ATHENa 2.0 and ATHENa Database of Results

Kris Gaj, Jens-Peter Kaps, Benjamin Y. Brewster, John Pham,
Ekawat Homsirikamol, and Rajesh Velegalati
George Mason University

Abstract

Benchmarking of cryptographic modules targeting FPGAs is a time intensive and challenging process. Benchmarking results depend on a myriad of variables beyond the properties inherent to the designs being evaluated, encompassing the tools, tool options, FPGA families, and languages used.

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. Since then, ATHENa has been constantly upgraded with new features, and has been adopted by several cryptographic engineering groups from all over the world.

In this talk, we will discuss our plans and experiments leading to a major overhaul of ATHENa, and the creation of its extended and improved version, we refer to as ATHENa 2.0. The major enhancements made to ATHENa include support for distributed computing based on the Condor job management system, new efficient option space exploration strategies, and graphical user interface for preparing, submitting, and monitoring ATHENa jobs. Additionally, the new and enhanced ATHENa is developed in Python (instead of Perl, used in the first version) and follows object oriented design principles, which facilitates maintenance of the program. Capabilities of the new environment have been demonstrated using GMU designs for five SHA-3 finalists: BLAKE, Groestl, JH, Keccak and Skein.

The tool is closely integrated with the GMU ATHENa database of results, available at http://cryptography.gmu.edu/athenadb. This database contains currently over 1300 results for FPGA and ASIC implementations of modern hash functions, with the special focus on Round 2 and Round 3 SHA-3 candidates. The database provides an easy-to-use graphical user interface for searching, filtering, and ranking of database entries. Majority of GMU results contain links to the corresponding source codes, publications, and replication scripts, which allow reproducibility of results, without the need of using ATHENa. All GMU source codes are also accompanied by the corresponding block diagrams.

ATHENa database is now open for submissions by other groups, and the graphical summary of results for five SHA-3 candidates collected using such submissions will be presented at the workshop. In the near future, ATHENa database will be also enhanced to allow submissions and presentation of results for secret-key ciphers, public key cryptosystems, and identity based cryptosystems.