

Springer-Verlag Berlin Heidelberg GmbH

Annette Werner

Elliptische Kurven in der Kryptographie



Springer

Dr. Annette Werner
Westfälische Wilhelms-Universität
Fachbereich Mathematik und Informatik
Einsteinstr. 62
48149 Münster
Deutschland
e-mail: werner@math.uni-muenster.de

Mathematics Subject Classification (2000): 94A60 (11G20, 14G50)

Die Deutsche Bibliothek – CIP-Einheitsaufnahme

Werner, Annette:

Elliptische Kurven in der Kryptographie / Annette Werner. - Berlin; Heidelberg; New York; Barcelona; Hongkong; London; Mailand; Paris; Tokio: Springer, 2002
(Springer-Lehrbuch)

ISBN 978-3-540-42518-2 ISBN 978-3-642-56351-5 (eBook)

DOI 10.1007/978-3-642-56351-5

Dieses Werk ist urheberrechtlich geschützt. Die dadurch begründeten Rechte, insbesondere die der Übersetzung, des Nachdrucks, des Vortrags, der Entnahme von Abbildungen und Tabellen, der Funksendung, der Mikroverfilmung oder der Vervielfältigung auf anderen Wegen und der Speicherung in Datenverarbeitungsanlagen, bleiben, auch bei nur auszugsweiser Verwertung, vorbehalten. Eine Vervielfältigung dieses Werkes oder von Teilen dieses Werkes ist auch im Einzelfall nur in den Grenzen der gesetzlichen Bestimmungen des Urheberrechtsgesetzes der Bundesrepublik Deutschland vom 9. September 1965 in der jeweils geltenden Fassung zulässig. Sie ist grundsätzlich vergütungspflichtig. Zuwiderhandlungen unterliegen den Strafbestimmungen des Urheberrechtsgesetzes.

<http://www.springer.de>

© Springer-Verlag Berlin Heidelberg 2002

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, daß solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften.

Satz: Datenerstellung durch die Autorin unter Verwendung eines Springer \LaTeX -Makropakets
Einbandgestaltung: *design & production* GmbH, Heidelberg

Gedruckt auf säurefreiem Papier SPIN: 10848997 44/3142ck 5 4 3 2 1 0

Für Marcus

Vorwort

Die Anwendung elliptischer Kurven in der Kryptographie ist ein Beispiel für die verblüffende Nützlichkeit der reinen Mathematik. Elliptische Kurven sind geometrische Objekte, die seit langem intensiv aus theoretischem Interesse studiert werden. Seit etwa 1985 finden sie Anwendung in kryptographischen Verfahren, mit denen z.B. geheime Botschaften übermittelt oder digitale Unterschriften geleistet werden können.

Diese Einführung soll Leser mit Grundkenntnissen in Algebra und Linearer Algebra möglichst zügig mit den mathematischen Grundlagen solcher Verfahren vertraut machen. Daher werden elliptische Kurven auf elementarem Niveau behandelt, auch wenn dies gelegentlich dazu führt, daß ein Resultat nur zitiert, aber nicht bewiesen werden kann. Um den Text noch zugänglicher zu machen, sind in einem Anhang die benötigten Begriffe und Resultate aus Algebra, Zahlentheorie und Komplexitätstheorie kurz zusammengestellt.

Dieses Buch ist aus zwei Vorlesungen hervorgegangen, die ich im Wintersemester 2000/2001 und im Sommersemester 2001 an der Westfälischen Wilhelms-Universität Münster gehalten habe. Ich bedanke mich herzlich bei meinen Hörerinnen und Hörern für ihr lebendiges Interesse. Mein Dank gilt ebenfalls Claudia Lücke und Gabi Weckermann für ihre Unterstützung beim Erstellen des LaTeX-Files sowie Christopher Deninger für einige hilfreiche Hinweise.

Münster, im November 2001

Annette Werner

Inhaltsverzeichnis

1. Public-Key-Kryptographie	1
1.1 RSA	2
1.2 Diskreter Logarithmus	4
1.2.1 Diffie-Hellman-Schlüsselaustausch	5
1.2.2 ElGamal-Verschlüsselung	6
1.2.3 ElGamal-Signatur	7
1.3 Geeignete Gruppen	8
2. Elliptische Kurven	11
2.1 Affine Kurven	12
2.2 Projektive Kurven	15
2.3 Elliptische Kurven	22
3. Elliptische Kurven über endlichen Körpern	55
3.1 Der Frobenius	55
3.2 Punkte zählen	57
3.3 Der Schoof-Algorithmus	63
3.4 Supersinguläre elliptische Kurven	66
4. Das Problem des diskreten Logarithmus für elliptische Kurven	75
4.1 Allgemeine Methoden	76
4.1.1 Enumerationsverfahren	76

4.1.2	Babystep-Giantstep-Algorithmus (BSGS)	76
4.1.3	Pohlig-Hellman-Verfahren	77
4.1.4	Pollard- ρ -Methode	79
4.1.5	Pollard- λ -Methode	82
4.2	Spezielle Methoden	82
4.2.1	Der MOV-Algorithmus	83
4.2.2	Anomale Kurven oder SSSA-Algorithmus	89
5.	Praktische Konsequenzen	97
5.1	Geeignete elliptische Kurven	97
5.2	Vergleich mit anderen Public Key-Verfahren	98
5.2.1	RSA	98
5.2.2	DL-Verfahren in \mathbb{F}_q^\times	102
5.3	ECDSA	104
6.	Anhang: Mathematische Grundlagen	111
6.1	Ganze Zahlen	111
6.2	Kongruenzen	114
6.3	Gruppen	117
6.4	Ringe und Körper	122
6.5	Polynome	125
6.6	Endliche Körper	128
6.7	Algebraisch abgeschlossene Körper	130
6.8	Einheitswurzeln	131
6.9	p -adische Zahlen	131
6.10	Komplexität	134
	Literaturverzeichnis	137
	Sachverzeichnis	141