Carlisle Adams
Ali Miri
Michael Wiener (Eds.)

LNCS 4876

Selected Areas in Cryptography

14th International Workshop, SAC 2007
Ottawa, Canada, August 2007
Revised Selected Papers

Carlisle Adams Ali Miri Michael Wiener (Eds.)

Selected Areas in Cryptography

14th International Workshop, SAC 2007
Ottawa, Canada, August 16-17, 2007
Revised Selected Papers

Springer

Volume Editors

Carlisle Adams
University of Ottawa, School of Information Technology and Engineering (SITE)
SITE Building, 800 King Edward Avenue, Ottawa, Ontario K1N 6N5, Canada
E-mail: cadams@site.uottawa.ca

Ali Miri
University of Ottawa, School of Information Technology and Engineering (SITE)
and Department of Mathematics and Statistics
Colonel By Hall (CBY), 161 Louis Pasture Street, Ottawa, Ontario K1N 6N5, Canada
E-mail: samiri@site.uottawa.ca

Michael Wiener
Cryptographic Clarity
20 Hennepin Street, Nepean, Ontario K2J 3Z4, Canada
E-mail: michael.james.wiener@gmail.com

Library of Congress Control Number: 2007941250

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

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-77359-2 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-77359-7 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12206629 06/3180 5 4 3 2 1 0

Lecture Notes in Computer Science 4876

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

Preface

SAC 2007 was the 14th in a series of annual workshops on Selected Areas in Cryptography. This is the first time this workshop was held at the University of Ottawa. Previous workshops were held at Queen's University in Kingston (1994, 1996, 1998, 1999, and 2005), Carleton University in Ottawa (1995, 1997, and 2003), University of Waterloo (2000 and 2004), Fields Institute in Toronto (2001), Memorial University of Newfoundland in St. Johns (2002), and Concordia University in Montreal (2006). The intent of the workshop is to provide a stimulating atmosphere where researchers in cryptology can present and discuss new work on selected areas of current interest. The themes for SAC 2007 were:

- Design and analysis of symmetric key cryptosystems
- Primitives for symmetric key cryptography, including block and stream ciphers, hash functions, and MAC algorithms
- Efficient implementations of symmetric and public key algorithms
- Innovative cryptographic defenses against malicious software

A total of 73 papers were submitted to SAC 2007. Of these, one was withdrawn by the authors, and 25 were accepted by the Program Committee for presentation at the workshop. In addition to these presentations, we were fortunate to have two invited speakers:

- Dan Bernstein: "Edwards Coordinates for Elliptic Curves"
- Moti Yung: "Cryptography and Virology Inter-Relationships." This talk was designated the Stafford Tavares Lecture.

We are grateful to the Program Committee and the many external reviewers for their hard work and expertise in selecting the program. They completed all reviews in time for discussion and final decisions despite events conspiring to compress the review schedule. We apologize if anyone was missed in the list of external reviewers.

We would like to thank the Ontario Research Network for Electronic Commerce (ORNEC) for financial support of the workshop. We would also like to thank Gail Deduk for administrative support and Aleks Essex and Terasan Niyomsataya for technical support.

Finally, we thank all those who submitted papers and the conference participants who made this year's workshop a great success.

October 2007

Carlisle Adams
Ali Miri
Michael Wiener

14th Annual Workshop on Selected Areas in Cryptography

August 16–17, 2007, Ottawa, Ontario, Canada

in cooperation with the
International Association for Cryptologic Research (IACR)

Conference Co-chairs

Carlisle Adams	University of Ottawa, Canada
Ali Miri	University of Ottawa, Canada
Michael Wiener	Cryptographic Clarity, Canada

Program Committee

Roberto Avanzi	Ruhr University Bochum, Germany
Orr Dunkelman	Katholieke Universiteit Leuven, Belgium
Ian Goldberg	University of Waterloo, Canada
Helena Handschuh	Spansion, France
M. Anwar Hasan	University of Waterloo, Canada
Antoine Joux	DGA, Université de Versailles St-Quentin-en-Yvelines, France
Pascal Junod	Nagravision, Switzerland
Tanja Lange	Technische Universiteit, Eindhoven, Netherlands
Arjen Lenstra	EPFL, Switzerland
Christof Paar	Ruhr University Bochum, Germany
Bart Preneel	Katholieke Universiteit Leuven, Belgium
Vincent Rijmen	Graz University of Technology, Austria
Matt Robshaw	France Telecom, France
Greg Rose	QUALCOMM, USA
Doug Stinson	University of Waterloo, Canada
Serge Vaudenay	EPFL, Switzerland
Robert Zuccherato	Entrust Inc., Canada

External Reviewers

Abdulaziz Alkhoraidly	Elena Andreeva	Thomas Baignères
Siavash Bayat-Sarmadi	Anja Becker	Côme Berbain
Daniel J. Bernstein	Eli Biham	Olivier Billet
Toni Bluher	Andrey Bogdanov	Reinier Broker

Christophe De Cannière
Scott Contini
Thomas Eisenbarth
Matthieu Finiasz
Jovan Golić
Arash Hariri
Laurent Imbert
David Jacobson
Alexandre Karlov
Cédric Lauradoux
Reynald Lercier
Marine Minier
Dag Arne Osvik
Souradyuti Paul
Emmanuel Prouff
Kai Schramm
Marc Stevens
Martin Vuagnoux
Huapeng Wu
Yaniv Carmeli
Christophe Doche
Lars Elmegaard-Fessel
Steven Galbraith
Johann Groβschädl
Phil Hawkes
Sebastiaan Indesteege
Shaoquan Jiang
Shahram Khazaei
Gregor Leander
Cameron McDonald
Bodo Möller
Elisabeth Oswald
Raphael Phan
Christian Rechberger
Yaniv Shaked
Nicolas Theriault
Johannes Wolkerstorfer
Brecht Wyseur
Jaewook Chung
Nevine Ebeid
Andreas Enge
Henri Gilbert
Tim Guneysu
Rafi Hen
Takanori Isobe
Marcelo Kaihara
Mario Lamberger
Kerstin Lemke
Florian Mendel
Jean Monnerat
Sylvain Pasini
Norbert Pramstaller
Arash Reyhani-Masoleh
Martijn Stam
Frederik Vercauteren
Hongjun Wu
Lu Xiao

Lecture Notes in Computer Science

Sublibrary 4: Security and Cryptology

Vol. 4887: S.D. Galbraith (Ed.), Cryptography and Coding. XI, 423 pages. 2007.

Vol. 4876: C. Adams, A. Miri, M. Wiener (Eds.), Selected Areas in Cryptography. X, 409 pages. 2007.

Vol. 4861: S. Qing, H. Imai, G. Wang (Eds.), Information and Communications Security. XIV, 508 pages. 2007.

Vol. 4859: K. Srinathan, C.P. Rangan, M. Yung (Eds.), Progress in Cryptology – INDOCRYPT 2007. XI, 426 pages. 2007.

Vol. 4856: F. Bao, S. Ling, T. Okamoto, H. Wang, C. Xing (Eds.), Cryptology and Network Security. XII, 283 pages. 2007.

Vol. 4833: K. Kurosawa (Ed.), Advances in Cryptology – ASIACRYPT 2007. XIV, 583 pages. 2007.

Vol. 4817: K.-H. Nam, G. Rhee (Eds.), Information Security and Cryptology - ICISC 2007. XIII, 367 pages. 2007.

Vol. 4812: P. McDaniel, S.K. Gupta (Eds.), Information Systems Security. XIII, 322 pages. 2007.

Vol. 4784: W. Susilo, J.K. Liu, Y. Mu (Eds.), Provable Security. X, 237 pages. 2007.

Vol. 4779: J.A. Garay, A.K. Lenstra, M. Mambo, R. Peralta (Eds.), Information Security. XIII, 437 pages. 2007.

Vol. 4776: N. Borisov, P. Golle (Eds.), Privacy Enhancing Technologies. X, 273 pages. 2007.

Vol. 4752: A. Miyaji, H. Kikuchi, K. Rannenberg (Eds.), Advances in Information and Computer Security. XIII, 460 pages. 2007.

Vol. 4734: J. Biskup, J. López (Eds.), Computer Security – ESORICS 2007. XIV, 628 pages. 2007.

Vol. 4727: P. Paillier, I. Verbauwhede (Eds.), Cryptographic Hardware and Embedded Systems - CHES 2007. XIV, 468 pages. 2007.

Vol. 4691: T. Dimitrakos, F. Martinelli, P.Y.A. Ryan, S. Schneider (Eds.), Formal Aspects in Security and Trust. VIII, 285 pages. 2007.

Vol. 4677: A. Aldini, R. Gorrieri (Eds.), Foundations of Security Analysis and Design IV. VII, 325 pages. 2007.

Vol. 4657: C. Lambrinoudakis, G. Pernul, A.M. Tjoa (Eds.), Trust, Privacy and Security in Digital Business. XIII, 291 pages. 2007.

Vol. 4637: C. Kruegel, R. Lippmann, A. Clark (Eds.), Recent Advances in Intrusion Detection. XII, 337 pages. 2007.

Vol. 4631: B. Christianson, B. Crispo, J.A. Malcolm, M. Roe (Eds.), Security Protocols. IX, 347 pages. 2007.

Vol. 4622: A. Menezes (Ed.), Advances in Cryptology - CRYPTO 2007. XIV, 631 pages. 2007.

Vol. 4593: A. Biryukov (Ed.), Fast Software Encryption. XI, 467 pages. 2007.

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

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

Vol. 4579: B.M. Hämmerli, R. Sommer (Eds.), Detection of Intrusions and Malware, and Vulnerability Assessment. X, 251 pages. 2007.

Vol. 4575: T. Takagi, T. Okamoto, E. Okamoto, T. Okamoto (Eds.), Pairing-Based Cryptography – Pairing 2007. XI, 408 pages. 2007.

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

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

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

Vol. 4464: E. Dawson, D.S. Wong (Eds.), Information Security Practice and Experience. XIII, 361 pages. 2007.

Vol. 4462: D. Sauveron, K. Markantonakis, A. Bilas, J.-J. Quisquater (Eds.), Information Security Theory and Practices. XII, 255 pages. 2007.

Vol. 4450: T. Okamoto, X. Wang (Eds.), Public Key Cryptography – PKC 2007. XIII, 491 pages. 2007.

Vol. 4437: J.L. Camenisch, C.S. Collberg, N.F. Johnson, P. Sallee (Eds.), Information Hiding. VIII, 389 pages. 2007.

Vol. 4392: S.P. Vadhan (Ed.), Theory of Cryptography. XI, 595 pages. 2007.

Vol. 4377: M. Abe (Ed.), Topics in Cryptology – CT-RSA 2007. XI, 403 pages. 2006.

Vol. 4356: E. Biham, A.M. Youssef (Eds.), Selected Areas in Cryptography. XI, 395 pages. 2007.

Vol. 4341: P.Q. Nguyên (Ed.), Progress in Cryptology - VIETCRYPT 2006. XI, 385 pages. 2006.

Vol. 4332: A. Bagchi, V. Atluri (Eds.), Information Systems Security. XV, 382 pages. 2006.

Vol. 4329: R. Barua, T. Lange (Eds.), Progress in Cryptology - INDOCRYPT 2006. X, 454 pages. 2006.

Vol. 4318: H. Lipmaa, M. Yung, D. Lin (Eds.), Information Security and Cryptology. XI, 305 pages. 2006.

Vol. 4307: P. Ning, S. Qing, N. Li (Eds.), Information and Communications Security. XIV, 558 pages. 2006.

Vol. 4301: D. Pointcheval, Y. Mu, K. Chen (Eds.), Cryptology and Network Security. XIII, 381 pages. 2006.

Vol. 4300: Y.Q. Shi (Ed.), Transactions on Data Hiding and Multimedia Security I. IX, 139 pages. 2006.

Vol. 4298: J.K. Lee, O. Yi, M. Yung (Eds.), Information Security Applications. XIV, 406 pages. 2007.

Vol. 4296: M.S. Rhee, B. Lee (Eds.), Information Security and Cryptology – ICISC 2006. XIII, 358 pages. 2006.

Vol. 4284: X. Lai, K. Chen (Eds.), Advances in Cryptology – ASIACRYPT 2006. XIV, 468 pages. 2006.

Vol. 4283: Y.Q. Shi, B. Jeon (Eds.), Digital Watermarking. XII, 474 pages. 2006.

Vol. 4266: H. Yoshiura, K. Sakurai, K. Rannenberg, Y. Murayama, S.-i. Kawamura (Eds.), Advances in Information and Computer Security. XIII, 438 pages. 2006.

Vol. 4258: G. Danezis, P. Golle (Eds.), Privacy Enhancing Technologies. VIII, 431 pages. 2006.

Vol. 4249: L. Goubin, M. Matsui (Eds.), Cryptographic Hardware and Embedded Systems - CHES 2006. XII, 462 pages. 2006.

Vol. 4237: H. Leitold, E.P. Markatos (Eds.), Communications and Multimedia Security. XII, 253 pages. 2006.

Vol. 4236: L. Breveglieri, I. Koren, D. Naccache, J.-P. Seifert (Eds.), Fault Diagnosis and Tolerance in Cryptography. XIII, 253 pages. 2006.

Vol. 4219: D. Zamboni, C. Krügel (Eds.), Recent Advances in Intrusion Detection. XII, 331 pages. 2006.

Vol. 4189: D. Gollmann, J. Meier, A. Sabelfeld (Eds.), Computer Security – ESORICS 2006. XI, 548 pages. 2006.

Vol. 4176: S.K. Katsikas, J. López, M. Backes, S. Gritzalis, B. Preneel (Eds.), Information Security. XIV, 548 pages. 2006.

Vol. 4117: C. Dwork (Ed.), Advances in Cryptology - CRYPTO 2006. XIII, 621 pages. 2006.

Vol. 4116: R. De Prisco, M. Yung (Eds.), Security and Cryptography for Networks. XI, 366 pages. 2006.

Vol. 4107: G. Di Crescenzo, A. Rubin (Eds.), Financial Cryptography and Data Security. XI, 327 pages. 2006.

Vol. 4083: S. Fischer-Hübner, S. Furnell, C. Lambrinoudakis (Eds.), Trust and Privacy in Digital Business. XIII, 243 pages. 2006.

Vol. 4064: R. Büschkes, P. Laskov (Eds.), Detection of Intrusions and Malware & Vulnerability Assessment. X, 195 pages. 2006.

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

Vol. 4047: M.J.B. Robshaw (Ed.), Fast Software Encryption. XI, 434 pages. 2006.

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

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

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

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

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

Vol. 3958: M. Yung, Y. Dodis, A. Kiayias, T.G. Malkin (Eds.), Public Key Cryptography - PKC 2006. XIV, 543 pages. 2006.

Vol. 3957: B. Christianson, B. Crispo, J.A. Malcolm, M. Roe (Eds.), Security Protocols. IX, 325 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. 3935: D.H. Won, S. Kim (Eds.), Information Security and Cryptology - ICISC 2005. XIV, 458 pages. 2006.

Vol. 3934: J.A. Clark, R.F. Paige, F.A.C. Polack, P.J. Brooke (Eds.), Security in Pervasive Computing. X, 243 pages. 2006.

Vol. 3928: J. Domingo-Ferrer, J. Posegga, D. Schreckling (Eds.), Smart Card Research and Advanced Applications. XI, 359 pages. 2006.

Vol. 3919: R. Safavi-Naini, M. Yung (Eds.), Digital Rights Management. XI, 357 pages. 2006.

Vol. 3903: K. Chen, R. Deng, X. Lai, J. Zhou (Eds.), Information Security Practice and Experience. XIV, 392 pages. 2006.

Vol. 3897: B. Preneel, S. Tavares (Eds.), Selected Areas in Cryptography. XI, 371 pages. 2006.

Vol. 3876: S. Halevi, T. Rabin (Eds.), Theory of Cryptography. XI, 617 pages. 2006.

Vol. 3866: T. Dimitrakos, F. Martinelli, P.Y.A. Ryan, S. Schneider (Eds.), Formal Aspects in Security and Trust. X, 259 pages. 2006.

Vol. 3860: D. Pointcheval (Ed.), Topics in Cryptology – CT-RSA 2006. XI, 365 pages. 2006.

Vol. 3858: A. Valdes, D. Zamboni (Eds.), Recent Advances in Intrusion Detection. X, 351 pages. 2006.

Vol. 3856: G. Danezis, D. Martin (Eds.), Privacy Enhancing Technologies. VIII, 273 pages. 2006.

Vol. 3786: J.-S. Song, T. Kwon, M. Yung (Eds.), Information Security Applications. XI, 378 pages. 2006.

Vol. 3108: H. Wang, J. Pieprzyk, V. Varadharajan (Eds.), Information Security and Privacy. XII, 494 pages. 2004.

Vol. 2951: M. Naor (Ed.), Theory of Cryptography. XI, 523 pages. 2004.

Vol. 2742: R.N. Wright (Ed.), Financial Cryptography. VIII, 321 pages. 2003.

¥495.00元

Table of Contents

Reduced Complexity Attacks on the Alternating Step Generator

Shahram Khazaei[1], Simon Fischer[2], and Willi Meier[2]

[1] EPFL, Lausanne, Switzerland
[2] FHNW, Windisch, Switzerland

Abstract. In this paper, we present some reduced complexity attacks on the Alternating Step Generator (ASG). The attacks are based on a quite general framework and mostly benefit from the low sampling resistance of the ASG, and of an abnormal behavior related to the distribution of the initial states of the stop/go LFSR's which produce a given segment of the output sequence. Our results compare well with previous results as they show a greater flexibility with regard to known output of the ASG, which amounts in reduced complexity. We will also give a closed form for the complexity of attacks on ASG (and SG) as presented in [13].

Keywords: Stream Cipher, Clock-Controlled Generator, Alternating Step Generator.

1 Introduction

The Alternating Step Generator (ASG), a well-known stream cipher proposed in [11], consists of two stop/go clocked binary LFSR's, $\mathsf{LFSR_X}$ and $\mathsf{LFSR_Y}$, and a regularly clocked binary LFSR, $\mathsf{LFSR_C}$ of which the clock-control sequence is derived. The original description of ASG [11] is as follows. At each time, the clock-control bit determines which of the two stop/go LFSR's is clocked, and the output sequence is obtained as bit-wise sum of the two stop/go clocked LFSR sequences. It is known [13, 8, 12] that instead of working with the original definition of ASG we can consider a slightly different description for which the output is taken from the stop/go LFSR which has been clocked. More precisely, at each step first $\mathsf{LFSR_C}$ is clocked; then if the output bit of $\mathsf{LFSR_C}$ is one, $\mathsf{LFSR_X}$ is clocked and its output bit is considered as the output bit of the generator, otherwise $\mathsf{LFSR_Y}$ is clocked and the output bit of the generator is taken from this LFSR. Since in a cryptanalysis point of view these two generators are equivalent, we use the later one all over this paper and for simplicity we still call it ASG.

Several attacks have been proposed on ASG in the literature. Most of these attacks are applied in a divide-and-conquer based procedure targeting one or two of the involved LFSR's. We will focus on a divide-and-conquer attack which targets one of the two stop/go LFSR's.

A correlation attack on individual $\mathsf{LFSR_X}$ or $\mathsf{LFSR_Y}$ which is based on a specific edit probability has been introduced in [10]. The amount of required keystream is linear in terms of the length of the targeted LFSR and the correct initial state

C. Adams, A. Miri, and M. Wiener (Eds.): SAC 2007, LNCS 4876, pp. 1–16, 2007.

of the targeted LFSR is found through an exhaustive search over all possible initial states. In [13] some reduced complexity attacks on ASG and SG (Shrinking Generator, see [2]) were presented and the effectiveness of the attacks was verified numerically for SG while only few general ideas were proposed for ASG without any numerical or theoretical analysis. These methods avoid exhaustive search over all initial states, however, the amount of needed keystream is exponential in terms of the length of the targeted LFSR. One of our contributions of this paper is to give a closed form for these reduced complexity attacks.

Our major objective of this paper is to investigate a general method which does not perform an exhaustive search over all possible initial states of the targeted LFSR. We will take advantage of the low *sampling resistance* of ASG. The notion of sampling resistance was first introduced in [1] and it was shown that a low sampling resistance has a big impact on the efficiency of time/memory/data trade-off attacks. Sampling is the capability of efficiently producing all the initial states which generate an output sequence starting with a particular m-bit pattern. Recently it was noticed that sampling may be useful along with other attacks in a unified framework [3]. The results of this paper represent a positive attempt to exploit such a connection for a concrete stream cipher.

For ASG, sampling is easy if the output length m is chosen to be about the total length of the two stop/go LFSR's. Another weakness of ASG which enables us to mount our attack is that different initial states of any of the two stop/go LFSR's have far different probabilities to be accepted as a candidate which can produce a given segment of length m of the output sequence. Systematic computer simulations confirm this striking behavior. The highly non-uniform distribution of different initial states of any of the stop/go LFSR's is valid for any segment of length about m, and the effect is more abnormal for some special outputs which we refer to as weak outputs. Thanks to the low sampling resistance of ASG we first try to find a subset of the most probable initial states which contains the correct one, then using the probabilistic edit distance [10] we distinguish the correct initial state. Our general approach can be faster than exhaustive search even if the amount of keystream is linear in terms of the length of the targeted LFSR, improving the results in [10]. With regard to reduced complexity attacks, our approach does assume less restricted output segments than in [13], a fact that has been confirmed by large-scale experiments. This enables attacks with significantly lower data complexity even for large instances of ASG (whereas asymptotical complexity is shown to be comparable over known methods).

The paper is organized as follows. In section 2 we will give a comprehensive list of the known attacks on ASG along with a short overview of them. A closed form for the reduced complexity attacks of [13] on ASG is given in Sect. 3. In Sect. 4 we present our attack in detail. Experimental results are in Sect. 5, and we finally conclude in Sect. 6.

2 Previous Attacks on ASG

Several attacks have been proposed on the ASG in the literature. This section will provide an overview of the different attacks. We will denote the length of

registers $\mathsf{LFSR_C}$, $\mathsf{LFSR_X}$ and $\mathsf{LFSR_Y}$ by L_C, L_X and L_Y, respectively. If we only use parameter L, we apply the simplification $L := L_C = L_X = L_Y$.

2.1 Divide-and-Conquer Linear Consistency Attack

It is shown in [11] that the initial state of $\mathsf{LFSR_C}$ can be recovered by targeting its initial state in a divide-and-conquer based attack based on the fact that the output sequence of the ASG can be split into the regularly clocked $\mathsf{LFSR_X}$ and $\mathsf{LFSR_Y}$ sequences, which are then easily tested for low linear complexity. Hence the complexity of this attack is $\mathcal{O}(\min^2(L_X, L_Y)2^{L_C})$ assuming that only the feedback polynomial of $\mathsf{LFSR_C}$ is available. Under the assumption that the feedback polynomial of all LFSR's are available, which is the basic assumption of all other known attacks (including ours in this paper), the complexity of this attack would be $\mathcal{O}(\min(L_X, L_Y)2^{L_C})$ instead, since a parity check test can be used in place of linear complexity test. In this case the attack is a linear consistency attack [17]. We will use the idea of this attack to sample ASG in Sect. 4.1.

2.2 Edit Distance Correlation Attack

A correlation attack on $\mathsf{LFSR_X}$ and $\mathsf{LFSR_Y}$ combined, which is based on a specific edit distance, was proposed in [8]. If the initial states of $\mathsf{LFSR_X}$ and $\mathsf{LFSR_Y}$ are guessed correctly, the edit distance is equal to zero. If the guess is incorrect, the probability of obtaining the zero edit distance was experimentally shown to exponentially decrease in the length of the output string. Later, a theoretical analysis of this attack was developed in [12, 5]. The minimum length of the output string to be successful for an attack is about four times total lengths of $\mathsf{LFSR_X}$ and $\mathsf{LFSR_Y}$. As the complexity of computing the edit distance is quadratic in the length of the output string, the complexity of this attack is $\mathcal{O}((L_X + L_Y)^2 2^{L_X+L_Y})$. In addition, it was shown that the initial state of $\mathsf{LFSR_C}$ can then be reconstructed with complexity $\mathcal{O}(2^{0.27L_C})$.

2.3 Edit Probability Correlation Attack

A correlation attack on individual $\mathsf{LFSR_X}$ or $\mathsf{LFSR_Y}$ which is based on a specific edit probability was developed in [10]. For a similar approach, see [13]. The edit probability is defined for two binary strings: an input string, produced by the regularly clocked targeted LFSR from an assumed initial state, and a given segment of the ASG output sequence. The edit probability is defined as the probability that the given output string is produced from an assumed input string by the ASG in a probabilistic model, where the LFSR sequences are assumed to be independent and purely random. It turns out that the edit probability tends to be larger when the guess about the LFSR initial state is correct. More precisely, by experimental analysis of the underlying statistical hypothesis testing problem, it was shown that the minimum length of the output string to be successful for an attack is about forty lengths of the targeted LFSR. As the complexity of computing the edit probability is quadratic in the length of

the output string, the complexity of reconstructing both LFSR initial states is $\mathcal{O}(\max^2(L_X, L_Y)2^{\max(L_X,L_Y)})$. This yields a considerable improvement over the edit distance correlation attack if L_X and L_Y are approximately equal and relatively large, as is typically suggested (for example, see, [15]).

Remark 1. Note that "edit distance correlation attack" means that the initial states of $\mathsf{LFSR_X}$ and $\mathsf{LFSR_Y}$ can be recovered regardless of the unknown initial state of $\mathsf{LFSR_C}$, whereas "edit probability correlation attack" means that the initial state of $\mathsf{LFSR_X}$ ($\mathsf{LFSR_Y}$) can be recovered regardless of unknown initial states of $\mathsf{LFSR_Y}$ ($\mathsf{LFSR_X}$) and $\mathsf{LFSR_C}$. However, the targeted LFSR initial states should be tested exhaustively. The main motivation for this paper is to investigate if the initial states of $\mathsf{LFSR_X}$ ($\mathsf{LFSR_Y}$) can be reconstructed faster than exhaustive search regardless of unknown initial states of $\mathsf{LFSR_Y}$ ($\mathsf{LFSR_X}$) and $\mathsf{LFSR_C}$.

2.4 Reduced Complexity Attacks

A first step to faster reconstruction of LFSR's initial states was suggested in [13], in which some reduced complexity attacks on ASG and SG are presented. In the next section, we will give a general expression in the parameter L_X, the length of target register $\mathsf{LFSR_X}$ (and in Appendix A, we give general expressions for SG). A second movement to faster reconstruction of LFSR initial states was suggested in [7], using an approach based on computing the posterior probabilities of individual bits of the regularly clocked $\mathsf{LFSR_X}$ and $\mathsf{LFSR_Y}$ sequences, when conditioned on a given segment of the output sequence. It is shown that these probabilities can be efficiently computed and the deviation of posterior probabilities from one half are theoretically analysed. As these probabilities represent soft-valued estimates of the corresponding bits of the considered LFSR sequences when regularly clocked, it is argued that the initial state reconstruction is thus in principle reduced to fast correlation attacks on regularly clocked LFSR's such as the ones based on iterative probabilistic decoding algorithms. Although this valuable work shows some vulnerability of the ASG towards fast correlation attacks, the practical use of these probabilities has not yet been deeply investigated. Nonetheless, these posterior probabilities can certainly be used to mount a distinguisher on ASG. This can be compared with [4], a similar work on SG for which a distinguisher was later developed in [9].

3 Johansson's Reduced Complexity Attacks

In [13] some reduced complexity attacks on the ASG and SG were presented, and the effectiveness of the attacks was verified numerically for the SG (while only few general ideas were proposed for the ASG without any numerical or theoretical analysis). We give a closed form for the reduced complexity attack on ASG, using the approximation $\binom{n}{w} \approx 2^{nh(w/n)}$ where $h(p)$ is the binary entropy function defined as

$$h(p) := -p\log_2(p) - (1-p)\log_2(1-p)\ . \tag{1}$$

In the first scenario, the attacker waits for a segment of M consecutive zeros (or ones) in the output sequence and assumes that exactly $M/2$ of them are from $\mathsf{LFSR_X}$. This is true with probability $\beta = \binom{M}{M/2}2^{-M}$. The remaining $L-M/2$ bits of $\mathsf{LFSR_X}$ are then found by exhaustive search. Time and data complexities of this attack are $C_T = L^2 2^{L-M/2}\beta^{-1} = L^2 2^{L+M/2}\binom{M}{M/2}^{-1}$ and $C_D = 2^{M-1}\beta^{-1} = 2^{2M-1}\binom{M}{M/2}^{-1}$ (using overlapping blocks of keystream). Ignoring the polynomial and constant terms and equaling the time and data complexities, we have $L - M/2 = M$, which shows $M = \frac{2}{3}L$. Thus the optimal complexities of this attack are $C_T = \mathcal{O}(L^2 2^{\frac{2}{3}L})$ and $C_D = \mathcal{O}(2^{\frac{2}{3}L})$. These arguments apply to both $\mathsf{LFSR_X}$ and $\mathsf{LFSR_Y}$.

Remark 2. The total time of the attack is composed of the time to filter the blocks of data with desired properties, and of the time to further process the filtered blocks. Although the unit of examination time of these two phases are not equal, we ignore this difference to simplify the analysis.

In another scenario in [13], it is suggested to wait for a segment of length M containing at most w ones (zeros) and make the assumption that only half of the zeros (ones) come from the $\mathsf{LFSR_X}$. All the ones (zeros) and the remaining zeros (ones) are assumed to come from the $\mathsf{LFSR_Y}$. This is true with probability $\beta = 2^{-w}\binom{M-w}{(M-w)/2}2^{-(M-w)}$. The time and data complexities of this attack are then $C_T = L^2 2^{L-(M-w)/2}\beta^{-1}$ and $C_D = 2^{M-1}\binom{M}{w}^{-1}\beta^{-1}$, respectively. With $w := \alpha M$, ignoring the constant and polynomial terms, and equaling the time and data complexities, we have $L-(1-\alpha)M/2+\alpha M = M-h(\alpha)M+\alpha M$, which results in $M = L/(3/2-\alpha/2-h(\alpha))$. The minimum value of the exponents $M(1-h(\alpha)+\alpha)$ is $0.6406L$, which is achieved for $\alpha \approx 0.0727$ (and hence $M = 0.9193L$ and $w = 0.0668L$). Therefore, the optimal complexities are $C_T = \mathcal{O}(L^2 2^{0.64L})$ and $C_D = \mathcal{O}(2^{0.64L})$. Note that this complexity is only for reconstruction of the initial state of $\mathsf{LFSR_X}$. The complexity for recovering the initial state of $\mathsf{LFSR_Y}$ highly depends on the position of ones (zeros) in the block. In the best case, the block starts with w ones (zeros) and the complexity becomes $C_T = L^2 2^{L-(M+w)/2}$. In the worst case, the attacker has to search for the positions of ones (zeros), and the complexity becomes $C_T = \binom{(M+w)/2}{w}L^2 2^{L-(M-w)/2}$. It is difficult to give an average complexity, but we expect that it is close to the worst case complexity. With $M = 0.9193L$ and $w = 0.0668L$, this gives $C_T = \mathcal{O}(L^2 2^{0.69L})$ to recover the initial state of $\mathsf{LFSR_Y}$. Consequently, as a distinguishing attack, this scenario operates slightly better than the previous one, but as an initial state recovery it is slightly worse.

4 New Reduced Complexity Attack

Before we describe our attack in detail, let us introduce some notations. Throughout the paper, the symbols Pr and E are respectively used for probability of an event and expectation of a random variable. For simplicity we do not distinguish

between random variables and their instances. We use $A := \{a_i\}$ for a general binary sequence, $A_k^m := \{a_i\}_{i=k}^m$ for a segment of it and $A^m := \{a_i\}_{i=1}^m$ for a prefix of length m. The number of 1's in A is denoted by $\mathrm{wt}(A)$. We define the first derivative of A as $\{a_i + a_{i+1}\}$ and denote it by $\dot{A}$. Let C, X, Y and Z denote the regular output sequences of $\mathsf{LFSR_C}$, $\mathsf{LFSR_X}$, $\mathsf{LFSR_Y}$ and the output sequence of the ASG itself, respectively. The initial state of the LFSR's can be represented by C^L, $X^L$and Y^L.

4.1 Sampling Resistance

Any initial state (C^L, X^L, Y^L) of ASG which can produce Z^m, a given prefix of the output sequence of ASG, is called a preimage of Z^m. The sampling resistance is defined as 2^{-m} where m is the maximum value for which we can efficiently produce all preimages of m-bit outputs. As will be shown in this subsection, the low sampling resistance of ASG is an essential ingredient for our attack. Let $\mathcal{A}(Z^m)$ denote the set of all preimages of Z^m. Based on the divide-and-conquer linear consistency attack, introduced in Sect. 2, we can compute $\mathcal{A}(Z^m)$ as in Alg. 1.

Algorithm 1. Sampling of ASG

Input: Output sequence Z^m of m bits.
Output: Find $\mathcal{A}(Z^m)$ with all preimages of Z^m.
1: Initially, set $\mathcal{A}(Z^m) = \emptyset$.
2: **for all** non-zero initial states C^L **do**
3: Set $\mathcal{X} = \mathcal{Y} = \emptyset$.
4: Compute C^m, a prefix of length m of the output sequence of $\mathsf{LFSR_C}$.
5: Based on C^m, split up Z^m into X^w and Y^{m-w}, where $w = \mathrm{wt}(C^m)$.
6: Add all (non-zero) X^L to $\mathcal{X}$, if $\mathsf{LFSR_X}$ can generate X^w.
7: Add all (non-zero) Y^L to $\mathcal{Y}$, if $\mathsf{LFSR_Y}$ can generate Y^{m-w}.
8: For all $X^L \in \mathcal{X}$ and $Y^L \in \mathcal{Y}$, add (C^L, X^L, Y^L) to the set $\mathcal{A}(Z^m)$.
9: **end for**

Let us discuss the complexity of Alg. 1. If $|\mathcal{A}(Z^m)| \leq 2^L$, then the overall complexity is 2^L, because the complexity of Steps 3 to 8 are $\mathcal{O}(1)$. On the other hand, if $|\mathcal{A}(Z^m)| > 2^L$, then Steps 3 to 8 introduce additional solutions, and overall complexity is about $|\mathcal{A}(Z^m)|$. The following statement is given under the assumption of balancedness, *i.e.* the average number of preimages of ASG for any output Z^m is about 2^{3L-m}, where $m \leq 3L$.

Statement 1. *Time complexity of Alg. 1 is* $C_T = \mathcal{O}(\max(2^L, 2^{3L-m}))$.

With the previous definition of sampling resistance, this algorithm can be considered as an efficient sampling algorithm iff $|\mathcal{A}(Z^m)| \geq \mathcal{O}(2^L)$ or equivalently $m \leq 2L$. That is, the sampling resistance of ASG is about 2^{-k} with $k = 2L$ the total length of the two stop/go LFSR's.

A related problem is how to find a multiset $\mathcal{B}$ with T uniformly random independent elements of $\mathcal{A}(Z^m)$. We suggest to modify Alg. 1 as follows: $\mathcal{A}(Z^m)$ is replaced by $\mathcal{B}$ and T is added as another input parameter. In Step 2, a uniform