**International Journal of Pure and Applied Mathematics**
**Volume 117 No. 21 2017, 779-787**
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
**url:** http://www.ijpam.eu
Special Issue



# Biometric Based Cryptography for Enhanced Security Mechanism

[1]K. Sai Prasanthi, [2]Hari Venkata Krishna, [3]Anusha, [4]Naveena and [5]Sri Saranya
[1]Koneru Lakshmaiah Education Foundation,
Department of CSE, India.
prasanthi1216@kluniversity.in
[2]Koneru Lakshmaiah Education Foundation,
Department of CSE, India.
hvkrishnakotha@gmail.com
[3,4,5]Koneru Lakshmaiah Education Foundation,
Department of CSE, India.

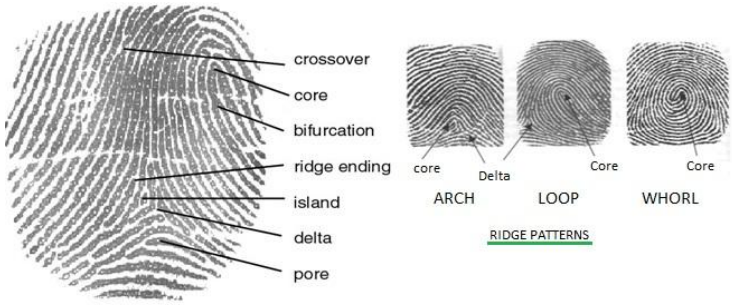
## Abstract

Advances in the field of Data Innovation likewise make Data Security an indistinguishable piece of it. To manage security, Authentication plays a vital part. Security has dependably been a noteworthy worry for confirmation over systems administration. Cryptographic techniques take care of the issue of security by actualizing different strategies for scratch trade. Encrypted message pair is the major constraint established by Elgamal Algorithm for two parties without the prior knowledge of each other over insecure communication channel. This calculation encrypts the message with the assistance of beneficiary's public key and sender's private key. This exploration paper manages the use of fingerprint as the private key for encryption and decryption for improved security. This paper exhibits a survey on the biometric verification methods and some future conceivable outcomes in this field. In biometrics, an individual should be distinguished in light of some trademark physiological parameters. A wide assortment of frameworks require dependable individual acknowledgment plans to either affirm or decide the personality of an individual asking for their administrations. The reason for such plans is to guarantee that the rendered administrations are gotten to just by an honest to goodness client, and not any other person. By utilizing biometrics it is conceivable to affirm or set up a person's character. The position of biometrics in the present field of Security has been delineated in this work. We have additionally laid out conclusions about the convenience of biometric verification frameworks, examination between various methods and their preferences and hindrances in this paper.

**Key Words:**Biometrics, authentication, elgamal, fingerprint, encryption, decryption.

# 1. Introduction

Cryptography contains different reflection levels of security system and it constructs the discipline of information encryption and decryption. System executive gives approved access over the system by actualizing system security and selection of its arrangements and approaches to anticipate unapproved get to. Approval has dependably been an indispensable piece of the security component. Biometric arrangement of recognizable proof uses special component of face, hands like iris, retina, finger impression, structure of the face to distinguish a man with an extraordinary trademark that separates the concerned individual from others. The arrangement of utilizing unique finger impression as a parameter for approval gives improved security to information exchange over the system. In non-biometric confirmation process, for example, use of passwords or Stick numbers, contingent on the length of the key, the data is particularly defenseless against unapproved access by people. Longer and irregular passwords are more secure than short words that contain lexicon words. Unique finger impression is an impression left by the grating edges of a human finger. They are shaped in people in their conclusive frame before birth and are constantly one of a kind. Fingerprints assume a critical part in criminological science. Unique mark coordinating techniques are ordered into three classes. They are connection based coordinating, details based coordinating and edge include based coordinating. Sergey Tulyakov propose to utilize symmetric hash capacities to secure biometric frameworks. Fuzzy extractor ties arbitrary information with biometric information to deliver interesting keys. There are three major process in Elgamal Cryptosystem: Key generation, Encryption, Decryption.




Fingerprint Image (Image-1)

**The Elgamal Cryptosystem**

*History*

In 1984 Taher ElGamal presented a cryptosystem which is based on the Discrete Logarithm Problem. It relies on the assumption that the DL cannot be found in feasible time, while the inverse operation of the power can be computed efficiently. The original public key system proposed by Diffi and Hellman requires interaction of both parties to calculate a common private key. This poses problems if the cryptosystem should be applied to communication

systems where both parties are not able to interact in reasonable time due to delays in transmission or unavailability of the receiving party.

Thus ElGamal simplify the Diffi key exchange algorithm by introducing a random exponent k. This exponent is a replacement for the private exponent of the receiving entity. Due to this simplify the algorithm can be used to encrypt in one direction, without the necessity of the second party to take actively part. The key advance here is that the algorithm can be used for encryption of electronic messages, which are transmitted by the means of public store-and-forward services.

*Key Generation*

The basic requirement for a cryptographic system is at least one key for symmetric algorithms and two keys for asymmetric algorithms.

The key generation steps are similar to the general scheme explained above. With ElGamal, only the receiver needs to create a key in advance and publish it. Following our naming scheme from above, we will now follow Bob through his procedure of key generation.

Bob will take the following steps to generate his key pair:

1. Prime and group generation

First Bob needs to generate a large prime p and the generator g of a multiplicative group $Z^*$ of the integers modulo p.

2. Private Key selection

Now Bob selects an integer b from the group Z by random and with the constraint $1 \leq b \leq p - 2$. This will be the private exponent.

3. Public key assembling

From this we can compute the public key part $g^b \bmod p$. The public key of Bob in the ElGamal cryptosystem is the triplet $(p, g, g^b)$ and his private key is b.

4. Public key publishing

The public key now needs to be published using some dedicated key server or other means, so that Alice is able to get hold of it.

*Encryption*

To encrypt a message M to Bob, Alice fi needs to obtain his public key triplet $(p, g, g^b)$ from a key server or by receiving it from him via unencrypted electronic mail. There is no security issue involved in this transmission, as the only secret part, b, is sent in $g^b$. Since the core assumption of the ElGamal cryptosystem says that it is infeasible to compute the discrete logarithm, this is safe. For the encryption of the plaintext message M, Alice has to follow these steps:

1. Obtain the public key

As described above, Alice has to acquire the public key part (p, g, $g^b$) of Bob from a trusted key server.

2. Prepare M for encoding

Write M as set of integers (m1, m2, . . .) in the range of $\{1, \ldots, p-1\}$. These integers will be encoded one by one.

3. Select random exponent

In this step, Alice will select a random exponent k that takes the place of the second party's private exponent in the Diffi key exchange. The randomness here is a crucial factor as the possibility to guess the k gives a sensible amount of the information necessary to decrypt the message to the attacker.

4. Compute public key

To transmit the random exponent k to Bob, Alice computes $g^k$ mod p and combines it with the cipher text that shall be sent to Bob.

5. Encrypt the plaintext

In this step, Alice encrypts the message M to the cipher text C. For this, she iterates over the set created in step 2 and calculates for each of the mi:

$c_i = m1 * (g^b)^k$

The cipher text C is the set of all $c_i$ with $0 < i \leq |M|$.

The resulting encrypted message C is sent to Bob together with the public key $g^k$ mod p

Derived from the random private exponent.

*Decryption*

After receiving the encrypted message C and the randomized public key $g^k$, Bob has to use the encryption algorithm to be able to read the plaintext M. This algorithm can be divided in a few single steps:

1. Compute shared key

The ElGamal cryptosystem helped Alice to define a shared secret key without Bob's interaction. This shared secret is the combination of Bob's private exponent b and the random exponent k chosen by Alice. The shared key is defined by the following equation:

$(g^k)^{p-1-b} = (g^k)^{-b} = b^{-bk}$

2. Decryption

For each of the cipher text parts $c_i$ Bob now computes the plaintext using

$m_i = (g^k)^{-b} * c_i \bmod p$

After combining all of the mi back to M he can read the message sent by Alice.

# 2. Proposed System

Among all the current biometric procedures, the unique mark is the best and secured highlight for the individual confirmation. This highlights empower us to utilize unique mark validation framework where security is a prime necessity. The accompanying investigation settled on unique finger impression as a decision of determination (Image-2). Here we can utilize the unique finger impression as the private key for the generation of key for encryption.

| Biometrics | Univer-sality | Unique-ness | Perma-nence | Collect-ability | Perfor-mance | Accept-ability | Circum-vention |
|---|---|---|---|---|---|---|---|
| Face | H | L | M | H | L | H | L |
| Fingerprint | M | H | H | M | H | M | H |
| Hand Geometry | M | M | M | H | M | M | M |
| Keystroke Dynamics | L | L | L | M | L | M | M |
| Hand vein | M | M | M | M | M | M | H |
| Iris | H | H | H | M | H | L | H |
| Retina | H | H | M | L | H | L | H |
| Signature | L | L | L | H | L | H | L |
| Voice | M | L | L | M | L | H | L |
| Facial Thermogram | H | H | L | H | M | H | H |
| DNA | H | H | H | L | H | L | L |

H=High, M=Medium, L=Low

Image 2

In the proposed system the private key (b) of Bob and the random number generated by Alice (k) are their respective Fingerprints. These Fingerprints are converted to their decimal values. The decimal value of the fingerprint obtained from the biometric authentication device which is used as the private key for the process.

Image 3

*Key Values*

Prime Number – p

Generator – g

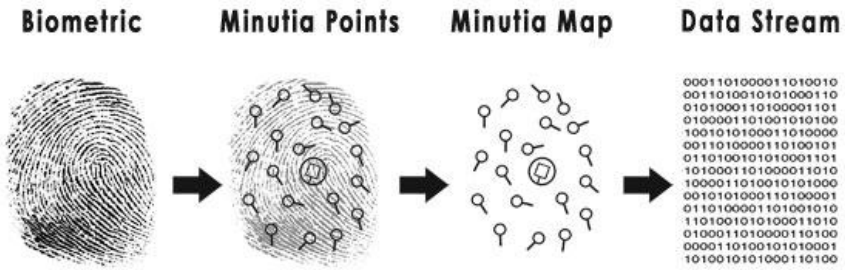
Private Key – Fingerprint value of Receiver (b)

Public Key – (p, g, $g^b$)

Random Number – Fingerprint value of Sender (k)

## Conversion of Fingerprint to Data Stream

The process of the conversion of Fingerprint to its Data Stream involves the steps as mentioned in image-4.




In biometrics and legal science, particulars are significant highlights of a unique mark, utilizing which examinations of one print with another can be made. Particulars include:

Ridge ending – the unexpected end of a ridge

Ridge bifurcation – a solitary edge that partitions into two edges

Short ridge, or independent ridge – a ridge that starts, voyages a short separation and afterward closes

Island – a solitary little ridge inside a short ridge or ridge finishing that isn't associated with every single other ridge

Ridge enclosure – a solitary edge that bifurcates and reunites in a matter of seconds thereafter to proceed as a solitary edge

Spur – a bifurcation with a short edge fanning out a more drawn out edge

Crossover or bridge – a short edge that keeps running between two parallel edges

Delta – a Y-formed ridge meeting

Core – a U-hand over the ridge design

## Conversion of Fingerprint Value to Private Key

The finger print of the sender and receiver are converted to equivalent decimal value. The decimal value of the finger print obtained from the biometric authentication device which is used as the private key.


In biometric this approach is used for encryption and decryption between two parties and ensures both authentication and non-repudiation. Here, Elgamal based encryption scheme used, instead of selecting random number, user's finger print is stored in database, it is retrieved only at the time of authentication, and no one can pose as a sender, because of his finger print identity. This works puts the cryptanalysts under pressure. The utilization of this novel calculation in biometric signature creation enhances the electronic keeping money security, as people in general and private keys are made without putting away and transmitting any private data anyplace finished the system.

# 3. Conclusion

The above research paper is proposed for enhanced network security. For this analysis, ElGamal algorithm has been implemented. The use of unique finger impression rather than arbitrary number as a private key in the calculation gives better security to information exchange over the system with high confidentiality. In future to avoid high level security threats we can upgrade the system by having multiparameter security mechanisms such as hybrid combinations of Deoxyribonucleic Acid (DNA) with finger print or with retina.

# References

[1] Tulyakov S., Farooq F., Mansukhani P., Govindaraju V., Symmetric hash functions for secure fingerprint biometric systems, Pattern Recognition Letters 28(16) (2007), 2427-2436.

[2] Whitfield Diffie, Martin E. Hellman, New Directions in Cryptography, Invited Paper (1976).

[3] Bhattacharyya D., Ranjan R., Das P., Kim T.H., Bandyopadhyay, S.K., Biometric authentication techniques and its future possibilities, Second International Conference on Computer and Electrical Engineering (2009), 652-655.

[4] Wikipedia, https://en.wikipedia.org/wiki/ElGamal_encryption.

[5] Jain A.K., Ross A., Pankanti S., Biometric: A Tool for Information Security, IEEE Trans. Information Forensics and Security 1(2) (2006), 125-144.

[6] Ian F. Blake, Theo Garefalakis, On the complexity of the discrete logarithm and diffie-hellman problems, J. Complex 20(2-3) (2004), 148–170.

[7] DNA security, http://securityaffairs.co/wordpress/33879/ security/ dna-cryptography.html.

[8] William Stallings, Cryptography and Network Security principles and practices, third Edition, Pearson Education (2003).

[9] Fingerprint-based crypto-biometric system

http://www.jis.eurasipjournals.com/content/2015/1/3.

[10] Balakumar P., Venkatesan R., Secure Biometric Key Generation Scheme for Cryptography, International Journal on Computer Science and Engineering 02(06) (2010), 1992-1995.

[11] Chandra S., Paul S., Saha B., Mitra S., Generate an Encryption Key by using Biometric Cryptosystems to secure transferring of Data over a Network, IOSR Journal of Computer Engineering 12(1) (2013), 16-22.