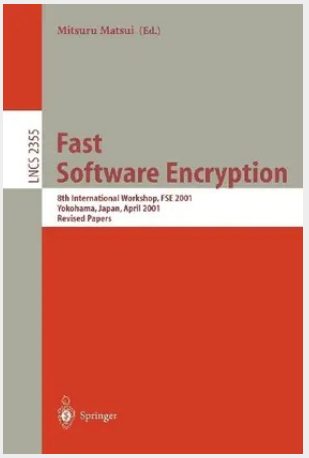
Matsui

Fast Software Encryption

8th International Workshop, FSE 2001 Yokohama, Japan, April 2-4, 2001, Revised Papers

Fast Software Encryption is an eight-year-old workshop on symmetric cryp- graphy, including the design and cryptanalysis of block and stream ciphers, as well as hash functions. The ?rst Fast Software Encryption Workshop was held in Cambridge in 1993, followed by Leuven in 1994, Cambridge in 1996, Haifa in 1997, Paris in 1998, Rome in 1999, and New York in 2000. This Fast Software Encryption Workshop, FSE 2001, was held from 2-4 April 2001 in Yokohama, Japan, in cooperation with the Institute of Industrial Science, of the University of Tokyo. This year a total of 46 papers were submitted to FSE 2001. After a t- month review process, 27 papers were accepted for presentation at the workshop. In addition, we were fortunate to be able to organize a special talk by Bart Preneel on the NESSIE project, a European initiative to evaluate cryptographic algorithms. The committee of this workshop was: General Chair Hideki Imai (The University of Tokyo) Program Committee Ross Anderson (Cambridge Univ.) Eli Biham (Technion) Cunsheng Ding (Singapore) Henri Gilbert (France Telecom) Dieter Gollman (Microsoft) Thomas Johansson (Lund Univ.) Lars Knudsen (Bergen Univ.) James Massey (Denmark) Mitsuru Matsui (Mitsubishi Electric, Chair) Kaisa Nyberg (Nokia) Bart Preneel (Katholieke Univ. Leuven) Bruce Schneier (Counterpane) We would like to thank all submitting authors and the committee members for their hard work. We are also appreciative of the ?nancial support provided by Mitsubishi Electric Corporation.

Fast Software Encryption is an eight-year-old workshop on symmetric cryp- graphy, including the design and cryptanalysis of block and stream ciphers, as well as hash functions. The ?rst Fast Software Encryption Workshop was held in Cambridge in 1993, followed by Leuven in 1994, Cambridge in 1996, Haifa in 1997, Paris in 1998, Rome in 1999, and New York in 2000. This Fast Software Encryption Workshop, FSE 2001, was held from 2-4 April 2001 in Yokohama, Japan, in cooperation with the Institute of Industrial Science, of the University of Tokyo. This year a total of 46 papers were submitted to FSE 2001. After a t- month review process, 27 papers were accepted for presentation at the workshop. In addition, we were fortunate to be able to organize a special talk by Bart Preneel on the NESSIE project, a European initiative to evaluate cryptographic algorithms. The committee of this workshop was: General Chair Hideki Imai (The University of Tokyo) Program Committee Ross Anderson (Cambridge Univ.) Eli Biham (Technion) Cunsheng Ding (Singapore) Henri Gilbert (France Telecom) Dieter Gollman (Microsoft) Thomas Johansson (Lund Univ.) Lars Knudsen (Bergen Univ.) James Massey (Denmark) Mitsuru Matsui (Mitsubishi Electric, Chair) Kaisa Nyberg (Nokia) Bart Preneel (Katholieke Univ. Leuven) Bruce Schneier (Counterpane) We would like to thank all submitting authors and the committee members for their hard work. We are also appreciative of the ?nancial support provided by Mitsubishi Electric Corporation.



53,49 €
49,99 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Artikelnummer: 9783540438694
Medium: Buch
ISBN: 978-3-540-43869-4
Verlag: Springer
Erscheinungstermin: 19.06.2002
Sprache(n): Englisch
Auflage: Erscheinungsjahr 2002
Serie: Lecture Notes in Computer Science
Produktform: Kartoniert
Gewicht: 1140 g
Seiten: 354
Format (B x H): 155 x 235 mm

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