International Journal of Security and Its Applications
Vol.8, No.1 (2014), pp.147-158
http://dx.doi.org/10.14257/ijsia.2014.8.1.14

Secured Session Key Agreement Protocol for Iris Cryptosystem Using Customized Elliptic Curve Cryptography

Usha. S[1] and Kuppuswami. S[2]

[1]*Assistant Professor (Sr.G), Department of EEE, Kongu Engineering College, Perundurai-638052, Tamil Nadu, India*
[2]*Professor and Principal, Kongu Engineering College, Perundurai-638052, Tamil Nadu, India*
[1]*sushamangal@gmail.com*, [2]*skuppu@gmail.com*

Abstract

E-Passports are issued to the citizens by many countries with biometric data like face, fingerprint and iris for foolproof identification. A first generation standard for E-Passport was proposed by International Civil Aviation Organisation. Due to security flaws in the proposed one, second generation standards with Extended Access Control mechanism was developed. To improve the security of E-Passport many proposals are being discussed. This paper suggests a new authentication protocol using Customized Elliptic Curve Cryptography to improve the reliability of E-Passport.

Keywords: *Elliptic Curve Cryptography, E-Passport, Feature Extraction, Iris, Normalisation, Segmentation*

1. Introduction

Since 2004, to avoid the intrusion of terrorists via border crossing, many countries started issuing E-Passports to the citizens. E-Passport contains RFID tags which are used to store data [2], process the information at low cost and transmit the information wirelessly. It also integrates with face biometrics [24] to control user authentication and fraud management.

In 2005, first generation E-Passport was developed using International Civil Aviation Organization (ICAO) standards to identify the persons with face biometrics while crossing borders. This standard has Passive Authentication (PA) [10] mechanism which proves the trustworthiness of data stored in the Machine Readable Zone (MRZ) of E-Passport but it does not prevent cloning. To prevent cloning of E-passport, Basic Access Control (BAC) [15] and Active Authentication (AA) mechanisms are introduced as optional. The BAC mechanism provides data to the terminal having physical access with the chip and AA [7] verifies whether the chip is cloned or not [24, 15].

In the year 2006, Extended Access Control (EAC) mechanism was suggested by European Union, to eliminate the security problems encountered in the first generation [24, 15]. To enhance the security it promotes additional biometrics like fingerprint and Iris. The problems encountered in this method are: data leakage, possibility of brute force attack to retrieve key, and opportunity of eaves dropping in the automated counters.

In 2008, Pasupathinathan *et al.*, suggested a novel method namely On-Line Secure E-Passport Protocol (OSEP) [24].In this method there is a possibility of selecting same Diffie Hellman parameters by two travelers.

In 2009, Mohamed Abid and Hossam Afifi suggested a new solution based on elliptic curve diffie-hellman agreement protocol [13]. As per the author's idea, elliptic curve is based

ISSN: 1738-9976 IJSIA

on selecting continuous 32 minutiae points from the finger print of the E-Passport holder. Since the fingerprint biometric is easily contaminated by noise, selecting continuous 32 same minutiae points at the receiver side may not possible. Hence in the proposed technique to eliminate the above problems a new authentication protocol using Customized Elliptic Curve Cryptography (CECC) is suggested.

2. Overview of Iris Verification System and CECC

Today, cryptography is vital for information security. Conventional cryptographic mechanisms like AES, Triple DES are used to enhance the data security. The success of these algorithms depends on the length of the key. Generally many users use short keys for easy remembrance. This increases the vulnerability of data. Biometric cryptography, [23] uses biometric features to encrypt the information, can overcome this problem. So in case of biometric based applications [16], enhanced security can be achieved by integrating biometrics and cryptographic concepts [18]. In the proposed biometric cryptography, iris biometrics and CECC are used to derive the cryptographic keys since iris has the most accurate feature when compared to all other biometrics [20].

In ECC better security can be achieved using smaller key size [3, 17] which minimizes the processing overhead. So ECC cryptosystems are used in commercial applications.

2.1. Iris Based Verification System

In iris based verification system a template is created from the captured eye during enrollment phase. When a person desires to be authenticated during verification phase, [9] his eye is first captured processed and then the template is created. This template is then compared with the other templates stored in a database until the person is identified [1]. The classical biometric system is shown in the Figure 1.

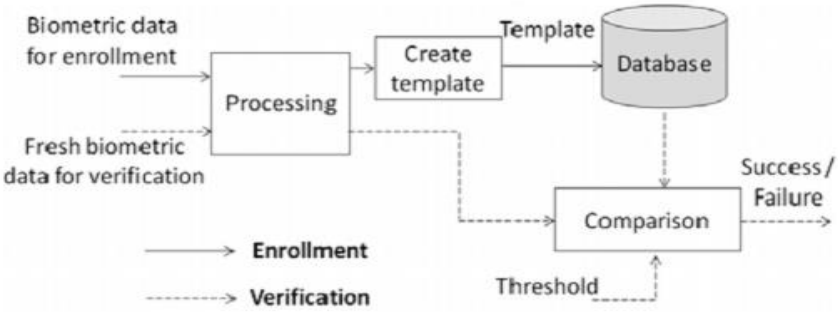

Figure 1. Biometric Verification System

2.2. Customized Elliptic Curve Cryptography

Cryptography, not only protects data from stealing or modification, but it can be used for user validation [11]. The keys used in ECC are logarithmic values, so it is not easier to recover the key. The security of ECC depends on the complexity of determining the key [21].

In the proposed method the session key is derived between client and server using customized CECC is in the following sequence [4, 14, 25].

- X and Y select an elliptic curve E defined over GF (p). They had chosen large prime q such that all the points in E (GF (p)) should be divisible q.

- X and Y select a point $G \in E$ (GF (p)) of order q.
- X selects an unpredictable integer N_1 in the interval [1, n-1].
- Y chooses the integer N_2 in [1, n-1].
- X computes point $Q_1 = N_1 * G$ and sends it to Y.
- Y computes point $Q_2 = N_2 * G$ and sends it to X.
- X now computes a common point $K \in E(GF(p))$:

$$K = N_1 * Q_2 \quad \text{and}$$

- Y now computes a common point $K \in E(GF(p))$:

$$K = N_2 * Q_1$$

Now the common key shared by both x and y is given in the equation 1.

$$K = N_1 * Q_2 = N_1 * (N_2 * G) = N_1 * N_2 * G = N_2 * (N_1 * G) = N_2 * Q_1 \qquad (1)$$

3. Proposed Method

The proposed technique has Registration Phase, Examination System (ES) Authentication Phase and E-Passport Verification Phase. In the registration phase 160 bit unique code is derived from the iris and from which cryptographic keys are generated. In the ES authentication phase, shared secret key between the E-Passport and the ES is generated to verify the reliability of ES. In the E-Passport verification phase, the authenticity of the E-passport holder is checked.

3.1. Registation Phase

In this phase, the preprocessed method developed by [6, 5] is used to segment and normalize the iris and 160 bit unique iris code is obtained from the normalized iris using SHA-1 algorithm.

The entities involved in the registration phase are shown in the Figure 2.

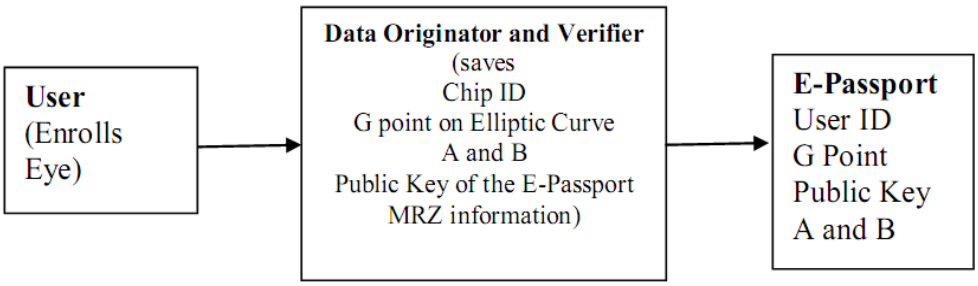

Figure 2. Registration Phase

The native country will issue an E-passport to the citizen at the time of registration. To generate elliptic curve parameters the user enrolls their eye as an input to Data Originator and Verifier (DOV).

Step 1: Generation of Unique Iris Code

Figure 3 shows thesSystem architecture of proposed method

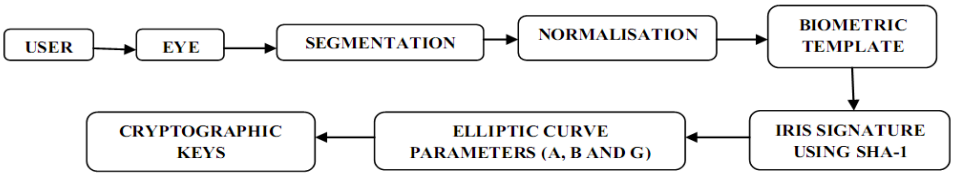

Figure 3. System Architecture

The architecture consists of segmentation system [12] used to localise the circular iris and pupil region, occluding eyelids , eyelashes, and reflections [8] from the input image. For this, canny edge detection is used to make the edges in the horizontal direction and then hough transform is implemented on it. The extracted iris region is then normalised into a rectangular block. Daugman recommended a rubber sheet model [12] for converting normal cartesian to polar transformation. As per this model, each pixel in the iris area maps into a pair of polar coordinates (r, θ), where r and θ are on the intervals of [0 1] and [0 2π] [19]. The polar form of normalized image is then given as an input for 1D Log gabor filters. Finally, the phase data from 1D Log-Gabor filters is extracted and quantised to four levels to encode the unique pattern of the iris into a bit-wise biometric template[26]. From the 9600 bits of biometric template, 160 unique digest bits are obtained using SHA-1 algorithm.

Input, Segmented, Normalized images and Biometric template are shown in the Figure 4a, 4b, 4c and 4d.

a) Input Eye b) Segmented Image c) Normalised Image d) Template

Figure 4. Results of Various Stages

Step 2: Generation of Public Key

From the unique template ECC parameters 'A' and 'B' are derived. Using this parameters elliptic curve points are generated by ECC algorithm (E_{109} (A, B)) [22]. From the points, 'G' point is chosen arbitrarily. The following pseudo code algorithm is then used to calculate the public key of the E-Passport.

Algorithm:
If A> B
Public Key = G * A
Else
Public Key = G * B
End if.

Finally ChipID, 'G' point, 'A', 'B', public key and conventional parameters of the E-passport are stored in the DOV's database. DOV also stores the same information in the RFID tag of E-Passport.

3.2. ES Authentication Phase

In this phase secured session key between E-Passport and Examination System is generated using customized ECC. This key is unique for each and every session. So that the intruder cannot easily retrieve the key and the information.

Figure 5 shows the steps involved in the process of shared secured session key generation between E-Passport and ES.

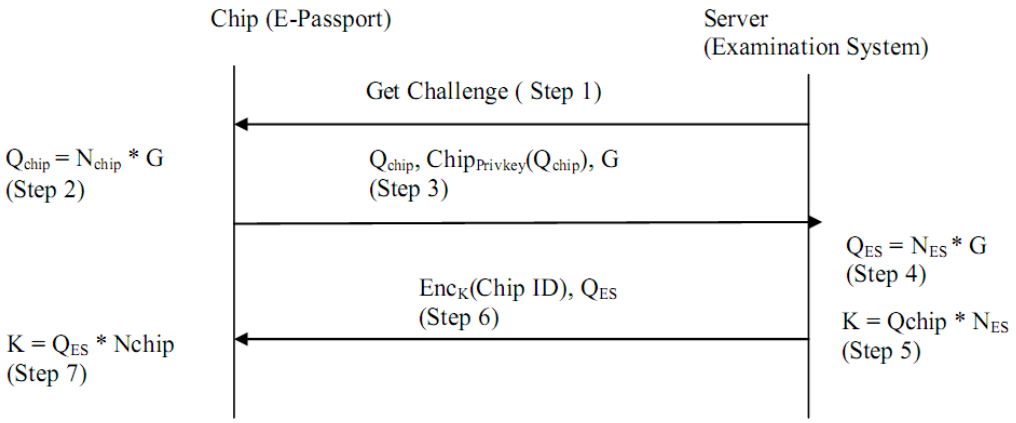

Figure 5. Line Diagram of Shared Session Key

Step 1: When E-Passport is presented to the ES it reads the information from the E-Passport and sends Get Challenge message to it.

Step 2: E-Passport generates a random Number 'Nchip' and calculates $Q_{chip} = N_{chip} * G$.

Step 3: E-Passport sends the 'Qchip','G' and encrypted value of 'Qchip' to ES. To avoid man in the middle attack, private key of the E-Passport is used for the encryption.

Step 4 & 5: The ES generates a random number 'N_{ES}' and calculates $Q_{ES}=N_{ES}*G$. Then it generates a shared session key 'K' as shown in the equation 2.

$$K = Q_{chip} * N_{ES} = (N_{chip} * G) * N_{ES} = (N_{chip} * N_{ES}) * G \qquad (2)$$

Step 6: ES sends the $Q_{ES\,,\,and}$ encrypted chipID values to E-Passport. In the proposed method AES algorithm and generated 'K' value is used for encryption. Since same key value is shared by client and server at the end of the protocol, symmetric key encryption (AES) is suggested for the proposed technique.

Step 7: On receiving the message from ES, E-Passport generates the same session key 'K' as shown in the equation 3 and decrypt the information using this 'K' value and AES algorithm.

$$K = Q_{ES} * N_{chip} = (N_{ES} * G) * N_{chip} = (N_{ES} * N_{chip}) * G \qquad (3)$$

Equation 2 and 3 shows that the session key 'K' derived by both the entity at the end of the protocol is same.

3.3. E-Passport Verification Phase

In this phase, to verify the identity of card holder the user enrolls the eye at the ES. The system generates 'A' and 'B' value in the same way as it was done during the first phase and compares it with the 'A' and 'B' values stored in the E-Passport to verify the authenticity of the card holder.

4. Results of the Proposed Method

The iris images used in the proposed method is collected from MMU1 and MMU2 public databases. Experiment is performed on 600 images.

4.1. Elliptic Curve Domain Parameters

Elliptic curve parameter 'A' and 'B' are derived from the 160 bit Iris signature. Table 1 shows the 'A' and 'B' values derived from 10 iris signatures.

Table 1. Elliptic Curve Domain Parameters

S.NO	IRIS IMAGES	A	B
1	Image 1.1	174	169
2	Image 2.1	91	79
3	Image 3.1	93	18
4	Image 4.1	56	55
5	Image 5.1	85	60
6	Image 6.1	80	57
7	Image 7.1	65	25
8	Image 8.1	107	0
9	Image 9.1	99	90
10	Image 10.1	102	45

4.2. Elliptic Curve Points

Using the above parameters (A, B) elliptic curve points for E-Passport is generated. The ECC points obtained are unique for each passport. Table 2 shows the elliptic curve points generated by the ECC algorithm $E_{109}(174,169)$ for the eye image shown in the Figure 4a.

Table 2. Elliptic Curve Points

(0 ,102)	(0 ,7)	(1 ,28)	(1, 81)	(2, 33) Public Key	(2, 76)	(4, 18)
(4, 91)	(5, 47)	(5 ,62)	(7 ,25)	(7 ,84)	(9 ,100)	(9, 9)
(10 ,43)	(10, 66)	(11 ,25)	(11, 84)	(12 ,11)	(12, 98)	(16 ,53)
(16, 56)	(17, 0)	(19, 12)	(19, 97)	(22, 24)	(22 ,85)	(23 ,39)
(23, 70)	(24 ,36)	(24 ,73)	(25 ,105)	(25, 4)	(28,32)	(28, 77)
(32 ,37)	(32, 72)	(34,33)	(34 ,76)	(37, 19)	(39, 85)	(40 ,43)
(40, 66)	(44, 38)	(44 ,71)	(46, 26)	(46,83)	(47, 102) G Point	(47, 7)
(48 ,24)	(48, 85)	(49 ,44)	(49, 65)	(50,50)	(50, 59)	(51 ,51)
(51 ,58)	(53 ,28)	(53 ,81)	(55, 28)	(59, 66)	(60, 48)	(60 ,61)

(62 ,102)	(62, 7)	(64, 46)	(64 ,63)	(65, 17)	(65, 92)	(67 ,99)
(67 ,10)	(69, 50)	(69, 59)	(71, 105)	(71 ,4)	(72, 101)	(72, 8)
(73, 33)	(73, 76)	(74, 46)	(84, 55)	(85, 1)	(85, 108)	(90 ,45)
(90, 64)	(91 ,25)	(91, 84)	(95, 0)	(96, 54)	(96,55)	(99, 50)
(99, 59)	(103 ,15)	(103, 94)	(106, 0)	(2, 76)		

4.3. Public Key Value for E-Passport

From the above elliptic curve points the public key of E-Passport is derived by using either 'A' multiplied by 'G' or 'B' multiplied by 'G' value. Table 3 shows the public key obtained for ten E-Passports.

Table 3. Public Key for E-Passports

S.NO	IRIS IMAGES	G	PUBLIC KEY
1	Image 1.1	(47,102)	(2,33)
2	Image 2.1	(61,21)	(43,21)
3	Image 3.1	(58,89)	(83,25)
4	Image 4.1	(59,49)	(102,44)
5	Image 5.1	(59,56)	(37,98)
6	Image 6.1	(55,47)	(67,76)
7	Image 7.1	(47,65)	(91,33)
8	Image 8.1	(52,60)	(57,91)
9	Image 9.1	(52,107)	(6,30)
10	Image 10.1	(50,33)	(41,3)

4.4. Shared Secured Session Key

Secured session key is generated using customized ECC algorithm. This key varies for each and every session, so that the intruders cannot retrieve the key easily. Table 4 shows the shared secure session key obtained for two sessions and for 10 E-passports.

Table 4. Shared Session Key for Two Sessions

Image	G point	Shared Key(First session)	Shared Key (Second Session)
1.1	(47,102)	[33 194 229 149 49 200 113 1 86 211 74 60 48 172 129 213]	[195 233 125 214 233 127 181 18 86 136 201 127 54 114 12 190]
2.1	(61,21)	[235 37 158 219 170 96 142 178 32 128 70 97 155 72 70 104]	[141 156 48 124 183 243 196 163 40 34 165 25 34 209 206 170]
3.1	(58,89)	[129 84 23 38 127 118 246 244 96 164 166 31 157 183 95 219]	[127 197 98 112 231 167 15 168 26 89 53 183 46 172 190 41]
4.1	(59,49)	[74 138 8 240 157 55 183 55 149 100 144 56 64 139 95 51]	[255 229 29 62 125 130 151 35 117 136 112 78 237 220 106 178]
5.1	(59,56)	[105 105 28 123 220 195 206 109 93 138 19 97 242 45 4 172]	[45 185 94 142 26 146 103 183 161 24 133 86 178 1

			59 51]
6.1	(55,47)	[93 188 152 220 201 131 167 7 40 189 8 45 26 71 84 110]	[173 30 65 206 189 67 230 74 241 162 141 77 112 220 158 48]
7.1	(47,65)	[67 236 62 93 238 110 112 106 247 118 111 255 234 81 39 33]	[158 236 183 219 89 209 108 128 65 124 114 209 225 244 251 241]
8.1	(52,60)	[69 196 140 206 46 45 127 189 234 26 252 81 199 198 173 38]	[51 109 94 188 84 54 83 78 97 209 110 99 221 252 163 39]
9.1	(52,107)	[11 206 249 196 91 216 164 142 218 27 38 235 12 97 200 105]	[185 236 225 140 149 10 251 250 107 15 219 250 79 247 49 211]
10.1	(50,33)	[165 243 198 161 27 3 131 157 70 175 159 180 60 151 193 136]	[2 18 155 184 97 6 29 26 5 44 89 46 45 198 179 131]

From the Table 4 it is understood that

- 'G' point generated from each Iris template has unique value.
- Shared session key generated is also unique for each E-Passport
- For each session the chip generates different session key

4.5. Security Analysis

During each session, ES encrypts the chipID using AES Algorithm and 'K' value. The generated cipher text is transmitted to the E-Passport. E-Passport decrypts the same using AES algorithm and 'K'. Table 5 shows the cipher text transmitted for two sessions for the same chipID.

Table 5. Cipher Text Transmission from ES to E-Chip for Two Sessions

Image	Cipher text (First session)	Cipher Text (Second Session)
Image1.1	v&7{7Q<8#p?"8%Z	]%8:#/6?IQC*.24
Image2.1	w6~ZNA+7!uZW*	p<}(+3Z=WOG`a
Image3.1	• G3m=AU[E39$5	(Rv~'Z}Nqar+yl@
Image4.1	qC6c56WwHT#'3x]i	/,dsTO(;7tT|-
Image5.1	.*LP2pXuI3msfg •	w$`!+p?ju.5%?}V5
Image6.1	a/PBKP^$qVlR t	)Rs$5+;]w5fm<57
Image7.1	_R7)L4k!a/wwa9	582jasn/ctr
Image8.1	-MKmP XM x!).ZC	M?1NMgDKTN
Image9.1	I9pVgk$X&r!hQ$-	?/E/<nT-@=-hoR
Image10.1	.@[n490cr4xQb;6r	#"0/!6F4~!(&2/_

From the above results it is identified that the proposed method satisfies the following security parameters.

Identification:

Same session key generated by E-Passport and ES shows that both the parties find the agreement of the other party's identity.

Authenticity:

Same session key resulting by the end of the protocol conveys that both the parties are confident about the authenticity of messages received during the exchange of information between each other.

Privacy:

E-Passport preserves privacy of data**,** since the passport exposes its data only to the legitimate person *i.e.,* ES and not for other malicious intruders.

Data confidentiality:

Since the proposed method uses the mutual safe and the sound session key, Data confidentiality is also assured between E-Passport and ES.

4.6. Biometric Analysis

The biometric analysis of the proposed method is evaluated by comparing the wrongly matched iris templates. Table 6 shows the comparative analysis of proposed method with the existing one described in [19].

Table 6. Template Mismatch and efficiency of Existing Method with Proposed Method

Number of Templates	Existing Method [19]		Proposed Method	
	No of Mismatch	Efficiency (%)	No of Mismatch	Efficiency (%)
150	3	98	1	99.3
300	11	96.3	6	98
450	20	95.6	9	98
600	29	95.2	19	96.8

From the table 6 it is observed that the proposed method has very few incorrect matching when compared to the one described in [19].

4.7. Time Analysis

In the proposed method both the client and server run in the same local host and the tool used is MATLAB 2010B. The time taken for generating a shared session key from iris template is 2.08851seconds on a 2.53 GHz core i5 processor with a 4GB installed RAM capacity. The time taken involves the following operations:

Server side operation (Examination System):

Receiving Q_{chip} data from E-Passport (0.529430 seconds)

QES generation $Q_{ES} = N_{ES} * G$ Here G = (47,102) (0.031231 seconds)

Transferring QES to E-Passport (0.469866 seconds)
Shared key Generation by Examination system $K = N_{ES} * Q_{chip}$ (0.008124 seconds)

Total time taken for server side operation is 1.038651 seconds.

Client side operation (E-Passport):
Qchip Generation = $N_{chip} * G$ (0.024544 seconds)

Transferring Qchip to Inspection System (0.512878 seconds)
Shared key Generation by Chip $K = N_{chip} * Q_{ES}$ (0.004915 seconds)

Total time taken for entire operation is **2.088851 seconds**

These results have been obtained without code optimization. If the system is implemented after code optimization, definitely, it would further reduce the total processing time. There will be variation of + or – 10% elapsed time when each time the software runs, since the random number generated for 'Q_{chip}' and 'Q_{ES}' generation will vary each time. So the number of ECC addition, doubling and multiplication time varies.

5. Conclusion

Use of biometric based identification cards like E-Passport E-Driving license and National Identification cards are emerging applications in many countries. Security is a major issue in these type of applications since they store sensitive data like fingerprint templates, iris templates *etc*. To enhance the security for these types of applications, in the proposed method, an iris based crypto system using customized Elliptic curve cryptography is suggested. As per the proposed method ECC parameters and ECC points are derived from the iris Signature. From these values public key of an E-Passport and shared secure key between E-Passport and the ES is generated. The proposed method satisfies the security goals like unique identification, data confidentiality and privacy of the E-Passport holder.

In the proposed method, data stored in the secured memory is leaked only when the E-Passport confirms the authenticity of ES with the help of shared secrecy, hence chances of data leakage is avoided. Since each session the key varies, brute force attack is not possible. In future the formal security analysis of the proposed system has to be verified using automatic protocol verification tools like AVISPA.

References

[1] M. Abid, S. Kanade, D. Petrovska-Delacretaz and B. Dorizzi, "Iris Based Authentication Mechanism for E-Passports", International Workshop on Security and Communication Networks, Karlstad, Sweden, **(2010)** May 26-28.
[2] A. B. Jeng and L.-Y.-Chen, "How to enhance the security of E-Passport", Proceedings of the Eighth International Conference on Machine Learning and Cybernetics, Baoding, China, **(2009)** July 12-15.
[3] A. Khalique, K. Sing and S. Sood, "Implementation of Elliptic Curve Digital Signature Algorithm", International Journal of Computer Applications, vol. 2, no. 2, **(2010)**, pp. 21-27.
[4] A. Burnett, F. Byrne, T. Dowling and A. Duffy, "A Biometric Identity Based Signature Scheme", International Journal of Network Security, vol. 5, no. 5, **(2007)**, pp. 317-326.
[5] J. Daugman, "Biometric Personal Identification System Based on Iris Analysis", U.S.patent, no. 5291, 560, **(1994)** March 1.
[6] J. G. Daugman, "How iris recognition works", IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, **(2004)**, pp. 21-30.
[7] S. Kc. Gaurav and P. A. Karger, "Security and Privacy Issues in Machine Readable Travel Documents (MRTDs)", 10th European Symposium on Research in Computer Security, Milan, Italy, **(2005)** September 14-16.

[8] F. Hao, R. Anderson and J. Daugman, "Combining Crypto with Biometrics Effectively", IEEE Transactions on Computers, vol. 55, no. 9, **(2006)**, pp. 1081-1088.
[9] J. M. H. Ali and A. E. Hassanien, "An Iris Recognition System to Enhance E-security Environment Based on Wavelet Theory", Advanced Modeling and Optimization, vol. 5, no. 2, **(2003)**, pp. 93-104.
[10] A. Jules, D. Molnar and D. Wagner, "Security and Privacy issues in E-Passports", First International Conference on Security and Privacy for Emerging Areas in Communications Networks, Athens, Greece, **(2005)** September 05-09.
[11] U. Mahalakshmi and V. S. Shankar Sriram, "An ECC Based Multibiometric System for Enhancing Security", Indian journal of Science and Technology, vol. 6, no. 4, **(2013)**, pp. 4299-4305.
[12] M. Raosaheb Bendre and S. Ashok Shivarkar, "An Improved Approach for IRIS Authentication System by Using Daugman's Rubber Sheet Model, Segmentation, Normalization and RSA Security Algorithm", International Journal of Computer Technology and Electronics Engineering, vol. 1, no. 3, **(2011)**, pp. 102-107.
[13] M. Abid and H. Afifi, "Towards a Secure E-Passport protocol based on biometrics", Journal of Information Assurance and Security, vol. 4, no. 4, **(2009)**, pp. 338-345.
[14] M. Abid and H. Afifi, "Secure E-Passport Protocol using Elliptic Curve Diffie-Hellman Key Agreement protocol", Proceedings of the Fourth International Conference on Information Assurance and Security, IEEE, Washington, DC, USA, **(2008)** September 8-10.
[15] P. Najera, F. Moyano and J. Lopez, "Security Mechanisms and Access Control Infrastructure for e-Passports and General Purpose e-Documents", Journal of Universal Computer Science, vol. 15, no. 5, **(2009)**, pp. 970-991.
[16] N. Ratha, J. Connell and R. Bolle, "Enhancing security and privacy in biometrics-based authentication systems", IBM Syst. Journal, vol. 40, no. 3, **(2001)**, pp. 614-634.
[17] S. Gajbhiye, M. Sharma and S. Dashputre, "A survey Report on Elliptic Curve Cryptography", International Journal of Electrical and Computer Engineering, vol. 1, no. 2, **(2011)**, pp. 195-201.
[18] S. G. Kande, D. Petrovska-Delacretaz and B. Dorizzi, "Enhancing Information Security and Privacy by combining Biometrics with Cryptography", Morgan & Claypool Publishers, San Rafael, **(2012)**.
[19] K. Saraswathi, B. Jeyaram and R. Balasubramanian, "Iris biometrics based Authentication and Key Exchange System", International Journal of Engineering and Technology, vol. 3, no. 1, **(2011)**, pp. 102-108.
[20] S. Dey and D. Samanta, "Improved Feature Processing for Iris Biometric Authentication System", International Journal of Electrical and Electronics Engineering, vol. 4, no. 2, **(2010)**, pp. 127-134.
[21] W. Stallings, "Cryptography and Network Security - Principles and Practice", Prentice-Hall, New Delhi, 4th Edition, **(2006)**, pp. 301-313.
[22] B. Thiruvaimalar Nathan, R. Meenakumari and S. Usha, "Formation of elliptic curve using Fingerprint for Network Security", Proceedings of International conference on Process Automation, Control and Computing, Coimbatore, India, **(2011)** July 20-22.
[23] U. Uludag, S. Pankanti, S. Prabhakar and A. K. Jain, "Biometric Cryptosystems: Issues and Challenges", Proceedings of IEEE, Seville, Spain, **(2004)** June 14-16.
[24] V. Pasupathinathan, J. Pieprzyk and H. Wang, "Security Analysis of Australian and E.U. E-Passport Implementation", Journal of Research Practice in Information Technology, vol. 40, no. 3, **(2008)**, pp. 187-205.
[25] L. Washington, "Elliptic Curves: Number Theory and Cryptography", Chapman and Hall, CRC, 1st edition, **(2003)**.
[26] H. Xiangqian Wu, N. Qi, K. Wang and D. Zhang, "A Novel Cryptosystem based on Iris Key Generation", Fourth International Conference on Natural Computation, Jilan, China, **(2008)** October 18-20.

Authors

S. Usha, presently working as an Assistant Professor(Senior Grade) in EEE Department, Kongu Engineering College, Perundurai, Erode, TamilNadu. She received her B.E.,in Electronics and Communication Engineering in1992 at Bharathiar University, Coimbatore. M.E. in Power Electronics and Drives in 2008 at Anna University, Chennai. She is presently working for her Ph.D in the area of Network Security. Her area of interest includes Network Security, Mobile ad hoc Networks and Digital Image Processing. email: sushamangal@gmail.com

S. Kuppuswami, presently working as Professor and Principal in Kongu Engineering College, Perundurai, Erode, TamilNadu. He has more than 35 years of experience in technical education in India and abroad. He received B.E in ECE in 1975, M.Sc.Engg in Applied Electronics in 1977 and Ph.D in Engg in Computer Science from University of Rennes I, France in 1986. His primary research interests include Software Engineering, Software Architecture, and Network Security. He is a life member of Computer Society of India and Indian Society of Technical Education. email:skuppu@gmail.com.