Contents

Cryptanalysis of Symmetric Key

Linear Regression Attack with F-test: A New SCARE Technique for Secret Block Ciphers ........................................ 3
   Si Gao, Hua Chen, Wenling Wu, Limin Fan, Jingyi Feng,
   and Xiangliang Ma

Compact Representation for Division Property ..................... 19
   Yosuke Todo and Masakatu Morii

An Automatic Cryptanalysis of Transposition Ciphers Using Compression . . . 36
   Noor R. Al-Kazaz, Sean A. Irvine, and William J. Teahan

SideChannel Attacks and Implementation

Side-Channel Attacks on Threshold Implementations Using a Glitch Algebra ........................................ 55
   Serge Vaudenay

Diversity Within the Rijndael Design Principles for Resistance to Differential Power Analysis ........................................ 71
   Merrielle Spain and Mayank Varia

NEON-SIDH: Efficient Implementation of Supersingular Isogeny Diffie-Hellman Key Exchange Protocol on ARM ........................................ 88
   Brian Koziel, Amir Jalali, Reza Azarderakhsh, David Jao,
   and Mehran Mozaffari-Kermani

Lattice-Based Cryptography

Server-Aided Revocable Identity-Based Encryption from Lattices ................. 107
   Khoa Nguyen, Huaxiong Wang, and Juanyang Zhang

Speeding up the Number Theoretic Transform for Faster Ideal Lattice-Based Cryptography ........................................ 124
   Patrick Longa and Michael Naehrig

An Efficient Lattice-Based Multisignature Scheme with Applications to Bitcoins ........................................ 140
   Rachid El Bansarkhani and Jan Sturm
Virtual Private Network

Breaking PPTP VPNs via RADIUS Encryption ........................................... 159
  Matthias Horst, Martin Grothe, Tibor Jager, and Jörg Schwenk

LEAP: A Next-Generation Client VPN and Encrypted Email Provider ........ 176
  Elijah Sparrow, Harry Halpin, Kali Kaneko, and Ruben Pollan

Implementation State of HSTS and HPKP in Both Browsers and Servers .... 192
  Sergio de los Santos, Carmen Torrano, Yaiza Rubio, and Félix Brezo

Signatures and Hash

Signer-Anonymous Designated-Verifier Redactable Signatures
  for Cloud-Based Data Sharing ................................................................. 211
    David Derler, Stephan Krenn, and Daniel Slamanig

Group Signature with Deniability: How to Disavow a Signature ............. 228
    Ai Ishida, Keita Emura, Goichiro Hanaoka, Yusuke Sakai,
    and Keisuke Tanaka

Sandwich Construction for Keyed Sponges: Independence Between
  Capacity and Online Queries ................................................................. 245
    Yusuke Naito

MultiParty Computation

Secure Error-Tolerant Graph Matching Protocols .................................... 265
    Kalikinkar Mandal, Basel Alomair, and Radha Poovendran

Efficient Verifiable Computation of XOR for Biometric Authentication .... 284
    Aysajan Abidin, Abdelrahman Aly, Enrique Argones Rúa,
    and Aikaterini Mitrokotsa

Verifiable Message-Locked Encryption ................................................... 299
    Sébastien Canard, Fabien Laguillaumie, and Marie Paindavoine

Symmetric Cryptography and Authentication

Security of Online AE Schemes in RUP Setting ..................................... 319
    Jian Zhang and Wenling Wu

An Efficient Entity Authentication Protocol with Enhanced Security
  and Privacy Properties ................................................................. 335
    Aysajan Abidin, Enrique Argones Rúa, and Bart Preneel
Probabilistic Generation of Trapdoors: Reducing Information Leakage of Searchable Symmetric Encryption

Kenichiro Hayasaka, Yutaka Kawai, Yoshihiro Koseki, Takato Hirano, Kazuo Ohta, and Mitsugu Iwamoto

System Security

AAL and Static Conflict Detection in Policy

Jean-Claude Royer and Anderson Santana De Oliveira

Component-Oriented Access Control for Deployment of Application Services in Containerized Environments

Kirill Belyaev and Indrakshi Ray

Generic Access Control System for Ad Hoc MCC and Fog Computing

Bilel Zaghdoudi, Hella Kaffel-Ben Ayed, and Wafa Harizi

Functional and Homomorphic Encryption

SecReach: Secure Reachability Computation on Encrypted Location Check-in Data

Hanyu Quan, Boyang Wang, Iraklis Leontiadis, Ming Li, and Yuqing Zhang

FHE Over the Integers and Modular Arithmetic Circuits

Eunkyung Kim and Mehdi Tibouchi

An Efficient Somewhat Homomorphic Encryption Scheme Based on Factorization

Gérald Gavin

Information Theoretic Security

Efficient, XOR-Based, Ideal \((t, n)\)-threshold Schemes

Liqun Chen, Thalia M. Laing, and Keith M. Martin

Efficient and Secure Multiparty Computations Using a Standard Deck of Playing Cards

Takaaki Mizuki

Efficient Card-Based Cryptographic Protocols for Millionaires’ Problem Utilizing Private Permutations

Takeshi Nakai, Yuuki Tokushige, Yuto Misawa, Mitsugu Iwamoto, and Kazuo Ohta
Malware and Attacks

Evaluation on Malware Classification by Session Sequence of Common Protocols
Shohei Hiruta, Yukiko Yamaguchi, Hajime Shimada, Hiroki Takakura,
Takeshi Yagi, and Mitsuaki Akiyama

An Efficient Approach to Detect TorrentLocker Ransomware in Computer Systems
Faustin Mbol, Jean-Marc Robert, and Alireza Sadighian

Detecting Malware Through Anti-analysis Signals - A Preliminary Study
Joash W.J. Tan and Roland H.C. Yap

Attackers in Wireless Sensor Networks Will Be Neither Random Nor Jumping – Secrecy Amplification Case
Radim Ošťádal, Petr Švenda, and Vashek Matyáš

Improved Attacks on Extended Generalized Feistel Networks
Valérie Nachef, Nicolas Marrière, and Emmanuel Volte

When Constant-Time Source Yields Variable-Time Binary: Exploiting Curve25519-donna Built with MSVC 2015
Thierry Kaufmann, Hervé Pelletier, Serge Vaudenay, and Karine Villegas

MultiParty Computation and Functional Encryption

On the Power of Public-key Function-Private Functional Encryption
Vincenzo Iovino, Qiang Tang, and Karol Żebrowski

A New Technique for Compacting Secret Key in Attribute-Based Broadcast Encryption
Sébastien Canard, Duong Hieu Phan, and Viet Cuong Trinh

An Efficient Construction of Non-Interactive Secure Multiparty Computation
Satoshi Obana and Maki Yoshida

An MPC-Based Privacy-Preserving Protocol for a Local Electricity Trading Market
Aysajan Abidin, Abdelrahman Aly, Sara Cleemput, and Mustafa A. Mustafa

Implementation of Verified Set Operation Protocols Based on Bilinear Accumulators
Luca Ferretti, Michele Colajanni, and Mirco Marchetti
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multi-core FPGA Implementation of ECC with Homogeneous Co-Z</td>
<td>637</td>
</tr>
<tr>
<td>Bo-Yuan Peng, Yuan-Che Hsu, Yu-Jia Chen, Di-Chia Chueh, Chen-Mou Cheng, and Bo-Yin Yang</td>
<td></td>
</tr>
<tr>
<td><strong>Network Security, Privacy, and Authentication</strong></td>
<td></td>
</tr>
<tr>
<td>DNSSEC Misconfigurations in Popular Domains</td>
<td>651</td>
</tr>
<tr>
<td>Tianxiang Dai, Haya Shulman, and Michael Waidner</td>
<td></td>
</tr>
<tr>
<td>Integral Privacy</td>
<td>661</td>
</tr>
<tr>
<td>Vicenç Torra and Guillermo Navarro-Arribas</td>
<td></td>
</tr>
<tr>
<td>Sharing Is Caring, or Callous?</td>
<td>670</td>
</tr>
<tr>
<td>Yu Pu and Jens Grossklags</td>
<td></td>
</tr>
<tr>
<td>Improving the Sphinx Mix Network</td>
<td>681</td>
</tr>
<tr>
<td>Filipe Beato, Kimmo Halunen, and Bart Mennink</td>
<td></td>
</tr>
<tr>
<td>User Authentication from Mouse Movement Data Using SVM Classifier</td>
<td>692</td>
</tr>
<tr>
<td>Bashira Akter Anima, Mahmood Jasim, Khandaker Abir Rahman, Adam Rulapaugh, and Md Hasanuzzaman</td>
<td></td>
</tr>
<tr>
<td>Distance Bounding Based on PUF</td>
<td>701</td>
</tr>
<tr>
<td>Mathilde Igier and Serge Vaudenay</td>
<td></td>
</tr>
<tr>
<td><strong>Posters</strong></td>
<td></td>
</tr>
<tr>
<td>Denying Your Whereabouts: A Secure and Deniable Scheme for Location-Based Services</td>
<td>713</td>
</tr>
<tr>
<td>Tassos Dimitriou and Naser Al-Ibrahim</td>
<td></td>
</tr>
<tr>
<td>Range Query Integrity in Cloud Data Streams with Efficient Insertion</td>
<td>719</td>
</tr>
<tr>
<td>Francesco Buccafurri, Gianluca Lax, Serena Nicolazzo, and Antonino Nocera</td>
<td></td>
</tr>
<tr>
<td>Vulnerability Analysis Using Google and Shodan</td>
<td>725</td>
</tr>
<tr>
<td>Kai Simon</td>
<td></td>
</tr>
<tr>
<td>Language-Based Hypervisors</td>
<td>731</td>
</tr>
<tr>
<td>Enrico Budianto, Richard Chow, Jonathan Ding, and Michael McCool</td>
<td></td>
</tr>
<tr>
<td>Internet Censorship in Italy: A First Look at 3G/4G Networks</td>
<td>737</td>
</tr>
<tr>
<td>Giuseppe Aceto, Antonio Montieri, and Antonio Pescapè</td>
<td></td>
</tr>
<tr>
<td>A Privacy-Preserving Model for Biometric Fusion</td>
<td>743</td>
</tr>
<tr>
<td>Christina-Angeliki Toli, Abdelrahman Aly, and Bart Preneel</td>
<td></td>
</tr>
</tbody>
</table>
Hybrid WBC: Secure and Efficient White-Box Encryption Schemes . . . . . . . 749
   Jihoon Cho, Kyu Young Choi, Orr Dunkelman, Nathan Keller,
   Dukjae Moon, and Aviya Vaidberg

Moving in Next Door: Network Flooding as a Side Channel
in Cloud Environments . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 755
   Yatharth Agarwal, Vishnu Murale, Jason Hennessey, Kyle Hogan,
   and Mayank Varia

Author Index . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 761
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