A STUDY ON ARITHMETIC LOGIC IN ELLIPTIC CURVE CRYPTOSYSTEMS USING DISCRETE LOGARITHM PROBLEMS

[1]ANU PIUS, [2]SENTHILKUMAR B

[1]M.Phil Research Scholar, [2]Assistant Professor

PRIST University, Thanjavur

Abstract: ***This research introduces the arithmetic logic behind elliptic curve cryptography. We initially discuss on notion about asymmetric key cryptosystems, which depend on mathematical issues which require large time for computing. Elliptic curve cryptosystems frame illustrations of PKC'S and depend on DLP. We additionally treat certain hypothesis about elliptic curves, particularly the ones over limited fields. Especially to evade certain critical bouts against ECDL, distinctive focus were proposed on certain parameters. Finally, we depict general strategies to take after when outlining ECDL.***

Keywords: Cryptography; Discrete logarithm problem; Elliptic curves.

1 Introduction

Everyelement possesses two keys in asymmetric key cryptography, those are: symmetric and asymmetric key.These are associated in a uniqueway by single way function. Trapdoor functions are ease to compute but hard to invert. The cryptographic security protocol is associated to complex inversing. Thus, this complex issue must be estimated in relative of time required by computers to compute this problem. Complexity theory deal with this notion of complex algorithms. Identifying complex problems is a vital mission in cryptography and utilized in protocols as cryptographic elementary. RSA is one amongprotocolswhich hinged on complex computing of enormous numbers. There exist certain algorithms which require less time to compute those numbers. For highersecurity level, RSA is not suitable and one has to identify for other alternatives to invert complex functions. DLP over limited field is additional cryptographic primitive utilized in security protocols. But they present flaw and distinctivecare is essential in designing such problem. In elliptic curves, one builds discrete logarithm on set of point of curve. This research elucidates how to buildthose system leading to effectivesingle way function and to evade attacks and weakness. This work is built on abstract of results obtained in [5].

Definition 2.1(One-way functions) Let **k** is a security parameter and **n** be a function of **k**. Let **f** be $\mathbf{f}: \{\mathbf{0},\mathbf{1}\}^* \rightarrow \{\mathbf{0},\mathbf{1}\}^*$.Then **f** is a one-way function if

1. **f** is easy to compute. For all **n** and $\mathbf{x} \in \{\mathbf{0},\mathbf{1}\}^{\mathbf{n}}$, there exists a deterministic polynomial time algorithm $\mathbf{f}_{\alpha}$such that $\mathbf{f}_{\alpha}(x) = \mathbf{f(x)}$.
2. **f** is hard to invert. To all probabilistic polynomial time algorithms **A**,

   $\Pr\{x \leftarrow \{0,1\}^n, y = f(x), x^1 \leftarrow A(1^n, y) | f(x^1) = y\} < \frac{1}{2^k}$,

In addition to the one-way property of encryption function, we also require Charles, who possesses the symmetric key $\mathbf{s}_K$ to decrypt the message. So we allow the decryption to be possible using a trapdoor, secret information that allows to easily inversing encryption function. Such functions are called single-way trapdoor functions.

These one-way trapdoor functions are constructing blocks of modern cryptosystems built on computational number-theoretic assumptions such as DLPs and integer factorization.

2.2The Discrete Logarithm Problem

All PKC's we treat in this researchdepend on the complexity of DLP. We will now define this problem.

Let Hbe an abelian (additive) group, and $g \in H$. Now suppose that $h \in \langle g \rangle \subset H$.One can question ourselves which $k \in \mathbb{Z}$ satisfies the identity $kg = h$.Finding such a k is DLP. More general:

Definition 2.2.1 Given an abelian group $H$and$g, h \in H$, the problem of discovering a $k \in \mathbb{Z}\ such\ that\ kg = h$(if it exists) is called DLP. Such an integer $k$is termed a discrete logarithm of $h$to base g.

If we write the identity of DLP multiplicatively, it becomes $g^k = h$.In this notation, the use of the word logarithm is more clear. In other words, a discrete logarithm is uniquely determined modulo the order of base. Therefore, we visualize discrete logarithms as elements of $\mathbb{Z}$/n $\mathbb{Z}$. Following notation as in [14], we sometimes write log (h) for the discrete logarithm of h to base g, if it exists.

Example 2.2.2. Let Hbe the group Z/11Z*. We'll try to determine a discrete logarithm of $\overline{10}$ to the base $\overline{2}$ in Z/11Z. The apparentmethod to perform this is by noting down all powers of $\overline{2}$ in Z/11Z until we hit $\overline{10}$. Now

$\mathbf{\overline{2}^{-1}=\overline{2}, \overline{2}^{2}=\overline{4}, \overline{2}^{3}=\overline{8}, \overline{2}^{4}=\overline{5}, \overline{2}^{5} = \overline{10}}$

Hence $\log_{\overline{2}} \overline{10} = 5$ .Note that the discrete logarithm of $\overline{\mathbf{10}}$to base $\overline{\mathbf{4}}$ do not exist in Z/11Z, since $\overline{\mathbf{10}} \notin \langle\overline{4}\rangle$.

In the above example, the group structure is much stiff to hold at first sight. This makes the problem harder. Hence we may say that the DLP will only be difficult, if structure of the underlying group is complex at first sight. In this research, we focus on the groups of the form Z/nZ*, and on groups given by elliptic curves.

Here we consider the group of point of elliptic curve over finite field and the related DLP.

3 Elliptic curves

In this section we formally state the ECDLP. We recall the generic algorithms to computeECDLP in exponential time. We also give emphasis that the DLP is easy for certain types of curves which can be avoided by selecting appropriate elliptic curve parameters.
We know that DLP in circumstances of limited fields can computed in subexponential time utilizing the index calculus algorithm. Foremost objective of this research is to have a similar subexponential time algorithm for computing the ECDLP. ECDLP is transferred for computing a system of multivariate polynomial equations.

3.1 Elliptic Curve Definition

Definition 3.1.1 Let $\mathbb{K}$ be afield. An elliptic curve over $\mathbb{K}$is well-defined by a non-singular affine Weierstrass equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_5, \quad (A)$$

Where$a_i \in \mathbb{K}$.

By non-singular we mean the curve is smooth: $\frac{\partial E}{\partial x}$and $\frac{\partial E}{\partial y}$ do not vanish simultaneously. In other words

the system of equations

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_5.$$
$$a_1y - 3x^2 - 2a_2x - a_4 = 0$$
$$2y + a_1x + a_3 = 0$$

has no common solutions in $\bar{\mathbb{K}}$

By applying a change of coordinates, the elliptic curve E can be transformed into a short Weierstrass form.

Theorem 3.1.2Let E is the elliptic curve given in (A). Assume $\bar{E}$ is another elliptic curve given by

$\bar{E}: y^2 + \tilde{a_1}xy + \tilde{a_3}y = x^3 + \tilde{a_2}x^2 + \tilde{a_4}x + \tilde{a_5}$,Then E and $\bar{E}$ are said to be isomorphic over $\mathbb{K}$if there exists u,r,s,t $\in \mathbb{K}$such that the change of coordinates

$$(x, y) \rightarrow (u^2 x + r, u^3 y + u^2 sx + t)$$

transforms the curve E to $\bar{E}$.

Proof. See Chapter 3 Section 3 of [28]

Corollary 3.1.3(Short Weierstrass form) Assume char ($\mathbb{K}$) $\notin \{2,3\}$. Let E be an elliptic curve given by the Weierstrass equation as in (A). Then there exist a, b $\in \mathbb{K}$ such that the elliptic curve $\bar{E}$given by

$\bar{E} : y^2 = x^3 + ax + b$is isomorphic to E.

Proof. See Chapter 3 Section 1 of [13].

3.2 The Group Law

Let E be an elliptic curve over a field $\mathbb{K}$, with char ($\mathbb{K}$) $\notin \{2,3\}$.This section initially elucidates geometrically followed by algebraically, the group law on an elliptic curve.

One approach to defining the group law on an elliptic curve is to do so in projective space, and then to reduce to the affine case by taking the point at infinity to be the point $[0 : 1 : 0]$[9]. Instead we take this setup for granted and begin to define the group law in the affine setting, denoting the point at infinity as O. The group law can then be defined geometrically. Suppose $P_1$and P_2 are two points on an elliptic curve and we wish to determine $P_1 \oplus P_2$. We connect the points $P_1$and P_2 with a line l. This line l will intersect the curve at a third point, which we will denote P_3. We then connect P_3. with the point at infinity, which will simply be a vertical line, in this case, with the line l'. The line l' will then intersect the curve E in a third point as well. It is this point that we will denote as $P_1 \oplus P_2$, the sum of P_1 and P_2 on E. Later, we will drop the $\oplus$ notation in favor of + where there should be no confusion. From this type of geometric construction we can immediately see how to define things algebraically.

Theorem 3.2.1(The Group Law) Let E be an elliptic curve over $\mathbb{K}$ with char ($\mathbb{K}$) $\notin \{2,3\}$,with defining equation $E : y^2 = x^3 + Ax + B$. Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be points on E such that $P_1, P_2 \neq O$. We define $P_1 + P_2 = P3 = (x_3, y_3)$as follows.

1. If $x_1 \neq x_2$ then $x_3 = m^2 - x_1 - x_2$, $y_3 = m(x_1 - x_3) - y_1$ where $m = \frac{y_2 - y_1}{x_2 - x_1}$
2. If $x_1 = x_2$ but $y_1 \neq y_2$, then $P_1 + P_2 = O$
3. If $P_1 = P_2$ and $y_1 \neq 0$, then $x_3 = m^2 - 2x_1, y_3 = m(x_1 - x_3) - y_1$ where $m = \frac{3x_1^2 + A}{2y_1}$

4.if $P_1 = P_2$ and $y_1 = 0$ then $P_1 + P_2 = O$.

Notice that we did not take into accounts that P_1 or P_2 could in fact be the point at infinity here. Doing so results in several special cases which we omit but can be found in a variety of sources including [7], [8], [15] and [19]. We can also define the group law algebraically over fields of characteristic 2 and 3; however we do not do it here. Excellent sources for these definitions are [7], [8] and [15, Appendix A].

Regardless of the field of definition, and including all special cases for points on E, we now have a group which satisfies the following properties.

Theorem 3.2.2 The addition law defined above on an elliptic curve E gives E the structure of an Abelian Group. We will denote the identity element as O, and the inverse of point P as -P.

Proof: proof can be found in [12].

Theorem 3.2.3 (Bezout's Theorem) Let C_1 and C_2 be two projective curves well-defined over C of degrees m and n which share common component. Then sum of intersection numbers, counting multiplicities, at point of intersection P is mn. See[12]for definition of intersection number.

3.3 Elliptic Curves Over Finite Fields

The above section is a general construction; the group law applies to elliptic curves over all fields. Since we are concerned with cryptographic applications, we will primarily deal with elliptic curves over limited fields. One still agree to same convention that O is point at infinity and is identity element for groups. When theory of elliptic curves over Q is fully developed, one translates all constructions with ease to a finite field F_q, for some $prime\ q\ or\ q = p^n\ for\ some\ n \in \mathbb{Z}$.

4The Elliptic Curve Discrete Logarithm Problem (ECDLP)

Elliptic curves were introduced for cryptography by Koblitz [17] and Miller [24], these curves defined over finite fields have become a substitute in description of asymmetric key cryptosystems which are adjacent analogs of existing schemes such as Diffie-Hellman Key

exchange schemes [32],[1] and digital signature algorithms [2], [25]. Their applications range to primality testing and integer factorization [22],[21].

Elliptic curves are good choices for design of cryptosystems mainly because they offer relatively small key sizes [20] and more efficient computations [6]. More importantly the ECDLP, which is the heart of the security of these cryptosystems, has no known sub exponential attack in general.

Definition 4.1. (ECDLP) Consider an elliptic curve E well-defined over a field $\mathbb{K}$. Let $P \in E$ be a point having order $and\ let\ Q \in E$. The elliptic curve discrete problem is to find $\beta, if\ it\ exists\ such$ that Q = [β] P.

The ECDLP is accepted to be a hard computational issue for a fitting size of parameters. Anyway there are some known assaults which could be effectively dodged. The majority of the assaults exchange the ECDLP to some other gathering where the DLP is simple. For instance, the Weil plunge and the GHS at¬tacks [10], [11] exchange the DLP for elliptic bends characterized over paired expansion fields to DLP for hyper elliptic bends, where subexponential calculations to take care of the discrete logarithm issue exist [16].In what tails we center around assaults that exchange the ECDLP to the DLP over limited field augmentations. We additionally feature that a large portion of the calculations are not ready to comprehend the ECDLP in subexponential time. The expectation is to build up a list math calculation to illuminate the ECDLP like the case it unravels the DLP over limited fields and their augmentations in subexponential time.

4.2 Point Counting

We are identifying for sets of order of large prime divisor. This was the exact main significance of speed of point counting playing a vital role in designing elliptic curve DLP. The computation of the order of a group for curves $C\ of\ genus\ g$defined over fields$F_q$can be performed efficiently by not too complicated algorithms if

- The curve C is already defined over a small subfield $F_{q0}$of F_q[27] [30] [26] or
- The genus $g\ is\ equal\ to$ 1, [3] [4] [9] or
- The characteristic of $F_q$is small, [23] or
- The genus of $C\ is$ 1 or 2, the field F_qFqis a prime field, and the curve C is the reduction modulo q of a curve C $w$ith complex multiplication over a given order $EndC$ in a CM-field. Here is the algorithm [29]

4.3 Elliptic Curve Cryptography

We realize that Diffie-Hellman key trade, and the ElGamal cryptosystem are cases of PKC's. To characterize these frameworks, we have utilized the gatherings F∗p. It isn't unpredictable to imagine that we additionally could have utilized an option limited abelian gatherings. Here, we will inspect how Diffie-Hellman key trade and the ElGamal cryptosystem work, when we utilize an elliptic bend. We consider just elliptic bends past constrained fields of trademark greater than 3.

4.4 Diffie-Hellman and ElGamal over elliptic curve groups

Bob and Alice want to exchange an encryption key of some symmetric encryption scheme. To do this safely, they choose an elliptic curve E/F_q, and they pick a point $P \in E(F_q)$ of order n. Alice then picks $1 < a < n$ and computes $A = [a]^P$ Here number a remains secret, and A is made asymmetric. Bob also picks some secret number $1 < b < n$, and determines a asymmetric point $B = [b]^P$. Now both Bob and Alice can determine $K = [b]A = [a]B$, and they use this point as encryption key.

Adjusting the cryptosystem is also not too hard. Bob and Alice wish to communicate. They first settle on an elliptic curve E/F_q, and pick some point P on this curve of order n. Alice picks her secret key $1 < a < n$, and determines the asymmetric key $A = [a]^P$. Bob has a message M $\in E(F_q)$. He then chooses $1 < k < n$, and computes $C_1 = [k]P\ and\ C_2 = M + [k]A$. He sends ($C_1$,$C_2$) to Alice. She can recover messages by solving

$C_2 - [a]C_1 = M + [k]A - [a][k]P = M$

4.5 Security Of PKC's Based On Elliptic Curves

Like before, it is clear that if someone can solve arbitrary DLPs on elliptic curve groups in reasonable time, he can easily crack Diffie-Hellman and ElGamal defined over elliptic curve groups.

For groups F^*_p, there exists an algorithm based on index calculus that has only subexponential running time. According to [18], it is not known whether elliptic curve groups also allow something like index calculus. Hence, at this time, for arbitrary elliptic curves, the best known general algorithm takes exponential time.

However, we still have to be careful. There do exist some algorithms, that solve the DLP rather fast for special elliptic curves. Hence, in order to keep communication secure, we have to stay away from these special cases.

An example of this is the SSSA-algorithm. When an elliptic curve E(F_q) consists of exactly q points, this algorithm solves a DLP on the group defined by E in polynomial time. Such elliptic curves are called anomalous. We will not treat this algorithm in this thesis, but we refer to [31] for a detailed explanation of the SSSA-algorithm when q is prime number.

Another algorithm that speeds up solving the DLP on certain elliptic curves is the MOV-algorithm. It's running time is subexponential when the elliptic curve on which we work is supersingular. The discoveries of these algorithms have shown that we have to be careful in choosing elliptic curves for cryptographic purposes. We should not consider anomalous nor super singular elliptic curves. According to [18], these are until now the only known dangerous classes of elliptic curves when it comes to cryptography.

5 Conclusion.

In this research work, Public key cryptosystems based on elliptic curve groups was examined, also called *elliptic curve cryptosystems* are remarkably secure. Till now, there are no other alternative algorithms which solves a random DLP on a random elliptic curve group in polynomial or subexponential time. Thus, set size must essential be kept relatively small, and making elliptic curve cryptosystems useful for small communication devices. However, we still have to be careful. Not every elliptic can be used for cryptographic purposes. We have to rule out super singular and anomalous elliptic curves. For these classes of curves, there exists relatively fast algorithms for solving the DLP, namely the *MOV-algorithm* and the *SSSA-algorithm* respectively. But if we stay away from these cases, elliptic curve cryptography is a secure way of encrypting messages

References

[1] ANSI X9.63-199x. Public Key Cryptography for the Financial Services Industry: Elliptic Curve Key Agreement and Transport Protocols, 1997.

[2] ANSI X9.62-199x. Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), 1998.

[3] A.O.L. Atkin, The number of points on an elliptic curve modulo a prime, E-mail on the Number Theory Mailing List, (1988).
[4] A.O.L. Atkin, The number of points on an elliptic curve modulo a prime, E-mail on the Number Theory Mailing List, (1991), 414-415.
[5] R. Avanzi, C. Doche, T. Lange, K. Nguyen and F. Vercauteren, *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, Chapman, (2006).
[6] D. Bernstein, T. Lange. ECRYPT Benchmarking of Cryptographic Systems. http://bench.cr.yp.to, 2013.
[7] I. F. Blake, G. Seroussi, and N. P. Smart. Elliptic curves in cryptography, volume 265 of London Mathematical Society Lecture Note Series. Cambridge University Press, Cambridge, 2000. Reprint of the 1999 original.
[8] Darrel Hankerson, Alfred Menezes, and Scott Vanstone. Guide to elliptic curve cryptography. Springer Professional Computing. Springer-Verlag, New York, 2004.
[9] N.D. Elkies, Explicite isogenics, Draft, (1991).
[10] S. Galbraith, F. Hess, N. Smart. Extending the GHS Weil descent attack. In Advances in cryptology–EUROCRYPT'02, vol. 2332 of LNCS, pages 29–44, 2002.
[11] S. Galbraith, N. Smart. A cryptographic application of Weildescent. In Cryptography and coding, vol. 1746 of LNCS, pages 191–200, 1999.
[12] C. G. Gibson. Elementary geometry of algebraic curves: an undergraduate introduction. Cambridge University Press, Cambridge, 1998.
[13] D. Hankerson, S. Vanstone, A. Menezes. Guide to elliptic curve cryptography. Springer Science and Business Media, 2004.
[14] J. Hoffstein, J. Pipher, and J. H. Silverman. An introduction to mathematical cryptography. Springer-Verlag, New York, 2008.
[15] Joseph H. Silverman. The arithmetic of elliptic curves, volume 106 of Graduate Texts in Mathematics. Springer-Verlag, New York, 1986.
[16] M. Jacobson, A. Menezes, A. Stein. Solving elliptic curve discrete logarithm problems using Weil descent. Journal Ramanujan Mathematical Society, vol. 16(3), pages 231–260, 2001.
[17] N. Koblitz. Elliptic curve cryptosystems. Mathematics of Computation, vol. 48(177), pages 203– 209, 1987.
[18] N. Koblitz, A. Menezes, and S. Vanstone. The state of elliptic curve cryptography. Designs, Codes and Cryptography, 19:173–193, 2000.
[19] Lawrence C. Washington. Elliptic curves. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2003. Number theory and cryptography.
[20] A. Lenstra, E. Verheul. Selecting cryptographic key sizes. Journal of Cryptology, vol. 14(4), pages 255–293, 2001.
[21] H. Lenstra. Factoring integers with elliptic curves. Annuals of Mathematics, vol. 126, pages 649– 673, 1987.
[22] A. Menezes. Elliptic Curve Public Key Cryptosystems. Kluwer Academic Publishers, 1993.
[23] J.F. Mestre, Lettre adressee a Gaudry et Harley, www.math.jussieu.fr/ mestre, (2000).
[24] V. Miller. Use of elliptic curves in cryptography. Advances in cryptology–CRYPTO 85, vol. 218 of LNCS, pages 417–426, 1986.
[25] National Institute for Standards and Technology. Digital signature standard, FIPS PUB 186, 1994.
[26] D. Shanks, Class number: A theory of factorization and generalization, Proc. Symp. Math., 20(1971), 415-440.
[27] V. Shoup, Lower bounds for discrete logarithms and related problems, Advences in Crryptology, 1233(1997), 256-266.
[28] J. Silverman. The Arithmetic of Elliptic Curves. GTM vol. 106, 1986. Expanded 2nd Edition, 2009.
[29] A.M. Spallek, Kurven vom Geschlecht 2 und ihre Anwendung in Asymmetric-key Kryptosystemen, Universitat Gesamthchhschule Essen, PhD. Thesis, (1994).
[30] S. Pohlig and M. Hellmann, An improvement algorithm for computing logarithms over GF(p) and its cryptographic signifiance, IEEE Tran. Inform. Theory, 24(1978), 106-110.
[31] A. Werner. Elliptische Kurven in der Kryptographie. Springer-Verlag, Berlin, 2002.
[32] W. Diffie, M. Hellman. New directions in cryptography. IEEE Trans. Information Theory, vol. IT-22(6), pages 644-654, 1976.