# HYPER-ELLIPTIC CURVE BASED SIGNCRYPTION SCHEMES FOR RESOURCE CONSTRAINT DEVICES IN IOT

**Santosh P. Jadhav, Prof. Georgi Balabanov, Prof. Vladmir poulkov.**

[1] *Faculty of Telecommunications, Technical University of Sofia Bulgaria*
*Spjadhav375@gmail.com,grb@tu-sofia.bg,vkp@tu-sofia.bg.*

**Abstract**

**The Internet of things has become part of our day to day life as many more devices are connecting to the internet, the number is increasing rapidly. IoT devices have become the element in our day to day life. Such as many tiny devices are continuously monitoring our health homes and providing sensitive information which can be analyzed and help for decision making. This important data must have enough security. Hence, the security and efficiency of these IoT devices play an important role therefore various efforts are made to make these resource constraint devices highly secure and efficient. Signcryption is one of the techniques to increase efficiency as compare to traditional signature then encryption schemes. Signcryption along with the hyper-elliptic curve (HECC) can reduce the computational cost of the encryption schemes along with the provision of higher security.**

**Keywords: Sighncryption, Resource constraint devices, Computational cost.**

## INTRODUCTION

The Internet of things is becoming a buzzword nowadays. Every year millions of devices are getting connected to the internet. There is an enhancement in several parameters that are part of IoT such as, IoT protocols, network efficiency, etc. everyone strives to make the IoT system more efficient and secure. In this paper, we had included schemes that help in increasing the efficiency and security of the IoT system. Encryption and digital signature are two basic building blocks of any encryption techniques used for securing communications. Digital signatures are used to verify and authenticate the digital messages or digital documents, the digital signature, and then

encryption is a method that is used for a decade for any cryptographic mechanism. These methods have drawbacks as the computation cost of which affects the efficiency and security of the communication system. Therefore new approach called sighncryption which is a combination of digital signature and encryption has emerged which perform signature and encryption in a single logical step. This signcryption approach improves the computational cost and several communications overhead when compared with traditional signature-then encryption schemes. In the case of IoT devices, they have limited resources as they are tiny in nature, such tiny devices in IoT have spread rapidly in past years, there security and performance must be the top priority. So highly secure encryption algorithm which is more suitable for such resource constraint must be chosen among the several encryption algorithms.[1].The embedded system is growing rapidly and many resource constraint devices such as mobile phones, smart cards, sensor nodes have become most in our day to day life. The most challenging task for embedded security is the implementations of public-key cryptography. HECC overcomes ECC because of the possibilities to work in a lightweight device. Therefore in this paper, we had considered HECC as an encryption algorithm which is part of sighncryption schemes. The attributes such as accuracy, performance, and security should be taken into consideration by the signcryption scheme. Internet of things is becoming a buzzword nowadays. Every year millions of devices are getting connected to the internet. There is an enhancement in several parameters that are part of IoT such as, IoT protocols, network efficiency, etc. everyone





ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

strives to make the IoT system more efficient and secure. In this paper, we had included schemes that help in increasing the efficiency and security of the IoT system. Encryption and digital signature are two basic building blocks of any encryption techniques used for securing communications. Digital signatures are used to verify and authenticate the digital messages or digital documents, the digital signature, and then encryption is a method that is used for a decade for any cryptographic mechanism. These methods have drawbacks as the computation cost of which affects the efficiency and security of the communication system. Therefore new approach called sighncryption which is a combination of digital signature and encryption has emerged which perform signature and encryption in a single logical step. This signcryption approach improves the computational cost and several communications overhead when compared with traditional signature then – encryption schemes. In the case of IoT devices, they have limited resources as they are tiny in nature, such tiny devices in IoT have spread rapidly in past years, there security and performance must be the top priority. So highly secure encryption algorithm which is more suitable for such resource constraint must be chosen among the several encryption algorithms.[1]. The embedded system is growing rapidly and many resource constraint devices such as mobile phones, smart cards, sensor nodes have become most in our day to day life. The most challenging task for embedded security is the implementations of public-key cryptography. HECC overcomes ECC because of the possibilities to work in a lightweight device. Therefore in this paper, we had considered HECC as an encryption algorithm which is part of sighncryption schemes. The attributes such as accuracy, performance, and security should be taken into consideration by the signcryption scheme.

## 1. LITERATURE REVIEW

The preferred In 1997 zhen et al. was the first to introduce a signcryption scheme which includes an elliptic curve-based sighncryption approach which saves 40% of communication cost and 58% of the computational cost as compared to the traditional approach of signature-then encryption approach [2]. This approach of zheng made researchers think about how signcryption can be useful to increase the efficiency of any system. Deng and bao signcryption scheme try to reduce the computational cost by 16 % and communication cost up to 85% [3]. Gamage et al. proposed the scheme which was enhancement Deng and Bao which provide authentication for secure messages [4]. Sharma et.al. Proposed the scheme which lacks public verifiability which was based on identity-based signcryption [5]. In 2005 Hwang RJ et.al. Proposed an elliptic curve-based signcryption scheme which was found to be suitable for lightweight devices. These schemes were found to be secure even when the sender's private key was compromised [6]. Nizamuddin et al. also carry out different signcryption schemes which also reduce the communication and computational time but they lack in public verifiability [7]. Public verifiable schemes based on HECC were proposed by Ch SA et al. this scheme lack forwarding secrecy.

## 2. PROPOSED SCHEME

In today's scenario, it is being noted that elliptic curve cryptography is being used in various applications. But it is found that the counterpart of ECC i.e. HECC is faster than ECC [8].

In the proposed system we try to demonstrate HECC based signcryption approach where Alice (A) and Bob (B) are the sender and receiver and malicious attacker (M). The proposed scheme consists of four different phases 1) Initiate 2) signcryption 3) unsigncryption 4) verification.

1) Initiate: In this phase selection of domain parameter and generation of required private and public keys as well as a certificate of public Keyes for every user

2) Signcryption phase: encryption using HECC and the digital signature is performed in a single logical step. And this signcrypted message sends from Alice to Bob.

3) In the Unsigncryption phase signcrypted messages are un-signcrypted by Bob and verification of the digital signature is done.

4) Verification is carried out in case if there is any dispute during the transmission of messages from Alice to Bob.

The following notation is used to describe the system

$\in_R$= randomly chosen

M = plaintext

C= ciphertext

s=Digital signature

$H$= one way hash function





ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

‖= concatenation

*G*= basic point on hyper elliptic curve

*O*=point of the hyperelliptic curve at infinity

*n* =order of *G(nG =0)*

$ID_A$ = identification of Alice

$ID_B$ = identification of Bob

$w_A/W_A$ = private and public keys of Alice

$w_B$ /$W_B$ =private and public keys of Bob

$x_R$ /$y_R$ = x and y coordinates of point R

E_k/D_k: Symmetric Encryption / Decryption

### A. Initialization

These phase consists of special case of an elliptic curve called a hyper elliptic curve i.e. HECC with genus g>=2.

Let us consider the HECC curve E Defined over the finite field $F_q$. Where q is any prime number.

$$y2 + h(x)y = f(x) \bmod q$$

$h(x) \in F[x]$ is a polynomial where the degree of $h(x) \leq g$ and $f(x) \in F[x]$ is a polynomial known as monic polynomial and the degree of $f(x) \leq 2g + 1$. With the satisfied condition that curve is not a singular curve.

The randomly selected private keys of *Alice* and *Bob* are selected integers $w_A, w_B . \epsilon\ R$ [1,*n*-1] . The correlated public keys are computed as $W_A = w_A G$, similarly and $W_B = w_B$ G. Alice and Bob are indifferently identified by the unique identifiers *IDA* and *IDB* respectively. The certificates CertA and CertB are issued by a certificate authority.

### B. Signcryption

The signcryption is done by Alice by performing the following steps

1) Checking the validity of the certificate of Bob and uses it to verify the public key of Bob.

2) Randomly select integer $r \in_R [1n - 1]$

3) Compute $R = rG = (x_R . y_R)$

4) Compute $K = (r + X_R w_A)W_B = (x_K . y_k)$ if $K \neq 0$ session key derived $k = H(x_K || ID_A || y_K || ID_B)$ where the required number of bits as the secret key of deployed symmetric encryption is generated by H

5) Compute cipher text C = $E_k$(M)

6) Compute the digital signature s= $tw_A$- r(mod n)

Where t is

$t = HMAC_k(M || x_R || ID_A || y_R \| ID_B)$

7) Signcrypted text is sent to Bob (R, C, s).

### C. Unsigncryption

Bob receives the signcrypted text in the form of (R, C, s) and starts the unsigncyption. By extracting the plaintext from the received cipher text.

1) Check the validity of certification of Alice and use it to verify the public key of Alice i.e. $W_A$

2) Compute $K = W_B(R + X_R W_A) = (X_K . Y_K)$ with session key $= H(x_K || ID_A || y_K || ID_B)$

3) Decrypt the cipher text as $M = D_K(C)$.

4) Compute $t = HMAC_k(M || x_R || ID_A || y_R \| ID_B)$

5) Verifies Alice signature by verifying $sG + R = tW_A$

Bob accepts *M* when this condition is achieved. Public Keyes are checked with their validation and verification by following check conditions.

1) Check $R \neq O$

2) $x_R, y_R \in F_q$

3) $R$ Should satisfy the defining equation of $E$.

If these conditions are not satisfied then unsighncryption is failed.

### D. Verification

Verification is carried out when any dispute is accrued and bob claims for the verification. The third-party judge asks Bob to provide $(R, C, s, M, K)$. The judge applies the following steps to solve Bob's argument.

1) Check the validity of $Cert_A$ and verifies the public key of Alice $W_A$.

2) If $M = D_k C$. Bob is right.

3) Compute $t = HMAC_K(M || x_R || ID_A || y_R \| ID_B)$

4) Signature of Alice is verified by checking the condition $sG + R = tW_A$. If condition satisfied Alice has sent (R, C, s) to Bob.

Strong blocks ciphers such AES must be used to perform high-security encryption schemes. Bob found the necessity to check the status of the Alice certificate in online certificate status protocol (OSCP) which is an internet protocol used for checking the revocation status of a digital certificate, we choose OSCP because it response contains fewer data than a typical certificate revocation list (CRL) and therefore suitable for the resource constraint device which can handle smaller data transmissions and also it discloses to the receiver that which network host uses which certificate at what particular time.

Figure 1 describes the communication in the proposed system. Among several available protocols for certificate validation use of (OSCP) is the better one when we are dealing with resource constraint devices. (CRL) certification revocation list is maintained to check certification revocation offline. The use of hyperelliptic curve cryptography will significantly reduce the size of the keys which directly affects the performance of the system.

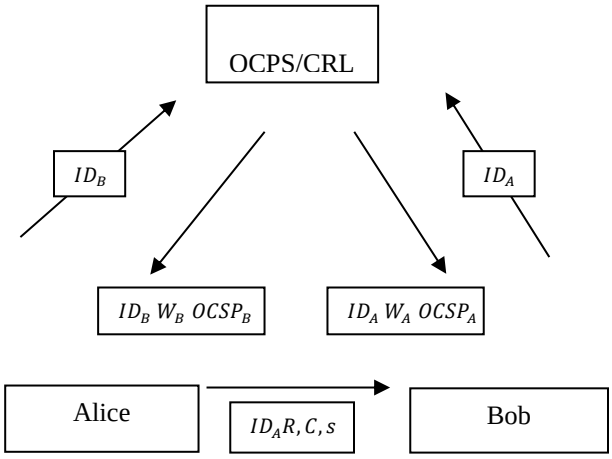


Fig: 1 Proposed Scheme

## 3. PERFORMANCE ANALYSIS

. It is observed that the use of the HECC and signcryption scheme reduced the computational time of the system and hence increase the efficiency of the system. Comparative result of HECC based signcryption and ECC based signcryption is shown to prove that HECC based signcyption is more suitable in case of resource constraint devices that are found in IoT

For demonstrating the performance, we had taken some messages block of various sizes and try to note the computational time. The implementation platform is an internet-connected pc running on the windows 7, Intel i3 processor having a speed 1.70 GHz and 4GB RAM capacity.

[TABLE 1: COMPUTATIONAL TIME]

| | **Computational Time** | | |
|---|---|---|---|
| ***Sr. no*** | ***Block sizes*** | ***ECC based signcryption(ms)*** | ***HECC based sighncryption(ms )*** |
| 1 | 5kb | 356 | 246 |
| 2 | 10kb | 395 | 269 |
| 3 | 20kb | 530 | 392 |

The tabular result shows that the computation time required for a block in HECC based signcryption approach is lesser than the time required by ECC based signcryption approach. Block of 5kb is given as input for ECC based sighncryption scheme where processor take 276 ms to perform all the computations while same load of 5kb was given to HECC based sighncryption scheme which required 170 ms of computational time. Similarly message of 10kb and 20 kb were passing as input for both scheme and computational time was recorded. Thus this shows that this approach is suitable for the resource constraint devices found in IoT. The efficiency of such devices increases and also we can assure the security of data transmission as the stronger and secure algorithms are used for encryption.

Considering the general performance metrics for light weight devices[10] which provides the generalized formula to which is given by

$$\text{General Metric } (A^{\alpha}, T_B^{\beta}, E_B^{\lambda}, C_B^{\tau}, N_B^{\mu}) = \frac{A^{\alpha}, T_B^{\beta}, E_B^{\lambda}, C_B^{\tau}}{N_B^{\mu}},$$

Where,





ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

A is the area;
TB the time to encrypt one block;
E is the energy;
CB is the number of cycles to encrypt one block;
NB is the block size;

α β λ τ and μ are power coefficients

The values of power coefficient while considering the software platform are [55]

| platform | Performance metric | $\alpha$ | B | λ | μ | τ |
|---|---|---|---|---|---|---|
| Software | Cycles/block | 0 | 0 | 0 | 0 | 1 |
| | Through output | 0 | -1 | 0 | -1 | 0 |
| | Code size * cycle count/block size | 1 | 0 | 0 | 1 | 1 |

Through output is given by

$$\text{Throughput} = \frac{T_B^{\beta} C_B^{\tau}}{N_B^{\mu}}$$

Substituting the values of poer coefficient

$$= \frac{246^{-1}}{5^{-1}} = 0.018 \text{ block/ms}$$

Thus, the efficiency gets increased which is very important parameter while considering the resource constraint devices in IoT. This shows that use of HECC based sighncryption approch becomes more suitable for the IoT devices.

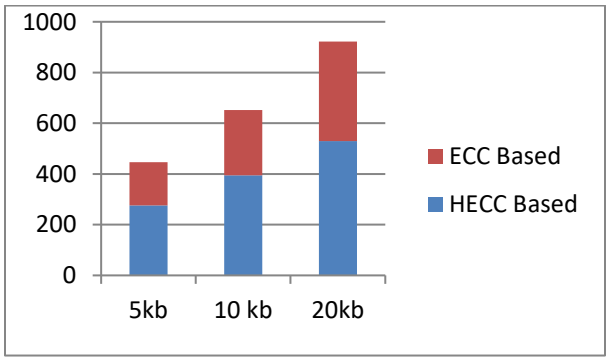


Fig 2: Computational cost in Milliseconds

## CONCLUSIONS

Implementation of HECC based signcryption approach increases the efficiency of the resource constraint devices in IoT and also the security is enhanced by using the stronger and secure cryptographic algorithm the result shows a reduction in computation cost was reduced by 45 % which is a noticeable achievement thus, the proposed scheme is most likely suitable for the resource constraint devices also called as lightweight devices. Thus, we can enhance the performance of the IoT system.

## REFERENCES


[1] S. P. Jadhav, G. Balabanov, V. Poulkov and J. R. Shaikh, "Enhancing the Security and Efficiency of Resource Constraint Devices in IoT," 2020 International Conference on Industry 4.0 Technology (I4Tech), Pune, India, 2020, pp. 163-166, doi: 10.1109/ signcryption or how to achieve cost (signature & encryption I4Tech48345.2020.9102639.

[2] Zheng Y (1997) Digital) cost (signature)+ cost (encryption). In: Advances in cryptologyCRYPTO'97. Springer, pp 165–179

[3] Bao F, Deng RH (1998) A signcryption scheme with signature directly verifiable by a public key. In Public-key cryptography. Springer, pp 55–59

[4] Gamage C, Leiwo J, Zheng Y (1999) Encrypted message authentication by firewalls. In: Lecture notes computer science (LNCS), PKC99, vol 1560. Springer-Verlag, pp 69–81

[5] Sharma G. Bala Verma AK "An identity-based ring signcryption scheme. In: IT convergence and security". Springer, 151–157

[6] Hwang RJ, Lai CH, Su FF " An efficient signcryption scheme with forwarding secrecy based on an elliptic curve. Appl Math Comput 167(2):870–88. 2005.

[7] Sasas 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

[8] Mrs. M.T.Wankhede-Barsgade, Dr. S.A. Meshram "Comparative study of an elliptic curve and hyperelliptic curve cryptography in a discrete logarithmic problem." IOSR Journal of Mathematics (IOSR-JM) e-ISSN: 2278-5728, p-

ISSN: 2319-765X. Volume 10, Issue 2 Ver. V (Mar-Apr. 2014), PP 61-63.

[9] Mohsen Toorani, Ali A. Beheshti "An Elliptic Curve-based Signcryption Scheme with Forward Secrecy" Reprinted from Journal of Applied Sciences, Vol. 9, No. 6, pp. 1025-1035, 2009 [DOI 10.3923/jas.2009.1025.1035

[10] Santosh pandurang jadhav. "Towards Light Weight Cryptography Schemes for Resource Constraint Devices in IoT" Journal of Mobile Multimedia, Vol. 15_1&2, 91–110. doi: 10.13052/jmm1550-4646.15125 c 2020 River Publishers.

[11] Bassam J. Mohd, Thaier Hayajneh, Athanasios Vasilakos. "A survey on lightweight block ciphers for low-resource devices: Comparative study and open issues. Journal of NetworkandComputerApplications58. P.73–93. 2015.

**Santosh Pandurang Jadhav**

Is a Ph.D. student at the Technical University of Sofia at Sofia, Bulgaria ince 2017. He received his B.E. in Information Technology Engineering from North Maharashtra University, India in 2007 and M.E. in Computer Science & Engineering from the Savitribai phule, Pune University of Maharashtra, India in 2012. As an Assistant Professor in NDMVPS's KBT college of engineering, Nashik, Maharashtra, India he has acquired a solid experience about 11 years of teaching in Information Technology Engineering.

Assistant Professor Georgi Balabanov is with the Faculty of Telecommunications at the Technical University of Sofia (TU-Sofia), Bulgaria. He received his PhD degree in communication Networks and Systems from TU-Sofia. He is affiliate researcher at TeleInfrastructure R&D Lab. Dr. Balabanov has participated in several scientific projects – both national and international. He has published more than 30 papers in conferences and journals. His research interests include Embedded Systems, Teletraffic Engineering, QoS, Internet of Things, Ambient Assisting Living Systems. He is an IEEE member.

Prof. Vladimir Poulkov has more than 35 years of industrial, research and teaching experience in the field of telecommunications. His expertise is in the field of information transmission theory, modulation and coding interference suppression, power control and resource management for next generation telecommunications networks, cyber physical systems. He has been leader of many national and international industrial, R&D and educational projects. He is author of more than 150 scientific publications and is leading BSc, MSc and PhD courses in the field of Information Transmission Theory, Broadband Transmission and Access Networks. Currently he is Head of "Teleinfrastructure" and "Electromagnetic Compatibility of Communication Systems" R&D Laboratories at the Technical University of Sofia, Chairman of Bulgarian Cluster Telecommunications, Vice-Chairman of European Telecommunicaitons Standartization Institute (ETSI) General Assembly, Senior IEEE Member.





ISSN (Print): 2204-0595
ISSN (Online): 2203-1731