PERGAMON

Applied Mathematics Letters 14 (2001) 545–547

Applied Mathematics Letters

www elsevier nl/locate/aml

A Family of Keystream Generators with Large Linear Complexity

L. J García-Villalba
Departamento de Sistemas Informáticos y Programación
Escuela Superior de Informática
Universidad Complutense de Madrid (U C M)
Ciudad Universitaria de Madrid s/n, 28040 Madrid, Spain
javiergv@sip ucm es

M. C Rodríguez-Palánquex
Departamento de Matemática Aplicada
Escuela Universitaria de Estadística
Universidad Complutense de Madrid (U C M)
Avda Puerta de Hierro s/n, 28040 Madrid, Spain
mcrodri@eucmax sim ucm es

Dedicated to Beatriz with love from her father

(Received June 2000, accepted July 2000)

Communicated by R Ahlswede

Abstract—In this work, a new class of keystream generators with a large linear complexity has been derived The design criteria are easily compatible with those given in the literature to prevent correlation attacks

Keywords—Cryptography, Information theory, Linear complexity, Pseudorandom sequence generators, Shift register

1. INTRODUCTION

Most common sequence generators in stream cipher systems are based on a combination of LFSRs and nonlinear functions Depending on whether the keystream involves one or more than one LFSR, the sequence generators are commonly classified into filter generators and combination generators In both cases, the linear complexity is a measure of the suitability of a keystream for its cryptographic application [1–7] In fact, the linear complexity of sequences obtained from a nonlinear combination of LFSR-sequences is mostly predictable Such is the case of many well-known generators proposals [5] (e g , clock-controlled generators, alternating step generators, cascade generators, etc) whose linear complexity is either linear or exponential in the number of

The authors want to thank the programme committee and the organizing committee of Eurocrypt 99 for giving them a stipend to present this work in the rump session of the conference

0893-9659/01/$ - see front matter Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX
PII S0893-9659(00)00191-9

storage cells employed On the other hand, the linear complexity of the filter generators depends exclusively on the particular form of the filter and the LFSR minimal polynomial Generally speaking, there is no systematic method to predict the resulting complexity This is the reason why only a few authors have faced the problem of the determination of the linear complexity for filter generators

The present work is concerned with the problem of the determination of the linear complexity for filter functions Three different steps can be pointed out First, a new class of nonlinear filter functions has been introduced These functions are based on the product of m PN-sequence phases Second, the linear complexity of such functions has been analyzed Last, as the characterization of these functions affects the maximum order terms exclusively, a wide class of filter functions with a guaranteed large linear complexity can be derived Moreover, this characterization is clearly compatible with the conditions described in [8] which prevent the nonlinear filter generators from several correlation attacks (inversion attacks, conditional correlation attacks, fast correlation attacks)

2. A NEW FAMILY OF NONLINEAR FILTERS

Let f be an m^{th}-order function applied to the stages of an LFSR of length L and minimal polynomial $P(D)$ $f = a_{n+t_1}\ a_{n+t_2} \times \quad \times a_{n+t_m}$ with $t_i = 2^k\ i\ \delta$ where $k,\ i,\ \delta \in N$ and $\gcd(\delta,\ 2^L - 1) = 1$, and let $\alpha \in GF(2^L)$ be a root of the minimal polynomial of the sequence produced by the LFSR of length L Then α^e with $e = 2^{e_1} + 2^{e_2} + \quad + 2^{e_m}$ where $0 \le e_1 < e_2 < \quad < e_m < L$ is a root of the minimal polynomial of the sequence generated by f if and only if the next determinant A_e does not equal zero That is,

$$A_e = \begin{vmatrix} \alpha^{t_1\,2^{e_1}} & \alpha^{t_2\,2^{e_1}} & \alpha^{t_{m-1}\,2^{e_1}} & \alpha^{t_m\,2^{e_1}} \\ \alpha^{t_1\,2^{e_2}} & \alpha^{t_2\,2^{e_2}} & \alpha^{t_{m-1}\,2^{e_2}} & \alpha^{t_m\,2^{e_2}} \\ & & & \\ \alpha^{t_1\,2^{e_m}} & \alpha^{t_2\,2^{e_m}} & \alpha^{t_{m-1}\,2^{e_m}} & \alpha^{t_m\,2^{e_m}} \end{vmatrix} \neq 0$$

If the determinant A_e equals zero, then the corresponding cyclotomic coset is said to be degenerate for the function f Let us analyse this choice of the stages of the filter, that is, replacing t_i by its value and making the next substitution $\alpha^{2^k\,\delta\,2^{e_i}} = \lambda_i$, the determinant A_e will be as follows

$$A_e = \begin{vmatrix} 1 & \lambda_1 & \lambda_1^{m-2} & \lambda_1^{m-1} \\ 1 & \lambda_2 & \lambda_2^{m-2} & \lambda_2^{m-1} \\ & & & \\ 1 & \lambda_m & \lambda_m^{m-2} & \lambda_m^{m-1} \end{vmatrix}$$

This determinant is a Vandermonde determinant Its value is well known

$$A_e = \prod (\lambda_i + \lambda_j), \qquad i = 1, \quad , m-1, \quad j = i, \quad , m$$

As we can see in the previous expression, $A_e \neq 0$ if $\lambda_i \neq \lambda_j$ Therefore,

$$\alpha^{2^k\,2^{e_i}\,\delta} \neq \alpha^{2^k\,2^{e_j}\,\delta} \Rightarrow \alpha^{2^k\,2^{(e_i - e_j)}\,\delta} \neq \alpha^{2^L - 1} = 1 \Rightarrow 2^k\ \ 2^{(e_i - e_j)}\ \ \delta \neq 2^L - 1$$

and the above fact only happens if $\gcd(\delta,\ 2^L - 1) = 1$ Consequently, the linear complexity of this new family of filter functions is lower bounded by $\binom{L}{m}$ because all the cosets of weight m are nondegenerate For $L = 257$ and $m = 129$ (typical values for the length of LFSR and the order of the filter in communication systems), $LC \approx 10^{76}$, that is, a very large linear complexity!

3. CONCLUSIONS

The keystream generators presented here provide a new class of sequence generators which satisfy the standard cryptographic requirements of large linear complexity and correlation immunity

REFERENCES

1 E J Groth, Generation of binary sequences with controllable complexity, *IEEE Trans Inform Theory* **IT-17**, 288–296, (1971)

2 E L Key, An analysis of the structure and complexity of nonlinear binary sequence generators, *IEEE Trans Inform Theory* **IT-22**, 732–736, (1976)

3 P V Kumar and R A Sholtz, Bounds on the linear span of bent sequences, *IEEE Trans Inform Theory* **IT-29**, 854–862, (1983)

4 R A Rueppel, *Analysis and Design of Stream Ciphers*, Springer-Verlag, Berlin, (1986)

5 R A Rueppel, Stream ciphers, In *Contemporary Cryptology*, (Edited by G J Simmons) IEEE Press, New York (1992)

6 J L Massey and S Serconek, Linear complexity of sequences with arbitrary period and a generalized discrete Fourier transform, advances in cryptology-CRYPTO'96, In *Lecture Notes in Computer Science, Vol 1109*, pp 358–371, Springer-Verlag, Berlin, (1996)

7 K G Paterson, Root counting, the DFT and the linear complexity of nonlinear filtering, *Designs, Codes, and Cryptography* **14**, 247–259, (1998)

8 J D Golic, On the security of shift register based keystream generators, In *Lecture Notes in Computer Science, Vol 809, Proceedings of the Fast Software Encryption International Workshop*, Springer-Verlag, (1994)