Takanori Isobe
Santanu Sarkar (Eds.)

LNCS 13774

Progress in Cryptology – INDOCRYPT 2022

23rd International Conference on Cryptology in India
Kolkata, India, December 11–14, 2022
Proceedings

Springer

Lecture Notes in Computer Science 13774

More information about this series at https://link.springer.com/bookseries/558

Takanori Isobe · Santanu Sarkar (Eds.)

Progress in Cryptology – INDOCRYPT 2022

23rd International Conference on Cryptology in India
Kolkata, India, December 11–14, 2022
Proceedings

Springer

Editors
Takanori Isobe
University of Hyogo
Hyogo, Japan

Santanu Sarkar
Indian Institute of Technology Madras
Chennai, India

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-031-22911-4 ISBN 978-3-031-22912-1 (eBook)
https://doi.org/10.1007/978-3-031-22912-1

Preface

With great pleasure, we present the proceedings of INDOCRYPT 2022, the 23rd International Conference on Cryptology in India, organized by The Chatterjee Group - Centers for Research and Education in Science and Technology (TCG CREST), the R. C. Bose Centre for Cryptology and Security, Indian Statistical Institute, Kolkata, and the Bose Institute, Kolkata, under the aegis of the Cryptology Research Society of India (CRSI).

INDOCRYPT began in 2000 under the leadership of Bimal Roy at the Indian Statistical Institute, Kolkata, with an intention to target researchers and academicians in the domain of cryptology. Since its inception, this annual conference has not only been considered as the leading Indian venue on cryptology but also has gained recognition among the prestigious cryptology conferences in the world. Over the last two decades, the conference was held in various cities of India, such as Kolkata (2000, 2006, 2012, 2016), Chennai (2001, 2004, 2007, 2011, 2017), Hyderabad (2002, 2010, 2019), New Delhi (2003, 2009, 2014, 2018), Bangalore (2005, 2015), Kharagpur (2008), Mumbai (2013), and Jaipur (2021). Due to COVID-19 pandemic restrictions, INDOCRYPT went online in 2020. This year was the fifth time the conference was hosted in Kolkata, but in a hybrid mode.

INDOCRYPT 2022 received 88 submissions from 30 different countries in total, among which the papers that were withdrawn before the deadline, or the ones that didn't match the submission policy, were not considered for evaluation. Finally, 74 papers were reviewed by three to four reviewers each. First, the papers went through a double-blind review phase. Next, after a two week discussion phase, with additional comments from the Program Committee members as well as the external reviewers, 31 papers by authors from 17 different countries were finally accepted for presentation in the program and inclusion in this proceedings.

We are immensely thankful to the 52 Program Committee members and the 64 external reviewers, who participated in the process of reviewing and subsequent discussions. Without their tremendous effort, the conference would not have been successful. We would also like to express our gratitude to Springer for their active cooperation and timely production of the conference proceedings. We managed the submissions, reviews, discussions, and proceedings very effectively using the online EasyChair conference management software system and would like to acknowledge this with great regard.

Our program also included three invited talks by V. Kamakoti from IIT Madras, India, Gregor Leander from Ruhr University Bochum, Germany, and Alexander May from Ruhr University Bochum, Germany. Moreover, there were three tutorial talks by Patrick Derbez from University of Rennes 1, France, Mridul Nandi from ISI Kolkata, India, and Santanu Sarkar from IIT Madras, India.

INDOCRYPT 2022 was organized by TCG CREST and the R. C. Bose Centre for Cryptology and Security with the Bose Institute providing the conference venue. We are extremely thankful to the General Co-chairs, Bimal Kumar Roy (ISI Kolkata)

and Joydeep Bhattacharya (TCG CREST), for coordinating all the issues related to the organization of the event. We would also like to take this opportunity to thank the Organizing Chair, Organizing Co-chairs, and all members of the Organizing Committee, for their relentless support in successfully hosting the conference.

We are also immensely thankful to the Government of India, the Government of West Bengal, and our sponsors Google, HDFC Bank, Vehere Interactive Pvt. Ltd., AON, KEWAUNEE International Group, TwoPiRadian Infotech Private Limited, and Bosch Global Software Technologies Private Limited, for their generous financial support towards the conference.

Last but not the least, we are extremely thankful to each of the 220 authors who submitted their articles to the conference and those who attended INDOCRYPT 2022.

October 2022

Takanori Isobe
Santanu Sarkar

Organization

General Chairs

Bimal Kumar Roy	ISI Kolkata, India
Joydeep Bhattacharya	TCG CREST, India

Program Co-chairs

Takanori Isobe	University of Hyogo, Japan
Santanu Sarkar	IIT Madras, India

Organizing Chair

Subhamoy Maitra	ISI Kolkata, India

Organizing Co-chairs

Somshubhro Bandyopadhyay	Bose Institute, India
Soumyajit Biswas	TCG CREST, India
Nilanjan Datta	TCG CREST, India

Sponsorship Chair

Rakesh Kumar	ISI Kolkata, India

Accommodation Chair

Bibhas Chandra Das	TCG CREST, India

Organizing Committee

Avik Chakraborti	TCG CREST, India
Shreya Dey	TCG CREST, India
Avijit Dutta	TCG CREST, India
Arpita Maitra	TCG CREST, India
Sougata Mandal	TCG CREST, India
Payel Sadhukhan	TCG CREST, India
Soumya Kanti Saha	TCG CREST, India

Laltu Sardar	TCG CREST, India
Bishakha Sarkar	TCG CREST, India

Program Committee

Avishek Adhakari	Presidency University, India
Shi Bai	Florida Atlantic University, USA
Christof Beierle	Ruhr University Bochum, Bochum, Germany
Rishiraj Bhattacharyya	NISER, India
Christina Boura	University of Versailles, France
Suvradip Chakraborty	ETH Zurich, Switzerland
Anupam Chattopadhyay	NTU, Singapore
Sherman Chow	Chinese University of Hong Kong, Hong Kong
Prem Laxman Das	SETS Chennai, India
Nilanjan Datta	TCG CREST, India
Avijit Dutta	TCG CREST, India
Ratna Dutta	IIT Kharagpur, India
Keita Emura	National Institute of Information and Communications Technology, Japan
Andre Esser	Technology Innovation Institute, Abu Dhabi, UAE
Indivar Gupta	DRDO, Delhi, India
Akinori Hosoyamada	NTT Social Informatics Laboratories, Japan
Mahavir Jhanwar	Ashoka University, India
Selcuk Kavut	Balikesir University, Turkey
Sumit Kumar Pandey	IIT Jammu, India
Jason LeGrow	Verginia Polytechnic Institute and State University, USA
Chaoyun Li	KU Leuven, Belgium
Fukang Liu	University of Hyogo, Japan
Arpita Maitra	TCG CREST, India
Takahiro Matsuda	National Institute of Advanced Industrial Science and Technology, Japan
Willi Meier	FHNW, Brugg-Windisch, Switzerland
Alfred Menezes	University of Waterloo, Canada
Sihem Mesnager	Universities of Paris VIII and XIII, LAGA Lab, France
Kazuhiko Minematsu	NEC, Kawasaki, Japan
Marine Minier	Loria, France
Pratyay Mukherjee	Swirlds Labs/Hedera, USA
Debdeep Mukhopadhyay	IIT Kharagpur, India
Mridul Nandi	ISI, India
David Oswald	University of Birmingham, UK
Saibal Pal	DRDO, Delhi, India

Chester Rebeiro	IIT Madras, Chennai, India
Francesco Regazzoni	University of Amsterdam, Netherlands
Raghavendra Rohit	Technology Innovation Institute, Abu Dhabi, UAE
Sushmita Ruj	University of New South Wales, Sydney, Australia
Somitra Sanadhya	IIT Jodhpur, India
Sourav Sen Gupta	NTU, Singapore
Nicolas Sendrier	Inria, France
Yixin Shen	Royal Holloway, University of London, UK
Bhupendra Singh	DRDO, Bangalore, India
Sujoy Sinha Roy	TU Graz, Austria
Pantelimon Stanica	Naval Postgraduate School, Monterey, USA
Ron Steinfeld	Monash University, Clayton, Australia
Atsushi Takayasu	The University of Tokyo, Japan
Meltem Turan	National Institute of Standards and Technology, USA
Rei Ueno	Tohoku University, Japan
Alexandre Wallet	Inria, France
Yuyu Wang	University of Electronic Science and Technology of China, China
Jun Xu	Institute of Information Engineering, Chinese Academy of Sciences, China

Additional Reviewers

Aikata Aikata
Anubhab Baksi
Pierre Briaud
Bin-Bin Cai
Anirban Chakraborty
Bishwajit Chakraborty
Donghoon Chang
Haokai Changmit Kumar Chauhan
Jorge Chavez-Saab
Pratish Datta
Sabyasachi Dutta
Paul Frixons
David Gerault
Chun Guo
Guifang Huang
Mitsugu Iwamoto
David Jacquemin
Floyd Johnson
Meenakshi Kansal
Hamidreza Khoshakhlagh
Fuyuki Kitagawa
Abhishek Kumar
Kaoru Kurosawa
Virginie Lallemand
Roman Langrehr
Jack P. K. Ma
Gilles Macario-Rat
Monosij Maitra
Siva Kumar Maradana
Subhra Mazumdar
Prasanna Mishra
Girish Mishra
Sayantan Mukherjee
Yusuke Naito
Lucien K. L. Ng
Tran Ngo
Ying-Yu Pan
Tapas Pandit
Amaury Pouly
Mayank Raikwar

Prasanna Ravi
Divya Ravi
Maxime Remaud
Yann Rotella
Debapriya Basu Roy
Partha Sarathi Roy
Rajat Sadhukhan
Yu Sasaki
AndrÃ© Schrottenloher
Jacob Schuldt
Xiangyu Su
Masayuki Tezuka
Toi Tomita
Hikaru Tsuchida
Natarajan Venkatachalam
Javier Verbel
Sulani Kottal Baddhe Vidhanalage
Deepak Vishwakarma
Xiuhua Wang
Harry W.H. Wong
Qianqian Yang
Rui Zhang
Liang Zhao
Lukas Zobernig

Contents

Protocols and Implementation

Cryptanalysis

Boolean Functions

Quantum Cryptography and Cryptanalysis

Post Quantum Cryptography