Choonsik Park
Seongtaek Chee (Eds.)

Information Security and Cryptology – ICISC 2004

LNCS 3506

7th International Conference
Seoul, Korea, December 2004
Revised Selected Papers

Springer

Choonsik Park Seongtaek Chee (Eds.)

Information Security and Cryptology – ICISC 2004

7th International Conference
Seoul, Korea, December 2-3, 2004
Revised Selected Papers

Springer

Volume Editors

Choonsik Park
Seongtaek Chee
NSRI (National Security Research Institute)
161 Gajeong-dong, Yuseong-gu, Daejeon, Korea
E-mail: {csp,chee}@etri.re.kr

Library of Congress Control Number: 2005926827

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

ISSN 0302-9743
ISBN-10 3-540-26226-1 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-26226-8 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11496618 06/3142 5 4 3 2 1 0

Lecture Notes in Computer Science 3506

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

Preface

The 7th International Conference on Information Security and Cryptology was organized by the Korea Institute of Information Security and Cryptology (KIISC) and was sponsored by the Ministry of Information and Communication of Korea.

The conference received 194 submissions, and the Program Committee selected 34 of these for presentation. The conference program included two invited lectures. Mike Reiter spoke on "Security by, and for, Converged Mobile Devices." And Frank Stajano spoke on "Security for Ubiquitous Computing." We would like to first thank the many researchers from all over the world who submitted their work to this conference. An electronic submission process was available. The submission review process had two phases. In the first phase, Program Committee members compiled reports (assisted at their discretion by subreferees of their choice, but without interaction with other Program Committee members) and entered them, via a Web interface, into the Web Review software. We would like to thank the developers, Bart Preneel, Wim Moreau, and Joris Claessens. Without the Web Review system, the whole review process would not have been possible. In the second phase, Program Committee members used the software to browse each other's reports, and discuss and update their own reports. We are extremely grateful to the Program Committee members for their enormous investment of time, effort, and adrenaline in the difficult and delicate process of review and selection.

We are most grateful to Dr. Jin Hong and Dr. Aaram Yun from NSRI (National Security Research Institute, Korea). Skillfully and patiently, they carried the main load of background work of the Program Co-chairs, in particular in setting up the submission and review servers, providing technical help to the authors and committee members, and in the preparation of this proceedings.

February 2005 Choonsik Park and Seongtaek Chee

Organization

General Chair

Pil Joong Lee	POSTECH, Korea

Program Committee Co-chairs

Choonsik Park	NSRI, Korea
Seongtaek Chee	NSRI, Korea

Program Committee

Alex Biryukov	Katholieke Universiteit Leuven, Belgium
Daniel Bleichenbacher	Bell Laboratories, USA
Kyo Il Chung	ETRI, Korea
Robert Deng	Singapore Management University, Singapore
Gene Itkis	Boston University, USA
Thomas Johansson	Lund University, Sweden
Antoine Joux	DCSSI Crypto Lab, France
Toshinobu Kaneko	Tokyo University of Science, Japan
Hyoung Joong Kim	Kangwon National University, Korea
Myung-Hwan Kim	Seoul National University, Korea
Seungjoo Kim	Sungkyunkwan University, Korea
Yongdae Kim	University of Minnesota, USA
Dong Hoon Lee	Korea University, Korea
Arjen K. Lenstra	Citibank, USA and Eindhoven University of Technology, The Netherlands
Masahiro Mambo	Tohoku University, Japan
Tsutomu Matsumoto	Yokohama National University, Japan
SangJae Moon	Kyungpook National University, Korea
David Naccache	Gemplus Card International, France
Phong Q. Nguyen	CNRS/École Normale Supérieure, France
Tatsuaki Okamoto	NTT Labs, Japan
Josef Pieprzyk	Macquarie University, Australia
David Pointcheval	École Normale Supérieure, France
Vincent Rijmen	IAIK, Graz University of Technology, Austria, and Cryptomathic

Matt Robshaw	Royal Holloway, University of London, UK
Jae-Cheol Ryou	Chungnam National University, Korea
Kouichi Sakurai	Kyushu University, Japan
Palash Sarkar	Indian Statistical Institute, India
William Whyte	NTRU Cryptosystems, USA
Sung-Ming Yen	National Central University, Taiwan, ROC
Moti Yung	Columbia University, USA
Yuliang Zheng	University of North Carolina at Charlotte, USA

Organizing Committee Chair

Ji Hong Kim	Semyung University, Korea

Organizing Committee

Young Sub Koo	Ministry of Information and Communication, Korea
Jae Sung Kim	KISA, Korea
Jeong Nyeo Kim	Electronics and Telecommunications Research Institute, Korea
Gwang Soo Rhee	Sookmyung Women's University, Korea
Kye Sang Lee	Dongeui University, Korea
Young Ho Park	Sejong Cyber University, Korea
Heekuck Oh	Hanyang University, Korea
Chang Han Kim	Semyung University, Korea
Kang Bin Yim	Soonchunhyang University, Korea
Jae Cheol Ha	Korea Nazarene University, Korea

External Reviewers

Michel Abdalla	Dario Catalano	Christophe Clavier
Seigo Arita	Fabienne Cathala	Scott Contini
Roberto Avanzi	Julien Cathalo	Jean-Sébastien Coron
Yoo-Jin Baek	Byungki Cha	Nora Dabbous-Costa
Claude Barral	Sanjit Chatterjee	Tanmoy Das
Olivier Benoît	Chien-Ning Chen	Christophe De Cannière
Carine Boursier-Guesdon	Jung Hee Cheon	Benne de Weger
An Braeken	Benoît Chevallier-Mames	Jean-François Dhem
Éric Brier	Eunsung Cho	Xuhua Ding
Julien Brouchier	Hamid Choukri	Christophe Doche

Håkan Englund
Pierre-Alain Fouque
Jacques Fournier
Steven Galbraith
Karine Gandolfi-Villegas
Pierre Girard
Benoît Gonzalvo
Louis Granboulan
Pascal Guterman
Jaime Gutierrez
Dong-Guk Han
Helena Handschuh
Martin Hell
Seokhie Hong
Nick Hopper
Yoshiaki Hori
Nick Howgrave-Graham
Chao-Chih Hsu
Misuk Huh
Kenji Imamoto
Marc Joye
Ju-Sung Kang
Vishal Kher
Jinhae Kim
Sangwook Kim
Jaehyung Ko
Xeno Kovah
Jin Kwak
Soonhak Kwon
Tanja Lange
Joseph Lano
Younggyo Lee
Hyang-Sook Lee
Insok Lee
Jeong Hyun Lee
Yingjiu Li
Hsi-Chung Lin
Chun-Shien Lu
Philip Mackenzie
Karthikeyan Mahadevan
Subhamoy Maitra
Stefan Mangard
Keith Martin
Gwenaëlle Martinet
Alexander Maximov
Robert McNerney
Frédéric Muller
Sean Murphy
Junghyun Nam
Khánh Quốc Nguyễn
Masayuki Numao
Katsuyuki Okeya
Francis Olivier
Ivan Osipkov
Elisabeth Oswald
Béatrice Péirani
Pascal Paillier
Je Hong Park
S.Y. Park
Kenny Paterson
Mireille Pauliac
Duong Hieu Phan
Stéphanie Porte
Anne-Marie Praden
Bart Preneel
Kyung-Hyune Rhee
Ludovic Rousseau
Scott Russell
Mark Shaneck
Kyungah Shim
Jun-Bum Shin
Wook Shin
Taizo Shirai
Igor Shparlinski
Stéphane Socié
Kyungho Son
Paul Souradyuti
Martijn Stam
Ron Steinfeld
Po-Chyi Su
Hung-Min Sun
Toshihiro Tabata
Tsuyoshi Takagi
Kouhei Tatara
Michael Tunstall
Lionel Victor
Guilin Wang
Peng Wang
Huaxiong Wang
Claire Whelan
Christopher Wolf
Hongjun Wu
Yongdong Wu
Yanjiang Yang
Huafei Zhu

Lecture Notes in Computer Science

For information about Vols. 1–3427

please contact your bookseller or Springer

Vol. 3535: M. Steffen, G. Zavattaro (Eds.), Formal Methods for Open Object-Based Distributed Systems. X, 323 pages. 2005.

Vol. 3532: A. Gómez-Pérez, J. Euzenat (Eds.), The Semantic Web: Research and Applications. XV, 728 pages. 2005.

Vol. 3526: S.B. Cooper, B. Löwe, L. Torenvliet (Eds.), New Computational Paradigms. XVII, 574 pages. 2005.

Vol. 3525: A.E. Abdallah, C.B. Jones, J.W. Sanders (Eds.), Communicating Sequential Processes. XIV, 321 pages. 2005.

Vol. 3524: R. Barták, M. Milano (Eds.), Integration of AI and OR Techniques in Constraint Programming for Combinatorial Problems. XI, 320 pages. 2005.

Vol. 3523: J.S. Marques, N.P. de la Blanca, P. Pina (Eds.), Pattern Recognition and Image Analysis, Part II. XXVI, 733 pages. 2005.

Vol. 3522: J.S. Marques, N.P. de la Blanca, P. Pina (Eds.), Pattern Recognition and Image Analysis, Part I. XXVI, 703 pages. 2005.

Vol. 3521: N. Megiddo, Y. Xu, B. Zhu (Eds.), Algorithmic Applications in Management. XIII, 484 pages. 2005.

Vol. 3520: O. Pastor, J. Falcão e Cunha (Eds.), Advanced Information Systems Engineering. XVI, 584 pages. 2005.

Vol. 3518: T.B. Ho, D. Cheung, H. Li (Eds.), Advances in Knowledge Discovery and Data Mining. XXI, 864 pages. 2005. (Subseries LNAI).

Vol. 3517: H.S. Baird, D.P. Lopresti (Eds.), Human Interactive Proofs. IX, 143 pages. 2005.

Vol. 3516: V.S. Sunderam, G.D. van Albada, P.M.A. Sloot, J.J. Dongarra (Eds.), Computational Science – ICCS 2005, Part III. LXIII, 1143 pages. 2005.

Vol. 3515: V.S. Sunderam, G.D. van Albada, P.M.A. Sloot, J.J. Dongarra (Eds.), Computational Science – ICCS 2005, Part II. LXIII, 1101 pages. 2005.

Vol. 3514: V.S. Sunderam, G.D. van Albada, P.M.A. Sloot, J.J. Dongarra (Eds.), Computational Science – ICCS 2005, Part I. LXIII, 1089 pages. 2005.

Vol. 3513: A. Montoyo, R. Mu\~noz, E. Métais (Eds.), Natural Language Processing and Information Systems. XII, 408 pages. 2005.

Vol. 3510: T. Braun, G. Carle, Y. Koucheryavy, V. Tsaoussidis (Eds.), Wired/Wireless Internet Communications. XIV, 366 pages. 2005.

Vol. 3509: M. Jünger, V. Kaibel (Eds.), Integer Programming and Combinatorial Optimization. XI, 484 pages. 2005.

Vol. 3508: P. Bresciani, P. Giorgini, B. Henderson-Sellers, G. Low, M. Winikoff (Eds.), Agent-Oriented Information Systems II. X, 227 pages. 2005. (Subseries LNAI).

Vol. 3507: F. Crestani, I. Ruthven (Eds.), Information Context: Nature, Impact, and Role. XIII, 253 pages. 2005.

Vol. 3506: C. Park, S. Chee (Eds.), Information Security and Cryptology – ICISC 2004. XIV, 490 pages. 2005.

Vol. 3505: V. Gorodetsky, J. Liu, V. A. Skormin (Eds.), Autonomous Intelligent Systems: Agents and Data Mining. XIII, 303 pages. 2005. (Subseries LNAI).

Vol. 3503: S.E. Nikoletseas (Ed.), Experimental and Efficient Algorithms. XV, 624 pages. 2005.

Vol. 3502: F. Khendek, R. Dssouli (Eds.), Testing of Communicating Systems. X, 381 pages. 2005.

Vol. 3501: B. Kégl, G. Lapalme (Eds.), Advances in Artificial Intelligence. XV, 458 pages. 2005. (Subseries LNAI).

Vol. 3500: S. Miyano, J. Mesirov, S. Kasif, S. Istrail, P. Pevzner, M. Waterman (Eds.), Research in Computational Molecular Biology. XVII, 632 pages. 2005. (Subseries LNBI).

Vol. 3499: A. Pelc, M. Raynal (Eds.), Structural Information and Communication Complexity. X, 323 pages. 2005.

Vol. 3498: J. Wang, X. Liao, Z. Yi (Eds.), Advances in Neural Networks – ISNN 2005, Part III. L, 1077 pages. 2005.

Vol. 3497: J. Wang, X. Liao, Z. Yi (Eds.), Advances in Neural Networks – ISNN 2005, Part II. L, 947 pages. 2005.

Vol. 3496: J. Wang, X. Liao, Z. Yi (Eds.), Advances in Neural Networks – ISNN 2005, Part II. L, 1055 pages. 2005.

Vol. 3495: P. Kantor, G. Muresan, F. Roberts, D.D. Zeng, F.-Y. Wang, H. Chen, R.C. Merkle (Eds.), Intelligence and Security Informatics. XVIII, 674 pages. 2005.

Vol. 3494: R. Cramer (Ed.), Advances in Cryptology – EUROCRYPT 2005. XIV, 576 pages. 2005.

Vol. 3493: N. Fuhr, M. Lalmas, S. Malik, Z. Szlávik (Eds.), Advances in XML Information Retrieval. XI, 438 pages. 2005.

Vol. 3492: P. Blache, E. Stabler, J. Busquets, R. Moot (Eds.), Logical Aspects of Computational Linguistics. X, 363 pages. 2005. (Subseries LNAI).

Vol. 3489: G.T. Heineman, I. Crnkovic, H.W. Schmidt, J.A. Stafford, C. Szyperski, K. Wallnau (Eds.), Component-Based Software Engineering. XI, 358 pages. 2005.

Vol. 3488: M.-S. Hacid, N.V. Murray, Z.W. Raś, S. Tsumoto (Eds.), Foundations of Intelligent Systems. XIII, 700 pages. 2005. (Subseries LNAI).

Vol. 3486: T. Helleseth, D. Sarwate, H.-Y. Song, K. Yang (Eds.), Sequences and Their Applications - SETA 2004. XII, 451 pages. 2005.

Vol. 3483: O. Gervasi, M.L. Gavrilova, V. Kumar, A. Laganà, H.P. Lee, Y. Mun, D. Taniar, C.J.K. Tan (Eds.), Computational Science and Its Applications – ICCSA 2005, Part IV. XXVII, 1362 pages. 2005.

Vol. 3482: O. Gervasi, M.L. Gavrilova, V. Kumar, A. Laganà, H.P. Lee, Y. Mun, D. Taniar, C.J.K. Tan (Eds.), Computational Science and Its Applications – ICCSA 2005, Part III. LXVI, 1340 pages. 2005.

Vol. 3481: O. Gervasi, M.L. Gavrilova, V. Kumar, A. Laganà, H.P. Lee, Y. Mun, D. Taniar, C.J.K. Tan (Eds.), Computational Science and Its Applications – ICCSA 2005, Part II. LXIV, 1316 pages. 2005.

Vol. 3480: O. Gervasi, M.L. Gavrilova, V. Kumar, A. Laganà, H.P. Lee, Y. Mun, D. Taniar, C.J.K. Tan (Eds.), Computational Science and Its Applications – ICCSA 2005, Part I. LXV, 1234 pages. 2005.

Vol. 3479: T. Strang, C. Linnhoff-Popien (Eds.), Location- and Context-Awareness. XII, 378 pages. 2005.

Vol. 3478: C. Jermann, A. Neumaier, D. Sam (Eds.), Global Optimization and Constraint Satisfaction. XIII, 193 pages. 2005.

Vol. 3477: P. Herrmann, V. Issarny, S. Shiu (Eds.), Trust Management. XII, 426 pages. 2005.

Vol. 3475: N. Guelfi (Ed.), Rapid Integration of Software Engineering Techniques. X, 145 pages. 2005.

Vol. 3468: H.W. Gellersen, R. Want, A. Schmidt (Eds.), Pervasive Computing. XIII, 347 pages. 2005.

Vol. 3467: J. Giesl (Ed.), Term Rewriting and Applications. XIII, 517 pages. 2005.

Vol. 3465: M. Bernardo, A. Bogliolo (Eds.), Formal Methods for Mobile Computing. VII, 271 pages. 2005.

Vol. 3464: S.A. Brueckner, G.D.M. Serugendo, A. Karageorgos, R. Nagpal (Eds.), Engineering Self-Organising Systems. XIII, 299 pages. 2005. (Subseries LNAI).

Vol. 3463: M. Dal Cin, M. Kaâniche, A. Pataricza (Eds.), Dependable Computing - EDCC 2005. XVI, 472 pages. 2005.

Vol. 3462: R. Boutaba, K.C. Almeroth, R. Puigjaner, S. Shen, J.P. Black (Eds.), NETWORKING 2005. XXX, 1483 pages. 2005.

Vol. 3461: P. Urzyczyn (Ed.), Typed Lambda Calculi and Applications. XI, 433 pages. 2005.

Vol. 3460: Ö. Babaoglu, M. Jelasity, A. Montresor, C. Fetzer, S. Leonardi, A. van Moorsel, M. van Steen (Eds.), Self-star Properties in Complex Information Systems. IX, 447 pages. 2005.

Vol. 3459: R. Kimmel, N.A. Sochen, J. Weickert (Eds.), Scale Space and PDE Methods in Computer Vision. XI, 634 pages. 2005.

Vol. 3458: P. Herrero, M.S. Pérez, V. Robles (Eds.), Scientific Applications of Grid Computing. X, 208 pages. 2005.

Vol. 3456: H. Rust, Operational Semantics for Timed Systems. XII, 223 pages. 2005.

Vol. 3455: H. Treharne, S. King, M. Henson, S. Schneider (Eds.), ZB 2005: Formal Specification and Development in Z and B. XV, 493 pages. 2005.

Vol. 3454: J.-M. Jacquet, G.P. Picco (Eds.), Coordination Models and Languages. X, 299 pages. 2005.

Vol. 3453: L. Zhou, B.C. Ooi, X. Meng (Eds.), Database Systems for Advanced Applications. XXVII, 929 pages. 2005.

Vol. 3452: F. Baader, A. Voronkov (Eds.), Logic for Programming, Artificial Intelligence, and Reasoning. XI, 562 pages. 2005. (Subseries LNAI).

Vol. 3450: D. Hutter, M. Ullmann (Eds.), Security in Pervasive Computing. XI, 239 pages. 2005.

Vol. 3449: F. Rothlauf, J. Branke, S. Cagnoni, D.W. Corne, R. Drechsler, Y. Jin, P. Machado, E. Marchiori, J. Romero, G.D. Smith, G. Squillero (Eds.), Applications of Evolutionary Computing. XX, 631 pages. 2005.

Vol. 3448: G.R. Raidl, J. Gottlieb (Eds.), Evolutionary Computation in Combinatorial Optimization. XI, 271 pages. 2005.

Vol. 3447: M. Keijzer, A. Tettamanzi, P. Collet, J.v. Hemert, M. Tomassini (Eds.), Genetic Programming. XIII, 382 pages. 2005.

Vol. 3444: M. Sagiv (Ed.), Programming Languages and Systems. XIII, 439 pages. 2005.

Vol. 3443: R. Bodik (Ed.), Compiler Construction. XI, 305 pages. 2005.

Vol. 3442: M. Cerioli (Ed.), Fundamental Approaches to Software Engineering. XIII, 373 pages. 2005.

Vol. 3441: V. Sassone (Ed.), Foundations of Software Science and Computational Structures. XVIII, 521 pages. 2005.

Vol. 3440: N. Halbwachs, L.D. Zuck (Eds.), Tools and Algorithms for the Construction and Analysis of Systems. XVII, 588 pages. 2005.

Vol. 3439: R.H. Deng, F. Bao, H. Pang, J. Zhou (Eds.), Information Security Practice and Experience. XII, 424 pages. 2005.

Vol. 3438: H. Christiansen, P.R. Skadhauge, J. Villadsen (Eds.), Constraint Solving and Language Processing. VIII, 205 pages. 2005. (Subseries LNAI).

Vol. 3437: T. Gschwind, C. Mascolo (Eds.), Software Engineering and Middleware. X, 245 pages. 2005.

Vol. 3436: B. Bouyssounouse, J. Sifakis (Eds.), Embedded Systems Design. XV, 492 pages. 2005.

Vol. 3434: L. Brun, M. Vento (Eds.), Graph-Based Representations in Pattern Recognition. XII, 384 pages. 2005.

Vol. 3433: S. Bhalla (Ed.), Databases in Networked Information Systems. VII, 319 pages. 2005.

Vol. 3432: M. Beigl, P. Lukowicz (Eds.), Systems Aspects in Organic and Pervasive Computing - ARCS 2005. X, 265 pages. 2005.

Vol. 3431: C. Dovrolis (Ed.), Passive and Active Network Measurement. XII, 374 pages. 2005.

Vol. 3430: S. Tsumoto, T. Yamaguchi, M. Numao, H. Motoda (Eds.), Active Mining. XII, 349 pages. 2005. (Subseries LNAI).

Vol. 3429: E. Andres, G. Damiand, P. Lienhardt (Eds.), Discrete Geometry for Computer Imagery. X, 428 pages. 2005.

Vol. 3428: Y.-J. Kwon, A. Bouju, C. Claramunt (Eds.), Web and Wireless Geographical Information Systems. XII, 255 pages. 2005.

Table of Contents

Invited Talks

Block Cipher and Stream Cipher

Public Key Cryptosystem

PKI and Related Implementation

Digital Signature

Elliptic Curve Cryptosystem

Provable Security and Primitives

Network Security

Steganography

Biometrics

Security by, and for, Converged Mobile Devices

Mike Reiter

CyLab. Electrical & Computer Engineering,
Carnegie Mellon University, USA
reiter@cmu.edu

Abstract. Inheriting the vast mobile phone market, converged mobile devices ("smartphones") are poised to become the first ubiquitous personal computing platform. In this talk we detail our vision of the smartphone as a universal access control device—replacing physical keys, access tokens, etc.—and describe our efforts to address some of the technical challenges that stand in the way of this vision. Our discussion will focus on: techniques to prevent the misuse of a stolen device; novel user interfaces that aid in the secure use of such a device; and the design of an access control framework for the variety of authorization scenarios that such a device must accommodate. We also describe our efforts to deploy this technology in a testbed on the Carnegie Mellon campus.

C. Park and S. Chee (Eds.): ICISC 2004, LNCS 3506, p. 1, 2005.

Security for Ubiquitous Computing

Frank Stajano

Computer Laboratory, University of Cambridge, UK
fms27@cam.ac.uk

Abstract. Ubiquitous computing, over a decade in the making, has finally graduated from whacky buzzword through fashionable research topic to something that is definitely and inevitably happening. This will mean revolutionary changes in the way computing affects our society: changes of the same magnitude and scope as those brought about by the World Wide Web. When throw-away computing capabilities are embedded in shoes, drink cans and postage stamps, security and privacy take on entirely new meanings. Programmers, engineers and system designers will have to learn to think in new ways. Ubiquitous computing is not just a wireless version of the Internet with a thousand times more computers, and it would be a naive mistake to imagine that the traditional security solutions for distributed systems will scale to the new scenario. Authentication, authorization, and even concepts as fundamental as ownership require thorough rethinking. At a higher level still, even goals and policies must be revised. One question we should keep asking is simply "Security for whom?" The owner of a device, for example, is no longer necessarily the party whose interests the device will attempt to safeguard. Ubiquitous computing is happening and will affect everyone. By itself it will never be "secure" (whatever this means) if not for the dedicated efforts of people like us who actually do the work. We are the ones who can make the difference. So, before focusing on the implementation details, let's have a serious look at the big picture.

C. Park and S. Chee (Eds.): ICISC 2004, LNCS 3506, p. 2, 2005.

Algebraic Attacks on Combiners with Memory and Several Outputs*

Nicolas T. Courtois

Axalto Cryptographic Research & Advanced Security, 36-38 rue de la Princesse, BP 45, F-78430 Louveciennes Cedex, France
courtois@minrank.org

Abstract. Algebraic attacks on stream ciphers [14] recover the key by solving an overdefined system of multivariate equations. Such attacks can break many LFSR-based stream ciphers, when the output is obtained by a Boolean function, see [14, 15, 16]. Recently this approach has been successfully extended also to combiners with memory, provided the number of memory bits is small, see [1, 16, 2]. In [2] it is shown that, for ciphers built with LFSRs and an arbitrary combiner using a subset of k LFSR state bits, and with l inner state/memory bits, a polynomial attack always do exist when k and l are fixed. Yet this attack becomes very quickly impractical: already when k and l exceed about 4.

In this paper we give a simpler proof of this result from [2], and prove a more general theorem. We show that much faster algebraic attacks exist for any cipher that (in order to be fast) outputs several bits at a time. In practice our result substantially reduces the complexity of the best attack known on four well known constructions of stream ciphers when the number of outputs is increased. We present interesting attacks on modified versions of Snow, E0, LILI-128 and Turing ciphers.

Keywords: algebraic cryptanalysis, LFSR-based stream ciphers, Boolean functions, combiners with memory, LILI-128, Turing cipher, Snow, E0.

Note: An extended version is available at eprint.iacr.org/2003/125/.

1 Introduction

In this paper we study LFSR-based stream ciphers. In such ciphers there is an inner state updated by an iterated linear function, and a stateful or stateless nonlinear combiner that produces the output, given the inner state of the first (linear) part. Our goal is to extend the recent very powerful and very general algebraic attacks on stream ciphers to the case of combiners with several outputs. Such constructions appear naturally if we want to construct ciphers being fast in practice.

* Work supported by the French Ministry of Research RNRT Project "X-CRYPT".

C. Park and S. Chee (Eds.): ICISC 2004, LNCS 3506, pp. 3–20, 2005.