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 8, 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 Point on an Elliptic Curve

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

$$y^2 = x^3 + ax + b \tag{1.1}$$

over a certain field $\mathbb{F}_p$, where a and b are the coefficients of the curve. Here we want to analyse only the

The curve is specified by the definition of the coefficients and the field $\mathbb{F}_p$ should be consider for simplicity the

1.2.1 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:

$$y^2 = x^3 + 7 \mod p \tag{1.2}$$

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

1.2.2 Proprierties

A point on the Bitcoin Elliptic Curve has some particular proprierties:

- 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 1.2. So it is easy to prove that the point $Q(x, p - y)$ belongs to the curve too.

Point addition

Suppose that A, B and C are points of an Elliptic Curve that satisfy

$$A + B + C = 0 \mod p \tag{1.3}$$

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.