Universität Mannheim

Lehrstuhl VI für Mathematik

Wolfgang K. Seiler

Im Herbst-/Wintersemester 2022 werde ich lesen

Kryptologie

Ort und Zeit: Dienstag, $13^{45} - 15^{15}$, A3.05 und Mittwoch, $13^{45} - 15^{15}$, A1.01
Übungen dazu: Mittwoch, $15^{30} - 17^{00}$, A1.01

Bis vor etwa fünfzig Jahren benutzten fast nur Militärs, Geheimdienste und Diplomaten kryptographische Verfahren. Der elektronische Zahlungsverkehr und später vor allem die Kommunikation und der Handel über Internet und Mobilfunk sorgten dann aber dafür, daß heute praktisch jeder von uns (meist unbewußt) Kryptographie anwendet und daß ständig neue Verfahren und Anwendungen dazukommen. Beispiele sind etwa die Quantenkryptographie, Kryptowährungen, digitale Wasserzeichen und vieles mehr.

Die meisten Verfahren, die heute praktisch angewandt werden, beruhen (im Gegensatz zu denen der Vergangenheit) auf mathematischen Problemen, größtenteils solchen aus der Zahlentheorie und Algebra. Auf diesen Verfahren wird der Schwerpunkt der Vorlesung liegen, auch wenn andere Ansätze natürlich auch behandelt werden. Wichtig ist es auch, zu jedem Verfahren die wichtigsten bekannten Angriffe dagegen zu kennen, denn nur so läßt sich die Sicherheit beurteilen und lassen sich die Parameter vernünftig wählen.

Die Vorlesung beginnt mit einer kurzen Diskussion von Aufgaben, Umfeld und Geschichte der Kryptographie, danach es um deren drei wichtigsten Säulen: Klassische Kryptoverfahren mit geheimen Schlüsseln, die für die Übertragung von Nachrichten benutzt werden, Verfahren mit öffentlichen Schlüsseln, die zur Vereinbarung von Schlüsseln für klassische Verfahren über unsichere Leitungen sowie für elektronische Unterschriften verwendet werden, und schließlich kryptographisch sichere Hashverfahren, die man unter anderem für effiziente elektronische Unterschriften, zur Sicherung der Integrität von Information und heute auch für Blockchains benötigt werden. Zum Schluß möchte ich noch kurz auf weitere Anwendungen wie kryptographische Protokolle und auf die Quantenkryptographie eingehen.

Parallel zur Vorlesung wird ein Skriptum erscheinen; ergänzende Literatur wird in der Vorlesung angegeben.

Voraussetzungen: Vorausgesetzt werden nur die mathematischen Grundvorlesungen der ersten drei Semester; alles andere wird in der Vorlesung behandelt.

Hörerkreis: Alle mathematischen Studiengänge. Für Wirtschaftsmathematiker zählt die Vorlesung zur Gruppe B.

B6, B4.08
D - 68131 Mannheim
Tel.: 0621 / 181 - 2515
Fax: 0621 / 181 - 2461
seiler@math.uni-mannheim.de
http://hilbert.math.uni-mannheim.de/∼seiler