Isogeny cordillera algorithm to obtain cryptographically good elliptic curves

J. Miret[1] **D. Sadornil**[2] **J. Tena**[3] **R. Tomàs**[1] **M. Valls**[1]

[1]Dept. de Matemàtica. Universitat de Lleida (Spain).
Email: {miret,rosana,magda}@eps.udl.es
[2]Dept. de Matemáticas. Universidad de Salamanca (Spain).
Email: sadornil@usal.es
[3]Dept. de Álgebra, Geometría y Topología. Universidad de Valladolid (Spain).
Email: tena@agt.uva.es

Abstract

The security of most elliptic curve cryptosystems is based on the intractability of the Elliptic Curve Discrete Logarithm Problem (ECDLP). Such a problem turns out to be computationally unfeasible when elliptic curves are suitably chosen. This paper provides an algorithm to obtain cryptographically good elliptic curves from a given one. The core of such a procedure lies on the usage of successive chains of isogenies, visiting different volcanoes of isogenies which are located in different ℓ–cordilleras.

Keywords: Cryptography; Elliptic Curves; Isogenies.

1 Introduction

During the last decades, the cryptographic community has paid significant attention to the usage of elliptic curves in the design of several security protocols (Koblitz 1987, Menezes 1993, Blake et al. 1999).

Such an increasing interest is mainly due to two aspects: on the one hand, solving the Discrete Logarithm Problem over the group of points of an elliptic curve (ECDLP) is computationally harder than solving it over the multiplicative group of a finite field (DLP) (indeed the Index–Calculus method can be applied over finite fields with subexponential complexity, but can not be implemented over elliptic curves (Silverman et al. 1998)). As a consequence, the size of the group can be significantly reduced and, hence, it permits the usage of shorter keys and parameters. This aspect is specially relevant when being used in hardware devices, which present memory and computation restrictions (Hankerson et al. 2003).

On the other hand, long–term–purpose cryptosystems require periodic refreshment of the setup of the systems. In this sense, in DLP–based cryptosystems the underlying finite field must be changed, while, in ECDLP–based cryptosystems, different curves can be chosen each time, without necessarily changing the finite field. Again, these property turns out to be interesting for hardware implemented algorithms, since the arithmetic of the processor can remain unchanged.

Nevertheless, not every elliptic curve offers the same security level, so curves should be carefully chosen when updating the systems. Cryptographically good elliptic curves should fit several conditions. Concerning its cardinal, it should have a prime divisor which was big enough to prevent the Pohlig–Hellman attack (Pohlig et al 1978). Moreover, in cryptosystems based on intractability of ECLDP, the curve should also be non–supersingular and with trace different to one (otherwise, the ECDLP could be reduced to the DLP over the multiplicative group of a small–degree extension of the base field) (Hankerson et al. 2003). Lately, supersingular curves are being used in cryptographic protocols based on pairings (Barreto et al 2000).

As a consequence, one approach to obtain good curves would be obtaining new ones from a given good one $E/\mathbb{F}_q$, while maintaining the same properties as the original curve. Even companies offering security services may want a reasonably large amount of such curves in *stock*, which could be offered to its customers when necessary.

Finding out isomorphic curves to $E/\mathbb{F}_q$ would indeed provide curves with the same cardinal (and hence, pressumibly same security). But, since these curves can be considered essentially the same curve, they not become, in fact, a valid alternative. More generally, it is well known (Husemöller 1987) that two elliptic curves over $\mathbb{F}_q$ have the same cardinal if, and only if, they are *isogenous*. That is to say, there exists a rational map that preserves the infinity point. Then, the cardinal of the kernel of such a map is called the *degree of the isogeny*, which is known to be bounded by a given threshold (Galbraith 1999).

Therefore, obtaining every isomorphism class of curves with the same cardinal as $E(\mathbb{F}_q)$ could be done by obtaining all the rational isogenies of $E/\mathbb{F}_q$, with degree under that bound. In addition, notice that only prime degree isogenies need to be considered, since each isogeny splits in isogenies with prime degrees.

Then, given an elliptic curve one can generate successive ℓ–isogenous curves. The curves obtained by means of this procedure are all isogenous, and can be represented by means of a graph structure called ℓ–*volcano* (Kohel 1996, Fouquet et al. 2002). Its nodes are isomorphism classes of elliptic curves, and each edge represents an ℓ–degree isogeny between neighbour curves. But, not every curve isogenous to $E/\mathbb{F}_q$ will necessarily belong to that volcano (however, it would hold for supersingular curves, but these ones are not interesting for ECDLP–based cryptography). Then, the set of every ℓ–volcanoes of curves with the same cardinal is denoted as ℓ–cordillera.

This work has been partially supported by grants TIC2003–09188, TIC2003–00950 and MTM2004–008076 from Spanish MCyT.

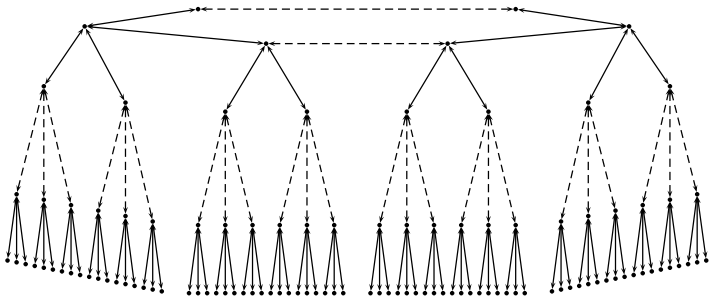

Figure 1: Volcano of 3–isogenies

So, this paper presents a procedure which permits obtaining every elliptic curve with the same cardinal than a given one, defined over the same finite field. This algorithm takes benefit of the fact that the curves in volcanoes of a ℓ_i–cordillera can also appear in some other ℓ_j–cordillera. Hence, once the curves in the ℓ_i–volcano of $E/\mathbb{F}_q$ are obtained, new ones can come out by studying, respectively, their ℓ_j–volcanoes (one algorithm to generate the curves of a 2–volcano is presented in (Miret et al. 2006)).

The remainder of the paper is organized as follows. Section 2 consists of a brief introduction to the computation of isogenies, as well as the construction of volcanoes and cordilleras. Section 3 presents in detail the algorithm proposed in the paper, whose behavior is also enlightened by means of some examples. Finally, Section 4 stands out the main conclusions, as well as suggests future work in this area.

2 Volcanoes of ℓ–isogenies of elliptic curves

The main concepts related to the study of isogenies of elliptic curves are given in this section. Likewise, the structure of a volcano of isogenies together with its features and properties (Fouquet et al. 2002) are also introduced.

2.1 Isogenies

Given an elliptic curve E over $\mathbb{F}_q$, determining an isogenous curve to that one is a feasible problem, under an algebraic point of view. Indeed, given a subgroup $G \subseteq E(\mathbb{F}_q)$, for instance the cyclic subgroup $\langle P \rangle$ generated by a point $P \in E(\mathbb{F}_q)$, a rational map $\mathcal{I}$ can be constructed, from the curve E and with kernel G. Then the quotient E/G is a new elliptic curve E', which is called *isogenous curve* of E under isogeny $\mathcal{I}$. Besides, the degree of the isogeny is defined as the cardinal of the subgroup G. In general, given two elliptic curves, E and E', it is said that they are isogenous curves if there exists a rational map between them that sends the infinity point in E to the infinity point in E'.

More concretely, given an elliptic curve of equation $E/\mathbb{F}_q:\ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, the coefficients of its isogenous curve of kernel G

$$E'/\mathbb{F}_q:\ y^2 + a'_1xy + a'_3y = x^3 + a'_2x^2 + a'_4x + a'_6,$$

can be straightforwardly obtained by means of Vélu formulae (Vélu 1971):

$$\begin{array}{l} a'_1 = a_1,\ a'_2 = a_2,\ a'_3 = a_3, \\ a'_4 = a_4 - 5t, \\ a'_6 = a_6 - b_2t - 7w, \end{array}$$

with

$$\begin{cases} t = \sum\limits_{T \in \mathcal{S}_G} t(T), \\ w = \sum\limits_{T \in \mathcal{S}_G} \left(u(T) + x(T)t(T)\right), \end{cases}$$

being S_G a system of representatives of the orbits of G under the action of the subgroup {-1, 1},

$$\begin{array}{rcl} t(T) & = & \begin{cases} 3x(T)^2 + 2a_2x(T) + a_4 - a_1y(T), \\ \qquad \text{if } T \in G \cap E[2] \\ 6x(T)^2 + b_2x(T) + b_4, \\ \qquad \text{if } T \in G \setminus E[2] \end{cases} \\ u(T) & = & 4x(T)^3 + b_2x(T)^2 + 2b_4x(T) + b_6, \end{array}$$

and the coefficients b_i are defined in the following way:

$$b_2 = a_1^2 + 4a_2, \quad b_4 = a_1a_3 + 2a_4, \quad b_6 = a_3^2 + 4a_6.$$

2.2 Isogeny volcanoes and cordilleras

Given an ordinary elliptic curve $E/\mathbb{F}_q$ and an ℓ–isogeny $\mathcal{I} : E \longrightarrow E'$, Kohel (Kohel 1996) introduced the notion of direction of the isogeny, according to the relation between the endomorphism rings $\mathcal{O}$ and $\mathcal{O}'$ of the curves. Actually, Kohel shows that $[\mathcal{O} : \mathcal{O}'] = 1, \ell$ or $1/\ell$, and depending on each case, it is said that the isogeny $\mathcal{I}$ is *horizontal, descending* or *ascending*, respectively. These notions of direction can be exploited to represented isogenous curves by means of graph structures.

Then, an ℓ–volcano (see (Fouquet et al. 2002)) is a directed graph whose nodes are isomorphism classes of elliptic curves and whose edges represent ℓ–isogenies among them. These graphs consist of a unique cycle at the top level, called *crater*, and from each node of the cycle hang $\ell - 1$ trees which are ℓ–ary complete, except in the case where the volcano is reduced to the crater. The leaves of these trees are located at the same level, which form what is called as the *floor* of the ℓ–volcano, while the remainding nodes of each tree constitute the volcanoside. Each node of the ℓ–volcano (except the leaves) has $\ell + 1$ edges. More precisely, nodes in the volcanoside have one ascending isogeny and ℓ descending ones, while nodes on the crater have two horizontal isogenies and $\ell - 1$ descending ones. The structure of an ℓ–volcano for $\ell = 3$ is given in Figure 1.

Given an elliptic curve E, its volcano of ℓ–isogenies will be denoted by $V_\ell(E)$. Taking into account that, for a given prime ℓ, the elliptic curves over a finite field $\mathbb{F}_q$ with the same cardinal can be distributed in several ℓ–volcanoes, the set of all these connex components will be named ℓ–*cordillera*.

The height of the volcano $V_\ell(E)$ associated to a curve $E/\mathbb{F}_q$ can be obtained considering the conductor f of the order $\mathbb{Z}[\pi]$, being π the endomorphism of Frobenius of the curve. More precisely, one can deduce that $h(V_\ell(E)) = v_\ell(f)$, that is the height of the volcano coincides with the ℓ–adic valuation of the integer f. Nevertheless, there are efficient algorithms to determine the height of a volcano which do not need to obtain f (see (Fouquet et al. 2002, Miret et al. 2006)).

Concerning the study of the connex components of an ℓ–cordillera, we can take advantage of next result.

Proposition 1 *Let ℓ and ℓ' be prime numbers. Then,*

i) All connex components of an ℓ–cordillera of elliptic curves have the same height.

ii) Elliptic curves which are in different levels of an ℓ–volcano must belong to different connex components of any ℓ'–cordillera, when $\ell' \neq \ell$.

Proof:

All curves with the same cardinal determine the same conductor of the order generated by their endomorphism of Frobenius. So the height of all volcanoes corresponding to these curves will be the same.

Regarding case *ii)* notice that if E and E' are two curves which belong to two different volcanoes V and V' of ℓ and ℓ'–isogenies, respectively, then the endomorphism rings satisfy $[\mathcal{O} : \mathcal{O}'] = \ell^n$ and $[\mathcal{O} : \mathcal{O}'] = (\ell')^{n'}$. Therefore, both relations can only hold when $n = n' = 0$. Consequently, E and E' must be located at a same level in V, as well as, also at a same level in V'.

3 Procedure to obtain isogenous curves

Let $\ell_1 < \ell_2 < .... < \ell_{lim}$ be prime numbers (different from the characteristic p of the field) so that the curve $E/\mathbb{F}_q$ admits ℓ_i–isogenies, i.e., for which $E/\mathbb{F}_q$ has a rational subgroup G of order ℓ_i generated by a point P of order ℓ_i. The algorithm that we present generates all the ℓ_i–isogenous curves of E until a threshold given prime ℓ_{lim}.

Then, given an initial curve E, this algorithm proceeds as follows. Firstly, its volcanoes $V_{\ell_1}(E)$ and $V_{\ell_2}(E)$ are completely constructed. Then, for each curve E' found in the second volcano and not contained in the first one, the volcano of ℓ_1–isogenies $V_{\ell_1}(E')$ is also obtained. Frequently, in these new ℓ_1–volcanoes will appear nodes that do not belong to $V_{\ell_2}(E)$. Hence, for each of them, its corresponding ℓ_2–volcano is also generated. Proceeding this way, different connex components of the ℓ_1 and ℓ_2 cordilleras are subsequently constructed. Once every curve appears in the ℓ_1–cordillera as well as in the ℓ_2–cordillera, the procedure goes on obtaining the ℓ_3–volcano $V_{\ell_3}(E)$. The algorithm proceeds similarly until all the ℓ_i–isogenies have been calculated, without obtaining new nodes, for ℓ_i ranging from ℓ_1 to ℓ_{lim}.

3.1 Algorithm

The pseudo–code of the algorithm sketched above is the following:

```
ALGORITHM All_Isogenous

INPUT
  E:  Elliptic Curve
  ℓ_lim:  Prime number
  L_E:  List of primes {ℓ_1, ℓ_2,..., ℓ_lim}
          in ascending order
          for which E has ℓ_i-isogenies

OUTPUT
  Isogenous:  List of elliptic curves
           with same cardinal as E

VARIABLES:
  ℓ, ℓ_act:  Prime numbers
  E', E'':  Elliptic Curves
  V:  List of volcano nodes
  new_curves:  Boolean
  For all Prime ℓ ∈ L_E
    Untreated[ℓ]:  List of elliptic curves
  EndFor

BEGIN ALGORITHM
  Isogenous := {E}
  For all Prime ℓ s.t.  ℓ ∈ L_E
    Untreated[ℓ] := ∅
  EndFor
  ℓ_act := Get_ℓ_act(L_E)
  Untreated[ℓ_act] := Add(E)
  new_curves := False
  While Not Empty(Untreated[ℓ_act])
    E' := Top(Untreated[ℓ_act])
    V := ℓ_act-volcano(E')
    For all elliptic curve E'' ∈ V
      If E'' ∈ Isogenous
        Untreated[ℓ_act] := Remove(E'')
      Else
        Isogenous := Add(E'')
        new_curves := True
        For all Prime ℓ ∈ L_E
          If ℓ ≠ ℓ_act
            Untreated[ℓ] := Add(E'')
          EndIf
        EndFor
      EndIf
    EndFor
    If new_curves
      ℓ_act := Get_ℓ_act(L_E)
      new_curves := False
    EndIf
    While Empty(Untreated[ℓ_act]) & ℓ_act ≤ ℓ_lim
      ℓ_act := Next(L_E)
    EndWhile
  EndWhile
  Return Isogenous
END ALGORITHM
```

This algorithm takes, as input values, the initial elliptic curve E, over $\mathbb{F}_q$, the prime until which we want to construct volcanoes and, finally, a list L_E with some prime factors of the cardinal of E. As output parameters, this algorithm returns the list of elliptic curves isogenous to E, whose degree is a composition of primes in L_E. These curves belong to the volcanoes obtained in the different ℓ_i–cordilleras.

In the algorithm, the list `Untreated[`ℓ_i`]` is used to store curves whose ℓ_i–volcano has not been constructed. On the other hand, the function `Top(Untreated[`ℓ_i`])` returns the first value of the list `Untreated[`ℓ_i`]`. Function ℓ_{act}`-volcano(`E`)` returns all nodes in the ℓ_{act}–volcano of E.

	Isogenous	ℓ_{act}	Untreated[2]	Untreated[3]	Untreated[5]
0	A	2	**A**	A	A
1	ABCD	3	$\emptyset$	**A**BCD	ABCD
2	ABCDE	2	**E**	BCD	ABCDE
3	ABCDEFGH	3	$\emptyset$	**B**CDFGH	ABCDEFGH
4	ABCDEFGH	3	$\emptyset$	**C**DGH	ABCDEFGH
5	ABCDEFGH	3	$\emptyset$	**D**H	ABCDEFGH
6	ABCDEFGH	5	$\emptyset$	$\emptyset$	**A**BCDEFGH
7	ABCDEFGHIJ	2	***I****J*	IJ	BCDFGH
8	ABCDEFGHIJ	3	$\emptyset$	**I**J	BCDFGH
9	ABCDEFGHIJ	5	$\emptyset$	$\emptyset$	**B**CDFGH
10	ABCDEFGHIJ	7	$\emptyset$	$\emptyset$	$\emptyset$

Table 1: Behaviour of the algorithm

3.2 Algorithm behaviour

In order to illustrate the behaviour of the algorithm, it is presented below how it would proceed in a hypothetical case (build up to show the performance step by step). Let {A, B, C, D, E, F, G, H, I, J } be elliptic curves with the same cardinal, which are distributed along the following cordilleras:

2–Cord.: {{A, B, C, D}, {E, F, G, H},{I, J}}
3–Cord.: {{A, E}, {B, F}, {C, G}, {D, H},{I, J}}
5–Cord.: {{A, E, I, J}, {B, C, D, F, G, H}}
⋮ ⋮

Let the input of the algorithm be elliptic curve A and $L_E = \{2, 3, 5\}$. Hence, $\ell_{act} = 2$ and $\ell_{lim} = 5$, so we will construct volcanoes of 2, 3 and 5 isogenies. With these values, our algorithm will work as shown in Table 1.
Notice that, in step 0, the list of isogenous curves has been initialized with the curve A. Then the algorithm generates its 2–volcano to obtain the curves 2–isogenous of A.

Those new curves obtained by means of the construction of new ℓ_i–volcanoes will be added to the list `Isogenous` at each step. The curves that are found in some ℓ_j–volcano, whose ℓ_i–volcano has not been constructed yet, are added to the list `Untreated`$[\ell_i]$. Therefore, in the first iteration, the 2–volcano of A is constructed. Then, the new curves obtained in $V_2(A)$ are B, C, D. Since they still do not belong to list `Isogenous`, they are also added to `Untreated[3]` and `Untreated[5]`.

Likewise, those curves in the ℓ_i–volcano that appear also in `Untreated`$[\ell_i]$ are eliminated from `Untreated`$[\ell_i]$. Thus, the curve considered in every iteration is the first one in the non–empty list `Untreated`$[\ell_i]$, where l_i is the smallest possible value. The algorithm proceeds similarly until all the `Untreated` lists are empty.

3.3 Experimental example

The previous algorithm has been implemented using the computer algebra system MAGMA (see (MAGMA-Handbook)). We show below a small example, considering the field $\mathbb{F}_{317}$ and the curves with cardinal 312. The curves are taken under the following model

$$E_{a,b}/\mathbb{F}_p : y^2 + axy + by = x^3,$$

with discriminant $\Delta = b^3(a^3 - 27b) \neq 0$. Every isomorphism class is univocally represented by the curve $E_{1,\lambda}/\mathbb{F}_p$ (being $\lambda = \frac{b}{a^3}$), except when $a = 0$, in which case the representative curve is $E_{0,1}/\mathbb{F}_p$. For the sake of simplicity, they can be parameterized in terms of λ as E_λ. Case $E_{0,1}$ can be denoted as E_0.

In this example, the input curve has been $E_{316}/\mathbb{F}_{317}$ and $L_E = \{2,3\}$. The cordilleras of volcanoes of 2 and 3 isogenies obtained successively by means of the algorithm are the following ones:

2–Cord.:{{E_{316},E_{259},E_{246},E_{205},E_{255},E_{284}},
{E_{137},E_{206},E_{36},E_{46},E_{119},E_{290}}
{E_{287},E_{87},E_{187},E_{250},E_{196},E_{70}},
{E_{149},E_{116},E_{51},E_{42},E_{200},E_{148}}}

3–Cord.:{{E_{316},E_{137},E_{287},E_{149}},
{E_{259},E_{206},E_{87},E_{116},E_{246},E_{36},E_{187},E_{51}},
{E_{205},E_{46},E_{250},E_{42}},
{E_{255},E_{290},E_{196},E_{148},E_{284},E_{119},E_{70},E_{200}}}

These volcanoes are depicted in Figure 2. Each node is labeled with the value λ and colored according the connex component of the 3–cordillera they belong to.

Notice that, in this particular case, the structure of volcanoes in the 2-cordillera and the ones in the 3-cordillera are different: 2–volcanoes have height 1 and craters with 2 nodes; 3–volcanoes have height 0 and craters with either 4 or 8 nodes. In this example, the cordilleras generated with the algorithm are in fact complete, since all the isomorphism classes (24 in total) with cardinal 312 over the field $\mathbb{F}_{317}$ appear. Besides, it should be also pointed out that these isomorphism classes are not distributed in the 2–cordillera and in the 3–cordillera at random: every 3–volcano contains curves of each one of the four 2–volcanoes and *vice versa*.

4 Conclusions and further work

Obtaining cryptographically good elliptic curves is needed when setting up elliptic curve cryptosystems, or even each time that the systems are updated. Taking a random curve and testing its suitability is costly and turns out to be unfeasible when a huge amount of them are needed.

Hence, in this paper we face the problem of obtaining such curves. A procedure to obtain good curves from a given one $E/\mathbb{F}_q$ is suggested. It is already known that curves in the ℓ–volcano of $E/\mathbb{F}_q$ are isogenous and, therefore, also cryptographically desirable. But, unfortunately, not every curve with the same cardinal will belong to that volcano. So, the core of the algorithm lies on the fact that curves that appear in a connex component of an ℓ_i–cordillera, will also appear in some other ℓ_j–cordillera, so the procedure of searching new curves can go on by jumping from one cordillera to one other.

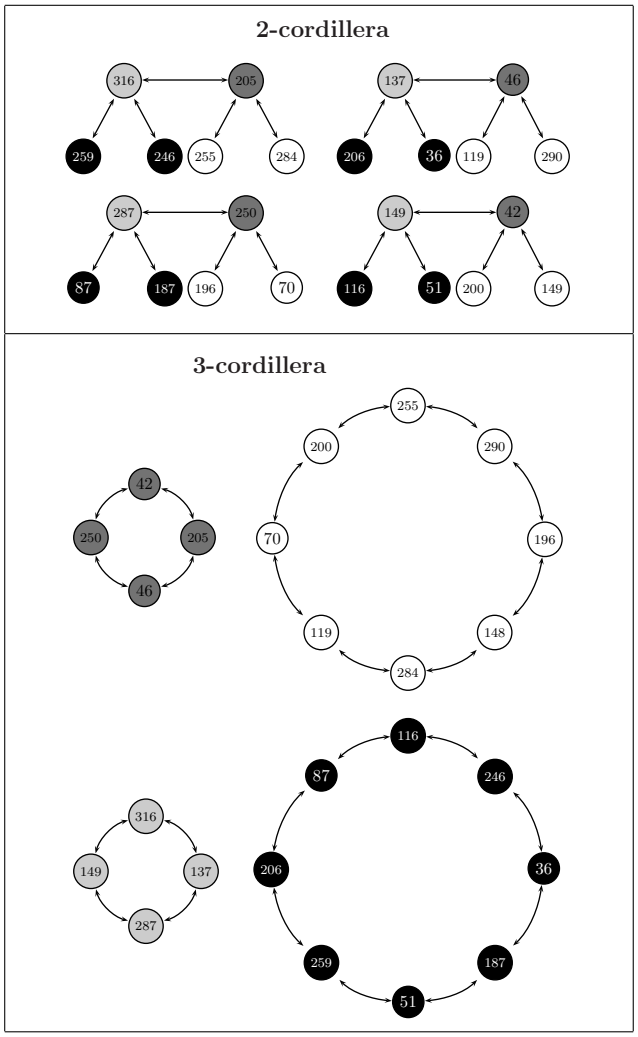

Figure 2:
Cordilleras obtained from $E_{316}/\mathbb{F}_{317}$ and $L_E = \{2,3\}$

Experimental results performed seem to show that the behaviour of this jumping process follows some particular patterns. An accurate study of these properties would be interesting, as well as could help in improving the presented algorithm.

References

Barreto, P., Kim, H., Lynn, B., and Scott, M. (2000), 'Efficient reduction on the jacobian variety of Picard curves', *Coding Theory, Cryptography and Related Areas*, 13-28, Springer.

Blake, I., Seroussi, G. and Smart, N. (1999), *Elliptic curves in cryptography.* London Mathematical Society, LNS 265. University Press.

Fouquet, M. and Morain, F. (2002), Isogeny Volcanoes and the SEA Algorithm, *in* 'Algorithmic Number Theory Symposium, ANTS-V', LNCS 2369, 276-291, Springer.

Galbraith, S. (1999), 'Constructing isogenies between elliptic curves over finite fields', *Journal of Computational Mathematics*, 2, 118-138.

Hankerson, D., Menezes, A., Vanstone, S. (2003), *Guide to Elliptic Curve Cryptography*, Springer.

Husemöller, D. (1987), *Elliptic curves.* GTM, 111, Springer.

Koblitz, N. (1987), 'Elliptic Curve Cryptosystems', *Mathematics of Computation*, 177, 203-209.

Kohel, D. (1996), Endomorphism rings of elliptic curves over finite fields, Ph.D., University of California, Berkeley.

MAGMA Group. *Handbook of Magma functions.* J. Canon and W. Bosma, eds. Available from `http://magam.maths.usyd.edu.au/`.

Menezes, A. (1993), *Elliptic curve public key cryptosystems*, Kluwer Academic Publishers.

Miret, J., Moreno, R., Sadornil, D., Tena, J., and Valls, M. (2006), 'An algorithm to compute volcanoes of 2–isogenies of elliptic curves over finite fields', *Applied Mathematics and Computation*, 176(2):739-750.

Pohlig, S., Hellman, M. (1978), 'An improved algorithm for computing logarithms over GF(p) and its cryptographic significance', *IEEE Trans. on Inform. Theory*, 24, 106-119.

Silverman, J., Suzuki, J. (1998), Elliptic Curve Discrete Logarithms and the Index Calculus, *in* 'Advances in Cryptology ASIACRYPT98', LNCS 1514, 110-125.

Vélu, J. (1971), 'Isogénies entre courbes elliptiques', *C. R. Acad. Sci. Paris, Ser. I Math., Serie A.*, 273:238-241.