Marcin Rogawski, Ekawat Homsirikamol, and Kris Gaj

SHA-3 Competition in Hardware - Methodology, Tools, and Results of Comparing Fourteen Round 2 SHA-3 Candidates using Reconfigurable Hardware

The SHA-3 Contest for the new standard in the area of cryptographic hash functions is currently in its Second Round, with 37 candidates already eliminated, and only 14 candidates left in the competition. So far, no serious cryptanalytic attack has been reported against any of the Round 2 candidates, which means that their security may be judged as adequate, similarly to the case of the final five AES candidates in 1999-2000. As history tells, performance in hardware and software becomes the next most important factor distinguishing remaining candidates, and may be a decisive factor in choosing finalists and eventually a winner of the SHA-3 competition.

In this talk, we will describe the status of our project on developing fair and comprehensive methodology and tools for comparing SHA-3 candidates using reconfigurable hardware. The highlights of our methodology include the definition of clear performance metrics, a uniform hardware interface for all SHA-3 candidates, clear optimization target, uniform design process, comprehensive verification, benchmarking and optimization method, and the way of presenting and comparing results facilitating the final decision process.

All 14 candidates have been designed and modeled in VHDL with the focus on uniformity and the code reuse. Each candidate has been implemented in at least three basic variants: with a 256-bit output, 512-bit output, and all-in-one, where the output size is selected at run-time. The throughput to area ratio was selected as the primary optimization target, and was shown to drive the development process, starting from the choice of a high-level architecture, through the implementation of basic operations, down to the choice of tools and tool options. All designs have been comprehensively benchmarked using multiple families of FPGAs from two major vendors, Xilinx and Altera, and the results normalized using the best known implementations of the current standard SHA-2 with equivalent security.

The results point to relatively large differences among all candidates, and the possibility of dividing all algorithms into several groups with comparable performance characteristics. Majority of candidates outperform the SHA-2 functions in terms of the throughput, but are more demanding in terms of the area. As a result, depending on a particular FPGA family and a hash function variant, only one to four SHA-3 candidates outperform SHA-2 in terms of the throughput to area ratio.