

Preface

The third successful completion of the INDOCRYPT conference series marks the acceptance of the series by the international research community as a forum for presenting high-quality research. It also marks the coming of age of cryptology research in India.

The authors for the submitted papers were spread across 21 countries and 4 continents, which goes a long way to demonstrate the international interest and visibility of INDOCRYPT. In the previous two conferences, the submissions from India originated from only two institutes; this increased to six for the 2002 conference. Thus INDOCRYPT is well set on the path to achieving two main objectives – to provide an international platform for presenting high-quality research and to stimulate cryptology research in India.

The opportunity to serve as a program co-chair for the third INDOCRYPT carries a special satisfaction for the second editor. Way back in 1998, the scientific analysis group of DRDO organized a National Seminar on Cryptology and abbreviated it as NSCR. On attending the seminar, the second editor suggested that the conference name be changed to INDOCRYPT. It is nice to see that this suggestion was taken up, giving us the annual INDOCRYPT conference series. Of course, the form, character, and execution of the conference series was the combined effort of the entire Indian cryptographic community under the dynamic leadership of Bimal Roy.

There were 75 submissions to INDOCRYPT 2002, out of which one was withdrawn and 31 were accepted. The invited talks were especially strong. Vincent Rijmen of AES fame gave a lecture on the design strategy for the recently accepted AES standard. Manindra Agrawal, Neeraj Kayal, and Nitin Saxena recently achieved a breakthrough by obtaining a polynomial time deterministic algorithm for primality testing. This was presented at an invited talk by the authors. GuoZhen Xiao, an eminent researcher in the theory of sequences and Boolean functions, presented a lecture on efficient algorithms for computing the linear complexity of sequences.

The reviewing process for INDOCRYPT was very stringent and the schedule was very tight. The program committee did an excellent job in reviewing the papers and selecting the final papers for presentation. These proceedings include the revised versions of the selected papers. Revisions were not checked and the authors bear the full responsibility for the contents of the respective papers.

Program committee members were assisted in the review process by external reviewers. The list of external reviewers is included in the proceedings. Our thanks go to all the program committee members and the external reviewers who put in their valuable time and effort in providing important feedback to the authors.

Organizing the conference involved many individuals. We would like to thank the general chairs V.P. Gulati and M. Vidyasagar for taking care of the actual

hosting of the conference. They were ably assisted by the organizing committee, whose names are included in the proceedings. Additionally, we would like to thank Kishan Chand Gupta, Sandeepan Chowdhury, Subhasis Pal, and Amiya Kumar Das for substantial help on different aspects of putting together this proceedings in its final form. Finally we would like to thank Springer-Verlag for active cooperation and timely production of the proceedings.

December 2002

Alfred Menezes
Palash Sarkar

INDOCRYPT 2002 was organized by the Institute for Development and Research in Banking Technology (IDRBT) and is an annual event of the Cryptology Research Society of India.

General Co-chairs

Ved Prakash Gulati
M. Vidyasagar

IDRBT, Hyderabad, India
Tata Consultancy Services, Hyderabad, India

Program Co-chairs

Alfred Menezes
Palash Sarkar

University of Waterloo, Canada
Indian Statistical Institute, India

Program Committee

Akshai Aggarwal	University of Windsor, Canada
Manindra Agrawal	Indian Institute of Technology, India
V. Arvind	Institute of Mathematical Sciences, India
Simon Blackburn	Royal Holloway, University of London, UK
Colin Boyd	Queensland University of Technology, Australia
ZongDuo Dai	Academia Sinica, China
Anand Desai	NTT MCL, USA
Ved Prakash Gulati	IDRBT, India
Anwar Hasan	University of Waterloo, Canada
Sushil Jajodia	George Mason University, USA
Charanjit Jutla	IBM, USA
Andrew Klapper	University of Kentucky, USA
Neal Koblitz	University of Washington, USA
Kaoru Kurosawa	Ibaraki University, Japan
Chae Hoon Lim	Sejong University, Korea
Subhamoy Maitra	Indian Statistical Institute, India
C.E. Veni Madhavan	Indian Institute of Science, India
Alfred Menezes	University of Waterloo, Canada
Rei Safavi-Naini	University of Wollongong, Australia
David Pointcheval	ENS Paris, France
Bart Preneel	Katholieke Universiteit Leuven, Belgium
A.K. Pujari	University of Hyderabad, India
Jaikumar Radhakrishnan	Tata Institute of Fundamental Research, India
Bimal Roy	Indian Statistical Institute, India
Palash Sarkar	Indian Statistical Institute, India
Vijay Varadharajan	Macquarie University, Australia
Stefan Wolf	University of Montreal, Canada
Chaoping Xing	National University of Singapore, Singapore
Amr Youssef	Cairo University, Egypt

Organizing Committee

S. Sankara Subramanian	IDRBT, India
Rajesh Nambiar	TCS, India
V. Visweswar	IDRBT, India
Ashutosh Saxena	IDRBT, India
V. Ravi Sankar	IDRBT, India
B. Kishore	TCS, India

External Referees

Kazumaro Aoki	Michael Jacobs	Selwyn Russell
Alexandra Boldyreva	Rahul Jain	Takeshi Shimoyama
Shiping Chen	Shaoquan Jiang	M.C. Shrivastava
Olivier Chevassut	Meena Kumari	Jason Smith
Sandeepan Choudhury	Yingjiu Li	Alain Tapp
Tanmoy K. Das	Sin'ichiro Matsuo	Ayineedi Venkateswarlu
Matthias Fitzi	Mridul Nandi	Lingyu Wang
Steven Galbraith	Laxmi Narain	Bogdan Warinschi
Sugata Gangopadhyaya	Satomi Okazaki	Yiqun Lisa Yin
Craig Gentry	Kapil Hari Paranjape	Sencun Zhu
Indivar Gupta	Rajesh Pillai	
Alejandro Hevia	Matt Robshaw	

Sponsoring Institutions

Acer India Pvt. Ltd., Bangalore
Cisco Systems India Pvt. Ltd., New Delhi
e-commerce magazine, New Delhi
HP India, New Delhi
IBM India Ltd., Bangalore
Infosys Technologies Ltd., Bangalore
Rainbow Information Technologies Pvt. Ltd. New Delhi
Society for Electronic Transactions and Security, New Delhi
Tata Consultancy Services, Mumbai

Table of Contents

Invited Talks

Security of a Wide Trail Design	1
<i>Joan Daemen and Vincent Rijmen</i>	
Fast Algorithms for Determining the Linear Complexity of Period Sequences	12
<i>Guozhen Xiao and Shimin Wei</i>	

Symmetric Ciphers

A New Class of Stream Ciphers Combining LFSR and FCSR Architectures	22
<i>François Arnault, Thierry P. Berger, and Abdelkader Nacer</i>	
Slide Attack on Spectr-H64	34
<i>Selçuk Kavut and Melek D. Yücel</i>	
On Differential Properties of Pseudo-Hadamard Transform and Related Mappings (Extended Abstract)	48
<i>Helger Lipmaa</i>	

New Public-Key Schemes

A Variant of NTRU with Non-invertible Polynomials	62
<i>William D. Banks and Igor E. Shparlinski</i>	
Tree Replacement and Public Key Cryptosystem	71
<i>S.C. Samuel, D.G. Thomas, P.J. Abisha, and K.G. Subramanian</i>	

Foundations

Never Trust Victor: An Alternative Resettable Zero-Knowledge Proof System	79
<i>Olaf Müller and Michael Nüsken</i>	
Asynchronous Unconditionally Secure Computation: An Efficiency Improvement	93
<i>B. Prabhu, K. Srinathan, and C. Pandu Rangan</i>	

Public-Key Infrastructures

- QPKI: A QoS-Based Architecture for Public-Key Infrastructure (PKI) 108
Ravi Mukkamala
- Towards Logically and Physically Secure Public-Key Infrastructures 122
Kapali Viswanathan and Ashutosh Saxena

Fingerprinting and Watermarking

- Cryptanalysis of Optimal Differential Energy Watermarking (DEW)
and a Modified Robust Scheme 135
Tanmoy Kanti Das and Subhamoy Maitra
- A 2-Secure Code with Efficient Tracing Algorithm 149
Vu Dong Tô, Reihaneh Safavi-Naini, and Yejing Wang
- Reed Solomon Codes for Digital Fingerprinting 163
Ravi Sankar Veerubhotla, Ashutosh Saxena, and Ved Prakash Gulati

Public-Key Protocols

- A Note on the Malleability of the El Gamal Cryptosystem 176
Douglas Wikström
- Authentication of Concast Communication 185
Mohamed Al-Ibrahim, Hossein Ghodosi, and Josef Pieprzyk
- Self-certified Signatures 199
Byoungcheon Lee and Kwangjo Kim
- Identity Based Authenticated Group Key Agreement Protocol 215
D. Nalla and K.C. Reddy

Boolean Functions

- Construction of Cryptographically Important Boolean Functions 234
Soumen Maity and Thomas Johansson
- Evolving Boolean Functions Satisfying Multiple Criteria 246
*John A. Clark, Jeremy L. Jacob, Susan Stepney, Subhamoy Maitra,
and William Millan*
- Further Results Related to Generalized Nonlinearity 260
Sugata Gangopadhyay and Subhamoy Maitra

Efficient and Secure Implementations

Modular Multiplication in $GF(p^k)$ Using Lagrange Representation	275
<i>Jean-Claude Bajard, Laurent Imbert, and Christophe Nègre</i>	
Speeding up the Scalar Multiplication in the Jacobians of Hyperelliptic Curves Using Frobenius Map	285
<i>YoungJu Choie and Jong Won Lee</i>	
Improved Elliptic Curve Multiplication Methods Resistant against Side Channel Attacks	296
<i>Tetsuya Izu, Bodo Möller, and Tsuyoshi Takagi</i>	

Applications

The Design and Implementation of Improved Secure Cookies Based on Certificate	314
<i>Jong-Phil Yang and Kyung-Hyune Rhee</i>	
A Certified E-mail System with Receiver's Selective Usage of Delivery Authority	326
<i>Kenji Imamoto and Kouichi Sakurai</i>	
Spending Offline Divisible Coins with Combining Capability	339
<i>Eikoh Chida, Yosuke Kasai, Masahiro Mambo, and Hiroki Shizuya</i>	
Efficient Object-Based Stream Authentication	354
<i>Yongdong Wu, Di Ma, and Changsheng Xu</i>	

Anonymity

The Security of a Mix-Center Based on a Semantically Secure Cryptosystem	368
<i>Douglas Wikström</i>	
New Identity Escrow Scheme for Anonymity Authentication	382
<i>Yong-Ho Lee, Im-Yeong Lee, and Hyung-Woo Lee</i>	

Secret Sharing and Oblivious Transfer

On Unconditionally Secure Distributed Oblivious Transfer	395
<i>Ventzislav Nikov, Svetla Nikova, Bart Preneel, and Joos Vandewalle</i>	
Non-perfect Secret Sharing over General Access Structures	409
<i>K. Srinathan, N. Tharani Rajan, and C. Pandu Rangan</i>	
On Distributed Key Distribution Centers and Unconditionally Secure Proactive Verifiable Secret Sharing Schemes Based on General Access Structure	422
<i>Ventzislav Nikov, Svetla Nikova, Bart Preneel, and Joos Vandewalle</i>	

Author Index	437
---------------------------	-----

Author Index

Abisha, P.J.	71	Nalla, Divya	215
Al-Ibrahim, Mohamed	185	Necer, Abdelkader	22
Arnault, François	22	Nègre, Christophe	275
Bajard, Jean-Claude	275	Nikov, Ventzislav	395, 422
Banks, William D.	62	Nikova, Svetla	395, 422
Berger, Thierry P.	22	Nüsken, Michael	79
Chida, Eikoh	339	Pieprzyk, Josef	185
Choie, YoungJu	285	Prabhu, B.	93
Clark, John A.	246	Preneel, Bart	395, 422
Daemen, Joan	1	Rajan, N. Tharani	409
Das, Tanmoy Kanti	135	Rangan, C. Pandu	93, 409
Gangopadhyay, Sugata	260	Reddy, K.C.	215
Ghodosi, Hossein	185	Rhee, Kyung-Hyune	314
Gulati, Ved Prakash	163	Rijmen, Vincent	1
Imamoto, Kenji	326	Safavi-Naini, Reihaneh	149
Imbert, Laurent	275	Sakurai, Kouichi	326
Izu, Tetsuya	296	Samuel, S.C.	71
Jacob, Jeremy L.	246	Saxena, Ashutosh	122, 163
Johansson, Thomas	234	Shizuya, Hiroki	339
Kasai, Yosuke	339	Shparlinski, Igor E.	62
Kavut, Selçuk	34	Srinathan, K.	93, 409
Kim, Kwangjo	199	Stepney, Susan	246
Lee, Byoungcheon	199	Subramanian, K.G.	71
Lee, Hyung-Woo	382	Takagi, Tsuyoshi	296
Lee, Im-Yeong	382	Thomas, D.G.	71
Lee, Jong Won	285	Tô, Vu Dong	149
Lee, Yong-Ho	382	Vandewalle, Joos	395, 422
Lipmaa, Helger	48	Veerubhotla, Ravi Sankar	163
Ma, Di	354	Viswanathan, Kapali	122
Maitra, Subhamoy ...	135, 246, 260	Wang, Yejing	149
Maity, Soumen	234	Wei, Shimin	12
Mambo, Masahiro	339	Wikström, Douglas	176, 368
Millan, William	246	Wu, Yongdong	354
Möller, Bodo	296	Xiao, Guozhen	12
Müller, Olaf	79	Xu, Changsheng	354
Mukkamala, Ravi	108	Yang, Jong-Phil	314
		Yücel, Melek D.	34

Progress in Cryptology - INDOCRYPT 2002

Third International Conference on Cryptology in India

Hyderabad, India, December 16-18, 2002

Menezes, A.; Sarkar, P. (Eds.)

2002, XII, 444 p., Softcover

ISBN: 978-3-540-00263-5