INTISARI

Elliptic Curve Digital Signature Algorithm (ECDSA) adalah algoritma kriptografi yang menjamin autentikasi dan integritas data pada sistem komunikasi modern seperti IoT dan *Collaborative Robot*. Namun, implementasi perangkat lunak ECDSA sering kali mengalami latensi tinggi akibat beban komputasi hashing. Penelitian ini mengusulkan sebuah Hardware Signature Authenticator (HSA) berbasis FPGA yang menerapkan arsitektur hardware-software co-design dengan mengintegrasikan SHA-256 Engine sebagai akselerator perangkat keras pada Programmable Logic (PL) dan algoritma ECDSA pada Processing System (PS) yang menjalankan PetaLinux. Implementasi dilakukan pada platform Zynq UltraScale+ MPSoC menggunakan Verilog untuk perangkat keras dan C++ untuk perangkat lunak. Hasil pengujian menunjukkan bahwa sistem mampu menghasilkan hash yang 100% sesuai dengan standar NIST, mencapai throughput stabil 1071 Mb/s, serta mempercepat pemrosesan data 1,5 GB hingga lebih dari 50 kali lipat dibandingkan implementasi perangkat lunak murni. Penggunaan sumber daya FPGA efisien dengan konsumsi daya hanya meningkat 0,13 Watt saat operasi hashing intensif. Sistem ini menjawab kebutuhan autentikasi data berkecepatan tinggi dan hemat daya pada lingkungan sumber daya terbatas.

Kata kunci : FPGA, *Hardware Signature Authenticator*, ECDSA, *SHA-256 Engine*, Akselerasi Perangkat Keras.

ABSTRACT

The Elliptic Curve Digital Signature Algorithm (ECDSA) is a cryptographic algorithm that ensures data authentication and integrity in modern communication systems such as IoT and collaborative robotics. However, software-based ECDSA implementations often suffer from high latency due to intensive hashing computations. This study proposes an FPGA-based Hardware Signature Authenticator (HSA) employing a hardware-software co-design architecture that integrates a SHA-256 Engine as a hardware accelerator in the Programmable Logic (PL) and the ECDSA algorithm in the Processing System (PS) running PetaLinux. The system was implemented on a Zynq UltraScale+ MPSoC platform using Verilog for hardware and C++ for software. Test results show that the system produces hash outputs 100% compliant with NIST standards, achieves a stable throughput of 1071 Mb/s, and accelerates the processing of 1.5 GB of data by over 50 times compared to a pure software implementation. FPGA resource utilization is efficient, with power consumption increasing only by 0.13 Watts during intensive hashing operations. This system addresses the need for high-speed, low-power data authentication in resource-constrained environments.

Keywords : FPGA, Hardware Signature Authenticator, ECDSA, SHA-256 Engine, Hardware Acceleration.