UNIVERSITY NAME

DOCTORAL THESIS

Hierarchical deterministic wallet

Author:
Daniele FORNARO

Supervisor:
Daniele MARAZZINA

A thesis submitted in fulfillment of the requirements for the degree of Mathematical Engeneering

in the

Research Group Name
Department or School Name

January 15, 2018

Declaration of Authorship

I, Daniele FORNARO, declare that this thesis titled, "Hierarchical deterministic wallet" and the work presented in it are my own. I confirm that:

- This work was done wholly or mainly while in candidature for a research degree at this University.
- Where any part of this thesis has previously been submitted for a degree or any other qualification at this University or any other institution, this has been clearly stated.
- Where I have consulted the published work of others, this is always clearly attributed.
- Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work.
- I have acknowledged all main sources of help.
- Where the thesis is based on work done by myself jointly with others, I have made clear exactly what was done by others and what I have contributed myself.

Signed:

Date:

"Thanks to my solid academic training, today I can write hundreds of words on virtually any topic without possessing a shred of information, which is how I got a good job in journalism."

Dave Barry

UNIVERSITY NAME

Abstract

Faculty Name
Department or School Name

Mathematical Engeneering

Hierarchical deterministic wallet

by Daniele FORNARO

The Thesis Abstract is written here (and usually kept to just this page). The page is kept centered vertically so can expand into the blank space above the title too...

Acknowledgements

The acknowledgments and the people to thank go here, don't forget to include your project advisor…

Contents

List of Figures

List of Tables

List of Abbreviations

LAH	**L**ist **A**bbreviations **H**ere
WSF	**W**hat (it) **S**tands **F**or

Physical Constants

Speed of Light $c_0 = 2.997\,924\,58 \times 10^8\ \mathrm{m\,s^{-1}}$ (exact)

List of Symbols

a	distance	m
P	power	W ($\mathrm{J\,s^{-1}}$)
ω	angular frequency	rad

For/Dedicated to/To my…

Chapter 1

Elliptic Curve Geometry

1.1 Introduction

Bitcoin security is based on public and private key cryptograpy. The main concept is that it is simple to compute the public key, knowing the private, but it is infeasible to calculate the private key, knowing the public.

In order to obtain this result a particular Elliptic Curve is used.

1.2 Elliptic Curve over $\mathbb{F}_p$

A point Q, which coordinates are x and y, belong to an Elliptic Curve if and only if Q satisfies the following equation:

$$y^2 = x^3 + ax + b \quad \text{over } \mathbb{F}_p \tag{1.1}$$

Where $\mathbb{F}_p$ is the finite field defined over the set of integers modulo p and a and b are the coefficients of the curve.

We can rewrite the equation 1.1 in the following way:

$$y^2 = x^3 + ax + b \mod p \tag{1.2}$$

Figure 1.1 shows some examples of Elliptic Curve over $\mathbb{F}_p$ with $a = -7$ and $b = 10$

1.2.1 Operations

A point on the Elliptic Curve has some particular properties:

- Symmetry
- Point addition
- Scalar multiplication

Symmetry

For every point in the x axis exists two points in the y axis. Suppose that a point $P(x, y)$ belongs to the Elliptic Curve, then it must satisfy the equation 1.1. So it is easy to prove that the point $Q(x, p - y)$ belongs to the curve too.

Furthermore we have $P = -Q$, from the moment that $P + Q = 0$ (see addition below).

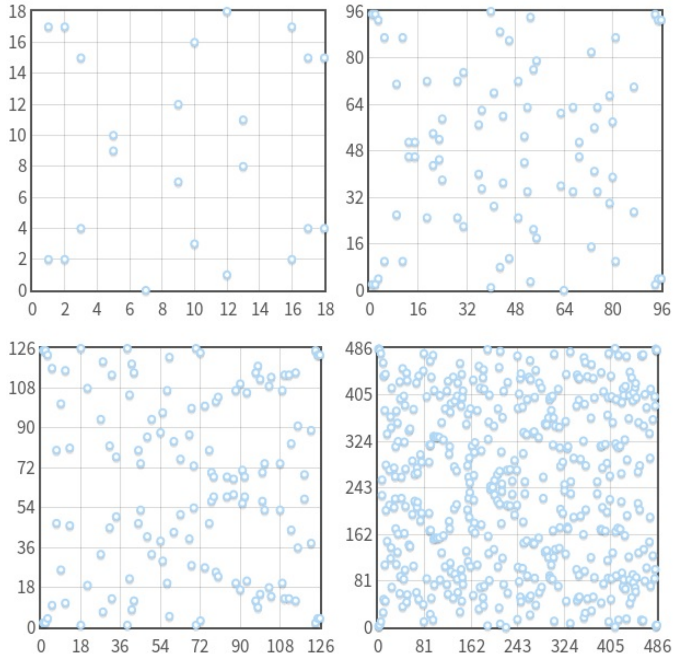

FIGURE 1.1: Points on the Elliptic Curve $y^2 = x^3 - 7x + 10 \mod p$, with $p = 19, 97, 127, 487$

Point addition

We need to change our definition of addition in order to make it works in $\mathbb{F}_p$. In this framework we claim that if three points are aligned over the finite field $\mathbb{F}_p$, then they have zero sum.
So $P + Q = R$ if and only if P, Q and $-R$ are aligned, in the sense shown in figure 1.2

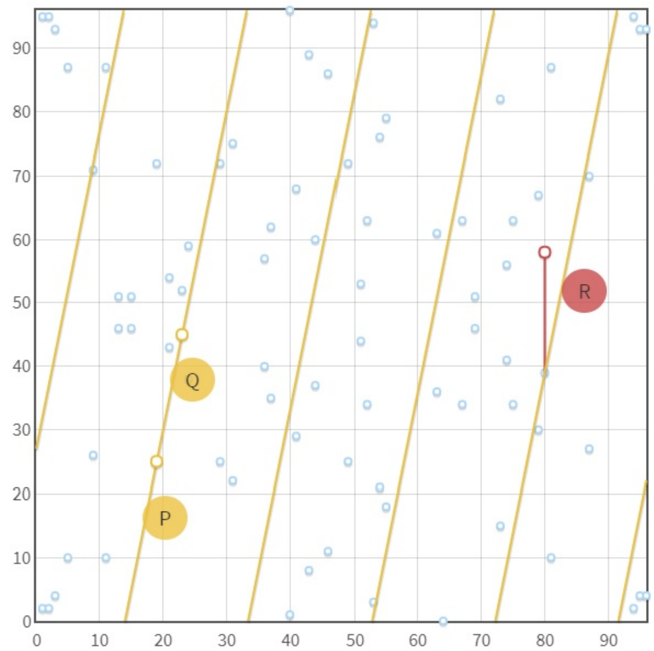

FIGURE 1.2: Elliptic Curve $y^2 = x^3 - 7x + 10 \mod 97$

The equations for calculating point additions are the follow:
Suppose that A and B belong to the Elliptic Curve.

$$A = (x_1, y_1) \quad B = (x_2, y_2)$$

Let's defined $A + B := (x_3, y_3)$
So we have:

$$s = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, & \text{if } x_1 \neq x_2 \\ \\ \dfrac{3x_1^2 + a}{2y_1}, & \text{if } x_1 = x_2 \end{cases}$$

$$x_3 = s^2 - x_1 - x_2 \mod p$$
$$y_3 = s(x_1 - x_3) - y_1 \mod p$$

Scalar multiplication

Once defined the addition, any multiplication can be defined as:

$$nP = \underbrace{P + P + \cdots + P}_{n \text{ times}}$$

When n is a very large number can be difficult or even infeasible to compute nP in this way, but we can use the *double and add algorithm* in order to perform multiplication in $\mathcal{O}(\log n)$ steps.

1.2.2 Group order

An elliptic curve defined over a finite field is a group and so it has a finite number of points. This number is called order of the group.
If the prime order is a very large number, it is impossible to count all the point in that field, but there is an algorithm that allows to calculate the order of a group in a fast and efficient way: *Schoof's algorithm*.

Cyclic subgroups

Let's consider a generic point P, we have:

$$nP + mP = \underbrace{P + \cdots + P}_{n \text{ times}} + \underbrace{P + \cdots + P}_{m \text{ times}} = \underbrace{P + \cdots + P}_{n+m \text{ times}} = (n+m)P$$

So multiple of P are closed under addition and this is enough to prove that the set of the multiples of P is a cyclic subgroup of the group formed by the elliptic curve.

The point P is called **generator** of the cyclic subgroup.

Remark *The order of P is linked to the order of the elliptic curve by Lagrange's theorem, which states that the order of a subgroup is a divisor of the order of the parent group.*

Remark *If the order of the group is a prime number, all the point P generate a subgroup with the same order of the group.*

1.3 Bitcoin private-public key cryptography

1.3.1 Bitcoin Elliptic Curve

Bitcoin uses a specific Elliptic Curve defined over the finite field of the natural numbers, where $a = 0$ and $b = 7$.

The equation 1.1 becomes:

$$y^2 = x^3 + 7 \mod p \tag{1.3}$$

The *mod p* (modulo prime number) indicates that this curve is over a finite field of prime order $p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$.

The *order* of this Elliptic Curve is a very large prime number, close to 2^{256}, but smaller then p.

Let's consider a particular point G, called generator, with:

$$x = 79BE667EF9DCBBAC55A06295CE870B07029BFCDB2DCE28D959F2815B16F81798$$
$$y = 483ADA7726A3C4655DA4FBFC0E1108A8FD17B448A68554199C47D08FFB10D4B8$$

From the moment that the order of the group is a prime number, the order of any subgroup is equal to the order of the entire group. In particular the order of the subgroup generated by G is equal to *order*.

Definition *A private key is a number choosen in the range beetwen 1 and* ***order****.*

Definition *A public key W is a point in the Bitcoin EC, derived from a private key k in the following way:*

$$W = k \cdot G \tag{1.4}$$

Where the multiplication between k and G is defined in the previous chapter.

This is a *one way* function, in the sense that computing the scalar multiplication, knowing the private key is simple, but make the reverse is infeasible.

Remark *It is infeasible to calculate a private key knowing the public key.*

1.3.2 Bitcoin keys rapresentation and addresses

In order to make it easy to store and recognise keys, some encods were designed.

A public key, a point in the EC, can be rapresented in two way: *uncompressed* or *compressed*.

Uncompressed public key

An uncompressed public key is rapresented in hexadecimal digits, and it is obtained simply concatenating the x coordinate with the y coordinate and adding 04 at the beginning, for a total of 130 hexadecimal digits.

Example of an uncompressed public key:
0450863AD64A87AE8A2FE83C1AF1A8403CB53F53E486D8511DAD8A04887E5B235
22CD470243453A299FA9E77237716103ABC11A1DF38855ED6F2EE187E9C582BA6

Compressed public key

A compressed public key is obtained simply taking the x coordinate and adding 02 at the begging if the y coordinate is even, 03 otherwise.
This is due to the *symmetry properties* of a point of the EC.

Example of a public key compressed:
0250863AD64A87AE8A2FE83C1AF1A8403CB53F53E486D8511DAD8A04887E5B2352

WIF Private Key

WIF stands for wallet import format and is the standard way used to write down a private key.

- Add a version number (80 for Bitcoin) in front of the private key, in order to recognize quickly for what cryptocurrency that private key was used.
- Add 01 at the end of the private key if you want a WIF *compressed*, none if you want a WIF *uncompressed*. The difference between these two types is that from a *compressed* private key a *compressed* public key is expected and from a *uncompressed* private key a *uncompressed* public key is expected.
- Addd a checksum at the end, obtained applying the SHA256 function twice to the string previously obtained, take the first 4 bytes (8 hexadecimal digits) and put them at the end of the string.
- Compute the Base58Encode, obtaining a 52 digit string.

Example of private key WIF:
KwdMAjGmerYanjeui5SHS7JkmpZvVipYvB2LJGU1ZxJwYvP98617

Address

Among the Bitcoin transactions, one of the most used is a *Pay-to-PubkeyHash*, meaning that in the transaction you will not write directly the public key, but the hash of that public key.
The hash function used in this freamwork is the HASH160 function, applied to the *compressed* public key. This is an irreversible procedure, so you cannot obtain the public key from the public key hash.

In order to obtain a valid Bitcoin address, it is needed to encode the *PubkeyHash* in base58, adding first the version in front, the checksum at the end and then encode everything with Base58Encode, obtaining a 34 digit string.

Example of an Address:
1BvBMSEYstWetqTFn5Au4m4GFg7xJaNVN2

Chapter 2

HD Wallet

A Bitcoin wallet is a structure used to store keys.

There exist two different type of wallets:

- Nondeterministic Wallets
- Deterministic Wallets

Remark *Bitcoin wallets contains keys, not coins.*

2.1 Nondeterministic Wallets

Appendix A

Frequently Asked Questions

A.1 How do I change the colors of links?

The color of links can be changed to your liking using:
`\hypersetup{urlcolor=red}`, or
`\hypersetup{citecolor=green}`, or
`\hypersetup{allcolor=blue}`.
If you want to completely hide the links, you can use:
`\hypersetup{allcolors=.}`, or even better:
`\hypersetup{hidelinks}`.
If you want to have obvious links in the PDF but not the printed text, use:
`\hypersetup{colorlinks=false}`.

Bibliography

Arnold, A. S. et al. (Mar. 1998). "A Simple Extended-Cavity Diode Laser". In: *Review of Scientific Instruments* 69.3, pp. 1236–1239. URL: http://link.aip.org/link/?RSI/69/1236/1.

Hawthorn, C. J., K. P. Weber, and R. E. Scholten (Dec. 2001). "Littrow Configuration Tunable External Cavity Diode Laser with Fixed Direction Output Beam". In: *Review of Scientific Instruments* 72.12, pp. 4477–4479. URL: http://link.aip.org/link/?RSI/72/4477/1.

Wieman, Carl E. and Leo Hollberg (Jan. 1991). "Using Diode Lasers for Atomic Physics". In: *Review of Scientific Instruments* 62.1, pp. 1–20. URL: http://link.aip.org/link/?RSI/62/1/1.