Efficient FPGA-based ECDSA Verification Engine for Permissioned Blockchains

Rashmi Agrawal, *Boston University*
Ji Yang, Haris Javaid, *Xilinx*
Contact: rashmi23@bu.edu

Permissioned blockchain platforms heavily depend on cryptography to provide a layer of trust within the blockchain network, thus verification of cryptographic signatures often becomes the bottleneck. ECDSA is the most commonly used cryptographic scheme in permissioned blockchains. In this work, we propose an efficient implementation of ECDSA signature verification on FPGA, in order to improve performance of permissioned blockchains that aim to use FPGA-based hardware accelerators. We propose several optimizations for modular arithmetic (e.g., custom multipliers and fast modular reduction) and point arithmetic (e.g., reduced number of point double and addition operations, and optimal width NAF representation). Based on these optimized modular and point arithmetic modules, we propose an ECDSA verification engine that can be used by any application for fast verification of signatures. We further optimize our ECDSA verification engine for Hyperledger Fabric (one of the most widely used blockchain platforms) by moving carefully selected operations to a precomputation block, thus simplifying the critical path of ECDSA signature verification. Our ECDSA engine running at 250MHz on Xilinx Alveo U250 accelerator card can perform a verification in 760 microseconds with a throughput of 1,315 verifications/second, which is ~2.5 times faster than state-of-the-art FPGA-based implementations. Our Hyperledger Fabric-specific ECDSA engine can perform a verification in 368 microseconds, and 2,717 verifications/second. With 10 engines, Hyperledger Fabric can achieve a throughput of 7,520 transactions/second.

Keywords: ECDSA signature verification, FPGA, Hyperledger Fabric

DOI: https://doi.org/10.1145/3490422.3502333