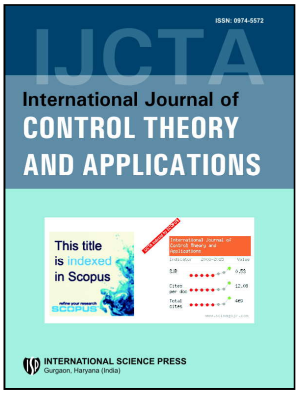

International Journal of Control Theory and Applications

ISSN : 0974-5572

© International Science Press

Volume 10 • Number 13 • 2017

Secure Online Medical Consultations Using Elliptic Curve Cryptography with Iris Biometric

Dindayal Mahto[*1] and Dilip Kumar Yadav[*2]

[#1,2] Department of Computer Applications National Institute of Technology Jamshedpur, Jamshedpur-831014, India, Emails: dindayal.mahto@gmail.com, dkyadav.ca@nitjsr.ac.in

Abstract: Information and communication technology (ICT) is a boon for exchanging messages instantly between two or more persons/systems. Taking the benefits of ICT, a patient may distantly get regular online medical consultations with his/her remote doctor. The backbone of ICT is the Internet, which is open-standard architecture. Due to openness of the architecture, there are many security vulnerabilities to online medical consultation systems. In order, to provide secure consultation between patient and doctor and, to maintain the privacy of patient information, this paper proposes a secure online medical consultations scheme using RSA and Elliptic Curve Cryptography (ECC) with iris biometric. We compare the efficiency of RSA and ECC with iris biometric. With growing key sizes, ECC is more efficient than RSA. The simulation results demonstrate that the proposed model offers high level of and robust security.

Keyword: Elliptic Curve Cryptography, Iris Biometric, Asymmetric-key Cryptography, Patient, Doctor

1. INTRODUCTION

The privacy of patient's online medical consultations information must be maintained. In order to maintain privacy of online consultations information, this paper uses ECC with iris biometric. Private keys of the patient and doctor must be confidential, non-sharable, and safe. Due to rapid breakthrough in cryptanalysis based on cryptographic keys, there is a demand of bigger cryptographic key bit length than existing ones. However bigger key length has many problems like difficulty to recall, feed into the system, and store in the system. If keys are stored somewhere, then keys may be stolen. In order to overcome the above difficulties of keys, this paper proposes a model to generate cryptographic keys using iris biometric features. These keys are generated dynamically as and when patient and doctor need. Finally the generated cryptographic keys are used to implement ECC for online medical consultations security.

This paper is organized as follows. Section-II describes the related works and literature reviews. Section-III describes ECC. Section-IV describes iris biometric. Section-V explains the proposed model. Section-VI explains a case study based on the proposed model. Section-VII describes security analysis of the proposed model and Section-VIII describes conclusion.

2. RELATED WORKS AND LITERATURE SURVEY

Online consultations between specialists and referring doctors develop novel ideas which can be applied to patient in timely and hassle free manner for providing best treatment to the patient [10]. Communication can be considered as the main ingredient in medical care [18]. In the literature, many researchers have illustrated the implementation of cryptographic models using biometric based keys. These keys are generated from biometric traits. A brief review of few selected papers is as follows: Hao et al. [7] have illustrated the implementation 128-bit AES cryptography model using iris based biometric cryptographic keys, which generates genuine iriscodes first, and then a re-generate-able binary digits known as biometric key gets created of up to 140 bits. Yao-Jen et al. [2] 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. [17] proposes voice-based cryptographic key generation, there is a risk of recording the voice-based password and later imposter can use it. Some of the other suggested approaches related to the crypto-biometrics are given in [6, 12-15, 19].

3. ELLIPTIC CURVE CRYPTOGRAPHY (ECC)

ECC is asymmetric-key cryptography scheme [5], proposed by two authors independently (Neil Koblitz [11] and Victor S. Miller [16]) in late 1985. In ECC, first of all, each character of the message must be converted into the form of a point(x, y). In this way, as many points are generated as the length of the message. These converted points are encrypted and decrypted by ECC algorithm. It is considered to be a competitor of RSA algorithm. The security of the RSA cryptosystem is based on the Integer Factorization Problem (IFP) and the security of ECC is based on the elliptic curve discrete logarithm problem (ECDLP). The main attraction of ECC over RSA is that the best known algorithm for solving the ECDLP takes full exponential time while to solve IFP of RSA takes sub-exponential time. Due to ECC's complex numerical calculation, it provides better security per bit with smaller key length than RSA. This means that significantly smaller parameters can be used in ECC than RSA, with equivalent levels of security. For example to achieve 112 bits of security level, RSA algorithm needs key size of 2048 bits, while ECC needs key size of 224-255 bits. The security level of ECC-160 and ECC-224 [1] are equivalent to the security level 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)

Security Bit Level	*RSA*	*ECC*
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	512

4. IRIS BIOMETRIC

Iris of an eyeball is a colored circular boundary that appears in the outer part of the pupil. Due to its distinctiveness, large amount and non-counterfeiting [7] texture pattern [3], iris compared to other biometrics traits provides highly reliable and accurate user identification method [4]. Iriscode is generated after finding the surrounded boundary between the iris and pupil portions and outer boundary between the iris and sclera portions of the eyeball's image. Here iris is localized as done by [7-9] and then the localized feature in turn generates the iriscode. The steps for generating iriscode are shown in the Fig. 2.

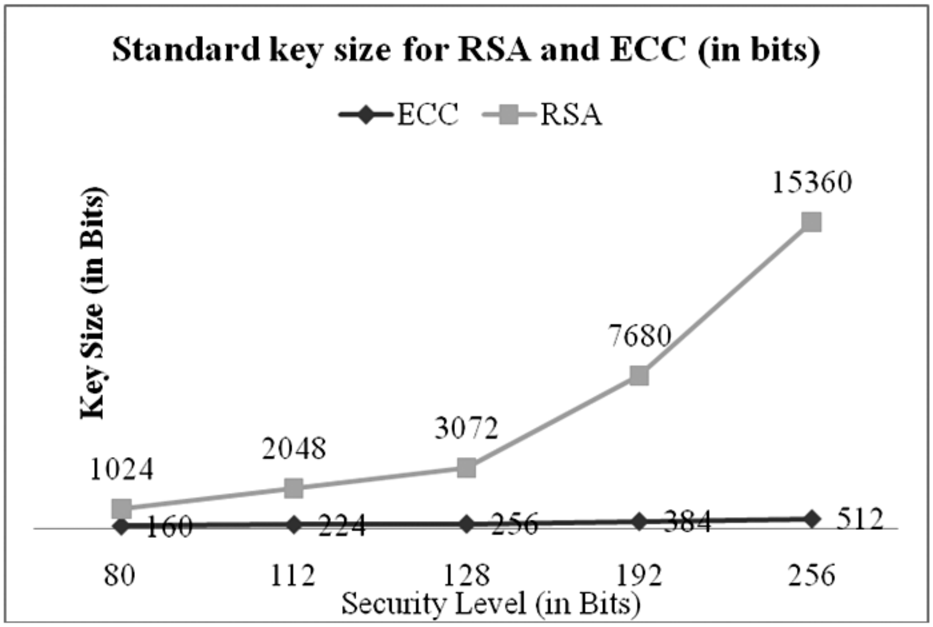

Figure 1: Comparable security bit level for cryptography key length

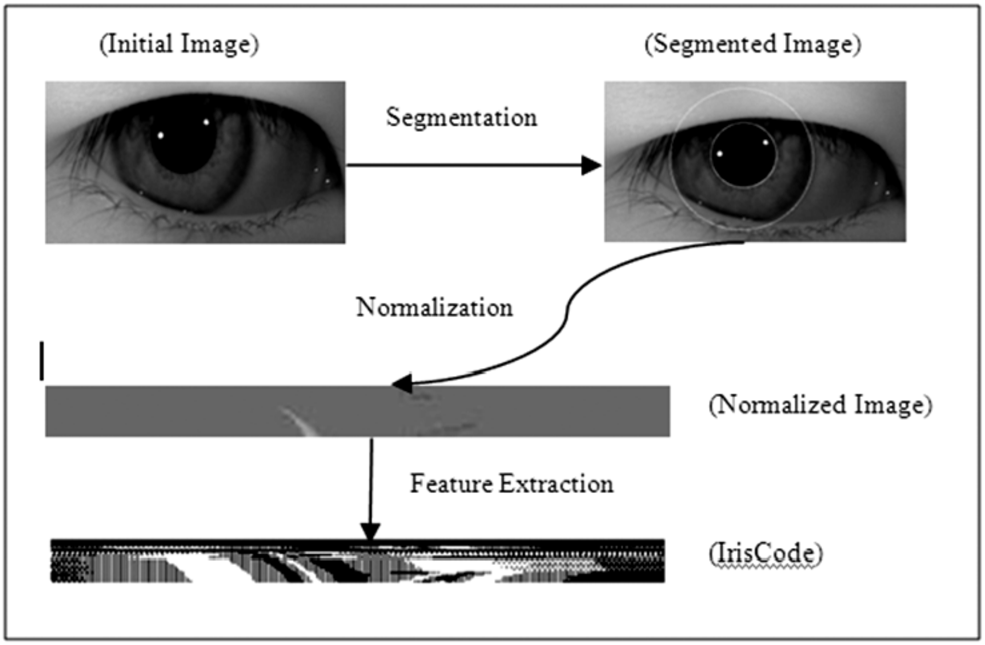

Figure 2: Step for generating iriscode

5. PROPOSED MODEL

The Fig. 3 shows the proposed model. This model uses iris traits of patient and doctor to generate their cryptographic keys, and then those keys are used in ECC to provide security of travelling message related to medical consultation between patient and doctor. Patient uses public key of doctor to generate cipher-message of his/her plain-query or plain-message and then generated cipher-message is sent to the doctor. When doctor decrypts and gets plain-message, and then he understands the problem of patient and write plain-prescription or plain-message. Plain-prescription gets encrypted using patient's public by doctor and then the generated

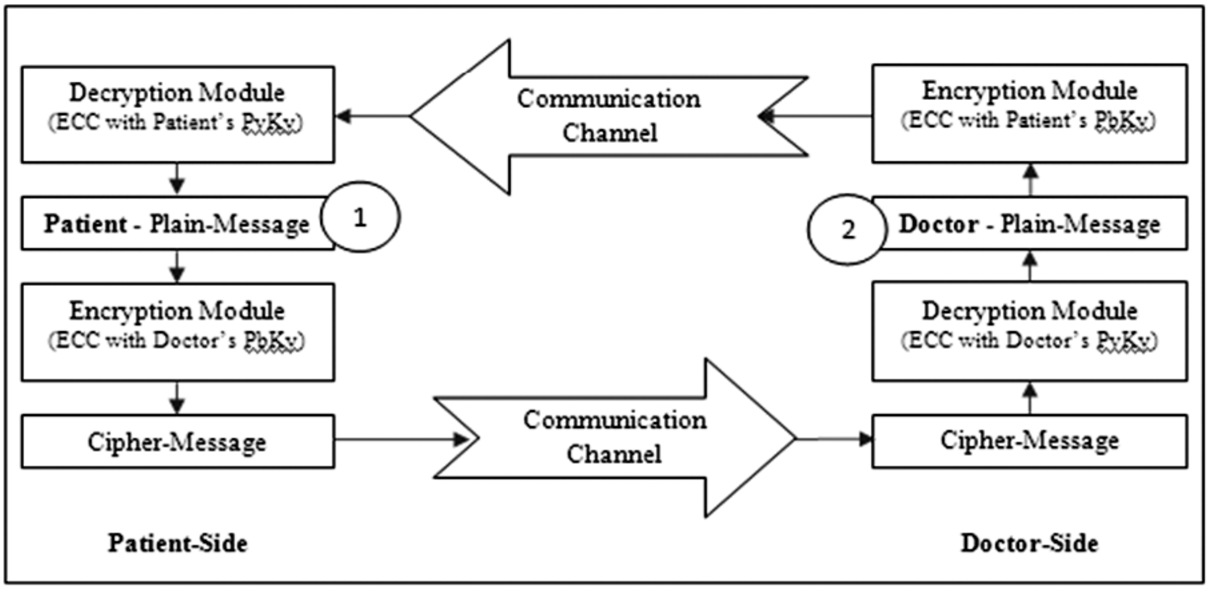

Figure 3: Proposed model for online medical consultation

cipher-prescription is sent to patient. In this way cycle is formed and they keep on sending their messages securely.

5.1. Steps of the proposed methodology

Step 1. Patient generates plain-message (query related to his/her ailment) to be asked from his/her doctor.

Step 2. ECC encryption module receives plain-message of the patient and generates cipher-message with the help of doctor's public key (Key exchange between patient and doctor is done prior to this step, the steps for key exchange is mentioned below in step. B).

Step 3. Cipher-message gets forwarded over communication channel to the doctor-end.

Step 4. At doctor-side, doctor's system gets and forwards the cipher-message to ECC decryption module system.

Step 5. The ECC decryption module generates plain-message with the help of doctor's private key (which is generated based on doctor's iriscode).

Step 6. Doctor enters the plain-message (prescription regarding to the query raised by patient) in the input screen of ECC encryption module system, which generates cipher-message using patient's public key and then forwards to patient.

Step 7. At patient-side, patient decrypts cipher message using his/her private key.

5.2. ECC Diffie-Hellman key exchange – for sharing secret key between doctor and patient

Cryptographic keys of patient and doctor get generated with the help of hash value of their iris codes. The generated hash value is randomized. Steps for generating private key, public key and shared secret key of users:

5.2.1. Global public elements

Step 1. Both doctor and patient select a big prime number 'p' and the ECC parameters 'a' and 'b' such that

$$y^2 \bmod p = (x^3 + ax + b) \bmod p; \tag{1}$$

where, $p>3$ and $4a^3+ 27b^2 \neq 0$.

Step 2. Base point: G(x, y) gets selected from the elliptic curve.

5.2.2. User Doctor key generation

Step 3. Private key of doctor: d_A = randomized hash value of doctor's iris codes.

Step 4. Public key of doctor: $P_A = d_A * G(x, y)$.

5.2.3. User Patient key generation

Step 5. Private key of patient: d_B = randomized hash value of patient's iris codes.

Step 6. Public key of patient: $P_B = d_B * G(x, y)$.

5.2.4. Calculation of secret key by User doctor

Step 7. Secret key of doctor: $S_K = d_A * P_{B.}$

5.2.5. Calculation of secret key by User patient

Step 8. Secret key of patient: $S_K = d_B * P_{A.}$

5.3. Message encryption

Sender (patient) generates plain-message as msg to be encoded as points Pmsg (x, y). These points are encrypted as a cipher-message and later same are decrypted. Steps for encryption are given below:

Step 1. Plain message (msg) gets coded as 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 (for decimal digits), 10, 11, . . . , 34, 35 (for upper case alphabets), 36, 37, …60, 61 (for lower case alphabets), 62, 63, 64 ……90, 91 (for special symbols).

Step 2. ECC Encryption module generates Pmsg = (x, y) from msg.

Step 3. This module selects a shared variable (shared between sender and receiver): h, which gets initialized with 1% of above generated secret key (S_K).

Step 4. 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 such that the value of x and y must satisfy the equation number 1. In this way, whole msg is converted into different points(x, y).

Step 5. The cipher-message is a collection of two points:

Cmsg = ((k * G), (Pmsg + k * P_A)), where k is randomly selected value by sender.

Step 6. ECC Encryption module forwards this cipher-message to recipient-end (doctor).

5.4. Message decryption

Receiver (doctor) gets cipher-message. He recovers plain-message from cipher-message using decryption module, which requires doctor's private key. Steps for decryption are given below:

Step 1. Doctor gets Cmsg = ((k * G), (Pmsg + k * P_A)

Step 2. Doctor multiplies the its private key with point1 of cipher message and then subtract the resultant point from point2 of cipher message:

$= ((P_{msg} + k * P_A) - (d_A * k * G))$

$= ((P_{msg} + k *(d_A * G)) - (d_A * (k * G)))$

$= P_{msg}$

Step 3. The decoding of msg=floor((P_{msg}(x)-1)/h). The msg gets rounded off through floor function.

Step 4. The decrypted-message is msg.

Step 5. The msg is decoded as decimal digits (from 0, 1, 2, 3, 4, 5, 6, 7, 8, 9), upper case alphabets (from 10, 11,. . . , 34, 35), lower case alphabets (from 36, 37, …60, 61), and special symbols (from 62, 63, 64 ……90, 91).

The same encryption and decryption processes have to be followed by doctor.

6. CASE STUDY

This case study proposes a secure online consultation between patient and doctor using ECC. Cryptographic keys of ECC are generated with help of iris biometric of sender and receiver.

6.1. Key generation and secret key exchange

Elliptic Curve Diffie-Hellman [6] Algorithm for key generation and key exchange are performed as follows:

6.1.1. Global public elements

Step 1. Let us consider global parameters of ECC as prime number p = 8191, a = 10, b = 17, G = (9, 3510) for encoding and decoding of message in elliptic curve.

Based on above parameters, the elliptic curve equation becomes:

$$y^2 \bmod 8191 = (x^3 + 10 * x + 17) \bmod 8191 \qquad (2)$$

where, p>3 and $4*10^3+ 27*17^2 \neq 0$.

6.1.2. User Doctor - key generation

Step 2. Private key of doctor is based on randomization of his iris code generated with help of right eye iris: $d_A = 4680$.

Step 3. Public key of doctor: $P_A = d_A * G (x, y) = 4680 * (9, 3510) = (6454, 7641)$.

6.1.3. User Patient - key generation

Step 4. Private key of patient is based on randomization of his iris code generated with help of right eye iris: $d_B = 4818$.

Step 5. Public key of patient is: $P_B(x, y) = d_B * G (x,y) = 4818 * (9, 3510) = (4329, 5845)$

6.1.4. Calculation of secret key by User doctor

Step 6. Secret key of doctor: $S_K = d_A * P_B = 4680*(4329, 5845) = (820, 7879)$.

6.1.5. Calculation of secret key by User patient

Step 7. Secret key of patient: $S_K = d_B * P_A = 4818*(6454, 7641) = (820, 7879)$.

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

6.2. Encryption of plain message by Patient Side Application (sender)

1. Patient Side Application generates plain message as: "Patient: Hello Sir, I am not feeling well, have headache and stomach pain, kindly suggest some medicines for me."
2. Encoding: Patient Side Application encodes the plain message into encoded message points in the elliptic curve as shown in the Fig. 4.
3. Encryption: Patient Side Application encrypts the encoded message points into cipher message points as shown in the Fig. 5 and send the same to Doctor.

6.3. Decryption of cipher message points by Doctor (receiver)

1. Decryption: Doctor Side Application decrypts cipher message points into encoded message points as shown as in the Fig. 4.
2. Decoding: Doctor Side Application decodes the encoded points into plain message.
3. Doctor gets plain message as: "Patient: Hello Sir, I am not feeling well, have headache and stomach pain, kindly suggest some medicines for me."
4. Doctor now can send message to the Patient. He has to follow same steps as followed by the Patient.

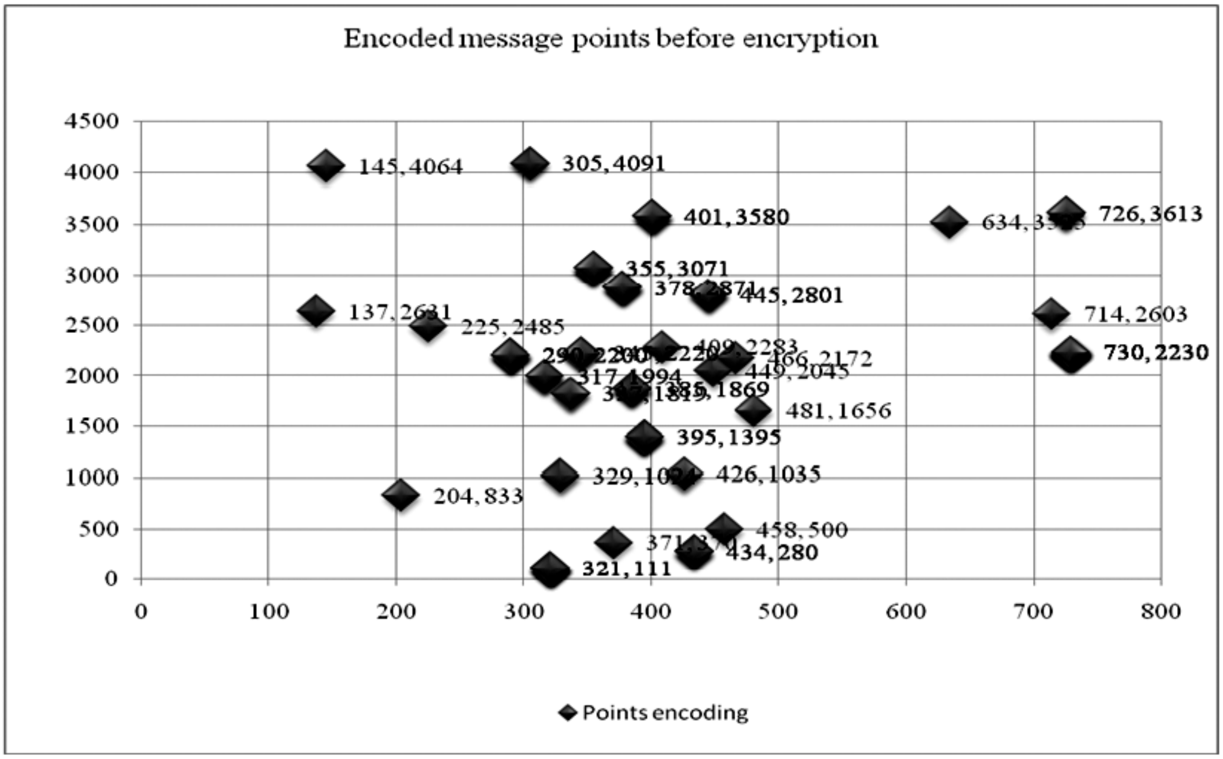

Figure 4: Encoded plain-message points before encryption

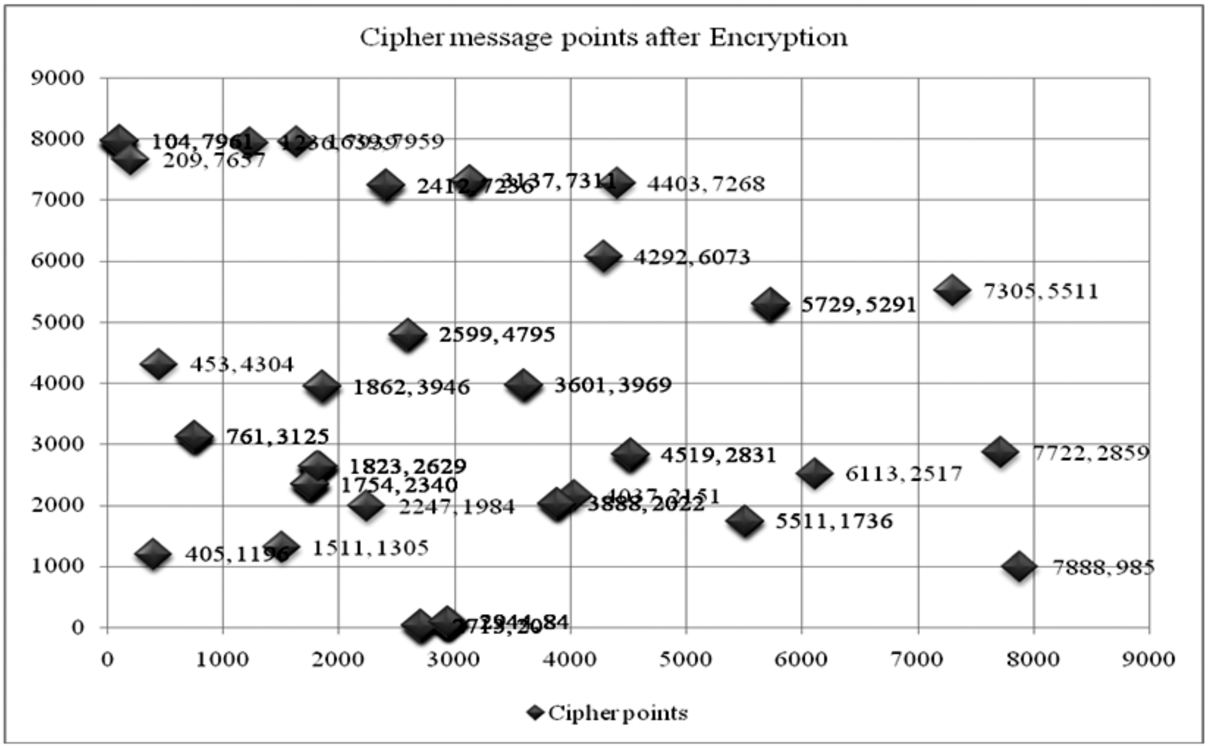

Figure 5: Cipher message points after encryption

6.4. The above Encryption (Step-B) and Decryption (Step-C) algorithms are applied for sending the secure prescription to the patient.

7. SECURITY ANALYSIS

This paper implements RSA and ECC with iris biometric based private keys for proving security to the online medical consultations between Patient and Doctor, using MATLAB R2008a on Intel Pentium dual-core processor (1.60 GHz, 533 MHz, 1 MB L2 cache) with 2GB DDR2 RAM. The iris biometric features provide most accurate and speed system for identifying a person. The efficiency of ECC over RSA is shown in Table 2 and in Figs. 6, 7, 8. From simulation result, 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 Fig. 8

Table 2
Time efficiency

	Input: Patient Above plain-message (113 bytes)					
	Encryption		*Decryption*		*Total Time*	
Security Bit Level	*ECC Enc. Time*	*RSA Enc. Time*	*ECC Dec. Time*	*RSA Dec. Time*	*ECC Total Time*	*RSA Total Time*
80	11.924	0.959574	26.8851	23.317651	38.8091	24.277225
112	43.7008	0.981524	30.3331	106.03375	74.0339	107.01527
128	62.4386	0.961092	31.406	212.60859	93.8446	213.56968
144	81.5034	0.971835	36.1522	315.06494	117.6556	316.03678

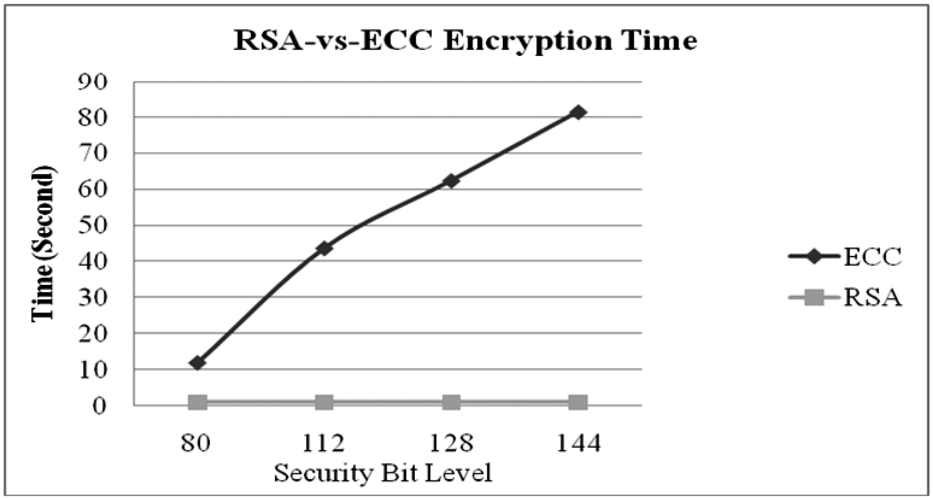

Figure 6: Encryption time (in seconds)

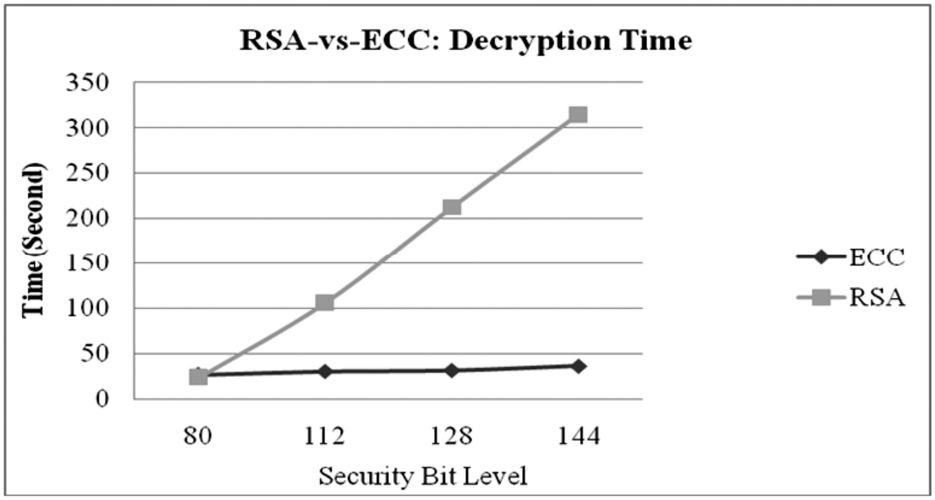

Figure 7: Decryption time (in seconds)

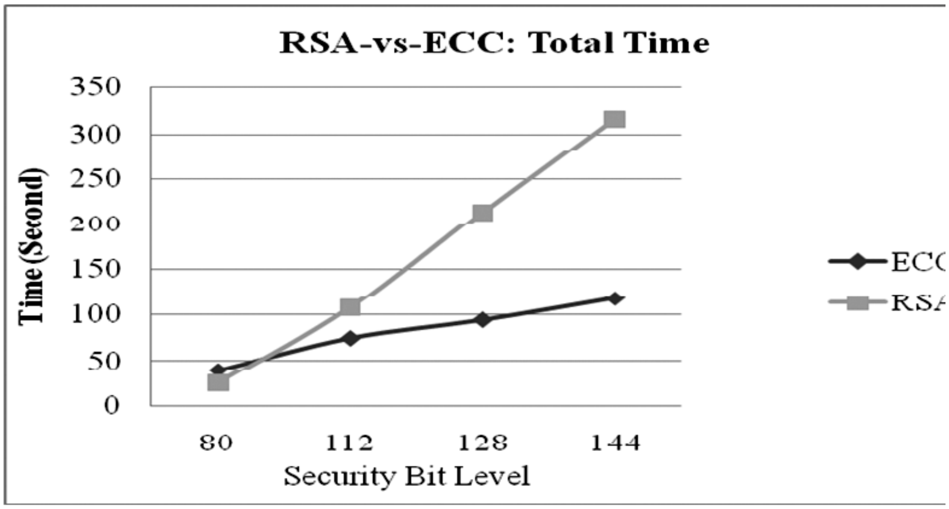

Figure 8: Total time (in seconds)

8. CONCLUSION

This paper proposed secure online medical consultations between Patient and Doctor using ECC with iris biometric. ECC offers better security with lesser key length than traditional public-key cryptography like RSA. Iris biometric offers highly reliable and accurate user authentication method due to its distinctiveness, large amount and non-counterfeiting texture pattern. This system provides better security based on the fusion of cryptography and biometric.

REFERENCES

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

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

[3] Daugman, J., "New methods in iris recognition", Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on 37(5), 1167-1175 (2007). DOI 10.1109/TSMCB.2007.903540

[4] Daugman, J., Downing, C., "Epigenetic randomness, complexity and singularity of human iris patterns", Proceedings of the Royal Society of London B: Biological Sciences 268(1477), 1737-1740 (2001). DOI 10.1098/rspb.2001.1696. URL http://rspb.royalsocietypublishing.org/content/268/1477/1737

[5] Diffie, W., Hellman, M., "New directions in cryptography", Information Theory, IEEE Transactions on 22(6), 644-654 (1976). DOI 10.1109/TIT.1976.1055638

[6] Dodis, Y., Reyzin, L., Smith, A., "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data", In: C. Cachin, J. Camenisch (eds.) Advances in Cryptology - EUROCRYPT 2004, Lecture Notes in Computer Science, vol. 3027, pp. 523-540. Springer Berlin Heidelberg (2004). DOI 10.1007/978-3-540-24676-331

[7] Hao, F., Anderson, R., Daugman, J., "Combining crypto with biometrics effectively", IEEE Transactions on Computers 55(9), 1081-1088 (2006). DOI 10.1109/TC.2006.138

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

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

[10] Kedar, I., Ternullo, J.L., Weinrib, C.E., Kelleher, K.M., Brandling-Bennett, H., Kvedar, J.C., "Internet based consultations to transfer knowledge for patients requiring specialised care: retrospective case review", BMJ 326(7391), 696-699 (2003)

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

[12] Mahto, D., Yadav, D., "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, pp. 1737-1742 (2015)

[13] Mahto, D., Yadav, D.K., "Network security using ECC with Biometric", In: K. Singh, A.K. Awasthi (eds.) QSHINE, LNICS-SITE, vol. 115, pp. 842-853. Springer Berlin Heidelberg (2013). DOI 10.1007/978-3-642-37949-973

[14] Mahto, D., Yadav, D.K., "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, pp. 1-6.IEEE (2015)

[15] Mahto, D., Yadav, D.K., "Security Improvement of One-Time Password Using Crypto-Biometric Model ", Proc. of 3rd Intl. Conf. on Advanced Computing, Networking and Informatics: ICACNI 2015, Vol. 2, chap., pp. 347-353. Springer India, New Delhi (2016). DOI 10.1007/978-81-322-2529-436

[16] Miller, V.S., "Use of elliptic curves in cryptography", In: H. Williams (ed.) Advances in Cryptology CRYPTO 85 Proc., Lecture Notes in Computer Science, vol. 218, pp. 417-426. Springer Berlin Heidelberg (1986). DOI 10.1007/3-540-39799-X31

[17] Monrose, F., Reiter, M.K., Li, Q., Wetzel, S., “Cryptographic key generation from voice”, In: Proc. of the 2001 IEEE Symposium on Security and Privacy, SP ’01, pp. 202-. IEEE Computer Society, Washington, DC, USA (2001)

[18] Ong, L.M., De Haes, J.C., Hoos, A.M., Lammes, F.B., “Doctor-patient communication: a review of the literature”, Social science & medicine 40(7), 903-918 (1995)

[19] Zhang, L., Sun, Z., Tan, T., Hu, S., “Robust biometric key extraction based on iris cryptosystem”, In: M. Tistarelli, M. Nixon (eds.) Advances in Biometrics, Lecture Notes in Computer Science, vol. 5558, pp. 1060-1069. Springer Berlin Heidelberg (2009). DOI 10.1007/978-3-642-01793-3107