MR2932936 94A60

Paul, Goutam (6-JDVP-NDM; Calcutta); **Maitra, Subhamoy** (6-ISI-NDM; Calcutta)

★RC4—stream cipher and its variants.

With a foreword by Bimal Roy.

Discrete Mathematics and its Applications (Boca Raton).

CRC Press, Boca Raton, FL, 2012. *xxvi*+285 *pp.* $89.95. *ISBN* 978-1-4398-3135-9

A stream cipher is one that encrypts a digital data stream one bit at a time with a keystream by termwise addition. It consists of a keystream generator which generates a pseudorandom keystream sequence from a short random key. As a typical stream cipher, RC4 was designed by R. Rivest in 1987. It was a propriety algorithm until 1994, and now has many industrial applications.

The book under review outlines the theory of RC4 stream ciphers and includes the main results of the authors' own investigations. It systematically summarizes the design principles of RC4 and its cryptographic security. After reviewing the description of RC4 and a theoretical analysis of the key scheduling algorithms and keystream generation, the authors introduce three popular attacks, i.e., distinguishing attacks, WEP (wired equivalent privacy) attacks and fault attacks, to indicate how RC4 resists malicious attacks. For applications and security considerations, byte-oriented and word-oriented variants of RC4 have been designed to remove some weaknesses of the original RC4. A new stream cipher HC-128, an RC4-like stream cipher, is also described in this book. At the end of each chapter, many important research problems are presented to promote further investigation.

This remarkable monograph is "the first one on RC4". The theory surrounding the development of RC4 is very helpful for the study of stream ciphers in general, as the authors say. The book will be of interest to scholars and students whose expertise lies in cryptography, applied mathematics, computer security, and so on. *Zhixiong Chen*