International Journal of Pure and Applied Mathematics
Volume 89 No. 4 2013, 547-552
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
doi: http://dx.doi.org/10.12732/ijpam.v89i4.8

ijpam.eu

AN ELLIPTIC CURVE METRIC ON THE FUNDAMENTAL GROUP OVER $GF(2^5)$

A.R. Rishivarman[1] §, B. Parthasarathy[2]
[1]SASTRA University
Tanjavur, Tamilnadu, INDIA
[1]Department of Mathematics
Dr. Pauls Engineering College
Tamilnadu, INDIA
[2]Department of Mathematics
Mailam Engineering College
Tamilnadu, INDIA

Abstract: Since the introduction of public-key cryptography by Diffe and Hellman in 1976, the potential for the use of the discrete logarithm problem in public-key cryptosystems has been recognized. Although the discrete logarithm problem as first employed by Diffe and Hellman was defined explicitly as the problem of finding logarithms with respect to a generator in the multiplicative group of the integers module a prime, this idea can be extended to arbitrary groups and in particular, to elliptic curve groups. The resulting public - key systems provide relatively small block size, high speed, and high security. In the present paper we define a metric on the fundamental group of elliptic curve over the Galois field $GF(2^5)$. The fact that defining a new metric among the elliptic curves has potential application in the theory of cryptography; especially to thwart fixed table attack.

Key Words: galois field, elliptic curve, finite field, metric, fundamental group, isomorphism class of curves

Received: August 17, 2013

§Correspondence author

1. Introduction

There are three families of public-key algorithms that have considerable significance in current data security practice. They are integer factorization, discrete logarithm, and elliptic curve based schemes[2][3]. Integer factorization based schemes such as RSA[4] and discrete logarithm based schemes such as Diffe -Hellman[5] provide intuitive ways of implementation. However both methods admit of sub-exponential algorithm of cryptanalysis[7]. In this regard elliptic curve cryptography, first introduced Koblitz[2] and Miller[3] may be the most cryptographic method available[6][8]. The best current brute force algorithm for cryptanalysis of ECC require $O(n^{1/2})$ steps where n is the order of the additive group. For example , using the best current brute force algorithms ECC with a key size of 173 bits provides the same level of cryptographic security as RSA with a key size of 1024 bits. This results in smaller system parameters band width savings, faster implementations and lower power consumptions. In addition, elliptic curve over finite fields offer an inexhaustible supply finite abelian groups , thus allowing more flexible fields selections than conventional discrete logarithm schemes. Because of these advantages ECC has attracted extensive attention in recent years[9][15]. In the present paper we define a metric on the fundamental group of elliptic curve over the Galois field $GF(2^5)$. The fact that defining a new metric among the elliptic curve have potential application in resisting fixed table attacks in the theory of cryptography. An irreducible polynomial taken for construction of the field is $f(x) = x^5 + x^2 + 1$.

2. Elliptic Curve

Let $GF(2^5)$ be a characteristic 2 finite field, and let$a, b \in GF(2^5)$ satisfy $b \neq 0 \in GF(2^5)$ Then a (non-super singular) elliptic curve $E(GF(2^5))$ over $GF(2^5)$ defined by the parameters $a, b \in GF(2^5)$ consists of the set of solutions or points$P = (x, y)$for $x, y \in GF(2^5)$ to the equation:

$$y^2 + xy = x^3 + ax^2 + b \, in \, GF(2^5)$$

together with an extra point O called the point at infinity[12][13]. (Here the only elliptic curves over$GF(2^5)$ of interest are non-super singular elliptic curves.)

3. Fundamandel Group of Elliptic Curve

Let C_1 andC_2 be any two elliptic curves with two common end points, contained in a region Ω, the two curves can be deformed into each other, and are said to

be homotopic inΩ. This is evidently an equivalence relation. We can thus divide all elliptic curves into equivalence classes, called homotopy classes; the curves in a homotopy class have common end points and can be deformed into each other with in Ω. It deserves to point out that different parametric representations of the same curve are always hemitropic. From this definition it can be shown that the elliptic curves from a point $z_0^{\square}$, with respect to the region Ω, form a group. That is, it can be established that;

- The associative law:$(C_1C_2)C_3$ is homotopic to$C_1(C_2C_3)$
- Existence of unit curve 1: $C1$and $1C$ are homotopic to$C$
- Existence of inverse: CC^{-1} and $C^{-1}C$ are homotopic to 1

The group which we have constructed is the homotopy group, or, the fundamental group, of the region Ω with respect to the pointz_0. As abstract group it does not depend on the point z_0. Therefore it can be shown that there is a point $\grave{z_0}$ such that homotopy group with respect to z_0 and$\grave{z_0}$ are isomorphic.

The explicit determination of homotopy group is simplified by the fact that the homotopy group is obviously a topological invariant. Indeed, by a topological mapping ofΩ onto $\Omega^{\square}$ any deformation in Ω can be carried over to $\Omega^{\square}$ and is seen to determine a product preserving one-to-one correspondence between the homotopy classes. Topologically equivalent regions have therefore isomorphic homotopy groups. The homotopy group of a disk reduces to the unit element; this means that any two curves with common end points are homotopic. In particular, the whole plane has likewise a homotopy group which reduces to the unit element. Therefore it can then be proved that, any simply connected region has a fundamental group which reduces to its unit element.

4. The Metric

The metric that we propose is based on the concepts of homotopy classes of elliptic curves. Two curves in the same isomorphism class will have a finite distance between them. The distance of a curve from all the curves in an isomorphism class different than its own will be defined to be infinity. Fundamental group of elliptic curve over the $GF(2^5)$ is an equivalence relation defined as follows.

Let the isomorphic curves be:

$$y^2 + xy = x^3 + a_i x^2 + b_i, i = 1, 2 \text{ over } GF(2^5)$$

C_1 is said to be isomorphic toC_2over $GF(2^5)$ if there exist a $t \in GF(2^5)$ such that $a_2 = t^4 a_1$ and $b_2 = t^6 b_1$ [16].

Let $g$be a generator of the multiplicative group of the field $z \in GF(2^5)$.Then given any non-zero element in $GF(2^5)$, there exist an integer $k \in \{0, 1, 2 \dots 2^4\}$ such that $z = g^k$. We will refer to the set $\{0, 1, 2 \dots 2^4\}$ as an index of g. Note that index set of g is not unique. Any complete system of modulo the irreducible polynomial $x^5 + x^2 + 1$ can act as an index set. We are always using the index set $\{-2^4/2 + 1, -2^4/2 + 2, \cdots - 1, 0, 1, \dots 2^4/2\}$. We are calling this index set as standard index set of a generator g.

Let C_1 and C_2be any two curves over$GF(2^5)$. If C_1 and $C_2$are not isomorphic, we define the distance between them to be infinite. Otherwise, let $t \in GF(2^5)$ be a field element which transforms the parameters of C_1 to those of C_2(parameters of C_2 to those ofC_1). Let $t = g^r$, where $r$is in the standard index set of g. There will be several ts which define the same isomorphism. Let $t_1, \dots, t_l$ 'define' the same isomorphism. Write $t_i = g^{\alpha_i}$; $1 \le i \le l$.Chose that$t_i$for which α_i is minimum. Then we define the distance between C_1 and C_2 to be$|r|$that is

$$d_g(C_1, C_2) = |r| \text{ if } C_1 \text{ and } C_2 \text{ isomorphic and } t = g^r,$$
$$d_g(C_1, C_2) = \infty \text{ Otherwise.}$$

Now we claim that $d_g$as defined above is a metric. Clearly, $d_g \ge 0$. Also, if C_1 and C_2 are the same curve, then they are isomorphic and so $t = 1$ and $r = 0$. Hence it follows that $d_g(C_1, C_2) = 0$ if $C_1 = C_2$. Converse is clear and easy.

Next we will show that $d_g(C_1, C_2) = d_g(C_2, C_1)$.
If these curves are not isomorphic then there is nothing to prove as both of the distances are∞. So let us assume that they are isomorphic. Let $t = g^r$,be the element in $GF(2^5)$which transforms the parameters of C_1 to those of C_2(that is,$a_2 = t^4 a_1, b_2 = t^6 b_1$). Note that such r is not unique. If we force r to be in the standard index set then it is unique. Then $t^{-1} = g^{-r}$ transforms parameters of $C_2$to those ofC_1(that is, $a_1 = t^{-4} a_2, b_1 = t^{-6} b_2$). Hence $d_g(C_1, C_2) = |r|$and$d_g(C_1, C_2) = |-r|$, which are the same.

Finally we have to prove the triangular equality, that is, for any three curves $C_i, i = 1, 2, 3$; $d_g(C_1, C_2) + d_g(C_2, C_3) \ge d_g(C_1, C_3)$. Clearly ,this is obvious if $C_1$is not isomorphic toC_2 or$C_2$is not isomorphic to C_3. So let us assume that $C_1$is isomorphic toC_2 and C_2be isomorphic to C_3. Isomorphism is an equivalence relation, and thus $C_1$is isomorphic to C_3 Let $C_i : y^2 + xy = x^3 + a_i x^2 + b_i$,$i = 1, 2, 3$ then there exist $t_1, t_2 \in GF(2^5)$ and indices r_1, r_2in the standard index set of $g$such that

$$a_2 = t_1^4 a_1, \;\; b_2 = t_1^6 b_1 \;\; t_1 = g^{r_1} \text{ and}$$

$a_3 = t_1^4 a_2 \;\; b_3 = t_1^6 b_2 \;\; t_2 = g^{r_2}$ now,
$a_3 = (t_1 t_2)^4 a_1 \;\; b_3 = (t_1 t_2)^6 b_1$.
Let $t_1 t_2 = t_3 = g^{r_3}$. then $r_3 \equiv r_1 + r_2 (mod\, p-1)$. Hence $r_3 \leq r_1 + r_2$. We have now

$d_g(C_1, C_2) = |r_1|$,
$d_g(C_2, C_3) = |r_2|$,
$d_g(C_1, C_3) = |r_3|$,
Hence,$d_g(C_1, C_2) + d_g(C_2, C_3) \geq d_g(C_1, C_3)$.

This establishes triangular inequality. Hence, the new metric.

5. Conclution

During the point multiplication operation[17] with pre-computations, storing the pre-computed table in affine coordinates is considered insecure as it may lead to fixed table attacks[15]. To thwart such attacks, it is recommended to randomize the table each time a table entry is used in the computation. As point randomizing technique [13] requires the point to be in projective coordinates. With the concepts of distance, we can efficiently use the Joye-Tymen curve randomization technique[**?**] to defeat fixed table attacks. Each time we use a table entry in the computation we shift the computation to an isomorphic curve, only storing the distance d_i. After computing the scalar multiplication we can return back to the original curve by going back to the distance of $\sum d_i$. A traditional implementation needs storing of two parameters ,one curve parameter one defining the isomorphism; and a finite field multiplication for each isomorphism. The proposed metric allows us to use a pre-computed table in affine coordinates without much performance penalty.

References

[1] E.R. Berlekamp, *Algebraic Coding Theory*, NY, McGraw-Hill, 1968.

[2] I. Blake, G. Seroussi, N. Smart, *Elliptic Curves in Cryptography*, Cambridge University Press, 1999.

[3] P. Buhler, H.W. Lenstra, C. Pomerance, *The Development of the Number Field Sieve*, Lecture Notes in Computer Science, Springer-Verlag, **1554** (1994).

[4] W. Diffie, M.E. Hellman, New directions in cryptography, *IEEE Trans. On Information Theory*, **22** (1976), 644-654.

[5] D.M. Gordon, A survey of fast exponention methods, *J. Algorithms*, **27** (1998), 129-146.

[6] J. Guajardo, C. Paar, Efficient algorithms for elliptic curve crypto systems, *Advances in Cryptology-CYYPTO 97*, **1462** (1997), 342-356.

[7] Y. Han, P. Leong, P. Tan, J. Zhang, Fast algorithms for elliptic curve cryptosystems over binary finite field, *Advances in Cryptology-CRYPTO'99*, **1716** (1999), 75-85.

[8] T. Itoh, S. Tsujii, A fast algorithm for computing multiplication inverses in $GF(2^m)$ using normal bases, *Information &Computation*, **78** (1988), 171-177.

[9] T. Kobayashi, H. Morita, K. Kobayashi, F. Hoshino, Fast elliptic curve algorithm combining Frobenius map and table referenced to adapt to higher characteristic, *Adapt to Higher Charecteristic, Advances in Cryptology-CRYPTO'99*, **1592** (1999), 176-189.

[10] N. Koblitz, *A Course in Number Theory and Cryptography*, 2nd Eds., Springer-Verlag, 1994.

[11] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, 2nd Ed., Spinger-Verlag, 1993.

[12] N. Koblitz, Elliptic Curve Cryptosystems, *Math. Compu.*, **48**, No. 177 (1987), 203-209.

[13] J.S. Coron, Resistance against differential power analysis for elliptic curve cryptosystems, (1999) 292-302.

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

[15] T. Izu, B. Möller, T. Takagi, Improved elliptic curve multiplication methods resistant against side channel attacks, *Proceedings of Indocrypt 2002*, Springer-Verlag, Volume 2551 (2002), 296-313.

[16] J.H. Silverman, *The Arithmetic of Elliptic Curves*, Springer, 1986.

[17] P. Balasubramanian, E. Karthikeyan, Elliptic curve scalar multiplication algorithm using complementary recoding, *Applied Mathematics and Computation* (2007), 01-06.