OPEN ACCESS Freely available online

Journal of Information Technology & Software Engineering

Research Article

Legal Challenges in E-passport and Solution by BIO-PUF Function

Sivasankari Narasimhan*

Department of Electronics and Communication, Mepco Schlenk Engineering College, Anna University, India

ABSTRACT

Today many countries are utilizing electronic passports. In that authentication and confidentiality is very much essential. In the late 1990s, biometrics-based templates come as an authentication tool. Many biometric-based authentication protocols and RFID based authentication techniques have been suggested for authenticity and confidentiality. In this paper, the authentication protocol is developed with biometrics and Physical Unclonable Function (PUF). The concept of Bio-PUF is introduced, to combine the biometric concept with an unclonable response from PUF has been arrived for authentication. The protocol uses simple cryptographic operations, a strong PUF circuit, and any biometrics to create a more secure Bio-PUF based E-passport authentication protocol. This will provide more reliable security.

Keywords: E-passport; Physically Unclonable Functions; Bio-PUF, Biometric template; Machine Readable Zone

INTRODUCTION

The passport authentication process is done for two things: First, the checking officials confirm that the passport holder is indeed the same person named on the passport with the corresponding ticket. Second, they confirm with the help of their computerized system that no forgeries are filed against the person. The second confirmation is needed for that person to enter into the destination country, or to make transit, their airline will have to pay to the home country. They try to avoid that expense by checking the correct status. In US airports, double passport checking has been done, because there is a possibility for forging a web check-in style boarding pass easily, so boarding pass is again scanned and checked to ensure the correct personality. The International Civil Aviation Organization standards (ICAO) specify face recognition as the checking biometric for identity verification in travel documents. So E-passports comprise of the digitized photographic face image of chip holder. The standard additionally specifies fingerprints and iris data as optional biometrics. In Malaysia, fingerprint information is verified. The countries US, Germany, Netherlands verify the face image. In our paper instead of taking additional biometrics, the chip to be located in a passport has to be made unique. With the government's approval, the interconnection between chip and other verifying factors has to be designed.

Originally E-passport records can be categorized into three areas VISA records, travel records, and biometric records which are described in ICAO standards [1]. In VISA records the basic information such as Issuing state, Document type, passport number, Sex, Date of birth and Nationality, and Number of entries are recorded. In travel records, Visa approvals, refusals, revocations, travel date, Inspection authority details, Mode of travel, duration of stay, are documented. For authentication, the sensitive biometric information such as iris, fingerprint, and face details are added. For accessing and authenticating one person some protocols are utilized. For checking authenticity and integrity, passive authentication is used. For avoiding cloning attacks, active and chip authentication protocols were developed. The details present in the E-passport chip are given in (Table 1).

Where DG refers to data groups. The main thing in E-passport is Machine Readable Zone (MRZ). The Machine Readable Zone numbers are allotted based on passport numbers which are issued in sequence, mainly by expiry and birth dates. Hence the number contains low entropy which can easily be attacked by intruders. Normal ISO 14443 tags sent a fixed (Unique Identification)UID as part of the anti-collision protocol (Followed in Italy) For MRZ, by allotting random number as its ID may be a solution while the problem is seeing at the lower level. But this is not. The sequence ID is assigned to track them individually for organizational convenience. But allotting a random ID may create organizationally and some hardware problems, that leads to some special nonlinear hardware also. Hence there should be methods to introduce randomness within the key derived from MRZ.

Correspondence to: Sivasankari Narasimhan, Department of Electronics and Communication Engineering, Mepco Schlenk Engineering College, Anna University, India. E-mail: sivani.sivasankari@gmail.com

Received: January 20, 2021, **Accepted:** February 04, 2021, **Published:** February 11, 2021

Citation: Narasimhan S (2021) Legal Challenges in E-passport and solution by BIO-PUF Function. J Inform Tech Softw Eng.11:250.

Table 1: E-Passport Structure Information

Data group #	Field information
DG1	MRZ
DG2	Encoded Face
DG3	Encoded Fingers
DG4	Encoded Irises
DG5	Displayed portrait
DG6	Future use
DG7	Displayed Signature
DG8	Data features
DG9	Structure features
DG10	Substance features
DG11	Additional Personal details
DG12	Additional document details
DG13	Optional details
DG14	Security Options for secondary biometrics
DG15	Active authentication public key
DG16	Persons to notify

MATERIALS AND METHODS

Preliminaries on E-passport authentication schemes

Passive Authentication (PA): The inspection system validates the contents in the E-passport chip. First, it verifies the DG 15 field which is the public key of the passport holder, and then it authenticates the hash function in each field. From a general point of view, passive authentication verifies all the data present in the E-passport without asking for any cryptographical computations. The main weakness in this kind of authentication is that the attacker can steal these data from the targeted user and he can impersonate him.

Active Authentication (AA): Here cryptographic computations are done based on asymmetric cryptosystem explained in [2]. E-Passport has to create the private and public key pair (Kpr, Kpu) which is unique for every E-Passport. The private key (Kpr) is stored in a secure chip. Sometimes it can be generated outside with the help of any crypto processor or inside the chip itself. Normally the cryptographic key pair is created inside the passport chip. The accuracy of the DG15 key (Kpu) is verified by some signature verification procedure and particular Challenge-Response communication between the verifying terminal and E-Passport. The communication will pass only if the respective private key is authentic. This authentication is useful to find any chip cloning. This method also failed if both public key and private key are changed.

Chip Authentication (CA): Since 2006, CA is adopted by the European Union in second-generation E-Passports with the Basic Access Control (BAC) method. In BAC all messages exchanged between the IS and ePassport are encrypted with symmetric cryptosystem. To avoid side-channel attacks from passport RFID chip, encryption has been performed. This method provides good authentication combined with passive authentication. But CA requires high-end processors with the capability of doing Diffie-Hellman key exchange. For performing this, Diffie-Hellman key exchange Standard interfaces are needed which is available only in Java Card 2.2.x.

Terminal Authentication (TA): In the second generation, the question of terminal rights has arrived. Information theft at terminals gave rise to restrictions to access biometrics information. This method is used with Extended Access Control (EAC). In EAC, the holder's biometrics is concealed to the terminals that have no right to read the information. To access the biometric information, terminal authentication by passport chip has been done. Challenge-Response communication between the terminal and passport chip takes place. The verification device has to send the document number, challenge, and hash of the session-unique data and signs it with its private key. RSA or ECDSA algorithm can be used for signing and verifying action between them which involves the private key of them. Without directly sending private keys, some computations help them to verify the results. EAC presents access rights to verification terminals permitting only authorized terminals to read or change certain data.

Basic Access Control (BAC): This kind of authentication shields against reading the passport without the holder's interest. Without BAC the E-Passport contents may be 'skimmed'. In BAC, Machine Readable Zone (MRZ) is the main thing for giving keys to the encryption and Message Authentication Code (MAC) modules procedures given in [3]. After deriving the keys, how the BAC authentication procedure is performed as given in (Table 2).

RFID Reader	MRZ
	$RN_{MRZ} \in_R \{0,1\}^{64}$
$\xleftarrow{RN_{MRZ}}$	
$RN_{RD} \in_R \{0,1\}^{64}$; $K_{RD} \in_R \{0,1\}^{128}$ Initial number$_{RD} = RN_{RD} \| RN_{MRZ} \| K_{RD}$ $E_{RD} = E_{ENC}$(Initial number$_{RD}$) $M_{RD} = EMAC_{MAC}(E_{RD})$	
$\xrightarrow{E_{RD}, M_{RD}}$	
	Decrypt and verify E_{RD}, M_{RD} $K_{MRZ} \in_R \{0,1\}^{128}$ Initial number$_{MRZ} = RN_{MRZ} \| RN_{RD} \| K_{MRZ}$ $E_{MRZ} = E_{ENC}$(InitialNumber$_{MRZ}$) $M_{MRZ} = EMAC_{MAC}(E_{MRZ})$ $KS_{seed} = K_{RD} \oplus K_{MRZ}$
$\xleftarrow{E_{MRZ}, M_{MRZ}}$	
Decrypt and verify E_{MRZ}, M_{MRZ} $KS_{seed} = K_{RD} \oplus K_{MRZ}$	

The forward and reverse channel communications occurred between RFID reader (verifier) to E-passport and E-passport to verifier respectively. With just simple XOR operation and MRZ information, an antenna can capture the forward channel communication. This is feasible within 25 Kms. The encryption used here is Triple DES. Crypt analysis with this algorithm is very easy nowadays.

Extended Access Control (EAC): Always authentication is done when the information stored in the target of evaluation is verified in the illicit chip of passport, that it can produce the same with the stored information. Forgery may be detected employing comparative verification of the facial image with the passport. However, it is difficult to surely detect a forged passport just by discriminating against the facial image. Certainly, there must be problems with Basic Access Control: These are the common problems that exist in all countries. An E-Passport equipped with EAC protects the additional biometric data using encryption. Each E-Passport will have unique keys to protect access to sensitive information.

RELATED WORKS

The authors of narrate about the E-passport structure as per the ICAO standard and security mechanisms [4-9]. Juels et.al explains about the standards that should be followed by ICAO and the various attacks on passports, they also explained about the mandatory passive authentication schemes and optional Basic Access Control and extended access control schemes [4]. BAC is an authentication procedure to ensure confidentiality feature, AA is used to avoid anti-cloning feature. It utilizes public key cryptography features. For active authentication, public-key encryption techniques such as RSA, Rabin Williams's signature, and Diffie Hellman are used for signing as per the ISO-9796-2 scheme. As a whole, the authors suggest the methods which are compatible with ICAO. Ingo Liersch also explained the protocols and possible threats on the E-passport [5,6]. The authors of Luca Calderoni suggests that active authentication will avoid chip cloning attack, but this authentication can't identify the cloning attack [9]. The concepts in are modified with PUF concepts which should be deployed inside the information-bearing chip [5]. Anshuman Sinha et.al explained different authentication methodologies for every generation [7].

Various protocols have been developed for avoiding the information hacking from E-Passport. One such scheme in Identity based cryptography explained by Li et al [10]. Karger et.al described some attacks named "splicing" "fake finger" attacks, followed by facial recognition threats by M [11]. Kosmerlj et al in [12]. Hoepman et al. discuss stolen terminals and one solves this problem by online authentication [13]. Hancke et.al intimated the possibility of data changes by an attacker in RFID communication between the reader and tag [14]. This introduces a threat to the RFID reader in E-passport also. Liu et al. explains the threat to the E-Passport with cracking machines [15].

As many countries have used different norms for providing traveling documents and issuing authorities, the authors of claim that the documents should be private to the individuals and promoted in cross-border cooperation and easy collaboration with international agreements [16]. At present, face, fingerprint, and iris biometrics are used for the identification system, just they are utilizing the images present in E-passport as physical verification.

The above-mentioned protocols are utilizing RFID tags and biometrics characteristics as the security tool keys. Now it is focussed on the problem of fake biometrics and the associated chips, (i.e) the chip is replaced by some other chip, and the cardholder image also changed. Hence there is a possibility for wrong person authentication as an accepted one. To solve this problem, the chip carried by the passport should be designed in a unique way to authenticate persons effectively by the person's chip. Even though the hackers are trying to change the chip the responses from the fake chip exhibit it to the verifiers.

The technique is named as the Physical Unclonable Function (PUF). The manufacturing variations in the chip lead to drastic functional variation in the chips. The same components or the same circuit can't able to produce the same results. This property is used as a physical unclonable function which will be more effective for authentication. Many PUF proposals for authentication of digital rights management and proprietary software also developed in the last decade. Now, this proposal is extended for E-passport biometric authentication. In our work, the PUF based protocols have been developed in every authentication procedure of E-Passport. This paper contributes to the following points:

- A new Bio-PUF passport authentication scheme for basic access and extended access control methods and also a generic construction method to create the one way MAC codes from the PUF.
- The mathematical proof and correctness of the protocols have been discussed.

PROPOSED APPROACH

Normally Inspection systems (IS) are issuing and verifying the truthfulness of passports. This working procedure is shown in Figure 1, Inspection systems have to get approval from the Document Verifier (DV) which priorly gets permission from the Country Verifying Signing Authorities (CVSA). CVCA issues the certificate to the DV and DV approves IS. Each IS has to approve E-Passport. The process of registration of E-passport utilizes the PUF circuit to obtain the response for the specified challenge from IS and face image. Conventional registration and authentication steps are followed in our protocol also. The Challenge-Response behaviour from each passport should be stored in IS and for each location, it can be transferred as per request. Further to avoid a dictionary attack, some primitive cryptographic operations have to

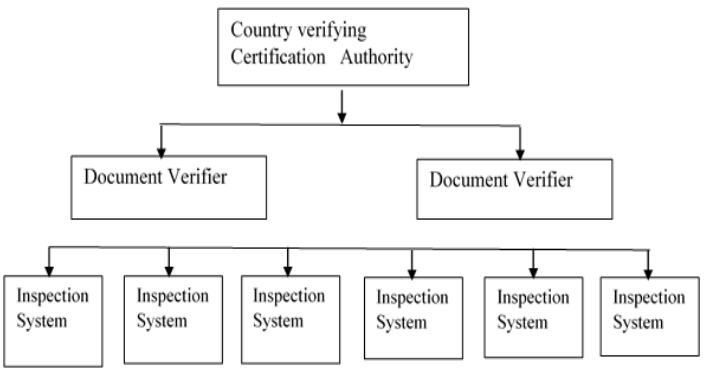

Figure 1: Authentication hierarchy.

be performed. The proposed PUF scheme enables the IS chip to verify the chip holder's authenticity.

Here it is assumed that all the passports are carrying the PUF chip and associated cryptographic module for its identity. (i.e) all the passport holders can be authenticated through this PUF protocol only after performing certain operations correctly. As per [17] generally, PUF has to possess some characteristics which are given below:

Easy to evaluate: For the given PUF chip and challenge (x), it is easy to evaluate the response $y = PUF(x)$

- **Unique:** $PUF(x)$ is the response that possesses some information about the identity of the physical entity embedding that PUF. This response can't be produced by any other physical entity.
- **Reproducible:** $y = PUF(x)$ is reproducible in the certain periods up to a small error.
- **Unclonable:** For a given PUF_1, it is hard to construct the same chip $(PUF_1 \neq PUF_2)$ and for all challenge set $\forall x \in C; PUF_1(x) \neq PUF_2(x)$
- **Unpredictable:** It is hard to predict $y_c = PUF(x_c)$ up to a small error, for x_c a random challenge such that $x_c \notin Q$ where Q is different challenge set.
- **One-way:** With only y and the corresponding PUF instance, it is hard to find the challenge (x) $PUF^{-1}(y) = x$
- Various categories and different PUF circuits are available any of the PUF circuit can be used without affecting passport's performance.

Chip authentication using PUF

To authenticate the chip and prove that the chip is genuine. Only a genuine chip can implement all communications and cryptographic procedures correctly. Each issuing country has a Unique Country Signing (CS) as a Trusted Authority. The CS sets up the PUF Challenge-Response storage database for every IS and passport. As well as the common cryptographic parameters for assisting the PUF based authentication procedure. To the Document Signer (DS) and IS. Each DS and each IS takes his unique Ocial Name as its identity (denoted by ID Issuer and ID_IS respectively).

System setup

CS has to possess a challenge $(C \in NC > 2)$, Through IS and DS the response behaviour of the PUF chip has to be collected and stored in the database of CS. For further cryptographic checking, triple-DES keys has been created. Information provided by Inspection System (IS) is given in (Table 3). Now let us see the Authentication protocols with PUF.

Basic access control

The passport contains seed data from MRZ_{Data}, The encryption and MAC keys are derived from unique PUF instance of the E-Passport chip and personal data stored in MRZ. The random number keys are encrypted using 3DES in block-cipher mode. The response from the PUF circuit is 160 bits. The diagrammatic view of BAC is shown in (Figure 2).

Table 3: Information in a certificate issued by IS.

Basic Information	Issuing Information Identity (IS-ID)
	Issuing country
	Expiration Date EXP
	Chip public parameters $< g, C_{pub} >$
Confidential Information	$< C, R, K_{IP} >$

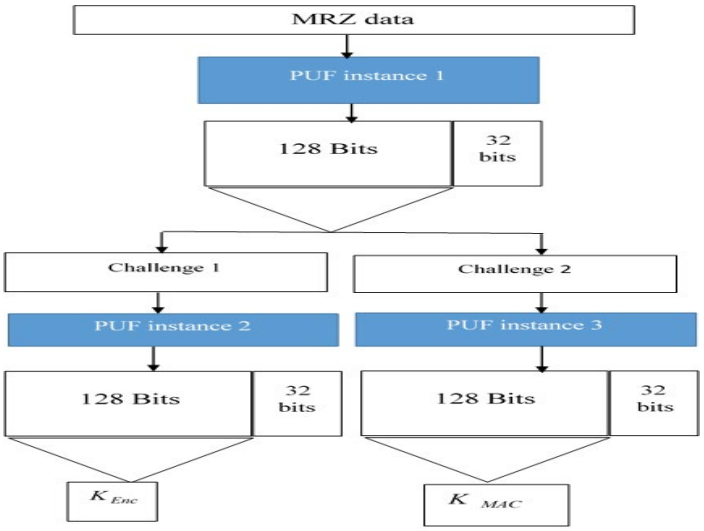

Figure 2: Basic access control keys derivation from PUF.

1. MRZ data is used as a challenge for the first PUF.

$$PUF_1(MRZ_{data}) \rightarrow \begin{bmatrix} Challenge_1 \\ Challenge_2 \end{bmatrix}$$

2. Next, the MAC and encryption keys are formed from challenges

$$\begin{bmatrix} Challenge_1 \\ Challenge_2 \end{bmatrix} \rightarrow \begin{bmatrix} PUF_2 \\ PUF_3 \end{bmatrix} \rightarrow \begin{bmatrix} K_{ENC} \\ K_{MAC} \end{bmatrix}$$

3. The first 56 bits of K_{ENC} constitute Ka, and the checksum is calculated using the DES algorithm. The computed checksum is appended to the key to make it 64 bits long.

$$K_{enc}(I.half) \rightarrow K_a$$

4. $K_{enc}(II.half) \rightarrow K_b$

5. The next 56 bits of K_{ENC}, and the checksum is calculated using the DES algorithm. The computed checksum is appended to the key to make it 64 bits long.

$$K_{enc}(I\ .half) \rightarrow K_b$$

The keys K_a and K_b are stored in IS center.

Key exchange protocol

The message sequence for challenge–response is summarized below. The nonce is eight bytes or 64 bits long.

1. The verification device generates a random number R_{IS} and encrypts with the triple-DES keys generated.

$$M_{vp} = 3DES(K_{ab}(R_{IS}))$$

2. The passport decrypts it and verifies if the random number matches. R_{IS} encrypts with the triple-DES keys generated.

$$R_{IS} = 3DES^{-1}(K_{ab}(R_{IS}))$$

3. Passport generates a random number Rp encrypts with the triple-DES keys.

$$M_{pv} = 3DES(K_{ab}(R_p))$$

4. The verification device decrypts the challenge and verifies if the random number matches. Rp encrypts with the triple-DES keys generated.

$$R_v = 3DES^{-1}(K_{ab}(R_p))$$

Extended access control

The passport contains seed data from Face biometrics and MRZ_{Data}, The encryption keys are derived from biometrics and personal data stored in MRZ. The challenge-response messaging occurs to verify the passport as per ISO 11770-2 using 3DES in block-cipher mode. Now the extended access control with biometric has been modified with PUF response which is shown in Figure 3,Challenges for PUF and Biometric data and MRZ data is diversified using data stored in the MRZ.

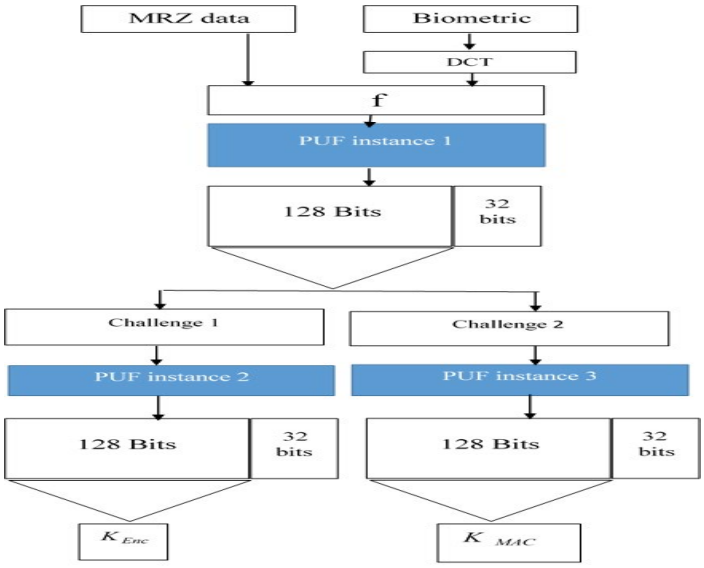

Figure 3: Extended access control key derivation.

$$f\begin{pmatrix} DCT(BT) \\ MRZ_{data} \end{pmatrix} \rightarrow challenge_1$$

1. Next, the diversified $challenge_1$ is formed from biometric data

$$f(MRZ_{data}, DCT(BT) \rightarrow challenge_1$$

2. The PUF response is used for creating two challenges.

$$PUF_1(challenge_1) \rightarrow \begin{bmatrix} Challenge_1 \\ Challenge_2 \end{bmatrix}$$

3.The MAC and encryption keys are formed from challenges

$$\begin{bmatrix} Challenge_1 \\ Challenge_2 \end{bmatrix} \rightarrow \begin{bmatrix} PUF_2 \\ PUF_3 \end{bmatrix} \rightarrow \begin{bmatrix} K_{ENC} \\ K_{MAC} \end{bmatrix}$$

4. The first 56 bits of P constitute Ka, and the checksum is calculated using the DES algorithm. The computed checksum is appended to the key to make it 64 bits long.

$$K_{enc}(I.half) \rightarrow K_a$$

5. The next 56 bits K_b, and the checksum is calculated using the DES algorithm. The computed checksum is appended to the key to make it 64 bits long.

$$K_{enc}(I\ .half) \rightarrow K_b$$

The keys K_a and K_b are stored in IS center.

Key exchange protocols are processed as per the procedure described in above section.

Comparison with different authentication mechanism with the technique proposed and our method is given in [11] (Table 4).

Table 4: Comparison with various EAC works.

Scheme	Carrier of authorization	Authorization mechanism	Authentication algorithm
Singapore EAC	DG13 on e-passport chip	Encryption on the EAC-KEY	Symmetric cryptographic algorithm (3DES)
EU-EAC	CA certificate	Indirectly authorization: the certificate chain	Asymmetric cryptographic algorithm (RSA)
IBC-EAC [12]	ID-Cert on Authorized Smartcard Directly Authorization (ID-Cert)	Direct authorization	Identity-Based Authentication protocol
Proposed Bio-PUF	MRZ+ Any of Biometrics (DG1+DG2/DG3/DG4)	Physical Unclonable function within the chip itself	Symmetric cryptographic algorithm (3DES)

DISCUSSIONS ON PASSPORT ATTACKS

A German security researcher Lukas Grunwald, RFID researcher also, demonstrated that he could clone the computer chip in an electronic passport. The fingerprint image stored in a passport and JPEG followed facial image can be replaced by some specially coded chip. The specially created chip can scratch the passport readers also. Our work is focussed that even the chip is cloned it should be detectable and misidentification of a person has to be avoided.

Algorithm based-brute force attack

The key agreement algorithms used in key exchange protocols are 3DES. As per ICAO standard, maximum it occupies 112 bits for E-passport. Hence there are just 2112 times only the attacker makes a trial and error. When the intruder knows some of n (plaintext, ciphertext) pairs, a basic result from probability theory says that almost at $\left(\frac{2^{112}+1}{n+1} \approx \frac{2^{112}}{n}\right)\frac{2^{112}}{n}$ the level he may find the correct private key of the passport holder. Now it has been combined with the PUF response circuit. The response behaviour of the PUF circuit is unknown. Hence it increases the complexity for the attacker.

Invasive attacks

Reverse engineering from the response also possible with the normal E-Passports. But in case of the PUF based E-passports, even the hackers try to do reverse engineering, due to variations in manufacturing effect it will indicate to the concerned authorities.

Information leaking attacks

Hackers can try for side-channel analysis such as power and electromagnetic analysis also possible with this E-passport threat. But all of the threats go as waste for the hacker due to the unclonable property of PUF. As per [18] minimum CRPs required for the attacker to correctly predict the response, CRP_{min} are given by

$$CRP_{\min} = \frac{k(k-1)(1-2\varepsilon)}{2+\varepsilon(k-1)} \approx \frac{k^2}{2}$$

A PUF circuit with 95% accuracy, has a minimum error rate of ε =5%. The minimum $CRP_{\min}$ required for fuzzy modelling of PUF is of the order of $\frac{k^2}{2}$. $CRP_{\min}$ can be increased by increasing the PUF size.

CONCLUSION

In this paper, PUF based protocols for Basic Access Control keys derivation and Extended Access Control keys derivation has been presented for the E-passport issuing schemes. This will be compatible as per ICAO standards. It also provides two main enhanced security features: a more trustable and unclonable authorization mechanism and a better terminal verification solution with biometrics. The main flaw of PUF based protocols is, the PUF circuits are not able to withstand their outputs for a long duration. Anyway, the method of unpredictability provides a better solution for authentication problems in association with biometrics.

REFERENCES

1. International Civil Aviation Organization (ICAO). Uniting aviation.
2. Stallings W. Cryptography and network security principles and practice 4th edition. Prentice Hall. India. 2005;1-592.
3. Liu Y, Kasper T, Lemke-Rust K, Paar C. E-passport: Cracking basic access control keys with COPACOBANA. SHARCS.2007.
4. Juels A, Molnar D, Wagner D. Security and privacy issues in e-passports. IEEE. 2005;1:74-88.
5. Liersch I. Electronic passports – from secure specifications to secure implementations. Inf Secur Tech Rep. 2009;4(2):96-100.
6. Calderoni L, Maio D. Cloning and tampering threats in e-passports. Expert Syst Appl. 2014;41(11):5066-5070.
7. Anshuman Sinha. A Survey of System Security in Contactless Electronic Passports. Int j crit infr prot. 2010;4(4): 154-164.
8. Li CH, Zhang XF, Jin H, Xiang W. E-passport EAC scheme based on Identity-Based Cryptography. Inf Process Lett. 2010;111(1):26-30.
9. Ranan A, Sportiello L. Implementation of security and privacy in e-Passports and the extended access control infrastructure. Int J Crit Infr Prot. 2014;7(4):233-243.
10. Gaurav SKC, Karger PA. Preventing attacks on machine readable travel documents (MRTDs). Cryptology Eprint Archive. 2005.
11. Kosmerlj M, Fladsrud T, Hjelmas E, Snekkenes E. Face recognition issues in a border control environment. In Advances in Biometrics. 2006;3832:33-39.
12. Hoepman JH, Hubbers E, Jacobs B, Oostdijk M, Schreur RW. Crossing borders: security and privacy issues of the european e-passport. In: Yoshiura H, Sakurai K, Rannenberg K, Murayama Y, Kawamura S. Advances in information and computer security. Lecture Notes in Computer Science. Berlin, Heidelberg. 2006;152-167.
13. Hancke GP. Practical attacks on proximity identification systems. IEEE Symposium on Security and Privacy. 2006;328-333.
14. Carluccio D, Lemke-Rust K, Paar C, Sadeghi AR. E-Passport: The global traceability or how to feel like a ups package. In: Lee J.K, Yi O, Yung M. Information security applications. Lecture Notes in Computer Science. Berlin. Heidelberg. 2007;391-404.
15. Liu Y, Kasper T, Lemke-Rust K, Paar C. E-Passport: Cracking basic access control keys. In: Meersman R, Tari Z. On the move to meaningful internet systems 2007: CoopIS, DOA, ODBASE, GADA, and IS. Lecture Notes in Computer Science. Berlin, Heidelberg. 2007;1531-1547.
16. Rodriguez VD. Legal challenges of biometric immigration control systems. Journal of Mexican Law. 2014;7(1):3-30.
17. Suh GE, Devadas S. Physical unclonable functions for device authentication and secret key generation. Annual Design Automation Conference. 2007;9-14.
18. Ruhrmair U, Sehnke F, Solter J, Dror G, Devadas S, Schmidhuber J. Modeling attacks on physical unclonable functions. ACM Conference on Computer and Communications Security. 2010;237-249.