iJRASET
International Journal For Research in Applied Science and Engineering Technology



# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 3 **Issue:** Issue II **Month of publication:** June 2015

**DOI:**

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

# Implementation of Elliptical Digital Signatures Using Montgomery Method

Prajna.D
*Student (Mtech) of Dept of Digital electronics, UTL tech limited, Bangalore,560012,India*

***Abstract- -The elliptic curve cryptosystems is given more importance and paid more intention because of its shortest key size and security than other public cryptosystems. The digital system based on ECDSA is one of the main stream digital signature systems. Elliptical digital signatures algorithm provides security services for resource constrained embedded devices where power ,memory and battery life of devices are most constrained. The ECDSA level security can be enhanced by tuning several parameters as parameter key size and the security level of ECDSA elementary modules such as hash function, elliptic curve point multiplication which used to generate public key and a pseudo stream generator generates private key. In this work we have a considered a key size equal to 163 bit, Montgomery point multiplication technique, and hashing functions SHA-1. The implementation results provides security evaluation and hardware performances in terms of area occupation and time computation and compare the results of previous work.***
***Index terms-Random generator, secure hash algorithm, Elliptic Curve digital signature algorithm. Koblitz curves, FPGA and cryptography.***

## I. INTRODUCTION

One of important cryptography which provides authentication, authorization and non-repudiation in digital signatures. The concept of digital signature is most powerful but difficult to achieve. Digital signatures schemes are the electronic version of handwritten signatures. The purpose is to provide an entity to bind its identity with particular information. The process of signing transforms the message and secret information hold by the entity known as signature. After the data has been signed, the document is verified by the signature verification process.Tranmitted data can be easily intercepted and interpreted. To achieve confidentiality between communication parties, encryption technique is used. The authentication algorithms mainly rely on the concept of encrypted data with private key and decrypted data using public key. This process is opposite the process which provides data confidentiality. The major advantage of public key cryptography which provides both authentication and data integrity. Hence public key cryptosystem are more preferred for signature generation. The signature generated by public key digital signature can be verified by any one as information verified is public. The importance of digital signatures in communication has the merits which leads to research into new cryptographic systems which is ECC.(Elliptical curve cryptography) especially growing number of memory limited mobile electronic devices. Several studies have been conducted in the last recent years for both hardware and software implementation of ECDSA (Elliptic curve digital signatures algorithm.).The majority is focused on basic algebraic operations or the efficient implementation of a protocol on finite field. The major weakness of this protocol whack uses random secret key. Random numbers which used for unpredictable or non-deterministic data into cryptography.
This paper is structured as follows: section II, a brief description of digital signature algorithm, section III elliptical curve cryptography using Montgomery method is developed. The proposed architecture is presented and analysed in section Ivan implementation of elliptical curve digital signature based on secure hash function, a 163-bit ecc and a random number generator is presented in the next section. Section VII gives the experimental setup and analysis and concludes the paper.

## II. DIGITAL SIGNATURE ALGORITHM

The DSA digital signature was developed by NSA and popularly known as digital signature standard, DSS of NIST(national institute of standards and technology) in 1994 and was specified in a U.S. Government Federal information processing standard (FIPS 186).It is an efficient variant of the ElGamal digital signature scheme intended for use in electronic mail, electronic funds transfer, electronic data interchange, software distribution, data storage and other applications which require data integrity and data authentication. Digital signature involves two process, one performed by the signer and other by the receiver of the digital signature.


©IJRASET 2015: All Rights are Reserved

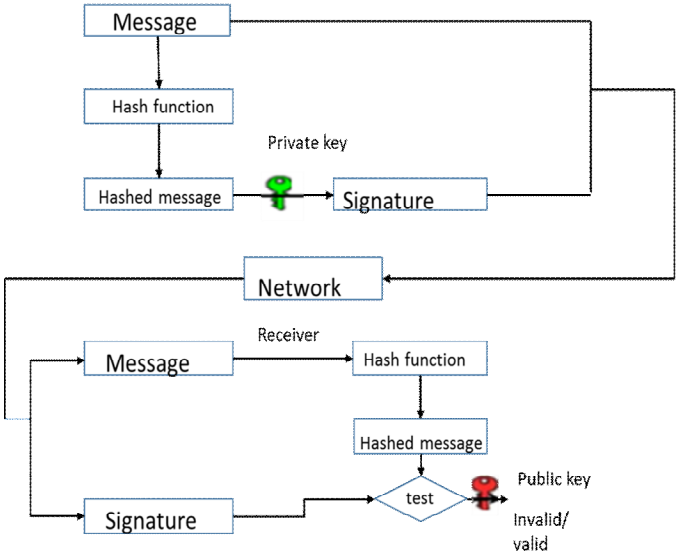
Key generation: Used to generate keys in digital signing.

Signature generation: Used to generate the signature for the message using the key obtained from the key generation phase.

Signature verification: Used by the recipient to verify the integrity of the received message. The receiver on receiving the message checks the signature and performs the signature verification operation on the received message with the sender's public key and compares the result with the signature to ascertain that the message has not tempered with.

Messages cannot be intercepted and and modified because the signature on the message will verify. Without the private key of the sender, the correct signature cannot be computed. An entity cannot impersonate another because each entity has a unique private key. The private key is only by the owner and is required to compute the digital signature of each message. Lastly, an entity cannot deny knowledge of a message containing their signature.

FIG.1 DIGITAL SIGNATURE ALGORITHM




## III. ELLIPTIC CURVE CRYPTOSYSTEMS

There are two main procedure for implementing public key cryptography: one based on modular multiplications as used in RSA and the other based on polynomial arithmetic in finite fields over a given elliptic curve in ECC.The smaller key sizes of ECC allows for less computational devices such as smart cards and embedded systems which is used in cryptography for safe data transmissions, message signing and verification and other means.The elliptical curve cryptosystems schemes mainly based on scalar multiplication of elliptic curve points ,inverse operations and the Elliptic curve discrete logarithm problem(ECDLP).

In the remainder of this article, we focus on elliptic curve over binary fields GF($2^m$).we use a polynomial representation is well suited for hardware implementation. To compute the scalar multiplication, we have to compute the point addition and point doubling on this curve. It has been proved that in affine representation there is need for computing inverse of an element in GF ($2^m$) to perform point addition and point doubling. Inversion is most time consuming and memory occupation. Therefore, projective coordinates can be used to avoid inversions.IN the following, Montgomery method is applied (fig2).An elliptic curve E over the finite field GF (2m) is defined by the simplified projective Weierstrass equation:

$$\mathbf{Y^2Z+XYZ=X^3+aX^2Z+bZ^3}$$

The montogomery method is based on the formulas for point doubling and point addition.

Let P=(X1, Y1, Z1) and Q=(X2, Y2, Z2) be points on the elliptic curve E.The addition point P+Q=(X3, Y3, Z3), is given with the



©IJRASET 2015: All Rights are Reserved

montogomery point addition operation as follows:

$Z_3= (X_1Z^2+Z_1X^{2)2}$

$X_3=x (X_1Z^2+Z_1X^2)^2+ (X_1Z^2) (Z_1X^2)$

The doubling of point P1 is 2*P1=(X3, Y3, Z3) by applying the Montgomery point doubling operation is given by equation:

$Z_3=X_1^2Z_1^2$

$X_3=(X_1^2)^2+ (CZ_1^2)^2$

Next step is to implementing the scalar point multiplication, which is the most operation in ECC.

Algorithm: Montogomery point multiplication method.

Input: k= (kn-1, kn-2…….k1, k0)2 with kn-1=1, P(X1, Z1) €E ($F2^m$)

OUTPUT: Q=KP

1. P1←P; P2←2P

2. For i from n-2 down to 0 do

3 .if (Ki=1) then

4. P1←P1+P2 P2←2P2

5 .else

6. P2←P2+P1; P1←2P1

7. End if

8. End for

9. Return (Q=P1)

## IV. PROPOSED ARCHITECTURE

The proposed architecture of Digtal signature algorithm is based on Elliptical curve cryptography(ECC) over binary field GF(2m).It consist of the following parts:
Montogomery method for the scalar multiplication (KP), secure hash algorithm (SHA-1), Elliptic curve point addition (ECC-ADD), a random number generartor (W7) and arithemetic operators.

### *A. Elliptic curve digital signatures algorithm(ECDSA)*

Elliptic curve digital signature algorithm (ECDSA) is the Elliptic curve analogue of the more widely used digital signature algorithm(DSA).ECDSA is the application of ECC to digital signature generation and verification.It was accepted in 2000 as an IEEE standard and FIPS standard. ECDSA provides the security services authentication, integrity and no-repudation.Its security is mainly based on the ECDLP and also depends on several parameters, the size of finite field which determines the public key size, finite field type and security of each block's ECDSA as point multiplication, private key size and output size of secure hash algorithm. Using this parameters can be used to compare the security level taking versions of ECDSA, which is relative comparison.

The transmitter will transmit a message to the receiver. Therefore, firstly it generates a pair key: the first is secret used for generating the signature. The second is public key sent to the receiver. The transmitter generates the signature with her private key



©IJRASET 2015: All Rights are Reserved

and the hashing function after he sends the set message signature and public key to the receiver and finally signature is verified with the public key to authenticate the message

.

The proposed ECDSA based on the Montgomery-form Elliptic curve digital signature algorithm.

*1) Key generation: The* key generation process is as described

Algorithm: Key pair generation

*a)* Select an elliptic curve E (a, b).
*b)* Select a point G € E (a, b) of order n.
*c)* Select a cryptographically strong random number d in the interval [1, n-1].
*d)* Compute the point Q=d G on the Montgomery form. (Compute using the scalar multiplication algorithm and the Y-coordinate recovery method)

Output the public key (G, n, Q) and the private key d.

*2) Signature generation*

To sign a message m, an entity does the following:

Algorithm: ECDSA signature generation

Input: The signer's private key d and a message M

Output: A signature (r, s) where the integers r, s are in [1, n-1].

*a)* Select a random or pseudo random generator k, 1<k<n-1.
*b)* Compute kG=(x1, y1).
*c)* Compute r=x1 mod n. If r=0 then go to step 1.
*d)* Compute $k^{-1}$ modn
*e)* Compute e=H (m) with the secure hash algorithm (SHA-1).
*f)* Compute s=$k^{-1}$ (e+d.r) mod n.if s=0 then goto step1.
*g)* The signature for the message is (r, s)

## V. SHA-1 HASH FUNCTION TECHNIQUE

It is proposed by the national security agency and published by the NIST.Hash functions are important security primitives used for authentication and data integrity. SHA allows the condensation both in the sender and receiver. They are used in conjunction with public key algorithms for both digital signatures and encryption techniques. The three SHA algorithms structured variety and are distinguished as SHA-0,SHA-1(SHA-160) and SHA-2 and other algorithms like SHA-256,SHA-385 and SHA-512,where is the length of hash H in bits. In this project, only SHA-1 is specially used in cryptographic algorithms, especially in message authentication schemes.

The basic requirements for a cryptographic hash functions as follows:

A. The input can be of any length.
B. The output must be fixed and should be in sequence length.
C. H (m) is relatively easy to compute for all value m.
D. H (m) is one-way.
E. H (m) is collision free.

A hash function maps a large collection of messages into small set of message digests, that can be used to produce a fixed-length digital signature.SHA-1 handles messages in blocks of 512bits which requires 80steps.One step handles five 32 variables by computing 32-bit modular additions(a+b mod 232) and certain 32-logical functions which depends on the step index. When all the blocks have been processed, the hash of the message is in five variables and produces 160-bit hash. The implementation consists of four main components: step function, message schedule, constants block and control logic. Step function determines the maximum clock cycle.

The message schedule stores 512-bits message bits and derives a 32-bit wise XORs and a rotation.



©IJRASET 2015: All Rights are Reserved

**V1.PSEUDO-RANDOM GENERATOR**

As mentioned earlier, the private key is a public key pair must be kept secret. For non-repudiation the private key must be completely inaccessible to all other parties.

An adversary who doesn't know the private key of the signatory, cannot generate the correct signature of the signatory. However, by using the signatory's public key, anyone can validly signed message. Therefore the potential weakness in both algorithms is the random value of k used to sign a message. The user must guard this value closely even if one were to be revealed, their secret signing key would be compromised. Similarly, in an

Attack that is less apparent, user should never sign two messages using the same random value K. If they do unknowgly an attacker can recover their signing key without even knowing the k they used. The securityof the ECDSA depends gratly on pseudo random generator. A high quality, hardware –based random generator is aboustely fundamental to provide a high level of information security. Because random numbers are the foundation of secure cryptographic solutions and protected communication protocols.The best random generator produces statically random and indeterminisic numbers.

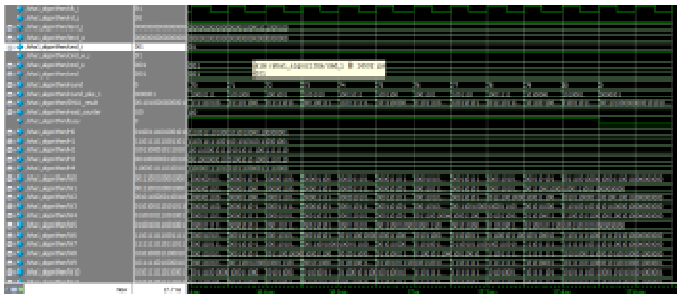
In this paper, W7 algorithm has been proposed, as a more reliable solution for random number generator by S.Thomas, D.Anthony, T.Berson.The W7 architecture consists of a control and functional unit. The functional unit is responsible for a keystream generator.This unit contains eight similar cells.The proposed architecture for the hardware implementation of a cell is presented in fig 6.A cell has two inputs and one output.The one output is the key and its same for all calls.the other input consists of control signals.Finally the output is one bit long.The outputs of a cell complete the keystream byte.

Each cell consists of three LFSR'S 38-, 43-, and 47-bit long and a majority function. Their initial state which is same for all is the symmetric encryption key.

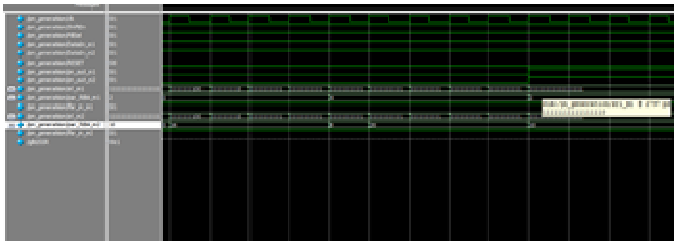
**VII.RESULTS AND ANALYSIS**

*A. Synthesis results and comparison*

*1) SHA-1:* The input given as clock reset and text message, command input. When command input is 010 and 011 it starts write and read respectively.After every $80^{th}$ cycle it starts counting again and we get sha-1 result and the message gets converted into hexadecimal and sent to the receiver.



*2) Pseudo Random Generator:* The input given as clock, reset, shift enable is 1 field selection 1 ,and data m1 and data m2 either 0 or 1 and it shifts left by one bit by xoring each bit we get the parallel output which will generate random integers for key pair generation for security and it is sent to the receiver side.



*3) Point Multiplication:* The input is given as xp, yp ,k,clk,reset, is given as input xq ,yq as output and signals we use here xA,Xb,next_a,next_b,mont-oper,mot_add,xpxoryp,int_k, sel_AB,sel_in, sel_Q, ce_A, ce_B, A_infinity, B_infinity, k_m_minus_1,



©IJRASET 2015: All Rights are Reserved

Volume 3, Special Issue-I1, June 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

mont_start, mont_done, reset_counter, count_down, last_step to perform operations.Current state changes 0 to 26..It performs multiplication division and squaring using point addition doubling.

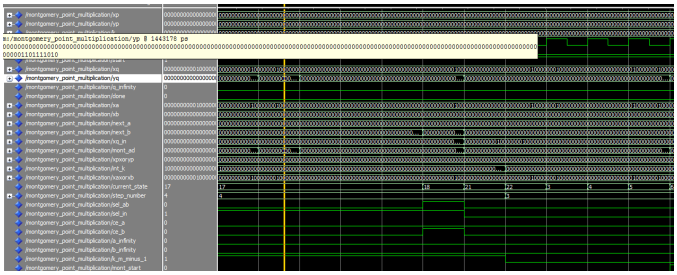


TABLE 1: Results of ECDSA blocks implemented designs

| | Occupation (Regs) | Occupation (LUTs) | Frequency (MHz) | Time (ns) |
|---|---|---|---|---|
| PRNG | 4800 | 2400 | 292.67 | 3.142 |
| Point multiplication | 720 | 1429 | 172 | 5.794 |
| SHA-1 | 894 | 1479 | 157 | 6.282 |

TABLE 2: Comparisons of previous results ECDSA blocks implemented designs

| | Occupation (Regs) | Occupation (LUTs) | Frequency (MHz) | Time (ns) |
|---|---|---|---|---|
| **PRNG** | 497 | 157 | **373** | 40.21ns |
| Point multiplication | 1709 | 3578 | 246.09 | 4.093ns |
| SHA-1 | 1063 | 1703 | 176 | 0.355ns |

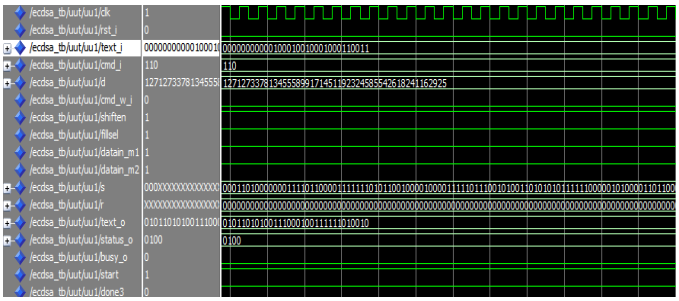
*B. Signature generation*

Signature Generation:

Input file="abcd" Private:0xd43fb7ff56a7486859d87f785db45b043129f6468ccff4 2d0001

Signature: r=0xb8d06fa44816c92b8b26f797e5f3cc07984d8b7f7e49a339

s=0xd74f17a1e19139d77558c6b2d16dcb1f4bb31da2ded2573





©IJRASET 2015: All Rights are Reserved

## VIII. CONCLUSION

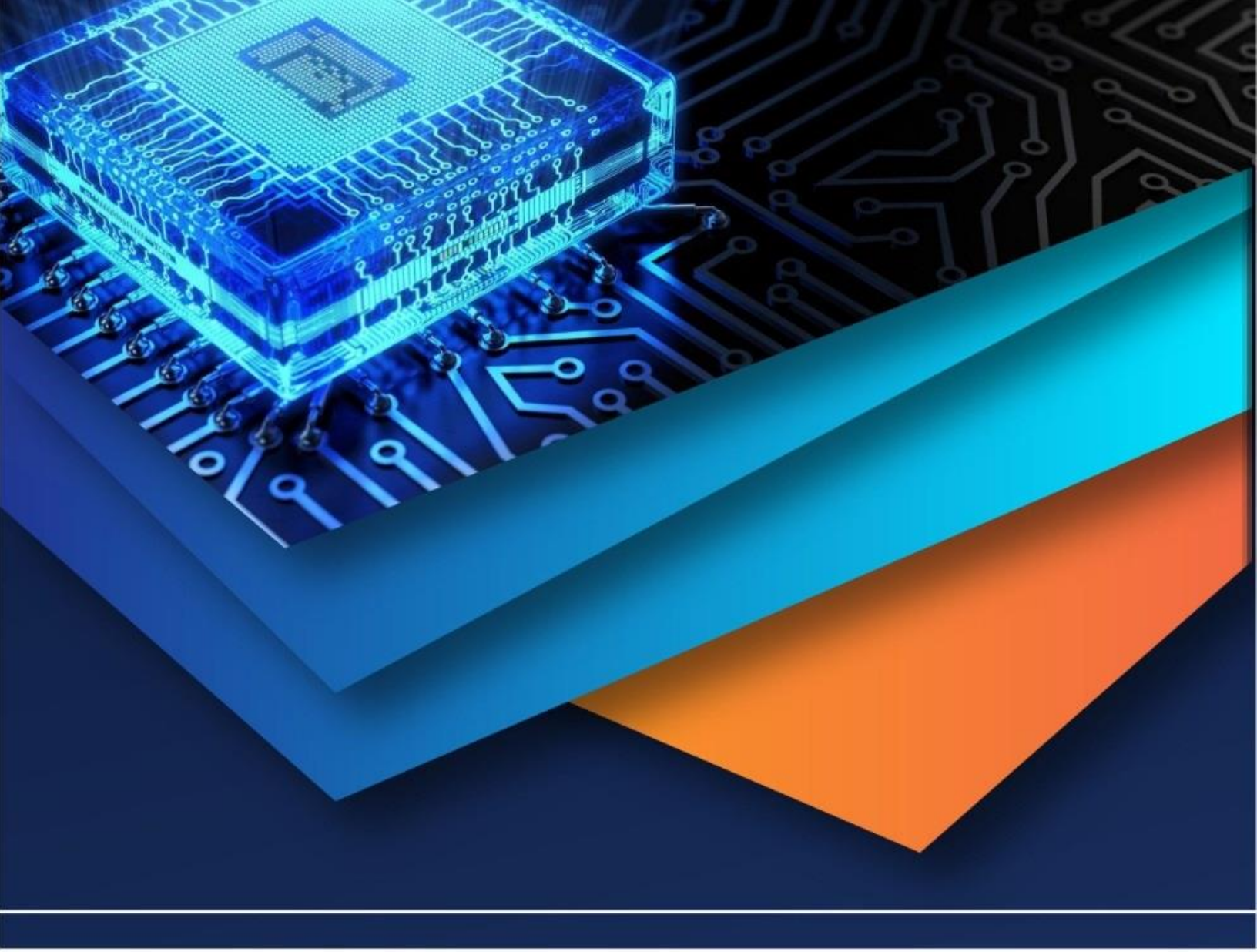
From the experimental results the hash function is used for condensation of message in message authentication schemes is used. Montgomery addition dobling is performed to do point multiplication. From the comparison blocks we get sha-1 block takes less area compared to PRNG.Point multiplication takes less and the fastest operation compare to previous results. Signature generation and signature verification is enhanced by using this modules which provides security .

## REFERENCES

[1] N. Koblitz, "Cm-curves With Good Cryptographic Properties," Advances in Cryptology—proc. 11th Ann. Int'l Cryptology Conf., IEEE, Pp. 279-287, 1992.
[2] K. J¨arvinen and J. Skytt¨a, "Cryptoprocessor for Elliptic Curve Digital Signature Algorithm (ECDSA)," Tech. Rep., Helsinki University Of Technology, Signal Processing Laboratory, 2007
[3] Michael Hutter, Martin Feldhofer, And Thomas Plos"an Ecdsa Processor for RFID Authentication"Rfidsec, IEEE transactions volume 6370, Pp. 189–202, 2010.
[4] Benjamin Glas, Oliver Sander, Vitali Stuckert, Klaus D.Muller-glaser, And Jurgen Becker " Prime Field ECDSA Signature Processing For Reconfigurable Embedded Systems" International Journal Of Reconfigurable Computing Volume 2011
[5] Certicom Corp., SEC 1: Elliptic Curve Cryptography, Published September 20, 2000
[6] M. Adleman, R. L. Rivest, and A. Shamir. "A Method for Obtaining Digital Signatures and Public-key Cryptosystems." IEEE transactions volume 21, Pp. 120–126, 1978.
[7] Koblitz, N. "Elliptic Curve Cryptosystems" Mathematics of Computation 48, 203–209 (1987).



©IJRASET 2015: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)