A Self-timed Ring based True Random Number Generator with Monitoring and Entropy Assessment

A. Cherkaoui, L. Fesquet, V. Fischer and A. Aubert

Introduction: True Random Numbers Generators (TRNG) rely on physical random processes to generate random bit sequences. Although security is the main requirement in cryptographic applications, to date very few published TRNG designs have been thoroughly evaluated from this point of view. TRNGs used for cryptographic applications with high security requirements (such as key generation for symmetric encryption) not only need to be unpredictable, but they must also be not manipulable. According to AIS31 new evaluation criteria for TRNGs [1], unpredictability is assessed using a stochastic model whereas the robustness to manipulation and active attacks can be guaranteed by monitoring the entropy source and the entropy extractor in order to detect abnormal behaviors of the generator. Online tests can be applied at startup or on demand to detect statistical defects in the output sequences. This demonstration shows how this approach can be applied for an Altera Cyclone III implementation of the recently proposed Self-timed ring based True Random Number Generator (STRNG) [2].

The self-timed ring based true random number generator: By following some simple design rules, a Self-Timed Ring (STR) can provide events which are equidistantly distributed in time with a built-in control of their relative phases [3]. The STRNG architecture and principle are depicted in Fig. 1. The L-stage STR provides L signals \(C_i\), \(1 \leq i \leq L\), having the same period \(T\), a constant phase difference \(\phi\) between them, and distributed over half an oscillation period of the STR output \((L\Delta\phi = \frac{T}{2})\). Each signal \(C_i\) is sampled with the same reference clock \(clk\) using a flip-flop. Therefore, whatever the sampling moment \(t\), there exists \(j\) such as \(t - t_j \leq \frac{T}{2}\), where \(t_j\) is the switching moment of the signal \(C_j\). If the jitter boundaries (e.g. the time interval around a signal edge in which over 99% of jitter variations occur) are larger than the phase difference \(\Delta\phi\), the signal \(C_j\) is sampled in its jitter boundaries as shown in Fig. 1. The obtained sample is then random, and subsequently the output of the XOR tree also.

\[
P(u_{(i)}=0) = 1 - 2\Phi\left(\frac{T}{4L\sigma}\right) + 2\Phi\left(\frac{2T}{4L\sigma}\right)
\]

\[
\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{-\frac{t^2}{2}} dt, \quad x \in \mathbb{R}
\]

A trade-off between the size of the design and its throughput can be obtained using an arithmetic post-processing consisting of a parity filter. An \(n^{th}\) order parity filter can be used to increase the entropy per output bit and remove residual bias, but at the cost of a lower throughput (the bitrate is divided by \(n\)).

Fig. 2 (a) Entropy of an output bit of the STRING as a function of its sampling moment (plotted between -\(\frac{T}{2}\) and \(\frac{T}{2}\)) for \(\Delta\phi = 10\) ps (b) Lower bound of entropy per output bit as a function of the number of STR stages L

Threat model and counter-measures: It has been noted in [5] that the main threat for the STRNG is to modify its internal configuration, i.e. the number of events in the STR, which may have three consequences: 1) changing the oscillation period without modifying the phase distribution (if \(L\) and \(N\) are still co-prime), or 2) changing the phase distribution (if \(L\) and \(N\) are not co-prime), or 3) forcing the STR in an unwanted oscillation mode called the burst mode of the STR [5] by forcing either too many events or too few events in the STR. The second and third possibilities are the worst in terms of security because the STRNG principle does not hold anymore (the uniform phase distribution is not guaranteed). The first case may lead to a (measurable) loss in the entropy per output bit since \(H_m\) decreases when \(T\) increases. To prevent an attacker from taking advantage of one of these flaws, some simple counter-measures can be adopted:

- \(L\) is a prime number (then whatever \(N\), it is co-prime with \(L\))
- A frequency meter measures the STR frequency in order to detect bursting behaviors and important frequency losses, note that this measurement does not require high precision since it is only used for comparison with pre-computed thresholds
- Frequency thresholds are computed based on specific entropy levels and serve to generate appropriate monitors
- A total failure alarm which instantly leads to resetting the STR with the appropriate number of events is generated when bursting behaviors or oscillation stoppage are detected or when the entropy loss is important enough with regards to the associated post-processing

Demonstration: We implemented the proposed design in an Altera Cyclone 3 device. We illustrate the approach for sizing the design, i.e. choosing the STR parameters depending on the measured jitter magnitude (for the technology in which the generator is implemented) in order to achieve a targeted lower bound for the entropy per output bit. We present the statistical testing results for the selected configurations. Afterwards, we show how entropy can be monitored and how the secured design can detect some simple active attacks and produce the appropriate alarms.

References