A Study on the Construction and Arithmetic of Lemniscates Curves

Dr. S. Joseph Robin
Associate Professor, Department of Mathematics, Scott Christian College
Nagercoil, Tamil Nadu, India
sjosephrobin@yahoo.com

Abstract **– This paper studies the mathematics of lemniscates curve, whose most common form is the locus of points the product of whose distances from two fixed points (the foci) a distance 2a away is the constant a^2, and explore the pairing based cryptography on this curve from theoretical and implementation point of view. In this regards, we first study the construction and arithmetic on lemniscates curve and then design a new cryptographic scheme.**

Keywords **– Cryptography, Pairing-based Cryptography, Elliptic Curve, Lemniscates Curve, Bilinear Pairing**

I. INTRODUCTION

In 1964 James Bernoulli, a member of famous Bernoulli family of mathematicians published his findings on a curve which he called a lemniscus. A lemniscus is Latin for the word ribbon. This curve is a special case of a Cassinian Oval and its arclength became very important for later work on elliptical functions. Another interesting fact about the lemniscates is that it is symmetric about the symmetric about the x-axis, the y-axis and the origin.

The Lemniscates is defined as the locus of a point, the product of whose distances from two fixed points (-a,0) and (a,0), the foci, is 2a units apart and is equal to a^2.

The Cartesian formula of Lemniscates is

$(x^2 + y^2)^2 = a^2(x^2 - y^2)$

The Parametric formula is

$x = cos\theta \pm \sqrt{cos2\theta}$

$y = sin\ \theta \pm \sqrt{cos2\theta}$

Figure 1 shows the shape of the Lemniscates.

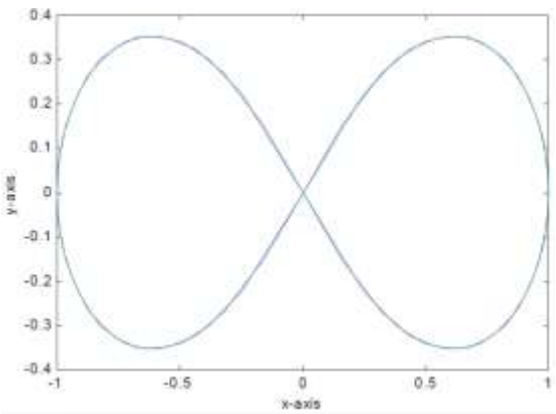

Fig. 1 Lemniscates Curve

II. THE LEMNISCATES FUNCTION

The lemniscates may appear peculiar at first glance, but many parallels exist between it and the sine function. For example, we may define the sine function as the inverse function of an integral in the following way:

$y = \sin s \Leftrightarrow s = \sin^{-1}y = \int_0^y \frac{1}{\sqrt{1-t^2}}\,dt.$

The lemniscates function $\Upsilon = \varphi(s)$ may also be defined as the inverse function of an integral

$\Upsilon = \varphi(s) \Leftrightarrow s = \int_0^{\Upsilon} \frac{1}{\sqrt{1-t^2}}\,dt.$

III. PROPERTIES OF φ(S)

The function satisfies several 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 lemniscates function φ(s) satisfies similar identities. In fact, we may regard the lemniscates function as a generalization of the sine function for different curve. Of course, the sine function is only relevant with respect with respect to the unit circle, whereas φ(s) pertains to the lemniscates. We see that the following is true of the lemniscates function:

Proposition 2:

If f(s) = φ(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 first three of these identities are not difficult to observe. The last part of Proposition 1 is simply restatement of the familiar identity $\cos^2 x = 1 - \sin^2 x$, where cos x is, of course, the derivative of sin x. Now although the similarity between this identity and the corresponding identity for the lemniscates function is clear, this is the least intuitive identity of φ(s).

The Addition law for φ(s):

The sine function satisfies the addition law sin(x+y) = sin x cos y + cos x sin y. So if we say f(x) = sin(x), then f(x+y) = f(x)f′(y) + f′(x)f(y). We will derive a similar result for φ(s), beginning with the following 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 α, β ∈ [0, 1] and $\Upsilon = \frac{\alpha\sqrt{1-\beta^4}+\beta\sqrt{1-\alpha^4}}{1+\alpha^2\beta^2} \in [0, 1]$

By letting x, y and z equal the three integrals above, respectively, and applying the φ function to both sides of the equation, we obtain

$\varphi(x+y) = \varphi(z) = \Upsilon = \frac{\alpha\sqrt{1-\beta^4}+\beta\sqrt{1-\alpha^4}}{1+\alpha^2\beta^2}$, $0 \le x+y \le \frac{\omega}{2}$.

Now since φ(x) = α and φ(y) = β, 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

$\varphi(x+y) = \frac{\varphi(x)\varphi'(y)+\varphi'(x)\varphi(y)}{1+\varphi^2(x)\varphi^2(y)}$, $0 \le x+y \le \frac{\omega}{2}$.

Now since both sides of this equation are analytic functions of x that are defined for all values x when y is any fixed value, the equation holds true for all values x and y.

The subtraction law for φ(s):

The subtraction law for φ(s) is easily derived from the addition law. Since φ(-x) = -φ(x) and φ′(-x)= φ′(x)

$\varphi(x-y) = \frac{\varphi(x)\varphi'(y)-\varphi'(x)\varphi(y)}{1+\varphi^2(x)\varphi^2(y)}$

Scalar Multiplication:

Then by replacing x and y with 2x and x, respectively, we have

$\varphi(3x)+\varphi(x) = \varphi(2x+x)+\varphi(2x-x) = \frac{2\varphi(2x)\varphi'(x)}{1+\varphi^2(2x)\varphi^2(x)}$.

Now using the doubling formula $\varphi(2x) = \frac{2\varphi(x)\varphi'(x)}{1+\varphi^4(x)}$

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

And finally, since $\varphi'^2(x) = 1 - \varphi^4(x)$, we have our result:

$\varphi(3x) = \varphi(x)\frac{3-6\varphi^4(x)-\varphi^8(x)}{1+6\varphi^4(x)-3\varphi^8(x)}$.

Now that we have an understanding of the lemniscates function and its properties, we may explore construction on the lemniscates.

The point on the lemniscates corresponding to arc length s can be constructed by straightedge and compass iff ϒ=φ(s) is a constructible number.

Noting that the lemniscates is defined by the equation $(x^2+y^2)^2 = a^2(x^2-y^2)$ and that $\Upsilon^2 = x^2+y^2$, we see that $\Upsilon^4 = x^2 - y^2$. Then by solving in terms of ϒ, we see that:

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

IV. THE CRYPTOGRAPHIC SCHEME ON LEMNISCATES CURVE (LCC)

The properties discussed above are on real numbers. Operations over the real numbers are slow and inaccurate due to the round-off errors. Cryptographic operations need to be faster and accurate. To make operations on Lemniscates to be more efficient, it needs the cryptography over prime field F_P. The field should be chosen with finitely large number of points suited for cryptographic operations.

A. Lemniscates on Prime field F_p

The equation of Lemniscates on a prime field F_p is

$(x^2+y^2)^2 \equiv a(x^2-y^2)\ (mod\ p)$

where a mod p ≠ 0

Here the elements of the finite field are integers between 0 and p-1. All the operations such as subtraction, multiplication and division involve integers between 0 and p-1. The prime number should be chosen in such a way there exists a finitely large number of points on this curve in order to make the security crypto system to be secure. Algebraic rules for addition and doubling of points described above can be adopted over F_p.

B. Domain parameter over F_p

The domain parameters over F_p are a sextuple T=(p,a,G,n,h); where p is the prime number defined for finite field F_p, a is the parameters for the curve, G is the generator point (x_G,y_G), a point on this curve is chosen for Cryptographic operations, n is the order of the curve. The scalar for point multiplication is chosen as a number between 0 and n-1, h is the cofactor where $h = \#F(F_p)/n.\#F(F_p)$ is the number of points on the Lemniscates curve.

C. Lemniscates Curve Key Pairs

All the public-key cryptographic schemes described has use key pairs known as Lemniscates curve key pairs. Given some Lemniscates curve domain parameters T=(p,a,G,n,h), or T=(m,f(x),a,G,n,h), a Lemniscates curve key pair (d,Q) associated with T consists of a Lemniscates

curve secrete key d which is an integer in the interval [1,n-1], and a Lemniscates curve public key $Q=(x_Q, y_Q)$ which is the point $Q=dG$.

D. Encryption and Decryption

To encrypt and send a message P_m to B, A chooses a random positive integer k and produces the cipher text C_m consisting of the pair of points.

$$C_m=[kG, P_m+kP_B]$$

Here A has used B's public key P_B. To decrypt the cipher text, B multiplies the first point in the pair by B's private key n_B and subtracts the result from the second point as shown below

$P_m+kP_B - n_B(kG)=P_m+k(n_BG)-n_B(kG)=P_m$

E. Key exchange:

Key exchange between users A and B can be accomplished as follows:

1. A select an integer n_A less than n. This is A's private key. A then generates a public key $P_A=n_A*G$; the public key is a point on F(a,b)
2. B similarly select a private key n_B and computes a public key P_B

Public keys are exchanged between the nodes A and B. A generates the secret key $k=n_A*P_B$. B generates the secret key $k=n_B*P_A$.

V. CONCLUSION

The scheme is simulated and compared with other cryptographic schemes. Comparison of the encryption time and decryption time using RSA, MPRSA, ECC and LCC were done and from the simulated results of LCC were proven that the LCC is best since it had the least encryption and decryption time. Further in ECC domain parameters there are two curve parameters but in Lemniscates only one parameter so that the computational time is considerably reduced.

REFERENCES

[1] N. Koblitz, "Elliptic Curve Cryptosystems", Mathematics of Computation, vol. 48, pp. 203-209. 1987.

[2] V. Miller, "Uses of Elliptic Curves in Cryptography", Advances in Cryptology; proceedings of Cryto'85, pp. 417-426,1986.

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

[4] Certicom Research. SEC 2:Recommended Elliptic Curve Domain parameters. Standards or efficient Cryptography Version 1.0, Sep 2000.

[5] W. R. Sam Emmanuel, C. Suyambulingom, "Safety Measures Using Sextic Curve Cryptography", International Journal of Computer Science and Engineering, Vol. 3(2), February 2011, pp. 800-806.

[6] W. R. Sam Emmanuel, "Performance Evaluation of Sextic Curve Cryptography and Probability Symmetric Curve Cryptography in Wireless Sensor Networks", International Journal of Computer Applications, Vol. 61(4), pp.23-27.

[7] Neal Koblitz. 2007. The uneasy relationship between Mathematics and Cryptography. Notes of the AMS, 54(8):972-979.

[8] William Stallings. 2004. Cryptography and Network Security Principles and Practices. 3rd ed. Pearson Education.

[9] Junfeng Fan, Kazuo Sakiyama, Ingrid Verbauwhede. 2008. Elliptic curve cryptography on embedded multicore systems. Journal of Design Automation for Embedded Systems, 123-134.

[10] Kanniah, Samsudin. 2007. Multi-threading elliptic curve cryptosystems. Proceedings of Telecommunications and Malaysia International conference on communications, 134-139.

[11] Lee, Wong. 2004. A random number generator based elliptic curve operations. Computers and Mathematics with Applications, 47:217-226.

