Cross joining de Bruijn sequences and Nonlinear Feedback Shift Registers

Johannes Mykkeltveit and **Janusz Szmidt**
Bergen (Norway), Zegrze (Poland)

Fast Software Encryption
London 2014

NLFSRs - Nonlinear Feedback Shift Registers

- Let $\mathbb{F}_2 = \{0, 1\}$ denote the binary field and $\mathbb{F}_2^n$ the vector space of all binary n-tuples.
- A binary Feedback Shift Register (FSR) of order n is a mapping

$$\mathfrak{F} : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^n$$

of the form

$$\mathfrak{F} : (x_0, x_1, \ldots, x_{n-1}) \longmapsto (x_1, x_2, \ldots, x_{n-1}, f(x_0, x_1, \ldots, x_{n-1})) \quad (1)$$

where the *feedback function* f is a Boolean function of n variables.

- The FSR is called *non-singular* if the mapping $\mathfrak{F}$ is one-to-one, i.e., $\mathfrak{F}$ is a bijection on $\mathbb{F}_2^n$.

NLFSRs - Nonlinear Feedback Shift Registers, cont.

- It was proved that the FSR is non-singular iff its feedback function has the form

$$f(x_0, x_1, \ldots, x_{n-1}) = x_0 + F(x_1, \ldots, x_{n-1}) \quad (2)$$

  where F is a Boolean function of $n-1$ variables.

- The FSR is called linear (LFSR) if the feedback function f is linear one and nonlinear (NLFSR) if the function f is nonlinear; i.e., the function f has higher degree terms in its Algebraic Normal Form (ANF).
- Further, we will consider nonsingular and nonlinear feedback shift registers.

De Bruijn sequences

- **Definition 1.** A de Bruijn sequence of order n is a sequence of length 2^n of elements of $\mathbb{F}_2$ in which all different n-tuples appear exactly once.
- It was proved by Flye Sainte-Marie in 1894 and independently by de Bruijn in 1946 that the number of cyclically inequivalent sequences satisfying the Definition 1 is equal to

$$B_n = 2^{2^{n-1}-n} \tag{3}$$

- **Definition 2.** A modified de Bruijn sequence of order n is a sequence of length $2^n - 1$ obtained from the de Bruijn sequence of order n by removing one zero from the tuple of n consecutive zeros.

Proposition 1. Let (s_t) be a de Bruijn sequence. Then there exists a Boolean function $F(x_1, \cdots, x_{n-1})$, such that

$$s_{t+n} = s_t + F(s_{t+1}, \cdots, s_{t+n-1}), \quad t = 0, 1 \cdots, 2^n - n - 1. \qquad (4)$$

(The proof is given in Golomb's book: *Shift Register Sequences*).

AN OLD PROBLEM

Construct or describe Boolean functions F which give all de Bruijn sequences.

Cross joint pairs

Definition 3. The pairs of states $\alpha = (u, U)$, $\widehat{\alpha} = (\overline{u}, U)$ and $\beta = (v, V)$, $\widehat{\beta} = (\overline{v}, V)$, where $\overline{u} = u + 1$ is a negation of a bit u, constitute a cross joint pair, if the order they occur in is $\alpha,\ \beta,\ \widehat{\alpha},\ \widehat{\beta}$.
The next fact is a classical result.
Proposition 2. Let (s_t) be a de Bruijn sequence satisfying (4) and let us assume that there is a cross-join pair U, V for the sequence (s_t). Let the Boolean function $G(x_1, \cdots, x_{n-1})$ be obtained from $F(x_1, \cdots, x_{n-1})$ by complementing $F(U), F(V)$, then $G(x_1, \cdots, x_{n-1})$ also generates a de Bruijn sequence (u_t), say.
We say that (u_t) is obtained from (s_t) by the cross-join pair operation.

Theorem. (*J. Mykkeltveit and J. Szmidt*)
Let (u_t), (v_t) be two de Bruijn sequences of degree n. Then (v_t) can be obtained from (u_t) by repeated application of the cross joint pair operation.

One term quadratic NLFSRs of order n

- $n = 27, \quad x_0 + x_1 + x_2 + x_4 + x_8 + x_{10} + x_{11} + x_{14} + x_{17} + x_{19} + x_{21} + x_6 x_{10}$
- $n = 28, \quad x_0 + x_4 + x_5 + x_6 + x_8 + x_{11} + x_{14} + x_{18} + x_{19} + x_{21} + x_{22} + x_{26} + x_{27} + x_8 x_{27}$
- $n = 29, \quad x_0 + x_3 + x_5 + x_6 + x_{11} + x_{12} + x_{16} + x_{19} + x_{22} + x_{23} + x_{27} + x_{20} x_{28}$

Thank you !