FPGA Cryptographic Primitive with Integrated PUF and TRNG Capability
Milos Drutarovsky and Michal Varchola, Technical University of Kosice, Slovakia

Abstract
The paper presents a new hardware element that can be used for simultaneous generation of random bits and PUF responses. The proposed structure is highly scalable and it can be easily implemented in FPGAs. Its performance and robustness is demonstrated on a cluster of elements implemented in Actel Fusion FPGA.

1. Introduction and Motivation
There are two distinct cryptographic primitives that extract randomness from hardware they are running on. The first one, the True Random Number Generator (TRNG) produces random values that are utilized in cryptographic algorithms. The second primitive, the Physical Unclonable Function (PUF) is a promising building block targeted for embedded security applications. PUF physical structures use unavoidable random variations in silicon manufacturing processes for identification of Integrated Circuits (ICs) or for generation of unique keys related to the target IC.

Ring Oscillators (ROs) are quite popular building blocks in TRNG as well as PUF designs. Standard ROs have significant dependency on power supply voltage and temperature that we have to take into account in particular design. Process variations in modern submicron technologies affect the ability of RO based PUFs (RO-PUFs) to extract unique chip-signatures from ROs located far away inside the device. Robust RO-PUFs extraction strategy requires comparison of only closely located ROs. Another problem demonstrated e.g. in [MSE10] for Xilinx FPGA indicates strong influence of surrounding logic on average frequencies of ROs used as building blocks of RO-PUFs.

Mutual locking of closely located ROs can cause serious problems in RO based TRNG (RO-TRNG) designs, especially when we use differential structures using closely placed identical ROs. Note that this is the case especially when designers try to minimize the influence of global processes that can be easily manipulated (e.g. by introducing a periodic signal to the power supply). However, these closely placed ROs can tend to lock and reduce significantly the TRNG entropy.

Some authors try to share classical ROs resources in integrated RO-PUF/RO-TRNG element. Due to above mentioned limitations of ROs, we believe that some other circuit structures should be used in security critical cryptographic applications when designing integrated PUF/TRNG block.

2. New Primitive based on Transient Effect Ring Oscillator Architecture
The architecture of proposed primitive and its principle is presented in Fig.1. It is based on Transition Effect Ring Oscillator (TERO) structure that was originally proposed for TRNG designs [VD10] and we call it Universal TERO (UTERO) element. The UTERO consists of a TERO loop and a PUF/TRNG bit extraction logic. Fig.1 shows compact extraction logic we can use in daisy chain configuration of several UTERO elements. We can use faster and larger parallel extraction logic when extraction speed is preferred.

The TERO loop uses two AND gates and two inverters. The UTERO operates as follows: When ctrl = ‘0’, the TERO loop is in reset state and no oscillations occur. The rising edge of the ctrl signal (the loop stimulation signal) causes transition oscillations in the loop if the next two conditions are fulfilled [Kac88]: the circuit should have a positive feedback and the RC time constant (defined by parasitic resistance and capacity) should be smaller than the total delay of all logic elements involved in the loop. In theory, oscillations never stop if the loop is ideally symmetrical. However, the circuit usually oscillates just for a short time and oscillations disappear after a while due to intrinsic asymmetry Td defined in [VD10] for TERO structure. This behavior is commonly named the oscillatory metastability [Kac88]. The Td factor represents the time difference between time delays of both halves of the loop. The average size Td of a well balanced TERO loop is comparable with random contributions to Td, which originate in a semiconductor intrinsic noise. This way, the number of oscillations is significantly affected by the random circuit noise, so the number of oscillations varies at the end of subsequent stimulation intervals. On the other hand, global perturbations (e.g. from the power supply) do not affect significantly the parameter Td because of the “differential” behavior of the loop. The random bit value can thus be defined as follows: an even number of generated half periods yields to random bit equal to ‘0’ and odd number yields to ‘1’. Unlike the structure in [VD10] that uses XOR and AND gates for controlling the loop, proposed architecture utilizes AND gates and inverters for stimulation of the oscillatory metastable state. This modification simplifies the UTERO control mechanism.

The TERO loop resembles a bi-stable butterfly PUF element presented in [KGM08]. The process, when both structures are resolving from transitional state is the same as it is the case in the bi-stable butterfly element: the output of the TERO loop falls to ‘0’ or ‘1’ final state depending on variations in manufacturing process. The principal difference between the two structures is that the TERO loop has a longer delay...
causing oscillatory metastable behavior that was described above. In order to reduce the bias of the PUF response, the authors in [KGM08] recommended keeping the loop as symmetric as possible. We believe that thanks to more logic elements involved in the TERO loop, the designer can better adjust the bias: he can do it iteratively and in small steps by a manual placement and routing.

The main advantage of the proposed UTERO structure is that it can be used for simultaneous generation of random bits and PUF responses. The PUF response bit corresponds to the output value of the TERO loop that converges to a state determined by the manufacturing process (signal A in Fig.1). The random bit is obtained by counting the number of oscillations and by taking the least significant bit of the counter (signal B in Fig.1). Despite the fact that the two output signals are generated in the same hardware (the TERO loop), they are mutually independent and the user can obtain four possible combinations at the end of the oscillatory state. Fig.1 shows that oscillations in signal A can converge to logic levels ‘1’ or ‘0’ due to randomness in the manufacturing process. The final value of signal B depends on the number of oscillations determined by the noise in logic gates involved in the TERO loop.

![Fig.1 UTERO element based on a four-element TERO loop giving simultaneously the PUF (signal A) and TRNG (signal B) output and a serial PUF/TRNG extraction logic.](attachment:image)

The PUF/TRNG bit extraction logic is also presented in Fig.1. The T flip-flop (implemented by D flip-flop with the feedback) in the bottom left corner of the extraction logic indicates at the end of the stimulation phase, whether the TERO loop generated odd or even number of oscillations. This signal is used as a TRNG output bit. It is cleared periodically after the TERO loop stimulation intervals in order to keep the TRNG output state-less. The UTERO element has a single output that can be used as a PUF or TRNG output. In order to get both PUF and TRNG outputs after each stimulation period, some additional logic would be necessary. We used the structure with multiplexed output in order to minimize the logic resources in the complete UTERO cluster (the set of UTERO elements). The output (PUF or TRNG) is selected using multiplexer MUX1 controlled by the trng/puf control signal. The D flip-flop in the bottom right corner serves for registering PUF/TRNG output and for shifting the result serially out from the UTERO cluster using the shift/load control signal and multiplexer MUX2. The clocking of this shift register flip-flop is enabled by the control signal dena. One UTERO cluster is composed of \( N \) UTERO elements. The bits generated in the cluster are output serially. This way, only local interconnections are needed between UTERO elements, so the routing is very simple.

3. The UTERO Evaluation Platform, Design and Testing Issues
We performed experiments on complete UTERO-based PUF/TRNG generators using Actel Fusion FPGA technology as we had 10 identical Actel evaluation boards available. We want to point out, that manual placement and routing is mostly necessary when implementing the UTERO element in FPGAs. For this reason, we implemented several versions of TERO structures, while changing iteratively topologies of UTERO elements (each element had the same topology in one iteration) until we got satisfactory PUF features (in particular a convenient bias of PUF bits).

The FPGA fabric of the used Actel M1AFS600 FPGA device consists of 24 building blocks. Each block is composed of a matrix of 16 x 36 logic elements (tiles). Each tile can be configured as a 3-input combinatorial logic function or as a flip-flop. Thus we needed 8 tiles per one UTERO element. Consequently, we could fit 72 UTERO elements in a single block. We decided to assign 3 complete blocks
for \( N = 216 \) UTERO elements to provide enough raw PUF bits, when PUF response should be used as a confidential key. This way, we got 216 PUF bits or 216 raw TRNG bits after each stimulation period. We selected XOR of \( M=18 \) raw TRNG bits for getting one output TRNG bit in order to provide robust and high quality TRNG output. When \( N = 216 \) and \( M = 18 \), 12 random bits per stimulation period can be obtained from all UTERO channels. The UTERO cluster occupies 1/8 of the selected FPGA fabric and it can thus be placed at eight different non-overlapping positions \( PL = 1, 2, \ldots, 8 \). The FPGA design with a highlighted UTERO cluster and \( PL = 7 \) is shown in Fig.2.

The block diagram of our UTERO evaluation platform is shown in Fig.3. It consists of Actel Fusion FPGA and Cypress USB interface controller. The FPGA design includes the cluster composed of \( N = 216 \) UTERO elements, control Finite State Machine (FSM), Cypress controller interface and AES engine. Each UTERO element in the cluster has the same topology.

**Fig.2** Placement \( PL = 7 \) of the entire design and detail of the UTERO element inside Actel Fusion FPGA. The highlighted UTERO cluster is placed in the right-top quarter of the device. The remaining logic elements represent AES core, control FSM and the USB interface. The zoomed region in top left corner represents single UTERO element layout.

**Fig.3** Evaluation platform containing the cluster of \( N = 216 \) UTERO elements, control FSM and Cypress USB controller interface and AES cipher

### 6. Experimental Results and Preliminary Conclusions

We performed majority of our PUF related measurements of UTERO elements with 10 available boards and 8 different placements \( PL = 1, 2, \ldots, 8 \) per board, in room ambient temperature (\( Ta = 24^\circ C \)) and nominal \( V_{core} = 1.5V \). In order to test the PUF performance in extreme conditions, we tested two selected boards out of recommended voltage and temperature ranges (\( V_{core} < 1.425V \) and \( > 1.575 V \), \( Ta < 0^\circ C \) and \( > 85^\circ C \)). All measurements in extreme conditions were done with AES core running, in order to provide as realistic worst case operating conditions as possible. Preliminary results indicate the proposed new hardware block fulfills requirements for the integrated PUF/TRNG generator and that it has many advantages when compared to the classical RO-based designs: it has low sensitivity to global perturbations and in the same time, the changing operating conditions do not affect its performance significantly. The proposed structure is scalable since UTERO elements are independent, many of them can run in parallel in both TRNG and PUF modes. The average inter-die Hamming distance is close to 50% what ensures the uniqueness of PUF responses in different devices. In order to obtain satisfactory results, manual placement of the TERO loop gates is necessary for guaranteeing the symmetry of the two half-loops. This optimization of the TERO loop topology is necessary only once per device family and all the loops remain the same inside the device. We showed that the UTERO cluster composed of 216 UTERO elements can generate over 75% stable PUF response bits and 900 random kbits per second in the TRNG mode of operation. The generated random bit sequences satisfied requirements for both FIPS and NIST tests.

### References:

[ACT09] Actel Fusion Family of Mixed Signal FPGAs, datasheet Rev. 1, Actel Corporation, July 2009  