ABSTRACT

Cryptography and implement the module lattice-based post-quantum key encapsulation mechanism (KEM) Saber as a case study. To achieve fast computation time, the architecture is fully implemented in hardware, including CCA transformations. Since polynomial multiplication plays a performance-critical role in the module and ideal lattice-based public-key cryptography, parallel polynomial multiplier architecture is proposed that overcomes memory access bottlenecks and results in a highly parallel yet simple and easy-to-scale design. Such multipliers can compute a full multiplication in 256 cycles, but are designed to target any area/performance trade-offs. Besides optimizing polynomial multiplication, we make important design decisions and perform architectural optimizations to reduce the overall cycle counts as well as improve resource utilization. In this paper we present the design and evaluation of a scalable low-area FPGA hardware architecture that serves as a building block to accelerate the costly operations of exponentiation and multiplication in , commonly required in security protocols relying on public key encryption, such as in key agreement, authentication and digital signature. The proposed design can process operands of different size using the same datapath, which exhibits a significant reduction in area without loss of efficiency if compared to representative state of the art designs