Synchronization of complex dynamics: when control theory enters the scene of cryptography

Gilles Millérioux

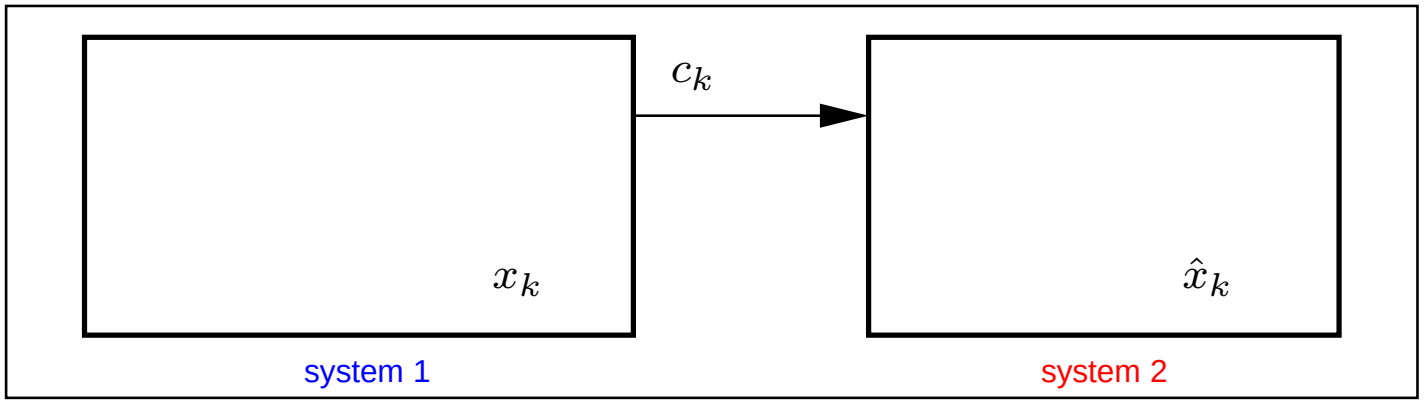
Université Henri Poincaré (Nancy, France)

Centre de Recherche en Automatique de Nancy

Outline

- Synchronization of complex dynamics
- Polytopic formulation
- Control theory and cryptography
- Video

Self-synchronization

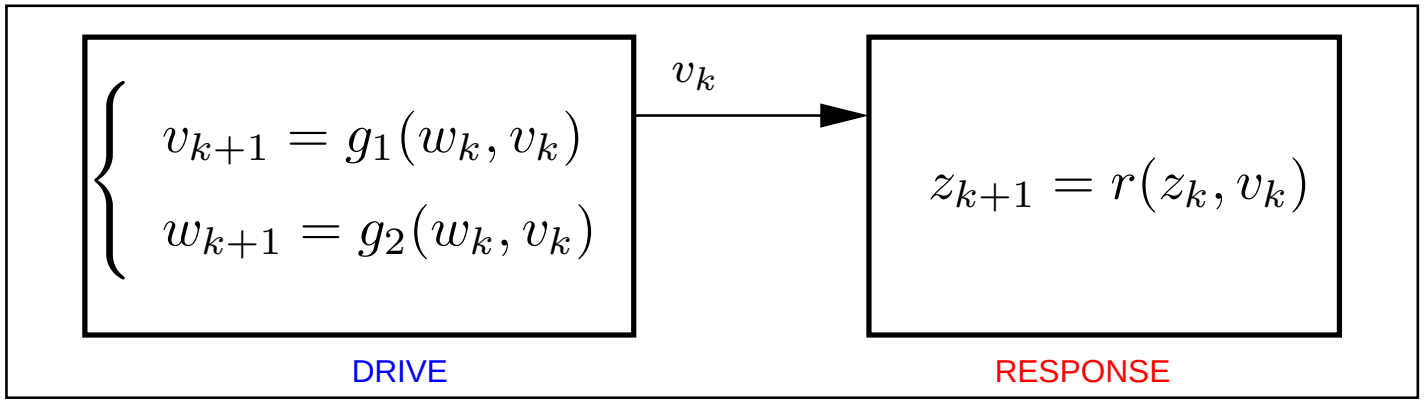


Definition: Systems 1 and 2 are self-synchronized if there exists a function f so that $f(x_k, \hat{x}_k) = 0$ without the help of any external signal forcing system 2 but the coupling c_k

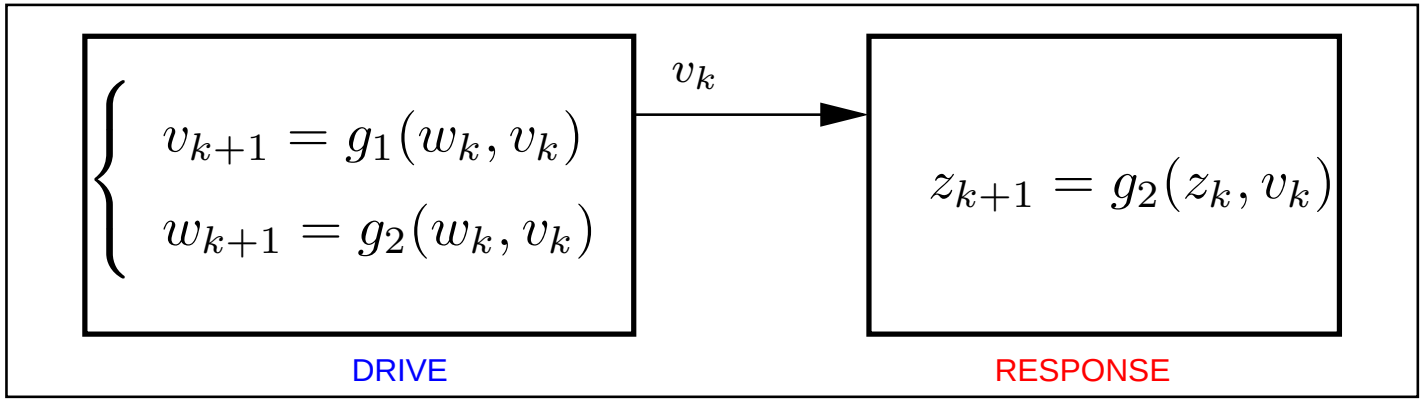
$\Rightarrow$ for example $\|x_k - \hat{x}_k\| = 0$ or $\|x_k - \hat{x}_{k+r}\| = 0$

Self-synchronization

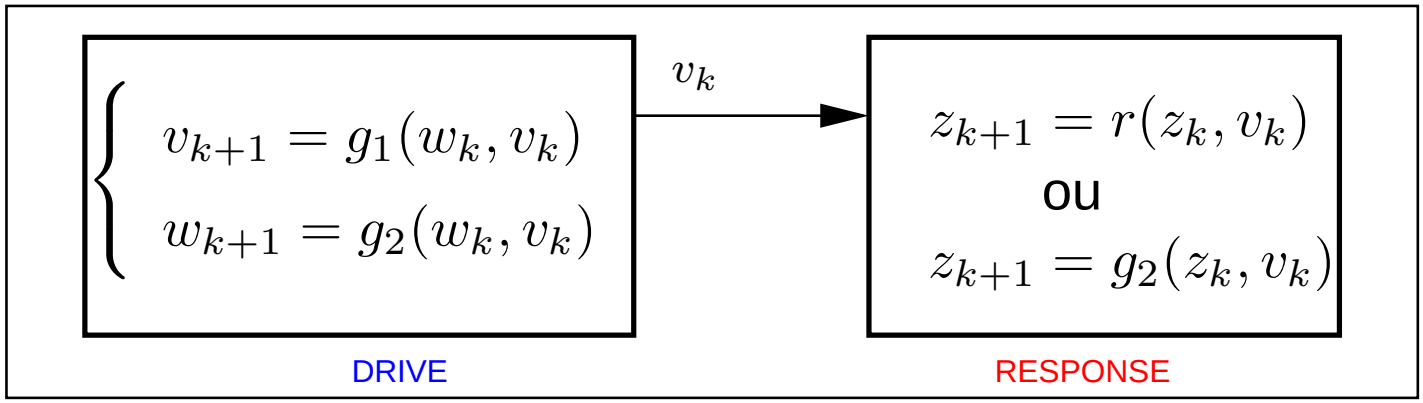
- heterogeneous configuration ($r \neq g_2$)



- homogeneous configuration ($r = g_2$)



Self-synchronization

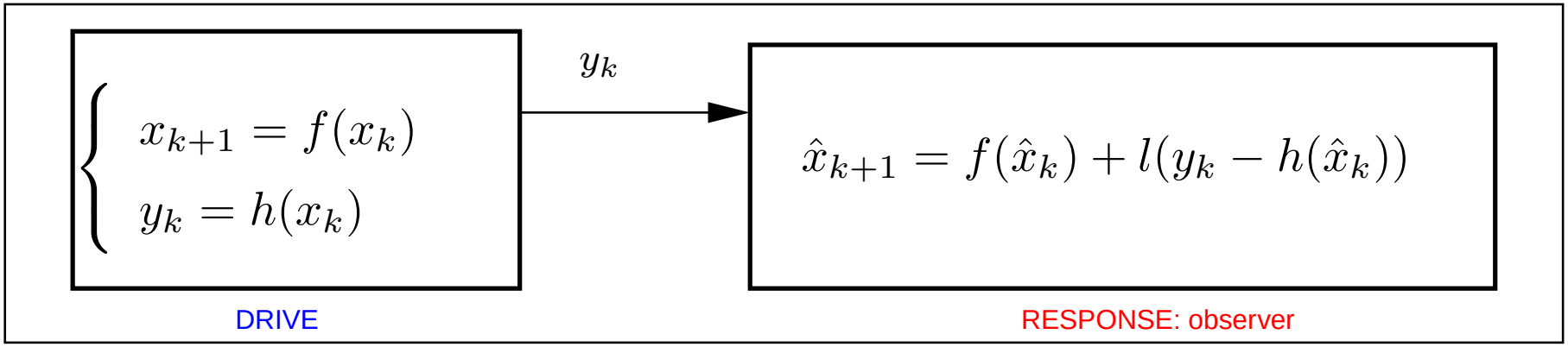


Chaos synchronization issue (first formulation)

- finding out r or $g_{1,2}$ of the DRIVE
- finding out a drive signal v_k

$$\lim_{k \to \infty} \|z_k - w_k\| = 0$$

Self-synchronization

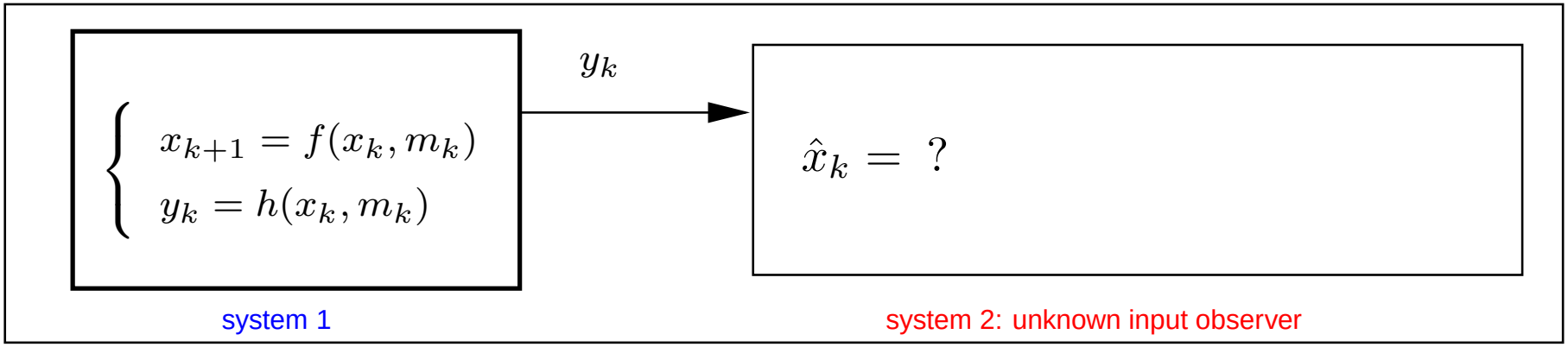


Chaos synchronization issue (observer formulation)

- finding out a function l
- finding out an output y_k

$$\lim_{k \to \infty} \|\hat{x}_k - x_k\| = 0$$

Self-synchronization

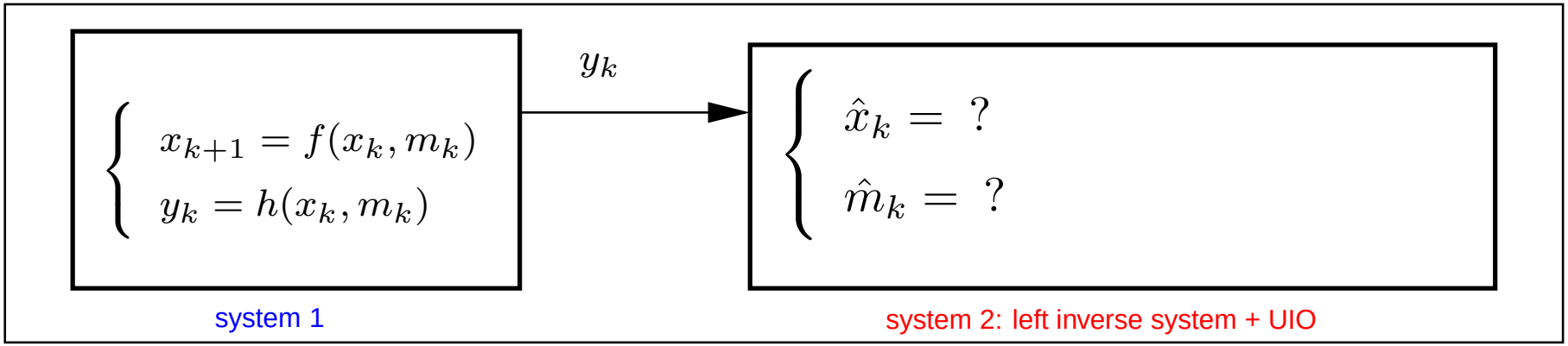


Finite time self-synchronization with unknown inputs

- finding out a system 2
- finding out an appropriate output y_k

$$\exists k_f < \infty, \quad \forall \hat{x}_0 \in U, \forall k > k_f \quad \text{and} \quad \forall m_k \ s.t \ \|x_k - \hat{x}_k\| = 0$$

Self-synchronization



Finite time self-synchronization with unknown inputs

- finding out a system 2
- finding out an appropriate output y_k

$$\exists k_f < \infty, \quad \forall \hat{x}_0 \in U, \forall k > k_f \quad \text{and} \quad \forall m_k \ s.t$$

$$\|x_k - \hat{x}_k\| = 0 \text{ and } \|\hat{m}_k - m_k\| = 0$$

Polytopic formulation

Nancy-Université

- Switched linear systems (Tent Map, Lozi Map)

$$\begin{cases} x_{k+1} &= A_i x_k \\ y_k &= C x_k \end{cases}$$

- Polynomial systems (Henon Map, Burger Map)

$$\begin{cases} x_{k+1} &= p(x_k, x_k^2, \ldots, x_k^{n-1}) x_k \\ y_k &= C x_k \end{cases}$$

$$\Leftrightarrow$$

LPV system with $\rho_k = h(x_k)$

$$\begin{cases} x_{k+1} &= \mathcal{A}(\rho_k) x_k \\ y_k &= C x_k \end{cases}$$

$\Rightarrow$ Polytopic observers with LMI-based design

Polytopic formulation

Nancy-Université

Polytopic decomposition principle: example

Drive system

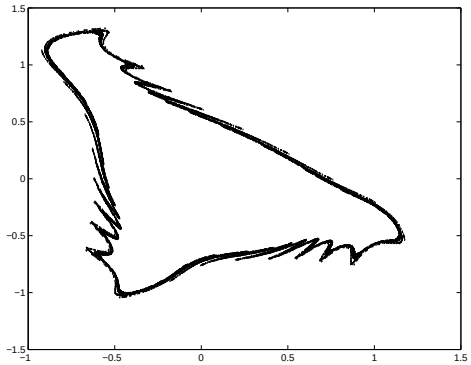
$$\begin{cases} v_{k+1} = -w_k + \alpha(-0.78v_k - 0.28v_k^2 + 0.98v_k^2 \cdot w_k(1 - v_k^2)) \\ w_{k+1} = (1 + 0.12\alpha)w_k \end{cases}$$

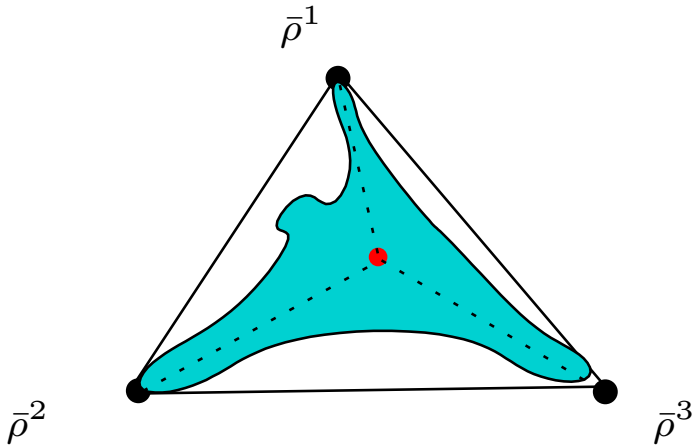
$$x_{k+1} = \begin{bmatrix} \alpha(-0.78 - 0.28v_k) & -1 + \alpha 0.98v_k^2 \cdot (1 - v_k^2)) \\ 0 & (1 + 0.12\alpha) \end{bmatrix} x_k$$

$$= \begin{bmatrix} \rho_k^1 & \rho_k^2 \\ 0 & (1 + 0.12\alpha) \end{bmatrix} x_k$$

with $x_k = [v_k \;\; w_k]^T$

Polytopic formulation





$$\Rightarrow \quad \rho_k = \sum_{i=1}^{3} \xi_k^i(\rho_k)\bar{\rho}^i$$

with $\sum_{i=1}^{3} \xi_k^i = 1$ and $\xi_k^i \geq 0$

$$\Rightarrow f(x_k) = \mathcal{A}(\rho_k)x_k = \sum_{i=1}^{N} \xi_k^i A_i x_k$$

Polytopic formulation

Nancy-Université

Recall of the general description ($\epsilon_k = x_k - \hat{x}_k$)

$$\epsilon_{k+1} = f(x_k) - f(\hat{x}_k) - l(y_k - h(\hat{x}_k))$$

Polytopic description (strictly equivalent)

$$\epsilon_{k+1} = \sum_{i=1}^{N} \xi_k^i A_i x_k - \sum_{i=1}^{N} \xi_k^i A_i \hat{x}_k - \sum_{i=1}^{N} \xi_k^i L_i C(x_k - \hat{x}_k)$$

The state reconstruction error obeys

$$\epsilon_{k+1} = \sum_{i=1}^{N} \xi_k^i (A_i - L_i C)\epsilon_k$$

$\Rightarrow$ stability of LPV polytopic systems

Polytopic formulation

Theorem 1 *ϵ_k globally converges to zero if there exist some symmetric matrices P_i, matrices G_i and F_i such that, $\forall (i,j) \in \{1,\ldots,N\} \times \{1,\ldots,N\}$, the following set of Linear Matrix Inequalities is feasible*

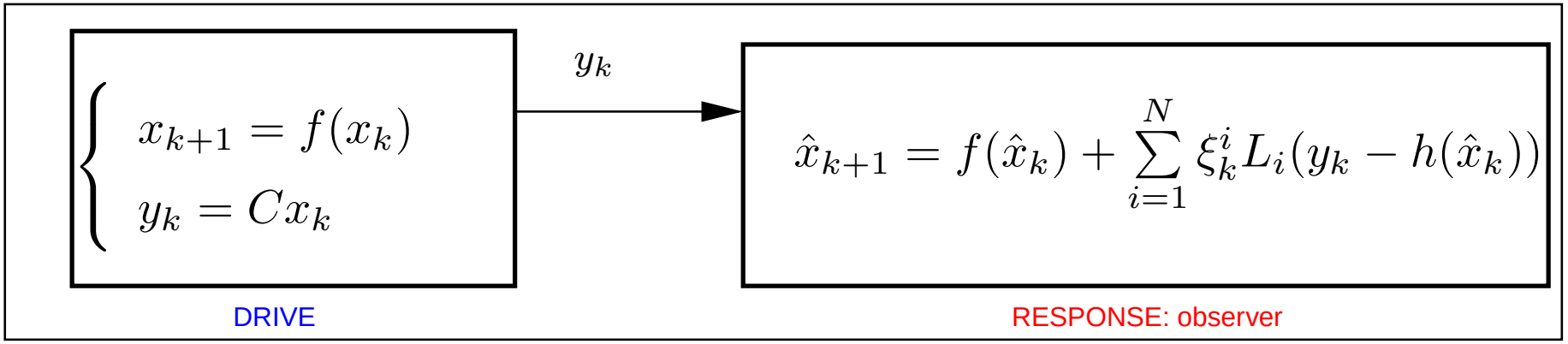
$$\begin{bmatrix} P_i & (G_i A_i - F_i C)^T \\ G_i A_i - F_i C & G_i + G_i^T - P_j \end{bmatrix} > 0 \qquad (1)$$

and $L_i = G_i^{-1} F_i$

The LMIs ensure the existence of a Lyapunov function $V : \mathbb{R}^n \to \mathbb{R}^+$ which fulfills :

$$V(\epsilon_{k+1}) - V(\epsilon_k) < 0 \quad \forall\, k \qquad (2)$$

Self-synchronization



Chaos synchronization issue (polytopic formulation)

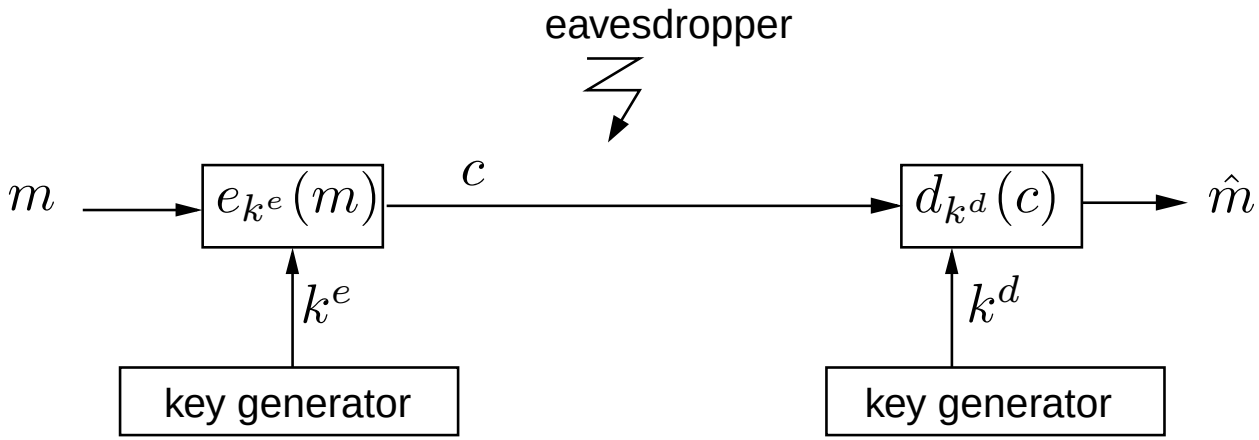
- finding out gains L_i (solving tractable LMIs)
- finding out a matrix C

$$\lim_{k \to \infty} \|\hat{x}_k - x_k\| = 0$$

Control concepts and ciphering

Nancy-Université

General ciphering setup



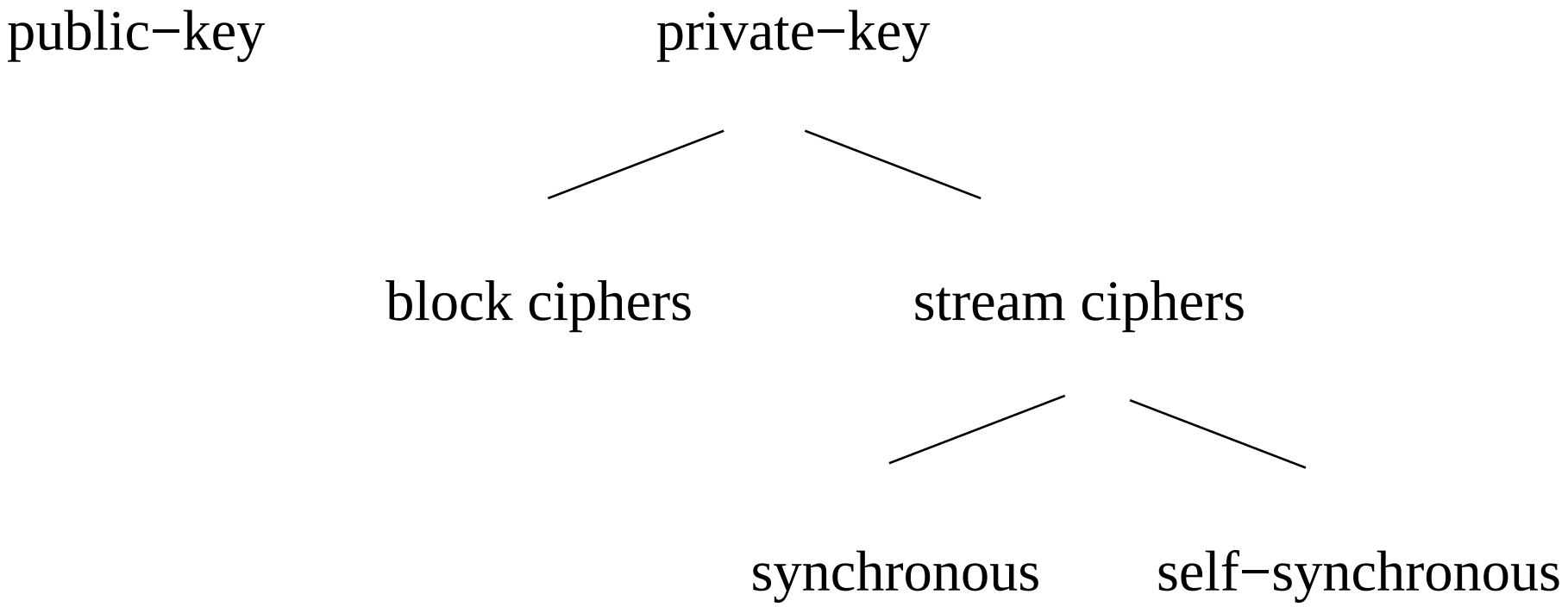
Cryptography must guarantee at least:

- confidentiality

Control concepts and ciphering

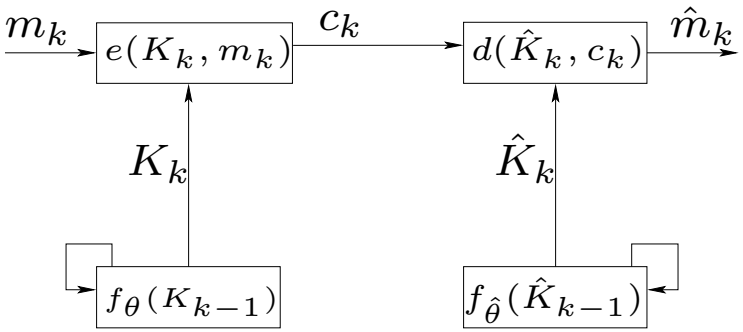
Nancy-Université

Classes of ciphers



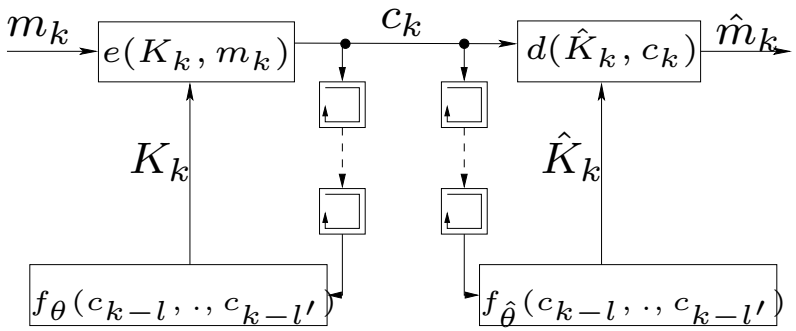
Control concepts and ciphering

Stream ciphers



Synchronizing Stream Cipher (SSC)

$$\begin{cases} K_k = f_\theta(K_{k-1}) \\ c_k = e(K_k, m_k) \end{cases}$$



Self Synchronizing Stream Cipher (SSSC)

$$\begin{cases} K_k = g_\theta(c_{k-l}, \ldots, c_{k-l'}) \\ c_k = e(K_k, m_k) \end{cases}$$

Control concepts and ciphering

Nancy-Université

Relative degree, left invertibility

$$\begin{cases} x_{k+1} = f_\theta(x_k, m_k) \\ y_k = h_\theta(x_k, [m_k]) \end{cases} \tag{3}$$

The relative degree of the system with respect to the quantity m_k is the required number r of iterations of the output y_k so that y_{k+r} depends on m_k which actually appears explicitly in the expression of y_{k+r}

$$\begin{aligned} y_{k+r} &= h(f_\theta^r(x_k, m_k)) \text{ for } r > 1 \\ &= h(x_k, m_k) \text{ for } r = 0 \end{aligned} \tag{4}$$

The dynamical system is left invertible if there exists a nonnegative integer $R < \infty$, called *inherent delay*, so that for any two inputs m_k and m'_k and any state x_k the following inference holds:

$$\begin{aligned} &h^{(0)}(x_k, m_k) \cdots h^{(R)}(x_k, m_k \cdots m_{k+R}) = h^{(0)}(x_k, m'_k) \cdots h^{(R)}(x_k, m'_k \cdots m'_{k+R}) \\ &\Rightarrow m_k = m'_k. \end{aligned} \tag{5}$$

Control concepts and ciphering

Flatness

$$\begin{cases} x_{k+1} = f_\theta(x_k, m_k) \\ y_k = h_\theta(x_k, [m_k]) \end{cases} \tag{6}$$

The system with dynamics f, input m_k and state vector x_k of dimension n is said to be flat if there exists an output y_k, referred to as a flat output, such that all system variables can be expressed as a function of the flat output and a finite number of its backward and/or forward iterates.

$$\begin{cases} x_k &= \mathcal{F}_\theta(y_{k+k_1}, \ldots, y_{k+k'_1}) \\ m_k &= \mathcal{G}_\theta(y_{k+k_2}, \ldots, y_{k+k'_2}) \end{cases} \tag{7}$$

Control concepts and ciphering

If the DRIVE has $r < \infty$, $R < \infty$ and is *flat*

DRIVE $\Leftrightarrow$ SSSC

$$\begin{array}{rcl} x_{k+1} & = & f_\theta(x_k, m_k) \\ y_k & = & h(x_k, [m_k]) \end{array} \quad \Leftrightarrow \quad \begin{array}{rcl} x_k & = & \mathcal{F}_\theta(y_{k+k_1}, \ldots, y_{k+k'_1}) \\ y_{k+r} & = & h(f_\theta^r(x_k, m_k))) = l(x_k, m_k) \end{array}$$

Identifying with

$$\begin{cases} K_k = g_\theta(c_{k-l}, \ldots, c_{k-l'}) \\ c_k = e(K_k, m_k) \end{cases}$$

gives

- key generator $g_\theta = \mathcal{F}_\theta$
- running key $K_k = x_k$,
- ciphertext $c_k = y_{k+r}$
- encrypting function $e = l$

Conclusion

- Observer-based approaches for self-synchronization
- Polytopic formulation defines an appropriate and general framework for chaotic systems
- Dynamical systems make sense in cryptography when defined over a finite field under the flatness condition

References

F. Anstett, G. Millérioux, and G. Bloch. Chaotic cryptosystems: Cryptanalysis and identifiability. *IEEE Trans. on Circuits and Systems : Regular papers*, 53(12):2673–2680, December 2006.

G. Millérioux, J. M. Amigó, and J. Daafouz. A connection between chaotic and conventional cryptography. *IEEE Trans. on Circuits and Systems I: Regular Papers*, 55(6), July 2008.

G. Millérioux and P. Guillot. Self-synchronizing stream ciphers and dynamical systems: state of the art and open issues. *International Journal of Bifurcation and Chaos*, 20(9), September 2010.

P. Vo Tan, G. Millérioux, and J. Daafouz. Left invertibility, flatness and identifiability of switched linear dynamical systems: a framework for cryptographic applications. *International Journal of Control*, 83(1):145–153, January 2010.