Halbierungen von Divisorklassen in der Kryptographie

Peter Birkner

Department of Mathematics and Computer Science
Eindhoven University of Technology

p.birkner@tue.nl

Abstract: In diesem Artikel geben wir einen Überblick über Halbierungen und wie sie in der Kryptographie von Nutzen sein können. Wir stellen Halbierungen von Punkten auf Elliptischen Kurven und von Divisorklassen von Hyperelliptischen Kurven vom Geschlecht zwei und drei vor und zeigen, wie diese eine effiziente Skalarmultiplikation ermöglichen und damit die Geschwindigkeit von Kryptosystemen erhöhen können.

1 Einleitung

In der Public-Key-Kryptographie spielen zwei mathematische Probleme eine wichtige Rolle, nämlich das Faktorisieren großer Zahlen (z. B. bei RSA), und das Berechnen des diskreten Logarithmus (DL) in geeigneten Gruppen. Damit die Berechnung des DL-Problems in der Kryptographie genutzt werden kann, müssen wir auf zwei Dinge achten: Wir brauchen erstens eine schnelle Arithmetik in der Gruppe, damit effizient ver- und entschlüsselt, d. h. „potenziert“ werden kann, und zweitens muss das Diskrete-Logarithmus-Problem (DLP) in der Gruppe „schwer“ zu lösen sein. Schwer bedeutet in diesem Zusammenhang, dass es keinen Polynomialzeit-Algorithmus gibt, mit dem man das DLP in der betrachteten Gruppe berechnen kann.

Wenn wir von Arithmetik in der DLP-Gruppe sprechen, dann meinen wir vor allem die Funktionen zur Berechnung von skalaren Vielfachen von Gruppenelementen, d. h. zu einem gegebenen Gruppenelement P und einer natürlichen Zahl n wollen wir das n-fache $[n]P = P + \ldots + P$ berechnen. Dies wird fast immer mit Varianten von Double-and-Add- oder Square-and-Multiply-Algorithmen gemacht. Dabei wird die Zahl n als Bitstring dargestellt und je nach Bitwert wird der Zwischenwert einfach nur verdoppelt oder verdoppelt und zusätzlich noch zu P addiert. Wir werden zeigen, dass die Berechnung von skalaren Vielfachen auch mit Halbierungen möglich ist. Das Ziel dabei ist es natürlich, die Skalarmultiplikation so schnell wie möglich zu machen. Ist eine Halbierung schneller als eine Verdopplung, kann ein Halve-and-Add-Algorithmus den Wert $[n]P$ schneller berechnen als der entsprechende Double-and-Add-Algorithmus.

Im Folgenden werden wir uns u. a. anschauen, wie man Halbierungen statt Verdopplungen einsetzen kann um skalare Vielfache zu berechnen (siehe auch [Sch00]). Dabei muss der Skalar n umgewandelt werden, und zwar muss er von der Form $n = \sum_{i=0}^{n-1} 2^i$ in die Form

$n = \sum_{j=0}^{n-1} 1/2^j$ umgewandelt werden.

In der Kryptographie sind besonders die Punktgruppen von Elliptischen Kurven und die Divisorklassengruppen von Hyperelliptischen Kurven von Interesse. Wir werden daher einen Überblick über Punkthalbierungen auf Elliptischen Kurven und Divisorklassenhalbierungen auf Hyperelliptischen Kurven vom Geschlecht zwei und drei geben.

2 Halbierungen

Was ist nun genau eine Halbierung? Wir geben zunächst eine allgemeine Erklärung. Sei G eine Gruppe und $P \in G$. Wir suchen nun eine weiteres Gruppenelement Q, so dass $P = [2]Q$ oder informal geschrieben: $[1/2]P = Q$. Das Halbieren ist also eine Art Umkehrabbildung des Verdoppelns.

Halbierungen können Kryptosysteme schneller machen, wenn die Halbierung schneller als die Verdopplung ist. In diesem Fall können skalare Vielfache (von Punkten auf Elliptischen Kurven oder Vielfache von Divisorklassen) schneller berechnet werden, und damit wird der Verschlüsslungs- und Entschlüsslungsvorgang beschleunigt. Skalare Vielfache werden fast ausschließlich mit Double-and-Add-Algorithmen berechnet, wobei der Skalar n als Bitstring geschrieben wird und bei der Berechnung je nach Bit verdoppelt oder verdoppelt und addiert wird. Der Skalar hat also die Form $n = \sum_{i=0}^{k-1} 2^i$. Bei der Halbierung wird der Skalar in der Form $n = \sum_{j=0}^{k-1} 1/2^j$ geschrieben, so dass $\sum_{i=0}^{k-1} [n_i 2^i]P = \sum_{j=0}^{k-1} [m_j 1/2^j]P$ gilt, und je nach gesetztem Bit wird eine Halbierung bzw. eine Halbierungen und eine Addition ausgeführt.

Die Betrachtung von Halbierungen in Divisorklassengruppen hat einen weiteren Grund: In den letzten Jahren konkurrieren die Hyperelliptischen mit den Elliptischen Kurven immer mehr und daher versucht man die Konzepte von Elliptischen Kurven ebenfalls auf Hyperelliptische zu übertragen. Da es Punkthalbierungen für Elliptische Kurven (EC) schon gibt und diese gewisse Vorteile bringen, macht es Sinn, ebenfalls Halbierungen von Divisorklassen auf Hyperelliptischen Kurven zu untersuchen.

Bisher gibt es nur sehr wenige Ergebnisse zu diesem Konzept. Kitamura et al. [KKT05] betrachten Divisorklassenhalbierungen auf Hyperelliptischen Kurven vom Geschlecht zwei über binären Körpern. Ihre Formeln decken eine sehr große Klasse von Kurven ab, aber die Geschwindigkeit der Halbierung reicht bei Weitem nicht an die der Verdopplung heran.

Wir haben eine spezielle Klasse von Geschlecht-2-Kurven untersucht und effiziente Halbierungsformeln gefunden, die nur unwesentlich langsamer als die Verdopplungen sind [Bir06]. Dabei haben wir uns ebenfalls auf Charakteristik 2 konzentriert, da dies eine Implementierung in Hardware ermöglicht und ausserdem sehr effiziente Formeln erlaubt. Zur Zeit führen Verdopplungen noch zu einer schnelleren Skalarmultiplikation als Halbierungen, da die zur Zeit besten Verdopplungsformeln minimal schneller sind als die Halbierungen. Dies ist aber z. B. im Geschlecht-3-Fall schon anders (siehe Abschnitt 4.2). Wir haben die Halbierungen im Geschlecht-2-Fall betrachtet, um zum einen zu zeigen, dass in Zukunft Halve-and-Add-Algorithmen die Double-and-Add-Algorithmen ersetzen können,

und zum anderen haben wir das für die betrachtete Klasse von Kurven bisher einzige Ergebnis von Kitamura et al. [KKT05] um einen Faktor von ungefähr 2 verbessert.

Für die Arithmetik in der Divisorklassengruppe wird Cantors Algorithmus verwendet. Dieser kombiniert zwei Divisorklassen im ersten Schritt und reduziert sie im zweiten Schritt so, dass die resultierende Divisorklasse wieder in Mumford-Darstellung (siehe [ACD+05, Theorem 4.145]) gegeben ist. Bei der Verdopplung einer Divisorklasse wird dieser Algorithmus ebenfalls eingesetzt. Das Verfahren von Cantor funktioniert allgemein für Kurven jeden Geschlechts und über jedem Grundkörper. Für Halbierungen existiert solch ein Algorithmus jedoch nicht. Daher müssen für einzelne Situationen (z. B. Geschlecht zwei oder Geschlecht drei über einem binären Körper) explizite Formeln zur Halbierung entwickelt werden. Genau das haben wir gemacht. Für den Geschlecht-2-Fall haben wir die Verdopplungsformeln von Lange [Lan05] genommen und sie „umgekehrt“ d. h. die Formeln werden in umgekehrten Reihenfolge berechnet, um aus einer (schon verdoppelten) Divisorklasse wieder die ursprüngliche (halbierte) Divisorklasse zu erhalten.

Wir werden im Folgenden kurz Halbierungen auf Elliptischen Kurven und auf speziellen Kurven vom Geschlecht zwei vorstellen. Schließlich geben wir einen kurzen Ausblick auf neueste Ergebnisse für Kurven vom Geschlecht drei.

3 Punkthalbierungen auf elliptischen Kurven

In diesem Abschnitt werden wir die Halbierung von Punkten auf Elliptischen Kurven besprechen. Wir verweisen dabei auf den Artikel von Knudsen [Knu99]. Für Details über Elliptische Kurven empfehlen wir Bücher, wie z. B. [Sil86] oder [ACD+05].

Vereinfacht gesagt ist eine Elliptische Kurve über einem Körper k die Menge aller Lösungen einer algebraischen Gleichung der Form

$$E : y^2 + h(x)y = f(x),$$

wobei $h \in k[X]$ ist und das Polynom $f \in k[X]$ den Grad drei hat und normiert ist. Die Lösungen $P = (a, b)$ der Gleichung heißen affine Punkte der Elliptischen Kurve, solche mit $a, b \in k$ heißen k-rational. Außerdem gibt es noch einen weiteren Punkt, den Punkt im Unendlichen, der auch k-rational ist. Die Menge der Punkte besitzt eine Gruppenstruktur, so dass man das DLP in dieser Gruppe betrachten kann. Für kryptographische Anwendungen betrachtet man den Fall, dass k ein endlicher Körper $\mathbb{F}_q$ ist, und beschränkt sich auf die endlich vielen $\mathbb{F}_q$-rationalen Punkte.

Um in einem Kryptosystem, das auf einer Elliptischen Kurve basiert, zu verschlüsseln oder zu entschüsseln, müssen wir skalare Vielfache von Punkten berechnen (eigentlich Potenzen von Punkten, aber die Punktgruppe wird additiv geschrieben). Wir benötigen also eine Arithmetik in dieser Gruppe. Für das Gruppengesetz gibt es Additionsformeln (siehe z. B. [Lan05]), die aus zwei Punkten einer Kurve einen neuen Punkt berechnen. Dies ist dann eine Addition auf der Kurve bzw. in der Punktgruppe. Eine Verdopplung eines Punktes P auf der Kurve ist eine Addition von P mit sich selbst, also $P + P$ oder auch $[2]P$.

Bei der Halbierung wollen wir zu einem gegebenen Punkt P einen weiteren Punkt Q finden, so dass $P = [2]Q$ bzw. $[1/2]P = Q$ gilt.

Um einen Eindruck von der Komplexität des Verdoppelns und Halbierens zu bekommen, geben wir hier die Laufzeiten für Punkthalbierung und -verdopplung (in affinen Koordinaten) für eine Elliptische Kurve der Form $y^2 + xy = x^3 + ax^2 + b$ über dem binären Körper $\mathbb{F}_{2^n}$ an.

Verdopplung	Halbierung
1I + 2M + 1S [ACD+05, Seite 297]	2M + 1SR + 1HT + 1TR [Knu99, Sch00]

Die Operationen im vorliegenden binären Körper sind dabei wie folgt abgekürzt: Inversion (I), Multiplikation (M), Wurzelextraktion (SR), Quadrierung (S), Half-Trace (HT) und Trace (TR).

4 Halbierung von Divisorklassen

Im vorigen Abschnitt haben wir Punkthalbierungen auf Elliptischen Kurven betrachtet. Nun wollen wir dieses Konzept verallgemeinern und ebenfalls auf Kurven höheren Geschlechts anwenden. Da die Punkte auf Hyperelliptischen Kurven keine Gruppenstruktur wie im elliptischen Fall besitzen, geht man zum Konzept der Divisoren über. Ein Divisor ist eine formale Summe von Punkten auf der Kurve. Man betrachtet nun spezielle Divisoren, sogenannte Hauptdivisoren und Divisoren vom Grad Null (für Details siehe [ACD+05]). Man führt nun eine Äquivalenzrelation auf der Menge der Divisoren vom Grad Null ein und sagt, dass zwei solche Divisoren äquivalent sind, wenn ihre Differenz ein Hauptdivisor ist. Dadurch entstehen Divisorklassen bzw. Äquivalenzklassen, deren Repräsentanten eine Gruppenstruktur bilden. Dies ist dann das analoge Konzept zur Punktgruppe bei elliptischen Kurven. In dieser sogenannten Divisorklassengruppe betrachtet man nun ebenfalls das DLP und erreicht dabei die gleiche Sicherheit wie im elliptischen Fall, aber mit einem kleineren Grundkörper. Nachteil ist, dass die Arithmetik in der Divisorklasse komplexer ist. Im hyperelliptischen Fall kann jede Divisorklasse in der Form $\overline{D} = [u, v]$ geschrieben werden, wobei u und v zwei Polynome sind, deren Grade kleiner oder gleich dem Geschlecht der Kurve sind. Diese Darstellung heißt Mumford-Darstellung und die Arithmetik in der Divisorklassengruppe basiert auf dieser Form.

4.1 Der Geschlecht-2-Fall

Wir betrachten nun Hyperelliptische Kurven vom Geschlecht 2, welche über Körpern der Charakteristik 2 definiert sind. Für diese Klasse von Kurven existieren bereits effiziente Additions- und Verdopplungsformeln (siehe [Lan05]). Damit können skalare Vielfache von Divisorklassen mit Hilfe von Double-and-Add-Algorithmen berechnet werden. Kitamura et al. [KKT05] haben sich mit der Halbierung von Divisorklassen beschäftigt und einen Algorithmus vorgestellt, der eine sehr große Klasse von Kurven abdeckt, aber nicht

sehr effizient ist, d. h. die Komplexität ist viel größer als bei der Verdopplungsfunktion und daher konnte die Geschwindigkeit der Skalarmultiplikation mit Halbierungen nicht gesteigert werden. Aber dennoch war es ein erster Schritt, Hyperelliptische Kurven ebenfalls mit einer Halbierungsfunktion auszustatten. Birkner [Bir06] hat für eine spezielle Klasse von Kurven, die besonders für Kryptosysteme interessant sind, eine Halbierungsfunktion vorgestellt, die nahe an die Geschwindigkeit des Verdoppelns herankommt. Dies zeigt, dass vielleicht in der Zukunft die Halbierungen die Verdopplungen ersetzen könnten und damit eine schnelle Skalarmultiplikation erreicht werden kann.

Hier die Resultate: Für eine hyperelliptische Kurve vom Geschlecht 2 über einem endlichen Körper $\mathbb{F}_{2^d}$ (d ungerade) der Form

$$C : y^2 + xy = x^5 + f_3x^3 + f_2x^2 + f_0$$

kann eine Halbierung einer Divisorklasse mit 1I + 8M + 5SR + 2S + 1 HT + 1TR Operationen berechnet werden. Zum Vergleich benötigen Kitamura et al. fast doppelt so viele Multiplikationen im Grundkörper (und dies sind zusammen mit den Inversionen die entscheidenen Operationen). Die bisher besten Verdopplungsformeln von Lange [Lan05] benötigen im Wesentlichen 1I + 6M für eine Kurve der gleichen Klasse.

Hat man eine Normalbasisdarstellung des Grundkörpers, können Quadrierungen und Wurzelextraktionen durch das Verschieben von Bits erreicht werden. Damit nehmen diese Operationen, genauso wie Additionen, nur einen unwesentlichen Einfluss auf die Komplexität und können als "kostenlos" angesehen werden. Die Funktionen Half-Trace und Trace sind Summen von Quadraten im Grundkörper und fallen damit in die gleiche Gruppe von Operationen. Insgesamt bedeutet dies, dass die Komplexität der Algorithmen (fast) ausschließlich von der Zahl der Inversionen und Multiplikationen abhängt.

4.2 Der Geschlecht-3-Fall

Im Geschlecht-3-Fall sind bisher noch keine Halbierungsformeln veröffentlich worden, ein entsprechender Artikel ist gerade in Arbeit. Wir haben für eine spezielle Klasse von Kurven vom Geschlecht 3 (ebenfalls über einem binären Körper) eine vollständige Fallunterscheidung angefertigt, die alle Halbierungs- und Verdopplungsfälle beeinhaltet. Manche Fälle treten mit einer extrem niedrigen Wahrscheinlichkeit auf, wir wollten aber dennoch eine vollständige Sammlung von Formeln angeben. Im Geschlecht-3-Fall konnten wir erreichen, dass die Halbierungen von Divisorklassen genauso schnell berechnet werden kann, wie die Verdopplung. Daher kann in diesem Fall ein Halve-and-Add-Algorithmus verwendet werden, um eine effiziente Skalarmultiplikation zu erreichen.

Im Geschlecht-3-Fall haben wir die expliziten Halbierungsformeln ähnlich wie im Geschlecht-2-Fall gefunden. Wir haben die Verdoppelungsformeln für den am häufigsten auftretenden Fall gewählt und deren "Reihenfolge umgekehrt", um eine Halbierung zu erhalten. Da für die weniger häufig auftretenden Fälle noch keine Verdopplungsformeln bekannt waren, haben wir diese ausgearbeitet und ebenfalls in umgekehrter Reihenfolge angewendet, um nun im jedem möglichen Fall, der bei einer Divisorklasse einer Gechlecht-3-Kurve

über einem binären Körper auftreten kann, eine Halbierung und Verdopplung berechnen zu können. Die Komplexität für die Halbierung im Fall mit der größten Wahrscheinlichkeit ist 1I + 10M + 2S + 9SR.

5 Fazit

Wir haben einen Überblick gegeben über die Möglichkeiten, die Punkthalbierungen bei Elliptischen Kurven und Halbierungen von Divisorklassen bei Hyperelliptischen Kurven bieten, um eine effziente Skalarmultiplikation für DLP-basierte Kryptosysteme zu ermöglichen. Weiterhin haben wir explizte Halbierungsformeln für eine spezielle Klasse von Hyperelliptischen Kurven vom Geschlecht 2 und 3 über binären Körpern entwickelt. Im Geschlecht-2-Fall sind die Verdopplungen noch minimal schneller, im Geschlecht-3-Fall sind Halbierungen und Verdopplungen gleich schnell, so dass Double-and-Add-Algorithmen auch durch Halve-and-Add-Algorithmen ersetzt werden können. Die expliziten Halbierungsformeln für Geschlecht-2-Kurven sind fast um einen Faktor 2 schneller als das einzige bisher veröffentlichte Resultat.

Danksagung

Ich möchte mich bei Tanja Lange für die wertvollen Kommentare und bei Nina Brandstätter für ihre Hilfe bei der Erstellung dieses Artikels bedanken.

Literatur

[ACD+05] Roberto M. Avanzi, Henri Cohen, Christophe Doche, Gerhard Frey, Tanja Lange, Kim Nguyen and Frederik Vercauteren: Handbook of Elliptic and Hyperelliptic Curve Cryptography. Chapman & Hall/CRC, 2005.

[Bir06] Peter Birkner: Efficient Divisor Class Halving on Genus Two Curves. To appear in: Proceedings of SAC 2006, LNCS vol. 4356, Springer-Verlag.

[Knu99] Erik Woodward Knudsen: Elliptic Scalar Multiplication Using Point Halving. In: ASIACRYPT '99, LNCS vol. 1716, pp. 135–149, Springer-Verlag.

[KKT05] Izuru Kitamura, Masanobu Katagi and Tsuyoshi Takagi: A Complete Divisor Class Halving Algorithm for Hyperelliptic Curve Cryptosystems of Genus Two. In: ACISP 2005, LNCS vol. 3574, pp. 146–157, Springer-Verlag.

[Lan05] Tanja Lange: Formulae for Arithmetic on Genus 2 Hyperelliptic Curves. Applicable Algebra in Engineering, Communication and Computing, 15(5):295–328, 2005.

[Sch00] Richard Schroeppel: Elliptic Curve Point Halving Wins Big. 2nd Midwest Arithmetical Geometry in Cryptography Workshop, Urbana, Illinois, November 2000.

[Sil86] Joseph Silverman: The Arithmetic of Elliptic Curves, Springer-Verlag, 1986.