Rezension des Buches

"Komplexitätstheorie und Kryptologie — Eine Einführung in die Kryptokomplexität"

von Jörg Rothe

Springer, 2008

ISBN: 1-1614-5216, 978-3-540-79744-9

Rolf Oppliger
eSECURITY Technologies

16. Februar 2010

1 Worüber ist das Buch?

Das zur Diskussion stehende Buch ist die deutschsprachige Übersetzung des Buches *Complexity Theory and Cryptology — An Introduction to Cryptocomplexity*, das 2005 vom gleichen Autor im Springer-Verlag erschienen ist (ISBN 3-540-22147-6 bzw. 978-3-540-22147-0). Es behandelt die Komplexitätstheorie bzw. deren Anwendung in der Kryptologie. Der Autor hat dafür den Begriff *Kryptokomplexität* geprägt und meint damit die Symbiose der beiden Forschungsgebiete *Kryptologie* und *Komplexitätstheorie*. Dieser Begriff ist geschickt gewählt und trifft das Thema der Arbeit sehr genau. Das Buch ist interessant und aus didaktischer Sicht wertvoll, weil es insbesondere einen neuen und in seiner Art auch einzigartigen Zugang zu Forschungsresultaten der modernen Kryptografie verschafft.

2 Was wird im Buch behandelt (Zusammenfassung)?

Wie der Titel suggeriert, führt das Buch in die Kryptokomplexität und seine wesentliche Aspeke ein. Nach einer kurzen Einführung in Kapitel 1 vermittelt das Buch in Kapitel 2 Hintergrundinformationen über Informatik und Mathematik. Die vermittelten Inhalte sind sorgfältig und zum Thema passend ausgewählt; sie umfassen Algorithmen, formale Sprachen und rekursive Funktionstheorie, Logik, Algebra, Zahlentheorie, Graphentheorie und Wahrscheinlichkeitstheorie. In Kapitel 3 werden die Grundlagen der Komplexitätstheorie eingeführt und im Detail erörtert. Dabei spielen insbesondere auch Fragen der Reduzierbarkeit und Vollständigkeit eine tragende Rolle. Mit diesen Begriffen werden in Kapitel 4 die Grundlagen der Kryptologie eingeführt. Schwerpunktmässig werden dabei klassische Verschlüsselungssysteme und perfekte Geheimhaltung im Sinne

von Shannon und dem One-Time Pad behandelt. In Kapitel 5 werden ein paar wichtige Komplexitätshierarchien auf der Basis von NP eingeführt, wie z.B. die Boolesche Hierarchie über NP und die polynomiale Hierarchie. In Kapitel 6 werden probabilistische (bzw. randomisierte) Algorithmen und dazugehörige Komplexitätsklassen im Detail erklärt und zueinander in Beziehung gesetzt. In den zwei letzten Kapiteln werden ein paar Aspekte von kryptografischen Systemen mit zwei Schlüsseln beleuchtet. So werden in Kapitel 7 das RSA Kryptosystem, das Testen von Primzahlen und das Faktorisierungsproblem für ganze Zahlen erörtert, während in Kapitel 8 ein paar asymmetrische Kryptosysteme und Protokolle, die auf dem diskreten Logarithmusproblem basieren, eingeführt und diskutiert werden. Namentlich geht es dabei um Diffie-Hellman, Elgamal und Rabin. Zuletzt enthält das Buch Übersichtslisten von verwendeten Figuren und Tabellen, eine ausführliche Referenzliste und einen Index. Zusammenfassend darf man sagen, dass das Buch das Thema, das im Grenzbereich zwischen der Kryptologie und der Komplexitätstheorie anzusiedeln ist, auf eine vollständige und sehr anschauliche Art und Weise behandelt.

3 Wie ist das Buch verfasst (Stil)?

Das Buch basiert auf Vorlesungen, die der Autor seit 1996 an deutschen Universitäten gehalten hat. Entsprechend ist das Buch als Lehrbuch konzipiert und in einem wissenschaftlichen Stil verfasst. Lehrsätze werden hergeleitet und streng mathematisch bewiesen. Der einführende Teil des Buches ist relativ knapp gehalten, so dass jemand, der mit den Grundlagen der Komplexitätstheorie und/oder Kryptologie noch nicht so vertraut ist, sinnvollerweise Komplementärliteratur heranziehen wird. Das trifft namentlich für die Komplexitätstheorie zu, verlangt ein echtes Verständnis der Kryptokomplexität doch tiefgreifende Kenntnisse über dieses Thema. Anders ausgedrückt könnte jemand, der sich in der Komplexitätstheorie nicht so auskennt, Schwierigkeiten haben, den Kernaussagen des Buches zu folgen und diese auch im Detail zu verstehen. Das Buch ist kein Handbuch über alle im Einsatz stehenden kryptografischen Algorithmen und Protokolle (dafür gibt es genügend andere Bücher). Vielmehr führt das Buch komplexitätstheoretische Ideen und Argumente ein und wendet diese auf kryptografische Situationen an. Das Resultat ist eine neue und sinnvolle Herangehungsweise an moderne kryptografische Forschungsresultate. Ein Leser des Buches wird mit grosser Wahrscheinlichkeit einen leichteren Zugang finden und für das Verständnis der kryptografischen Beweise, die man in der Literatur findet, weniger Zeit benötigen. Diese Beweise sind manchmal auch für Mathematiker ohne weitgehende komplexitätstheoretische Kenntnisse schwer zugänglich und verständlich. Entsprechend kann das Buch diesen Lesern ihre (Forschungs-)Arbeit wesentlich erleichtern.

4 Würden Sie das Buch weiterempfehlen?

Ja, ich würde das Buch jemandem, der auf dem Gebiet der Komplexitätstheorie und/oder Kryptologie arbeitet, unbedingt weiterempfehlen. Jemand, der auf dem Gebiet der Komplexitätstheorie arbeitet, kann von der Lektüre insofern profitieren, als er oder sie etwas über mögliche Anwendungen im Gebiet der Kryptologie in Erfahrung bringen kann. Umgekehrt kann jemand, der auf dem Gebiet der Kryptologie arbeitet, insofern profi-

tieren, als er oder sie eine mathematisch präzise Art und Weise lernen kann, wie man kryptografische Primitive einführen und deren Sicherheit beweisen kann. Das Buch wendet sich an Studenten und Studentinnen der Informatik, der Mathematik und des Ingenieurwesens. Natürlich kann das Buch auch Forschern, Dozierenden und Praktikern empfohlen werden. Schliesslich eignet sich das Buch auch zum Selbststudium. Vom Thema und Aufbau her ist das Buch so einzigartig, dass es in jede Bibliothek über Kryptologie oder Komplexitätstheorie gehört.

Der Gutachter ist Titularprofessor an der Universität Zürich (Schweiz).