- JOURNEES SCIENTIFIQUES SEMBA 2011 -

SELF-TIMED RINGS AS ENTROPY SOURCES IN FPGA

Abdelkarim CHERKAOUI (LaHC)
Viktor FISCHER (LaHC)
Alain AUBERT (LaHC)
Laurent FESQUET (TIMA)

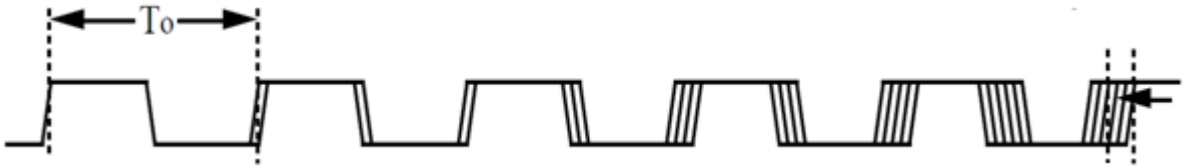
LaHC / TIMA lab
Rhônes-Alpes Region PhD Fund
SEMBA PROJECT – ISLE Cluster

October 2011

Université Jean Monnet– St-Etienne FRANCE

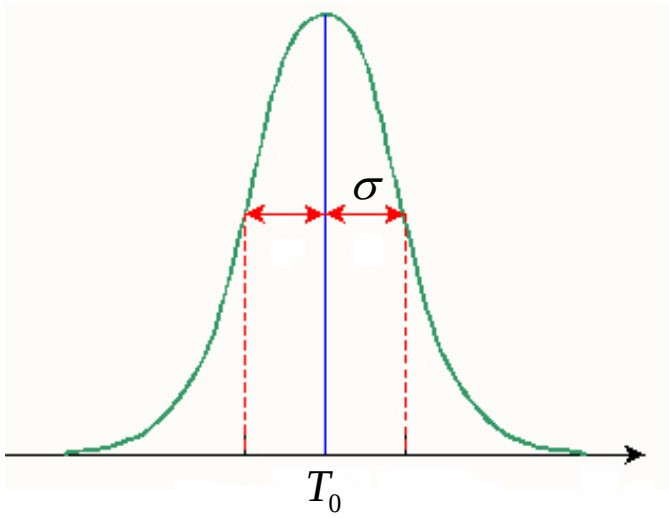
Introduction

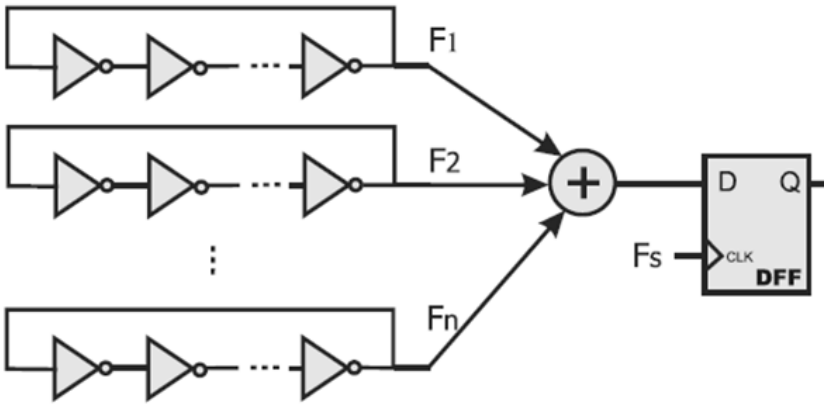
- **True Random Numbers Generator (TRNG)**
  - Generate random binary sequences
  - One of the basic cryptographic primitives
- **Jitter in Ring Oscillators**



Due to noise, period deviates from its ideal value

$$T = \mathrm{N}(T_0, \sigma^2)$$





- **RO-based TRNG Principle**

Sample a jittery clock to generate randomness

Objective

- Performances and security of True Random Number Generators (TRNG) depend on the quality of the entropy source

- Inverter Ring Oscillators (IRO) are the most widely used solution as entropy source in FPGAs
  - Easy to implement
  - High random jitter magnitude
  - **But:** low robustness to voltage and manufacturing process variabily

Improving RO robustness ➡ **Improving TRNG robustness**

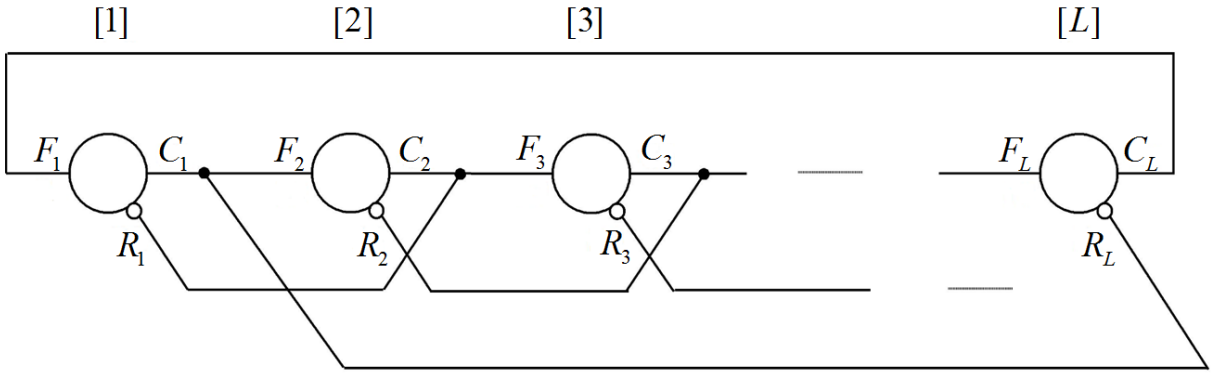
- Self-Timed rings (STR) have been studied on ASIC targets (these studies show an improved robustness to process variability) but haven't been characterized yet as entropy sources

Outline

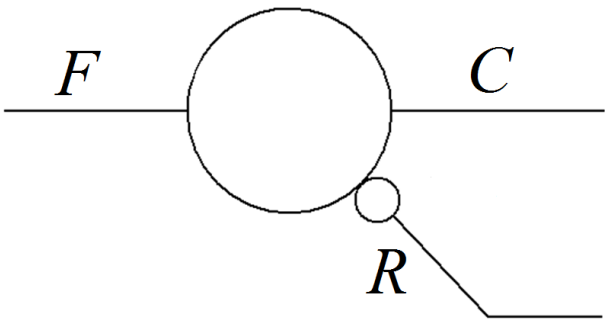
- **STR Architecture and Behavior**
- **Jitter in IRO and STR**
- **Experimental Results**
  - Sensitivity to Voltage And Process Variability
  - Jitter measurements
- **Conclusion**

STR Architecture

- Ring structure



- Basic stage cell : C-Element (Muller gate) + Inverter



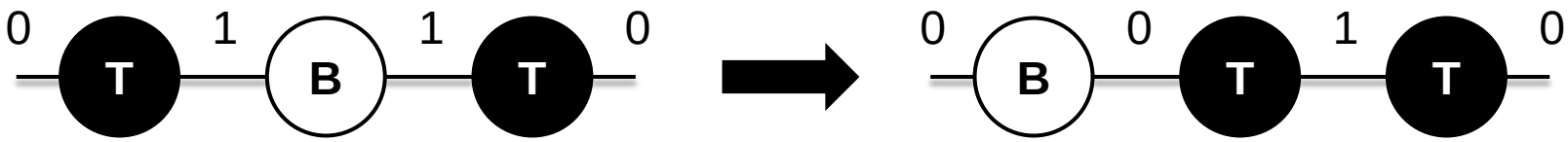
F	R	C
0	0	C^{-1}
0	1	0
1	0	1
1	1	C^{-1}

A Bubbles and Tokens Story

- Data representation

Bubble	Output's stage is equal to its input
Token	Output's stage is different from its input

- Propagation Rule
  - A token propagates from left to right to the next stage if it contains a bubble
  - A bubble propagates from right to left to the previous stage if it contains a token

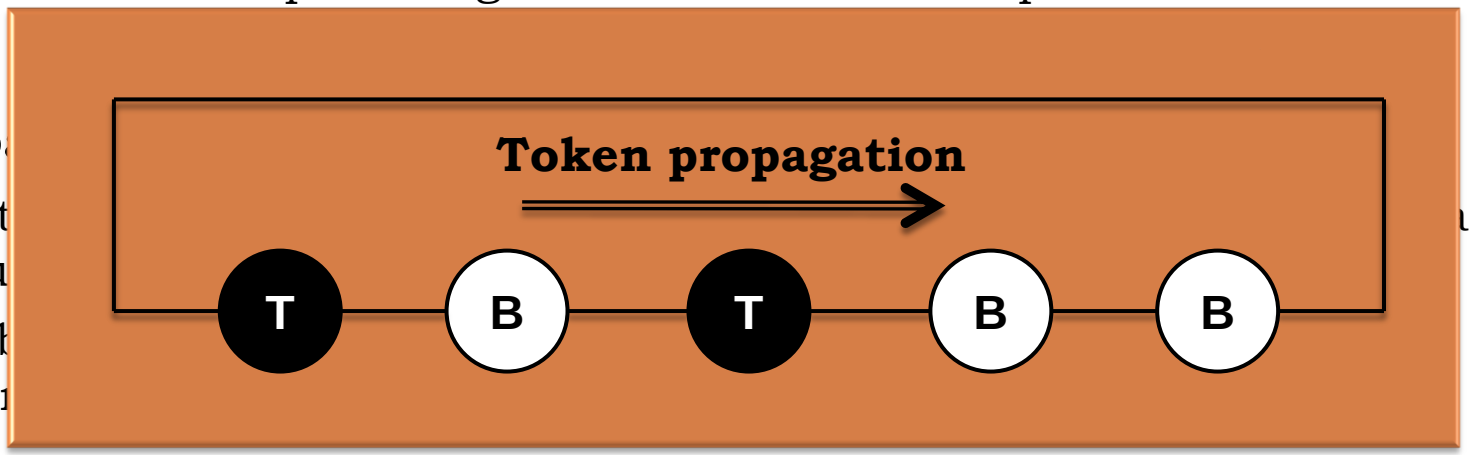


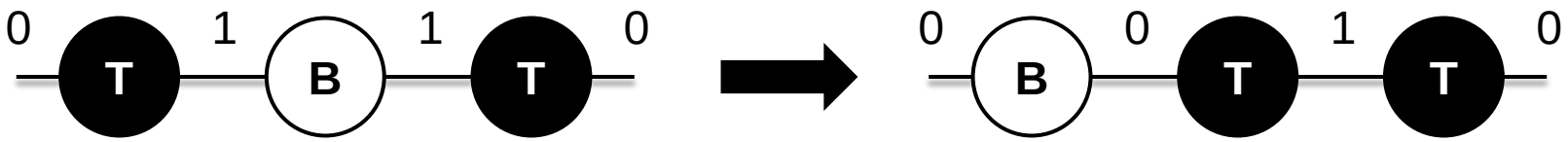
A Bubbles and Tokens Story

- Data representation

Bubble	Output's stage is equal to its input
Token	Output's stage is different from its input

- Prop
  - A t
    bu
  - A
    co



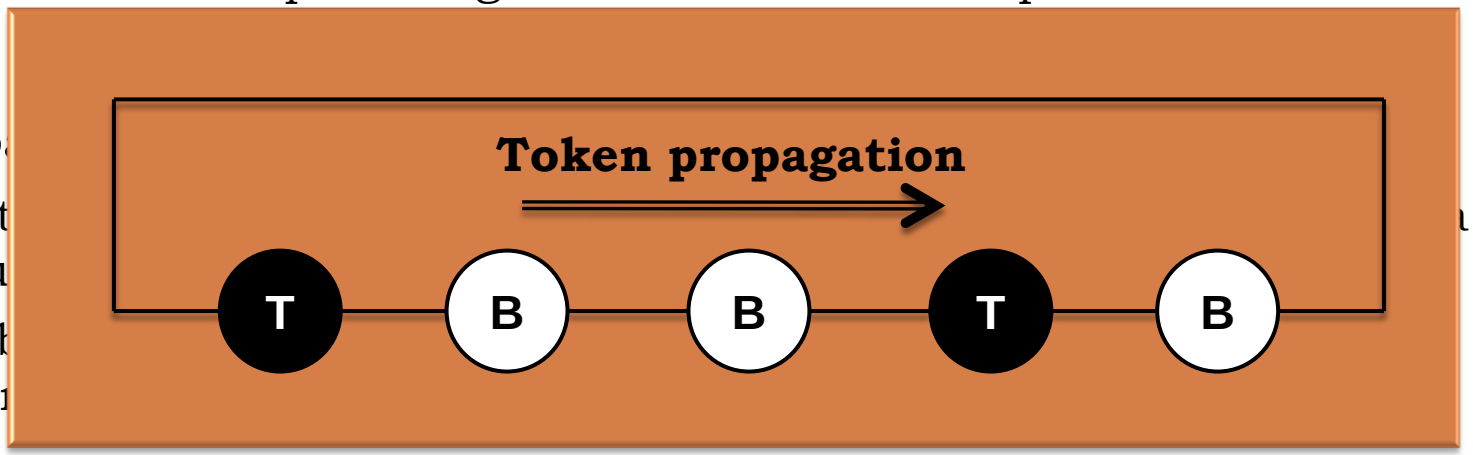


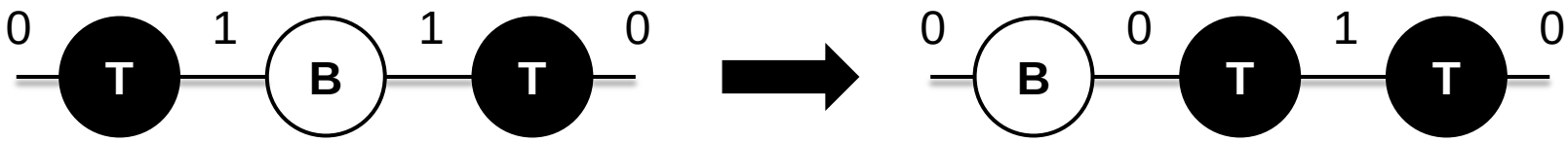
A Bubbles and Tokens Story

- Data representation

Bubble	Output's stage is equal to its input
Token	Output's stage is different from its input

- Prop
  - A t
    bu
  - A
    co





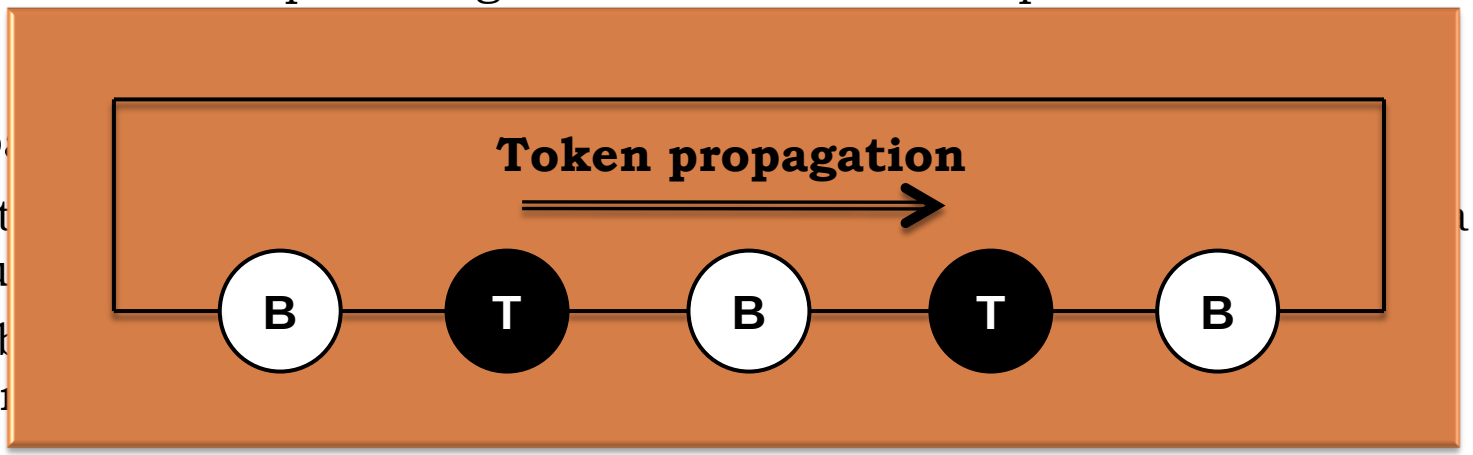
A Bubbles and Tokens Story

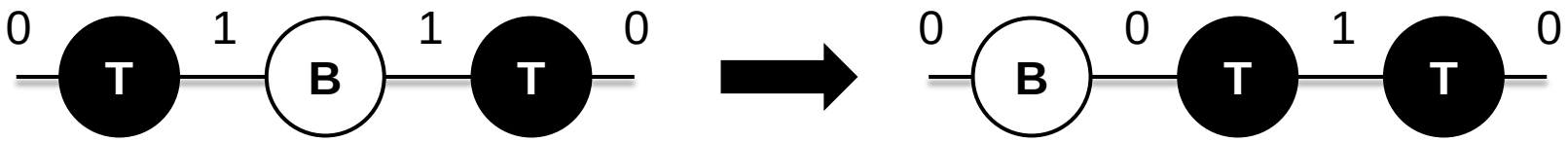
- Data representation

  Bubble Output's stage is equal to its input

  Token Output's stage is different from its input

- Prop
  - A t
    bu
  - A t
    co



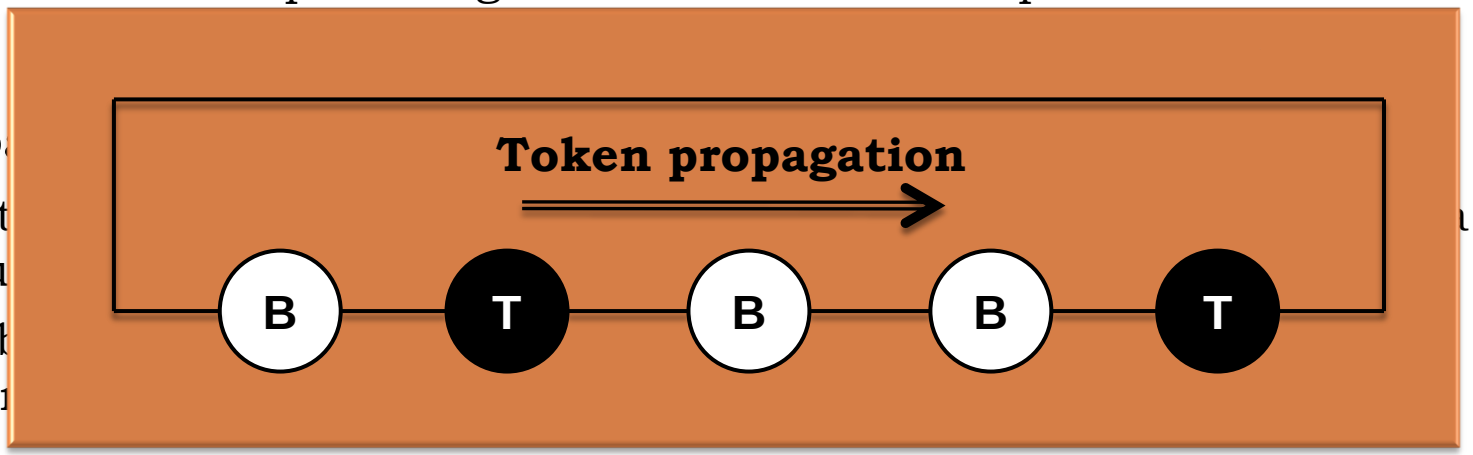


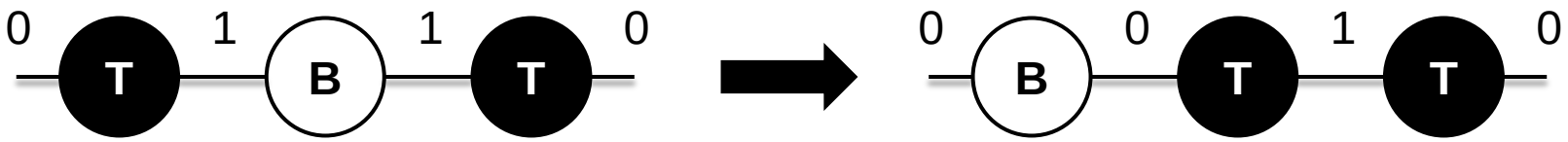
A Bubbles and Tokens Story

- Data representation

Bubble	Output's stage is equal to its input
Token	Output's stage is different from its input

- Prop
  - A t
    bu
  - A
    co



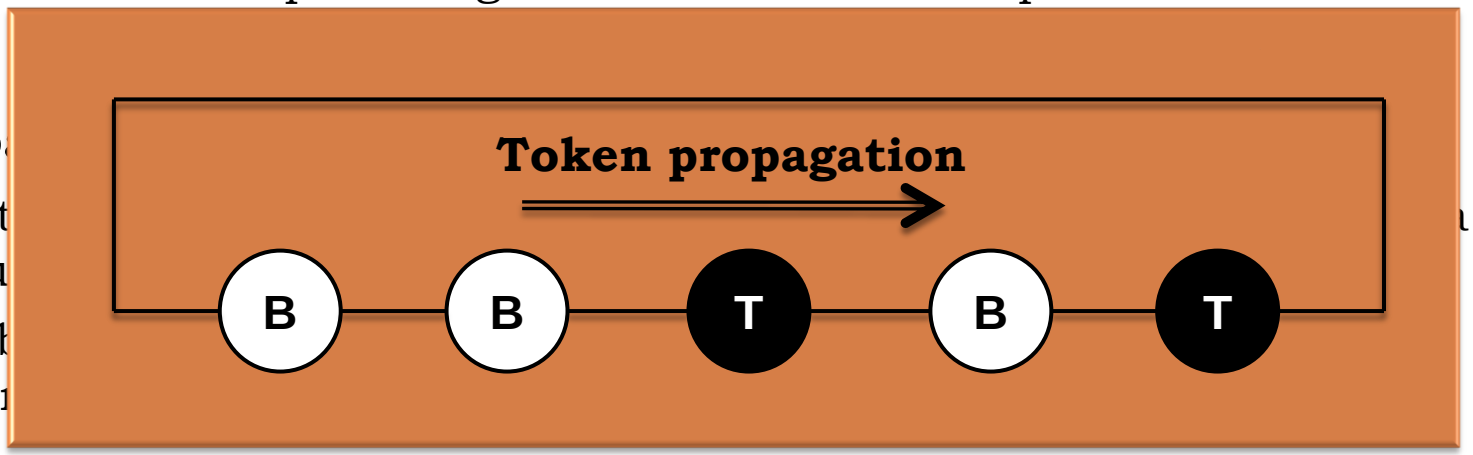


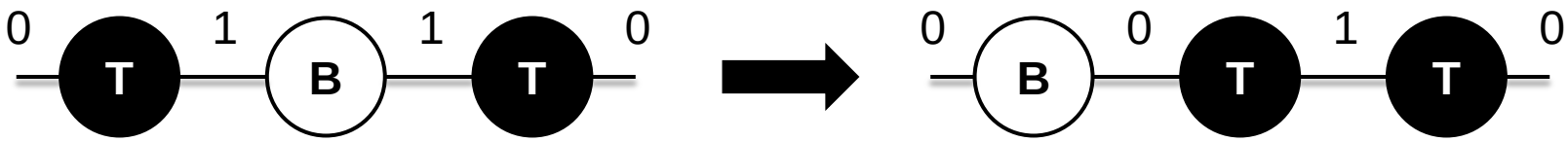
A Bubbles and Tokens Story

- Data representation

Bubble	Output's stage is equal to its input
Token	Output's stage is different from its input

- Prop
  - A t
    bu
  - A
    co



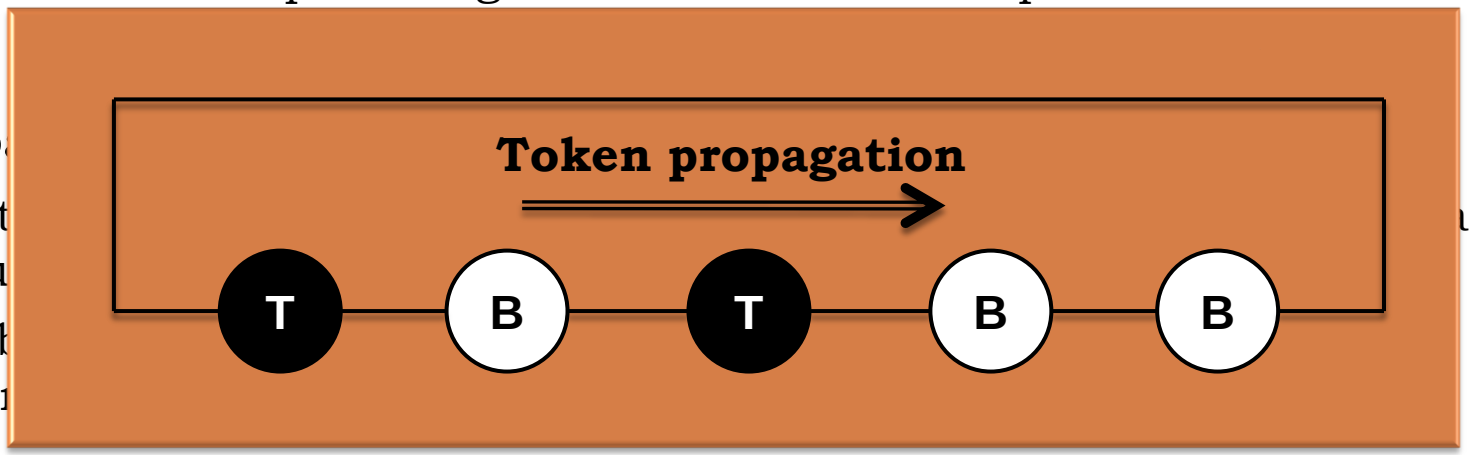


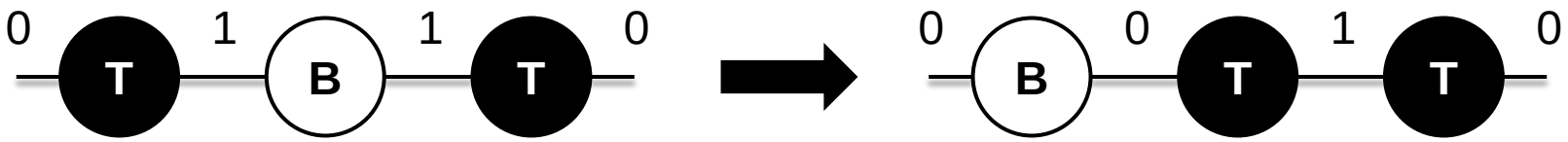
A Bubbles and Tokens Story

- Data representation

Bubble	Output's stage is equal to its input
Token	Output's stage is different from its input

- Prop
  - A t
    bu
  - A
    co



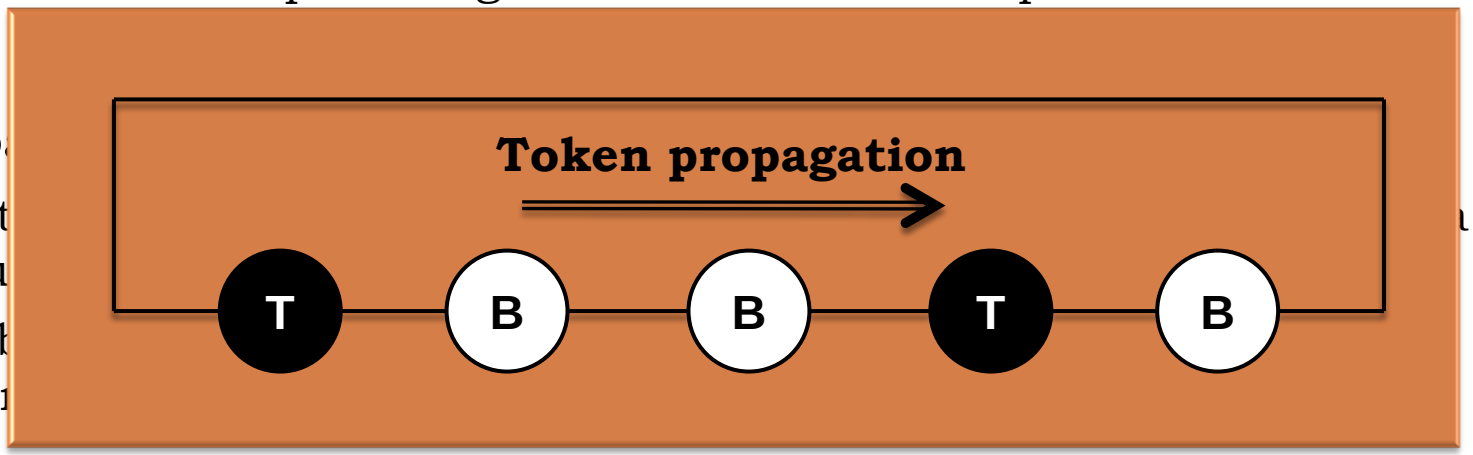


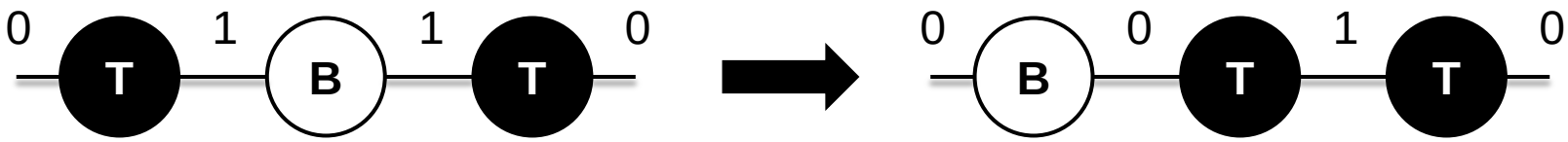
A Bubbles and Tokens Story

- Data representation

Bubble	Output's stage is equal to its input
Token	Output's stage is different from its input

- Prop
  - A t
    bu
  - A
    co





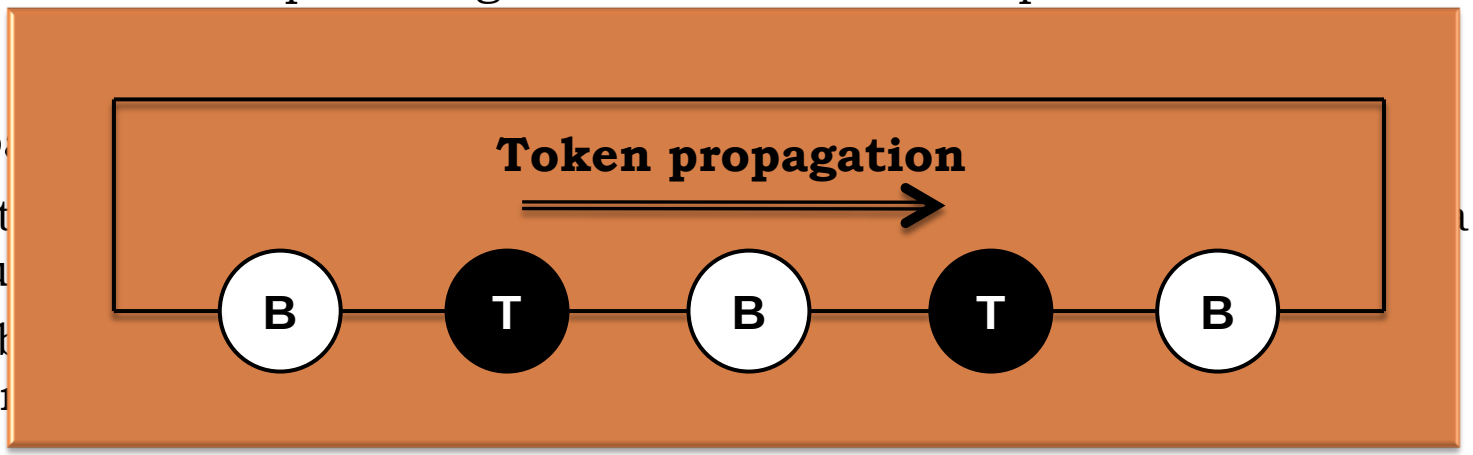
A Bubbles and Tokens Story

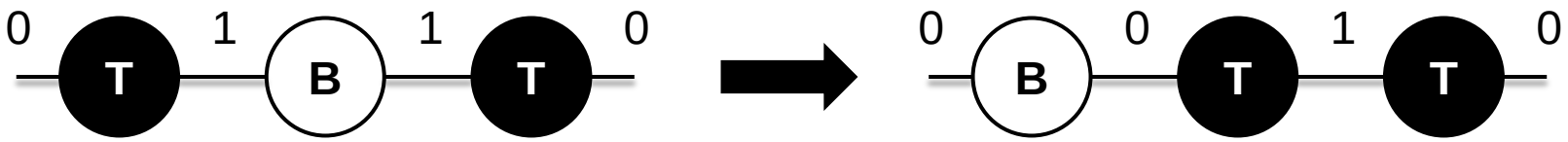
- Data representation

  Bubble Output's stage is equal to its input

  Token Output's stage is different from its input

- Prop
  - A t
    bu
  - A t
    co



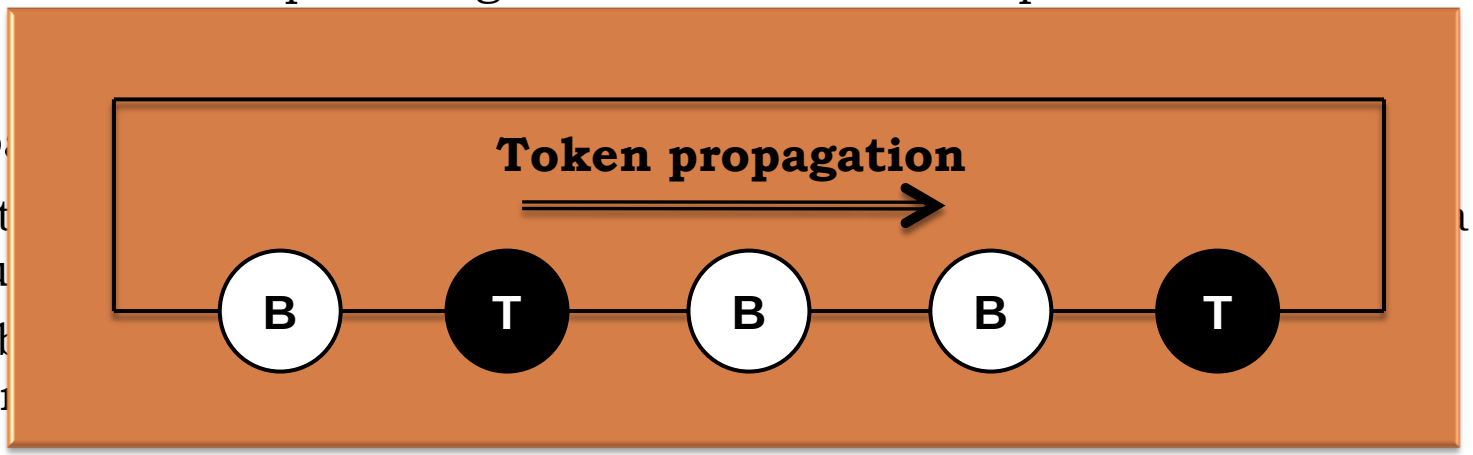


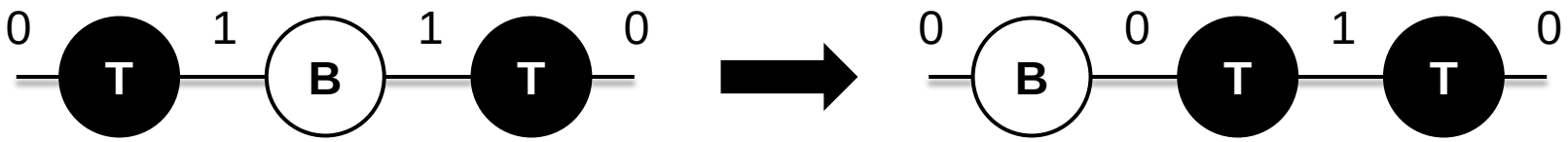
A Bubbles and Tokens Story

- Data representation

Bubble	Output's stage is equal to its input
Token	Output's stage is different from its input

- Prop
  - A t
    bu
  - A
    co



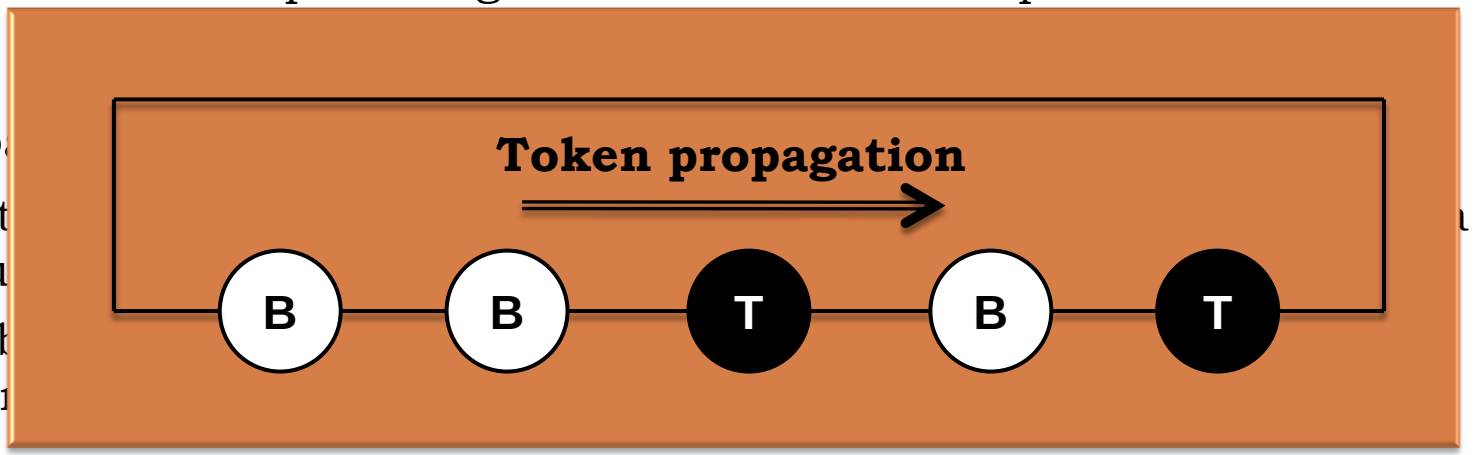


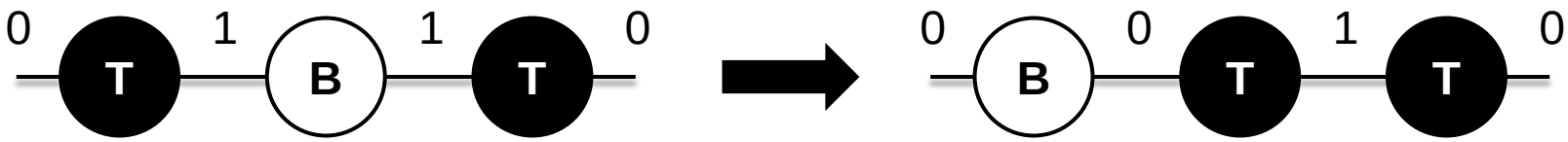
A Bubbles and Tokens Story

- Data representation

Bubble	Output's stage is equal to its input
Token	Output's stage is different from its input

- Prop
  - A t
    bu
  - A
    co



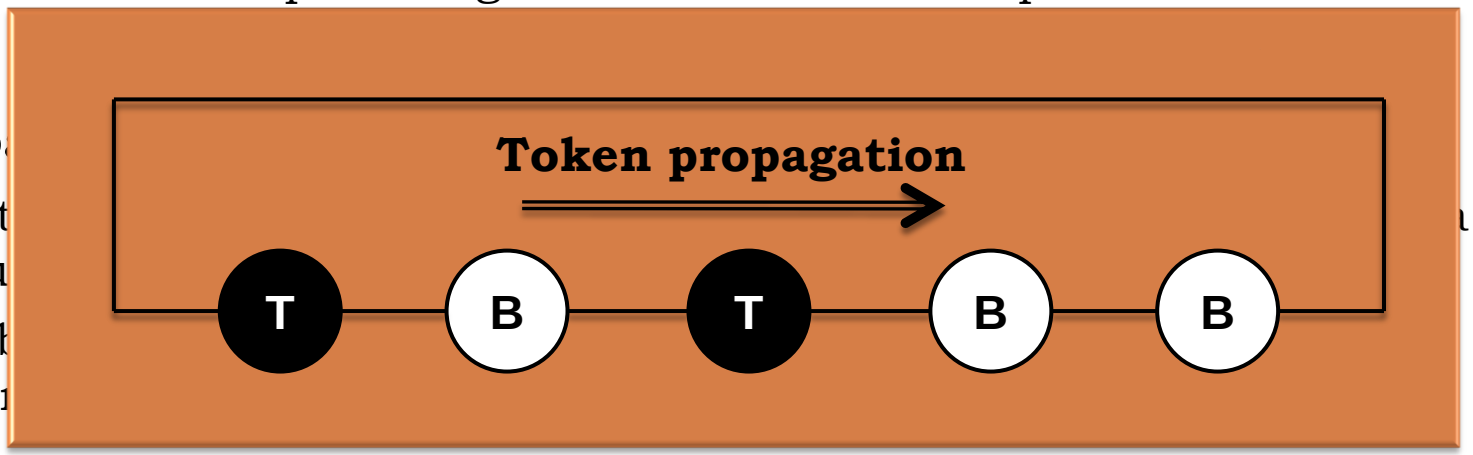


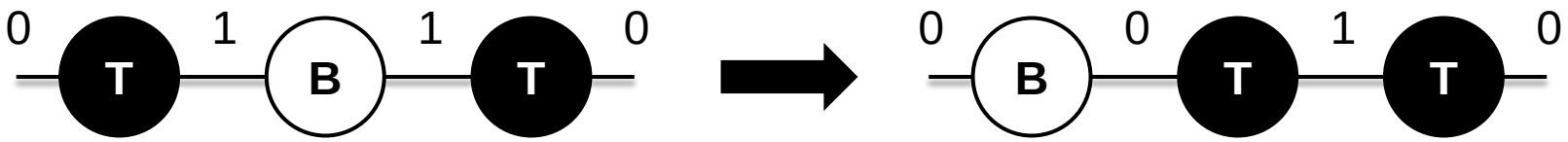
A Bubbles and Tokens Story

- Data representation

Bubble	Output's stage is equal to its input
Token	Output's stage is different from its input

- Prop
  - A t
    bu
  - A
    co



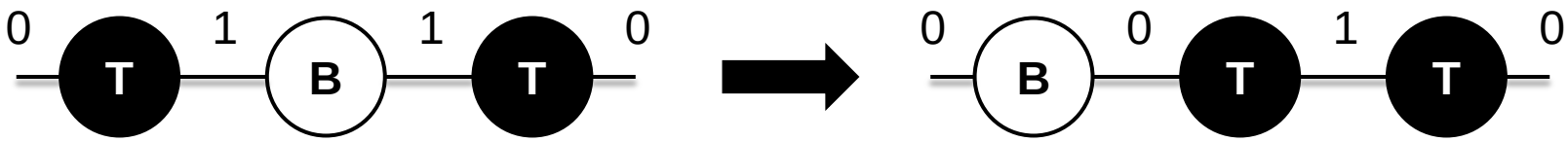


A Bubbles and Tokens Story

- Data representation

Bubble	Output's stage is equal to its input
Token	Output's stage is different from its input

- Propagation Rule
  - A token propagates from left to right to the next stage if it contains a bubble
  - A bubble propagates from right to left to the previous stage if it contains a token



Steady Regime

- Steady Regime shows 2 oscillation modes

Evenly-spaced	Tokens evenly spread all around the ring and propagate with a constant spacing
Burst	Tokens get together to form a cluster that propagates around the ring

- Example : 32-stage ring

- What causes tokens to evenly-spread around the ring independently from the initialization state and the propagation delays disparities ?

- Is it possible to predict the oscillation mode ? How ?

Steady Regime

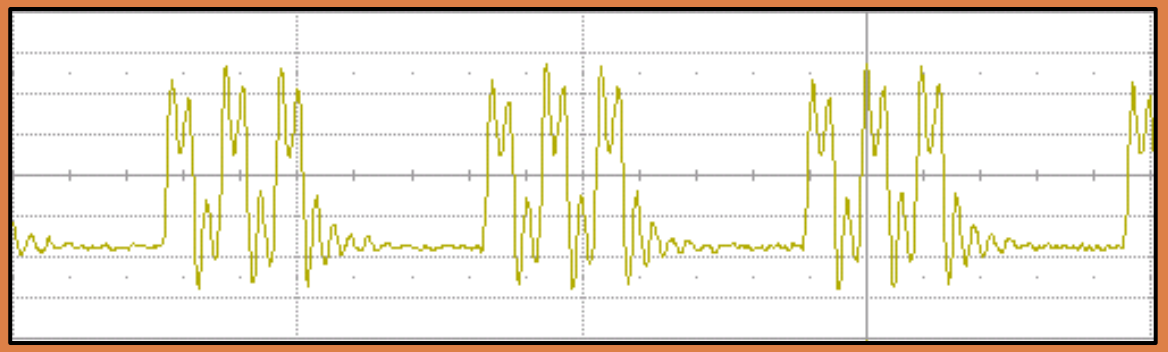
- Steady Regi
  Evenly-space

  Burst

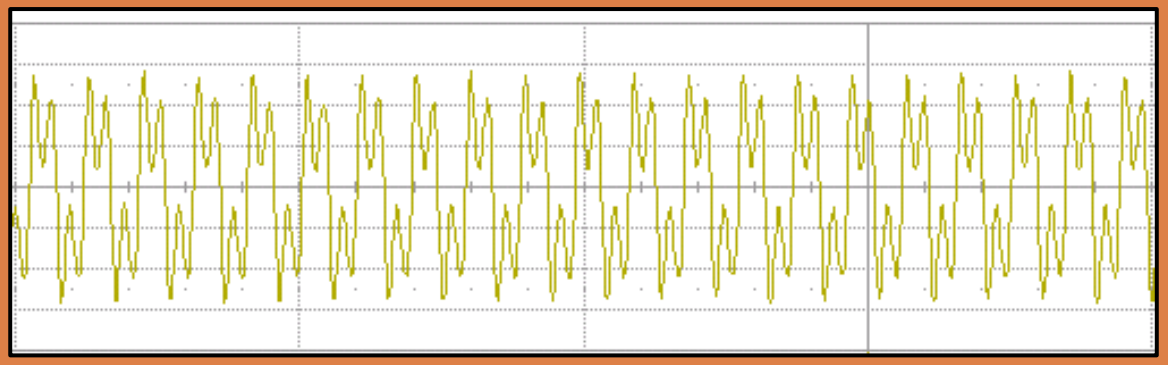
- Example : 32

- What cause
  from the ini

- Is it possible



(a) 6 tokens in burst Mode



(b) 14 tokens in evenly-spaced Mode

Steady Regime

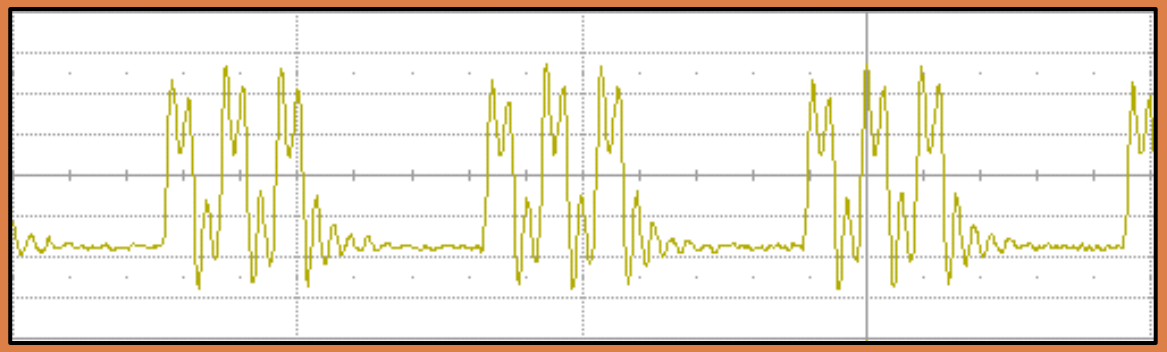
- Steady Regi
  Evenly-space

  Burst

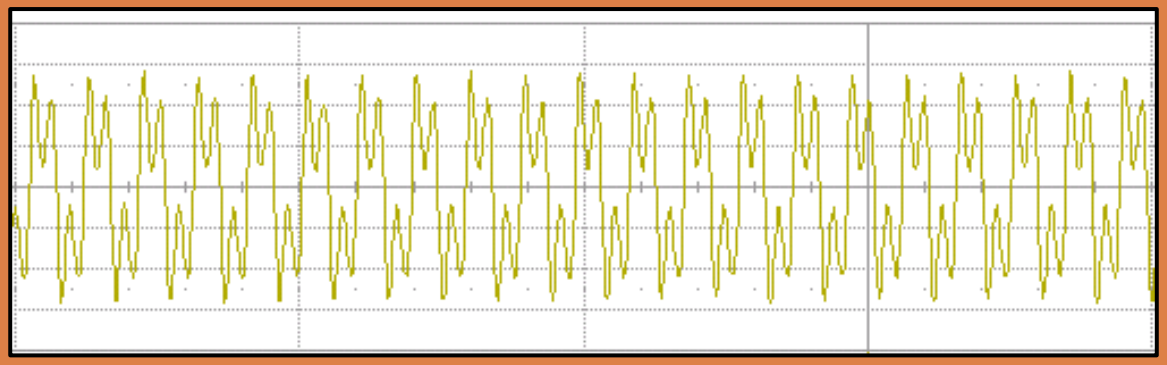
- Example : 32

- What cause
  from the ini

- Is it possible



(a) 6 tokens in burst Mode



(b) 14 tokens in evenly-spaced Mode

Evenly-spaced mode is observed for number of tokens going from 10 to 22

Steady Regime

- Steady Regime shows 2 oscillation modes

Evenly-spaced	Tokens evenly spread all around the ring and propagate with a constant spacing
Burst	Tokens get together to form a cluster that propagates around the ring

- Example : 32-stage ring

- What causes tokens to evenly-spread around the ring independently from the initialization state and the propagation delays disparities ?

- Is it possible to predict the oscillation mode ? How ?

The Charlie Effect

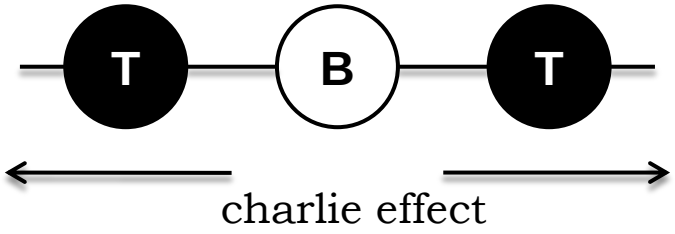
- Propagation delay of a Rendez-Vous element depends on the relative arrival times of the inputs

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

- **Evenly-spaced mode locking phenomenon**

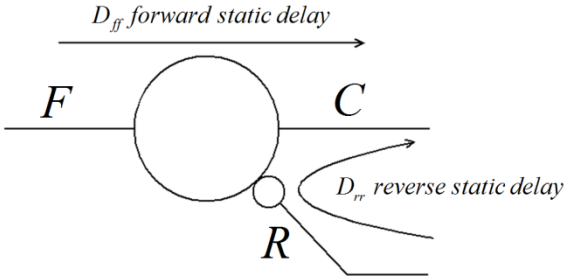
two tokens evolving closely push away from each other due to the Charlie effect

… until each token applies the same effect to its neighbours



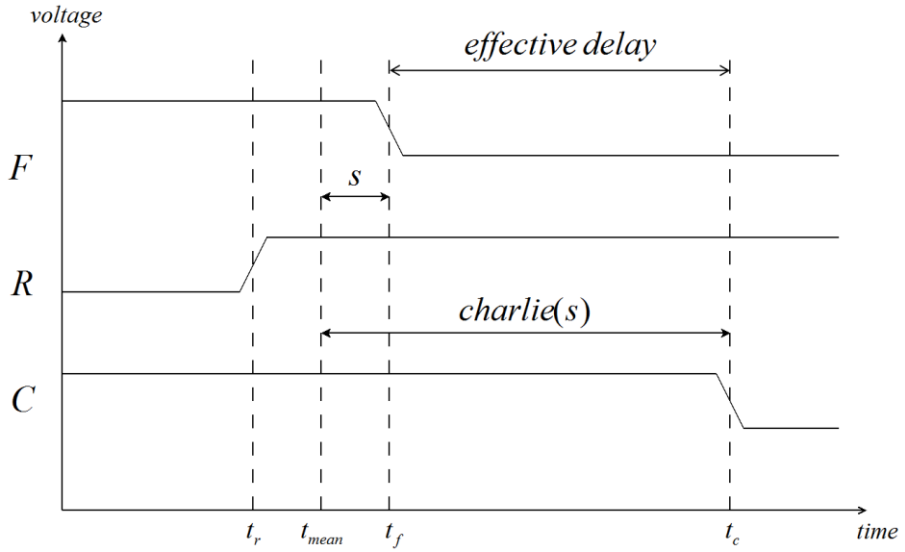
- Sufficient condition to guarantee the evenly-spaced mode

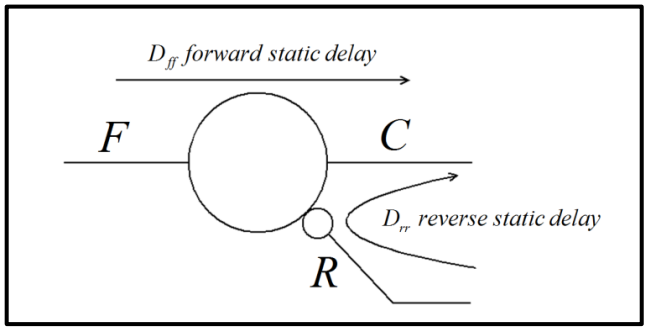
$$\frac{D_{ff}}{D_{rr}} = \frac{N_T}{N_B}$$

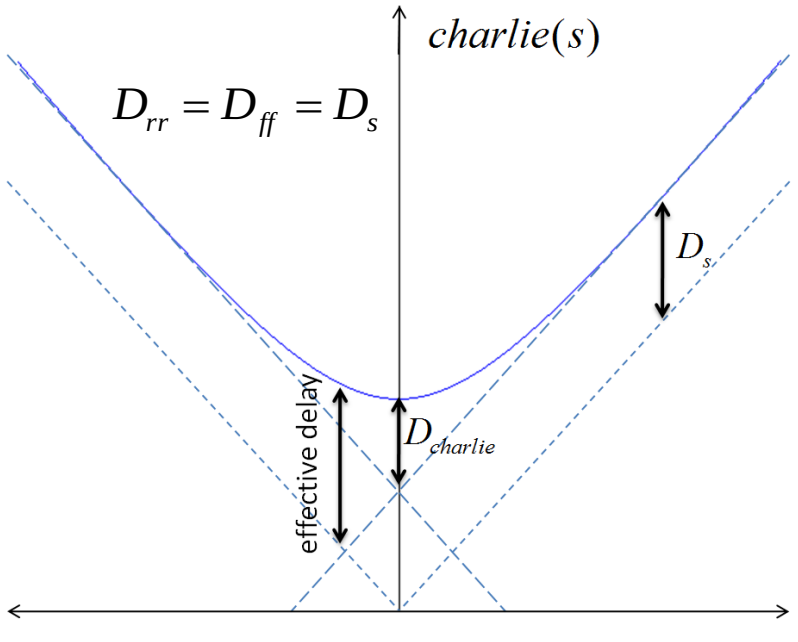


The Charlie Diagram

- The Charlie effect is modelized with Charlie diagrams







- The analytical Charlie expression

$$charlie(s) = D_s + \sqrt{D_{charlie}^{\ 2} + s^2}$$

STR in FPGA targets

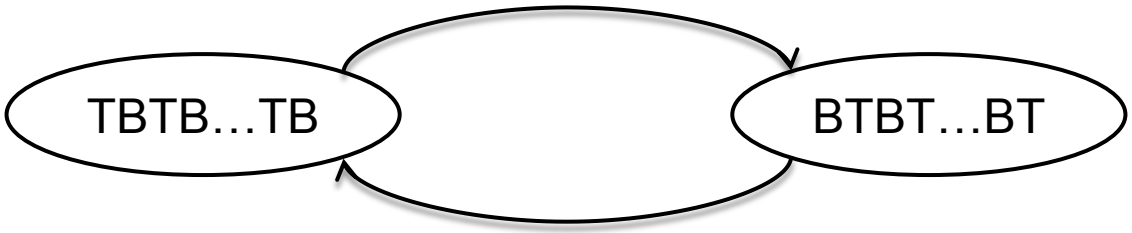
- Ring stage implementation
  - One stage (Muller gate + inverter) per LUT (Look-Up-Table)
  - Stages are placed manually to reduce interconnection delays

$$D_{rr} = D_{ff}$$

- Consequences
  - The evenly spaced mode is set by initializing the ring with as many tokens as bubbles

$$N_T = N_B$$

  - Ideally separation times are null and the Charlie effect is maximal, frequency is independent from the ring length



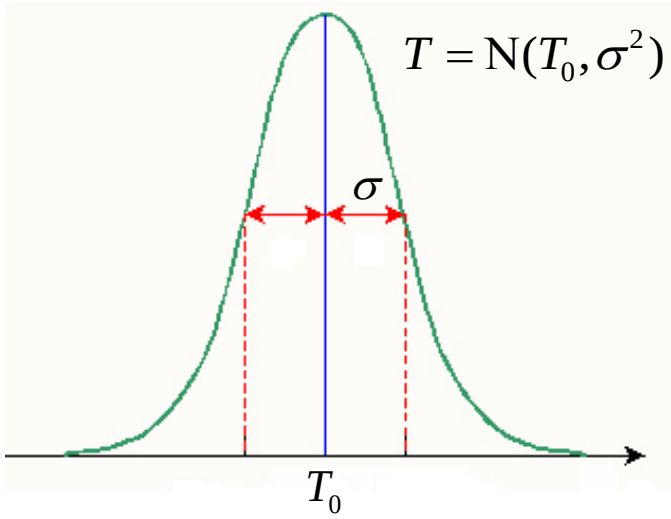
$$T_{osc} = 4(D_s + D_{charlie})$$

Jitter in Ring Oscillators

- Two types of jitter must be considered in TRNGs

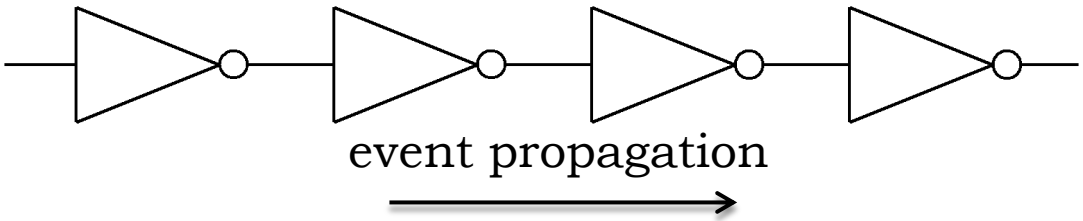
Local Gaussian Jitter	unpredictable, source of randomness
Global Deterministic Jitter	due to external global influences (for example a modulation of the power supply), can be used to attack TRNGs

- **Period jitter**
  - deviation in time of the oscillation period T from its ideal value
  - the standard deviation σ of a population of T values is used to measure the period jitter



Jitter in IRO

- Local Gaussian jitter
  - Period is defined by the propagation of one event around the ring during two laps
  - The event accumulates jitter each time it crosses a ring stage



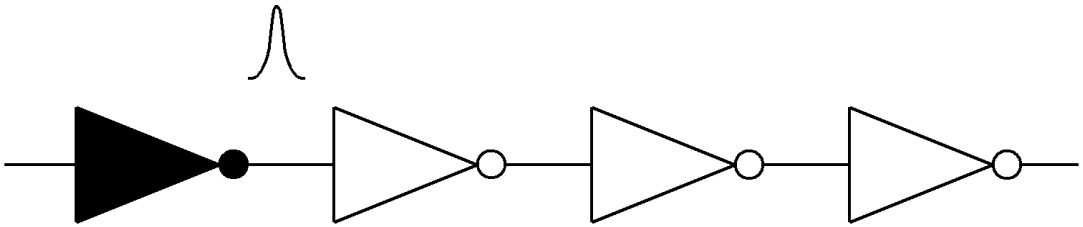
$$\sigma_{period} = \sqrt{2k}\sigma_g$$

- Global deterministic jitter
  - Accumulates linearly in the structure

$$D_{\det} = \sum_{i=1}^{2k} D_{\det_i}$$

Jitter in IRO

- Local Gaussian jitter
  - Period is defined by the propagation of one event around the ring during two laps
  - The event accumulates jitter each time it crosses a ring stage



event propagation

$$\sigma_{period} = \sqrt{2k}\,\sigma_g$$

standard-deviation related to the propagation time of one single gate (jitter of one single gate)

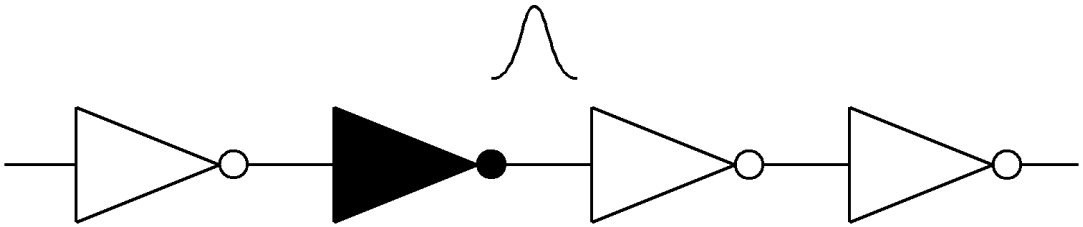
number of stages

- Global deterministic jitter
  - Accumulates linearly in the structure

$$D_{\det} = \sum_{i=1}^{2k} D_{\det_i}$$

Jitter in IRO

- Local Gaussian jitter
  - Period is defined by the propagation of one event around the ring during two laps
  - The event accumulates jitter each time it crosses a ring stage



event propagation

$$\sigma_{period} = \sqrt{2k}\sigma_g$$

standard-deviation related to the propagation time of one single gate (jitter of one single gate)

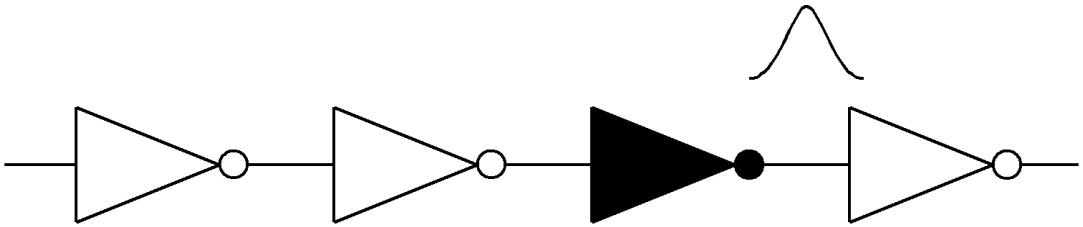
number of stages

- Global deterministic jitter
  - Accumulates linearly in the structure

$$D_{\det} = \sum_{i=1}^{2k} D_{\det_i}$$

Jitter in IRO

- Local Gaussian jitter
  - Period is defined by the propagation of one event around the ring during two laps
  - The event accumulates jitter each time it crosses a ring stage



event propagation

$$\sigma_{period} = \sqrt{2k}\sigma_g$$

standard-deviation related to the propagation time of one single gate (jitter of one single gate)

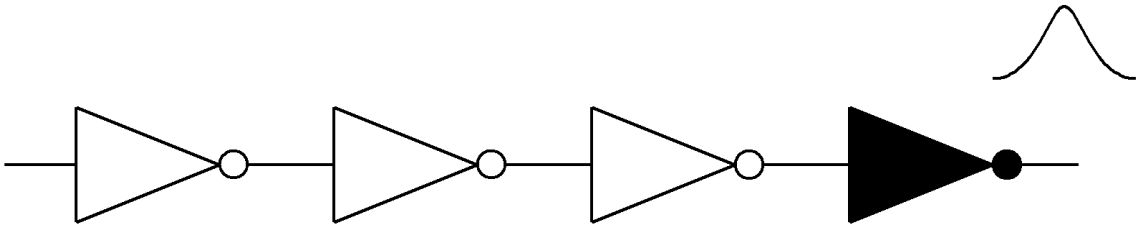
number of stages

- Global deterministic jitter
  - Accumulates linearly in the structure

$$D_{\det} = \sum_{i=1}^{2k} D_{\det_i}$$

Jitter in IRO

- Local Gaussian jitter
  - Period is defined by the propagation of one event around the ring during two laps
  - The event accumulates jitter each time it crosses a ring stage



event propagation

$$\sigma_{period} = \sqrt{2k}\sigma_g$$

standard-deviation related to the propagation time of one single gate (jitter of one single gate)

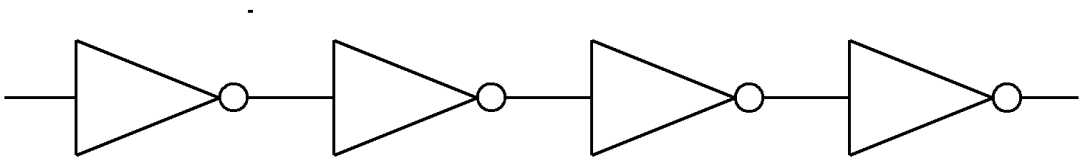
number of stages

- Global deterministic jitter
  - Accumulates linearly in the structure

$$D_{\det} = \sum_{i=1}^{2k} D_{\det_i}$$

Jitter in IRO

- Local Gaussian jitter
  - Period is defined by the propagation of one event around the ring during two laps
  - The event accumulates jitter each time it crosses a ring stage



event propagation

$$\sigma_{period} = \sqrt{2k}\,\sigma_g$$

standard-deviation related to the propagation time of one single gate (jitter of one single gate)

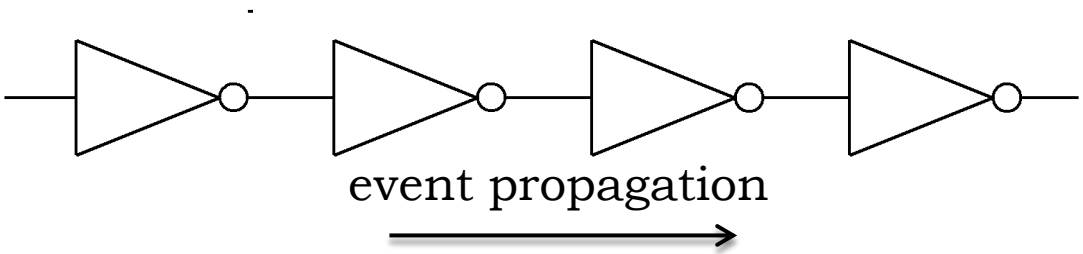
number of stages

- Global deterministic jitter
  - Accumulates linearly in the structure

$$D_{\det} = \sum_{i=1}^{2k} D_{\det_i}$$

Jitter in IRO

- Local Gaussian jitter
  - Period is defined by the propagation of one event around the ring during two laps
  - The event accumulates jitter each time it crosses a ring stage



$$\sigma_{period} = \sqrt{2k}\sigma_g$$

- Global deterministic jitter
  - Accumulates linearly in the structure

deterministic contribution during one period

$$D_{\det} = \sum_{i=1}^{2k} D_{\det_i}$$

deterministic contribution when the event crosses stage i

Jitter in STR

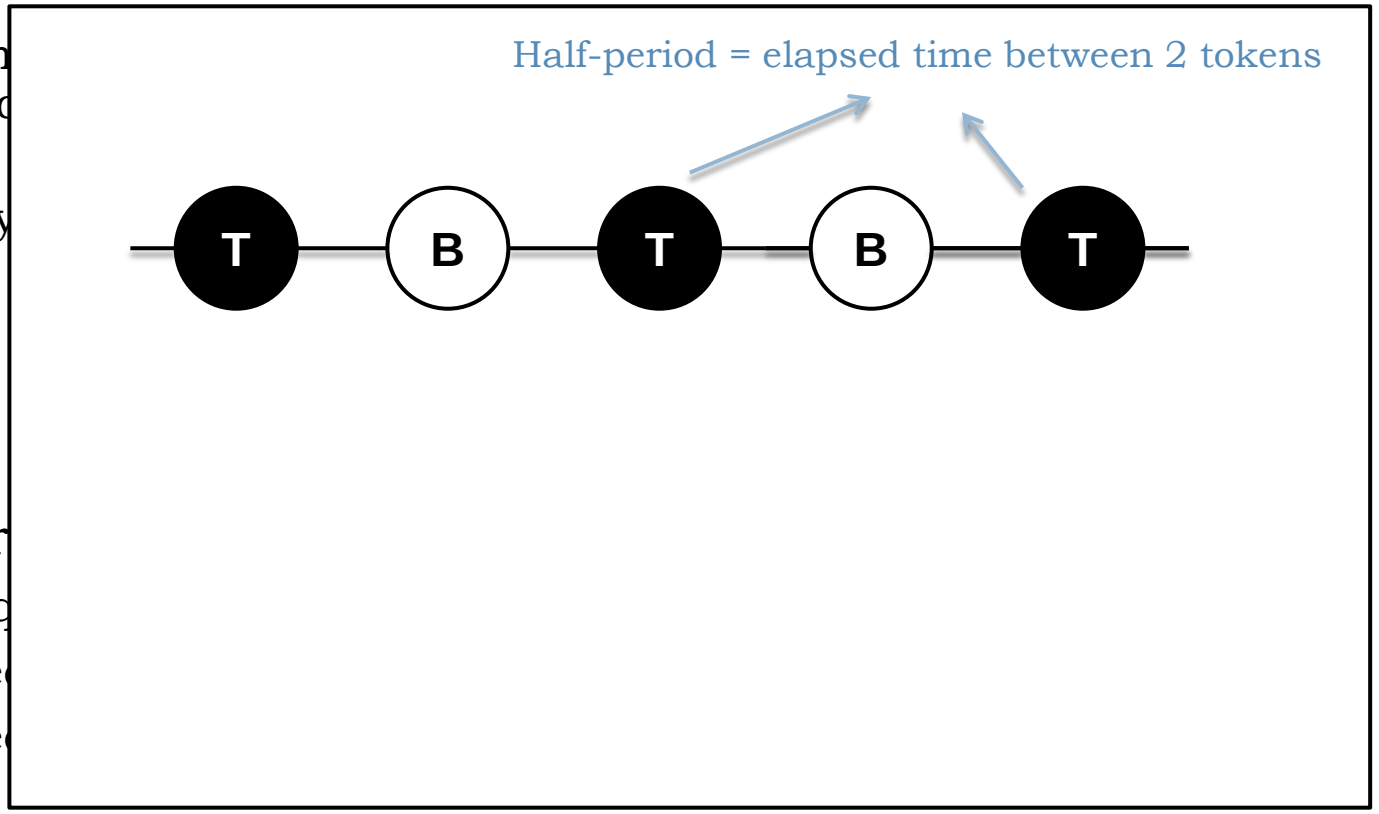
- Local Gaussian jitter
  - Half-period is defined by the elapsed time between two successive tokens
  - Each event crossing a ring experiences an uncertainty in its propagation delay due to the local Gaussian jitter
  - The effect of jitter accumulation is only temporary: the Charlie effect constantly regulates the tokens temporal spacing

$$\sigma_{period} \approx \sqrt{2}\sigma_g$$

- Global deterministic jitter
  - Applied equally to each token
  - Attenuated due to the difference
  - Attenuated due to the Charlie effect

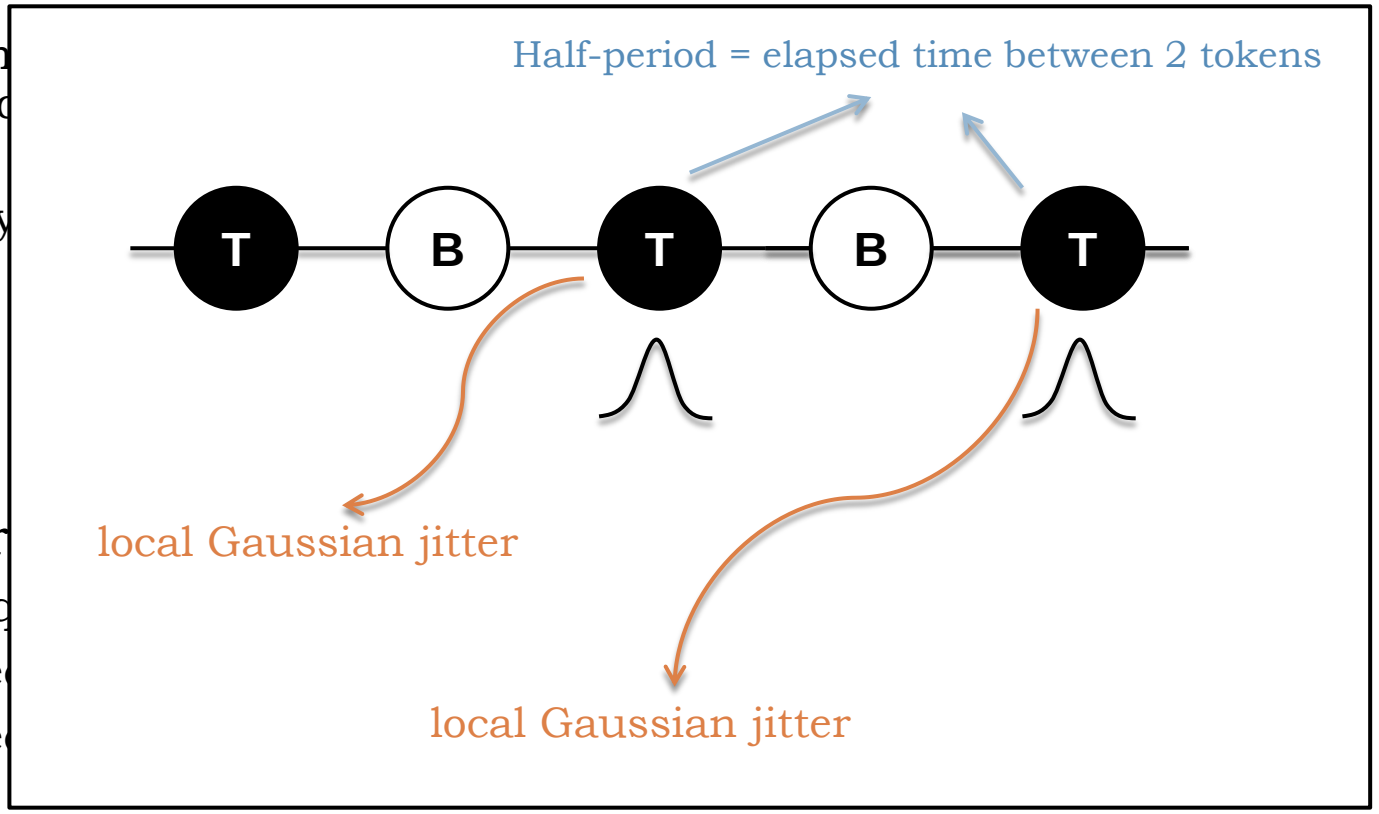
Jitter in STR

- Local Gaussian jitter
  - Half-period is defined by the elapsed time between two successive tokens
  - Each even
    propagati
  - The effect
    constantly
- Global deter
  - Applied eq
  - Attenuate
  - Attenuate



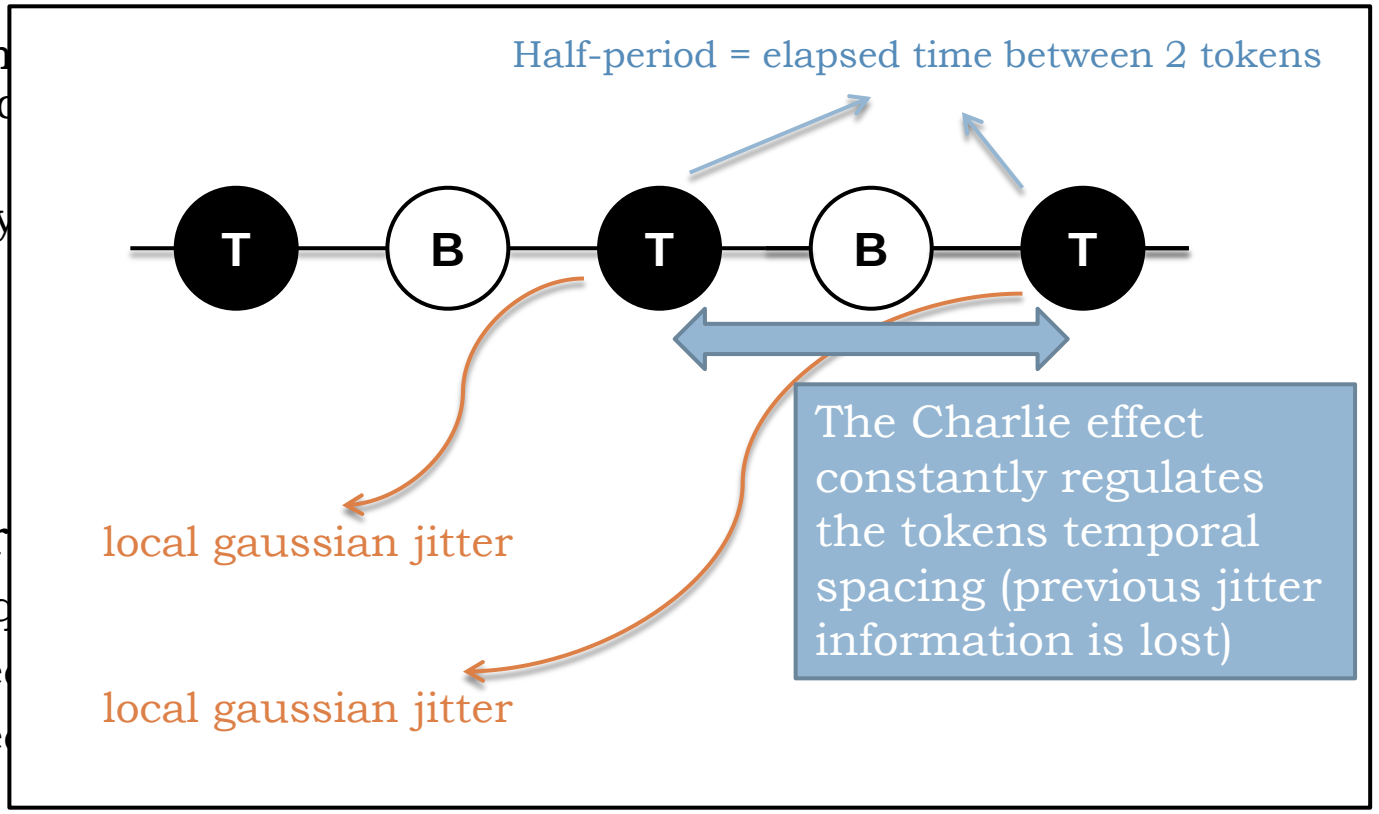
Jitter in STR

- Local Gaussian jitter
  - Half-period is defined by the elapsed time between two successive tokens
  - Each even
    propagati
  - The effect
    constantly
- Global deter
  - Applied eq
  - Attenuate
  - Attenuate



Jitter in STR

- Local Gaussian jitter
  - Half-period is defined by the elapsed time between two successive tokens
  - Each even
    propagati
  - The effect
    constantly
- Global deter
  - Applied eq
  - Attenuate
  - Attenuate



Jitter in STR

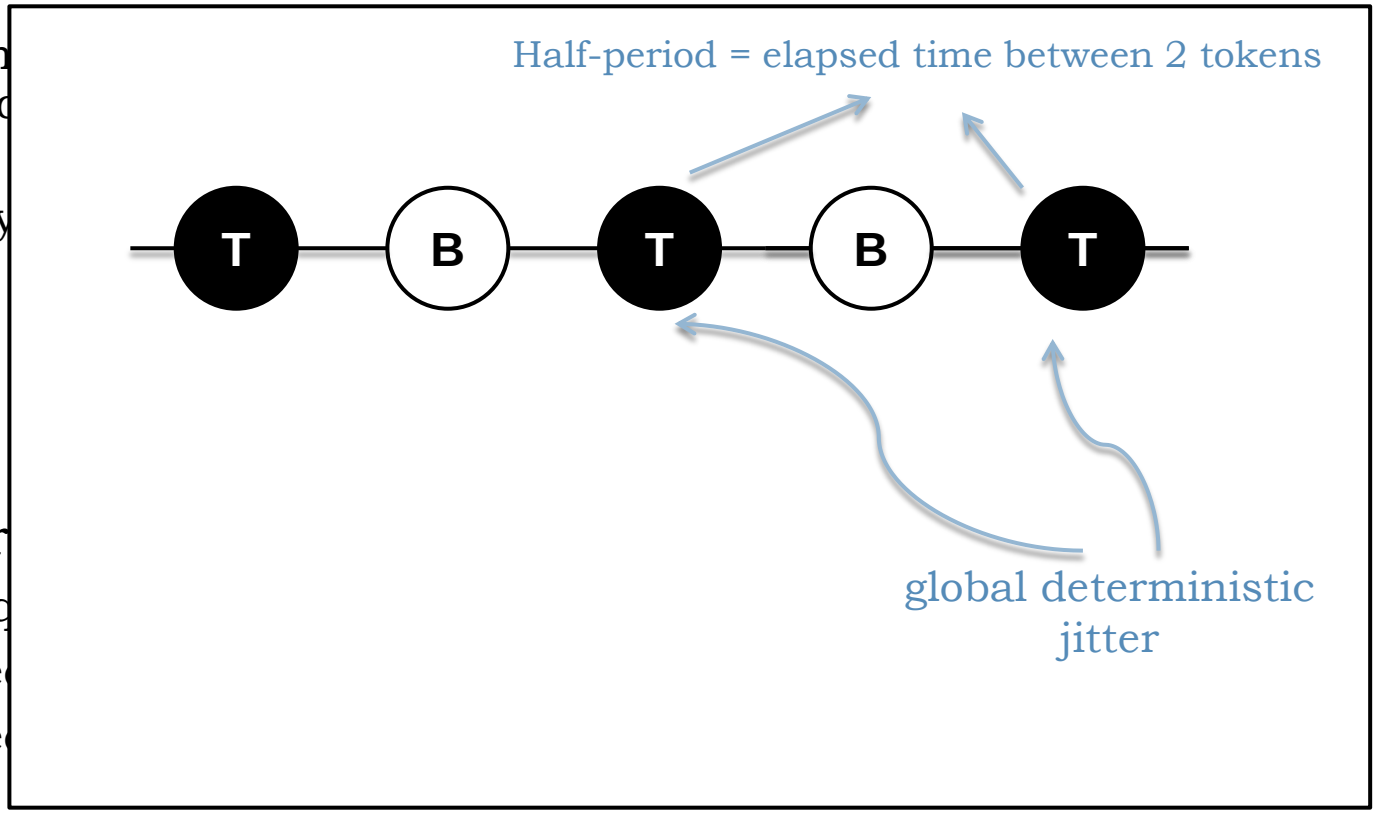
- Local Gaussian jitter
  - Half-period is defined by the elapsed time between two successive tokens
  - Each event crossing a ring experiences an uncertainty in its propagation delay due to the local Gaussian jitter
  - The effect of jitter accumulation is only temporary: the Charlie effect constantly regulates the tokens temporal spacing

$$\sigma_{period} \approx \sqrt{2}\sigma_g$$

- Global deterministic jitter
  - Applied equally to each token
  - Attenuated due to the difference
  - Attenuated due to the Charlie effect

Jitter in STR

- Local Gaussian jitter
  - Half-period is defined by the elapsed time between two successive tokens
  - Each even
    propagatio
  - The effect
    constantly
- Global deter
  - Applied eq
  - Attenuate
  - Attenuate



Jitter in STR

- Local Gaussian jitter
  - Half-period is defined by the elapsed time between two successive tokens
  - Each event crossing a ring experiences an uncertainty in its propagation delay due to the local Gaussian jitter
  - The effect of jitter accumulation is only temporary: the Charlie effect constantly regulates the tokens temporal spacing

$$\sigma_{period} \approx \sqrt{2}\sigma_g$$

- Global deterministic jitter
  - Applied equally to each token
  - Attenuated due to the difference
  - Attenuated due to the Charlie effect

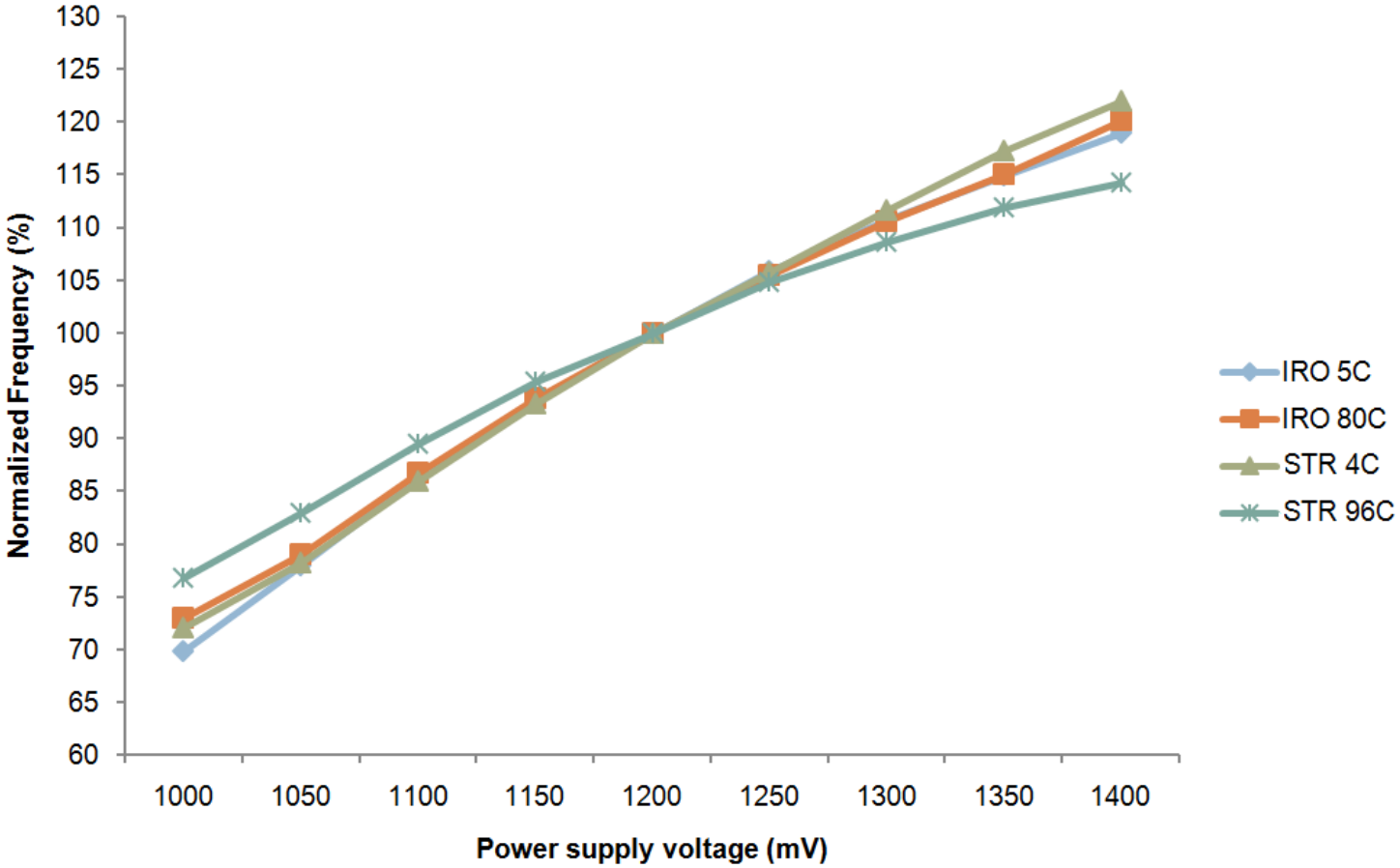
Experimental Results

- Experimental setup
  - 5 boards designed especially for TRNG applications featuring ALTERA Cyclone III devices and linear voltage regulators
  - Wide band digital oscilloscope Lecroy Wavepro 735 ZI (3.5 GHz bandwidth – 40 GS/s)
  - LVDS (Low Voltage Differential Signaling) interface
  - Active differential probes (4 GHz bandwidth)

- Objectives
  - Compare the sensitivity to voltage variations of IRO and STR
  - Evaluate and confirm the robustness of STR to process variability
  - Measure jitter in IRO to estimate the jitter generated locally in one single gate
  - Measure jitter in STR to confirm our proposed model

Robustness to Voltage Variations (1)

- Normalized frequency Vs power supply voltage



$$F_n = \frac{F}{F_{nom}}$$

Robustness to Voltage Variations (2)

- Normalized frequency excursion for power supply voltage sweep

$$\Delta F = \frac{F_{\max} - F_{\min}}{F_{nom}}$$

	Nominal frequency (Mhz)	Normalized frequency excursion
IRO 5C	375.82	49.15 %
IRO 25C	73.49	47.72 %
IRO 80C	22.84	47.07 %
STR 4C	653.47	49.95 %
STR 24C	432.54	44.20 %
STR 48C	407.90	**38.72 %**
STR 64C	368.58	**38.87 %**
STR 96C	320.48	**37.38 %**

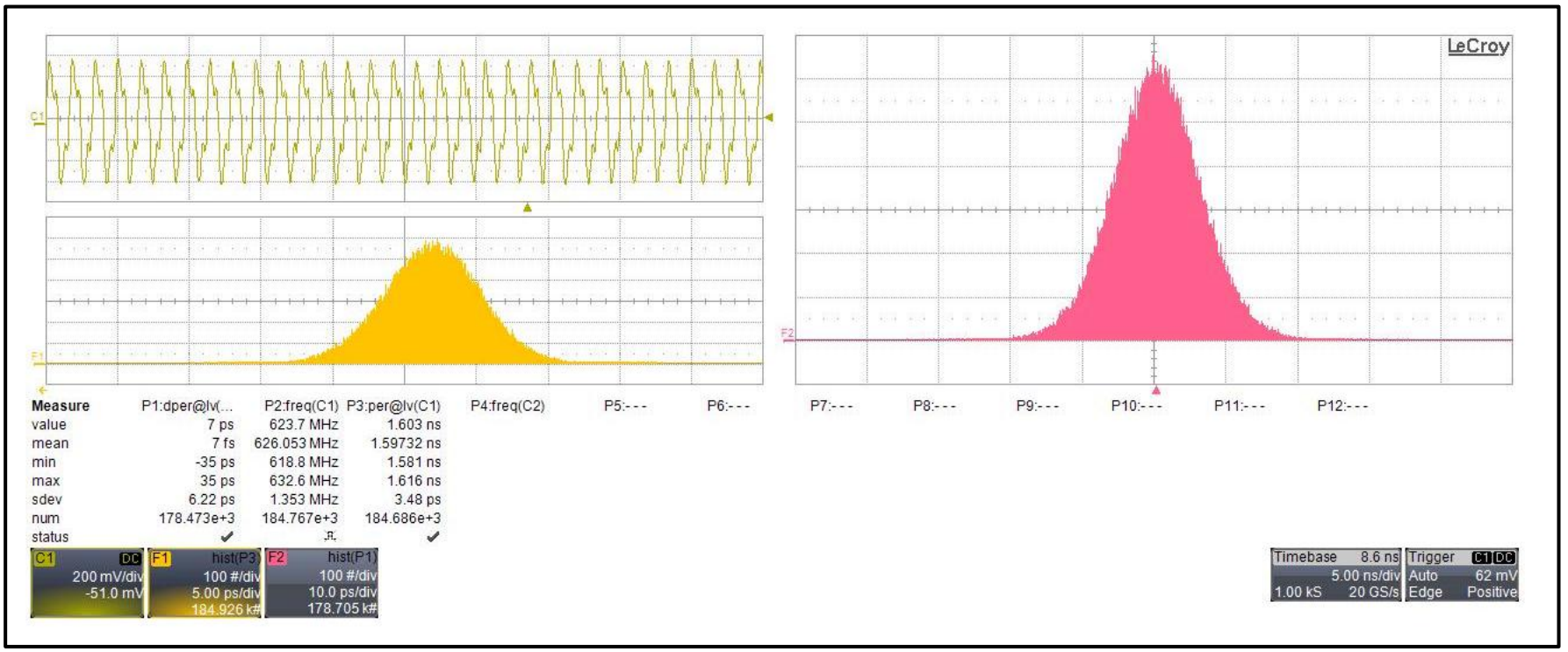
Robustness to Process Variability

- The same bit-stream is sent to each of the 5 available boards
- Relative standard deviation of measured period values is used to evaluate the sensitivity to manufacturing process variability

	Board 1	Board 2	Board 3	Board 4	Board 5	Relative standard deviation
IRO 3C	654.42	646.84	641.56	645.60	642.12	**0.79 %**
IRO 5C	305.72	306.44	302.54	304.87	302.20	**0.62 %**
STR 4C	669.05	660.06	658.60	659.90	655.62	**0.76 %**
STR 96C	328.16	328.54	327.55	328.47	327.46	**0.15 %**

Jitter in STR and IRO

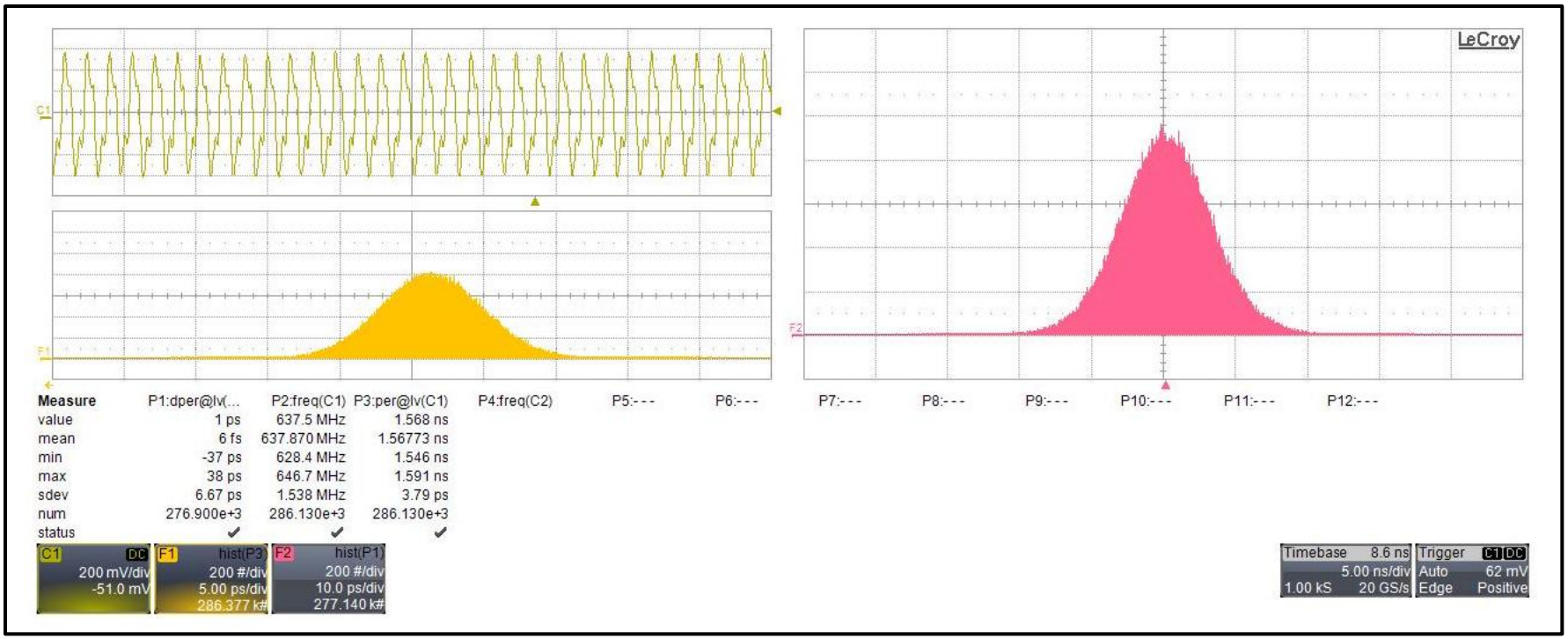
- Without deterministic noise and surrounding logic, both oscillators exhibit gaussian jitter



IRO 3C

Jitter in STR and IRO

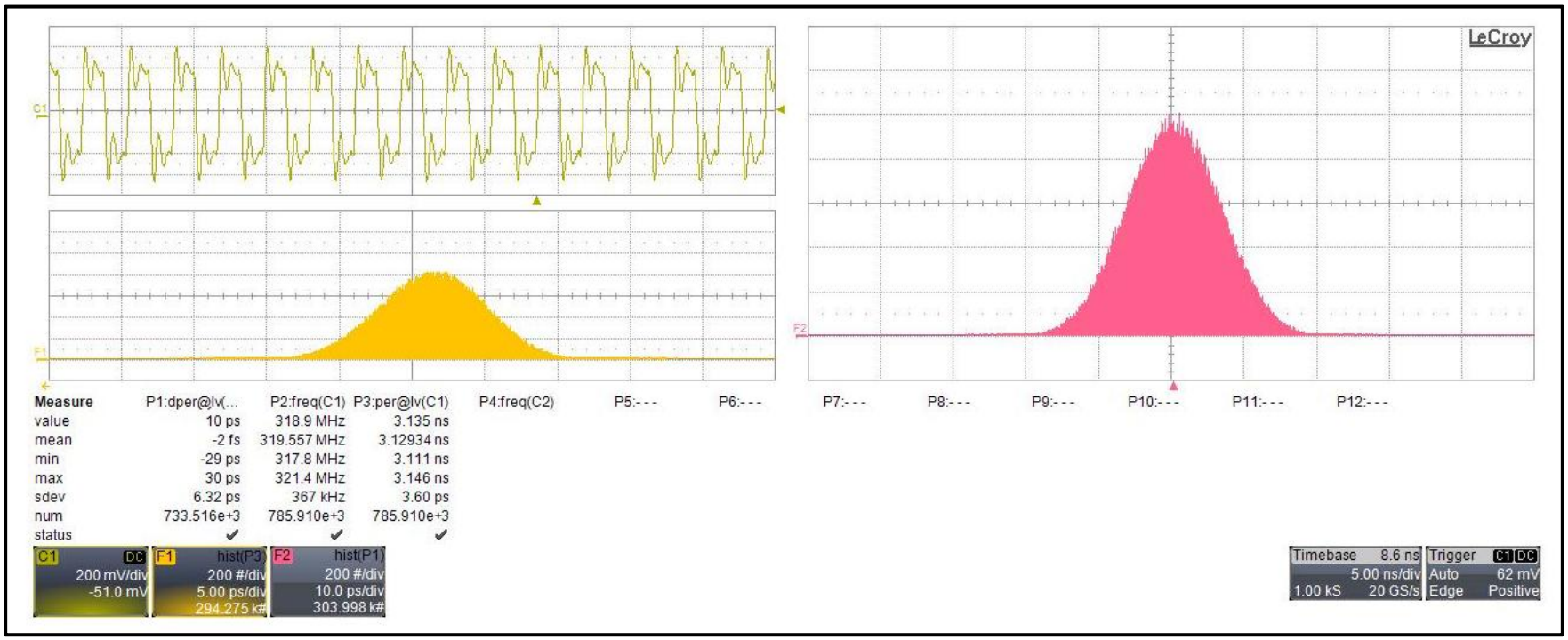
- Without deterministic noise and surrounding logic, both oscillators exhibit gaussian jitter



STR 4C

Jitter in STR and IRO

- Without deterministic noise and surrounding logic, both oscillators exhibit gaussian jitter

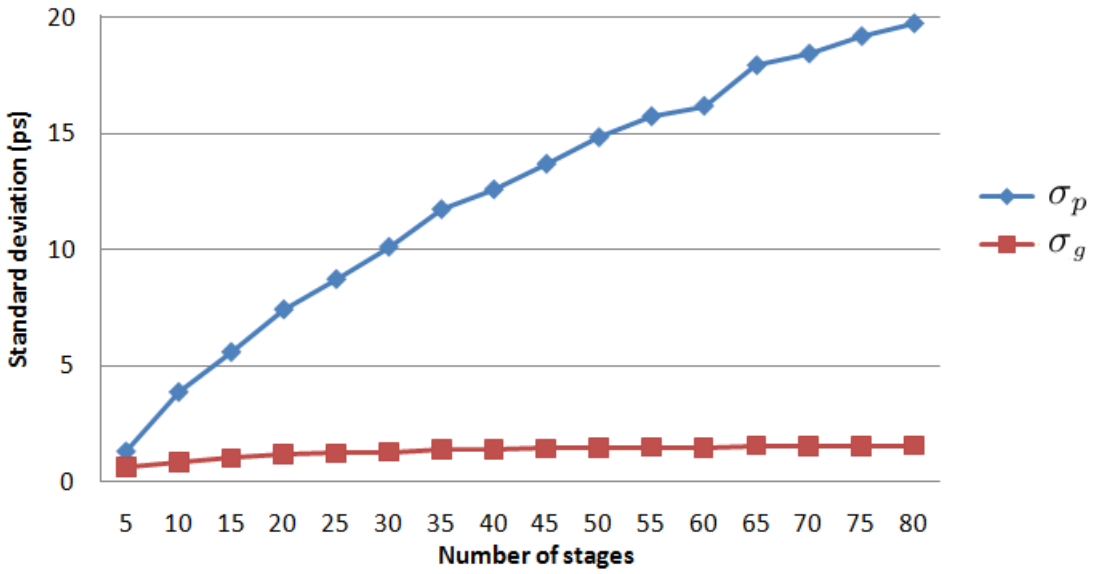


STR 96C

Jitter Measurements: IRO

EXPERIMENTAL RESULTS

- IRO
  - σ_p standard deviation related to the period jitter
  - σ_g standard deviation related to the jitter of one single gate



- The curve verifies a square-root accumulation tendency

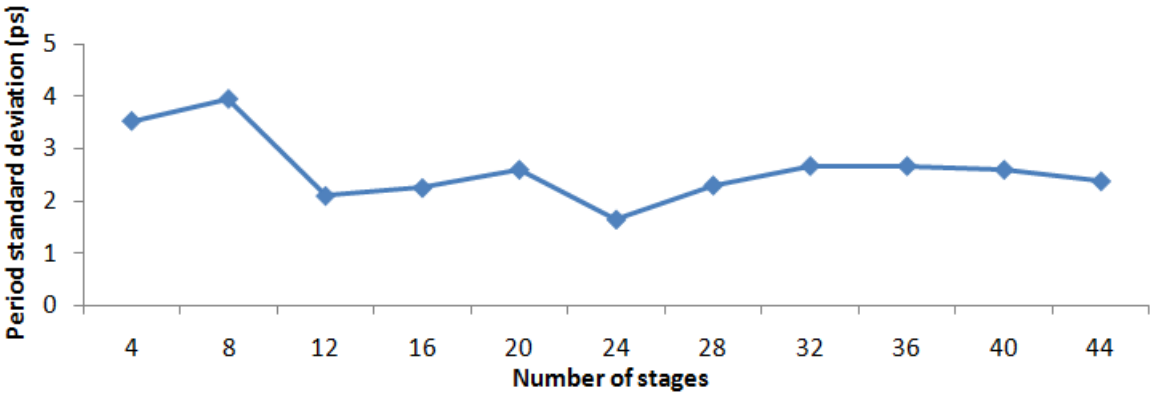
$$\sigma_g = \frac{\sigma_{period}}{\sqrt{2k}}$$

- The jitter of one single gate is estimated from the curve

$$\sigma_g \approx 2\,ps$$

Jitter Measurements: STR

- STR
  - σ_p standard deviation related to the period jitter
  - σ_g standard deviation related to the jitter of one single gate



- Period jitter is constant with respect to the number of elements (especially for high number of stages)

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

- Measured value verifies the proposed model

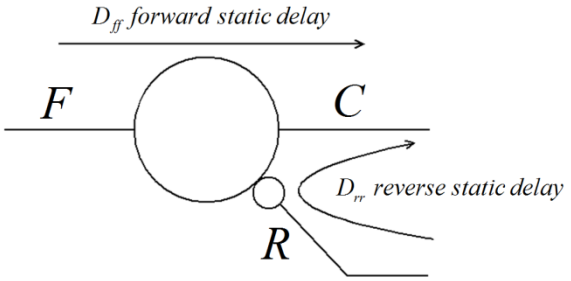
$$\sqrt{2}\sigma_g \approx 2.8ps \quad \Rightarrow \quad \sigma_{period} \approx \sqrt{2}\sigma_g$$

Conclusion

	IRO	STR
Behavior	one event evolving in the ring	several events evolving in the ring simultaneously
Period	varies linearly with number of stages	constant in the configuration Nt=Nb
Logic resources usage	**low**	higher than IRO, depending on the aimed robustness
Power consumption	**low**	probably higher than IRO
Robustness to process variability	increases with number of stages	**increases with number of stages while maintaining high frequency**
Robustness to voltage variations	Low	**increases with number of stages**
Jitter	**increases with number of stages** (square root accumulation)	Constant with number of stages, **each stage acts like an independent jitter source**

Analysis, Perspectives

- Ideally, when *Nt* = *Nb* and *Dff* = *Drr:*
  - Separation times are null
  - The Charlie effect is maximal



- Experiment shows that:
  - Increasing the number of stages improves the robustness to voltage variations
  - When increasing the number of stages, jitter stabilizes around its theoritical value when the Charlie effect is maximal

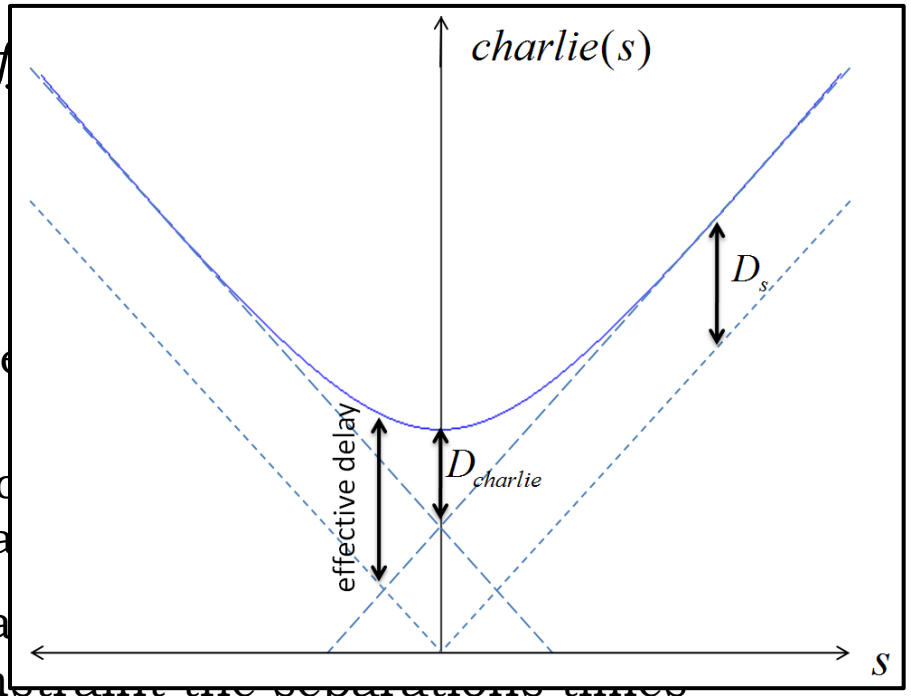
→ Increasing the number of stages seem to constraint the separations times near the « valley » of the Charlie curve

- This hypothesis needs to be explored by taking into account routing in the temporal model

→ Develop a variable stage timing parameters model

Analysis, Perspectives

- Ideally, when *Nt* = *Nb* and *Df*
  - Separation times are null
  - The Charlie effect is maximal
- Experiment shows that:
  - Increasing the number of stage variations
  - When increasing the number o theoritical value when the Cha



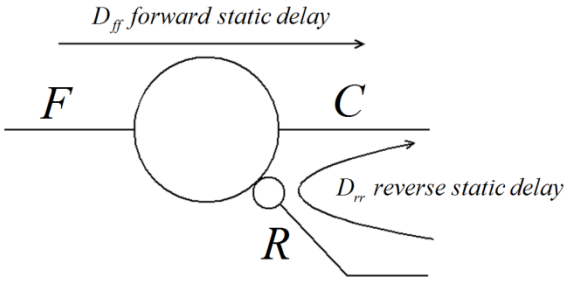
Increa
to con
near the « valley » of the Charlie curve

- This hypothesis needs to be explored by taking into account routing in the temporal model

Develop a variable stage timing parameters model

Analysis, Perspectives

- Ideally, when *Nt* = *Nb* and *Dff* = *Drr:*
  - Separation times are null
  - The Charlie effect is maximal



- Experiment shows that:
  - Increasing the number of stages improves the robustness to voltage variations
  - When increasing the number of stages, jitter stabilizes around its theoritical value when the Charlie effect is maximal

→ Increasing the number of stages seem to constraint the separations times near the « valley » of the Charlie curve

- This hypothesis needs to be explored by taking into account routing in the temporal model

→ Develop a variable stage timing parameters model

Ongoing Works

- A variable stage timing parameters model for STRs initialized with as many tokens as bubbles
  - Characterization and analysis of the separation times with respect to delay propagation disparities

- A secure and robust TRNG featuring self-timed rings
  - A proof of security based on the jitter model
  - First results: TRNG passes FIPS statistical tests with a 100 Mb\s throughput

Thank you !