Grenze International Journal of Engineering and Technology, Jul Issue

Lightweight Cryptographic Key Communication Technique in Wireless Network based on Hyperelliptic Cryptosystem(HECC)

[1]S. Sarvalakshmi and [2]CH. Suneetha
[1]Assistant Professor in Mathematics, MR PG College, Vijayanagaram, India
radhika1483@gmail.com
[2]Associate Professor in Mathematics, GITAM University, Visakhapatnam, India
gurukripachs@gmail.com

***Abstract*—Key management plays a major role in public key cryptosystem, especially using session keys changing the session key from time to time enhances the robustness of the cipher at every stage of its transmission from one end to the other. The mission of protecting the session keys against the adversary can be achieved by perfect forward secrecy (PFS). The present paper explains the digital signature algorithm with perfect forward secrecy (PFS) basing on Hyper Elliptic Curve Cryptosystem. Hyper Elliptic Curve Cryptosystem (HECC) provides equal security level as other conventional public key cryptosystems with shorter key length. The proposed digital signature algorithm strengthens the cipher in all directions of confidentiality authentication and integrity.**

***Index Terms*— Encryption, Decryption, Hyper Elliptic Curve Cryptography HECC, Divisors.**

I. INTRODUCTION

Public key cryptography is a new technology in cryptography archive record, discovered by Whitfield Diffe and Martin Hellman in 1976. Most popular public key cryptosystems are RSA, Deffi-Hellman key exchange protocols based on discrete logarithm of hard numbers. Elliptic curve cryptography is a revolutionary in public key cryptography proposed by Neil Koblitz and Miller in 1985 [1,2,3]. Since then, abundant research been done by several researchers. Two major issues influence the public key cryptography (i) key size (ii) computational risk. In view of these two factors Elliptic curve cryptography (ECC) has become popular and plenty of research has been done by several cryptographers over decades. Hyperelliptic curve cryptography (HECC) is generality of ECC introduced by Neil Koblitz [1]. HECC is one of the alternatives of ECC with simple base field used under constrained environment.

II. BASIC DEFINITION AND NOTATION

A. Definition: A field with finite number of elements is known as finite field, denoted by F_q. A prime integer n satisfying $b=a^n$ [4,5] is called the dimension of the field.

*B. Definition***:** A subset E of afield F is called subfield if E itself is a field under the same composition as F. Here F is called field extension of E and is denoted by F/E

Grenze ID: 01.GIJET.7.2.33
© Grenze Scientific Society, 2021

C. *Definition* : A field extension F/E is known as algebraic if an element a in F is algebraic over E. E is s algebraically closed if a non-zero polynomial with coefficients in E has roots in E, and is denoted by $\overline{E}$ [4,5]

A Hyper Elliptical Curve (HEC) of genus $g \geq 2$ over the finite field F_q is defined as $y^2+h(x)y=f(x) \bmod q$. Here h(x), f(x) are polynomials in the field. F(x) with degree of $h(x) \leq g$ and h(x) is monic with degree $\leq 2g+1$. The curve is nonsingular if there is no point in the algebraic closure of F_q satisfying the equations $2y+h(x)=0$ $h'(x)y - f'(x)=0$. Set of all points $\{P(p_1,p_2)/ (p_1,p_2) \in FXF\}$ is called set of rational points, and there is a special point denoted by ∞. If $P= (p_1, p_2)$ is a point on the curve HEC, then $\tilde{P}=(p_1, p_2-h(p_2))$ is called opposite point. If $P=\tilde{P}$ then P is called a special point, otherwise P is called an ordinary point. The chord and tangent rule like elliptic curve does not apply here for the curves with genus $g \geq 2$ because any intersecting line on the curve intersects at (2g+1) points on the curve. An abelian group structure is formed by set of all divisors of Jacobian of HEC with the composition addition of divisors.

D. *Definition*: *Divisors*: A divisor is the summation of scalar multiplication of points on the hyper elliptic curve HEC $D= \sum_{p_i \in HC} m_i p_i$, $m_i \in Z$, except for finite number of m_i. Here m_i is called the order of the divisor D at the point P [6]. The degree of the divisor D is $\sum_{p_i \in HC} m_i$ and is denoted by deg (D)= $\sum_{p_i \in HC} m_i$

If the degree of the divisor is zero it is denoted byD^0. The divisors $D_1= \sum_{p \in HC} m_i p_i$ and $D_2= \sum_{p \in HC} n_i p_i$ can be added as $D_1+D_2= \sum_{p \in HC} (m_i + n_i) p$

Set of all divisors forms a group under the composition addition of divisors.

Set of all divisors with degree zero is subgroup of set of divisors. $D^0 \subset D$.

The greatest common divisor of D_1, D_2 is $\gcd(D_1,D_2)= \sum_{p \in HC} \min(m_i, n_i) p - (\sum_{P \in HC} \min(m_i, n_i))\infty$ so, greatest common divisor of two devices D_1,D_2 has degree Zero.

A divisor D^0 is said to be principal divisor if it is the divisor of rational function R.

D= div(R) where R is a rational function in the finite field of the curve $\overline{K}(HC)$, $R \in \overline{K}(HC)$ and $\overline{K}(HC)$ is the algebraic closure of the field K.

If $R= G_1/ G_2 \in \overline{K}(HC)$, then the order of R at the point $P \in HC$ is $ord_p(R) = ord_p(G_1)-ord_p(G_2)$.

Set of all principal devisors P is a sub group of set of all divisors of degree zero.

$P \subset D^0 \subset D$

E. *Definition*: If D^0 is group of divisors of degree zero, P is group of principal divisors then a quotient group $J=D^0/P$ is called Jacobian of the curve HEC.

For two divisors D_i, D_j for $i \neq j$.

$D_i \sim D_j \Rightarrow D_i - D_j \in P$ then D_i, D_j are equivalent divisors.

F. Definition: If D is a divisor D= $\sum_{p \in HC} m_p P$ then the support of D is a set of all points in the divisor, denoted by Supp(D)

Supp(D)= { $p \in HC / m_p \neq 0$ }

G. Definition: A divisor D is semi reduced [6] if it takes the form

D= $\sum_{p_i \in HC} m_i p_i - (\sum m_i)\infty$, p_i's are point on the curve HC such that if P $\in$ Supp(D) then $\tilde{P} \notin Supp(D)$ if P is an ordinary point .

If P is a special point, then P= $\tilde{P}$ then m_i= 1

H. Definition: A semi reduced divisor is said to be reduced if it satisfies the property $\sum m_i \leq g$,the genus of the curve. A divisor on the hyper elliptic curve can be represented in two ways (i) simple point representation like a point on elliptical curve(ii) Mumford representation as polynomials. In point representation a divisor is summation of scalar multiplication of points D = $\sum m_i p_i$

In Mumford representation a reduced divisor is represented by polynomials [u(x),v(x)] which useful for computation in the extension $\bar{K}$(HC).where u(x) is a monic polynomial given by

$$u(x) = \prod (x - x_i)^{m_i}.$$

x_i are the $x-$ cordinates of the points in the support with multiplicities m_i.

$$v(x) = \sum \pi \frac{x - x_i}{x_{i-} x_j} \text{ for } j \neq i$$

The degree of the polynomial v(x) is one less than the degree of U(x) and less than or equal to g.

v(x) is a polynomial such that V $(x_i) = y_i$ for $m_i \neq 0$

$u(x)/(v(x))^2 + v(x)h(x) - f(x)$

To find out the polynomial V(x) we use chines remainder theorem of polynomials. In the field F, if $p_1(x), p_2(x)$ ... ...are polynomials;$q_1(x), q_2(x)$ ... . are relatively prime polynomials pairwise.

Then

$$f(x) \equiv p_1(x) \bmod q_1$$
$$\equiv p_2(x) \bmod q_2$$
$$\vdots$$
$$\equiv p_k(x) \bmod q_k$$

$Q = \prod_i q_i$ $Q_i = \frac{Q}{q_i}$, $1/Q = \sum_i \frac{M_i}{q_i}$

$f(x) = [P_1 M_1 Q_1 + P_2 M_2 Q_2 + \ldots\ldots\ldots] \bmod Q$

For example,

$$y^2 = x^5 - 4x^4 - 14x^3 + 36x^2 + 45x$$

Consider the points P = (3,0) Q=(5,0) R=(1,8)

The divisor

D = [P]+[Q]+[R] =3[0] in Munford representation is D = [u(x), v(x)]

$u(x) = (x-3)(x-5)(x-1)$

$=(x-3)(x^2-6x+5)$

$= x^3-6x^2+5x-3x^2+18x-15$

$=x^3-9x^2+23x-15$

$v(x) = r x^2+s x + t$

v(3)=0, v(5)=0, v(1)=8

$9 r + 3s + t =0$

$25 r +5 s +t=0,$

Solving $r + s+ t =8$

$v(x) = x^2-8x+15$

$\therefore D = [x^3-9x^2+23x-15, x^2-8x+15]$

III. Addition of Divisors [Contour Algorithm]

Since there is a bijection mapping from the points on the curve to the divisors in Jocobian Jac(E) one can define the arithmetic on divisors. An algorithm for adding two reduced divisors in the Mumford form is called contour algorithm. The result in contour algorithm is also in Mumford form.
Suppose

$D_1 = (a_1, b_1) = [a_1(n), b_1(n)]$

$D_2 = (a_2, b_2) = [a_2(n), b_2(n)]$ are two reduced divisors in the Mumford form then the steps involved in contour algorithm are

1. Computation of polynomials $d_1, E_1, E_2 \in \bar{K}$ (n)
   Where $d_1 = \gcd(a_1, a_2)$ and $d_1 = E_1 a_1 + E_2 a_2$
2. Using extended Euclidean algorithm
   Computation of the polynomials d, F_1, $F_2 \in \bar{K}$ (n)
   Where $d = \gcd(d, b_1+b_2+h)$ and $d = F_1 d_1 + F_2(b_1+b_2+h)$
3. $T_1 = F_1 E_1$
   $T_2 = F_1 E_2$
   $T_3 = F_2$
   From these three equation $d = T_1 a_1 + T_2 a_2 + T_3 (b_1+b_2+h)$
4. Set $a = \frac{a_1 a_2}{d^2}$
   $b = \frac{T_1 a_1 b_1 + T_2 a_2 b_1 + T_3(b_1 b_2 + f)}{d} (mod\ a)$
5. $a' = \frac{f - bh - b^2}{a}$
   $b' = -h - b (mod\ a')$
6. If $\deg(a') > g$ then set $a=a', b=b'$ and go to step 5 until $\deg(a') \leq g$
7. a' is mode monic polynomial
8. $D_1 + D_2 = (a', b')$.

IV. Hyper Elliptic Curve Discrete Logarithm Problem (HCDLP):

The strength of HECC depends on discrete logarithm problem [7]. Consider two divisors D1, D2 of the jacobian group. It is hard to find an integer l such that $D2 = lD1, 0 \leq l \leq n-1$ where n is the order of the divisor D1

V. Perfect Forward Secrecy (PFS)

Perfect Forward Secrecy is a special feature in public key cryptography to protect the future communication whenever the most recent key is hacked or compromised. This is a process of safeguarding the main key, by frequently changing the session keys. So a minimum amount of secret and sensitive information of the data is exposed whenever the transmission of the data is interrupted by the adversary.

VI. Literature Survey

Hyper elliptic curve cryptosystem achieved a good characteristic of maintaining same security level when compared to other public key cryptosystems, with an additional advantage of using small key size. Hyper Elliptic Curve (HEC) with genus 3 has a base field of 60 bit whereas Elliptic Curve (EC) takes 180 bits, RSA has 1024 bits. Key storage space is also very small when compared to other public key cryptosystems. This is the reason that HECC is considered as better alternative of ECC, by several researchers in the history of cryptography. The strength of HECC depends on hardness of solving Hyper Elliptic Curve Discrete Logarithm Problem (HCDLP) which involves the arithmetic on divisors in the jacobian group. This is another good feature of HECC which attracts the attentions of cryptographers. Nizamuddin etal [8] proposed an efficient signencryptian schemes basing on HECC with an additional feature of forward secrecy. R Ganesan, K.Vivekanandan [9,10,11] proposed hybrid security schemes for E-Commerce using HECC. Y. Lin and S. Yong-xuan, [12] proposed Digital signal algorithm based on HECC . Yasuyuki Sakai Kouichi Sakurai [13] proposed HECC in small characteristic. P. Vijay Kumar et.al. [14] proposed comparative study of HEC over prime field

VII. Proposed Scheme

The present paper explains the secret key communication amongst multiple legitimate peers in a group of network, using Hyper elliptic curve cryptosystem. All the genuine users of the group can communicate one another by sharing different individual secret keys. Here a Hyper elliptic curve HEC with genus ≥ 2, over the finite field F_q is public, with q as large prime number $\geq 2^{80}$ When two users Alice and Bob want to transmit the messages, they agree upon to use the curve HEC (F_q) and divisor D of order n. The divisor D is selected so that the order of the divisor is a big prime number in the Jacobian Jac (F_q) n $\geq 2^{80}$.

Alice selects a large random number k less than the order of the group, a divisor K on the curve computes H=KD, $I=D^1+Kk$. Alice publishes H, I as her public keys. Similarly, Bob selects a large number m less than the order of the group, a divisor M on the curve. He computes J=Md, $L=D^1+Mm$. He publishes J, L as his public keys.

VIII. Encryption

A code table assigning all ASCII characters to divisors is an agreement between the users. If Bob wants to communicate the secret key for a specific communication, it is assigned to a divisor S on the curve, S is a pair of polynomials $[a_1(x), b_1(x)]$. Two polynomials are combined together by algebra of functions say

$S=P_1a_1(x)+P_2b_1(x)$ with P_1, P_2 as arbitrary constants.

Bob encrypts the secret key S using his secret key and Alice's public key as

$S^E=S+mH+I+mM$. He communicate S^E to Alice is a public channel.

The Hyper Elliptic Curve $HC(F_q)$,the divisor D are public.

Alice	Bob
H,I are public keys	J,L are public keys
Large random number k, Divisor K are secret keys	Large random number m, Divisor M are secret keys

For authenticating the message Bob combines Alice's public key H, S^E together and finds the one way hash function $H[H \parallel S^E]$, the hash value is tagged to the encrypted secret key and communicates to Alice.

IX. Decryption

Alice after receiving the encrypted secret key along with authentication has value first verifies the hash value first verifies the hash value then decrypts the secret key as

$S= S^E$ -kJ-L-kK=S

S=S+mH+I+mM-kJ-L-kK

$S=S+mkD+D^1+kK$ +mM-kmD-D^1-mM-kK

S=S

X. Security Analysis

Hyper Elliptic cryptosystems (HECC) provide solution for key distribution, information exchange, signencryption and digital signature. The security of the HECC depends on the strength of Discrete Logarithm Problem (DLP). A well-known attack on ECC is Pollard-Rho attack to break the discrete logarithm ECDLP. Since HE curve arithmetic is heavy and cumbersome implementing the Pollard Rho attack to crack the discrete logarithm problem is not so easy as in ECC.

Through the encryption keys are fully or partially compromised future keys will not be damaged since the document is twice digitally signed by encrypting the secret key S to S^E, appending the hash value $H[H \parallel S^E]$to the document. Since the message is authenticator at two different stages digital signature and append Hash value, an adversary cannot generate and replace the legal digital signature. This provides the cipher perfect forward secrecy and protects against the signature forgery. The communicated message achieves another good property non-repudiation since the divisors used for digital signature is an agreement between the users. To obtain the perfect forward secrecy, the legitimate users can change S time to time. Basic operations in HECC is scalar multiplication of divisors.

XI. Performance Analysis

Research shows that addition and point doubling operations are more cumbersome in HECC, when compared to ECC. So EC $\left[F_2^{31}\right]$ has group order 2^{62}, time taken for addition or Scalar multiplication is 0.82 secs; EC $\left[F_2^{31}\right]$ has group order 2^{63}, time consumption is 1.62 seconds.

Coming to the conventional El-Gamal encryption HECC with genus2 has operation size very small when compared to ECC as genus ≥ 2.

So HECC is more advantageous under some special circumstances, due to the feature that it has short operand size.

XII. Conclusions

Hyperelliptic curve cryptosystem provides all the required features of a good encryption algorithm like confidentiality, integrity, nonrepudiation, forward secrecy. It protects the cipher from signature forgery using limited resources maintaining same level of security as the other conventional public key cryptosystems. The present digital signature algorithm is more secure with less computation overhead and computation cost.

References

[1] Neil Koblitz, “An elliptic curve implementation of the finite field digital signature algorithm”, in Advances in cryptology, (CRYPTO 1998), Springer Lecture Notes in computer science, 1462, 327-337,1998.

[2] Koblitz N., “A course in number theory and cryptography”, Springer-Verlag New York Inc., 1987.

[3] Koblitz N., “Elliptic curve cryptosystems, mathematics of computation”, Vol. 48, No. 177, pp. 203-209, January 1987.

[4] M. Fouquet, P. Gaudry and R. Harley. An extension of Satoh’s algorithm and its implementation. J. Ramanujan Math. Soc., 15, 281–318, 2000.

[5] G. Frey and H.-G. R¨uck. A remark concerning m-divisibility and the discrete logarithm problem in the divisor class group of curves. Math. Comp., 62, 865– 874, 1994.

[6] D.G. Cantor. Computing in the Jacobian of a hyperelliptic curve. Math. Comp., 48, 95–101, 1987.

[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] "Signcryption schemes with forward secrecy based on hyperelliptic curve cryptosystem " , Nizamuddin; Shehzad Ashraf Ch.; Noorul Amin, IEEE 2011 "978-1-4577-1169-5/11/$26 © 200 IEEE"

[9] 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.

[10] 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.

[11] R. Ganesan, M. Gobil and 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.

[12] 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, vol. 17, no. 2, pp. 100-108, April 2010.

[13] Yasuyuki Sakai Kouichi Sakurai, "Design of Hyperelliptic Cryptosystems in Small Characteristic and a Software Implementation over F_2^n Advances in Cryptology — ASIACRYPT'98 pp 80-94

[14] P. Vijayakumar, V. Vijayalakshmi, G. Zayaraz, "Comparative Study of Hyperelliptic Curve Cryptosystem over Prime Field and Its Survey" International Journal of Hybrid Information Technology , Vol.17 .No.1(2014)