

*Commenced Publication in 1973*

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

## Editorial Board

David Hutchison

*Lancaster University, Lancaster, UK*

Takeo Kanade

*Carnegie Mellon University, Pittsburgh, PA, USA*

Josef Kittler

*University of Surrey, Guildford, UK*

Jon M. Kleinberg

*Cornell University, Ithaca, NY, USA*

Friedemann Mattern

*ETH Zurich, Zurich, Switzerland*

John C. Mitchell

*Stanford University, Stanford, CA, USA*

Moni Naor

*Weizmann Institute of Science, Rehovot, Israel*

C. Pandu Rangan

*Indian Institute of Technology, Madras, India*

Bernhard Steffen

*TU Dortmund University, Dortmund, Germany*

Demetri Terzopoulos

*University of California, Los Angeles, CA, USA*

Doug Tygar

*University of California, Berkeley, CA, USA*

Gerhard Weikum

*Max Planck Institute for Informatics, Saarbrücken, Germany*


More information about this series at <http://www.springer.com/series/7410>


Josef Pieprzyk · Suriadi Suriadi (Eds.)

# Information Security and Privacy

22nd Australasian Conference, ACISP 2017  
Auckland, New Zealand, July 3–5, 2017  
Proceedings, Part I

*Editors*

Josef Pieprzyk   
Queensland University of Technology  
Brisbane, QLD  
Australia

Suriadi Suriadi   
Queensland University of Technology  
Brisbane, QLD  
Australia

ISSN 0302-9743                      ISSN 1611-3349 (electronic)  
Lecture Notes in Computer Science  
ISBN 978-3-319-60054-3              ISBN 978-3-319-60055-0 (eBook)  
DOI 10.1007/978-3-319-60055-0

Library of Congress Control Number: 2017943039

LNCS Sublibrary: SL4 – Security and Cryptology

© Springer International Publishing AG 2017

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Printed on acid-free paper

This Springer imprint is published by Springer Nature  
The registered company is Springer International Publishing AG  
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

# Preface

The 22nd Australasian Conference on Information Security and Privacy was organized in beautiful New Zealand on the Massey University campus in Auckland, July 3–5, 2017. This was the first time that the conference was organized outside Australia.

This year we received 150 submissions. Each paper got assigned to four referees. In the first stage of the review process, the submitted papers were read and evaluated by the Program Committee members. In the second stage, the papers were scrutinized during an extensive discussion. Finally, the Program Committee chose 45 regular and ten short papers to be included in the conference program. The authors of the accepted papers had ten days for revision and preparation of final versions. The revised papers were not subject to editorial review and the authors bear full responsibility for their contents. The submission and review process was supported by the EasyChair conference submission server. We thank the EasyChair people for letting us use it.

The Program Committee voted for the best paper using the Doodle software. We nominated four papers with best reviews. Out of the four, two papers were the preferred options with no clear winner. We decided to award the ACISP2017 Best Paper Award to the two papers:

- “Dynamic Searchable Symmetric Encryption with Physical Deletion and Small Leakage” by Peng Xu, Shuai Liang, Wei Wang, Willy Susilo, Qianhong Wu and Hai Jin
- “Multi-user Cloud-Based Secure Keyword Search” by Shabnam Kasra Kerman-shahi, Joseph K. Liu and Ron Steinfeld

The awards were handed during the conference dinner.

The Jennifer Seberry Lecture this year was delivered by Clark Thomborson from the University of Auckland, New Zealand. The keynote lecture was presented by L. Jean Camp from Indiana University, USA. The program also included invited talks by well-known researchers working in different areas of cybersecurity. They were Dong Seong Kim, University of Canterbury, New Zealand; Dongxi Liu, CSIRO/Data61, Australia; Surya Nepal, CSIRO/Data61, Australia; Paul Pang, Unitec Institute of Technology, New Zealand; Peter Pilley, Department of Internal Affairs, New Zealand; Ian Welch, Victoria University of Wellington, New Zealand and Henry B. Wolfe, University of Otago, New Zealand.

We would like to thank the Program Committee members and the external reviewers for their effort and time to evaluate the submissions. Big thanks go to Julian Jang-Jaccard and Paul Watters for their excellent job in the organization of the conference. We are indebted to the team at Springer for their continuous support of the conference and for their help in the production of the conference proceedings.

July 2017

Josef Pieprzyk  
Suriadi Suriadi

# ACISP 2017

The 22nd Australasian Conference on Information Security  
and Privacy

Massey University, Auckland, New Zealand  
July 3–5, 2017

**In Co-operation with IACR**



**Sponsored by Massey University**



## General Co-chairs

Julian Jang-Jaccard  
Paul Watters

Massey University, New Zealand  
La Trobe University, Australia

## Program Co-chairs

Josef Pieprzyk  
Suriadi Suriadi

Queensland University of Technology, Australia  
Queensland University of Technology, Australia

## Program Committee

Cristina Alcaraz  
Claudio Agostino Ardagna  
Giuseppe Ateniese  
Man Ho Au  
Milton Baar  
Joonsang Baek  
Lynn Batten  
Colin Boyd

University of Malaga, Spain  
Università degli Studi di Milano, Italy  
Stevens Institute of Technology, USA  
Hong Kong Polytechnic University, SAR China  
Macquarie University, Australia  
Khalifa University of Science, UAE  
Deakin University, Australia  
Norwegian University of Science and Technology,  
Norway  
RMIT University, Australia  
University of Texas at Dallas, USA  
University of Salerno, Italy  
Leidos and Johns Hopkins University, USA  
University Technology Sydney, Australia

Serdar Boztas  
Alvaro Cardenas  
Aniello Castiglione  
Ebrima Ceesay  
Jinjun Chen

Shiping Chen	Data61 - CSIRO, Australia
Xiaofeng Chen	Xidian University, China
Kim-Kwang	University of Texas at San Antonio, USA
Raymond Choo	
Christophe Doche	Macquarie University, Australia
Ernest Foo	Queensland University of Technology, Australia
David Galindo	University of Birmingham, UK
Colm Gannon	DCET - Internal Affairs, New Zealand
Swee-Huay Heng	Multimedia University, Malaysia
Andreas Holzer	Google Inc., USA
Xinyi Huang	Fujian Normal University, China
Mitsugu Iwamoto	University of Electro-Communications, Japan
Sanjay Jha	University of New South Wales, Australia
Akinori Kawachi	The University of Tokushima, Japan
Peter Kieseberg	SBA Research, Austria
Dong Seong Kim	University of Canterbury, New Zealand
Howon Kim	Pusan National University, South Korea
Jongkil Kim	Data61 - CSIRO, Australia
Ryan Ko	University of Waikato, New Zealand
Marina Krotofil	Hamburg University of Technology, Germany
Noboru Kunihiro	University of Tokyo, Japan
Mirosław Kutylowski	Wrocław University of Science and Technology, Poland
Junzuo Lai	Singapore Management University, Singapore
Shujun Li	University of Surrey, UK
Kaitai Liang	Aalto University, Finland
Dongxi Liu	Data61 - CSIRO, Australia
Joseph Liu	Monash University, Australia
Shengli Liu	Shanghai Jiao Tong University, China
Javier Lopez	University of Malaga, Spain
Jiqiang Lu	Institute for Infocomm Research, Singapore
Rongxing Lu	University of New Brunswick, Canada
Félix Gómez Mármol	University of Murcia, Spain
Weizhi Meng	Technical University of Denmark, Denmark
Kazuhiko Minematsu	NEC Corporation, Japan
Chris Mitchell	Royal Holloway - University of London, UK
Paweł Morawiecki	Polish Academy of Sciences, Poland
Kirill Morozov	Tokyo Institute of Technology, Japan
Yi Mu	University of Wollongong, Australia
Surya Nepal	Data61 - CSIRO, Australia
Ivica Nikolić	Nanyang Technological University, Singapore
Thomas Peyrin	Nanyang Technological University, Singapore
Man Qi	Canterbury Christ Church University, UK
Kenneth Radke	Queensland University of Technology and CERT Australia, Australia
Reza Reyhanitabar	NEC Laboratories Europe, Germany

Jun Shao	Zhejiang Gongshang University, China
Taeshik Shon	Ajou University, South Korea
Haya Shulman	Fraunhofer SIT, Germany
Tony Skjellum	Auburn University, USA
Ron Steinfeld	Monash University, Australia
Chunhua Su	Japan Advanced Institute of Science and Technology, Japan
Willy Susilo	University of Wollongong, Australia
Shaohua Tang	South China University of Technology, China
Juan Tapiador	Universidad Carlos III de Madrid, Spain
Clark Thomborson	University of Auckland, New Zealand
Fergus Toolan	UCD School of Computer Science, Ireland
Petros Wallden	University of Edinburgh, UK
Cong Wang	City University of Hong Kong, SAR China
Huaxiong Wang	Nanyang Technological University, Singapore
Yu Wang	Deakin University, Australia
George Weir	University of Strathclyde, UK
Sheng Wen	Deakin University, Australia
Henry B. Wolfe	University of Otago, New Zealand
Chi Yang	Unitec Institute of Technology, New Zealand
Guomin Yang	University of Wollongong, Australia
Yanjiang Yang	Huawei Singapore Research Center, Singapore
Wun-She Yap	Universiti Tunku Abdul Rahman, Malaysia
Xun Yi	RMIT University, Australia
Tsz Hon Yuen	Huawei Singapore Research Center, Singapore
Aaram Yun	Ulsan National Institute of Science and Technology, South Korea
Xuyun Zhang	University of Auckland, New Zealand

## Additional Reviewers

Fatma Al Maqbali	Ed Dawson	Andrei Kelarev
Janaka Alawatugoda	Nabil El Ioini	Jeongsu Kim
Yoshinori Aono	Gerardo Fernandez	Jianchang Lai
Shahriar Badsha	Filippo Gaudenzi	Anna Lauks-Dutka
Anubhab Baksi	Junqing Gong	Hyung Tae Lee
Arcangelo Castiglione	Zheng Gong	Nan Li
Luigi Catuogno	Fuchun Guo	Xiaoyu Li
Claire Che	Jian Guo	Xingye Lu
Jiahui Chen	Jingjing Guo	Lin Lyu
Jie Chen	Felix Günther	Jinhua Ma
Rongmao Chen	Jinguang Han	Moesfa Soeheila
Ji-Jian Chin	Shuai Han	Mohamad
Craig Costello	Yasufumi Hashimoto	Mihai Moraru
Hui Cui	Shoichi Hirose	Khoa Nguyen



Phuong Ha Nguyen  
Tobias Nilges  
David Nuñez  
Xu Peiming  
Jiang Peng  
Thye Way Phua  
Ananth Raghunathan  
Fang-Yu Rao  
Juan E. Rubio  
Kyoji Shibutani  
Siang Meng Sim  
Le Su

Bing Sun  
Benjamin HongMengTan  
Syh-Yuan Tan  
Srinivas Vivek  
Riad Wahby  
Jianfeng Wang  
Yunling Wang  
Yunhua Wen  
Qianhong Wu  
Lingling Xu  
Rui Xu  
Shengmin Xu

Shota Yamada  
Xu Yang  
Yu Yu  
Zuoxia Yu  
Shiwei Zhang  
Xiao Zhang  
Xiaoyu Zhang  
Yuexin Zhang  
Zongyang Zhang  
Peng Zhiniang

## **Abstracts of Invited Talks**

# Jennifer Seberry Lecture: Contextual Privacy

Clark Thomborson

Computer Science Department  
University of Auckland, Auckland, New Zealand  
cthombor@cs.auckland.ac.nz

**Abstract.** Could you design a computer system which respects all forms of privacy that are relevant to its users? What forms of privacy are important to you personally, and in what contexts are they important? How can a user obtain a “private place” in a computerised system? Is it feasible and economic for a system to afford a particular form of privacy to its users? Is it socially appropriate, or legal, for a system to grant a privacy request? Which privacy requests should be denied? Can you identify all of the “assets at risk” in a privacy-protective system? I won’t attempt to answer any of these questions fully! However I will get you started on finding your own answers, for the next system you design, for the next privacy analysis you perform, and for the next system you use. My explanations are grounded in Lawrence Lessig’s taxonomy of control and liberty, in Alan Westin’s taxonomy of private states, in Helen Nissenbaum’s legal theory of contextual integrity, and in the Jericho Forum’s Identity Commandments. I’ll draw examples from commonly-encountered systems such as Facebook.

# Key Note Lecture: Security as Risk Communication

L. Jean Camp

School of Informatics  
Indiana University, Indianapolis, USA  
ljcamp@indiana.edu

**Abstract.** In usable security design, opaque designs enable the user take an action seamlessly rather than requiring some understanding of the underlying system design. However, security choices inherently require some information, or the default option is to prevent all risky behaviors without interaction. In fact, blocking desired action without communication is one reason that individuals may abandon security technologies even when the risks these technologies mitigate are known.

Incentives cannot work unless there are two conditions. First, the incentives must be visible. Second, there must be a clear action to take in response to the incentives. Both of these outcomes are the goal of translucent design. A truly transparent design can overwhelm and under-inform the user with information about configuration, the nature of the security technology, and the elements of a risk that are mitigated.

Risk communication allows individuals to easily see the consequences of their action. The ideal design, of making visible user-action-system-consequence, may be overwhelming or context-dependent. Risk communication is neither transparent nor opaque; but rather consists of security technologies that are easy to use, communicate risk choices only to the degree necessary to avoid inadvertent fatal choices, can be overcome in a straight-forward manner if the individual chooses to take a risk, or if the system is in error.

# **Key Note Lecture: I Was Sure that Was My Password... and Other Just so Law Enforcement Stories**

Peter Pilley

Department of Internal Affairs, Manukau, New Zealand

**Abstract.** With the advent of communications devices and software being encrypted by design there is now a number of new risks presenting themselves some predicted and some only becoming apparent now.

Who owns the data that is encrypted? What right or access does a family have to the encrypted data of a sibling or Son/Daughter at the time of their death? How can law enforcement be seen to be able to successfully investigate a suspect if they have taken steps to encrypt their communications platform or device?

These are not new fears or technologies but they do raise some interesting questions and scenarios. Encrypted networks such as TOR and platforms such as WhatsApp are potentially removing the traditional investigation methods from the investigator Agencies are turning to, and in some instances failing in the use of., more advanced interception techniques. How do we as Law Enforcement manage this, and more importantly how as a community do we need to see it managed?

# Graphical Security Models

Dong Seong Kim

Department of Computer Science and Software Engineering  
University of Canterbury, Christchurch, New Zealand  
`dongseong.kim@canterbury.ac.nz`

**Abstract.** Graphical security models can be used to assess the network security. Purely graph based (e.g., Attack Graphs) security models have a state-space explosion problem. Tree-based models (e.g., Attack Trees) cannot capture the attack paths information explicitly. In this talk, we briefly introduce a scalable security model named hierarchical attack representation models (HARM) to deal with the above mentioned issues. First, I present how the HARM with other methods to evaluate the effectiveness of Moving Target Defenses. Second, I present how the HARM can be used to evaluate the security of Internet of Things. Finally, research revenues in the graphical security modeling and assessment will be discussed in brief.

# Compact-LWE for Lightweight Public Key Encryption and Leveled IoT Authentication

Dongxi Liu

CSIRO, Data61, Melbourne, Australia  
Dongxi.Liu@data61.csiro.au

**Abstract.** Leveled authentication allows resource-constrained IoT devices to be authenticated at different strength levels according to the particular types of communication. To achieve efficient leveled authentication, a lightweight public key encryption scheme is introduced in this talk, which can produce very short ciphertexts without sacrificing its security.

The semantic security of this scheme is based on the Learning With Secretly Scaled Errors in Dense Lattice (referred to as Compact-LWE) problem designed in CSIRO. This problem is a variant of the Learning With Errors (LWE) problem, but with two improvements (i.e., secretly scaled errors, which can be very big, and dense lattice, which has small fundamental parallelepiped) that make Compact-LWE resistant against well-known lattice-based attacks to LWE. In addition to the security proof, we verify, with a public attack tool, that the lattice-based attacks, which are successful on LWE, cannot succeed on Compact-LWE even for a small dimension parameter (e.g., a lattice of dimension 13).

The evaluation of our scheme and a leveled Needham-Schroeder-Lowe public key authentication protocol on the Contiki operating system and Sky motes will also be introduced.

# Orchestration and Automation of Cybersecurity: Issues and Challenges

Surya Nepal

Data61 CSIRO, Canberra, Australia  
surya.nepal@data61.csiro.au

**Abstract.** Almost all present cybersecurity expenditure and activities (85%) focuses on designing solutions to prevent known cybersecurity threats. No matter how much efforts are put in preparation and prevention, these solutions are not working and cyberattacks and data breaches are inevitable. Current compromise-to-discovery time can be 30 to 60 days. One the one hand, the number of incidents of cyberattacks and data breaches are increasing every year; the increase in time required to detect cyberattacks and data breaches is causing higher reputational, operational and economic loss due to the impact on the continuity of the business. On the other hand, we have a limited pool of security experts who can focus on human-intensive tasks such as analysing programs/protocols, designing patches, understanding a compromise and responding/recovering from a compromise. Current approaches are mostly manual, signature base, reactive and not robust and resilient. Furthermore, the increasing complexity of the cyberspace and its dynamic nature makes it impossible for humans to effectively secure and protect the cyber system. These space requires a paradigm shift towards more orchestrated and automated cybersecurity solutions so security experts could be more efficiently utilised and small-to-medium businesses can have access to more advanced cybersecurity capabilities through software-as-a-service. A number of organisations have already started taking some actions to automate and orchestrate incident response processes, while researchers have started to explore the coordinated response of the human body immune system towards building autonomic, resilient cyber systems. This talk explores the potential opportunities and issues to automate and orchestrate cybersecurity solutions.



# UniteCloud: A Resilient Private Cloud Platform for Education and Research Service

Paul S. Pang

High Tech Transdisciplinary Research Network  
and Department of Computer Science  
Unitec Institute of Technology, Auckland, New Zealand  
ppang@unitec.ac.nz

**Abstract.** UniteCloud is a cloud-computing platform developed in Unitec Institute of Technology to provide a solution to resilient infrastructure and data services. UniteCloud has been constructed using OpenStack with its peak computational capability up to 500 virtual machines and maximum storage allocation 64 tera-bytes per virtual machine. The resiliency of UniteCloud is achieved by three novel components. CloudViz-3D is a top-level interactive cloud monitoring system that monitors the running status of cloud and notifies users before any disaster occurs. rVVM is a low latency and high consistency high availability system that generates real time backup and disaster recovery. CRaaS is an offline disaster recovery system that provides decentralized service checkpoint/restart over commodity networks. In addition, the platform supports group collaborative working, editing, big data processing and machine learning algorithmic experiments with its open source implementation of Gitlab, ShareLatex, HadoopDataCenter and TensorFlow. With all its resilient service features, UniteCloud is specializing in supplying eLearning and eResearch services for New Zealand tertiary students and staffs.

# Software Defined Networking as a Security Enabler for Enterprises

Ian Welch

School of Engineering and Computer Science  
Victoria University of Wellington, Wellington  
New Zealand

`ian.welch@vuw.ac.nz`

**Abstract.** Industry commentators have raised concerns about software-defined networking (SDN) as looking “like a nice squishy target to spies and crooks” and a “nightmare” from a risk assessment point-of-view. Security concerns include worries that it will be impossible to secure the perimeter because the network architecture is no longer fixed, the controller managing the control plane is centralised, and a single point of failure and the software-centric approach is highly vulnerable to exploitation as opposed to current hardware-based approaches.

We argue that some of these concerns are not new and software defined network provides an approach to implementing secure enterprise networks that can lead to better enforcement and greater assurance. This talk will address concerns and explain how we are working with other academics and commercial partners on the development of a software defined security platform that leverages these advantages over traditional approaches.

# Mobile Phone Security Issues

Henry B. Wolfe

Department of Information Science  
University of Otago, Dunedin, New Zealand  
hank.wolfe@otago.ac.nz

**Abstract.** We take for granted every day that we are safe from any given risk because we are protected by various standards, statutes, and laws. The mobile phone has become ubiquitous and there are currently more than 8 billion connections and almost 5 billion mobile phones in use around the world. It is really nothing more than a small computer with a radio transmitter and receiver and other communications devices (Wi-Fi, Bluetooth, etc) integrated into it. Smart phones may also have the ability to record photos, videos and sound. Most have a built in Global Positioning Satellite System capability. Some phones may also have Near Field Communications (NFC). Each of these capabilities may result in various risks. Every generation of mobile phone has expanded its capabilities and we are now able to communicate with the Internet in addition to normal telephone activity.

A long with these capabilities come a number of risks. Some of these are normally associated with using the Internet, so mobile users are exposed to malware of various kinds from that source. However, there are other more insidious risks that are less known. The purpose of this presentation is to discuss the current risks associated with mobile phone use including malware; loss, theft, seizure; communications interception, loss of privacy; location logging and tracking; and bugging. Most people are not aware of these threats. They assume that their service provider has put in place measures to eliminate any risks as well as protect their privacy (by the use of cryptography). 100% safe mobile phone use will unlikely ever be possible. This presentation will cover mitigating alternatives that can be put in place to reduce the identified mobile phone risks. These will be graphically portrayed and clearly described and defined in terms and language that non-technical people will understand.

# Contents – Part I

## Public Key Encryption

Tightly-Secure Encryption in the Multi-user, Multi-challenge Setting with Improved Efficiency. . . . .	3
<i>Puwen Wei, Wei Wang, Bingxin Zhu, and Siu Ming Yiu</i>	
Hierarchical Functional Encryption for Linear Transformations . . . . .	23
<i>Shiwei Zhang, Yi Mu, Guomin Yang, and Xiaofen Wang</i>	
KDM-Secure Public-Key Encryption from Constant-Noise LPN . . . . .	44
<i>Shuai Han and Shengli Liu</i>	
Long-Term Secure Commitments via Extractable-Binding Commitments . . . .	65
<i>Ahto Buldas, Matthias Geihs, and Johannes Buchmann</i>	

## Attribute-Based Encryption

New Proof Techniques for DLIN-Based Adaptively Secure Attribute-Based Encryption. . . . .	85
<i>Katsuyuki Takashima</i>	
Attribute-Based Encryption with Expressive and Authorized Keyword Search . . . . .	106
<i>Hui Cui, Robert H. Deng, Joseph K. Liu, and Yingjiu Li</i>	
Towards Revocable Fine-Grained Encryption of Cloud Data: Reducing Trust upon Cloud . . . . .	127
<i>Yanjiang Yang, Joseph Liu, Zhuo Wei, and Xinyi Huang</i>	

## Identity-Based Encryption

Mergeable and Revocable Identity-Based Encryption . . . . .	147
<i>Shengmin Xu, Guomin Yang, Yi Mu, and Willy Susilo</i>	
ID-Based Encryption with Equality Test Against Insider Attack . . . . .	168
<i>Tong Wu, Sha Ma, Yi Mu, and Shengke Zeng</i>	
Lattice-Based Revocable Identity-Based Encryption with Bounded Decryption Key Exposure Resistance. . . . .	184
<i>Atsushi Takayasu and Yohei Watanabe</i>	

## Searchable Encryption

Dynamic Searchable Symmetric Encryption with Physical Deletion and Small Leakage . . . . .	207
<i>Peng Xu, Shuai Liang, Wei Wang, Willy Susilo, Qianhong Wu, and Hai Jin</i>	
Multi-user Cloud-Based Secure Keyword Search. . . . .	227
<i>Shabnam Kasra Kermanshahi, Joseph K. Liu, and Ron Steinfeld</i>	
Fuzzy Keyword Search and Access Control over Ciphertexts in Cloud Computing . . . . .	248
<i>Hong Zhu, Zhuolin Mei, Bing Wu, Hongbo Li, and Zongmin Cui</i>	
Secure and Practical Searchable Encryption: A Position Paper . . . . .	266
<i>Shujie Cui, Muhammad Rizwan Asghar, Steven D. Galbraith, and Giovanni Russello</i>	

## Cryptanalysis

Fault Attacks on XEX Mode with Application to Certain Authenticated Encryption Modes. . . . .	285
<i>Hassan Qahur Al Mahri, Leonie Simpson, Harry Bartlett, Ed Dawson, and Kenneth Koon-Ho Wong</i>	
How to Handle Rainbow Tables with External Memory. . . . .	306
<i>Gildas Avoine, Xavier Carpent, Barbara Kordy, and Florent Tardif</i>	
Improved Factoring Attacks on Multi-prime RSA with Small Prime Difference. . . . .	324
<i>Mengce Zheng, Noboru Kunihiro, and Honggang Hu</i>	
Efficient Compilers for After-the-Fact Leakage: From CPA to CCA-2 Secure PKE to AKE. . . . .	343
<i>Suvradip Chakraborty, Goutam Paul, and C. Pandu Rangan</i>	
Improved Integral Attack on HIGHT. . . . .	363
<i>Yuki Funabiki, Yosuke Todo, Takanori Isobe, and Masakatu Morii</i>	
Cryptanalysis of Simpira v2 . . . . .	384
<i>Ivan Tjuawinata, Tao Huang, and Hongjun Wu</i>	
Statistical Integral Distinguisher with Multi-structure and Its Application on AES . . . . .	402
<i>Tingting Cui, Ling Sun, Huaifeng Chen, and Meiqin Wang</i>	
Conditional Differential Cryptanalysis for Kreyvium . . . . .	421
<i>Yuhei Watanabe, Takanori Isobe, and Masakatu Morii</i>	

**Digital Signatures**

Practical Strongly Invisible and Strongly Accountable Sanitizable Signatures . . . . .	437
<i>Michael Till Beck, Jan Camenisch, David Derler, Stephan Krenn, Henrich C. Pöhls, Kai Samelin, and Daniel Slamanig</i>	
Tightly-Secure Signatures from the Decisional Composite Residuosity Assumption. . . . .	453
<i>Xiao Zhang, Shengli Liu, and Dawu Gu</i>	
<b>Author Index</b> . . . . .	469

## Contents – Part II

### Symmetric Cryptography

Analysis of Toeplitz MDS Matrices. . . . .	3
<i>Sumanta Sarkar and Habeeb Syed</i>	
Reforgeability of Authenticated Encryption Schemes . . . . .	19
<i>Christian Forler, Eik List, Stefan Lucks, and Jakob Wenzel</i>	
Indifferentiability of Double-Block-Length Hash Function Without Feed-Forward Operations. . . . .	38
<i>Yusuke Naito</i>	

### Software Security

FFFuzzer: Filter Your Fuzz to Get Accuracy, Efficiency and Schedulability . . .	61
<i>Fan Jiang, Cen Zhang, and Shaoyin Cheng</i>	
Splitting Third-Party Libraries' Privileges from Android Apps . . . . .	80
<i>Jiawei Zhan, Quan Zhou, Xiaozhuo Gu, Yuewu Wang, and Yingjiao Niu</i>	
SafeStack <sup>+</sup> : Enhanced Dual Stack to Combat Data-Flow Hijacking . . . . .	95
<i>Yan Lin, Xiaoxiao Tang, and Debin Gao</i>	

### Network Security

Prover Efficient Public Verification of Dense or Sparse/Structured Matrix-Vector Multiplication . . . . .	115
<i>Jean-Guillaume Dumas and Vincent Zucca</i>	
JSFfox: Run-Timely Confining JavaScript for Firefox . . . . .	135
<i>Weizhong Qiang, JiaZhen Guo, Hai Jin, and Weifeng Li</i>	

### Malware Detection

PriMal: Cloud-Based Privacy-Preserving Malware Detection. . . . .	153
<i>Hao Sun, Jinshu Su, Xiaofeng Wang, Rongmao Chen, Yujing Liu, and Qiaolin Hu</i>	
A New Malware Classification Approach Based on Malware Dynamic Analysis. . . . .	173
<i>Ying Fang, Bo Yu, Yong Tang, Liu Liu, Zexin Lu, Yi Wang, and Qiang Yang</i>	

## Privacy

Privacy-Preserving Aggregation of Time-Series Data with Public Verifiability from Simple Assumptions . . . . .	193
<i>Keita Emura</i>	
Privacy-Utility Tradeoff for Applications Using Energy Disaggregation of Smart-Meter Data . . . . .	214
<i>Mitsuhiro Hattori, Takato Hirano, Nori Matsuda, Rina Shimizu, and Ye Wang</i>	
Private Graph Intersection Protocol . . . . .	235
<i>Fucaï Zhou, Zifeng Xu, Yuxi Li, Jian Xu, and Su Peng</i>	
Computing Aggregates Over Numeric Data with Personalized Local Differential Privacy . . . . .	249
<i>Mousumi Akter and Tanzima Hashem</i>	
An Efficient Toolkit for Computing Private Set Operations . . . . .	261
<i>Alex Davidson and Carlos Cid</i>	

## Authentication

Privacy-Preserving k-time Authenticated Secret Handshakes . . . . .	281
<i>Yangguang Tian, Shiwei Zhang, Guomin Yang, Yi Mu, and Yong Yu</i>	
Exploring Effect of Location Number on Map-Based Graphical Password Authentication . . . . .	301
<i>Weizhi Meng, Wang Hao Lee, Man Ho Au, and Zhe Liu</i>	
A QR Code Watermarking Approach Based on the DWT-DCT Technique. . .	314
<i>Yang-Wai Chow, Willy Susilo, Joseph Tonien, and Wei Zong</i>	

## Elliptic Curve Cryptography

Generating Complete Edwards Curves . . . . .	335
<i>Theo Fanuela Prabowo and Chik How Tan</i>	
Secure GLS Recomposition for Sum-of-Square Cofactors. . . . .	349
<i>Eunkyung Kim and Mehdi Tibouchi</i>	
Differential Addition on Twisted Edwards Curves . . . . .	366
<i>Reza Rezaeian Farashahi and Seyed Gholamhossein Hosseini</i>	



**Short Papers**

Certificate Transparency with Enhancements and Short Proofs . . . . .	381
<i>Abhishek Singh, Binanda Sengupta, and Sushmita Ruj</i>	
Update-Tolerant and Revocable Password Backup. . . . .	390
<i>Moritz Horsch, Johannes Braun, Dominique Metz, and Johannes Buchmann</i>	
Redactable Graph Hashing, Revisited (Extended Abstract) . . . . .	398
<i>Andreas Erwig, Marc Fischlin, Martin Hald, Dominik Helm, Robert Kiel, Florian Kübler, Michael Kümmerlin, Jakob Laenge, and Felix Rohrbach</i>	
On the Security of Designing a Cellular Automata Based Stream Cipher . . . .	406
<i>Swapan Maiti, Shamit Ghosh, and Dipanwita Roy Chowdhury</i>	
Stegogames . . . . .	414
<i>Clark Thomborson and Marc Jeanmougin</i>	
A Feasibility Evaluation of Fair and Privacy-Enhanced Matchmaking with Identity Linked Wishes. . . . .	422
<i>Dwight Horne and Suku Nair</i>	
Fully Context-Sensitive CFI for COTS Binaries . . . . .	435
<i>Weizhong Qiang, Yingda Huang, Deqing Zou, Hai Jin, Shizhen Wang, and Guozhong Sun</i>	
Dual-Mode Cryptosystem Based on the Learning with Errors Problem. . . . .	443
<i>Jingnan He, Wenpan Jing, Bao Li, Xianhui Lu, and Dingding Jia</i>	
Process Control Cyber-Attacks and Labelled Datasets on S7Comm Critical Infrastructure. . . . .	452
<i>Nicholas R. Rodofile, Thomas Schmidt, Sebastian T. Sherry, Christopher Djamaludin, Kenneth Radke, and Ernest Foo</i>	
Solving the DLP with Low Hamming Weight Product Exponents and Improved Attacks on the GPS Identification Scheme. . . . .	460
<i>Jason H.M. Ying and Noboru Kunihiro</i>	
<b>Author Index</b> . . . . .	469