Lynn Margaret Batten
Reihaneh Safavi-Naini (Eds.)

LNCS 4058

Information Security and Privacy

11th Australasian Conference, ACISP 2006
Melbourne, Australia, July 2006
Proceedings

Springer

Lynn Margaret Batten
Reihaneh Safavi-Naini (Eds.)

Information Security and Privacy

11th Australasian Conference, ACISP 2006
Melbourne, Australia, July 3-5, 2006
Proceedings

Springer

Volume Editors

Lynn Margaret Batten
Deakin University
221 Burwood Highway, Burwood 3125, Victoria, Australia
E-mail: lmbatten@deakin.edu.au

Reihaneh Safavi-Naini
University of Wollongong
Centre for Information Security
Wollongong, NSW 2519, Australia
E-mail: rei@uow.edu.au

Library of Congress Control Number: 2006927435

CR Subject Classification (1998): E.3, K.6.5, D.4.6, C.2, E.4, F.2.1, K.4.1

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN	0302-9743
ISBN-10	3-540-35458-1 Springer Berlin Heidelberg New York
ISBN-13	978-3-540-35458-1 Springer Berlin Heidelberg New York

Springer is a part of Springer Science+Business Media

springer.com

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11780656 06/3142 5 4 3 2 1 0

Lecture Notes in Computer Science 4058

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

Lecture Notes in Computer Science

For information about Vols. 1–3950

please contact your bookseller or Springer

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

Vol. 4055: J. Lee, J. Shim, S.-g. Lee, C. Bussler, S. Shim (Eds.), Data Engineering Issues in E-Commerce and Services. IX, 290 pages. 2006.

Vol. 4054: A. Horváth, M. Telek (Eds.), Formal Methods and Stochastic Models for Performance Evaluation. VIII, 239 pages. 2006.

Vol. 4053: M. Ikeda, K.D. Ashley, T.-W. Chan (Eds.), Intelligent Tutoring Systems. XXVI, 821 pages. 2006.

Vol. 4044: P. Abrahamsson, M. Marchesi, G. Succi (Eds.), Extreme Programming and Agile Processes in Software Engineering. XII, 230 pages. 2006.

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

Vol. 4041: S.-W. Cheng, C.K. Poon (Eds.), Algorithmic Aspects in Information and Management. XI, 395 pages. 2006.

Vol. 4040: R. Reulke, U. Eckardt, B. Flach, U. Knauer, K. Polthier (Eds.), Combinatorial Image Analysis. XII, 482 pages. 2006.

Vol. 4039: M. Morisio (Ed.), Reuse of Off-the-Shelf Components. XIII, 444 pages. 2006.

Vol. 4038: P. Ciancarini, H. Wiklicky (Eds.), Coordination Models and Languages. VIII, 299 pages. 2006.

Vol. 4037: R. Gorrieri, H. Wehrheim (Eds.), Formal Methods for Open Object-Based Distributed Systems. XVII, 474 pages. 2006.

Vol. 4036: O. H. Ibarra, Z. Dang (Eds.), Developments in Language Theory. XII, 456 pages. 2006.

Vol. 4034: J. Münch, M. Vierimaa (Eds.), Product-Focused Software Process Improvement. XVII, 474 pages. 2006.

Vol. 4033: B. Stiller, P. Reichl, B. Tuffin (Eds.), Performability Has its Price. X, 103 pages. 2006.

Vol. 4027: H.L. Larsen, G. Pasi, D. Ortiz-Arroyo, T. Andreasen, H. Christiansen (Eds.), Flexible Query Answering Systems. XVIII, 714 pages. 2006. (Sublibrary LNAI).

Vol. 4026: P. Gibbons, T. Abdelzaher, J. Aspnes, R. Rao (Eds.), Distributed Computing in Sensor Systems. XIV, 566 pages. 2006.

Vol. 4025: F. Eliassen, A. Montresor (Eds.), Distributed Applications and Interoperable Systems. XI, 355 pages. 2006.

Vol. 4024: S. Donatelli, P. S. Thiagarajan (Eds.), Petri Nets and Other Models of Concurrency - ICATPN 2006. XI, 441 pages. 2006.

Vol. 4021: E. André, L. Dybkjær, W. Minker, H. Neumann, M. Weber (Eds.), Perception and Interactive Technologies. XI, 217 pages. 2006. (Sublibrary LNAI).

Vol. 4020: A. Bredenfeld, A. Jacoff, I. Noda, Y. Takahashi, RoboCup 2005: Robot Soccer World Cup IX. XVII, 727 pages. 2006. (Sublibrary LNAI).

Vol. 4018: V. Wade, H. Ashman, B. Smyth (Eds.), Adaptive Hypermedia and Adaptive Web-Based Systems. XVI, 474 pages. 2006.

Vol. 4016: J.X. Yu, M. Kitsuregawa, H.V. Leong (Eds.), Advances in Web-Age Information Management. XVII, 606 pages. 2006.

Vol. 4013: L. Lamontagne, M. Marchand (Eds.), Advances in Artificial Intelligence. XIII, 564 pages. 2006. (Sublibrary LNAI).

Vol. 4012: T. Washio, A. Sakurai, K. Nakashima, H. Takeda, S. Tojo, M. Yokoo (Eds.), New Frontiers in Artificial Intelligence. XIII, 484 pages. 2006. (Sublibrary LNAI).

Vol. 4011: Y. Sure, J. Domingue (Eds.), The Semantic Web: Research and Applications. XIX, 726 pages. 2006.

Vol. 4010: S. Dunne, B. Stoddart (Eds.), Unifying Theories of Programming. VIII, 257 pages. 2006.

Vol. 4009: M. Lewenstein, G. Valiente (Eds.), Combinatorial Pattern Matching. XII, 414 pages. 2006.

Vol. 4007: C. Àlvarez, M. Serna (Eds.), Experimental Algorithms. XI, 329 pages. 2006.

Vol. 4006: L.M. Pinho, M. González Harbour (Eds.), Reliable Software Technologies – Ada-Europe 2006. XII, 241 pages. 2006.

Vol. 4005: G. Lugosi, H.U. Simon (Eds.), Learning Theory. XI, 656 pages. 2006. (Sublibrary LNAI).

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

Vol. 4003: Y. Koucheryavy, J. Harju, V.B. Iversen (Eds.), Next Generation Teletraffic and Wired/Wireless Advanced Networking. XVI, 582 pages. 2006.

Vol. 4001: E. Dubois, K. Pohl (Eds.), Advanced Information Systems Engineering. XVI, 560 pages. 2006.

Vol. 3999: C. Kop, G. Fliedl, H.C. Mayr, E. Métais (Eds.), Natural Language Processing and Information Systems. XIII, 227 pages. 2006.

Vol. 3998: T. Calamoneri, I. Finocchi, G.F. Italiano (Eds.), Algorithms and Complexity. XII, 394 pages. 2006.

Vol. 3997: W. Grieskamp, C. Weise (Eds.), Formal Approaches to Software Testing. XII, 219 pages. 2006.

Vol. 3996: A. Keller, J.-P. Martin-Flatin (Eds.), Self-Managed Networks, Systems, and Services. X, 185 pages. 2006.

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

Vol. 3994: V.N. Alexandrov, G.D. van Albada, P.M.A. Sloot, J. Dongarra (Eds.), Computational Science – ICCS 2006, Part IV. XXXV, 1096 pages. 2006.

Vol. 3993: V.N. Alexandrov, G.D. van Albada, P.M.A. Sloot, J. Dongarra (Eds.), Computational Science – ICCS 2006, Part III. XXXVI, 1136 pages. 2006.

Vol. 3992: V.N. Alexandrov, G.D. van Albada, P.M.A. Sloot, J. Dongarra (Eds.), Computational Science – ICCS 2006, Part II. XXXV, 1122 pages. 2006.

Vol. 3991: V.N. Alexandrov, G.D. van Albada, P.M.A. Sloot, J. Dongarra (Eds.), Computational Science – ICCS 2006, Part I. LXXXI, 1096 pages. 2006.

Vol. 3990: J. C. Beck, B.M. Smith (Eds.), Integration of AI and OR Techniques in Constraint Programming for Combinatorial Optimization Problems. X, 301 pages. 2006.

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

Vol. 3987: M. Hazas, J. Krumm, T. Strang (Eds.), Location- and Context-Awareness. X, 289 pages. 2006.

Vol. 3986: K. Stølen, W.H. Winsborough, F. Martinelli, F. Massacci (Eds.), Trust Management. XIV, 474 pages. 2006.

Vol. 3984: M. Gavrilova, O. Gervasi, V. Kumar, C.J. K. Tan, D. Taniar, A. Laganà, Y. Mun, H. Choo (Eds.), Computational Science and Its Applications - ICCSA 2006, Part V. XXV, 1045 pages. 2006.

Vol. 3983: M. Gavrilova, O. Gervasi, V. Kumar, C.J. K. Tan, D. Taniar, A. Laganà, Y. Mun, H. Choo (Eds.), Computational Science and Its Applications - ICCSA 2006, Part IV. XXVI, 1191 pages. 2006.

Vol. 3982: M. Gavrilova, O. Gervasi, V. Kumar, C.J. K. Tan, D. Taniar, A. Laganà, Y. Mun, H. Choo (Eds.), Computational Science and Its Applications - ICCSA 2006, Part III. XXV, 1243 pages. 2006.

Vol. 3981: M. Gavrilova, O. Gervasi, V. Kumar, C.J. K. Tan, D. Taniar, A. Laganà, Y. Mun, H. Choo (Eds.), Computational Science and Its Applications - ICCSA 2006, Part II. XXVI, 1255 pages. 2006.

Vol. 3980: M. Gavrilova, O. Gervasi, V. Kumar, C.J. K. Tan, D. Taniar, A. Laganà, Y. Mun, H. Choo (Eds.), Computational Science and Its Applications - ICCSA 2006, Part I. LXXV, 1199 pages. 2006.

Vol. 3979: T.S. Huang, N. Sebe, M.S. Lew, V. Pavlović, M. Kölsch, A. Galata, B. Kisačanin (Eds.), Computer Vision in Human-Computer Interaction. XII, 121 pages. 2006.

Vol. 3978: B. Hnich, M. Carlsson, F. Fages, F. Rossi (Eds.), Recent Advances in Constraints. VIII, 179 pages. 2006. (Sublibrary LNAI).

Vol. 3977: N. Fuhr, M. Lalmas, S. Malik, G. Kazai (Eds.), Advances in XML Information Retrieval and Evaluation. XII, 556 pages. 2006.

Vol. 3976: F. Boavida, T. Plagemann, B. Stiller, C. Westphal, E. Monteiro (Eds.), Networking 2006. Networking Technologies, Services, and Protocols; Performance of Computer and Communication Networks; Mobile and Wireless Communications Systems. XXVI, 1276 pages. 2006.

Vol. 3975: S. Mehrotra, D.D. Zeng, H. Chen, B.M. Thuraisingham, F.-Y. Wang (Eds.), Intelligence and Security Informatics. XXII, 772 pages. 2006.

Vol. 3973: J. Wang, Z. Yi, J.M. Zurada, B.-L. Lu, H. Yin (Eds.), Advances in Neural Networks - ISNN 2006, Part III. XXIX, 1402 pages. 2006.

Vol. 3972: J. Wang, Z. Yi, J.M. Zurada, B.-L. Lu, H. Yin (Eds.), Advances in Neural Networks - ISNN 2006, Part II. XXVII, 1444 pages. 2006.

Vol. 3971: J. Wang, Z. Yi, J.M. Zurada, B.-L. Lu, H. Yin (Eds.), Advances in Neural Networks - ISNN 2006, Part I. LXVII, 1442 pages. 2006.

Vol. 3970: T. Braun, G. Carle, S. Fahmy, Y. Koucheryavy (Eds.), Wired/Wireless Internet Communications. XIV, 350 pages. 2006.

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

Vol. 3968: K.P. Fishkin, B. Schiele, P. Nixon, A. Quigley (Eds.), Pervasive Computing. XV, 402 pages. 2006.

Vol. 3967: D. Grigoriev, J. Harrison, E.A. Hirsch (Eds.), Computer Science – Theory and Applications. XVI, 684 pages. 2006.

Vol. 3966: Q. Wang, D. Pfahl, D.M. Raffo, P. Wernick (Eds.), Software Process Change. XIV, 356 pages. 2006.

Vol. 3965: M. Bernardo, A. Cimatti (Eds.), Formal Methods for Hardware Verification. VII, 243 pages. 2006.

Vol. 3964: M. Ü. Uyar, A.Y. Duale, M.A. Fecko (Eds.), Testing of Communicating Systems. XI, 373 pages. 2006.

Vol. 3963: O. Dikenelli, M.-P. Gleizes, A. Ricci (Eds.), Engineering Societies in the Agents World VI. XII, 303 pages. 2006. (Sublibrary LNAI).

Vol. 3962: W. IJsselsteijn, Y. de Kort, C. Midden, B. Eggen, E. van den Hoven (Eds.), Persuasive Technology. XII, 216 pages. 2006.

Vol. 3960: R. Vieira, P. Quaresma, M.d.G.V. Nunes, N.J. Mamede, C. Oliveira, M.C. Dias (Eds.), Computational Processing of the Portuguese Language. XII, 274 pages. 2006. (Sublibrary LNAI).

Vol. 3959: J.-Y. Cai, S. B. Cooper, A. Li (Eds.), Theory and Applications of Models of Computation. XV, 794 pages. 2006.

Vol. 3958: M. Yung, Y. Dodis, A. Kiayias, T. Malkin (Eds.), Public Key Cryptography - PKC 2006. XIV, 543 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. 3955: G. Antoniou, G. Potamias, C. Spyropoulos, D. Plexousakis (Eds.), Advances in Artificial Intelligence. XVII, 611 pages. 2006. (Sublibrary LNAI).

Vol. 3954: A. Leonardis, H. Bischof, A. Pinz (Eds.), Computer Vision – ECCV 2006, Part IV. XVII, 613 pages. 2006.

Vol. 3953: A. Leonardis, H. Bischof, A. Pinz (Eds.), Computer Vision – ECCV 2006, Part III. XVII, 649 pages. 2006.

Vol. 3952: A. Leonardis, H. Bischof, A. Pinz (Eds.), Computer Vision – ECCV 2006, Part II. XVII, 661 pages. 2006.

Vol. 3951: A. Leonardis, H. Bischof, A. Pinz (Eds.), Computer Vision – ECCV 2006, Part I. XXXV, 639 pages. 2006.

¥513.00元

Preface

The 11th Australasian Conference on Information Security and Privacy (ACISP 2006) was held in Melbourne, 3–5 July, 2006. The conference was sponsored by Deakin University, the Research Network for a Secure Australia, and was organized in cooperation with the University of Wollongong. The conference brought together researchers, practitioners and a wide range of other users from academia, industries and government organizations.

The program included 35 papers covering important aspects of information security technologies. The papers were selected from 133 submissions through a two-stage anonymous review process. Each paper received at least three reviews by members of the Program Committee, and was then scrutinized by the whole committee during a two-week discussion. There were 19 papers eligible for the "best student paper" award. The award was given to Yang Cui from the University of Tokyo for the paper "Tag-KEM from Set Partial Domain One-Way Permutations."

In addition to the regular papers the program also included three invited talks. Bart Preneel gave an invited talk entitled "Electronic Identity Cards: Threats and Opportunities." Mike Burmester's talk was "Towards Provable Security for Ubiquitous Applications." The details of the third talk had not been finalized at the time of publication of these proceedings.

We wish to thank all the authors of submitted papers for providing the content for the conference; their high-quality submissions made the task of selecting a program very difficult. We are indebted to the diligence and enthusiasm of the Program Committee members in ensuring selection of the most deserving papers and to the external reviewers who helped in the refereeing process. We wish to thank our sponsors, Research Network for a Secure Australia, for their support of the main speakers and students as well as Springer for their continued support of ACISP. We further wish to thank Judy Chow, the conference secretary, for her many organizational skills and patience with the registration process, and our Technical Chair, Jeffrey Horton, for his continuous effort and meticulous attention to every detail, which made the task of the Program Co-chairs so much easier.

Without the help of all the above this conference would not have been a possibility.

July 2006

Lynn Batten
Reihaneh Safavi-Naini

ACISP 2006

July 3–5, 2006, Melbourne, Australia

General Chair
Lynn Batten, Deakin University, Australia

Program Co-chairs
Lynn Batten, Deakin University, Australia
Reihaneh Safavi-Naini, University of Wollongong, Australia

Technical Chair
Jeffrey Horton, University of Wollongong, Australia

Program Committee

Tuomas Aura	Microsoft Research, UK
Feng Bao	Institute for Infocomm Research, Singapore
Colin Boyd	QUT, Australia
Liqun Chen	Hewlett-Packard Laboratories, UK
Kefei Chen	Shanghai Jiaotong University, China
Nicolas T. Courtois	Axalto Smart Cards, France
Robert Deng	Singapore Management University, Singapore
Marc Dacier	Eurecom Institute, France
Ed Dawson	QUT, Australia
Josep Domingo	University of Tarragona, Catalonia
Dieter Gollmann	Hamburg University of Technology, Germany
Juan Gonzalez Nieto	QUT, Australia
Goichiro Hanaoka	Nat. Inst. of Adv. Industrial Sci. and Tech., Japan
Markus Jakobsson	Indiana University, USA
Marc Joye	Gemplus & CIM-PACA, France
Tanja Lange	Technical University of Denmark, Denmark
Byoungcheon Lee	Joongbu University, Korea
Javier Lopez	University of Malaga, Spain
Subhamoy Maitra	Indian Statistical Institute, Kolkata, India
Catherine Meadows	Naval Research Lab, USA
Atsuko Miyaji	JAIST, Japan
Nasir Memon	New York Polytechnic, USA
SangJae Moon	Kyungpook National University, Korea
Keith Martin	Royal Holloway, University of London, UK
Peng Ning	North Carolina State University, USA
Kaisa Nyberg	Helsinki University of Technology and Nokia, Finland
Eiji Okamoto	Tsukuba University, Japan
Giuseppe Persiano	Università di Salerno, Italy
Josef Pieprzyk	Macquarie University, Australia
David Pointcheval	CNRS/ENS, Paris, France
Bimal Roy	Indian Statistical Institute, Kolkata, India
Palash Sarkar	Indian Statistical Institute, India

Jennifer Seberry	University of Wollongong, Australia
Juji Shikata	Yokohama National University, Japan
Nigel Smart	University of Bristol, UK
Douglas Stinson	University of Waterloo, Canada
Tim Strayer	BBN Technologies, USA
Clark Thomborson	University of Auckland, New Zealand
Serge Vaudenay	EPFL, Switzerland
Vijay Varadharajan	Macquarie University, Australia
Victor K. Wei	Chinese University of Hong Kong, Hong Kong

External Reviewers

Masayuki Abe
Joel Alwen
Nuttapong Attrapadung
Roberto M. Avanzi
Gildas Avoine
Thomas Baignères
Daniel J. Bernstein
Srimanta Bhattacharya
Olivier Billet
Mark Branagan
Emmanuel Bresson
Jaimee Brown
Billy Brumley
Debrup Chakraborty
Zhaohui Cheng
Andrew Clark
Christophe Clavier
Yvonne Cliff
Scott Contini
Yang Cui
Paolo D'Arco
Vanesa Daza
Ling Dong
Ratna Dutta
Stefan Dziembowski
Sarah Edwards
Mari Carmen Fernandez-Gago
Matthieu Finiasz
Eiichiro Fujisaki
Jun Furukawa
Clemente Galdi
Zheng Gong
Aline Gouget
Vanessa Gratzer
Jens Groth
JaeCheol Ha
Matt Henricksen
Jason Hinek
Xuan Hong
Zhenjie Huang
Sarath Indrakanti
Toshiyuki Isshiki
Tetsuya Izu
Christine Jones
Ari Juels
Lars Knudsen
Sandeep Kumar
Noboru Kunihiro
Kaoru Kurosawa
Eyal Kushilevitz
David Lapsley
Jens Ove Lauf
HoonJae Lee
Corrado Leita
Qiming Li
Ching Lin
Joseph Liu
Carl Livadas
Yu Long
Yi Lu
John Malone-Lee
Antoni Martínez-Ballesté
Sebastia Martin
Krystian Matusiewicz
Bill Millan
Hideyuki Miyake
Kunihiko Miyazaki
Jean Monnerat
Mridul Nandy
Stan Nurislov
Wakaha Ogata
Juan J. Ortega
Akira Otsuka
Vikram PAdman
Dan Page
Sylvain Pasini
Ahmed Patel
Kenny Paterson
Kun Peng
Pai Peng
Krzysztof Pietrzak
Jordi Castellà Roca
Rodrigo Roman
Kurt Rosenfeld
Chun Ruan
Naouel Ben Salem
Sumanta Sarkar
Francesc Sebé
Taha Sencar
Abdulattif Shikfa
SeongHan Shin
Leonie Simpson
Agustí Solanas
Masakazu Soshi
Ron Steinfeld
Gene Tsudik
Udaya Kiran Tupakula
Ivan Visconti
Martin Vuagnoux
Zhiguo Wan
Guilin Wang
Huaxiong Wang
Pan Wang
Ruizhong Wei
Mi Wen
Jian Weng
Christopher Wolf
Katsunari Yoshioka
Qinghua Zhang
Rui Zhang
Weiliang Zhao
Huafei Zhu

Table of Contents

Stream Ciphers

Symmetric Key Ciphers

Network Security

Cryptographic Applications

Secure Implementation

Signatures

Theory

Invited Talk

Security Applications

Provable Security

Protocols

Hashing and Message Authentication

Algebraic Attacks on Clock-Controlled Stream Ciphers

Sultan Al-Hinai[1], Lynn Batten[2,*], Bernard Colbert[2], and Kenneth Wong[1]

[1] Information Security Institute (ISI)
Queensland University of Technology (QUT), Australia
[2] Deakin University, Australia

Abstract. We present an algebraic attack approach to a family of irregularly clock-controlled bit-based linear feedback shift register systems. In the general set-up, we assume that the output bit of one shift register controls the clocking of other registers in the system and produces a family of equations relating the output bits to the internal state bits. We then apply this general theory to four specific stream ciphers: the (strengthened) stop-and-go generator, the alternating step generator, the self-decimated generator and the step1/step2 generator. In the case of the strengthened stop-and-go generator and of the self-decimated generator, we obtain the initial state of the registers in a significantly faster time than any other known attack. In the other two situations, we do better than or as well as all attacks but the correlation attack. In all cases, we demonstrate that the degree of a functional relationship between the registers can be bounded by two. Finally, we determine the effective key length of all four systems.

Keywords: clock control, stream cipher, linear feedback shift register, irregular clocking, algebraic attack.

1 Introduction

Algebraic attacks, in which the generation of equations assists in determining the initial state or the key-stream of a cipher, were first applied to block ciphers and public key cryptosystems by Courtois and Pieprzyk [8, 13]. Algebraic attacks have been effectively applied to linear feedback shift register (LFSR) based systems as demonstrated in [1, 2, 6, 9, 10, 11, 12]. Our interest in this paper is their application to a class of bit-based LFSRs, which has not yet been examined from this direction — the irregularly clocked LFSR systems. We show that algebraic attacks are effective against this class of stream ciphers and we provide improvements to currently known attacks. In particular, known attacks against the Beth-Piper [3] strengthened stop-and-go cipher depend on the generation of weight three polynomials which cannot be done efficiently. We present a fast attack that is independent of the weight of the polynomial used.

[*] This author wishes to thank the Australian Research Council for support of this work with a Discovery grant.

L. Batten and R. Safavi-Naini (Eds.): ACISP 2006, LNCS 4058, pp. 1–16, 2006.

Irregular clocking in LFSRs is used to enhance their complexity and consequent security. Zenner [27] has developed a general approach to attacking such ciphers by guessing at the clocking through a clock cycle and applies this approach to several ciphers including A5/1, the stop-and-go generator, the alternating step generator and the step1/step2 generator with varying levels of success. Molland [20] introduces a general approach for dealing with LFSR systems with two registers where one register controls the clocking of the other. This applies to the basic stop-and-go generator, LILI-128 and step1/step2 generator. To our knowledge, the only algebraic attack on such a cipher is that on LILI-128 in [12], but guessing the clock control is an integral part of the approach.

Clock-controlled ciphers assume the existence of an underlying clock that maintains a consistent set of basic time intervals against which a register and its output can be compared. A bit-based LFSR system can then be established in a number of ways. A register can be stepped in synchrony with the underlying clock; it may move more slowly than the underlying clock, taking more than one basic unit to shift the registers; but it can be assumed that it will never shift faster than the clock as otherwise we can adjust the basic clocking time to the step time of the register. Similarly, the output from a system of clock-controlled LFSRs can be synchronized with the clock time or can be slowed down or varied against the clock time. If a register shifts with the basic time interval, we refer to is as *regularly clocked*. If the output is delivered with the basic time interval, we refer to it as *regular output*.

We shall focus on four systems, which fall into the above types. The Beth-Piper strengthened stop-and-go generator uses two regularly clocked registers and one irregularly clocked register along with regular output. The alternating step generator has one regularly clocked register and two which are irregularly clocked. Again, the output is regular. In the self-decimated generator, the output is irregular while the sole register actually clocks regularly. The step1/step2 generator has two irregularly clocked LFSRs with irregular output.

In the next section, we introduce the notation standardized throughout the paper and present our generic approach to determining algebraic equations involving the initial state bits from bit-based clock-controlled ciphers in which a linear combination of bits from regularly clocked registers determines the clocking of the others. Our aim is to recover the initial state bits. We ignore key initialization schemes altogether and compute effective key length assuming that the key and initial state of the registers are one and the same. We therefore use the phrase *effective key length*, and make the assumption that for computational purposes eighty bit registers are safe from a brute force attack. In subsequent sections, we use the equations to find the initial states of the four ciphers mentioned above. In the case of the strengthened stop-and-go generator and of the self-decimated generator, we obtain the initial state of the registers in a significantly faster time than any other known attack. In the other two situations, we do better than or as well as all attacks but the correlation attack. In all cases, we demonstrate relationships between the registers indicating that a low degree multiple of the polynomials corresponding to irregularly clocked registers can be bounded by two. Finally, we determine the effective key length of all four systems and present our computational results.

2 The General Set-Up

We consistently label registers A, B and C with lengths l, m and n. The i^{th} bit of register A at time t is denoted by A_i^t and so the output bit is A_l^t. Similarly for registers B and C. We use z^t to denote the output from the entire system at time t. M denotes the number of monomials occurring in a given system of equations. If this system is linear, the complexity of solving the system is in general about M^3; if the system is sparse, this reduces to M^2 [25]. If the system is quadratic, the complexity of using the linearisation methods in [12] is about $\binom{M}{2}^3$. In this paper, we make use of both linear algebra and Gröbner bases methods of solving equations. All computations are performed using the F_4 algorithm in Magma 2.11 [19] on the SGI Origin 3000 using CPU at 600 MHz.

In setting up a general approach to acquiring an equation from a clock-controlled stream cipher of our type, we need to consider three things: first of all, which LFSR controls the clocking (we always use the letter A for this register), secondly, which bits of the controlling register are used to determine the clocking, and thirdly, the effect on the shift of the controlled register. Suppose that the i^{th} bit of A controls the clocking of B in such a way that if it is 0, B does not clock and if it is 1, B clocks j times. In this case, we can express the change to the k^{th} position of B as follows:

$$B_k^t = B_k^{t-1}(A_i^{t-1} \oplus 1) \oplus B_{k-j}^{t-1} A_i^{t-1}. \tag{1}$$

Of course, this applies if $(k-j) > 0$ as otherwise, we need to accommodate the feedback polynomial into the equation, which is easily done. Modifications can also be made to take into consideration the use of several bits of A being used to determine the clocking of B and in cases where more than one register is used in determining the clocking of other registers. As we shall see in the basic stop-and-go generator, a system as simple as the above is inherently weak because if the sum of two consecutive output bits is 1, we already get information about bits in register A. In the more general situation of a polynomial P in the bits of A controlling the clocking of the register B, equation (1) becomes

$$B_k^t = B_k^{t-1}(P \oplus 1) \oplus B_{k-j}^{t-1} P. \tag{2}$$

We state and prove the following theorem involving several regularly clocked registers A_i.

Theorem. *Consider a bit-based LFSR system with k regularly clocked LFSRs A_i of length l_i respectively, $1 \leq i \leq k$, in which a linear polynomial L involving bits of the A_i determines the clocking of a register B of length m as described in (2). Suppose the output z^t at time t is the binary sum of the outputs of all registers. Then the initial state of all A_i can be recovered from a system of quadratic equations, and can subsequently be used to recover the output of B.*

Proof. We have $z^t = B^t_m \oplus \sum_i A^t_{l_i}$, and using (2), can write

$$z^{t+1} = B^t_m(L \oplus 1) \oplus B^t_{m-j} L \oplus \sum_i A^{t+1}_{l_i}. \tag{3}$$

Therefore, $$z^t \oplus z^{t+1} = L(B^t_m \oplus B^t_{m-j}) \oplus \sum_i (A^t_{l_i} \oplus A^{t+1}_{l_i}). \tag{4}$$

Multiplying by $L \oplus 1$, this results in an equation of degree at most two involving the bits of the A_i:

$$(L \oplus 1)(z^t \oplus z^{t+1}) = (L \oplus 1) \sum_i (A^t_{l_i} \oplus A^{t+1}_{l_i}). \tag{5}$$

This quadratic system can be solved for all bits of the registers A_i by running off sufficiently many output bits from the system. The output of B can then be calculated from

$$B^t_m = z^t \oplus \sum_i A^t_{l_i}.$$ □

The above theorem indicates that using more than one regularly clocked register in a linear way to produce the output of the system adds no additional security, as one sufficiently long such register will suffice. This confirms, as a special case, the result of [23]. Although the assumptions of the Theorem apply only to the stop-and-go generator in our list of target ciphers, the method used in the proof applies to a general class of clock-controlled LFSR based systems, those in which a linear function of register bits controls the clocking of several registers. The alternating step and step1/step2 ciphers fall into this category. As we shall see in section 4, the method also works on a system with only one register - the self-decimated generator.

The generation of the equations (sufficiently many to be able to derive a solution from them for the unknowns) is independent of the register values, and so is assumed to be a precomputation procedure. In all cases below, we use a maximum of approximately 2 GB of memory for equation generation. While A produces linear equations from its feedback polynomial, B is producing higher degree equations and so its output is always used in the output of the entire system, which is therefore also highly non-linear. Our aim is therefore to reduce the high degree of the output equations. In each of the four systems discussed below, we take combinations of consecutive output bits in order to obtain reduced degree equations. We compare our attack against each system with other best attacks, based on the keystream requirements, the attack complexity, and the precomputation complexity. We also determine the effective key length for securing the system against the attacks.