_0 from state S_0 and a different message block M_1 from state S_1. The inputs to the permutation p would be:

- Path 0: $(S_{r0} \oplus M_0) \parallel S_c$
- Path 1: $(S_{r1} \oplus M_1) \parallel S_c$

For these two inputs to be identical, the rate parts must be equal: $S_{r0} \oplus M_0 = S_{r1} \oplus M_1$. This can be rearranged to $M_1 = M_0 \oplus (S_{r0} \oplus S_{r1})$. Let's define the difference in the rate parts as $\Delta = S_{r0} \oplus S_{r1}$. Then, for any message block M, if we process M from state S_0 and process $M \oplus \Delta$ from state S_1, the inputs to the permutation p will be identical. This creates a predictable relationship—a period—that can be exploited.

The challenge, therefore, reduces to finding two message

histories, H_0 and H_1, that lead to a collision in the c-bit capacity. This is a classical problem solvable with a generic birthday attack. An adversary can simply compute the Ascon function for approximately $2^{c/2}$ different message prefixes and store the resulting capacity states. A collision is expected to be found with high probability. This becomes the classical pre-computation step of the overall attack.

6.2 Definition of a Simon's Function for Ascon

With the attack vector identified, we can now formally define a Simon's function for Ascon's duplex mode.

Pre-computation: The adversary first performs a classical birthday search to find two distinct message prefixes, H_0 and H_1, such that processing them results in states $S_0 = (S_{r0}, S_c)$ and $S_1 = (S_{r1}, S_c)$ with a common capacity value S_c. This search requires on the order of $O(2^{c/2})$ classical queries to the Ascon oracle. From this, the adversary computes the r-bit rate difference $\Delta = S_{r0} \oplus S_{r1}$.

The adversary defines a Simon's function f that operates on an $(r+1)$-bit input, which we denote as $(b \parallel x)$, where b is a single bit and x is an r-bit string. The function is defined using quantum oracle access to the full Ascon AEAD process, which we denote as $\mathcal{A}_k(\text{AD}, P)$. For simplicity, we assume no associated data and that H_b and x form the plaintext.

$$f(b \parallel x) = \mathcal{A}_k(\text{empty}, H_b \parallel x)$$

The output of the function is the final authentication tag.

Periodicity Analysis: The hidden period for this function is $s = (1 \parallel \Delta)$. We must show that $f(z) = f(z \oplus s)$ for any input $z = (b \parallel x)$.

Let's evaluate $f(z \oplus s)$:

$$\begin{aligned} f((b \parallel x) \oplus (1 \parallel \Delta)) &= f((b \oplus 1) \parallel (x \oplus \Delta)) \\ &= \mathcal{A}_k(\text{empty}, H_{b\oplus 1} \parallel (x \oplus \Delta)) \end{aligned}$$

Let's trace the state for both $f(b \parallel x)$ and $f((b\oplus 1) \parallel (x\oplus\Delta))$ after the prefix has been processed.

- For the input $(b \parallel x)$, the process starts with history H_b, leading to the intermediate state (S_{rb}, S_c). It then absorbs the final block x. The input to the next permutation call is $(S_{rb} \oplus x) \parallel S_c$.
- For the input $((b \oplus 1) \parallel (x \oplus \Delta))$, the process starts with history $H_{b\oplus 1}$, leading to the intermediate state $(S_{r(b\oplus 1)}, S_c)$. It then absorbs the final block $(x \oplus \Delta)$. The input to the next permutation call is $(S_{r(b\oplus 1)} \oplus (x \oplus \Delta)) \parallel S_c$.

Let's analyse the rate part for the second case. By definition, $\Delta = S_{r0} \oplus S_{r1}$.

- If $b = 0$, the rate part is $(S_{r1} \oplus (x \oplus \Delta)) = (S_{r1} \oplus x \oplus S_{r0} \oplus S_{r1}) = (S_{r0} \oplus x)$.
- If $b = 1$, the rate part is $(S_{r0} \oplus (x \oplus \Delta)) = (S_{r0} \oplus x \oplus S_{r0} \oplus S_{r1}) = (S_{r1} \oplus x)$.

In both scenarios, the rate part for the input $((b \oplus 1) \parallel (x \oplus \Delta))$ is identical to the rate part for the input $(b \parallel x)$. Since the capacity part S_c is also identical (by construction from the pre-computation), the full b-bit input to the permutation is the same in both cases.

$$p((S_{rb} \oplus x) \parallel S_c) = p((S_{r(b\oplus 1)} \oplus (x \oplus \Delta)) \parallel S_c)$$

Because the inputs to the permutation are identical, the resulting states will be identical, and all subsequent operations (including further permutation calls and the final tag generation) will also be identical. Therefore, the final tags will be equal: $f(b \parallel x) = f((b \oplus 1) \parallel (x \oplus \Delta))$. This confirms that our function f has the period $s = (1 \parallel \Delta)$ as required.

6.3 The Full Attack Algorithm

The complete attack proceeds in three stages:

The adversary makes approximately $O(2^{c/2})$ classical queries to the Ascon oracle, $\mathcal{A}_k(\text{empty}, H_i)$, for randomly chosen prefixes H_i. For each query, the adversary must be able to deduce the internal capacity state S_c after processing H_i. This might require some knowledge of the key, or it can be done in a chosen-key setting. Assuming this is possible, the adversary stores the pairs (H_i, S_{ci}) and searches for a collision $S_{ci} = S_{cj}$ for $i \neq j$. Upon finding one, it sets $H_0 = H_i$, $H_1 = H_j$, and computes the rate difference Δ.

The adversary constructs a quantum oracle for the Simon's function $f(b \parallel x)$ defined above. It then executes Simon's algorithm. This requires $O(r+1)$ quantum queries to the oracle U_f. The algorithm returns the $(r+1)$-bit period $s = (1 \parallel \Delta)$. This step confirms the value of Δ found in the classical stage.

With the knowledge of H_0, H_1, and Δ, the adversary can now break the integrity of the AEAD scheme. It can perform a universal forgery. For any message M for which it can observe a valid tag T, it can construct a different message M' that is also authenticated by T. For example, if $M = H_0 \parallel M_{\text{suffix}}$, the adversary can forge the tag for $M' = H_1 \parallel (M_{\text{suffix}} \oplus \Delta)$. Since the internal state evolution is identical after the prefix, the final tag will be the same. This fundamentally breaks the authenticity guarantee of Ascon-AEAD.

6.4 Complexity and Feasibility Analysis

The overall complexity of the attack is dominated by the most expensive step.

- **Classical Complexity:** The pre-computation stage requires $O(2^{c/2})$ classical queries and corresponding storage.
- **Quantum Complexity:** The period-finding stage requires $O(r)$ quantum queries to the specially constructed Simon's oracle. Each query to the Simon's oracle involves one or more calls to the underlying Ascon oracle.

Let's apply this to the standardised Ascon variants:

- **Ascon-AEAD128:** This variant has a capacity $c = 192$ bits and a rate $r = 128$ bits.

– Classical Complexity: $O(2^{192/2}) = O(2^{96})$.
– Quantum Complexity: $O(128)$.
The attack is bottlenecked by the classical collision search. The effective security of Ascon-AEAD128 against this specific quantum structural attack is therefore approximately 96 bits, not the claimed 128 bits.

- **Ascon-Hash256 / Ascon-XOF128:** These variants have a capacity $c = 256$ bits and a rate $r = 64$ bits.
– Classical Complexity: $O(2^{256/2}) = O(2^{128})$.
– Quantum Complexity: $O(64)$.
Here, the classical complexity matches the target 128-bit security level for collision resistance. The attack does not offer a practical advantage over generic classical collision-finding attacks.

The table below quantifies the impact of this theoretical attack.

Table 2 Complexity Analysis of Simon's Attack on Ascon Variants

Ascon Variant	Capacity (c)	Rate (r)	Classical Complexity $O(2^{c/2})$	Quantum Complexity $O(r)$	Effective Security Bound
Ascon-AEAD128	192 bits	128 bits	2^{96}	128	96 bits
Ascon-Hash256	256 bits	64 bits	2^{128}	64	128 bits

While the attack is not practical for Ascon-AEAD128 due to the infeasible $O(2^{96})$ classical pre-computation, its existence is of high theoretical significance. It demonstrates that the security margin in the powerful Q2 model is lower than the classical security claim. The very structure of the sponge construction, with its division of the state into a public-facing rate and a hidden capacity, creates the precise structure that this hybrid classical-quantum attack can exploit. The capacity c is no longer just an abstract security parameter against generic attacks; it is a direct variable in the complexity of a concrete structural attack.

7. Security Implications and Broader Context

The construction of a theoretical Simon's attack on Ascon provides a new lens through which to view its post-quantum security. The implications extend beyond the specific complexity numbers, touching upon the fundamental properties of sponge constructions and the nature of quantum threats to symmetric-key cryptography.

7.1 Ascon's Security in the Q2 Model

The analysis reveals that Ascon's security is not monolithic but is dependent on the adversary's capabilities. In the standard classical model, Ascon-AEAD128 provides its target 128 bits of security. However, in the Q2 model, where an adversary can make superposition queries, the security is demonstrably lower. The period-finding attack reduces the effective security bound to 96 bits, dictated by the complexity of the classical birthday search for a capacity collision. This finding, while theoretical, constitutes a significant security reduction. It implies that the full 128-bit security claim for Ascon-AEAD128 does not hold against all possible post-quantum adversaries. This aligns with recent research into the post-quantum security of keyed sponge constructions, which has yielded security bounds that are sub-ideal. For instance, a 2025 ePrint by Hosoyamada proves post-quantum security for the Ascon AEAD mode up to approximately $\min(2^{c/3}, 2^{\kappa/3})$ queries, which for Ascon-128 would be $\min(2^{192/3}, 2^{128/3}) = \min(2^{64}, 2^{42.6})$, a different but similarly sub-optimal bound derived through a modular proof approach. The analysis in this report provides a concrete attack vector that helps to explain why such reduced bounds appear: the underlying structure permits the extraction of secret information with complexity tied to the capacity, not just the key size.

7.2 Connection to the Collapsing Property

The implications of this attack extend to a fundamental concept in post-quantum hash function security: the **collapsing property**. A hash function H is said to be collapsing if it is computationally infeasible for an adversary to find a superposition $|\psi\rangle = \sum \alpha_x |x\rangle$ such that measuring $H(|\psi\rangle)$ reveals more information about $|\psi\rangle$ than a direct measurement of $|\psi\rangle$ would. Roughly, it means that applying the hash function to a superposition is computationally equivalent to first measuring the superposition and then classically hashing the outcome. This property is a necessary strengthening of collision resistance for a hash function to be safely used in post-quantum protocols like quantum-secure commitment schemes. It has been shown that sponge constructions are collapsing if the underlying permutation f is modelled as a random function or a random non-invertible permutation. However, the proof was notably left open for the case where f is an invertible random permutation—which is precisely the model for Ascon-p. The Simon's attack constructed in this report provides strong evidence that the Ascon sponge construction is **not collapsing**. The attack succeeds precisely because it preserves a specific quantum structure through the oracle calls. The algorithm prepares a state $\frac{1}{\sqrt{2}}(|z\rangle + |z \oplus s\rangle)$, and the Ascon oracle, when acting on this state, does not "collapse" it into a useless measurement. Instead, it maintains the periodic structure, allowing the adversary to distinguish it from a random function and recover the period s. Since the duplex and sponge constructions are provably equivalent in security, a structural weakness in one implies a weakness in the other. This connects a specific, concrete attack to a fundamental, abstract security property, suggesting that sponge constructions based on public, invertible permutations may not be suitable as drop-in replacements for random oracles in all post-quantum contexts.

7.3 Design Recommendations for Post-Quantum Sponges

The analysis naturally leads to recommendations for designing future sponge-based primitives intended to be secure in the Q2 model against period-finding attacks. The goal of

these countermeasures is to disrupt the ability of an adversary to create and detect a hidden periodicity.

- **Increase Capacity:** The most straightforward, if brute-force, defence is to significantly increase the size of the capacity, c. The complexity of the attack presented here is bottlenecked by the classical $O(2^{c/2})$ search. If the capacity is chosen such that $c/2$ is greater than or equal to the claimed classical security level (e.g., for 128-bit security, require $c \geq 256$), then this specific attack becomes no more efficient than generic classical attacks. Ascon's hashing modes already follow this principle, but the AEAD mode does not.
- **Break State Symmetry and Periodicity:** The attack relies on the fact that the permutation p is applied identically in each round and is independent of the history. Future designs could introduce mechanisms to break this symmetry. For example, the permutation could be tweaked with a value derived from a running hash of the message history, or the round constants could be made dependent on the input. This would prevent two different histories, even with a capacity collision, from having an identical state evolution.
- **Employ Keyed Permutations:** The attack targets a public permutation. If the core permutation were keyed, and the key schedule was designed to be updated during the absorbing phase, it would become significantly harder for an adversary to predict and control the state evolution. This would complicate the construction of a consistent Simon's function.

Acknowledgments We express our gratitude to the National Institute of Information and Communications Technology (NICT). This research was made possible through the support provided for Dr. Anandarup ROY's visit to Sakurai Lab at Kyushu University by the Foreign Researcher Invitation Program of NICT.

References

[1] National Institute of Standards and Technology. Announcing lightweight cryptography selection. Online, February 2023. Accessed: August 3, 2025.

[2] Meltem Sönmez Turan, Kerry McKay, Donghoon Chang, Jinkeon Kang, Noah Waller, John Kelsey, Lawrence Bassham, and Duhyeong Hong. Status report on the final round of the nist lightweight cryptography standardization process. Technical Report NISTIR 8454, National Institute of Standards and Technology, June 2023.

[3] Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Martin Schläffer. Ascon v1.2: Lightweight authenticated encryption and hashing. *Journal of Cryptology*, 34(3):33, 2021.

[4] Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Martin Schläffer. Ascon – Lightweight Cryptography. Official Project Website, 2024. Accessed: August 3, 2025.

[5] Samuel Jaques, Michael Naehrig, Martin Roetteler, and Fernando Virdia. Implementing Grover oracles for quantum key search on AES and LowMC. In *Advances in Cryptology – EUROCRYPT 2020*, volume 12106 of *Lecture Notes in Computer Science*, pages 280–310. Springer, 2020.

[6] Lov K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, pages 212–219. ACM, 1996.

[7] Nathalie Lang, Stefan Lucks, Bart Mennink, and Suprita Talnikar. Security of the ascon authenticated encryption mode in the presence of quantum adversaries. Cryptology ePrint Archive, Paper 2025/411, 2025.

[8] Yujin Oh, Kyungbae Jang, Anubhab Baksi, and Hwajeong Seo. Depth-optimized quantum circuits for ASCON: AEAD and HASH. *Mathematics*, 12(9):1337, 2024.

[9] Dan Boneh and Mark Zhandry. Quantum-secure message authentication codes. In *Advances in Cryptology – EUROCRYPT 2013*, volume 7881 of *Lecture Notes in Computer Science*, pages 592–608. Springer, 2013.

[10] Andris Ambainis, Mike Hamburg, and Dominique Unruh. Quantum security proofs using semi-classical oracles. In *Advances in Cryptology – CRYPTO 2019*, volume 11693 of *Lecture Notes in Computer Science*, pages 269–295. Springer, 2019.