

Table of Contents

Authentication I

Commitment and Authentication Systems	1
<i>Alexandre Pinto, André Souto, Armando Matos, and Luís Antunes</i>	
Unconditionally Secure Blind Signatures	23
<i>Yuki Hara, Takenobu Seito, Junji Shikata, and Tsutomu Matsumoto</i>	

Keynote Lecture

Random Systems: Theory and Applications	44
<i>Ueli Maurer</i>	

Group Cryptography

Optimising SD and LSD in Presence of Non-uniform Probabilities of Revocation	46
<i>Paolo D'Arco and Alfredo De Santis</i>	
Trade-Offs in Information-Theoretic Multi-party One-Way Key Agreement	65
<i>Renato Renner, Stefan Wolf, and Jürg Wullschlegel</i>	
Improvement of Collusion Secure Convolutional Fingerprinting Information Codes	76
<i>Joan Tomàs-Buliart, Marcel Fernandez, and Miguel Soriano</i>	

Private and Reliable Message Transmission

On Exponential Lower Bound for Protocols for Reliable Communication in Networks	89
<i>K. Srinathan, C. Pandu Rangan, and R. Kumaresan</i>	
Almost Secure (1-Round, n -Channel) Message Transmission Scheme	99
<i>Kaoru Kurosawa and Kazuhiro Suzuki</i>	

Invited Talk

Construction Methodology of Unconditionally Secure Signature Schemes	113
<i>Junji Shikata</i>	

Authentication II

New Results on Unconditionally Secure Multi-receiver Manual Authentication	115
<i>Shuhong Wang and Reihaneh Safavi-Naini</i>	
Unconditionally Secure Chaffing-and-Winning for Multiple Use	133
<i>Wataru Kitada, Goichiro Hanaoka, Kanta Matsuura, and Hideki Imai</i>	

Invited Talk

Introduction to Quantum Information Theory	146
<i>Iordanis Kerenidis</i>	

Secret Sharing

Strongly Multiplicative Hierarchical Threshold Secret Sharing	148
<i>Emilia Käsper, Ventzislav Nikov, and Svetla Nikova</i>	
Secret Sharing Comparison by Transformation and Rotation.....	169
<i>Tord Ingolf Reistad and Tomas Toft</i>	

Invited Talk

Anonymous Quantum Communication (Extended Abstract)	181
<i>Gilles Brassard, Anne Broadbent, Joseph Fitzsimons, Sébastien Gambs, and Alain Tapp</i>	

Applications of Information Theory

Efficient Oblivious Transfer Protocols Achieving a Non-zero Rate from Any Non-trivial Noisy Correlation.....	183
<i>Hideki Imai, Kirill Morozov, and Anderson C.A. Nascimento</i>	
Cryptographic Security of Individual Instances.....	195
<i>L. Antunes, S. Laplante, A. Pinto, and L. Salvador</i>	
Author Index	211