

# IEICE TRANSACTIONS

O-122-2-1  
月 v.96A  
刊 n.1 ✓

## on Fundamentals of Electronics, Communications and Computer Sciences

### ■ Special Section on Cryptography and Information Security

### ■ Special Section on Wideband Systems

#### **Special Section on Cryptography and Information Security**

- 1 FOREWORD ..... Tsutomu MATSUMOTO

#### **PAPERS**

##### ■ Symmetric Key Cryptography

- 2 Improving the Permutation Layer of Type 1, Type 3, Source-Heavy, and Target-Heavy Generalized Feistel Structures ..... Shingo YANAGIHARA *and* Tetsu IWATA
- 15 On the Construction of Boolean Functions with Optimal Algebraic Immunity Based on Factorization of Numbers of Variables ..... Huajin CHEN, Wenfeng QI, *and* Chuanguai MA
- 25 Security of Hash-then-CBC Key Wrapping Revisited ..... Yasushi OSAKI *and* Tetsu IWATA
- 35 Cryptanalysis of INCrypt32 in HID's iCLASS Systems ..... ChangKyun KIM, Eun-Gu JUNG, Dong Hoon LEE, Chang-Ho JUNG, *and* Daewan HAN

##### ■ Public Key Based Protocols

- 42 Efficient (Hierarchical) Inner-Product Encryption Tightly Reduced from the Decisional Linear Assumption ..... Tatsuaki OKAMOTO *and* Katsuyuki TAKASHIMA
- 53 Ciphertext-Policy Delegatable Hidden Vector Encryption and Its Application ..... Mitsuhiro HATTORI, Takato HIRANO, Takashi ITO, Nori MATSUDA, Takumi MORI, Yusuke SAKAI, *and* Kazuo OHTA
- 68 Efficient Secure Auction Protocols Based on the Boneh-Goh-Nissim Encryption ..... Takuho MITSUNAGA, Yoshifumi MANABE, *and* Tatsuaki OKAMOTO
- 76 Generic Construction of Strongly Secure Timed-Release Public-Key Encryption ..... Atsushi FUJIOKA, Yoshiaki OKAMOTO, *and* Taiichi SAITO
- 92 Message Recovery Signature Schemes from Sigma-Protocols ..... Masayuki ABE, Tatsuaki OKAMOTO, *and* Koutarou SUZUKI
- 101 Modeling Leakage of Ephemeral Secrets in Tripartite/Group Key Exchange ..... Mark MANULIS, Koutarou SUZUKI, *and* Berkant USTAOGLU
- 111 Scalable Privacy-Preserving Data Mining with Asynchronously Partitioned Datasets ..... Hiroaki KIKUCHI, Daisuke KAGAWA, Anirban BASU, Kazuhiko ISHII, Masayuki TERADA, *and* Sadayuki HONGO

##### ■ Hash Functions

- 121 Meet-in-the-Middle Preimage Attacks on AES Hashing Modes and an Application to Whirlpool ..... Yu SASAKI

(continued over leaf)



- 131 Boomerang Distinguishers on MD4-Based Hash Functions: First Practical Results on Full 5-Pass HAVAL Compression Function ..... Yu SASAKI
- 141 Open-Key Distinguishers for the Internal Block Cipher of Tweaked Lesamnta ..... Yu SASAKI and Kazumaro AOKI

■ **Foundations**

- 150 Random Sampling Reduction with Precomputation ..... Masayuki YOSHINO and Noboru KUNIHIRO
- 158 Computing a Sequence of 2-Isogenies on Supersingular Elliptic Curves ..... Reo YOSHIDA and Katsuyuki TAKASHIMA
- 166 Multiparty Simultaneous Quantum Identity Authentication Secure against Fake Signal Attacks ..... Atsushi WASEDA
- 171 On Constant-Weight Multi-Valued Sequences from Cyclic Difference Sets ..... Takayasu KAIDA and Junru ZHENG

■ **Implementation**

- 177 A New Type of Fault-Based Attack: Fault Behavior Analysis ..... Yang LI, Kazuo OHTA, and Kazuo SAKIYAMA
- 185 Correlated Noise Reduction for Electromagnetic Analysis ..... Hongying LIU, Xin JIN, Yukiyasu TSUNOO, and Satoshi GOTO
- 196 General Fault Attacks on Multivariate Public Key Cryptosystems ..... Yasufumi HASHIMOTO, Tsuyoshi TAKAGI, and Kouichi SAKURAI
- 206 Efficient Implementation of NTRU Cryptosystem Using Sliding Window Methods ..... Mun-Kyu LEE, Jung Woo KIM, Jeong Eun SONG, and Kunsoo PARK

■ **System Security**

- 215 Implementation of a Memory Disclosure Attack on Memory Deduplication of Virtual Machines ..... Kuniyasu SUZAKI, Kengo IJIMA, Toshiki YAGI, and Cyrille ARTHO
- 225 Catching the Behavioral Differences between Multiple Executions for Malware Detection ..... Takahiro KASAMA, Katsunari YOSHIOKA, Daisuke INOUE, and Tsutomu MATSUMOTO

**LETTERS**

- 233 Provable Security against Cryptanalysis with Impossible Differentials ..... Kazumaro AOKI
- 237 A Parallelizable PRF-Based MAC Algorithm: Well beyond the Birthday Bound ..... Kan YASUDA
- 242 Rogue Key Attacks on Lu et al.'s Verifiably Encrypted Signature Scheme ..... Bennian DOU, Hong ZHANG, Chun-Hua CHEN, and Chungen XU
- 244 Key Substitution Attacks on Multisignature Schemes ..... Bennian DOU, Hong ZHANG, Chun-Hua CHEN, and Chungen XU

**Special Section on Wideband Systems**

- 246 FOREWORD ..... Makoto ITAMI

**PAPERS**

- 247 Software Radio-Based Distributed Multi-User MIMO Testbed: Towards Green Wireless Communications (*INVITED*) ..... Hidekazu MURATA, Susumu YOSHIDA, Koji YAMAMOTO, Daisuke UMEHARA, Satoshi DENNO, and Masahiro MORIKURA
- 255 Performance Analysis of Coded-Sequence Self-Encoded Spread Spectrum over Rayleigh Fading Channel ..... Poomathi DURAISAMY and Lim NGUYEN
- 264 Primary Signal to Noise Ratio Estimation Based on AIC for UWB Systems ..... Masahiro FUJII and Yu WATANABE
- 274 Examination of Effective UWB Avoidance Based on Experiments for Coexistence with Other Wireless Systems ..... Huan-Bang LI, Kunio YATA, Kenichi TAKIZAWA, Noriaki MIYAZAKI, Takashi OKADA, Kohei OHNO, Takuji MOCHIZUKI, Eishin NAKAGAWA, and Takehiko KOBAYASHI
- 285 Detection Capability of Downlink Signals in Mobile WiMAX and 3GPP LTE with an FFT-Based UWB Receiver ..... Kenichi TAKIZAWA, Hiroataka YAMANE, Huan-Bang LI, Feng LU, Kohei OHNO, Takuji MOCHIZUKI, Takashi OKADA, Kunio YATA, Hisashi NISHIKAWA, and Takehiko KOBAYASHI



## LETTERS

- 293 A Max-Min Approach to Channel Shortening in OFDM Systems ..... Tsukasa TAKAHASHI and Teruyuki MIYAJIMA  
296 Hybrid DCT/DST Precoding Scheme for the PAPR Reduction of OFDM Systems ..... Soobum CHO and Sang Kyu PARK

## Regular Section

### PAPERS

#### ■ Digital Signal Processing

- 298 Reliable Data Transmission for Resonant-Type Wireless Power Transfer ..... Shinpei NOGUCHI, Mamiko INAMORI, and Yukitoshi SANADA  
304 Minimizing False Peak Errors in Generalized Cross-Correlation Time Delay Estimation Using Subsample Time Delay Estimation ..... SooHwan CHOI and DooSeop EOM

#### ■ VLSI Design Technology and CAD

- 312 A Thermal-Aware High-Level Synthesis Algorithm for RDR Architectures through Binding and Allocation ..... Kazushi KAWAMURA, Masao YANAGISAWA, and Nozomu TOGAWA

#### ■ Algorithms and Data Structures

- 322 Fast Bit-Parallel Polynomial Basis Multiplier for  $GF(2^m)$  Defined by Pentanomials Using Weakly Dual Basis ..... Sun-Mi PARK, Ku-Young CHANG, Dowon HONG, and Changho SEO

#### ■ Cryptography and Information Security

- 332 Enhanced Side-Channel Cube Attacks on PRESENT ..... Xinjie ZHAO, Shize GUO, Fan ZHANG, Tao WANG, Zhijie SHI, and Hao LUO

#### ■ Vision

- 340 Deterioration of Visibility of Scrolling Text Presented Nearby Image Moving in the Opposite Direction ..... Ken KIHARA, Marina SEKI, and Sakuichi OHTSUKA

#### ■ Concurrent Systems

- 345 Computation of Sublanguages for Synthesizing Decentralized Supervisors for Timed Discrete Event Systems ..... Masashi NOMURA and Shigemasa TAKAI

## LETTERS

#### ■ Circuit Theory

- 356 Reduced Reconfigurable Logic Circuit Design Based on Double Gate CNTFETs Using Ambipolar Binary Decision Diagram ..... Hiroshi NINOMIYA, Manabu KOBAYASHI, and Shigeyoshi WATANABE

#### ■ Cryptography and Information Security

- 360 Generalized Construction of Boolean Function with Maximum Algebraic Immunity Using Univariate Polynomial Representation ..... Shaojing FU, Chao LI, and Longjiang QU  
363 Linear Complexity of Binary Whiteman Generalized Cyclotomic Sequences of Order 4 ..... Xiaoping LI, Wenping MA, Tongjiang YAN, and Xubo ZHAO

#### ■ Information Theory

- 367 Several Types of Sequences with Optimal Autocorrelation Properties ..... Fanxin ZENG, Xiaoping ZENG, Xiangyong ZENG, Zhenyu ZHANG, and Guixin XUAN

#### ■ Coding Theory

- 373 Low Complexity Decoder Design for Non-binary LDPC Coded MIMO System Using Quasi-Orthogonal STBC ..... Yier YAN and Moon Ho LEE  
377 Construction of Shift Distinct Sequence Sets with Zero or Low Correlation Zone ..... Xiaoyu CHEN, Chengqian XU, Yubo LI, and Kai LIU

#### ■ Communication Theory and Signals

- 383 Channel Localization Mechanism for Wi-Fi Systems ..... Sungho HWANG and Kyungjun KIM  
387 Channel Condition Number Based Switching Detection Scheme in MIMO-OFDM System ..... Jang-Kyun AHN, Seung-Jun YU, and Hyoung-Kyu SONG

#### ■ Intelligent Transport System

- 391 Traffic Flow Simulator Using Virtual Controller Model ..... Haijun LIANG, Hongyu YANG, and Bo YANG

■ Image

394 Region Diversity Based Saliency Density Maximization for Salient Object Detection

..... Xin HE, Huiyun JING, Qi HAN, and Xiamu NIU

---

398 ABSTRACTS (IEICE Trans. Fundamentals (Japanese Edition), Vol. J96-A, No. 1)

Original Contributions in English

Copyright © 2013 by The Institute of Electronics, Information and Communication Engineers

The IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences has been selected for coverage in the following ISI (Institute for Scientific Information) products/services.

- Science Citation Index Expanded (included in "Web of Science")
- Current Contents (Edition: Engineering, Computing and Technology)
- ISI Alerting Services
- CompuMath Citation Index\*

\*CompuMath Citation Index includes bibliographic information from over 600 journals, books, and proceedings on computers and mathematics.