Modélisation et validation des générateurs aléatoires cryptographiques pour les systèmes embarqués

LAYAT Kevin [1]
Directeur : ELBAZ-VINCENT Philippe [2]
Encadrante : DUMAS Cécile [3]

[1] LabEx PERSYVAL-Lab (ANR-11-LABX-0025)
[2] Institut Fourier
[3] Université Grenoble Alpes, CEA, LETI, MINATEC Campus

17 décembre 2015

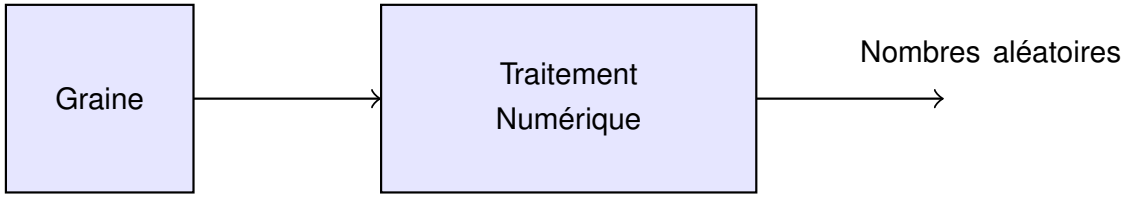
Outline

Importance de l'aléa

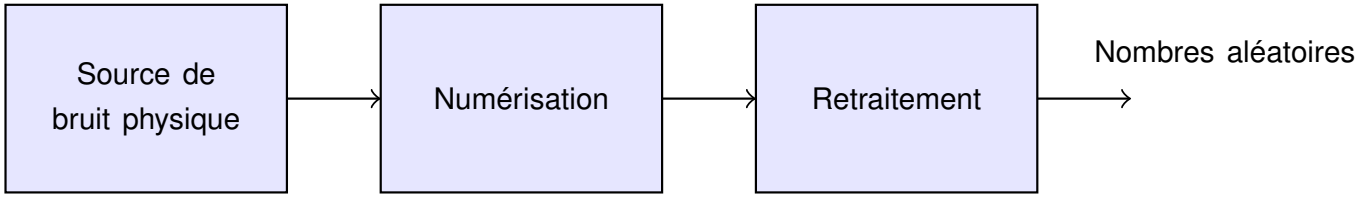
- Utilisation en cryptographie.
  - Génération de clés.
  - Protocoles de chiffrement, de signature.
  - Contres-mesures.
  - ...
- Conséquence d'une mauvaise utilisation :
  - Récupération de la clé privée DSA ([NS02]).
  - Signature de jeux piratés PS3 ([Ove10]).
  - Factorisation de la clé RSA ([Hen12, LHA+12]).
- Propriétés attendues :
  - Imprédictibilité.
  - Indépendance.
  - Identiquement distribuées.

Construction d'un générateur

- Générateur déterministe :



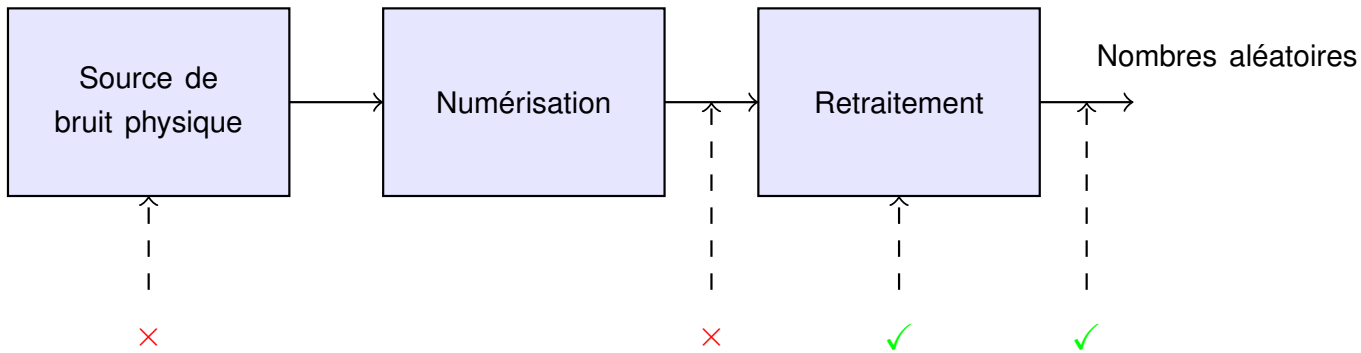
- Générateur non-déterministe :



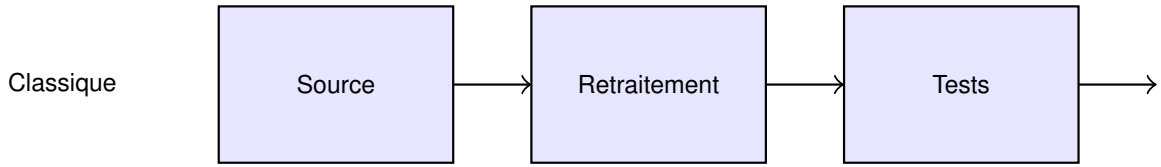
Construction d'un générateur

Référentiel Général de Sécurité, ANSSI, juin 2014 [ANS14]

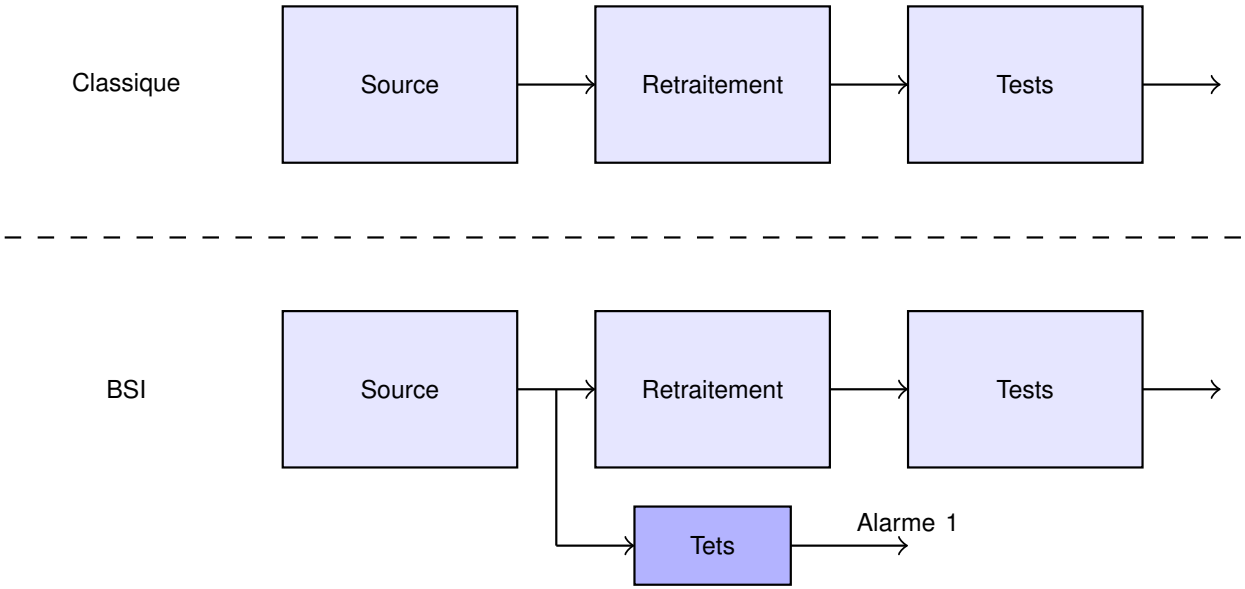
«Les règles et recommandations applicables aux générateurs d'aléa se basent sur le constat qu'il est aujourd'hui très difficile de fournir une preuve convaincante concernant la qualité de l'aléa issu d'un générateur physique, alors qu'il est relativement aisé de se convaincre de la qualité d'un bon retraitement.»



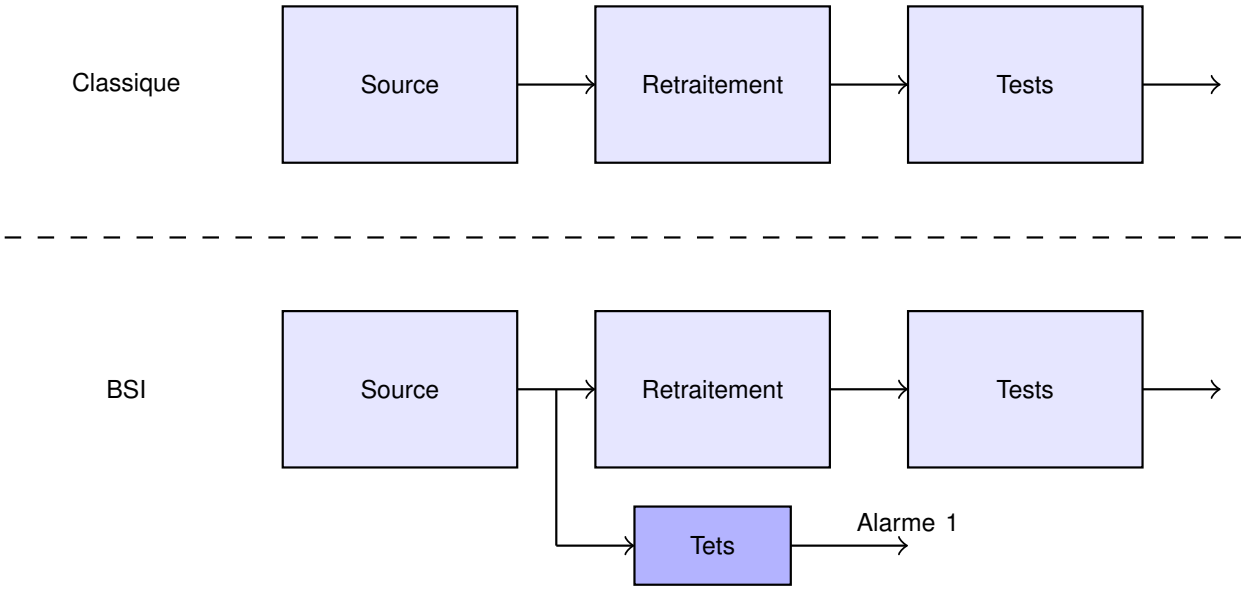
Différentes Schématisations



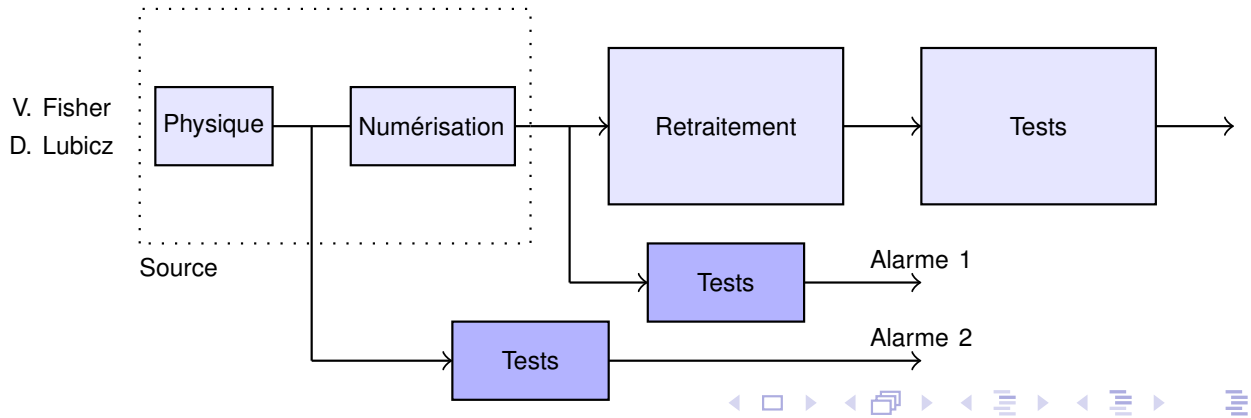
Différentes Schématisations



Différentes Schématisations



[VF14]

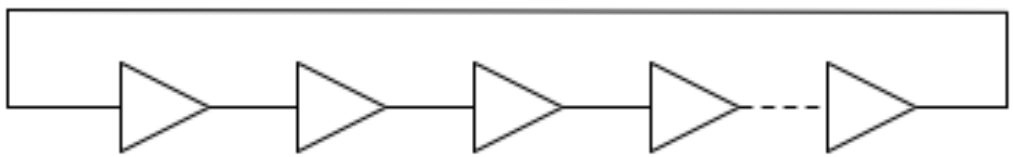


Outline

Sources classiques avec modèles stochastiques

Les standards (BSI [KS11], NIST [BKS12],...) imposent de disposer d'un modèle stochastique pour l'étude d'une source d'entropie.

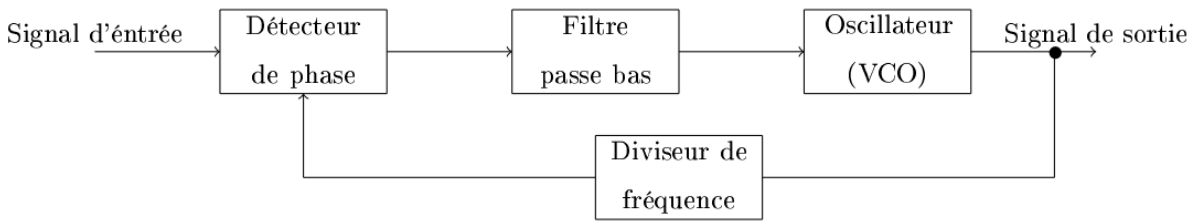
- Bruit de phase :
  - Dans les anneaux d'oscillateurs [BLMT10].



Sources classiques avec modèles stochastiques

Les standards (BSI [KS11], NIST [BKS12],...) imposent de disposer d'un modèle stochastique pour l'étude d'une source d'entropie.

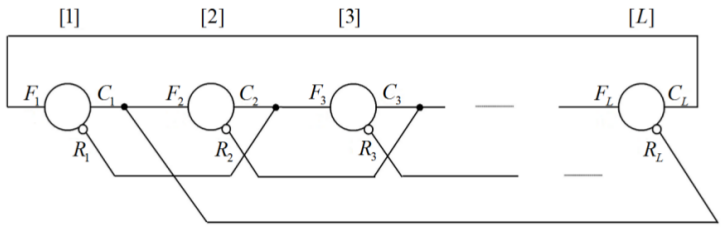
- Bruit de phase :
  - Dans les anneaux d'oscillateurs [BLMT10].
  - Dans les boucles à verrouillage de phase ou PLL [BFV10].



Sources classiques avec modèles stochastiques

Les standards (BSI [KS11], NIST [BKS12],...) imposent de disposer d'un modèle stochastique pour l'étude d'une source d'entropie.

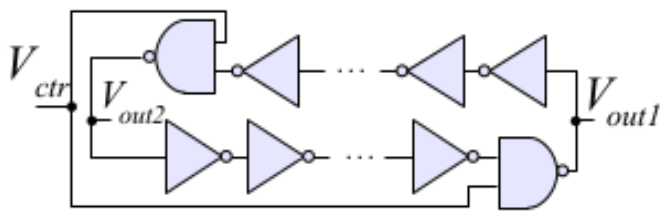
- Bruit de phase :
  - Dans les anneaux d'oscillateurs [BLMT10].
  - Dans les boucles à verrouillage de phase ou PLL [BFV10].
  - Dans les anneaux d'oscillateurs asynchrones [CFAF13].



Sources classiques avec modèles stochastiques

Les standards (BSI [KS11], NIST [BKS12],...) imposent de disposer d'un modèle stochastique pour l'étude d'une source d'entropie.

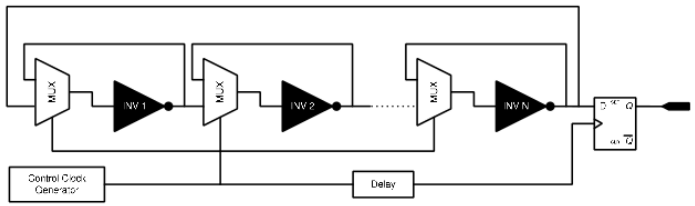
- Bruit de phase :
  - Dans les anneaux d'oscillateurs [BLMT10].
  - Dans les boucles à verrouillage de phase ou PLL [BFV10].
  - Dans les anneaux d'oscillateurs asynchrones [CFAF13].
  - Dans les « Transition effect ring oscillator » ou TERO [VD10].



Sources classiques avec modèles stochastiques

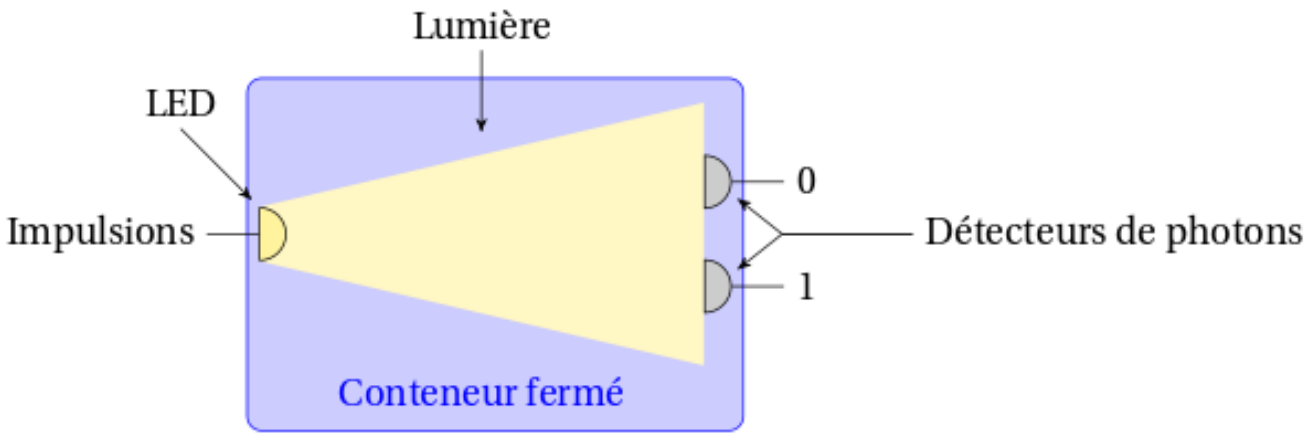
Les standards (BSI [KS11], NIST [BKS12],...) imposent de disposer d'un modèle stochastique pour l'étude d'une source d'entropie.

- Bruit de phase :
  - Dans les anneaux d'oscillateurs [BLMT10].
  - Dans les boucles à verrouillage de phase ou PLL [BFV10].
  - Dans les anneaux d'oscillateurs asynchrones [CFAF13].
  - Dans les « Transition effect ring oscillator » ou TERO [VD10].
- Phénomènes de Métastabilité [VHYSK08].



Sources quantiques avec modèles stochastiques

- Propriétés des photons [Qua10a, Qua10b].

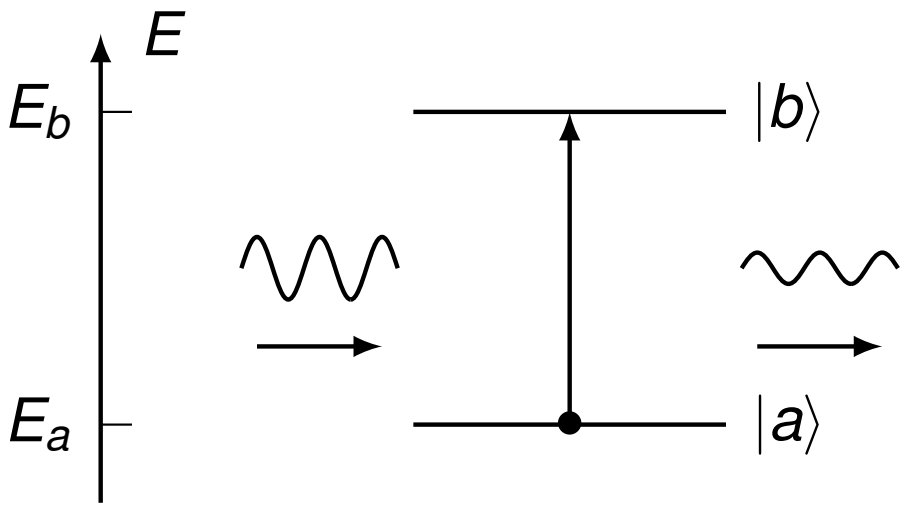


Sources quantiques avec modèles stochastiques

- Propriétés des photons [Qua10a, Qua10b].

Propositions :

- Particules à 2 états [Val05].

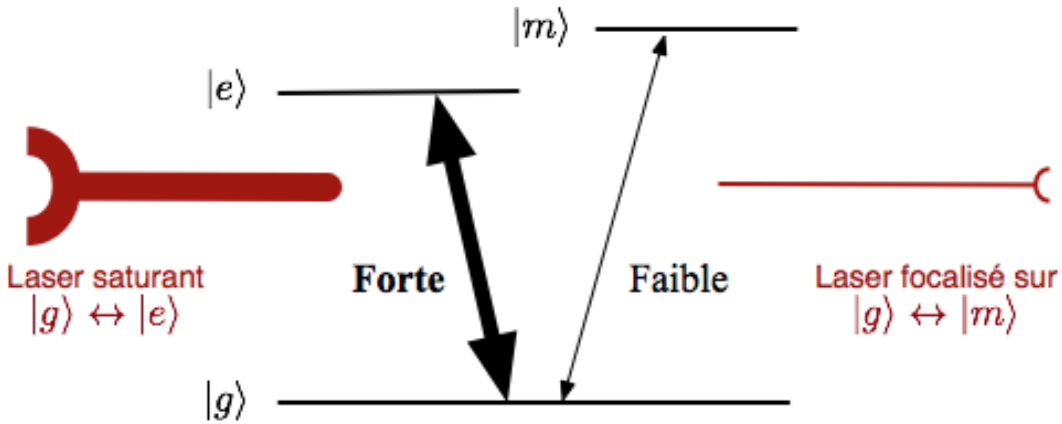


Sources quantiques avec modèles stochastiques

- Propriétés des photons [Qua10a, Qua10b].

Propositions :

- Particules à 2 états [Val05].
- Métastabilité quantique [CK85].



Sauts quantiques

- On définit les probabilités P_b et P_n d'être en période blanche ou en période noire. Les équations cinétiques nous donnent :

$$\frac{dP_n}{dt} = -R_b P_n + R_n P_b.$$
$$\frac{dP_b}{dt} = -R_n P_b + R_b P_n.$$

avec R_b et R_n dépendants des coefficients d'Einstein et des densités spectrales des lasers.

- Par une analyse de probabilité on obtient, pour les durées des périodes, les densités :

$$\begin{cases} f_n(t) = R_- e^{-R_- t}, \\ f_b(t) = R_+ e^{-R_+ t}. \end{cases}$$

- Phénomène physique dont on connaît le comportement probabiliste.

Conclusion

Problématique : Disposer de modèles stochastiques précis pour les sources d'entropies.

Proposition : Étudier les sources d'entropie quantiques. En particulier la métastabilité quantique.

- Avantages :
  - Modèles stochastiques sont inhérents aux phénomènes physiques.
  - Thèmes bien étudiés dans la littérature notamment dans l'informatique quantique.
  - Miniaturisation des technologies.

Outline

Test statistique

- Hypothèse nulle $\mathcal{H}_0$ sur le modèle de la source X :
  Soit $(X_1, \ldots, X_n)$ un échantillon de X,
  $\mathcal{H}_0$: « $(X_1, \ldots, X_n)$ IID suivant $\mathcal{D}_X$ ».

  Dans la méthodologie actuelle,
  $X_i \in \{0, 1\}$ et $\mathcal{H}_0$: « $(X_1, \ldots, X_n)$ est IID suivant $Ber(\frac{1}{2})$ ».

- Statistique du test : $S = f(X_1, \ldots, X_n)$.
- Théorie : Sous $\mathcal{H}_0$, S converge en distribution vers $\mathcal{D}_S$.
- Pratique : Avec une séquence d'observations $(x_1, \ldots, x_n)$:
  - On calcule $s = f(x_1, \ldots, x_n)$.
  - ÉCHEC (rejet $\mathcal{H}_0$) si s est "peu probable" sous $\mathcal{H}_0$.
  - SUCCÈS (pas de rejet de $\mathcal{H}_0$) sinon.

Problématiques liés aux tests statistiques

- Règle de décision.
  - Région de rejet.
  - *p*-valeur.
- Modèle de la source pour l'hypothèse $\mathcal{H}_0$ est trop restrictif :
  - Pas représentatif des contraintes physiques.
  - Aucune intuition de l'hypothèse alternative.
- Perte de la temporalité :
  - Effet de moyenne pour les résultats.
- Hypothèse implicite d'homogénéité de la source dans la méthodologie actuelle.

Solutions proposées

Problématique : Hypothèse implicite de l'homogénéité des séquences.

Proposition : Analyse temporelle de l'homogénéité des séquences basée sur les chaînes de Markov. Le but est de prouver si une séquence est homogène ou constituée de blocs homogènes.

Problématique : Modèles statistiques éloignés des réalités physiques.

Proposition : Étude des modèles de Markov cachés (HMM) pour l'analyse des générateurs.

Chaîne de Markov Homogène

- Chaîne de Markov à espace de temps discret et à espace d'état discret :

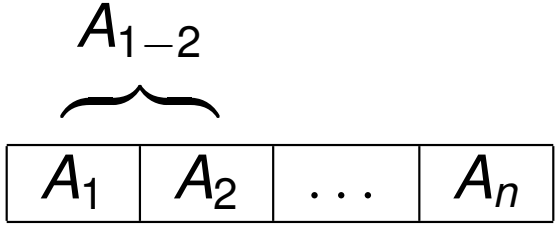
$$\text{CM} : \xrightarrow{\pi} X_0 \xrightarrow{A_1} X_1 \xrightarrow{A_2} X_2 \xrightarrow{A_3} \cdots \xrightarrow{A_{T-1}} X_{T-1}$$

Chaîne de Markov homogène

«Un processus stochastique est homogène si les probabilités de transitions sont indépendantes du temps écoulé.»

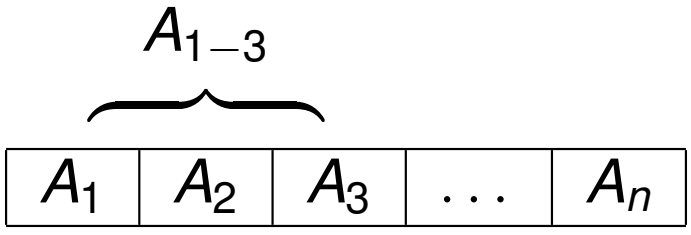
Test de l'homogénéité

- Division de la séquence S en n sous-séquences S_i.
- Calcul de la matrice de transition A_i de chaque sous-séquence S_i.



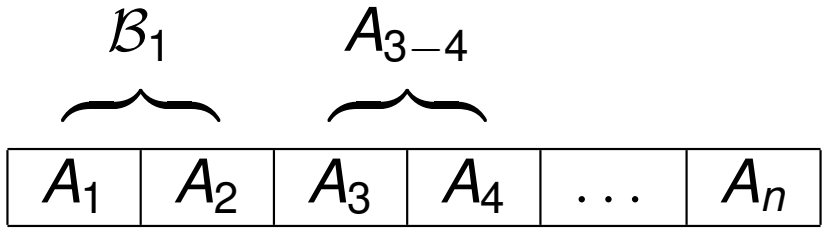
- Choix d'une fonction de comparaison f.
- Calcul de $||f(A_1, A_{1-2})||$ et $||f(A_2, A_{1-2})||$.
- Si l'une de ces valeurs dépasse un seuil fixé $\rightarrow$ problème homogénéité. On continue le test avec un nouveau bloc de sous-séquences.
- Sinon on continue le test avec le même bloc.

Test de l'homogénéité



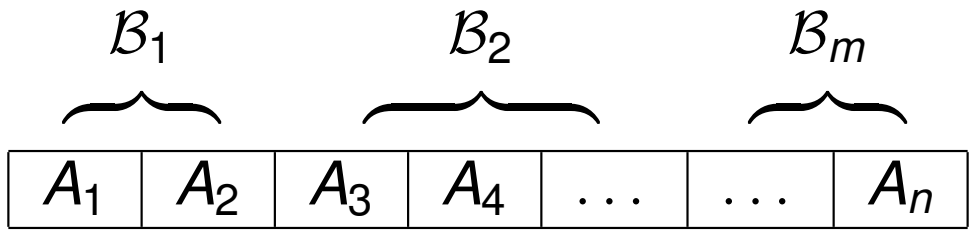
- Calcul de $||f(A_1, A_{1-3})||$, $||f(A_2, A_{1-3})||$ et $||f(A_3, A_{1-3})||$.
- Si l'une de ces valeurs dépasse un seuil fixé $\rightarrow$ problème homogénéité. On continue le test avec un nouveau bloc de sous-séquences.
- Sinon on continue le test avec le même bloc.

Test de l'homogénéité



- Calcul de $||f(A_3, A_{3-4})||$ et $||f(A_4, A_{3-4})||$.
- Si l'une de ces valeurs dépasse un seuil fixé $\rightarrow$ problème homogénéité. On continue le test avec un nouveau bloc de sous-séquences.
- Sinon on continue le test avec le même bloc.

Test de l'homogénéité

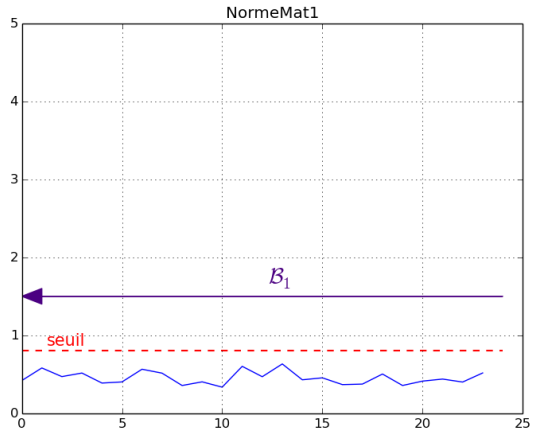


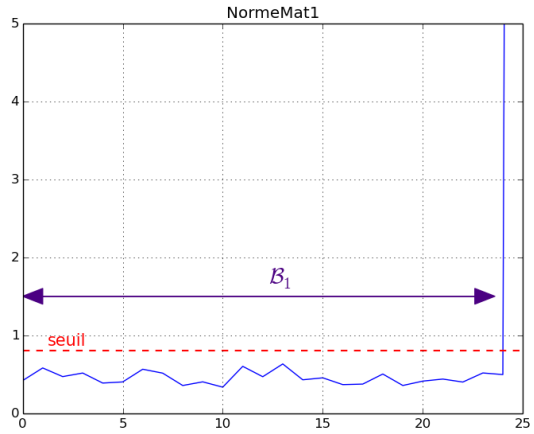
- A la fin, nous avons une suite de blocs ne présentant pas de défaut significatif dans l'homogénéité de la matrice de transition.
- Plusieurs paramétrages possibles de l'algorithme.

Exemple

- Séquence jouet générée avec quatre matrices de transitions différentes (coupure à 25%, 50% et 75%).
- Exemple pour la norme matricielle 1 :

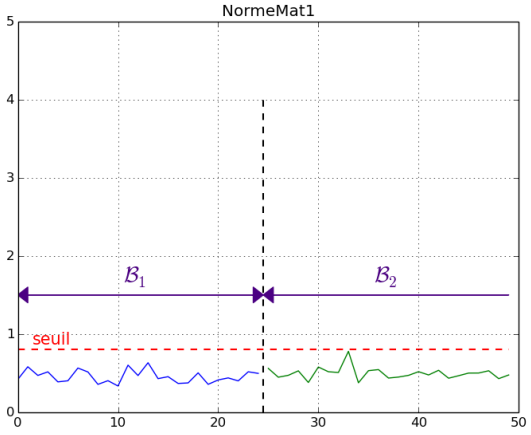
$$||R||_{1\text{Mat}} = \max_{0 \leqslant j \leqslant 2^M - 1} \sum_{i=0}^{2^M - 1} |r_{ij}|,$$

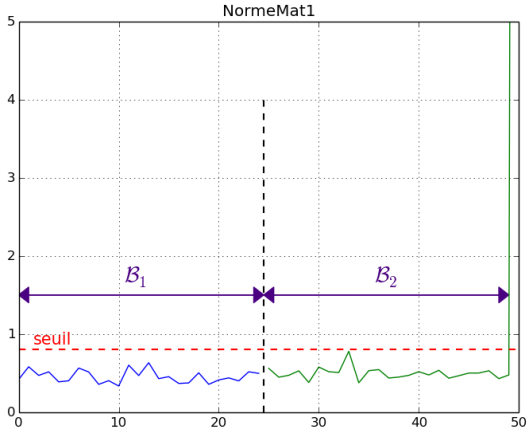




Exemple

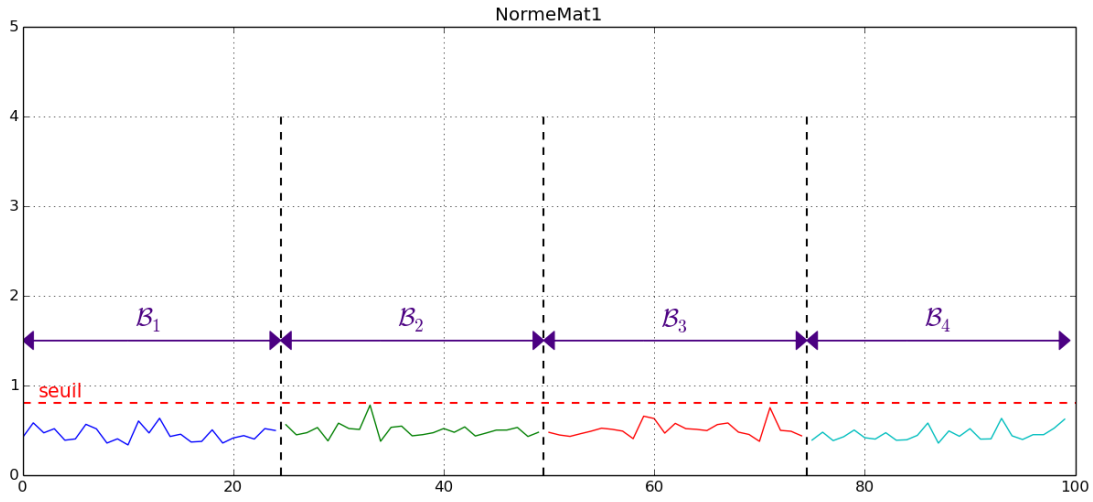
- Séquence jouet générée avec quatre matrices de transitions différentes (coupure à 25%, 50% et 75%).





Exemple

- Séquence jouet générée avec quatre matrices de transitions différentes (coupure à 25%, 50% et 75%).



Exemple sur un générateur industriel

- Phénomène physique : bruit de phase.

Nb de blocs	Alphabit [LS07] (% réussis)	Rabbit [LS07] (% reussis)
1	71%	82%

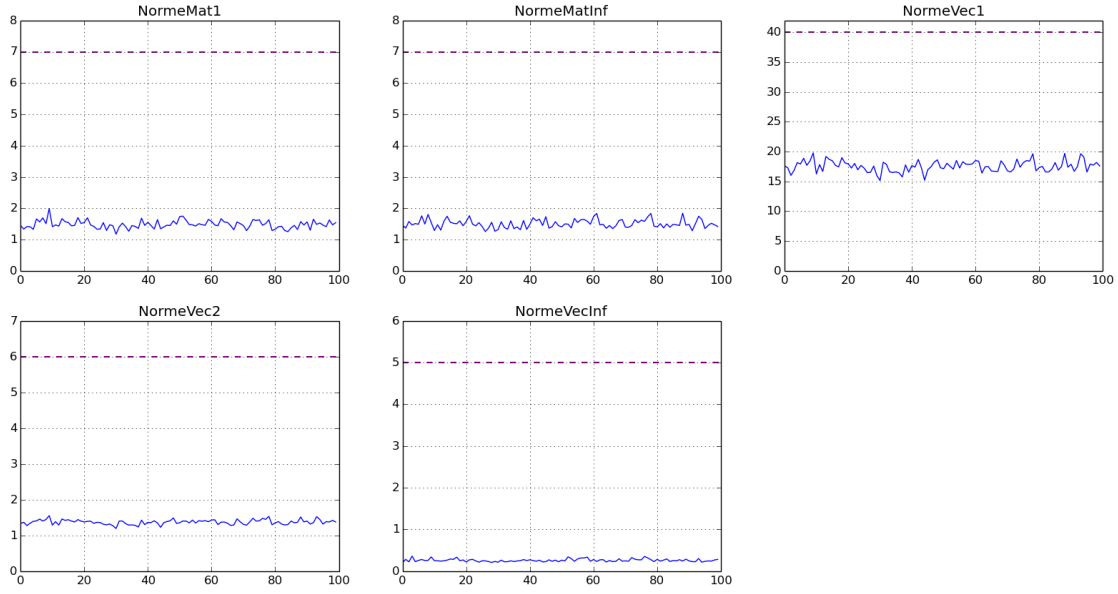


FIGURE : Évolution des matrices d'erreurs relatives pour la séquence avant et après découpage

Exemple sur un générateur industriel

Nb de blocs	Alphabit (% réussis)	Rabbit (% reussis)
13	0%	15%

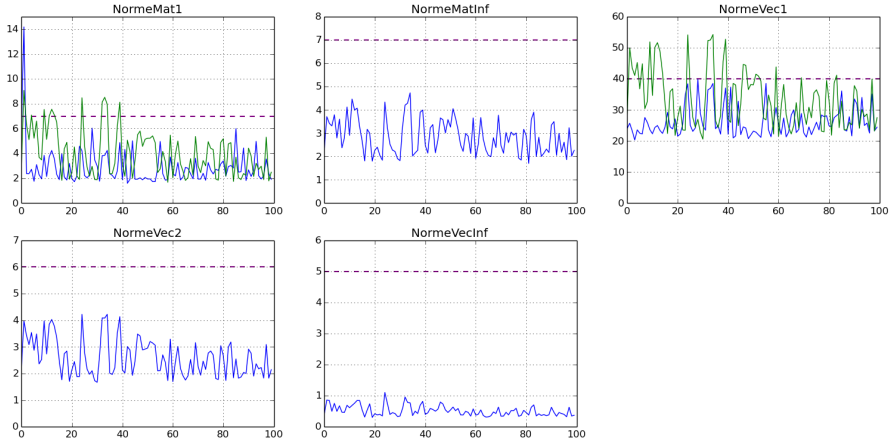


FIGURE : Évolution des matrices d'erreurs relatives pour la séquence avant et après découpage

- Sur le plus grand bloc homogène de la séquence : Alphabit 0% et Rabbit 24%.
  $\rightarrow$ autres défauts que l'hétérogénéité.

Solutions proposées

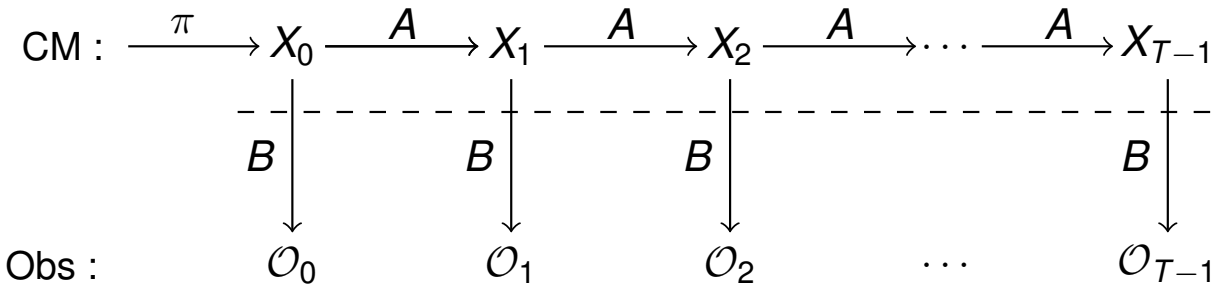
Problématique : Hypothèse implicite de l'homogénéité des séquences.

Proposition : Analyse temporelle de l'homogénéité des séquences basée sur les chaînes de Markov.

Problématique : Modèles statistiques éloignés des réalités physiques.

Proposition : Étude des modèles de Markov cachés (HMM) pour l'analyse des générateurs.

Modèles de Markov cachées (HMM)

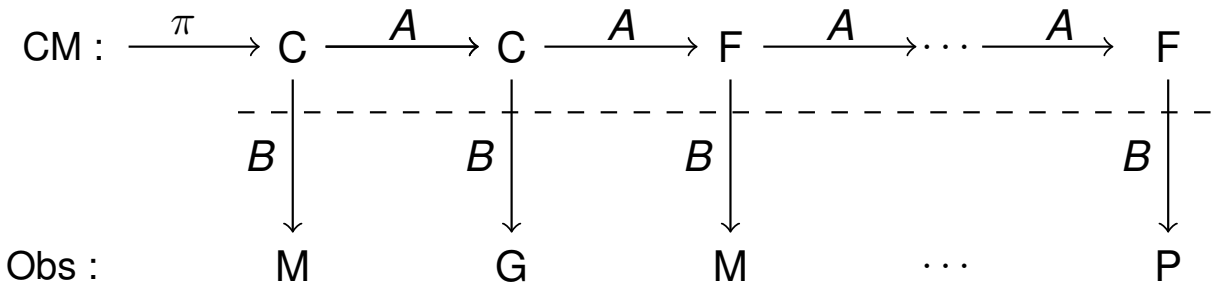


- Une chaîne de Markov homogène $(X_k)_k$ qui n'est pas directement observable.
- Une suite d'observation $(\mathcal{O}_k)_k$ qui dépend de la chaîne de Markov.
- Un modèle est noté $\lambda = (\pi, A, B)$.

Exemple pour la dendrochronologie

- Étude de la température en fonction de la taille des cernes des arbres.
- Deux températures : Froid (F) et Chaud (C).
- Trois tailles : Petit (P), Moyen (M) et Grand (G).

$$\pi = \begin{array}{cc} C & F \\ (0.6 & 0.4) \end{array}, \quad A = \begin{array}{c} \\ C \\ F \end{array} \begin{array}{c} \begin{array}{cc} C & F \end{array} \\ \begin{pmatrix} 0.7 & 0.3 \\ 0.4 & 0.6 \end{pmatrix} \end{array}, \quad B = \begin{array}{c} \\ C \\ F \end{array} \begin{array}{c} \begin{array}{ccc} P & M & G \end{array} \\ \begin{pmatrix} 0.1 & 0.4 & 0.5 \\ 0.7 & 0.2 & 0.1 \end{pmatrix} \end{array}.$$



Problèmes liés aux HMM

Problème 1

Connaissant le modèle $\lambda = (\pi, A, B)$ et les observations $\mathcal{O}$, on cherche à calculer la probabilité $P(\mathcal{O}|\lambda)$ que ces observations correspondent au modèle.

$$\pi = \begin{array}{cc} C & F \\ \end{array} \begin{pmatrix} 0.6 & 0.4 \end{pmatrix}, \quad A = \begin{array}{c} C \\ F \end{array} \begin{array}{cc} C & F \\ \end{array} \begin{pmatrix} 0.7 & 0.3 \\ 0.4 & 0.6 \end{pmatrix}, \quad B = \begin{array}{c} C \\ F \end{array} \begin{array}{ccc} P & M & G \\ \end{array} \begin{pmatrix} 0.1 & 0.4 & 0.5 \\ 0.7 & 0.2 & 0.1 \end{pmatrix}.$$

- On connaît $\mathcal{O} = (G, P)$.
- $P(\mathcal{O}|\lambda) = \sum_X P(\mathcal{O}, X|\lambda)$.

Méthode de Baum-Welch (voir problème 3).

Problèmes liés aux HMM

Problème 2

Connaissant le modèle $\lambda = (\pi, A, B)$ et les observations $\mathcal{O}$, on cherche à calculer la séquence d'états optimale correspondant à la chaîne de Markov cachée.

$$\pi = \begin{array}{cc} C & F \\ \end{array} \begin{pmatrix} 0.6 & 0.4 \end{pmatrix}, \quad A = \begin{array}{c} \\ C \\ F \end{array} \begin{array}{cc} C & F \\ \end{array} \begin{pmatrix} 0.7 & 0.3 \\ 0.4 & 0.6 \end{pmatrix}, \quad B = \begin{array}{c} \\ C \\ F \end{array} \begin{array}{ccc} P & M & G \\ \end{array} \begin{pmatrix} 0.1 & 0.4 & 0.5 \\ 0.7 & 0.2 & 0.1 \end{pmatrix}.$$

- On connaît $\mathcal{O} = (G, P)$.
- X_o telle que $P(\mathcal{O}, X_o|\lambda) = \max_X P(\mathcal{O}, X|\lambda)$.
- $X_o = (X_{1,o}, X_{2,o})$ telle que pour tout i, $P(\mathcal{O}, X_{i,o}|\lambda) = \max_{X_j} P(\mathcal{O}, X_j|\lambda)$.

Méthode de Baum-Welch (pb 3) ou algorithme de Viterbi.

Exemple problème 2

Pour une séquence d'observation : $\mathcal{O} = (P, M, P, G)$

États	$P(X, \mathcal{O}\|\lambda)$	Probabilité Normalisée
CCCC	$4.116 \cdot 10^{-4}$	0.0427
CCCF	$3.528 \cdot 10^{-5}$	0.0037
CCFC	$7.056 \cdot 10^{-4}$	0.0733
CCFF	$2.117 \cdot 10^{-4}$	0.0220
CFCC	$5.040 \cdot 10^{-5}$	0.0052
CFCF	$4.320 \cdot 10^{-6}$	0.0004
CFFC	$3.024 \cdot 10^{-4}$	0.0314
CFFF	$9.072 \cdot 10^{-5}$	0.0094
FCCC	$1.098 \cdot 10^{-3}$	0.1140
FCCF	$9.408 \cdot 10^{-5}$	0.0098
FCFC	$1.882 \cdot 10^{-3}$	0.1954
FCFF	$5.645 \cdot 10^{-4}$	0.0586
FFCC	$4.704 \cdot 10^{-4}$	0.0489
FFCF	$4.032 \cdot 10^{-5}$	0.0042
FFFC	$2.822 \cdot 10^{-3}$	0.2931
FFFF	$8.467 \cdot 10^{-4}$	0.0879

TABLE : Calcul des probabilités selon le point de vue programmation dynamique.

Exemple Problème 2

Pour une séquence d'observation : $\mathcal{O} = (P, M, P, G)$

Symbole	Position 1	Position 2	Position 3	Position 4
C	0.1881	0.5195	0.2289	0.8040
F	0.8119	0.4805	0.7711	0.1960

TABLE : Calcul des probabilités selon le modèle des chaînes de Markov.

- Les deux séquences sont différentes : FFFC et FCFC.
- Deux méthodes de résolutions en fonction du point de vue.

Problèmes liés aux HMM

Problème 3

Connaissant les observations $\mathcal{O}$ ainsi que les dimensions de A et de B, on cherche à calculer le modèle $\lambda = (\pi, A, B)$ qui maximise la probabilité de $P(\mathcal{O}|\lambda)$.

- On connaît $\mathcal{O} = (G, P)$.
- $\hat{\lambda} = (\hat{\pi}, \hat{A}, \hat{B})$ tel que $P(\mathcal{O}|\hat{\lambda}) = \max_{\lambda} P(\mathcal{O}|\lambda)$.

Résolution du problème 3 : Inférences des modèles

- Méthodes itératives :
  - Initialisation avec λ_0.
  - Estimation de λ_{i+1} à partir de λ_i.
  - Calcul de $P(\mathcal{O}|\lambda_{i+1})$.
  - Si $P(\mathcal{O}|\lambda_{i+1}) > P(\mathcal{O}|\lambda_i)$ on continue les itérations.
- Méthode de Baum-Welch [BPW70] et méthode du gradient [CBM98].
- La différence entre les méthodes est sur l'étape d'estimation de λ_{i+1}.
  - Calcul d'espérance de transitions (BW).
  - Descente de gradient (G).

Distance entre les modèles

Première idée de distance :

$$d(A, A') = \sqrt{\frac{1}{N} \sum_{i=0}^{N-1} \sum_{j=0}^{M-1} (A_{ij} - A'_{ij})^2}.$$

Contre exemple :

$$A = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix},$$

et

$$A' = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}, \quad B' = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ 0 & 1 \end{pmatrix},$$

produisent la même séquence $\mathcal{O} = (1, 1, 1, 1, \dots)$.

Distance entre les modèles

- Distance idéale :
  - Tenir compte de la construction des matrices des modèles.
  - Tenir compte des séquences produites par les modèles.
- Variante de la divergence de Kulback-Liebler [Kul68], pour deux modèles λ et λ' :

$$\mathcal{D}(\lambda, \lambda') = \frac{1}{T} \log \left(\frac{\sum_{i=0}^{N-1} \xi(\lambda, i, T)}{\sum_{i=0}^{N-1} \xi(\lambda', i, T)} \right),$$

avec pour $t \in \{1, \ldots, T\}$:

$$\xi(\lambda, i, t) = \sum_{j=0}^{N-1} NA_{ji}\, B_{j\mathcal{O}_t}\, \xi(\lambda, j, t-1).$$

Exemple

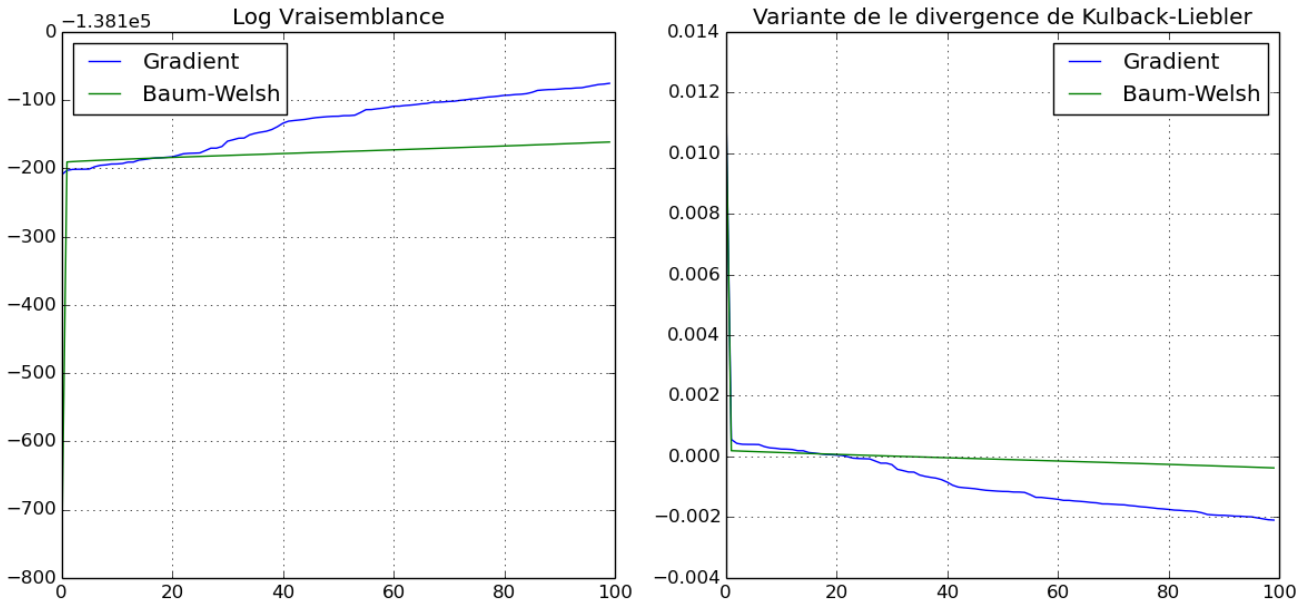


FIGURE : Méthodes de Baum-Welch et de gradient $T = 50\,000$, $I = 100$, $A_0 = M_R$ et $B_0 = M_R$.

Implantation

En Pari/GP sur un processeur Intel Core i7-3840QM 2.8GHz :

N	T	Itérations	Baum-Welch (s)	Gradient (s)
16	1 000	10	17	33
16	10 000	10	177	347

TABLE : Comparaison des temps de calcul entre l'algorithme de Baum Welch et du gradient.

Utilisation des HMM

- Simulation de propriétés statistiques :
  - Séquence construite sur le modèle λ.
  - Inférence du modèle par méthode BW ou G $\rightarrow \hat{\lambda}$.
  - Construction d'une séquence basée sur $\hat{\lambda}$.
  - Comparaison des résultats aux tests statistiques

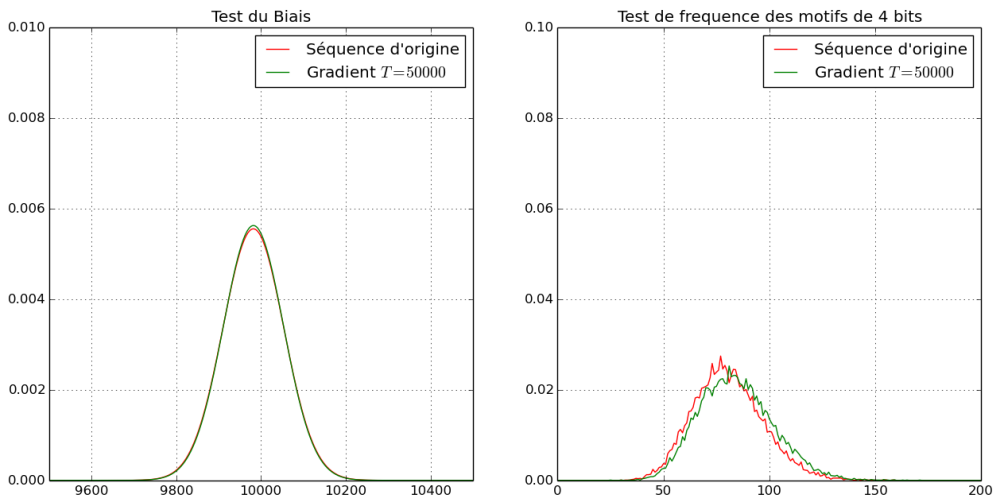


FIGURE : Comparaison du comportement statistique entre la séquence `HMM_R` et la séquence issue du modèle $\lambda_{\mathrm{R,G,50\,000,A}}$.

Outline

Contributions et perspectives

- Proposer des modèles stochastiques pour de nouvelles sources d'entropies.
  - Définir le comportement probabiliste des sources.

  → Proposer des estimations d'entropie.

  → Définir des tests dédiés aux modèles.
- Élargir les modèles utilisés dans les tests statistiques :
  - Étude des chaînes de Markov et proposition de tests statistiques.
  - Étude des chaînes de Markov cachées.

  → Proposition de tests à base de HMMs.
- Présenter une étude temporelle des séquences :
  - Outil de découpage en blocs homogènes basés sur les chaînes de Markov.

  → Étude temporelle pour d'autres modèles.

FIN

Merci pour votre attention.

ANSSI.
Annexe b1 au référentiel général de sécurité (version 2.0) : Choix et dimensionnement des mécanismes cryptographiques, 2014.
http://www.ssi.gouv.fr/uploads/2014/11/RGS_v-2-0_B1.pdf.

F. Bernard, V. Fischer, and B. Valtchanov.
Mathematical Model of Physical RNGs Based On Coherent Sampling.

Tatra Mountains - Mathematical Publications, 2010.
https://hal-ujm.archives-ouvertes.fr/ujm-00531665/file/2010_tatra.pdf.

Elaine Barker, John Kelsey, and John Bryson Secretary.
Nist draft special publication 800-90b recommendation for the entropy sources used for random bit generation, 2012.
http://csrc.nist.gov/publications/drafts/800-90/draft-sp800-90b.pdf.

M. Baudet, D. Lubicz, J. Micolod, and A. Tassiaux.
On the security of oscillator-based random number, 2010.
https://perso.univ-rennes1.fr/david.lubicz/articles/gda.pdf.


L.E. Baum, G.S. Petrie, and N. Weiss.
A maximization technique occuring in the statistical analysis of probabilistic functions of markov chains.
Annals of Mathematical Statistics 41, 1970.
http://projecteuclid.org/download/pdf_1/euclid.aoms/1177697196.


O. Cappe, V. Buchoux, and E. Moulines.
Quasi-newton method for maximum likelihood estimation of hidden markov models.
Speech and Signal Processing, ICASSP98, 1998.
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.38.1821&rep=rep1&type=pdf.


A. Cherkaoui, V. Fischer, A. Aubert, and L. Fesquet.
A self-timed ring based true random number generator.
International symposium on advanced research in asynchronous circuits and systems, 2013.
https://hal.archives-ouvertes.fr/ujm-00840593/document.


R. J. Cook and H. J. Kimble.
Possibility of direct observation of quantum jumps.
Physical Review Letters, 1985.
http://authors.library.caltech.edu/10990/1/COOprl85.pdf.

N. Heninger.
There's no need to panic over factorable keys–just mind your ps and qs, 2012.
https://freedom-to-tinker.com/blog/nadiah/new-research-theres-no-need-panic-over-factorable-keys

W. Killmann and W. Schindler.
A proposal for : Functionality classes for random number generators, 2011.
http://www.ibbergmann.org/AIS31_Functionality_classes_for_random_number_generators.pdf.

S. Kullback.
Information theory and statistics.
Courier Corporation, 1968.

A. K. Lenstra, J. P. Hughes, M. Augier, J. W. Bos, T. Kleinjung, and C. Wachter.
Ron was wrong, whit is right, 2012.
https://eprint.iacr.org/2012/064.pdf.

P. L'Ecuyer and R. Simard.
Testu01 : A c library for empirical testing of random number generators.
ACM TRANSACTIONS ON MATHEMATICAL SOFTWARE, 2007.
http://www.iro.umontreal.ca/~lecuyer/myftp/papers/testu01.pdf.


P.Q. Nguyen and I.E. Shparlinski.
The insecurity of the digital signature algorithm with partially known nonces.
Journal of Cryptology, 2002.
http://link.springer.com/article/10.1007/s00145-002-0021-3.


Fail Overflow.
Consol hacking 2010 : Ps2 epic fail, 2010.
https://events.ccc.de/congress/2010/Fahrplan/attachments/1780_27c3_console_hacking_2010.pdf.


ID Quantique.
Quantis-oem application note.
2010.
http://www.idquantique.com/images/stories/PDF/quantis-random-generator/quantis-appnote.pdf.


ID Quantique.
Random number generation using quantum physics.
2010.
http://www.idquantique.com/images/stories/PDF/quantis-random-generator/quantis-whitepaper.pdf.


B. Valeur.
Lumière et luminescence : ces phénomènes lumineux qui nous entourent.
2005.


M. Varchola and M. Drutarovsky.
New high entropy element for fpga based true random number generators.
In *Cryptographic Hardware and Embedded Systems, CHES 2010*, volume 6225 of *Lecture Notes in Computer Science*, pages 351–365. 2010.
http://www.iacr.org/archive/ches2010/62250341/62250341.pdf.


D. Lubicz V. Fisher.
Embedded evaluation of randomness in oscillator based elementary trng.
Workshop on Cryptographic Hardware and Embedded Systems 2014 (CHES 2014), 2014.


I. Vasyltsov, E. Hambardzumyan, K. Young-Sik, and B. Karpinskyy.
Fast digital trng based on metastable ring oscillator.
5154 :164–180, 2008.
https://www.iacr.org/archive/ches2008/51540162/51540162.pdf.