university of groningen

faculty of mathematics
and natural sciences

Identity-based encryption using supersingular curves with the Weil pairing

Bachelor Project Mathematics

March 2014

Student: R. W. Mak

First supervisor: Prof.dr. J. Top

Second supervisor: Prof.dr. H. Waalkens

Abstract

In this paper we examine identity based encryption using the Weil pairing for supersingular elliptic curves over finite fields $\mathbb{F}_p$ with p suitable, large, primes. We examine a specific algorithm suggested in Washington [2008] and describe why and how it works. We show an implementation of this algorithm in Magma. Finally, we show that it is possible to perform this algorithm for different elliptic curves and offer examples of such curves.

Contents

1 Introduction

Elliptic curves are seeing more and more frequent use in cryptography. These are curves of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1}$$

By a change of coordinates we can show that this is equivalent to $y^2 = x^3 + Ax + B$ over fields of characteristic not equal to 2 or 3 as shown in Silverman [2009]. In this paper we examine an example of identity based encryption which uses the Weil pairing. The algorithm, described on page 184-186 of Washington [2008], uses elliptic curves that are supersingular over finite fields $\mathbb{F}_p$ for specific primes p. Note that in this paper, O will be the symbol used to refer to the identity element in elliptic curves.

Definition An elliptic curve $E : y^2 = x^3 + Ax + B$ is *supersingular* over a field K of characteristic p if O is the only point of order p in $E(\overline{K})$

We start off by defining and constructing the Weil pairing. We will also mention a few important properties of this bilinear pairing. Then we will describe the algorithm and explain why it works. Finally, we look at extensions of this algorithm to more supersingular curves.

This paper assumes a basic knowledge of elliptic curves and their structure.

2 The Weil pairing

Given a field K with characteristic not dividing a positive integer n and an elliptic curve E over K, we would like to construct a pairing

$$e_n : E[n] \times E[n] \to \{x \in \overline{K}^{\times} | x^n = 1\} \tag{2}$$

where $E[n] = \{P \in E(\overline{K}) | nP = O\}$ (that is, the points of order n over E). This is called the Weil pairing and in this section we will construct it. The method of construction largely is adapted from Washington [2008].

Definition A *divisor* is a formal sum of points

$$\sum_i a_i[P_i] \in \mathbb{Z}[E(\overline{K})]$$

for $P_j \in E(\overline{K})$ for some elliptic curve E over a field F and $a_i \in \mathbb{Z}$.

For a divisor

$$D = \sum_i a_i[P_i],$$

the *degree* is the sum of the integer coefficients

$$\deg(D) = \sum_i a_i \in \mathbb{Z},$$

and the *sum* is the sum of points

$$\mathrm{sum}(D) = \sum_i a_i P_i \in E(\overline{K}).$$

Definition For a function f on an elliptic curve E and a point $P \in E$:

- f has a *zero* at P if $f(P) = 0$.
- f has a *pole* at P if $f(P) = \infty$.

For a given point P we can always write f in the form

$$f = u_P^r f'$$

where u_P is a rational function on E with a zero of multiplicity 1 at P and $f'(P) \neq 0, \infty$. Then the *order* of f at the point P is defined as

$$\mathrm{ord}_P(f) = r$$

The *divisor* of f is defined as

$$\mathrm{div}(f) = \sum_{P \in E(\overline{K})} \mathrm{ord}_P(f)[P] \in \mathbb{Z}[E(\overline{K})]$$

Theorem 2.1. *Given a divisor D of degree 0 on an elliptic curve E, there exists a function f on E with*

$$div(f) = D$$

if and only if

$$sum(D) = \mathcal{O}$$

A proof of this theorem can be found on page 343-344 of Washington [2008]. By this theorem, given a $T \in E[n]$ we know that there exists a function f such that

$$\mathrm{div}(f) = n[T] - n[\mathcal{O}]$$

since then $\mathrm{sum}(\mathrm{div}(f)) = nT - n\mathcal{O} = \mathcal{O} - n\mathcal{O} = \mathcal{O}$ and $\mathrm{div}(f)$ is of degree zero. This means that the function f has a zero of order n at the point T, and a pole of order n at the point $\mathcal{O}$.

Similarly, given a $T' \in E[n^2]$ such that $nT' = T$ we can find a function g such that

$$\mathrm{div}(g) = \sum_{R \in E[n]} [T' + R] - [R]$$

since $\operatorname{div}(g)$ is of degree zero and

$$\operatorname{sum}(\operatorname{div}(g)) = \sum_{R \in E[n]} T' + R - R = \sum_{R \in E[n]} T' = n^2 T' = nT = \mathcal{O}.$$

This is because $\#E[n] = n^2$ by the following theorem:

Theorem 2.2. *Given a field K with a characteristic that does not divide a positive integer n, the set $E[n] \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ and hence contains exactly n^2 elements.*

A proof of this is on p. 80-86 of Washington [2008].

Now define the function h to be 'multiply by n'. $f \circ h$ will then have a zero of order n at all points $T' + R$, $R \in E[n]$ as

$$n(T' + R) = nT' + nR = T + \mathcal{O} = T$$

In addition, $f \circ h$ will have a pole of order n at all points $R \in E[n]$. In other words,

$$\begin{aligned} \operatorname{div}(f \circ h) = \sum_{P \in E(\overline{K})} \operatorname{ord}_P(f)[P] &= \sum_{R \in E[n]} n[T' + R] - \sum_{R \in E[n]} n[R] \\ &= \sum_{R \in E[n]} n[T' + R] - n[R] \end{aligned}$$

By a similar argument, we know that g has n^2 zeros of order 1, the points $T' + R$, $R \in E[n]$. It also has n^2 poles of order 1, the points $R \in E[n]$. In other words,

$$\begin{aligned} g = u_{T'+R}^{1} g' &\Rightarrow g^n = u_{T'+R}^{n} (g')^n \\ g = u_R^{-1} g'' &\Rightarrow g^n = u_R^{-n} (g'')^n \end{aligned}$$

where $u_{T'+R}$, u_R, g' and g'' are defined as before. This means that g^n has zeros and poles of order n and $-n$ respectively. However, here these zeros and poles are the same points as for g. Therefore

$$\begin{aligned} \operatorname{div}(f \circ h) &= \sum_{R \in E[n]} n[T' + R] - n[R] \\ &= \operatorname{div}(g^n) \end{aligned}$$

Using the following theorem we can show that $\operatorname{div}(f \circ n) = \operatorname{div}(g^n)$ implies that $c \cdot (f \circ n) = g$ for some constant c.

Theorem 2.3. *(See page 342 in Washington [2008]). A function f over an elliptic curve E for which $\operatorname{div}(f) = 0$ is a constant function.*

Corollary 2.4. *Given functions f and g over an elliptic curve E for which $div(f) = div(g)$, we know that for some constant c,*

$$f = cg$$

Proof. By contradiction: suppose that we have two functions f and g over an elliptic curve E for which $\operatorname{div}(f) = \operatorname{div}(g)$ but $f \neq cg$ for a constant c. Then there must be a function h that is not constant such that $f = hg$. However, since $\operatorname{div}(f) = \operatorname{div}(g)$ we know that f and g have the same poles and zeros. Hence h cannot have any zeros and poles and must be a constant function. □

This means that indeed $c \cdot (f \circ n) = g^n$ for some constant c. Therefore if we take some $S \in E[n]$ and a point $P \in E(\overline{K})$ we have that

$$\begin{aligned} g(P+S)^n &= c(f \circ n)(P+S) = cf(nP+nS) = cf(nP) = g(P)^n \\ \frac{g(P+S)^n}{g(P)^n} &= 1 \end{aligned}$$

and hence

$$\frac{g(P+S)}{g(P)}$$

is an n^{th} root of unity.

2.1 Properties of the Weil pairing

The Weil pairing has several interesting properties, but the three most relevant properties here are that

1. $$e_n(T, T) = 1,$$

2. $$\begin{aligned} e_n(S_1 + S_2, T) &= e_n(S_1, T)e_n(S_2, T) \\ e_n(S, T_1 + T_2) &= e_n(S, T_1)e_n(S, T_2) \end{aligned}$$

   for all $S_i, T_i \in E$.

   Note that this also means that

   $$e_n(mS, T) = e_n(S, T)^m = e_n(S, mT) \tag{3}$$

   for all $S, T \in E$ and $m \in \mathbb{Z}_{>0}$.

3. Finally, if $e_n(S, T) = 1$ for a given T and every S, then $T = \mathcal{O}$. Similarly, if $e_n(S, T) = 1$ for given S and every T, then $S = \mathcal{O}$.

3 The algorithm

This algorithm was taken from Washington [2008]. The elliptic curve used here is the supersingular curve $y^2 = x^3 + 1$. In addition we define 2 hash functions. First of all H_1, a hash function that takes a string of bits and outputs a point of order ℓ on the elliptic curve E. H_2 is a hash function that takes an element in $\mathbb{F}_{p^2}$ of order ℓ and outputs a binary string. Finally, we define a modified Weil pairing $\tilde{e}_n(P, Q) = e_n(P, \beta(Q))$ where $\omega \in \mathbb{F}_{p^2}$ such that ω is an element of order 3 and for a $Q = (x, y)$, $\beta(Q) = (\omega x, y)$.

1. Setting up the system

```
Choose a large prime $\ell > 3$ such that $p = 6\ell - 1$ is also a prime of the form $2 \pmod 3$ and a point $P$ of order $\ell$ in $E(\mathbb{F}_p)$.
Choose a random $s \in \mathbb{F}_\ell^\times$.
Compute $P_{pub} = sP$.
Make $p$, $H_1$, $H_2$, $P$, $P_{pub}$ public but keep $s$ secret (i.e. only the central authority knows $s$).
```

2. Creating a private key User with identity *ID*

```
Compute $Q_{ID} = H_1(ID) \in E(\mathbb{F}_p)$
Compute $D_{ID} = sQ_{ID} \in E(\mathbb{F}_p)$
Send $D_{ID}$ to the user.
```

3. Encrypting a message Message *M* sent to a user of identity *ID*

```
Compute $Q_{ID} = H_1(ID)$
Choose a random $r \in \mathbb{F}_\ell^\times$
Compute $g_{ID} = \tilde{e}_\ell(Q_{ID}, P_{pub})$
Let the cyphertext be $(u, v) = (rP, M \oplus H_2(g_{ID}^r))$ where $\oplus$ indicates bitwise addition mod 2, also known as bitwise XOR.
```

4. Decrypting the message

```
Compute $h_{ID} = \tilde{e}_\ell(D_{ID}, u)$
Compute $m = v \oplus H_2(h_{ID})$
```

4 Explaining the algorithm

In this section I will discuss parts of the algorithm.

4.1 The requirement that $p \equiv 5$ (mod 6)

Equivalent to setting $p = 6\ell - 1$ is requiring that $p \equiv 5 \pmod 6$. We do this because of the following theorems:

Theorem 4.1. *An elliptic curve E over $\mathbb{F}_p$ for a prime $p \geq 5$ is supersingular if and only if $\#E(\mathbb{F}_p) = p + 1$.*

A proof of this theorem can be found on page 131 of Washington [2008].

Theorem 4.2. *An elliptic curve E over $\mathbb{F}_p$ given by $y^2 = x^3 + B$ for $a \in \mathbb{F}_p$ is supersingular if $p = 5$ (mod 6).*

Proof. By theorem 4.1 we know that if E has $p + 1$ over $\mathbb{F}_p$ it is supersingular. Since $\mathbb{F}_p$ is cyclic, $x \mapsto x^3$, $x^3 \mapsto x^3 + B$ and $y \mapsto y^2$ are all bijections. Thus every point x in $\mathbb{F}_p$ has a unique y such that $y^2 = x^3 + B$. In addition, we have the point O, meaning that we have $p + 1$ points on this curve. Therefore it is supersingular. □

Another important result is the following:

Theorem 4.3. *For an elliptic curve over a finite field $\mathbb{F}_p$ we have that either*

$$E(\mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z}$$

for $n = \#E(\mathbb{F}_p)$ or

$$E(\mathbb{F}_p) \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$$

with $n_1 \mid n_2$ and $n_1 n_2 = \#E(\mathbb{F}_p)$.

A proof for this theorem can be found on page 97 of Washington [2008], except for the requirements that $n = \#E(\mathbb{F}_p)$ and that $n_1 n_2 = \#E(\mathbb{F}_p)$. However, this follows from the fact that these are isomorphisms and hence must have the same number of elements. Additionally we use the fact that $\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$ has $n_1 n_2$ elements.

Because of these theorems we know that for this particular elliptic curve over this finite field, we have that

$$E(\mathbb{F}_p) \cong \mathbb{Z}/6\ell\mathbb{Z}$$

After all, neither $2 \mid 3\ell$, $3 \mid 2\ell$ nor $6 \mid \ell$, and ℓ of course cannot be factored as it is prime. By the Chinese Remainder Theorem we thus know that

$$E(\mathbb{F}_p) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$$

Hence $6E(\mathbb{F}_p) \cong \mathbb{Z}/\ell\mathbb{Z}$ has only elements of order ℓ (and one element of order 1, the identity element) and it is trivial to find such an element. What's more, $\mathbb{Z}/\ell\mathbb{Z}$ is cyclic and hence so is $E(\mathbb{F}_p)$.

4.2 Finding the element of order 3, ω

We know that there is no element of order 3 in $\mathbb{F}_p^\times$, because $\#\mathbb{F}_p^\times = p-1 = 6\ell-2$ which is not divisible by 3. In order to find such an element we want to find an extension of $\mathbb{F}_p$. All solutions to the polynomial $X^3 - 1$ are elements of order 3. However, as $X = 1$ is an element of $\mathbb{F}_p$ this is not an irreducible polynomial. Factoring out this solution we find $X^3 - 1 = (X-1)(X^2+X+1)$. Solutions of X^2+X+1 must be elements of order 3, and this is an irreducible polynomial. Since the degree of this polynomial is 2,

$$\mathbb{F}_p[X]/(X^2+X+1) = \mathbb{F}_{p^2}$$

In other words, such an ω is one of the solutions to the irreducible polynomial in $\mathbb{F}_{p^2}$. Since ω is a nontrivial cube root, we also know the following:

Theorem 4.4. *The mapping $\beta : (x,y) \mapsto (\omega x, -y)$, $\beta(\mathcal{O}) = \mathcal{O}$ is an automorphism on the curve $E : y^2 = x^3 + B$.*

Proof. We need to show that β (1) sends points on E to E, (2) is a homomorphism, and (3) is invertible. We are looking at points $P = (x_1, y_1)$ and $Q = (x_2, y_2)$, both in $E(\overline{\mathbb{F}_p})$.

1. In order to show that β sends $E(\overline{\mathbb{F}_p})$ to itself, we only need to show that if $\omega x, -y$ is a point on $E(\overline{\mathbb{F}_p})$ then so is (x,y). Indeed

   $$(-y)^2 = (\omega x)^3 + B \Rightarrow y^2 = \omega^3 x + B \Rightarrow y^2 = x^3 + B$$

   meaning that $(x,y) \in E(\overline{\mathbb{F}_p})$.

2. To show that β is a homomorphism we need to show that $\beta(P+Q) = \beta(P)+\beta(Q)$. There are four different possibilities for addition (Washington [2008] defines these additions on page 14):

   (a) $x_1 \neq x_2$, $y_1 \neq y_2$. In this case $P + Q = (m^2 - x_1 - x_2, m(2x_1 + x_2 - m^2) - y_1)$ with $m = \frac{y_2 - y_1}{x_2 - x_1}$.

   $$\begin{aligned} \beta(P+Q) &= \beta\left(m^2 - x_1 - x_2, m(2x_1 + x_2 - m^2) - y_1\right) \\ &= \left(\omega(m^2 - x_1 - x_2), -m(2x_1 + x_2 - m^2) + y_1\right) \end{aligned}$$

   $$\begin{aligned} \beta(P) + \beta(Q) &= (\omega x_1, -y_1) + (\omega x_2, -y_2) \\ &= \beta\left(\left(\frac{-y_2 + y_1}{\omega x_2 - \omega x_2}\right)^2 - \omega x_1 - \omega x_2, \left(\frac{-y_2 + y_1}{\omega x_2 - \omega x_2}\right)\left(2\omega x_1 + \omega x_2 - \left(\frac{-y_2 + y_1}{\omega x_2 - \omega x_2}\right)^2\right) + y_1\right) \\ &= \beta\left(\left(\frac{-1}{\omega} m\right)^2 - \omega x_1 - \omega x_2, \left(\frac{-1}{\omega} m\right)\left(2\omega x_1 + \omega x_2 - \left(\frac{-1}{\omega} m\right)^2\right) + y_1\right) \\ &= \beta\left(\frac{1}{\omega^2} m^2 - \omega x_1 - \omega x_2, \frac{-1}{\omega} m\left(2\omega x_1 + \omega x_2 - \frac{1}{\omega^2} m^2\right) + y_1\right) \\ &= \beta\left(\left(\frac{1}{\omega^2}\right) m^2 - \omega x_1 - \omega x_2, m\left(2x_1 + x_2 - \left(\frac{1}{\omega^3}\right) m^2\right) + y_1\right) \\ &= \beta\left(\left(\frac{1}{\omega^3}\right) \omega(m^2 - x_1 - x_2), -m\left(2x_1 + x_2 - \left(\frac{1}{\omega^3}\right) m^2\right) + y_1\right) \\ &= \left(\omega(m^2 - x_1 - x_2), -m(2x_1 + x_2 - m^2) + y_1\right) \end{aligned}$$

   So indeed $\beta(P + Q) = \beta(P) + \beta(Q)$.

   (b) $x_1 = x_2$, $y_1 \neq y_2$. In this case $Q = -P$ and $P + Q = \mathcal{O}$.

   $$\beta(P + Q) = \beta(\mathcal{O}) = \mathcal{O}$$

   $$\begin{aligned} \beta(P) + \beta(Q) &= \beta(P) + \beta(-P) \\ &= (\omega x, -y)) + (-\omega(x), -y) \\ &= \beta(P) - \beta(P) \\ &= \mathcal{O} \end{aligned}$$

(c) $P = Q$, $y_1 \neq 0$. In this case $P + Q = (m^2 - 2x_1, m(3x_1 - m^2) - y_1)$ with $m = \frac{3x_1^2}{2y_1}$.

$$\begin{aligned}\beta(P + Q) &= \beta(m^2 - 2x_1, m(3x_1 - m^2) - y1) \\ &= (\omega(m^2 - 2x_1), -m(3x_1 - m^2) + y1)\end{aligned}$$

$$\begin{aligned}\beta(P) + \beta(Q) &= (\omega x_1, -y_1) + (\omega x_2, -y_2) \\ &= \left(\left(\frac{3(\omega x_1)^2}{-2y_1}\right)^2 - 2\omega x_1, \left(\frac{3(\omega x_1)^2}{-2y_1}\right)\left(3\omega x_1 - \left(\frac{3(\omega x_1)^2}{-2y_1}\right)^2\right) + y_1\right) \\ &= \left(\omega^4 m^2 - 2\omega x_1, -\omega^2 m\left(3\omega x_1 - \omega^4 m^2\right) + y_1\right) \\ &= \left(\omega m^2 - 2\omega x_1, -m\left(3\omega^3 x_1 - \omega^6 m^2\right) + y_1\right) \\ &= \left(\omega(m^2 - 2x_1), -m\left(3x_1 - m^2\right) + y_1\right)\end{aligned}$$

So again, $\beta(P + Q) = \beta(P) + \beta(Q)$

(d) $P = Q$, $y_1 = 0$. In this case $P + Q = \mathcal{O}$.

$$\beta(P + Q) = \beta(\mathcal{O}) = \mathcal{O}$$

$$\beta(P) + \beta(Q) = (0, 0) + (0, 0) = \mathcal{O}$$

This proves that β is indeed a homomorphism.

3. In order to show that β is invertible we can simply find an inverse. We try $\beta^{-1}((x, y)) = (\omega^2 x, -y)$:

$$\begin{aligned}\beta(\beta^{-1}((x, y))) = \beta((\omega^2 x, -y)) = (\omega(\omega^2 x), -(-y)) = (\omega^3 x, y) = (x, y) \\ \beta^{-1}(\beta((x, y))) = \beta^{-1}((\omega x, -y)) = (\omega^2(\omega x), -(-y)) = (\omega^3 x, y) = (x, y)\end{aligned}$$

Therefore this is indeed an inverse, meaning that β is invertible and thus is a bijection.

Therefore β is an automorphism. □

It is of importance that this element is not in $\mathbb{F}_p$. Suppose we simply took the normal Weil pairing of the points Q_{ID} and P_{pub}. We saw before that $6E(\mathbb{F}_p) \cong \mathbb{Z}/\ell\mathbb{Z}$ and by construction both Q_{ID} and P_{pub} are in $6E(\mathbb{F}_p)$. This is a cyclic group and hence we can find an integer m such that $Q_{ID} = mP_{pub}$. Therefore

$$e_\ell(Q_{ID}, P_{pub}) = e_\ell(mP_{pub}, P_{pub}) = e_\ell(P_{pub}, P_{pub})^m = 1^m = 1$$

Theorem 4.5. *$\tilde{e}_\ell(P, P)$ results in a nontrivial root of unity when $P \neq \mathcal{O}$.*

Proof. We know that $P \in E(\mathbb{F}_p)$ and $\omega P \notin E(\mathbb{F}_p)$ and so there is no element $a \in \mathbb{F}_p$ such that $aP = \omega P$. By the theorem 2.2, we know that $E[\ell] \cong \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ as ℓ certainly does not divide p. Since these groups are cyclic and we have two independent elements, we also have two generators of those groups. Hence $\mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z} \cong \langle P \rangle \times \langle \omega P \rangle$. Since all elements in $E[\ell]$ are in this direct sum of cyclic groups, $e_\ell(P, \omega P) = 1$ would mean that $e_\ell(P, Q) = 1$ for any given $Q \in \langle \omega P \rangle$. We previously showed that it would also be 1 for any $Q \in \langle P \rangle$. Therefore this pairing results in the trivial root of unity for any $Q \in E[\ell]$. By the third property of the Weil pairing stated in section 2.1 we then know that $P = \mathcal{O}$. Then we know that the modified Weil pairing will always result in a nontrivial root of unity. □

4.3 Where can the ℓ^{th} roots of unity be found?

Theorem 4.6. *For a finite field $\mathbb{F}_p$ with $p = a\ell - 1$ for an integer a and a prime ℓ, all ℓ^{th} roots of unity are in $\mathbb{F}_{p^2}^{\times}$*

Proof. First we check if all elements of order ℓ are in $\mathbb{F}_p^{\times}$. In fact, there are no points of order ℓ in $\mathbb{F}_p^{\times}$, as $\#\mathbb{F}_p^{\times} = p - 1 = a\ell - 2$ which is not divisible by ℓ.

Now we check if all elements of order ℓ are in $\mathbb{F}_{p^2}^{\times}$ instead. $\#\mathbb{F}_{p^2}^{\times} = p^2 - 1 = a^2\ell^2 - 2a\ell$ which is indeed divisible by ℓ. Hence there is at least one element of order ℓ as ℓ is prime. Additionally, $\mathbb{F}_{p^2}^{\times}$ is cyclic, meaning that all points of order ℓ will be contained there. Hence all elements of order ℓ can be found in $\mathbb{F}_{p^2}^{\times}$. □

4.4 An example H_1

In step 2.1 we first use the hash function H_1. This is a function that has as input a string of bits of arbitrary length and outputs a point of order ℓ on E. The function used here is one suggested in Washington [2008].

H_1 Input a string of bits ID and output a point on E

```
Use some hash function $H$ to send $ID$ to $H(ID) \in \mathbb{F}_p$.
Let $H(ID)$ be the $y$ coordinate $y$ of a point on $E$.
Calculate the corresponding $x = (y^2 - 1)^{1/3}$.
$H_2(ID) = 6(x, y) \in E(\mathbb{F}_{p^2})$
```

Theorem 4.7. *This H_1 will always result in a unique x_{ID} such that the point lies on $E(\mathbb{F}_{p^2})$.*

Proof. First we define two bijections on $\mathbb{F}_p$:

$$f : x \mapsto x^3$$
$$g : y \mapsto y + 1$$

Since these are both bijections, $g(f(x)) = x^3 + 1$ is also a bijection. Since $y \mapsto y^2$ is also a bijection on $\mathbb{F}_p$ for every element y there must then also exist an x such that $y^2 = x^3 + 1$. Since these are all bijections, such an x is also unique. □

Theorem 4.8. *This H_1 will result in a point of order ℓ or* 1.

Proof. We already showed at the end of section 4.1 that $6E(\mathbb{F}_p) \cong \mathbb{Z}/\ell\mathbb{Z}$. Since ℓ is prime, there are only points of order 1 or ℓ in $\mathbb{Z}/\ell\mathbb{Z}$. □

In fact, we can easily find all the points in $E(\mathbb{F}_p)$ that are are mapped to $\mathcal{O}$, the point of order 1. This is the only point of order 1 in $\mathbb{Z}/\ell\mathbb{Z}$ is 1 since ℓ is prime. The elements are the points of order 6,

$$E(\mathbb{F}_p)[6] = \{(2, \pm 3), (0, \pm 1), (-1, 0), \mathcal{O}\}.$$

Since our hash function doesn't map anything to $\mathcal{O}$, there are only 5 elements that could be mapped to: the elements with y-coordinate $0, \pm 1$, and ± 3. In other words, we could prevent an element of order 1 resulting from the hash function if we don't get any of the above y-coordinates. In any case, however, the chance of getting a point of order ℓ is $1/\ell$ which is very small for large ℓ.

4.5 An example H_2

In order to send points from $\mathbb{F}_{p^2}$ to a string of bits, we first use the trace to send it to $\mathbb{Z}$. First we need to know two things:

Theorem 4.9 (Page 482, Washington [2008])**.**

$$\mathbb{F}_{p^n} = \{x \in \overline{\mathbb{F}_p} \mid x^{p^n} = x\}$$

Definition (Page 54, Lidl and Niederreiter [1997]) The *trace* is defined as

$$\mathrm{Tr}_{\mathbb{F}_{p^n}}(x) = x + x^p + \cdots + x^{p^{n-1}}$$

It turns out that the trace always sends elements to $\mathbb{F}_p$ and that it is a linear transformation over $\mathbb{F}_p$. (Page 55-56, Lidl and Niederreiter [1997])

In our case, we are dealing with elements of the form $c + d\omega$ where ω is our element of order 3. However, this will work for any element in a finite field of the form $\mathbb{F}_{p^2} = \mathbb{F}[\sqrt{b}]$ for some $b \in \mathbb{F}_p$, and this is what we will be dealing with for the rest of this paper. Additionally, since we are only interested in the trace over $\mathbb{F}_{p^2}$, we will simply use $\mathrm{Tr}(x)$ to mean $\mathrm{Tr}_{\mathbb{F}_{p^2}}(x)$. We use the following theorem:

Theorem 4.10.

$$(c + d\sqrt{b})^P = c - d\sqrt{b}$$

for $c, d \in \mathbb{F}_p$, $\sqrt{d} \in \mathbb{F}_{p^2} \backslash \mathbb{F}_p$

Proof. We start out by calculating, remembering that $x^p \equiv x \mod p$ for $x \in \mathbb{F}_p$:

$$\begin{aligned}(c + d\sqrt{b})^p &= (c + d\sqrt{b})^p \\ &= c^p + d^p(\sqrt{b})^p \\ &= c + db^{\frac{p-1}{2}}\sqrt{d}\end{aligned}$$

Note that $b^{p-1} = 1$ in $\mathbb{F}_p$, and so $b^{\frac{p-1}{2}}$ is a second root of unity, i.e. $+1$ or -1. In addition, $b^{\frac{p-1}{2}}$ cannot equal $+1$, as this would mean that

$$(\sqrt{b})^p = b^{\frac{p-1}{2}}\sqrt{b} = \sqrt{b}$$

which would imply by theorem 4.9 that $\sqrt{b} \in \mathbb{F}_p$ which we showed not to be true. Hence $b^{\frac{p-1}{2}} = -1$ and hence

$$(c + d\sqrt{b})^p = c - d\sqrt{b}$$

□

Therefore have that $\mathrm{Tr}(c + d\sqrt{b}) = 2c$, as

$$\begin{aligned}\mathrm{Tr}(c + d\sqrt{b}) &= (c + d\sqrt{b}) + (c + d\sqrt{b})^p \\ &= c + d\sqrt{b} + c^p + d^p(\sqrt{b})^p \\ &= c + d\sqrt{b} + c - d\sqrt{b} \\ &= 2c\end{aligned}$$

However, in our case ω is a solution to $X^2 + X + 1$, where we have that $\omega = -\frac{1}{2} \pm \frac{\sqrt{-3}}{2}$. This means that

$$\mathrm{Tr}(c + d\omega) = \mathrm{Tr}(c - \frac{d}{2} \pm \frac{\sqrt{-3}}{2}) = 2c - d$$

This means that we need to do some basic maths to find that in the case $\omega = \frac{1}{2} + \frac{\sqrt{-3}}{2}$ (we will not discuss the other case here as it is essentially the same)

$$d = \frac{2(c + d\omega) - \mathrm{Tr}(c + d\omega)}{2\omega + 1}$$

Finally define

$$H_2 : (c + d\omega) \mapsto 2c - d + pd$$

The most important property is that that this is injective, so there will be no collisions. At this point we have a point in $\mathbb{Z}$ and from this point on it is trivial to send such an integer to a string of bits (by for example representing the integer in base 2).

4.6 Decrypting the message

Theorem 4.11. *Part 4 of the algorithm correctly decrypts the encrypted message.*

Proof. Indeed, Washington [2008] shows that $m = M$, since

$$\begin{aligned} m = v \oplus H_2(g_{ID}) &= (M \oplus H_2(g_{ID}^r)) \oplus H_2(\tilde{e}_\ell(D_{ID}, u)) \\ &= (M \oplus H_2(g_{ID}^r)) \oplus H_2(\tilde{e}_\ell(sQ_{ID}, rP)) \\ &= (M \oplus H_2(g_{ID}^r)) \oplus H_2(\tilde{e}_\ell(Q_{ID}, P)^{rs}) \\ &= (M \oplus H_2(g_{ID}^r)) \oplus H_2(\tilde{e}_\ell(Q_{ID}, sP)) \\ &= (M \oplus H_2(g_{ID}^r)) \oplus H_2(\tilde{e}_\ell(Q_{ID}, P_{pub})^r) \\ &= (M \oplus H_2(g_{ID}^r)) \oplus H_2(g_{ID}^r) \\ &= M \end{aligned}$$

because the Weil pairing is bilinear as shown in (3) and this also applies to our modified Weil pairing as

$$\tilde{e}_\ell(mS, nT) = e_\ell(mS, \omega(nT)) = e_\ell(mS, n(\omega T)) = e_\ell(S, \omega T)^{mn} = \tilde{e}_\ell(S, T)^{mn}$$

□

4.7 A note on the curve used

All of the previous arguments actually work for any curve $y^2 = x^3 + B$ with $B \in \mathbb{F}_p^\times$. It turns out that all of these curves have the same j-invariant which means that they are isomorphic to each other. However, we will discuss exactly what the j-invariant is and its implications in the next section.

4.8 An actual implementation of the algorithm

Using all the above, Magma (`http://magma.maths.usyd.edu.au/`) code was written to implement this algorithm. The code, along with inline explanations of exactly how things were implemented, is in appendix A.

5 Generalising the algorithm to more curves

As can be seen from the in-depth discussion of the algorithm, all that is really necessary is a supersingular elliptic curve and a homomorphism $\sigma : E \to E$ for which all elements in $E(\mathbb{F}_p)$ are mapped to elements in $E(\mathbb{F}_{p^2})$. Such a mapping is called an endomorphism.

Definition Page 50-51, Washington [2008]. An *endomorphism* is a homomorphism $\alpha : E(K) \to E(K)$ such that $\alpha(x, y) = (r_1(x), r_2(x)y)$ where r_1 and r_2 are rational functions of the form $p(x)/q(x)$.

The *degree* of an endomorphism $\alpha(x,y) = (r_1(x), r_2(x)y)$ with $r_1(x) = p(x)/q(x)$ is $\deg(\alpha(x,y)) = \max\{\ \deg(p(x)),\ \deg(q(x))\ \}$. In fact, this maximum equals $\deg(p(x))$, since otherwise O would not be mapped to O.

Washington [2008] shows that any endomorphism of the form

$$(x,y) \mapsto (R_1(x,y), R_2(x,y))$$

can be reduced to the form stated in the definition which is why only that form is used.

Earlier we looked at the mapping $(x,y) \mapsto (\omega x, -y)$. This is, as was stated, an automorphism, which is an invertible endomorphism. However, we have no need for an invertible mapping, as no part of the algorithm depends on it. This means that we can instead look for curves on which are defined suitable endomorphisms. Suitable in this case means that for an endomorphism $\alpha : E \to E$ we have that $\tilde{e}_\ell(P,Q) = e_\ell(P, \alpha(Q))$ results in a nontrivial ℓ^{th} root of unity for $P, Q \in E(\mathbb{F}_p)$. In addition, we would like curves for which $E[\ell]$ is contained in $E(\mathbb{F}_{p^k})$ for small k so that we know where we can find all the ℓ^{th} roots of unity.

5.1 The j-invariant

In order to be able to talk about elliptic curves more generally we will use the j-invariant.

Definition The *j-invariant* of a curve $E : y^2 = x^3 + Ax + B$ is defined to be

$$j(E) = \frac{1728(4A^3)}{4A^3 + 27B^2}$$

The j-invariant can be determined for more general elliptic curves of the form (1), but this is a rather large equation which can be constructed based on information given on page 42 in Silverman [2009] so we will leave it out.

The j-invariant is very useful because of the following theorem, the proof of which can be found on page 45 of Silverman [2009].

Theorem 5.1. *Two elliptic curves E and E' are isomorphic over a field $\overline{K}$ if and only if*

$$j(E) = j(E')$$

Because of this theorem, we can describe endomorphisms for a single curve and then extend this to all curves with the same j-invariant.

5.2 Endomorphisms of degree 2

Now we will describe some classes of curves and corresponding endomorphisms. In this paper we will look at endomorphisms of degree 2 as they are described in detail by Silverman [1994]. Silverman shows that there are exactly 3 classes of curves for which an endomorphism of degree 2 exists:

1. $y^2 = x^3 + x,$ $\qquad j = 1728, \quad \alpha = 1 + \sqrt{-1}$

   $$(x, y) \mapsto \left(\alpha^{-2}\left(x + \frac{1}{x}\right), \alpha^{-3}y\left(1 - \frac{1}{x^2}\right)\right)$$

2. $y^2 = x^3 + 4x^2 + 2x,$ $\qquad j = 8000, \quad \alpha = \sqrt{-2}$

   $$(x, y) \mapsto \left(\alpha^{-2}\left(x + 4 + \frac{2}{x}\right), \alpha^{-3}y\left(1 - \frac{2}{x^2}\right)\right)$$

3. $y^2 = x^3 - 35x + 98,$ $\qquad j = -3375, \ \alpha = \dfrac{1 + \sqrt{-7}}{2}$

   $$(x, y) \mapsto \left(\alpha^{-2}\left(x - \frac{7(1-\alpha)^4}{x + \alpha^2 - 2}\right), \alpha^{-3}y\left(1 + \frac{7(1-\alpha)^4}{(x + \alpha^2 - 2)^2}\right)\right)$$

In other words, for the classes of curves with j-invariant 1728, 8000, and -3375 we have the endomorphism of degree 2 described above. We must determine several things before these curves can be used, however: over which finite fields $\mathbb{F}_p$ are these curves supersingular, and do these endomorphisms result in a nontrivial root of unity when used with the modified Weil pairing?

5.3 When are these curves supersingular?

Washington [2008] shows that curves with j-invariant 1728 are supersingular over $\mathbb{F}_p$ if and only if $p \equiv 3 \pmod 4$. For j-invariant 8000 and -3375, however, we need to look at the endomorphism ring $\mathrm{End}(E)$. We require one definition and two theorems (taken and adapted from Silverman [2009]):

Definition (Silverman [2009]) A *definite quaternion algebra* is an algebra $\mathcal{K}$ of the form

$$\mathcal{K} = \mathbb{Q} + \mathbb{Q}\gamma + \mathbb{Q}\delta + \mathbb{Q}\gamma\delta$$

with the following properties:

1. $\gamma^2, \delta^2 \in \mathbb{Q}$
2. $\gamma^2 < 0$
3. $\delta^2 < 0$
4. $\delta\gamma = -\gamma\delta$

Note that because of this last property, quaternion algebras are not commutative.

Theorem 5.2 (Page 102, Silverman [2009])**.** *The endomorphism ring of an elliptic curve over a field with characteristic not zero is either*

1. *$\mathbb{Z}$.*
2. *An order in an imaginary quadratic field, i.e. a subring of the form*
$$\{m + n\alpha \mid n, m \in \mathbb{Z}, \alpha = \sqrt{-d} \text{ for some } d \in \mathbb{Z}_{>0}\} \subset \mathbb{Z}[i]$$
3. *An order in a quaternion algebra, i.e. a subring of the form*
$$\{k + l\epsilon + m\eta + n\epsilon\eta \mid k, l, m, n \in \mathbb{Z}\} \subset \mathcal{K}$$

Theorem 5.3 (Page 145, Silverman [2009])**.** *If End(E) is an order in a quaternion algebra, E is supersingular.*

In other words, if we can find primes p such that for $E(\mathbb{F}_p)$, End(E) is not commutative we know that E is supersingular. We do this by taking the suggested endomorphism and the Frobenius endomorphism which is defined as follows:

$$F(x, y) = (x^p, y^p).$$

We would like to see when the given endomorphisms of degree 2 (we will call this endomorphism β) do not commute with the Frobenius endomorphism, i.e.:

$$F \circ \beta \neq \beta \circ F.$$

We will only work out the example for curves with j-invariant 8000 as the case with j-invariant -3375 is very much alike.

5.3.1 Curves with j-invariant 8000

We would like to check when F and $\beta : (x, y) \mapsto \left(\alpha^{-2}\left(x + 4 + \frac{2}{x}\right), \alpha^{-3}y\left(1 - \frac{2}{x^2}\right)\right)$ don't commute. We will use Fermat's little theorem ($x^p \equiv x \pmod{p}$ for $x \in \mathbb{F}_p$) and the fact that $(x + y)^p \equiv x^p + y^p \pmod{p}$.

$$\begin{aligned}
(F \circ \beta)(x, y) &= (\beta \circ F)(x, y)\\
F\left(\alpha^{-2}\left(x + 4 + \frac{2}{x}\right), \alpha^{-3}y\left(1 - \frac{2}{x^2}\right)\right) &= \alpha(x^p, y^p)\\
\left((\alpha^{-2})^p\left(x + 4 + \frac{2}{x}\right)^p, (\alpha^{-3})^p y^p\left(1 - \frac{2}{x^2}\right)^p\right) &= \left(\alpha^{-2}\left(x^p + 4 + \frac{2}{x^p}\right), \alpha^{-3}y^p\left(1 - \frac{2}{(x^p)^2}\right)\right)\\
\left((\alpha^{-2})^p\left(x^p + 4^p + \frac{2^p}{x^p}\right), (\alpha^{-3})^p y^p\left(1^p - \frac{2^p}{(x^2)^p}\right)\right) &= \left(\alpha^{-2}\left(x + 4 + \frac{2}{x}\right), \alpha^{-3}y\left(1 - \frac{2}{x^2}\right)\right)\\
\left((\alpha^p)^{-2}\left(x + 4 + \frac{2}{x}\right), (\alpha^p)^{-3}y\left(1 - \frac{2}{x^2}\right)\right) &= \left(\alpha^{-2}\left(x + 4 + \frac{2}{x}\right), \alpha^{-3}y\left(1 - \frac{2}{x^2}\right)\right)
\end{aligned}$$

In other words, End(E) is commutative when $\alpha \equiv \alpha^p \pmod{p}$. This is only true when $\alpha = \sqrt{-2} \in \mathbb{F}_p$, i.e. when -2 is a square in $\mathbb{F}_p^\times$. In other words, End(E) is not commutative when -2 is not a square in $\mathbb{F}_p^\times$. This is what we will use.

First, we look at squares of -2 in $\mathbb{F}_{p^2}$. We know that $\#\mathbb{F}_{p^2} = p^2 - 1$ is divisible by 8 for odd primes p, as $p^2 - 1 \pmod{4} = (p+1)(p-1) \mod 4$. Since p is odd, either $p+1$ or $p-1$ is $2 \pmod{4} = 0 \pmod{2}$, and the other will be $0 \pmod{4} = 4 \pmod{4}$. Hence $(p+1)(p-1) \equiv 0 \pmod{8}$. Hence all elements of order 8 are in $\mathbb{F}_{p^2}^\times$. Let us take the element $\zeta = \frac{1}{2}\sqrt{2} + \frac{1}{2}\sqrt{-2}$. This is indeed an element of order 8, and so $\zeta^4 = 1$. We will show that this is a square root of -2.

$$\begin{aligned}(\zeta - \zeta^{-1})^2 &= \zeta^2 - 2 + \zeta^6 \\ &= \zeta^2(1 + \zeta^4) - 2 \\ &= -2\end{aligned}$$

In order to see when -2 is a square in $\mathbb{F}_p^\times$ as well, we will check when $\zeta - \zeta^1 \in \mathbb{F}_p^\times$. This element is in $\mathbb{F}_p^\times$ if and only if $(\zeta - \zeta^{-1})^p = \zeta - \zeta^{-1}$ as we used earlier. In addition, remember that ζ has order 8, so $\zeta^p = \zeta^{p \pmod{8}}$. There are four possibilities:

1. $p \equiv 1 \pmod{8}$

$$(\zeta - \zeta^{-1})^p = \zeta - \zeta^{-1}$$

   So indeed -2 is a square in $\mathbb{F}_p^\times$ and our curve is not supersingular.

2. $p \equiv 3 \pmod{8}$

$$\begin{aligned}(\zeta - \zeta^{-1})^p &= \zeta^3 - \zeta^5 \\ &= \zeta + \zeta^3 \\ &= \zeta - \zeta^{-1}\end{aligned}$$

   Again we find that -2 is a square and our curve is not supersingular.

3. $p \equiv 5 \pmod{8}$

$$\begin{aligned}(\zeta - \zeta^{-1})^p &= \zeta^5 - \zeta^3 \\ &= -\zeta + \zeta^{-1}\end{aligned}$$

   $-\zeta + \zeta^{-1} \neq \zeta - \zeta^{-1}$ because if it were true, $2(\zeta + \zeta^{-1}) = 0$, meaning that $\zeta = \zeta^{-1} \Rightarrow \zeta^2 = 1$. Hence -2 is not a square and our curve is supersingular.

4. $p \equiv 7 \pmod{8}$

$$(\zeta - \zeta^{-1})^p = -\zeta + \zeta^{-1}$$

   This is the same as the previous case, so we know that again our curve is supersingular.

We see that curves of j-invariant are supersingular over $\mathbb{F}_p$ precisely when $p \equiv 5$ or 7 (mod 8).

We will describe how to choose ℓ to get desirable primes. In the case $p \equiv 5 \pmod 8$, take a prime $\ell \equiv 3 \pmod 4$ such that $p = 2\ell - 1$ is prime. In the case $p \equiv 7 \pmod 8$, take any prime ℓ such that $p = 8\ell - 1$ is prime.

5.4 Are the endomorphisms suitable?

We saw that the curves are supersingular if and only if $\alpha \notin \mathbb{F}_p$. In this case, the endomorphism β will send points of order ℓ with coordinates in $\mathbb{F}_p$ to points of order ℓ with coordinates not in $\mathbb{F}_p$.

5.5 Final note on the algorithm

By theorem 4.3 we know that we either have

$$E(\mathbb{F}_p) \cong \mathbb{Z}/a\ell\mathbb{Z} \Rightarrow aE(\mathbb{F}_p) = \mathbb{Z}/\ell\mathbb{Z}$$

or, for $b, c \in \mathbb{F}_p$ such that $a = bc$,

$$E(\mathbb{F}_p) \cong \mathbb{Z}/b\mathbb{Z} \times \mathbb{Z}/c\ell\mathbb{Z} \Rightarrow aE(\mathbb{F}_p) = \mathbb{Z}/\ell\mathbb{Z}$$

In other words, if we take $p = a\ell - 1$ for an a such as we have determined earlier, we know that $aE(\mathbb{F}_p) = \mathbb{Z}/\ell\mathbb{Z}$, which is exactly what we require.

References

Paulo L.M. Barreto, Ben Lynn, and Michael Scott. Constructing elliptic curves with prescribed embedding degrees. In Stelvio Cimato, Giuseppe Persiano, and Clemente Galdi, editors, *Security in Communication Networks*, volume 2576 of *Lecture Notes in Computer Science*, pages 257–267. Springer Berlin Heidelberg, 2003. ISBN 978-3-540-00420-2. doi: 10.1007/3-540-36413-7_19.

David Freeman. Constructing pairing-friendly elliptic curves with embedding degree 10. In Florian Hess, Sebastian Pauli, and Michael Pohst, editors, *Algorithmic Number Theory*, volume 4076 of *Lecture Notes in Computer Science*, pages 452–465. Springer Berlin Heidelberg, 2006. ISBN 978-3-540-36075-9. doi: 10.1007/11792086_32.

Rudolf Lidl and Harald Niederreiter. *Finite Fields (Encyclopedia of Mathematics and its Applications)*. Cambridge University Press, 1997. ISBN 0521392314.

Alfred J. Menezes, Tatsuaki Okamoto, and Scott A Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field. *IEEE Transactions on Information Theory*, 39(5):1639–1646, 1993.

René Schoof. Nonsingular plane cubic curves over finite fields. *Journal of combinatorial theory, Series A*, 46(2):183–211, 1987.

Joseph Silverman. *The arithmetic of elliptic curves*. Springer-Verlag, New York, 2009. ISBN 9780387094939.

Joseph H Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151. Springer Science & Business Media, 1994.

Lawrence Washington. *Elliptic Curves: Number theory and cryptography*. Chapman & Hall/CRC, Boca Raton, FL, 2008. ISBN 1420071467.

A Magma code for the implementation

Words in blue are names of variables. Words in red are algebraic structures. Lines in green are comments.

```
//We start off by determinging ell. RandomPrime(n)
//gives us a prime of size n bits.

ell:=RandomPrime(200);

//We loop until we find an ell such that 6*ell - 1 is prime

while not IsPrime(6*ell-1)
    do ell:=RandomPrime(200);
end while;

p:=6*ell-1;

//We define several structures here:
//      F_p is the finite field with p elements
//      PR<x> is the polynomial ring over F_p
//      F_p^2 is the finite field with p^2 elements
//      E is the elliptic curve y^2 = x^3 + 1 over F_p
//      E2 is the same curve over F_p2
F_p:=GF(p);
PR<x>:=PolynomialRing(F_p);
F_p2<a>:=ext<F_p | x^2 + x + 1>;
E:=EllipticCurve([F_p!0,F_p!1]);
E2:=EllipticCurve([F_p2!0,F_p2!1]);

//CREATING THE PRIVATE KEY

//Random(E) gives us a random point in E
//As we showed, this will give us a point of order 1 or ell,
//with a point of order 1 being very rare.
P:=6*Random(E);

//Random(ell) gives us a random number less than ell
//We check to make sure it is not zero, then determine Ppub
s:=Random(ell);
while s eq 0
        do s:=Random(ell);
end while;
```

```

Ppub:=s*P;

//Here we determine the ID. Since we are not  that interested
//in the hash functions H1 and H2 I simply chose an integer
//to be the identity. Usually we would have an identity in
//the form of a string of bits which we would then need to
//hash to F_p
ID:=2;

//This is half of the hash function H1, the part that sends
//elements of F_p to E. H1IDy and H1IDx are the x and y
//coordinates of the resulting point respectively
H1IDy:= F_p!ID;
H1IDx:= Root(H1IDy^2 - 1, 3);
QID:= 6*E![H1IDx, H1IDy];

//Determine DID and make it a point in E(F_p2) because
//Magma requires two points to be over the same field for the
//Weil pairing
DID:=s*QID;
DID:=E2!DID;


//SENDING A MESSAGE M
//This is our message M. Again this would usually be a string
//of bits, but for our purposes an integer will suffice.
M:=2500000;

//As we chose F_p2 to be the  extension of F_p over x^2 + x + 1
//our element a turns out to be a nontrivial cube root of unity
//so we may use it for our modified Weil pairing. Note that
//Magma requires we specify the orders of the points for which
//we perform this pairing. In this case, ell.
betaPpub:=E2![a*Ppub[1],-Ppub[2]];
QID:=E2!QID;
gID:=WeilPairing(QID, betaPpub, ell);
r:=Random(ell);
u:=r*P;
Z:= Integers();

//Here we take gID^r and send it to the integers. Since this
```

```
//element lies in F_p2, Magma will not simply convert it.
//However, it can be shown that for gIDr = c + a*d,
//Trace(gIDr) = c - d/2 and
//d = (2a - Trace(gIDr))/(2*a + 1)
//Since we are only interested in this hashing resulting in
//the same value every time, we can simply send gIDr to
// c - d/2 + p*d
//This is in fact an injective homomorphism
gIDr:= gID^r;
gIDrc:= Trace(gIDr);
gIDrd:= (2*gIDr - gIDrc)/(2*a + 1);
H2gIDr:= Z!gIDrc + p*(Z!gIDrd);

//We take the bitwise XOR of M and H2gIDr
v:=BitwiseXor(M, H2gIDr);

//DECRYTING THE MESSAGE

//Here we again apply the modified Weil pairing.
betau:=E2![a*u[1],-u[2]];
hID:=WeilPairing(DID,betau, ell);

//Here we apply the same H2 as previously.
hIDc:= Trace(hID);
hIDd:= (2*hID - hIDc)/(2*a + 1);
H2hID:= Z!hIDc + p*(Z!hIDd);

//We calculate the bitwise XOR of v and H2hID and output
//the resulting m. This m should be the same as our
//original message M.
m:=BitwiseXor(v, H2hID);
m;
```