International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 5 Issue VII, July 2017- Available at www.ijraset.com

Algebraic Curve Cryptographic Schemes: A Survey

Geenia[1], Mrs. Ritu Nagpal[2]
[1]*Research Scholar,* [2]*Assistant Professor, Department of Computer Science*
Guru Jambheshwar University, Hisar, India

Abstract*: *Various Public-Key Cryptographic Schemes rely upon security and performance among other functionalities. Since the introduction of Public-Key Cryptography by Diffie and Hellman in 1976, a number of schemes have been proposed based on Discrete Logarithm Problem. Among these, Elliptic Curve Cryptography (ECC) is the most mysterious and not easily understood. It is based on algebraic curve arithmetic. The paper starts with brief introduction of Elliptic Curve Arithmetic. Many other cryptosystems based on Discrete Logarithm Problem were introduced using different curves like Hyper-elliptic Curve Cryptography, Edward Curve Cryptography, and Probability Symmetric Curve Cryptography etc. This paper presents all forms of curve based public key cryptographic schemes and their features. The properties of these curves have also been discussed.
Keywords: Cryptosystem, Elliptic Curves, PSCC, SCC, HECC, encryption, decryption

I. INTRODUDCTION

In the age of electronic connectivity across world, and viruses, fraud, eavesdropping, there is great need for security across networks. Network security protects data from unauthorized access. All data cannot be protected physically; the data that is being shared through network needs to be secured. Some hardware and software technologies are used to manage usability and integrity of data. To protect data, cryptography is used which helps in converting data to unintelligible code. Two processes are involved i.e. encryption and decryption. Two types of cryptographic techniques are private key and public key encryption. Private Key cryptography uses one shared key for encryption and decryption at sender and receiver's end respectively where as public key cryptography uses two keys that need not to be shared.

The idea of public key cryptography was given by Diffie and Hellman [1] in 1975 to address disadvantages of Private Key Cryptography. In this scheme, the keys shared are not kept secret but authenticity is maintained. And there is one important property that one cannot retrieve private key by knowing about public key. The security of Asymmetric Cryptosystems requires some fundamental security features i.e. Confidentiality, Non-repudiation and Key Authentication [2].

A key pair is selected and computation is required to derive one key from another which is believed to be very difficult [3]. Various schemes that have been introduced are RSA, ElGamal and Elliptic Curve Cryptography. RSA is based on factorization problem [4] .We will discuss here Elliptic curves and other curve based cryptosystems developed after it.

This paper discusses various cryptosystems based on public key algorithm using algebraic curves. The most widely known algorithm i.e. Elliptic Curve Cryptography is described in section 2. Section 3 describes the use of Hyper-elliptic curves in cryptosystems. Section 4 presents other recently developed algorithms to replace ECC for harder security. Two such algorithms are Probability Symmetric Curve Cryptography (PSCC) and Sextic Curve Cryptography (SCC). Section 5 concludes the paper.

II. ELLIPTIC CURVE CRYPTOGRAPHY

A. Elliptic Curve

Elliptic Curve Cryptography (ECC) is based on elliptic curve theory proposed by Miller [5] and Koblitz [6] which is used for creating smaller keys for encryption. The points on Elliptic curve form an abelian group. General equation of elliptic curves is:

$$Y^2=X^3+AX^2+B, \text{ where}$$

A and B are integer constants and $4A^2+27B\neq0$.

B. Elliptic Curve Cryptosystem

Elliptic curve cryptosystem is a technique based on Discrete Logarithm Problem(DLP) which states that - If a point on elliptic curve let us say P is multiplied n times such that R= nP, where n is sufficiently large then given P and R, it is difficult to find n [7]. This can be found by taking discrete log which takes very large time. So main operation in ECC is point multiplication with a large scalar. ECC can be implemented in many fields like prime field, binary field and extended binary field. Scalar multiplication is the basic operation in ECC and its implementation must be computationally less expensive. ECC gives an advantage when limited memory devices are to be used. ECC is a complicated algorithm often used as hardware because its software implementation is not

very efficient for real time tasks. It consists of various arithmetic operations that can be configured on hardware easily. It is generally considered that, for operands of a few hundred of bits, S/M ~ 0.8, M being the cost of a modular multiplication and S that of a squaring. The cost of a modular inversion is much higher than that of multiplication. In smartcards it has been observed that I/M ~ 100, I being the cost of a modular inversion[8].

C. *Arithmetic of Elliptic Curve*

There are four basic operations possible on elliptic curves i.e. addition, subtraction, multiplication and inversion of points. Any operation on two points on the curve results into third point which also lies on the same curve.

1) *Addition:* There is a chord-and-tangent property for addition operation on curves where two points if known can be used to get a third point on curve which is the addition of the given two points. The set of points on elliptic curves forms an abelian group where all the points if subjected to any mathematical operation such as addition or multiplication gives resulting points belonging to that set only. Here the resulting points lie on the curve itself. A point at infinity is considered and symbolically represented as ∞. By drawing a line through the two points taken randomly on a curve say P and Q, the third point of intersection on curve is the mirror reflection of the point R which is the arithmetic addition of these two points [9]. The explicit formulae for addition of points on elliptic curves are:

$$X_3 = Z^2 - X_1 - X_2 \pmod p$$
$$Y_3 = Z\,(X_1 - X_3) - Y_1 \pmod p \text{ where,}$$
$$Z = (Y_2 - Y_1) / (X_2 - X_1) \pmod p$$

2) *Multiplication:* Several multiplication algorithms exist like Kasturba [10] and Montgomery [11] algorithm. One that is used mostly is binary add and shift Montgomery algorithm [12]. We actually need two operations to complete one multiplication algorithm and this include a doubling operation also which needs to be explained. .

3) *Doubling:* For adding any point to itself is the doubling operation and tangent rule applies here. The Tangent drawn through the point say P, intersects the curve on a point which is the mirror reflection of point 2P [7]. The explicit formulae for doubling the point on elliptic curve are:

$$X_3 = (3X_1^2 + A / 2Y_1)^2 - 2X_1 \pmod p$$
$$Y_3 = (3X_1^2 + A/2Y_1)\,(X_1 - X_3) - Y_1 \pmod p$$

4) *Inversion:* Here division operation is replaced by inversion operation due to modulus operation involved. Multiplicative inversion is the most difficult operation during implementation of algorithm. For this problem, projective coordinates are introduced which when used instead of affine coordinates no inversion operation is required.

III. HYPER-ELLIPTIC CURVE CRYPTOGRAPHY

Definition (hyper-elliptic curve) Let K be a field and let K* be the algebraic closure of K. A Hyperelliptic curve C of genus g over K (g >= 1) is an equation of the form

$$C: v^2 + h(u)v = f(u) \text{ in } K[u,v] ,$$

where h(u) is a polynomial of degree at most g, f(u) is a monic polynomial of degree 2g+1. Hyper-elliptic curves do not have singular points [13].

In 1988, Koblitz [14] put forward this algorithm as an improvement to ECC. It is also based on discrete logarithm based problem. These cryptosystems are suitable for embedded processors, where less power must be used and time is also less because short operand size is possible. Selection of curve is the most important step while implementing hyper-elliptic curve cryptographic scheme. Factors like choice of curve, scalar multiplication method influence speed of encryption .To implement a discrete log cryptosystem using hyper-elliptic curves we need a curve for which arithmetic over field K can be efficiently implemented and the order of Jacobian of curve say J(K) of C should be divisible by a prime number of at least 45 decimal digits. Assuming HEC of genus g over field K_q where $q=p^n$, we can have q^g possible divisors which form Abelian group on which group operations can be easily implemented.

A. *Advantages*

1) Main advantage of using this curve is high efficiency and shorter key length.
2) Security of hyper-elliptic curve cryptosystems is reliable because it has exponent complexity and no attacking algorithm is yet found with sub exponent complexity.
3) 60 bits of HECC match the security level of ECC with 180 bits and 1024 bits of RSA[15][16].

4) If the hyper-elliptic curve is chosen very carefully, only pollard rho attack is possible on it to crack.

B. Discrete Logarithm Problem in HEC

The DLP on J[K] can be stated as follows: If we have two divisors say d_1 and d_2 which belong to J[K] , then finding an integer m is the problem such that $d_1=md_2$. The operations include group addition and group doubling of divisors. Most general algorithm for addition and doubling is Cantor algorithm [17]. In this algorithm 1 inversion is required per addition and doubling operation which is very expensive operation [18].

IV. PSCC AND SCC

These two curves are a new milestone in symmetric curve cryptography. There are many algebraic curves based on which many cryptosystems have been designed.

A. Probability Symmetric Curve

Probability Symmetric Curve is a cubic curve widely used in theory of probability. The standard form of the curve is denoted by C(b,c) :

$$6y^2 = b\{11 - 18x + 9x^2 - 2x^3\} + c$$

Using the curve equation and a line which intersects the curve three times, we get a monotonic polynomial in x. The cubic polynomial has three roots of which two roots are our two known points say P and Q, third root can be calculated by arithmetic addition of these two points [19]. Thus PSCC gives a new approach to point addition and point doubling. The addition can be expressed as:

$$X_{P+Q} = -X_P - X_{Q+}(9a - 6j^2)/2a \pmod p$$
$$Y_{P+Q} = j(X_P - X_R) - Y_P \pmod p$$

B. Sextic Curve

It is another new approach which ensures harder security as compared to ECC. Sextic Curve or Atriphthaloid Curve is a six degree curve having large search space if DLP is considered here. General form of equation of curve denoted by S(a,b) :

$$X^4(X^2 + Y^2) - (aX^2 - b)^2 = 0$$

The discriminant of the curve must not be zero because if it is zero, curve will have cusps and curve will not be smooth which is not preferred in group operations on curves. The method of performing point addition and point doubling operation on this curve is same as PSCC. The equation produces different formulae for arithmetic addition and doubling of points on this curve. We have $X_{P+Q} = -X_P - X_Q - (1+2jk)/j^2 \pmod p$ and $Y_{P+Q} = j(X_P - X_{P+Q}) - Y_P \pmod p$, where line of intersection has equation $Y=jX + k$ [20].

Performance of PSCC and SCC when evaluated by using communication through sensor networks, the simulation results showed lesser amount of time for encryption in both as compared to ECC. For 64 bit key size PSCC takes 0.1 ms while ECC takes 0.5 ms [21].

V. CONCLUSION

This paper gives basic knowledge about various curve based cryptosystems. Shorter bit lengths in HECC have implementation advantage over ECC. It allows for bit lengths 50-80 while ECC allows 160-256 bit length keys. PSCC and SCC allowed much lesser time for encryption as compared to ECC algorithm. These three cryptosystems propose an improvement to ECC and can be implemented for higher level of secrecy and lesser amount of time.

Further, we would focus on other finite fields used with these curves like binary field, Optimized Extension Fields (OEF) etc. in future

REFERENCES

[1] W.Diffie and M.Hellman, "New directions in cryptography," IEEE transactions on Information Theory, vol. 22, no. 6, pp. 644–654, 1976.
[2] Ritu Makani, Yogesh Chaba , " Key Management based Multilevel Security Using Digital Signature and Encryption Techniques ," in International Research Journal of Computer Science (IRJCS) , vol. 1, no. 3 ,pp. 13-17 ,2014, ISSN 2393-9842.
[3] D. R. Hankerson, S. A. Vanstone, and A. J. Menezes, Guide to elliptic curve cryptography. New York: Springer, 2003.
[4] Ritu Makani, Navpreet Kaur , "Enhancing security by Authenticating the Diffie-Hellman Key Exchange Algorithm using RSA ," in International Journal of Information Technology and Knowledge Management , vol. 7, pp 188-194 , 2014.
[5] V.S.Miller, "Use of elliptic curves in cryptography," in Advances in cryptology, CRYPTO '85, vol. 218, pp. 417–426, 1986.
[6] N.Koblitz, "Elliptic curve cryptosystems," in Math. Computer, vol. 48, pp.203–209, 1987.

[7] J. Silverman, "Advanced Topics in the Arithmetic of Elliptic Curves," in Springer-Verlag, New York, 1994.
[8] V. Gayoso Martinez et al., "Implementation of Cryptographic Algorithms for Elliptic Curves," in Geometry, Algebra and Applications: From Mechanics to Cryptography, Springer International Publishing, 2016, pp. 121–133.
[9] Neal Koblitz, "Introduction to Elliptic Curves and Modular Form," Second Edition, Springer, 1993.
[10] F. Rodriguez-Henriquez and Q. K. Kog, "On fully parallel Karatsuba multipliers for GF(2m)," in International Journal of Network Security, vol.11, no.3, pp.155–162, 2010.
[11] C.-L.Wu, D.-C. Lou and T.-J. Chang, "An efficient Montgomery exponentiation algorithm for public-key cryptosystems," in Intelligence and Security Informatics, 2008.
[12] S. Revathi et al., "An Improved Scalar Multiplication over GD(2m) for ECC," in International Journal of Computer Applications , vol.163, no. 2,2017,ISSN 0975 – 8887.
[13] Henri Cohen et al. , "Handbook of Elliptic And Hyperelliptic Curve Cryptography" , Tailor and Francis Group, LLC, 2006.
[14] N.Koblitz, "Hyperelliptic cryptosystems," in Journal of Cryptology, pp.139-150, 1989.
[15] X. Zhou et al., "Hyper-elliptic curves based group signature," in Control and Decision Conference, CCDC '09, pp. 2280-2284, 2009.
[16] X. Zhou and X. Yang, "Hyper-Elliptic Curves Cryptosystem Based Blind Signature," in Pacific-Asia Conference on Knowledge Engineering and Software Engineering, KESE '09, 2009.
[17] D. Cantor, "Computing in the Jacobian of a Hyperelliptic curve," in Math. Comp, vol. 48, 1987.
[18] Gonda et al., "Improvements of addition algorithm on genus 3 Hyperelliptic curves and their implementations," in Proc. of SCIS, pp. 89–96 , 2004.
[19] W.R. Sam Emmanuel et al., "Safety Measures using Probability Symmetric Curve Cryptography," in International Journal of Computer Applications, vol.31, no.11,2011,ISSN 0975-8887.
[20] W.R. Sam Emmanuel et al., "Safety Measures using Sextic Curve Cryptography," in International Journal on Computer Science and Engineering, vol. 3,no. 2,2011, ISSN 0975-3397.
[21] W.R. Sam Emmanuel et al., "Performance Evaluation of Sextic Curve Cryptography and Probability Symmetric Curve Cryptography in Wireless Sensor Network," in International Journal of Computer Applications, vol. 61, no.4, 2013, ISSN 0975-8887.