Einfache Halbringe und ihre kryptographische Anwendung

Jens Zumbrägel · jzumbr@math.uzh.ch

Institut für Mathematik, Universität Zürich
Winterthurerstr. 190, CH - 8057 Zürich

Halbringe sind verallgemeinerte Ringe, in denen negative Elemente nicht zu existieren brauchen. Formal ist ein *Halbring* eine Struktur $(R, +, \cdot)$ bestehend aus einer Menge R und zwei Verknüpfungen $+$, $\cdot$, so dass $(R, +)$ eine kommutative Halbgruppe ist, $(R, \cdot)$ eine Halbgruppe, und dass beide Distributivgesetze gelten. Wir nehmen weiterhin die Existenz eines Elements $0 \in R$ an, welches sich neutral in $(R, +)$ und absorbierend in $(R, \cdot)$ verhält.

Halbringe sind beispielsweise die natürlichen Zahlen $(\mathbb{N} = \{0, 1, 2, 3, \dots\}, +, \cdot)$, der boolesche Halbring $(\{0, 1\}, \texttt{or}, \texttt{and})$, und der Endomorphismenhalbring $(\mathrm{End}(M), +, \circ)$ eines kommutativen Monoids $(M, +, 0)$. Die Halbringstruktur ist im Wesentlichen die schwächste, für die noch eine sinnvolle Matrixmultiplikation definiert werden kann.

Endliche Halbringe und Matrizen über diesen können in der Public-Key Kryptographie angewendet werden, um Operationen von kommutativen Halbgruppen auf Mengen zu konstruieren, die effizient berechenbar sind, jedoch im Allgemeinen schwierig zu invertierende Bahnenabbildungen besitzen. Solche Operationen bieten einen natürlichen Rahmen, um DL-basierte Kryptosysteme zu verallgemeinern, bei denen die Halbgruppe $(\mathbb{Z}, \cdot)$ durch Exponentiation auf einer zyklischen Gruppe operiert, siehe [MMR05].

Wenn man nun Operationen unter Verwendung von Halbringen konstruiert, welche sich homomorph auf kleinere Halbringe abbilden lassen, dann ist das Kryptosystem anfällig für Angriffe, die vom verkleinerten homomorphen Bild ausgehen. Diese Angriffe sind vergleichbar mit dem Pohlig-Hellman-Algorithmus zur Berechnung diskreter Logarithmen in zyklischen Gruppen von Nichtprimzahl-Ordnung. Daher ist es für kryptographische Zwecke wichtig, dass der Halbring *einfach* d. h. kongruenz-frei ist, da in diesem Fall kein kleineres homomorphes Bild existiert.

Die vollständige Klassifikation von endlichen einfachen Halbringen in [Zu07] (siehe auch [Mo04]) liefert zahlreiche Beispiele, nämlich gewisse Teilhalbringe von Endomorphismenhalbringen endlicher kommutativer idempotenter Monoide, welche bijektiv den endlichen Verbänden entsprechen. Es ist dadurch mit wenig Computer-Ressourcen möglich, auch sehr große Halbringe und deren Verknüpfungen zu erzeugen. Diese Vielfalt von einfachen Endomorphismenhalbringen bieten zahlreiche Möglichkeiten, Halbgruppenoperationen zu konstruieren, die unter anderem aufgrund der Effizienz für Public-Key Kryptographie potenziell interessant sind. Die Konstruktion von kryptographisch geeigneten Operationen ist Gegenstand meiner aktuellen Forschung.

Literatur

[Mo04] Chris Monico. On finite congruence-simple semirings. *J. Algebra* 271 (2004), no. 2, 846–854 arXiv:math.RA/0205083, Mai 2002.

[MMR05] Gérard Maze, Chris Monico, Joachim Rosenthal. Public Key Cryptography based on Semigroup Actions. arXiv:cs.CR/0501017v2, Januar 2005, erscheint in *Adv. Math. Commun.*.

[Zu07] Jens Zumbrägel. Classification of finite congruence-simple semirings with zero. arXiv:math.RA/0702416, Feburar 2007.