Hybrid architecture of LPV dynamical systems in the context of cybersecurity

Hamid Boukerrou[1] Gilles Millerioux[1] Marine Minier [2]

1. Centre de Recherche en Automatique de Nancy
2. Laboratoire Lorrain de Recherche en Informatique et ses Applications

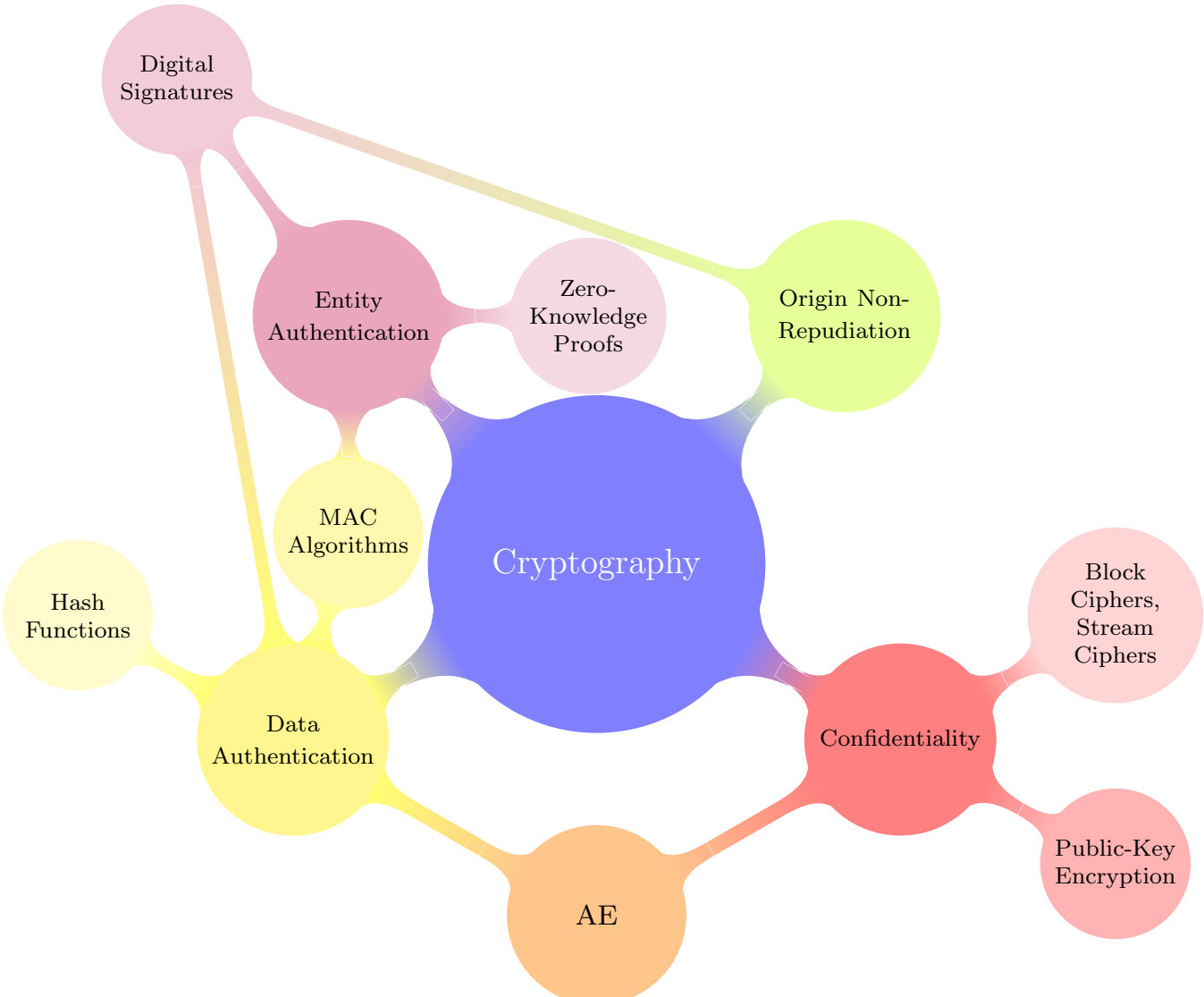
Days of Departement Algorithms, Computation, Image and Geometry

June 17, 2021

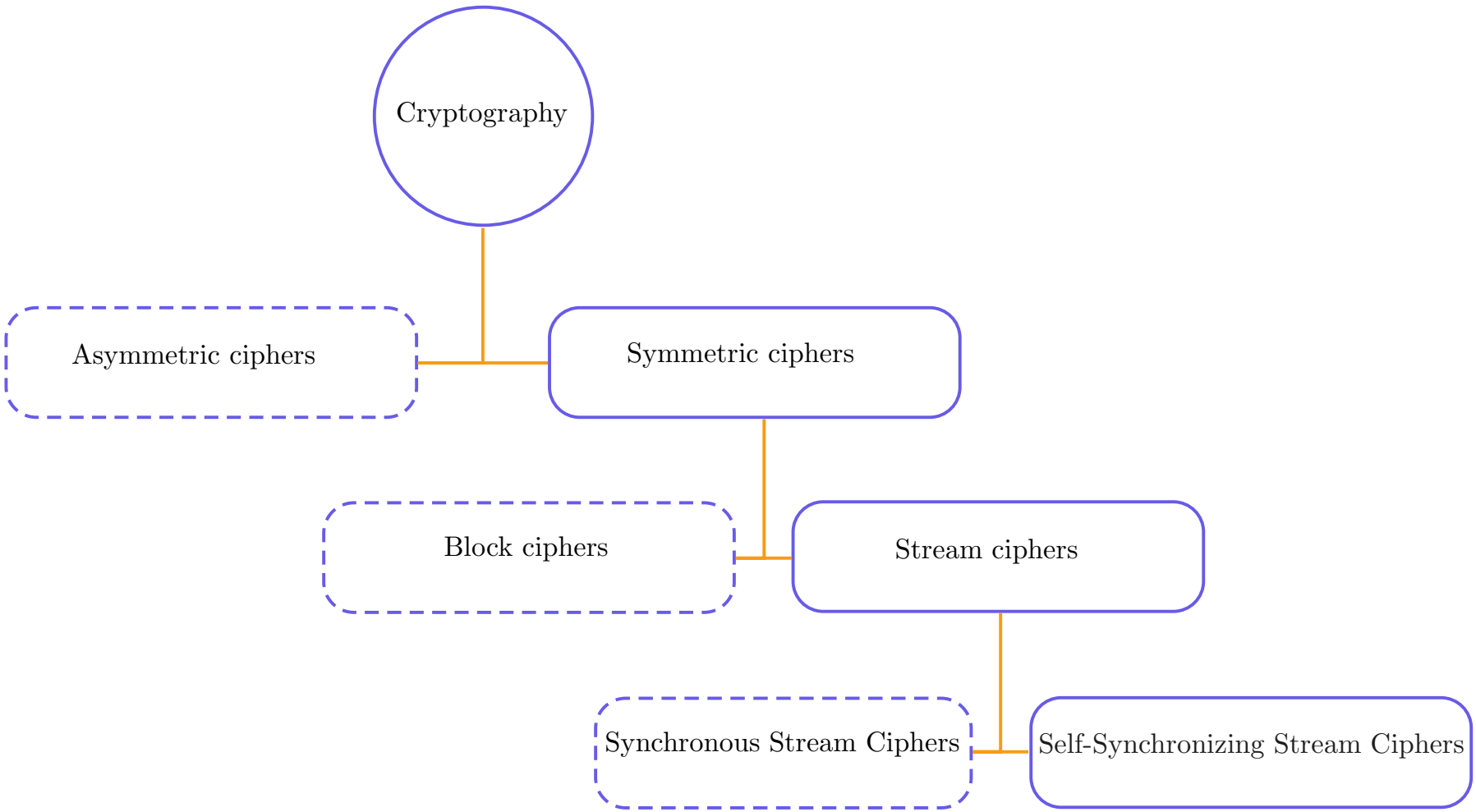
Overview

1. Cryptography
2. Generalities on stream ciphers
3. Self-synchronizing stream ciphers & Linear Parameter Varying (LPV) systems
4. Design of a hybrid architecture for a statistical Self-Synchronizing Stream Ciphers

Cryptography

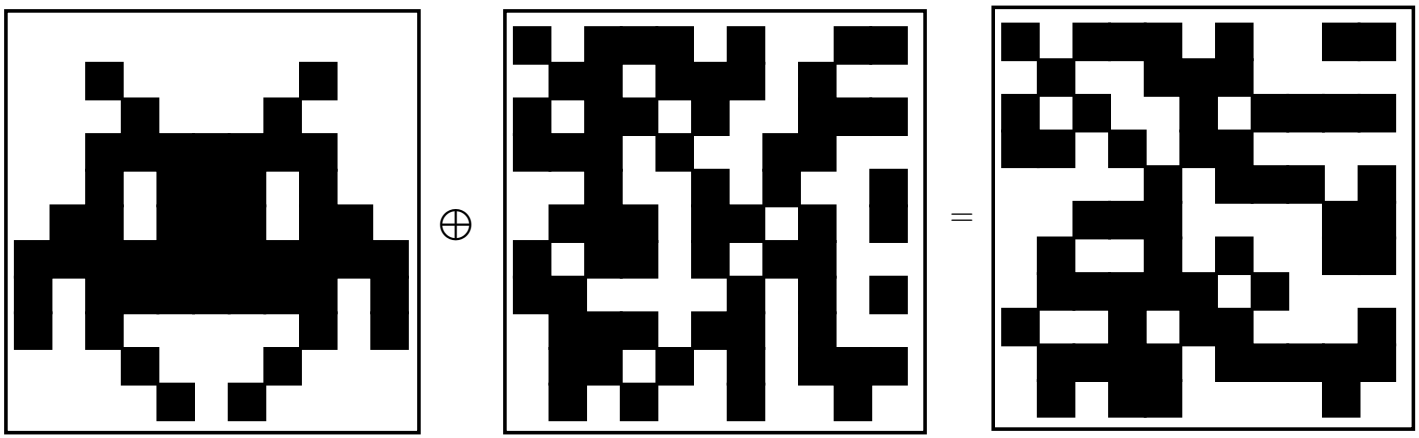


Stream ciphers



Vernam cipher (One Time Pad)

- An encryption technique that cannot be broken (encryption 100% sure).

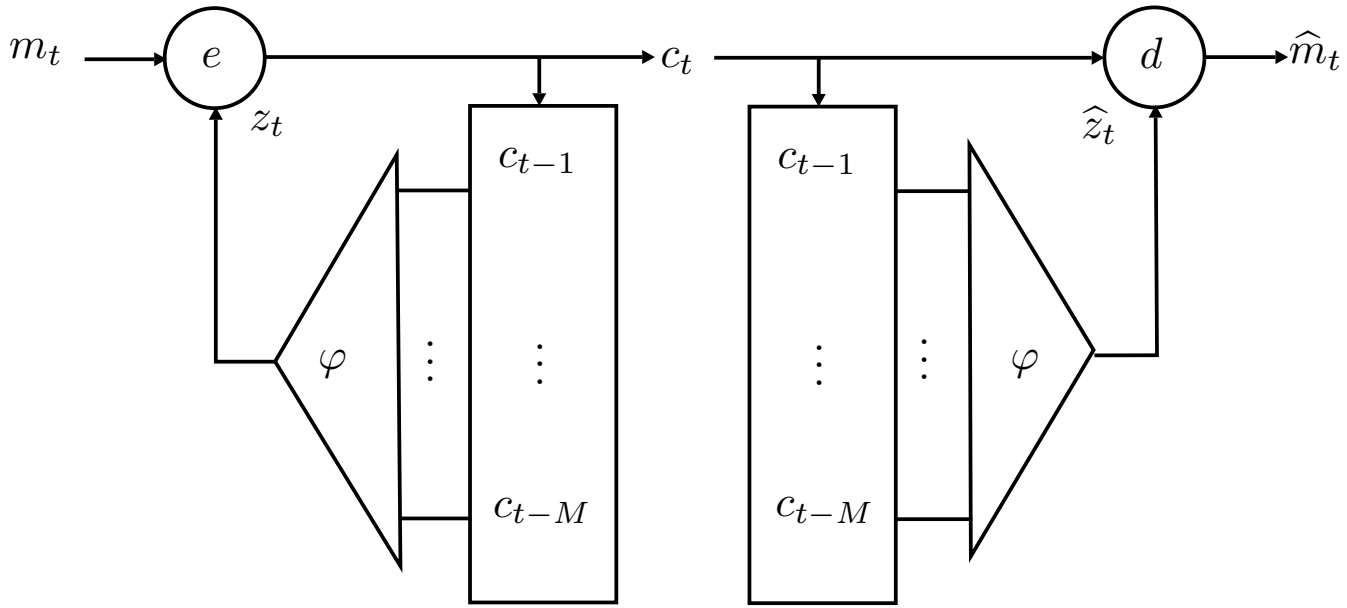


Plaintext Key Ciphertext

The key must:

- never be reused.
- be truly random.
- be at least as long as the plaintext.

Self-Synchronizing Stream Cipher (SSSC) [Maurer. 1991]



- Ciphering equation:

$$\begin{cases} z_t = \varphi(c_{t-l-M+1}, \ldots, c_{t-l}), \\ c_t = e(z_t, m_t) \end{cases}$$

- Deciphering equation:

$$\begin{cases} \widehat{z}_t = \varphi(c_{t-l-M+1}, \ldots, c_{t-l}), \\ \widehat{m}_t = d(\widehat{z}_t, c_t) \end{cases}$$

- HBB [Palash Sarkar. 2003], SSS [P.Hawkes, M.Paddon et al. 2004], Moustique [J.Daemen and P.Kitsos. 2005], Stanislas [G.Millerioux, M.Minier et al. 2020].

Flatness

$$S : \begin{cases} x_{t+1} = f(x_t, m_t), \\ c_t = h(x_t, m_t) \end{cases}$$

Definition

The system (S) is said to be flat if there exists a variable c_t, called a flat output, such that all system variables can be expressed as a function of the flat outputs and a finite number of its backward and forward shifts. In other words, there exist two functions F and G such that:

$$\begin{cases} x_t = F(c_{t+s_1}, \ldots, c_{t+s'_1}), \\ m_t = G(c_{t+s_2}, \ldots, c_{t+s'_2}) \end{cases}$$

where s_1 , s'_1 , s_2 and $s'_2 \in \mathbb{Z}$.

LPV system (Linear Parameter Varying) Single Input Single Output

- Ciphering Side:

$$\Sigma_\rho \begin{cases} x_{t+1} = A_{\rho(t)} x_t + B_{\rho(t)} m_t \\ c_t = C_{\rho(t)} x_t + D_{\rho(t)} m_t \end{cases} \tag{1}$$

where m_t, $c_t \in \mathbb{F}$ and $\mathbb{F}$ a finite field.

- A is the dynamical matrix:

$$A_{\rho(t)} = \begin{pmatrix} & 1 & & & & 1 & & \\ 1 & \rho^1(t) & 1 & & & & \rho^2(t) & \\ & & & 1 & & & & \\ & & & & \rho^3(t) & & & \\ 1 & \rho^4(t) & \rho^5(t) & & & 1 & & \rho^6(t) \\ & & & & & & 1 & \\ & & & & & & & 1 \\ \rho^7(t) & 0 & \rho^8(t) & 1 & 0 & \rho^9(t) & 0 & 0 \end{pmatrix}$$

Stanislas[G.Millerioux, M.Minier et al. 2020]: $\rho^i(t) \rightarrow$ S-box$(c_t, c_{t-1}, \ldots, c_{t-s}, K_i)$.

Characterization of flatness

- Ciphering equation:

$$\begin{cases} x_{t+1} = A_{\rho(t)} x_t + B_{\rho(t)} m_t, \\ c_{t+1} = C_{\rho(t)} x_t \end{cases}$$

- Deciphering equation:

$$\begin{cases} \widehat{x}_{t+1} = P_{\rho(t)} \widehat{x}_t + B c_t, \\ \widehat{m}_t = C_{\rho(t)} A_{\rho(t)} \widehat{x}_t + c_t \end{cases}$$

Where

$$P_{\rho(t)} = A_{\rho(t)} - BC \prod_{l=t+K}^{t} A_{\rho(l)}$$

- Synchronization equation: $\varepsilon_t = \hat{x}_{t+r} - x_t$

$$\varepsilon_{t+M} = P_{\rho(t+M)} P_{\rho(t+M-1)} \cdots P_{\rho(t)} \cdot \varepsilon_t$$

- We can show that if an LPV system is flat then: $\exists M \in \mathbb{N}, t \geq 0, \varepsilon_{t+M} = 0$ then

$$P_{\rho(t+M)} P_{\rho(t+M-1)} \cdots P_{\rho(t)} = 0$$

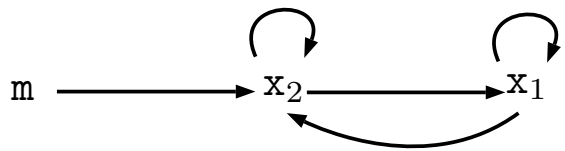
So, $x_t = \hat{x}_t$ and $m_t = \hat{m}_t$

How to construct a flat system ?

- Issue: Mortality problem (NP-Hard).
- Graph-oriented approach.

Complexity and security

- Graph-oriented approach:



- State space equation of the LPV system:

$$\Sigma_\rho \begin{cases} x_{t+1} = A_{\rho(t)} x_t + B_{\rho(t)} m_t \\ c_t = C_{\rho(t)} x_t + D_{\rho(t)} m_t \end{cases} \qquad A_\rho(t) = \begin{pmatrix} 1 & 1 \\ 1 & \rho(t) \end{pmatrix}, B = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, C = \begin{pmatrix} 0 & 1 \end{pmatrix}$$

- Security $\rightarrow$ diffusion delay.

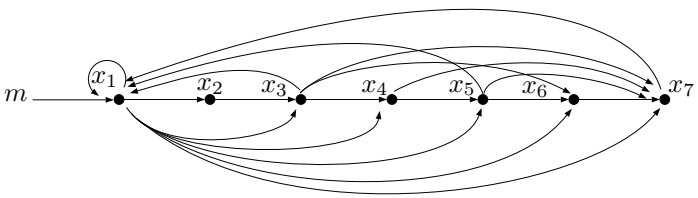
Definition (Diffusion delay)

Let p denotes the power of a matrix $Z \in M_n(\mathbb{F})$. Diffusion delay is the smallest value, denoted by d_0, of p such that Z^p does not have any zero coefficient.

The more the integers n (dimension) and n_a (number of edges), the more the security.

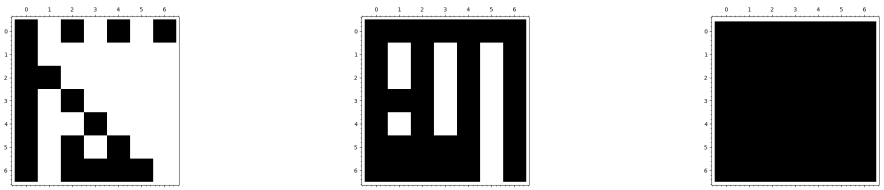
Diffusion delay

- The graph corresponds to a flat structured LPV system. (dimension: $n = 7$, edges: $na = 15$)



$$A = \begin{pmatrix} 1 & 0 & \rho(t) & 0 & \rho(t) & 0 & \rho(t) \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & \rho(t) & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}$$

- Powers of A^p with $p \in [1,3]$.

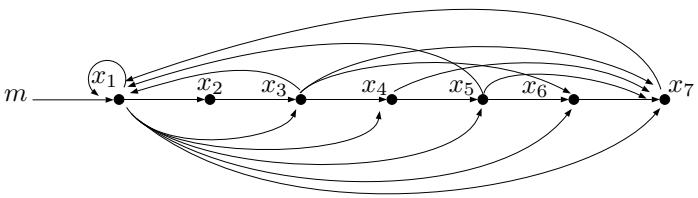


(a) A (b) A^2 (c) A^3

- Black squares represent diffusion $\rightarrow$ good diffusion.

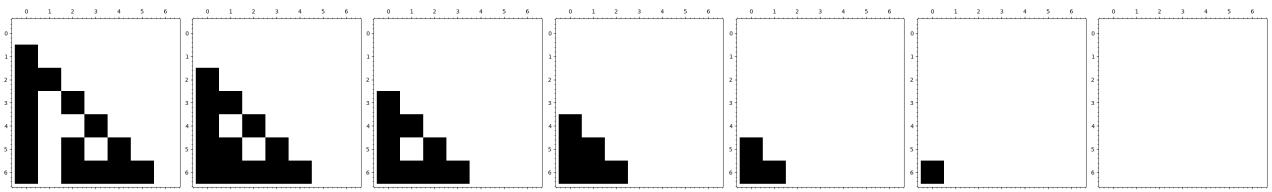
Diffusion delay

- The graph corresponds to a flat structured LPV system. (dimension: $n = 7$, edges: $na = 15$)



$$P = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & \rho(t) & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}$$

- Powers of P^p with $p \in [1, 7]$.

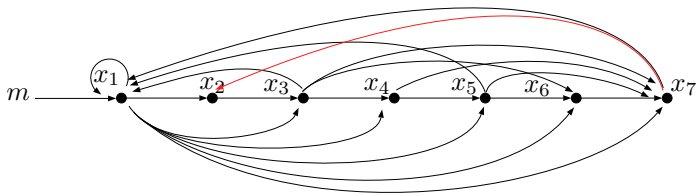


(a) P (b) P^2 (c) P^3 (d) P^4 (e) P^5 (f) P^6 (g) P^7

- Black squares represent diffusion $\rightarrow$ bad diffusion & triangular.

Diffusion delay

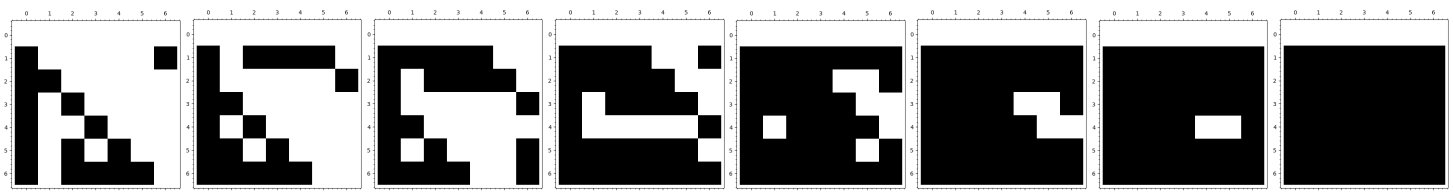
- The graph corresponds to a not-flat structured LPV system. (dimension: $n = 7$, edges: $na = 15$)



$$\begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & \rho(t) & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix} \rightarrow \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & \rho(t) & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}$$

A P

- Powers of P^p with $p \in [1, 7] \rightarrow$ good diffusion & non-triangular.

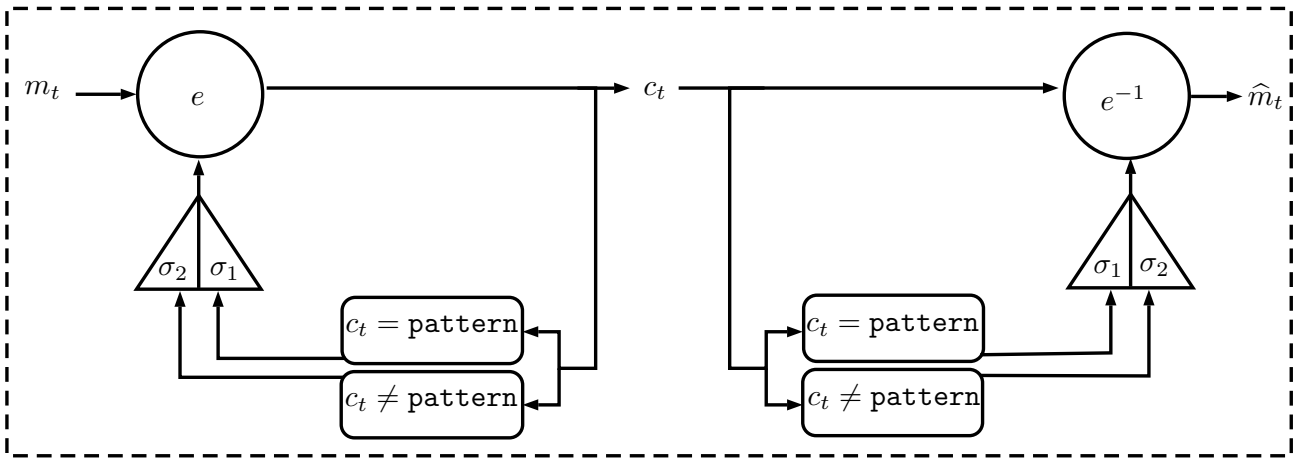


(a) P (b) P^2 (c) P^3 (d) P^4 (e) P^5 (f) P^6 (g) P^7 (h) P^8

A statistical self-synchronizing hybrid architecture

[H.boukerrou, G.Millerioux and M.Minier. LPVS'21]

The hybrid architecture with switching rule σ obeys the following state space representation at the:



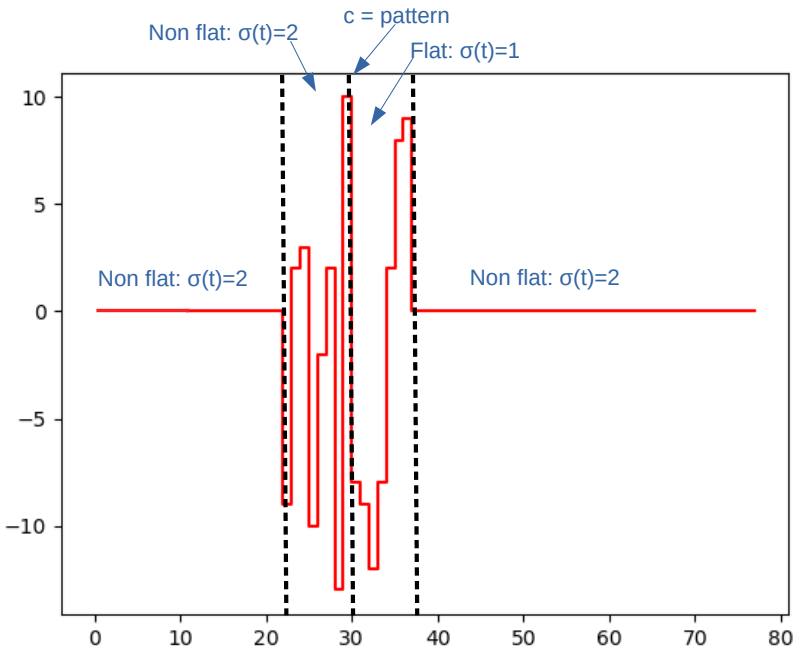
$\sigma(t) = 1$:

- the dynamical system is flat.
- the system gets the self-synchronization property.
- diffusion is not optimal.

$\sigma(t) = 2$:

- the dynamical system is not flat.
- the system does not get the self-synchronization property.
- diffusion is much more significant.

Proof-of-Concept Example

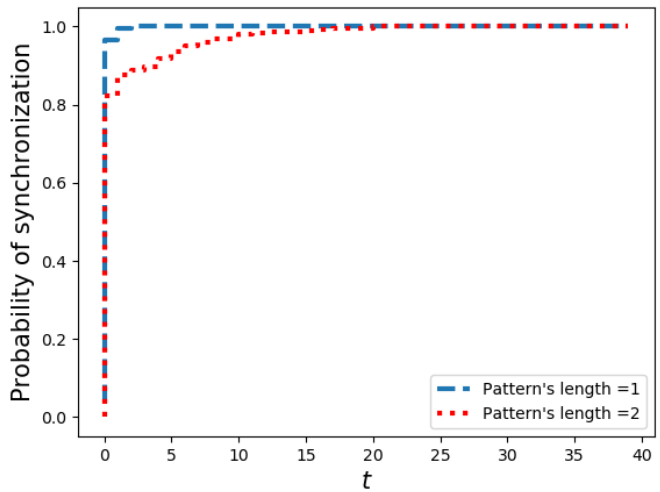


Time evolution of the error $m_t - \hat{m}_{t+1}$

- $t > 0$: synchronization $\rightarrow$ cipher and the decipher $\rightarrow \sigma(t) = 2$.
- $t = 21$: introduce a disturbance into the cryptogram.
- $t = 30$: $c_t = \textit{pattern} \rightarrow \sigma(t) = 1$.
- $t > 37$: both the cipher and the decipher switch on mode $\sigma(t) = 2$.

A statistical self-synchronizing hybrid architecture

- An LPV system is statistical self-synchronizing if ,
$\lim_{t \to +\infty} Pr[x_t = \hat{x}_t] = 1$



successful resynchronizations after a time t

- Statistical VS Deterministic:

	Deterministic	Statistical
Synchronization	++	+
Security	+	++

Conclusion & further work: Multiple Input Multiple Output (MIMO)

In progress...

- Construction of MIMO
- Security of MIMO

Thank You!