CHES 2013
Workshop on Cryptographic Hardware and Embedded Systems

A VERY HIGH SPEED TRUE RANDOM NUMBER GENERATOR WITH ENTROPY ASSESSMENT

A. Cherkaoui [1 2], V. Fischer [2], L. Fesquet [1] and A. Aubert [2]

[1] TIMA laboratory (Grenoble – FRANCE)
[2] Hubert Curien laboratory (Saint-Etienne – FRANCE)

Santa Barbara, August 2013

Context of this Work

- **Cryptography (confidential keys)**
  - **Unpredictable,** non manipulable, good statistical properties

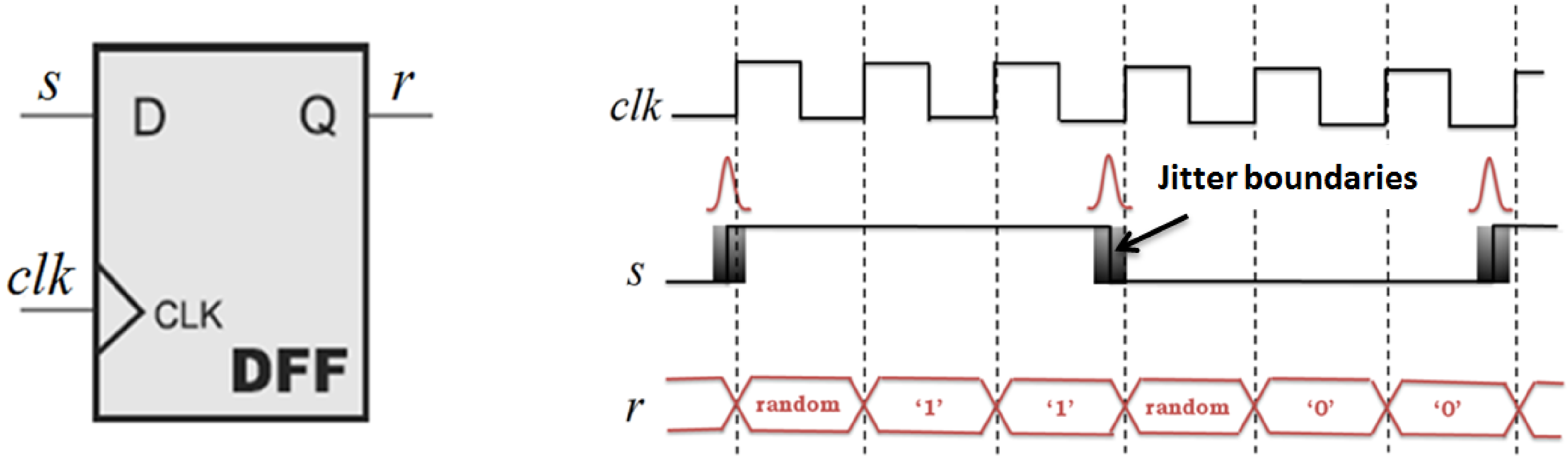
- **Ideal RNG** = generates **independent** and **uniformly distributed** random numbers

In practice
- **DRNG** = Deterministic Random Number Generator
- **TRNG** = True Random Number Generator

- **TRNGs** exploit **physical random processes** (e.g. radioactivity, electrical noise, jitter …)

- **Unpredictability** = **entropy per output bit** of the TRNG (**physical model** of the entropy source and extraction)

Extracting Random Numbers from Jitter



Simple TRNG using a flip-flop and two oscillating signals [1]

- **Challenges**
  - Jitter zone around a signal edge is very short (<1% of the oscillation period)
  - Synchronisation (be in time with the jitter)

[1] R.C. Fairfield, R.L. Mortenson and K.B. Coulthart, "An LSI Random Number Generator (RNG)", in the proceedings of CRYPTO 84 on Advances in cryptology, pages 203-230, NY USA, 1985.

Self-timed Ring based TRNG

- **STR** = oscillators in which several events propagate without colliding
- **STR highly suitable as source of random jitter [2]**
- **Self-timed ring based TRNG (STRNG) presented in [3]**
  - TRNG principle and basic mechanisms
  - Prototype in Altera and Xilinx FPGAs
  - Statistical evaluation at 16 Mbit/s
  - Main features: extracts randomness from the jitter of a STR, regardless the jitter magnitude + no synchronisation is needed

---

[2] 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.

[3] A. Cherkaoui, V. Fischer, L. Fesquet and A. Aubert, "A Self-timed Ring Based True Random Number Generator". In the International symposium on advanced research in asynchronous circuits and systems – ASYNC 2013. Pp. 99-106. Santa Monica, California, USA (May 2013).

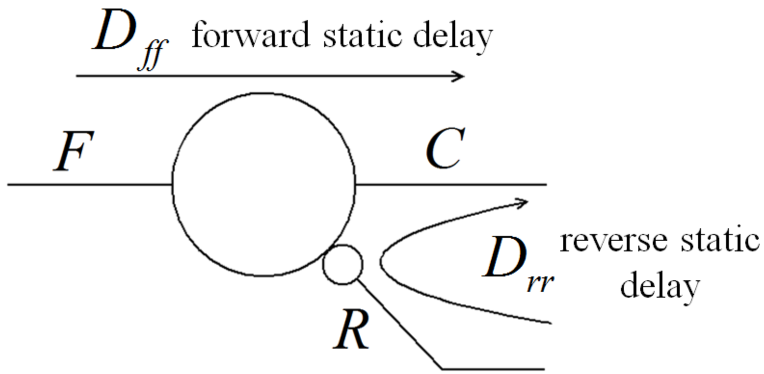
Contribution

- **A stochastic model for the STRNG**
  - A simple entropy assessment : a **lower bound for the entropy per output bit**
  - No empirical parameter, **only physical/measurable parameters**
- **A design strategy using the model and measurements**
- **Design in Altera Cyclone III and Xilinx Virtex 5 FPGAs, evaluation at 400 Mbit/s**

Outline

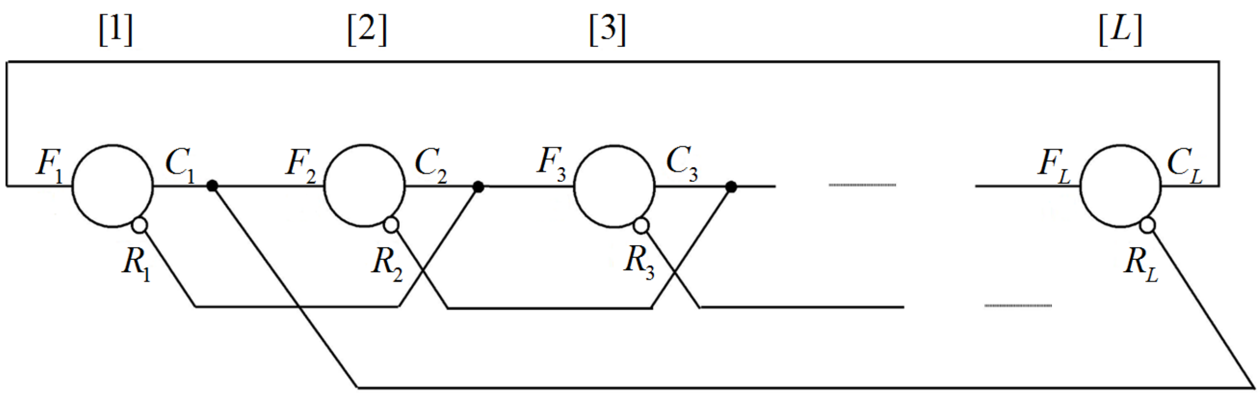
1. Self-timed ring oscillators : state of the art
2. STRNG architecture and principle
3. STRNG stochastic model
   - Lower bound of entropy per output bit
   - Practical use of the model
4. STRNG design and evaluation
5. Conclusion

STR Architecture



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

(a)



(b)

(a) Stage structure and truth table (b) Self-timed ring architecture

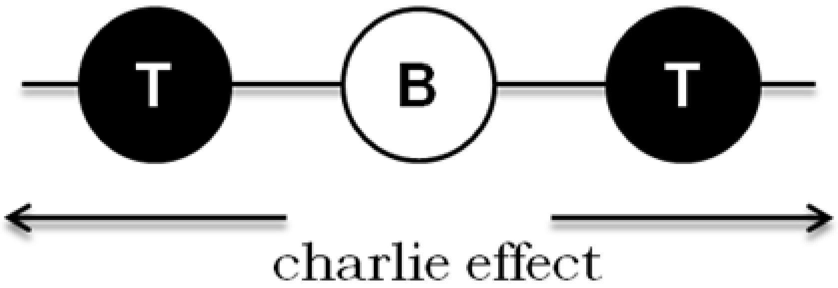
[4] I. E. Sutherland, "Micropipelines", in Communications of the ACM (Association of Computing Machinery), Vol/Issue:32/6, pages 720-738, 1989.

The Charlie effect

- **Propagation delay of a Muller gate depends on the relative arrival times of its two inputs**

Charlie Effect The closer are the input events, the longer is the stage propagation delay

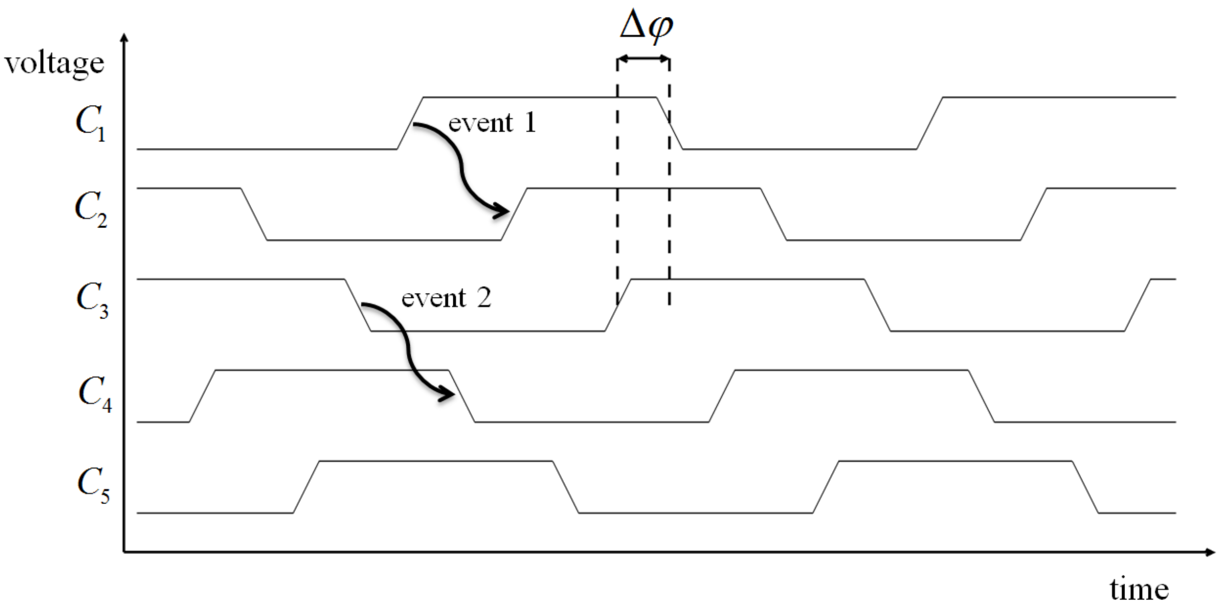
- **Evenly-spaced propagation locking mechanism**



Influence of the Charlie effect on the propagation of two events

Multiphase STR

- **Several events propagate evenly-spaced in time thanks to inherent analog mechanisms (Charlie effect)**



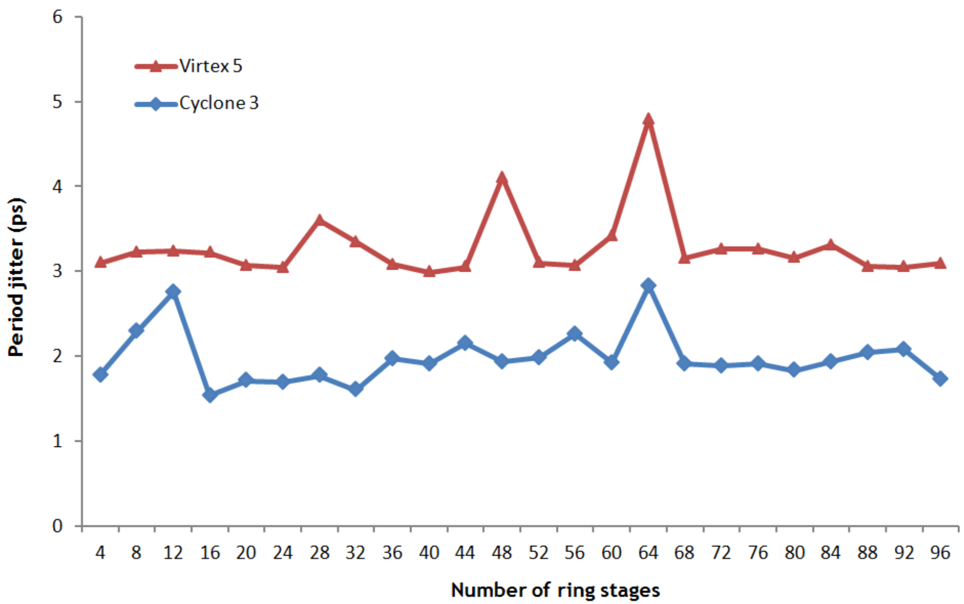
Evenly-spaced propagation of 2 events in a 5-stage STR

- **If the number of events N and the number of stages L are co-prime, the ring exhibits L different equi-distant phases with** $\Delta\varphi = \frac{T}{2L}$

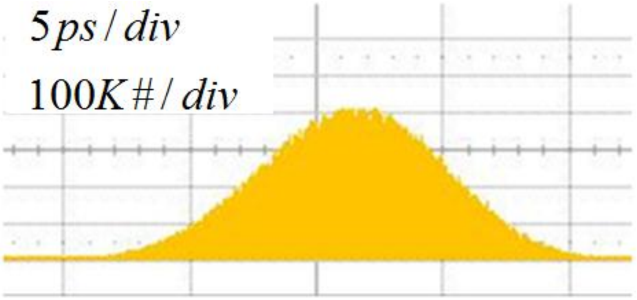
[5] S. FAIRBANKS, "High Precision Timing using Self-timed Circuits", Technical report no. UCAM-CL-TR-738, University of Cambridge, Computer Laboratory, January 2009, url: http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-738.pdf

Jitter in STR

- **Timings between successive events are auto-controlled**
  - **Jitter locally generated** in the ring stage barely propagates to other stages
  - **Deterministic variations are attenuated**



STR Period jitter with N=L/2 vs. the number of stages



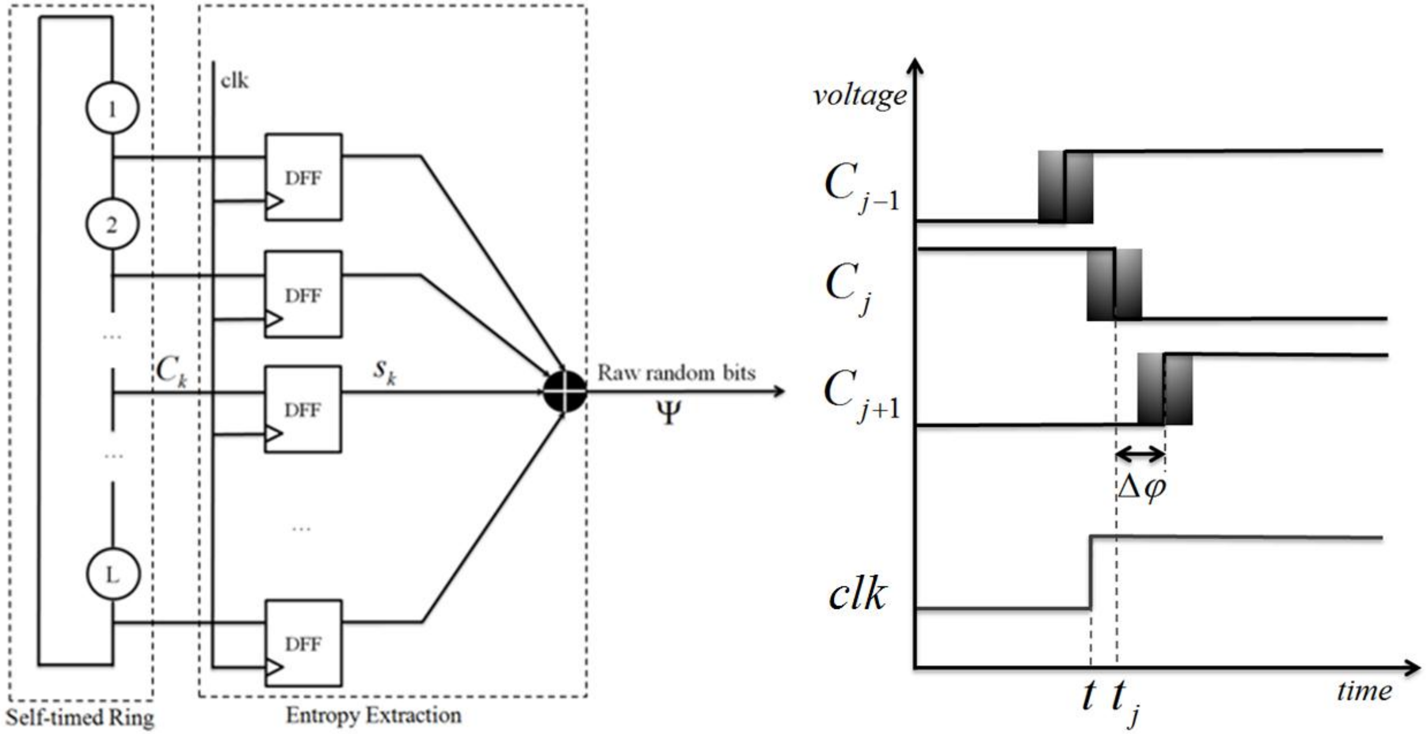
Period histogram of a 96-stage STR in Altera Cyclone III (N=48)

[2] 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.

Outline

1. Self-timed ring oscillators : state of the art
2. STRNG architecture and principle
3. STRNG stochastic model
   - Lower bound of entropy per output bit
   - Practical use of the model
4. STRNG design and evaluation
5. Conclusion

STRNG Architecture and Principle



STRNG core architecture and entropy extraction principle

- **STR: Multiphase, evenly-spaced signals**
- **Entropy extractor: Sample each signal with a reference clk, XOR tree**
- **STR phase resolution: ~ jitter interval around an output edge**

Outline

1. Self-timed ring oscillators : state of the art

2. STRNG architecture and principle

3. STRNG stochastic model
   – Lower bound of entropy per output bit
   – Practical use of the model

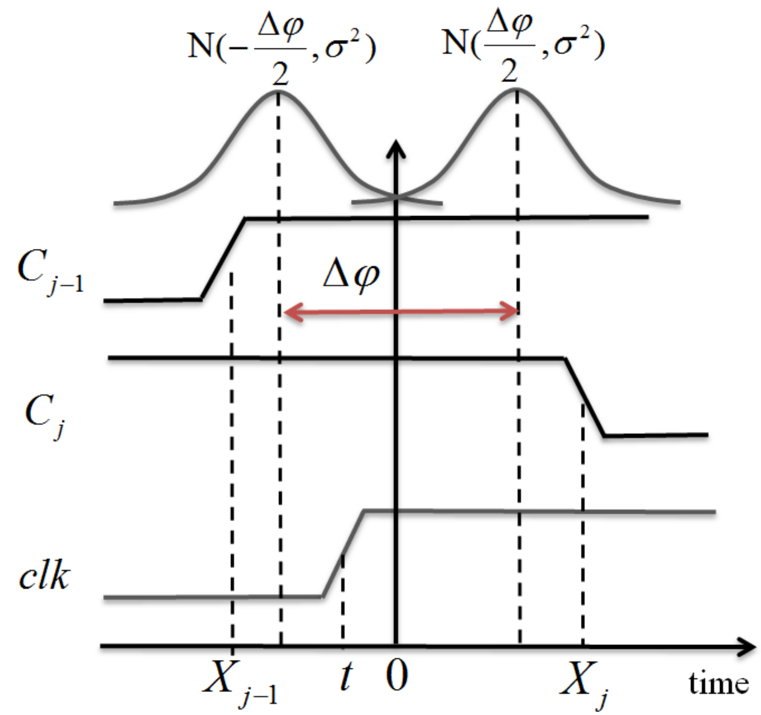
4. STRNG design and evaluation

5. Conclusion

Modeling of the Entropy Extraction (1)

- **STR output signals**
  - Mean time between 2 successive events -> **intrinsec locking mechanisms of the STR**
  - Effective event timing -> **jitter** and its **standard deviation**

$$X_{j-1} = N(-\frac{\Delta\varphi}{2}, \sigma^2) \quad , \quad X_j = N(\frac{\Delta\varphi}{2}, \sigma^2)$$



Detailed view of two successive events in the STR

- **Objective**
  - Compute the probability that the sampled bit is ‘1’ or ‘0’
  - Compute the entropy per output bit of the TRNG

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

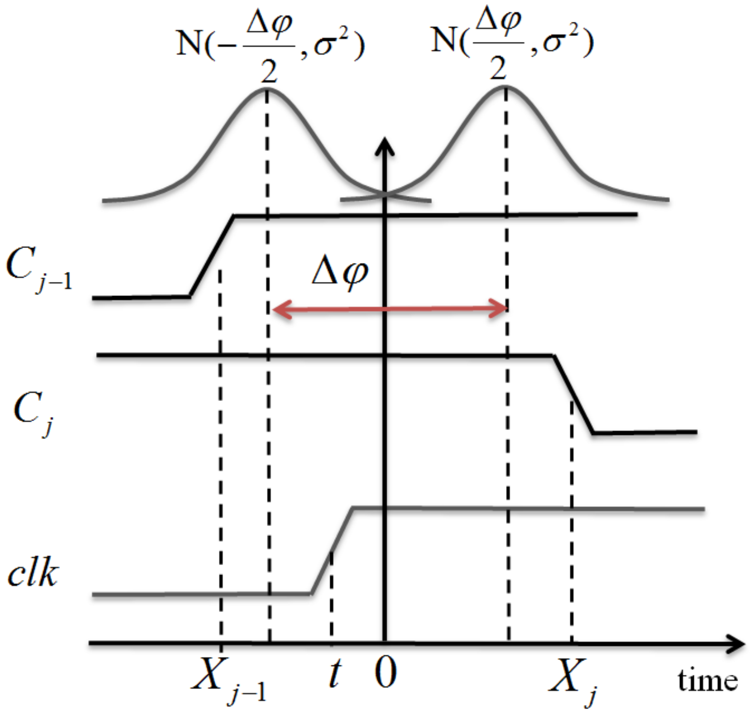
Modeling of the Entropy Extraction (2)

- **Probability to sample a value 'u' in the signal Ψ**

$X_{j-1} \leq t$	$X_j \leq t$	ω	ψ
false	false	'1'	$\bar{u}$
false	true	'0'	u
true	false	'0'	u
true	true	'1'	$\bar{u}$

$$\Rightarrow \quad P(u) = p + p' - 2pp'$$

with
$$\begin{cases} p = P(X_j \leq t) = \Phi\left(\frac{t - \Delta\varphi/2}{\sigma}\right) \\ p' = P(X_{j-1} \leq t) = \Phi\left(\frac{t + \Delta\varphi/2}{\sigma}\right) \\ \Phi(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{\frac{-t^2}{2}} dt \quad , x \in \mathrm{R} \end{cases}$$



Detailed view of two successive events in the STR

Results

- **Probability to sample a value 'u' in the signal Ψ**

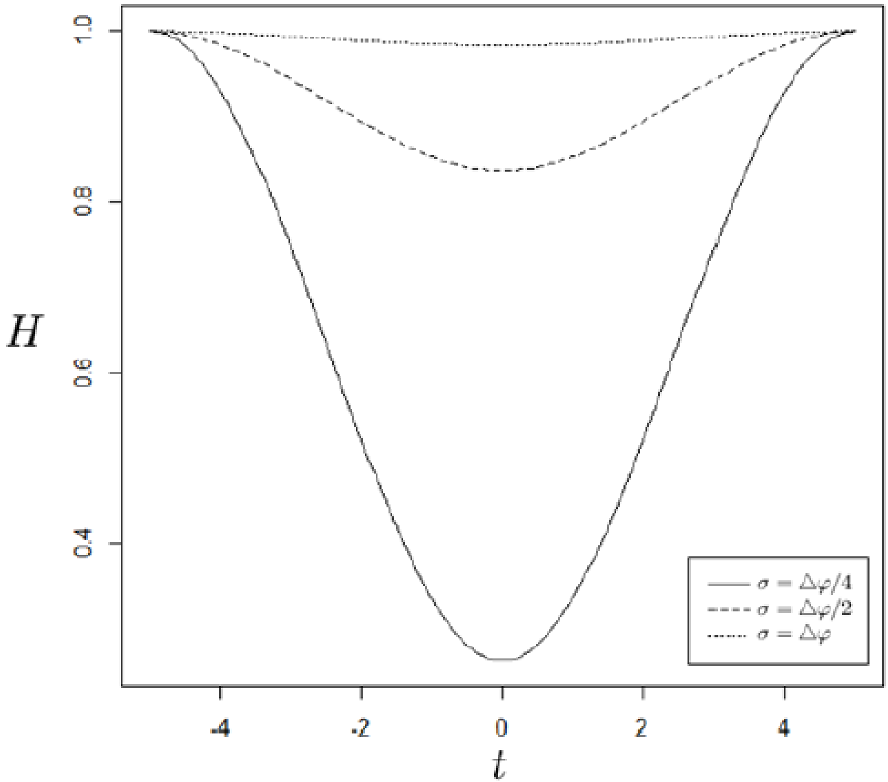
$$P(u) = \Phi(\frac{t - T/4L}{\sigma}) + \Phi(\frac{t + T/4L}{\sigma}) - 2\Phi(\frac{t - T/4L}{\sigma})\Phi(\frac{t + T/4L}{\sigma})$$

- **Entropy is minimum when t=0**

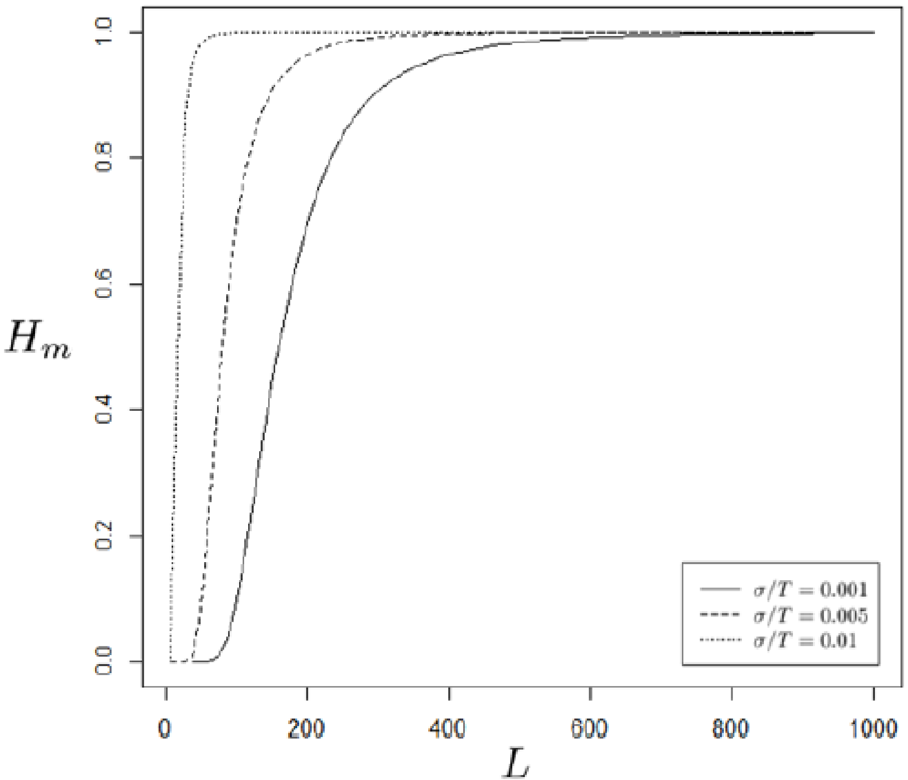
$$H_m = -P(u)_{t=0}\log_2(P(u)_{t=0}) - (1 - P(u)_{t=0})\log_2(1 - P(u)_{t=0})$$

$$\textit{with} \quad P(u)_{t=0} = 1 - 2\Phi(\frac{T}{4L\sigma}) - 2(\Phi(\frac{T}{4L\sigma}))^2$$

Entropy in Time and Lower Entropy Bound



Entropy as a function of time



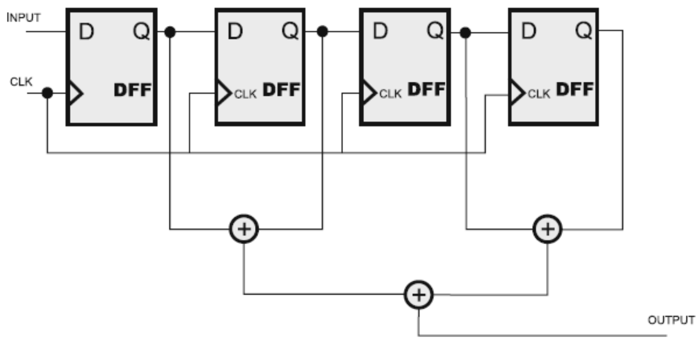
Lower entropy bound as a function of the number of STR stages

➡ **Lower entropy bound increases with the number of ring stages**

Arithmetic Post-processing

- **Data compression with a parity filter**
  - **Increased entropy** per output bit, but **at reduced bit rate**

$$P(u)_{output} = 0.5 - 2^{n-1}(P(u)_{input} - 0.5)^n$$



Architecture of a 4th order parity filter

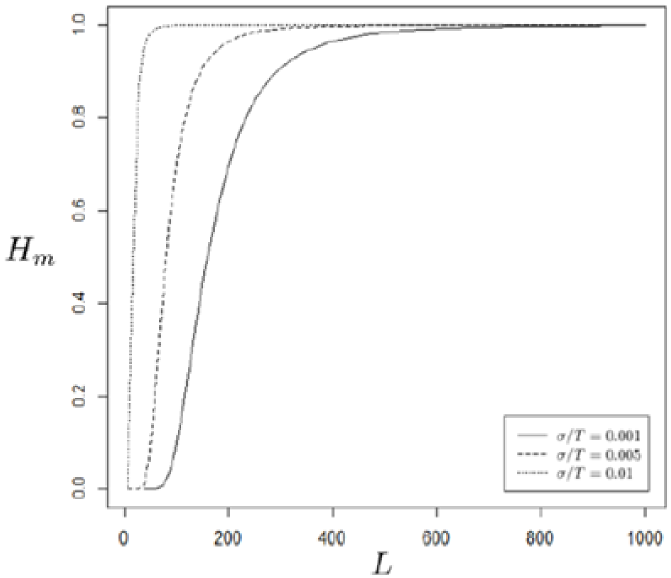
- **Tune the area/bit rate trade-off for the STRNG**

[6] R. B. Davies, « Exclusive OR (XOR) and hardware random number generators » (2002). url: http://www.robertnz.net/pdf/xor2.pdf

Practical Use of the Model

- Measure the STR **oscillation period** and **jitter magnitude**

- Plot the **lower entropy bound curve** as function of the number of stages



Lower entropy bound as a function of the number of STR stages

- Select the **number of STR stages L** so that Hm>0.99

- <u>OR:</u> Select L depending on size/area requirements then **compute n the filter order** to achieve Hm>0.99

Outline

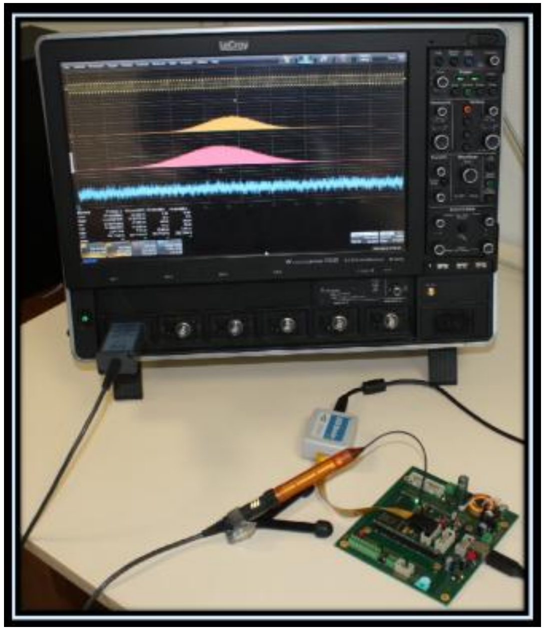
1. Self-timed ring oscillators : state of the art
2. STRNG architecture and principle
3. STRNG stochastic model
   - Lower bound of entropy per output bit
   - Practical use of the model
4. STRNG design and evaluation
5. Conclusion

STRNG Implementation

- One **4-input LUT** (Look-up-table) **per stage**
  - 2 inputs for the signals *F* and *R*, 1 feedback for the memory state and 1 initialization input (*SET* or *RESET*)
- Take care of stage structures and placement to **avoid bottlenecks**
- **Hard-wired connexions** between stages and adjacent flip-flops
- **Sampling clock:** external 16 MHz quartz + PLL for multiplication
- **Data transfer:** LVDS (Low Voltage Differential Signaling) transfer to acquisition card, acquisition at **400 Mbit/s**
- **Generic software parity filter** for evaluation purposes

Measurement of the Entropy Source

- **Experimental setup**
  - Wideband digital oscilloscope (3.5 GHz bandwidth and 40 Gsample/s) + Lecroy statistical tools
  - **Differential oscilloscope probes**
  - **Low Voltage Differential Signaling** (LVDS) FPGA outputs



- **STR jitter measurement**
  - Measure the **minimum jitter** that can be present in the device
  - Jitter magnitude around one signal edge is estimated by ([3])

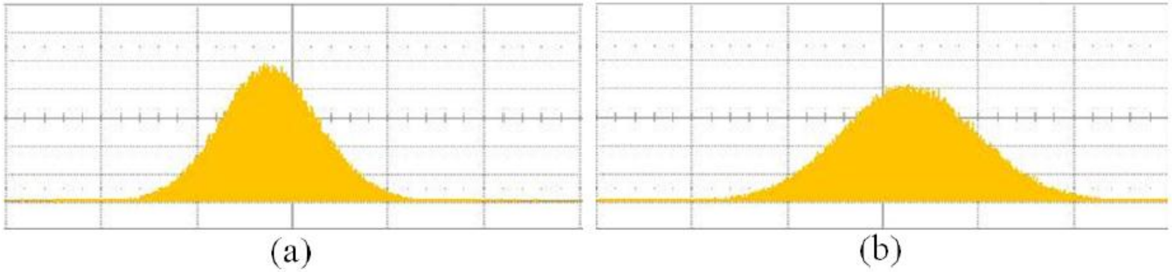
$$\sigma \approx \frac{\sigma_{period}}{\sqrt{2}}$$

- **Phase resolution measurement**
  - Mean phase resolution is computed using the following equation

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

Measurement Results

- **All tested configurations showed a Gaussian jitter profile**



Period distribution histogram of a 127-stage STR with 64 tokens
(a) Altera Cyclone III (b) Xilinx Virtex 5 (scales are 5 ps per horizontal division and 100 kilo sample per vertical division)

Device	STR		Measurements	
	L	N	T	$\Delta\varphi$
Cyclone III	63	32	2.44 ns	19.3 ps
	127	64	3.11 ns	12.2 ps
	255	128	2.93 ns	5.7 ps
	511	256	3.31 ns	3.2 ps
Virtex 5	63	32	2.82 ns	21.4 ps
	127	64	2.83 ns	11.8 ps
	255	128	2.45 ns	5.5 ps
	511	256	2.87 ns	2.9 ps

Jitter and phase resolution measurement

- **Jitter magnitude**

$$\sigma_{Cyclone} \approx 2ps$$

$$\sigma_{Virtex} \approx 2.5ps$$

Evaluation : AIS31 Test Suite

Device	STR		Raw data		Model		Compressed data	
	L	$\Delta\varphi$	T1-T4	T5-T8	H_m	n_{min}	$n_{p_{min}}$	Throughput
Cyclone III ($\sigma_{Cyclone} \approx 2ps$)	63	19.3 ps	0%	0/4	0	-	7	57 Mbit/s
	127	12.2 ps	0%	0/4	0.02	483	4	100 Mbit/s
	255	5.7 ps	45%	1/4	0.58	7	2	200 Mbit/s
	511	3.2 ps	99%	3/4	0.91	2	2	200 Mbit/s
Virtex 5 ($\sigma_{Virtex} \approx 2.5ps$)	63	21.4 ps	0 %	0/4	0	-	8	50 Mbit/s
	127	11.8 ps	10 %	1/4	0.13	60	3	133 Mbit/s
	255	5.5 ps	58%	2/4	0.78	4	2	200 Mbit/s
	511	2.9 ps	61%	3/4	0.97	2	2	200 Mbit/s

Statistical evaluation results for the STRNG at 400 Mbit/s

- T1-T4 : FIPS 140-1 passing rates (1000 sequences of 20.000 bits)
- T5-T8 : passing tests out of 4 (~ 1 Mbyte of data)
- H_m : lower entropy per bit bound
- $n_{\min}$: minimal filter order to achieve 0.99 (**model**)
- $n_{p_{\min}}$: filter order used in **practice** to pass T1-T8 tests
- Throughput : effective bit rate after compression

Evaluation : NIST Test Suite

- NIST SP 800-22 test suite on 1000 sequences of 1.000.000 bits with a 0.01 confidence level

- STRNG with **L=511 and compression rate of 3 passes all NIST tests** in **Altera Cyclone III**
  - Effective throughput = **133 Mbit/s**

- STRNG with **L=511 and compression rate of** 4 **passes all NIST tests** in **Xilinx Virtex 5**
  - Effective throughput = **100 Mbit/s**

---

[7] "A statistical test suite for random and pseudo-random number generators for cryptographic applications". NIST special publication (SP) 800-22 rev. 1 (2008). url: http://csrc.nist.gov/CryptoToolKit/tkrng.html

Outline

1. Self-timed ring oscillators : state of the art
2. STRNG architecture and principle
3. STRNG stochastic model
   – Lower bound of entropy per output bit
   – Practical use of the model
4. STRNG design and evaluation
5. Conclusion

Conclusion

- Self-timed ring based TRNG
  - Extracts randomness from the jitter of a STR, **regardless the jitter magnitude**
  - The design is flexible: **area, bit rate and security level can be tuned** with a very low design effort
  - Passes AIS31 and NIST tests at high bit rates (**a few hundred Mbit/s**)

- A stochastic model for the STRNG
  - A simple yet useful entropy assessment for the generator
  - Links the **security level** with the **physical parameters** of the generator
  - Uses **only measurable parameters**
  - Approach validated in Altera and Xilinx FPGAs

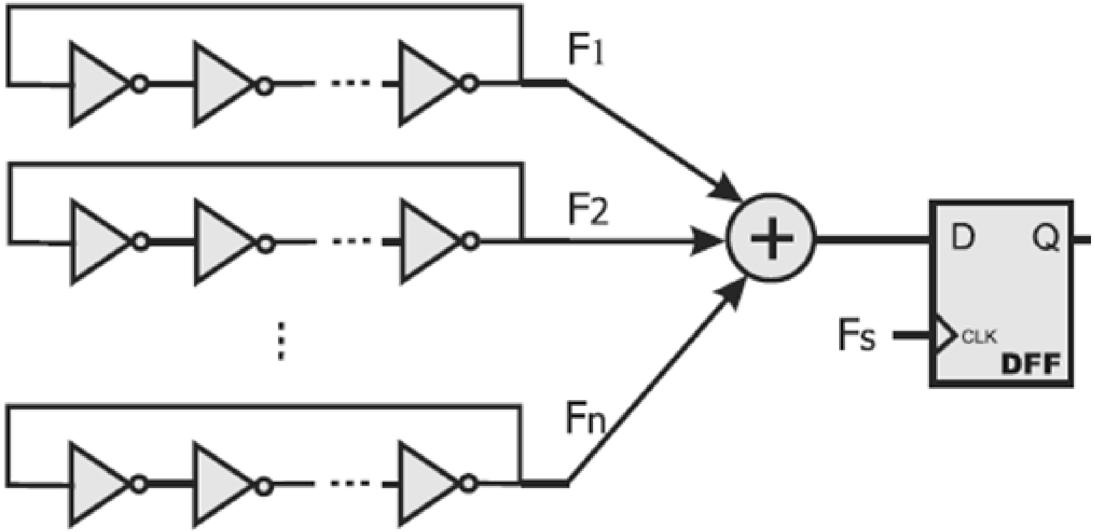
Conclusion (Not in the Paper)

- **1 Patent**
- **2 circuits** (ST CMOS 28 nm and AMS CMOS .35 µm)
- **Future works**
  - **Alarms, specific embedded tests** (counting the number of events …)
  - Embedded measurement of the entropy source
  - **Robustness evaluation** (voltage variations, EM attacks …)

Thank you

Appendix

Inverter Ring Oscillator based TRNG



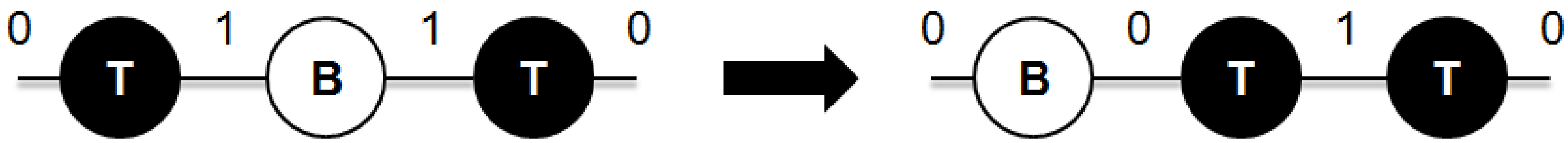
IRO-based TRNG architecture [8]

- **Known issues**
  - Number of needed ROs **grows exponentially** with the decreasing size of the jitter
  - **True randomness** vs. Pseudo randomness -> predictability
- **Critical security issue**
  - **Dependence between the rings** (locking)

[8] 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).

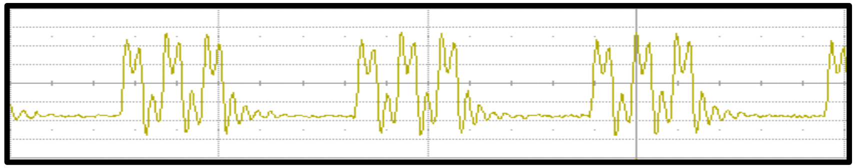
STR Behavior

- **Bubbles and tokens abstraction**

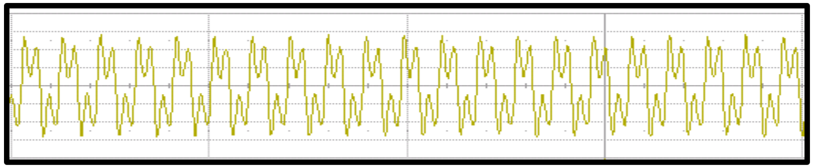


Token propagation in a self-timed ring

- **Two oscillation modes**



Burst

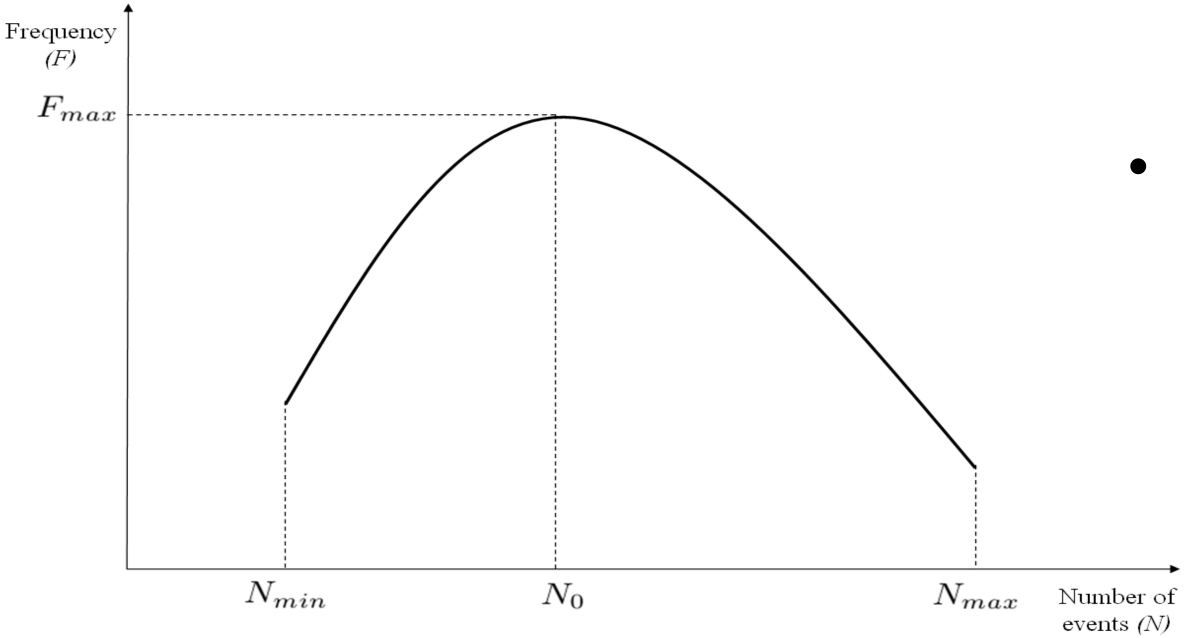


Evenly-spaced

- Final state of STR for a fixed design depends on the **ring occupancy**
  - **Set at the ring initialization**

Frequency Behavior

- STR final state depends on
  - **Charlie** and **drafting effect magnitude**
  - **Forward** and **reverse propagation delay ratio** (Dff/Drr)
  - **Occupancy or ratio between number of events** and **number of stages** (N/L)



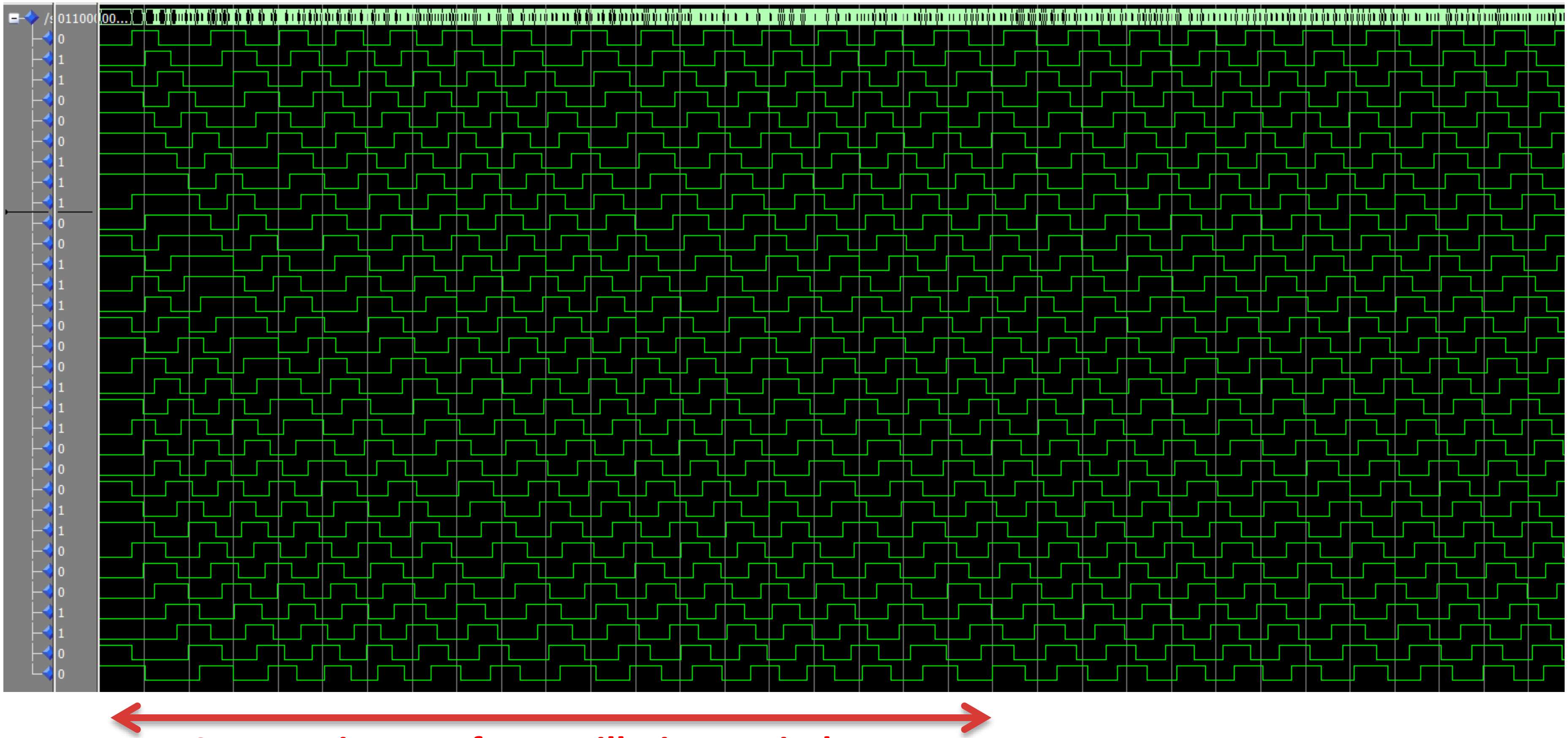
STR Frequency as a function of its occupancy

- Maximum frequency achieved for

$$\frac{N_0}{L - N_0} \approx \frac{D_{ff}}{D_{rr}}$$

STR startup

- A few events re-arrange themselves as they start propagating in the ring



Startup time = a few oscillation periods

Controlled timings in STR

- Simulation with ~ 500 ps propagation delays
- Librairies include Charlie and drafting effects
- A 1000 ps variation is introduced
- It progressively disappears as the events propagate in the ring