

Universität Paderborn FB Mathematik & Informatik    AG Algorithmische Mathematik

# Grundlagen der Rijndael Funktionen

Joachim von zur Gathen

Universität Paderborn

## Endliche algebraische Bereiche

Rijndael Grundlagen

Kombination von

- **Algebra** (Struktur) und
- **Informatik** (im Computer darstellbare Objekte).

Joachim von zur Gathen  
28. Juni 2001

Universität Paderborn

## Anwendungen in der Informatik

Rijndael Grundlagen

- Fehlerbeseitigung bei Datenübertragungen (Satelliten, CD)
- Hashing
- Kommunikation in Rechnernetzen (Routing)
- Kryptographie

Joachim von zur Gathen  
28. Juni 2001

Universität Paderborn

## Zahlen

Rijndael Grundlagen

- Leopold Kronecker 1886: „Die ganzen Zahlen hat der liebe Gott gemacht, alles andere ist Menschenwerk.“
- **Z** : ... -3, -2, -1, 0, 1, 2, 3, 4, ...
- Ring der ganzen Zahlen.
- Addition, Subtraktion.
- Multiplikation.

Joachim von zur Gathen  
28. Juni 2001

Universität Paderborn

## Division?

Rijndael Grundlagen

- Division?
- In allg. nicht möglich!
- Division mit Rest:  
33 geteilt durch 5:

$$33 = 6 \cdot 5 + 3$$

Quotient     Modul     Rest

Joachim von zur Gathen  
28. Juni 2001

Universität Paderborn

## Division mit Rest

Rijndael Grundlagen


- Division mit Rest:


$$a = q \cdot m + r, \quad 0 \leq r < m$$


Quotient     Modul     Rest


- Schreibweise:  $a \equiv r \pmod{m}$ .
- Also:  $a - r$  ist durch  $m$  teilbar.


Joachim von zur Gathen  
28. Juni 2001


 Universität Paderborn	<h3>Modulares Rechnen</h3>
Rijndael Grundlagen	<ul style="list-style-type: none"> <li>• <math>\mathbb{Z}_m = \{0, 1, \dots, m-1\}</math>                      Addition, Subtraktion,                      Multiplikation "modulo <math>m</math>".</li> <li>• Übliche Rechenregeln:                      „<math>\mathbb{Z}_m</math> ist ein Ring“.</li> <li>• Division??</li> </ul>
Joachim von zur Gathen 28. Juni 2001	7


 Universität Paderborn	<h3>Euklidischer Algorithmus</h3>
Rijndael Grundlagen	<ul style="list-style-type: none"> <li>• Euklid, ca. 300 v. Chr.</li> </ul> $  \begin{aligned}  &= -4 \cdot 8 + 3 \cdot 11 \\  &= -1 \cdot 8 + 3 \cdot (11 - 8) \\  \bullet \quad 11 &= 1 \cdot 8 + 3 \\  \bullet \quad 8 &= 2 \cdot 3 + 2 &= -1 \cdot 8 + 3 \cdot 3 \\  \bullet \quad 3 &= 1 \cdot 2 + 1 &= 3 - 1 \cdot (8 - 2 \cdot 3) \\  &= 3 - 1 \cdot 2  \end{aligned}  $
Joachim von zur Gathen 28. Juni 2001	8


 Universität Paderborn	<h3>Modulare Inverse</h3>
Rijndael Grundlagen	<ul style="list-style-type: none"> <li>• Also: <math>1 = -4 \cdot 8 + 3 \cdot 11</math>. Oder:</li> <li>• <math>1 \equiv -4 \cdot 8 \pmod{11}</math>  <math>\equiv 7 \cdot 8 \pmod{11}</math></li> <li>• Also: das Inverse von 8 modulo 11 ist 7.</li> </ul>
Joachim von zur Gathen 28. Juni 2001	9


 Universität Paderborn	<h3>Körper</h3>
Rijndael Grundlagen	<ul style="list-style-type: none"> <li>• Falls <math>m</math> eine Primzahl ist, so hat jedes <math>a</math> (mit <math>a \not\equiv 0 \pmod{m}</math>) ein Inverses modulo <math>m</math>.</li> <li>• Division in <math>\mathbb{Z}_m</math> geht immer (außer durch 0).</li> </ul> <p style="text-align: center;">„<math>\mathbb{Z}_m</math> ist ein Körper.“</p>
Joachim von zur Gathen 28. Juni 2001	10


 Universität Paderborn	<h3>Nichtkörper</h3>
Rijndael Grundlagen	<p>Aber <math>m=12, a=2</math>:</p> $x \cdot 2 = 1 + 12 \cdot y$ <p>hat keine Lösung.</p>
Joachim von zur Gathen 28. Juni 2001	11


 Universität Paderborn	<h3>Der Bereich <math>\mathbb{Z}_m</math></h3>
Rijndael Grundlagen	<p>Unendlicher Bereich <math>\mathbb{Z}</math>,                  Modul <math>m \in \mathbb{Z}</math>.</p> <p><math>\Rightarrow</math> modulares Rechnen im                  endlichen Bereich <math>\mathbb{Z}_m</math>.</p>
Joachim von zur Gathen 28. Juni 2001	12


 Universität Paderborn	<h3>Der Körper <math>\mathbb{Z}_2</math></h3>
Rijndael Grundlagen	<ul style="list-style-type: none"> <li>• Für die Informatik wichtigster Fall:  <math>m=2</math>: <math>\mathbb{Z}_2 = \{0, 1\}</math>.</li> <li>• <math>1+1=0</math>                      „Addition modulo 2“, „exklusives oder“.</li> <li>• insbesondere: <math>1 = -1</math>.</li> <li>• Sprungbrett für wiederholtes Anwenden.</li> </ul>
Joachim von zur Gathen 28. Juni 2001	13


 Universität Paderborn	<h3>Polynome</h3>
Rijndael Grundlagen	<ul style="list-style-type: none"> <li>• <math>\mathbb{Z}_2[x]</math>: Polynome über <math>\mathbb{Z}_2</math>  <math>a = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0</math>,  <math>a_n, \dots, a_0 \in \mathbb{Z}_2 = \{0, 1\}</math>.</li> <li>• Falls <math>a_n = 1</math>: <math>n = \text{Grad von } a</math>.</li> <li>• Addition, Subtraktion: Bit für Bit.</li> <li>• Kurzschreibweise: <math>(a_n a_{n-1} \dots a_0)</math>.</li> </ul>
Joachim von zur Gathen 28. Juni 2001	14


 Universität Paderborn	<h3>Polynome</h3>
Rijndael Grundlagen	<ul style="list-style-type: none"> <li>• <math>a = (10011011) = x^7 + x^4 + x^3 + x + 1</math>.</li> <li>• <math>b = (11001101) = x^7 + x^6 + x^3 + x^2 + 1</math>.</li> <li>• Addition:  <math>a + b = (01010110) = x^6 + x^4 + x^2 + x</math>.</li> <li>• Multiplikation:  <math>a \cdot b = x^{14} + x^{13} + x^{11} + x^{10} + x^8 + x^6 + x^5 + x^3 + x^2 + x + 1</math>.</li> </ul>
Joachim von zur Gathen 28. Juni 2001	15


 Universität Paderborn	<h3>Der Bereich <math>\mathbb{Z}_2[x] / \langle m \rangle</math></h3>
Rijndael Grundlagen	<p>Unendlicher Bereich <math>\mathbb{Z}_2[x]</math>,                  Modul <math>m \in \mathbb{Z}_2[x]</math>.</p> <p><math>\Rightarrow</math> modulares Rechnen im                  endlichen Bereich <math>\mathbb{Z}_2[x] / \langle m \rangle</math>.</p>
Joachim von zur Gathen 28. Juni 2001	16


 Universität Paderborn	<h3>Modulares Rechnen mit Polynomen</h3>
Rijndael Grundlagen	<p><math>m = x^8 + x^4 + x^3 + x + 1 \in \mathbb{Z}_2[x]</math>                  (Rijndael)</p> <p><math>a = x^7 + x^4 + x^3 + x + 1</math>  <math>b = x^7 + x^6 + x^3 + x^2 + 1</math>  <math>a \cdot b = x^{14} + x^{13} + x^{11} + x^{10} + x^8 + x^6 + x^5 + x^3 + x^2 + x + 1</math></p>
Joachim von zur Gathen 28. Juni 2001	17


 Universität Paderborn	<h3>Modulares Rechnen mit Polynomen</h3>
Rijndael Grundlagen	<p><math>m = x^8 + x^4 + x^3 + x + 1 \in \mathbb{Z}_2[x]</math>                  (Rijndael)</p> <p><math>a \cdot b = x^{14} + x^{13} + x^{11} + x^{10} + x^8 + x^6 + x^5 + x^3 + x^2 + x + 1</math></p>
Joachim von zur Gathen 28. Juni 2001	18


 Universität Paderborn	<b>Modulares Rechnen mit Polynomen</b>
Rijndael Grundlagen	$m = x^8 + x^4 + x^3 + x + 1 \in \mathbb{Z}_2[x]$ <p style="text-align: center;"><b>(Rijndael)</b></p> $a \cdot b = x^{14} + x^{13} + x^{11} + x^{10} + x^8 + x^6 + x^5 + x^3 + x^2 + x + 1$ $= (x^6 + x^5 + x^3) \cdot m + (x^4 + x^2 + x + 1)$
Joachim von zur Gathen 28. Juni 2001	19

 Universität Paderborn	<b>Modulares Rechnen mit Polynomen</b>
Rijndael Grundlagen	$m = x^8 + x^4 + x^3 + x + 1 \in \mathbb{Z}_2[x]$ <p style="text-align: center;"><b>(Rijndael)</b></p> $a \cdot b = x^{14} + x^{13} + x^{11} + x^{10} + x^8 + x^6 + x^5 + x^3 + x^2 + x + 1$ $= (x^6 + x^5 + x^3) \cdot m + (x^4 + x^2 + x + 1)$ $a \cdot b \equiv x^4 + x^2 + x + 1 \pmod{m}$
Joachim von zur Gathen 28. Juni 2001	20

 Universität Paderborn	<b>Allgemeine Division mit Rest</b>
Rijndael Grundlagen	$a = q \cdot m + r, \quad 0 \leq \text{Grad } r < \text{Grad } m$ $a \equiv r \pmod{m}$
Joachim von zur Gathen 28. Juni 2001	21

 Universität Paderborn	<b>Noch mehr Körper...</b>
Rijndael Grundlagen	<ul style="list-style-type: none"> <li>• Eine ganze Zahl <math>p</math> ist <b>prim</b>, genau wenn sie nur die Teiler <math>\pm 1</math> und <math>\pm p</math> hat.</li> <li>• Entsprechend: Ein Polynom <math>m</math> in <math>\mathbb{Z}_2[x]</math> ist <b>irreduzibel</b>, genau wenn es nur die Teiler <math>1</math> und <math>m</math> hat.</li> <li>• Falls <math>m</math> irreduzibel ist, so hat jedes Polynom <math>a</math> (mit <math>a \not\equiv 0 \pmod{m}</math>) ein Inverses modulo <math>m</math>.</li> </ul>
Joachim von zur Gathen 28. Juni 2001	22

 Universität Paderborn	<b>Noch mehr Körper...</b>
Rijndael Grundlagen	<ul style="list-style-type: none"> <li>• Division in <math>\mathbb{Z}_2[x]/\langle m \rangle</math> geht immer (außer durch 0).</li> <li>• „<math>\mathbb{Z}_2[x]/\langle m \rangle</math> ist ein Körper.“</li> <li>• Wenn <math>m</math> Grad <math>n</math> hat, so besteht <math>\mathbb{Z}_2[x]/\langle m \rangle</math> aus den Polynomen <math>a_{n-1}x^{n-1} + \dots + a_1x + a_0</math> mit <math>a_{n-1}, \dots, a_0 \in \{0, 1\}</math>, hat also <math>2^n</math> Elemente.</li> </ul>
Joachim von zur Gathen 28. Juni 2001	23

 Universität Paderborn	<b>Noch mehr Körper...</b>
Rijndael Grundlagen	<ul style="list-style-type: none"> <li>• Bezeichnung:  <math display="block">\mathbb{F}_{2^n} = \mathbb{Z}_2[x]/\langle m \rangle</math>                 (Nur wenn <math>m</math> irreduzibel ist.)             </li> </ul>
Joachim von zur Gathen 28. Juni 2001	24

**Der Körper  $F_{256}$**

Rijndael Grundlagen

- In Rijndael:  $m = x^8 + x^4 + x^3 + x + 1$ .
- Wir rechnen in  $F_{256} = F_{2^8} = \mathbb{Z}_2[x]/(m)$ .
- Element von  $F_{256}$  = ein Byte.  
 (Beachte:  $F_{256} \neq \mathbb{Z}_{256}$ !)

Joachim von zur Gathen  
28. Juni 2001

**Inverse**

Rijndael Grundlagen

- Die 255 Elemente  $a$  von  $F_{256}$  ungleich Null haben ein Inverses  $\text{inv}(a)$ . Wir setzen noch  $\text{inv}(0) = 0$ .
- Dann erhalten wir eine Abbildung

$$\text{inv}: F_{256} \rightarrow F_{256}$$

$$a \rightarrow \text{inv}(a).$$

Joachim von zur Gathen  
28. Juni 2001

**Nichtlinear!**

Rijndael Grundlagen

- Wichtige Eigenschaft:  
 $\text{inv}$  ist **nichtlinear**.
- Beispiel: das Vertauschen  $(a_0, a_1) \rightarrow (b_0, b_1) = (a_1, a_0)$  von zwei Bits ist linear, denn es gilt immer  $a_0 + b_1 = 0$ .

Joachim von zur Gathen  
28. Juni 2001

**Rijndaels S-Box**

Rijndael Grundlagen

- $\text{inv}$  kommt in Rijndaels ByteSub vor.  
 (Nachher kommt in ByteSub noch eine lineare Transformation.)
- Es ist die einzige nichtlineare Transformation, ähnlich wie die S-Boxen in DES.

Joachim von zur Gathen  
28. Juni 2001

**Lineare Angriffe**

Rijndael Grundlagen

- Jedes noch so komplizierte Verknüpfen von linearen Transformationen liefert eine lineare Transformation.
- Ein Kryptosystem, das nur aus linearen Transformationen besteht, fällt dem **linearen Angriff** zum Opfer.
- Also: Nichtlinearität ist notwendig.

Joachim von zur Gathen  
28. Juni 2001

**Einfachheit**

Rijndael Grundlagen

- Grosser Vorteil von ByteSub gegenüber den S-Boxen von DES.
- Dies ist eine natürliche, durchsichtige Operation, die einfach zu beschreiben ist.
- Darin ist wohl keine **Hintertür** eingebaut.

Joachim von zur Gathen  
28. Juni 2001

Universität Paderborn

Rijndael Grundlagen

Der Bereich  $\mathbb{F}_{256}[z]/\langle f \rangle$

Unendlicher Bereich  $\mathbb{F}_{256}[z]$ ,  
 Modul  $f \in \mathbb{F}_{256}[z]$ .

$\Rightarrow$  modulares Rechnen im  
 endlichen Bereich  $\mathbb{F}_{256}[z]/\langle f \rangle$ .

Joachim von zur Gathen  
 28. Juni 2001

Universität Paderborn

Rijndael Grundlagen

Der Bereich  $\mathbb{F}_{256}[z]/\langle f \rangle$

- Rijndael:  
 $f = z^4 + 1$   
 $= (z+1)^4 = z^4 + 4z^3 + 6z^2 + 4z + 1$   
 in  $\mathbb{F}_{256}[z]$ .
- $f$  ist nicht irreduzibel.
- Nicht jedes Polynom ( $\neq 0$ ) in  $\mathbb{F}_{256}[z]$  hat ein Inverses modulo  $f$ .

Joachim von zur Gathen  
 28. Juni 2001

Universität Paderborn

Rijndael Grundlagen

Der Bereich  $\mathbb{F}_{256}[z]/\langle f \rangle$

- Aber manche haben ein Inverses.
- Zum Beispiel

$$c = (x+1) \cdot z^3 + z^2 + z + x \cdot z$$

in  $\mathbb{F}_{256}[z]/\langle z^4+1 \rangle =$   
 $\mathbb{Z}_2[x, z]/\langle x^8+x^4+x^3+x+1, z^4+1 \rangle$ .

Joachim von zur Gathen  
 28. Juni 2001

Universität Paderborn

Rijndael Grundlagen

Der Bereich  $\mathbb{F}_{256}[z]/\langle f \rangle$

- Ein Element  $w = b_3z^3 + b_2z^2 + b_1z + b_0$  von  $\mathbb{F}_{256}[z]/\langle f \rangle$  braucht 4 Bytes = 1 Wort.
- Die Operation MixColumn in Rijndael ist die Multiplikation mit  $c$ , modulo  $z^4+1$ . Dies ist eine lineare Operation.

Joachim von zur Gathen  
 28. Juni 2001

Universität Paderborn

Rijndael Grundlagen

Der Bereich  $\mathbb{F}_{256}[z]/\langle f \rangle$

- Die Reduktion modulo  $z^4+1$  ist besonders einfach:

$$c_6 \quad c_5 \quad c_4 \quad c_3 \quad c_2 \quad c_1 \quad c_0$$

Joachim von zur Gathen  
 28. Juni 2001

Universität Paderborn


Rijndael Grundlagen

Der Bereich  $\mathbb{F}_{256}[z]/\langle f \rangle$

- Die Reduktion modulo  $z^4+1$  ist besonders einfach:

$$\begin{array}{cccc} & c_6 & c_5 & c_4 \\ c_3 & c_2 & c_1 & c_0 \\ \hline c_3 & c_6+c_2 & c_5+c_1 & c_4+c_0 \end{array}$$

Joachim von zur Gathen  
 28. Juni 2001

 Universität Paderborn	
Rijndael Grundlagen	<ul style="list-style-type: none"><li>• In RijndaelsByteSub kommt noch die Operation <math>a \rightarrow t_1 \cdot a + t_0 \pmod{x^8+1}</math> auf einem Byte <math>a</math> vor, wobei <math>t_1</math> und <math>t_0</math> feste Bytes sind.</li><li>• Dies ist linear und wieder besonders einfach zu berechnen.</li></ul>
Joachim von zur Gathen 28. Juni 2001	