On the Linear Complexity of Binary *Half-ℓ-Sequences*

Zhihua Niu[1,2] and Yuqi Sang[1]
(Corresponding author: Zhihua Niu)

School of Computer Engineering and Science, Shanghai University[1]
Shanghai 200444, China
Email: zhniu@shu.edu.cn
Key Laboratory of Applied Mathematics (Putian University), Fujian Province University[2]
Fujian Putian, 351100, China

(Received Apr. 6, 2021; Revised and Accepted Apr. 5, 2022; First Online Apr. 23, 2022)

Abstract

Binary *half-ℓ-sequences* are $\varphi(q)/2$-periodic sequences generated by a Feedback with Carry Shift Register(FCSR) with connection integer q. In this paper, we focus on the linear complexity of binary *half-ℓ-sequences*. We give some upper and lower bounds of their linear complexity. The numerical experiment shows that for most binary *half-ℓ-sequences* the linear complexity is close to the upper bound.

Keywords: Binary Sequence; Feedback with Carry Shift Register; Half-ℓ-Sequence; Linear Complexity

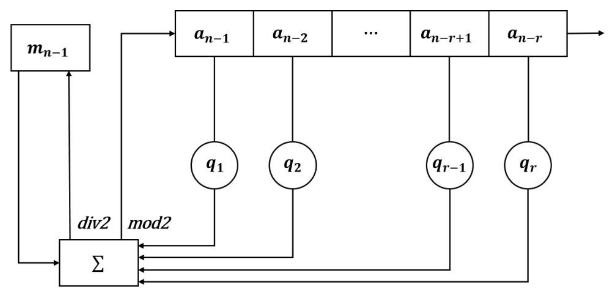

Figure 1: Feedback with carry shift register

1 Introduction

Linear Feedback Shift Registers(LFSRs) are widely used in information theory, coding theory, and cryptography. Klapper and Goresky [10] proposed Feedback with Carry Shift Registers(FCSRs), a new type of feedback shift registers as an alternative to LFSRs. The main idea of FCSR is to add a memory to LFSR. Figure 1 shows the structure of FCSR with connection integer $q = -1 + q_1 2^1 + q_2 2^2 + \ldots + q_r 2^r$, where $q_i \in \{0, 1\}$ and $r = \lceil \log_2(q+1) \rceil$ is the length of the FCSR. $\sum$ represents integer addition and $m_n \in \mathbb{Z}$.

The operation of the shift register is defined as follows:

1) Compute the sum $\sigma = \sum_{i=1}^{r} q_i a_{n-i} + m_{n-1}$;

2) Shift the contents one step to the right, outputting the right almost bit a_{n-r};

3) Place $a_n = \sigma_n \pmod 2$ into the leftmost shift register;

4) Replace the memory integer m_{n-1} with $m_n = (\sigma_n - a_{n+r})/2 = \lfloor \sigma_n/2 \rfloor$.

Klapper and Goresky discussed some basic properties of sequences produced by FCSRs [10]. To obtain stream ciphers with better performance, some researchers tried to combine LFSRs with FCSRs [6, 19]. Some researchers proposed shift registers base on modified FCSRs, such as ring FCSR [3, 11], F-FCSR [1] and X-FCSR [2].

For a (binary) sequence $s^\infty = s_0, s_1, \ldots$ generated by an FCSR of the shortest length with connection integer q, we denote

$$\Phi_2(s^\infty) = \lceil \log_2(q+1) \rceil,$$

called the *2-adic complexity* of s^∞. And s^∞ is periodic with period $T = \mathrm{ord}_q(2)$, where $\mathrm{ord}_q(2)$ is the multiplicative order of 2 modulo q. It is clear, if $T = \varphi(q)$, where $\varphi(-)$ is the Euler function, then s^∞ reaches its maximum period. Such sequence is referred to as the *ℓ-sequence* [10]. If $T = \varphi(q)/2$, s^∞ is called the *half-ℓ-sequence* in [8, 18], which will be discussed in this work. In this case, the connection integer q is prime and $q \equiv \pm 1 \pmod 8$. For details on FCSRs, the reader is referred to the classic books [7, 9].

An LFSR or an FCSR can generate any binary periodic sequence s. The length of the shortest LFSR (resp. FCSR) capable of producing s is called the linear complexity (resp. *2-adic complexity*) of s. In cryptography, as candidates of keys in stream cipher systems, binary sequences must have large “complexity”.

We should remark that it seems that there is no relationship between the linear complexity and the *2-adic complexity* of a sequence. For example, any m-sequence of period $2^n - 1$ has the maximal *2-adic complexity* $\log_2(2^{2^n-1} - 1)$ (see [17]) but its linear complexity is n. So it is necessary to consider the linear complexity for sequences generated by an FCSR.

Indeed, the linear complexity of *ℓ-sequences* has been widely investigated. C. Seo and S. Lee [15] discussed the linear complexity of *ℓ-sequences* when connection integer q is 2-prime or strong 2-prime. Q. C. Wang and H. Xu [13] deduced the linear complexity of *ℓ-sequences* when q is of form p^e with any prime p. L. Tan and Q. C. Wang [16] studied the stability of the linear complexity of *ℓ-sequences*. A. Arshad [4] described the behavior of frequency distribution of various patterns in binary *ℓ-sequences*.

In this paper, we study the linear complexity of binary *half-ℓ-sequences*, which has not been touched on in the literature. In Section 2, we introduce some related notions and lemmas. In Sections 3, we give some bounds for the linear complexity of binary *half-ℓ-sequences* generated by an FCSR with a prime connection integer $q \equiv 1 \pmod 8$. In Section 4, we give some bounds for sequences with $q \equiv 7 \pmod 8$. Finally, we summarize the work in Section 5.

2 Preliminaries

For our discussion, we need the exponential representation of FCSR sequences proposed by Klapper [10].

Definition 1. *[10] Let s^∞ be a periodic binary sequence generated by an FCSR with connection integer q. Then there exists $A \in \mathbb{Z}_q$ such that for all $i = 0, 1, 2, \ldots$ we have*

$$s_i = A \cdot 2^{-i} \pmod q \pmod 2. \tag{1}$$

Then, we introduce some definitions and lemmas about characteristic polynomial, generating function, cyclotomic polynomial, and order of the polynomial, which are important in our proof.

Definition 2. *[5] Let s^∞ be a T-period sequence over $\mathbb{F}_2$. A polynomial of the form*

$$f(x) = 1 + c_1x + c_2x^2 + \ldots + c_rx^r \in \mathbb{F}_2[x]$$

is called the characteristic polynomial of s^∞ if

$$s_i = c_1s_{i-1} + c_2s_{i-2} + \ldots + c_rs_{i-r}, \forall i \geq r.$$

The characteristic polynomial with the lowest degree is called the minimal polynomial, denoted by $m(x)$. The linear complexity of s^∞ is defined as the degree of $m(x)$, denoted as $LC(s^\infty)$.

Definition 3. *[5] Let s^∞ be a T-periodic sequence over $\mathbb{F}_2$, the polynomial of the form*

$$S(x) = s_0 + s_1x + s_2x^2 + \ldots \in \mathbb{F}_2[x] \tag{2}$$

is called the generating function of s^∞.

Lemma 1. *[5] Let s^∞ be a T-periodic sequence with generating polynomial $S(x)$ defined by Equation (2). Then the linear complexity of s^∞ is*

$$LC(s^\infty) = T - \deg(gcd(x^T - 1, S(x))).$$

Definition 4. *[14] Let $g(x) \in \mathbb{F}_2[x]$ be a nonzero polynomial. If $g(0) \neq 0$, then the least positive integer m for which $g(x)$ divides $1 + x^m$ is called the order of $g(x)$ and denoted by $ord(g(x))$.*

The order of a polynomial is also called the period of it.

Lemma 2. *[14] Let $m(x)$ be the minimal polynomial of s^∞ of the least period T, then $ord(m(x)) = T$.*

Lemma 3. *[14] Let $h(x) = g_1(x)^{n_1}g_2(x)^{n_2}\ldots g_k(x)^{n_k}$, where $g_1(x), g_2(x), \ldots, g_k(x)$ are pairwise relatively prime nonzero polynomials and $n_1, n_2, \ldots, n_k \in \mathbb{N}$. Then $ord(h(x)) = 2^\xi m$, where ξ is the least positive integer such that $2^\xi \geq \max\{n_1, n_2, \ldots, n_k\}$ and m is $lcm(ord(g_1(x)), ord(g_2(x)), \ldots, ord(g_k(x)))$.*

Definition 5. *[14] Let n be a positive integer with $p \nmid n$, and e be an n-th root of unity over $\mathbb{F}_2$, then*

$$Q_n(x) = \prod_{\substack{i=1,\\ gcd(i,n)=1}}^{n} (x - e^i) \tag{3}$$

is the n-th cyclotomic polynomial over $\mathbb{F}_2$.

According to the theory of cyclotomic polynomial [14], we have

$$1 + x^n = \prod_{d|n} Q_d(x) \tag{4}$$

and

$$Q_d(x) = \prod_{i=1}^{\varphi(d)/\deg(r_i(x))} r_i(x), \tag{5}$$

where $r_i(x)$ is an irreducible polynomial of degree $ord_d(2)$.

3 Bounds on Linear Complexity of Binary *half-ℓ-sequences* with Prime Connection Integer $q \equiv 1 \pmod 8$

In this section, we discuss the linear complexity of binary *half-ℓ-sequences* generated by FCSR with a prime connection integer $q \equiv 1 \pmod 8$.

Lemma 4. *[8] Let s^∞ be a binary half-ℓ-sequence generated by an FCSR with prime connection integer $q \equiv 1 \pmod 8$. Then s^∞ is balanced, and the first half of s^∞ is the bit-wise complement of its second half.*

Lemma 4 deduces the following lemma.

Lemma 5. *Let s^∞ be a binary half-ℓ-sequence generated by an FCSR with prime connection integer $q \equiv 1 \pmod 8$. Then $f(x) = 1 + x + x^{(q-1)/4} + x^{(q-1)/4+1}$ is a characteristic polynomial of s^∞.*

From the above lemma, we immediately get a general upper bound for linear complexity.

Theorem 1. *Let s^∞ be a binary half-ℓ-sequence generated by an FCSR with prime connection integer $q \equiv 1 \pmod 8$. Then we have*

$$LC(s^\infty) \le (q-1)/4 + 1.$$

Proof. By Lemma 5, we have $LC(s^\infty) \le \deg(f(x)) = (q-1)/4 + 1$. □

Below we give two lower bounds. The first (Theorem 3) is obtained by analyzing the characteristic polynomial of binary *half-ℓ-sequences*. The second lower bound (Theorem 4) is from the exponential representation of binary FCSR sequences.

Theorem 2. *Let s^∞ be a binary half-ℓ-sequence generated by an FCSR with prime connection integer $q \equiv 1 \pmod 8$. Write*

$$\frac{q-1}{2} = 4 \cdot 2^{e_0} p_1^{e_1}$$

with odd prime p_1 and $e_i \in \mathbb{N}$ for $i \in \{0,1\}$. Then we have

$$LC(s^\infty) \ge 1 + 2^{e_0+1} + ord_{p_1^{e_1}}(2).$$

Proof. Let I_d be the set of all the factors of d, for example, $I_{12} = \{1,2,3,4,6,12\}$. By Lemma 5, we see that

$$f(x) = (1+x)(1+x^{p_1^{e_1}})^{2^{e_0+1}}$$

is a characteristic polynomial of s^∞. According to Equactions (4) and (5),

$$\begin{aligned} f(x) =& (1+x)^{1+2^{e_0+1}} \prod_{d \mid p_1^{e_1}} Q_d(x)^{2^{e_0+1}} \\ =& (1+x)^{1+2^{e_0+1}} \prod_{d \mid p_1^{e_1}} \Big(\prod_{i=1}^{\varphi(d)/\deg(r_{i_d}(x))} r_{i_d}(x) \Big)^{2^{e_0+1}}. \end{aligned}$$

Since the minimal polynomial $m(x) \mid f(x)$, then

$$m(x) = (1+x)^a \prod_{j=1}^{k} \Big(\prod_{i=1}^{c_j} r_{i_{d_j}}(x) \Big)^{b_j}$$

where $d_j \mid p_1^{e_1}$, $1 \le k \le \#I_{p_1^{e_1}}$, $1 \le b_j \le 2^{e_0+1}$, $0 \le a \le 1 + 2^{e_0+1}$, and $1 \le c_j \le \varphi(d_j)/\deg(r_{i_{d_j}}(x))$.

From Lemma 3,

$$ord(m(x)) = 2^\xi \cdot lcm(d_1, d_2, \ldots, d_k),$$

where ξ is the least positive integer such that $2^\xi \ge \max\{a, b_1, \ldots, b_k\}$. From Lemma 2, $ord(m(x)) = (q-1)/2 = 2^{e_0+2} p_1^{e_1}$. Hence,

$$2^\xi = 2^{e_0+2}, lcm(d_1, d_2, \ldots, d_k) = p_1^{e_1}.$$

Clearly, $1 + 2^{e_0+1}$ is the least positive integer such that $2^\xi \ge 2^{e_0+2}$. For $d_j \mid p_1^{e_1}$, we have $\deg(r_{i_j}(x)) > 1$. So the degree of $m(x)$

$$\begin{aligned} \deg(m(x)) \ge& \deg((1+x)^{1+2^{e_0+1}} \prod_{j=1}^{k} r_{i_{d_j}}(x)) \\ \ge& 1 + 2^{e_0+1} + \sum_{j=1}^{k} ord_{d_j}(2). \end{aligned}$$

Since $d_j \mid p_1^{e_1}$ and $lcm(d_1, d_2, \ldots, d_k) = p_1^{e_1}$, there must exist some $1 \le k \le \#I_{p_1^{e_1}}$ such that $p_1^{e_1} \in \bigcup_{j=1}^{k} I_{d_j}$. So we have

$$\sum_{j=1}^{k} ord_{d_j}(2) > ord_{p_1^{e_1}}(2)$$

and

$$LC(s^\infty) = \deg(m(x)) \ge 1 + 2^{e_0+1} + ord_{p_1^{e_1}}(2).$$

□

Based on Theorem 2, we give a more general result.

Theorem 3. *Let s^∞ be a binary half-ℓ-sequence generated by an FCSR with prime connection integer $q \equiv 1 \pmod 8$. Write*

$$\frac{q-1}{2} = 4 \cdot 2^{e_0} p_1^{e_1} p_2^{e_2} \ldots p_t^{e_t}$$

with odd primes p_i, $e_0 \in \mathbb{N} \cup \{0\}$ and $e_i \in \mathbb{N}$ for $1 \le i \le t$. Then we have

$$LC(s^\infty) \ge 1 + 2^{e_0+1} + \max\{ord_{p_1^{e_1}}(2), \ldots, ord_{p_t^{e_t}}(2)\}.$$

Proof. Similar to Theorem 2,

$$f(x) = (1+x)^{1+2^{e_0+1}} \prod_{\substack{d>1, \\ d \mid \prod_{i=1}^{t} p_i^{e_i}}} \Big(\prod_{i=1}^{\varphi(d)/\deg(r_{i_d}(x))} r_{i_d}(x) \Big)^{2^{e_0+1}}$$

is a characteristic polynomial of s^∞. Let $m(x)$ be the minimal polynomial of s^∞, then

$$m(x) = (1+x)^a \prod_{j=1}^{k} \Big(\prod_{i=1}^{c_j} r_{i_{d_j}}(x) \Big)^{b_j},$$

where $d_j \mid \prod_{i=1}^{t} p_i^{e_i}$, $1 \le k \le \#I_{\prod_{i=1}^{t} p_i^{e_i}}$, $1 \le b_j \le 2^{e_0+1}$, $0 \le a \le 1 + 2^{e_0+1}$, and $1 \le c_j \le \varphi(d_j)/\deg(r_{i_{d_j}}(x))$. According to Lemma 3, we have $ord(m(x)) = 2^\xi \cdot lcm(d_1, d_2, \ldots, d_k)$, then $2^\xi = 2^{e_0+2}$ and $lcm(d_1, d_2, \ldots, d_k) = \prod_{i=1}^{t} p_i^{e_i}$.

Similar to Theorem 2,

$$\deg(m(x)) \geq 1 + 2^{e_0+1} + \sum_{j=1}^{k} ord_{d_j}(2).$$

Since $d_j \mid p_1^{e_1} p_2^{e_2} \ldots p_t^{e_t}$ and $lcm(d_1, \ldots, d_k) = \prod_{i=1}^{t} p_i^{e_i}$, there must exist some $1 \leq k \leq \#I_{p_1^{e_1} \ldots p_t^{e_t}}$ such that $\{p_1^{e_1}, \ldots, p_t^{e_t}\} \subset \bigcup_{j=1}^{k} I_{d_j}$. For $\gcd(a, b) = 1$, $ord_{ab}(2) = lcm(ord_a(2), ord_b(2)) \geq \max\{ord_a(2), ord_b(2)\}$. We can deduce

$$\sum_{j=1}^{k} ord_{d_j}(2) \geq \max\{ord_{p_1^{e_1}}(2), \ldots, ord_{p_t^{e_t}}(2)\}$$

and

$$LC(s^{\infty}) \geq 1 + 2^{e_0+1} + \max\{ord_{p_1^{e_1}}(2), \ldots, ord_{p_t^{e_t}}(2)\}.$$

□

Next, by Definition 1, we give a lower bound in Theorem 4.

Theorem 4. *Let s^{∞} be a binary half-ℓ-sequence generated by an FCSR with prime connection integer q. Then we have*

$$LC(s^{\infty}) \geq 1 + \lfloor \log_2(q) \rfloor.$$

Proof. From Definition 2, the generating function of sequence s^{∞} is

$$S(x) = \sum_{i=0}^{\infty} A \cdot 2^{-i} \pmod{q} \pmod{2} x^i \tag{6}$$

Let β be the prime such that $2^{\beta} < q$ and $2^{\beta+1} > q$, from Definition 1, we have

$$s_{T-1-\beta} = 2^{-T+(\beta+1)} \equiv 1 \pmod{q} \pmod{2}$$

and

$$s_{T-1-i} = 2^{-T+1+i} \equiv 0 \pmod{q} \pmod{2},$$

where $0 \leq i \leq \beta - 1$. Let $A = 1$ in Equation (6), then

$$S(x) = \sum_{i=0}^{T-1-(\beta+1)} s_i x^i + x^{T-1-\beta},$$

and

$$\deg(S(x)) \leq T - 1 - \lfloor \log_2(q) \rfloor.$$

From Lemma 1,

$$LC(s^{\infty}) = T - \deg(\gcd(x^T - 1, S(x))) \geq 1 + \lfloor log_2(q) \rfloor.$$

□

Remark 1. *The result in Theorem 4 holds for either $q \equiv 1 \pmod{8}$ or $q \equiv 7 \pmod{8}$.*

For all binary *half-ℓ-sequences* with prime $q \equiv 1 \pmod{8}$ and $q < 5000$, by the BM algorithm [12] and the results in the above theorems, we can check that about 82% of binary *half-ℓ-sequences* whose linear complexity achieves the upper bound in Theorem 1.

Example 1. *Let us consider the FCSR with connection integer $q = 41 = 2^0 \times 5 \times 8 + 1$, the period is $(q-1)/2 = 20$. With the constant $A = 1$, binary half-ℓ-sequence s^{∞} is given by*

$$s_i = 21^i \pmod{41} \pmod{2} \tag{7}$$

where $i = 0, 1, 2, \ldots$, then the first period of s^{∞} is

$$s^{20} = 11100111110001100000$$

From Theorem 1, $LC(s^{\infty}) \leq (q-1)/4 + 1 = 11$. From Theorem 3, $LC(s^{\infty}) \geq 1 + 2^{0+1} + ord_5(2) = 7$. And from Theorem 4, $LC(s^{\infty}) \geq 1 + \lfloor log_2(41) \rfloor = 6$. By the BM algorithm, the linear complexity $LC(s^{\infty}) = 11$.

4 Bounds on Linear Complexity of Binary *half-ℓ-sequences* with Prime Connection Integer $q \equiv 7 \pmod{8}$

In this section, we discuss the linear complexity of binary *half-ℓ-sequences* with prime $q \equiv 7 \pmod{8}$. We give an upper bound in Theorem 5 and a lower bound in Theorem 6, respectively.

For a T-periodic binary sequence s^{∞}, let $W_H(s^{\infty})$ denote the Hamming weight of the first period of s^{∞}, i.e. the number of 1's in one period of s.

Theorem 5. *Let s^{∞} be a binary half-ℓ-sequence s^{∞} generated by an FCSR with prime $q \equiv 7 \pmod{8}$. If $W_H(s^{\infty})$ is odd, then $LC(s^{\infty}) \leq (q-1)/2$. And if $W_H(s^{\infty})$ is even, then $LC(s^{\infty}) \leq (q-1)/2 - 1$.*

Proof. Let $W_H(s^{\infty})$ be even, then $(1 + x) \mid S(x)$. By Lemma 1, we have

$$\deg(\gcd(x^T - 1, S(x))) \geq \deg(1 + x)$$

and hence

$$LC(s^{\infty}) \leq (q-1)/2 - 1.$$

Let $W_H(s^{\infty})$ be odd, we know that $(1 + x) \nmid S^T(x)$. Similarly,

$$LC(s^{\infty}) \leq (q-1)/2.$$

□

Theorem 6. *Let s^{∞} be a binary half-ℓ-sequence generated by an FCSR with $q \equiv 7 \pmod{8}$. Write*

$$\frac{q-1}{2} = p_1^{e_1} p_2^{e_2} \ldots p_t^{e_t}$$

with odd primes p_i and $e_i \in \mathbb{N}$ for $1 \leq i \leq t$. Then we have

$$LC(s^{\infty}) \geq \max\{ord_{p_1^{e_1}}(2), ord_{p_2^{e_2}}(2), \ldots, ord_{p_t}^{e_t}(2)\}.$$

Proof. Let $m(x)$ be the minimal polynomial of s^∞. From Definition 4, we can deduce $m(x)|(1+x^{(q-1)/2})$.

Let $(q-1)/2 = \prod_{i=1}^{t} p_i^{e_i}$, then we have

$$ord(m(x)) = (q-1)/2 = \prod_{i=1}^{t} p_i^{e_i}.$$

Similar to Theorem 3,

$$1 + x^{(q-1)/2} = (1+x) \prod_{\substack{d>1,\\ d|p_1^{e_1}p_2^{e_2}\ldots p_t^{e_t}}} Q_d(x).$$

Suppose $m(x) = \prod_{j=1,b_j\geq 1}^{k} Q_{d_j}(x)^{b_j}$, where $d_j \mid \prod_{j=1}^{k} p_j^{e_j}$, $d_j > 1, b_j \geq 1$. From Lemma 3, we have

$$ord(m(x)) = 2^\xi \cdot lcm(d_1, d_2, \ldots, d_k),$$

where ξ is the least integer such that $2^\xi \geq \max\{b_1, b_2, \ldots, b_k\}$.

According to Lemma 2, $ord(m(x)) = \prod_{i=1}^{t} p_i^{e_i}$, we have

$$2^\xi = 1, lcm(d_1, d_2, \ldots d_k) = \prod_{i=1}^{t} p_i^{e_i}.$$

By Theorem 3, $LC(s^\infty) \geq \max\{ord_{p_1^{e_1}}(2), \ldots, ord_{p_t^{e_t}}(2)\}$. □

The result in Theorem 4 is also suitable for the case $q \equiv 7 \pmod 8$.

For prime $q < 5000$ with $q \equiv 7 \pmod 8$, we can check that about 86% of binary *half-ℓ-sequences* whose linear complexity achieves the upper bound.

Example 2. *Let us consider a binary half-ℓ-sequence s^∞ with $q = 47 = 5\times 8+7$, and the period of s^∞ is $(q-1)/2 = 23$. With the constant $A = 1$, the sequence is given by*

$$s_i = 24^i \pmod{47} \pmod 2 \tag{8}$$

where $i = 0, 1, 2, \ldots$. Then the first period of s^∞

$$s^{23} = 10001100100111010100000$$

From Theorem 3, $LC(s^\infty) \leq (q-1)/2 - 1 = 23$. From Theorem 4, $LC(s^\infty) \geq ord_{23}(2) = 11$. From 6 $LC(s^\infty) \geq 1 + \lfloor log_2(47)\rfloor = 7$. By the BM algorithm, the linear complexity is $LC(s^\infty) = 23$.

5 Conclusions

In this paper, we have discussed the linear complexity of binary *half-ℓ-sequences* generated by FCSRs. Based on the theory of FCSR and cyclotomic polynomial, we give some bounds of linear complexity and some examples. The numerical experiment shows that the linear complexity of most binary *half-ℓ-sequences* achieves the upper bound.

Acknowledgments

This work was partially supported by the National Key Research and Development Program of China(2018YFB0704400), Key Laboratory of Applied Mathematics of Fujian Province University (Putian University) (NO. SX202102), the National Nature Science Foundation of Shanghai (Grant No. 19ZR1417700), the Research and Development Program in Key Areas of Guangdong Province(Grant No.2018B010113001), the State Key Program of National Nature Science Foundation of China (Grant No. 61936001).

References

[1] F. Arnault and T. Berger, "F-FCSR: Design of a new class of stream ciphers," in *International Workshop on Fast Software Encryption, Lecture Notes in Computer Science*, vol. 3557, pp. 83–97, 2005.

[2] F. Arnault and T. Berger, "X-FCSR – A new software oriented stream cipher based upon FCSRs," in *Progress in Cryptology – INDOCRYPT 2007, Lecture Notes in Computer Science*, vol. 4859, pp. 341–350, Springer, 2007.

[3] F. Arnault and T. Berger, "A new approach for FCSRs," in *Selected Areas in Cryptography*, pp. 433–448, Springer, 2009. .

[4] A. Arshad, "Feedback with carry shift registers and (in-depth) security of ciphers based on this primitive," in *15th International Bhurban Conference on Applied Sciences and Technology (IBCAST'18)*, pp. 431–438, Pakistan, 2018.

[5] T. W. Cusick and C. Ding, *Stream ciphers and number theory.* Elsevier, 1998. ISBN: 9780444516312.

[6] L. Dong and J. Wang, "Novel analysis of stream cipher combing LFSR and FCSR," in *International Conference on Frontiers in Cyber Security*, vol. 879, pp. 23–38, 2018.

[7] M. Goresky and A. Klapper, *Algebraic shift register sequences.* Cambridge: Cambridge University Press, 2012. ISBN: 9781107014992.

[8] T. Gu and A. Klapper, "Distribution properties of half-ℓ-sequence," in *Sequences and Their Applications - SETA 2014, Lecture Notes in Computer Science*, vol. 8865, pp. 234–245, Cham, 2014.

[9] M. S. Hwang and I. C. Lin, *Introduction to Information and Network security (6ed, in Chinese).* Taiwan: Mc Graw Hill, 2017.

[10] A. Klapper and M. Goresky, "Feedback shift registers, 2-adic span, and combiners with memory," *Journal of Cryptology*, vol. 10, no. 2, pp. 111–147, 1997.

[11] Z. Lin, D. Pei, and D. Lin, "Fast construction of binary ring FCSRs for hardware stream ciphers," *Designs, Codes and Cryptography*, vol. 86, no. 4, pp. 939–953, 2018.

[12] J. Massey, "Shift-register synthesis and BCH decoding," *IEEE Transactions on Information Theory*, vol. 15, no. 1, pp. 122–127, 1969.

[13] W. Qi and H. Xu, "On the linear complexity of FCSR sequences," *Applied mathematics-A journal of Chinese universities*, vol. 18, no. 3, pp. 318–324, 2003.

[14] L. Rudolf and N. Harald, *Introduction to finite fields and their applications*. Cambridge: Cambridge university press, 1994. ISBN: 9780521460941.

[15] C. Seo, S. Lee, and Y. Sung, "A lower bound on the linear span of an FCSR," *IEEE Transactions on Information Theory*, vol. 46, no. 2, pp. 691–693, 2000.

[16] L. Tan and W. Qi, "On the k-error linear complexity of l-sequences," *Finite Fields and Their Applications*, vol. 16, no. 6, pp. 420–435, 2010.

[17] T. Tian and W. Qi, "2-adic complexity of binary m-sequences," *IEEE Transactions on Information Theory*, vol. 56, no. 1, pp. 450–454, 2009.

[18] Q. C. Wang and C. H. Tan, "New bounds on the imbalance of a half-l-sequence," in *2015 IEEE International Symposium on Information Theory (ISIT)*, pp. 2688–2691, 2015.

[19] N. Yerukala and V. Nalla, "Alternating step generator using FCSR and LFSRs: A new stream cipher," *International Journal of Intelligent Engineering and Systems*, vol. 12, no. 5, pp. 130–138, 2019.

Biography

Zhihua Niu was born in 1976 in Shanxi, China. She received the B.S. degree in Mathematics Education from Huaibei Normal University in 1998, and the M.S. degree in Computational Mathematics from Xi'an Jiaotong University in 2002, and the Ph.D. degree in Cryptography from Xidian University in 2005. She is now with the School of Computer Engineering and Science, Shanghai University, China. She worked as a visiting scholar supervised by Prof. Andrew Klapper in University of Kentucky(Lexington) during 2013-2014. Her research interests include pseudo-random sequences, cryptography and information security.

Yuqi Sang was born in 1996 in Henan, China. He was received the B.E. degree in Materials Science from Henan University of Science and Technology. He is now studying for a master's degree at the School of Computer Engineering and Science in Shanghai University.