Delta University Scientific Journal
Journal home page: https://dusj.journals.ekb.eg

Multi Digital Identity Based on Isomorphic Authenticated Elliptic Curve for RFID Applications

Esam A. A. Hagras
Electronics and Communications Dept., Delta univ. for Science and Technology, Gamasa City, Dakahlia, Egypt, esam.hagras@deltauniv.edu.eg

ABSTRACT

This paper presents an enhanced isomorphic authenticated encryption scheme for Radio Frequency Identification (RFID) based on Multi Digital Identity (multi message) encryption and authentication verification (ESS-MDI). The proposed system utilizes the isomorphic elliptic curve (IEC) property to create an elliptic curve hidden layer, which enhances the security during encryption. Additionally, it employs the digital signature based on elliptic curve to ensure message authenticity. The proposed system also incorporates time-based restrictions for process execution or forbidding, which further strengthens the security of the scheme. The effectiveness of the proposed system is demonstrated through experimental results and comparison with existing state-of-the-art systems, which validate its robustness, efficiency, and security. The proposed system offers a secure and efficient solution for RFID multi-message encryption and authentication verification in various applications, such as financial transactions, IOT systems, and e-commerce.

Keywords: *isomorphic authenticated encryption, elliptic curve, smart card, security protocol, IOT*.

1. Introduction

Smart cards have become an essential tool for secure information storage and communication in various domains, such as banking, e-commerce, and healthcare. One of the significant challenges in RFID security is to ensure confidentiality, authenticity, and integrity of the information stored and transmitted through the card. Message encryption and authentication verification are critical techniques to achieve these security objectives in RFID systems (Madhusudhan *et all*.), IOT systems (Ray *et all*.), and e-commerce (Elkamchouchi *et all*.).

In recent years, there has been a growing interest in developing efficient and secure isomorphic authenticated encryption systems for smart cards. Isomorphic authenticated encryption combines the features of encryption and digital signature in a single step, which reduces computational overhead and enhances security (Biswojit *et all*.). Several isomorphic authenticated encryption schemes have been proposed in the literature, such as the RSA-based isomorphic authenticated encryption scheme, the ElGamal-based isomorphic authenticated encryption scheme, and the elliptic curve-based isomorphic authenticated encryption scheme (Moath *et all*.).

Among these schemes, the elliptic curve-based isomorphic authenticated encryption scheme has received much attention due to its advantages over other schemes in terms of security and efficiency (Shamsher *et all*.). Several researchers have proposed different elliptic curve-based isomorphic authenticated encryption schemes for RFID message encryption and authentication verification .

In (Anuj *et all*.) proposed RFID authentication protocol based on elliptic curve isomorphic authenticated encryption provides enhanced security attributes, further validation in real-world scenarios. (Ping *et all*.) proposed EC-based isomorphic authenticated encryption scheme addresses the shortcomings of existing schemes and leverages the high security of elliptic curve cryptography. The scheme is evaluated in terms of security, computational overhead, and communication overhead, and shows potential for secure and efficient application in

smart lock key management systems with favorable bit-oriented performance. (Abid *et all*) proposed lightweight multi-message and multi-receiver hybrid isomorphic authenticated encryption scheme based on hyper elliptic curve offers enhanced security attributes, including confidentiality, resistance against reply attack, integrity, authenticity, non-repudiation, public verifiability, forward secrecy, and unforgeability. The scheme boasts low computational costs, making it suitable for deployment in low-resource devices and heterogeneous environments. In (Biswojit Nayak *et all*) proposed isomorphic authenticated encryption scheme for IoT combines digital signature and symmetric key encryption, reducing computational complexity and communication overhead. The scheme uses ECC with shorter key lengths to offer the same security level as other public key cryptosystems with lower computational and communication costs, making it suitable for IoT scenarios with low-power efficiency. (Noori et al.) proposed scheme based on ECC for mutual authentication in RFID-based IoT medical care systems offers lower computational and communication costs, shorter elliptic curve point multiplication time, and improved security. It addresses the security shortcomings of RFID authentication and shows promising results in terms of efficiency and security. However, some of these schemes suffer from some limitations, such as low security, high computational overhead, and lack of time-based restrictions. However, these schemes suffer from some limitations, such as low security, high computational overhead, and lack of time-based restrictions.

This paper presents an efficient identity-based isomorphic authenticated encryption scheme for RFID applications, which provides both confidentiality and authenticity of messages. The proposed scheme is based on elliptic curve cryptography (ECC) and offers provable security, meaning that its security can be mathematically proven. The scheme is designed for resource-constrained devices like smart cards, which typically have limited processing power and memory. It offers efficient encryption and decryption operations, making it suitable for applications with stringent computational requirements. The paper presents a detailed analysis of the proposed scheme's security and performance, and compares it with other existing schemes. The results show that the proposed scheme offers improved efficiency while maintaining a high level of security, making it suitable for smart card-based message encryption and authentication verification in various applications. The organization of this paper is as follows: Section 2, presents the preliminaries and scheme preparation. Section 3 presents a detailed study of the ESS-MDI scheme. Section 4, provides the numerical analysis and their discussions. Finally, section 5 summarizes the main conclusion.

2. Preliminaries

2.1. Elliptic Curve Over Prime Field

An elliptic curve over the field F_p with parameters a and b (Davood *et al.*), denoted by E(p,a,b), is a set of points (x,y) that satisfy the equation $y^2 \equiv x^3 + ax + b \pmod p$, along with a special "point at infinity" denoted as O. For two elliptic curves E(p,a,b) and E(p,a',b'), they are called isomorphic if there exists a non-zero integer $t \in p$ such that the transformation $(x,y) \rightarrow (x',y')$ given by:

$$x' = t^2x,\ y' = t^3y \tag{1}$$

that maps E (p, a, b) onto E (p, a', b'). In other words, if we apply this transformation to all the points in E(p,a,b), we get a new set of points that satisfy the equation for E(p,a',b'). The EC order, denoted by #E, is the sum of the total number of points that lie on the EC and a point at infinity, denoted by O ($x = \infty; y = \infty$), as defined in (Ahmed Kamal *et al.*). In cryptographic applications, a specific point on the EC, called the generator point G, is used to compute public points for both the sender and receiver, denoted by P_A and P_B, respectively. The computation of these public points is based on the generator point G, and is a fundamental step in EC: $P_A = n_A .G$, $P_B = n_B.G$ where n_A is the private key of the sender, and n_B is the private key of the recipient. The sender and receiver can calculated the EC Secret Key (SK) between them using

$$SK = n_A.P_B = n_A.n_B.G = n_B.n_A.G = n_B.P_A \tag{2}$$

3. Proposed Scheme

In the proposed ESS-MDI scheme, the verifier decrypts the message encrypted using the characteristics of IEC and digitally unsigns it using the attribute of the elliptic curve. The main feature of the proposed scheme is that it fulfills the efficiency in the computational cost and communication overhead desired in identification protocols. The ESS-MME scheme consists of five algorithms namely, the ID initialization phase algorithm, Multi Key Generator (MKG) algorithm, the signature ID algorithm, the unsigned ID algorithm, the ID authentication phase algorithm. The ID initialization phase algorithm indicates the system parameters and functions used in the system and made it publicly available. The system asks for the Tag secret key (private key) and keeps it secret. The secret key is used in the signature ID algorithm to calculate the sign for all messages. The user uses his identity ID as a message for authentication to using the messages in the unsigned ID algorithm using key exchange which is given corresponding to his identity [13]. To authenticate the user, the system runs the authentication algorithm using the signcrypted and unsigncrypted messages. Finally, the system makes a decision that the Tag is authenticated or rejected using the system ID authentication phase algorithm as shown in Fig .2 and Fig .3

3.1. The ID Initialization phase algorithm

The main parameter (Key Schedule) used in the proposed scheme are given in Table 1:

Table 1. Key Schedule.

Symbol	Description
(p, a, b)	Elliptic curve parameters.
q	is a large prime factor of p-1
i	Isomorphism parameters.
X	a number chosen uniformly at random form [1, …, q - 1]
SK	EC Secret key.
ISK	IEC Secret key.
G	Basepoint chosen randomly from the points on the EC (public to all).
K	Verification key.
n_T	Tag private key, chosen uniformly at random form [1, …, q - 1].
PU_T	Tag public key ($PU_T = n_T . G$, a point on EC).
n_R	Reader private key, chosen uniformly random form [1, …, q - 1].
PU_R	Reader public key ($PU_T = n_T . G$, a point on EC).
KH	A keyed one-way hash function.
mod	Modular arithmetic.
$\oplus$	XOR operation.

The main system functions used in the proposed scheme are:

3.2. One way hash function H(.).

The hash function (SHA) takes a message of variable length as input and produces a fixed-output length. The SHA has the one-way property i.e., given k and a message input m, computing H(m) = K must be easy and given k, it is hard to compute m such that H(m) = K. The minimum security from minimum hash output length is at least 128

bits. There are many types of secure hash functions which are given by the National Institute of Standards and Technology (Ahmed Kamal *et al*.).

3.3. The One-way keyed hash function KH (.).

In the one-way keyed hash function, the secret key K is used to hash a message m. In most practical application, it sufficient to define KH (m) = H (K, m) (Saddam *et al*.).

3.4. Elliptic curve message encryption

The Tag encrypt the message using the EC secret key and perform the second layer of encryption using the hidden IEC and the steps will be as follows:

1. Divide the message into groups integers < p.
2. Use the EC secret key to compute the first layer of message encryption

$$C_{L1} = SK \oplus m \tag{3}$$

3. Divide the K to (K_x, K_y)
4. Compute the isomorphism parameter i

$$i = K_x \oplus K_y \tag{4}$$

5. Convert SK (x, y) to ISK (x_i ,y_i) using eq.(1) and i
6. Use the ISK to compute the second hidden layer of encryption for the message

$$C_{L2} = ISK \oplus m_t \tag{5}$$

3.5. *Elliptic curve message decryption*

The Reader decrypt the message using the IEC secret key and perform the second layer of decryption using the EC secret key and the steps will be as follows:

1. Divide the K' to (K'$_x$, K'$_y$)
2. Compute the isomorphism parameter i

$$i = K'_x \oplus K'_y \tag{6}$$

3. Compute the EC SK using eq. (2)
4. Convert SK (x, y) to ISK (x_i, y_i) using eq. (1) and i
5. Use the IEC secret key to compute the first layer of decryption for the message

$$C_{L1} = ISK \oplus C_{L2} \tag{7}$$

6. Use the SK to compute the second layer of decryption for the

$$m_t = SK \oplus C_{L1} \tag{8}$$

3.6 *The public parameters*

If a user wants to login the system, he attaches his RFID to the input device. The system ask for n_T . If wrong, the system rejects the smart card. If OK the system identification process to the smart card.

$$\{EC, q, G, P_{UT}, P_{UR}, KH(m), H(.), \text{sign ID } (.)\}$$

3.7 *The Multi Key Generator algorithm*

The MKG take the SHA output (K = 128 bit) to generate K_t output bit. The MKG separate K to two parts K_R, K_L and exchange it. The two exchanged parts differed using nonlinear function.

$$\alpha = SL^{7+t}(K_R) \quad (9)$$

$$\beta = RR^{13+t}(K_L) \quad (10)$$

$$K_t = \alpha(K_{t-1}) \parallel \beta(K_{t-1}) \quad (11)$$

If only t = 1 then do nothing $K_1 = K$

SL: Shift left, RR: Rotate right, ‖ concatenate.

The MKG takes t rounds to generate the K_t keys. the operation is fast and easy to do using microprocessor, the final output K_t is the concatenation of α, β so that:

$$K_1 = K, \qquad K_2 = \alpha(K_1) \parallel \beta(K_1), K_3 = \alpha(K_2) \parallel \beta(K_2) \ldots \quad (12)$$

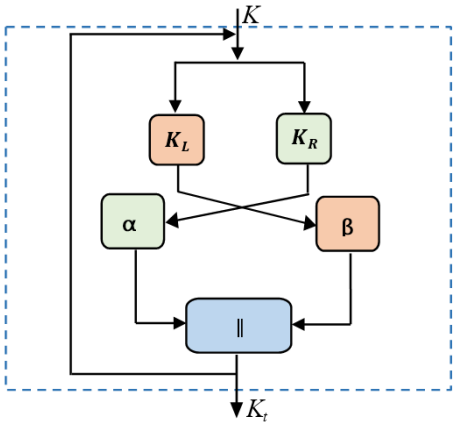

Fig. 1. Cryptosystem Multi key generation diagram.

3.8. *The signature ID algorithm*

The messages m_1, m_2, m_3, ….m_t represents the user secure inputs fingerprint, eye print, face recognition, etc. all inputs stored in Tag, when user use Tag to inter the system, it asks for secret key n_t for more security if it OK the system and Tag follow the steps:

Step-1: the user inserts the RFID card in the reader that ask for the Tag private key and the user ID.

Step-2: Tag generates (X) 128 random number bits.

Step-3: Tag compute SHA 128 to output K using the random number (X) and the parameters of elliptic curve.

$$K = H(PU_R \,.\, X) \bmod P \quad (13)$$

Step-4: Compute multi keys K_t using MKG to encrypt messages m_1,m_2,m_3,….m_t.

$$K_t = K_1, K_2, K_3 \ldots K_t \qquad t = 1,2,3\ldots. \quad (14)$$

Step-5: Encrypt messages C_1,C_2,C_3,…..,C_t according to the Elliptic curve message encryption steps using the output of MKG.

Step-6: Compute *r* keyed hash KH for messages $m_1, m_2, m_3, \ldots m_t$ using the relation.

$$r_t = \mathrm{HK}\ (m_t) \tag{15}$$

Step-7: Compute the multi message signature using the random number X, the keyed hash value r_t and the user private key n_T.

$$S = (X/r + n_T) \bmod q \tag{16}$$

The multi message isomorphic authenticated encryption consists of the encrypted message C_t, the signature S and the keyed hash r. the Tag send (C_t, S, r) to the reader.

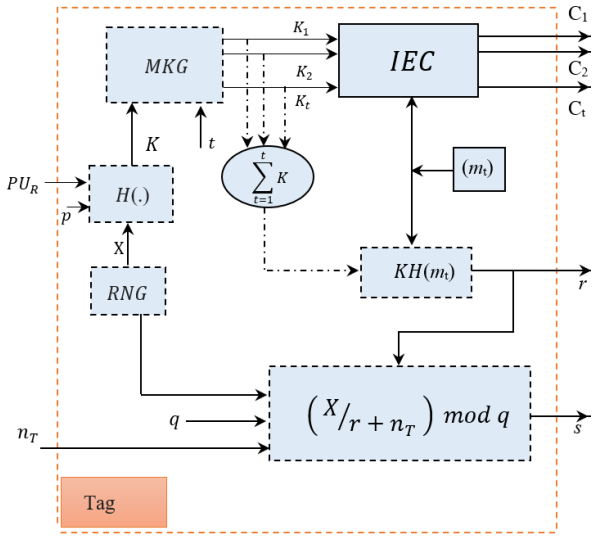

Fig. 2 Proposed Isomorphic Elliptic Curve authenticated encryption.

3.9. *The unsigned ID algorithm*

The Reader verifies the signature parameters (S, r) sent from the Tag using the characteristics of elliptic curve differ Hellman key exchange as in eq. (2) to get Tag secret key (n_R, PU_T) and the system performs the following operations:

Step-1: Calculate (K′) decryption key using hash function SHA using (n_R, P_{UT}), the signature and keyed hash values (S, r).

$$K' = \mathrm{H}((\mathrm{Y}.\ P_{UT}) + (\mathrm{Y}.\ \mathrm{r}.\ \mathrm{G})) \tag{17}$$

Step-2: Compute secret keys K_t using MKG to decrypt messages $m_1, m_2, m_3, \ldots m_t$.

$$K'_t = K'_1, K'_2, K'_3 \ldots K'_t \qquad t = 1,2,3\ldots. \tag{18}$$

Step-3: Decrypt messages $m_1, m_2, m_3, \ldots m_t$ using according to the Elliptic curve message decryption steps using the output of MKG.

Step-4: Compute the keyed hash (r') for the inserted ID messages $m_1, m_2, m_3 \ , \ldots . m_t$ using keyed hash KH of the choose message m.

$$r' = HK\ (m') \tag{19}$$

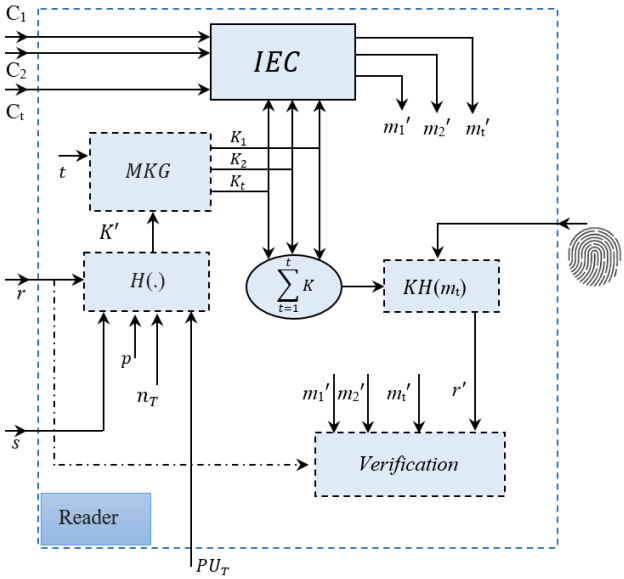

Fig. 3. Elliptic curve unisomorphic authenticated encryption multi digital identity Protocol using RFID decision.

3.10. *The ID authentication phase algorithm*

The system authenticates the Tag by checking the following:

l) Calculate The time interval between T and T′.

- If (T - T′) ≥ ∇T then the system terminate the process and reject the Tag where T is the time response and ∇T is the accepted time interval for transfer delay.

- If (T - T′) < ∇T then the system accept the process and continue the Tag authentication.

2) Compare ($m = m'$), If equal the system continue authenticating Tag, if not the system terminates the process.

3) Compare (r = r′), If equal the system continue authenticating Tag, if not the system terminates the process.

4) If (T — T′) < ∇T, (m = m′) and ($r = r'$), then the system accept the process and authenticate the Tag.

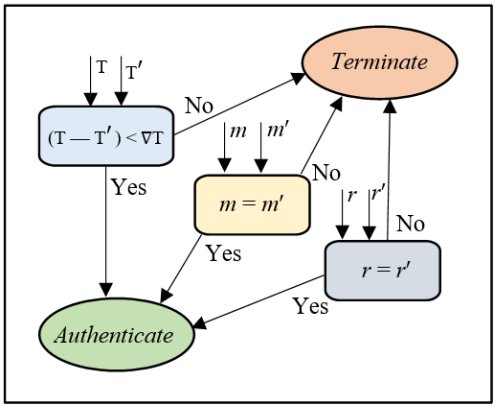

Fig. 4. Authentication decision.

Proof

Proof that the encryption key k use in the sign ID algorithm is the same as to the decryption key k\ used in the unsign ID algorithm.

$K = H(P_{UR} . X) \bmod P.$

$K' = H((Y. P_{UT}) + (Y.r.G)).$

$Y = S. n_R,\ S = (X/r + n_T) \bmod q$

$K' = H(S.n_R .P_{UT} + S.n_R .r.G) \bmod p.$

$= H(X. n_R . n_T .G/r+n_T + X. n_R .r .G/r+n_T). \bmod p.$

$= H((X. n_R .G/ r+n_T)(r+n_T)) \bmod p.$

$= H(X. n_R . G) \bmod p.$

$= H (X. P_{UR}) \bmod p.$

$K'=K$

The encryption key K is equal to the decryption key K' .

4. Simulation and evaluation

In this section, numerical simulation example was performed using laptop CPU@2.90 GHz, 16GB RAM, intel Core i7-4910MQ, Windows 10 (64-bit), Mathematica 11 for scheme execution, analysis and key generation. The elliptic curve prime number and main parameters of the EC are taken from standard 192-bit NIST ECC, the hash function is 128 bit length and the keyed hash output length is 128 bit. The used parameters are in hexadecimal. The generated algorithm parameters are as follows:

SK =(BA583DB1E7AA885B9983B447EA910820944928EB5B44FBBE,F031B33A305674A5D236338B5F362E1879C5A87B1E8EAE9F).

ISK =(D1A2B4124FECB3865A156873F19492B36927046356CD9B4,DE723191E4D7D2BB76FB30AB6DCADD7D8C4FC390C6ADE).

G =(DCFAE88431B518AA62B8284560ADC8089CF762E99AF790A2,EFB15395244E47F5259A93F4893DA06CB4F9DFE36CA99CB).

q =(CC659017BCD3978A00235B692D3BD747).

$X = b390e6357c$

- User A his private key n_T.

$n_T = 8c71645cb3$

- the public key of the Tag is calculated and it is given by

PU_T =(BDA05FCBD7DF25A1AE8A92604229E30872F0A7C41105B1C3,455434A36894A463EF05432815C0937EE94A1793E469D092)

- reader generates a random number as his private key n_R .

$n_R = 8c71645cb3$

- reader calculates its public key PU_R which is given by:

PU_R =(8FCA0870F66502BCAF4438C5D99DE2B69E9482D4C0B3D499,D3A90A1256B6763D16AAB17426E83BAC12863248FA90E976)

4.1 *The multi-message isomorphic authenticated encryption algorithm*

Suppose that a user wants to execute a process between tag and reader, the user selects tag and the reader send and receive messages by doing the following:

Let m_t = 81B4DA77E6B855A31E5C50B130EE690B,

biometric messages stored in the tag and it will be entered to the reader by a biometric connected device, the tag and the reader can authenticate the process

- User A performs the following operations:

1. Generate a random number X
2. Calculate K the output of SHA using eq. (13) with the parameter length of K=128 bit.

   K = C331FC481859B4EC9447E5D2D39F4CF7
3. The random MKG Compute the secret multi-keys to get the " i " isomorphism parameter for the IEC and the keyed hash function by using eq. (4, 9, 10, 11, 12, 14):

   K_t = E5BB5A032664F2AF7A6CC0B1C56E6581,

   i = 71FCBFD1F5FBBE58
4. encrypt the message m_1, m_2, m_3 using IEC in eq. (3, 4, 5):

   C_1 = F8B2EECDA1622D9DAF82F5AED2EDC5B6

   C_2= A4CF7E9457ABF8301B31B7B7C1881472
5. Generate the keyed hash KH values as in eq. (15):

   r_t = DA3DA362D84F5FA7EC408C6F1013C1D4,
6. Calculate the message signature as in eq. (16):

   S_t = D9D92120A0B75118936A2A772DB22766,

   The Tag sends all the signcrypted values $\{C_t, r_t, S_t\}$ to Reader

4.2 *The multi-message un-isomorphic authenticated encryption algorithm*

The reader verifies and unsigncrypted the signcrypted message by the doing following

Calculate K the output of SHA by using eq. (17)

K = C331FC481859B4EC9447E5D2D39F4CF7

the MKG generates K_t to Calculate i using eq. 18 for any message t where t = 1,2,3…

Kt = E5BB5A032664F2AF7A6CC0B1C56E6581

i = 71FCBFD1F5FBBE58

decrypted messages C1, C2,.. Ct by using eq.(7, 8) to get

mt = 81B4DA77E6B855A31E5C50B130EE690B,

Compute the values of keyed SHA by using eq.(14):

r_t' = DA3DA362D84F5FA7EC408C6F1013C1D4,

Verify that the values r1, r2,… , rt = r1, r2,…,rt . m1, m2,… , mt = m′1, m′2,…,m′t If it holds in time , the tag and the reader accept all messages between them.

5. Conclusions

An efficient multi digital identity-based isomorphic authenticated encryption elliptic curve scheme cryptography for RFID applications has been proposed in this paper. The scheme provides both confidentiality and authenticity of

messages, and is designed for resource-constrained devices like smart cards. The proposed scheme offers provable security and efficient encryption and decryption operations, making it suitable for applications with stringent computational requirements. Through a detailed analysis of security and performance, the proposed scheme has been shown to offer improved efficiency while maintaining a high level of security. Overall, this scheme is a promising solution for smart card-based message encryption and authentication verification in various applications, offering a viable approach for secure communication in resource-constrained environments.

References

Ahmed Kamal Ibrahim, Esam A. A. A. Hagras, Adel Alfhar, H. A. El-Kamchochi, “Chaotic Isomorphic Elliptic Curve Cryptography for Secure Satellite Image Encryption”, ITC-Egypt'2021 978-1-6654-4574-0/21/$31.00 ©2021, ADC, Egypt 2021.

Ahmed Kamal Ibrahim, Esam A. A. A. Hagras, Adel Alfhar, H. A. El-Kamchochi, “Dynamic Chaotic Biometric Identity Isomorphic Elliptic Curve (DCBI-IEC) for Crypto Images”, 2020 2nd International (ICCCI 2020), ISBN: 978-1-7281-5799-3, 24 June 2020.

Ahmed Kamal Ibrahim, Esam A. A. A. Hagras, Adel Alfhar, H. A. El-Kamchochi, "Dynamic Fractional Chaotic Biometric Isomorphic Elliptic Curve for Partial Image Encryption", Journal of (ComSIS), 11079-22135-1-RV, 2020-05-02.

Abid ur Rahman, "A Lightweight Multi-Message and Multi-Receiver Heterogeneous Hybrid authenticated encryption Scheme based on Hyper Elliptic Curve", international Journal of Advanced Computer Science and Applications, Vol. 9, No. 5, 2018.

Anuj K. Singh, Arun Solanki, Anand Nayyar, and Basit Q., "Elliptic Curve authenticated encryption-Based Mutual Authentication Protocol for Smart Cards", MDPI, Appl. Sci. 2020, 10, 8291.

Biswojit Nayak, "Elliptic Curve Cryptography-Based authenticated encryption Scheme with a Strong Designated Verifier for the Internet of Things" Advances in Intelligent Systems and Computing vol. 1101, no. 43, pp. 485-492, 2020.

Davood Noori, Hassan Sh., Masood Niazi, "An elliptic curve cryptosystem-based secure RFID mutual authentication for Internet of things in healthcare environment”, Wireless Com Network, (2022) 2022:64.

Elkamchouchi, H. M., Eman F. Abu Elkhair, and Yasmine A. "An efficient proxy authenticated encryption scheme based on the discrete logarithm problem". International J. of Information Technology, 2013.

H. Elkamchouchi, A. Emarah, E. A. A. Hagras. "A New Public Key Signcrypted Challenge Response Identification Protocol Using Smart Card", The 2006 (ICCES'06)", Egypt 2006.

Madhusudhan R., Manjunath Hegde, Imran Memon, " A secure and enhanced elliptic curve cryptography-based dynamic authentication scheme using smart card", vol. 31, no. 11, pp. 203-209, 2018.

Moath Al-Zubi, Ahmad Adel Abu-Shareha, "Efficient authenticated encryption scheme based on El-Gamal and Schnorr ", Multimedia Tools and Applications, Springer Nature 2018.

P.P. Ray, "A survey on internet of things architectures". J. King Saud Univ. Comput. Inform. Sci. vol.30, no.3, pp.291–319, 2018.

Ping Zhang, Yamin Li, and Huanhuan Chi, "An Elliptic Curve authenticated encryption Scheme and Its Application", Wireless Communications and Mobile Computing Volume 2022, Article ID 7499836, 11 pages.

Shamsher Ullah, Xiang-Yang Li, Lan Zhang, "A Review of authenticated encryption Schemes Based on Hyper Elliptic Curve”, 3rd International Conference on Big Data Computing and Communications, vol. 55, no. 17, pp. 218-225, 2017.

Saddam H., Syed S., Mueen U., Jawaid Iqbal, and Chin-Ling Chen, "A Comprehensive Survey on authenticated encryption Security Mechanisms in Wireless Body Area Networks", MDPI, Sensors 2022, 22, 1072.