Alex Lafnitzegger

8 – 12 – 13

**Elliptic Curve Based Cryptology**

1. *Abstract*

I intend to go over the use of mathematics in cryptology, focusing specifically on the use of elliptic curves. This is mostly because this seems the most interesting method of cryptography, but it also seems to employ material that relates well to the multivariable mathematics we are discussing in class. However I would hardly say it’s a direct application of the topics we’ve covered, it’s simply in the same sort of scope with regards to multivariable operations. In addition to this, I think it might be wise to go over the underlying mathematical concepts that contribute to this school of cryptology, such as the Discrete Logarithmic Problem, Cyclical Groups, Public Key Algorithms and Modular Arithmetic.

1. *Introduction*

Cryptology dates back to as early as 2000 BC, where little complex math was used (or needed for that matter) and the majority of encryption methods were either basic or analog. However, with the advent of digital information, messages of greater length can be encrypted with great complexity with technological assistance to speed up the process. But at the same time, encryptions methods need to be complex enough that a message can’t easily be broken by a system not meant to receive it. One such complex means of encryption is the use of an elliptical curve, mapping information of a message into the points of the curve and placing these points into cyclical subgroups in particular. Throughout the course of this report, I will build up a foundation to explain how this process works.

1. *Background*

First of all and most basically, we must define what a group is so that we may create our own operators later on.

Definition iii.1: *A* group *is a set of elements G together with an operation ○ which combines two elements of G. A group has the following properties:*

1. *The group operation ○ is* closed. *That is, for all a,b* $\in $ *G, it holds that a○b = c* $\in $ *G.*
2. *The group operation is* associative. *That is, a○(b○c) = (a○b)○c for all a,b,c* $\in $ *G.*
3. *There is an element* 1 $\in $ *G called the* neutral element *(or* identity element*), such that a ○ 1 = 1 ○ a = a for all a* $\in $ *G.*
4. *For each a* $\in $ *G there exists an element a*-1 $\in $ *G, called the* inverse *of a, such that a ○ a*-1 = *a*-1 *○ a =* 1.
5. *A group G is* abelian *(or* commutative) *if, furthermore, a ○ b = b ○ a for all a,b* $\in $ *G.*

The most basic example of a group would then be the set of all real numbers, with two basic operations inside this group being addition and multiplication. The neutral elements of these two operations are clearly 0 and 1, respectively, both of which are contained in the set of all real numbers. However, for what we will be doing with elliptic curves, we will need to create different operators that will ensure the legitimacy of the curve acting as a group itself.

Modular arithmetic is what is learned as ‘clock arithmetic’. Here, we will interpret it colloquially as a value that can be converted into a another similar value in a subset of its universe of discourse. More specifically as it applies to numbers. The operation is referred to as the modulo, is represented by ‘mod’ in equations, and follows the following definition:

Definition iii.2: *Let a, r, m* $\in $***Z*** *(where* ***Z*** *is the set of all integers) and m > 0. We write*

$$a ≡r mod m$$

*if m divides a – r.*

*m is called the* modulus *and r is called the* remainder.

For example in the use of this operator, we can see that 6 $≡$ 2 mod 4 since 6 – 2 = 4 which is divisible by the modulus 4. Similarly, 10 $≡$ 2 mod 4 since 8 is divisible by 4 as well. This operator also applies to negative integers.

Finally, we shall combine both the concept of groups and modular arithmetic to establish a solid idea of finite groups as they will pertain to cryptology.

Definition iii.3: *A group (G, ○) is* finite *if it has a finite number of elements. We denote the* cardinality *or* order *of the group G by* |*G*|.

Simply put, one can take |G| to be the number of elements in G. It’s also important to note:

Definition iii.4: *The* order *ord(a) of an element a of a group (G, ○) is the smallest positive integer k such that*

$$a^{k}=a○a○\cdots ○a=1;a occurs k times$$

*where* 1 *is the identity element of G.*

For an example of this in tandem with the modulo, I first need to establish a bit of notation. The set $Z\_{n}^{\*}$is the set of all integers smaller than and relatively prime to *n*. An integer *a* is relatively prime to another *b* if *a* and *b* do not share any prime factors. However, we will be using prime values for *n* so we need not worry ourselves with the intricacies of relative primes.Now, in this example, we are looking for ord(*a*) where *a* = 3 for the group $Z\_{11}^{\*}$:

 *a*1 = 3

 *a*2 = *a ∙ a =* 3 *∙* 3 = 9

 *a*3 = *a*2 *∙ a* = 9 *∙* 3 = 27 $≡$5 mod 11

 *a*4 = *a*3 *∙ a* = 5 *∙* 3 = 15 $≡$4 mod 11

 *a*5 = *a*4 *∙ a* = 4 *∙* 3 = 12 $≡$1 mod 11

By this example, ord(3) = 5, but if the series of equations were to continue, one would notice a pattern where the powers of a run through the sequence {3,9,5,4,1}. Thus, by our modulo operation, we have formed a cyclic group from our finite group.

Definition iii.5: *A group G which contains an element α with a maximum order ord(α) =* |*G*| *is said to be* cyclic. *Elements with maximum order are called* primitive elements *or* generators.

These cyclic finite groups form the basis of discrete logarithmic problems as they pertain to cryptology since it limits a set of elliptic curve points, but more importantly, it contributes to the idea of the Discrete Logarithmic Problem, a predominant topic and issue that crops up in modern computational cryptology.

The Discrete Logarithmic Problem in $Z\_{p}^{\*}$ is defined as such:

Definition iii.6: *Given is the finite cyclic group* $Z\_{p}^{\*}$ *of order p –* 1 *and a primitive element α* $\in Z\_{p}^{\*}$ *and another element β* $\in Z\_{p}^{\*}$*. The Discrete Logarithmic Problem is the problem of finding an integer* 1 ≤ *x ≤ p –* 1 *such that:*

$$α^{x}≡β mod p$$

This is obviously an issue in computation but it can also be trouble with computers ill-equipped to handle potentially high values of *αx*, depending on the values of *β* and *p* of course. However, setting up an encryption in this manner can be of great help as well since it means that same encryption is that difficult to crack.

Finally, we need to familiarize ourselves with the concept of asymmetric cryptology, if only briefly. For the following explanation, the means by which messages are encoded and decoded (not necessarily both) will be referred to as keys. In asymmetric cryptology, there are (at least) two keys, one of which is defined as the private key. All others are public keys. In this case, public keys provide people with the means of encoding a message, but no message can be properly decoded without the private key, possessed by those with the authority to receive the message. As an example, think of a public mailbox. The public key is the slot through into which a person might insert a letter. Because of the way mailboxes are built, once the letter is inserted, it is extremely difficult to retrieve it, unless of course you possess the key to the box. Then it is a simple task of retrieving letters and delivering them, but only the local mailmen possess the ability to retrieve these letters, so their literal keys would be the private keys of asymmetric cryptology. This will be important to remember later at the end of the elliptical curve encryption process.

1. *Elliptic Curve Cryptology*

First, we must establish what an elliptic curve refers to.

Definition iv.1: *The* elliptic curve *over* ***Z****p, p >* 3, *is the set of pairs (x,y)* $\in $***Z****p which fulfill*

$$y^{2}≡x^{3}+a∙x+b mod p$$

*together with an imaginary* point of infinity *O, where*

$$a,b\in Z\_{p}$$

*and the condition* 4*∙ a*3 + 27 *∙ b*2 ≠ 0 mod *p.*

Typically, the elliptic curve should appear to be of a shape described by Figure 1.

Figure 1:



The elliptic curve also has its own operations as a group, addition and, as a byproduct, multiplication with the act of doubling being a special case. However, these operators are simply named this manner and do not resemble the operators of standard mathematics. Each variable in this group is a point (x,y) on the elliptic curve so the operators must produce a point also on the curve. To do this, addition takes two points (x1,y1) and (x2,y2) on the curve, draws a straight line between them and receives a third point of intersection on the curve (which is typical given the shape of most elliptical curves). This point, let’s call it (x3,y3), is the reflection of the operators sum across the x-axis, indicating that the sum of (x1,y1) and (x2,y2) is (-x3,y3). By comparison, when doubling a single point, you take the tangent line of that point as the line of intersection. Then you follow a similar system as addition, where the reflection of the next intersection point is the product of the operator. A visual representation of addition and doubling can be seen in Figures 2 and 3 respectively.

Figure 2: 

Figure 3:



Most cryptosystems, however, are incapable of geometric constructions, but luckily, relatively simple mathematical expressions exist that allow points to be added together and doubled computationally:

$$x\_{3}=s^{2}-x\_{1}-x\_{2} mod p$$

$$y\_{3}=s\left(x\_{1}-x\_{3}\right)-y\_{1} mod p$$

where

$$s=\left\{\begin{array}{c}\frac{y\_{2}-y\_{1}}{x\_{2}-x\_{1}} mod p;if \left(x\_{1},y\_{1}\right)\ne (x\_{2},y\_{2})\\\frac{3x\_{1}^{2}+a}{2y\_{1}} mod p;if \left(x\_{1},y\_{1}\right)=(x\_{2},y\_{2})\end{array}\right.$$

The first case refers to point addition, the second refers to doubling. The *a* in the second case refers to the coefficient used in the formula for the elliptical curve. Finally, we use *O* as the groups neutral element. Now, with the way elliptic curves are set up, it is possible to set up a cyclic group comprised of all points on the curve based on the following theorem:

Theorem 1: *the points on an elliptic curve together with O have cyclic subgroups. Under certain conditions all points on an elliptic curve form a cyclic group.*

Now, since a cyclic group is contained in the elliptic curve, a discrete logarithm can be set up for the purpose of using the points for encryption. First, some notation given by Hasse’s Theorem.

Hasse’s Theorem: *Given an elliptic curve E modulo p, the number of points on the elliptic curve is denoted by #E and is bounded by:*

$$p+1-2\sqrt{p} \leq \#E \leq p+1+2\sqrt{p}$$

So, to form an Elliptic Curve Discrete Logarithmic Problem we just need to work with the following.

Definition iv.2: *Given is an elliptic curve E. We consider a primitive element P and another element T. The* Elliptic Curved Discrete Logarithm Problem *is finding the integer d, where* 1≤*d*≤#E, such that:

$$P+P+…+P=dP=T;P is repeated d times$$

In this case, *T* would be used as a the public key, the point from which anyone may create a message, where *d*, as an integer determining where the primitive is, is used as the private key. Due to the nature of the system, someone with no prior knowledge of the private key would have a difficult time determining where P since multiple combinations of elements in the curve can share specific results.

1. *Possibilities and Conclusion*

Branching off from this, since elliptical curves are among the more complex of the various algorithms used in cryptology, I suppose one could study further cryptological concepts. I would have a basic grasp of some fragment of cryptology and could easily use that to try and understand other means of encryption. Or, this could make a good lead into the securities of security systems, though I’d hardly call that a school of math. It’s more a subset of computer science. However, given the use of special curves and geometry here, I imagine the field of topology, if it were used in a case like this, could yield incredibly complex encryption algorithms. Perhaps too complicated for common computers to handle, and likely there would be too much information and calculations for a human brain with no time to do so. Still, in an age of rapid technological advance, complex systems as this may one day be considered basic in comparison to a newer system that a computer may be able to run. Besides, I have it on good authority that the original idea for elliptical curve based cryptology partially belongs to Neal Koblitz, one of the current staff at the UW. So this is likely to be a legitimate academic field of study in mathematics.

Bibliography

Nikooghadam, Morteza, Ali Zakerolhosseini, and Mohsen Ebrahimi Moghaddam. “Efficient utilization of elliptic curve cryptosystem for hierarchical access control”. *Journal of Systems and Software*, Oct. 2010: 1917-1929. *Science Direct*. Web. 20 Aug. 2013.

Paar, Christof, and Jan Pelzl. *Understanding Cryptography*. New York: Springer, 2011. Print.

Schneier, Bruce. *Applied Cryptography*. 2nd ed. Hoboken, NJ: Wiley, 1996. Print.

“Elliptic curve.” *Wikipedia: The Free Encyclopedia*. Wikimedia Foundation, Inc. 22 July 2004. Web. 20 Aug. 2013.