International Journal of Computer Applications Technology and Research
Volume 12–Issue 05, 09-16, 2023, ISSN:-2319–8656
DOI:10.7753/IJCATR1205.1003

Protocol Built by Chaotic Map and Elliptic Curve Cryptography for Key Exchange

Dr. Abdul-Wahab Sami Ibrahim
University Mustansiriyah
College of Education, Department of Computer Science
Baghdad, Iraq

Majed Ismael Sameer
University Kufa
College of Computing and Mathematics
Department of Computer Science
Baghdad, Iraq

Abstract: The elliptical curve system has received great interest in the science of security systems, and this has a great number of advantages. When linked with chaotic systems, it gave a broad comprehensiveness in the science of finding common keys between the two parties or in a system as a server that distributes the common keys among the participants in the distress.

The proposed algorithm reduces processor load, reduces power consumption, increases processing speed, enhances storage efficiency , requires smaller certificates, and is good at saving bandwidth. Where ECC gives high-level arithmetic operations ECC is an algebraic structure in wide areas for a large number of points and any point in the Cartesian coordinates, as well as for a number of prime numbers generated from the chaotic three-dimensional system using the multiplication and addition algorithm of the elliptical curved system. This paper suggested a new event in the implementation method: the inputs to the elements of the controlling parameters and the initial conditions of the symmetric chaotic functions produce an ECC by a secret shared key between two parties or a number of parties participating in the group, and all these points of the share keys lie on the points of the curve. and this key technology is available for authentication, confidentiality, and non-repudiation.

Keywords: Diffie-Hellman; communication channe l;ECC; chaotic map; share key .

1. INTRODUCTION

The main benefit of using ECC technology is that it provides the same level of protection with a smaller switch length compared to RSA. Thus, it will reduce the execution time of the algorithm processing as well as reduce the processing cost [1, 2]. Elliptic Curve Cryptography (ECC) is a popular algorithm that provides a higher level of security.

Smaller key sizes with lower resource consumption, which makes it an ideal choice for resource-constrained devices. The unpredictability introduced by the chaotic maps in the proposed algorithm is in addition to the fact that the algorithms make the model easy to implement, fast, and powerful against the attacker. The more coordinated the chaotic functions, the higher the level of safety and the better the quality. Chen et al. [3] suggest a symmetric image encoding algorithm with a 3D cat map and logistics map for mixing image data with an extra layer of confusion between them, resulting in an image with normal encoding after every two rounds of mixing. The cryptography also uses Chen's chaotic key generation system. Parrick and others [4] used as a result of two logistics maps to choose one of the eight randomly designed modes to encode every pixel in the image. Designed by Liu and Wang [5] as a one-time master-stream encoding for color image encoding on a piecewise linear chaos map (PWLCM) to calculate mainstream color image coding. The main stream is based on another sequence obtained from the Chebyshev map.

The authors, Moncef Amara and Amar Siad [6], discussed elliptical curve coding (ECC) and its performance in In terms of speed of implementation and security compared to traditional encryption algorithms like RSA, Points are generated by specifying the prime number P. The authors Ali Soleyamani, Md. Jan Nordin, and Zulkarnain Md. Ali discussed [7]. ECC The map table method is used to encode the image. ECC points are generated by choosing the largest Prime No. A mapping table is generated using points created by an elliptical curve. The points generated are set image pixels to perform encoding.

Requires good ECC technology awareness and a mathematical background compared to elliptical curves. elliptic curves In addition, elliptic curves are not ellipses [8, 9], and after all, they are It is defined as an ellipse because EC is a derivative of cubic equations (1). Sangook Moon: To perform numerical operations, develop a more efficient and novel approach to scalar point multiplication from the method of double multiplication and existing addition, then apply redundant recoding that originates from the root. 4 Booth's algorithm [10] L. Young. sign to Aydos et al protocol is not safe for humans in midfield attack by any attacker [11].

Koblitz and Miller were the first to use the elliptic curve cryptography technique [12]. Ravi Kodali and N. Sarma use Elliptic Curve Cryptography symmetric encryption with the Koblitz's encoding to encode or map the data into points locating on the Elliptic Curve, and it is one of the main basics of the Elliptic Curve Cryptography [13]. J. Nafeesa Begum and others Improved multi-level defensive messaging system ECC access control defense message system Redirects a message to parties or recipients based on message criteria for quick action [14]. Several algorithms have been developed to solve the problem. However, the effectiveness of any algorithm is determined by the type of curve and the properties of k, where k is a random number [15]. Arezou and others [16] have made effective use of the elliptic curve cipher in building a three-factor authentication.

system for satellite communications when it comes to implementing ECC cloud computing security.

Kumar & Grover's and other [17] focused on applying the ECC algorithm for encryption and decryption processes to improve cloud computing security and protect privacy. Anand and Perumal [18] introduced a method to prevent any user from gaining unwanted access to confidential data stored in the cloud. (ECC) is known to be superior to public-key cryptography approaches in wireless devices. Helps reduce device processing time. Wang and others [19] presented a work based on the concept of ECC and introduced a new way to secure ECC output. Shenet and others [20] The Java language facilitated the usage of ECC by analyzing its capabilities and dealing with digital signatures, key exchange, and key generation.

2. RESEARCH PROBLEM

The problem of generating share keys between the two parties using the Diffie-Hellman algorithm is not solved in large numbers due to the time delay in implementing the protocol with a large number of iterations, which leads to a decrease in the efficiency of the implementation of the algorithm. The research problem was solved by making the protocol algorithm strong, solid, and robust against fraudulent party attacks. This is done by using chaotic functions that are related to certain properties, such as the sensitivity of parameters and initial conditions[21,22,23].

The research problem is solved by making the protocol algorithm robust against fraudulent party attacks, and this is done by using chaotic functions associated with certain properties such as sensitivity parameters and initial conditions. And the results of that algorithm are from research [24,25,26]. It led to the generation of common keys between the two parties or between the two parties for the common keys, and these shared keys are in the form of points with arranged pairs and are located exclusively on the points of the curve, which makes the protocol algorithm strong and strong against fraudulent attacks.

3. ELLIPTIC CURVES OVER REAL NUMBERS

Elliptic curves are not elliptical[12] .It is so named because it is described by cubic equations, similar to those used to calculate the circumference of an ellipse. In general, cubic equations for elliptical curves take the following form, known as the Weierstrass equation (1):

$y^2+axy+by=x^3+cx^2+dx+e$……………….(1)

where a,b,c,d and e are real numbers and take on values in the four real numbers.For our purpose, it is sufficient to limit ourselves to the form of equations (2).

$y^2=x^3+a\,x+b$………………………………..(2)

Such equations are said to be cubic, or of three degrees, because the highest exponent they contain is a three [21, 22]. The elliptic curve (E) is a non-singular algebraic plane curve defined over a finite field Fp, where x, y, a, b Fp. The clarity of this equation (2) is shown in figure 1

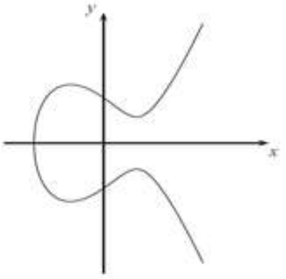

FIGURE 1. An Elliptic Curve E defined over a finite field Fp

3.1. Addition And Multiplication Of Elliptic Points

Assuming P1 ,P2 and R be three points on ellipse curve[23].Let

The addition stage first method used is R=P1+P2=(xR,yR) is determined by the following rules(3) and (4).

m=(y2-y1)/(x2-x1) mod p if P1 not equal P2 or

m=(3x1^2+a)/(2y1) mod p if P1 equal P2

xR=(m^2−x1−x2) mod P ………….(3)

yR =(m(x1−xR) – y1) mod P ………….(4)

Where a,b are coefficients of equation (2) and x ,y are coordinates.

The Multiplication stage second is defined as repeated addition; for example,

4P1=P1+P1+P1+P1 .

For example, let P1=(3,10) and P2=(9,7) then

m=((7-10)/(9-3))mod 23=(-3/6)mod 23=(-1/2)mod 23=11

xR=(11^2-3-9)mod23=17

yR=(11(3-17)-10)mod 23=20

P1+P2=(17,20)

To find 2P1|

m=((3(3^2)+1)/2*10)mod 23=6

xR =(6^2-3-3)mod 23=7

yR =(6(3-7)-10)mod 23=12

And then 2P1=(7,12)

Note: To generate a curve with about 2^160 points, a prime with a length of about 160 bits is required.

4. AN OVERVIEW ON HENON CHAOTIC MAP SYSTEM

In this section, an overview on Henon chaotic map system as important one of the 3-D chaotic map systems, which is used in this work. Henon chaotic map system is described by formula 5 which illustrates a set of the three function of Henon chaotic map system[24,25,26].

x(i+1)=a-(y(i)^2)-b*(z(i)) |
y(i+1)=x(i) |…………(5)
z(i+1)=y(i) |

when initial values 1.54<|a |<2, 0<|b |<1. and -0.9<=(x or y or z)<=1

x(1)=1; y(1)=0;z(1)=0; %% Initial conditions The initial value are x=1, y=0.1, z=0,

N=5000; %% let N is the number of iterates example

a=1.6;b=0.2; %% Sets the parameters example

it has a chaotic attractor as shown in Fig.(2).

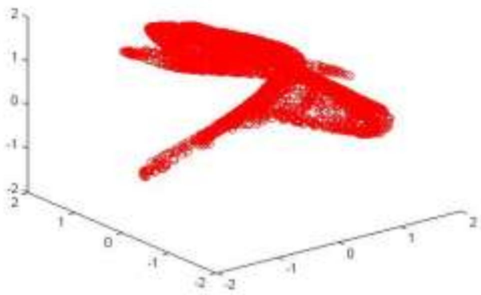

Fig.(2) Three Dimension Henon Map

5. DESIGN PROTOCOL BASED ON HENON CHAOTIC MAP AND ECC Square

Discusses the design of the proposed algorithm for the shared key exchange protocol between the parties or parties using chaotic functions of three dimensions in order to create a secure channel in order to exchange information in a reliable and secure manner against hackers and attackers of the protocol shown in the figure (3).

All the notations used in the Henon maps protocol are described in Table 1. Assume Alice and Bob are two participants in a key agreement process. The algorithm consists of the following parts:

STEP 1 :Inlet two parameter a , b and three Initial conditions Xo ,Yo, Zo to the Henon chaotic map system .

STEP 2: Operation between multiplication or any operation between them output henon maps.

STEP 3:Extract primary Pi from step 2.

STEP 4:Alice compute Ya .

In the form of ordered pairs calculated from the points through the proposed algorithm and its output, which is located within the points of the elliptic curve

then send to Bob.

STEP 5:Bob compute Yb.

In the form of ordered pairs calculated from the points through the proposed algorithm and its output, which is located within the points of the elliptic curve.

then send to Alice.

STEP 6 :Both Alice and Bob are compute K=share key.

In the form of ordered pairs calculated from the points through the proposed algorithm and its output, which is located within the points of the elliptic curve.

Table 1: Notations used in Henon's Maps Protocol

Symbol	Definition
A,B	Identifiers of Alice and Bob, respectively
Xa ,Xb	Private key for A and B
P	Primary number hidden
Ya= In the form of ordered pairs calculated from the points through the proposed algorithm and its output, which is located within the points of the elliptic curve	Send to B
Yb= In the form of ordered pairs calculated from the points through the proposed algorithm and its output, which is located within the points of the elliptic curve	Send to A
K= In the form of ordered pairs calculated from the points through the proposed algorithm and its output, which is located within the points of the elliptic curve	Finally established session key between Alice and Bob
K=Ha=Hb	note

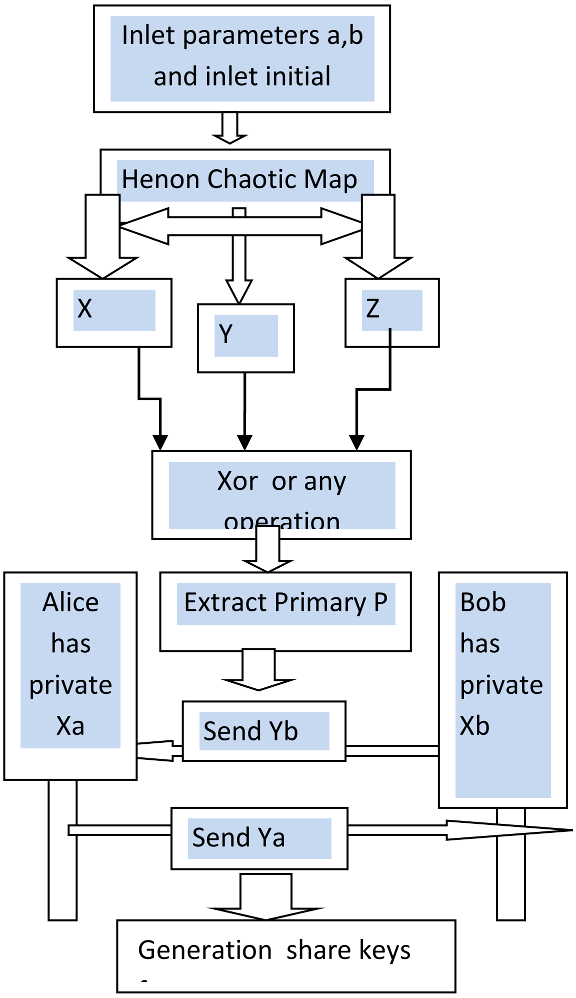

Fig. (3) General diagram of the protocol relay on chaotic and ECC

An important steps in design the proposed protocol :Extract primary Pi from step 2.

First : Let's give a more detailed definition of a prime number.

The algorithm that was used to design and extract the prime numbers is shown as in the table(2)

The algorithm that was used to design and extract the prime numbers is shown as in the table(2)

Table (2 Prepare the primes numbers from chaotic sequences results

```
Algorithm Prepare the prime numbers  from step 2
Stage
Process:
Input:
P1: chaotic sequences results from step 2
N=number of iteration
Output:
Prepare the prime numbers  sequences
Initial:
m=0;
 Loop i ← 1 to N
   if(isprime(p1(i(((
        m=m+1
      hh(m)=p1(i(
   end if
End Loop i;
Loop i ←1 to m
    if hh(m)>=2
print ←prime number hh(m)
end if
End Loop m;
End.
```

Second : Alice will need the primes generated by the proposed algorithm, and then she will need the private key Xa to generate the public keys in the form of ordered pairs located within the points of the ellipse and send them to Bob. Likewise, Bob will also need the primes generated by the proposed algorithm, and he has the private key Xb to generate Public keys in the form of ordered pairs are located within the points of the ellipse and send to Alice.

Third: Here each party will generate the common key or a number of common keys and also be in the form of arranged pairs and located within the curve points of the ellipse, and these keys can be distributed to the rest of the participants in the exchange of information within the security communication channels.

6. ANALYZE AND EFFICIENCY OF THE PROPOSED PROTOCOL

In this paper , a practical programs of a proposed algorithm and a practical programs of all experimental and security analysis tests are designed by using MATLAB language release R2012a for 64bit Windows 7 Home Premium operating system. The computer used to perform these tests is a Dell Laptop with Intel (R) Core™ i3-3217u CPU@ 1.8GHz and 6 GB installed memory.

We have two parameter a=1.4 b=0.3

and three initial condition Xo=0.1 ,Yo=0.1 and Zo=0.3

Number of Iteration =50

Alice has private key Xa=3

Bob has private key Xb=9

Alice and Bob are Compute Pi as the hide from chaotic map three dimension

Pi=primary number =2441 281 293 1867 269 2113 139 331 1447 2063 307

Extract from each prime number a number of pairs that lie at the points of the curve of equation (1) for the following algorithm of generating a number of points for the arranged pairs that fall within the points of the ellipse in table(3).

Table(3) Algorithm of generate a number of points for the arranged pairs that fall within the points of the ellipse

```
Algorithm Prepare the generate a number of points for
the arranged pairs  that fall within the points of the
ellipse.
Process:
Input:
P: primary number
Output:
Prepare the generate a number of points GEN( a,b,p)
sequences
Initial:
i=1;
G=[];
for x=0:p
    for y=0:p
        if mod(y^2,p)==mod((x^3+a*x+b),p)  % This
equation must be satisfied by x and y for the given
value of a, b and p.
            G(i,:)=[x y];
            i=i+1;
        else
        end;end;end; End.
```

The results after applying the algorithm in the table (3) are shown:

```
GEN( a, b, p)
 >> [G]  =GEN( 2,2, 2441)
At p=2441
G =
         0        837
         0       1604
         1        759
         1       1682
         4        131
         4       2310
         5        523
         5       1918
         6        899
         6       1542
        11        415
```

And so continue from the result. But we choose one of those pairs that lie within the points of the curve of equation (2). And let the pair be in the fifth sequence, which is

```
     4    131
At     p= 281
>> [G]  =GEN( 2,2,281)
G =
    0   132
    0   149
    1    75
    1   206
    2    24
    2   257
    3    63
    3   218
    5    74
    5   207
    7    42
    7   239
    8   116
```

```
8   165
11   136
```

Table(4) Multiplication algorithm for the ellipse curve

```
Algorithm Prepare the generate a number of points for
the arranged pairs that fall within the points of the
ellipse.
Process:
Input:
P: primary number; a,b,p,n,x,y
Output:
Prepare the results of multiple private key with function
GEN generate a number  pair sequences
Initial:
if n ==1
    resx = x;
    resy = y;
    return;
end
if n>=2
    [xsub,ysub]=NP(a,b,p,n-1,x,y);
    if xsub==Inf && ysub == Inf
        resx=Inf;
        resy=Inf;
    else
        [resx,resy]=Add(a,b,p,x,y,xsub,ysub);
    End;end;end;
End.
```

And so continue from the result. But we choose one of those pairs that lie within the points of the curve of equation (2) .And let the pair be in the fifth sequence, which is

2   24

The process will continue for the rest of the prime numbers generated by the chaotic three-dimensional calculation algorithm.

The next step is:

The multiplication algorithm for the ellipse curve is algorithm of NP .It is shown in Table No.(4)

Note that the private key for Alice =3. The result was the creation of a file for each party, as follows:

First:

Private key for Alice=3

And because the addition is multiplication, for example, P+P=2P because p first same as p another.

But 3P=P+P+P we need algorithm add curve ellibts because 3P=P+P+P=2P+P then 2P not similar to P.

Say to Q=2P then 3P=2P+P=Q+P

And as follows for the addition algorithm .It is shown in Table No.(5) for the ellipse.

Table(5) The addition algorithm for the ellipse

```
Algorithm Prepare the generate a number of points for
the arranged pairs that fall within the points of the
ellipse.
Process:
Input:
P: primary number; a,b,p,n,x,y
Output:
Prepare the results of multiple private key with function
GEN generate a number  pair sequences
Initial:
function [ resx,resy ] = Add( a,b,p,x1,y1,x2,y2 )
if x1==x2 && y1==y2
    k=modfrac(3*x1^2+a,2*y1,p);
    resx = mod(k^2-x1-x2,p);
    resy = mod(k*(x1-resx)-y1,p);
end
if x1==x2 && y1~=y2
    resx = inf;
    resy = inf;
end
if x1 ~= x2
    k=modfrac(y2-y1,x2-x1,p);
    resx = mod(k^2-x1-x2,p);
    resy = mod(k*(x1-resx)-y1,p);
end;End.
```

When we use the addition and multiplication algorithm together, we will get the following results.

Note that the private key for Alice =3

Alice compute YA1 of the Elliptic curves then send to Bob

YA1=

```
*****************
470   485
11   136
254   233
241   1183
156   8
2064   140
53   106
295   291
961   551
932   471
158   58
```

And also ,Private key for Bob=9

Bob compute YB1 of the Elliptic curves then send to Alice

YB1=

```
288   579
224   118
166   263
1851   1044
```

251	66
878	1195
33	137
239	142
727	100
1768	1808
245	157

Alice compute Share key of the Elliptic curves

K=

1708	39
60	95
196	228
681	313
134	13
736	439
34	68
74	237
50	667
1245	1193
300	140

Bob compute Share key

K=

1708	39
60	95
196	228
681	313
134	13
736	439
34	68
74	237
50	667
1245	1193
300	140

When Alice receives the pop file, Alice will also use the multiplication and addition algorithm to find the common keys between Alice and Bob, and also does the same process for Bob's steps, and the results are as follows for the shared keys

The table of share keys obtained by Alice from the algorithm

1708	39
60	95
196	228
681	313
134	13
736	439
34	68
74	237
50	667
1245	1193
300	140

The table of share keys obtained by Bob from the algorithm

1708	39
60	95
196	228
681	313
134	13
736	439
34	68
74	237
50	667
1245	1193
300	140

And because the time taken to implement is of great importance to the protocol, it depends on the number of iterations that must be implemented for the chaotic Henon-maps three-dimensional functions. The higher the number of iterations, the longer the time for executing the protocol algorithm and the results shown as shown in the table (6), which shows the relationship between the time taken to implement the algorithm with the number of iterations to implement the protocol.

Table (6) Correlation time taken to implement the algorithm with the number of iterations

Number of iteration	taken to implement the algorithm	Number of participants in group
25	6.041915	6
50	8.808280	11
60	9.243908	12
70	13.124462	14
85	13.040652	14

7. Analysis of the key space

In the proposed algorithm, Henon's chaotic function maps are generated, and each requires a control parameters value and a sequential initial conditions value for the chaotic map. where they are used as input of algorithm protocol keys, if the underlying control variables and values are precisely in 10^14,

the total space of the Key 10^5 x10^5 x10^5x10^5x10^5=10^25

that length 10^25 very good for resistant brute

8. CONCLUSIONS

The protocol for the ECC algorithm was developed using the chaotic functions of the three-dimensional Hennon-Map system, the symmetry of this algorithm was introduced with the control of parameters and conditions of the initials. You get the results of this protocol algorithm to give different results while changing from the very slight input, from the implementation and analysis of the algorithm as presented, the following conclusions are obtained:

1. Prime numbers are hidden and not public. It is only visible in matlab code because it will be among the software accounts in Matlab code, sender code, and recipient code.

2. It is possible to increase the number of participants in the group by increasing the number of common keys that they exchange among themselves, and this work is inferred by increasing the number of iterations that are made for the three-dimensional chaotic functions of Henon maps. Also, the results showed that there were a limited number of participants. The number can be increased by increasing the power of the computer specifications.

3. Any change in the value of the corresponding input values between the two parties will make these keys, which act as input sensitive, sensitive to those changes in case of manipulation or attack, such as changing any key of the values entered into the algorithm from the control parameters or initial conditions, and it will be very sensitive because it will display results. Shared keys other than the previous original results between the two parties when manipulating any number of required bits and the algorithm will be efficient and effective for all anti brute force attack programs.

It should include trust and security between the group participants so that keeping the corresponding entries is guaranteed by certain entities of the protocol algorithm distribution and not just known to some unspecified party .If only two parties share the common key and there are no participants in the set, an arithmetic operation can be performed, such as adding up the points for the shared keys that are within the points of the ellipse for that set.

9. REFERENCES

[1] W. Diffie and M. E. Hellman. New directions in cryptography. IEEE Trans. Inform. Theory, IT-22 :644-654, Nov 1976.

[2] A. M. Johnston, P. S. Gemmell, “Authenticated key exchange Provably Secure Against the Man-in-Middle Attack”, Journal of Cryptology, Springer , 2002, Vol. 15 Number 2 pp. 139-148.

[3] G. Chen, Y. Mao, and C. K. Chui, ‘‘A symmetric image encryption scheme based on 3D chaotic cat maps,’’ Chaos, Solitons Fractals, vol. 21, no. 3, pp. 749–761, Jul. 2004.

[4] N. K. Pareek, V. Patidar, and K. K. Sud, ‘‘Image encryption using chaotic logistic map,’’ Image Vis. Comput., vol. 24, no. 9, pp. 926–934, Sep. 2006.

[5] H. Liu and X. Wang, ‘‘Color image encryption based on one-time keys and robust chaotic maps,’’ Comput. Math. with Appl., vol. 59, no. 10, pp. 3320–3327, May 2010.

[6] Moncef Amara and Amar Siad, “Elliptic Curve Cryptography and its Applications”, IEEE 7th Int. Workshop on Systems, Signal Processing and their Applications, (2011), 247-250.

[7] Ali Soleyamani, Md Jan Nordin,Zulkarnain Md Ali, “A Novel Public Key Image Encryption based on Elliptic Curves over Prime Group Field”, Journal of image and Graphics, (2013), Vol. 1 No.1, 43-49.

[8] William Stallings, "Cryptography and Network Security Principles and Practice", Fifth Edition, 2011,300p.

[9] Darrel Hankerson, Alfred Menezes and Scott Vanstone, Guide to Elliptic Curve Cryptography", © SpringerVerlag New York, Inc. ,2004,14-30p

[10] Sangook Moon, "A Binary Redundant Scalar Point Multiplication in Secure Elliptic Curve Cryptosystems", International Journal of Network Security, Vol.3, No.2, 2006, PP.132-137.

[11] Liu Yongliang, Wen Gao, Hongxun Yao, and Xinghua Yu , "Elliptic Curve Cryptography Based Wireless Authentication Protocol", International Journal of Network Security, Vol.4, No.1, 2007, PP.99-106.

[12] V. Miller, “Uses of elliptic curves in cryptography”, in Proceedings of the Conference on the Theory and Application of Cryptographic Techniques (CRYPTO), 1985, pp. 417–426.

[13] Ravi Kishore Kodali and N.V.S Narasimha Sarma, "ECC Implementation using Koblitz’s Encoding", in Proceedings of the Conference on Communication Engineering and Network Technologies (CENT), Elsevier, 2012, pp. 411- 417.

[14] J. Nafeesa Begum, K. Kumar and Dr. V. Sumathy, "Multilevel Access Control in Defense Messaging System Using Elliptic Curve Cryptography", in Proceedings of the International Conference on Computing Communication and Networking Technologies (ICCCNT), IEEE, 2010, pp. 1-9.

[15] Kumari, A., Jangirala, S., Abbasi, M. Y., Kumar, V., & Alam, M.,“ESEAP: ECC basedsecure and efficient mutual authentication protocol using smart card,”Journal of Information Security and Applications,51, 102443, 2020.

[16] Arezou Ostad-Sharif, Dariush Abbasinezhad-Mood, Morteza Nikooghadam, “Efficient utilization of elliptic curve cryptography in design of a three-factor authentication protocol for satellite communications,”Computer Communications 147, 85–97, 2019.

[17] Kumar, D., & Grover, H. S.,“A secure authentication protocol for wearable devicesenvironment using ECC,”Journal of Information Security and Applications,47, 8-15, 2019.

[18] Anand, S., & Perumal, V.,“EECDH to prevent MITM attack in cloud computing,”Digital Communications andNetworks,5(4), 276-287, 2019.

[19] Wang H., He D., Ji Y., “Designated-verifier proof of assets for bitcoin exchange using elliptic curve cryptography,”Future Generation Computer Systems, 2017.http://dx.doi.org/10.1016/j.future.2017.06.028.

[20] Shen, Y., Sun, Z., & Zhou, T.,“Survey on Asymmetric Cryptography Algorithms,”In2021 IEEE International Conference on Electronic Information Engineering

and ComputerScience (EIECS)(pp. 464-469), September, 2021.

[21] Rashmi K. Gawande, Pravin S. Kulkarni & Kamlesh A. Ganar,"Multi Level Image Encryption using Chaotic Mapping And Elliptic CurveCryptography",International Conference On Engineering Innovation and Technology, ISBN : 978-93-81693-77-3, Nagpur, pp. 69-70,1st July, 2012.

[22] PRIYANSI PARIDA , CHITTARANJAN PRADHAN , XIAO-ZHI GAO ,DIPTENDU SINHA ROY,"Image Encryption and Authentication With Elliptic Curve Cryptography and Multidimensional Chaotic Maps ",Received March 10, 2021, accepted March 31, 2021, date of publication April 9, 2021, date of current version June 1, pp.76191-76192,2021. Digital Object Identifier 10.1109/ACCESS.2021.3072075 .

[23] Revanna C R, Keshavamurthy C,"Hybrid Method of Document Image Encryption using ECC and Multiple Chaotic Maps ",International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8 Issue-4, pp.1615-1616,November 2019.

[24] Alia Karim Abdul Hassan," Proposed Hyper chaotic System for Image Encryption"(IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 7, No. 1, pp.37-38,2016.

[25] W. Strunk Jr., E.B. White, The Elements of Style, third ed., Macmillan, New York, 1979, 350 p.

[26] Dr. Abdul-Wahab Sami Ibrahim ,Majed Ismael Sameer, " Protocol Build by chaotic map for Exchange Key Share", IJCSIS July 2022 Volume 20 No. 7 , ISSN 1947 5500.