

Contents

Cryptanalysis of Symmetric Key

Linear Regression Attack with F-test: A New SCARE Technique for Secret Block Ciphers	3
<i>Si Gao, Hua Chen, Wenling Wu, Limin Fan, Jingyi Feng, and Xiangliang Ma</i>	
Compact Representation for Division Property	19
<i>Yosuke Todo and Masakatu Morii</i>	
An Automatic Cryptanalysis of Transposition Ciphers Using Compression . . .	36
<i>Noor R. Al-Kazaz, Sean A. Irvine, and William J. Teahan</i>	

SideChannel Attacks and Implementation

Side-Channel Attacks on Threshold Implementations Using a Glitch Algebra	55
<i>Serge Vaudenay</i>	
Diversity Within the Rijndael Design Principles for Resistance to Differential Power Analysis	71
<i>Merrielle Spain and Mayank Varia</i>	
NEON-SIDH: Efficient Implementation of Supersingular Isogeny Diffie-Hellman Key Exchange Protocol on ARM	88
<i>Brian Koziel, Amir Jalali, Reza Azarderakhsh, David Jao, and Mehran Mozaffari-Kermani</i>	

Lattice-Based Cryptography

Server-Aided Revocable Identity-Based Encryption from Lattices	107
<i>Khoa Nguyen, Huaxiong Wang, and Juanyang Zhang</i>	
Speeding up the Number Theoretic Transform for Faster Ideal Lattice-Based Cryptography	124
<i>Patrick Longa and Michael Naehrig</i>	
An Efficient Lattice-Based Multisignature Scheme with Applications to Bitcoins	140
<i>Rachid El Bansarkhani and Jan Sturm</i>	

Virtual Private Network

Breaking PPTP VPNs via RADIUS Encryption	159
<i>Matthias Horst, Martin Grothe, Tibor Jager, and Jörg Schwenk</i>	
LEAP: A Next-Generation Client VPN and Encrypted Email Provider.	176
<i>Elijah Sparrow, Harry Halpin, Kali Kaneko, and Ruben Pollan</i>	
Implementation State of HSTS and HPKP in Both Browsers and Servers. . . .	192
<i>Sergio de los Santos, Carmen Torrano, Yaiza Rubio, and Félix Brezo</i>	

Signatures and Hash

Signer-Anonymous Designated-Verifier Redactable Signatures for Cloud-Based Data Sharing	211
<i>David Derler, Stephan Krenn, and Daniel Slamanig</i>	
Group Signature with Deniability: How to Disavow a Signature	228
<i>Ai Ishida, Keita Emura, Goichiro Hanaoka, Yusuke Sakai, and Keisuke Tanaka</i>	
Sandwich Construction for Keyed Sponges: Independence Between Capacity and Online Queries	245
<i>Yusuke Naito</i>	

MultiParty Computation

Secure Error-Tolerant Graph Matching Protocols.	265
<i>Kalikinkar Mandal, Basel Alomair, and Radha Poovendran</i>	
Efficient Verifiable Computation of XOR for Biometric Authentication	284
<i>Aysajan Abidin, Abdelrahman Aly, Enrique Argones Rúa, and Aikaterini Mitrokotsa</i>	
Verifiable Message-Locked Encryption	299
<i>Sébastien Canard, Fabien Laguillaumie, and Marie Paindavoine</i>	

Symmetric Cryptography and Authentication

Security of Online AE Schemes in RUP Setting	319
<i>Jian Zhang and Wenling Wu</i>	
An Efficient Entity Authentication Protocol with Enhanced Security and Privacy Properties	335
<i>Aysajan Abidin, Enrique Argones Rúa, and Bart Preneel</i>	

Probabilistic Generation of Trapdoors: Reducing Information Leakage of Searchable Symmetric Encryption	350
<i>Kenichiro Hayasaka, Yutaka Kawai, Yoshihiro Koseki, Takato Hirano, Kazuo Ohta, and Mitsugu Iwamoto</i>	

System Security

AAL and Static Conflict Detection in Policy	367
<i>Jean-Claude Royer and Anderson Santana De Oliveira</i>	
Component-Oriented Access Control for Deployment of Application Services in Containerized Environments.	383
<i>Kirill Belyaev and Indrakshi Ray</i>	
Generic Access Control System for Ad Hoc MCC and Fog Computing	400
<i>Bilel Zaghdoudi, Hella Kaffel-Ben Ayed, and Wafa Harizi</i>	

Functional and Homomorphic Encryption

SecReach: Secure Reachability Computation on Encrypted Location Check-in Data	419
<i>Hanyu Quan, Boyang Wang, Iraklis Leontiadis, Ming Li, and Yuqing Zhang</i>	
FHE Over the Integers and Modular Arithmetic Circuits	435
<i>Eunkyung Kim and Mehdi Tibouchi</i>	
An Efficient Somewhat Homomorphic Encryption Scheme Based on Factorization	451
<i>G��rald Gavin</i>	

Information Theoretic Security

Efficient, XOR-Based, Ideal (t, n) –threshold Schemes.	467
<i>Liqun Chen, Thalia M. Laing, and Keith M. Martin</i>	
Efficient and Secure Multiparty Computations Using a Standard Deck of Playing Cards.	484
<i>Takaaki Mizuki</i>	
Efficient Card-Based Cryptographic Protocols for Millionaires’ Problem Utilizing Private Permutations	500
<i>Takeshi Nakai, Yuuki Tokushige, Yuto Misawa, Mitsugu Iwamoto, and Kazuo Ohta</i>	

Malware and Attacks

Evaluation on Malware Classification by Session Sequence of Common Protocols	521
<i>Shohei Hiruta, Yukiko Yamaguchi, Hajime Shimada, Hiroki Takakura, Takeshi Yagi, and Mitsuaki Akiyama</i>	
An Efficient Approach to Detect TorrentLocker Ransomware in Computer Systems.	532
<i>Faustin Mbol, Jean-Marc Robert, and Alireza Sadighian</i>	
Detecting Malware Through Anti-analysis Signals - A Preliminary Study. . . .	542
<i>Joash W.J. Tan and Roland H.C. Yap</i>	
Attackers in Wireless Sensor Networks Will Be Neither Random Nor Jumping – Secrecy Amplification Case	552
<i>Radim Ošťádal, Petr Švenda, and Vashek Matyáš</i>	
Improved Attacks on Extended Generalized Feistel Networks	562
<i>Valérie Nachev, Nicolas Marrière, and Emmanuel Volte</i>	
When Constant-Time Source Yields Variable-Time Binary: Exploiting Curve25519-donna Built with MSVC 2015.	573
<i>Thierry Kaufmann, Hervé Pelletier, Serge Vaudenay, and Karine Villegas</i>	

MultiParty Computation and Functional Encryption

On the Power of Public-key Function-Private Functional Encryption	585
<i>Vincenzo Iovino, Qiang Tang, and Karol Żebrowski</i>	
A New Technique for Compacting Secret Key in Attribute-Based Broadcast Encryption.	594
<i>Sébastien Canard, Duong Hieu Phan, and Viet Cuong Trinh</i>	
An Efficient Construction of Non-Interactive Secure Multiparty Computation.	604
<i>Satoshi Obana and Maki Yoshida</i>	
An MPC-Based Privacy-Preserving Protocol for a Local Electricity Trading Market.	615
<i>Aysajan Abidin, Abdelrahman Aly, Sara Cleemput, and Mustafa A. Mustafa</i>	
Implementation of Verified Set Operation Protocols Based on Bilinear Accumulators.	626
<i>Luca Ferretti, Michele Colajanni, and Mirco Marchetti</i>	

Multi-core FPGA Implementation of ECC with Homogeneous Co-Z Coordinate Representation	637
<i>Bo-Yuan Peng, Yuan-Che Hsu, Yu-Jia Chen, Di-Chia Chueh, Chen-Mou Cheng, and Bo-Yin Yang</i>	

Network Security, Privacy, and Authentication

DNSSEC Misconfigurations in Popular Domains	651
<i>Tianxiang Dai, Haya Shulman, and Michael Waidner</i>	
Integral Privacy	661
<i>Vicenç Torra and Guillermo Navarro-Arribas</i>	
Sharing Is Caring, or Callous?	670
<i>Yu Pu and Jens Grossklags</i>	
Improving the Sphinx Mix Network	681
<i>Filipe Beato, Kimmo Halunen, and Bart Mennink</i>	
User Authentication from Mouse Movement Data Using SVM Classifier	692
<i>Bashira Aker Anima, Mahmood Jasim, Khandaker Abir Rahman, Adam Rulapaugh, and Md Hasanuzzaman</i>	
Distance Bounding Based on PUF.	701
<i>Mathilde Igier and Serge Vaudenay</i>	

Posters

Denying Your Whereabouts: A Secure and Deniable Scheme for Location-Based Services	713
<i>Tassos Dimitriou and Naser Al-Ibrahim</i>	
Range Query Integrity in Cloud Data Streams with Efficient Insertion	719
<i>Francesco Bucchafurri, Gianluca Lax, Serena Nicolazzo, and Antonino Nocera</i>	
Vulnerability Analysis Using Google and Shodan	725
<i>Kai Simon</i>	
Language-Based Hypervisors	731
<i>Enrico Budianto, Richard Chow, Jonathan Ding, and Michael McCool</i>	
Internet Censorship in Italy: A First Look at 3G/4G Networks	737
<i>Giuseppe Aceto, Antonio Montieri, and Antonio Pescapè</i>	
A Privacy-Preserving Model for Biometric Fusion.	743
<i>Christina-Angeliki Toli, Abdelrahman Aly, and Bart Preneel</i>	

Hybrid WBC: Secure and Efficient White-Box Encryption Schemes	749
<i>Jihoon Cho, Kyu Young Choi, Orr Dunkelman, Nathan Keller,</i> <i>Dukjae Moon, and Aviya Vaidberg</i>	
Moving in Next Door: Network Flooding as a Side Channel in Cloud Environments	755
<i>Yatharth Agarwal, Vishnu Murale, Jason Hennessey, Kyle Hogan,</i> <i>and Mayank Varia</i>	
Author Index	761



<http://www.springer.com/978-3-319-48964-3>

Cryptology and Network Security
15th International Conference, CANS 2016, Milan, Italy,
November 14-16, 2016, Proceedings
Foresti, S.; Persiano, G. (Eds.)
2016, XVI, 762 p. 116 illus., Softcover
ISBN: 978-3-319-48964-3