@INPROCEEDINGS{1568517,
author={Juliato, M. and Araujo, G. and Lopez, J. and Dahab, R.},
journal={IEEE International Conference on Field-Programmable Technology},
title={A custom instruction approach for hardware and software implementations of finite field arithmetic over F2163 using Gaussian normal bases},
year={2005},
month={dec.},
volume={},
number={},
pages={ 5 - 12},
abstract={In this paper we explore the potential use of custom instructions in a reconfigurable hardware platform to accelerate arithmetic operations in the binary field F2163 using a Gaussian normal basis representation. System-on-chip (SOC) techniques based on field programmable gate arrays (FPGAs) are used, making it possible to run real applications on the system while considering all execution overheads. Thus we are able to fairly compare hardware and software performances, as well as precisely determine their speedups. Using this approach, we show that a field multiplication can be accelerated over 2619 times when implemented in hardware. Moreover, using this fast field multiplier in a hardware/software approach, we accelerate point multiplication, the fundamental operation of ECC, over 116 times.},
keywords={ Gaussian normal basis representation; binary field; field programmable gate array; finite field arithmetic; hardware implementation; reconfigurable hardware platform; software implementation; system-on-chip; Gaussian processes; digital arithmetic; field programmable gate arrays; logic design; reconfigurable architectures; system-on-chip;},
doi={10.1109/FPT.2005.1568517},
ISSN={},}