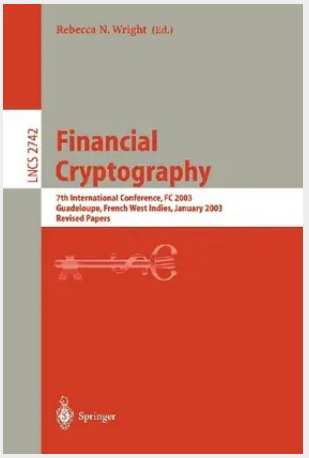
Wright

Financial Cryptography

7th International Conference, FC 2003, Guadeloupe, French West Indies, January 27-30, 2003, Revised Papers



53,49 €
49,99 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

The 7th Annual Financial Cryptography Conference was held January 27–30, 2003, in Guadeloupe, French West Indies. Financial Cryptography is organized by the International Financial Cryptography Association. Financial Cryptography 2003 received 54 paper submissions, of which one was withdrawn. The remaining papers were carefully reviewed by at least three members of the program committee. The program committee selected 17 papers for inclusion in the conference, revised versions of which are included in this proceedings. In addition to the submitted papers, the program included interesting and entertaining invited talks by Tim Jones on digital cash and by Richard Field on the interactions between technology and the United Nations. There were also several panels, on micropayments, economics of security, and trusted computing platforms, some of which are represented by contributions in these proceedings, and a rump session chaired by Juan Garay. We thank the program committee (listed on the next page) for their hard work in selecting the program from these papers. We also thank the external referees who helped with the reviewing task: N. Asokan, Danny Bickson, -manuel Bresson, Dario Catalano, Xuhua Ding, Louis Granboulan, Stuart Haber, Amir Herzberg, Bill Horne, Russ Housley, Yongdae Kim, Brian LaMacchia, Phil MacKenzie, Maithili Narasimha, Phong Nguyen, Kaisa Nyberg, David Poi- cheval, Tomas Sander, Yaron Sella, Mike Szydlo, Anat Talmy, Ahmed Tew?k, Susanne Wetzel, Shouhuai Xu, and Jeong Yi. (Apologies for any omissions - advertent.

Micropayment and E-cash.- Using Trust Management to Support Transferable Hash-Based Micropayments.- A Micro-Payment Scheme Encouraging Collaboration in Multi-hop Cellular Networks.- On the Anonymity of Fair Offline E-cash Systems.- Retrofitting Fairness on the Original RSA-Based E-cash.- Panel: Does Anyone Really Need MicroPayments?.- Does Anyone Really Need MicroPayments?.- The Case Against Micropayments.- Security, Anonymity, and Privacy.- On the Economics of Anonymity.- Squealing Euros: Privacy Protection in RFID-Enabled Banknotes.- How Much Security Is Enough to Stop a Thief?.- Attacks.- Cryptanalysis of the OTM Signature Scheme from FC'02.- "Man in the Middle" Attacks on Bluetooth.- Fault Based Cryptanalysis of the Advanced Encryption Standard (AES).- Panel: Economics of Security.- Economics, Psychology, and Sociology of Security.- Fair Exchange.- Timed Fair Exchange of Standard Signatures.- Asynchronous Optimistic Fair Exchange Based on Revocable Items.- Auctions.- Fully Private Auctions in a Constant Number of Rounds.- Secure Generalized Vickrey Auction Using Homomorphic Encryption.- Panel: Trusted Computing Platforms.- Trusted Computing Platforms: The Good, the Bad, and the Ugly.- On TCPA.- Cryptographic Tools and Primitives.- On The Computation-Storage Trade-Offs of Hash Chain Traversal.- Verifiable Secret Sharing for General Access Structures, with Application to Fully Distributed Proxy Signatures.- Non-interactive Zero-Sharing with Applications to Private Distributed Decision Making.

Artikelnummer: 9783540406631
Medium: Buch
ISBN: 978-3-540-40663-1
Verlag: Springer
Erscheinungstermin: 29.07.2003
Sprache(n): Englisch
Auflage: 1. Auflage 2003
Serie: Lecture Notes in Computer Science
Produktform: Kartoniert
Gewicht: 1040 g
Seiten: 328
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)