International Conference on "Latest Innovations in Engineering, Management, Social Science and Education"
The International Centre Goa, Panjim, Goa (India)
28th October 2018 www.conferenceworld.in ISBN:978-93-87793-54-5

Biometric key generation for Elliptic Curve Cryptography

Ms. Yogita S. Pagar
Research Scholar[CSE]
Swami Ramanand Teerth Marathwada University,Nanded

Dr. G.V. Chowdhary
Director & Professor
School of Computational Sciences
Swami Ramanand Teerth Marathwada University, Nanded (M.S.) 431606

Abstract:
For Human users it is very difficult to remember long cryptographic keys. Therefore, many scientists are trying to use biometric features of the user instead of memorable password to produce hard and unrepeatable cryptographic keys and to construct the key unpredictable to a hacker who is deficient of important knowledge about the user's biometrics. In this paper, generating the strong bio-crypt key based on fingerprint minutiae is presented. At first, the minutiae points are extracted from the fingerprint image based on image processing algorithms. Then, the extracted fingerprint minutiae are used for generating a private key. From those minutiae, elliptic curve is generated by using elliptic curve cryptography generation algorithm. Thus, elliptic curve based on biometric data to validate the identity of the user was created. We have implemented by considering three fingers of a particular person to improve a security. This analysis confirms that our solution corresponds to the security goals defined in the paper.

Keywords: *Elliptic Curve, Finger Print, Minutiae, Elliptic Curve Cryptography, Public Key Infrastructure, Biometric Security*

I. INTRODUCTION

Cryptography is the study of hiding information. Modern cryptography intersects the disciplines of computer science, mathematics and engineering. Numerous Applications of cryptography include ATM cards, computer passwords, e-passport, e-driving license and e-commerce. Cryptology prior to the modern age was almost synonymous with encryption, the conversion of information from a readable state to nonsense. The sender retained the ability to decrypt the information and therefore avoid unauthorized persons being able to read it [3][4].

Biometrics is a science of measuring physical and/or behavioral characteristics that are unique to each individual. Biometric technology verifies that an individual is who he/she claims to be. The physical Biometrics are hand or palm Geometry, Finger- prints, Facial Characteristics, retina, iris etc...

Bio-cryptography is emerging as a powerful solution which can combine the advantages of conventional cryptography and biometric security [11].

The motivation of the research is achieving a security concept in transaction of information for humans by using fingerprint combined with encryption algorithm Elliptic curve cryptography (Bio-Cryptography) [2].

A method is proposed for generation of unique cryptographic key which is generated using fingerprints of the user. The proposed approach reduces the cost associated with lost keys, addresses non-repudiation issues and provides increased security of digital content.

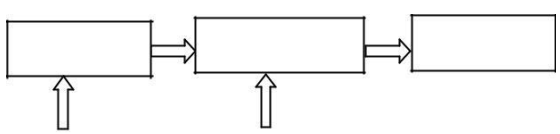
In this paper, emphasis is given on an efficient bio-cryptographic security protocol designed for client/server authentication in current mobile computing environment, with a reasonable assumption that server is secure. In this protocol, fingerprint biometric is used in user verification, protected by a computationally efficient Public Key Infrastructure (PKI) scheme, Elliptic Curve Cryptography (ECC). Fingerprint features are not only used for biometric verification but also for cryptographic key generation. Our security analysis shows that the proposed protocol can provide a secure and trustworthy authentication of remote mobile users over insecure network.

Cryptography, then, not only protects data from theft or alteration, but can also be used for user authentication. There are, in general, three types of cryptographic schemes typically used to accomplish these goals: secret key (or symmetric) cryptography, public-key (or asymmetric) cryptography, and hash functions. In all cases, the initial unencrypted data is referred to as plaintext. It is encrypted into cipher text, which will in turn be decrypted into usable plaintext. Some specific security requirements, including:

1) Authentication: The process of proving one's identity. The primary forms of host-to-host authentication on the internet today
   are name-based or address-based, both of which are notoriously weak.
2) Privacy/confidentiality: Ensuring that no one can read the message except the intended receiver.
3) Integrity: Assuring the receiver that the received message has not been altered in any way from the original.
4) Non-repudiation: A mechanism to prove that the sender really sent this message [3].

II. CRYPTOGRAPHIC ALGORITHMS

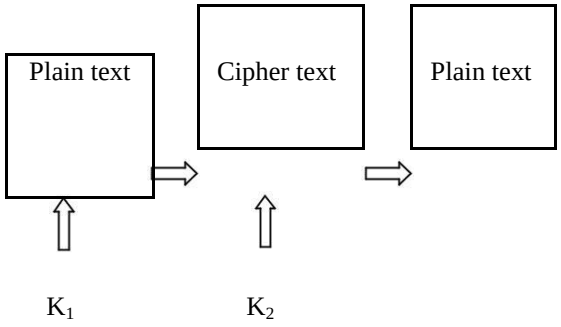
1) Secret Key Cryptography (SKC): Uses a single key for both encryption and decryption.
2) Public Key Cryptography (PKC): Uses one key for encryption and another for decryption.
3) Hash Functions: Uses a mathematical transformation to irreversibly "encrypt" information.



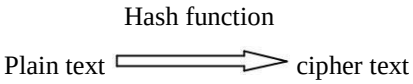
Plain text Cipher text Plain text

K_1 K_1

(a) Secret (symmetric) key cryptography .SKC uses single key for both encryption and decryption.



(b) Public key (asymmetric) cryptography uses two keys, one for encryption and other for decryption.



(c) Hash function (one way cryptography). Hash function has no key. Since the plain text is no recoverable from the plain text [13].

Fig . Types of cryptography

III.PUBLIC-KEY CRYPTOGRAPHY (PKC)

Public-key cryptography is a cryptographic approach which involves the use of asymmetric key algorithms instead of or in addition to symmetric key algorithms. Unlike symmetric key algorithms, it does not require a secure initial exchange of one or more secret keys to both sender and receiver. The asymmetric key algorithms are used to create a mathematically related key pair: a secret private key and a published public key.

A. RSA

The first, and still most common, PKC implementation, named for the three MIT mathematicians who developed it Ronald Rivest, Adi Shamir, and Leonard Adleman. RSA today is used in hundreds of software products and can be used for key exchange, digital signatures, or encryption of small blocks of data. RSA uses a variable size encryption block and a variable size key. The key-pair is derived from a very large number, n, that is the product of two prime numbers chosen according to special rules; these primes may be 100 or more digits in length each, yielding an n with roughly twice as many digits as the prime factors. The public key information includes n and a derivative of one of the factors of n; an attacker cannot determine the prime factors of n (and, therefore, the private key) from this information alone and that is what makes the RSA algorithm so secure. (Some descriptions of PKC erroneously state that RSA's safety is due to the difficulty in factoring large prime numbers.

B. Diffie-Hellman

After the RSA algorithm was published, Diffie and Hellman came up with their own algorithm. D-H is used for secret-key exchange only, and not for authentication or digital signatures. It is one of the earliest practical examples of Key exchange implemented within the field of cryptography. The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher. It is a type of key exchange.

C. Elliptic Curve Cryptography (ECC)

ECC can offer levels of security with small keys comparable to RSA and other PKC methods. It was designed for devices with limited compute power and/or memory, such as smartcards.

The Public-Key Cryptography Standards are specifications produced by RSA Laboratories in cooperation with secure systems developers worldwide for the purpose of accelerating the deployment of public-key cryptography. First published in 1991 as a result of meetings with a small group of early adopters of public-key technology, the PKCS documents have become widely referenced and implemented.

Briefly outline the basics of elliptic curves over finite fields and the cryptography applications related to elliptic curves.

Equation of Elliptic curve $y^2=(x^3+ax+b) \bmod p$

It is an abelian group

- Closure: If a and b belong to G, then a.b is also in G.
- Associative: a.(b.c)=(a.b).c for all a,b,c in G
- Identity element : There is an element e in G such that a.e=e.a=a
- Inverse element: For each a in G there is an element in a' in G such that a.a'=a'. a=e
- Commutative: a.b=b.a for all a,b in G D.

Hash Functions

A hash function is any well-defined procedure or mathematical function that converts a large, possibly variable-sized amount of data into a small datum, usually a single integer that may serve as an index to an array (cf. associative array). The values returned by a hash function are called hash values, hash codes, hash sums, checksums or simply hashes.

IV.PROPOSED METHOD

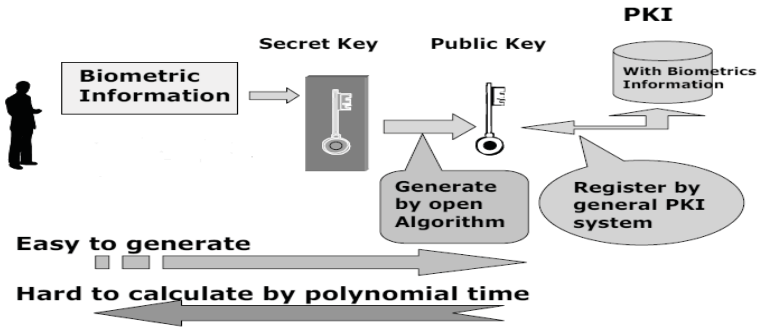


Fig.1 The combination of biometrics and PKI

A method is proposed for generation of unique cryptographic key which is generated using figure prints of the user, which are stable throughout person's lifetime. The proposed approach reduces the cost associated with lost approach has reduced the complicated sequence of the operation to generate crypto keys as in the traditional cryptography system . The key is derived directly from the figure print data and is not stored in the database, since it creates more complexity to crack or guess the cryptographic keys. Biometrics, cryptography and data hiding will provide good perspectives for information security. We proposed an algorithm for deriving provide high security with good performance in terms of computational and bandwidth requirements. There are several biometric systems in existence that deal with cryptography, but the proposed figure print parameter based cryptographic key introduces a novel method to generate cryptographic key. This approach is implemented in MATLAB and can generate variable size cryptographic key, with minimum amount of time complexity, which is aptly suited for any real time cryptography [6].

The strength of present day cryptosystem lies mainly in the key used for encryption. The problem to remember, protect and manage private key is a major issue in case of asymmetric ciphers. By using proven one way mathematical functions, multiplication of two large primes and secure hash function, we propose a robust and stable fingerprint key generation scheme. This scheme enables the generation of secure and cancelable cryptographic key with a very small FAR. The key can be used as private key for elliptic curve.

Presently biometric templates (fingerprint, face and iris) in chips are exposed to clandestine scanning which does not assure security. Data confidentiality is also compromised since existing system uses RSA (Rivest, Shamir, Adleman) algorithm. In this project, minutiae coordinate points are derived from biometric template. From that coordinate points elliptic curve is generated using elliptic curve algorithm.

Exact minutiae extraction is vital for all minutiae-based finger print recognition system. It has three steps to extract the minutiae. Final step is elliptic curve generation [4].

- Binarization

- Thinning
- Noise removal & Minutiae extraction
- Elliptic curve points generation

A)Binarization

Binarization is used to reduce the surrounding noise in the image. Image binarization is the process of turning a grayscale image to a black and white image. In a gray-scale image, a pixel can take on 256 different intensity values while each pixel is assigned to be either black or white in a black and white image. This conversion from gray-scale to black and white is performed by applying a threshold value to the image. When a threshold is applied to an image, all pixel values are compared to the input threshold. Any pixel values below the threshold are set to zero, and any values greater than the threshold are set to one. By the end of this process, all pixel values within the image are either zero or one, and the image has been converted to binary format.

B) Thinning

After binarization, another major pre processing technique applied to the image is thinning, which reduces the thickness of all ridge lines to a single pixel. Following thinning, the location and orientation of the minutiae should still be the same as in the original image to ensure accurate estimation of their locations. There are a variety of thinning methods employed in today's systems. Here we used central line thinning method and normal mat lab thinning comment then got exact minutiae from the finger print.

C) *Minutiae Extraction*

Accurate minutiae detection is an essential component for all minutiae-based fingerprint recognition systems. Without accurate minutiae detection, the results and performance of a system are not reliable. In the proposed method, Euclidian distance method is used to extract minutiae. The resulting information consists of the following for each minutia:

Location within the image

Termination or bifurcation [5]

D) *Elliptic Curve Cryptography*

Cryptography is the practice and study of hiding information. Modern cryptography intersects the disciplines of mathematics, computer science, and engineering. In the proposed method elliptic curve coefficients are derived from minutiae. The generated elliptic curves will be used to generate security keys (i.e. private key, public key) which enables the network be secured one. The network security can be implemented using these security keys [6].

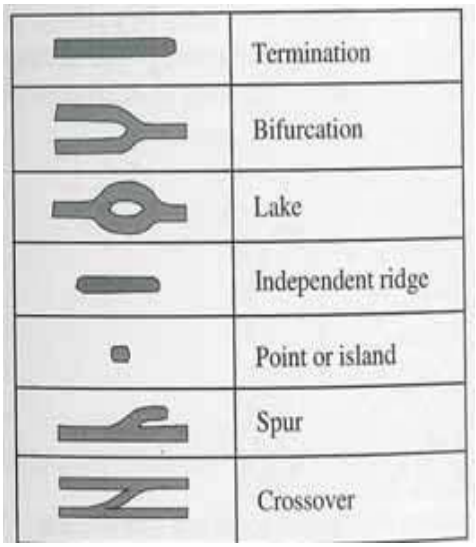


Fig.2. Types of minutiae

Procedure for Elliptic Curve cryptography:

[1] Get values of elliptic curve $y^2 = (x^3 + ax + b) \bmod p$. Variables a, b and p are chosen from fingerprint minutiae.

[2] Calculate curve point using curve fitting approach.

[3] Find point of infinity. Let us call this as variable n of type long int. To do so we perform a multiplication operation of a base point from 1P, 2P, 3P, and so on. Every resultant point is searched in the set of curve points. If found point_of_infinity is incremented, else final result is declared.

[4] Both A and B select a base point for communication. Base point is selected such that it has its maximum multiples lying on the curve. Base point is G. Data structure used is a structure "base" with two fields.(one for x co-ordinate and other for y co-ordinate).

Steps 1 through 4 are initialization steps and are executed by both parties.

[5] Sender A's private key is generated from his fingerprint.

[6] A calculates its public key PA = G * nA

[7] Receiver B's private key is generated from B's fingerprint.

[8] B calculates its public key PB = G * nB

[9] For the message to be transmitted decide a message point is Pm , it is a structure of type point.

[10] Public key of B is known to A. A wants to send a message to B. It uses B's public key PB, to encrypt the message point into ciphertext pair of points.

i.e. PC = [(nA * G), (Pm + kPB)]

B receives a pair of points PC. B uses his private key nB.

[11]To compute the plain text points B executes steps 12 onwards:

[12][(Pm + kPB) – (nB(kG)]

[13] [(Pm + kPB) + (– (nB(kG))] using the property that –P = (xP, -yP) and finally gets the decrypted message [9].

Performance Evaluation:

False Acceptance Rate(FAR)=Number of imposter accepted/Total number of imposter trials

False Rejection Rate(FRR)=Number of imposter Rejected/Total number of imposter trials

V. THE SIMULATION RESULTS DEVELOPED IN THE MATLAB IS PRESENTED

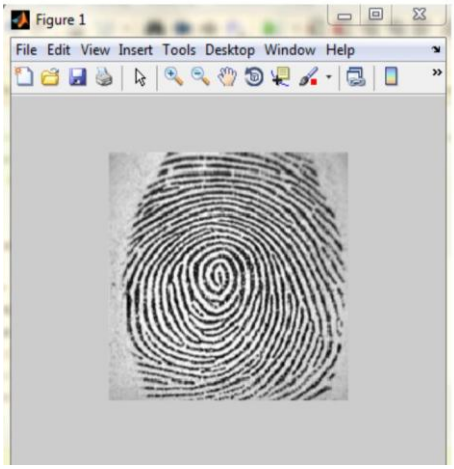


Fig.3. Original image

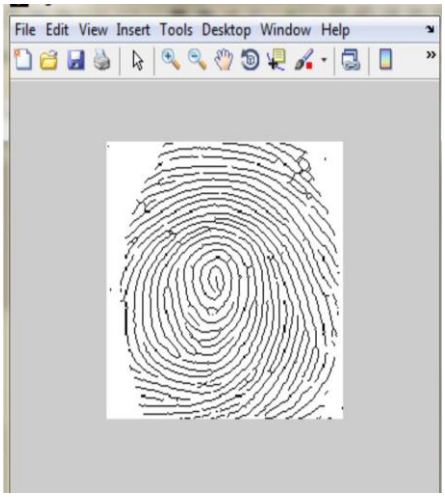


Fig.5. Thinned image

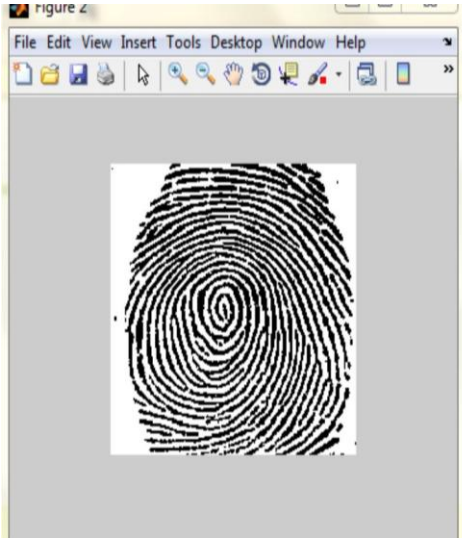


Fig.4. Binary image

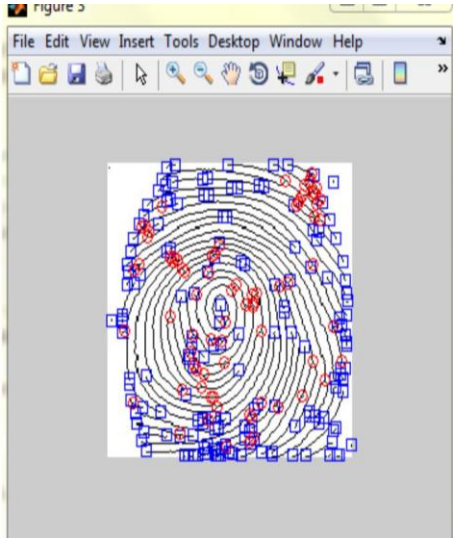


Fig.6. Bifurcated and Terminated point

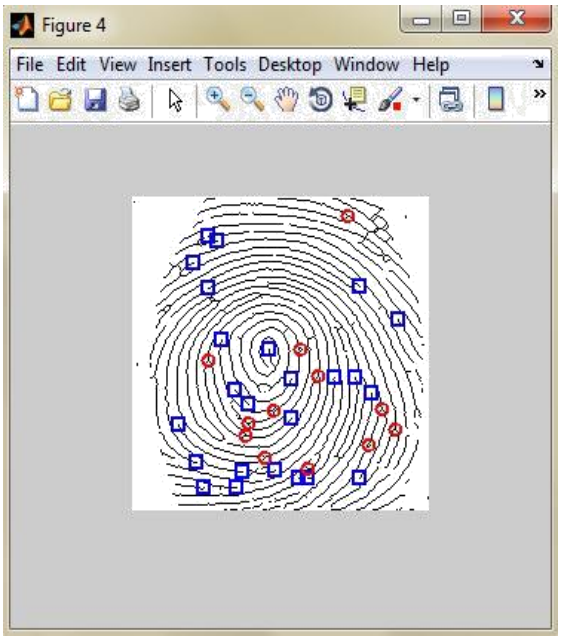


Fig.7. Bifurcated and terminated point after removing spurs minutiae points

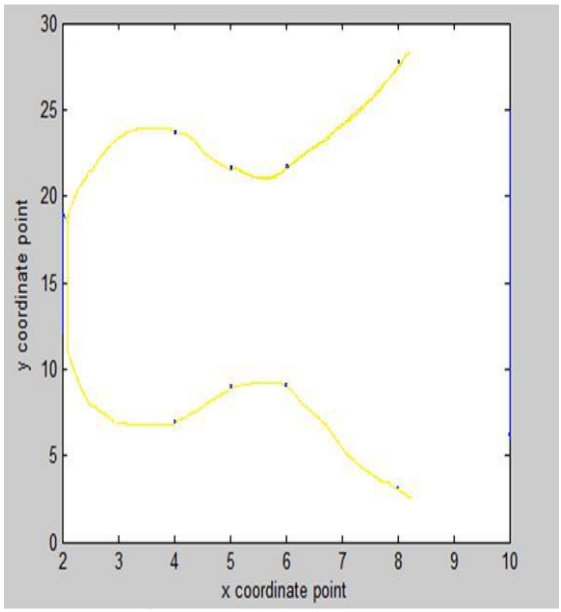


Fig.8. Elliptic curve generated from the

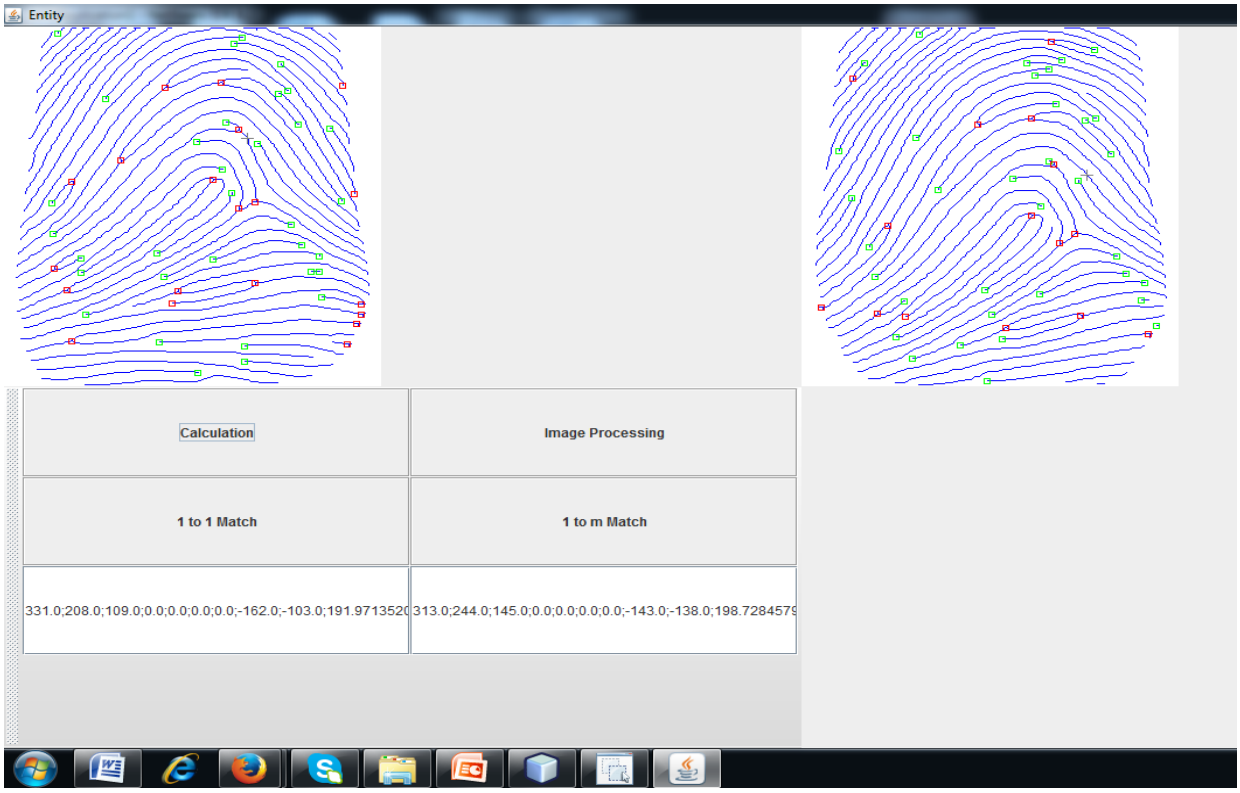


Fig 9: Minutiae Points Extraction and Key Generation

VII. CONCLUSION AND FUTURE SCOPE

Best authentication system can be generated by using the proposed method. In this method, biometric is used for the person identification. Even one system produces false identification for a genuine person with the help of other system the false rejection rate is reduced. It provides Security and reliability in networks for communication. This method is simple and the efficient.

Since most of the existing biometric ID documents like e-Passport and driving license are having storage fields for finger print, face and iris. In the proposed method Finger print used as biometric template. So, in the future we can implement the proposed system without enhancing the present method.

This project can also be extended to the face and iris recognition. It can improve the reliability of the real time system. The proposed method can be developed for different applications like image retrieval, military areas, investigation departments, and industrial automation.

REFERENCES

[1] Zhe Liu, Xinyi Huang, Zhi Hu, Muhammad Khurram Khan, Hwajeong Seo, and Lu Zhou , ," On Emerging Family of Elliptic Curves to Secure Internet of Things: ECC Comes of Age", IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. XX, NO. XX, JAN 2016

[2] Bharati Kashyap, K.J.Satao," Implementation of Multi Biometric cryptosystem for information security using ECC", Science Direct ,2015

[3] Alwyn, Andrew B.J and David C.L Ngo (2016) 'Biometric Hash: High-Confidence Face Recognition', IEEE Transaction On Circuits And Systems For Video Technology, Vol 16, pp 771-775.

[4] A. Juels, D. Molnar, D. Wagner, "Security and Privacy Issues in E-passports", *IEEE Secure Comm '05*, page(s): 74 – 88, 2005.

[5] V. Pasupathinathan, J. Pieprzyk, H. Wang, "Formal analysis of icao's e-passport specification", In: Brankovic, L., Miller, M. (eds.) Australasian Information Security Conference (AISC2008). Conferences in Research and Practice in Information Technology (CRPIT), vol. 81, Australian Computer Society (2008).

[6] Justice and Home Affairs: Eu standard specifications for security features and biometrics in passports and travel documents. Technical report, European Union (2006).

[7] G. S. KC, P. A. Karger, "Security and Privacy Issues In Machine Readable Travel Documents (MRTDs)", 10th European Symposium on Research in Computer Security (ESORICS 2005) Milan, Italy, 14-16 September 2015.

[8] J.H. Hoepman, E. Hubbers, B. Jacobs, M. Oostdijk, R.W. Schreur, "Crossing Borders: Security and Privacy Issues of the European e-Passport", 1st Int. Workshop on Security, IWSEC 2006, LNCS 4266, pages 152-167, Kyoto, Japan, 2006.

[9] V. Pasupathinathan, J. Pieprzyk, H. Wang, "An On- Line Secure E-Passport Protocol", Book Chapter in Information Security Practice and Experience Volume 4991/2008, pages 14-28, Springer Berlin / Heidelberg, 14th March 2016.

[10] Mike Burmester, Tri Van Le, Breno De Medeiros, Gene Tsudik, "Universally Composable RFID Identification and Authentication Protocols", Transactions on Information and System Security (TISSEC), Volume 12 Issue 4, 2009.

[11] A. Juels and M. Sudan. "A fuzzy vault scheme", in A. Lapidoth and E. Teletar, editors, Proc. IEEE Int. Symp. Information Theory, page 408, 2002

[12] Mohamed Abid and Hossam Afifi, "Towards a secure e-Passport protocol based on biometrics" Journal of Information Assurance and security IEEE 4 (2009) 338-345.

[13] U. Uludag and A. Jain, "Securing Fingerprint Template: Fuzzy Vault with Helper Data", Proc. IEEE Workshop on Privacy Research In Vision (PRIV), New York City, NY, June 2006.

[14] G.P. Hancke, "Practical Attacks on Proximity Identification Systems (Short Paper)," *IEEE Symp. Security and Privacy (S&P 06)*, IEEE CS Press, 2006, pp. 32