A Physical Approach for Stochastic Modeling of TERO-based TRNG

Patrick Haddad[1,2], Viktor FISCHER[1], Florent BERNARD[1], and Jean NICOLAI[2]

1: Jean Monnet University Saint-Etienne, France

2: ST Microelectronics Rousset, France

CHES 2015 – Saint-Malo, France

September 2015

Random numbers in cryptography

- Random number generators constitute an essential part of (hardware) cryptographic modules
- The generated random numbers are used as:
  - Cryptographic keys (high security requirements)
  - Masks in countermeasures against side channel attacks
  - Initialization vectors, nonces, padding values, ...

Random numbers in logic devices

RANDOM NUMBER GENERATORS
(RNG)

DETERMINISTIC RNGs (DRNGs)

PHYSICAL TRUE RNGs (P-TRNGs)

DRNG + P-TRNG = Hybrid RNG

life.augmented

LABORATOIRE Hubert CURIEN
UMR • CNRS • 5516 • ST-ETIENNE

Classical versus modern TRNG evaluation approach

- Two main security requirements on RNGs:
  - R1: Good statistical properties of the output bitstream
  - R2: Output unpredictability
- Classical approach:
  - Assess both requirements using statistical tests – often impossible
- Modern ways of assessing security:
  - Evaluate statistical parameters using statistical tests
  - Evaluate entropy using entropy estimator (stochastic model)
  - Test online the source of entropy using dedicated statistical tests

Our objectives

Propose a stochastic model of TERO-based TRNG [a]

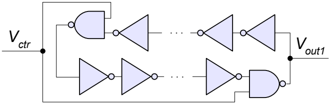
- Based on physical parameters quantifiable inside the device
- Can be used for online entropy assessment

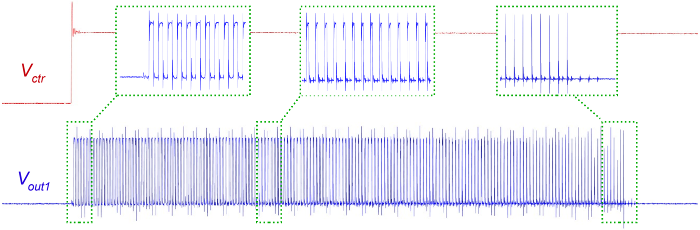
[a] M. Varchola and M. Drutarovsky, *New high entropy element for FPGA based true random number generators*, CHES 2010

Transition effect ring oscillator (TERO)

Principle:

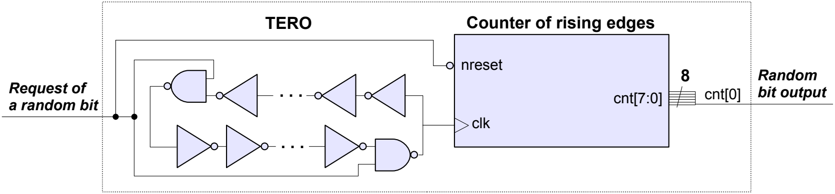
- Even number of inverters and two control gates in a loop
- Oscillates temporarily because of the difference in two branches
- Number of oscillations varies because of the intrinsic noise





TERO-based P-TRNG

Implementation:



- An asynchronous 8-bit counter counts random number of oscillations
- We use the counter to characterize the TERO
- The LSB of the counter (*cnt*(0)) is used also as the random bit (TRNG output)

Outlines of the modeling

Since the P-TRNG is periodically restarted, the counter values are mutually independent, therefore:

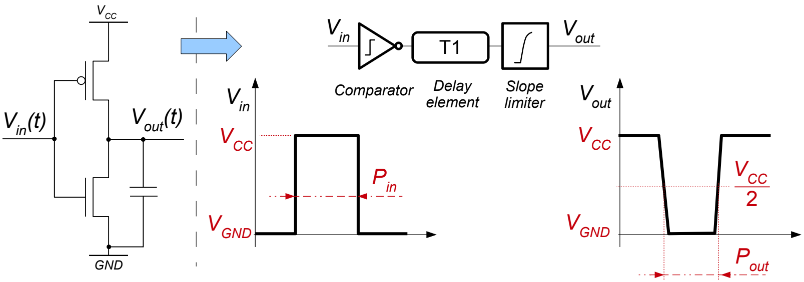
$$Entropy = -p_1 \cdot log_2(p_1) - (1 - p_1) \cdot log_2(1 - p_1),$$

where $p_1 = Pr\{cnt(0) = 1\}$.

We want to determine p_1, therefore, we need to analyze and characterize the distribution of counter values.

A noiseless inverter

Behavior of a noiseless inverter:

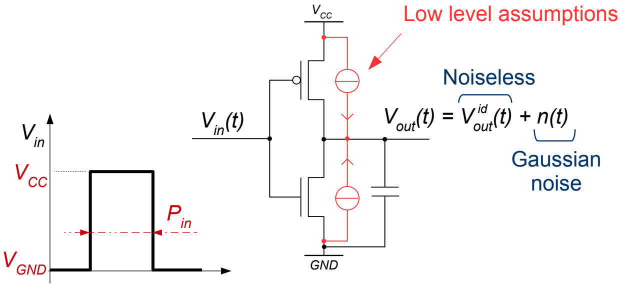


Analyzed by Reyneri *et al.*, [2] they determined $P_{out} = f(P_{in})$

[2] Reyneri *et al.*, *Oscillatory metastability in homogeneous and inhomogeneous flip-flops, IEEE SSC, 1990*

A noisy inverter

Behavior of a noisy inverter:

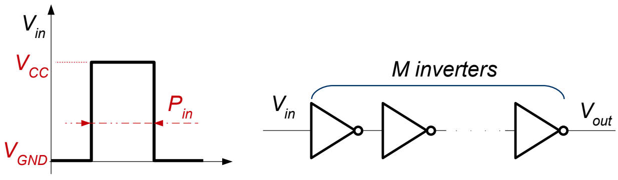


In the paper, using the model of Reyneri *et al.*, we determine

$P_{out} \sim \mathcal{N}(f(P_{in}), \sigma^2)$ (see *Lemma 1*)

An chain of M inverters

Impact of the noise on a chain of inverters:

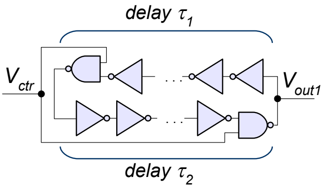


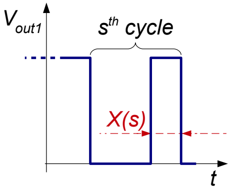
We apply *Lemma 1* to each inverter of the chain

We obtain $P_{out} \sim \mathcal{N}(F(P_{in}, M), G(\sigma^2, M))$

A loop of inverters

Impact of the noise on the duty cycle:





$$X(s) \sim N\left(\frac{\tau_1+\tau_2}{2} + \frac{\tau_2-\tau_1}{2}\cdot R^s,\ \sigma^2\cdot\frac{R^{2s+1}-1}{(1+H_d)^2-1}\right)$$

Geometric series (ratio R)

Stochastic model of TERO P-TRNG

The model characterizes distribution of counter values

- Objective: We want to get $Pr\{cnt = s\}$
- We just know the distribution of $X(s)$

We can use the equivalence $cnt > s \iff X(s) > 0$

Then

$$Pr\{cnt > s\} = \frac{1}{2}\left[1 - erf\left(K \cdot \frac{1 - R^{s-s_0}}{\sqrt{R^{2s+1} - 1}}\right)\right]$$

R is the ratio of the geometric series

K reflects the jitter σ^2

s_0 reflects the difference $\tau_1 - \tau_2$

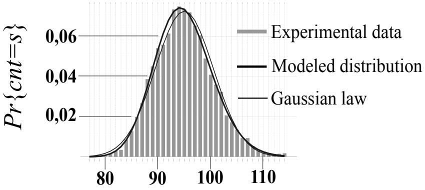
and

$$Pr\{cnt = s\} = Pr\{cnt \leq s\} - Pr\{cnt \leq s+1\}$$

Experimental validation

Validation of the modeled distribution using a χ^2 test

Experiment: TERO 1 in an ST Microelectronics 28 nm ASIC



$K = 35{,}680$
$s_0 = 94{,}152$
$R = 1{,}0153$

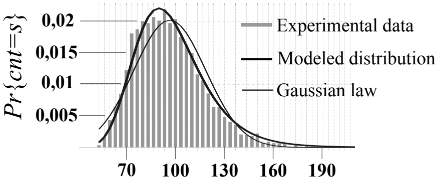
For a significance level $\alpha = 0.05$ and 38 degrees of freedom, the test statistic has to be lower than 53.384

Our model: the test statistic is 40.35
Gaussian law: the test statistic is 149.3

Experimental validation

Validation of the modeled distribution using a χ^2 test

Experiment: TERO 2 in an ST Microelectronics 28 nm ASIC



$K = 9{,}6939$
$s_0 = 90{,}675$
$R = 1{,}013$

For a significance level $\alpha = 0.05$ and 76 degrees of freedom, the test statistic has to be lower than 97.351

Our model: the test statistic is 33.97
Gaussian law: the test statistic is $> 10^6$

Entropy estimation

From our physical analysis we know $Pr\{cnt = s\}$
From $Pr\{cnt = s\}$ we compute $p_1 = Pr\{cnt(0) = 1\}$

Recall: Since the TERO is periodically restarted, the subsequent counter values are mutually independent and thus

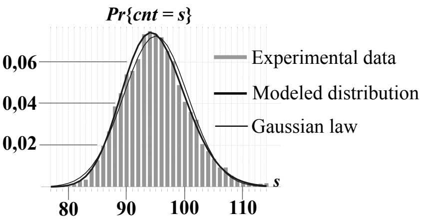
$$H_{sample} = -\sum_{s \in \mathbb{N}} p_s \log_2(p_s)$$

$$H_{lsb} = -p_1 \cdot log_2(p_1) - (1 - p_1) \cdot log_2(1 - p_1)$$

The second term represents the entropy of our TERO P-TRNG

Estimated entropy

Application of the model to TERO 1 and TERO 2



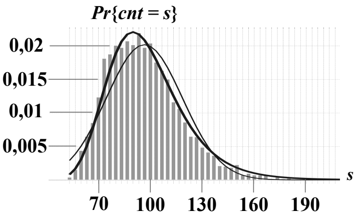
$K = 35{,}680$

$s_0 = 94{,}152$

$R = 1{,}0153$

$H_{sample} = 4{,}47$

$H_{lsb} > 0{,}999$



$K = 9{,}6939$

$s_0 = 90{,}675$

$R = 1{,}013$

$H_{sample} = 6{,}32$

$H_{cnt(0)} > 0{,}999$

- In the two cases the entropy of the raw binary signal exceeds the value 0.997 required by AIS31
- All generated bit streams passed tests T0 to T8 of AIS 31

life.augmented

LABORATOIRE Hubert CURIEN UMR • CNRS • 5516 • ST-ETIENNE

Conclusions

- We presented a **stochastic model** of the TERO P-TRNG
- The model is based on **transistor-level assumptions**
- The model was **validated** in an ASIC implemented using 28 nm ST Microelectronics technology
- We derived the **entropy** from this model
- The entropy and the output bit rate can be **easily managed** using the model

Our thanks to Nicolas Bruneau, Michel Agoyan and Yannick Teglia for their help and availability in numerous discussions.

This work has received fundings from the European Union's Horizon 2020 research and innovation programme in the framework of the project HECTOR

This work has received fundings from the European ENIAC Joint Undertaking (JU) in the framework of the project TOISE

life.augmented

LABORATOIRE Hubert CURIEN UMR • CNRS • 5516 • ST-ETIENNE