International conference on Advanced Techniques in Communication Networking and Automation

RESEARCH ARTICLE OPEN ACCESS

DESIGN OF SECURE MEMORY FOR VLSI BASED CRYPTO SYSTEM

M.Vijayalakshmi[1], Somu K[2], V.Suresh[3]

PG Student, VLSI Design, Department of ECE, Maha Barathi Engineering College, India[1]
(vijayalakshmi27620@gmail.com)
Professor, Department of ECE, Maha Barathi Engineering College, India[2]
(somu.pgp@gmail.com)
Assistant Professor, Department of ECE, Maha Barathi Engineering College, India[3]
(vsureshme@gmail.com)

ABSTRACT

The Elliptic Curve Cryptographic (ECC) technique is employed for the security standards like Security Key Management (SKM), digital signature, data authentication and so on. The ECC technique is capable of undertaking the sequential and equivalent mode processes through the unified design that is used equally for binary field and the leading area of cryptosystems. Furthermore, a progressive transposition method and control information route are combined to the ECC mainframe, which offers the efficient throughput and the vitality adaptive calculating with low power. The Dual-field Montgomery Multiplier- Carry Save Adder (DMM-CSA) structure is designed for the ECC system. The DMM structure has been developed by using CSA in this method. That adder requires a number of the Full Adder for the circuit design, which has occupied more area. To overcome this problem, this work introduces theDual Field Vedic Multiplier - Look up Table Carry Select Adder (DVM-LCSLA) which is used to increase the Performance of the ECC scheme for 256 bit. The first aim of all methods mentioned above is to develop a high-performance modular inversion for the ECC technique by employing Application Specified Integrated Chip (ASIC) and Field Programmable Gate array (FPGA) implementation with the help of Verilog code. FPGA **results indicated that the power utilization, time delay information and Hardware area overhead are analyzed in DVM-LCSLA used in ECC system compared to the state-of-art methods**.

1. INTRODUCTION

Semiconductor technology rapidly develops and micro architectural developments continue to increase which results in performance gap between processors and memory. Moore's law states that for every two years processor technology doubles in performance and speed. Modern processors use L1 and L2 as two levels in cache memories to reduce latency and bandwidth. Secure memory for cryptography has been proposed to improve system performance, since effective capacity can be increased by compressing data stored in on-chip caches which reduces cache misses. When the processor technology increases, speed increases faster because on-chip cache memory hierarchies can store more data in megabyte size. Off-chip memory speed is considerably low compared to processor speed. When the multiprocessor is utilized by system design, it requires more access to memory.

2. RELATED WORKS

2.1 CACHE MEMORY

Cache memory is a volatile computer memory which provides high speed access to the processor and stores frequently used computer programs, applications and data. It stores data until the computer is powered up. This may be located on CPU chip or module. The transfer of data between the main memory and the cache memory occurs in blocks of fixed sizes known as cache lines. Cache data entries are created when cache lines are copied from the main memory to the cache which includes the copied data with the requested memory location.

2.2 CACHE OPERATION OVERVIEW

The proportion of data access results from a cache hit is known as hit rate which is a measure of the cache"s effectiveness for a given algorithm or program. When a data transfer is needed from the main memory than the

cache, the read misses delay execution while the write would take place without that issue, since execution can be continued by the processor as data is copied to the main memory. The write policy controls the timing of the write operation. The writing has two basic approaches namely: write through and write-back.

Tracking the location in which it has been written over are performed. The locations which are tracked are then marked for later writing which would be performed to the store back.

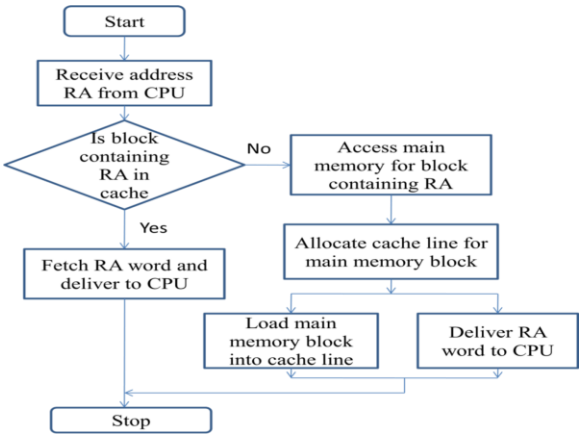

Fig 2.2 Cache Read Operation

2.3 CACHE MEMORY IN CRYPTOGRAPHY SYSTEM

A naive way to approach using cache behaviour is the construction of a database which matches hit/miss profiles collected from an attack run with pre-computed profiles for encrypting a plain-text under all possible keys. Although this sort of attack would be successful, the amount of storage and computational power required to mount such an attack is cripplingly large. In order to improve on this naive approach, our work employs analysis on, and knowledge of, the algorithms under attack.

This analysis forms relationships between parts of secret information based on the behaviour of the cache when the algorithm is run. Such relationships can be used to weaken the cipher, or perhaps directly produce the secret information, with some extra processing after the collection of cache profiles.

When discussing these techniques, we make several assumptions about the ability of the attacker and the composition of the device being attacked.

3. ANALYSIS OF CRYPTOGRAPHY ALGORITHMS

Cryptography offers a way for securing and authenticating the transmission of information across insecure communication channels. It permits us to save sensitive information or transmit it over insecure communication networks so that unauthorized persons cannot study it.

The study (A. M. Qadir and N. Varol et al., 2019) focused on implementingthe two most widely used symmetric encryption techniques, i.e., DES and AES, implemented in MATLAB software. Encryption algorithm plays an important role in message security. Where simulation, time, memory usages and level of encryption the major issue of concern. After implementation, these techniques are compared with memory required for implementation, simulation time required for encryption and avalanche effect.

3.1 ADVANCE ENCRYPTION STANDARDS (AES)

AES algorithm can help any combination of data (128) and a key length of 128, 192, and 256 bits. AES lets in a 128-bit data length that may be divided into four simple operational blocks. Those blocks are handled as an array of bytes and organized as a matrix of the order of 4×4, known as the state on which the simple operations of the AES algorithm are performed.

The study (J. SairaBanu et al., 2013) focused on the AES algorithm to provide security for smart cards in applications like the Internet. The main objective of this paper is to increase the AES algorithm throughput through hardware and software techniques. Architectural optimization of hardware technology such as pipeline, loop unrolling and iterative design is addressed. To increase the speed of the algorithm by processing multiple rounds simultaneously. Software parallelization techniques with OpenMP standard are used to increase the algorithm's speed compared to its sequential version. A pipelined architecture AES- 128 core is implemented using Xilinx xc5vlx110t-1 device can achieve a throughput of 31.25Gbps, which is more effective than previous ASIC implementations. By implementing the AES algorithm using OpenMP, we achieve a speedup of 1.08 in the dual-

core processor. This author uses pipeline technology and parallel technology with the open MP standard to increase throughput.

3.2 OVERVIEW OF CACHE MEMORY ATTACKS IN ELLIPTIC CURVE CRYPTOGRAPHY

The Elliptic Curve Cryptographic (ECC) technique is employed for the security standards like Security Key Management (SKM), digital signature, data authentication, etc. The ECC technique can undertake the sequential and equivalent mode processes through the unified design used equally for the binary field and the leading area of cryptosystems. Furthermore, a progressive transposition method and control information route are combined to the ECC mainframe, which offers the efficient throughput and the vitality adaptive calculating with low power. The Dual-field Montgomery Multiplier- Carry Save Adder (DMM-CSA) structure is designed for the ECC system.

The DMM structure has been developed by using CSA in this method. That adder requires a number of the Full Adder for the circuit design, which has occupied more area. To overcome this problem, this work introduces the Dual Field Vedic Multiplier - Lookup Table Carry Select Adder (DVM-LCSLA), which is used to increase the ECC scheme's Performance for 256 bit.

The first aim of all methods mentioned above is to develop a high-performance modular inversion for the ECC technique by employing Application Specified Integrated Chip (ASIC) and Field Programmable Gate array (FPGA) implementation the help of Verilog code. **FPGA** results indicated that the power utilization, time delay information and Hardware area overhead are analyzed in DVM-LCSLA used in the ECC system compared to the state-of-art methods**.**

3.3 DUAL FIELD MULTIPLIERS - ECC ARCHITECTURE

The ECC processor supports practical security application like ECDSA and extensive data encryption and decryption systems, containing all original Error correction based calculation and general predictable processes called step binary, step accumulation, coordinate conversion, numbering multiplication, Montgomery pre-processing, Montgomery supported processing, inversion, and predictable field multiplication. Arbitrary elliptic curves and finite field can be organizer-designed for tractability. Figure3.1 demonstrates the DVM-LCSLA structure with four Accumulation Units (AUs) of combined DVM and CSLA.

The system consists of the core manager, Error Correction scheduler and Montgomery Scheduler (MS). The foremost manager translates the information towards operating the Error Correction unit and Clock Control Unit (CCU). Each error Correction operation includes an order of linked exponentiations and accompaniments. Thus the elliptic cryptography scheduler performs the giving out of the instruction of the data-path elements iteratively.

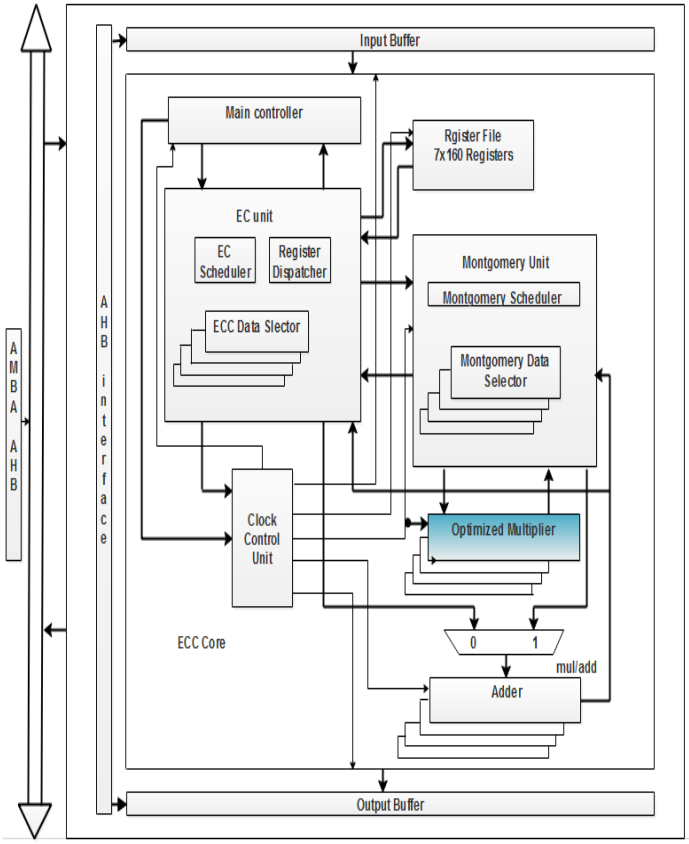

Fig 3.3 The block diagram of the Dual-field Montgomery Multiplier- Carry Save Adder architecture

4. SIMULATION RESULTS

The proposed Elliptic Curve Cryptography with multiplier design has been captured in Verilog Hardware Description

Language (HDL), implementation has been done on Xilinx ISE Design Suite 14.1 targeting Virtex-6 FPGA device.

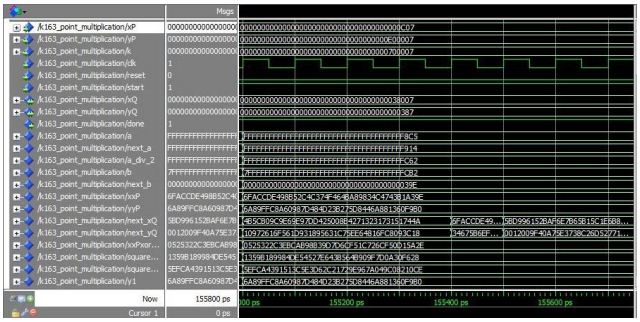

Fig 4.1 Simulation Result

The Simulation Output Result of Proposed Vedic Multiplier is shown in above figure 4.1. This Multiplier is used in ECC architecture. As a result, the proposed Dual Field Vedic Multiplier - Lookup Table Carry Select Adder can achieve higher throughput and much smaller Area-Time Product (ATP) than previous strategies.

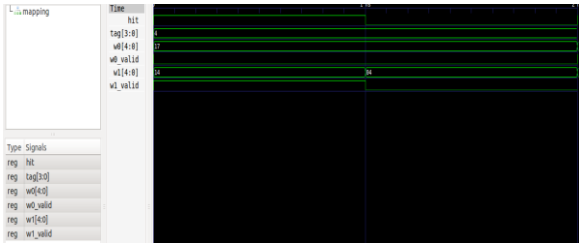

Fig 4.2: Simulation Results of Hit – Miss Logic result

The simulation response of Hit –Miss Logic is shown in Figure 4.2. During the simulation, cache enters the Tag Compare state, where it investigates the labels and checks the legitimate bit to choose whether there is a store hit or miss.

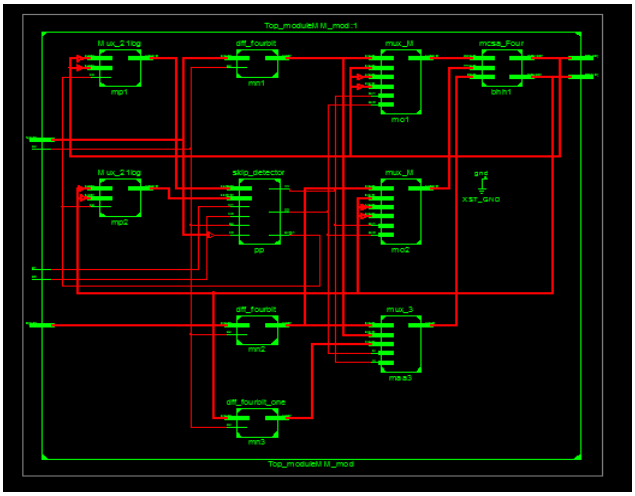

Fig 4.3 RTL Schematic of DVM-LCSLA

The RTL schematic diagram of the Proposed DVM-LCSLA Multiplier is shown in above figure 4.3. As compared to other multipliers, the proposed DVM-LCSLA Multiplier has a low area because of the fewer number of adder levels in the underlying algorithm.

5. CONCLUSION

In this research work so far has been fairly successful in developing techniques to use cache behavior information in a cryptography setting. The example starts by analyzing the flow of data through the algorithm in question to form relationships between bits of secret information. These relationships are brought about by the ability to reason about the behavior of the cache while the algorithm is running. In this work able to control the plaintext input to the algorithm in order to solidify these relationships and inspect possible values of secret information. This process narrows the possible values it can take so that key search may be executed more efficiently. Clearly our attack, like most side-channel attacks, is specialized to a given cryptographic algorithm and cannot easily be generalized to other algorithms even if they are similar in structure.

REFERENCES

1. A. M. Qadir and N. Varol, “A Review Paper on Cryptography,” 2019 7th International Symposium on Digital Forensics and Security (ISDFS) Barcelos, Portugal, 2019, pp. 1-6, DOI: 10.1109/ISDFS.2019.8757514
2. Abhishek Joshi, Mohammad Wazid, R.H. Goudar, An Efficient Cryptographic Scheme for Text Message Protection Against Brute Force and Cryptanalytic Attacks, Procedia Computer Science, Volume 48, 2015, Pages 360-366, ISSN 1877-0509.
3. AlveoNimbix Cloud. Available online: https://www.nimbix.net/alveotrial (accessed on 23 March 2020).
4. l. “Article: A Symmetric Key Cryptographic Algorithm.” International Journal of Computer Applications 2010; 1(14):1–4, DOI: 10.5120/331-502.

5. Azarderakhsh, Reza, and ArashReyhani-Masoleh. "Parallel and high-speed computations of elliptic curve cryptography using hybrid-double multipliers." IEEE Transactions on Parallel and Distributed Systems 26.6 (2015): 1668-1677.
6. Azarderakhsh, Reza, and MehranMozaffari-Kermani. "High-performance two-dimensional finite field multiplication and exponentiation for cryptographic applications." IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems 34.10 (2015): 1569-1576.
7. Chiou, CheWun, Chiou-Yng Lee, Jim-Min Lin, Yun-Chi Yeh, and Jeng-Shyang Pan. "Low-latency digit-serial dual basis multiplier for lightweight cryptosystems." IET Information Security 11, no. 6 (2017): 301-311.
8. D. Halperin, T. Kohno, T. S. Heydt-Benjamin, K. Fu, and W. H. Maisel, “Security and privacy for implantable medical devices,” IEEE Pervasive Comput., vol. 7, no. 1, pp. 30–39, Jan./Mar. 2008.
9. D. P. Kaur and V. Sulochana, "Design and Implementation of Cache Coherence Protocol for High-Speed Multiprocessor System," 2018 2nd IEEE International Conference on Power Electronics, Intelligent Control and Energy Systems (ICPEICES), Delhi, India, 2018, pp. 1097-1102.
10. D.Gu,J.Li,S.Li, ZMa,Z.Guo, and J.Liu,” Differential fault analysis on lightweight block ciphers with statical cryptanalysis techniques”, FDTC,september 2012.