symmetry

MDPI

Article

Pseudo Random Binary Sequence Based on Cyclic Difference Set

Md. Selim Al Mamun [1] and Fatema Akhter [2,*]

[1] Department of Computer Science and Engineering, Jatiya Kabi Kazi Nazrul Islam University, Trishal 2224, Bangladesh; mamun0013@jkkniu.edu.bd

[2] Graduate School of Natural Science and Technology, Okayama University, Okayama 700-8530, Japan

* Correspondence: fatema@s.okayama-u.ac.jp

Received:18 June 2020 ; Accepted: 14 July 2020 ; Published: 22 July 2020

Abstract: With the increasing reliance on technology, it has become crucial to secure every aspect of online information where pseudo random binary sequences (PRBS) can play an important role in today's world of Internet. PRBS work in the fundamental mathematics behind the security of different protocols and cryptographic applications. This paper proposes a new PRBS namely MK (Mamun, Kumu) sequence for security applications. Proposed sequence is generated by primitive polynomial, cyclic difference set in elements of the field and binarized by quadratic residue (QR) and quadratic nonresidue (QNR). Introduction of cyclic difference set makes a special contribution to randomness of proposed sequence while QR/QNR-based binarization ensures uniformity of zeros and ones in sequence. Besides, proposed sequence has maximum cycle length and high linear complexity which are required properties for sequences to be used in security applications. Several experiments are conducted to verify randomness and results are presented in support of robustness of the proposed MK sequence. The randomness of proposed sequence is evaluated by popular statistical test suite, i.e., NIST STS 800-22 package. The test results confirmed that the proposed sequence is not affected by approximations of any kind and successfully passed all statistical tests defined in NIST STS 800-22 suite. Finally, the efficiency of proposed MK sequence is verified by comparing with some popular sequences in terms of uniformity in bit pattern distribution and linear complexity for sequences of different length. The experimental results validate that the proposed sequence has superior cryptographic properties than existing ones.

Keywords: finite field; primitive polynomial; quadratic residue; pseudo random binary sequence; NIST statistical test suite

1. Introduction

Pseudo random binary sequences (PRBS) are widely used in many applications such as wireless communications and cryptography [1–4]. In cryptography, many security protocols such as SSL/TLS, HTTP are developed based on pseudo random sequences. Randomness of a sequence indicates the degree of difficulty of predicting next bit in that sequence whether it is physical or statistical analysis. Such ideal random sequences can easily be produced from natural resources, for example, atmospheric noises, radioactive decay and other natural phenomena. However, reproducibility of such sequences is impossible mathematically because of variation in natural resources [4,5]. Due to this disadvantage, sources of such true random sequences are unreliable for practical computer applications. On the counterpart, pseudo random sequences are derived using mathematical formulas but have some standard properties that are investigated in true random sequences. Sequences can be regenerated using deterministic mathematics and a large sequence can be produced in short time using small random seeds. Reproducibility and features like true random sequence make pseudo random

sequences an essential part of different mathematical protocols in cryptography and security based computer applications.

In recent years, many cryptographic systems have been developed based on pseudo random sequences. The levels of security of such applications rely mostly on the degree of randomness of sequences being used. Sequences for cryptographic applications are evaluated by some distinguishing properties such as cycle length of sequence also called period, linear complexity, correlation and uniformity of zeros and ones in sequence. Sequences having long cycle length, high linear complexity and uniform bit pattern are considered to be ideal for security applications. In literature, various studies are being conducted in an attempt to generate ideal pseudo random sequences. There are several sequences such as Maximum value-sequence [6], Gold sequence [7] and Kasami sequence [8] possess long cycle length and good correlation properties. However, linear complexity of these sequences is low, hence unsuitable in security based applications. Contrarily, sequences such as NTU sequence [9], Sidelnikov sequence [10–12] and Legendre sequence [13–15] possess high linear complexity. However, a closer look to literature reveals their shortcomings in correlation property compared to other sequences, hence, have limited applications. An increasing number of studies are still in progress to find pseudo random sequences with all desired properties for specific applications.

Considering the above mentioned correspondences, in this work, we propose a new PRBS, MK sequence with an aim to use in cryptographic applications in future. The proposed sequence is generated from a primitive element of finite field and cyclic difference set in elements of the extension field. Finally, the elements are binarized i.e., 0's and 1's, using quadratic residue and quadratic nonresidue. The randomness of proposed sequence is evaluated with popular statistical test suite namely NIST (*National Institute of Standards and Technology*) STS (*Statistical Test Suite*) 800-22 [16,17]. Several sequences up to 10 million bits are generated using proposed method to demonstrate the robustness of the proposal in statistical characteristics set by NIST. Then, linear complexity and uniformity of bit pattern distribution properties of MK sequence are investigated and numerical results are demonstrated theoretically for different length of sequences. Finally, we verify the efficiency of proposed sequence by comparing with sequences generated from primitive polynomial and primitive element. In this work, we compare our results with NTU sequence [9].

Rest of the paper is organized as follows: Section 2 presents mathematical definition of properties and some basics of finite field related to proposed research. Section 3 describes generation of proposed sequence with necessary mathematics. Section 4 evaluates our proposal using NIST, experiments with linear complexity and uniformity and compared results with NTU sequence. Finally, Section 5 summarizes the contributions of this paper and concludes with some prospects for future work.

2. Preliminaries

This section briefly describes fundamental terminologies related to finite field theory and mathematical definitions of primitive polynomial, primitive element, quadratic residue, quadratic nonresidue and linear complexity of pseudo random sequence.

2.1. Notation and Convention

Throughout this paper, we use following notations to present definitions, properties and terms related to pseudo random sequences:

- p : a prime number.
- $\mathbb{F}_p$: prime field of p elements.
- $\mathbb{F}_{p^m}$: finite field of p^m elements where m is a non-negative integer and $m \geq 2$.
- $\mathbb{F}^*_{p^m}$: $\mathbb{F}_{p^m} - \{0\}$.
- $f(x)$: a primitive polynomial of degree m in characteristic field $\mathbb{F}_{p^m}$.
- ω : a primitive element of primitive polynomial, $f(x)$.
- λ : period of sequence.

2.2. Primitive Polynomial

In field theory, a primitive polynomial is a minimal polynomial whose root is a primitive element determining the extension field. Finite field, $\mathbb{F}^*_{p^m}$ constructs a cyclic group with respect to multiplication and consists of $p^m - 1$ non-zero elements. Every finite field has a generator and every non-zero element is represented as a power of the generator.

Definition 1. *A generator of a finite field $\mathbb{F}^*_{p^m}$ is an element of order $p^m - 1$ and the powers of generator runs through all elements of $\mathbb{F}^*_{p^m}$.*

Let, g be a generator of $\mathbb{F}^*_{p^m}$, any non-zero element is derived from power of g, i.e., g^i for $i = 0, 1, .., p^m - 2$. g^i is said to be primitive if and only if $\gcd(i, p^m - 1) = 1$. In particular, there are a total of $\varphi(p^m - 1)$ different primitive elements [18] of $\mathbb{F}^*_{p^m}$ where $\varphi(\cdot)$ represents *euler totient function* [19].

Definition 2. *A polynomial $f(x)$ is said to be primitive if and only if ω, i.e., root of $f(x)$, forms a cyclic group consisting of all elements in $\mathbb{F}^*_{p^m}$.*

Following two conditions hold for $f(x)$ to be primitive polynomial:

① $x^{p^m-1} \equiv 1 (\mathrm{mod}\ f(x))$,
② $x^k \not\equiv 1 (\mathrm{mod}\ f(x))$ for $1 \leq k \leq p^m - 2$.

It is well known that the number of primitive polynomials of degree m is $\dfrac{\varphi(p^m - 1)}{m}$ in $\mathbb{F}^*_{p^m}$.

Theorem 1. *For a generator g in $\mathbb{F}^*_{p^m}$, a non-zero element $g^{(p^m-1)/(p-1)}$ in prime field $\mathbb{F}_p$ is a generator of $\mathbb{F}^*_p$ as well.*

Proof. Let, g be a generator of $\mathbb{F}^*_{p^m}$ whose order is $p^m - 1$. Then, for a non-zero element g^i, its order can be derived as follows:

$$\frac{p^m - 1}{\gcd(i, p^m - 1)}. \tag{1}$$

Therefore, for $g^{(p^m-1)/(p-1)}$, the order is $p - 1$. This implies that $g^{(p^m-1)/(p-1)}$ is a generator of $\mathbb{F}^*_p$. □

Theorem 2. *A polynomial of degree n over a finite field has at most n roots.*

Proof. Here we prove by induction over n. The result is clearly true for $n = 0$ and $n = 1$. Let $f(x)$ be a polynomial with degree m. Let us assume that $f(x)$ has at most m roots where $m < n$. If a is a root of $f(x)$, a polynomial of degree n over a field, then $f(x) = (x - a)q(x)$ where $q(x)$ has degree $n - 1$ and $q(a) \neq 0$. If $f(x)$ has no root other than a, we are done. On the other hand, if $f(b) = 0$ then either $a = b$ or $q(b) = 0$. This follows by induction that $f(x)$ has at most n roots. □

Theorem 3. *For any element $a \neq 0$ in $\mathbb{F}^*_{p^m}$ we have $a^q = 1$ where $q = p^m - 1$.*

Proof. Let m be the order of a in $\mathbb{F}^*_{p^m}$, i.e., the least positive integer for which $a^m = 1$. Then $F_{sub} := \{1, a, a^2, \cdots, a^{m-1}\}$ is a subgroup of $\mathbb{F}^*_{p^m}$. Since m divides q, we have,

$$a^q = (a^m)^{\frac{q}{m}} = 1^{\frac{q}{m}} = 1$$

□

2.3. Quadratic Residue and Quadratic Nonresidue

An element a in finite field $\mathbb{F}_p^*$ is a quadratic residue modulo p if it is congruent to a perfect square in $\mathbb{F}_p$, i.e., there exists an element x such that:

$$a \equiv x^2 \mod p \tag{2}$$

If there is no such x, then a is called quadratic nonresidue modulo p. In this work, we utilize quadratic residue in extension field $\mathbb{F}_{p^m}^*$.

Definition 3. *For any element a in $\mathbb{F}_{p^m}^*$, it is quadratic residue (QR) and quadratic nonresidue (QNR) if*

$$\begin{aligned} &a \in QR \text{ if and only if } a^{\frac{p^m-1}{2}} = 1 \\ &a \in QNR \text{ if and only if } a^{\frac{p^m-1}{2}} = -1 \\ &\textit{Furthermore,} \\ &|QR| = \frac{p^m-1}{2} = |QNR| \end{aligned} \tag{3}$$

Proof. Let a be an element in $\mathbb{F}_{p^m}^*$. Then by the fact in Theorem 3, $a^{p^m-1} = 1$. It follows that every element $a \in \mathbb{F}_{p^m}^*$ is a root of polynomial $x^{p^m-1} - 1 = 0$. On the other hand, by Theorem 2 the polynomial can have at most $p^m - 1$ roots in $\mathbb{F}_{p^m}^*$.

From both the facts, it can be concluded that $x^{p^m-1} - 1 = 0$ has $p^m - 1$ roots. Consequently, since $x^{p^m-1} - 1 = (x^{\frac{p^m-1}{2}} - 1)(x^{\frac{p^m-1}{2}} + 1)$ and the field has no zero divisors, we get either $x^{\frac{p^m-1}{2}} - 1 = 0$ or $x^{\frac{p^m-1}{2}} + 1 = 0$. Again, Theorem 2 implies that both factors $(x^{\frac{p^m-1}{2}} - 1)$ and $(x^{\frac{p^m-1}{2}} + 1)$ must have exactly $\frac{p^m-1}{2}$ roots.

If $a = x^2$ is a quadratic residue in $\mathbb{F}_{p^m}^*$, then $a^{\frac{p^m-1}{2}} = x^{p^m-1} = 1$. Hence, a is a root of $x^{\frac{p^m-1}{2}} - 1$. Therefore, $|QR| \leq \frac{p^m-1}{2}$. On the other hand, by Theorem 2 polynomial $x^2 - a$ has at most two roots for any quadratic residue a. Therefore,

$$p^m - 1 = \mid \mathbb{F}_{p^m}^* \mid \leq \sum_{a \in QR} \mid \{x : x^2 = a\} \mid \leq 2 \times \mid QR \mid .$$

We conclude that $\mid QR \mid = \frac{p^m-1}{2}$ and QR is equal to set of roots of $x^{\frac{p^m-1}{2}} - 1 = 0$. Then it follows that, $\mid QNR \mid = \frac{p^m-1}{2}$ and QNR is equal to set of roots of $x^{\frac{p^m-1}{2}} + 1 = 0$. □

2.4. Linear Complexity

Linear complexity is a measure of unpredictability of a sequence. A sequence of low linear complexity can be easily determined if a number of consecutive terms of the sequence is known. Only $2 \times l$-consecutive terms are required to recover a sequence with l-linear complexity. Therefore, sequence with high linear complexity is a fundamental requirement for security applications.

Definition 4. *Linear complexity is defined as the length of the shortest linear feedback shift register (LFSR) that can generate the sequence. Linear complexity is considered to be zero for sequence of length zero.*

Definition 5. *Let $LC_i(\mathcal{S})$ be the linear complexities of first i elements of a sequence $\mathcal{S}$ where $i = 0, 1, 2, \cdots, (\lambda - 1)$. Then, linear complexity profile of the sequence is considered as the finite sequence $LC_0(\mathcal{S}), LC_1(\mathcal{S}), ..., LC_{(\lambda-1)}(\mathcal{S})$.*

Let, $\mathcal{S}$ be a sequence of period λ. The linear complexity $\mathrm{LC}(\mathcal{S})$ is presented as:

$$\mathrm{LC}(\mathcal{S}) = \lambda - \deg(\gcd(x^{\lambda} - 1, h_{\mathcal{S}}(x))), \tag{4}$$

where h_S is called the generating polynomial. For a sequence $\mathcal{S}_\lambda = \{s_i\}$ where $i = 0, 1, \cdots, \lambda - 1$, generating polynomial is defined as:

$$\begin{aligned} h_{\mathcal{S}} &= s_0 + s_1 x + s_2 x^2 + \cdots + s_{\lambda-1} x^{\lambda-1} \\ &= \sum_{i=0}^{\lambda-1} s_i x^i. \end{aligned} \tag{5}$$

This work is focused on binary sequence. Therefore, $gcd(x^{\lambda} - 1, h_{\mathcal{S}})$ in Equation (4) is computed in $\mathbb{F}_2$. A popular algorithm, Berlekamp-Massey algorithm [20] can find linear complexity in $\mathbb{F}_{p^m}$.

3. Proposal of MK Sequence

3.1. Cyclic Difference Set

In this section, we introduce cyclic difference set which differs from the ones proposed in [21–24]. In this work, we use differences in elements in extension field to change order of elements and named cyclic difference set in this work. For a given prime p and a non-negative integer m, any extension field element $X_i : X_i \in \mathbb{F}^*_{p^m}$ can be presented as:

$$X_i = c_0 x^0 + c_1 x^1 + c_2 x^2 + \cdots + c_{m-1} x^{m-1} \tag{6}$$

The construction of cyclic difference set X'_i from elements of X_i for $i = 0, 1, 2, \cdots, (p^m - 2)$ is given below:

$$\begin{aligned} X'_i =& (c_0 - 1)x^0 + (c_1 - 1)x^1 + (c_2 - 2)x^2 + \\ & \cdots + (c_{m-1} - 1)x^{m-1} \\ =& \sum_{j=0}^{m-1} (c_j - 1)x^j \end{aligned} \tag{7}$$

Cyclic difference set randomizes sequence bits by changing the order of extension field elements which are converted to sequence bits later.

3.2. Generation Algorithm

For a given prime p and a non-negative integer m, generation of proposed pseudo random binary sequence $S = \{s_0, s_1, s_2, \cdots, s_{p^m-2}\}$ of length $\lambda = p^m - 1$ is presented here. The procedure composes of four phases that are described below (Algorithm 1):

Algorithm 1 Proposed Algorithm for MK Sequence.

① *Primitive polynomial and primitive element:*
Generate a primitive polynomial $f(x)$ over $\mathbb{F}^*_{p^m}$ as defined in Section 2.2. Let, ω be a primitive root of $f(x)$ defined as $\omega^i = \sum_{j=0}^{m-1} c_j x^j$. A primitive root is a reduced residue of order $p^m - 1$.

② *Generation of all elements in $\mathbb{F}^*_{p^m}$:*
Every element in $\mathbb{F}^*_{p^m}$ is congruent to some power $\omega^i \mod f(x)$ of ω, and i can be reduced mod $p^m - 1$. Therefore, any element X_i in $\mathbb{F}^*_{p^m}$ can be generated as follows:
$X_i = \omega^i \mod f(x)$ for $i = 0, 1, 2, \cdots, (p^m - 2)$.

③ *Generation of cyclic difference set:*
Now, generate cyclic difference set X'_i from elements of X_i for $i = 0, 1, 2, \cdots, (p^m - 2)$ as described in Section 3.1:

$$X'_i = \sum_{j=0}^{m-1} (c_j - 1) x^j$$

④ *Binary sequence using quadratic residue:*
For any element $a \in X'$, sequence element s_i in proposed sequence $\mathcal{S}_{\geq} = \{s_0, s_1, ..., s_{m-2}\}$ of length $\lambda = p^m - 1$ is generated using quadratic residue, i.e., $a^{\frac{p^m-1}{2}} = 1$ as follows:

$$s_i = \begin{cases} 0 & \text{when } a^{\frac{p^m-1}{2}} = 1 \text{ for } a \in X' \\ 1 & \text{when } a^{\frac{p^m-1}{2}} = -1 \text{ for } a \in X' \end{cases} \tag{8}$$

4. Experimental Results

In this section, we evaluate our proposed MK sequence. First, the effectiveness is verified using NIST STS [16,17]. Then, experimental results of linear complexity and uniformity are presented. Finally, a comparison with existing NTU sequence is presented.

4.1. Randomness Analysis

In cryptography, PRBS is adopted in many applications as the primary security component. Therefore, the efficiency of PRBS must be verified with standard statistical measures before practical applications. Several statistical test suits such as NIST, DIEHARD, Gustafson, CryptXS suite, and Donald Knuth [25–28] are available to verify randomness of a sequence. However, NIST is regarded as the most complete test suite for verification of randomness of a sequence. NIST is composed of 15 statistical tests which measure different behaviors of binary sequences to verify their randomness. All tests are independent that reveal various deviations from random behavior. Each test computes a probability value called p value from given binary sequence. The p value falls within range [0,1]. When p value equals to 1, it means that the sequence is random. Again, when p value equals to 0, it means that the sequence is not random. When the value is greater than a given value, $\alpha \in (0, 1)$, the sequence is considered random with a confidence of $1 - \alpha$. In other cases, it is not considered random.

This work considers value of α is 0.01 as suggested in studies [29–31]. A value $\alpha = 0.01$ indicates a probability of one sequence out of hundred to be rejected. A sequence is random with a confidence of 99% when p value is higher than 0.01. Similarly, it is not random with a confidence of 99% when p value is less than 0.01. The range of acceptable proportions is determined by the following expression:

$$1 - \alpha \pm 3\sqrt{\frac{\alpha}{n}} \tag{9}$$

where n is sample size. For sample size, $n = 1000$, the acceptable interval is between $[0.98056, 0.99943]$. Any proportion outside of this interval is regarded as non-random [25]. The randomness of proposed MK sequence is verified by using NIST 800-22 test suite. Sequence with at least 10^6 bits is applied as input to NIST test suite. The experimental result is listed in Table 1. The experiment is conducted using primitive polynomial $x^3 + x + 3$, $p = 467$ and $m = 3$. In NIST test suite, some tests such as random excursions variant, random excursions, and non-overlapping template test comprise of several number of tests. Therefore, minimum and maximum results for those tests are listed in Table 1. The results in Table 1 demonstrate that MK sequence successfully passed all tests defined in NIST suite.

Table 1. NIST test results for proposed sequence.

Statistical Test	Portion of Successful Sequences $\geq$ 0.01	Result
Frequency	0.997	◯
Block frequency	0.991	◯
Cumulative sums (1)	0.997	◯
Cumulative sums (2)	0.996	◯
Runs	0.995	◯
Longest run	0.992	◯
Rank	0.991	◯
Fast fourier transform	0.989	◯
Non-overlapping template	max: 0.997	◯
	min: 0.983	◯
Overlapping template	0.986	◯
Maurer's universal statistical	0.990	◯
Approximate entropy	0.984	◯
Random excursions	max: 1.000	◯
	min: 0.974	◯
Random Excursions Variant	max: 1.000	◯
	min: 0.983	◯
Serial (1)	0.987	◯
Serial (2)	0.989	◯
Linear complexity	0.984	◯

◯: success, ×: failure.

4.2. Linear Complexity Analysis

In this experiment, linear complexity and linear complexity profile of different sequences are analyzed to understand the statistical behavior of proposed sequence. As a measure of unpredictability these properties are extensively studied in cryptography. The linear complexity is calculated from the length of shortest linear feedback shift register (LFSR) [6]. Similarly, the n-th linear complexity can be calculated from the length of LFSR that can produce first n elements of the sequence. A series of n-th linear complexities is considered as the linear complexity profile. In this work, Berlekamp-Massey algorithm [20] is utilized to derive both linear complexity and linear complexity profile of MK sequence. It should be noted that linear complexity is expected to be $\frac{n}{2}$ for a sequence of length n [32–34]. Table 2 summarizes the linear complexity analysis of MK sequence for different sets of p and m. The numerical results in Table 2 demonstrate that for length n, proposed sequence has linear complexity of $\frac{n}{2}$ which is equal to ideal.

Table 2. Results of linear complexity for proposed sequence.

p, m	Length of Sequence	Linear Complexity
$p = 5, m = 3$	124	62
$p = 7, m = 3$	342	171
$p = 7, m = 5$	16,806	8403
$p = 11, m = 5$	161,050	80,525
$p = 101, m = 3$	1,030,300	515,150
$p = 467, m = 3$	101,847,562	50,923,781

Figure 1 shows linear complexity profile of MK sequence for primitive polynomial $x^3 + 3x + 2$, $p = 7$ and $m = 3$ in extension field $\mathbb{F}_{7^3}$. In Figure 1, the green line represents linear complexity profile for ideal random sequence where the red line does for the proposed MK sequence. The linear complexity profile curve in Figure 1, can be approximated to ideal $\frac{n}{2}$ line curve, with the length and linear complexity of the sequence. The experimental results indicate that proposed sequence has expected linear complexity like ideal one.

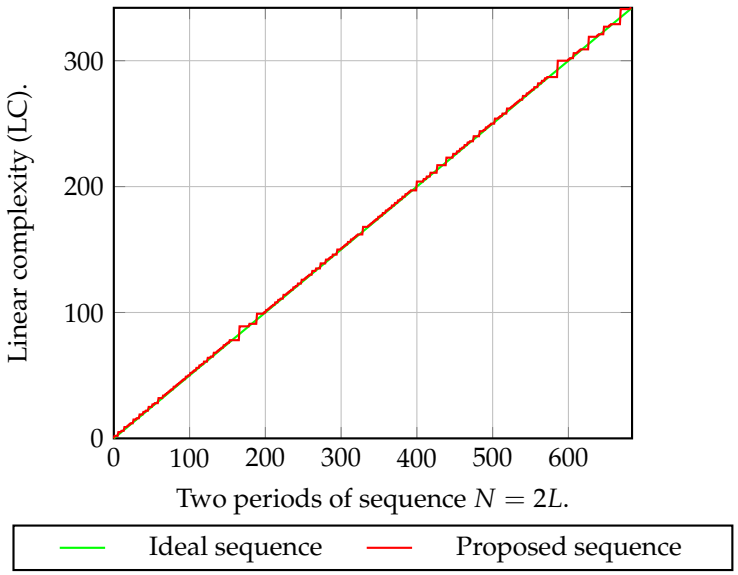


Figure 1. Result of linear complexity profile of proposed MK sequence for $p = 7$ and $m = 3$.

4.3. Result of Uniformity

Evaluation of randomness of a PRBS is a challenging task. Some important measures are introduced in Golomb's postulates which work as basis to form basic properties for a pseudorandom sequence to be random looking. One important measure in Golomb's [35–37] postulates is uniformity of bits in sequence, which is determined by the number of 0's and 1's in it. A random sequence of n-bits is expected to have approximately $\frac{n}{2}$ bits of 0's and $\frac{n}{2}$ bits of 1's. Inspired by this postulate, herein, we study distribution of bit pattern of proposed MK sequence for evaluation of its uniformity.

The experimental results of bit pattern distribution of the proposed sequence for different sets of p and m are presented in Tables 3 and 4. The experiments are conducted using primitive polynomials $x^5 + 4x + 2$ and $x^3 + x + 3$ respectively. For any bit pattern, the number of 0's almost equals to the number of 1's. The experimental results ensure that QR/QNR-based binarization can successfully generate uniform sequence of equal number of 0's and 1's. This uniform behavior is consistent and continued even when considered pattern length is increased.

Table 3. Result of uniformity test for $p = 5, m = 5$.

Pattern Length	Bit Pattern	# of Appearance
1	0	1562
	1	1562
2	00	781
	01	781
	10	781
	11	781
3	000	385
	001	396
	010	396
	011	385
	100	396
	101	385
	110	385
	111	396

Table 4. Result of uniformity test for $p = 467, m = 3$.

Pattern Length	Bit Pattern	# of Appearance
1	0	50,923,781
	1	50,923,781
2	00	25,461,890
	01	25,461,891
	10	25,461,891
	11	25,461,890
3	000	12,731,725
	001	12,730,165
	010	12,730,165
	011	12,731,726
	100	12,730,165
	101	12,731,726
	110	12,731,726
	111	12,730,164

4.4. Evaluation by Comparison

This section evaluates our proposed sequence by comparing with other sequence generated from primitive polynomial. We consider NTU sequence [9] for this purpose as it is derived from primitive polynomial, trace function and Legendre symbol that matches ours methodically for fair comparison. Linear complexity and uniformity of bit pattern distribution of sequences are taken into consideration while comparing two sequences. For linear complexity, we derived linear complexity for different length of proposed MK and NTU sequences. Table 5 shows comparison results of linear complexity. For n bit sequence, linear complexity of the proposed sequence is $\frac{n}{2}$ which is similar to ideal. On the other hand, linear complexity of NTU sequence is lower than proposed sequence, i.e., ideal value. Then, we investigated linear complexity profile of both sequences and the result is showed in Figure 2 for $p = 5$ and $m = 3$. The result indicates that the linear complexity profile of proposed sequence is almost similar to ideal. On the other hand, for NTU sequence it becomes saturated at a lower point and lags far behind the proposed sequence.

Table 5. Comparison of linear complexity between proposed and NTU [9] sequence.

Length of Sequence	Linear Complexity	
	Proposed Sequence	**NTU Sequence**
$p = 5, m = 3$	62	62
$p = 7, m = 3$	171	114
$p = 7, m = 5$	8403	5602
$p = 11, m = 5$	80,525	32,210
$p = 101, m = 3$	515,150	20,606
$p = 463, m = 3$	50,923,781	437,114

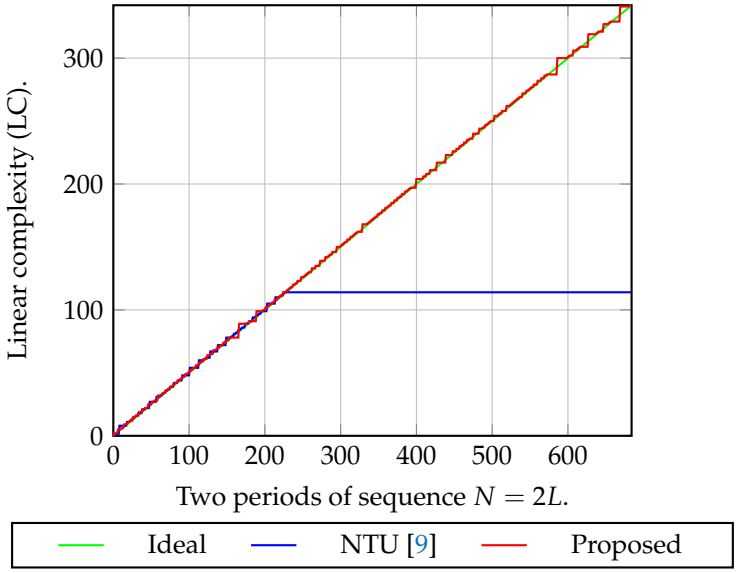
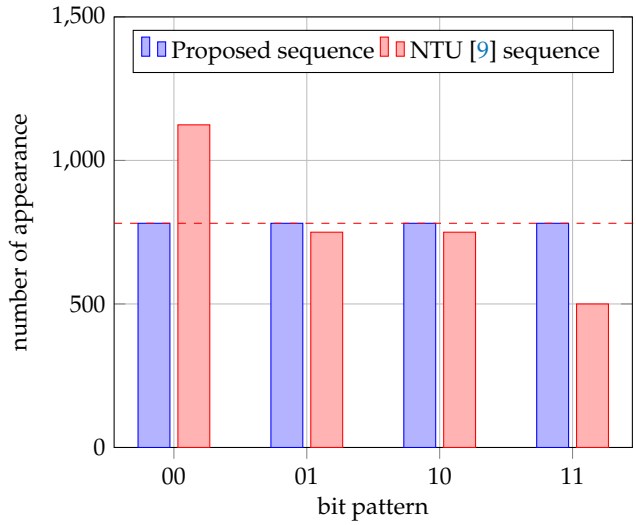


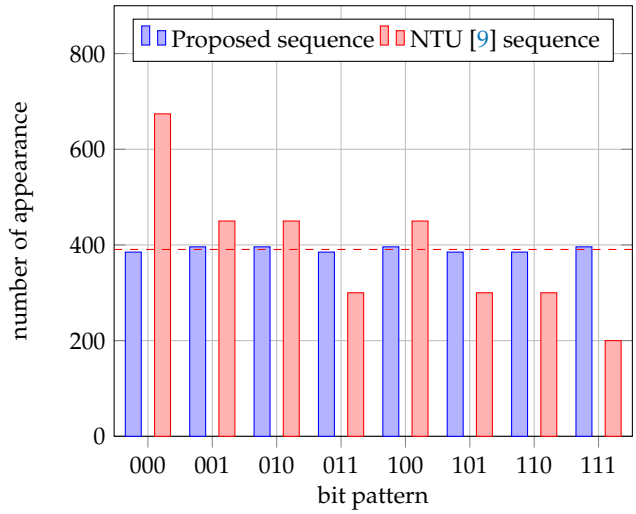
Figure 2. Comparison of linear complexity profile between proposed and NTU [9] sequence for $p = 7$ and $m = 3$.

For comparison of uniformity of bit pattern distribution, we consider 2-bit pattern, i.e., $(00, 01, 10, 11)$ and 3-bit pattern, i.e., $(000, 001, 010, 011, 100, 101, 110, 111)$ to compare their number of appearance in the sequence. It should be noted that for ideal sequence, the number of appearance of any bit pattern should be equal in a sequence. The comparison result for 2 bit pattern and 3 bit pattern for $p = 5$ and $m = 5$ is showed in Figure 3. In Figure 3, dotted horizontal red line indicates the ideal value for bit pattern. The results indicate that bit patterns are equally distributed for proposed MK sequence. However, for NTU sequence, pattern distribution is irregular and varies more with increasing number of bit pattern considered.

It should be noted that the randomness of proposed MK sequence is evaluated by experimental results. However, theoretical analysis on computation complexity of different properties of sequence is still worth of further investigation in future.



(**a**) Result of uniformity for 2-bit pattern distribution.



(**b**) Result of uniformity for 3-bit pattern distribution.

Figure 3. Comparison of uniformity between proposed MK sequence and NTU sequence for $p = 5$ and $m = 5$.

5. Conclusions

In this work, we proposed a new pseudo random binary sequence, i.e., MK sequence with an aim to use in security of applications. The proposed sequence is derived from a primitive polynomial in extension field, cyclic difference set and finally binarized using quadratic residue and quadratic nonresidue. The proposed sequence is uniform in terms of zeros and ones, has maximum cycle length and high linear complexity that are prerequisite for any security applications. Numerical results are presented for different length of sequences in support of the claim. Our method was verified with statistical randomness test suite, NIST STS 800-20 package where proposed MK sequence successfully passed all statistical randomness tests. The results confirmed that proposed sequence has high degree of randomness, statistical characteristics conforming to ideal sequence and uniform in bit distribution. In future, we will consider security measure as a function of parameters, e.g., p and m of the proposed algorithm for specific applications and would like to derive theoretical proof of properties presented in this paper. In addition, we want to apply our proposed sequence in practical cryptographic applications such as stream cipher, steganography and investigate its

worthiness for security applications and compare with other cryptographically secured pseudo random sequence generator such as AES-128-CTR, ChaCha20 and SHAKE-128 [38–40].

Author Contributions: Individual contributions to this article: Conceptualization, S.A.M. and F.A.; methodology, S.A.M. and F.A.; software and coding, F.A.; validation, S.A.M. and F.A.; writing—original draft preparation, S.A.M. and F.A.; writing—review and editing, S.A.M. and F.A.; supervision, S.A.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Acknowledgments: The authors thank the anonymous referees for their careful reading and helpful suggestions, which help to improve the quality of this paper.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Lambić, D.; Nikolić, M. Pseudo-random number generator based on discrete-space chaotic map. *Nonlinear Dyn.* **2017**, *90*, 223–232. [CrossRef]
2. Akhter, F.; Nogami, Y.; Kusaka, T.; Taketa, Y.; Tatara, T. Binary sequence generated by alternative trace map function and its properties. In Proceedings of the 2019 Seventh International Symposium on Computing and Networking Workshops (CANDARW), Nagasaki, Japan, 26–29 November 2019; pp. 408–411.
3. Akhter, F.; Al Mamun, M.S. Pseudo random binary sequence: A new approach over finite field and its properties. In Proceedings of the 2017 International Conference on Electrical, Computer and Communication Engineering (ECCE), Cox's Bazar, Bangladesh, 16–18 February 2017; pp. 676–680.
4. Šajić, S.; Maletić, N.; Todorović, B.M.; Šunjevarić, M. Random binary sequences in telecommunications. *J. Electr. Eng.* **2013**, *64*, 230–237. [CrossRef]
5. Pasqualini, L.; Parton, M. Pseudo random number generation: A reinforcement learning approach. *Procedia Comput. Sci.* **2020**, *170*, 1122–1127. [CrossRef]
6. Golomb, S.W. *Shift Register Sequences*; Aegean Park Press: Walnut Creek, CA, USA, 1967.
7. Gold, R. Optimal binary sequences for spread spectrum multiplexing (Corresp.). *IEEE Trans. Inf. Theory* **1967**, *13*, 619–621. [CrossRef]
8. Kasami, T. *Weight Distribution Formula for Some Class of Cyclic Codes*; Report No. R-285; Coordinated Science Laboratory, University of Illinois; 1966.
9. Nogami, Y.; Tada, K.; Uehara, S. A geometric sequence binarized with Legendre symbol over odd characteristic field and its properties. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.* **2014**, *97*, 2336–2342. [CrossRef]
10. Yu, N.Y.; Gong, G. New construction of *M*-ary sequence families with low correlation from the structure of Sidelnikov sequences. *IEEE Trans. Inf. Theory* **2010**, *56*, 4061–4070. [CrossRef]
11. Su, M.; Winterhof, A. Autocorrelation of Legendre–Sidelnikov Sequences. *IEEE Trans. Inf. Theory* **2010**, *56*, 1714–1718. [CrossRef]
12. Kim, Y.T.; San Kim, D.; Song, H.Y. New *M*-Ary Sequence families with low correlation from the array structure of Sidelnikov sequences. *IEEE Trans. Inf. Theory* **2014**, *61*, 655–670.
13. Zierler, N. *Legendre Sequences*; Technical Report; Massachusetts Institute of Technology, Lincoln Laboratory: Lincoln, NE, USA, 1958.
14. No, J.S.; Lee, H.K.; Chung, H.; Song, H.Y.; Yang, K. Trace representation of Legendre sequences of Mersenne prime period. *IEEE Trans. Inf. Theory* **1996**, *42*, 2254–2255.
15. Ding, C.; Hesseseth, T.; Shan, W. On the linear complexity of Legendre sequences. *IEEE Trans. Inf. Theory* **1998**, *44*, 1276–1278. [CrossRef]
16. Rukhin, A.; Soto, J.; Nechvatal, J.; Smid, M.; Barker, E. *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*; Technical Report; Booz Allen & Hamilton inc Greensboro Drive: McLean, VA, USA, 2001.
17. Bassham, L.E., III; Rukhin, A.L.; Soto, J.; Nechvatal, J.R.; Smid, M.E.; Barker, E.B.; Leigh, S.D.; Levenson, M.; Vangel, M.; Banks, D.L.; et al. *Sp 800-22 rev. 1a. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*; National Institute of Standards & Technology: Gaithersburg, MD, USA, 2010.

18. Koblitz, N. *A Course in Number Theory and Cryptography*; Springer Science & Business Media, Berlin, Germany, 1994; Volume 114.
19. Lehmer, D. On Euler's totient function. *Bull. Am. Math. Soc.* **1932**, *38*, 745–751. [CrossRef]
20. Massey, J. Shift-register synthesis and BCH decoding. *IEEE Trans. Inf. Theory* **1969**, *15*, 122–127. [CrossRef]
21. Cohen, S.D. Generators in cyclic difference sets. *J. Comb. Theory Ser. A* **1989**, *51*, 227–236. [CrossRef]
22. Xia, B. Cyclotomic difference sets in finite fields. *Math. Comput.* **2018**, *87*, 2461–2482. [CrossRef]
23. Dillon, J.F.; Dobbertin, H. New cyclic difference sets with Singer parameters. *Finite Fields Their Appl.* **2004**, *10*, 342–389. [CrossRef]
24. Polhill, J. Generalizations of partial difference sets from cyclotomy to nonelementary abelian p-groups. *Electron. J. Comb.* **2008**, *15*, R125. [CrossRef]
25. Murillo-Escobar, M.; Cruz-Hernández, C.; Cardoza-Avendaño, L.; Méndez-Ramírez, R. A novel pseudorandom number generator based on pseudorandomly enhanced logistic map. *Nonlinear Dyn.* **2017**, *87*, 407–425. [CrossRef]
26. Marsaglia, G. DIEHARD Test Suite. 1998. Volume 8. Available online: http://www.Stat.Fsu.Edu/pub/diehard (accessed on 20 March 2014).
27. Gustafson, H.; Dawson, E.; Nielsen, L.; Caelli, W. A computer package for measuring the strength of encryption algorithms. *Comput. Secur.* **1994**, *13*, 687–697. [CrossRef]
28. Knuth, G. *The Art of Computer Programming, Seminumerical Algorithms—Volume 2: Addition*; Wesley: Reading, MA, USA, 1998.
29. Sulak, F.; Uğuz, M.; Kocak, O.; DOğanaksoy, A. On the independence of statistical randomness tests included in the NIST test suite. *Turk. J. Electr. Eng. Comput. Sci.* **2017**, *25*, 3673–3683. [CrossRef]
30. Patidar, V.; Sud, K.K.; Pareek, N.K. A pseudo random bit generator based on chaotic logistic map and its statistical testing. *Informatica* **2009**, *33*, 441–452.
31. Sÿs, M.; Matyáš, V. Randomness testing: Result interpretation and speed. In *The New Codebreakers*; Springer: New York, NY, USA, 2016; pp. 389–395.
32. Hu, H.; Liu, L.; Ding, N. Pseudorandom sequence generator based on the Chen chaotic system. *Comput. Phys. Commun.* **2013**, *184*, 765–768. [CrossRef]
33. Yang, L.; Xiao-Jun, T. A new pseudorandom number generator based on a complex number chaotic equation. *Chin. Phys. B* **2012**, *21*, 090506.
34. Liu, L.; Miao, S.; Hu, H.; Deng, Y. Pseudorandom bit generator based on non-stationary logistic maps. *IET Inf. Secur.* **2016**, *10*, 87–94. [CrossRef]
35. Helleseth, T., Golomb's randomness postulates. In *Encyclopedia of Cryptography and Security*; van Tilborg, H.C.A.; Jajodia, S., Eds.; Springer: Boston, MA, USA, 2011; pp. 516–517._351. [CrossRef]
36. Doğanaksoy, A.; Sulak, F.; Uğuz, M.; Şeker, O.; Akcengiz, Z. New statistical randomness tests based on length of runs. *Math. Probl. Eng.* **2015**, *2015*. [CrossRef]
37. Ers, H.W. On the significance of golomb's randomness postulates in cryptography. *Philips J. Res* **1988**, *43*, 185–222.
38. Schwabe, P.; Stoffelen, K. All the AES you need on Cortex-M3 and M4. In *International Conference on Selected Areas in Cryptography*; Springer: Cham, Switzerland, 2016; pp. 180–194.
39. De Santis, F.; Schauer, A.; Sigl, G. ChaCha20-Poly1305 authenticated encryption for high-speed embedded IoT applications. In Proceedings of the Design, Automation & Test in Europe Conference & Exhibition (DATE), Lausanne, Switzerland, 27–31 March 2017; pp. 692–697.
40. Gao, X. Comparison analysis of Ding's RLWE-based key exchange protocol and NewHope variants. *Adv. Math. Commun.* **2019**, *13*, 221. [CrossRef]