Comments on P802.1AEef D0.3 (8^{th} February 2026)

Alexander Zeh, Florian Mendel
Infineon Technologies AG
Munich, Germany
{alexander.zeh, florian.mendel}@infineon.com

Abstract

We propose an improved partitioning of Ethernet information for the lightweight cipher ASCON, extending the current proposal in IEEE P802.1AEef D0.3. The proposed approach reduces the number of required cryptographic operations for MACsec Service Data Units (MSDUs) of arbitrary size in the confidentiality protection mode, and for selected configurations in integrity protection mode. Analytical and experimental results show a reduction of up to 20% in cryptographic operations, with the most pronounced gains observed for small payload sizes (more than 10% below 96 bytes MSDU size).

Index Terms

AES-GCM, Ascon, Ascon-AEAD128, Ascon-XPN-128, Ethernet, IEEE802.1AE, MACsec, Security.

I. Introduction

The current IEEE draft P802.1AEef D0.3 introduces the lightweight cipher Ascon [3], [5] as a second ciphersuite alongside AES-GCM [4], as used in IEEE 802.1AE MACsec [2]. We first present the basic notation required for Ascon in Section II. Section III summarizes the relevant parts of the IEEE P802.1AEef D0.3 specification and defines the Ascon* proposal. In Section IV, we provide explicit calculations of the cryptographic computation savings achieved by Ascon* relative to the current draft. We conclude in Section V.

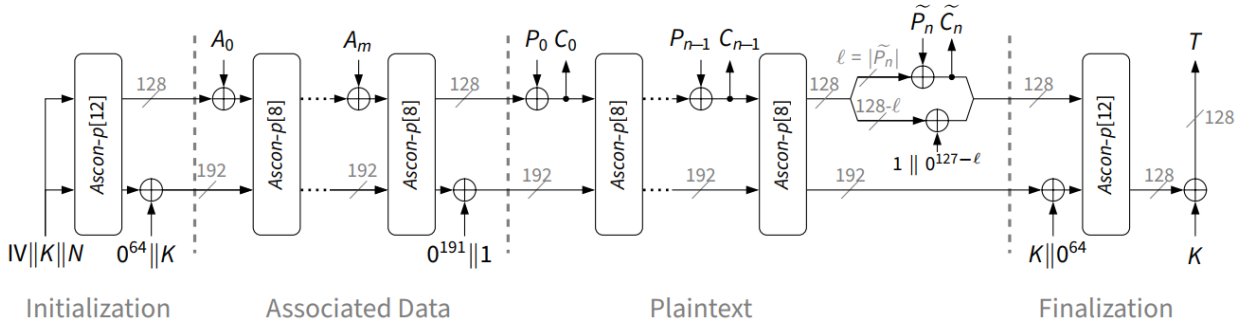

Fig. 1. `Ascon-AEAD128` encryption as in [3, Fig. 5]. We have $m+1$ authentication blocks and $n+1$ plaintext blocks of length 128 bit.

II. Lightweight-Cipher Ascon and Its Padding

We shortly recall relevant parameters of Ascon [3], [5] for AEAD128 encryption mode as illustrated in Fig. 1. The nonce N has a length of 128 bit (not to be confused with the fixed initialization vector IV). The parameters m and n are obtained from the authentication data A and the plaintext P as follows:

$$A_0, A_1, \ldots, A_m \leftarrow A \,\|\, 1 \,\|\, 0^*,$$
$$P_0, P_1, \ldots, P_n \leftarrow P \,\|\, 1 \,\|\, 0^*,$$

where A_i (resp. P_i) are blocks of length 128 bit. Note that in case A (resp. P) has a length of a multiple of 128 bit, the last block A_m (resp. P_n) is $1 \,\|\, 0^{127}$. In Ascon, the last plaintext block $P_n \leftarrow \widetilde{P}_n \,\|\, 1 \,\|\, 0^*$ is not absorbed during the main processing phase, but effectively handled in the finalization stage. Overall, we have $m+n+1$ Ascon-p[8] blocks and two Ascon-p[12] blocks.

III. Current Specification and Proposition for MACsec

According to the current draft P802.1AEef D0.3 [1, Section 14.9] the authentication data A for Confidentiality Protection for Ascon-XPN-128 consists of the 6-octet Destination MAC Address (DA), 6-octet Source MAC Address (SA) and the first four octets of the SecTAG (i.e., 2-octet Ethertype and 2-octet "TCI‖AN‖SL"). It does not contain the 4-octet Packet Number (PN) nor the 8-octet (optional) Secure Channel Indicator (SCI) compared to AES-GCM as in [2, Section 14.5-14.8] (resp. as XPN and SSCI). The PN and SCI are "moved" to the nonce N (see [1, Section 14.9.4]), i.e.,

$$\mathrm{N} \leftarrow \mathrm{PN} \,\|\, \mathrm{XPN} \,\|\, 0^{16} \,\|\, \mathrm{SCI}, \tag{1}$$

where XPN has length of 16 bit (compared to 32 bit for AES-GCM). Table I summarizes the differences (and additionally contains a new proposition denoted as Ascon*). The exact length of A is 16 octets (in Confidentiality Protection mode) leads

TABLE I

Comparison of the input for three cipher suites AES-GCM, Ascon and Ascon* for an Ethernet frame with confidentiality protection with MACsec for authenticated data A, the nonce N and the ciphertext C. According to IEEE802.1AE-2018 the corresponding data A' is 44 octets long, while for Ascon as in [1] it is reduced to 16 octets. Note, that the nonce of Ascon contains additional fields that are not shown here. Furthermore, the 8-octet SCI for the nonce of AES-GCM is reduced to a 4-octet Short SCI (SSCI) while the 4-octet Packet Number (PN) is extended to an 8-octet eXtended PN (XPN) and therefore marked with (Y) – the resulting nonce length is 96 bits (vs. 128 bits for Ascon with a 48-bit XPN).

Field	**Size**	**AES-GCM**			**Ascon**			**Ascon***		
	(Octets)	**A'**	**N'**	**C'**	**A**	**N**	**C**	**A***	**N***	**C***
DA ‖ SA	12	Y	-	-	Y	-	-	Y	-	-
EtherType	2	Y	-	-	Y	-	-	Y	-	-
TCI ‖ AN ‖ SL	2	Y	-	-	Y	-	-	-	Y	-
PN	4	Y	(Y)	-	-	(Y)	-	-	(Y)	-
SCI	8	Y	(Y)	-	-	Y	-	-	Y	-
MSDU	M	-	-	Y	-	-	Y	-	-	Y
ICV	16 (8)	-	-	-	-	-	-	-	-	-
FCS	4	-	-	-	-	-	-	-	-	-

to an unfortunate padding of Ascon causing two 16-octet blocks A_0 and A_1, i.e.,

$$\begin{aligned} A_0 &\leftarrow \mathrm{DA} \,\|\, \mathrm{SA} \,\|\, \mathrm{EtherType} \,\|\, \mathrm{TCI} \,\|\, \mathrm{AN} \,\|\, \mathrm{SL}, \\ A_1 &\leftarrow 1 \,\|\, 0^{127}. \end{aligned}$$

Accordingly, in Ascon* we propose relocating the two-octet field TCI ‖ AN ‖ SL of the authenticated data A into the nonce N of (1). We obtain:

$$\begin{aligned} \mathrm{N}^* &\leftarrow \mathrm{PN} \,\|\, \mathrm{XPN} \,\|\, \mathrm{TCI} \,\|\, \mathrm{AN} \,\|\, \mathrm{SL} \,\|\, \mathrm{SCI}, \\ A_0^* &\leftarrow \mathrm{DA} \,\|\, \mathrm{SA} \,\|\, \mathrm{EtherType} \,\|\, 1 \,\|\, 0^{15}. \end{aligned}$$

This change eliminates the need for the second 128-bit associated-data block A_1. The next section quantifies the resulting savings in cryptographic computations as a function of the User Data/MSDU size M for both Confidentiality Protection and Integrity Protection modes.

IV. Improvements for Confidentiality Protection and Integrity Protection

As introduced in Section II, we have

$$m + n + 1 \tag{2}$$

Ascon-p[8] blocks and two Ascon-p[12] blocks (for initialization and finalization).

We define the ration R of complexity with (2) for the defined AEAD128 mode as:

$$R \stackrel{\text{def}}{=} \frac{(m^* + n^* + 1) \cdot 8 + 2 \cdot 12}{(m + n + 1) \cdot 8 + 2 \cdot 12}. \tag{3}$$

For Confidentiality Protection, we have $m = 1$ and $m^* = 0$ and we obtain from (3):

$$\begin{aligned} R_C &= \frac{(0 + n + 1) \cdot 8 + 2 \cdot 12}{(1 + n + 1) \cdot 8 + 2 \cdot 12} \\ &= \frac{(n+1) \cdot 8 + 24}{(n+1) \cdot 8 + 32}, \\ &= \frac{(n+1) + 3}{(n+1) + 4}. \end{aligned} \tag{4}$$

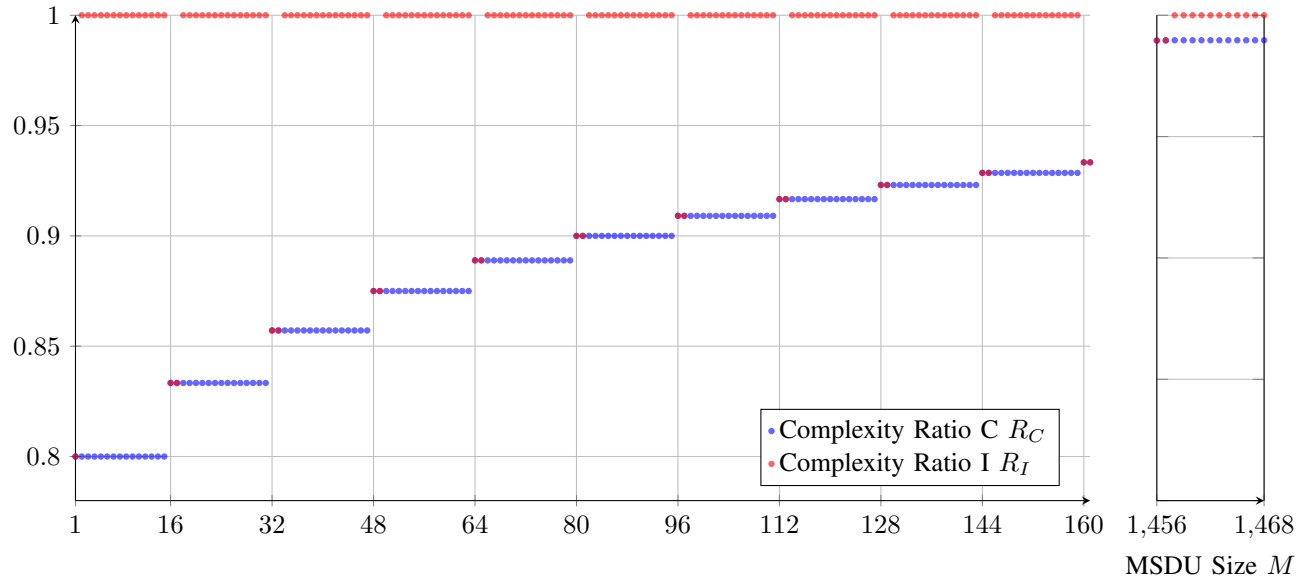

Fig. 2. Complexity ratios of Ascon* relative to Ascon are shown for confidentiality protection $R_C(M)$ (blue) and integrity protection $R_I(M)$ (red). For integrity protection a reduction of complexity $R_I < 1$ occurs for only for $M = \{0, 1\} \bmod 16$. In contrast, confidentiality protection achieves reduced complexity $R_C < 1$ for all values of M. Notably, for short frames with $M < 96$ the complexity is reduced by more than 10 %.

Note that for the sake of simplicity we consider in the following only data length in terms of octets and not bits. (This is quite common in practice for most applications and communication protocols.)

With $n + 1 = n^* + 1 = \lceil (M + 1)/16 \rceil$ in (4) leads to:

$$R_C(M) = \frac{\lceil (M+1)/16 \rceil + 3}{\lceil (M+1)/16 \rceil + 4}. \tag{5}$$

For short frames with $M < 16$, we obtain $R_C(< 16) = 4/5$, while $R_C(1456) = 95/96$, meaning a saving of $1/96 = 1.04\%$. We illustrate R_C as in (5) in Fig. 2 (in blue).

For Integrity Protection, we have $n^* = n = 0$ and obtain from (3):

$$\begin{aligned} R_I &= \frac{(m^* + 1) \cdot 8 + 2 \cdot 12}{(m + 1) \cdot 8 + 2 \cdot 12} \\ &= \frac{(m^* + 1) + 3}{(m + 1) + 3}. \end{aligned} \tag{6}$$

With $m + 1 = \lceil (M + 1 + 16)/16 \rceil$ and $m^* + 1 = \lceil (M + 1 + 14)/16 \rceil$, we obtain from (6);

$$R_I(M) = \frac{\lceil (M+1+14)/16 \rceil + 3}{\lceil (M+1+16)/16 \rceil + 3}. \tag{7}$$

Note that for $M = 16$, we obtain $R_I(16) = 5/6$. We plot both complexity ratios $R_C(M)$ as in (5) and $R_I(M)$ as in (7) in Fig. 2.

V. Conclusion

We revisited how Ethernet header fields are mapped to Ascon inputs in MACsec and proposed a minimal change that removes an avoidable 128-bit absorption of associated data. Specifically, by moving the two octets TCI $\|$ AN $\|$ SL from A into the nonce, the authentication data shrinks from an exact 16 octets to 14 octets, so Ascon's padding no longer forces a second block A_2. This simple repartitioning preserves the on-wire MACsec frame format and nonce uniqueness requirements while reducing the number of Ascon calls needed to process a frame.

Our analysis quantifies the savings. In confidentiality protection mode the complexity reduction yielding up to 20% fewer cryptographic operations for very short MSDUs. In integrity protection, we obtain up to 16.7% fewer operations.

Security and interoperability are maintained. The proposal does not alter the Ethernet encapsulation or MACsec processing pipeline; it only changes which fields are supplied as A versus nonce to the AEAD. Nonce uniqueness continues to rely on PN/XPN and SCI as in the draft, and adding TCI $\|$ AN $\|$ SL to the nonce does not weaken this guarantee.

Practically, the removal of one A absorption per frame shortens the Ascon permutation schedule, reducing latency and energy, particularly beneficial for hardware datapaths and low-power endpoints.

We therefore recommend adopting the proposed A/nonce repartitioning for Ascon in IEEE P802.1AEef. Alternatively, the size of the authentication data could be reduced by other measures, such as removing the EtherType field.

REFERENCES

[1] IEEE 802.1 Working Group, "Current Draft P802.1AEef/D0.3 (8th February 2026): Standard for Local and Metropolitan Area Networks— Media Access Control (MAC) Security—Amendment 5: Ascon Cipher Suite," PAR approved 10 December 2025, expires 31 December 2029.

[2] IEEE Std 802.1AE-2018, "IEEE Standard for Local and Metropolitan Area Networks— Media Access Control (MAC) Security," IEEE, Aug. 2018. doi: 10.1109/IEEESTD.2018.8585421

[3] M. Sönmez Turan, K. McKay, J. Kang, J. Kelsey, und D. Chang, "Ascon-Based Lightweight Cryptography Standards for Constrained Devices: Authenticated Encryption, Hash, and Extendable Output Functions", National Institute of Standards and Technology, NIST Special Publication (SP) 800-232, Aug. 2025. doi: 10.6028/NIST.SP.800-232.

[4] National Institute of Standards and Technology (NIST), "Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC," NIST Special Publication 800-38D, Nov. 2007. doi: 10.6028/NIST.SP.800-38D.

[5] C. Dobraunig, M. Eichlseder, F. Mendel, and M. Schläffer, "Ascon v1.2: Lightweight Authenticated Encryption and Hashing," Journal of Cryptol, vol. 34, no. 3, p. 33, Jun. 2021, doi: 10.1007/s00145-021-09398-9.