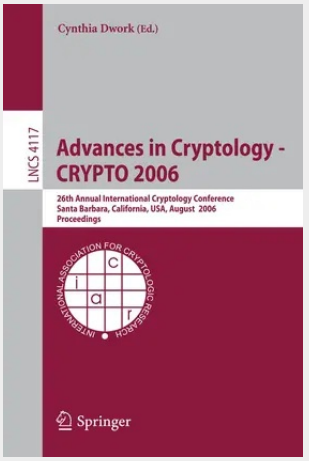
Dwork

Advances in Cryptology - CRYPTO 2006

26th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 2006, Proceedings



This book constitutes the refereed proceedings of the 26th Annual International Cryptology Conference, CRYPTO 2006, held in Santa Barbara, California, USA in August 2006. The 34 revised full papers presented together with 2 invited lectures were carefully reviewed and selected from 250 submissions. The papers address all current foundational, theoretical and research aspects of cryptology, cryptography, and cryptanalysis as well as advanced applications.

These are the proceedings of Crypto 2006, the 26th Annual International Cr- tology Conference. The conference was sponsored by the International Assoc- tion of Cryptologic Research, in cooperation with the IEEE Computer Society Technical Committee on Security and Privacy, and the Computer Science - partment of the University of California, Santa Barbara. The conference was held in Santa Barbara, California, August 20–24, 2006. The conference received 220 submissions, out of which the Program C- mittee selected 34 for presentation. Submission and selection of papers was done ´ using the IChair sofware, developed at the Ecole Polytechnique F´ ed´ erale de Lausanne (EPFL) by Thomas Baign` eres and Matthieu Finiasz. Aided in part by comments from the committee and external reviewers, the authors of - cepted papers had roughly six weeks in which to prepare ?nal versions for these proceedings. These were not subject to editorial review. The committee chose “On the Power of the Randomized Iterate,” by Iftach Haitner, Danny Harnik, and Omer Reingold, to receive the Best Paper award. ThecommitteealsoinvitedOdedRegevandDavidWagnertospeakontopics of their choice. Their talks were entitled, respectively, “Lattice-Based Crypt- raphy” and “Cryptographic Protocols for Electronic Voting.” We continued the tradition of a “Rump Session” of very brief presentations. The cryptology community provides a collaborative and supportive envir-
mentforexcitingresearch,andthesuccessofpreviousCryptoconferencesfosters enthusiasm for participation in subsequent ones. I am deeply grateful to all the authors who submitted papers, not only for their contribution to this conference but also for maintaining this tradition.

53,49 €
49,99 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Artikelnummer: 9783540374329
Medium: Buch
ISBN: 978-3-540-37432-9
Verlag: Springer
Erscheinungstermin: 08.08.2006
Sprache(n): Englisch
Auflage: 1. Auflage 2006
Serie: Lecture Notes in Computer Science
Produktform: Kartoniert
Gewicht: 1070 g
Seiten: 622
Format (B x H): 152 x 229 mm