Kris Gaj, Jens-Peter Kaps, Venkata Amirineni, Marcin Rogawski, Ekawat Homsirikamol, Benjamin Y. Brewster, John Pham, and Michal Varchola

ATHENa – Automated Tool for Hardware EvaluatioN: Toward Fair and Comprehensive Benchmarking of Cryptographic Hardware using FPGAs

A fair and comprehensive benchmarking of cryptographic hardware is a challenging and time consuming task, plagued by evaluation pitfalls and objective difficulties. Some examples of evaluation pitfalls include taking credit for improvements in technology, choosing a convenient (but not necessarily fair) performance measure, comparing designs with either different functionality or developed using a different optimization target. Objective difficulties are even more challenging to overcome, and include lack of standard interfaces, influence of tools and their options, differences between a stand-alone performance vs. performance as a part of a bigger system, and the dependence of the obtained results on the time spent for optimization.

During CryptArchi 2009, the GMU team has announced its plans for the creation of an open-source benchmarking environment called ATHENa – Automated Tool for Hardware EvaluatioN, aimed at an automated generation of optimized results for multiple FPGA families from different vendors. At this point, we are pleased to report that ATHENca is one year old, and growing fast :-).

The environment supports majority of FPGA families from two major vendors (Xilinx and Altera), it automatically selects the best device within a given family, and runs the entire verification, synthesis, and implementation process in batch mode. It implements several heuristic algorithms for design space exploration, including exhaustive search, placement search, and batch elimination. Some of the most recent features include new enhanced ATHENa setup, support for multi-core processing, automated verification of designs through simulation runs in batch mode, enhanced error and progress reports, etc.

The tool can be employed to perform four major types of comparisons, the comparison of cryptographic algorithms (e.g. candidates in the SHA-3 contest), cryptographic architectures and implementations (e.g., basic iterative vs. unrolled), hardware platforms (e.g. Xilinx Virtex 5 vs. Altera Stratix III), and languages and tools (e.g., VHDL vs. Verilog or Synplify Pro vs. Xilinx XST). In this talk we will describe the application of our tool to the comparison of 14 Round 2 SHA-3 candidates, and present several other case studies illustrating the benefits and challenges of using ATHENa to optimize and compare cryptographic hardware.

The tool is accompanied by a comprehensive web site (available at http://cryptography.gmu.edu/athena) serving as a focal point of the project, which is planned to contain the repository of project scripts and sample configuration files, specifications of the proposed uniform interfaces for the most common cryptographic transformations, comprehensive testbenches and test vectors, reference software implementations, open source HDL codes, case studies, and interactive tables of results (with the support for searching, filtering, and ranking of database entries).