Journal of Ambient Intelligence and Humanized Computing
https://doi.org/10.1007/s12652-020-02830-1

ORIGINAL RESEARCH

Improving security against cache memory attacks for dual field multiplier design based on elliptic curve cryptography

R. Vijay Sai[1] · Har Narayan Upadhyay[2]

Received: 2 October 2020 / Accepted: 9 December 2020

Abstract
The elliptic curve cryptographic (ECC) technique is employed for various security standards like security key management, digital signature and data authentication. The ECC technique is capable of undertaking sequential and equivalent mode processes through the unified design that is used equally for binary field and in the leading area of cryptosystems. Furthermore, a progressive transposition method and control information route are combined with the ECC mainframe, which offers efficient throughput, and adaptive calculation 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 using CSA in this method. The adder requires more number of Full Adders for the circuit design, which has occupied more area. To overcome this problem, this work introduces the dual 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 the methods mentioned above is to develop a high-performance modular inversion for the ECC technique by employing application specified integrated chip and field programmable gate array (FPGA) implementation with the help of Verilog code. FPGA results indicate the analysis of power utilization, time delay information and Hardware area overhead in DVM-LCSLA used in ECC system compared to the state-of-art methods.

Keywords Application specified integrated circuit · Dual-field Vedic multiplier · Elliptic curve cryptography · Field programmable gate array · Lookup table carry select adder

1 Introduction

Nowadays, the ECC technique is used for high-security standards, which is providing security information and transaction applications such as personal digital assistants (PDA), cellular phones, smart cards, web servers, SKM, digital signature, finance, and data authentication. The ECC technique is the powerful public-key cryptography (PKC) technique, which is employed to secure the information in wireless devices (Chiou et al. 2017; Hosspain and Kong 2015; Liu et al. 2017; Zhu et al. 2013). The ECC technique provides more safety to the modern Rivets-Shamir-Adleman (RSA) security with expressively shorter-key length (SKL). The FPGA technology is recycled for a hardware execution of linked reproduction, which provides a shorter design time, low cost and high flexibility of the system (Lai and Huang 2011; Liu et al. 2017). The wireless security system is employed for two types of cryptography such as public and shorter key cryptography (PKC and SKC). The SKC design architecture is compact and in crucial small size. The PKC design produces an essential technology for necessary arrangement, digital signature and encryption and decryption (Lee et al. 2014; Guitouni et al. 2011; Azarderakhsh and Mozaffari-Kermani 2015; Azarderakhsh et al. 2015).

The reliable communication systems offer an integrated platform like reliability, data confidentiality, message authentication for the security services. These services are not possible without secure group key management protocol. The group key agreement (GKA) technique is following different kinds of group key management organizations like centralized, distributed, and contributory. But the main drawback of this technique is limited computational complexity (Esmaeildoust et al. 2013; Debiao et al. 2016). The ECC technique is based on elliptic curves, which are defined as prime fields, binary

✉ R. Vijay Sai
vijaysai@it.sastra.edu

Har Narayan Upadhyay
hnu@ece.sastra.edu

[1] School of Computing, SASTRA Deemed to be University, Thanjavur, Tamilnadu, India

[2] School of Electrical and Electronics Engineering, SASTRA Deemed to be University, Thanjavur, Tamilnadu, India

Published online: 05 January 2021

fields and finite fields (Yeh et al. 2013). The RSA algorithm is widely used for secure data transmission. But RSA algorithm is presently helpless because of the fast factoring attack in cryptanalysis. The ECC technique provides higher security compared to RSA algorithm (Debiao and Zeadally 2015; Kimmo and Mozaffari-Kermani 2014; Kuang et al. 2016; Meher and Lou 2017; Shukla et al. 2020).

In elliptic curve system, more time is required to operate the ECC in number based reproduction (Sonali and Shekhar 2016). The amount based reproduction is classified into two atomic blocks: ECC point adding (ECCPA) and ECC plug replication (ECCPR). However, GF (p) is a support to particular elliptic curve but cannot support several elliptic curves (Sonali et al. 2016). The ECC system is implemented by using digit-serial Gaussian normal basis (GNB) multipliers. The GNB multiplier will be recycled where efficient outcomes are needed, and this method provides less robustness (Sonali et al. 2016; Sree et al. 2017; Vijeyakumar et al. 2016; Perianin et al. 2020).

To overcome this problem, the ECC processor structure addresses improvements which is based on two aspects like power and system performance. In this paper, the DMM and DVM multipliers are used for cryptography system design, of which multipliers are designed by different kinds of adders such as optimized carry look ahead adder (OCLA), optimized carry bypass adder (OCBA), and look up carry select adder (LCSLA). First, the DVM-LCSLA method reduces the cycles for multiplicative inversion over a finite field. Twin field multiplier is also accepted for the additional processing speed. Instantly, DVM-LCSLA scheduler has controlled the data-path for both serial and parallel power modes (Sai et al. 2019). Hence, the vitality—adaptive system, calculating improvement with active control concert trade-off is introduced. These methods provide better performance regarding FPGA and ASIC than the conventional manner. FPGA implementation results indicated that the reduced power utilization, decreased time delay information and minimized Hardware area overhead are achieved. The remaining part of this work is discussed as follows:

Section 2 discusses the operation of dual field multipliers with ECC architecture
Section 3 discusses the function of proposed DVM-LCSLA method
Section 4 discusses simulation result and performance evaluation
Section 5 discusses the conclusion and future scope of the work

2 Dual field multipliers: ECC architecture

The ECC processor supports practical security applications like ECDSA and extensive data encryption and decryption systems, containing all original error correction based calculation and general predictable processes called as step binary, step accumulation, coordinate conversion, numbering multiplication, Montgomery pre-processing, Montgomery supported processing, inversion, and predictable field multiplication. Arbitrary elliptic curve and finite field can be organiser-designed for the tractability. Figure 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 operation of the instruction of data-path elements iteratively. Then elliptic cryptography component contains register contributor (RC) and four EC data selectors to contact the Montgomery unit (MU) and dual-field adders underneath similar (four AUs) and sequential (one AU) control styles Fig. 1.

The elliptic cryptography information chooser deciphers controller instruction after the elliptic cryptography and then the central controller near the MU for linked reproduction process and the dual-field adder is used on behalf of the modular adding operation. Then read data (RD) has stored an intermediate result to the register bank. In this architecture, two multipliers will be used such as Montgomery multiplier and dual field Vedic multiplier. These multipliers are optimized with the help of different adders such as

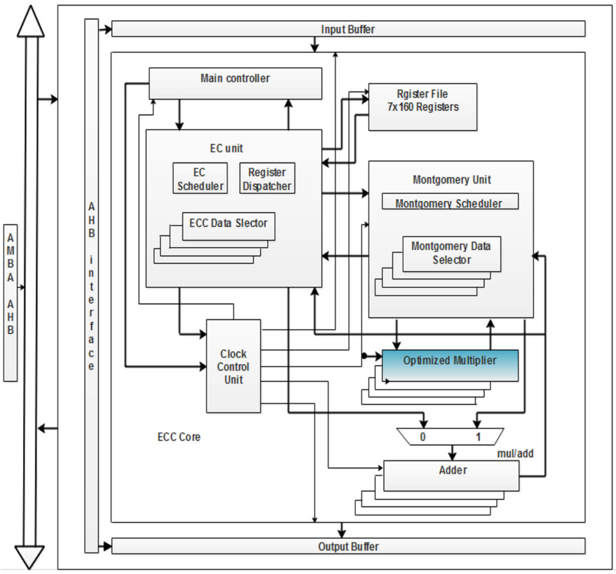


Fig. 1 The block diagram of the dual-field Montgomery multiplier-carry save adder architecture

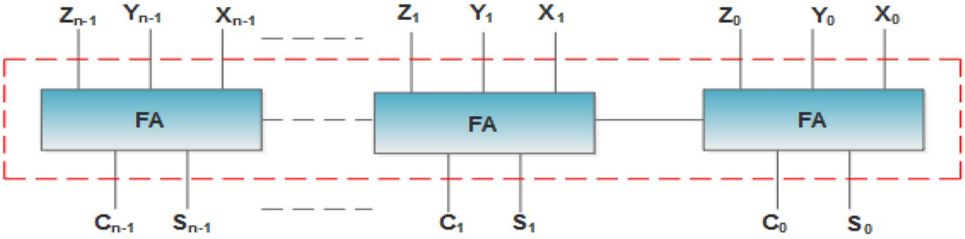


Fig. 2 Block diagram of the DMM-CSA

OCLA, OCBA, and LCSLA which is explained in following sections.

2.1 DMM-CSA structure

The CSA is one of the digital adder employed in computer microarchitecture to calculate the sum of several N-bit numbers in binary value. The differences from another digital adder that produces binary outputs of similar dimensions of the same input and the order of limited bit is an arrangement of the transmit bit. In this work, the DMM architecture is designed for the ECC system by using CSA circuit.

In the CSA, a long carry propagation is one of the main problems, because this adder has required several full adder circuits. Hence, this CSA design has occupied more area. Existing design utilizes more hardware and also has poor ASIC performances Fig. 2. To improve the ASIC and FPGA performances, we have proposed four methods such as DMM-OCLA, DMM-OCBA, DMM-LCSLA, and DVM-LCSLA- methods which are implemented to analyze output performance.

2.2 DMM-OCLA structure

In the past years, most research works has been focusing on the minimizing delay of the addition operation. The system of high performance and high speeds are being invented, which need high-speed adders and addition being the fundamental function of the most circuit. Figure 3 shows the architecture of the existing CLA structure.

The existing CLA design requires several full adder (FA) circuits for given input bits (A_0, A1, A_2, B_0, B_1, B_2). For example, 8-bit CLA adder design requires eight FA circuit that needs more area. With the help of FA design, we can able to design 8 bit CLA which has shown Fig. 4.

An optimized CLA using FA design with register is used instead of two or more FA design requirement. The output data are stored in the register based input clock cycle. In the OCLA, reduced carry propagation delay, where the circuit design occupies less area compared to DMM-CSA method is done.

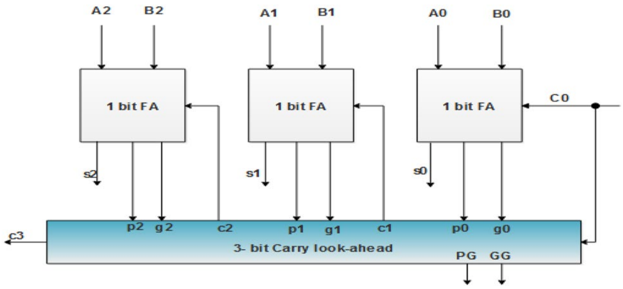


Fig. 3 Existing CLA architecture

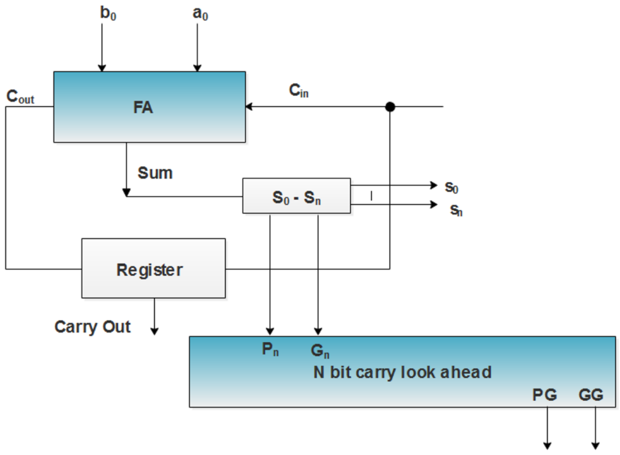


Fig. 4 Structure of optimized DMM-CLA

2.3 DMM-OCBA structure

Figure 5 shows the circuit diagram of the CBA structure. In the CBA, the input is believed to be stacked in equal, and skip data (signal) of all blocks are set up at same time. The first skipped block requires to have the even size as an un-skipped block before it achieves the objective that all the chief multiplexer's data sources show up independently in the CBA.

The conventional CBA design requires several numbers of logic gates, of which circuit design occupies more area in the multiplier design. Therefore, the LUT circuit is utilized for CBA design of the DMM design. The collection of LUT substitutes ensures execution calculation within the similar

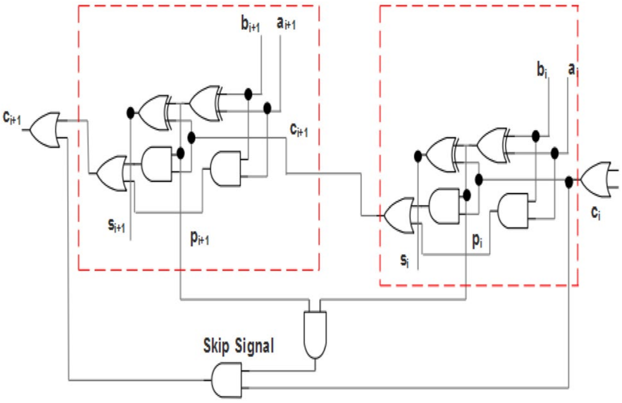


Fig. 5 A circuit diagram of existing CBA structure

collective index process. Then the time consumption will be substantial, meanwhile recovering an assessment after recollection is quicker associated with contribution and production process. The optimized LUT-CBA architecture is exposed in Fig. 6 in which dispensation time and area will also be less when compared to the existing CBA adder design.

2.4 DMM-LCSLA structure

The elementary knowledge of this work is to use LUT as a substitute of ripple carry adder (RCA) through $C_{in} = 1$. The architecture of the CSLA with its Binary to Excess-1 Converter (BEC) is revealed in Fig. 7.

The block diagram of the first optimized LCSLA adder is depicted in Fig. 8, by using the optimized LCSLA architecture used in fast arithmetic process applications. Hence the lower power consumption is accomplished with reduced hardware area overhead and used in high-speed applications. The LCSLA is operating in numerous complex structures to cut the transmit circulation interruption.

The elementary knowledge of this exertion is to customise LUT as an alternative of RCA through the consistent LCSLA in the direction of accomplishing subject area and control depletion. The main advantage of this LCSLA is

Fig. 6 Block diagram of the DMM-OCBA structure

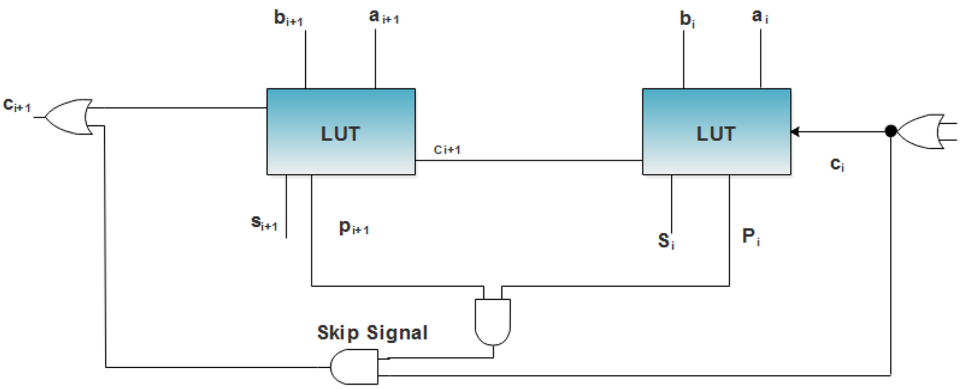


Fig. 7 Block diagram of the existing CSLA

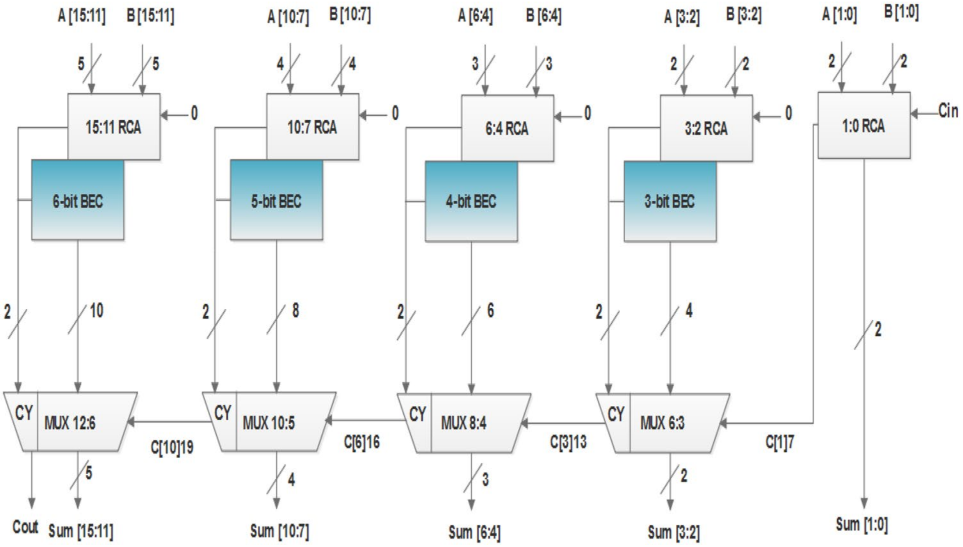
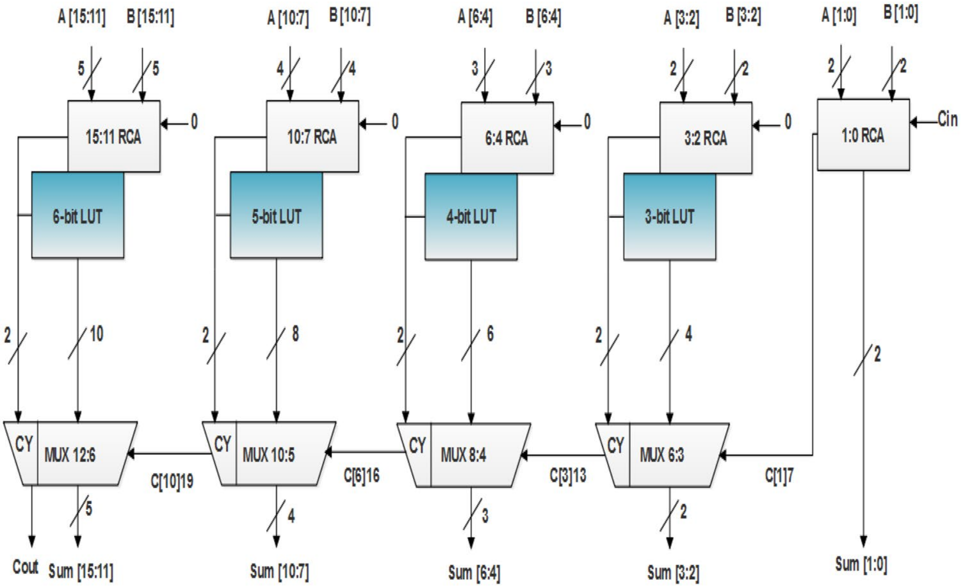


Fig. 8 Block diagram of the optimized LUT-CSLA



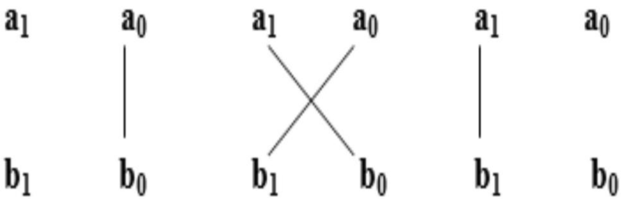


Fig. 9 2×2 Vedic multiplication

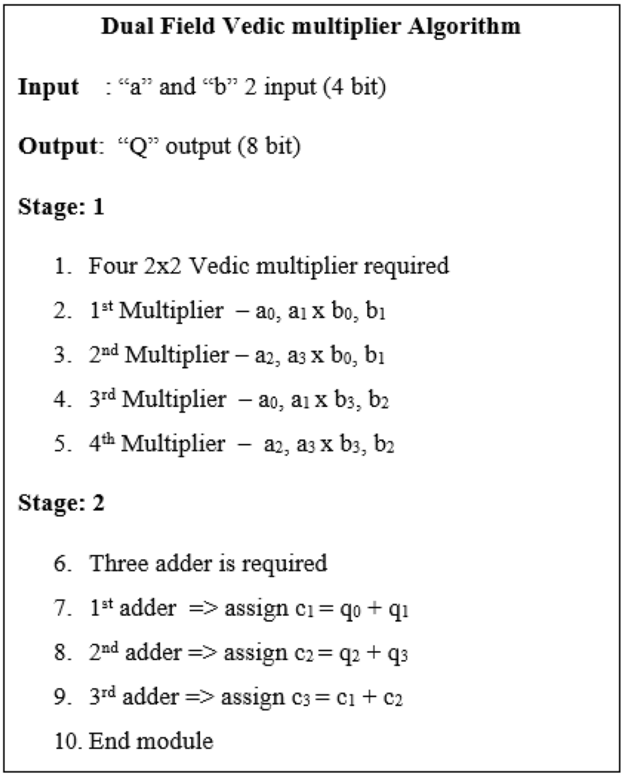
that the time taken to perform RCA has been reduced, and it consists of one full adder and one-half adder.

The input arrival time is smaller than the multiplexer collection input arrival time. Established on the collection line input C_{in}, this adder provides each LUT output or multiplexer output. Therefore, the DMM-LUTCSLA method has improved computation time of the ECC system. But this adder is not much suitable for the Montgomery multiplier design, due to LCSLA design, implemented for DVM design of the ECC system.

3 Proposed DVM-LCSLA method

Figure 9 shows 2 × 2 multiplication by using a Vedic multiplier. The ECC configuration can be realized by using a 8 × 8 double field Vedic multiplier.

The Vedic multiplier configuration is executed by utilizing LCSLA [shown in 2.1.4]. In this strategy, two kind of fields, for example, binary field and prime field are utilized for cryptography systems. Several essential standards and substitute—plans utilized in Vedic science are implemented to determine total numeric multiplication. The Vedic multiplier design is fast and appearing differently in relation to the Montgomery multipliers. The Vedic multiplier is applied to all sorts of cutting edge plans. Here think about the Urdhva Triyagbhyam increase, which has binary duals, multiplicand (a_1, a_0) and multiplier (b_1, b_0). Thus, the results



Dual Field Vedic multiplier Algorithm

Input : "a" and "b" 2 input (4 bit)

Output: "Q" output (8 bit)

Stage: 1

1. Four 2x2 Vedic multiplier required
2. 1st Multiplier – a_0, a_1 x b_0, b_1
3. 2nd Multiplier – a_2, a_3 x b_0, b_1
4. 3rd Multiplier – a_0, a_1 x b_3, b_2
5. 4th Multiplier – a_2, a_3 x b_3, b_2

Stage: 2

6. Three adder is required
7. 1st adder => assign $c_1 = q_0 + q_1$
8. 2nd adder => assign $c_2 = q_2 + q_3$
9. 3rd adder => assign $c_3 = c_1 + c_2$
10. End module

Fig. 10 Working procedure of 4×4 DVM

after duplication technique of binary numbers give 4-piece of yield.

For the most part, Vedic multiplier is following the underneath steps,

Step 1 The perpendicular multiplication of least significant bits (LSB) produce a definitive outcome of the least significant bits

Step 2 At that point the inclining multiplication of LSB multiplicand bits and most significant bit (MSB) of multiplier realizes the multiplier bits freely.

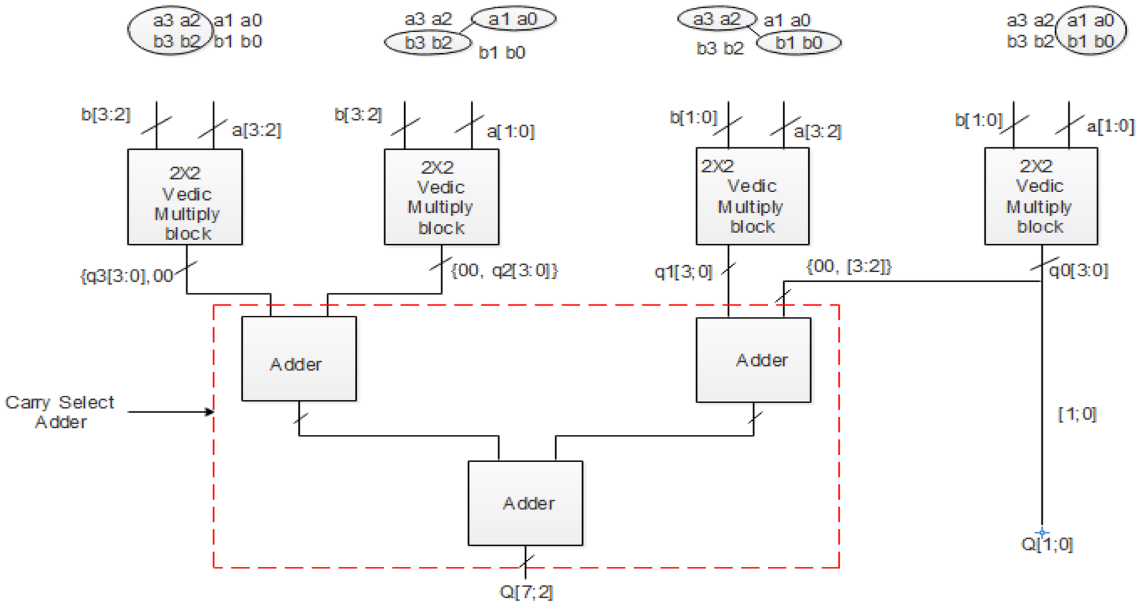
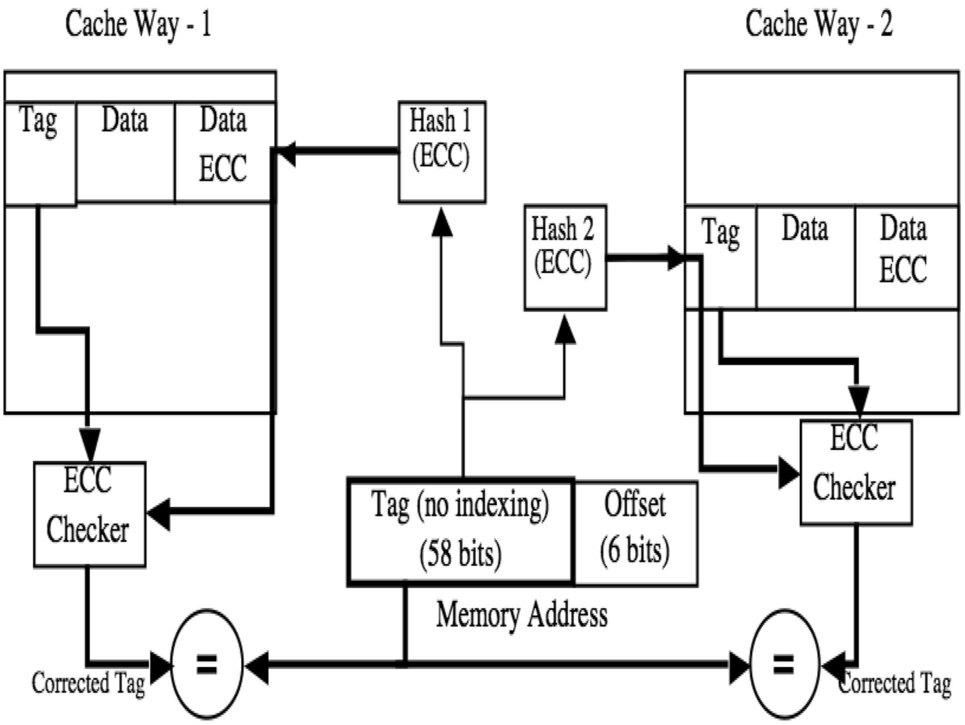


Fig. 11 4x4 dual field Vedic multiplier block diagram

Fig. 12 Fault tolerant cache architecture



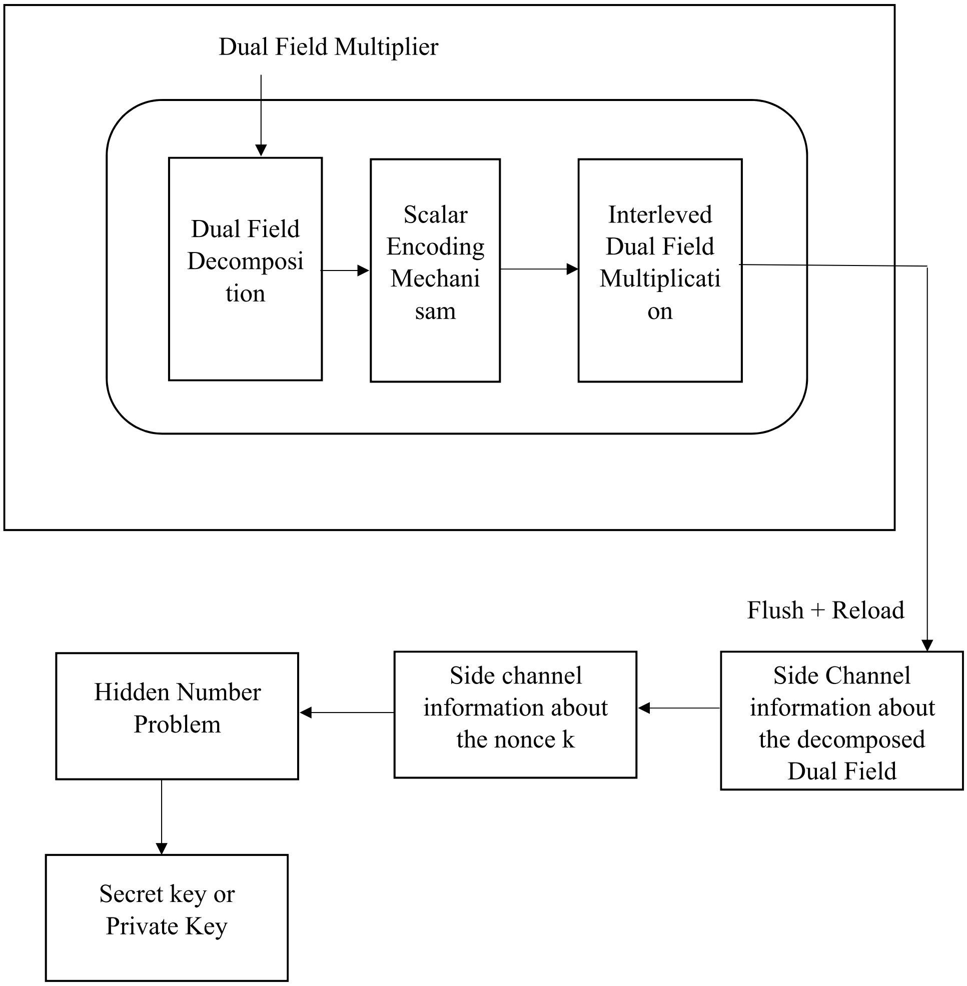
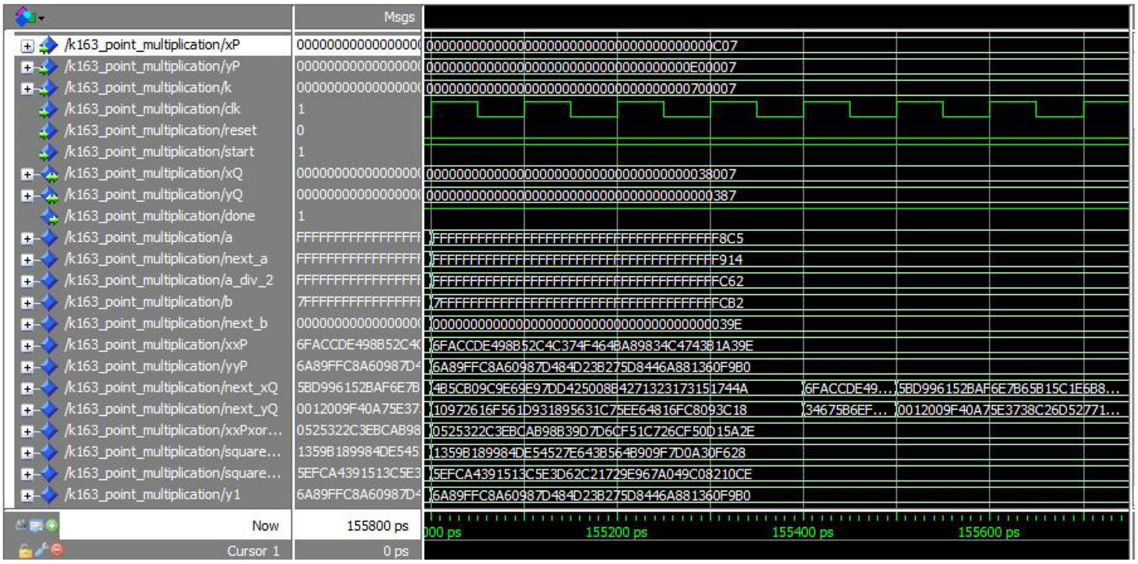

Dual Field Multiplier
Dual Field Decomposi tion
Scalar Encoding Mechani sam
Interleved Dual Field Multiplicati on
Flush + Reload
Side Channel information about the decomposed Dual Field
Side channel information about the nonce k
Hidden Number Problem
Secret key or Private Key

Fig. 13 Overall work flow of side channel attack against cache



	Msgs	
/k163_point_multiplication/xP	0000000000000000(	0000000000000000000000000000000000000C07
/k163_point_multiplication/yP	0000000000000000(	0000000000000000000000000000000000E00007
/k163_point_multiplication/k	0000000000000000(	0000000000000000000000000000000000700007
/k163_point_multiplication/clk	1	
/k163_point_multiplication/reset	0	
/k163_point_multiplication/start	1	
/k163_point_multiplication/xQ	0000000000000000(	0000000000000000000000000000000000038007
/k163_point_multiplication/yQ	0000000000000000(	0000000000000000000000000000000000000387
/k163_point_multiplication/done	1	
/k163_point_multiplication/a	FFFFFFFFFFFFFFFFI	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF8C5
/k163_point_multiplication/next_a	FFFFFFFFFFFFFFFFI	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF914
/k163_point_multiplication/a_div_2	FFFFFFFFFFFFFFFFI	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFC62
/k163_point_multiplication/b	7FFFFFFFFFFFFFFFI	7FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFCB2
/k163_point_multiplication/next_b	0000000000000000(	000000000000000000000000000000000000039E
/k163_point_multiplication/xxP	6FACCDE498B52C4(	6FACCDE498B52C4C374F464BA89834C4743B1A39E
/k163_point_multiplication/yyP	6A89FFC8A60987D4	6A89FFC8A60987D484D23B275D8446A881360F9B0
/k163_point_multiplication/next_xQ	5BD996152BAF6E7B	4B5CB09C9E69E97DD425008B427132317315174 4A · 6FACCDE49… · 5BD996152BAF6E7B65B15C1E6B8…
/k163_point_multiplication/next_yQ	0012009F40A75E37	10972616F561D931895631C75EE64816FC8093C18 · 34675B6EF… · 0012009F40A75E3738C26D52771…
/k163_point_multiplication/xxPxor…	0525322C3EBCAB98	0525322C3EBCAB98B39D7D6CF51C726CF50D15A2E
/k163_point_multiplication/square…	1359B189984DE545	1359B189984DE54527E643B564B909F7D0A30F628
/k163_point_multiplication/square…	5EFCA4391513C5E3	5EFCA4391513C5E3D62C21729E967A049C08210CE
/k163_point_multiplication/y1	6A89FFC8A60987D4	6A89FFC8A60987D484D23B275D8446A881360F9B0
Now	155800 ps	
Cursor 1	0 ps	

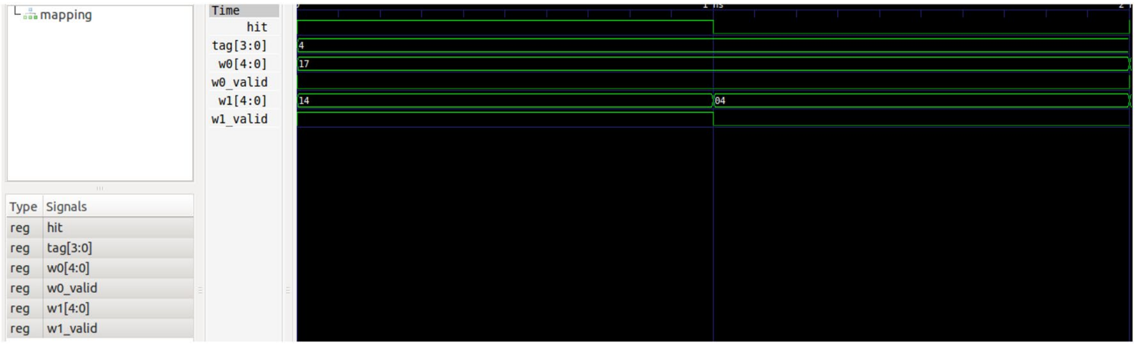
Fig. 14 Simulation result

The including system gives the second bit of last outcome

Step 3 Increase the MSB of the multiplicand and the multiplier. The creation is added to the past multiplier to accomplish in stage 2 additional system. By then, aggregate and correspondence are evaluated as the third and quarter piece of the finishing thing.

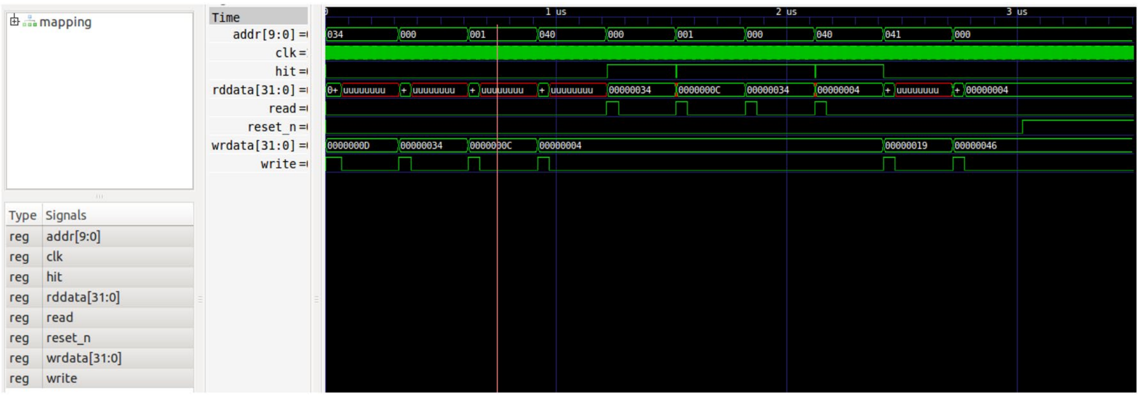
Figure 9 shows the outline of the 2×2 increase by using a Vedic multiplier Fig. 9.

The 4×4 DVM of the block diagram is showed up in Fig. 10. In segment 2.1.5, the estimation of the Dual Field Vedic multiplier is presented. As demonstrated by this diagram, the Verilog code is made to affirm the results. This



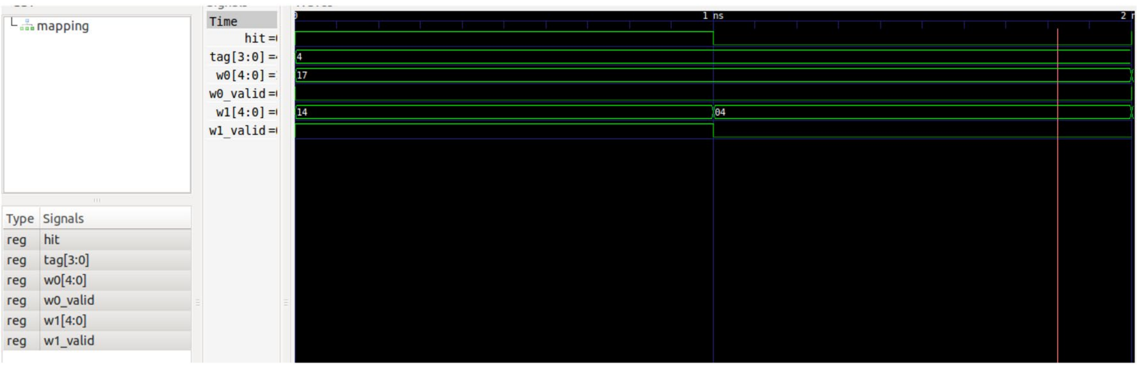
Type	Signals
reg	hit
reg	tag[3:0]
reg	w0[4:0]
reg	w0_valid
reg	w1[4:0]
reg	w1_valid

Fig. 15 Simulation results of hit—miss logic result



Type	Signals
reg	addr[9:0]
reg	clk
reg	hit
reg	rddata[31:0]
reg	read
reg	reset_n
reg	wrdata[31:0]
reg	write

Fig. 16 Simulation results of RAM—cache

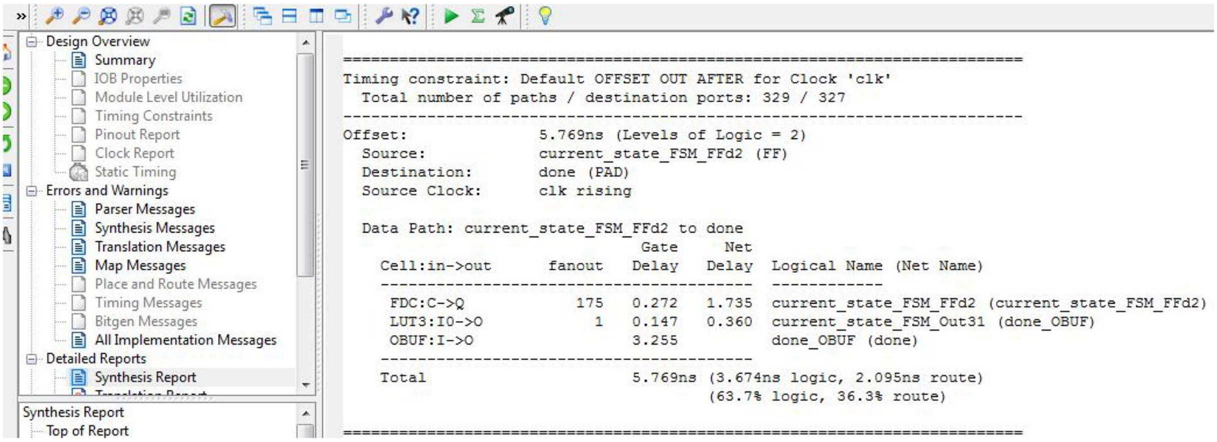


Type	Signals
reg	hit
reg	tag[3:0]
reg	w0[4:0]
reg	w0_valid
reg	w1[4:0]
reg	w1_valid

Fig. 17 Simulation results of tag valid array

block contains four 2×2 multiplier block and three viper block. In this diagram, a_0 to a_3 and b_0 to b_3 address as four-bit input regard.

4x4 dual field Vedic multiplier block diagram is appeared in Fig. 11. From the outset, Least Significant Bit (LSB) of the two data (a0, a1 and b0, b1) is given to the commitment of 2×2 multiplier block to perform increment movement. In the subsequent stage, a2, a3 and b0, b1, third stage a_0, a_1 and b_2, b_3, at definite stage a_2, a_3, and b_2, b_3 values play out the 2×2 multiplier movement. Last two stage multiplier puts away one adder similarly as the starting two-stage multiplier sets aside in one more adder. The two adders results gives the commitment of the last adder. Finally, 8-bit results are passed on in the yield of the DVM structure. The proposed FPGA execution of LCSLA technique based execution estimations are generous than the current procedure (Karthikeyan and Jagadeeswari 2020).



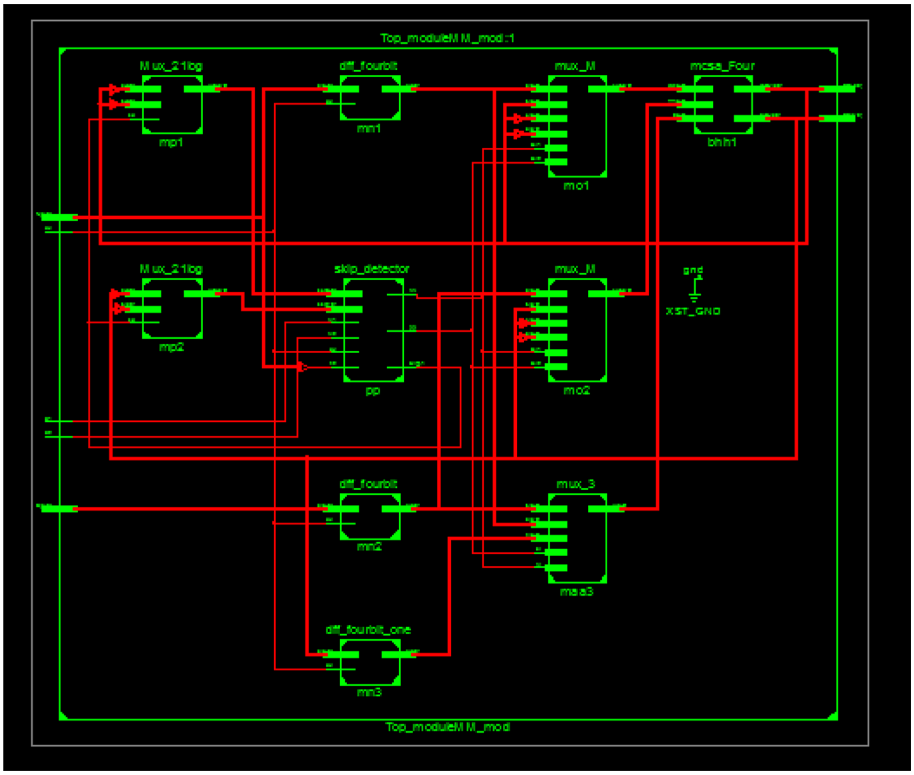
```
==========================================================================
Timing constraint: Default OFFSET OUT AFTER for Clock 'clk'
  Total number of paths / destination ports: 329 / 327
--------------------------------------------------------------------------
Offset:                 5.769ns (Levels of Logic = 2)
  Source:               current_state_FSM_FFd2 (FF)
  Destination:          done (PAD)
  Source Clock:         clk rising

  Data Path: current_state_FSM_FFd2 to done
                                Gate     Net
    Cell:in->out      fanout   Delay   Delay  Logical Name (Net Name)
    ----------------------------------------  ------------
     FDC:C->Q            175   0.272   1.735  current_state_FSM_FFd2 (current_state_FSM_FFd2)
     LUT3:I0->O            1   0.147   0.360  current_state_FSM_Out31 (done_OBUF)
     OBUF:I->O                 3.255          done_OBUF (done)
    ----------------------------------------
    Total                      5.769ns (3.674ns logic, 2.095ns route)
                                       (63.7% logic, 36.3% route)

==========================================================================
```

Fig. 18 Point multiplication delay obtained with DVM-LCSLA

Fig. 19 RTL schematic of DVM-LCSLA



3.1 Cache memory for elliptic curve cryptography with error correction scheme

In this work, first, the whole multiplication algorithm has been unrolled with the goal that no additional cycles are squandered for circle tasks. Second, we reused the working registers as a memory cache to diminish the quantity of fundamental burden tasks. A wide range of hashing capacities can be utilized to plan address to various areas in the cache ways. It has been recently demonstrated that XOR planning accomplish less miss rates when contrasted with the set-acquainted cache structure. Since the ECC data is stored with every data zone stored in the cache, values are encoded before they are composed inside the storage space so as to create the ECC bits.

Error correcting codes utilized for this reason for existing are themselves hashing capacities that create a piece vector from another information vector. As this hashing is accomplished for fault identification purposes, we propose to utilize the ECC encoding circuit as the hashing capacity of the slanted cache and expel the stored ECC bits from the cache structure all together and utilize the ECC bits for ordering. Figure 12 shows the proposed architecture where the registered ECC bits for the tags are not, at this point stored inside the cache ways however rather the ECC is utilized as the hashing capacity and the figured ECC pieces are utilized as the records to the cache ways.

The Fig. 13 shows the overall work flow of side channel attack against cache. Upon reading of the tag, the read esteem is checked for any conceivable delicate errors before the stored tag is looked at against the tag some portion of the memory address for a potential cache hit result. This new technique, diminishes the successful territory of the cache and makes it less inclined to delicate errors.

4 Results and discussions

The proposed elliptic curve cryptography with multiplier design has been captured in Verilog hardware description language (HDL), and implementation has been done on Xilinx ISE Design Suite 14.1 targeting Virtex-6 FPGA device.

The simulation output result of proposed Vedic multiplier is shown in above Fig. 14. This multiplier is used in ECC architecture. As a result, the proposed dual field Vedic multiplier—look up table carry select adder can achieves a higher throughput and much smaller area-time product (ATP) than previous strategies

The simulation response of hit–miss logic is shown in Fig. 15. During 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

The simulation response of RAM-cache is shown in Fig. 16. By using this proposed dual field Vedic multiplier—look up table carry select adder the performance of cache is improved perfectly

The simulation response of tag valid array is shown in Fig. 17. The tag substantial cluster has been utilized for getting to the information from the information array and keeping up the bits.

The simulation output result of point multiplication delay in proposed DVM-LCSLA multiplier is shown in above Fig. 18.

The RTL schematic diagram of proposed DVM-LCSLA multiplier is shown in above Fig. 19. As compared to other multipliers, the proposed DVM-LCSLA multiplier has a low area because of less number of adder levels in the underlying algorithm.

The floor plan view of proposed dual field Vedic multiplier-look up table carry select adder based cryptography is shown in Fig. 20.

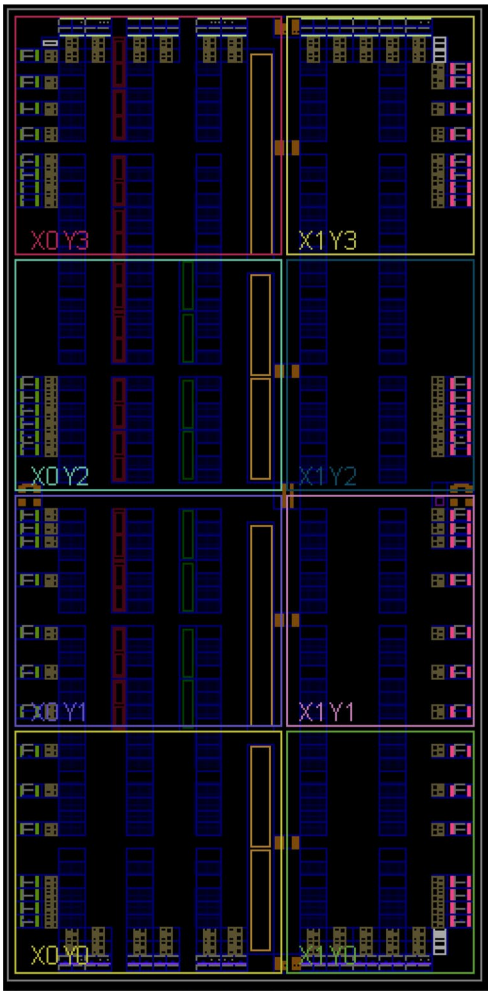


Fig. 20 DVM-LCSLA-floor plan view

Table 1 and Fig. 21 discuss the performance analysis of power consumption. This comparison clearly states that the proposed dual field Vedic multiplier-look up table carry select adder based memory design obtain the best results against power consumption as compared with existing methods, for example total power consumption of proposed system is 18.63 μW.

Figure 22 discuss the performance analysis of time complexity. In this comparison, it clearly states that the proposed dual field Vedic multiplier-look up table carry select adder based memory design obtain best results against time complexity as compared with existing methods, for example overall time complexity of proposed system is 6 s only.

Figure 23 discusses the performance analysis of Area overhead. This comparison clearly states that the

Table 1 Performance analysis of power consumption

Parameters	Two way tagged cache (μw)	Undeviating adaptive sheltered cryptography (μw)	DVM-LCSLA(μw)
Read time power	35.501	21.231	15.61
Write time power	35.0531	20.121	17.20
Total power Consumption	46.231	23.021	18.63

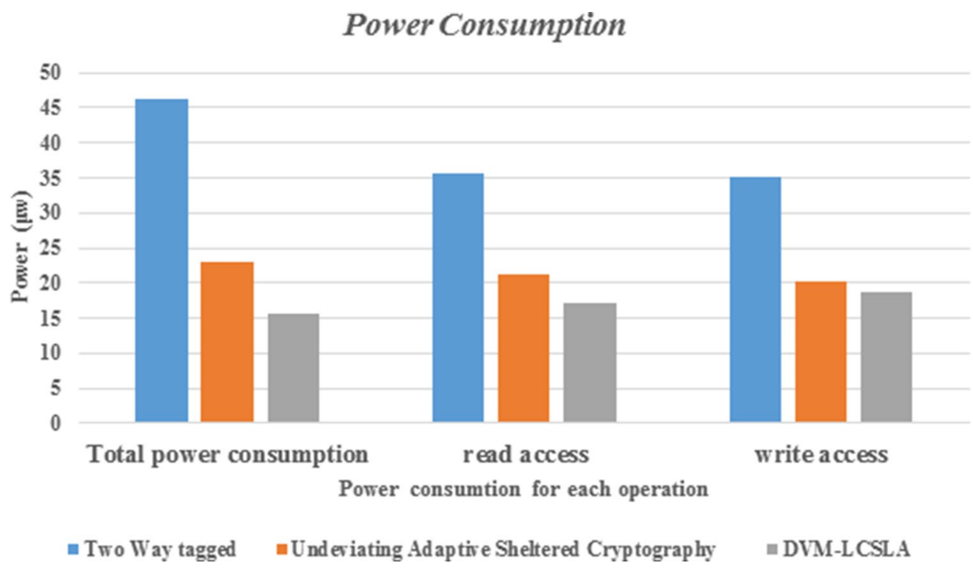


Fig. 21 Performance analysis of power consumption

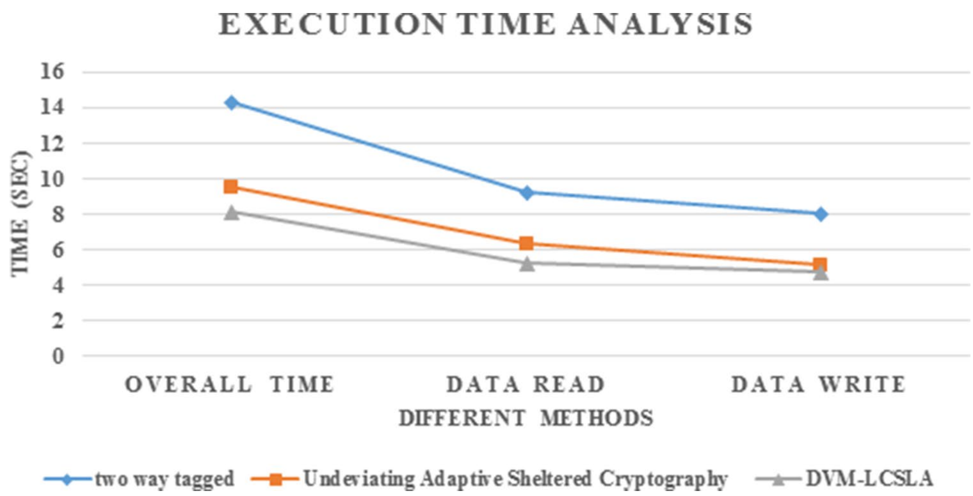


Fig. 22 Performance comparison of time analysis

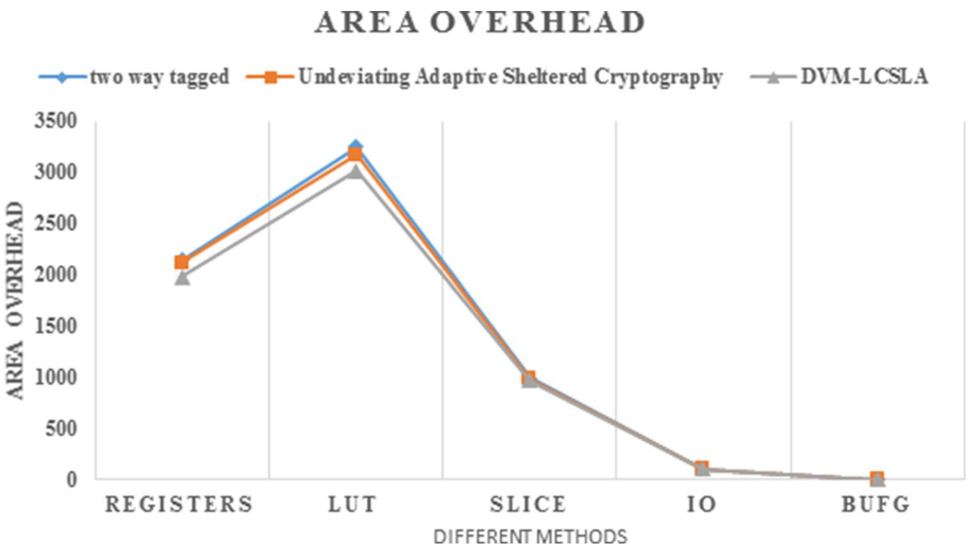


Fig. 23 Performance comparison of area overhead

proposed dual field Vedic multiplier-look up table carry select adder based memory design produce best results against area overhead as compared with existing methods

5 Conclusion

This work introduces dual field Vedic multiplier-look up table carry select adder architecture for cryptography based system. The proposed DVM-LCSLA is developed based on Xilinx software by using Verilog code. In this method, the multiplier is used to perform the multiplication operation, where, this multiplier, as an alternative to the accumulator, the LCSLA accumulator was used to evaluate constraints such as controller power and interrupted delay. Among existing methods, DVM-LCSLA method give better results in FPGA and ASIC performances. In FPGA implementation, factors like requirement of LUT, flip-flops, and frequency have been improved in DVM-LCSLA. Hence the hardware area overhead reduction (86.01%), Power Reduction (74.63%) and time delay (29.61%) are reduced in proposed DVM-LCSLA with 180 nm technology, and Hardware Area overhead Reduction (46.77%), Power Reduction (78.42%) and time delay (21.23%), are reduced than the conventional methods in 45 nm technology. In the future work, ECC architecture and internal blocks will be optimized to minimize the ASIC and FPGA performances further.

References

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

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

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

Debiao H, Zeadally S (2015) An analysis of RIFD authentication schemes for internet of things in healthcare environment using elliptic curve cryptography. IEEE Internet Things J 2(1):72–83

Debiao H, Wang H, Khan MK, Wang L (2016) Lightweight anonymous key distribution scheme for smart grid using elliptic curve cryptography. IET Commun 10(14):1795–1802

Esmaeildoust M, Schinianakis D, Javashi H, Stouraitis T, Navi K (2013) Efficient RNS implementation of elliptic curve point multiplication over GF(p). IEEE Trans Very Large Scale Integr Syst 21(8):1545–1549

Guitouni Z, Chotin-Avot R, Machhout M, Mehrez H, Tourki R (2011) High performances ASIC based elliptic curve cryptographic processor over GF(2m). International Journal of Computer Applications, Foundation of Computer Science, 2011, Special Issue on Network Security and Cryptography (NSC) (4), pp 1–10. https://doi.org/10.5120/4342-039

Hosspain MS, Kong Y (2015) High-performance FPGA implementation of modular inversion over F_256 for elliptic curve cryptography. In: 2015 IEEE international conference on data science and data intensive systems (DSSP). IEEE

Karthikeyan S, Jagadeeswari M (2020) Performance improvement of elliptic curve cryptography system using low power, high speed 16×16 Vedic multiplier based on reversible logic. J Ambient Intell Human Comput. https://doi.org/10.1007/s12652-020-01795-5

Kimmo UJ, Mozaffari-Kermani M (2014) Efficient algorithm and architecture for elliptic curve cryptography for extremely constrained secure applications. IEEE Trans Circuits Syst I Regul Pap 61(4):1144–1155

Kuang S-R, Wu K-Y, Lu R-Y (2016) Low-cost high-performance VLSI architecture for Montgomery modular multiplication. IEEE Trans Very Large Scale Integr Syst 24(2):434–443

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

Lee JW, Chung SC, Chang HC, Lee CY (2014) Efficient power-analysis-resistant dual-field elliptic curve cryptographic processor using heterogeneous dual-processing-element architecture. IEEE Trans Very Large Scale Integr Syst 22(1):49–61

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

Meher, PK, Lou X (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 I Regul Pap 64(2):399–408

Perianin T, Carré S, Dyseryn V et al (2020) End-to-end automated cache-timing attack driven by machine learning. J Cryptogr Eng. https://doi.org/10.1007/s13389-020-00228-5

Sai RV et al (2019) Undeviating adaptive sheltered cryptography (UASC) method based low power and high secure cache memory design. Microprocess Microsyst 71:102876

Shukla V, Singh O, Mishra G, Tiwari R (2020) A novel approach for reversible realization of 4 × 4 bit Vedic multiplier circuit. In: Advances in VLSI, communication, and signal processing. Lecture notes in electrical engineering, vol 587, pp 733–746. https://doi.org/10.1007/978-981-32-9775-3_67

Sonali SK, Shekhar HB (2016) High speed, low power Vedic multiplier using reversible logic gate. Int J Sci Res (IJSR) 5(9):570–573

Sonali SK, Kharat GU, Bodakeonali SH (2016) A review on Vedic multiplier using reversible logic gate. Int J Innov Res Sci Eng Technol 5(4):5838–5844

Sree K, Mrudula ST, Geetha K, Ramachandra R (2017) Speed efcient 64 Bit MAC design using Vedic multiplier and reversible logic gates. Int J Adv Res Innov Ideas Educ 3(6):370–376

Vijeyakumar KN, Kalaiselvi S, Saranya K (2016) VLSI implementation of high speed area efficient arithmetic unit using Vedic mathematics. ICTACT J Microelectron 2(1):198–202

Yeh H-L, Chen T-H, Kuei-Jung H, Shih W-K (2013) Robust elliptic curve cryptography-based three factor user authentication providing privacy of biometric data. IET Inf Secur 7(3):247–252

Zhu Y, Ahn G-J, Hu H, Ma D, Wang S (2013) Role-based cryptosystem: a new cryptographic RBAC system based on role-key hierarchy. IEEE Trans Inf Forensics Secur 8(12):2138–2153