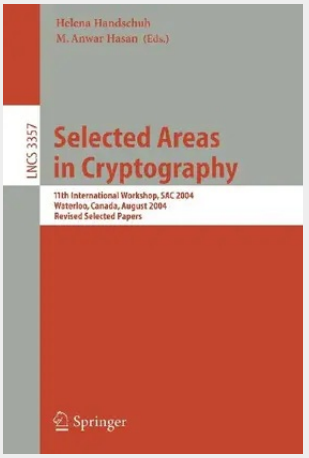
Handschuh / Hasan

Selected Areas in Cryptography

11th International Workshop, SAC 2004, Waterloo, Canada, August 9-10, 2004, Revised Selected Papers

SAC 2004 was the eleventh in a series of annual workshops on Selected Areas in Cryptography. This was the second time that the workshop was hosted by the University of Waterloo, Ontario, with previous workshops being held at Queen'sUniversityinKingston(1994,1996,1998and1999),CarletonUniversity in Ottawa (1995, 1997 and 2003), the Fields Institute in Toronto (2001) and Memorial University of Newfoundland in St. John's (2002). The primary intent of the workshop was to provide a relaxed atmosphere in which researchers in cryptography could present and discuss new work on selected areas of current interest. This year's themes for SAC were: – Design and analysis of symmetric key cryptosystems. – Primitives for symmetric key cryptography, including block and stream - phers, hash functions, and MAC algorithms. – E?cient implementation of cryptographic systems in public and symmetric key cryptography. – Cryptographic solutions for mobile (web) services. A record of 117 papers were submitted for consideration by the program committee. After an extensive review process, 25 papers were accepted for p- sentation at the workshop (two of these papers were merged). Unfortunately, many good papers could not be accommodated this year. These proceedings contain the revised versions of the 24 accepted papers. The revised versions were not subsequently checked for correctness. Also, we were very fortunate to have two invited speakers at SAC 2004. • Eli Biham arranged for some breaking news in his talk on "New Results on SHA-0 and SHA-1." This talk was designated as the Sta?ord Tavares L- ture.

SAC 2004 was the eleventh in a series of annual workshops on Selected Areas in Cryptography. This was the second time that the workshop was hosted by the University of Waterloo, Ontario, with previous workshops being held at Queen'sUniversityinKingston(1994,1996,1998and1999),CarletonUniversity in Ottawa (1995, 1997 and 2003), the Fields Institute in Toronto (2001) and Memorial University of Newfoundland in St. John's (2002). The primary intent of the workshop was to provide a relaxed atmosphere in which researchers in cryptography could present and discuss new work on selected areas of current interest. This year's themes for SAC were: - Design and analysis of symmetric key cryptosystems. - Primitives for symmetric key cryptography, including block and stream - phers, hash functions, and MAC algorithms. - E?cient implementation of cryptographic systems in public and symmetric key cryptography. - Cryptographic solutions for mobile (web) services. A record of 117 papers were submitted for consideration by the program committee. After an extensive review process, 25 papers were accepted for p- sentation at the workshop (two of these papers were merged). Unfortunately, many good papers could not be accommodated this year. These proceedings contain the revised versions of the 24 accepted papers. The revised versions were not subsequently checked for correctness. Also, we were very fortunate to have two invited speakers at SAC 2004. ¿ Eli Biham arranged for some breaking news in his talk on "New Results on SHA-0 and SHA-1." This talk was designated as the Sta?ord Tavares L- ture.



53,49 €
49,99 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Artikelnummer: 9783540243274
Medium: Buch
ISBN: 978-3-540-24327-4
Verlag: Springer
Erscheinungstermin: 31.01.2005
Sprache(n): Englisch
Auflage: 1. Auflage 2005
Serie: Lecture Notes in Computer Science
Produktform: Kartoniert
Gewicht: 1150 g
Seiten: 358
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)