NEW METHOD OF RANDOMNESS EXTRACTION BASED ON A MODIFIED RING OSCILLATOR FOR CRYPTOGRAPHIC TRNGS EMBEDDED IN FPGAS

Michal Varchola

Department of Electronics and Multimedia Communication,
Technical University of Košice
Park Komeského 13, 04120 Košice, Slovakia
email: michal@varchola.com

1. INTRODUCTION

Random Number Generators (RNGs) play a crucial role in modern cryptographic systems. Random sequences are used as session keys, signature parameters, ephemeral keys, challenges and in zero knowledge protocols in underlying cryptographic algorithms [1] and thus they must fulfill strict statistical properties and should be unpredictable. A RNG of insufficient quality can weaken an otherwise strong cryptographic system.

True RNGs (TRNGs) are preferred for cryptographic applications from a security point of view because they employ a physical phenomena that is not possible to describe in a deterministic way. Furthermore, there is a strong requirement for using a single chip for the entire cryptographic system implementation. Field Programmable Gate Arrays (FPGAs) are a suitable platform for such a task thanks to reconfigurability. However, FPGAs consist of digital circuits designed to operate deterministically. Despite this fact, there still exists a behavior of logic blocks that is supposed to be random.

Employing suitable randomness sources in an FPGA is still a challenging research task which recent papers included in [2] underline. The most popular randomness sources in FPGAs are – jitter caused by time instability of clock signals [3], time delay instability of logic components [4], [5] and analogue properties of the logic gates (metastability) [6].

A new method of randomness extraction is described in this paper. The method uses recently observed behavior of Modified Ring Oscillator (MRO) with an even number of inverting elements. Entropy accumulated using this principle seems to be higher in comparison to jitter of a standard Ring Oscillator (RO). Furthermore, the extraction mechanism can easily detect when the source of randomness is out of order.

This paper is organized as follows: Section 2 proposes the new method of randomness extraction. The results of a preliminary evaluation are described in section 3. The conclusion and future work plans are given in the last section.
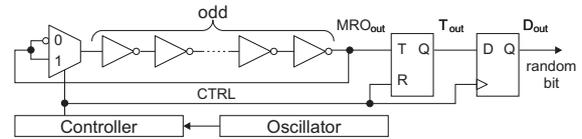

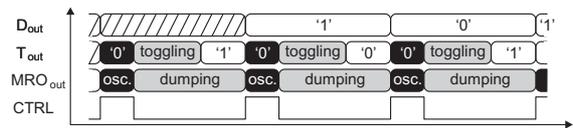
Fig. 1. Block diagram of the new method.

Fig. 2. Timing diagram of the new method.

2. DESCRIPTION OF THE PRINCIPLE

The block diagram of the proposed method is depicted in Fig. 1. Main blocks are – a MRO, that consists of odd number of inverters and multiplexer, a randomness extractor (T-Flip-Flop (TFF) and D-Flip-Flop (DFF)), and a controller.

Timing of the random bit generation is shown in Fig. 2. The controller produces the control signal $CTRL$ derived from the oscillator. $CTRL$ is used for switching between an even or odd number of inverters in the MRO as well as for controlling the extractor ($'1'$ resets TFF) and buffering the output bit (DFF samples T_{out} at the rising edge of $CTRL$).

The random bit is generated as follows. An odd number of the MRO's inverters causes oscillations (oscillatory mode). After a while the MRO is switched into the dumping mode (even number of inverters). Oscillations do not stop immediately in this mode and the excited pulse in the MRO continues to travel around the chain. The length of the $'1'$ period of the pulse is shortened by each loop until the oscillation disappears completely. The number of loops completed differs in each cycle of the $CTRL$ and thus can represent a source of randomness. The TFF resolves number of loops as follows; even $- T_{out} =' 0'$, odd $- T_{out} =' 1'$. The random bit is buffered by the DFF finally.
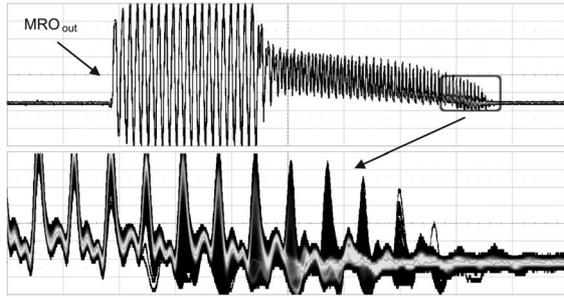
Fig. 3. MRO_{out} of one cycle of $CTRL$ with zoom of the area where the oscillations disappear randomly.
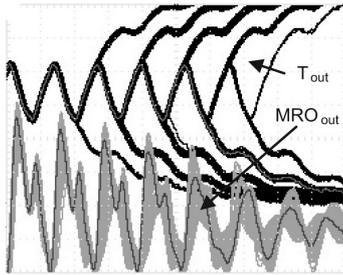

Fig. 4. Resolving disappeared oscillations by the TFF.

3. EXPERIMENTAL RESULTS OF THE PRINCIPLE

The method described above was implemented in the Actel Fusion M7AFS600 FPGA. The MRO was synthesized using components of the Actel Fusion Macro Library and was placed manually in order to have cells as close as possible.

Evaluation was done by a digital storage oscilloscope. Waveforms were captured using infinite persistence display mode in order to record the waveform evolution in previous cycles of the $CTRL$. The frequency of $CTRL$ was $1\,MHz$ and MRO uses 11 inverters. The behavior of the MRO during one cycle (oscillatory and dumping mode) is shown in the upper half of the Fig. 3. The most critical part – oscillations that disappear randomly is shown as a zoom in the bottom half. It is possible to notice a deterministic evolution of signal with slight jitter at the left side of the zoom. The middle part of the zoom shows a randomly disappeared oscillation. Fig. 4 shows output of the TFF (black waveform) that resolves disappearing oscillations in the MRO (gray waveform). There is an indication that the amount of entropy is higher in comparison to entropy of the standard RO jitter. The histogram of an averaged count of random bits that fits the Gaussian distribution is shown in Fig. 5.

During experiments it was observed that the bias depends when the TFF toggles – toggling at the rising edge of the MRO_{out} causes more '0' output bits and vice versa. Temperature influence was tested using freezing spray. Lower temperature causes more oscillations during dumping mode.
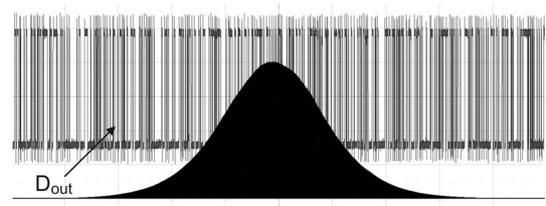

Fig. 5. The histogram of the averaged random bits.

4. CONCLUSION AND FUTURE WORK

A new method of randomness extraction based on an MRO was described in this paper. The main advantage of this method could be higher entropy rate in comparison to a standard RO. The proper operation of a random source is possible to evaluate by simply counting the loops in dumping mode. Whenever the number of loops do not fit in the threshold region, an alarm can be issued.

Future work involves deeper research on the reason why the oscillations disappear randomly and employing the described principle in the reliable TRNG. Design structure will be improved in order to reduce the bias and the dependence on operating conditions and to increase the throughput by shortening excitation of the pulse. The generated random sequence will be evaluated by statistical tests and the next step would be formulation of the stochastic model. The principle will be evaluated in various FPGA families as well.

5. REFERENCES

[1] W. Schindler, *Cryptographic Engineering.* Springer, 2009, ch. Random Number Generators for Cryptographic Applications, pp. 5–23, iSBN: 978-0-387-71816-3.

[2] B. Sunar, *Cryptographic Engineering.* Springer, 2009, ch. True Random Number Generators for Cryptography, pp. 55–73, iSBN: 978-0-387-71816-3.

[3] V. Fischer and M. Drutarovský, "True random number generator embedded in reconfigurable hardware," in *Cryptographic Hardware and Embedded Systems - CHES 2002, Redwood Shores, CA, USA, August 13-15, 2002, Revised Papers*, ser. LNCS, vol. 2523. Springer, 2002, pp. 415–430.

[4] B. Sunar, W. J. Martin, and D. R. Stinson, "A provably secure true random number generator with built-in tolerance to active attacks," *IEEE Transactions on Computers*, vol. 56, no. 1, pp. 109–119, January 2007.

[5] V. Fischer, F. Bernard, N. Bochard, and M. Varchola, "Enhancing security of ring oscillator-based rng implemented in fpga," in *Field-Programable Logic and Applications (FPL)*, September 2008, pp. 245–250.

[6] I. Vasyltsov, E. Hambardzumyan, Y. S. Kim, and B. Karpinskyy, "Fast digital trng based on metastable ring oscillator," in *Cryptographic Hardware and Embedded Systems - CHES 2008, Washington, DC, USA, August 10-13, 2008, Proceedings*, ser. LNCS, vol. 5154. Springer, 2008, pp. 164–180.