A Spectral Approach for Characterizing the Self-Synchronization of Stream Ciphers

Jérémy Parriaux[1] Philippe Guillot[2] Gilles Millérioux[1]

Nancy University, CNRS,
Research Center for Automatic Control of Nancy (CRAN UMR 7039), France,
jeremy.parriaux@esstin.uhp-nancy.fr, gilles.millerioux@esstin.uhp-nancy.fr,

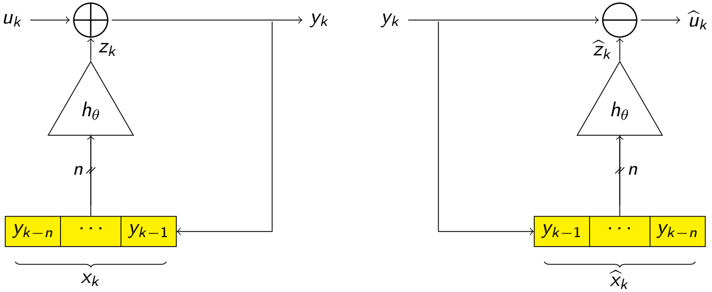
Paris 8 University
Laboratoire Analyse, Géométrie et Applications (LAGA UMR 7539), France
philippe.guillot@univ-paris8.fr

February 16, 2011

Outline

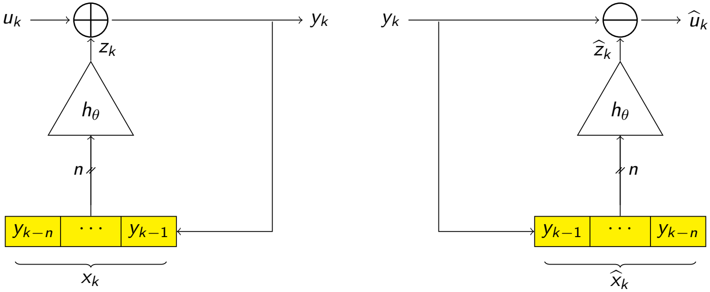
Self-synchronizing Stream Ciphers

Canonical form



θ	key	y_k	cipher-text
m_k	plain-text	$\widehat{m}_k$	recovered plain-text
x_k	state of the cipher	$\widehat{x}_k$	state of the decipher
z_k	complex sequence	$\widehat{z}_k$	complex sequence
f_θ	next-state function	h_θ	output function

Self-synchronizing Stream Ciphers
Canonical form

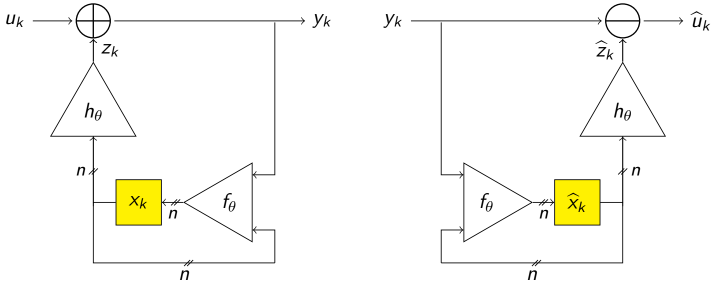


Advantages

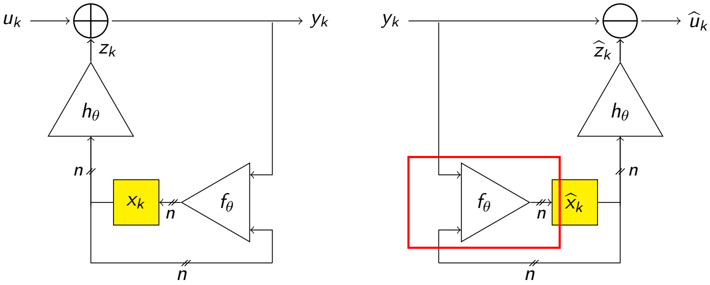
- Synchronization of cipher and decipher is structural property
- Does not require any external synchronization protocol

Self-synchronizing Stream Ciphers

Recursive form

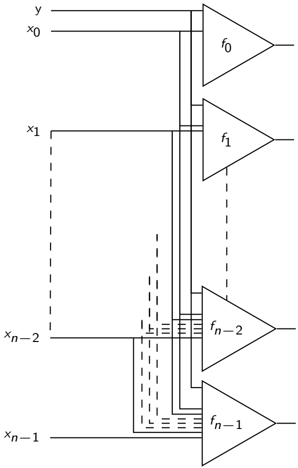


Self-synchronizing Stream Ciphers
Recursive form



Question

- How to characterize the functions f_θ so that $\forall k > k_t$ the state $\widehat{x}_k$ does not depend on the initial state $\widehat{x}_0$?
- Is there any non strict T function f_θ that can be used ?

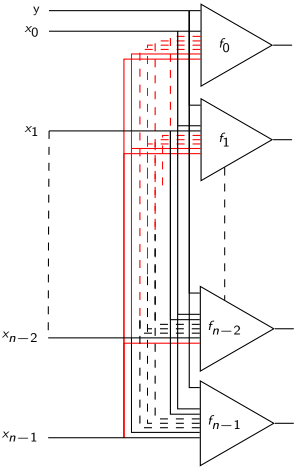


strict T-function (parameter)

$f_0(y)$
$f_1(y, x_0)$
$\vdots$
$f_{n-2}(y, x_0, \ldots, x_{n-4}, x_{n-3})$
$f_{n-1}(y, x_0, \ldots, \ldots, x_{n-3}, x_{n-2})$

Non strict T-function

$f_0(y, x_0, \ldots, x_{n-2}, x_{n-1})$
$f_1(y, x_0, \ldots, x_{n-2}, x_{n-1})$
$\vdots$
$f_{n-2}(y, x_0, \ldots, x_{n-2}, x_{n-1})$
$f_{n-1}(y, x_0, \ldots, x_{n-2}, x_{n-1})$



strict T-function (parameter)

$$f_0(y)$$
$$f_1(y, x_0)$$
$$\vdots$$
$$f_{n-2}(y, x_0, \ldots, x_{n-4}, x_{n-3})$$
$$f_{n-1}(y, x_0, \ldots, \ldots, x_{n-3}, x_{n-2})$$

Non strict T-function

$$f_0(y, x_0, \ldots, x_{n-2}, x_{n-1})$$
$$f_1(y, x_0, \ldots, x_{n-2}, x_{n-1})$$
$$\vdots$$
$$f_{n-2}(y, x_0, \ldots, x_{n-2}, x_{n-1})$$
$$f_{n-1}(y, x_0, \ldots, x_{n-2}, x_{n-1})$$

Self-synchronization

Definition (Self-Synchronizing sequence)

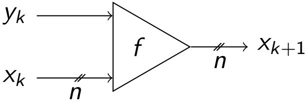
A sequence (y) is self-synchronizing with respect to f if there exists an integer k_y so that for all initial state x_0 and $\widehat{x}_0$

$$\forall k \geq k_y, \; x_k = \widehat{x}_k$$

Definition (Finite time self-synchronization)

The function f is finite time self-synchronizing if the minimum value k_y is upper bounded when (y) stands in the set of all input sequences. The upper bound is called the self-synchronization delay of f.

Self-Synchronizing Stream Ciphers
Equations



Decomposition of the next-state function

$$f^0, f^1 : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^n$$

$$f(y_k, x_k) = \begin{cases} f^0(x_k) \text{ if } y_k = 0 \\ f^1(x_k) \text{ if } y_k = 1 \end{cases} \quad (1)$$

Iterated function

$$\begin{aligned} \phi_i(y, x_0) &= f(y_i, f(y_{i-1}, f(\ldots, f(y_0, x_0) \cdots))) \\ &= f^{y_i} \circ f^{y_{i-1}} \circ \cdots \circ f^{y_1} \circ f^{y_0}(x_0) \end{aligned} \quad (2)$$

Spectral Analysis

Walsh Transform (of a Boolean function $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$)

$$\forall v \in \mathbb{F}_2^n,\ \widehat{f_\chi}(v) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) + x \cdot v} \tag{3}$$

Walsh Matrix (of a vectorial Boolean function $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^m$)

$$\forall u \in \mathbb{F}_2^m,\ v \in \mathbb{F}_2^n,\ w_{u,v}^f = \sum_{x \in \mathbb{F}_2^n} (-1)^{u \cdot f(x) + v \cdot x} \tag{4}$$

Composition of vectorial Boolean functions

$$W_{f \circ g} = \frac{1}{2^n} W_f \times W_g \tag{5}$$

Outline

The system is self-synchronizing with synchronization delay $i+1$

$$\Longleftrightarrow$$

The function $\phi_i(y, x_0)$ is constant with respect to x_0 (or the function $\phi_i^y(x_0)$ is constant)

Walsh matrix of ϕ_i restricted to a sequence $y \in \mathbb{F}_2^{i+1}$

$$W_{\phi_i^y} = \frac{1}{2^{n \cdot i}} W_{f^{y_i}} \times \cdots \times W_{f^{y_0}} \tag{6}$$

Walsh matrix of a constant function

$$\begin{pmatrix} 2^n & 0 & \cdots & 0 \\ \pm 2^n & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ \pm 2^n & 0 & \cdots & 0 \end{pmatrix}$$

Finite time self-synchronization

$$W_{f^0} = \begin{pmatrix} 2^n & 0 & \cdots & 0 \\ w_{2,1} & w_{2,2} & \cdots & w_{2,2^n} \\ \vdots & \vdots & & \vdots \\ w_{2^n,1} & w_{2^n,2} & \cdots & w_{2^n,2^n} \end{pmatrix} \quad W_{f^1} = \begin{pmatrix} 2^n & 0 & \cdots & 0 \\ w_{2,1} & w_{2,2} & \cdots & w_{2,2^n} \\ \vdots & \vdots & & \vdots \\ w_{2^n,1} & w_{2^n,2} & \cdots & w_{2^n,2^n} \end{pmatrix}$$

$W^*_{f^0}$ $W^*_{f^1}$

Conditions on W_{f^0} and W_{f^1}

Finite time self-synchronization

$\Longleftrightarrow$

$W^*_{f^0}$ and $W^*_{f^1}$ generate a nilpotent semigroup.

Nilpotent reduced Walsh matrix

Nilpotent deduced Walsh matrix

- Triangular reduced Walsh matrix $\Leftrightarrow$ strict T-function
- Levitzky: Any semigroup of nilpotent operators is triangularizable

Three kinds of nilpotent Walsh matrices

1. those which are already triangular f_T
2. those that can be triangularized by a change of basis whose matrix is a Walsh matrix $(b \circ f_T \circ b^{-1})$
3. those that cannot be triangularized with such a matrix

Remark

If two reduced Walsh matrices W^*_{f0}, W^*_{f1} span a nilpotent semigroup of nilpotency class greater than n, it necessary corresponds to Case 3.

Outline

Let $f : \mathbb{F}_2 \times \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^n$ $(n = 3)$ be,

$$f(y,x) = (y+1)f^0(x) + yf^1(x)$$

with

$$\begin{cases} f_0^0(x) = & x_1 + x_0x_1 + x_2 + x_0x_2 \\ f_1^0(x) = & x_1 + x_0x_1 + x_0x_2 + x_1x_2 + x_0x_1x_2 \\ f_2^0(x) = & x_2 + x_0x_2 \end{cases}$$

and

$$\begin{cases} f_0^1(x) = & x_0x_1 + x_0x_2 + x_1x_2 \\ f_1^1(x) = & x_2 + x_0x_1x_2 \\ f_2^1(x) = & x_1x_2 \end{cases}$$

The class of nilpotency of the semigroup generated by $W_{f^0}^*$ and $W_{f^1}^*$ is $\mathcal{C} = 4 > n$. It can only be achieved in Case 3.

Outline

Extension to statistical self-synchronization

Definition (Statistical self-synchronization)

A function f is statistically self-synchronizing if $\lim_{k \to +\infty} \text{Prob}(K_Y \leq k) = 1$, where K_Y is the random synchronization delay for the random sequence (Y).