Int. J. Advanced Networking and Applications
Volume: 05, Issue: 02, Pages:1883-1885 (2013) ISSN : 0975-0290

A New Public Key Cryptosystem based on Weil Pairing

B. K. Sharma
School of Studies in Mathematics, Pt. Ravishankar Shukla University Raipur (C.G.) 492010 India
Email: sharmabk07@gmail.com
Hemlal Sahu
School of Studies in Mathematics, Pt. Ravishankar Shukla University Raipur (C.G.) 492010 India
Email: hemlalsahu@gmail.com

----------**ABSTRACT**----------
In 1987 Koblitz and Miller first proposed public key cryptosystems using the group of points of an elliptic curve over a finite field. The security of these cryptosystems was based upon the presumed intractability of the problem of computing logarithm in the elliptic curve group. Now we propose a new cryptosystem over elliptic curves whose security is based on expressing a torsion point in terms of the basis points. Since latter is more complicated than solving ECDLP. Consequently our cryptosystem is more secure than all cryptosystems based on ECDLP.

Keywords - **Cryptography; cryptosystem; Elliptic curve; Weil pairing.**

Date of Submission: September 02, 2013 Date of Acceptance: October 07,2013

I. INTRODUCTION

Since the invention of public-key cryptography in 1976 by Whitfield Diffie and Martin Hellman [1] numerous public-key cryptographic systems have been proposed. The security of all of these systems was based on the difficulty of solving a mathematical problem. First realized public key cryptosystem was RSA [2] based on problem of solving factoring. In 1987 Koblitz [3] and Miller [4] first proposed public key cryptosystems using the group of points of an elliptic curve over a finite field. The security of these cryptosystems was based upon the presumed intractability of the problem of computing logarithm in the elliptic curve group The main advantage of Elliptic Curve Cryptography (ECC) is that its cipher key is much shorter than other cryptographies on the premise of same security. Shorter key means less management time and smaller storage which supplies convenience to realization of software and hardware. ECC hasn't been attacked by subexponent algorithm till now. So the scheme depends on difficulty of solving ECDLP is believed to be safer than those based on DLP [5] and IFP. Here we are proposing a cryptosystem whose security depends on difficulty of expressing a torsion point of Elliptic Curve into linear combination of basis points. If we are able to solve latter, then ECDLP can be easily solved. Thus our proposed cryptosystem is more secure. We first describe some requirements used in this paper.

II. ELLIPTIC CURVE

Let K = F_q be a finite field, where q is a power of some prime number. The Weierstrass equation of an elliptic curve over K can be written in the following form

$$y^2 + cxy + dy = x^3 + ax + b, where\ a, b, c, d \in K$$

If $q > 3$ then by a linear change of variables above equation can be reduced into too simpler form

$$y^2 = x^3 + ax + b\ with\ a, b \in GF(q)\ and\ 4a^3 + 27b^2 \neq 0\ .$$

An elliptic curve over K is the set of solutions of the Weierstrass equation with a point O, called point at infinity. An adding operation can be defined over the elliptic curve, which turns the set of the points of the curve into a group. The adding operation between two points is defined as follows.

In affine coordinate, let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be two points on the elliptic curve, neither being the point at infinity over $GF(q)$. The inverse of a point P_1 is $-P_1 = (x_1, -y_1)$. If $P_1 \neq -P_2$ then $P_1 + P_2 = P_3 = (x_3, y_3)$ with

$$x_3 = \lambda^2 - x_1 - x_2, y_3 = \lambda(x_1 - x_3) - y_1$$

where

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{if } P1 \neq P2 \\ \frac{3x_1^2 + a}{2y_1} & \text{if } P1 = P2 \text{ (doubling)} \end{cases}$$

III. TORSION POINTS

Let $m \geq 1$ be an integer. A point $P \in E$ satisfying $mP = O$ (point at infinity) is called point of order m in the group E. The set of points of order m is denoted by

$$E[m] = \{P \in E; mP = O\}$$

Such points are called points of finite order or torsion points. If P and Q are in E[m] then $P + Q$ and $-P$ are also in $E[m]$, so $E[m]$ is subgroup of E.

Volume: 05, Issue: 02, Pages:1883-1885 (2013) ISSN : 0975-0290

Proposition Let $m \geq 1$ be an integer

(1) Let E be an elliptic curve over R or C. Then
$$E(K)[m] = \frac{Z}{mZ} \times \frac{Z}{mZ}$$
(2) Let E be an elliptic curve over Fp and assume that p does not divide m then there exists a value k such that
$$E(F_{p^{jk}})[m] = \frac{Z}{mZ} \times \frac{Z}{mZ} \; for\ all\ j \geq 1$$

Proof. For the proof of proposition refer [6], Corollary III 6.4.

According to proposition, if we allow points with coordinates in a sufficiently large field, then E[m] looks like a 2-dimensional vector space over the field Z/mZ. Let's choose basis P_1, P_2 in $E[m]$. Then any element P € E[m] can be expressed in terms of the basis elements as P = $aP_1 + bP_2$ for unique a, b in Z/mZ. Expressing a point in terms of the basis points P_1, P_2 is more complicated than solving ECDLP.

IV. WEIL PAIRING.

Weil pairing is denoted by e_m, takes as input a pair of points $P, Q \in E[m]$ and gives as output an m[th] root of unity $e_m(P, Q)$.The bilinearity of the Weil pairing is expressed by the equations
$$e_m(P, Q_1 + Q_2) = e_m(P, Q_1).\ e_m(P, Q_2)..$$
$$e_m(P_1 + P_2, Q).\ e_m(P_1, Q).\ e_m(P_2, Q).$$
The weil pairing has many useful properties
(1) The values of the Weil pairing satisfy $(e_m(P, Q))^m = 1$ for all $P, Q \in E[m]$.
(2) The Weil pairing is alternative,which means that $e_m(P, Q) = 1$ for all P € E[m]
(3) TheWeil pairing is nondegenerate, which means that if $e_m(P, Q) = 1$ for all $Q \in E[m]$ then $P = O$.
For details refer [7].

Lemma If $P = aP_1 + bP_2, Q = cP_1 + dP_2$ and $\xi = e_m(P_1, P_2)$ then
$$e_m(P, Q) = \xi^{ad-bc.}$$

Proof.

$$e_m(P, Q) = e_m(aP_1 + bP_2, cP_1 + dP_2)$$
$$= e_m(aP_1, cP_1 + dP_2)e_m(bP_2, cP_1 + dP_2)$$
$$= e_m(aP_1, cP_1)e_m(aP_1, dP_2)e_m(bP_2, cP_1)e_m(bP_2, dP_2)$$
$$= e_m(P_1, P_2)^{ad}\ e_m(P_2, P_1)^{bc}$$
$$= e_m(P_1, P_2)^{ad-bc}$$
$$= \xi^{ad-bc.}$$

Now we propose a cryptosystem which security depends on expressing a point of elliptic curve in terms of the basis points.

V. A NEW PUBLIC KEY CRYPTOSYSTEM

We describe our new cryptosystem. The implementation of the proposed scheme involves the system initialization phase, the key generation phase, the encryption phase and the decryption phase.

System initialization phase

In the system initialization phase, the following commonly required parameters are generated to initialize the scheme.
(1) A field size q, which is selected such that, $q = p$ if p is an odd prime; otherwise, $q = 2n$' as q is a prime power.
(2) Two parameters $a, b \in Fq$ that define the equation of non supersingular elliptic curve E over Fq ($y^2 = x^3 + ax + b\ (mod q)$ in the case $q > 3$, where $4a^3 + 27b^2 \neq 0$) .
(3) A large prime number m, and basis points P_1 and P_2 of $E[m]$
(4) Weil pairing e_m: $E[m] \times E[m] \longrightarrow G$ where G is a multiplicative group of m[th] roots of unity generated by ξ = $e_m(P_1, P_2)$.

Key generation phase

In key generation phase, receiver U generates his public key, as follows
(1) Select randomly two numbers a and b from [1 to m − 1] and calculate
$$P = aP_1 + bP_2$$
(2) P is public key for U.

Encryption generation phase

Sender encrypts the message m', by executing the following steps:
(1) Randomly select two numbers c and d from [1 to m − 1] and calculate
$$Q = cP_1 + dP_2$$
(2) Calculate following $e_m(P, -cP_1 + dP_2) = \xi^{ad+bc.} = \gamma$
(3) Let message m', be an element of G. Send ($m'.\gamma$, Q) to receiver U.

Decryption generation phase.

The receiver recovers the message m', as follows.
(1) Compute $e_m(aP_1 - bP_2, Q) = \xi^{ad+bc.} = \gamma$
(2) Determine message m', by $m'.\gamma.\gamma^{-1} = m'$,

VI. SECURITY ANALYSIS

Lemma. If one can express a point of elliptic curve into linear combination of basis points then he can easily solve ECDLP.

Proof.

Solving the ECDLP for P means that if Q is a multiple of P,then find m so that $Q = mP$. If Q is any point of elliptic curve then expressing Q in terms of the basis means finding m_1 and m_2, so that $Q = m_1 P_1 + m_2 P_2$. If we can solve the latter, then given P and Q, write $P = m_1 P_1 + m_2 P_2$. and $Q = n_1 P_1 + n_2 P_2$.. Since P_1 and P_2 are independent, if $Q = kP$, then
$$m_1 = k\, n_1\, mod\ (order P_1.)$$
$$m_2 = k\, n_2\, mod\ (order P_2.).$$

Volume: 05, Issue: 02, Pages:1883-1885 (2013) ISSN : 0975-0290

From this one can solve for k modulo the order of P.

Attack1 Suppose eavesdropper is able to solve ECDLP. Since P_1 and P_2 are independent. So P can not be expressed as scalar multiple of P_1 and P_2. Hence we cannot use ECDLP to find the values of a and b from P.

Attack2 From public keys P and Q, eavesdropper can try to find $ad + bc$. He will calculate $e_m(P,Q) = \xi^{ad-bc}$. To
determine $ad - bc$, he will have to solve DLP in G. But DLP in G for non supersingular elliptic curve is too hard [8]. Suppose eavesdropper becomes success to solve DLP in G, and he gets $ad - bc$. Then from knowledge of $ad - bc$, to find $ad + bc$ is infeasible. Consequently from the knowledge of public keys eavesdropper cannot decrypt message.

Attack3 We use secret key to encrypt message. So choosen plaintext attack is not possible here.

VII. EFFICIENCY ANALYSIS

There are many efficient multiple scalar multiplications scheme exists to compute the form $kP + lQ$. Qiping Lin, Fangguo Zhang [9] gave efficient pre-computation scheme of $kP + lQ$ by using conjugate and co-Z addition formulas where k and l are integers, and P and Q are points on a curve.

VIII. CONCLUSION

Security of our scheme depends on expressing a torsion point into linear combination of basis points. This is more complicated than solving ECDLP. Consequently our scheme is more secure than all cryptosystems based on ECDLP. Since there are many efficient multiple scalar multiplications scheme exists to compute the form $kP + lQ$. So our scheme is efficient also.

REFERENCES

[1] W. Diffie, M. Hellman., New directions in cryptography, *IEEE trans. Inf. Theory*, 1976, 22(6), 644-654.

[2] R.L. Rivest, A. Shamir.; L. Adleman, A method for obtaining digital signatures and public key cryptosystems, *Communication of the ACM* ,21(1978),120-126.

[3] N, Koblitz,,Elliptic curve cryptosystems, *Mathematics of Computation* ,48 (1987) 203-209.

[4] V.S. Miller, Uses of elliptic curves in cryptography, in: Advances in Cryptology- Crypto'85, *Lecture Notes in Computer Science*, 218, Springer-Verlag, Berlin, 1986, pp. 417-426.

[5] T. E1Gamal, A public key cryptosystem and a signature scheme based on discrete logarithms, *IEEE Trans. Inf. Theory*, 1985, IT-31(4): 469-472.

[6] J. H. Silverman., The Arithmetic of elliptic curves, volume 106 of Graduate Texts in Mathematics, Springer-Verlag New York, 1986.

[7] J. Hoffistein, J. Pipher, and J. H. Silverman, An Introduction to mathematical Cryptography, Springer

[8] A. Menezes., T. Okamoto and S. Vanstone, Reducing elliptic curve logarithms to logarithms in a finite field, *IEEE Transactions on Information Theory*, Vol. 39 (1993) pp. 1639-1646.

[9] Qiping Lin and Fangguo Zhang , Efficient pre computation schemes of kP + lQ" *Information Processing Letters* 112 (2012) 462-466

[10] A. Menezes. And S. Vanstone, Elliptic curve cryptosystems and their implementation, *Journal of Cryptology*,Vol. 6 (1993) pp. 209-224.

Authors Biography

B. K. Sharma prof., in School of Studies in Mathematics, Pt. Ravishankar Shukla University Raipur (C.G.) India. He has been working for long time in the field of Non Linear Operator Theory and currently in Cryptography. He and his research scholars work on many branches of public key cryptography. He is a life member of Indian Mathematical society and the Ramanujan Mathematical Society.

Hemlal Sahu holds degree of B.Sc and M.Sc in Mathematics from Pt. Ravishankar Shukla University Raipur, (C.G.) India. Currently he is an assistant professor in mathematics at Govt. P. G. College Dantewada Chhattisgarh, India. His scientific interests lie in the fields of elliptic curve based public key cryptosystems.