

Digitale Signaturen für Datenströme

Vom Fachbereich
Elektrotechnik und Informatik der Universität Siegen
genehmigte Dissertation
zur Erlangung des akademischen Grades

Doktor der Ingenieurwissenschaften
(Dr.-Ing.)

von Dipl.-Ing. Niko Schweitzer

Referent:	Prof. Dr. rer. nat. Christoph Ruland
Korreferent:	Prof. Dr.-Ing. Firoz Kaderali
Tag der Einreichung:	7. November 2002
Tag der mündlichen Prüfung:	18. März 2003

Schriften zur Nachrichtenübermittlungstechnik

Herausgeber: Prof. Dr. Christoph Ruland

Band 7

Niko Schweitzer

Digitale Signaturen für Datenströme



Aachen 2003

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Schweitzer, Niko:

Digitale Signaturen für Datenströme / Niko Schweitzer.

Aachen : Shaker, 2003

(Schriften zur Nachrichtenübermittlungstechnik ; Bd. 7)

Zugl.: Siegen, Univ., Diss., 2003

ISBN 3-8322-1417-8

Copyright Shaker Verlag 2003

Alle Rechte, auch das des auszugsweisen Nachdruckes, der auszugsweisen oder vollständigen Wiedergabe, der Speicherung in Datenverarbeitungsanlagen und der Übersetzung, vorbehalten.

Printed in Germany.

ISBN 3-8322-1417-8

ISSN 1431-6560

Shaker Verlag GmbH • Postfach 101818 • 52018 Aachen

Telefon: 02407 / 95 96 - 0 • Telefax: 02407 / 95 96 - 9

Internet: www.shaker.de • eMail: info@shaker.de

Vorwort

Die vorliegende Arbeit entstand während meiner Tätigkeit als Wissenschaftlicher Mitarbeiter am Institut für Nachrichtenübermittlung der Universität Siegen.

Dem Institutsleiter, Herrn Prof. Dr. rer. nat. Christoph Ruland, danke ich herzlich für die Möglichkeit zur Durchführung dieser Arbeit, die eingeräumte eigenverantwortliche Arbeitsweise und die ständige Bereitschaft zur wissenschaftlichen Diskussion sowie für seine wertvollen Hinweise und Anregungen.

Mein Dank gilt ferner Herrn Prof. Dr.-Ing. Firoz Kaderali, Leiter des Lehrstuhls Kommunikationssysteme der Fernuniversität Hagen, für sein Interesse an dieser Arbeit und die Übernahme des Korreferates.

Auch möchte ich mich bei Herrn Prof. Dr. Wolfgang Merzenich für den Vorsitz der Prüfungskommission bedanken.

Weiterhin danke ich meinen Kollegen Christian Geuer-Pollmann, Christine Haßler, Luigi Lo Iacono, Oliver Jung, Sven Kuhn, Matthias Schneider, Christoph Stepping und Kai Wollenweber für die stets konstruktive Zusammenarbeit und die ausgesprochen angenehme Arbeitsatmosphäre.

Besonderer Dank gilt Katja Bertolo und allen meinen Freunden, die mich stets beim Verfassen dieser Arbeit motiviert und auch manchmal auf andere Gedanken gebracht haben.

Meinen Eltern danke ich dafür, dass sie mir das Studium ermöglichten, mich stets unterstützt und gefördert haben.

Siegen, im Januar 2003

Niko Schweitzer

Zusammenfassung

Durch die Verbreitung und Entwicklung vernetzter Rechnerysteme wie das Internet entstehen vielfältige Sicherheitsprobleme. Berichte über Angriffe und Schäden durch Computerviren, Trojanische Pferde oder Hacker verdeutlichen den Bedarf nach geeigneten Schutzmaßnahmen. Zusätzliche Sicherheitsanforderungen entstehen durch Bestrebungen, elektronische Geschäftsprozesse, häufig als E- oder M-Commerce bezeichnet, über offene Netzwerke wie das Internet abzuwickeln. Neben dem bekanntesten Schutzziel, Kommunikationsinhalte oder Kommunikationsbeziehungen vertraulich zu halten, werden Sicherheitsdienste wie Prüfbarkeit der Authentizität digitaler Daten zunehmend bedeutender.

Zur Gewährleistung der Authentizität sind digitale Signaturen ein anerkannter und vielfältig nutzbarer kryptographischer Mechanismus. Signaturalgorithmen besitzen allerdings den Nachteil, Berechnungen erst durchführen zu können, wenn vollständige Datensätze verfügbar sind. Ist eine zeitnahe Be- oder Verarbeitung von Daten erforderlich, sind diese meist ungeeignet und nicht anwendbar.

Gefördert durch steigende Bandbreite digitaler Netzwerke entstehen vermehrt Anwendungen, die Datenströme übertragen und zeitnah verarbeiten. Gängige Beispiele sind digitale Audio-, Video- oder Datenübertragungen, die direkt während des Empfangs konsumiert werden, ohne eine vollständige Speicherung von Datensätzen vorzunehmen. Um in solchen Anwendungsbereichen auf digitalen Signaturen basierende Sicherheitsdienste anbieten zu können, ist die Entwicklung und Untersuchung spezieller Algorithmen und Verfahren erforderlich.

Die vorliegende Arbeit behandelt die Problematik der Berechnung und Verifikation digitale Signaturen für Datenströme. Es werden Authentifikationsverfahren für Datenströme vorgestellt sowie neue Datenstrom-Signaturverfahren entwickelt, beschrieben und untersucht.

Der praktische Teil der Arbeit beschreibt ein entwickeltes Framework zur Implementation und Nutzung von Datenstrom-Signaturverfahren in Java. Weiterhin werden Implementationen und Messergebnisse dargestellt.

Abstract

With the rapid growth of open communication networks like the Internet more and more incident reports of damages caused by computer viruses, malicious software or hacker attacks are published. This obviously illustrates the demand for security services to prevent and detect attacks. Additional security requirements arise from electronic business transactions performed over insecure networks. Besides the objective of keeping communications confidential other security services as data integrity and authenticity become increasingly important.

Digital signatures are a frequently used cryptographic primitive to ensure authenticity of digital data. Signing digital streams is however more problematic as signing messages in whole. Traditional signature schemes are message oriented and require entire datasets for signature calculation and verification.

Digital streams are very long (or potentially infinite) sequences of bits which are sent to one or multiple receivers and are processed and consumed more or less at input rate without much delay. Therefore it is infeasible to obtain and store streams entirely in order to check authenticity by applying traditional digital signature schemes. Streams may include for instance online news, stock and data feeds, radar and medical data transmissions or digitized audio and video.

This work focuses on signing digital streams. After describing difficulties arising from streamed data processing, requirements for stream signatures are discussed and interesting application areas are pointed out. In the main part various new signature schemes for signing streamed data are presented and system properties are worked out.

The practical part introduces a flexible framework for implementation and usage of stream signature schemes in Java. Furthermore implementation results are presented.

Inhaltsverzeichnis

1	Einführung	1
1.1	Sicherheitsdienste	2
1.2	Datenströme	4
1.3	Digitale Signatur	6
1.4	Authentikation und Digitale Signatur von Datenströmen	7
1.5	Anwendungen für Datenstrom-Signaturverfahren	8
2	Stand der Technik	11
2.1	Verkettete Authentikatoren	11
2.2	Hashwert-Tabellen	14
2.3	Authentikationsbäume	16
2.4	Weitere Verfahren	20
3	Bewertungskriterien für Datenstrom-Signaturverfahren	21
3.1	Broadcast-Tauglichkeit	21
3.2	Online-Tauglichkeit	21
3.2.1	Online-Signatur	22
3.2.2	Online-Verifikation	24
3.2.3	Maximaler Durchsatz	25
3.2.4	Verzögerung	26
3.3	Parallelisierbarkeit	28
3.4	Datenexpansion	28
3.5	Fehlerfortpflanzung	29
3.6	Selbstsynchronisation	30
3.7	Sicherheitseigenschaften	30
3.7.1	Sicherheit kryptographischer Algorithmen	30
3.7.2	Systemsicherheit	30
4	Basistechniken	33
4.1	Digitale Signaturen	33
4.1.1	Digitale Signaturen mit Anhang	34
4.1.2	Digitale Signaturen mit Nachrichtenrückgewinnung	35
4.1.3	Signatur-Modulation	38
4.1.4	Signatur-Modulation mit Spreizung	40
4.2	Teilsignaturen	43
4.3	Verkettung	44
4.4	Verzögerungsfreies Signieren	45

4.5	Selbstsynchronisation	45
4.6	Statistische Selbstsynchronisation	47
4.7	Nomenklatur für Datenstrom-Signaturverfahren	52
5	Authentikation von Datenströmen mit Datenexpansion	55
5.1	Signaturen ohne Verkettung, mit Datenexpansion, ohne Selbstsynchronisation	55
5.2	Signaturen mit Verkettung, mit Datenexpansion, ohne Selbstsynchronisation	63
5.2.1	Allgemeine Beschreibung	63
5.2.2	Verkettung von Teilsignaturen	66
5.2.3	Verkettung von Datenblöcken	68
5.2.4	Verkettung von Verifikationsergebnissen	71
5.2.5	Verkettung von Teilsignaturen und Verifikationsergebnissen	73
5.2.6	Vergleich der Verfahren	76
5.3	Signaturen mit Verkettung, mit Datenexpansion, mit Selbstsynchronisation	77
5.3.1	Allgemeine Beschreibung	77
5.3.2	Verkettung von Teilsignaturen	81
6	Digitale Signatur von Datenströmen ohne Datenexpansion	85
6.1	Signaturen mit Verkettung, ohne Datenexpansion, ohne Selbstsynchronisation	85
6.1.1	Allgemeine Beschreibung	85
6.1.2	Verkettung signierter Blöcke und skalierbarer Fehlerfortpflanzung	88
6.2	Signaturen mit Verkettung, ohne Datenexpansion, mit Selbstsynchronisation	93
6.3	Vergleich von Verfahren ohne Datenexpansion	99
7	Vergleich ausgewählter Datenstrom-Signaturverfahren	101
7.1	Wahl der Vergleichsverfahren	101
7.2	Systemeigenschaften	102
7.3	Systemparameter	104
7.4	Berechnungszeiten von Basisalgorithmen	105
7.4.1	Implementationsplattform	105
7.4.2	Hash-Algorithmen	105
7.4.3	Signaturalgorithmen	106
7.4.4	Ver- und Entschlüsselung	109
7.4.5	Scrambler/Descrambler	109
7.5	Signatur-, Verifikations- und Demodulationszeiten	110
7.6	Durchsatz	111
7.7	Bestimmung von Block- und Synchronisationsmusterlänge bei vorgegebenem Durchsatz	117
7.8	Datenexpansion	119
7.9	Zusammenfassung	120
8	Implementation von Datenstrom-Signaturverfahren	121

8.1	Rahmenbedingungen und Anforderungen	121
8.2	Java Kryptographie Architektur: JCA/JCE	122
8.2.1	Einordnung	123
8.2.2	Designanforderungen	124
8.2.3	Engine Classes	124
8.2.4	Cryptography Service Provider (CSP)	126
8.3	Aufbau und Struktur des Datenstrom-Signatur Frameworks	128
8.3.1	Paket-Hierarchie des Frameworks	128
8.3.2	Stromsignierer und Stromverifizierer	130
8.3.3	Stromsignatur-Provider	133
8.4	Ausgewählte Komponenten	134
8.4.1	Scrambler	134
8.4.2	Spreizung	135
8.4.3	Kombinationsfunktion	135
8.4.4	Scanner	136
8.4.5	Padding	136
8.4.6	Messwertgewinnung	137
8.5	Nutzung des Frameworks	139
8.6	Testklassen für Datenstrom-Signaturverfahren	142
8.6.1	Konfiguration von Testklassen	142
8.6.2	Darstellung der Ergebnisse	144
8.7	Tests von Datenstrom-Signaturverfahren	147
8.7.1	Ergebnisse NCh/Ex/NSyn	147
8.7.2	Ergebnisse Ch/Ex/NSyn	150
8.7.3	Ergebnisse Ch/Ex/Syn	152
8.7.4	Ergebnisse Ch/NEx/Syn	154
9 Zusammenfassung und Ausblick		157
Anhang		158
A Notation		159
B Systemeigenschaften ausgewählter Datenstrom-Signaturverfahren		163
B.1	Durchsatz und Expansion	163
B.2	Block- und Synchronisationsmusterlänge bei vorgegebenem Durchsatz	169
C Java Cryptography Service Provider		175
C.1	Verfügbare CSPs	175
C.2	Unterstützte Algorithmen	175
C.3	Berechnungszeiten kryptographischer Algorithmen	175
D Quelltext-Beispiele		183
D.1	NCh/Exp/NSyn-Signierer	183
D.2	NCh/Exp/NSyn-Verifizierer	184

E Hilfs- und Testanwendungen	187
Literaturverzeichnis	195