International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 18 (2017) pp. 7105-7114


# One-Time Password Communication Security Improvement using Elliptic Curve Cryptography with Iris Biometric

**Dindayal Mahto [#1], Dilip Kumar Yadav [#2]**

[#] *Department of Computer Applications, National Institute of Technology Jamshedpur, Jamshedpur-831014, India.*

[1]*Orcid ID: 0000-0001-5599-4928*

**Abstract**

Nowadays, all e-commerce systems getting most of the bill amounts through ATM or debit card, credit card or online account transfer. In order to transfer bill amount from customer's account to seller's account, a One-Time Password (OTP) is needed which is valid for only one transaction, is generated by OTP Transaction Server of the Bank to authenticate their clients and to counter network eavesdropping / replay attacks. However, if the OTP itself gets attacked then there might be a chance of attacking to the current transaction and bank account of the client. In this paper, a model is proposed for improving the security of OTPs using ECC with iris biometric for e-commerce transactions. This model offers an improvement of security of OTP with shorter key length than the Rivest-Shamir-Adleman (RSA) algorithm and also avoids remembering the private keys, since the private keys are generated dynamically as and when required.

**Keywords:** One-Time Password (OTP), Elliptic Curve Cryptography (ECC), Biometrics, Iris, RSA

## INTRODUCTION

In an e-commerce transaction, an OTP is communicated between OTP transaction server and client to authenticate client and to avoid eavesdropping / replay attacks. In an e-commerce environment, privacy of an OTP message must be maintained. If the OTP gets attacked then there might be a chance of attacking the current transaction as well as bank account of the client. Therefore, this paper proposes a model for improving the security of OTPs using ECC with iris biometric for e-commerce transactions. The private and public keys of ECC are generated with the help of user's iris biometric features. ECC being an asymmetric cryptography has a limitation of managing the private keys. A private key of the client must be kept secret and not told to or shared with other. Due to rapid breakthrough in cryptanalysis, there are demands of large cryptographic keys. Large cryptography keys lead to memory or total recall problems. If such keys are stored somewhere then also there may be a chance of vulnerability of keys to steal. In order to overcome the above difficulties of managing keys, this paper proposes a model to generate the keys using iris biometric features. These keys are generated dynamically as and when a client needs. Finally the generated cryptographic keys are used to implement ECC for OTP security.

This paper is organized as follows. In section-2, related works and literature reviews are described. In section-3, OTP is described. In section-4, ECC is described. In section-5, iris biometric is described. In section-6, the proposed model is explained. In section-7, a case study based on the proposed model is explained. In section-8, security analysis of the proposed model is mentioned, and conclusion is stated in section-9.

## RELATED WORKS AND LITERATURE REVIEWS

In literature, many researchers have illustrated the implementation of cryptographic models using biometric keys. These keys are generated from biometric traits. A brief review of few selected papers is presented here. Hao et al. [1] have illustrated the implementation of 128-bit AES cryptography model using iris based biometric cryptographic keys, which generates genuine iris codes first, and then a re-generate-able binary digits known as biometric key gets created of up to 140 bits. Janbandhu et al. [2] suggested a technique to generate private key for RSA based digital signature model using a 512 byte iris template, which generates a larger number, based on iris template till the number becomes eligible for co-prime with Euler Totient Function. Once the number gets generated, then the number becomes private key for the client. Yao-Jen et al. [3] proposes face based cryptographic-key generation. The main problem with face biometric is that after certain years shape and size of face changes, and then False Rejection Rate increases. Monrose et al. [4] proposed a voice-based cryptographic key generation. Some of the other suggested approaches related to the crypto-biometrics are given in [5, 6, 7, 8, 9, 10, 28].

## ONE-TIME PASSWORD (OTP)

An OTP is a password valid for only one transaction, is generated by OTP Transaction Server in the response of transferring fund from user's bank account to recipient's account. It is the mechanism to authenticate the legitimate client and to counter eavesdropping/replay attacks occur during fund transfer between two parties in a network [11]. However, an OTP itself needs its security during transmission in Client/Server architecture.

## ELLIPTIC CURVE CRYPTOGRAPHY (ECC)

ECC was proposed by two independent authors (Neil Koblitz [12] and Victor S. Miller [13]) in late 1985. ECC algorithms are public-key algorithms that provide the same features as RSA algorithms. However, their security is based on the hardness of the elliptic curve discrete logarithm problem (ECDLP). Currently the best algorithms known, Pohlig-Hellman algorithm and Pollard's rho algorithm, to solve the ECDLP, have fully exponential running time of $O(\sqrt{p})$, where p is the largest prime, in contrast to the sub-exponential-time algorithms known for the integer factorization problem of RSA. This means that a desired security level can be achieved with significantly smaller keys in elliptic curve systems than is possible with their RSA counterparts [29]. The security level of ECC-160 and ECC-224 [14] are equivalent to the security level of of RSA-1024 and RSA-2048 respectively is shown in the Table 1 and in the Fig. 1.

**Table 1:** RSA and ECC - Cryptography key length (in bits) Public Key Size [14]

| Security Bits level | RSA | ECC |
|---|---|---|
| 80 | 1024 | 160 |
| 112 | 2048 | 224 |
| 128 | 3072 | 256 |
| 192 | 7680 | 384 |
| 256 | 15360 | 512 |

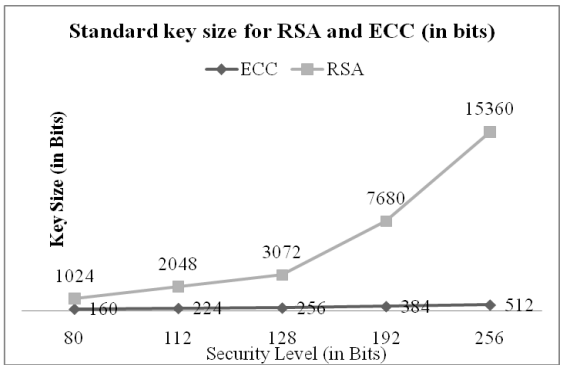


**Figure 1:** Comparable security bit level for cryptography key length

## IRIS BIOMETRIC

An iris of a human eye is a circular portion between pupil (the darkest portion of the eye) and sclera (mostly white portion of the eye) as shown in Fig. 2 [15].

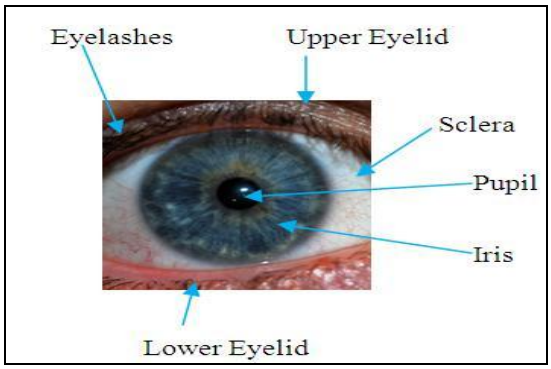


**Figure 2:** Iris with other parts of an eye

Iris is gaining a lot of attention nowadays due to its distinctiveness, large amount and non-counterfeiting [1] texture pattern [16] such as coronas, freckles, furrows, stripes, crypts and other minute characteristics. Iris compared to other biometrics traits provides highly reliable and accurate user identification method [22]. The pioneering concept of identifying human-being based on unique features of iris and pupil was first proposed by Flom and Safir [23]. Although the father of full-fledge practical iris recognition system is considered to Daugman [24], [16]. Daugman proposed a method for rapid visual recognition of personal identity that was described based on the failure of a statistical test of independence. Boles et al. [26] extracted unique features from the grey-level profiles of the iris and later same were represented using wavelet transform (WT) zero crossing and then used few selected intermediate resolution levels for matching. Gupta at al. [25] proposed iris recognition using corner detection of both irises. The paper proposes to generate user's cryptographic key from user's iris biometric feature.

This paper uses an iris recognition algorithm which consists of four major steps which are: (i) iris localization from the iris image database of like Institute of Automation, Chinese Academy of Sciences(CASIA), UBIris, etc. (ii) iris normalization, (iii) iris feature extraction and (iv) iris matching.

Flow for generating iris-code is given in the Fig. 3.

Detailed for generation of iris-code is mentioned below:

First of all localization of inner pupil boundary is performed using Circular Hough Transformation (CHT). In case of occlusions and images mixed-up by artifacts such as shadows and noise, CHT gives better performance. The outer iris circle is detected by circular summation of intensity approach from the determined pupil center and radius. The localized iris image is transformed from cartesian co-ordinate to polar co-

ordinate system to handle different size, variation in illumination and pupil dilation. The normalized region of interest is convolved with 1-D Log-Gabor filters. The intermediate data from 1-D Log-Gabor filters is retrieved and quantized to encode the unique pattern of the iris into iris-code [1], [17], [18], [19], [21].

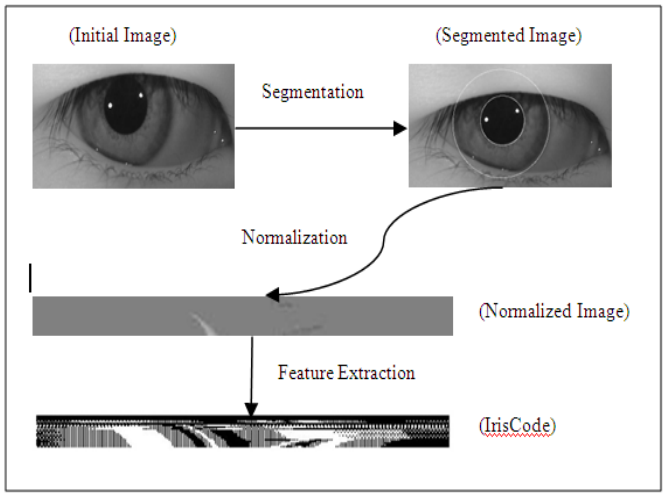


**Figure 3:** Iris-Code generation

## PROPOSED MODEL

The Fig. 4 shows the proposed model. This model uses irises of bank clients for generating their cryptographic keys, and then the keys are used in ECC to provide data communication security while sending the OTP from OTP Transaction Server to client. At the client-end, client decrypts and gets the plain-OTP that is used for input screen on the secured website of the bank. If the entered OTP is valid with respect to current transaction, then transaction gets successfully executed, otherwise transaction gets canceled.

**Steps of the proposed methodology :**

Step I. OTP Transaction Server (OTS) generates plain-OTP.

Step II. ECC Encryption Module receives plain-OTP and generates cipher-OTP with the help of client's public key.

Step III. Cipher-OTP gets forwarded over communication channel to the client's mobile.

Step IV. At Client-Side, Client mobile gets and forwards the cipher-OTP to ECC Decryption Module.

Step V. The ECC Decryption Module decrypts cipher-OTP with the help of client's private key to retrieve plain-OTP.

Step VI. Client enters the recently retrieved plain-OTP in the OTP input screen on the secured website of the bank.

Step VII. If the entered plain-OTP matches with original-OTP for the transaction, then transaction gets successfully executed otherwise, transaction is canceled.

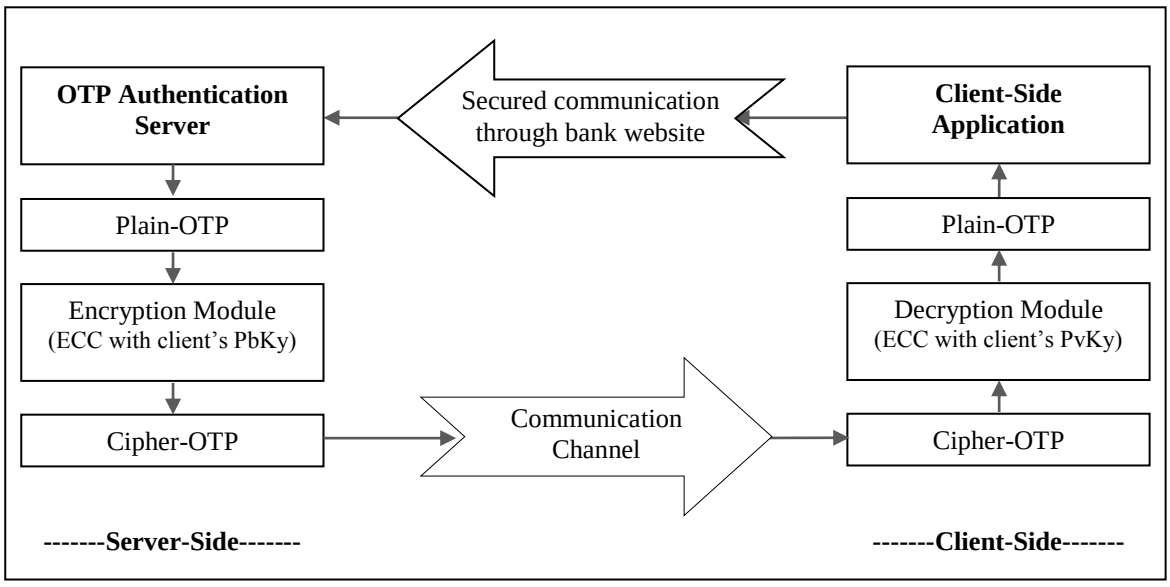


**Figure 4:** Proposed Models

**Method for generating public key and private key :**

Cryptographic keys of client get generated with the help of hash value of iris-code of client. The generated hash value is randomized, which is considered as private key for the client named as Alice. The private key for Alice is $d_A$. In order to generate the Public key for Alice, following steps are performed:

Step I. Both Alice and OTS select a big prime number 'p' and the ECC parameters 'a' and 'b' such that

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

Where, $4a^3 + 27b^2 \neq 0$

Step II. Base point: G(x, y) gets selected from the elliptic curve.

Step III. Calculate client's public key:

$$P_A = d_A * G(x, y)$$

Step IV. Calculate server's public key:

$$P_B = d_B * G(x, y)$$

Step V. Generating secret key by client and server: $s_K = d_A * P_B = d_B * P_A$

**OTP Message Encryption :**

OTS generates plain-OTP as msg to be encoded as points Pmsg (x, y) as shown in the Fig. 5. These points are encrypted as a cipher-OTP and later same are decrypted.

Steps for encryption are given below:

Step I. ECC Encryption Module generates

Pmsg = (x, y) from msg.

Step II. This Module selects a global variable: h, which gets initialized with 1% of secret-key. The secret-key gets generated during key exchange step.

Step III. Calculate, x=msg*h+i; takes the value of i from 1 to h-1 and keeps on trying to get an integral value of y. Thus, msg is generated as the form of encoded point(x,y) is shown in the Fig. 5.

Step IV. The cipher-OTP is a collection of two points: Cmsg = ((k * G), (Pmsg + k * PA)), where k is randomly selected value by OTS.

Step V. ECC Encryption Module forwards this cipher-OTP to Alice as shown in the Fig. 6.

**OTP Message Decryption :**

Steps for decrypting cipher-OTP

Step I. Alice gets Cmsg = ((k * G), (Pmsg + k * $P_A$))

Step II. Alice multiplies the its private key with point1 of cipher OTP and then subtract the resultant point from point2 of cipher OTP:

$$= ((Pmsg + k * P_A) - (d_A * k * G))$$
$$= ((Pmsg + k *( d_A * G)) - (d_A * (k * G)))$$
$$= Pmsg$$

Step III. The decoding of msg = floor((Pmsg(x)-1)/h)

Step IV. Finally the decrypted-OTP is msg.

**CASE STUDY**

This study proposes a data communication security model for OTP using ECC and keys of ECC are generated with the help of iris biometric.

**Elliptic Curve Diffie-Hellman [20] Algorithm for key key exchange :**

Here, global parameters of ECC are:

Prime number p=8191, a=10, b=17, G=(9, 3510), h=1% of secret key (ie.$s_K(x)$), for encoding and decoding of OTP in elliptic curve. Based on global parameters, the elliptic curve equation becomes:

$$y^2 \bmod 8191 = (x^3 + 10\,x + 17) \bmod 8191 \quad (2)$$

Steps for key exchange:

Step I. Private key of Alice (i.e. Client) is generated based on randomization of iris code of his right eye iris with random value: $d_A$=4680

Step II. Public key of Alice is:

$$P_A(x, y) = d_A * G(x, y)$$
$$= 4680 * (9, 3510)$$
$$= (6454, 7641)$$

Step III. Private key of OTS (i.e. OTP Transaction Server) is based on random value: $d_B$= 4818

Step IV. Public key of OTS is:

$$P_B(x, y) = d_B * G(x, y)$$
$$= 4818 * (9, 3510)$$
$$= (4329, 5845)$$

Step V. Calculation of secret-key by Alice is:

$$s_k(x, y) = d_A * P_B$$

$$= 4680 * (4329, 5845)$$

$$= (820, 7879)$$

Step VI. Calculation of secret-key by OTS is:

$$s_k(x, y) = d_B * P_A$$

$$= 4818 * (6454, 7641)$$

$$= (820, 7879)$$

In this way, both parties get same secret key i.e. $s_k(x, y) = (820, 7879)$. The variable h gets rounded value of 1% of $s_k(x) = 8$.

**Encryption of plain OTP message by OTS (sender) :**

*Steps for encryption*

Step I. OTS generates plain OTP message as: '32145688'

Step II. Encoding: OTS encodes the plain OTP into encoded OTP points in the elliptic curve as shown in Table 2 and in the Fig. 5.

Step III. Encryption: OTS encrypts the encoded OTP points into cipher OTP points as shown in Table 3 and in the Fig. 6 and send the same to Alice.

Here the OTP is generated by OTP Transaction Server and same is passed to do encryption using elliptic curve cryptography, which uses public key of sender generated with the help of iris biometric features of the sender.

**Decryption of cipher OTP points by Alice (receiver) Steps for decryption of cipher-OTP:**

Step I. Decryption: Alice decrypts cipher OTP points into encoded OTP points as shown as in Table 2 and in the Fig. 5.

Step II. Decoding: Alice decodes the encoded points into plain OTP message.

Step III. Alice gets plain OTP message as: 32145688.

Step IV. Alice enters the plain OTP message into the input screen for OTP on the secured website of the bank.

Step V. If entered OTP matches with original OTP for the transaction, then transaction get successfully executed, otherwise transaction gets canceled.

**Table 2:** Encoded OTP points in the elliptic curve

| $P_{msg}(X)$ | $P_{msg}(Y)$ |
|---|---|
| 27 | 2979 |
| 17 | 3687 |
| 9 | 3510 |
| 33 | 2201 |
| 45 | 2819 |
| 50 | 165 |
| 65 | 458 |
| 65 | 458 |

**Table 3** Cipher OTP points in the elliptic curve

| $C_{msg}(X)$ | $C_{msg}(Y)$ |
|---|---|
| 8120 | 3840 |
| 2979 | 3342 |
| 1408 | 4575 |
| 7343 | 4128 |
| 4696 | 4548 |
| 3372 | 3807 |
| 6320 | 4084 |
| 6320 | 4084 |

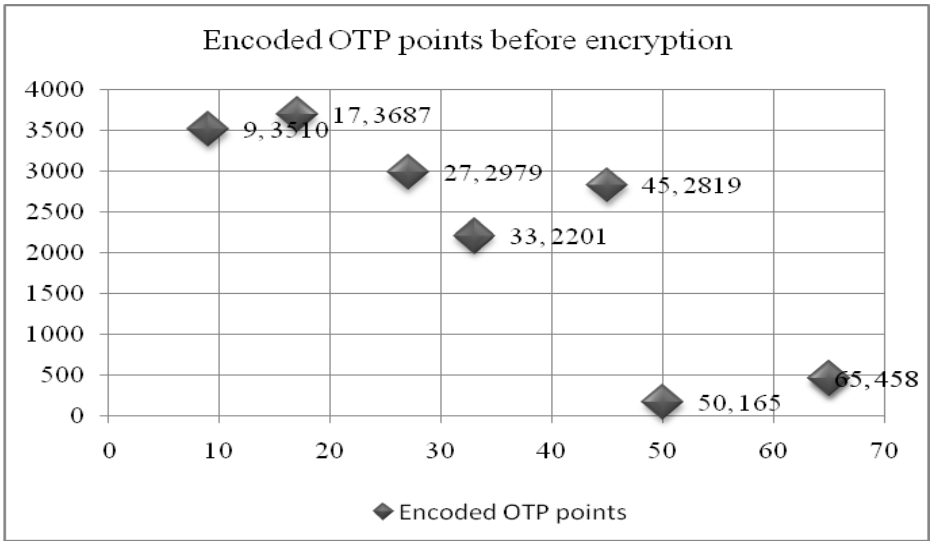


**Figure 5.** Encoded OTP points in the elliptic curve

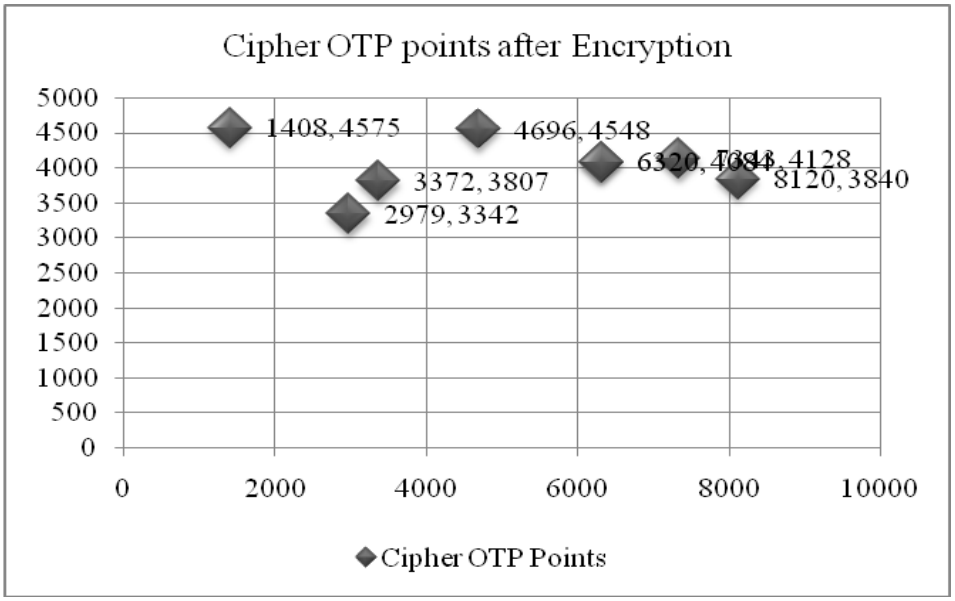


**Figure 6.** Cipher OTP points in the elliptic curve

**Table 4** Points Encoding and Decoding Time

(in seconds)

| Security Bit Level | Encoding | Decoding |
|---|---|---|
| 80 | 0.0049 | 0.003 |
| 112 | 0.1418 | 0.0017 |
| 128 | 0.4269 | 0.0018 |
| 144 | 0.1888 | 0.0017 |

**Table 5** Encryption Time (in seconds)

| Security Bit Level | ECC (Biometric) | ECC (Plain) | RSA |
|---|---|---|---|
| 80 | 2.1685 | 2.8004 | 0.136601 |
| 112 | 9.9855 | 12.921 | 0.163538 |
| 128 | 15.0882 | 13.33 | 0.167184 |
| 144 | 20.2308 | 22.2057 | 0.138512 |

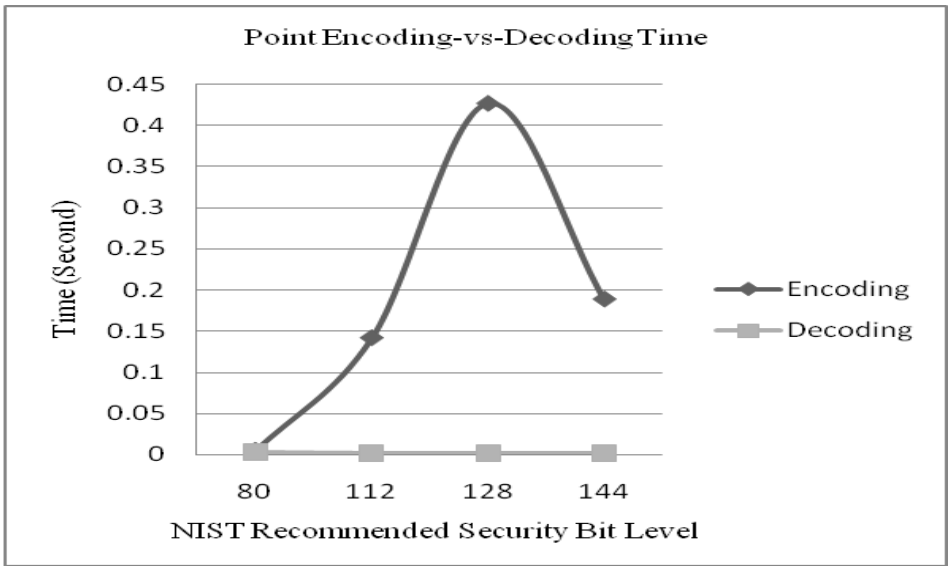


**Figure 7.** Point encoding and decoding time

## SECURITY ANALYSIS OF THE PROPOSED MODEL

This paper implements RSA, ECC with random private keys, and ECC with iris biometric based private keys, using MATLAB R2008a on Intel Pentium dual-core processor (1.60 GHz, 533 MHz, 1 MB L2 cache) with 2GB DDR2 RAM. The OTP message is encoded in the elliptic curve as x and y coordinates. The encoded points are encrypted in elliptic curve. The encrypted points become cipher-OTP. At recipient-end, he needs to decrypt cipher-OTP first then needs to decode the points to recover plain-OTP message. The OTP message encoding time is higher than OTP message decoding as shown in the Table 4 and in Fig.7. The efficiency of ECC

over RSA is shown in Tables 5, 6, 7 and in Figs. 8, 9, 10. It is found that RSA is very efficient in encryption and slow in decryption while ECC is slow in encryption and very efficient in decryption. Overall ECC is more efficient than RSA as shown in the Table 7 and Fig. 10.

The Tables 5-7 and Fig. 8-10 show the comparison of security strength of RSA, ECC and ECC with iris biometric. It is found that when smaller length of key for RSA is used, then RSA is more efficient, but when large key length for RSA is used, then RSA becomes inferior than ECC and ECC with iris biometric.

**Table 6** Decryption Time (in seconds)

| Security Bit Level | ECC (Biometric) | ECC (Plain) | RSA |
|---|---|---|---|
| 80 | 5.91 | 2.9918 | 5.537156 |
| 112 | 6.93 | 3.3787 | 20.410795 |
| 128 | 7.3584 | 3.5209 | 46.478193 |
| 144 | 8.4785 | 4.1697 | 77.764168 |

**Table 7** Total Time (in seconds)

| Security Bit Level | ECC (Biometric) | ECC (Plain) | RSA |
|---|---|---|---|
| 80 | 8.08 | 5.79 | 5.67 |
| 112 | 16.92 | 16.30 | 20.57 |
| 128 | 22.45 | 16.85 | 46.65 |
| 144 | 28.71 | 26.38 | 77.90 |

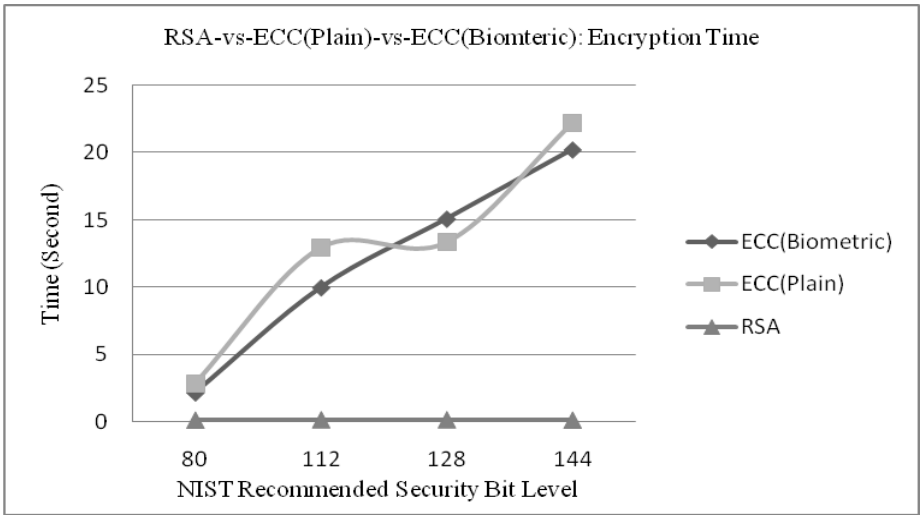


**Figure 8.** RSA-vs-ECC(Plain)-vs-ECC(Biometric): Encryption Time

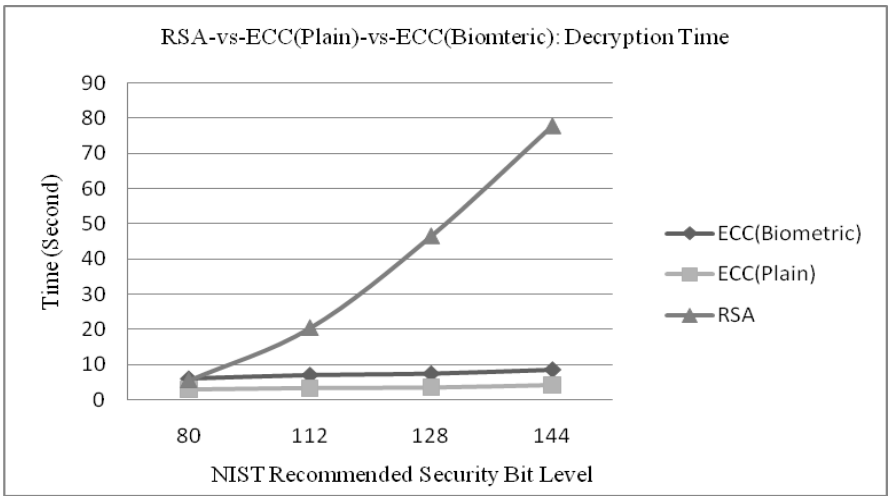


**Figure 9.** RSA-vs-ECC(Plain)-vs-ECC(Biometric): Decryption Time

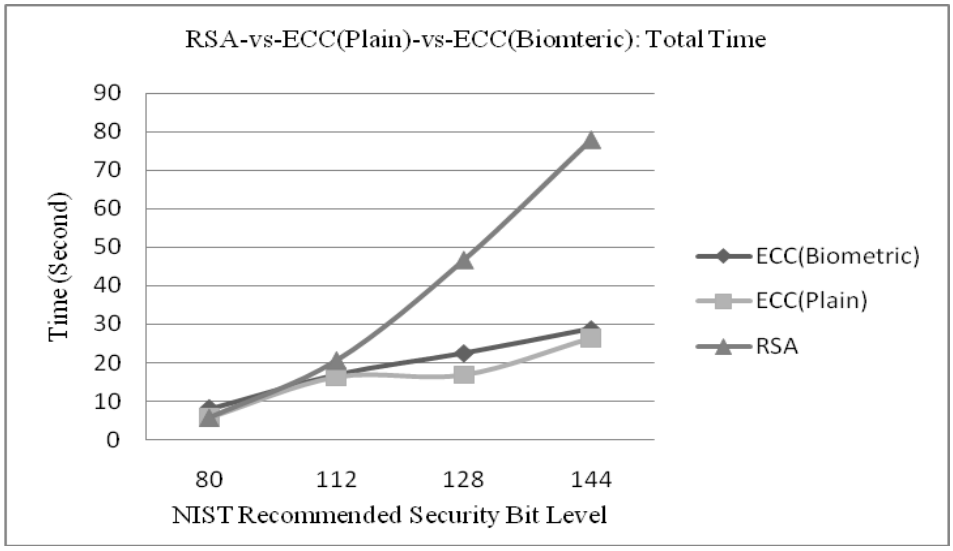


**Figure 10.** RSA-vs-ECC(Plain)-vs-ECC(Biometric): Total Time

## CONCLUSION

This paper proposes a model for security improvement of OTP using ECC with iris biometric. ECC offers better security with lesser key length. Iris biometric offers highly reliable and accurate user authentication method due to its distinctiveness, large amount and non-counterfeiting texture pattern. Nowadays all e-commerce firms do monetary transaction with the help of OTPs. OTP message communication is not secure and completely dependent on the SMS provider's security mechanisms. The proposed model mitigates the demerits of the present OTP message communication for e-commerce transactions.

## ACKNOWLWDGEMENT

Authors are very thankful for the comments and suggestions provided by reviewers and editors.

## REFERENCES

[1] F. Hao, R. Anderson, J. Daugman, Combining crypto with biometrics effectively, IEEE Transactions on Computers 55 (9) (2006) 1081-1088.

doi:10.1109/TC.2006.138.

[2] P. K. Janbandhu, M. Y. Siyal, Novel biometric digital signatures for internet- based applications, Information Management & Computer Security 9 (5) (2001) 205-212.

[3] Y.-J. Chang, W. Zhang, T. Chen, Biometrics-based cryptographic key generation, in: Multimedia and Expo, 2004. ICME '04. 2004 IEEE International Conference on, Vol. 3, 2004, pp. 2203-2206 Vol.3. doi:10.1109/ICME.2004.1394707.

[4] F. Monrose, M. K. Reiter, Q. Li, S. Wetzel, Cryptographic key generation from voice, in: Proc. of the 2001 IEEE Symposium on Security and Privacy, SP '01, IEEE Computer Society, Washington, DC, USA, 2001, pp. 202-.

[5] Y. Dodis, L. Reyzin, A. Smith, Fuzzy extractors: How to generate strong keys from biometrics and other noisy data, in: C. Cachin, J. Camenisch (Eds.), Advances in Cryptology - EUROCRYPT 2004, Vol. 3027 of Lecture Notes in Computer Science, Springer Berlin Heidelberg, 2004, pp. 523- 540. doi:10.1007/978-3-540-24676-3_31.

[6] L. Zhang, Z. Sun, T. Tan, S. Hu, Robust biometric key extraction based on iris cryptosystem, in: M. Tistarelli, M. Nixon (Eds.), Advances in Biometrics, Vol. 5558 of Lecture Notes in Computer Science, Springer Berlin Heidelberg, 2009, pp. 1060- 1069. doi:10.1007/978-3-642-01793-3_107.

[7] D. Mahto, D. K. Yadav, Enhancing security of one-time password using elliptic curve cryptography with biometrics for e- commerce applications, in: Computer, Communication, Control and Information Technology (C3IT),2015 Third International Conference on, IEEE, 2015, pp. 1-6.

[8] D. Mahto, D. K. Yadav, Network security using ECC with Biometric, in: K. Singh, A. K. Awasthi (Eds.), QSHINE, Vol. 115 of LNICS-SITE, Springer Berlin Heidelberg, 2013, pp. 842-853. doi:10.1007/978-3-642- 37949-9_73.

[9] D. Mahto, D. Yadav, Enhancing security of one-time password using elliptic curve cryptography with finger-print biometric, in: Computing for Sustainable Global Development (INDIACom), 2015 2nd International Conference on, 2015, pp. 1737- 1742.

[10] D. Mahto, D. K. Yadav, Proc. of 3rd Intl. Conf. on Advanced Computing, Networking and Informatics: ICACNI 2015, Vol. 2, Springer India, New Delhi, 2016, Ch. Security Improvement of One-Time Password Using Crypto-Biometric Model, pp. 347-353. doi:10.1007/978-81-322-2529-4_36.

[11] N. Haller, The s/key one-time password system, Network Working Group.

[12] N. Koblitz, Elliptic curve cryptosystems, Mathematics of Computation 48 (177) (1987) 203-209.

[13] V. S. Miller, Use of elliptic curves in cryptography, in: H. Williams (Ed.), Advances in Cryptology CRYPTO 85 Proc., Vol. 218 of Lecture Notes in Computer Science, Springer Berlin Heidelberg, 1986, pp. 417-426. doi:10.1007/3-540-39799- X_31.

[14] E. Barker, W. Barker, W. Burr, W. Polk, M. Smid, Recommendation for key management part 1: General (revision 3), NIST Special Publication 800-57 (2012) 1- 147.

[15] S. Jogi, B. Sharma, Methodology of iris image analysis for clinical diagnosis, in: Medical Imaging, m-Health and Emerging Communication Systems (MedCom), 2014 International Conference on, 2014, pp. 235- 240. doi:10.1109/MedCom.2014.7006010.

[16] J. Daugman, New methods in iris recognition, Systems, Man, and Cyber- netics, Part B: Cybernetics, IEEE Transactions on 37 (5) (2007) 1167-1175.

doi:10.1109/TSMCB.2007.903540.

[17] K. Hollingsworth, K. Bowyer, P. Flynn, The best bits in an iris code, Pattern Analysis and Machine Intelligence, IEEE Transactions on 31 (6) (2009) 964-973. doi:10.1109/TPAMI.2008.185.

[18] S. Bakshi, H. Mehrotra, B. Majhi, Real-time iris segmentation based on image morphology, in: Proc. of the 2011 International Conference on Communication, Computing & Security, ACM, 2011, pp. 335-338.

[19] S. P. Jogi, B. B. Sharma, Methodology of iris image analysis for clinical diagnosis, in: Medical Imaging, m-Health and Emerging Communication Systems (MedCom), 2014 International Conference on, IEEE, 2014, pp. 235-240.

[20] W. Diffie, M. Hellman, New directions in cryptography, Information Theory, IEEE Transactions on 22 (6) (1976) pp. 644-654.

doi:10.1109/TIT.1976.1055638.

[21] Masek, Libor. Recognition of human iris patterns for biometric identification. The University of Western Australia 2 (2003).

[22] J. Daugman, C. Downing, Epigenetic randomness, complexity and singularity of human iris patterns, Proceedings of the Royal Society of London B: Biological Sciences 268 (1477) (2001) pp. 1737-1740.

[23] L. Flom and A. Safir, Iris Recognition System, U.S. Patent No. 4641349(1987)

[24] J. Daugman, High confidence visual recognition of persons by a test of statistical independence, IEEE Trans. Pattern Anal. Machine Intell. 15, pp. 1148–1161, 1993.

[25] P. Gupta, H. Mehrotra, A. Rattani, A. Chatterjee and A.K. Kaushik. Iris recognition using corner detection. Proceedings of the 23rd International Biometric Conference, Montreal, Canada, July 16-21,2006, 1-5.

[26] W.W. Boles, B. Boashah, A Human Identification Technique Using Images of the Iris and Wavelet Transform. IEEE Transaction on Signal Processing Vol. 46 (1998) 1185-1188

[27] D. Hankerson D, A.J. Menezes, S. Vanstone, Guide to elliptic curve cryptography. Springer Science & Business Media; 2006 Jun 1.

[28] D. Mahto, and D. K. Yadav, "Secure Online Medical Consultations Using Elliptic Curve Cryptography with Iris Biometric", International Journal of Control Theory and Applications, Vol. 10(13), pp. 169- 179, 2017

[29] D. Mahto, D. A. Khan, and D. K. Yadav. "Security Analysis of Elliptic Curve Cryptography and RSA." In Proceedings of the World Congress on Engineering, vol. 1. pp. 419- 422, London, U.K., June 29 - July 1, 2016.