International Journal of Safety and Security Engineering
Vol. 14, No. 6, December, 2024, pp. 1729-1742
Journal homepage: http://iieta.org/journals/ijsse

# A New Approach to Improving the Security of the 5G-AKA Using Crystals-Kyber Post-Quantum Technologies and ASCON Algorithm

Rasha Hussein Joudah[1*], Mehdi Ebady Manaa[1,2]

[1] Department of Information Networks, College of Information Technology, University of Babylon, Hilla 51002, Iraq
[2] Intelligent Medical Systems Department, College of Sciences, Al-Mustaqbal University, Hilla 51001, Iraq

Corresponding Author Email: rashahussein@uobabylon.edu.iq



https://doi.org/10.18280/ijsse.140608

**Received:** 22 July 2024
**Revised:** 26 September 2024
**Accepted:** 26 November 2024
**Available online:** 31 December 2024

***Keywords:***
*5G-AKA protocol, 5G security, 5G authentication, Crystals-Kyber, ASCON*

**ABSTRACT**

The 5G-AKA protocol includes several vulnerabilities related to security and privacy. This paper proposes improving the standard 5G-AKA protocol by enhancing security and privacy, such as optimal forward secrecy, resilience against linkability attacks, and protection against malicious SN networks. The proposed protocol, called KyberPQ-AKA, includes two stages of development. In the first stage, a Crystals-Kyber KEM-based method creates keys and safely exchanges them within the AKA protocol environment. In the second stage, the lightweight encryption algorithm ASCON replaces traditional encryption in the protocol to work on devices with limited resources. Moreover, key encapsulation (KEM) mechanisms improve the protection of user identity and complete privacy. KyberPQ-AKA makes it easier to adapt to a quantum-secure environment and provides additional security and authentication benefits by switching from the AES encryption algorithm to the lightweight ASCON algorithm. KEM Crystals-Kyber post-quantum, a criterion NIST recently chose, and KEM candidates for the fourth round after quantum from NIST used in the suggested protocol. The results on connection and calculation costs indicate that the KyberPQ-AKA protocol is practical and superior to standard 5G-AKA. We also proved the security of KyberPQ-5G using the ProVerif tool and by applying the protocol using Mininet with RYU Controller to test the protocol. The results proved this in comparison with the standard 5G-AKA protocol.

## 1. INTRODUCTION

In 2015, the International Telecommunication Union (ITU) published a document titled "IMT Vision; 5G Architecture and Overall Goals " outlining three usage scenarios for mobile broadband (eMBB) extremely high reliability and low latency (uRLLC) and widespread machine-to-machine communication (MTC). It also details eight performance metrics, like peak speed and network congestion levels. When you look at 5th generation tech versus generation tech in terms of speed and connectivity per area size, it is a leap; at least ten times faster connectivity and smoother data transfer with minimal latency in the milliseconds range per square kilometer coverage area. The setup of a 5th generation network involves a mix of technologies. The structure of traditional mobile communication networks is mainly divided into access networks, transmission networks, and core networks [1]. Due to the introduction of new technologies such as network function virtualization, software-defined networking, and multi-access edge computing, 5G networks have a more complex network form than 4G. In terms of network participants, in addition to traditional communication equipment manufacturers and basic telecommunications companies, due to the introduction of new technologies in the 5G era, cloud, big data, Internet data centers, and other manufacturers have joined the 5G network to form all links, and multi-domain vertical industry entities are also deeply involved in the development of 5G converged applications.

Fifth-generation communication (5G) is a new type of information infrastructure that realizes the interconnection of people, machines, and things and is an important driving force for the digital transformation of the economy and society.5G security is an important foundation and a solid guarantee for the high-quality development of 5G. To do a good job in 5G security, it is necessary to understand the characteristics of 5G security objectively and actively respond to 5G security risks and challenges.

The international standard defines the enhanced 5G security standard [2]. The overall architecture of the 5G network continues the characteristics of the 2/3/4G communication network. Still, it adopts the three-layer architecture of the access layer, the core network layer, and the application layer. However, new technologies such as network function virtualization, network slicing, edge computing, service architecture, and network capability openness have been introduced at the core network layer. The network architecture has undergone major changes, has higher performance indicators than 4G, and supports more diverse business scenarios. In line with the evolution of the network, 5G network security is also constantly evolving and improving.

Based on inheriting the hierarchical and domain-based security architecture of the 4G network, the 3GPP R15 version defines stronger security capabilities than 4G: first, the new service domain security adopts perfect registration, discovery, authorization security mechanisms and security protocols to ensure the security of the 5G service architecture [3]. The second is to adopt a unified authentication framework, which can integrate multiple access authentication methods of different standards to ensure the continuity of the authentication process when switching between heterogeneous networks. The third is to enhance data privacy protection, use encryption to transmit user identities, and support user plane data integrity protection to prevent attackers from using the air interface to transmit user identities in plain text to track the user's location and information illegally. The fourth is to enhance the security of inter-network roaming, provide end-to-end protection of inter-network signaling of network operators, and prevent the outside world from obtaining sensitive data between operators' networks. The release16 (R16) and release17 (R17) stages have further optimized the existing security infrastructure. On the one hand, it provides enhanced security capabilities. For example, the SBA architecture service is defined to enhance the security mechanism, including a finer-grained authorization mechanism between network elements, stronger user plane data transmission protection between operators, etc., to ensure the security of data transmission on the signaling plane and the user plane inside the core network. In addition, 3GPP also introduced the user plane integrity protection mechanism of the 5G SA network into the 5G NSA network and the 4G network to further enhance air interface security. On the other hand, it enables vertical industry security.

The development of 5G networks still faces certain security challenges. Developing new technologies and applications of 5G has brought new security risks and challenges. It needs to be viewed from the perspective of development, systematization, objectivity, and cooperation in order to achieve the coordinated promotion of 5G security and development. To ensure the provision of high-quality services, 5G networks need advanced security standards that surpass those of previous generations of mobile networks. Therefore, the 3GPP organization has developed key authentication protocols such as the authentication and key agreement protocol (5G-AKA) and the enhanced protocol for third-generation authentication (EAP-AKA') to ensure the security of the initial user authentication process in 5G networks. However, researchers in recent studies have revealed some loopholes in the 5G-AKA protocol, which makes it vulnerable to numerous [4]. The transmission is to prevent attackers from tracking or intercepting it. It also provides user-level data protection to ensure that it is not manipulated during transmission over communication networks. In addition to improving security, 5G networks provide a complex architecture that combines multiple technologies such as virtualization, software-defined networking, and end-to-end multi-access computing, increasing the need for advanced and integrated security solutions to ensure the protection of data and networks from growing threats [5].

This work presents a way to create the 5G AKA protocol using advanced encryption algorithms like quantum Crystals-Kyber and ASCON Lightweight, which have many security benefits. We consider practical factors like compatibility with previous and future generations of mobile devices, payload efficiency, and adaptability to quantum communication standards. A formal security analysis is conducted using verification tools such as the ProVerif tool to ensure the effectiveness of the proposed protocol in achieving high levels of security and efficiency.

The remainder of the structure paper is as follows: Section 2 reviews related work of proposed studies on the AKA protocol. Section 3 is the background of the AKA protocol and important algorithms. Section 4 includes the methodology and proposed system. Section 5 includes results and discussion. Finally, Section 6 concludes the paper by summarizing the contributions and outlining future research directions.

## 2. RELATED WORK

The authentication process in fifth-generation networks depends on the 5G-AKA protocol. However, it suffers from security vulnerabilities that allow revealing the user's identity, tracking his location, and other security breaches, so the researchers have tried to correct this vulnerability. Wang et al. [6] presented an improved version of the 5G-AKA privacy protection protocol. In this new protocol, researchers are trying to address the weaknesses of the existing protocol, especially in the face of Link attacks from active attackers. It also provides a comprehensive analysis of those attacks and their causes. It provides protocol improvements to mitigate their effects while maintaining compatibility with SIM cards and the infrastructure of existing 5G networks. Use the Tamarin tool, an official verification tool, to prove that the 5G-AKA network meets the security objectives of privacy, authentication, and confidentiality. 5G-AKA' is designed using the elliptic curve integrated encryption system (ECIES-KEM) to encapsulate keys and encrypt challenges sent from the home network (HN). The cost of additional time provided by the new protocol is minimal (an increase of 0.02% to 0.03%).

Hernández and Cervelló-Pastor [7] presented a lightweight test designed to evaluate machine learning (ML) applications in fifth-generation networks. This test enhances containerization technology to Create ML network functions on the Mininet network simulator. The paper demonstrates the use of this test by experimenting with real-time bandwidth prediction using a repeating neural network with long-term memory (LSTM). The proposed test integrates mininet and Docker containers consisting of Containernet, NVIDIA Container Runtime, Ubuntu Bionic Beaver and NVIDIA GPU. Two types of Docker containers are used: one for data collection and the other for running ML algorithms. The experiment aims to predict network traffic using an LSTM neural network. The setup was performed on a single device equipped with an Intel i9 CPU, 64GB RAM, and an NVIDIA GeForce RTX 2080 GPU. The model showed high accuracy in predicting traffic for two base stations. The performance evaluation indicated the minimum load from containerization, with GPUs significantly reduced the training time and evaluated the proposed method by performance, resource, accuracy, quantity, and quality.

Basin et al. [8] presented a comprehensive formal analysis of the 5G authentication protocol and key agreement (AKA), standardized by the 3GPP group. The analysis was performed using the Tamarin security protocol verification tool, revealing serious security flaws and suggesting provable secure fixes. The formal model and analysis techniques developed can be

applied to future updates of the 5G standard and other AKA protocols.

Koutsos [9] proposed using formal methods for analyzing the 5G-AKA authentication protocol, specifically applying the Bana-Comon indistinguishability logic. The author models protocol instances and messages using terms and predicates to represent computational indistinguishability. The security properties are proved by deducing the security properties from a set of axioms in the Pana-common model. The analysis in this research shows that except for the IMSI-catcher attack, most of the known attacks on AKA protocols still apply to 5G-AKA. It introduces a novel linkability attack against PRIV-AKA, which is a modified version of the AKA protocol previously claimed to be unlinkable. The author proposes a modified version of the 5G-AKA protocol, which is designed to enhance privacy while adhering to the limitations of 5G-AKA efficiency. The enhanced protocol introduces the concept of σ-unlinkability, which allows an accurate estimation of the specificity of the protocol. It provides official proof that the updated protocol satisfies the possibility of unlinking using the Bana-Comon model and achieves mutual authentication. The analysis shows that although 5G-AKA improves on previous versions by preventing IMSI-catcher attacks, it is still vulnerable to many known attacks and shows that the proposed protocol is not linkable, which provides stronger privacy guarantees compared to the original 5G-AKA protocol. The analysis and proposed improvements are based on official models, which may not capture all the practical nuances of real-world deployments.

Sakamoto et al. [10] presented a documented AES-based encryption scheme with an associated data schema (AEAD) called Rocca. Rocca's design leverages AES-NI and SIMD instructions to achieve the high performance and security required for 6G systems. The scheme uses a new round function that includes AES rounds and 128-bit XOR operations, optimized for minimum critical path and increased efficiency. It was suggested that a circular function be used to reduce the critical path by avoiding doing consecutive AES and XOR operations in the same round. This function is meant to protect against known attacks on similar schemes, such as those in the AEGIS family and Tiaoxin-346. Encryption/decryption speeds of up to 150Gbps have been achieved, which significantly outperforms existing schemes such as SNOW-V, Aegis-256, and Waes-256-GCM. Evaluations and benchmarks were carried out on the Intel(R) Core (TM) i7-1068ng7 CPU with a speed of 2.30GHz and 32GB RAM. Rocca has achieved up to 180.55Gbps in encryption mode only for large data volumes (16384 bytes). As for the EAAD mode, Rocca outperformed other schemes significantly, achieving as much as 97.55Gbps. The system has maintained high security levels, providing 256-bit security against key recovery attacks and 128-bit security against forgery attacks. The system is limited to handling messages and associated data up to certain lengths (for example, 2128 messages for a fixed key).

Abd El-Latif et al. [11] proposed a new secure mechanism for data encryption using quantum walks (QWs), specifically controlled alternative quantum walks (CAQWs). They have built a new S-box method integrated with encryption technologies, taking advantage of the encryption features inherent in QWs to enhance security in 5G-IoT environments.

The evaluation measures used in the paper include key area analysis to ensure that the key area is large enough to resist brute force attacks, correlation of adjacent pixels to measure the correlation between adjacent pixels in encrypted and native frames, with the aim of obtaining values close to zero in encrypted frames, Pixel count change rate (NPCR) to assess the effect of changing pixel values in encrypted frames compared to the original frames, graph analysis to ensure uniform distribution, information entropy to measure randomness and uniform distribution of pixel values in encrypted frames, with the aim of obtaining entropy values close to 8 bits, key sensitivity to assess the sensitivity of the encryption algorithm to changes in the key., And time complexity to measure the time needed to encrypt files of different sizes. The proposed encryption methods have shown significant improvements in security and performance. Still, the implementation of quantum walks, especially multi-walk systems, requires significant physical resources and complicates the realization of quantum walks.

Xiao and Wu [12] proposed the 5G-IPAKA protocol as a significant enhancement over the conventional 5G Authentication and Key Agreement (AKA) protocol in their study titled "5G-IPAKA: An Improved Primary Authentication and Key Agreement Protocol for 5G Networks." This protocol addresses key security vulnerabilities by replacing the traditional static shared key with a dynamically derived key, thereby mitigating risks associated with shared-key attacks. Additionally, 5G-IPAKA implements a challenge-response mechanism at the Serving Network (SN) level, enhancing mutual authentication and reducing the likelihood of replay attacks. The authors employed the mixed-strand space model to rigorously verify protocol security, ensuring backward compatibility with existing systems while providing notable improvements in both security and performance. Among the most significant practical outcomes presented in the study is the protocol's ability to reduce authentication time in modern cellular networks without compromising security. Furthermore, 5G-IPAKA tackles privacy concerns, such as preventing user location tracking, and achieves Perfect Forward Secrecy, safeguarding prior communications even if a key leak occurs in the future.

The proposed approach shows significant improvements in encryption and decryption times, key generation efficiency, and overall security, which makes it a valuable contribution to the field of cloud security in fifth-generation networks. However, further real-world validation and exploration of its applicability to different types of curves is essential for its wider adoption.

## 3. BACKGROUND

### 3.1 5G-AKA protocol analysis

The 5G-AKA protocol is divided into two phases, namely the registration and challenge-response phases, which will be described separately below.

1). Registration section

The registration stage is not a stage unique to the 5G-AKA protocol. It must go through this stage when the 5G public network wants to execute the authentication protocol, and it is the same, as shown in Figures 1-3:

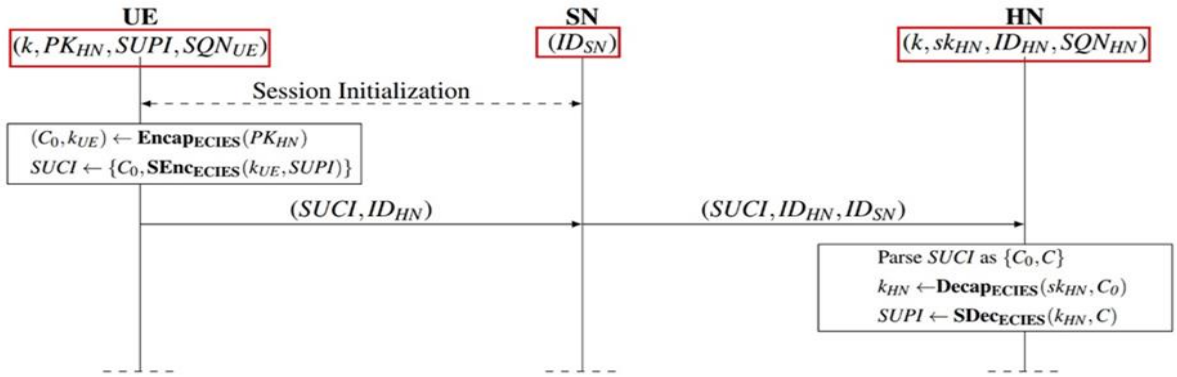


**Figure 1.** The initiation phase of 5G-AKA

The red box indicates what the three entities knew before they started. During the registration process, the UE side box hides the SUPI (the user identifier in 5G) using the ECIES component (converting SUPI into SUCI). This resolves the previous issue of transmitting IMSI numbers in clear text prior to 5G, representing a significant advancement in protecting user privacy in 5G [13]. The main reason is that the symmetric key system loses its role here. UE is a lot, and after the introduction of symmetric keys, I don't know which UE symmetric key to use for decryption. Still, the introduction of the public key system also leads to the problem of difficulty in quantum-resisting (which is also what 3GPP is currently discussing). After calculating the SUCI, the UE sends the SUCI and HN to the SN (Service Network), and the signal strength typically determines which service network to use. After receiving the SN, the SN adds its IDSN to it and then sends it to the HN, which then restores the SUCI to SUPI through the ECIES component. In this way, the registration process is over; as mentioned above, the registration process actually mainly completes the process of passing SUCI; HN will have SUCI after it uses UDM (an entity in HN) to query the user's subscription data to determine which authentication method to choose, generally 5G-AKA (because it is the first choice, as long as the device supports it, choose it) [14].

2). Challenge-response phase

This stage cannot be said to be unique to the 5G-AKA protocol but can only be said to be unique as follows:

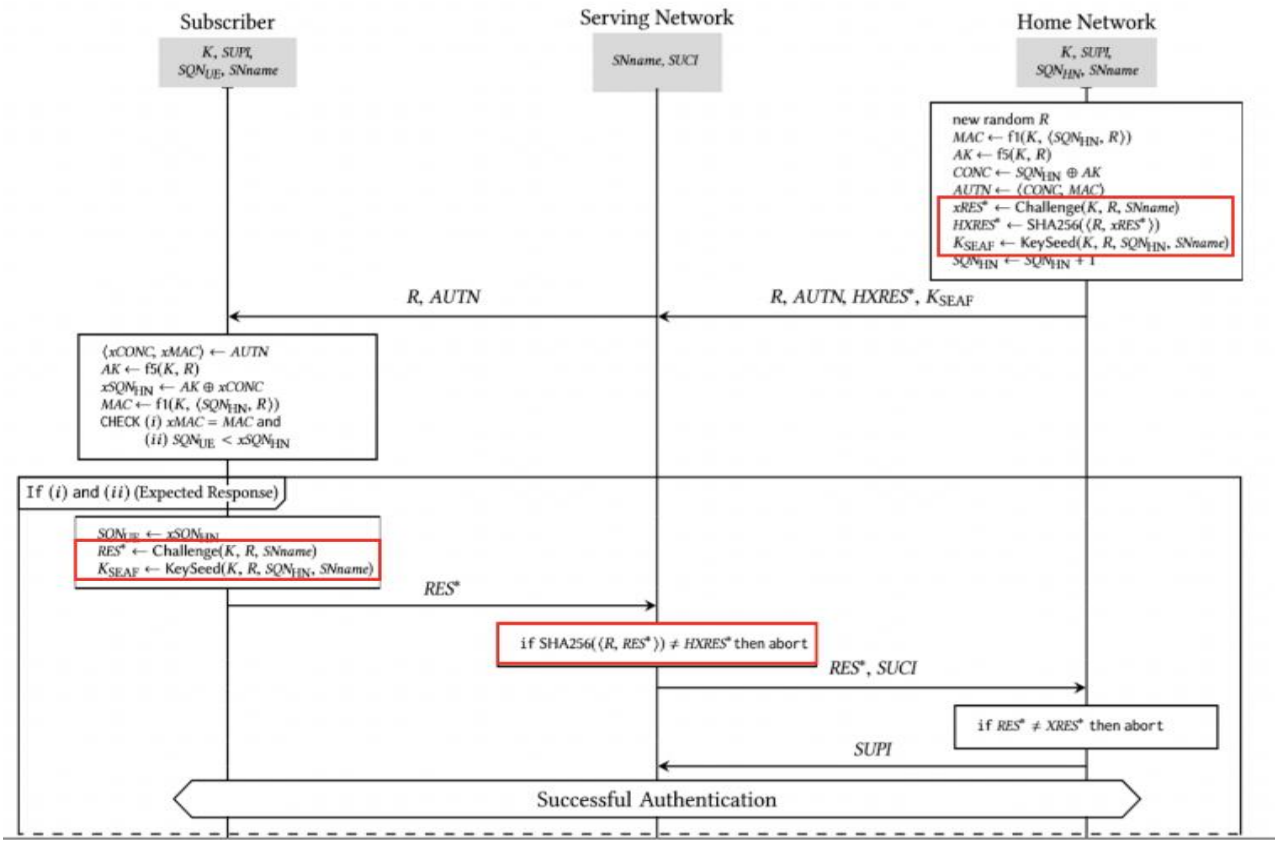


**Figure 2.** The certification process of 5G-AKA

The part of the gray box is also where the individual entity implements what it already knows (be careful when understanding the protocol).

After the registration process, the authentication protocol was selected, which is assumed to be the 5G-AKA protocol. Then, the HN side creates an authentication quadruple (the steps are shown in the box), where R is a 128-bit random number, AUTN is an authentication token (note that the token has information like an AK, the XOR value of SQNHN (i.e., CONC), and a MAC value; and HXRES* is the hash of the expected response value. There is also a difference between the AKA protocol of 5G and 4G, which shows that HN has yet to put a lot of trust in SN, which helps stop malicious SN. Finally, there is a KSEAF, which is a generated anchor key, which is used to derive the key after successful authentication below. In addition, the SN name was introduced in the calculation of HXRES* and SEAF, which is also different from the 4G authentication protocol [15, 16].

The SN sends the random number R and the authentication token AUTN to the UE after receiving the authentication quadruple that HN sent. The UE divides the AUTN into CONC and MAC after receiving the message from the SN, and then, in order to recover the serial number SQNHN, it first calculates the AK using the shared key k and the received random number R (the purpose of the AK, in this case, is to hide the serial number in the message), and then XORs with the CONC to produce SQNHN. After getting the serial number, calculate the MAC by yourself (note that the serial number on the HN side is used to calculate the MAC here, not the serial number on the UE side), and compare it with the received MAC value, there will be the following three situations:

• If the MAC values are the same and the serial number on the UE side is smaller than the serial number on the HN side (anti-replay), the HN's authentication (based on the shared key k) is completed.

• If the MAC value is the same but the sequence number on the UE side is greater than the sequence number on the HN side, then the UE will think that there is a problem with the sequence number out of step and will resynchronize; the UE side will generate a packet to the HN because the behavior here is different from the above case; a well-known attack in 5G-AKA is introduced: a linkability attack (exposing the user's privacy), and the main way to solve this attack is to eliminate or cover up this behavioral inconsistency (currently discussed by 3GPP).

• If the MAC values are different, the authentication fails.

If the UE completes the HN's authentication (i.e., Scenario 1 above), the UE side will generate RES* and KSEAF and send the response value RES* to the SN for authentication [17, 18].

### 3.2 Post-quantum cryptography

Post-quantum cryptography refers to cryptographic algorithms that are safe against quantum computer attacks. Traditional public key encryption systems, such as those based on integer analysis (for example, RSA) and discrete logarithms (for example, DSA, DH), are vulnerable to quantum computers, specifically the Shor algorithm, which can solve these problems efficiently. Peter Schur demonstrated in 1994 that a sufficiently potent quantum computer could defeat such encryption schemes, highlighting this vulnerability [19].

In response to this looming threat, the National Institute of Standards and Technology (NIST) has initiated a process to standardize quantum-resistant encryption algorithms. In July 2022, NIST chose Crystals-Kyber as Standardization's primary key encapsulation (KEM) mechanism. Crystals-Kyber and four other algorithms (BIKE, classic McEliece, HQC, and bike) were selected for further evaluation and possible standardization in subsequent rounds.

CRYSTALS-Kyber (Kyber) is a key encapsulation mechanism designed to be resistant to quantum attacks. Kyber is based on how difficult the problems are in network-based encryption, which is currently considered safe against quantum computer attacks. It works through a set of three algorithms:

1) KeyGen (): This is a non-deterministic algorithm that generates a public and secret key pair (pk, sk).

Choose a polynomial ring: $R = \frac{Zq[x]}{X^n+1}$

q=a prime modulus (typically 3329)

n=a power of 2 (typically 256), which defines the degree of polynomials.

Generate private key: Sample a secret polynomial s from a noise distribution, which is designed to have small coefficients.

Generate public key: Sample a random matrix A from $R^{(K\times K)}$, where k depends on the security level. Sample a random 'small' error vector e from the noise distribution. Compute the public polynomial vector

$$t = As + e(\mathrm{mod}\cdot q) \tag{1}$$

Public key: (A, t), matrix A and vector t

Private key: sk =s. Secret polynomial vector s.

2) Encaps (pk): this algorithm uses the public key pk to generate C ciphertext and a symmetric key K. It is also non-deterministic.

To encrypt $m$ using the public key (**A**,**t**), the encryption procedure calculates two values (**u**, $v$).

$$u = A^T r + e1 \tag{2}$$

$$v = t^T r + e2 + m \tag{3}$$

where, $A^T$ is the transpose of the public matrix A, r is a randomly sampled vector, and e1, and e2 are noise vector. Cyphertext consist of the values **u,v**.

3) Decaps (sk, c): this deterministic algorithm uses the secret key sk and the ciphertext c to retrieve the symmetric key k or signal a failure.

Given the private key **s** and a cyphertext (**u**,***v***), the decryption is straightforward. We compute a *noisy* result $m_n$.

$$m_n = v - s^T u \tag{4}$$

This result is noisy because the computation does not yield the original message m. By looking at the equations, we can see that:

$$m_n = e^T r + e_2 + m + S^T e1 \tag{5}$$

The original message $m$ can be recovered from $m_n$ by considering the distribution of the noise terms. The coefficients of $m$ is scaled to be significantly larger than the

noise so they can be distinguished, and the original message can be accurately recovered.

In the context of post-quantum cryptography, Kyber offers several advantages, such as efficiency and security, making it a promising candidate for widespread adoption in securing communications against future quantum threats. By applying Kyber and similar quantum resistance algorithms, systems can protect sensitive information and communications against potential attacks by quantum computers [20].

### 3.3 ASCON lightweight

ASCON is the winning algorithm in the NIST lightweight password contest. The ASCON algorithm adopts a dual input structure, which is divided into four stages: initialization, linked data processing, plain text processing, and a termination function. The authors of the ASCON algorithm recommend two versions of the algorithm: ASCON-128 and ASCON-128A, which differ in block lengths of 64 bits and 128 bits, respectively, with Version 2 having the advantage of performance in processing long data. ASCON has high key flexibility, a small core offset state of only 320 bits, a simple wheel function design, and a bit-slicing design concept. A 5-bit S-box (for example, used as the kernel for Keccak's S-box) is used to implement a lightweight approach and has no known side-channel attacks [21].

ASCON is a "sponge" type of encryption algorithm that is used to get both privacy and integration at the same time. It does this by using authenticated encryption with linked data (AEAD), which is different from the usual way of doing things, which is to do encryption and hash calculation separately. The internal structure of Ascon consists of a state: it consists of a table with five rows and 64 columns, where each cell contains one bit. Keys: used to modify the state via XOR operations with stored values. Padding: ASCON adds padding to the data to make it fit the block size by putting one "1" bit after enough "0" bits to fill the block [22]. The processing in ASCON authenticated encryption mode consists of the following three main steps. The word mentioned below is 64 bits. Additionally, the processing time of Step (2) depends on the length of the input data. However, the processing time of initialization and finalization is constant regardless of the input data length.

Step (1): Initialization: The state is initialized using the key K, nonce N, and initialization value IV.

Step (2): Iteration (Data Processing): The associated data (AD) is divided and processed for input. Then, in encryption, the plaintext is processed iteratively along with the input, and ciphertext C is the output. In decryption, the divided ciphertext C is processed as input, and plaintext P is output.

Step (3): Finalization: The key is re-input, and the tag T is output.

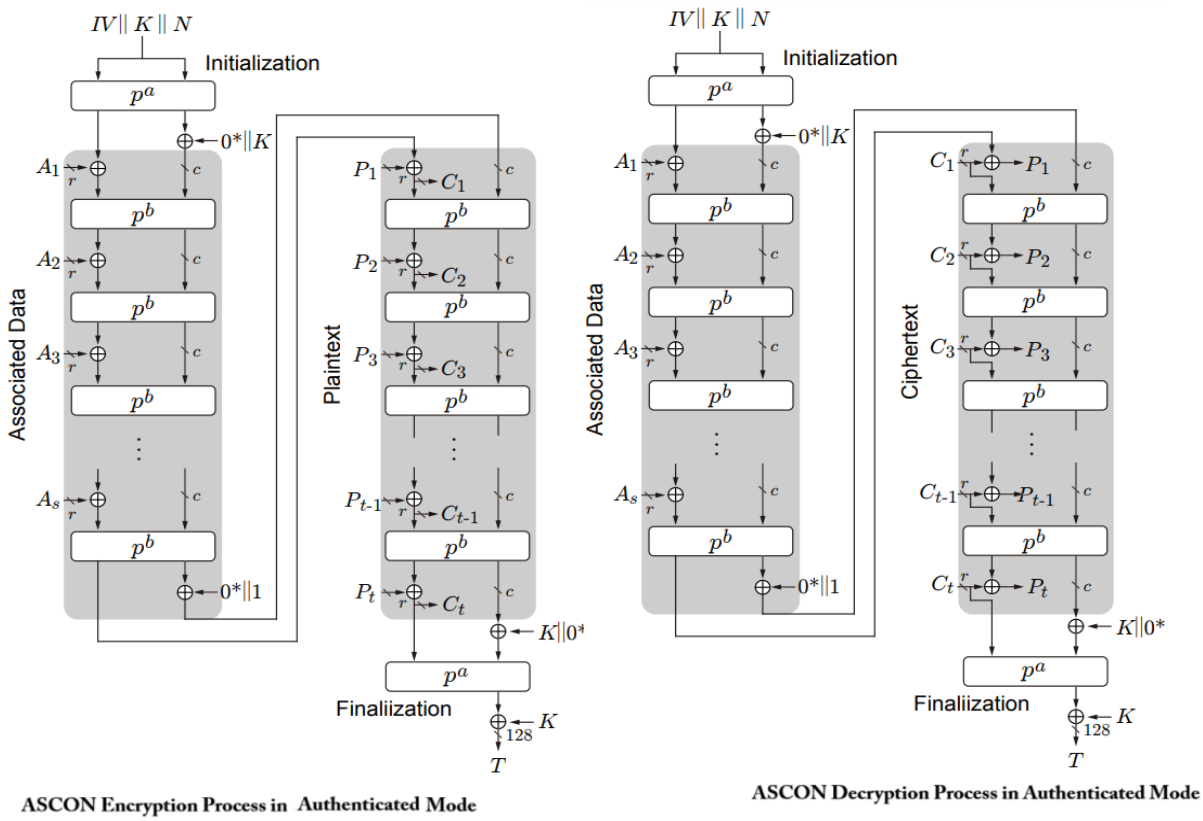


**Figure 3.** Authenticated encryption and decryption in ASCON

## 4. METHODOLOGY

### 4.1 KyberPQ-AKA protocol

**Integration of Crystals-Kyber into 5G-AKA:** Our proposal suggests that the 5G-AKA protocol could be made better by using Crystals-Kyber, a quantum key encapsulation mechanism (KEM), to make it safer from both quantum attacks and known attacks in classical networks. Crystals-Kyber provides strong security due to its reliance on mathematical problems that are difficult to solve even with quantum computers, making it a future alternative to

traditional encryption algorithms used in the 5G-AKA protocol. Crystals-Kyber has been integrated into the authentication process of the 5G-AKA protocol by replacing traditional encryption mechanisms with a post-quantum key encapsulation mechanism. The process includes the following:

1) Creating secret public and private keys: user devices (UE) and the home network create a pair of public and private keys based on the key generation method in Crystals-Kyber.

2) Key encapsulation: the session key is encapsulated using the public key of the home network (HN) and generates an encrypted text that is sent to the service network (SN).

3) Data transfer: the service network sends the encrypted text to the home network.

4) Unwrapping: the home network uses the private key to unwrap the ciphertext and recover the session key.

5) Authentication: The session key is used to establish mutual authentication between the user's equipment and the home network.

Crystals-Kyber offers several advantages over traditional encryption methods:

**Resistance to quantum attacks:** Crystals-Kyber is resistant to attacks that quantum computers may carry out because it is based on complex mathematical problems, such as random networks.

**Improved performance:** Studies show that Crystals-Kyber is characterized by high performance in terms of the time taken to create, wrap, and unpack keys. This makes it more efficient in practical environments.

Long-term security: with the rapid progress in the development of quantum computers, Crystals-Kyber provides strong and long-term protection against possible future attacks, making it a sustainable choice for communication systems.

Thus, the integration of Crystals-Kyber into the 5G-AKA protocol enhances the security and efficiency of the authentication and agreement process on keys, making them more ready for future challenges in cryptography.

**Replacing AES with ASCON:** The advanced encryption standard (AES) has been the cornerstone of encryption protocols, including the 5G authentication protocol and the key agreement (5G-AKA). However, with the growing demand for lightweight, efficient, and secure encryption methods, especially for Internet of Things (IoT) environments, the need for an alternative has become obvious. ASCON, a lightweight encryption algorithm, has been proposed as an alternative to AES in the 5G-AKA protocol due to its efficiency and security features suitable for restricted environments.

The integration of ASCON into the 5G-AKA protocol involves replacing all cases where AES is currently used with ASCON. This process includes:

1). Encryption and decryption: All messages previously encrypted with AES are now encrypted with ASCON. This change improves the speed of the encryption process and reduces the computational burden on the hardware.

2). Message authentication: ASCON generates message authentication codes (MACs) to ensure the integrity and authenticity of messages exchanged during the authentication process.

Replacing AES with ASCON in the 5G-AKA protocol leads to several important benefits:

• Computational efficiency: ASCON's lightweight design reduces the time required for encryption operations, thereby speeding up the overall authentication process. This efficiency is especially useful in scenarios involving many IoT devices that require fast and secure authentication.

• Enhanced security: by adopting a modern encryption algorithm such as ASCON, the protocol is better prepared to deal with current and future security threats, including those posed by quantum computing developments.

• Reduce power consumption: ASCON's design reduces power consumption, which is critical for battery-powered devices in IoT networks. This reduction in energy use extends the operational life of the devices and contributes to more sustainable network operations.

In short, replacing AES with ASCON in the 5G-AKA protocol not only addresses current vulnerabilities but also improves the protocol's performance and security, making it more suitable for the next generation of mobile networks and IoT applications.

### 4.2 Proposed methodology

KyberPQ-AKA protocol was implemented in the Ubuntu 22.04 environment using Python, including the Mininet emulator and Ryu controller for communication between UE, SSN, and HN. The protocol has been emulated using functions of the 5G core network that include the 5G-AKA protocol authentication process. Encryption and decryption operations with ASCON replacer were used instead of the AES used in the standard protocol version. The proposed approach is shown in Figure 4.

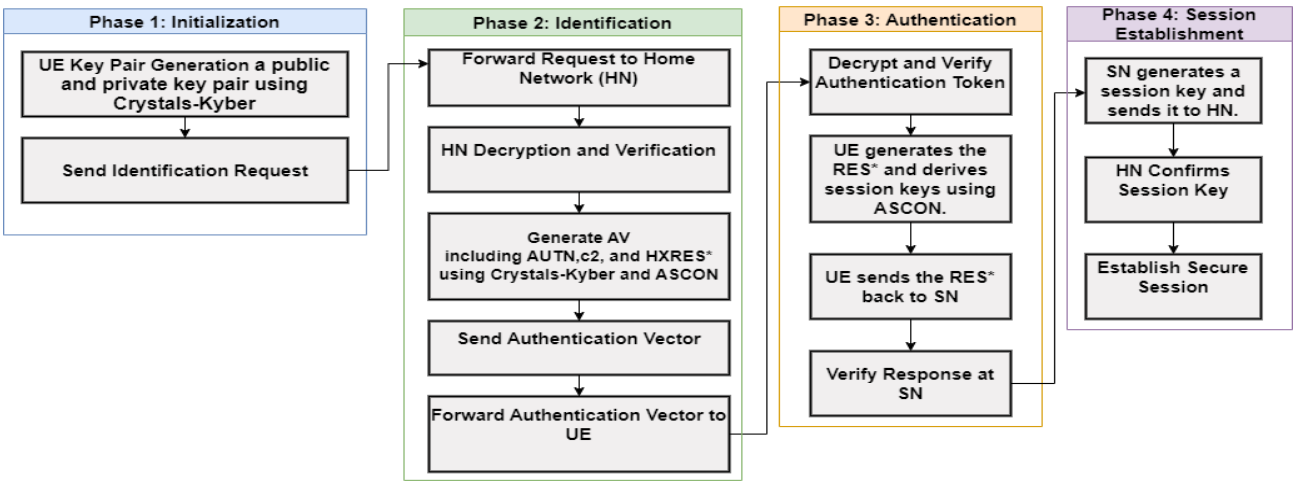


**Figure 4.** Proposed system phases

**Phase 1: The identification phase**

1) SN identification request to the UE.

2) Identification response from UE:

- At the UE, generate public key and private key $(PK_{UE}, SK_{UE})$ using Crystals-Kyber:

$$Kyber.Gen() \rightarrow (PK_{UE}, SK_{UE})$$

- Encapsulate the shared secret key $(K_s1)$ and HN's public key $(PK_{HN})$ using Crystals-Kyber:

$$Kyber.Encaps(PK_{HN}) \rightarrow (C_1, K_s1)$$

- UE side encrypt SUPI using ASCON by use $K_s1$

$$SUCI \rightarrow E_{K_S1}(SUPI||PK_{UE}||ID_{SN})$$

- Compute the MAC tag using HMAC:

$$MAC_{UE} = HMAC(K_s1, SUCI)$$

- Sends $(C_1, SUCI, MAC_{UE}, ID_{HN})$ to SN

3) Message from SN to HN:

- After the SN has received the message from the UE, it forwards $(C_1, SUCI, MAC_{UE}, ID_{HN})$

4) Identification at HN:

- The HN decapsulate $C_1$, to retrieve $K_s1$:

$$Kyber.Decaps(C_1, SK_{HN}) \rightarrow K_s1$$

- The HN decrypts SUCI and verify the MAC

$$Dec_{K_S1}(SUCI) \rightarrow (SUPI, PK_{UE}, ID_{SN})$$
$$Verify\ MAC_{UE} = HMAC\ (SUCI, K_S1)$$

**Phase 2: Authentication Phase**

After a successful MAC check at the HN, the HN uses SUPI to get UE's long-term key K based on SUPI, derive the key $K_{S2}$ and ciphertext $C_2$ with the correct KEM encapsulation algorithm and $PK_{UE}$

**1)** Authentication Vector Generation:

- The HN makes use of these steps to compute an authentication vector:

$$(C_2, Ks2) \leftarrow Kyber.Encaps(PK_{UE})$$
$$CK = ASCON(K, Ks2)$$
$$IK = ASCON(K, Ks2)$$
$$MAC = ASCON - MAC\ (K, Ks2, RSN)$$
$$AUTN = ASCON - Enc(K, Ks2, RSN) \parallel MAC$$
$$HXRES^* = SHA256(RSN, XRES^*)$$
$$K_{AUSF} = ASCON - KDF(CK, IK, Ks2)$$
$$K_{AUSF} = ASCON - KDF(K_{AUSF})$$
$$M = ASCON - Enc(K3, SUPI)$$

**2)** Message Transmission:

HN sends AUTN,HXRES*,M, and $C_2$ to SN , which then forward AUTN and $C_2$ to the UE.

**3)** Response from the UE:

- The UE decapsulates $C_2$ to obtain $K_S2$

$$Kyber.Decaps(C_2, SK_{UE}) \rightarrow K_S2$$

- The UE compute the response and key materials:

$$RES = ASCON - MAC(K, K_S2)$$
$$K_{AUSF} = ASCON - KDF(CK, K1, K_S2)$$
$$K_{SEAF} = ASCON - KDF(K_{AUSF})$$

- The UE sends RES* to the SN.

**4)** Verification at SN:

- The SN verification the response:
  $Verify\ SHA256(RES^*, RSN) = HXRES^*$
- If the verification is successful, SN computes

$$K3 = RES^* \oplus f_5(K, K_S2)$$

And decrypts M to obtain the SUPI and $K_{SEAF}$.

By meticulously following these instructions, the 5G-AKA protocol can be improved with post-quantum security by using Crystals-Kyber and low-cost cryptographic efficiency using ASCON, making it a viable solution for future 5G networks (Figure 5). To explain more details, the following pseudocode is provided.

**KyberPQ-AKA Protocol Process**

**Input**: SUCI/GUTI from UE
**Output**: Authentication result (Success/Failure), SUPI, Derived Keys
**Step 1: UE Initialization**
UE generates Crystals-Kyber key pair:
(PKUE,SKUE) = Kyber.KeyGen()
UE sends SUCI/GUTI and PKUE to SN over an insecure channel.
UE → SN: Send (SUCI/GUTI, PKUE)
**Step 2: SN Forwards Request to HN**
SN forwards SUCI/GUTI and PKUE to HN over a secure channel.
SN → HN: Send (SUCI/GUTI, PKUE)
**Step 3: HN Generates Shared Secret and Keys**
HN performs Crystals-Kyber encapsulation:
(Kshared,CKYBER) = Kyber.Encapsulate(PKUE)
HN generates random challenge R.
HN computes:MAC = ASCON MAC(Kshared,R) AUTN = (R,MAC,CKYBER)
HN derives keys using KDF:
KSEAF = KDF(Kshared,SEAF Context)
KAMF = KDF(KSEAF,AMF Context)
KNASenc = KDF(KAMF,NASenc Context) KNASint = KDF(KAMF,NASint Context)
KRRCenc = KDF(KSEAF,RRCenc Context)
KRRCint = KDF(KSEAF,RRCint Context)
KUPenc = KDF(KSEAF,UPenc Context)
HN → SN: Send AUTN
**Step 4: SN Sends Challenge to UE**
SN sends AUTN to UE.
SN → UE: Send AUTN
**Step 5: UE Processes AUTN and Derives Keys**
UE performs Crystals-Kyber decapsulation:
Kshared = Kyber.Decapsulate(SKUE,CKYBER)
UE computes:
MAC′ = ASCON MAC(Kshared,R)

UE verifies:
if MAC′ == MAC then
UE derives keys:
KSEAF = KDF(Kshared,SEAF Context)
KAMF = KDF(KSEAF,AMF Context)
KNASenc = KDF(KAMF,NASenc Context) KNASint = KDF(KAMF,NASint Context)
KRRCenc = KDF(KSEAF,RRCenc Context)
KRRCint = KDF(KSEAF,RRCint Context)
KUPenc = KDF(KSEAF,UPenc Context) UE sends Authentication Response to SN.
UE → SN: Send AuthenticationResponse
else
Authentication failure; UE aborts the procedure.
UE → SN: Send AuthenticationFailure end if

**Step 6: SN Forwards Response to HN**

SN forwards the UE's response to HN.
SN → HN: Forward AuthenticationResponse or AuthenticationFailure

**Step 7: HN Verifies UE's Response**

if Response is Authentication Response then
Authentication successful.
HN sends SUPI and derived keys to SN.
HN → SN: Send (SUPI, Derived Keys)
SN acknowledges to UE.
SN → UE: Send Authentication Accept
else
Authentication failure.
HN notifies SN of the failure.
HN → SN: Send AuthenticationFailure
SN informs UE.
SN → UE: Send AuthenticationReject
end if

**Step 8: Secure Communication Using Derived Keys**

After successful authentication, UE and SN use derived keys for secure communication:
1. Use KNASenc for NAS message encryption with ASCON.
2. Use KNASint for NAS message integrity protection with ASCON.
3. Use KRRCenc and KRRCint for RRC message encryption and integrity.
4. Use KUPenc for user plane data encryption.

**End**

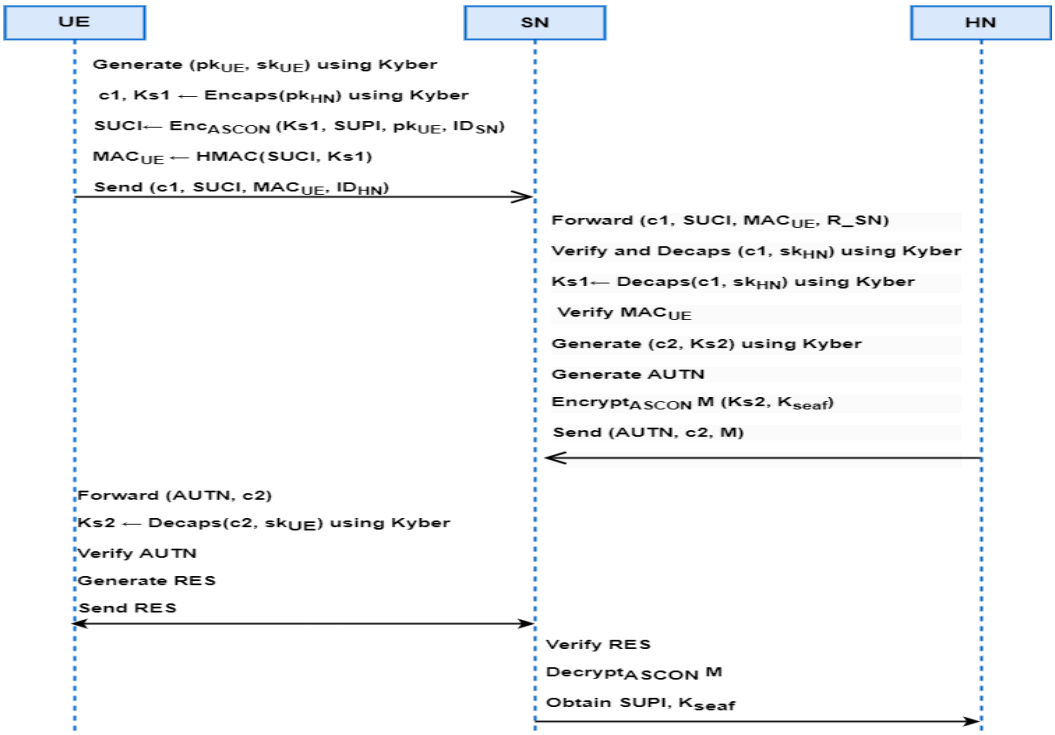


**Figure 5.** Proposed system with 5G-AKA process

## 5. RESULTS AND DISCUSSION

The KyberPQ-AKA proposed protocol was implemented in the Ubuntu 22.04 Environment Using Python, Mininet emulator, and Ryu controller for communication between user devices (UE), service network (SN), and home network (HN). The integration of Crystals-Kyber and ASCON into the 5G-AKA protocol aims to enhance security and efficiency. Here, we present the results of our assessment and discuss the implications.

### 5.1 Key generation and encryption/decryption times

Table 1 below shows the difference between Crystals-Kyber KEM performance times in terms of key generation, encapsulation, and decryption. The unit of time measurement is Seconds.

Through the above results, Crystals-Kyber proves its efficiency in key generation and wrapping/unwinding times. Keys are quantitative, resistant to attacks, and difficult to predict even in quantum devices, making them suitable for

real-time applications in 5G networks and beyond generations. Performance metrics indicate that the Kyber512 offers the fastest overall times, which helps in scenarios that require fast key exchanges.

**Table 1.** Evaluation time of Crystals-Kyber

| Algorithms | KeyGen Time | Encrypt Avg Time | Decrypt Avg Time |
|---|---|---|---|
| **Kyber512** | 0.006 | 0.010 | 0.015 |
| **Kyber 768** | 0.111 | 0.016 | 0.025 |
| **Kyber1024** | 0.018 | 0.024 | 0.037 |

### 5.2 Communication and account costs

We will make a simple comparison between our application of the standard 5G-AKA protocol and KyberPQ-AKA protocol based on Kyber in terms of connection and calculation costs comparison (see Table 2). The use of Crystals-Kyber has significantly reduced the calculation times while maintaining or improving security.

The results showed that the proposed protocol using Crystals-Kyber outperformed the standard 5G-AKA protocol, especially in key generation and encapsulation/decapsulation times. This optimization is important for reducing latency in 5G networks.

**Table 2.** Comparison between 5G-AKA and KyberPQ-AKA

| Metric | 5G-AKA | Proposed (KyberPQ-AKA) |
|---|---|---|
| **Key Generation (ms)** | 0.180 | 0.006 |
| **Encapsulation (ms)** | 0.180 | 0.010 |
| **Decapsulation (ms)** | 0.180 | 0.015 |
| **Communication Overhead** | Moderate | Low |
| **Computation Overhead** | High | Low |

### 5.3 ASCON efficiency and safety

The process of replacing ASCON in the 5G Protocol-AKA instead of AES includes a merge process in all cases where AES was used in the protocol, and this process includes:

Encryption and decryption: Messages that are pre-encrypted using AES are encrypted using ASCON, which improves the speed of the encryption process and reduces the computational burden on the devices.

1) Replacing ASCON with AES in the 5G-AKA protocol leads to several important benefits:
2) Computational efficiency: The main benefit of ASCON's lightweight design is reducing the time required for encryption operations and speeding up the overall authentication process. This is especially important in scenarios involving many IoT devices that need fast and secure authentication.
3) Enhanced protection: using ASCON, the protocol becomes better equipped to face current and future security threats, including those that arise because of quantum computing developments.
4) Reducing energy consumption is a major design goal of ASCON due to its importance for devices with batteries in IoT networks. Low energy consumption extends the operational life of devices and achieves more sustainable networks.

Replacing AES with ASCON in the 5G Protocol-AKA addresses current vulnerabilities. It improves protocol performance and security, making it more suitable for the next generation of mobile networks and IoT applications. ASCON's use of encryption also enhances protocol security by providing lightweight and efficient encryption, suitable for resource-limited devices in IoT environments.

Table 3 shows five coding tests based on the values of the input parameters in the MILENAGE algorithm. The Opc, KC, and Sres values generated by ASCON differ from those generated by AES, which may indicate that ASCON has different ways of encrypting data, and this increases security by increasing randomness and reducing the chances of predicting the output through its calculation in entropy and avalanche effect for keys. This difference in values reflects improvements in system security, as ASCON provides increased randomness and unpredictable encryption values, thereby reducing the predictability of the output and making it more difficult for attackers to manipulate the algorithm.

ASCON is characterized by its ability to provide a high level of security in multiple scenarios, especially when complexity and randomness of outputs are important factors and in environments that require resource efficiency.

**Table 3.** Keyset of MILENAGE with AES and ASCON

| | AES | ASCON |
|---|---|---|
| | **Keyset # 1** | |
| **Ki** | Abcdefabcdefabcdefabcdefabcdefab | abcdefabcdefabcdefabcdefabcdefab |
| **Op** | 00112233445566778899aabbccddeeff | 00112233445566778899aabbccddeeff |
| **Rand** | 1234567890abcdef1234567890abcdef | 1234567890abcdef1234567890abcdef |
| **Opc** | f0d19e87e63e84f2eb278659424b1f7d | 92fa116ea8588a5b275173b0c1d61361 |
| **Kc** | 34e67ebc652ef342 | 3e8dd9c3dcdeff41 |
| **Sres** | f1b19d87 | 2dc2fb2a |
| | **Keyset # 2** | |
| **Ki** | 00112233445566778899aabbccddeeff | 00112233445566778899aabbccddeeff |
| **Op** | a1b2c3d4e5f60718293a4b5c6d7e8f90 | a1b2c3d4e5f60718293a4b5c6d7e8f90 |
| **Rand** | 0f1e2d3c4b5a69788796a5b4c3d2e1f0 | 0f1e2d3c4b5a69788796a5b4c3d2e1f0 |
| **Opc** | bd020590b106a8aef625767edbe37b38 | 361a5ac4f2edb2c3b89b95d876c9c973 |
| **Kc** | 9480c2d08cf1dcf1 | b4de4df4d4295555 |
| **Sres** | 0841d9fd | f26627ef |
| | **Keyset # 3** | |
| **Ki** | 1234567890abcdef1234567890abcdef | 1234567890abcdef1234567890abcdef |
| **Op** | 1a2b3c4d5e6f708192a3b4c5d6e7f809 | 1a2b3c4d5e6f708192a3b4c5d6e7f809 |
| **Rand** | Abcdefabcdefabcdefabcdefabcdefab | abcdefabcdefabcdefabcdefabcdefab |

| | | |
|---|---|---|
| **Opc** | 2dfd93e592a7a8d60fc77427199887f4 | 3ec7c4c3636576d0e4a1b050ea1476d8 |
| **Kc** | 850d417dad3c4c81 | 41df7367af65ee34 |
| **Sres** | 3e7eca85 | c0e89045 |
| | **Keyset #4** | |
| **Ki** | Abcdefabcdefabcdefabcdefabcdefab | abcdefabcdefabcdefabcdefabcdefab |
| **Op** | 0f0e0d0c0b0a09080706050403020100 | 0f0e0d0c0b0a09080706050403020100 |
| **Rand** | feedc0ffee1234567890abcdef123456 | feedc0ffee1234567890abcdef123456 |
| **Opc** | 257189f0220d73d1d28f266f04223de3 | b643bf54f64122dd1d4866b3035f2d54 |
| **Kc** | b8f50b844ab180d0 | e5efb1a62940fe74 |
| **Sres** | 6127a4dd | 15bc6905 |
| | **Keyset #5** | |
| **Ki** | feedc0ffee1234567890abcdef123456 | feedc0ffee1234567890abcdef123456 |
| **Op** | deadbeefcafe1234567890abcdefabcd | deadbeefcafe1234567890abcdefabcd |
| **Rand** | 0a0b0c0d0e0f0102030405060708090a | 0a0b0c0d0e0f0102030405060708090a |
| **Opc** | 3d8e0adb1f9c5d4a98a9f84399473244 | d30f43cce6914c9a659de220975e9c1e |
| **Kc** | 28cb47090b2df818 | 6350c6e7d930ce25 |
| **Sres** | 013ec371 | 35959210 |

Table 4 shows five coding tests based on the values of the input parameters in the MILENAGE algorithm. The "opc" values differ between the two tables, reflecting the different cryptographic processes used to deduce them. The values of kc and SREs also differ between the tables due to the different cryptographic primitives used in the MILENAGE algorithm. The change in the encryption algorithm affects the generation of these values. The same key combinations (ki, op, and Rand) remain the same across both tables. However, encryption produces different results for `opc,`` KC,` and 'SREs' due to different underlying algorithms (AES vs. ASCON). The table shows how the choice of primitive encryption can affect the output in an authentication protocol and key agreement such as 5G-AKA.

Table 4 shows the performance metrics when applying the AES algorithm within the MILENAGE in the standard version of the 5G-AKA protocol, one of the most used algorithms in modern data encryption systems.

Table 5 illustrates the performance metrics when applying the ASCON algorithm. This lightweight encryption algorithm enhances network efficiency, particularly in energy-constrained environments. Our proposed methodology utilizes it as an alternative to traditional encryption in the adaptive KyberPQ-5G-AKA protocol.

**Table 4.** Evolution metrics of MILENAGE with AES

| Evolution Metrics | Value |
|---|---|
| Time | 0.000427Sec |
| Memory usage: Current | 0.001257MB |
| Memory usage: Peak | 0.004346MB |
| Entropy of OPC | 4.0000bits |
| Avalanche effect | 44.53% change |

**Table 5.** Evolution metrics of MILENAGE with ASCON

| Evolution Metrics | Value |
|---|---|
| Time | 0.008224 Sec |
| Memory usage: Current | 0.000161MB |
| Memory usage: Peak | 0.003093MB |
| Entropy of OPC | 3.7500bits |
| Avalanche effect | 50.00% change |

### 5.4 Security validation using ProVerif

The security of the proposed protocol has been validated using ProVerif, the official verification tool. ProVerif allows the analysis of security characteristics such as confidentiality, authenticity, and integration within encryption protocols. The analysis of ProVerif confirmed that the proposed protocol with Crystals-Kyber and ASCON shows strong resistance to various types of attacks:

Confidentiality: Crystals-Kyber's use ensures that the subscription identifier (SUPI) remains confidential and protected by quantum-resistant key wrapping mechanisms.

Authenticity: ASCON integration provides strong message authentication, ensuring the integrity and authenticity of messages exchanged during the authentication process.

Integrity: ProVerif confirmed that the protocol maintains data integrity by preventing unauthorized modifications. Table 5 summarizes the evolution metrics of MILENAGE with ASCON. Table 6 provides the security features validated by ProVerif, including confidentiality, integrity, and authenticity. Figure 6 shows the standard version of the 5G-AKA protocol, and Figure 7 shows the verification of the KyberPO-AKA protocol.

**Table 6.** Security features validated by ProVerif

| Security Feature | Result |
|---|---|
| Confidentiality | Achieved (Quantum-safe) |
| Authenticity | Achieved |
| Integrity | Achieved |
| Resistance to Link Attacks | Achieved |
| Resistance to Replay Attacks | Achieved |
| Forward Secrecy | Achieved |

The proposed improved protocol provides a higher level of security than the standard protocol, as it prevents attacks from accessing keys and identities. This makes it the ideal option for use in environments that require high security, as shown in Figures 6 and 7.

The results of the performance evaluation and security checks show that the proposed protocol provides a significant improvement in protection and efficiency due to several main things, as follows:

The proposed protocol generates keys faster, encrypts more, and decrypts more than the standard 5G-AKA protocol version. This reduces latency and improves the user experience in 5G networks, thereby improving performance.

The use of quantum-resistant Crystals-Kyber provides long-term security for the complex mathematical operations used in it and the key distribution process, reliably without sending data that could be intercepted. ASCON adds additional layers of security through strong encryption and authentication capabilities, thereby providing enhanced security.

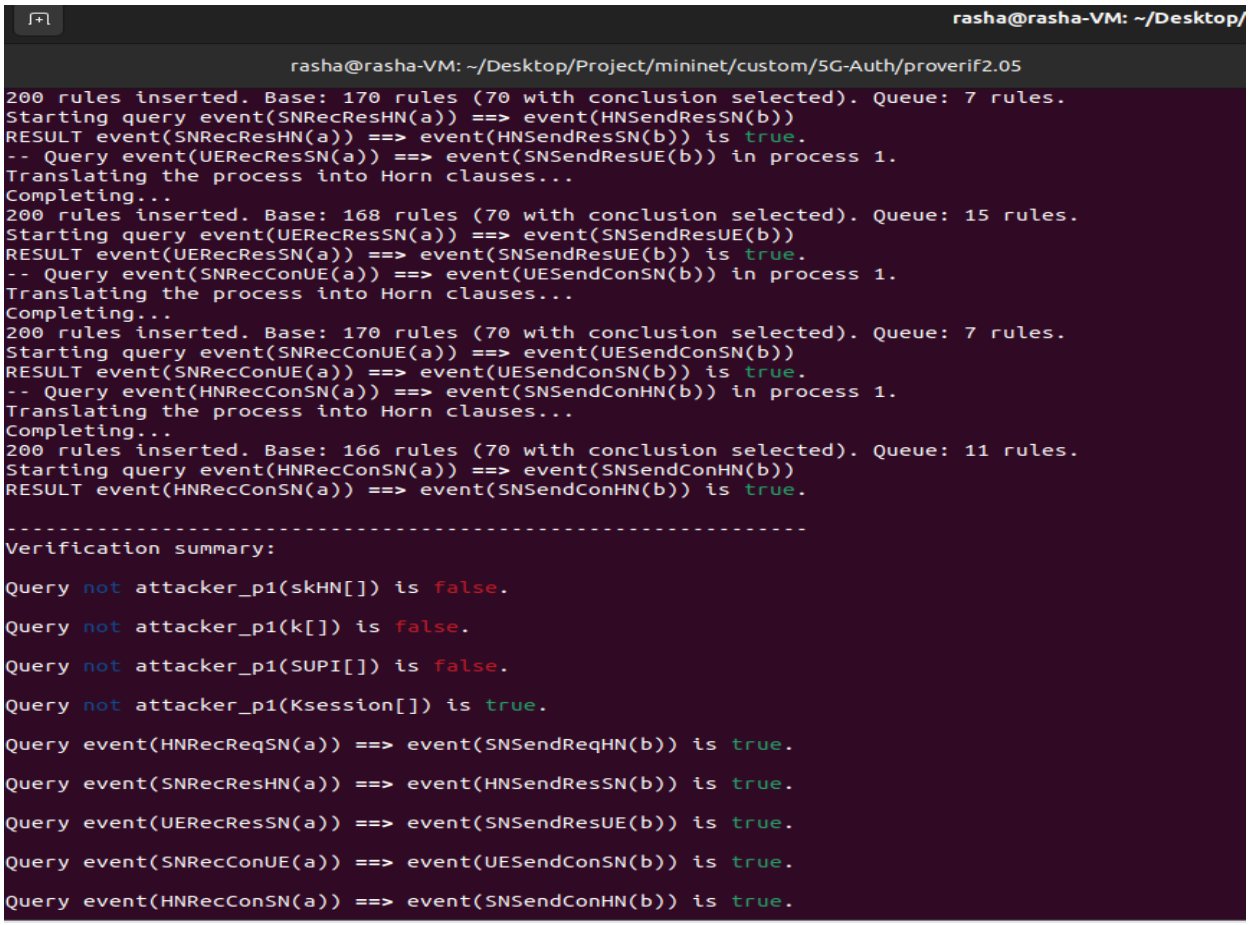


**Figure 6.** Evaluation of 5G-AKA protocol

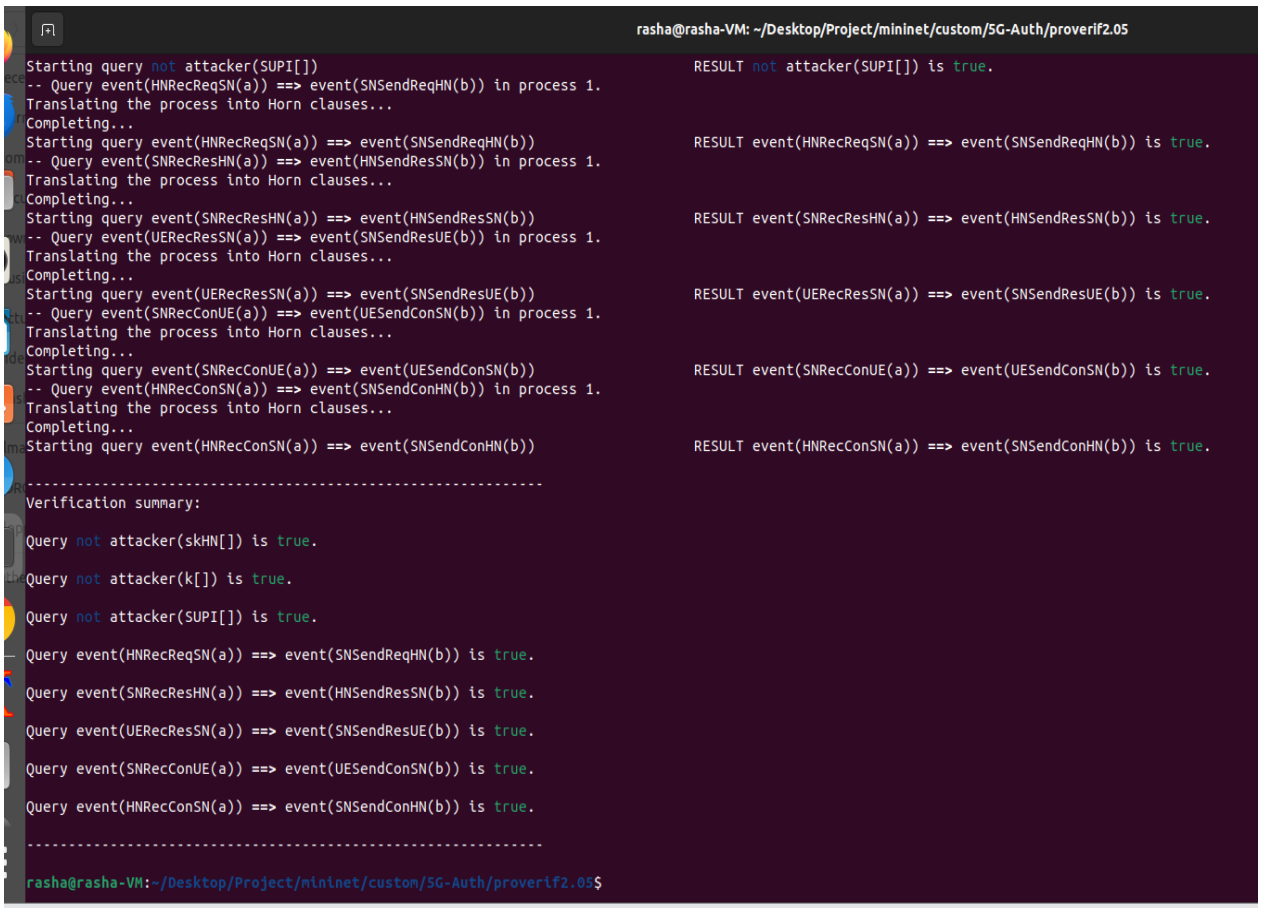


**Figure 7.** Evaluation of KyberPQ-AKA protocol.

Reduces low energy consumption by using ASCON, which reduces energy for battery-powered devices, which contributes to extending the life of the device and more sustainable operations, thereby providing energy efficiency

The efficiency of the protocol and the low computational load make it suitable for large deployments, including huge IoT networks and the comprehensive infrastructure of the fifth-generation network, and thus provide the required scalability of networks

Using Crystals-Kyber and ASCON, improvements to the 5G-AKA protocol provide a viable solution in the future for fifth-generation networks and beyond, addressing current vulnerabilities while being prepared for future security challenges, especially with the adoption of a quantum method in key generation and distribution. It also improves performance and energy efficiency, making it suitable for a wide range of applications in next-generation communication systems.

In this summary of the proposal, the main results achieved through the development of an improved security model for the fifth generation of communication networks (5G) to counter various cyberattacks were highlighted. Utilizing encryption methods that are resistant to quantum attacks, such as Crystals-Kyber, and light encryption methods, such as ASCON, has improved the current authentication protocol known as 5G-AKA. The improvements made in this work have proven their ability to enhance security and privacy in the fifth generation of networks, which has proven to improve several aspects, including

1). Mutual authentication between the user's device and the network: using Crystals-Kyber, which relies on the KEM method, addressed this problem by indirectly exchanging keys, as well as a way to authenticate the parties to make sure that the network the user is connected to is the real network, as well as making sure that the user's identity is the truth and not fake.

2). Authentication and key exchange using Crystals-Kyber have been optimized to provide long-term security against quantum attacks, especially after using the LWE concept.

3). Improved speed and performance: The results showed that the developed protocol is superior to the traditional protocol in encryption speed and reduced resource consumption. Due to the use of the ASCON lightweight encryption algorithm, it is suitable for devices with limited capabilities, such as Internet of Things (IoT) devices.

4). Optimize energy consumption: The study showed that the use of light algorithms such as ASCON has contributed significantly to reducing energy consumption, which enhances the network's energy efficiency.

As the limitation of proposed:

Adaptation of the post-quantum concept to the AKA-5G network due to the high rate of data transmission and for scheduling and synchronization.

Information leaks in 5G network programming and architecture due to the complex programming and API abstraction level.

The complex post-quantum algorithms concepts and mathematical modeling make them a new trend in 5G by NIST. They include new nonlinear equations and specific requirements for hardware and programming, especially for 5G networks.

## 6. CONCLUSION

Despite 3GPP's great emphasis on subscriber privacy, it was necessary to modify the 5G Protocol AKA to address inherited structural gaps. These parameters should be optimized to operate in a fast and lightweight environment for low-level devices. To address this problem in immunity, we have proposed an improved protocol that uses ASCON to encrypt communications between UE and SN and based Crystals-Kyber to key encapsulation and agreement. The integration of Crystals-Kyber and ASCON into the 5G-AKA protocol significantly enhances security and efficiency, as explained in the paragraph results. Crystals-Kyber provides powerful protection against quantum attacks with low latency on major exchanges. Thanks to its lightweight design, ASCON offers improved computational efficiency and lower power consumption. These improvements make the proposed protocol a viable solution for future fifth-generation networks, especially in environments with high-security requirements and resource-limited hardware. A formal analysis of the standard protocol was also conducted with the proposed protocol. The proposed version proved its superiority in complete resistance against possible attacks, as the attacker was unable to access any of the keys or identity. In contrast, the standard protocol showed that it suffers from weaknesses, as the attacker was able to access the secret key, internal key, and identity. However, the attacker could not get to the session.

## REFERENCES


[1] Prasad, A.R., Arumugam, S., Sheeba, B., Zugenmaier, A. (2018). 3GPP 5G security. Journal of ICT Standardization, River Publishers, 6(1-2): 137-158. https://doi.org/10.13052/jicts2245-800X.619

[2] ETSI, T. (2018). 133 501 V15.2.0, 5G: Security architecture and procedures for 5G system (3GPP TS 33.501 version 15.2.0, Release 15). https://www.etsi.org/deliver/etsi_ts/133500_133599/133501/15.02.00_60/ts_133501v150200p.pdf.

[3] Manaa, M.E., Hussain, S.M., Alasadi, S.A., Al-Khamees, H.A. (2024). DDoS attacks detection based on machine learning algorithms in IoT environments. Inteligencia Artificial, 27(74): 152-165. https://doi.org/10.4114/intartif.vol27iss74pp152-165

[4] Tang, Q., Ermis, O., Nguyen, C.D., De Oliveira, A., Hirtzig, A. (2022). A systematic analysis of 5g networks with a focus on 5g core security. IEEE Access, 10: 18298-18319. https://doi.org/10.1109/ACCESS.2022.3151000

[5] Al-Ameer, A.A., Bhaya, W.S. (2023). Intelligent intrusion detection based on multi-model federated learning for software defined network. International Journal of Safety & Security Engineering, 13(6): 1135-1141. https://doi.org/10.18280/ijsse.130617

[6] Wang, Y., Zhang, Z., Xie, Y. (2021). Privacy-preserving and standard-compatible AKA protocol for 5G. In 30th USENIX Security Symposium (USENIX Security 21), USENIX Association, August, pp. 3595-3612. https://www.usenix.org/conference/usenixsecurity21/presentation/wang-yuchen.

[7] Hernández, C., Cervelló-Pastor, C. (2019). Lightweight testbed for machine learning evaluation in 5G networks. In JITEL 2019 – XIV Jornadas de Ingeniería Telemática, Zaragoza, Spain: Proceedings Book, pp. 1-6. http://hdl.handle.net/2117/185190.

[8] Basin, D., Dreier, J., Hirschi, L., Radomirovic, S., Sasse, R., Stettler, V. (2018). A formal analysis of 5G authentication. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, pp. 1383-1396. https://doi.org/10.1145/3243734.3243846

[9] Koutsos, A. (2019). The 5G-AKA authentication protocol privacy. In 2019 IEEE European Symposium on Security and Privacy (EuroS&P), Stockholm, Sweden, pp. 464-479. https://doi.org/10.1109/EuroSP.2019.00041

[10] Sakamoto, K., Liu, F., Nakano, Y., Kiyomoto, S., Isobe, T. (2022). Rocca: An efficient AES-based encryption scheme for beyond 5G (full version). Cryptology ePrint Archive. https://doi.org/10.46586/tosc.v2021.i2.1-30

[11] Abd El-Latif, A.A., Abd-El-Atty, B., Mazurczyk, W., Fung, C., Venegas-Andraca, S.E. (2020). Secure data encryption based on quantum walks for 5G internet of things scenario. IEEE Transactions on Network and Service Management, 17(1): 118-131. https://doi.org/10.1109/TNSM.2020.2969863

[12] Xiao, Y., Wu, Y. (2022). 5G-IPAKA: An improved primary authentication and key agreement protocol for 5G networks. Information, 13(3): 125. https://doi.org/10.3390/info13030125

[13] Cremers, C., Dehnel-Wild, M. (2019). Component-based formal analysis of 5G-AKA: Channel assumptions and session confusion. In Network and Distributed System Security Symposium (NDSS), Internet Society, San Diego, CA, USA. http://doi.org/10.14722/ndss.2019.23394

[14] Rellstab, A. (2019). Formalizing and verifying generations of AKA protocols (Master's Thesis, ETH Zurich). https://doi.org/10.3929/ethz-b-000372339

[15] Xiao, Y., Gao, S. (2022). Formal verification and analysis of 5G AKA protocol using mixed strand space model. Electronics, 11(9): 1333. https://doi.org/10.3390/electronics11091333

[16] Xiao, Y., Gao, S. (2022). 5GAKA-LCCO: A secure 5G authentication and key agreement protocol with less communication and computation overhead. Information, 13(5): 257. https://doi.org/10.3390/info13050257

[17] Cho, S., Yeom, C., Won, Y. (2021). Implementation of efficient 5G AKA protocol for light-weight environment. *Sustainability*, 13(16): 8982. https://doi.org/10.3390/su13168982

[18] Joudah, R.H., Manaa, M.E. (2024). Implementing of 5G authentication and key agreement protocol: Practical security measures. In 2024 21st International Multi-Conference on Systems, Signals & Devices (SSD), Erbil, Iraq, pp. 735-744. https://doi.org/10.1109/SSD61670.2024.10549167

[19] Avanzi, R., Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J.M., Schwabe, P., Seiler, G., Stehlé, D. (2019). CRYSTALS-Kyber algorithm specifications and supporting documentation. NIST PQC Round, 2(4): 1-43. https://pq-crystals.org/kyber/data/kyber-specification-round3-20210131.pdf.

[20] Richter, M., Bertram, M., Seidensticker, J., Tschache, A. (2022). A mathematical perspective on post-quantum cryptography. Mathematics, 10(15): 2579. https://doi.org/10.3390/math10152579

[21] Dobraunig, C., Eichlseder, M., Mendel, F., Schläffer, M. (2021). Ascon v1.2: Lightweight authenticated encryption and hashing. Journal of Cryptology, 34: 1-42. https://doi.org/10.1007/s00145-021-09398-9

[22] Dobraunig, C., Eichlseder, M., Mendel, F., Schläffer, M. (2015). Cryptanalysis of Ascon. In Topics in Cryptology – CT-RSA 2015: The Cryptographer's Track at the RSA Conference 2015, San Francisco, CA, USA, pp. 371-387. https://doi.org/10.1007/978-3-319-16715-2_20