

# Advanced Encryption Standard

Designaspekte von *Rijndael*

Detlef Kraus

Michael Welschenbach

SRC Security Research & Consulting

Bonn

2001

# Advanced Encryption Standard

- **1997**  
NIST startet AES-Wettbewerb
  - **1998**  
Fünfzehn Kandidaten treten an
  - **1999**  
Fünf Kandidaten bleiben
  - **2000**  
Rijndael wird als AES nominiert
- **MARS**  
(IBM)
  - **RC6**  
(RSA)
  - **Rijndael**  
(Daemen, Rijmen)
  - **Serpent**  
(Anderson, Biham, Knudson)
  - **Twofish**  
(Schneier et. al.)

# AES Designkriterien

- Sicherheit
- Sicherheit
- Sicherheit
- Geschwindigkeit
- Implementierbarkeit (Soft-/Hardware)
- Ressourcenbedarf

# Sicherheit

- Alle (1999er) Kandidaten erfüllen die Anforderungen an die Sicherheit vor allen bekannten Angriffen
- Rijndael, Serpent und Twofish können mit geringen Einbußen an Performanz gegen DPA- und Timing-Attacken gehärtet werden
- Schutzmaßnahmen beeinträchtigen Rijndael am wenigsten

# Geschwindigkeit und Speicherbedarf

	8051				ARM			
	Code-size (Bytes)	RAM (Bytes)	Key Schedule (Cycles)	Encryption (Cycles)	Code-size (Bytes)	RAM (Bytes)	Key Schedule (Cycles)	Encryption (Cycles)
RC6	596	205	43K	14K	460	176	2K	1K
Rijndael	512	49	4K		1148 2620	0 16	3K 1K*	
Twofish	879	68	18K		696	48	8K**	

DES:  $\approx$ 59K Cycles pro Block

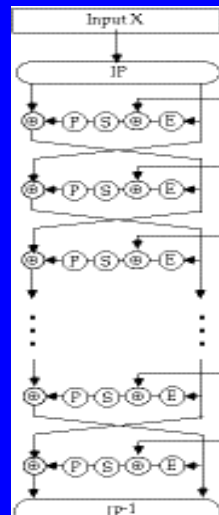
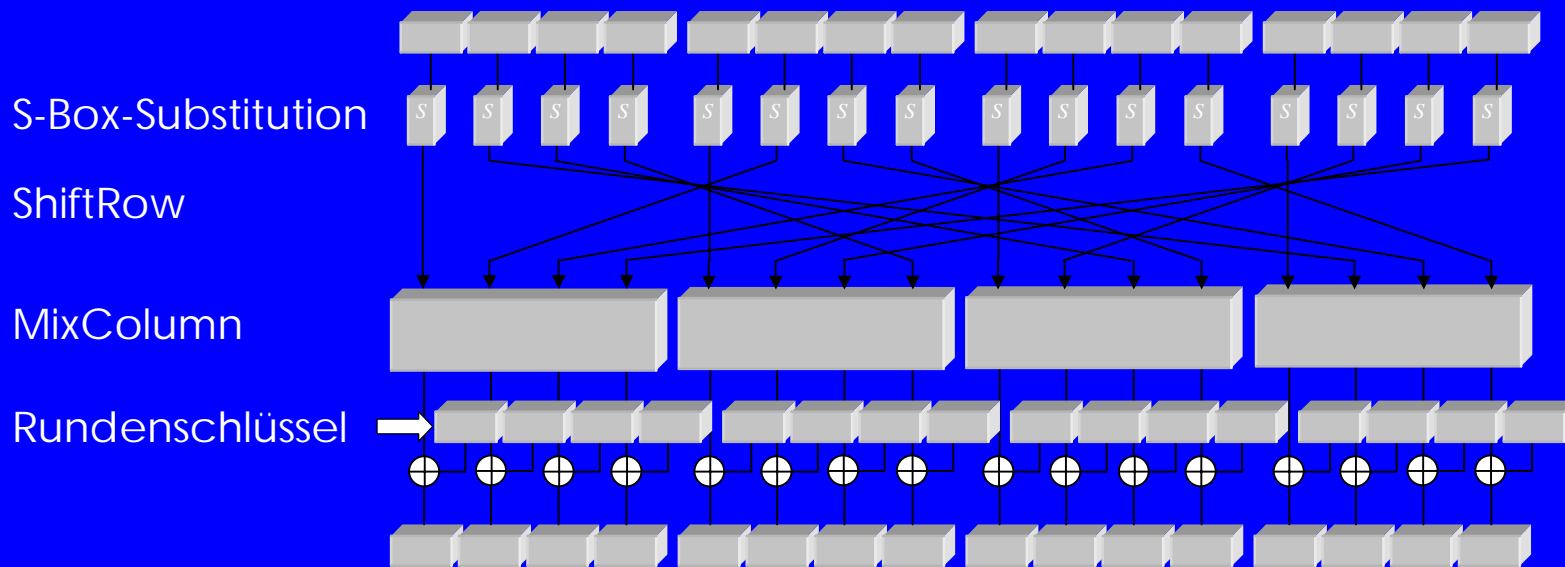
\* 1K Tabellen

\*\* 4K Tabellen

# Performanz

	8051 @ 3,57MHz	ARM @ 28,56MHz
RC6	165 Byte/sec	151.260 Byte/sec
Rijndael	3.005 Byte/sec	311.492 Byte/sec
Twofish	525 Byte/sec	56.289 Byte/sec

# Die Struktur von Rijndael



Welschenbach: Cryptography in C and C++, Apress, 2001

# Die Struktur von Rijndael

1. Addition des ersten Rundenschlüssels zum Klartext
2. Reguläre Runden (variable Anzahl)
3. Letzte verkürzte Runde (ohne MixColumn)

⇒ Jede Operation ist vom Schlüssel abhängig

# Variable Schlüssellängen und Rundenzahlen

<i><b>Anzahl Runden</b></i>	<i>Blocklänge in Bit</i>		
<i>Schlüssellänge in Bit</i>	128	(192)	(256)
128	<b>10</b>	<b>12</b>	<b>14</b>
192	<b>12</b>	<b>12</b>	<b>14</b>
256	<b>14</b>	<b>14</b>	<b>14</b>

# Substitutions-Box

## Designziele:

Minimierung der Anfälligkeit für

- Algebraische Angriffe
- Lineare und differentielle Kryptoanalyse

Operation hoher Komplexität in  $GF(2^8)$

Invertierbarkeit

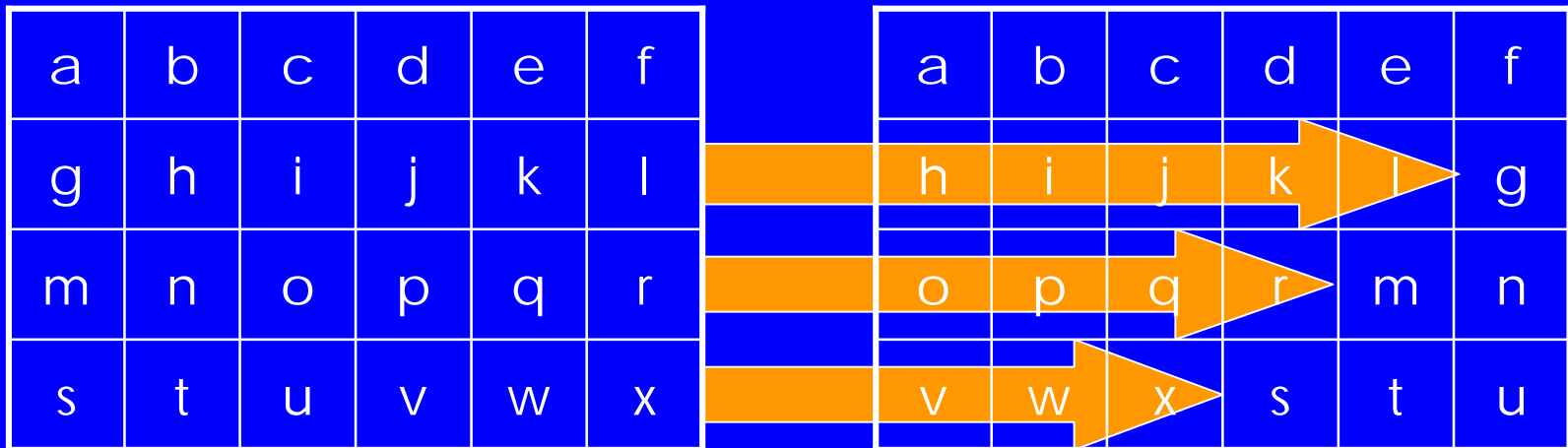
Einfachheit der Implementierung

# Substitutions-Box

1. Jedes Byte  $\neq 0$  wird in  $GF(2^8)$  invertiert
2. Invertierbare affine Transformation über  $GF(2)$ :

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

# Permutation: ShiftRow



- Sorgt für wechselnde Byte-Interaktionen in MixColumn
- Invertierbar
- Schnell

# Diffusion: MixColumn

a	b	c	d	e	f
g	h	i	j	k	l
m	n	o	p	q	r
s	t	u	v	w	x

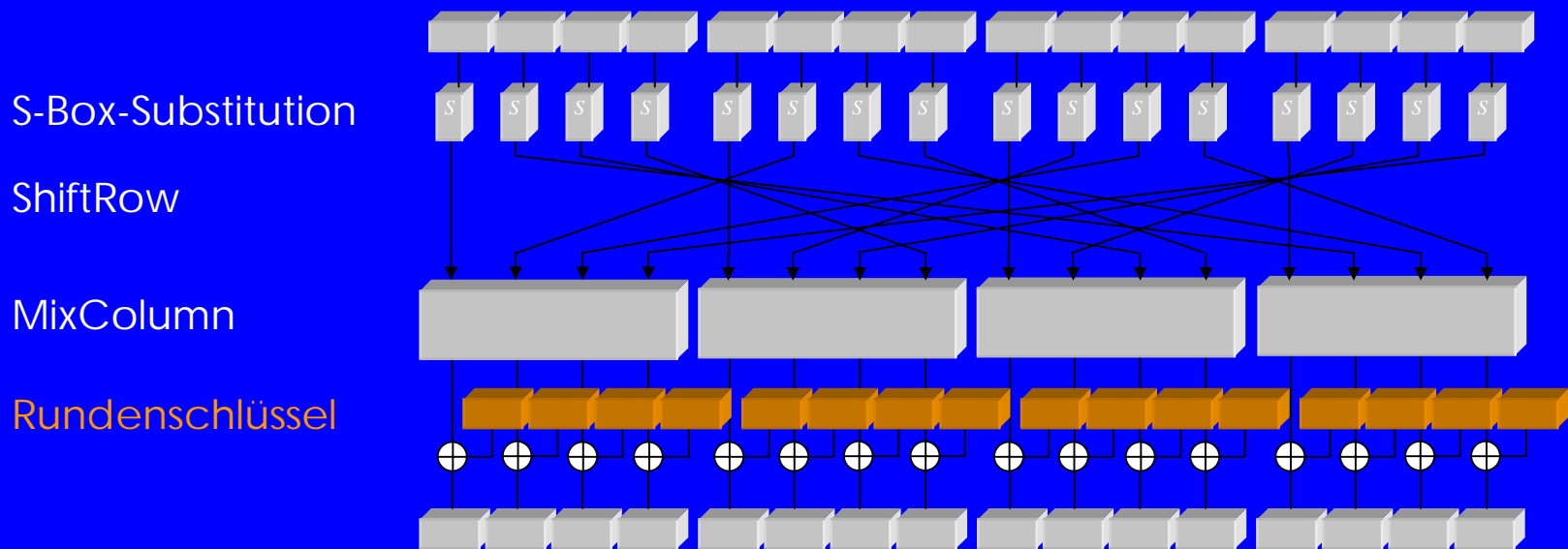
Operationen in  $GF(2^8)[X]$

Designkriterien:

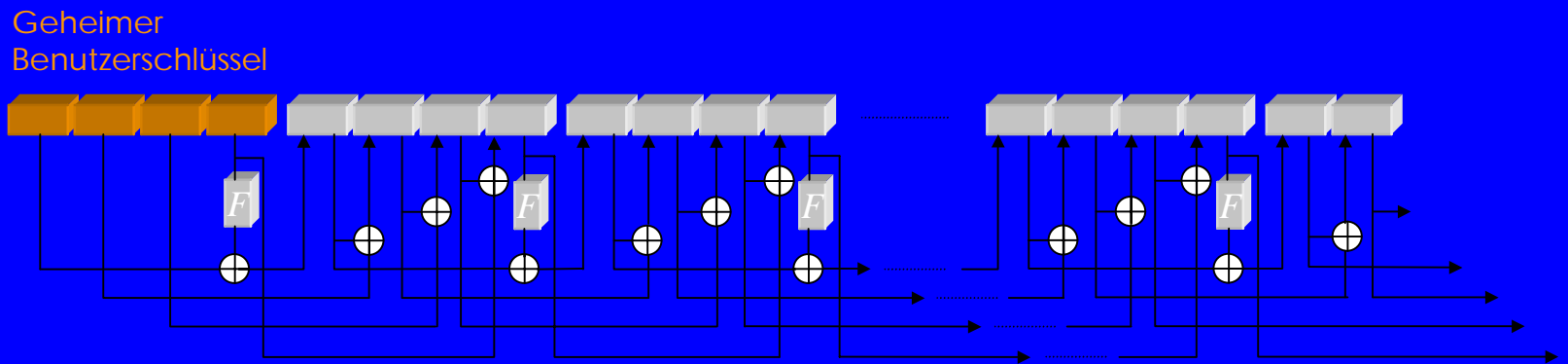
- Starke Diffusionswirkung
- Invertierbarkeit
- Performanz

$$\begin{bmatrix} a \\ g \\ m \\ s \end{bmatrix} \leftarrow \begin{bmatrix} '02' & '03' & '01' & '01' \\ '01' & '02' & '03' & '01' \\ '01' & '01' & '02' & '03' \\ '03' & '01' & '01' & '02' \end{bmatrix} \begin{bmatrix} a \\ g \\ m \\ s \end{bmatrix}$$

# Addition des Rundenschlüssels



# Erzeugung der Rundenschlüssel



Welschenbach: Cryptography in C and C++, Apress, 2001

$F$  Funktion  $F$ : S-Box(Links-Rotation(Wort)  $\oplus$  Konstante)

- Nichtlinear, nicht invertierbar
- Starke Diffusionswirkung auf Benutzerschlüssel
- Schnell
- Es gibt keine schwachen Schlüssel

# Power Analysis

- Schutzmaßnahmen für alle AES-Kandidaten erforderlich
  - Software
    - Balancierung des Stromverbrauchs durch komplementäre Argumente
    - Verschleierung durch Dummy Code
    - Eliminierung von Programmverzweigungen
    - Teilung von Zwischenresultaten (Chari et al.)
    - Duplication Method (Goubin et al.)
    - Maskierung von Daten (Messerges)
  - Hardware
    - Stabilisierung des Stromverbrauchs
    - Verschleierung durch Rauschen

## DPA-empfindliche Operationen

	MARS	RC6	Rijndael	Serpent	Twofish
Table Lookup	two 8 to 32, or one 9 to 32	none	one 8 to 8	none, or eight 4 to 4	eight 4 to 4, or two 8 to 8
Boolean	XOR	XOR	XOR	XOR, AND, OR	XOR
Shift	variable	variable	fixed		fixed
Mult. ( $2^{32}$ )	X	X			
Add. ( $2^{32}$ )	X	X			X
Mult. in $GF(2^8)$			X		X
Permutation				X	
Linear Transformation	X			X	

And The Winner Is...

**RIJNDAEL**

*„... a fast, flexible and elegant cipher“*

IBM MARS TEAM, Mai 2000