International Journal of Pure and Applied Mathematics
Volume 119 No. 15 2018, 1043-1049
ISSN: 1314-3395 (on-line version)
url: http://www.acadpubl.eu/hub/
Special Issue

http://www.acadpubl.eu/hub/

Safe communication and custody of the password using Elliptic Curve over finite field

[1]D. Sravana Kumar

[1] Associate Professor in Physics,

Dr VS Krishna Govt.Degree College,

Visakhapatnam, India

skdharanikota@gmail.com

[2]CH. Suneetha

[2]Associate Professor in Mathematics,

GITAM University,

Visakhapatnamn India

gurukripachs@gmail.com

[3]P. Sirisha

[3] Faculty in Mathematics,

Indian Maritime University,

Visakhapatnam, India

sirinivas06@gmail.com

Abstract-In the modern digital world electronic communication has become mandatory. In these days we need password or PIN everywhere. Encryption, communication and memorizing the password have become annoying and painful difficulties in digital network. The task of cracking the password is a piece of cake for the active intruder of the present generation to gain unauthorized data. In the present paper authors designed an innovative method for safe communication and custody of the password or PIN using elliptic curve over finite field.

Key Words-Elliptic curve over finite field, Encryption, Decryption

I. INTRODUCTION

Despite the fact that the password is very small in size with low entropy it is vital in all transmissions. The rapid progress of the digital platform for all types of communications has given the place for cyber attacks like password cracking, interrupting the communication etc. A potential intruder easily nabs the password through social engineering. In order to improve security and robustness of the password it is necessary to shield it and transmits very securely. The present paper explains an innovative method for safe custody of password or PIN in its journey from one source to the other via public channel.

II. LITERATURE SURVEY

In 1992 Bellovin and Merritt [1] have given a protocol Encrypted Key Exchange (EKE) using combination of symmetric and public key cryptography to resists dictionary attacks. It is a classical Diffie-Hellman key exchange protocol where both the flows are encrypted with password as common symmetric key. Many additions have been done to extend EKE addressing the issues plaintext equivalent attacks. Gong et.al [2] proposed public key techniques in conjunction with password authentication. In that paper they suggested that an authenticated server with pair of private or public keys protects weak human passwords Aagainst strong attacks. Tsenget.al.[3] employed Diffie-Hellman key exchange scheme to repair the security flaws using one-way hash function. But Yang et.al.[4] pointed out that Tseng's protocol improved the password scheme but it has the weakness of Denial of Service (DOS) attack. They identified that in Tseng's scheme an adversary can intercept the action "request for change

of password" by the legal user and can modify the password without the notice of the legal user. In this direction of improvement of key exchange protocols David Cash et.al.[5] proposed Twin Diffie-Hellman protocols similar to the computation of D-H problem. M.Bellare et.al. [6] constructed user friendly password based protocols for group communications such as e-conference. Bholi [7] poposed a framework for robust group key agreement. The plan of the framework gives the security of the password against harmful insiders of the group and active adversaries in the public network. In 2009 Huang et.al. [8]proposed some group key protocols by using Discrete Logarithm Problem DLP to increase the efficiency of Tseng's scheme. D. Mahto, Dilip Kumar Yadav[9] proposed a scheme for enhancing the security of one time password by using elliptic curve. All these protocols contain many security flaws and proved to have informal arguments subsequently by other researchers.

III. ELLIPTIC CURVE CRYPTOGRAPHY (ECC)

A. An affine equation E

$$y^2 + b_1xy + b_3y = x^3 + b_2x^2 + b_4x + b_6 \quad (1)$$

over the set of real numbers is said to be weierstrass equation, where b_1, b_2, b_3 ,b_4, b_6 and x, y are real numbers. An elliptic curve for cryptographic purpose is defined by the equation over the prime field F_p.

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

B. Group laws of elliptic curve

Let E be an elliptic curve defined over the finite field of integers K. Addition of two points uses chord-and-tangent rule to get the third point [1,2,3]. The set of all points on the elliptic curve over the finite field with addition as binary operation forms an abelian group with ∞, the point at infinity as identity element.

C. Geometric rules of Addition

Let $P(x_1,y_1)$ and $Q(x_2,y_2)$ be two points on the elliptic curve E. The sum of the two points P and Q is $R(x_3,y_3)$ which is the reflection of the point of intersection of the line through the points P, Q and the elliptic curve about x axis. The same geometric interpretation also applies to two points P and –P, with the same x-coordinate. Here the points are joined by a vertical line, which is regarded as the intersecting point on the curve at the point infinity. P + (-P) = ∞, the identity element which is the point at infinity [1,2,3].

D. Doubling the point on the elliptic curve

If $P(x_1,y_1)$is point on the elliptic curve then 2P is the reflection of the point of intersection of the tangent line at P and the elliptic curve about x axis [1,2,3].Example of addition of two points and doubling of a point are shown in the following figures 1 and figure 2 for the elliptic curve

$$y^2 = x^3-x. \quad (3)$$

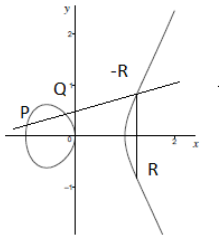


Figure 1.Geometric addition

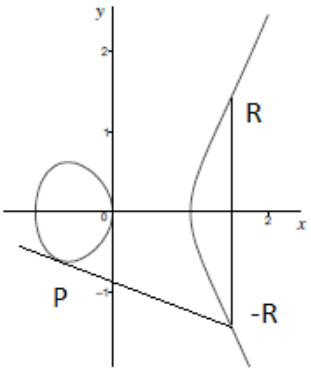


Figure 2. Geometric doubling

1) *Identity :* P + ∞ = ∞ +P = P for all E where ∞ is the point at infinity.

2) *Negatives*: If P(x,y) is a point on the elliptic curve then(x,y) + (x,-y) = ∞. Where $(x,-y)$ is the negative of P denoted by –P.

3) *Point addition:* If $P(x_1,y_1)$, $Q(x_2,y_2)$ are two points where P ≠ Q. Then P + Q = (x_3,y_3) [1,2]where

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2 \text{ and}$$

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

4) *Point Doubling:* Let $P(x_1,y_1) \in E(K)$ where $P \neq -P$ then

$2P = (x_3, y_3)$ [1,2] where $x_3 = \left(\frac{3x_1^2 + a}{2y_1} \right)^2 - 2x_1$ and

$y_3 = \left(\frac{3x_1^2 + a}{2y_1} \right) x_1 - x_3 - y_1$

5) *Point Multiplication:* Let P be any point on the elliptic curve over the prime field of integers. Then the operation multiplication of P is defined as repeated addition [17]. kP = P+P+……..ktimes.

E. Elliptic Curve Discrete logarithmic Problem(ECDLP)

The strength of Elliptic Curve Cryptography depends on the hard problem known Elliptic Curve Discrete Logarithmic Problem [3,4,6,19,20]. Consider an equation Q = xP where $Q,P \in E(F_p)$ the elliptic curve over the prime field and $x \in [1,2,\ldots\ldots p-1]$. It is relatively easy to calculate Q given x and P. But it is relatively hard to determine $x = \log_P Q$ given Q and P .

F. Parity of a Number

Parity of an integer is its quality to decide whether the number is odd or even. It depends on the remainder when the number is divided by 2. An even number has 0 parity and an odd number has parity 1. The parity function is a Boolean function plays role in theoretical investigation of circuit complexity.

G. Circular Shift

Circular shift is the operation of sliding the bits to next positions either by moving first entry to last or last to first. It is just similar to the cyclic permutation that is mainly used for cryptography to permute the bit sequences. For instance if $B = b_0\ b_1\ b_2\ b_3\ b_4\ b_5\ b_6\ b_7$ circular right shift 3 times represents $B_1 = b_5\ b_6\ b_7\ b_0\ b_1\ b_2\ b_3\ b_4$ and circular left shift represents $B_1 = b_3\ b_4\ b_5\ b_6\ b_7\ b_0\ b_1\ b_2$

H. Proposed Method

To overcome the security flaws ofmentioned in the above survey the present paper explains secure transmission of the password from one source to the other. Here the encrypted password is embedded in a large random text at different selected positions and communicated to the other entity via public channel using elliptic curve over finite field. The positions where the encrypted password characters in the large random text are selected by the host and calculated by the receiver. In the present system an elliptic curve over finite field # $E_q(a,b)$ having large number of points on it is published. A few elliptic curves processing the below listed features are useful for cryptographic purpose to avoid the risk of many physical attacks such as side channel attack and fault attack. The good desirable features of elliptic curve for cryptographic purpose are

1. To get rid of the risk of Pollig-Hellman attack the order of the selected elliptic curve # $E_q(a,b)$ should not be factorizes into small primes

2. The curve must be non-super singular

3. The selected curve should be non-anomalous, i.e., the order # $E_q(a,b) \neq q$.

Since all the points on the elliptic curve with addition as binary operation forms an abelian group with the point at infinity as identity element, an additional note to select the elliptic curve is the order of the elliptic curve # $E_q(a,b)$ must be a prime number. Because if the order of the group is prime it is cyclic. If two users Alice and Bob want to communicate the messages via public channel they share a point G(x,y) that acts as the generator of the cyclic group as the secret for their communication. Since every point is generator of the cyclic group and the published curve has large number of points on it, multiple numbers of peers can transmit the messages simultaneously. Each party in the group of multiple peers shares the secret keys $G_1,G_2\ldots\ldots G_n$ where n is the order of the group.

1) Encryption: If Alice wants to communicate password having the characters K_i , i = 1 to 4 ($K_1K_2K_3K_4$) to Bob

a) She selects 8 large random numbers n_i less than the order of the generator and calculates the points $P_i = n_iG$, where i = 1to 8.

b) Again she calculates $m_1 = [n_1n_2]_{modn3}$, $m_2 = [n_3n_4]_{modn5}$, $m_3 = [n_5n_6]_{modn7}$ and $m_4 = [n_7n_8]_{modn1}$. In computing these values Alice takes care that no two m_j are equal, where j = 1 to 4

c) Alice encrypts the password characters K_1,K_2,K_3andK_4 using three different techniques parity of numbers, circular bit shifting operation and logical XOR operation.She finds the parity of the selected random numbers n_i,i = 1 to 8 to get 8 bit binary number $B = b_1b_2b_3b_4b_6b_7b_8$. i.e, the number n_i is odd then the parity of that number is 1, otherwise 0. m_1,m_2,m_3,m_4 values computed in the above step 2 are adjusted to mod 8. The bits of the 8 bit binary number $B = b_0\ b_1\ b_2\ b_3\ b_4\ b_5\ b_6\ b_7$ are right circular shifted the number of times equal to $(m_1)_{mod8}$ to get the binary number B_1. For example if $(m_1)_{mod8}$ is 3 the bits of $B = b_0\ b_1\ b_2\ b_3\ b_4\ b_5\ b_6\ b_7$ are right circular shifted 3 times to get $B_1 = b_5\ b_6\ b_7\ b_0\ b_1\ b_2\ b_3\ b_4$. To use the technique parity of a number large random numbers n_i,i = 1 to 8 may be randomly odd and even.

d) Then logical XOR operation is performed between ASCII binary equivalent of the first character

K_1 and the binary number B_1obtained by right circular shift. The resulting 8 bit binary number is K_{1E}

$K_{1E} = B_1 \oplus$ ASCII BIN(K_1)

$K_{iE} = B_i \oplus$ ASCII BIN(K_i),

where B_i = circular Shift $B(m_i)_{mod8}$,i = 1 to 4.

e) Then the binary numbers K_{iE} ,i = 1 to 4 are coded to ASCII equivalent characters C_i ,i = 1 to 4. These characters C_1, C_2, C_3 and C_4 are inserted at the positions m_1, m_2 , m_3 and m_4 respectively in the selected random text. For instance if m_i = 356 then the 356thcharacter of the random text is replaced by the first character C_1. Similarly the character at m_i^{th} position is replaced by C_i ,i=1 to 4

f) Alice communicates the points P_i , i = 1 to 8 and the random text in which the encrypted password characters are embedded to Bob via universal channel.

J) Decryption

Before decrypting the password Bob constructs table of all points on the elliptic curve as multiples of generator G $P_i = n_iG$

1. After receiving the random text and points $P_i = n_iG$ first picks up the values n_i , where i = 1to 8 from the constructed table.

$P_1 = n_1G$, $P_2 = n_2G$ and so on.

2. He calculates the values $m_1 = [n_1n_2]_{modn3}$, $m_2 = [n_3n_4]_{modn5}$, $m_3 = [n_5n_6]_{modn7}$ and $m_4 = [n_7n_8]_{modn1}$ where the encrypted password characters are inserted.

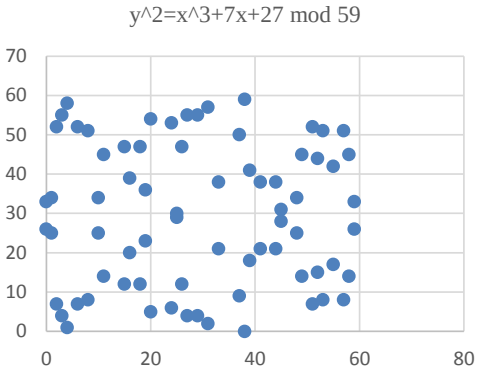
3. Then Bob locates the encrypted password characters at the positions m_1, m_2, m_3, m_4 respectively in the received random text. He finds the parity of the received random numbers n_i,i = 1 to 8 to get 8 bit binary number B = $b_0b_1b_2b_3b_4b_6b_7$.The above computed m_1, m_2, m_3, m_4 values are adjusted to mod 8. The bits of the 8 bit binary number B =b_0 b_1 b_2 b_3 b_4 b_6 b_7 are right circular shifted the number of times equal to $(m_1)_{mod8}$ to get the binary number B_1. Then logical XOR operation is performed between ASCII binary equivalents $K_{1E}$of the first cipher character C_1 and the binary number. The resulting 8 bit binary number is K_1.

$K_i = B_i \oplus$ ASCII BIN(K_{iE}),

where B_i = circular Shift of B $(m_i)_{mod8}$ times, where i = 1 to 4

4. Equivalent ASCII characters of B_i where i = 1 to 4 reveals the password $K_1K_2K_3K_4$

Example: Consider an elliptic curve $y^2 = x^3 + 7x + 27$ and let p = 59. This curve satisfies all the above listed required properties. Since the order of the curve $E_{59}(7,27)$ is a prime number 73 the group is cyclic. The graph of the curve is



Let the generator be G(3,55).The table expressing all the points as the multiples of generator is

1G = (3,55); 2G = (11,14); 3G = (18,47); 4G = (24,6); 5G = (25,30); 6G = (59,33);7G = (55,42); 8G = (52,15); 9G = (0,26); 10G = (2,52); 11G = (8,51); 12G = (15,47);13G = (20,5); 14G = (27,55); 15G = (39,18); 16G = (48,25); 17G = (51,7); 18G = (57,51); 19G = (59,26); 20G = (38,59); 21G = (1,25); 22G = (4,58); 23G = (10,34); 24G = (16,39);25G = (24,53); 26G = (26,47); 27G = (31,2); 28G = (37,9); 29G = (38,0); 30G = (53,8);31G = (44,21); 32G = (39,41); 33G = (0,33); 34G = (3,4); 35G = (6,52); 36G = (15,12); 37G = (19,36); 38G = (29,55); 39G = (33,38); 40G = (58,45); 41G = (53,51); 42G = (49,14); 43G = (41,38); 44G = (45,28); 45G = (2,7) 46G = (6,7); 47G = (11,45); 48G = (18,12); 49G = (25,29); 50G = (31,57); 51G = (37,50); 52G = (58,14); 53G = (52,44); 54G = (55,17); 55G = (57,8); 56G = (45,31); 57G = (41,21); 58G = (44,38);59G = (48,34); 60G = (49,45); 61G = (51,52); 62G = (10,25); 63G = (1,34); 64G = (4,1);65G = (8,8); 66G = (16,20); 67G = (19,23); 68G = (20,54); 69G = (26,12); 70G = (27,4); 71G = (29,4);72G = (33,21); 73G = ∞

5. Encryption:

a) Alice publishes the elliptic curve curve E_{59} (7,27) on public channel and shares the generator G(3,55) as the secret key with Bob. Let n_1 = 51, n_2 = 9, n_3 = 16, n_4 = 28, n_5 = 37, n_6 = 62, n_7 = 44, n_8 = 71

b) Alice calculates the points $P_1 = n_1G$= (37,50), $P_2 = n_2G$= (0,26), $P_3 = n_3G$= (48,25), $P_4 = n_4G$= (37,9) ,$P_5 = n_5G$= (19,36) , $P_6 = n_6G$= (10,25) , $P_7 = n_7G$= (45,28), $P_8 = n_8G$= (29,4)

c) Again she calculates $m_1 = (459)_{mod16}$= 11, m_2= $(448)_{mod37}$=4 , m_3= $(2331)_{mod44}$= 6, m_4 = $(3124)_{mod51}$ = 13

d) Let the password to be communicated is 'SSSg' Alice finds the parity of the selected random numbers n_i, i = 1 to 8 to get B = 11001001. Then m_1, m_2, m_3, m_4 values are adjusted to mod 8.Therefore,$m_1=(11)_{mod8}$=3, $m_2=(4)_{mod8}$=4, $m_3=(6)_{mod8}$=6, $m_4=(13)_{mod8}$=5. The bits of the 8 bit

binary number B = 11001001 are right circular shifted the number of times equal to $(m_1)_{mod8}$ = 3 to get the binary number B_1 as 00111001. Now to get B_2,B has been right circular shifted to the number of times equal to $(m_2)_{mod8}$=4.Then B_2= 10011100. To get B_3,B has been right circular shifted to the number of times equal to $(m_3)_{mod8}$=6.Then B_3= 00100111. To get B_4,B has been right circular shifted to the number of times equal to $(m_4)_{mod8}$=5.Then B_4= 01001110.

e) Then logical XOR operation is performed between ASCII binary equivalent of the first character K_1 where

K_1 = S =01010011 and the binary number B_1=00111001. The resulting 8 bit binary number is K_{1E} =01101010.i.e., K_{1E} = $B_1 \oplus$ASCII BIN(K_1)= 01101010

K_2 = S =01010011 and the binary number B_2=10011100. The resulting 8 bit binary number is K_{2E} =11001111.i.e., K_{2E}= $B_2 \oplus$ ASCII BIN(K_2)=11001111

K_3 = S =01010011 and the binary number B_3=00100111. The resulting 8 bit binary number is K_{3E} =01110100.i.e., K_{3E}= $B_3 \oplus$ ASCII BIN(K_3)=01110100

K_4 = g = 01100111 and the binary number B_4=01001110. The resulting 8 bit binary number is K_{4E} = 00101001. i.e., K_{4E}= $B_4 \oplus$ ASCII BIN(K_4)=00101001

f) Then the binary numbers K_{1E} = 01101010= j = C_1 (coded to ASCII equivalent characters)
K_{2E}= 11001111 = Ï = C_2

K_{3E}= 01110100 = t = C_3

K_{4E}= 00101001 =) = C_4

These characters C_1,C_2,C_3 and C_4 are inserted at the positions m_1=11, m_2=4 , m_3=6 and m_4= 13 respectively in the selected random text.

The encrypted message for SSSS is jÏt).Alice selects the a random plain text

"zse5thnkl(p6e&c;s0+gwi$ve5g*qnj%esdtyn@fg w7exfynkm"

The encrypted characters jÏt) are inserted in the position of 11,4,6,13 of the random text. Then Alice communicates the random text "zseÏttnkl(j6)&c;s0+gwi$ve5g*qnj%esdtyn@fgw7exf ynkm" in which the encrypted password is embedded at the positions 11,4,6,13 and the points (37,50), (0,26), (48,25), (37,9), (19,36), (10,25) ,(45,28),(29,4) to Bob in public channel.

6. Decryption:

a) Bob after receiving plain text "zseÏttnkl(j6)&c;s0+gwi$ve5g*qnj%esdtyn@fgw7exf ynkm" in which the encrypted password is embedded and the points (37,50), (0,26), (48,25), (37,9), (19,36), (10,25), (45,28),(29,4)first picks up the values n_1 = 51, n_2 = 9, n_3 = 16, n_4 = 28, n_5 = 37, n_6 = 62, n_7 = 44, n_8 = 71 from the table of points he constructed as multiples of generator.

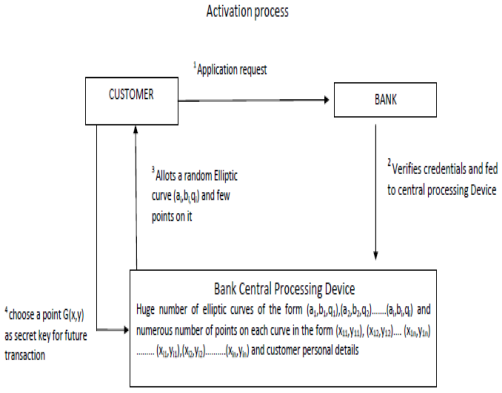
b) He calculates the values m_1 = $(459)_{mod16}$= 11 , m_2= $(448)_{mod37}$=4 ,m_3= $(2331)_{mod44}$= 6, m_4 = $(3124)_{mod51}$ = 13 where the encrypted password characters are inserted.

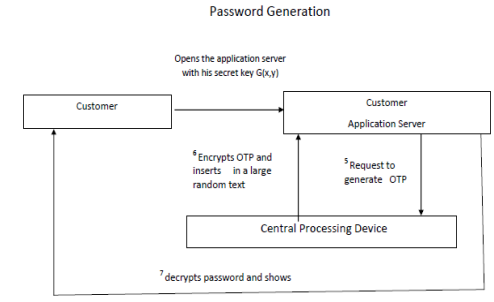
c) Bob locates the encrypted password characters 'jÏt)' in the received random text.

d) He performs logical XOR operation between ASCII binary equivalents $K_{1E},K_{2E},K_{3E},K_{4E}$of the characters jÏt) and 8 bit binary number B_1,B_2,B_3,B_4 to get 8 bit binary numbers K_1,K_2,K_3 and K_4.

$K_1 = K_{1E}$ XOR B_1 =01010011
$K_2 = K_{2E}$ XOR B_2 =01010011
$K_3 = K_{3E}$ XOR B_3 =01010011
$K_4 = K_{4E}$ XOR B_4 =01100111

e) The equivalent ASCII characters of K_1,K_2,K_3 and K_4 reveals the password "SSSg"





IV. REFERENCES

[1] Koblitz N., "Elliptic curve cryptosystems, mathematics of computation", Vol. 48, No.177, pp. 203-209, January 1987.

[2] Miller V.,"Uses of elliptic curves in Cryptography" In advances in Cryptography (CRYPTO 1985), Springer LNCS, 1985, vol. 218, pp 417-4 26.

[3] Maurer U., A. Menzes and E. Teske, analysis of GHS weil decent attack on theECDLP over characteristic two fields of composite degree". LMS journal of computation and Mathematics, 5:127-174, 2002.

[4] W.C. Ku & S.D. Wang "Cryptanalysis of modified authenticated key agreement protocol", Electronic letters Vol. 36, No. 21, 2000, pp 1770-71.

[5] Areej Omar Baalghusun, OlfaFahadAbusalem, Zahra Abbas Al Abbas, JayaprakashKar, "Authenticated Key Agreement Protocols: A Comparative Study, Journal of Information Security, 2015, 6, 51-58

[6] Steven MBellovin. Michael Merritt, Encrypted Key Exchange: Password-Based Protocols. Secure Against Dictionary Attacks https://www.cs.columbia.edu/~smb/ papers/neke.pdf.

[7] L. Gong, M. Lomas, R. Needham and J.Saltzer, "Protecting poorly chosen secrets from guessing attacks", IEEE journal on selected areas in communications, Vol.11, No.5, June 1993.

[8] Tseng Y-M, Jan,J-Y, Chien H-Y, "On the security of methods for protecting password transmission", International journal of Information, 2001,12, 469-476.

[9] Yeh,H-Y; nSun,H-M, "Simple authenticated key agreement protocol resisting to password guessing attacks", ACMSIGOPS Oper, Syst.Rev.2002,36, 14-22

[10] David Cash and EikeKiltz and VictorShoup**,** "Twin Diffie-Hellman problem and applications https://eprint.iacr.org/2008/067

[11] M. Bellare, D. Pointcheval and R. Rogaway, "Advances in cryptology", EUROCRYPT 2000, LNCS – 1807 (2000) 139-155

[12] JM Bholi, "A framework for robust group key agreement", International conference on computational science and applications ICCSA-2006, 355-364, Glasgow, UK, May 2006.

[13] K.H. Huang, Y.F. Chung, H.H. Lee, F. Lai and T.S. Chen, "A Conference Key Agreement Protocol with Fault-tolerant Capability", Computer standards and interfaces, Vol 31, No.2, Jan 2009.

[14] D. Mahto, Dilip Kumar Yadav, Enhancing security of one-time password using Elliptic Curve Cryptography with finger-print biometricieeexplore.ieee.org/document/7100545 /

[15] Miyaji , Nakabayashi and Takano "Elliptic curves with low embedding degree", Journal of Cryptology, 2006, Volume 19, Number 4, Pages 553-562.

[16] Washington, Lawrence C., "Elliptic Curves: Number theory and cryptography", Chapman and Hall, Boca Raton, FL, 2nd. Ed., 2008.

[17] Arron Blumenfeld, "Discrete logarithms on Elliptic curves", 2011