Universität Bonn
Institut für Informatik IV
Seminar WS1998/99
Grundlagen und Verfahren moderner Kryptographie

Neben der zu jedem Vortrag angegebenen Literatur lohnt sich zur Motivation immer ein Blick in die entsprechenden Abschnitte aus [1], [13] und [14].

1 Einführung

Der Vortrag soll zunächst einen Überblick über die Themen des Seminars geben und die formale Behandlung der Probleme motivieren. Desweiteren sollen wichtige Grundlagen aus der Komplexitätstheorie (Probabilistische Algorithmen, Orakelmaschinen, Nicht-Uniformität) und einige Konventionen und Fakten zur Wahrscheinlichkeitsrechnung behandelt werden.
Literatur: [9] Chapter 1, [8] Chapter 1 & A, [1] Kapitel 1, [12]

2 One Way Functions

Grundlegende Bausteine in der Kryptographie sind die sogenannten One-Way-Functions und ihre Variationen. Nach einer formalen Definition sollen verschiedene Beispiele für solche Funktionen (insbes. RSA) betrachtet werden. Ferner soll der Begriff des Hard-core predicate einer One-Way-Function eingeführt werden.
Literatur: [8] Chapter 2, [9], Chapter 2 Notwendige Fakten aus der Zahlentheorie finden sich in [8], Chapter B.

3 Pseudo Random Generators & Functions

Bei der Konstruktion beweisbar sicherer Verschlüsselungssysteme spielt der Zufall eine entscheidende Rolle. Daher werden in diesem Vortrag sogenannte Pseudo Random Generatoren untersucht. Diese müssen in der Kryptographie besondere Eigenschaften besitzen. Zentral ist hierbei das Konzept der Ununterscheidbarkeit. Dieses wird formal definiert, und nachdem wir uns von der Existenz von der Definition entsprechender Pseudo Random Generatoren überzeugt haben, werden einige Konstruktionen vorgestelltϒ. Schließlich wird der Begriff einer Pseudo Random Function eingeführt und entsprechende Beispiele betrachtet.
Literatur: [8] Chapter 3, [9] Chapter 3 & 4

4 Private Key Encryption

Hierbei geht es um die klassische Verschlüsselung zur Geheimhaltung von Nachrichten. Nach einer kurzen Einführung in symmetrische Verschlüsselungsverfahren wird eine formale Definition von

Sicherheit im Sinne der Ununterscheidbarkeit gegeben. Anschließend werden verschiedene Verfahren auf ihre Sicherheit hin untersucht.
Literatur: [8] Chapter 5, ggf. sollte auch auf [2] zurückgegriffen werden.

5 Public Key Encryption

Zunächst werden Public Key Verfahren definiert und einige Beispiele auf mögliche Sicherheitslücken untersucht. Daraus ergeben sich zwei äquivalente formale Definitionen von Sicherheit. Zur Konstruktion sicherer Systeme werden probabilistische Public Key Verfahren eingeführt und ihre Sicherheit nachgewiesen.
Literatur: [8] Chapter 6

6 Authentication

In diesem Vortrag geht es darum, Veränderungen von Nachrichten durch einen Angreifer sicher zu erkennen. Nach der Vorstellung einiger Methoden wird eine formale Definition für Sicherheit gegeben und diese für eine Reihe von Verfahren nachgewiesen.
Literatur: [8] Chapter 7

7 Digital Signatures

Digitale Signaturen dienen der sicheren Indentifikation eines Absenders und der Authentizität der gesendeten Nachricht. Zunächst werden die Sicherheitsanforderungen formal definiert und einige Verfahren analysiert. Mit Hilfe von probabilistischen Methoden können nachweisbar sichere Signaturverfahren konstruiert werden. Schließlich wird ein praktisches auf RSA basierendes Signaturverfahren vorgestellt.
Literatur: [8] Chapter 8

8 Key Distribution

Wie können sich zwei Parteien in einem verteilten System mit aktiven Gegnern über die Identität des jeweils anderen sicher werden und einen gemeinsamen Sitzungsschlüssel austauschen?
Literatur: [8] Chapter 9 und ggf. [3].

9 Interactive Proof Systems

Zunächst soll kurz die Betrachtung interaktiver (Zero-Knowledge) Beweissysteme motiviert werden (u.a. mit einem Beispiel). Dann werden interaktive Beweissysteme formal definiert und ihre Mächtigkeit diskutiert. Am Beispiel Graph-Non-Isomorphism wird ein konkretes Beweissystem vorgestellt. Schließlich werden Bit-Commitment schemes vorgestellt und ihre Konstruktion erläutert.
Literatur: [9] 6.1, 6.2 & 6.4.1, [11]

10 Zero Knowledge Proofs

Zunächst werden der Begriff Zero-Knowledge und entsprechende Komplexitätsklassen definiert. Dann wird für das Graph-Isomorphie-Problem gezeigt, daß es einen Zero-Knowledge-Beweis besitzt. Wichtig ist hier das sog. Simulationsparadigma (siehe auch [1], Kapitel 4). Schließlich wird die sequentielle Komposition von Zero-Knowledge-Beweisen untersucht.
Literatur: [9] 6.3

11 NP & Zero Knowledge Proofs

Mit Hilfe von Bit-Commitment schemes wird gezeigt, daß jede Sprache aus NP einen Zero-Knowledge-Beweis besitzt. Dazu wird ein Zero-Knowledge-Beweissytem für 3-Färbbarkeit von Graphen angegeben und die Zero-Knowledge-Eigenschaft nachgewiesen.
Literatur: [9] 6.4

12 Two Party Protocols

Als Beispiel für ein Protokoll, an dem zwei Parteien beteiligt sind, wird das gleichzeitige unterzeichnen eines Vertrages betrachtet. Dabei wird u.a. auf ein anderes weit verbreitetes Subprotokoll, das sog. Oblivious Transfer zurückgegriffen.
Literatur: [6], [7]

13 Multi Party Protocols

Wie können mehrere Parteien gemeinsam eine Funktion berechnen, deren Eingaben unter den Parteien verteilt sind und die diese auch geheim halten möchten? Das vorgestellte Protokoll benutzt als Bausteine wieder Oblivious Transfer und eine andere grundlegende Konstruktion, das sog. Verifiable Secret Sharing. Dabei handelt es sich ebenfalls um ein Protokoll, mit dem ein Geheimnis in n Stücke aufgeteilt wird und nur mit einer Mindestanzahl dieser Stücke rekonstruiert werden kann. Jeder Besitzer eines Stücks soll aber sicher sein, wirklich ein Stück des Geheimnisses zu besitzen.
Literatur: [4] Section 3 & [10]

14 Voting

Es wird ein Protokoll zur Durchführung einer elektronischen Wahl vorgestellt, das mit Hilfe kryptographischer Verfahren viele typische Anforderungen an ein Wahlverfahren nachweisbar erfüllt.
Literatur: [5]

Literatur

[1] A. Beutelspacher, J. Schwenk, K.-D. Wolfenstetter: *Moderne Verfahren der Kryptographie*, 2. verbesserte Auflage, Vieweg 1998

[2] M. Bellare, A. Desai, E. Jokipii and P. Rogaway: *A Concrete Security Treatment of Symmetric Encryption: Analysis of the DES Modes of Operation*, FOCS'97. 1997
`http://www-cse.ucsd.edu/users/mihir/papers/sym-enc.html`

[3] M. Bellare and P. Rogaway, *Entity Authentication and key distribution*, Crypto 93, 1993
http://www-cse.ucsd.edu/users/mihir/papers/key-distribution.html

[4] B. Chor, S. Goldwasser, S. Micali, B. Awerbuch: *Verifiable Secret Sharing and Achieving Simultaneity in the Presence of Faults*, FOCS'85, 383 – 395, 1985

[5] J. Cohen, M. Fischer: *A Robust and Verifiable Secure Election Scheme*, FOCS'85, 372 – 382, 1985

[6] S. Even, O. Goldreich, A. Lempel: *A Randomized Protocol for Signing Contracts*, Communications of the ACM, Vol. 28, No. 6, 637 – 647, 1985

[7] M. Fischer, S. Micali, C. Rackoff: *Secure Protocol for the Oblivious Transfer (Extended Abstract)*, Journal of Cryptology, 9(3), 191 – 195, Summer 1996.

[8] S. Goldwasser, M. Bellare: *Lecture Notes on Cryptography*, MIT 1997,
http://www-cse.ucsd.edu/users/mihir/papers/gb.html

[9] O. Goldreich: *Foundations of Cryptography (Fragments of a Book)*, Weizmann Institute of Science, 1995,
http://theory.lcs.mit.edu/ oded/frag.html

[10] O. Goldreich: *Foundations of Cryptography (Lecture Notes from 1989)*, Lectures 14-15: Cryptographic Protocols,
http://theory.lcs.mit.edu/ oded/ln89.html

[11] O. Goldreich: *Probabilistic Proof Systems (A Survey)*, ECCC Technical Report Series, No. TR94-008, 1994,
ftp://ftp.eccc.uni-trier.de/pub/eccc/reports/1994/TR94-008/index.html

[12] C.H. Papadimitriou: *Computational Complexity*, Addison-Wesley, 1994

[13] R. L. Rivest: *Cryptography*, Chapter 13 in: Handbook of Theoretical Computer Science, Vol. A, MIT Press/Elsevier, 1990

[14] B. Schneier: *Angewandte Kryptographie*, Addison-Wesley, 1996