

*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>

Raphael C.-W. Phan · Moti Yung (Eds.)

# Paradigms in Cryptology – Mycrypt 2016

Malicious and Exploratory Cryptology

Second International Conference, Mycrypt 2016  
Kuala Lumpur, Malaysia, December 1–2, 2016  
Revised Selected Papers

*Editors*

Raphael C.-W. Phan  
Multimedia University, MMU  
Cyberjaya  
Malaysia

Moti Yung  
Snap and Columbia University  
New York, NY  
USA

ISSN 0302-9743                      ISSN 1611-3349 (electronic)  
Lecture Notes in Computer Science  
ISBN 978-3-319-61272-0              ISBN 978-3-319-61273-7 (eBook)  
DOI 10.1007/978-3-319-61273-7

Library of Congress Control Number: 2017944355

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 first and only Mycrypt up to 2015 was Mycrypt 2005, wherein an unconventional cryptography session featured papers with ideas that were beyond the norm. Since Mycrypt 2005, substantial breakthroughs have been made in crypto and security in the past decade, including notions pertaining to malicious security, i.e., where security is no longer simply against bad guys but where good guys who are conventionally viewed as mostly defensive can equally be adversarial. These align well with recent trends wherein trusted parties need not necessarily be trustworthy, and where insiders can potentially be malicious.

Mycrypt 2016 was a rejuvenation of the Mycrypt series with a particular focus on paradigm-shifting crypto research and thinking outside the current box. Jointly organized by the Multimedia University and Cyber Security Malaysia in cooperation with the International Association for Cryptologic Research (IACR), it was held in Kuala Lumpur, Malaysia, during December 1–2, 2016, at the Pullman Kuala Lumpur City Centre Hotel, just before Asiacypt 2016 took place in Hanoi.

The technical Program Committee (PC) comprised 41 experts from 19 countries with an additional 51 external reviewers. We adopted a hybrid journal-like style where there were two separate and independent calls each with its own review process. Each submission was put through two stages, where after stage one some papers without major issues were accepted or those without scientific merit rejected, while others were put through to stage two for a further review after obtaining rebuttals from authors. Every worthwhile submission was reviewed by at least two reviewers, and up to six reviewers for some submissions requiring substantial deliberations. The server handling the submissions, reviews, and discussions was hosted by Microsoft via its Conference Management Toolkit (CMT). We thank all the PC members and external reviewers for their passion and commitment to see this through. Note that in defying convention, we have listed the PC and external reviewers in alphabetical order based on first name first! This is not a new paradigm, but is somewhat unusual in the West.

A total of 51 complete submissions were processed through the review phases after filtering checks, from which 21 papers were finally accepted for inclusion in the technical program, with authors spanning 14 countries. Of these submissions, three paradigm-revisiting papers that garnered a significant number of positive comments and interest from PC members and external reviewers are listed in these proceedings under the “Revisiting Tradition” category. Papers under “Different Paradigms” touch on alternative or new perspectives on doing cryptography, while the “Cryptofication” papers aim to bridge the gap between the physical world and the cryptographic world. “Malicious Crypto” papers deal with the issues of backdoors, malware, and leakages, while papers under “Advances in Cryptanalysis” aim to revisit existing cryptanalytic techniques toward new formulations or measures. The “Primitives and Features” papers are those that propose new variants of cryptographic primitives or new features. Finally, the “Cryptanalysis Correspondence” section presents two concise papers that

had the unique feature of being able to obtain rebuttals from the authors of the attacked schemes as part of an extended review process.

After much deliberation and considering the points made by PC members and external reviewers, the paper “Another Look at Tightness II: Practical Issues in Cryptography” by Sanjit Chatterjee, Neal Koblitz, Alfred Menezes and Palash Sarkar was awarded Best Paper.

Mycrypt 2016 had the pleasure of two keynote talks, namely, Xavier Boyen of QUT speaking on human primacy in crypto and Neal Koblitz of the University of Washington discussing paradigm shifts in our disciplinary culture. There was also an IEICE invited talk sponsored by the IEICE Malaysia Section, by Goichiro Hanaoka on user-friendly crypto.

As an additional twist to an otherwise conventionally structured program, several Insight Papers were solicited for presentation at Mycrypt 2016 and/or inclusion in the proceedings. Insight Papers were invited from researchers on their celebrated or recent breakthrough results: these were notably on multi-prover interactive proofs, human encryption, algebraic cryptanalysis, watermarking programs, polytopic cryptanalysis, and the division property. Authors of such papers had the option of presenting at Mycrypt 2016 physically or pre-recording a video clip to be shown during Mycrypt 2016 to the audience.

We thank the general chairs, Wei-Chuen Yau and Geong-Sen Poh, as well as the local secretariat led by Cyber Security Malaysia for supporting the venue logistics and outreach. We are also grateful to Tourism Malaysia for sponsoring the cultural dance performance during the banquet dinner.

Starting with Mycrypt 2016, the Mycrypt series will continue to focus on beyond-norm, paradigm-shifting, unconventional cryptography as we firmly believe that a field can only advance if its research community revisits conventional paradigms, rocks the crypto boat, questions the status quo, and raises controversial issues. Mycrypt will thus henceforth be known as the International Conference on *Malicious and Exploratory Cryptology*, and be co-located with major crypto/security conferences to maximize the impact of its frontier-stretching theme.

April 2017

Raphaël C.-W. Phan  
Moti Yung

# Organization

## Program Chairs

Raphaël C.-W. Phan  
Moti Yung

MMU, Malaysia  
Snap and Columbia University, USA

## General Chairs

Wei-Chuen Yau  
Geong-Sen Poh

Xiamen University, Malaysia  
MIMOS, Malaysia

## Program Committee

Adam Young  
Angelos Kiayias

Ahmad-Reza Sadeghi  
Alfred Menezes  
Andrew Odlyzko  
Angela Sasse  
Arjen Lenstra  
Bart Preneel  
Catherine Meadows  
Chris Mitchell  
David Naccache  
Ed Dawson

Elisa Bertino  
Graham Steel  
Gregory Neven  
Helena Handschuh  
Ivan Visconti  
Jean-Philippe Aumasson  
Jonathan Katz  
Josef Pieprzyk  
Kaoru Kurosawa  
Kristian Gjøsteen  
Lars Knudsen  
Marine Minier  
Markus Dürmuth  
Markus Jakobsson  
Moti Yung (Chair)

Cryptovirology Labs, USA  
National and Kapodistrian University of Athens,  
Greece  
Technische Universität (TU) Darmstadt, Germany  
University of Waterloo, Canada  
University of Minnesota, USA  
University College London (UCL), UK  
EPFL, Switzerland  
University of Leuven (KU Leuven), Belgium  
Naval Research Lab, USA  
Royal Holloway, University of London (RHUL), UK  
Université Paris II, France  
Queensland University of Technology (QUT),  
Australia  
Purdue University, USA  
Inria, France  
IBM Research–Zurich, Switzerland  
Cryptography Research Inc., USA  
Università degli Studi di Salerno, Italy  
Kudelski Security, Switzerland  
University of Maryland, USA  
QUT, Australia  
Ibaraki University, Japan  
NTNU, Norway  
Danmarks Tekniske Universitet (DTU), Denmark  
LORIA, France  
Ruhr-Universität Bochum (RUB), Germany  
Agari and ZapFraud, USA  
Snap and Columbia University, USA

Nasir Memon	New York University, USA
Neal Koblitz	University of Washington, USA
Orr Dunkelman	University of Haifa, Israel
Peter Y.A. Ryan	Université du Luxembourg
Phillip Rogaway	University of California (UC) Davis, USA
Raphaël C.-W. Phan (Chair)	Multimedia University (MMU), Malaysia
Reihaneh Safavi-Naini	University of Calgary, Canada
Ronald Cramer	CWI and Universiteit Leiden, The Netherlands
San Ling	Nanyang Technological University (NTU), Singapore
Sherman S.M. Chow	Chinese University of Hong Kong
Shiho Moriai	NICT, Japan
Tatsuaki Okamoto	Nippon Telegraph and Telephone (NTT), Japan
Vincent Rijmen	KU Leuven and iMinds, Belgium
Yvo Desmedt	University of Texas at Dallas, USA and UCL, UK

## External Reviewers

Alexander Koch	Jens Zumbärgel	Rafael Misoczki
Alfredo Rial Duran	John Chan	Robert Granger
Anton Stiglic	Jonathan Bootle	Russell W.F. Lai
Benjamin Wesolowski	Jong Hwan Park	Scott Ruoti
Cristina Onete	Kazuki Yoneyama	Sébastien Canard
Daniel Masny	Keita Emura	Shiwei Zhang
Duane Wilson	Khoa Nguyen	Sigurd Eskeland
Edoardo Persichetti	Koutarou Suzuki	Subhamoy Maitra
Frédérique Elise Oggier	Laura Luzzi	Sylvain Ruhault
Gäetan Leurent	Luisa Siniscalchi	Tom Ristenpart
Guomin Yang	Mark Marson	Vanishree Rao
Hossein Siadati	Michele Ciampi	Viet Tung Hoang
Huaxiong Wang	Nicolas Sendrier	Wakaha Ogata
Hyung Tae Lee	Palash Sarkar	Yannick Seurin
Irene Giacomelli	Peng Jiang	Yu Sasaki
Jae Hong Seo	Peter B. Rønne	Yu Yu
Jean-Pierre Tillich	Pierre-Louis Cayrel	Yusi James Zhang

## In Cooperation with

The International Association for Cryptologic Research (IACR)

## Sponsoring Institutions

Cyber Security Malaysia  
 IEICE Malaysia Section  
 Multimedia University (MMU)  
 Tourism Malaysia



# Contents

## Keynotes

The Case For Human Primacy in Cryptography (Summary from the Keynote Lecture) . . . . .	3
<i>X. Boyen</i>	
Time for a Paradigm Shift in Our Disciplinary Culture? . . . . .	11
<i>Neal Koblitz</i>	

## Revisiting Tradition

Another Look at Tightness II: Practical Issues in Cryptography . . . . .	21
<i>Sanjit Chatterjee, Neal Koblitz, Alfred Menezes, and Palash Sarkar</i>	
Another Look at Anonymous Communication: Security and Modular Constructions . . . . .	56
<i>Russell W.F. Lai, Henry K.F. Cheung, Sherman S.M. Chow, and Anthony Man-Cho So</i>	
Challenges with Assessing the Impact of NFS Advances on the Security of Pairing-Based Cryptography . . . . .	83
<i>Alfred Menezes, Palash Sarkar, and Shashank Singh</i>	

## Different Paradigms

Key Recovery: Inert and Public . . . . .	111
<i>Colin Boyd, Xavier Boyen, Christopher Carr, and Thomas Haines</i>	
Honey Encryption for Language: Robbing Shannon to Pay Turing? . . . . .	127
<i>Marc Beunardeau, Houda Ferradi, Rémi Géraud, and David Naccache</i>	
Randomized Stopping Times and Provably Secure Pseudorandom Permutation Generators . . . . .	145
<i>Michal Kulis, Pawel Lorek, and Filip Zagorski</i>	

## Cryptofication

A Virtual Wiretap Channel for Secure Message Transmission. . . . .	171
<i>Setareh Sharifian, Reihaneh Safavi-Naini, and Fuchun Lin</i>	

Necessary and Sufficient Numbers of Cards for Securely Computing  
Two-Bit Output Functions . . . . . 193  
*Danny Francis, Syarifah Ruqayyah Aljumid, Takuya Nishida,  
Yu-ichi Hayashi, Takaaki Mizuki, and Hideaki Sone*

**Malicious Cryptography**

Controlled Randomness – A Defense Against Backdoors  
in Cryptographic Devices . . . . . 215  
*Lucjan Hanzlik, Kamil Kluczniak, and Mirosław Kutylowski*

Malware, Encryption, and Rerandomization – Everything Is Under Attack . . . 233  
*Herman Galteland and Kristian Gjølsteen*

Protecting Electronic Signatures in Case of Key Leakage . . . . . 252  
*Mirosław Kutylowski, Jacek Cichoń, Lucjan Hanzlik, Kamil Kluczniak,  
Xiaofeng Chen, and Jianfeng Wang*

**Advances in Cryptanalysis**

A New Test Statistic for Key Recovery Attacks Using Multiple Linear  
Approximations . . . . . 277  
*Subhabrata Samajder and Palash Sarkar*

Tuple Cryptanalysis: Slicing and Fusing Multisets . . . . . 294  
*Marine Minier and Raphaël C.-W. Phan*

Improvements of Attacks on Various Feistel Schemes . . . . . 321  
*Emmanuel Volte, Valérie Nachev, and Nicolas Marrière*

**Primitives and Features**

Updatable Functional Encryption . . . . . 347  
*Afonso Arriaga, Vincenzo Iovino, and Qiang Tang*

Linking-Based Revocation for Group Signatures: A Pragmatic Approach  
for Efficient Revocation Checks . . . . . 364  
*Daniel Slamanig, Raphael Spreitzer, and Thomas Unterluggauer*

CARIBE: Cascaded IBE for Maximum Flexibility and User-Side Control . . . 389  
*Britta Hale, Christopher Carr, and Danilo Gligoroski*

Multi-authority Distributed Attribute-Based Encryption with Application  
to Searchable Encryption on Lattices . . . . . 409  
*Veronika Kuchta and Olivier Markowitch*

One-Round Exposure-Resilient Identity-Based Authenticated Key Agreement with Multiple Private Key Generators . . . . . 436  
*Atsushi Fujioka*

**Cryptanalysis Correspondence**

Attacks on the Basic cMix Design: On the Necessity of Commitments and Randomized Partial Checking . . . . . 463  
*Herman Galteland, Stig F. Mjølsnes, and Ruxandra F. Olimid*

Cryptanalysis of an Identity-Based Convertible Undeniable Signature Scheme . . . . . 474  
*Rouzbeh Behnia, Syh-Yuan Tan, and Swee-Huay Heng*

**Invited and Insight Papers**

Towards User-Friendly Cryptography . . . . . 481  
*Goichiro Hanaoka*

Multi-prover Interactive Proofs: Unsound Foundations . . . . . 485  
*Claude Crépeau and Nan Yang*

Human Public-Key Encryption . . . . . 494  
*Houda Ferradi, Rémi Géraud, and David Naccache*

Two Philosophies for Solving Non-linear Equations in Algebraic Cryptanalysis . . . . . 506  
*Nicolas T. Courtois*

Watermarking Cryptographic Programs . . . . . 521  
*Ryo Nishimaki*

From Higher-Order Differentials to Polytopic Cryptanalysis . . . . . 544  
*Tyge Tiessen*

Division Property: Efficient Method to Estimate Upper Bound of Algebraic Degree . . . . . 553  
*Yosuke Todo*

**Author Index** . . . . . 573