# Symmetrische Kryptoverfahren

Prof. Dr.-Ing. Damian Weber

Hochschule für Technik und Wirtschaft des Saarlandes

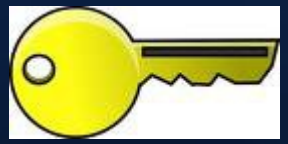
# Inhalt

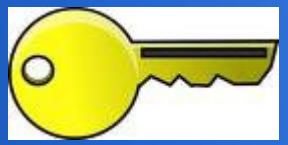
- Grundbegriffe
- Stromchiffren
- Blockchiffren
- Modi
- AES-Finalisten
- Cryptanalysis

# 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

# Basisoperationen

XOR

Shift, Rotate

AND, OR, ADD, MUL

# Basisoperation 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 (1949):

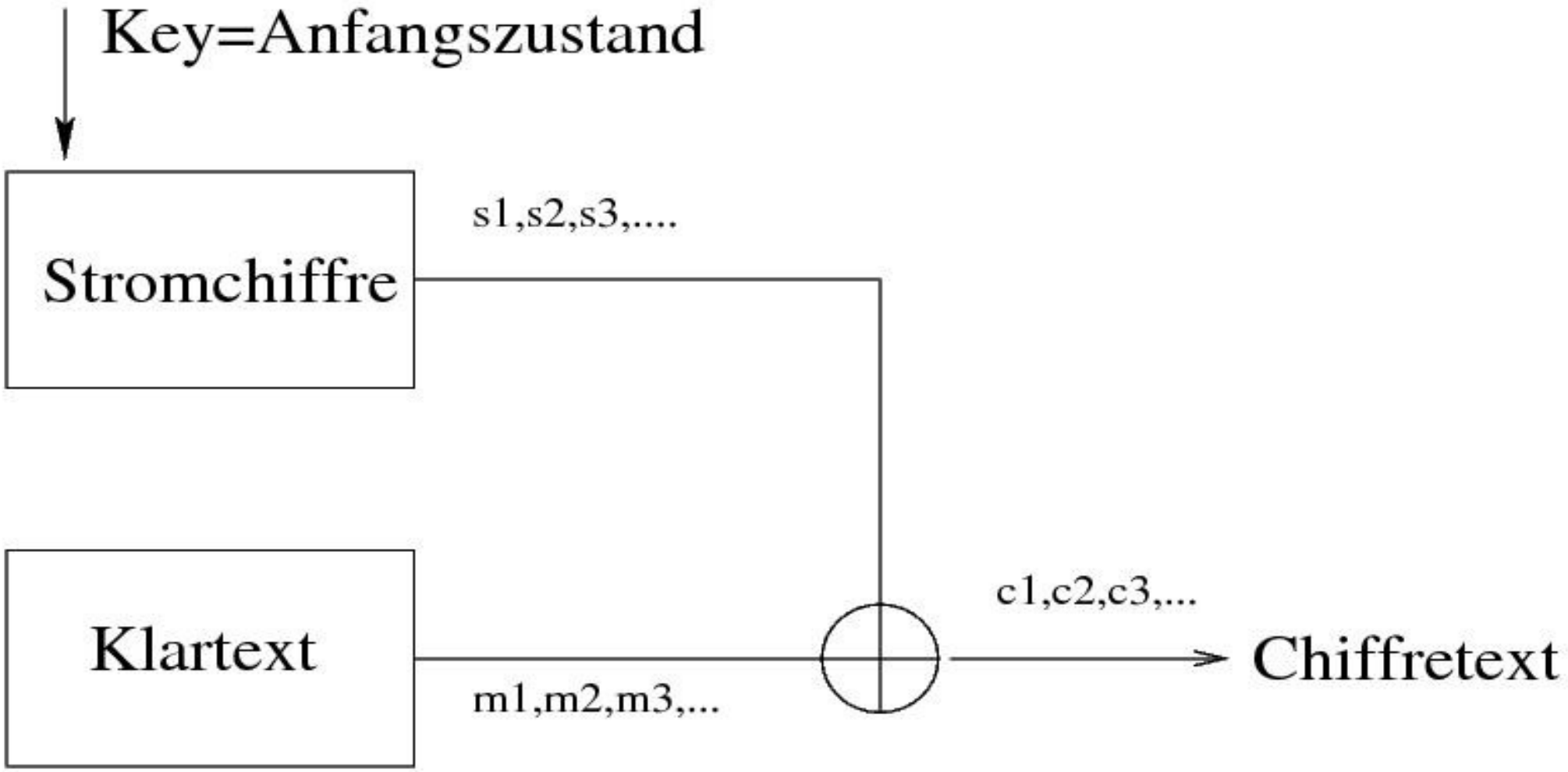
wenn R eine *zufällige* Folge von Bits ist, dann ist

$P \oplus R$

eine sichere Verschlüsselung von P

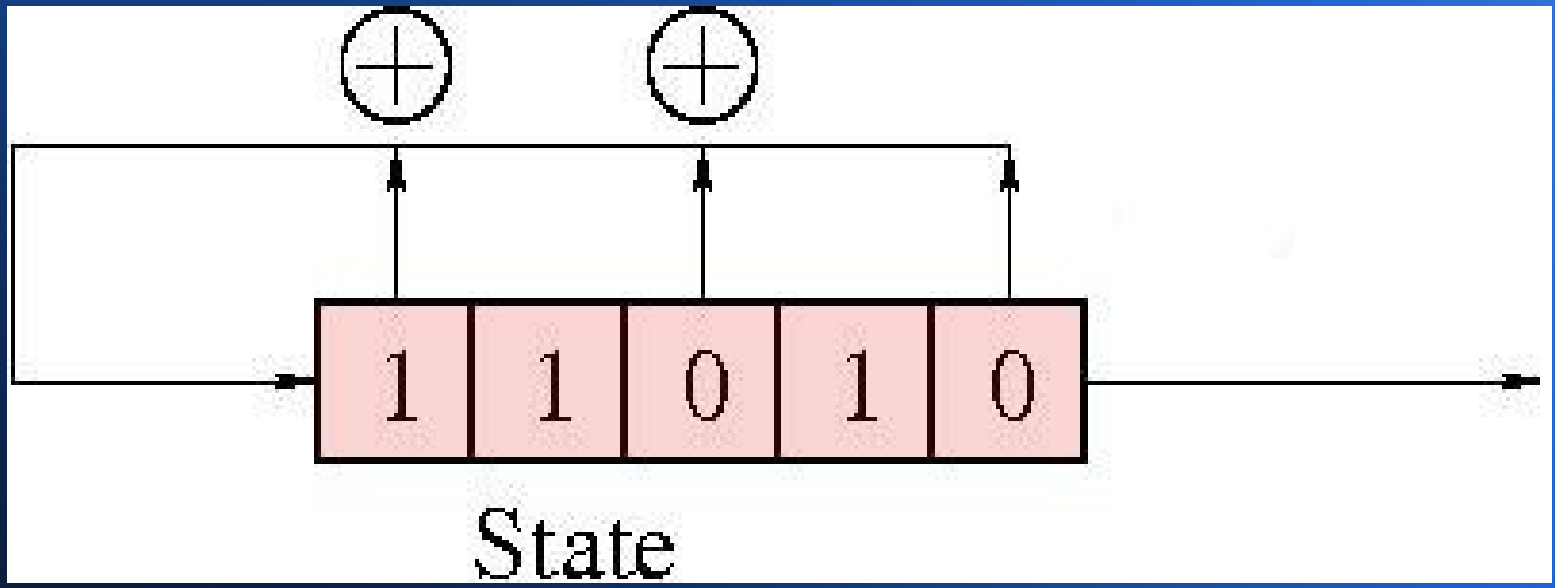
**absolute Sicherheit:**
gegen Angreifer mit unbegrenzter Rechenleistung

# Stromchiffren




Geheimnis: Anfangszustand des Stromchiffre

# Zufallsfolgen in Hardware




LFSR: linear feedback shift register

Zustand = Werte aller Bits im internen 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

beobachte 5 Bits → kann $s_0, s_1, s_2, s_3, s_4$ ermitteln → ganze Folge

# LFSR: linear, algebraisch analysierbar

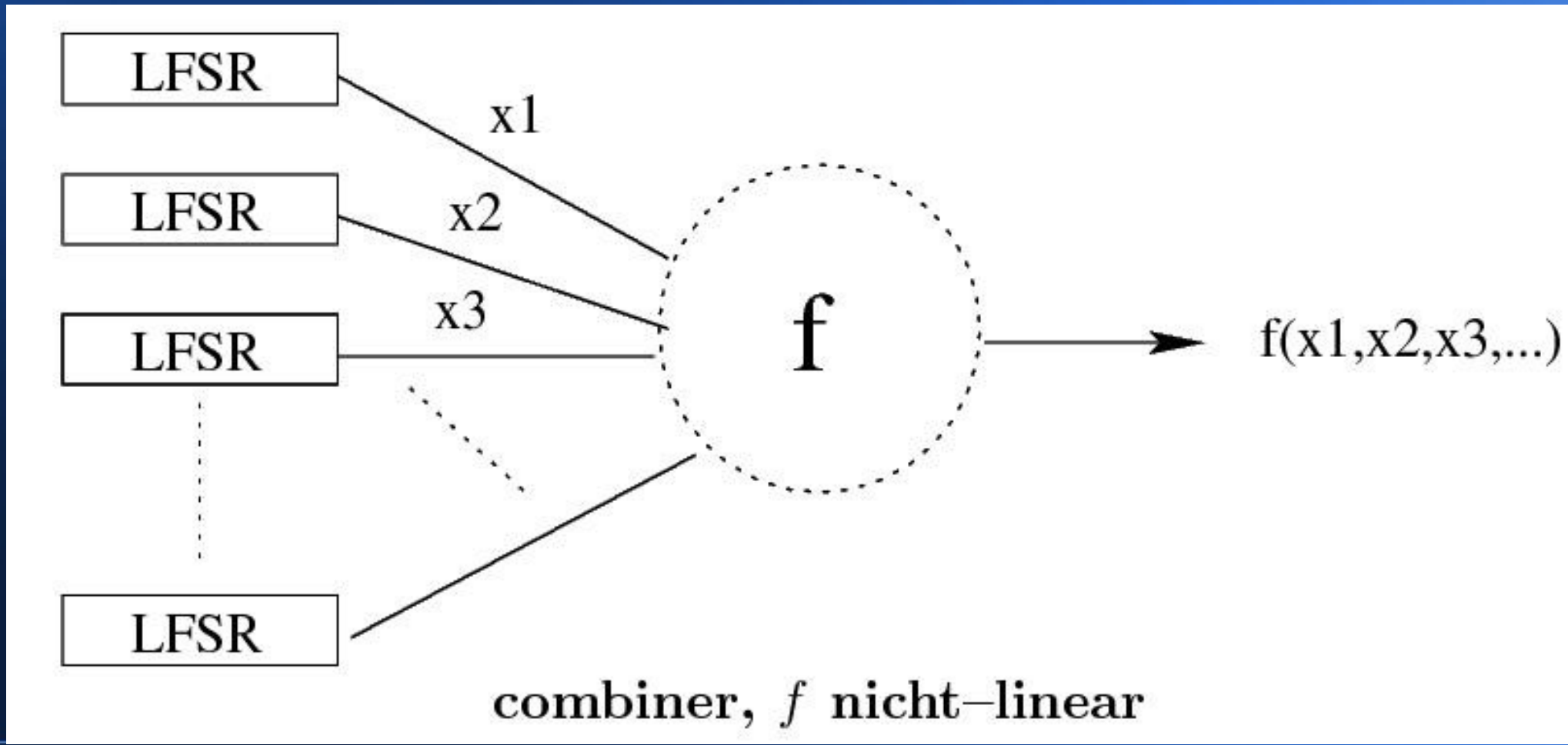
lineares Gleichungssystem lösen

Gauß-Algorithmus mod 2

→ Anfangszustand bestimmen
= geheimer Schlüssel

# LFSRs in sicherem Design: Linearität zerstören

z.B. 4 LFSRs beim $E_0$ Chiffre: 25, 31, 33, 39 bits




divide-and-conquer Attacken: LFSRs separierbar

# Stromchiffren in der Anwendung

- RC4: gebrochen (2013)
- E0: Bluetooth, gebrochen in $2^{38}$ Operationen
- A5/1: in Echtzeit mit 2 TB Lookup-Table gebrochen

Lichtblick: europäischer eSTREAM-Wettbewerb

Software: `Salsa20,HC-128,Rabbit,SOSEMANUK`
Hardware: `Grain, MICKEY, Trivium`

# eSTREAM

| Cipher | Authors | Key / IV | H/S |
|---|---|---|---|
| HC-128 | Hongjun Wu | 128 Bit / 128 Bit | S |
| Rabbit | Martin Boesgaard, Mette Vesterager, Thomas Pedersen,Jesper Christiansen, Ove Scavenius | 128 Bit / 64 Bit | S |
| Salsa20/12 | Dan J. Bernstein | 256 Bit / 64 Bit | S |
| Sosemanuk | Come Berbain, Olivier Billet, Anne Canteaut, Nicolas Courtois, Henri Gilbert, Louis Goubin, Aline Gouget, Louis Granboulan, Cédric Lauradoux, Marine Minier, Thomas Pornin, Hervé Sibert | 128 Bit / 128 Bit | S |
| Grain | Martin Hell, Thomas Johansson, Willi Meier | 80 Bit / 64 Bit | H |
| MICKEY | Steve Babbage, Matthew Dodd | 80 Bit / 80 Bit | H |
| Trivium | Christophe De Cannière, Bart Preneel | 80 Bit / 80 Bit | H |

# Stromchiffren, Fazit

- Performance sehr gut
- relativ viel geheime Forschung
- Empfehlungen eSTREAM-Projekt beachten

`https://en.wikipedia.org/wiki/ESTREAM`

# Blockchiffren

simple Idee: Block für Block verschlüsseln

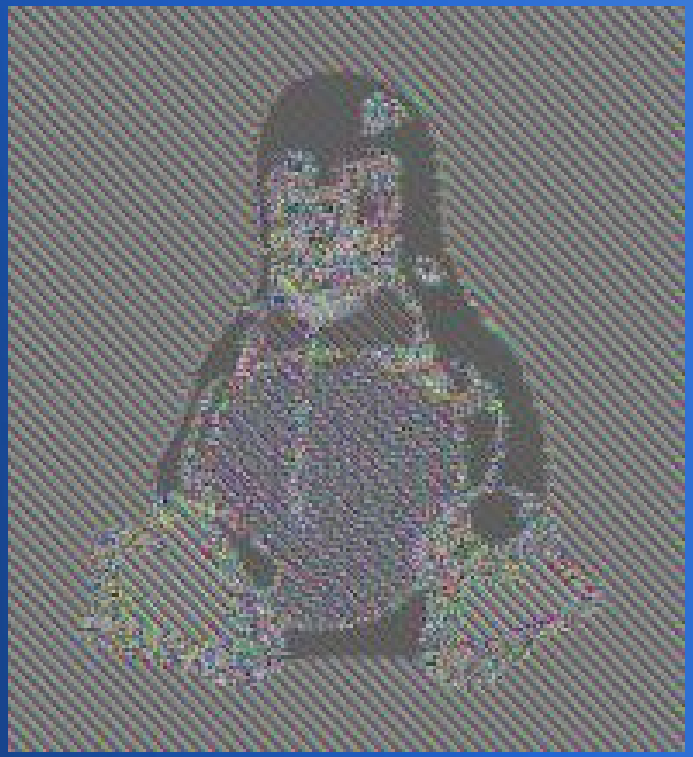
Wenn *x* ein *b*-Bit-Block ist, dann ist
$y = E_K(x)$ der verschlüsselte *b*-Bit-Block

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)

$$C_i = P_i \oplus O_i$$

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

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

Key size: 128, 256

# Standards

- Standard war DES bis 2002: 56 Bit Schlüssel

  72057594037927936 mögliche Schlüssel

- AES-Wettbewerb-Gewinner 26.11.2001: Rijndael, folgende Kriterien
  - Security
  - Cost
  - Implementation Characteristics

# AES: security

- better compared to other submitted algorithms
- indistinguishable from random
- mathematical model
- attacks during evaluation process

# AES: cost

- licensing
- computation time
- memory requirements

# AES: Implementation Characteristics

- Flexibility
  - key / block sizes
  - portability
  - usage as stream cipher / MAC / PRNG / Hash
- Hardware / Software
- Simplicity

# Symmetrische Kryptographie:
## Parameter

- Schlüssellänge (≥ 128 Bit)
- Blocklänge (≥ 128 Bit)
- Runden (≥ 10)

# AES-Finalisten

| Cipher | Authors | Rounds | Cryptanalysis |
|---|---|---|---|
| Rijndael (AES) | Vincent Rijmen, John Daemen | 10, 12, 14 | $2^{126}$ Time |
| Twofish | Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, Niels Ferguson | 16 | 6 Rounds, $2^{256}$ Time |
| Serpent | Ross Anderson, Eli Biham, Lars Knudsen | 32 | 11 Rounds, $2^{116}$ PT, $2^{107}$ Time |
| MARS | Carolynn Burwick, Don Coppersmith, Edward D'Avignon, Rosario Gennaro, Shai Halevi, Charanjit Jutla, Stephen M. Matyas, Luke O'Connor, Mohammad Peyravian, David Safford, Nevenko Zunic | 32 | 21 Rounds |
| RC6 | Rivest, Matt Robshaw, Ray Sidney, Yiqun Lisa Yin | 20 | 15 Rounds |
| | | | |
| | | | |

andere Empfehlungen : IDEA, Blowfish, Camellia, CAST