Constructing a Diversified FCSR with a Given Connection Integer

Zhiqiang Lin and Dingyi Pei

College of Mathematics and Information Science, Guangzhou University,
Guangzhou 510006, China
linzhiqiang0824@yahoo.cn; gztcdpei@scut.edu.cn

Abstract. A new FCSR representation called a diversified representation is used to replace the Galois one, avoiding the LFSRization attack. Hence, to build hardware and software oriented diversified FCSRs becomes an important problem. In this paper, we show a method of constructing a diversified FCSR for hardware implementation with a given connection integer. The construction is simple and convenient. And the diversified FCSRs we get are able to meet the hardware criteria.

Keywords: stream cipher, 2-adic number, diversified FCSRs, l-sequences

1 Introduction

FCSRs was first proposed to generate sequences for cryptographic applications by Klapper and Goresky in 1994 [14]. According to their nonlinearity, FCSRs have been suggested as an alternative to LFSRs for avoiding the drawback of linear structure. The generated sequences of FCSRs are 2-adic sequences. A 2-adic sequence is associated with a 2-adic integer p/q. The statistical properties of these sequences have been presented in [9] [10] [14] [15].

FCSRs are usually implemented by hardware and software using the Galois representation rather than the Fibonacci one [11]. Family of hardware stream ciphers based on FCSRs–F-FCSRs [1] [2] [3] [4] and family of software stream ciphers based on FCSRs–X-FCSRs [5] [7] were proposed for stream cipher design. However, Galois FCSRs were exposed to a very powerful attack [12] [16] by LFSRization of them.

In [4] [7], a new FCSR representation called a ring or diversified representation was proposed to respond to the LFSRization attack. This new representation is based on the transition faction with matrix instead of with Boolean functions. Other advantages were brought by this new representation if the transition function is well-chosen. To build hardware oriented FCSRs, the criteria are that the critical path length must be equal to 1 and the fan-out must be 2. For software applications, a particular realization suitable for software utilization has been given. This realization uses a specific circuit which acts essentially on binary

words. In [6], Arnault et al. have generalized diversified FCSRs through particular automata called 2-adic automata. These automata have been constructed of inputs and outputs, with the entries of matrices in the set of 2-adic integers.

In this paper, we focus on the hardware stream cipher designed in the form of a special king of 2-adic automata, called ternary diversified FCSRs. The criteria to build this automaton were presented in [4] [6]. The criteria could be achieved by well-chosen of the transition matrix A:
—the matrix must be composed of −1,0 and 1, the over-diagonal must be full of 1, $a_{n-1,0} = 1$, and the number of no-zero elements for a given row or a given column must be at most two;
—the connection integer $q = det(I - 2A)$ must be prime and the order of 2 module q must be $|q| - 1$ for preserving the output sequences of good statistical properties.

To get a suitable transition matrix, in [6], the authors have presented an efficient algorithm. They pick a random matrix in the form of the requirements, and then test whether the connection integer $q = det(I - 2A)$ meets the standards. But it is time-consuming because they have to compute and test q every time. So an open problem has been presented: How can a diversified FCSR be constructed when a connection integer is specified?

We solve this problem in this paper. The method of our construction is simple and convenient. It is more efficient than the algorithm above. Theorem 4 and Theorem 5 in section 3 are our main results, and through the results we also prove a conjecture in [6]: For each given q of size n, there is a transition matrix with a critical path of length 1 and fan-out 2. This paper is organized as follows: In section 2, we recall some properties of 2-adic integers and the concepts of diversified FCSRs. In section 3, we present our construction. In section 4, we make a conclusion and point out some deficiencies of our construction.

2 Diversified FCSRs

In this section, we briefly introduce some properties of 2-adic integers and some notations. Then we present the criteria to build hardware oriented FCSRs.

2.1 2-adic integers and notations

First, we recall some properties of 2-adic numbers. For more details, the readers could refer to [8].

A 2-adic integer is formally a power series $s = \sum_{i=0}^{\infty} s_i 2^i$ with $s_i \in \{0, 1\}$. The set of 2-adic integers is a ring denoted by $\mathbb{Z}_2$. Addition and multiplication in $\mathbb{Z}_2$ can be performed by reporting the carries to the higher order terms, i.e., $2^n + 2^n = 2^{n+1}$ for all $n \in \mathbb{N}$. s is a positive integer if there exists an integer K such that $s_n = 0$ for all $n \geq K$. Moreover, any odd integer q has an inverse in $\mathbb{Z}_2$ which can be computed by $q^{-1} = \sum_{n=0}^{\infty} q'^n$, where $q' = 1 - q$.

The following theorems present the relationship between eventually periodic sequences and 2-adic integers.

Theorem 1. *Let $s = \sum_{i=0}^{\infty} s_i 2^i$ be a 2-adic integers, with $s_i \in \{0,1\}$. Denote $S = (s_i)_{i\in\mathbb{N}}$. Then the sequences S is eventually periodic if and only if there exists two numbers p and q in $\mathbb{Z}$, q odd, such that $s = p/q$. Moreover, S is strictly periodic if and only if $pq \leq 0$ and $|p| \leq |q|$.*

Theorem 2. *Let $s = \sum_{i=0}^{\infty} s_i 2^i = p/q$ with $s_i \in \{0,1\}$, $pq \leq 0$, $|p| \leq |q|$, q odd and $gcd(p,q) = 1$. Denote $S = (s_i)_{i\in\mathbb{N}}$. Then S is strictly periodic and the period of S is the order of 2 modulo q, i.e., the smallest integer P such that $2^P \equiv 1(modq)$, $T \geq |q| - 1$.*

Definition 1. *An l-sequence is a periodic sequence $S = (s_i)_{i\in\mathbb{N}}$ such that $s = \sum_{i=0}^{\infty} s_i 2^i = p/q$ with $s_i \in \{0,1\}$, $pq \leq 0$ and the order of 2 modulo q is $|q| - 1$.*

In this paper, we use the notations proposed in [6].

Given a sequence $a = (a(t))_{t\in\mathbb{N}}$ of elements in $\{0,1\}$, we have

$$\sum_{t\geq t_0} a(t)2^{t-t_0} = a(t_0)2^0 + a(t_0+1)2^1 + \cdots$$

in $\mathbb{Z}_2$.

A time dependent vector m in $\{0,1\}^n$ is denoted at time t by $m(t) = (m_0(t), \ldots, m_{n-1}(t))$. And we denote

$$M(t_0) = \sum_{t\geq t_0} m(t)2^{t-t_0}$$

in $\mathbb{Z}_2$, i.e., $M(t_0) = (M_0(t_0), \ldots, M_{n-1}(t_0))$, where

$$M_i(t_0) = m_i(t_0)2^0 + m_i(t_0+1)2^1 + \cdots ,$$

$0 \leq i \leq n-1$.

For any matrix T of size $n \times n$, we denote by T^* the adjugate of T. That is, with $T = (t_{i,j})_{0\leq i,j\leq n-1}$ and $T^* = (t^*_{i,j})_{0\leq i,j\leq n-1}$, we have

$$t^*_{i,j} = (-1)^{i+j} \begin{vmatrix} t_{0,0} & \cdots & t_{0,i-1} & t_{0,i+1} & \cdots & t_{0,n-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ t_{j-1,0} & \cdots & \vdots & \vdots & \cdots & t_{j-1,n-1} \\ t_{j+1,0} & \cdots & \vdots & \vdots & \cdots & t_{j+1,n-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ t_{n-1,0} & \cdots & t_{n-1,i-1} & t_{n-1,i+1} & \cdots & t_{n-1,n-1} \end{vmatrix}$$

The following property of determinants is important for our construction in this paper:

Proposition 1. *Let A be a matrix over a ring R of size $n \times n$. Let $E_{i,j}$ be the matrix with a single 1 in position i, j. Then $det(A + \lambda E_{i,j}) = det(A) + \lambda Cof_{i,j}$, where $Cof_{i,j}$ denotes the cofactor i, j of the matrix A.*

2.2 Binary and ternary diversified FCSRs

A new FCSR representation was first introduced in [4] for responding to the attack against the stream ciphers based on Galois FCSRs [12].

Definition 2. *A binary diversified FCSR is an automaton composed of a main shift register of n binary cells $m = (m_0, m_1, \ldots, m_{n-1})$, and a carry register of n integer cells $c = (c_0, c_1, \ldots, c_{n-1})$. It is updated using the following relations:*

$$\begin{cases} m(t+1) = Am(t) + c(t) \ mod \ 2 \\ c(t+1) = Am(t) + c(t) \ \ div \ 2 \end{cases}$$

where A is a $n \times n$ matrix with entries 0 or 1 in $\mathbb{Z}$, called transition matrix.

Binary diversified FCSRs is a special kind of no-input binary 2-adic FSMs which have been presented in [6]. Moreover, in [6], using subtracter-with-carry to compute the difference between two 2-adic integers, the authors have proposed an extension of binary 2-adic FSMs, which allows the entries of the matrices in $\{-1, 0, 1\}$. These automata are called ternary 2-adic FSMs. Here, we only care about the no-input ones.

Definition 3. *A ternary diversified FCSR is the same automaton as the one defined in Definition 2 except for the entries of the transition matrix A in $\{-1, 0, 1\}$.*

Binary diversified FCSRs is a special kind of ternary diversified FCSRs, hence ternary diversified FCSRs is often called diversified FCSRs for short. There are some properties of 2-adic FSMs presented in [6], which are also the behaviors of diversified FCSRs.

Proposition 2. *Consider a diversified FCSR composed of main register m and carry register c. The transition matrix is A. Let $M(t_0) = \sum_{i=0}^{\infty} m(i+t_0)2^i$. Then we have*

$$M(t_0 + 1) = AM(t_0) + c(t_0)$$

Theorem 3. *The series $M_i(t_0)$ observed in each cell of the main register are 2-adic expansion of p_i/q with $p_i \in \mathbb{Z}$ and with integer $q = det(I - 2A)$. q is called the connection integer of the automaton.*

2.3 Hardware oriented FCSRs and hardware criteria

To build hardware oriented FCSRs, we use diversified FCSRs to replace Galois FCSRs for avoiding the powerful attack proposed in [12]. The reader can refer to [4] for more details of hardware oriented FCSRs. Here, we focus on the choice of the transition matrix A for hardware implementation.

We first consider some of the characteristics of hardware implementation: Critical path— the critical path length is the maximum number of logic gates the signal has to pass though. If this number is low, the automaton can be clock

at a higher rate.
Fan-out— the signal of a binary cell should drive a minimal number of gates as exposed in [13]. Large fan-out makes possible differential power analysis attacks.
Cost— the number of logic gates must be as small as possible to lower consumption and cost of the automaton.

Shorter length of critical, small fan-out and lower cost lead to high clock frequencies. These data can be computed from the transition matrix A:
— the critical path length is the smallest integer j such that 2^j is greater or equal to the highest Hamming weight of the rows a_i;
— the fan-out is the highest Hamming weight of the columns b_i;
— the cost is the Hamming weight of A.

The critical path of length 1 and fan-out 2 is the minimum, so the requirements of the transition matrix $A = (\alpha_{i,j})_{0 \le i,j \le n-1}$ of size $n \times n$ are as follows:
— the over-diagonal must be full of 1 and $\alpha_{n-1,0} = 1$ (to preserve the shifting);
— the number of no-zeros for any given row or a given column must be at most two (to preserve the critical length 1 and fan-out 2);
— $q = det(I - 2A)$ is prime, and the order of 2 modulo q is $|q| - 1$ (to preserve outputting l-sequences).

An algorithm has been given to choose a suitable transition matrix for hardware implementation in [6]. In this algorithm, a matrix A has been constructed in the form of the requirements, then $q = det(I - 2A)$ is tested whether it is prime and whether 2 is the primitive root modulo q. If q passes the test, A is a suitable matrix. However, this algorithm is time-consuming, because every time q has to be computed and tested whether it is primitive. Hence, at the end of the paper [6], the authors leave an open problem: How can a diversified FCSR be constructed when a connection integer is specified? Fortunately, we find a method to solve this problem. By our method, for a given integer q, we can immediately construct a suitable A, without any test and complicated computation. Our construction will be showed in the next section.

3 Construction A with a given q

Given a negative odd integer q, we will construct a matrix $A = (\alpha_{i,j})_{0 \le i,j \le n-1}$ with entries in $\{-1, 0, 1\}$ meeting the requirements as follows:
— the over diagonal must be full of 1 and $\alpha_{n-1,0} = 1$;
— the number of no-zero elements for a given row or a given column must be at most two;
— $q = det(I - 2A)$.

Lemma 1. *Let*

$$A_0 = (a_{i,j})_{0 \le i,j \le n-1} = \begin{pmatrix} 0 & 1 & & & \\ & 0 & 1 & & \\ & & \ddots & \ddots & \\ & & & 0 & 1 \\ 1 & & & & 0 \end{pmatrix} \text{ and } A_0' = (a'_{i,j})_{0 \le i,j \le n-1} = \begin{pmatrix} 0 & 1 & & & \\ & 0 & 1 & & \\ & & \ddots & \ddots & \\ & & & 0 & 1 \\ 1 & & & & 1 \end{pmatrix}$$

be two matrices over $\mathbb{Z}$ *of size* $n \times n$*, the over diagonals of* A_0 *and* A'_0 *are full of 1,* $a_{n-1,0} = a'_{n-1,0} = a'_{n-1,n-1} = 1$*, and the other entries are all* 0*. Let* $B_0 = (b_{i,j})_{0 \le i,j \le n-1} = I - 2A_0$*,* $B'_0 = (b'_{i,j})_{0 \le i,j \le n-1} = I - 2A'_0$*. Then* $det(B_0) = 1 - 2^n$*,* $det(B'_0) = -1 - 2^n$*, and the adjoint matrices of* B_0 *and* B'_0 *are*

$$B_0^* = (b_{i,j}^*)_{0 \le i,j \le n-1} = \begin{pmatrix} 1 & 2 & 2^2 & \cdots & 2^{n-1} \\ 2^{n-1} & 1 & 2 & \cdots & 2^{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 2 & 2^2 & 2^3 & \cdots & 1 \end{pmatrix}$$

where $b_{i,j}^* = 2^{(j-i) mod n}$*, for* $0 \le i, j \le n-1$*;*

$$B_0'^* = (b_{i,j}'^*)_{0 \le i,j \le n-1} = \begin{pmatrix} -1 & -2 & -2^2 & \cdots & -2^{n-2} & 2^{n-1} \\ 2^{n-1} & -1 & -2 & \cdots & -2^{n-3} & 2^{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 2^2 & 2^3 & 2^4 & \cdots & -1 & 2 \\ 2 & 2^2 & 2^3 & \cdots & 2^{n-1} & 1 \end{pmatrix}$$

where
$b_{i,j}'^* = 2^{(j-i) mod n}$*, for* $0 \le i \le n-1$*,* $0 \le j \le n-2$ *and* $i > j$*;*
$b_{i,j}'^* = -2^{(j-i) mod n}$*, for* $0 \le i \le n-1$*,* $0 \le j \le n-2$ *and* $i \le j$*;*
$b_{i,n-1}'^* = 2^{n-1-i}$*, for* $0 \le i \le n-1$*.*

Proof. $det(B_0)$ and $det(B'_0)$ can be computed directly. B_0^* and $B_0'^*$ can be computed with classical inversion algorithms. □

Our idea is that given a initial matrix A_0 or A'_0 defined in Lemma 1, we replace a 0 of the matrix with an 1 or -1 each time following the requirements of A mentioned at the beginning of this section, and each time we get a new matrix A_{new}. Denote $B = I - 2A_{new}$. $Det(B)$ is made to approach to q step by step, and finally equal to q. By Proposition 1, we can choose a position for replacing the 0 through observing the adjoint matrix B^* of B, which seems to help achieving our goal. However, it is troublesome that we have to compute B^* in every step, because B^* is changing every time. Fortunately, we find that some elements of B^* are invariant when modifying some entries in the lower triangular of B.

Lemma 2. *Let* B_0 *be the matrix defined in Lemma 1, i.e.,*

$$B_0 = (b_{i,j})_{0 \le i,j \le n-1} = \begin{pmatrix} 1 & -2 & & \\ & \ddots & \ddots & \\ & & \ddots & -2 \\ -2 & & & 1 \end{pmatrix}$$

where $b_{i,i} = 1$ *for* $0 \le i \le n-1$*,* $b_{i,i+1} = -2$ *for* $0 \le i \le n-2$*,* $b_{n-1,0} = -2$*, and other entries are all* 0*. Suppose* $B_0^* = (b_{i,j}^*)_{0 \le i,j \le n-1}$ *is the adjoint*

matrix of B_0. Change some elements $b_{i,j}(i > j)$ of B_0, and suppose they are $b_{i_0,j_0}, b_{i_1,j_1}, \ldots, b_{i_{g-1},j_{g-1}}$ for $i_t > j_t$ $(0 \le t \le g-1)$, $i_0 < i_1 < \cdots < i_{g-1}$ and $j_0 > j_1 > \cdots > j_{g-1}$. Denote $B_1 = (c_{i,j})_{0 \le i,j \le n-1}$ as the new matrix, where $c_{i,j} = b_{i,j}$ for $i, j \ne i_t, j_t$ $(0 \le t \le g-1)$, and c_{i_t,j_t} $(0 \le t \le g-1)$ are the changed elements. Denote $B_1^* = (c_{i,j}^*)_{0 \le i,j \le n-1}$ as the adjoint matrix of B_1. Then

$$c_{k,l}^* = b_{k,l}^* \text{ for } k < l,\ k \le i_0 \text{ and } l \ge j_0.$$

Moreover, if we use $B_0' = \begin{pmatrix} 1 & -2 & & \\ & \ddots & \ddots & \\ & & 1 & -2 \\ -2 & & & -1 \end{pmatrix}$ *which is also defined in Lemma 1 to replace B_0, the result is still valid.*

Proof. Consider $b_{k,l}^*$ $(k < l)$, we have

$$b_{k,l}^* = (-1)^{k+l} det(B_{k,l}^*)$$

where $B_{k,l}^*$ is a matrix of size $(n-1) \times (n-1)$ by deleting the lth row the kth column of B_0, i.e.,

$$B_{k,l}^* = \begin{pmatrix} b_{0,0} & \cdots & b_{0,k-1} & b_{0,k+1} & \cdots & b_{0,l} & b_{0,l+1} & \cdots & b_{0,n-1} \\ \vdots & \cdots & \vdots & \vdots & \cdots & \vdots & \vdots & \cdots & \vdots \\ b_{k-1,0} & \cdots & b_{k-1,k-1} & b_{k-1,k+1} & \cdots & b_{k-1,l} & b_{k-1,l+1} & \cdots & b_{k-1,n-1} \\ b_{k,0} & \cdots & b_{k,k-1} & b_{k,k+1} & \cdots & b_{k,l} & b_{k,l+1} & \cdots & b_{k,n-1} \\ \vdots & \cdots & \vdots & \vdots & \cdots & \vdots & \vdots & \cdots & \vdots \\ b_{l-1,0} & \cdots & b_{l-1,k-1} & b_{l-1,k+1} & \cdots & b_{l-1,l} & b_{l-1,l+1} & \cdots & b_{l-1,n-1} \\ b_{l+1,0} & \cdots & b_{l+1,k-1} & b_{l+1,k+1} & \cdots & b_{l+1,l} & b_{l+1,l+1} & \cdots & b_{l+1,n-1} \\ \vdots & \cdots & \vdots & \vdots & \cdots & \vdots & \vdots & \cdots & \vdots \\ b_{n-1,0} & \cdots & b_{n-1,k-1} & b_{n-1,k+1} & \cdots & b_{n-1,l} & b_{n-1,l+1} & \cdots & b_{n-1,n-1} \end{pmatrix}$$

$$= \begin{pmatrix} D & & 0 \\ & E & \\ * & & F \end{pmatrix}$$

where

$$D = \begin{pmatrix} b_{0,0} & \cdots & b_{0,k-1} \\ \vdots & \ddots & \vdots \\ b_{k-1,0} & \cdots & b_{k-1,k-1} \end{pmatrix} = \begin{pmatrix} 1 & -2 & & 0 \\ & 1 & -2 & \\ & & \ddots & \ddots \\ 0 & & & 1 \end{pmatrix}$$

$$E = \begin{pmatrix} b_{k,k+1} & b_{k,k+2} & \cdots & b_{k,l} \\ b_{k+1,k+1} & b_{k+1,k+2} & \cdots & b_{k+1,l} \\ \vdots & \vdots & \cdots & \vdots \\ b_{l-1,k+1} & b_{l-1,k+2} & \cdots & b_{l-1,l} \end{pmatrix} = \begin{pmatrix} -2 & & & 0 \\ & -2 & & \\ & & \ddots & \\ * & & & -2 \end{pmatrix}$$

$$F = \begin{pmatrix} b_{l+1,l+1} & \cdots & b_{l+1,n-1} \\ \vdots & \cdots & \vdots \\ b_{n-1,l+1} & \cdots & b_{n-1,n-1} \end{pmatrix} = \begin{pmatrix} 1 & -2 & & 0 \\ & 1 & -2 & \\ & & \ddots & \ddots \\ 0 & & & 1 \end{pmatrix}$$

Then, $det(B^*_{k,l}) = det(D)det(E)det(F) = (-2)^{l-k}$, and $b^*_{k,l} = (-1)^{k+l} \cdot (-2)^{l-k} = 2^{l-k}$. We can see that b_{i_t,j_t} $(0 \le t \le g-1)$ are all in the position $*$ of $B_{k,l}$ and E, so changing b_{i_t,j_t} can not effect the value of $det(B^*_{k,l})$. It implies that $c^*_{k,l} = b^*_{k,l} = 2^{l-k}$ for $k < l$, $k \le i_0$ and $l \ge j_0$.

Moreover, if we use B'_0 to replace B_0, $F' = \begin{pmatrix} 1 & -2 & & 0 \\ & 1 & -2 & \\ & & \ddots & \ddots \\ 0 & & & 1 \end{pmatrix}$ is substituted for F in the above proof, and other discussions are similar. Therefore, the result is still valid. □

Now we can construct A with some special q.

Let $q = -2^n - q_{n-1}2^{n-1} - \cdots - q_1 2 + 1$ be a negative odd integer. In the following we assume that $n \ge 3$ and at least one coefficient among $q_i (2 \le i \le n-1)$ is 1. It is easy to see that the conclusions of the following theorem are also true for these exclusive cases by Lemma 1.

Theorem 4. *Given a negative odd integer q. Let $q = -2^n - q_{n-1}2^{n-1} - \cdots - q_1 2 + 1$, where $q_i = 0$ or 1 for $1 \le i \le n-1$. Let $s = (q_{n-1}, q_{n-2}, \ldots, q_2)$ be a vector of size $n-2$, and suppose that there is no consecutive 1 in s, i.e.,*

$$s = (0, \ldots, 0, q_{i_0}, 0, \ldots, 0, q_{i_1}, 0, \ldots, 0, \ldots, 0, \ldots, 0, q_{i_{k-1}}, 0, \ldots, 0),$$

where $q_{i_j} = 1$ $(0 \le j \le k-1, 2 \le i_j \le n-1)$ are all the elements equal to 1 in s, $i_j - i_{j+1} \ge 2$ for $0 \le j \le k-2$. Then we can construct a matrix A with entries in $\{-1, 0, 1\}$, meeting the requirements presented at the beginning of this section. The construction is as follows:
Denote $A = (\alpha_{i,j})_{0 \le i,j \le n-1}$ of size $n \times n$.

If $q_1 = 0$, set $\alpha_{i,i+1} = 1$ for $0 \le i \le n-2$, $\alpha_{n-1,0} = 1$, $\alpha_{i_j+j-1,j} = 1$ for $0 \le j \le k-1$ and other elements of A equal to 0, then A meets the requirements.

If $q_1 = 1$, set $\alpha_{i,i+1} = 1$ for $0 \le i \le n-2$, $\alpha_{n-1,0} = \alpha_{n-1,n-1} = 1$, $\alpha_{i_j+j-1,j} = -1$ for $0 \le j \le k-1$ and other elements of A equal to 0, then A meets the requirements.

Proof. If $q_1 = 0$, let $A_0 = (a_{i,j})_{0\le i,j\le n-1}$, $B_0 = (b_{i,j})_{0\le i,j\le n-1} = I - 2A_0$ and $B_0^* = (b^*_{i,j})_{0\le i,j\le n-1}$ be the matrices defined in Lemma 1. Then the construction above is equal to change $a_{i_j+j-1,j}$ into 1 for $0 \le j \le k-1$, which corresponds to change $b_{i_j+j-1,j}$ into -2. It is easy to see that $i_j+j-1 > j$ because $i_j \ge 2$. Since $i_j - i_{j+1} \ge 2$ for $0 \le j \le k-2$, then $i_{j+1}+j < i_j+j-1$ for $j = k-2, k-3, \ldots 1, 0$. Therefore we have

$$\begin{aligned} det(I-2A) &= det(B_0) - 2b^*_{0,i_0-1} - 2b^*_{1,i_1+1-1} - \cdots - 2b_{k-1,i_{k-1}+k-1-1} \\ &= det(B_0) - 2\times 2^{i_0-1} - 2\times 2^{i_1-1} - \cdots - 2\times 2^{i_{k-1}-1} \\ &= -2^n - 2^{i_0} - 2^{i_1} - \cdots - 2^{i_{k-1}} + 1 = q \end{aligned}$$

by Proposition 1, Lemma 1 and Lemma 2. It is easy to see that every element changed in this construction is in different rows and columns.

The proof of the case $q_1 = 1$ is similar to the proof above, starting with the matrix A_0' defined in Lemma 1 instead of A_0. □

If there exists consecutive 1 in s, the construction in Theorem 4 is invalid. However, we can dispose s by a fact:

$$2^{t+s} + 2^{t+s-1} + \cdots + 2^t = 2^{t+s+1} - 2^t,$$

where $t, s \in \mathbb{N}$. Hence, if there exists consecutive 1 in s, i.e., a string of $0\underbrace{11\cdots1}_{l}0$ in s, we can change it into $1\underbrace{00\cdots0}_{l-1}-10$.

Two special cases for existing consecutive 1 in s are considered in the following theorem :

Theorem 5. *Given a negative odd integer q. Let $q = -2^n - q_{n-1}2^{n-1} - \cdots - q_1 2 + 1$, where $q_i = 0$ or 1 for $1 \le i \le n-1$. Then we can construct a matrix A with entries in $\{-1, 0, 1\}$, meeting the requirements presented at the beginning of this section. The construction is as follows:*

Let $s = (q_{n-1}, q_{n-2}, \ldots, q_2)$ be a vector of size $n-2$. From right to left, do the following by iteration: if there is a string of 1 in s, i.e., $0\underbrace{11\cdots1}_{l}0$, change it into $1\underbrace{00\cdots0}_{l-1}-10$. At the end of the iteration, we get a new vector $s' = (s'_{n-1}, \ldots, s'_2)$.

Then we have:

Case 1: there is no consecutive 1 in s', such as

$$s' = (0, \ldots, 0, s'_{i_0}, 0, \ldots, 0, s'_{i_1}, 0, \ldots, 0, \ldots, 0, \ldots, 0, s'_{i_{k-1}}, 0, \ldots, 0),$$

where s'_{i_j} $(0 \le j \le k-1, 2 \le i_j \le n-1)$ *are all the no-zero elements in* s', $i_j - i_{j+1} \ge 2$ *for* $0 \le j \le k-2$. *We construct* A *as in Theorem 4:*
Denote $A = (\alpha_{i,j})_{0 \le i,j \le n-1}$ *of size* $n \times n$.

If $q_1 = 0$, *set* $\alpha_{i,i+1} = 1$ *for* $0 \le i \le n-2$, $\alpha_{n-1,0} = 1$, $\alpha_{i_j+j-1,j} = s'_{i_j}$ *for* $0 \le j \le k-1$ *and other elements of* A *equal to* 0, *then* A *meets the requirements.*

If $q_1 = 1$, *set* $\alpha_{i,i+1} = 1$ *for* $0 \le i \le n-2$, $\alpha_{n-1,0} = \alpha_{n-1,n-1} = 1$, $\alpha_{i_j+j-1,j} = -s'_{i_j}$ *for* $0 \le j \le k-1$ *and other elements of* A *equal to* 0, *then* A *meets the requirements.*

Case 2: there is consecutive 1 *in the left of* s', *i.e.,*

$$s' = (s'_{n-1}, s'_{n-2}, \ldots, s'_l, s'_{l-1}, 0, \ldots, 0, s'_{i_0}, 0, \ldots, 0, s'_{i_1}, 0, \ldots, 0, \ldots, 0, \ldots, 0, s'_{i_{m-1}}, 0, \ldots, 0),$$

where $s'_{n-1} = s'_{n-2} = \cdots = s'_l = 1$ *and* $s'_{l-1} = 0 (l > 2)$, s'_i $(l \le i \le n-1)$ *and* s'_{i_j} $(0 \le j \le m-1)$ *are all the no-zero elements in* s. *Then let* $s'' = (s''_n, s''_{n-1}, \ldots, s''_2)$ *be a vector of size* $n-1$, *where* $s''_n = s''_{n-1} = \cdots = s''_{l+1} = 0$, $s''_l = -1$ *and* $s''_i = s'_i$ *for* $i < l$. *Denote a matrix* $A_1 = (\beta_{i,j})_{0 \le i,j \le n}$ *of size* $(n+1) \times (n+1)$.

If $q_1 = 0$, *set* $\beta_{i,i+1} = 1$ *for* $0 \le i \le n-1$, $\beta_{n,0} = 1$, $\beta_{i_j+j-1,j} = s''_{i_j}$ *for* $0 \le j \le m-1$, *and other elements of* A_1 *equal to* 0, *then* A_1 *meets the requirements.*

If $q_1 = 1$, *set* $\beta_{i,i+1} = 1$ *for* $0 \le i \le n-1$, $\beta_{n,0} = \beta_{n,n} = 1$, $\beta_{i_j+j-1,j} = -s''_{i_j}$ *for* $0 \le j \le m-1$, *and other elements of* A_1 *equal to* 0, *then* A_1 *meets the requirements.*

Proof. The construction is the same as Theorem 4 after s has been changed into s' or s''. Hence we only need to prove that the disposal of s is feasible. Through the discussion before this theorem, we have

$$s'_{n-1}2^{n-1} + s'_{n-2}2^{n-2} + \cdots + s'_2 2^2 = q_{n-1}2^{n-1} + q_{n-2}2^{n-2} + \cdots + q_2 2^2.$$

Then, if $q_1 = 0$, by Theorem 4, we have
case 1:

$$\begin{aligned} det(I - 2A) &= -2^n - s'_{i_0}2^{i_0} - s'_{i_1}2^{i_1} - \cdots - s'_{i_{k-1}}2^{i_{k-1}} + 1 \\ &= -2^n - s'_{n-1}2^{n-1} - \cdots - s'_2 2^2 + 1 \\ &= -2^n - q_{n-1}2^{n-1} - \cdots - q_2 2^2 - q_1 2 + 1 = q \end{aligned}$$

case 2:

$$\begin{aligned} det(I - 2A_1) &= -2^{n+1} - s''_{i_0}2^{i_0} - s''_{i_1}2^{i_1} - \cdots - s''_{i_{m-1}}2^{i_{m-1}} + 1 \\ &= -2^{n+1} - s''_n 2^n - s''_{n-1}2^{n-1} - \cdots - s''_2 2^2 + 1 \\ &= -2^{n+1} + 2^l - s'_{l-1}2^{l-1} - \cdots - s'_2 2^2 + 1 \\ &= -2^n - 2^{n-1} - \cdots - 2^l - s'_{l-1}2^{l-1} - \cdots - s'_2 2^2 + 1 \\ &= -2^n - s'_{n-1}2^{n-1} - \cdots - s'_2 2^2 + 1 \\ &= -2^n - q_{n-1}2^{n-1} - \cdots - q_2 2^2 - q_1 2 + 1 = q \end{aligned}$$

If $q_1 = 1$, the proof is similar to the computation above. □

It is a pity that the construction of Theorem 5 can not get a shortest diversified FCSR with a given q, and in case 2 we even construct a longer one than the size of q. Maybe there exists a method to construct a shortest diversified FCSR with a given integer, but we have not found it yet.

Example 1. $q = -747$

We have $-747 = -2^9 - 2^7 - 2^6 - 2^5 - 2^3 - 2^2 + 1$, then $q_1 = 0$ and $s = (s_8, s_7, \ldots, s_2) = (0111011) = (011110 - 1) = (1000 - 10 - 1)$.

Let $i_0 = 8, i_1 = 4, i_2 = 2, s_{i_0} = 1, s_{i_1} = -1, s_{i_2} = -1$. Set $A = (\alpha_{i,j})_{0 \le i,j \le 8}$, $\alpha_{i,i+1} = 1$ for $0 \le i \le 7$, $\alpha_{80} = \alpha_{70} = 1$ and $\alpha_{41} = \alpha_{32} = -1$. We get

$$A = \begin{pmatrix} 0 & 1 & 0 & 0\,0\,0\,0\,0\,0 \\ 0 & 0 & 1 & 0\,0\,0\,0\,0\,0 \\ 0 & 0 & 0 & 1\,0\,0\,0\,0\,0 \\ 0 & 0 & -1 & 0\,1\,0\,0\,0\,0 \\ 0 & -1 & 0 & 0\,0\,1\,0\,0\,0 \\ 0 & 0 & 0 & 0\,0\,0\,1\,0\,0 \\ 0 & 0 & 0 & 0\,0\,0\,0\,1\,0 \\ 1 & 0 & 0 & 0\,0\,0\,0\,0\,1 \\ 1 & 0 & 0 & 0\,0\,0\,0\,0\,0 \end{pmatrix}$$

and $det(I - 2A) = -747$.

Example 2. $q = -937$

We have $-937 = -2^9 - 2^8 - 2^7 - 2^5 - 2^3 - 2 + 1$, then $q_1 = 1$ and $s = (s_8, s_7, \ldots, s_2) = (1101010)$. Let $s' = (s'_7, \ldots, s'_2) = (00 - 101010)$.

Let $i_0 = 7, i_1 = 5, i_2 = 3, s'_{i_0} = -1, s_{i_1} = 1, s_{i_2} = 1$. Set $A = (\beta_{i,j})_{0 \le i,j \le 9}$, $\beta_{i,i+1} = 1$ for $0 \le i \le 8$, $\beta_{90} = \beta_{99} = \beta_{60} = 1$ and $\beta_{51} = \beta_{42} = -1$. We get

$$A = \begin{pmatrix} 0 & 1 & 0 & 0\,0\,0\,0\,0\,0\,0 \\ 0 & 0 & 1 & 0\,0\,0\,0\,0\,0\,0 \\ 0 & 0 & 0 & 1\,0\,0\,0\,0\,0\,0 \\ 0 & 0 & 0 & 0\,1\,0\,0\,0\,0\,0 \\ 0 & 0 & -1 & 0\,0\,1\,0\,0\,0\,0 \\ 0 & -1 & 0 & 0\,0\,0\,1\,0\,0\,0 \\ 1 & 0 & 0 & 0\,0\,0\,0\,1\,0\,0 \\ 0 & 0 & 0 & 0\,0\,0\,0\,0\,1\,0 \\ 0 & 0 & 0 & 0\,0\,0\,0\,0\,0\,1 \\ 1 & 0 & 0 & 0\,0\,0\,0\,0\,0\,1 \end{pmatrix}$$

and $det(I - 2A) = -937$.

4 Conclusions

In this paper, we have given a method of constructing a diversified FCSR for hardware implementation with a given connection integer q. This construction is simple, convenient and useful for hardware oriented FCSRs. It is more efficient

than the algorithm presented in [6]. The results of this paper have solved an open problem and a conjecture came up in [6]. However, this construction can not get a shortest diversified FCSR with a given integer. Therefore, to find a method to solve this problem is still open.

References

1. Arnault, F., Berger, T.P.: F-FCSR: design of a new class of stream ciphers. In: Gilbert, H., Handschuh, H. (eds.) FSE. Lecture Notes in Computer Science, vol. 3557, pp. 83-97. Springer, New York (2005)
2. Arnault, F., Berger, T.P., Lauradoux, C.: The FCSR: primitive specification and supporting documentation. ECRYPT - Network of Excellence in Cryptology. http://www.ecrypt.eu.org/stream/ (2005)
3. Arnault, F., Berger, T.P., Lauradoux, C.: Update on F-FCSR stream cipher. ECRYPT - Network of Excellence in Cryptology. http://www.ecrypt.eu.org/stream/ (2006)
4. Arnault, F., Berger, T.P., Lauradoux, C., Minier, M., Pousse, B.: A new approach for FCSRs. In: M.J.J. Jr., Rijmen, V., Safavi-Naini, R., (eds.) Selected Areas in Cryptography. Lecture Notes in Computer Science, vol. 5867, pp. 433-448. Springer, New York (2009)
5. Arnault, F., Berger, T.P., Lauradoux, C., Minier, M.: X-FCSRa new software oriented stream cipher based upon FCSRs. In: Srinathan, K., Rangan, C.P., Yung, M. (eds.) INDOCRYPT. Lecture Notes in Computer Science, vol. 4859, pp. 341-350. Springer, New York (2007)
6. Arnault, F., Berger, Benjamin Pousse: A matrix approach for FCSR automata. In: Cryptography and Communications, Vol. 3, Num. 2, pp.109-139. Springer, New York (2010)
7. Berger, T.P., Minier, M., Pousse, B.: Software oriented stream ciphers based upon FCSRs in diversified mode. In: Roy, B.K., Sendrier, N. (eds.) INDOCRYPT. Lecture Notes in Computer Science, vol. 5922, pp. 119-135. Springer, New York (2009)
8. Goresky, M., Klapper, A.: 2-adic shift registers. In Fast Software Encryption - FSE93, volume 809 of Lecture Notes in Computer Science, pages 174-178. Springer-Verlag (1993)
9. Goresky, M., Klapper, A.: Arithmetic crosscorrelations of feedback with carry shift register sequences. IEEE Trans. Inf. Theory 43(4), 1342-1345 (1997)
10. Goresky, M., Klapper, A.: Periodicity and distribution properties of combined FCSR sequences. In: Gong, G., Helleseth, T., Song, H.Y., Yang, K., (eds.) SETA. Lecture Notes in Computer Science, vol. 4086, pp. 334-341. Springer, New York (2006)
11. Goresky, M., Klapper, A.: Fibonacci and Galois representations of feedback-with-carry shift registers. IEEE Trans. Inf. Theory 48(11), 2826-2836 (2002)
12. Hell, M., Johansson, T.: Breaking the F-FCSR-H Stream Cipher in Real Time. In: Pieprzyk, J. (ed.) ASIACRYPT. Lecture Notes in Computer Science, vol. 5350, pp. 557-569. Springer, New York (2008)
13. Joux, A., Delaunay, P.: Galois LFSR, embedded devices and side channel weaknesses. In: Progress in CryptologyINDOCRYPT 2006. Lecture Notes in Computer Science 4329, pp. 436-451. Springer, New York (2006)
14. Klapper, A., Goresky, M.: 2-adic shift registers. In: Anderson, R.J. (ed.) FSE. Lecture Notes in Computer Science, vol. 809, pp. 174-178. Springer, New York (1993)

15. Klapper, A., Goresky, M.: Large period nearly deBrujin FCSR sequences. In: Advances in CryptologyEurocrypt 1995. LNCS 921, pp. 263-273. Springer, New York (1995)
16. Stankovski, P., Hell, M., Johansson, T.: An efficient state recovery attack on X-FCSR-256. In: Dunkelman, O. (ed.) FSE. Lecture notes in computer science, vol. 5665, pp. 23-37. Springer, New York (2009)