AN AUTHENTICATION SECRET KEY GENERATION SCHEME USING BILINEAR SELF- PAIRING MAP BASED ON ELLIPTIC CURVE CRYPTOGRAPHY

Manoj Kumar
Assistant Professor, Department of Mathematics and Statistics,
Gurukula Kangri Vishwavidyalaya, Haridwar-249404(Uttrakhand), India
Email: sdmkg1@gmail.com

ABSTRACT

Elliptic curve cryptography (ECC) is an alternative approach for RSA scheme. Compared to its traditional counter parts, ECC offers the same level of security using much smaller keys. This result in faster computations and savings in memory, power and bandwidth those are especially important in constrained environments. More significantly, the advantage of ECC over its competitors increases, as the security needs increase over time. The present paper consist of an introduction of a multi self- pairing bilinear map on finitely generated free R -modules with rank three, where R is a commutative ring with unity. A multi self bilinear pairing on elliptic curve is constructed and we used this pairing map to generate secret shared key for a group communication.

Keywords: *Authentication protocols, Elliptic curve cryptography, Bilinear paring maps, Torsion Points, Finite Fields.*

1. INTRODUCTION

Recently authors, Kumar and Gupta [11] obtained cryptographic schemes based on elliptic curves over the ring $Z_p[i]$. In the present paper, we introduced a multi self- pairing bilinear map on finitely generated free R -modules with rank three, where R is a commutative ring with unity. We used this pairing map to generate secret shared key for group communication. In the recent years, pairing based cryptographic schemes on elliptic curve have been a very active field of research in cryptography. The concept of pairing in cryptography was first introduced by Weil [19]. Generally pairings map pairs of points on an elliptic curve into the multiplicative group of a finite field. The use of pairings in cryptography has developed at an extraordinary pace since the publication of the paper of Joux [8]. Joux's paper is of great interest to cryptographers, who want to start investigating further applications of pairings. The next two important applications of pairings are the identity-based encryption scheme of Boneh and Franklin [2] and the short signature scheme of Boneh, Lynn and Shacham [3]. Since then, there has been a flurry of activity in the design and analysis of cryptographic protocols using pairings. Pairings have been accepted as an indispensable tool for the protocol designer. There has also been a tremendous amount of work on the realization and efficient implementation of bilinear pairings using the Tate pairing on elliptic curves, hyperelliptic curves, and more general kinds of abelian varieties [7, 9, 13, 15, 17, 18].

Let E with $y^2 = x^3 + ax + b$ be an elliptic curve defined over a finite field F. Then, we know that [6, 10, 14, 16] each elliptic curve point can be described by two coordinates $x, y \in F$. In this case we say that elliptic curve points belong to two dimensional affine plane $A_F^2 = \{(x, y) \in F \times F\}$. Suppose the coordinates (x, y) of the affine plane $A_F^2 = \{(x, y) \in F \times F\}$ are mapped to the coordinates (X, Y, Z) of projective plane $P_F^3 = \{(X, Y, Z) \in F \times F \times F\}$ as

$$(X, Y, Z) = (x.Z^c, y.Z^d, 1) \text{ or } x = X / Z^c \text{ and } y = Y / Z^d \quad (1)$$

where c, d are integers.

After applying the Jacobian projective transformation with $c = 2$ and $d = 3$, elliptic curve E can be rewritten as

$$E: Y^2 = X^3 + aXZ^4 + bZ^6 .$$

If $P_1 = (X_1, Y_1, Z_1)$ and $P_2 = (X_2, Y_2, Z_2)$ are two distinct points on the projective plane then their point addition $\left(P_3 = (X_3, Y_3, Z_3) = P_1 + P_2\right)$ and point doubling $(P_3 = 2P_1)$ can be described as follows:

1.1 Addition of Two Distinct Points:

Case-I : If $x_1 \neq x_2$ then we have

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{\frac{Y_2}{Z_2^{\,d}} - \frac{Y_1}{Z_1^{\,d}}}{\frac{X_2}{Z_2^{\,c}} - \frac{X_1}{Z_1^{\,c}}} = \frac{(Y_2 Z_1^{\,d} - Y_1 Z_2^{\,d}) Z_2^{\,c} Z_1^{\,c}}{(X_2 Z_1^{\,c} - X_1 Z_2^{\,c}) Z_2^{\,d} Z_1^{\,d}}$$

It is obvious from above expression that λ exist because $x_1 \neq x_2$.

Now the point P_3 can be calculated as

$$x_3 = \lambda^2 - x_1 - x_2 = \left(\frac{(Y_2 Z_1^{\,d} - Y_1 Z_2^{\,d}) Z_2^{\,c} Z_1^{\,c}}{(X_2 Z_1^{\,c} - X_1 Z_2^{\,c}) Z_2^{\,d} Z_1^{\,d}} \right)^2 - \frac{X_1 Z_2^{\,c} + X_2 Z_1^{\,c}}{Z_2^{\,c} Z_1^{\,c}}$$

$$= \frac{(Y_2 Z_1^{\,d} - Y_1 Z_2^{\,d}) Z_2^{\,3c} Z_1^{\,3c} - (X_1 Z_2^{\,c} + X_2 Z_1^{\,c})(X_2 Z_1^{\,c} - X_1 Z_2^{\,c})^2 Z_2^{\,2d} Z_1^{\,2d}}{(X_2 Z_1^{\,c} - X_1 Z_2^{\,c}) Z_2^{\,2d+c} Z_1^{\,2d+c}}$$

$$y_3 = \lambda(x_1 - x_3) - y_1$$

$$= \frac{(Y_2 Z_1^{\,d} - Y_1 Z_2^{\,d}) Z_2^{\,c} Z_1^{\,c}}{(X_2 Z_1^{\,c} - X_1 Z_2^{\,c}) Z_2^{\,d} Z_1^{\,d}} \left(\frac{X_1}{Z_1^{\,c}} - \frac{(Y_2 Z_1^{\,d} - Y_1 Z_2^{\,d})^2 Z_2^{\,3c} Z_1^{\,3c} - (X_1 Z_2^{\,c} + X_2 Z_1^{\,c})(X_2 Z_1^{\,c} - X_1 Z_2^{\,c})^2 Z_2^{\,2d} Z_1^{\,2d}}{(X_2 Z_1^{\,c} - X_1 Z_2^{\,c}) Z_2^{\,2d+c} Z_1^{\,2d+c}} \right) - \frac{Y_1}{Z_1^{\,d}}$$

$$= \frac{(Y_2 Z_1^{\,d} - Y_1 Z_2^{\,d}) Z_2^{\,c} Z_1^{\,c}}{(X_2 Z_1^{\,c} - X_1 Z_2^{\,c}) Z_2^{\,d} Z_1^{\,d}} \left(\frac{(2X_1 Z_2^{\,c} + X_2 Z_1^{\,c})(X_2 Z_1^{\,c} - X_1 Z_2^{\,c})^2 Z_2^{\,2d} Z_1^{\,2d} - (Y_2 Z_1^{\,d} - Y_1 Z_2^{\,d})^2 Z_2^{\,3c} Z_1^{\,3c}}{(X_2 Z_1^{\,c} - X_1 Z_2^{\,c}) Z_2^{\,2d+c} Z_1^{\,2d+c}} \right) - \frac{Y_1}{Z_1^{\,d}}$$

$$= \frac{(Y_2 Z_1^{\,d} - Y_1 Z_2^{\,d})(2X_1 Z_2^{\,c} + X_2 Z_1^{\,c})(X_2 Z_1^{\,c} - X_1 Z_2^{\,c})^2 Z_2^{\,2d+c} Z_1^{\,2d+c} - (Y_2 Z_1^{\,d} - Y_1 Z_2^{\,d})^3 Z_2^{\,4c} Z_1^{\,4c}}{(X_2 Z_1^{\,c} - X_1 Z_2^{\,c}) Z_2^{\,3d+c} Z_1^{\,3d+c}} - \frac{Y_1}{Z_1^{\,d}}$$

$$= \frac{((Y_2 Z_1^{\,d} - Y_1 Z_2^{\,d})(2X_1 Z_2^{\,c} + X_2 Z_1^{\,c}) - Y_1 Z_2^{\,d}(X_2 Z_1^{\,c} - X_1 Z_2^{\,c}))(X_2 Z_1^{\,c} - X_1 Z_2^{\,c})^2 Z_2^{\,2d} Z_1^{\,2d} - (Y_2 Z_1^{\,d} - Y_1 Z_2^{\,d})^3 Z_2^{\,3c} Z_1^{\,3c}}{(X_2 Z_1^{\,c} - X_1 Z_2^{\,c}) Z_2^{\,3d} Z_1^{\,3d}}$$

Using (1) and Jacobian projective transformation with $c = 2$ and $d = 3$, P_3 is given by

$$X_3 = (Y_2 Z_1^{\,3} - Y_1 Z_2^{\,3})^2 - (X_1 Z_2^{\,2} + X_2 Z_1^{\,2})(X_2 Z_1^{\,2} - X_1 Z_2^{\,2})^2 ,$$

$$Y_3 = ((Y_2 Z_1^{\,3} - Y_1 Z_2^{\,3})(2X_1 Z_2^{\,2} + X_2 Z_1^{\,2}) - Y_1 Z_2^{\,3}(X_2 Z_1^{\,2} - X_1 Z_2^{\,2})) - (Y_2 Z_1^{\,3} - Y_1 Z_2^{\,3})^3 ,$$

and $$Z_3 = (X_2 Z_1^{\,2} - X_1 Z_2^{\,2}) Z_2 Z_1 .$$

Case-II : If $x_1 = x_2$ then we have $P_3 = P_1 + P_2 = O$, where O is the point at infinity of the elliptic curve E in projective coordinates. It can be easily seen that for Jacobian projective coordinates, the point at infinity has the form $(1,1,0)$.

1.2 Addition of Two Equal Points:

For point doubling we can take $P_1 = P_2$ then $P_3 = P_1 + P_2 = 2P_1 = (X_3, Y_3, Z_3)$.

We have

$$\lambda = \frac{3x_1^{\,2} + a}{2y_1} = \frac{3X_1^{\,2} Z_1^{\,d} + aZ_1^{\,2c+d}}{2Z_1^{\,2c} Y_1}$$

Obviously λ exists if $y_1 \neq 0$. So we get

$$x_3 = \lambda^2 - 2x_1 = \frac{(3X_1^2 + aZ_1^{2c})^2 Z_1^{2d}}{4Z_1^{4c}Y_1^2} - 2\frac{X_1}{Z_1^c} = \frac{(3X_1^2 + aZ_1^{2c})^2 Z_1^{2d} - 8Z_1^{3c}X_1Y_1^2}{4Z_1^{4c}Y_1^2}$$

$$y_3 = \lambda(x_1 - x_3) - y_1 = \lambda(3x_1 - \lambda^2) - y_1$$

$$= \frac{(3X_1^2 + aZ_1^{2c})^2 Z_1^d}{2Z_1^{2c}Y_1}\left(3\frac{X_1}{Z_1^c} - \frac{(3X_1^2 + aZ_1^{2c})^2 Z_1^{2d}}{4Z_1^{4c}Y_1^2}\right) - \frac{Y_1}{Z_1^d}$$

$$= \frac{12X_1Y_1^2(3X_1^2 + aZ_1^{2c})^2 Z_1^{3c+2d} - (3X_1^2 + aZ_1^{2c})^3 Z_1^{4d} - 8Z_1^{6c}Y_1^4}{8Z_1^{6c+d}Y_1^3}$$

Using (1) and Jacobian projective transformation with $c = 2$ and $d = 3$, the doubling of point P_1 is given by $P_3(X_3, Y_3, Z_3)$

where $X_3 = (3X_1^2 + aZ_1^4)^2 - 8X_1Y_1^2$,

$Y_3 = 12X_1Y_1^2(3X_1^2 + aZ_1^4) - (3X_1^2 + aZ_1^4)^3 - 8Y_1^4$,

and $Z_3 = 2Z_1Y_1$.

Point subtraction can be performed as $P_3 = P_1 - P_2 = P_1 + (-P_2)$ where $-P_2$ is the additive inverse of P_2 and $-P_2 = (X_2, -Y_2, Z_2)$.

Here it is remarkable that we are no need of division and multiplication operations for calculating elliptic curve point P_3 on the projective plane.

2. CONSTRUCTION OF BILINEAR SELF PARING MAP

In this section we will construct a multi self-pairing on finitely generated free R-modules with rank 3. At the end of this section we will also discuss an auxiliary result which will be helpful in the next section.

According to the terminology as in the references [1, 3, 4, 5], let R be a commutative ring with unity, P be a finitely generated free R-module with rank 3 and (l, m, n) be a generating pair for P. We consider elements $a = u_1l + v_1m + w_1n$, $b = u_2l + v_2m + w_2n$, $c = u_3l + v_3m + w_3n$ in P, where $u_i, v_i, w_i \in P$ for each $i = 1, 2, 3$.

For some fixed $\alpha, \beta, \gamma \in R$ where all α, β and γ are not zero at the same time, we construct a pairing map

$$f_{\alpha,\beta,\gamma} : P \times P \times P \rightarrow P \tag{2}$$

defined by

$$f_{\alpha,\beta,\gamma}(a,b,c) = [u_1(v_2w_3 - v_3w_2) + v_1(u_3w_2 - u_2w_3) + w_1(u_2v_3 - u_3v_2)].(\alpha l + \beta m + \gamma n) \tag{3}$$

It can be easily seen that the pairing map (2) defined by (3) is non- trivial and well defined map.

For this, if $a = a'$, $b = b'$ and $c = c'$ then we have $u_i = u_i'$, $v_i = v_i'$ and $w_i = w_i'$ for each $i = 1, 2, 3$ by independency of (l, m, n). This implies $f_{\alpha,\beta,\gamma}(a,b,c) = f_{\alpha,\beta,\gamma}(a',b',c')$. Therefore the map is well defined.

Proposition-1[12]: The pairing $f_{\alpha,\beta,\gamma}(a,b,c)$ has the following properties:

(i) **Identity :** $f_{\alpha,\beta,\gamma}(a,a,a) = 0$ for all $a \in P$.

(ii) **Bilinearity :** If $a, b, c, d \in P$ then we have

$$f_{\alpha,\beta,\gamma}(a+b,c,d) = f_{\alpha,\beta,\gamma}(a,c,d) + f_{\alpha,\beta,\gamma}(b,c,d),$$

$$f_{\alpha,\beta,\gamma}(a,b+c,d) = f_{\alpha,\beta,\gamma}(a,b,d) + f_{\alpha,\beta,\gamma}(a,c,d),$$

and $$f_{\alpha,\beta,\gamma}(a,b,c+d) = f_{\alpha,\beta,\gamma}(a,b,c) + f_{\alpha,\beta,\gamma}(a,b,d).$$

(iii) **Anti- symmetry :** $f_{\alpha,\beta,\gamma}(a,b,c) = -f_{\alpha,\beta,\gamma}(b,c,a)$ for all $a, b, c \in P$.

(iv) **Non- degeneracy :** If $a, b, c \in P$ then $f_{\alpha,\beta,\gamma}(a,b,0) = 0 = f_{\alpha,\beta,\gamma}(a,0,c) = f_{\alpha,\beta,\gamma}(0,b,c)$.

Also, if $f_{\alpha,\beta,\gamma}(a,b,c) = 0$ for all $b, c \in P$, then $a = 0$.

Moreover, if $f_{\alpha,\beta,\gamma}(a,b,c) = 0$ for all $c \in P$ then $a = kb$ for some constant k.

3. CONSTRUCTION OF BILINEAR SELF PARING MAP ON ELLIPTIC CURVES

In this section, we will extend the multi self pairing (constructed in previous section) on elliptic curve over the finite fields. At the end of this section we will also discuss an auxiliary result which will be useful in the next section.

Let E be an elliptic curve. Then a point $P \in E$ is said to be a torsion point[18] if there exist a positive integer m such that $mP = O$. The smallest such integer is called the order of P. An n-torsion point is a point $P \in E$ satisfying $nP = O$.

Also let K be a field with characteristic zero or a prime p (p is relatively prime to n) and let $E = E(\overline{K})$ be an elliptic curve over $\overline{K}$ where $\overline{K}$ is an algebraic closure of K. Also let $E(K)[n]$ denote the subgroup of n-torsion point in $E(K)$, where $n \neq 0$.

For our simplicity we will denote $E(\overline{K})[n]$ by $E[n]$.

It can be easily checked that $E[n] \approx Z_n \oplus Z_n \oplus Z_n$.

Let $\{U, V, W\}$ for some fixed generating pair for $E[n]$. Then the points $P, Q, R \in E[n]$ can be expressed as $P = a_1U + b_1V + c_1W$, $Q = a_2U + b_2V + c_2W$, $R = a_3U + b_3V + c_3W$, where a_i, b_i, c_i for each $i = 1, 2, 3$ are integers in $[0, n-1]$.

Now for some fixed integers $\alpha, \beta, \gamma \in [0, n-1]$,where all α, β, γ are not zero at the same time, we construct a map

$$f^n{}_{\alpha,\beta,\gamma} : E[n] \times E[n] \times E[n] \rightarrow E[n] \tag{4}$$

defined by

$$f^n{}_{\alpha,\beta,\gamma}(P, Q, R) = [a_1(b_2c_3 - b_3c_2) + b_1(a_3c_2 - a_2c_3) + c_1(a_2b_3 - a_3b_2)].(\alpha U + \beta V + \gamma W) \tag{5}$$

It can be easily checked the map (4) defined by (5) is well defined.

Proposition-2[12] : The pairing map $f^n{}_{\alpha,\beta,\gamma}(P, Q, R)$ constructed as above, satisfies the following postulates :

(i) Identity : $f^n{}_{\alpha,\beta,\gamma}(P, P, P) = O$ for all $P \in E[n]$.

(ii) Bilinearity : If $P, Q, R, S \in E[n]$, then we have

$$f^n{}_{\alpha,\beta,\gamma}(P + Q, R, S) = f^n{}_{\alpha,\beta,\gamma}(P, R, S) + f^n{}_{\alpha,\beta,\gamma}(Q, R, S),$$

$$f^n{}_{\alpha,\beta,\gamma}(P, Q + R, S) = f^n{}_{\alpha,\beta,\gamma}(P, Q, S) + f^n{}_{\alpha,\beta,\gamma}(P, R, S),$$

and

$$f^n{}_{\alpha,\beta,\gamma}(P, Q, R + S) = f^n{}_{\alpha,\beta,\gamma}(P, Q, R) + f^n{}_{\alpha,\beta,\gamma}(P, Q, S).$$

(iii) Anti-symmerty : $f^n{}_{\alpha,\beta,\gamma}(P, Q, R) = -f^n{}_{\alpha,\beta,\gamma}(Q, P, R)$ for all $P, Q, R \in E[n]$.

(iv) Non-degeneracy : If $P, Q, R \in E[n]$ then $f^n{}_{\alpha,\beta,\gamma}(P, Q, O) = O = f^n{}_{\alpha,\beta,\gamma}(P, O, R) = f^n{}_{\alpha,\beta,\gamma}(O, Q, R)$.

Also if $f^n{}_{\alpha,\beta,\gamma}(P, Q, R) = O$ for all $Q, R \in E[n]$, then $P = O$.

Moreover if $f^n{}_{\alpha,\beta,\gamma}(P, Q, R) = O$ for all $R \in E[n]$, then $P = kQ$ for some constant k.

(v) Compatibility : If $P \in E[nk]$, $Q \in E[n]$ and $R \in E[n]$ then $f^n{}_{\alpha,\beta,\gamma}(kP, Q, R) = kf^n{}_{\alpha,\beta,\gamma}(P, Q, R)$,

if $P \in E[n]$, $Q \in E[nk]$ and $R \in E[n]$ then $f^n{}_{\alpha,\beta,\gamma}(P, kQ, R) = kf^n{}_{\alpha,\beta,\gamma}(P, Q, R)$,

also $P \in E[n]$, $Q \in E[n]$ and $R \in E[nk]$ then $f^n{}_{\alpha,\beta,\gamma}(P, Q, kR) = kf^n{}_{\alpha,\beta,\gamma}(P, Q, R)$.

4. CRYPTOGRAPHIC APPLICATIONS

In this section we will apply multi self bilinear pairing (constructed in previous section) to elliptic curve cryptography. A protocol is a multi-party algorithm, defined by a sequence of steps precisely specifying the actions required by three or more parties in order to achieve a specified objective. Key establishment is a process or protocol whereby a shared secret becomes available to three or more parties, for subsequent cryptographic use. A key agreement protocol is a key establishment technique in which a shared secret is derived by three (or more) parties as a function of information contributed by, or associated with, each of these, such that no party can predetermine the resulting value. The key agreement protocol is contributory if

each party equally contributes to the key and guarantees its freshness. Key authentication is the property whereby one party is associated that no other party aside from an especially identified second party may gain access to a particular secret key. Key authentication is said to be implicit if each party sharing the key is assured that no other party can learn the secret shared key.

For a prime number p (p is large enough) and a positive integer r, we denote $q = p^r$. Let E be an elliptic curve over a finite field F_q. Then given $P \in E(F_q)$ with order n and $Q \in \langle P \rangle$, to find k such that $Q = kP$, is known as elliptic curve discrete log problem (ECDLP) in $E(F_q)$. Also for given P, aP, bP to find abP is known as Diffie-Hellman problem for elliptic curves. Actually it is known as Diffie-Hellman key exchange protocol for elliptic curves.

Now the proposed cryptographic schemes can be described as follow :

(i) We Select a large prime s such that $E[s] \subseteq E(F_{q^k})$ for some smallest integer k.

(ii) Next we select a generating pair $\{U, V, W\}$ in $E[s]$ and integers $\alpha, \beta, \gamma \in [0, l-1]$ which determine the pairing $f^s{}_{\alpha,\beta,\gamma}$.

Let the parameters $(P, Q, R, f^s{}_{\alpha,\beta,\gamma})$ be publicly known and let $h : E(F_q) \to Z/l$ be hash functions.

Now our proposed $f^s{}_{\alpha,\beta,\gamma}$- pairing can be apply to cryptographic scheme namely authenticated key agreement on elliptic curves. To apply the proposed scheme, we assume that three communication parties Alice, Bob and Carol wish to share a common secret information. Now we are in the position to explain authenticated elliptic curve Diffie-Hellman key agreement for three parties, which consists of the following phases:

Phase-I: It consists of the following steps

1) Alice, Bob and Carol randomly select secret integers $a, b, c \in (1, s-1)$ respectively.
2) They respectively compute aP, bP, cP.
3) They broadcast the above computed values.

Now the public values of the system are $(P, Q, R, aP, bP, cP, f^s{}_{\alpha,\beta,\gamma})$.

Phase-II: It consists of the following steps

1) Alice computes $S_A = a.bP.cP = abcP$ (because $P \in E[n]$) and $f^s{}_{\alpha,\beta,\gamma}(aP, Q, R)$. She sends $h(S_A) f^s{}_{\alpha,\beta,\gamma}(aP, Q, R)$ to Bob and Carol.
2) Bob computes $S_B = b.aP.cP = abcP$ and $f^s{}_{\alpha,\beta,\gamma}(bP, Q, R)$. He sends $h(S_B) f^s{}_{\alpha,\beta,\gamma}(bP, Q, R)$ to Alice and Carol.
3) Carol computes $S_C = c.aP.bP = abcP$ and $f^s{}_{\alpha,\beta,\gamma}(cP, Q, R)$. He sends $h(S_C) f^s{}_{\alpha,\beta,\gamma}(cP, Q, R)$ to Alice and Bob.

It is evident that $S_A = S_B = S_C = abcP = S_{ABC}$ (say).

Phase-III: It consists of the following steps

1) Alice receives $I_A = h(S_B) f^S_{\alpha,\beta,\gamma}(bP, Q, R) \| h(S_C) f^S_{\alpha,\beta,\gamma}(cP, Q, R)$

Using the bilinearity of pairing $f^s{}_{\alpha,\beta,\gamma}$, Alice obtains $I_A = h(S_{ABC}) bc f^s{}_{\alpha,\beta,\gamma}(P, Q, R)$.

Alice computes $h(S_A)^{-1} (\mathrm{mod}\, s)$ to obtain her secret share key as $K_A = ah(S_A)^{-1} I_A$.

2) Next Bob receives $I_B = h(S_A) f^S_{\alpha,\beta,\gamma}(aP, Q, R) \| h(S_C) f^S_{\alpha,\beta,\gamma}(cP, Q, R)$

$$= h(S_{ABC}) ac f^S_{\alpha,\beta,\gamma}(P, Q, R)$$

To obtain secret share key, Bob calculates $h(S_B)^{-1} (\mathrm{mod}\, s)$ and compute his shared secret key as

$$K_B = bh(S_B)^{-1} I_B .$$

3) Finally Carol receives $I_C = h(S_A) f^S_{\alpha,\beta,\gamma}(aP, Q, R) \| h(S_B) f^S_{\alpha,\beta,\gamma}(bP, Q, R)$

$$= h(S_{ABC}) ab f^S_{\alpha,\beta,\gamma}(P, Q, R)$$

To obtain secret share key, Carol calculates $h(S_C)^{-1} (\mathrm{mod}\, s)$ and compute his shared secret key as

$$K_C = ch(S_C)^{-1} I_C .$$

It can be easily verified that $K_A = K_B = K_C = abc\, f^{s}_{\alpha,\beta,\gamma}(P,Q,R) = K$ (say).

Thus there has been established an authenticated common secret key among multiparty Alice, Bob and Carol.

5. SECURITY ANALYSIS

It is obvious from the proposed authenticated elliptic curve Diffie Hellman protocol that the common secret key $K = abc\, f^{s}_{\alpha,\beta,\gamma}(P,Q,R)$ is designed by the contribution of each involved party (Alice, Bob, Carol). This results in the complexity for the attacker.

For this suppose an active adversary is capable to reform, delay or interpose the message. Now possible attacks on Bob and Carol can be described as:

If K_B or K_C secret common key calculated by Bob or Carol, then it can be represented as $K_B = b\, f^{s}_{\alpha,\beta,\gamma}(d_1P,Q,R)$ or $K_C = c\, f^{s}_{\alpha,\beta,\gamma}(d_2P,Q,R)$ where d_1 or d_2 are introduced by adversary. It means that adversary can alter the first flow of the proposed protocol with $f^{s}_{\alpha,\beta,\gamma}(d_1P,Q,R)$ or $f^{s}_{\alpha,\beta,\gamma}(d_2P,Q,R)$. To compute $bf^{s}_{\alpha,\beta,\gamma}(d_1P,Q,R)$ or $cf^{s}_{\alpha,\beta,\gamma}(d_2P,Q,R)$ adversary requires to calculate $bf^{s}_{\alpha,\beta,\gamma}(P,Q,R)$ or $cf^{s}_{\alpha,\beta,\gamma}(P,Q,R)$ respectively. But in the second flow, the only expression calculating $bf^{s}_{\alpha,\beta,\gamma}(P,Q,R)$ or $cf^{s}_{\alpha,\beta,\gamma}(P,Q,R)$ is $h(S_B)f^{s}_{\alpha,\beta,\gamma}(bP,Q,R)$ or $h(S_C)f^{s}_{\alpha,\beta,\gamma}(cP,Q,R)$ respectively. This shows that for adversary to compute $bf^{s}_{\alpha,\beta,\gamma}(P,Q,R)$ or $cf^{s}_{\alpha,\beta,\gamma}(P,Q,R)$ respectively from $h(S_B)f^{s}_{\alpha,\beta,\gamma}(bP,Q,R)$ or $h(S_C)f^{s}_{\alpha,\beta,\gamma}(cP,Q,R)$ is intractable without the knowledge of K_B or K_C.

Similarly attack on Alice can be described as:

Suppose key calculated by Alice is $K_A = ah(S_A)^{-1} f^{s}_{\alpha,\beta,\gamma}(d_3P,Q,R)$ where d_3 is introduced by the adversary. Now if assume that $d_3 = d_4h(S_A)$ where d_4 is known by adversary and independent of $h(S_A)$, then $K_A = ah(S_A)^{-1} f^{s}_{\alpha,\beta,\gamma}\left(d_4h(S_A)P,Q,R\right) = af^{s}_{\alpha,\beta,\gamma}\left(d_4P,Q,R\right)$. Also to calculate $d_4h(S_A)f^{s}_{\alpha,\beta,\gamma}\left(P,Q,R\right)$, where d_4 is known by adversary, is intractable without calculating $h(S_A)f^{s}_{\alpha,\beta,\gamma}\left(P,Q,R\right)$. Further if d_3 is independent of $h(S_A)$, then it is impossible to calculate the key of Alice because K_A depends upon $h(S_A)^{-1}$.

6. CONCLUSIONS

Using $f^{s}_{\alpha,\beta,\gamma}$- pairing in cryptography is based on the difficulty of computing $h(S_B)f^{s}_{\alpha,\beta,\gamma}(bP,Q,R)$, $h(S_C)f^{s}_{\alpha,\beta,\gamma}(cP,Q,R)$ and $h(S_A)f^{s}_{\alpha,\beta,\gamma}(aP,Q,R)$, without knowing the secret values a,b and c (of Alice, Bob and Carol respectively) in the construction of the self pairing bilinear map $f^{s}_{\alpha,\beta,\gamma}$. To compute $bf^{s}_{\alpha,\beta,\gamma}(d_1P,Q,R)$ or $cf^{s}_{\alpha,\beta,\gamma}(d_2P,Q,R)$, adversary requires to calculate $bf^{s}_{\alpha,\beta,\gamma}(P,Q,R)$ or $cf^{s}_{\alpha,\beta,\gamma}(P,Q,R)$ respectively. But in the second flow the only expression calculating $bf^{s}_{\alpha,\beta,\gamma}(P,Q,R)$ or $cf^{s}_{\alpha,\beta,\gamma}(P,Q,R)$ is $h(S_B)f^{s}_{\alpha,\beta,\gamma}(bP,Q,R)$ or $h(S_C)f^{s}_{\alpha,\beta,\gamma}(cP,Q,R)$ respectively. This shows that for adversary to compute $bf^{s}_{\alpha,\beta,\gamma}(P,Q,R)$ or $cf^{s}_{\alpha,\beta,\gamma}(P,Q,R)$ respectively from $h(S_B)f^{s}_{\alpha,\beta,\gamma}(bP,Q,R)$ or $h(S_C)f^{s}_{\alpha,\beta,\gamma}(cP,Q,R)$ is intractable without the knowledge of K_B or K_C. Furthermore to calculate $d_4h(S_A)f^{s}_{\alpha,\beta,\gamma}\left(P,Q,R\right)$, where d_4 is known by adversary, is intractable without calculating $h(S_A)f^{s}_{\alpha,\beta,\gamma}\left(P,Q,R\right)$. In fact, it is impossible to calculate the secret key of Alice because her key K_A depends upon $h(S_A)^{-1}$. Thus $f^{s}_{\alpha,\beta,\gamma}$ pairing with only public values is as hard as solving the discrete logarithm problem on elliptic curves. Our schemes include only one random secret key per user. This is more efficient and secure than using two random secret keys in the known schemes existing in the literature.

REFERENCES

[1] Bhattacharya P.B., Jain S.K. and Nagpaul S.R., Basic abstract algebra, Cambridge university press, United Kingdom, 1995.

[2] Boneh, D. and Franklin, M., Identity-based encryption from the Weil pairing, Advances in Cryptology-CRYPTO 2001, Lecture Notes in Computer Science, 2139, 213-229. Full version: SIAM Journal on Computing, 2003, 32: 586-615.
[3] Boneh, D., Lynn, B. and Shacham, H., Short signatures from the Weil pairing, Advances in Cryptology-ASIACRYPT 2001, Lecture Notes in Computer Science, 2248, (2001)514-532. Full version: Journal of Cryptology, 2004, 17: 297-319.
[4] Gallian **,** J. A.**,** Contemporary abstract algebra, Narosa publishing house, New Delhi, 1998.
[5] Gilbert, W. J.**,** Modern algebra with application, Willey-Interscience, New York, 2004.
[6] Hankerson, D. and Menezes, J. A., Vanstone S., Guide to Elliptic Curve Cryptography, Springer-Verlag, Germany, 2004.
[7] Hardy, G. H., Wright E. M., An introduction to the theory of numbers, oxford university press, United Kingdom, 1938.
[8] Joux, A., A one round protocol for tripartite Diffie-Hellman, Algorithmic Number Theory: 4th International Symposium, ANTS-IV, Lecture Notes in Computer Science, 1838, 385-393, (2000). Full version: Journal of Cryptology, 2004, 17:263–276.
[9] Koblitz N.**,** Elliptic Curve Cryptosystem, Journal of Mathematics Computation, 1987, 48(177):203-209.
[10] Kumar M., A secure and efficient authentication protocol based on elliptic curve Deffie-Hellman algorithm and zero knowledge property, International Journal of Soft Computing and Engineering, 2013, 3(5):137-142.
[11] Kumar M. and Gupta P., Cryptographic schemes based on Elliptic Curve over the Ring Zp[i], Applied Mathematics, (2016, 7(3):304-312.
[12] Kumar M., Gupta P. and Kumar A., A Novel and Secure Multi-party Key Exchange Scheme Using Trilinear Pairing Map Based on Elliptic Curve Cryptography, International Journal of Pure and Applied Mathematics, 2017, 116(1).
[13] Miller V., Use of elliptic curves in cryptography, Advances in Cryptology-CRYPTO, 85 (LNCS 218), 1985, 417-426.
[14] Nemati H., Information security and Ethics: Concept, Methodologies, Tools, and Applications, Information science reference, New York, 2007.
[15] Silverman, J.**,** The Arithmetic of Elliptic Curves, Springer- Verlag, New York, 1986.
[16] Sklavos N. and Zhang X., Wireless security and cryptography specifications and implementations, Chapman and Hall/CRC, United Kingdom, 2007.
[17] Stinson, D. R.**,** Cryptography theory and practice, Chapman and Hall/CRC, United Kingdom, 2006.
[18] Washington, L.C.**,** Elliptic curves number theory and cryptography, Chapman and Hall/CRC, United Kingdom, 2008.
[19] Weil, André Sur les fonctions algébriques à corps de constantes fini. (French) C. R. Acad. Sci. Paris , 1940,210: 592–594.