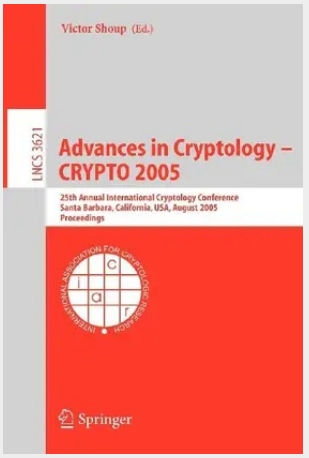
Shoup

Advances in Cryptology - CRYPTO 2005

25th Annual International Cryptology Conference, Santa Barbara, California, USA, August 14-18, 2005, Proceedings

These are the proceedings of Crypto 2005, the 25th Annual International Cr- tology Conference. The conference was sponsored by the International Assoc- tion for Cryptologic Research (IACR) in cooperation with the IEEE Computer ScienceTechnicalCommitteeonSecurityandPrivacyandtheComputerScience DepartmentoftheUniversityofCaliforniaatSantaBarbara.Theconferencewas held in Santa Barbara, California, August 14–18, 2005. Theconferencereceived178submissions,outofwhichtheprogramcommittee selected33forpresentation.Theselectionprocesswascarriedoutbytheprogram committee via an “online” meeting. The authors of selected papers had a few weeks to prepare ?nal versions of their papers, aided by comments from the reviewers. However, most of these revisions were not subject to any editorial review. This year, a “Best Paper Award” was given to Xiaoyun Wang, Yiqun Lisa Yin, and Hongbo Yu, for their paper “Finding Collisions in the Full SHA-1.” The conference program included two invited lectures. Ralph Merkle del- ered an IACR Distinguished Lecture, entitled “The Development of Public Key Cryptography:a PersonalView; and Thoughts on Nanotechnology.”Dan Boneh gave an invited talk, entitled “Bilinear Maps in Cryptography.” We continued the tradition of a “rump session,” featuring short, informal presentations (usually serious, sometimes entertaining, and occasionally both). ˜ The rump session was chaired this year by Phong Q. Nguyˆ en.

These are the proceedings of Crypto 2005, the 25th Annual International Cr- tology Conference. The conference was sponsored by the International Assoc- tion for Cryptologic Research (IACR) in cooperation with the IEEE Computer ScienceTechnicalCommitteeonSecurityandPrivacyandtheComputerScience DepartmentoftheUniversityofCaliforniaatSantaBarbara.Theconferencewas held in Santa Barbara, California, August 14¿18, 2005. Theconferencereceived178submissions,outofwhichtheprogramcommittee selected33forpresentation.Theselectionprocesswascarriedoutbytheprogram committee via an ¿online¿ meeting. The authors of selected papers had a few weeks to prepare ? nal versions of their papers, aided by comments from the reviewers. However, most of these revisions were not subject to any editorial review. This year, a ¿Best Paper Award¿ was given to Xiaoyun Wang, Yiqun Lisa Yin, and Hongbo Yu, for their paper ¿Finding Collisions in the Full SHA-1.¿ The conference program included two invited lectures. Ralph Merkle del- ered an IACR Distinguished Lecture, entitled ¿The Development of Public Key Cryptography:a PersonalView; and Thoughts on Nanotechnology.¿Dan Boneh gave an invited talk, entitled ¿Bilinear Maps in Cryptography.¿ We continued the tradition of a ¿rump session,¿ featuring short, informal presentations (usually serious, sometimes entertaining, and occasionally both). ¿ The rump session was chaired this year by Phong Q. Nguy¿ en.



53,49 €
49,99 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Artikelnummer: 9783540281146
Medium: Buch
ISBN: 978-3-540-28114-6
Verlag: Springer
Erscheinungstermin: 01.08.2005
Sprache(n): Englisch
Auflage: 2005
Serie: Lecture Notes in Computer Science
Produktform: Kartoniert
Gewicht: 1800 g
Seiten: 572
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)