Helena Handschuh
M. Anwar Hasan (Eds.)

LNCS 3357

Selected Areas in Cryptography

11th International Workshop, SAC 2004
Waterloo, Canada, August 2004
Revised Selected Papers

Springer

Helena Handschuh   M. Anwar Hasan (Eds.)

Selected Areas in Cryptography

11th International Workshop, SAC 2004
Waterloo, Canada, August 9-10, 2004
Revised Selected Papers

Springer

Volume Editors

Helena Handschuh
Gemplus, Issy-les-Moulineaux, France
E-mail: Helena.Handschuh@gemplus.com

M. Anwar Hasan
University of Waterloo, Waterloo, Ontario, Canada
E-mail: ahasan@ece.uwaterloo.ca

Library of Congress Control Number: 2004117402

CR Subject Classification (1998): E.3, D.4.6, K.6.5, F.2.1-2, C.2, H.4.3

ISSN 0302-9743
ISBN 3-540-24327-5 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: 11376224 06/3142 5 4 3 2 1 0

Lecture Notes in Computer Science 3357

Preface

SAC 2004 was the eleventh in a series of annual workshops on Selected Areas in Cryptography. This was the second time that the workshop was hosted by the University of Waterloo, Ontario, with previous workshops being held at Queen's University in Kingston (1994, 1996, 1998 and 1999), Carleton University in Ottawa (1995, 1997 and 2003), the Fields Institute in Toronto (2001) and Memorial University of Newfoundland in St. John's (2002). The primary intent of the workshop was to provide a relaxed atmosphere in which researchers in cryptography could present and discuss new work on selected areas of current interest. This year's themes for SAC were:

- Design and analysis of symmetric key cryptosystems.
- Primitives for symmetric key cryptography, including block and stream ciphers, hash functions, and MAC algorithms.
- Efficient implementation of cryptographic systems in public and symmetric key cryptography.
- Cryptographic solutions for mobile (web) services.

A record of 117 papers were submitted for consideration by the program committee. After an extensive review process, 25 papers were accepted for presentation at the workshop (two of these papers were merged). Unfortunately, many good papers could not be accommodated this year. These proceedings contain the revised versions of the 24 accepted papers. The revised versions were not subsequently checked for correctness.

Also, we were very fortunate to have two invited speakers at SAC 2004.

- Eli Biham arranged for some breaking news in his talk on "New Results on SHA-0 and SHA-1." This talk was designated as the Stafford Tavares Lecture.
- Yevgeniy Dodis enlightened us with "Basing Cryptography on Biometrics and Other Noisy Data."

We are very grateful to the program committee and to the numerous external reviewers for their hard work and precious help. They collectively produced over 380 review reports in less than two months, which was quite a challenge. We have tried to list all of them in these proceedings and we sincerely hope we did not omit anyone.

We are also indebted to the University of Waterloo, Queen's University Kingston, Mitsubishi Electric Corporation, and Research in Motion Ltd. for their financial support of the workshop.

Special thanks are due to K.U.Leuven for kindly providing the Webreview software, Julien Brouchier for running both the submission server and Webreview, Janet Bullock for perfectly handling registrations, and Jaewook Chung and the local arrangements committee from the University of Waterloo for setting up the website and organizing a very nice and entertaining workshop.

Last but not least we would like to thank all submitters and all the participants who made this year's workshop a great success.

November 2004 Helena Handschuh and M. Anwar Hasan

11th Annual Workshop on Selected Areas in Cryptography

August 9–10, 2004, Waterloo, Ontario, Canada

Program and General Chairs

Helena Handschuh	Gemplus, France
M. Anwar Hasan	University of Waterloo, Canada

Program Committee

Carlisle Adams	University of Ottawa, Canada
Henri Gilbert	France Télécom, France
Mike Just	Carleton University, Canada
Charanjit Jutla	IBM, USA
Arjen Lenstra	Lucent Technologies, USA and T.U. Eindhoven, The Netherlands
Stefan Lucks	Universität Mannheim, Germany
Mitsuru Matsui	Mitsubishi Electric, Japan
Alfred Menezes	University of Waterloo, Canada
Shiho Moriai	Sony Computer Entertainment Inc., Japan
Kaisa Nyberg	Nokia, Finland
Bart Preneel	Katholieke Universiteit Leuven, Belgium
Matt Robshaw	Royal Holloway University of London, UK
Douglas R. Stinson	University of Waterloo, Canada
Serge Vaudenay	EPFL, Switzerland
Michael Wiener	Cryptographic Clarity, Canada

Local Arrangements Committee

Janet Bullock, Jaewook Chung, Agustin Dominguez, M. Anwar Hasan, Arash Reyhani-Masoleh, and Siavash B. Sarmadi

Sponsors

University of Waterloo
Mitsubishi Electric Corporation
Research in Motion Ltd.
Queen's University Kingston

External Referees

Frederik Armknecht
Gildas Avoine
Steve Babbage
Thomas Baignères
Lejla Batina
Come Berbain
Florent Bersani
Eli Biham
Olivier Billet
Antoon Bosselaers
Eric Brier
Jaewook Chung
Carlos Cid
Jean-Sébastien Coron
Nicolas Courtois
Paolo D'Arco
Christophe De Cannière
Nevine Ebeid
Soichi Furuya
Guang Gong
Louis Goubin
Shai Halevi
Darrel Hankerson
Jason Hinek
Daisuke Inoue
Tetsu Iwata
Shaoquan Jiang
Antoine Joux
Pascal Junod
Masayuki Kanda
John Kelsey
Kazukuni Kobara
Matthias Krause
Ulrich Kühn
Joseph Lano
Yi Lu
Jonathan Lutz
Kazuhiko Minematsu
Serge Mister
Jean Monnerat
Sumio Morioka
James Muir
Sean Murphy
Junko Nakajima
Kazuomi Oishi
Sıddıka Berna Örs
Matthew Parker
Kenny Paterson
Josyula R. Rao
Arash Reyhani-Masoleh
Pankaj Rohatgi
Taiichi Saito
Fumihiko Sano
Akashi Satoh
Werner Schindler
Jasper Scholten
Kyoji Shibutani
Takeshi Shimoyama
Taizo Shirai
Dirk Stegemann
Daisuke Suzuki
Jacques Traoré
Dai Watanabe
Brecht Wyseur
Yongjin Yeom
Erik Zenner
Robert Zuccherato

Lecture Notes in Computer Science

For information about Vols. 1–3262

please contact your bookseller or Springer

Vol. 3385: R. Cousot (Ed.), Verification, Model Checking, and Abstract Interpretation. XII, 483 pages. 2004.

Vol. 3382: J. Odell, P. Giorgini, J.P. Müller (Eds.), Agent-Oriented Software Engineering V. X, 239 pages. 2004.

Vol. 3381: M. Bieliková, B. Charon-Bost, O. Sýkora, P. Vojtáš (Eds.), SOFSEM 2005: Theory and Practice of Computer Science. XV, 428 pages. 2004.

Vol. 3363: T. Eiter, L. Libkin (Eds.), Database Theory - ICDT 2005. XI, 413 pages. 2004.

Vol. 3362: G. Barthe, L. Burdy, M. Huisman, J.-L. Lanet, T. Muntean (Eds.), Construction and Analysis of Safe, Secure, and Interoperable Smart Devices. IX, 257 pages. 2004.

Vol. 3360: S. Spaccapietra, E. Bertino, S. Jajodia, R. King, D. McLeod, M.E. Orlowska, L. Strous (Eds.), Journal on Data Semantics II. XI, 233 pages. 2004.

Vol. 3358: J. Cao, L.T. Yang, M. Guo, F. Lau (Eds.), Parallel and Distributed Processing and Applications. XXIV, 1058 pages. 2004.

Vol. 3357: H. Handschuh, M.A. Hasan (Eds.), Selected Areas in Cryptography. XI, 354 pages. 2004.

Vol. 3356: G. Das, V.P. Gulati (Eds.), Intelligent Information Technology. XII, 428 pages. 2004.

Vol. 3353: J. Hromkovič, M. Nagl, B. Westfechtel (Eds.), Graph-Theoretic Concepts in Computer Science. XI, 404 pages. 2004.

Vol. 3350: M. Hermenegildo, D. Cabeza (Eds.), Practical Aspects of Declarative Languages. VIII, 269 pages. 2004.

Vol. 3348: A. Canteaut, K. Viswanathan (Eds.), Progress in Cryptology - INDOCRYPT 2004. XIV, 431 pages. 2004.

Vol. 3347: R.K. Ghosh, H. Mohanty (Eds.), Distributed Computing and Internet Technology. XX, 472 pages. 2004.

Vol. 3344: J. Malenfant, B.M. Østvold (Eds.), Object-Oriented Technology. ECOOP 2004 Workshop Reader. VIII, 215 pages. 2004.

Vol. 3342: E. Şahin, W.M. Spears (Eds.), Swarm Robotics. X, 175 pages. 2004.

Vol. 3341: R. Fleischer, G. Trippen (Eds.), Algorithms and Computation. XVII, 935 pages. 2004.

Vol. 3340: C.S. Calude, E. Calude, M.J. Dinneen (Eds.), Developments in Language Theory. XI, 431 pages. 2004.

Vol. 3339: G.I. Webb, X. Yu (Eds.), AI 2004: Advances in Artificial Intelligence. XXII, 1272 pages. 2004. (Subseries LNAI).

Vol. 3338: S.Z. Li, J. Lai, T. Tan, G. Feng, Y. Wang (Eds.), Advances in Biometric Person Authentication. XVIII, 699 pages. 2004.

Vol. 3337: J.M. Barreiro, F. Martin-Sanchez, V. Maojo, F. Sanz (Eds.), Biological and Medical Data Analysis. XI, 508 pages. 2004.

Vol. 3336: D. Karagiannis, U. Reimer (Eds.), Practical Aspects of Knowledge Management. X, 523 pages. 2004. (Subseries LNAI).

Vol. 3334: Z. Chen, H. Chen, Q. Miao, Y. Fu, E. Fox, E.-p. Lim (Eds.), Digital Libraries: International Collaboration and Cross-Fertilization. XX, 690 pages. 2004.

Vol. 3333: K. Aizawa, Y. Nakamura, S. Satoh (Eds.), Advances in Multimedia Information Processing - PCM 2004, Part III. XXXV, 785 pages. 2004.

Vol. 3332: K. Aizawa, Y. Nakamura, S. Satoh (Eds.), Advances in Multimedia Information Processing - PCM 2004, Part II. XXXVI, 1051 pages. 2004.

Vol. 3331: K. Aizawa, Y. Nakamura, S. Satoh (Eds.), Advances in Multimedia Information Processing - PCM 2004, Part I. XXXVI, 667 pages. 2004.

Vol. 3329: P.J. Lee (Ed.), Advances in Cryptology - ASIACRYPT 2004. XVI, 546 pages. 2004.

Vol. 3328: K. Lodaya, M. Mahajan (Eds.), FSTTCS 2004: Foundations of Software Technology and Theoretical Computer Science. XVI, 532 pages. 2004.

Vol. 3326: A. Sen, N. Das, S.K. Das, B.P. Sinha (Eds.), Distributed Computing - IWDC 2004. XIX, 546 pages. 2004.

Vol. 3323: G. Antoniou, H. Boley (Eds.), Rules and Rule Markup Languages for the Semantic Web. X, 215 pages. 2004.

Vol. 3322: R. Klette, J. Žunić (Eds.), Combinatorial Image Analysis. XII, 760 pages. 2004.

Vol. 3321: M.J. Maher (Ed.), Advances in Computer Science - ASIAN 2004. XII, 510 pages. 2004.

Vol. 3320: K.-M. Liew, H. Shen, S. See, W. Cai (Eds.), Parallel and Distributed Computing: Applications and Technologies. XXIV, 891 pages. 2004.

Vol. 3317: M. Domaratzki, A. Okhotin, K. Salomaa, S. Yu (Eds.), Implementation and Application of Automata. XII, 336 pages. 2004.

Vol. 3316: N.R. Pal, N.K. Kasabov, R.K. Mudi, S. Pal, S.K. Parui (Eds.), Neural Information Processing. XXX, 1368 pages. 2004.

Vol. 3315: C. Lemaître, C.A. Reyes, J.A. González (Eds.), Advances in Artificial Intelligence – IBERAMIA 2004. XX, 987 pages. 2004. (Subseries LNAI).

Vol. 3314: J. Zhang, J.-H. He, Y. Fu (Eds.), Computational and Information Science. XXIV, 1259 pages. 2004.

Vol. 3312: A.J. Hu, A.K. Martin (Eds.), Formal Methods in Computer-Aided Design. XI, 445 pages. 2004.

Vol. 3311: V. Roca, F. Rousseau (Eds.), Interactive Multimedia and Next Generation Networks. XIII, 287 pages. 2004.

Vol. 3309: C.-H. Chi, K.-Y. Lam (Eds.), Content Computing. XII, 510 pages. 2004.

Vol. 3308: J. Davies, W. Schulte, M. Barnett (Eds.), Formal Methods and Software Engineering. XIII, 500 pages. 2004.

Vol. 3307: C. Bussler, S.-k. Hong, W. Jun, R. Kaschek, D.. Kinshuk, S. Krishnaswamy, S.W. Loke, D. Oberle, D. Richards, A. Sharma, Y. Sure, B. Thalheim (Eds.), Web Information Systems – WISE 2004 Workshops. XV, 277 pages. 2004.

Vol. 3306: X. Zhou, S. Su, M.P. Papazoglou, M.E. Orlowska, K.G. Jeffery (Eds.), Web Information Systems – WISE 2004. XVII, 745 pages. 2004.

Vol. 3305: P.M.A. Sloot, B. Chopard, A.G. Hoekstra (Eds.), Cellular Automata. XV, 883 pages. 2004.

Vol. 3303: J.A. López, E. Benfenati, W. Dubitzky (Eds.), Knowledge Exploration in Life Science Informatics. X, 249 pages. 2004. (Subseries LNAI).

Vol. 3302: W.-N. Chin (Ed.), Programming Languages and Systems. XIII, 453 pages. 2004.

Vol. 3300: L. Bertossi, A. Hunter, T. Schaub (Eds.), Inconsistency Tolerance. VII, 295 pages. 2004.

Vol. 3299: F. Wang (Ed.), Automated Technology for Verification and Analysis. XII, 506 pages. 2004.

Vol. 3298: S.A. McIlraith, D. Plexousakis, F. van Harmelen (Eds.), The Semantic Web – ISWC 2004. XXI, 841 pages. 2004.

Vol. 3296: L. Bougé, V.K. Prasanna (Eds.), High Performance Computing - HiPC 2004. XXV, 530 pages. 2004.

Vol. 3295: P. Markopoulos, B. Eggen, E. Aarts, J.L. Crowley (Eds.), Ambient Intelligence. XIII, 388 pages. 2004.

Vol. 3294: C.N. Dean, R.T. Boute (Eds.), Teaching Formal Methods. X, 249 pages. 2004.

Vol. 3293: C.-H. Chi, M. van Steen, C. Wills (Eds.), Web Content Caching and Distribution. IX, 283 pages. 2004.

Vol. 3292: R. Meersman, Z. Tari, A. Corsaro (Eds.), On the Move to Meaningful Internet Systems 2004: OTM 2004 Workshops. XXIII, 885 pages. 2004.

Vol. 3291: R. Meersman, Z. Tari (Eds.), On the Move to Meaningful Internet Systems 2004: CoopIS, DOA, and ODBASE, Part II. XXV, 824 pages. 2004.

Vol. 3290: R. Meersman, Z. Tari (Eds.), On the Move to Meaningful Internet Systems 2004: CoopIS, DOA, and ODBASE, Part I. XXV, 823 pages. 2004.

Vol. 3289: S. Wang, K. Tanaka, S. Zhou, T.W. Ling, J. Guan, D. Yang, F. Grandi, E. Mangina, I.-Y. Song, H.C. Mayr (Eds.), Conceptual Modeling for Advanced Application Domains. XXII, 692 pages. 2004.

Vol. 3288: P. Atzeni, W. Chu, H. Lu, S. Zhou, T.W. Ling (Eds.), Conceptual Modeling – ER 2004. XXI, 869 pages. 2004.

Vol. 3287: A. Sanfeliu, J.F. Martínez Trinidad, J.A. Carrasco Ochoa (Eds.), Progress in Pattern Recognition, Image Analysis and Applications. XVII, 703 pages. 2004.

Vol. 3286: G. Karsai, E. Visser (Eds.), Generative Programming and Component Engineering. XIII, 491 pages. 2004.

Vol. 3285: S. Manandhar, J. Austin, U.B. Desai, Y. Oyanagi, A. Talukder (Eds.), Applied Computing. XII, 334 pages. 2004.

Vol. 3284: A. Karmouch, L. Korba, E.R.M. Madeira (Eds.), Mobility Aware Technologies and Applications. XII, 382 pages. 2004.

Vol. 3283: F.A. Aagesen, C. Anutariya, V. Wuwongse (Eds.), Intelligence in Communication Systems. XIII, 327 pages. 2004.

Vol. 3282: V. Guruswami, List Decoding of Error-Correcting Codes. XIX, 350 pages. 2004.

Vol. 3281: T. Dingsøyr (Ed.), Software Process Improvement. X, 207 pages. 2004.

Vol. 3280: C. Aykanat, T. Dayar, İ. Körpeoğlu (Eds.), Computer and Information Sciences - ISCIS 2004. XVIII, 1009 pages. 2004.

Vol. 3279: G.M. Voelker, S. Shenker (Eds.), Peer-to-Peer Systems III. XI, 300 pages. 2004.

Vol. 3278: A. Sahai, F. Wu (Eds.), Utility Computing. XI, 272 pages. 2004.

Vol. 3275: P. Perner (Ed.), Advances in Data Mining. VIII, 173 pages. 2004. (Subseries LNAI).

Vol. 3274: R. Guerraoui (Ed.), Distributed Computing. XIII, 465 pages. 2004.

Vol. 3273: T. Baar, A. Strohmeier, A. Moreira, S.J. Mellor (Eds.), <<UML>> 2004 - The Unified Modelling Language. XIII, 454 pages. 2004.

Vol. 3272: L. Baresi, S. Dustdar, H. Gall, M. Matera (Eds.), Ubiquitous Mobile Information and Collaboration Systems. VIII, 197 pages. 2004.

Vol. 3271: J. Vicente, D. Hutchison (Eds.), Management of Multimedia Networks and Services. XIII, 335 pages. 2004.

Vol. 3270: M. Jeckle, R. Kowalczyk, P. Braun (Eds.), Grid Services Engineering and Management. X, 165 pages. 2004.

Vol. 3269: J. Lopez, S. Qing, E. Okamoto (Eds.), Information and Communications Security. XI, 564 pages. 2004.

Vol. 3268: W. Lindner, M. Mesiti, C. Türker, Y. Tzitzikas, A. Vakali (Eds.), Current Trends in Database Technology - EDBT 2004 Workshops. XVIII, 608 pages. 2004.

Vol. 3267: C. Priami, P. Quaglia (Eds.), Global Computing. VIII, 377 pages. 2004.

Vol. 3266: J. Solé-Pareta, M. Smirnov, P.V. Mieghem, J. Domingo-Pascual, E. Monteiro, P. Reichl, B. Stiller, R.J. Gibbens (Eds.), Quality of Service in the Emerging Networking Panorama. XVI, 390 pages. 2004.

Vol. 3265: R.E. Frederking, K.B. Taylor (Eds.), Machine Translation: From Real Users to Research. XI, 392 pages. 2004. (Subseries LNAI).

Vol. 3264: G. Paliouras, Y. Sakakibara (Eds.), Grammatical Inference: Algorithms and Applications. XI, 291 pages. 2004. (Subseries LNAI).

Vol. 3263: M. Weske, P. Liggesmeyer (Eds.), Object-Oriented and Internet-Based Technologies. XII, 239 pages. 2004.

Table of Contents

Stream Cipher Cryptanalysis

Side-Channel Analysis

Block Cipher Design

Efficient Implementations

Secret Key Cryptography I

Cryptanalysis

Cryptographic Protocols

Secret Key Cryptography II

An Improved Correlation Attack on A5/1

Alexander Maximov[1], Thomas Johansson[1], and Steve Babbage[2]

[1] Dept. of Information Technology, Lund University, Sweden
[2] Vodafone Group R&D, UK

Abstract. A new approach to attack A5/1 is proposed. The proposed attack is a refinement of a previous attack by Ekdahl and Johansson. We make two important observations that lead to a new attack with improved performance.

1 Introduction

The security of GSM conversation is based on usage of the A5 family of stream ciphers. Many hundred million customers in Europe are protected from the over-the-air piracy by the stronger version in this family, the A5/1 stream cipher. Other customers on other markets use the weaker version A5/2. The approximate design of A5/1 was leaked in 1994, and in 1999 the exact design of both A5/1 and A5/2 was discovered by Briceno [1]. As the result, a lot of investigations of the A5 stream ciphers were done.

The first analysis of the A5/1 cipher resulted in "Guess-and-Determine" type of attacks [2]. Then a time-memory trade-off attack was proposed by Biryukov, Shamir, and Wagner [3], which in some cases can break A5/1 in seconds. Unfortunately, it needs to use a huge precomputational time and about 4 × 73Gb of hard memory. The attack complexity grows exponentially depending on the length of the LFSRs in the design of the cipher. Another attack was presented by Biham and Dunkelman [4]. Their attack breaks the cipher within $2^{39.91}$ A5/1 clocking assuming $2^{20.8}$ bits of keystream available. This attack has expensive assymptotic behaviour. In 2002, Krause, [5] presented a general attack on LFSR-based stream ciphers, called BDD-based cryptanalysis. This attack requires computation complexity of $n^{O(1)}2^{an}, a < 1$ polynomial time operations, where a is a constant depending on the cipher and n is the combined shift registers length. For A5/1, the attack achieves $a = 0.6403$, so the complexity is again exponential in the shift registers length.

A completely different way to attack A5/1 was proposed by Ekdahl and Johansson in 2001 [6]. The attack needs a few minutes for computations, and 2-5 minutes of conversation (plaintext). The idea behind the attack came from correlation attacks. This is the only attack for which the complexity does not grow exponentially with the shift register length.

Finally, very recently Barkan, Biham and Keller [7] investigated the usage of the A5 ciphers in GSM. They demonstrated an active attack where a false base station can intercept a conversation and perform a man in the middle attack. By asking for usage of the weak A5/2 algorithm in the conversation with the

H. Handschuh and A. Hasan (Eds.): SAC 2004, LNCS 3357, pp. 1–18, 2005.

base station and then breaking it, the false base station finds the session key which is also used in the A5/1 protected conversation with the mobile unit. In [7] the authors also propose the passive memory-time trade-off ciphertext only attack. As one of the examples, if 5 minutes of conversation is available, then the attack needs one year of precomputations with 140 computers working together, 22×200GBs hard discs. Then the attack can be done in time 2^{28} by one PC. Obviously, the authors did not try to implement the attack and the complexity was just estimated.

In this paper a new approach to attack the A5/1 stream cipher is proposed. We consider the Ekdahl-Johansson attack as the basis, and apply several new improvements. As the result, the new attack now needs only less then 1 minute of computations, and a few seconds of known conversation. It does not need any notable precomputation time, and needs reasonable space of operation memory.

For the case of a ciphertext-only attack on A5/1, we use the fact that some redundancy is part of the plaintext. There are at least two kinds of redundancy that are explicit and may be used in an attack where only ciphertext is available. *The first* kind is the fact that coding is done before encryption, which results in linear relationships in the plaintext since the parity check symbols are also encrypted. This observation was used in [7]. *The second* kind of redundancy is the fact that during silence, a special frame including a large number of zeros is sent [8]. Silence occurs very often, but unfortunately these frames used for silence are transmitted less frequently, one to initialise a period of silence and then two each second. The attack that we propose can be considered in a ciphertext-only scenario, in which case we use this redundancy during silence to get some known outputs from the cipher.

Although several of the previous attacks are sufficient to break A5/1 in a known plaintext attack, we believe that further progress is very important. The A5/1 stream cipher is perhaps the most used cipher in the world, and from the wireless communication channel interception of the communication is very easy. Mobile base stations are not expensive to buy and they can be used to record GSM conversations.

The paper is organized as follows. In Section 2 a short description of the cipher A5/1 is given. The basic Ekdahl-Johansson attack on A5/1 is briefly described in Section 3. Then, in Section 4, we give new ideas to improve the attack in general. The details and particulars of the attack simulations are described in Section 4.2. Then in Section 5 the results of our simulations are presented.

2 Description of A5/1

A GSM conversation between A and B is a sequence of frames, each sent in about 4.6 milliseconds. Each frame consists of 228 bits – 114 bits of which is the message from A to B, and the second half bits are representing communication from B to A. One session is encrypted with a secret *session key* K. For the jth frame the running key generator is initialised with mixture of K and the publicly known *frame counter*, denoted by F_j. It then generates 228 bits of running key for the current frame. The ciphertext is a binary xor of the running key and the plaintext.

A5/1 consists of 3 LFSRs of lengths 19, 22, and 23, which are denoted R_1, R_2, and R_3, respectively. The LFSRs are clocked in an irregular fashion. Each of them has one tap-bit, C_1, C_2, and C_3, respectively. In each step, 2 or 3 LFSRs are clocked, depending on the current values of the bits C_1, C_2, and C_3. Thus, the clocking control device implements the majority rule, shown in the table on the right. Note, for each step the probability that an individual LFSR is being clocked is 3/4.

values of			clocking		
C_1	C_2	C_3	R_1	R_2	R_3
$1 \oplus c$	c	c	×	√	√
c	$1 \oplus c$	c	√	×	√
c	c	$1 \oplus c$	√	√	×
c	c	c	√	√	√

After the initialisation procedure for the LFSRs, 228 bits of running key are produced, using irregular clocking. In each step one bit of the running key is calculated as the binary xor of the current output bits from the LFSRs.

The initialisation process uses the session key K and the known frame counter F_n. First the LFSRs are initialised to zero. They are then clocked 64 times, ignoring the irregular clocking, and the key bits of K are consecutively xored in parallel to the feedback of each of the registers. In the second step the LFSRs are clocked 22 times, ignoring the irregular clocking, and the successive bits of F_n are again xored in parallel to the feedback of the LFSRs. Let us call the state of LFSRs at this time the *initial state* of the frame. In the third step the LFSRs are clocked 100 times *with* irregular clocking, but ignoring outputs. Then, the LFSRs are clocked 228 times with the irregular clocking, producing 228 bits of the running key. For a more detailed description of A5/1 we refer to [1].

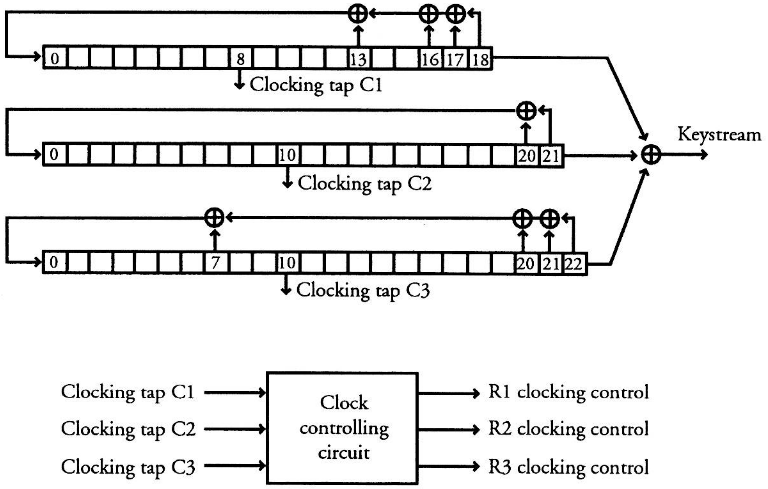

Fig. 1. The structure of A5/1 cipher

3 A Short Description of the Ekdahl-Johansson Attack on A5/1

This attack was proposed in 2002 by Ekdahl and Johansson. The idea behind the attack came from correlation attacks, and is based on the linearity of the initialisation procedure. The attack needs a set of m frames (about 20000-50000 in their attack), during one session, i.e., when the session key K is not changed.

For notation purposes, let the key $K = (k_1, \ldots, k_{64})$, and the frame counter $F_j = (f_1, \ldots, f_{22})$, where $k_i, f_j \in \mathbf{F}_2$, $i = 1..64, j = 1..22$. Denote by $u_1^j(l_1)$, $u_2^j(l_2)$, and $u_3^j(l_3)$ the output bits of LFSRs, if they are independently *clocked* l_1, l_2, and l_3 times, respectively, *after* the LFSRs being in the initial state, and when the current frame is number j. The 228 bits of the running key are then denoted as $v^j(101), \ldots, v^j(100+228)$, and every $v^j(t) = u_1^j(l_1) \oplus u_2^j(l_2) \oplus u_3^j(l_3)$, for *some unknown* l_1, l_2, l_3.

Note, that $u_1^j(l_1)$ is a linear combination of K and F_j bits, since all operations before the initial state are linear. I.e., $u_1^j(l_1)$ can be represented as $u_1^j(l_1) = X_{1,l_1}(F_j) + Y_{1,l_1}(K)$, where $X_{1,l_1}(F_j)$ is a known fixed value and $Y_{1,l_1}(K) = \sum_{i=1}^{64} y_{1,l_1,i} \cdot k_i$ is a linear function with known coefficients $y_{1,l_1,i} \in \mathbf{F}_2$.

With the same arguments we define

$$\begin{aligned} u_1^j(l_1) &= X_{1,l_1}(F_j) + Y_{1,l_1}(K), \\ u_2^j(l_2) &= X_{2,l_2}(F_j) + Y_{2,l_2}(K), \\ u_3^j(l_3) &= X_{3,l_3}(F_j) + Y_{3,l_3}(K), \end{aligned}$$

where $X_{a,l_a}(F_j)$ and the coefficients $y_{a,l_a,i} \in \mathbf{F}_2$, for $a = 1, 2, 3$, $l_a = 0, 1, \ldots, 100+228$, $i = 1, \ldots, 64$ are precomputed and fixed. Let us write

$$s_1(l_1) = Y_{1,l_1}(K), \qquad s_2(l_2) = Y_{2,l_2}(K), \qquad s_3(l_3) = Y_{3,l_3}(K). \tag{1}$$

Our target is to estimate 19 bits from the first LFSR $s_1(0), \ldots, s_1(18)$, 22 bits from the second LFSR $s_2(0), \ldots, s_2(21)$, and 23 bits from the third LFSR $s_3(0), \ldots, s_3(22)$. These 64 bits map one-to-one to 64 bits of the key K, if the frame counter F_j is given.

For notation purposes we write $E \overset{p}{=} \hat{E}$, when $\hat{E}$ appears to be an estimator for E, such that $\Pr\{E = \hat{E}\} = p$, for some probability p. $\hat{E}$ can be derived from accessible data, or assumed (guessed).

One can think about the data we have access to as a binary table of m frames in the form

$$\begin{pmatrix} v^1(101) & v^1(102) & \ldots & v^1(100+228) \\ v^2(101) & v^2(102) & \ldots & v^2(100+228) \\ & & \vdots & \\ v^m(101) & v^m(102) & \ldots & v^m(100+228) \end{pmatrix}.$$

The idea behind the attack is to observe that $v^j(101) \overset{p}{=} s_1(l_1) + s_2(l_2) + s_3(l_3) + X_{1,l_1}(F_j) + X_{2,l_2}(F_j) + X_{3,l_3}(F_j)$ for some $p \neq 1/2$, if l_1, l_2, l_3 are chosen properly. The probability $p = \frac{1}{2} + \frac{1}{2}\Pr\{(l_1, l_2, l_3) \text{ at time } t\}$, where $\Pr\{(l_1, l_2, l_3) \text{ at time } t\}$ is the probability that at time 101 the LFSRs were