FACULTY
OF INFORMATION
TECHNOLOGY
CTU IN PRAGUE

ASSIGNMENT OF MASTER'S THESIS

Title:	Summation polynomials and the discrete logarithm problem on elliptic curve
Student:	Bc. Matyáš Hollmann
Supervisor:	Ing. Ivo Petr, Ph.D.
Study Programme:	Informatics
Study Branch:	Computer Security
Department:	Department of Information Security
Validity:	Until the end of winter semester 2020/21

Instructions

Discrete logarithm problem (DLP) is a fundamental problem arising in modern cryptography. While there exist subexponential algorithms that solve DLP in multiplicative groups of finite fields, no such algorithms are known for groups of points of elliptic curves (ECDLP). Attempts to develop index calculus methods for elliptic curves include so called summation polynomials that give algebraic relations whose solution may give a solution of ECDLP.

The goal of the thesis is to get acquainted with cryptography of elliptic curves, give thorough description of the state of the art of the summation polynomial algorithm, implement it in suitable language and test its performance. Student will focus on available methods of effective generation and solution (Groebner basis and other methods) of algebraic relations appearing in the algorithm.

References

[1] I. Semaev, New algorithm for the discrete logarithm problem on elliptic curves, Cryptology ePrint Archive, Report 2015/310
[2] S. D. Galbraith and S. W. Gebregiyorgis, Summation polynomial algorithms for elliptic curves in characteristic two, Cryptology ePrint Archive, Report 2014/806

prof. Ing. Róbert Lórencz, CSc.
Head of Department

doc. RNDr. Ing. Marcel Jiřina, Ph.D.
Dean

Prague February 22, 2019

FACULTY
OF INFORMATION
TECHNOLOGY
CTU IN PRAGUE

Master's thesis

Summation polynomials and the discrete logarithm problem on elliptic curve

Bc. Matyáš Hollmann

Department of Information Security
Supervisor: Ing. Ivo Petr, Ph.D.

April 11, 2019

Acknowledgements

THANKS (remove entirely in case you do not with to thank anyone)

Declaration

I hereby declare that the presented thesis is my own work and that I have cited all sources of information in accordance with the Guideline for adhering to ethical principles when elaborating an academic final thesis.

I acknowledge that my thesis is subject to the rights and obligations stipulated by the Act No. 121/2000 Coll., the Copyright Act, as amended. In accordance with Article 46(6) of the Act, I hereby grant a nonexclusive authorization (license) to utilize this thesis, including any and all computer programs incorporated therein or attached thereto and all corresponding documentation (hereinafter collectively referred to as the "Work"), to any and all persons that wish to utilize the Work. Such persons are entitled to use the Work in any way (including for-profit purposes) that does not detract from its value. This authorization is not limited in terms of time, location and quantity. However, all persons that makes use of the above license shall be obliged to grant a license at least in the same scope as defined above with respect to each and every work that is created (wholly or in part) based on the Work, by modifying the Work, by combining the Work with another work, by including the Work in a collection of works or by adapting the Work (including translation), and at the same time make available the source code of such work at least in a way and scope that are comparable to the way and scope in which the source code of the Work is made available.

In Prague on April 11, 2019 . . . .

Czech Technical University in Prague
Faculty of Information Technology
© 2019 Matyáš Hollmann. All rights reserved.
This thesis is school work as defined by Copyright Act of the Czech Republic. It has been submitted at Czech Technical University in Prague, Faculty of Information Technology. The thesis is protected by the Copyright Act and its usage without author's permission is prohibited (with exceptions defined by the Copyright Act).

0.0.1 Citation of this thesis

Hollmann, Matyáš. *Summation polynomials and the discrete logarithm problem on elliptic curve.* Master's thesis. Czech Technical University in Prague, Faculty of Information Technology, 2019.

Abstrakt

V několika větách shrňte obsah a přínos této práce v českém jazyce.

Klíčová slova Replace with comma-separated list of keywords in Czech.

Abstract

Summarize the contents and contribution of your work in a few sentences in English language.

Keywords Replace with comma-separated list of keywords in English.

Contents

List of Figures

Introduction

Chapter **1**

Mathematical background

In this chapter we are going to define terms that will be used in the rest of this thesis. The first part is focused on terms common in general algebra, the second part will deal with elliptic curves and a little bit of algebraic geometry.

1.1 Introduction to general algebra

Definition 1.1.1. A **group** G is an ordered pair $(M, \circ)$, where M is a non-empty set and binary operation $\circ : M \times M \to M$ (sometimes called the group law of G) that satisfies three requirements known as group axioms:

- $\forall x, y, z \in M : x \circ (y \circ z) = (x \circ y) \circ z,$ (associativity)
- $\exists e \in M, \forall x \in M : e \circ x = x \circ e = x,$ (identity element)
- $\forall x \in M, \exists x^{-1} \in M : x \circ x^{-1} = x^{-1} \circ x = e.$ (inverse element)

Remark. M is closed under the operation $\circ$.

Notational Remark. When we are gonna talk about an element g of a group G ($g \in G$) we are actually gonna mean that g is an element of the underlying set M ($g \in M$).

Groups satisfying commutativity law:

- $\forall x, y \in M : x \circ y = y \circ x,$

are called **Abelian groups** (in honour of a famous Norwegian mathematician Niels Henrik Abel [1]).

Definition 1.1.2. If the set M has a finite number of elements, $G = (M, \circ)$ is a **finite** group. **Order** of the finite group G is the number of elements of the underlying set M and we denote it by $\#G$. If the set M is infinite, the order of G is infinite as well.

Remark. In every group there exist just one unique identity element. Also for every element $q \in G$ there exists just one inverse element denoted q^{-1} in the multiplicative notation and $-q$ in the additive notation. Inverse of a product of two group elements is a product of respective inverses in the reversed order (order does matter in non-commutative groups).

Identity element in additive notation is called **zero** and denoted by 0, in the multiplicative notation **unit** and denoted 1.

In an additive group G we define **multiplication** by an integer (repeated application of the group law) as follows:

$$\forall p \in G,\ \forall k \in \mathbb{Z} : kp := \begin{cases} \underbrace{p + p + \cdots + p}_{\text{k-times}} & k > 0, \\ 0 \text{ (identity element)} & k = 0, \\ \underbrace{(-p) + (-p) + \cdots + (-p)}_{\text{k-times}} & k < 0. \end{cases}$$

In a multiplicative group G we define **exponentiation** (repeated application of the group law) in a similar manner:

$$\forall p \in G,\ \forall k \in \mathbb{Z} : p^k := \begin{cases} \underbrace{p \cdot p \cdot \cdots \cdot p}_{\text{k-times}} & k > 0, \\ 1 \text{ (identity element)} & k = 0, \\ \underbrace{p^{-1} \cdot p^{-1} \cdot \cdots \cdot p^{-1}}_{\text{k-times}} & k < 0. \end{cases}$$

Definition 1.1.3. Order of an element $a \in G$ is the smallest positive integer k such that: $a^k = 1$ (similarly $ka = 0$ in additive notation), we denote it by $\#a = k$, if there isn't such k we say the order of a is infinite (this case may only happen if G itself is of infinite order and we are mostly interested in finite groups in this thesis). Elements of finite order are sometimes called **torsion** elements.

Remark. Order of the identity element $\in G$ is always 1 and due to the uniqueness of the identity element it's also the only element $\in G$ this order.

CHAPTER 2

Discrete logarithm problem on elliptic curves

Chapter 3

State-of-the-art

Chapter **4**

Algorithms

Pollard-Rho Pohling-Hellmann BabySteps-Giants (mention mods) F4, F5 Groebner SumPoly [**?**]

Chapter 5

Analysis and design

Chapter 6

Realisation

Conclusion

Bibliography

[1] THE EDITORS OF ENCYCLOPAEDIA BRITANNICA. *Niels Henrik Abel: NORWEGIAN MATHEMATICIAN.* Encyclopaedia Britannica [online]. Apr 2, 2019 [Accessed on 2019-04-10]. Available at: `https://www.britannica.com/biography/Niels-Henrik-Abel`

Appendix A

Acronyms

GUI Graphical user interface

XML Extensible markup language

Appendix B

Contents of enclosed CD

```
readme.txt ............ the file with CD contents description
exe ....................... the directory with executables
src ..................... the directory of source codes
  wbdcm ...................... implementation sources
  thesis ....... the directory of LaTeX source codes of the thesis
text ........................ the thesis text directory
  thesis.pdf ................ the thesis text in PDF format
  thesis.ps .................. the thesis text in PS format
```