Josef Pieprzyk
Hossein Ghodosi
Ed Dawson (Eds.)

LNCS 4586

Information Security and Privacy

12th Australasian Conference, ACISP 2007
Townsville, Australia, July 2007
Proceedings

Josef Pieprzyk Hossein Ghodosi
Ed Dawson (Eds.)

Information Security and Privacy

12th Australasian Conference, ACISP 2007
Townsville, Australia, July 2-4, 2007
Proceedings

Springer

E2007003302

Volume Editors

Josef Pieprzyk
Macquarie University, Department of Computing
Center for Advanced Computing - Algorithms and Cryptography
Sydney, NSW 2109, Australia
E-mail: josef@ics.mq.edu.au

Hossein Ghodosi
James Cook University
School of Mathematics, Physics, and Information Technology
Townsville, QLD 4811, Australia
E-mail: hossein@cs.jcu.edu.au

Ed Dawson
Queensland University of Technology, Information Security Institute
Brisbane, QLD 4001, Australia
E-mail: e.dawson@qut.edu.au

Library of Congress Control Number: 2007929635

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 3-540-73457-0 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-73457-4 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12086818 06/3180 5 4 3 2 1 0

Preface

The 12th Australasian Conference on Information Security and Privacy—ACISP2007—was held in Townsville, Queensland, July 2–4, 2007. This was the first conference to be organized outside the traditional three venues: Brisbane and Gold Coast, Melbourne, and Sydney and Wollongong. The conference was sponsored by James Cook University, Center for Advanced Computing – Algorithm and Cryptography at Macquarie University, Information Security Institute at Queensland University of Technology, and the Research Network for Secure Australia. We would like to thank Matthieu Finiasz and Thomas Baignères from EPFL, LASEC, Switzerland for letting us use their iChair software that facilitated the submission and revision processes.

Out of 132 submissions, the Program Committee (PC) selected 33 papers after a rigorous review process. Each paper got assigned to at least three referees. Papers submitted by members of the PC got assigned to five referees. In the first stage of the review process, the submitted papers were read and evaluated by the PC members and then in the second stage, the papers were scrutinized during a three-week-long discussion. We would like to thank the authors of all papers (both accepted and rejected) for submitting their papers to the conference. A special thanks go to the members of the PC and the external referees who gave their time, expertise and enthusiasm in order to select the best collection of papers.

As in previous years, we held a competition for the "best student paper." To be eligible, a paper had to be co-authored by a postgraduate student whose contribution was more than 50%. Eight papers entered the competition. The winner was Norbert Pramstaller from Graz University of Technology, Austria, for the paper "Second Preimages for Iterated Hash Functions and Their Implications on MACs."

This year we had only one invited talk, which was given by Andreas Enge. The title of the talk was "Contributions Cryptographic Curves."

We would like to express our thanks to Springer and in particular, to Alfred Hofmann and Ronan Nugent for their continuing support of the ACISP conference and for help in the conference proceeding production. Further, we thank Michelle Kang, who helped us with the setting up and maintenance of the ACISP Web site, Vijayakrishnan Pasupathinathan, who took care of the iChair server and ACISP mailbox, Adam Shah for installation of the iChair server and Elizabeth Hansford for assisting with conference organization.

July 2007

Josef Pieprzyk
Hossein Ghodosi
Ed Dawson

Organization

ACISP 2007

July 2–4, 2007, Townsville, Queensland, Australia

General Co-chairs

Hossein Ghodosi	James Cook University, Australia
Ed Dawson	QUT, Australia

Program Chair

Josef Pieprzyk	Macquarie University, Australia

Program Committee

Paul Ashley	IBM, Australia
Tuomas Aura	Microsoft, USA
Lynn Batten	Deakin University, Australia
Colin Boyd	QUT, Australia
Andrew Clark	QUT, Australia
Scott Contini	Macquarie University, Australia
Nicolas Courtois	University College London, UK and Gemalto, France
Yvo Desmedt	University College London, UK
Christophe Doche	Macquarie University, Australia
Ed Dawson	QUT, Australia
Hossein Ghodosi	James Cook University, Australia
Jovan Golić	Telecom, Italy
Dieter Gollmann	TUHH, Germany
Peter Gutmann	University of Auckland, New Zealand
Kwangjo Kim	ICU, Korea
Sevin Knapskog	NTNU, Norway
Kaoru Kurosawa	Ibaraki University, Japan
Tanja Lange	TU/e, Netherlands
Javier Lopez	University of Malaga, Spain
Keith Martin	Royal Holloway, UK
Mitsuru Matsui	Mitsubishi Electric, Japan
Paul Montague	Motorola, Australia
Yi Mu	University of Wollongong, Australia
Andrew Odlyzko	University of Minnesota, USA
Eiji Okamoto	University of Tsukuba, Japan
Rafail Ostrovsky	UCLA, USA

David Poincheval	ENS, France
Bart Preneel	K.U.Leuven, Belgium
Bimal Roy	ISICAL, India
Rei Safavi-Naini	University of Wollongong, Australia
	University of Calgary, Canada
Jennifer Seberry	University of Wollongong, Australia
Igor Shparlinski	Macquarie University, Australia
Ron Steinfeld	Macquarie University, Australia
Willy Susilo	University of Wollongong, Australia
Henk van Tilborg	TU/e, Netherlands
Serge Vaudenay	EPFL, Switzerland
Huaxiong Wang	Macquarie University, Australia
	Nanyang Technological University, Singapore
Henry Wolfe	University of Otago, New Zealand

External Reviewers

Ajith Abraham	Avishek Adhikari	Isaac Agudo
Man Ho Au	Joonsang Baek	Vittorio Bagini
Yun Bai	Thomas Baignères	Rana Barua
Daniel J. Bernstein	Peter Birkner	Xavier Boyen
Yang Cui	Jan Camenisch	Christophe De Cannière
Alvaro Cardenas	Dario Catalano	Agnes Chan
Chris Charnes	Benoit Chevallier-Mames	Sherman S. M. Chow
Yvonne Cliff	Tanmoy Das	Pascal Delaunay
Dang Nguyen Duc	Ernest Foo	Pierre-Alain Fouque
Jun Furukawa	Krzysztof M. Gaj	David Galindo
Juan Garay	Danilo Gligoroski	M. Choudary Gorantla
Jens Groth	Kishan Chand Gupta	Goichiro Hanaoka
Kjetil Haslum	Swee-Huay Heng	Jonathan Herzog
Shoichi Hirose	Michael Hitchens	Jeffrey Horton
Xinyi Huang	Laurent Imbert	Sebastiaan Indesteege
Mahabir Prasad Jhanwar	Emilia Käsper	Lars R. Knudsen
Markulf Kohlweiss	Divyan M. Konidala	Takeshi Koshiba
Kerstin Lemke-Rust	Vo Duc Liem	Chu-Wee Lim
Liang Liu	Liang Lu	Anna Lysyanskaya
Mark Manulis	Abe Masayuki	Krystian Matusiewicz
Luke McAven	Miodrag Mihaljevic	Ilya Mironov
Guglielmo Morgari	Sean Murphy	Pablo Najera
Gregory Neven	Antonio Nicolosi	Svetla Nikova
Wakaha Ogata	Jose A. Onieva	Dunkelman Orr
Pascal Paillier	Sylvain Pasini	Kenny Paterson
Maura Paterson	Goutam Paul	Souradyuti Paul
Kun Peng	Slobodan Petrovic	Raphael C.-W. Phan
Le Trieu Phong	Geraint Price	Havard Raddum

Mohammad Reza Reyhanitabar
Chun Ruan
Siamak Shahandashti
Makoto Sugita
Qiang Tang
Toshio Tokita
Frederik Vercauteren
Guilin Wang
Yan Wang
Benne de Weger
Qianhong Wu
Qingsong Ye
Sèbastien Zimmer

Rodrigo Roman
Yasuyuki Sakai
Nicholas Sheppard
Daisuke Suzuki
Christophe Tartary
Jacques Traore
Charlotte Vikkelsoe
Peishun Wang
Yongge Wang
Christopher Wolf
Guangwu Xu
Hongbo Yu

Greg Rose
Somitra Sanadhya
Jason Smith
Katsuyuki Takashima
Clark Thomborson
Pim Tuyls
Martin Vuagnoux
Shuhong Wang
Brent Waters
Hongjun Wu
Bo-Yin Yang
Steve Zdancewic

Lecture Notes in Computer Science 4586

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

Editorial Board

Lecture Notes in Computer Science

For information about Vols. 1–4489

please contact your bookseller or Springer

Vol. 4600: H. Comon-Lundh, C. Kirchner, H. Kirchner (Eds.), Rewriting, Computation and Proof. XVI, 273 pages. 2007.

Vol. 4595: D. Bošna\vcki, S. Edelkamp (Eds.), Model Checking Software. X, 285 pages. 2007.

Vol. 4592: Z. Kedad, N. Lammari, E. Métais, F. Meziane, Y. Rezgui (Eds.), Natural Language Processing and Information Systems. XIV, 442 pages. 2007.

Vol. 4591: J. Davies, J. Gibbons (Eds.), Integrated Formal Methods. IX, 660 pages. 2007.

Vol. 4590: W. Damm, H. Hermanns (Eds.), Computer Aided Verification. XV, 562 pages. 2007.

Vol. 4589: J. Münch, P. Abrahamsson (Eds.), Product-Focused Software Process Improvement. XII, 414 pages. 2007.

Vol. 4588: T. Harju, J. Karhumäki, A. Lepistö (Eds.), Developments in Language Theory. XI, 423 pages. 2007.

Vol. 4587: R. Cooper, J. Kennedy (Eds.), Data Management. XIII, 259 pages. 2007.

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

Vol. 4584: N. Karssemeijer, B. Lelieveldt (Eds.), Information Processing in Medical Imaging. XX, 777 pages. 2007.

Vol. 4583: S.R. Della Rocca (Ed.), Typed Lambda Calculi and Applications. X, 397 pages. 2007.

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

Vol. 4581: A. Petrenko, M. Veanes, J. Tretmans, W. Grieskamp (Eds.), Testing of Software and Communicating Systems. XII, 379 pages. 2007.

Vol. 4578: F. Masulli, S. Mitra, G. Pasi (Eds.), Fuzzy Logic and Applications. XVIII, 693 pages. 2007. (Sublibrary LNAI).

Vol. 4577: N. Sebe, Y. Liu, Y. Zhuang (Eds.), Multimedia Content Analysis and Mining. XIII, 513 pages. 2007.

Vol. 4576: D. Leivant, R. de Queiroz (Eds.), Logic, Language, Information, and Computation. X, 363 pages. 2007.

Vol. 4574: J. Derrick, J. Vain (Eds.), Formal Techniques for Networked and Distributed Systems – FORTE 2007. XI, 375 pages. 2007.

Vol. 4573: M. Kauers, M. Kerber, R. Miner, W. Windsteiger (Eds.), Towards Mechanized Mathematical Assistants. XIII, 407 pages. 2007. (Sublibrary LNAI).

Vol. 4572: F. Stajano, C. Meadows, S. Capkun, T. Moore (Eds.), Security and Privacy in Ad-hoc and Sensor Networks. X, 247 pages. 2007.

Vol. 4570: H.G. Okuno, M. Ali (Eds.), New Trends in Applied Artificial Intelligence. XXI, 1194 pages. 2007. (Sublibrary LNAI).

Vol. 4569: A. Butz, B. Fisher, A. Krüger, P. Olivier, S. Owada (Eds.), Smart Graphics. IX, 237 pages. 2007.

Vol. 4566: M.J Dainoff (Ed.), Ergonomics and Health Aspects of Work with Computers. XVIII, 390 pages. 2007.

Vol. 4565: D.D. Schmorrow, L.M. Reeves (Eds.), Foundations of Augmented Cognition. XIX, 450 pages. 2007. (Sublibrary LNAI).

Vol. 4564: D. Schuler (Ed.), Online Communities and Social Computing. XVII, 520 pages. 2007.

Vol. 4561: V.G. Duffy (Ed.), Digital Human Modeling. XXIII, 1068 pages. 2007.

Vol. 4560: N. Aykin (Ed.), Usability and Internationalization, Part II. XVIII, 576 pages. 2007.

Vol. 4559: N. Aykin (Ed.), Usability and Internationalization, Part I. XVIII, 661 pages. 2007.

Vol. 4549: J. Aspnes, C. Scheideler, A. Arora, S. Madden (Eds.), Distributed Computing in Sensor Systems. XIII, 417 pages. 2007.

Vol. 4548: N. Olivetti (Ed.), Automated Reasoning with Analytic Tableaux and Related Methods. X, 245 pages. 2007. (Sublibrary LNAI).

Vol. 4547: C. Carlet, B. Sunar (Eds.), Arithmetic of Finite Fields. XI, 355 pages. 2007.

Vol. 4546: J. Kleijn, A. Yakovlev (Eds.), Petri Nets and Other Models of Concurrency – ICATPN 2007. XI, 515 pages. 2007.

Vol. 4545: H. Anai, K. Horimoto, T. Kutsia (Eds.), Algebraic Biology. XIII, 379 pages. 2007.

Vol. 4544: S. Cohen-Boulakia, V. Tannen (Eds.), Data Integration in the Life Sciences. XI, 282 pages. 2007. (Sublibrary LNBI).

Vol. 4543: A.K. Bandara, M. Burgess (Eds.), Inter-Domain Management. XII, 237 pages. 2007.

Vol. 4542: P. Sawyer, B. Paech, P. Heymans (Eds.), Requirements Engineering: Foundation for Software Quality. IX, 384 pages. 2007.

Vol. 4541: T. Okadome, T. Yamazaki, M. Makhtari (Eds.), Pervasive Computing for Quality of Life Enhancement. IX, 248 pages. 2007.

Vol. 4539: N.H. Bshouty, C. Gentile (Eds.), Learning Theory. XII, 634 pages. 2007. (Sublibrary LNAI).

Vol. 4538: F. Escolano, M. Vento (Eds.), Graph-Based Representations in Pattern Recognition. XII, 416 pages. 2007.

Vol. 4537: K.C.-C. Chang, W. Wang, L. Chen, C.A. Ellis, C.-H. Hsu, A.C. Tsoi, H. Wang (Eds.), Advances in Web and Network Technologies, and Information Management. XXIII, 707 pages. 2007.

Vol. 4536: G. Concas, E. Damiani, M. Scotto, G. Succi (Eds.), Agile Processes in Software Engineering and Extreme Programming. XV, 276 pages. 2007.

Vol. 4534: I. Tomkos, F. Neri, J. Solé Pareta, X. Masip Bruin, S. Sánchez Lopez (Eds.), Optical Network Design and Modeling. XI, 460 pages. 2007.

Vol. 4531: J. Indulska, K. Raymond (Eds.), Distributed Applications and Interoperable Systems. XI, 337 pages. 2007.

Vol. 4530: D.H. Akehurst, R. Vogel, R.F. Paige (Eds.), Model Driven Architecture- Foundations and Applications. X, 219 pages. 2007.

Vol. 4529: P. Melin, O. Castillo, L.T. Aguilar, J. Kacprzyk, W. Pedrycz (Eds.), Foundations of Fuzzy Logic and Soft Computing. XIX, 830 pages. 2007. (Sublibrary LNAI).

Vol. 4528: J. Mira, J.R. Álvarez (Eds.), Nature Inspired Problem-Solving Methods in Knowledge Engineering, Part II. XXII, 650 pages. 2007.

Vol. 4527: J. Mira, J.R. Álvarez (Eds.), Bio-inspired Modeling of Cognitive Tasks, Part I. XXII, 630 pages. 2007.

Vol. 4526: M. Malek, M. Reitenspieß, A. van Moorsel (Eds.), Service Availability. X, 155 pages. 2007.

Vol. 4525: C. Demetrescu (Ed.), Experimental Algorithms. XIII, 448 pages. 2007.

Vol. 4524: M. Marchiori, J.Z. Pan, C.d.S. Marie (Eds.), Web Reasoning and Rule Systems. XI, 382 pages. 2007.

Vol. 4523: Y.-H. Lee, H.-N. Kim, J. Kim, Y. Park, L.T. Yang, S.W. Kim (Eds.), Embedded Software and Systems. XIX, 829 pages. 2007.

Vol. 4522: B.K. Ersbøll, K.S. Pedersen (Eds.), Image Analysis. XVIII, 989 pages. 2007.

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

Vol. 4519: E. Franconi, M. Kifer, W. May (Eds.), The Semantic Web: Research and Applications. XVIII, 830 pages. 2007.

Vol. 4517: F. Boavida, E. Monteiro, S. Mascolo, Y. Koucheryavy (Eds.), Wired/Wireless Internet Communications. XIV, 382 pages. 2007.

Vol. 4516: L. Mason, T. Drwiega, J. Yan (Eds.), Managing Traffic Performance in Converged Networks. XXIII, 1191 pages. 2007.

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

Vol. 4514: S.N. Artemov, A. Nerode (Eds.), Logical Foundations of Computer Science. XI, 513 pages. 2007.

Vol. 4513: M. Fischetti, D.P. Williamson (Eds.), Integer Programming and Combinatorial Optimization. IX, 500 pages. 2007.

Vol. 4511: C. Conati, K. McCoy, G. Paliouras (Eds.), User Modeling 2007. XVI, 487 pages. 2007. (Sublibrary LNAI).

Vol. 4510: P. Van Hentenryck, L. Wolsey (Eds.), Integration of AI and OR Techniques in Constraint Programming for Combinatorial Optimization Problems. X, 391 pages. 2007.

Vol. 4509: Z. Kobti, D. Wu (Eds.), Advances in Artificial Intelligence. XII, 552 pages. 2007. (Sublibrary LNAI).

Vol. 4508: M.-Y. Kao, X.-Y. Li (Eds.), Algorithmic Aspects in Information and Management. VIII, 428 pages. 2007.

Vol. 4507: F. Sandoval, A. Prieto, J. Cabestany, M. Graña (Eds.), Computational and Ambient Intelligence. XXVI, 1167 pages. 2007.

Vol. 4506: D. Zeng, I. Gotham, K. Komatsu, C. Lynch, M. Thurmond, D. Madigan, B. Lober, J. Kvach, H. Chen (Eds.), Intelligence and Security Informatics: Biosurveillance. XI, 234 pages. 2007.

Vol. 4505: G. Dong, X. Lin, W. Wang, Y. Yang, J.X. Yu (Eds.), Advances in Data and Web Management. XXII, 896 pages. 2007.

Vol. 4504: J. Huang, R. Kowalczyk, Z. Maamar, D. Martin, I. Müller, S. Stoutenburg, K.P. Sycara (Eds.), Service-Oriented Computing: Agents, Semantics, and Engineering. X, 175 pages. 2007.

Vol. 4501: J. Marques-Silva, K.A. Sakallah (Eds.), Theory and Applications of Satisfiability Testing – SAT 2007. XI, 384 pages. 2007.

Vol. 4500: N. Streitz, A. Kameas, I. Mavrommati (Eds.), The Disappearing Computer. XVIII, 304 pages. 2007.

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

Vol. 4498: N. Abdennahder, F. Kordon (Eds.), Reliable Software Technologies – Ada Europe 2007. XII, 247 pages. 2007.

Vol. 4497: S.B. Cooper, B. Löwe, A. Sorbi (Eds.), Computation and Logic in the Real World. XVIII, 826 pages. 2007.

Vol. 4496: N.T. Nguyen, A. Grzech, R.J. Howlett, L.C. Jain (Eds.), Agent and Multi-Agent Systems: Technologies and Applications. XXI, 1046 pages. 2007. (Sublibrary LNAI).

Vol. 4495: J. Krogstie, A. Opdahl, G. Sindre (Eds.), Advanced Information Systems Engineering. XVI, 606 pages. 2007.

Vol. 4494: H. Jin, O.F. Rana, Y. Pan, V.K. Prasanna (Eds.), Algorithms and Architectures for Parallel Processing. XIV, 508 pages. 2007.

Vol. 4493: D. Liu, S. Fei, Z. Hou, H. Zhang, C. Sun (Eds.), Advances in Neural Networks – ISNN 2007, Part III. XXVI, 1215 pages. 2007.

Vol. 4492: D. Liu, S. Fei, Z. Hou, H. Zhang, C. Sun (Eds.), Advances in Neural Networks – ISNN 2007, Part II. XXVII, 1321 pages. 2007.

Vol. 4491: D. Liu, S. Fei, Z.-G. Hou, H. Zhang, C. Sun (Eds.), Advances in Neural Networks – ISNN 2007, Part I. LIV, 1365 pages. 2007.

Vol. 4490: Y. Shi, G.D. van Albada, J. Dongarra, P.M.A. Sloot (Eds.), Computational Science – ICCS 2007, Part IV. XXXVII, 1211 pages. 2007.

¥646.00元

Table of Contents

Stream Ciphers

Hashing

Biometrics

Secret Sharing

Cryptanalysis

Public Key Cryptography

Authentication

E-Commerce

Security

An Analysis of the Hermes8 Stream Ciphers

Steve Babbage[1], Carlos Cid[2], Norbert Pramstaller[3], and Håvard Raddum[4]

[1] Vodafone Group R&D,
Newbury, United Kingdom
steve.babbage@vodafone.com
[2] Information Security Group,
Royal Holloway, University of London
Egham, United Kingdom
carlos.cid@rhul.ac.uk
[3] IAIK, Graz University of Technology
Graz, Austria
norbert.pramstaller@iaik.tugraz.at
[4] Dept. of Informatics, The University of Bergen,
Bergen, Norway
haavardr@ii.uib.no

Abstract. Hermes8 [6,7] is one of the stream ciphers submitted to the ECRYPT Stream Cipher Project (eSTREAM [3]). In this paper we present an analysis of the Hermes8 stream ciphers. In particular, we show an attack on the latest version of the cipher (Hermes8F), which requires very few known keystream bytes and recovers the cipher secret key in less than a second on a normal PC. Furthermore, we make some remarks on the cipher's key schedule and discuss some properties of ciphers with similar algebraic structure to Hermes8.

Keywords: Hermes8, Stream Cipher, Cryptanalysis.

1 Introduction

Hermes8 is one of the 34 stream ciphers submitted to eSTREAM, the ECRYPT Stream Cipher Project [3]. The cipher has a simple byte-oriented design, consisting of substitutions and shifts of the state register bytes. Two versions of the cipher have been proposed. Originally, the cipher Hermes8 [6] was submitted as candidate to eSTREAM. Although no weaknesses of Hermes8 were found during the first phase of evaluation, the cipher did not seem to present satisfactory performance in either software or hardware [4]. As a result, a slightly modified version of the cipher, named Hermes8F [7], was submitted for consideration during the second phase of eSTREAM. In this paper we present an analysis of the Hermes8 stream ciphers. In Section 2 we present an alternative description of the Hermes8 ciphers. Section 3 describes an attack against the latest version of Hermes8. Section 4 contains some remarks on the key schedule of Hermes8, while we discuss some algebraic properties of the ciphers in Section 5.

J. Pieprzyk, H. Ghodosi, and E. Dawson (Eds.): ACISP 2007, LNCS 4586, pp. 1–10, 2007.

2 Description of Hermes8F

According to [7], Hermes8F is a stream cipher based on the Substitution– Permutation network principle. Hermes8F is defined for two different key lengths: Hermes8F-80 uses 80-bit keys, while Hermes8F-128 uses 128-bit keys. The cipher uses two byte-oriented registers: a 17-byte state register and a 10-byte key register (16 bytes for Hermes8F-128). Additionally, there is a single byte register *Accu*, which seems to have the use of a memory register (Figure 1). The diffusion is provided by moving pointers through both registers, while non-linearity is provided by the AES S-Box [2].

The main operation of the cipher consists of the following steps:

1. XOR the value stored at *Accu* with a byte from the state register and a byte from the key register;
2. Use the previous result as input for the AES S-Box;
3. Replace the state register value used in step 1. by the output of the S-Box;
4. Store the output of the S-Box also in *Accu*;
5. Increment both the state and key register pointers (denoted by $p1$ and $p2$, respectively).

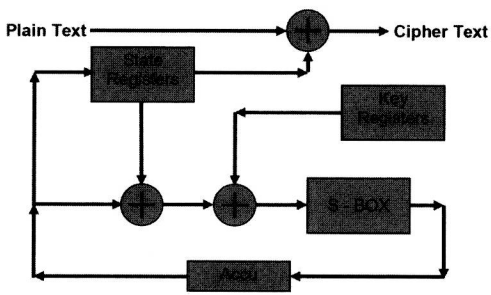

Fig. 1. Hermes8F stream cipher [7]

The steps above are performed at each clocking. A round of the cipher consists of 17 clockings. At every 7 clockings, two bytes of the key register are updated. The updating function is also based on the AES S-Box (Section 4). In the cipher's initialization, the encryption key is loaded into the key register, and the IV is loaded into the state register. The register *Accu* starts with the zero byte as content[1]. The initialization process consists of five rounds (i.e. 85 clockings), and so all the state registers are updated five times before the cipher enters

[1] In Hermes8, the initial value of *Accu* is key-dependent; see Section 4.

the normal mode of operation. The first bytes of the keystream are produced after two further rounds. The output consists of 8 bytes from the state register, taken from alternating positions of the register. Further bytes of the output are produced at every two rounds. More details of the algorithm can be found in [7].

2.1 Alternative Description of Hermes8F

We note that it follows from the description above that during the cipher operation, the contents of the registers *Accu* and state$[p1 - 1]$ are always the same. Thus a more natural description of Hermes8F is given in Figure 2. It consists of the state register R, which is represented as a feedback shift register of length 17, defined as

$$s_i^t = \text{state}[p1 + i] \quad , \quad 0 \le i \le 16,$$

where state$[p1]$ is the byte addressed by pointer $p1$ at time t. This FSR is updated according to the following relations:

$$\begin{aligned} s_i^{t+1} &= s_{i+1}^t \quad , \quad 0 \le i \le 15, \\ s_{16}^{t+1} &= S(s_0^t \oplus s_{16}^t \oplus k^t), \end{aligned}$$

where the byte k^t is the output of the key register K at time t (that is, $k[p2]$), and S represents the AES S-Box.

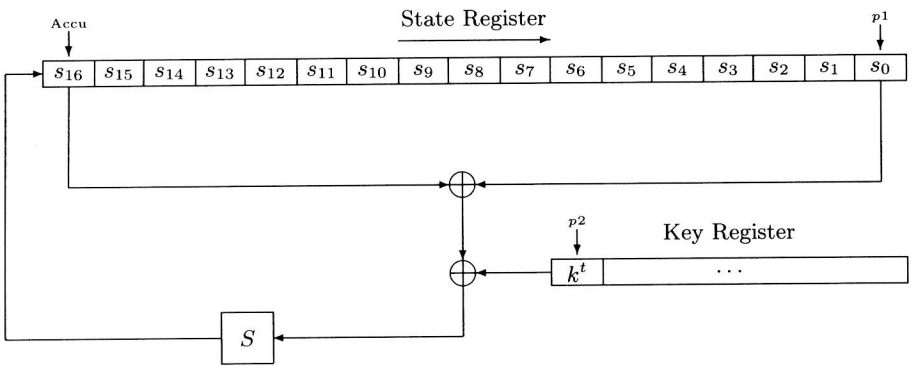

Fig. 2. Hermes8F as a feedback shift register

In our attack, we need to consider the reverse cipher (clocking the generator backwards, and so generating the keystream blocks in reverse order[2]). The relation of the feedback register of the reverse cipher is given by

$$\begin{aligned} s_0^t &= S^{-1}(s_{16}^{t+1}) \oplus s_{16}^t \oplus k^t \\ &= S^{-1}(s_{16}^{t+1}) \oplus s_{15}^{t+1} \oplus k^t. \end{aligned}$$

The inverse cipher is depicted in Figure 3.

[2] As pointed out by one of the anonymous referees, the backward keystream was also used in the attack described in [5].