Generation of True Random Numbers using quasi-Monte Carlo methods

Ana I Gomez, Domingo Gómez-Pérez, Florian Pausinger

Universidad de Cantabria, Queen's University Belfast

MCQMC 2018

Introduction

TRNGs use physical processes to generate random numbers. Some characteristics

- Underlying physical process must be not possible to control
- Principle used to extract entropy and physical phenomenon limits the bit rate

Randomness source available from hardware accelerators (FPGAs, CPDs, ASICs).
Application to embedded security systems (cryptographic system-on-chip).
Methodology AIS 31

Introduction

Challenges in modern embedded TRNG design

i Finding a good quality source of randomness available in the digital technology

ii Finding an efficient and robust principle of randomness extraction

iii Guaranteeing the security (e.g. by a robust design or by an efficient online testing).

Introduction

Mathematical assessment of the security: Lower bound of entropy per output bit

$$H(X) = -p \cdot \log_2(p) - (1-p) \cdot \log_2(p),$$

where X is a random variable and p, bit probability

- Designs based on a stochastic model of the random process.
- If minimal entropy per output bit approaches 1, then the TRNG is an ideal RNG.

TRNG Design

TRNG design by Cherkaoui et al. [1] that exploits the jitter noise of events propagating in a self-timed ring

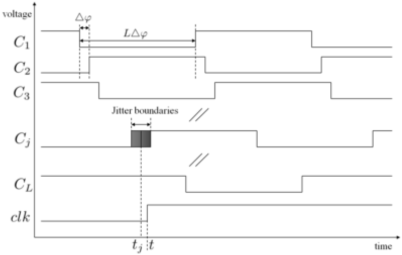
- Self-timed rings are oscillators in which several events can evolve evenly-spaced in time.
- Jitter noise make the significant instants of a digital signal vary from their ideal position in time.

The distance between two events is given by the phase difference

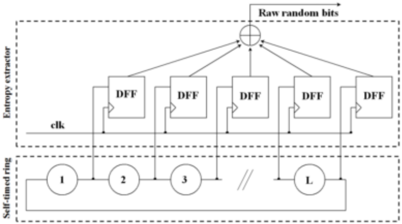
$$\Delta\phi = \frac{T}{2L}$$

where T, oscillation period. L, number of stages of the design.

TRNG Design



voltage
$\Delta\varphi$
$L\Delta\varphi$
C_1
C_2
C_3
Jitter boundaries
C_j
C_L
clk
t_j
t
time



Raw random bits
Entropy extractor
DFF
DFF
DFF
DFF
DFF
clk
Self-timed ring
1
2
3
L

stochastic model

$\{C_i\}_{i=0}^{L-1}$: STR output signals, ordered by its mean time arrival t_i
$\{X_i\}_{i=0}^{L-1}$: random variable represents time position of each event, probability distribution $\mathrm{N}(t_i, \sigma^2)$
For a sampling time t, if $\sigma < \Delta\phi$

$$P[X_j < t] = \Phi(\frac{t - t_j}{\sigma}), P[X_{j-1} < t] = \Phi(\frac{t - t_j - \Delta\phi}{\sigma})$$

Then, the probability that the output bit value at time t is equal to u is the probability of the XOR of the previous value

$$P_u(t) = 1 - \Phi(\frac{t - t_j}{\sigma}) - \Phi(\frac{t - t_j - \Delta\phi}{\sigma}) \\ + 2\Phi(\frac{t - t_j}{\sigma})\Phi(\frac{t - t_j - \Delta\phi}{\sigma})$$

stochastic model

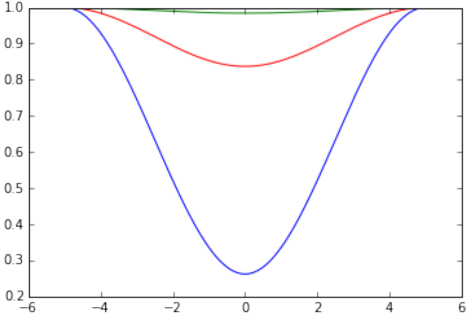


Figure: H versus t. $\sigma = \Delta\phi/4$ (Blue line), $\sigma = \Delta\phi/2$(red line), corresponds to $\sigma = \Delta\phi$(green line)

Non deterministic sampling time (jitter noise), t is the realization of a random variable $Z \sim \mathrm{N}(t_s, \sigma^2_{\mathrm{clk}})$

$$P[X_j < Z] = \int_{-\infty}^{\infty} \Phi(\frac{t' - t_j}{\sigma}) \cdot f_z(\frac{t' - t}{\sigma_{\mathrm{clk}}}) dt'$$

$$P[X_{j-1} < Z] = \int_{-\infty}^{\infty} \Phi(\frac{t' - t_j - \Delta\phi}{\sigma}) \cdot f_z(\frac{t' - t}{\sigma_{\mathrm{clk}}}) dt'$$

$$P_u(t) = 1 - P[X_j < Z] - P[X_{j-1} < Z] + 2 \cdot P[X_{j-1} < Z]\ P[X_j < Z]$$

stochastic model

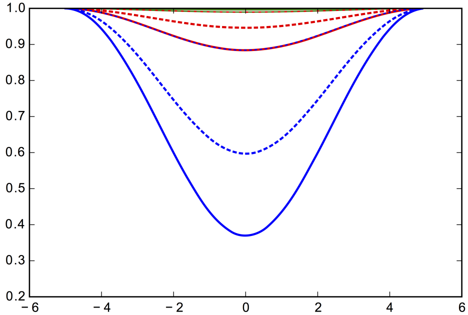


Figure: H versus t. $\sigma = \Delta\phi/4$ (Blue line), $\sigma = \Delta\phi/2$(red line), corresponds to $\sigma = \Delta\phi$(green line). Continous line corresponds to $\sigma_{clk} = \sigma/2$, segmented line to $\sigma_{clk} = \sigma$, and dotted line corresponds to $\sigma_{clk} = 2\sigma$

Results

Minimum entropy when n successive input bits are combined into one output bit for

- Random sampling points
  Example: $\sigma = \frac{\Delta\phi}{4}, H \sim 1$ after 40 bits
- Uniform distributed sampling points
  Example: $\sigma = \frac{\Delta\phi}{4}, H \sim 1$ after 20 bits when $f_{clock} = \frac{36}{125}\Delta\phi$

Open problems

Finding an optimal set of sampling points, regarding:

- Optimal parameters for the underlying digital design
- Several STR with different frequencies

- Cherkaoui, A., Fischer, V., Aubert, A., & Fresquet, L. *A Self-timed Ring Based True Random Number Generator.* In International symposium on advanced research in asynchronous circuits and systems- ASYNC 2013. (99–106), 2013.
- Cherkaoui, A., Fischer, V., Aubert, A., & Fresquet, L. *A Very High Speed True Random Number Generator with Entropy Assesment*. In Cryptographic Hardware and Embedded Systems. CHES 2013. (179–196), 2013.

Thanks for your attention!