Some Results on FCSR Automata With Applications to the Security of FCSR-Based Pseudorandom Generators

François Arnault, Thierry P. Berger, and Marine Minier

***Abstract*—This article describes new theoretical results concerning the general behavior of a Feedback with Carry Shift Register (FCSR) automaton. They help to better understand how the initial parameters must be chosen to use this automaton as a basic block of a filtered stream cipher. These results especially concern the structure of the transition graph of an FCSR automaton and the number of iterations of the FCSR transition function required to reach the main part of the graph. A potential linear weakness and a easy way to prevent the corresponding attack are also given.**

***Index Terms*—2-adic numbers, feedback with carry shift registers, pseudo-random generator, stream ciphers, transition function graph.**

I. Background on FCSR Automata

The Feedback with Carry Shift Registers (FCSRs) were introduced first by Klapper and Goresky in [10]. In [1], T. Berger and F. Arnault proposed to use them as the core of a filtered stream cipher. We first recall how an FCSR automaton works. For more details, the reader could refer to [1], [4], and [11].

A. Representation of Eventually Periodic Binary Sequences With 2-Adic Numbers

First, we will recall briefly some basic properties of 2-adic numbers. For a more theoretical approach the reader can refer to [4], [7], [8], [10], [12].

A 2-adic integer is formally a power series $s = \sum_{n=0}^{\infty} s_n 2^n$, $s_n \in \{0, 1\}$. Such a series does not always converge in the classical sense. However, it can be considered as a formal object. Actually, this series always converges if we consider the 2-adic topology. The set of 2-adic integers is 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 $n \in \mathbb{N}$. If there exists an integer N such that $s_n = 0$ for all $n \geq N$, then s is a positive integer. Moreover, every odd integer q has an inverse in $\mathbb{Z}_2$ which can be computed by the formula $q^{-1} = \sum_{n=0}^{\infty} q'^n$, where $q = 1 - q'$.

The following theorem gives a complete characterization of eventually periodic 2-adic binary sequences in terms of 2-adic integers (see [8] for the proof).

Theorem 1: Let $S = (s_n)_{n \in \mathbb{N}}$ be a binary sequence and let $s = \sum_{n=0}^{\infty} s_n 2^n$ be the associated 2-adic integer. The sequence S is eventually periodic if and only if there exist 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 $|p| \leq |q|$.

An important fact for applications is that the period of the rational number p/q is known (cf. [8]).

Manuscript received March 12, 2007; revised October 10, 2007. This work was supported in part by the French National Agency of Research under Grant ANR-06-SETI-013.

F. Arnault and T. P. Berger are with XLIM-DMI, UMR CNRS 6172, Université de Limoges, 87060 Limoges cedex, France (e-mail: arnault@unilim.fr).

M. Minier is with CITI Laboratory, INSA de Lyon, 69621 Villeurbanne Cedex, France (e-mail: marine.minier@insa-lyon.fr).

Communicated by A. Canteaut, Associate Editor for Complexity and Cryptography.

Digital Object Identifier 10.1109/TIT.2007.913244

Theorem 2: Let S be an eventually periodic binary sequence, and let $s = p/q$, with q odd and p and q coprime, be the corresponding 2-adic number in its rational representation. The period of S is the order of 2 modulo q, i.e., the smallest integer T such that $2^T \equiv 1 (\mathrm{mod} q)$.

The period T is always less or equal to $|q| - 1$. If q is prime, then T divides $|q| - 1$. If $T = |q| - 1$, the corresponding sequence S is called a ℓ-sequence. For more details on ℓ-sequences see [10], [11].

B. FCSR Automaton in Galois Mode

Feedback with Carry Shift Registers (FCSR) automata was firstly introduced by Klapper and Goresky in [10]. This first version corresponds to the analog of LFSR in Fibonnacci mode. In [8], they introduced a Galois' version of FCSR which seems more suitable for practical implementation. In this paper, we describe only FCSR in Galois mode.

An FCSR automaton is defined using an odd negative connection integer q of binary size n : $2^n < -q < 2^{n+1}$.

Let d be the positive integer $d = (1 - q)/2$ and let $d = \sum_{i=0}^{n-1} d_i 2^i$ its binary expansion. Note that $d_{n-1} = 1$. We denote by $J = \{i : 0 \leq i \leq n - 2, d_i \neq 0\}$ the support of d but without the $n - 1$ position. If ℓ denotes the cardinality of J, we arrange J in the following way: $J = \{i_1, \ldots, i_\ell\}$, with $i_j < i_{j+1}$, $\forall j \in [1 \ldots \ell]$.

The automaton then consists of two registers:

- a main register M composed of n cells denoted by m_i $(0 \leq i \leq n - 1)$;
- a carries register C composed of ℓ cells denoted by c_{i_j} $(1 \leq j \leq \ell)$.

For simplicity, we consider that the carries register C contains n cells c_i $(0 \leq i \leq n - 1)$, with $c_i = 0$ if $d_i = 0$. However, the true size of a FCSR automaton is $n + \ell$ cells.

The transition function of the registers at time t can be written at the cell level:

$$m_i(t + 1) = m_{i+1}(t) \oplus d_i c_i(t) \oplus d_i m_0(t)$$
$$c_i(t + 1) = d_i(m_{i+1}(t)c_i(t) \oplus c_i(t)m_0(t) \oplus m_0(t)m_{i+1}(t))$$

where $\oplus$ denotes the bitwise XOR.

C. Properties of the Transition Function of a FCSR Automaton

To each state of the main register M and of the carries register C, we can associate the following integers m and c (also denoted by $m(t)$ and $c(t)$ at time t): $m = \sum_{i=0}^{n-1} m_i 2^i$ and $c = \sum_{i=0}^{n-2} c_i 2^i$. These integers are called the contents of M and C. If the main register and the carries register contain the integer $m(t)$ and $c(t)$ at time t, we say that the automaton is in state $(m(t), c(t))$. Let $p(t)$ denote the integer $m(t) + 2c(t)$.

Lemma 1: ([9]): We have $2p(t + 1) \equiv p(t) \mathrm{mod} q$.

Proposition 1: ([8]): If a FCSR automaton is in the state $(m, c) = (m(0), c(0))$ at time $t = 0$, it computes the 2-adic expansion of the rational 2-adic number p/q (where $p = m + 2c$), which is produced by the cell m_0: $p/q = \sum_{t \geq 0} m_0(t) 2^t$.

Distinct initial states can produce the same sequence.

Definition 1: Two states (m, c) and (m', c') are said equivalent if they satisfy $m + 2c = m' + 2c'$, i.e., $p = p'$.

As a direct consequence of Proposition 1, we have the following proposition.

Proposition 2: Two states (m, c) and (m', c') are equivalent if and only if they compute the same 2-adic fraction p/q, i.e., the sequences observed in the cell m_0 are equal and correspond to the 2-adic expansion of p/q, with $p = m + 2c$.

D. Structure of the Graph of a FCSR Automaton

To each binary automaton with k cells, we can associate its transition graph which is defined as follows: The nodes are the 2^k possible states. There exists an edge from a state A to a state B iff the state B is the image of A by the transition function of the automaton.

There is a bijection between the cyclotomic cosets $C_p = \{p2^i \mathrm{mod} q\}$ and the connected components of the graph of the FCSR automaton with connection integer q. A state (m, c) belongs to the component associated with C_p, where $p = m + 2c$. This is a consequence of the fact that two states are equivalent if and only if they eventually converge to a same state after the same finite number of iterations. This result will be proved in Section II-A Proposition 5.

In particular, the graph of a FCSR automaton has always two single node connected components associated with $p = 0$ and $p = -q$. They correspond to the invariant states $(0, 0)$ and $(2^n - 1, d - 2^{n-1})$ (in the latter, all the $n + \ell$ cells contain the bit value 1).

If the order of 2 modulo q is exactly $T = |q| - 1$, i.e., the automaton generates ℓ-sequences, the graph contains only one more component with $2^{n+l} - 2$ points, considered as a main cycle of length $|q| - 1$ to which many tails converge (see [1], for more details).

Definition 2: We say that a FCSR automaton with connection integer q is optimal if the order of 2 modulo q is exactly $T = |q| - 1$.

In Section II-B, we will bound the lengths of the tails in the graph of any FCSR automaton.

E. Sequences Produced by the Main Register of a FCSR

Now we will look at the sequences of bits produced by the cells of the main register. These sequences are denoted $M_i = (m_i(t))_{t\in\mathbb{N}}$, for $0 \le i \le n - 1$. The following theorem was proved in [4].

Theorem 3: ([4]): Consider a FCSR automaton with negative connection integer $q = 1 - 2d$. Let n be the bitlength of d. Then, for all i such that $0 \le i \le n - 1$, there exists an integer p_i such that the sequence M_i observed in the cell number i of the main register is the 2-adic expansion of p_i/q. Moreover, the integers p_i satisfy the following recurrence relation:

$$p_i = q\Big(m_i(0) + 2c_i(0)\Big) + 2p_{i+1} + 2d_i p_0$$

with the convention $c_i(t) = 0$ when $d_i = 0$.

From now, we will use the following notations.

- Content of a cell (cell level): $m_i = m_i(0), c_i = c_i(0)$.
- Content of a whole register (integer level): $m = m(0), c = c(0)$.
- Observed sequences, in a specific cell of the main register, from time t_0: $M_i(t_0) = (m_i(t))_{t\ge t_0}$ for $0 \le i \le n - 1$.
  In particular $M_i(0) = M_i$ for $0 \le i \le n - 1$.
- The 2-adic fractions corresponding to these sequences: $M_i(t_0) = p_i(t_0)/q$, i.e., $p_i(t_0)$ is the integer satisfying the relation: $p_i(t_0) = q \times \sum_{t\ge t_0} m_i(t)2^i$.

Note that $p_i = p_i(0)$ for $0 \le i \le n - 1$ and $p = p_0 = p_0(0)$.

F. Some Properties of 2-Adic Rational Numbers

We present in this section some elementary properties of the 2-adic sequences, required to demonstrate results of the next section. These results are relatively simple and essentially known (see [7], [10], [11] for further details).

First, we introduce the following notations:

- $A_q = \{p/q | 0 \le p \le -q\}$ the set of the 2-adic periodic sequences with a denominator equal to q: $2^n < -q < 2^{n+1}$.
- $A_q^* = \{p/q | 0 < p < -q\}$ and $p/q = \sum_{i=0}^{\infty} a_i 2^i$
- $\mathbb{N}_k = \{0, 1, \cdots, 2^k - 1\} = \{\sum_{i=0}^{k-1} a_i 2^i, a_i = 0 \mathrm{or} 1\}$

Proposition 3: Remember that $2^n < -q \le 2^{n+1}$. We have the following properties:

- The map f_n from A_q^* to $\mathbb{N}_n$ defined by $f_n(p/q) = p/q \mathrm{mod} 2^n$ is surjective.
- The map f_{n+1} from A_q to $\mathbb{N}_{n+1}$ defined by $f_n(p/q) = p/q \mathrm{mod} 2^{n+1}$ is injective.

Corollary 1: For any odd q satisfying $2^n < -q \le 2^{n+1}$ and any $p, 0 < p < |q|$, there is no sequence of $n + 1$ consecutive zeros and there is no sequence of $n + 1$ consecutive ones in the 2-adic expansion of p/q.

Corollary 2: If the order of 2 modulo q is maximal (i.e., equals to $-q - 1$), then the 2^n sequences with n consecutive bits appear at least one time and at most two times in a period of the binary expansion of any $p/q \in A_q^*$.

Corollary 3: If the order of 2 modulo q is maximal (i.e., equals to $-q - 1$) and if $p/q \in A_q^*$, then the subsequence with n consecutive bits all equal to 0 (respectively, all equal to 1) appears one and only one time in the period of the binary expansion of p/q.

II. New Results on FCSR Automata

We present in this section some important results concerning the number of transitions necessary to reach a cycle (the cycle when we consider an optimal FCSR) and the entropy of a FCSR automaton. Indeed, while the total number of states of an FCSR automaton is $2^{n+\ell}$, a cycle is composed of T states (where T is the order of 2 modulo q). The other states are distributed on tails or trees which converge quickly to this cycle. Thus, we want to determine an upper bound on the lengths of tails that are attached to a cycle (or the cycle).

In the case of an optimal FCSR (that could be used in a stream cipher construction), the cycle is composed of $|q| - 1$ states (with always $2^n \le |q| - 1 < 2^{n+1}$). To guarantee some properties of FCSR based stream ciphers, we do not want the optimal FCSR to output pseudorandom data before it has reached the cycle.

A. Explicit Determination of Sequences M_i

In this paragraph, we will determine the exact values of each p_i (or $p_i(t)$) defined in Theorem 3. We always suppose that the initial state of the automaton is not a fixed point of the transition function, i.e., $0 < p < |q|$.

To simplify the presentation, we suppose from now that $t_0 = 0$ without loss of generality. We also need to introduce the following notations, for $0 \le i \le n - 1$:

$$d^{(i)} = \sum_{j=0}^{i-1} d_j 2^j, \delta^{(i)} = \sum_{j=i}^{n-1} d_j 2^{j-i}$$

so that $d = d^{(i)} + 2^i \delta^{(i)}$

$$u^{(i)} = \sum_{j=0}^{i-1} (m_j + 2c_j)2^j, \nu^{(i)} = \sum_{j=i}^{n-1} (m_j + 2c_j)2^{j-i}$$

so that $p = u^{(i)} + 2^i \nu^{(i)}$.

Proposition 4: With the above notations, we have the following relation:

$$p_i = q\nu^{(i)} + 2p\delta^{(i)}. \quad (1)$$

Proof: We perform the proof by induction on i. For $i = 0$ we have $p_0 = p, \delta^{(0)} = d$, and $\nu^{(0)} = p$. Hence, $q\nu^{(0)} + 2p\delta^{(0)} = p(q + 2d) = p = p_0$.

Suppose now that the relation (1) is true for i. Let us prove that the relation stays true at step $i+1$. From Theorem 3, we have $p_i = q(m_i(0)+$

$2c_i(0)) + 2p_{i+1} + 2d_ip_0$. We also can write $\delta^{(i)} = d_i + 2\delta^{(i+1)}$ and $\nu^{(i)} = m_i + 2c_i + 2\nu^{(i+1)}$. Using the induction hypothesis, we obtain

$$q\nu^{(i)} + 2p\delta^{(i)} = p_i = q(m_i(0) + 2c_i(0)) + 2p_{i+1} + 2d_ip$$
$$= q(\nu^{(i)} - 2\nu^{(i+1)}) + 2p_{i+1} + 2(\delta^{(i)} - 2\delta^{(i+1)})p.$$

Canceling $q\nu^{(i)}$ and $2p\delta^{(i)}$ on both sides we obtain $2p_{i+1} = 2q\nu^{(i+1)} + 4p\delta^{(i+1)}$. This is the relation (1) for $i+1$: $p_{i+1} = q\nu^{(i+1)} + 2p\delta^{(i+1)}$ and this concludes our proof. □

Corollary 4: Assume that (m, c) and (m', c') are two equivalent states, and that p_i/q and p_i'/q are the respective fractions whose expansion is given by the cells m_i and m_i'. Then we have $p_i \equiv p_i' \bmod q$. Moreover, if (m', c') is in a cycle, then $0 \leq p_i' < |q|$.

Proof: By Proposition 2, the result is true for the special case $i = 0$. By Proposition 4, we have $p_i \equiv 2p\delta^{(i)}$ and $p_i' \equiv 2p'\delta^{(i)}$ modulo q for any i. We obtain $p_i' \equiv 2p'\delta^{(i)} = 2p\delta^{(i)} \equiv p_i$ modulo q, and this is the first claim. If (m', c') is in a cycle then the sequence p_i/q is periodic so we have $0 \leq p_i' < q$ from Theorem 1. This proves the second claim. □

The following proposition revisits the notion of equivalent states in view of the transition function. The proof given here concerns the general (optimal or not) case.

Proposition 5: Two states are equivalent if and only if they eventually converge to a same state after the same number of iterations.

Proof: Assume that the states (m, c) and (m', c') are equivalent. There exists a positive integer k such that the states obtained by applying k times the transition function to the initial states produce the same state on a cycle. At this point, for each i, from Definition 3, the sequences $(m_i(t))_{t\geq k}$ and $(m_i'(t))_{t\geq k}$ are both periodic. By Theorem 1, we obtain $0 \leq p_i(k) < -q$ and $0 \leq p_i'(k) < -q$. By Corollary 4, we have $p_i(k) \equiv p_i'(k)$ modulo q, so $p_i(k) = p_i'(k)$ for each i. Using that $m(k) + 2c(k) = p(k) = p'(k) = m'(k) + 2c'(k)$, we see that $c(k) = c'(k)$ also. Hence, the two states reached at step k are equal.

The converse is easy, using Lemma 1. □

B. Maximum Length of the Tails of the FCSR Graph

The properties described above are useful to compute the number of transitions required to reach a cycle. Consider a FCSR automaton with connection integer q. We say that the automaton is synchronized if it has reached a state on a cycle. We consider here each binary sequence M_i of the main register.

Definition 3: We say that the cell m_i is synchronized at time t if the sequence of the $(m_i(t + j))_{j\geq 0}$ values is periodic, i.e., $m_i(t + j) = m_i(t + j + T), \forall j \geq 0$, for some period $T > 0$.

Lemma 2: The state (m, c) belongs to a cycle if and only if all the cells of the main register are synchronized.

Proof: Assume that all cells of the main register are synchronized. By Proposition 5, The state (m, c) is equivalent to a state (m', c') which belongs to a cycle. Starting from this state (m', c'), the content of each cell of the main register is a sequence $M_i' = (m_i'(t))_{t\geq 0}$. The values $M_i(t)$ and $M_i'(t)$ are equal as soon as t is large enough. But the sequences M_i and M_i' are both periodic so $M_i(t)$ and $M_i'(t)$ are equal for all $t \geq 0$. As a consequence, we obtain $m = m'$. As $m + 2c = m' + 2c'$, we obtain also $c = c'$. This shows that the state (m, c) belongs to a cycle. The converse is clear. □

Proposition 6: The cell m_i is synchronized at time t if and only if we have $0 < p_i(t) < |q|$.

Proof: The cell m_i is synchronized at time t if and only if the sequence $M_i(t)$ is periodic, which is equivalent to $0 < p_i(t) < |q|$ (cf. Theorem 1). □

Lemma 3: Adding or subtracting a positive integer $b = \sum_{i=0}^{m-1} b_i 2^i$ of bit length m to the 2-adic fraction p/q when $0 < p < |q|$ affects at most the $m + n + 1$ first bits.

Proof: Consider the addition case. Denote $(r(t))_{t\geq 0}$ the 2-adic expansion of the fraction p/q. By Corollary 1, there is at least one integer k such that $m \leq k \leq m + n$ with $r(k) = 0$. Adding 2^k to p/q would change the bit $r(k)$ and leave the other terms of the sequence unchanged. But $b < 2^m \leq 2^k$. So that, adding b changes only some bits of lower weight $r(j)$ with $j \leq k$. The subtraction case is similar. □

Hence, a bound on the number of iterations required for each cell to synchronize, will provide a general bound for the synchronization of the whole automaton.

Lemma 4: $\forall i$ such that $0 \leq i \leq n-1$, we have: $6q < p_i < -8q$.

Proof: For $i = 0$, we have $0 \leq p_0 = p < -q$ so the claim is true in that case. Assume now that $i > 0$. From the definitions given above, we have

$$0 \leq \delta^{(i)} < 2^{n-i}, \quad 0 \leq d^{(i)} < 2^i,$$
$$0 \leq \nu^{(i)} < 3 \times 2^{n-i}, \quad 0 \leq u^{(i)} < 3 \times 2^i.$$

By Proposition 4, we have $p_i = \nu^{(i)} - 2\nu^{(i)}d^{(i)} + 2u^{(i)}\delta^{(i)}$. Using the above inequalities, we get

$$-3 \times 2^{n+1} < -2\nu^{(i)}d^{(i)} \leq p_i$$
$$\leq \nu^{(i)} + 2u^{(i)}\delta^{(i)} < 3 \times (2^{n+1} + 2^{n-1}).$$

But, $2^n \leq -q \leq 2^{n+1}$. We finally obtain $6q < p_i < -8q$. □

The main result of this section is the following theorem.

Theorem 4: Suppose that a FCSR automaton with connection integer q starts from the state (m, c). Then it will be synchronized after at most $n+4$ iterations (n denotes the length of the main register). More generally, the lengths of the tails of the graph of a FCSR automaton are at most $n + 4$.

Proof: There exists a state (m', c') which is equivalent to (m, c) and belongs to a cycle. As the sequence of bits obtained in the cell m_i is periodic, we have $0 < p_i' < |q|$. From Corollary 4, we have $p_i' \equiv p_i$ modulo q for each i such that $0 \leq i \leq n-1$. Also, from Lemma 4, we have $6q < p_i < -8q$. Hence $p_i = p_i' + b_iq$ for small integers b_i satisfying $-7 \leq b_i \leq 6$. The integers $|b_i|$ have a bit length at most 3, so the theorem follows finally from Lemma 3. □

We have performed an experimentation summed up in Fig. 1. We have computed for 100 000 random initial values the number of iterations required to reach the cycle for three different q optimal values. We observe that this number of iterations is with high probability well below the bound given in Theorem 4. Thus, the convergence toward the cycle in case of an optimal FCSR is very fast.

This is not surprising. The bound $n + 4$ provided by the Theorem relies on the time to find a zero (or a one) in a particular sequence, and Corollary 1 was used to bound this time to $n + 1$. However, if we consider this sequence as Bernouilli trials, we can expect that the average position of the first 0 is 2. So synchronization is expected to occur after the first 6 steps, for most cells. Moreover, the register is synchronized as soon as all of its cells are. Using further the hypothesis of Bernouilli trials, we can expect that when the size of the register doubles, the synchronization time is increased by 1. This is in accordance with the results of Fig. 1, which shows that the size of q does not mainly influence the time required for the synchronization process.

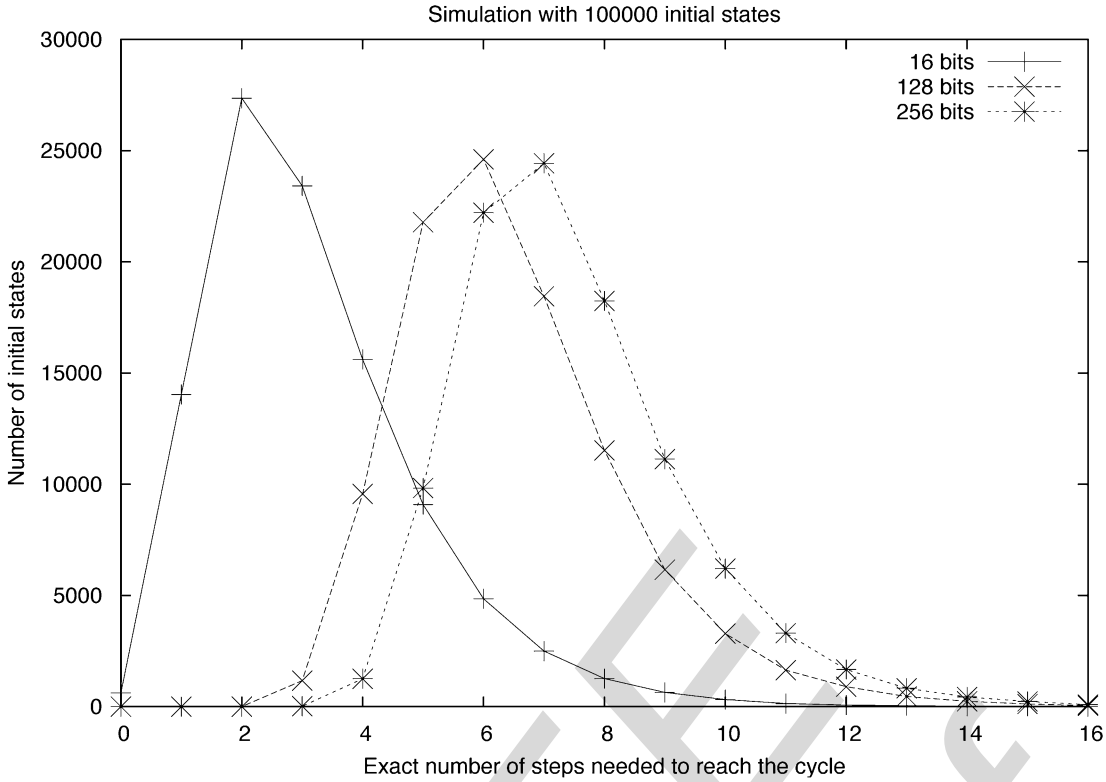

Fig. 1. Number of initial states in function of the exact number of transitions they need to reach the cycle. Three simulations have been done using 100 000 random initializations and with three register sizes: 16, 128, and 256 bits.

III. A Potential Attack on F-FCSR Pseudorandom Generators

A. Review on F-FCSR Pseudorandom Generators

A simple way to construct a pseudorandom generator using FCSRs is to filter the cells of its main register with some boolean functions. If the parameters of the FCSR automaton are correctly chosen, its natural nonlinear behavior makes algebraic attacks infeasible [1], [4].

So, it is not necessary to use a Boolean function with a high nonlinearity. A simple linear function could be used to filter the content of the FCSR main register. This choice appears to be well suited for two main reasons: these functions have an optimal resilience order and offer better resistance to correlation attacks. Moreover, they are efficient and easy to implement for hardware and software applications.

The family of F-FCSR generators (see [1], [2], [4], [5] for example) uses this model: at each iteration t, the bit (or byte in some cases) of output keystream $z(t)$ is obtained by filtering the content of the main register of an optimal FCSR using a linear function.

B. Linear Weakness of a FCSR Automaton

The potential weakness described here addresses degenerate behavior of the FCSR automaton which can occur when the transition function of the FCSR is linear. This happens when all the cells of the carries register contain a 0 bit and, at the same time, the feedback bit m_0 is also 0. In this case, the transition function becomes a simple circular permutation of the contents of the cells of the main register

$$m_i(t+1) = m_{(i+1 \bmod n)}(t), \quad \forall i, 0 \leq i \leq n-1.$$

Suppose that this situation occurs during r consecutive transitions of the FCSR from time t_0. Since a F-FCSR generator filters the FCSR main register using a linear function, the output corresponding to these r iterations linearly depends on the values $m_i(t_0)$ contained in the cells of the main register. Clearly, this fact could be used to design a fast attack. For example, the F-FCSR-16 generator outputs 16 bits at each iteration and the size of the main register contains 256 cells. If $r = 16$, then the linear behavior would allow a system of 256 linear equations in 256 unknowns to be written down. It would be easy to solve this system to recover the complete state of the main register at time t_0, assuming that the 256 linear equations are linearly independent (if they are not, the partial information retrieved is likely to be sufficient to break the generator by an exhaustive search on the space of the remaining possible states).

Let us estimate the *a priori* probability of such a linear behavior to occur. For that purpose, the following lemma is helpful.

Lemma 5: The two conditions follow:
1) carries register is 0 and the first r bits of $p_0(t)/q$ are 0;
2) carries register is 0 and $m_i(t) = 0$ for all $i, 0 \leq i < r$

are equivalent.

Proof: If Condition 2 holds, then the transition function is linear during r steps. Hence $m_i(t+1) = m_{i+1}(t)$ and then $m_0(t+i) = m_i(t)$ so that the r first bits of $p_0(t)/q$ are 0. The converse is also true since the first r bits of $p_0(t)/q$ are the $m_0(t+i)$ for $0 \leq i < r$.

The number of states corresponding to the event $c(t) = 0$ and $m_i(t) = 0$ for all $i, 0 \leq i < r$ is 2^{n-r}. Since the total number of states of the automaton is $2^{n+\ell}$, the expected probability of the event equals to $2^{-(\ell+r)}$. As an example, for the stream cipher F-FCSR-16, the chosen parameters were $n = 256$, $\ell = 130$ and $r = 16$, and we obtain an *a priori* probability for that event of 2^{-146}.

C. How to Definitively Avoid This Weakness

Using the following proposition, we have a simple argument to show that this weakness is very easily prevented.

Proposition 7: Let s be the least integer such that $d_s = 1$. Assume that $m_i = c_i = 0$ for all i such that $0 \leq i \leq s$. Then the current state of the automaton is not on the cycle.

Proof: We have $d^{(s+1)} = 2^s$, $u^{(s+1)} = 0$ and $v^{(s+1)} = p/2^{s+1}$. Also, $q = 1 - 2d = 1 - 2(d^{(s+1)} + 2^{s+1}\delta^{(s+1)}) = 1 - 2d^{(s+1)} - 2^{s+2}\delta^{(s+1)}$. Hence $q + 2^{s+2}\delta^{(s+1)} = 1 - 2d^{(s+1)} = 1 - 2^{s+1} < 0$. From Proposition 4, we get $p_{s+1} = qv^{(s+1)} + 2p\delta^{(s+1)} = qp/2^{s+1} + 2p\delta^{(s+1)}p_{s+1} = p/2^{s+1}\left(q + 2^{s+2}\delta^{(s+1)}\right) < 0$. From Proposition 6, the current state of the automaton is not on the cycle. □

Consequently, suppose that a FCSR automaton is clocked more than $n+4$ iterations before output is used. If the number r of required equations is greater than s, the situation described in Section III-B cannot occur. This is the case for F-FCSR-16 and F-FCSR-H, the candidates to the second eSTREAM phase for the Profile 2. In these ciphers, the automaton is clocked enough times at each change of IV for the resulting state to be on the cycle. Moreover, $s = 2$ in both cases, and the linear behavior of the automaton cannot occur during more than two consecutive steps.

IV. Conclusion

In this correspondence, we have given more precise results concerning the general behavior of FCSR automata especially optimal ones. Our main result concerns the number of iterations required to reach a cycle which is bounded by $n + 4$ where n represents the bit length of the main register.

In view of the results proved here, we provide some hints in the secure design of pseudorandom generators using an optimal FCSR automaton as a component. First of all, the minimal entropy of an optimal FCSR corresponds to a space of $|q| - 1$ states (with $2^n \leq |q| - 1 < 2^{n+1}$) and is obtained when the automaton has reached a state on the cycle. This is guaranteed after only $n + 4$ iterations. We thus obtain an upper bound on the number of initial transitions needed before output can be used. Moreover, we could initialize a FCSR with $c(0) = 0$ to prevent two equivalent initial states resulting from different keys. In this case, the initial entropy is exactly set to n bits, and it does not decrease when the transition function is applied.

We also described a potential weakness of FCSR based pseudorandom generators, which should occur if the transition function is linear during several consecutive iterations. However, we show that such a bad behavior cannot occur if the setup method used before extracting data is well designed. The trick to use here is to clock the automaton $n + 4$ times before to output any data.

Acknowledgment

The authors would like to thank the anonymous referees for their helpful comments, remarks, and suggestions.

References

[1] F. Arnault and T. P. Berger, "F-FCSR: Design of a new class of stream ciphers," *Fast Software Encryption - FSE 2005*, ser. Lecture Notes in Computer Science, vol. 3557, pp. 83–97, 2005, Berlin, Germany: Springer-Verlag.

[2] F. Arnault, T. P. Berger, and C. Lauradoux, Preventing weaknesses on F-FCSR in IV mode and tradeoff attack on F-FCSR-8. ECRYPT—Stream Cipher Project Report 2005/075, 2005 [Online]. Available: http://www.ecrypt.eu.org/stream/

[3] F. Arnault, T. P. Berger, and C. Lauradoux, Update on F-FCSR stream cipher. ECRYPT - Network of Excellence in Cryptology, Call for stream Cipher Primitives - Phase 2 2006 [Online]. Available: http://www.ecrypt.eu.org/stream/

[4] F. Arnault and T. P. Berger, "Design and properties of a new pseudorandom generator based on a filtered FCSR automaton," *IEEE Trans. Comput.*, vol. 54, no. 11, pp. 1374–1383, Nov. 2005.

[5] ***[Please provide location--ED.]*** T. Berger and F. Arnault, "Design of new pseudorandom generators based on filtered FCSR automaton," in *Proc. ECRYPT Network of Excellence - SASC Workshop Record*, 2004, pp. 109–120.

[6] T. P. Berger and M. Minier, , S. Maitra, C. E. Veni Madhavan, and R. Venkatesan, Eds., "Two algebraic attacks against the F-FCSRs using the IV mode," in *Progress in Cryptology - INDOCRYPT 2005*. New York: Springer-Verlag, 2005, vol. 3797, pp. 143–154, Lecture Notes in Computer Science.

[7] M. Goresky and A. Klapper, "Arithmetic crosscorrelations of feedback with carry shift register sequences," *IEEE Trans. Inf. Theory*, vol. 43, no. 4, pp. 1342–1345, Jul. 1997.

[8] M. Goresky and A. Klapper, "Fibonacci and Galois representations of feedback-with-carry shift registers," *IEEE Trans. Inf. Theory*, vol. 48, no. 11, pp. 2826–2836, Nov. 2002.

[9] E. Jaulmes and F. Muller, "Cryptanalysis of the F-FSCR stream cipher family," in *Proc. 12th Annu. Worksh. Sel. Areas Cryptogr.*, 2005, vol. 3897, Lecture Notes in Computer Science, pp. 20–35, Berlin, Germany: Springer-Verlag.

[10] A. Klapper and M. Goresky, "2-adic shift registers," *Fast Software Encryption - FSE'93*, ser. Lecture Notes in Computer Science, vol. 809, pp. 174–178, 1993, Berlin, Germany: Springer-Verlag.

[11] A. Klapper and M. Goresky, "Feedback shift registers, 2-adic span, and combiners with memory," *J. Crypt.*, vol. 10, pp. 111–147, 1997.

[12] N. Koblitz, *P-Adic Numbers, P-Adic Analysis and Zeta-Functions*. New York: Springer-Verlag, 1997.

François Arnault received the Ph.D. degree in mathematics from the University of Poitiers, France, in 1993.

In 1994, he joined the University of Limoges, France, as an Assistant Professor, and joined a team working on arithmetic, coding theory and cryptography. His research interests include cryptography, algorithmic number theory, and primality.

Thierry P. Berger received the Ph.D. degree and the French Habilitation (Mathematics) from the University of Limoges, France.

From 1992, he has been with the University of Limoges, where he is currently Professor in the Department of Mathematics. He is the Scientific Head of the Coding and Cryptography group of this department. His research interests include finite algebra, automorphism group of codes, links between coding and cryptography, stream cipher, and pseudorandom generators.

Marine Minier received the Ph.D. degree from the University of Limoges, France, in 2002.

In 2005, she joined the INSA de Lyon (Institut National des Sciences Appliques), as an Assistant Professor, in the CITI Laboratory, a team working in telecommunications. Her research interests include symmetric key cryptography, and security in sensor networks and in ambient networks.