Der Advanced Encryption Standard (AES)

Prof. Dr. Rüdiger Weis

TFH Berlin

Sommersemester 2008

Geschichte des AES

Die Struktur des AES

Angriffe auf den AES

Aktuelle Ergebnisse

DerAdvanced Encryption Standard (AES)

AES = “Advanced Encryption Standard”:

128-bit Blockchiffre.

3 Varianten: 128-bit, 192-bit und 256-bit Schlüssel.

Ziele:

- Sicherer als Triple-DES
- Effizienter als Triple-DES

Geschichte des AES, 1. Teil

1997 Ausschreibung des AES.

1998 1. AES-Konferenz; Präsentation von 15 Kandidaten.
"The Demolition Derby begins."

1999 2. AES-Konferenz; danach Auswahl der 5 Finalisten.

15 Kandidaten

Feistel-Netzwerk			**S.-P. Netzerk**		**Sonstige**
(wie DES)		(erweitert)	allgemein	Square-artig	
DEAL	DFC	Cast-256	SAFER+	Crypton	Frog
Loki97	E2	MARS	Serpent	Rijndael	HPC
Magenta	RC6				
Twofish					

“Major Attacks”: DEAL, Frog, HPC, Loki97, Magenta

Finalisten: MARS, RC6, Rijndael, Serpent, Twofish

Geschichte des AES 2. Teil

April 2000 3. AES-Konferenz, Diskussion der Finalisten Mars, RC6, Rijndael, Twofish und Serpent.

Oktober 2000 Rijndael wird ("draft") Standard.

6 Monate später AES wird endgültig als Standard bestätigt.

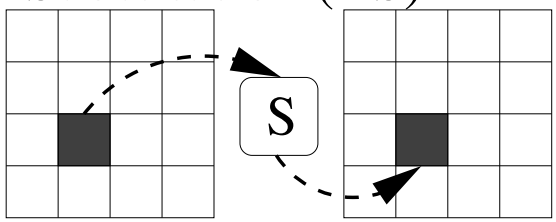
Die Struktur des AES

- Vier Basis-Operationen
- Eine AES-Runde als Kombination der vier Basis-Operationen
- Der „Key Schedule“: Aus einem kurzen Chiffrier-Schlüssel (128 bit–256 bit) werden 11–15 Rundenschlüssel (jeweils 128 bit).

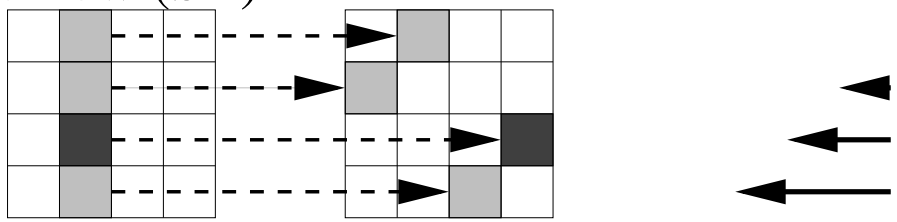
  Anzahl Rundenschlüssel $= 1 +$ Anzahl Runden

Die Basis-Operationen

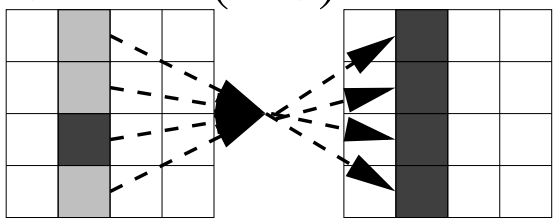
Byte Substitution (BS)



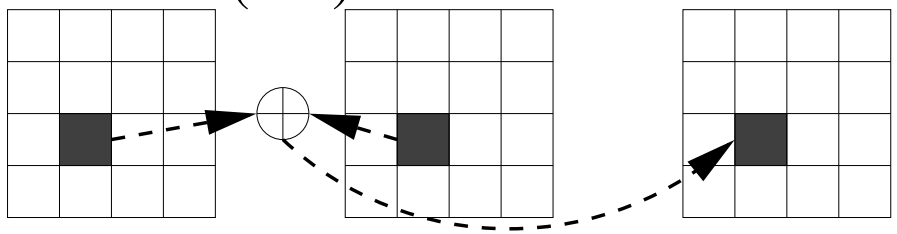
Shift Row (SR)



Mix Column (MC)



Key Addition (KA)



Die Byte Substitution

Anwendung einer invertierbaren S-Box

$$S : \{0,1\}^8 \rightarrow \{0,1\}^8$$

mit einer sehr einfachen algebraischen Struktur.

Algebraische Struktur

Man kann $z = S(x)$ in zwei Schritten berechnen:

1. Berechnung des Inversen:

   Wenn $x = 0$, dann $y := 0$. Sonst $y = x^{-1}$ (in $\mathrm{GF}(2^8)$).

2. Affine Transformation:

   $z := Ay + b$

   Dabei sind die Matrix $A \in \{0,1\}^{8\times 8}$ und der Vektor $b \in \{0,1\}^8$ definierte Konstanten; y und z werden (wie b) als Bit-Vektoren aus $\{0,1\}^8$ betrachtet.

Sinn dieser speziellen Konstruktion für die S-Box: Optimale Widerstandsfähigkeit gegen differentielle und lineare Kryptanalyse.

Die Mix Column Operation

$$\overbrace{(y_1, y_2, y_3, y_4)}^{\vec{y}} := \mathrm{MC}\overbrace{(x_1, x_2, x_3, x_4)}^{=\vec{x}}$$

Die Spalten $\vec{x}$ und $\vec{y}$ fassen wir als Vektoren auf: $\vec{x}, \vec{y} \in \mathrm{GF}(2^8)^4$.
Die Mix-Column-Operation ist eine Matrix-Operation über $\mathrm{GF}(2^8)$:
$\vec{y} := A\vec{x}$:

$$\vec{y} := \begin{pmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{pmatrix} \vec{x}.$$

Eigenschaften von Mix Column

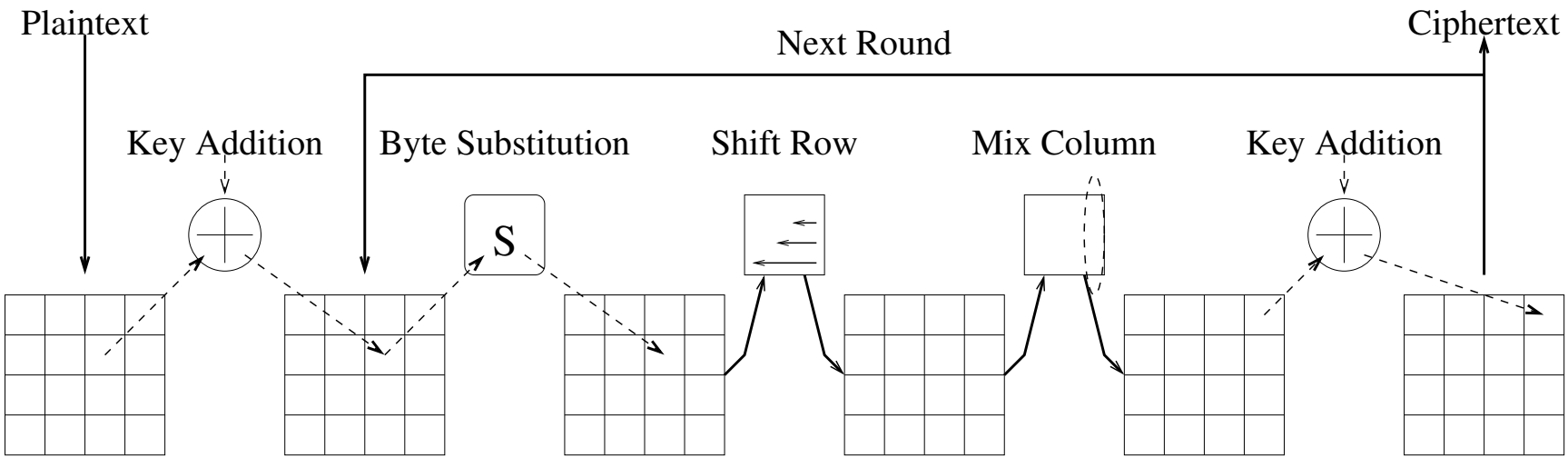
Invertierbarkeit:

Die Matrix A ist invertierbar über GF(2^8). Deshalb ist die Mix Column Operation invertierbar.

Ausbreitung von Differenzen:

Eine Differenz in genau einem der Eingabe-Werte x_i führt zu einer Differenz in allen vier Ausgabewerten y_1, y_2, y_3, y_4.

Die Rundenstruktur



Der “Key Schedule” (für 128-bit Schlüssel):

Es bez. $W[\cdot]$ einen 32-bit Wert (= 1 Spalte in der Matrix).
Aus dem 128-bit Chiffrierschlüssel $W[0], \ldots, W[3]$ sollen die Rundenschlüssel $W[4j+0], \ldots, W[4j+3]$ berechnet werden.

If $(i \bmod 4) = 0$
then $W[i] := W[i-4] \oplus f(W[i-1]) \oplus \mathrm{const}(i)$
else $W[i] := W[i-4] \oplus W[i-1]$

Kennt man i und zwei der Werte $W[i-4]$, $W[i-1]$ und $W[i]$, kann man den dritten leicht berechnen.

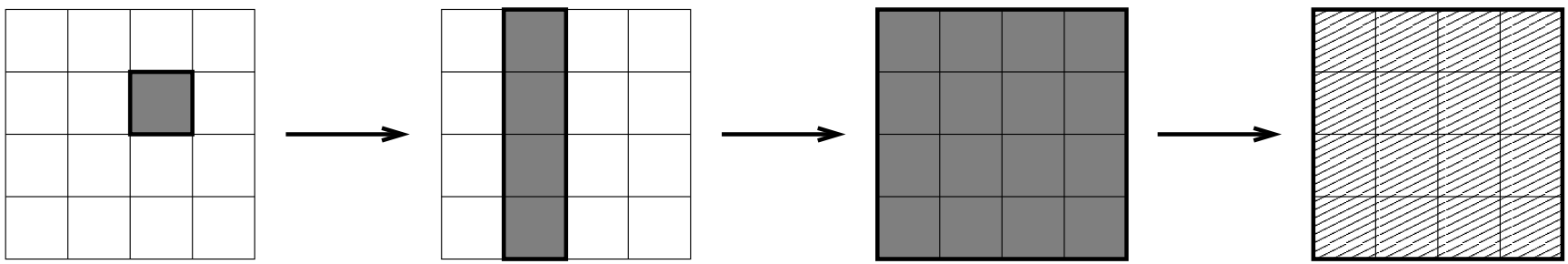
Angriffe auf den AES

Der gegenwärtige Stand der Forschung erlaubt es nicht, für eine (praktikable) Blockchiffre *nachzuweisen*, dass sie sicher ist.

Vertrauen in die Sicherheit einer Chiffre gewinnt man, wenn es trotz intensiver jahrelanger Analyse niemandem gelingt, einen durchschlagenden Angriff zu finden (bzw. zu publizieren).
Deshalb:

- Man berücksichtige die „besten“ bekannten Angriffe
- und halte möglichst einen *Sicherheitsabstand* von ihnen ein („einige Runden mehr“).

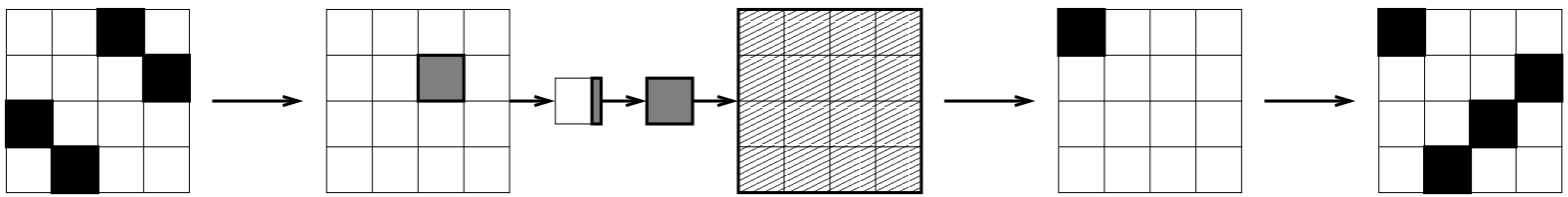
3 Runden des AES



Angriff auf 6 Runden des AES

(stammt von den AES-Autoren selbst)

- Wähle 2^{32} Klartexte.
- „Rate“ 9 Schlüsselbytes (2^{72} Einheiten Rechenzeit)

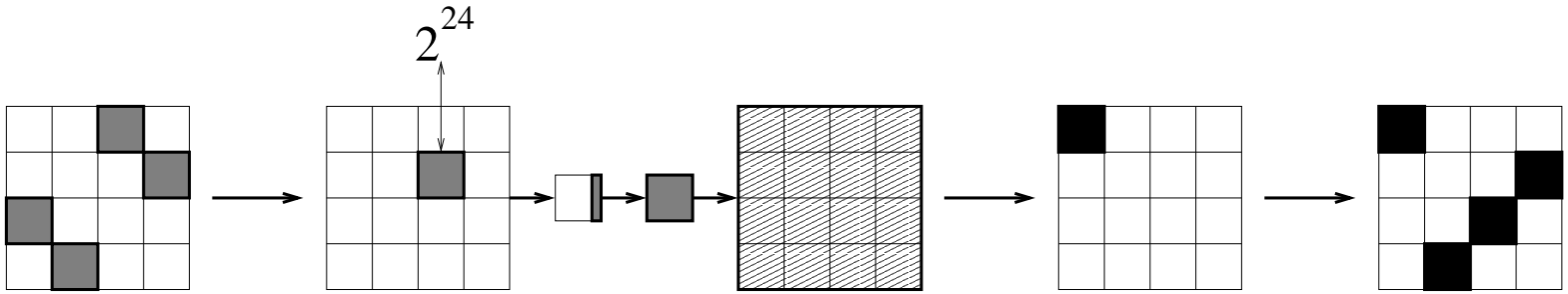


- 2^8 partielle Verschlüsselungen pro „Einheit“
  (jede Einheit entspricht etwa einer AES-Verschlüsselung)

$\rightarrow$ Rechenzeit $\approx$ 2^{72} Verschlüsselungs-Operationen

Verbesserter Angriff (6 Runden)

- Wähle 2^{32} Klartexte.
- „Rate“ 5 Schlüsselbytes
  (2^{40} Einheiten Rechenzeit, jede entspricht $\approx$ 1 Verschl.)



$\longrightarrow$ Rechenzeit $\approx$ 2^{40} Verschlüsselungs-Operationen

Erweiterung des Angriffs auf 7 Runden

Möglich mit 2^{128} Klartexten (= Codebuch).

Rechenzeit entspricht etwa 2^{120} Verschlüsselungsoperationen (nicht mitgerechnet die Zeit zur Erstellung des Code-Buchs).

Theoretischer Angriff (für 128-bit Schlüssel), aber besser als Brute Force (Suche über den gesamten Schlüsselraum).

Wieviele Runden werden gebraucht?

Angriffe, die *noch knapp* effizienter sind als Brute Force:

Chiffre (Schl.-Länge)	# Runden	
	definiert	Angriff
Rijndael/AES (128)	10	7
Rijndael/AES (192)	12	(8) 7
Rijndael/AES (256)	14	9
Twofish (128–256)	16	(8) 6
Serpent (128–256)	32	(10–11) 9

Stand: Ende 2001. Werte in Klammern stellen Verbesserungen gegenüber den dem NIST im Sommer 2000 bekannten Werten dar.

Wie relevant sind „akademische Angriffe“?

- Die „besten“ Angriffe sind total unpraktikabel (da sie z.B. 2^{128} Klartext-Chiffretext-Paare erfordern):
  - *„Angriffe können nur besser werden.“*
  - *“Let us destroy all the useless planets in our solar system, to get room for storage.”*
- Andere Sichtweise (Bsp. AES, 128-bit Schlüssel):
  - Angriffe auf 5 Runden sind einfach.
  - Angriffe auf 6 Runden sind vorstellbar (2^{32} Paare).
  - Angriffe auf 7 Runden sind bisher nur theoretisch möglich.

„Darf es etwas mehr sein?“

Manchen erscheint der „Sicherheitsspielraum“ des AES als zu gering. Einige Vorschläge zur Abhilfe:

1. Variable Anzahl an Runden.
2. Triple AES.
3. Nur die Variante mit 256-bit Schlüsseln einsetzen (14 Runden), kürzere Schlüssel ggf. „strecken“.
4. Andere Chiffren einsetzen, z.B. Twofish oder Serpent.

Risiken und Nebenwirkungen:

Variable Anzahl an Runden. Gefährlich! Beispiel: 24 Runden AES und 25 Runden AES unter dem gleichenSchlüssel ...

Triple AES. OK, aber vielleich Overkill.

Nur die Variante mit 256-bit Schlüsseln einsetzen ... Guter Ansatz, aber Vorsicht: Beim „Strecken“ kann man sich auch „in's Knie schiessen“!

Andere Chiffren einsetzen, z.B. Twofish oder Serpent. Nachteil: Andere Chiffren werden weniger genau untersucht werden wie der AES.

Aktuelle Ergebnisse

Nutzen meistens die einfache algebraische Struktur der S-Box.
Zwei interessante Ergebnisse:

- AES als geschlossene algebraische Formel
- Angriff auf den AES durch Lösen eines nichtlinearen Gleichungssystems

AES als geschlossene algebraische Formel

Es existiert eine einfache geschlossene algebraische Formel für die Blockchiffre Rijndael. Die Größe der Formel hängt nur linear von der Anzahl der Runden ab.

(Im Allgemeinen würde man von einer Blockchiffre erwarten, dass jede geschlossene algebraische Formel viel zu groß *wäre, um jemals aufgeschrieben werden zu können.)*

AES als geschlossene algebraische Formel (2)

Eine Runde des AES verwendet den Rundenschlüssel $k^{(r)}$ und bildet die 128-bit Eingabe $a^{(r)}$ auf die Ausgabe $a^{(r+1)}$ ab:

$$a_{i,j}^{(r+1)} = k_{i,j}^{(r)} + \sum_{e_r=0}^{3} \sum_{d_r=0}^{7} \frac{w_{i,e_r,d_r}}{\left(a_{e_r,e_r+j}^{(r)}\right)^{2^{d_r}}}$$

(Berechnungen im Körper GF(2^8).)

AES als geschlossene algebraische Formel (3)

2 Runden:

$$a_{i,j}^{(r+1)} = k_{i,j}^{(r)} + \sum_{e_r=0}^{3} \sum_{d_r=0}^{7} \frac{w_{i,e_r,d_r}}{\left(k_{i,j}^{(r-1)} + \sum_0^3 \sum_0^7 \frac{w_{\dots}}{\left(a_{\dots}^{(r-1)}\right)^{2^{\cdots}}} \right)^{2^{d_r}}}$$

Allgemein:
Bei r Runden enthält man eine Art Kettenbruch mit r Bruchstrichen ...

Zusammenfassung

AES: 128-bit Blockchiffe, sehr effizient

- einige Kritik an geringem Sicherheitsspielraum
- noch relativ jung, aber in einigen Jahren ebenso gut untersucht wie der DES heute
- Triple DES wird, trotz AES, noch lange Zeit weiter genutzt werden

Danksagungen

Danksagungen

- Aus einer Vorlesung von Stefan Lucks
- Erstellt mit Freier Software