Efficient modular squaring in binary fields on CPU supporting AVX and GPU

Paweł Augustynowicz, Andrzej Paszkiewicz
Faculty of Cybernetics
Military University of Technology
Warsaw, Poland
{pawel.augustynowicz,andrzej.paszkiewicz}@wat.edu.pl

This paper deals with the acceleration of modular squaring operation in binary fields on both modern CPUs and GPUs. The key idea is based on applying bit-slicing methodology with a view to maximizing the advantage of *Single Instruction Multiple Data* (SIMD) and *Single Instruction Multiple Threads* (SIMT) execution patterns. The developed implementation of modular squaring was adjusted to testing for the irreducibility of binary polynomials of some particular forms.

Keywords: GPU, SIMD, Parallel Algorithms.