Marina Stoll

Public-Key Verschlüsselung von der LPN-Annahme

Bachelorarbeit

BACHELOR MASTER Publishing

Stoll, Marina: Public-Key Verschlüsselung von der LPN-Annahme, Hamburg, Bachelor + Master Publishing 2016
Originaltitel der Abschlussarbeit: Public-Key Verschlüsselung von der LPN-Annahme

Buch-ISBN: 978-3-95993-016-1
PDF-eBook-ISBN: 978-3-95993-516-6
Druck/Herstellung: Bachelor + Master Publishing, Hamburg, 2016
Zugl. Ruhr-Universität Bochum, Bochum, Deutschland, Bachelorarbeit, 2012

Bibliografische Information der Deutschen Nationalbibliothek:
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Hermannstal 119k, 22119 Hamburg
http://www.bachelor-master-publishing.de, Hamburg 2016
Printed in Germany

Inhaltsverzeichnis

1 Einleitung

In dieser Arbeit beschäftigen wir uns mit dem sogenannten *Learning Parity with Noise* Problem (kurz: LPN) und Public-Key Verschlüsselungsverfahren, die darauf aufbauen. Die LPN-Annahme ist eine von vielen Sicherheitsannahmen, die in der Kryptographie Verwendung finden. Andere bekannte Annahmen/Probleme sind die diskreter-Logarithmus-Annahme, die Diffie-Hellman-Annahmen und die RSA-Annahme, welche von sogenannten Quantencomputern gebrochen werden könnten und Verfahren, die auf diesen Annahmen basieren, wären dann unbrauchbar. Quantenrechner beruhen auf einem noch theoretischen Konzept, aber es ist nur noch eine Frage der Zeit, bis diese sehr leistungsstarken Computer einsatzfähig werden. Das LPN-Problem kann jedoch auch nicht von Quantencomputern gelöst werden und daher ist es wichtig, Kryptosysteme zu entwickeln, die auf der LPN-Annahme aufbauen. Während es bei RSA um die Faktorisierung von Zahlen geht, handelt das LPN-Problem vom Lernen eines Vektors s nach dem Erhalt des Skalarprodukts $\langle s, a\rangle$ mit einem zufälligen Vektor a, wobei das Skalarprodukt zusätzlich mit einem Noise Bit versehen wird, was das Berechnen des Vektors s erschwert.

Das LPN-Problem hat in der Kryptographie viel Verwendung gefunden. Es wird zum Beispiel in den bekannten *HB-Protokollen* von Hopper und Blum [1] verwendet, deren Sicherheit auf der Härte des LPN-Problems basiert.

Wir werden hier Public-Key Kryptosysteme beleuchten: zum Verschlüsseln wird ein öffentlicher Schlüssel und zum Entschlüsseln ein geheimer Schlüssel benutzt. Als Grundlage dieser Arbeit dient die Ausführung „More on average case vs approximation complexity“ von Mikhail Alekhnovich [2], die er 2003 auf der *IEEE Symposium on Foundations of Computer Science* Konferenz vorgestellt hat. In seiner Arbeit stellt er zwei Verfahren vor, die auf dem LPN-Problem basieren und beweist deren Sicherheit.

Ein anderes, sehr wichtiges Verschlüsselungsverfahren, das auf einer noch stärkeren Annahme basiert und ebenso nicht von Quantenrechnern geknackt werden kann, ist das *McEliece-Kryptosystem*, das von Robert McEliece im Jahre 1978 entwickelt wurde [3]. Dieses benutzt fehlerkorrigierende Goppa Codes und tarnt diese als allgemeine lineare Codes. Die Verschlüsselung an sich ähnelt der von Alekhnovich: es wird ein Matrix-Vektor-Produkt gebildet und mit ei-