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

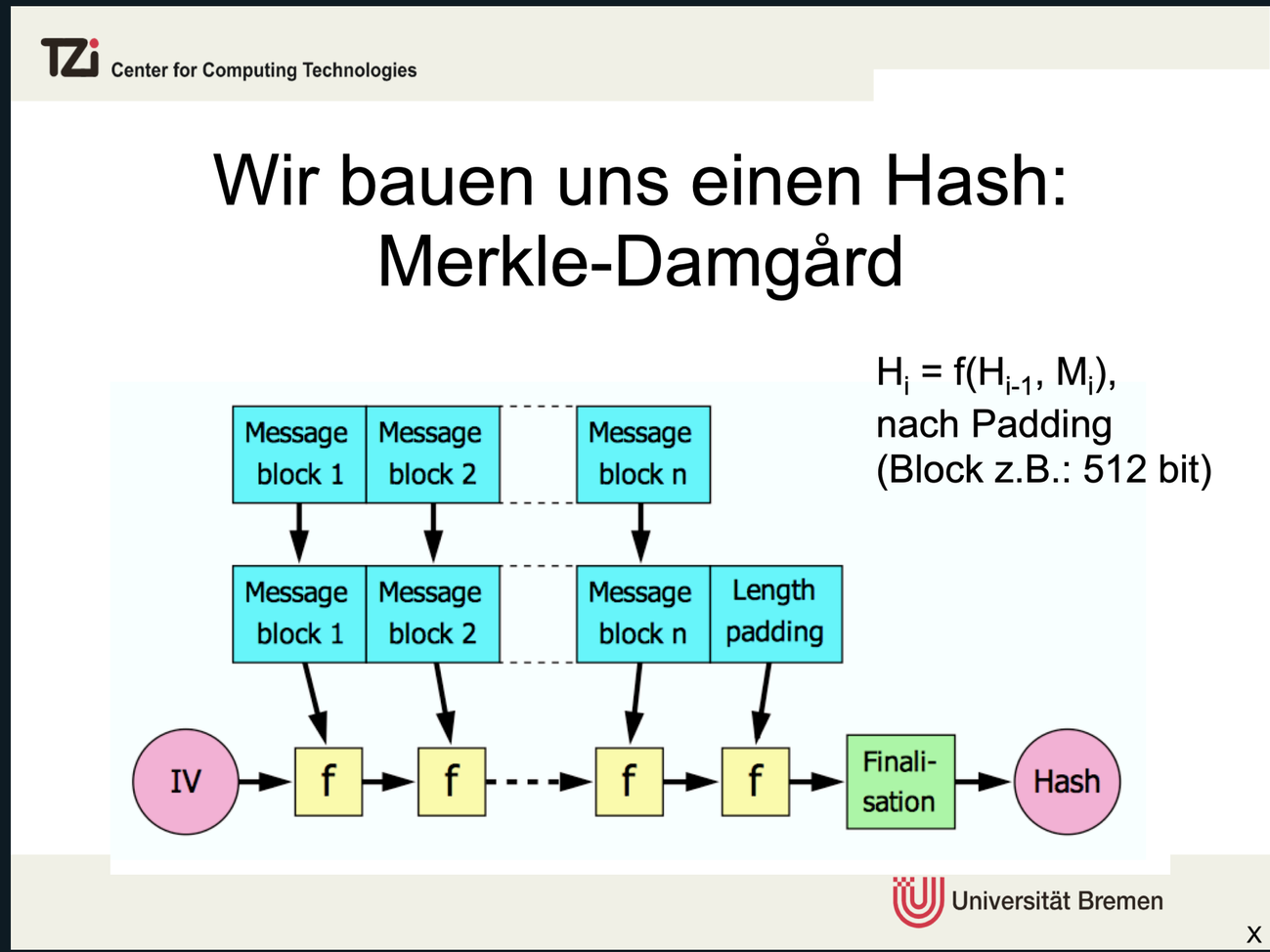
Aktuelle Auswahl

- 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"



Sponge

Grundlage von SHA-3

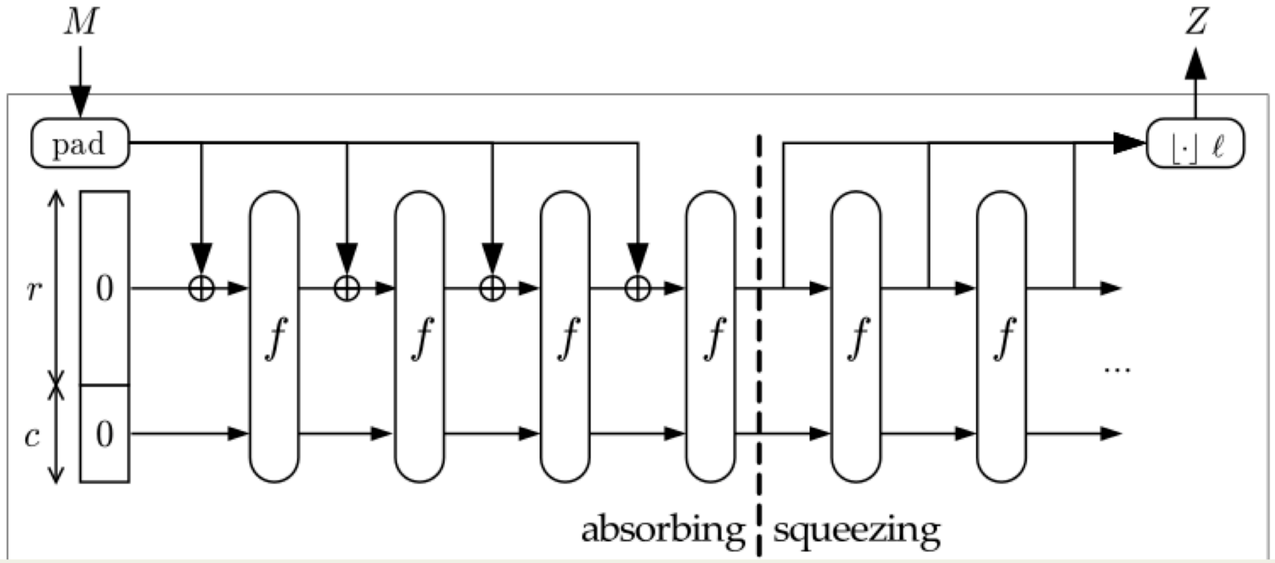
Phasen:

— Aufsaugen (absorb)
— Herauspressen (squeeze)

Einige Bits unsichtbar durchreichen (c)

TZi

Sponge mode:
b = r (bitrate) + c (capacity)



Universität Bremen

X

MACs

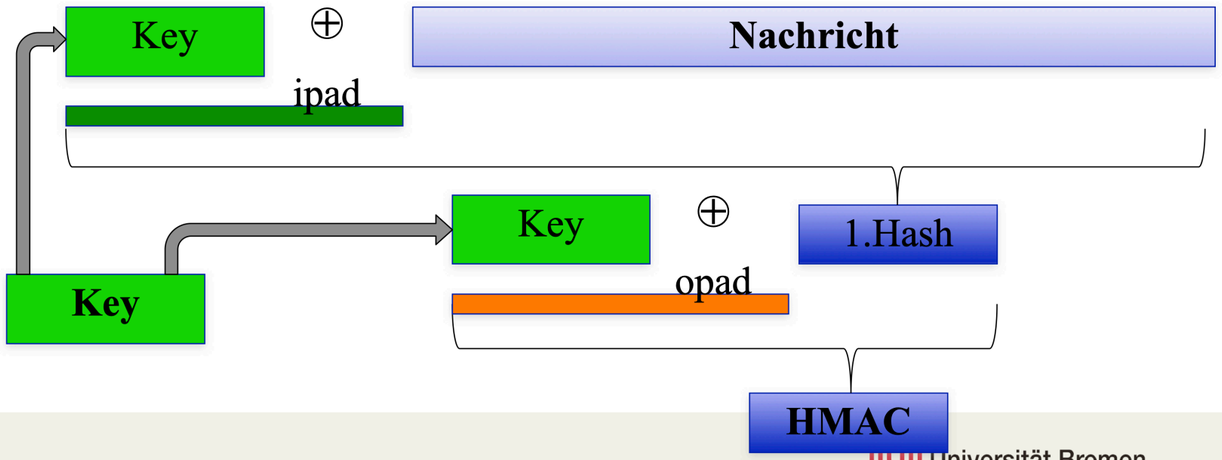
MAC: z.B.

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

TZi Center for Computing Technologies

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

- $HMAC_K(M) = h(K \oplus opad \,||\, h(K \oplus ipad \,||\, M))$ (RFC 2104)



Universität Bremen

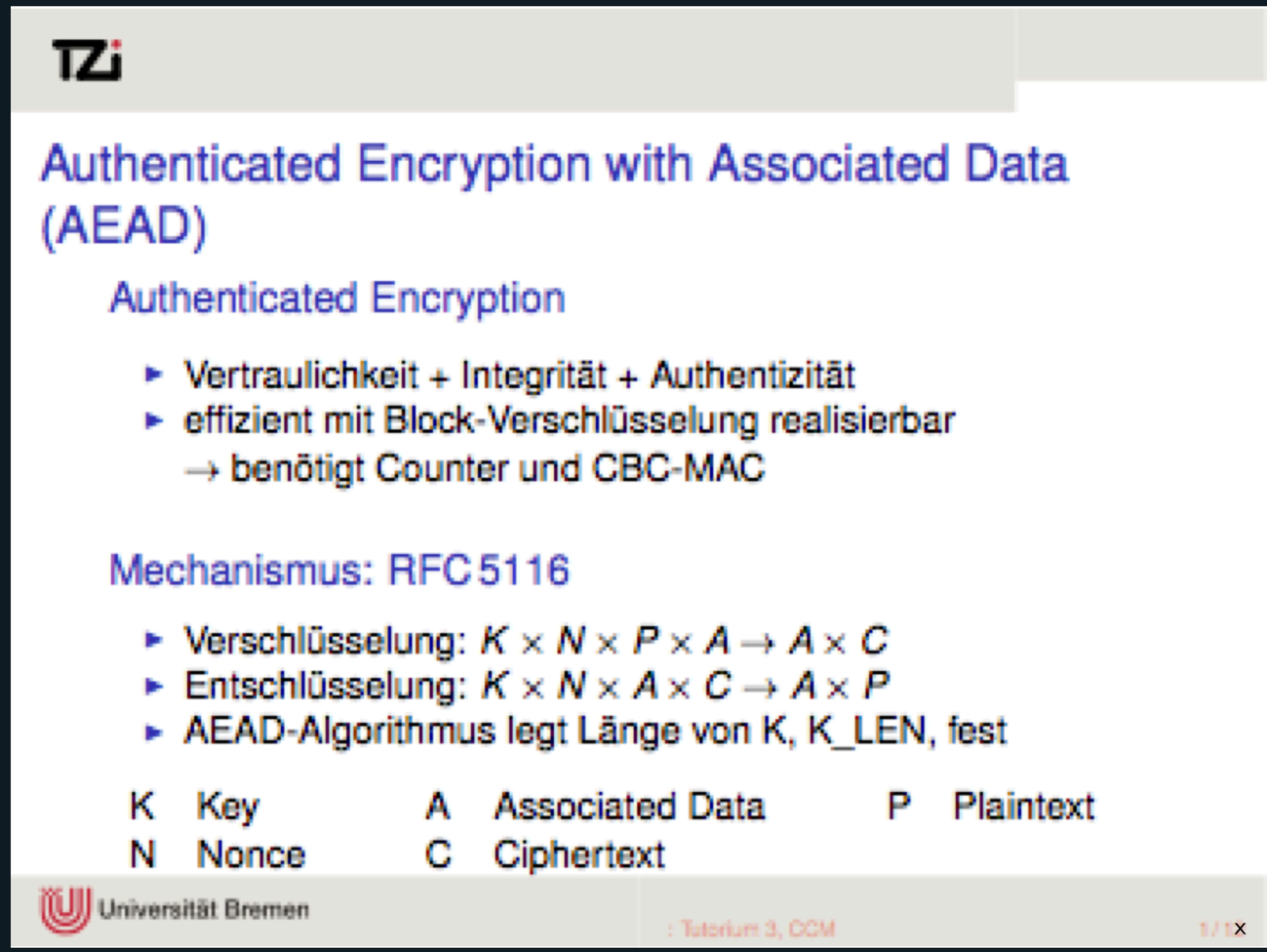
x

AEAD

Authenticated Encryption
with
Associated Data

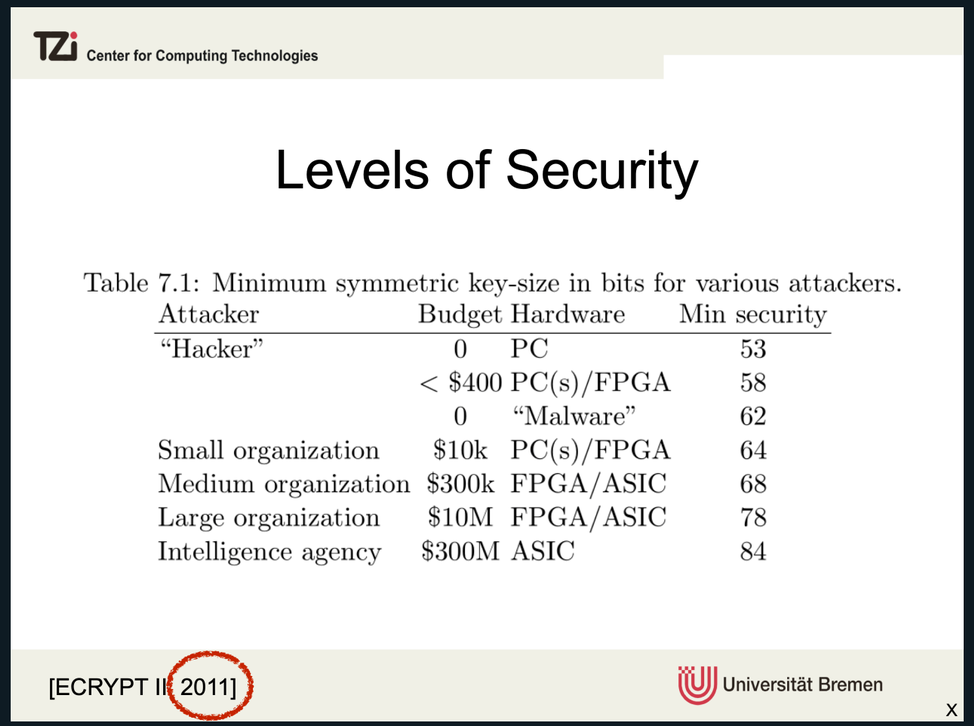
Verschluesselung
(Vertraulichkeit)
Authentisierung (Integrität)

➔ Blockwoche



Levels of Security

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



Center for Computing Technologies

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

Universität Bremen