25 Años de Criptografía con Curvas Elípticas

Juan G. Tena
IMUVA
Universidad de Valladolid
Email: tena@agt.uva.es

***Resumen*—Se describe brevemente el nacimiento y los principales hitos en el desarrollo histórico de la Criptografía con Curvas Elípticas, sus fortalezas y vulnerabilidades. Se examinan las condiciones exigibles a una curva elíptica para ser *criptográficamente fuerte* y las estrategias para encontrar tales curvas. Finalmente se analiza el caso particular de la Criptografía con Curvas Elípticas en el contexto de las tarjetas inteligentes.**

***Palabras clave*—curvas elípticas; logaritmo discreto; curvas criptográficamente buenas; isogenias; pairings; tarjetas inteligentes**

I. Introducción

Las curvas elípticas han ocupado un papel central en Matemáticas desde hace tres siglos y sus notables propiedades, aritméticas y geométricas, han encontrado aplicación en múltiples problemas y campos matemáticos.

Su empleo en Criptografía es sin embargo reciente, pudiéndose situar su inicio en los dos artículos siguientes:

- V. Miller: Use of elliptic curves in Cryptography, CRYPTO'85, 1985, [13].
- N. Koblitz: Elliptic Curve Cryptography, Math. Comp., 1987, [9].

En ambos, los autores proponen implementar el Problema del Logaritmo Discreto (PLD) en el grupo de puntos de una curva elíptica definida sobre un cuerpo finito, en lugar de en el grupo multiplicativo de un tal cuerpo, como se hacía clásicamente. La motivación aducida es que tal grupo de puntos resulta inmune a ataques criptoanalíticos, como el Index-Calculus, lo que permite una seguridad equivalente con longitudes de clave mucho menores.

Sin embargo, la idea de Miller y Koblitz permaneció inicialmente en el ámbito académico y aún en 1997 R. Rivest escribía:

The security of cryptosystems based on elliptic curves is not well understood, due in large part to the abstruse nature of elliptic curves.

La implantación del nuevo paradigma debe mucho a la compañía Certicom (creada en 1985 por S.A. Vanstone y R. Mullin) y al grupo investigador de la Universidad de Waterloo (A.J. Menezes, S.A.Vanstone, etc).

It was enterely Scott Vanstone and his students and collaborators who transformed ECC from a gleam in two mathematicians'eyes to something that was ready from prime time. (N. Koblitz).

Actualmente la Criptografía con Curvas Elípticas (ECC) es una disciplina madura y consolidada, teórica y tecnológicamente. Los libros y artículos, los congresos y seminarios sobre el tema son muy numerosos y compañías e instituciones como NIST, Certicom, IEEE, RSA Laboratories, etc incluyen Criptografía Elíptica en sus standards.

Sin embargo, el camino recorrido no ha estado exento de obstáculos. Algunos de ellos han sido debidos a problemas de implementación:

1. Cálculo del cardinal del grupo de puntos de la curva elíptica. Los algoritmos para su determinación (SEA, T. Satoh, etc, [1], [2]) son costosos.
2. Identificación de los mensajes a cifrar m con puntos P_m de la curva elíptica utilizada.
3. Optimización de las operaciones (suma y multiplicación escalar) con puntos de la curva. Diversos algoritmos, utilizando diferentes tipos de coordenadas (afines, proyectivas, etc) y diferentes ecuaciones para la curva (Weiertrass, Hess, Montgomery, Edwards, etc), [8], [1] han sido propuestos.

Por otra parte, en Criptografía, ninguna propuesta está exenta de vulnerabilidades. En el caso de las curvas elípticas, su rica estructura matemática es un arma de doble filo, ya que puede ser explotada también por el criptoanálisis.

Un ejemplo clásico es el algoritmo de Menezes–Okamoto–Vanstone (MOV, 1993), [14], que permite reducir el PLD para una curva elíptica E, definida sobre el cuerpo finito $\mathbf{F}_q$, al PLD sobre un cuerpo extensión $\mathbf{F}_{q^k}$, para un cierto número k (dependiente de E) al cual se denomina *grado de inmersión de la curva* E. El algoritmo MOV utiliza como herramienta el denominado pairing de Weil. Los pairing (de Weil, Tate, etc) son aplicaciones bilineales definidas sobre una curva elíptica y con valores en un grupo cíclico, ver [2], [6].

La utilidad criptoanalítica del algoritmo MOV depende del grado de inmersión k, ya que solo resulta eficiente si k es pequeño. En particular Menezes, Okamoto y Vanstone muestran que esto ocurre para las curvas elípticas denominadas supersingulares, en las que el valor de k es a lo sumo 6. Por ello tales curvas se consideran vulnerables para criptosistemas basados en el PLD. Cabe señalar que, sin embargo, las curvas

ISBN: 978-84-9717-323-0

supersingulares son idóneas para su empleo en otra rama de la Criptografía, la Criptografía Basada en la Identidad, [12].

La idea de Criptografía Basada en la Identidad fue introducida por A. Shamir (CRYPTO 1984), ver [12]. En ella la clave pública de un usuario puede deducirse de su nombre (o cualquier otra información relacionada con su identidad). Shamir propuso esquemas de firma e intercambio de claves basadas en la identidad, pero no sistemas de cifrado. D. Bonech y M. Franklin (CRYPTO 2001), [3], proponen un criptosistema basado en la identidad, utilizando el pairing de Weil sobre curvas elípticas.

Actualmente existen propuestas de criptosistemas, esquemas de firma y esquemas de intercambio de claves basadas en pairings. A diferencia de los criptosistemas basados en el PLD elíptico la Criptografía basada en la identidad requiere curvas elípticas con grado de inmersión pequeño, las denominadas *pairing friendly curves*.

Otra herramienta, propia de las curvas elípticas, que permite el diseño de criptosistemas y protocolos criptográficos son las isogenias. Una isogenia es una aplicación lineal entre dos curvas elípticas, ver [6]. En el caso de un cuerpo base finito $\mathbf{F}_q$ dos curvas elípticas, definidas sobre $\mathbf{F}_q$, son isógenas (es decir existe una isogenia no nula entre ellas) si y solo si tienen igual cardinal.

Sin embargo, dadas dos curvas elípticas sobre $\mathbf{F}_q$ y con igual cardinal, encontrar explícitamente una isogenia entre ambas es un problema computacionalmente difícil, lo que posibilita utilizar este problema en el diseño de criptosistemas de clave pública. A. Rostovsov y A. Stolbunov (Eurocrypt' 2006), proponen un criptosistema basado en *estrellas* de isogenias, [18].

Como un último ejemplo de la fecundidad de las curvas elípticas citemos su aplicación en dos técnicas auxiliares del criptosistema RSA, métodos de factorización y tests de primalidad:

- Métodos de factorización: algoritmo de H.W. Lenstra Jr., 1987, [1], [6].
- Tests de primalidad: test de S. Goldwaser–J. Kilian, 1996 y test de A.O.L. Atkins–F. Morain, 1993, [4].

II. Curvas Elípticas

En la sección anterior hemos resumido la aparición y el desarrollo de la Criptografía basada en curvas elípticas, pero no hemos precisado que son tales curvas. Podemos tomar como definición la siguiente, [1], [6],

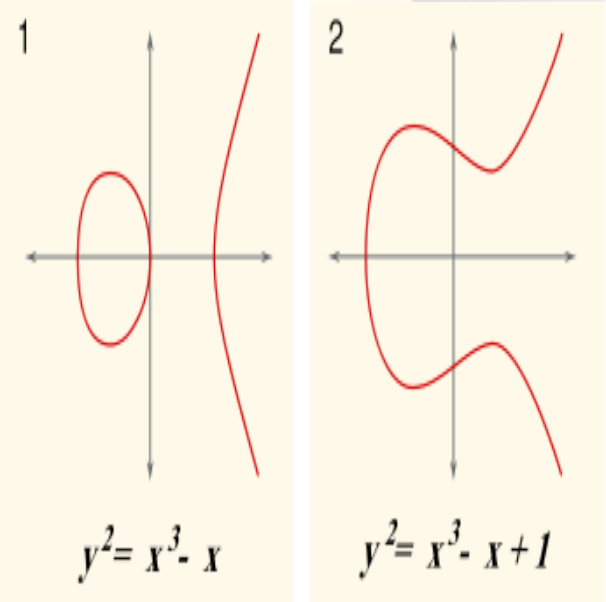
Definición 1: Una *Curva Elíptica* E definida sobre un cuerpo k (por ejemplo el cuerpo de los números complejos $\mathbf{C}$, los reales $\mathbf{R}$, un cuerpo finito $\mathbf{F}_q$, etc) es una curva proyectiva, no singular, admitiendo una ecuación, definida sobre k, en la denominada *Forma Normal de Weierstrass*:

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,\ a_i \in k$$

Una tal curva admite un único punto en el infinito, el $O = (0 : 1 : 0)$ (punto del infinito en la dirección del eje **y**). Si $Car(k) \neq 2, 3$ (es decir cuerpo no binario ni ternario) la forma de Weiertrass puede reducirse a la ecuación más simple:

$$E : y^2 = x^3 + Ax + B,\ A, B \in k$$

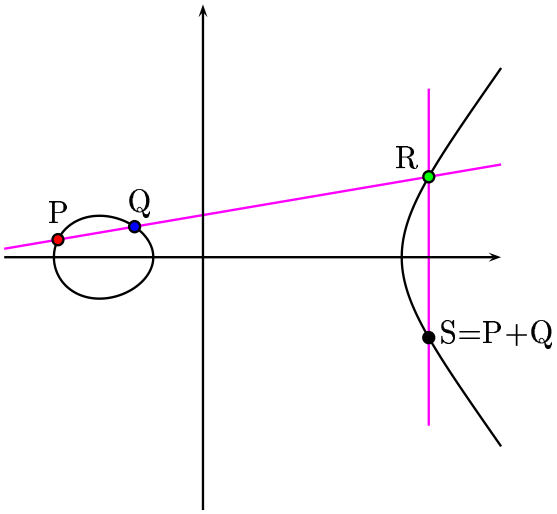
La gráfica de esta curva, para el cuerpo $\mathbf{R}$ de los números reales, toma una de las dos formas siguientes:



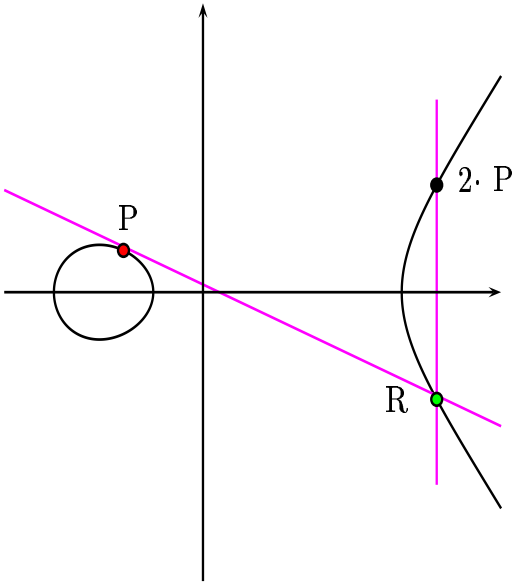
Denotaremos con $E(k)$ al conjunto de puntos de la curva E con coordenadas en el cuerpo k (incluido el punto en el infinito O). La utilidad de las curvas elípticas deriva de la posibilidad de dotar a $E(k)$ de una estructura de grupo abeliano (con O como elemento neutro). La ley de grupo puede definirse geométricamente. Por simplicidad supongamos Car$(k) \neq 2, 3$ y $E : y^2 = x^3 + Ax + B$ y recordemos que, por el teorema de Bezout, una recta L corta a E en tres puntos.

Definición 2: La suma de dos puntos $P, Q \in E(k)$ es el punto simétrico, respecto del eje x, del tercer punto de intersección con la cúbica de la recta que une P y Q. Si $P = Q$, (en cuyo caso se habla de doblado del punto) se sustituye cuerda por tangente.

Las dos figuras siguientes muestran gráficamente las operaciones de suma y doblado de puntos:



Suma de Puntos en Curva Elíptica



Doblado de Punto en Curva Elíptica

Consideremos ahora el caso particular de un cuerpo base finito $k = \mathbf{F}_q,\ q = p^m$. Se tiene entonces, [1], [6].

Teorema 3: Sea E una curva elíptica definida sobre $\mathbf{F}_q$.

1. Sea $N = \#(E(\mathbf{F}_q))$ el cardinal de la curva. Se verifica el teorema de Hasse:
$$q + 1 - 2\sqrt{q} \leq N \leq q + 1 + 2\sqrt{q}$$
Es decir $N = q + 1 - t,\ \text{con}\ |t| \leq 2\sqrt{q}$.
2. El grupo abeliano finito tiene la estructura siguiente, $E(\mathbf{F}_q) \simeq \mathbf{Z}/n_1\mathbf{Z} \times \mathbf{Z}/n_2\mathbf{Z}$
donde $N = n_1 n_2,\ \ n_2|n_1,\ \ n_2|q-1$.

En la Introducción se ha hecho referencia a las curvas elípticas supersingulares,

Definición 4: Una curva elíptica E definida sobre el cuerpo finito $\mathbf{F}_q,\ q = p^m,$ se llama supersingular si p divide a t

III. Logaritmo Discreto Elíptico

Recordemos el Problema del Logaritmo Discreto (PLD), [6].

Definición 5: Sea $G = \langle g \rangle$ un grupo cíclico finito con cardinal N (clásicamente el grupo G considerado era $\mathbf{F}_q^* = \mathbf{F}_q - \{0\}$ con cardinal $N = q - 1$). Si $x \in G$, se denomina logaritmo discreto de x en la base g al entero natural $n \leq N$ tal que $g^n = x$.

Conocidos g y n es computacionalmente sencillo calcular x. Sin embargo conocidos g y x, es computacionalmente intratable determinar n (Problema del Logaritmo Discreto).

Diversos sistemas criptograficos (J. Massey–J. Omura, T. ElGamal), esquemas de firma electronica (T. ElGamal, C. P. Schnorr, DSA) e intercambio de claves (W. Diffie–M. E. Hellman) están basados en el PLD, [8].

La seguridad del logaritmo discreto ha sido exhaustivamente estudiada. Podemos clasificar los algoritmos para resolver el PLD en tres tipos, [6]:

1. Algoritmos válidos en cualquier grupo (todos los cuales tienen un coste exponencial): Rho de J. M. Pollard, Baby Steps Giant Steps (BSGS), etc.
2. Algoritmo de R. Silver– G. C. Pohlig–M.E. Hellman: Eficiente para grupos cuyo cardinal tiene todos sus factores primos *pequeños*. En consecuencia el cardinal del grupo debería poseer un factor primo grande para ser seguro.
3. Algoritmos tipo *Index Calculus*.

El método del Index-Calculus se ha aplicado con éxito (coste subexponencial) a los cuerpos finitos $\mathbf{F}_q$, en particular los binarios $\mathbf{F}_{2^m}$. Actualmente se considera necesario un tamaño mínimo para el cardinal de estos cuerpos de 1024 bits, lo que obliga a aumentar el tamaño de las claves y por tanto los recursos computacionales necesarios.

Una posibilidad alternativa es substituir el grupo $G = \mathbf{F}_q^*$ por otros inmunes al Index Calculus. Esta fué la motivación de Miller y Koblitz para su propuesta del Problema del Logaritmo Discreto Elíptico (PLDE): Dada una curva elíptica E sobre $\mathbf{F}_q$ y puntos P y $Q = nP$ en $E(\mathbf{F}_q)$ encontrar n.

El PLDE ofrece las siguientes ventajas sobre el PLD clásico:

- Flexibilidad: Fijado el cuerpo $\mathbf{F}_q$ existen muchas curvas elípticas sobre él, lo que ofrece la posibilidad de cambiar periódicamente la curva, manteniendo $\mathbf{F}_q$ (y su aritmética).
- El grupo $E(\mathbf{F}_q)$ es inmune al Index Calculus, lo que lo hace más seguro que el grupo $\mathbf{F}_q^*$:
  1. El ataque al PLDE (utilizando el algoritmo de Pollard) para una curva elíptica sobre $\mathbf{F}_p$, p primo de 160 bits, exige aproximadamente 10^{24} operaciones elementales.
  2. El ataque al DLP (utilizando el método del Index Calculus) para $\mathbf{F}_p^*$, p primo de 160 bits, necesita solo 10^9 operaciones.

- Esta posibilidad de claves más cortas hace especialmente idónea a la Criptografía con curvas elípticas para su uso en plataformas con capacidad computacional reducida como tarjetas inteligentes, RFID, redes de sensores, etc.

Comparación de tamaños de clave (NIST)

PLD/RSA	$PLDE$	$Ratio$
1024	163	1 : 6
3072	256	1 : 12
7680	384	1 : 20
15360	512	1 : 30

Ataques al PLDE, como el ya mencionado método MOV, propiciaron la búsqueda de otras alternativas como base del logaritmo discreto. Es el caso de las Curvas Hiperelípticas, [10], generalización de las elípticas. Estas curvas vienen dadas por una ecuación del tipo:

$$C : y^2 + h(x)y = f(x) \mid \ gr(h) \leq g, \ gr(f) = 2g + 1$$

(Las curvas elipticas corresponden al caso $g = 1$).

Sin embargo el PLD sobre (las jacobianas de) curvas hiperelípticas se ha mostrado vulnerable, para $g > 2$, frente a variantes del Index Calculus: algoritmos de L. M. Adleman–J. De Marrais–M. D. Huang (1994) y de P. Gaudry (2000), [2], [6].

III-A. Curvas elípticas criptográficamente buenas

Aunque actualmente el PLDE se considera seguro, algunas precauciones son necesarias en la elección de la curva elíptica base E:

1. El cardinal de E debe ser adecuado (primo o con un factor primo grande) para evitar el ataque de Silver-Pohlig-Hellman.
2. Con grado de inmersión "grande"(en particular no supersingulares) para evitar el ataque MOV.
3. Evitar las denominadas curvas *Anómalas*, curvas sobre $\mathbf{F}_p$ (p primo), y con cardinal p, curvas para las que el PLDE es fácil: ataques de I.A. Semaev (1998), T. Satoh–K. Araki (1998) y N. Smart (1999), [6].
4. E debe ser inmune al ataque por Descenso de Weil, tipo de ataque propuesto por G. Frey en 2001 y desarrollado por P. Gaudry, A.J. Menezes, N. Smart, etc [2].

Dos vías, ambas costosas, pueden utilizarse para elegir una curva elíptica *buena* (a salvo de las debilidades mencionadas):

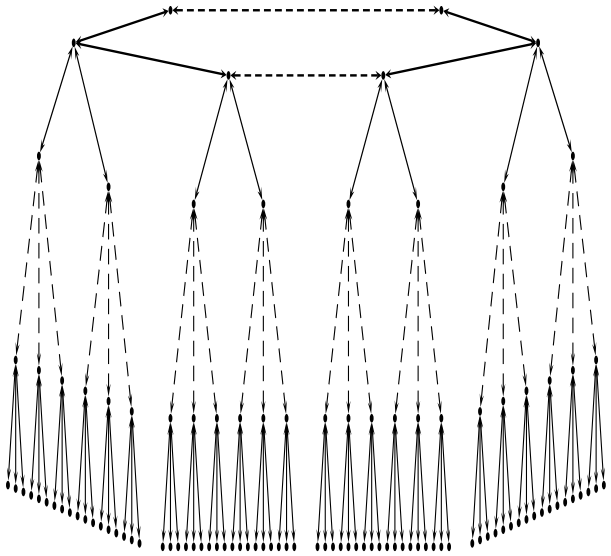
- Tomar curvas aleatoriamente, calcular su cardinal y comprobar si es adecuado.
- Construcción de curva elíptica con cardinal adecuado prefijado. Ello es factible empleando un método debido a A. O. L. Atkin–F. Morain, [4]

Una tercera vía consiste en el empleo de isogenias. Como se ha señalado, dos curvas isógenas tienen igual cardinal. Por tanto, partiendo de una curva *criptográficamente buena* (con cardinal adecuado N), todas las curvas obtenidas a partir de ellas como imágenes por isogenias serán también buenas. Ello justifica el estudio de tales relaciones de isogenia.

Consideremos el conjunto de todas las curvas elípticas (definidas salvo isomorfía) sobre un cuerpo finito dado $\mathbf{F}_q$, $q = p^m$ y con cardinal N. Sea ℓ un primo diferente de la característica p del cuerpo y consideremos todas las posibles isogenias de grado ℓ entre tales curvas (ver [6] para el concepto de grado de una isogenia). Tal conjunto puede considerarse como un grafo dirigido $\mathcal{G}(\mathcal{N}, \ell)$, con aristas dichas ℓ-isogenias. Es posible asignar a estas aristas un cierto sentido (horizontal, ascendente o descendente) y por tanto estratificar a $\mathcal{G}(\mathcal{N}, \ell)$ en pisos o niveles, [11].

Definición 6: Cada componente conexa de $\mathcal{G}(\mathcal{N}, \ell)$ se denomina un ℓ-volcán.

El nombre de volcán responde a su similitud con un cono volcanico, de hecho en un ℓ-volcán se habla de cráter, ladera y suelo. La noción de grafo de ℓ-isogenias y ℓ-volcanes se debe a D. R. Kohel (Ph. D. Thesis, 1996), [11] y posteriormente su estructura y propiedades han sido estudiadas por otros investigadores: M. Fouquet–F. Morain (LNCS 2369, 2002) [5], J.Miret–R.Moreno–D.Sadornil–J.Tena–M.Valls (Applied Mathematics and Computation, 2006 y 2008), [15], etc.



Estructura de un 3-Volcán

El grafo total $\mathcal{G}(\mathcal{N}, \ell)$ está formado por varios ℓ-volcanes y puede denominarse una ℓ-cordillera, [16].

IV. Curvas Elípticas y Tarjetas Inteligentes

Aunque las primeras tarjetas de crédito se remontan a 1950 (Diners Club), las Tarjetas Inteligentes (Smart Cards), con chip incorporado, se popularizan a partir de 1980 (en 1986 se define el standard ISO para ellas) y se integran en la telefonía móvil (Tarjetas SIM: Subscriber Identificatio Module) a partir de 1990.

Los usos actuales de las tarjetas hacen necesaria la implantación en las mismas de sistemas criptográficos (esquemas de cifrado, certificados, firma digital, etc).

La posibilidad ya mencionada de claves más cortas y la flexibilidad en la elección de las mismas, convierten a las curvas elípticas en candidatos privilegiados para la Criptografía implementada en tarjetas inteligentes:

- En 1996 un grupo de empresas, Europay, MasterCard y VISA (EMV) definieron la especificación de tarjetas inteligentes para su uso en servicios financieros.
- En 2001 este grupo propone el empleo (EMV 40 Elliptic Curve Technical Report), de curvas elípticas como alternativa al RSA para Autenticación Estática de Datos (SDA), Autenticación Dinámica de Datos (DDA) y cifrado autónomo.

Además de los ataques criptoanalíticos específicos, propios del sistema criptográfico concreto utilizado, la Criptografía en tarjetas es susceptible de un tipo de ataques activos denominados *Side Channel Attacks*, [2]. Estos ataques se basan en que la alimentación y el reloj de las tarjetas inteligentes son proporcionados por el lector.

Es posible entonces, si se tiene acceso a la tarjeta y se dispone de instrumentos adecuados, medir el consumo, tiempo de computación, etc de la tarjeta, mientras ésta realiza operaciones criptográficas. Tal información puede ser usada por un atacante para obtener la clave privada guardada en la tarjeta. Veamos en particular un tipo de side channel attacks específico de la Criptografía con curvas elípticas.

IV-A. Zero-Value Point Attacks

L. Goubin, 2003, [7], muestra como un atacante puede detectar, midiendo el consumo de la tarjeta, la aparición de puntos de la curva con abscisa u ordenada nulos y después de varias ejecuciones, conseguir la clave secreta d almacenada en la tarjeta. De forma más precisa, suponiendo que un cierto bit de la clave d es 0 ó 1, el atacante intenta crear un punto con alguna de sus coordenadas cero. Si tal punto realmente aparece su suposición era correcta. Posteriormente T. Akishita y T. Takagi (LNCS 2851, Springer, 2003) generalizan el ataque de Goubin a curvas en las que algunos parámetros intermedios usados en el doblado y suma de puntos de la curva elíptica son cero.

¿Es posible obtener curvas inmunes a los ZVPA? N. Smart (LNCS 2779, Springer, 2003) y Akishita-Takagi proponen, partiendo de una curva *buena* (con cardinal adecuado, etc) buscar curvas isogenas a la dada hasta encontrar una adecuada (en particular sin puntos con coordenadas nulas). Para ello construyen ℓ-isogenias, para sucesivos primos ℓ, hasta encontrar una curva resistente.

Un problema de este método es que el coste de las ℓ -isogenias aumenta con el grado ℓ, como puede apreciarse en la tabla adjunta para la curva 192r1 del SECG (Standard for Efficient Cryptography):

ℓ	tiempo (seg.)
5	0.04
11	0.91
13	5.97
23	44.30
37	267.04
59	995.20
73	3474.73

Si una curva resistente no se encuentra para los primeros primos ℓ, el coste de encontrar una curva buena puede ser disuasorio.

Un método alternativo (J.M. Miret–D. Sadornil–J. Tena–R. Tomas–M. Valls, [17], consiste en la construcción de caminos de isogenias mediante búsquedas en los ℓ volcanes. Tal método encuentra la forma más rápida para ir de una curva vulnerable dada a otra resistente.

La tabla siguiente compara los resultados obtenidos (para la curva 192r1 del SECG) con el método de Smart y el alternativo. Con el método de Smart la primera curva resistente se obtiene mediante una 23-isogenia. En nuestro caso se obtiene con una 5-isogenia seguida de una 13-isogenia.

192r1	Smart	Nuestra propuesta
Grado Isógena resistente	23	5-13
Tiempo de cálculo (seg.)	44.30	6.01
Tiempo de la búsqueda (seg.)	51.24	6.99

AGRADECIMIENTOS

Este trabajo ha sido parcialmente financiado por el proyecto de investigación MTM2010-21580-C02-02 del Ministerio de Economía y Competitividad.

REFERENCIAS

[1] I. Blake, G. Seroussi, N. Smart, “Elliptic Curves in Cryptography”, London Mathematical Society Lecture Note Series 265, Cambridge University Press, 2000.
[2] I. Blake, G. Seroussi, N. Smart, “Advances in Elliptic Curves in Cryptography”, London Mathematical Society Lecture Note Series 317, Cambridge University Press, 2005.
[3] D. Bonech, M. Franklin, “Identity-based encryption from the Weil pairing”, CRYPTO 2001, LNCS 2139, pp. 213-229, Springer, 2001.
[4] R. Crandall, C. Pomerance, “Prime Numbers”, Second Edition, Springer, 2005.
[5] M. Fouquet, F. Morain, “Isogeny Volcanoes and the SEA Algorithm”, Proc. ANTS-V, LNCS 2369, pp. 276-291, Springer, 2002.
[6] S.D. Galbraith, “The Mathematics of Public Key Cryptography”, Cambridge U. Press, 2012.
[7] L. Goubin, ““A refined power-analysis attack on elliptic curve cryptosystems”, PKC 2003, LNCS 2567, pp. 199-211, Springer, 2003.
[8] D. Hankerson, A. Menezes, S. Vanstone, “Guide to Elliptic Curve Cryptography”, Springer, 2004.
[9] N. Koblitz, “Elliptic curve cryptosystems”, Math. Comp. 48, pp. 203-209, 1987.
[10] N. Koblitz, “Hyperelliptic criptosystems”, J. Crypt. 1, pp. 139-150, 1989.
[11] D. R. Kohel, “Endomorphism rings of elliptic curves over finite fields”, Ph. D. Thesis, U. California, Berkeley, 1996.
[12] L. Martin, “Identity-Based Encryption”, Artech House, 2008.

[13] V.S. Miller, “Use of elliptic curves in Crypography”, CRYPTO 1985, LNCS 218, pp. 417-426, Springer, 1986.
[14] A. Menezes, “Elliptic Public Key Cryptography”, Kluwer, 1993.
[15] J. Miret, R. Moreno, D. Sadornil, J. Tena, M. Valls, “Computing the height of volcanoes of ℓ–isogenies of elliptic curves over finite fields”, Applied Mathematics and Computation 196, no. 1, pp. 67-76, 2008.
[16] J. Miret, D. Sadornil, J. Tena, R. Tomas, M. Valls, “Exploiting Isogeny Cordillera Structure to Obtain Cryptography Good Elliptic Curves”, J. Research and Practice in Information Technology, Vol. 47, no 4, pp. 255-265, 2008.
[17] J. Miret, D. Sadornil, J. Tena, R. Tomas, M. Valls, “On avoiding ZVP attacks using isogeny volcanoes”, LNCS 5379, pp. 266-277, Springer, 2009.
[18] A. Rostovtsev, A. Stolbunov, “Public-key cryptosystem based on isogenies”, Cryptology ePrint Archive, Report 2006/145, 2006, http://eprint.iacr.org/.