

Table of Contents

Public Key Crypto Applications

Universal η_T Pairing Algorithm over Arbitrary Extension Degree.....	1
<i>Masaaki Shirase, Yuto Kawahara, Tsuyoshi Takagi, and Eiji Okamoto</i>	
Convertible Undeniable Proxy Signatures: Security Models and Efficient Construction	16
<i>Wei Wu, Yi Mu, Willy Susilo, and Xinyi Huang</i>	
Secret Signatures: How to Achieve Business Privacy Efficiently?	30
<i>Byoungcheon Lee, Kim-Kwang Raymond Choo, Jeongmo Yang, and Seungjae Yoo</i>	

Biometrics/Information Hiding

Implementation of BioAPI Conformance Test Suite Using BSP Testing Model	48
<i>Jihyeon Jang, Stephen J. Elliott, and Hakil Kim</i>	
Information Hiding in Software with Mixed Boolean-Arithmetic Transforms	61
<i>Yongxin Zhou, Alec Main, Yuan X. Gu, and Harold Johnson</i>	
Geometrically Invariant Image Watermarking in the DWT Domain	76
<i>Shijun Xiang and Hyoun-Joong Kim</i>	

Secure Hardware

Implementation of LSM-Based RBAC Module for Embedded System ...	91
<i>Jae-Deok Lim, Sung-Kyong Un, Jeong-Nyeo Kim, and ChoelHoon Lee</i>	
Iteration Bound Analysis and Throughput Optimum Architecture of SHA-256 (384, 512) for Hardware Implementations	102
<i>Yong Ki Lee, Herwin Chan, and Ingrid Verbauwhede</i>	
A Compact Architecture for Montgomery Elliptic Curve Scalar Multiplication Processor	115
<i>Yong Ki Lee and Ingrid Verbauwhede</i>	

Secure Systems

Windows Vault: Prevention of Virus Infection and Secret Leakage with Secure OS and Virtual Machine	128
<i>Yoshiki Sameshima, Hideaki Saisho, Tsutomu Matsumoto, and Norihisa Komoda</i>	
An Architecture Providing Virtualization-Based Protection Mechanisms Against Insider Attacks	142
<i>Frederic Stumpf, Patrick Röder, and Claudia Eckert</i>	
Detecting Motifs in System Call Sequences	157
<i>William O. Wilson, Jan Feyereisl, and Uwe Aickelin</i>	

Wireless and Mobile Security

Comparative Studies in Key Disagreement Correction Process on Wireless Key Agreement System	173
<i>Toru Hashimoto, Takashi Itoh, Masazumi Ueba, Hisato Iwai, Hideichi Sasaoka, Kazukuni Kobara, and Hideki Imai</i>	
Breaking 104 Bit WEP in Less Than 60 Seconds	188
<i>Erik Tews, Ralf-Philipp Weinmann, and Andrei Pyshkin</i>	
Efficient Implementation of the Pairing on Mobilephones Using BREW	203
<i>Motoi Yoshitomi, Tsuyoshi Takagi, Shinsaku Kiyomoto, and Toshiaki Tanaka</i>	

Application Security/Secure Systems

Security Analysis of MISTY1	215
<i>Hidema Tanaka, Yasuo Hatano, Nobuyuki Sugio, and Toshinobu Kaneko</i>	
A Generic Method for Secure SBox Implementation	227
<i>Emmanuel Prouff and Matthieu Rivain</i>	
On the Security of a Popular Web Submission and Review Software (WSaR) for Cryptology Conferences	245
<i>Swee-Won Lo, Raphael C.-W. Phan, and Bok-Min Goi</i>	

Access Control/DB Security

Authorization Constraints Specification of RBAC	266
<i>Lilong Han, Qingtan Liu, and Zongkai Yang</i>	

Dynamic Access Control Research for Inter-operation in Multi-domain Environment Based on Risk	277
<i>Zhuo Tang, Ruizuan Li, Zhengding Lu, and Zhumu Wen</i>	

A Compositional Multiple Policies Operating System Security Model ...	291
<i>Lei Xia, Wei Huang, and Hao Huang</i>	

Smart Cards/Secure Systems

Longer Randomly Blinded RSA Keys May Be Weaker Than Shorter Ones	303
<i>Colin D. Walter</i>	

Differential Power Analysis of HMAC Based on SHA-2, and Countermeasures.....	317
<i>Robert McEvoy, Michael Tunstall, Colin C. Murphy, and William P. Marnane</i>	

Provably Secure Countermeasure Resistant to Several Types of Power Attack for ECC.....	333
<i>JaeCheol Ha, JeaHoon Park, SangJae Moon, and SungMing Yen</i>	

Anonymity and P2P Security

Risk & Distortion Based K -Anonymity	345
<i>Shenkun Xu and Xiaojun Ye</i>	

Optimizing Quality Levels and Development Costs for Developing an Integrated Information Security System	359
<i>Myeonggil Choi and Sangmun Shin</i>	

ICRep: An Incentive Compatible Reputation Mechanism for P2P Systems	371
<i>Junsheng Chang, Huaimin Wang, Gang Yin, and Yangbin Tang</i>	

Author Index.....	387
-------------------	-----