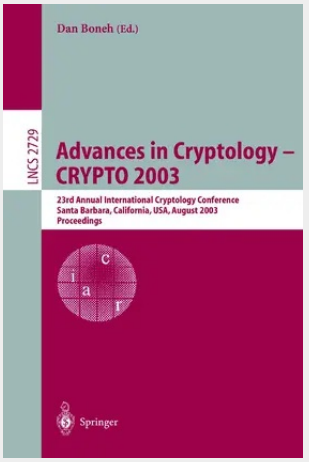
Boneh

Advances in Cryptology -- CRYPTO 2003

23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings

Crypto 2003, the 23rd Annual Crypto Conference, was sponsored by the Int- national Association for Cryptologic Research (IACR) in cooperation with the IEEE Computer Society Technical Committee on Security and Privacy and the Computer Science Department of the University of California at Santa Barbara. The conference received 169 submissions, of which the program committee selected 34 for presentation. These proceedings contain the revised versions of the 34 submissions that were presented at the conference. These revisions have not been checked for correctness, and the authors bear full responsibility for the contents of their papers. Submissions to the conference represent cutti- edge research in the cryptographic community worldwide and cover all areas of cryptography. Many high-quality works could not be accepted. These works will surely be published elsewhere. The conference program included two invited lectures. Moni Naor spoke on cryptographic assumptions and challenges. Hugo Krawczyk spoke on the ‘SI- and-MAc’approachtoauthenticatedDi?e-HellmananditsuseinthelKEpro- cols. The conference program also included the traditional rump session, chaired by Stuart Haber, featuring short, informal talks on late-breaking research news. Assembling the conference program requires the help of many many people. To all those who pitched in, I am forever in your debt. I would like to ?rst thank the many researchers from all over the world who submitted their work to this conference. Without them, Crypto could not exist. I thank Greg Rose, the general chair, for shielding me from innumerable logistical headaches, and showing great generosity in supporting my e?orts.

Crypto 2003, the 23rd Annual Crypto Conference, was sponsored by the Int- national Association for Cryptologic Research (IACR) in cooperation with the IEEE Computer Society Technical Committee on Security and Privacy and the Computer Science Department of the University of California at Santa Barbara. The conference received 169 submissions, of which the program committee selected 34 for presentation. These proceedings contain the revised versions of the 34 submissions that were presented at the conference. These revisions have not been checked for correctness, and the authors bear full responsibility for the contents of their papers. Submissions to the conference represent cutti- edge research in the cryptographic community worldwide and cover all areas of cryptography. Many high-quality works could not be accepted. These works will surely be published elsewhere. The conference program included two invited lectures. Moni Naor spoke on cryptographic assumptions and challenges. Hugo Krawczyk spoke on the ‘SI- and-MAc’approachtoauthenticatedDi?e-HellmananditsuseinthelKEpro- cols. The conference program also included the traditional rump session, chaired by Stuart Haber, featuring short, informal talks on late-breaking research news. Assembling the conference program requires the help of many many people. To all those who pitched in, I am forever in your debt. I would like to ?rst thank the many researchers from all over the world who submitted their work to this conference. Without them, Crypto could not exist. I thank Greg Rose, the general chair, for shielding me from innumerable logistical headaches, and showing great generosity in supporting my e?orts.



106,99 €
99,99 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Artikelnummer: 9783540406747
Medium: Buch
ISBN: 978-3-540-40674-7
Verlag: Springer
Erscheinungstermin: 04.08.2003
Sprache(n): Englisch
Auflage: 1. Auflage 2003
Serie: Lecture Notes in Computer Science
Produktform: Kartoniert
Gewicht: 979 g
Seiten: 636
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)