



# Modèles discrets pour la sécurité informatique : des méthodes itératives à l'analyse vectorielle.

Jean-François COUCHOT  
Soutenance d'HDR : le 30/01/16

## Rapporteurs :

Olivier BOURNEZ  
Jean-Paul COMET  
Juan-Pablo ORTEGA

Professeur à l'Ecole Polytechnique.  
Professeur à l'Université de Nice Sophia Antipolis.  
Professeur à l'Université de St. Gallen–Suisse.

## Examineurs :

Sylvain CONTASSOT-VIVIER  
Raphaël COUTURIER  
Christophe GUYEUX

Professeur à l'Université de Lorraine.  
Professeur à l'Univ. Bourgogne Franche-Comté.  
Professeur à l'Univ. Bourgogne Franche-Comté.

# Réseau booléen (définition)



- Une fonction  $f : \mathbb{B}^N \rightarrow \mathbb{B}^N$ ,  $x = (x_1, \dots, x_N) \mapsto (f_1(x), \dots, f_N(x))$
- Un schéma de mise à jour de la suite  $(x^t)^{t \in \mathbb{N}}$  des configurations :
  - *Parallèle synchrone* :  $x^{t+1} = f(x^t)$ .
  - *Unaire* : à partir de la *stratégie unaire*  $(s^t)^{t \in \mathbb{N}} \in [\mathbb{N}]^{\mathbb{N}}$ , modification de l'élément  $s^t$  de  $x^t$

$$x^{t+1} = (x_1^{t+1}, \dots, x_n^{t+1}) \text{ où } x_i^{t+1} = \begin{cases} f_i(x^t) & \text{si } i = s^t \\ x_i^t & \text{sinon.} \end{cases}$$

- *Généralisé* : à partir de la *stratégie généralisée*  $(s^t)^{t \in \mathbb{N}} \in \mathcal{P}([\mathbb{N}])^{\mathbb{N}}$ , modification des éléments de  $x^t$  dans  $s^t \subset [\mathbb{N}]$

$$x^{t+1} = (x_1^{t+1}, \dots, x_n^{t+1}) \text{ où } x_i^{t+1} = \begin{cases} f_i(x^t) & \text{si } i \in s^t \\ x_i^t & \text{sinon} \end{cases}$$

$$(x_1, x_2, x_3) \mapsto ((\overline{x_1} + \overline{x_2}).x_3, x_1.x_3, x_1 + x_2 + x_3).$$


- 

# Dépendance entre éléments

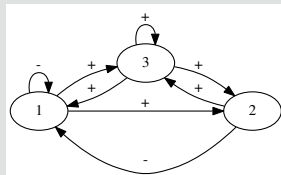


- Mat. de  $\{-1, 0, 1\}^{N^2}$  des « dérivées partielles »  $f'_{ij} = \frac{f_i(\bar{x}^j) - f_i(x)}{\bar{x}_j - x_j}$ .
- Représentée par un *graphe des interactions* orienté :
  - Sommets :  $[N]$
  - Arcs :  $j \xrightarrow{s} i$  si  $\exists x \in \mathbb{B}^N$  tq.  $f'_{ij}(x) = s, s \in \{-1, 1\}$

## Graphes des interactions de

$$(x_1, x_2, x_3) \mapsto ((\bar{x}_1 + \bar{x}_2) \cdot x_3, x_1 \cdot x_3, x_1 + x_2 + x_3).$$

$$f' = \begin{pmatrix} \frac{(x_1 + \bar{x}_2) \cdot x_3 - (\bar{x}_1 + \bar{x}_2) \cdot x_3}{\bar{x}_1 - x_1} & \frac{(\bar{x}_1 + x_2) \cdot x_3 - (\bar{x}_1 + \bar{x}_2) \cdot x_3}{\bar{x}_2 - x_2} & \dots \\ \frac{\bar{x}_1 \cdot x_3 - x_1 \cdot x_3}{\bar{x}_1 - x_1} & 0 & \dots \\ \frac{(\bar{x}_1 + x_2 + x_3) - (x_1 + x_2 + x_3)}{\bar{x}_1 - x_1} & \dots & \dots \end{pmatrix}$$





1. Introduction : itérations de réseaux booléens (07–09)
2. Des systèmes dynamiques discrets au chaos (09–12)
3. Application à la génération de nombres pseudo-aléatoires (11–...)
4. Application au masquage d'information (11–...)
5. Conclusion



1. Introduction : itérations de réseaux booléens (07–09)
2. Des systèmes dynamiques discrets au chaos (09–12)  
Bahi, Guyeux, Richard
3. Application à la génération de nombres pseudo-aléatoires (11–...)
4. Application au masquage d'information (11–...)
5. Conclusion

# Contexte : chaos selon Devaney



## Définition (Chaos selon Devaney)

$k$  continue sur  $(\mathcal{X}, d)$  est chaotique si elle est transitive, régulière et fortement sensible aux conditions initiales.

- *Transitivité* : pour chaque point, chacun de ses voisinages a un futur pouvant contenir tout point de l'espace.
- *Régularité* : l'ensemble de ses points périodiques est dense dans  $\mathcal{X}$ .
- *Forte sensibilité aux cond. initiales* : pour chaque point, chacun de ses voisinages a un point dont un futur est éloigné.

# “Chaoticité” des itérations unaires/généralisées



- $\mathcal{X}_u = \mathbb{B}^N \times [\mathbb{N}]^{\mathbb{N}}$  et  $G_{f_u} : \mathcal{X}_u \rightarrow \mathcal{X}_u$  tq.  $G_{f_u}(x, s) = (F_{f_u}(x, s_0), \sigma(s))$  [Guy10] :
  - $F_{f_u} : \mathbb{B}^N \times [\mathbb{N}] \rightarrow \mathbb{B}^N, (x, i) \mapsto (x_1, \dots, x_{i-1}, f_i(x), x_{i+1}, \dots, x_N)$
  - $\sigma : [\mathbb{N}]^{\mathbb{N}} \rightarrow [\mathbb{N}]^{\mathbb{N}}$  t.q.  $\forall t \in \mathbb{N}, \sigma(s)_t = s_{t+1}$
- Distance  $d : d((x, s), (x', s')) = d_H(x, x') + d_S(s, s')$

## Théorème (Fonctions t.q. $G_{f_u}$ est chaotique [BCG12b])

Soit  $f : \mathbb{B}^N \rightarrow \mathbb{B}^N$ . Les itérations de la fonction  $G_{f_u}$  sont chaotiques si et seulement si  $\text{GIU}(f)$  est fortement connexe.

## Théorème (Fonctions t.q. $G_{f_g}$ est chaotique)

Soit  $f : \mathbb{B}^N \rightarrow \mathbb{B}^N$ . Les itérations de la fonction  $G_{f_g}$  sont chaotiques si et seulement si  $\text{GIG}(f)$  est fortement connexe.



# Générer un graphe GIU fortement connexe

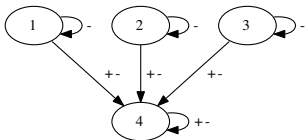
- Méthode naïve : suppressions successives aléatoires d'arcs de  $\text{GIU}(\neg)$ .

## Théorème (Fonctions avec GIU fort. connexe [BCGR11])

Soit  $f$  une fonction de  $\mathbb{B}^N$  vers lui-même telle que  $\Gamma(f)$  :

1. N'a pas de cycle de longueur supérieure ou égale à deux.
2. Chacun des sommets avec une boucle + a aussi une boucle -.
3. Chacun des sommets est accessible depuis un sommet avec une boucle -.

Alors,  $\text{GIU}(f)$  est fortement connexe.



$\rightsquigarrow \left\{ \begin{array}{l} 34226 \text{ fonctions} \\ 520 \text{ non isomorphes} \end{array} \right.$



1. Introduction : itérations de réseaux booléens (07–09)
2. Des systèmes dynamiques discrets au chaos (09–12)
3. Application à la génération de nombres pseudo-aléatoires (11–...)  
Bahi, Bakiri, Contassot-Vivier, Guyeux, Heam, Richard, Wang
4. Application au masquage d'information (11–...)
5. Conclusion

# PRNG par itérations unaires



## Algorithme [BCGW11]

**Input:** une fonction  $f$ , un nombre d'itérations  $b$ , une configuration initiale  $x^0$  (N bits)

**Output:** une configuration  $x$  (N bits)

$x \leftarrow x^0$ ;

**for**  $i = 1, \dots, b$  **do**

$s \leftarrow \text{Random}(N)$ ;

$x \leftarrow F_{f_u}(x, s)$ ;

**end**

return  $x$ ;

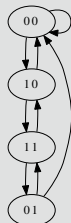
- *Random* : un PRNG (N bits).
- Remarques :
  - $b = 1 \rightsquigarrow$  itérations (chaotiques) de  $F_{f_u}$
  - Quid de l'uniformité de la sortie ?

# Condition néc. suff. pour l'uniformité



## Théorème (Uniformité de la sortie [BCGR11])

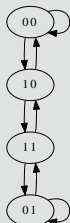
Soit  $f : \mathbb{B}^N \rightarrow \mathbb{B}^N$ ,  $\text{GIU}(f)$  son graphe d'itérations,  $\check{M}$  sa matrice d'adjacence. Si  $\text{GIU}(f)$  est fortement connexe, alors la sortie du générateur de nombres pseudo-aléatoires suit une loi qui tend vers la distribution uniforme ssi  $\frac{1}{N} \check{M}$  est doublement stochastique.



- $g(x_1, x_2) = (\overline{x_1}, x_1 \overline{x_2})$

- $M_g = \frac{1}{2} \begin{pmatrix} 1010 \\ 1001 \\ 1001 \\ 0110 \end{pmatrix}$

- $\pi_g = (\frac{4}{10}, \frac{1}{10}, \frac{3}{10}, \frac{2}{10})$



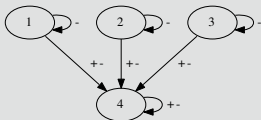
- $h(x_1, x_2) = (\overline{x_1}, x_1 \overline{x_2} + \overline{x_1} x_2)$

- $M_h = \frac{1}{2} \begin{pmatrix} 1010 \\ 0101 \\ 1001 \\ 0110 \end{pmatrix}$

- $\pi_h = (\frac{1}{4}, \frac{1}{4}, \frac{1}{4}, \frac{1}{4})$

# Succès pratiques et limites théoriques

- Seules 16 vérifient les hypothèses du théorème précédent.
- $b$  : nombre d'itérations suffisant pour une déviation p.r. la distribution uniforme inf. à  $10^{-4}$  (temps de mélange).



| Nom                | Définition                                           | $b$      |
|--------------------|------------------------------------------------------|----------|
| $\mathcal{F}_1$    | 14, 15, 12, 13, 10, 11, 8, 9, 6, 7, 4, 5, 2, 3, 1, 0 | 206      |
| $\vdots$           | $\vdots$                                             | $\vdots$ |
| $\mathcal{F}_9$    | 14, 15, 12, 13, 10, 11, 9, 8, 7, 6, 5, 4, 3, 2, 0, 1 | 42       |
| $\vdots$           | $\vdots$                                             | $\vdots$ |
| $\mathcal{F}_{16}$ | 14, 15, 13, 12, 11, 10, 9, 8, 7, 6, 5, 4, 3, 2, 1, 0 | 206      |

- Succès de tous les PRNGs issus de ces fonctions aux tests du *National Institute of Standards and Technology* (NIST).
- Erreur de raisonnement :
  - Générateur prouvé chaotique seulement pour  $b = 1$ .
  - Pas compatible avec la pratique :  $b \geq 42$  nécessaire pour suivre une loi uniforme (à  $10^{-4}$  près).
  - $\rightsquigarrow$  Étendre la théorie.

# Formalisation de $b$ itérations unaires

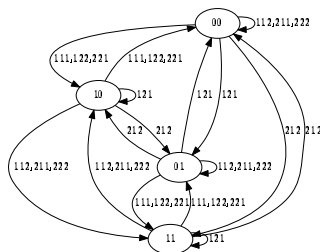
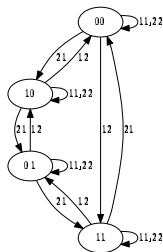
- $\mathcal{X}_u = \mathbb{B}^N \times [N]^{\mathbb{N}}$  et  $G_{f_u,b} : \mathcal{X}_u \rightarrow \mathcal{X}_u$  tq.

$$G_{f_u,b}(x, s) = (F_{f_u}(\dots(F_{f_u}(x, s_0), \dots), s_{b-1}), \sigma^b(s))$$

- Distance  $d((x, s), (x', s')) = d_H(x, x') + d''_S(s, s')$

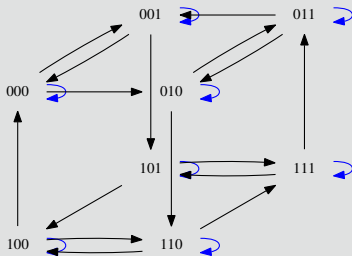
## Théorème (Fonctions t.q. $G_{f_u,b}$ est chaotique [CCVHG16])

La fonction  $G_{f_u,b}$  est chaotique sur  $(\mathcal{X}_u, d)$  si et seulement si le graphe d'itérations  $\text{GIU}_b(f)$  est fortement connexe.



# GIU fortement connexe par construction

- CLPFD : approche de type « générer, tester ».
- $f^*(x_1, x_2, x_3) = (x_2 \oplus x_3, \overline{x_1 x_3} + x_1 \overline{x_2}, \overline{x_1 x_3} + x_1 x_2)$  : très faible  $b$ .
- $f^*$  : 3-cube ss le *cycle hamiltonien* 000, 100, 101, 001, 011, 111, 110, 010, 000.



$$M = \frac{1}{3} \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

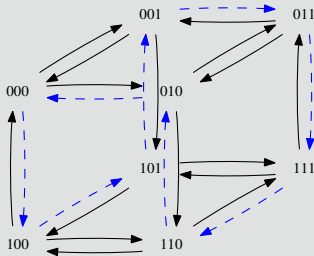
## Théorème ( N-cube privé d'un cycle hamiltonien [CHG<sup>+</sup>14])

Dans un N-cube, dans lequel un cycle hamiltonien a été enlevé :

- La matrice de Markov engendrée est doublement stochastique.
- Le graphe GIU correspondant est fortement connexe.

# GIU fortement connexe par construction

- CLPFD : approche de type « générer, tester ».
- $f^*(x_1, x_2, x_3) = (x_2 \oplus x_3, \overline{x_1 x_3} + x_1 \overline{x_2}, \overline{x_1 x_3} + x_1 x_2)$  : très faible  $b$ .
- $f^*$  : 3-cube ss le *cycle hamiltonien* 000, 100, 101, 001, 011, 111, 110, 010, 000.



$$M = \frac{1}{3} \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

## Théorème ( N-cube privé d'un cycle hamiltonien [CHG<sup>+</sup>14])

Dans un N-cube, dans lequel un cycle hamiltonien a été enlevé :

- La matrice de Markov engendrée est doublement stochastique.
- Le graphe GIU correspondant est fortement connexe.



# Cycle hamiltonien équilibré



- Intuition de convergence rapide vers la distribution uniforme : supprimer un cycle hamiltonien équilibré (chaque bit nié autant de fois).
- Extension de *Robinson-Cohn* [ZS04] : preuve de l'existence (sans construction) de cycle hamiltonien équilibré.

## Théorème (Constr. de cycle hamiltonien équilibré [CCVHG16])

*Il existe une séquence (et construction de celle-ci) dans l'extension de l'algorithme de Robinson-Cohn telle que le cycle est équilibré.*

- Pratique : grande famille de cycles hamiltonien équilibrés ( $N \leq 16$ ).

# Évaluation de l'écart / distribution uniforme

## Théorème (Temps de mixage sans chemin hamiltonien [CCVHG16])

*On considère un  $N$ -cube dans lequel un chemin hamiltonien a été supprimé et la fonction de probabilités  $p$  définie sur l'ensemble des arcs comme suit :*

$$p(e) \begin{cases} = \frac{1}{2} + \frac{1}{2N} \text{ si } e = (v, v) \text{ avec } v \in \mathbb{B}^N, \\ = \frac{1}{2N} \text{ sinon.} \end{cases}$$

*La chaîne de Markov associée converge vers la distribution uniforme et*

$$t_{\text{mix}}(\varepsilon) \leq \lceil \log_2(\varepsilon^{-1}) \rceil 4(8N^2 + 4N \ln(N + 1))$$

- Remarques sur la preuve :
  - Itérations paresseuses  $\neq$  algorithme.
  - Hypothèse très faible : suppressions d'un arc entrant et d'un arc sortant par nœud.
  - Pratiquement :  $4(8N^2 + 4N \ln(N + 1)) \rightsquigarrow 4(2N \ln(2N + 8))$ .

# Et les itérations généralisées ?



```
... for  $i = 1, \dots, k$  do  
     $s \leftarrow \text{Set}(\text{Random}(2^N));$   
     $x \leftarrow F_{fg}(x, s);$   
end  
...
```

## Théorème (Uniformité de la sortie ds le cas généralisé)

Si  $\text{GIG}(f)$  est fortement connexe, alors la sortie du PRNG suit une loi qui tend vers la distribution uniforme ssi  $\frac{1}{2^N} \check{M}$  est une matrice doublement stochastique.

## Nombre moyen d'appels à un générateur binaire par bit généré

- Unaires : ↗
- Généralisées : ↘

# Plateforme d'implantation FPGA [BCG16]



## Bilan d'implantation de PRNGs sur FPGA

| Débits (Gb/s) | Test U01                                                                |                          |
|---------------|-------------------------------------------------------------------------|--------------------------|
|               | KO                                                                      | OK                       |
|               | Xorshift (8–16)<br>LFSR (6–10)<br><br>TGFSR (0.7–1.3)<br>LCG (0.02–0.3) | PCG32 (0.3), MRG32 (0.4) |

# Plateforme d'implantation FPGA [BCG16]



## Bilan d'implantation de PRNGs sur FPGA

| Débits (Gb/s) | Test U01                                                                |                                                                                        |
|---------------|-------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
|               | KO                                                                      | OK                                                                                     |
|               | Xorshift (8–16)<br>LFSR (6–10)<br><br>TGFSR (0.7–1.3)<br>LCG (0.02–0.3) | PCG32 (0.3), MRG32 (0.4)<br>Négation, unaire (0.031–3.5)<br>Hamiltonien, unaire (0.05) |

Détails d'implantation :

- Stratégie : extraite de XorShift128+.
- N : négation (32), unaire (16),
- Mélange : négation (variable), unaire (190),

# Plateforme d'implantation FPGA [BCG16]



## Bilan d'implantation de PRNGs sur FPGA

|  | Test U01                                                                |                                                                                                                           |
|--|-------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|
|  | KO                                                                      | OK                                                                                                                        |
|  | Xorshift (8–16)<br>LFSR (6–10)<br><br>TGFSR (0.7–1.3)<br>LCG (0.02–0.3) | Hamiltonien, généralisé (2)<br><br>PCG32 (0.3), MRG32 (0.4)<br>Négation, unaire (0.031–3.5)<br>Hamiltonien, unaire (0.05) |

Détails d'implantation :

- Stratégie : extraite de XorShift128+.
- N : négation (32), unaire (16), généralisé ( $4 \times 4$ ).
- Mélange : négation (variable), unaire (190), généralisé (4).

# Plateforme d'implantation FPGA [BCG16]



## Bilan d'implantation de PRNGs sur FPGA

| Débits (Gb/s) | Test U01                                                                |                                                                                                                                                            |
|---------------|-------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
|               | KO                                                                      | OK                                                                                                                                                         |
|               | Xorshift (8–16)<br>LFSR (6–10)<br><br>TGFSR (0.7–1.3)<br>LCG (0.02–0.3) | Xor avec 3 PRNGs [FWGB14] (8)<br>Hamiltonien, généralisé (2)<br><br>PCG32 (0.3), MRG32 (0.4)<br>Négation, unaire (0.031–3.5)<br>Hamiltonien, unaire (0.05) |

Détails d'implantation :

- Stratégie : extraite de XorShift128+.
- N : négation (32), unaire (16), généralisé ( $4 \times 4$ ).
- Mélange : négation (variable), unaire (190), généralisé (4).



1. Introduction : itérations de réseaux booléens (07–09)
2. Des systèmes dynamiques discrets au chaos (09–12)
3. Application à la génération de nombres pseudo-aléatoires (11–...)
4. Application au masquage d'information (11–...)  
Bahi, Bittar, Couturier, Darazi, Fadil, Friot, Guyeux
5. Conclusion



# Marquage de média : un processus itératif



## Définition (Embarquement dhCI étendu [BCG11b])

Soit un hôte  $x$ ,  $u_m$  les indices de ses bits modifiables,  $\phi_m$  leur valeur,  $y$  un message,  $q$  un nombre d'itérations. L'algorithme d'embarquement retourne le résultat de l'embarquement de  $\hat{y}$  dans  $x$ , t. q. :

- La fonction  $f_l : \mathbb{B}^l \rightarrow \mathbb{B}^l$ ,  $l = |u_m|$ .
- Une stratégie  $(s_y)^{t \in \mathbb{N}} \in [l]^{\mathbb{N}}$  est instanciée en fonction de  $y$ .
- $\hat{y}$  est définie par  $(\hat{y}, \_) = G_{f_l}^q(\phi_m, s_y)$ .

## Théorème (Stego-sécurité et chaos-sécurité [BCG12b])

Si  $(s_y)$  est indépendante de  $x$ , si  $f_l$  est tq. GIU( $f_l$ ) fortement connexe et a une matrice de Markov doublement stochastique.

- Le marquage est  $\epsilon$ -stégo sécurisé.
- Le marquage est chaos sécurisé.
- Particularisation dans différents domaines (spatial, fréquentiel).
- Robustesse évaluée.

# Embarquons plus qu'un bit



## Définition (Marquage non binaire chaotique [FGB11])

- Marque  $m \in \mathbb{B}^P$ .
- Support modifiable pour la marque :  $x^0 \in \mathbb{B}^N$ .
- Stratégie de place  $s_p \in [N]^{\mathbb{N}}$  : élément de  $x$  modifié à l'itération  $t$ .
- Stratégie de choix  $s_c \in [P]^{\mathbb{N}}$  : indice de l'élément de  $m$  embarqué à l'itération  $t$ .
- Stratégie de mélange  $s_m \in [P]^{\mathbb{N}}$  : élément de  $m$  inversé à l'itération  $t$ .

On remplace  $x$  par  $x^t \in \mathbb{B}^N$  avec  $x_i^t = \begin{cases} m_{s_c^t}^{t-1} & \text{si } s_p^t = i \\ x_i^{t-1} & \text{sinon} \end{cases}$  et  $m_i^t = \begin{cases} \overline{m_i^{t-1}} & \text{si } s_m^t = i \\ m_i^{t-1} & \text{sinon} \end{cases}$

## Théorème (Correction et complétude du marquage [BCF<sup>+</sup>13])

Soit  $\mathfrak{S}(s_p) = \{S_p^1, S_p^2, \dots, S_p^k\}$ ,  $k = |\mathfrak{S}(s_p)|$  et  $\mathfrak{S}(s_c)_{|D} = \{S_c^{d_1}, S_c^{d_2}, \dots, S_c^{d_k}\}$  où  $d_i$  est la dernière date où l'élément  $i \in \mathfrak{S}(s_p)$  a été modifié. «  $\mathfrak{S}(s_c)_{|D} = \llbracket 0; P-1 \rrbracket$  » est une condition nécessaire et suffisante pour l'extraction du message du média marqué.



- Tatouage de documents PDF : très peu étudié.
- STDM : un (des) schémas les plus robustes et les plus sécurisés de tatouage.

## STDM dans les PDF textuels [BDCC15]

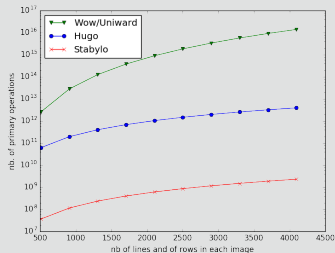
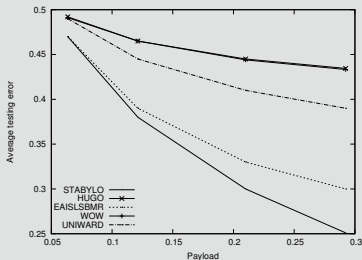
- Hôte : l'ensemble des abscisses des caractères du document.
- Application de STDM avec comme compromis :
  - Robustesse : possibilité de retrouver la marque face à chaque attaque laissant le document lisible.
  - Imperceptibilité : difficile de distinguer l'hôte original du document marqué.

# Stéganographie : introduction avec STABYLO

- Stéganographie :
  - Objectif : embarquer un message de manière imperceptible.
  - Méthode : construction d'une carte de distorsion des éléments modifiables.
  - Évaluation de la sécurité : étude de la détectabilité par stéganalyse.

## STeg. with Adaptive, Bbs, binarY emb. at LOw cost [CCG15]

- Carte de distorsion : les pixels de bord peuvent être modifiés.
- Faible complexité : produit de convolution de Canny sur des petites fenêtres.

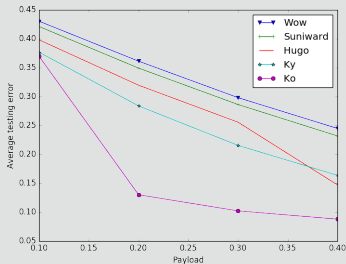


# Stéganographie : analyse vectorielle discrète

- Détectabilité de modification :
  - Facile : les régions uniformes, les bords clairement définis...
  - Difficile : les textures, le bruit, les régions “chaotiques”...  $\leftrightarrow$  courbes de niveau très perturbées.
- Mathématiques des courbes de niveau : gradient, matrice hessienne.
- Signature d'une image :  $P : [I] \times [L] \rightarrow \mathbb{R}$  et pas  $\mathbb{R}^2 \rightarrow \mathbb{R}$ .

## Gradient dans des image [CCFG16]

- Approches usuelles : convolutions avec des noyaux de type “Sobel”, “Prewitt”,...
- Proposition : noyaux de taille variable (entre 3 et 13)
  1.  $K_y$  : symétrique, centré, approximation discrète de dérivée seconde.
  2.  $K_o$  : à base de polynômes d'interpolation.





1. Introduction : itérations de réseaux booléens (07–09)
2. Des systèmes dynamiques discrets au chaos (09–12)
3. Application à la génération de nombres pseudo-aléatoires (11–...)
4. Application au masquage d'information (11–...)
5. Conclusion



- Fonctions engendrant des itérations chaotiques : CS sur le graphe d'interactions, par suppression d'1 cycle hamiltonien équilibré.
- Application aux PRNG : étude théorique et pratique de la sortie en fonction du nombre d'itérations.
- Masquage d'information : de la propriété de transitivité du chaos à l'analyse vectorielle discrète.



- Cycles hamiltoniens équilibrés :
  - S'affranchir de l'algorithme *Robinson-Cohn* : trop restrictif.
  - Génération exhaustive de cycles non isomorphes : une forme canonique.
  - Équilibre local, global : conséquences dans un PRNG.
- Générateurs de nombres pseudo-aléatoires :
  - S'affranchir du générateur interne.
  - Majorer finement le délai d'obtention de la distribution uniforme.
  - Exploiter le GIG à la place du GIU.
- Masquage d'information :
  - Creuser la piste « Analyse vectorielle ».
  - Stéganalyse par Deep Learning : comprendre pourquoi cela marche.
  - Tatouage STDM dans un PDF : comment contrer les attaques ?



# Bilan académique



- Encadrement doctoral :
  - Soutenue : Bassam Alkindy (dec. 15, 40%).
  - En cours : Youssra Fadil (mar. 17, 50%), Mohamed Bakiri (dec. 17, 50%), Nesrine Khernane (dec. 18, 50%).
- 10 Reviews de journaux internationaux référencés.
- 1 projet région (15–18) “capteurs multimédias collaboratifs : une approche intégrée de la sécurité et de la robustesse”.
- Publications depuis l'intégration dans DISC-AND :

| Journaux internationaux                                         | Conférences internationales                                                                                                                                                             |
|-----------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [BCG12a, BCG12b, BCGS12]<br>[CDS13, CCG15, BDCC15]<br>[CCVHG16] | [AAG <sup>+</sup> 15, BCFG12a, BCFG12b, BCF <sup>+</sup> 13]<br>[BCG11a, BCG11b]<br>[BCGR11, BCGW11, CDS12, CHG <sup>+</sup> 14]<br>[FCCG15, BCC <sup>+</sup> 15, BCG16, CCFG16, KCM16] |

- Mandat d'élu : conseil d'institut de l'IUT BM (10–14).
- Responsabilité pédagogique : responsable de la LP SIL CAM, TeProw (14–. . .).



Bassam AlKindy, Bashar Al-Nuaimi, Christophe Guyeux, Jean-François Couchot, Michel Salomon, Reem Alsraj, and Laurent Philippe.

---

Binary particle swarm optimization versus hybrid genetic algorithm for inferring well supported phylogenetic trees.

In Claudia Angelini, Paola M. V. Rancoita, and Stefano Rovetta, editors, *Computational Intelligence Methods for Bioinformatics and Biostatistics - 12th International Meeting, CIBB 2015, Naples, Italy, September 10-12, 2015, Revised Selected Papers*, volume 9874 of *Lecture Notes in Computer Science*, pages 165–179. Springer, 2015.



Bassam Alkindy, Jean-François Couchot, Christophe Guyeux, and Michel Salomon.

Finding the core-genes of chloroplast species.

Journées SeqBio 2013, Montpellier, November 2013.



B. Al Bouna, J. F. Couchot, R. Couturier, Y. A. Fadil, and C. Guyeux.

Performance study of steganalysis techniques.

In *Applied Research in Computer Science and Engineering (ICAR), 2015 International Conference on*, pages 1–7, Lebanon, October 2015.



Jacques Bahi, Jean-François Couchot, Nicolas Friot, Christophe Guyeux, and Kamel Mazouzi.

Quality studies of an invisible chaos-based watermarking scheme with message extraction.

In *IHMSP'13, 9th Int. Conf. on Intelligent Information Hiding and Multimedia Signal Processing*, pages 547–550, Beijing, China, October 2013.



Jacques Bahi, Jean-François Couchot, Nicolas Friot, and Christophe Guyeux.

Application of steganography for anonymity through the internet.



Jacques Bahi, Jean-François Couchot, Nicolas Friot, and Christophe Guyeux.

A robust data hiding process contributing to the development of a semantic web.

In *INTERNET'2012, 4-th Int. Conf. on Evolving Internet*, pages 71–76, Venice, Italy, June 2012.



Jacques Bahi, Jean-François Couchot, and Christophe Guyeux.

Performance analysis of a keyed hash function based on discrete and chaotic proven iterations.

In *INTERNET 2011, the 3-rd Int. Conf. on Evolving Internet*, pages 52–57, Luxembourg, Luxembourg, June 2011.

Best paper award.



Jacques Bahi, Jean-François Couchot, and Christophe Guyeux.

**Steganography : a class of algorithms having secure properties.**

*In IIH-MSP-2011, 7-th Int. Conf. on Intelligent Information Hiding and Multimedia Signal Processing*, pages 109–112, Dalian, China, October 2011.



Jacques Bahi, Jean-François Couchot, and Christophe Guyeux.

**Quality analysis of a chaotic proven keyed hash function.**

*International Journal On Advances in Internet Technology*, 5(1) :26–33, 2012.



Jacques Bahi, Jean-François Couchot, and Christophe Guyeux.

**Steganography : a class of secure and robust algorithms.**

*The Computer Journal*, 55(6) :653–666, 2012.



Mohammed Bakiri, Jean-François Couchot, and Christophe Guyeux.

FPGA implementation of f2-linear pseudorandom number generators based on zynq mp soc : A chaotic iterations post processing case study.

In Christian Callegari, Marten van Sinderen, Panagiotis G. Sarigiannidis, Pierangela Samarati, Enrique Cabello, Pascal Lorenz, and Mohammad S. Obaidat, editors, *Proceedings of the 13th International Joint Conference on e-Business and Telecommunications (ICETE 2016) - Volume 4 : SECRIPT, Lisbon, Portugal, July 26-28, 2016.*, pages 302–309. SciTePress, 2016.



Jacques Bahi, Jean-François Couchot, Christophe Guyeux, and Adrien Richard.

On the link between strongly connected iteration graphs and chaotic boolean discrete-time dynamical systems.



Jacques Bahi, Jean-François Couchot, Christophe Guyeux, and Michel Salomon.

Neural networks and chaos : Construction, evaluation of chaotic networks, and prediction of chaos with multilayer feedforward network.

*Chaos, An Interdisciplinary Journal of Nonlinear Science*, 22(1) :013122–1 – 013122–9, March 2012.  
9 pages.



Jacques Bahi, Jean-François Couchot, Christophe Guyeux, and Qianxue Wang.

Class of trustworthy pseudo random number generators.

In *INTERNET 2011, the 3-rd Int. Conf. on Evolving Internet*, pages 72–77, Luxembourg, Luxembourg, June 2011.



Ahmad W. Bitar, Rony Darazi, Jean-François Couchot, and Raphaël Couturier.

Blind digital watermarking in pdf documents using spread transform dither modulation.

*Multimedia Tools and Applications*, pages 1–19, 2015.



Jean-François Couchot, Raphaël Couturier, Yousra Ahmed Fadil, and Christophe Guyeux.

A second order derivatives based approach for steganography.

In *Secrypt 2016, 13th Int. Conf. on Security and Cryptography*, pages 424–431, Lisbon, July 2016.



Jean-François Couchot, Raphaël Couturier, and Christophe Guyeux.

STABYLO : steganography with adaptive, bbs, and binary embedding at low cost.

*Annales des Télécommunications*, 70(9-10) :441–449, 2015.





Jean-François Couchot, Sylvain Contassot-Vivier, Pierre-Cyrille Héam, and Christophe Guyeux.

Random walk in a  $n$ -cube without hamiltonian cycle to chaotic pseudorandom number generation : Theoretical and practical considerations.

*International Journal of Bifurcation and Chaos*, 2016.

Accepted on Oct 2016.



Jean-François Couchot, Karine Deschinkel, and Michel Salomon.

Suitability of artificial neural network for MEMS-based flow control.

In Julien Bourgeois and Michel de Labachellerie, editors, *dMEMS 2012, Workshop on design, control and software implementation for distributed MEMS*, pages 1–6, Besançon, France, April 2012. IEEE CPS.



Jean-François Couchot, Karine Deschinkel, and Michel Salomon.

Active MEMS-based flow control using artificial neural network.

*Mechatronics*, 23(7) :898–905, October 2013.

Available online.



Jean-François Couchot, Pierre-Cyrille Héam, Christophe Guyeux, Qianxue Wang, and Jacques Bahi.

Pseudorandom number generators with balanced gray codes.

In *Secrypt 2014, 11th Int. Conf. on Security and Cryptography*, pages 469–475, Vienna, Austria, August 2014.



Yousra Ahmed Fadil, Jean-François Couchot, Raphaël Couturier, and Christophe Guyeux.

Steganalyzer performances in operational contexts.

In *IHH-MSP 2015, 11th Int. Conf. on Intelligent Information Hiding and Multimedia Signal Processing*, pages 429–432, Adelaide, Australia, September 2015.



Nicolas Friot, Christophe Guyeux, and Jacques Bahi.  
Chaotic iterations for steganography - stego-security and  
chaos-security.

---

In Javier Lopez and Pierangela Samarati, editors,  
*SECURITY'2011, Int. Conf. on Security and Cryptography.*  
*SECURITY is part of ICETE - The International Joint*  
*Conference on e-Business and Telecommunications*, pages  
218–227, Sevilla, Spain, July 2011. SciTePress.



Xiaole Fang, Qianxue Wang, Christophe Guyeux, and  
Jacques M. Bahi.  
Fpga acceleration of a pseudorandom number generator  
based on chaotic iterations.  
*J. Inf. Secur. Appl.*, 19(1) :78–87, February 2014.



Christophe Guyeux.  
*Le désordre des itérations chaotiques et leur utilité en*  
*sécurité informatique.*

Thèse de Doctorat, LIFC, Université de Franche-Comté, 13 décembre 2010.

Rapporteurs : Pascale Charpin, Directrice de Recherche, INRIA-Rocquencourt ; Eric Filiol, Professeur, ESIEA-Laval ; Pierre Spitéri, Professeur Emérite, IRIT-ENSEEIH.

Examineurs : Michel de Labachellerie, Directeur de recherche CNRS, Université de Franche-Comté ; Laurent Larger, Professeur, Université de Franche-Comté ; Jean-Claude Miellou, Professeur, Université de Franche-Comté ; Congduc Pham, Professeur, Université de Pau. Directeur : Jacques M. Bahi, Professeur, Université de Franche-Comté.



N. Khernane, J.-F. Couchot, and A. Mostefaoui.

**Maximizing network lifetime in wireless video sensor networks under quality constraints.**

In *MOBIWAC 2016 : The 14th ACM\* International Symposium on Mobility Management and Wireless Access*, November 2016.



A. J. van Zanten and I. N. Suparta.

Totally balanced and exponentially balanced gray codes.

*Discrete Analysis and Operational Research*, 11 :81–98,  
2004.

