Einfache Halbringe und ihre kryptographischen Anwendungen

Jens Zumbrägel

www.math.uzh.ch/user/jzumbr
Institut für Mathematik
Universität Zürich

7. Kryptotag · 9. November 2007
b-it Bonn

Gliederung

Einfache Halbringe

verallgemeinerte Ringe, die keine Reduktion auf ein kleineres homomorphes Bild besitzen

Einweg-Operationen

schwierig invertierbare Operationen von Halbgruppen auf Mengen

Einweg-Operationen mit einfachen Halbringen

ein neues, effizientes Public-Key-Kryptosystem??

Gliederung

1. Einfache Halbringe
   - Halbringe
   - Einfachheit
   - Klassifikation einfacher Halbringe
2. Einweg-Operationen
   - Einweg-Operationen und Protokolle
   - Beispiele
3. Einweg-Operationen mit einfachen Halbringen
   - Zweiseitige Operationen
   - Beispiele

Was ist ein Halbring?

Halbringe sind "Ringe ohne additiv inverse Elemente".

Definition

Eine Struktur $(R, +, \cdot)$ heißt Halbring, wenn

- $(R, +)$ ein kommutativer Monoid mit neutralem Element 0 ist,
- $(R, \cdot)$ eine Halbgruppe ist, in der 0 absorbierend ist,
- und die Distributivgesetze $(x + y) \cdot z = x \cdot z + y \cdot z$ und $x \cdot (y + z) = x \cdot y + x \cdot z$ gelten.

Beispiele

- die *natürlichen Zahlen* $(\mathbb{N} = \{0, 1, 2, 3, \dots\}, +, \cdot)$
- der *tropische Halbring* $(\bar{\mathbb{R}} = \mathbb{R} \cup \{\infty\}, \min, +)$, "Null" ist ∞
- der *Boole'sche Halbring* $(\mathbb{B} = \{0, 1\}, \texttt{or}, \texttt{and})$

Halbringe sind zahlreich

Größe	Halbringe	Ringe
2	4	2
3	22	2
4	283	11
5	4’717	2
6	108’992	4
7	8’925’672	2
2...7	9’039’691	23

Einfache Halbringe

Definition

Ein Halbring R heißt einfach wenn gilt:
Ist $S \neq \{0\}$ ein Halbring und $f : R \to S$ ein surjektiver Homomorphismus, so ist f auch injektiv (also gilt $S \cong R$).

Beispiele

- Die Abbildung $f : \mathbb{N} \to \mathbb{B}, f(n) = \begin{cases} 0 & \text{für } n = 0 \\ 1 & \text{für } n \geq 1 \end{cases}$
  ist ein surjektiver Halbringhomomorphismus, der nicht injektiv ist. Also ist der Halbring $\mathbb{N}$ *nicht* einfach.
- Der Halbring $\mathbb{B}$ ist dagegen einfach.

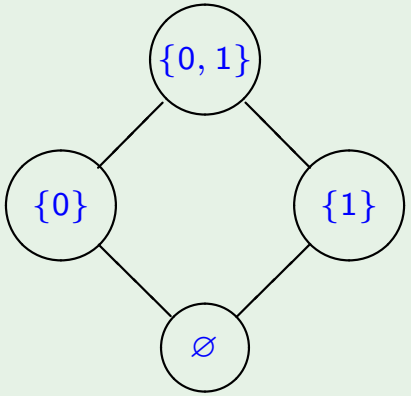
Verbände und Halbringe

Definition

Ein Verband ist eine geordnete Menge $(L, \leq)$, so dass für je zwei Elemente $x, y \in L$ das Supremum $x \vee y$ und das Infimum $x \wedge y$ existiert.

Beispiel

$L = \mathcal{P}(\{0, 1\})$



- $(L, \vee)$ ist ein kommutatives Monoid.
- Die Monoidendomorphismen $R = End(L, \vee)$ bilden einen Halbring, wobei $f + g, f \cdot g$ für $f, g \in R$ wie folgt definiert ist:

$$(f + g)(x) = f(x) \vee g(x), \quad (f \cdot g)(x) = f(g(x)) \quad (x \in L).$$

Klassifikation einfacher Halbringe

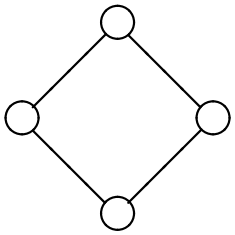
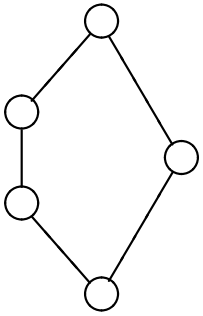
Satz ([Zum07])

Sei R ein endlicher Halbring mit mehr als 2 Elementen, der kein Ring ist. Dann sind äquivalent:

- *R ist einfach.*
- *Es gibt einen endlichen Verband $(L, \leq, \vee, \wedge)$ und einen injektiven Homomorphismus $R \hookrightarrow \mathrm{End}(L, \vee)$, so dass alle $f \in \mathrm{End}(L, \vee)$ mit $|\operatorname{Im} f| \leq 2$ im Bild von R liegen.*
  "R ist ein dichter Unterhalbring von $\mathrm{End}(L, \vee)$."

Beispiele von Endomorphismenhalbringen

L	$\mathrm{End}(L, \vee)$
	$\mathbb{B}$, Boole'scher HR
	R_6
	R_{20}

L	$\mathrm{End}(L, \vee)$
	R_{16}
	R_{43}

Ein einfacher Halbring mit 6 Elementen

R6 = ({0,1,a,b,c,d},+,*)

+	0	a	b	c	1	d
0	0	a	b	c	1	d
a	a	a	b	c	1	d
b	b	b	b	1	1	d
c	c	c	1	c	1	d
1	1	1	1	1	1	d
d	d	d	d	d	d	d

*	0	a	b	c	1	d
0	0	0	0	0	0	0
a	0	0	0	a	a	b
b	0	a	b	a	b	b
c	0	0	0	c	c	d
1	0	a	b	c	1	d
d	0	c	d	c	d	d

Ein einfacher Halbring mit 20 Elementen

R20 = ({0,1,a,b,c,d,e,f,g,h,i,j,k,l,m,n,o,p,q,r},+,*)

+	0	a	b	c	d	e	f	g	h	i	j	k	l	m	1	n	o	p	q	r
0	0	a	b	c	d	e	f	g	h	i	j	k	l	m	1	n	o	p	q	r
a	a	a	b	c	d	e	f	g	h	i	j	k	l	m	1	n	o	p	q	r
b	b	b	b	c	e	e	f	g	h	i	k	k	l	m	1	n	o	p	q	r
c	c	c	c	c	f	f	f	h	h	i	l	l	l	1	1	n	p	p	q	r
d	d	d	e	f	d	e	f	g	h	i	j	k	l	m	1	n	o	p	q	r
e	e	e	e	f	e	e	f	g	h	i	k	k	l	m	1	n	o	p	q	r
f	f	f	f	f	f	f	f	h	h	i	l	l	l	1	1	n	p	p	q	r
g	g	g	g	h	g	g	h	g	h	i	m	m	1	m	1	n	o	p	q	r
h	h	h	h	h	h	h	h	h	h	i	1	1	1	1	1	n	p	p	q	r
i	i	i	i	i	i	i	i	i	i	i	n	n	n	n	n	n	q	q	q	r
j	j	j	k	l	j	k	l	m	1	n	j	k	l	m	1	n	o	p	q	r
k	k	k	k	l	k	k	l	m	1	n	k	k	l	m	1	n	o	p	q	r
l	l	l	l	l	l	l	l	1	1	n	l	l	l	1	1	n	p	p	q	r
m	m	m	m	1	m	m	1	m	1	n	m	m	1	m	1	n	o	p	q	r
1	1	1	1	1	1	1	1	1	1	n	1	1	1	1	1	n	p	p	q	r
n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	q	q	q	r
o	o	o	o	p	o	o	p	o	p	q	o	o	p	o	p	q	o	p	q	r
p	p	p	p	p	p	p	p	p	p	q	p	p	p	p	p	q	p	p	q	r
q	q	q	q	q	q	q	q	q	q	q	q	q	q	q	q	q	q	q	q	r
r	r	r	r	r	r	r	r	r	r	r	r	r	r	r	r	r	r	r	r	r

*	0	a	b	c	d	e	f	g	h	i	j	k	l	m	1	n	o	p	q	r
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
a	0	0	0	0	0	0	0	0	0	0	a	a	a	a	a	a	b	b	b	c
b	0	0	0	0	a	a	a	b	b	c	a	a	a	b	b	c	b	b	c	c
c	0	a	b	c	a	b	c	b	c	c	a	b	c	b	c	c	b	c	c	c
d	0	0	0	0	0	0	0	0	0	0	d	d	d	d	d	d	g	g	g	i
e	0	0	0	0	a	a	a	b	b	c	d	d	d	e	e	f	g	g	h	i
f	0	a	b	c	a	b	c	b	c	c	d	e	f	e	f	f	g	h	h	i
g	0	0	0	0	d	d	d	g	g	i	d	d	d	g	g	i	g	g	i	i
h	0	a	b	c	d	e	f	g	h	i	d	e	f	g	h	i	g	h	i	i
i	0	d	g	i	d	g	i	g	i	i	d	g	i	g	i	i	g	i	i	i
j	0	0	0	0	0	0	0	0	0	0	j	j	j	j	j	j	o	o	o	r
k	0	0	0	0	a	a	a	b	b	c	j	j	j	k	k	l	o	o	p	r
l	0	a	b	c	a	b	c	b	c	c	j	k	l	k	l	l	o	p	p	r
m	0	0	0	0	d	d	d	g	g	i	j	j	j	m	m	n	o	o	q	r
1	0	a	b	c	d	e	f	g	h	i	j	k	l	m	1	n	o	p	q	r
n	0	d	g	i	d	g	i	g	i	i	j	m	n	m	n	n	o	q	q	r
o	0	0	0	0	j	j	j	o	o	r	j	j	j	o	o	r	o	o	r	r
p	0	a	b	c	j	k	l	o	p	r	j	k	l	o	p	r	o	p	r	r
q	0	d	g	i	j	m	n	o	q	r	j	m	n	o	q	r	o	q	r	r
r	0	j	o	r	j	o	r	o	r	r	j	o	r	o	r	r	o	r	r	r

Gliederung

1. Einfache Halbringe
   - Halbringe
   - Einfachheit
   - Klassifikation einfacher Halbringe
2. Einweg-Operationen
   - Einweg-Operationen und Protokolle
   - Beispiele
3. Einweg-Operationen mit einfachen Halbringen
   - Zweiseitige Operationen
   - Beispiele

Was ist eine Einweg-Operation?

Definition (vgl. [MMR07])

Sei $(A, \cdot)$ Halbgruppe und X Menge. Eine Einweg-Operation ist eine Operation $\varphi : A \times X \to X$ von A auf X, so dass:

- φ ist effizient berechenbar,
- für generische $x, y \in X$ ist es schwierig, $a \in A$ zu finden mit $\varphi(a, x) = y$ (unter der Voraussetzung der Existenz).

Beispiel (Exponentiation in Gruppen)

- $A = (\mathbb{Z}_n, \cdot)$
- $X = (G, \cdot)$ Gruppe der Ordnung n (mit schwierigem DLP)
- $\varphi : (\mathbb{Z}_n, \cdot) \times G \to G, \quad \varphi(a, x) := x^a.$

Verallgemeinerung des DLP

Sei $\varphi : A \times X \to X$ eine Einweg-Operation. Betrachte das Problem:

- gegeben $x, y \in X$, so dass $\tilde{a} \in A$ mit $\varphi(\tilde{a}, x) = y$ existiert
- finde $a \in A$, so dass $\varphi(a, x) = y$

Algorithmen

- erschöpfende Suche
  Laufzeit $O(\min\{|A|, |X|\})$
- Pollard-ρ-Variante im "Gruppenanteil" der Halbgruppe $(A, \cdot)$: eine Kollision $\varphi(a, x) = \varphi(b, y)$ impliziert $\varphi(b^{-1}a, x) = y$
  Laufzeit $O(\sqrt{|X|})$

Gibt es einen generischen Algorithmus mit Laufzeit $O(\sqrt{|X|})$?

Ein Protokoll zum Schlüsselaustausch

Sei $\varphi : A \times X \to X$ eine Einweg-Operation von $(A, \cdot)$ auf X. Seien ferner $C_A, C_B \subseteq A$ Teilmengen mit $ab = ba$ für $a \in C_A$, $b \in C_B$.

Protokoll

Alice	öffentlich	Bob
	wähle $x \in X$	
wähle $a \in C_A$	$\varphi(a, x) \in X$	
	$\varphi(b, x) \in X$	wähle $b \in C_B$
$\varphi(a, \varphi(b, x))$		$\varphi(b, \varphi(a, x))$

Der gemeinsame Schlüssel ist
$\varphi(a, \varphi(b, x)) = \varphi(ab, x) = \varphi(ba, x) = \varphi(b, \varphi(a, x))$.

Sicherheitsrelevantes Problem:

- gegeben x, $y_A = \varphi(a, x)$, $y_B = \varphi(b, x)$ mit $ab = ba$
- finde $k = \varphi(ab, x)$

Beispiele für Einweg-Operationen

- **Konjugation in Gruppen** [KLCHKP00]
  $A = X = (G, \cdot)$ Gruppe, $\varphi(a, x) := a \cdot x \cdot a^{-1}$
  Betrachte z.B. die Zopf-Gruppe $G = B_n = \langle \sigma_1, \ldots, \sigma_{n-1} \rangle$ mit n Strängen.
  Setze $C_A = \langle \sigma_1, \ldots, \sigma_{m-1} \rangle$ und $C_B = \langle \sigma_{m+1}, \ldots, \sigma_{n-1} \rangle$.
- **Endomorphismen elliptischer Kurven** [Cou06]
  sei E eine elliptische Kurve mit Endomorphismenring $\mathcal{O}$
  $A = Cl(\mathcal{O})$ die Klassengruppe
  $X = \{$die zu E isomorphen elliptischen Kurven$\}$
  konstruiere Einweg-Operation $\varphi : Cl(\mathcal{O}) \times X \to X$

Gliederung

1. Einfache Halbringe
   - Halbringe
   - Einfachheit
   - Klassifikation einfacher Halbringe
2. Einweg-Operationen
   - Einweg-Operationen und Protokolle
   - Beispiele
3. Einweg-Operationen mit einfachen Halbringen
   - Zweiseitige Operationen
   - Beispiele

Zweiseitige Operationen

Sei $(G, \cdot)$ eine Halbgruppe und $U \subseteq G$ eine Unterhalbgruppe.

- $(A, \cdot) = U \times U$ mit Verknüpfung $(a, b) \cdot (c, d) := (a \cdot c, d \cdot b)$
- $X = G$
- $\varphi : A \times X \to X$, $\varphi((a, b), x) = a \cdot x \cdot b$

Dies ist ein Kandidat für eine Einweg-Operation: Das Problem

$$\text{gegeben } x, y \in X \quad \text{finde } a, b \in U \text{ mit } a \cdot x \cdot b = y$$

scheint allgemein schwierig zu sein.

Matrizen über Halbringen

Matrixmultiplikation

Für Matrizen $A = (a_{ij})$ und $B = (b_{ij})$ über einen Halbring R definiere $A \cdot B = (c_{ij})$ wie üblich:

$$c_{ij} = \sum_{k=1}^{n} a_{ik} \cdot b_{kj}.$$

Dann ist $\mathrm{Mat}_{n \times n}(R)$ wieder ein Halbring.

- R mit Eins einfach $\Rightarrow$ $\mathrm{Mat}_{n \times n}(R)$ einfach
- Tools wie Eigenwerte, Diagonalisierung usw. sind nicht verfügbar

Eine zweiseitige Operation mit Halbringen

Sei R ein endlicher einfacher Halbring und $(Z, \cdot) \subseteq (R, \cdot)$ ein kommutativer Unterhalbring. Wähle $B_1, B_2 \in \mathrm{Mat}_{n \times n}(R)$.

- $A = Z[B_1] \times Z[B_2]$ (kommutativ)
- $X = \mathrm{Mat}_{n \times n}(R)$
- $\varphi : A \times X \to X$, $\varphi((p(B_1), q(B_2)), C) = p(B_1) \cdot C \cdot q(B_2)$

Bemerkungen

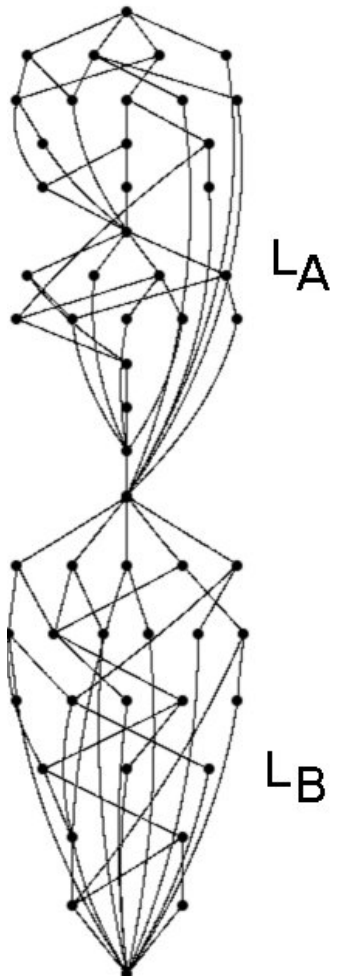
- offenbar keine adhoc- oder Lineare-Algebra-Attacken
- R einfach $\Rightarrow$ keine Pohlig-Hellman-Attacken auf kleinere Instanzen möglich
- variiere Größen $|R|$ und n je nach Hardware-Ressourcen

Eine weitere zweiseitige Operation

Seien L_A, L_B Verbände und sei L der zusammengesetzte Verband $\begin{smallmatrix} L_A \\ \cdot \\ L_B \end{smallmatrix}$.

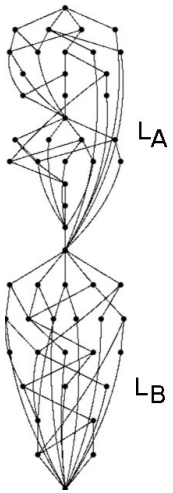
Betrachte den einfachen Halbring $R = \mathrm{End}(L, \vee)$.

- $(A, \cdot) = R \times R$ mit Verknüpfung $(f, g) \cdot (h, k) := (f \circ h, k \circ g)$
- $X = R$
- $\varphi : A \times X \to X$, $\varphi((f, g), x) = f \circ x \circ g$



Eine weitere zweiseitige Operation (2)

Seien R_A bzw. R_B alle Endomorphismen von L, die L_B bzw. L_A unverändert lassen. Dann gilt $f \circ g = g \circ f$ für alle $f \in R_A$, $g \in R_B$.



Protokoll

Alice	öffentlich	Bob
	wähle $x \in X$	
wähle $f_1, f_2 \in R_A$	$f_1 \circ x \circ f_2 \in X$	
	$g_1 \circ x \circ g_2 \in X$	wähle $g_1, g_2 \in R_B$
$f_1 \circ g_1 \circ x \circ g_2 \circ f_2$		$g_1 \circ f_1 \circ x \circ f_2 \circ g_2$

Zusammenfassung

- zahlreiche **einfache Halbringe** in vielen Größen sind konstruierbar
- **Einweg-Operationen** bieten eine natürliche Rahmenstruktur, um DL-basierte Kryptosysteme zu verallgemeinern
- effiziente zweiseitige **Einweg-Operationen mit einfachen Halbringen** sind möglich
  weitere Untersuchungen notwendig

- J.M. Couveignes, *Hard Homogeneous Spaces*, Preprint, 15 pages, eprint.iacr.org/2006/291 (2006).
- K.H. Ko, S.J. Lee, J.H. Cheon, J.W. Han, J. Kang, C. Park, *New public-key cryptosystem using braid groups*, CRYPTO 2000, Lecture Notes in Comput. Sci. **1880** (2000), 166–183.
- G. Maze, C. Monico, J. Rosenthal, *Public Key Cryptography based on Semigroup Actions*, Adv. in Math. of Communications. **1** (2007), no. 4, 489–507.
- J. Zumbrägel, *Classification of finite congruence-simple semirings with zero*, Preprint, 16 pages, arXiv:math.RA/0702416 (2007).