ISSN:0975-9646

A Survey on Various Algorithms Used for Elliptic Curve Cryptography

Christina Thomas[#1], Gnana Sheela K[*2] , Saranya P Krishnan[#3]

[#]*Department of ECE, Cochin University of Science and Technology*
Toc H Institute of Science of Technology
PO Box-682313, Kerala, India
[*] *Department of ECE, Cochin University of Science and Technology*
Toc H Institute of Science of Technology
PO Box-682313, Kerala, India

***Abstract*-- This survey paper reviews latest existing encryption techniques and their security issues. Elliptic Curve Cryptography is gaining attraction with their high level of security with low cost,small key size and smaller hardware realization. A review on various algorithms to perform scalar multiplication on both prime fields and binary fields more effectively has been done. Initially, the double and add algorithm performed in different multipliers always resulted in a long serial point operations and also maintained a challenging critical path delay. But later on, efficient high speed Elliptic Curve Cryptographic processor for binary fields in projective coordinates to improve performance of scalar multiplication has been designed. The recently proposed architecture considers the karatsuba multiplier which is designed for high speed and area constrained applications that reduces the number of clock cycles and the multiplication steps. The new architecture provides integrated high throughput with high power efficiency.**

***Keywords*—Binary Field, Elliptic Curve Cryptography, Encryption, Karatsuba Multiplier .**

I. INTRODUCTION

Cryptography is the science which allows only authenticated access to information. Earlier encoding was used to exchange confidential matters amongst government agencies. Today,it is an important feature in everyday life.This is due to the necessity of transferring messages such as credit card numbers,bank transactions securely over the network. The authorised access of information is carried out by a small secret information known as key.Information to be secured known as plain text is transformed into unintelligent information known as cipher text by encryption operation with key as the secret parameter.The original plaintext can be retrieved back from the cipher text using decryption with the help of decryption key.

The two categories of Cryptography algorithm are symmetric (private) and asymmetric (public) cryptosystems. In symmetric systems a single key is used to encrypt/decrypt the plain text to/from cipher text.Both the communicating parties have access to the secret keys is one of the main limitation of private key cryptography. In asymmetric systems encryption and decryption operations done with two separate keys one of which is public and other is private key. The private key owned by its owner and the public key is known for all other parties. When sender X needs to send data to receiver Y, he encrypts his message with Y's public key. This message will be decrypted only with Y's private key. Thus Y only can read the message even if there is a third party spy on the channel. Elliptic Curve Cryptography (ECC) is preferred when compared with conventional asymmetric cryptosystems such as RSA because of lower power consumption and higher speed which are useful for wireless applications.

Elliptic Curve Cryptography (ECC) is gaining attraction with their high level of security with small low cost, key size and smaller hardware realization.ECC is one of the most advanced research topic in VLSI. Over the last 2 decades, Elliptic Curve Cryptography has emerged from a mere curiosity into a secure family of public key cryptosystems used in practical applications. It was first proposed independently by N. Koblitz and V. Miller in 1985. ECC provides more security per key bit compared to other public key standards.ECC has become attractive in applications such as smart cards ,set top boxes, low power portable devices(cell phone). In all those applications, an elliptic curve scalar multiplier serves as a basic building block for secret key exchange, authentication and certification.

Hardware implementation of ECC has also attained considerable interest and Field-programmable gate arrays (FPGAs) form an ideal platform for implementing cryptographic algorithms because of its programmability and high speed and also they are resource constrained. On FPGAs inherent parallelism and custom design of hardware architecture speeds up the execution of ECC.

Elliptic curve scalar multiplication kP, where k is a scalar(integer) and P is a point on the curve, is the most important operation in elliptic curve cryptosystems. In order to compute elliptic curve scalar multiplication, majority of designs use the three-layer hierarchical strategy depicted in Fig.1.Scalar multiplication includes repeated point additions and point doublings.

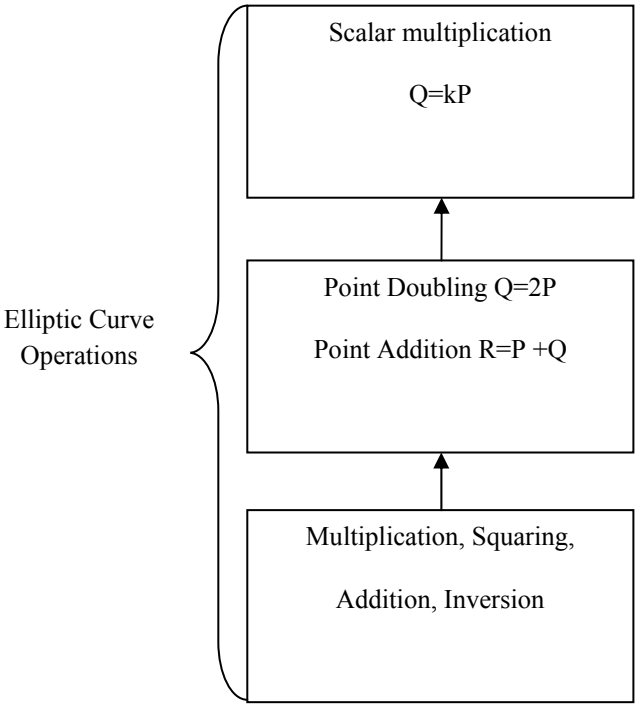

Fig. 1 Three-Layer Model for Elliptic Curve Scalar Multiplication

Elliptic curves defined only on finite fields are employed for cryptography to make the operations on elliptic curves accurate and more efficient. According to the two finite fields that offer secure implementation are prime field (F_p) and Binary field (F_2^m).Elliptic curves over binary fields $F2^m$ or prime fields Fq can be represented by one of the following equations:

$$y^2 + xy = x^3 + ax^2 + b \quad (1)$$

$$y^2 + y = x^3 + ax + b \quad (2)$$

Points on an elliptic curve are expressed in terms of their coordinates P(x, y). 'a' and 'b' are the points on elliptic curve.Elliptic curve arithmetic involves addition of two points on a curve to yield another point on the curve.

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 + \left(\frac{y_2 - y_1}{x_2 - x_1}\right) + x_1 + x_2 \quad (3)$$

$$y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 + x_3) - y_1 \quad (4)$$

and doubling of a point to yield another point:

$$x_3 = \left(x_1 + \frac{y_1}{x_1}\right)^2 + \left(x_1 + \frac{y_1}{x_1}\right) + a_2 \quad (5)$$

$$y_3 = x_3\left(x_1 + \frac{y_1}{x_1} + 1\right) + x_1^2 \quad (6)$$

In the next section, this review focuses on some of the recent existing encryption techniques and their security issues. Various algorithms are proposed to perform scalar multiplication on both prime fields and binary fields more effectively. This paper also explains different multipliers implemented in order to perform trade off analysis of area and performance for elliptic curve cryptography and also different processor architectures are also discussed.

The paper is organized as follows. Section II presents related work on existing research papers. In Section III, comparative analysis of different parameters of selective architectures is done. Finally the conclusion over the discussion is given in the section IV.

II. RELATED WORK

Lijun Gao et al (1999) developed high-speed elliptic curve scalar multipliers with maximal flexibility,least development time and low hardware cost [1]. A compact speedy elliptic curve scalar multiplier with variable key size is implemented in the form of a coprocessor using a Xilinx FPGA. This implementation consumes the internal SRAM or registers of the FPGA and has the whole scalar multiplier implemented using a single FPGA chip. A pipelined digit-serial modified Massey-Omura multiplier is constructed and is used in the design. The algorithms of EC scalar multiplication and EC addition/subtraction are used in this design. The scalar multiplier is implemented with a parameterized VHDL description and is then mapped to a Xilinx FPGA. By changing the parameter for key size and by re- synthesis, a different instance can be acquired.

In 2000, Orlando G et al proposed a processor architecture for elliptic curves cryptosystems over fields $GF(2^m)$ [2].The important features of this architecture are the use of a digit-serial multiplier, an optimized bit-parallel squarer and two programmable processors. The squarer and the multiplier architectures can be optimized for any field polynomial or field order by reconfiguration.The implementation results show that this architecture executes the projective coordinates version of the Montgomery scalar multiplication algorithm and can perform elliptic curve scalar multiplications with arbitrary points in 0.21 m sec in the field $GF(2^{167})$.

Orlando G et al (2001) developed a new elliptic curve processor architecture for the computation of point multiplication for elliptic curves defined over prime fields [3]. This is a scalable architecture in terms of area and speed specially designed for memory-rich hardware platforms. This processor uses a recent type of high-radix Montgomery multiplier that depends on the pre computation of commonly used values and on the use of multiple processing engines. The results show that the computation of a point multiplication in a curve defined over $GF(2^{192}-2^{64}-1)$ could be computed in about 3 m sec using the projective coordinates algorithms and the double-and-add algorithm.

Hodjat A et al (2005) introduced a high performance and scalable elliptic curve processor which is designed to be resistant against timing attacks [4]. The point multiplication algorithm (double-add-subtract) is modified so that the processor performs the same operations for every 3 bits of the scalar k independent of the bit pattern of the 3 bits. As a result, it is not possible to extract the key pattern using a timing attack. The architecture of this processor is based on the Galois Field of $GF(2^n)$ and the bit-serial field multiplier

and squarer are designed. The processor is configurable for all values of n(number of bits) and the delay of point multiplication is [18(n+3) + (n+3)/2 + 1]×(n/3) clock cycles.

In 2006, Schinianakis D M et al presented a VLSI Residue Number System (RNS) architecture of an Elliptic Curve Point Multiplier [5]. In the proposed approach,in order to replace typical finite field circuits with RNS ones, necessary mathematical conditions that need to be satisfied are carried out. It has shown that such an application is feasible and leads to a significant improvement in the execution time of a scalar point multiplication. The important results are derived from the synthesis tool, proving the efficiency of the proposed implementation in terms of delay.

Sandoval M M et al (2007) explained a hardware architecture for GF(2^m) multiplication and its evaluation in a hardware architecture for elliptic curve scalar multiplication [6]. The architecture is a parameterizable digit-serial implementation for any field order, m. Here,digit serial multiplication algorithm is used.The results show that the size of the digit to use in an application of the proposed multiplier architecture will be determined by the area assigned to the multiplier and also the latency of the multiplier is reduced by the size of the digit.

In 2008,Ansari B et al proposed a high-performance scalar architecture for elliptic curve scalar multiplication based on the Montgomery ladder method over finite field GF(2^m) [7] . A pseudo pipelined word-serial finite field multiplier, with word size w, apt for the scalar multiplication is also developed. The hardware implementation shows that, the proposed scheme performs a scalar multiplication in 25(m-1) clock cycles, which is approximately 2.75 times faster than a straightforward implementation.

Xu W et al (2009) derived a pseudo-pipelined VLSI architecture of two Elliptic Curve Scalar Multiplications over GF(2^m) with uniform addressing [8]. The proposed architecture includes three word-serial finite field (FF) multipliers, having a word size w for each FF multipliers. Compared with 25(m-l) clock cycles to compute one Elliptic Curve Multiplication(ECMLT) in paper [7], it takes only 20(m-l) clock cycles to compute two ECMLTs using this pipelined architecture. So it is proved that the computation time for two ECMLTs is the shortest by using this approach.

In 2010,Fan H et al described a simple way to split input operands and this allows for fast VLSI implementations of subquadratic Karatsuba-Ofman multipliers[9].Initially perform a few Karatsuba-Ofman's Algorithm (KOA) iterations to reduce the whole space complexities, and then a quadratic multiplication algorithm on small input operands to achieve relatively high speed performance. This hybrid approach can provide a trade-off between the time and space complexities, by selecting different stop conditions for the KOA iterations. The proposed algorithm uses a simple and straightforward method to split input operands. The theoretical XOR gate delay of the proposed subquadratic Karatsuba- Ofman multiplier is reduced significantly. It is reduced by about 33% and 25% for n = 2t and n = 3t (t > 1), respectively. The proposed method can be used for practical VLSI applications, like designs of hybrid GF(2^n) multipliers.

MuthuKumar B et al(2010) presented an elliptic curve cryptography (ECC) coprocessor, which is a dual-field processor with projective coordinates[10]. An architecture for scalar multiplication is also implemented.The coprocessor can be adapted both prime field and binary field.It also contains a control unit with 256 bit serial and parallel operations , The experimental result shows that the EC point scalar multiplication with coordinate conversion can be done with 368 μs at 75MHz with core power of 68.4mW over GF(p) and in 252μs at 114 MHz with 58.2mW over GF(2^m).Both can be achieved under the 1.6V supply voltage in the parallel mode with 4 Arithmetic Units. The core power also can be further reduced to 48mW over GF(p) and 38mW over GF(2m), respectively. The synthesis result shows that proposed design provides integrated high throughput with low power consumptions.

In 2010,Rahuman A.K et al proposed an architecture based on Lopez-Dahab elliptic curve point multiplication algorithm and uses Gaussian normal basis for GF(2^{163}) field arithmetic[11].Two new word-level arithmetic units over GF(2^{163}) has been designed and in order to achieve high throughput ,parallelized elliptic curve point doubling and addition algorithms with uniform addressing based on Lopez-Dahab method are derived. Implementation results show that this architecture uses 16,209 slices and has a maximum frequency of 143 MHZ. The design is roughly 4.8 times faster with two times increased hardware complexity and GF (2^{193}) research was based on using the efficient Montgomery add and double algorithm, the Karatsuba- Offman multiplier and the Itoh-Tsjuii algorithm for the inverse component. 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 like key generation, encryption and decryption.

In 2010, Zhang Y et al developed a high performance elliptic curve cryptographic processor over GF(2^{163}) [12]. It has three finite field (FF) RISC cores and a main controller to achieve instruction-level parallelism (ILP) for elliptic curve point multiplication.A FF arithmetic instruction set AB, A + B, $(A + B)^2$ and A^4 for parallelized algorithm for ECC point multiplication is developed ,where the $(A + B)^2$ and A^4 are proposed to decrease clock cycles needed in the loop of algorithm and Itoh–Tsujii's finite field inversion respectively while not affecting critical path of the system. The interconnection among three FF cores and the main controller is obtained based on the analysis of both critical path and data dependency. The implementation shows that proposed architecture can finish one ECC point multiplication in 1428 cycles, and the performance is nearly five times faster with six times larger in area than the implementation reported in literature [7].

Hamilton M et al (2011) provided a comparison between different modular multipliers, when working with a Mersenne prime modulus, suitable for use in an elliptic

curve processor[13]. Mersenne primes allow for the use of fast modular reduction techniques.The multipliers presented here includes serial multiplier, Booth multiplier and Montgomery multiplier and they are compared against speed, area and power consumption. The results show that the Montgomery, Booth2 and Serial multipliers are all closely matched in the power they consume. However the area used by these multipliers is much higher than the circuits that implement the multiplication in a serial way. The standard deviation of the power consumption of the Booth2 multiplier was lowest for a bit length of 127 bits and as a result it reduces the possibility of the circuit being susceptible to power analysis attacks. The Montgomery multiplier design has the merit of being able to perform modular multiplications.When working with a modulus of special form such as 2n-1, the most efficient design is a Booth2 multiplier. The Booth2 design has a low area similar to a serial multiplier but a much higher throughput due to the recoding used. Performing the full n*n-bit multiplication and reduction in a single clock cycle with a fully parallel multiplier would give a very high throughput but also a long critical path.

Rezai et al (2011) explained an approach using a novel finite field multiplication and a high performance scalar multiplication algorithm for wireless network authentication on prime fields [14]. Constant Length Non Zero (CLNZ) sliding window method is used on the signed-digit multiplier in order to reduce the multiplication steps. Also, point addition and point doubling operation are computed in parallel.Window technique and signed-digit representation are used in order to reduce the number of point operation.The results show that the proposed finite field multiplication reduces the number of multiplication steps at about 40%-82.4% in compare with Montgomery modular multiplication algorithm.Also the efficiency of the proposed implementation approach enhances about 88%-97% in compare with the implementation approach of traditional window Non Adjacent Form(NAF) elliptic curve scalar multiplication algorithm and enhances about 77% in compare with the implementation approach of window NAF elliptic curve scalar multiplication.

In 2012 Chung S Z et al proposed a new elliptic curve cryptographic (ECC) processor architecture [15]. This processor contains a 3 pipelined-stage full-word Montgomery multiplier and supports both finite field operations and elliptic curve scalar multiplication over prime field. The proposed processor is resistant to the simple power analysis (SPA) attack by using the Montgomery ladder-based elliptic curve scalar multiplication. Both hardware sharing and parallelization techniques are used to improve the hardware performance.One of the main merit of this scheme is pre-computations for domain conversion has overcome and generating constants by performing several modular multiplication and modular addition in hardware with reused arithmetic unit. Upon synthesis the processor performs a 256-bit ECSM in 120μs over prime field with 540K gate counts.

Mahdizadeh H et al(2013), presented a new and highly efficient architecture for elliptic curve scalar point multiplication[16]. Here in order to achieve the maximum architectural and timing improvements,the critical path of the Lopez–Dahab scalar point multiplication architecture are reordered and reorganized such that logic structures are implemented in parallel and operations in the critical path are diverted to non critical paths. The proposed design can compute scalar multiplication over GF (2^{163}) in 9.6 μs with maximum achievable frequency of 250 MHz. Another implementation variant for less resource consumption is also proposed; with $G = 33$, ,where G is the digit size of the underlying digit-serial finite-field multiplier, the design performs the same operation in 11.6 μs at 263 MHz on the same platform. The synthesis results show that, in the first implementation, 17 929 slices or 20% of the chip area is occupied, which makes it suitable for speed-critical cryptographic applications, while in the second implementation 14,203 slices or 16% of the chip area is utilized, which makes it suitable for applications that may require speed–area trade off.

Roy S S et al(2013) designed a high speed ECC processor for binary fields on FPGA [17].This paper uses a theoretical model to approximate the delay of different characteristic two primitives used in an elliptic curve scalar multiplier architecture (ECSMA) implemented on k input lookup table (LUT)-based field-programmable gate arrays.Here a pipelined bit parallel karatsuba multiplier and Itoh-Tsuji's algorithm is used. By using karatsuba multiplier the multiplication steps and number of clock cycles are reduced. Experimental results for GF(2^{163}) show that, when the ECSMA is suitably pipelined, optimized field primitives and enhanced scheduling of point arithmetic ,the scalar multiplication can be performed in only 9.5 μs.

Reyes A C(2013) et al evaluated 5 different software implementations of algorithms to compute scalar multiplication over prime and binary fields in cryptographic schemes based on Elliptic Curve Cryptography (ECC) [18]. For evaluation, the key generation algorithm in ECC consisting on a single scalar multiplication was implemented on a P500h LG smarthphone, which includes an ARM processor running at 600MHz. It was found that, scalar multiplication runs 8 times faster for ECC defined over prime fields, being the NAF the best performer method. For ECC over binary fields, the best performer method was wNAF. Less arithmetic operations are needed to calculate the scalar multiplication .However, both *NAF* and *wNAF* method require more memory.

In 2013 Rezai A et al analysed a new and efficient implementation approach for the elliptic curve cryptosystem (ECC) based on a novel finite field multiplication in GF(2^m) and an efficient scalar multiplication algorithm [19]. This new finite field multiplication algorithm performs zero chain multiplication and required additions in only one clock cycle instead of several clock cycles. By using modified Barrel shifter; the partial result is also shifted in one clock cycle. Both the canonical recoding technique and the sliding window method are used to the multiplier to reduce the average number of required clock cycles. Here point addition and point doubling operations are computed in parallel. The

sliding window method and the signed-digit representation are also applied to reduce the average number of point operations. Based on the analysis, the computation cost is effectively reduced in both the proposed finite field multiplication algorithm and the proposed implementation approach of ECC.

Leca C L et al (2014) evaluated point operations and proposed an efficient algorithm for combining simple operations such as point tripling (3P),quadrupling (4P), double and add (2P+Q), in order to obtain a significantly less time-consuming method for scalar multiplication, and this aims at reducing the number of inversions required for the operation[20]. The proposed algorithm made an efficient use of the previous point operations as long as the scalars factorization is achieved by one of the integers: 4, 3, 2 in the presented order. The proposed algorithm also managed to increase the overall performance of scalar multiplication and reduce the complexity of the operation by lowering the number of inversions involved compared to the double and add algorithm.

In 2014,Lee J W et al proposed a new heterogeneous dual-processing element (dual-PE) architecture and a priority-oriented scheduling of right-to-left double-and-add-always EC scalar multiplication (ECSM) with randomized processing technique[21]. By this, a power-analysis-resistant dual-field ECC (DF-ECC) processor is achieved. For this dual-PE design, a memory hierarchy with local memory synchronization scheme is also used to improve data bandwidth. After implementation, the proposed processor with 0.41 mm^2 core area executed one complete ECSM operation including data domain conversion in 0.34 ms over GF(p^{160}) and 0.29 ms over GF(2^{160}).

Liao K eta al (2014), a high-speed constant-time division module with optimized architecture is proposed[22]. The presented algorithm computes a single multiplicative inverse or division in constant m iterations, i.e. m clock cycles, in GF(2^m), which obtains a drastic reduction (specifically more than 50%) on computing time. This novel division module achieves lower area-time complexity, which makes it a good option for high performance ECC design**.**

Munoz P R et al(2014) presented the design of crypto processors using two multipliers over finite field GF(2^{163}) with digit-level processing[23]. The arithmetic operations were implemented in hardware using Gaussian Normal Bases (GNB) representation and the scalar multiplication kP was performed on Koblitz curves using window-NAF algorithm with window size(w) = 2, 4, 8 and 16 on koblitz curves. The hardware implementation results show that the designed crypto processors present a very good trade-off between computation time and area, obtaining a higher performance. The designed crypto processors use roughly the 17% of the Arithmetic LUTs of the FPGA, and the best one performs the scalar multiplication in 5.05 µs for w = 16.

In 2014,Pontie S et al described the implementation of a new scalar multiplication algorithm based on randomized windows method[24]. The scalar multiplication uses a table of precomputed points in order to accelerate the processing of the key vector. Here, the processing of a specific bit of the k coefficient will occur at different time offsets for each computation. This desynchronizes the power traces and hence makes harder to develop a differential side channel attack. Here, Jacobian coordinates are prefered to work with. The conversion from Jacobian to the traditional affine coordinates requires a modular inversion, but all the point computations do not, thus largely saving computation time.

Pontie S et al (2014) developed a coprocessor that supports all critical operations of an ECC cryptosystem [25].The proposed algorithm scans left-to-right the scalar with a window method. This algorithm is secure against SPA timing analysis attacks and DPA(Differential Power Analysis).Here one can choose the secure level against DPA attacks by forcing area or forcing time of computation.But the coprocessor uses more slices than other implementations and thereby consumes more area due to the pre compute table that occupies 53% of total area.

This section describes various high speed elliptic curve cryptographic processor architecture that provide integrated high throughput with low power consumption.Various approaches for finite field multiplication are also explained. All approaches have their own advantages and disadvantages. Out of all these Karatsuba multiplier is the best because it reduces the multiplication steps and the number of clock cycles.

III. COMPARATIVE ANALYSIS

In this section the essential parameters used to design elliptic curve cryptographic processor has been compared based on their result analysis. Area,performance and computation times are analysed against each architecture proposed by different authors.The experimental results show that design of Hodjat A [4] consumes large area compared to others explained in the literature.Performance of 10µs thereby 45% saving time is obtained in the approach explained by Roy S.S[12].

TABLE I COMPARISON OF DIFFERENT PARAMETERS

Author	Performance	Frequency	Area consumeed
Muthukumar B.(2010)	368µs-GF(p) 22µs-GF(2^m)	73MHz	-
Rahuman A.K(2010)	4.8 times faster	14.3MHz	16,209 slices
Chung S.Z(2012)	120µs	-	540K gate counts
Mahdizadeh H(2013)	9.6µs-first implementation 11.6µs-second implementation	250MHz-first implementation 263MHz-second implementation	17,929 slices-first implementation 14,203 slices- second implementation
Roy S.S et al (2013)	10µs with 45%saving time	-	3789 slices (50% saving area)
Lee J.W(2014)	.34ms-GF(p^{160}) .29ms-GF(2^{160})	-	.41 mm^2 core area

The double and add algorithm performed in different multipliers always resulted in a long serial point operations and also maintained a competitive critical path delay.As a result the hardware complexity of the design is increased. The elliptic curves defined on affine coordinates requires inversion operations which is time consuming and costly for hardware implementations. While using a digit serial multiplier it is not clear the best digit size to achieve a good performance that meets the constraints for a specific application. The main drawback while using window method in scalar multiplication is large area is consumed because of variable window size and also not able to perform an actual side channel attack.

Therefore, it is efficient to design a high speed Elliptic Curve Cryptographic processor for binary fields in projective coordinates to improve performance of scalar multiplication.In recent papers ,the karatsuba multiplier is designed for high speed and area constrained applications that reduces the multiplication steps and the number of clock cycles.The new architecture provides integrated high throughput with low power consumption.

IV. CONCLUSION

In this survey paper,a literature review on recent existing encryption techniques and their security issues had been presented. A review on various algorithms to perform scalar multiplication on both prime fields and binary fields more effectively had done. The recent papers focused on karatsuba multiplier for high speed and area constrained applications. It was observed that Montgomery ladder-based ECSMA results in 45% saving in time and 50% saving in area. The saving in area is achieved by the sub quadratic complexity of the Karatsuba multiplier and optimized field primitives.

ACKNOWLEDGMENT

The authors wish to acknowledge the Management of Toc H Institute of Science & Technology for their whole hearted support and also to the ECE department for guiding us in developing this journal.

REFERENCES

[1] L. Gao, S. Shrivastava, and G. E. Sobelman, *Elliptic Curve Scalar Multiplier Design Using FPGAs* , C.K. Koc and C. Paar Ed., Berlin Heidelberg :Springer-Verlag,1999.

[2] G. Orlando1 and C. Paar*, A High-Performance Reconfigurable Elliptic Curve Processor for GF(2^m),* C.K. Koc and C. Paar Eds., Berlin Heidelberg: Springer-Verlag, 2000.

[3] G. Orlando1 and C. Paar, *A Scalable GF(p) Elliptic Curve Processor Architecture for Programmable Hardware*, C.K. Koc and C. Paar Ed.,Berlin Heidelberg: Springer-Verlag, 2001.

[4] A. Hodjat, D. D. Hwang and I. Verbauwhede, "A Scalable and High Performance Elliptic Curve Processor with Resistance to Timing Attacks*",IEEE Proc. of the Int. Conf. on Information Technology: Coding and Computing* , vol.1,no.1,pp. 538-543,2005.

[5] D.M. Schinianakis, A.P. Kakarountas, and T. Stouraitis, "A New Approach to Elliptic Curve Cryptography: an RNS Architecture", *IEEE Electrotechnical Conf*., pp.1241– 1245,2006.

[6] M.M.Sandoval, C.F.Uribe, R. Cumplido and I.A.Badillo, "An Area/Performance Trade-Off Analysis of a GF(2^m) Multiplier Architecture for Elliptic Curve Cryptography",*Elsevier- Computers & Electrical Engineering ,* vol 35, issue 1, pp. 54–58,Jan. 2007.

[7] B.Ansari and M. A.Hasan, "High-Performance Architecture of Elliptic Curve Scalar Multiplication", *IEEE Trans. on Computers*, vol. 57, no. 11, pp. 1241 – 1245, 2008.

[8] W.Xu and Z.Yan, "A Pseudo-pipelined VLSI Architecture of Two Elliptic Curve Scalar Multiplications", *IEEE Int. Conf. of Electron Devices and Solid-State Circuits*, pp.258 – 261,2009.

[9] H.Fan, J.Sun, M.Gu and K.Y.Lam, "Overlap-free Karatsuba-Ofman Polynomial Multiplication Algorithms*", IET Information security*, vol. 4, no. 1, pp. 8-14, 2010.

[10]B.MuthuKumar and S.Jeevananthan, "High Speed Hardware Implementation of an Elliptic Curve Cryptography (ECC) Co-Processor", *Conf.on Trendz in Information Sciences & Computing* ,pp.176-180,2010.

[11] A.K.Rahuman and Dr. G.Athisha, "Reconfigurable Architecture for Elliptic Curve Cryptography", *Proc. of the Int. Conf. on Communication and Computational Intelligence*, pp.461-466, Dec.2010.

[12] Y.Zhang, D.Chen, Y.Choi, L.Chen and S.B.Ko, "A High Performance ECC Hardware Implementation With Instruction-Level Parallelism Over GF(2^{163})",*Elsevier-journal of Microprocessors & Microsystems,* vol 34 issue 6,pp. 228-236,Oct. 2010.

[13] M.Hamilton, W. P. Marnane and A. Tisserand, "A Comparison on FPGA of Modular Multipliers Suitable for Elliptic Curve Cryptography over GF(p) for Specific p Values*", IEEE 21st Int. Conf. on Field Programmable Logic and Applications*, pp.273 – 276, Sept. 2011.

[14] A. Rezai and P.Keshavarzi, "High-Performance Implementation Approach of Elliptic Curve Cryptosystem for Wireless Network Applications "*,Int. Conf. on Consumer Electronics, Communications and Networks,* pp. 1323 – 1327,April 2011.

[15] S.C. Chung, J.W.Lee, H.C.Chang, and C.Y.Lee, "A High-Performance Elliptic Curve Cryptographic Processor over GF(p) with SPA Resistance", *IEEE Int.Sym. on Circuits and Systems* ,pp. 1456 – 1459, May 2012.

[16]H.Mahdizadeh and M. Masoumi, "Novel Architecture for Efficient FPGA Implementation of Elliptic Curve Cryptographic Processor Over GF(2163*)" IEEE Trans. on Very Large Scale Integration Systems*, Vol. 21, No. 12, pp.2330-2333,Dec. 2013.

[17] S.S.Roy, C.Rebeiro, and D.Mukhopadhyay, "Theoretical Modeling of Elliptic Curve Scalar Multiplier on LUT-Based FPGAs for Area and Speed", *IEEE Trans. on Very Large Scale Integration Systems*, vol. 21, no. 5, pp.901-909,May 2013.

[18] A.C.Reyes, A.K.V.Castillo, M.M.Sandoval and A.D.P´erez, "A Performance Comparison of Elliptic Curve Scalar Multiplication Algorithms on Smartphones" *Int. Conf. on Electronics, Communications and Computing*,pp. 114 – 119, 2013

[19] A. Rezai and P. Keshavarzi, "A New Finite Field Multiplication Algorithm to Improve Elliptic Curve Cryptosystem Implementations", *Journal of Information Systems and Telecommunication,* vol. 1, no. 2,pp.119-129,June 2013.

[20] C.L.Leca, and C.I. Rincu, "Combining Point Operations for Efficient Elliptic Curve Cryptography Scalar Multiplication", *10th Int. Conf. on Communications,* pp. 1 – 4,May 2014.

[21] J.W. Lee and H.C. Chang, "Efficient Power-Analysis-Resistant Dual-Field Elliptic Curve Cryptographic Processor Using Heterogeneous Dual-Processing-Element Architecture" , *IEEE Trans. on Very Large Scale Integration Systems*, Vol. 22, No. 1,pp.49-61 Jan. 2014.

[22] K.Liao, X. Cui, N.Liao, T.Wang, X.Zhang, Y.Huang, and D.Yu, "High-speed Constant-time Division Module for Elliptic Curve Cryptography Based on GF(2^m)", *IEEE Int. Symp. on Circuits and Systems* ,pp:818 – 821,2014.

[23] P.R.Munoz, V.T.Olaya and J. V.Medina, "Design of Elliptic Curve Cryptoprocessors over GF(2163) on Koblitz Curves*",IEEE Latin American Symp.on Circuits and Systems*,pp.1-4,2014.

[24] S.Pontie and P.Maistri, "Randomized Windows for Secure Scalar Multiplication on Elliptic Curves" *IEEE 25th Int. Conf. on Application - specific Systems, Architectures and Processors* , pp.78 - 79,2014.

[25] S.Pontie and P.Maistri, "Design of a Secure Architecture for Scalar Multiplication on Elliptic Curves", *10th Conf. on Ph.D. Research in Microelectronics and Electronics*, pp.1-4,July 2014.