ReSecu_4_AmBRAMs

TOWARDS INCREASED RELIABILITY AND HARDWARE SECURITY ON MODERN NANOSCALE FPGAS

Contact: **Petr Pfeifer** *(petr.pfeifer@tul.cz)*

Institute of Information Technology and Electronics (ITE, FM), Technical University of Liberec, Czech Republic and BTU Cottbus-Senftenberg, Germany

*M*otivation – Wide portfolio of **new technologies** in design and manufacturing of advanced integrated circuits enables **higher integration of complex structures** at **ultra-high nanoscale densities**, but also sensitivity to various changes of the internal nanostructures and their parameters, resulting in the requirement of advanced measurements and complex **reliability assessments**.

ReSecu4AmBRAMs is a set of tools and methods based on AmBRAMs lab-on-chip platform and focused on safety and security of modern systems.

✓ **Internal parameter measurements in FPGAs**
✓ Device and **platform identification**
✓ Identification of **crosstalk** path and **mutual impacts**
✓ **Identification of changes** in internal parameters
✓ **Parameter-aware placement**
✓ … and much more !

The principle and utilization of BRAMS
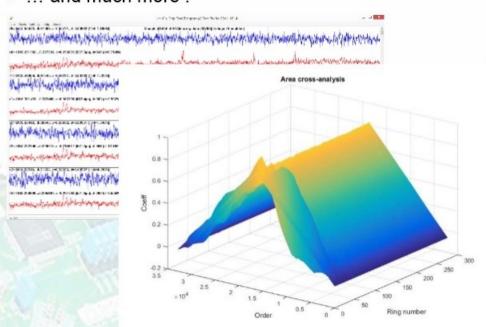

Area cross-analysis

AmBRAMs is new method and developed advanced Analysis Tool and Framework for Advanced Measurements and Reliability Assessments on Modern Nanoscale FPGAs creates revolutionary new set of tools enables complex lab-on-chip solutions in nanoscale FPGAs. The key method is based on the basic principle of on-chip parameter measurements utilizing programmable structures. Available FPGA blocks are configured into multiple oscillators across the chip and the resulting data streams are sampled in the synchronous memory blocks as a new way of using block memory (BRAM) blocks.
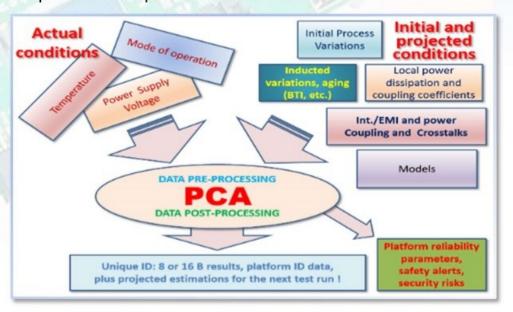
It will be presented on VLIW soft processor cores equipped with a security IP, and also showing POF solutions and related functionality. Detection of power voltage variation using AmBRAMs technology is incorporated in the processor application and demonstrating it on a complex processor system. Presented on 28nm LP or 20nm HP UltraScale Xilinx FPGA devices. Widely used 28nm FPGA solution will also show simple HW adjustments enabling support of power supply change required the demonstrator and for adaptive control presented as well.

AmBRAMs has been enhanced of advanced measurements and data processing supporting platform identification and security support functionality including tampering detection preferably in modern nanoscale programmable devices.

Available for FPGAs from 90 nm down to 20 nm technologies.

References

[1] PFEIFER, P., KACZER, B., PLIVA, Z.: A Reliability Lab-on-chip Using Programmable Arrays, 52nd IEEE International Reliability Physics Symposium, Hawaii, USA, 2014, DOI: 10.1109/IRPS.2014.6861123

[2] PFEIFER, P.: Towards Increased Reliability and Hardware Security using Advanced Measurements and Data Processing on Modern Nanoscale FPGAs, Joint MEDIAN&TRUDEVICE Open Forum, 30 September 2014, Amsterdam, The Netherlands