

Parallel generation of pseudo-random sequences

Who?

1100001010100110001001100100111010010110110001100000
0100001100101000011010101110010011101000011000100110
111101101010111000011110... =

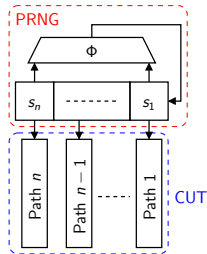
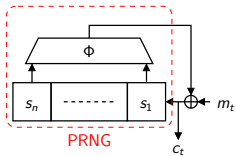
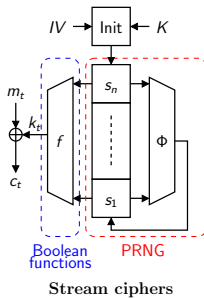
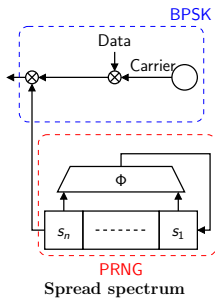
(Cedric Lauradoux)₁₀

—
1993524591318275015328041611344215036460140087963

When?

14/10/2008 (simply today)

Applications of sequences



Outline

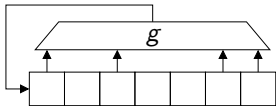
- Is it interesting to study shift register theory ?
- History of the parallel generation of *m*-sequences
 - *m*-sequences
 - *Decimation*
 - *Shift register transformations*
 - *The windmill generator*
- The extended windmill generator
 - *PFB transformation and windmill generator*
 - *NLFSRs*
- Wind to water: the case of *ℓ*-sequences
 - *ℓ*-sequences
 - *the watermill*
- Conclusions

Introduction

Is it interesting to study shift register theory ?

Sequences the backbone of symmetric cryptography: more precisely Non-Linear Feedback Shift Registers.

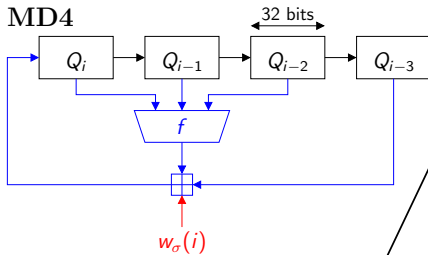
NLFSRs



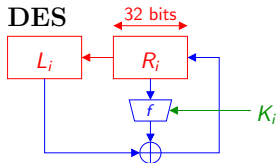
Problems:

- Period
- alphabet
- speed

MD4



DES



Introduction

Is it interesting to study shift register theory ?

Remembering some discussion:

[Student] How to choose the parameters for a PRNG ?

[Advisor] Well, there exist security parameters like a proven period, the size or the number of taps in the feedback. . .

[Student] Okay, but there is still many candidates that meet the criteria. So what is the next step ?

[Advisor] Do you know how to roll a dice ?

History of the parallel generation of m -sequences

m -sequences ?

Example

- $\frac{1+x}{1+x+x^2} = 11011011011 \dots$
- $\frac{1+x+x^2}{1+x+x^4} = 01111010110 \dots$
- $\frac{1+x+x^2+x^3+x^4+x^5+x^6+x^7+x^8}{1+x^6+x^8} = 11111111000000110000 \dots$

If we have $a(x) = \sum_{i=0}^{\infty} a_i X^i = \frac{p(x)}{q^*(x)}$:

$$a_i = \text{Tr}(p(x)\alpha^i).$$

History of the parallel generation of m -sequences

Definitions

Theorem

Let $S = (s_i)$ an infinite sequence. S is periodic iff $\exists p$ and $q, q^*(0) \neq 0, \deg(p) \leq \deg(q^*)$ such that $s(x) = p(x)/q^*(x)$.

Theorem

If p and q^* are relatively prime, the period T of $s(x) = p(x)/q^*(x)$ is **the order of $q(x)$** .

Result

If $q^*(x)$ is **primitive**, i.e. **irreducible** and $\text{ord}(q(x)) = 2^m - 1$, then $T = 2^m - 1$ with $m = \deg(q^*(x))$.

Comment

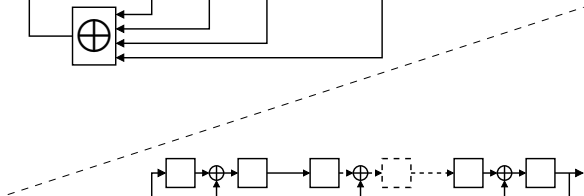
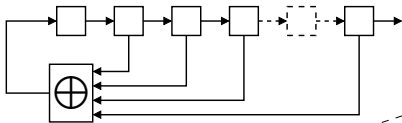
$q^*(x)$ is the **characteristic polynomial** of S defined as the reciprocal of the connection/feedback polynomial $q(x)$:

$$q^*(x) = x^n q\left(\frac{1}{x}\right).$$

History of the parallel generation of m -sequences

Linear Feedback Shift Registers (LFSRs)

Fibonacci setup

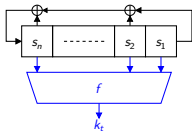


Galois setup

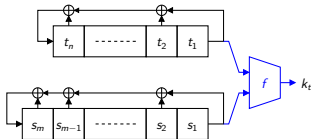
History of the parallel generation of m -sequences

The stream ciphers of our grandfathers

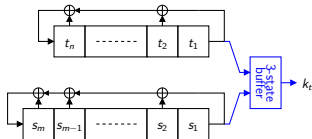
The filter generator



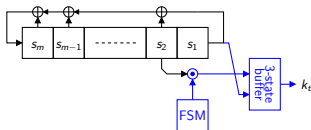
The combiner generator



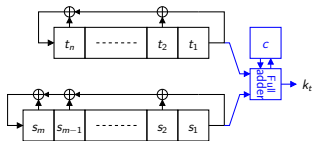
The shrinking generator



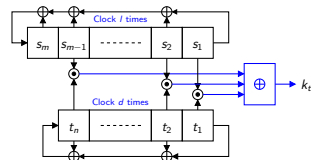
The self shrinking generator



The summation generator



The Multispeed inner product generator



History of the parallel generation of m -sequences

Decimation

Let S be an infinite sequence over an alphabet \mathcal{A} :

$$S = s_0, s_1, s_2 \cdots$$

For an integer v , a v -decimation of S is the set of sub-sequences defined by:

$$\begin{aligned} S_v^0 &= (s_0, s_v, \cdots) \\ S_v^1 &= (s_1, s_{1+v}, \cdots) \\ &\vdots \quad \quad \quad \vdots \\ S_v^{v-2} &= (s_{v-2}, s_{2v-2}, \cdots) \\ S_v^{v-1} &= (s_{v-1}, s_{2v-1}, \cdots) . \end{aligned}$$

History of the parallel generation of m -sequences

4 solutions

- Strict decimation
- Parallel feedforward transformation (PFF)
- Parallel feedback transformation (PFB)
- Windmill generator

History of the parallel generation of m -sequences

Strict decimation

Theorem

[Zierler1959,Rueppel1986]. Let S be a sequence produced by an LFSR whose feedback polynomial $q(x)$ is irreducible in \mathbf{F}_2 of degree n . Let α be a root of $q(x)$ and let T be the period of $q(x)$. Let S_v^i be a sub-sequence resulting from the v -decimation of S . Then, S_v^i can be generated by an LFSR with the following properties:

- The minimum polynomial of α^v in \mathbf{F}_{2^m} is the connection polynomial $q'(x)$ of the resulting LFSR.
- The period T' of $q'(x)$ is equal to $\frac{T}{\gcd(v,T)}$.
- The degree n' of $q'(x)$ is equal to the multiplicative order of $q(x)$ in $\mathbf{Z}_{T'}$.

History of the parallel generation of m -sequences

PFB transformation

Notation

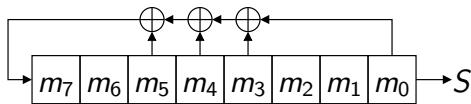
	<i>Memory cell</i>	<i>Content</i>
<i>One register</i>	m_i	$(m_i)_t$
<i>Many registers</i>	m_i^k of R_k	$(m_i^k)_t$

Example

Let consider the LFSR defined by the following relations:

$$(m_7)_{t+1} = (m_3)_t \oplus (m_4)_t \oplus (m_5)_t \oplus (m_0)_t$$

$$(m_i)_{t+1} = (m_{i+1}) \text{ if } i \neq 7.$$



History of the parallel generation of m -sequences

PFB transformation

The PFB transformation **virtually clocks an LFSR ν -times**.

Thus, we need to implement the previous equations for the successive states $(m_7)_{t+j}$ for $1 \leq j \leq \nu$ ($\nu = 3$):

$$(m_7)_{t+1} = (m_3)_t \oplus (m_4)_t \oplus (m_5)_t \oplus (m_0)_t$$

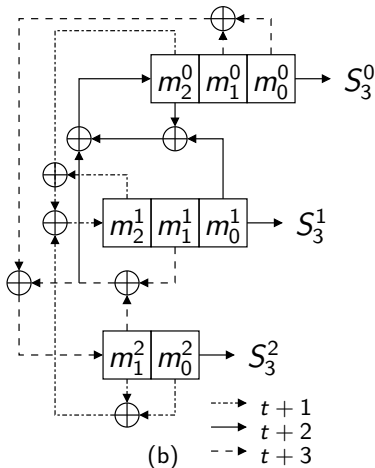
$$(m_7)_{t+2} = (m_4)_t \oplus (m_5)_t \oplus (m_6)_t \oplus (m_1)_t$$

$$(m_7)_{t+3} = (m_5)_t \oplus (m_6)_t \oplus (m_7)_t \oplus (m_2)_t$$

$$(m_i)_{t+3} = (m_{i+3})_t \text{ if } i < 5.$$

History of the parallel generation of m -sequences

PFB transformation



Well, it is a bloody mess !

History of the parallel generation of m -sequences

The windmill generator

Theorem

[Smeets1988] Let n and v be integers such that $1 \leq v < n$. Let $\alpha(x) = \sum \alpha_i x^i$ and $\beta(x^{-1}) = \sum \beta_i x^{-i}$ be two polynomials over \mathbf{F}_k such that $\alpha(0) = 1$ and $\beta(0) \neq 1$. There exist a permutation σ of $1, 2, \dots, v-1$ and a length parameters $\ell(i)$ such that the polynomial defined by:

$$q(x) = \alpha(x^v) - \beta(x^{-v}x^n)$$

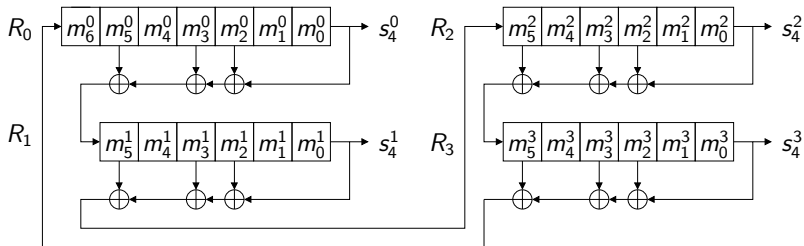
is the primitive feedback polynomial of the sequence S associated to the generator shown on the next slide!

History of the parallel generation of m -sequences

The windmill generator

The windmill generator has been used in the **E0 stream cipher** (Bluetooth):

Four LFSRs \Rightarrow Four 4-vane windmills



$$q(x) = x^{25} + x^{20} + x^{12} + x^8 + 1$$

History of the parallel generation of m -sequences

The windmill generator

v	4		8		16	
n	$\#_{pri}$	$\#_{irr}$	$\#_{pri}$	$\#_{irr}$	$\#_{pri}$	$\#_{irr}$
9	1	1				
15	2	4				
17	28	28	0	0		
23	82	86	1	1	0	0
25	314	318	6	6	0	0
31	1063	1063	3	3	0	0
33	3285	4092	15	18	0	0
39	11482	13566	10	12	0	0
41	51144	51148	54	54	0	0
47	178253	178368	40	40	1	1
49	678916	684122	170	172	0	0
55	2229834	2439982	137	161	1	3

How to compute this table ?

Irreducibility test

Definition

A polynomial $q \in \mathbf{F}_k[X]$ is irreducible, if $\deg(q) > 0$ and if all the divisor of q is a constant or a multiple of q by a constant.

Algorithm	Worst case
Ben-Or	$nM(n) \log kn$
Rabin	$nM(n) \log k \log n$

- $M(n) = n \log n \log \log n$ (assuming FFT-based multiplication)

Comment

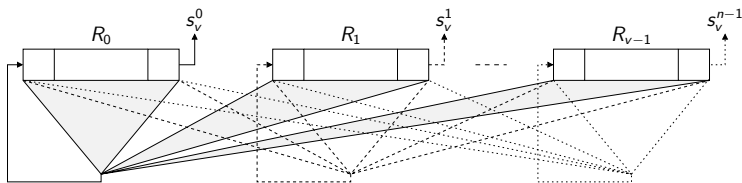
However, in practice we can expect to have $\log n M(n) \log kn$ with Ben-Or because a random polynomial is expected to have a factor of small degree.

The extended windmill generator

PFB transformation and windmill generator

The feedback function F_i in the PFB transformation can be decomposed as the sum modulo two of v sub-functions $f_{i,j}$ which depends only of a given register R_j :

$$F_i = \bigoplus_{j=0}^{v-1} f_{i,j}.$$



The extended windmill generator

PFB transformation and windmill generator

Prop. *A v -vane windmill polynomial of degree n corresponds to a shift-registers network issue from a PFB transformation with at most 2 functions $f_{i,j}$ associated to the feedback function F_i , $0 \leq i < v$.*

Proof *The feedback function can be written:*

$$(m_{n-1}^k)_{t+1} = \bigoplus_{i=0}^{\lfloor n/v \rfloor} \alpha_{vi+j-1} (m_{vi+j-1}^{\sigma_1(k)})_t \oplus \bigoplus_{j=0}^{\lfloor n/v \rfloor} \beta_{m-iv+j-1} (m_{m-vi+j-1}^{\sigma_2(k)})_t$$

with $k > n - v$ and σ_1 and σ_2 are two permutation of $1, 2 \dots v - 1$ defined by:

$$\begin{aligned}\sigma_1(k) &= \lfloor \frac{n}{v} \rfloor + k - 1 \bmod v \\ \sigma_2(k) &= n + k \bmod v.\end{aligned}$$

The extended windmill generator

PFB transformation and windmill generator

Result

The windmill generator is only a subset of the PFB transformation with only 2 $f_{i,j}$ per F_i .

How to find the others ?

- modify σ_1 ? not possible because $\alpha(0) \neq 0$.
- so modify σ_2 :

$$\sigma'_2(k) = n + k - \phi \pmod v.$$

- if $\phi = 0 \leftarrow$ the original windmill setup
- if $n + k - \phi = 0 \pmod v \leftarrow$ the original setup with $\beta(x) = 1$
- otherwise new setup !

The extended windmill generator

New definition

Definition

The primitive polynomial

$$q(x) = \alpha(x^v) - x^{n-\phi}\beta(x^{-v}) - x^n$$

with $\alpha(0) \neq 0$, $\beta(x) \neq 0$ if $\phi = 0$ and $\beta(0) = 0$ otherwise and $0 \leq \phi < v$ defines the set of all PFB transformation with at most 2 functions $f_{i,j}$ associated to F_i , $0 \leq i < v$ and generating m -sequences.

Is it a good news ? Yes, we can find good polynomials of degree $d = 3 \pmod 8$.

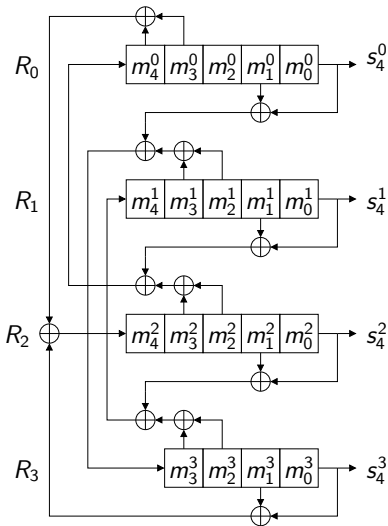
The extended windmill generator

New result

v	4		8		16	
n	$\#_{pri}$	$\#_{irr}$	$\#_{pri}$	$\#_{irr}$	$\#_{pri}$	$\#_{irr}$
9	1	1	0	0	0	0
11	1	1	0	0	0	0
13	6	6	0	0	0	0
15	9	12	0	0	0	0
17	38	38	2	2	0	0
19	31	31	3	3	0	0
21	39	41	2	2	0	0
23	172	179	4	4	0	0
25	479	491	19	19	0	0
27	238	281	4	5	0	0
29	571	573	2	2	0	0
31	2133	2133	16	16	0	0
33	4901	6100	34	46	3	3
35	3473	3702	18	18	4	4

The extended windmill generator

New result



$$q(x) = x^{19} + x^{13} + x^9 + x^4 + 1$$

The extended windmill generator

Non Linear Feedback Shift registers

Definition

The feedback functions of a **non-linear non-singular extended windmill generator** are defined by:

$$F_k = m_0^{\sigma_1(k)} \oplus g(m_{\alpha_{i_1}}^{\sigma_1(k)}, m_{\alpha_{i_2}}^{\sigma_1(k)}, \dots, m_{\beta_{j_1}}^{\sigma_2(k)}, m_{\beta_{j_2}}^{\sigma_2(k)}, \dots)$$

with g a Boolean function and:

$$\begin{aligned}\sigma_1(k) &= \lfloor \frac{n}{v} \rfloor + k - 1 \bmod v \\ \sigma_2(k) &= n + k - \phi \bmod v.\end{aligned}$$

Is it a good news ? It is an empty definition (choice for g : 2^{2^m})
but at least it is a **research direction**...

Wind to water: the case of l -sequences

l -sequences ?

Example

- $\frac{1}{5} = \dots 110011001101$
- $\frac{1}{7} = \dots 010101010111$
- $-\frac{1}{7} = \dots 1001001001001$

Definition

The canonical Hensel form of a **2-adic integer** a is defined by:

$$a = \sum_{i=0}^{\infty} a_i 2^i.$$

If we have $\sum_{i=0}^{\infty} a_i 2^i = \frac{A}{q}$:

$$a_i = 2^{-i} A \pmod{q} \pmod{2}.$$

Wind to water: the case of ℓ -sequences

Definitions

Theorem $S = (s_i)$ an infinite sequence. S is periodic iff $\exists p$ and q , **relatively prime**, q odd such that $p/q = \sum_{i=0}^{\infty} s_i 2^i$ with $q < 0 \leq p, p \leq -q$.

Theorem If p and q are relatively prime, q odd, the period T of p/q is the order of 2 modulo q .

Result If q is well chosen, then $T = q - 1$.

Wind to water: the case of ℓ -sequences

What about the 4 solutions ?

- Strict decimation: very bad **[Lauradoux2008]**
- Parallel feedforward transformation (PFF): not known...
- Parallel feedback transformation (PFB) **[Lauradoux2008]**
- Watermill generator **[Lauradoux2009 ?]**

Wind to water: the case of ℓ -sequences

The watermill generator

Let q be a prime number of maximal order such that:

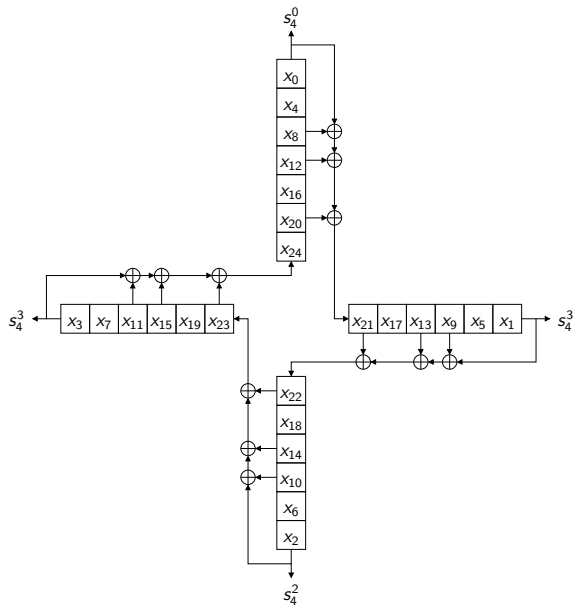
$$q = \alpha + 2^{n-\phi} \beta + 2^n$$

with $\alpha = \sum \alpha_i 2^{i\nu}$, $\alpha_0 = 1$ and $\beta = \sum \beta_i 2^{-i\nu} \dots$

Conclusion

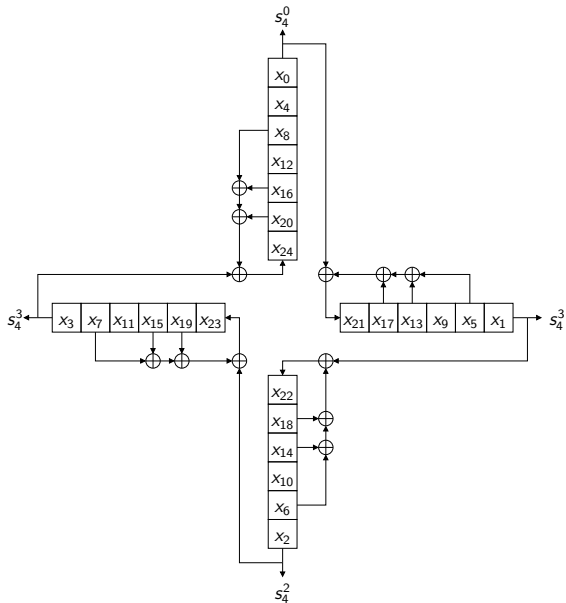
Why is it called the windmill generator ?

Conclusion



A. $f(x) = x^{25} + x^{20} + x^{12} + x^8 + 1$

Conclusion



$$B. f(x) = x^{25} + x^{17} + x^{13} + x^5 + 1$$