Lecture Notes in Computer Science 10095

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

Orr Dunkelman · Somitra Kumar Sanadhya (Eds.)

Progress in Cryptology – INDOCRYPT 2016

17th International Conference on Cryptology in India
Kolkata, India, December 11–14, 2016
Proceedings

Springer

Editors
Orr Dunkelman
University of Haifa
Haifa
Israel

Somitra Kumar Sanadhya
Indraprashtha Institute of Information Technology (IIIT-D)
New Delhi
India

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-49889-8 ISBN 978-3-319-49890-4 (eBook)
DOI 10.1007/978-3-319-49890-4

Library of Congress Control Number: 2016957382

LNCS Sublibrary: SL4 – Security and Cryptology

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

Since its introduction in 2000, INDOCRYPT has been widely acknowledged as the leading Indian venue for cryptography. As part of this tradition, INDOCRYPT 2016 was held during December 11–14, in Kolkata. This was the fourth time the conference was hosted Kolkata since its introduction by Prof. Bimal Roy. Past venues were held throughout India: Kolkata (2000, 2006, 2012, 2016), Chennai (2001, 2004, 2007, 2011), Hyderabad (2002, 2010), New Delhi (2003, 2009, 2014), Bangalore (2005, 2015), Kharagpur (2008), and Mumbai (2013).

INDOCRYPT 2016 attracted 84 submissions from 20 different countries, out of which 23 were selected at the end of a long review process: Most papers were reviewed by at least three committee members, whereas papers co-authored by Program Committee members were reviewed by at least five reviewers. In addition to the 283 reviews (produced with the aid of 91 additional reviewers), the Program Committee generated 223 comments during the discussion phase. We would like to express our sincere gratitude to all the members of the Program Committee, as well as all the external reviewers who helped in the challenging reviewing process.

The submission and review process was done using the iChair software package. We wish to express our sincere gratitude to Thomas Baignères and Matthieu Finiasz for the iChair software, which facilitated a smooth and easy submission and review process.

In addition to the 23 presentations of accepted papers, the attendees of INDOCRYPT also enjoyed three invited talks given by leading experts. Claudio Orlandi (Denmark) spoke about "Faster Zero-Knowledge Protocols for General Circuits and Applications"; the talk by François-Xavier Standaert (Belgium) covered "Leakage-Resilient Symmetric Cryptography"; and Tetsu Iwata (Japan) discussed "Breaking and Repairing Security Proofs of Authenticated Encryption Schemes."

Finally, we would like to thank the general chair, Prof. Bimal Roy, and the local organizing team comprising members from the Applied Statistics Unit, the R.C. Bose Center for Cryptology and Security at ISI Kolkata, and the Cryptology Research Society of India.

December 2016

Orr Dunkelman
Somitra Sanadhya

Organization

General Chair

Bimal Roy	Indian Statistical Institute Kolkata, India

Program Chairs

Orr Dunkelman	University of Haifa, Israel
Somitra Sanadhya	Indraprastha Institute of Information Technology Delhi, India

Program Committee

Diego Aranha	University of Campinas, Brazil
Jean-Philippe Aumasson	Kudelski Security, Switzerland
Steve Babbage	Vodafone Group, UK
Begül Bilgin	KU Leuven, Belgium
Rishiraj Bhattacharya	Indian Statistical Institute Kolkata, India
Céline Blondeau	Aalto University, Finland
Andrey Bogdanov	Technical University of Denmark, Denmark
Itai Dinur	Ben-Gurion University of the Negev, Israel
Helena Handschuh	Cryptography Research, USA and KU Leuven, Belgium
Carmit Hazay	Bar-Ilan University, Israel
Takanori Isobe	Sony Corporation, Japan
Nathan Keller	Bar-Ilan University, Israel
Tanja Lange	Technische Universiteit Eindhoven, The Netherlands
Gaëtan Leurent	Inria, France
Atefeh Mashatan	Ryerson University, Canada
Florian Mendel	Graz University of Technology, Austria
Katerina Mitrokotsa	Chalmers University of Technology, Sweden
Amir Moradi	Ruhr-Universität Bochum, Germany
Debdeep Mukhopadhyay	IIT Kharagpur, India
David Naccache	ENS, France
Michael Naehrig	Microsoft Research, USA
Elisabeth Oswald	University of Bristol, UK
Arpita Patra	Indian Institute of Science, Bangalore
Thomas Peyrin	Nanyang Technological University, Singapore
Axel Poschmann	NXP Semiconductors, Germany
Vanishree Rao	PARC, USA

Francisco Rodríguez-Henríquez	CINVESTAV-IPN, Mexico
Bimal Roy	Indian Statistical Institute Kolkata, India
Santanu Sarkar	IIT Madras, India
Jean-Pierre Seifert	Technische Universität Berlin, Germany
Sourav Sen Gupta	Indian Statistical Institute Kolkata, India
François-Xavier Standaert	UCL, Belgium
Muthuramakrishnan Venkitasubramaniam	University of Rochester, USA
Xiaoyun Wang	Tsinghua University, China

Additional Reviewers

Gora Adj
Shashank Agarwal
Gilad Asharov
Josep Balasch
Subhadeep Banik
Paulo S.L.M. Barreto
Rana Barua
Srimanta Bhattacharya
Johannes Blömer
Debrup Chakraborty
Suvradip Chakraborty
Ayantika Chatterjee
Amit Kumar Chauhan
Chien-Ning Chen
Ran Cohen
Deirdre Connolly
Somindu C.R.
Abhijit Das
Poulami Das
Thomas De Cnudde
David Derler
Sandra Díaz-Santiago
Ning Ding
Christoph Dobraunig
Luis J. Dominguez Perez
Tuyet Duong
Ratna Dutta
Romain Gay
Satrajit Ghosh
Siyao Gou
Lorenzo Grassi
Hannes Gross
Mike Hamburg
Shoichi Hirose
Harunaga Hiwatari
Mike Hutter
Dirmanto Jap
Mahabir Jhawar
Bhavana Kanukurthi
Mikko Kiviharju
Ilya Kizhvatov
François Koeune
Kim Laine
Bei Liang
Patrick Longa
Atul Luykx
Monosij Maitra
Subhamoy Maitra
Daniel Malinowski
Mark Marson
Takahiro Matsuda
Siang Meng Sim
Santos Merino del Pozo
Guillermo Morales-Luna
Pratyay Mukherjee
Sayantan Mukherjee
Mridul Nandi
Khoa Nguyen
Ruben Niederhagen
Eduardo Ochoa-Jiménez
Tobias Oder
Claudio Orlandi
Elena Pagnin
Sumit Kumar Pandey
Tapas Pandit
Sikhar Patranabis
Oxana Poburinnaya
Antigoni Polychroniadou
Somindu Ramanna
Guillaume Rambaud
Shantanu Rane
Joost Renes
Bastian Richter
Lil Rodríguez-Henríquez
Sushmita Ruj
Debapriya Basu Roy
Vishal Saraswat
Pascal Sasdrich
Tobias Schneider
Kyoji Shibutani
Igor Shparlinski
Danilo Šijačić
Deng Tang
Mehdi Tibouchi
Ayineedi Venkateswarlu
Vincent Verneuil
Qingju Wang
Benjamin Wesolowski
Alexander Wild
Bo-Yin Yang
Hong-Sheng Zhou

Invited Talks

Leakage-Resilient Symmetric Cryptography - Overview of the ERC Project CRASH, Part II

François-Xavier Standaert

ICTEAM Institute, Crypto Group, Université catholique de Louvain, Ottignies-Louvain-la-Neuve, Belgium
fstandae@uclouvain.be

Abstract. Side-channel analysis is an important concern for the security of cryptographic implementations, and may lead to powerful key recovery attacks if no countermeasures are deployed. Therefore, various types of protection mechanisms have been proposed over the last 20 year. The first solutions in this direction were typically aiming at reducing the amount of information leakage directly at the hardware level, and independent of the algorithm implemented. Over the years, a complementary approach (next denoted as leakage-resilience) emerged, trying to exploit the formalism of modern cryptography in order to design new constructions and security models in which the guarantees of provable security can be extended from mathematical objects towards physical ones. This naturally raises the question whether the formal results obtained in these models are practically relevant (both in terms of performance and security)?

The development of sound connections between the formal models of leakage-resilient (symmetric) cryptography and the practice of side-channel attacks was one of the main objectives of the CRASH project funded by the European Research Council. In this talk, I will survey a number of results we obtained in this direction. For this purpose, I will start with a separation result for the security of stateful and stateless primitives. I will then follow with a discussion of (*i*) pseudorandom building blocks together with the theoretical challenges they raise, and (*ii*) authentication, encryption and authenticated encryption schemes together with the practical challenges they raise. I will finally conclude by discussing emerging trends in the field of physically secure implementations.

The extended version of this abstract is available from [1].

Reference

1. http://perso.uclouvain.be/fstandae/PUBLIS/184.pdf

Faster Zero-Knowledge Protocols for General Circuits and Applications

Claudio Orlandi

Aarhus University, Aarhus, Denmark

Abstract. *Zero-knowledge protocols (ZKP)* [GMR85] are one of the cornerstones of modern cryptography. In a nutshell, a ZKP allows a prover P (with a secret input x) to persuade a verifier V that $f(x) = 1$ for some public function f, without the V learning any other information about x.

A large body of literature has investigated the efficiency of ZKP for statements with a rich algebraic structure, starting from Schnorr's classic ZKP for discrete logarithm [Sch89]. However, the lack of efficient ZKP for interesting, non-algebraic statements (such as "*I know x such that SHA - 256 (x) = y*" for a public y), has arguably prevented the application of ZKPs to real-world applications.

In this talk I will describe two recent ZKPs for arbitrary circuits, ZKGC [JKO13] and ZKBoo [GMO16], together with their applications.

The first protocol (ZKGC), leveraging on the impressive advances in the field of practically efficient secure two-party computation (2PC), proposes to perform *zero-knowledge from garbled Boolean circuits*. As opposed to general 2PC (where many copies of the circuit must be garbled to achieve active security), when constructing ZKP it is enough to garble and evaluate *a single circuit*. Moreover, due to the nature of the application (since the verifier has no secret input), more efficient special purpose *privacy-free garbling schemes* [FNO15] can be used instead.

The second protocol instead (ZKBoo) follows a more classic "commit-challenge-response" structure (i.e., is a Σ-protocol). In ZKBoo the prover decomposes the computation of the function f in such a way that subsets of the computation can be checked by the verifier without revealing any information about the input to the computation, following the approach proposed by [IKOS07].

ZKGC and ZKBoo both have interesting properties: ZKGC leads to *smaller proof sizes* and, since it is based on garbled circuits, it can be combined very naturally with pre-existing secure computation tools towards building interesting applications such as: enforcing input validity in secure two-party computation [Bau16, KMW16], attributed-based key exchange with general policies [KKL$^+$16], privacy-preserving credentials [CGM16], ZKPs for RAM programs [HMR15], etc.

ZKBoo on the other hand is *faster* and can be used for both Boolean and arithmetic circuits. Perhaps most importantly, ZKBoo can be made *non-interactive* using the Fiat-Shamir [FS86] heuristic. This qualitative advantage allows to use ZKBoo in applications such as (post-quantum) signature schemes from symmetric-key primitives [DOR$^+$16], blind certificate authorities [WPaR16], etc.

It is exciting to see the growing number of applications which are enabled (or benefit) by the advances in the realm of ZKPs, and it seems likely that future research will make use of these tools in designing cryptographic solutions to interesting problems.

From a technical point of view, the main bottleneck in ZKGC and ZKBoo is their communication complexity, which in both cases is proportional to the number of non-linear gates in f times the security parameter (resulting in proof sizes in the order of hundreds of kylobytes for functions like SHA-1/256). Whether and how we can overcome this is a major and very exciting research question.

Acknowledgements. Research supported by: the Danish National Research Foundation and The National Science Foundation of China (grant 61361136003) for the Sino-Danish Center for the Theory of Interactive Computation; the European Union Seventh Framework Programme ([FP7/2007-2013]) under grant agreement number ICT-609611 (PRACTICE).

References

[Bau16] Baum, C.: On garbling schemes with and without privacy. In: Zikas, V., De Prisco, R. (eds.) Security and Cryptography for Networks - 10th International Conference, SCN 2016, Amalfi, Italy, 31 August – 2 September 2016, Proceedings, pp. 468–485. Springer, Switzerland (2016)

[CGM16] Chase, M., Ganesh, C., Mohassel, P.: Efficient zero-knowledge proof of algebraic and non-algebraic statements with applications to privacy preserving credentials. In: Robshaw, M., Katz, J. (eds.) Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, 14–18 August 2016, Proceedings, Part III, pp. 499–530. Springer, Heidelberg (2016)

[DOR+16] Derler, D., Orlandi, C., Ramacher, S., Rechberger, C., Slamanig, D.: Digital signatures from symmetric-key primitives. In: Manuscript (2016)

[FNO15] Frederiksen, T.K., Nielsen, J.B., Orlandi, C.: Privacy-free garbled circuits with applications to efficient zero-knowledge. In: Oswald, E., Fischlin, M. (eds.) Advances in Cryptology - EUROCRYPT 2015 - 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, 26–30 April 2015, Proceedings, Part II, pp. 191–219.Springer, Heidelberg (2015)

[FS86] Fiat, A., Shamir, A.: How to prove yourself: practical solutions to identification and signature problems. In: Odlyzko, A.M. (ed.) Advances in Cryptology — CRYPTO 1986, pp. 186–194. Springer, Heidelberg (1986)

[GMO16] Giacomelli, I., Madsen, J., Orlandi, C.: Zkboo: faster zero-knowledge for boolean circuits. In: 25th USENIX Security Symposium, USENIX Security 16, Austin, TX, USA, 10–12 August 2016, pp. 1069–1083 (2016)

[GMR85] Goldwasser, S., Micali, S., Rackoff, C.: The knowledge complexity of interactive proof-systems (extended abstract). In: Proceedings of the 17th Annual ACM Symposium on Theory of Computing, 6–8 May 1985, Providence, Rhode Island, USA, pp. 291–304 (1985)

[HMR15] Hu, Z., Mohassel, P., Rosulek, M.: Efficient zero-knowledge proofs of non-algebraic statements with sublinear amortized cost. In: Gennaro, R., Robshaw M. (eds.) Advances in Cryptology - CRYPTO 2015 - 35th Annual Cryptology Conference, Santa Barbara, CA, USA, 16–20 August 2015, Proceedings, Part II, pp. 150–169. Springer, Heidelberg (2015)

[IKOS07] Ishai, Y., Kushilevitz, E., Ostrovsky, R., Sahai, A.: Zero-knowledge from secure multiparty computation. In: Proceedings of the Thirty-ninth Annual ACM Symposium on Theory of Computing, STOC 2007, pp. 21–30. ACM (2007)

[JKO13] Jawurek, M., Kerschbaum, F., Orlandi, C.: Zero-knowledge using garbled circuits: how to prove non-algebraic statements efficiently. In: 2013 ACM SIGSAC Conference on Computer and Communications Security, CCS 2013, Berlin, Germany, 4–8 November 2013, pp. 955–966 (2013)

[KKL+16] Kolesnikov, V., Krawczyk, H., Lindell, Y., Malozemoff, A.J., Rabin, T.: Attribute-based key exchange with general policies. CCS 2016 (2016). http://eprint.iacr.org/2016/518

[KMW16] Katz, J., Malozemoff, A.J., Wang, X.: Efficiently enforcing input validity in secure two-party computation. Cryptology ePrint Archive, Report 2016/184 (2016). http://eprint.iacr.org/2016/184

[Sch89] Schnorr, C.-P.: Efficient identification and signatures for smart cards. In: CRYPTO, pp. 239–252 (1989)

[WPaR16] Wang, L., Pass, R., Shelat, A., Ristenpart, T.: Secure channel injection and anonymous proofs of account ownership. Cryptology ePrint Archive, Report 2016/925 (2016) http://eprint.iacr.org/2016/925

Contents

Public-Key Cryptography

Blending FHE-NTRU Keys – The Excalibur Property 3
Louis Goubin and Francisco José Vial Prado

Approximate-Deterministic Public Key Encryption from Hard Learning Problems 25
Yamin Liu, Xianhui Lu, Bao Li, Wenpan Jing, and Fuyang Fang

Adaptively Secure Strong Designated Signature 43
Neetu Sharma, Rajeev Anand Sahu, Vishal Saraswat, and Birendra Kumar Sharma

The Shortest Signatures Ever 61
Mohamed Saied Emam Mohamed and Albrecht Petzoldt

Cryptographic Protocols

CRT-Based Outsourcing Algorithms for Modular Exponentiations. 81
Lakshmi Kuppusamy and Jothi Rangasamy

Verifiable Computation for Randomized Algorithm 99
Muhua Liu, Ying Wu, and Rui Xue

UC-secure and Contributory Password-Authenticated Group Key Exchange . . . 119
Lin Zhang and Zhenfeng Zhang

Side-Channel Attacks

Score-Based vs. Probability-Based Enumeration – A Cautionary Note 137
Marios O. Choudary, Romain Poussier, and François-Xavier Standaert

Analyzing the Shuffling Side-Channel Countermeasure for Lattice-Based Signatures 153
Peter Pessl

Implementation of Cryptographic Schemes

Atomic-AES: A Compact Implementation of the AES Encryption/Decryption Core 173
Subhadeep Banik, Andrey Bogdanov, and Francesco Regazzoni

Fast Hardware Architectures for Supersingular Isogeny Diffie-Hellman Key Exchange on FPGA 191
Brian Koziel, Reza Azarderakhsh, and Mehran Mozaffari-Kermani

AEZ: Anything-But EaZy in Hardware 207
Ekawat Homsirikamol and Kris Gaj

Functional Encryption

Private Functional Encryption: Indistinguishability-Based Definitions and Constructions from Obfuscation 227
Afonso Arriaga, Manuel Barbosa, and Pooya Farshim

Revocable Decentralized Multi-Authority Functional Encryption 248
Hikaru Tsuchida, Takashi Nishide, Eiji Okamoto, and Kwangjo Kim

Symmetric-Key Cryptanalysis

On Linear Hulls and Trails 269
Tomer Ashur and Vincent Rijmen

Related-Key Cryptanalysis of Midori 287
David Gérault and Pascal Lafourcade

Some Proofs of Joint Distributions of Keystream Biases in RC4 305
Sonu Jha, Subhadeep Banik, Takanori Isobe, and Toshihiro Ohigashi

Practical Low Data-Complexity Subspace-Trail Cryptanalysis of Round-Reduced PRINCE 322
Lorenzo Grassi and Christian Rechberger

Foundations

On Negation Complexity of Injections, Surjections and Collision-Resistance in Cryptography 345
Douglas Miller, Adam Scrivener, Jesse Stern, and Muthuramakrishnan Venkitasubramaniam

Implicit Quadratic Property of Differentially 4-Uniform Permutations 364
Theo Fanuela Prabowo and Chik How Tan

Secret Sharing for mNP: Completeness Results 380
Mahabir Prasad Jhanwar and Kannan Srinathan

New Cryptographic Constructions

Receiver Selective Opening Security from Indistinguishability Obfuscation 393
Dingding Jia, Xianhui Lu, and Bao Li

Format Preserving Sets: On Diffusion Layers of Format Preserving Encryption Schemes 411
Kishan Chand Gupta, Sumit Kumar Pandey, and Indranil Ghosh Ray

Author Index 429