Introduction to Cryptography
Part VII: Symmetric Cryptography (Again)

André Schrottenloher

Inria Rennes
Team CAPSULE

Constructing Hash Functions

How to transform a block cipher into a compression function

Reminder

A **block cipher** is a family of **permutations** of $\{0,1\}^n$ indexed by a key.

50 years of symmetric cryptography have shown that we know better how to construct **permutations** than **non-invertible functions**.

Reminder

- A **compression function** is a **non-invertible** function $\{0,1\}^m \times \{0,1\}^n \rightarrow \{0,1\}^n$ ($\simeq$ fixed-length hash function).
- Security: collisions, preimages, second preimages.

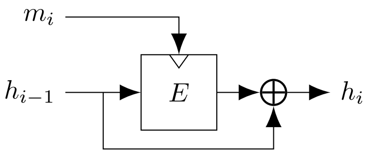
How to transform a block cipher into a compression function

There are several **secure modes** (see poly), for example Davies-Meyer:

How to transform a block cipher into a compression function

There are several **secure modes** (see poly), for example Davies-Meyer:

- Use key as message block input $m_i \in \{0,1\}^m$
- Use block as chaining value input $h_i \in \{0,1\}^n$
- XOR block to the output to make it non-invertible



$$h_i = h_{i-1} \oplus E_{m_i}(h_{i-1})$$

If the block cipher is **ideal**, the DM-based compression function is secure.

Note that...

...it is also **very easy** to produce insecure modes, for example:

$$f(h_{i-1}, m_i) = E_{m_i \oplus h_{i-1}}(m_i \oplus h_{i-1}) \oplus m_i$$

$\Longrightarrow$ one can produce preimages.

Note that...

...it is also **very easy** to produce insecure modes, for example:

$$f(h_{i-1}, m_i) = E_{m_i \oplus h_{i-1}}(m_i \oplus h_{i-1}) \oplus m_i$$

$\implies$ one can produce preimages.

Attack

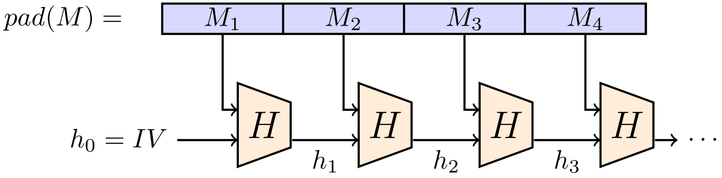
- Notice that if $m_i \oplus h_{i-1} = c$, then:

$$f(h_{i-1}, m_i) = E_c(c) \oplus m_i$$

- Fix $m_i = E_c(c)$, choose $h_{i-1} = E_c(c) \oplus c$, then:

$$f(h_{i-1}, m_i) = 0$$

Merkle-Dåmgard domain extender



From a fixed-length compression function
$H : \{0,1\}^m \times \{0,1\}^n \to \{0,1\}^n$:

- **pad** the message using a secure padding
- Separate the message in blocks of size m
- Absorb the blocks by iterating the compression function

Theorem (informal)

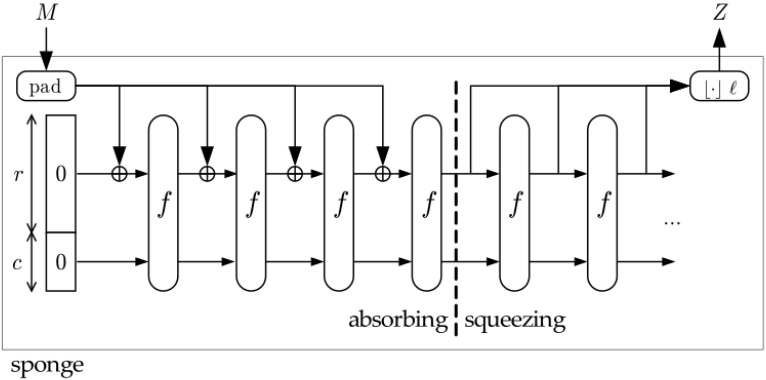
If the compression function is (collision, preimage, second-preimage)-resistant, and the padding scheme is secure, the MD extension is resistant.

MD: caution

- Many algorithmic attacks using the iterated construction;
- Proof of security guarantees only $n/2$ bits where n is the size of the chaining value, for collisions **and preimages**;
- For more security, one needs a bigger chaining value (128 is not enough).

(Duplex) Sponges

The Sponge: hash functions



- f is a **cryptographic permutation**
- Speed of absorption determined by the **rate** r
- Security determined by the **capacity** c

Attacks (examples)

Collisions

Find two pairs of messages such that the inner part collides: $2^{c/2}$.

Preimages

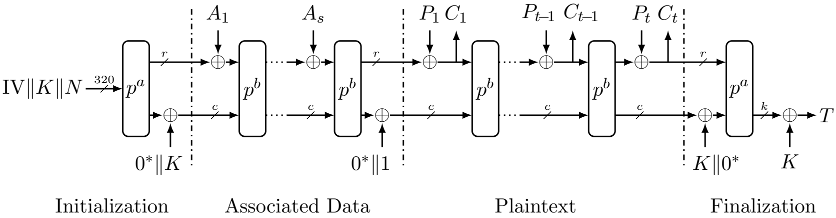
Compute forwards from the initial state and backwards from the output: try to collide on the inner part: $2^{c/2}$.

ASCON-AEAD

- Winner of the NIST lightweight cryptography competition
- Based on a **Duplex Sponge** mode

https://csrc.nist.gov/csrc/media/Presentations/2023/the-ascon-family/images-media/june-21-mendel-the-ascon-family.pdf

ASCON-AEAD



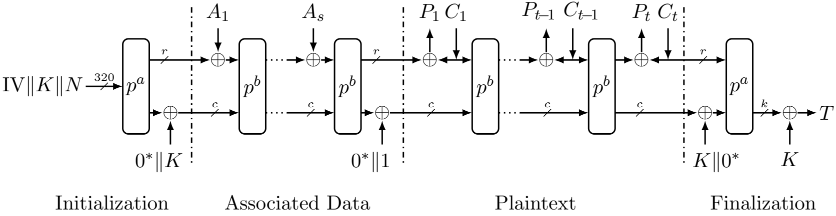
Parameters of ASCON-128

Security	128
Key	128
Rate	64
Capacity	256
Rounds (a,b)	12, 6

Caution

The mode is **nonce-based**: N should not be reused with different messages.

Ascon: decryption



Constructing a Block Cipher

Constructing a Block Cipher

Shannon identified two properties that a symmetric cipher should satisfy, which are still loosely present in nowadays' designs.

Confusion

The relation between the key, plaintext and ciphertext should be complex.

Diffusion

A minor change in the plaintext should affect the entire ciphertext.

These criteria are rather unquantifiable, which is why nowadays we rely directly on **cryptanalysis** studies.

Shannon, "A Mathematical Theory of Cryptography", 1945

Round of a Substitution-Permutation Network

Addition of a round key

The round key is derived from the master key using a **key scheduling** routine.

Substitution layer $\implies$ "confusion"

Applies a small nonlinear **S-Box** to the bytes / nibbles of the state.

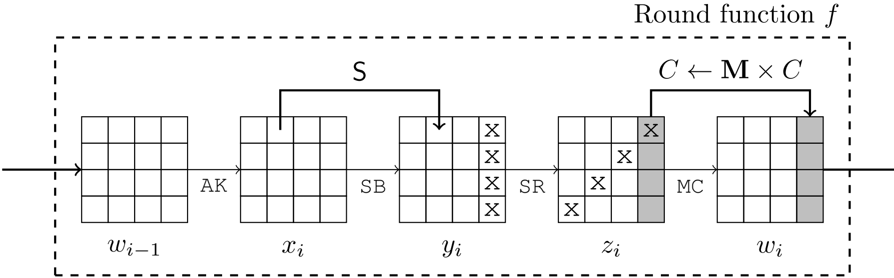
Permutation layer $\implies$ "diffusion"

Applies a large linear function to the state.

Linear / nonlinear over $\mathbb{F}_2$ or extensions.

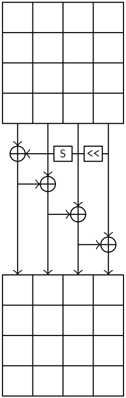
Example: AES

- Standardized by NIST in 2001 to replace DES
- Chosen after an open competition: the candidate's name was Rijndael, and its authors Daemen and Rijmen



- 128 bits of state (16×8)
- 128, 192 or 256 bits of key
- 10, 12 or 14 rounds

AES (-128) Key-scheduling



+ round constants.

- Bytes of the state and key are viewed as members of $\mathbb{F}_{2^8}$.
- Operations (except S-Box) are linear over $\mathbb{F}_{2^8}$.

Cryptanalysis

- Cryptanalysis of **modes** (encryption, hash function) focuses on generic attacks that would contradict the security proofs / conjectures, or would have been overlooked
- Cryptanalysis of **primitives** searches for "anything that distinguishes this function from random"

There exists a **wide array of techniques** classified depending on the **type of properties** that they exploit:

- Linear cryptanalysis: exploiting biases in Boolean functions
- Algebraic cryptanalysis: exploiting the algebraic expressions of Boolean functions
- Differential cryptanalysis: exploiting differential properties of functions
- ...

Checklist

- Statistical indistinguishability vs. computational indistinguishability: definition with one and two games
- IND-CPA, proof that ElGamal is IND-CPA
- Notion of IND-CCA security
- RSA cryptosystem, RSA assumption
- Discrete log, DDH, CDH, the birthday paradox
- Notion of digital signature scheme, unforgeability
- Hash functions and their security (collision, preimage, second preimage)
- Symmetric encryption (not the definitions of all the modes), block ciphers