
Vorwort zur sechsten Auflage

In der sechsten Auflage meiner Einführung in die Kryptographie habe ich die Darstellung der mathematischen Modelle, die die Sicherheit kryptographischer Verfahren beschreiben, deutlich erweitert. Ich behandle jetzt die elementare Wahrscheinlichkeitstheorie im ersten Kapitel um dort schwierige Berechnungsprobleme, die Grundlage kryptographischer Sicherheit, definieren zu können. Modelle für die Sicherheit symmetrischer Verschlüsselungsverfahren finden sich in Kapitel 4. Neben der Theorie perfekter Geheimhaltung wird dort auch semantische Sicherheit und Chosen-Plaintext-Sicherheit und Ciphertext-Sicherheit vorgestellt. Auch die Kapitel 8 „Public-Key-Verschlüsselung“ und 12 „Digitale Signaturen“ wurden entsprechend erweitert. Auch die Fehler, auf die mich Leserinnen und Leser hingewiesen haben, habe ich beseitigt. Ich bedanke mich herzlich für die Aufmerksamkeit.

Darmstadt, im Dezember 2015

Johannes Buchmann

Vorwort zur fünften Auflage

In der fünften Auflage meiner Einführung in die Kryptographie habe ich die Beweise für die Sicherheit des Lamport-Diffie-Einmalsignaturverfahren und des Merkle-Signaturverfahren erweitert und einen Abschnitt über algebraische Angriffe auf Blockchiffren neu aufgenommen. Es handelt sich dabei um eine Angriffstechnik, die neue Anforderungen an die Konstruktion von kryptographischen Verfahren stellt. Immer wieder erhalte ich Emails von Lesern, die mich auf Fehler hinweisen und Verbesserungsvorschläge machen. Dafür bin ich sehr dankbar und habe versucht, die Anregungen zu berücksichtigen.

Darmstadt, im Oktober 2009

Johannes Buchmann

Vorwort zur vierten Auflage

In der vierten Auflage meiner Einführung in die Kryptographie habe ich auch diesmal den Stand der Forschung im Bereich Faktorisieren und Berechnung diskreter Logarithmen aktualisiert. Neu aufgenommen wurde das Merkle-Signaturverfahren. Dieses Verfahren wurde etwa zeitgleich mit dem RSA-Signaturverfahren erfunden. Nachdem Peter Shor gezeigt hat, dass Quantencomputer das Faktorisierungsproblem und die in der Kryptographie relevanten Diskrete-Logarithmen-Probleme in Polynomzeit lösen können, hat das Merkle-Verfahren neue Relevanz bekommen. Es stellt nämlich eine Alternative zu den heute verwendeten Signaturverfahren dar, die alle unsicher würden, wenn genügend große Quantencomputer gebaut werden können. Außerdem habe ich die Fehler, die mir seit Erscheinen der dritten Auflage bekannt geworden sind, korrigiert. Für die vielen Hinweise, die ich von Lesern erhalten habe, bedanke ich mich sehr.

Darmstadt, im Dezember 2007

Johannes Buchmann

Vorwort zur dritten Auflage

In die dritte Auflage meiner Einführung in die Kryptographie habe ich Aktualisierungen und einige neue Inhalte aufgenommen. Aktualisiert wurde die Diskussion der Sicherheit von Verschlüsselungs- und Signaturverfahren und der Stand der Forschung im Bereich Faktorisieren und Berechnung diskreter Logarithmen. Neu aufgenommen wurde die Beschreibung des Advanced Encryption Standard (AES), des Secure Hash Algorithmus (SHA-1) und des Secret-Sharing-Verfahrens von Shamir. Außerdem habe ich die Fehler, die mir seit Erscheinen der zweiten Auflage bekannt geworden sind, korrigiert. Für die vielen Hinweise, die ich von Lesern erhalten habe, bedanke ich mich sehr.

Darmstadt, im Mai 2003

Johannes Buchmann

Vorwort zur zweiten Auflage

In die zweite Auflage meiner Einführung in die Kryptographie habe ich eine Reihe neuer Übungsaufgaben aufgenommen. Außerdem habe ich die Fehler, die mir seit Erscheinen der ersten Auflage bekannt geworden sind, korrigiert und einige Stellen aktualisiert. Für die vielen Hinweise, die ich von Lesern erhalten habe, bedanke ich mich sehr.

Darmstadt, im Dezember 2000

Johannes Buchmann

Vorwort

Kryptographie ist als Schlüsseltechnik für die Absicherung weltweiter Computernetze von zentraler Bedeutung. Moderne kryptographische Techniken werden dazu benutzt, Daten geheimzuhalten, Nachrichten elektronisch zu signieren, den Zugang zu Rechnernetzen zu kontrollieren, elektronische Geldgeschäfte abzusichern, Urheberrechte zu schützen usw. Angesichts dieser vielen zentralen Anwendungen ist es nötig, dass die Anwender einschätzen können, ob die benutzten kryptographischen Methoden effizient und sicher genug sind. Dazu müssen sie nicht nur wissen, wie die kryptographischen Verfahren funktionieren, sondern sie müssen auch deren mathematische Grundlagen verstehen.

Ich wende mich in diesem Buch an Leser, die moderne kryptographische Techniken und ihre mathematischen Fundamente kennenlernen wollen, aber nicht über die entsprechenden mathematischen Spezialkenntnisse verfügen. Mein Ziel ist es, in die Basistechniken der modernen Kryptographie einzuführen. Ich setze dabei zwar mathematische Vorbildung voraus, führe aber in die Grundlagen von linearer Algebra, Algebra, Zahlentheorie und Wahrscheinlichkeitstheorie ein, soweit diese Gebiete für die behandelten kryptographischen Verfahren relevant sind.

Das Buch ist aus einer Vorlesung entstanden, die ich seit 1996 in jedem Sommersemester an der Technischen Universität Darmstadt für Studenten der Informatik und Mathematik gehalten habe. Ich danke den Hörern dieser Vorlesung und den Mitarbeitern, die die Übungen betreut haben, für ihr Interesse und Engagement. Ich danke allen, die das Manuskript kritisch gelesen und verbessert haben. Besonders bedanke ich mich bei Harald Baier, Gabi Barking, Manuel Breuning, Safuat Hamdy, Birgit Henhagl, Andreas Kottig, Markus Maurer, Andreas Meyer, Stefan Neis, Sachar Paulus, Thomas Pfahler, Marita Skrobic, Tobias Straub, Edlyn Teske, Patrick Theobald und Ralf-Philipp Weinmann. Ich danke auch dem Springer-Verlag, besonders Martin Peters, Agnes Herrmann und Claudia Kehl, für die Unterstützung bei der Abfassung und Veröffentlichung dieses Buches.

Darmstadt, im Juli 1999

Johannes Buchmann



<http://www.springer.com/978-3-642-39774-5>

Einführung in die Kryptographie

Buchmann, J.

2016, XXVI, 330 S. 13 Abb., Softcover

ISBN: 978-3-642-39774-5