Lecture Notes in Computer Science 11478

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

Yuval Ishai · Vincent Rijmen (Eds.)

Advances in Cryptology – EUROCRYPT 2019

38th Annual International Conference on the Theory and Applications of Cryptographic Techniques
Darmstadt, Germany, May 19–23, 2019
Proceedings, Part III

Springer

Editors

Yuval Ishai
Technion
Haifa, Israel

Vincent Rijmen
COSIC Group
KU Leuven
Heverlee, Belgium

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-17658-7 ISBN 978-3-030-17659-4 (eBook)
https://doi.org/10.1007/978-3-030-17659-4

LNCS Sublibrary: SL4 – Security and Cryptology

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

Preface

Eurocrypt 2019, the 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, was held in Darmstadt, Germany, during May 19–23, 2019. The conference was sponsored by the International Association for Cryptologic Research (IACR). Marc Fischlin (Technische Universität Darmstadt, Germany) was responsible for the local organization. He was supported by a local organizing team consisting of Andrea Püchner, Felix Günther, Christian Janson, and the Cryptoplexity Group. We are deeply indebted to them for their support and smooth collaboration.

The conference program followed the now established parallel track system where the works of the authors were presented in two concurrently running tracks. The invited talks and the talks presenting the best paper/best young researcher spanned over both tracks.

We received a total of 327 submissions. Each submission was anonymized for the reviewing process and was assigned to at least three of the 58 Program Committee members. Committee members were allowed to submit at most one paper, or two if both were co-authored. Submissions by committee members were held to a higher standard than normal submissions. The reviewing process included a rebuttal round for all submissions. After extensive deliberations the Program Committee accepted 76 papers. The revised versions of these papers are included in these three volume proceedings, organized topically within their respective track.

The committee decided to give the Best Paper Award to the paper "Quantum Lightning Never Strikes the Same State Twice" by Mark Zhandry. The runner-up was the paper "Compact Adaptively Secure ABE for $\mathtt{NC}^1$ from k Lin" by Lucas Kowalczyk and Hoeteck Wee. The Best Young Researcher Award went to the paper "Efficient Verifiable Delay Functions" by Benjamin Wesolowski. All three papers received invitations for the *Journal of Cryptology*.

The program also included an IACR Distinguished Lecture by Cynthia Dwork, titled "Differential Privacy and the People's Data," and invited talks by Daniele Micciancio, titled "Fully Homomorphic Encryption from the Ground Up," and François-Xavier Standaert, titled "Toward an Open Approach to Secure Cryptographic Implementations."

We would like to thank all the authors who submitted papers. We know that the Program Committee's decisions can be very disappointing, especially rejections of very good papers that did not find a slot in the sparse number of accepted papers. We sincerely hope that these works eventually get the attention they deserve.

We are also indebted to the members of the Program Committee and all external reviewers for their voluntary work. The committee's work is quite a workload. It has been an honor to work with everyone. The committee's work was tremendously simplified by Shai Halevi's submission software and his support, including running the service on IACR servers.

Finally, we thank everyone else—speakers, session chairs, and rump-session chairs—for their contribution to the program of Eurocrypt 2019. We would also like to thank the many sponsors for their generous support, including the Cryptography Research Fund that supported student speakers.

May 2019

Yuval Ishai
Vincent Rijmen

Eurocrypt 2019

The 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques

Sponsored by *the International Association for Cryptologic Research*

May 19–23, 2019
Darmstadt, Germany

General Chair

Marc Fischlin	Technische Universität Darmstadt, Germany

Program Co-chairs

Yuval Ishai	Technion, Israel
Vincent Rijmen	KU Leuven, Belgium and University of Bergen, Norway

Program Committee

Michel Abdalla	CNRS and ENS Paris, France
Adi Akavia	University of Haifa, Israel
Martin Albrecht	Royal Holloway, UK
Elena Andreeva	KU Leuven, Belgium
Paulo S. L. M. Barreto	University of Washington Tacoma, USA
Amos Beimel	Ben-Gurion University, Israel
Alex Biryukov	University of Luxembourg, Luxembourg
Nir Bitansky	Tel Aviv University, Israel
Andrej Bogdanov	Chinese University of Hong Kong, SAR China
Christina Boura	University of Versailles and Inria, France
Xavier Boyen	QUT, Australia
David Cash	University of Chicago, USA
Melissa Chase	MSR Redmond, USA
Kai-Min Chung	Academia Sinica, Taiwan
Dana Dachman-Soled	University of Maryland, USA
Ivan Damgård	Aarhus University, Denmark
Itai Dinur	Ben-Gurion University, Israel
Stefan Dziembowski	University of Warsaw, Poland
Serge Fehr	Centrum Wiskunde & Informatica (CWI) and Leiden University, The Netherlands
Juan A. Garay	Texas A&M University, USA
Sanjam Garg	UC Berkeley, USA

Christina Garman	Purdue University, USA
Siyao Guo	New York University Shanghai, China
Iftach Haitner	Tel Aviv University, Israel
Shai Halevi	IBM Research, USA
Brett Hemenway	University of Pennsylvania, USA
Justin Holmgren	Princeton University, USA
Stanislaw Jarecki	UC Irvine, USA
Dakshita Khurana	Microsoft Research New England, USA
Ilan Komargodski	Cornell Tech, USA
Gregor Leander	Ruhr-Universität Bochum, Germany
Huijia Lin	UCSB, USA
Atul Luykx	Visa Research, USA
Mohammad Mahmoody	University of Virginia, USA
Bart Mennink	Radboud University, The Netherlands
Tal Moran	IDC Herzliya, Israel
Svetla Nikova	KU Leuven, Belgium
Claudio Orlandi	Aarhus University, Denmark
Rafail Ostrovsky	UCLA, USA
Rafael Pass	Cornell University and Cornell Tech, USA
Krzysztof Pietrzak	IST Austria, Austria
Bart Preneel	KU Leuven, Belgium
Christian Rechberger	TU Graz, Austria
Leonid Reyzin	Boston University, USA
Guy N. Rothblum	Weizmann Institute, Israel
Amit Sahai	UCLA, USA
Christian Schaffner	QuSoft and University of Amsterdam, The Netherlands
Gil Segev	Hebrew University, Israel
abhi shelat	Northeastern University, USA
Martijn Stam	Simula UiB, Norway
Marc Stevens	CWI Amsterdam, The Netherlands
Stefano Tessaro	UCSB, USA
Mehdi Tibouchi	NTT, Japan
Frederik Vercauteren	KU Leuven, Belgium
Brent Waters	UT Austin, USA
Mor Weiss	Northeastern University, USA
David J. Wu	University of Virginia, USA
Vassilis Zikas	University of Edinburgh, UK

Additional Reviewers

Divesh Aggarwal
Shashank Agrawal
Gorjan Alagic
Abdelrahaman Aly
Andris Ambainis
Prabhanjan Ananth
Gilad Asharov
Tomer Ashur
Arash Atashpendar
Benedikt Auerbach
Christian Badertscher
Saikrishna Badrinarayanan
Shi Bai
Josep Balasch

Marshall Ball
James Bartusek
Balthazar Bauer
Carsten Baum
Christof Beierle
Fabrice Benhamouda
Iddo Bentov
Mario Berta
Ward Beullens
Ritam Bhaumik
Jean-François Biasse
Koen de Boer
Dan Boneh
Xavier Bonnetain
Charlotte Bonte
Carl Bootland
Jonathan Bootle
Joppe Bos
Adam Bouland
Florian Bourse
Benedikt Bünz
Wouter Castryck
Siu On Chan
Nishanth Chandran
Eshan Chattopadhyay
Yi-Hsiu Chen
Yilei Chen
Yu Long Chen
Jung-Hee Cheon
Mahdi Cheraghchi
Celine Chevalier
Nai-Hui Chia
Ilaria Chillotti
Chongwon Cho
Wutichai Chongchitmate
Michele Ciampi
Ran Cohen
Sandro Coretti
Ana Costache
Jan Czajkowski
Yuanxi Dai
Deepesh Data
Bernardo David
Alex Davidson
Thomas Debris-Alazard
Thomas De Cnudde
Thomas Decru
Luca De Feo
Akshay Degwekar
Cyprien Delpech de Saint Guilhem
Ioannis Demertzis
Ronald de Wolf
Giovanni Di Crescenzo
Christoph Dobraunig
Jack Doerner
Javad Doliskani
Leo Ducas
Yfke Dulek
Nico Döttling
Aner Ben Efraim
Maria Eichlseder
Naomi Ephraim
Daniel Escudero
Saba Eskandarian
Thomas Espitau
Pooya Farshim
Prastudy Fauzi
Rex Fernando
Houda Ferradi
Dario Fiore
Ben Fisch
Mathias Fitzi
Cody Freitag
Georg Fuchsbauer
Benjamin Fuller
Tommaso Gagliardoni
Steven Galbraith
Nicolas Gama
Chaya Ganesh
Sumegha Garg
Romain Gay
Peter Gazi
Craig Gentry
Marios Georgiou
Benedikt Gierlichs
Huijing Gong
Rishab Goyal
Lorenzo Grassi
Hannes Gross
Jens Groth
Paul Grubbs
Divya Gupta
Felix Günther
Helene Haagh
Björn Haase
Mohammad Hajiabadi
Carmit Hazay
Pavel Hubáček
Andreas Huelsing
Ilia Iliashenko
Muhammad Ishaq
Joseph Jaeger
Eli Jaffe
Aayush Jain
Abhishek Jain
Stacey Jeffery
Zhengfeng Ji
Yael Kalai
Daniel Kales
Chethan Kamath
Nathan Keller
Eike Kiltz
Miran Kim
Sam Kim
Taechan Kim
Karen Klein
Yash Kondi
Venkata Koppula
Mukul Kulkarni
Ashutosh Kumar
Ranjit Kumaresan
Rio LaVigne
Virginie Lallemand
Esteban Landerreche
Brandon Langenberg
Douglass Lee
Eysa Lee
François Le Gall
Chaoyun Li
Wei-Kai Lin
Qipeng Liu
Tianren Liu
Alex Lombardi
Julian Loss
Yun Lu
Vadim Lyubashevsky
Fermi Ma

Saeed Mahloujifar
Christian Majenz
Rusydi Makarim
Nikolaos Makriyannis
Nathan Manohar
Antonio Marcedone
Daniel Masny
Alexander May
Noam Mazor
Willi Meier
Rebekah Mercer
David Mestel
Peihan Miao
Brice Minaud
Matthias Minihold
Konstantinos Mitropoulos
Tarik Moataz
Hart Montgomery
Andrew Morgan
Pratyay Mukherjee
Luka Music
Michael Naehrig
Gregory Neven
Phong Nguyen
Jesper Buus Nielsen
Ryo Nishimaki
Daniel Noble
Adam O'Neill
Maciej Obremski
Sabine Oechsner
Michele Orrù
Emmanuela Orsini
Daniel Ospina
Giorgos Panagiotakos
Omer Paneth
Lorenz Panny
Anat Paskin-Cherniavsky
Alain Passelègue
Kenny Paterson
Chris Peikert
Geovandro Pereira
Léo Perrin
Edoardo Persichetti
Naty Peter
Rachel Player
Oxana Poburinnaya
Yuriy Polyakov
Antigoni Polychroniadou
Eamonn Postlethwaite
Willy Quach
Ahmadreza Rahimi
Sebastian Ramacher
Adrián Ranea
Peter Rasmussen
Shahram Rasoolzadeh
Ling Ren
Joao Ribeiro
Silas Richelson
Thomas Ricosset
Tom Ristenpart
Mike Rosulek
Dragos Rotaru
Yann Rotella
Lior Rotem
Yannis Rouselakis
Arnab Roy
Louis Salvail
Simona Samardziska
Or Sattath
Guillaume Scerri
John Schanck
Peter Scholl
André Schrottenloher
Sruthi Sekar
Srinath Setty
Brian Shaft
Ido Shahaf
Victor Shoup
Jad Silbak
Mark Simkin
Shashank Singh
Maciej Skórski
Caleb Smith
Fang Song
Pratik Soni
Katerina Sotiraki
Florian Speelman
Akshayaram Srinivasan
Uri Stemmer
Noah Stephens-Davidowitz
Alan Szepieniec
Gelo Noel Tabia
Aishwarya Thiruvengadam
Sergei Tikhomirov
Rotem Tsabary
Daniel Tschudy
Yiannis Tselekounis
Aleksei Udovenko
Dominique Unruh
Cédric Van Rompay
Prashant Vasudevan
Muthu Venkitasubramaniam
Daniele Venturi
Benoît Viguier
Fernando Virdia
Ivan Visconti
Giuseppe Vitto
Petros Wallden
Alexandre Wallet
Qingju Wang
Bogdan Warinschi
Gaven Watson
Hoeteck Wee
Friedrich Wiemer
Tim Wood
Keita Xagawa
Sophia Yakoubov
Takashi Yamakawa
Arkady Yerukhimovich
Eylon Yogev
Nengkun Yu
Yu Yu
Aaram Yun
Thomas Zacharias
Greg Zaverucha
Liu Zeyu
Mark Zhandry
Chen-Da Liu Zhang

Abstracts of Invited Talks

Differential Privacy and the People's Data

IACR Distinguished Lecture

Cynthia Dwork[1]

Harvard University
dwork@seas.harvard.edu

Abstract. Differential Privacy will be the confidentiality protection method of the 2020 US Decennial Census. We explore the technical and social challenges to be faced as the technology moves from the realm of information specialists to the large community of consumers of census data.

Differential Privacy is a definition of privacy tailored to the statistical analysis of large datasets. Roughly speaking, differential privacy ensures that anything learnable about an individual could be learned independent of whether the individual opts in or opts out of the data set under analysis. The term has come to denote a field of study, inspired by cryptography and guided by theoretical lower bounds and impossibility results, comprising algorithms, complexity results, sample complexity, definitional relaxations, and uses of differential privacy when privacy is not itself a concern.

From its inception, a motivating scenario for differential privacy has been the US Census: data of the people, analyzed for the benefit of the people, to allocate the people's resources (hundreds of billions of dollars), with a legal mandate for privacy. Over the past 4–5 years, differential privacy has been adopted in a number of industrial settings by Google, Microsoft, Uber, and, with the most fanfare, by Apple. In 2020 it will be the confidentiality protection method for the US Decennial Census.

Census data are used throughout government and in thousands of research studies every year. This mainstreaming of differential privacy, the transition from the realm of technically sophisticated information specialists and analysts into much broader use, presents enormous technical and social challenges. The Fundamental Theorem of Information Reconstruction tells us that overly accurate estimates of too many statistics completely destroys privacy. Differential privacy provides a measure of privacy loss that permits the tracking and control of cumulative privacy loss as data are analyzed and re-analyzed. But provably no method can permit the data to be explored without bound. How will the privacy loss "budget" be allocated? Who will enforce limits?

More pressing for the scientific community are questions of how the multitudes of census data consumers will interact with the data moving forward. The Decennial Census is simple, and the tabulations can be handled well with existing technology. In contrast, the annual American Community Survey, which covers only a few million households yearly, is rich in personal details on subjects from internet access in the home to employment to ethnicity, relationships among persons in the home, and fertility. We are not (yet?) able to

[1] Supported in part by NSF Grant 1763665 and the Sloan Foundation.

offer differentially private algorithms for every kind of analysis carried out on these data. Historically, confidentiality has been handled by a combination of data summaries, restricted use access to the raw data, and the release of public-use microdata, a form of noisy individual records. Summary statistics are the bread and butter of differential privacy, but giving even trusted and trustworthy researchers access to raw data is problematic, as their published findings are a vector for privacy loss: think of the researcher as an arbitrary non-differentially private algorithm that produces outputs in the form of published findings. The very *choice* of statistic to be published is inherently not privacy-preserving! At the same time, past microdata noising techniques can no longer be considered to provide adequate privacy, but generating synthetic public-use microdata while ensuring differential privacy is a computationally hard problem. Nonetheless, combinations of exciting new techniques give reason for optimism.

Towards an Open Approach to Secure Cryptographic Implementations

François-Xavier Standaert[1]

UCL Crypto Group, Université Catholique de Louvain, Belgium

Abstract. In this talk, I will discuss how recent advances in side-channel analysis and leakage-resilience could lead to both stronger security properties and improved confidence in cryptographic implementations. For this purpose, I will start by describing how side-channel attacks exploit physical leakages such as an implementation's power consumption or electromagnetic radiation. I will then discuss the definitional challenges that these attacks raise, and argue why heuristic hardware-level countermeasures are unlikely to solve the problem convincingly. Based on these premises, and focusing on the symmetric setting, securing cryptographic implementations can be viewed as a tradeoff between the design of modes of operation, underlying primitives and countermeasures.

Regarding modes of operation, I will describe a general design strategy for leakage-resilient authenticated encryption, propose models and assumptions on which security proofs can be based, and show how this design strategy encourages so-called leveled implementations, where only a part of the computation needs strong (hence expensive) protections against side-channel attacks.

Regarding underlying primitives and countermeasures, I will first emphasize the formal and practically-relevant guarantees that can be obtained thanks to masking (i.e., secret sharing at the circuit level), and how considering the implementation of such countermeasures as an algorithmic design goal (e.g., for block ciphers) can lead to improved performances. I will then describe how limiting the leakage of the less protected parts in a leveled implementations can be combined with excellent performances, for instance with respect to the energy cost.

I will conclude by putting forward the importance of sound evaluation practices in order to empirically validate (by lack of falsification) the assumptions needed both for leakage-resilient modes of operation and countermeasures like masking, and motivate the need of an open approach for this purpose. That is, by allowing adversaries and evaluators to know implementation details, we can expect to enable a better understanding of the fundamentals of physical security, therefore leading to improved security and efficiency in the long term.

[1] The author is a Senior Research Associate of the Belgian Fund for Scientific Research (FNRS-F.R.S.). This work has been funded in part by the ERC Project 724725.

Fully Homomorphic Encryption from the Ground Up

Daniele Micciancio

University of California, Mail Code 0404, La Jolla,
San Diego, CA, 92093, USA
daniele@cs.ucsd.edu
http://cseweb.ucsd.edu/~daniele/

Abstract. The development of fully homomorphic encryption (FHE), i.e., encryption schemes that allow to perform arbitrary computations on encrypted data, has been one of the main achievements of theoretical cryptography of the past 20 years, and probably the single application that brought most attention to lattice cryptography. While lattice cryptography, and fully homomorphic encryption in particular, are often regarded as a highly technical topic, essentially all constructions of FHE proposed so far are based on a small number of rather simple ideas. In this talk, I will try highlight the basic principles that make FHE possible, using lattices to build a simple private key encryption scheme that enjoys a small number of elementary, but very useful properties: a simple decryption algorithm (requiring, essentially, just the computation of a linear function), a basic form of circular security (i.e., the ability to securely encrypt its own key), and a very weak form of linear homomorphism (supporting only a bounded number of addition operations.)

All these properties are easily established using simple linear algebra and the hardness of the Learning With Errors (LWE) problem or standard worst-case complexity assumptions on lattices. Then, I will use this scheme (and its abstract properties) to build in a modular way a tower of increasingly more powerful encryption schemes supporting a wider range of operations: multiplication by arbitrary constants, multiplication between ciphertexts, and finally the evaluation of arithmetic circuits of arbitrary, but a-priory bounded depth. The final result is a *leveled*[1] FHE scheme based on standard lattice problems, i.e., a scheme supporting the evaluation of arbitrary circuits on encrypted data, as long as the depth of the circuit is provided at key generation time. Remarkably, lattices are used only in the construction (and security analysis) of the basic scheme: all the remaining steps in the construction do not make any direct use of lattices, and can be expressed in a simple, abstract way, and analyzed using solely the weakly homomorphic properties of the basic scheme.

Keywords: Lattice-based cryptography · Fully homomorphic encryption · Circular security · FHE bootstrapping

[1] The "leveled" restriction in the final FHE scheme can be lifted using "circular security" assumptions that have become relatively standard in the FHE literature, but that are still not well understood. Achieving (non-leveled) FHE from standard lattice assumptions is the main theoretical problem still open in the area.

Contents – Part III

Foundations I

Efficient Secure Computation

Quantum II

Signatures I

Best Paper Awards

Information-Theoretic Cryptography

Cryptanalysis

Foundations II

Signatures II