

# Some Remarks on FCSRs and Implications for FCSR-based Stream Ciphers

Simon Fischer<sup>1</sup>, Willi Meier<sup>2</sup>, and Dirk Stegemann<sup>3</sup>

<sup>1</sup> Siemens AG, Zug (Switzerland)

<sup>2</sup> FHNW, 5210 Windisch (Switzerland)

<sup>3</sup> University of Mannheim, 68131 Mannheim (Germany)

## 1 Introduction

Feedback with carry shift registers (FCSRs) have been discussed for over ten years in the context of efficient pseudorandom number generation, particularly as an alternative to linear feedback shift registers (LFSRs) [6, 10, 11]. Similarly to LFSRs, FCSRs have an underlying algebraic structure that facilitates their analysis, and their output sequences have many desirable statistical properties [7, 9, 12–14]. Besides their direct applications as pseudorandom number generators, they have proven useful as building blocks for hardware-oriented stream ciphers [10].

A common stream cipher design principle is to use a keystream generator to produce a pseudorandom stream of running key bits  $\mathbf{z} = (z_t)_{t \geq 0}$ , which is added bitwise to the plaintext stream  $(p_t)_{t \geq 0}$  in order to obtain the ciphertext  $(c_t)_{t \geq 0}$  with  $c_t = p_t \oplus z_t$ . The receiver computes the same keystream  $\mathbf{z}$  and recovers the plaintext via  $p_t = c_t \oplus z_t$ . Many keystream generators operate as finite state machines (FSMs). Their initial state is derived from a secret key  $\mathcal{K}$  and a public initialization vector  $\text{IV}$  by a procedure named *key/IV setup*, and in each clock  $t$  the FSM outputs a piece of keystream and changes its state according to the state transition function. Particularly, the FSM of the F-FCSR stream cipher family [1, 2] computes the keystream bits by applying a Boolean filter function  $g$  to the current content of various register cells of an FCSR.

In this paper, we observe various structural properties of FCSRs and their output sequences and indicate implications for FCSR-based stream ciphers. All our results have been experimentally confirmed with the computer algebra system Magma [5]. Due to space restrictions, we omit the proofs in this extended abstract.

## 2 Feedback With Carry Shift Registers (FCSRs)

Throughout this abstract, we will denote by  $\text{wt}(d)$  the Hamming weight of a binary vector  $d$ , and we will tacitly identify a vector  $(u_0, \dots, u_{k-1}) \in \{0, 1\}^k$  with the integer  $u = \sum_{i=0}^{k-1} u_i 2^i$ .

An FCSR of length  $n$  in Fibonacci architecture contains a main register with  $n$  binary cells  $(y_0, \dots, y_{n-1})$  and fixed binary feedback taps  $(d_0, \dots, d_{n-1})$  as well as an additional  $l$ -bit memory  $b$ . From an initial state  $(y, b)$ , the FCSR outputs in each clock  $t$  the value  $y_0$ , computes the sum  $\sigma = b + \sum_{i=0}^{n-1} y_i d_{n-i-1}$  over the integers and updates the register and memory according to  $b = \sigma \text{ div } 2$  and  $y = (\sigma \text{ mod } 2, y_{n-1}, \dots, y_1)$ .

An FCSR of length  $n$  in Galois architecture contains  $n$  binary main register cells  $x_i$  with fixed binary feedback taps  $(d_0, \dots, d_{n-1})$  and  $n - 1$  memory cells  $a_0, \dots, a_{n-2}$ . Starting from an initial state  $(x, a)$ , the Galois FCSR outputs in each clock the value  $x_0$ , computes the sums  $\sigma_i = x_{i+1} + a_i d_i + x_0 d_i$  for  $0 \leq i < n$  (with  $x_n = 0$  and  $a_{n-1} = 0$ ) and updates  $x_i$  to  $\sigma_i \text{ mod } 2$  and  $a_i$  to  $\sigma_i \text{ div } 2$  for all  $0 \leq i < n - 1$ . We will assume that memory cells are only present at those positions with feedback taps, i.e.,  $a_i = 0$  if  $d_i = 0$  for all  $0 \leq i < n - 1$ .

We call an FCSR-state (and a state of a finite state machine in general) *periodic* if, left to run, the FCSR will return to that same state after a finite number of steps. We call a sequence  $\mathbf{u} = (u_i)_{i \geq 0}$  *strictly periodic* (or simply *periodic*) with period  $T$  if  $u_{i+T} = u_i$  for all  $i \geq 0$ . We call a sequence  $\mathbf{u}$  *eventually periodic* if there exists a  $t \geq 0$  such that  $\mathbf{u}' = (u_i)_{i \geq t}$  is periodic.

A 2-adic integer is a formal power series  $\alpha = \sum_{i=0}^{\infty} u_i 2^i$  with  $u_i \in \{0, 1\}$ . The collection of all such formal power series forms the ring of 2-adic numbers. This ring especially contains rational numbers  $p/q$ , where  $p$  and  $q$  are integers and  $q$  is odd. There is a one-to-one correspondence between rational numbers  $\alpha = p/q$  (with odd  $q$ ) and eventually periodic binary sequences  $\mathbf{u}$  which associates to each such rational number  $\alpha$  the bit sequence  $\mathbf{u} = (u_0, u_1, \dots)$  of its 2-adic expansion. The sequence  $\mathbf{u}$  is strictly periodic if and only if  $\alpha \leq 0$  and  $|\alpha| \leq 1$  [1].

We identify a Galois state  $(x, a)$  with the integer  $p = x + 2a$ , a Fibonacci state  $(y, b)$  with the integer  $p = b2^n - \sum_{k=0}^{n-1} \sum_{i=0}^k q_i y_{k-i} 2^k$ , and define for both architectures the connection integer  $q$  as  $q = 1 - 2d$ . Then the output of the FCSR is the 2-adic expansion of  $\alpha = \frac{p}{q}$ . Moreover, the output will be strictly periodic if and only if  $0 \leq p \leq |q|$  [1, 8]. For an initial state corresponding to  $p \in \mathbb{Z}_{|q|}$ , the sequence of integer representations of the states  $(p_t)_{t \geq 0}$  is given by  $p_t = 2^{-t}p \bmod q$  and the  $t$ -th output bit can be computed as  $z_t = p_t \bmod 2 = (2^{-t}p \bmod q) \bmod 2$ .

If  $0 < p < |q|$ ,  $q$  odd, and  $p$  and  $q$  are coprime, the period of the sequence  $(p_t)_{t \geq 0}$  is the order of 2 modulo  $q$  [1]. The period reaches its maximum  $|q| - 1$  if  $q$  is a (negative) prime for which 2 is a primitive root. We call such FCSRs *maximum-length FCSRs* and the sequences they produce *l-sequences*.

### 3 Properties of FCSRs and $l$ -sequences

#### 3.1 Sequences produced by the Galois Register Cells

The sequence  $(x_{i,t})_{t \geq 0}$  of values taken by the main register cell  $i$  of a Galois FCSR is again an FCSR-sequence, more precisely the 2-adic expansion of  $p_i/q$  with  $p_i = F_i(x, a) \cdot q + M_i \cdot p$ ,  $F_i(x, a) = \sum_{j=i}^{n-1} (x_j + 2a_j) 2^{j-i}$ , and with constants  $M_i = 2 \sum_{j=i}^{n-1} d_j 2^{j-i}$  [3]. This expression can be further simplified for periodic initial states as follows.

**Proposition 1.** *For a maximum-length Galois FCSR with connection integer  $q$ , a periodic initial state  $(x(0), a(0))$ , and  $p_0 = x(0) + 2a(0)$ , the sequence  $(x_{i,t})_{t \geq 0}$  of values taken by a fixed main register cell  $i$  corresponds to  $(p_{t+s_i} \bmod 2)_{t \geq 0}$  with  $s_i = -\log_2(M_i) \bmod q$  and  $M_i = 2 \sum_{j=i}^{n-1} d_j 2^{j-i}$ .*

Proposition 1 implies that the sequence  $(x_{i,t})_{t \geq 0}$  corresponds to the sequence produced by the whole FCSR (which is in turn equal to the sequence  $(x_{0,t})_{t \geq 0}$ ) shifted by  $s_i$  positions. Note that the phase shifts  $s_i$  are independent of the initial state  $p$  and depend on  $i$  (and  $q$ ) only.

#### 3.2 Mappings between periodic Galois and Fibonacci States

There is an onto function  $E : \{(x, a)\} - \{(1, \dots, 1; a_0, \dots, a_{n-2})\} \rightarrow \mathbb{Z}_{|q|}$  that assigns to a Galois state  $(x, a)$  the number  $E(x, a) = x + 2a \bmod q$  [8]. Moreover, there exists a one to one mapping  $S$  from  $\mathbb{Z}_{|q|}$  onto the set  $L$  of strictly periodic states of the Fibonacci FCSR with connection integer  $q$  except for the state  $(1, \dots, 1; \text{wt}(q+1) - 1)$ . For an initial state of a Galois FCSR with connection integer  $q$ , we can compute a periodic initial state of a Fibonacci FCSR with connection integer  $q$  and vice versa such that the two registers will produce the same output [8].

Obviously, the mapping  $E$  from the Galois states to  $\mathbb{Z}_{|q|}$  is not one to one, i.e., generally more than one state is mapped to the same  $p \in \mathbb{Z}_{|q|}$ . However, we can compute for a given  $p \in \mathbb{Z}_{|q|}$  the uniquely determined corresponding periodic state  $(x, a)$ , thereby providing a possible answer to the open question raised in [8] how to intrinsically characterize the periodic states corresponding to a particular  $p \in \mathbb{Z}_{|q|}$ .

**Proposition 2.** *For all  $p \in \mathbb{Z}_{|q|}$ , the only strictly periodic state  $(x, a)$  with  $x + 2a = p$  of a maximum-length Galois FCSR with connection integer  $q$  is given by  $x_i = M_i \cdot p \bmod q \bmod 2$  and  $a = (p - x)/2$  with  $M_i$  defined as in Prop. 1.*

*Remark 1.* With Prop. 2, we can define a one to one function  $\tilde{E}$  mapping periodic Galois states onto  $\mathbb{Z}_{|q|}$ . With  $\tilde{E}$  and  $S$ , we obtain a bijective mapping between periodic Fibonacci states and periodic Galois states.

### 3.3 Autocorrelations of $l$ -sequences

In order to be suitable for stream cipher applications, FCSR-sequences and in particular  $l$ -sequences should have reasonable pseudorandomness properties. One important property is the autocorrelation of the sequence. In general, we define the autocorrelation  $\theta_\tau(\mathbf{u})$  of a binary sequence  $\mathbf{u} = (u_i)_{i \geq 0}$  with shift  $\tau$  as the correlation of the sequences  $(u_i)_{i \geq 0}$  and  $(u_{i+\tau})_{i \geq 0}$ , i.e.,

$$\theta_\tau(\mathbf{u}) = \sum_{i \geq 0} (-1)^{u_i \oplus u_{i+\tau}} = |\{i : u_i \oplus u_{i+\tau} = 0\}| - |\{i : u_i \oplus u_{i+\tau} = 1\}| .$$

The expected autocorrelation of  $l$ -sequences can be shown to be zero [14]. However, how to compute the exact autocorrelation for a given shift  $\tau$  is believed to be difficult [7] and is only known for  $q = p^e$ , where  $p$  is prime and  $e \geq 2$ , and  $\tau$  of a special form [14].

Our contribution is a method for computing the autocorrelations based on counting the number of occurrences of particular  $(\tau + 1)$ -bit blocks in the sequence [4, 9].

**Proposition 3.** *Let  $\mathbf{u}$  denote an  $l$ -sequence produced by a maximum-length FCSR with prime connection integer  $q$ . Then, for a given shift  $\tau > 0$  the autocorrelation  $\theta_\tau(\mathbf{u})$  is equal to  $4B(\tau, q) - (q - 1 \bmod 2^{\tau+1})$ , where  $B(\tau, q)$  denotes the number of  $\beta \in \mathbb{Z}_{2^{\tau-1}}$  such that  $2\beta q \bmod 2^{\tau+1} > -q \bmod 2^{\tau+1}$ .*

*Remark 2.* The effort required for computing  $\theta_\tau(\mathbf{u})$  is dominated by the computation of  $B(\tau, q)$ . Currently, we do not know how to compute this value more efficiently than testing all values of  $\beta$ , which requires little memory, but  $\mathcal{O}(\tau \cdot 2^\tau)$  computations. Hence, our method is at present only efficiently applicable to small shifts  $\tau$ .

## 4 Implications for FCSR-based Stream Ciphers

The filter function of the F-FCSR stream cipher family [1, 2] computes the binary XOR of its inputs, and its initialization procedure ensures that the initial state of the generator is periodic. Hence, by Prop. 1, the keystream generation procedure is equivalent to taking the bitwise XOR-sum of different parts of the same  $l$ -sequence, while the starting position is given by the initial state. This design is motivated by the conjecture that linear and 2-adic operations are unrelated and that the correlation between two distant parts of the same  $l$ -sequence is low [1]. Based on Prop. 1, we can explicitly compute these distances for the family member F-FCSR-H and show that they are almost evenly distributed over the period of the sequence.

An alternative construction for stream cipher FSMs are combination generators which consist of a small number of feedback shift registers and a Boolean function  $f$  that combines the output sequences of the internal registers in order to produce the output keystream. Propositions 1 and 2 imply that a Galois-based filter generator like F-FCSR can be equivalently represented as a combination generator that contains as many Galois FCSRs as the filter function  $g$  has inputs, where the FCSR producing the sequence  $(x_{i,t})_{t \geq 0}$  is initialized with  $p_{s_i}$ . Furthermore, one or more Galois registers in the combination generator may be replaced by Fibonacci registers producing the same output according to Remark 1. We can also build an equivalent filter generator based on a Fibonacci FCSR with the following result, which is an immediate consequence of Props. 1 and 2.

**Corollary 1.** *The value  $x_i$  of the  $i$ -th cell in the main register of the Galois FCSR can be computed from the strictly periodic state  $(y, b)$  of the corresponding Fibonacci FCSR by  $x_i = M_i \left( b2^n - \sum_{k=0}^{n-1} \sum_{j=0}^k d_{j-1} y_{k-j} 2^k \right) \bmod q \bmod 2$  .*

## References

1. F. Arnault and T.P. Berger. Design and properties of a new pseudorandom generator based on a filtered FCSR automaton. *IEEE Trans. Comp.*, 54(11):1374–1383, 2005.
2. F. Arnault, T.P. Berger, and C. Lauradoux. Update on F-FCSR stream cipher. eSTREAM, ECRYPT Stream Cipher Project, Report 2006/025, 2006. <http://www.ecrypt.eu.org/stream>.
3. F. Arnault, T.P. Berger, and M. Minier. Some results on FCSR automata with applications to the security of FCSR-based pseudorandom generators. *IEEE Trans. Inform. Theory*, 2008.
4. L. Blum, M. Blum, and M. Shub. A simple unpredictable pseudo-random number generator. *SIAM J. Comput.*, 15(1):364–383, 1986.
5. W. Bosma, J. Cannon, and C. Playoust. The magma algebra system. i. the user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997.
6. R. Couture and P. L’Ecuyer. On the lattice structure of certain linear congruential sequences related to AWC/SWB generators. *Math. Comput.*, 62(206):799–808, 1994.
7. M. Goresky and A. Klapper. Arithmetic crosscorrelations of feedback with carry shift registers. *IEEE Trans. Inform. Theory*, 43:1342–1345, 1997.
8. M. Goresky and A. Klapper. Fibonacci and galois representations of feedback-with-carry shift registers. *IEEE Trans. Inform. Theory*, 48(11):2826–2836, 2002.
9. M. Goresky and A. Klapper. Periodicity and distribution properties of combined FCSR sequences. In G. Gong et al., editors, *Proc. of SETA 2006*, volume 4086 of *LNCS*, pages 334–341. Springer, 2006.
10. A. Klapper and M. Goresky. Feedback shift registers, 2-adic span, and combiners with memory. *Journal of Cryptology*, 10:111–147, 1997.
11. G. Marsaglia and A. Zaman. A new class of random number generators. *Annals of Appl. Prob.*, 1(3):462–480, 1992.
12. W. Qi and H. Xu. Partial period distribution of FCSR sequences. *IEEE Trans. Inform. Theory*, 49(3):761–765, 2003.
13. C. Seo, S. Lee, Y. Sung, K. Han, and S. Kim. A lower bound on the linear span of an FCSR. *IEEE Trans. Inform. Theory*, 46(2):691–693, 2000.
14. H. Xu and W.-F. Qi. Autocorrelations of maximum-length FCSR sequences. *SIAM J. Discrete Math.*, 20(3):568–577, 2006.