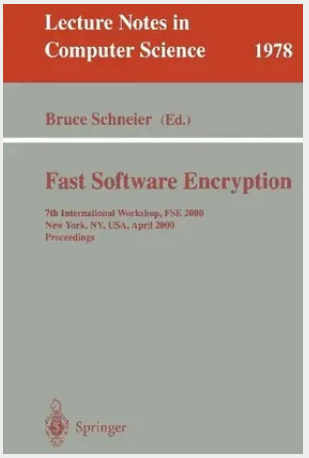
Schneier

Fast Software Encryption

7th International Workshop, FSE 2000, New York, NY, USA, April 10-12, 2000. Proceedings

Since 1993, cryptographic algorithm research has centered around the Fast So- ware Encryption (FSE) workshop. First held at Cambridge University with 30 attendees, it has grown over the years and has achieved worldwide recognition as a premiere conference. It has been held in Belgium, Israel, France, Italy, and, most recently, New York. FSE 2000 was the 7th international workshop, held in the United States for the rst time. Two hundred attendees gathered at the Hilton New York on Sixth Avenue, to hear 21 papers presented over the course of three days: 10{12 April 2000. These proceedings constitute a collection of the papers presented during those days. FSE concerns itself with research on classical encryption algorithms and - lated primitives, such as hash functions. This branch of cryptography has never been more in the public eye. Since 1997, NIST has been shepherding the Adv- ced Encryption Standard (AES) process, trying to select a replacement algorithm for DES. The rst AES conference, held in California the week before Crypto 98, had over 250 attendees. The second conference, held in Rome two days before FSE 99, had just under 200 attendees. The third AES conference was held in conjunction with FSE 2000, during the two days following it, at the same hotel.

Since 1993, cryptographic algorithm research has centered around the Fast So- ware Encryption (FSE) workshop. First held at Cambridge University with 30 attendees, it has grown over the years and has achieved worldwide recognition as a premiere conference. It has been held in Belgium, Israel, France, Italy, and, most recently, New York. FSE 2000 was the 7th international workshop, held in the United States for the rst time. Two hundred attendees gathered at the Hilton New York on Sixth Avenue, to hear 21 papers presented over the course of three days: 10{12 April 2000. These proceedings constitute a collection of the papers presented during those days. FSE concerns itself with research on classical encryption algorithms and - lated primitives, such as hash functions. This branch of cryptography has never been more in the public eye. Since 1997, NIST has been shepherding the Adv- ced Encryption Standard (AES) process, trying to select a replacement algorithm for DES. The rst AES conference, held in California the week before Crypto 98, had over 250 attendees. The second conference, held in Rome two days before FSE 99, had just under 200 attendees. The third AES conference was held in conjunction with FSE 2000, during the two days following it, at the same hotel.



53,49 €
49,99 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Artikelnummer: 9783540417286
Medium: Buch
ISBN: 978-3-540-41728-6
Verlag: Springer
Erscheinungstermin: 14.02.2001
Sprache(n): Englisch
Auflage: 1. Auflage 2001
Serie: Lecture Notes in Computer Science
Produktform: Kartoniert
Gewicht: 1020 g
Seiten: 324
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)