

# Table of Contents

## Boolean Functions

Boolean Function Design Using Hill Climbing Methods <i>William Millan, Andrew Clark, and Ed Dawson</i> .....	1
Enumeration of Correlation Immune Boolean Functions <i>Subhamoy Maitra and Palash Sarkar</i> .....	12
On the Symmetric Property of Homogeneous Boolean Functions <i>Chengxin Qu, Jennifer Seberry, and Josef Pieprzyk</i> .....	26

## Key Management

Publicly Verifiable Key Escrow with Limited Time Span <i>Kapali Viswanathan, Colin Boyd, and Ed Dawson</i> .....	36
Accelerating Key Establishment Protocols for Mobile Communication <i>Seungwon Lee, Seong-Min Hong, Hyunsoo Yoon, and Yookun Cho</i> .....	51
Conference Key Agreement from Secret Sharing <i>Chih-Hung Li and Josef Pieprzyk</i> .....	64

## Cryptanalysis

On $m$ -Permutation Protection Scheme Against Modification Attack <i>W. W. Fung and J. W. Gray, III</i> .....	77
Inversion Attack and Branching <i>Jovan Dj. Golić, Andrew Clark, and Ed Dawson</i> .....	88

## Signatures

Fail-Stop Threshold Signature Schemes Based on Elliptic Curves <i>Willy Susilo, Rei Safavi-Naini, and Josef Pieprzyk</i> .....	103
Divertible Zero-Knowledge Proof of Polynomial Relations and Blind Group Signature <i>Khanh Quoc Nguyen, Yi Mu, and Vijay Varadharajan</i> .....	117
Repudiation of Cheating and Non-repudiation of Zhang's Proxy Signature Schemes <i>Hossein Ghodosi and Josef Pieprzyk</i> .....	129

## **RSA Cryptosystems**

On the Security of an RSA Based Encryption Scheme <i>Siguna Müller</i> .....	135
Generalised Cycling Attacks on RSA and Strong RSA Primes <i>Marc Gysin and Jennifer Seberry</i> .....	149
RSA Acceleration with Field Programmable Gate Arrays <i>Alexander Tiountchik and Elena Trichina</i> .....	164

## **Group Cryptography**

Changing Thresholds in the Absence of Secure Channels <i>Keith M. Martin, Josef Pieprzyk, Rei Safavi-Naini, and Huaxiong Wang</i> .	177
A Self-Certified Group-Oriented Cryptosystem Without a Combiner <i>Shahrokh Saeednia and Hossein Ghodosi</i> .....	192

## **Network Security**

Companion Viruses and the Macintosh: Threats and Countermeasures <i>Jeffrey Horton and Jennifer Seberry</i> .....	202
An Implementation of a Secure Version of NFS Including RBAC <i>Paul Ashley, Bradley Broom, and Mark Vandenwauwer</i> .....	213

## **Electronic Commerce**

Group Signatures and Their Relevance to Privacy-Protecting Off-Line Electronic Cash Systems <i>Jacques Traoré</i> .....	228
Efficient Electronic Cash Using Batch Signatures <i>Colin Boyd, Ernest Foo, and Chris Pavlovski</i> .....	244
Evolution of Fair Non-repudiation with TTP <i>Jianying Zhou, Robert Deng, and Feng Bao</i> .....	258

## **Access Control**

Authorization in Object Oriented Databases <i>Yun Bai and Vijay Varadharajan</i> .....	270
An Analysis of Access Control Models <i>Gregory Saunders, Michael Hitchens, and Vijay Varadharajan</i> .....	281

**Odds and Ends**

Efficient Identity Based Parameter Selection for Elliptic Curve  
Cryptosystems  
*Arjen K. Lenstra* ..... 294

Characterization of Optimal Authentication Codes with Arbitration  
*Dingyi Pei, Yuqiang Li, Yejing Wang, and Rei Safavi-Naini* ..... 303

A Functional Cryptosystem Using a Group Action  
*Akihiro Yamamura* ..... 314

**Author Index** ..... 327

Information Security and Privacy

4th Australasian Conference, ACISP'99, Wollongong,

NSW, Australia, April 7-9, 1999, Proceedings

Pieprzyk, J.; Safavi-Naini, R.; Seberry, J. (Eds.)

1999, XII, 332 p., Softcover

ISBN: 978-3-540-65756-9