From C to Hardware: Toward Using High-Level Synthesis for Hardware Benchmarking of Candidates in Cryptographic Contests

ECE Ph.D. Seminar
by
Ekawat Homsirikamol

Committee Members:
Dr. Kris Gaj (Director)
Dr. Jens Peter-Kaps
Dr. Angelos Stavrou
Dr. Bernd-Peter Paris

Friday, September 9th, 2016
1:30-2:30 PM

ENGR 2901

Abstract

The growing number of candidates competing in the cryptographic contests, such as CAESAR, makes the hardware performance evaluation extremely time consuming, tedious, and imprecise, especially at the early stages of the competitions. The main difficulties include the long time necessary to develop and verify Register-Transfer Level (RTL), hardware description language code of all candidates, and the need of developing (or at least tweaking) code for multiple variants and architectures of each algorithm. High-Level Synthesis (HLS), based on the newly developed Xilinx Vivado HLS tool, offers a potential solution to the aforementioned problems.

In order to verify a potential validity of this approach, we have first applied both the traditional RTL methodology and the newly proposed HLS-based methodology to the current NIST standard in the area of symmetric block ciphers, AES. The same methodologies have been further applied to compare the rankings of candidates in Round 3 of the SHA-3 contest for a new cryptographic hash function standard, and selected candidates in Round 2 of the CAESAR competition for a new portfolio of modern authenticated ciphers. Our studies have demonstrated a high correlation between the rankings of the evaluated algorithms, obtained using both investigated methodologies. In particular, after applying HLS, the algorithm rankings in terms of the three major performance metrics - throughput, area, and throughput to area ratio - have either remained unchanged or have been affected only for algorithms with the very similar RTL performance. At the same time, a substantial speed-up in terms of the development time has been achieved.