

Preliminary Analysis of Interleaving PN-Sequences

Sara D. Cardell[1(✉)], Amparo Fúster-Sabater[2], and Verónica Requena[3]

[1] Centro de Matemática, Computação e Cognição, UFABC, Santo André-SP, Brazil
s.cardell@ufabc.edu.br
[2] Instituto de Tecnologías Físicas y de la Información (CSIC), Madrid, Spain
amparo@iec.csic.es
[3] Departamento de Matemáticas, Universidad de Alicante, Alicante, Spain
vrequena@ua.es

Abstract. Some pseudorandom sequences with good crytographic features can be obtained from the interleaving of other families of sequences with unsuitable properties. PN-sequences obtained from maximum-length Linear Feedback Shift Registers exhibit good statistical aspects, such as balancedness, large period, adequate distribution of 0s and 1s and excellent autocorrelation, although their linearity makes them vulnerable against cryptographic attacks. In this work, we present a preliminary analysis on the random features of the interleaving of shifted versions of a PN-sequence. The application of statistical and graphic tests and their corresponding results complete the work.

Keywords: PN-sequence · t-interleaved sequence · Statistical tests · Randomness

1 Introduction

The interleaving of sequences has been a topic quite studied in the literature [12,25,26]. Interesting algebraic and geometric results can be obtained by interleaving term by term integer sequences [17]. In [36], the authors obtained new families of almost balanced binary sequences with an optimal auto-correlation value. As an extension of this work, in [19] the author investigated at what extent interleaved binary sequences with period $4p$ obtained with the technique given in [36] from Legendre and Hall sequences have high linear complexity. Furthermore, in [27] the authors explored the linear complexity of three families of binary sequences built from interleaving Legendre sequences, generalized GMW sequences and twin-prime sequences (see also [38]). The interleaving of pseudorandom sequences has been also used for signal synchronization (see [6]). Here, the author constructed a binary timing sequence produced by interleaving shorter pseudorandom sequences and discovered the parameter values giving the minimum acquisition time. This paper also shows that there exists an optimum number of component sequences for a proper interleaving.

© Springer Nature Switzerland AG 2021
O. Gervasi et al. (Eds.): ICCSA 2021, LNCS 12949, pp. 287–297, 2021.
https://doi.org/10.1007/978-3-030-86653-2_21

The output sequences of a maximum-length LFSR (Linear Feedback Shift Register) are called PN-sequences (or m-sequences) [24]. Some keystream generators combine these PN-sequences using nonlinear functions in order to increase their linear complexity and destroy their linearity producing keystream sequences for cryptographic purposes. A very popular group of keystream generators is the family of decimation-based sequence generators. Inside this class, the shrinking generator was the first one to be introduced [16]. This generator is very easy to implement and its formation rule is based on the irregular decimation of one PN-sequence using the position of the ones of another PN-sequence. In [8], the authors proved that the sequence produced by the shrinking generator (the shrunken sequence) can be also generated interleaving shifted versions of a PN-sequence. The vulnerability of this generator consists in the fact that the shifts are known (see [8]), i.e., a shrunken sequence cannot be generated from random shifted versions of a given PN-sequence. Some authors used this fact to perform cryptanalytic attacks in order to break this generator (see for instance [7–11]). A natural way to get over this weakness is to modify the shifts or to interleave PN-sequences produced by different primitive polynomials.

In [12], the authors introduced the concept of t-interleaved sequence defined as the sequence resultant of interleaving t sequences. They focused on the study of the characteristics of the sequences obtained interleaving shifted versions of a single PN-sequence with different shifts. In this work, we present a preliminary study on the randomness of these sequences. Furthermore, we perform an important battery of tests such as FIPS $140-2$, created by the National Institute of Standard and Technology [37], Maurer's Universal Statistical Test [31], and Lempel-Ziv Complexity Test [18] as well as some graphic tests effective to investigate the behaviour of these sequences. The sequences that pass all the tests above and have pseudorandom behaviour are potential candidates to be used as keystream sequences in stream cipher applications [4,33]. Recall that in stream ciphers the encryption is made XOR-ing the plaintext and the keystream. The decryption is also made XOR-ing the ciphertext and the keystream. This keystream must satisfy certain randomness characteristics, since the security of the cipher depends completely on such a sequence. For example, the shrinking generator is part of the internal structure of different stream ciphers as the EP0619659A2 [15], an European patent application; or the Decim^{v2}, a hardware oriented stream cipher submitted to the ECRYPT Stream CipherProject (eSTREAM) [1], among other applications [5,14]. In addition, the shrunken sequence has been considered as a particular solution of a kind of linear difference equations. In [13,22] the authors analyzed cryptographic parameters of this decimated sequence in terms of solutions to linear equations. This sequence has been also studied as the output sequence of linear elementary cellular automata (CA) [8]. In [8] the authors used these CA and their properties to recover the complete shrunken sequence. Therefore, it would be interesting to study these applications using the t-interleaving sequences instead of the shrunken sequence and compare the results.

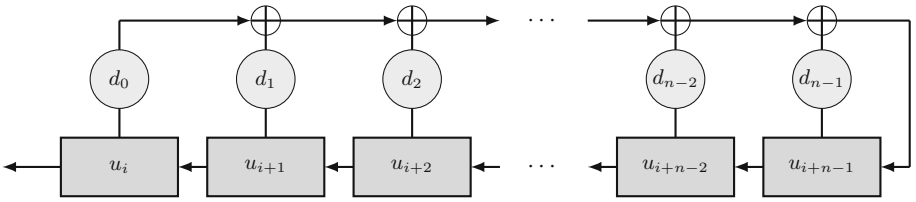


Fig. 1. An LFSR of length n

This paper is organized as follows: In Sect. 2, we introduce some basic notions and generalities about PN-sequences and the interleaving of such sequences. In Sect. 3, we perform a randomness analysis of the interleaving of shifted versions of a PN-sequence. Tables, figures and numerical results of the applied tests are also provided. At last, in Sect. 4, we conclude our research with some finale statements and some directions for the future.

2 Fundamentals and Basic Concepts

Let $\mathbb{F}_2 = \{0, 1\}$ be the binary field, also known as the Galois field of two elements. Let $\{u_i\} = \{u_0, u_1, u_2, u_3, \ldots\}$ be a binary sequence, that is, each term of the sequence satisfies $u_i \in \mathbb{F}_2$, $i \geq 0$. We say that $\{u_i\}$ is a periodic sequence if there exists a positive integer τ such that $u_{i+\tau} = u_i$, for all $i \geq 0$. This number τ is known as the period of the sequence.

Let n be a positive integer and $d_0, d_1, \ldots, d_{n-1}$ some elements of $\mathbb{F}_2$. A sequence $\{u_i\}$ is called a binary n-th order linear recurring sequence if it satisfies

$$u_{i+n} = d_{n-1}u_{i+n-1} + d_{n-2}u_{i+n-2} + \ldots + d_1u_{i+1} + d_0u_i, \qquad i \geq 0 \qquad (1)$$

The relation in (1) is known as an n-th order linear recurrence relationship (l.r.r). The polynomial of degree n given by

$$p(x) = x^n + d_{n-1}x^{n-1} + d_{n-2}x^{n-2} + \ldots + d_1x + d_0 \in \mathbb{F}_2[x],$$

is called the characteristic polynomial of the l.r.r. (and the characteristic polynomial of $\{u_i\}$).

The generation of linear recurring sequences can be carried out through Linear Feedback Shift Registers (LFSRs) [24]. An LFSR of length n is a device composed of n interconnected stages. The initial state (stage contents at round zero) is the seed, and since the register operates in a deterministic form, the resultant sequence is completely determined by the initial state. The input of each round is a bit resultant from applying a linear transformation function to a previous state (see Fig. 1). If the characteristic polynomial $p(x)$ of the corresponding l.r.r. is primitive, then the LFSR is said to be a maximum-length. Furthermore, the resultant sequence $\{u_i\}$ obtained from a maximum-length LFSR of n stages is called PN-sequence (or m-sequence) and its period is $\tau = 2^n - 1$ (2^{n-1} ones and $2^{n-1} - 1$ zeros) [24].

The linear complexity of a sequence, denoted by LC, can be defined as the lowest order l.r.r. that produces the sequence (in other words, the length of the shortest LFSR that produces it). The Berlekamp-Massey algorithm can determine the characteristic polynomial and the LC of the sequence given $2 \cdot LC$ bits of the sequence [29]. Therefore, it is obvious that the LC must be as large as possible and that LFSRs should never operate as keystream generators (since their LC is quite low). Their linearity has to disappear; that is, their LC has to grow in order to consider their output sequences for cryptographic goals.

The following definition introduces the concept of t-interleaved sequence, the main notion of this paper.

Definition 1. *The sequence* $\{v_j\}$ *is a* t***-interleaved sequence*** *if it is obtained interleaving* t *sequences* $\{a_i^{(1)}\}$, $\{a_i^{(2)}\}$, ..., $\{a_i^{(t)}\}$, *all of them with the same period* τ. *As a consequence, the sequence* $\{v_j\}$ *has the following form:*

$$\{v_j\} = \left\{a_0^{(1)}, a_0^{(2)}, \ldots, a_0^{(t)}, a_1^{(1)}, a_1^{(2)}, \ldots, a_1^{(t)}, \ldots, a_{\tau-1}^{(1)}, a_{\tau-1}^{(2)}, \ldots, a_{\tau-1}^{(t)}\right\}.$$

In this work, we consider that each one of the sequences $\{a_i^{(k)}\}$, $k = 1, \ldots, t$, is a shifted version a PN-sequence $\{a_i\}$. It is worth noticing that if the characteristic polynomial of $\{a_i\}$ is primitive with degree n, then the resultant t-interleaved sequence is nearly balanced with $t \cdot 2^{n-1}$ ones.

In [12], the authors studied the period and LC of the interleaving of PN-sequences. They mostly focused on the interleaving of 2^r (a power of two) PN-sequences produced by the same primitive polynomial, that is, shifted versions of one single PN-sequence. In Sect. 3, we perform a deeper analysis on the random characteristics of these new interleaving sequences, maintaining the focus on the interleaving of shifted versions of a PN-sequence.

3 Randomness of the *t*-interleaved Sequences

Currently, an important and widely studied topic is to design non-linear lightweight cryptography generators that produce sequences with good distribution and statistical properties [8,20]. The study of randomness and unpredictability of the sequences obtained by random number generators is essential to assess the quality of them and their use in many applications as cryptography, numerical analysis, information transmission, or game theory, among others [1,21,23]. For that, we need some tools to evaluate whether a generator is random or not.

There are different statistical batteries and graphic techniques to carry out this purpose. In this work, we present some results obtained through some of the main statistical tests, as FIPS 140-2, Maurer's Universal Statistical Test, and Lempel-Ziv Complexity Test.

Moreover, we show some graphic tests, as chaos game or return map, which help us to visualize the sequences generated and determine if they can be considered random. It is worth highlighting that although the sequences pass all these

tests, it does not mean we have a perfect random number generator, but the confidence in the generator increases. Moreover, we should expect some sequences to appear nonrandom and fail at least some of the tests. However, if many sequences fail the tests, we should be suspicious that our generator is not good.

In our study, we have analyzed hundreds of t-interleaved sequences for different values of t and generated from characteristic polynomials of degree L, with $15 \leq L \leq 21$. In this section, we show the media of the values obtained for t-interleaved sequences obtained with various characteristic polynomials of degree 21.

Firstly, we expose results obtained for our t-interleaved sequences using the statistical tests mentioned above.

FIPS 140-2

The FIPS $140-2$ is composed of four statistical tests which evaluate whether a given sequence of numbers is random. For this goal, we need to assess binary streams of 20000 bits. Any failure in some of these tests means that the sequence must be rejected. Next, we give a little introduction about these tests and the criteria used to determine whether a sequence pass each of the tests.

1. *Monobit test*: Count the number of 0 and 1 in the bitstream. If we denote by X the number of 1s, then the test is passed if $X \in (9725, 10275)$.
2. *Poker test*: Divide the sequence into blocks of 4 bits. Count and save the number of coincidences of the 16 possible decimal values for the 4 bit blocks. Let $f(i)$ be the number of times that each one of these values appear, with $i \in [0, 15]$. Compute

$$X = \frac{16}{5000} \sum_{i=1}^{16} f(i)^2 - 5000.$$

   If $X \in (1.03, 57.4)$, then the test is passed.
3. *Runs test*: A run is a maximal succession of consecutive identical bits (all ones or all zeros) within the bitstream. Count and store the frequencies of runs of all lengths (of lengths 1 through 6) in the sequence. For the intentions of this test, runs with length >6 are considered in the range of length 6. If the runs occurred are each within the corresponding interval specified in Table 1, then the test is passed.
4. *Long runs test*: Long runs are runs of length ≥ 26 (either zeros or ones).

We show the results of the Runs test by a graphic representation. In Fig. 2, we determine that the test is passed if the runs (runs of zeros, represented by a red line, and runs of ones, represented by a blue line) that occur are each within the green lines which represent the specific intervals determined in Table 1.

Table 1. Required intervals for the different lengths of runs in the Runs Test

Length of the run	Required interval
1	2,315–2,685
2	1,114–1,386
3	527–723
4	240–384
5	103–209
6+	103–209

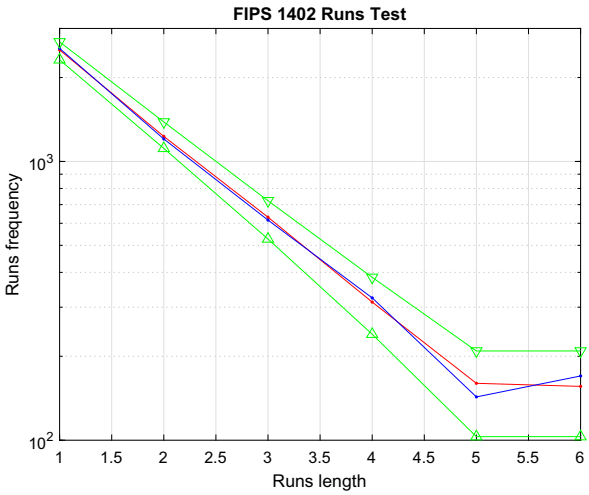


Fig. 2. Runs test for a 4-interleaved sequence of degree $L = 16$. (Color figure online)

Maurer's Universal Test
This test is one of the 15 tests from the NIST statistical suite [3] for cryptographic use. It locates the most general class of statistical faults. The randomness of a binary sequence is checked by the entropy of the sequence, which is calculated from the repetition intervals of blocks of length l in the sequence. The sequence can be considered random, if the p-valued obtained is ≥ 0.01.

Lempel-Ziv Compression Test
This is a compression algorithm which replace strings that repeat in the sequence with references to locations where they appeared first or with the length of repeated pattern. The aim of this test is to determine how far the sequence evaluated can be compressed. For this, the number of distinct patterns in the sample stream will be analyzed. It is considered to be random if it can not be compressed. If the p-value is greater or equal to 0.01, then Lempel-Ziv Test is passed.

All the analyzed t-interleaved sequences have successfully passed each one of the previous tests. Table 2 presents a small sample of the results obtained in Monobit test, Poker test, Maurer's Universal test, and Lempel-Ziv test, given different t-interleaved sequences obtained by characteristic polynomials of degree 21. All these values are the average of the results obtained for any sample of t-interleaved sequences studied.

Table 2. Statistical test results for t-interleaved sequences obtained by characteristic polynomials of degree 21.

t-interleaved	Monobit test	Poker test	Maurer's test	Lempel-Ziv test
3	10008	20.6272	0.5778	0.9719
4	10001	16.2688	0.5715	0.6703
5	10018	16.9600	0.0594	0.0931
6	9838	10.7584	0.2842	0.5584
7	9945	17.4656	0.1482	0.6703
8	9934	15.4048	0.1422	0.6703

Next, we present two powerful graphic tools, the return application and chaos game, which allow us to analyze the behaviour of our t-interleaved sequences from a visual representation.

Return map

The return map visually measures the entropy of the sequence. This method is an important cryptanalysis tool for chaotic cryptosystems introduced in [35] to destroy diverse schemes based on the Lorenz system.

A interesting way to explore a random number generator is to create a visualisation of the numbers that it produces. This type of methods should not be considered as a formal analysis of the study of pseudorandom sequences, but it can get a rough impression of the functioning of these. Obtaining a cloud with patterns or fractals means that the sequence is non-random.

Figure 3 exhibits the return application of the 5-interleaved sequence generated by $p(x) = x^{16} + x^{14} + x^{12} + x + 1$. We observe that the graph is a messy cloud without patterns which means that our sequences are random.

However, Figs. 4a and 4b are return applications of two 8-interleaved sequences generated with a characteristic polynomial of degree 16 and 17, respectively; we can observe the lack of randomness of these sequences since that present clear patterns. At first glance, it seems that these imperfect sequences only appear in some particular cases where t is a power of 2.

Chaos game

The chaos game is a most popular algorithm for approximating IFS fractals [2,28,34]. This algorithm allows to carry out the conversion of a given sequence into a $2D$ representation of that. As return application, this method is used

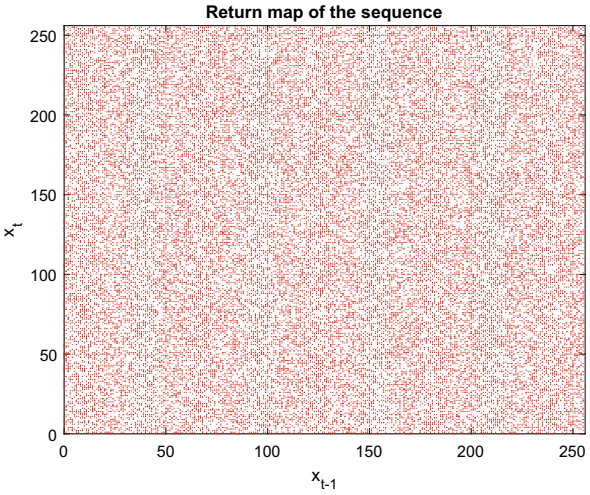
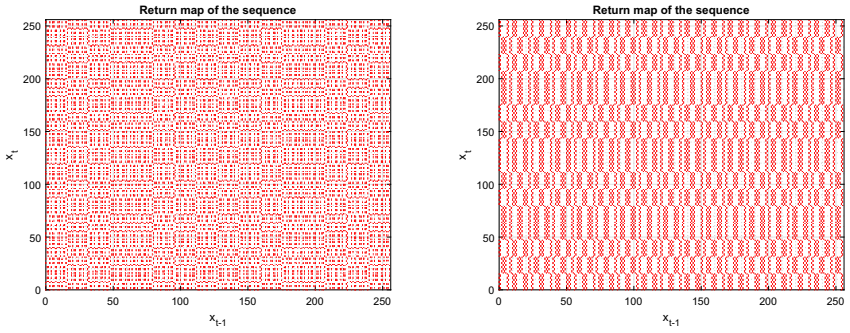


Fig. 3. Return map of a 5-interleaved sequence of degree 16.



(a) Return map of a 8-interleaved sequence of degree 17.

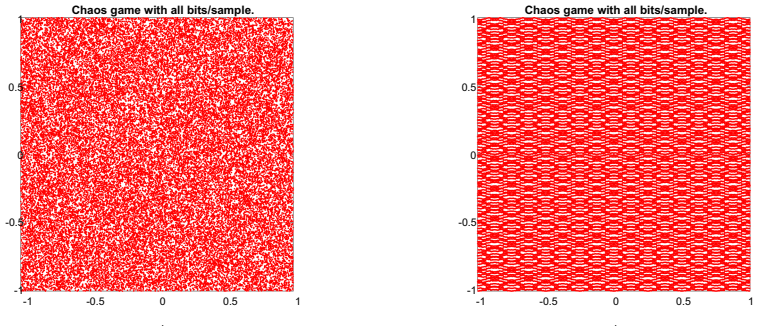
(b) Return map of a 8-interleaved sequence of degree 16.

Fig. 4. Return maps of imperfect 8-interleaved sequences.

to analyze random number generators using visual representations of the data generated [30,32].

In Fig. 5a, we show the chaos game representation of the 5-interleaved sequence given previously. In this case, there is no any shape or figure, it is a disordered cloud of points which implies good randomness. However, in Fig. 5b, we obtain the chaos game for an 8-interleaved sequence generated with the characteristic polynomial of degree 16, $q(x) = x^{16} + x^{13} + x^{11} + x^{10} + x^9 + x^6 + x^3 + x^2 + 1$. In fact, we can observe a fractal structure repeated in this representation. It means that our sequence cannot been considered random. These chaos game representations with such a well-defined patterns have only occurred on

rare occasions, in a very insignificant percentage of t-interleaved sequences. However, as in the return map case, these imperfect sequences have the peculiarity that the value of t is a power of 2.



(a) Chaos game of a 5-interleaved sequence of degree 16.

(b) Chaos game of a 8-interleaved sequence of degree 16.

Fig. 5. Chaos game of t-interleaved sequences.

4 Conclusions

In this paper, we perform a preliminary analysis on the randomness of the t-interleaved sequences. We use statistical and graphic tools to analyze the random behaviour of these sequences. All our sequences have passed the statistical tests successfully. Therefore, these sequences are suitable as keystream sequences in stream cipher applications. Using two important graphic representations in the analysis of pseudorandom number generators, we have observed that for some particular cases, as for instance when t is a power of 2, we can obtain sequences that cannot be considered random. As a future work, we would like to analyze with more detail these cases where our sequences fail in order to determine the best values of t for which we can generate t-interleaved sequences with good cryptographic properties. We would also like to study the interleaving of PN-sequences generated from different primitive polynomials since that it could contribute to obtain better cryptographic results.

Acknowledgments. This work was in part supported by Comunidad de Madrid (Spain) under project CYNAMON (P2018/TCS-4566), co-funded by FSE and European Union FEDER funds. The third author is partially supported by Spanish grant VIGROB-287 of the Universitat d'Alacant.

References

1. Wu, H.: The stream cipher HC-128. In: Robshaw, M., Billet, O. (eds.) New Stream Cipher Designs. LNCS, vol. 4986, pp. 39–47. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-68351-3_4

2. Barnsley, M.: Fractals Everywhere. Academic Press, Cambridge (1988)
3. Bassham, L., et al.: A statistical test suite for random and pseudorandom number generators for cryptographic applications (16 September 2010). https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=906762
4. Biryukov, A., Perrin, L.: State of the art in lightweight symmetric cryptography. IACR Cryptol. ePrint Arch. **2017**, 511 (2017)
5. Bishoi, S.K., Senapati, K., Shankar, B.: Shrinking generators based on σ-LFSRs. Discret. Appl. Math. **285**, 493–500 (2020). https://www.sciencedirect.com/science/article/pii/S0166218X20303346
6. Bluestein, L.I.: Interleaving of pseudorandom sequences for synchronization. IEEE Trans. Aerosp. Electron. Syst. AES **4**(4), 551–556 (1968)
7. Caballero-Gil, P., Fúster-Sabater, A., Pazo-Robles, M.E.: New attack strategy for the shrinking generator. J. Res. Pract. Inf. Technol. **41**(2), 171–180 (2009)
8. Cardell, S.D., Aranha, D.F., Fúster-Sabater, A.: Recovering decimation-based cryptographic sequences by means of linear CAs. Logic J. IGPL **28**(4), 430–448 (2020)
9. Cardell, S.D., Fúster-Sabater, A.: Cryptanalysing the shrinking generator. Procedia Comput. Sci. **51**, 2893–2897 (2015)
10. Cardell, S.D., Fúster-Sabater, A.: Performance of the cryptanalysis over the shrinking generator. In: Herrero, Á., Baruque, B., Sedano, J., Quintián, H., Corchado, E. (eds.) International Joint Conference. CISIS 2015. Advances in Intelligent Systems and Computing, vol. 369. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-19713-5_10
11. Cardell, S.D., Fúster-Sabater, A., Ranea, A.: Linearity in decimation-based generators: an improved cryptanalysis on the shrinking generator. Open Math. **16**(1), 646–655 (2018)
12. Cardell, S.D., Fúster-Sabater, A., Requena, V.: Interleaving shifted versions of a PN-sequence. Mathematics **9**(687), 1–23 (2021)
13. Cardell, S.D., Fúster-Sabater, A.: Linear models for high-complexity sequences. In: Gervasi, O., et al. (eds.) ICCSA 2017, Part I. LNCS, vol. 10404, pp. 314–324. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-62392-4_23
14. Díaz Cardell, S., Fúster-Sabater, A.: Cryptography with Shrinking Generators. SM, Springer, Cham (2019). https://doi.org/10.1007/978-3-030-12850-0
15. Coppersmith, D., Herzberg, A., Krawczyk, H.M., Kutten, S., Mansour, Y.: A shrinking generator for cryptosystems (1987). https://patents.google.com/patent/EP0619659A2/en
16. Coppersmith, D., Krawczyk, H., Mansour, Y.: The shrinking generator. In: Stinson, D.R. (ed.) CRYPTO 1993. LNCS, vol. 773, pp. 22–39. Springer, Heidelberg (1994). https://doi.org/10.1007/3-540-48329-2_3
17. Crilly, T.: Interleaving integer sequences. Math. Gaz. **91**(520), 27–33 (2007)
18. Doğanaksoy, A., Göloğlu, F.: On Lempel-Ziv complexity of sequences. In: Gong, G., Helleseth, T., Song, H.-Y., Yang, K. (eds.) SETA 2006. LNCS, vol. 4086, pp. 180–189. Springer, Heidelberg (2006). https://doi.org/10.1007/11863854_15
19. Edemskiy, V.: On the linear complexity of interleaved binary sequences of period 4p obtained from hall sequences or Legendre and hall sequences. Electron. Lett. **50**(8), 604–605 (2014)
20. Eisenbarth, T., Kumar, S., Paar, C., Poschmann, A., Uhsadel, L.: A survey of lightweight-cryptography implementations. IEEE Des. Test Comput. **24**(6), 522–533 (2007)

21. Fluhrer, S.R., McGrew, D.A.: Statistical analysis of the alleged RC4 keystream generator. In: Goos, G., Hartmanis, J., van Leeuwen, J., Schneier, B. (eds.) FSE 2000. LNCS, vol. 1978, pp. 19–30. Springer, Heidelberg (2001). https://doi.org/10.1007/3-540-44706-7_2
22. Fúster-Sabater, A.: Generation of cryptographic sequences by means of difference equations. Appl. Math. Inf. Sci. **8**, 475–484 (2014)
23. Gennaro, R.: Randomness in cryptography. IEEE Secur. Priv. **4**(02), 64–67 (2006)
24. Golomb, S.W.: Shift Register-Sequences. Aegean Park Press, Laguna Hill (1982)
25. Gong, G.: Theory and applications of q-ary interleaved sequences. IEEE Trans. Inf. Theory **41**(2), 400–411 (1995)
26. Jiang, S., Dai, Z., Gong, G.: On interleaved sequences over finite fields. Discret. Math. **252**, 161–178 (2002)
27. Li, N., Tang, X.: On the linear complexity of binary sequences of period $4n$ with optimal autocorrelation value/magnitude. IEEE Trans. Inf. Theory **57**(11), 7597–7604 (2011)
28. Martyn, T.: The chaos game revisited: yet another, but a trivial proof of the algorithm's correctness. Appl. Math. Lett. **25**(2), 206–208 (2012). https://www.sciencedirect.com/science/article/pii/S0893965911003922
29. Massey, J.: Shift-register synthesis and BCH decoding. IEEE Trans. Inf. Theory **15**(1), 122–127 (1969)
30. Mata-Toledo, R.A., Willis, M.A.: Visualization of random sequences using the chaos game algorithm. J. Syst. Softw. **39**(1), 3–6 (1997). https://www.sciencedirect.com/science/article/pii/S0164121296001586
31. Maurer, U.M.: A universal statistical test for random bit generators. J. Cryptol. **5**(2), 89–105 (1992). https://doi.org/10.1007/BF00193563
32. Orúe, A.B., Fúster-Sabater, A., Fernández, V., Montoya, F., Hernández, L., Martín, A.: Herramientas gráficas de la criptografía caótica para el análisis de la calidad de secuencias pseudoaleatorias, p. 180–185. Actas de la XIV Reunión Española sobre Criptología y Seguridad de la Información, RECSI XIV, Menorca, Illes Balears, Spain (October 2016)
33. Orúe, A.B., Hernández, L., Martín, A., Montoya, F.: A lightweight pseudorandom number generator for securing the Internet of Things. IEEE Access **5**, 27800–27806 (2017)
34. Peitgen, H.O., Jurgens, H., Saupe, D.: Chaos and Fractals: New Frontiers of Science. Springer, Heidelberg (2004). https://doi.org/10.1007/b97624
35. Pérez, G., Cerdeira, H.A.: Extracting messages masked by chaos. Phys. Rev. Lett. **74**, 1970–1973 (1995). https://link.aps.org/doi/10.1103/PhysRevLett.74.1970
36. Tang, X., Ding, C.: New classes of balanced quaternary and almost balanced binary sequences with optimal autocorrelation value. IEEE Trans. Inf. Theory **56**(12), 6398–6405 (2010)
37. U.S. Department of Commerce: FIPS 186, Digital signature standard. Federal Information Processing Standards Publication 186, N.I.S.T., National Technical Information Service, Springfield, Virginia (1994)
38. Xiong, H., Qu, L., Li, C., Fu, S.: Linear complexity of binary sequences with interleaved structure. IET Commun. **7**(15), 1688–1696 (2013)