Annals of the University of Craiova, Mathematics and Computer Science Series
Volume 43(1), 2016, Pages 27–32
ISSN: 1223-6934

Dedicated to Marius Iosifescu
on the occasion of his 80th anniversary

Nonlinearities on cryptographic shift registers

Nicolae Constantinescu, Oana Adriana Ţicleanu, and Alin Golumbeanu

Abstract. Symmetric cryptographic keys generation systems with a high complexity needs nonlinear mathematical models. This condition is due to the necessity of increasing the complexity of attack on the cryptographic model. In this regard, the present paper takes on a new approach of constructing these systems, having as a starting point combinations based on solutions at the border of nonlinear equations.

Key words and phrases. nonlinear cryptography, Berlekamp-Massey method, cryptographic bound solutions.

1. Introduction

Of great importance in the field of data protection are the mathematical models that generate the keys for the cryptographic models used regularly, more exactly symmetric ciphers, in accordance with [4], [5], [6], [7]. These offer a substantial protection against unauthorized access of various eavesdropping methods on commutation lines. The main problem of a symmetric algorithm is based on the generation of a random and secret number and getting that number by any means based on algorithm with exponential complexity. This problem of generating the random number is felt in practice in implementing a cryptographic software, because the software is based on generating this random number.

Using a pseudorandom generator for encryption which has cryptographic properties, presumes that the space from which the numbers are generated to be large enough so that the probability of breakage will be small. This generator with cryptographic properties is an algorithm or a function which has prior defined the algorithm or the function and all the bits generated to a point. In this way the values of the next bits can't be found with a probability higher than $\frac{1}{2} + e$ if the initial data - seed - are not considered, and the value of e decreases exponentially according to a security parameter s which can present, by example, the length of the seed used by the pseudorandom generator.

A big part of the generators proposed until now consist of a binary number of shift registers of maximum length, combined with a binary function [8], [16], [17], [18]. These registers are created so that the binary function will alternated the generator linearity, giving an output sequence with a high linear complexity, [1]. The problem of determining the linear complexity of a sequence was studied in Berlekamp-Massey Algorithm (1962/1969). These solutions are given for particular cases in which we have a linear degree well suited for the combination functions. It is necessary to

Received May 20, 2016.

use a method more complex for the case in which the equivalent linear complexity calculated is very high.

2. Berlekamp-Massey particular case study

In the case of determining the linear complexity (Berlekamp-Massey), we have a periodic sequence x defined over a space $GF(q)$ and the notation:

$$x(t) = \frac{g(t)}{1 - t^{per\ x}},$$

namely the linear shift register sequence [11], [12], [14], [19].

The size of the shortest possible linear shift register has the possibility of producing a sequence, namely the minimal polynomial degree f_x as follows:

$$\mathcal{L}(x) = deg\ f_x,$$

which caries the name of linear complexity of sequence.

It was proven that the method implemented in Berlekamp-Massey (BMA) algorithm [2], [3] is efficient for determining the localization polynomial error in decoding Reed-Solomon codes and BCH codes. In BMA it is determined the error of the polynomial used for defining the nonlinear qualities of the shift registers. By this the LFSR properties are used for developing Berlekamp-Massey algorithm. The most important of this are described in the following. Next we present some of the LFSR properties used in developing Berlekam-Massey algorithm.

2.1. Linear systems of shift register. We consider linear feedback shift register ([7]) of length λ with $a_0 \neq 0$, which generates a sequence of date of form

$$\alpha_0, \alpha_1, \ldots, \alpha_{\lambda-1}, \alpha_\lambda, \ldots.$$

The first part of data from the sequence λ, $\alpha_0, \alpha_1, \ldots, \alpha_{\lambda-1}$, represent cascaded registers, and the data from the sequence after $\alpha_{\lambda-1}$ satisfy the following relation:

$$\sum_{i=0}^{\lambda} a_i, \alpha_{j-1} = 0, \quad \text{where} \quad j = \alpha, \alpha + 1, \ldots \tag{1}$$

According to relation (1), designing a LFSR of length α which has the first N values $\alpha_0, \alpha_1, \ldots, \alpha_{N-1}$, where $N \leq \alpha$, we will consider the initial seed achieved with the help of a nonlinear function. If $N \geq \alpha$, we will have in addition to the initial data the condition that all coefficients $\alpha_0, \alpha_1, \ldots, \alpha_\lambda,\ \alpha_0 \neq 0$, must satisfy the next relation:

$$\begin{bmatrix} \alpha_0 & \alpha_1 & \ldots & \alpha_\lambda \\ \alpha_1 & \alpha_2 & \ldots & \alpha_{\lambda+1} \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_{N-1-\lambda} & \alpha_{N-\lambda} & \ldots & \alpha_{N-1} \end{bmatrix} \begin{bmatrix} a_\lambda \\ a_{\lambda-1} \\ \vdots \\ a_0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \tag{2}$$

This way of treating the problem is bases the following theorem (2.1 from [3]):

Theorem 2.1. *If a LFSR of length λ generates the sequence $\alpha_0, \alpha_1, \ldots, \alpha_{N-1}$, then any LFSR which generates a sequence with length λ', satisfies*

$$\lambda' \geq N + 1 - \lambda \tag{3}$$

Demonstrating this theorem is the same with the demonstration of theorem from [3]. The idea from which the demonstration is composed takes into consideration λ_n as the minimal length of all LFSRs which can generate $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$. It can be observed that λ_n is monotone and ascending by parameter n. From this we can see that if some LFSRs of length λ_n generate $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ but not the sequence $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}, \alpha_n$, then the following relation will result

$$\lambda_{n+1} \geq max[\lambda, n+1-\lambda_n] \tag{4}$$

Exactly these allow us to define the methods of selection of points which represent shift registers parameters.

3. Nonlinearities construction for the feedback registers system

In the classical case a generator is modeled based on some linear parameters like the coefficients of a polynomial. In the following we will construct the data selection coefficients which enter the generation process of the string according to some parameters on the particular elliptical points, defined as an unbranched extension $\mathbb{Q}_q$ of degree n with the ring class $\mathbb{Z}_q$ and the residual field $\mathbb{F}_q$ [9], [10].

For $a_0, b_0 \in \mathbb{R}$ with $a_0 \geq b_0 > 0$, is defined the AGM iteration (the main sequence) for $k \in \mathbb{N}$ and we will have

$$(a_{k+1}, b_{k+1}) = \left(\frac{a_k + b_k}{2}, \sqrt{a_k b_k}\right).$$

Then $b_k \leq b_{k+1} \leq a_{k+1} \leq a_k$ and $0 \leq a_{k_1} - b_{k+1} \leq (a_k - b_k)/2$; therefore the limits equality exists $\lim\limits_{k\to\infty} a_k = \lim\limits_{k\to\infty} b_k$. These general value is named AGM of a_0 and b_0 and is denoted by $AGM(a_0, b_0)$. It can be shown that

$$\frac{a_k}{b_k} - 1 \leq \frac{a_0 - b_0}{2^k b_k} \leq \frac{1}{2^k}\left(\frac{a_0}{b_0} - 1\right),$$

such that, after a number of steps characterized by a logarithmic complexity calculus we have $a_k/b_k = 1+\epsilon_k < 1$. A square convergence will be obtained from the expansion of the Taylor series of $1/\sqrt{1+\epsilon_k}$:

$$\frac{a_{k+1}}{b_{k+1}} = \frac{a_k + b_k}{2\sqrt{a_k b_k}} = \frac{2+\epsilon_k}{2\sqrt{1+\epsilon_k}} = 1 + \frac{\epsilon_k^2}{8} - \frac{\epsilon_k^3}{8} + \frac{15\epsilon_k^4}{128} - \frac{7\epsilon_k^5}{64} + O(\epsilon_k^6). \tag{5}$$

We note with $\sqrt{c}$ for $c \in 1 + 8\mathbb{Z}_q$ the single element $d \in 1 + 4\mathbb{Z}_q$ with $d^2 = c$. The elements $a, b \in \mathbb{Z}_q$ with $a/b \in 1 + 8\mathbb{Z}_q$, $a' = (a+b)/2$ and $b' = b\sqrt{a/b}$ belong to $\mathbb{Z}_q$ and $a'/b' \in 1 + 8\mathbb{Z}_q$. More than this, in the case of $a, b \in 1 + 4\mathbb{Z}_q$ and $a', b' \in 1 + 4\mathbb{Z}_q$. Giving all of this the main sequence will converge if and only if $a/b \in 1 + 16\mathbb{Z}_q$. For $a/b \in 1 + 8\mathbb{Z}_q$, it will not converge.

Let $a, b \in 1+4\mathbb{Z}_q$ with $a/b \in 1+8\mathbb{Z}_q$ and the elliptic curve $E_{a,b}$ defined by equation $y^2 = x(x-a^2)(x-b^2)$. We keep in mind that $E_{a,b}$ is not a minimalist Weierstrass model, and the modulo reduction 2 of this model is singular. The next lemma offers an isomorphism for the curve $E_{a,b}$ at a minimal model, which represents an improvement of the result from [13].

Lemma 3.1. *Let $a, b \in 1+4\mathbb{Z}_q$ with $a/b \in 1+8\mathbb{Z}_q$ and the elliptic curve $E_{a,b}$ defined by equation $y^2 = x(x-a^2)(x-b^2)$. Then the isomorphism*

$$(x,y) \longmapsto \left(\frac{x-ab}{4}, \frac{y-x+ab}{8}\right)$$

transforms the curve $E_{a,b}$ in $y^2+xy = x^3+rx^2+sx+t$ with the next values:

$$\begin{cases} r &= \dfrac{-a^2+3ab-b^2-1}{4}, \\ s &= \dfrac{-a^3b+2a^2b^2-ab^3}{8}, \\ t &= \dfrac{-a^4b^2+2a^3b^3-a^2b^4}{64}. \end{cases} \tag{6}$$

In addition, $r \in 2\mathbb{Z}_q$, $s \in 8\mathbb{Z}_q$, $t \equiv -\left(\dfrac{a-b}{8}\right)^2$ (modulo 16) and the equation defines a minimal Weierstrass model.

The next proposition shows that the *AGM* iteration constructs a sequence of elliptical curves all of them having the construction based on isomorphisms which are based on the initial curve.

Proposition 3.2. *Let $a, b \in 1+4\mathbb{Z}_q$ with $a/b \in 1+8\mathbb{Z}_q$ and the elliptical curve $E_{a,b}$ defined by equation $y^2 = x(x-a^2)(x-b^2)$. Let $a' = (a+b)/2$, $b' = \sqrt{ab}$ and $E_{a',b'} : y^2 = x(x-a'^2)(x-b'^2)$. Then the curves $E_{a,b}$ and $E(a',b')$ are characterized by equation*

$$\phi : E_{a,b} \to E_{a',b'} : (x,y) \longmapsto \left(\frac{(x+ab)^2}{4x}, y\frac{(x-ab)(x+ab)}{8x^2}\right),$$

and the main part from ϕ is $\langle(0,0)\rangle$. More then that, the operation ϕ on the differential interval dx/y is

$$\phi^*\left(\frac{dx}{y}\right) = 2\frac{dx}{y}.$$

Let the normal elliptical curve $\overline{E}$ defined by equation $y^2+xy = x^3+c$ with $c \in \mathbb{F}_q^*$ and let $\mathcal{E}$ its canonical transformation. We take any $r \in \mathbb{Z}_q$ such that $r^2 \equiv c(modulo\ 2)$ and let $a_0 = 1+4r$ and $b_0 = 1-4r$. Then Lemma 3.1 shows that E_{a_0,b_0} is isomorph for a transformation from $\overline{E}$ to $\mathbb{Z}_q$ so that $j(E_{a_0,b_0}) \equiv j(\overline{E})(modulo\ 2)$.

Let a sequence of generators $(a_k, b_k)_{k=0}^{\infty}$ and taking into consideration the elliptical curves E_{a_k,b_k}. The Proposition 3.2 presumes that $\Phi_2(j(E_{a_{k+1},b_{k+1}}), j(E_{a_k,b_k})) = 0$ and an easy calculus shows that $j(E_{a_{k+1},b_{k+1}}) \equiv j(E_{a_k,b_k})^2(modulo\ 2)$. We keep in mind that $\Phi_2(X,Y)$ and $(j(E_{a_{k+1},b_{k+1}}), j(E_{a_k,b_k}))$ satisfy the condition of Proposition 3.2. Next we can deduce the following conclusion:

$$j(E_{a_k,b_k}) \equiv \Sigma^k(j(\mathcal{E}))\ (modulo\ 2^{k+1}).$$

The next proposition shows that it can be translated into an isomorphism which can to brought to a form of which attack complexity if of non-polynomial order.

Proposition 3.3. *Having the two elliptic curves $E_{a,b} : y^2 = x(x-a^2)(x-b^2)$ and $E_{c,d} : y'^2 = x'(x'-c^2)(x'-d^2)$ defined over $\mathbb{Q}_q$ with $a, b, c, d \in 1+4\mathbb{Z}_q$ and $a/b, c/d \in$*

$1 + 8\mathbb{Z}_q$, then the curves $E_{a,b}$ and $E_{c,d}$ are isomorphic if and only if $x' = u^2x$ and $y' = u^3y$ with $u^2 = \dfrac{c^2 + d^2}{a^2 + b^2}$. More than that $\left(\dfrac{a}{b}\right)^2 = \left(\dfrac{c}{d}\right)$ or $\left(\dfrac{a}{b}\right)^2 = \left(\dfrac{d}{c}\right)^2$.

Let the invariant differentials $\omega = dx/y$ and $\omega' = dx'/y'$ on $E_{a,b}$ and $E_{\Sigma(a),\Sigma(b)}$, respectively. Then

$$\Sigma^*(\omega') = (\lambda \circ \phi)^*(\omega') = 2u^{-1}\omega,$$

with $u^2 = \dfrac{\Sigma(a)^2 + \Sigma(b)^2}{a'^2 + b'^2}$. We define $\zeta = a/b = 1 + 8c$ and $\zeta' = a'/b' = 1 + 8c'$. Then the Proposition 3.3 also implies that:

$$\zeta'^2 = \Sigma(\zeta)^2 \quad \text{or} \quad \zeta'^2 = \frac{1}{\Sigma(\zeta)^2}.$$

Substituting $\zeta = 1 + 8c$ and $\zeta' = 1 + 8c'$ in the equation above and dividing by 16, we can conclude that $c' \equiv \Sigma(c)(\textit{modulo } 4)$ or $c' \equiv -\Sigma(c)(\textit{modulo } 4)$. Taylor extension of $1 + 8c' = (1 + 4c)/\sqrt{1 + 8c}$ modulo 32 show that $c' \equiv c^2(\textit{modulo } 4)$. Because the first iteration c is a square α^2 modulo 4, and from $\Sigma(\alpha^2) \equiv \alpha^4(\textit{modulo } 4)$, we can conclude that $\zeta'^2 = \Sigma(\zeta)^2$. We keep in mind that this implies that

$$\zeta' = \frac{a'}{b'} = \Sigma(\zeta) = \Sigma\left(\frac{a}{b}\right), \tag{7}$$

because $\zeta' \equiv \zeta \equiv 1(\textit{modulo } 8)$. Substituting $b'^2 = a'^2\Sigma(b)/\Sigma(a)^2$ in the expression for u^2 and taking the square roots it will lead us to

$$u = \pm\frac{\Sigma(a)}{a'}.$$

Although the main sequence $(a_k, b_k)_{k=0}^{\infty}$ does not converge at singularities and the elliptical curves sequence $(E_{a_{nk},b_{nk}})_{k=0}^{\infty}$ doesnt converge because there is

$$\lim_{k\to\infty} j(E_{a_{nk},b_{nk}})$$

and it is equal with the invariant j of curve canonical transformation $\overline{E}$, we can have local convergence, at the boundary. These will be the set of points that define the method of selection of shifting registers used in cryptography.

4. Conclusion

Shift registers systems have a equivalent linear complexity to resisting cryptographic attacks. In order to obtain an exponential complexity, even in the case of attacks based on the case described by Berlekamp-Massey, it is necessary to define a nonlinear method of parameter selection for shift register. Through this a LFSR (Linear Shift Register) turns into a NLFSR (NonLinear Shift Register). In the present paper it was presented the way in which this type of parameters that assure the nonlinearity of such system can by defined. In our future work we aim to implement this model in order to study the Equivalent Linear Complexity, specifically how Berlekamp-Massey works in case proposed.

References

[1] T. Herlestam, On the complexity of functions of linear shift register sequences, *IEEE ISIT 1982*, Les Arcs, France.

[2] E.R. Berlekamp, *Algebraic coding theory*, McGraw-Hill, New York, 1968.

[3] J.L. Massey, Shift-register synthesis and BCH decoding, *IEEE Trans. Inf. Theory* (1969), IT-**15**(1), 122–127.

[4] J.Dj. Golić, R. Menicocci, Correlation Analysis of the Alternating Step Generator, *Designs, Codes and Cryptography* (2004) **31**(1), 51–74.

[5] S.R. Ghorpade, S. Ul Hasan, M. Kumari, Primitive polynomials, singer cycles and word-oriented linear feedback shift registers, *Designs, Codes and Cryptography* (2011) **58**(2), 123–134.

[6] N.R. Pillai, S.S. Bedi, Algebraic attacks on a class of stream ciphers with unknown output function, *Designs, Codes and Cryptography* (2013) **69**(3), 317–330.

[7] T. Johansson, A shift register construction of unconditionally secure authentication codes, *Designs, Codes and Cryptography* (1994) **4**(1), 69–81.

[8] S. Ronjom, Improving algebraic attacks on stream ciphers based on linear feedback shift register over F_{2^k}, *Designs, Codes and Cryptography* (online 2016), DOI:10.1007/s10623-016-0212-9, 1–15.

[9] Z. Ma, W.F. Qi, T. Tian, On affine sub-families of the NFSR in Grain, *Designs, Codes and Cryptography* (2015) **75**(2), 199–212.

[10] T. Tian , W.F Qi, On the largest affine sub-families of a family of NFSR sequences, *Designs, Codes and Cryptography* (2014) **71**(1), 163–181.

[11] J.Dj. Golić, R. Menicocci, Edit Probability Correlation Attacks on Stop/ Go Clocked Keystream Generators, *Journal of Cryptology* (2003) **16**(1), 41–68.

[12] W. Meier, O. Staffelbach, Fast correlation attacks on certain stream ciphers, *Journal of Cryptology* (1989) **1**(3), 159–176.

[13] W. Meier, O. Staffelbach, Correlation properties of combiners with memory in stream ciphers, *Journal of Cryptology* (1992) **5**(1), 67–86.

[14] J.Dj. Golić, M. Salmasizadeh, E. Dawson, Fast Correlation Attacks on the Summation Generator, *Journal of Cryptology* (2000) **13**(2), 245-262.

[15] J.Dj. Golić, Correlation properties of a general binary combiner with memory, *Journal of Cryptology* (1996) **9**(2), 111–126.

[16] A. Klapper, M. Goresky, Feedback shift registers, 2-adic span, and combiners with memory, *Journal of Cryptology* (1997) **10**(2), 111–147.

[17] M. Zhang , Maximum Correlation Analysis of Nonlinear Combining Functions in Stream Ciphers, *Journal of Cryptology* (2000) **13**(3), 301–314.

[18] E. Biham, Cryptanalysis of Triple Modes of Operation, *Journal of Cryptology* (1999) **12**(3), 161–184.

[19] J.P. Aumasson, L. Henzen, W. Meier, M. Naya-Plasencia, Quark: A Lightweight Hash, *Journal of Cryptology* (2013) **26**(2), 313–339.

(Nicolae Constantinescu) Associate Professor, University of Craiova, 13 A.I. Cuza, Craiova, Romania
E-mail address: nikyc@central.ucv.ro

(Oana Adriana Ţicleanu) Research Assistant, University of Craiova, 13 A.I. Cuza, Craiova, Romania
E-mail address: oana.ticleanu@inf.ucv.ro

(Alin Golumbeanu) Doctoral School of Sciences, University of Craiova, 13 A.I. Cuza, Craiova, Romania
E-mail address: alin.golumbeanu@inf.ucv.ro