

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>

Arpita Patra · Nigel P. Smart (Eds.)

Progress in Cryptology – INDOCRYPT 2017

18th International Conference on Cryptology in India
Chennai, India, December 10–13, 2017
Proceedings

Editors

Arpita Patra
Indian Institute of Science (IISc)
Bengaluru
India

Nigel P. Smart
Department of Computer Science
University of Bristol
Bristol
UK

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-71666-4 ISBN 978-3-319-71667-1 (eBook)
<https://doi.org/10.1007/978-3-319-71667-1>

Library of Congress Control Number: 2017959624

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

INDOCRYPT 2017, the 18th International Conference on Cryptology in India, was held at Institute of Mathematical Sciences, Chennai, India, during December 10–13, 2017. The INDOCRYPT series of conferences began in 2000 under the leadership of Prof. Bimal Roy of the Indian Statistical Institute and is organized under the aegis of the Cryptology Research Society of India (CRSI). The conference focused on all technical aspects of cryptology.

The submissions for INDOCRYPT 2017 were due on August 27, 2017. In response to the call for papers, we received 75 submissions from around 20 countries, out of which 19 were chosen for inclusion in the program. The review process was conducted in two stages. In the first stage, each paper was reviewed by at least three independent reviewers, with papers from Program Committee members receiving at least five reviews. This was followed by a week-long rigorous and detailed discussion phase to decide on the acceptance of the submissions. Reviewers with potential conflicts of interest for specific papers were excluded from all discussions about those papers. The 43 members of the Program Committee were aided in this tedious and time-consuming task by many external reviewers. We would like to thank them all for their service, their expert opinions, and their spirited contributions to the review process. The authors had to revise their papers according to the suggestions of the referees and submit the camera-ready versions by October 15.

The submission and review process was done using Shai Halevi's Web Submission and Review Software. We wish to express our sincere gratitude to Shai Halevi for the software, which facilitated a smooth and easy submission and review process.

INDOCRYPT 2017 had three invited speakers with two from academia and one from the Government of India. Elette Boyle (Israel) enlightened the audience on "Recent Advances in Function and Homomorphic Secret Sharing". Tancrède Lepoint (USA) spoke on the interesting topic of "Post-Quantum Cryptography Using Module Lattices". The speech of Saikat Datta (Policy Director, Centre for Internet & Society, India) covered policy-making in India on Cryptography.

Finally, we would like to thank the general chairs, Prof. C. Pandu Rangan (Indian Institute of Technology Madras) and Prof. R. Balasubramanian (Institute of Mathematical Sciences); the team at the Indian Institute of Science who maintained the conference website; and the local organizing team at the Indian Institute of Technology, Madras, for their sincere hard work and for the local organization matters for the conference. We are especially grateful to our sponsors for their generous support of the conference. We would also like to express our appreciation to Springer for their active cooperation and timely production of the proceedings.

Finally, we would like to thank all the authors who submitted their work to INDOCRYPT 2017, and all the attendees. Without your spirited participation, the conference would not be a success. We hope you enjoy the proceedings of this year's INDOCRYPT conference.

December 2017

Nigel P. Smart
Arpita Patra

INDOCRYPT 2017

18th International Conference on Cryptology in India

Chennai, India
10–13 December, 2017

General Chairs

C. Pandu Rangan	Indian Institute of Technology Madras, India
R. Balasubramanian	Institute of Mathematical Sciences, India

Program Chairs

Arpita Patra	Indian Institute of Science, India
Nigel P. Smart	University of Bristol, UK

Program Committee

Adeline Roux-Langlois	CNRS/IRISA, France
Aggelos Kiayias	University of Edinburgh, UK
Alessandra Scafuro	North Carolina State University, USA
Andrey Bogdanov	Technical University of Denmark, Denmark
Anja Lehmann	IBM Research - Zurich, Switzerland
Bart Preneel	KU Leuven, Belgium
Benny Pinkas	Bar-Ilan University, Israel
Bhavana Kanukurthi	Indian Institute of Science, India
Carmit Hazay	Bar-Ilan University, Israel
Chris Brzuska	Hamburg University, Germany
Christophe Petit	Oxford University, UK
Debdeep Mukhopadhyay	Indian Institute of Technology Kharagpur, India
Dennis Hofheinz	Karlsruhe Institute of Technology, Germany
Francois-Xavier Standaert	Catholic University of Louvain, Belgium
Georg Fuchsbauer	ENS Paris, France
Giuseppe Persiano	University of Salerno, Italy
Goutam Paul	Indian Statistical Institute Kolkata, India
Helena Handschuh	Rambus Cryptography Research and KU Leuven, Belgium
Itai Dinur	Ben-Gurion University, Israel
Jesper Buus Nielsen	Aarhus University, Denmark
Jonathan Katz	University of Maryland Park, USA
Joppe W. Bos	NXP Semiconductors, Belgium

Kaoru Kurosawa	Ibaraki University, Japan
Kenny Paterson	Royal Holloway, University of London, UK
Krzysztof Pietrzak	IST Austria, Austria
Manoj Prabhakaran	Indian Institute of Technology Bombay, India
Marc Fischlin	Darmstadt University of Technology, Germany
Martin Albrecht	Royal Holloway, University of London, UK
Mike Rosulek	Oregon State, USA
Nishanth Chandran	Microsoft Research Bangalore, India
Ranjit Kumerasan	Microsoft Research Redmond, USA
Rosario Gennaro	City University New York, USA
Shweta Agrawal	Indian Institute of Technology Madras, India
Somitra Kr. Sanadhya	Ashoka University, India
Takahiro Matsuda	AIST, Japan
Tancrède Lepoint	SRI, USA
Thomas Johansson	Lund University, Sweden
Thomas Schneider	Darmstadt University of Technology, Germany
Vipul Goyal	Carnegie Mellon University, USA
Yu Sasaki	NTT Secure Platform Laboratories, Japan

External Reviewers

Alessandro Amadori	Shay Gueron	Sai Lakshmi Bhavana
Nuttapong Attrapadung	Mike Hamburg	Obbattu
Shi Bai	Mike Hutter	Sikhar Patranabis
Iddo Bentov	Ryo Kikuchi	Alice Pellet-Mary
Pauline Bert	Ágnes Kiss	Ben Pring
Begül Bilgin	Fuyuki Kitagawa	Chen Qian
Estuardo Alpirez Bock	Abhishek Kumar	Peter Rindal
Suvradip Chakraborty	Prabhat Kushwaha	Debapriya Basu Roy
Liqun Chen	Chaoyun Li	Yusuke Sakai
Madhuparna Das	Pierre Loidreau	Sruthi Sekar
Nayana Das	Monosij Maitra	Aishwarya
Nilanjan Datta	Daniel Malinowski	Thiruvengadam
Daniel Demmler	Alex Malozemoff	Yan Bo Ti
Orr Dunkelman	Bimal Mandal	Prashant Vasudevan
Dario Fiore	Sogol Mazaheri	Christian Weinert
Ran Gelles	James McKee	Kazuki Yoneyama
Mohona Ghosh	Michele Minelli	
Dahmun Goudarzi	Michael Naehrig	

Post-quantum Cryptography Using Module Lattices (Invited Talk)

Tancrède Lepoint 

SRI International, New York, USA

Recent advances in quantum computing and the announcement by the National Institute of Standards and Technology (NIST) to define new standards for digital-signature, encryption, and key-establishment protocols, spurred on the design and analysis of many post-quantum cryptographic schemes. One of the most efficient quantum-resilient alternatives for the above basic primitives is that of lattice cryptography.

Many lattice cryptography schemes are based on the *learning-with-error* problem over a ring R_q . Fix size parameters $k, \ell \geq 1$ and an ‘error’ probability χ on R_q . Let $A_{s,\chi}$ on $R_q^\ell \times R_q$ be the probability distribution obtained by choosing a vector $a \in R_q^\ell$ uniformly at random, choosing $e \in R_q$ according to χ , and outputting $(a, \langle a, s \rangle + e)$ where additions are performed in R_q . In the (decision) learning-with-error problem, the goal is to distinguish $A_{s,\chi}$, for a uniformly random secret $s \in R_q^\ell$, from the uniform distribution over $R_q^\ell \times R_q$. Most past works have described digital signature schemes, encryption schemes, and key encapsulation mechanisms in one of two ways. Either they set the parameters $k = \ell = 1$ and $R_q = \mathbf{Z}_q[x]/(x^n + 1)$ or they set $k, \ell > 1$ and $R_q = \mathbf{Z}_q$. The former choice results in schemes based on the hardness of the Ring-LWE and Ring-SIS problems (or the NTRU problem), while the latter choice of parameters results in schemes based on the LWE and SIS problems. In this talk, we consider the general case where $k, \ell \geq 1$ and $R = \mathbf{Z}_q[x]/(x^n + 1)$: this case results in schemes based on the Module-LWE and Module-SIS problems [3].

First, we explain how “module lattices” enable to design cryptographic primitives that are not only simple to implement securely, conservatively designed, and have a small memory footprint, but are *modular*, i.e., easily enable to vary security while keeping the same core operations. Then, we present *Kyber* [1], a key encapsulation mechanism, and *Dilithium* [2], a digital signature, part of CRYSTALS—*Cryptographic Suite for Algebraic Lattices*—, a portfolio of cryptographic primitives based on the Module-LWE and Module-SIS hardness assumptions submitted to the NIST call for post-quantum standards.

References

1. Bos, J.W., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J.M., Schwabe, P., Stehlé, D.: CRYSTALS - kyber: a cca-secure module-lattice-based KEM. *IACR Cryptology* (2017). ePrint Archive, 2017:634
2. Ducas, L., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., Stehlé, C.: CRYSTALS - dilithium: digital signatures from module lattices. *IACR Cryptology* (2017). ePrint Archive, 2017:633
3. Langlois, A., Stehlé, D.: Worst-case to average-case reductions for module lattices. *Des. Codes Crypt.* **75**(3), 565–599 (2015)

Contents

Recent Advances in Function and Homomorphic Secret Sharing (Invited Talk)	1
<i>Elette Boyle</i>	
A Note on Ring-LWE Security in the Case of Fully Homomorphic Encryption	27
<i>Guillaume Bonnoron and Caroline Fontaine</i>	
Architecture Level Optimizations for Kummer Based HECC on FPGAs.	44
<i>Gabriel Gallin, Turku Ozlum Celik, and Arnaud Tisserand</i>	
Bricklayer Attack: A Side-Channel Analysis on the ChaCha Quarter Round	65
<i>Alexandre Adomnica, Jacques J. A. Fournier, and Laurent Masson</i>	
CCA-secure Predicate Encryption from Pair Encoding in Prime Order Groups: Generic and Efficient.	85
<i>Sanjit Chatterjee, Sayantan Mukherjee, and Tapas Pandit</i>	
Cold Boot Attacks on NTRU	107
<i>Kenneth G. Paterson and Ricardo Villanueva-Polanco</i>	
Differential Cryptanalysis of 18-Round PRIDE.	126
<i>Virginie Lallemand and Shahram Rasoolzadeh</i>	
DSA Signing Key Recovery with Noisy Side Channels and Variable Error Rates	147
<i>Jiji Angel, R. Rahul, C. Ashokkumar, and Bernard Menezes</i>	
Efficient Construction of Diamond Structures	166
<i>Ariel Weizmann, Orr Dunkelman, and Simi Haber</i>	
Efficient Optimal Ate Pairing at 128-Bit Security Level.	186
<i>Md. Al-Amin Khandaker, Yuki Nanjo, Loubna Ghammam, Sylvain Duquesne, Yasuyuki Nogami, and Yuta Kodera</i>	
Fast Scalar Multiplication for Elliptic Curves over Binary Fields by Efficiently Computable Formulas	206
<i>Saud Al Musa and Guangwu Xu</i>	
Field Lifting for Smaller UOV Public Keys	227
<i>Ward Beullens and Bart Preneel</i>	

Gabidulin Matrix Codes and Their Application to Small Ciphertext Size Cryptosystems	247
<i>Thierry P. Berger, Philippe Gaborit, and Olivier Ruatta</i>	
Lightweight Design Choices for LED-like Block Ciphers	267
<i>Sumanta Sarkar, Habeeb Syed, Rajat Sadhukhan, and Debdeep Mukhopadhyay</i>	
Looting the LUTs: FPGA Optimization of AES and AES-like Ciphers for Authenticated Encryption	282
<i>Mustafa Khairallah, Anupam Chattopadhyay, and Thomas Peyrin</i>	
Improved Differential Cryptanalysis on Generalized Feistel Schemes	302
<i>Ivan Tjuawinata, Tao Huang, and Hongjun Wu</i>	
Improvements for Gate-Hiding Garbled Circuits	325
<i>Mike Rosulek</i>	
Recovering Short Generators of Principal Fractional Ideals in Cyclotomic Fields of Conductor $p^z q^\beta$	346
<i>Patrick Holzer, Thomas Wunderer, and Johannes A. Buchmann</i>	
Revisiting a Masked Lookup-Table Compression Scheme	369
<i>Srinivas Vivek</i>	
Several Masked Implementations of the Boyar-Peralta AES S-Box	384
<i>Ashrut Ghoshal and Thomas De Cnudde</i>	
Author Index	403