Elliptic Curve Cryptography

Sascha Brauer
Universität Paderborn

July 25, 2011

Contents

1 Introduction

The on-going evolution in modern hardware leads to greater risks for classical cryptosystems. To increase security, it is necessary to use larger keys for steady protection against attacks. The use of elliptic curves allows us to achieve similar security using much shorter keys. On the one hand this would reduce the hardware required, on the other hand the level of security would increase if we were to invest the same key size into elliptic curve cryptography as we would use in a non-elliptic curve cryptosystem.
This essay gives the basics needed to understand elliptic curves and shows how to integrate them in the popular *ElGamal* cryptosystem. It is structured as follows:
Section 1: Cyclic groups, the discrete logarithm and the *ElGamal* cryptosystem are introduced.
Section 2: It will be shown how elliptic curves are defined over the real numbers and over finite fields.
Section 3: The notions from the sections 1 and 2 will be put together to an elliptic curve

cryptosystem.
All notations used in this paper are consistent with the notations in [4].

2 The Discrete Logarithm

The fundamental idea behind the usage of elliptic curve cryptography, as well as the *ElGamal* cryptosystem itself, is that it is difficult to solve the *discrete logarithm* problem. A few things are needed to define the problem and to show its use in a cryptographic context.

2.1 Cyclic Groups

The *discrete logarithm* is a problem described in a setting with *cyclic groups.* While the classic logarithm is defined as a solution x of the equation $a^x = b$ with given a, b over the real or complex numbers, the *discrete logarithm* is the analogous problem within a *cyclic group.*

Definition 1. *A group $(G, \circ)$ is called a* cyclic group *if $|G| < \infty$ and there exists an element $g \in G$ (called* generator*), such that for every $h \in G$ there exists some $m \in \mathbb{Z}$, such that $g^m = h$ where $g^m = \underbrace{g \circ g \circ \ldots \circ g}_{m-times}$*
$n := |G|$ is called order *of the* cyclic group *G.*
The order *of an element $g \in G$ is defined as the smallest integer i such that $g^i = 1$.*

Though not explicitly shown here, it is important to note that $(\mathbb{Z}_p^*, \cdot)$ is a cyclic group, if p is prime[4]. Also let an element $a \in \mathbb{Z}_p^*$ be denoted as a *primitive element* if and only if it has order $p - 1$.

Example 2. *The multiplicative group $\mathbb{Z}_5^* = \{1, 2, 3, 4\}$ forms a cyclic group of order $n = 4$ with the generator 3. This can be shown by computing the powers of 3:*

$$3^1 = 3 \textit{ (mod 5)} \qquad 3^2 = 4 \textit{ (mod 5)} \qquad 3^3 = 2 \textit{ (mod 5)} \qquad 3^4 = 1 \textit{ (mod 5)}$$

Cyclic groups of any order n can be produced by defining $G := \{i^0, \ldots, i^{n-1}\}$ for an arbitrary integer i, if you let $i^n = i^0$. However this type of group is *isomorphic* to $(\mathbb{Z}_n, +)$, which obviously is an additive cyclic group. Through the isomorphic relation the two groups are basically the same.

Now we can define the *discrete logarithm* on a cyclic group.

Definition 3. *Given a cyclic group $(G, \cdot)$, a generator g of G and an element $h \in G$ find x, $0 \leq x \leq n - 1$ such that*

$$g^x = h$$

We call x the discrete logarithm *of h and denote it by $\log_g h$.*

2.2 Discrete Logarithm in Cryptosystems

The intuitive motivation above suggests that the discrete logarithm may be useful in a cryptographic context. It turns out that the exponentiation in cyclic groups can be computed efficiently while computing the discrete logarithm is a much harder problem[4]. The *square-and-multiply algorithm* [4] allows us to compute the power of a number with complexity being linear in the bit length of the exponent rather than being proportional to the exponent itself.
The discrete logarithm $\log_a b = x$ in a cyclic group G of order n may be solved by computing $a^2, a^3 \ldots$, eventually computing $a^i = b$ and thus solving the discrete logarithm. Assuming multiplication takes $\mathcal{O}(1)$ time it is obvious that this simple method solves the problem in $\mathcal{O}(n)$. In [4] one can find a description of this algorithm along with another method, which also solves discrete logarithms in the same time. This very extensive way of solving the problem is improved by several algorithms. Some of them are *Shanks' Algorithm*, *Pollard Rho Algorithm*, *Pohlig-Hellman Algorithm* and the *Index Calculus Method*. It should be noticed that the *Pohling-Hellman Algorithm* works more efficient, if n (which is equal to $p-1$ in $\mathbb{Z}_p^*$) has only got small prime factors. For further details see [4].
The most efficient algorithm currently known to solve the discrete logarithm uses the so called *Number Field Sieve* which was first developed the factorize integers. This method solves the discrete logarithm in $\mathcal{O}\left(\exp\left((3^{\frac{2}{3}} + o(1))(\log n)^{\frac{1}{3}}(\log\log n)^{\frac{2}{3}}\right)\right)$ [2].
Having seen this, we can say that the discrete logarithm problem is infeasible to solve on appropriately chosen groups, i.e. if you chose $\mathbb{Z}_p^*$ as your group, then p should have at least 300 digits and $p-1$ should have at least one large prime factor [4].

2.3 ElGamal Cryptosystem

While efficient methods exist for computing the power of a number in a cyclic group, they do not for computing the discrete logarithm, thus making this operation very useful for cryptography. One public-key cryptosystem that uses this is the *ElGamal Cryptosystem* which is defined in [4] and restated here.

Cryptosystem 4. *Let p be a prime and $(\mathbb{Z}_p^*, \cdot)$ be a multiplicative cyclic group where the discrete logarithm problem is infeasible. Also let $\alpha \in \mathbb{Z}_p^*$ be a primitive element. Let $P = \mathbb{Z}_p^*$ denote the set of plain-texts and $C = \mathbb{Z}_p^* \times \mathbb{Z}_p^*$ the set of cypher-texts. Then the set of keys is defined as*

$$K = \{(p, \alpha, a, \beta) | \beta = \alpha^a \mod p\}$$

The tuple (p, α, β) forms the public key, while a is the private key. Additionally let $k \in \mathbb{Z}_{p-1}$ be a secret random integer. The encryption function e_K and the decryption function d_K are defined as

$$e_K(x, k) = (y_1, y_2)$$
$$d_K(y_1, y_2) = y_2((y_1)^a)^{-1} \textit{ (mod p)}$$

where

$$y_1 = \alpha^k \mod p$$
$$y_2 = x\beta^k \mod p$$

For a more sophisticated description, as well as the proof of correctness for this cryptosystem refer to [1].
Now a simple example should demonstrate how the ElGamal cryptosystem works.

Example 5. *Alice chooses $p = 211$ and $\alpha = 2$. Let the private key be $a = 151$. She computes $\beta = 2^{151} = 187 \mod 211$ and publishes $(211, 2, 187)$ as her public key.*

Bob wants to send Alice the message $x = 123$ and chooses $k = 81$ as his random secret integer. He computes

$$y_1 = 2^{81} = 86 \mod 211$$
$$y_2 = 123 \cdot 187^{81} = 123 \cdot 135 = 147 \mod 211$$

and delivers his cypher $(86, 147)$ to Alice. She computes

$$d_K(86, 147) = 147 \cdot (86^{151})^{-1} = 147 \cdot 135^{-1} = 147 \cdot 186 = 123 \mod 211$$

and has the plain-text Bob wanted to send her.

In the example we can see that Alice needs to compute the inverse of an element in the cyclic group used. She can do this efficiently by using the *extended euclidean algorithm* which is presented in [4].

3 Elliptic Curves

Next we will introduce *elliptic curves*. To provide an intuitive approach we will define them over the real numbers and give a geometric definition before looking at them in a formal way.

Definition 6. *For constants $a, b \in \mathbb{R}$, we define E as the set of points $(x, y) \in \mathbb{R}^2$ satisfying the equation*

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

together with a special $\mathcal{O}$ called the point at infinity.
If $4a^3 + 27b^2 \neq 0$, then E is called elliptic curve*, else E is called* singular curve*.*

The following proof will show that $4a^3 + 27b^2 \neq 0$ is a necessary and sufficient criterion to ensure that $x^3 + ax + b$ has three distinct roots.

Proof. Assume that $x^3 + ax + b$ has a double root which is not 0. Then we can factor $x^3 + ax + b$ into:

$$\begin{aligned} x^3 + ax + b &= (x - c)(x - d)^2 \\ &= (x - c)(x^2 - 2dx + d^2) \\ &= x^3 + (-c - 2d)x^2 + (d^2 + 2dc)x - cd^2 \end{aligned}$$

By comparison of the coefficients we get:

$$\begin{array}{lc} & c + 2d = 0 \wedge a = d^2 + 2dc \wedge b = -cd^2 \\ \Leftrightarrow & c = -2d \wedge a = d^2 + 2dc \wedge b = -cd^2 \\ \Leftrightarrow & a = d^2 - 4d^2 = -3d^2 \wedge b = 2d \cdot d^2 = 2d^3 \\ \Leftrightarrow & a^3 = -27d^6 \wedge b^2 = 4d^6 \qquad (1) \\ \Leftrightarrow & 4a^3 = -108d^6 \wedge 27b^2 = 108d^6 \\ \Leftrightarrow & 0 = -108d^6 + 108d^6 = 4a^3 + 27b^2 \end{array}$$

In the equivalence (1) the solution for the cubic root is unique, since $b = -2d^3$ would not yield the original polynomial. □

With respect to Definition 6 an elliptic curve can be visualised as a graph in $\mathbb{R}^2$. In this geometric context the point at infinity can be arranged at the top of the y-axis making it necessary that the top of the y-axis is identified with its bottom, thus placing the point at infinity there, too [5].

Example 7. *Two curves over the real numbers.*

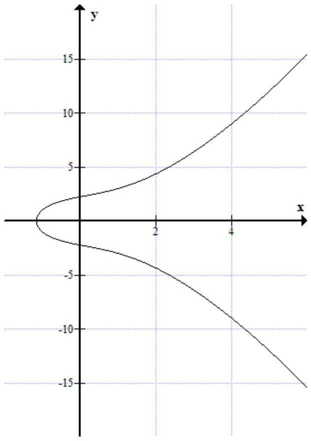

Figure 1: $y^2 = x^3 + 3x + 5$

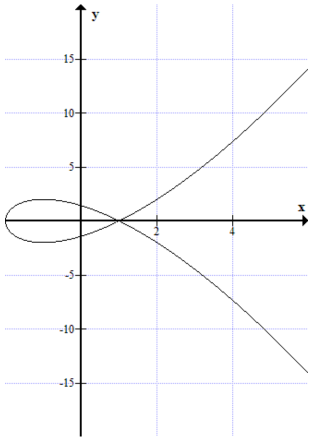

Figure 2: $y^2 = x^3 - 3x + 2$

Figure 1 shows an elliptic curve $(4 \cdot 3^3 + 27 \cdot 5^2 = 27 \cdot (4 + 25) \neq 0)$
Figure 2 shows a singular curve $(4 \cdot (-3)^3 + 27 \cdot 2^2 = -27 \cdot 4 + 27 \cdot 4 = 0)$

The problem evolving with singular curves is that there is a point on the curve (regarding Figure 2 this would be $(1,0)$) where the curve intersects itself. At this point there are two different tangent lines to the same point. We will see why this is a problem when we define an operation on the points of an elliptic curve.

3.1 Points on an Elliptic Curve form a Group

We will now define a binary operation on elliptic curves E called *addition* which will be denoted by $+$. Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be two points on an elliptic curve E. For now suppose $x_1 \neq x_2$. A line L drawn through P and Q will intersect E in a third point [4] which we denote by R'. When R' is reflected through the x-axis we obtain another point R we define as the sum of P and Q.

Example 8. *Suppose $E : y^2 = x^3 + 4x + 9$ and $P = (0,3)$, $Q = (-1,2)$. The line L through P and Q is given by the equation $y = x + 3$. Now we substitute L into E, which yields*

$$(x+3)^2 = x^3 + 4x + 9 \Leftrightarrow x^3 - x^2 - 2x = 0$$

We know that P and Q are in $L \cap E$, so $x = 0$ and $x = -1$ are solutions for $x^3 - x^2 - 2x = 0$. By polynomial division we can compute

$$x^3 - x^2 - 2x = x(x+1)(x-2)$$

Since $y = x + 3$ and $x = 2$ is the third solution for our intersection we get $R' = (2,5)$. After reflection through the $x-axis$ we get $P + Q = (2,-5)$.

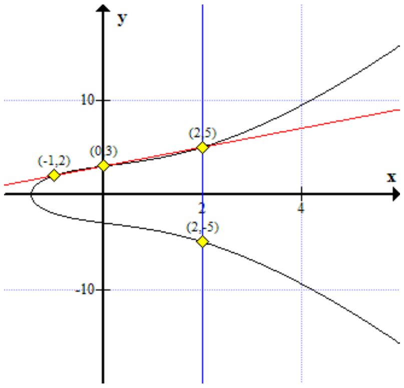

Figure 3: E with L and the points P, Q, R', R

Now we need to have a look at the addition in the case that $x_1 = x_2$. Again we differentiate between two cases. First suppose $y_1 = -y_2$. Then the line L through P and Q is vertical. Therefore the third intersection of L and E must be $\mathcal{O}$. Since reflecting $\mathcal{O}$ through the x-axis yields $\mathcal{O}$, the sum is $\mathcal{O}$.
Now suppose that $y_1 = y_2$. We can assume that $y_1 \neq 0$ (if $y_1 = 0$ we can treat it like the

first case). If we want to add P to itself, we need to define L as the tangent line to E at P. The slope of L can be computed as an implicit derivation of E. Afterwards R can be computed in the common manner.

Example 9. *Given are $E : y^2 = x^3 + 3x + 5$ and $P = (1, 3)$. If we want to compute $P + P$, we need the implicit derivation of E. At first we need to write E in it's implicit form, which is*

$$y^2 - x^3 - 3x - 5 = 0$$

Now we differentiate the implicit form of E in both directions

$$\tfrac{dE}{dy} = 2y$$
$$\tfrac{dE}{dx} = -3x^2 - 3$$

The derivations in the two directions form the gradient ∇E which is a normal vector to the tangent line at (x, y). Thus the slope of the tangent can be computed as

$$-\tfrac{\frac{dE}{dx}}{\frac{dE}{dy}} = \tfrac{3x^2+3}{2y}$$

Substituting P yields $\frac{3+3}{6} = 1$. Since $L : y = x + a$ and $3 = 1 + a \Rightarrow a = 2$, thus $L : y = x + 2$. Solving $L \cap E$ produces $R' = (-1, 1)$ and thus $P + P = (-1, -1)$.

In the case of a singular curve we were unable to uniquely define the tangent to the point where the curve intersects itself. It would not be possible to add that point to itself, which would prevent the addition from being a closed operation on E.
There is one more issue we need to clarify. Suppose we want to compute $P + \mathcal{O}$ for any $P = (x_1, y_1)$ on E. With respect to our intuitive geometric definition we gave for $\mathcal{O}$ the line through P and $\mathcal{O}$ is vertical. The third point on that line would be $(x_1, -y_1)$ (we already saw this in a different case). Reflecting this point through the x-axis yields P. This means that $\mathcal{O}$ acts as the neutral element for the addition of points.
Putting everything together we have defined a group $(E, +)$ with $\mathcal{O}$ as the identity element. We have seen that the addition on E is closed. It is also commutative (turning it into an abelian group), because the line L trough two points P and Q is unique (thus $P + Q$ and $Q + P$ produce the same line). Since $\mathcal{O}$ is the identity we can also denote $-(x, y) = (x, -y)$ because (x, y) and $(x, -y)$ are inverse elements with respect to the addition (in the second case of the definition of the addition of points we saw that the sum of points with this form is $\mathcal{O}$, which is the neutral element of the addition). It is rather tedious to show that addition is associative (i.e. that $(P+Q)+R = P+(Q+R)$). The interested reader can find the proof in [3].

3.2 Elliptic Curves over Finite Fields

Point addition on elliptic curves over the real numbers has a very nice geometric interpretation but is not useful in a cryptographic context. What we need to integrate elliptic curves into ElGamal is a cyclic group. This can be achieved by defining elliptic curves over a finite field. To give a basic understanding it is sufficient to show how this is done in $\mathbb{Z}_p$ for any prime $p > 3$.

Definition 10. *For a prime $p > 3$ and constants $a, b \in \mathbb{Z}_p$ such that $4a^3 + 27b^2 \neq 0 \mod p$, let an* elliptic curve over $\mathbb{Z}_p$ *be defined as the set E points $(x, y) \in \mathbb{Z}_p \times \mathbb{Z}_p$ satisfying the equation*

$$y^2 = x^3 + ax + b \mod p$$

together with a special $\mathcal{O}$ called the point at infinity.

Example 11. *Suppose we want to compute the points on $E : y^2 = x^3 + 5 \mod 7$. Candidates for points are all $(x, y) \in \mathbb{Z}_7 \times \mathbb{Z}_7$. The intuitive approach is to compute squares $y^2, y \in \mathbb{Z}_7$. Then compute $x^3 + 5$ for all $x \in \mathbb{Z}_7$ and check for equality. The quadratic residues* $\mod 7$ *are*

$$0^2 = 0 \quad 1^2 = 1 \quad 2^2 = 4 \quad 3^2 = 2 \quad 4^2 = 2 \quad 5^2 = 4 \quad 6^2 = 1$$

The following table will demonstrate the computation of points on E.

x	$x^3 + 5 \mod 7$	y
0	5	–
1	6	–
2	6	–
3	4	$2, 5$
4	6	–
5	4	$2, 5$
6	4	$2, 5$

Figure 4: Points on E over $\mathbb{Z}_7$

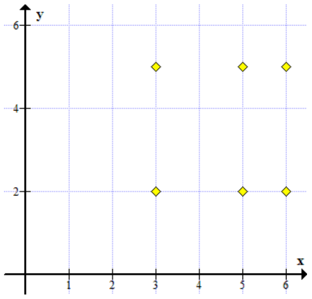

Figure 5: $y^2 = x^3 + 5 \mod 7$

Thus $E = \{\mathcal{O}, (3, 2), (3, 5), (5, 2), (5, 5), (6, 2), (6, 5)\}$.

As we can see in Figure 5 the addition of points on this elliptic curve does not offer a nice geometric approach like the ones over the real numbers. For this reason we have to define the addition of two points on an elliptic curve over $\mathbb{Z}_p$ in the following manner.

Definition 12. *Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be points on an elliptic curve E over $\mathbb{Z}_p$. If $x_1 = x_2$ and $y_1 = -y_2$ then*

$$P + Q = \mathcal{O},$$

else let $P + Q = R = (x_3, y_3)$

$$x_3 = m^2 - x_1 - x_2 \mod p$$
$$y_3 = m(x_1 - x_3) - y_1 \mod p$$

where

$$m = \begin{cases} (y_2 - y_1)(x_2 - x_1)^{-1} & \textit{if } P \neq Q \\ (3x_1^2 + a)(2y_1)^{-1} & \textit{if } P = Q \end{cases}$$

Additionally we define $\forall P \in E$*:*

$$\mathcal{O} + P = P + \mathcal{O} = P$$
$$-P = -(x, y) = (x, -y) \mod p$$

Note that this is basically the same definition as the addition on elliptic curves over the real numbers, if they were introduced formally. Observe that division has changed from $\frac{a}{b}$ to ab^{-1}. This is important since it is not trivial to find the multiplicative inverse in $\mathbb{Z}_p$. The following definition is valid for all elliptic curves and serves for convenient use later.

Definition 13. *Let* $P \in E$ *be any point on an elliptic curve* E *over* $\mathbb{Z}_p$ *and* $k \in \mathbb{Z}$

$$kP = \begin{cases} \sum_{i=1}^{k} P & \textit{if } k > 0 \\ \mathcal{O} & \textit{if } k = 0 \\ -\sum_{i=1}^{|k|} P & \textit{if } k < 0 \end{cases}$$

Example 14. *Suppose* $E : y^2 = x^3 + 5 \mod 7$ *and* $P = (3, 2)$*. By computing*

$$m = (3 \cdot 3^2)(2 \cdot 2)^{-1} = 6 \cdot 2 = 5 \mod 7$$
$$x_3 = 5^2 - 3 - 3 = 4 - 3 - 3 = 5 \mod 7$$
$$y_3 = 5(3 - 5) - 2 = 4 - 2 = 2 \mod 7$$

we can see that $2P = P + P = (5, 2)$*. Next we could compute* $3P = (5, 2) + (3, 2)$*.*

$$m = (2 - 2)(3 - 5)^{-1} = 0 \cdot 3 = 0 \mod 7$$
$$x_3 = 0^2 - 5 - 3 = 6 \mod 7$$
$$y_3 = 0(5 - 6) - 2 = 0 - 2 = 5 \mod 7$$

it follows that $3P = (6, 5)$*. Continuing in this manner yields*

P	$(3,2)$
$2P$	$(5,2)$
$3P$	$(6,5)$
$4P$	$(6,2)$
$5P$	$(5,5)$
$6P$	$(3,5)$
$7P$	$\mathcal{O}$

Figure 6: Multiples of P on E

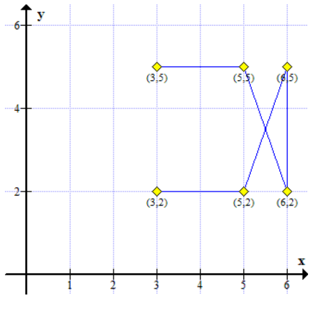

Figure 7: $i \cdot (3, 2)$ on E

Figure 6 shows us that $(3, 2)$ *is a generator of* E*.*

Example 14 actually showed us that there are elliptic curves that are cyclic groups. Since any additive group of prime order is cyclic (as shown in [4]), we are able to tell if an elliptic curve over a finite field has this characteristic by computing the number of points on it. For large p this task becomes quite extensive using the explicit method (listing all points on E). For an explanation of efficient algorithms and how to construct elliptic curves of prime order see [4].

4 Elliptic Curve Cryptosystem

For an actual application of elliptic curves in an ElGamal cryptosystem we need to take some of the definitions from the previous chapters and modify them slightly.

Definition 15. *Given an elliptic curve E of prime order, a generator P of E and an element $Q \in E$ find x such that*

$$xP = Q$$

We call x the discrete logarithm for an elliptic curve *of Q and denote it by $\log_P Q$.*

The advantage of the discrete logarithm for elliptic curves is that most of the algorithms mentioned in section 2.2 do not work if the elliptic curve is chosen appropriately [5].
Notice that only two things must be adapted to realise ElGamal elliptic curve cryptosystems. Modular multiplication has to change to addition of points, and modular exponentiation has to change to scalar multiplication of points [5].

4.1 ElGamal Elliptic Curve Cryptosystem

Let us now define an *ElGamal Elliptic Curve Cryptosystem*

Cryptosystem 16. *Let $E \mod p$ be an elliptic curve of prime order for a large prime p and $\alpha, \beta \in E$. Let $P = E$ denote the set of plaint-texts and $C = E \times E$ the set of cypher-texts. Then the set of keys is defined as*

$$K = \{(E \mod p, \alpha, a, \beta) | \beta = a\alpha\}$$

The tuple $(E \ (mod\ p), \alpha, \beta)$ forms the public key, while a is the private key. Let additionally $k \in \mathbb{Z}$ be a random integer. The encryption function e_K and the decryption function d_K are defined as

$$e_K(x, k) = (y_1, y_2)$$
$$d_K(y_1, y_2) = y_2 - ay_1$$

where

$$y_1 = k\alpha$$
$$y_2 = x + k\beta$$

Definition 16 makes the assumption that the plain-texts are represented as points on E. A discussion on how to represent messages as points on elliptic curves can be found in [5].

Example 17. *Alice chooses* $E: \ y^2 = x^3+2x+3 \mod 1237$ *and* $\alpha = (1,3)$. *She decides that* $a = 5$ *is her private key and computes* $\beta = 5(1,3) = (146,1137)$ *and publishes* $\big(y^2 = x^3+2x+3 \mod 1237, (1,3), (146,1137)\big)$ *as her public key.*
Bob wants to send Alice the message $x = (3,7)$ *and he chooses* $k = 3$ *as his random integer. He computes*

$$y_1 = 3(1,3) = (534,679)$$
$$y_2 = (3,7) + 3(146,1137) = (296,18)$$

and delivers his cypher $((534,679),(296,18))$ *to Alice. She computes*

$$x = (296,18) - 5(534,679) = (296,18) - (428,756) = (296,18) + (428,481) = (3,7)$$

and has the plain-text Bob wanted to send her.

References

[1] Taher El Gamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, 31(4):469–472, 1985.

[2] Daniel M. Gordon. Discrete logarithms in *f(p)* using the number field sieve. *SIAM J. Discrete Math.*, 6(1):124–138, 1993.

[3] James S. Milne. *Elliptic Curves.* BookSurge Publishers, 2006.

[4] Douglas R. Stinson. *Cryptography: Theory and Practice, Third Edition (Discrete Mathematics and Its Applications).* Chapman & Hall/CRC, 2005.

[5] Wade Trappe and Lawrence C. Washington. *Introduction to Cryptography with Coding Theory.* Prentice Hall, 2002.