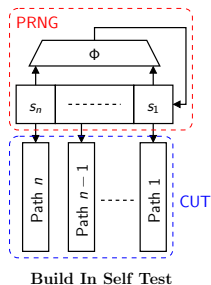
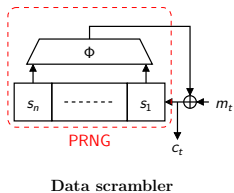
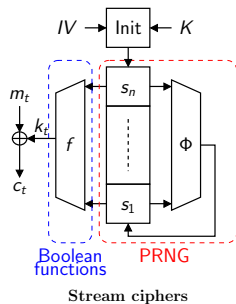
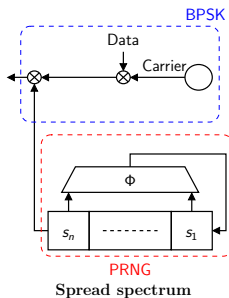


Towards non-linear feedbacks

Who? Cédric Lauradoux

When? December 2, 2008

Applications of sequences

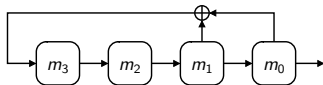


Outline

- Shift register theory fundamentals
- Universal windmill generators:
 - parallel random number generators;
 - parallel generation of m -sequences;
 - windmill generators (extension);
- Symmetric feedback functions:
 - Symmetric functions;
 - Ideas.
- Conclusions

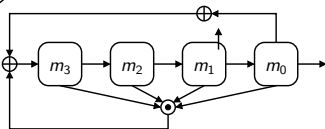
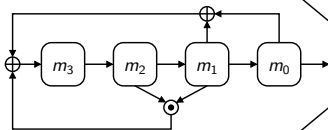
Shift register theory fundamentals

Linear Feedback Shift Registers



Period: $T = 2^n - 1$

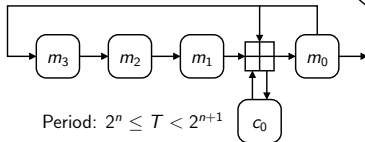
Quadratic Feedback Shift Registers



$$\overline{m_0 \vee m_1 \vee m_2 \vee m_3}$$

Period: $T = 2^n$

Feedback with Carry Shift Registers



Period: $2^n \leq T < 2^{n+1}$

Shift register theory fundamentals

non-linear

Theorem

[De Bruijn1946] *There is exactly $\frac{2^{2^n-1}}{2^n}$ NLFSRs of period 2^n .
(The number of LFSRs of period $2^n - 1$ is $\frac{\phi(2^n-1)}{2^n} \approx \frac{2^n}{n}$.)*

Theorem

[Golomb1967] *The feedback function f of an NLFSR of period 2^n is defined:*

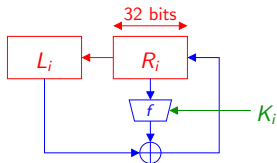
$$f(x_0, x_1, \dots, x_{n-1}) = x_0 \oplus g(x_1, x_2, \dots, x_{n-1}).$$

Such NLFSRs is called a non-singular shift register.

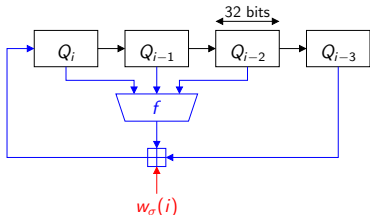
Shift register theory fundamentals

Modern cryptography

- Block ciphers: Feistel scheme (DES, RC6. . .)



- Hash functions: (MD4, MD5, MD6. . .)



Shift register theory fundamentals

Modern cryptography

- eSTREAM Portfolio:

| Software profile | Hardware profile |
|------------------|------------------|
| HC-128 | Grain |
| Rabbit | Mickey |
| Salsa20/12 | Trivium |
| Sosemanuk | |

- other designs:

- ▶ Keeloq (block/stream)
- ▶ Squash (MAC)

Shift register theory fundamentals

So if everybody use NLFSRs, it must be well-mastered ??
Ask the question to Ron Rivest. . .

How to explore non-linear feedback functions ?

- constraints on the variables
- reduced the choice for the feedback function

Universal windmill generators

Definition

A v -vane universal windmill generator is a network of v shift registers non-linearly interconnected, $v \geq 1$. The size of the vane R_k is $\ell(k)$. The interconnection network defined the feedback of a register R_k by:

$$m_{\ell(k)}^k(t+1) = g(m_{\alpha_{i_1}}^{\sigma_1(k)}(t), m_{\alpha_{i_2}}^{\sigma_1(k)}(t), \dots, m_{\beta_{j_1}}^{\sigma_2(k)}(t), m_{\beta_{j_2}}^{\sigma_2(k)}(t), \dots)$$

with σ_1 and σ_2 are 2 permutations of $1, 2, \dots, v - 1$.

Universal windmill generators

Example

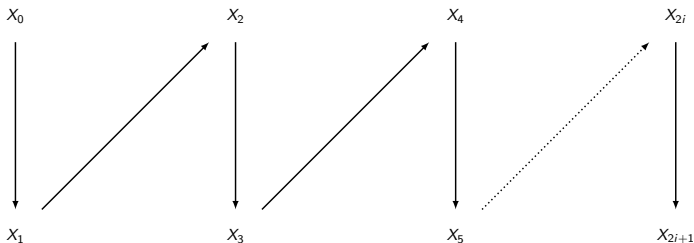
Nothing yet! waiting for simulation results!
Don't worry some entertainment is following. . .

Parallel random number generator

Simple example

The basic linear congruential generator (LCG):

$$X_{t+1} = aX_t + c \text{ mod } n.$$



$$S = X_0, X_1, X_2, \dots, X_{2i+1}, \dots$$

Parallel random number generator

LCG: parallel implementation

More generally, we have:

$$X_{t+i} = a^i X_0 + \left(\frac{a^i - 1}{a - 1} \right) \cdot c \bmod n.$$

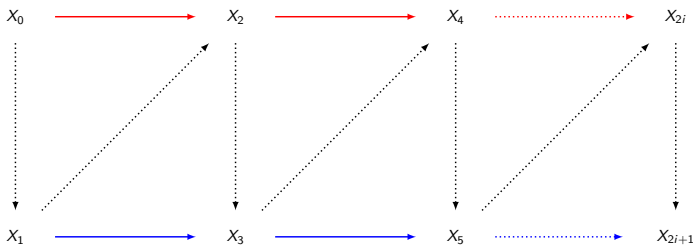
Then, we obtain for $t = \frac{u}{k}$:

$$X_{k(u+1)} = a^k X_{ku} + \left(\frac{a^k - 1}{a - 1} \right) \cdot c \bmod n$$

$$k = 2, u = 0 \text{ and } u = \frac{1}{2} \begin{cases} S_2^0 = X_0, X_2, X_4 \cdots X_{2i} \cdots \\ S_2^1 = X_1, X_3, X_5 \cdots X_{2i+1} \cdots \end{cases}$$

Parallel random number generator

Applications



SIMD/MIMD computers

Vector processor

Parallel random number generator

The problem

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:

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

Knowing S , how to generate the sub-sequences S_v^i ?
(Jeopardy: knowing the S_v^i how to find the shortest S ?)

Parallel random number generator

Other generators

- Linear congruential generator:

$$X_{k(u+1)} = a^k X_{ku} + \left(\frac{a^k - 1}{a - 1} \right) \cdot c \pmod{n}.$$

- Blum Blum Shub (p, q are 2 large prime numbers):

$$X_{k(u+1)} = X_{ku}^{2^k \pmod{(p-1)(q-1)}} \pmod{pq}.$$

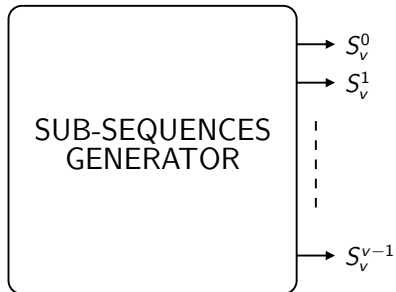
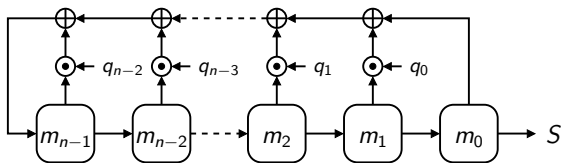
- FCSRs

[Lauradoux et Roeck 2008]

$$(x_i)_\tau = \begin{cases} (x_0)_{\tau-m+i} \oplus \bigoplus_{k=0}^{m-2-i} a_{i+k} [(x_0)_{\tau-k-1} \oplus (c_{i+k})_{\tau-k-1}] & \text{if } m-v \leq i < m \\ (x_{i+v})_t \oplus \bigoplus_{k=0}^{d-1} a_{i+k} [(x_0)_{\tau-k-1} \oplus (c_{i+k})_{\tau-k-1}] & \text{if } i < m-v \end{cases}$$

$$(c_i)_\tau = [(x_0)_{\tau-1} \oplus (x_{i+1})_{\tau-1}] [(x_0)_{\tau-1} \oplus (c_i)_{\tau-1}] \oplus (x_0)_{\tau-1}$$

Parallel generation of m -sequences



Parallel generation of m -sequences

4 solutions exist to obtain parallel LFSRs:

- decimation: properties of m -sequences; **[Zierler1959]**
- parallel feedforward transformation (PFF); **[Hsia1969]**
- **parallel feedback transformation** (PFB); **[Hurd1974]**
- **windmill generators**. **[Smeets1988]**

Parallel generation of m -sequences

Solution I: decimation

Theorem

[Zierler1959]. Let S be an m -sequence of characteristic polynomial q with root α . The *sub-sequences* S_v^i of S are also some m -sequences such that:

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

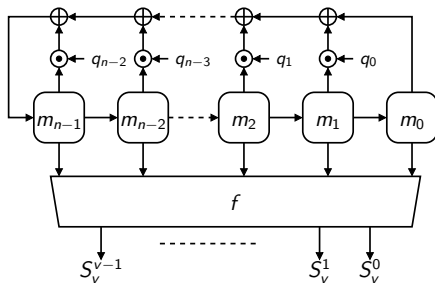
A given S_v^i can be generated by an LFSR.

Parallel generation of m -sequences

Solution II: parallel feedforward

Idea *Based on the exponential representation of m -sequences:*

$$u_t = \text{Tr}(\alpha^i x)$$



Parallel generation of m -sequences

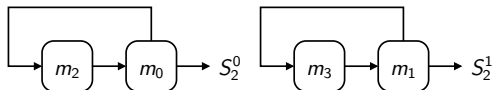
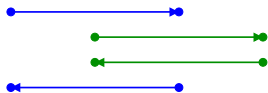
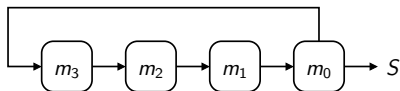
Solution III: parallel feedback

Idea

Clock v times the LFSR in one clock cycle !?

Example

A PFB transformation on a simple cycling register:



Parallel generation of m -sequences

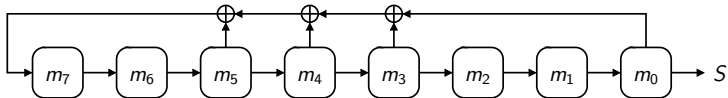
Solution III: a more elaborate example

Example

Let consider the LFSR defined by the following relations:

$$m_7(t+1) = m_3(t) \oplus m_4(t) \oplus m_5(t) \oplus m_0(t)$$

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



Parallel generation of m -sequences

Solution III: a more elaborate example

To apply the PFB transformation, we need to implement the previous equations for the successive states $m_7(t+j)$ for $1 \leq j \leq v$ ($v = 3$):

$$m_7(t+1) = m_3(t) \oplus m_4(t) \oplus m_5(t) \oplus m_0(t)$$

$$m_7(t+2) = m_4(t) \oplus m_5(t) \oplus m_6(t) \oplus m_1(t)$$

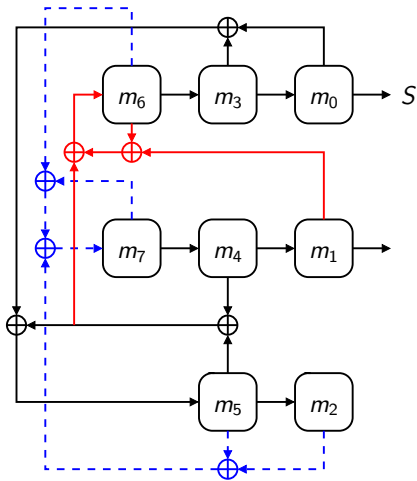
$$m_7(t+3) = m_5(t) \oplus m_6(t) \oplus m_7(t) \oplus m_2(t)$$

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

Now, we start the unpleasant part...

Parallel generation of m -sequences

Solution III: the **bloody** mess



Parallel generation of m -sequences

Solution IV: windmills

Definition

[Smeets1988] A v -vane windmill generator is a network of v shift registers linearly interconnected, $v \geq 1$. The size of the vane k is $\ell(k)$. The interconnection network is defined by:

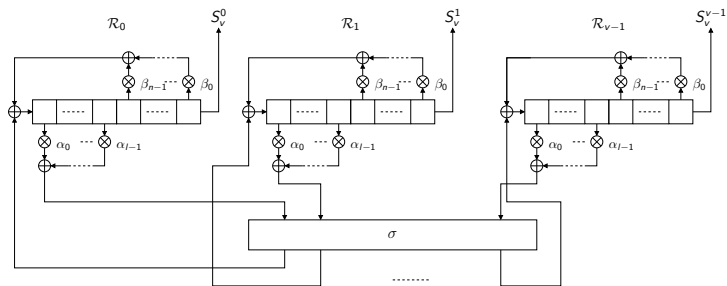
$$m_{\ell(k)}^k(t+1) = \bigoplus_{i=0}^{\ell(\sigma(k))} \alpha_i m_i^{\sigma(k)}(t) \oplus \bigoplus_{j=0}^{\ell(k)} \beta_j m_j^k(t)$$

with σ a permutation of $1, 2, \dots, v-1$.

Such a generator is an (n, v, σ, ℓ) -windmill generator.

Parallel generation of m -sequences

Solution IV: first figure



Parallel generation of m -sequences

Solution IV: property

Theorem

[Smeets1988] Let n and v be integers such that $1 \leq v < n$, a permutation σ and a length function ℓ . Let $\alpha(x) = \sum \alpha_i x^i$ and $\beta(x^{-1}) = \sum \beta_i x^{-i}$ be two polynomials over \mathbf{F}_2 such that $\alpha(0) = 1$ and $\beta(0) \leq 1$. The polynomial defined by:

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

is the connection polynomial of the sequences S associated to an (n, v, σ, ℓ) -windmill generator .

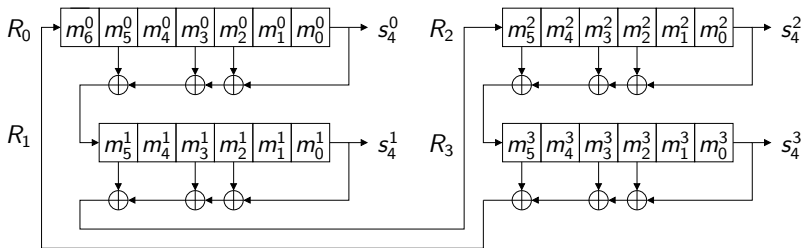
q is called a windmill polynomial.

Parallel generation of m -sequences

Solution IV: exemple

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

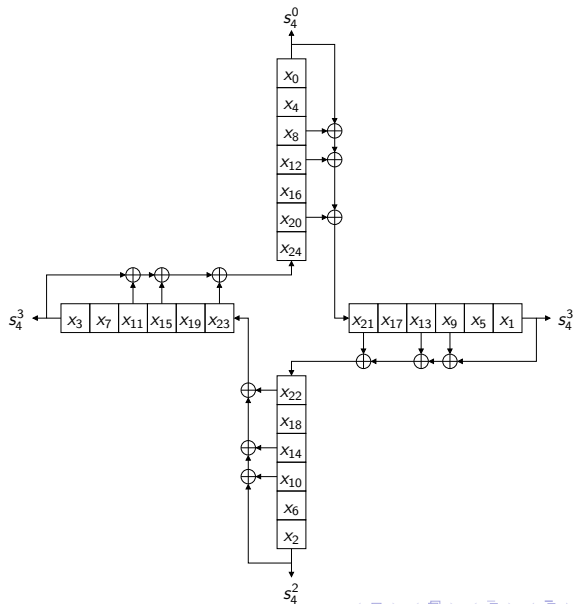
Four LFSRs \Rightarrow Four 4-vane windmills



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

Parallel generation of m -sequences

Solution IV: why is called windmill?



Windmill generators

Even Don Quichotte has some weapons!



Windmill generators

Testing irreducibility

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.

Many algorithms:

- Berlekamp;
- Knuth-Alanen;
- Shoup;
- Ben-Or;
- Rabin;
- Argnt. . .

Windmill generators

Irreducibility test

Theorem

[Rabin] Let p_1, p_2, \dots, p_k be all the prime divisor of n , and denote $n_i = \frac{n}{p_i}$ for $1 \leq i \leq k$. A polynomial $f \in \mathbf{F}_q[x]$ of degree n is irreducible in $\mathbf{F}_q[x]$ iff $\gcd(f, x^{q^{n_i}} - 1) = 1$, for $1 \leq i \leq k$, and f divides $x^{q^n} - x$.

Theorem

[Ben-Or] For $i \geq 1$, the polynomial $x^{q^i} - x \in \mathbf{F}_q[x]$ is the product of all monic irreducible polynomials whose degree divides i .

| 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)

Windmill generators

How many they are

| 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 |

Windmill generators

How many they are

Theorem

[Cohen1989] *There is no (n, v, σ, ℓ) -windmill polynomials, $v = 2^i, i > 0$ such that $n = 3 \pmod 8$ or n even.*

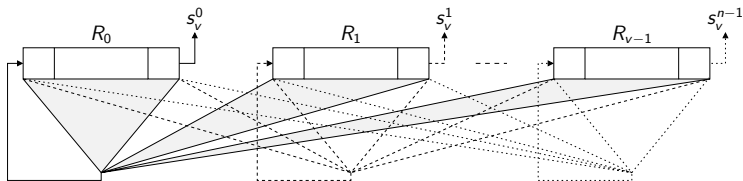
First observed by Smeets and later proved by Cohen while studying the Galois group the windmill polynomials.

There is something to do with the PFB transformation and the windmill generators.

Windmill generators

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 which depends each of a given register R_j :



The windmill generator is the **optimal case** for a PFB transformation!

Windmill generators

PFB transformation and windmill generator

Remark

An (n, v, σ, ℓ) -windmill generator corresponds to a shift-registers network issued from a PFB transformation. The feedback F_i of R_i depends at most on the contribution of 2 registers

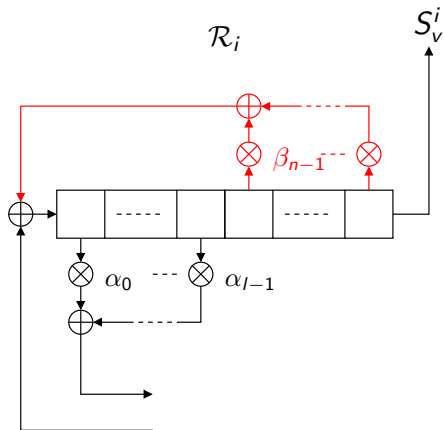
Comment

Let consider a windmill polynomial $q(x) = \alpha(x^v) + \beta(x^{-v})x^n$.
We have:

- $\beta(x) \neq 1$, F_i depends exactly on 2 registers:
- $\beta(x) = 1$, F_i depends exactly on 1 registers.

Windmill generators

Extension



Windmill generators

Extension

Instead of the original windmill polynomial:

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

let consider the linear universal windmill polynomial:

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

with $\phi < v$.

$$m_{\ell(k)}^k(t+1) = \bigoplus_{i=0}^{\ell(\sigma_1(k))} \alpha_i m_i^{\sigma_1(k)}(t) \oplus \bigoplus_{j=0}^{\ell(\sigma_2(k))} \beta_j m_j^{\sigma_2(k)}(t)$$

Windmill generators

Extension

Let see what we can achieve with ϕ :

- $\phi = 0 \leftarrow$ the original definition;
- $n - \phi = 0 \pmod v$, $q(x) = \alpha(x) + x^n$;
- otherwise we have something new: parameters (n, v, τ, ℓ, ϕ) .

Example

An $(19, 4, \sigma, \ell, 2)$ -universal windmill generator:

$$\alpha(x) = 1 + x$$

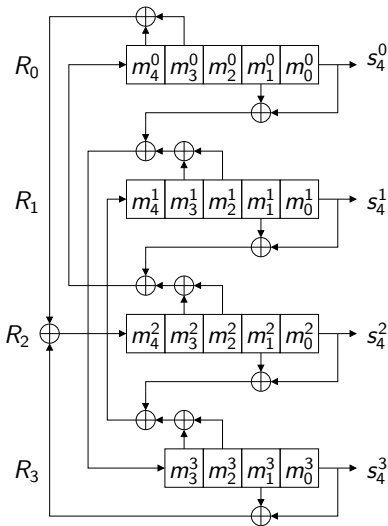
$$\beta(x) = x + x^2$$

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

Interesting: $19 = 3 \pmod 8$.

Windmill generators

Extension



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

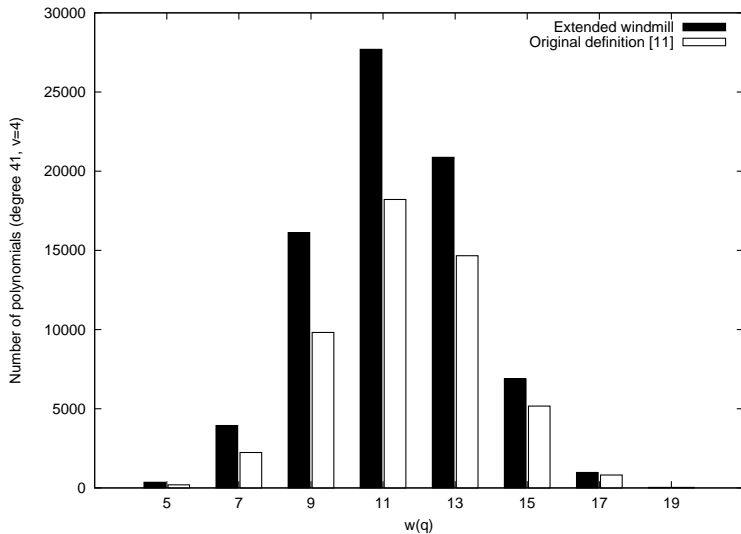
The extended windmill generator

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 |

Windmill generators

$n = 41, v = 4$



Windmill generators

Security

A windmill polynomial q is likely to have a multiple of low Hamming weight of the form $Q(x) = (1 + x^{iv})q(x)$:

$$\begin{aligned}q(x) &= x^{41} + x^{37} + x^{33} + x^{32} + x^{29} + x^{28} + x^{25} + x^{24} + x^{21} \\ &+ x^{20} + x^{17} + x^{16} + x^{13} + x^{12} + x^9 \\ &+ x^8 + x^5 + x^4 + 1\end{aligned}$$

has for multiple $Q(x) = (1 + x^4) \times q(x) = x^{45} + x^{36} + x^5 + 1$.

Conclusions

- Universal ?

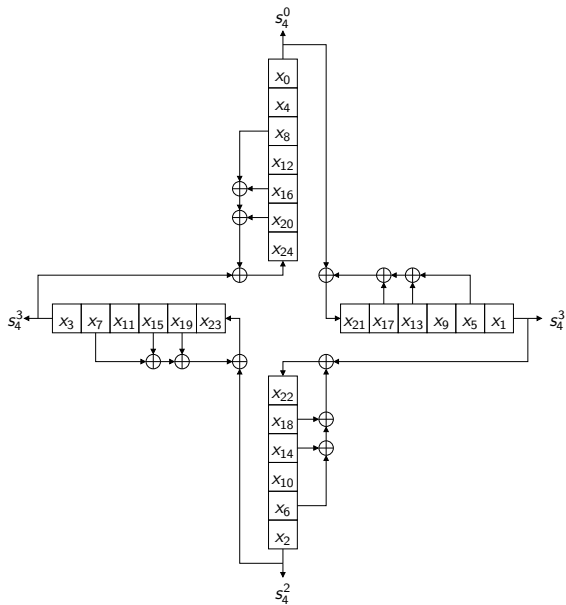
Theorem

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

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

with $\alpha = \sum \alpha_i 2^{iv}$, $\alpha_0 = 1$ and $\beta = \sum \beta_i 2^{-iv} \dots$ is the connection integer of an $(n, v, \sigma, \ell, \phi)$ -watermill generator.

- NLFSRs ? coming soon in 2009.
- A first paper submitted at IEEE TC.



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