Ed Dawson
Serge Vaudenay (Eds.)

LNCS 3715

Progress in Cryptology – Mycrypt 2005

First International Conference
on Cryptology in Malaysia
Kuala Lumpur, Malaysia, September 2005, Proceedings

Springer

Ed Dawson   Serge Vaudenay (Eds.)

Progress in Cryptology – Mycrypt 2005

First International Conference
on Cryptology in Malaysia
Kuala Lumpur, Malaysia, September 28-30, 2005
Proceedings

Springer

Volume Editors

Ed Dawson
Queensland University of Technology
Information Security Institute
GPO Box 2434 (Level 7, 126 Margaret Street)
Brisbane Qld 4001, Australia
E-mail: e.dawson@qut.edu.au

Serge Vaudenay
Ecole Polytechnique Fédérale de Lausanne (EPFL)
Security and Cryptography Laboratory (LASEC)
1015 Lausanne, Switzerland
E-mail: serge.vaudenay@epfl.ch

Library of Congress Control Number: 2005932807

CR Subject Classification (1998): E.3, D.4.6, K.6.5, C.2, K.4, F.2.1-2

ISSN 0302-9743
ISBN-10 3-540-28938-0 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-28938-8 Springer Berlin Heidelberg New York

Springer is a part of Springer Science+Business Media

springeronline.com

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11554868 06/3142 5 4 3 2 1 0

Lecture Notes in Computer Science 3715

Preface

Mycrypt 2005 was the inaugural international conference on cryptology hosted in Malaysia. The conference was co-organized by the Information Security Research Lab at Swinburne University of Technology (Sarawak Campus), NISER (National ICT Security and Emergency Response Centre) and INSPEM (Institute for Mathematical Research) at UPM (University Putra Malaysia). Mycrypt 2005 was held in Kuala Lumpur, Malaysia during September 28–30 2005, in conjunction with the e-Secure Malaysia 2005 convention.

There were 90 paper submissions from 23 countries covering all areas of cryptologic research, from which 19 were accepted. We would like to extend our thanks to all authors who submitted papers to Mycrypt 2005. Each paper was sent anonymously to at least 3 members of the International Program Committee for reviews and comments. The review comments were then followed by discussions among the Program Committee. A recipient of the Best Paper Award was also selected after voting among Program Committee members. The winning paper was "Distinguishing Attacks on T-functions" by Simon Künzli (FH Aargau, Swizerland), Pascal Junod (Nagravision SA, Switzerland) and Willi Meier (FH Aargau, Swizerland). These proceedings contain revised versions of all the accepted papers.

The conference program included three keynote papers: Hideki Imai (Tokyo University) presented a paper entitled "Trends and Challenges for Securer Cryptography in Practice". Moti Yung (Columbia University) presented a paper entitled "Efficient Secure Group Signatures with Dynamic Joins and Keeping Anonymity Against Group Managers". Colin Boyd (QUT) presented a paper entitled "Security of Two-Party Identity-Based Key Agreement".

We are extremely grateful for the time and effort of all the members of the Program Committee in the review process. Their names may be found overleaf. This group was assisted by an even larger group of experts. A list of names is also provided. We hope that it is complete. We give special thanks to Thomas Baignères and Matthieu Finiasz for handling the servers during the review process and preparing the proceedings. The Web-based submission software was written by Chanathip Namprempre with additions by Andre Adelsbach and Andrew Clark. The review process and Program Committee discussions were supported by the Web-based review software developed by Bart Preneel, Wim Moreau and Joris Claessens.

We wish to acknowledge the excellent Mycrypt Local Organizing Committee led by the General Chair, Raphael C.-W. Phan; and the support of MOSTI (Ministry of Science, Technology & Innovation), MEWC (Ministry of Energy, Water & Communications), MCMC (Malaysia Communications & Multimedia Commission), MAMPU (Malaysian Administrative Modernisation & Management Planning Unit), SIRIM (Standards & Industrial Research Institute of Malaysia) and the Malaysian National Computer Confederation (MNCC).

September 2005 — Ed Dawson and Serge Vaudenay

Mycrypt 05

International Conference on Cryptology in Malaysia

September 28–30, 2005, Kuala Lumpur, Malaysia

General Chair

Raphael C.-W. Phan, *Swinburne University of Technology*
Sarawak, Malaysia

Program Chairs

Ed Dawson, *Queensland University of Technology (QUT)*
Brisbane, Australia

Serge Vaudenay, *Ecole Polytechnique Fédérale de Lausanne*
Lausanne, Switzerland

Program Committee

Feng Bao	Institute for Infocomm Research, Singapore
Jean-Sébastien Coron	University of Luxembourg, Luxembourg
Ronald Cramer	Leiden University, The Netherlends
Ed Dawson	Queensland University of Technology, Australia
Yvo Desmedt	University College London, UK
Juan M. González Nieto	Queensland University of Technology, Australia
Helena Handschuh	Gemplus, France
Norbik Idris	Universiti Technologi Malaysia, Malaysia
Antoine Joux	DGA and Université Versailles St. Quentin, France
Marc Joye	Gemplus & CIM-PACA, France
Jonathan Katz	University of Maryland, USA
Kwangjo Kim	Information & Communications University, Korea
Xuejia Lai	Shanghai Jiaotong University, China
Kwok-Yan Lam	Tsinghua University, China
Arjen K. Lenstra	Lucent Technologies, USA and Technische Universiteit Eindhoven, The Netherlands
Stefan Lucks	University of Mannheim, Germany
Wenbo Mao	Hewlett-Packard Labs, UK
Mitsuru Matsui	Mitsubishi Electric, Japan
Rushdan Md Said	University Putra Malaysia, Malaysia
Chris Mitchell	Royal Holloway, University of London, UK
Shiho Moriai	Sony Computer Entertainment, Japan
Gregory Neven	Katholieke Universiteit Leuven, Belgium
Phong Nguyen	CNRS/Ecole Normale Superieure, France
Andrew Odlyzko	University of Minnesota, USA

Eiji Okamoto	University of Tsukuba, Japan
Tatsuaki Okamoto	NTT, Japan
Raphael C.-W. Phan	Swinburne University of Tech., Sarawak, Malaysia
Josef Pieprzyk	University of Macquarie, Australia
Bart Preneel	Katholieke Universiteit Leuven, Belgium
Jean-Jacques Quisquater	Université Catholique de Louvain, Belgium
Pandu Rangan	IIT Madras, India
Vincent Rijmen	Graz University of Technology, Austria
Mohammad Umar Siddiqi	Multimedia University, Malaysia
Serge Vaudenay	EPFL, Switzerland
Sung-Ming Yen	National Central University, Taiwan

External Referees

Michel Abdalla
Masayuki Abe
Kazumaro Aoki
Frederik Armknecht
Gildas Avoine
Thomas Baignères
Chris Vanden Berghe
Olivier Billet
Wieb Bosma
Colin Boyd
An Braeken
Christophe De Cannire
Dario Catalano
Julien Cathalo
Chien-ning Chen
Benoît Chevallier-Mames
Kuo-Zhe Chiou
JaeGwi Choi
Andrew Clark
Scott Contini
Nicolas Courtois
Christophe Doche
Serge Fehr
Matthieu Finiasz
Soichi Furuya
Praveen Gauravaram
Damien Giry
Eu-Jin Goh
Bok-Min Goi
Louis Granboulan
Robbert de Haan
Chao-Chih Hsu
Tetsu Iwata
Ellen Jochemsz
Pascal Junod
Seny Kamara
Hyun Jeong Kim
Kazukuni Kobara
Caroline Kudla
Ulrich Khn
Tanja Lange
Joe Lano
Philippe Léglise
Julie Lescut
Benoit Libert
Vo Duc Liem
Hsi-Chung Lin
Pascal Manet
Stefan Mangard
Bill Millan
Atsuko Miyaji
Havard Molland
Jean Monnerat
Peter Montgomery
Sumio Morioka
Siguna Mueller
Hirofumi Muratani
Jorge Nakahara, Jr.
Kenny Nguyen
Svetla Nikova
Elisabeth Oswald
Pascal Paillier
Olivier Pereira
Duong Hieu Phan
Christian Rechberger
Leonid Reyzin
Yasuyuki Sakai
Palash Sarkar
Taizo Shirai
Joseph Silverman
Jason Smith
Martjn Stam
François-Xavier Standaert
Dirk Stegemann
Ron Steinfeld
Hung-Min Sun
Katsuyuki Takashima
Qiang Tang
Emin Tatli
Shinobu Ushirozawa
Eric Verheul
Zhiguo Wan
Guilin Wang
Huaxiong Wang
Shiuh-Jeng Wang
Benne de Weger
Andreas Wespi
William Whyte
Christopher Wolf
Chi-Dian Wu
Yongdong Wu
Yanjiang Yang
Bo Zhu
Huafei Zhu

Lecture Notes in Computer Science

For information about Vols. 1–3613

please contact your bookseller or Springer

Vol. 3728: V. Paliouras, J. Vounckx, D. Verkest (Eds.), Integrated Circuit and System Design. XV, 753 pages. 2005.

Vol. 3718: V.G. Ganzha, E.W. Mayr, E.V. Vorozhtsov (Eds.), Computer Algebra in Scientific Computing. XII, 502 pages. 2005.

Vol. 3715: E. Dawson, S. Vaudenay (Eds.), Progress in Cryptology – Mycrypt 2005. XI, 329 pages. 2005.

Vol. 3714: H. Obbink, K. Pohl (Eds.), Software Product Lines. XIII, 235 pages. 2005.

Vol. 3712: R. Reussner, J. Mayer, J.A. Stafford, S. Overhage, S. Becker, P.J. Schroeder (Eds.), Quality of Software Architectures and Software Quality. XIII, 289 pages. 2005.

Vol. 3711: F. Kishino, Y. Kitamura, H. Kato, N. Nagata (Eds.), Entertainment Computing - ICEC 2005. XXIV, 540 pages. 2005.

Vol. 3710: M. Barni, I. Cox, T. Kalker, H.J. Kim (Eds.), Digital Watermarking. XII, 485 pages. 2005.

Vol. 3708: J. Blanc-Talon, W. Philips, D. Popescu, P. Scheunders (Eds.), Advanced Concepts for Intelligent Vision Systems. XXII, 725 pages. 2005.

Vol. 3706: H. Fuks, S. Lukosch, A.C. Salgado (Eds.), Groupware: Design, Implementation, and Use. XII, 378 pages. 2005.

Vol. 3703: F. Fages, S. Soliman (Eds.), Principles and Practice of Semantic Web Reasoning. VIII, 163 pages. 2005.

Vol. 3702: B. Beckert (Ed.), Automated Reasoning with Analytic Tableaux and Related Methods. XIII, 343 pages. 2005. (Subseries LNAI).

Vol. 3699: C.S. Calude, M.J. Dinneen, G. Paun, M.J. Pérez-Jiménez, G. Rozenberg (Eds.), Unconventional Computation. XI, 267 pages. 2005.

Vol. 3698: U. Furbach (Ed.), KI 2005: Advances in Artificial Intelligence. XIII, 409 pages. 2005. (Subseries LNAI).

Vol. 3697: W. Duch, J. Kacprzyk, E. Oja, S. Zadrożny (Eds.), Artificial Neural Networks: Formal Models and Their Applications – ICANN 2005, Part II. XXXII, 1045 pages. 2005.

Vol. 3696: W. Duch, J. Kacprzyk, E. Oja, S. Zadrożny (Eds.), Artificial Neural Networks: Biological Inspirations – ICANN 2005, Part I. XXXI, 703 pages. 2005.

Vol. 3695: M.R. Berthold, R. Glen, K. Diederichs, O. Kohlbacher, I. Fischer (Eds.), Computational Life Sciences. XI, 277 pages. 2005. (Subseries LNBI).

Vol. 3693: A.G. Cohn, D.M. Mark (Eds.), Spatial Information Theory. XII, 493 pages. 2005.

Vol. 3691: A. Gagalowicz, W. Philips (Eds.), Computer Analysis of Images and Patterns. XIX, 865 pages. 2005.

Vol. 3690: M. Pěchouček, P. Petta, L.Z. Varga (Eds.), Multi-Agent Systems and Applications IV. XVII, 667 pages. 2005. (Subseries LNAI).

Vol. 3687: S. Singh, M. Singh, C. Apte, P. Perner (Eds.), Pattern Recognition and Image Analysis, Part II. XXV, 809 pages. 2005.

Vol. 3686: S. Singh, M. Singh, C. Apte, P. Perner (Eds.), Pattern Recognition and Data Mining, Part I. XXVI, 689 pages. 2005.

Vol. 3685: V. Gorodetsky, I. Kotenko, V. Skormin (Eds.), Computer Network Security. XIV, 480 pages. 2005.

Vol. 3684: R. Khosla, R.J. Howlett, L.C. Jain (Eds.), Knowledge-Based Intelligent Information and Engineering Systems, Part IV. LXXIX, 933 pages. 2005. (Subseries LNAI).

Vol. 3683: R. Khosla, R.J. Howlett, L.C. Jain (Eds.), Knowledge-Based Intelligent Information and Engineering Systems, Part III. LXXX, 1397 pages. 2005. (Subseries LNAI).

Vol. 3682: R. Khosla, R.J. Howlett, L.C. Jain (Eds.), Knowledge-Based Intelligent Information and Engineering Systems, Part II. LXXIX, 1371 pages. 2005. (Subseries LNAI).

Vol. 3681: R. Khosla, R.J. Howlett, L.C. Jain (Eds.), Knowledge-Based Intelligent Information and Engineering Systems, Part I. LXXX, 1319 pages. 2005. (Subseries LNAI).

Vol. 3679: S.d.C. di Vimercati, P. Syverson, D. Gollmann (Eds.), Computer Security – ESORICS 2005. XI, 509 pages. 2005.

Vol. 3678: A. McLysaght, D.H. Huson (Eds.), Comparative Genomics. VIII, 167 pages. 2005. (Subseries LNBI).

Vol. 3677: J. Dittmann, S. Katzenbeisser, A. Uhl (Eds.), Communications and Multimedia Security. XIII, 360 pages. 2005.

Vol. 3675: Y. Luo (Ed.), Cooperative Design, Visualization, and Engineering. XI, 264 pages. 2005.

Vol. 3674: W. Jonker, M. Petković (Eds.), Secure Data Management. X, 241 pages. 2005.

Vol. 3672: C. Hankin, I. Siveroni (Eds.), Static Analysis. X, 369 pages. 2005.

Vol. 3671: S. Bressan, S. Ceri, E. Hunt, Z.G. Ives, Z. Bellahsène, M. Rys, R. Unland (Eds.), Database and XML Technologies. X, 239 pages. 2005.

Vol. 3670: M. Bravetti, L. Kloul, G. Zavattaro (Eds.), Formal Techniques for Computer Systems and Business Processes. XIII, 349 pages. 2005.

Vol. 3666: B.D. Martino, D. Kranzlmüller, J. Dongarra (Eds.), Recent Advances in Parallel Virtual Machine and Message Passing Interface. XVII, 546 pages. 2005.

Vol. 3665: K. S. Candan, A. Celentano (Eds.), Advances in Multimedia Information Systems. X, 221 pages. 2005.

Vol. 3664: C. Türker, M. Agosti, H.-J. Schek (Eds.), Peer-to-Peer, Grid, and Service-Orientation in Digital Library Architectures. X, 261 pages. 2005.

Vol. 3663: W.G. Kropatsch, R. Sablatnig, A. Hanbury (Eds.), Pattern Recognition. XIV, 512 pages. 2005.

Vol. 3662: C. Baral, G. Greco, N. Leone, G. Terracina (Eds.), Logic Programming and Nonmonotonic Reasoning. XIII, 454 pages. 2005. (Subseries LNAI).

Vol. 3661: T. Panayiotopoulos, J. Gratch, R. Aylett, D. Ballin, P. Olivier, T. Rist (Eds.), Intelligent Virtual Agents. XIII, 506 pages. 2005. (Subseries LNAI).

Vol. 3660: M. Beigl, S. Intille, J. Rekimoto, H. Tokuda (Eds.), UbiComp 2005: Ubiquitous Computing. XVII, 394 pages. 2005.

Vol. 3659: J.R. Rao, B. Sunar (Eds.), Cryptographic Hardware and Embedded Systems – CHES 2005. XIV, 458 pages. 2005.

Vol. 3658: V. Matoušek, P. Mautner, T. Pavelka (Eds.), Text, Speech and Dialogue. XV, 460 pages. 2005. (Subseries LNAI).

Vol. 3655: A. Aldini, R. Gorrieri, F. Martinelli (Eds.), Foundations of Security Analysis and Design III. VII, 273 pages. 2005.

Vol. 3654: S. Jajodia, D. Wijesekera (Eds.), Data and Applications Security XIX. X, 353 pages. 2005.

Vol. 3653: M. Abadi, L. de Alfaro (Eds.), CONCUR 2005 – Concurrency Theory. XIV, 578 pages. 2005.

Vol. 3652: A. Rauber, S. Christodoulakis, A M. Tjoa (Eds.), Research and Advanced Technology for Digital Libraries. XVIII, 545 pages. 2005.

Vol. 3650: J. Zhou, J. Lopez, R.H. Deng, F. Bao (Eds.), Information Security. XII, 516 pages. 2005.

Vol. 3649: W.M. P. van der Aalst, B. Benatallah, F. Casati, F. Curbera (Eds.), Business Process Management. XII, 472 pages. 2005.

Vol. 3648: J.C. Cunha, P.D. Medeiros (Eds.), Euro-Par 2005 Parallel Processing. XXXVI, 1299 pages. 2005.

Vol. 3646: A. F. Famili, J.N. Kok, J.M. Peña, A. Siebes, A. Feelders (Eds.), Advances in Intelligent Data Analysis VI. XIV, 522 pages. 2005.

Vol. 3645: D.-S. Huang, X.-P. Zhang, G.-B. Huang (Eds.), Advances in Intelligent Computing, Part II. XIII, 1010 pages. 2005.

Vol. 3644: D.-S. Huang, X.-P. Zhang, G.-B. Huang (Eds.), Advances in Intelligent Computing, Part I. XXVII, 1101 pages. 2005.

Vol. 3642: D. Ślezak, J. Yao, J.F. Peters, W. Ziarko, X. Hu (Eds.), Rough Sets, Fuzzy Sets, Data Mining, and Granular Computing, Part II. XXIII, 738 pages. 2005. (Subseries LNAI).

Vol. 3641: D. Ślezak, G. Wang, M. Szczuka, I. Düntsch, Y. Yao (Eds.), Rough Sets, Fuzzy Sets, Data Mining, and Granular Computing, Part I. XXIV, 742 pages. 2005. (Subseries LNAI).

Vol. 3639: P. Godefroid (Ed.), Model Checking Software. XI, 289 pages. 2005.

Vol. 3638: A. Butz, B. Fisher, A. Krüger, P. Olivier (Eds.), Smart Graphics. XI, 269 pages. 2005.

Vol. 3637: J. M. Moreno, J. Madrenas, J. Cosp (Eds.), Evolvable Systems: From Biology to Hardware. XI, 227 pages. 2005.

Vol. 3636: M.J. Blesa, C. Blum, A. Roli, M. Sampels (Eds.), Hybrid Metaheuristics. XII, 155 pages. 2005.

Vol. 3634: L. Ong (Ed.), Computer Science Logic. XI, 567 pages. 2005.

Vol. 3633: C. Bauzer Medeiros, M. Egenhofer, E. Bertino (Eds.), Advances in Spatial and Temporal Databases. XIII, 433 pages. 2005.

Vol. 3632: R. Nieuwenhuis (Ed.), Automated Deduction – CADE-20. XIII, 459 pages. 2005. (Subseries LNAI).

Vol. 3631: J. Eder, H.-M. Haav, A. Kalja, J. Penjam (Eds.), Advances in Databases and Information Systems. XIII, 393 pages. 2005.

Vol. 3630: M.S. Capcarrere, A.A. Freitas, P.J. Bentley, C.G. Johnson, J. Timmis (Eds.), Advances in Artificial Life. XIX, 949 pages. 2005. (Subseries LNAI).

Vol. 3629: J.L. Fiadeiro, N. Harman, M. Roggenbach, J. Rutten (Eds.), Algebra and Coalgebra in Computer Science. XI, 457 pages. 2005.

Vol. 3628: T. Gschwind, U. Aßmann, O. Nierstrasz (Eds.), Software Composition. X, 199 pages. 2005.

Vol. 3627: C. Jacob, M.L. Pilat, P.J. Bentley, J. Timmis (Eds.), Artificial Immune Systems. XII, 500 pages. 2005.

Vol. 3626: B. Ganter, G. Stumme, R. Wille (Eds.), Formal Concept Analysis. X, 349 pages. 2005. (Subseries LNAI).

Vol. 3625: S. Kramer, B. Pfahringer (Eds.), Inductive Logic Programming. XIII, 427 pages. 2005. (Subseries LNAI).

Vol. 3624: C. Chekuri, K. Jansen, J.D. P. Rolim, L. Trevisan (Eds.), Approximation, Randomization and Combinatorial Optimization. XI, 495 pages. 2005.

Vol. 3623: M. Liśkiewicz, R. Reischuk (Eds.), Fundamentals of Computation Theory. XV, 576 pages. 2005.

Vol. 3622: V. Vene, T. Uustalu (Eds.), Advanced Functional Programming. IX, 359 pages. 2005.

Vol. 3621: V. Shoup (Ed.), Advances in Cryptology – CRYPTO 2005. XI, 568 pages. 2005.

Vol. 3620: H. Muñoz-Avila, F. Ricci (Eds.), Case-Based Reasoning Research and Development. XV, 654 pages. 2005. (Subseries LNAI).

Vol. 3619: X. Lu, W. Zhao (Eds.), Networking and Mobile Computing. XXIV, 1299 pages. 2005.

Vol. 3618: J. Jedrzejowicz, A. Szepietowski (Eds.), Mathematical Foundations of Computer Science 2005. XVI, 814 pages. 2005.

Vol. 3617: F. Roli, S. Vitulano (Eds.), Image Analysis and Processing – ICIAP 2005. XXIV, 1219 pages. 2005.

Vol. 3615: B. Ludäscher, L. Raschid (Eds.), Data Integration in the Life Sciences. XII, 344 pages. 2005. (Subseries LNBI).

Vol. 3614: L. Wang, Y. Jin (Eds.), Fuzzy Systems and Knowledge Discovery, Part II. XLI, 1314 pages. 2005. (Subseries LNAI).

Table of Contents

Invited Talk I

Stream Ciphers Analysis

Cryptography Based on Combinatorics

Cryptographic Protocols

Invited Talk II

Implementation Issues

Unconventional Cryptography

Invited Talk III

Block Cipher Cryptanalysis

Homomorphic Encryption

Trends and Challenges for Securer Cryptography in Practice

Hideki Imai

Institute of Industrial Science, The University of Tokyo,
Research Center for Information Security,
National Institute of Advanced Industrial Science and Technology

As the importance of information security is widely recognized today, development of cryptography in practical use is rapidly taking place. On the other hand, however, many cases have been reported, where problems are found in the cryptographic systems already in use, or where the cryptographic systems are broken. Causes for a cryptographic system to get corrupted can be: defects in cryptographic algorithm designs; defects in implementation; defects in attack models and definitions of security; progress in computers and attack algorithms; inapplicability due to the change of environment. It is to be noted that the cryptographic system that has been created in the circumstance where there can be some kind of defects is generally vulnerable to breakdown. In the world of cryptography, we should regard "Anything that can happen, happens."

In the first half of my lecture, I will show you some examples of vulnerability in cryptography and measures against it. First, as examples of imminent crises, I will talk about the WEP (Wired Equivalent Protocol) vulnerability, which is a wireless LAN encryption; vulnerability in hash functions; implementation attacks in IC cards; and the issue of "quantum cryptography" Y-00. Next, as a near-future danger, I will talk about serious attacks to a 1024-bit RSA cryptosystem, and lastly, the realization of quantum computers, as an example of future crisis. It is important to evaluate cryptographic systems systematically and continually, in dealing with these crises. As an example of an organization that performs such execution, I will introduce CRYPTREC of Japan.

However, even if all these dangers are prevented, cryptographic systems can be broken, because we cannot prevent human errors and unauthorized acts inside the cryptographic systems completely. In the second part of this lecture, I will talk about Fail-Safe Techniques for Information Security, as a measure against such human-related issues. First, I will discuss the fundamental concept of these techniques. Next, I will introduce, as examples of the fundamental technology in this field, how to construct public-key infrastructures and person authentication systems that are robust against the leakage of secret keys and secret verification data.

Lastly, I will introduce the Research Center for Information Security, at the National Institute of Advanced Industrial Science and Technology, which was established on April 1st of this year and is expected to contribute greatly, in future, in constructing and maintaining the high-level information security of IT systems.

E. Dawson and S. Vaudenay (Eds.): Mycrypt 2005, LNCS 3715, p. 1, 2005.

Distinguishing Attacks on T-Functions

Simon Künzli[1], Pascal Junod[2], and Willi Meier[1]

[1] FH Aargau, 5210 Windisch, Switzerland
{s.kuenzli, w.meier}@fh-aargau.ch
[2] Nagravision SA (Kudelski Group), 1033 Cheseaux, Switzerland
pascal.junod@nagra.com

Abstract. Klimov and Shamir proposed a new class of simple cryptographic primitives named T-functions. For two concrete proposals based on the squaring operation, a single word T-function and a previously unbroken multi-word T-function with a 256-bit state, we describe an efficient distinguishing attack having a 2^{32} data complexity. Furthermore, Hong *et al.* recently proposed two fully specified stream ciphers, consisting of multi-word T-functions with 128-bit states and filtering functions. We describe distinguishing attacks having a 2^{22} and a 2^{34} data complexity, respectively. The attacks have been implemented.

Keywords: Stream cipher, T-function, square mapping, distinguishing attack, statistical cryptanalysis

1 Introduction

Binary additive stream ciphers encrypt a plaintext stream by combining it with a key stream by means of an XOR operation (the decryption simply being the XOR of the key stream with the ciphertext stream). The key stream consists of a pseudo-random bit sequence usually generated by iteration of an *update function*, the latter being initialized with a secret state. One expects that the sequence generated by a cryptographically secure stream cipher is statistically indistinguishable from a truly random sequence (and this for any adversary with some limited computational power), and that there exists no key-recovery attack better than brute-force.

Recently, Klimov and Shamir [7, 8, 9, 10, 6] proposed a new framework for highly efficient mappings which could be used as primitives in stream ciphers and other cryptographic schemes. These primitives consist of *triangular functions* (T-functions) which are built with help of fast arithmetic and Boolean operations widely available on high-end microprocessors or on dedicated hardware implementations; these mappings come with provable properties such as invertibility and a single-cycle structure. As an example, the mapping TF-0 is proposed in [7], which is defined by $x \mapsto x + (x^2 \vee C) \bmod 2^n$ for an n-bit state x and with $C \equiv 5, 7 \pmod 8$. As the maximal length of a cycle may be too short for typical values of n (e.g. $n = 64$), and as state-recovery attacks have been described [2, 8], TF-0 is not meant to be directly used for cryptographic purposes.

E. Dawson and S. Vaudenay (Eds.): Mycrypt 2005, LNCS 3715, pp. 2–15, 2005.

Considering cryptographic applications, several efficient multi-word T-functions are proposed in [9]. Some of these proposals have been broken by Mitra and Sarkar [13] using time-memory tradeoffs. Based on the results of Klimov and Shamir, a new class of multi-word T-functions and two fully specified stream ciphers have been proposed by Hong *et al.* [3, 4]. Their schemes TSC-1 and TSC-2 have a transparent design and allow for some flexibility.

1.1 Contributions of This Paper

In this paper, we analyse several proposals of T-functions and exhibit substantial weaknesses in some of these constructions. The flaws are extended to dedicated attacks.

First we analyse the statistical properties of the pure square mapping, which allows us to find an efficient distinguisher (with an expected 2^{32} data complexity) on TF-0 as well as on a previously unbroken multi-word mapping described in [9] and labeled here as TF-0m, both based on the squaring operation. TF-0m operates on a 256-bit state and the output sequence consists of the 32 most significant bits.

Then, we cryptanalyse the TSC-family of stream ciphers [4], which operates on a 128-bit state and outputs 32 bits of the state using a filtering function. We find a very efficient distinguisher for TSC-1 with an expected 2^{22} data complexity; for TSC-2, we describe a different distinguishing attack with an expected 2^{34} data complexity.

To confirm our theoretical results, the distinguishing attacks have been implemented and run many times with success. Our distinguishers have a negligible error probability and a remarkably small time complexity.

1.2 Notational Conventions

We analyse cryptographic schemes consisting of an internal state $x \in \mathcal{X}$, an update function $\mathsf{f} : \mathcal{X} \to \mathcal{X}$ and an output function $\mathsf{g} : \mathcal{X} \to \mathcal{Y}$. In the case where time instants are relevant, we will denote x^t the state at time t (distinction of powers will be clear from the context). Hence, the iterative scheme maps the state x^t to $x^{t+1} = \mathsf{f}(x^t)$ and outputs $y^t = \mathsf{g}(x^t)$. The seed of the iteration is obtained from the secret key with help of a key scheduling process. The keystream K consists in the concatenation of successive outputs, namely $K = y^0||y^1|| \cdots$.

We assume throughout this paper the threat model of a known-plaintext attack, i.e., we assume to know some part of the keystream K. Our purpose is then to distinguish K from a uniformly distributed random sequence, or to recover the state at any time.

In the case where the state is a vector formed by some words, we will denote a single word by x_j and the state as $x = (x_0, x_1, \ldots)$. Adopting the common notation, $[x]_i$ is the $(i+1)$-st least significant bit-slice of the state, $[x]_0$ denoting the rightmost bit-slice. Consequently, $[x_j]_i$ is the $(i+1)$-st least significant bit of word j. The operation $\mathrm{msb}_m(x)$ states for the m most significant bits of x. Arithmetic operations are performed modulo 2^n with typical word size $n = 32$ or 64 bit. Boolean operations are performed on all n bits in parallel and are denoted by $\wedge$ (AND), $\vee$ (OR), and by $\oplus$ (XOR). Finally, $\lll k$ denotes a cyclic left shift by k positions.

2 Cryptanalysis of Square Mappings

Klimov and Shamir have proposed different types of T-functions based on the squaring operation [7, 9]. After introducing the framework of this section, we focus on the pure square mapping and derive a hypothesis about their probability distribution. This distribution is used in order to distinguish the proposed mappings TF-0 and TF-0m with significant advantage.

Let us consider a scheme which consists of an update function f and an output function g with the notation of Sect. 1.2. Let us further define the random variables X and X' over the set $\mathcal{X} = \{0,1\}^n$, with uniformly distributed X and with $X' = \mathsf{f}(X)$. Equivalently, Y and Y' are random variables over $\mathcal{Y} = \{0,1\}^m$ with uniformly distributed Y and with $Y' = \mathsf{g}(\mathsf{f}(X))$. Given $\Pr_Y$, $\Pr_{Y'}$ and some uniform random or pseudo-random output respectively, we can perform a statistical test (e.g. a Neyman-Pearson test, see Appendix A for more details) in order to assign the output to a distribution. We are interested in the overall complexity of the distinguisher corresponding to some designated overall error probability π_e.

For small[1] word sizes n, the distribution $\Pr_{Y'}$ can be determined by an exhaustive computation of $\mathsf{g}(\mathsf{f}(x))$ for all 2^n elements x, resulting in a precomputation time complexity of $\mathcal{O}(2^n)$ and a memory complexity (measured with the number of required memory cells) of $\mathcal{O}(2^m)$. Given both distributions and a designated overall error probability, the data complexity of an optimal distinguisher is estimated with help of the squared Euclidean imbalance (see Appendix A). We assume that the test is performed in real-time, hence we do not need additional memory in order to store the data. The online time complexity is identical to the data complexity.

However, a precomputation of $\Pr_{Y'}$ might be infeasible for large values of n (e.g. $n = 64$ bit). We perform some detailed analysis of $\Pr_{Y'}$ for small word sizes n and establish an analytical hypothesis for the approximated distribution of Y', considering *only the most biased* elements. This significantly reduces the offline time and memory complexity, but might increase the online time and data complexity of the distinguisher, given some π_e. For small word sizes n, the hypothesis can be verified with the accurate distributions, and for large n, the quality of the hypothesis will be directly examined by the experimental data complexity of the distinguisher.

2.1 Distribution of the Pure Square Mapping

Let us define the pure square mapping $\mathsf{f}(x) = x^2 \bmod 2^n$ and $\mathsf{g}(x) = \mathrm{msb}_m(x)$ with $m = n/2$, which we will refer as PSM. Apart from the least significant bit, f

[1] The term *small* is used with respect to current computational possibilities, i.e. $n \lesssim 40$ bit for personal computers nowadays.

is a T-function. Iteration produces some fixed points such as 0 or 1, hence f can not be considered as an update function for a real application. However, we will be able to reduce more complex single-cycle mappings to some modified square mappings and apply the results obtained in this section; in other words, we will consider the pure square mapping as an ideal case, resulting in distinguishers with minimal data complexity compared to modified square mappings.

We first mention that Klimov and Shamir [7] found an analytical expression for probabilities of single bits of the square mapping. Applying the notation $X' = \mathsf{f}(X)$ for an uniformly distributed X, they found that $\Pr([X']_0 = 0) = \frac{1}{2}$, $\Pr([X']_1 = 0) = 1$ and $\Pr([X']_i = 0) = \frac{1}{2}(1 + 2^{-\frac{i}{2}})$ for $i > 1$. However, as we will have to deal with an additional carry bit later on (which would reduce this bias significantly), we are more interested in the distribution of words.

We explain how to derive highly biased probability distributions for $X' = \mathsf{f}(X)$ and $Y' = \mathsf{g}(\mathsf{f}(X))$. As shown in the next proposition, f is not a permutation, resulting in an unbalanced distribution of X' (there are some predictable elements $\mathsf{f}(x)$ with exceptionally large bias).

Proposition 1. *Consider the function* $\mathsf{f} : \{0,1\}^n \to \{0,1\}^n$ *with* $\mathsf{f}(x) = x^2 \bmod 2^n$. *For successive elements* $x \in \{0, \ldots, 2^n - 1\}$, *the images* $\mathsf{f}(x)$ *have a cyclic structure with cycle length* 2^{n-2}. *Hence* f *is neither injective nor surjective.*

Proof. As $x^2 - \left(2^{n-1} + x\right)^2 = 0 \bmod 2^n$, we have two cycles of length 2^{n-1}, and as $\left(2^{n-2} + x\right)^2 - \left(2^{n-2} - x\right)^2 = 0 \mod 2^n$, both cycles have two mirrored sequences of length 2^{n-2}. Hence the output of successive numbers x has the shape $abc \ldots cbaabc \ldots cba$. □

Due to the specified output function in PSM, the bias is transferred to the distribution of Y'. For a truly random scheme, any element of the output occurs with probability $\pi_0 = 2^{-n/2}$. For the particular scheme PSM, we observed (for small word sizes n) that there exist 4 outcomes with biased probability $2 \cdot \pi_0$, 12 outcomes with biased probability $1.5 \cdot \pi_0$ and so on. This property appears to be independent of n, and we therefore can establish a hypothesis for the most biased elements (which are explicitly known). Let $\mathcal{Y}_i$ be the aggregate containing elements of constant biased probability π_i. The parameter s_i denotes the cardinality of $\mathcal{Y}_i$, and n_i denotes the minimal word size for a stable occurrence of π_i. The parameters n_i, s_i and π_i are summarized in Tab. 1. Then we have for $i = 0, \ldots, k$ (limited by the condition $n \geq n_k$)

$$\begin{aligned} \mathcal{Y}_0 &= \{2^{(n-n_0)/2} \cdot j^2; \qquad j = 0, \ldots, s_0\} \\ \mathcal{Y}_i &= \{2^{(n-n_i)/2} \cdot (1 + 8j); j = 0, \ldots, s_i\} \\ \mathcal{Y}_\infty &= \mathcal{Y} - \textstyle\sum \mathcal{Y}_i \;. \end{aligned} \tag{1}$$

The values in Tab. 1 are determined with empirical methods, however n_i and s_i are exact at least for word sizes within our computational possibilities. In the case of PSM, π_i is exact for $i = 0, 1$, but fluctuating for $i > 1$ so we have to take an average value. A further approximation is done with the remaining elements in $\mathcal{Y}_\infty$, which are assigned to a constant (standardised) probability. The number