

Contents

Electronic Money

- Spending Programs: A Tool for Flexible Micropayments1
Josep Domingo-Ferrer and Jordi Herrera-Joancomartí (Uni Rovira i Virgili, Spain)
- Money Conservation via Atomicity in Fair Off-Line E-Cash 14
Shouhuai Xu (Fudan Univ., P. R. China), Moti Yung (CertCo, USA), Gendu Zhang, and Hong Zhu (Fudan Univ., P. R. China)
- Engineering an eCash System.....32
Tim Ebringer and Peter Thorne (Univ. of Melbourne, Australia)

Electronic Payment and Unlinkability

- Unlinkable Electronic Coupon Protocol with Anonymity Control37
Toru Nakanishi, Nobuaki Haruna, and Yuji Sugiyama (Okayama Univ., Japan)
- On the Security of the Lee-Chang Group Signature Scheme and Its Derivatives 47
Marc Joye (Gemplus, France), Narn-Yih Lee (Nan-Tai Inst. of Tech., Taiwan, R.O.C.), and Tzonelih Hwang (Cheng-Kung Univ., Taiwan, R.O.C.)

Secure Software Components, Mobile Agents, and Authentication

- Security Properties of Software Components 52
Khaled Khan, Jun Han, and Yuliang Zheng (Monash Univ., Australia)
- Methods for Protecting a Mobile Agent's Route57
Dirk Westhoff, Markus Schneider, Claus Unger, and Firoz Kaderali (Fern Uni. Hagen, Germany)
- Non-interactive Cryptosystem for Entity Authentication 72
Hyung-Woo Lee(Chonan Univ., Korea), Jung-Eun Kim, and Tai-Yun Kim (Korea Univ., Korea)

Network Security

- Implementation of Virtual Private Networks at the Transport Layer 85
Jorge Davila (Uni Politecnica de Madrid, Spain), Javier Lopez (Uni de Malaga, Spain), and Rene Peralta (Univ. of Wisconsin-Milwaukee, USA)

Performance Evaluation of Certificate Revocation Using k -Valued Hash Tree 103
Hiroaki Kikuchi, Kensuke Abe, and Shohachiro Nakanishi (Tokai Univ., Japan)

Active Rebooting Method for Proactivized System: How to Enhance the Security against Latent Virus Attacks 118
Yuji Watanabe and Hideki Imai (Univ. of Tokyo, Japan)

Digital Watermarking

Highly Robust Image Watermarking Using Complementary Modulations .. 136
Chun-Shien Lu, Hong-Yuan Mark Liao, Shih-Kun Huang, and Chwen-Jye Sze (Academia Sinica, Taiwan, R.O.C.)

Region-Based Watermarking for Images 154
Gareth Brisbane, Rei Safavi-Naini (Wollongong, Australia), and Philip Ogunbona (Motorola Australian Research Center, Australia)

Digital Watermarking Robust Against JPEG Compression 167
Hye-Joo Lee, Ji-Hwan Park (PuKyong Nat'l Univ., Korea), and Yuliang Zheng (Monash Univ., Australia)

Protection of Software and Data

Fingerprints for Copyright Software Protection 178
Josef Pieprzyk (Univ. of Wollongong, Australia)

A Secrecy Scheme for MPEG Video Data Using the Joint of Compression and Encryption 191
Sang Uk Shin, Kyeong Seop Sim, and Kyung Hyune Rhee (PuKyong Nat'l Univ., Korea)

Electronic Money, Key Recovery, and Electronic Voting

On Anonymous Electronic Cash and Crime 202
Tomas Sander and Amnon Ta-Shma (Int'l Computer Science Inst., USA)

On the Difficulty of Key Recovery Systems 207
Seungjoo Kim, Insoo Lee (KISA, Korea), Masahiro Mambo (Tohoku Univ., Japan), and Sungjun Park (KISA, Korea)

An Improvement on a Practical Secret Voting Scheme 225
Miyako Ohkubo, Fumiaki Miura, Masayuki Abe, Atsushi Fujioka, and Tatsuaki Okamoto (NTT Inf. Sharing Platform Lab., Japan)

Digital Signatures

Undeniable Confirmer Signature	235
<i>Khanh Nguyen, Yi Mu, and Vijay Varadharajan (Univ. of Western Sydney, Australia)</i>	
Extended Proxy Signatures for Smart Cards	247
<i>Takeshi Okamoto, Mitsuru Tada (JAIST, Japan), and Eiji Okamoto (Univ. of Wisconsin-Milwaukee, USA)</i>	
A New Digital Signature Scheme on ID-Based Key-Sharing Infrastructures	259
<i>Tsuyoshi Nishioka (Mitsubishi Electric Corp., Japan), Goichiro Hanaoka, and Hideki Imai (Univ. of Tokyo, Japan)</i>	
Cryptanalysis of Two Group Signature Schemes	271
<i>Marc Joye (Gemplus, France), Seungjoo Kim (KISA, Korea), and Narn-Yih Lee (Nan-Tai Inst. of Tech., Taiwan, R.O.C.)</i>	
Author Index	277