ELLIPTIC CURVES AND CRYPTOGRAPHY

DANIEL KLINE

Abstract. This paper establishes a thorough definition for elliptic curves, establishes that the points on an elliptic curve form a group under addition, and explores how and why elliptic curves are used in cryptography.

Contents

1. Elliptic Curves

Before we can define an elliptic curve, we need to introduce some important notation and concepts.

Let K be a field and $\overline{K}$ be the algebraic closure of K.

Definition 1.1. The *affine n-space (over K)* is the set of n-tuples over $\overline{K}$. It is denoted as

$$\mathbb{A}^n = \mathbb{A}^n(\overline{K}) = \{(x_1, ..., x_n) \mid x_i \in \overline{K}\}.$$

Definition 1.2. Let $(x_1, ..., x_{n+1}), (y_1, ..., y_{n+1}) \in \mathbb{A}^{n+1} \setminus 0$. Consider the equivalence relation where $(x_1, ..., x_{n+1}) \sim (y_1, ..., y_{n+1})$ if there exists $\lambda \in \overline{K}^\times$ such that $x_i = \lambda y_i$ for all i. We denote this equivalence class as

$$[x_1, ..., x_{n+1}] = \{(\lambda x_1, ..., \lambda x_{n+1}) \mid \lambda \in \overline{K}^\times\}.$$

We say that $x_1, ..., x_{n+1}$ are the *homogenous coordinates* of the equivalence class. We call the set of these equivalence classes the *projective n-space (over K)*. We denote this as

$$\mathbb{P}^n = \mathbb{P}^n(\overline{K}) = \{[x_1, ..., x_{n+1}] \mid (x_1, ..., x_{n+1}) \in \mathbb{A}^{n+1} \setminus 0\}.$$

Date: AUGUST 29, 2016.

Definition 1.3. A *Weierstrass equation* is an equation of the following form:

$$Y^2Z = X^3 + aXZ^2 + bZ^3,$$

where $a, b \in K$ for some field K with $\text{char}(K) \neq 2, 3$.

Let's look at the solutions of a Weierstrass equation in projective space $\mathbb{P}^2$.

Proposition 1.4. *Let*

$$f(X, Y, Z) = Y^2Z - (X^3 + aXZ^2 + bZ^3).$$

(i) *If $(x_1, x_2, x_3) \in \mathbb{A}^3 \setminus 0$ is a solution of f, then every element of the equivalence class $[x_1, x_2, x_3] \in \mathbb{P}^2$ is a solution.*
(ii) *If (x_1, x_2, x_3) is not a solution of f, then every element of the equivalence class $[x_1, x_2, x_3]$ is not a solution of f.*

Proof. (i) Let $(x_1, x_2, x_3) \in \mathbb{A}^3 \setminus 0$ such that $f(x_1, x_2, x_3) = 0$. Let $\lambda \in \overline{K}^\times$. Then,

$$\begin{aligned} f(\lambda x_1, \lambda x_2, \lambda x_3) &= \lambda^3(f(x_1, x_2, x_3)). \\ &= \lambda^3 \cdot 0. \\ &= 0. \end{aligned}$$

Therefore, for all $\lambda \in \overline{K}^\times$, $f(\lambda x_1, \lambda x_2, \lambda x_3) = 0$.

(ii) Let $(x_1, x_2, x_3) \in \mathbb{A}^3 \setminus 0$ such that $f(x_1, x_2, x_3) \neq 0$. Let $\lambda \in \overline{K}^\times$. Then,

$$f(\lambda x_1, \lambda x_2, \lambda x_3) = \lambda^3(f(x_1, x_2, x_3)).$$

Because λ is a unit, λ^3 is a unit, which implies it is not a zero divisor. So, $f(x_1, x_2, x_3) \neq 0 \implies \lambda^3(f(x_1, x_2, x_3)) \neq 0$. Therefore, for all $\lambda \in \overline{K}^\times$, $f(\lambda x_1, \lambda x_2, \lambda x_3) \neq 0$.

□

Remark 1.5. In a Weierstrass equation, if $Z = 0$, then $X^3 = 0$. Since K is a field, this implies $X = 0$. Then, for any value $Y \in \overline{K}$, $(0, Y, 0)$ is a solution to this equation. So, the only element of $\mathbb{P}^2$ that is a solution to a Weierstrass equation and has a Z coordinate of 0 is $[0, 1, 0]$.

All other solutions to a Weierstrass equation, i.e. when $Z \neq 0$, are of the form $[X, Y, 1]$, where $X, Y \in \overline{K}$. So, for ease of notation, the solutions to a Weierstrass equation in $\mathbb{P}^2$ can be viewed as the set of solutions $(x, y) \in \mathbb{A}^2$ of the equation

$$y^2 = x^3 + ax + b$$

along with the point $[0, 1, 0]$. The point $[0, 1, 0]$ is considered to be a point at infinity i.e. a point that is on every vertical line in $\mathbb{A}^2$.

Definition 1.6. The *discriminant* of a Weierstrass equation is defined as

$$\Delta = 4a^3 + 27b^2.$$

Let's look at some examples of Weierstrass equations.

Examples 1.7. The set of real solutions of a Weierstrass equation can be displayed graphically. Here are a few examples:

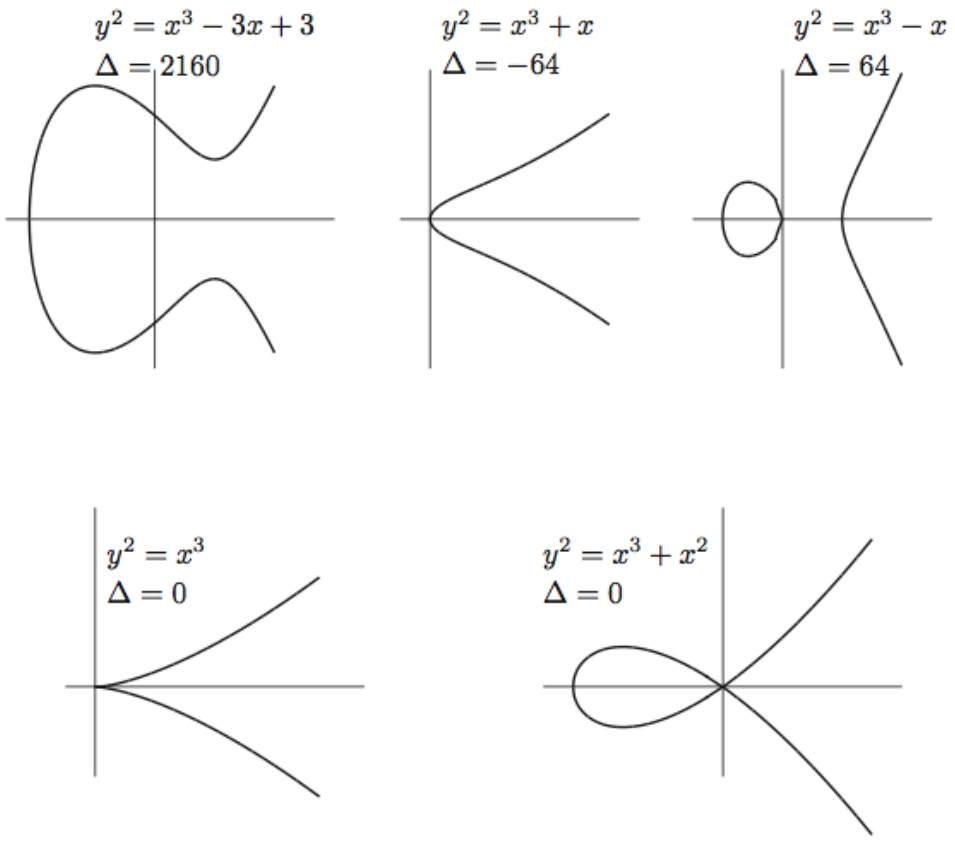

FIGURE 1. Examples of elliptic curves (This figure is from [1])

Noticeably, of the Weierstrass equations above, the equations in the first row have non-zero discriminants and the equations in the second row have zero discriminants. Furthermore, the graph of the equation $y^2 = x^3$ has a sharp point called a cusp and the graph of the equation $y^2 = x^3 + x^2$ intersects itself at a point. In other words, both of the equations in the second row have a point that does not have a well-defined tangent line. We call such equations *singular*. Equations like those in the first row that do not have such points are called *non-singular*. We now make this idea precise.

Definition 1.8. Let $S \subset \mathbb{P}^{n+1}$ be the set of solutions to a nonconstant, homogenous polynomial

$$f(X_1, ..., X_n) = 0.$$

The point $P \in S$ is a *singular point* if

$$\frac{\partial f}{\partial X_1}(P) = ... = \frac{\partial f}{\partial X_n}(P) = 0.$$

The set S is *singular* if there exists a singular point $P \in S$. Otherwise, we call S *non-singular* and f a *non-singular equation.*

Remark 1.9. Noticeably, the point at infinity $[0, 1, 0]$ is never a singular point. To see this, we need to look at a Weierstrass equation of the form:

$$f(X, Y, Z) = Y^2Z - (X^3 + aXZ^2 + bZ^3) = 0.$$

Then,

$$\frac{\partial f}{\partial Z} = Y^2 + (2aXZ + 3bZ^2).$$
$$\frac{\partial f}{\partial Z}([0, 1, 0]) = 1 \neq 0.$$

Therefore, $[0, 1, 0]$ is not a singular point. So, the only possible singular points are the solutions $(x, y) \in \mathbb{A}^2$ of the simplified Weierstrass equation:

$$f(x, y) = y^2 - (x^3 + ax + b) = 0.$$

Theorem 1.10. *Let S be the set of solutions of a Weierstrass equation $f(x, y) = y^2 - (x^3 + ax + b)$ and Δ be the discriminant of this Weierstrass equation. The set S is singular if and only if $\Delta = 0$*

Proof. (i) First, we will show that if S is singular, then $\Delta = 0$. Suppose S is singular at the point $P_0 = (x_0, y_0)$. Then,

$$f(x_0, y_0) = y_0^2 - (x_0^3 + ax_0 + b) = 0.$$
$$\frac{\partial f}{\partial x}(x_0, y_0) = -(3x_0^2 + a) = 0 \implies a = -3x_0^2.$$
$$\frac{\partial f}{\partial y}(x_0, y_0) = 2y_0 = 0 \implies y_0 = 0.$$

The first and second line above imply $b = 2x_0^3$. By 1.6,

$$\Delta = 4a^3 + 27b^2 = 4(-3x_0^2)^3 + 27(2x_0^3)^2 = 0.$$

(ii) Now, we will show that if $\Delta = 0$, then S is singular. The discriminant $\Delta = 0$ if and only if the cubic $x^3 + ax + b$ has a double root x_0. The value x_0 is a double root if and only if it is a root of $x^3 + ax + b$ and its derivative $3x^2 + a$. Then,

$$f(x_0, 0) = 0^2 - (x_0^3 + ax_0 + b) = 0.$$
$$\frac{\partial f}{\partial x}(x_0, 0) = -(3x_0^2 + a) = 0.$$
$$\frac{\partial f}{\partial y}(x_0, 0) = 2(0) = 0.$$

Therefore, $(x_0, 0)$ is a singular point and S is singular.

□

Now, we are ready to define an elliptic curve.

Definition 1.11. Let E be the union of the two following:

(i) the set of solutions to a non-singular Weierstrass equation of the form
$$y^2 = x^3 + ax + b$$
so that $\Delta = 4a^3 + 27b^2 \neq 0$

(ii) a point at infinity which we will call $\mathscr{O}$

E is an *elliptic curve*.

Remark 1.12. We use the notation E/K when we want to communicate that the associated Weierstrass equation has coefficients in K. We use the notation $E(K)$ for the set of points on E with coordinates in K along with the point at infinity $\mathscr{O}$.

2. The Additive Group of an Elliptic Curve

The points on an elliptic curve are naturally an additive group, which we will explore in this section. First, we define the binary operation "addition" on the points of an elliptic curve.

Definition 2.1 (Additive Law of Elliptic Curves)**.** Let E be an elliptic curve and $P, Q \in E$. Let L be the line through the points P and Q (if $P = Q$, then L is the line tangent to the Weierstrass equation of E at the point P)[1]. L intersects E at a third point[2] R. Let L' be the line through $\mathscr{O}$ and R. L' intersects E at a third point which we call $P \oplus Q$.

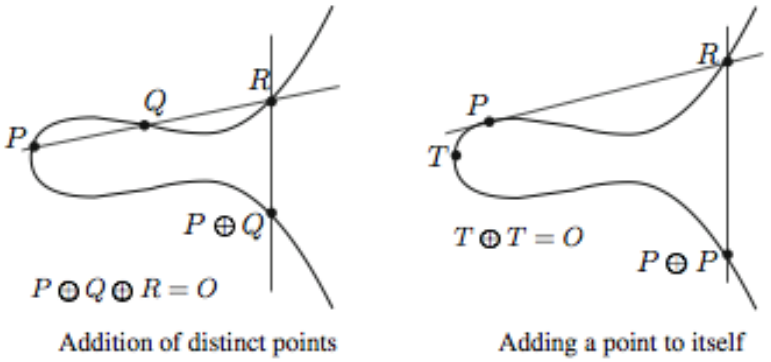

FIGURE 2. Additive Law of Elliptic Curves (This figure is from [1])

Remark 2.2. The graphs above show the real solutions to the Weierstrass equation. It is easy to see that $P \oplus Q$ is geometrically the reflection of point R across the x-axis.

[1]If $P \neq Q$, then it is clear that the line between them is unique. If $P = Q$, then the line we are considering is the line tangent to the Weierstrass equation f that is associated with E at the point $P = (r, s)$. This tangent line is given by $\frac{\partial f}{\partial x}(P)(x - r) + \frac{\partial f}{\partial y}(P)(y - s) = 0$. This line is unique if and only if either $\frac{\partial f}{\partial x}(P) \neq 0$ or $\frac{\partial f}{\partial y}(P) \neq 0$ i.e. if and only if f is non-singular.

[2]Bezout's Theorem guarantees that a line will intersect a Weierstrass equation in three points (counting multiplicity). More on Bezout's Theorem can be found in Fulton's *Algebraic Curves*.

Theorem 2.3. *$(E, \oplus)$ is an abelian group with identity $\mathscr{O}$. In other words,*

(i) *E is closed under $\oplus$.*
(ii) *For all $P \in E$, $P \oplus \mathscr{O} = \mathscr{O}$.*
(iii) *For all $P \in E$, there exists $P' \in E$ such that $P \oplus P' = \mathscr{O}$.*
(iv) *For all $P, Q, R \in E$, $P \oplus (Q \oplus R) = (P \oplus Q) \oplus R$.*
(v) *For all $P, Q \in E$, $P \oplus Q = Q \oplus P$.*

Proof. (i) $P \oplus Q$ is well-defined and in E by 2.2.

(ii) Consider $P \oplus \mathscr{O}$. By the definition of $\mathscr{O}$, the line that goes through P and $\mathscr{O}$ must be the vertical line that goes through P. This line then intersects E at three points: P, $\mathscr{O}$, and P', the point that is the reflection of P across the x-axis. Then, by the additive law, $P \oplus \mathscr{O}$ is the point that is the reflection of P' across the x-axis. This is the point P, so $P \oplus \mathscr{O} = P$.

(iii) Let $P \in E$. Let P' be the point that is the reflection of P across the x-axis. We want to determine $P \oplus P'$. If $P = \mathscr{O}$, then the reflection point $P' = \mathscr{O}$. E has a well-defined tangent line at $\mathscr{O}$ with multiplicity 3. Therefore, $\mathscr{O} + \mathscr{O} = \mathscr{O}$. If the y-coordinate of P is 0, then $P' = P$. So, the additive law tells us to consider the line that is tangent to the Weierstrass equation at the point P. Based on Figure 4.1, it is clear that when the y-coordinate of P is 0, the tangent line to P is a vertical line. So, $\mathscr{O}$ is on this line and the reflection point of $\mathscr{O}$ across the x-axis is $\mathscr{O}$. Therefore, in this case, $P \oplus P' = P \oplus P = \mathscr{O}$. Finally, in all other cases, the line through P and P' is a vertical line, which includes $\mathscr{O}$. So, $P \oplus P' = \mathscr{O}$. Thus, in all cases, if P' is the point P reflected across the x-axis, $P \oplus P' = \mathscr{O}$.

(iv) The associative law can be shown using the explicit formulas developed below, but this is surprisingly cumbersome and so is not shown here. A geometric proof of associativity can be found in Fulton's *Algebraic Curves*.

(v) $P \oplus Q$ is determined by the line that goes through P and Q. This is the same line that goes through the points Q and P. So, $P \oplus Q = Q \oplus P$.

□

Now that we have shown that $(E, \oplus)$ is an abelian group with identity $\mathscr{O}$, for the remainder of this paper, we will use the following notation conventions:

- We will write $P + Q$ for $P \oplus Q$.
- If $P + Q = \mathscr{O}$, we will write $Q = -P$. Notice that $-P$ is the point P reflected across the x-axis.
- We will write nP for $P + ... + P$ (n times).

Now, we will establish explicit formulas to add points on an elliptic curve.

Theorem 2.4 (Elliptic Curve Algorithm)**.** *Let E be an elliptic curve with Weierstrass equation*

$$y^2 = x^3 + ax + b,$$

and let $P, Q \in E$.

(a) *Suppose that $P = \mathscr{O}$ or $Q = \mathscr{O}$. Then, $P+Q = Q$ or $P+Q = P$ respectively.*
(b) *Otherwise, $P, Q \in E \setminus \{\mathscr{O}\}$. Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$.*
  (i) *If $x_1 = x_2$ and $y_1 = -y_2$ so that $Q = -P$, then $P + Q = \mathscr{O}$.*

(ii) *Otherwise, define*

$$\lambda = \begin{cases} \frac{x_2 - x_1}{y_2 - y_1} & : P \neq Q \\ \frac{3x_1^2 + a}{2y_1} & : P = Q \end{cases}$$

Let $x_3 = \lambda^2 - x_1 - x_2$ *and* $y_3 = \lambda(x_1 - x_3) - y_1$. *Then,* $P + Q = (x_3, y_3)$.

Proof. Part a and part (i) of b were shown in Theorem 4.5. For part (ii) of b, notice that if $P \neq Q$, then λ is the slope of the line through P and Q, and if $P = Q$, then λ, which is found by implicit differentiation, is the slope of the line that is tangent to E at the point P. Then, this line is of the form $y = \lambda x + c$, where $c = y_1 - \lambda x_1$, since P is on this line. To find the other point where this line and E intersect, we substitute this y into the Weierstrass equation:

$$(\lambda x + c)^2 = x^3 + ax + b.$$

$$x^3 - \lambda^2 x^2 + (a - 2c\lambda)x + (b - c^2) = 0.$$

This equation has three roots, where two of them must be x_1 and x_2, since P and Q are on both this line and the Weierstrass equation. Let x_3 be the third root. Then,

$$x^3 - \lambda^2 x^2 + (a - 2c\lambda)x + (b - c^2) = (x - x_1)(x - x_2)(x - x_3).$$

The coefficient of x^2 on the right hand side is $-x_1 - x_2 - x_3$. Therefore, $-\lambda^2 = -x_1 - x_2 - x_3$, which implies $x_3 = \lambda^2 - x_1 - x_2$. Plugging x_3 into the line $y = \lambda x + c$ results in $y_3 = \lambda x_3 + c$. So, the point other than P and Q that is on this line and the Weierstrass equation is the point (x_3, y_3). For the additive law, we have to reflect this point over the x-axis, so that

$$P + Q = (x_3, -y_3) = (\lambda^2 - x_1 - x_2, \lambda(x_1 - x_3) - y_1).$$

□

For cryptographic purposes, it is useful to work with a field K such that $E(K)$ is a set of finitely many points. So, from now on, we will only consider $E(\mathbb{F}_p)$ on an elliptic curve $E/\mathbb{F}_p$, for p prime. The work we did above shows that an elliptic curve $E \subset \mathbb{P}^2(\overline{\mathbb{F}_p})$ is a group under addition. Before we continue, we need to show that $E(\mathbb{F}_p) \subset E$ is also a group.

Proposition 2.5. *Let* $E/K \subset \mathbb{P}^2(\overline{K})$ *be an elliptic curve. Then,* $E(K)$ *is a subgroup of* E.

Proof. $E(K)$ has the identity element $\mathcal{O}$ by definition. For all $(x, y) \in E(K)$, the additive inverse $(x, -y)$ is also in $E(K)$. So, to show that $E(K)$ is a subgroup of E, we only need to show that $E(K)$ is closed under addition.

Let $P, Q \in E(K)$ so that P and Q have coordinates in K. Then, the line L connecting them has coefficients in K. The third point of intersection R between L and E/K has coordinates that are given by the explicit formulas in 2.4. Therefore, these coordinates are rational combinations of the coefficients of L and E/K. So, $R \in E(K) \implies P + Q = -R \in E(K)$. □

3. Modern Cryptography

The practice of encoding secret messages is as old as written language itself. Most cryptosystems, the methods of encrypting messages, rely on both the sending and receiving parties having the cipher, which is the rule used to encode and subsequently decode messages. Some examples throughout history have been Julius Caesar's shift ciphers and the Enigma machines used by the Germans during WWII.

However, with today's technology, it may not be feasible for the sending party to securely tell the receiving party what the common cipher is. The solution to this is to construct a cryptosystem so that our two parties do not have exactly the same, or symmetric, information. The concept of an asymmetric cryptosystem, a.k.a. public key cryptosystems, was first introduced in Whitfield Diffie and Martin Hellman's seminal 1976 paper "New Direction in Cryptography."

In this section, we will explore two public key cryptosystems: the Diffie-Hellman Key Exchange and the Elgamal Public Key Cryptosystem. Both of these systems are based on the Discrete Logarithm Problem (DLP).

Definition 3.1. Let G be a group. The *Discrete Logarithm Problem* for G is the problem of finding an algorithm that takes in $x, y \in G$ (where y is in the subgroup generated by x) and outputs an integer m such that $y = x^m$.

Examples 3.2. Each group therefore has its own DLP, so it is natural to wonder if some of these problems are harder than others. Let q be a prime that takes 2^k bits to represent. Let's look at the DLP for three groups: $(\mathbb{F}_q, +)$, $(\mathbb{F}_q^\times, \cdot)$, and $(E(\mathbb{F}_q), +)$.

(i) For $(\mathbb{F}_q, +)$, given $x, y \in \mathbb{F}_q$, the DLP is to find an algorithm that computes an integer m such that $xm = y$. This can be solved using the Euclidean algorithm and takes $O(\log q)$, or $O(k)$, steps. We say that such a problem can be solved in *polynomial time* in k.
(ii) For $(\mathbb{F}_q^\times, \cdot)$, given $x, y \in \mathbb{F}_q^\times$, the DLP is to find an algorithm that computes an integer m such that $x^m = y$. There exist algorithms called *index calculus* methods that can solve this in $O(q^\epsilon)$, or $O(2^{\epsilon k})$, steps for all $\epsilon > 0$. We say that such a problem can be solved in *subexponential time* in k.
(iii) For $(E(\mathbb{F}_q), +)$, given $P, Q \in E(\mathbb{F}_q)$, the DLP is to find an algorithm that computes an integer m such that $mP = Q$. The fastest algorithms that solve this take $O(\sqrt{q})$, or $O(2^{\frac{k}{2}})$, steps. We say that such a problem can be solved in *exponential time* in k.

Because the DLP for $(E(\mathbb{F}_q), +)$ takes substantially longer to solve, elliptic curves are commonly used in cryptography. So, this DLP will be our focus for the remainder of the paper. We call this specific DLP the Elliptic Curve Discrete Logarithm Problem (ECDLP).

Now, we will look at the Diffie-Hellman Key Exchange and Elgamal Public Key Exchange for elliptic curves.

3.1. **Diffie-Hellman Key Exchange.**

The Diffie-Hellman Key Exchange is not a true asymmetric cryptosystem, because it does not by itself encode and decode messages. Instead, it is an asymmetric way to establish a symmetric cryptosystem. It is important to understand this system, because it is the first publicized use of asymmetric reasoning in cryptography.

The goal of the Diffie-Hellman Key Exchange is for two parties, Alice and Bob, to share a common key without the need for a secure information channel. This key allows them to subsequently establish a symmetric cryptosystem. There are four parts to the Diffie-Hellman Key Exchange:

(1) Alice and Bob agree upon and post publicly a finite field $\mathbb{F}_q$, an elliptic curve $E/\mathbb{F}_q$, and a point $P \in E(\mathbb{F}_q)$.
(2) Alice chooses a secret integer a and calculates $A = aP$. Bob chooses a secret integer b and calculates $B = bP$.
(3) Alice publicly publishes A and Bob publicly publishes B. At this point, all parties (including outside parties) know A and B, but only Alice knows a and only Bob knows b.
(4) Alice calculates aB and Bob calculates bA.

$$aB = a(bP) = b(aP) = bA.$$

Both Alice and Bob obtain the point abP. This value can now be used as a key that Alice and Bob can use to encrypt and decrypt messages, and thereby establish a symmetric cryptosystem.

3.2. **Elgamal Public Key Cryptosystem.**

Despite the fact that the Diffie-Hellman Key Exchange incorporates asymmetric thinking, this system only achieves the exchange of a shared number that was not explicitly chosen by either party. This shared number can be used as a key, but because neither party chose this number, it cannot be a specific message.

A true Public Key Cryptosystem (PKC) allows for the secure exchange of a particular message, or a plaintext. In many cases, including this one, a plaintext is converted to a number. One way to do this is to convert each letter of the plaintext to a number and string these numbers together. A popular system for encoding a character is the ASCII system. Taher Elgamal published one of the first public key cryptosystems in 1985. There are four parts to the Elgamal PKC:

(1) Alice and Bob agree upon and post publicly a finite field $\mathbb{F}_q$, an elliptic curve $E/\mathbb{F}_q$, and a point $P \in E(\mathbb{F}_q)$.
(2) Alice chooses a secret integer a and calculates $A = aP$. Alice then publicly publishes A.
(3) Bob chooses a plaintext $M \in E(\mathbb{F}_q)$ and a random integer k. Bob calculates $B_1 = kP \in E(\mathbb{F}_q)$ and $B_2 = M + kA$. Bob publicly publishes B_1 and B_2.
(4) Alice computes

$$B_2 - (aB_1) = (M + kA) - (aka) = M + kaP - akP = M.$$

This string of equivalences proves that $B_2 - (aB_1) = M$, which shows that Alice does in fact extract the message that Bob encrypted. Of course, the above calculation $B_2 - (aB_1)$ can be done without any knowledge of the values M and k, which is vital since Alice knows neither the value M nor k.

3.3. **Security.**

Just as people develop new ways to encrypt information, people are always looking for ways to break encoding methods. So, the usefulness of new cryptosystems rest in the security of these cryptosystems. The security of a cryptosystem can be measured by how difficult it is for a third party to break the code, or put more practically, how many steps it takes for the most efficient known algorithm to solve the cryptosystem.

It is easy to see that breaking the Diffie-Hellman Key Exchange is no harder than solving the ECDLP, and in fact, no algorithm yet exists that can solve the Diffie-Hellman Key Exchange faster than the algorithms that solve the ECDLP. If a person can break the Diffie-Hellman Key Exchange, then they can break the Elgamal PKC, and if a person can break the Elgamal PKC then they can break the Diffie-Hellman Key Exchange. In other words, breaking the Diffie-Hellman Key Exchange and the Elgamal PKC are equivalently difficult problems, which are subsequently both equivalently difficult to solving the ECDLP. Thus, the Elgamal PKC is a cryptosystem that the best known algorithms take exponential time to break. Moreover, the steps involved in the Elgamal PKC are computationally very feasible, because they only involve addition on the points of elliptic curves, which is a procedure given by explicit formulas. The security and computational feasibility of cryptosystems involving elliptic curves are the reasons why elliptic curves are popularly used in cryptography.

Acknowledgments. It is a pleasure to thank my mentor, Eric Stubley, for his help with this paper.

References

[1] J. H. Silverman. The Arithmetic of Elliptic Curves 2nd Edition. Springer Science+Business Media, LLC. 2009, 1986.
[2] J. Hoffstein, J, Pipher, and J. H. Silverman. An Introduction to Mathematical Cryptography. Springer Science+Business Media New York. 2008, 2014.
[3] W. Fulton. Algebraic Curves. Addison-Wesley Publishing Company Advanced Book Program. 1989.
[4] W. Diffie, M.E. Hellman. New Directions in Cryptography. IEEE Trans. Inf. Theory IT-22(6), 644-654. 1976.