ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 2, March 2013

Differential Power Analysis (DPA) Attack on Dual Field ECC Processor for Cryptographic Applications

J.Sam Suresh [1],A.Manjushree[2], M.Kavinandhini[3], V.Lalitha[4]
[1]Assistant Professor, Department of Electronics and Communication Engineering, ACET, Tirupur, India.
[2, 3, 4] Department of Electronics and Communication Engineering, ACET, Tirupur, India.

Abstract— Exchange of private information over a public medium must incorporate a method for data protection against unauthorized access. Elliptic curve cryptography is one of the best Public Key Cryptography algorithm as it provides high security at lesser bit sizes than RSA and also it operates with higher throughput, lower power consumption, and lesser area requirements .The Elliptic curve cryptography processor focuses on the analysis and counteracts of elliptic curve implementations against side-Channel attacks. When simple power analysis is not feasible differential power analysis can be tried. Differential Power Analysis tries to exploit the relationship between the processed data and the power consumption. To enhance the data security against the DPA attack in network communication, a dual field ECC processor supporting all finite field operations is proposed. A key-blinded technique is designed against power analysis attacks. The proposed ECC processor is designed using hardware description language and implement on FPGA to analysis individuality with other cryptographic algorithms.

***Index Terms*—DPA, Dual field, ECC, Galois field, Public curve cryptography.**

I. INTRODUCTION

As the demand of wired and wireless communication keeps exploding, data security is become an urgent need for modern communication such as ranging from secure commerce and payments to private and protecting passwords. One essential aspect for secure communications is that of cryptography, cryptography is an essential part of today's information systems, and it helps to provide accountability, fairness, accuracy, and confidentiality. Cryptography was used to secure secret communications from military leaders, diplomats, spies and it was extensively used by governments to protect their diplomatic post. The cryptographic process is a complicated mathematical formulation, the more complex-the more difficult to break. Encryption can provide a means of securing information with respect to our own personal information like medical records, tax records, credit history, employment history, etc [7]. Encryption can also provide a means of message authentication [1].Cryptography systems can be broadly classified into symmetric-key systems that use a single key that both the sender and recipient have, and public-key systems that use two keys, a public key known to everyone and a private key that only the recipient of messages uses. Elliptical Curve Cryptography (ECC) is a public key cryptography.

The Public key cryptography, unlike private key cryptography, does not require any shared secret between the communicating parties but it is much slower than the private key cryptography. A public key for encryption only and a secret private key for decryption. The public key cannot be used to decrypt the information. It has attracted increasing attention in recent years due to its shorter key length requirement in comparison with other public-key cryptosystems such as RSA. A shorter key length means reduced power consumption and computing effort and less storage requirement in various devices and components [2].

Table.1.Comparison of Key Size

ECC key size	RSA key size	Key-size Ratio
163	1024	1:6
256	3072	1:12
384	7680	1:20
512	15560	1:30

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 2, March 2013

As shown in Table 1 the ECC key sizes are so much shorter than RSA keys, the length of the public key and private key is much shorter in elliptic curve cryptosystems. This results in faster processing times and lower demands on memory and bandwidth .Elliptic Curve Cryptography is a public key cryptosystem that is becoming increasingly popular. There are so many challenges to implement a public key cryptography algorithm such as execution time, integrated methods, memory requirement etc. They provide high levels of security and do not require an initial private key exchange between the communicating parties. ECC has been widely adopted in modern security standards to provide robustness for secure data transaction such as data and finance authentication, digital signature and security key management, etc. ECC is based on the difficulty of solving the Elliptic Curve Discrete Logarithm Problem (ECDLP).

II. COMPARISION WITH OTHER ALGORITHMS

The most important difference between ECC and other conventional cryptosystems is that for a well-chosen curve, the best method currently known for solving the ECDLP is fully exponential, while sub-exponential algorithms exist for conventional cryptosystems. Clearly, ECC keys take much more effort to break compared to RSA and DSA keys [2]. Due to this, many people believe that ECDLP is intrinsically harder than the other two problems. While this deduction might be true, We do not know if a fast and efficient elliptic curve DL algorithm that runs in sub-exponential time will be discovered, say, in the next ten years, or if another class of weak curves will be identified that could compromise the security of elliptic curve cryptosystems[10].

III. ELLIPTIC CURVE CRYPTOGRAPHY

Elliptic curve cryptography (ECC) has become popular due to its superior strength per bit compared to existing public key algorithms RSA, this superiority translates to equivalent security levels with smaller keys, bandwidth savings, and faster implementations, making ECC very appealing .The area of ECC researched is the arithmetic blocks of elliptic curve cryptographic co-processor over GF (2^m).It is capable of calculating point addition, point multiplication and squaring. [1] - [3] the mathematical operations of ECC is defined over the elliptic curve

$y^2 = x^3 + ax + b$, where $4a^3 + 27b^2 \neq 0$ (1)

Each value of the 'a' and 'b' gives a different elliptic curve. All points (x, y) which satisfies (1) plus a point at infinity lies on the elliptic curve. The public key is a point in the curve and the private key is a random number. The public key is obtained by multiplying the private key with the generator point G in the curve. The generator point G, the curve parameters 'a' and 'b', together with few more constants constitutes the domain parameter of ECC. Generally, EC curves have no singularity; the condition of singularity is shown below

$$\frac{\partial F}{\partial x}(x_0, y_0) = \frac{\partial F}{\partial y}(x_0, y_0) = 0$$

Or, $2y_0 = -f'(x_0) = 0$

Or, $f(x_0) = f'(x_0) = 0$

∴ F has a double root

$y^2 = x^3 + Ax + B$

For double roots,

$x^3 + Ax + B = 3x^2 + A = 0$

$x^2 = -A/3$

Also, $x^4 + Ax^2 + Bx = 0$

$$\frac{A^2}{9} - \frac{A^2}{3} + Bx = 0$$

$$x = \frac{2A^2}{9B}$$

$$3\left(\frac{2A^2}{9B}\right)^2 + A = 0$$

$$4A^2 + 27B^2 = 0$$

Each value of the 'a' and 'b' gives a different elliptic curve. All points (x, y) which satisfies (1) plus a point at infinity lies on the elliptic curve. The public key is a point in the curve and the private key is a random number. The public key is obtained by multiplying the private key with the generator point G in the curve. The generator point G, the curve parameters 'a' and 'b', together with few more constants constitutes the domain parameter of ECC.ECC is performed in either [1] and [4] in two finite fields: prime field GF (p) or binary extension field GF (2^m) [2]. An efficient processor that supports elliptic curve cryptographic applications over GF (p) has been

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 2, March 2013

designed on a reconfigurable device for the field GF (2^m) .The proposed structure is capable of calculating point multiplication and additions using a single coordinate to contain the point information. Efforts to have unified architectures for GF (p) and GF (2^m) multiplier have also been achieved [6] and [4]. The difference between multipliers in GF (p) and GF (2^m) is their delay times [8].Dual field approaches were proposed to proposed to unify GF (p) and GF (2^m) ECC systems, emphasizing the flexibility and scalability for a wider range of applications, a unified word-based Montgomery multiplier with scalable field are proposed. With the proposed control and data applications, unified word-based Montgomery multipliers with scalable field are proposed. With the proposed control and data path architecture, the dual-field Montgomery inversion is integrated into the processor to improve the performance. The energy-adaptive data path is to provide dynamic controllability for the trade-off among power, energy and performance.

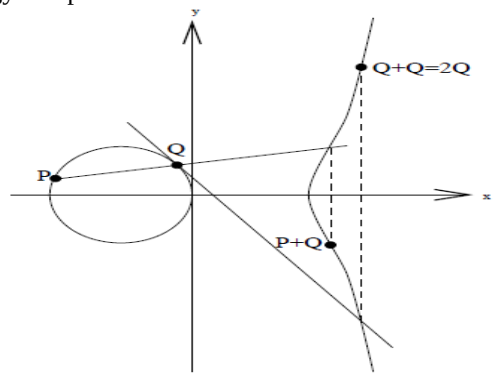

Fig. 1 Elliptic Curve Cryptography

Even if the ECC is secure at cryptanalysis, the private data of an unprotected hardware device can be extracted by physical attacks due to side-channel leakage. The power-analysis attacks initially can reveal the key value by analyzing the power consumption of a cryptographic implementation such as on an application-specified integrated circuit (ASIC), field programmable gate array (FPGA).During the device processing simple power-analysis (SPA) attacks can distinguish the key value through visual inspection because of the specifically active circuit with direct hardware scheduling. The double-and-add-always method is usually used to avoid the variation of power consumption over time [6]. Fig 1 illustrates one particular operation using real numbers.

A.POINT MULTIPLICATION

A basic operation of any elliptic curve cryptosystem is an elliptic curve point multiplication given [9] and [3] as $Q = kP = P+P+\ldots\ldots..+P$

Where P is a point on an elliptic curve E and k is an integer in a range 1k < order (P) .Accordingly, the elliptic curve point multiplication means that the point P is added to itself k times. The order of the point P is if and only if P multiplied with results in the point at infinity. This is formally described as follows:

Order (P) $=n_0 \Leftrightarrow n_0P=0_\infty$.

The strength of an elliptic curve cryptosystem lies in the fact that if E, Q and P are given, it is a very hard task to recover k. The integer k is usually very large and, therefore, it would be too slow to calculate Q just by adding P to itself k times. Thus, efficient elliptic curve point multiplication methods are needed. The simplest and oldest of such methods is the binary method which is also known as the double-and-add-method[10].An efficient point multiplication method which is an optimized version of a method based on the Montgomery's method, this efficient elliptic curve point multiplication method is called the Montgomery point multiplication in projective coordinates. It performs the point multiplication in projective coordinates and it is developed using projective coordinate equations, and also refer [11].

B.GEOMETRICAL ANALYSIS OF POINT ADDITION

Point addition is the addition of two points J and K on an elliptic curve to obtain another point L on the same elliptic curve. Consider two points J and K on an elliptic curve [9] as shown in Fig.3. If K ≠ -J then a line drawn through the points J and K will intersect the elliptic curve at exactly one more point–L [8] and [10].The reflection of the point –L with respect to x-axis gives the point L, which is the result of addition of points J and K. Thus on an elliptic curve L = J + K. If K = -J the line through this point intersects at a point at infinity O. Hence J + (-J) = O. This is shown in Figure. O is the additive identity of the elliptic curve group. A negative of a point is the reflection of that point with respect to x-axis [12].

Point addition rules:

1. $\infty+\infty=0$
2. $(x1, y1)+\infty=(x1, y1)$

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 2, March 2013

3. (x1, y1)+(x1,-y1) = ∞
4. (x1, y1)+(x2, y2) =(x3, y3)

Where:

If $x_1=x_2$, $\lambda \frac{y2-y1}{x2-x1}$

If $x_1==x_2$, $\lambda=\frac{3x_1^2+a}{2y1}$

x_3= (λ2-x1-x2)

y_3 = (λ(x1-x3)-y1)

C.DUAL FIELD CONSIDERATION

The above discussion is about modular multiplication is in fact in integer ring *Zn*. The dual field problem should be considered when we design a modular multiplier. They will be limited by length. Fig 2 shows the field classification available in ECC.

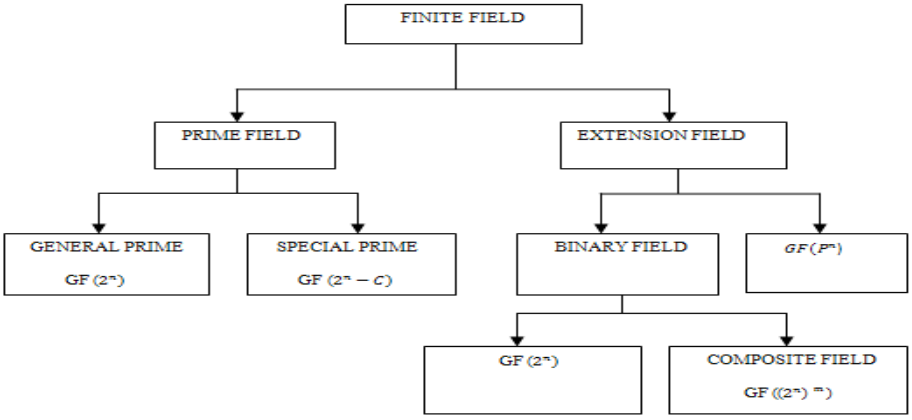

Fig. 2 Hierarchy of finite field system

Field is essentially a special kind of ring and finite field (or Galois field) is a subclass of field. The hierarchy of finite field system is illustrated with these fields, GF (*p*) and GF (2^m) are used most popularly [12]. So it is about dual field subsequently, we only mean these two fields. Since GF (*p*) is the subclass of integer ring, the modular operations and facts are fully applicable to GF (*p*). The only difference is that odd *n* there is replaced by odd prime *p*. In GF (2^m), addition (or subtraction) is carry (or borrow) free, and thus multiplication and division are also different from those of integers, since these high-level operations are based on those basic ones. Accordingly, the basic hardware arithmetic units for GF (2^m) are different from those for GF (*p*) is shown in Fig 3.

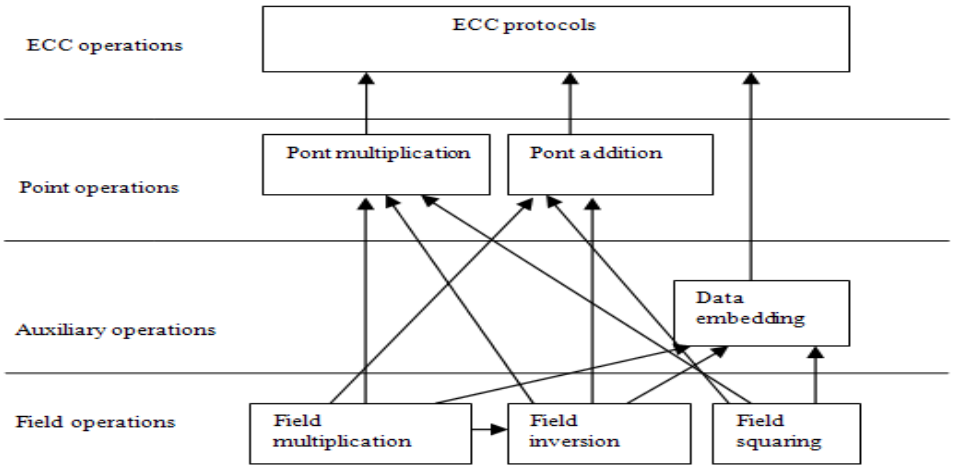

Fig.3 Interaction between different operations

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 2, March 2013

IV. DPA ATTACKS

The differential power-analysis (DPA) attacks computing the correlation between the target power traces and power model can reveal the key value due to the existence of key-dependent operations in every round of calculations. Hiding technique with algorithm- independent dedicated circuit is a common approach to protect cryptographic processors from attackers collecting the key-dependent characteristics of power traces. So that a new efficient countermeasure to overcome the DPA attacks by computing the overall ECC functions in a randomized Montgomery domain is proposed. The feature is to mask the intermediate values is not only the arithmetic but also the temporary register. It adopts simple logic circuit to counteract DPA attacks, the hardware cost overhead could be significantly reduced, and the maximum operating frequency of the protected design is same as that of unprotected design using the conventional Montgomery algorithm [5] and [7].

V. ECC ARCHITECTURE AGAINST DPA ATTACKS

The architecture is suitable for performing ECC based on projective coordinate. The architecture consists of two computational modules and two control units [5] and [9]. The Montgomery module generates the key, which has a scheduler and data selector. Elliptic curve cryptography module encodes the data using the key generated by Montgomery module. Fig 4 shows the architecture of ECC which consists of few blocks. Buffer is used to the intermediate results of key value. Clock control unit issues and controls the clock to Montgomery module; buffer and prime field adder .Performance in ECC can be further developed by means of Carry look ahead adder which is exploited as prime field adder. Montgomery inversion algorithm is coded in an efficient manner to generate the key. In addition, the triumph of data selector and CLA prepares the processor to produce high throughput with reduced area. The Montgomery data selector does not allow repeated data and hence, it is very difficult for crypt analyzers using Brute-Force attacks, so it is highly secured. Data selector involves simple operations like XOR and shifting, which further reduces the complexity and the area. Data scheduler is used to control the data selector based on user input and clock signal.

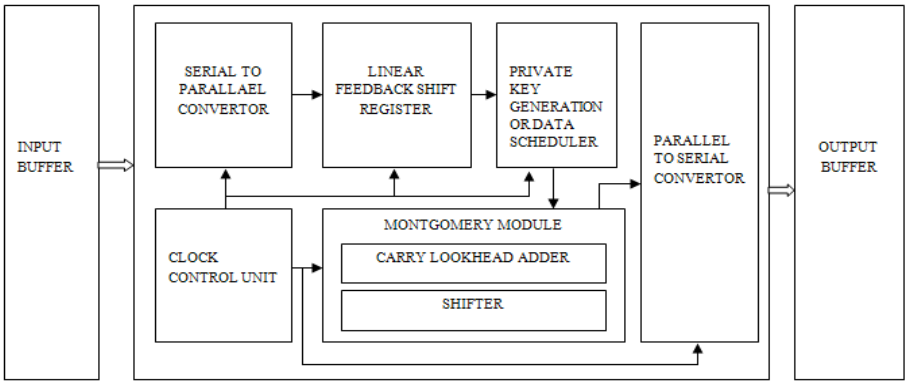

Fig. 4 Architecture of ECC processor

A countermeasure to overcome the DPA attacks [5] and [7] by computing the overall ECC functions in a randomized Montgomery domain is performed. The feature of our approach is to mask the intermediate values not only the arithmetic but also the temporary register. Thus it is unnecessary to extend the key length, customize the circuit, and modify the algorithm in ASIC or FPGA design flow. Since our proposed design adopts simple logic circuit to counteract DPA attacks, the hardware cost overhead could be significantly reduced, and the maximum operating frequency of the protected design is the same as that of the unprotected design using the conventional Montgomery algorithm. In addition, by reducing the iteration time of the divisions, which dominates other field operations in the computation time, the speed can be further improved.

The fundamental concept of DPA countermeasure is to break the dependence between intermediate values and power traces. For achieving the point calculation, the Montgomery algorithm is adopted to perform the field arithmetic in a specific domain such that A=a (mod p), where a is in the integer domain and is the Montgomery constant with n-bit field length. [7].

VI. SURVEY OF ECC APPLICATIONS

When the ECC was first introduced in 1985, there was a lot of skepticism about its security. However, ECC has since come a long way. After nearly a decade of serious study and scrutiny, ECC has yielded highly efficient

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 2, March 2013

and secure. Presently, many product vendors have incorporated ECC in their products, and this number has only been on the rise. Uncertainty still exists among some proponents of traditional cryptographic systems, but they are starting to become more accepting of this promising new technology. RSA Security Inc., for example, has long voiced concern regarding the security of ECC since its introduction. In recent years, however, RSA Security has researched on efficient ECC algorithms, and even acquired a patent on a storage-efficient basis conversion algorithm. Moreover, it has also integrated ECC into some of its products, acknowledging the fact that ECC has begun to establish itself as both secure and efficient. An important factor for this emerging trend is the incorporation of ECDSA in several government and major research institution security standards, including IEEE P1363, ANSI X9.62, ISO 11770-3 and ANSI X9.63. Another factor is the strong promotion of the use of ECC through a Canadian-based Certicom Corporation. Certicom is a company that specializes in information security solutions in a mobile computing environment through providing software and services to its clients. Over the years, Certicom has published numerous papers in support of ECC and has also implemented ECC in all of its commercial products. Its success prompted many other companies to look more closely at the benefits and security of ECC. Now, ECC is becoming the mainstream cryptographic scheme in all mobile and wireless devices. Results of the survey can be broadly divided into four categories: the Internet, smart cards, PDAs and PCs.

A.INTERNET

In September 2002, SUN Microsystems contributed to the implementation of an ECC cryptographic library and also a common hardware architecture for accelerating ECC (as well as RSA) to be used in open SSL. Open SSL is a developmental toolkit for the implementation of SSL (Secure Sockets Layer) and TLS (Transport Layer Security) protocols, which are commonly used today in over-the-web transactions and secure document transfers. SUN hopes to promote ECC standardization with SSL, which is the dominant security protocol used on the web today.

In late 1998, the Treasury Department's Bureau of Engraving and Printing completed a four-month e-commerce pilot program involving the use of smart cards and ECC with SET (Secure Electronic Transaction) specifications. SET is a standard that enables secure credit card transactions over the Internet. The pilot program tested the use of smart cards, embedded with ECC technology, in making online purchases. This program involved a total of nine companies, including MasterCard, Certicom (who supplied the ECC algorithms), Digital Signature Trust Co. (who supplied the MasterCard smart cards) and Globe Set (a SET vendor), just to name a few. The previous version of SET, version 1.0, supports only RSA Data Security encryption algorithms, but MasterCard hopes to add ECC to the upcoming version of SET.

B.SMART CARDS

Smart cards are one of the most popular devices for the use of ECC. Many manufacturing companies are producing smart cards that make use of elliptic curve digital signature algorithms. These manufacturing companies include Phillips, Fujitsu, MIPS Technologies and Data Key, while vendors that sell these smart cards include Funge Wireless and Entrust Technologies. Smart cards are very flexible tools and can be used in many situations. For example, smart cards are being used as bank (credit/debit) cards, electronic tickets and personal identification (or registration) cards.

C.PDAs

PDAs are considered to be a very popular choice for implementing public key cryptosystems because they have more computing power compared to most of the other mobile devices, like cell phones or pagers. However, they still suffer from limited bandwidth and this makes them an ideal choice for using ECC. In the January of 1998, 3Com4 Corporation teamed up with Certicom to implement ECC in future versions of its Palm Pilot organizer series and Palm Computing platform. This new feature will provide protection of confidential information on the hand-held organizers, user authentication in wireless communications and e-commerce transactions, and also ensure data integrity and proof of transactions PCs. Constrained devices have been considered to be the most suitable platforms for implementing the ECC. Recently, several companies have created software products that can be used on PCs to secure data, encrypt e-mail messages and even instant messages with the use of ECC. PC Guardian Technologies are one such company that created the Encryption plus Hard Disk and Encryption plus Email software products. The former makes use of both RSA and EC Diffie-Hellman while the latter makes use of a strong 233- bit ECC key to encrypt its private AES keys Since the 28 July 2000, Palm Inc. has separated from 3Com, and is now a fully independent company. The Top Secret Messenger software was developed by Encryption Software Inc. It encrypts the messages of some of the most popular instant messaging programs today, like ICQ and MSN. It can also be used with e-mail clients such as Microsoft Outlook and Outlook

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 2, March 2013

Express to encrypt e-mail messages. This product uses both private and public key cryptosystems, including a 307-bit key for its implementation of the ECC.

VII. CONCLUSION

This paper proposes an ECC processor based on Montgomery algorithm, its efficiency and security makes it an attractive alternative to conventional cryptosystem, and also security against DPA attacks.

REFERENCES

[1] Akashi Satoh and Kohji Takano," A Scalable Dual-Field Elliptic Curve Cryptographic Processor", IEEE Transactions on Computers, vol. 52, no. 4, April 2003.

[2] Ray C. C. Cheung, Student Member, IEEE, Nicolas Jean-baptiste Telle, Wayne Luk, Member, IEEE, and Peter Y. K. Cheung,," Customizable Elliptic Curve Cryptosystems"IEEE Transactions On Very Large Scale Integration (VLSI) Systems, vol. 13, no. 9, September 2005.

[3] Jin Park Dept. of Electronics and Computer Engineering & RRC HECS, Chonnam National University, Korea Jeong-Tae Hwang Dept. of Electronics and Computer Engineering & RRC.

[4] HECS, Chonnam National University, Korea Young-Chul Kim Dept. of Electronics and Computer Engineering & RRC HECS, Chonnam National University, Korea , "FPGA and ASIC Implementation of ECC Processor for Security on Medical Embedded System" IEEE Transactions on Computers, May 2005.

[5] Ciaran J. Mcivor, Máire Mcloone, and John V. Mccanny, Fellowieee," Hardware Elliptic Curve Cryptographic Processor over GF (P)"IEEE Transactions on Circuits and Systems—I: Regular Papers, vol. 53, no. 9, Sep 2006.

[6] Patrick Longa and Ali Miri, "Fast and Flexible Elliptic Curve Point Arithmetic over Prime Fields", IEEE Transactions on Computers, vol. 57, no. 3, March 2008.

[7] Jyu-Yuan Lai and Chih-Tsun Huang," Elixir: High-Throughput Cost-Effective Dual-Field Processors and the Design Framework for Elliptic Curve Cryptography", IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 16, no. 11, Nov 2008.

[8] Mohamed N. Hassa and Mohammed Benaissa,"Embedded Software Design of Scalable Low-Area Elliptic-Curve Cryptography", IEEE Embedded Systems Letters, vol. 1, no. 2, Aug 2009.

[9] Mohamed N. Hassa and Mohammed Benaissa and Patrick Longa and Ali Miri," Fast and Flexible Elliptic Curve Point Arithmetic over Prime Fields", IEEE Transactions on Computers, vol. 57, no. 3, March 2008.

[10] Kris Gaj, Soonhak Kwon, Patrick Baier, Paul Kohlbrenner, Member, IEEE, Hoang Le,Mohammed Khaleeluddin, Ramakrishna Bachimanchi, and Marcin Rogawski Sieve,"Area-Time Efficient Implementation of the Elliptic Curve Method of Factoring in Reconfigurable Hardware for Application in the Number Field," IEEE Transactions On Computers, vol. 59, no. 9, Sep 2010.

[11] Arun Kumar,Dr.s.sTyagi, Manisha Rana, Neha Aggarwal, Pawan Bhadana,"A Comparative Study of Public Key Cryptosystem based on ECC and RSA",International Journal on Computer Science and Engineering,ISSN:0975-3397,vol 3,no.5,May 2011.

[12] Jyu-Yuan Lai and Chih-Tsun Huang," Energy-Adaptive Dual-Field Processor for High-Performance Elliptic Curve Cryptographic" Applications IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 19, no. 8, Aug 2011.

[13] Jen-Wei Lee, Ju-Hung Hsiao, Hsie-Chia Chang, and Chen-Yi Lee," An Efficient DPA Countermeasure with Randomized Montgomery Operations for DF-ECC Processor,"IEEE Transactions on Circuits and Systems—II: Express Briefs, Vol. 59, No. 5, May 2012.

[14] C.Tokunaga and D. Blaauw," Securing encryption systems with a switched capacitor current equalizer", IEEE J.Solid-State Circuits, vol 45, no.1, pp 23-31, Jan 2010.

[15] P.C. Liu, H.C. Chang and C.Y Lee," A low overhead DPA countermeasure circuit based on ring oscillators", IEEE Transactions on Circuits and Systems—II: Express Briefs, vol.57, no.7, pp.546-550, Jul.2010.

AUTHOR BIOGRAPHY

.J.Sam Suresh: He completed his B.E.in Electronics and Communication Engineering and M.Tech in VLSI Design. Currently he is working as an Assistant Professor at Angel College of Engineering and Technology, Tirupur. His research project is based on MEMS pressure Sensor. He is a member of IEEE.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 2, March 2013

A. Manjushree: At present she is final year student of Bachelor of Engineering degree in Electronics and Communication Engineering at Angel of Engineering and Technology, Tirupur. She is a member in The Institution of Electronics and Telecommunication Engineers.

M.Kavinandhini: At present she is final year student of Bachelor of Engineering degree in Electronics and Communication Engineering at Angel of Engineering and Technology, Tirupur. She is a member in The Institution of Electronics and Telecommunication Engineers.

V.Lalitha: At present she is final year student of Bachelor of Engineering degree in Electronics and Communication Engineering at Angel of Engineering and Technology, Tirupur. She is a member in The Institution of Electronics and Telecommunication Engineers.