COMMUNAUTÉS DE RECHERCHE ACADÉMIQUE RhôneAlpes
T.I.C. ET USAGES INFORMATIQUES INNOVANTS
LABORATOIRE Hubert CURIEN UMR • CNRS • 5516 • ST-ETIENNE
CNRS - Grenoble INP - UJF

Génération de Nombres Aléatoires à l'aide de Circuits Asynchrones

Avril 2013

Abdelkarim CHERKAOUI
Viktor FISCHER
Alain AUBERT
LaHC / SES group
Laurent FESQUET
TIMA / CIS group

RhôneAlpes Région

Contexte

- **« Générateurs de nombres aléatoires vrais enfouis dans des circuits asynchrones »**
  - Thèse en cotutelle LaHC (Saint-Etienne) et TIMA (Grenoble)
  - Démarrée fin 2010, financée par la région Rhône-Alpes

- **Motivations de ces recherches**
  - Evolution des méthodes d'évaluation des TRNGs (True Random Number Generator)
  - Effort récents de standardisation des TRNGs (norme AIS31)
  - Résultats récents sur les anneaux de Muller et leur applications

Généralités sur les RNGs

- La cryptographie moderne est basée sur la confidentialité des clés échangées
- Les clés secrètes doivent être **imprévisibles**, non manipulables et avoir de bonnes propriétés statistiques
- RNG idéal = objet mathématique générant des nombres aléatoires indépendants et uniformément répartis

En pratique

DRNG = Deterministic Random Number Generator

TRNG = True Random Number Generator

- Les TRNGs exploitent une source physique d'aléa
  - Phénomènes quantiques (radioactivité, photon vs lame réfléchissante)
  - Bruit thermique omniprésent dans les circuits électroniques

Evaluation des RNGs

- TRNGs et DRNGs : Evaluation de séquences de bits à l'aide de tests statistiques standard (NIST, FIPS, DIEHARD)

- TRNGs : Modélisation de la source physique et de l'extraction d'entropie, entropie minimale par bit de sortie du TRNG

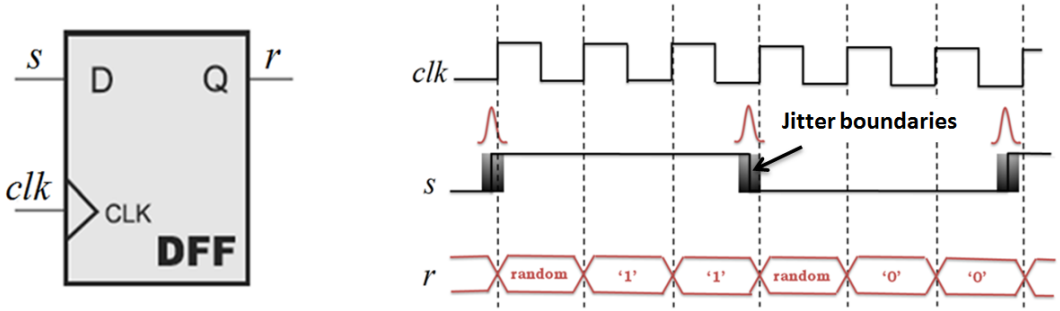
- La norme AIS31 (proposée par la BSI, agence gouvernementale allemande) définit les critères d'évaluation pour les TRNGs
  - Bonnes propriétés statistiques (commun avec les DRNGs)
  - Imprévisibilité : preuve par la modélisation de la source d'entropie

- 3 classes de fonctionnalité pour les TRNGs
  - **PTG.1 :** TRNG + testabilité (total failure, startup et online tests)
  - **PTG.2 :** PTG.1 + modèle stochastique
  - **PTG.3 :** PTG.2 + post-traitement cryptographique (ex : AES)

TRNGs dans les circuits numériques

- 2 techniques pour extraire le bruit
  - A partir du jitter (instabilité temporelle d'un signal oscillant due au bruit)
  - Résolution d'une situation de métastabilité

- Extraction du jitter
  - Comptage d'un signal oscillant, résolution d'un circuit bistable
  - Echantillonnage d'un signal pendant son basculement

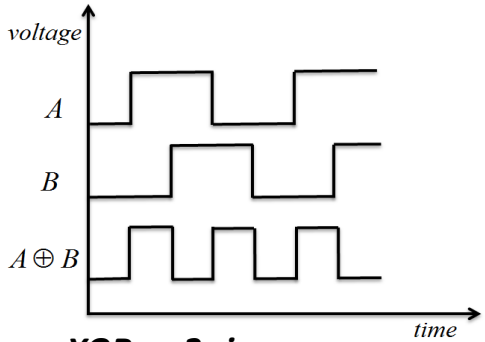


Générateur de nombres aléatoires simple utilisant une bascule et deux signaux oscillants

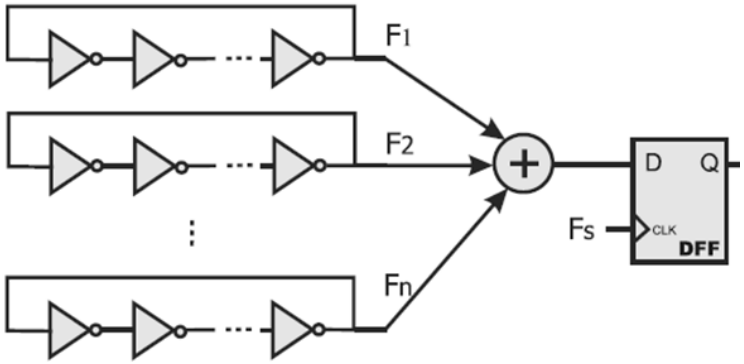
- Difficultés
  - Taille du jitter (<1% de la période d'oscillation, de l'ordre de la picoseconde)
  - Problèmes de synchronisation, de temporisations

Extraction du jitter d'oscillateurs en anneau

- Approche globale avec des anneaux à inverseurs
  - « Raccourcir » le temps entre 2 événements successifs
  - Problème du collecteur de coupons
  - En pratique : une centaine de RO de 9 étages pour extraire un jitter = 2% de la période d'oscillation
  - Phase-drift => pseudo-aléa + locking



XOR-er 2 signaux pour « rapprocher » des événements dans le temps



Extraction du jitter de plusieurs anneaux à inverseurs

- STRNG (Self-timed ring based TRNG)
  - Réglage précis et contrôle du temps écoulé entre événements successifs
  - Evénements synchronisés (pas de pseudo-aléa)
  - Réduction importante de la surface

B. Sunar, W.J. Martin, and D.R. Stinson, "A Provably Secure True Random Number Generator with Built-In Tolerance to Active Attacks". IEEE Transactions on Computers, Vol. 58, pp. 109-119 (2007)

Plan

Contexte

I – Introduction

II – Générateur de Nombres Aléatoires Vrais à base d'Anneau de Muller

- **Principe de fonctionnement**
- **Architecture et caractéristiques de l'anneau**
- **Comportement temporel**

IV – Modélisation du Générateur

- **Courbes d'entropie**
- **Usage pratique du modèle**

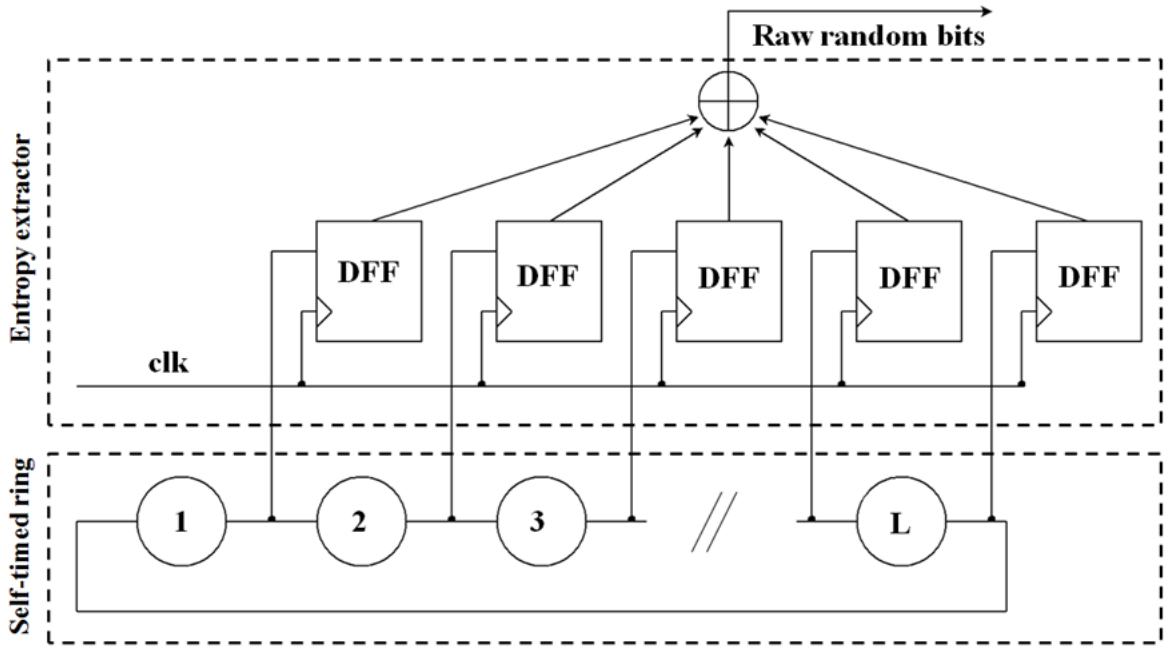
V – Implantation sur des cibles FPGA

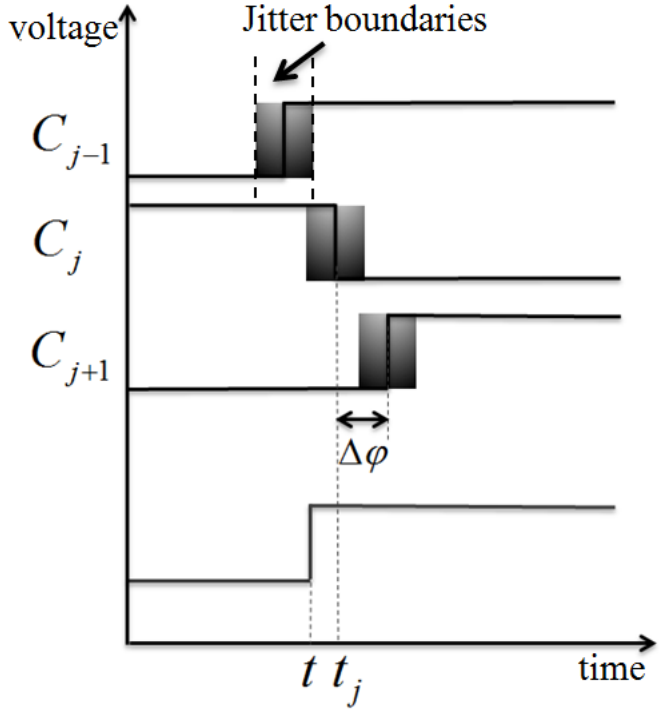
- **Design et contraintes d'implantation**
- **Mesures et évaluation statistique**

Conclusion

II – STRNG (Self-timed Ring Based TRNG)

Principe de fonctionnement





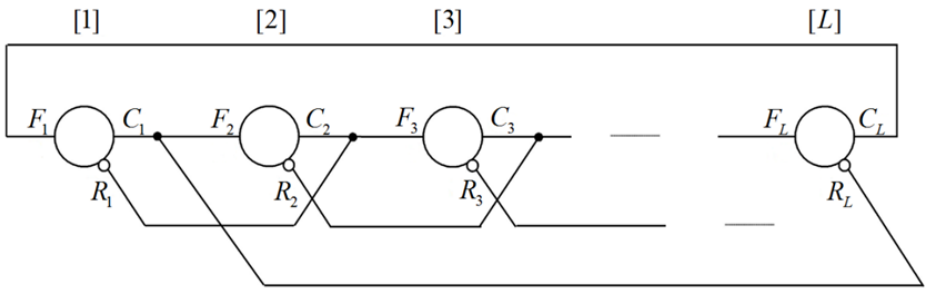
- Les anneaux de Muller permettent une résolution de phase fractionnaire du temps de propagation d'un étage
- Le jitter mesuré à la sortie d'un étage est majoritairement issu d'un bruit blanc généré localement dans cet étage

---

A. Cherkaoui, V. Fischer, A. Aubert and L. Fesquet, "A Self-timed Ring based True Random Number Generator", in proceedings of the International Symposium on Asynchronous Circuits and Systems, ASYNC 2013.

Architecture de l'anneau

- FIFO asynchrone à base de cellules de Muller en boucle fermée



Architecture d'un anneau de Muller

F	R	C
0	0	C^{-1}
0	1	0
1	0	1
1	1	C^{-1}

Table de vérité d'un étage de l'anneau

- Protocole de requêtes/acquittements assurant la propagation des données sans collisions

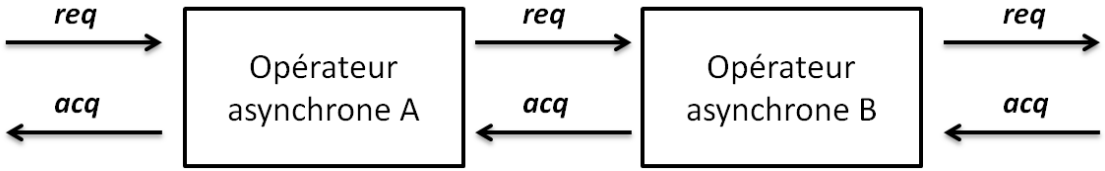


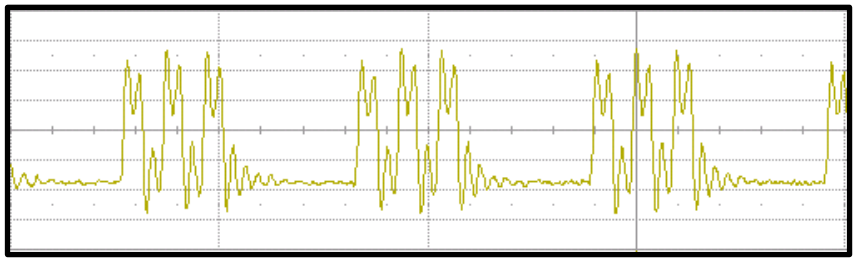
Schéma du protocole de communication

- Abstraction bulles/jetons

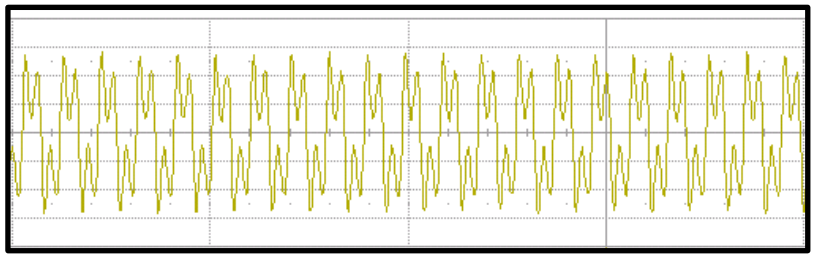
Propagation d'un jeton dans l'anneau

Comportement temporel (1)

- 2 modes d'oscillation



Propagation « burst » de 6 jetons dans un anneau à 24 étages



Propagation « evenly-spaced » de 10 jetons dans un anneau à 24 étages

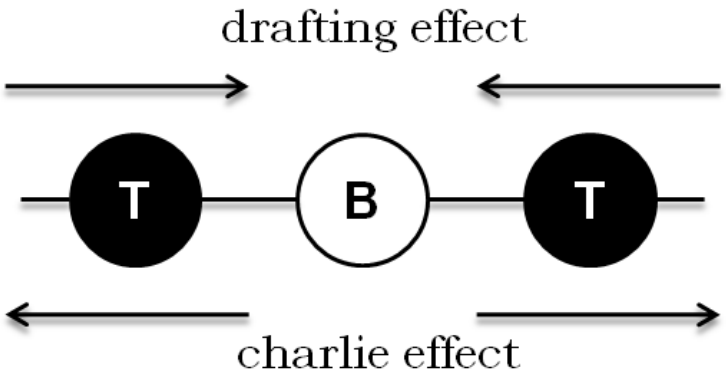
- Phénomènes analogiques intrinsèques à la structure de l'étage

L'effet Charlie

Plus les événement en entrée sont proches plus le temps de propagation est long

L'effet Drafting

Plus le temps séparant deux basculements successifs de la sortie est court, plus le temps de propagation est court

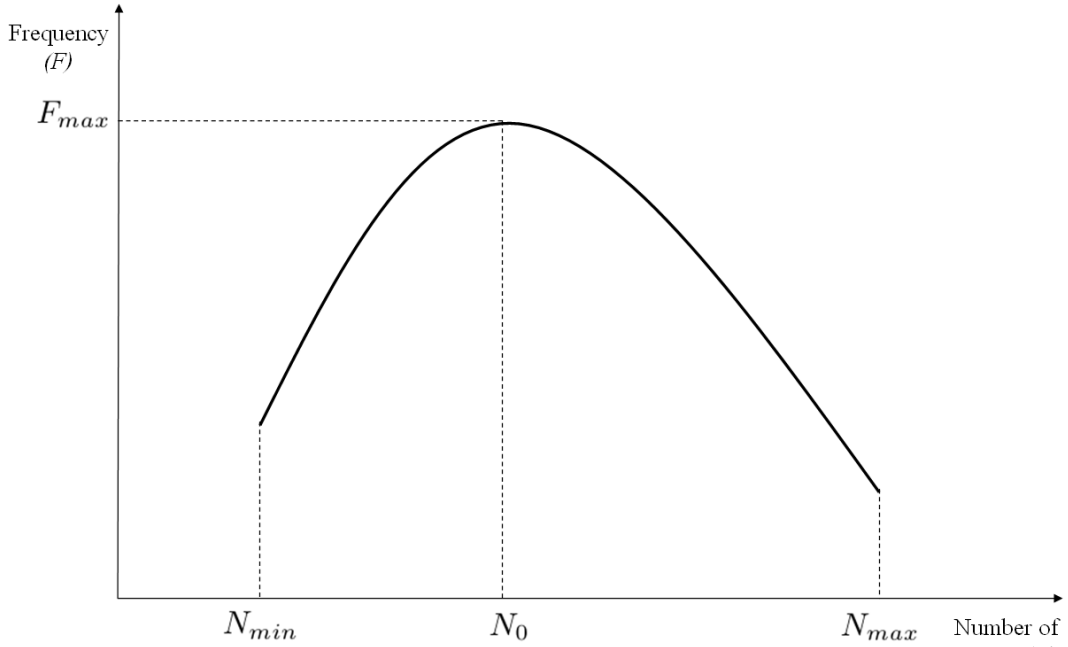


Comportement temporel (2)

- Mode de fonctionnement (*evenly-spaced* ou *burst*) et point de fonctionnement en régime *evenly-spaced* permanent dépendent de
  - Amplitude des effets Charlie et Drafting
  - Rapport *Dff/Drr* (délais de propagation statiques pour les entrées *F* et *R*)
  - Rapport *Nt/Nb* (nombre de jetons/nombre de bulles)

- Le mode *evenly-spaced* pour un anneau à *L* étages est obtenu pour un intervalle de jetons autour de *N* tel que

$$N_0 = \frac{D_{ff}}{D_{rr}} \times (L - N_0)$$



Allure de la courbe de fréquence d'un anneau de Muller en fonction de son taux d'occupation

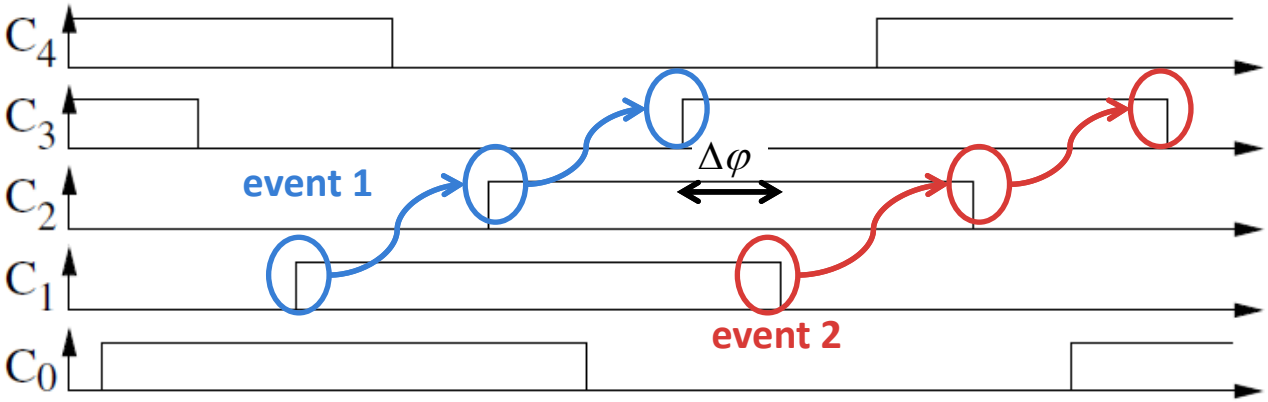
Génération de signaux multi-phase

- Propagation régulière de *N* événements dans un anneau à *L* étages
  - Différence de phase entre deux étages séparés par n étages

$$\varphi_n = n \times \frac{N}{L} \times 180^o$$

  - N et L premiers entre eux => autant de phases que d'étages

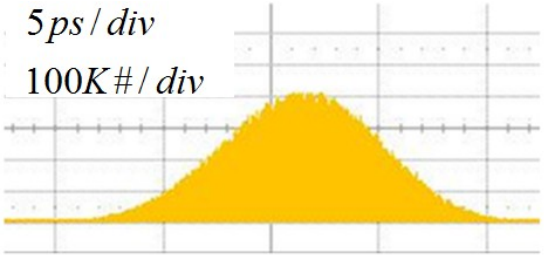
$$\boxed{\Delta\varphi = \frac{T}{2L}}$$



Propagation de 2 événements dans un anneau à 5 étages

S. FAIRBANKS, "High Precision Timing using Self-timed Circuits", Technical report no. UCAM-CL-TR-738, University of Cambridge, Computer Laboratory, January 2009, url: http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-738.pdf

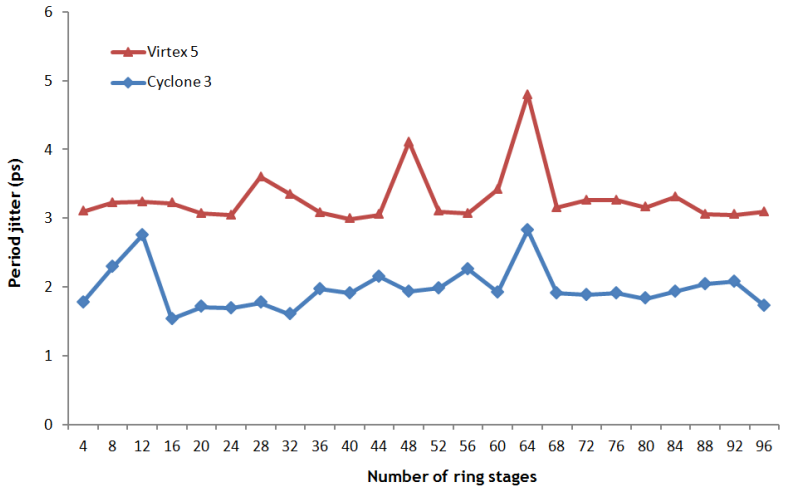
Jitter dans les anneaux de Muller

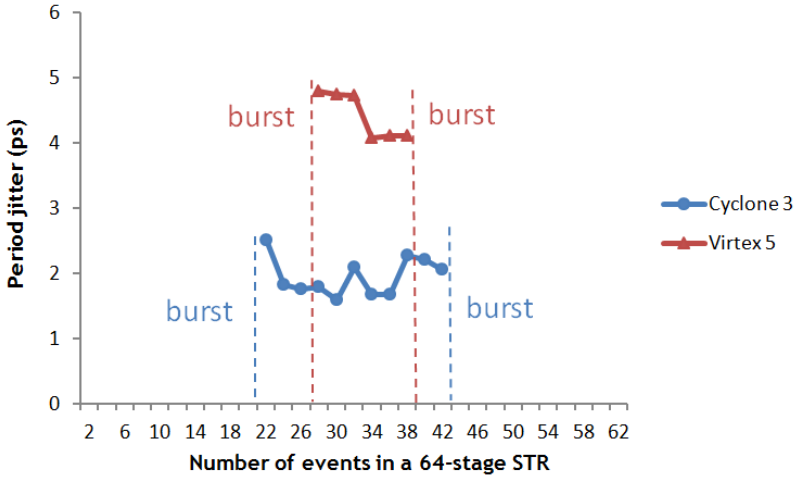


Distribution de la période d'un anneau à 96 étages initialisé avec 42 événements (FPGA Altera) : Gaussienne de faible amplitude

- Le temps qui sépare les événements est asservi par les effets Charlie et Drafting

➡ **Jitter d'un événement issu majoritairement du bruit blanc Gaussien généré localement dans l'étage que traverse cet événement**





A. Cherkaoui, V. Fischer, A. Aubert and L. Fesquet, "Comparison of Self-timed and Inverter Ring Oscillators as Entropy Sources in FPGAs", in Design, Automation and Test in Europe conference, DATE12, pages 1325-1330, March 2012.

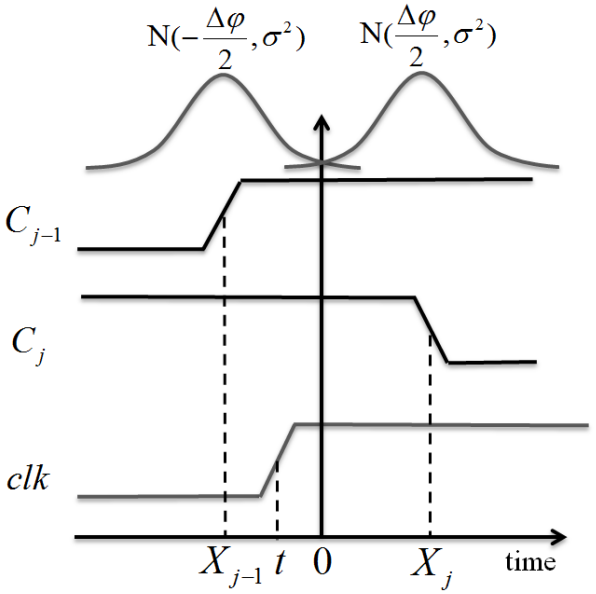
III – Modélisation du STRNG

Modélisation de l'extraction d'entropie

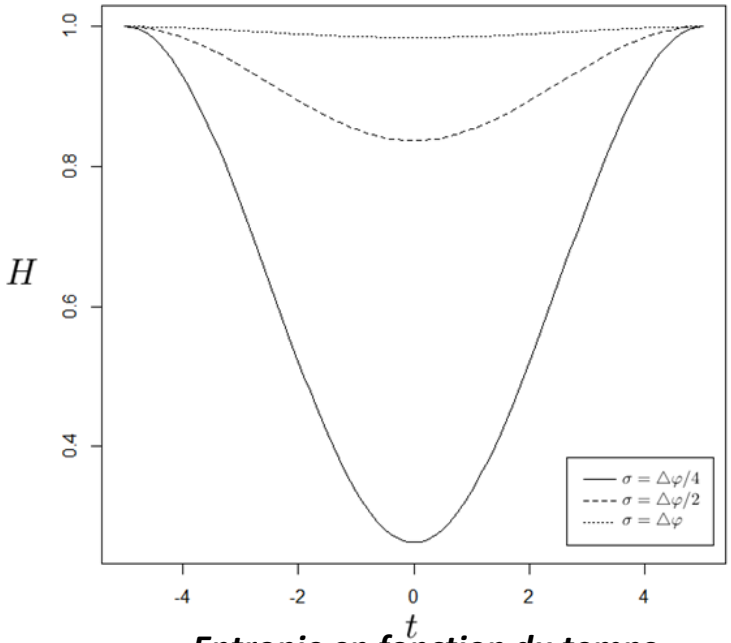
- Probabilité d'échantillonner une donnée 'u' en fonction de l'instant d'échantillonnage

$$P(u) = \Phi\left(\frac{t-\frac{T}{4L}}{\sigma}\right) + \Phi\left(\frac{t+\frac{T}{4L}}{\sigma}\right) - 2\Phi\left(\frac{t-\frac{T}{4L}}{\sigma}\right) \times \Phi\left(\frac{t+\frac{T}{4L}}{\sigma}\right)$$

Fonction de répartition de la loi normale centrée réduite



Modélisation de l'extraction d'entropie



Entropie en fonction du temps

- Entropie en fonction de l'instant d'échantillonnage

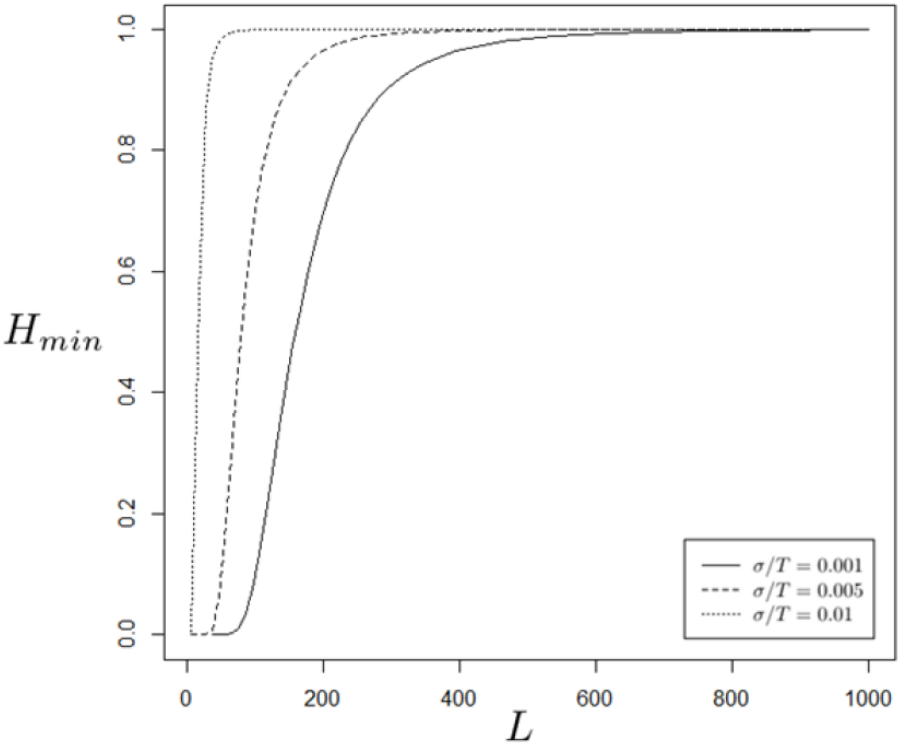
$$H(t) = -P(u)\log_2(P(u)) - (1-P(u))\log_2(1-P(u))$$

Entropie minimale par bit de sortie

- Entropie minimale par bit de sortie, fonction du nombre d'étages, de la période d'oscillation et de la taille du jitter :

$$H_{\min} = -P_{t=0}(u)\log_2(P_{t=0}(u)) - (1-P_{t=0}(u))\log_2(1-P_{t=0}(u))$$

avec $$P_{t=0}(u) = 1 - 2\Phi\left(\frac{T}{4L\sigma}\right) + 2\Phi^2\left(\frac{T}{4L\sigma}\right)$$



Entropie minimale en sortie du STRNG en fonction du nombre d'étages de l'anneau

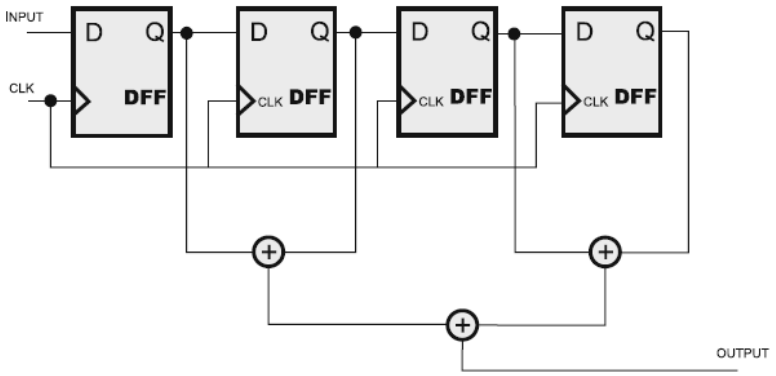
Dimensionnement du générateur

Choisir le nombre d'étages de l'anneau en fonction de paramètres mesurés pour garantir un taux d'entropie minimale visé en sortie du générateur

Stratégie alternative pour le dimensionnement

- Post-traitement arithmétique : filtre de parité

$$p_{out}(u) = 0.5 + 2^{n-1}(p_{in}(u) - 0.5)^n \xrightarrow{n \to \infty} 0$$



Structure d'un filtre de parité d'ordre 4

- Principe : XOR-er n bits successifs en sortie du générateur
  - Augmente l'entropie par bit
  - Mais réduit le débit par n

- Intérêt : réglage surface/consommation VS débit

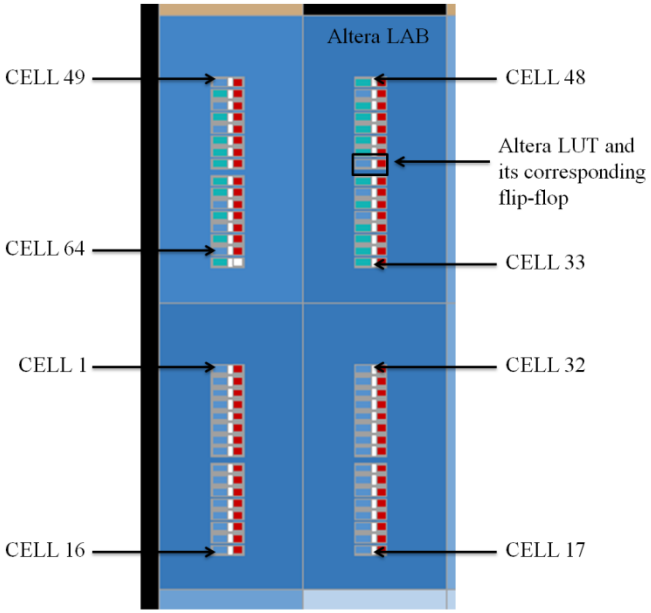
V – Implantation dans des cibles FPGA

Implantation à base de LUTs

- 1 LUT (Look-up-table) à 4 entrées par étage
  - 2 entrées pour les signaux *F* et *R*
  - 1 entrée rebouclée à la sortie pour l'état mémoire
  - 1 entrée d'initialisation (*SET* ou *RESET*)

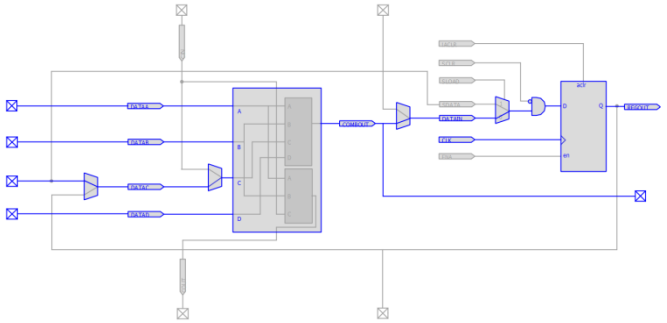
I0	I1	I2	I3	S
0	0	0	0	0
0	0	0	1	1
0	0	1	0	0
0	0	1	1	0
0	1	0	0	1
0	1	0	1	1
0	1	1	0	0
0	1	1	1	1
1	-	-	-	0

Description d'un étage de l'anneau avec un générateur de fonctions à 4 entrées



Topologie d'un anneau à 63 étage sur Altera Cyclone 3

- Topologie évitant les « bottlenecks »
- Connexions étage / bascule « hard-wired »



Mesures et Evaluation

- Mesures et tests AIS31 (~ 1 Mo de données) à 400 Mbit/s

Device	STR		Measurements		Model		Raw data		Compressed data		
	L	N	T	$\triangle\varphi$	H_{min}	n_{min}	T1-T4	T5-T8	$n_{p_{min}}$	AIS31	Throughput
Cyclone III	63	32	2.44 ns	19.3 ps	0	-	0%	0/4	7	PASS	57 Mbit/s
	127	64	3.11 ns	12.2 ps	0.02	483	0%	0/4	4	PASS	100 Mbit/s
	255	128	2.93 ns	5.7 ps	0.58	7	45%	1/4	2	PASS	200 Mbit/s
	511	256	3.31 ns	3.2 ps	0.91	2	99%	3/4	2	PASS	200 Mbit/s
Virtex 5	63	32	2.82 ns	21.4 ps	0	-	0 %	0/4	8	PASS	50 Mbit/s
	127	64	2.83 ns	11.8 ps	0.13	60	10 %	1/4	3	PASS	133 Mbit/s
	255	128	2.45 ns	5.5 ps	0.78	4	58%	2/4	2	PASS	200 Mbit/s
	511	256	2.87 ns	2.9 ps	0.97	2	61%	3/4	2	PASS	200 Mbit/s

Nombre d'étages (L), nombre d'événements (N), période d'oscillation (T), résolution de phase (phi), entropie minimale en sortie (H_min), ordre minimal du filtre pour atteindre 0.99 (n_min), Résultats des tests AIS31 sur les données brutes (Raw data), ordre minimal du filtre en pratique pour passer tous les tests (np_min), débit effectif (throughput), Jitter (déviation standard) = 2 ps pour Cyclone, 2.5 ps pour Virtex

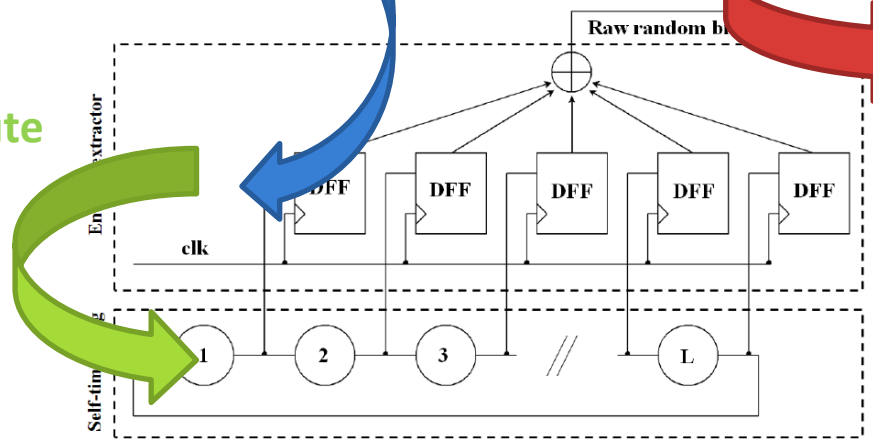
- Tests NIST (~ 120 Mo de données)
  - Cyclone *L=511*, filtre d'ordre 3, débit effectif = 133 Mbit/s
  - Virtex *L=511*, filtre d'ordre 4, débit effectif = 100 Mbit/s

Perspectives : durcissement du générateur

Attaques EM :
- harmonique
- pulse

Injection de signal déterministe via le rail d'alim

Injection de faute par lasers



Principale menace : blocage de l'anneau ou modification du nb de bulles/jetons

Contremesure : contrôler en permanence le nombre d'événements qui circulent

- Contre-mesures
  - Nombre d'étages premier
  - Alarme : Mesure de fréquence

- Test embarqués
  - Test de biais et suites successives de '0' (Runs)

Conclusion

- L'anneau de Muller permet de résoudre plusieurs problématiques
  - Réglage fin du temps écoulé entre événements successifs
  - Asservissement des temps grâce à des effets inhérents à la structure des étages, ne nécessitant pas de synchronisation externe
  - Robustesse aux bruits déterministes, dominance du bruit blanc Gaussien

- Générateur de nombres aléatoires vrais à base d'anneau de Muller (STRNG)
  - Possibilité d'extraire le jitter quelque soit sa taille à très haut débit (~200 Mbit/s sur cibles FPGA)
  - Le taux d'entropie en sortie est réglable par le design (nombre d'étages de l'anneau)
  - La surface, consommation et débit peuvent être facilement adaptés en fonction du cahier de charges

The End