Exploiting Isogeny Cordillera Structure to Obtain Cryptographically Good Elliptic Curves*

Josep M. Miret, Rosana Tomàs and Magda Valls

Dept. de Matemàtica. Univ. de Lleida
Jaume II, 69. 25001, Lleida (Spain)
Email: {miret,rosana,magda}@eps.udl.es

Daniel Sadornil

Dept. de Matemáticas, Estadística y Computación. Univ. de Cantabria
Avda. de Castros, s/n. 39005, Santander (Spain)
Email: sadornild@unican.es

Juan Tena

Dept. de Álgebra, Geometría y Topología. Univ. de Valladolid
Prado de la Magdalena, s/n. 47005, Valladolid (Spain)
Email: tena@agt.uva.es

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; Isogeny Volcanoes
ACM Classifications: E.3, K.4.4.

1. INTRODUCTION

During the last decades, the cryptographic community has paid significant attention to the usage of elliptic curves defined over a finite field F_q 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 cannot 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).

* This work has been partially supported by grants MTM2004–008076, TIN2006-15662-C02-02 and MTM2007–66842-C02-02 from Spanish MCyT.

Manuscript received: 25 June 2008
Communicating Editor: Ljiljana Brankovic

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 over which the curves are defined. Again, this 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 is 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, with trace different to one and low embedding degree (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 (Bareto *et al*, 2000).

As a consequence, one approach to obtain good curves would be obtaining new ones from a given good one E/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 their customers when necessary.

Finding out isomorphic curves to E/F_q would indeed provide curves with the same cardinal (and hence, presumably the same security). But, since these curves can be considered essentially the same curve, they do not become, in fact, a valid alternative. More generally, it is well known (Husemöller, 1987) that two elliptic curves over F_q have the same cardinal if, and only if, they are *isogenous*. That is to say, a rational map exists that preserves the infinity point. Then, the cardinal of the kernel of such a map is called the *degree of the isogeny*.

Therefore, obtaining every isomorphism class of curves with the same cardinal as $E(F_q)$ could be done by obtaining all the rational isogenies of E/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 bound by a given threshold (Galbraith, 1999).

Then, given an elliptic curve and a fixed prime ℓ, 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/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.

So, this paper presents a procedure which allows us to obtain 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 also appear in some other ℓ_j–cordillera. Hence, once the curves in the ℓ_i–volcano of E/F_q are obtained, new ones can come out by studying, respectively, their ℓ_j–volcanoes (an 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, its behaviour is also enlightened by means of some examples. Finally, Section 4 lays 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 F_q, determining an isogenous curve to E is a feasible problem, from an algebraic point of view. Indeed, given a rational non–trivial subgroup $G \subset E(F_q)$, for instance the cyclic subgroup $\langle P \rangle$ generated by a point $P \in E(F_q)$, a rational map 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 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 non–trivial rational map between them that sends the infinity point in E to the infinity point in E'.

More concretely, given an elliptic curve of Weierstrass equation

$$E / F_q : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6,$$

the coefficients of its isogenous curve of kernel G

$$E' / F_q : y^2 + a_1' xy + a_3' y = x^3 + a_2' x^2 + a_4' x + a_6',$$

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

$$a_1' = a_1, \quad a_2' = a_2, \quad a_3' = a_3,$$
$$a_4' = a_4 - 5t,$$
$$a_6' = a_6 - b_2 t - 7w.$$

with

$$t = \sum_{T \in S_G} t(T), \quad w = \sum_{T \in S_G} \left(u(T) + x(T) t(T) \right).$$

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

$$t(T) = \begin{cases} 3x(T)^2 + 2a_2 x(T) + a_4 - a_1 y(T), & \text{if} \quad T \in G \cap E[2] \\ 6x(T)^2 + b_2 x(T) + b_4, & \text{if} \quad T \in G - E[2] \end{cases}$$
$$u(T) = 4x(T)^3 + b_2 x(T)^2 + 2b_4 x(T) + b_6,$$

and the coefficients b_i are defined in the following way:

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

2.2 Isogeny Volcanoes and Cordilleras

Given an ordinary elliptic curve E/F_q and an ℓ–isogeny $I: E \longrightarrow E'$, Kohel (1996) introduced the notion of direction of the isogeny, according to the relationship between the endomorphism rings O and O' of the curves. Actually, Kohel shows that $[O:O']=1$, ℓ or $1/\ell$, and depending on each case, it is said that the isogeny I is *horizontal, descending* or *ascending*, respectively. This notion of direction can be exploited to represent 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

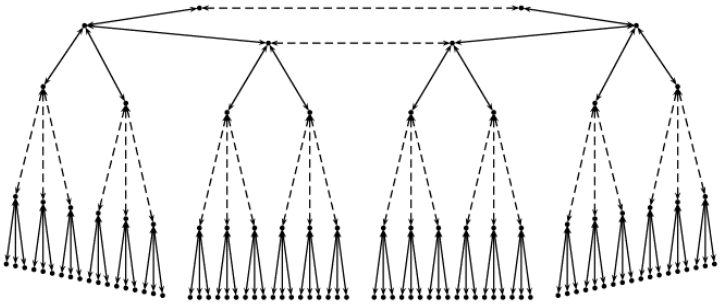


Figure 1: Structure of a volcano of 3–isogenies

of a unique cycle (with one, two or more nodes) at the top level, called *crater*, and from each node of the cycle hang ℓ-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 the *floor* of the ℓ–volcano, while the remaining nodes of each tree constitute the volcanoside. Each node of the ℓ–volcano (except the leaves) has ℓ+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 ℓ-1 descending ones (for craters with length greater than 2). The structure of a general ℓ–volcano for ℓ=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 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/F_q can be obtained considering the conductor f of the order $Z[\pi]$, being π the Frobenius endomorphism 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, i.e. the volcanoes, we can use the following 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 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 both belong to two different volcanoes V and V' of ℓ and ℓ–isogenies, respectively, then the endomorphism rings satisfy $[O:O']=\ell^n$ and $[O:O']=(\ell)^{n'}$. Therefore, both relations can only hold when $n=n'=0$. Consequently, E and E' must be located at the same level in V, as well as, at the same level in V'.

2.3 Amount of Isomorphism Classes

Concerning the total number of nodes involved in a cordillera, it corresponds to the number of isomorphism classes of elliptic curves over F_q, namely, the *Hurwitz class number* of the order $Z[\pi]$, being π the endomorphism of Frobenius of the curve. It is well known that this value can be expressed in terms of the class numbers of certain orders (Cox, 1989), which can be obtained computing the number of primitive positive quadratic forms of each discriminant.

More in detail, given a non–supersingular elliptic curve E over F_q, its endomorphism ring O can be identified with an order of the imaginary quadratic field $K = Q\left(\sqrt{t^2 - 4q}\right)$, where t is the trace of the Frobenius endomorphism of E (i.e. the difference between q+1 and the cardinal of E). Then, the discriminant of $Z[\pi]$ is $d_\pi = t^2 - 4q = f_0^2 d$, , and its conductor is

$$f = \begin{cases} f_0, & \text{if} \quad d \equiv 1 \pmod 4, \\ \dfrac{f_0}{2}, & \text{otherwise} \quad . \end{cases}$$

As well, the discriminant of the integer ring of K coincides with the discriminant of the field K, which is

$$d_K = \begin{cases} d, & \text{if} \quad d \equiv 1 \pmod 4, \\ 4d, & \text{otherwise} \quad . \end{cases}$$

The endomorphism rings of the curves with trace t can be identified with orders O such that $Z[\pi] \subseteq O \subseteq O_K$, where O_K is the ring of integers of K. The discriminant of each O is $D = g^2 d_K$, where $g \mid f$.

Then the *Hurwitz class number* can be given as follows

$$H(t^2 - 4q) = \sum_{Z[\pi] \subseteq O \subseteq O_K} \frac{2}{\left|O^*\right|} h(O),$$

where $h(O)$ denotes the number of isomorphism classes of curves with endomorphism ring O. Notice that to consider every possible O, one needs to deal with every possible discriminant D. Hence, when the cardinal of the curves in the cordillera and the factorization of $t^2 - 4q$ is known, this can be efficiently computed (for instance with MAGMA (MAGMA-Handbook, 2006)). From a practical point of view, the result is satisfying since it allows us to control the number of expected nodes in each cordillera, in the case that the cardinal of the curves is known.

3. PROCEDURE TO OBTAIN ISOGENOUS CURVES

Let $\ell_1 < \ell_2 < \ldots < \ell_{lim}$ be prime numbers (different from the characteristic p of the field) so that the curve E/F_q admits ℓ_i –isogenies, i.e., for which E/F_q has a rational subgroup G of order ℓ_i. The algorithm that we present generates all the ℓ_i–isogenous curves of E until a given threshold 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 of E' is also obtained. Frequently, in these new ℓ_1–volcanoes nodes will appear 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 of 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}. In the case that the *Hurwitz class number* can be computed, it can be used to control the percentage of the whole amount of curves already visited in each cordillera.

3.1 Algorithm

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

```
ALGORITHM All_Isogenous
INPUT
 E: Elliptic Curve
 ℓlim: Prime number
 LE: List of primes {ℓ1, ℓ2, ..., ℓlim } in ascending order
     for which E has ℓi -isogenies
OUTPUT
 Isogenous: List of elliptic curves with same
            cardinal as E

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

BEGIN ALGORITHM
 Isogenous:= {E}
   For all Prime ℓ s.t. ℓ ∈ LE
     Untreated[ℓ]:= ∅
   EndFor
 ℓact:= Get_ℓact (LE)
 Untreated[ℓact]:= Add(E)
 new_curves:= False
 While Not Empty(Untreated[ℓact])
   E':= Top(Untreated[ℓact])
   V:= ℓact -volcano(E')
   For all elliptic curve E''∈V
     If E''∈ Isogenous
       Untreated[ℓact]:= Remove(E'')
     Else
       Isogenous:= Add(E'')
       new_curves:= True
       For all Prime ℓ ∈ LE
         If ℓ≠ℓact
           Untreated[ℓ]:= Add(E'')
         EndIf
```

```
        EndFor
      EndIf
    EndFor
    If new_curves
      ℓact:= Get_ℓact (LE)
      new_curves:= False
    EndIf
    While Empty(Untreated[ℓact]) & ℓact≤ℓlim
      ℓact:= Next(LE)
    EndWhile
  EndWhile
  Return Isogenous
END ALGORITHM
```

This algorithm takes, as input values, the initial elliptic curve E over F_q and a list L_E with some prime numbers ℓ_i for which exist ℓ_i–isogenies. We denote by ℓ_{lim} the highest value in L_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 elliptic 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. Typically, this function would find a path from the initial node towards the crater of the volcano and then would go through every node in the volcanoside (Fouquet *et al*, 2002; Miret *et al*, 2006). In addition, this function can also admit a parallel implementation to improve its performance (Martínez *et al*, 2006).

Using this procedure, one can obtain a broad range of elliptic curves with the same *good* cardinal (exploiting the fact that one has an initial good curve). Notice that an alternative method would be taking random curves and checking their cardinality. This approach is much more expensive, since the cost of obtaining the cardinal (using the usual SEA algorithm) is higher than computing a low–degree isogenous curve.

3.2 Experimental Example

The previous algorithm has been implemented using the computer algebra system MAGMA (see MAGMA-Handbook, 2006). We show an illustrative example, considering the field F_{691} and the curves with cardinal m=700=$2^2 5^2 7$ and t^2-4q= -2700=-$2^2 3^3 5^2$. In this case, the Hurwitz class number is $H(t^2\text{-}4q)$=38. Each isomorphism class is denoted as E_j, where j is the j–invariant of the curves in the class.

The proposed algorithm has been executed to obtain the construction of the 2, 3, 5 and 7–cordillera. More in detail, the curves in each connex component are the following (the curves in the same component are shown grouped).

As can be deduced from the ℓ–adic valuations of t^2-4q, the heights of the 2, 3 and 5 volcanoes is 1, while the 7–volcanoes are flat.

Taking E_{53}: $y^2 = x^3 + 2x + 114$ as the initial curve, the algorithm provides two connex components of the 2 and 3–cordilleras (see Figure 2), which involve 6 isomorphism classes (out of 38).

$$2-Cord.\quad \begin{array}{l}\{\{E_0, E_{102}\}, \{E_{53}, E_{52}, E_{440}, E_{460}\}, \{E_{674}, E_{61}, E_{91}, E_{172}\},\\ \{E_{651}, E_{83}, E_{540}, E_{686}\}, \{E_{428}, E_{87}, E_{181}, E_{345}\},\\ \{E_{170}, E_{98}, E_{317}, E_{406}\}, \{E_{647}, E_{101}, E_{118}, E_{468}\},\\ \{E_{635}, E_{143}, E_{289}, E_{654}\}, \{E_{497}, E_{161}, E_{316}, E_{676}\},\\ \{E_{619}, E_{192}, E_{573}, E_{610}\}\}\end{array}$$

$$3-Cord.\quad \begin{array}{l}\{\{E_0, E_{53}\}, \{E_{102}, E_{52}, E_{440}, E_{460}\},\\ \{E_{540}, E_{345}, E_{61}, E_{101}, E_{317}, E_{676}, E_{610}, E_{654}\},\\ \{E_{83}, E_{87}, E_{406}, E_{172}, E_{118}, E_{573}, E_{316}, E_{289}\},\\ \{E_{686}, E_{181}, E_{91}, E_{98}, E_{468}, E_{192}, E_{161}, E_{143}\},\\ \{E_{651}, E_{428}, E_{170}, E_{647}, E_{674}, E_{635}, E_{619}, E_{497}\}\}\end{array}$$

$$5-Cord.\quad \begin{array}{l}\{\{E_0, E_{428}, E_{651}\}, \{E_{52}, E_{192}, E_{406}, E_{91}, E_{676}, E_{101}, E_{289}\},\\ \{E_{53}, E_{497}, E_{674}, E_{635}, E_{619}, E_{647}, E_{170}\},\\ \{E_{440}, E_{61}, E_{118}, E_{98}, E_{143}, E_{610}, E_{316}\},\\ \{E_{102}, E_{83}, E_{686}, E_{540}, E_{345}, E_{87}, E_{181}\},\\ \{E_{460}, E_{161}, E_{654}, E_{172}, E_{317}, E_{468}, E_{573}\}\}\end{array}$$

$$7-Cord.\quad \begin{array}{l}\{\{E_0\}, \{E_{53}\}, \{E_{102}\}, \{E_{428}, E_{651}\}, \{E_{52}, E_{440}, E_{460}\},\\ \{E_{61}, E_{161}, E_{406}, E_{610}, E_{468}, E_{289}\},\\ \{E_{83}, E_{345}, E_{686}, E_{87}, E_{540}, E_{181}\},\\ \{E_{91}, E_{316}, E_{317}, E_{192}, E_{118}, E_{654}\},\\ \{E_{98}, E_{573}, E_{101}, E_{143}, E_{172}, E_{676}\},\\ \{E_{170}, E_{619}, E_{647}, E_{635}, E_{674}, E_{497}\}\}\end{array}$$

Hence, it is necessary to jump to the 5–cordillera to seek other isomorphism classes (Figure 3). This 5–volcano of E_{53} provides six new classes not previously visited, so six more 2–volcanoes can also be generated (Figure 4) which again provide access to other isomorphism classes. The algorithm would proceed constructing their 3–volcanoes (for instance the one corresponding to E_{497} (collected in Figure 5). Finally, from the curves in this volcano, the two remaining connex components of the 2–cordillera are already reached, so the whole 38 isomorphism classes have been detected. In this particular case, it is not necessary to take benefit of the 7–cordillera structure (Figure 6).

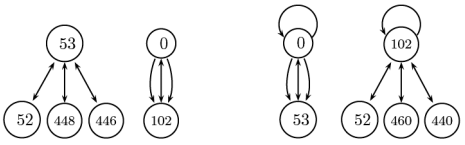


Figure 2: Volcanoes of 2 and 3–isogenies

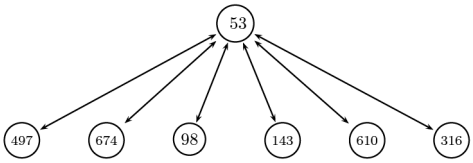


Figure 3: Volcano of 5–isogenies

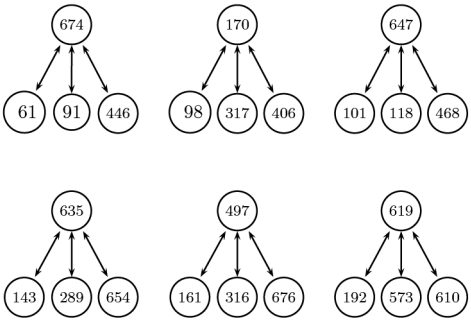


Figure 4: Volcanoes of 2–isogenies

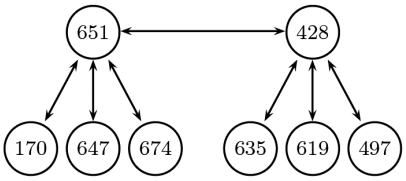


Figure 5: Volcano of 3–isogenies

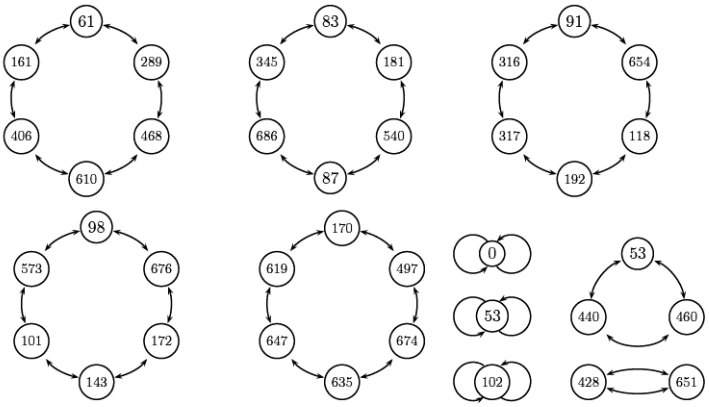


Figure 6: Cordillera of 7–volcanoes

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 E/F_q is suggested. It is already known that curves in the ℓ–volcano of E/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.

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, and could also 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.

COX, D. (1989): *Primes of the form x^2+ny^2*. Wiley–Interscience.

FOUQUET, M. and MORAIN, F. (2002): Isogeny volcanoes and the SEA algorithm, *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. and 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. Thesis, University of California, Berkeley.

MAGMA GROUP. (2006): *Handbook of Magma functions*. CANON, J. and BOSMA, W. (Eds.), edition 2:13.

MARTÍNEZ, S., TOMÀS, R., ROIG, C., VALLS, M. and MORENO, R. (2006): Parallel calculation of volcanoes for cryptographic uses. *7th Workshop on Parallel and Distributed Scientific and Engineering Computing*, PDSEC-IPDPS'06. IEEE Computer Society Press. Digital Object Identifier: 10.1109/IPDPS.2006.1639608.

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. and 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. and 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.

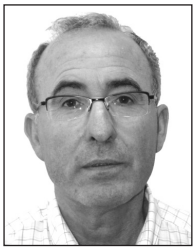
BIOGRAPHICAL NOTES

Josep M. Miret received the M.S. in Mathematics from the Universitat de Barcelona (UB), Spain, in 1983 and the Ph.D. degree in Mathematics from the Universitat Politècnica de Catalunya (UPC), Spain, in 1999. He is currently an associate professor of mathematics at the Universitat de Lleida (UdL), Spain, and leads the Cryptography and Graph Theory Research Group. His research interests include enumerative geometry, cryptography with elliptic and hyperelliptic curves and its computational aspects.

Josep M. Miret


Daniel Sadornil

Daniel Sadornil received the B.S. degree in mathematics (1999), the M.S. degree in algebra (2001) and the Ph.D. in mathematics (2004) from the University of Valladolid, Spain. During 1999–2004 he had a pre-doctoral grant from the Spanish government. From 2004 to 2008 he was assistant professor at the University of Salamanca, Spain. Now, he is doctor assistant professor at the University of Cantabria, Spain. His research interests include cryptography and number theory. Currently he is particularly interested in primality test, elliptic and hyperelliptic curves and applications to cryptography.


Juan Tena

Juan Tena received the B.S. degree in mathematics from Madrid University, Spain, in 1967, the M.S. degree in number theory from Grenoble University, France, in 1970 and the Ph.D. degree in mathematics from Madrid University in 1973. During 1973–1982 he was at the Universities of Valladolid, Madrid and Santander and since 1983 he has been at the University of Valladolid, Spain, where he is professor of algebra. His research interests include cryptography, number theory and error correcting codes. Currently he is specially interested in primality tests, isogeny of elliptic curves and its applications to elliptic curve cryptography.


Rosana Tomàs

Rosana Tomàs received the B.S. degree in computer science from the Universitat de Lleida (UdL), Spain, in 2002 and the M.S. degree in computer science from the Universitat Rovira i Virgili (URV), Spain, in 2004. She is currently a Ph.D. student of computer science at the UdL in the Cryptography and Graph Theory Research Group in the Department of Mathematics of this university. Her research interests include elliptic curve cryptography and smart card security.


Magda Valls

Magda Valls received the M.S. in mathematics from the Universitat Autònoma de Barcelona (UAB), Spain, in 1994, and the Ph.D. in applied mathematics from the Universitat Politècnica de Catalunya (UPC), in 2001 respectively. She is currently an associate professor of mathematics at the Universitat de Lleida (UdL), Spain, and member of the Cryptography and Graph Theory Research Group. Her research interests include cryptography, computational security and elliptic curve cryptosystems.