

# **2013 International Conference on Security and Cryptography**

## **(SECRYPT 2013)**

**Reykjavik, Iceland**  
**29-31 July 2013**



**IEEE Catalog Number: CFP1382N-POD**  
**ISBN: 978-1-4799-4638-9**

# CONTENTS

---

## INVITED SPEAKERS

### KEYNOTE SPEAKERS

A Data-as-a-Service Framework for IoT Big Data <i>Laurence T. Yang</i>	IS-5
IP-Oriented QoS and QoE in the Next Generation Networks - Application to Wireless Networks <i>Pascal Lorenz</i>	IS-7
The Smart Grid and the Internet should be Friends <i>Donal O'Mahony</i>	IS-9
Instantaneous Frequency Analysis <i>David Naccache</i>	

## PAPERS

### FULL PAPERS

InCC: Hiding Information by Mimicking Traffic In Network Flows <i>Luis Campo Giralte, Cristina Conde, Isaac Martin De Diego and Enrique Cabello</i>	5
Efficient Simultaneous Privately and Publicly Verifiable Robust Provable Data Possession from Elliptic Curves <i>Christian Hanser and Daniel Slamanig</i>	15
Improving Block Cipher Design by Rearranging Internal Operations <i>Liran Lerman, Jorge Nakahara Jr and Nikita Veshchikov</i>	27
A Security-enhanced Design Methodology for Embedded Systems <i>Alberto Ferrante, Jelena Milosevic and Marija Janjušević</i>	39
A Key-revocable Attribute-based Encryption for Mobile Cloud Environments <i>Tsukasa Ishiguro, Shinsaku Kiyomoto and Yutaka Miyake</i>	51
Trust-based Secure Cloud Data Storage with Cryptographic Role-based Access Control <i>Lan Zhou, Vijay Varadharajan and Michael Hitchens</i>	62
A Dynamic Watermarking Model for Embedding Reducible Permutation Graphs into Software <i>Ioannis Chionis, Maria Chroni and Stavros D. Nikolopoulos</i>	74
HoneydV6: A Low-interaction IPv6 Honeypot <i>Sven Schindler, Bettina Schnor, Simon Kiertscher, Thomas Scheffler and Eldad Zack</i>	86
Which Side Are You On? - A New Panopticon vs. Privacy <i>Miltiadis Kandiis, Lilian Mitrou, Vasilis Stavrou and Dimitris Gritzalis</i>	98
Meet-in-the-Middle Preimage Attacks Revisited - New Results on MD5 and HAVAL <i>Yu Sasaki, Wataru Komatsubara, Yasuhide Sakai, Lei Wang, Mitsugu Iwamoto, Kazuo Sakiyama and Kazuo Ohta</i>	111
Modelling SCADA and Corporate Network of a Medium Voltage Power Grid under Cyber Attacks <i>E. Ciancamerla, M. Minichino and S. Palmieri</i>	123

Towards Cryptographic Function Distinguishers with Evolutionary Circuits <i>Petr Svenda, Martin Ukrop and Vashek Matyas</i>	135
Extending the Ciphertext-Policy Attribute Based Encryption Scheme for Supporting Flexible Access Control <i>Bo Lang, Runhua Xu and Yawei Duan</i>	147
Secure Second Price Auctions with a Rational Auctioneer <i>Boaz Catane and Amir Herzberg</i>	158
iOS Encryption Systems - Deploying iOS Devices in Security-critical Environments <i>Peter Teufl, Thomas Zefferer, Christof Stromberger and Christoph Hechenblaikner</i>	170
Security Evaluation and Optimization of the Delay-based Dual-rail Pre-charge Logic in Presence of Early Evaluation of Data <i>Simone Bongiovanni, Giuseppe Scotti and Alessandro Trifiletti</i>	183
Behavior-based Malware Analysis using Profile Hidden Markov Models <i>Saradha Ravi, N. Balakrishnan and Bharath Venkatesh</i>	195
An Efficient Approach to Assessing the Risk of Zero-Day Vulnerabilities <i>Massimiliano Albanese, Sushil Jajodia, Anoop Singhal and Lingyu Wang</i>	207
Secure Alert Tracking in Supply Chain <i>Mehdi Khalfaoui, Refik Molva and Laurent Gomez</i>	219
Differential Power Analysis of HMAC SHA-2 in the Hamming Weight Model <i>Sonia Belaïd, Luk Bettale, Emmanuelle Dottax, Laurie Genelle and Franck Rondepierre</i>	230
Secure Computation of Hidden Markov Models <i>Mehrdad Aliasgari and Marina Blanton</i>	242
Adaptive Resource Management for Balancing Availability and Performance in Cloud Computing <i>Ravi Jhavar and Vincenzo Piuri</i>	254
<b>SHORT PAPERS</b>	
Privacy-preserving SVANETs - Privacy-preserving Simple Vehicular Ad-hoc Networks <i>Jan Hajny, Lukas Malina, Zdenek Martinasek and Vaclav Zeman</i>	267
Topological Study and Lyapunov Exponent of a Secure Steganographic Scheme <i>Jacques M. Bahi, Nicolas Friot and Christophe Guyeux</i>	275
LMM - A Common Component for Software License Management on Cloud <i>Shinsaku Kiyomoto, Andre Rein, Yuto Nakano, Carsten Rudolph and Yutaka Miyake</i>	284
Dynamic Proofs of Retrievability from Chameleon-Hashes <i>Stefan Rass</i>	296
On the Security of the XOR Sandwiching Paradigm for Multiple Keyed Block Ciphers <i>Ruth Ng Ii-Yung, Khoongming Khoo and Raphael C.-W. Phan</i>	305
Redactable Signature Scheme for Tree-structured Data based on Merkle Tree <i>Shoichi Hirose and Hidenori Kuwakado</i>	313
SVD-based Digital Image Watermarking on approximated Orthogonal Matrix <i>Yevhen Zolotavkin and Martti Juhola</i>	321

Massive Group Message Authentication with Revocable Anonymity <i>Boaz Catane and Amir Herzberg</i>	331
Partially Wildcarded Attribute-based Encryption and Its Efficient Construction <i>Go Ohtake, Yuki Hironaka, Kenjiro Kai, Yosuke Endo, Goichiro Hanaoka, Hajime Watanabe, Shota Yamada, Kouhei Kasamatsu, Takashi Yamakawa and Hideki Imai</i>	339
Policy-based Security Assessment of Mobile End-user Devices - An Alternative to Mobile Device Management Solutions for Android Smartphones <i>Thomas Zefferer and Peter Teufl</i>	347
Intent Security Testing - An Approach to Testing the Intent-based Vulnerability of Android Components <i>Sébastien Salva, Stassia R. Zafimiharisoa and Patrice Laurençot</i>	355
Preimage Attack on BioHashing <i>Patrick Lacharme, Estelle Cherrier and Christophe Rosenberger</i>	363
An Efficient and Provably Secure Certificateless Identification Scheme <i>Ji-Jian Chin, Raphael C.-W. Phan, Rouzbeh Behnia and Swee-Huay Heng</i>	371
Improving 802.11 Fingerprinting of Similar Devices by Cooperative Fingerprinting <i>Clémentine Maurice, Stéphane Onno, Christoph Neumann, Olivier Heen and Aurélien Francillon</i>	379
Instance-based Anomaly Method for Android Malware Detection <i>Borja Sanz, Igor Santos, Xabier Ugarte-Pedrero, Carlos Laorden, Javier Nieves and Pablo G. Bringas</i>	387
A New Fully Auditable Proposal for an Internet Voting System with Secure Individual Verification and Complaining Capabilities <i>Maidor Huarte, Iñaki Goirizelaia, Juan José Unzilla, Jon Matías and Juan J. Igarza</i>	395
Symmetric Searchable Encryption for Exact Pattern Matching using Directed Acyclic Word Graphs <i>Rolf Haynberg, Jochen Rill, Dirk Achenbach and Jörn Müller-Quade</i>	403
Enhanced Truncated Differential Cryptanalysis of GOST <i>Nicolas T. Courtois, Theodosios Mourouzis and Michal Misztal</i>	411
Privacy-preserving Realization of the STORK Framework in the Public Cloud <i>Bernd Zwattendorfer and Daniel Slamanig</i>	419
The Usability of CAPTCHAs on Smartphones <i>Gerardo Reynaga and Sonia Chiasson</i>	427
From a Logical Approach to Internal States of Hash Functions - How SAT Problem Can Help to Understand SHA- $\star$ and MD $\star$ <i>Florian Legendre, Gilles Dequen and Michaël Krajecki</i>	435
Policy-based Non-interactive Outsourcing of Computation using Multikey FHE and CP-ABE <i>Michael Clear and Ciarán McGoldrick</i>	444
Recovering RSA Private Keys on Implementations with Tampered LSBs <i>Constantinos Patsakis</i>	453
On the Effectiveness of Dynamic Taint Analysis for Protecting against Private Information Leaks on Android-based Devices <i>Golam Sarwar, Olivier Mehani, Roksana Boreli and Mohamed-Ali Kaafar</i>	461

## POSTERS

Non-random Properties of Compression and Hash Functions using Linear Cryptanalysis <i>Daniel Santana de Freitas and Jorge Nakahara Jr</i>	471
On the Connection between $t$ -Closeness and Differential Privacy for Data Releases <i>Josep Domingo-Ferrer</i>	478
AVON - A Fast Hash Function for Intel SIMD Architectures <i>Matt Henricksen and Shinsaku Kiyomoto</i>	482
Development of Device Identity using WiFi Layer 2 Management Frames for Combating Rogue APs <i>Jonny Milliken, Valerio Selis, Kian Meng Yap and Alan Marshall</i>	488
Are Biometric Web Services a Reality? - A Best Practice Analysis for Telebiometric Deployment in Open Networks <i>Dustin van der Haar and Basie von Solms</i>	494
Abusing Social Networks with Abuse Reports - A Coalition Attack for Social Networks <i>Slim Trabelsi and Hana Bouaffif</i>	500
Diagnostic Category Leakage in Helper Data Schemes for Biometric Authentication <i>Joep de Groot, Boris Skoric, Niels de Vreede and Jean-Paul Linnartz</i>	506
A Game Theory based Repeated Rational Secret Sharing Scheme for Privacy Preserving Distributed Data Mining <i>Nirali R. Nanavati and Devesh C. Jinwala</i>	512
Practical and Exposure-resilient Hierarchical ID-based Authenticated Key Exchange without Random Oracles <i>Kazuki Yoneyama</i>	518
Identity Security in Biometric Systems based on Keystroking <i>Lucjan Hanzlik and Wojciech Wodo</i>	524
Efficient Characteristic 3 Galois Field Operations for Elliptic Curve Cryptographic Applications <i>Vinay S. Iyengar</i>	531
Related-key Impossible Differential Cryptanalysis of Full-round HIGHT <i>Saeed Rostami, Sadegh Bamohabbat Chaffiri and Seyed Amir Hossein Tabatabaei</i>	537
Survey and Benchmark of Lightweight Block Ciphers for Wireless Sensor Networks <i>Mickaël Cazorla, Kevin Marquet and Marine Minier</i>	543
Privacy-enhanced Perceptual Hashing of Audio Data <i>Heiko Knospe</i>	549
Efficient Group Signatures with Verifier-local Revocation Employing a Natural Expiration <i>Lukas Malina, Jan Hajny and Zdenek Martinasek</i>	555
Public-key Cryptography from Different Assumptions - A Multi-bit Version <i>Herve Chabanne, Gerard Cohen and Alain Patey</i>	561
Not All ISPs Equally Secure Home Users - An Empirical Study Comparing Wi-Fi Security Provided by UK ISPs <i>Z. Cliffe Schreuders and Adil M. Bhat</i>	568

Approaching Encryption through Complex Number Logarithms <i>George Stergiopoulos, Miltiadis Kandias and Dimitris Gritzalis</i>	574
Keystroke Authentication with a Capacitive Display using Different Mobile Devices <i>Matthias Trojahn, Christian Schadewald and Frank Ortmeier</i>	580
MINHO - A Novel Authentication Scheme based on Pre-Authentication Service <i>Hasan Kadhem</i>	586
A Model-driven Approach for Securing Software Architectures <i>Mario Arrigoni Neri, Marco Guarnieri, Eros Magri, Simone Mutti and Stefano Paraboschi</i>	595
Database Anomalous Activities - Detection and Quantification <i>Elisa Costante, Sokratis Vavilis, Sandro Etalle, Jerry den Hartog, Milan Petkovic and Nicola Zannone</i>	603
A Preliminary Application of Generalized Fault Trees to Security <i>Daniele Codetta-Raiteri</i>	609
E3SN - Efficient Security Scheme for Sensor Networks <i>Hassan Noura, Steven Martin and Khaldoun Al Agha</i>	615
AUTHOR INDEX	623