Jitter Estimation with High Accuracy for Oscillator-Based TRNGs

Shaofeng Zhu, Hua Chen, Linmin Fan, Meihui Chen, Wei Xi, Dengguo Feng

TCA Laboratory, Institute of Software, Chinese Academy of Sciences

November 13, 2018

Outline

Introduction

Preliminaries: Signal Model, Entropy Evaluation, Jitter Estimation

Jitter Estimation with High Accuracy

Jitter Estimation on FPGA

Comparisons and Conclusion

Random Numbers and TRNGs

- Random Numbers
  - Applications in cryptography: secret keys, IVs, paddings, nonces, random masks for countermeasure, etc..
  - Properties: good statistical properties, unpredictability.
- True Random Number Generators (TRNGs)
  - Digitization of random physical phenomenon (jitter, chaos, metastability, etc.) or random events (keystrokes, etc.).
  - Can generate random numbers with unpredictability.

Are the TRNGs secure for applications ?

To evaluate the TRNGs

- Statistical Tests
  - NIST SP800-22[1], Diehard[2], etc..
  - Only test the statistical properties, but not the unpredictability.
- Entropy Evaluation: to quantitatively measure the unpredictability.
  - Based on output sequence: NIST SP800-90B[3].
    When pseudo-randomness is mixed in the output sequence, overestimation of the entropy may happen.
  - Based on the model of random signals of the TRNGs

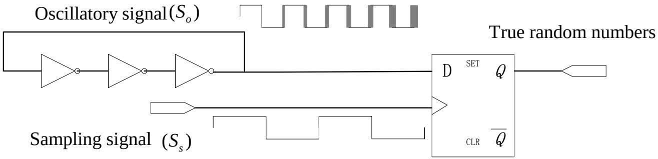
[1] Andrew Rukhin et al. *NIST SP800-22: A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications.*

[2] George Marsaglia. "The Marsaglia random number CDROM including the DIEHARD battery of tests of randomness". In: *Diehard Tests* (1995).

[3] Meltem Sonmez Turan et al. *NIST SP800-90B: Recommendation for the Entropy Sources Used for Random Bit Generation.*

Ring Oscillator-based TRNGs

- Advantages
  Easy to implement on logic device, resource-saving, etc..
- Structure



- Noises on logic devices
  - Uncorrelated random noise (mainly thermal noise)
  - Correlated random noise (mainly low-frequency flicker noise)
- Source of the Randomness
  Jitter: the STD[4] of the periods, will be accumulated in the sampling interval
  Components: thermal jitter and flicker jitter

[4] standard deviation

Related Works on Jitter Estimation

- External estimation
  - Measuring equipments such as oscilloscopes.
  - Additional jitter from Input/Output circuits and pins
- Internal estimation–Valtchanov et al.[5]
  - Counter-based jitter estimation–counting rising edges of S_o in fixed intervals.
  - Accumulated jitter $\approx$ the STD of the number of rising edges
  - Approximate estimation with quantization
- Improvement of Ma et al.[6] (CHES'2014)
  - Count both the rising and falling edges of S_o
  - Actually reduces the quantization step size by half

---

[5] Boyan Valtchanov et al. "Modeling and observing the jitter in ring oscillators implemented in FPGAs". In: *DDECS*. 2008.

[6] Yuan Ma et al. "Entropy Evaluation for Oscillator-Based True Random Number Generators". In: *CHES*. 2014.

Related Works on Jitter Estimation

- Fischer et al.[7] (CHES'2014)
  - Based on Monte Carlo method
  - Estimation error is smaller than 5% in simulation.
- ☐ The above mentioned methods actually estimate the total jitter.
- Haddad et al.[8]: jitter separating approach
  - To gain the ratio of thermal jitter in the total jitter
  - Also use a counter-based method to estimate the total jitter

[7] Viktor Fischer and David Lubicz. "Embedded Evaluation of Randomness in Oscillator Based Elementary TRNG". In: *CHES*. 2014, postnote.

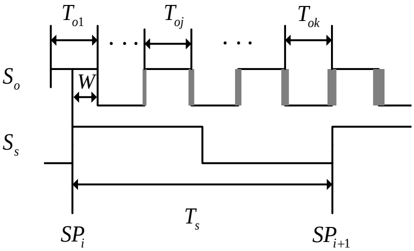
[8] Patrick Haddad et al. "On the assumption of mutual independence of jitter realizations in P-TRNG stochastic models". In: *DATE*. 2014, postnote.

Motivation

- Overestimation of jitter will result in the overestimation of the randomness–serious problem!
- Error (quantization error) will be introduced in previous counter-based jitter estimation methods. It will cause the overestimation of the jitter.
- Jitter estimation should be efficient when implemented on-line .

Signal Model

- Notions in the signal model

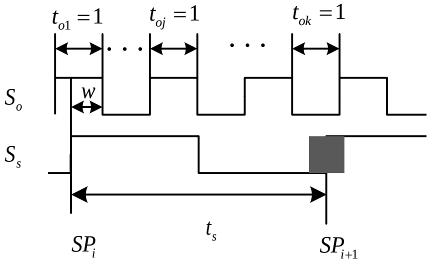


- The edge intervals of S_o, $T_{o1} \cdots T_{oj} \cdots T_{ok}$ has mean μ_o and standard deviation σ_o;
  μ_o: half mean period of S_o;
  σ_o: half period jitter of S_o, will be accumulated in T_s.
- T_s is stable.
- The waiting time $W \sim \boldsymbol{U}(0, \mu_o)$[9], and is independent from the current T_s.

[9] Wolfgang Killmann and Werner Schindler. "A Design for a Physical RNG with Robust Entropy Estimators". In: *CHES 2008*.

Signal Model

- Normalization
  - $T_s \to t_s = \frac{T_s}{\mu_o}, T_{oj} \to t_{oj} = \frac{T_{oj}}{\mu_o}, \sigma_o \to \sigma = \frac{\sigma_o}{\mu_o},\ \mu_o \to 1, W \to w = \frac{W}{\mu_o}$.
  - The μ_o can be measured from the frequency of S_o.
- Equivalent signal model



  - Edge interval t_{oj} is stable, $t_{o1} = \cdots = t_{oj} = \cdots = 1$.
  - t_s has mean value μ_s and standard deviation σ_s;
    σ_s: total jitter=(thermal+flicker) jitter, $\sigma_s^2 = (\sigma_s^{th})^2 + (\sigma_s^{fl})^2$.
  - $w \sim \boldsymbol{U}(0,1)$ and is independent from the current t_s.

Entropy Evaluation

TCA

- Assumptions
  1. Only the uncorrelated thermal noise is taken into account.
  2. Edge intervals $T_{o1} \cdots T_{oj} \cdots T_{ok} \sim \boldsymbol{N}(\mu_o, \sigma_o^2)$
  3. $t_s \sim \boldsymbol{N}(\mu_s, (\sigma_s^{th})^2)$
- Lower bound of the entropy, contributed by the thermal noise[10]

$$H_{min} = 1 - \frac{4}{\pi^2 \ln(2)} e^{-\pi^2 (\sigma_s^{th})^2}. \tag{1}$$

- H_{min} is determined by σ_s^{th}, precisely estimating σ_s^{th} is important!

[10] Mathieu Baudet et al. "On the Security of Oscillator-Based Random Number Generators". In: *J. Cryptology* (2011).

Jitter Estimation

- Jitter in t_s maybe too small to be measured.
- Take a longer measuring interval t_m, the thermal jitter is "sqrt" accumulated with the interval size.
- Estimation for the σ_s^{th}
  1. Separating

$$\sigma_m^{th} = r_{th}\sigma_m, \sigma_s^{th} = \sqrt{\frac{t_s}{t_m}}\sigma_m^{th}. \tag{2}$$

  2. Approximating: t_m is short enough so that the σ_m^{th} dominates over the σ_m^{fl}

$$\sigma_m^{th} \approx \sigma_m, \sigma_s^{th} \approx \sqrt{\frac{t_s}{t_m}}\sigma_m. \tag{3}$$

- The total jitter σ_m should be estimated first.

Introduction

Preliminaries: Signal Model, Entropy Evaluation, Jitter Estimation

Jitter Estimation with High Accuracy

Jitter Estimation on FPGA

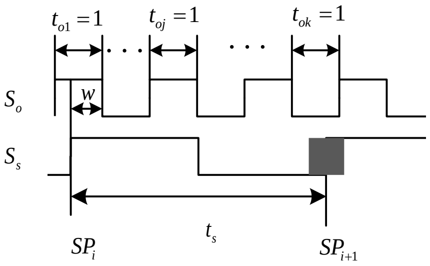
Comparisons and Conclusion

Error Investigation

Counter-based jitter method of Ma et al.

- Edge-counting
  X: the number of the rising and falling edges of S_o in t_m
- Approximation
  $$Var(t_m) \approx Var(X). \tag{4}$$
  Vs. t_m, X is easy to measure on the chip.
- Estimation
  $$\sigma_m = \sqrt{Var(t_m)} \approx \sqrt{Var(X)}. \tag{5}$$

Error Investigation



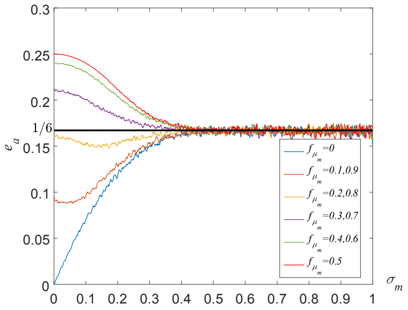
- Source of error

$$X = \lfloor t_m - w + 1 \rfloor_{q=1}.(q : quantization\ step) \qquad (6)$$

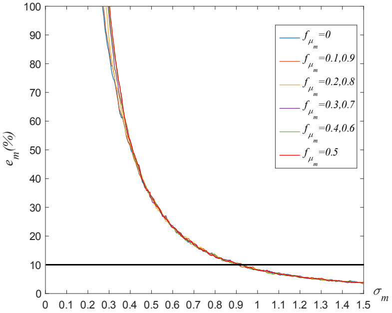
1. waiting time factor:$(-w+1)$ 2. the quantization

Error Investigation

- Evaluation of the errors
  - Errors of the approximation (4): abs error e_a=Var(X)−Var(t_m), rel error $e_r = \frac{|e_a|}{\text{Var}(t_m)}$
  - Error level of Ma's method: $e_m = \frac{1}{2} e_r$



(a) Absolute error e_a



(b) Error level e_m

To Correct the Error

- Sheppard's Correction[11]
  For a random variable v with continuous distribution, its rounding quantized value $v_q = [v]_q$. The quantization error $e_q = v - v_q$ will approximately follow $\boldsymbol{U}(-q/2, q/2)$ and be independent from v.

$$\mathrm{E}(v) = \mathrm{E}(v_q), \mathrm{E}(v^2) = \mathrm{E}(v_q^2) - q^2/12. \tag{7}$$

[11] William Fleetwood Sheppard. "On the Calculation of the most Probable Values of Frequency-Constants for Data arranged according to Equidistant Division of a Scale". In: *Proceedings of the London Mathematical Society* (1897).

Analysis and Correction

In the jitter estimation case,

- $\mathrm{Var}(X)$ and $\mathrm{Var}(t_m)$

$$X = \lfloor t_m - w + 1 \rfloor_{q=1} = [t_m - w + 0.5]_{q=1}. \tag{8}$$

$$e_q = (t_m - w + 0.5 - X) \sim U(-0.5, 0.5) \tag{9}$$

w and e_q are approximately independent from t_m

$$\mathrm{Var}(X) = \mathrm{Var}(t_m - w + 0.5 - e_q) \approx \mathrm{Var}(t_m) + \mathrm{Var}(w) + \mathrm{Var}(e_q). \tag{10}$$

The deviation between $\mathrm{Var}(t_m)$ and $\mathrm{Var}(X)$ is indeed caused by w and e_q.

Analysis and Correction

- New approximation for $\mathrm{Var}(t_m)$

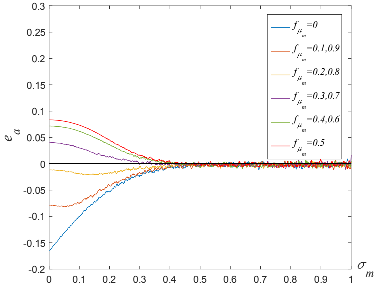
$$\mathrm{Var}(t_m) \approx \mathrm{Var}(X) - \mathrm{Var}(w) - \mathrm{Var}(e_q) \approx \mathrm{Var}(X) - 1/6. \tag{11}$$

- New estimation for σ_m

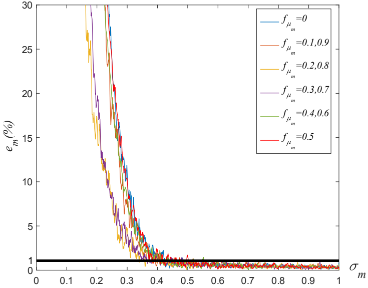
$$\sigma_m \approx \sqrt{\mathrm{Var}(X) - 1/6}. \tag{12}$$

Analysis and Correction

- Evaluation of the errors
  - Errors of new approxiamtion (11): e_a=Var$(X)-\frac{1}{6}-$Var(t_m), $e_r = \frac{|e_a|}{\text{Var}(t_m)}$
  - Error level of our method : $e_m = \frac{1}{2} e_r$



(a) Absolute error e_a

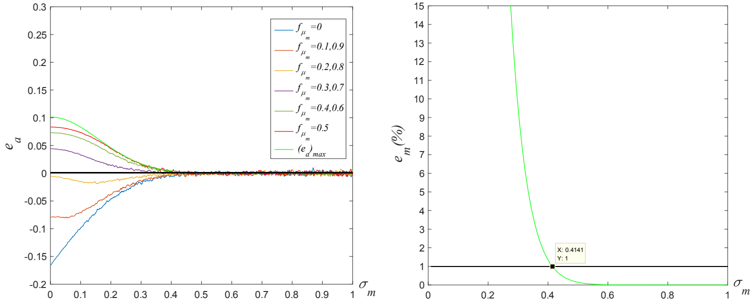


(b) Error level e_m

Theoretical Error Analysis

- Upper bound of the errors

$$(e_a)_{max} \approx \frac{1}{\pi^2} e^{-2\pi^2\sigma_m^2}, \ (e_m)_{max} \approx \frac{1}{2\pi^2\sigma_m^2} e^{-2\pi^2\sigma_m^2} \quad (13)$$



(a) Theoretical absolute error e_a (b) Theoretical error level e_m

An Efficient Calculation of Var(X)

- Ordinary Calculation

$$\text{Var}(X) = \frac{\sum_{i=1}^{N} x_i^2}{N} - (\frac{\sum_{i=1}^{N} x_i}{N})^2, \tag{14}$$

  needs $N + 1$ multiplications, N is the sample size.
- In modern logic devices, σ_m is usually very small, so the counting results $x_1, \cdots, x_N$ will vary slightly around $\bar{x}$.
- The sample space of X is small too. $\mathcal{S}_X = \{p_i | p_i = \lfloor \bar{x} \rfloor - l + i; 1 \leq i \leq 2l; 5 \leq l \ll N\}$ can cover most of the counting results.
- New calculation
  1. Count $x_1, \cdots, x_N$ on $p_1, \cdots, p_{2l}$, record with $c_1, \cdots, c_{2l}$
  2. Calculate

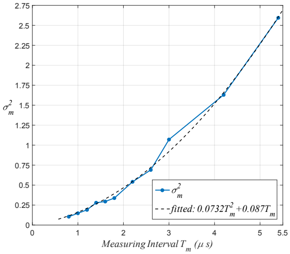
$$\text{Var}(X) = \frac{\sum_{i=1}^{2l} c_i \cdot (p_i - \bar{x})^2}{N}. \tag{15}$$

  Only $4l$ ($\ll N + 1$) multiplications are needed.

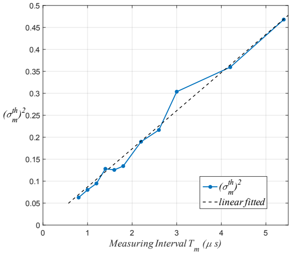
TCA

Off-line Estimation

- Steps:
  1. Count the edges of the oscillatory signal in intervals with different sizes (T_m s)
  2. Estimate the total jitter σ_m with the proposed method.
  3. Separate the jitter: fit σ_m^2-T_m by $\sigma_m^2 = aT_m^2 + bT_m$, $\sigma_m^{th} = r_{th}\sigma_m = \sqrt{\frac{b}{b+aT_m}}\sigma_m$
- Setups: 3-inverters RO on Altera Cyclone IV FPGA with 305MHz, $T_m : 0.8\mu s \rightarrow 5.4\mu s$
- Results:



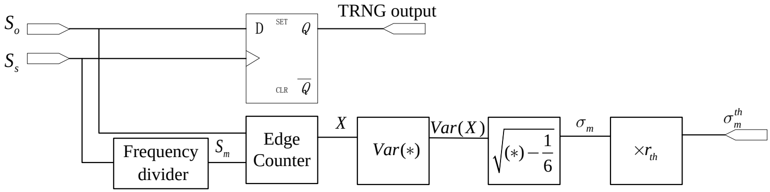
(a) Total jitter



(b) Thermal jitter

On-line Estimation

- Vs. Off-line Estimation: size of T_m is fixed.
- Steps
  1. Pre-calculate $r_{th} = \sqrt{\frac{b}{b+aT_m}}$, configure it in the circuit.
  2. Estimate σ_m with the proposed method on the line.
  3. Calculate $\sigma_m^{th} = r_{th}\sigma_m$ on the line.
- Circuit model diagram for On-line estimation



Introduction

Preliminaries: Signal Model, Entropy Evaluation, Jitter Estimation

Jitter Estimation with High Accuracy

Jitter Estimation on FPGA

Comparisons and Conclusion

Comparisons

Figure: Comparisons of different methods

Methods	Error Level	Requirement for σ_m	Theoretically confirmed
Ma's in CHES2014	10%	0.92	no
Fischer's in CHES2014	5%	Undefined	no
Ours	1%	0.4141	yes

- Advantages: high accurate, theoretically confirmed error, fast assessment.

Summary and Future Work

- Summary
  - We correct the error in the counter-based methods.
  - The error level of our estimation can be lower than 1%
  - Efficiency is an additional advantage of our method.
- Future work

  Further decrease the requirement for σ_m and estimate it in a shorter interval, in order to reduce the ratio of the flicker jitter in the total jitter. Then the jitter separating approach is no longer necessary

Thanks for your attention!