Proposition on IEEE802.1AEef

IEEE 802 Interim – Security Working Group
May 10-15, 2026
Munich, Germany

A. Zeh, F. Mendel

2026

[Owner: AZeh Doc ID: IEEE_Interim_802.1AEef Vers.: v07]

Table of contents

1 Lightweight Crypto ASCON and NIST.SP.800-232 3

2 Status of IEEE P802.1AEef/D0.3 7

3 Proposition Ascon* 11

4 Advantages for Confidentiality (C) and Integrity (I) Protection 13

Table of contents

1	**Lightweight Crypto ASCON and NIST.SP.800-232**	**3**
2	Status of IEEE P802.1AEef/D0.3	7
3	Proposition Ascon*	11
4	Advantages for Confidentiality (C) and Integrity (I) Protection	13

Lightweight Crypto ASCON NIST.SP.800-232

4.1.1. Encryption

This section outlines the encryption algorithm of Ascon-AEAD128, which comprises four phases: initialization, associated data processing, plaintext processing, and finalization (see Fig. 5).

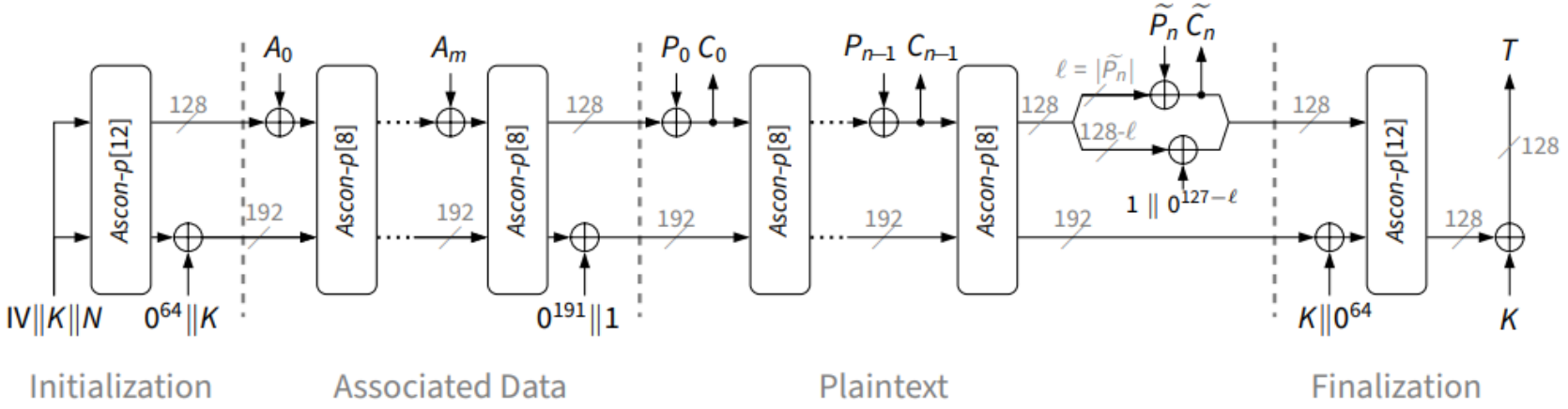


Figure 5. Ascon-AEAD128 encryption

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-232.ipd.pdf

NIST.SP.800-232
Potential Trap

if $|A| > 0$ **then** ▷ Processing Associated Data

$A_0, \ldots, A_{m-1}, \widetilde{A_m} \leftarrow \text{parse}(A, 128)$

$A_m \leftarrow \text{pad}(\widetilde{A_m}, 128)$

for $i = 0$ to m **do**

$\mathcal{S} \leftarrow \mathit{Ascon\text{-}p}[8]((\mathcal{S}_{[0:127]} \oplus A_i) \| \mathcal{S}_{[128:319]})$

end for

end if

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-232.ipd.pdf

Lightweight Crypto ASCON
General AEAD Encryption with Parameters r=128, c=192.

Processing Associated Data

if $|A| > 0$ **then**

$A_1 \dots A_s \leftarrow r$-bit blocks of $A \| 1 \| 0^*$

for $i = 1, \dots, s$ **do**

$S \leftarrow p^b((S_r \oplus A_i) \| S_c)$

$S \leftarrow S \oplus (0^{319} \| 1)$

Processing Plaintext

$P_1 \dots P_t \leftarrow r$-bit blocks of $P \| 1 \| 0^*$

for $i = 1, \dots, t-1$ **do**

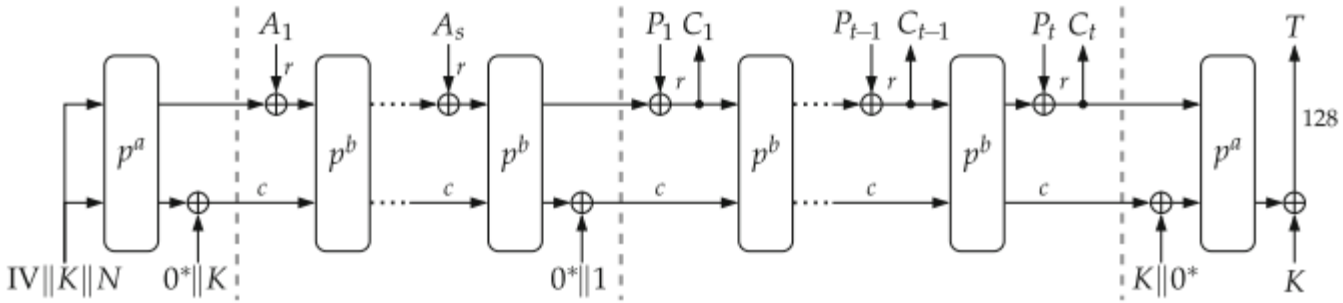
$S_r \leftarrow S_r \oplus P_i$

$C_i \leftarrow S_r$

$S \leftarrow p^b(S)$

$S_r \leftarrow S_r \oplus P_t$

$\tilde{C}_t \leftarrow \lfloor S_r \rfloor_{|P| \bmod r}$



(a) Encryption $\mathcal{E}_{k,r,a,b}$

https://link.springer.com/article/10.1007/s00145-021-09398-9

Table of contents

1 Lightweight Crypto ASCON and NIST.SP.800-232 3

2 **Status of IEEE P802.1AEef/D0.3** **7**

3 Proposition Ascon* 11

4 Advantages for Confidentiality (C) and Integrity (I) Protection 13

Status of IEEE P802.1AEef/D0.3
Comparison of AES-GCM and ASCON

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

Status of IEEE P802.1AEef/D0.3
ASCON Nonce Generation

– The (exact) AAD length of 16 Byte in Int+Conf will cause **two** Ascon-p[8] blocks (instead of one).

In “Springer” Notation, we have then for ASCON;

– A_1 = DA || SA || EtherType || TCI+AN+SL

– $A_2 = 1 \,||\, (0)^{127}$

In “NIST” Notation;

– A_0 = DA || SA || EtherType || TCI+AN+SL

– $A_1 = 1 \,||\, (0)^{127}$

Status of IEEE P802.1AEef/D0.3
ASCON Nonce Generation

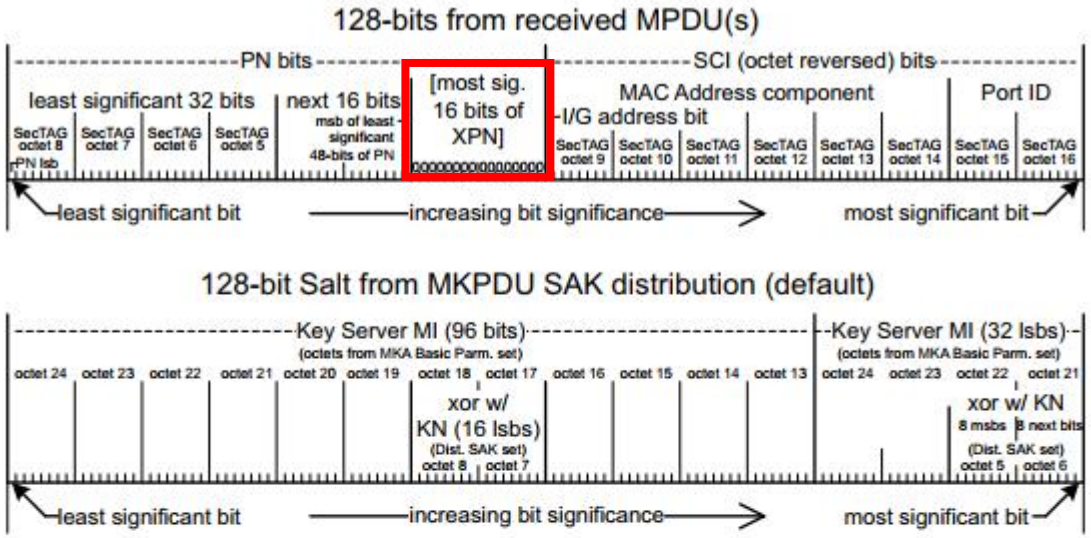


Figure 14-2—Ascon-XPN-128 Nonce construction

The 128 bits contributed to the nonce by the extended Packet Number and the transmitter's SCI are shown in the upper part of Figure 14-2, and are (reading from right to left, most to least significant) as follows:

- The 8 most significant bits are the 8 least significant bits of the SCI's Port Identifier.
- The next 8 significant bits are the 8 most significant bits of the SCI's Port Identifier.
- The next 6 octets comprise the SCI's MAC Address, with the most significant bits being those of the least significant octet of the SCI when that is treated as a binary number as specified in 9.1.
- The next 16 bits are zero, and correspond to the 16 most significant bits of the extended Packet Number, which are restricted to zero for this Cipher Suite.
- The next 48 bits are the 48 least significant bits of the extended Packet Number.

NOTE 2—The SCI contribution to the nonce corresponds to a little endian interpretation of its reception order (if present in the SecTAG), chosen to avoid the need to reverse the octets on reception for Cipher Suite processing. The PN contribution to the nonce corresponds to the numeric evaluation of the PN field as specified in 9.1 since arithmetic operations (range comparison and increment) are required for PN processing.

Table of contents

1 Lightweight Crypto ASCON and NIST.SP.800-232 3

2 Status of IEEE P802.1AEef/D0.3 7

3 **Proposition Ascon*** **11**

4 Advantages for Confidentiality (C) and Integrity (I) Protection 13

Proposition
Reducing A to 14 octets

Field	Size (Octets)	AES-GCM A'	AES-GCM N'	AES-GCM C'	Ascon A	Ascon N	Ascon C	Ascon* A*	Ascon* N*	Ascon* 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	-	-	-	-	-	-	-	-	-

Proposition

- Reducing the A to 14 octets, i.e., $A^* = DA \,||\, SA \,||\, EtherType$,
- Resulting in **one** 16 octet Ascon-p[8] block, i.e., $A_1 = A^* \,||\, 1 \,||\, (0)^{15}$
- Moving the last two octets of the SECTag to the IV, more precisely to the most significant 16 bits of the XPN, which are currently filled by zero.

Table of contents

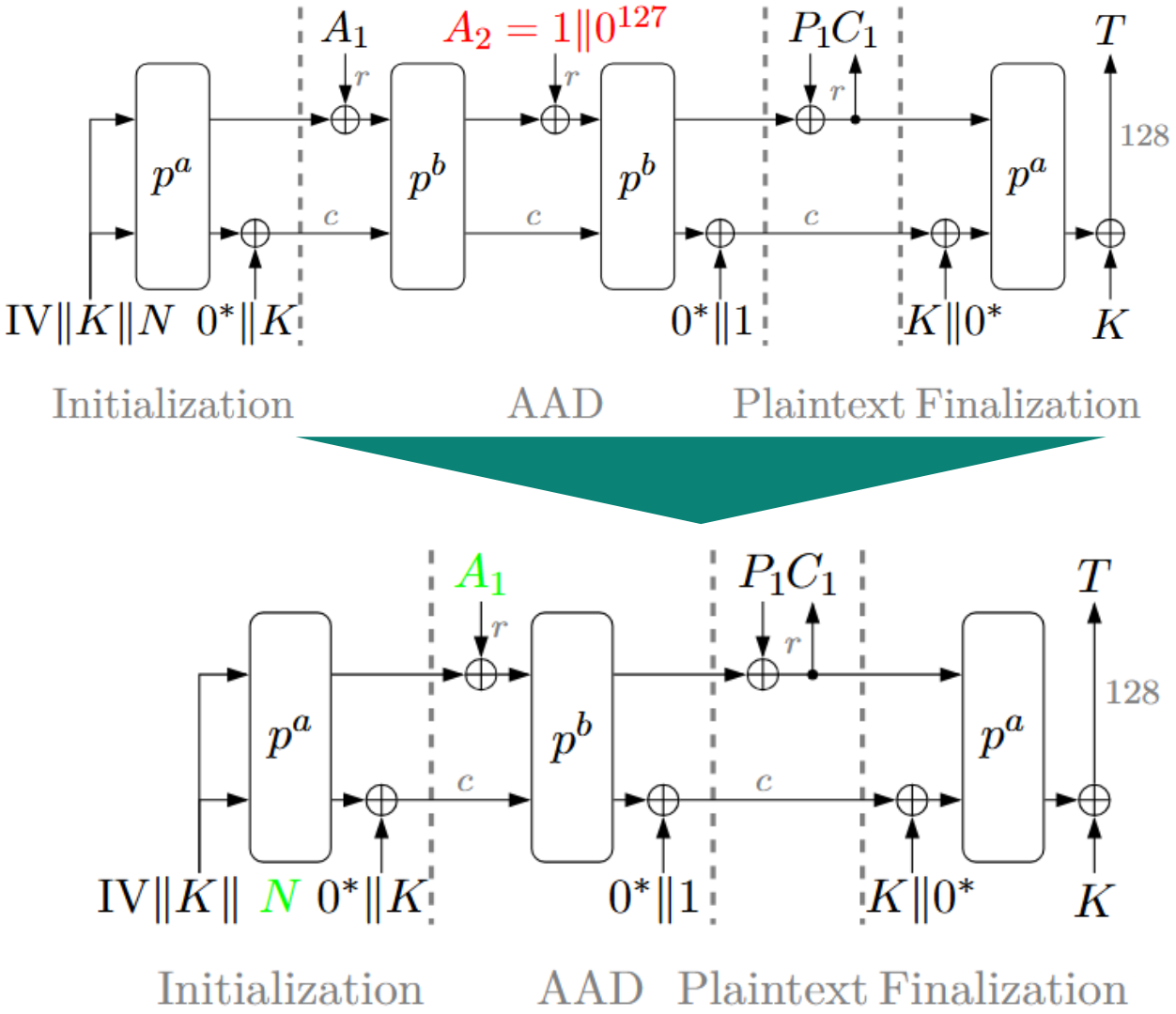
1 Lightweight Crypto ASCON and NIST.SP.800-232 3

2 Status of IEEE P802.1AEef/D0.3 7

3 Proposition Ascon* 11

4 **Advantages for Confidentiality (C) and Integrity (I) Protection** **13**

Illustration of Reduction for Confidentiality Protection |MSDU| < 16 Bytes



A_1 = DA || SA || EtherType || TCI+AN+SL

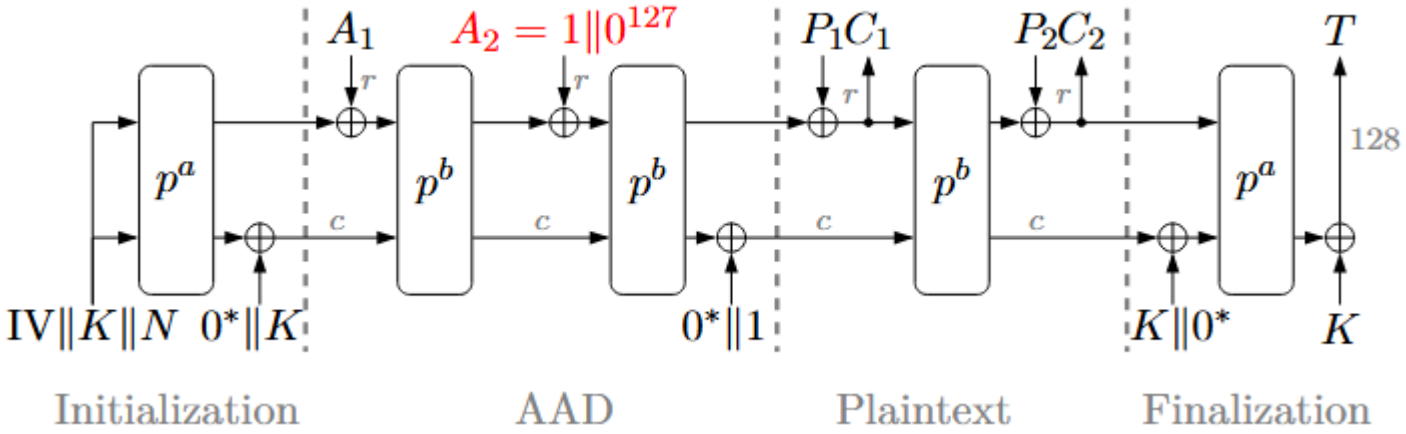
$A_2 = 1 \| (0)^{127}$

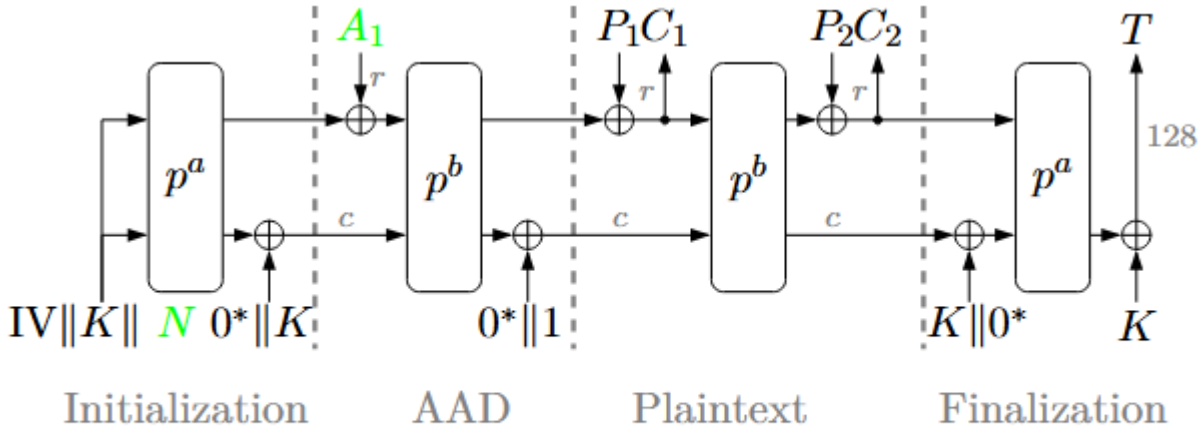
A_1 = DA || SA || EtherType || 1 || $(0)^{15}$

Complexity **Ratio** for |MSDU| < 16 for a=12 and b= 8 is

$$\frac{a+b+a}{a+b+b+a} = \frac{32}{40} = \frac{4}{5}$$

Illustration of Reduction for Confidentiality Protection |MSDU| = 16 Bytes





A_1 = DA || SA || EtherType || TCI+AN+SL

A_2 = 1 || $(0)^{127}$

A_1 = DA || SA || EtherType || 1 || $(0)^{15}$

Complexity **Ratio** for |MSDU| = 16 for a=12 and b= 8 is

$$\frac{a+b+b+a}{a+b+b+b+a} = \frac{40}{48} = \frac{5}{6}$$

Complexity Reduction
For Confidentiality Protection (R_C) and Integrity Protection (R_I)

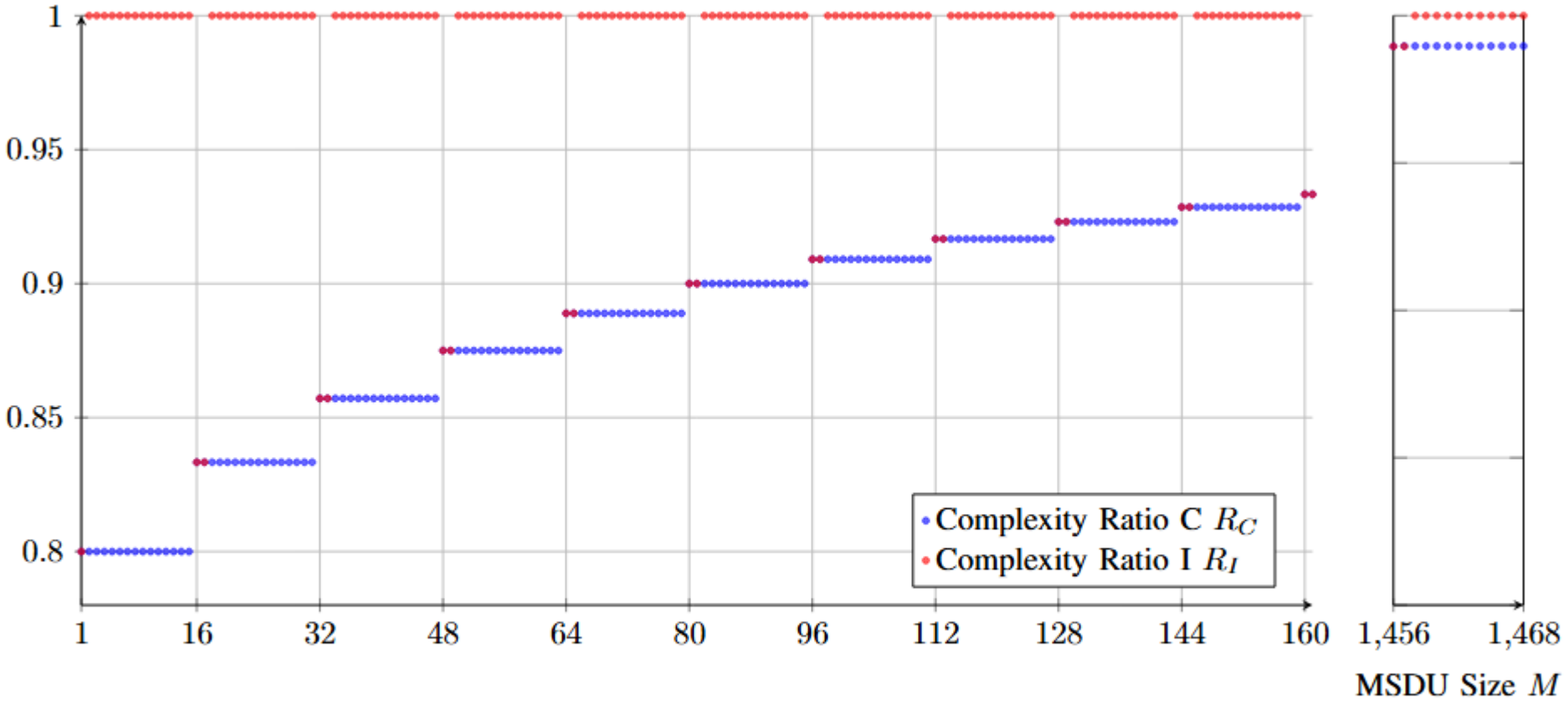


Fig. 2. Complexity ratios of Ascon* relative to Ascon are shown for confidentiality protection $R_C(M)$ (blue) and integrity protection $R_I(M)$ (red). For integrity protection a reduction of complexity $R_I < 1$ occurs for only for $M \bmod 16 = \{0, 1\}$. In contrast, confidentiality protection achieves 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 %.


Infineon