

Rene Algesheimer

Elliptische Kurven als alternatives Public Key-Verfahren im Homebanking-Standard HBCI

Diplomarbeit

Bibliografische Information der Deutschen Nationalbibliothek:

Bibliografische Information der Deutschen Nationalbibliothek: Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de/> abrufbar.

Dieses Werk sowie alle darin enthaltenen einzelnen Beiträge und Abbildungen sind urheberrechtlich geschützt. Jede Verwertung, die nicht ausdrücklich vom Urheberrechtsschutz zugelassen ist, bedarf der vorherigen Zustimmung des Verlags. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen, Auswertungen durch Datenbanken und für die Einspeicherung und Verarbeitung in elektronische Systeme. Alle Rechte, auch die des auszugsweisen Nachdrucks, der fotomechanischen Wiedergabe (einschließlich Mikrokopie) sowie der Auswertung durch Datenbanken oder ähnliche Einrichtungen, vorbehalten.

Copyright © 2000 Diplomica Verlag GmbH
ISBN: 9783832425548

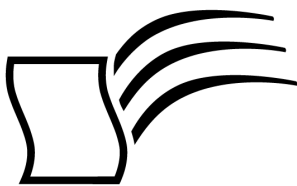
Rene Algesheimer

Elliptische Kurven als alternatives Public Key-Verfahren im Homebanking-Standard HBCI

Rene Algesheimer

Elliptische Kurven als alternatives Public Key-Verfahren im Homebanking-Standart HBCI

Diplomarbeit
an der Johannes Gutenberg-Universität Mainz
Fachbereich Mathematik
Januar 2000 Abgabe



Diplomarbeiten Agentur

Dipl. Kfm. Dipl. Hdl. Björn Bedey
Dipl. Wi.-Ing. Martin Haschke
und Guido Meyer GbR

Hermannstal 119 k
22119 Hamburg

agentur@diplom.de
www.diplom.de

ID 2554

Algesheimer, Rene: Elliptische Kurven als alternatives Public Key-Verfahren im Homebanking-
Standart HBCI / Rene Algesheimer -
Hamburg: Diplomarbeiten Agentur, 2000
Zugl.: Mainz, Universität, Diplom, 2000

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 in der jeweils geltenden Fassung zulässig. Sie ist grundsätzlich vergütungspflichtig. Zuwiderhandlungen unterliegen den Strafbestimmungen des Urheberrechtes.

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.

Die Informationen in diesem Werk wurden mit Sorgfalt erarbeitet. Dennoch können Fehler nicht vollständig ausgeschlossen werden, und die Diplomarbeiten Agentur, die Autoren oder Übersetzer übernehmen keine juristische Verantwortung oder irgendeine Haftung für evtl. verbliebene fehlerhafte Angaben und deren Folgen.

Dipl. Kfm. Dipl. Hdl. Björn Bedey, Dipl. Wi.-Ing. Martin Haschke & Guido Meyer GbR
Diplomarbeiten Agentur, <http://www.diplom.de>, Hamburg 2000
Printed in Germany



Diplomarbeiten Agentur

Wissensquellen gewinnbringend nutzen

Qualität, Praxisrelevanz und Aktualität zeichnen unsere Studien aus. Wir bieten Ihnen im Auftrag unserer Autorinnen und Autoren Wirtschaftsstudien und wissenschaftliche Abschlussarbeiten – Dissertationen, Diplomarbeiten, Masterarbeiten, Staatsexamensarbeiten und Studienarbeiten zum Kauf. Sie wurden an deutschen Universitäten, Fachhochschulen, Akademien oder vergleichbaren Institutionen der Europäischen Union geschrieben. Der Notendurchschnitt liegt bei 1,5.

Wettbewerbsvorteile verschaffen – Vergleichen Sie den Preis unserer Studien mit den Honoraren externer Berater. Um dieses Wissen selbst zusammenzutragen, müssten Sie viel Zeit und Geld aufbringen.

<http://www.diplom.de> bietet Ihnen unser vollständiges Lieferprogramm mit mehreren tausend Studien im Internet. Neben dem Online-Katalog und der Online-Suchmaschine für Ihre Recherche steht Ihnen auch eine Online-Bestellfunktion zur Verfügung. Inhaltliche Zusammenfassungen und Inhaltsverzeichnisse zu jeder Studie sind im Internet einsehbar.

Individueller Service – Gerne senden wir Ihnen auch unseren Papierkatalog zu. Bitte fordern Sie Ihr individuelles Exemplar bei uns an. Für Fragen, Anregungen und individuelle Anfragen stehen wir Ihnen gerne zur Verfügung. Wir freuen uns auf eine gute Zusammenarbeit

Ihr Team der Diplomarbeiten Agentur

Dipl. Kfm. Dipl. Hdl. Björn Bedey —
Dipl. Wi.-Ing. Martin Haschke —
und Guido Meyer GbR —

Hermannstal 119 k —
22119 Hamburg —

Fon: 040 / 655 99 20 —
Fax: 040 / 655 99 222 —

agentur@diplom.de —
www.diplom.de —

Vorwort

Diese Arbeit beschreibt meine Forschungen am Fachbereich Mathematik der Johannes Gutenberg-Universität Mainz im Rahmen meiner Diplomprüfung. Ich hoffe, dass diese meine Arbeit zukünftigen Forschungen dient und HBCI als Sicherheitsstandard möglicherweise verbessert.

Besonderen Dank möchte ich den folgenden Personen für Ihre unerschöpfliche Unterstützung und Aufmunterung während meiner Arbeitsphase aussprechen.

An erster Stelle richtet sich mein Dank an *Prof. Dr. Gerd Hofmeister*, der mir durch sein „Seziermesser der Kritik“ auf eine stets lebenswerte Art half, die Sprachmelodie der Mathematik zu erfassen.

Weiterhin möchte ich Herrn *Prof. Dr. Albrecht Beutelspacher* herzlich danken, der mir trotz seines straffen Zeitplans die Möglichkeit gab, bei ihm und im Fach Kryptologie meine Diplomarbeit zu schreiben.

Für die Idee zu dieser Arbeit, für viele mathematische Gespräche und für noch mehr mühevollen Kleinarbeit gilt mein besonderer Dank Herrn *Detlef Hühnlein*, Secunet Security Networks AG Frankfurt. Auch Herrn Dr. *Johannes Merkle*, Secunet Security Networks AG Frankfurt, gilt mein Dank für seine haarstäubenden Skizzen zu den elliptischen Kurven.

Meiner ehemaligen Übungsleiterin Frau *Dr. Heike Neumann* ist es sicherlich zuzuschreiben, dass mein Interesse für die Kryptologie so entfacht wurde.

Begeistert schien keiner meiner Korrekturassistenten über den dicken Stapel Papier gewesen zu sein, der plötzlich vor Ihnen auf dem Tisch lag. Dennoch haben sie alle durchgehalten.

Ständige mathematische Ansprechpartnerin war Frau *Joy Müller*, IBM Cryptography Research Group Zürich. Sie hat sicherlich den härtesten Teil der Korrektur übernommen. Für ihre inhaltliche Korrektur und Finesse sei ein besonderer Dank ausgesprochen.

Hätte Exaktheit einen Namen, so würde sie bestimmt *Norman Hänsler* heißen. Ihm gilt mein Dank für seine hervorragend kleinliche Korrektur meines wissenschaftlichen Arbeitens, für sein großes Ohr in dieser Zeit und viele herzhaftes Lachen.

Für die Bereitschaft und Interesse, sich in fremdes Terrain zu wagen und meine Arbeit auf Rechtschreibung Korrektur zu lesen, richtet sich mein Dankeschön an *Julia Löhr* und meinen Daddy *Edgar Algesheimer*.

Mein letztes Dankeschön gebührt all jenen stillen Freunden, die sich so selten über mangelnde Zeit mit mir beklagten, meiner Familie für die Harmonie und Joy für den tiefen Sinn.

Mainz, den 1.1.2000

René Algesheimer

INHALTSVERZEICHNIS

Tabellenverzeichnis.....	IX
Abbildungsverzeichnis.....	X
Abkürzungsverzeichnis.....	XII
 <u>KAPITEL 1: VORBEMERKUNGEN</u>	 <u>1</u>
1.1 PROBLEMSTELLUNG UND ZIELSETZUNG.....	3
1.2 METHODIK UND VORGEHENSWEISE.....	4
 <u>KAPITEL 2: EINIGE GRUNDLAGEN</u>	 <u>7</u>
2.1 EINIGE ZAHLENTHEORETISCHE ASPEKTE.....	9
2.2 EINIGE KRYPTOGRAPHISCHE ASPEKTE.....	19
2.2.1 Terminologie.....	19
2.2.2 Einweg- und Hashfunktionen.....	25
2.2.3 Das Faktorisierungsproblem.....	28
2.2.4 Das Problem des diskreten Logarithmus.....	29
2.2.5 Zusammenfassung und Ausblick.....	32
2.3 KRYPTOGRAPHISCHE VERSCHLÜSSELUNGSSYSTEME.....	33
2.3.1 Anforderungen.....	33
2.3.2 Symmetrische Verschlüsselung mit dem DES.....	34
2.3.3 Asymmetrische Verschlüsselung.....	38
2.3.3.1 Der RSA.....	40
2.3.3.2 Das ElGamal-Verschlüsselungssystem.....	42
2.4 DIGITALE SIGNATUREN.....	45
2.4.1 Anforderungen.....	45
2.4.2 Der Digital Signature-Algorithm (DSA).....	47
2.5 AUTHENTIFIKATION MIT DEM MAC.....	50
2.6 CHIPKARTEN ALS SICHERHEITSMEDIUM.....	52
2.7 ZUSAMMENFASSUNG	55
 <u>KAPITEL 3: DEFINITION, ABGRENZUNG UND ENTWICKLUNG DES HOMEBANKING</u>	 <u>57</u>
3.1 BEGRIFFSBESTIMMUNG HOMEBANKING.....	59
3.2 DIE ENTWICKLUNG DES HOMEBANKING IN DEUTSCHLAND.....	62
3.3 ANFORDERUNGEN AN EINEN NEUEN HOMEBANKING-STANDARD.....	65
3.3.1 Anforderungen an die Sicherheit.....	65
3.3.2 Anforderungen an das Design.....	67
3.4 ZUSAMMENFASSUNG UND AUSBLICK.....	68

KAPITEL 4: HBCI – HOMEBANKING COMPUTER INTERFACE	69
4.1 DER FORMALE AUFBAU VON HBCI.....	71
4.1.1 Die Syntax.....	71
4.1.2 Der Aufbau einer HBCI-Nachricht.....	73
4.1.3 Erstellung und Empfang einer Nachricht.....	74
4.1.4 Der Dialog zwischen Kunde und Kreditinstitut.....	75
4.2 SICHERHEIT IN HBCI UND ÜBERPRÜFUNG DER ANFORDERUNGEN.....	78
4.2.1 Anforderungen an die Sicherheit.....	81
4.2.2 Anforderungen an das Design.....	90
4.3 ALTERNATIVEN ZU HBCI.....	94
4.4 ZUSAMMENFASSUNG UND AUSBLICK.....	98
KAPITEL 5: ELLIPTISCHE KURVEN IN DER KRYPTOLOGIE	99
5.1 EINFÜHRUNG IN DIE THEORIE DER ELLIPTISCHEN KURVEN.....	101
5.1.1 Kurven in der Ebene.....	101
5.1.2 Definition von elliptischen Kurven.....	104
5.1.3 Elliptische Kurven als Gruppen.....	110
5.1.4 Die Gruppenoperationen in der affinen Ebene.....	117
5.1.5 Elliptische Kurven über endlichen Körpern.....	120
5.1.6 Die Ordnung von $E(K, \oplus, \circ)$	122
5.1.7 Weil-Paarungen.....	130
5.2 ELLIPTISCHE KURVEN IN DER PUBLIC KEY-KRYPTOGRAPHIE.....	132
5.2.1 Das Diskrete Logarithmus-Problem für elliptische Kurven.....	132
5.2.2 Elliptische Kurven und Geheimtexte.....	133
5.2.3 Verschlüsselungsverfahren mit elliptischen Kurven.....	136
5.2.4 Signaturverfahren mit elliptischen Kurven.....	138
KAPITEL 6: ELLIPTISCHE KURVEN ALS SICHERHEITSBAUSTEIN IN HBCI	141
6.1 KRYPTOGRAPHISCH SCHWACHE ELLIPTISCHE KURVEN.....	143
6.1.1 Singuläre elliptische Kurven.....	144
6.1.2 Supersinguläre elliptische Kurven.....	146
6.1.3 Elliptische Kurven mit Spur 1 und Spur 2.....	146
6.1.4 Kritische elliptische Kurven.....	147
6.2 KRYPTOGRAPHISCH STARKE ELLIPTISCHE KURVEN.....	148
6.3 DIE SICHERHEIT VON EC-SYSTEMEN IM VERGLEICH ZUM RSA UND DSA.....	151
6.4 VORTEILE DER INTEGRATION DER EC-KRYPTOSYSTEME IN HBCI.....	158
6.5 ZUSAMMENFASSUNG.....	162
Literaturverzeichnis.....	163
Anhang A – Beispiel einer Einzelüberweisung in HBCI.....	175
Anhang B – Wer ist Alice, Bob und Mallory?.....	178
Erklärung zur Diplomarbeit.....	179

TABELLENVERZEICHNIS

<u>KAPITEL 2: EINIGE MATHEMATISCHE GRUNDLAGEN</u>	<u>7</u>
Tabelle 2-1: Das R-Schema.....	12
Tabelle 2-2: Das P-Q-Schema.....	13
Tabelle 2-3: Komplexität eines Algorithmus.....	22
Tabelle 2-4: Laufzeit verschiedener Klassen von Algorithmen.....	23
Tabelle 2-5: Faktorisierung mit dem speziellen Zahlkörpersieb.....	29
 <u>KAPITEL 3: DIE ENTWICKLUNG DES HOMEBANKING</u>	 <u>57</u>
Tabelle 3-1: Der Strukturwandel im Bankbetrieb.....	64
 <u>KAPITEL 4: HBCI – HOMEBANKING COMPUTER INTERFACE</u>	 <u>69</u>
Tabelle 4-1: HBCI-Versionen.....	71
Tabelle 4-2: Trennzeichen in der HBCI-Syntax.....	73
Tabelle 4-3: Segmente vor der Verschlüsselung.....	74
Tabelle 4-4: Segmente nach der Verschlüsselung.....	75
Tabelle 4-5: Anforderung an die Identität.....	89
Tabelle 4-6: Anforderung an die Authentifikation.....	89
Tabelle 4-7: Anforderung an die Integrität.....	89
Tabelle 4-8: Anforderung an die Vertraulichkeit.....	90
Tabelle 4-9: Anforderung an die Doppeleinreichungskontrolle.....	90
Tabelle 4-10: Anforderung an die Nicht-Abstreitbarkeit.....	90
 <u>KAPITEL 5: ELLIPTISCHE KURVEN IN DER KRYPTOLOGIE</u>	 <u>99</u>
Tabelle 5-1: Naive Bestimmung von $\#E(F_p)$	125
Tabelle 5-2: Bestimmung von $\#E(F_p)$ über $\text{ord}(P)$	126
Tabelle 5-3: Verfahren zur Ermittlung der Gruppenordnung.....	128
Tabelle 5-4: Vergleich der Gruppen Z_p^* und $E(Z_p)$	132
 <u>KAPITEL 6: ELLIPTISCHE KURVEN ALS SICHERHEITSBAUSTEIN IN HBCI</u>	 <u>141</u>
Tabelle 6-1: Erforderliche Rechenleistung zur Bestimmung eines ECDL mit dem Rho-Algorithmus.....	153
Tabelle 6-2: Erforderliche Rechenleistung zur Faktorisierung ganzer Zahlen mit dem Zahlkörpersieb.....	153
Tabelle 6-3: Erforderliche Schlüsselgrößen beim RSA, DSA und EC-Systemen bei vergleichbarer Sicherheitsstufe.....	154
Tabelle 6-4: Vergleich zwischen RSA, DSA und EC-Systemen.....	155
Tabelle 6-5: Das richtige Kryptosystem für jede Anwendung.....	157

ABBILDUNGSVERZEICHNIS

KAPITEL 2: EINIGE MATHEMATISCHE GRUNDLAGEN	7
Abbildung 2-1: Funktionsschema einer Verschlüsselung.....	21
Abbildung 2-2: Symmetrische Verschlüsselung.....	34
Abbildung 2-3: Blockchiffrierung.....	35
Abbildung 2-4: Der DES als Feistel-Netzwerk.....	37
Abbildung 2-5: Der Triple-DES.....	38
Abbildung 2-6: Asymmetrische Verschlüsselung.....	39
Abbildung 2-7: Die Funktionsweise der RSA-Verschlüsselung.....	40/41
Abbildung 2-8: Die Funktionsweise der ElGamal-Verschlüsselung.....	43
Abbildung 2-9: Die Funktionsweise der DSA-Signatur.....	48/49
Abbildung 2-10: Die Funktionsweise des MAC.....	51
Abbildung 2-11: Angriffsmöglichkeiten bei der Verwendung von Chipkarten.....	53
Abbildung 2-12: Kryptografische Bausteine.....	55
 KAPITEL 3: DIE ENTWICKLUNG DES HOMEBANKING	 57
Abbildung 3-1: Electronic-Banking als Schnittstelle zwischen Kunde und Bank.....	59
Abbildung 3-2: Electronic-Banking.....	60
Abbildung 3-3: Das PIN / TAN-Verfahren.....	62
Abbildung 3-4: Aspekte einer sicheren Transaktion.....	65
Abbildung 3-5: Mögliche Angriffe auf eine Homebanking-Transaktion.....	66
 KAPITEL 4: HBCI – HOMEBANKING COMPUTER INTERFACE	 69
Abbildung 4-1: Der Aufbau einer Kundennachricht.....	73
Abbildung 4-2: Der Dialog in HBCI.....	76
Abbildung 4-3: Authentifizierung von Chipkarte und Lesesystem.....	79
Abbildung 4-4: Merkmale des DDV-Sicherheitsverfahrens in HBCI.....	80
Abbildung 4-5: Merkmale des RDH-Sicherheitsverfahrens in HBCI.....	81
Abbildung 4-6: Das RDH-Verfahren in HBCI.....	84/85
Abbildung 4-7: Angriffe auf die Doppeleinreichungskontrolle.....	88
Abbildung 4-8: Homebanking via OFX.....	95

KAPITEL 5: ELLIPTISCHE KURVEN IN DER KRYPTOLOGIE	99
Abbildung 5-1: Elliptische Kurven in allgemeiner Weierstraß-Normalform.....	105
Abbildung 5-2: Elliptische Kurven in reduzierter Weierstraß-Normalform.....	107
Abbildung 5-3: Singuläre elliptische Kurven.....	109
Abbildung 5-4: Die Punktaddition $\oplus$ für zwei Punkte P und Q mit $P \neq Q, -Q$	111
Abbildung 5-5: Die Punktaddition $\oplus$ für den Fall $P = Q$	112
Abbildung 5-6: Das neutrale Element $\mathcal{O}$ der Gruppe $E (K, \oplus, \mathcal{O})$	114
Abbildung 5-7: Das zu P inverse Element $-P$ der Gruppe $E (K, \oplus, \mathcal{O})$	114
Abbildung 5-8: Nachweise des Assoziativgesetzes in der Gruppe $E (K, \oplus, \mathcal{O})$	115
Abbildung 5-9: Herleitung der Gruppenformeln für die Gruppenverknüpfung $\oplus$	117
Abbildung 5-10: Die Funktionsweise der EC-ElGamal-Verschlüsselung.....	137
Abbildung 5-11: Die Funktionsweise der ECDSA-Signatur.....	139
 KAPITEL 6: ELLIPTISCHE KURVEN ALS SICHERHEITSBAUSTEIN IN HBCI	 141
Abbildung 6-1: Vergleich der Sicherheitsstufen von RSA, DAS und EC-Systemen....	156

ABKÜRZUNGSVERZEICHNIS

A^2	Die euklidische oder affine Ebene.....	102
A^n	Der n -dimensionale affine Raum.....	102
$a b, a b$ *	Bezüglich der Verknüpfung $*$ ist das Element a ein Teiler von b ...	10
$\bar{a}$	Die Restklasse von $a \bmod m$	13
$C_f / K, C_f$	Kurve in der affinen Ebene, die durch $f(x_1, x_2) = 0$ in K mit $f \in K[x_1, x_2]$ definiert ist.....	102
$C_f(\bar{K})$	Die Menge aller Punkte (x, y) der affinen Ebene mit $x, y \in \bar{K}$, für die $f(x, y) = 0$ mit $f \in K[x_1, x_2]$ gilt.....	102
$\text{char}(K)$	Die Charakteristik eines Körpers K	15
$\Delta(E)$	Die Diskriminante einer elliptischen Kurve E	108
E / K	Eine elliptische Kurve E über einem Körper K	105
$E(K)$	Die Menge der K -rationalen Punkte von E / K	105
$E(K, \oplus, \circ)$	Die auf $E(K)$ definierte Gruppe bzgl. $\oplus$ mit neutralem Element $\circ$	103
$E(K)[n], E[n]$	Die Menge aller n -Torsionspunkte aus $E(K)$	131
$\# E(K)$	Die Gruppenordnung von $E(K, \oplus, \circ)$	123
F_p	Der endliche Körper mit p Elementen, p prim.....	
F_q	Der endliche Körper mit q Elementen, $q = p^n$, p prim, n eine natürliche Zahl.....	
F_p^*	Die multiplikative Gruppe eines endlichen Körpers F_p	
f_x	Die partielle Ableitung $\partial f / \partial x$ von f nach x	103
$\text{ggT}(x, y), (x, y)$	Der größte gemeinsame Teiler von x und y	11
$\text{grad } f$	Der Grad einer Funktion.....	102
$j(E)$	Die j -Invariante einer elliptischen Kurve E	110
$\bar{K}$	Der algebraische Abschluss eines Körpers K	101
K^+	Die additive Gruppe eines Körpers K	
K^*	Die multiplikative Gruppe eines Körpers K	
$K[x_1, x_2]$	Der Polynomring über K	102
$\mathbb{N}$	Die Menge der natürlichen Zahlen.....	11
$O(g(n))$	Die asymptotische Notation zur Abschätzung von Komplexitäten oder Laufzeiten von Algorithmen.....	22
$\circ$	Der unendliche (projektive) Punkt der Gruppe $E(K, \oplus, \circ)$	103
P^2	Die projektive Ebene.....	103
P^n	Der n -dimensionale projektive Raum.....	103
$P \oplus Q$	Die Punktaddition der Punkte P und Q einer elliptischen Kurve E	110
nP	Die skalare Multiplikation eines Punktes P einer elliptischen Kurve E	112
$\varphi(x)$	Die Eulersche φ -Funktion $\varphi(x) = \{y \mid 0 < y < x \text{ und } (x, y) = 1\} $	42

$S(P, C, K)$	Ein kryptografisches Verschlüsselungssystem mit einem Plaintext P , einer Menge C von Chiffretexten und einer Menge K von Schlüsseln.....	20
$W(x = y)$	Die Wahrscheinlichkeit dafür, dass das Argument $x = y$ zutrifft....	30
$\left(\frac{x}{p}\right)$	Das Legendre-Symbol für $x \in \mathbb{Z}_p^*$ und $p \geq 3$ eine Primzahl.....	17
$\mathbb{Z}$	Die Menge der ganzen Zahlen.....	15
$\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}_n$	Der Ring der ganzen Zahlen modulo n	15

Beh.	Behauptung
Bew.	Beweis
bzgl.	Bezüglich
d.h.	Das heißt
i.d.R.	In der Regel
m.a.W.	Mit anderen Worten
o.B.d.A.	Ohne Beschränkung der Allgemeinheit
z.z.	Zu zeigen

BTX	Der Bildschirmtext.....	62
CEPT	Conférence Européenne des Administration des Postes.....	67
DES	Der <i>Data Encryption-Standard</i>	35
DL	Das Problem des diskreten Logarithmus oder <i>Discrete Logarithm Problem</i> , die Berechnung diskreter Logarithmen in endlichen Gruppen.....	29
DSA	Der <i>Digital Signature-Algorithm</i>	47
EC	Elliptic Curves.....	101
ECDL	Das <i>Elliptic Curve Discrete Logarithm-Problem</i>	133
EDIFACT	Electronic Data Interchange for Administration Commerce and Transport.....	72
F, IF	Das Faktorisierungsproblem oder <i>Integer Factorization</i> , die Berechnung der Primfaktorzerlegung einer natürlichen Zahl..	28
GSM	Groupe Spéciale Mobile / Global System Mobile.....	72
HBCI	Homebanking Computer Interface.....	69
HTML	Hypertext Markup Language.....	94
HTTP	Hypertext Transport Protocol.....	94
ISDN	Integrated Services Digital Network.....	72
MAC	Der <i>Message-Authentication Code</i>	50
MIPS	Million Instructions Per Second.....	29
OFC	Open Financial Connectivity.....	94
OFX	Open Financial Exchange.....	94
PPT	Probabilistic Polynomial Time Algorithm.....	19
RSA	Der <i>Rivest Shamir-Adleman</i> - Algorithmus.....	40
SigG	Das Deutsche Signaturgesetz.....	80
URL	Uniform Resource Locator.....	95
ZKA	Der Zentrale Kredit-Ausschuss.....	62

Kapitel 1

VORBEMERKUNGEN

In diesem kurzen einführenden Kapitel sollen die Problemstellung und Zielsetzung der vorliegenden Arbeit verdeutlicht werden.

Ferner soll die angewandte Methodik erläutert und ein Überblick zu den einzelnen Kapitel dieser Arbeit gegeben werden.

INHALT

- 1.1 Problemstellung und Zielsetzung
- 1.2 Methodik und Vorgehensweise

1.1 Problemstellung und Zielsetzung

In der Wirtschaft sind Zahlungen mit die wichtigsten Vorgänge. Die Digitalisierung von Zahlungen ist deshalb eine wichtige Voraussetzung für die bevorstehende Digitalisierung vieler Prozesse der Wirtschaft.

Die Transaktionssicherheit ist dabei eine der wichtigsten Grundlagen zu einer erfolgreichen Durchführung von Zahlungen über offene Netze und damit oberste Aufgabe der Kryptologie. In Deutschland versucht sich der Standard *Homebanking Computer Interface*, kurz HBCI, dieser Aufgabe zu stellen.

In dieser Arbeit soll der Begriff des Homebanking zunächst definiert und abgegrenzt werden. Aus einer kurzen geschichtlichen Betrachtung der Homebanking-Entwicklung in Deutschland entstehen Sicherheits- und Design-Anforderungen an einen neuen Homebanking-Standard. Wir wollen HBCI als neuen deutschen Homebanking-Standard vorstellen und überprüfen, ob HBCI diesen Anforderungen gerecht wird. Weiterhin werden wir durch Betrachtung möglicher Alternativen zu HBCI aufzeigen, dass HBCI zwar noch Defizite in sich trägt, aber derzeit keine Alternativen für den deutschen Markt zu sehen ist.

Ziel dieser Arbeit ist es, elliptische Kurven als alternativen Public Key-Baustein für HBCI vorzuschlagen. Wir werden deshalb elliptische Kurven vorstellen und die Vorteile aufzeigen, die eine solche Integration für HBCI bringen würde. Nach dem derzeitigen wissenschaftlichen Stand können dadurch eine höhere Sicherheit, Transaktionseffizienz, Kosteneinsparungen und eine Angleichung an das deutsche Signaturgesetz (SigG) als wesentliche Verbesserungen erreicht werden.

Da HBCI aufgrund seiner offenen Struktur einer technischen Realisierung dieser Idee nicht im Wege steht, liegt es lediglich am Zentralen Kredit-Ausschuss (ZKA), diesen Vorschlag zu prüfen und möglicherweise für HBCI zu standardisieren.

1.2 Methodik und Vorgehensweise

Diese Arbeit ist im Bewusstsein der neuen Rechtschreibreform geschrieben, um ihren aktuellen Inhalt auch in der Form widerzuspiegeln.

Mit dem Ziel, den Leser stärker in die Thematik der Arbeit einzubeziehen, wird im Folgenden das personalisierte „wir“ als Ansprache verwendet. Damit sei stets die Gemeinschaft von Autor und Leser angesprochen.

Durch einen umfangreichen Grundlagenteil soll dem fachunfremden Leser in dieser Arbeit das thematische Verständnis erleichtert werden. Es werden lediglich einige wesentliche mathematische Grundbegriffe vorausgesetzt.

Das KAPITEL 2 dieser Arbeit widmet sich einigen *Grundlagen*:

Für den Verlauf der Arbeit ist es unbedingt erforderlich, ein gemeinsames kryptografisches und zahlentheoretisches Vokabular zu besitzen. In diesem Kapitel werden wir versuchen, diese elementaren Begriffe und Sätze stringent und klar darzulegen.

Die *Entwicklung des Homebanking* soll in KAPITEL 3 betrachtet werden:

Da Homebanking derzeit ein sehr angesagtes Thema in den Medien ist, scheint es erforderlich, unterschiedliche, im Raum stehende Begriffe, wie Online-Banking, Internet-Banking oder Homebanking, voneinander abzugrenzen. Aufgrund der Geschichte und der Entwicklung des Homebanking in Deutschland entsteht die Notwendigkeit eines neuen Homebanking-Standards. Dieser muss sich einigen Anforderungen an Sicherheit und an das Design stellen, die wir in diesem Kapitel herausarbeiten wollen.

In KAPITEL 4 wollen wir *HBCI – Homebanking Computer Interface* als neuen deutschen Homebanking-Standard vorstellen und die an den neuen Homebanking-Standard gestellten Anforderungen in HBCI überprüfen. Weiterhin sollen mögliche Alternativen zu HBCI betrachtet werden. Dabei werden wir feststellen, dass es derzeit in Deutschland keine Alternative zu HBCI gibt; dennoch sind einige Defizite in HBCI der aktuellen Version 2.1 enthalten.

Da wir elliptische Kurven als alternativen Sicherheitsbaustein für HBCI vorschlagen wollen, sollen im KAPITEL 5 *Elliptische Kurven in der Kryptologie* betrachtet und notwendige mathematische Hintergründe anschaulich aufgezeigt werden.