Доклади на Българската академия на науките
Comptes rendus de l'Académie bulgare des Sciences

Tome 76, No 12, 2023

ENGINEERING SCIENCES

Electronics

POWER EFFICIENT IMPLEMENTATION OF ECC USING LCSLA BASED DUAL FIELD VEDIC MULTIPLIER

Senthil Kumar Sengottaiyan[#], Vadivel Subramaniam[*], Yuvaraja Thangavel[**], Karthick Sekar[***]

Received on August 26, 2023
Presented by Ch. Roumenin, Member of BAS, on October 31, 2023

Abstract

The Elliptic Curve Cryptographic (ECC) technique is employed for security standards such as Security Key Management (SKM), digital signature, data authentication and so on. The ECC technique is capable of sequential and parallel mode processes through a unified design. It is used for both equally binary fields and prime fields of cryptosystems. The DMM structure has been developed using CSA. This adder requires a greater amount of Full Adder circuits, which occupy more area. To overcome this problem, this paper discusses four different methods, such as DMM-Optimized Carry Look Ahead Adder, DMM-Optimized Carry Bypass Adder, DMM-Look up Table Carry Select Adder, and Dual Field Vedic Multiplier – LCSLA, which is used to increase the performance of the ECC. The parameters like power utilization, time delay information, and hardware area overhead are analyzed and compared with existing methods. Among those four methods, the DVM-LCSLA method gave better results in FPGA and ASIC performances.

Key words: application specified integrated circuit, dual-field Vedic multiplier, elliptic curve cryptography, field programmable gate array, lookup table carry select adder

Introduction. The ECC technique is the powerful Public-Key Cryptography (PKC) technique, which is employed to secure information in wireless devices [1–5].

[#]Corresponding author.
DOI:10.7546/CRABS.2023.12.09

The ECC technique provides more safety than modern Rivest–Shamir–Adleman (RSA) security with expressively Shorter-Key Length (SKL). The FPGA technology is recycled for hardware execution of linked reproduction, which provides a shorter design time, low cost and high flexibility of the system [6–9]. The DMM and DVM multipliers are used for cryptography system design and multipliers are designed by different kinds of adders, such as OCLA, OCBA, and LCSLA. First, the DVM-LCSLA method reduces the cycles for multiplicative inversion over a finite field. The Dual field multiplier is also accepted for the additional processing speed [10–15]. Instant, DVM-LCSLA scheduler controls the data-path for both serial and parallel power modes. These methods provide better performance regarding FPGA and ASIC than the conventional one.

Related work. Esmaeildoust et al. [16] have presented an efficient Reduced Number System (RNS) operation of Elliptic Curve Point Multiplication (ECPM) on GF(p). In this paper, the ECPM technique is presented over the RNS technique. By using the RNS method, substantial dynamic ranges are decomposed between small parallel paths, which operate at high speed and consume low power. The main drawback of this method is that the fixed point arithmetic is restricted. Debiao et al. [17] proposed the ECC system using the Anonymous Key Distribution (AKD) system. This AKD system for smart grid provided stronger security for data transactions, but it cannot offer several essential attributes of the smart meter anonymity. Yeh et al. [18] presented a tough elliptic curve cryptography-based Fan and Lin authentication system based on the smart card, password, and biometrics. This authentication system is implemented using security requirements. But, this method is only suitable for the biometric system. Debiao and Zeadally [19] have presented an investigation of Radio Frequency Identification (RFID) verification systems designed for the Internet of Things (IoT) in health care situations using ECC. In this work, the RFID technique is the main methodology of IoT in healthcare location. The RFID authentication systems provide security and performance for the data transaction system. But this technique has not fulfilled all security requirements. The above-discussed work surrounds numerous difficulties like increased power consumption, high critical path, more hardware utilization, and FPGA utilization. To conquer these problems, the proposed methods are implemented to improve the ASIC and FPGA implementation results.

Materials and methods. *Dual field multipliers – ECC architecture.* The ECC processor supports practical security applications such as ECDSA and extensive data encryption and decryption systems, containing all original error correction based calculations. In general, predictable processes called step binary, step accumulation, coordinate conversion, numbering multiplication, Montgomery pre-processing, Montgomery supported processing, inversion, and predictable field multiplication are used. Figure 1 demonstrates the DVM-LCSLA structure with four Accumulation Units (AUs) of DVM and CSLA. The system consists of the

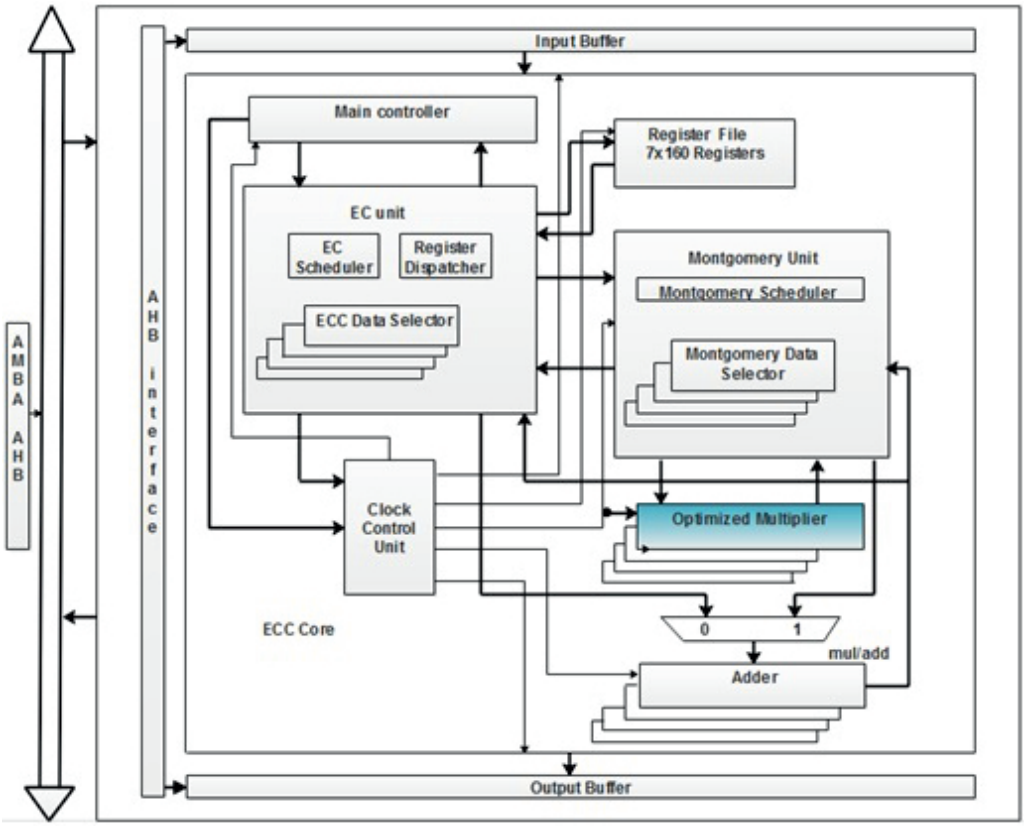


Fig. 1. The block diagram of the DVM-LCSLA architecture

core manager, Error Correction scheduler and Montgomery Scheduler (MS). The foremost manager translates the information to the Error Correction unit and Clock Control Unit (CCU). Each error correction operation includes an order of linked exponentiation and accompaniment. Thus, the elliptic cryptography scheduler performs the distributed instruction of the data-path elements iteratively. The elliptic cryptography component contains Register Contributor (RC) and four EC data selector to contact the Montgomery Unit (MU) and dual-field adders underneath similar (four AUs) and sequential (one AU) control styles [5].

These multipliers are optimized with the help of different adders such as OCLA, OCBA and LCSLA which are explained in the following sections.

DMM-OCBA structure. In CBA, the adder input is assumed to be loaded in parallel and skip data (signal) of all blocks are ready at the same time. The conventional CBA requires several numbers of logic gates, which circuit design occupies more area in the multiplier design. Therefore, the LUT circuit is utilized for OCBA for DMM design.Then the time consumption will become substantial, meanwhile recovering an assessment after recollection is quicker associated with contribution and production process.

DMM-LCSLA structure. The optimized LCSLA architecture is used in fast arithmetic process applications. Hence, the lower power consumption is accomplished with reduced hardware area overhead and high-speed applications. The LCSLA is operating in numerous complex structures to cut the transmit circulation interruption.

The main advantage of this LCSLA is that the time taken to perform RCA has been reduced and it consists of one full adder and one-half adder. The input arrival time is smaller than the multiplexer collection input arrival time. Therefore, the DMM-LUT LCSLA method improved computation time of the ECC system.

DVM-LCSLA structure. In this method, the two types of fields, such as the binary field and prime field are used for cryptography systems. Several vital principles and substitute formulations are used in Vedic mathematics, which is used to resolve complete numeric multiplication. The Vedic Multiplier architecture is high-speed compared to the Montgomery multipliers. Here, consider the Urdhva-Tiryakbhayam multiplication, which has binary dual multiplicand and multiplier. The block diagram of 4×4 DVM is shown in Fig. 2. According to this diagram, the Verilog code is written to verify the results.

Initially, the Least Significant Bit (LSB) of the two inputs (a0, a1 and b0, b1) is given to the input of a 2×2 multiplier block to perform a multiplication operation. In the 2nd stage, a2, a3 and b0, b1, 3rd stage a0, a1 and b2, b3, in the final stage, the a2, a3, and b2, b3 values are performed using the 2×2 multiplier operation. The last two-stage multiplier value is stored in one adder and the first two-stage multiplier value is stored in one more adder. Those two adders' results are given the input of the final adder. Finally, 8-bit results are delivered in the output of the DVM design. While designing the 233 bit Vedic

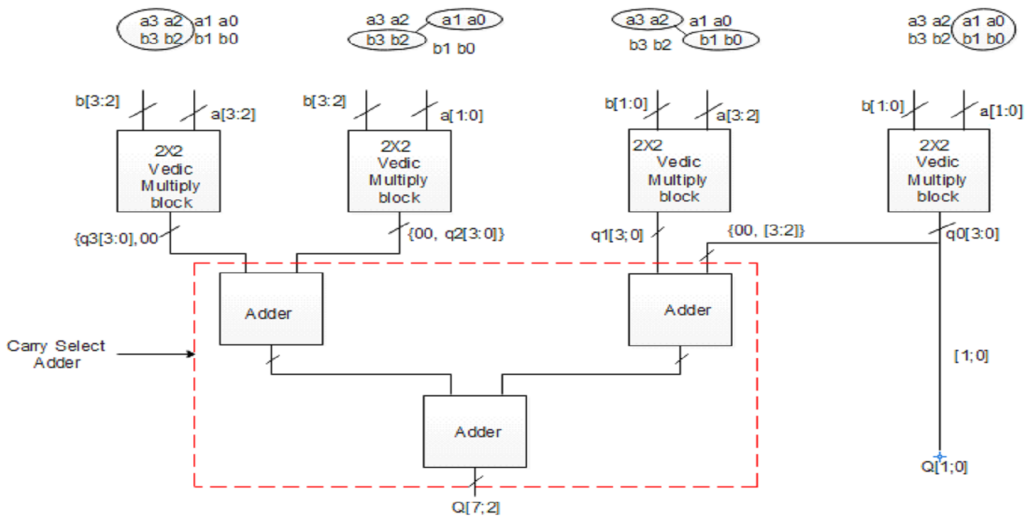


Fig. 2. 4×4 dual field Vedic multiplier block diagram

multiplier, many different bits of multipliers are used, such as 233 bit, 117 bit and 54 bit. The FPGA implementation of LCSLA method based performance metrics is more valid than the existing methods. All the methods have been implemented and analysed. The FPGA and ASIC performances are mentioned in the following sections.

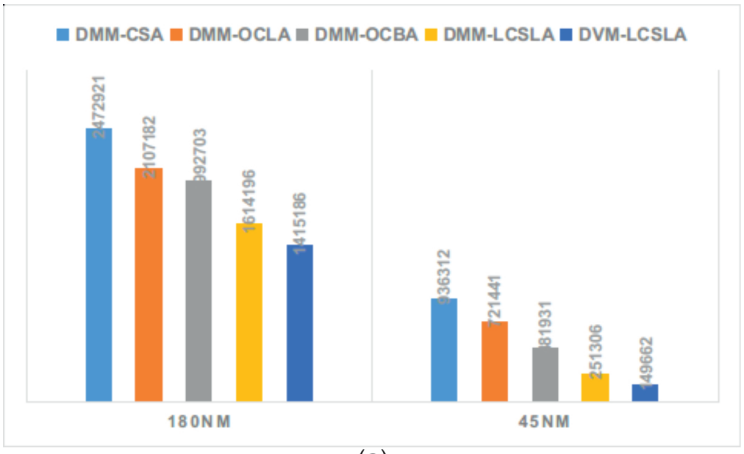
Results and discussion. The DVM-LCSLA structure is simulated and the timing diagram is verified in Modalism 10.4c using Verilog code. FPGA performance is analyzed for different devices such as Virtex-6 and Virtex-7 by employing Xilinx ISE tool. In DVM-LCSLA, ASIC implementation of ECC is verified by using Cadence tools in 180 nm as well as 45 nm. The proposed architecture result has been taken in both 180 nm and 45 nm technology. We have concluded that DVM is a good multiplier among the four multipliers. The hardware area overhead reduction of 84.01%, power reduction of 72.79% and time delay reduction of 20.33% have been obtained in 45 nm technology. By using 180 nm technology, the proposed method achieved a hardware area overhead reduction of 42.77%, power reduction of 71.09% and time delay reduction of 28.61%. The comparison of the hardware area overhead, power consumption, and time delay reduction for the different methods are shown in Fig. 3.

Table 1 presents the performance comparison of different virtex devices for various methods for analyzing performance limitations. Table 1 shows that the LUT, flip-flop, slices are reduced and operating frequency is increased in the DVM-LCSLA method as compared to the existing method. Due to the reduction of those parameters, the area has been minimized in the ECC architecture.

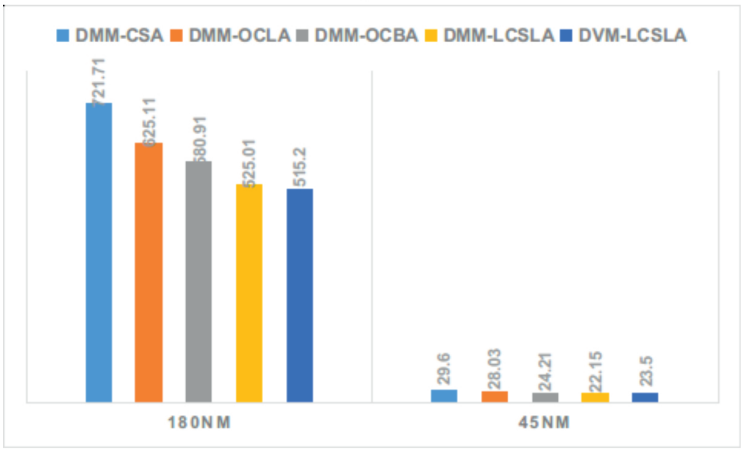
T a b l e 1

Performance analysis of different Xilinx Virtex devices for various methods

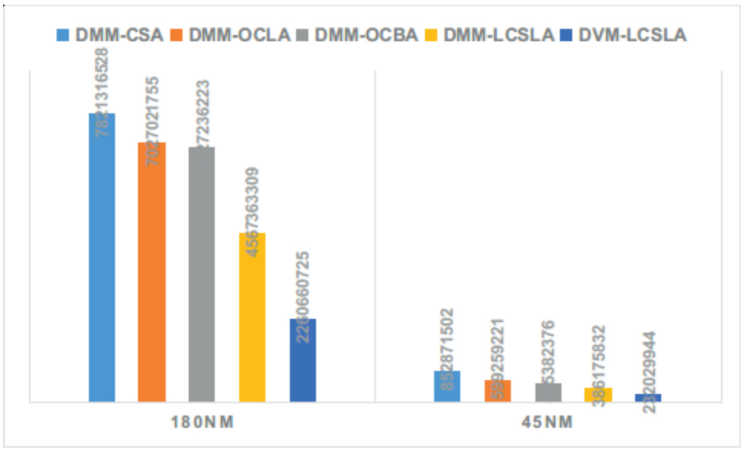
Target FPGA	Circuit	LUT	Flip-flop	Slice	Number of DSP	Frequency (MHz)
Virtex6 xc6vcx240t	DMM-CSA	119981/150720	85/109984	86/301440	768/768	20.42
	DMM-OCLA	98526/150720	88/109984	81/301440	736/768	25.55
	DMM-OCBA	90235/150720	78/109984	75/301440	699/768	25.62
	DMM-LCSLA	82256/150720	65/109984	70/301440	781/768	30.55
	DVM-LCSLA	**79594/150720**	**58/73608**	**72/301440**	**656/768**	**39.64**
Virtex7 xc7vx550t	DMM-CSA	98217/346400	73/99219	76/692800	3580/2880	37.64
	DMM-OCLA	95625/346400	69/99219	70/692800	3454/2880	20.21
	DMM-OCBA	88254/346400	65/99219	68/692800	3125/2880	26.15
	DMM-LCSLA	81546/346400	61/99219	63/692800	2968/2880	30.32
	DVM-LCSLA	**77054/346400**	**50/692800**	**50/692800**	**2784/2880**	**38.22**
Virtex7 xc7vx485t	DMM-CSA	98462/303600	45/99465	58/607200	3500/2800	34.66
	DMM-OCLA	95235/303600	54/99465	56/607200	3312/2800	25.12
	DMM-OCBA	91254/303600	56/99465	51/607200	3125/2800	28.65
	DMM-LCSLA	86325/303600	51/99465	50/607200	2935/2800	31.75
	DVM-LCSLA	**84726/303600**	**45/99465**	**48/607200**	**2705/2800**	**38.42**



(a)



(b)



(c)

Fig. 3. Comparison of the hardware area overhead (a), power consumption (b), and time delay reduction (c) for the different methods

Conclusion. In this paper, four architectures have been implemented for cryptography systems, such as DVM-LCSLA, DMM-OCLA, DMM-OCBA and DMM-CSLA in Xilinx software using Verilog code. In this multiplier, alternative to the usual accumulator, the LCSLA accumulator has been used to evaluate the concert constraints such as area, controller power, interrupted time delay, APP and ADP. Among those four methods, DVM-LCSLA method gave better results in FPGA and ASIC performances. In FPGA implementation the LUT, slices, flip-flops, and frequency have been improved in DVM-LCSLA. Similarly in ASIC implementation, the hardware area overhead reduction of 84.01%, power reduction of 72.79% and time delay reduction of 20.33% have been obtained in 45 nm technology. By using 180 nm technology, the proposed method achieved a hardware area overhead reduction of 42.77%, power reduction of 71.09% and time delay is 28.61% reduced than the conventional methods.

REFERENCES

[1] Chiou C. W., C.-Y. Lee, J.-M. Lin, Y.-C. Yeh, J.-S. Pan (2017) Low-latency digit-serial dual basis multiplier for lightweight cryptosystems, IET Inf. Secur., **11**(6), 301–311.

[2] Hossain M. S., Y. Kong (2015) High-performance FPGA implementation of modular inversion over F_256 for elliptic curve cryptography. In: Proc. 2015 IEEE Int. Conf. on Data Science and Data Intensive Systems (DSDIS), `https://doi.org/10.1109/DSDIS.2015.47`.

[3] Liu Z., D. Liu, X. Zou (2017) An efficient and flexible hardware implementation of the dual-field elliptic curve cryptographic processor, IEEE Trans. Ind. Electron., **64**(3), 2353–2362.

[4] Wang Z., K. Ma, Z. Ma, H. Fu et al. (2022) A 20.7–43.8-GHz low power reconfigurable frequency multiplier for multiple 5G-mm-wave bands, IEEE J. Solid-State Circuits, **57**(8), 2348–2361.

[5] Lai J.-Y., C.-T. Huang (2011) Energy adaptive dual-field processor for high performance elliptic curve cryptography application, IEEE Trans. VLSI Syst., **19**(8), 1512–1517.

[6] Lee J.-W., S.-C. Chung, H.-C. Chang, C.-Y. Lee (2014) Efficient power-analysis-resistant dual-field elliptic curve cryptographic processor using heterogeneous dual-processing-element architecture, IEEE Trans. VLSI Syst., **22**(1), 49–61.

[7] Li J., W. Wang, J. Zhang, Y. Luo (2021) Innovative dual binary field architecture for point multiplication of elliptic curve cryptography, IEEE Access, **9**(4), 12405–12419.

[8] Azarderakhsh R., M. Mozaffari-Kermani (2015) High-performance two-dimensional finite field multiplication and exponentiation for cryptographic applications, IEEE Trans. Comput.-Aided Des., **34**(10), 1569–1576.

[9] Azarderakhsh R., A. Reyhani-Masoleh (2015) Parallel and high-speed computations of elliptic curve cryptography using hybrid-double multipliers, IEEE Trans. Parallel Distrib. Syst., **26**(6), 1668–1677.

[10] Azarderakhsh R., K. U. Jarvinen, M. Mozaffari-Kermani (2014) Efficient algorithm and architecture for elliptic curve cryptography for extremely constrained secure applications, IEEE Trans. Circuits Syst., **61**(4), 1144–1155.
[11] Kuang S.-R., K.-Y. Wu, R.-Y. Lu (2016) Low-cost high-performance VLSI architecture for Montgomery modular multiplication, IEEE Trans. VLSI Syst., **24**(2), 434–443.
[12] Meher P. K., X. Lou (2017) Low-latency, low-area, and scalable systolic-like modular multipliers for GF(2^m) based on irreducible all-one polynomials, IEEE Trans. Circuits Syst., **64**(2), 399–408.
[13] Khan A., A. N. Bahar, R. Arya (2022) Efficient design of Vedic square calculator using quantum dot cellular automata (QCA), IEEE Trans. Circuits Syst. II: Express Briefs, **69**(3), 1587–1591.
[14] Chen H., H. Yang, W. Song, Z. Lu, Y. Fu (2021) Symmetric-mapping LUT-based method and architecture for computing XY-like functions, IEEE Trans. Circuits Syst. I: Regular Papers, **68**(3), 1231–1244.
[15] Bianchi V., I. De Munari (2020) A modular Vedic multiplier architecture for model-based design and deployment on FPGA platforms, Microprocess. Microsyst., **76**(2), 1456–1467.
[16] Esmaeildoust M., D. Schinianakis, H. Javashi, T. Stouraitis, K. Navi et al. (2013) Efficient RNS implementation of elliptic curve point multiplication over GF(p), IEEE Trans. VLSI Syst., **21**(8), 1545–1549.
[17] Debiao H., H. Wang, M. K. Khan, L. Wang (2016) Lightweight anonymous key distribution scheme for smart grid using elliptic curve cryptography, IET Commun., **10**(14), 1795–1802.
[18] Yeh H.-L., T.-H. Chen, K.-J. Hu, W.-K. Shih (2013) Robust elliptic curve cryptography-based three factor user authentication providing privacy of biometric data, IET Inf. Security, **7**(3), 247–252, https://doi.org/10.1049/iet-ifs.2011.0348.
[19] Debiao H., S. Zeadally (2015) An analysis of RIFD authentication schemes for internet of things in healthcare environment using elliptic curve cryptography, IEEE IoT J., **2**(1), 72–83.

K. S. R. College of Engineering
Tiruchengode, Tamilnadu, India
e-mail: s.senthilkumar@ksrce.ac.in

**Kongunadu College of Engineering
and Technology
Thottiam, Trichy
e-mail: kstyuvaraja@gmail.com

*Department of ECE
K. S. R. College of Engineering
Tiruchengode, Tamilnadu, India
e-mail: ecevadivel@gmail.com

***Department of Electrical Electronics
and Communication Engineering
GITAM Deemed to be University
Bengaluru, India
e-mail: karthickapplied@gmail.com