Elliptic Curve Cryptography

Student Name: T. Butterfield

Supervisor Name: M. Bordewich

Submitted as part of the degree of BSc Computer Science to the

Board of Examiners in the Department of Computer Sciences, Durham University

February 26, 2021

***Abstract* —** These instructions give you guidelines for preparing the final paper. DO NOT change any settings, such as margins and font sizes. Just use this as a template and modify the contents into your final paper. Do not cite references in the abstract.

The abstract must be a Structured Abstract with the headings **Context/Background**, **Aims**, **Method**, **Results**, and **Conclusions**. This section should not be longer than half of a page, and having no more than one or two sentences under each heading is advised.

Background - Diffie-Hellman, RSA, ...

Aims - Create system implementing ECC safe curves

Method - Euclid's extended algorithm, point addition, point multiplication, ...

Results - Cannot discover information about private key, enables secure communication

Conclusions - Strength of ECC, smaller key size than RSA, much more suitable for mobile devices

***Keywords* —** Put a few keywords here.

Elliptic Curve Cryptography, Elliptic Curve Diffie-Hellman, Elliptic Curve Digital Signature Algorithm

I INTRODUCTION

This section briefly introduces the general project background, the research question you are addressing, and the project objectives. It should be between 2 to 3 pages in length. Do not change the font sizes or line spacing in order to put in more text.

Note that the whole report, including the references, should not be longer than 20 pages in length. The system will not accept any report longer than 20 pages. It should be noted that not all the details of the work carried out in the project can be represented in 20 pages. It is therefore vital that the Project Log book be kept up to date as this will be used as supplementary material when the project paper is marked. There should be between 10 and 20 referenced papers—references to Web based pages should be less than 10%.

- Abstract & Introduction make 5% of paper
- Adequacy of Abstract
- Description of background - Diffie-Hellman, RSA, ECC
- Discussion of aims and achievements - Aimed to create system which implemented safe curves

II RELATED WORK

This section presents a survey of existing work on the problems that this project addresses. it should be between 2 to 4 pages in length. The rest of this section shows the formats of subsections as well as some general formatting information for tables, figures, references and equations.

- 15% of paper
- Adequacy of literature surveyed
- Critical analysis

A Main Text

The font used for the main text should be Times New Roman (Times) and the font size should be 12. The first line of all paragraphs should be indented by 0.25in, except for the first paragraph of each section, subsection, subsubsection etc. (the paragraph immediately after the header) where no indentation is needed.

B Figures and Tables

In general, figures and tables should not appear before they are cited. Place figure captions below the figures; place table titles above the tables. If your figure has two parts, for example, include the labels "(a)" and "(b)" as part of the artwork. Please verify that figures and tables you mention in the text actually exist. make sure that all tables and figures are numbered as shown in Table 1 and Figure 1.

Table 1: UNITS FOR MAGNETIC PROPERTIES

Symbol	Quantity	Conversion from Gaussian

C References

The list of cited references should appear at the end of the report, ordered alphabetically by the surnames of the first authors. References cited in the main text should use Harvard (author, date) format. When citing a section in a book, please give the relevant page numbers, as in (Budgen 2003, p293). When citing, where there are either one or two authors, use the names, but if there are more than two, give the first one and use "et al." as in , except where this would be ambiguous, in which case use all author names.

You need to give all authors' names in each reference. Do not use "et al." unless there are more than five authors. Papers that have not been published should be cited as "unpublished" (Euther 2006). Papers that have been submitted or accepted for publication should be cited as "submitted for publication" as in (Futher 2006) . You can also cite using just the year when the author's name appears in the text, as in "but according to Futher (2006), we ...". Where an authors has more than one publication in a year, add 'a', 'b' etc. after the year.

III SOLUTION

This section presents the solutions to the problems in detail. The design and implementation details should all be placed in this section. You may create a number of subsections, each focussing on one issue.

This section should be between 4 to 7 pages in length.

- 25% of paper
- Adequacy of the solution -
- Specification and design - written in python, command line interface
- Outline of implementation issues - issues with communicating over a network, client instances must be on same local device
- Description of tools used - various python libraries: Pyro4, AES, base64, hashlib, secrets
- Verification and Validation -
- Discussion of testing - Graphs from testing of security and efficiency of system: number of 1 bits vs time, log key value vs time, various curves vs time.

IV RESULTS

this section presents the results of the solutions. It should include information on experimental settings. The results should demonstrate the claimed benefits/disadvantages of the proposed solutions.

This section should be between 2 to 3 pages in length.

- 25% of paper
- Description of the evaluation method adopted - evaluated by trying to break the encryption and demonstrating that it would take an infeasible amount of time
- Clarity of results

V EVALUATION

This section should between 1 to 2 pages in length.

- 20% of paper
- Suitability of approach
- Discussion of strengths and limitations of the system - limitations with communicating over networks, works well with multiple client instances on a local machine
- Discussion of algorithms used - ECDH, ECDSA, point addition and point multiplication
- Appraisal of project organisation

VI CONCLUSIONS

This section summarises the main points of this paper. Do not replicate the abstract as the conclusion. A conclusion might elaborate on the importance of the work or suggest applications and extensions. This section should be no more than 1 page in length.

The page lengths given for each section are indicative and will vary from project to project but should not exceed the upper limit. A summary is shown in Table 2.

- 5% of paper
- Description of the main findings

Table 2: SUMMARY OF PAGE LENGTHS FOR SECTIONS

	Section	Number of Pages
I.	Introduction	2–3
II.	Related Work	2–3
III.	Solution	4–7
IV.	Results	2–3
V.	Evaluation	1-2
VI.	Conclusions	1

- Clarity of conclusions
- Discussion of further work

References

Budgen, D. (2003), *Software Design*, 2nd edn, Addison Wesley.

Euther, K. (2006), Title of paper. unpublished.

Futher, R. (2006), Title of paper 2. submitted for publication.