Criptografía de curva elíptica

Introducción

El algoritmo de firma digital de curva elíptica (mejor conocido por su acronimo en inglés ECDSA), es la rama de la matemática aplicada criptográficamente que se utiliza en el algoritmo para generar las claves públicas y privadas que utiliza Bitcoin para que solamente el poseedor de una clave privada pueda firmar una transacción para enviar esos Bitcoin a otra dirección. En este apunte explicaremos la matemática modular, los campos finitos, las curvas elípticas para crear ecuaciones unidireccionales, lo que significa que se puede construir una clave privada (un número) y calcular fácilmente la clave pública (otro número) asociada a esta misma. Sin embargo, no puedo tomar la clave pública y fácilmente calcular su clave privada. Con la tecnología actual es virtualmente imposible encontrar una clave privada asociada a una clave pública utilizando fuerza bruta para obtenerla. Empecemos por las curvas elípticas.

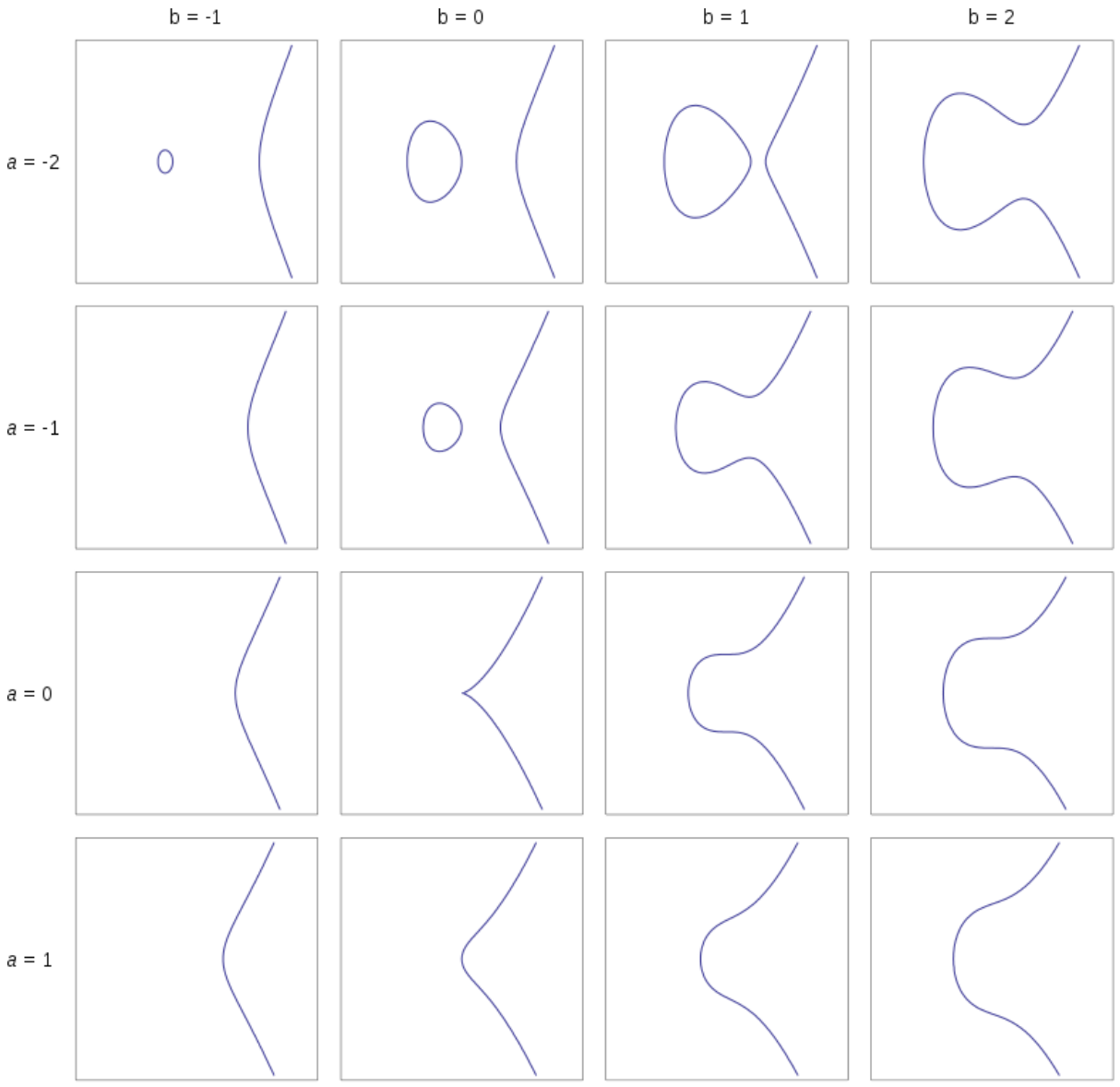
Curvas elípticas

En matemáticas, una curva elíptica es una curva algebraica plana definida por una ecuación:

$$\{(x,y) \in R^2 \mid y^2 = x^3 + ax + b, 4a^3 + 27b^2 \neq 0\} \cup \{0\}$$

La definición de curva elíptica también requiere que la curva sea no singular. Geométricamente, esto significa que el gráfico no tiene cúspides, auto intersecciones o puntos aislados. Algebraicamente, esto se cumple si y solo si el discriminante es distinto de nulo.

Esta ecuación, se puede representar de las siguientes maneras variando los parámetros "a" y "b", donde a y b son números reales. Este tipo de ecuación se llama ecuación de Weierstrass.



Distintas curvas elípticas, variando {a,b}, la región que se muestra es [−3,3]

Las curvas elípticas son útiles debido a las propiedades que exhiben. Las curvas elípticas son grupos. Los conjuntos numéricos se definen si poseen las siguientes propiedades:

1. Conjunto cerrado: Si a y b están en un grupo G, entonces a + b está en el grupo G
2. Propiedad asociativa: (a + b) + c = a + (b + c)
3. Elemento de identidad: a + 0 = 0 + a = a
4. Para cada a existe b tal que a + b = 0
5. Solo para grupos Abelianos, conmutatividad: a + b = b + a

Además de estas propiedades las curvas elípticas tienen sus propias propiedades:

1. El elemento de identidad es el punto en el infinito, 0
2. El inverso del punto P es el simétrico del eje x
3. La adición se define como: dados tres puntos alineados, puntos que no son cero, P, Q y R tienes P + Q + R = 0. El orden no importa para estos tres puntos, por lo tanto, P + (Q + R) = 0 , (P + Q) + R = 0, (P + R) + Q = 0, etc. Esto nos permite probar que las curvas elípticas son tanto conmutativas como asociativas.

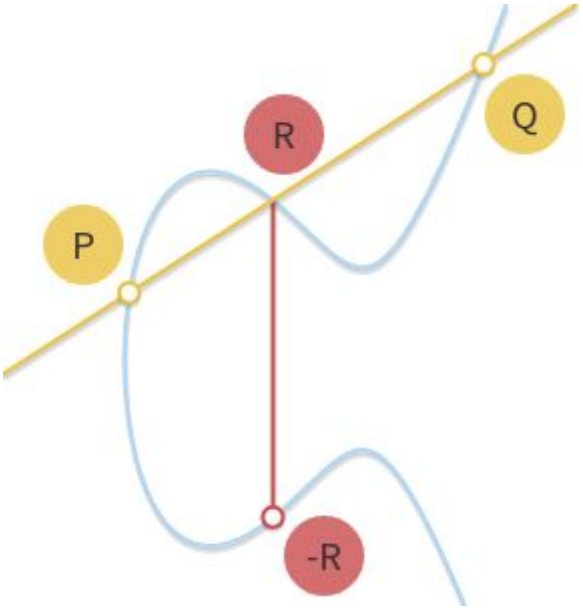
Operaciones con curvas elípticas

Adición

La ecuación anterior también nos da una ecuación para sumar dos puntos y calcular el tercer punto. Como se dijo antes, sabemos que cuando una línea pasa por dos puntos en una curva, pasará por un tercer punto. Y sabemos que:

$$\{P + Q + R = 0 \ ^{\vee} \ P + Q = -R\}$$

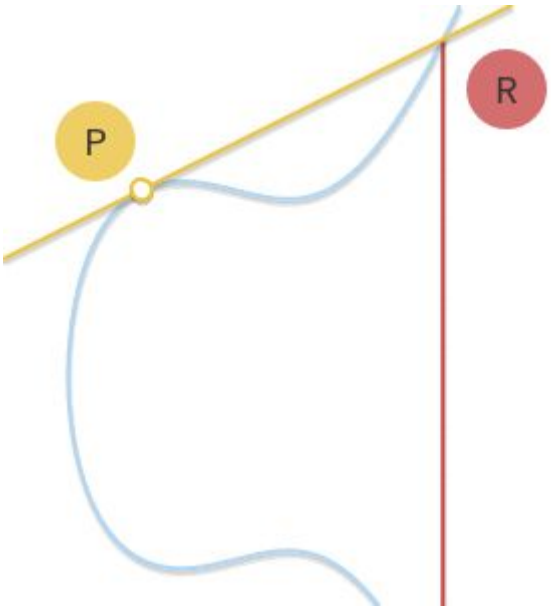
Y sabemos que -R es solo el inverso del punto R reflejado en el eje X. Como se ve en la siguiente imagen:



Adición utilizando curvas elípticas

Punto de duplicación

Hay otros puntos que también resultan interesantes, son los puntos en donde P es tangente a la curva, de modo que solo hay dos puntos de intersección entre la curva y la recta.



Punto de duplicación

Como P es tangente a la curva, los puntos P y Q son iguales

$$\{P = Q\}$$

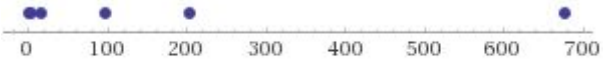
y, por lo tanto, de la ecuación anterior se desprende:

$$\{P + P + = - R \check{} 2P = - R\}$$

Por esta razón se denomina duplicación de puntos para las curvas elípticas.

Conjuntos finitos

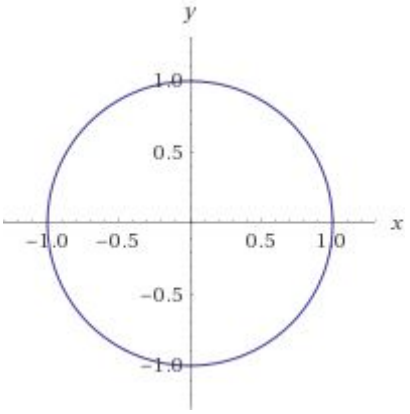
Un conjunto finito de números es simplemente una cierta cantidad de números agrupados. Los números reales son un conjunto infinito de números y el conjunto (3, 97, 205, 1,678, 17) es un conjunto finito de números. Esto significa que la multiplicación, la suma, la resta y la división (excluyendo la división por cero) están definidas y satisfacen las reglas de la aritmética conocidas como axiomas de campo. En la siguiente imagen podemos verlos representados sobre la recta de los números reales:



Un conjunto de puntos finitos de los números reales

Un conjunto de números más interesante y útil es el conjunto de enteros módulo p, donde p es un número primo. Módulo se refiere a la distancia de esos números con respecto al 0. Un

ejemplo de esto pueden ser los números {17,-17}. Un ejemplo en dos dimensiones puede ser todos los números cuya distancia al origen sea 1, representado como la circunferencia unitaria.



Un conjunto de puntos finitos en dos dimensiones

Matemática modular

En matemática, la aritmética modular es un sistema de aritmética para enteros, donde los números se "envuelven" al alcanzar un cierto valor: el módulo (módulo plural). El enfoque moderno de la aritmética modular fue desarrollado por Carl Friedrich Gauss en su libro *"Disquisitiones Arithmeticae"*, publicado en 1801.

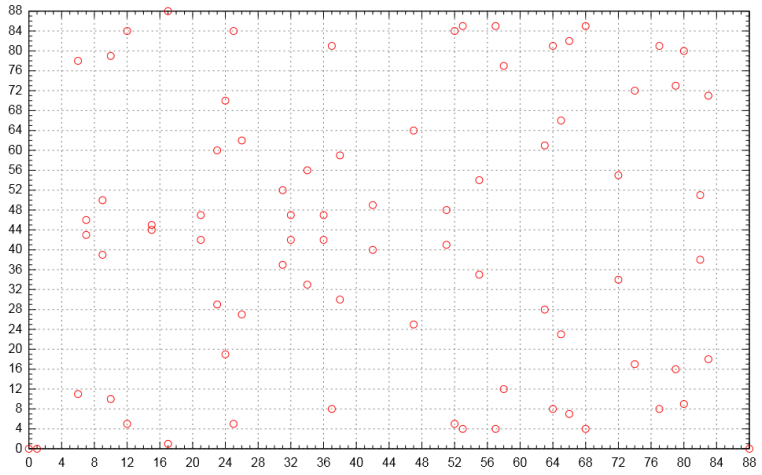
Un uso familiar de la aritmética modular se encuentra en el reloj de 12 horas, en el que el día se divide en dos períodos de 12 horas. En este caso usamos módulo 12, de esta forma 5 módulo 12 = 5, y también 17 módulo 12 = 5.

Curvas elípticas y conjuntos finitos combinados

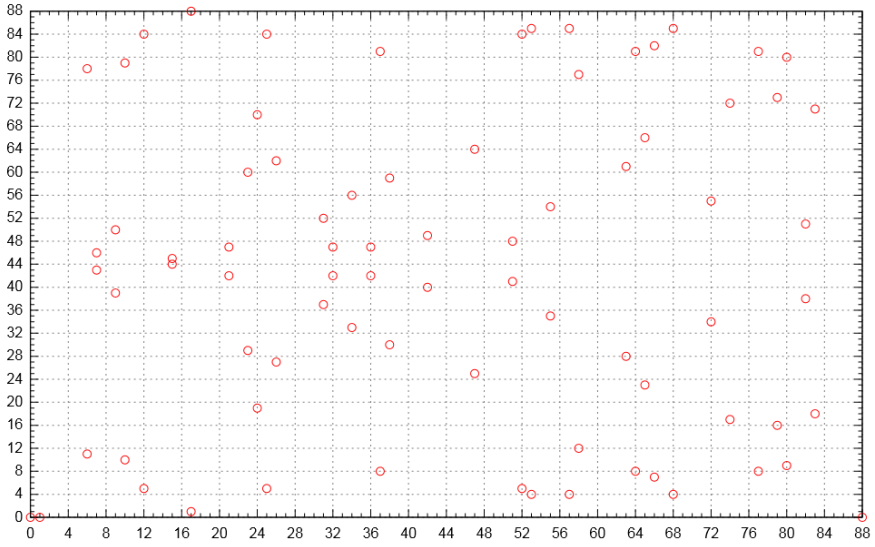
Cuando uno combina estos dos campos lo que se obtiene es la criptografía de curva elíptica sobre espacios finitos. La ecuación que describe este campo es:

$$\{(x,y) \in F_p^2 \mid y^2 \equiv x^3 + ax + b \pmod p \ , \ 4a^3 + 27b^2 \neq 0 \pmod p\} \cup \{0\}$$

Si queremos representar esta ecuación, lo que obtenemos son los siguientes gráficos:

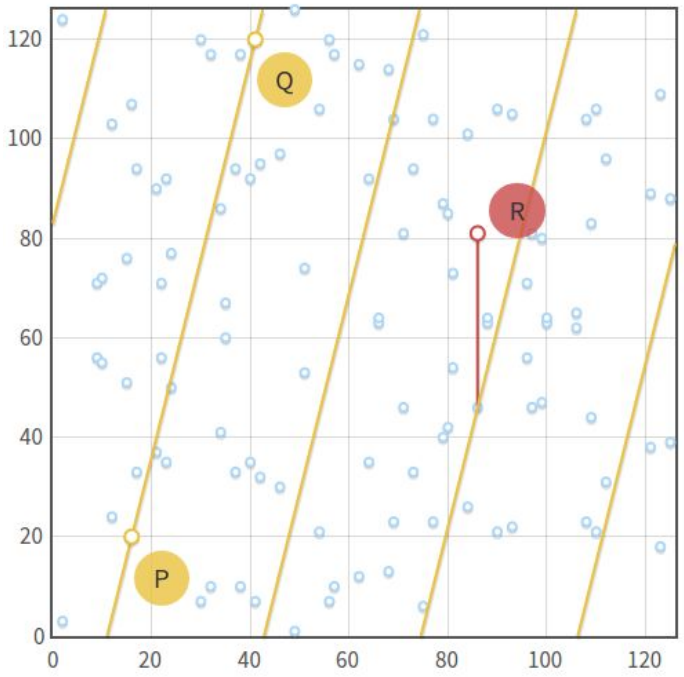


Conjunto de puntos afines de la curva elíptica $y^2 = x^3 - x$ sobre el campo finito F_{61}.



Conjunto de puntos afines de la curva elíptica $y^2 = x^3 - x$ sobre el campo finito F_{89}.

Si observan bien, los puntos guardan simetría, lo que significa que todavía podemos utilizar la suma de puntos P + Q = -R donde dibujamos una línea que conecta P, Q y R y reflejamos R, para obtener -R. En un conjunto finito, las curvas elípticas se ven muy diferentes. Es similar al juego de los 1980 “Asteroid" en el que salíamos de la parte superior de la pantalla e ingresamos en la parte inferior de la misma. En la siguiente figura podemos apreciar la operatoria de la adición de puntos:



La adición de puntos de las curvas elípticas se sigue cumpliendo, incluso cuando utilizamos un conjunto finito de puntos.

En donde se sigue cumpliendo que:

$$\{P + Q + R = 0 \ ˇ \ P + Q = - R\}$$

Aunque las curvas elípticas estén definidas sobre un conjunto finito de puntos aún conservan todas las propiedades de un conjunto matemático, como lo describimos en los puntos anteriores.

Multiplicación escalar

Repasemos rápidamente que si una línea pasa por dos puntos en una curva elíptica pasará por un tercer punto y la ecuación que nos relaciona estos puntos es:

$$\{P + Q + R = 0 \ ˇ \ P + Q = - R\} \ Adición \ de \ puntos$$

Además, si P es tangente a la curva elíptica, entonces la ecuación que nos relaciona estos puntos es:

$$\{P + P + = - R \ ˇ \ 2P = - R\} \ Duplicación \ de \ punto$$

La adición de puntos y la duplicación de puntos nos permiten definir la multiplicación escalar para curvas elípticas:

$$\{xP = R\}\ Multiplicación\ escalar$$

Donde x es un escalar, P es un punto tangente a la curva y R es el punto resultante de adicionar P en sí mismo x veces. Hagamos un ejemplo sencillo:

$$\{3P = R\}\ primer\ paso,\ se\ define\ el\ escalar$$

$$\{P + 2P = R\}\ segundo\ paso,\ se\ descompone\ el\ 3\ en\ 1 + 2$$

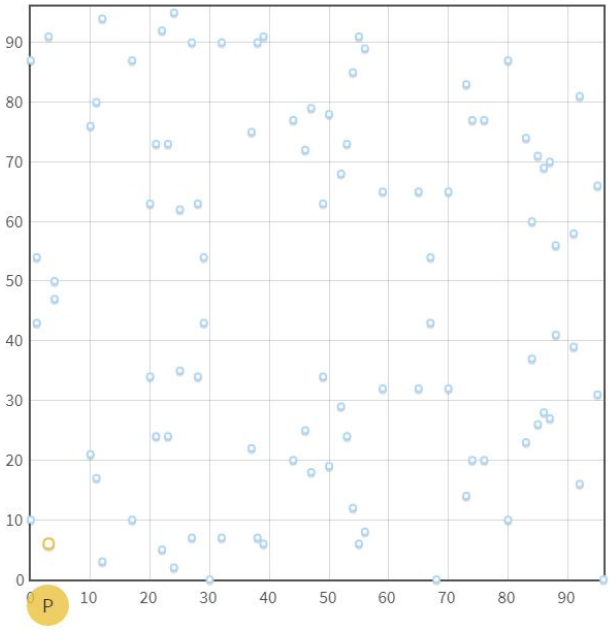
$$\{P + Q = R\}\ tercer\ paso,\ el\ punto\ 2P\ es\ igual\ a\ el\ punto\ Q\ por\ propiedad\ de\ duplicación\ de\ punto$$

Sumamos el punto P y el punto Q para obtener R. Así es cómo la adición de puntos y la duplicación de puntos nos permiten crear la multiplicación escalar.

Las curvas elípticas sobre campos finitos tienen las mismas propiedades de los conjuntos y podemos adicionar continuamente P con sigo mismo creando la multiplicación escalar.

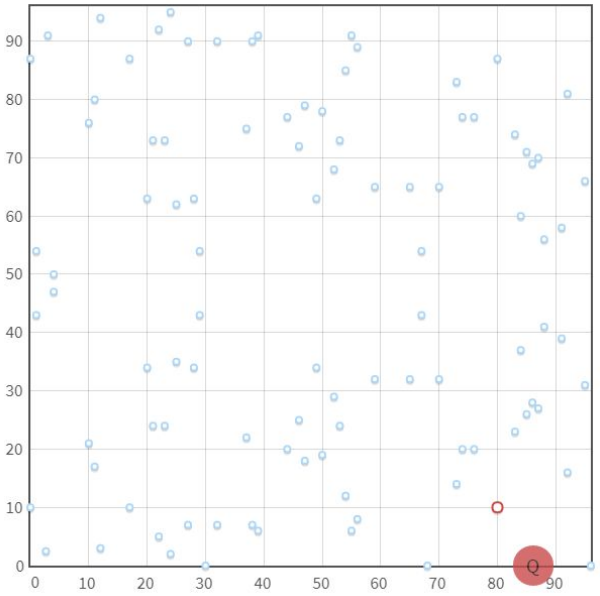
Recordemos nuestro ejemplo del reloj que usamos para las operaciones de matemática modular. Cuando se adiciona P a sí mismo una y otra vez, es similar a mover P alrededor de un reloj. Esto lo podemos ver en las siguientes imágenes asociadas al ejemplo realizado.

Paso 1:



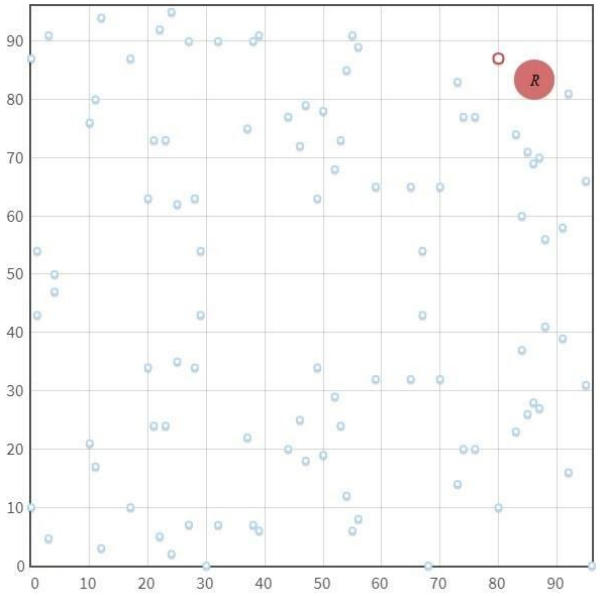
En este caso x es igual a 1 entonces P=Q

Paso 2:



En este caso x es igual a 2 entonces 2P=Q

Paso 3



En este caso x es igual a 3 entonces P+2P=R

En el caso de Bitcoin, se utilizan los siguientes parámetros de las curvas elipticas:

1.Módulo del número primo: $2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$ ⟶ este es un número realmente muy grande. También se representa en hexadecimal como: FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE FFFFFC2F

2.Curva elíptica donde a = 0 y b = 7

3.Punto base P en hexadecimal = 04 79BE667E F9DCBBAC 55A06295 CE870B07 029BFCDB 2DCE28D9 59F2815B 16F81798 483ADA77 26A3C465 9DA4FBFC 0E1108A8 F8174B448 A6855419 9C47

4.Orden en hexadecimal = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE BAAEDCE6 AF48A03B BFD25E8C D0364141

Existe un estándar de criptografía administrados por la organización, Standards for Efficient Cryptography Group (SEC), Bitcoin utiliza el estándar secp256k1.

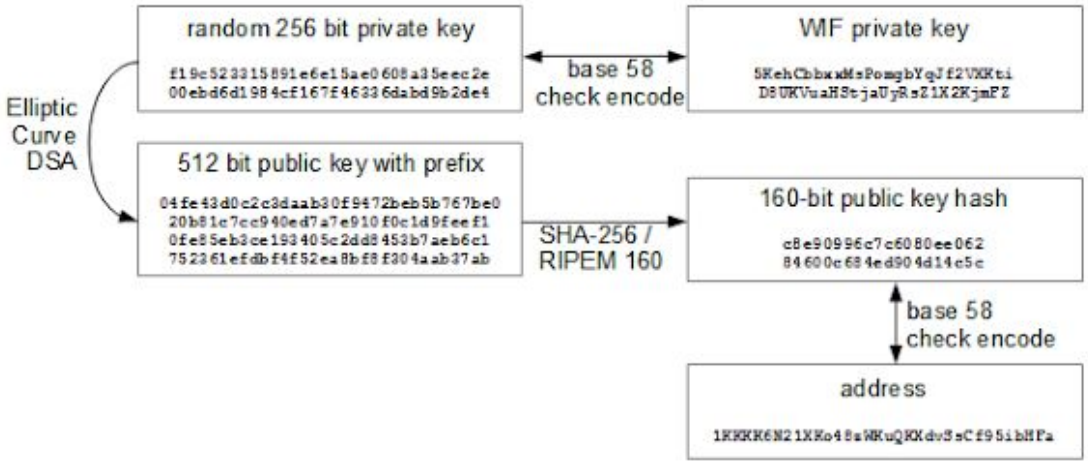
Por lo tanto, la clave privada para Bitcoin es solo un número elegido arbitrariamente entre 1 y el orden anterior mencionado. La clave pública puede ser fácilmente derivada a través de la multiplicación escalar conociendo la clave privada.

Una vez obtenida una clave privada (de una fuente de números random) y se multiplica por el punto base P, y se obtiene un nuevo punto (x, y) en el campo finito de curvas elípticas. Esta es tu clave pública. Es computacionalmente fácil usar su clave privada y multiplicarla por el punto

base para obtener la clave pública, pero es computacionalmente difícil comenzar con la clave pública y hacer el camino inverso para calcular la clave privada.

Claves públicas y privadas y direcciones Bitcoin

En el siguiente gráfico se muestra como se relacionan las claves públicas y privadas para obtener una dirección de Bitcoin



Es un tema que estudiaremos en detalle más adelante, en el tema de direcciones Bitcoin.