An Attack on Disguised Elliptic Curves

David Mireles Morales *

Mathematics Department
Royal Holloway, University of London
Egham, Surrey, TW20 0EX
UK

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 private 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 [5] for a survey), 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 [1], 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 [1] 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 modulus (we refer the reader to the original paper for further details). The second construction is based on an idea of Frey [2] 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.

* The author wishes to thank Steven Galbraith for his helpful comments throughout the elaboration of this article. The work described in this paper has been supported in part by a scholarship from the Mexican Council of Science and Technology CONACYT and by the European Commission through the IST Programme under Contract IST-2002-507932 ECRYPT. The information in this document reflects only the author's views, is provided as is and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

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 $\mathbf{F}_{q^n}[x_1, y_1, z_1, x_2, y_2, z_2]$. Analogously, the doubling formula is given by polynomials in the coordinates of the point with coefficients in $\mathbf{F}_{q^n}$.

Every element x of $\mathbf{F}_{q^n}$ can be described as an n-tuple $(x_0, x_1, \ldots, x_{n-1}) \in \mathbf{F}_q^n$ with respecto to an $\mathbf{F}_q$-basis $\{\alpha_i\}_1^n$ of $\mathbf{F}_{q^n}$. Furthermore, multiplication of two n-tuples is given by n quadratic polynomials. We will use the notation x to represent both the field element $x \in \mathbf{F}_{q^n}$ and the n-tuple over $\mathbf{F}_q$.

If we describe 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

$$(x_1, y_1, z_2) + (x_2, y_2, z_2) = \left(f_i\left(x_1, y_1, z_1, x_2, y_2, z_2\right)\right)_{i=1}^{3n}.$$

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

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

$$\left(\tilde{f}_i(x_1, y_1, z_1, x_2, y_2, z_2)\right)_{i=1}^{3n} = U\left(f_i\left(U^{-1}(x_1, y_1, z_1), U^{-1}(x_2, y_2, z_2)\right)_{i=1}^{3n}\right).$$

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 $\tilde{P} = U \cdot P$. Throughout the article $\tilde{P}$ will denote the blinded image $U \cdot P$ of P.

The *blinded description* of the elliptic curve will consist of the polynomials $\tilde{f}_i$ and $\tilde{g}_i$, the image $\tilde{P}_0$ under U of a point P_0 on $\mathbf{E}$ and the order of the curve.

In [1] 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 "translation 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 apply to 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 possession of the public key to compute a bilinear 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, starting with a different $\mathbf{F}_q$-basis of $\mathbf{F}_{q^n}$ corresponds to conjugating U by an invertible matrix, and 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 variants 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 variant with basic functionality; this attack alone does not recover U, but will greatly reduce the search space. Building upon our first attack, we then show a second attack that completely recovers U in some special cases. This second attack can be seen as a warning against careless implementations.

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 in $\mathrm{GL}_n(\mathbf{F}_q)$ 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 in $\mathrm{GL}_{3n}(\mathbf{F}_q)$ 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

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

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

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

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

Note that there is not a unique set of polynomials (f_x, f_y, f_z) giving addition formulae for the curve $\mathbf{E}$. For example, one can multiply the polynomials by a given homogeneous polynomial in the coordinates of one of the points and still get addition formulae that work generically.

3.1 Attack 1

In this first attack we assume that we know the blinded image $\tilde{P}_0 = UP_0$ 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 $\mathbf{E}$ simply by computing random multiples of P_0.

In our attack we will need the image under U of two different projective representatives of the same point. We can find such a pair of points in several ways, for example, taking two random points $\tilde{P}$ and $\tilde{Q}$, and performing the operations

$$\tilde{P}_1 = 2(\tilde{P} + \tilde{Q})$$

and

$$\tilde{P}_2 = 2\tilde{P} + \tilde{Q} + \tilde{Q}.$$

It is reasonable to assume that the two representations P_1 and P_2 of the same point differ by a random element of $\mathbf{F}_{q^n}$ as the polynomials giving $2P + Q + Q$ and $2(P + Q)$ have different degrees and one is not a multiple of the other. There is therefore no reason to expect any constraint in the value by which these two projective points differ when P and Q are taken at random, as the proportionality constant by which P_1 and P_2 differ is the value of a non-constant rational function evaluated in two random points P and Q on $\mathbf{E}$.

Fix polynomials f_x, f_y and f_z giving projective addition formulae for the elliptic curve $\mathbf{E}$. That is, given two points P_1 and P_2 on $\mathbf{E}$, then a projective point P_3 such that $P_3 = P_1 + P_2$ can be found as

$$P_3 = (f_x, f_y, f_z)(P_1, P_2).$$

If P_1 and P_2 are two different projective representatives of the same point, with coordinates $P_1 = (x_1, y_1, z_1)$ and $P_2 = (\lambda x_1, \lambda y_1, \lambda z_1)$, for every point Q the projective coordinates of $P_1 + Q$ and $P_2 + Q$ will be related by

$$P_1 + Q = (x_3, y_3, z_3), \quad P_2 + Q = (\lambda^s x_3, \lambda^s y_3, \lambda^s z_3),$$

for a fixed integer s. For any triple of polynomials (f_x, f_y, f_z) giving generic addition formulae on the curve, the polynomials (f_x, f_y, f_z) have to be homogeneous in the coordinates of the first and second points. The degree of the formulae in the variables corresponding to the first point will give us the value of s.

For the attack to succeed we need λ^s to generate $\mathbf{F}_{q^n}$. If λ is a random element of $\mathbf{F}_{q^n}$, it is easy to prove that the probability that λ^s does not generate $\mathbf{F}_{q^n}$ over $\mathbf{F}_q$ is bounded above by $s(q-1)/(q^n-1)$, which is very small in practice. If we are unlucky then the attack can be repeated for different pairs of points $(\tilde{P}_1, \tilde{P}_2)$ until we find λ such that λ^s generates $\mathbf{F}_{q^n}$. We will shortly describe how to determine if this is the case.

The previous discussion still applies for blinded points and blinded addition formulae. Notice that given the way the blinded addition formulae were obtained, we have that

$$\tilde{P} + \tilde{Q} = \widetilde{(P + Q)}.$$

Let $\tilde{P}_1 = U \cdot P_1$ and $\tilde{P}_2 = U \cdot P_2$ be the blinded version of the points P_1 and P_2 in the previous paragraphs. For a blinded point $\tilde{Q}$, the coordinates of $\widetilde{(P_1 + Q)}$ and $\widetilde{(P_2 + Q)}$ will differ by the matrix $M = U[\lambda^s]U^{-1}$.

Now let $\{\tilde{Q}_i\}$ be a set of $m > 3n$ random blinded points. The discussion above tells us that for $1 \leq i \leq m$ we have

$$\widetilde{(P_2 + Q_i)} = U[\lambda^s]U^{-1}\widetilde{(P_1 + Q_i)}$$

If our set of random points is large enough, then we can recover the matrix $M = U[\lambda^s]U^{-1}$ simply by computing the sets $\{\tilde{P}_1 + \tilde{Q}_i\}_i$ and $\{\tilde{P}_2 + \tilde{Q}_i\}_i$, and finding the matrix M transforming one into the other. In this case note that the matrix M depends only upon $\tilde{P}_1$ and $\tilde{P}_2$.

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 $[\lambda^s]$ for our fixed $\mathbf{F}_q$-basis of $\mathbf{F}_{q^n}$. We have thus found a restriction in the possible choices for U, as U must satisfy

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

and have coefficients in $\mathbf{F}_q$. 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.

It would be natural to try to repeat the previous construction using different pairs of points $\{\tilde{P}_1', \tilde{P}_2'\}$ instead of $\{\tilde{P}_1, \tilde{P}_2\}$ to further narrow down the possibilities for U. However, this wouldn't give us any extra information: suppose that $P_1' = (x_1, y_1, z_1)$ and $P_2' = (\mu x_1, \mu y_1, \mu z_1)$ differ by μ, then we can find the corresponding matrix N transforming the set $\{\widetilde{(P_1' + Q_i)}\}$ into $\{\widetilde{(P_2' + Q_i)}\}$, giving us the following condition on U:

$$N = U[\mu^s]U^{-1}.$$

If $\mu^s = \sum a_i(\lambda^s)^i$ (we use that λ^s generates $\mathbf{F}_{q^n}$) then $N = \sum a_i M^i$, and it follows that for a given matrix U if $U[\lambda^s]U^{-1} = M$, then automatically

$$N = U[\mu^s]U^{-1},$$

so every matrix U satisfying equation (5) for $[\lambda^s]$ and M would work for $[\mu^s]$ and N 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 Us. If we wanted to perform a multivariate attack against the scheme representing 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. $5m$) as we now describe. To find a basis for a vector space in which the element of U must lie one rewrites equation (5) as

$$MU = U[\lambda^s]. \tag{6}$$

[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 $\{\alpha_j^\sigma\}$.

This last equation gives us the relations that the entries of U must satisfy. To see that the dimension of the vector space of matrices U satisfying equation (6) is $9m$ one can argue as follows:

If we diagonalize M and $[\lambda^s]$ over some extension $\mathbf{F}_{q^r}$ of $\mathbf{F}_q$ as $M_D = D_1^{-1} M D_1$ and $M_D = D_2^{-1}[\lambda^s] D_2$, it is easy to see that the set of U's satisfying (6) and the set of matrices V satisfying

$$M_D V = V M_D, \tag{7}$$

are related by multiplication on the left by D_1 and on the right by D_2. In particular they have the same dimension as $\mathbf{F}_{q^r}$-vector spaces. Since the matrix $[\lambda^s]$ has as eigenvalues all the Galois conjugates of λ^s, each with multiplicity 3, the matrix M_D has m different values in the diagonal, each repeated 3 times. It is now easy to see that the vector space of matrices V satisfying (7) has dimension $9m$ as $\mathbf{F}_{q^r}$-vector space, since it is necessary and sufficient that V maps the 3-dimensional eigenspaces corresponding to a given eigenvalue onto themselves.

To prove that the space of matrices U satisfying (6) defined over $\mathbf{F}_p$ also has dimension $9m$, it suffices to see that the space of matrices U satisfying (6) over $\mathbf{F}_{q^r}$ has dimension $9m$ and mention that using the fact that the conditions for U are defined over $\mathbf{F}_q$, a standard argument (see for example [3] Proposition A.2.2.10) proves that there is a basis for the $\mathbf{F}_{q^r}$-vector space with elements defined over $\mathbf{F}_q$. An analogous argument proves that if the XZ and Y-spaces were mapped onto themselves then the dimension of the vector space of matrices satisfying (6) is $5m$.

3.2 Attack 2

As mentioned before, there are several variants of the disguised curve proposal in [1]. We now show how to improve the previous attack for one of these variants. 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 in equations (1)-(4) above (as we have mentioned, one could give different addition formulae). We will also assume that the XZ (resp. Y)-space is mapped onto itself under U (see [1]) and that $\mathrm{char}(\mathbf{F}_q) > 2$, although the same techniques can be used for characteristic 2 curves. Since U maps the XZ and Y-spaces separately, we will write $U = U_{XZ} \oplus U_Y$, where U_{XZ} denotes the action of U on the XZ-space and U_Y gives the action of U on the Y-space.

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

Take two random $3n$-tuples $\tilde{A}_1$ and $\tilde{A}_2$, corresponding to the blinded representation of the vectors [2] $A_1 = (x_1, y_1, z_1)$ and $A_2 = (x_2, y_2, z_2)$ in $\mathbf{F}_{q^n}^3$. If we apply the blinded addition formulae to $\tilde{A}_1$ and $\tilde{A}_2$ we will get a $3n$-tuple

[2] 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.

$\tilde{A}_3 = UA_3$ for some vector $A_3 = (x_3, y_3, z_3)$. It is clear that A_3 is the result of applying the unblinded addition formulae to the points A_1 and A_2.

If we now consider the $3n$-tuple $\tilde{A}'_1$ obtained from $\tilde{A}_1$ by multiplying the coordinates corresponding to the XZ-space by 2 (and which would thus correspond to the vector $A'_1 = (2x_1, y, 2z_1)$) and "add" it to $\tilde{A}_2$ to obtain the $3n$-tuple $\tilde{A}'_3$ (corresponding to $A'_3 = (x'_3, y'_3, z'_3)$), a simple analysis of the addition formulae shows that $8z_3 = z'_3$ and $8x_3 \neq x'_3$.

We now have that

$$8\tilde{A}_3 - \tilde{A}'_3 = U(8A_3 - A_3) = U(8x_3 - x'_3, 8y_3 - y'_3, 0)$$

It is now clear that the $3n$-tuple $8\tilde{A}_3 - \tilde{A}'_3$ 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 $U\{(x, y, 0)|x, y \in \mathbf{F}_{q^n}\}$. Since the XZ-space and the Y-space are scrambled onto themselves this is equivalent to finding a basis for the vector space $U\{(x, 0, 0)|x \in \mathbf{F}_{q^n}\}$.

We will now find the matrix U using only linear algebra. Consider a $3n$-tuple $\tilde{A}_1$ corresponding to a point $A_1 = (x_1, y_1, 0)$ (we can identify this point using the previous construction). If we "add" it to another $3n$-tuple $\tilde{A}_2$ (corresponding to $A_2 = (x_2, y_2, z_2)$) and analyze the addition formulae (1)-(4), we see that the Y-coordinate of the addition of A_1 and A_2 is $x_1^3 z_2^4 y_1$, that is, the n-tuple corresponding to the Y-coordinate of the addition of

$$\tilde{A}_1 + \tilde{A}_2 = \widetilde{(A_1 + A_2)}$$

of $\tilde{A}_1$ and $\tilde{A}_2$ is given by $U_Y(x_1^3 z_2^4 y_1)$. Notice that this is a linear function in the n-tuple corresponding to the coefficients of the Y-coordinate given by the matrix $L = U_Y[x_1^3 z_2^4]U_Y^{-1}$. If we use vectors A_1 and A_2 where the values of x_1, x_2, y_2, z_2 are fixed (albeit unknown) elements of $\mathbf{F}_{q^n}$ but y_1 is represented as a formal n-tuple (ie. by variables), we can recover the matrix L.

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 $\sum_{i=0}^{n-1} a_i \lambda^i$.

If we repeat this computation using $\tilde{A}'_1$ and $\tilde{A}''_1$ 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. Notice that we started

with a point $\tilde{A}_1 = U(x_1, y_1, 0)$ for which we have now found the value of x_1, this will give us information on U, as we can read $U_{XZ}(x_1, 0)$, directly from $\tilde{A}_1$. Since we also find the value of x_1', an analogous condition is satisfied for the point $\tilde{A}_1'$

We can now recover U. Knowing how some points with $z = 0$ are transformed gives us information about U as follows: if we write vectors v corresponding to the XZ-space as $2m$-tuples $v = (x, z)$, then writing $U = U_{XZ} \oplus U_Y$ we know how $U_{XZ} \cdot (x, 0)$ behaves for at least two values of x, which is equivalent to knowing a vector space of codimension at least $4m$ on which U_{XZ} lies. Coupling this with the first attack we described, which finds a $4m$-dimensional vector space in which U_{XZ} lies, gives generically a unique possibility for U_{XZ}.

4 Conclusions

We have cryptanalysed the hidden pairing scheme of [1] based on disguising an elliptic curve. Our attacks show that to obtain a secure system one would have to massively increase the memory requirements of the public keys in the proposal of [1]. Our results do not apply to the proposal of Frey since [2] does not specify a method to compute the group law on an elliptic curve.

References

1. 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.
2. Frey, G. How to disguise an elliptic curve (Weil descent). *The 2nd Elliptic Curve Cryptography Workshop (ECC '98)* (1998). Available from http://www.cacr.math.uwaterloo.ca/conferences/1998/ecc98.frey.ps.
3. Hindry, M., and Silverman, J. H. *Diophantine geometry: An introduction*, vol. 201 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.
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.
5. Paterson, K. G. Cryptography from pairings. In *Advances in elliptic curve cryptography*, I. Blake, G. Seroussi, and N. Smart, Eds., vol. 317 of *London Math. Soc. Lecture Note Ser.* Cambridge Univ. Press, Cambridge, 2005, pp. 215–251.