Ascon-Keccak AEAD Algorithm

Stephan Müller

June 19, 2024

Stephan.Mueller at atsec dot com
atsec information security

Abstract

Ascon was selected as finalist in the NIST Lightweight Cryptography competition in 2023. In addition, Ascon was selected as primary choice in the final portfolio of the CAESAR competition. The Ascon specification defines among others an encryption scheme offering authenticated encryption with associated data (AEAD) which is based on a duplex mode of a sponge. With that it is the first of such algorithm selected and about to be standardized by NIST.

The sponge size is comparatively small, 320 bits, as expected for lightweight cryptography. With that, the strength of the defined AEAD algorithm is limited to 128 bits. Albeit, the definition of the Ascon AEAD algorithm integrates with the associated sponge, it is mathematically not bound to exactly this sponge function. Thus, the Ascon AEAD specification can be used with a different sponge and still operate as defined by the Ascon authors.

This specification defines the Ascon-Keccak AEAD algorithm which replaces the Ascon sponge with the Keccak sponge, leaving the Ascon AEAD algorithm unchanged. The selected parameters for Ascon-Keccak AEAD offer two algorithm strengths: Ascon-Keccak 256 with a ~~classic~~ security strength ~~of 256 bits and a quantum security strength of 128 bits~~compliant to the NIST security category 5. In addition, Ascon-Keccak 512 provides an algorithm ~~with 512 bit classic security strength and 256 bit quantum security strength~~ exhibiting a significantly stronger mechanism than the NIST security category 5. The selected parameters for Ascon-Keccak 256 offer a significant higher performance on 64-bit architectures than Ascon-128 and Ascon-128a. The performance of Ascon-Keccak 512 is in league with Ascon-128. Yet, with the Keccak sponge size of 1600 bits, Ascon-Keccak cannot be considered a lightweight cryptographic algorithm any more. A reference implementation of the algorithm is given with leancrypto.

Contents

List of Tables

1 Introduction

With the selection as finalist in the NIST Lightweight Cryptography competition in 2023 and being the primary choice of the final portfolio of the CAESAR competition, Ascon is a well-recognized algorithm suite. It contains an encryption schema offering authenticated encryption with associated data (AEAD) based on a duplex mode of a sponge . It is the first of such algorithm selected and about to be standardized by NIST.

The size of the sponge comparatively small, 320 bits, which is appropriate and expected for lightweight cryptography. However, that size only allows a security strength of 128 bits for the AEAD algorithm. Even though, the Ascon AEAD algorithm definition integrates the the associated sponge , it is mathematically not bound to exactly this sponge function. Following that thought, the Ascon AEAD specification can be used with a different sponge and still operate as defined by the Ascon authors.

This specification uses the Keccak sponge as defined [1] and integrates it into the Ascon AEAD algorithm. The selected parameters result in the following two algorithms:

- Ascon-Keccak 256 with a ~~classic~~ security strength ~~of 256 bits~~ compliant to the NIST security category 5 ~~and a quantum security strength of 128 bits~~,
- Ascon-Keccak 512 providing an algorithm ~~with~~ which is ~~512 bit classic security strength~~significantly stronger than the NIST security category 5 following [5] appendix A.5 ~~and 256 bit quantum security strength~~.

A reference implementation of the algorithm is given with leancrypto.¶

The use of Keccak sponge in a duplex mode was first proposed in [3] whose considerations apply to this definition as well. The Keccak authors define an AEAD algorithm named Keyak which uses the Keccak sponge function in a similar approach as outlined in this document for Ascon-Keccak. However, the Ascon-Keccak specification did not consider Keyak. The reason is the following: due to Ascon being accepted by NIST as part of the lightweight cryptography competition, an AEAD algorithm specification using a sponge function is considered a finalist during the public competition. Thus, this accepted AEAD specification is used and simply the sponge function is replaced with appropriate parameter sets with the expectation that the security analysis of Ascon is still applicable.

2 Ascon-Keccak AEAD Algorithm Specification

The Ascon specification provided with [4] contains in section 2.4 the algorithm definition for the AEAD encryption and decryption operation. This algorithm specification outlines how the sponge state is initialized with key, IV and a nonce, how the associated data is authenticated, how plaintext data is transformed into ciphertext and vice versa, and how the authentication tag is obtained.

Name	Key (Bits)	Nonce (Bits)	Tag (Bits)	Data Block (Bits)	Rounds p^a	Rounds p^b
Ascon-Keccak 256	256	128 to 256	128 to 256	1,088	24	24
Ascon-Keccak 512	512	128 to 512	128 to 512	576	24	24

Table 1: Parameters for recommended authentication encryption schemes

The Ascon permutation operation forming the basis for the sponge is defined in [4] section 2.6.

Finally, the parameter sets for Ascon-128 and Ascon-128a are defined in [4] section 2.2 which defines the sizes of the key, nonce and authentication tag along with the Ascon sponge round counts.

The following sections define the Ascon-Keccak AEAD algorithm based on the same structure as the original Ascon specification [4].

2.1 Recommended Parameter Sets

The authenticated encryption uses the parameter sets defined in Table 1. It specifies the same parameters as the original Ascon definition in [4] section 2.2.

The basic considerations for the selected parameter sets are the following:

- The Keccak permutation state size and the round counts are equal to the definition of Keccak-p[1600,24] specified in [1], i.e. the definition used for SHA-3 and SHAKE.
- Ascon-Keccak 256 segments the Keccak sponge state size into the rate / capacity equal to the parameters used for SHA3-256 defined in [1], i.e. capacity of 512 bits and rate 1,088 bits.
- Ascon-Keccak 512 segments the Keccak sponge state size into the rate / capacity equal to the parameters used for SHA3-512 defined in [1], i.e. capacity of 1,024 bits and rate 576 bits.

From the basic considerations for the parameter sets, the following Ascon-Keccak parameter set rationale applies:

- The key size is defined to be equal to half of the selected capacity of the sponge.
- The tag size is at least 128 bits as required by the Ascon specification, but is allowed to be larger up to the key size. This is based on the fact that the tag is obtained from the data block of the sponge state which is modified by the key as the last Ascon AEAD encryption / decryption step. Thus, the tag shall not be larger than the key size.
- The data block size is equal to the rate of the selected sponge.

2.2 Authenticated Encryption

The authenticated encryption is defined to be basically equal to the ASCON encryption specification given in [4] section 2.4 with adjustments only due to KECCAK specifics of the state size and the increased size of the tag.

2.2.1 Initialization

The initialization vector is defined based on the specification given in [4] section 2.4.1. Considering that KECCAK also operates on 64-bit words, the IV size is equally defined as 64 bit value using the parameter set defined in Table 1.¶

To provide proper domain separation for the applied tag size, the IV construction is extended to include the size of the tag value. Therefore, the IV is defined as:¶

$$IV_{k,r,a,b,t} - k||r||a||b||t||0^{1600-k}$$

with:¶

- k referencing the key size in bytes represented by an 8-bit integer,¶
- r referencing the rate in bytes represented by an 8-bit integer,¶
- a referencing the initialization and finalization round number represented by an 8-bit integer,¶
- b referencing the intermediate round number represented by an 8-bit integer,¶
- t referencing the tag size in bytes represented by an 8-bit integer,¶

The applied IVs are as follows for the example of the minimum and maximum tag sizes – when using other tag sizes, the fifth byte in the IV must be set accordingly:÷

- ASCON-KECCAK 256 with tag size 128 bits: 0x0100044000180018208818181000000 0¶
- ASCON-KECCAK 256 with tag size 256 bits: 0x2088181820000000
- ASCON-KECCAK 512 with tag size 128 bits: 0x0200024000180018404818181000000 0¶
- ASCON-KECCAK 512 with tag size 512 bits: 0x4048181840000000

Considering that the KECCAK sponge size is 1,600 bits compared to the ASCON sponge size of 320 bits, and the requirement that the key is inserted at the end of the sponge state, the initialization is performed with the following steps:

$$S \leftarrow IV_{k,r,a,b,t}||K||N$$

This is followed by a second insertion of the key after a sponge operation:

$$S \leftarrow p^a(S) \oplus (0^{1600-k}||K)$$

Thus, the initialization is identical to the specification of [4] section 2.4.1 after applying the KECCAK sponge size.

2.2.2 Processing of Associated Data

The processing of the associated data is fully identical to the specification of [4] section 2.4 with the only difference that the domain separation constant inserted into the last bit of the sponge state must consider the KECCAK state size:

$$S \leftarrow S \oplus (0^{1599}||1)$$

2.2.3 Processing Plaintext / Ciphertext

The processing of the plaintext / ciphertext is fully identical to the specification of [4] section 2.4.

2.2.4 Finalization

The finalization is fully identical to the specification of [4] section 2.4 with the exception that the tag is defined as follows depending on the chosen tag size t:

$$S \leftarrow p^a(S \oplus (0^r||K||0^{c-k})$$

$$T \leftarrow \lceil S \rceil^t \oplus \lceil K \rceil^t$$

with

$$128 \leq t \leq k$$

2.3 Permutation

As already indicated in the preceding sections, the KECCAK permutation as specified in [1] section 5.2 is applied to replace the ASCON permutation operation. Specifically, the permutation of KECCAK-p[1600,24] is applied, which is also the basis for SHA-3 and SHAKE.

3 Security Claims

The ASCON-KECCAK 256 algorithm provides 256-bit security strength, and ASCON-KECCAK 512 provides 512-bit security strength for the protection of the confidentiality of the data. The security strength of the integrity depends on the selected tag length and can reach 256-bit security strength for ASCON-KECCAK 256 and 512-bit security strength for ASCON-KECCAK 512 if the largest tag size is selected.

The number of processed plaintext and associated data blocks protected by the encryption algorithm is limited to the same number as specified in [4] section 3.1: 2^{64} blocks. This translates into $2^{71}+2^{67}$ bytes for ASCON-KECCAK 256 and $2^{70}+2^{67}$ bytes for ASCON-KECCAK 512. As stated in [4] section 3.1: "In order

Requirement	Ascon-Keccak 256 (Bits)	Ascon-Keccak 512 (Bits)
Confidentiality of plaintext	256	512
Integrity of plaintext	128 to 256	128 to 512
Integrity of associated data	128 to 256	128 to 512
Integrity of public message number	128 to 256	128 to 512

Table 2: Security claims for recommended parameter configurations of Ascon-Keccak

to fulfill the security claims stated in Table 2, implementations must ensure that the nonce (public message number) is never repeated for two encryptions under the same key, and that decrypted plaintexts are only released after successful verification of the final tag. The difference between the family members is in their robustness against other adversaries beyond the classical security claim and is discussed in the following."

The security strength of the confidentiality depends on the capacity of the Keccak sponge where the attack complexity is $2^{c/2}$ which implies that the robustness of Ascon-Keccak 256 is 256 bits ($c = 512$), and Ascon-Keccak 512 is 512 bits ($c = 1024$) based on the assessment given in [4] section 3.1. The security strength claims are supported by the numbers specified in [1] Appendix A.1 for SHA3-256 and SHA3-512 considering that the Keccak sponge is operated identically to SHA3-256 and SHA3-512, respectively.

According to [4] section 3.1, the same holds true for key recovery attacks.

The security strength of the integrity of the plaintext and associated data depends on the size of the tag which is allowed to be between 128 bits and 256 or 512 bits, respectively.

Considering Grover's algorithm, the security strength against a quantum adversary depends on the key size and the capacity of the Keccak sponge. It is therefore defined as $min(key\ size, 2^{c/4})$. Therefore, Ascon-Keccak 256 has a security strength of 128 bits and Ascon-Keccak 512 has a security strength of 256 bits against quantum adversaries. However, as outlined in [5] Appendix A.5, this naïve calculation only considers the quadratic quantum speedup but ignores the "long-running serial computation, which is difficult to implement in practice. In a realistic attack, one has to run many smaller instances of the algorithm in parallel, which makes the quantum speedup less dramatic." Thus, considering the table in [5] Appendix A.5, the security strength of Ascon-Keccak is therefore defined as:¶

- Ascon-Keccak 256 complies with NIST security category 5.¶
- Ascon-Keccak 512 is significantly stronger than NIST security category 5. Considering it operates the Keccak sponge equivalent to SHA3-512 the security of Ascon-Keccak 512 is compliant to the security strength of

SHA3-512 as defined in table 5 in [5] Appendix A.5 by requiring 2^{274} classical gates for an optimal key recovery attack. This indicates a significantly stronger algorithm than the NIST security category 5.

As outlined in [4] section 3.1, except for the single-use requirement, there are no constraints on the choice of the nonce (public message number); in particular, it is possible to use a simple counter.

4 Security Analysis

The entire specification of Ascon-Keccak is based on the identical reuse of Ascon AEAD with the difference that the sponge is replaced. The following subsections provide the security analysis of the relevant components following [4] chapter 6.

4.1 Analysis of Authenticated Encryption

The security analysis given in [4] section 6.2.2 applies in full considering that the Ascon authenticated encryption is applied. The deviations from the Ascon specification have the following effect:

- Initialization: The algorithm difference places the key into the last bits of the sponge state. As the Ascon sponge size is different than the Keccak sponge size, the mathematical representation of the operation differs. Yet, this mathematical difference has no bearing on the security posture of the algorithm.
- Finalization: The tag size differs to allow larger tag sizes at most equal to the key size. As the key size is also strictly smaller than the capacity of the Keccak sponge , and the largest allowed tag size are equal to the key size, the specification is identical to the Ascon concepts. Thus, security analysis results from Ascon applies in full.
- Endianess: The difference in endianess between the Ascon sponge and the Keccak sponge mentioned in chapter 5 is considered to have no impact on the security posture as still all data is processed in the same manner.

4.2 Analysis of the Permutation

As the Keccak permutation is operated identical to the SHA3-256 and SHA3-512 hashing operation, the security analysis provided by [2] chapter 4 is applicable based on the claims in [1] Appendix A. Thus, this security analysis applies to the specified Ascon-Keccak algorithms in full.

5 Reference Implementation

A reference implementation of Ascon-Keccak is provided with leancrypto. To demonstrate also that its implementation matches the aforementioned specification, the following considerations are applied:

- The library implements Ascon-128 and Ascon-128a which are both demonstrated to match the implementation given in [4] by using the test vectors obtained from the Ascon reference implementation.
- The Ascon-128 and Ascon-128a implementation is such that the Ascon AEAD operation is separated from the sponge implementation.
- The Ascon-Keccak 256 and 512 implementations are provided by simply replacing the Ascon permutation and applying the Keccak sponge size for the initialization operation. Thus, the Ascon AEAD code is shared for both Ascon-128/128a and Ascon-Keccak.
- The Keccak sponge implementation is also used for the SHA-3 algorithm family which is demonstrated to correctly generate the respective message digests using the NIST reference implementation provided with the ACVP service including obtaining official certificates, such as A4850.
- Considering that the Ascon sponge is operated in big-endian mode whereas the Keccak sponge is operated in little-endian mode, an appropriate bit-swap logic is applied when inserting data into or retrieving data from the sponge.

5.1 Performance of Ascon-Keccak

Based on the reference implementation, the following performance data is obtained. The following tables show the performance data with the C implementation of both sponges, Keccak and Ascon. Albeit accelerated sponge implementations are also present in leancrypto for both, they cannot be used for comparison, naturally.

Hardware	Word size	Ascon-128	Ascon-128a	Ascon-Keccak 256	Ascon-Keccak 512
AMD Ryzen 9 5950X	64-bit	11.33s	9.86s	7.91s	12.99s
ARM Cortex-A72	64-bit	32.93s	23.08s	19.54s	31.96s
ARM Cortex-A76	64-bit	18.23s	13.03s	10.12s	16.81s
Apple M2	64-bit	9.56s	7.01s	5.32s	9.20s
Intel 11th Gen Core i7 - 1165G7	64-bit	11.72s	8.18s	7.02s	11.85s
Intel 12th Gen Core i7 - 1280P	64-bit	10.32s	6.94s	6.24s	10.46s
Intel Atom Z530	32-bit	335.92s	205.51s	298.28s	441.94s
Intel Core Ultra 7 155H	64-bit	11.90s	8.37s	7.57s	13.48s
RISC-V SiFive U74	64-bit	160.31s	110.43s	106.90s	175.45s

Table 3: Encryption/Decryption of 1 GB Data with Ascon and Ascon-Keccak

Hardware	Word size	Ascon-128	Ascon-128a	Ascon-Keccak 256	Ascon-Keccak 512
ARM Cortex-A8 r2p5 v7l	32-bit (with 32 64-bit registers)	11.18s	15.31s	16.62s	29.73s
ARM Cortex-A7 r0p5 v7l	32-bit (with 16 64-bit registers)	27.38s	39.99s	42.18s	76.38s

Table 4: Encryption/Decryption of 100 MB Data with Ascon and Ascon-Keccak

The performance may look a bit surprising at first considering that Ascon-Keccak 256 is always faster on 64-bit architectures[1][2] than the fastest Ascon

[1]The 32-bit ARM Cortex-A7 shows that Ascon-Keccak is generally slower than Ascon AEAD. It is assumed that this is due to the fact that this CPU only offers 16 64-bit registers compared to ARM Cortex-A8 which offers 32 64-bit registers. Thus, the Keccak state of 25 64-bit integers will not fit completely into the existing numbers of registers, requiring the compiler to either reload existing registers or to split the processing of some 64-bit integers into sets of two 32-bit operations.

[2]The 32-bit Intel Atom Z530 has no 64-bit registers and thus the larger number of 64-bit

AEAD algorithm and knowing that the KECCAK sponge (a) is more complex and (b) performed with a significant larger round count. But the factor of the processed data block size plays the leading role. For ASCON-KECCAK it is defined to be equal to the rate which is significantly larger than for ASCON AEAD. Thus the data is processed by ASCON-KECCAK in much larger data blocks than for ASCON AEAD.

operations with KECCAK imply a significant more set of 32-bit operations compared to ASCON AEAD.

Acknowledgements

The author thanks Caroline Holz auf der Heide, and Joachim Vandersmissen for comments on earlier drafts of the paper.

References

[1] *FIPS PUB 202 SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions*. NIST, August 2015. https://doi.org/10.6028/NIST.FIPS.202.

[2] G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche. *The KECCAK reference*. January, 2011. http://keccak.noekeon.org/Keccak-reference-3.0.pdf.

[3] Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche. Duplexing the sponge: Single-pass authenticated encryption and other applications. In Ali Miri and Serge Vaudenay, editors, *Selected Areas in Cryptography - 18th International Workshop, SAC 2011, Toronto, ON, Canada, August 11-12, 2011, Revised Selected Papers*, volume 7118 of *Lecture Notes in Computer Science*, pages 320–337. Springer, 2011.

[4] Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Martin Schläffer. *Ascon Sumission to NIST*. May 31, 2021. https://ascon.iaik.tugraz.at/files/asconv12-nist.pdf.

[5] NIST. Submission requirements and evaluation criteria for the post-quantum cryptography standardization process. Official Call for Proposals, National Institute for Standards and Technology, December 2016.

