

Table of Contents

Invited Talk

Revisiting Software Protection	1
<i>Paul C. van Oorschot</i>	

Network Security

Enabling Shared Audit Data	14
<i>Adrian Baldwin, Simon Shiu</i>	
Cryptographically Generated Addresses (CGA)	29
<i>Tuomas Aura</i>	
Validating and Securing Spontaneous Associations between Wireless Devices	44
<i>Tim Kindberg, Kan Zhang</i>	
Single Sign-On Using Trusted Platforms	54
<i>Andreas Pashalidis, Chris J. Mitchell</i>	

Public-Key Algorithms

Easy Verifiable Primitives and Practical Public Key Cryptosystems	69
<i>David Galindo, Sebastià Martín, Paz Morillo, Jorge L. Villar</i>	
Reactively Secure Signature Schemes	84
<i>Michael Backes, Birgit Pfizmann, Michael Waidner</i>	
Validating Digital Signatures without TTP's Time-Stamping and Certificate Revocation	96
<i>Jianying Zhou, Feng Bao, Robert Deng</i>	
A Fast Signature Scheme Based on New On-line Computation	111
<i>Takeshi Okamoto, Hirofumi Katsuno, Eiji Okamoto</i>	

Cryptographic Protocols

Distributed RSA Signature Schemes for General Access Structures	122
<i>Javier Herranz, Carles Padró, Germán Sáez</i>	
Divisible Voting Scheme	137
<i>Natsuki Ishida, Shin'ichiro Matsuo, Wakaha Ogata</i>	

Unconditionally Secure Homomorphic Pre-distributed Bit Commitment and Secure Two-Party Computations	151
<i>Anderson C.A. Nascimento, Joern Mueller-Quade, Akira Otsuka, Goichiro Hanaoka, Hideki Imai</i>	

The Design and Implementation of Protocol-Based Hidden Key Recovery	165
<i>Eu-Jin Goh, Dan Boneh, Benny Pinkas, Philippe Golle</i>	

Invited Talk

Intrinsic Limitations of Digital Signatures and How to Cope with Them .	180
<i>Ueli Maurer</i>	

Protocol Attacks

On the Security of Fair Non-repudiation Protocols	193
<i>Sigrid Gürgens, Carsten Rudolph, Holger Vogt</i>	

Security Analysis of a Password Authenticated Key Exchange Protocol ..	208
<i>Feng Bao</i>	

Attacks on Public Key Algorithms

Zero-Value Point Attacks on Elliptic Curve Cryptosystem	218
<i>Toru Akishita, Tsuyoshi Takagi</i>	

Cryptanalysis of an Algebraic Privacy Homomorphism	234
<i>David Wagner</i>	

Analysis of the Insecurity of ECMQV with Partially Known Nonces	240
<i>Peter J. Leadbitter, Nigel P. Smart</i>	

Block Ciphers

Hardware-Focused Performance Comparison for the Standard Block Ciphers AES, Camellia, and Triple-DES	252
<i>Akashi Satoh, Sumio Morioka</i>	

A Note on Weak Keys of PES, IDEA, and Some Extended Variants	267
<i>Jorge Nakahara Jr., Bart Preneel, Joos Vandewalle</i>	

Foundations of Differential Cryptanalysis in Abelian Groups	280
<i>Tomasz Tyksiński</i>	

Authorization

Trust and Authorization in Pervasive B2E Scenarios	295
<i>Laurent Bussard, Yves Roudier, Roger Kilian-Kehr, Stefano Crosta</i>	

A Logic Model for Temporal Authorization Delegation with Negation	310
<i>Chun Ruan, Vijay Varadharajan, Yan Zhang</i>	

Watermarking

Zero-Distortion Authentication Watermarking	325
<i>Yongdong Wu</i>	
Designated Verification of Non-invertible Watermark	338
<i>Hyejoung Yoo, Hyungwoo Lee, Sangjin Lee, Jongin Lim</i>	

Software Security

Proactive Software Tampering Detection	352
<i>Hongxia Jin, Jeffery Lotspiech</i>	
Run-Time Support for Detection of Memory Access Violations to Prevent Buffer Overflow Exploits	366
<i>Pramod Ramarao, Akhilesh Tyagi, Gyungho Lee</i>	
Towards a Business Process-Driven Framework for Security Engineering with the UML	381
<i>José L. Vivas, José A. Montenegro, Javier López</i>	

Codes and Related Issues

Error Correcting and Complexity Aspects of Linear Secret Sharing Schemes	396
<i>Yvo Desmedt, Kaoru Kurosawa, Tri Van Le</i>	
Systematic Treatment of Collusion Secure Codes: Security Definitions and Their Relations	408
<i>Katsunari Yoshioka, Junji Shikata, Tsutomu Matsumoto</i>	
Short c -Secure Fingerprinting Codes	422
<i>Tri Van Le, Mike Burmester, Jiangyi Hu</i>	
The Role of Arbiters in Asymmetric Authentication Schemes	428
<i>Goichiro Hanaoka, Junji Shikata, Yumiko Hanaoka, Hideki Imai</i>	

Author Index	443
------------------------	-----

Information Security

6th International Conference, ISC 2003, Bristol, UK,

October 1-3, 2003, Proceedings

Boyd, C.; Mao, W. (Eds.)

2003, XII, 448 p., Softcover

ISBN: 978-3-540-20176-2