IEEE TRANSACTIONS ON

INFORMATION THEORY

A Journal Devoted to the Theoretical and Experimental Aspects of Information Transmission, Processing, and Utilization

JUNE 2008 VOLUME 54 NUMBER 6 IETTAW (ISSN 0018-9448)

SPECIAL ISSUE ON INFORMATION THEORETIC SECURITY

Introduction to the Special Issue on Information Theoretic Security

THIS special issue of the IEEE TRANSACTIONS ON INFORMATION THEORY is devoted to the exciting research field of Information Theoretic Security. Cryptographic systems that are currently employed in practice are predominantly based on unproven mathematical assumptions such as the assumed infeasibility of factoring large integers and finding discrete logarithms over large finite fields. Advances in cryptoanalytic attack algorithms and new computing technologies such as quantum computers may eventually render these systems insecure and, thus, obsolete in the future. As such, among both information security researchers and practitioners there has long been a sense of urgency to investigate novel encryption and authentication systems that do not rely on unproven mathematical assumptions for their security. The past two decades have witnessed a number of significant developments in information theoretic security, including the discovery of unconditionally secure encryption schemes, authentication codes and signature methods, and the development of quantum key distribution protocols.

Research papers that have been selected for inclusion in this special issue cover a broad range of important topics in information theoretic security, including

- authentication,
- broadcast security,
- channel capacity,
- key agreement,
- two and multiparty computation,
- network coding,
- quantum cryptography,
- secret sharing,
- steganography,
- wire-tap channels,
- complexity of non-number-theoretic problems, and
- anonymity.

Two papers address bounds for unconditionally secure authentication codes. In addition to the more traditional model for authentication, where a sender and a receiver share a short secret key, the paper by Naor, Segev, and Smith examines also a model where the sender and the receiver are connected by a low-bandwidth auxiliary channel that allows the sender to "manually" authenticate a short message to the receiver. The paper by Safavi-Naini and Wild considers a strong attack scenario where an adversary is adaptive and has access to authentication and verification oracles.

Five papers investigate security issues related to broadcast channels. Csiszár and Narayan find new bounds for secrecy capacities of channels with one input terminal, multiple-output terminals, and a public noiseless channel of unlimited capacity. Khisti, Tchamkerten, and Wornell study parallel broadcast channels with one sender, multiple intended receivers, and one eavesdropper. This is followed by Liang, Poor, and Shamai who investigate fading broadcast channels with confidential messages. Liu, Marić, Spasojević, and Yates study secrecy capacity regions for discrete memoryless interference and broadcast channels with independent confidential messages. Finally, Stinson and Zaverucha investigate new bounds for secure frameproof codes that find applications in secure broadcasting.

Two papers fall into the area of secure key agreement. Continuing their earlier work on confidential communication over wireless channels, Bloch, Barros, Rodrigues, and McLaughlin develop practical secret key agreement protocols over Gaussian and quasi-static fading wiretap channels. Yakovlev, Korzhik, and Morales-Luna present new ideas for key distribution protocols over noisy wiretap channels that offer information theoretic security in the presence of an active adversary.

Four papers are concerned with secure multiparty computation. Kosut and Tong investigate a problem in distributed source coding where an unknown number of sensors can be controlled by a malicious intruder. Their work is followed by two papers, one by Kurosawa, Kishimoto, and Koshiba and the other by Nascimento and Winter, both of which investigate information theoretically secure oblivious transfer protocols. Wang and Desmedt study message transmission in a reliable and privacy-preserving manner over a network that can be modeled by a directed graph.

Network coding is an emerging area of importance. The paper by Jaggi, Langberg, Katti, Ho, Katabi, Medard, and Effros addresses security issues with network coding. Specifically, the authors design polynomial-time, rate-optimal network codes that work in the presence of Byzantine nodes.

Two papers are directly related to quantum cryptography. The paper by Horodecki, Horodecki, Horodecki, Leung, and Oppenheim provides proofs for the unconditional security of a quantum key distribution protocol that is based on distilling pbits, whereas the other paper by Horodecki, Pankowski, Horodecki, and Horodecki investigates bound entangled states that have a positive distillable secure key rate.

Three papers examine secret sharing. Beimel and Livne study new secret sharing schemes based on matroids. Cramer, Daza, Gracia, Leander, and Padro reveal connections between codes, matroids, and multiplicative linear secret sharing schemes. Koga employs information-spectrum methods to investigate threshold schemes.

Three papers are devoted to steganography. Anthapadmanabhan, Barg, and Dumer show how to achieve the maximum attainable rate of fingerprinting codes under the marking assumption. Shikata and Matsumoto propose models for unconditionally secure stegosystems against active attacks over an insecure channel. Wang and Moulin show bounds and constructions for perfectly secure steganography.

Digital Object Identifier 10.1109/TIT.2008.921909

Two papers address the classical wiretap channels. Merhav considers a wiretap channel where a wiretapper is allowed to have access to both coded information and side information via channels that are more noisy than the respective channels of between a sender and a legitimate decoder. Tekin and Yener investigate the General Gaussian Multiple Access Wire-Tap Channel (GGMAC-WT) and the Gaussian Two-Way Wire-Tap Channel (GTW-WT) which are common in multiuser wireless communications.

The paper by Kiayias and Yung study the hardness of the Reed–Solomon codes when applied in cryptography. This is followed by a paper by Venkitasubramaniam, He, and Tong where anonymous communication in a wireless environment is investigated.

We have six correspondences addressing different aspects of information theoretic security. Nascimento, Barros, Skludarek, and Imai show that the commitment capacity of the Gaussian channel is infinite. Dziembowski and Maurer prove a tight lower bound on storage for key agreement in the bounded-storage model. Wolf and Wullschleger introduce various monotones and use them to derive lower bounds in multiparty computations. Ho, Leong, Koetter, Medard, and Effros propose an information theoretic approach for detecting Byzantine modifications in networks employing random linear network coding. Zhao, Gui, Chen, Han, and Guo study the hardness of key distillation for reverse reconciliation continuous variable quantum key distribution. Finally, Hayashi and Yamamoto show new coding theorems for the Shannon cipher.

ACKNOWLEDGMENT

We would like to thank all the authors, including those whose papers were not selected for publication in this special issue, for their contributions to the research field. During the prolonged period of reviewing, we sought help from numerous expert reviewers for their scientific opinions on submissions to the special issues. Without their assistance it would not have been possible to select the final list of papers for publication from the large number of high-quality submissions. We would also like to thank H. Vincent Poor, the past Editor-in-Chief for IEEE TRANSACTIONS ON INFORMATION THEORY, and Ezio Biglieri, the current Editor-in-Chief for their support for this special issue. Thanks also go to Yukiko Ito for her tireless assistance during the editing process.

HIDEKI IMAI, *Guest Editor-in-Chief*
Faculty of Science and Engineering
Chuo University
Kasuga, Bunkyo-ku,
Tokyo, 112-8551 Japan
Research Center for Information Security (RCIS)
National Institute of Advanced Industrial
Science and Technology (AIST)
Sotokanda, Chiyoda-ku,
Tokyo, 101-0021, Japan,

GOICHIRO HANAOKA, *Guest Editor*
RCIS, AIST
Sotokanda, Chiyoda-ku,
Tokyo, 101-0021 Japan

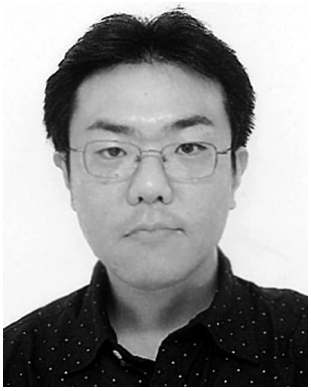
UELI MAURER, *Guest Editor*
Department of Computer Science
ETH Zurich
CH-8092 Zurich, Switzerland

YULIANG ZHENG, *Guest Editor*
Department of Software and Information Systems
University of North Carolina
Charlotte, NC 28223 USA

Hideki Imai (M'74–SM'88–F'92) received the B.E., M.E., and Ph.D. degrees in electrical engineering from the University of Tokyo in 1966, 1968, and 1971, respectively.

From 1971 to 1992, he was on the faculty of Yokohama National University, Yokohama, Japan. From 1992 to 2006, he was a Professor in the Institute of Industrial Science, the University of Tokyo. In 2006, he was appointed as an Emeritus Professor of the University of Tokyo and a Professor of Chuo University. Concurrently, he serves as the Director of Research Center for Information Security, National Institute of Advanced Industrial Science and Technology. His current research interests include information theory, coding theory, cryptography, and information security.

From IEICE (the Institute of Electronics, Information and Communication Engineers), Dr. Imai received Best Book Awards in 1976 and 1991, Best Paper Awards in 1992, 2003, and 2004, the Yonezawa Memorial Paper Award in 1992, the Achievement Award in 1995, the Inose Award in 2003, and the Distinguished Achievement and Contributions Award in 2004. He also received a Golden Jubilee Paper Award from the IEEE Information Theory Society in 1998, and Official Commendations from the Minster of Internal Affairs and Communications in June 2002 and from the Minister of Economy, Trade and Industry in October 2002. He was awarded Honor Doctor degree by Soonchunhyang University, Korea, in 1999 and Docteur Honoris Causa degree by the University of Toulon Var, France, in 2002. He is also the recipient of the Ericsson Telecommunications Award in 2005. He was awarded Wilkes Award from the British Computer Society in 2007. He is a member of the Science Council of Japan. He was elected a Fellow of IEEE, IEICE, and IACR (International Association for Cryptologic Research) in 1992, 2001, and 2007, respectively. He has chaired many committees of scientific societies and organized a number of international conferences. He served as the President of the Society of Information Theory and its Applications in 1997, of the IEICE Engineering Sciences Society in 1998, and of the IEEE Information Theory Society in 2004. He is currently the Chair of CRYPTREC (Cryptography Techniques Research and Evaluation Committee of Japan).



Goichiro Hanaoka received the bachelor's degree in electronic engineering from the University of Tokyo, Tokyo, Japan, in 1997 and the masters and Ph.D. degrees in information and communication engineering from the University of Tokyo in 1999 and 2002, respectively.

From 2002 to 2005, he was a Research Fellow of the Japan Society for the Promotion of Science (JSPS). Since 2005, he has been with the National Institute of Advanced Industrial Science and Technology, Japan. He has coauthored more than 60 international conference and journal papers.

Dr. Hanaoka served as a member of program committee for many international conferences, such as ICISC'07, Pairing'07, SPRE-WWW'07, CT-RSA'07, Inscrypt'07, I CISC'06, ACISP'06, ICISC'05, ANCS'05, ICICS'04, ACISP'04, ACNS'04, PKC'04, CT-RSA'04. He received the Wilkes Award from the British Computer Society in 2007, the Best Paper Award of SCIS from IEICE in 2006, the TELECOM System Technology Award in 2004, the 20th Anniversary Prize of ISEC SCIS in 2003, and the Best Paper Award from SITA in 2000.

Ueli Maurer (S'85–M'90–SM'94–F'03) was born in St. Gallen, Switzerland, in 1960. He graduated in electrical engineering (1985) and received the Ph.D. degree in technical sciences (1990), both from the Swiss Federal Institute of Technology Zurich (ETH), Switzerland.

From 1990 to 1991, he was a DIMACS Research Fellow in the Department of Computer Science at Princeton University, Princeton, NJ, and in 1992, he joined the Computer Science Department at ETH Zurich. There he is a Professor of Computer Science and Head of the Information Security and Cryptography Research Group. His research interests include information security, the theory and applications of cryptography, information theory, theoretical computer science, and discrete mathematics. He holds several patents for cryptographic systems and has served as a consultant for many companies and government organizations. He serves on a few management and scientific advisory boards and is cofounder of Visonys, a Zurich-based security software company.

Prof.Maurer has served extensively as an Editor, including as Associate Editor of the IEEE TRANSACTIONS ON INFORMATION THEORY, and as a member of program committees. Currently he is the Editor-in-Chief of the *Journal of Cryptology*, Editor-in-Chief of Springer Verlag's book series in Information Security and Cryptography, and serves on the Board of Directors of the International Association for Cryptologic Research (IACR).

Yuliang Zheng (S'87–M'91–SM'98) received the B.Sc. degree in computer science from Nanjing Institute of Technology, Nanjing, China, in 1982 and the M.E. and Ph.D. degrees, both in electrical and computer engineering, from Yokohama National University, Yokohama, Japan, in 1988 and 1991 respectively.

From 1982 to 1984, he was with the Guangzhou Institute for Communication Research, Guangzhou (Canton), China. From 1991 to 2001, he was on the faculty of Australian Defence Force Academy, University of Wollongong and Monash University, all in Australia. Currently he is a Full Professor of Information Technology, and serves as the founding Director of the Information Security and Assurance Center, University of North Carolina, Charlotte. He is the designer of HAVAL, the first one-way hash algorithm family that provides the flexibility for users to choose appropriate member algorithms for specific applications. He is widely known as the inventor of the signcryption public key cryptographic algorithm. His research interests include cryptography, network security, and their applications in real world systems. He has consulted widely for industries and government agencies at all levels on cyber security and privacy issues, is the cofounder of Calyptix Security Corporation.

Dr. Zheng is a member of IACR and ACM. He has chaired a number of international conferences and is a cofounder of the PKC international conference series dedicated to the practice and theory in public key cryptography. Currently, he serves as an Associate Editor of *The Computer Journal* published by the Oxford University Press and the British Computer Society.

IEEE INFORMATION THEORY SOCIETY

IEEE TRANSACTIONS ON INFORMATION THEORY (ISSN 0018-9448) is published monthly by The Institute of Electrical and Electronics Engineers, Inc. Responsibility for the contents rests upon the authors and not upon the IEEE, the Society/Council, or its members. **IEEE Corporate Office**: 3 Park Avenue, 17th floor, New York, NY 10016-5997. **IEEE Operations Center**: 445 Hoes Lane, Piscataway, NJ 08854-4141. **NJ Telephone**: +1 732 981 0060. **Price/Publication Information**: Individual copies: IEEE Members $20.00 (first copy only), nonmembers $76.00 per copy. (Note: Postage and handling charge not included.) Member and nonmember subscription prices available upon request. Available in microfiche and microfilm. **Copyright and Reprint Permissions**: Abstracting is permitted with credit to the source. Libraries are permitted to photocopy for private use of patrons, provided the per-copy fee indicated in the code at the bottom of the first page is paid through the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923. For all other copying, reprint, or republication permission, write to Copyrights and Permissions Department, IEEE Publications Administration, 445 Hoes Lane, Piscataway, NJ 08854-4141. Periodicals Postage Paid at New York, NY and at additional mailing offices. **Postmaster**: Send address changes to IEEE TRANSACTIONS ON INFORMATION THEORY, IEEE, 445 Hoes Lane, Piscataway, NJ 08854-4141. GST Registration No. 125634188. CPC Sales Agreement #40013087. Return undeliverable Canada addresses to: Pitney Bowes IMEX, P.O. Box 4332, Stanton Rd., Toronto, ON M5W 3J4, Canada. Printed in U.S.A.

Digital Object Identifier 10.1109/TIT.2008.925832