World Academy of Science, Engineering and Technology
International Journal of Computer and Systems Engineering
Vol:18, No:02, 2024

Design and Implementation of a Hardened Cryptographic Coprocessor with 128-bit RISC-V Core

Authors : Yashas Bedre Raghavendra, Pim Vullers

Abstract : This study presents the design and implementation of an abstract cryptographic coprocessor, leveraging AMBA(Advanced Microcontroller Bus Architecture) protocols - APB (Advanced Peripheral Bus) and AHB (Advanced High-performance Bus), to enable seamless integration with the main CPU(Central processing unit) and enhance the coprocessor's algorithm flexibility. The primary objective is to create a versatile coprocessor that can execute various cryptographic algorithms, including ECC(Elliptic-curve cryptography), RSA(Rivest–Shamir–Adleman), and AES (Advanced Encryption Standard) while providing a robust and secure solution for modern secure embedded systems. To achieve this goal, the coprocessor is equipped with a tightly coupled memory (TCM) for rapid data access during cryptographic operations. The TCM is placed within the coprocessor, ensuring quick retrieval of critical data and optimizing overall performance. Additionally, the program memory is positioned outside the coprocessor, allowing for easy updates and reconfiguration, which enhances adaptability to future algorithm implementations. Direct links are employed instead of DMA(Direct memory access) for data transfer, ensuring faster communication and reducing complexity. The AMBA-based communication architecture facilitates seamless interaction between the coprocessor and the main CPU, streamlining data flow and ensuring efficient utilization of system resources. The abstract nature of the coprocessor allows for easy integration of new cryptographic algorithms in the future. As the security landscape continues to evolve, the coprocessor can adapt and incorporate emerging algorithms, making it a future-proof solution for cryptographic processing. Furthermore, this study explores the addition of custom instructions into RISC-V ISE (Instruction Set Extension) to enhance cryptographic operations. By incorporating custom instructions specifically tailored for cryptographic algorithms, the coprocessor achieves higher efficiency and reduced cycles per instruction (CPI) compared to traditional instruction sets. The adoption of RISC-V 128-bit architecture significantly reduces the total number of instructions required for complex cryptographic tasks, leading to faster execution times and improved overall performance. Comparisons are made with 32-bit and 64-bit architectures, highlighting the advantages of the 128-bit architecture in terms of reduced instruction count and CPI. In conclusion, the abstract cryptographic coprocessor presented in this study offers significant advantages in terms of algorithm flexibility, security, and integration with the main CPU. By leveraging AMBA protocols and employing direct links for data transfer, the coprocessor achieves high-performance cryptographic operations without compromising system efficiency. With its TCM and external program memory, the coprocessor is capable of securely executing a wide range of cryptographic algorithms. This versatility and adaptability, coupled with the benefits of custom instructions and the 128-bit architecture, make it an invaluable asset for secure embedded systems, meeting the demands of modern cryptographic applications.

Keywords : abstract cryptographic coprocessor, AMBA protocols, ECC, RSA, AES, tightly coupled memory, secure embedded systems, RISC-V ISE, custom instructions, instruction count, cycles per instruction
Conference Title : ICCEM 2024 : International Conference on Computers and Embedded Microprocessors
Conference Location : Tokyo, Japan
Conference Dates : February 26-27, 2024