# Píldora nº 49: ¿Por qué pueden utilizarse las curvas elípticas para cifrar?

## Escena 1: Criptografía de curvas elípticas

En 1987, Neal Koblitz y Victor Miller propusieron de forma independiente utilizar curvas elípticas sobre cuerpos finitos para implementar algunos criptosistemas ya existentes, lo que se conoce como Criptografía de Curva Elíptica o ECC (Elliptic Curve Cryptography).

La ventaja que ofrece esta nueva criptografía es que se pueden emplear claves más pequeñas que las utilizadas en otros criptosistemas muy extendidos como el RSA y ElGamal, manteniendo la misma seguridad.

Para analizar tanto el funcionamiento como la seguridad de esos criptosistemas, antes es preciso comprender qué son las curvas elípticas, y por qué pueden aplicarse al campo de la Criptografía.

## Escena 2: Curvas elípticas y suma de puntos

De manera resumida, una curva elíptica definida sobre los números reales es una curva cúbica definida en el plano por una ecuación de la forma $y^2 + a\,xy + b\,y = x^3 + c\,x^2 + d\,x + e$, de modo que sus infinitos puntos (x, y) tienen como coordenadas números reales, con la condición adicional de que la curva no se cruce sobre sí misma ni presente picos. La figura 1 muestra ejemplos de curvas elípticas (azul) y curvas que no consideran como tal (rojo).

Es posible sumar dos puntos de una curva elíptica obteniendo como resultado otro punto de la curva mediante las fórmulas adecuadas, aunque también se puede interpretar gráficamente por el método de la cuerda y tangente. En la figura 2, el punto R es el resultado de sumar los puntos P y Q. Este punto suma se determina trazando la cuerda que pasa por los puntos P y Q, luego se considera el tercer punto de corte de la curva, es decir -R, y se toma como resultado el punto de la curva simétrico de este último.

## Escena 3: Curvas elípticas en criptografía

Ahora bien, en criptografía no se utilizan las curvas anteriores debido a los errores de redondeo asociados a los números reales, al ser utilizados en computadoras, sino que se utilizan curvas elípticas definidas sobre cuerpos finitos. Este hecho se traduce en que las curvas tienen un número finito de puntos cuyas coordenadas son números enteros. Esta característica es de extrema importancia para poder realizar cálculos con los puntos de modo eficiente y sin errores de redondeo.

En la práctica, se consideran dos tipos de cuerpos finitos para las curvas elípticas en criptografía: los cuerpos primos $F_p$, que tienen un número primo de elementos, y los cuerpos binarios $F_2^m$, cuyo número de elementos es una potencia prima de dos.

La operación que se considera en estos casos también es la suma de puntos, de modo que cuando se suma un mismo punto muchas veces consigo mismo se obtiene otro punto, Q = P + P, n veces, que no es sino el producto de un número entero por un punto de la curva, n veces P.

## Escena 4: Seguridad de la criptografía de curvas elípticas

Al igual que la seguridad del criptosistema RSA se basa en la dificultad de resolver el problema de la factorización de un número entero muy grande y la del criptosistema de ElGamal se fundamenta en el problema del logaritmo discreto, la seguridad de la criptografía de curvas elípticas depende de la dificultad de resolver otro problema matemático: el problema del logaritmo elíptico, también llamado del logaritmo discreto en curvas elípticas (ECDLP por sus siglas en inglés).

De manera simplificada, este problema se puede expresar de la siguiente forma: dado un punto de la curva Q obtenido como el producto de un número entero n por un punto P, el problema consiste en obtener el valor de n siendo conocidos los puntos P y $Q = n \cdot P$. Como se puede apreciar, el logaritmo elíptico es la formulación aditiva del logaritmo discreto, esto es, las exponenciaciones y productos del segundo se transforman en productos y sumas en el primero.

A pesar de tratarse de un problema de formulación sencilla, a día de hoy no se ha descubierto ningún mecanismo eficiente para resolver este problema, lo que permite que la criptografía de curvas elípticas sea considerada, al menos, tan segura como el criptosistema RSA.

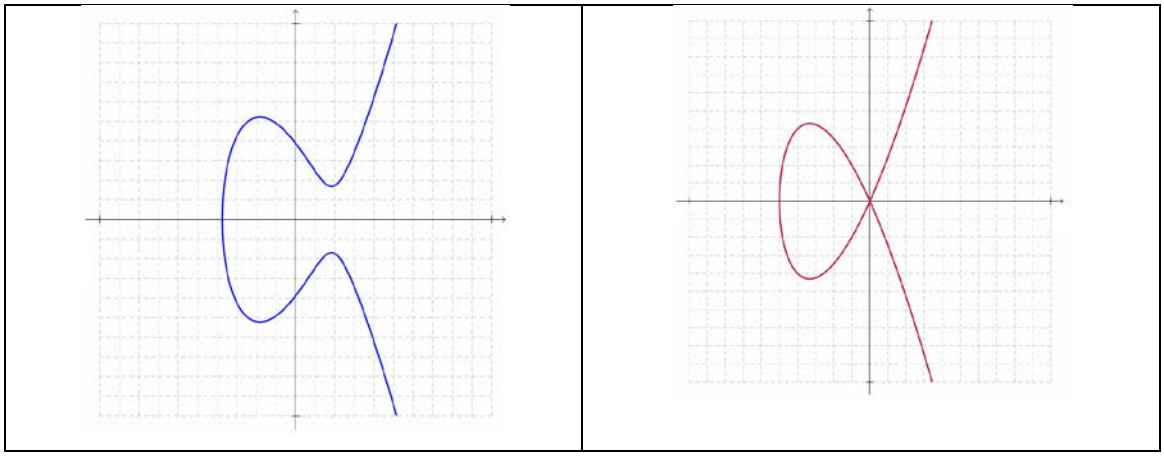

Figura 1. Curva elíptica (azul) y curva no considerada elíptica (rojo)

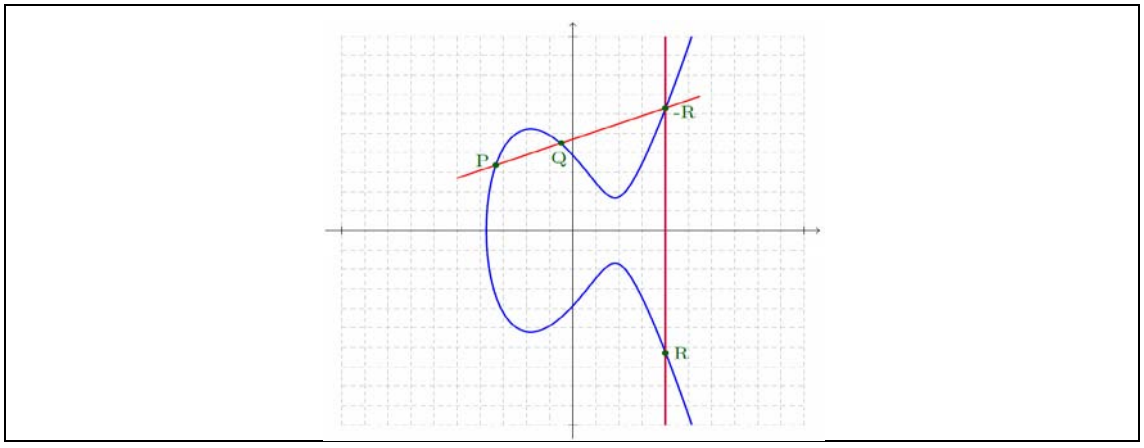


Figura 2. Suma de puntos en una curva elíptica.

Madrid, enero de 2018

Autores del guión: *Víctor Gayoso Martínez y Luis Hernández Encinas*

Dirección Proyecto Thoth: *Jorge Ramió Aguirre, Alfonso Muñoz Muñoz*

creative commons
Attribution
Noncommercial
No derivative works