International Journal of Engineering & Technology, 7 (2.33) (2018) 1117-1119

SPC

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Bilinear Pairings on Lemniscates Curve

G. Jai Arul Jose[1], Louay A. Hussein Al-Nuaimy[2],Md Mastan[3]

[1,2,3] Assistant Professor, Department of Computer Science & MIS,
Oman College of Management & Technology, Halban, Sultanate of Oman
**Corresponding author Email: [1]g.jai.areul@omancollege.edu.com [2]loay.alneimy@omancollege.edu.com*
[3]mastan.mohammed@omancollege.edu.com

Abstract

Bilinear pairings, also called bilinear mappings, have developed as an important active area of cryptographic research. The Tate and Weil pairings were proposed for the use of cryptography such as identity-based cryptography, attribute base cryptography, pairing based cryptography, and short signatures. A bilinear pairing is a mapping of a pair of points on an elliptic curve defined on any field *F* to an element of the multiplicative group of a finite extension of *F*. Bilinear mappings transfer the discrete logarithm problem from a curve defined over a finite field to the multiplicative group of a finite field. In geometry, Lemniscates curve is a plane curve based on two given points called foci. These foci are located at distance *2a* from each other. In this work, bilinear pairings is applied to Lemniscates curve with the model of elliptic curve pairings.

Keywords–*Bilinear pairing, Curve Arithmetic, Lemniscates curve, Elliptic Curve, Cryptography*

1. Introduction

Bilinear pairings is used to develop inventive protocols to send and receive secret messages between two or more parties. The purpose of this work is to study bilinear pairings and apply it on Lemniscates curves. During 1964 an individual, James Bernoulli, from well-known Bernoulli family (of mathematicians) published his research on a symmetric curve which he called it as *lemniscus*. The word *lemniscus* in Latin means ribbon. The *lemniscus* curve is a special type of a Cassinian Oval. This Lemniscates curve is symmetric with respect to the origin, and the coordinate axes. This symmetricity is an important property of this curve. The definition of Lemniscates curve is the locus of a point, which the product of those distances from 2 fixed points (-*a*, 0) and (*a*, 0), called the foci, is at a distance of *2a* units and is equivalent to a^2. The Cartesian formula of Lemniscates is $(x^2 + y^2)^2 = 2a^2(x^2 - y^2)$. Figure 1 shows the curve which the value of *a* = 5. The polar coordinate equation of the curve is $x = r\cos\theta$ and $y = r\sin\theta$

2. Operations on the Lemniscates Curve

Let us set $t^2 = x^2 + y^2$.
Then, the equation of Lemniscates is become $t^4 = 2a^2(x^2 - y^2) = 2a^2(x^2 + y^2 - 2y^2) = 2a^2(t^2 - 2y^2)$
i.e.; $t^4 - 2a^2t^2 = -4a^2y^2 \quad \Rightarrow \quad y^2 = \frac{2a^2t^2 - t^4}{4a^2} \quad \Rightarrow \quad y = \pm\frac{\sqrt{2a^2t^2 - t^4}}{2a}$
also, we can write the equation of the Lemniscates as $t^4 = 2a^2(x^2 - y^2) = 2a^2(2x^2 - x^2 - y^2)$
$= 2a^2(2x^2 - t^2)$

i.e.; $t^4 + 2a^2t^2 = 4a^2x^2 \quad \Rightarrow \quad x^2 = \frac{2a^2t^2 + t^4}{4a^2} \quad \Rightarrow \quad x = \pm\frac{\sqrt{2a^2t^2 + t^4}}{2a}$
There will be two issues; the first issue is how to select the sign of *x* and *y*; the second issue is the *t* shall lie on at which interval.

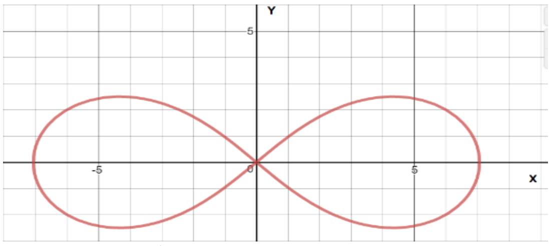

Fig. 1 Lemniscates Curve

For the first case, if there is a point (*x*, *y*) on the Lemniscates curve, the other points are (-*x*, *y*), (*x*, -*y*) and (-*x*, -*y*). So, it is sufficient to parameterize the Lemniscates curve on the first quadrant. The remaining curve could be found by the property of symmetricity of the Lemniscates curve.
Therefore, we take, $x = \frac{\sqrt{2a^2t^2 + t^4}}{2a}$
and $= \frac{\sqrt{2a^2t^2 - t^4}}{2a}$.
For the second case, note that the Lemniscates curve passes through the origin and crosses the *x*-axis at (1, 0). The point (0, 0) links to *t* = 0 and (1, 0) links to *t* = 1. Therefore *t* should be in the interval [0, 1]

1.2. The Arc Length of Lemniscates

Consider *a* > 0, where *a* is a real number.
Let $F_1 = (a, 0)$ and $F_2 = (-a, 0)$ be the foci on R^2.
Let $C = \{ P \in R^2; PF_1 . PF_2 = a^2 \}$.
Let us develop the equation of the curve *C* on polar coordinates.

We have $P = (r\ cos\ \theta, r\ sin\ \theta)$:
Then $PF_1^2 = r^2 + a^2 - 2ar\cos\theta, PF_2^2 = r^2 + a^2 + 2ar\cos\theta$
Hence, $(r^2 + a^2 - 2ar\cos\theta)(r^2 + a^2 + 2ar\cos\theta) = (r^2 + a^2)^2 - 4a^2r^2\cos^2\theta = a^4$
$r^4 + 2r^2a^2 + a^4 - 4a^2r^2\cos^2\theta = a^4$
$r^2 = 2a^2(2\cos^2\theta - 1) = 2a^2\cos 2\theta$
In case of $P \in C$ is on the 1st quadrant. Let s be the length of arc among $O = (0, 0)$ & P.
Therefore $s = \int_0^\theta \sqrt{r^2 + \left(\frac{d\theta}{dr}\right)^2}\ d\theta$. Since $d\theta = \frac{d\theta}{dr}dr,\ s = \int_0^r \sqrt{r^2 + \left(\frac{d\theta}{dr}\right)^{-2}}\ \frac{d\theta}{dr}\ dr$.
Hence $= \int_0^r \sqrt{1 + r^2\left(\frac{d\theta}{dr}\right)^2}\ dr$.
As
$r = a\sqrt{2\cos 2\theta}, \frac{dr}{d\theta} = -\frac{2a\sin 2\theta}{\sqrt{2\cos 2\theta}}, Thus\ \frac{d\theta}{dr} = -\frac{\sqrt{2\cos 2\theta}}{2a\sin 2\theta}\ that\ is\ \left(\frac{d\theta}{dr}\right)^2 = \frac{\cos 2\theta}{2a^2\sin^2 2\theta}$
$\cos 2\theta = \frac{r^2}{2a^2}$, $\sin^2 2\theta = 1 - \cos^2 2\theta$

$$= \frac{4a^4 - r^4}{4a^4}\ \ Hence\ \left(\frac{d\theta}{dr}\right)^2 = \frac{r^2}{4a^4 - r^4}$$

Therefore, the arc length of Lemniscates is

$$s = \int_0^r \sqrt{\frac{4a^4}{4a^4 - r^4}}\ dr = \int_0^r \frac{2a^2}{\sqrt{4a^4 - r^4}}dr$$

2.2. The Lemniscates Function

The Lemniscates curve may appear unusual at initial look, but various parallels exist between it and of the sine function. i.e.; the sine function might be defined as the inverse integral function as below:
$y = sin\ s \Leftrightarrow s = sin^{-1}y = \int_0^y \frac{1}{\sqrt{1-t^2}}\ dt$.
The Lemniscates function $\Upsilon = \varphi(s)$ can also be defined as inverse function of an integral
$\Upsilon = \varphi(s) \Leftrightarrow s = \int_0^\Upsilon \frac{1}{\sqrt{1-t^2}}dt$.

2.3. The Properties of φ(s)

The function of Lemniscates satisfies various interesting identities:
Proposition 1:
If $f(x) = sin\ x$, then:

1) $f(x+2\pi) = f(x)$
2) $f(-x) = -f(x)$
3) $f(\pi - x) = f(x)$
4) $f'^2(x) = 1 - f^2(x)$

The function of Lemniscates $\varphi(s)$ fulfils related identities. In fact, we may view the function of Lemniscates as a conjecture of the sine function for several curves. Of course, the sine function is only significant with respect to the unit circle, whereas $\varphi(s)$ pertains to the Lemniscates curve. We notice the following propositions are true of the function of Lemniscates:
Proposition 2:
If $f(s) = \varphi(s)$, then:

1) $f(s+2\omega) = f(s)$
2) $f(-s) = -f(s)$
3) $f(\omega - s) = f(s)$
4) $f'^2(s) = 1 - f^4(s)$

The identities 1, 2 and 3 are very easy to observe. The 4th of first Proposition is simply rewritten of the well-known identity $cos^2x = 1 - sin^2x$, where $cos\ x$ is, in fact, the differentiation of $sin\ x$. Now though the similarity among this identity and the corresponding identity for the function of Lemniscates is clear, this is the least intuitive identity of $\varphi(s)$.

2.4. The Subtraction and Addition Laws for φ(S)

The trigonometry sine function fulfil the addition law $sin(x+y) = sin\ x\ cos\ y + cos\ x\ sin\ y$. Therefore, if we say $f(x) = sin\ (x)$, then $f(x+y) = f(x)f'(y) + f'(x)f(y)$. We derive a related result for $\varphi(s)$, starting with the below identity:

$$\int_0^\alpha \frac{1}{\sqrt{(1-t^4)}}\ dt + \int_0^\beta \frac{1}{\sqrt{(1-t^4)}}dt = \int_0^\Upsilon \frac{1}{\sqrt{(1-t^4)}}\ dt$$

where $\alpha, \beta \in [0, 1]$ and $\Upsilon = \frac{\alpha\sqrt{1-\beta^4} + \beta\sqrt{1-\alpha^4}}{1+\alpha^2\beta^2} \in [0, 1]$
By allowing x, y and z equal the 3 integrals above, respectively, and applying the φ function to both of the sides of the equation, we get

$\varphi(x+y) = \varphi(z) = \Upsilon = \frac{\alpha\sqrt{1-\beta^4} + \beta\sqrt{1-\alpha^4}}{1+\alpha^2\beta^2}$, $0 \le x+y \le \frac{\omega}{2}$.
Now, since $\varphi(x) = \alpha$ and $\varphi(y) = \beta$, we have
$\varphi(x+y) = \varphi(z) = \Upsilon = \frac{\varphi(x)\sqrt{1-\varphi^4(y)} + \varphi(y)\sqrt{1-\varphi^4(x)}}{1+\varphi^2(x)\varphi^2(y)}$, $0 \le x+y \le \frac{\omega}{2}$.
And the last of our basic φ properties implies that $\sqrt{1 - \varphi^4(x)} = \varphi'(x)$, yielding

$\varphi(x+y) = \frac{\varphi(x)\varphi'(y)+\varphi'(x)\varphi(y)}{1+\varphi^2(x)\varphi^2(y)}$, $0 \le x+y \le \frac{\omega}{2}$.
Since both sides of the equation are analytic functions of x which are defined $\forall\ x$ when y is any fixed value, the equation holds true $\forall\ x$ and y.
The subtraction law for $\varphi(s)$ shall be easily derived from the addition law. Since $\varphi(-x) = -\varphi(x)$ and $\varphi'(-x) = \varphi'(x)$
$\varphi(x-y) = \frac{\varphi(x)\varphi'(y)-\varphi'(x)\varphi(y)}{1+\varphi^2(x)\varphi^2(y)}$

2.5. Scalar Multiplication

From addition law, we can get $\varphi(2x) = \frac{2\varphi(x)\varphi^{|}(x)}{1+\varphi^4(x)}$.
By replacing x and y with $2x$ and x, respectively, we get
$\varphi(3x) + \varphi(x) = \varphi(2x+x) + \varphi(2x-x) = \frac{2\varphi(2x)\varphi'(x)}{1+\varphi^2(2x)\varphi^2(x)}$.
Now using the doubling formula
$\varphi(2x) = \frac{2\varphi(x)\varphi'(x)}{1+\varphi^4(x)}$

$$\varphi(3x) + \varphi(x) = \frac{\left(2\frac{\left(2\varphi(x)\varphi^{|}(x)\right)}{1+\varphi^4(x)}\varphi^{|}(x)\right)}{1 + \left(\frac{2\varphi(x)\varphi^{|}(x)}{1+\varphi^4(x)}\right)^2\varphi^2(x)}$$

Finally, since $\varphi'^2(x) = 1 - \varphi^4(x)$, we get our result:
$\varphi(3x) = \varphi(x)\frac{3-6\varphi^4(x)-\varphi^8(x)}{1+6\varphi^4(x)-3\varphi^8(x)}$.
With these understanding, we explore the creation on the Lemniscates. The point over the Lemniscates with respect to the arc length s could be constructed by straight edge and compass iff $\Upsilon = \varphi(s)$ is a constructible number. By Noting that as the Lemniscates be defined by the equation $(x^2 + y^2)^2 = 2a^2(x^2 - y^2)$ and that $\Upsilon^2 = x^2 + y^2$, we note that $\Upsilon^4 = x^2 - y^2$. Then by solving in terms of Υ, we see that:

$$x = \pm\sqrt{\frac{1}{2}(r^2 + r^4)}\ ;\ \ y = \pm\sqrt{\frac{1}{2}(r^2 - r^4)}$$

2.6. Lemniscates on Prime Field F_p

The equation of Lemniscates on a prime field F_p is
$(x^2 + y^2)^2 \equiv 2a^2(x^2 - y^2)\ (mod\ p)$
Here $a\ mod\ p \neq 0$ and p is a prime number.
Here the elements of the field are integers from 0 to $p - 1$. Every arithmetic operations comprise of whole numbers from 0 to $p - 1$.

The algebraic rules discussed in previous section is used on the prime field F_p.

3. Bilinear Pairings

In this section how the bilinear pairings is defined and the properties of bilinear pairing is discussed with respect to Lemniscates curve.

3.1. Definition of Pairings

Let p be a prime number. Let (G_1, +) be an additive cyclic group of points of a lemniscates curve L over a finite field F of order p and with identity I. Let (G_2, *) be a multiplicative cyclic group of order p with identity 1. A bilinear pairing is a function map e on (G_1, G_2), written as

$e : G_1 \times G_1 \rightarrow G_2$,

which satisfies the following conditions:

1. Bilinear: $\forall$ A, B, C $\in G_1$,

e(A + B, C) = e(A, C) e(B, C)

e(A, B + C) = e(A, B) e(A, C)

2. Non-degenerate: e(A, B) $\neq$ 1 for some A, B $\in G_1$.

3. Alternating: $\forall A \in G_1$, e(A, A) = 1

and e(B, C) = $e(C, B)^{-1}$

4. Compatible: $\forall A \in L[pp^{\backslash}]$, $B \in L[p]$ and p, $p^{\backslash} \in Z$, we have $e_{pp^{\backslash}}(A, B) = e_p([p^{\backslash}]A, B)$.

3.2. Pairing on Lemniscates

Before defining the Pairing, take a look at divisor groups and divisor is necessary. Let L be an lemniscates curve defined over the field F. The divisor group of L is an abelian group which is denoted by div(L), generated by the points A of L. Hence, a divisor $D \in \mathrm{div}(L)$ is the formal sum

$$D = \sum_{A \in L(F)} n_p(A)$$

where $n_p \in$ Z and n_p is zero for all but finitely more $A \in L(F)$. The following are some results about divisor and divisor group:

1. The degree of a divisor D, *deg D*, is the coefficients n_p of

$$D = \sum_{A \in L(F)} n_p(A)$$

2. A divisor is principal, if *deg D* is zero and

$$D = \sum_{A \in L(F)} n_p(A) = I$$

3. Let L be a lemniscates curve over field F and let A, B $\in L(F)$. Then (A) ~ (B) iff A = B.

4. Let L be lemniscates curve over a field F and let D be a divisor in *div*(L). Then $\exists$ unique point A $\in$ *div*(L) fulfilling D ~ (A) – (I). We define $\tau : D_p \rightarrow P$, i.e.; τ sends each divisor D_p in div(L) to the associated point A.

5. Let A be a point on an lemniscates curve, f_A a function, and D_A = (A) − (I) a divisor such that div(f_A) = D_A . Then $f_A(D_A)$ = $f_A(A)/f_P(I)$.

4. Conclusion

Lemniscates curve is symmetric curve and have many interesting properties. Pairing on elliptic and hyper elliptic curve have been used in many cryptographic scheme. Presently research shows pairing on elliptic curve is better than pairing on elliptic curves. In this article we discussed the point arithmetic on the symmetric curve lemniscates and presented the bilinear pairing on this curve. This study has to be improved with the development of algorithm for pairing operations.

References

[1] Alfred Menezes; An introduction to Pairing-Based Cryptography. Article, 27-Oct-2013.

[2] Andreas Enge; Bilinear pairings on elliptic curves. Article, 14-Feb-2014.

[3] A. Menezes, P. Van Orschot, and S.Vanstone. Handbook of Applied Cryptography. CRC press, 1997.

[4] http://en.wikipedia.org/wiki/Cyclic group.

[5] K. Araki, T. Satoh and S. Miura. Overview of Elliptic Curve Cryptography. Public Key Cryptography, PKC'98, LNCS 1431, 29–48.

[6] C. Sajeev, G. Jai Arul Jose, "Elliptic Curve Cryptography Enabled Security for Wireless Communication", International Journal on Computer Science and Engineering, Vol. 02, No. 06, pp. 2187-2189, 2010.

[7] Douglas R. Stinson; Cryptography, Theory and Practice. Chapman & Hall/CRC, 3rd Edition, 2006.

[8] Joseph H. Silverman and John Tate; Rational Points on Elliptic Curves. Springer, 2nd Edition, 1994.

[9] Benbouziane T., Houary, H., Kahoui, M.: Polynomial Parametrization of nonsingular algebraic curves. University of Firenze, Firenze, 2000.

[10] Gahleitner, M., J¨uttler, B., Schicho, J.: Approximate parametrization of planar cubics. In Curve and Surface Fitting. Nashboro Press, St. Malo, 2002.

[11] Joseph H. Silverman, The Arithmetic of Elliptic Curves. Springer, 2nd Edition, 2009.

[12] Salman A, Diehl W, Kaps JP. A light-weight hardware/software co-design for pairing-based cryptography with low power and energy consumption. InField Programmable Technology (ICFPT), 2017 International Conference on 2017 Dec 11 (pp. 235-238). IEEE.

[13] El Mrabet N, Joye M, editors. Guide to Pairing-Based Cryptography. CRC Press; 2017 Jan 6.

[14] Barreto PS, Costello C, Misoczki R, Naehrig M, Pereira GC, Zanon G. Subgroup security in pairing-based cryptography. InInternational Conference on Cryptology and Information Security in Latin America 2015 Aug 23 (pp. 245-265). Springer, Cham.