Überblick bisher gehaltener Lehrveranstaltungen *(Auswahl)*

Christopher Wolf

Vorlesungen

Kryptographie II (2+1 SWS / 4 LP)

Sommersemester 2010 an der Ruhr-Universität Bochum

Quelle: http://www.cits.rub.de/lehre/krypto2ss10.html

Die Vorlesung beschäftigt sich mit modernen Methoden der Public-Key Kryptographie. Dazu wird ein Angreifermodell definiert und die Sicherheit der vorgestellten Verschlüsselungs-, Hash- und Signaturverfahren unter wohldefinierten Komplexitätsannahmen in diesem Angreifermodell nachgewiesen.

Themenübersicht

- Diffie-Hellman Schlüsselaustausch
- CPA und CCA-Angreifermodell
- Trapdoor Einwegpermutationen
- Verschlüsselung: RSA, ElGamal, Goldwasser-Micali, Rabin, Paillier
- Hashfunktion und das Hash & Sign Paradigma
- Einwegsignaturen
- Signaturen aus kollisionsresistenten Hashfunktionen
- Random-Oracle Modell

Diskrete Mathematik I (4+2 SWS / 8 LP)

Wintersemester 2012/13 an der Ruhr-Universität Bochum

Quelle: http://www.cits.rub.de/lehre/ws1213/dismath1.html

In der Veranstaltung wurde Moodle verwendet.

Die Vorlesung richtet sich an Studierende der Mathematik, der Angewandten Informatik und der IT-Sicherheit. Diskrete Mathematik beschäftigt sich überwiegend mit endlichen Strukturen. Die Vorlesung gliedert sich in 5 Abschnitte. Abschnitt 1 ist der Kombinatorik gewidmet. Insbesondere werden grundlegende Techniken vermittelt, um sogenannte Zählprobleme zu lösen.
In Abschnitt 2 beschäftigen wir uns mit der Graphentheorie. Graphen werden zur Modellierung von Anwendungsproblemen benutzt. Wir behandeln Techniken zur Graphexploration und weitere ausgesuchte Graphprobleme. Abschnitt 3 vermittelt Grundkenntnisse in elementarer Zahlentheorie und endet mit einem Ausblick auf kryptographische Anwendungen. Grundlegende Designtechniken für effiziente Algorithmen bilden das zentrale Thema von Abschnitt 4. Daneben geht es auch um das Aufstellen und Lösen von Rekursionsgleichungen, wobei sogenannte erzeugende Funktionen zum Einsatz kommen. Abschnitt 5 der Vorlesung liefert eine Einführung in elementare Wahrscheinlichkeitstheorie.

Der Werkzeugkasten – SAGE in Kryptographie und Kryptanalyse (2+1 SWS / 4 LP)

Sommersemester 2011, 2012 und 2013 an der Ruhr-Universität Bochum

Quellen:

- *http://www.cits.rub.de/lehre/sagess11.html*
- *http://www.cits.rub.de/lehre/sose12/sagesose12.html*
- *http://www.cits.rub.de/lehre/ss13/sagess13.html*

In allen drei Veranstaltungen wurde Moodle verwendet.

Das Modul eignet sich für interessierte Studierende in jedem Studienjahr der Bachelor-Phase. Außer normalen Schulkenntnissen in Mathematik sowie Vorkenntnissen in mindestens einer Programmiersprache werden keine Vorkenntnisse erwartet.

In der Antike wurden kryptographische Nachrichten noch auf kahle Kopfhaut geschrieben (die Haare wuchsen vor dem "Versand" der Nachricht nach), Authentifizierung erfolgte mittels Tonscherben und ganze Kulturen kamen ohne Kryptographie aus, da allein Lese- und Schreibfertigkeiten ausreichten, um Nachrichten vor hinlänglich großen Bevölkerungsschichten geheim zu halten.
Inzwischen sind wir einige Schritte weiter und ohne massive Rechnerunterstützung wäre Kryptographie nicht mehr denkbar: Sei es das Multiplizieren von 300-stelligen Ziffern, das Potenzieren in Primkörpern - überall stehen uns Rechner zu Seite. Daher ist es nur logisch, Rechner auch im Bereich Kryptanalyse einzusetzen: Statt selbst Buchstaben auszuzählen erledigt dies ein Programm, statt Primfaktoren von Hand auszuprobieren wird ein entsprechender Sieb-Algorithmus implementiert. Die vorliegende Vorlesung soll eine erst Einführung in das Computeralgebrasystem SAGE geben sowie dessen konkreter Nutzen für mathematische Fragestellungen, insbesondere aus der Kryptographie. Die Vorlesung hat dabei einen hohen Praxis-Anteil in Form von (kleineren) Programmierprojekten.
Der hier erworbene Leistungsnachweis gilt auch als Mathematik-Software-Leistungsnachweis.

Seminare

Bachelor-Seminar Diskrete Mathematik (2 SWS / 4 LP)

Sommersemester 2014 an der Ruhr-Universität Bochum

Quelle: http://www.cits.rub.de/lehre/ss14/semdismath.html

Wer mit dem Navi seinen Weg zum Ziel findet nutzt einen schnellen Algorithmus zur Suche in Graphen. Wer eine Versicherung abschließt dem wird auf Grund von möglicher, stochastisch berechneter Schadenswahrscheinlichkeit eine monatliche Prämienzahlung zugewiesen.
Wer im Internet bestellt nutzt Restklassenarithmetik um vertrauliche Daten sicher zu übertragen. In allen drei Fällen kommt Mathematik über diskreten Strukturen zum Einsatz um unser Leben angenehmer oder zumindest risikofreier zu machen.
In diesem Seminar beleuchten wir verschiedene Aspekte aus dem Bereich der diskreten Mathematik.

Behandelte Themen:

1. Matroide oder Wann funktionieren Greedy-Algorithmen
2. Algorithmus Quicksort und seine Laufzeit
3. Flüsse und Schnitte in Netzwerken
4. Gray Codes
5. Vollständige Charakterisierung zyklischer Gruppen
6. Vollständige Charakterisierung endlicher Körper

Bachelor-Master-Seminar Symmetrische Kryptanalyse (2 SWS / 4 LP)

Wintersemester 2013/14 an der Ruhr-Universität Bochum

Quelle: http://www.cits.rub.de/lehre/ws1314/symcrypt1314.html

Kryptanalyse beschäftigt sich mit dem Knacken von geheimen Funktionen wie z.B. Blockchiffren (z.B. AES), Stromchiffren (z.B. die Handy-Verschlüsslung A5) oder Hash-Funktionen (z.B.SHA-3).

In diesem Seminar werden wir gemeinsam für verschiedene symmetrische kryptographische Primitive mögliche Angriffe betrachten. Dies beinhaltet z.B. lineare und differentielle Kryptanalyse, Angriffe auf weit verbreitete Verfahren wie DECT aber auch weiter gehende Angriffe wie SAT-Solver gegeben Blockchiffren.

Behandelte Themen:

1. Wahrscheinlich gut: Lineare Kryptanalyse (Teil lineare Kryptanalyse)
2. Die Guten ins Töpfchen: Differentielle Kryptanalyse (Teil differentielle Kryptanalyse)
3. Mithören beim Telefonieren - Angriff auf DECT
4. Bit für Bit verdächtig: Differentielle Kryptanalyse gegen Stromchiffren / Beispiele (Beispiele)
5. Ja was sehen wir denn da? - Differentielle Kryptanalyse gegen Stromchiffren / Modelle (Modelle)
6. Der große Hammer: Multiple Differentiale im Überblick
7. Und sagst Du's nicht, dann piecks ich Dich! - SAT-Solver und Fault-Injection
8. Hash-Funktion auf der Streckbank: Differentielle Kryptanalyse von MD5
9. Was lief damals schief? - Kollisionsangriff auf SHA-1 im Überblick
10. Wir statuieren ein Exempel: Beispielhafte Krypanalyse einer Hash-Funktion

Bachelor-Master-Seminar Post-Quantum Kryptographie (2 SWS / 4 LP)

Wintersemester 2010/11 an der Ruhr-Universität Bochum

Quelle: http://www.cits.rub.de/lehre/sempostqkryptows10.html

Da Quantenrechner mit einer genügend großen Anzahl von Quantenbits (q-Bits) sowohl effizient faktorisieren wie auch Logarithmen in endlichen Gruppen berechnen können, macht dies kryptographische Verfahren wie RSA und ECC unsicher.

In diesem Seminar behandeln wir alternative kryptographische Primitive, die selbst in einer Post-Quantum-Welt verwendet werden können, um sichere Kommunikation zu ermöglichen.

Behandelte Themen:

1. Where is the Quantum Computer?
2. Schnelle Hash-Trees
3. Multivariate Quadratische Public Key Systeme
4. Hidden Field Equations HFE and Isomorphisms of Polynomials IP
5. Cryptanalysis of the HFE Public Key Cryptosystem
6. A Summary of McEliece-Type Cryptosystems and their Security
7. How to Achieve a McEliece-based Digital Signature Scheme
8. Lattices in der Kryptographie
9. The Learning with Errors Problem