Datenstrukturen zum parallelen Potenzieren in endlichen Körpern

Michael Nöcker

Endliche Körper $\mathbb{F}_{q^n}$, insbesondere die mit Charakteristik 2, spielen eine wichtige Rolle bei vielen heutigen Anwendungen, so auch in der modernen Kryptographie. Die Frage, wie man endliche Körper abbildet, ist eine der Schlüsselfragen einer erfolgreichen Implementierung.

Die vorliegende Arbeit diskutiert diese Frage auf dem Hintergrund des parallelen Potenzierens. Potenzieren ist die Grundoperation hinter einer ganzen Familie von asymmetrischen Kryptosystemen, die alle auf dem diskreten Logarithmus aufbauen. Der Ausgangspunkt ist ein erweitertes Modell für Additionsketten. Dieses Modell beinhaltet zwei verschiedene Schritttypen. Ein jedem dieser Schritte zugeordnetes Gewicht berücksichtigt die grundlegenden arithmetischen Eigenschaften bezüglich einer gewählten Basisdarstellung von $\mathbb{F}_{q^n}$. Wir entwickeln einen neuen Algorithmus für paralleles Potenzieren und beweisen in diesem Modell eine neue untere Schranke für das gestellte Problem. Beide Ansätze zeigen, dass das Gewicht der Schlüssel ist, um die mögliche Verbesserung einer Basisdarstellung durch paralleles Rechnen vorab abzuschätzen.

Wir diskutieren verschiedene Versionen der beiden gebräuchlichsten Basen für $\mathbb{F}_{q^n}$: Polynom- und Normalbasen. Insbesondere entwickeln wir Algorithmen für normale Elemente, die durch Gaußperioden erzeugt sind. Ein neuer Algorithmus verbindet schnelle Polynommultiplikation und die kostenlose Berechnung des Frobeniusautomorphismus für Primpotenz-Gaußperioden. Dieser Ansatz verallgemeinert einen Algorithmus für prime Gaußperioden. Ein weiteres neues Werkzeug, genannt zerlegbare Gaußperioden, wird genutzt, um dieses Ergebnis auf alle endlichen Körper zu verallgemeinern, in denen normale allgemeine Gaußperioden existieren. Eine Normalbasendarstellung, die auf solchen Gaußperioden aufbaut, erweist sich als am besten geeignet für massiv-paralleles Potenzieren in endlichen Körpern.

Alle wichtigen Algorithmen wurden implementiert und experimentell verglichen. Ein neuer skalierbarer Algorithmus für paralleles Potenzieren fasst alle behandelten Ideen zusammen. Er zeigt, wie schnelle Polynommultiplikation und massives paralleles Rechnen zusammenarbeiten können, falls normale Gaußperioden die Basisdarstellung sind.