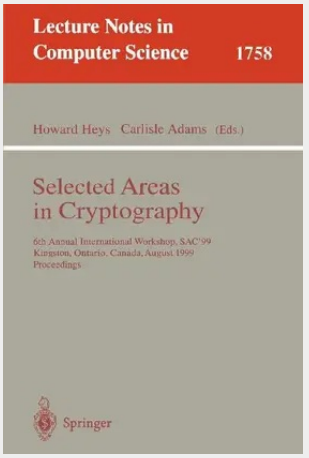
Heys / Adams

Selected Areas in Cryptography

SAC'99 was the sixth in a series of annual workshops on Selected Areas in Cryptography. Previous workshops were held at Carleton University in Ottawa (1995 and 1997) and at Queen's University in Kingston (1994, 1996, and 1998). The intent of the annual workshop is to provide a relaxed atmosphere in which researchers in cryptography can present and discuss new work on selected areas of current interest. The themes for the SAC'99 workshop were: { Design and Analysis of Symmetric Key Cryptosystems { E cient Implementations of Cryptographic Systems { Cryptographic Solutions for Web/Internet Security The timing of the workshop was particularly fortuitous as the announcement by NIST of the v e nalists for AES coincided with the rst morning of the workshop, precipitating lively discussion on the merits of the selection! A total of 29 papers were submitted to SAC'99 and, after a review process that had all papers reviewed by at least 3 referees, 17 were accepted and p- sented. As well, two invited presentations were given: one by Miles Smid from NIST entitled \From DES to AES: Twenty Years of Government Initiatives in Cryptography"and the other by Mike Reiter from Bell Labs entitled \Password Hardening with Applications to VPN Security". The program committee for SAC'99 consisted of the following members: Carlisle Adams, Tom Cusick, Howard Heys, Lars Knudsen, Henk Meijer, Luke O'Connor, Doug Stinson, Stao rd Tavares, and Serge Vaudenay.

SAC¿99 was the sixth in a series of annual workshops on Selected Areas in Cryptography. Previous workshops were held at Carleton University in Ottawa (1995 and 1997) and at Queen¿s University in Kingston (1994, 1996, and 1998). The intent of the annual workshop is to provide a relaxed atmosphere in which researchers in cryptography can present and discuss new work on selected areas of current interest. The themes for the SAC¿99 workshop were: { Design and Analysis of Symmetric Key Cryptosystems { E cient Implementations of Cryptographic Systems { Cryptographic Solutions for Web/Internet Security The timing of the workshop was particularly fortuitous as the announcement by NIST of the v e nalists for AES coincided with the rst morning of the workshop, precipitating lively discussion on the merits of the selection! A total of 29 papers were submitted to SAC¿99 and, after a review process that had all papers reviewed by at least 3 referees, 17 were accepted and p- sented. As well, two invited presentations were given: one by Miles Smid from NIST entitled \From DES to AES: Twenty Years of Government Initiatives in Cryptography"and the other by Mike Reiter from Bell Labs entitled \Password Hardening with Applications to VPN Security". The program committee for SAC¿99 consisted of the following members: Carlisle Adams, Tom Cusick, Howard Heys, Lars Knudsen, Henk Meijer, Luke O¿Connor, Doug Stinson, Stao rd Tavares, and Serge Vaudenay.



53,49 €
49,99 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Artikelnummer: 9783540671855
Medium: Buch
ISBN: 978-3-540-67185-5
Verlag: Springer
Erscheinungstermin: 23.02.2000
Sprache(n): Englisch
Auflage: 2000
Serie: Lecture Notes in Computer Science
Produktform: Kartoniert
Gewicht: 394 g
Seiten: 241
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)