Entropy of the Inner State of an FCSR

Andrea Röck
INRIA Paris - Rocquencourt, France

Kryptotag, 9th Novembre 2007

Outline

- FCSR
- Entropy after one Iteration
- Final Entropy
- Lower Bound
- Conclusion

Part 1

FCSR

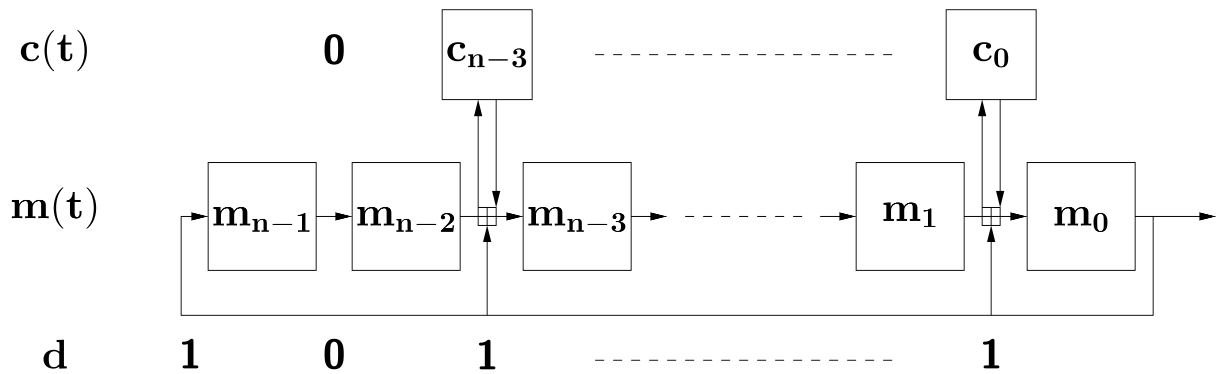
Introduction

- **Feedback with Carry Shift Register (FCSR):**
  Introduced by **[Goresky Klapper 97]**, **[Marsaglia Zamand 91]** and **[Couture L'Ecuyer 94]**.

- Binary FCSR in Galois architecture **[Goresky Klapper 02]**.

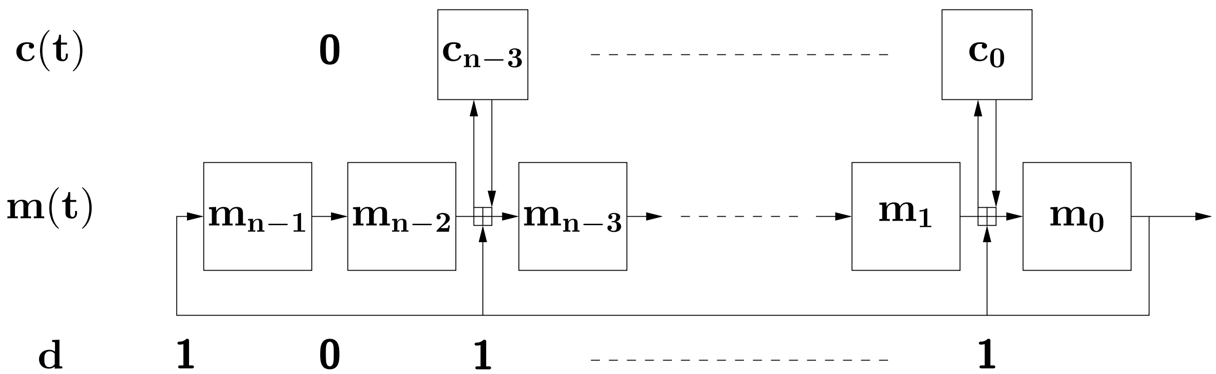
- Used in stream cipher *e.g.* the eSTREAM candidate F-FCSR **[Arnault Berger 05].**

FCSR in Galois architecture (1)



- n: Size of main register.
- d: Integer which determines feedback positions. Carry bit if $d_i = 1$.
- $(m(t), c(t))$: State at time t with
  - $m(t) = \sum_{i=0}^{n-1} m_i(t) 2^i$: 2-adic description of the main register.
  - $c(t) = \sum_{i=0}^{n-1} c_i(t) 2^i$: 2-adic description of the carry register, where $c_i(t) = 0$ for $d_i = 0$.

FCSR in Galois architecture (2)



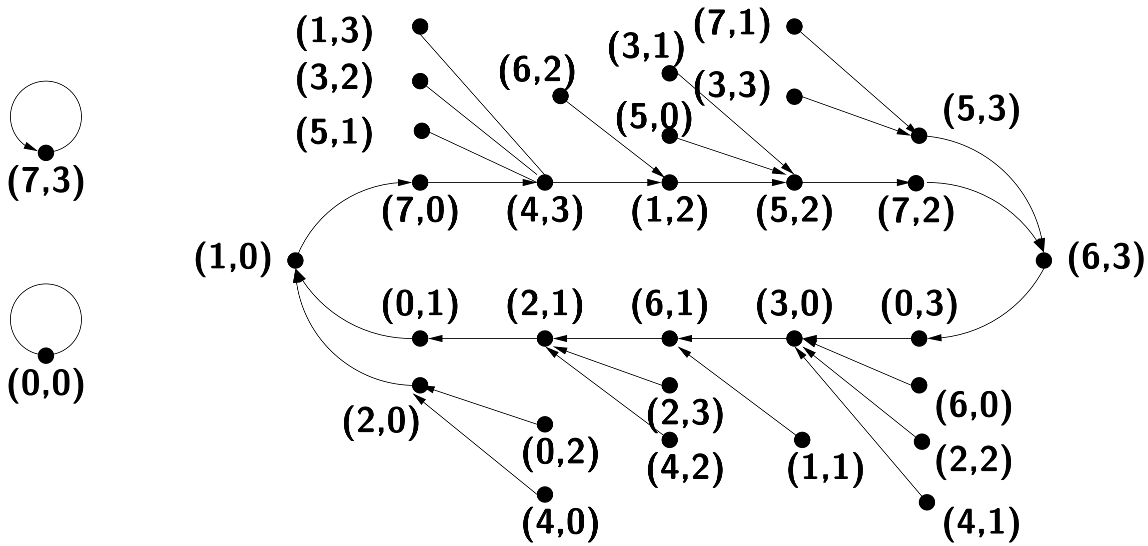
- **Update function:**

$$
\begin{aligned}
m_{n-1}(t+1) &= m_0(t), \\
d_i = 1 : 2c_i(t+1) + m_i(t+1) &= m_0(t) + c_i(t) + m_{i+1}(t), \\
d_i = 0 : m_i(t+1) &= m_{i+1}(t).
\end{aligned}
$$

Properties

- $q = 1 - 2d$ thus $q < 0$.
- $p = m + 2c$ thus $0 \leq p \leq |q|$.
- The output of the FCSR is the 2-adic description of
$$\frac{p}{q}.$$
- The output of the FCSR has the maximal period of $|q| - 1$ if and only if 2 has order $|q| - 1$ modulo q.

Entropy



- We have
  - n bits in the main register and
  - $\ell = HammingWeight(d) - 1$ carry bits.
- Initial Entropy: $n + \ell$ bits.
- Entropy after one iteration: $H(1)$.
- Final Entropy: H^f.

Part 2

Entropy after one Iteration

Idea

- **Initial entropy:** $n + \ell$.
- **Question:**
  Entropy loss after one feedback?
- **Method:**
  - Counting the number of $(m(0), c(0))$'s which produce the same $(m(1), c(1))$.
  - Using the equations of the update function.

Method

- Let $(m(0), c(0))$ be an initial state which produces $(m(1), c(1))$.
- We want a different $(m'(0), c'(1))$ to produce the same $(m(1), c(1))$.
- Only possible positions to change are i such that $d_i = 1$ and $m_{i+1}(0) + c_i(0) = 1$.
- For j such positions there are
  - $2^j - 1$ other initial states which produce the same $(m(1), c(1))$.
  - $\binom{\ell}{j} 2^n - j$ states $(m(1), c(1))$ in this category.
- Entropy after one iteration:

$$H(1) = \sum_{j=0}^{\ell} 2^{n-j} \binom{\ell}{j} \frac{2^j}{2^{n+\ell}} \log_2 \left(\frac{2^{n+\ell}}{2^j} \right) = n + \frac{\ell}{2}.$$

Part 3

Final Entropy

Final Entropy

- **Goal:** Entropy when we reached the cycle.
- **Idea:** How many (m, c)'s create the same $p = m + 2c$.
- **Lemma:** Let us take an FCSR with maximal period and let $v(p)$ denote the number of states (m, c) with $p = m + 2c$. Each $0 \leq p \leq |q|$ correspond to a point to the cycle which is reached by $v(p)$ initial values after the same number of iterations and thus has a probability of $\frac{v(p)}{2^{n+\ell}}$.
- **Method:** Get $v(p)$ by looking at bit per bit addition of m and $2c$.
- **Final Entropy:**

$$H^f = \sum_{p=0}^{|q|} \frac{v(p)}{2^{n+\ell}} \log_2 \left(\frac{2^{n+\ell}}{v(p)} \right)$$

Notations

- $i = \lfloor \log_2(p) \rfloor$: Most significant bit in p which is 1.
- $\ell' = \#\{j \leq i | d_{j-1} = 1\}$: Number of feedback positions smaller or equal to i.
- $r(p) = max\{j < i | d_{j-1} = 0, p_j = 1\}$: Index where a carry of the bit by bit addition is not forwarded.
- $f_1(r)$: Helping function.

$$f_1(r) = \begin{cases} 2^r & \text{for } r \geq 0 \\ 1 & \text{for } r = -1 \end{cases}$$

- $\ell''(r) = \#\{j < r | d_{j-1} = 1\}$: Number of feedback positions smaller than r.

4 Cases (1)

- **Case a**: $1 < i < n$ and $d_{i-1} = 0$

$$H_a(n, i, \ell, \ell') = 2^i \, 2^{\ell' - n - \ell}(n + \ell - \ell').$$

- **Case b**: $1 < i < n$ and $d_{i-1} = 1$

$$H_b(n, r, \ell, \ell', \ell'') = f_1(r) 2^{-n-\ell} \Big[\; 2^{\ell'-2} \left(3 \; 2^{\ell' - \ell'' - 1} + 1\right)(n + \ell - \ell'') \\ -2^{\ell''} S_1(\ell' - \ell'') \Big].$$

4 Cases (2)

- **Case c**: $i = n$ and $2^n \leq p \leq |q|$

$$H_c(n, r, \ell, \ell'') = f_1(r) 2^{-n} \Big[\quad 2^{-1} \left(2^{\ell - \ell''} - 1 \right) (n + \ell - \ell'') \\ -2^{\ell'' - \ell} S_2(\ell - \ell'') \Big].$$

- **Case d**: $0 \leq p \leq 1$ ("$i = 0$")

$$H_d(n, \ell) = 2^{-n-\ell}(n + \ell).$$

Approximation

- Approximating $\sum_{x=2^{k-1}+1}^{2^k} x\log_2(x)$ and $\sum_{x=1}^{2^k-1} x\log_2(x)$ by using

$$\frac{1}{2}\Big(x\log_2(x) + (x+1)\log_2(x+1)\Big) \approx \int_x^{x+1} y\log_2(y)\,dy$$

  for large x.

- Result for some arbitrary values of d.

n	d	ℓ	H^f	lb H^f	ub H^f	lb H^f , $k>5$	ub H^f, $k>5$
8	0xAE	4	8.3039849	8.283642	8.3146356	8.3039849	8.3039849
16	0xA45E	7	16.270332	16.237686	16.287598	16.270332	16.270332
24	0xA59B4E	12	24.273305	24.241851	24.289814	24.273304	24.273305
32	0xA54B7C5E	17		32.241192	32.289476	32.272834	32.272834

Part 4

Lower Bound

Lower Bound of the Final Entropy

- Proof that final entropy is $\geq n$ for all FCSR in Galois architecture by using previous algorithm.
- **Induction Base:**
  An FCSR, where the feedback positions are all group together at the least significant position, has a final entropy larger than n.
- **Induction Step:**
  If we move a feedback position one position to the left, the final entropy increases.

Part 5

Conclusion

Conclusion

- After one iteration we loose already $\ell/2$ bits of entropy.
- We presented an algorithm which calculates the final state entropy of an FCSR with maximal period.
- The algorithm works in $O(n^2)$ if the values of the sums $\sum_{x=2^{k-1}+1}^{2^k} x\log_2(x)$ and $\sum_{x=1}^{2^k-1} x\log_2(x)$ are known. Otherwise we need $O(2^\ell)$ steps to calculate the sums.
- The approximation of the sum works very well for large k.
- For all FCSR the final entropy is larger than n bits.