Implementation of Hyperelliptic Curve Based Signcryption Approach

Pushpendra Kumar, Archana Singh, Aditya Dayal Tyagi

Abstract— Data Security has become a challenging task due to natural problems of power, memory and processing constraints over the wireless network. Hyper elliptic curve cryptosystem (HECC) is a well suited public key cryptosystem, for the situation where resources are limited, because of its shorter key size and effectiveness. HECC can be used to develop a cryptosystem that can sign and authenticate documents and encrypt / decrypt messages efficiently for constrained devices in wireless networks. In this paper, we proposed a resource efficient signcryption schemes based on Hyperelliptic curve cryptosystem. Our proposed scheme can save up to 40% computational cost and a minimum of 40% of Communication Overhead Compared with existing schemes.

Index Terms— Hyperelliptic Curve Cryptosystem(HECC), Jacobian group, genus, Signcryption, Hyperelliptic Curve Deffie-Hellman(HECDH), Hyperelliptic Curve Digital Signature Algorithm(HECDSA),Elliptic Curve Cryptosystem(ECC)

1 Introduction

INFORMATION Security is a major issue mostly in wireless network. We required integrity, authenticity, confidentiality and non-repudiation when we send a message over an insecure channel such as internet. These are the four main security goals that should be achieved. In earlier days the cryptography was mostly used for message confidentiality.

There are many symmetric and asymmetric encryption algorithms. Symmetric encryption techniques are faster while asymmetric encryption technique has less problem of key distribution.

Public key cryptography was discovered nearly three decades ago and proved to be a revolution in the cryptography world [1-2]. The secure and authenticated communication is provided by the Digital Signature and Encryption techniques [3]. Hyper elliptic curve cryptosystem, which is the natural generalization of Elliptic curve cryptosystem suitable for getting high security in resource constrained environment, was invented by N.Koblitz[4].

HECC, which is based on hyper elliptic curve, is an alternate to Elliptic curve and provide same security using smaller base field.

Security of HECC is based on "difficulty of solving discrete logarithmic problem (HCDLP)" which is as follows-

D1 and D2 are devisor in Jacobian group and order of D1 is n then find an integer k, 0≤k≤n-1 such that D2=kD1.

HECC provide the same level of security with shorter parameters, as compared with other cryptosystem for example the 60 bits base field of HECC provide same level of security as 180-bits of ECC and 1024 bits of RSA[5-7].

HECC can be implemented efficiently in case of genus 3 as 60 bits parameters can be implemented with a single computer. The algorithm used to solve HCDLP has exponential complexity on the same base field high genus(g≤4) increase the number of curve so it becomes easy to select secure curves.

The asymmetric cryptographic techniques make easy to achieve the authenticity of the message, the sender can select anyone of the digital signature scheme and selection depends on the level of security.

Two decade before, message encryption and digital signature considered as a two step approach as "Signature-then-Encryption", which have main disadvantages of high communication and processing cost. In signcryption both the operations are combined logically into a single step [3].

Signcryption, is a logical combination of two words signature and encryption, which was first coined by Y. Zheng [3], reduces the computation and communication overhead.

2 Related Work

Signcryption based on hyperelliptic curve cryptosystem[13] provide the functionality of both Encryption and Digital Signature into a logically single step.

In [8-10] architectures for secure banking and E-commerce communication using Hyperelliptic Curve Encryption were proposed using HEC-Elgamal technique[9] define as follows-

Encryption

Calculate $Q=k\,D$ and $Q=(u(x),v(x))$

Calculate $P_k=k\,P_k$ and $P_k=(u(x),v(x))$

Calculate $C_m=(Q, P_m+P_k)$ or $C_m=(((u(x),v(x)), (u(x),v(x)))$

Decryption

Extract from $C_m=(Q, P_m+P_k)$

Calculate $\eta_b Q$

Extract P_m+P from C_m

Calculate $P_m=P_m+P_k - \eta_b Q$

For the authenticity of message the architectures do not use standard Digital Signature.

In [11] author proposed generalized equations for hyperelliptic curve digital signature algorithms(HECDSA)[13] and shorthand digital signature which is defined in following table

TABLE I

HECDSA	*Signing(r, s)*	*Verification*
HECDSS1	$r=hash([k\,D]_e, m)$ $S=((k/(r+d_a))\bmod n$	$R=s(P_a+r\,D)$ $r'=[R]_e \bmod n$ check $hash(r', m)=r$
HECDSS2	$r=hash([k\,D]_e, m)$ $S=((k/(1+rd_a))\bmod n$	$R=s(r\,P_a+D)$ $r'=[R]_e \bmod n$ check $hash(r', m)=r$

HECDSA and HEC-Elgamal are used to provide authenticity and confidentiality in hyperelliptic curve cryptosystem[12] but the computation cost and communication overhead is very high and so not suitable for wireless networks, satellite communication etc. so to overcome these problem we proposed signcryption schemes based on HECC using HECDSS1.

3 PROPOSED SCHEME

Our proposed scheme works as follows

Select C a hyperelliptic curve of genus g≥2 defined over finite field Fq and defined by –

$$y2 + h(x,y)=f(x) \bmod q \qquad (1)$$

h(x) ∈ F[x] is a polynomial and degree of h(x)≤g.

f(x) ∈F[x] is a monic polynomial and degree off(x)≤2g+1.

The points on hyperelliptic curve do not form a group like points on elliptic curve. By soliciting a special point at infinity and points on C, an Abelian group called Jacobian group $J_c(F_q)$ can be formed. The order of Jacobian group is o(Jc(Fq)) and is always defined as

$$(\sqrt{q} - 1)^{2g} \leq o((J_c(F_q)) \leq ((\sqrt{q} + 1)^{2g} \qquad (2)$$

After forming the Jacobian group selects D the generator of the group and represented in Mumford form as

$$D=(a(x),b(x))=(\sum_{i=}^{g} I \quad x^{i} \quad , \quad \sum_{i=0}^{g-} I \quad x^{i} \quad) \quad J_c(\quad F_q \quad) \qquad (3)$$

Let $[\ ]_e$: $J_c(F_q) \rightarrow Z_q$ be a mapping function use to map jacobian group element to integer.

Initalization :

TABLE III

q:a large prime number(q≥2^{80}) C: a hyperelliptic curve over prime field F_q D: a devisor of large prime order n in Jc(F_q), n≥2^{80}. d_a : sender private key d_a {0,1,2,….,p-1} P_a : sender public key P_a= d_aD d_b : receiver private key d_b €{0,1,2,….,p-1}	P_b : receiver public key P_b= d_bD $[\ ]_e$: a function which map a devisor to integer value H : a one way hash function KH; keyed hash function m:message c:cipher text E_k/D_k: symmetric Encryption / Decryption

Signcryption Phase:

Sender obtain receiver public key P_b from certificate authority and use Signcryption(k, P_a, P_b ,d_a ,m ,s) routine to generate signcrypted text for message m.

Signcryption(k, P_a, P_b ,d_a ,m ,s)

1. Select a random number k € {0,1,2,3,…………n-1}
2. Compute kP_b
3. Compute $(K_1,K_2) = H([kP_b]_e)$
4. $c=E_{k1}(m)$
5. Compute $r=KH_{k2}(c)$
6. Compute $s=(k/(r+ d_a))\bmod n$

Signcrypted text for message m is (c,r,s)

Send signcrypted text

Unsigncryption Phase:

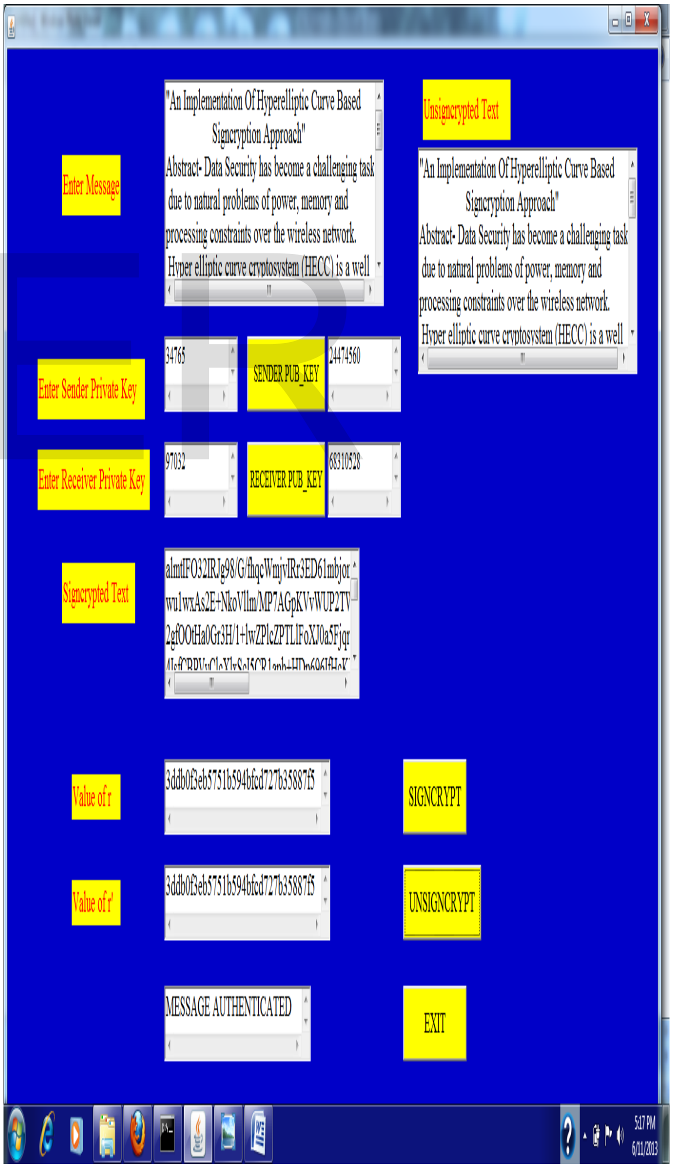
Receiver will obtain sender public key from certificate authority and follow the following steps to unsigncrypt the message.

Unsigncryption(k,P_a,P_b,d_b,c,r,s):

1. Compute $u=sd_b \bmod n$
2. Compute $(K_1,K_2)=H([uP_a+urD]_e)$
3. Compute $r' = KH_{k2}(c)$
4. Compute $m= Dk_1(m)$

Check if r=r' then accept the message

Otherwise reject



Enter Message

"An Implementation Of Hyperelliptic Curve Based
Signcryption Approach"
Abstract- Data Security has become a challenging task
due to natural problems of power, memory and
processing constraints over the wireless network.
Hyper elliptic curve cryptosystem (HECC) is a well

Unsigncrypted Text

"An Implementation Of Hyperelliptic Curve Based
Signcryption Approach"
Abstract- Data Security has become a challenging task
due to natural problems of power, memory and
processing constraints over the wireless network.
Hyper elliptic curve cryptosystem (HECC) is a well

Enter Sender Private Key: 34765
SENDER PUB_KEY: 24474560

Enter Receiver Private Key: 97032
RECEIVER PUB_KEY: 68310528

Signcrypted Text

almtIFO32IRJg98/G/fhqcWmjvIRr3ED61mbjor
wu1wxAs2E+NkoVllm/MP7AGpKVvWUP2TV
2gfOOtHa0Gr3H/1+lwZPlcZPTLIFoXJ0a5Fjqr

Value of r: 3ddb0f3eb5751b594bfcd727b35887f5

Value of r': 3ddb0f3eb5751b594bfcd727b35887f5

MESSAGE AUTHENTICATED

Fig. 1 Snapshot of Implementation of Hyperelliptic curve based signcryption algorithm

4 SECURITY ANALYSIS OF THE PROPOSED SCHEME

A. Confidentiality

To achieve this we must make the data non-intelligible to the interceptor/eavesdropper. This is called confidentiality. The proposed scheme uses symmetric encryption scheme to encrypt the message by the encryption key K1.To find K1, an attacker needs to calculate db from $P_b=d_b$ D which is computationally infeasible (HCDLP).

B. Unforgeability

It is computationally infeasible to generate sender Signcrypted text for an attacker. An attacker needs private key of sender as well as secret k to generate sender Signcrypted text. An attacker should solve HCDLP $P_a=d_a$ D to find sender private key da and secret k which are computationally infeasible.

C. .Non-repudiation

It is computationally feasible for a third party to resolve dispute between sender and receiver in an event where sender denies the origination of the Signcrypted text. Any trusted third party can resolve the dispute between sender and receiver in our proposed schemes using zero-knowledge protocol.

D. Public verifiability

The property when sender denies his sign the recipient can prove in a secure way that just legitimate sender has signed the message. The receiver can verify the signcrypted text through judge using zero-knowledge protocol in our proposed schemes.

5 COMMUNICATION COST ANALYSIS OF THE PROPOSED SCHEME

Cost is one of the major parameters of a cryptography technique. The comparative computation and communication cost analysis of our proposed scheme is as follows-

A. Comparative computational cost analysis

The major and expensive operation in HECC based schemes is hyperelliptic curve devisors scalar multiplication (HECDM). Signature and encryption technique have total 5 HECDM operations, 2 HECDM operations in encrypt and signing process and 3 HECDM operations in verify and decrypting process. Our proposed scheme has total 3 HECDM operations, one operation in signcryption process and two operations in unsigncryption process. On the base of these major operations Saving in computation cost is (2HECDM/ 5HECDM)=40%.

B. Communication cost analysis

Iin wireless media, usage of bandwidth is a major issue, so less communication cost is necessary. For this we assume that

| hash(u) |=|KH(u)|=|n|
C'= Chiper text in Signature then encryption technique
C=Chiper text in Signcryption technique
|C|=|m|
if |m|≥| D| then |C'|≥ 2|m|
if |m|≤ |D| then |C'|=2|D|
|D|=4|n| in case of genus 2.
Savings in communication overhead is

$$\frac{(|KH(u)|+|C'|+|n|)-(|KH(u)|+|C|+|n|)}{(|KH(u)|+|C'|+|n|)}$$

Which depends on the choice of parameters and amount of data. Minimum saving in communication overhead is 40%.

6 CONCLUSIONS

Hyperelliptic curve cryptography is on its way from pure academic interest to industrial applications. Due to the probabilistic results and creating at least double expansion of the message the Encryption techniques, based on ECC and HECC, did not gain popularity and problem can be solved by using the signcryption technique which provide the functionality of both Digital signature and encryption with a significant lower cost than the existing techniques. Our proposed signcryption schemes on Hyperelliptic curve shorthand digital signature algorithm fulfill all the security parameters of signcryption. The proposed scheme reduces 40% computation cost and a minimum of 40% communication overhead compare to existing signature and encryption approaches and is more suitable for m-commerce and wireless media due to small key size less computation cot and communication overhead.

REFERENCES

[1] C. Paul and J, Menezes, A, Vanstone "*Handbook of Applied Cryptography*" CRC Press, 1996.

[2] W. Diffie, M. Hellman, "New directions in cryptography" IEEE Trans. Inform. Theory Vol 22 Issue 6, pp 472–492,1976 978-1-4577-0768-1/11/$26.00 ©2011 IEEE

[3] Y, Zheng. "Digital signcryption or how to achieve cost (signature encryption) << cost (signature) +cost (encryption)" In *CRYPTO '97: Proceedings of the 17th Annual International Cryptology Conference on Advances in Cryptology*, pages 165{179, London,UK,1997.Springer-Verlag.

[4] N. Koblitz "Hyperelliptic cryptosystems " Journal of Cryptology Volume 1, Number 3, pages 139-150 1989

[5] X. Zhou "Improved Ring Signature Scheme Based on Hyper-Elliptic Curves "IEEE International Conference on Future Information Technology and Management Engineering, FITME pp 373-376 2009

[6] X. Zhou, X. Yang and P. Wei "Hyper-elliptic curves based group signature" Control and Decision Conference,CCDC '09, Chinese pp 2280-2284, 2009

[7] X. Zhou and Xiaoyuan Yang; "Hyper-Elliptic Curves Cryptosystem Based Blind Signature" Pacific-Asia Conference on Knowledge Engineering and Software Engineering, KESE '09 2009

[8] R. Ganesan and K. Vivekanandan "A Novel Hybrid Security Model for E-Commerce Channel" International Conference on Advances in Recent Technologies in Communication and Computing 2009

[9] R. Ganesan and K. Vivekanandan "A Secured Hybrid Architecture Model for Internet Banking (e-Banking) Journal of Internet Banking and Commerce vol. 14, no.1 April 2009,

[10] R. Ganesan, M. Gobi1and K. Vivekanandan "A Novel Digital

Envelope Approach for A Secure E-Commerce Channel" International Journal of Network Security,Vol.11, No.3, PP.121127, Nov. 2010

[11] Y. Lin and S. Yong-xuan "Effective generalized equations of secure hyperelliptic curve digital Signature algorithms" The Journal of China Universities of Posts and Telecommunications 17(2) pp 100–108 April 2010

[12] Dr. Suryakant Thorat, Mr. Madhav Bokare " A Dymanic Method To Secure Confidential Data Using Signcryption With Steganography". International Journal Of Engineering Science & Advanced Technology, Volume-2, Issue-2, 183 – 191, Mar-Apr 2012

[13] Nizamuddin, Shehzad Ashraf Ch., Waqas Nasar, Qaisar Javaid "Efficient Signcryption Schemes based on Hyperelliptic Curve Cryptosystem" 978-1-4577-0768-1/11/ ©2011 IEEE