Universität Mannheim

Lehrstuhl VI für Mathematik

Wolfgang K. Seiler

Im Frühjahrs-/Sommersemester 2025 werde ich lesen

Kryptologie

Ort und Zeit: Dienstag, $13^{45} - 15^{15}$ und Mittwoch, $13^{45} - 15^{15}$, A3.03
Übungen dazu: Mittwoch, $15^{30} - 17^{00}$, A3.03

Auch wenn es uns oft nicht bewußt ist, benutzen wir alle fast ständig kryptographische Verfahren: Bargeldloser Zahlungsverkehr, Mobilfunk, Kommunikation und Handel über das Internet wären in ihrer heutigen Form ohne Kryptographie nicht möglich. Hinzu kamen in den letzten Jahren neue Anwendungen wie nicht nur für Kryptowährungen wichtige Blockchains, digitale Wasserzeichen und vieles mehr,

Während ältere Verfahren meist auf willkürlich definierten kombinatorischen Substitutionen beruhten, verwenden die meisten heute aktuellen Verfahren zahlentheoretische oder algebraische Methoden. Diese sollen auch den Schwerpunkt der Vorlesung bilden, auch wenn andere Ansätze natürlich auch kurz behandelt werden. Wichtig ist es auch, zu jedem Verfahren die wichtigsten bekannten Angriffe zu verstehen, denn nur so läßt sich die Sicherheit beurteilen und Parameter wie Blocklängen können vernünftig gewählt werden. Deshalb ist neben der Kryptographie auch die Kryptanalyse ein wichtiger Bestandteil der Kryptologie, wobei in letzter Zeit auch potentielle Angriffe mit Quantencomputern eine zunehmende Rolle spielen.

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 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 einschließlich Lehramt

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