Kil-Hyun Nam
Gwangsoo Rhee (Eds.)

LNCS 4817

# Information Security and Cryptology – ICISC 2007

**10th International Conference**
**Seoul, Korea, November 2007**
**Proceedings**

Springer

Kil-Hyun Nam Gwangsoo Rhee (Eds.)

# Information Security and Cryptology – ICISC 2007

10th International Conference
Seoul, Korea, November 29-30, 2007
Proceedings

Springer

Volume Editors

Kil-Hyun Nam
National Defense University
122-875 Susaek-dong, Eunpyung-gu, Seoul 122-875, Korea
E-mail: khnam@kndu.ac.kr

Gwangsoo Rhee
Sookmyung Women's University
52 Hyochangwon-gil, Yongsan-Ku, Seoul 140-742, Korea
E-mail: rhee@sookmyung.ac.kr

Library of Congress Control Number: 2007939824

CR Subject Classification (1998): E.3, G.2.1, D.4.6, K.6.5, F.2.1, C.2, J.1

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-76787-8 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-76787-9 Springer Berlin Heidelberg New York



Springer is a part of Springer Science+Business Media

springer.com


Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12192021 06/3180 5 4 3 2 1 0

# Preface

ICISC 2007, the Tenth International Conference on Information Security and Cryptology, was held in Seoul, Korea, during November 29–30, 2007. It was organized by the Korea Institute of Information Security and Cryptology (KIISC) in cooperation with the Ministry of Information and Communication (MIC), Korea. The aim of this conference was to provide a forum for the presentation of new results in research, development, and applications in the field of information security and cryptology. It also intended to be a place where research information can be exchanged.

The conference received 123 submissions from 24 countries, covering all areas of information security and cryptology. The review and selection processes were carried out in two stages by the Program Committee (PC) of 57 prominent researchers via online meetings through the iChair Web server. First, each paper was blind reviewed by at least three PC members, and papers co-authored by the PC members were reviewed by at least five PC members. Second, individual review reports were revealed to PC members, and detailed interactive discussion on each paper followed. Through this process the PC finally selected 28 papers from 14 countries. The authors of selected papers had a few weeks to prepare final versions of their papers, aided by comments from the reviewers. The proceedings contained the revised versions of the accepted papers. However, most of these final revisions were not subject to any further editorial review.

The conference program included two invited talks from eminent researchers in information security and cryptology. The invited speakers were Daniel J. Bernstein from University of Illinois at Chicago and Mitsuru Matsui from Mitsubishi Electric Corporation.

We would like to thank everyone who contributed to the success of this conference. First, thanks to all the authors who submitted papers to this conference. Second, thanks to all 57 members of the PC listed overleaf. It was a truly nice experience to work with such talented and hard-working researchers. Third, thanks to all the external reviewers for assisting the PC in their particular areas of expertise. Fourth, we would like to thank all the participants of the conference who made this event an intellectually stimulating one through their active contribution. We would also like to thank the iChair developers in EPFL for allowing us to use their software. Finally, we are delighted to acknowledge the partial financial support provided by CIST, KISIA, NICS Tech, NITGEN, STG Security, and TSonNet.

November 2007

Kil-Huyn Nam
Gwangsoo Rhee

# ICISC 2007

The 10th International Conference on
Information Security and Cryptology

November 29–30, 2007
Olympic Parktel, Seoul, Korea

*Organized by*
Korea Institute of Information Security and Cryptology (KIISC)
(http://www.kiisc.or.kr)

*In cooperation with*
Ministry of Information and Communication (MIC), Korea
(http://www.mic.go.kr)

## Organization

### General Chair

| | |
|---|---|
| Min Surp Rhee | Dankook University, Korea |

### Program Co-chairs

| | |
|---|---|
| Kil-Hyun Nam | National Defense University, Korea |
| Gwangsoo Rhee | Sookmyung Women's University, Korea |

### Program Committee

| | |
|---|---|
| Michel Abdalla | ENS and CNRS, France |
| Joonsang Baek | Institute for Infocomm Research, Singapore |
| Alex Biryukov | University of Luxembourg, Luxembourg |
| Bill Caelli | Queensland University of Technology, Australia |
| Kyo-il Chung | ETRI, Korea |
| Jean-Sebastien Coron | University of Luxembourg, Luxembourg |
| Frederic Cuppens | ENST Bretagne, France |
| Ed Dawson | Queensland University of Technology, Australia |
| Bart De Decker | Katholieke Universiteit Leuven, Belgium |
| Orr Dunkelman | Katholieke Universiteit Leuven, Belgium |
| Eduardo B. Fernandez | Florida Atlantic University, USA |
| Pierre-Alain Fouque | Ecole Normale Superieure, France |
| Mario Marques Freire | University of Beira Interior, Portugal |
| Marc Girault | Orange Labs, France |

| | |
|---|---|
| Philippe Golle | Palo Alto Research Center, USA |
| Dieter Gollmann | Hamburg University of Technology, Germany |
| Goichiro Hanaoka | AIST, Japan |
| Hiroaki Kikuchi | Tokai University, Japan |
| Kwangjo Kim | ICU, Korea |
| Christopher Kruegel | Technical University Vienna, Austria |
| Chi Sung Laih | National Cheng Kung University, Taiwan |
| Kwok-Yan Lam | Tsinghua University, China |
| Kristin E. Lauter | Microsoft Research, USA |
| Dong Hoon Lee | Korea University, Korea |
| Pil Joong Lee | POSTECH, Korea |
| Arjen K. Lenstra | EPFL, Switzerland |
| Yingjiu Li | Singapore Management University, Singapore |
| Javier Lopez | University of Malaga, Spain |
| Masahiro Mambo | University of Tsukuba, Japan |
| Mark Manulis | Ruhr University of Bochum, Germany |
| Keith Martin | Royal Holloway, University of London, UK |
| Mitsuru Matsui | Mitsubishi Electric Corporation, Japan |
| Atsuko Miyaji | JAIST, Japan |
| SangJae Moon | Kyungpook National University, Korea |
| Yi Mu | University of Wollongong, Australia |
| Jesper Buus Nielsen | University of Aarhus, Denmark |
| DaeHun Nyang | Inha University, Korea |
| Rolf Oppliger | eSECURITY Technologies, Switzerland |
| D'Arco Paolo | University of Salerno, Italy |
| Kunsoo Park | Seoul National University, Korea |
| Sangwoo Park | National Security Research Institute, Korea |
| Raphael Chung-Wei Phan | EPFL, Switzerland |
| Rei Safavi-Naini | University of Calgary, Canada |
| Kouichi Sakurai | Kyushu University, Japan |
| Palash Sarkar | Indian Statistical Institute, India |
| Dongkyoo Shin | Sejong University, Korea |
| Willy Susilo | University of Wollongong, Australia |
| Tsuyoshi Takagi | Future University, Hakodate, Japan |
| Jozef Vyskoc | VaF s.r.o., Slovakia |
| Guilin Wang | Institute for Infocomm Research, Singapore |
| Dongho Won | Sungkyunkwan University, Korea |
| Sung-Ming Yen | National Central University, Taiwan, ROC |
| Yongjin Yeom | National Security Research Institute, Korea |
| Fangguo Zhang | Sun Yat-sen University, China |
| Alf Zugenmaier | DoCoMo Euro-Labs, Germany |

## Organizing Chair

| | |
|---|---|
| Dong-gue Park | Soonchunhyang University, Korea |

## Organizing Committee

| | |
|---|---|
| Hoon Ko | Information and Communications University(ICU), Korea |
| DaeHun Nyang | Inha University, Korea |
| Jintae Oh | Electronics and Telecommunications Research Institute(ETRI), Korea |
| Kangbin Yim | Soonchunhyang University, Korea |
| Joongcheol Moon | National Security Research Institute(NSRI), Korea |
| Changho Seo | Kongju National University, Korea |
| Jaesung Kim | Korea Information Security Agency(KISA), Korea |
| Sangjin Kim | Korea University of Technology and Education, Korea |
| Sehyun Park | Chung-Ang University, Korea |

## External Reviewers

Imad Aad
Sultan Zayid Al-Hinai
Man Ho Au
Jean-Philippe Aumasson
Vicente Benjumea
Jean-Luc Beuchat
Annalisa De Bonis
Reinier Broker
Sebastien Canard
Ku-Young Chang
Ee-Chien Chang
Jiun-Ming Chen
Chien-Ning Chen
Wang Chih-Hung
S.Y. Chiou
Kuo-Zhe Chiou
Dickson K.W. Chiu
Yong-je Choi
Celine Coma
Nora Cuppens
Rennie deGraff
Holger Dreger
Dang Nguyen Duc
Chun-I Fan
Gerardo Fernandez
Umberto Ferraro
Ernest Foo
Georg Fuchsbauer
Soichi Furuya
D.J. Guan
JaeCheol Ha
Keisuke Hakuta
Kyusuk Han
Dong-Guk Han
Chao-Chih Hsu
Xinyi Huang
Sebastiaan Indesteege
Toshiyuki Isshiki
Tetsu Iwata
Tetsuya Izu
Ik Rae Jeong
Dimitar Jetchev
Shaoquan Jiang
Marcelo Kaihara
Nathan Keller
Dmitry Khovratovich
Jin Ho Kim
Shinsaku Kiyomoto
Hiroki Koga
Yuichi Komano
Divyan M. Konidala
Noboru Kunihiro
Wen-Chung Kuo
Eun Jeong Kwon
Yunho Lee
HoonJae Lee
Tieyan Li
Wanqing Li
Vo Duc Liem
Wei-Chih Lien
Hsi-Chung Lin
Breno de Medeiros
Anton Mityagin
Peter Montgomery
Daesung Moon
Yusuke Naito
Toshiya Nakajima
Cedric Ng
Mototsugu Nishioka
Masao Nonaka
Katsuyuki Okeya
Dag Arne Osvik
Ranjan Pal
Tae Jun Park
Maura Paterson
Kun Peng
Geong Sen Poh
Deike Priemuth-Schmid

Roberto De Prisco
Havard Raddum
Matthieu Rivain
Rodrigo Roman
Chun Ruan
Akashi Satoh
Sven Schaege
Scarlet Schwiderski-Grosche
Jae Woo Seo
Siamak F. Shahandashti
Ning Shang
Jong Hoon Shin
Masaaki Shirase
Leonie Simpson
Claudio Soriente
Chunhua Su
Hongwei Sun
Kenichi Takahashi
Terry Lam Vinh The
Julien Thomas
Jacques Traore
Jheng-Hong Tu
Yoshifumi Ueshige
Masashi Une
Ivan Visconti
Camille Vuillaume
Shuhong Wang
Baodian Wei
Christopher Wolf
Bo-Ching Wu
Yeon-Hyeong Yang
Bo-Yin Yang
Shenglin Yang
Fan Zhang
Chang-An Zhao
Xingwen Zhao
Sebastien Zimmer

## Sponsoring Institutions

| | |
|---|---|
| CIST, Korea | http://cist.korea.co.kr/ |
| KISIA, Korea | http://www.kisia.or.kr/ |
| NICS Tech, Korea | http://www.nicstech.com/ |
| NITGEN, Korea | http://www.nitgen.com/ |
| STG Security, Korea | http://www.stgsecurity.com/ |
| TSonNet, Korea | http://www.tsonnet.co.kr/ |

# Lecture Notes in Computer Science

Sublibrary 4: Security and Cryptology

Vol. 4856: F. Bao, S. Ling, T. Okamoto, H. Wang, C. Xing (Eds.), Cryptology and Network Security. XII, 283 pages. 2007.

Vol. 4833: K. Kurosawa (Ed.), Advances in Cryptology – ASIACRYPT 2007. XIV, 583 pages. 2007.

Vol. 4817: K.-H. Nam, G. Rhee (Eds.), Information Security and Cryptology - ICISC 2007. XIII, 367 pages. 2007.

Vol. 4784: W. Susilo, J.K. Liu, Y. Mu (Eds.), Provable Security. X, 237 pages. 2007.

Vol. 4779: J.A. Garay, A.K. Lenstra, M. Mambo, R. Peralta (Eds.), Information Security. XIII, 437 pages. 2007.

Vol. 4776: N. Borisov, P. Golle (Eds.), Privacy Enhancing Technologies. X, 273 pages. 2007.

Vol. 4752: A. Miyaji, H. Kikuchi, K. Rannenberg (Eds.), Advances in Information and Computer Security. XIII, 460 pages. 2007.

Vol. 4734: J. Biskup, J. López (Eds.), Computer Security – ESORICS 2007. XIV, 628 pages. 2007.

Vol. 4727: P. Paillier, I. Verbauwhede (Eds.), Cryptographic Hardware and Embedded Systems - CHES 2007. XIV, 468 pages. 2007.

Vol. 4691: T. Dimitrakos, F. Martinelli, P.Y.A. Ryan, S. Schneider (Eds.), Formal Aspects in Security and Trust. VIII, 285 pages. 2007.

Vol. 4677: A. Aldini, R. Gorrieri (Eds.), Foundations of Security Analysis and Design IV. VII, 325 pages. 2007.

Vol. 4657: C. Lambrinoudakis, G. Pernul, A.M. Tjoa (Eds.), Trust, Privacy and Security in Digital Business. XIII, 291 pages. 2007.

Vol. 4637: C. Kruegel, R. Lippmann, A. Clark (Eds.), Recent Advances in Intrusion Detection. XII, 337 pages. 2007.

Vol. 4622: A. Menezes (Ed.), Advances in Cryptology - CRYPTO 2007. XIV, 631 pages. 2007.

Vol. 4593: A. Biryukov (Ed.), Fast Software Encryption. XI, 467 pages. 2007.

Vol. 4586: J. Pieprzyk, H. Ghodosi, E. Dawson (Eds.), Information Security and Privacy. XIV, 476 pages. 2007.

Vol. 4582: J. López, P. Samarati, J.L. Ferrer (Eds.), Public Key Infrastructure. XI, 375 pages. 2007.

Vol. 4579: B.M. Hämmerli, R. Sommer (Eds.), Detection of Intrusions and Malware, and Vulnerability Assessment. X, 251 pages. 2007.

Vol. 4575: T. Takagi, T. Okamoto, E. Okamoto, T. Okamoto (Eds.), Pairing-Based Cryptography – Pairing 2007. XI, 408 pages. 2007.

Vol. 4521: J. Katz, M. Yung (Eds.), Applied Cryptography and Network Security. XIII, 498 pages. 2007.

Vol. 4515: M. Naor (Ed.), Advances in Cryptology - EUROCRYPT 2007. XIII, 591 pages. 2007.

Vol. 4499: Y.Q. Shi (Ed.), Transactions on Data Hiding and Multimedia Security II. IX, 117 pages. 2007.

Vol. 4464: E. Dawson, D.S. Wong (Eds.), Information Security Practice and Experience. XIII, 361 pages. 2007.

Vol. 4462: D. Sauveron, K. Markantonakis, A. Bilas, J.-J. Quisquater (Eds.), Information Security Theory and Practices. XII, 255 pages. 2007.

Vol. 4450: T. Okamoto, X. Wang (Eds.), Public Key Cryptography – PKC 2007. XIII, 491 pages. 2007.

Vol. 4437: J.L. Camenisch, C.S. Collberg, N.F. Johnson, P. Sallee (Eds.), Information Hiding. VIII, 389 pages. 2007.

Vol. 4392: S.P. Vadhan (Ed.), Theory of Cryptography. XI, 595 pages. 2007.

Vol. 4377: M. Abe (Ed.), Topics in Cryptology – CT-RSA 2007. XI, 403 pages. 2006.

Vol. 4356: E. Biham, A.M. Youssef (Eds.), Selected Areas in Cryptography. XI, 395 pages. 2007.

Vol. 4341: P.Q. Nguyên (Ed.), Progress in Cryptology - VIETCRYPT 2006. XI, 385 pages. 2006.

Vol. 4332: A. Bagchi, V. Atluri (Eds.), Information Systems Security. XV, 382 pages. 2006.

Vol. 4329: R. Barua, T. Lange (Eds.), Progress in Cryptology - INDOCRYPT 2006. X, 454 pages. 2006.

Vol. 4318: H. Lipmaa, M. Yung, D. Lin (Eds.), Information Security and Cryptology. XI, 305 pages. 2006.

Vol. 4307: P. Ning, S. Qing, N. Li (Eds.), Information and Communications Security. XIV, 558 pages. 2006.

Vol. 4301: D. Pointcheval, Y. Mu, K. Chen (Eds.), Cryptology and Network Security. XIII, 381 pages. 2006.

Vol. 4300: Y.Q. Shi (Ed.), Transactions on Data Hiding and Multimedia Security I. IX, 139 pages. 2006.

Vol. 4298: J.K. Lee, O. Yi, M. Yung (Eds.), Information Security Applications. XIV, 406 pages. 2007.

Vol. 4296: M.S. Rhee, B. Lee (Eds.), Information Security and Cryptology – ICISC 2006. XIII, 358 pages. 2006.

Vol. 4284: X. Lai, K. Chen (Eds.), Advances in Cryptology – ASIACRYPT 2006. XIV, 468 pages. 2006.

Vol. 4283: Y.Q. Shi, B. Jeon (Eds.), Digital Watermarking. XII, 474 pages. 2006.

Vol. 4266: H. Yoshiura, K. Sakurai, K. Rannenberg, Y. Murayama, S.-i. Kawamura (Eds.), Advances in Information and Computer Security. XIII, 438 pages. 2006.

Vol. 4258: G. Danezis, P. Golle (Eds.), Privacy Enhancing Technologies. VIII, 431 pages. 2006.

Vol. 4249: L. Goubin, M. Matsui (Eds.), Cryptographic Hardware and Embedded Systems - CHES 2006. XII, 462 pages. 2006.

Vol. 4237: H. Leitold, E.P. Markatos (Eds.), Communications and Multimedia Security. XII, 253 pages. 2006.

Vol. 4236: L. Breveglieri, I. Koren, D. Naccache, J.-P. Seifert (Eds.), Fault Diagnosis and Tolerance in Cryptography. XIII, 253 pages. 2006.

Vol. 4219: D. Zamboni, C. Krügel (Eds.), Recent Advances in Intrusion Detection. XII, 331 pages. 2006.

Vol. 4189: D. Gollmann, J. Meier, A. Sabelfeld (Eds.), Computer Security – ESORICS 2006. XI, 548 pages. 2006.

Vol. 4176: S.K. Katsikas, J. López, M. Backes, S. Gritzalis, B. Preneel (Eds.), Information Security. XIV, 548 pages. 2006.

Vol. 4117: C. Dwork (Ed.), Advances in Cryptology - CRYPTO 2006. XIII, 621 pages. 2006.

Vol. 4116: R. De Prisco, M. Yung (Eds.), Security and Cryptography for Networks. XI, 366 pages. 2006.

Vol. 4107: G. Di Crescenzo, A. Rubin (Eds.), Financial Cryptography and Data Security. XI, 327 pages. 2006.

Vol. 4083: S. Fischer-Hübner, S. Furnell, C. Lambrinoudakis (Eds.), Trust and Privacy in Digital Business. XIII, 243 pages. 2006.

Vol. 4064: R. Büschkes, P. Laskov (Eds.), Detection of Intrusions and Malware & Vulnerability Assessment. X, 195 pages. 2006.

Vol. 4058: L.M. Batten, R. Safavi-Naini (Eds.), Information Security and Privacy. XII, 446 pages. 2006.

Vol. 4047: M.J.B. Robshaw (Ed.), Fast Software Encryption. XI, 434 pages. 2006.

Vol. 4043: A.S. Atzeni, A. Lioy (Eds.), Public Key Infrastructure. XI, 261 pages. 2006.

Vol. 4004: S. Vaudenay (Ed.), Advances in Cryptology - EUROCRYPT 2006. XIV, 613 pages. 2006.

Vol. 3995: G. Müller (Ed.), Emerging Trends in Information and Communication Security. XX, 524 pages. 2006.

Vol. 3989: J. Zhou, M. Yung, F. Bao (Eds.), Applied Cryptography and Network Security. XIV, 488 pages. 2006.

Vol. 3969: Ø. Ytrehus (Ed.), Coding and Cryptography. XI, 443 pages. 2006.

Vol. 3958: M. Yung, Y. Dodis, A. Kiayias, T.G. Malkin (Eds.), Public Key Cryptography - PKC 2006. XIV, 543 pages. 2006.

Vol. 3957: B. Christianson, B. Crispo, J.A. Malcolm, M. Roe (Eds.), Security Protocols. IX, 325 pages. 2006.

Vol. 3956: G. Barthe, B. Grégoire, M. Huisman, J.-L. Lanet (Eds.), Construction and Analysis of Safe, Secure, and Interoperable Smart Devices. IX, 175 pages. 2006.

Vol. 3935: D.H. Won, S. Kim (Eds.), Information Security and Cryptology - ICISC 2005. XIV, 458 pages. 2006.

Vol. 3934: J.A. Clark, R.F. Paige, F.A.C. Polack, P.J. Brooke (Eds.), Security in Pervasive Computing. X, 243 pages. 2006.

Vol. 3928: J. Domingo-Ferrer, J. Posegga, D. Schreckling (Eds.), Smart Card Research and Advanced Applications. XI, 359 pages. 2006.

Vol. 3919: R. Safavi-Naini, M. Yung (Eds.), Digital Rights Management. XI, 357 pages. 2006.

Vol. 3903: K. Chen, R. Deng, X. Lai, J. Zhou (Eds.), Information Security Practice and Experience. XIV, 392 pages. 2006.

Vol. 3897: B. Preneel, S. Tavares (Eds.), Selected Areas in Cryptography. XI, 371 pages. 2006.

Vol. 3876: S. Halevi, T. Rabin (Eds.), Theory of Cryptography. XI, 617 pages. 2006.

Vol. 3866: T. Dimitrakos, F. Martinelli, P.Y.A. Ryan, S. Schneider (Eds.), Formal Aspects in Security and Trust. X, 259 pages. 2006.

Vol. 3860: D. Pointcheval (Ed.), Topics in Cryptology – CT-RSA 2006. XI, 365 pages. 2006.

Vol. 3858: A. Valdes, D. Zamboni (Eds.), Recent Advances in Intrusion Detection. X, 351 pages. 2006.

Vol. 3856: G. Danezis, D. Martin (Eds.), Privacy Enhancing Technologies. VIII, 273 pages. 2006.

Vol. 3786: J.-S. Song, T. Kwon, M. Yung (Eds.), Information Security Applications. XI, 378 pages. 2006.

Vol. 3108: H. Wang, J. Pieprzyk, V. Varadharajan (Eds.), Information Security and Privacy. XII, 494 pages. 2004.

Vol. 2951: M. Naor (Ed.), Theory of Cryptography. XI, 523 pages. 2004.

Vol. 2742: R.N. Wright (Ed.), Financial Cryptography. VIII, 321 pages. 2003.

# Table of Contents

## Cryptanalysis – I

Cryptanalysis of a Hash Function Proposed at ICISC 2006 ............ 1
*Willi Geiselmann and Rainer Steinwandt*

Cryptanalysis of Reduced Versions of the HIGHT Block Cipher from CHES 2006 ........................................ 11
*Jiqiang Lu*

A Cryptanalysis of the Double-Round Quadratic Cryptosystem ........ 27
*Antoine Scemama*

## Access Control

A Lightweight Privacy Preserving Authentication and Access Control Scheme for Ubiquitous Computing Environment .................... 37
*Jangseong Kim, Zeen Kim, and Kwangjo Kim*

Establishing RBAC-Based Secure Interoperability in Decentralized Multi-domain Environments ........................................ 49
*Jinwei Hu, Ruixuan Li, and Zhengding Lu*

Handling Dynamic Information Release ............................ 64
*Li Jiang, Lingdi Ping, and Xuezeng Pan*

## Cryptanalysis – II

Improving the Time Complexity of Matsui's Linear Cryptanalysis ...... 77
*Baudoin Collard, F.-X. Standaert, and Jean-Jacques Quisquater*

On Large Distributions for Linear Cryptanalysis .................... 89
*Alexander Maximov*

Passive Attacks on a Class of Authentication Protocols for RFID ...... 102
*Basel Alomair, Loukas Lazos, and Radha Poovendran*

Side Channel Attacks on Irregularly Decimated Generators ............ 116
*Chuan-Wen Loe and Khoongming Khoo*

## System Security

Asynchronous Pseudo Physical Memory Snapshot and Forensics on Paravirtualized VMM Using Split Kernel Module ...................... 131
*Ruo Ando, Youki Kadobayashi, and Youichi Shinoda*

Filesystem Activity Following a SSH Compromise: An Empirical Study of File Sequences ................................................ 144
*Jesus Molina, Xavier Chorin, and Michel Cukier*

A Secure Virtual Execution Environment for Untrusted Code .......... 156
*Yan Wen and Huaimin Wang*

## Biometrics

Liveness Detection of Fingerprint Based on Band-Selective Fourier Spectrum .......... 168
*Changlong Jin, Hakil Kim, and Stephen Elliott*

## Cryptographic Protocols

Improving Upon the TET Mode of Operation .......... 180
*Palash Sarkar*

## Hash Functions – I

New Local Collisions for the SHA-2 Hash Family .......... 193
*Somitra Kumar Sanadhya and Palash Sarkar*

Multi-collision Attack on the Compression Functions of MD4 and 3-Pass HAVAL .......... 206
*Hongbo Yu and Xiaoyun Wang*

## Block and Stream Ciphers

Differential Cryptanalysis of T-Function Based Stream Cipher TSC-4 ... 227
*Haina Zhang and Xiaoyun Wang*

New Results on Impossible Differential Cryptanalysis of Reduced AES .......... 239
*Wentao Zhang, Wenling Wu, and Dengguo Feng*

## Copyright Protection

A Note About the Traceability Properties of Linear Codes .......... 251
*Marcel Fernandez, Josep Cotrina, Miguel Soriano, and Neus Domingo*

## Smart Cards

Power Analysis Attacks on MDPL and DRSL Implementations .......... 259
*Amir Moradi, Mahmoud Salmasizadeh, and Mohammad T. Manzuri Shalmani*

Safe-Error Attack on SPA-FA Resistant Exponentiations Using a HW Modular Multiplier .......... 273
*Chong Hee Kim, Jong Hoon Shin, Jean-Jacques Quisquater, and Pil Joong Lee*

## Elliptic Curve Cryptosystems

Generalized MMM-Algorithm Secure Against SPA, DPA, and RPA ..... 282
*Atsuko Miyaji*

Pairing-Friendly Elliptic Curves with Small Security Loss by Cheon's Algorithm ..... 297
*Aya Comuta, Mitsuru Kawazoe, and Tetsuya Takahashi*

## Hash Functions – II

Analysis of Multivariate Hash Functions ..... 309
*Jean-Philippe Aumasson and Willi Meier*

Colliding Message Pair for 53-Step HAS-160 ..... 324
*Florian Mendel and Vincent Rijmen*

Weaknesses in the HAS-V Compression Function ..... 335
*Florian Mendel and Vincent Rijmen*

## Authentication and Authorization

Security-Preserving Asymmetric Protocol Encapsulation ..... 346
*Raphael C.-W. Phan and Serge Vaudenay*

**Author Index** ..... 367

# Cryptanalysis of a Hash Function Proposed at ICISC 2006

Willi Geiselmann[1] and Rainer Steinwandt[2]

[1] Institut für Algorithmen und Kognitive Systeme, Fakultät für Informatik, Universität Karlsruhe (TH), Am Fasanengarten 5, 76128 Karlsruhe, Germany
geiselma@ira.uka.de
[2] Department of Mathematical Sciences, Florida Atlantic University, 777 Glades Road, Boca Raton, FL 33431, USA
rsteinwa@fau.edu

**Abstract.** A simple method for constructing collisions for Shpilrain's polynomial-based hash function from ICISC 2006 is presented. The attack relies on elementary linear algebra and can be considered as practical: For the parameters suggested, we give a specific collision, computed by means of a computer algebra system.

**Keywords:** cryptanalysis, hash function.

## 1 Introduction

In [Shp06] Shpilrain proposes a hash function $H$ which builds on the Merkle-Damgård construction [Dam90, Mer90] and relies on computations in the quotient of a polynomial ring. In [Cha06] Chang reports that the underlying compression function is easy to invert and that a meet-in-the-middle attack enables a preimage attack on $H$. According to Chang's complexity estimate, for the specific parameters proposed in [Shp06] the computational effort for mounting such a preimage attack appears to be in the magnitude of $2^{80}$ operations.

The collision attack we describe below can be considered as practical—for the specific parameters proposed in [Shp06] we give a collision of two equal length bitstrings with about 10.2 KByte each. Shpilrain's proposed hash function $H$ does not involve padding, but the collision given below remains valid if the usual Merkle-Damgård strengthening is applied to $H$.

## 2 The Proposal from ICISC 2006

Let $p(x) \in \mathbb{F}_2[x]$ be a univariate polynomial of degree $n$ over the finite field with two elements. Moreover, let $\alpha$ be the residue class of $x$ in the quotient $R := \mathbb{F}_2[x]/(p(x))$, thus $p(\alpha) = 0$. We remark that [Shp06] writes "$R = \mathbb{F}_{2^n} = \mathbb{F}_2[x]/(p(x))$" which suggests $p(x)$ to be irreducible, but the specific polynomial $p(x)$ proposed is reducible.

K.-H. Nam and G. Rhee (Eds.): ICISC 2007, LNCS 4817, pp. 1–10, 2007.

### 2.1 General Construction

To define the hash function $H$, two elements $h_0, h_1 \in R$ are fixed, and the hash value of an individual bit is defined as

$$\begin{aligned} H(0) &:= h_0, \\ H(1) &:= h_1 \end{aligned} \quad . \tag{1}$$

Next, a triple $(u_0, u_1, u_2) \in R^3$ is used to fix a binary operation $\circ$ on $R$:

$$\begin{aligned} \circ : \quad R^2 &\longrightarrow R \\ (r_1, r_2) &\longmapsto r_1 \circ r_2 := u_0 + r_1 \cdot r_2 + r_1^2 \cdot u_1 + r_2^2 \cdot u_2 \end{aligned} \tag{2}$$

To hash a bitstring $M$, the following procedure is used:

1. Going from left to right, the bitstring $M$ is split into 32-bit blocks $M = B_1 \parallel B_2 \parallel \cdots \parallel B_\ell$, where the last block $B_\ell$ has less than 32 bit, if the length of $M$ is not a multiple of 32. There is no padding.
2. The hash value of each single 32-bit block $B_i = B_{i,0} \parallel \cdots \parallel B_{i,31}$ is computed by applying the above operation $\circ$ one bit at a time, going from left to right:

$$H(B_i) := (\ldots((H(B_{i,0}) \circ H(B_{i,1})) \circ H(B_{i,2}))\ldots) \circ H(B_{i,31})$$

   (where the hash value $H(B_{i,j})$ of a single bit $B_{i,j}$ is given by (1)).
3. The hash value $H(M)$ of $M$ is computed by applying the operation $\circ$ one block at a time, going from left to right:

$$H(M) := (\ldots((H(B_0) \circ H(B_1)) \circ H(B_2))\ldots) \circ H(B_\ell)$$

The value $H(M)$ is the output of the hash function for input $M$.

### 2.2 Suggested Parameters

As specific parameter choice, [Shp06] suggests the following:

$$\begin{aligned} p(x) &:= x^{163} + x^7 + x^6 + x^5 + x^4 + x + 1 \\ h_0 &:= \alpha^7 + 1 \\ h_1 &:= \alpha^8 + 1 \\ (u_0, u_1, u_2) &:= (1, \alpha^2, \alpha) \end{aligned}$$

To demonstrate the practicality of the attack proposed below, in Section 3.3 we construct a specific collision for this parameter choice.

## 3 Finding Collisions

As already indicated above, the notation "$R = \mathbb{F}_{2^n} = \mathbb{F}_2[x]/(p(x))$" in [Shp06] suggests the considered polynomial $p(x)$ to be irreducible. However, with a computer algebra system like Magma [BCP97] one easily checks that the proposed polynomial splits into four irreducible factors from $\mathbb{F}_2[x]$. Namely, for $p(x) = x^{163} + x^7 + x^6 + x^5 + x^4 + x + 1$ we have $p(x) = q_1(x) \cdot q_2(x) \cdot q_3(x) \cdot q_4(x)$, where

$$\begin{aligned}
q_1(x) &:= x^9 + x^7 + x^5 + x + 1, \\
q_2(x) &:= x^{18} + x^{14} + x^{12} + x^{11} + x^6 + x^4 + 1, \\
q_3(x) &:= x^{38} + x^{36} + x^{33} + x^{31} + x^{30} + x^{28} + x^{24} + x^{22} + x^{21} + x^{20} + x^{19} \\
&\quad + x^{17} + x^{16} + x^{12} + x^{10} + x^8 + x^7 + x^4 + x^3 + x^2 + 1, \\
q_4(x) &:= x^{98} + x^{94} + x^{93} + x^{91} + x^{90} + x^{88} + x^{87} + x^{84} + x^{82} + x^{73} + x^{69} \\
&\quad + x^{68} + x^{67} + x^{65} + x^{64} + x^{61} + x^{58} + x^{55} + x^{54} + x^{53} + x^{46} \\
&\quad + x^{45} + x^{44} + x^{43} + x^{42} + x^{41} + x^{39} + x^{37} + x^{31} + x^{29} + x^{28} \\
&\quad + x^{26} + x^{25} + x^{24} + x^{20} + x^{18} + x^{17} + x^{14} + x^{13} + x^9 + x^8 + x^7 \\
&\quad + x^6 + x^5 + x^3 + x^2 + 1 \quad .
\end{aligned}$$

Thus, before discussing the core part of our attack, it is worth discussing briefly how to exploit such a factorization for a collision search.

### 3.1 Using the Chinese Remainder Theorem

According to the Chinese Remainder Theorem, any factorization of the polynomial $p(x)$ into coprime factors $q_1(x) \dots, q_s(x)$ yields a decomposition of the ring $R = \mathbb{F}_2[x]/(p(x))$ into a direct product of rings $R_i := \mathbb{F}_2[x]/(q_i(x))$:

$$R \simeq R_1 \times \cdots \times R_s$$

As the hash function $H$ composes the hash values of the individual 32-bit blocks with simple ring operations, it looks tempting to exploit this isomorphism of rings to perform the collision search "one $R_i$ at a time". Suppose we have found two bitstrings $M_1, M_2$ whose lengths are multiples of 32 and which satisfy

$$H(M_1) \equiv H(M_2) \pmod{q_s(x)} \quad ,$$

i. e., we have a collision in the $R_s$-component. Owing to the Merkle-Damgård structure of $H$, we then have

$$H(M_1 \parallel T) \equiv H(M_2 \parallel T) \pmod{q_s(x)}$$

for arbitrary bitstrings $T$ appended to $M_1$ and $M_2$. Thus, if we heuristically (though actually incorrectly) take the values $H(M_1 \parallel T)$ and $H(M_2 \parallel T)$ as being uniformly and independently distributed modulo $q_{s-1}(x)$, we would expect that within $O(2^{\deg(q_{s-1}(x))})$ random attempts for $T$, we encounter a pair of messages $M_1 \parallel T_{s-1}$, $M_2 \parallel T_{s-1}$ whose hash values coincide in the $R_{s-1} \times R_s$-component of $R$. If the degree of $q_{s-1}$ is small, this approach can be efficient enough. In our experiments we used the linear algebra technique described in the next section to reduce the computational effort for finding a matching $T_{s-1}$.

Now assume we have found a matching "tail" $T_{s-1}$ and that the length of $T_{s-1}$ is a multiple of 32. Then we can apply the same reasoning as before to extend the collision

$$H(M_1 \parallel T_{s-1}) \equiv H(M_2 \parallel T_{s-1}) \pmod{q_{s-1}(x) \cdot q_s(x)}$$

from $R_{s-1} \times R_s$ to $R_{s-2} \times R_{s-1} \times R_s$: Analogously as before, now we test bitstrings $T_{s-2}$ until

$$H(M_1 \parallel T_{s-1} \parallel T_{s-2}) \equiv H(M_2 \parallel T_{s-1} \parallel T_{s-2}) \pmod{q_{s-2} \cdot q_{s-1} \cdot q_s}$$

holds. In this way, we can process the components $R_s, R_{s-1}, \ldots, R_1$ one by one, starting from a collision in a single component.

*Example 1.* For the specific parameters from Section 2.2 we have $s = 4$, and the degrees of $q_1(x)$, $q_2(x)$ and $q_3(x)$ are rather small—namely 9, 18 and 38. Thus, once we know a pair of messages colliding in the larger $R_4$-component (of size $2^{98}$), deriving a full collision that is valid in $R$ should be straightforward. Indeed, in our actual computations this worked as expected.

### 3.2 Using Linear Algebra

In view of the above discussion, the parameter choice in [Shp06] does not seem to offer an adequate security level, and constructing a collision in the component $R_4$ (of size $2^{98}$) seems to be the most time-consuming task for mounting such an attack. In this section we show that such a collision can be found easily, without implementing a full birthday attack in $R_4$.

*Remark 1.* We describe the attack for an irreducible polynomial $p(x)$ of degree $n$, i. e., for $R \simeq \mathbb{F}_{2^n}$. For the specific parameter set from Section 2.2, this linear algebra based part is exploited for $R_4$ and $R_3$ only, but the attack technique as such does not rely on the described shortcut via the Chinese Remainder Theorem. In particular, simply imposing $p(x)$ to be irreducible of degree 163 does not appear to be an adequate countermeasure to rule out the attack.

Let $R' \subseteq R$ be the image of $H$ when being restricted to messages whose length is a multiple of 32 (i. e., we have no incomplete last blocks). To each 32-bit block $B$, we can assign the following map $\phi_B$, which captures the update of $H$'s internal state when appending $B$ to a message whose length is a multiple of 32.

$$\begin{aligned} \phi_B : R' &\longrightarrow R' \\ h &\longmapsto h \circ H(B) \end{aligned}$$

The map $\phi_B$, is affine in the sense that it splits into the sum of the $\mathbb{F}_2$-linear map $h \mapsto h \cdot H(B) + h^2 \cdot u_1$ and the constant shift $H(B)^2 \cdot u_2 + u_0$. If we consider a sequence of blocks $B_1, \ldots, B_t$, then the composition

$$\phi_{B_1 \| B_2 \| \cdots \| B_t}(h) := \phi_{B_t}(\phi_{B_{t-1}}(\ldots \phi_{B_1}(h)) \ldots)$$