# On the linear complexity of shrunken sequences

Ana I. Gómez
Universidad Rey Juan Carlos
Móstoles, Madrid, Spain
ana.gomez.perez@urjc.es

Domingo Gómez-Pérez
Universidad de Cantabria
Santander, Spain
domingo.gomez@unican.es

Verónica Requena
Universidad de Alicante
Alicante, Spain
vrequena@ua.es

**Abstract**

The shrinking generator is a pseudorandom bit generator based on the combination of two linear feedback shift registers of maximum period. These registers are synchronized with a common clock and produce binary sequences with good statistical properties. Due to its simplicity and efficient implementation, the shrinking generator is particularly suitable for stream cipher cryptographic schemes and most proposed attacks rely on the properties of the generator. Consequently, its analysis serves as the foundation for other interleave constructions. In our work, we present a closed formula for the linear complexity of its output. Additionally, we establish the first bound on its linear complexity profile. Our techniques involve two-dimensional arrays and their interleave structure, which could prove valuable for other pseudorandom bit generators.

## 1 Introduction

Pseudo-Random Number Generators (PRNGs) are deterministic algorithms [10, 21] used to generate number sequences which appear to be random. They are employed for cryptographic applications such as key and nonce generation, digital signatures, masking protocols, IoT security, etc.

Linear Feedback Shift Registers (LFSRs) play an important part in the design of cryptographic PNRGs [15, 23]. Binary sequences generated by maximal-period LFSRs, whose characteristic polynomial is primitive, are called PN-sequences or m-sequences [13]. These have been extensively used in many and diverse applications such as e-Commerce, mobile wireless communications, digital broadcasting, or cryptography (stream ciphers) [3, 20], because they exhibit the largest possible period and present good randomness properties such as balancedness, low correlation, excellent run distribution, and so forth. However, they are easily predictable due to their inherent linearity. In order to ensure their cryptographic suitability, maintaining at the same time the pseudorandomness properties, different design techniques are applied: non-linear filtering, combinatorial generators, clock-controlled generators, or the irregular decimation of PN-sequences, among others. We focus our attention on the latter.

Irregularly decimating the output sequences of m-sequences generates powerful PN-RGs [9] i.e. it produces sequences with good cryptographic properties. One of the most important generators in this family is the *shrinking generator (SG)* [8], built from two LFSRs with different lengths. This generator is fast, easy to implement, and generates good cryptographic sequences, which is appropriated for efficient applications in low-end devices such as stream cipher cryptosystems [2, 4, 9]. A great family of decimation-based sequence generators have emerged from the former: the self-shrinking generator [19], the generalized self-shrinking generator [16], the modified self-shrinking generator [17], and the $t$-modified self-shrinking generator [7]. Each of these generators are based on same principle, with different approaches to avoid certain attacks to the linearity of the construction. We focus on the shrinking generator, because it is the original architecture of the generators as a starting study that we hope can be extended for the derived families.

The row by row (snake like) folding of a sequences produces arrays which are useful in single periodic or aperiodic applications. This structure in the shrinking generator was explored by Cardell et al. [6] in order to characterize the cryptographic related properties.

Our analysis is based on the transformation of sequences into arrays using the Chinese remainder theorem (CRT). This is equivalent to folding a sequence along the leading diagonal of an array whose dimensions are relatively prime. The equivalence in this case between both array construction methods has already been studied and understood [14]. This implies that in the case of a sequence built by the shrinking generator the columns are cyclic shifts of a shorter m-sequence. This fundamental difference to the row by row folding is crucial to study the properties of the array.

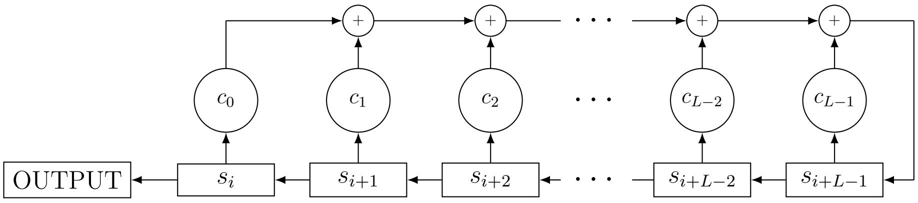
This paper is structured as follows: Section 2 introduces the necessary background and presents the main theorem of our study. In Section 3, we provide the proof of the main result with a detailed and rigorous justification for our theorem. Finally, we finish the paper with conclusions and future works in Section 4, where we summarize our findings and suggest potential directions for future research

## 2 Mathematical Preliminaries and main result

Let $\mathbb{N}_0 = \{0, 1, 2, \ldots\}$ be the set of nonnegative integers and $\mathbb{F}_2 = \{0, 1\}$ the Galois field of two elements. A *binary sequence* $(s_i)$ is a mapping from $\mathbb{N}_0$ to $\mathbb{F}_2$. It is *periodic* if there exists a positive integer $T$ such that $s_{i+T} = s_i$, for all $i \in \mathbb{N}_0$.

A linear feedback shift register (LFSR) [13] is an electronic device with $L$ memory cells (stages) with binary content. At every clock pulse, the binary element of each stage is shifted to the adjacent one and a new element is computed through the linear feedback to fill the empty stage (see Figure 1).

Figure 1: LFSR of length $L$



We present the definition of two security metrics for sequences which rely on LFSRs: the *linear complexity* and the *linear complexity profile.*

**Definition 1.** Let $L$ be a positive integer and $c_0, c_1, \dots, c_{L-1} \in \mathbb{F}_2$. A binary sequence $\mathbf{s} = (s_i)$ satisfying

$$s_{i+L} = \sum_{j=0}^{L-1} c_j s_{i+j}, \tag{1}$$

for all $i \in \mathbb{N}_0$ is called an ($L$-th order) *linear recurring sequence (LRS)* and the monic polynomial

$$C(x) = x^L + \sum_{j=0}^{L-1} c_j x^j \in \mathbb{F}_2[x]$$

is the *characteristic polynomial* of the recurrence and we say that the sequence is generated by $C(x)$. The minimal order of an LRS is called *linear complexity* and denoted by $L(\mathbf{s})$, that describes the unique *minimal polynomial.* This is equivalent to the shortest LFSR that generates such a sequence.

The *linear complexity profile* denoted by $L(\mathbf{s}, N)$ is the function depending on $N$ that outputs the smallest order $L$ such that $s_0, \dots, s_{N-1}$ are the first elements of the $L$-th order LRS.

In cryptographic applications, the linear complexity must be large and resemble the expected value of a random sequence, which is approximately half the period, that is, $L(\mathbf{s}) \simeq T/2$ [22]. It is clear that a low linear complexity implies the sequence is predictable [5, 12, 18]. However, it fails to capture irregularities in part of the sequence, that can be detected by the linear complexity profile. The latter is a non-decreasing function on $N$ and, for a $T$-periodic sequence $\mathbf{s}$, $L(\mathbf{s}) = L(\mathbf{s}, 2T)$.

A linear recurring sequence generated by an LFSR of order $L$ such that its least period is $2^L - 1$ is called *maximal length sequence* or *m-sequence.* These kind of sequences are easily generated using the *trace function.* For $\mathbb{F}_{2^L}$, the Galois field of $2^L$ elements, we consider the trace function:

$$\mathrm{Tr}(x) = \sum_{i=0}^{L-1} x^{2^i}.$$

We recall the following properties for m-sequences, which can be found in [13, Definition 4.6, Corollary 4.6, Property 5.3, Theorem 5.3]. We denote the polynomial rings $\mathbb{F}_2[x] \subset \mathbb{F}_2[x, y]$.

**Proposition 2.** *Let $(a_i)$ be an m-sequence generated by a polynomial $p(x) \in \mathbb{F}_2[x]$ of degree $L$. It satisfies the following statements:*

- *Its period is $T = 2^L - 1$.*
- *The number of ones occurring within a period is $2^{L-1} = {}^{(T+1)}/_2$ and the number of zeros is $2^{L-1} - 1 = {}^{(T-1)}/_2$.*
- *It has the shift-and-add property, i.e. for any $k_1, k_2 \in \mathbb{N}_0$, either $a_{i+k_1} + a_{i+k_2} = 0$ for every $i \in \mathbb{N}_0$ or there exists $k_3 \in \mathbb{N}_0$ such that the sum equals $a_{i+k_3}$ for every $i \in \mathbb{N}_0$.*
- *For a primitive element $\alpha \in \mathbb{F}_{2^L}$, there exists $k \in \mathbb{N}_0$ such that $a_i = \mathrm{Tr}(\alpha^{i+k})$ for every $i \in \mathbb{N}_0$.*

In order to define a *shrunken sequence*, we consider two m-sequences $(a_i)$ and $(b_i)$ with characteristic polynomials $p_1(x), p_2(x) \in \mathbb{F}_2[x]$ of degrees $L_1$ and $L_2$, with $L_1 \le L_2$. We restrict ourselves to the case $\gcd(L_1, L_2) = 1$, so that the periods $2^{L_1} - 1$ and $2^{L_2} - 1$ are coprime as well. The *shrinking generator* is the decimation of $(b_i)$ by $(a_i)$, i.e. the subsequence of $(b_i)$ that selects only indices for which $a_i = 1$. In other words, ordering increasingly the set $I = \{i \in \mathbb{N}_0 \mid a_i = 1\}$, we obtain a sequence $(i_j)$ in $\mathbb{N}_0$. The shrinking generator output is the sequence given by $(b_{i_j})$ with $i_j \in I$, denoted by $\mathbf{s} = (s_j)$. It is called shrunken sequence and its least period is $(2^{L_2} - 1)2^{L_1-1}$. Regarding the linear complexity, the only known bounds are $L_2 2^{L_1-2} < L(\mathbf{s}) \le L_2 2^{L_1-1}$ [8]. However, those bounds are not tight and it has been an open problem to calculate it theoretically.

Moreover, Fuster-Sabater and Caballero Gil [11] prove that the minimal polynomial is of the form $(p(x))^m$, where $2^{L_1-2} < m \le 2^{L_1-1}$ and $p(x)$ is the minimal polynomial of $(b_i)$. The main result of this paper is the following one. The proof is given in Section 3.

**Theorem 3.** *The linear complexity of a shrunken sequence $\mathbf{s}$ is*

$$L(\mathbf{s}) = L_2 \cdot 2^{L_1-1}, \quad \textit{when } 2^{L_1} \cdot (2^{L_1} - 1) < L_2.$$

*Under the same assumptions, the linear complexity profile $L(\mathbf{s}, N)$ is equal to $L(\mathbf{s})$ if $N > L_2 \cdot 2^{L_1}$.*

A *two-dimensional array* of periods $n_1$ and $n_2$ is a mapping $\mathbf{A} : \mathbb{N}_0^2 \to \mathbb{F}_2$ satisfying $\mathbf{A}(\alpha_1 + n_1, \alpha_2 + n_2) = \mathbf{A}(\alpha_1, \alpha_2)$, for every $(\alpha_1, \alpha_2) \in \mathbb{N}_0^2$.

The *composition method* is able to construct a two-dimensional array from an initial sequence and a shift sequence, see for example [14]. It starts from an $n_1$-periodic binary sequence $(e_i)$ and a $n_2$-periodic integer sequence $(t_j)$, referred as *column* and *shift*, respectively. The resulting array is defined by

$$\mathbf{A}(i, j) = e_{i-t_j}. \tag{2}$$

If the periods $n_1$ and $n_2$ are coprime, the diagonal $s_j = \mathbf{A}(j \mod n_1, j \mod n_2)$ covers the whole array by the Chinese Remainder Theorem. This transformation is called *unfolding* of an array and the result is the *unfolded sequence.*

The following result, which is a consequence of [6, Proposition 2], shows that any shrunken sequence is the unfolding of an array obtained by the composition method. While the original result applies to the row by row or interleave method, it is possible to transform from interleave method to the composition method in many cases [14]. We recall that, for an m-sequence with period $2^{L_1} - 1$, the number of ones within a period is $2^{L_1-1}$.

**Proposition 4** ([6, 14])**.** *Let $L_1, L_2$ be coprime positive integers with $L_1 < L_2$ and let $(a_i)$, $(b_i)$ be m-sequences with (coprime) periods $T_1 = 2^{L_1} - 1$ and $T_2 = 2^{L_2} - 1$. Let $\delta \in \{1, \dots, T_2 - 1\}$ such that $T_1 \cdot \delta = 2^{L_1-1} \mod T_2$. Denote by $(i_j)$ the sequence of indices belonging to the set $I$ defined previously, i.e. $a_{i_j} = 1$ and define the $(2^{L_1-1})$-periodic sequence*

$$t_j = \delta \cdot i_j - j \mod T_2.$$

*Then, the shrunken sequence is the result of unfolding the array given by the composition of $(b_i)$ and $(t_j)$.*

Let us recall the definition of linear complexity for two-dimensional arrays [1].

**Definition 5.** A polynomial $C = \sum_{(\alpha_1,\alpha_2)\in S\subset\mathbb{N}_0^2} c_{\alpha_1,\alpha_2} x^{\alpha_1} y^{\alpha_2} \in \mathbb{F}_2[x, y]$ is *valid* for the two-dimensional array $\mathbf{A}$ when the equation

$$\sum_S c_{\alpha_1,\alpha_2} \mathbf{A}(\alpha_1 + \beta_1, \alpha_2 + \beta_2) = 0 \tag{3}$$

holds for every $\beta_1, \beta_2 \in \mathbb{N}_0$. In this case, we also say that $\mathbf{A}$ *satisfies* the two-dimensional linear recurrence relation given by $C$. If it holds for specific $\beta_1, \beta_2$, we say that the equation is valid at $(\beta_1, \beta_2)$ for $\mathbf{A}$. For the case of periodic two-dimensional arrays, the set of all valid polynomials forms a zero-dimensional ideal and the number of solutions counting its multiplicity in the algebraic closure is known as the *linear complexity* of the array.

We finish this section summarizing some known facts about the linear complexity of arrays and its relation with that of the corresponding unfolded sequences [1].

**Proposition 6.** *Given $\mathbf{A}$, $(e_i)$, and $(t_j)$, defined as in Equation (2), the following facts hold:*

1. *If a polynomial in $\mathbb{F}_2[x]$ is valid for $\mathbf{A}$, it is a multiple of the minimal polynomial of $(e_i)$.*

2. *The minimal polynomial of the unfolded sequence is the smallest-degree polynomial $D(z)$ such that $D(xy)$ is valid for $\mathbf{A}$.*

3. *The linear complexity of $\mathbf{A}$ equals that of its unfolded sequence.*

*Proof.* For the first item, suppose that $C(x)$ is valid for $\mathbf{A}$, then

$$\sum_S c_{\alpha_1}\mathbf{A}(\alpha_1+\beta_1,\beta_2)=0.$$

Taking into account Equation (2)

$$\sum_S c_{\alpha_1}e_{\alpha_1+\beta_1+t_{\beta_2}}=0,$$

which implies that it is a characteristic polynomial of $(e_i)$, i.e. it is a multiple of the minimal polynomial of $(e_i)$.

For the second item, the unfolded sequence $s_i=\mathbf{A}(i \mod n_1, i \mod n_2)$ for all $j\in\mathbb{N}_0$. A characteristic polynomial for $(s_i)$, $D(z)$, satisfies

$$0=\sum_{j=0}^{L} d_j s_{i+j}=\sum_{j=0}^{L} d_j\mathbf{A}(i+j \mod n_1, i+j \mod n_2),$$

which implies that the polynomial $D(xy)$ is valid for $\mathbf{A}$ by Equation (3). The last item is proven in [1] and this finishes the proof. □

## 3 Proof of the main result

We are ready to prove Theorem 3. The shrunken sequence defined by the m-sequences $(a_i)$ and $(b_i)$, with minimal polynomials $p_1(x)$ and $p_2(x)$ of degrees $L_1$ and $L_2$, is, according to Proposition 4, the unfolding of an array. Namely, of $\mathbf{A}(i,j)=b_{i-t_j}$, which is obtained as the composition of $(b_i)$, with period $T_2=2^{L_2}-1$, and a shift sequence $(t_j)$, whose period is $\tau=2^{L_1-1}$.

We will prove that the ideal of valid polynomials for the array is $(p_2(x),y^\tau-1)$, from where the theorem's first statement follows. On one hand, it is straightforward that $p_2(x),y^\tau-1$ are valid polynomials.

On other hand, any valid polynomial is in the ideal, note that

$$(y+1)^\tau=y^\tau-1 \qquad\text{and}\qquad (y+1)^{\tau-1}=1+y+y^2+\cdots+y^{\tau-1}.$$

We consider firstly a valid polynomial in $\mathbb{F}_2[x]$. By the first item of Proposition 6, it must be a multiple of $p_2(x)$. Suppose that there exists a valid polynomial not in the ideal above. We can assume that it takes the form

$$C(x,y)=\sum_{i=0}^{\tau-1}C_i(x)(y+1)^i \qquad (\deg C_i(x)<\deg p_2(x),\ \forall i),$$

with at least one index $i$ for which $C_i(x)=\sum_i c_i x^i$ is not the zero polynomial. Let $n$ be the lowest of those indices. Then, we have

$$(y+1)^{\tau-1-n}\,C(x,y)=C_n(x)(y+1)^{\tau-1}+D(x,y)(y+1)^\tau,$$

so that $C_n(x)(y+1)^{\tau-1} = \sum_i \sum_{j=0}^{\tau-1} c_i x^i y^j$ is valid. In particular, for every $l = 0, \ldots, T_2 - 1$, it holds at $(l, 0)$. Fix a primitive element $\alpha \in \mathbb{F}_{2^{L_2}}$. According to Proposition 2, there exists $k \in \mathbb{N}_0$ such that $b_i = \mathrm{Tr}(\alpha^{i+k})$, for every $i \in \mathbb{N}_0$. Then, for every index $l$,

$$0 = \sum_{i=0}^{L_2-1} \sum_{j=0}^{\tau-1} c_i b_{i+l-t_j} = \mathrm{Tr}\left(\alpha^{k+l} \sum_{i=0}^{L_2-1} c_i \alpha^i \sum_{j=0}^{\tau-1} \alpha^{-t_j}\right) = 0.$$

The power set $\{\alpha^{k+l} \mid l = 0, \ldots, T_2 - 1\}$ equals the whole $\mathbb{F}_{2^{L_2}}^*$. Therefore, it must be

$$\left(\sum_{i=0}^{L_2-1} c_i \alpha^i\right)\left(\sum_{j=0}^{\tau-1} \alpha^{-t_j}\right) = 0.$$

Since $C_n(x)$ is not zero, neither is the first factor. Writing $T_1 = 2^{L_1} - 1$ and $(i_j)$ and $\delta$ as in Proposition 4, we get

$$0 = \sum_{j=0}^{\tau-1} \alpha^{j-\delta \cdot i_j} = \sum_{j=0}^{\tau-1} (\alpha')^{T_1 \cdot (j-\delta \cdot i_j)} = \sum_{j=0}^{\tau-1} (\alpha')^{(2\cdot\tau-1)\cdot j - \tau \cdot i_j}$$

so that $\alpha'$ is a root of $G(x) = x^{(2\tau-1)\cdot\tau} \sum_{i=0}^{\tau-1} x^{(2\cdot\tau-1)\cdot j-\tau\cdot i_j}$, where $(\alpha')^{T_1} = \alpha$. However, the polynomial $G(x)$ has degree less than $2 \cdot \tau \cdot (2 \cdot \tau - 1)$ but this is a contradiction with the fact that $\alpha'$ is a primitive root and its minimal polynomial has degree $L_2$. This completes the proof of the first statement.

For the other one, for $N > L_2(2^{L_1-1})$, we are going to calculate $L(\mathbf{s}, N)$. Take a linear recurrence that holds for $N$ points of sequence $\mathbf{s}$, then there is a characteristic polynomial $p(z)$ associated to the linear recurrence. The first $N$ positions of the sequence $\mathbf{s}$ evenly spaced with constant separation in the array $\mathbf{A}$, then at least $L_2$ points in each column corresponds to the first $N$ elements of the sequence. Due to the fact that each column is the m-sequence $(b_i)$ with $p_2(x)$ then $\mathbf{A}$ can be reconstructed, therefore $p(z)$ is a characteristic polynomial for $\mathbf{s}$ and $\deg p(x) \geq L(\mathbf{s})$. This finishes the proof.

## 4 Conclusions and future work

In this paper, we have a obtained the exact value of the linear complexity of shrunken sequences under a certain condition. We conjecture that this result holds on a more general settings, due to observation of computer experiments carried on. As far as we know, this work is also the first one which studies the linear complexity profile of shrunken sequences and provides an initial bound. Our computational experiments also suggest that the linear complexity is maximal, even in parts of the sequence, when sufficient number of terms are taken. This fact limits the applicability of attacks based on the linear structure of the sequence, given a more stronger security than initially expected.

Further studies on the linear complexity of the generalized sequences are left as an open problem. The starting point could be to analyse several computational simulations on the linear complexity and the linear complexity profile.

As a future work, we would like to obtain some improved bounds for these sequences; and, also to study the linear complexity profile for the other families of decimation-based sequences generators. Results on this direction may lead to establish a relation between arrays and these families of sequences, which could help to deepen the understanding of these generators and obtain stronger results in statistical properties like number of runs, balancedness, etc.

**Acknowledgements**

The work of the second author was supported by Protocolos Seguros En Redes Descentralizadas (Ayuda Financiada Contrato Programa Gob Cantabria -UC). The work of the third author was partially supported by the I+D+i project VIGROB-287 of the Universitat d'Alacant.

## References

[1] Rafael Arce-Nazario, Francis Castro, Domingo Gomez-Perez, Oscar Moreno, José Ortiz-Ubarri, Ivelisse Rubio, and Andrew Tirkel. Multidimensional linear complexity analysis of periodic arrays. *Applicable Algebra in Engineering, Communication and Computing*, 31:43–63, 2020.

[2] Côme Berbain, Olivier Billet, Anne Canteaut, Nicolas Courtois, Henri Gilbert, Louis Goubin, Aline Gouget, Louis Granboulan, Cédric Lauradoux, Marine Minier, Thomas Pornin, and Hervé Sibert. Sosemanuk, a fast software-oriented stream cipher. In Matthew Robshaw and Olivier Billet, editors, *New Stream Cipher Designs: The eSTREAM Finalists*, pages 98–118, Berlin, Heidelberg, 2008. Springer Berlin Heidelberg.

[3] Alex Biryukov and Leo Perrin. State of the art in lightweight symmetric cryptography. Cryptology ePrint Archive, Report 2017/511, 2017. https://ia.cr/2017/511.

[4] Susil Kumar Bishoi, Kedarnath Senapati, and BR Shankar. Shrinking generators based on $\sigma$-LFSRs. *Discrete Applied Mathematics*, 285:493–500, 2020.

[5] Simon R. Blackburn. The linear complexity of the self-shrinking generator. *IEEE Transactions on Information Theory*, 45(6):2073–2077, 1999.

[6] Sara D. Cardell, Diego F. Aranha, and Amparo Fúster-Sabater. Recovering decimation-based cryptographic sequences by means of linear CAs. *Logic Journal of the IGPL*, 28(4):430–448, 2020.

[7] Sara D. Cardell and Amparo Fúster-Sabater. The t-modified self-shrinking generator. In Yong Shi, Haohuan Fu, Yingjie Tian, Valeria V. Krzhizhanovskaya, Michael Harold Lees, Jack Dongarra, and Peter M. A. Sloot, editors, *Computational Science – ICCS 2018*, pages 653–663, Cham, 2018. Springer International Publishing.

[8] Don Coppersmith, Hugo Krawczyk, and Yishay Mansour. The shrinking generator. In Douglas R. Stinson, editor, *Advances in Cryptology — CRYPTO' 93*, pages 22–39, Berlin, Heidelberg, 1994. Springer Berlin Heidelberg.

[9] Sara D. Cardell and Amparo Fúster-Sabater. *Cryptography with Shrinking Generators: Fundamentals and Applications of Keystream Sequence Generators Based on Irregular Decimation.* Springer Briefs in Mathematics. Springer International Publishing, 2019.

[10] Elena Dubrova and Martin Hell. Espresso: A stream cipher for 5g wireless communication systems. *Cryptography and Communications*, 9:273–289, 2017.

[11] Amparo Fúster-Sabater and Pino Caballero-Gil. Linear solutions for cryptographic nonlinear sequence generators. *Physics Letters A*, 369(5–6):432–437, 2007.

[12] Amparo Fúster-Sabater and Sara D. Cardell. Linear complexity of generalized sequences by comparison of PN-sequences. *Revista de la Real Academia de Ciencias Exactas, Físicas y Naturales. Ser. A. Matemáticas (RACSAM)*, 114(4):79–97, 2020.

[13] Solomon W Golomb and Guang Gong. *Signal design for good correlation for Wireless Communication, Cryptography, and Radar.* Cambridge University Press, 2005.

[14] Ana I Gómez, Domingo Gómez-Pérez, and Andrew Tirkel. Generalised gmw sequences. In *2021 IEEE International Symposium on Information Theory (ISIT)*, pages 1806–1811. IEEE, 2021.

[15] Shabbir Hassan and Mohammad Ubaidullah Bokhari. Design of pseudo random number generator using linear feedback shift register. *International Journal of Engineering and Advanced Technology (IJEAT)*, 9(2):1956–1965, 2019.

[16] Yupu Hu and Guozhen Xiao. Generalized self-shrinking generator. *IEEE Trans on Information Theory*, 50(4):714–719, 2004.

[17] Ali Kanso. Modified self-shrinking generator. *Computers & Electrical Engineering*, 36(5):993–1001, 2010.

[18] Edwin L. Key. An analysis of the structure and complexity of nonlinear binary sequence generators. *IEEE Transactions on Information Theory*, 22(6):732–736, 1976.

[19] Willi Meier and Othmar Staffelbach. The self-shrinking generator. In Alfredo De Santis, editor, *Advances in Cryptology — EUROCRYPT'94*, pages 205–214, Berlin, Heidelberg, 1995. Springer Berlin Heidelberg.

[20] Amalia Beatriz Orúe López, Luis Hernández Encinas, Agustín Martín Muñoz, and Fausto Montoya Vitini. A lightweight pseudorandom number generator for securing the internet of things. *IEEE Access*, 5:27800–27806, 2017.

[21] Orúe López, Amalia Beatriz, Luis Hernández Encinas, and Fausto Montoya Vitini. Trifork, a new pseudorandom number generator based on lagged Fibonacci maps. *Journal of Computer Science and Engineering*, 2(2):46–51, 2010.

[22] F. Pichler, editor. *Linear Complexity and Random Sequences*, volume 219 of *Lecture Notes in Computer Science*. Springer-Verlag, 1986.

[23] Hamed Rahimov, Majid Babaei, and Mohsen Farhadi. Cryptographic PRNG based on combination of LFSR and chaotic logistic map. *Applied Mathematics*, 2:1531–1534, 2011.