



HAL
open science

Selected Areas in Cryptography

Benjamin Smith, Huapeng Wu

► **To cite this version:**

Benjamin Smith, Huapeng Wu. Selected Areas in Cryptography. SAC 2022 - International Conference on Selected Areas in Cryptography, Lecture Notes in Computer Science, LNCS-13742, Springer International Publishing, 2024, Selected Areas in Cryptography, 978-3-031-58410-7. 10.1007/978-3-031-58411-4 . hal-04579052

HAL Id: hal-04579052

<https://inria.hal.science/hal-04579052v1>

Submitted on 8 Nov 2024

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons Attribution 4.0 International License

Lecture Notes in Computer Science

13742


Founding Editors


Gerhard Goos
Juris Hartmanis

Editorial Board Members

Elisa Bertino, *Purdue University, West Lafayette, IN, USA*

Wen Gao, *Peking University, Beijing, China*

Bernhard Steffen , *TU Dortmund University, Dortmund, Germany*

Moti Yung , *Columbia University, New York, NY, USA*

The series Lecture Notes in Computer Science (LNCS), including its subseries Lecture Notes in Artificial Intelligence (LNAI) and Lecture Notes in Bioinformatics (LNBI), has established itself as a medium for the publication of new developments in computer science and information technology research, teaching, and education.

LNCS enjoys close cooperation with the computer science R & D community, the series counts many renowned academics among its volume editors and paper authors, and collaborates with prestigious societies. Its mission is to serve this international community by providing an invaluable service, mainly focused on the publication of conference and workshop proceedings and postproceedings. LNCS commenced publication in 1973.

Benjamin Smith · Huapeng Wu
Editors

Selected Areas in Cryptography

29th International Conference, SAC 2022
Windsor, ON, Canada, August 24–26, 2022
Revised Selected Papers

Editors

Benjamin Smith
Inria and École Polytechnique
Institut Polytechnique de Paris
Palaiseau, France

Huapeng Wu
Electrical and Computer Engineering
University of Windsor
Windsor, ON, Canada

ISSN 0302-9743

ISSN 1611-3349 (electronic)

Lecture Notes in Computer Science

ISBN 978-3-031-58410-7

ISBN 978-3-031-58411-4 (eBook)

<https://doi.org/10.1007/978-3-031-58411-4>

© The Editor(s) (if applicable) and The Author(s), under exclusive license
to Springer Nature Switzerland AG 2024

This work is subject to copyright. All rights are solely and exclusively licensed 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, expressed 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.

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

Paper in this product is recyclable.

Preface

Selected Areas in Cryptography (SAC) is Canada’s annual cryptography research conference, held since 1994. The 29th edition of SAC took place at the University of Windsor, in Ontario, from August 24 to 26, 2022. Due to the ongoing COVID-19 pandemic, SAC 2022 was a hybrid event, with talks and discussion streamed online. The conference was preceded by a two-day summer school on August 22 and 23, with tutorials on isogeny-based cryptography and real-world post-quantum cryptography from Javad Doliskani, Benjamin Smith, and Douglas Stebila.

Each SAC conference covers four areas of research in cryptography. Three of these areas are permanent:

- Design and analysis of symmetric key primitives and cryptosystems, including block and stream ciphers, hash functions, MAC algorithms, cryptographic permutations, and authenticated encryption schemes;
- Efficient implementations of symmetric, public key, and post-quantum cryptography;
- Mathematical and algorithmic aspects of applied cryptography, including post-quantum cryptology.

The fourth area is selected as a special topic for each edition of SAC. For SAC 2022, this area was

- Theory and practice of isogeny-based cryptography.

We received 53 submissions; these were reviewed in a double-blind peer review process coordinated by the Program Committee. Regular submissions received three reviews; submissions involving members of the Program Committee received five reviews. Overall, our 34 Program Committee members, and their 28 subreviewers, wrote 172 reviews. Twenty-one of the submissions were accepted for presentation at SAC 2022 and publication in these proceedings.

There were three invited talks at SAC 2022. Nadia Heninger gave the Stafford Tavares lecture virtually: “On the passive compromise of TLS keys and other cryptanalytic adventures”. Benjamin Wesolowski gave the second invited talk in person, on “Hard problems for isogeny-based cryptography”. Finally, Wouter Castryck gave the third invited talk on “Efficient key recovery attacks on SIDH”.

We would like to thank all of our colleagues who helped to make SAC 2022 a success, especially given the continuing complications all around the world due to the COVID-19 pandemic. We thank the Program Committee members for excellent work under a tight schedule. We are also grateful to the many others who participated in the review process: Gora Adj, Foteini Baldimtsi, Christof Beierle, Francesco Berti, Kevin Carrier, Arcangelo Castiglione, James Clements, Patrick Derbez, Thomas Espitau, Anna Lisa Ferrara, Manuela Flores, Clemente Galdi, Gayathri Garimella, Lydia Garms, Hosein Hadipour, Ryoma Ito, Amandine Jambert, Mikhail Kudinov, Norman Lahr, Fukang Liu, Liam Medley, Matthias Meijers, Mridul Nandi, Patrick Neumann, Richard Petri, Robert

Primas, Krijn Reijnders, and Florian Weber. We also thank the invited speakers for their excellent presentations, the summer school lecturers for animating a dynamic in-person event, and the SAC steering committee for their helpful advice and guidance. We are also appreciative of the financial support provided by the University of Windsor and by the Communications Security Establishment of Canada.

Finally, special thanks are due to Jo Asuncion for providing administrative assistance and we appreciate the help in the local arrangements offered by Lisa Geloso, Andria Ballo, Raqib Asif, Chen Zhang, and Hamza Bin Zaheer.

December 2023

Benjamin Smith
Huapeng Wu

Organization

Program Committee

Riham AlTawy	University of Victoria, Canada
Melissa Azouaoui	NXP Semiconductors, USA
Paulo Barreto	University of Washington Tacoma, USA
Jean-François Biasse	University of South Florida, USA
Olivier Blazy	École polytechnique, France
Claude Carlet	Université Paris 8, France and University of Bergen, Norway
Wouter Castryck	KU Leuven, Belgium
Carlos Cid	Simula UiB, Norway and Okinawa Institute of Science and Technology, Japan
Craig Costello	Microsoft Research, USA
Luca De Feo	IBM Research Europe, Switzerland
Maria Eichlseder	Graz University of Technology, Austria
Aurore Guillevic	Inria Nancy, France and Aarhus University, Denmark
Kathrin Hövelmanns	TU Eindhoven, the Netherlands
Michael J. Jacobson Jr.	University of Calgary, Canada
Yunwen Liu	Independent Researcher
Subhamoy Maitra	Indian Statistical Institute Kolkata, India
Kalikinkar Mandal	University of New Brunswick, Canada
Chloe Martindale	University of Bristol, UK
Barbara Masucci	University of Salerno, Italy
Ruben Niederhagen	Academia Sinica, Taiwan and University of Southern Denmark, Denmark
Abderrahmane Nitaj	University of Caen Normandy, France
Lorenz Panny	Academia Sinica, Taipei, Taiwan
Elizabeth A. Quaglia	Royal Holloway, University of London, UK
Francisco Rodríguez-Henríquez	CINVESTAV-IPN, México and CRC-TII, United Arab Emirates
Yann Rotella	Université de Versailles Saint-Quentin, France
Simona Samardjiska	RU Nijmegen, the Netherlands
Nicolas Sendrier	Inria, France
Leonie Simpson	Queensland University of Technology, Australia
Benjamin Smith	Inria and École polytechnique, Institut Polytechnique de Paris, France

Djiby Sow	Cheikh Anta Diop University, Senegal
Douglas Stebila	University of Waterloo, Canada
Katsuyuki Takashima	Waseda University, Japan
Yosuke Todo	NTT Secure Platform Laboratories, Japan
Yuntao Wang	Osaka University, Japan
Huapeng Wu	University of Windsor, Canada

Additional Reviewers

Gora Adj	Hosein Hadipour
Foteini Baldimtsi	Ryoma Ito
Christof Beierle	Amandine Jambert
Francesco Berti	Mikhail Kudinov
Kevin Carrier	Norman Lahr
Arcangelo Castiglione	Fukang Liu
James Clements	Liam Medley
Patrick Derbez	Matthias Meijers
Thomas Espitau	Mridul Nandi
Anna Lisa Ferrara	Patrick Neumann
Manuela Flores	Richard Petri
Clemente Galdi	Robert Primas
Gayathri Garimella	Krijn Reijnders
Lydia Garms	Florian Weber

Invited Talks

On the Passive Compromise of TLS Keys and Other Cryptanalytic Adventures

Nadia Heninger

Computer Science and Engineering, University of California San Diego, 9500 Gilman
Drive, La Jolla, CA, 92093-0021 USA
nadiyah@cs.ucsd.edu

Abstract. It is well known in the cryptographic literature that the most common digital signature schemes used in practice can fail catastrophically in the presence of faults during computation. I will discuss recent joint work using passive and active network measurements to analyze organically-occurring faults in billions of digital signatures generated by tens of millions of hosts. We find that a persistent rate of apparent hardware faults in unprotected implementations has resulted in compromised certificate RSA private keys for years. Finally, we will put this work in the context of other cryptographic flaws that can be exploited in the wild.

Hard Problems for Isogeny-Based Cryptography

Benjamin Wesolowski

Institut de Mathématiques de Bordeaux, 351, Cours de la Libération, 33405 Talence,
France

`benjamin.wesolowski@ens-lyon.fr`

Abstract. Isogeny-based cryptography is one of the few branches of public-key cryptography that promises to resist quantum attacks. The security of these cryptosystems relates to the (presumed) hardness of a variety of computational problems: finding paths in large “isogeny graphs”, computing endomorphisms of elliptic curves, or inverting group actions. We present these problems, and analyse how they relate to each other: which are equivalent, easier, or harder, and how they relate to cryptosystems.

Efficient Key Recovery Attacks on SIDH

Wouter Castryck

Department of Electrical Engineering, KU Leuven, Oude Markt 13 - bus 5005, 3000
Leuven, Belgium
wouter.castryck@gmail.com

Abstract. It is well known in the cryptographic literature that the most common digital signature schemes used in practice can fail catastrophically in the presence of faults during computation. I will discuss recent joint work using passive and active network measurements to analyze organically-occurring faults in billions of digital signatures generated by tens of millions of hosts. We find that a persistent rate of apparent hardware faults in unprotected implementations has resulted in compromised certificate RSA private keys for years. Finally, we will put this work in the context of other cryptographic flaws that can be exploited in the wild.

Contents

Lattices and ECC

Profiling Side-Channel Attacks on Dilithium: A Small Bit-Fiddling Leak Breaks It All	3
<i>Vincent Quentin Ulitzsch, Soundes Marzougui, Mehdi Tibouchi, and Jean-Pierre Seifert</i>	
On the Weakness of Ring-LWE mod Prime Ideal \mathfrak{q} by Trace Map	33
<i>Tomoka Takahashi, Shinya Okumura, and Atsuko Miyaji</i>	
2DT-GLS: Faster and Exception-Free Scalar Multiplication in the GLS254 Binary Curve	53
<i>Marius A. Aardal and Diego F. Aranha</i>	

Differential Cryptanalysis

Key-Recovery Attacks on CRAFT and WARP	77
<i>Ling Sun, Wei Wang, and Meiqin Wang</i>	
Differential Analysis of the Ternary Hash Function Troika	96
<i>Christina Boura, Margot Funk, and Yann Rotella</i>	
Another Look at Differential-Linear Attacks	116
<i>Orr Dunkelman and Ariel Weizman</i>	

Cryptographic Primitives

Injective Rank Metric Trapdoor Functions with Homogeneous Errors	139
<i>Étienne Burle, Philippe Gaborit, Younes Hatri, and Ayoub Otmani</i>	
PERKS: Persistent and Distributed Key Acquisition for Secure Storage from Passwords	159
<i>Gareth T. Davies and Jeroen Pijnenburg</i>	
Improved Circuit-Based PSI via Equality Preserving Compression	190
<i>Kyoohyung Han, Dukjae Moon, and Yongha Son</i>	

Isogeny-based Cryptography I

Revisiting Meet-in-the-Middle Cryptanalysis of SIDH/SIKE
with Application to the \$IKEp182 Challenge 213
Aleksei Udovenko and Giuseppe Vito

Patient Zero & Patient Six: Zero-Value and Correlation Attacks on CSIDH
and SIKE 234
Fabio Campos, Michael Meyer, Krijn Reijnders, and Marc Stöttinger

An Effective Lower Bound on the Number of Orientable Supersingular
Elliptic Curves 263
Antonin Leroux

Block Ciphers

Finding All Impossible Differentials When Considering the DDT 285
Kai Hu, Thomas Peyrin, and Meiqin Wang

A Three-Stage MITM Attack on LowMC from a Single
Plaintext-Ciphertext Pair 306
Lulu Zhang, Meicheng Liu, and Dongdai Lin

Collision-Based Attacks on White-Box Implementations of the AES
Block Cipher 328
Jiqiang Lu, Mingxue Wang, Can Wang, and Chen Yang

Differential Cryptanalysis II

Advancing the Meet-in-the-Filter Technique: Applications to CHAM
and KATAN 355
Alex Biryukov, Je Sen Teh, and Aleksei Udovenko

Improved the Automated Evaluation Algorithm Against Differential
Attacks and Its Application to WARP 376
Jiali Shi, Guoqiang Liu, and Chao Li

Isogeny-based Cryptography II

Faster Cryptographic Hash Function from Supersingular Isogeny Graphs 399
*Javad Doliskani, Geovandro C. C. F. Pereira,
and Paulo S. L. M. Barreto*

Protocols and PRFs

From Plaintext-Extractability to IND-CCA Security 419
Ehsan Ebrahimi

Farasha: A Provable Permutation-Based Parallelizable PRF 437
*Najwa Aaraj, Emanuele Bellini, Ravindra Jejurikar, Marc Manzano,
 Raghvendra Rohit, and Eugenio Salazar*

A Sponge-Based PRF with Good Multi-user Security 459
Arghya Bhattacharjee, Ritam Bhaumik, and Mridul Nandi

Author Index 479