

isec 2024: Fragestunde 2024W47

Kryptographie

Symmetrisch (beide haben selben Schlüssel)

- Verschlüsselung (Chiffre): AES
- Hash: SHA-2-256, SHA-2 → MAC: HMAC
- Kombi: AEAD (s. auch Blockwoche)

Asymmetrisch (jeder hat eigenes Schlüsselpaar)

- Nächste Woche

Symmetrische Verschlüsselung

AES

Symmetrische Verschlüsselung

AES: Blockchiffre

- Blockgröße 128 bit (16 Bytes)
- Schlüssellänge 128, 192, 256 bit

Betriebsarten:

- ECB: schlecht
- CBC: alt (padding!)
- CTR: aktuell

Zufallszahlen

Hash

Funktion: beliebig langer Input → konstant langer output

kryptographischer Hash:

Anforderungen:

- Kollisionsresistenz
 - Geburtstagsparadox
- Urbild
- Urbild2

Aktuelle Auswahl

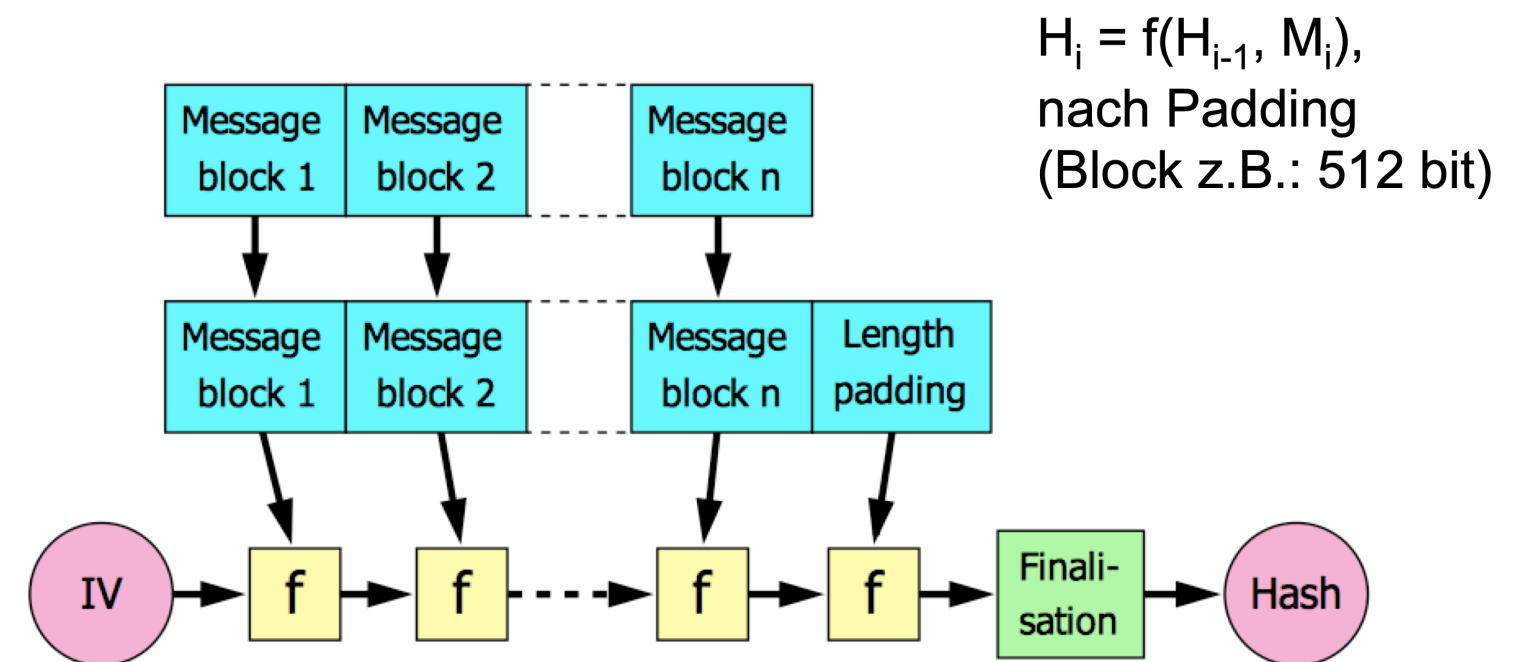
- SHA2 (z.B. SHA-256)
Merkle-Damgård
- SHA3, SHAKE
Sponge

Merkle-Damgård

Grundlage von ~~SHA-1~~, SHA-2
(SHA-256, SHA-512)

Problem: "Length extension attacks"

Wir bauen uns einen Hash: Merkle-Damgård



Sponge

Grundlage von SHA-3

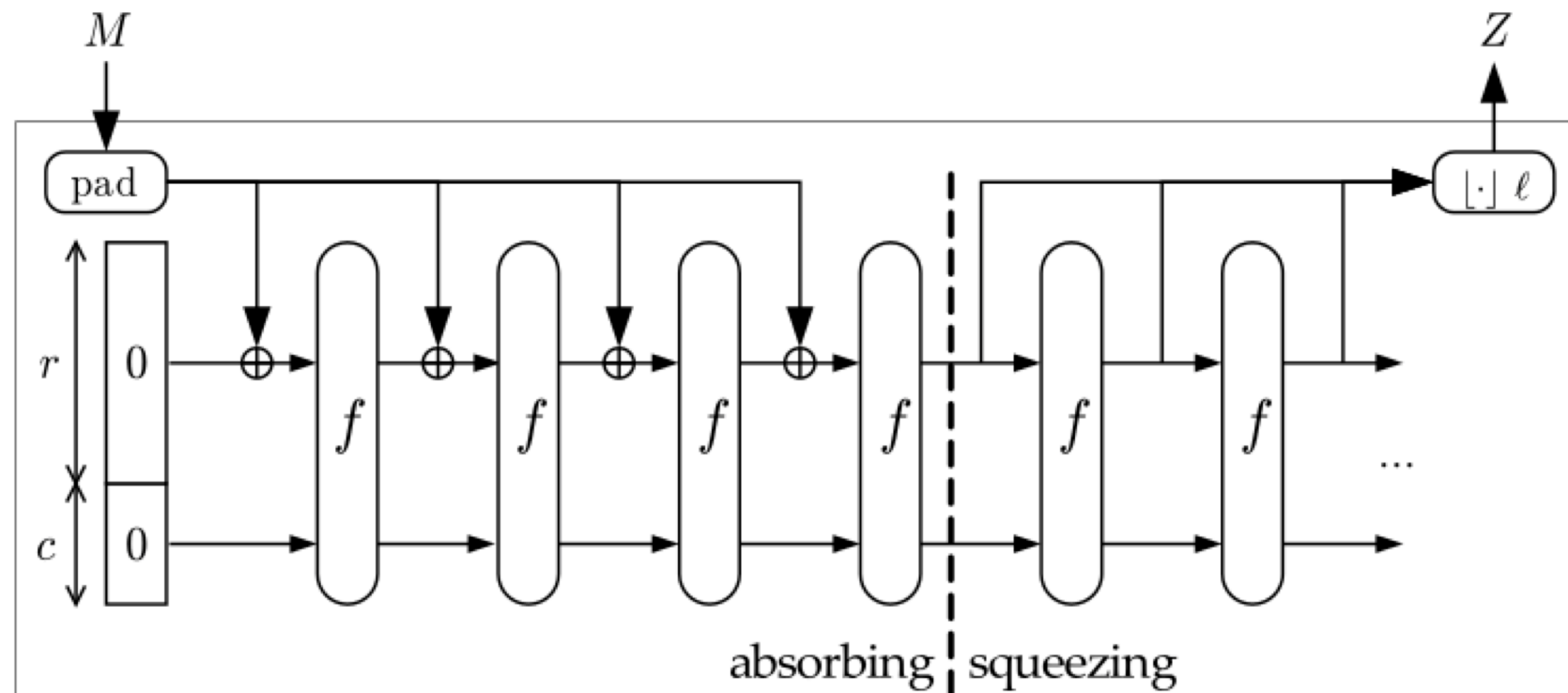
Phasen:

- Aufsaugen (absorb)
- Herauspressen (squeeze)

Einige Bits unsichtbar durchreichen (c)

TZi

Sponge mode:
 $b = r \text{ (bitrate)} + c \text{ (capacity)}$



Universität Bremen

X

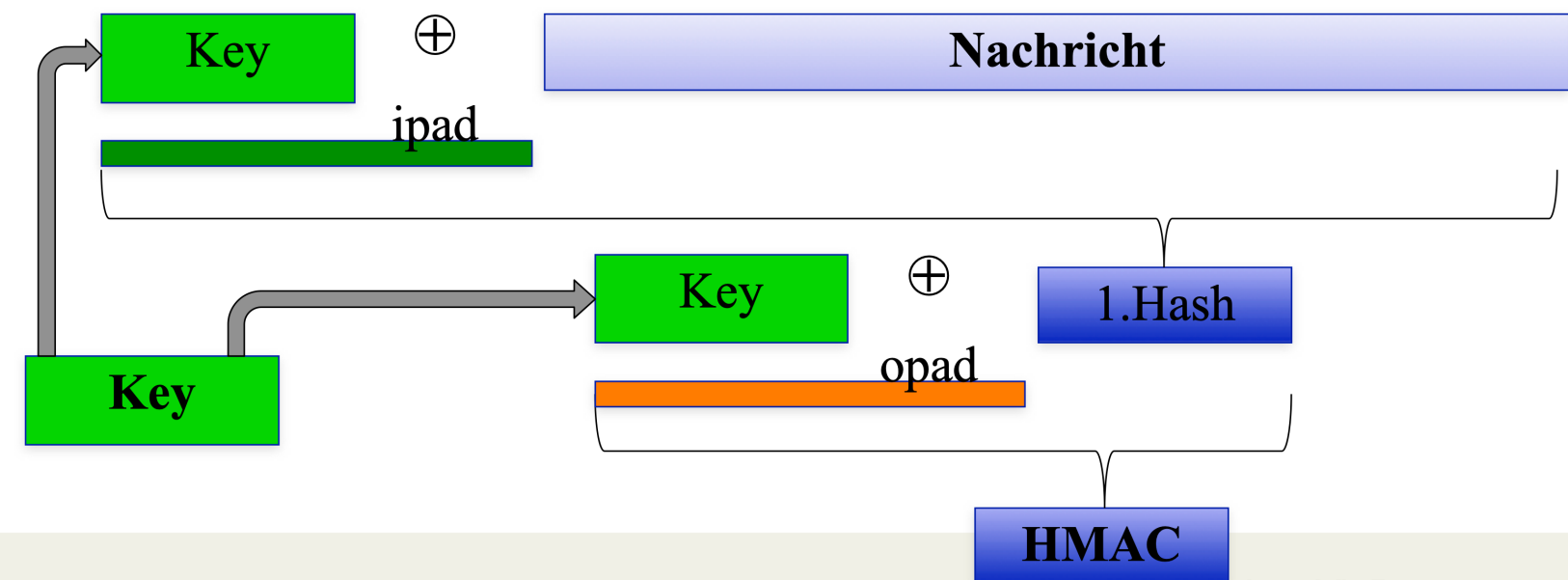
MACs

MAC: z.B.

- via Hash mit "Schlüssel"
 - **HMAC**
 - KMAC
- via Blockchiffre
 - z.B. mit CBC (CBC-Mac, CMAC)

Einsatz von Hash-Funktionen für MACs: **HMAC**

▶ $\text{HMAC}_K(M) = h(K \oplus \text{opad} \parallel h(K \oplus \text{ipad} \parallel M))$ (RFC 2104)



AEAD

Authenticated Encryption
with
Associated Data

Verschlüsselung
(Vertraulichkeit)
Authentisierung (Integrität)

→ Blockwoche



Authenticated Encryption with Associated Data (AEAD)

Authenticated Encryption

- ▶ Vertraulichkeit + Integrität + Authentizität
- ▶ effizient mit Block-Verschlüsselung realisierbar
→ benötigt Counter und CBC-MAC

Mechanismus: RFC 5116

- ▶ Verschlüsselung: $K \times N \times P \times A \rightarrow A \times C$
- ▶ Entschlüsselung: $K \times N \times A \times C \rightarrow A \times P$
- ▶ AEAD-Algorithmus legt Länge von K, K_LEN, fest

K	Key	A	Associated Data	P	Plaintext
N	Nonce	C	Ciphertext		



Universität Bremen

: Tutorium 3, CCM

1/1x

Levels of Security

Äquivalenz zu brute force mit
angegebener Anzahl von Bits:
 2^n — was brauchen wir?

Center for Computing Technologies

Levels of Security

Table 7.1: Minimum symmetric key-size in bits for various attackers.

Attacker	Budget	Hardware	Min security
"Hacker"	0	PC	53
	< \$400	PC(s)/FPGA	58
Small organization	0	"Malware"	62
	\$10k	PC(s)/FPGA	64
Medium organization	\$300k	FPGA/ASIC	68
Large organization	\$10M	FPGA/ASIC	78
Intelligence agency	\$300M	ASIC	84

[ECRYPT II 2011]

Universität Bremen

x

Levels of Security

Level (Bits)	Encryption	Hash	RSA, D-H	ECC
80	(3DES)	(SHA-1)	1024	160
112	(3DES)	SHA-224*), SHA-256*)	2048	224
128	AES-128	SHA-256*)	3072	256
192	AES-192	SHA-384*)	7680	384
256	AES-256	SHA-512	15360	521

*) oder SHA-512/nnn