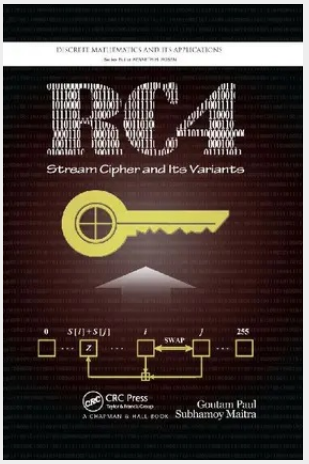
Paul / Maitra

RC4 Stream Cipher and Its Variants

RC4 Stream Cipher and Its Variants is the first book to fully cover the popular software stream cipher RC4. With extensive expertise in stream cipher cryptanalysis and RC4 research, the authors focus on the analysis and design issues of RC4. They also explore variants of RC4 and the eSTREAM finalist HC-128. After an introduction to the vast field of cryptology, the book reviews hardware and software stream ciphers and describes RC4. It presents a theoretical analysis of RC4 KSA, discussing biases of the permutation bytes toward secret key bytes and absolute values. The text explains how to reconstruct the secret key from known state information and analyzes the RC4 PRGA in detail, including a sketch of state recovery attacks. The book then describes three popular attacks on RC4: distinguishing attacks, Wired Equivalent Privacy (WEP) protocol attacks, and fault attacks. The authors also compare the advantages and disadvantages of several variants of RC4 and examine stream cipher HC-128, which is the next level of evolution after RC4 in the software stream cipher paradigm. The final chapter emphasizes the safe use of RC4. With open research problems in each chapter, this book offers a complete account of the most current research on RC4.

RC4 Stream Cipher and Its Variants is the first book to fully cover the popular software stream cipher RC4. With extensive expertise in stream cipher cryptanalysis and RC4 research, the authors focus on the analysis and design issues of RC4. They also explore variants of RC4 and the eSTREAM finalist HC-128.After an introduction to the vast field of cryptology, the book reviews hardware and software stream ciphers and describes RC4. It presents a theoretical analysis of RC4 KSA, discussing biases of the permutation bytes toward secret key bytes and absolute values. The text explains how to reconstruct the secret key from known state information and analyzes the RC4 PRGA in detail, including a sketch of state recovery attacks. The book then describes three popular attacks on RC4: distinguishing attacks, Wired Equivalent Privacy (WEP) protocol attacks, and fault attacks. The authors also compare the advantages and disadvantages of several variants of RC4 and examine stream cipher HC-128, which is the next level of evolution after RC4 in the software stream cipher paradigm. The final chapter emphasizes the safe use of RC4. With open research problems in each chapter, this book offers a complete account of the most current research on RC4.



90,70 €
90,70 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Artikelnummer: 9780367382162
Medium: Buch
ISBN: 978-0-367-38216-2
Verlag: CRC Press
Erscheinungstermin: 19.09.2019
Sprache(n): Englisch
Auflage: 1. Auflage 2019
Produktform: Kartoniert
Gewicht: 477 g
Seiten: 311
Format (B x H): 156 x 234 mm

Kundenservice Verlag Dr. Otto Schmidt KG
Neumannstraße 10, 40235 Düsseldorf | kundenservice@otto-schmidt.de | 0221-93738-997 (Inland)