On the Efficiency of Isogeny Based Signatures

Submitted by

Robert W.V. Gorrie
B.ASc. Computer Science (McMaster University)

Under the guidance of
Douglas Stebila

*Submitted in partial fulfillment of
the requirements for the award of the degree of*

**Masters of Science
in
Computer Science**

Department of Computing and Software
McMaster University
Hamilton, Ontario, Canada

Fall Semester 2017

Abstract

¡Abstract here¿

Contents

List of Figures

Chapter 1

Introduction

1.1 Background and Recent Research

1.1.1 ¡any sub section here¿

1.1.2 Literature Survey

1.2 Layout of Paper

¡Sub-subsection title¿

some text[1], some more text

¡Sub-subsection title¿

even more text[1], and even more.

1.3 Motivation

[1] ¡footnote here¿

Chapter 2

Technical Background

2.1 Isogenies

2.1.1 ¡Sub-section title¿

2.1.2 ¡Sub-section title¿

some text[2], some more text

2.1.3 ¡Sub-section title¿

2.1.4 ¡Sub-section title¿

Refer figure 4.1.

2.2 SIDH

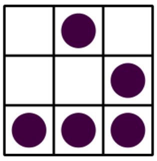

Figure 2.1: ¡Caption here¿

2.2.1 ¡Sub-section title¿

2.3 Fiat-Shamir

2.4 Isogeny Based Signatures

Chapter 3

Batching Operations for Isogenies

3.1 Batching Procedure in Detail

3.2 Implementation

3.3 Results

¡Future work here¿

Chapter 4

Compressed Signatures

4.1 Compression of Public Keys

4.1.1 ¡Sub-section title¿

4.1.2 ¡Sub-section title¿

some text[2], some more text

4.1.3 ¡Sub-section title¿

4.1.4 ¡Sub-section title¿

Refer figure 4.1.

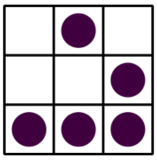

Figure 4.1: ¡Caption here¿

4.1.5 ¡Sub-section title¿

4.2 Implementation

4.3 Results

Chapter 5

Discussion & Conclusion

5.1 Results & Comparisons

5.2 Additional Opportunities for Batching

5.3 Future Work

¡Conclusion here¿

Acknowledgments

¡Acknowledgements here¿

¡Name here¿

¡Month and Year here¿
National Institute of Technology Calicut

References

[1] ¡Name of the reference here¿, `<urlhere>`

[2] ¡Name of the reference here¿, `<urlhere>`