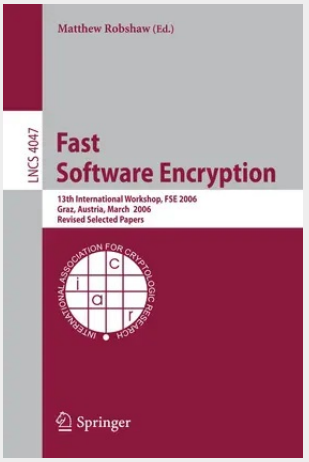
Robshaw

Fast Software Encryption

13th International Workshop, FSE 2006, Graz, Austria, March 15-17, 2006, Revised Selected Papers

Fast Software Encryption (FSE) 2006 is the 13th in a series of workshops on symmetric cryptography. It has been sponsored for the last ?ve years by the International Association for Cryptologic Research (IACR), and previous FSE workshops have been held around the world: 1993 Cambridge, UK 1994 Leuven, Belgium 1996 Cambridge, UK 1997 Haifa, Israel 1998 Paris, France 1999 Rome, Italy 2000 New York, USA 2001 Yokohama, Japan 2002 Leuven, Belgium 2003 Lund, Sweden 2004 New Delhi, India 2005 Paris, France The FSE workshop is devoted to research on fast and secure primitives for symmetric cryptography, including the design and analysis of block ciphers, stream ciphers, encryption schemes, analysis and evaluation tools, hash fu- tions, and message authentication codes. This year more than 100 papers were submitted to FSE for the ?rst time. After an extensive review by the ProgramCommittee, 27 papers were presented at the workshop. Of course, the programwould not have been complete without the invited speaker, and the presentation by Eli Biham on the early history of di? erential cryptanalysis was particularly appreciated by workshop attendees.

Fast Software Encryption (FSE) 2006 is the 13th in a series of workshops on symmetric cryptography. It has been sponsored for the last ?ve years by the International Association for Cryptologic Research (IACR), and previous FSE workshops have been held around the world: 1993 Cambridge, UK 1994 Leuven, Belgium 1996 Cambridge, UK 1997 Haifa, Israel 1998 Paris, France 1999 Rome, Italy 2000 New York, USA 2001 Yokohama, Japan 2002 Leuven, Belgium 2003 Lund, Sweden 2004 New Delhi, India 2005 Paris, France The FSE workshop is devoted to research on fast and secure primitives for symmetric cryptography, including the design and analysis of block ciphers, stream ciphers, encryption schemes, analysis and evaluation tools, hash fu- tions, and message authentication codes. This year more than 100 papers were submitted to FSE for the ?rst time. After an extensive review by the ProgramCommittee, 27 papers were presented at the workshop. Of course, the programwould not have been complete without the invited speaker, and the presentation by Eli Biham on the early history of di? erential cryptanalysis was particularly appreciated by workshop attendees.



53,49 €
49,99 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Artikelnummer: 9783540365976
Medium: Buch
ISBN: 978-3-540-36597-6
Verlag: Springer
Erscheinungstermin: 06.07.2006
Sprache(n): Englisch
Auflage: 1. Auflage 2006
Serie: Lecture Notes in Computer Science
Produktform: Kartoniert
Gewicht: 678 g
Seiten: 434
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)