 CMES, vol.105, no.1, pp.47-68, 2015

Optimal Adaptive Genetic Algorithm Based Hybrid Signcryption Algorithm for Information Security

R. Sujatha[1], M. Ramakrishnan[2], N. Duraipandian[3] and B. Ramakrishnan[4]

Abstract: The functions of digital signature and public key encryption are simultaneously fulfilled by signcryption, which is a cryptographic primitive. To securely communicate very large messages, the cryptographic primitive called signcryption efficiently implements the same and while most of the public key based systems are suitable for small messages, hybrid encryption (KEM-DEM) provides a competent and practical way. In this paper, we develop a hybrid signcryption technique. The hybrid signcryption is based on the KEM and DEM technique. The KEM algorithm utilizes the KDF technique to encapsulate the symmetric key. The DEM algorithm utilizes the Adaptive Genetic Algorithm based Elliptic curve cryptography algorithm to encrypt the original message. Here, for the security purpose, we introduce the three games and we proved the attackers fail to find the security attributes of our proposed signcryption algorithm. The proposed algorithm is analyzed with Daniel of Service (DOS), Brute Force attack and Man In Middle (MIM) attacks to ensure the secure data transaction.

Keywords: Hybrid Signcryption, KEM, DEM, Adaptive Genetic Algorithm, Elliptic Curve Cryptography.

1 Introduction

Basic task of cryptography is to guard the secrecy of messages transmitted over public communication lines. To encode a message in a way that an eavesdropper cannot decode it, for this purpose we use encryption schemes which use some secret information (a key) [Kaoru Kurosawa,Masayuki Abe and Rosario Gennaro (2011)].Traditional public infrastructure (PKI) based cryptosystems permits any

[1] Assistant Professor, Velammal Engineering College, Anna University, India.
[2] Professor & Head, School of Computer Applications, Madurai Kamarajar University, India.
[3] Principal, Velammal Engineering College, Anna University, India.
[4] Associate Professor, Department of Computer Science and Research Centre, S.T. Hindu College, Madurai Kamarajar University, India.

user to decide their own private key and the related public key. Linking the user's identity and the public key, the public key is submitted to a certification authority (CA), which verifies the user's identity and issues a certificate. Therefore, to maintain, PKI based systems need digital certificate management that is too cumbersome. [Adi Shamir (2005)] introduced the notion of uniqueness based cryptography (IBC) to decrease the burden on the CA [Pandu Rangan, Sharmila Deva Selvi and Sree Vivek (2011)]. In an ID-based cryptography, from an arbitrary string corresponding to this user's identity (e.g. an email address, a telephone number, and etc.) public key of each user is easily computable. The private key generator (PKG) then computes a private key for each user, using its master key. This property avoids the requirement of using digital certificates (which contain Certificate Authority (CA)'s signature on each user's public key) and associates implicitly a public key (i.e. user identity) to each user within the system [Jianying Zhou, Joseph K. Liu, Joonsang Baek (2011)].

IBC suffers from an inherent issue called the key escrow problem, i.e. because the PKG is in charge for the generation of the private keys of all the users in the system, it has the capability to get better confidential information meant for any user or sign instead of a legitimate user. [Sattam, Al-Riyami, Kenneth and Paterson (2003)] introduced Certificateless cryptography (CLC) to address the key escrow problem, while avoiding the use of certificates and the need for a CA. Partitioning private keys into two components is the principle behind CLC: an identity based partial private key (known to the PKG) and a non-certified private key (which is unknown to the PKG). This technique has the ability to combine the best features of IBC and PKI. A number of certificateless encryption and signature schemes resulting from identity based encryption and signature schemes have been efficiently constructed and were established safe under different assumptions [Pandu Rangan, Sharmila Deva Selvi and Sree Vivek (2011)].

Confidentiality and authenticity are the security goals that are required for a secure communication through an insecure channel. Encryption schemes are used to attain confidentiality and digital signature schemes suggest enforceability [Sharmila Deva Selvi, Sree Vivek and Pandu Rangan (2010)]. The security of communications can be provided by the encryption and digital signature which are the two fundamental cryptographic mechanisms. They have been viewed as significant but distinct building blocks of various cryptographic systems, until the before decade [Mohsen Toorani, Ali , and Beheshti (2009)]. In public key schemes, a traditional method is to digitally sign a message then followed by an encryption (signature-then-encryption) that has two problems: Low effectiveness and high cost of such summation, and the case that any arbitrary scheme cannot guarantee the security. The signcryption is a comparatively new cryptographic technique which in a sin-

gle logical step thought to fulfill the functionalities of digital signature and encryption, and can efficiently reduce the computational costs and communication overheads in comparison with the traditional signature-then-encryption schemes [Mohsen Toorani ,Ali and Beheshti(2010)]. [Yuliang Zheng(1997)] proposed the first digital signcryption scheme that offers both confidentiality and authentication in a single logical step with lower computational cost and communication overhead than sign then encrypt (StE) or encrypt then sign (EtS) approach. Many signcryption schemes were proposed since then [Sharmila Deva Selvi, Sree Vivek and Pandu Rangan (2010)].

To perform secrecy communication for large messages hybrid encryption scheme can be used that separates the encryption into two parts: one part uses public key techniques to encrypt a one-time symmetric key and the other part make use of the symmetric key to encrypt the actual message. In this type of construction, the public key part of the algorithm is called as Key Encapsulation Mechanism (KEM) and the symmetric key part is called as Data Encapsulation Mechanism (DEM) [Fagen Li, Masaaki Shirase and Tsuyoshi Takagi(2009)]. [Cramer and Shoup (2004)] proposed a standard model where the asymmetric and symmetric parts of the cryptosystem are formally separated into an asymmetric KEM and a symmetric DEM. The authors here proposed a separate security criteria for the KEM and the DEM and observed that if the criteria is satisfied it guarantees that the overall encryption scheme was secure. Dent [Alexander Dent (2005)] extended the above proposed model to the signcryption setting by proposing new security criteria for the KEM and the DEM. All the previous constructs for certificateless cryptosystem were based on bilinear pairing [Jong Hwan Park, Kyu Young Choi, Yeon Hwang and Dong Hoon Lee (2007)]. [Joonsang Baek, Reihaneh Safavi and Willy Susilo(2005)] proposed the first certificateless cryptosystem without using the bilinear pairing. Usually certificateless cryptosystem is prone to key replacement attack because if the public keys are not certified anyone can replace the public key of any legitimate user in the system. The challenging task in the design of certificateless cryptosystem is to come up with a scheme that provides security even if the public key of the user is replaced. The excellent survey by Dent [Alexander Dent (2008)] gives a comprehensive overview of the design of provably secure certificateless encryption scheme [Pandu Rangan, Sharmila Deva Selvi and Sree Vivek (2011)].

2 Related Works

[Aftab Ali,aider Abbas and Farrukh Aslam Khan (2013)], introduced Fuzzy Attribute-Based Signcryption (FABSC), a innovative security component that made a appropriate tradeoff in the middle of security and versatility. FABSC powers fuzzy

Attribute-based encryption to empower information encryption, access control, and digital signature for a patient's medicinal data in a BAN. It joined digital signature and encryption, and gave privacy, genuineness, unforgeability, and intrigue safety. They hypothetically demonstrated that FABSC is proficient and attainable. They likewise broke down its security level in pragmatic BANs. They demonstrated that their plan was indistinct against versatile selected cipher text assaults under the bilinear Diffie-Hellman reversal issue and existential unforgeability against versatile picked messages assaults under the q-strong Diffie-Hellman issue in the irregular oracle model. Their plan had the accompanying preferences. To begin with, it accomplished secrecy, trustworthiness, verification, and non-renouncement in a sensible single step. Second, it permitted a sensor hub in a character based cryptography to make an impression on an Internet host in an public key foundation. Third, it splitted the signcryption into two stages: i) offline stage; and ii) online stage. In the offline stage, most substantial reckonings were carried out without the information of a message. In the online stage, just light processing's were carried out when a message was accessible. Their plan was extremely suitable to give a security response for coordinating WSN into the IoT.

[Andrew Markham , Bangdao Chen and Zheng Yan (2013)] considered the likelihood of employing the human intuitive channel as a part of BSN applications. Legitimately outlined HH and HD channels offered the validness and trustworthiness of information exchanged. They might be useful to secure data exchanged over DD channel which could be caught, erased, or adjusted by the aggressor. What's more, they have proposed a gathering responsibility convention model. The human-intelligent channels-based gathering duty conventions were additionally examined. They have examined the conceivable assaults and countermeasures. Thirdly, ECDH-SHCBK and ECDH-HCBK are outlined. MITM assault, which was the primary issue of ECDH, which was exterminated. Contrasting with key pre-distribution conventions, their two conventions can without much of a stretch change bargained and lapsed keys. In the meantime, they give a conceivable method for progressively designating IDs in a system.

[Gang Yu, Xiaoxiao Ma, Yong Shen and Wenbao Han (2010)] presented in the beginning a security model for identity based generalized signcryption that is more absolute than existing model. Secondly, an identity based generalized signcryption scheme was proposed. Thirdly, in this entire model, the security proof of the new scheme was given. The new scheme has less implementation complexity compared with existing identity based generalized signcryption. Additionally, with the existing normal signcryption schemes, the new scheme has similar computation complexity. At first they characterized the formal definition of CLGSC; then, for those primitive, they gave the security thoughts; later, the CLGSC plan was exhibited.

[Nadia and Al Saidi (2012)] displayed a generally composed signcryption plan employing the compression capacity of fractal encoding and decoding strategy. Right away the message is encrypted applying a skilled encoded strategy, and a safe advanced digital signature is developed utilizing hash function. The fractal codes of a digital signature are added to the encoded message to be transmitted, developing the favorable circumstances of fractal image coding (FIC). The hash function is developed for the acquired encoded message, after decryption at the receiver side. To recognize the respectability of the message, by contrasting the acquired hash and the ascertained one the check procedure is achieved. The message is recognized just if the confirmation methodology is achievable, or else the message is overlooked. To demonstrate that the plan gives important security necessities, the proposed plan is investigated and examined from the aggressor perspective.

[Wenjian Xie and Zhang (2010)] presented a competent certificateless signcryption scheme. This scheme is based on bilinear pairing and for signcrypt and unsigncrypt phases, it required only two pairing operations. Based on the hardness assumptions of DLP, CDHP, q-SDHP and q-BDHIP, the security of their scheme is developed. [Hui fang Ji , Wenbao Han and Long Zhao (2012)] presented a certificateless generalized signcryption (CLGSC). Initially they defined the formal definition of CLGSC; then, for those primitive, we gave the security notions; later, the CLGSC scheme is proposed. [Prashant Kushwah and Sunder Lal (2010)] presented an easy certificateless generalized Signcryption and also a well-organized identity based generalized signcryption scheme.

[Gang Yu, Xiaoxiao Ma, Yong Shen and Wenbao Han (2010)] presented in the beginning a security model for identity based generalized signcryption that is more absolute than existing model. Secondly, an identity based generalized signcryption scheme was proposed. Thirdly, in this entire model, the security proof of the new scheme was given. The new scheme has less implementation complexity compared with existing identity based generalized signcryption. Additionally, with the existing normal signcryption schemes, the new scheme has similar computation complexity. [Pengcheng Li, Mingxing, Xiao Li and Wengang Liu (2010)] presented a well-organized certificateless signcryption scheme. They were considering a more realistic adversarial model and proving the security against insider attacks which guarantees secrecy and validity, and verified it secure under the random oracle model. Their scheme does not require pairing to signcrypt a message and only needs two pairing operations in designcrypt stage. It is also proved in performance analysis that their scheme was competent and realistic.

[Alexander Dent, Marc Fischlin, Mark Manulis and Martin Stam (2010)] provided a formal treatment of secrecy for such schemes. Both in the random oracle model and the standard model, they offered constructions meeting their notions. As part

of this they showed that than Fiat-Shamir signatures full domain hash signatures attain a weaker level of secrecy. Then they examined the connection of confidential signatures to signcryption schemes. For confidential signature schemes and high-entropy messages, they also presented formal security models for deterministic signcryption schemes for high-entropy and low-entropy messages, and prove encrypt-and-sign to be secure. At last, they showed that one can derandomize any signcryption scheme in our model and achieve a protected deterministic scheme.

[Mohsen Toorani, Ali and Beheshti (2009)] presented elliptic curve-based signcryption scheme that concurrently provided the security attributes of message confidentiality, verification, integrity, unforgeability, and non-repudiation. Their algorithm also has the attribute of public verifiability so any third party can verify the signature without any need for the private keys of the participants. Their algorithm also has the attribute of forward secrecy of message confidentiality so even if the sender's private key is revealed, no one else can extract the plaintext of the previously signcrypted texts. It has great advantages to be deployed in resource-constrained devices such as mobile phones, as their algorithm is based on elliptic curve cryptography and uses symmetric ciphering for encrypting messages. As a one-pass scheme, their algorithm is also so attractive for security establishment in store-and-forward applications such as E-mail and Short Message Service.

[Nadia and Al Saidi (2012)] presented a well-organized signcryption scheme using the compression ability of fractal encoding and decoding scheme. At first the message is encrypted using a capable encrypted method, and a secure digital signature is constructed using hash function. The fractal codes of a digital signature are added to the encrypted message to be transmitted, using the advantages of fractal image coding (FIC). The hash function is constructed for the received encrypted message, after decryption at the receiver side. To identify the integrity of the message, by comparing the received hash with the calculated one the verification process is performed. The message is acknowledged only if the verification process is success, or else the message is ignored. To prove that the scheme provides necessary security requirements, the proposed scheme is analyzed and discussed from the attacker viewpoint.

3 Problem Definition

In existing cryptographic schemes, the message and sender's signature are achieved after decrypting the encrypted message. Then the signature is verified using sender's public key. Thus, anyone who knows the sender's public key can verify the message easily. But in signcryption, in order to verify the signature the receiver has to use the own private key. The major disadvantage of AES algorithm based signcryption technique is that there is a need to get the key to the party with whom to share the

data. So we need to have a very secure way to get the key to the other party. These existing encryption scheme is only useful when encrypting the own information as opposed to when sharing encrypted information. The main contribution of this research is to obtain high confidentiality and integrity in the field of information security.

4 Proposed Method Of Hybrid Signcryption Algorithm Based On ECC and Adaptive GA

Our ultimate aim is to build the optimal signcryption based on KEM and DEM, the KEM is performed based on the Key Derivation Function (KDF) using the secure pseudo random number generation technique. The KEM algorithm is used for transferring the secret symmetric key; to share the secret key the additional key will be required for different cryptographic reason such as encryption process, integrity protection algorithm. For this purpose here, we used the key derivation function to derive secret key from any other key or known information using the secure pseudo-random number functions.

Fig. 1 represents the block diagram of the entire proposed methodology.

The various properties of KDF, functionality of pseudo-random number generator and the key expansion function. In conventional signcryption algorithm, the DEM is performed based on the AES encryption algorithm. In our proposed method, the AES algorithm is replaced by optimal Elliptic Curve Cryptography (ECC) algorithm based on Adaptive Genetic Algorithm (AGA).

4.1 Signcryption algorithm

The key generation algorithm: The probabilistic algorithm that takes any two prime numbers (p, q) as input and gives the output public key $P_k(n,e)$ and private key $S_k(n,d)$ and symmetric key C_k (p, q) Key generation algorithm $\rightarrow (P_k, S_k, C_k)$.

Data encryption mechanism (DEM): The probabilistic algorithm (AES) that takes original message M and the symmetric key C_k and gives the output ciphertext CM. (M, C_k) Key generation algorithm $\rightarrow (CM)$.

Key derivation key: The probabilistic algorithm that takes input as an integer n and length of an integer*nLen*and it gives the output (z, Z) where z a random integer is selected from 0 to $n-1$ and Z is *nLen* string value in the form of most significant bit first which is transformed from z. $(n,$ *nLen*$)$ Key derivation key $\rightarrow (z, Z)$.

Encryption: The probabilistic algorithm that takes input random integer z and receiver's public key $P_k(n,e)$ it produces the output (c, C) where c is the ciphertext of z and C is *nLen* string value in the form of most significant bit first which is

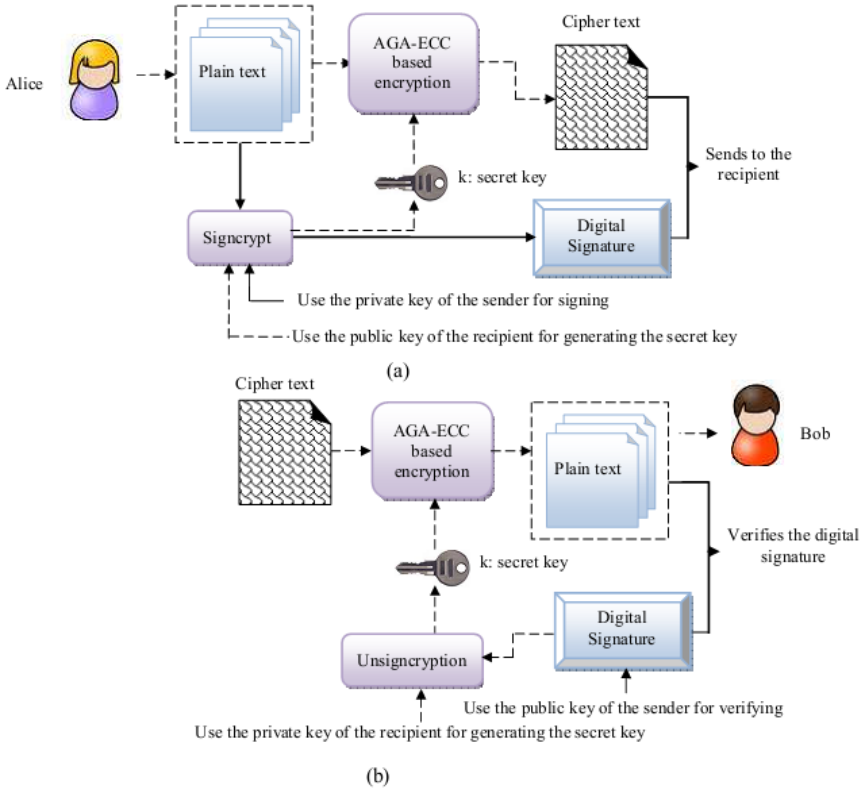

Figure 1: Proposed Optimal Signcryption algorithm.

transformed from c. $(P_k, (n,e))$ Encryption $\rightarrow (c, C)$. In our proposed method, this encryption can be done by ECC algorithm.

Key derivation function: The probabilistic algorithm (hashing algorithm (MD5)) that takes input random integer Z and length of the key encryption key *kekLen* is derived from Z and it gives the output (KEK)key encryption key. $(Z, kekLen)$ Key derivation function $\rightarrow (KEK)$.

Wrapping function: The probabilistic algorithm (Wrap) that takes input as symmetric key C_k and key encrypting key (KEK) and gives the output wrapped key WK. (C_k, KEK) Wrapping function $\rightarrow WK$.

Concatenation: The probabilistic algorithm that takes input wrapped keyWK, ciphertext C and outputs encapsulated key EK.

Signcryption: The probabilistic algorithm that takes input ciphertext CM, sender's private key $S_k \quad (n,d)$, encapsulated key EK and outputs the signcrypted data (δD). $(CM, S_k, (n,d), EK)$ Signcryption $\rightarrow (\delta D)$.

Unsigncryption process

Signature verification: The probabilistic algorithm that takes input sender's public key $S(P_k)$, signcrypted data δD, and if the produced output will be 1 then the signature is valid else it returns $\perp$ which represents invalid signature. $(S(P_k), \delta D)$

$$\text{Signature verification} \rightarrow 1 \; or \; \perp.$$

Detach: The probabilistic algorithm that takes input EK and outputs the wrapped key WK, cipher text C.

Decryption: The probabilistic algorithm that takes input cipher text C the receiver's private key $S_k(n,d)$ it produces the output Z.

Key derivation function: The probabilistic algorithm (hashing algorithm (MD5)) that takes input integer Z and length of the key encryption key *kekLen* is derived from Z and it gives the output (KEK) key encryption key. $(Z, kekLen)$

$$\text{Key derivation function} \rightarrow (KEK).$$

Unwrapping function: The probabilistic algorithm (Wrap) that takes input as wrapped key WK and key encrypting key (KEK) and gives the output symmetric key C_k. (WK, KEK)

$$\text{Wrapping function} \rightarrow C_k.$$

Data encryption mechanism (DEM): The probabilistic algorithm (AES) that takes ciphertext CM and the symmetric key C_k and gives the output original message M. (CM, C_k)

$$\text{Key generation algorithm} \rightarrow (M).$$

Pseudo code for Signcryption Algorithm

p	a large prime number
q	a prime number which divides
g	an element in Z_p with order q modulo p
m	a message
$E_k(m)$	symmetric encryption algorithm with secret key k
$D_k(m)$	symmetric decryption algorithm with secret key k
$hash$	a one-way hash function
$KH_{k'}$	a keyed one-way hash function with key k'
x_a	sender's private key, randomly chosen from $1 \leq x_a \leq q-1$
y_a	sender's public key, $y_a \equiv g^{xa} \pmod p$
x_b	receiver's private key, randomly chosen from $1 \leq x_b \leq q-1$
y_b	receiver's public key, $y_b \equiv g^{xb} \pmod p$

Sender's Signcryption

1. Select x uniformly and randomly from $1 \leq x \leq q-1$.
2. Calculate $k = hash(y_b^x \pmod p)$.
3. Split k into k_1 and k_2 of appropriate length.
4. Calculate $r = KH_{k2}(m)$.
5. $s \equiv x/(r+x_a) \pmod q : SCS1$
   $s \equiv x/(1+x_a.r) \pmod q : SCS2$
6. $c = E_{K_1}(m)$
7. Send the signcrypted text (c,r,s).

Receiver's Unsigncryption

1. Recover k using r,s,g,p,q,y_a,x_b
   $k = hash((y_a.g^r)^{s.x_b} \pmod p) : SCS1$
   $k = hash((y_a^r.g)^{s.x_b} \pmod p) : SCS2$
2. Split k into k1 and k2.
3. $m = D_{k1}(c)$
4. Calculate KH_{k2}(m) and accept m as a valid message if KH_{k2}(m)= r.

4.2 Elliptic curve Cryptography (ECC)

ECC based encryption

Here in the signcryption algorithm, we have utilize an ECC method for create a private and public key for the encryption. ECC has certain advantages when compared to the other encryption algorithms such as short key, high security, high speed, small storage space and low bandwidth. The private and public keys are generated by the ECC method makes the data more secure for embedding and also the generated keys are robust. The key generation and formation are described below.

Key Generation by ECC

Elliptic Curve Cryptography (ECC) is also known as public key cryptography, it usually have a couple of keys, a public key and a private key, and a set of operations related with the keys to do the cryptographic operations. Small key size is the main advantage of ECC.

The operations of elliptic curve cryptography are defined over two finite fields: Prime field and Binary field. The suitable field is selected with finitely huge number of points for cryptographic operations. Here, we have used prime field operations by choosing a prime number P_{rm}, and finitely large numbers of basic points are generated on the elliptic curve, such that the generated points bp are between 0 to Z. Then, we randomly select one basic point $p_r(R_1,R_2)$ for cryptographic operations and this point satisfies the equation of the elliptic curve on a prime field, which is defined as,

$$v^2 \mod P_{rm} = u^3 + \alpha u + \beta \mod P_{rm} \tag{1}$$

In our proposed methodology, AGA is applied in this point, ie., instead of randomly selecting one basic point $p_r(R_1,R_2)$, here we are calculating the optimal point from bp which satisfies the constraint. This AGA optimization is described in section 4.3. In Equ. (2), α and β are the parameters that defining the curve, and u and v are the coordinate values of the generated points bp. We optimal basic point p_r to perform the cryptography, we need to select a private key pv_{ky} on the sender side, which is also an optimal integer less than P_{rm} and generate a public key pu_{ky} $=pv_{ky} * p_r$. Now each text T_{xt} has individual private pv_{ky} and public keys pu_{ky}. The private and public values are added and that decimal value is converted into the binary value. Then least significant bit is chosen. This DataStream is used for the encryption of text.

Encryption and Decryption

The data is encrypted using the ECC technique. The message is encrypted by using ECC and sends that encrypted message to the receiver side. The encrypted message is send in the form of,

$$\gamma = (E_m, C_j) \tag{2}$$

$$E_m = O_m * p_r \tag{3}$$

$$q_j = (u,v) + O_m * (S(p_v) * p_r) \tag{4}$$

In Equ. (2), E_m is encrypted message it is calculated by Equ. (3) i.e. the multiplication of the original message O_m with the basic pointp_r and q_j is computed by Equ. (4). In Equ. (4) $S(pv_{ky})$ is the private key of the sender. This message γ is send to the receiver.

4.3 Adaptive Genetic Algorithm (AGA)

As the convergence rate of the conventional GA is low, AGA is utilized in our proposed technique to speed up the convergence rate. The adaptive GA is employed with the help of Cauchy mutation in the mutation operator. Cauchy mutation is the mutation operator introduced in the genetic algorithm to speed up GA process and also to enhance the GA performance. Here, the private key pv_{ky} of the ECC is selected by using AGA. The major drawback of ECC is the primer field selection which is randomly chosen. In order to overcome the issue, here we use AGA for selecting the prime number for optimal private key pv_{ky}. Thus the GA with Cauchy mutation operator will produce the optimal prime number which is used for key generation process and thus the optimal features will be obtained. The GA with Cauchy mutation operation is shown below.

Adaptive Genetic Algorithm (GA) is a meta heuristic algorithm that minimizes the natural evolution process. Most probably, it used to spawn elucidations to optimization and search problems. It spawns elucidations to optimization problems using techniques stirred by natural evolution, such as inheritance, mutation, selection, and crossover.

Initial Phase: Initially the populations of the chromosomes $x_i, (i = 1,2,...T)$ are generated randomly. T denotes the size of the population. The chromosome (x_i) contain the some integer values randomly generated which are less than the prime number selected (γ_i).

Fitness function: Fitness value of each parameter is calculated and the chromosome which has the highest fitness value is selected as the best chromosome.

$$F(i,j) = \min(er) \tag{5}$$

In Eq. (5), $er(i,j)$ is the error rate of t^{th} parameter.

Selection of Chromosomes: One or more parent chromosomes are selected based on the 'T/2' best chromosomes which have minimum fitness and new solution is created.

Crossover: Single point crossover is performed at the crossover rate of (C_r) and hence ('T/2') offspring are obtained. In every crossover operation, (TC_r) genes are exchanged between corresponding parents.

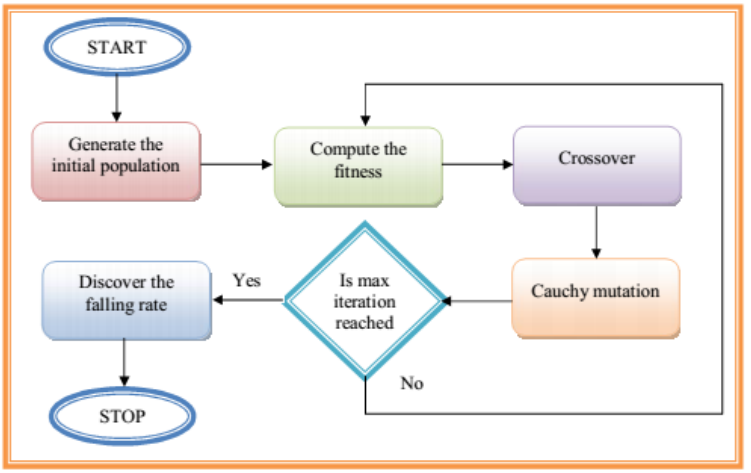

Figure 2: Flowchart of the Adaptive Genetic Algorithm.

Mutation: Individuals are perturbed probabilistically to bring a change in the individuals. Using mutation operator, there is a probability that some new features might appear due to change in the chromosome. Cauchy mutation is used to mutate the individuals according to the equation given below. Mutation is performed on the basis of pre-determined mutating probability. In case the Cauchy mutation is applied, random variable 'x' is a Cauchy distribution. The Cauchy distribution function is defined as

$$F(x) = \frac{1}{2} + \frac{1}{\pi} \arctan(x) \tag{6}$$

Updation: In the sixth step initial chromosome replaced by new chromosome. Next to the mutation process the initial population chromosomes are replaced by the ('T/2') elected and new 'T/2' offspring chromosomes.

Termination Criteria: The process is continued until it meets the termination criteria. Thus the optimal private key obtained by using the AGA is substituted in $pu_{ky} = pv_{ky} * p_r$ to get the optimal encryption in ECC based signcryption algorithm.

5 Results and Discussion

The proposed methodology for secured data transaction in a network is implemented in Java with user defined network. Some of the screenshots are described as follows

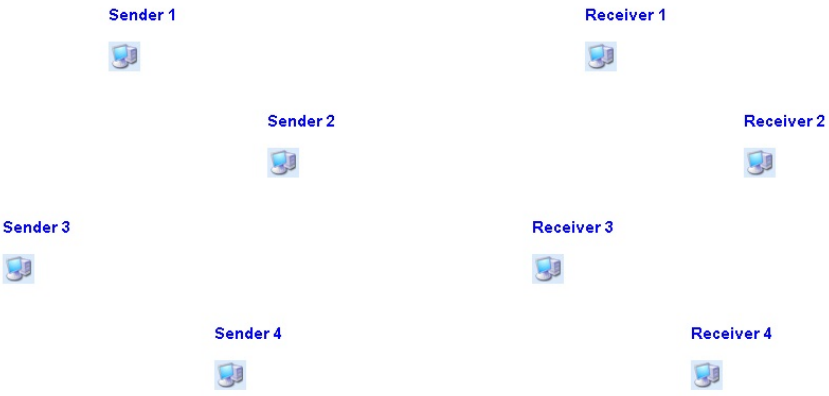

Figure 3: Network representation.

Here we organized a network with some nodes in which the data transfer to be held. Initially the sender node has to select the receiver node to which node the data to be transferred. The sender can transfer the data to any node inside the network in a secured way based on our optimal signcryption algorithm. This can be represented in Fig. 3 and Fig. 4.

Here in Fig. 4 the Receiver1 is selected by the sender1 node for data transfer. After selecting the receiver node, the sender will tranfer the data or message which is presented in Fig. 5.

While transfering the data, hackers or unauthorized node may try to hack the data. We analyzed 3 types of attacks such as DOS, Brute Force and Man In Middle attacks. The Hackers will try to break the secret keys to get the data. In Fig. 6 DOS attack is presented and the attacker hacked some data which is 20% similar to the original data. Once the receiver got the message successfully, the it sends the acknowlegement to the sender which is described in Fig. 7.

5.1 Comparative Analysis

Here Tab. 1 represents the encryption time of various cryptographic encryption algorithm with various lengths. Our proposed ECC algorithm outperforms the existing algorithms with less encryption time.

The proposed optimal ECC algorithm encrypts the text in minimum time when compared to the existing algorithm. Here in Tab.1, the encryption algorithms are tested with varying length text messages such as “Welcome”, “Encryption” and “Where are you?”. Our proposed algorithm utilizes only less amount of time.

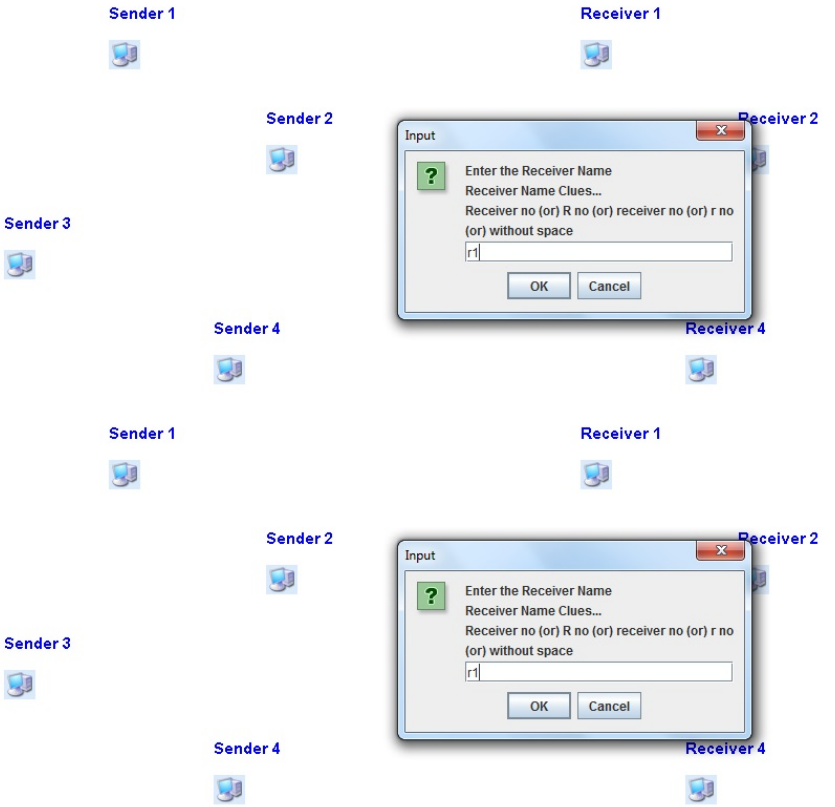

Figure 4: Receiver node selection by the Sender 2.

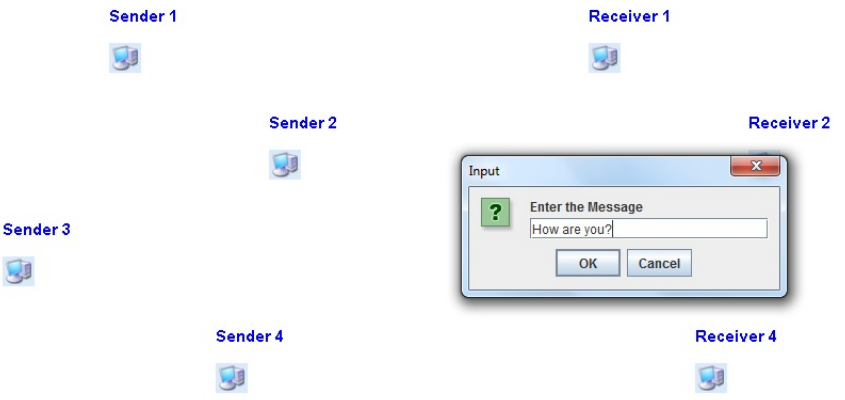

Figure 5: Data tranfer process.

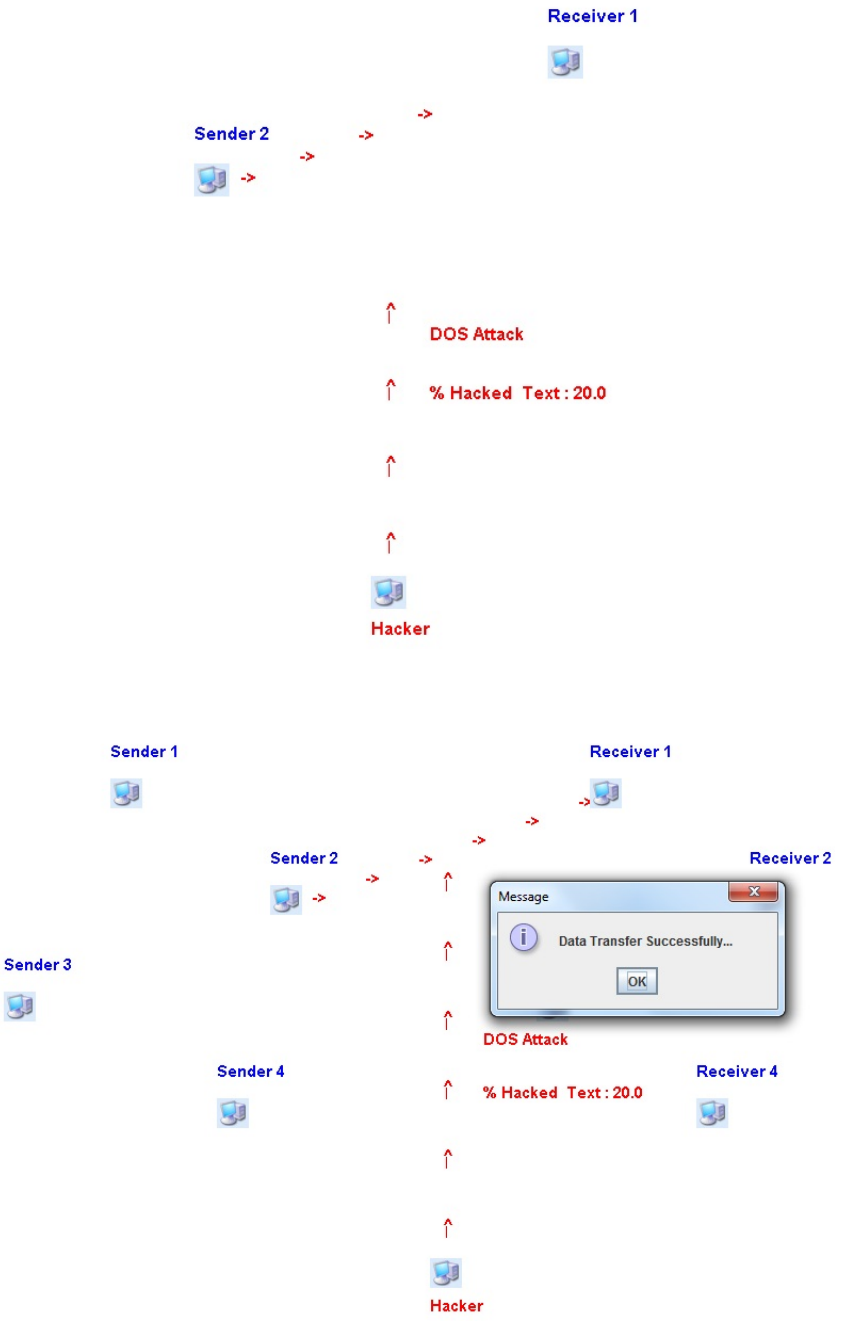

Figure 7: The Data transferred to the receiver 1.

Table 1: Encryption time analysis of various cryptographic algorithms.

Encryption algorithm	Encryption time (in ms)		
	Length 7 (Welcome)	Length 10 (Encryption)	Length 12 (Where are you?)
AES	324	394	593
DES	316	389	582
RSA	310	386	578
Conventional ECC	291	358	491
Proposed AGA-ECC	286	352	497

Our proposed security system is analyzed with various attacks such as brute force attack, Daniel of Service (DOS) and Man in Middle (MIM) attack. While using these attacks, the security of the system is evaluated in terms of key breaking time, decrypted text and similarity of the hacked text.

Table 2: Key Similarity.

Algorithm	Similarity (in %)		
	Brute force attack	DOS attack	MIM attack
AES	48.5566	33.6322	24.6358
DES	44.4444	30.5669	21.8544
RSA	29.6296	26.5622	18.6635
Conventional ECC	23.1072	34.8718	15.3846
Proposed AGA-ECC	24.6913	22.2222	14.8148

The similarity of the hacked text can be analyzed in Tab. 2 and Tab. 3. The similarity between the original and the hacked text is evaluated by employing the distance measure. In Tab. 3, the hacked texts are presented. The similarity measure is described in Tab. 2, in which the value of similarity is low for our proposed optimal ECC algorithm. It provides high security when compared to the other encryption algorithms.

Fig. 8 represents the key breaking time for various encryption algorithm while employing various security attacks. In this, our proposed algorithm is fighting strongly with attacks and the encryption key can be broke after a long time only. Here the key breaking time is better for our proposed algorithm while the others performs less.

Table 3: Decrypted Text.

Algorithm	Decrypted text		
	Brute force attack	DOS attack	MIM attack
AES	eareou?	ar you?	We aru?
DES	reareu?	We you?	Weayou?
RSA	ere ou?	Waeyou?	Wray o?
Conventional ECC	Wheeyu?	Whe ou?	W reou?
Proposed AGA-ECC	Wheeyu?	haryou?	W ero?

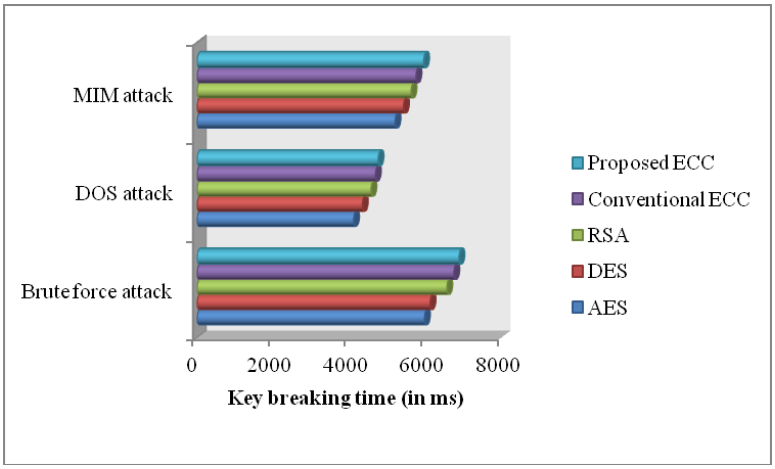

Figure 8: The comparison of key breaking time between proposed and existing algorithms.

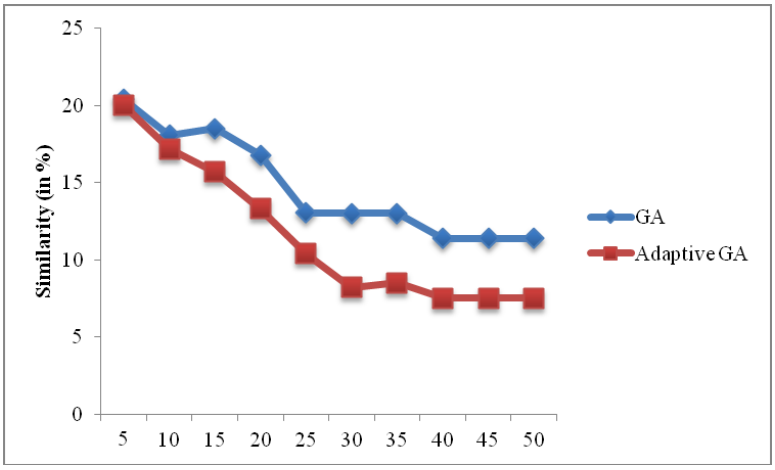

Figure 9: Fitness convergence comparison.

While using the optimization algorithm the fitness convergence plays the major role. Here in Adaptive GA, The similarity is used as the fitness, ie., the similarity between original and hacked text. This is the minimization problem so the fitness converges towards zero. Fig. 9 represents the convergence graph for both conventional GA and adaptive GA. Our Adaptive GA has minimum fitness when compared to GA.

Table 4: Computational Time analysis with existing techniques.

Algorithm	Time (in ms)
Conventional Signcryption	483
Signcryption with ECC	464
Signcryption with optimal ECC based on GA	443
Signcryption with optimal ECC based on AGA	412

The computational time is the most important process in the information transaction security. Cryptographic algorithms play a major role in it. The complexity of the algorithm depends upon the encryption time. Here Tab. 4 describes the computational time of our proposed Signcryption with optimal ECC based on AGA algorithm with other existing techniques. From the above results we observed that the proposed signcryption scheme outperforms the existing algorithm and leads to the secured data transaction.

6 Conclusion

The hybrid signcryption is based on the KEM and DEM technique in which the KEM algorithm utilizes the KDF (key derivative function) technique to encapsulate the symmetric key. The KDF generates key encryption key (KEK) to encrypt the symmetric key based on the random integer and Optimal ECC encryption algorithm. At the receiver side, the designcryption algorithm processes the signcrypted data then it utilizes the KDF technique to find the key encryption key with the help of the private key of the receiver. Afterwards the decapsulation process helps to find the symmetric key with the help of the key encryption key. The decryption process is applied to the cipher text to obtain the original message based on the symmetric key. From the encryption time, key similarity, key breaking time and computational time our proposed method outperforms the existing techniques.

References

Al-Riyami, S. S.; Paterson, K. G. (2003): Certificateless public key cryptography. *Advances in Cryptology ASIACRYPT*, *Lecture Notes in Computer Science* vol. 2894, pp. 452–473.

Al-Saidi, N. M. (2012): An efficient signcryption method using fractal image coding scheme. *International Journal of Applied Mathematics and Informatics*, vol. 6, no. 4, pp. 189-197.

Baek, J.; Safavi-Naini, R.; Susilo, W. (2005): Certificateless public key encryption without pairing in Information Security. *ISC 2005, Lecture Notes in Computer Science, Springer*, vol. 3650 , pp. 134–148.

Cheng, Z.; Comley, R. (2005): Efficient certificateless public key encryption. *Proceedings of Eurocrypt 91, LNCS 547.*

Chowhan, S. S.; Shinde, G. N. (2008): Iris Biometrics Recognition Application in Security Management. *ICCES, Tech. Science Press, Academic Journals,* vol. 6, no. 1, pp. 1-12.

Cramer, R.; Shoup, V. (2004): Design and analysis of practical public key encryption schemes secure against adaptive chosen ciphertext attack, *SIAM Journal on Computing,* vol. 33, no. 1, pp.167-226.

Dent, A. W. (2008): A survey of certificateless encryption schemes and security models. *International Journal of Information Security*, vol. 7, no. 5, pp. 349–377.

Dent, A. W.; Fischlin, M.; Manulis, M.; Stam, M.; Schröder, D. (2010): Confidential Signatures and Deterministic Signcryption. *Proceedings of 13th International Conference on Practice and Theory in Public Key Cryptography*, vol. 6056, pp. 462-479.

Dent, A. W. (2005): Hybrid Signcryption Schemes with outsider Security. *Information Security, Lecture Notes in Computer Science,* vol. 3650, pp. 203-217.

Dent, A. W. (2005): Hybrid Signcryption Schemes with Insider Security. *Information Security and Privacy, Lecture Notes in Computer Science*, vol. 3574, pp. 253-266.

Dodis, Y.; Gennaro, R.; Håstad, J.; Krawczyk, H.; Rabin, T. (2004): Randomness Extraction and Key derivation Using the CBC, Cascade, and HMAC Modes. *In Advances in Cryptology-CRYPTO 2004, Springer Berlin Heidelberg*, pp. 494-510.

Huang, X.; Chen, B.; Markham, A.; Wang, Q.; Yan, Z.; Roscoe, A. W. (2013): Human interactive secure key and Identity exchange protocols in body sensor networks. *Information Security, IET*, vol. 7, no. 1, pp. 30-38.

Irum, S.; Ali, A.; Khan, F. A.; Abbas, H. (2013): A Hybrid Security Mechanism for Intra WBAN and Inter WBAN Communication. *International Journal of Distributed Sensor Networks,* vol. 2013, pp. 1-11.

Huifang, J.; Wenbao, H.; Long, Z. (2012): Certificateless Generalized Signcryption. *International conference on medical physics and Biomedical Engineering*, vol. 33, pp. 962-967.

Kurosawa, K.; Abe, M.; Gennaro, R. (2011): Tag-KEM/DEM: A New Framework for Hybrid Encryption and a New Analysis of Kurosawa-Desmedt KEM in proceedings of *Eurocrypt*, pp. 128-146.

Kushwah, P.; Lal, S. (2010): Efficient Generalized Signcryption Schemes. *ACR Cryptology ePrint Archive*, pp. 346.

Li, P. C.; He, M. X.; Li, X.; Liu, W. G. (2010): Efficient and Provably Secure Certificateless Signcryption from Bilinear Pairings, *Journal of Computational Information Systems*, vol. 6, no. 11, pp. 3643-3650.

Li, F.; Shirase, M.; Takagi, T. (2009): Certificateless Hybrid Signcryption. *Information Security Practice and Experience*, *Lecture Notes in Computer Science*, vol. 5451, pp. 112-123.

Liu, J. K.; Baek, J.; Zhou, J. (2011): Online/Offline Identity-Based Signcryption Revisited. *Journal of Information Security and Cryptology*, vol. 6584, pp. 36-51.

Liu, J. K.; Au, M. H.; Susilo, W. (2007): Self-generated-certificate public key cryptography and certificateless signature/encryption scheme in the standard model, Extended abstract, *ASIACCS , Proceedings of the 2nd ACM symposium on Information, Computer and Communications Security,* pp. 273–283.

Park, J. H.; Choi, K. Y.; Hwang, J. Y.; Lee, D. H. (2007): Certificateless public key encryption in the selective ID security model (without random oracles). *Lecture Notes in Computer Science*, *Springer.* vol. 4575, pp. 60–82.

Selvi, S. S. D.; Vivek, S. S.; Rangan, C. P. (2010): Identity Based Public Verifiable Signcryption Scheme. *Proceedings of the 4th international conference on Provable security*, vol. 2241, pp. 244-260.

Selvi, S. S. D.; Vivek, S. S.; Rangan, C. P. (2011): Cryptanalysis of Certificateless Signcryption Schemes and an Efficient Construction Without Pairing. *Journal of Information Security and Cryptology*, vol. 6151, pp. 75-92.

Shamir, A. (2005): Identity-based cryptosystems and signature schemes, *Advances in Cryptology, CRYPTO - 1984, Lecture Notes in Computer Science, Springer*, vol. 196, pp 47–53.

Shoup, V. (2000): Using Hash Functions as a Hedge against Chosen Ciphertext Attack. *Advances in Cryptology — EUROCRYPT,Lecture Notes in Computer Science,*

vol. 1807, pp. 275-288.

Sun, Y.; Zhang, F.; Baek, J. (2007): Strongly secure certificateless public key encryption without pairing. *Cryptology and Network Security - CANS, Lecture Notes in Computer Science,* vol. 4856, pp. 194–208.

Toorani, M.; Beheshti, A. A. (2009): An Elliptic Curve-based Signcryption Scheme with Forward Secrecy. *Journal of Applied science, 2009,* vol. 9, pp. 1025-2035.

Toorani, M.; Beheshti, A. A. (2010): Cryptanalysis of an Elliptic Curve-based Signcryption Scheme. *International Journal of Network Security*, vol. 10, pp. 51-56.

Xie, W.; Zhang, Z. (2010): Efficient and Provably Secure Certificateless Signcryption from Bilinear Maps. *Proceedings of International Conference on Wireless Communications, Networking and Information Security*, pp. 558- 562.

Yu, G.; Ma, X.; Shen, Y.; Han, W. (2010): Provable Secure Identity Based Generalized Signcryption Scheme. *Journal of Theoretical Computer Science*, vol. 411, no. 40-42, pp. 3614-3624.

Zheng, Y. (1997): Digital signcryption or how to achieve cost (signature & encryption) $<<$ cost(signature) + cost (encryption). *Advances in Cryptology, CRYPTO - 1997, Lecture Notes in Computer Science*, vol. 1294, pp. 165–179.