Published in *SASC 2007 - Stream Ciphers Revisited, February 2007*
Special Workshop hosted by the ECRYPT Network of Excellence

On 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 an FCSR automaton that allow to better understand the initial parameters that must be chosen to use this automaton as a basic block of a filtering stream cipher. The results demonstrated here especially concern the structure of the subjacent graph of an FCSR automaton, its entropy and the number of iterations of the FCSR transition function required to reach the main part of the graph. A linear weakness and a way to discard the induced potential attack are also given. The parameters chosen for the two candidates F-FCSR-16 and F-FCSR-H make this attack impossible.

Keywords: Stream ciphers, FCSR, 2-adic expansion, transition function graph.

1 Background on FCSR automata

The Feedback with Carry Shift Registers 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].

1.1 FCSR Automaton

Definition of an FCSR automaton

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

Let d be the positive integer $d = (1-q)/2$ and $d = \sum_{i=0}^{n-1} d_i 2^i$ 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 except for the $n-1$ position. If ℓ denotes the cardinal of J, we arrange J in the following way: $J = \{i_1, \ldots, i_\ell\}$, with $i_j < i_{j+1},\ \forall j \in [1..\ell]$.

The automaton is then constituted of two registers:

* XLIM-DMI, UMR CNRS 6171, Université de Limoges, 123 avenue A. Thomas, 87060, Limoges cedex, France arnault@unilim.fr thierry.berger@unilim.fr
** CITI laboratory, INSA de Lyon, 21 Avenue Jean Capelle, F-69621 Villeurbanne Cedex, France marine.minier@insa-lyon.fr

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

For simplicity, we consider that the carry 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 $n + \ell$.

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

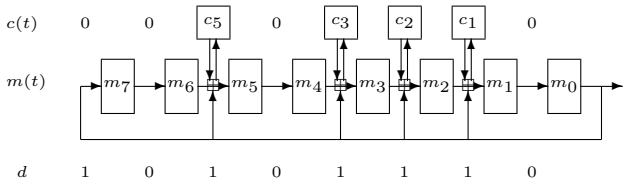
$$m_i(t+1) = m_{i+1}(t) \oplus d_i c_i(t) \oplus d_i m_0(t)$$
$$c_i(t+1) = d_i \left(m_{i+1}(t)c_i(t) \oplus c_i(t)m_0(t) \oplus m_0(t)m_{i+1}(t)\right)$$

where $\oplus$ denotes the bitwise XOR.

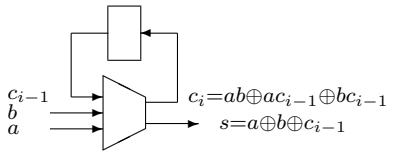
Hardware description of a FCSR automaton

A FCSR automaton can be easily realized for hardware applications. Its circuit is close to those of FCSR's in Galois mode. More details can be found in [6, 1, 4]. We give a simple example of such hardware circuit:

Example 1. $q = -347$, so $d = 174 = 0\text{xAE}$, $k = 8$ and $\ell = 4$



where the symbol $\boxplus$ denotes the addition with carry, i.e., it corresponds to the following scheme:



1.2 Properties of the transition function of a FCSR automaton

To each state of the main register M and of the carry register C, we could 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.

Published in *SASC 2007 - Stream Ciphers Revisited, February 2007*
Special Workshop hosted by the ECRYPT Network of Excellence

If the main register and the carry 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 $m(t) + 2c(t)$.

It is easy to prove that the integers $p(t)$ satisfy the following recurring relation: $p(t+1) = \frac{p(t)-qm_0(t)}{2}$.

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 $p = p(0) = m + 2c$), which is produced by the cell m_0:
$p/q = \sum_{t \geq 0} m_0(t) 2^t$.

The 2-adic expansion of the rational number p/q is essentially the division of p by q following the increasing powers of 2. The reader can refer to [4, 7, 8, 10, 12] for more details.

The most important result, for our application, about 2-adic rational numbers is the following:

Theorem 1. *Let S be an eventually periodic binary sequence, and $s = p/q$, with q odd and p and q coprime, be the corresponding 2-adic number in its rational representation. The periode of S is the order of 2 modulo q, i.e., the smallest integer t such that $2^t \equiv 1 \pmod{q}$. Moreover, if $0 \leq p \leq -q$, the sequence is periodic.*

Definition 1. *We say that an FCSR automaton with connection integer q is optimal if the order of 2 modulo q is exactly $T = |q| - 1$. Note that the connection integer of an optimal FCSR automaton is always a prime number.*

1.3 Structure of the graph of an optimal FCSR automaton

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

The graph of a FCSR automaton contains always two fixed points: the corresponding values of (m, c) for these states are $(0, 0)$ and $(2^n - 1, d - 2^{n-1})$ respectively, corresponding to the development of the 2-adic fractions $0 = 0/q$ and $-1 = |q|/q$.

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

Proposition 1. *Two states are equivalent if and only if they eventually converge to a same state after the same number of iterations.*

If the FCSR automaton is optimal, the graph of the transition function is composed of exactly three connected components: the two single point components corresponding to the two fixed points and a component containing all the $2^{n+l} - 2$ remaining points, composed itself of a main cycle of size $|q| - 1$ and of tails or trees converging to this cycle. More details concerning such a graph and some simple examples could be found in [4].

In the case of an optimal FCSR automaton, Proposition 1 could then be reformulated as follows:

Proposition 2. *Two non-invariant states of an optimal FCSR automaton are equivalent if and only if they eventually converge to the same state of the main cycle in the same number of steps.*

1.4 Sequences produced by the main register of a FCSR

Now we will look at the sequences of values taken by the binary cells of the main register, that could be written: $M_i = (m_i(t))_{t\in\mathbb{N}}$, for $0 \leq i \leq n-1$, the sequence of binary memories for a particular i. The following theorem was proved in [4].

Theorem 2. *[4] Consider an FCSR automaton with negative connection integer $q = 1 - 2d$. Let n be the bitlength of d. Then, for all i such that $0 \leq i \leq n-1$, 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 relations:*

$$p_i = qm_i(0) + 2p_{i+1} \text{ if } d_i = 0,$$
$$p_i = q(m_i(0) + 2c_i(0)) + 2p_{i+1} + 2p_0 \text{ if } d_i = 0.$$

Putting $c_i(t) = 0$ when $d_i = 0$, both cases can be written $p_i = q\big(m_i(0) + 2c_i(0)\big) + 2p_{i+1} + 2d_ip_0$.

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: $M_i(t_0) = (m_i(t))_{t\geq t_0}$ for $0 \leq i \leq n-1$. In particular $M_i(0) = M_i$ for $0 \leq i \leq n-1$.

– 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:

$$p_i(t_0) = q \times \sum_{t \geq t_0} m_i(t) 2^i.$$

We also have: $p_i = p_i(0)$ for $0 \leq i \leq n-1$ and $p = p_0 = p_0(0)$.

1.5 Some properties of 2-adic rational numbers

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

First, we introduce the following notations:

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

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

– *the f_n map that associates p/q to $p/q \bmod 2^n$ is a surjection from A_q^* in $\mathbb{N}_n$.*
– *the f_{n+1} map that associates p/q to $p/q \bmod 2^{n+1}$ is an injection from A_q in $\mathbb{N}_{n+1}$.*

Corollary 1. *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 periode of the binary expansion of any $p/q \in A_q^*$.*

Corollary 2. *If the order of 2 modulo q is maximal (i.e. equals to $-q-1$) and if $p/q \in A_q^*$, then the sequences with n consecutive bits all equal to 0 (resp. all equal to 1) appear one and only one time in the periode of the binary expansion of any $p/q \in A_q^*$. Moreover, there is no sequence composed of $n+1$ consecutive 0s nor 1s in such an expansion.*

2 New results on FCSR automata

We present in this section some important results concerning the number of transitions necessary to reach the main cycle and the entropy of an

optimal FCSR automaton. Indeed, even if the number of possible states of an FCSR automaton is $2^{n+\ell}$, the main cycle is composed of $|q|-1$ states when the FCSR is optimal (with always $2^n \leq |q|-1 < 2^{n+1}$). The other states are distributed on tails or trees which converge quickly to the main cycle. To guarantee some properties of FCSR based stream ciphers, we don't want the FCSR to output pseudorandom data before it has reached the main cycle. Thus, we want to determine an upper bound on the length of tails that are attached to the main cycle.

2.1 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 2. 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 $0 \leq i \leq n-1$:

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

$$u^{(i)} = \sum_{j=0}^{i-1} (m_j + 2c_j) 2^j, \quad \nu^{(i)} = \sum_{j=i}^{n-1} (m_j + 2c_j) 2^{j-i}, \quad \text{so that } p = u^{(i)} + 2^i \nu^{(i)}.$$

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

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

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 2, we have $p_i = q(m_i(0) + 2c_i(0)) + 2p_{i+1} + 2d_i p_0$. 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:

$$\begin{aligned} q\nu^{(i)} + 2p\delta^{(i)} = p_i &= q(m_i(0) + 2c_i(0)) + 2p_{i+1} + 2d_i p \\ &= q(\nu^{(i)} - 2\nu^{(i+1)}) + 2p_{i+1} + 2(\delta^{(i)} - 2\delta^{(i+1)})p. \end{aligned}$$

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

2.2 Maximum length of the tails of the FCSR graph

All the properties described above are essential to compute the number of transitions required to reach the main cycle in the case of an optimal FCSR (or a final cycle otherwise). If we consider the optimal FCSR automaton with connection integer q, we say that the automaton is synchronized if it has reached a state on the main cycle. We consider here each binary sequence M_i of the main register. 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 periode $T > 0$.

Proposition 5. *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). □

Corollary 3. *Adding or substracting a positive integer $b = \sum_{i=0}^{m} b_i 2^i$ to the 2-adic fraction p/q affects at most the $m+n$ first bits.*

Proof. In the one hand, in the addition case, the carry is propagated by the 1 and stopped at the first met 0. For the subtraction case, the inverse case occurs. In the other hand, from Corollary 2, we have demonstrated that the maximal length of consecutive bits all at 0 or all at 1 is n. This fact concludes our proof. □

Then, 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 1. *$\forall i$ such as $0 \leq i \leq n-1$, we have: $6q < p_i < -8q$.*

Corollary 4. *for all i such as $0 \leq i \leq n-1$, if p_i is written $p_i = bq + p'$ with $0 < p' < |q|$ then the binary expression of $|b|$ is composed of at most 3 bits: $|b| = b_0 + 2b_1 + 4b_2$.*

The main result of this Section is the following theorem:

Theorem 3. *Suppose that an optimal FCSR automaton of connection integer q is in state (m, c) at time t, then it will be synchronized after at most $n+3$ iterations (n denotes the length of the main register). More generally, the length of the tails of the graph of an optimal FCSR automaton is at most $n+3$.*

Proof. From Lemma 1, at time t, for all i, we have $6q < p_i(t) < -8q$. Suppose that there exists $p'_i(t)$ such as $p'_i(t) = p_i(t) \mod q$. The corresponding cell m'_i will be synchronized after j steps if $p'_i(t+j)/q = p_i(t+j)/q$. From Corollary 4, we have $p_i(t) = bq + p'_i(t)$ with $0 < p'_i(t) < |q|$ and $-7 \leq b \leq 6$. Then $|b|$ is written on at most 3 bits. The computation of $b + p'_i(t)/q$ only affects the first $n+3$ bits from Corollary 3. Then the cell m_i will be synchronized in at most $n+3$ iterations. □

We just described above the worst case of synchronization i.e. an upper bound for the number of steps required for an FCSR to synchronize. We examined in detail small examples, and we observed that the number of steps required to reach the main cycle is in most cases well under this upper bound. The following table presents the data obtained from these small examples:

q	n	ℓ	maximal length	number of max. tails	average length	variance
-157	7	4	7	7	2.29	1.52
-461	8	5	10	2	2.50	2.24
-821	9	5	10	12	2.54	2.19
-1499	10	6	11	92	2.82	2.39

2.3 Entropy

In a stream cipher, the key (and the IV) is usually used to set the initial state of an automaton. Then the automaton is used to ensure a good diffusion of differences resulting from initialization with different keys. In this process, it is very important that most of the entropy provided by the key be preserved. Indeed, such a loss of entropy could be seen as a potential weakness as it permits to improve time/memory/data attacks as done against the first version of stream cipher MICKEY [5] by J. Hong and W. Kim in [9].

Usually, except in some particular cases such as LFSRs of length n (where the number of states that can be reached after any number of transitions is maximal and is equal to $2^n - 1$), the entropy is not always known and computable. In the FCSR case, we have the following property (see [3] for more details). We assume that the FCSR is initialized with a random non-weak key (i.e. the initial state is not made of zeroes only, nor of ones only):

Property. The minimal number of states which can be reached after any number of transitions of an optimal FCSR automaton is $|q| - 1$.

Published in *SASC 2007 - Stream Ciphers Revisited, February 2007*
Special Workshop hosted by the ECRYPT Network of Excellence

This value corresponds, in fact, to the size of the main cycle of an optimal FCSR automaton. More precisely, the minimal entropy is reached when the current state belongs to the main cycle. So, using Theorem 3, we could now make this property more precise:

Corollary 5. *The number of states which can be reached after any number of transitions of an optimal FCSR does not decrease anymore after* $n+3$ *transitions. In any case, it does not decrease under* $|q|-1$.

3 A potential attack on F-FCSR pseudorandom generators

3.1 Recall 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 non-linear behavior directly discards algebraic attacks [4, 1].

So, it is not necessary to use a Boolean function with a high non-linearity, a simple linear function could be used to filter the content of the FCSR main register. This choice appears judicious for two main reasons: those functions are optimal in terms of resilient order and allow to discard a possible correlation attack. Moreover, they are efficient and easy to implement for hardware and software applications.

The family of F-FCSR generators (see [4, 2, 1, 6] for example) uses this model: at each iteration t, the keystream $z(t)$ corresponding with the output bit (or byte for some particular cases) is obtained by filtering the content of the main register of an optimal FCSR with a linear function.

3.2 Linear weakness of a FCSR automaton

The potential weakness described here addresses degenerated states of the FCSR automaton that occur when the transition function of the FCSR is linear, i.e. when at the same time, all the cells of the carry register and the feedback bit m_0 take the 0 bit value. The transition function becomes then a simple rotation of the contents of the cells of the main register:

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

Suppose that this situation occurs during r consecutive transitions of the FCSR at time t_0. Since a F-FCSR generator filters the FCSR

main register using a linear function, the output corresponding to these r iterations from time t_0 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 an 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 weakness would allow to produce a system of 256 linear equations with 256 unknowns. Once this system is solved, the complete state of the main register at time t_0 could be recovered.

We now want to estimate the corresponding probability of such an event to occur. For that purpose, the following lemma is needed:

Lemma 2. *The condition "carry bits equal to 0 and $p_0(t)/q$ begins with a sequence of r bits equal to 0" is equivalent with "carry bits equal to 0 and $m_i(t) = 0$ for all i, $0 \leq i < r$".*

Proof. If the carry register is empty (all the carry bits are equal to 0) then the transition function is linear, i.e. $m_i(t+1) = m_{i+1}(t)$ and then $m_0(t+i) = m_i(t)$ because of the null carry register. The converse is clear. □

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 chosen parameters of F-FCSR 16 with $n = 256$, $\ell = 130$ and $r = 16$, we obtain a probability 2^{-146} for that event.

3.3 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 6. *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 main cycle.*

Proof. We have $d^{(s+1)} = 2^s$, $u_{s+1} = 0$ and $v^{(s+1)} = p/2^{s+1}$. We have $q = 1 - 2d = 1 - 2(d^{(s+1)} + 2^{s+1}\delta^{(s+1)}) = 1 - 2d^{(s+1)} - 2^{s+2}\delta^{(s+1)}$. So $q + 2^{s+2}\delta^{(s+1)} = 1 - 2d^{(s+1)} = 1 - 2^{s+1} < 0$. From the Proposition 4, we have

$$p_{s+1} = qv^{(s+1)} + 2p\delta^{(s+1)} = qp/2^{s+1} + 2p\delta^{(s+1)} = p/2^{s+1}\left(q + 2^{s+2}\delta^{(s+1)}\right) < 0.$$

From Proposition 5, the current state of the automaton is not on the main cycle. □

Consequently, suppose that a FCSR automaton is clocked more than $n+3$ iterations before it is used to output some data. If the number r of required equations is greater than s, the situation described in Section 3.2 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: the automata are clocked more than $n+3$ iteration at each change of IV and $s=2$ in both cases.

Moreover, this precaution ensures a good diffusion of any changes in the initial state cf. [3].

4 Conclusion

In this paper, 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 the main cycle which is bounded by $n+3$ where n represents the bit length of the main register.

From the results proved here, we can provide some minimal security conditions when using an optimal FCSR automaton as a component of a pseudorandom generator. 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 main cycle. This is guaranteed after only $n+3$ iterations. We thus obtain an upper bound on the number of initial transitions needed before output be used. Moreover, we could initialize an FCSR with $c(0)=0$ to prevent two equivalent initial states resulting from different keys. Indeed, if $c(0)=0$, then two distinct initial states are not equivalent and cannot converge to the same state in the same number of steps. In this case, the initial entropy is exactly equal to n bits, and it can not decrease anymore.

We 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 event can occur only with a negligible probability if the setup method used before extracting data is well designed. The precaution needed here is to clock the automaton $n+3$ times so that it reaches the main cycle.

References

1. F. Arnault and T.P. Berger. F-FCSR: design of a new class of stream ciphers. In *Fast Software Encryption - FSE 2005*, volume 3557 of *Lecture Notes in Computer*

Science, pages 83–97. Springer-Verlag, 2005.
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. 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. http://www.ecrypt.eu.org/stream/.
4. François Arnault and Thierry P. Berger. Design and properties of a new pseudo-random generator based on a filtered FCSR automaton. *IEEE Trans. Computers*, 54(11):1374–1383, 2005.
5. Steve Babbage and Matthew Dodd. The stream cipher MICKEY (version 1). ECRYPT Stream Cipher Project Report 2005/015, 2005. http://www.ecrypt.eu.org/stream.
6. T. Berger and F. Arnault. Design of new pseudorandom generators based on filtered FCSR automaton. In *ECRYPT Network of Excellence - SASC Workshop Record*, pages 109–120, 2004. Available via www.isg.rhul.ac.uk/research/projects/ecrypt/stvl/sasc.html.
7. Mark Goresky and Andrew Klapper. Arithmetic crosscorrelations of feedback with carry shift register sequences. *IEEE Transactions on Information Theory*, 43(4):1342–1345, 1997.
8. Mark Goresky and Andrew Klapper. Fibonacci and galois representations of feedback-with-carry shift registers. *IEEE Transactions on Information Theory*, 48(11):2826–2836, 2002.
9. Jin Hong and Woo-Hwan Kim. Tmd-tradeoff and state entropy loss considerations of streamcipher mickey. In Subhamoy Maitra, C. E. Veni Madhavan, and Ramarathnam Venkatesan, editors, *INDOCRYPT*, volume 3797 of *Lecture Notes in Computer Science*, pages 169–182. Springer, 2005.
10. A. Klapper and M. Goresky. 2-adic shift registers. In *Fast Software Encryption - FSE'93*, volume 809 of *Lecture Notes in Computer Science*, pages 174–178. Springer-Verlag, 1993.
11. A. Klapper and M. Goresky. Basic results: Feedback shift registers, combiners with memory, and 2-adic span. available at http://www.cs.uky.edu/ klapper/fcsrs.html, 2003.
12. N. Koblitz. p-adic numbers, p-adic analysis and zeta-functions. Springer-Verlag, 1997.