International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-3, September 2019

An Efficient Signcryption Scheme for Secure Authentication using Hyper Elliptic Curve Cryptography and Keccak Hashing

Vani Rajasekar, J. Premalatha, K. Sathya

Abstract: ***The need for security is a challenging task nowadays due to the transition from wired to wireless networks, emergence of Internet of Things (IoT), Mobile Networks, Wireless Sensor Networks (WSN) and Radio Frequency Identification System (RFID). Generally wireless systems are prone to insecurity and resource (power) constraint, to deal with these challenges many solutions has been proposed in cryptography. One such important development is light weight cryptography particularly signcryption.Signcryption is a logical combination of digital signature and encryption in a single step therefore the cost of communication and computation is very less compared to the existing signature then encryption scheme. Till date many signcryption techniques were raised based on El-Gamal, RSA and Elliptic Curve Cryptography (ECC). The proposed research work highlights the limitations of existing signcryption based on ECC and it proposes the efficient light weight cryptographic scheme of signcryption based on Hyper Elliptic Curve Cryptography (HECC) and Keccak hashing. Further the proposed research work achieves all the security metrics such as confidentiality, integrity, non- repudiation, forward secrecy and public verifiability.***

Keywords: Signcryption, ECC, HECC, Keccak Hashing, Authentication, Forward Secrecy.

I. INTRODUCTION

In resource constraint environment authentication and confidentiality are important security requirements particularly the applications such as E-Voting, E-Payment, E-Passport, etc. requires sender privacy and user anonymity. For this many security schemes have been proposed but unfortunately all those schemes were not well suited for advanced wireless networks, wireless transactions and mobile networks. The major development in the arena of security is signcryption which combines authentication and digital signature in a single step. Till today many signcryption schemes have been proposed based on El-Gamal, Schnorr, RSA, and ECC [1]. The proposed signcryptionscheme uses HECC for encryption and Keccak hashing for generating digital signature. The Keccak hashing also called as SHA-3 generates the hash of 512 bits and the major advantage of it is impossible for the hacker to forge this 512 bit digest compared to SHA-1 and SHA-2.

Manuscript published on 30 September 2019
* Correspondence Author
Vani Rajasekar*, Dept of CSE, Kongu engineering college, Perundurai, Erode, India. Email: vanikecit@gmail.com.
Dr.J.Premalatha, Dept of IT, Kongu engineering college, Perundurai, Erode, India. Email: jprem@kongu.ac.in.
K.Sathya, Dept of CT/UG, Kongu engineering college, Perundurai, Erode, India. Email: pearlhoods@gmail.com.

It has been shown from results that our scheme provides more security features compared to the above mentioned signcryption schemes and also the NIST recommended key size of HECC is 80 bits while the key size of RSA is 1024 bits and ECC is 160 bits.

As per the existing literature study it has been identified that signcryption based on El-Gamal, RSA and ECC suffers from high communication cost and computational overhead because of their larger key size. The proposed work reduces the cost of communication and computation by around 50% and it also enhances the security properties such as data confidentiality, integrity, unforgeability, forward secrecy, non repudiation, public verifiability. The term lightweight cryptography refers to provide high security with low computational and communicational cost with less key size.The proposed research works compares and analyze the signcryption based on ECC with signcryption based on HECC and imposes the results to show that signcryption with HECC and Keccak hashing stands better.From the security analysis it has been shown that the signcryption based on ECC fails to provide forward secrecy which is a major challenge in the applications such as E-transactions.

II. SURVEY ON EXISTING SIGNCRYPTION SCHEMES

Zheng [2] has first coined the word signcryption in 1997which is based on El-Gamal cryptosystem. Later Zheng [3] proposed a modified signcryption technique with hash function that involves simple mathematical operations such as +,-,*,%. They have shown that their signcryption scheme reduces the computational and communication cost up to 40% compared to traditional signature then encryption [4] scheme. And also their signcryption scheme was publically verifiable but that does not provide forward secrecy. Sharma et al [5] proposed a method for blind signcryption which is based on discrete logarithmic problem (DLP). Yang et al [6] has proposed a restrictive blind signature based on factorization problem and discrete logarithmic problem. They identified the challenges and restrictions of Sharma et al [5] method and provided a solution with un-traceability.

Zhang and Imai [7] proposed a signcryption scheme based on ECC and shown that their scheme equals the security features of signcryption with RSA and El-Gamal. Their scheme provided a 50% less communication cost and 48% less computational cost but their system lacks public verifiability and forward secrecy.Toorani [8] has overcome the challenges in Zhang and Imai model such that their proposed signcryption scheme with ECC has an added advantage of having public verifiability and forward secrecy therefore

it met the lightweight requirement of resource constrained environment.Ganesan [9] has proposed a scheme based on HECC and El-Gamal technique which is typically used in E-Commerce and Banking applications. Public verifiable scheme have been proposed in [10] which is also built over HECC.

It has been shown that these schemes have been proposed to satisfy computational and communicational cost but these scheme fails to provide forward secrecy.

The major security requirement for digital signature is to prevent against chosen cipher text (CCA) attack. The CCA attack implies that the adversary has no idea about cipher text but he queries the system with number of messages of his own choice. The protection against CCA is also referred to as non- malleability. If any attacker tries to modify the signcrypted envelope, the receiver points that by comparing the received message digest with the generated one which is explained in [12] and also this scheme has been proven to prevent against the Chosen cipher text and message attacks. Quisquater [14] proposed a signcryption scheme based on Diffie-Hellman. Their scheme addresses the problem of non-repudiation which uses the concept of direct verifiable.

III. KECCAK HASH FUNCTION

Hash functions are used in various cryptographic applications that ensure the authenticity of digital signature. Digitalsignatureis generally a mathematical technique used to validate the authenticity and integrity of a message which takes an electronic file and generates a short digest. Any small change made to the message by an attacker will cause drastic change to the message digest. NIST has proposed an elegant and convincing advanced hash standard called Keccak Secure Hash Algorithm (SHA)-3 algorithm which is less complex in computing message digest and more secure than existing SHA algorithms. The Keccak hash function generates the same hash length as of SHA-2 but its internal structure varies significantly from the rest of SHA family. Another interesting property of Keccak hashing is that it prevent against cube attacks, which is applicable to the polynomial that is completely unknown. This hashing technique is known for its clarity of construction that runs well on different computing devices which leads to easy analysis and high performance in hardware implementations. The algorithm uses sponge construction to generate hash as shown in the Fig 1.the sponge function is a cryptographic hashing in which the message blocks are XORed at the beginning to form initial bits of state.

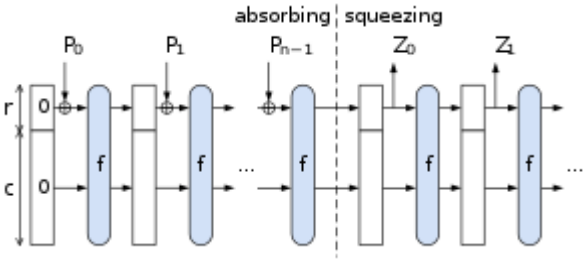

Fig.1: Keccak hashing sponge construction

In the above figure $p_0$to p_{n-1} are input and $z_0$to z_{n-1} are output. Let us consider an input string N width of the bit blocks as b, rate of bit block as r, length of bit block as d, a permutation function f, a padding function pad.The "c" here is an unused capacity which is desired to resist collision given by c=b-r. The sponge construction function is given by z=sponge[f, pad, r](N,d) which works as follows:

Step 1: Pad the input N bits using the padding function produce a padded string p with a length divisible by r.

Step 2: Break p into n consecutive bits as $p_0, p_1,\ldots,p_{n-1}$

Step 3: Initialize the state s with b zero bits.

Step 4: For each block of p_i

Extend by adding c zero bits which yields a length b

XOR with s

Apply the block permutation function f to the result yielding a new state s.

Step 5: Initialize z to the empty string

Step 6: If the length of z is less than d

Append first r bits to z

If z is still less than d, apply the permutation function f to s to yield a new state s.

Step 7: Truncate z to d bits.

Another important feature of Keccak SHA-3 is that it contains smaller state size where s contains 5*5 array of w bit words(ie w=64) and b=5*5*w which is 5*5*64=1600 bits total. This small state size implies that it can be used to test cryptanalytic attacks hence find a major role in light weight cryptographic applications.

IV. SIGNCRYPTION AND UNSIGNCRYPTION USING HECC

The proposed signcryption is based on hyper elliptic curve cryptosystem and also the scheme is based on Digital Signature Standard (DSS). The notations used here are given as follows:

Let C be the Hyper elliptic curve over prime field be taken overF_q

Consider a large prime number q where $q>2^{80}$

Choose a divisor D of large prime order n where n≥280

Let H be the Keccak hash function

Let d_a be the sender's private key where d_aε0,1,2,…p-1

Calculate sender's public key as $p_a = d_a D$

Let d_b be the receiver's private key where d_bε 0,1,2,…p-1f

Calculate receiver's public key as pb = db D

Let m be the plain text to be sent

Let $E_k$and D_k be the encryption and decryption respectively

Let (c,R,S) be the signcrypted tuple

The hyper elliptic curve over genus g≥2 curve is given by the equation (1)

$$y^2 + h(x)y = f(x) mod q \quad (1)$$

Table 1. Security analysis of proposed and existing schemes

Methods	Authentication	Confidentiality	Integrity	Un-forgeability	Non-repudiation	Forward Secrecy	Public verifiability
Proposed	Yes	Yes	Yes	Yes	Directly	Yes	Yes
Hwang[1]	Yes	Yes	Yes	Yes	Another protocol	Yes	No
Zheng[2]	Yes	Yes	Yes	Yes	Another protocol	Yes	No
Zhang[12]	Yes	Yes	Yes	Yes	Another protocol	No	No
Toorani[8]	Yes	Yes	Yes	Yes	Another protocol	Yes	Yes
Shama[4]	Yes	Yes	Yes	Yes	Another protocol	No	No
Libert[14]	Yes	Yes	Yes	Yes	Directly	Yes	No
Yang[6]	Yes	Yes	Yes	Yes	Directly	Yes	No

Where h(x) is polynomial where the degree of h(x)≤g and f(x) ε F[x] is a polynomial called as monic polynomial. The degree of f(x)≤ 2g+1. The Mumford representation of divisor D is shown in (2).

$$D = \big(a(x), b(x)\big) = \{ \sum_{i=0}^{g} x^i a_i \sum_{i=0}^{g-1} x^i b_i \} \varepsilon j_c(F_q) \quad (2)$$

A. Signcryption using HECC encryption:

Once the pubic key of the receiver p_b is known, the signcrypted tuple has to be calculated using HECC using Signcryption (k,d_a,p_a,p_b, m). The steps involved in signcryption are as follows:

Step1: Select a random number say k, k ε 1,2,3,…n-1

Step 2: Calculate K1=H(kD)

Step 3: Calculate K2=H(kp_b)

Step 4: Calculate the cipher text as c=E_{K2}(m)

Step 5: Calculate r=H_{K1}(m||binding info)

Step 6: Compute S=(k/(r+d_a))mod n

Step 7: Calculate R=rD

After these seven steps the signcrypted tuple (c,R,S) is transmitted to the receiver.

B. Unsigncryption using HECC decryption:

When the receiver receives the signcrypted tuple it decrypts the cipher text by HECC decryption and again generates digital signature value to validate the authenticity of the sender. The steps involved in unsigncryption (p_a,d_b,p_b, c, R, S) are as follows:

Step 1: Compute K1=H(S(p_a +R)

Step 2: Compute K2=H(S(d_b (p_a +R))

Step 3: Identify message from cipher text as m=D_{K2}(c)

Step 4: Compute r=H_{K1}(m||binding info)

Step 5: Check for R=rD, If true accepts the message else reject the message

V. SECURITY ANALYSIS ON THE PROPOSED METHOD

The proposed signcryption method satisfies all the security requirements needed for the controlled applications which are authentication, integrity, confidentiality, unforgeability, non repudiation, forward secrecy and public verifiability. The proof of security requirements given here is depends on Hyper Elliptic Curve Discrete Logarithmic Problem (HECDLP) which is hard problem and it is computationally infeasible. The HECDLP is given by a hyper elliptic curve C over prime order q and finite field F_q and J is a Jacobian of curve C, D1 and D2 are the divisors in J. The order of D1 is n, choose a random integer k such that 0 ≤ k ≤ n-1. The HECDLP is defined by the equation D2=kD1 and it is computationally infeasible to find k if D1 and D2 are known by the attacker.The table 1 shows the security analyses on the proposed method with the existing signcryption schemes.

A. Authentication:

The proposed method should ensures both the message authentication and as well as sender authentication. The generated cipher text (c,R,S) where c is cipher text and R,S are signature specific as defined in step 6 and step 7 on signcrytpion using HECC. The Keccak hash function specified here is collision resistant and even though the value chosen for D is known by the attacker it is infeasible to find k in (3) as defined in HECDLP.

K1=H(kD) (3)

B. Confidentiality:

In the proposed scheme the message confidentiality breach can be possible only if the attacker knows the key K2 in c=E_{K2}(m) but it is computationally infeasible by the definition of HECDLP. It can be analyzed using three cases which are as follows:

Case 1: Consider a situation where an attacker knows p_a,$p_b$and D which are publically available and he tries to find k, in such a case solving k from (3) is computationally infeasible by the definition of HECDLP.

Case 2:Consider an equation (4) in which S, p_a and R arepublically available and if an attacker wants to find K2 he needs to identify private key of the receiver d_b from (5) but by the definition of HECDLP solving it is computationally infeasible.

K2=H(S(d_b (p_a +R)) (4)

p_b= Dd_b (5)

Case 3: Consider an equation to find S in signcryption using HECC (6), if an attacker needs to find k he has to

calculate d_a but finding it is computationally infeasible both from (6) and (7).

$$S=(k/(r+d_a))\bmod n \quad (6)$$

$$p_a= Dd_a \quad (7)$$

C. Integrity:

The integrity here is defined as the receiver of the message should verify the originality of the sender. The sender computes the signcrypted tuple (c,R,S) and send to the receiver. If an attacker modifies the cipher text c to c', hence R and S value will also be changed to R' and S' respectively. Inorder to generate a legitimate signature, attacker needs to solve (7) and (8) to get the value of r. For solving (8) attacker needs to know binding info and K1. Obtaining binding info is possible for the attacker but identifying K1 seems to be impossible because of HECDLP. By chance if an attacker is able to find K1 to generate a valid x, he cannot be able to generate valid S because for that he needs to find the private key of sender d_a to satisfy the equation (6).

$$r=H_{K1}(m||\text{binding info}) \quad (8)$$

D. Unforgeability:

As said in the case of integrity, for an attacker to unforge the signcrypted tuple (c,R,S) he needs to identify the private key of the sender d_a for solving (6) and (7) but identifying d_a seems to be computationally infeasible by the definition of HECDLP.

E. Non-repudiation:

Here the unique identification process in public verification method can be used to identify the legitimacy of the sender. Consider a case if the sender denies of sending a message, the receiver send signcryptedtupple, binding info and private key (d_a,c, R, S, binding info) to the public verification process. The public verification judge analyses the received parameters and prove the legitimacy of sender.

F. Forward secrecy:

Forward secrecy is also defined as even if the private key of the sender is identified by the attacker he should not be able to identify the session key used for encryption.

Case 1: Consider a case where $d_a$is identified by the attacker and he tries to find session key K2. For finding K2 attacker needs to find S and R in (4). To compute S attacker needs to find k and r in (6) which is computationally infeasible as by the definition of HECDLP.Hence forward secrecy is achieved here by means that even though if a private key is identified by the attacker the message will remain b confidential.

G. Public verifiability:

Public verifiability is defined as the trusted third party can verify the originality of the sender. In the proposed method the judge of public verification process receives the parameters such as (m, S,p_a, R) and compute the following three steps to identify the legitimacy of sender as well as receiver.

Step 1: Compute K1=H(S(p_a +R)

Step 2: Compute $r=H_{K1}$(m||binding info)

Step 3: Check for R=rD, if true signcrypted text is valid else signcryptedtex is invalid

VI. COMPARTIVE COMMUNICATION AND COMPUTATIONAL COST ANALYSIS

The major need for any resource constraint environment is security and lower computational, communicational cost. The proposed method is analyzed both the cost in the following sections.

A. Communication cost analysis:

Since bandwidth is major constraint in wireless media, designing any cryptographic technique in this media should focus on lowering the communication cost. In any design the choosing of parameters will decide the communication overhead which depends on amount of information to be processed and transmitted. Comparative computational analysis along with size of plain text and signcrypted text is given in the table 2. The parameters to be considered for analysis are given as follows:

- Let $|H(u)|= HK1(u) \approx |q|$ where q is a large prime and $q \geq 2160$
- Let $|H(u)|= HK1(u) \approx 2|n|$ where n is a large prime and $n \geq 280$
- $D = (a(x), b(x)) = \{\sum_{i=0}^{g} x^i a_i \sum_{i=0}^{g-1} x^i b_i\}\, \varepsilon j_c(F_q)$ Where $a_i, b_i \leq 2^n$ which implies that $|D| \geq 2|n|$ for genus 2 hyper elliptic curve.
- Let |x| = |m|
- Let $|x'| = 2|D|$ if $|m| \leq |D|$
- Let $|x'| \geq 2|D|$ if $|m| \geq |D|$

The proposed method reduces the communication overhead in a well defined manner as compared to the existing schemes which are as follows:

1. The communication cost reduction of proposed method compared to [7] and it is given by the equation (9).

$$\frac{(|x| + |H(u)| + |q|) - (|x| + |D| + |n|)}{|x| + |H(u)| + |q|} \quad (9)$$

2. Similarly the communication cost reduction of proposed method compared to [1] and it is given by the equation (10).

$$\frac{(|x| + |H(u)| + 2|q|) - (|x| + |D| + |n|)}{|x| + |H(u)| + 2|q|} \quad (10)$$

3. Similarly the communication cost reduction of proposed method compared to [12] and it is given by the equation (11).

Table 2. Communication cost analysis of proposed and existing schemes

Method	Communication cost	Size of plain text	Size of signcrypted text
Proposed	|x| + |D| + |n|	Session key: 128 bits Text: 1300 bits	128+512= 640 bits 1300+512=1812 bits
Hwang[1]	|x| + |H(u)| + 2|q|	Session key: 128 bits Text: 1300 bits	128+320+320= 768 bits 1300+320+320=1940 bits
Toorani[8]	|x| + |H(u)| + 2|q|	Session key: 128 bits Text: 1300 bits	128+320+320= 768 bits 1300+320+320=1940 bits
Nizamuddin[16]	|x| + |H(u)| + |n|	Session key: 128 bits Text: 1300 bits	128+320+240= 688 bits 1300+320+240=1860 bits
Nizamuddin[15]	|x| + |D| + |n|	Session key: 128 bits Text: 1300 bits	128+320+240= 688 bits 1300+320+240=1860 bits

$$\frac{(|x| + |H(u)| + |n|) - (|x| + |D| + |n|)}{|x| + |H(u)| + |n|} \quad (11)$$

4. The communication cost of proposed method is equal to [15], [16] and it is given by the equation (12).

$$\frac{(|x| + |D| + |n|)) - (|x| + |D| + |n|)}{(|x| + |D| + |n|)} \quad (12)$$

From the table 2 it has been proved that the proposed system contains very less computational overhead compared to that of already existing schemes.

B. Computational cost analysis:

The results are executed in a PC using Mat lab have i3 Intel core processor with speed of 2.53GHz and 4 GB RAM with the operating system Windows 10. From the execution it has been proved that the proposed algorithm has very less computational power compared to that of already existing schemes. The operation which is more time consuming in the proposed system is Hyper Elliptic Curve Divisor Scalar multiplication (HECDM) therefore the proposed scheme is compared with respect to HECDM with the existing schemes.

The operations which are consider for calculating computational cost are HECDM, ECPM (Elliptic Curve Point Multiplication), ECPA (Elliptic Curve Point Addition), KH(Keyed Hash), MUL (Multiplication), DIV (Division), ADD (Addition), HECDA(Hyper Elliptic Curve Divisor Scalar Addition). The table 3 shows that the proposed method is efficient in terms of computational cost compared to that of all the existing schemes. Hence it is light weight such that it uses less computational power where as it satisfies all the security requirements such as Authentication, Integrity, Confidentiality, Non-repudiation, Forward secrecy, Un forgeabiltiy as specified in table 1 needed for the controlled applications.

VII. CONCLUSION

In concluded remarks the proposed research work, signcryption based on Hyper elliptic curve cryptography and Keccak hashing is most suitable for energy constrained environment. The major advantage of this scheme is to provide less computational and communicational cost with all the necessary security requirements. The analysis of literature and results of proposed method has indicated that this system provides 55% less communication and 50% less computational cost on average when compared to the existing signcryption schemes. Therefore it is concluded that the proposed system is light weight cryptographic scheme and it can find its major role in applications such as wireless devices, mobile devices, Border security applications, Military applications and IoT applications. Vani Rajasekar [18,19,20] have coined that the signcryption based on hyper elliptic cryptography have produced less computational and communicational overhead compared to other existing schemes.

Table 3. Computational cost analysis of proposed and existing schemes

Method	Operations to be considered	Computational time for sender	Computational time for receiver
Proposed	HECDM:3 HECDA:1 ADD:1 DIV:1 KH:2	5.3 ms	4.2 ms
Hwang[1]	ECPM:4 ECPA:1 ADD:1 MUL:1 KH:1	9.3 ms	12.2 ms
Toorani[8]	ECPM:4 ECPA:1 ADD:3 MUL:1 KH:2	10.3 ms	12.8 ms
Nizamuddin[16]	HECDM:4 HECDA:1 ADD:1 DIV:1 MUL:1 KH:1	6.1 ms	5.8 ms
Nizamuddin[15]	HECDM:4 HECDA:1 ADD:1 DIV:1 MUL:2 KH:1	5.8 ms	4.12 ms

VIII. DATA AVAILABILITY STATEMENT

The data supporting the results reported in this work are generated in our simulation experiments in our study. No external data set repository is used for this experimental analysis.

CONFLICTS OF INTEREST

The authors declare here that they have no conflict of interest.

FUNDING STATEMENT

The authors declare here that they got no funding for this research work.

REFERENCES:

1. Hwang RJ, Lai CH, Su FF (2005) An efficient signcryption scheme with forward secrecy based on elliptic curve. Appl Math Comput 167(2):870–881
2. Zheng Y (1997) Digital signcryption or how to achieve cost (signature & encryption)<<cost (signature)+ cost (encryption). In: Advances in cryptologyCRYPTO'97. Springer, pp 165–179
3. Zheng Y (1997) Signcryption and its applications in efficient public key solutions. In International Workshop on Information Security, Tatsunokuchi, Ishikawa Japan, September 17-19, 1997. Springer,Berlin, Heidelberg, p 291–312
4. Varalakshmi L, Florence SG (2013) An enhanced encryption algorithm for video based on multiplehuffman tables. Multimedia Tools Appl 64(3):717–729
5. N. Sharma, and B. K. Sharma, "New Provably Secure Blind Signature Scheme with Weil Pairing," International Journal of Advancements in Research & Technology, 3(5), May-2014.
6. P. Yang, "A new blind signature based on the discrete logarithm problem for untraceability," Applied Mathematics and Computation, 164(3), pp. 837–841, 2008.
7. Zheng Y, Imai H (1998) How to construct efficient signcryption schemes on elliptic curves. Inf Process Lett 68(5):227–233
8. Toorani M, Beheshti AA (2010) An elliptic curve-based signcryption scheme with forward secrecy.Xiv:1005.1856
9. Ganesan R, Vivekanandan K (2009) A novel hybrid security model for e-commerce channel. In: International conference on advances in recent technologies in communication and computing, 2009.
10. Ch SA, uddin N, Sher M (2012) Public verifiable signcryption schemes with forward secrecy based on hyperelliptic curve cryptosystem. In: Information systems, technology and management, communications in computer and information science, vol 285. Springer Berlin Heidelberg, pp 135–142
11. Goldwasser, S., S. Micali and R. Rivest, 1988. A Digital Signature Scheme Secure Against Adaptive Chosen Message Attacks, SIAM, Journal on Computing, 17(2): 281-308.
12. Zhang B, Jia Z, Zhao C (2018) An efficient Certificateless generalized Signcryption scheme. SecurCommunNetw 2018:1–11
13. Galindo D, Garcia FD (2009) A Schnorr-like lightweight identity-based signature scheme. AFRICACRYPT 9:135–148
14. Libert B and Quisquater JJ (2004) Efficientsigncryption with key privacy from gap Diffie-Hellman groups. In International Workshop on Public Key Cryptography, Singapore, Singapore, 1-4 March 2004. Springer, Berlin, Heidelberg, p 187–200
15. Nizamuddin, Ch SA, Nasar W, Javaid Q (2011) Efficient signcryption schemes based on hyperelliptic curve cryptosystem. In: 7th international conference on emerging technologies (ICET), 2011, pp 1–4
16. Nizamuddin, Ch SA, Nasar W, Javaid Q (2015) An Efficient signcryption scheme with forward secrecy and public verifiability based on hyper elliptic curve cryptography, Multimedia Tools Appl 74:1711-1723, DOI 10.1007/s11042-014-2283-9.
17. Premalatha J, Sathya K, and Vani Rajasekar, "Hyperelliptic Based Signcryption with Sensor-Seeded Random Number", International journal of computers and communications, Vol.10, ISSN: 2074-1294,pp:18-22,2016
18. K Sathya, J Premalatha, Vani Rajasekar, "Sensor-Seeded Cryptographically Secure Random Number Generation", Indian Journal of Science, ISSN:2319-7730,Vol.3, pp:157-163,2016.
19. J Premalatha, Rajasekar Vani, K Sathya, "Biometric Signcryption using Hyperelliptic Curve and Cryptographically Secure Random Number",Asian Journal of Research in Social Sciences and Humanities, Vol.6, pp:462-472,2016.
20. Premalatha J, Sathya K, and Vani Rajasekar,"Secure Signcryption on Hyper Elliptic Curve with Sensor-Based Random Number", Journal of Recent Advances on Computer Engineering, ISBN: 978-1-61804-336-8,pp:95-98, 2015.

AUTHORS PROFILE

Vani Rajasekar completed her B.Tech(IT), M.Tech (Information and cyberwarefare) in department of IT Kongu engineering college. She is pursuing her PhD (Information and Communication Engineering) in the area of Network security. Presently she is working as assistant professor in the department of CSE Kongu engineering college for past 3 years. Her area of interest includes Network security, Cryptography and Wireless networks.

Dr.J.Premalatha completed BE(ECE), ME(CSE), PhD(Information and Communication Engineering). She is working as professor in the department of IT Kongu engineering college. Her teaching experience is 28 years. Her area of interest includes Network security, Cryptography, Computer networks and Database Management system.

K.Sathya completed her B.Tech(IT), M.Tech (Information and cyberwarefare) in dept of IT Kongu engineering college. She is pursuing her PhD (Information and Communication Engineering) in the area of Network security. Presently she is working as assistant professor in the department of CT/UG Kongu engineering college for past 3 years. Her area of interest includes Network security, Computer networks.