

Table of Contents

Key Distribution

Bounds and Constructions for Unconditionally Secure Distributed Key Distribution Schemes for General Access Structures	1
<i>Carlo Blundo, Paolo D'Arco (Università di Salerno)</i> <i>Vanessa Daza, and Carles Padró (Universitat Politècnica de Catalunya)</i>	
Privacy Amplification Theorem for Noisy Main Channel	18
<i>Valeri Korjik, Guillermo Morales-Luna (CINVESTAV-IPN),</i> <i>and Vladimir B. Balakirsky (EIDMA)</i>	

Protocols

Efficient Kerberized Multicast in a Practical Distributed Setting.....	27
<i>Giovanni Di Crescenzo (Telcordia Technologies)</i> <i>and Olga Kornievskaja (University of Michigan)</i>	
Suitability of a Classical Analysis Method for E-commerce Protocols.....	46
<i>Sigrid Gürgens (GMD-SIT) and Javier Lopez (University of Malaga)</i>	

Enhancing Technologies

Hypocrates (A New Proactive Password Checker)	63
<i>Carlo Blundo, Paolo D'Arco, Alfredo De Santis,</i> <i>and Clemente Galdi (Università di Salerno)</i>	
Lenient/Strict Batch Verification in Several Groups.....	81
<i>Fumitaka Hoshino, Masayuki Abe,</i> <i>and Tetsutaro Kobayashi (NTT Corporation)</i>	

Privacy

Absolute Privacy in Voting	95
<i>Dmitri Asonov (Humboldt-Universität zu Berlin),</i> <i>Markus Schaal (Technische Universität Berlin), and</i> <i>Johann-Christoph Freytag (Humboldt-Universität zu Berlin)</i>	
A Logical Model for Privacy Protection	110
<i>Tsan-sheng Hsu, Churn-Jung Liao,</i> <i>and Da-Wei Wang (Academia Sinica)</i>	

Software Protection

DISSECT: DIStribution for SEcURITY Tool	125
<i>Enriquillo Valdez (Polytechnic University of New York)</i> <i>and Moti Yung (CertCo, Inc.)</i>	
An Approach to the Obfuscation of Control-Flow of Sequential Computer Programs	144
<i>Stanley Chow, Yuan Gu, Harold Johnson (Cloakware Corporation),</i> <i>and Vladimir A. Zakharov (Moscow State University)</i>	

Message Hiding I

A Practical and Effective Approach to Large-Scale Automated Linguistic Steganography	156
<i>Mark Chapman (Omni Tech Corp.),</i> <i>George I. Davida (University of Wisconsin-Milwaukee), and</i> <i>Marc Rennhard (Swiss Federal Institute of Technology)</i>	
Robust New Method in Frequency Domain Watermarking	166
<i>David Sánchez, Agustín Orfila, Julio César Hernández,</i> <i>and José María Sierra (Carlos III University)</i>	

PKI Issues and Protocols

On the Complexity of Public-Key Certificate Validation	183
<i>Diana Berbecaru, Antonio Lioy, and</i> <i>Marius Marian (Politecnico di Torino)</i>	
Liability of Certification Authorities: A Juridical Point of View	204
<i>Apol·lònia Martínez-Nadal and</i> <i>Josep L. Ferrer-Gomila (Universitat de les Illes Balears)</i>	

Hardware Implementations

Experimental Testing of the Gigabit IPSec-Compliant Implementations of Rijndael and Triple DES Using SLAAC-1V FPGA Accelerator Board	220
<i>Pawel Chodowiec, Kris Gaj (George Mason University),</i> <i>Peter Bellows, and Brian Schott (University of Southern California)</i>	
Elliptic Curve Arithmetic Using SIMD	235
<i>Kazumaro Aoki (NTT Communications), Fumitaka Hoshino,</i> <i>Tetsutaro Kobayashi, and Hiroaki Oguro (NTT Corporation)</i>	

On the Hardware Implementation of the 3GPP Confidentiality and Integrity Algorithms	248
<i>Kostas Marinis (National Technical University of Athens), Nikos K. Moshopoulos, Fotis Karoubalis (Atmel Hellas), and Kiamal Z. Pekmestzi (National Technical University of Athens)</i>	
Efficient Implementation of Elliptic Curve Cryptosystems on an ARM7 with Hardware Accelerator	266
<i>Sheng-Bo Xu and Lejla Batina (Securelink B.V.)</i>	

Cryptanalysis and Prevention

A Theoretical DPA-Based Cryptanalysis of the NESSIE Candidates FLASH and SFLASH.....	280
<i>Rainer Steinwandt, Willi Geiselmann, and Thomas Beth (Universität Karlsruhe)</i>	
Quadratic Relations for S-Boxes: Their Minimum Representations and Bounds	294
<i>Routo Terada and Paulo G. Pinheiro (University of S. Paulo)</i>	
Approximate Power Roots in Z_m	310
<i>Ismael Jiménez-Calvo (C.S.I.C.) and German Sáez-Moreno (Universitat Politècnica de Catalunya)</i>	
Securing Elliptic Curve Point Multiplication against Side-Channel Attacks	324
<i>Bodo Möller (Technische Universität Darmstadt)</i>	

Implementations

A Flexible Role-Based Access Control Model for Multimedia Medical Image Database Systems	335
<i>Sofia Tzelepi and George Pangalos (Aristotelian University)</i>	
A Secure Publishing Service for Digital Libraries of XML Documents	347
<i>Elisa Bertino, Barbara Carminati (Università di Milano), and Elena Ferrari (Università dell'Insubria)</i>	

Non-repudiation Techniques

An Optimistic Non-repudiation Protocol with Transparent Trusted Third Party	363
<i>Olivier Markowitch and Steve Kremer (Université Libre de Bruxelles)</i>	

Persistent Authenticated Dictionaries and Their Applications	379
<i>Aris Anagnostopoulos (Brown University),</i> <i>Michael T. Goodrich (University of California), and</i> <i>Roberto Tamassia (Brown University)</i>	

Contracts and Auctions

Efficient Optimistic N-Party Contract Signing Protocol	394
<i>Josep L. Ferrer-Gomila, Magdalena Payeras-Capellà,</i> <i>and Llorenç Huguet-Rotger (Universitat de les Illes Balears)</i>	
Efficient Sealed-Bid Auctions for Massive Numbers of Bidders with Lump Comparison	408
<i>Koji Chida, Kunio Kobayashi,</i> <i>and Hikaru Morita (NTT Corporation)</i>	

Message Hiding II

Oblivious Image Watermarking Robust against Scaling and Geometric Distortions	420
<i>Francesc Sebé and Josep Domingo-Ferrer (Universitat Rovira i Virgili)</i>	
Fingerprinting Text in Logical Markup Languages	433
<i>Christian D. Jensen (Trinity College Dublin)</i>	

Payments

SPEED Protocol: Smartcard-Based Payment with Encrypted Electronic Delivery	446
<i>Antonio Ruiz, Gregorio Martínez, Oscar Cánovas,</i> <i>and Antonio F. Gómez (University of Murcia)</i>	
Efficient Transferable Cash with Group Signatures	462
<i>Ik Rae Jeong, Dong Hoon Lee,</i> <i>and Jong In Lim (Korea University)</i>	

Security Applications

An Auditable Metering Scheme for Web Advertisement Applications	475
<i>Liqun Chen and Wenbo Mao (Hewlett-Packard Laboratories)</i>	

Broker-Based Secure Negotiation of Intellectual Property Rights	486
<i>Jaime Delgado (Universitat Pompeu Fabra), Isabel Gallego</i>	
<i>(Universitat Politècnica de Catalunya), and Xavier Perramon</i>	
<i>(Universitat Pompeu Fabra)</i>	

Network and OS Security

Design of the Decision Support System for Network Security	
Management to Secure Enterprise Network	497
<i>Jae Seung Lee (ETRI) and</i>	
<i>Sang Choon Kim (Samchok National University)</i>	

Measuring False-Positive by Automated Real-Time Correlated Hacking	
Behavior Analysis	512
<i>Jia Wang and Insup Lee (University of Pennsylvania)</i>	

Design of UNIX System for the Prevention of Damage Propagation	
by Intrusion and Its Implementation Based on 4.4BSD	536
<i>Kenji Masui, Masahiko Tomoishi,</i>	
<i>and Naoki Yonezaki (Tokyo Institute of Technology)</i>	

Author Index	553
--------------------	-----