BULGARIAN ACADEMY OF SCIENCES

CYBERNETICS AND INFORMATION TECHNOLOGIES • Volume **18**, No 4
Sofia • 2018 Print ISSN: 1311-9702; Online ISSN: 1314-4081
DOI: 10.2478/cait-2018-0048

A New Enhanced Authentication Mechanism Using Session Key Agreement Protocol

S. Usha[1]*, S. Kuppuswami*[2]*, M. Karthik*[1]

[1]*Department of EEE, Kongu Engineering College, Perundurai - 638 052, Tamil Nadu, India*
[2]*Kongu Engineering College, Perundurai -638 052, Tamil Nadu, India*
E-mails: sushamangal@gmail.com skuppu@gmail.com karthikprm@gmail.com

Abstract**:** *Cryptographic protocols are the backbone of information security. Unfortunately the security of several important components of these protocols can be neglected. This causes violation of personal privacy and threats to democracy. Integration of biometrics with cryptography can overcome this problem. In this paper an enhanced session key agreement protocol which uses the data derived from iris signature is suggested to improve the security of biometric based applications like e-Passport, e-Driving license, etc. The authenticity and security properties of the proposed protocol are analyzed using ProVerif tool and demonstrate it satisfies the intended properties.*

Keywords**:** *Elliptic curve cryptography, e-Passport, examination system, secrecy, authentication, ProVerif.*

1. Introduction

Since 2004, to avoid the intrusion of terrorists via crossing the border, many countries have started issuing e-Passports to the citizens. e-Passport contains RFID tags [1] which are used to store data, process the information on low cost and transmit the information via wireless communication. It also integrates with face biometrics to control user authentication.

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. In the year 2006, Extended Access Control (EAC) [2] mechanism was suggested by the European Union, to eliminate the security problems encountered in the first generation. To enhance the security it promotes additional biometrics like fingerprint and iris. Eavesdropping, cloning of a chip and retrieval of key are the problems encountered in these conventional standards.

In 2008, Pasupathinathan, Pieprzyk and Wang [3] recommended a novel method for Australian e-Passport namely On-line Secure e-Passport Protocol (OSEP). In this method there is a chance of selecting same key values by the two travelers. In 2009, Mohamed Abid and Hossam Afifi [4] suggested a new solution based on elliptic curve Diffie-Hellman agreement protocol. As per the author's idea, an elliptic curve is based on selecting continuous 32 minutiae points from the fingerprint 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 be possible. Hence in the proposed technique to eliminate the above problems a new session key agreement protocol using Elliptic Curve Cryptography (ECC) which uses the data derived from iris signature is suggested. By using the biometric features, the proposed system provides strong user authentication and by using ECC the proposed scheme provides stronger session key agreement function [5].

1.2. Contribution of the paper

Protection of data and network security has been greatly researched. Enhance the security with best performance is mandatory in the case of border control applications like e-Passport. Several exiting protocols have failed to satisfy the security properties and performance accuracy. Hence in the proposed method conventional cryptographic concepts are integrated with biometrics. In the method being proposed, security enhanced mechanism based on variation of Diffie-Hellman key agreement protocol using ECC between e-Passport and the Examination System (ES) was implemented. The elliptic curve parameters A, B and G are derived from iris code. From these parameters public key of e-Passport and session key between e-Passport and ES is generated. The formal security of the proposed protocol was verified using ProVerif tool. This article also demonstrates the efficiency comparison of the proposed protocol based on the parameters like Mutual authentication between client and server, Key agreement, Certificate Comparison, Computational cost and communication cost with other existing protocols. The efficiency comparison shows that the proposed one and Yang & Chang et al. protocol have the same performance metrics. Hence further analysis of proposed one with Yang & Chang et al. was done based on the security properties like Prevention of Guessing attack, Prevention of replay attack, session key security and Forward security. The comparative analysis highlights that the proposed protocol is light weight, robust with efficient and it is perfectly suitable for real-time biometric based authenticated applications.

1.3. Outline of the paper

The remainder of the paper is organized as follows: Section 2 shows the background of the elliptic curve cryptography. In Section 3 the various phases of the proposed protocol is discussed. In Section 4 the intended security properties of proposed protocol is verified using the ProVerif tool. In the same section the efficiency performance and security properties of proposed protocol is compared with the existing one. At the end, Section 5 concludes the paper.

2. Background of elliptic curve cryptography

In this section, the basics of elliptic curves over finite fields and principles of Elliptic curve cryptography is outlined in a few words.

2.1. Elliptic curve group operation over GF(p)

In 1985, N. Koblitz and V. Miller first suggested Elliptic curve cryptography which is based on the algebraic structure of elliptic curves over finite fields [10]. The ECC comes under the category Abelian group [11] and the keys used in ECC are generally logarithmic values, so it cannot be easier to retrieve the key [35]. Hence ECC provides more security than RSA with smaller key size. As the keys size is very small, processing overheads are automatically reduced [12]. The Key size for 160 bit ECC system provides security strength comparable to a 1024 bits RSA cryptosystem [21, 33, 34].

Elliptic curves are not ellipses. Let p be an odd prime, $p > 3$ [12]. The irreducible polynomial for elliptic curve E defined over GF(p) with x_1, y_1, K and $L \in$ GF(p) and $4K_3 + 27L_2 \neq 0$ (mod p) which is given in the next Equation is used in the proposed work:

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

2.2. A variation of Diffiee-Hellman key agreement using elliptic curve

This protocol is a new variant of the Diffie-Hellman protocol using Elliptic Curve Cryptography (ECC). The description of the algorithm is [4]:

- User 1 (U1) and User 2 (U2) select an elliptic curve E defined over GF(p). They choose large prime q such that all points in E(GF(p)) should be divisible by q.
- U1and U2 select a point $G \in E(\text{GF}(p))$ of order q.
- U1 selects a unpredictable integer N_{C} in the interval [1, $n - 1$].
- U2 chooses the integer N_{ES} in [1, $n - 1$].
- U1 computes point $Q_{\text{C}} = N_{\text{C}} * G$ and sends it to U2.
- U2 computes point $Q_{\text{ES}} = N_{\text{ES}} * G$ and sends it to U1.
- U1 now computes a common point $K \in E(\text{GF}(p))$:
- $K = N_{\text{C}} * Q_{\text{ES}}$ and
- U2 now computes a common point $K \in E(\text{GF}(p))$:
- $K = N_{\text{ES}} * Q_{\text{C}}$.
- Then the shared key generated by both the end having equal value is given in the equation
- $K = N_{\text{C}} * Q_{\text{ES}} = N_{\text{C}} * (N_{\text{ES}} * G) = N_{\text{C}} * N_{\text{ES}} * G = N_{\text{ES}} * (N_{\text{C}} * G) = N_{\text{ES}} * Q_{\text{C}}$.

3. Proposed session key agreement protocol

Bio-Cryptography is an upcoming powerful solution which can be integrated with the advantages of conventional cryptography and biometrics [13]. Hence, to improve the security of the proposed session key agreement protocol, the G point derived from the iris biometrics is used in the conventional elliptic curve cryptography [14, 31]. The security of the proposed scheme is based on public key cryptosystem, discrete logarithm and biometrics [15]. In the proposed session key agreement protocol elliptic curve parameters like A, B, and G point are derived from the iris signature of the e-Passport holder. From the derived G point shared secret session key *k* between client and server is generated. Here e-Passport is acting as a client and Examination System (ES) is a server which is available at the airport in the country visited by the e-Passport holder. The proposed method has three phases namely registration phase, session key generation phase and verification phase.

3.1. First phase: Generation of elliptic curve parameters and public key from Iris

At the time of registration to obtain an e-Passport (Smart Card), the user enrols iris in the Data Originator system of their native country. The registration phase from this phase the iris code of the user and elliptic curve parameters are generated from the iris are shown in Fig. 1.

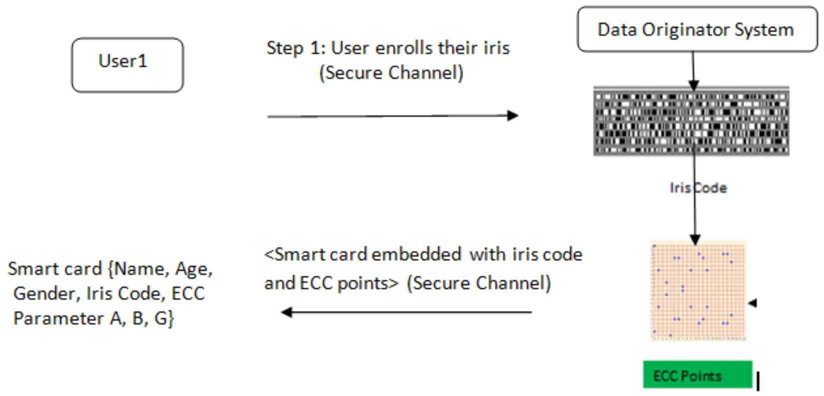

Fig. 1. Registration phase

Step 1. User enrols his/her iris to the Data Originator System (DOS) during the registration phase.

Step 2. From the enrolled iris, 160 unique iris signature is generated by the Daugman recommended method [16], and ECC parameters as explained in Fig. 2.

Step 3. Then the Data originator system stores the value of *A*, *B*, *G* and conventional parameters like age, gender, name, etc., in its database as well as in the Machine Readable Zone (MRZ) of e-Passport (Smart Card).

Step 4. The smart card is then handed over to the user.

The pre-processing stages of iris from which the keys derived by the data originator system is shown in Fig. 2.

The first stage is image acquisition and this is followed by iris segmentation which isolates the iris region in a digital eye image. This process comprises of identifying the inner and outer borders of the iris. In order to balance the differences in the image capturing distances and in the size of the pupil, it is common to change the segmented iris area into a fixed length and dimensionless polar coordinate system. It is usually done using a method proposed by Daugman [16], which is the third stage of the process known as normalization. From the normalized eye image using 1D Gabor filters 9600 bits iris code is extracted. From the 9600 bits of biometric template, 160 unique digest bits are obtained using SHA-1 algorithm, [17, 18, 30] from which ECC parameters *A* and *B* are derived. Then Using ECC algorithm ECC points are generated from which the point *G* is arbitrarily chosen. In the proposed method 600 iris images are taken from MMU1 public database.

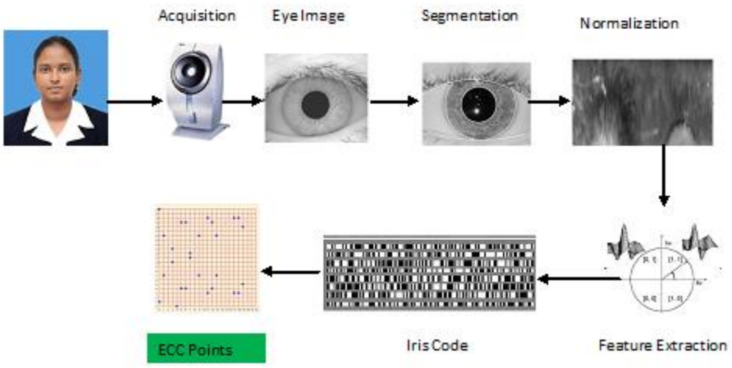

Fig. 2. Stages of iris pre-processing

The results of first phase details are shown in the Table 1. It is realized from the table that the *A*, *B*, *G* and public key value generated for each iris are unique.

Table 1. Cryptographic parameters of various iris images

Image	Hash Value	Template	*A*	*B*	*G*	Public key
1.1	33476c2ea6f8695e7358 96628be7b0cbc4a27be4	001100110100011101101100001011101010011011111100001101001010111100111001101011000100101100110001010001011111001111011000011001011110001001010001001111011111100100	107	47	(56,72)	(54,15)
2.1	449be6735d80f81c5aa11 41a46e4b84a9c64f29c1	01000100100110111111001100111001101011101100000000111111000000111000101101010100001010000001101001000110111001001011100001001010100111000110010011110010100111000001	72	22	(45,59)	(16,93)
3.1	d0191a4f6fad31123dd3 ac45b6fc83cd595b96b6	11010000000110010001101001001111011011111010110100110001000100100011110111010011101011000100010110110110111111001000000111100110101011001010110111001011010110110	75	0	(53,90)	(50,28)
4.1	cb41de20af4e2b90f6a8 f56df19b6979087b5fba	11001011010000011101111000100000101011110100111000101011100100001111011010101000111101010110110111110001100110110110100101111001000010000111101101011111101111010	52	26	(55,23)	(33,40)
5.1	ed25d9dc73c1ece62e035 82c971b711b2bcc58ca	11101101001001011101100111011100011100111100000011110110011100110001011100000000110101100000101100100101110001101101110001000110110010101111001100010110001100101 0	91	42	(59,23)	(99,58)

3.2. Second phase: Shared session key generation

In this phase secured session key between e-Passport and Examination system is generated using ECC. The key is unique for each and every session. So that the intruder cannot easily retrieve the key and the information. The proposed system under consideration consists of two connected components: e-Passport (Chip) and Examination System (ES). e-Passport contains chip ID, elliptic curve parameters like *A*, *B*, *G* point public key and conventional parameters like age, gender, etc. The ES also has its cryptographic key values. The entire operation of the proposed protocol is shown in the Fig. 3 and the notations used in the protocol are described in Table 2.

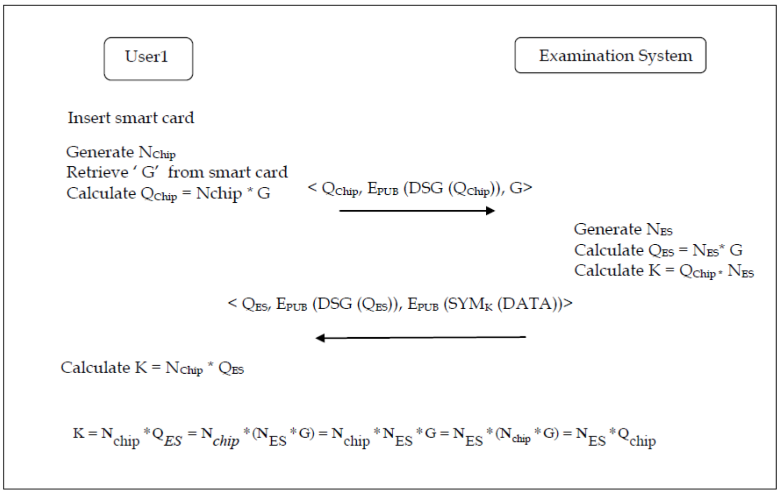

Fig. 3. Proposed key agreement protocol

Table 2. Notations used in the proposed key agreement protocol

Notation	Meaning
N_{chip}	Nonce created by the e-Passport
G	Elliptic curve point generated from biometric templates
E_{pub}	Public Encryption (Uing Receiver Public Key)
DSG	Digital Signature
N_{ES}	Nonce created by the Examination System
K	Created Session Key
SYM	Symmetric Encryption

Step 1. During the visit of e-Passport holder to foreign countries at the airport, for verification purpose e-Passport (Chip or Client) is presented to ES. After reading the MRZ information from e-Passport, ES sends Get challenge message to e-Passport. On receiving it, chip generated a nonce N_{chip} and computes $Q_{chip} = N_{chip} * G$; G is retrieved from e-Passport.

Step 2. Digital signature of Q_{chip} value is calculated. This signature is encrypted using the public key of the Examination system. Then the message $\langle Q_{chip}, G, E_{pub}(DSG(Q_{chip}))\rangle$ values are sent to the Examination system. To prevent man in the middle attack digital signature concept is used in the proposed method.

Step 3. On receiving message 1 from e-Passport, ES generates a nonce N_{ES} and calculates $Q_{ES} = N_{ES}*G$. Then it computes the shared key $K = Q_{chip}*N_{ES}$.

Step 4. Digital signature of Q_{ES} value is calculated. This signature is encrypted using the public key of the Examination system. Then the message $\langle Q_{chip}, E_{pub}(DSG(Q_{chip})), SYM_K(Data)\rangle$ values are sent to the Examination system.

Third part of the message contains data which is to be transmitted from Examination system to e-Passport in a secure way. Before transmission the information is first converted into cipher text using AES algorithm where the key value used is the generated k value. To add more security in the transmission again the information is encrypted using a public key of e-Passport.

Step 5. On receiving the message from the ES, e-Passport calculates the shared secret key K by using the equation $K = Q_{ES}*N_{chip}$ and decrypts the information.

Table 3 shows the results of shared session key generated between client and server for two sessions.

Table 3. Shared session key for two sessions

No	Iris	G	SHARED SESSION KEY (1st TIME)	SHARED SESSION KEY (2nd TIME)
1	Iris1.jpg	(56, 72)	[191 109 108 129 158 201 117 176 67 174197 2 22 124 6121]	[45 185 94 142 26 146 103 183 161 24 133 86 178 1 59 51]
2	Iris2.jpg	(45, 59)	[13 97 248 55 12 173 29 65 47 128 184 77 20 62 18 87]	[241 134 33 119 83 195 123 155 159 149 141 144 98 8 80 110]
3	Iris3.jpg	(53, 90)	[207 205 32 132 149 213 101 239 102 231 223 249 249 135 100 218]	[221 117 54 121 75 99 191 144 236 207 211 127 155 20 125 127]
4	Iris4.jpg	(55, 23)	[132 196 4 115 65 76 175 46 212 167 177 40 62 72 187 244]	[127 197 98 112 231 167 15 168 26 89 53 183 46 172 190 41]
5	Iris5.jpg	(59, 23)	[129 84 23 38 127 118 246 244 96 164 166 31 157 183 95 219]	[210 12 174 195 180 138 30 239 22 76 180 202 129 186 37 135]

It is realized from Table 3, that the session key generated for the two sessions are different and unique for each e-Passport.

4. Validation of session key agreement protocol using ProVerif

ProVerif is an efficient cryptographic protocol verifier based on Pi calculus [6]. This tool is used to verify authenticity and strong secrecy properties of various cryptographic protocols [7]. It can handle an unbounded number of sessions of the protocol. In ProVerif, the adversary has power over the system by vigorously monitoring communication channels and ability to capture, modify, send, or resend messages. ProVerif provides a trace of the intruder's attack if the protocol has a security problem. Figure 4 shows the structure of the ProVerif.

4.1. Structure of the ProVerif

The structure of the ProVerif is shown in Fig. 4.

ProVerif takes as input a model of protocol in the form of Pi calculus plus cryptography along with the security properties the user wants to prove. The tool automatically translates the protocol into horn clauses and security properties [8, 9] to derivable queries on these clauses. Clauses represent the computational abilities of the attacker and the messages of the protocol. ProVerif uses an algorithm based resolution to check the fact whether it is derivable from the horn clauses. Facts represent the initial knowledge possessed by an attacker. If the fact is not derivable this means that there is no attack, otherwise there is a possibility of attack by the adversary. In the proposed method Proverif tool is used for formal modelling, since ProVerif is performed automatically, and the errors can be easily detected [38, 39].

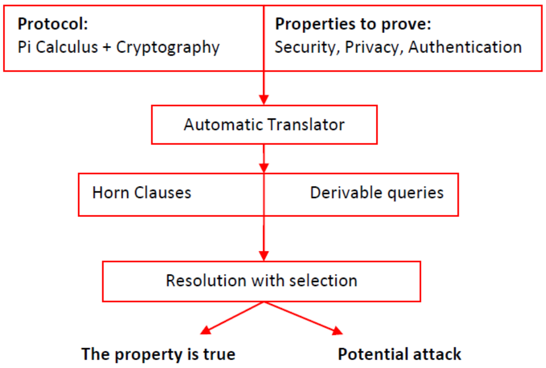

Fig. 4. Structure of ProVerif

4.2. Formal modeling using ProVerif

The proposed protocol is modeled, based on the message sequence shown in Fig. 4 using ProVerif [19, 20, 32]. The ProVerif code consists of signature, equational theory for symmetric encryption, asymmetric encryption, proposed ECC operation, main processes, e-Passport process, and ES processes.

The formal modelling of the proposed protocol was verified using ProVerif .The formal modelling consists of 3 process namely Main Process, e-Passport Process and ES (Examination System process).

4.2.1. Main process

In the main process public key for the e-Passport and ES along with the signed public key for the e-Passport is created and transmitted via the public channel. The processes are modeled that they can run in any order and at any time. The ProVerif code for the main process is:

```
process
   new skchip: sskey; (* new signed private key of a e-Passport*)
   new G: eccpoint
   new ses: skey; (* private key of ES*)
   new schip: skey; (* Private key of e-Passport*)
    let pes = pk (ses) in out(c, pes); (* Public key (pes) of ES*)
    let pchip=pk (schip) in out (c, pchip); (* Public key (pchip) of e-Passport)
    let pkchip = spk (skchip) in out(c, pkchip); (* signed private key of e-Passport*)
    ( (!EchipA(skchip,pkchip,schip,pes)) | (!ESB(pkchip,pchip,ses)) )
    (*multiple sessions of e-Passport and ES*)
```

4.2.2. e-Passport process

In this process nonce N_{chip} is created and Q_{chip} value is computed. Then message 1 $\langle Q_{chip}, G, E_{pub}(\mathrm{DSG}(Q_{chip}))\rangle$ is created and transmitted from e-Passport to ES. The ProVerif code for e-Passport Process is:

```
let EchipA (skchip: sskey, pkchip: spkey, schip: skey, pes: pkey) =
  in(c, x: bitstring); (* Receiving getchallenge message from ES*)
  new nchip: nonce (* generates nonce nchip*)
    let Qchip = emult(nchip,G) in  (*calculates Qchip*)
out(c,(eccpoint_to_bitstring(Qchip),aenc(sign(eccpoint_to_bitstring(Qchip),skchip),pes)));
(* message 1 is transmitted via channel c*)
     event acceptsEchip (sekey);
     in(c, (m: bitstring, n: bitstring));
 (* received QES and secret message encrypted using shared secrecy *)
     let Qes= bitstring_to_eccpoint (n) in
     let (= sekey) = shkey (Qes, nchip) in
 (* computes the same key using the received QES*)
     let (= s) = adec (sdec (m, sekey), schip) in (* decrypts the message m using shared
key*)
     event termEchip (sekey, pkchip).
```

4.2.3. ES processes

In this process nonce N_{ES} is created and Q_{ES} value is computed. Then message 2 $\langle Q_{chip}, E_{pub}(\mathrm{DSG}(Q_{chip})), \mathrm{SYM}_K(\mathrm{Data})\rangle$ is created and transmitted from ES to e-Passport. The ProVerif code for the ES Process is:

```
let ESB (pkchip: spkey, pchip: pkey, ses: skey) =
 new s1: bitstring;
 out(c, s1); (* Get challenge message is transmitted to channel*)
  in(c, (m: bitstring, n: bitstring));
(*received 'Qchip' and signed information*)
   event acceptsES (sekey, pkchip);
    let Qchip = bitstring_to_eccpoint (m) in
    let y = adec (n, ses) in (* Decrypt the information*)
    let (=eccpoint_to_bitstring (Qchip), =pkchip) = checksign(y, pkchip) in
(* check the signature*)
    new nes: nonce; (* creates new nonce nes *)
     let Qes = emult (nes, G) in (* compute Qes*)
     let (= sekey) = shkey (Qchip, nes) in
(* compute shared key *)
     out(c, (aenc ((senc(s, sekey)), pchip), eccpoint_to_bitstring (Qes)));
(* transmit the secret message s and Qes*)
     event termES (sekey).
```

4.3. Result analysis

The security goals like secrecy, authentication and data integrity between e-Passport to ES and ES to e-Passport are analysed using this formal modal. To verify the secrecy of message *s* and shared key *k* the following attacker model is used in the program code.

query attacker(s).

query attacker(sekey).

To verify the authentication between the parties the following CA is used in the program code.

query x: key,y:spkey; event(termEchip(x,y))➔event(acceptsES(x,y)).

query x: key; inj-event (termES(x))➔inj-event(acceptsEchip(x)).

The output of the model is:

-- Query inj-event (termES (x_29)) ➔ inj-event (acceptsEchip (x_29))

Completing…

Starting query inj-event (termES (x_29)) ➔ inj-event (acceptsEchip (x_29))

RESULT inj-event (termES (x_29)) ➔ inj-event (acceptsEchip (x_29)) is true.

-- Query event (termEchip (x_189,y_190)) ➔ event(acceptsES(x_189,y_190))

Completing…

Starting query event (termEchip (x_189,y_190)) ➔ event(acceptsES(x_189,y_190))

RESULT event (termEchip (x_189, y_190)) ➔ event (acceptsES (x_189,y_190)) is true.

-- Query not attacker (sekey [])

Completing…

Starting query not attacker (sekey [])

RESULT not attacker (sekey []) is true.

-- Query not attacker(s[])

Completing…

Starting query not attacker(s[])

RESULT not attacker(s[]) is true.

The above output result conveys the proposed model satisfies the security goals.

4.4. Security goals of the proposed protocol

It is proved from the output results, that the proposed method satisfies the following security goals.

Secrecy: The value *s* is known only by e-Passport and ES.

Authentication of e-Passport to ES: If ES reaches the end of the protocol, it believes that it has shared the secret key *K* with e-Passport and e-Passport was its interlocutor.

Authentication of ES to e-Passport: If e-Passport reaches the end of the protocol with shared secret key *K* it is believed that the key is proposed by ES for use by e-Passport for that session.

4.5. Comparative analysis

To analyse the performance of the proposed protocol the efficiency of the suggested protocol is calculated in terms of Mutual authentication, Key agreement, Computational cost and communication cost. The obtained results are compared with the existing methodologies and the results are projected in the Table 4.

Table 4. Efficiency comparison

Scheme	Properties					
	MA	KA	Cert. Comp.	Pair Comp.	Comp. cost	Comm. cost (Number of Messages)
Tian, Wong and Zhu [22]	Yes	Yes	Yes	No	3PM +1PA+1SKD	4
Wu, Chiu and Chieu [23]	No	No	No	Yes	3PM + 1PA	2
Jia et al. [24]	No	No	Yes	Yes	4PM + 1PA	2
Abichar, Mhamed and Elhassan [25]	Yes	Yes	Yes	No	2PM + 2PA +1MM	3
Yang and Chang [26]	**Yes**	**Yes**	**No**	**No**	**3PM + 2PA**	**2**
Debiao, Chen and Zhang [28]	Yes	Yes	No	No	5PM + 2PA	2
He, J. Chen and Y. Chen [29]	Yes	Yes	No	No	5PM + 3PA	2
Farouk, Fouad and Abdelhafez [27]	Yes	Yes	No	No	3PM + 5PA	2
S. K. Hafizul Islam and Biswas [35]	Yes	Yes	No	No	10PM	2
Reddy at al.[37]	Yes	Yes	No	No	3PM + 13Th	3
Proposed Scheme	**Yes**	**Yes**	**No**	**No**	**3PM + 2PA**	**2 Messages**

From the results in Table 4, it is inferred that the proposed protocol satisfies the following properties like mutual authentication between the two communication parties, supports key agreement protocol, certificate computations are not required. Computational cost and number of communication messages are less when compared to existing schemes except the scheme proposed by Yang & Chang. Henceforth, the security properties of the proposed scheme are compared with Yang & Chang (2009) scheme and the result is listed in the Table 5.

Table 5. Comparison of security properties

Security Property	Yang & Chang	Proposed Scheme
Prevention of Guessing Attack	Yes	Yes
Prevention of Replay attack	Yes	Yes
Mutual Authentication	Yes	Yes
Session Key Security	Yes	Yes
Forward Security	No	Yes

It infers from Table 5, that the proposed scheme provides forward security along with the other security properties listed. Hence the proposed scheme is more secure when compared to YC scheme.

5. Conclusion

In the proposed method ECC parameters *A* and *B* are derived from the Iris Signature. By passing these parameters to the ECC algorithm ECC points are generated. From these points G point is chosen arbitrarily. This G point is used to generate a shared secure key between e-Passport and the ES. Then the formal analysis of key agreement protocol is modeled using automatic protocol verification tool ProVerif. The three security properties of the protocol namely security, authentication between e-Passport to ES and vice versa are encoded in the model. The positive results from the output convey that the intended properties of the protocol hold good. Since the same key is used, privacy of the e-Passport data also hold good. The e-Passport leaked the confidential data only to the ES and not to other adversaries.

References

1. Juels, A., D. Molnar, D. Wagner. Security and Privacy Issues in E-Passports. – IEEE Secure Communication, 2005, pp. 74-88.
2. Justice and Home Affairs. EU Standard Specifications or Security Features and Biometrics in Passports and Travel Documents. Technical Report, European Union, 2006.
3. Pasupathinathan, V., J. Pieprzyk, H. Wang. Security Analysis of Australian and E.U. e-Passport Implementation. – Journal of Research and Practice in Information Technology, Vol. **40**, 2008, No 3, pp. 187-206.
4. Abid, M., H. Afifi. Secure e-Passport Protocol Using Elliptic Curve Diffie-Hellman Key Agreement Protocol. – In: Proc. of IEEE 4th International Conference on Information Assurance and Security, Italy, 2008, pp. 99-102.
5. Yoon, E. J., K. Y. Yoo. Robust Biometrics-Based Multi-Server Authentication with Key Agreement Scheme for Smart Cards on Elliptic Curve Cryptosystem. – The Journal of Supercomputing, Vol. **63**, No 1, pp. 235-255.
6. Dalal, N., J. Shah, K. Hisaria, D. Jinwala. A Comparative Analysis of Tools for Verification of Security Protocols. – International Journal of Communications, Network and System Sciences, Vol. **3**, 2010, pp. 779-787.
7. Al-Hamadi, H., C. Y. Yeun, M. J. Zemerly, M. Al-Qutayri, A. Gawanmeh. Verifying Mutual Authentication for the DLK Protocol Using ProVerif Tool. – International Journal for Information Security Research, Vol. **2**, 2012, No 1, pp. 256-265.
8. Blanchet, B. Automatic Proof of Strong Secrecy for Security Protocols. – In: Proc. of IEEE Symposium on Security and Privacy, 2004, pp. 86-100.
9. Blanchet, B. Proverif: Automatic Cryptographic Protocol Verifier User Manual, 2005.
10. Stallings, W. Cryptography and Network Security. 4th Edition. Prentice-Hall of India Pvt. Ltd, 2007.
11. Yongliang, L., W. Gao, H. Yao, X. Yu. Elliptic Curve Cryptography Based Wireless Authentication Protocol. – International Journal of Network Security, Vol. **5**, 2007, No 3, pp. 327-337.
12. Sui, A., C. Lukas, K. Hui, Y. Yixian, K. P. Chow. Elliptic Curve Cryptography Based Authentication Key Agreement with Pre-Shared Password. – Journal of Electronics (China), Vol. **22**, 2005, No 3, pp. 268-272.
13. Xi, K., T. Ahmad, F. Han, J. Hu. A Fingerprint Based Bio-Cryptographic Security Protocol Designed for Client/Server Authentication in Mobile Computing Environment. – Security and Communication Networks, Vol. **4**, 2011, No 5, pp. 487-499.
14. Kande, S. Generating and Sharing Biometrics Based Session Keys for Secure Cryptographic Applications. – In: International IEEE Conference on Biometrics: Theory, Applications and Systems, USA, 2010, pp. 1-7.
15. Li, C. T., M. S. Hwang. An Online Biometrics-Based Secret Sharing Scheme for Multiparty Cryptosystem Using Smart Cards. – International Journal of Innovative Computing, Information and Control, Vol. **6**, 2010, No 5, pp. 2181-2188.
16. Daugman, J. Biometric Personal Identification System Based on Iris Analysis. U.S. Patent 5291, 560, 1994.

17. U s h a, S., S. K u p p u s w a m i. Secured Session Key Agreement Protocol for Iris Cryptosystem Using Customized Elliptic Curve Cryptography. – International Journal of Security and Its Applications, Vol. **8**, 2014, No 1, pp.147-158.
18. A b i d, M., S. K a n a d e, D. P e t r o v s k a-D e l e c r e t a z, M. D o r i z z i. Iris Based Authentication Mechanism for e-Passports. – In: International Workshop on Security and Communication Networks, Karlstad, 2010, pp. 1-5.
19. Q i X i e, Q., N. D o n g, X. T a n, D. S. W o n g, G. W a n g. Improvement of a Three-Party-Based Key Exchange Protocol with Formal Verification. – Information Technology and Control, Vol. **42**, 2013, No 3, pp. 231-237.
20. S a l a i w a r a k u l, A. Verification of Secure Biometric Authentication Protocols. PhD Thesis, University of Birmingham, United Kingdom, 2010.
21. H a u, Y. W., M. K h a l i l-h a n i, M. N. M a r s o n o. System-Based Hardware/Software Co-Design of Elliptic Curve Cryptography System for Network Mutual Authentication. – Malaysian Journal of Computer Science, Vol. **24**, 2011, No 2, pp. 111-130.
22. T i a n, X., D. S. W o n g, R. W. Z h u. Analysis and Improvement of Authenticated Key Exchange Protocol for Sensor Networks. – IEEE Communications Letters, Vol. **9**, 2005, No 11, pp. 970-972.
23. W u, S. T., J. H. C h i u, B. C. C h i e u. ID-Based Remote Authentication with Smart Cards on Open Distributed System from Elliptic Curve Cryptography. – In: Proc. of IEEE International Conference on Electro Information Technology, 2005.
24. J i a, Z., Y. Z h a n g, H. S h a o, Y. L i n, J. W a n g. A Remote User Authentication Scheme Using Bilinear Pairings and ECC. – In: Proc. of 6th International Conference on Intelligent System Design and Applications, 2006, pp. 1091-1094.
25. A b i c h a r, P. E., A. M h a m e d, B. E l h a s s a n. A Fast and Secure Elliptic Curve Based Authenticated Key Agreement Protocol for Low Power Mobile Communications. – In: Proc. of International Conference on Next Generation Mobile Applications, Services and Technologies, 2007, pp. 235-240.
26. Y a n g, J. H., C. C. C h a n g. An ID-Based Remote Mutual Authentication with Key Agreement Scheme for Mobile Devices on Elliptic Curve Cryptosystem. – Computers and Security, Vol. **28**, 2009, No 3, pp. 138-143.
27. F a r o u k, A., M. M. F o u a d, A. A. A b d e l h a f e z. Analysis and Improvement of Pairing-Free Certificate-Less Two-Party Autheticated Key Agreement Protocol for Grid Computing. – International Journal of Security, Privacy and Trust Management, Vol. **3**, 2014, No 1, pp. 23-36.
28. C h e n, D. J., R. Z h a n g. A More Secure Authentication Scheme for Telecare Medicine Information Systems. – Journal of Medical Systems, Vol. **36**, 2012, No 3, pp. 1989-1995.
29. H e, D., J. C h e n, Y. C h e n. A Secure Mutual Authentication Scheme for Session Initiation Protocol Using Elliptic Curve Cryptography. – Security and Communication Networks, Vol. **5**, 2012, No 12, pp. 1423-1429.
30. V e r m a, M., R. R a n i. Significant Secret Image Sharing Based on Boolean Operation. – Cybernetics and Information Technologies, Vol. **17**, 2017, No 2, pp. 134-150.
31. R e d d y, A. G., E.-J. Y o o n, A. K. D a s, V. O d e l u, K.-Y. Y o o. Design of Mutually Authenticated Key Agreement Protocol Resistant to Impression Attacks for Multi-Server Environment. – IEEE Access, Vol. **5**, 2017, pp. 3622-3639.
32. L i u, W., Q. X i e, S. W a n g, B. H u. An Improved Authenticated Key Agreement Protocol for Telecare Medicine Information System. – Springer Plus, Vol. **5**, 2016, 2012, pp. 2-16.
33. Q i u, S., G. X u, H. A h m a d, Y. G u o. An Enhanced Password Authentication Scheme for Session Initiation Protocol with Perfect Forward Secrecy. – PLoS ONE, Vol. **13**, 2018, No 3.
34. Y o o n, E.-J., K. D. A s h o k, K.-Y. Y o o, R. A l a v a l a p a t i. Lightweight Authentication with Key-Agreement Protocol for Mobile Network Environment Using Smart Cards. – IET Information Security, 2016, 10. 10.1049/iet-ifs.2015.0390.
35. H a f i z u l-I s l a m, S. K., G. P. B i s w a s. Apairing- Free Identity-Based Two-Party Authenticated Key Agreement Protocol for Secure and Efficient Communication. – Journal of King Saud University – Computer and Information Sciences, Vol. **29**, 2017, pp. 63-73.

36. L u, Y., L. L i, X. Y a n g, Y. Y a n g. Robust Biometrics Based Authentication and Key Agreement Scheme for Multi-Server Environments Using Smart Cards. – PLoS ONE, Vol. **10**, 2015, No 5, e0126323. pmid:25978373.
37. R e d d y, A. G., A. K. D a s, V. O d e l u, K.-Y. Y o o. An Enhanced Biometric Based Authentication with Key-Agreement Protocol for Multi-Server Architecture Based on Elliptic Curve Cryptography. 2016.
38. L i u, W., Q. X i e, S. W a n g, B. H u. An Improved Authenticated Key Agreement Protocol for Telecare Medicine Information System. – Springer Plus, 2016.
39. X i e, Q., Z. T a n g. Biometric Based Authentication Scheme for Session Initiation Protocol. – Springer Plus, 2016.
40. U s h a, K. S. A Biometric Based Session Key Agreement Using Modified Elliptic Curve Cryptography. – The International Arab Journal of Information Technology, Vol. **12**, 2015, No 2, pp. 155-162.

Received 09.05.2018; Second Version 21.08.2018; Accepted 17.09.2018