Authenticated ciphers offer potential benefits to the Internet of Things (IoT) devices. The CAESAR competition sought optimal authenticated ciphers based on several criteria, including performance in resource-constrained environments. In this study, we developed true lightweight implementations of five Round 3 CAESAR candidates: ACORN, CLOC-AES, NORX, SILC AES(563,541),(593,575), and SILCLED. We extended the implementation of ACORN with countermeasures against side-channel attacks. We compared two SCA-protected, FPGA-based realizations of ACORN with the designs for the current standard, AES-GCM, equivalent in terms of the area and throughput, respectively. We then adapted one of these implementations to the use in a novel key management scheme for hardware security based on logic locking and obfuscation. In the second part of this study, the goal was to set the foundation for the early, systematic, and comprehensive study of the hardware efficiency of the most promising Post-Quantum Cryptography (PQC) public-key ciphers. In particular, we developed a high-speed, constant-time, full hardware implementation of NTRUEncrypt Short Vector Encryption Scheme (SVES) (fully compliant with the corresponding IEEE standard), and two leading Round 2 candidates in the NIST PQC standardization effort - NewHope, and Kyber. We also investigated the potential for speeding up implementations of the NTRU-based Key Encapsulation Mechanisms (KEMs), using software/hardware codesign, and developed a special benchmarking platform based on Xilinx Zynq UltraScale+ multiprocessor system-on-chip. The developed PQC implementations can be combined with high-speed implementations of secret-key authenticated ciphers to provide robust long-term protection of information in cloud computing and other high-performance applications.