Hashfunktionen und symmetrische Kryptographie

Prof. Dr.-Ing. Damian Weber

Hochschule für Technik und Wirtschaft des Saarlandes

Inhalt

- Symmetrische Kryptographie

  Stromchiffren, Blockchiffren, Modi

- Hashfunktionen

  was ist das

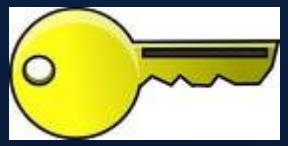
  wozu braucht man das

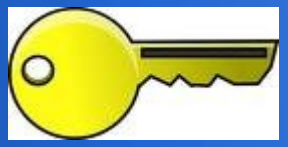
  wie macht man es kaputt ;-)

Symmetrische Kryptographie

Alice

Bob





Symmetrische Kryptographie

- Gleicher Schlüssel bei Sender und Empfänger

- Beispiel Cäsar
- Beispiel Substitutionschiffre

```
Key: abcdefghijklmnopqrstuvwxyzäöü
     wvilkbqrödazngmtfxüsyeäujhpco
Vözlygqütmzösöa

ög lkx äöüükgüqkükzzüirwbs qkrcxs Vözlygq hy lkg äöirsöqüskg Xküümyxikg örxkx
Voxqkx. Lwü nwirs Vözlygqütmzösöa hy kögkn Srknw emg rmrkx Vklkysygq.
```

großer Schlüsselraum, aber kein brute-force-Angriff nötig

Symmetrische Kryptographie

One-Time-Pad

Stromchiffren

Blockchiffren

XOR: Exklusiv-Oder, Entweder-Oder

bitweise Addition (XOR, exklusiv–oder, $\bigoplus$)

x_1	x_2	$x_1 \oplus x_2$
0	0	0
0	1	1
1	0	1
1	1	0

Stromchiffre	s
Klartext	m
Chiffretext	$c = m \oplus s$
Klartext	$m \oplus s \oplus s = m$

aber auch

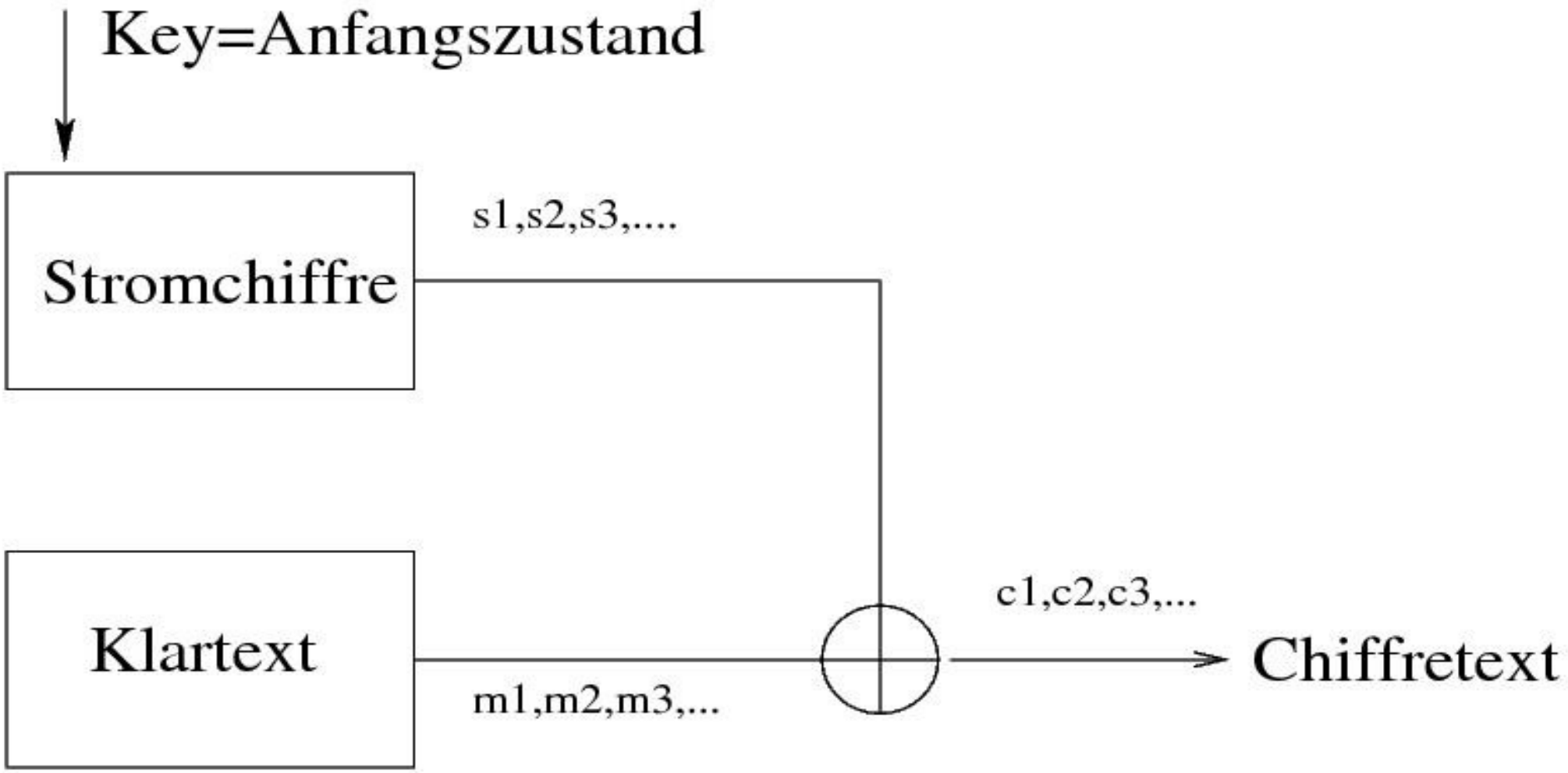
$$c \oplus m = s$$

One Time Pad

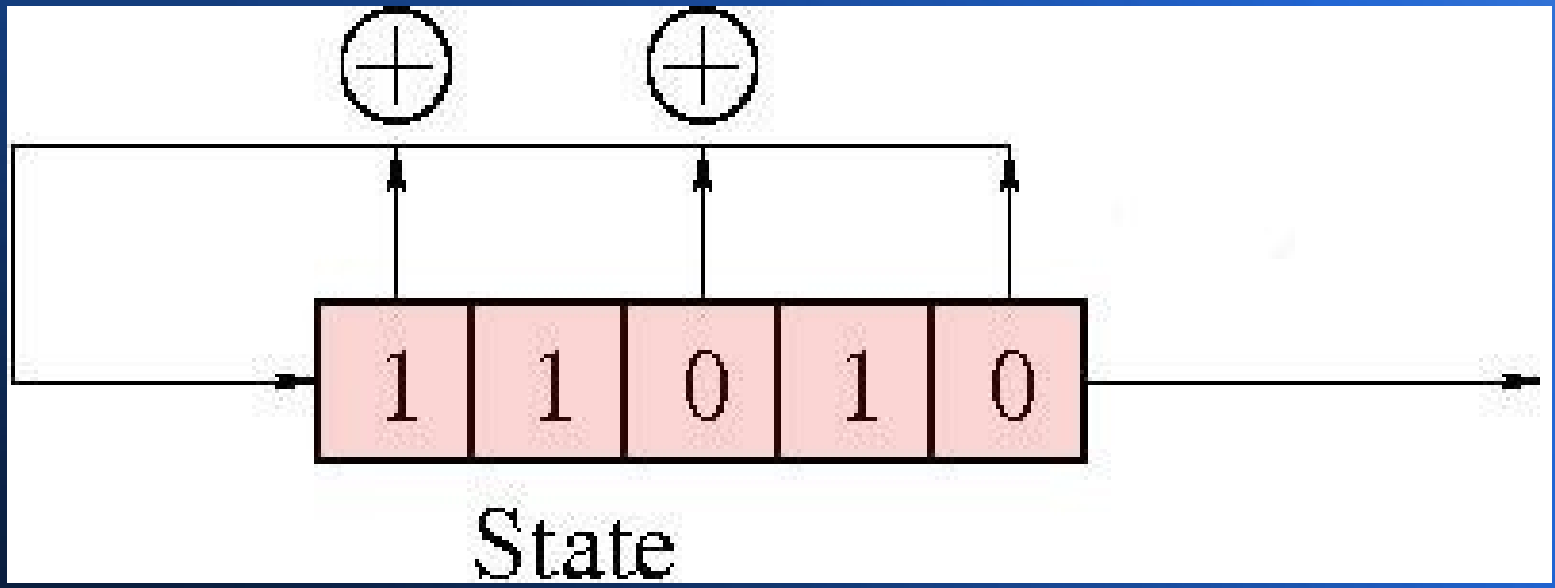
Shannon:
wenn R eine *zufällige* Folge von Bits ist,
dann ist P+R eine sichere Verschlüsselung von P

Sicherheit gegen Angreifer
mit unbegrenzter Rechenleistung

Stromchiffren



Zufallsfolgen in Hardware



LFSR: linear feedback shift register

LFSR: linear, algebraisch analysierbar

$L = 5$, Periode $2^5 - 1$

$$s_j = b_1 s_{j-1} \oplus b_2 s_{j-2} \oplus \cdots \oplus b_L s_{j-L}, j \geq L$$

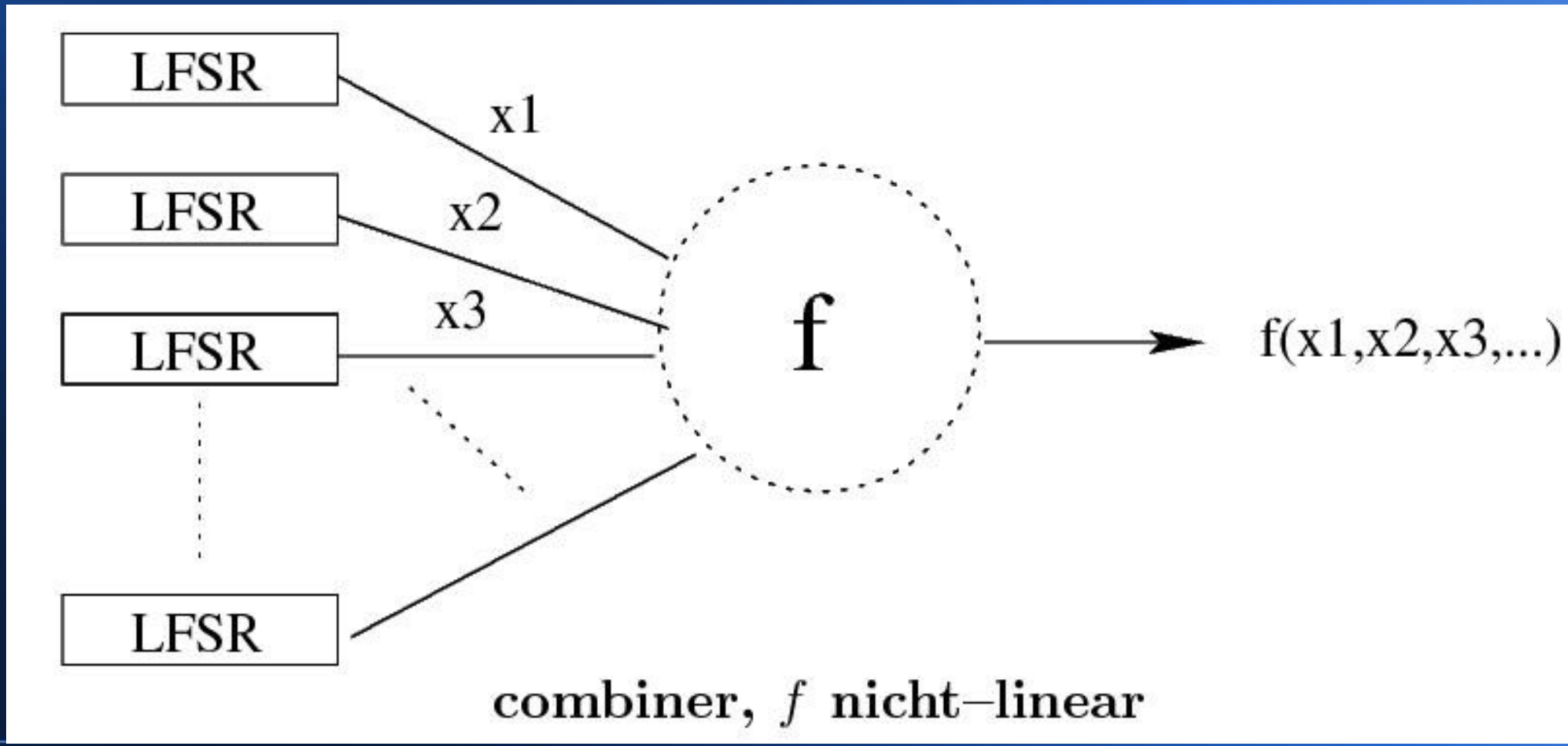
b_i's	0 1 0 0 1	*Feedback*
key	1 1 1 1 1	*Startzustand*

erzeugte Folge

1 1 1 1 1 0 0 1 1 0 1 0 0 1 0 0 0 0 1 0 1 0 1 1 1 0 1 1 0 0 0

16 Einsen, 15 Nullen

Kombinierte LFSRs: Linearität zerstört



Stromchiffren in der Anwendung

RC4: SSL, 1K Initialdatenstrom wegwerfen, trotzdem vom Einsatz abzuraten

E0: Bluetooth, gebrochen in 2^{38} Operationen

A5/1: GSM 2^{39} Operationen

Salsa20: relativ neu (2005)

Stromchiffren, Fazit

- Performance sehr gut
- relativ wenig zivile Forschung
- relativ viel geheime Forschung
- schwierig, spezielles Verfahren zu empfehlen

Blockchiffren

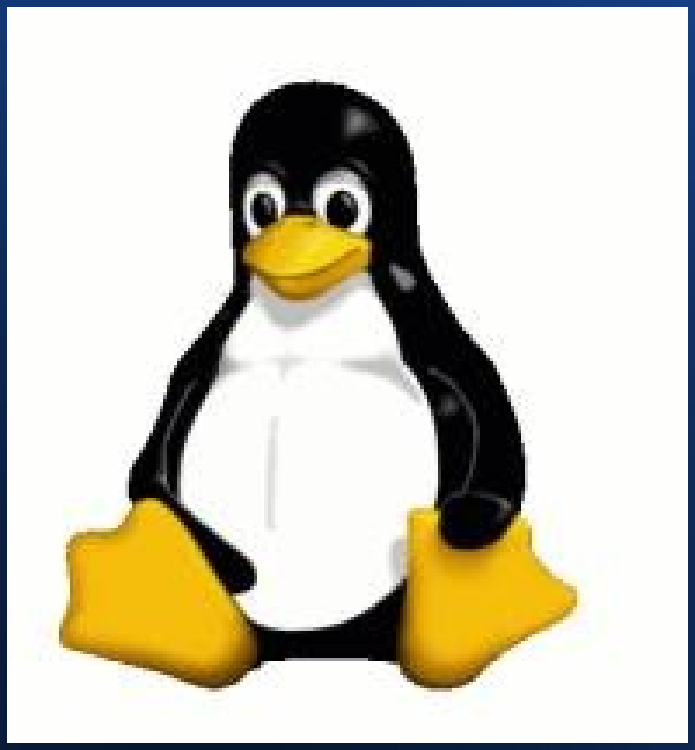
Blocklänge 128 Bit

simple Idee: Block für Block verschlüsseln

ECB = Electronic Codebook Mode

(falls ohne weitere Vereinbarung, schlechte Wahl)

Blockchiffren



ECB-Modus

Blockchiffren Modi

ECB, CBC, CFB, OFB, CTR

CBC: $C_i = E_k(P_i \oplus C_{i-1})$, $C_0 = IV$

CFB: $C_i = E_k(C_{i-1}) \oplus P_i$, $C_0 = IV$

OFB: (stream cipher)

$$C_i = P_i \oplus O_i$$

$$O_i = E_k(O_{i-1}), \quad O_0 = IV$$

CTR: $C_i = P_i \oplus E_k(\text{nonce} \,||\, i)$

Key size: 128 / 256

Symmetrische Kryptographie

- Standard DES bis 2002: 56 Bit

  72057594037927936 mögliche Schlüssel

- AES-Wettbewerb beendet am 26.11.2001:
  DES-Nachfolger ist Rijndael

- Attacken: Differentielle+Lineare Kryptoanalyse
  (bei AES-Design vermieden)

Aufbau

Iteration von

Konfusion (S-Box, bijektive Abb.)

Diffusion (Permutation von Bitpositionen)

= Runden … (Attacken auf reduzierte Rundenzahl)

Empfehlenswerte Verfahren

Alle AES Finalteilnehmer:

- AES (Rijndael)
- Twofish
- Serpent
- Mars
- RC6

Andere: 3DES, Blowfish, IDEA, Camellia, CAST5