International Journal of Pure and Applied Mathematics
Volume 116 No. 1 2017, 1-14
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
doi: 10.12732/ijpam.v116i1.1

A NOVEL AND SECURE MULTI-PARTY KEY EXCHANGE SCHEME USING TRILINEAR PAIRING MAP BASED ON ELLIPTIC CURVE CRYPTOGRAPHY

Manoj Kumar[1], Pratik Gupta[2] §, Ajay Kumar[3]

[1,2]Departement of Mathematics
Gurukul Kangri Vishwavidyalaya
Haridwar, 249404, INDIA

[3]Defence Scientific Information and Documentation
Defence Research and Development Organizations
Delhi, 110054, INDIA

Abstract: Elliptic curves have been broadly studied more than hundred years. Recently they have become a tool in various important applied fields such as coding theory, pseudo-random bit generation, number theory algorithms, etc. In the present paper we have proposed a trilinear pairing map based on elliptic curve using finitely generated free R -modules with rank three, where R is a commutative ring with unity; and we used this pairing map to a multi party key exchange scheme. Since the secret shared key generated among the members of the group is constructed by the contribution of each member of the group, it increases the security of the proposed scheme.

AMS Subject Classification: 94A60, 14G50
Key Words: elliptic curve, free modules, authentication, torsion points, finite field, Jacobian, projective transformation

Received: September 26, 2016
Revised: June 15, 2017
Published: August 29, 2017

§Correspondence author

1. Introduction

Elliptic curve cryptography(ECC) has been an active area of research since 1985 when Koblitz [1] and Miller [2] independently suggested using elliptic curves for public-key cryptography. A lot of work has been done on elliptic curve cryptography. Because elliptic curve cryptography offers the same level of security as compared to RSA with considerably shorter keys, it has replaced traditional public key cryptosystems, especially, in environments where short keys are important. In 2009, Koblitz et. al. [3] proposed the serpentine course of a paradigm shift on ECC in which they described the sometimes surprising twists and turns in this paradigm shift and compared this study with the commonly accepted Ideal Model of how research and development function in cryptography. Very recently Kumar and Gupta [4] obtained cryptographic schemes based on elliptic curves over the ring $Z_p[i]$. In the present paper, we introduced a trilinear pairing 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 deedful domain of research in cryptography. The concept of pairing in cryptography was first introduced by Weil [5]. Generally pairings map use of pair of points on an elliptic curve into the multiplicative group of a finite field. The use of pairings by the publication of the paper of Joux [6] in cryptography has developed at an extraordinarypace. The identity-based encryption scheme of Boneh and Franklin [7] and, the short signature scheme of Boneh et. al. [8] are important applications of pairings in cryptography. In last four decades pairing maps are continuously studied by several researchers [9, 10, 11, 12].

Let E with $y^2 = x^3 + bx + c$ be an elliptic curve defined over a finite field F, where the coefficients a and b in the elliptic curve equation must satisfy the non singularity condition $4a^3 + 27b^2 = 0$. Then, we know that [13, 14, 15] each elliptic curve point can be described by two coordinates $x, y \in F$. 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

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

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 ($P_3 = (X_3, Y_3, Z_3) = P_1 + P_2$) and point doubling ($P_3 = 2P_1$) can be described as follows:

1.1. Addition of Points on Projective Plane

Case I. If $x_1 \neq x_2$ then we have

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

It is obvious from above expression that λ exist because $x_1 \neq x_2$. Now the point P_3 can be calculated as

$$\begin{aligned}
x_3 =& \lambda^2 - x_1 - x_2 \\
=& \frac{(Y_2 Z_1^d - Y_1 Z_2^d) Z_2^c Z_1^c}{(X_2 Z_1^c - X_1 Z_2^c) Z_2^d Z_1^d}^2 - \frac{X_1 Z_2^c + X_2 Z_1^c}{Z_2^c Z_1^c} \\
=& \frac{(Y_2 Z_1^d - Y_1 Z_2^d) Z_2^{3c} Z_1^{3c} - (X_1 Z_2^c + X_2 Z_1^c)(X_2 Z_1^c - X_1 Z_2^c) Z_2^{2d} Z_1 2d}{(X_2 Z_1^c - X_1 Z_2^c) Z_2^{2d+c} Z_1^{2d+c}}, \\
y_3 =& \lambda(x_1 - x_3) - y_1 \\
=& \frac{(Y_2 Z_1^d - Y_1 Z_2^d) Z_2^c Z_1^c}{(X_2 Z_1^c - X_1 Z_2^c) Z_2^d Z_1^d} \\
& \left(\frac{X_1}{Z_1^c} - \frac{(Y_2 Z_1^d - Y_1 Z_2^d) Z_2^{3c} Z_1^{3c} - (X_1 Z_2^c + X_2 Z_1^c)(X_2 Z_1^c - X_1 Z_2^c)^2 Z_2^{2d} Z_1 2d}{(X_2 Z_1^c - X_1 Z_2^c) Z_2^{2d+c} Z_1^{2d+c}} \right) \\
& - \frac{Y_1}{Z_1^d},
\end{aligned}$$

calculated as

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

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

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

$$\begin{aligned}
X_3 =& (Y_2 Z_1^3 - Y_1 Z_2^3)^2 - (X_1 Z_2^2 + X_2 Z_1^2)(X_2 Z_1^2 - X_1 Z_2^2), \\
Y_3 =& ((Y_2 Z_1^3 - Y_1 Z_2^3)(2X_1 Z_2^2 + X_2 Z_1^2) - Y_1 Z_2^3 (X_2 Z_1^2 - X_1 Z_2^2))
\end{aligned}$$

$$- (Y_2 Z_1^3 - Y_1 Z_2^3)^3,$$

and

$$Z_3 = (X_2 Z_1^2 - X_1 Z_2^2) Z_1 Z_2.$$

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 from $(1, 1, 0)$.

1.2. Point Doubling on Projective Plane

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

$$\begin{aligned}
x_3 =& \lambda^2 - 2x_1 \\
=& \frac{(3X_1^2 + aZ_1^{2c})^2 Z_1^{2d}}{4Z_1^{4c} Y_1^2} - \frac{2X_1}{Z_1^c} \\
=& \frac{3X_1^2 + aZ_1^{2c})^2 Z_1^{2d} - 8Z_1^{3c} X_1 Y_1^2}{4Z_1^{4c} Y_1^2}, \\
y_3 =& \lambda(x_1 - x_3) - y_1 \\
=& \lambda(3x_1 - \lambda^2) - y_1 \\
=& \frac{12X_1 Y_1^2 (3X_1^2 + aZ_1^{2c})^2 Z_1 3c + 2d - (3X_1^2 + aZ_1^{2c})^3 Z_1^{4d} - 8Z_1 6c Y_1^4}{8Z_1^{6c+d} Y_1^3}.
\end{aligned}$$

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

$$X_3 = (3X_1^2 + aZ_1^4)^2 - 8X_1 Y_1^2, \quad Y_3 = 12X_1 Y_1^2 (3X_1^2 + aZ_1^4) - (3X_1^2 + aZ_1^4)^3 - 8Y_1^4,$$

and $Z_3 = 2Z_1 Y_1$.

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 a Trilinear Pairing on Finitely Generated Free R-Modulus

In this section we will construct trilinear 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 [16, 17, 18], 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

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

defined by

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

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.

2.1. Proposition

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

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

then $a=kb$ for some constant k.

Proof. (i) Let $a\in P$. Then we have

$$\begin{aligned} f_{\alpha,\beta,\gamma}(a,a,a) =&[(u_1(v_1w_1-w_1v_1)+v_1(u_1w_1-u_1w_1)\\ &+w_1(u_1v_1-u_1v_1)](\alpha l+\beta m+\gamma n)=0. \end{aligned}$$

(ii) Let $a,b,c,d\in P$. Then we have

$$\begin{aligned} f_{\alpha,\beta,\gamma}(a+b,c,d) =&[(u_1+u_2)(v_3w_4-v_4w_3)+(v_1+v_2)(u_4w_3-u_3w_4)\\ &+(w_1+w_2)(u_3v_4-u_4v_3)].(\alpha l+\beta m+\gamma n)\\ =&[(u_1(v_3w_4-v_4w_3)+v_1(u_4w_3-u_3w_4)\\ &+w_1(u_3v_4-u_4v_3)](\alpha l+\beta m+\gamma n)\\ &+[u_2(v_3w_4-v_4w_3)+v_2(u_4w_3-u_3w_4)\\ &+w_2(u_3v_4-u_4v_3)](\alpha l+\beta m+\gamma n)\\ =&f_{\alpha,\beta,\gamma}(a,c,d)+f_{\alpha,\beta,\gamma}(b,c,d). \end{aligned}$$

Similarly, it can be easily verified that

$$\begin{aligned} f_{\alpha,\beta,\gamma}(a,b+c,d) =&f_{\alpha,\beta,\gamma}(a,b,d)+f_{\alpha,\beta,\gamma}(a,c,d),\\ f_{\alpha,\beta,\gamma}(a,b,c+d) =&f_{\alpha,\beta,\gamma}(a,b,c)+f_{\alpha,\beta,\gamma}(a,b,d). \end{aligned}$$

(iii) Let $a,b,c\in P$. Then we have

$$\begin{aligned} f_{\alpha,\beta,\gamma}(a,b,c) =&[u_1(v_2w_3-v_3w_2)+v_1(u_3w_2-u_2w_3)\\ &+w_1(u_2v_3-u_3v_2)](\alpha l+\beta m+\gamma n)\\ =&-[u_2(v_1w_3-v_3w_1)+v_2(u_3w_1-u_1w_3)\\ &+w_2(u_1v_3-u_3v_1)].(\alpha l+\beta m+\gamma n)\\ =&-f_{\alpha,\beta,\gamma}(b,c,a). \end{aligned}$$

(iv) Let$a,b\in P$. Then we have

$$f_{\alpha,\beta,\gamma}(a,b,0)=[(u_1(0-0)+v_1(0-0)+w_1(0-0)].(\alpha l+\beta m+\gamma n)=0.$$

In a similar manner we can show that $f_{\alpha,\beta,\gamma}(a,0,c)=0$ and $f_{\alpha,\beta,\gamma}(0,b,c)=0$ for all $a,b,c\in P$.

If $f_{\alpha,\beta,\gamma}(a,b,c) = 0$ for all $b, c \in P$ then we have

$$[u_1(v_2w_3 - v_3w_2) + v_1(u_3w_2 - u_2w_3) + w_1(u_2v_3 - u_3v_2)].(\alpha l + \beta m + \gamma n) = 0,$$

for all $b, c \in P$.

This implies $u_1 = v_1 = w_1 = 0$. Therefore $a = 0$.

Let $f_{\alpha,\beta,\gamma}(a,b,c) = 0$for all $c \in P$. Then we have

$$[u_1(v_2w_3 - v_3w_2) + v_1(u_3w_2 - u_2w_3) + w_1(u_2v_3 - u_3v_2)].(\alpha l + \beta m + \gamma n) = 0$$

On rearranging the terms in above expression, we get

$$[u_3(v_1w_2 - v_2w_1) + v_3(u_1w_2 - u_2w_1) + w_3(u_1v_2 - u_2v_1)].(\alpha l + \beta m + \gamma n) = 0$$

This implies that $\frac{u_1}{u_2} = \frac{v_1}{v_2} = \frac{w_1}{w_2} = k$ for some constant k *i.e.* $a = kb$.

3. Construction of a Trilinear Pairing on Elliptic Curves

In this section, we will extend the trilinear 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.

3.1. Torsion Points on An Elliptic Curve, see [10]

Let E be an elliptic curve. Then a point $P \in E$ is said to be a torsion point 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 $nP = O$.

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 $E[n]$.

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 sme time, we construct a map

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

defined by

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

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

3.2. Proposition

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) **Bilinearity:** $f^n_{\alpha,\beta,\gamma}(P,Q,R) = -f^n_{\alpha,\beta,\gamma}(Q,P,R)$ 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 if $P \in E[n], Q \in E[n]$ and $R \in E[nk]$, then

$$f^n_{\alpha,\beta,\gamma}(kP,Q,kR) = kf^n_{\alpha,\beta,\gamma}(P,Q,R).$$

Proof. *(i)* Let $P \in E[n]$. Then we have

$$\begin{aligned} f^n_{\alpha,\beta,\gamma}(P,P,P) =& [a_1(b_1c_1 - b_1c_1) + b_1(a_1c_1 - a_1c_1) \\ & + c_1(a_1b_1 - a_1b_1)](\alpha U + \beta V + \gamma W) = O. \end{aligned}$$

(ii) Let $P, Q, R, S \in E[n]$. Then we have

$$\begin{aligned} f^n_{\alpha,\beta,\gamma}(P+Q,R,S) =& [(a_1+a_2)(b_3c_4 - b_4c_3) + (b_1+b_2)(a_4c_3 - a_3c_4) \\ & + (c_1+c_2)(a_3b_4 - a_4b_3)](\alpha U + \beta V + \gamma W) \\ =& [a_1(b_3c_4 - b_4c_3) + b_1(a_4c_3 - a_3c_4) + c_1(a_3b_4 - a_4b_3) \\ & (\alpha U + \beta V + \gamma W) \\ & + [a_2(b_3c_4 - b_4c_3) + b_2(a_4c_3 - a_3c_4) + c_2(a_3b_4 - a_4b_3) \\ & (\alpha U + \beta V + \gamma W) \\ =& f^n_{\alpha,\beta,\gamma}(P,R,S) + f^n_{\alpha,\beta,\gamma}(Q,R,S), \end{aligned}$$

Similarly, it can be easily verified that

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

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) Let $P, Q, R \in E[n]$. Then we have

$$\begin{aligned} f^n_{\alpha,\beta,\gamma}(P,Q,R) =& [a_1(b_2c_3 - b_3c_2) + b_1(a_3c_2 - a_2c_3) \\ & + c_1(a_2b_3 - a_3b_2)](\alpha U + \beta V + \gamma W) \\ =& -[a_2(b_1c_3 - b_3c_1) + b_2(a_3c_1 - a_1c_3) \\ & + c_2(a_1b_3 - a_3b_1)](\alpha U + \beta V + \gamma W) \\ =& -f^n_{\alpha,\beta,\gamma}(Q,P,R). \end{aligned}$$

(iv) Let $P, Q \in E[n]$. Then we have

$$f^n_{\alpha,\beta,\gamma}(P,Q,O) = [a_1(0-0) + b_1(0-0) + c_1(0-0)].(\alpha U + \beta V + \gamma W) = O$$

In a similar manner we can show that

$$f^n_{\alpha,\beta,\gamma}(P,O,R) = O$$

and

$$f^n_{\alpha,\beta,\gamma}(O,Q,R) = O$$

for all $P, Q, R \in E[n]$.

If $f^n_{\alpha,\beta,\gamma}(P,Q,R) = O$ for all $Q, R \in E[n]$ then we write

$$[a_1(b_2c_3 - b_3c_2) + b_1(a_3c_2 - a_2c_3) + c_1(a_2b_3 - a_3b_2)].(\alpha U + \beta V + \gamma W) = O$$

for all $Q, R \in E[n]$ this implies $a_1 = b_1 = c_1 = 0$. Therefore $P = O$.

(v) Let $P \in E[nk], Q \in E[n]$ and $R \in E[n]$. Then we have

$$\begin{aligned} f^n_{\alpha,\beta,\gamma}(kP,Q,R) =& [ka_1(b_2c_3 - b_3c_2) + kb_1(a_3c_2 - a_2c_3) \\ & + kc_1(a_2b_3 - a_3b_2)].(\alpha U + \beta V + \gamma W), \\ f^n_{\alpha,\beta,\gamma}(kP,Q,R) =& k[a_1(b_2c_3 - b_3c_2) + b_1(a_3c_2 - a_2c_3) \\ & + c_1(a_2b_3 - a_3b_2)].(\alpha U + \beta V + \gamma W), \\ f^n_{\alpha,\beta,\gamma}(kP,Q,R) =& kf^n_{\alpha,\beta,\gamma}(P,Q,R). \end{aligned}$$

Similarly, it can be easily verified that

$$f^n_{\alpha,\beta,\gamma}(P,kQ,R) = kf^n_{\alpha,\beta,\gamma}(P,Q,R)$$

and

$$f^n_{\alpha,\beta,\gamma}(kP,Q,kR) = kf^n_{\alpha,\beta,\gamma}(P,Q,R).$$

4. Application of Trilinear Pairing to Cryptography

In this section we will apply trilinear pairing (constructed in previous section) to elliptic curve cryptography. A protocol defined by a sequence of steps absolutely specifying the actions required by three or more parties in order to achieve a specified objective. In cryptography, 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. It 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 large prime number p and a positive integer r, we denote $q = p^r$. Let E be an elliptic curve over a finite field F_q, given $P \in E(F_q)$ with order n and

$Q \in < P >$, 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 DiffieHellman 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 $f^s_{\alpha,\beta,\gamma}(P, Q, R)$. 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.

4.1. Authenticated Elliptic Curve Diffie Hellman Key Agreement for 3-Parties

It consists of the following phases

Phase 1: Key generation Phase

• Alice, Bob and Carol randomly select secret integers $a, b, c \in (1, s-1)$ respectively.

• They respectively compute aP, bP, cP.

• 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 2: Transmission Phase

• 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.

• 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.

• Carol computes $S_C = c.aP.bP = abcP$ and $f^s_{\alpha,\beta,\gamma}(cP, Q, R)$. He sends $h(S_C)f^s_{\alpha,\beta,\gamma}(cP, Q, R)$ Alice and Bob.

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

Phase 3: Authenticated secret share key generation Phase

• Alice receives $I_A = h(S_B)f^s_{\alpha,\beta,\gamma}(bP, Q, R) \parallel h(S_C)f^s_{\alpha,\beta,\gamma}(cP, Q, R)$. Using the bilinearity of pairing $f^s_{\alpha,\beta,\gamma}$, Alice obtains

$I_A = h(S_{ABC})bcf^s_{\alpha,\beta,\gamma}(P, Q, R)$. Alice computes $h(S_A)^{-1}(mods)$ to obtain her secret share key as $K_A = ah(S_A)^{-1}I_A$.

• Next Bob receives

$$\begin{aligned} I_B =& h(S_B) f^s_{\alpha,\beta,\gamma}(aP, Q, R) \parallel h(S_C) f^s_{\alpha,\beta,\gamma}(cP, Q, R) \\ =& h(S_{ABC}) acf^s_{\alpha,\beta,\gamma}(P, Q, R). \end{aligned}$$

To obtain secret share key, Bob calculates $h(S_B)^{-1}(mods)$ and compute his shared secret key as $K_B = bh(S_B)^{-1} I_B$.

• Finally Carol receives

$$\begin{aligned} I_C =& h(S_A) f^s_{\alpha,\beta,\gamma}(aP, Q, R) \parallel h(S_B) f^s_{\alpha,\beta,\gamma}(bP, Q, R) \\ =& h(S_{ABC}) abf^s_{\alpha,\beta,\gamma}(P, Q, R). \end{aligned}$$

To obtain secret share key, Carol calculates $h(S_C)^{-1}(mods)$ and compute his shared secret key as $K_C = ch(S_C)^{-1} I_C$. It can be easily verified that $K_A = K_B = K_C = abcf^s_{\alpha,\beta,\gamma}(P, Q, R) = K$ (say). Thus there has been established an authenticated common secret key among multiparty Alice, Bob and Carol.

5. Authenticity of the Proposed Scheme

It is obvious from the proposed authenticated elliptic curve Diffie Hellman protocol that the common secret key $K = abcf^s_{\alpha,\beta,\gamma}(P, Q, R)$ 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 $K_B = bf^s_{\alpha,\beta,\gamma}(d_1 P, Q, R)$ or $K_C = cf^s_{\alpha,\beta,\gamma}(d_2 P, Q, R)$ where d_1 or d_2 are introduced by adversary. It means that adversary can alter the first flow of the proposed protocol with $f^s_{\alpha,\beta,\gamma}(d_1 P, Q, R)orf^s_{\alpha,\beta,\gamma}(d_2 P, Q, R)$. To compute

$$bf^s_{\alpha,\beta,\gamma}(d_1 P, Q, R) \text{ or } cf^s_{\alpha,\beta,\gamma}(d_2 P, Q, R)$$

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 $K_A = ah(S_A)^{-1} f^s_{\alpha,\beta,\gamma}(d_3 P, Q, R)$ where d3 is introduced by the

adversary. Now if assume that $d_3 = d_4 h(S_A)$ where d_4 is known by adversary and independent of $h(S_A)$, then $K_A = ah(S_A)^{-1} f^s_{\alpha,\beta,\gamma}(d_4 h(S_A)P, Q, R) = af^s_{\alpha,\beta,\gamma}(d_4 P, Q, R)$. Also to calculate $d_4 h(S_A) f^s_{\alpha,\beta,\gamma}(P, Q, R)$, where d_4 is known by adversary, is intractable without calculating $h(S_A) f^s_{\alpha,\beta,\gamma}(P, Q, R)$. 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. Conclusion

In the present paper we proposed a trilinear pairing map $f_{\alpha,\beta,\gamma} : P \times P \times P \to P$ where P is a finitely generated free- R module with rank three and R is a commutative ring with unity. We apply the structure of this trilinear pairing map to the elliptic curves. Further we show that this trilinear pairing map on elliptic curve is applicable to the current cryptographic schemes. We expect that the proposed trilinear pairing to be more useful in cryptography or in pure mathematics. Thus $f^s_{\alpha,\beta,\gamma}$ pairing with only public values is very difficult as solving the discrete logarithm problem on elliptic curves. Our protocol 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.

Acknowledgement

This research work is supported by University Grant commission (UGC), New Delhi, India, under the Junior Research Fellowship scheme. Authors are thankful to the referees for their precious comments and suggestions, which are really help us to improve the quality of this article.

References

[1] N. Koblitz, Elliptic curve cryptosystem, *Journal of Mathematics Computation*, **48** (1987), 203-209, **doi:** 10.1090/S0025-5718-1987-0866109-5

[2] V. Miller, Use of elliptic curves in cryptography, *Advances in Cryptology-CRYPTO*, **85** (1985), 417-426, **doi:** 10.1007/3-540-39799-X31.

[3] A.H. Koblitz, N. Koblitz, A. Menezes, Elliptic curve cryptography: The serpentine course of a paradigm shift, *Journal of Number Theory*, **131**, No. 5 (2011), 781-814, **doi:** 10.1016/j.jnt.2009.01.006.

[4] M. Kumar, P. Gupta, Cryptographic schemes based on elliptic curve over the ring Zp[i], *Applied Mathematics*, **7**, No. 3 (2016), 304-312, **doi:** 10.4236/am.2016.72027.

[5] André Weil, Sur les fonctions algébriques à corps de constantes fini, *C.R. Acad. Sci. Paris*, **210** (1940), 592594.

[6] A. Joux, A one round protocol for tripartite Diffie-Hellman, In: *Algorithmic Number Theory: 4-th International Symposium*, ANTS-IV, Lecture Notes in Computer Science, 1838, 385393, (2000); Full version: *Journal of Cryptology*, **17** (2004), 263276, **doi:** 10.1007/1072202823.

[7] D. Boneh, M. Franklin, Identity-based encryption from the Weil pairing, *Advances in Cryptology CRYPTO 2001*, Lecture Notes in Computer Science, 2139, 213229; Full version: *SIAM Journal on Computing*, **32** (2003), 586615, **doi:** 10.1007/3-540-44647-813.

[8] D. Boneh, B. Lynn, H. Shacham, Short signatures from the Weil pairing, *Advances in Cryptology ASIACRYPT 2001*, Lecture Notes in Computer Science, 2248 (2001), 514532; Full version: *Journal of Cryptology*, **17** (2004), 297319, **doi:** 10.1007/s00145-004-0314-9.

[9] J. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1986.

[10] D.R. Stinson, *Cryptography Theory and Practice*, Chapman and Hall/CRC, United Kingdom, 2006.

[11] L.C. Washington, *Elliptic Curves Number Theory and Cryptography*, Chapman and Hall/CRC, United Kingdom, 2008.

[12] G.H. Hardy, E.M. Wright, *An Introduction to the Theory of Numbers*, Oxford University Press, United Kingdom, 1938.

[13] N. Sklavos, X. Zhang, *Wireless Security and Cryptography Specifications and Implementations*, Chapman and Hall/CRC, United Kingdom, 2007.

[14] H. Nemati, *Information Security and Ethics: Concept, Methodologies, Tools, and Applications*, Information Science Reference, New York, 2007.

[15] D. Hankerson, J.A. Menezes, S. Vanstone, *Guide to Elliptic Curve Cryptography*, Springer-Verlag, Germany, 2004.

[16] P.B. Bhattacharya, S.K. Jain, S.R. Nagpaul, *Basic Abstract Algebra*, Cambridge University Press, United Kingdom, 1995.

[17] W.J. Gilbert, *Modern Algebra with Application*, Willey-Interscience, New York, 2004.

[18] J.A. Gallian, *Contemporary Abstract Algebra*, Narosa Publishing House, New Delhi, 1998.