Penerbit Akademia Baru

Journal of Advanced Research Design

Journal homepage:
https://akademiabaru.com/submit/index.php/ard
ISSN: 2289-7984

Enhancing Secure 5G-AKA Protocol using ASCON Lightweight Cryptography

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

[1] Department of Information Networks, College of IT, University of Babylon, Hillah, Babylon, Iraq
[2] Intelligent Medical System Department, College of Sciences, Al-Mustaqbal University, Babylon, Iraq

ARTICLE INFO

Article history:
Received 2 February 2025
Received in revised form 30 June 2025
Accepted 10 July 2025
Available online 20 July 2025

Keywords:
5G-AKA; 5G authentication; ASCON; lightweight encryption; 5G security

ABSTRACT

With the rapid development of communication generations and fifth generation (5G) networks, network security issues have become more prominent and mutual authentication between users and networks has become crucial to protect privacy and prevent cyber-attacks. Authentication has evolved from previous generations such as GSM, CDMA, UMTS and LTE to 5G, which relies on protocols such as 5G-AKA and EAP-AKA'. The 5G-AKA protocol is one of the most important authentication protocols for securing 3GPP equipment, but it faces security challenges such as Link attacks. 5G-AKA is constantly being improved to support forward secrecy and address security attacks, requiring new improvements to mitigate these challenges. This paper proposes to apply a lightweight algorithm, the ASCON algorithm, to replace the AES used in the 5G-AKA standard that performs encryption and additional authentication simultaneously, which enhances the efficiency and strong security of the exchange of authentication parameters between UE and HN. The protocol was implemented using a Mininet and Python network emulator to integrate the algorithm within a 5G network architecture. Evaluation metrics based on NIST criteria, such as memory usage (current and peak), entropy and avalanche effect, showed a clear performance improvement compared to the previous protocol version using AES.

1. Introduction

As the latest generation of mobile communication technology, 5G communication networks aim to provide higher speed and capacity for communication between mobile devices and can customize network functions according to business scenarios through network slicing functions, such as for Internet of Vehicles scenarios. Low-latency transmission is required and high bandwidth is required

* *Corresponding author*
E-mail address: mahdi.ebadi@uomus.edu.iq

https://doi.org/10.37934/ard.139.1.201217

for streaming media services. To realize the above functions, the 5G core network adopts a Service Based Architecture (SBA) according to Ji *et al.,* [1]. SBA splits the network elements and all network elements are connected to the system through interfaces, so that the services of the 5G core network run at a finer granularity than traditional network elements and are loosely coupled to each other, allowing the upgrade of individual services. The impact on other services is minimal, which makes the configuration, expansion and upgrade of the core network more convenient. Compared with 4G networks, the 5G core network has a greater exposure surface, so the 5G core network faces many new security issues, as discussed by Manaa *et al.,* [2]. Among them, business security is a new security threat faced by the 5G core network.

The 5G core network architecture under the 3GPP standard is shown in Figure 1.

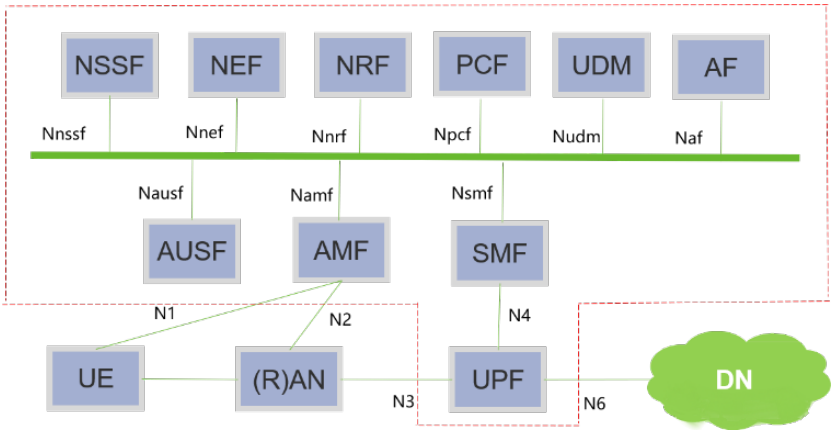

Fig. 1. 5G core network architecture

As mobile communication systems are used more and more widely in social life, especially as 5G further takes enterprise-level applications as its core application scenarios, security has become a factor that cannot be ignored in mobile communication systems including 5G, as highlighted by Ahmad *et al.,* [3].

As 5G technology continues to be promoted around the world, strong security measures are needed to defend against threats and ensure the integrity of the network, so the role of security is becoming increasingly important. The 5G security standards are defined by the key security standards organization for 5G-3rd Generation Partnership Project (3GPP) which is a collaboration of six telecommunication standardization organizations to develop global mobile telecommunications standards. 3GPP Depends on SA3 (Security Group) for Developing & Maintaining 3GPP Technologies Security Standards, Including European Telecommunications Standards Institute, Another Major Player in Defining Security Standards for 5G. 5G security standards from ETSI have also been produced, such as the NFV (Network Functions Virtualization) security standard (providing guidance for secure virtualized network functions and associated services).These include the GSMA security standards that apply to mobile network operators and 5G-ENS (5G Exchange Network Security) standard for critical infrastructure providers , as reported by Dutta *et al.,* [4], 3GPP [5] and Manaa *et al.,* [6].

Mobile users are connected to the mobile network through the universal subscriber identity module (USIM) card and both users and operators want to get security guarantees from the communication protocols used, such as the confidentiality of user voice and SMS. The authentication and key agreement (AKA) can realize mutual authentication between the user and operator networks, complete the work of negotiating session keys and establish a secure channel to ensure the security of subsequent communication and data transmission. Attackers may exploit security

vulnerabilities in communication protocols to launch attacks, which will seriously threaten personal privacy and property security as present, as demonstrated by Braeken *et al.,* [7]. The security of 5G communication is heavily dependent on the security of the 5G AKA protocol, so the security analysis of the 5G AKA protocol is particularly important, but the complexity of the protocol process makes it difficult to find its security vulnerabilities manually. In this paper, the security protocol verification tool Tamarin is used to conduct a formal analysis of the 5G AKA protocol in order to better find its security vulnerabilities, so as to promote the improvement and perfection of the protocol standard, so that the 5G AKA protocol can provide better security assurance for users and operators after the full commercialization of 5G networks , as noted by Liyanage *et al.,* [8].

The 5G AKA protocol is used to realize authentication and key negotiation between the user and the operator's network. The entities involved are user equipment (user equipment, UE), the service network (service network, SN) connected by the user in a short distance and the operator's home network (home network, HN) corresponding to the user. Because SN includes the security anchor function (the function of the security anchor, the assistance fund), the home network HN includes the authentication service function (the function of the authentication server, the type), the authentication certificate library and the processing function (the authentication credential storage library and the processing function, ARPF). This article introduces enhancing the 5G AKA protocol by implementing a highly efficient key agreement method tailored for the intricate 5G environment. To address the imperative need for swift encryption and decryption processes, we seamlessly integrated the ASCON algorithm, surpassing the capabilities of the conventional AES.

2. Related Works

The 5G-AKA protocol ensures the security of communications in a 5G network. However, previous studies have identified a security vulnerability in this protocol that allows for the disclosure and manipulation of user information through passive or active attacks. This vulnerability was present in previous versions of 5G and was not properly fixed. Researchers have attempted to rectify this vulnerability. Some of the proposed solutions require additional equipment or changes to the protocol's architecture, whereas others increase the load on devices or networks. Therefore, we will compare previous studies in terms of their contributions, application methods and results. Arapinis *et al.,* [9] used ProVerif to analyse the AKA protocol in 3G networks, found attacks on user location and identity anonymity and proposed corresponding solutions. Focusing on the encryption mechanism of sequence numbers, Borgaonkar *et al.,* [10] Using incomplete encryption of variables, an information decryption attack is cleverly designed. The attacker mainly plays the role of the decryption algorithm by collecting many authentication failure responses. Specifically, the attacker first makes the UE and HN repeatedly authenticate. and through information truncation and other means, the authentication results alternate between success and failure. Every time a failure response is obtained, the attacker will replay the outdated message to ensure that the result is of the resynchronization type, so-called "replay" It refers to sending the same message more than twice. After many repeated operations, the attacker can collect multiple re-step type failure responses. Then based on the characteristics of XOR calculation, the attacker uses an iterative method to calculate the sequence bit by bit. The binary encoding of the number. Finally, the attacker can infer the user's privacy, such as communication activities, geographical location, etc., based on changes in the deciphered encoding over a period.

In the era of 4G networks, Hussain *et al.,* [11] proposed a model-based testing method based on symbolic model checking and cryptographic protocol verification and used ProVerif to analyse the EPS AKA protocol in 4G networks and found authentication replay attacks and spoofing attacks on

user location, but did not propose specific defence measures. With the development of 5G technology, the coexistence of 4G network and 5G network has gradually formed and many researchers have begun to analyse the 5G AKA protocol. Ferrag *et al.,* [12] conducted a comprehensive study on authentication and privacy protection schemes in 4G and 5G networks and summarized the corresponding coping strategies and formal and non-formal security analysis techniques, which provided ideas for the future research direction of 5G network security.

In terms of formal analysis of the 5G AKA protocol, Basin *et al.,* [13] performed a formal analysis of the 5G AKA protocol using Tamarin. Based on 3GPP TS 33.501 v15.1.0 [14], the first formal model of the 5G AKA protocol is provided for the security objectives extracted from the 5G security standard, However, they modelled the AUSF and ARPF entities as one large HN entity, which cannot accurately describe the process of the 5G AKA protocol. Cremers *et al.,* [15], based on 3GPP TS 33.501 v0.7.0 [5], analysed the 5G AKA protocol by modelling AUSF and ARPF in HN as two separate participating entities and found an attack caused by session contention. However, the protocol version they analysed was older and they only partially analysed the authentication properties between UE, SN and HN. Edris *et al.,* [16], based on 3GPP TS 33.501 v15.5.0, used ProVerif to evaluate the security of the 5G AKA protocol but did not provide an effective solution to the identified problems.

Cao *et al.,* [17] designed a lightweight secure access authentication protocol for the concurrent connection of massive devices in 5G networks and used ProVerif and Scyther to formally analyse the protocol. Ouaissa *et al.,* [18] have also used AVISPA to perform a formal analysis of variant protocols related to the 5G AKA protocol. However, XOR operations in ProVerif are implemented through user-defined equations, limiting the security quality of the verification. Scyther and AVISPA cannot customize security properties and support few cryptographic operations. These tools have corresponding limitations in the formal analysis of the protocol.

At present, most formal analyses of the 5G AKA protocol by scholars are based on the R15 standard in the 5G technical specifications issued by 3GPP or earlier. The newly released R16 [19] and the latest R17 standard in the 5G technical specification (released in December 2020) differ only slightly in the 5G AKA protocol, with R17 adding only optional AKMA functions. Therefore, this paper refers to the protocol in the R17 standard v17.0.0 version and selects Tamarin, with built-in XOR and other operations, to comprehensively evaluate the impact of these modifications on protocol security.

The security of 5G connections is highly dependent on the 5G-AKA protocol. Previous studies using AES encryption have highlighted some weaknesses. Our paper presents the ASCON algorithm as a potential improvement over AES, with the aim of enhancing performance and strong security.

3. Methodology

3.1 5G-AKA Protocol Process

5G-AKA includes an initialization phase and a challenge-response phase. The overall process of 5G-AKA is shown in Figure 2.

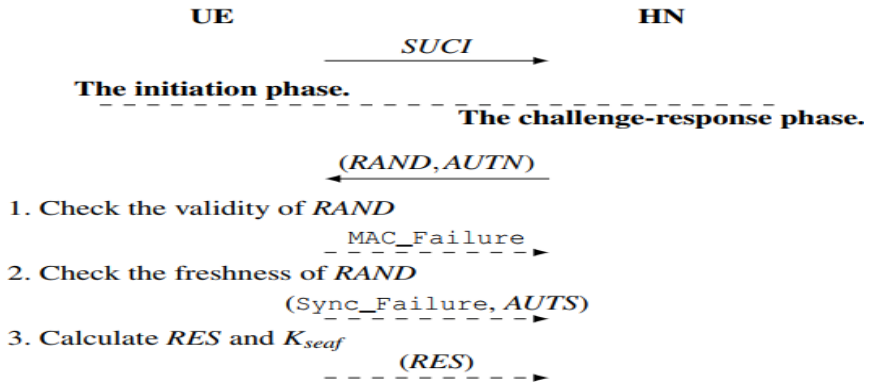

Fig. 2. 5G-AKA overall process

In the initialization phase, the UE uses the HN's public key and the ECIES encryption algorithm to encrypt the SUPI to obtain the SUCI and send it to the HN. In the challenge-response phase, HN randomly selects a challenge (RAND) and calculates AUTN (where AUTN includes MAC and hidden SQNHN). After receiving RAND and AUTN, first, the UE uses MAC to check the validity of the message. If the check fails, it returns a MAC_Failure message; next, the UE compares SQNHN and SQNUE to check the freshness of the message. If the check fails, the Sync_Failure and AUTS messages are returned. The UE uses the AUTS message to resynchronize with the HN; finally, when all checks pass, the UE calculates the response value RES and anchor Key K_{seaf} and sends the response value RES to HN , as discussed by Koutsos [20].

i. Initialization Phase: As shown in Figure 3, the contents in brackets below UE, SN and HN are known. During the initialization process, the UE side uses the ECIES component to encrypt and hide SUPI to obtain SUCI. This is also an improvement in privacy protection of the 5G system compared to the 3G/4G system. After getting the SUCI, the UE sends (SUCI, IDHN) to the SN. After receiving it, the SN adds its own IDSN and adds (SUCI, IDHN, IDSN), is sent to HN and HN restores SUCI to SUPI through the ECIES component. At this point, the initialization process is completed.

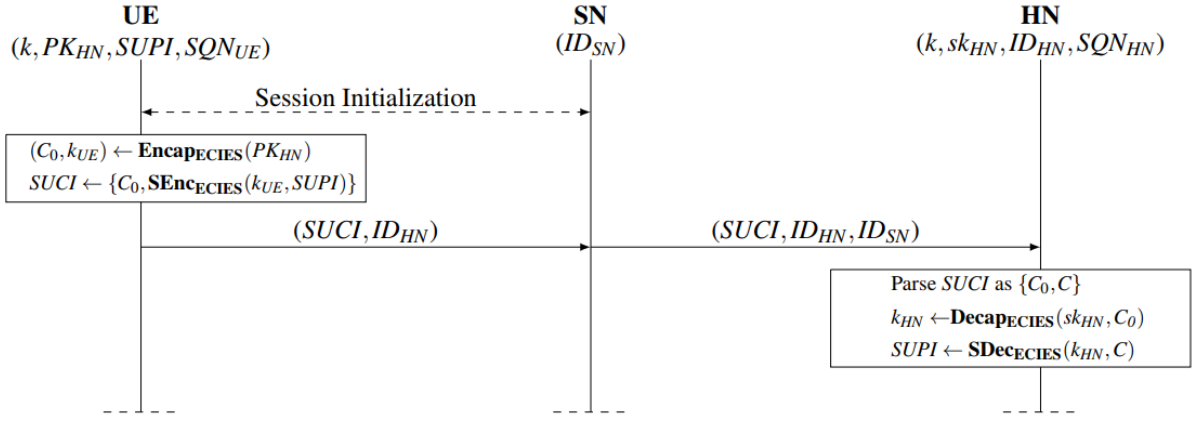

Fig. 3. Initialization phase of 5G-AKA

ii. Challenge-Response Phase: As shown in Figure 4, in the challenge-response phase, the UE and HN verify through a series of challenge-responses and establish an anchor key (i.e. Kseaf) with the SN. This phase includes TS 33.501. A series of encryption functions specified the following is a brief introduction to the challenge response process:

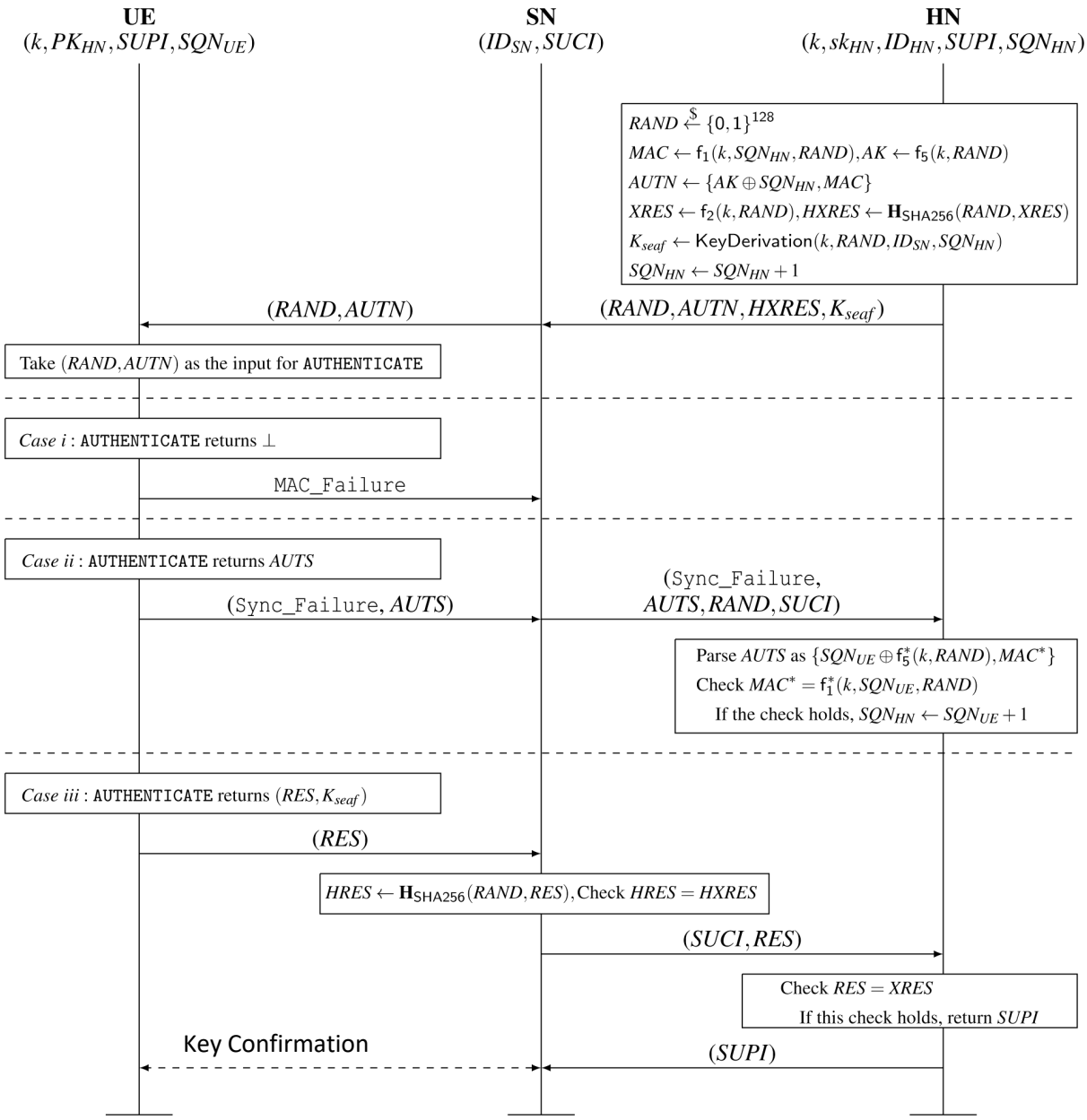

Fig. 4. Challenge-response phase in 5G-AKA

- After initialization, the HN generates an authentication quadruple (RAND, AUTN, HXRES, KSEAF). Details of this calculation are shown in Figure 4. RAND is a 128-bit random number, AUTN is an authentication token (including CONC and MAC, with CONC being AK XOR SQNHN) and HXRES is RAND hashed with XRES.
- The SN forwards (RAND, AUTN) to the UE.
- Upon receiving (RAND, AUTN), the UE splits AUTN into CONC and MAC, computes AK using shared key k and RAND, XORs AK with CONC to derive SQNHN and verifies MAC against received MAC.
- If MACs match and UE's SQN is less than HN's, authentication with HN succeeds. UE computes RES and KSEAF, sending RES to the SN for authentication.
- If MACs match but UE's SQN exceeds HN's, UE initiates resynchronization by sending a Sync_Failure message with AUTS to the SN.

- If MACs do not match, authentication fails and the SN receives a MAC_Failure message.
- The SN verifies RES by hashing it and comparing with HN's hash. Upon successful verification, the SN sends SUPI back to the HN, completing UE authentication.

These steps are detailed by Dehnel-Wild *et al.,* [21], Yadav *et al.,* [22] and Braeken [23].

3.2 MILENAGE

This section describes the algorithms used in the protocol. We provide a brief description of the purpose of using these algorithms and their basic principles. MILENAGE is a set of algorithms developed by the 3GPP Security Working Group for authentication and key generation. Although it is not an official standard because it is a kit provided in 3GPP, the protocol has been implemented using MILENAGE. It has seven encryption functions, f1, f1*, f2, f3, f4, f5 and f5*. Functions marked with * are synchronization functions that are used to check whether UE and HN have calculated the same values. The method of these functions is the same as with the original function. The first three functions (f1, f1* and f2) are authentication functions, while the remaining four functions (f3, f4, f5 and f5*) are functions used to create keys. As shown in Figure 5, we show how the f1 – f5 functions work in HN , as per ETSI [24].

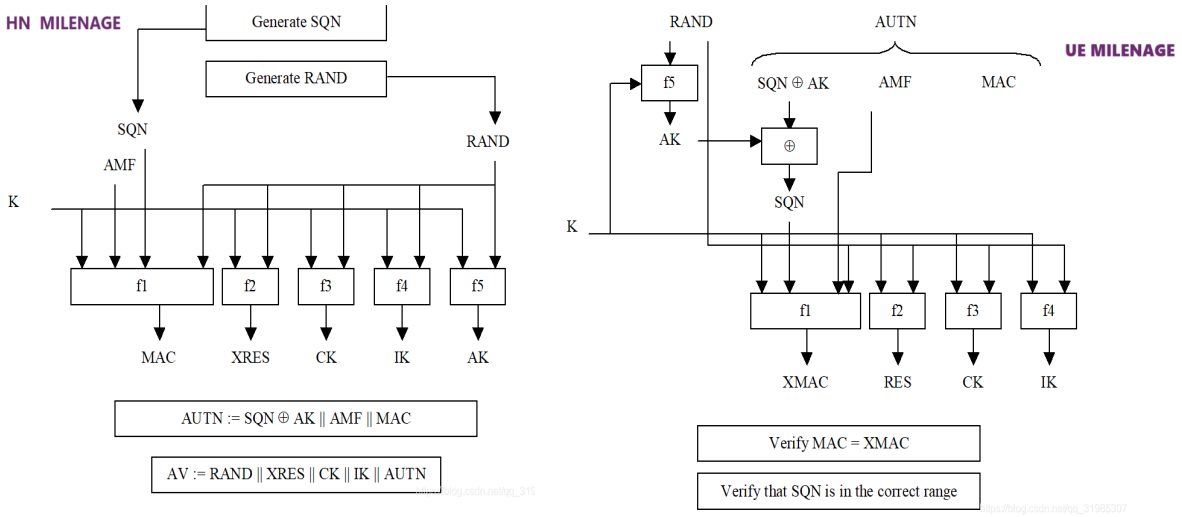

Fig. 5. MILENAGE set in UE and HN side

Figure 2 shows the process of the MILENAGE algorithm, with inputs as K, RAND and AUTN, where AUTN (Authentication Token) consists of SQN (Sequence Number), AK (Anonymity Key), AMF (Authentication Management Field) and MAC (Message Authentication Code). The algorithm outputs XMAC (expected MAC), RES, CK, IK and the intermediate value AK. The encryption algorithm in f5 is the kernel function. In principle, any function that meets the criteria of 128-bit key length, 128-bit input and 128-bit output can be used as a kernel function, but the standard recommends using the AFS-128 algorithm as the kernel function, which is what is implemented in practical engineering applications, using the AES-128 algorithm. Details are aligned with ETSI's guidelines [24].

Table 1
Input and output parameters of *MILENAGE set*

Parameter	Size (Bits)	Comment
AK	48	anonymous key, the output of functions f5 and f5*
AMF	16	Authentication management field, field which is used as the input to functions f1 and f1*
c1,c2,c3,c4 ,c5	128	constant, XOR it with intermediate variables.
CK	128	confidentiality key that is the output of the function f3.
IK	128	integrity key, the output of function f4
IN1	128	value composed of SQN and AMF, used to calculate the functions f1 and f1*.
K	128	subscriber key, input to functions f1, f1*, f2, f3, f4, f5 and f5*.
MAC-A	64	network authentication code output by function f1
MAC-S	64	resynchronization authentication code output by function f1*.
OP	128	operator variant configuration field that is part of the functions f1, f1*, f2, f3, f4, f5 and f5*.
OP_C	128	value derived from OP and K and used within the computation of the functions.
r1,r2,r3,r4,r5	0 to 127	An integer, which defines amounts by which intermediate variables are cyclically rotated.
RAND	128	random number challenge used as input to f1, f1*, f2, f3, f4, f5 and f5*
RES	64	authentication response value is output by f2.
SQN	48	sequence number as input to functions f1 and f1* (For f1* this input is more precisely called SQN_{MS})
TEMP	128	value used within the computation of the functions.
Output values of f1, f1*, f2, f3, f4, f5 and f5*		

3.3 ASCON Lightweight Authenticated Encryption and Hashing

The field of lightweight cryptography (LWC) specifically targets the development of cryptographic mechanisms for environments constrained by limited memory, power and processing capabilities, conditions frequently encountered in Internet of Things (IoT) deployments, as mentioned by Ali *et al.,* [25]. Despite these stringent resource restrictions, maintaining robust data security remains critical. Accordingly, various lightweight ciphers, including ASCON, have been devised to minimize resource consumption while upholding strong security guarantees , as shown by Tew *et al.,* [26].The Ascon algorithm, recognized as one of the NIST-approved solutions for lightweight encryption, exemplifies a "sponge-based" architecture designed to provide both confidentiality and integrity, namely Authenticated Encryption with Associated Data (AEAD)—rather than separately handling encryption and hashing. Internally, Ascon manages a state organized into five rows and 64 columns (each cell representing a single bit). Keys are used to modify this state via XOR operations with stored values. To accommodate different input sizes, Ascon pads the data by appending one "1" bit, followed by enough "0" bits to fill the block. Its encryption routine begins by initializing the state with a predetermined number and a key, then processes any associated data if present and ultimately integrates the message data. The process concludes by generating a “tag” signature that validates the authenticity of the output, thus preventing unauthorized manipulation. Algorithm-based security remains a major focus in cryptographic research; in this context, Ascon’s design effectively thwarts data manipulation and prevents illicit alteration or decryption without the correct key. Its lightweight nature allows for wide deployment, making it especially suitable for devices with constrained resources, such as those in industrial networks and IoT environments. As Dobraunig *et al.,* [27,28] emphasize, ASCON dynamically illustrates how efficiency and security can be cohesively realized within a single encryption algorithm.

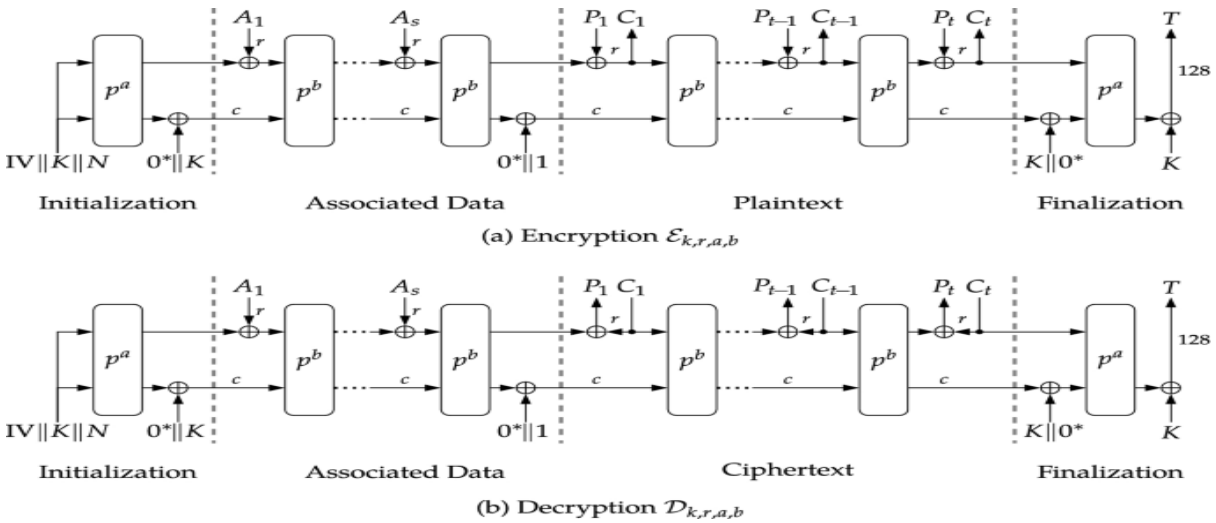

Fig. 6. Authenticated encryption (a) Decryption (b) in Ascon

3.4 Proposed System

Our proposed methodology focuses on enhancing the security and efficiency of the 5G-AKA protocol by replacing the AES algorithm with the ASCON lightweight encryption algorithm for the purpose of addressing the existing vulnerabilities in AES identified by previous studies as we have previously indicated. When applying the ASCON algorithm, its performance is better in terms of memory usage, entropy and security against certain types of cryptographic attacks. We propose an improvement on the 5G-AKA protocol by applying the ASCON algorithm. The improved sections of the AKA protocol marked by shield increase the encryption speed in source-specific devices using ASCON and they become immune to risk marked by a lock. Thus, we achieve confidentiality, authentication and integrity in the application of the protocol, as shown in Figure 7.

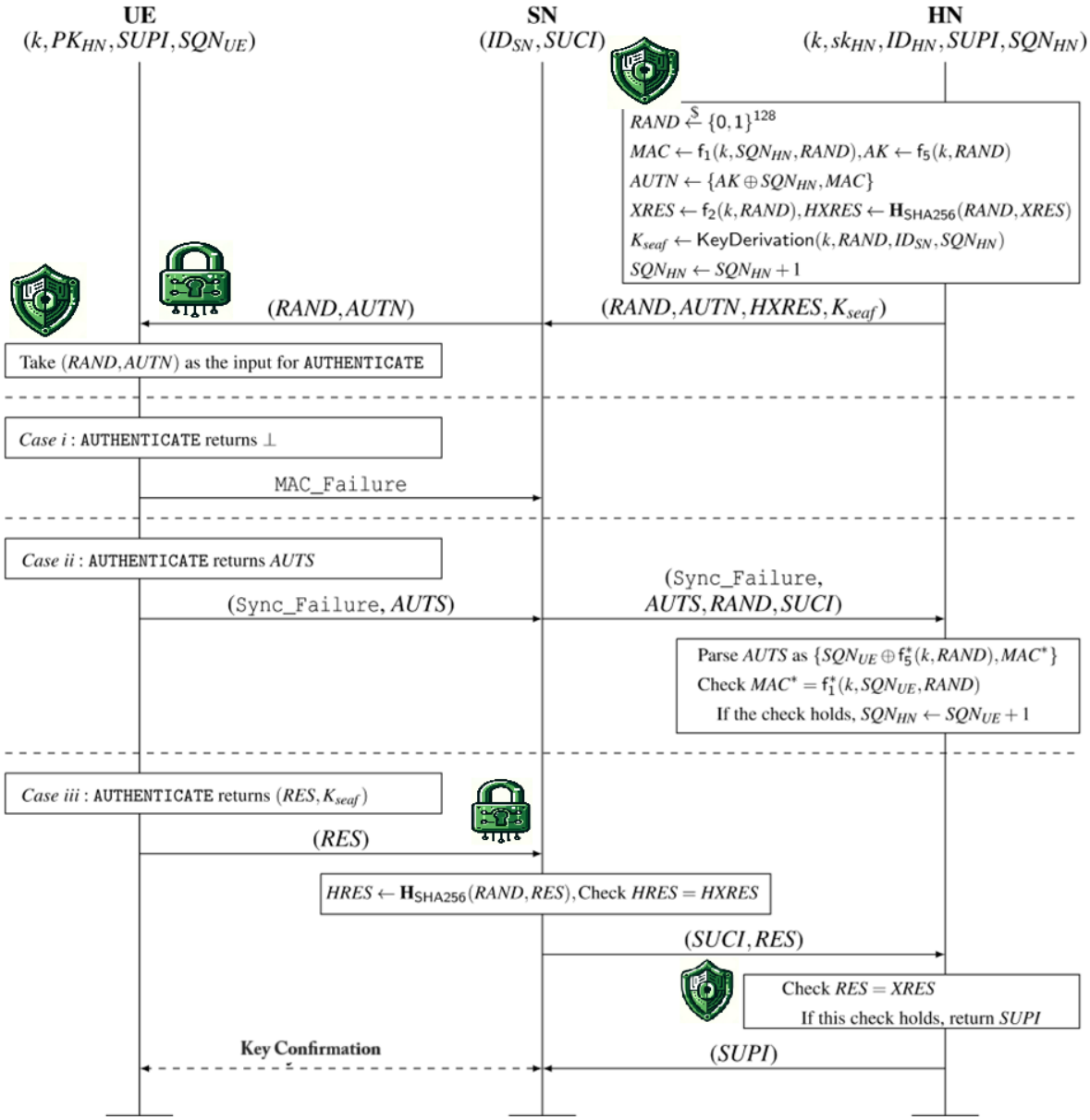

Fig. 7. Improving 5G-AKA protocol

Implemented ASCON lightweight to encrypt parameters within the authentication process of the 5G-AKA protocol and provide encryption for MAC failure messages.

The MILENAGE algorithm found in the 5G-AKA protocol architecture to implement the f1 to f5 function using Mininet emulator using the Python, as in Figure 8, we replaced AES encryption algorithms with ASCON, where they are used to encrypt and decrypt between UE, SN to protect user information SUCI. Replacing this algorithm led to increased entropy, reduced memory usage, etc. as described in the results in section 8.

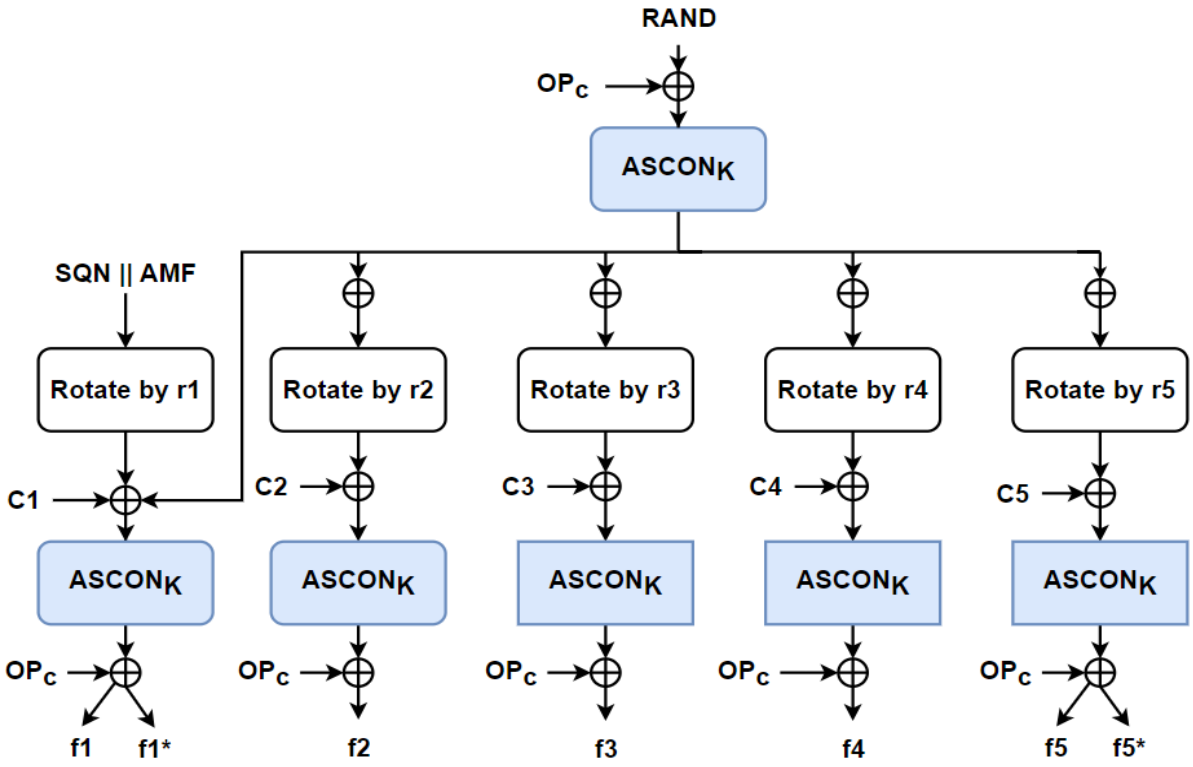

Fig. 8. Proposed MILENAGE with ASCON

3.4.1 Environment and topology

Implemented 5G-AKA protocol in the Ubuntu 22.04.3 LTS Linux operating system and Mininet emulator using the Python language on a 16-MB RAM laptop. Figure 9 show topology build in Mininet emulation.

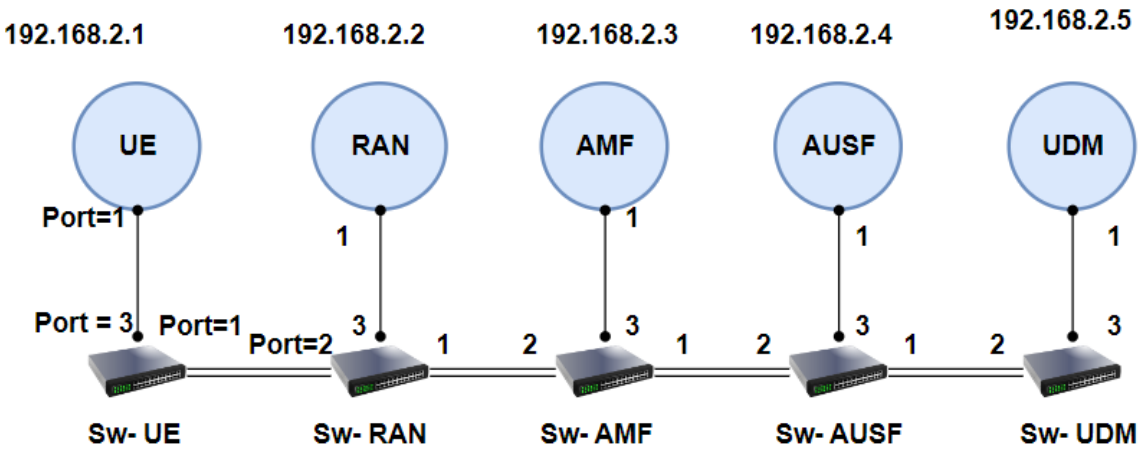

Fig. 9. 5G topology architecture

3.4.2 Formula of methodology

i. Initial XOR Operator: $c_1 = (SQN||AMF) \oplus RAND$

ii. Rotation and Operate for each phase:

$c_2 = Rotate(c_1, r_1) \oplus OP_c \oplus ASCON_K$

$c_3 = Rotate(c_2, r_2) \oplus OP_c \oplus ASCON_K$

$$c_4 = Rotate(c_3, r_3) \oplus OP_c \oplus ASCON_K$$
$$c_5 = Rotate(c_4, r_4) \oplus OP_c \oplus ASCON_K$$
$$c_6 = Rotate(c_5, r_5) \oplus OP_c \oplus ASCON_K$$

iii. Final Functions:

$$f_1 = c_2 \oplus OP_c \oplus ASCON_k$$
$$f_1^* = Rotate(f_1, r_1) \oplus OP_c \oplus ASCON_k$$
$$f_2 = c_3 \oplus OP_c \oplus ASCON_k$$
$$f_3 = c_4 \oplus OP_c \oplus ASCON_k$$
$$f_4 = c_5 \oplus OP_c \oplus ASCON_k$$
$$f_5 = c_6 \oplus OP_c \oplus ASCON_k$$
$$f_5^* = Rotate(f_5, r_5) \oplus OP_c \oplus ASCON_k$$

4. Results

To clarify the reasons for replacing ASCON with AES (advanced encryption standard) in encryption applications, especially in cases such as fifth-generation networks that deal directly with devices with limited sources that use 5G protocols AKA, through a number of mathematical, cryptographic and performance evaluations. Here, we study several mathematical and cryptographic factors that explain why ASCON is considered more useful or more convenient in specific scenarios when compared to AES.

4.1 Robust Security

i. Side channel protection: use ASCON is designed against such types of attacks as timing and power analysis due to its algebraic structure that eliminated complex searches in table searches and input-dependent bitwise operations.

ii. Differential and Linear Cryptanalysis: The ASCON algorithm architecture design is characterized by its strong resistance to differential and linear cryptanalysis. S-boxes in AES have been analysed in several studies for vulnerabilities, despite their security. ASCON relies on a smaller and more transparent design, which reduces the chances of those attacks. Mathematically, this is reflected in the low probabilities of differential and linear analysis. In addition, the circular ASCON function is specially designed to repel linear and differential analysis techniques, which ensures high security of the algorithm. This focus on resisting those attacks makes ASCON stand out and a strong competitor for secure communications and data protection applications.

4.2 Efficiency and Performance

They require fewer logic gates in hardware due to their reliance on basic bit operations and built-in S-boxes. This simplified design leads to reduced energy use and faster calculations.

ASCON requires less static and dynamic memory than AES. In scenarios where memory is of the essence, ASCON provides a mathematical advantage by minimizing the storage needs of keys and intermediate states in cryptography.

In Table 2 and Table 3 we show 3 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 derive them.

In Table 2, the `opc` values are derived using AES, while in Table 3, they are derived using ASCON.

Table 2
Keyset of MILENAGE with AES

Keyset # 1	
ki	90dca4eda45b53cf0f12d7c9c3bc6a89
op	3ffcfe5b7b1111589920d3528e84e655
Rand	9fddc72092c6ad036b6e464789315b78
opc	1bcf8d2446348f7abe36abb745e6fc48
kc	e22396864d948026
sres	ecf5f588
Keyset # 2	
ki	5122250214c33e723a5dd523fc145fc0
op	c9e8763286b5b9ffbdf56e1297d0887b
rand	81e92b6c0ee0e12ebceba8d92a99dfa5
opc	a98e4bc03eacff70ef633d2097b66b1b
kc	d3615140a85c3b36
sres	1cb2007e
Keyset # 3	
ki	b73a90cbcf3afb622dba83c58a8415df
op	b672047e003bb952dca6cb8af0e5b779
rand	b120f1c1a0102a2f507dd543de68281f
opc	717f49040df715c712bbe3daf77ddc2d
kc	e83e3532392723cd
sres	c03a28a5

The values of kc and SREs these values also differ between the tables, as a result of the different encoding 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, but the encryptions produce different results for `opc`,` KC` and 'SREs' due to different underlying algorithms (AES vs ASCON). This shows how the choice of primitive encryption can affect the output in an authentication protocol and a key agreement such as 5G-AKA.

Table 3
Keyset of MILENAGE with ASCON

Keyset # 1	
ki	90dca4eda45b53cf0f12d7c9c3bc6a89
op	3ffcfe5b7b1111589920d3528e84e655
Rand	9fddc72092c6ad036b6e464789315b78
opc	5443bfce1b73bab17e6339da86c588b4
kc	6a5d8a74f1246ad2
sres	32fa85c8
Keyset # 2	
ki	5122250214c33e723a5dd523fc145fc0
op	c9e8763286b5b9ffbdf56e1297d0887b
rand	81e92b6c0ee0e12ebceba8d92a99dfa5
opc	362edb223c0e73bd4819aa4d2a6f7c32
kc	900c0f2782676911
sres	d215cd64
Keyset # 3	
ki	b73a90cbcf3afb622dba83c58a8415df
op	b672047e003bb952dca6cb8af0e5b779
rand	b120f1c1a0102a2f507dd543de68281f
opc	939af96afb6cdb83d9af4944b1e496eb
kc	809205324312e048
sres	615d74e2

Table 4
Evolution metrics of MILENAGE with AES

Evolution Metrics	Value
Memory usage: Current	0.001223 MB
Memory usage: Peak	0.004312 MB
Entropy of OPC	3.8750 bits
Avalanche effect	47.66% change

Table 5
Evolution metrics of MILENAGE with ASCON

Evolution Metrics	Value
Memory usage: Current	0.000161 MB
Memory usage: Peak	0.003093 MB
Entropy of OPC	4.0000 bits
Avalanche effect	48.44% change

Based on the tables above, the current memory usage for AES is 0.001223MB, while ASCON is 0.000161 MB, ASCON consumes significantly less memory than AES. This makes it a more efficient option for lightweight and resource-limited devices.

$$\frac{M_{ASCON,Current}}{M_{AES,Current}} = \frac{0.000161}{0.001223} \approx 7.6 \quad (1)$$

and Peak Memory Usage:

$$\frac{M_{ASCON,Peak}}{M_{AES,Peak}} = \frac{0.004312}{0.003093} \approx 1.39 \quad (2)$$

ASCON exhibits a higher degree of unpredictability, a desirable property for security purposes. This increased unpredictability or rising entropy, suggests that ASCON offers a more secure encryption mechanism compared to alternatives.

$$Increase\ in\ Entropy = E_{ASCON} - E_{AES} = 0.125\ bits \quad (3)$$

The avalanche effect measures how sensitive the output is to small changes in the input. A higher value indicates a more stable and secure algorithm. ASCON has a slightly better avalanche effect than the comparative algorithm.

$$Increase\ in\ Avalanch\ Effect = AE_{ASCON} - AE_{AES} = 0.78\% \quad (4)$$

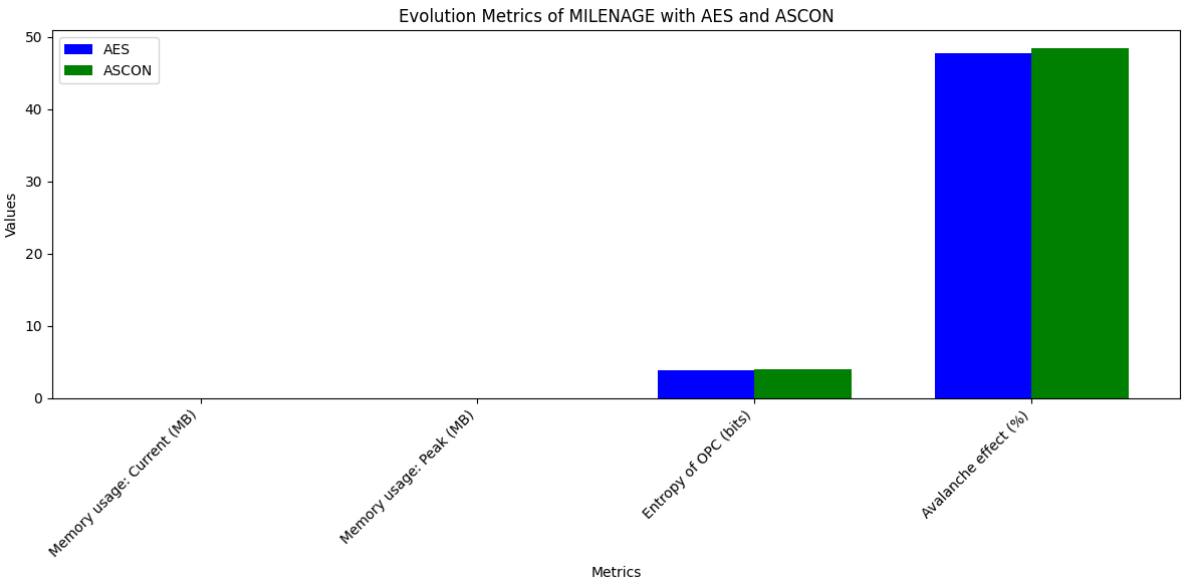

Fig. 9. Evaluation measurements in graph

4. Conclusion

The 5G authentication protocol AKA is compromised during authentication because the messages sent between UE and SEAF are not encrypted. Despite 3GPP's great emphasis on subscriber privacy, it was necessary to modify the 5G Protocol AKA to address inherited structural gaps. We also expect that if the protocol is adopted as it is in the possible future standards of 6G, it will have serious consequences because it will inherit the vulnerabilities arising from 5G. These parameters should be optimized in such a way that they can be operated 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 SSN. The performance evaluation showed that a slight increase in entropy (0.125 bits) with ASCON provides more unpredictability in the encryption process, which enhances security. Moreover, the high impact of the breakdown (an increase of 0.78%) with ASCON indicates a better spread, which makes it difficult for attackers to predict patterns. In terms of memory usage, ASCON is significantly more efficient, using about 7.6 times less current memory and 1.39 times less peak memory than AES. This efficiency is critical for resource-limited environments, such as mobile devices and IoT applications, that dominate fifth-generation networks. The 5G Protocol AKA requires a balance between security, performance and efficiency. ASCON's high security metrics and lower memory usage make it a convenient option. For applications where memory and security are critical, ASCON provides a significant advantage over AES. Therefore, the replacement of AES with ASCON in the 5G Protocol AKA is justified by ASCON's improved security features and more efficient memory use, which makes it a better choice for modern cryptographic applications, especially in the context of 5G technology.

Acknowledgement

This research was not funded by any grant.

References

[1] Ji, Xinsheng, Kaizhi Huang, Liang Jin, Hongbo Tang, Caixia Liu, Zhou Zhong, Wei You *et al.,* "Overview of 5G security technology." *Science China Information Sciences* 61, no. 8 (2018): 081301. https://doi.org/10.1007/s11432-017-9426-4

[2] Manaa, Mehdi Ebady and Rasha Hussein Jwdha. "A Proactive Data Security Scheme Of Files Using Minhash Technique." *Journal of Theoretical and Applied Information Technology* 96, no. 24 (2018).
[3] Ahmad, Ijaz, Tanesh Kumar, Madhusanka Liyanage, Jude Okwuibe, Mika Ylianttila and Andrei Gurtov. "Overview of 5G security challenges and solutions." *IEEE Communications Standards Magazine* 2, no. 1 (2018): 36-43. https://doi.org/10.1109/MCOMSTD.2018.1700063
[4] Dutta, Ashutosh and Eman Hammad. "5G security challenges and opportunities: A system approach." In *2020 IEEE 3rd 5G world forum (5GWF)*, pp. 109-114. IEEE, 2020. https://doi.org/10.1109/5GWF49715.2020.9221122
[5] 3GPP, B. "Security architecture and procedures for 5G system." *Technical Specification (TS) 3GPP TS 33.501 V17. 0.0 (2020–2012)* (2020).
[6] Manaa, Mehdi, Ahmed Obaid and Mohammed Dosh. "Unsupervised approach for email spam filtering using data mining." *EAI Endorsed Transactions on Energy Web* 8, no. 36 (2021).
[7] Braeken, An, Madhusanka Liyanage, Pardeep Kumar and John Murphy. "Novel 5G authentication protocol to improve the resistance against active attacks and malicious serving networks." *Ieee Access* 7 (2019): 64040-64052. https://doi.org/10.1109/ACCESS.2019.2914941
[8] Liyanage, Madhusanka, Ijaz Ahmad, Ahmed Bux Abro andrei Gurtov and Mika Ylianttila, eds. *A comprehensive guide to 5G security*. Hoboken: John Wiley & Sons, 2018. https://doi.org/10.1002/9781119293071
[9] Arapinis, Myrto, Loretta Mancini, Eike Ritter, Mark Ryan, Nico Golde, Kevin Redon and Ravishankar Borgaonkar. "New privacy issues in mobile telephony: fix and verification." In *Proceedings of the 2012 ACM conference on Computer and communications security*, pp. 205-216. 2012. https://doi.org/10.1145/2382196.2382221
[10] Borgaonkar, Ravishankar, Lucca Hirschi, Shinjo Park and Altaf Shaik. "New privacy threat on 3G, 4G and upcoming 5G AKA protocols." *Cryptology ePrint Archive* (2018). https://doi.org/10.2478/popets-2019-0039
[11] Hussain, Syed, Omar Chowdhury, Shagufta Mehnaz and Elisa Bertino. "LTEInspector: A systematic approach for adversarial testing of 4G LTE." In *Network and Distributed Systems Security (NDSS) Symposium 2018*. 2018. https://doi.org/10.14722/ndss.2018.23313
[12] Ferrag, Mohamed Amine, Leandros Maglaras, Antonios Argyriou, Dimitrios Kosmanos and Helge Janicke. "Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes." *Journal of Network and Computer Applications* 101 (2018): 55-82. https://doi.org/10.1016/j.jnca.2017.10.017
[13] Basin, David, Jannik Dreier, Lucca Hirschi, Saša Radomirovic, Ralf Sasse and Vincent Stettler. "A formal analysis of 5G authentication." In *Proceedings of the 2018 ACM SIGSAC conference on computer and communications security*, pp. 1383-1396. 2018. https://doi.org/10.1145/3243734.3243846
[14] 3GPP, B. "Security architecture and procedures for 5G system." *Technical Specification (TS) 3GPP TS 33.501 V17. 0.0 (2020–2012)* (2020).
[15] Cremers, Cas and Martin Dehnel-Wild. "Component-based formal analysis of 5G-AKA: Channel assumptions and session confusion." In *Network and Distributed System Security Symposium (NDSS)*. Internet Society, 2019. https://doi.org/10.14722/ndss.2019.23394
[16] Edris, Ed Kamya Kiyemba, Mahdi Aiash and Jonathan Kok-Keng Loo. "Formal verification and analysis of primary authentication based on 5G-AKA protocol." In *2020 Seventh International Conference on Software Defined Systems (SDS)*, pp. 256-261. IEEE, 2020. https://doi.org/10.1109/SDS49854.2020.9143899
[17] Cao, Jin, Zheng Yan, Ruhui Ma, Yinghui Zhang, Yulong Fu and Hui Li. "LSAA: A lightweight and secure access authentication scheme for both UE and mMTC devices in 5G networks." *IEEE Internet of Things Journal* 7, no. 6 (2020): 5329-5344. https://doi.org/10.1109/JIOT.2020.2976740
[18] Ouaissa, Mariya and Mariyam Ouaissa. "An improved privacy authentication protocol for 5G mobile networks." In *2020 International Conference on Advances in Computing, Communication & Materials (ICACCM)*, pp. 136-143. IEEE, 2020. https://doi.org/10.1109/ICACCM50413.2020.9212910
[19] 3GPP. "Security Architecture and Procedures for 5G System." *3GPP TS 33.501*, v16.0.0. (2019).
[20] Koutsos, Adrien. "The 5G-AKA authentication protocol privacy." In *2019 IEEE European symposium on security and privacy (EuroS&P)*, pp. 464-479. IEEE, 2019. https://doi.org/10.1109/EuroSP.2019.00041
[21] Dehnel-Wild, Martin and Cas Cremers. "Security vulnerability in 5G-AKA draft." *Department of Computer Science, University of Oxford, Tech. Rep* (2018): 14-37.
[22] Yadav, Awaneesh Kumar, Manoj Misra, Pradumn Kumar Pandey, An Braeken and Madhusanka Liyange. "An improved and provably secure symmetric-key based 5G-AKA Protocol." *Computer Networks* 218 (2022): 109400. https://doi.org/10.1016/j.comnet.2022.109400
[23] Braeken, An. "Symmetric key based 5G AKA authentication protocol satisfying anonymity and unlinkability." *Computer Networks* 181 (2020): 107424. https://doi.org/10.1016/j.comnet.2020.107424
[24] ETSI. "ETSI TS 135 205 V17.0.0 (2022-04) Technical Specification Universal Mobile Telecommunications System (UMTS); LTE; 3G Security; Specification of the MILENAGE Algorithm Set..." (2022). https://www.etsi.org/deliver/etsi_ts/135200_135299/135205/17.00.00_60/ts_135205v170000p.pdf

[25] Ali, Tasnuva, Azni Haslizan Ab Halim and Nur Hafiza Zakaria. "3D Lightweight Cryptosystem Design for IoT Applications Based on Composite S-Box." *International Journal of Computational Thinking and Data Science* 3, no. 1 (2024): 40-54. https://doi.org/10.37934/ctds.3.1.4054

[26] Tew, Jia Jian, Chia Yee Ooi and Yeam Tan Chong. "Compact Hardware Implementation Of The CLEFIA Block Cipher." *Journal of Advanced Research in Computing and Applications* 30, no. 1 (2023): 1-6. https://doi.org/10.37934/arca.30.1.16

[27] Dobraunig, Christoph, Maria Eichlseder, Florian Mendel and Martin Schläffer. "Cryptanalysis of ascon." In *Topics in Cryptology—CT-RSA 2015: The Cryptographer's Track at the RSA Conference 2015, San Francisco, CA, USA, April 20-24, 2015. Proceedings*, pp. 371-387. Springer International Publishing, 2015. https://doi.org/10.1007/978-3-319-16715-2_20

[28] Dobraunig, Christoph, Maria Eichlseder, Florian Mendel and Martin Schläffer. "Ascon v1. 2: Lightweight authenticated encryption and hashing." *Journal of Cryptology* 34 (2021): 1-42. https://doi.org/10.1007/s00145-021-09398-9