2. Conclusion and Future Work

In this work, we have presented a new algorithmic-algebraic scheme based in the Lai — Massey structure for constructing permutations of dimension $n = 2k$, $k \geqslant 2$. For the common case $k = 8$, we have obtained new cryptographically strong 8-bit permutations having better resistance to algebraic attacks in comparison with the inversion function in $\mathrm{GF}(2^8)$ which so far has the best-known values for nonlinearity and differential uniformity. Compared to the best nonlinearity (108, for $k = 4$) offered by the construction presented in [6] and later generalized in [7], the nonlinearity for the permutations obtained by our scheme slightly decrease up to 104, but to the best of our knowledge the schemes presented in [6, 7] can not produce involutions and orthomorphisms with strong cryptographic properties, so we can conclude that the new structure presented in this work is more powerful and attractive due to the diversity of permutations that can be constructed. Interestingly, the involutions and orthomorphisms founded in this work have comparable classical cryptographic properties like those constructed by using spectral-linear and spectral-difference methods [8]. The main advantage of our 8-bit permutations is that they can be constructed using smaller 4-bit components which could be useful for the implementation of the S-Box in hardware or using a bit-sliced approach. We only presented a new scheme that can help to find permutations, involutions and orthomophisms with rather good cryptographic properties. There are several questions (theoretical results, hardware and bit-sliced implementations, efficient methods of masking) about the construction suggested in this work which are left as future work.

REFERENCES

1. http://www.sagemath.org. Sage Mathematics Software (Version 8.1). 2018.
2. *Vaudenay S. and Junod P.* Fox, a New Family of Block Ciphers. http://crypto.junod.info/sac04a.pdf. 2004.
3. *Feng D., Feng X., Zhang W., et al.* Loiss: a byte oriented stream cipher. LNCS, 2011, vol. 6639, pp. 109–125.
4. *Gligoroski D., Odegard R. S., Mihova M., et al.* Cryptographic hash function Edon-R. Proc. IWSCN, Trondheim, 2009, pp. 1–9.
5. *Gilboa Sh. and Gueron Sh.* Balanced Permutations Even-Mansour Ciphers. Cryptology ePrint Archive, Report 2014.
6. *De la Cruz Jiménez R. A.* Generation of 8-bit S-Boxes Having Almost Optimal Cryptographic Properties Using Smaller 4-bit S-Boxes and Finite Field Multiplication. 2017. www.cs.haifa.ac.il/orrd/LC17/paper60.pdf.
7. *Fomin D.* New classes of 8-bit permutations based on a butterfly structure. Pre-proc. CTCrypt'18-Suzdal, 2016, pp. 199–211.
8. *Menyachikhin A.* Spectral-linear and spectral-difference methods for generating cryptographically strong S-Boxes. Pre-proc. CTCrypt'16-Yaroslavl, 2016, pp. 232–252.

UDC 621.391:519.7 DOI 10.17223/2226308X/12/43

SOME PROPERTIES OF THE OUTPUT SEQUENCES OF COMBINED GENERATOR OVER FINITE FIELDS

Aulet R. Rodriguez

The sequences are an important part of the cryptography and analysis of their properties is of great interest. In this paper, the following characteristics of combined generator are analyzed: period of output sequences and the distribution of elements in the output sequences over finite field.

Keywords: *finite field, correlation-immune function, resilient function, balanced function, combined generator.*

Introduction

The randomness is an important property in the cryptographic scheme. One of the components that ensure this property is the random sequence that is built by generators. The elements of random sequences can be used as initialization vectors, in cyclic codes, as keys in block cipher, and in stream cipher. The combined generator presents one class of generators that are used to obtain pseudorandom sequence. Examples of its use are stream ciphers: A.1 of standard GSM [1], Grain, Trivium [2]. The most results belong to generators over the field GF(2) [1, 3, 4].

In this work, we analyze the following characteristics for combined generator: period of the output sequence and distribution elements in output sequence over finite field.

Let $P = \mathrm{GF}(q)$ be a finite field with q elements, $F_1(x), \ldots, F_k(x)$ be polynomials with coefficients in P of degrees $m_1, \ldots, m_k$ respectively. We assume that $F_1(x), \ldots, F_k(x)$ are primitive polynomials [5], also $\gcd(m_i, m_j) = 1$ for each $i \neq j$. For each function $\varphi : P^k \to P$, we consider the combined generator [1, 6, 7] with the output sequence

$$v(i) = \varphi(u_1(i), u_2(i), \ldots, u_k(i)), \quad i \geqslant 0,$$

where u_j is a linear recurring sequence over P with minimal polynomial $F_j(x)$.

1. Period

In [6] the general bounds for the period of combined generator and the exact equality in the case GF(2) is presented. In this work, we give bounds for the period of a given generator for one class of function over any finite field and show, how this period can be calculated.

Theorem 1. If φ has the form

$$\varphi(x_1, \ldots, x_k) = \sum_{s=1}^{k} \sum_{1 \leqslant i_1 < i_2 < \ldots < i_s \leqslant k} c_{i_1 i_2 \ldots i_s} x_{i_1} x_{i_2} \ldots x_{i_s},$$

then period $T(v)$ of sequence v satisfies the conditions

$$\frac{(q^{m_1} - 1) \ldots (q^{m_k} - 1)}{(q-1)^k} \,\Big|\, T(v) \quad \text{and} \quad T(v) \,\Big|\, \frac{(q^{m_1} - 1) \ldots (q^{m_k} - 1)}{(q-1)^{k-1}}.$$

Theorem 2. In conditions of theorem 1, if $b_i = F_i(0)(-1)^{m_i}$, $i = 1, \ldots, k$, and $m = m_1 \ldots m_k$, then

$$T(v) = \frac{(q^{m_1} - 1) \ldots (q^{m_k} - 1)}{(q-1)^k} d,$$

where $d = \mathrm{lcm}(\mathrm{ord}(b_{i_1}^{m/m_{i_1}} \ldots b_{i_s}^{m/m_{i_s}}) : c_{i_1 i_2 \ldots i_s} \neq 0)$. Moreover, d is the minimal number in $\mathbb{N}$ for which

$$\varphi(x_1, \ldots, x_k) = \varphi(b_1^{dm/m_1} x_1, \ldots, b_k^{dm/m_k} x_k).$$

Corollary 1. In conditions of theorem 1, if exist such $i_1, \ldots, i_k$ for which $b_{i_1}^{m/m_{i_1}} \ldots b_{i_s}^{m/m_{i_s}}$ is a primitive element or function $\varphi(x_1, \ldots, x_k)$ is linear in variables x_1, …, x_k, then

$$T(v) = \frac{(q^{m_1} - 1) \ldots (q^{m_k} - 1)}{(q-1)^{k-1}}.$$

2. Frequencies

For each element $c \in P^*$, we define the following function $\psi_c : P^k \to \mathbb{C}^*$, where $\mathbb{C}^*$ is multiplicative group of complex numbers, as follows

$$\psi_c(x_1, \dots, x_k) = \chi(c\varphi(x_1, \dots, x_k)),$$

where χ is character of $(P, +)$, $\chi(x) = e^{2\pi i \mathrm{tr}^P_{P_0}(x)/p}$, for all $x \in P$, $P_0 = \mathrm{GF}(p)$ is the prime field and $\mathrm{tr}^P_{P_0}(x)$ is the trace of x over P_0. For every function $\psi : P^k \to \mathbb{C}^*$, it is shown [8], that, for any $(x_1, \dots, x_k) \in P^k$,

$$\psi_c(x_1, \dots, x_k) = \frac{1}{q^k} \sum_{\mathbf{a} \in P^k} W_\psi(\mathbf{a}) \chi_{\mathbf{a}}(x_1, \dots, x_k), \quad W_{\psi_c}(\mathbf{a}) = \sum_{\mathbf{b} \in P^k} \psi_c(\mathbf{b}) \overline{\chi}(\mathbf{ab}),$$

where $\overline{\chi}$ is the conjugate character.

The class of correlation-immune and resilient function over any field is defined in [9]. In this work, we analyze $(k-1)$-resilient function. We shall calculate the value

$$N_l(z, v) = |\{i \in \{0, \dots, l-1\} : v(i) = z\}|,$$

where $l \in \mathbb{N}$, $l \leqslant T = (q^{m_1} - 1) \dots (q^{m_k} - 1)/(q-1)^{k-1}$.

Theorem 3. If $\varphi(x_1, \dots, x_k)$ is $(k-1)$-resilient function and $m = m_1 + \dots + m_k$, then

$$\left| N_l(z, v) - \frac{l}{q} \right| \leqslant \frac{(q-1)^{(k+2)/2}}{q} C_l,$$

where

$$C_l = \begin{cases} \left(\dfrac{4}{\pi^2} \ln(T) + \dfrac{9}{5} \right) q^{m/2}, & \text{if } l < T, \\ (q^m - T)^{1/2}, & \text{if } l = T. \end{cases}$$

Corollary 2. If $\varphi(x_1, \dots, x_k) = a_1 x_1 + \ldots + a_k x_k$, then

$$\left| N_l(z, v) - \frac{l}{q} \right| \leqslant \frac{q-1}{q} C_l.$$

For a linear function the Niederreiter's bounds [10, theorem 2] are better than our bounds in whole period. But for to use the Niederreiter's bounds, it is necessary to know the whole period, in practice we have only an interval of the period, which makes our bounds more accurate in the latter case. Now, we shall show that, in general, for other $(k-1)$-resilient functions we can use our bounds when the Niederreiter's bounds does not work, or vice-versa.

Denoting by R_{k-1} the set of all $(k-1)$-resilient functions, in R_{k-1} we define the binary relation $\sim$ as follows:

$$\forall \varphi_1, \varphi_2 \in R_{k-1} \Big(\varphi_1 \sim \varphi_2 \Leftrightarrow$$

$$\Leftrightarrow \exists \text{ permutation } \pi \left(\forall (x_1, \dots, x_k) \in P^k \left(\varphi_2(x_1, \dots, x_k) = \pi(\varphi_1(x_1, \dots, x_k)) \right) \right) \Big).$$

This relation is an equivalence. If we can determine the period and the distribution of elements for the function φ_1, we can also make it for the function φ_2. Let us show that it cannot always take the function linear like representatives of the classes.

Proposition 1. Let $P = \mathrm{GF}(2^2)$, $\varphi(x_1, x_2) = x_1^2 + x_2$. A permutation polynomial $\pi(x)$ and a_1, a_2 for which $\pi(\varphi(x_1, x_2)) = a_1 x_1 + a_2 x_2$, do not exist.

For function φ in proposition 1, it is necessary to use the bound of theorem 3. But if $\varphi(x_1, x_2) = x_1^2 + x_2^2$, we can use the Niederreiter's bounds.

REFERENCES

1. *Alferov A. P., Zubov A. Y., Kuz'min A. S., and Cheremushkin A. V.* Osnovy kriptografii [Basics of Cryptography]. Moscow, Gelios ARV Publ., 2001. (in Russian)
2. *Matthew R. and Oliver B.* New Stream Ciphers Designs. Springer, 2008.
3. *Andreas K.* Stream Cipher. Springer, 2013.
4. *Bilyak I. B. and Kamlovskii O. V.* Chastotnye kharakteristiki tsiklov vykhodnykh posledovatel'nostey kombiniruyushchikh generatorov nad polem iz dvukh elementov [The frequency characteristics of cycle of output sequences combining generator over the field of two elements]. Prikladnaya Diskretnaya Matematika, 2015, no. 3(29), pp. 17–31. (in Russian)
5. *Lidl R. and Niederreiter H.* Finite Fields. Encyclopedia of Mathematics and its Applications. Cambridge University Press, 1997.
6. *Fomichev V. M.* Fomichev V.M. Diskretnaya matematika i kriptologiya Diskretnaya matematika i kriptologiya [Discrete Mathematics and Cryptology. Moscow, Dialog-MEPhI Publ., 2010. (in Russian)
7. *Rueppel R. A.* Analysis and Design of Stream Ciphers. Springer Verlag, 1986.
8. *Kamlovskii O. V.* Kolichestvo poyavleniy elementov v vykhodnykh posledovatel'nostyakh fil'truyushchikh generatorov [Distribution properties of sequences produced by filtering generators]. Prikladnaya Diskretnaya Matematika, 2013, no. 3(21), pp. 11–25. (in Russian)
9. *Camion P. and Canteaut A.* Correlation-Immune and Resilient Function over a Finite Alphabet and Their Application in Cryptography. Springer, 1998.
10. *Niederreiter H.* Weights of cyclic codes. Information and Control, 1997, vol. 34, pp. 130–140.

UDC 003.26 DOI 10.17223/2226308X/12/44

DISCRETE LOGARITHM FOR NILPOTENT GROUPS AND CRYPTANALYSIS OF POLYLINEAR CRYPTOGRAPHIC SYSTEM[1]

V. A. Roman'kov

We present an efficient algorithm to compute a discrete logarithm in a finite nilpotent group, or more generally, in a finitely generated nilpotent group. Special cases of a finite p-group (p is a prime) and a finitely generated torsion free nilpotent group are considered. Then we show how the derived algorithm can be generalized to an arbitrary finite or finitely generated nilpotent group respectively. We suppose that group is presented by generating elements and defining relators or as a subgroup of a triangular matrix group over a prime finite field (in finite case) or over the ring of integers (in torsion-free case). On the base of the derived algorithm we give a cryptanalysis of some schemes of polylinear cryptography known in the literature.

Keywords: *discrete logarithm, nilpotent group, polylinear system, cryptanalysis.*

Introduction

Let G be a group. We say that the *discrete logarithm* is (efficiently) *computable* in G if there is an efficient algorithm that finds an exponent $x \in \mathbb{Z}$ for any expression of the form $f = g^x$, where $g, f \in G$. The problem of determining x given g and $f = g^x$ is called the *discrete logarithm problem* in G. The classical Diffie — Hellman exchange protocol, the ElGamal system and many other cryptographic schemes, protocols and systems are based

[1] The author is supported by RFBR, project No. 18-41-550001a.