A Biometric Based Secure Session Key Agreement using Modified Elliptic Curve Cryptography

Usha Subramaniam[1] and Kuppuswami Subbaraya[2]
[1]Department of Electrical and Electronic Engineering, Kongu Engineering College, India
[2]Kongu Engineering College, India

Abstract: *Protection of data and network security has been greatly researched. To enhance the security in the case of border control applications like E-Passport, conventional cryptographic concepts are integrated with biometrics. To avoid the intrusion of terrorists after the terrorists attack of 9/11, many countries begin to issue E-Passport to their citizens contains biometric data like face, fingerprint and iris. The first generation E-Passport developed as per the standards and specifications of international civil aviation organization is confirmed to be lacking confidence and has numerous threats. The second generation E-Passport, was designed as per the mechanism of extended access control also submits lots of threats especially in safety and confidentiality. In this article, security enhanced mechanism based on variation of Diffie-Hellman key agreement protocol using Elliptic Curve Cryptography (ECC) between E-Passport and the Examination System (ES) is suggested. In the proposed method elliptic curve parameters A, B and G are derived from the minutiae points of the fingerprint. From these parameters public key of E-Passport and session key between E-Passport and ES is generated. The security analysis of the proposed solution confirms the security goal of the biometric based system. The proposed protocol is developed using MATLAB (R2010b) tool.*

Keywords: *Active authentication, data originator, verifier, ECC, e-passport, ES, passive authentication.*

Received March 16, 2013; accepted July 11, 2013; published online April 23, 2014

1. Introduction

E-Passports are biometric identification document contains RFID tags [9], which are used to store data, processing the information at low cost and transmitting the information wirelessly. E-Passport is incorporated with biometrics, Public Key Infrastructure (PKI) and radio frequency identification technologies [3] to manage user authentication and fraud management problems. E-Passport standard specifications are:

1. 13.56 MHz frequency for communication. (Inductive coupling between the tag and Examination System (ES) is used for signal propagation) [2].
2. Tags of size 125mm×88mm.
3. 32 to 144 KB inbuilt EEPROM stores Data Group. Information (DG1-DG16). These groups used to store Machine Readable Zone (MRZ) information, extracted biometric feature, public keys etc.
4. Power required for the tag to operate as per standard specification is 55mw.

In order to, maintain global operability in between E-Passport and ES, the International Civil Aviation Organisation (ICAO) specifies a standard data structure to store the data elements like MRZ [13] encoded biometric information, certificates etc., as per the ICAO [5] specification, 16 DGI has to be written in the E-Passport at the issuing time by the resident country of E-Passport holder. The digitally signed hash value of these data group named Security Data Element (SDE) is also stored. Table 1 shows the E-Passport logical data structure.

Table 1. E-passport logical data structure.

Data Group	Data Element
1st DG	Document Details
2nd DG	Encoded Face Value
3rd DG	Encoded Finger Print
4th DG	Encoded Iris
5th DG	Displayed Portrait
6th DG	Reserved for Future Use
7th DG	Signature
8th,9th and 10th DG	Data Features
11th,12th and 13th	Additional Details
14th DG	Certificate Authority Public Key
15th DG	Active Authentication Public Key
16th DG	Persons to Notify
SDE	Security Data Elements

In 2005, the ICAO has developed the above standards for first generation E-Passport in order to avoid the intrusion of terrorists via country borders. As per the standard, a passport booklet contains a contactless, smart card processor embedded [6] within it. The processor is used to store the facial feature information of the card holder along with the personal information. The stored information must be presented to the border control officials at the instance of confirmation. Mandatory operation involved at the border control to improve security as per this standard is Passive Authentication (PA). The primary goal of PA allows the ES to prove the data stored in the E-

Passport is reliable. The optional mechanisms to rectify skimming and eaves dropping problems are Basic Access Control (BAC) and Active Authentication (AA) [11]. The BAC mechanism makes only the reader having physical access with the date can read the MRZ information of the chip and AA [8] verifies whether the chip is redundant or not.

Hao *et al*. [4] developed a new standard proposal Extend Access Control (EAC), to eliminate the security problems encountered in the first generation passport. It promotes additional biometrics like fingerprint and iris for further security. The proposed protocol **c**onsists of 3 steps [14]:

1. BAC (Mutual Authentication).
2. Chip Authentication (CA).
3. Terminal Authentication (TA).

CA is a protocol for terminal to authenticate the chip and TA is a protocol for chip to authenticate the terminal.

2. Literature Survey

Juels *et al.* [9] explain the secrecy and confidentiality issues of the first generation passport. According to their observation, since contact less chip is embedded [11] there is a possibility of data leakage from the E-Passport without direct contact with ES. Therefore, data available in the chip will be eavesdropping. The key used for BAC is derived from MRZ information, so that the entropy of the key used for authentication is low, causes brute force attack to find out the key value. The risk of eaves dropping is more, if the border control is fully automated. This causes possible collection of E-Passport data by the intruder.

In 2006, aware about these weaknesses, a new proposal has suggested by European Union (EU) known as EAC provides E-Passport specification for second generation protocol. Pasupathinathan *et al.* [18], Justice and Home Affairs (European Committee) [10] identified the shortcomings in the EAC protocol. The authors express their concerns that the EAC protocol still uses BAC to derive the session key. So, the problems present in BAC are also addressed here.

Pasupathinathan *et al.* [17] suggested a novel idea called On-line Secure E-Passport protocol (OSEP). They recommended a mutual authentication between the E-Passport chip and the ES. As per their findings the drawbacks of the EAC proposal are: ES receives a chain of certificates for verification, Makes extensive use of PKI, verification of certificates needs entire certificate hierarchy, EAC also requires cross certification [19] among countries.

Abid and Afifi [1] identify the problem in the OSEP protocol which are: There is a possibility of choosing the same diffie- hellman parameters by two travelers and this protocol verifies whether the E-Passport is reliable or not but not its owner. The authors also suggested a new solution based on elliptic curve Diffie-Hellman agreement protocol for avoiding above threats. In their method they generate elliptic curve based on selecting 32 minutiae points from the finger print of the E-Passport holder in an ordered manner. But, in real time scenario, to verify the user's identity selecting 32 points in an ordered manner is a critical task.

In the proposed method to rectify the above problems, a new authentication protocol by making a slight modification over the protocol based on variation in Diffie-Hellman key agreement protocol using Elliptic Curve Cryptography (ECC) is suggested. In the proposed method, elliptic curve parameters A, B and G are derived from the all minutiae points and these values are stored in the E-Passport chip and database of the DOV. From this a shared secret session key between E-Passport and ES is generated.

3. Background of ECC

In this section, the basics of elliptic curves over finite fields and principles of ECC are outlined in a few words.

3.1. Elliptic Curve Group Operation Over GF(p)

Koblitz and Miller first suggested ECC which is based on algebraic structure of elliptic curves over finite fields. The ECC comes under the category of abelian group and the keys [20] used in ECC are generally, logarithmic values, so it cannot be easier to retrieve the key values. Hence, ECC provides more security than RSA with smaller key size. As the keys size is very small, processing overheads are automatically reduced. The key size for ECC is only 256 bits whereas for RSA the key size is 3072 bits.

Elliptic curves are not ellipses. Let *p* be an odd prime > 3. The irreducible polynomial as shown in the Equation 1 which is the basic foundation for elliptic curve *E* defined over GF(p) is used in the proposed method [20].

$$y_1{}^2 = x_1^3 + Kx_1 + L\ (mod\ p) \qquad (1)$$

With, x_1, y_1, K and $L\ \varepsilon\ GF(p)$ and $4K^3+27L^2 \neq 0$ $(mod\ p)$ [12]. This constraint on elliptic curve ensures that the cubic on the right does not have multiple roots.

3.2. A Variation of Diffie-Hellman Key Agreement using Elliptic Curve

This protocol is a new variant of the Diffie-Hellman protocol using ECC. The description of algorithm is:

- *U1* and *U2* select an elliptic curve *E* defined over *GF*(*p*). They chosen large prime *q* such that all the points in *E*(*GF*(*p*)) should be divisible *q*.

- *U1* and *U2* select a point $G \in E(GF(p))$ of order q.
- *U1* selects a unpredictable integer N_C in the interval $[1, n\text{-}1]$.
- *U2* chooses the integer N_{ES} in $[1, n\text{-}1]$.
- *U1* computes point $Q_c=N_c*G$ and sends it to *U2*.
- *U2* computes point $Q_{ES}=N_{ES}*G$ and sends it to *U1*.
- *U1* now computes a common point $K \in E(GF(p))$:$K=N_c * Q_{ES}$.
- *U2* now computes a common point $K \in E(GF(p))$: $K=N_{ES} * Qc$.

Now, both *U1* and *U2* generates same secret session key as given in Equation 2.

$$\begin{aligned} K &= N_C*Q_{ES}=N_C*(N_{ES}*G)=N_C*N_{ES}*G \\ &= N_{ES}*(N_C*G)=N_{ES}*Q_C \end{aligned} \tag{2}$$

4. Proposed Research Work

The proposed methodology has 3 phases. The first phase is registration phase. In this, elliptic curve coordinates A, B, G and elliptic curve points are derived from the finger print minutiae points like termination and bifurcation of the user during registration time. The second phase is the ES authentication. Here, in order to make secret communication between the passport chip and ES of the country visited by the holder, a shared session key is derived. The third phase is the E-Passport holder authentication; here, ES will make sure that E-Passport holder is legitimate and not an impostor.

4.1. Registration Phase

During registration time the user first enrolls the fingerprint. From the finger print template the DOV finds out the coordinate points (*x*, *y* and angle) from fingerprint minutiae. From this value parameters of elliptic curve A, B and G are calculated. The Figure 1 shows the entities involved during registration phase.

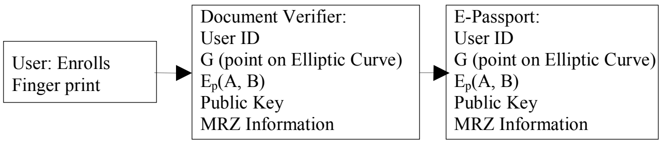

Figure 1. Registration phase.

During registration time User *ID*, *G* point on the elliptic curve, *Ep(A,B)*, public key of the E-Passport, parameters like name, country, age, gender etc., are stored in the DOV's database. DOV also writes the same information in the MRZ part of the E-Passport chip. After this process is completed the E-Passport will be issued to the user.

4.1.1. Algorithm Level Design of Registration Phase

The flow chart of the registration phase as shown in Figure 2.

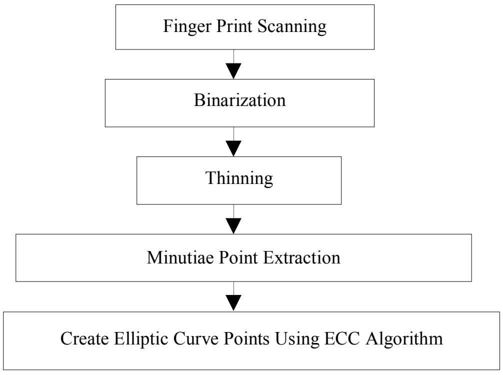
Finger Print Scanning
Binarization
Thinning
Minutiae Point Extraction
Create Elliptic Curve Points Using ECC Algorithm

Figure 2. Flow chart of registration phase.

- *Step1. Finger Print Image*: Finger print images are acquired from FVC 2004 public database and scanned using R303A scanner.
- *Step 2. Binarization*: In this process a gray scale image is converted into binary format of the image. In the proposed method, adaptive thresholding technique is used for binarization. In this method, each pixel is set with a new value (1 or 0), using Equation 3.

$$Inew = (n1, n2) = \begin{cases} 1 & if\ Iold >= Local\_mean \\ 0 & otherwise \end{cases} \tag{3}$$

Where, *Inew* and *Iold* are the new and old frame intensity [16].

- *Step 3. Thinning*: After binarization, thinning [7] process is applied over the image, which reduces the thickness of all ridge lines to a single pixel. In the proposed method, central line thinning methodology is used.
- *Step 4. Noise Removal*: Following the thinning process, a final stage of noise removal is conducted to eliminate noise produced from the previous processes. This stage focuses on removing the unwanted segments near the outer boundaries of the image which were produced during the binarization phase. Such segments need to be removed because they do not represent the true ridge structure of the original fingerprint.
- *Step 5. Minutiae Extraction*: In this process the information about the minutiae points like position of the minutiae points within the image, orientation angle and nature (termination or bifurcation) are extracted. In the proposed method, the crossing number is used to locate the terminations and bifurcations within the final thinned image.
- *Step 6. Creation of Elliptic Curve Coordinates*: From the finger print minutiae coefficients the Elliptic curve coordinate values A, B and G point [15] are derived.

4.2. ES Authentication Phase

In this phase the ES has proved itself as a reliable one to the chip. The processes which are taken place during this authentication phase are shown in the Figure 3.

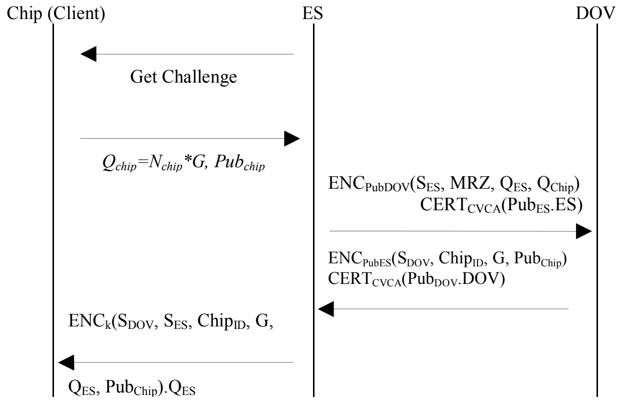
Chip (Client)
ES
DOV
Get Challenge
$Q_{chip}=N_{chip}*G$, Pub_{chip}
$ENC_{PubDOV}(S_{ES}$, MRZ, Q_{ES}, $Q_{Chip})$
$CERT_{CVCA}(Pub_{ES}.ES)$
$ENC_{PubES}(S_{DOV}$, $Chip_{ID}$, G, $Pub_{Chip})$
$CERT_{CVCA}(Pub_{DOV}.DOV)$
$ENC_k(S_{DOV}$, S_{ES}, $Chip_{ID}$, G,
Q_{ES}, $Pub_{Chip}).Q_{ES}$

Figure 3. ES authentication phase.

- When, the visitor presenting the E-Passport to the ES of the visiting country, on reading the contents present in the MRZ information of the chip, in response to this ES sends Get Challenge command to the chip.
- On receiving the command, the chip generates a secret random number N_{chip} and calculates $Q_{chip}=N_{chip}*G$ and sends this value to ES.
- ES generates a signature contains the MRZ information along with the received Q_{chip} value. The signature is encrypted using public key of the DOV and the secret information along with the certificate of ES is transmitted to the DOV of the chip's holder country.
- DOV decrypts the received information and recognize the reliability of ES. If the ES is reliable reader in order to answering it, DOV generates the signature as given in Equation 4.

$$S_{DV} = SIGN_{DOV}(MRZ \ / \ Q_{chip} \ / \ Pub_{ES}) \qquad (4)$$

  Then, encrypted information by using public key of the ES as shown in the flow diagram along with the certificate of DOV is transferred to the ES.
- The ES generates a secret random number N_{ES} and calculates $Q_{ES}=N_{ES}*G$ and secret shared session key as given in Equation 5:

$$K = Q_{chip} * N_{ES} = (N_{chip} * G) * N_{ES} = (N_{chip} * N_{ES}) * G \qquad (5)$$

- Then, information received from DOV along with its signature, and Q_{ES} value is encrypted using K then transmitted to chip.
- In the last step, the chip generates a same secret shared session key K as given in Equation 6 and decrypt the received information to conform the genuineness of ES.

$$K = Q_{ES} * N_{chip} = (N_{ES} * G) * N_{chip} = (N_{ES} * N_{chip}) * G \qquad (6)$$

4.3. E-Passport Holder Authentication Phase

In the proposed method, to verify the authenticity, the user enrols their fingerprint in the scanner, available in the ES. The ES extracts feature, and verifies whether the template is matched with the template present in the E-Passport. If ES identifies the E-Passport holder is genuine, ES and the chip will agree about a shared session key. After that, the chip can release its protected data to the ES in a secure way.

5. Results and Security Analysis of the Proposed Protocol

Since, the proposed algorithm is related to images, it is very easy to handle images in MATLAB as compared to other languages like C, C++ and Java etc., the finger print images without noises are taken from FCA2004 database and by using R303A scanner. In the proposed algorithm all the phases are implemented using MATLAB (R2010b).

5.1. Registration Phase

In the registration Phase, the minutiae points are extracted from the finger print.

5.1.1. Termination Data

The Table 2, shows the termination coordinate points and corresponding orientation angle for the sample finger print (Only 7 termination values are given).

Table 2. Matrix for termination data.

Row Index	Column Index	Angle
176	50	120.96
26	67	338.19
74	72	21.80
128	76	270
144	93	36.87
239	90	0
231	100	11.30

5.1.2. Bifurcation Data

For the finger print taken for processing, 28 Bifurcation points are obtained. The Table 3 shows the (x, y) coordinate points and bifurcation angles obtained. (Only 7 Bifurcation values are given).

Table 3. Matrix for bifurcation data.

Row Index	Column Index	Angle
120	33	68.19
143	33	78.69
177	38	111.80
67	72	210.96
88	93	158.19
209	95	216.87
26	116	168.69
88	93	158.19

5.1.3. Public Key and Elliptic Curve Coordinates for E-Passport

The Public key of the E-Passport derived from sample fingerprint is $E_{109}(61,73)$. The elliptic curve coordinate values are $A=15$, $B=11$ and G point is (2, 7).

5.2. ES Authentication Phase

In the First step, the protocol is running between E-Passport and ES of visiting country.

In the Second step, the same existing protocol between ES and DOV is used. Since, the protocol running between ES and DOV is universally acceptable, no modification is suggested in the proposed method.

In the third step Shared session key is generated in between ES and E-Passport using proposed algorithm. The server (ES of visiting country) and the client (E-Passport) are assumed to be running in the same local host.

5.2.1. Implementation Details

1. E-Passport shared session key generation:
    - *Sskeychip.m*: This program is running in the chip for generating shared secret session key.
    - *FromES.m*: This is a function added with the Sskeychip.m. This is a client server program to retrieve messages from Examination system
    - *ChipToES.m*: This is a client server program used to transfer information from chip to Examination system.
2. ES shared session key generation:
    - *SskeyES.m*: Used to create shared session key between Examination system and E-Passport
    - *FromES.m*: This is client server program transmit messages to E-Passport
    - *ChipToES.m*: This is client server program used to receive information from chip to ES.

The Table 4 conveys the processes that are taken place at the client E-Passport System. The Table 5 shows the processes that are taken place at the server ES.

Table 4. Shared session key generation at E-passport.

INPUT: (Elliptic curve Parameters) Ep(A,B)
Prime Number (p): 109
Base Point G: (2,7) Taken from the elliptic curve points generated from finger print minutiae.
A = 15, B = 11
N_{chip}(Random Number): 229 (Not transmitted).
Q_{CHIP}:(57,43) (Qchip = Nchip*G) i.e., (Qchip = 229*(2,7)). This information is transmitted to the Examination system, using ChipToES.m program.
Q_{ES}: (21,70).This QES information is received from ES using client server program FromES.m.
Shared KEY by chip: (22,78). This is a shared key generated by the chip using modified ECC algorithm.i.e., K = Nchip*QES = Nchip * (NES*G).
For Decrypt: Algorithm Used is AES and Block size is 16.
Cipher Text received is: 40 117 139 103 60 164 109 180 50 188 75 64 67 187 112 239 28 1 224 137 146 34 6 170 190 55 152 158 7 228 251 192.
Key Used is: 141 156 48 124 183 243 196 163 40 34 165 25 34 209 206 170.
Plain text: SDV,SES,CHIPID,G,Pubchip.

Table 5. Shared session key generation at ES.

INPUT 1.a(Elliptic curve Parameters) Ep(A, B)
Prime Number (p): 109
Base Point G: (2,7) Taken from the elliptic curve points generated from finger print minutiae.
A = 15, B = 11.
NES (Random Number): 243 (Not transmitted).
QES: (21, 70) (QES=NES*G). This information is transmitted to the E-Passport.
QCHIP: (57, 43). Qchip information is received from E-Passport.
Shared KEY by chip: (22, 78). This is a shared key generated by the ES using modified ECC algorithm.i.e Key= NES*Qchip = NES* (Nchip*G).
For Encryption Algorithm AES is used.
Plain Text: SDV, SES, CHIPID, G, Pubchip.
Key Used: 141 156 48 124 183 243 196 163 40 34 165 25 34 209 206 170.
Cipher Text transmitted: 40 117 139 103 60 164 109 180 50 188 75 64 67 187 112 239 28 1 224 137 146 34 6 170 190 55 152 158 7 228 251 192.

The Tables 4 and 5 results convey that the shared session key generated between E-Passport and the ES is *141 156 48 124 183 243 196 163 40 34 165 25 34 209 206 170.*

5.3. Third Phase

In this phase the genuineness of the E-Passport holder is checked.

5.4. Security Analysis of the Proposed Method

The results show that the:

- Arbitrarily chosen *G* point generated from each finger print (each Passport chip) has a unique value.
- Shared Session key generated is also unique for each E-Passport.
- Two chips will not generate same session key.
- For each session the chip generates different session key.

The Table 6 shows the shared session key generated between E-Passport and ES for 10 finger prints which are taken from FVC 2004 database and the Table 7 for 10 finger prints which are taken from R303A database.

Table 6. Shared session key generated (FVC 2004).

S. No	**Image**	**G Point**	**Shared Key(First Session)**	**Shared Key (Second Session)**
1	101_1.tif	(47,14)	143 20 228 95 206 234 22 122 90 54 222 221 75 234 37 67	33 194 229 149 49 200 113 1 86 211 74 60 48 172 129 213
2	102_1.tif	(46,84)	177 74 123 128 89 217 192 85 149 76 146 103 76 230 0 50	185 236 225 140 149 10 251 250 107 15 219 250 79 247 49 211
3	103_1.tif	(56,84)	140 228 177 107 34 181 136 148 170 134 196 33 232 117 157 243	185 236 225140 149 10 251 250 107 15 219 250 79 247 49 211
4	104_1.tif	(48,51)	33 194 229 149 49 200 113 1 86 211 74 60 48 172 129 213	82 6 86 10 48 106 46 8 90 67 127 210 88 235 87 206
5	105_1.tif	(51,40)	102 102 205 118 249 105 86 70 158 123 227 157 117 12 199 217	40 211 151 232 115 6 184 99 31 62 216 13 133 141 53 240
6	106_1.tif	(44,61)	81 142 210 149 37 115 140 235 218 196 156 73 230 14 169 211	74 138 8 240 157 55 183 55 149 100 144 56 64 139 95 51
7	107_1.tif	(51,84)	235 37 158 219 170 96 142 178 32 128 70 97 155 72 70 104	53 144 203 138 240 187 185 231 140 52 59 82 185 55 115 201
8	108_1.tif	(47,86)	165 243 198 161 27 3 131 157 70 175 159 180 60 151 193 136	58 62 160 12 252 53 51 44 237 246 229 233 163 46 148 218
9	109_1.tif	(48,36)	146 235 95 254 230 174 47 236 58 215 28 119 117 49 87 143	140 228 177 107 34 181 136 148 170 134 196 33 232 117 157 243
10	110_1.tif	(48,32)	12 193 117 185 192 241 182 168 49 195 153 226 105 119 38 97	130 119 224 145 13 117 1 149 180 72 121 118 22 224 145 173

Table 7. Shared session key generated (R303A).

S.No	Image	G point	Shared Key (First Session)	Shared Key (Second Session)
1	F1.bmp	(55,12)	76 97 67 96 218 147 192 160 65 178 46 83 125 225 81 235	140 228 177 107 34 181 136 148170 134 196 33 232 117 157 243
2	F2.bmp	(61,73)	221 117 54 121 75 99 191 144 236 207 211 127 155 20 125 127	128 6 24 148 48 37 49 95 134 158 78 31 9 71 16 18
3	F3.bmp	(46,2)	68 194 158 219 16 58 40 114 245 25 173 12 154 15 218 170	126 106 42 254 85 30 6 122 117 250 250 207 71 166 217 129
4	F4.bmp	(55,40)	33 194 229 149 49 200 113 1 86 211 74 60 48 172 129 213	127 197 98 112 231 167 15 168 26 89 53 183 46 172 190 41
5	F5.bmp	(50,33)	12 193 117 185 192 241 182 168 49 195 153 226 105 119 38 97	168 127 246 121 162 243 231 29 145 129 166 123 117 66 18 44
6	F6.bmp	(57,1)	158 236 183 219 89 209 108 128 65 124 114 209 225 244 251 241	45 185 94 142 26 146 103 183 161 24 133 86 178 1 59 51
7	F7.bmp	(51,17)	143 20 228 95 206 234 22 122 90 54 222 221 75 234 37 67	51 109 94 188 84 54 83 78 97 209 110 99 221 252 163 39
8	F8.bmp	(52,9)	53 144 203 138 240 187 185 231 140 52 59 82 185 55 115 201	102 102 205 118 249 105 86 70 158 123 227 157 117 12 199 217
9	F9.bmp	(53,14)	134 92 12 11 74 176 224 99 229 202 163 56 124 26 135 65	68 194 158 219 16 58 40 114 245 25 173 12 154 15 218 170
10	F10.bmp	(46,76)	108 255 4 120 84 241 154 194 170 82 170 197 27 243 175 74	74 138 8 240 157 55 183 55 149 100 144 56 64 139 95 51

5.5. Security Goals of the Proposed Method

- *Identification*: Since, in the proposed method the shared session key generated by the both E-Passport and ES shows that both the party obtain the guarantee of other party's identity.
- *Authenticity*: E-Passport and ES are sure about the authenticity of messages received during the conversation with each other, because of same session key derived by the end of the protocol.
- *Privacy*: E-Passport maintain its privacy of data, since, the E-Passport revealed its data only to the authenticated person i.e., ES and not for other malicious intruder.
- *Data Confidentiality*: Data confidentiality is also guaranteed by secure transmission between E-Passport and ES, since the proposed method uses the logarithmic based ECC algorithm.

In the proposed method it is difficult to retrieve the session key, since elliptic curve Diffie-Hellman key agreement protocol uses the discrete logarithm.

5.6. Time Analysis of the Proposed Method

The Table 8 shows the time required for ECC operation.

Table 8. Time required for ECC operation.

S.No	Operation	Proposed time in sec(Tool Used Matlab)
1	ECC Addition	Elapsed time is 0.003532 seconds.
2	ECC Doubling	Elapsed time is 0.004738 seconds.
3	ECC Multiplication	Elapsed time is 0.024762 seconds.

The Table 9 conveys the time required to complete the process at client side and the Table 10 shows the time required to complete process at server side.

Table 9. Session key generation time at client (E-Passport).

S.No	Operation	Elapsed Time (Seconds)
1	Qchip Generation=Nchip*G Here G=(2, 7). (ECC addition, ECC doubling and ECC multiplication)	0.021821
2	Transferring Qchip to Examination system(Client Server interaction in the local host):	0.858294
3	Receiving QIS data from Examination System(Client Server interaction in the local host)	1.558492
4	Shared key Generation by Chip: K=Nchip*QES (ECC addition, ECC doubling and ECC multiplication)	0.004639
5	Decrypt the cipher text from ES using AES algorithm with shared session key	0.004207
6	**Total time taken for entire operation**	**2.447453**

Table 10. Session key generation time at server (ES).

S.No	Operation	Elapsed Time (Seconds)
1	Receiving Qchip data from E-Passport. (Client Server interaction in the local host)	0.537673
2	QES Generation=NES * G Here G=(2, 7) (ECC addition, ECC doubling and ECC multiplication.	0.023149
3	Transferring QES to E-Passport (Client Server interaction in the local host)	0.473696
4	Shared key Generation by Inspection system. K =NES*Qchip.(ECC addition, ECC doubling and ECC multiplication	0.011322
5	Encrypt the information using AES and send to chip. (Client Server interaction in the local host)	0.006515
6	**Total time taken for entire operation**	**1.052355**

When the E-Passport is presented to the visiting country's ES, the total time required to generate session key by the proposed method after the client and server interaction is 2.45 seconds. There will be variation of + or – 10% Elapsed time when each time the software runs. Since, the random number generated for Qchip and Q_{ES} generation will vary each time. So, the number of ECC addition, Doubling and Multiplication time varies.

6. Conclusions and Future work

In the proposed method, cryptographic keys are generated using biometrics and conventional cryptographic algorithms. By using these keys a shared session key is generated between E-Passport and ES. Since, biometric concept is integrated with the conventional cryptography, this method is used to develop a best authentication system. The proposed method satisfies the following security goals like unique identification, Authenticity of the message, data confidentiality by the shared secure of session key, privacy of the E-Passport holder and Integrity of data guaranteed by signatures.

The proposed method can also be used to transmit information securely for real time applications like medical imaging, online-transactions, e-driving license, ATM cards, computer passwords and electronic commerce.

6.1. Future work

- The security of the session key has to be validated using any automatic protocol verification tool like AVISPA.

- Various attacks like man in the middle, unauthorized user attack and replay attack has to be analyzed.
- Possibility of biometric leakage in the E-Passport authentication phase has to be rectified and biometric analysis of the proposed method has to be done.

References

[1] Abid M. and Afifi H., "Secure E-Passport Protocol using Elliptic Curve Diffie-Hellman Key Agreement Protocol," *in Proceedings of the 4th International Conference on Information Assurance and Security*, Naples, Italy, pp. 99-102, 2008.

[2] Baith A., Abdel-Hamid A., and Youssri K., "Implementation of an Improved Secure System Detection for E-passport by using EPC RFID Tags," *International Journal of Computer, Information, Systems and Control Engineering*, vol. 3, no. 12, pp. 66-70, 2009.

[3] Burmester M., Van T., de Medeiros B., and Tsudik G., "Universally Composable RFID Identification and Authentication Protocols," *ACM Transactions on Information and System Security*, vol. 12, no. 4, pp. 1-30, 2009.

[4] Hao F., Anderson R., and Daugman J., "Combining Crypto with Biometrics Effectively," *IEEE Transaction Computers*, vol. 55, no. 9, pp. 1081-1088, 2006.

[5] International Civil Aviation Organization., "Doc9303: Machine Readable Travel Documents," available at: http://www.icao.int/Security/mrtd/Downloads/Technical%20Reports/ICAO_MRTD_History_of_Interoperability.pdf, last visited 2004.

[6] International Civil Aviation Organization., "Doc9303: Machine Readable Travel Documents," available at: www.passport.go.kr/ img/download/vol1.pdf, last visited 2006.

[7] Jain K., Lin H., Pankanti S., and Bolle R., "An Identity Authentication System using Fingerprints," *in Proceedings of the IEEE*, Virginia, USA, pp. 1365-1388, 1997.

[8] Jeng B. and Chen Y., "How to Enhance the Security of E-Passport," *in Proceedings of the 8th International Conference on Machine Learning and Cybernetics*, Baoding, China, pp. 2922-2926, 2009.

[9] Juels A., Molnar D., and Wagner D., "Security and Privacy Issues in E-Passports," *in Proceedings of the 1st International Conference on Security and Privacy for Emerging Areas in Communications Networks*, Washington, USA, pp. 74-88, 2005.

[10] Justice H., "Eu Standard Specifications of Security Features and Biometrics in Passports and Travel Documents," *Technical Report*, European Union, 2006.

[11] KC S. and Karger A., "Security and Privacy Issues in Machine Readable Travel Documents," *in Proceedings of the 10th European Symposium on Research in Computer Security*, Milan, Italy, pp.14-16, 2005.

[12] Khalique A., Singh K., and Sandeep S., "Implementation of Elliptic Curve Digital Signature Algorithm," *the International Journal of Computer Applications*, vol. 2, no. 2, pp. 21-27, 2010.

[13] Meingast M., King J., and Mulligan K., "Embedded RFID and Everyday Things: A Case Study of the Security and Privacy Risks of the U.S. E-Passport," *in Proceedings of the IEEE International Conference on RFID*, Texas, USA, pp. 7-14, 2007.

[14] Najera P., Moyano F., and Lopez J., "Security Mechanisms and Access Control Infrastructure for E-Passports and General Purpose e-Documents," *the Journal of Universal Computer Science*, vol. 15, no. 5, pp. 970-99, 2009.

[15] Nathan T., Meenakumari R., and Usha S., "Formation of Elliptic Curve using Finger Print for Network Security," *International Conference on Process Automation*, *Control and Computing*, Coimbatore, India, pp. 1-5, 2011.

[16] Ne'ma B. and Ali H., "Multi Purpose Code Generation using Fingerprint Images," *the International Arab Journal of Information Technology*, vol. 6, no. 4, pp. 418-423, 2009.

[17] Pasupathinathan V., Pieprzyk J., and Wang H., "An On-Line Secure E-Passport Protocol," *in the Proceedings of the 4th International Conference on Information Security Practice and Experience*, Berlin, German, pp. 14-28, 2008.

[18] Pasupathinathan V., Pieprzyk J., and Wang H., "Security Analysis of Australian and E.U. E-Passport Implementation," *the Journal of Research and Practice in Information Technology*, vol. 40, no. 3, pp. 187-205, 2008.

[19] Vaudenay S., "E-Passport Threats," *Security and Privacy*, *IEEE*, vol. 5, no. 6, pp. 61-64, 2007.

[20] William S., *Cryptography and Network Security*, Prentice-Hall, India, 2007.

Usha Subramaniam presently working as an Assistant Professor (Senior Grade) in Electrical and Electronic Engineering Department, Kongu Engineering College, TamilNadu. She received her BE degree, in electronics and communication engineering in 1992 at Bharathiar University, Coimbatore. ME degree in Power Electronics and Drives in 2008 at Anna University, Chennai. Her area of interest includes network security, mobile Ad-Hoc networks and digital image processing.

Kuppuswami Subbaraya presently working as Professor and Principal in Kongu Engineering College, TamilNadu. He has more than 35 years of experience in technical education in India and Abroad. He received BE degree in ECE in 1975, MSc degree engineering in applied electronics in 1977 and PhD degree in engineering in computer science from University of Rennes I, France in 1986. His primary research interests are software engineering, software architecture, project management and network security. He is a life member of computer society of india and indian society of technical education.