Table of Contents

Invited Talk

All Sail, No Anchor III: Risk Aggregation and Time's Arrow 1
Bob Blakley, G.R. Blakley

Network Security

Traversing Middleboxes with the Host Identity Protocol 17
Hannes Tschofenig, Andrei Gurtov, Jukka Ylitalo, Aarthi Nagarajan, Murugaraj Shanmugam

An Investigation of Unauthorised Use of Wireless Networks in Adelaide, South Australia 29
Phillip Pudney, Jill Slay

An Efficient Solution to the ARP Cache Poisoning Problem 40
Vipul Goyal, Rohit Tripathy

Cryptanalysis

On Stern's Attack Against Secret Truncated Linear Congruential Generators 52
Scott Contini, Igor E. Shparlinski

On the Success Probability of χ^2-attack on RC6 61
Atsuko Miyaji, Yuuki Takano

Solving Systems of Differential Equations of Addition.................. 75
Souradyuti Paul, Bart Preneel

Group Communications

A Tree Based One-Key Broadcast Encryption Scheme with Low Computational Overhead 89
Tomoyuki Asano, Kazuya Kamio

Dynamic Group Key Agreement in Tree-Based Setting................. 101
Ratna Dutta, Rana Barua

Immediate Data Authentication for Multicast in Resource Constrained Network 113
C.K. Wong, Agnes Chan

Elliptic Curve Cryptography

Redundant Trinomials for Finite Fields of Characteristic 2 122
Christophe Doche

Efficient Tate Pairing Computation for Elliptic Curves over Binary Fields 134
Soonhak Kwon

A Complete Divisor Class Halving Algorithm for Hyperelliptic Curve Cryptosystems of Genus Two 146
Izuru Kitamura, Masanobu Katagi, Tsuyoshi Takagi

Mobile Security

Using “Fair Forfeit” to Prevent Truncation Attacks on Mobile Agents . . . 158
Min Yao, Kun Peng, Ed Dawson

An Improved Execution Integrity Solution for Mobile Agents 170
Michelangelo Giansiracusa, Selwyn Russell, Andrew Clark, John Hynd

RFID Guardian: A Battery-Powered Mobile Device for RFID Privacy Management 184
Melanie R. Rieback, Bruno Crispo, Andrew S. Tanenbaum

Side Channel Attacks

Enhanced DES Implementation Secure Against High-Order Differential Power Analysis in Smartcards 195
Jiqiang Lv, Yongfei Han

Improved Zero Value Attack on XTR 207
Régis Bevan

Efficient Representations on Koblitz Curves with Resistance to Side Channel Attacks 218
Katsuyuki Okeya, Tsuyoshi Takagi, Camille Vuillaume

Evaluation and Biometrics

SIFA: A Tool for Evaluation of High-Grade Security Devices 230
Tim McComb, Luke Wildman

Cancelable Key-Based Fingerprint Templates 242
Russell Ang, Rei Safavi–Naini, Luke McAven

Public Key Cryptosystems

Hybrid Signcryption Schemes with Insider Security 253
Alexander W. Dent

On the Possibility of Constructing Meaningful Hash Collisions for Public Keys 267
Arjen Lenstra, Benne de Weger

Tunable Balancing of RSA 280
Steven D. Galbraith, Chris Heneghan, James F. McKee

Access Control I

Key Management for Role Hierarchy in Distributed Systems 293
Celia Li, Cungang Yang, Richard Cheung

A Formalization of Distributed Authorization with Delegation 303
Shujing Wang, Yan Zhang

Signatures I

Two Improved Partially Blind Signature Schemes from Bilinear Pairings . 316
Sherman S.M. Chow, Lucas C.K. Hui, S.M. Yiu, K.P. Chow

On the Security of Nominative Signatures 329
Willy Susilo, Yi Mu

Invited Talk

Who Goes There? Internet Banking: A Matter of Risk and Reward 336
Adrian McCullagh, William Caelli

Access Control II

Role Activation Management in Role Based Access Control 358
Richard W.C. Lui, Sherman S.M. Chow, Lucas C.K. Hui, S.M. Yiu

VO-Sec: An Access Control Framework for Dynamic Virtual Organization 370
Hai Jin, Weizhong Qiang, Xuanhua Shi, Deqing Zou

Threshold Cryptography

An Efficient Implementation of a Threshold RSA Signature Scheme 382
Brian King

GBD Threshold Cryptography with an Application to RSA Key Recovery 394
Chris Steketee, Jaimee Brown, Juan M. González Nieto, Paul Montague

An $(n-t)$-out-of-n Threshold Ring Signature Scheme 406
Toshiyuki Isshiki, Keisuke Tanaka

Protocols I

Deposit-Case Attack Against Secure Roaming 417
Guomin Yang, Duncan S. Wong, Xiaotie Deng

Security Requirements for Key Establishment Proof Models: Revisiting Bellare–Rogaway and Jeong–Katz–Lee Protocols 429
Kim-Kwang Raymond Choo, Yvonne Hitchcock

Group Signatures

Group Signature Schemes with Membership Revocation for Large Groups 443
Toru Nakanishi, Fumiaki Kubooka, Naoto Hamada, Nobuo Funabiki

An Efficient Group Signature Scheme from Bilinear Maps 455
Jun Furukawa, Hideki Imai

Group Signature Where Group Manager, Members and Open Authority Are Identity-Based 468
Victor K. Wei, Tsz Hon Yuen, Fangguo Zhang

Protocols II

Analysis of the HIP Base Exchange Protocol 481
Tuomas Aura, Aarthi Nagarajan, Andrei Gurtov

ID-based Authenticated Key Agreement for Low-Power Mobile Devices .. 494
Kyu Young Choi, Jung Yeon Hwang, Dong Hoon Lee, In Seog Seo

Signatures II

On the Security of Two Key-Updating Signature Schemes 506
Xingyang Guo, Quan Zhang, Chaojing Tang

Building Secure Tame-like Multivariate Public-Key Cryptosystems: The New TTS 518
Bo-Yin Yang, Jiun-Ming Chen

Invited Talk

Potential Impacts of a Growing Gap Between Theory and Practice in Information Security 532
Yvo Desmedt

Credentials

Security Analysis and Fix of an Anonymous Credential System 537
Yanjiang Yang, Feng Bao, Robert H. Deng

Counting Abuses Using Flexible Off-line Credentials 548
Kemal Bicakci, Bruno Crispo, Andrew S. Tanenbaum

Symmetric Cryptography

Cryptanalysis of Two Variants of PCBC Mode When Used for Message Integrity 560
Chris J. Mitchell

New Cryptographic Applications of Boolean Function Equivalence Classes 572
William L. Millan

Author Index 585

Springer

http://www.springer.com/978-3-540-26547-4

Information Security and Privacy
10th Australasian Conference, ACISP 2005, Brisbane,
Australia, July 4-6, 2005, Proceedings
Boyd, C.; González Nieto, J.M. (Eds.)
2005, XIV, 594 p., Softcover
ISBN: 978-3-540-26547-4