Rene Algesheimer

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

Diplomarbeit

Diplom.de

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.

ISBN: 9783832425548

Rene Algesheimer

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

Diplom.de

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

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

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, Magisterarbeiten, 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 liebenswerte 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 mühevolle 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 herzhafte Lacher.
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

ABBILDUNGSVERZEICHNIS

ABKÜRZUNGSVERZEICHNIS

A^2	Die euklidische oder affine Ebene.....	102
A^n	Der *n*-dimensionale affine Raum.....	102
$a \mid b$, a | b	Bezüglich der Verknüpfung * ist das Element *a* ein Teiler von *b*...	10
$\overset{*}{\overline{a}}$	Die Restklasse von *a* mod *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
$C_f(\overline{K})$	Die Menge aller Punkte (*x, y*) der affinen Ebene mit $x, y \in \overline{K}$, für die *f* (*x, y*) =0 mit $f \in K[x_1, x_2]$ gilt.....	102
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, $\oplus$, $\mathcal{O}$)	Die auf *E* (*K*) definierte Gruppe bzgl. $\oplus$ mit neutralem Element $\mathcal{O}$.....	103
E (K) [*n*],*E* [*n*]	Die Menge aller *n*-Torsionspunkte aus *E* (*K*).....	131
# *E* (*K*)	Die Gruppenordnung von E ($K, \oplus, \mathcal{O}$).....	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
ggT(x,y), (x,y)	Der größte gemeinsame Teiler von *x* und *y*.....	11
grad f	Der Grad einer Funktion.....	102
j (*E*)	Die *j*-Invariante einer elliptischen Kurve *E*.....	110
$\overline{K}$	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
$\mathcal{O}$	Der unendliche (projektive) Punkt der Gruppe E (K, $\oplus$, $\mathcal{O}$).....	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 $\varphi(x) = \left\lvert \{ y \mid 0 < y < x \text{ und } (x, y) = 1 \} \right\rvert$.....	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 *Data Encryption-Standard*	35
DL	Das Problem des diskreten Logarithmus oder *Discrete Logarithm Problem*, die Berechnung diskreter Logarithmen in endlichen Gruppen	29
DSA	Der *Digital Signature-Algorithm*	47
EC	Elliptic Curves	101
ECDL	Das *Elliptic Curve Discrete Logarithm-Problem*	133
EDIFACT	Electronic Data Interchange for Administration Commerce and Transport	72
F, IF	Das Faktorisierungsproblem oder *Integer Factorization*, 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 *Message-Authentication Code*	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 *Rivest Shamir-Adleman*- 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

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 Rechtschreibereform 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.