Contents

1 Permutation **2**
1.1 Introduction . . . 2
1.2 The sponge construction . . . 2
1.3 The duplex construction . . . 3
1.4 Permutation in ASCON . . . 3
1.4.1 Substitution-Permutation network . . . 3
1.4.2 Constant addition layer p_C . . . 4
1.4.3 Substition layer p_C . . . 4
1.4.4 Diffusion layer p_C . . . 4
1.5 Design of the permutation . . . 5

Lightweight Crytolography Challenges and Approaches

Aitaza, A.	Ozan	Anastasios, T.	Maugueret, A. D.
aka2973@thi.de	abc1234@thi.de	abc1234@thi.de	adm5462@thi.de

May 2024

1 Permutation

1.1 Introduction

Permutation is a fundamental concept in cryptography. It is used in various cryptographic algorithms such as block ciphers, hash functions, and stream ciphers. A permutation is a bijective mapping from a set to itself. While it is a simple operation, it is actually one of the most important concepts used within the ASCON family.

1.2 The sponge construction

An interesting application of permutation in cryptography is the **sponge construction**. It relies on a fixed-length permutation and a padding rule to create a sponge function that can map variable-length input to variable-length output. [1]

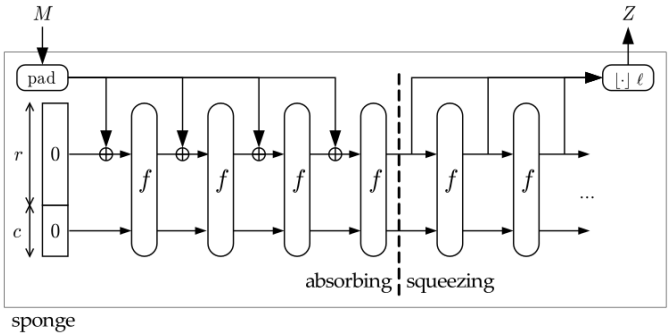

Figure 1: The sponge construction.

A sponge function is made up of three components: a state memory S containing b bits, a function $f : \{0,1\}^b \to \{0,1\}^b$ and a padding function P. [1, 2]

- S is divided into two parts: the rate r and the capacity c. The rate is the part of the state that is XORed with the input message, while the capacity is the part that is not. The capacity is also the part that is permuted by the function f
- f produces a pseudo random permutation of the 2^b possible states
- P is a function that pads the input message to a multiple of r

The sponge function is performed iteratively in two phases: the **absorbing phase** and the **squeezing phase**. The padded input M which is cut into r bit blocks. In the absorbing phase, chucks of the input message are mixed at the beginning of the buffer using XOR operations. This can be seen in Figure 1 with the operation $r \oplus P_i$. At each step, this new buffer is again passed through f causing a small amount of data to be "absorbed" into the semi-randomised buffer. [1, 2, 3]

In the squeezing phase, the buffer is read out in chunks of the desired output length. This is done by applying f to the buffer and outputting the first r bits of the result. This process is repeated until the output Z with the desired

length ℓ is reached. [1, 2, 3]

The last c bits are neither XORed nor directly output.

1.3 The duplex construction

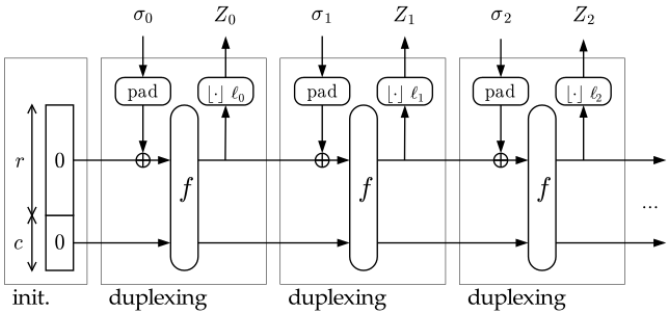

Figure 2: The duplex construction.

An alternation of the sponge construction is the **duplex construction**. Permutation function f, padding function P and parameter bitrate r are also used in the duplex construction, while σ is the input string and ℓ is the requested number of bits. [1, 2, 4]

While the sponge function is stateless between calls, the duplex version alternates between absorbing data into the state and squeezing data out of the state, where the output depends on all the previous inputs. [4, 5] During the absorption phase, input data is XORed with the rate part of the state and then permuted using the permutation function. During the squeezing phase, output data is obtained by reading from the rate part of the state while keeping the capacity part fixed.

1.4 Permutation in ASCON

The ASCON family uses the concept of permutation in its design. The components of the encryption and hashing schemes are the two 320-bit permutations p^a and p^b, where a and b are the number of times the round transformations are performed. For example, the parameters for ASCON-128 are $a = 12$ and $b = 6$, while being $a = 12$ and $b = 8$ for ASCON-128a. The permutation function is based on a substitution-permutation network (SPN) structure. [3, 6]

1.4.1 Substitution-Permutation network

It is a type of block cipher that uses a series of substitution and permutation operations.

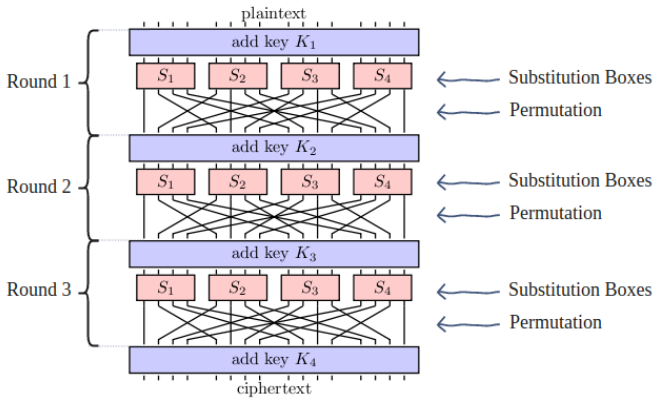

Figure 3: SPN structure.

SPN structures consists of boxes called S-boxes that perform substitution operations and P-boxes that perform permutation operations. The S-boxes and P-boxes transform (sub-)blocks of input bits into output bits. Some

common operations include simple and efficient XOR and bitwise rotation. [7]

In the case of ASCON, the round transformation p is based on an SPN structure. It consists of three main components: the constant addition layer p_C, the substitution layer p_S, and the linear diffusion layer p_L. [3, 6]

$$p = p_C \circ p_S \circ p_L$$

In order to prepare the 320-bit state for the round transformations, the state is first divided into five 64-bit words. The round transformation p is then applied to the state. [3]

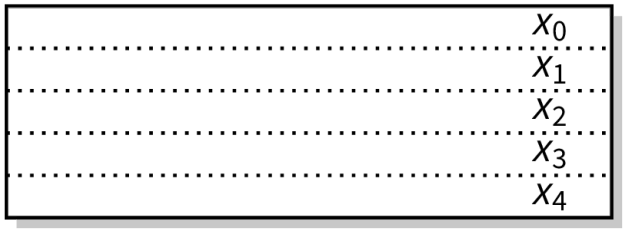

Figure 4: The state divided into 5 64-bit words.

In each round of the permutation p of ASCON, the following operations are performed:

1.4.2 Constant addition layer p_C

In p_C, a round specific 1-byte constant is XORed to x_2. [6, 8]

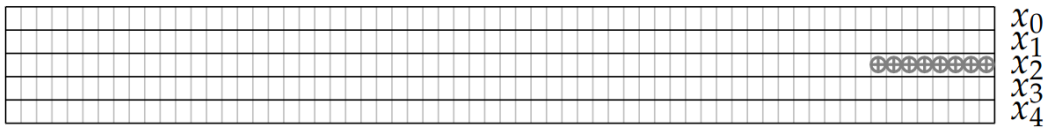

Figure 5: The constant addition layer p_C.

1.4.3 Substition layer p_C

In p_S, a 5-bit S-box is applied to each byte of the state. It is the application of a 5-bit S-box 64 times in parallel vertically. [6, 8]

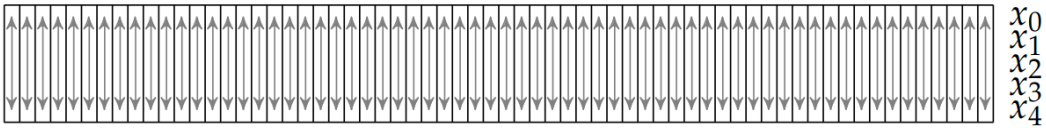

Figure 6: The substitution layer p_S.

1.4.4 Diffusion layer p_C

in p_L, a linear diffusion matrix is applied to the state which only consists of XOR and right rotation of the 64-bit words x_0, x_1, x_2, x_3, x_4. [6, 8]

The linear layer can be described as follows:

$\sum_0(x_0) = x_0 \oplus (x_0 \ggg 19) \oplus (x_0 \ggg 28)$

$\sum_1(x_1) = x_1 \oplus (x_1 \ggg 61) \oplus (x_1 \ggg 39)$

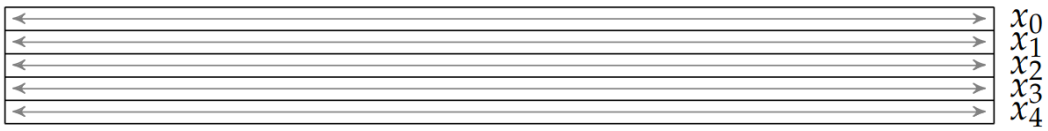

Figure 7: The diffusion layer p_L.

$\sum_2(x_2) = x_2 \oplus (x_2 \ggg 1) \oplus (x_2 \ggg 6)$

$\sum_3(x_3) = x_3 \oplus (x_3 \ggg 10) \oplus (x_3 \ggg 17)$

$\sum_4(x_4) = x_4 \oplus (x_4 \ggg 7) \oplus (x_4 \ggg 41)$

[6, 8]

1.5 Design of the permutation

There are several design criteria that need to be considered when designing a permutation for cryptographic purposes. In ASCON security was prioritised but also the performance was taken into account.

For the constant addition layer p_C, the round constants are chosen to prevent certain types of attacks and are added to the state in a simple, predictable manner for ease of computation. They are positioned strategically to facilitate efficient pipelining with other operations.

The S-box used in the substitution layer p_S is carefully designed to meet various criteria, including invertibility, resistance against differential and linear cryptanalysis, and efficient implementation in hardware and software.

The linear diffusion layer mixes the bits within each word of the state. It is designed to resist linear and differential cryptanalysis while providing good diffusion. The rotation constants are chosen similar to those used in SHA-2 functions to balance performance and security.

[3]

References

[1] Keccak Team. *Sponge Duplex Construction*. Accessed 14-May-2024. 2024. URL: https://keccak.team/sponge_duplex.html.

[2] Wikipedia. *Sponge Function*. Oct. 2023. URL: https://en.wikipedia.org/wiki/Sponge_function#Duplex_construction.

[3] Christoph Dobraunig et al. "Ascon v1.2: Lightweight Authenticated Encryption and Hashing". In: *J. Cryptol.* 34.3 (2021), p. 33. DOI: 10.1007/s00145-021-09398-9. URL: https://doi.org/10.1007/s00145-021-09398-9.

[4] Guido B and D, Joan and Michaël P. "Cryptographic Sponge Functions". In: *Cryptographic Sponge Functions* (Jan. 2011).

[5] Charlotte Lefevre and Bart Mennink. *Generic Security of the Ascon Mode: On the Power of Key Blinding*. Cryptology ePrint Archive, Report 2023/796. https://eprint.iacr.org/2023/796. 2023.

[6] IAIK. *Ascon Specification*. https://ascon.iaik.tugraz.at/specification.html. Accessed: May 14, 2024. 2024.

[7] Anusheh Zohair Mustafeez. *What are Substitution-Permutation Networks?* https://www.educative.io/answers/what-are-substitution-permutation-networks. 2024.

[8] Cihangir Tezcan. "Analysis of Ascon, DryGASCON, and Shamash Permutations". In: *International Journal of Information Security Science* 9.3 (2020), pp. 172–187.