Steven D. Galbraith
Mathematics of Public Key Cryptography

Cambridge University Press, 2012,
630 pp., ISBN-13: 9781107013926 , € 51,30

Das vorliegende Buch behandelt die mathematischen Grundlagen der Kryptographie mit öffentlichem Schlüssel. Im Vordergrund der Darstellung liegen die Mathematik und die Algorithmen aus Algebra, Zahlentheorie und Geometrie, mit Hilfe derer aktuelle, in der Praxis verwendete Kryptosysteme mit öffentlichem Schlüssel und solche der nächsten Generation implementiert oder angegriffen werden können. Algebraischen Kurven und der kurvenbasierten Kryptographie wird ein besonderes Gewicht gegeben, aber die auf dem Faktorisierungsproblem beruhende Kryptographie und die gitterbasierte Kryptographie werden ebenfalls ausführlich behandelt. Einige der Themen erscheinen hier erstmalig gebündelt und in Lehrbuchform.

Die an den Leser gestellten Voraussetzungen sind ein Grundwissen über Gruppen, Ringe, Körper sowie Kryptographie, Algorithmen und Komplexität, wie sie in Veranstaltungen eines Bachelorstudiums vermittelt werden. Der Autor räumt in seiner Darstellung Gründlichkeit und Präzision einen höheren Stellenwert ein als einer größtmöglichen Allgemeinheit oder Optimalität der beschriebenen Algorithmen. Zudem sind in den laufenden Text zahlreiche Übungsaufgaben eingearbeitet. Damit eignet sich das Buch sowohl als Begleitmaterial zu einer Vorlesung, als auch zum Selbststudium. Vom Inhalt her umfaßt das Buch das Kernwissen, welches für einen Start in die eigene Forschung im Rahmen einer Promotion im Bereich der mathematischen Kryptographie erforderlich ist.

Das Buch ist mit 630 Seiten und über 600 Literaturreferenzen umfangreich ausgefallen. Es unterteilt sich in die folgenden Teile: „Background“, „Algebraic Groups“ und „Exponentiation, Factoring and Discrete Logarithms“, „Lattices“, „Cryptography Related to Discrete Logarithms“, „Cryptography Related to Integer Factorisation“ und „Advanced Topics in Elliptic and Hyperelliptic Curves“ mit Abschnitten zu Isogenien und Paarungen. Weitere Details zum Inhalt sind unter `http://www.math.auckland.ac.nz/~sgal018/crypto-book/crypto-book.html` zu finden.

Florian Heß (Oldenburg)

Weitere Bücher können auf der Seite `http://www.fachgruppe-computeralgebra.de/Buecher` oder direkt bei Anne Frühbis-Krüger (`fruehbis-krueger@math.uni-hannover.de`) zur Besprechung angefordert werden.