Grenze International Journal of Engineering and Technology, January Issue

Forward Secrecy Maintenance by Digital Signature Based on Hyperelliptic Cryptosystem

Sarvalakshmi Surampally[1] and Suneetha CH[2]
[1]Scholar in GITAM (Deemed to Be University), Department of mathematics, Visakhapatnam, 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.**

Keywords: **Encryption, Decryption, Hyper Elliptic Curve Cryptography HECC, Divisors.**

I. INTRODUCTION

Public key cryptography is an advanced technology in cryptography archive record, discovered by Whitfield Diffe and Martin Hellman in 1976. Most popular public key cryptosystems are RSA, Diffie-Hellman key exchange protocols based on discrete logarithm of hard numbers.
Elliptic curve cryptography is a revolutionary in public key cryptography put forward 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 a finite number of elements is known as finite field, denoted by F_q. A prime integer ν satisfying $\alpha=\beta^{\nu}$ [4,5] is called the dimension of the field.

Grenze ID: 01.GIJET.11.1.320

B. Definition:

F is field and *E* is a nonempty subset of *F*, *E* is said to be a field if *E* itself a field with respect to same binary operations on *F*. Here *F* is called field extension of *E*, denoted by *F/E.*

C. Definition:

If an element α in *F* is algebraic over *E* then the field extension *F*/*E* is algebraic. A non-zero polynomial with coefficients in *E* has roots in *E* then we say that *E* is algebraically closed and is denoted by Ê. [4,5].

A *Hyper Elliptical Curve (HEC)* of genus g ≥ 2 over the finite field F_q is defined as r^2+h(s)r=f(s) mod q. Here h(s), f(s) are polynomials in the field F with degree of h(s) ≤ g and h(s) is monic with degree ≤ 2 g +1. The curve is nonsingular if there is no point in the algebraic closure of F_q satisfying the equations 2r+h(s)=0, h' (s)r – f' (s)=0. Set of all points {*P* (p_1, p_2)/ (p_1, p_2) ∈ *F*x*F*} is called set of rational points, and we denote ∞ as a special point. Take a point P= (p_1, p_2) 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 do not apply here for the curves with genus g ≥ 2 because any intersecting line on the curve intersects at (2 g +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:

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

If the degree of the divisor is zero it is denoted by D^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= $\sum_{p \in HC} (m_i + n_i)p$

If we take addition as a binary operation then the set of all divisors forms a group.

D^0 is the set of all divisors with degree zero and it is subgroup of set of divisors *D*. i.e. $D^0 \subset D$.

We define *g. c. d.* (D_1, D_2) = $\sum_{p \in HC} \min(m_i, n_i)p - (\sum_{P \in HC} \min(m_i, n_i))\infty$ and it is called the greatest

Common divisor of two devisors D_1, D_2. So, greatest common divisor of two devisors D_1, D_2 has degree Zero.

If D^0 is the divisor of rational function $\mathscr{R}$ then D^0 is called a principal divisor.

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

If $\mathscr{R}$ = $\hat{G}_1/\hat{G}_2 \in \bar{K}(HC)$, then the order of $\mathscr{R}$ at the point P ∈ *HC* is $ord_p(\mathscr{R}) = ord_p(\hat{G}_1) - ord_p(\hat{G}_2)$.

A set consisting of all principal devisors *P* form a sub group of set of all divisors of degree zero.

$P \subset D^0 \subset D$

E. Definition: The Jacobian of the curve HEC is a quotient group J=D^0/P where D^0 is group of divisors of degree zero& *P* is group of principal divisors.

The two divisors D_i, D_j are said to be equivalent divisors if $D_i \sim D_j \Rightarrow D_i - D_j \in P$ for i ≠ j.

F. Definition: Let *D*= $\sum_{p \in HC} m_p P$ be a divisor. The support of a divisor *D* is the set of points{ $p \in HC / m_p \neq 0$ } and it is denoted by Supp(*D*). i.e. Supp(*D*)= { $p \in HC / m_p \neq 0$ }

G. Definition: A divisor *D* is in the form *D*= $\sum_{p_i \in HC} m_p p_i - (\sum m_p)\infty$ having the following properties

$m_p \geq 0$

If P≠ $\tilde{P}$ and $m_p > 0$ then $m_{\tilde{p}} = 0$

If P= $\tilde{P}$ and $m_p > 0$ then $m_{\tilde{p}} = 1$ is called a semi-reduced divisor [6] and it is a zero-degree divisor.

H. Definition: A semi reduced divisor is said to be reduced if it satisfies the property $\sum m_p \leq$ 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 [μ (x), ν(x)] which useful for computation in the extension $\overline{K}(HC)$. where μ(x) is a monic polynomial given by

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

x_i are the $x-$ cordinates of the points in the supp(D) with multiplicities m_i.

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

The degree of the polynomial ν (x) is less than the degree of μ (x) and less than or equal to g

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

$$\mu(x)/[(\nu(x))^2 + \nu(x)h(x) - f(x)]$$

To find out the polynomial ν (x) we use Chinese 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

$$f(x) \equiv p'_1(x) \bmod q'_1$$
$$\equiv p'_2(x) \bmod q'_2$$
$$\vdots$$
$$\equiv p'_k(x) \bmod q'_k$$

$Q = \prod_i q'_i$ $\quad Q_i = \frac{Q}{q'_i}$, $1/Q = \sum_i \frac{M_i}{q'_i}$

$f(x) = [p'_1 M_1Q_1 + p'_2M_2Q_2 + \ldots\ldots\ldots] \bmod Q$

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 = [μ(x), ν(x)]

$\mu(x) = (x-3)(x-5)(x-1)$

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

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

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

$\nu(x) = r x^2 + s x + t$

$\nu(3)=0, \nu(5)=0, \nu(1)=8$

$9 r + 3s + t = 0$

25 r +5 s +t=0,

r + s+ t =8, By solving these equations we get

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

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

II. Addition of Divisors [Contour Algorithm]

Since there is a bijection mapping from the points on the curve to the divisors in Jacobian 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

- Computation of polynomials $d'_1, \dot{E}_1, \dot{E}_2 \in \bar{K}(n)$
  Where $d'_1 = g.c.d.(a^*_1, a^*_2)$ and $d'_1 = \dot{E}_1 a^*_1 + \dot{E}_2 a^*_2$
- Using extended Euclidean algorithm
  Computation of the polynomials $d', F_1, F_2 \in \bar{K}(n)$
  Where $d' = g.c.d.(d', b^*_1+b^*_2+h)$ and $d' = F_1 d'_1 + F_2(b^*_1+b^*_2+h)$
- $T_1 = F_1\dot{E}_1$

$T_2 = F_1\dot{E}_2$

$T_3 = F_2$

From these three equation $d' = T_1 a^*_1 + T_2 a^*_2 + T_3 (b^*_1+b^*_2+h)$

- Set $\tilde{a} = \frac{a^*_1 a^*_2}{d'^2}$

  $\tilde{b} = \frac{T_1 a^*_1 b^*_1 + T_2 a^*_2 b^*_1 + T_3(b^*_1 b^*_2 + f)}{d'} (mod\ \tilde{a})$

- $\tilde{a}' = \frac{f - \tilde{b}h - \tilde{b}^2}{\tilde{a}}$

$\tilde{b}' = -h - \tilde{b} (mod\ \tilde{a}')$

- If deg $(\tilde{a}') > g$ then set $\tilde{a} = \tilde{a}'$, $\tilde{b} = \tilde{b}'$ and go to step 5 until deg $(\tilde{a}') \leq g$.
- $\tilde{a}'$ is monic polynomial
- $D_1 + D_2 = (\tilde{a}', \tilde{b}')$.

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 ⌊ such that D1= ⌊ D2,0 ⌊ 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 maintain 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 rely on rigorousness 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.

V. Proposed Scheme

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 Rohit and Anu 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 $\geq 2^{80}$.

Rohit chooses a big arbitrary number a lesser than the order of the group and a divisor A on the curve. He calculates A_1= a (*D*+ A) and A_2= a A
A_1, A_2 are made public by Rohit, 'a' is the secret key for Rohit.

In the same way Anu choose a large number b at random $\leq 2^{80}$, a divisor B and calculates.
B_1= b (D+ B); B_2= b B
She Publishes B_1, B_2 keeping the random number 'b' as secret.
Here A_1, A_2, B_1, B_2 act as general public keys of Rohit and Anu respectively.
In the next phase Rohit again computes A B = a B_2, Anu computes B A = b A_2, publishes as specific public keys to each other. specific public keys to each other plays a major role in encryption/decryption.
Several genuine users of the same group can establish communication using the general public keys A_1, A_2, B_1, B_2 and sharing the specific public keys pairwise to each other.

VI. Digital Signature Algorithm

If Anu wants to sign her document digitally, she selects a divisor S on the curve. S has a pair of polynomials μ(x), ν(x), S = [μ(x), ν(x)]

For conventional encryption, single polynomial C(x) is generated. For example

C (x)=k[μ(x)] + h[ν(x)]

S is encrypted as S^E=bA_1+AB+ S

Anu appends the digital signature to her encrypted document and communicates to rohit.

Rohit after receiving the document verifies the digital signature of as S=S^E-aB_1-BA

$$S= bA_1+AB+ S -aB_1-BA$$

$$S= ba (D+A) +aB_2+S-ab(D+B)-bA_2$$

$$S =baD + baA +abB + S – abD - abB - baA$$

$$S = S$$

To maintain the perfect forward secrecy anu combines S, S^E together and finds the one-way hash function $H[S \parallel S^E]$, communicates to Rohit for authenticating the communication.

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

TABLE I

Rohit	Anu
A_1, A_2 general public keys.	B_1, B_2 general public keys.
AB specific public key to Communication with Anu.	BA specific public key to Communication with Rohit.
Large random number a, A are secret.	Large random number b, B are secret.

VII. SECURITY ANALYSIS

Hyper Elliptic cryptosystems (HECC) provide solution for key distribution, information exchange, sign encryption 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 curves 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 toS^E, appending the hash value $H[S \parallel S^E]$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.

VIII. 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.

IX. CONCLUSIONS

Hyper elliptic 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 provided equal 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)