ABSTRACT

The design of a high performance elliptic curve cryptographic processor over GF(2^{163}), is one of the five binary fields recommended by National Institute of Standards and Technology (NIST) for Elliptic Curve Cryptographic based Algorithm (ECCA). The proposed architecture is based on Lopez-Dahab elliptic curve point multiplication algorithm and uses Gaussian normal basis for GF(2^{163}) field arithmetic. To achieve high throughput rates, two new word-level arithmetic units over GF(2^{163}) and parallelized elliptic curve point doubling and addition algorithms with uniform addressing based on Lopez-Dahab method are derived.

Here, the designed hardware that executes the ECC algorithm that response on the ability of making the scalar multiplication over the GF (2^{193}) in a restricted number of clock cycles. The hardware design was based upon an optimized Finite State Machine (FSM), with a single cycle 193 bits multiplier, field adder and a field squarer. The different optimizations at the hardware level improve the acceleration of the ECC scalar multiplication; increases frequency and speed of operation such as key generation, encryption and decryption.

The FPGA's dedicated multipliers and carry-chain logic are used to obtain the small data path. It can handle all finite field operations over 256-bit prime fields and all elliptic curves of a specified form. The results prove that the proposed data path is suitable for a high-performance and compactness cryptosystem supporting both RSA and ECC over GF(p).

The cryptographic algorithms such as RC5, Triple DES, and AES are analyzed based on the factors like, power consumption, memory usage,

speed, number of input/outputs. As a result the algorithm with less power consumption and memory is implemented for designing low power highly securable crypto processor.

Intrusion rule processing in reconfigurable hardware enables intrusion detection and prevention. The proposed architecture called “BV-TCAM” is presented, which is implemented for an FPGA-based Network Intrusion Detection Systems (NIDS). The BV-TCAM architecture combines the Ternary Content Addressable Memory (TCAM) and the Bit Vector (BV) algorithm to effectively compress the data representation and throughput.

Then, FPGA-based architecture is proposed for Network intrusion detection systems (NIDs) monitor network traffic to detect suspicious and anomaly activity in network transmissions. Feature extraction module (FEM) is first developed to summarize network information to be used.

Pattern matching is the critical part in NIDS. Fast pattern matching algorithm is the key to improve the system performance. Here, a fast reverse pattern matching algorithm and the hardware implementation suitable with Field Programmable Gate Array (FPGA) are proposed. The parallel pattern matching system provides a high throughput of 4 Gbps with no data loss, which proves the information processing rate of this design.

From the results obtained, it is observed that, for using reconfigurable architecture methods of elliptic curve cryptography, the various cryptography algorithms RC5, TDES, AES and Intrusion Detection systems had better performance in terms of execution time, compactness, throughput and storage.