Lecture Notes in Computer Science **10031**

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

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

Jung Hee Cheon · Tsuyoshi Takagi (Eds.)

Advances in Cryptology – ASIACRYPT 2016

22nd International Conference on the Theory and Application of Cryptology and Information Security
Hanoi, Vietnam, December 4–8, 2016
Proceedings, Part I

Springer

Editors
Jung Hee Cheon
Seoul National University
Seoul
Korea (Republic of)

Tsuyoshi Takagi
Kyushu University
Fukuoka
Japan

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-662-53886-9 ISBN 978-3-662-53887-6 (eBook)
DOI 10.1007/978-3-662-53887-6

Library of Congress Control Number: 2016956613

LNCS Sublibrary: SL4 – Security and Cryptology

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer-Verlag GmbH Germany
The registered company address is: Heidelberger Platz 3, 14197 Berlin, Germany

Preface

ASIACRYPT 2016, the 22nd Annual International Conference on Theory and Application of Cryptology and Information Security, was held at InterContinental Hanoi Westlake Hotel in Hanoi, Vietnam, during December 4–8, 2016. The conference focused on all technical aspects of cryptology, and was sponsored by the International Association for Cryptologic Research (IACR).

Asiacrypt 2016 received a total of 240 submissions from all over the world. The Program Committee selected 67 papers from these submissions for publication in the proceedings of this conference. The review process was made via the usual double-blind pier review by the Program Committee comprising 43 leading experts in the field. Each submission was reviewed by at least three reviewers and five reviewers were assigned to submissions co-authored by Program Committee members. This year, the conference operated a two-round review system with a rebuttal phase. In the first-round review the Program Committee selected the 140 submissions that were considered of value for proceeding to the second round. In the second-round review the Program Committee further reviewed the submissions by taking into account their rebuttal letter from the authors. The selection process was assisted by a total of 309 external reviewers. These two-volume proceedings contain the revised versions of the papers that were selected. The revised versions were not reviewed again and the authors are responsible for their contents.

The program of Asiacrypt 2016 featured three excellent invited talks. Nadia Heninger gave a talk on "The Reality of Cryptographic Deployments on the Internet," Hoeteck Wee spoke on "Advances in Functional Encryption," and Neal Koblitz gave a non-technical lecture on "Cryptography in Vietnam in the French and American Wars." The conference also featured a traditional rump session that contained short presentations on the latest research results of the field. The Program Committee selected the work "Faster Fully Homomorphic Encryption: Bootstrapping in Less Than 0.1 Seconds" by Ilaria Chillotti, Nicolas Gama, Mariya Georgieva, and Malika Izabachène for the Best Paper Award of Asiacrypt 2016. Two more papers, "Nonlinear Invariant Attack—Practical Attack on Full SCREAM, iSCREAM, and Midori64" by Yosuke Todo, Gregor Leander, Yu Sasaki and "Cliptography: Clipping the Power of Kleptographic Attacks" by Alexander Russell, Qiang Tang, Moti Yung, Hong-Sheng Zhou were solicited to submit full versions to the *Journal of Cryptology*.

Many people contributed to the success of Asiacrypt 2016. We would like to thank the authors for submitting their research results to the conference. We are very grateful to all of the Program Committee members as well as the external reviewers for their fruitful comments and discussions on their areas of expertise. We are greatly indebted to Ngo Bao Chau and Phan Duong Hieu, the general co-chairs for their efforts and overall organization. We would also like to thank Nguyen Huu Du, Nguyen Quoc Khanh, Nguyen Duy Lan, Duong Ngoc Thai, Nguyen Ta Toan Khoa, Nguyen Ngoc Tuan,

Le Thi Lan Anh, and the local Organizing Committee for their continuous supports. We thank Steven Galbraith for expertly organizing and chairing the rump session.

Finally we thank Shai Halevi for letting us use his nice software for supporting the paper submission and review process. We also thank Alfred Hofmann, Anna Kramer, and their colleagues at Springer for handling the editorial process of the proceedings. We would like to express our gratitude to our partners and sponsors: XLIM, Microsoft Research, CISCO, Intel, Google.

December 2016

Jung Hee Cheon
Tsuyoshi Takagi

ASIACRYPT 2016

The 22nd Annual International Conference on Theory and Application of Cryptology and Information Security

Sponsored by the International Association for Cryptologic Research (IACR)

December 4–8, 2016, Hanoi, Vietnam

General Co-chairs

Ngo Bao Chau	VIASM, Vietnam and University of Chicago, USA
Phan Duong Hieu	XLIM, University of Limoges, France

Program Co-chairs

Jung Hee Cheon	Seoul National University, Korea
Tsuyoshi Takagi	Kyushu University, Japan

Program Committee

Elena Andreeva	KU Leuven, Belgium
Xavier Boyen	Queensland University of Technology, Australia
Anne Canteaut	Inria, France
Chen-Mou Cheng	National Taiwan University, Taiwan
Sherman S.M. Chow	Chinese University of Hong Kong, Hong Kong, SAR China
Nico Döttling	University of California, Berkeley, USA
Thomas Eisenbarth	Worcester Polytechnic Institute, USA
Georg Fuchsbauer	École Normale Supérieure, France
Steven Galbraith	Auckland University, New Zealand
Sanjam Garg	University of California, Berkeley, USA
Vipul Goyal	Microsoft Research, India
Jens Groth	University College London, UK
Sylvain Guilley	Secure-IC S.A.S., France
Alejandro Hevia	Universidad de Chile, Chile
Antoine Joux	Foundation UPMC and LIP6, France
Xuejia Lai	Shanghai Jiaotong University, China
Hyung Tae Lee	Nanyang Technological University, Singapore
Kwangsu Lee	Sejong University, Korea
Dongdai Lin	Chinese Academy of Sciences, China
Feng-Hao Liu	Florida Atlantic University, USA
Takahiro Matsuda	AIST, Japan
Alexander May	Ruhr University Bochum, Germany

Florian Mendel	Graz University of Technology, Austria
Amir Moradi	Ruhr University Bochum, Germany
Svetla Nikova	KU Leuven, Belgium
Tatsuaki Okamoto	NTT, Japan
Elisabeth Oswald	University of Bristol, UK
Thomas Peyrin	Nanyang Technological University, Singapore
Rei Safavi-Naini	University of Calgary, Canada
Peter Schwabe	Radboud University, The Netherlands
Jae Hong Seo	Myongji University, Korea
Damien Stehlé	ENS de Lyon, France
Ron Steinfeld	Monash University, Australia
Rainer Steinwandt	Florida Atlantic University, USA
Daisuke Suzuki	Mitsubishi Electric, Japan
Mehdi Tibouchi	NTT, Japan
Yosuke Todo	NTT, Japan
Hoang Viet Tung	University of California Santa Barbara, USA
Dominique Unruh	University of Tartu, Estonia
Ivan Visconti	University of Salerno, Italy
Huaxiong Wang	Nanyang Technological University, Singapore
Meiqin Wang	Shandong University, China
Aaram Yun	UNIST, Korea

External Reviewers

Michel Abdalla
Aysajan Abidin
Shashank Agrawal
Shweta Agrawal
Ahmad Ahmadi
Mamun Akand
Saed Alsayigh
Joël Alwen
Abdelrahaman Aly
Daniel Apon
Muhammad Rizwan Asghar
Tomer Ashur
Nuttapong Attrapadung
Benedikt Auerbach
Saikrishna Badrinarayanan
Shi Bai
Razvan Barbulescu
Lejla Batina
Georg T. Becker
Christof Beierle
Fabrice Benhamouda
Begül Bilgin
Céline Blondeau
Tobias Boelter
Carl Bootland
Jonathan Bootle
Yuri Borissov
Christina Boura
Colin Boyd
Wouter Castryck
Dario Catalano
Andrea Cerulli
Gizem Cetin
Pyrros Chaidos
Nishanth Chandran
Yu-Chen Chang
Lin Changlu
Binyi Chen
Cong Chen
Jie Chen
Ming-Shing Chen
Yu Chen
Céline Chevalier
Chongwon Cho
Kyu Young Choi
HeeWon Chung
Kai-Min Chung
Eloi de Chérisey
Michele Ciampi
Craig Costello
Joan Daemen
Ricardo Dahab
Wei Dai
Bernardo David
Thomas de Cnudde
David Derler
Apoorvaa Deshpande
Christoph Dobraunig
Yarkin Doroz
Ming Duan
Léo Ducas

Dung Hoang Duong
Maria Eichlseder
Martianus Frederic Ezerman
Xiong Fan
Pooya Farshim
Serge Fehr
Max Fillinger
Dario Fiore
Victor Fischer
Marc Fischlin
Thomas Fuhr
Jake Longo Galea
David Galindo
Peter Gazi
Essam Ghadafi
Mohona Ghosh
Zheng Gong
Rishab Goyal
Hannes Gross
Vincent Grosso
Berk Gulmezoglu
Chun Guo
Jian Guo
Qian Guo
Divya Gupta
Iftach Haitner
Dong-Guk Han
Kyoohyung Han
Shuai Han
Goichiro Hanaoka
Christian Hanser
Mitsuhiro Hattori
Gottfried Herold
Felix Heuer
Takato Hirano
Shoichi Hirose
Wei-Chih Hong
Yuan-Che Hsu
Geshi Huang
Guifang Huang
Jialin Huang
Xinyi Huang
Pavel Hubacek
Ilia Iliashenko
Mehmet Sinan Inci
Vincenzo Iovino
Gorka Irazoqui
Ai Ishida
Takanori Isobe
Tetsu Iwata
Aayush Jain
Sune Jakobsen
Yin Jia
Shaoquan Jiang
Chethan Kamath
Sabyasachi Karati
Sayasachi Karati
Yutaka Kawai
Carmen Kempka
HeeSeok Kim
Hyoseung Kim
Jinsu Kim
Myungsun Kim
Taechan Kim
Paul Kirchner
Elena Kirshanova
Fuyuki Kitagawa
Susumu Kiyoshima
Jessica Koch
Markulf Kohlweiss
Vladimir Kolesnikov
Thomas Korak
Yoshihiro Koseki
Ashutosh Kumar
Ranjit Kumaresan
Po-Chun Kuo
Robert Kübler
Thijs Laarhoven
Ching-Yi Lai
Russell W.F. Lai
Virginie Lallemand
Adeline Langlois
Sebastian Lauer
Su Le
Gregor Leander
Kwangsu Lee
Gaëtan Leurent
Anthony Leverrier
Jingwei Li
Ming Li
Wen-Ding Li
Benoit Libert
Fuchun Lin
Tingting Lin
Meicheng Liu
Yunwen Liu
Zhen Liu
Zidong Lu
Yiyuan Luo
Atul Luykx
Vadim Lyubashevsky
Bernardo Magri
Mary Maller
Alex Malozemoff
Antonio Marcedone
Benjamin Martin
Daniel Martin
Marco Martinoli
Daniel Masny
Maike Massierer
Mitsuru Matsui
Willi Meier
Bart Mennink
Peihan Miao
Kazuhiko Minematsu
Nicky Mouha
Pratyay Mukherjee
Sean Murphy
Jörn Müller-Quade
Valérie Nachef
Michael Naehrig
Matthias Nagel
Yusuke Naito
Mridul Nandi
María Naya-Plasencia
Kartik Nayak
Khoa Nguyen
Ivica Nikolic
Ventzislav Nikov
Ryo Nishimaki
Anca Nitulescu
Koji Nuida
Maciej Obremski
Toshihiro Ohigashi
Miyako Ohkubo
Sumit Kumar Pandey
Jong Hwan Park

Seunghwan Park
Alain Passelègue
Christopher Patton
Bo-Yuan Peng
Rachel Player
Antigoni Polychroniadou
Bertram Pöttering
Sebastian Ramacher
Vanishree Rao
Shuqin Ren
Reza Reyhanitabar
Bastian Richter
Thomas Ristenpart
Mike Rosulek
Hansol Ryu
Akshayaram Srinivasan
Yusuke Sakai
Kochi Sakumoto
Amin Sakzad
Simona Samardjiska
Yu Sasaki
Pascal Sasdrich
Falk Schellenberg
Benedikt Schmidt
Tobias Schneider
Jacob Schuldt
Okan Seker
Nicolas Sendrier
Jae Hong Seo
Minhye Seo
Yannick Seurin
Masoumeh Shafienejad
Barak Shani
Danilo Sijacic
Alice Silverberg
Siang Meng Sim
Dave Singelee
Luisa Siniscalchi
Daniel Slamanig
Nigel Smart
Raphael Spreitzer
Douglas Stebila
Christoph Striecks
Takeshi Sugawara
Yao Sun
Berk Sunar
Koutarou Suzuki
Alan Szepieniec
Mostafa Taha
Somayeh Taheri
Junko Takahashi
Katsuyuki Takashima
Benjamin Tan
Jean-Pierre Tillich
Junichi Tomida
Yiannis Tselekounis
Himanshu Tyagi
Thomas Unterluggauer
Damien Vergnaud
Gilles Villard
Vanessa Vitse
Damian Vizar
Michael Walter
Han Wang
Hao Wang
Qiungju Wang
Wei Wang
Yuyu Wang
Yohei Watanabe
Hoeteck Wee
Wei Wei
Mor Weiss
Mario Werner
Bas Westerbaan
Carolyn Whitnall
Alexander Wild
Baofeng Wu
Keita Xagawa
Zejun Xiang
Hong Xu
Weijia Xue
Shota Yamada
Takashi Yamakawa
Hailun Yan
Jun Yan
Bo-Yin Yang
Bohan Yang
Guomin Yang
Mohan Yang
Shang-Yi Yang
Kan Yasuda
Xin Ye
Wentan Yi
Scott Yilek
Kazuki Yoneyama
Rina Zeitoun
Fan Zhang
Guoyan Zhang
Liang Feng Zhang
Liangfeng Zhang
Tao Zhang
Wentao Zhang
Yusi Zhang
Zongyang Zhang
Jingyuan Zhao
Yongjun Zhao
Yixin Zhong
Hong-Sheng Zhou
Xiao Zhou
Jincheng Zhuang

Local Organizing Committee

Co-chairs

Ngo Bao Chau	VIASM, Vietnam and University of Chicago, USA
Phan Duong Hieu	XLIM, University of Limoges, France

Members

Nguyen Huu Du	VIASM, Vietnam
Nguyen Quoc Khanh	Vietcombank, Vietnam
Nguyen Duy Lan	Microsoft Research, USA
Duong Ngoc Thai	Google, USA
Nguyen Ta Toan Khoa	NTU, Singapore
Nguyen Ngoc Tuan	VIASM, Vietnam
Le Thi Lan Anh	VIASM, Vietnam

Sponsors

XLIM
Microsoft Research
CISCO
Intel
Google

Invited Talks

Advances in Functional Encryption

Hoeteck Wee

ENS, Paris, France
wee@di.ens.fr

Abstract. Functional encryption is a novel paradigm for public-key encryption that enables both fine-grained access control and selective computation on encrypted data, as is necessary to protect big, complex data in the cloud. In this talk, I will provide a brief introduction to functional encryption and an overview of the state of the art, with a focus on constructions based on lattices.

CNRS, INRIA and Columbia University. Supported in part by ERC Project aSCEND (H2020 639554) and NSF Award CNS-1445424.

The Reality of Cryptographic Deployments on the Internet

Nadia Heninger

University of Pennsylvania, Philadelphia, USA

Abstract. Security proofs for cryptographic primitives and protocols rely on a number of (often implicit) assumptions about the world in which these components live. They assume that implementations are correct, that specifications are followed, that systems make sensible choices about error conditions, and that reliable sources of random numbers are present. However, a number of real world studies examining cryptographic deployments have shown that these assumptions are often not true on a large scale, with catastrophic effects for security. In addition to simple programming errors, many real-world cryptographic vulnerabilities can be traced back to more complex underlying causes, such as backwards compatibility, legacy protocols and software, hard-coded resource limits, and political interference in design choices.

Many of these issues appear on the surface to be at an entirely different level of abstraction from the cryptographic primitives used in their construction. However, by taking advantage of the structure of many cryptographic primitives when used at Internet scale, it is possible to uncover fundamental vulnerabilities in implementations. I will discuss the interplay between mathematical cryptanalysis techniques and the thorny implementation issues that lead to vulnerable cryptographic deployments in the real world.

Contents – Part I

Contents – Part II