Method for the Simultaneous Generation of Two Nonlinear Pseudo Random Sequences: 5-ary and Binary

ZHANETA N. SAVOVA[1], ANTONIYA T. TASHEVA[2], ROSEN A. BOGDANOV[3]
[1]Computer Systems and Technologies Department,
Faculty of Artillery, Air Defense and Communication and Information Systems,
National Military University,
1 Karel Shkorpil Street, Shumen, 9700,
BULGARIA

[2]Computer Systems Department,
Faculty of Computer Systems and Technologies,
Technical University of Sofia, 8 Kliment Ohridski Blvd, Sofia, 1000,
BULGARIA

[3]Communication Networks and Systems Department
Faculty of Artillery, Air Defense and Communication and Information Systems,
National Military University,
1 Karel Shkorpil Street, Shumen, 9700,
BULGARIA

Abstract: - Multi-level signals and sequences have become a significant aspect of modern high-speed communication systems. Hence, to ensure the confidentiality and integrity of the transmitted information, advanced methods and devices are necessary to produce strong cryptographic properties for not only binary but also for nonbinary keystreams, which can be used in resource-constrained microcontrollers. The proposed method and apparatus generate both a balanced nonlinear 5-ary pseudo-random sequence and a binary keystream sequence. The nonlinearity is determined by applying shrinking and multiplexing techniques to the generated linear 5-ary pseudo-random sequence and the running zero in its conversion to a binary balanced sequence.

Key-Words: - Nonbinary Pseudo Random Sequence, Nonlinear Pseudo Random Number Generation, pLFSR, Cryptography, Multilevel Signals, PAM-5.

Received: April 23, 2022. Revised: August 21, 2023. Accepted: November 15, 2023. Published: December 31, 2023.

1 Introduction

Encryption is an effective way to protect sensitive information while it is stored on media or transmitted over an untrusted communication channel over a network, allowing the information to be read and processed only by the authorized entities for which it is intended. Two basic types of cryptographic algorithms, also known as ciphers, are used in cryptography: symmetric ciphers and asymmetric ciphers. Symmetric ciphers, in turn, are classified as block ciphers and stream ciphers.

Stream ciphers are very fast and simple because they are generated by performing a bitwise XOR operation on a pseudo-random sequence of bits, called a keystream, and the information which has to be protected. Stream ciphers effectively implement the principles of the One Time Pad cipher, which is considered secure from an information theory perspective.

Various types of stream ciphers generated using block ciphers or Linear Feedback Shift Registers (LFSR) have been developed. Pseudo-random generators based on block ciphers have high computational complexity and are not suitable for application in resource constrained devices. On the other hand, LFSR registers offer a fast and efficient method for generating a linear pseudo-random sequence. To be applicable in cryptography, additional means of ensuring nonlinearity in the output sequence are applied to them. The current research is in the use of structures based on *LFSR* registers: filter generators, combinational

generators, or clock-controlled generators, and in the use of generators in finite fields, [1], [2], [3]. For instance, modern 3GPP over-the-air standards employ such structures to provide security technologies: confidentiality and integrity. For example, the word-oriented stream cipher SNOW 3G, [4], is utilized for both encryption and integrity purposes in UMTS, Extended Coverage GSM for IoT (EC-GSM-IoT), and 5G-NR. Another example is the stream ciphers ZUC, [5], [6], which is applied in LTE and 5G-NR.

Multilevel signaling has played a crucial role in enhancing the data transfer rates that current wire infrastructures can support. It provides high-speed symbol transfer rates while keeping the observed line rates relatively low. For example, a version known as PAM-5, which uses 5 levels of Pulse Amplitude Modulation, enables Gigabit Ethernet (GbE) to achieve 1Gbps data rates and 10^{-10} or lower bit error rates, [7]. A new PWAM signaling scheme is proposed in, [8], which combines dual-mode PAM-5 and PWM-2 to enhance high-speed data transmission capabilities by increasing the minimum pulse width, in comparison to the traditional PWAM scheme.

In, [9], is introduced a new method 4D PAM-7 for data center applications, involving a combination of trellis coded modulation and seven-level pulse amplitude modulation (PAM-7).

Nowadays, the term „Automotive Ethernet“, [10] primarily refers to in-vehicle networking, which encompasses communication between the different Electronic Control Units (ECUs) within a car. The authors state that two automotive Ethernet Physical layer technologies were developed, namely 100BASE-T1 and 1000BASE-T1. The current standard 802.3ab-1999 (CL40) for 1000BASE-T uses Four-Dimensional Five Level Pulse Amplitude Modulation (4D-PAM-5) and 802.3bp-2016 for 1000BASE-T1 uses PAM-3 idle symbols.

The paper compares PAM-N (N = 4, 5, 6, 7, and 8) optical signals operating at 103.12 Gbps, [11]. From the results, the PAM-5 signal is more suitable than other PAM-N signals considering the effect of chromatic dispersion for 10km single-mode fiber transmission using LAN-WDM (Wavelength-Division Multiplexing) wavelength.

As can be seen from the above, multi-level signals and sequences are emerging as a prominent feature in today's high-speed communication systems. Therefore, to ensure the security of these multi-level sequences, advanced methods and devices are required to generate not only binary but also nonbinary keystreams with strong cryptographic properties for use in embedded applications utilizing microcontrollers with low computational power and small memory.

In the context of improving higher education in security and defense, [12], innovative practical solutions would increase the knowledge of academic staff and students in the field of pseudo-random sequences and their mathematical principles.

2 Problem Formulation

In this section, we give a brief description of the problem formulation and some preliminaries that we use for the solution.

To simultaneously generate both binary and nonbinary keystreams, we make use of the mathematical background of the extended Galois Field GF(p^n) with an arbitrary prime number p, in conjunction with the properties of devices that generate p-ary linear recurrence sequences. The implementation of finite Galois fields in cryptographic algorithms is motivated by their ability to perform precise calculations without any rounding.

Linear Feedback Shift Registers (LFSR) based on a Galois Field GF(p) with a base p other than 2 can be used to generate non-binary linear recurrent sequences. For instance, the ternary and quinary recurrent sequences can form the foundation of devices that generate ternary and quinary keystream sequences. These sequences are suitable for synchronous stream ciphers within multi-level PAM signals that have 3 and 5 levels, correspondingly.

In the following third section, we present techniques that transform a linear sequence into a nonlinear one to obtain cryptographically secure nonlinear key sequences.

2.1 Mathematical Background of Extended Galois Field GF(p^n)

If the order of the Galois Field GF(q) can be expressed as a power of the prime p ($q = p^n$), where n is a positive integer greater than or equal to 2, then the field GF(q) is considered as an extension of the Galois Field GF(p) with a degree of n. In such cases, the notation Extended Galois Field GF(p^n) is applied.

To create an Extended Galois Field GF(p^n), an irreducible polynomial $p(x)$ over GF(p) is selected, [13]. Let α be an element that satisfies the equation p(α) = 0, then α is a root of $p(x)$. In this way, the elements of the field GF(p^n) are all polynomials of degree $n - 1$, which are elements of the ring GF(p)[x]. The coefficients of the polynomials belong to the GF(p).

$$GF(p^n) = \{a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 \mid a_i \in GF(p)\}. \quad (1)$$

The arithmetic is mostly computed using polynomial arithmetic modulo the irreducible polynomial $p(x)$. Two main algebraic operations, addition (4) and multiplication (5), between two elements $f(\alpha)$ and $g(\alpha)$ of GF(p^n), are defined:

$$f(\alpha) = \sum_{i=0}^{n-1} a_i\alpha^i = a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 \quad (2)$$

$$g(\alpha) = \sum_{i=0}^{n-1} b_i\alpha^i = b_{n-1}\alpha^{n-1} + \cdots + b_1\alpha + b_0 \quad (3)$$

Addition:

$$\big(f(\alpha) + g(\alpha)\big) = \sum_{i=0}^{n-1} [(a_i + b_i) \bmod p].\alpha^i \in GF(p^n). \quad (4)$$

Multiplication:

$$f(\alpha).g(\alpha) = r(\alpha),$$

where $r(\alpha)$ is the remainder, when dividing the result $c(\alpha)$ (5) by the irreducible polynomial $p(\alpha)$ of degree less than n

$$f(\alpha).g(\alpha) = \sum_{k=0}^{2(n-1)} c_k\alpha^i = c(\alpha), \quad (5)$$

with coefficients

$$c_k = \sum_{i+j=k} a_i\, b_j \bmod p, \quad 0 \le i \le n-1, 0 \le j \le n-1. \quad (6)$$

The basic operations in the extended Galois fields are elucidated by an example of the field GF(3^2). The irreducible polynomial $p(x) = x^2 + x + 2$ is used. Table 1 presents all elements of GF(3^2) in the form of polynomials, as ordered pairs of coefficients and as the power of the primitive element α.

The polynomial and n-tuple representations are better suited for addition and subtraction arithmetic operations, whereas the power of the primitive element α representation leads to faster computation for multiplication and division arithmetic operations. The following formulas are used:

If $a = \alpha^x$, $b = \alpha^y \in$ GF(p^n), then their product c is:

$$c = a.b = \alpha^x.\alpha^y = \alpha^{(x+y) \bmod (p^n-1)} \quad (7)$$

and their quotient d is

$$d = \frac{a}{b} = \frac{\alpha^x}{\alpha^y} = \alpha^{(x-y) \bmod (p^n-1)}. \quad (8)$$

As corollary of the division (8) the multiplicative inverse element a^{-1} is given by

$$a^{-1} = \frac{1}{a} = \frac{\alpha^{p^n-1}}{\alpha^x} = \alpha^{(p^n-1-x) \bmod (p^n-1)}. \quad (9)$$

Table 1. GF(3^2) elements with irreducible polynomial $p(x) = x^2 + x + 2$

№	Polynomial Representation	Representation as 2-tuple	Power of α
0	0.α + 0	0 0	**0**
1	0.α + 1	0 1	α^0
2	0.α + 2	0 2	α^4
3	1.α + 0	1 0	α^1
4	1.α + 1	1 1	α^7
5	1.α + 2	1 2	α^6
6	2.α + 0	2 0	α^5
7	2.α + 1	2 1	α^2
8	2.α + 2	2 2	α^3

The following are examples of the arithmetic operations addition, subtraction, multiplication and division of two elements 2 and 7 from GF(3^2).

Addition: 2 + 7 = (2 + 2.α + 1) = 2.α = 6.

Subtraction: 2 – 7 = (2 – 2.α – 1) = 1 + 1.α = 4.

Multiplication:

$2.7 = \alpha^4.\alpha^2 = \alpha^{6 \bmod 8} = \alpha^6 =$ 1 2 = 5.

Division: $2/7 = \alpha^4 / \alpha^2 = \alpha^{2 \bmod 8} = \alpha^2 =$ 2 1 = 7.

Multiplicative inverse:

$2^{-1} = 1/\alpha^4 = \alpha^8/\alpha^4 = \alpha^4 =$ 0 2 = 2.

$7^{-1} = 1/\alpha^2 = \alpha^8/\alpha^2 = \alpha^6 =$ 1 2 = 5.

2.2 p-ary Linear Feedback Shift Register with Galois Architecture

In this subsection, we briefly recall the basics of the p-ary Linear Feedback Shift Register (pLFSR) with Galois Architecture and its properties, [14].

The block diagram of the p-ary linear feedback shift register with Galois Architecture is shown in Figure 1. It consists of L-count delay elements a_i, i = 0, 1, …, L − 1, each of which can store one p-ary digit in the interval [0, p], where p is a prime. The output of the last significant element a_0 is put in each multiplier in a Galois Field GF(p) as it is multiplied by the coefficients q_{i+1}, i =0, 2, …, L - 2, and it is added to the content of the previous element a_i through the adder in the Galois Field GF(p). The content of the element a_0 is taken out to the output and it forms a part of the output p-ary linear sequence $\boldsymbol{A}$. During the work of the pLFSR register, whenever the content of the element i is being shifted into element i-1 for each i, $1 \le i \le L - 1$, the following recurrence relations (1) are executed:

$$a_i' = (a_{i+1} + q_{i+1}a_0) \bmod p, \quad \text{for } 0 \le i \le L-2$$
$$a_{L-1}' = q_L a_0 \bmod p \tag{10}$$

The multipliers of the feedbacks $q_i, i = 1, 2, \dots, L$ in the pLFSR register are determined by the coefficients of the primitive polynomial $q(x)$ (11) in GF(p^L) to create p-ary m-sequence with a maximum period $T = p^L - 1$.

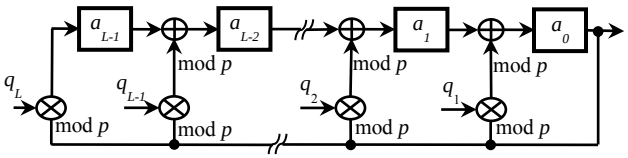

Fig. 1: p-ary Linear Feedback Shift Register with Galois architecture

If $q_L \neq 0$, the feedback polynomial $q(x)$

$$q(x) = q_L x^L + q_{L-1}x^{L-1} + \cdots + q_1 x - 1, \tag{11}$$

of degree L and the polynomial $h(x)$ of the initial state $(a_{L-1}, \dots, a_1, a_0)$

$$h(x) = a_{L-1}x^{L-1} + a_{L-2}x^{L-2} + \cdots + a_1 x + a_0 \tag{12}$$

define the generated output p-ary m-sequence $\boldsymbol{A} = (a_0, a_1, a_2, \dots)$. In this case, the generating function $O(x)$ of the pLFSR output sequence $\boldsymbol{A}$ is

$$O(x) = -\frac{h(x)}{q(x)}. \tag{13}$$

3 Problem Solution

In this section, we provide a method for generating a 5-ary nonlinear pseudo-random sequence and a binary key sequence, which is suitable for use as a synchronous stream cipher in a communication and network environment involving resource-constrained devices with increased security and efficiency of the encryption and decryption processes.

The block diagram of a keystream generator for stream ciphers is shown in Figure 2. It consists of a 5LFSR register, a selection rule block, and a binary sequence converter. The selection rule block introduces nonlinearity into the output of the 5LFSR sequence $\boldsymbol{A}$ using shrinking and multiplexing. As a result, the selection rule block produces balanced nonlinear 5-ary sequence $\boldsymbol{B}$. The binary sequence converter ensures the uniform distribution of the zero and one bits in the output keystream $\boldsymbol{C}$ by involving a running zero mechanism.

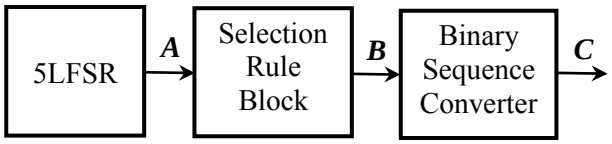

Fig. 2: Generator of a 5-ary nonlinear pseudo-random sequence and a binary keystream sequence

3.1 5-ary Linear Feedback Shift Register with Galois Architecture

For higher speed performance, the Galois field GF(5^L) was chosen based on the byte organization of processors in resource-constrained devices. Thus, the period of the output sequence $\boldsymbol{A}$ from the 5LFSR register is $T = 5^L - 1$. For ease of comprehension the proposed method for generating a 5-ary nonlinear pseudo-random sequence and a binary key sequence will be explained with the specific example shown in Figure 3.

The example uses a 5LFSR register of length 8. The primitive polynomial $q(x)$ (5)

$$q(x) = x^8 + 4x^6 + 4x^5 + 2x^4 + 2x^3 + 3x^2 + 4x + 3 \tag{14}$$

is chosen from all 48 750 primitive polynomials in GF(5^8). To construct the concrete 5LFSR scheme, the primitive polynomial (14) must be transformed into the form (11). For the transformation, the algorithm proposed in, [15], is used to determine the feedback multipliers by multiplying with the constant

$$c = \frac{4}{3} \bmod 5 = 4.2 \bmod 5 = 3. \tag{15}$$

The transformation gives the polynomial

$$\acute{q}(x) = 3x^8 + 2x^6 + 2x^5 + x^4 + x^3 + 4x^2 + 2x - 1 \tag{16}$$

that defines the 5LFSR scheme in Figure 3.

3.2 Selection Rule Block

For better resistance against correlation attacks, the choice of the nonlinear function is made in correspondence with the value of the first 5-ary digit a_{5i} of each group of five digits $(a_{5i}, a_{5i+1}, \dots, a_{5i+4}), i = 0, 1, \dots$ stored in a buffer. The first 5-ary digit determines which of the nonlinearity techniques is to be executed. If it is equal to zero, shrinking technique is executed and the 5-ary digit is not outputted. If it is greater than zero, first it is decremented and then the new value controls the output of the 4:1 multiplexer MX which forms a nonlinear 5-ary sequence. The new value $a_{5i} - 1$ determines which of the other four 5-ary digits $(a_{5i+1}, \dots, a_{5i+4}), i = 0, 1, \dots$ is to be

displayed at the output of the nonlinear 5-ary sequence. Thus, the 5-ary nonlinear output sequence ***B*** is a shrunken and multiplexed version of the linear output 5-ary sequence ***A***.

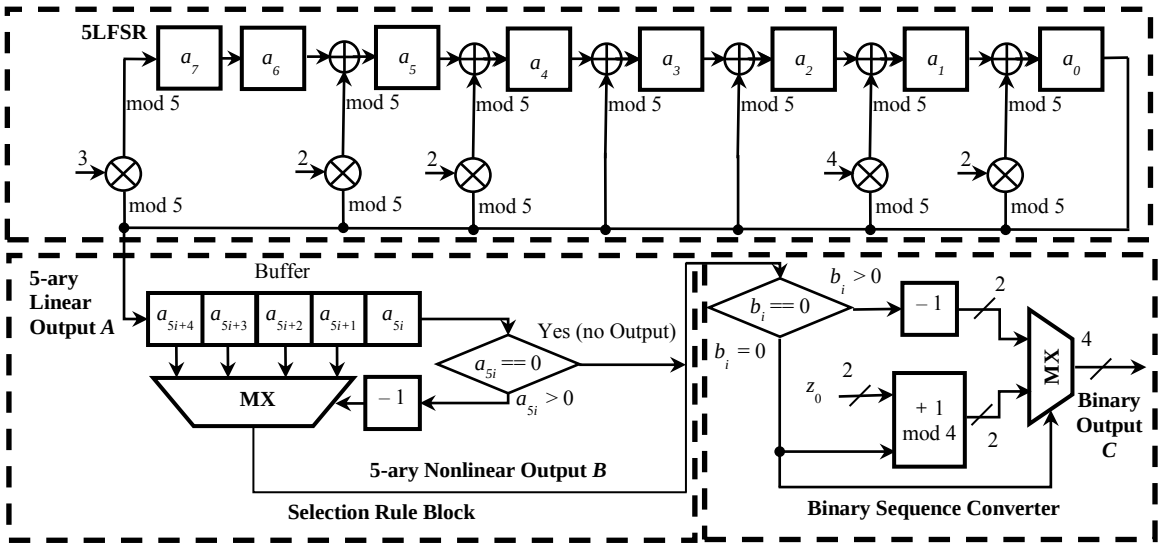

Fig. 3: Example of a generator of a 5-ary nonlinear pseudo-random sequence and a binary keystream sequence

An example of the work of the generator of a 5-ary nonlinear pseudo-random sequence and a binary keystream sequence from Figure 3 are shown in Table 1, but it only presents the first 16 outputs of the choice rule. The content of the buffer is presented in the second column of the table, the output of the choice rule – in the third column, and the fourth – the output of the balanced binary sequence converter.

In the example shown in Table 2, the initial seed of the 5LFSR is the 5-ary sequence $\underbrace{(0,0,\dots,1)}_{8}$. The buffer contains five in number 5-ary digits.

If the first one of them is a 0, the nonlinear operation of the shrinking technique is executed and there is no value produced at the output (in Table 2, it is marked with "–").

If the first digit is different from 0, its decremented value determines which input of the 4:1 multiplexer will be produced at the output of the choice rule (in Table 2, it is marked with a bold 5-ary digit).

The period $T_{\boldsymbol{B}}$ of the nonlinear 5-ary sequence, [16], is $T_{\boldsymbol{B}} = 2^2.5^{L-1}$, and the appearance count of each 5-ary digit $i = 0, 1, \dots, 4$ is equal to:

$$N_i = 2^2.5^{L-2}, i = 0, 1, \dots, 4. \qquad (17)$$

Hence, the 5-ary nonlinear pseudo-random sequence is balanced.

Table 2. Example of the work of the generator from Figure 3

№	Buffer					Choice rule	Binary representation
	a_{5i}	a_{5i+1}	a_{5i+2}	a_{5i+3}	a_{5i+4}		
0	1	**2**	3	0	0	2	01
1	2	3	**4**	1	4	4	11
2	2	0	**2**	1	1	2	01
3	2	3	**2**	1	4	2	01
4	4	0	4	3	**0**	0	**01**
5	3	4	3	**1**	2	1	00
6	3	1	1	**3**	2	3	10
7	2	2	**2**	3	1	2	01
8	4	4	2	1	**2**	2	01
9	0	1	0	4	2	–	–
10	1	**4**	1	4	2	4	11
11	1	**2**	0	4	0	2	01
12	2	1	**4**	0	3	4	11
13	0	4	1	0	2	–	–
14	2	1	**1**	2	2	1	00
15	0	2	3	3	1	–	–

3.3 Binary Sequence Converter

The binary sequence converter converts every 5-ary digit in a 2-bit sequence as the output binary sequence has an equal number of 0's and 1's, i.e. it is balanced. Every 5-ary digit b_i, i = 0, 1, … of the nonlinear 5-ary sequence is checked whether it has 0

value. If $b_i = 0$, the value of the MOD 4 counter is increased by 1 and the acquired 2 output bits of the counter are produced at the output of the generator through the 2:1 multiplexer. The initial value of the counter is the 2-bit representation of a digit q_0 that determines the initial state of the running zero. If $b_i > 0$, the value of b_i is decremented and through the 2:1 multiplexer, the binary code of b_i is outputted.

The balanced binary sequence converter presents every one of the 5-ary digits b_i in the interval $[1, 4]$through the binary representation of the $b_i - 1$ number, and the 5-ary zero as a running zero with an initial value of z_0. Every i-th appearance of the zero is presented by the value of a running zero $z_i, i = 1, 2, \dots$, realized by an equality:

$$z_i = (z_{i-1} + 1) \bmod 4 \tag{18}$$

where i is the i-th occurrence of zero in the 5-ary nonlinear sequence.

The running zero increases additionally the security of the method for generating binary keystream, because it masks the 5-ary zero consecutively with different 5-ary digits, which are different from zero.

The fourth column of Table 1 shows the output of the balanced binary sequence converter. In the given example the initial value of the running zero, $z_0 = 0$, is chosen. Because of that, the first appearance of 5-ary zero in row 4 is represented by the 2-bit binary representation of the digit 1.

The period T_c of the balanced binary sequence is $T_c = 2^3.5^{L-1}$, and the appearance count of each bit is, [16]:

$$N_{b_0} = N_{b_1} = 2^2.5^{L-1} \tag{19}$$

4 Conclusion and Feature Work

The article proposes an approach and an apparatus for a synchronous stream cipher that generates both a balanced nonlinear 5-ary pseudo-random sequence and a binary keystream sequence.

This method is suitable for the cryptographic protection of confidential data using a stream cipher with a proposed balanced nonlinear 5-ary pseudo-random sequence as a key stream when 5-level signals are transmitted in a communication environment. As a supplement, the balanced binary pseudo-random sequence is applicable to binary data encryption in a network environment that includes resource-constrained devices.

Two key features determine the enhanced reliability and cryptographic resistance of the proposed method. The main one is the use of shrinking and multiplexing techniques to introduce nonlinearity into the generated linear *p*-ary pseudo-random sequence, where *p* is an arbitrary prime. The second one, a running zero is introduced when converting the nonlinear 5-ary sequence into a balanced binary sequence. This not only enhances the security of the method but also masks the 5-ary zero with different 5-ary digits that are not zero in a consecutive manner.

However, there are some practical issues with the hardware design of the proposed method that need to be addressed. With the current focus on the fourth industrial revolution Industry 4.0, [17], companies are integrating new technologies, including the Internet of Things (IoT), cloud computing, and big data, as well as artificial intelligence and machine learning, into their production facilities and throughout their operations to ensure cybersecurity in the operations of companies that manufacture, improve and distribute their products.

The majority of network traffic on IoT devices lacks encryption, exposing sensitive and personal data to cyberattacks such as malware attacks, including ransomware, phishing attacks, denial of service attacks as well as other forms of data breaches or thefts. The suggested method and apparatus are optimal for employing stream cipher to encrypt network traffic involving IoT devices with limited resources. From a practical consideration, we need to design the Field Programmable Gate Arrays (FPGAs), [18], [19], or Application Specific Integrated Circuits (ISICs), [20], [21], hardware implementation of the proposed apparatus, which will allow faster execution of the algebraic addition and multiplication operations in the Galois field GF(5).

Acknowledgement:
The authors would like to thank the reviewers for their helpful comments.

References:

[1] S. W. Golomb and G. Gong, *Signal Design for Good Correlation: For Wireless Communication, Cryptography, and Radar*, Cambridge University Press, New York, NY, USA, 2005.

[2] Chenchev, Ivaylo, Adelina Aleksieva-Petrova, and Milen Petrov. Authentication Mechanisms and Classification: A Literature Survey. *Intelligent Computing: Proceedings of the 2021 Computing Conference, Vol. 3*. Springer International Publishing, 2021.

[3] Klein, Andreas. *Stream Ciphers.* Springer Verlag London. 2013.

[4] ETSI/SAGE Specification, Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2. Document 2: SNOW 3G Specification, 2006, [Online]. https://www.gsma.com/aboutus/wp-content/uploads/2014/12/snow3gspec.pdf (Accessed Date: October 18, 2023).

[5] ETSI/SAGE Specification, Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3. Document 2: ZUC Specification, 2011, [Online]. https://www.gsma.com/aboutus/wp-content/uploads/2014/12/eea3eia3zucv16.pdf (Accessed Date: October 18, 2023).

[6] Abdrabou, Mohammed, Ahmed Prince, and Sameh Hosny. Implementation for EEA3 algorithm based on 3GPP Standard. *14th International Computer Engineering Conference (ICENCO)*. IEEE, 2018, p. 137-140.

[7] IEEE Standard Association, IEEE Standard for Ethernet, IEEE Std 802.3™-2015, IEEE Computer Society, [Online]. https://www.onetel.de/wp-content/uploads/2016/11/802.3-2015_SECTION1.pdf (Accessed Date: October 18, 2023).

[8] H.-U. Kim and J.-K. Kang, High-speed Serial Interface using PWAM Signaling Scheme, *2022 19th International SoC Design Conference (ISOCC)*, Gangneungsi, Korea, Republic of, 2022, pp. 255-256, doi: 10.1109/ISOCC56007.2022.10031330.

[9] Stojanović, N., Prodaniuc, C., Liang, Z., Wei, J., Calabró, S., Rahman, T., Xie, C., 4D PAM-7 Trellis Coded Modulation for Data Centers, *IEEE Photonics Technology Letters*, Vol. 31, No. 5, pp. 369-372, 1 March 2019, doi 10.1109/LPT.2019.2895686.

[10] Matheus, Kirsten, and Thomas Königseder. *Automotive Ethernet*. Cambridge University Press, 2021.

[11] J. Y. Huh, J. K. Lee, S. -K. Kang and J. C. Lee, Analysis of PAM-N (N=4, 5, 6, 7 and 8) signals operating at 103.125 Gbps for next-generation Ethernet, *12th International Conference on Optical Internet 2014 (COIN)*, Jeju, Korea (South), 2014, pp. 1-2, doi: 10.1109/COIN.2014.6950548.

[12] Marchisio, M., Roman, F., Sacchet, M., Spinello, E., Linko, N., Malgorzata, G., Madgalena, R. and Cristian-Emil, M., Teachers' digital competences before and during the COVID-19 pandemic for the improvement of security and defence higher education. *16th International Conference e-Learning, EL 2022-Held at the 16th Multi-Conference on Computer Science and Information Systems, MCCSIS 2022*, 2022, pp. 68-75.

[13] Beletsky, Anatoly. An Effective Algorithm for the Synthesis of Irreducible Polynomials over a Galois Fields of Arbitrary Characteristics. *WSEAS Transactions on Mathematics*, vol. 20, 2021, pp.508-519, https://doi.org/10.37394/23206.2021.20.54.

[14] M. Goresky, A. Klapper, Fibonacci and Galois Representations of Feedback-With-Carry Shift Registers, *IEEE Trans. on Inform. Theory, vol. 48*, pp. 2826−2836, November 2002.

[15] Tasheva, A., Savova-Tasheva, Z., Petrov, B., Stoykov, K. Determining the feedback multipliers in a p-ary linear feedback shift registers. *WSEAS Transactions on Systems and Control*, vol.13, 2018, pp.420-424.

[16] Tasheva, Antoniya Todorova, Zhaneta Nikolova Tasheva, and Aleksandar Petrov Milev. Generalization of the self-shrinking generator in the Galois Field GF (p^n). *Advances in Artificial Intelligence* 2011, 2011: 1-10.

[17] Kraus, N., Kraus, K., Shtepa, O., Hryhorkiv, M. and Kuzmuk, I., Artificial intelligence in established of industry 4.0. *WSEAS Transactions on Business and Economics*, vol. 19, 2022, pp.1884-1900, https://doi.org/10.37394/23207.2022.19.170.

[18] Balasubramanian, P. and Mastorakis, N.E., FPGA based implementation of distributed minority and majority voting based redundancy for mission and safety-critical applications. *International Journal of Circuits and Electronics*, 2016. *arXiv preprint arXiv: 1611.09446*.

[19] Shiyang, H., Hui, L., Qingwen, L., Fenghua, L. A Time-Area-Efficient and Compact ECSM Processor over GF (p). *Chinese Journal of Electronics*, *32*(6), 2023, pp. 1355-1366.

[20] Balasubramanian, P. and Mastorakis, N.E., ASIC-based implementation of synchronous section-carry based carry lookahead adders. *Recent Advances in Circuits, Systems, Signal Processing and Communications*, 2016, *arXiv preprint arXiv: 1603.07961*.

[21] Patwari, N. D., Srivastav, A., Kabra, M., Jonna, P., Rao, M. Design and evaluation of

finite field multipliers using fast XNOR cells. In *Proceedings of the Great Lakes Symposium on VLSI 2023*, 2023, pp. 163-166.

Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)

The authors equally contributed to the present research, at all stages from the formulation of the problem to the final findings and solution.

Sources of Funding for Research Presented in a Scientific Article or Scientific Article Itself

The article was prepared with the financial support of the National Scientific Program "Security and Defence", funded by the Ministry of Education and Science of the Republic of Bulgaria, in implementation of Decision № 731 of 21.10.2021 of the Council of Ministers of the Republic of Bulgaria.

Conflict of Interest

The authors have no conflicts of interest to declare that are relevant to the content of this article.