An Attack on Disguised Elliptic Curves

David Mireles
Mathematics Department
Royal Holloway, University of London
Egham, Surrey, TW20 0EX
United Kingdom
d.mireles-morales@rhul.ac.uk

December 12, 2006

Abstract

We present an attack on one of the Hidden Pairing schemes proposed by Dent and Galbraith. We drastically reduce the number of variables necessary to perform a multivariate attack and in some cases we can completely recover the public key. Our attack relies only on knowledge of the public system parameters.

1 Introduction

The use of pairings in cryptography has had a number of important implications. In [4] the Weil pairing is used to reduce the Discrete Logarithm problem from the group of points of an elliptic curve $\mathbf{E}(\mathbf{F}_q)$ to the multiplicative group of invertible elements of a finite field $\mathbf{F}_{q^n}^*$ for a suitable n. In recent years, pairings for elliptic curves have found more constructive applications (see [1]), which simply stated depend on the fact that they provide some elliptic curves with a gap Diffie-Hellman group structure: a group in which the decision Diffie-Hellman problem is easy, and yet the computational Diffie-Hellman problem remains hard.

In [2], Dent and Galbraith take this construction one step further and explore the idea of Trapdoor Decisional Diffie-Hellman groups: groups for which the knowledge of certain trapdoor information is sufficient to efficiently solve the DDH, whereas solving the DDH without the trapdoor information is believed to be hard. In [2] the authors describe two such constructions, both based on elliptic curves. The first one depends on elliptic curves over the ring $\mathbb{Z}/N\mathbb{Z}$ where $N = pq$ is an RSA moduli (we refer the reader to the original paper for further details). The second construction is based on an idea of Frey [3] that consists of "disguising" elliptic curves. In the next section we will give a detailed description of this construction and then we will proceed to describe an attack on it.

2 Disguising Elliptic Curves

This proposal consists of taking the Weil restriction of an elliptic curve with respect to $\mathbf{F}_{q^n}/\mathbf{F}_q$ and then transforming the group operation equations using a linear change of variables. We will first explain how to obtain multivariate polynomials describing the group law and then we will describe the blinding proccedure using an invertible linear transformation.

Let $\mathbf{E}$ be an elliptic curve defined over a finite field $\mathbf{F}_{q^n}$, and let $P_i = (x_i : y_i : z_i)$ for $i \in \{1, 2\}$ be two points on the curve, then the addition of P_1 and P_2 is given by $P_1 + P_2 = (f_x, f_y, f_z)$ where f_x, f_y, f_z are homogeneous polynomials in $\mathbf{F}_{q^n}[x_{1,2}, y_{1,2}, z_{1,2}]$. Analogously, the doubling formula is given by polynomials in the coordinates of the point with coefficients in $\mathbf{F}_q$.

Take now $\{\alpha_i\}$ an $\mathbf{F}_q$-basis of $\mathbf{F}_{q^n}$. Every element $\underline{x}$ of $\mathbf{F}_{q^n}$ can be described an n-tuple $(x_0, x_1, \ldots, x_{n-1})$. Furthermore, multiplication of two n-tuples is given by n degree two polynomials.

If we describe a represent a point in $\mathbf{E}$ as a $3n$-tuple of elements of $\mathbf{F}_q$, then the addition formula can be given by $3n$ polynomials of degree 8 in the $6n$ variables describing the two points (respectively, point doubling is given by $3n$ polynomials of degree 7). To establish some notation let's say that the addition is given by polynomials f_i, that is

$$(\underline{x}_1 : \underline{y}_1 : \underline{z}_2) + (\underline{x}_2 : \underline{y}_2 : \underline{z}_2) = \left(f_i\left(\underline{x}_1, \underline{y}_1, \underline{z}_1, \underline{x}_2, \underline{y}_2, \underline{z}_2\right)\right)_{i=1}^{3n}.$$

We will also denote the doubling polynomials as $g_i(\underline{x}, \underline{y}, \underline{z})$.

In order to blind the elliptic curve we will choose some matrix $U \in GL_{3n}(\mathbf{F}_q)$, and define the blinded polynomials

$$\left(\tilde{f}_i(\underline{x}_1, \underline{y}_1, \underline{z}_1, \underline{x}_2, \underline{y}_2, \underline{z}_2)\right)_{i=1}^{3n} = U\left(f_i\left(U^{-1}(\underline{x}_1, \underline{y}_1, \underline{z}_1), U^{-1}(\underline{x}_2, \underline{y}_2, \underline{z}_2)\right)_{i=1}^{3n}\right).$$

We will construct the blinded doubling polynomials $\tilde{g}_i$ in a similar fashion and to blind a point $P = (x, y, z)$ we simply write its coordinates as n-tuples with respect to our basis and act on the $3n$-tuple thus obtained with U as $\tilde{P} = U \cdot P$.

The blinded description of the elliptic curve will consist of the polynomials $\tilde{f}_i$ and $\tilde{g}_i$, the image under U of a point on $\mathbf{E}$ and the order of the curve.

In [2] different variants of the scheme are discussed, for instance, it is suggested to take U mapping the XZ space onto itself, both for functionality and implementation convenience.A further variant of the scheme has a more restrictive public key, consisting of a blinded point $\tilde{P} = U \cdot P$ and the blinded version of the doubling and "tranlation by P" formulae, this has the disadvantage that it is not possible to compute arbitrary multiples of a point (see the original paper for the details). Our attack does not include this variant.

The goal of disguising an elliptic curve is to construct a trapdoor DDH group. Thus, an attack on the scheme is any algorithm that allows someone in possesion of the public key to compute the Weil pairing on the curve. Under such considerations, to break the scheme one does not need to recover the original blinding matrix U, all that is needed is a matrix

U' taking our blinded curve to an $\mathbf{F}_{q^n}$ isomorphic curve, in particular, if we start with a different $\mathbf{F}_q$ basis of $\mathbf{F}_{q^n}$, recovering U conjugated by an invertible matrix is enough to break the scheme.

3 The Attack

In this section we describe our attack on the disguised curve scheme. The attack is based on some simple observations coupled with standard linear algebra. For some implementations we are able to completely recover the disguising matrix U (with respect to our $\mathbf{F}_q$ basis).

We first present a general attack that will work on any implementation with basic functionality, this attack alone does not recover U, but will greatly reduce the search space. We then show how to completely recover U in some special cases.

Throughout this section we will fix an $\mathbf{F}_q$ basis $\{\alpha_i\}_1^n$ of $\mathbf{F}_{q^n}$ and whenever we speak of the matrix associated with multiplication by $\lambda \in \mathbf{F}_{q^n}$, it will be with respect to this basis. If $P = (x, y, z)$ is a point in $\mathbf{F}_{q^n}^3$, then $[\lambda]$ will denote the matrix corresponding to multiplication by λ in each coordinate.

For future reference, we present the standard addition formulae for curves given by equations of the form $y^2 = x^3 + Ax + B$:

$$(x_1, y_1, z_1) + (x_2, y_2, z_2) = (f_x, f_y, f_z)$$

where

$$f_x = z_1 z_2 D N^2 - D^3(x_1 z_2 + x_2 z_1) \tag{1}$$

$$f_y = N(z_1 z_2 N^2 - D^2 x_1 z_2 - 2D^2 x_2 z_1) + D^3 x_2 z_1 \tag{2}$$

$$f_z = D^3 z_1 z_2 \tag{3}$$

$$N = y_1 z_2 - y_2 z_1 \quad \text{and} \quad D = x_1 z_2 - x_2 z_1. \tag{4}$$

3.1 Attack 1

In this first attack we assume that we know the blinded image of a point P_0 in $\mathbf{E}(\mathbf{F}_{q^n})$ and blinded doubling and adding formulae. We don't assume knowledge of the size of $\mathbf{E}(\mathbf{F}_{q^n})$ or of the unblinded version of the curve addition formulae. Notice that we can find random points on $\mathbf{E}$ computing random powers of P_0.We can also find different representatives of the same point, for example

$$2 * (P_0 + Q) = 2 * (P_0) + Q + Q.$$

Let P_1 and P_2 be two different blinded representations of the same point. If the unblinded coordinates (in $\mathbf{F}_{q^n}$) of P_1 and P_2 are $(x_1 : y_1 : z_1)$ and $(\lambda x_1 : \lambda y_1 : \lambda z_1)$ respectively, then there is a fixed number s such that the unblinded coordinates of the points $P_1 + Q$ and $P_2 + Q$ will differ by λ^s for every i.This is because the point addition polynomials must be homogeneous in the coordinates of each point. It also tells us how to

compute s: we can read it off from the degree of the addition formulae in each set of variables.

Now let $\{Q_i\}$ be a "large" set of random points. The discussion above tells us that the blinded representations of P_1+Q_i and P_2+Q_i are related by the linear transformation $M = U[\lambda^s]U^{-1}$.

If our set of random points is large ($m > 3n$ would be enough) we can recover the matrix $M = U[\lambda^s]U^{-1}$. The eigenvalues of M will be λ^s and its Galois conjugates. We choose one of them [1] and work with it as λ^s.

Once we have identified λ^s, we can trivially compute the matrix $[\lambda^s]$. We have thus found a restriction in the possible choices for U, as they must satisfy

$$M = U[\lambda^s]U^{-1} \tag{5}$$

and have coefficients in $\mathbf{F}_q$ [2]. There is not a unique solution to equation (5), so further work has to be done to recover U. Notice that not every matrix U satisfying (5) can be used as secret key, as its action on points must also be compatible with the point adding and doubling operations.

If λ is a random element of $\mathbf{F}_{q^n}$, the probability that λ^s does not generate $\mathbf{F}_{q^n}$ over $\mathbf{F}_q$ is bounded above by $s(q-1)/(q^n-1)$, so we can repeat the construction described above until we find λ such that λ^s generates $\mathbf{F}_{q^n}$. It is reasonable to assume that the two representations of the same point P_1 and P_2 that we have constructed differ by a random element of $\mathbf{F}_{q^n}$ as , for instance, the polynomials giving $2P+Q+Q$ and $2(P+Q)$ have different degrees and one is not a multiple of the other, so there is no reason to expect any constraint in the value by which this two projective points differ when P and Q are taken at random.

It would be natural to try to repeat the previous construction using different pairs of points $\{P_1', P_2'\}$ to further narrow down the possibilities for U. However, this wouldn't give us any extra information: suppose that P_1' and P_2' differ by μ and we find a matrix N such that $N = U[\mu]U^{-1}$. If $\mu = \sum a_i\lambda^i$ (we substitute λ^s by λ and use that it generates $\mathbf{F}_{q^n}$) then $[\mu] = \sum a_i[\lambda]^i$ and

$$U[\mu]U^{-1} = U\left(\sum a_i[\lambda]^i\right)U^{-1} = \sum a_i M^i,$$

so every matrix U working for λ would work for μ and we don't get any extra infomation repeating the construction.

Finally notice that the condition $M = U[\lambda^s]U^{-1}$ puts some serious restrictions on the possible U's. If we just represent the coefficients of U as variables in $\mathbf{F}_q$, instead of having $9m^2$ variables ($5m^2$ when the Y-space is mapped separately) we reduce the possibilities to $9m$ variables (resp. $5m$). See Appendix A for further dettails.

[1] Choosing the "wrong" λ amounts to twisting the original elliptic curve with some element σ of the Galois group of $\mathbf{F}_{q^n}$ over $\mathbf{F}_q$, this doesn't affect the attack as the DDH would still be solvable. Equivalently this can be seen as choosing the $\mathbf{F}_q$ basis $\{\alpha_j^\sigma\}$.

[2] See Appendix A for a method to compute the vector space which contains all possible U's.

3.2 Attack 2

To perform this attack we make a series of assumptions on the system implementation. We will assume knowledge of at least one blinded point in the curve, we also assume that the unblinded version of the addition formulae is given by the polynomials we presented above (one could give different addition formulae, i.e., multiplying the standard formulae with a fixed homogeneous polynomial). We will also assume that the XZ (resp. Y) space is mapped onto itself under U (see [2]). We also assume $\mathrm{char}(\mathbf{F}_q) > 2$, although the same techniques can be used for characteristic 2 curves.

In this attack we will first identify the image of the vectors of the form $Z = 0$ under the scrambling matrix U.

Take two $3n$-tuples A_1 and A_2, which correspond to the blinded representation of the points $P_1 = (x_1, y_1, z_1)$ and $P_2 = (x_2, y_2, z_2)$ (points in $\mathbf{F}_{q^n}^3$). If we apply the addition formulae to these two $3n$-tuples we will get a $3n$-tuple corresponding to UP_3 for some point $P_3 = (x_3, y_3, z_3)$. It is clear that P_3 is the result of applying the unblinded addition formula to the points P_1 and P_2 [3].

If we now consider the $3n$-tuple A_1' obtained from A_1 by multiplying the coordinates corresponding to the XZ space by 2 (and which would thus correspond to the point $P_1' = (2x_1, y, 2z_1)$) and add it to A_2 to obtain the $3n$-tuple A_3' (corresponding to $P_3' = (x_3', y_3', z_3')$, a simple analysis of the addition formulae shows that $8z_3 = z_3'$ and $8x_3 \neq x_3'$.

It is now clear that the $3n$-tuple $8A_3 - A_3'$ is the image under U of a point of the form $(X, Y, 0)$. If we repeat this experiment sufficiently many times we can find a basis for the vector space $U\left((X, Y, 0) | X, Y \in \mathbf{F}_{q^n}\right)$. Since the XZ space and the Y space are scrambled onto themselves this is equivalent to finding a basis for the vector space $U\left((X, Y, 0) | X \in \mathbf{F}_{q^n}\right)$.

We will now find the matrix U using only linear algebra.

Consider a $3n$-tuple A_1 corresponding to a point with $z_1 = 0$ (we can identify this point using the previous construction). If we "add" it to another $3n$-tuple A_2 (corresponding to (x_2, y_2, z_2)) and analyze the addition formulae (1), we see that the n-tuple corresponding to the Y coordinate of the addition is given by $U(x_1^3 z_2^4 y_1)$. Notice that this is a linear function in the n-tuple corresponding to Y given by $L = U[x_1^3 z_2^4]U^{-1}$. Remember that from step 1 we have a matrix $M = U[\lambda]U^{-1}$; since λ generates $\mathbf{F}_{q^n}$ over $\mathbf{F}_q$, then there exist $a_i \in \mathbf{F}_q$ such that

$$x_1^3 z_2^4 = \sum_{i=0}^{n-1} a_i \lambda^i,$$

but this implies that

$$L = \sum_{i=0}^{n-1} a_i M^i,$$

turning the process around, using linear algebra we can recover the a_i's since we know M and L. We can now find the value of $x_1^3 z_2^4$ which is given by $\sum_{i=0}^{n-1} a_i \lambda^i$.

[3] It doesn't matter that the points might not be on the elliptic curve, as our interest is only in evaluating the polynomials corresponding to the addition formulae.

If we repeat this computation using A_1' and A_1'' with corresponding X coordinates x_1' and x_1+x_1' we can find the values of $x_1'^3 z_2^4$ and $(x_1+x_1')^3 z_2^4$. Knowing $x_1^3 z_2^4$, $x_1'^3 z_2^4$ and $(x_1+x_1')^3 z_2^4$, taking cube roots we can calculate $x_1/(x_1+x_1')$ and $x_1'/(x_1+x_1')$, from which we can recover x_1,x_1' and z_2^4.

We can now recover U. Knowing how points with $Z=0$ are transformed gives us half the entries of U as follows: if we write vectors v corresponding to the XZ space as $2m$-tuples $v=(\underline{x},\underline{z})$, then writing $U = U_{XZ} \oplus U_Y$ we know how $U_{XZ}\cdot(\underline{x},0)$ behaves, which is equivalent to knowing half the entries of U_{XZ} . Coupling this with the first attack we described, which finds a $2m$ dimensional vector space in which U_{XZ} lies, gives a unique possibility for U_{XZ}.

A Appendix: Some linear algebra

Take M and N two $n\times n$ matrices with entries in $\mathbf{F}_q$. Suppose there is a matrix U in $\mathbf{F}_q$ such that

$$M = U^{-1}NU, \tag{6}$$

and we want to know what are the possible U's with this property.

First we will describe how to compute an n-dimensional $\mathbf{F}_q$ vector space which contains all the possible U's if the characteristic polynomial of M is irreducible. Then we will say how to compute such a vector space for M and N as in our attack.

If the characteristic polynomial of M is irreducible we know that it has n different roots, and that they all lie in $\mathbf{F}_{q^n}$. Therefore, we can find a basis of $\mathbf{F}_{q^n}^n$ formed with eigenvectors of M, all of which have different eigenvalues. Notice that standard linear algebra tells us that the characteristic polynomial of M is the same as that of N, we can therefore find a corresponding basis for N.

It is easy to see that if $M = U^{-1}NU$, then U needs to map an eigenvector of M with eigenvalue λ to an eigenvector of N with the same eigenvalue. That is, if u_λ is a λ-eigenvector of M and v_λ a λ-eigenvector of N, then

$$U\cdot u_\lambda = \mu v_\lambda \tag{7}$$

for some $\mu\in\mathbf{F}_{q^n}^*$.

If we take some $\sigma\in \mathrm{Gal}(\mathbf{F}_{q^n}/\mathbf{F}_q)$ and make it act on equation (7) (remembering that U has coefficients in $\mathbf{F}_q$), we get

$$U\sigma(u_\lambda) = \sigma(\mu)\sigma(v_\lambda)$$

and since $\sigma(u_\lambda)$ is an eigenvector of M with eigenvalue $\sigma(\lambda)$, we conclude that knowing $U\cdot u_\lambda$ is enough to calculate U. Notice that the set of possible U's is in bijection with $\mathbf{F}_{q^n}^\times$, which is a 1-dimensional $\mathbf{F}_{q^n}$ vector space, we will now describe how to compute a n dimensional $\mathbf{F}_q$ basis for it.

Take a $\mathbf{F}_q$-basis $\{\alpha_i\}$ of $\mathbf{F}_{q^n}$. Compute the n $\mathbf{F}_q$-matrices U_i that send v_λ to $\alpha_i u_\lambda$ as we have just described. Then $U=\sum a_i U_i$ for some $a_i\in\mathbf{F}_q$, in other words, $\{U_i\}$ is a $\mathbf{F}_q$ basis for a vector space containing all the U's such that $M=U^{-1}NU$.

In the case of our attack, we have matrices M and N, possibly of size $3n \times 3n$, and the characteristic polynomial is the cube of an irreducible polynomial. The construction of a basis of a vector space containing all the U's is a trivial generalization of the previous case.

The only thing we have to take into account is that the dimension of the eigenspace of each eigenvalue is 3, so all we know is that the image under U of a λ-eigenvector lies in a 3-dimensional $\mathbf{F}_{q^n}$ vector space. Again, if we know how U maps the eigenspace associated to some λ, we can compute the action of U in the whole vector space, so in order to compute a basis for a space containing the U's (notice that now there are non-zero matrices which are not invertible) we just repeat the previous algorithm with 3 eigenvectors instead of just 1 in the eigenspaces of both M and N.

References

[1] Boneh, D., and Franklin, M. K. Identity-based encryption from the weil pairing. In *CRYPTO* (2001), J. Kilian, Ed., vol. 2139 of *Lecture Notes in Computer Science*, Springer, pp. 213–229.

[2] Dent, A., and Galbraith, S. Hidden pairings and trapdoor ddh groups. In *ANTS* (2006), F. Hess, S. Pauli, and M. E. Pohst, Eds., vol. 4076 of *Lecture Notes in Computer Science*, Springer, pp. 436–451.

[3] Frey, G. How to disguise an elliptic curve (weil descent).

[4] Menezes, A. J., Okamoto, T., and Vanstone, S. A. Reducing elliptic curve logarithms to logarithms in a finite field. *IEEE Trans. Inform. Theory 39*, 5 (1993), 1639–1646.