

Table of Contents

E-Voting without 'Cryptography'	1
<i>Dahlia Malkhi, Ofer Margo, Elan Pavlov</i>	
An Implementation of a Universally Verifiable Electronic Voting Scheme Based on Shuffling	16
<i>Jun Furukawa, Hiroshi Miyauchi, Kengo Mori, Satoshi Obana, Kazue Sako</i>	
Financial Instruments in Recommendation Mechanisms	31
<i>Markus Jakobsson</i>	
Secure Combinatorial Auctions by Dynamic Programming with Polynomial Secret Sharing	44
<i>Koutarou Suzuki, Makoto Yokoo</i>	
A Second-Price Sealed-Bid Auction with Verifiable Discriminant of p_0 -th Root	57
<i>Kazumasa Omote, Atsuko Miyaji</i>	
A Two-Server, Sealed-Bid Auction Protocol	72
<i>Ari Juels, Michael Szydlo</i>	
Secure Vickrey Auctions without Threshold Trust	87
<i>Helger Lipmaa, N. Asokan, Valtteri Niemi</i>	
Almost Optimal Hash Sequence Traversal	102
<i>Don Coppersmith, Markus Jakobsson</i>	
Cryptographic Primitives Enforcing Communication and Storage Complexity	120
<i>Philippe Golle, Stanislaw Jarecki, Ilya Mironov</i>	
CryptoComputing with Rationals	136
<i>Pierre-Alain Fouque, Jacques Stern, Geert-Jan Wackers</i>	
Privacy Tradeoffs: Myth or Reality?	147
<i>Rebecca N. Wright, L. Jean Camp, Ian Goldberg, Ronald L. Rivest, Graham Wood</i>	
An Improved Fast Signature Scheme without Online Multiplication	152
<i>Takeshi Okamoto, Mitsuru Tada, Atsuko Miyaji</i>	
Timed Release of Standard Digital Signatures	168
<i>Juan A. Garay, Markus Jakobsson</i>	

VIII Table of Contents

Quasi-Efficient Revocation of Group Signatures	183
<i>Giuseppe Ateniese, Dawn Song, Gene Tsudik</i>	
The Dark Side of Threshold Cryptography	198
<i>Shouhuai Xu and Moti Yung</i>	
Split-and-Delegate: Threshold Cryptography for the Masses	220
<i>Daniel E. Geer, Jr., Moti Yung</i>	
Redistribution of Mechanical Secret Shares	238
<i>Yvo Desmedt, Rei Safavi-Naini, Huaxiong Wang</i>	
Reliable MIX Cascade Networks through Reputation	253
<i>Roger Dingledine, Paul Syverson</i>	
Offline Payments with Auditable Tracing	269
<i>Dennis Kügler, Holger Vogt</i>	
Fileteller: Paying and Getting Paid for File Storage	282
<i>John Ioannidis, Sotiris Ioannidis, Angelos D. Keromytis, Vassilis Prevelakis</i>	
Author Index	301