

(CS7555-16CS72P01)
INDIAN INSTITUTE OF TECHNOLOGY KHARAGPUR
KHARAGPUR 721302

RECOMMENDATION ON MS THESIS

Name of the Student: **Anindya Ganguly**

Title of the Thesis: **A Study of Hyperelliptic-Curve Cryptography**

Please send detailed report on the thesis on separate sheet, and specify recommendation by ticking any one of the following **

SELECTED

* the thesis be accepted for award of MS degree

OR

* the thesis is acceptable subject to clarification of certain points at the time of viva-voce
(Please enclose list of the points).

OR

* the thesis is acceptable subject to modification/clarification/revision
(Please enclose your suggestions for the modification etc. desired)
After modification the thesis should not be referred back to me.

OR

* the thesis is acceptable subject to modification/clarification/revision
(Please enclose your suggestions for the modification etc. desired)
After modification the thesis should be referred back to me for final Assessment.

OR

* the thesis be rejected (please enclose your comments).

LETTER GRADE AWARDED: (Please see table below): EX

Strengths of the Thesis (of 16CS72P01):

This is an excellent thesis on a difficult subject. Chapter 2 gives a comprehensive treatment of mathematics required for the problem under consideration. Chapter 3 is on Jacobian order computation. Chapter 4 contains a detailed analysis of the cryptographic primitive that the authors construct using their hyperelliptic curve. Apart from the research contributions, this thesis will help the reader gain good exposure to the elliptic curve cryptography.

Weakness of the Thesis (of 16CS72P01):

Nil.

Questions to be asked during Thesis Defence (of 16CS72P01):

1. Is it possible to explain the connection between the efficiency of finite field operations and operation over hyperelliptic curves by using a small example?
2. Can you comment on the role of the choice of irreducible polynomials defining a finite field and the efficiency of the operation over it?

** It may be mentioned that the standard of an MS thesis at Indian Institute of Technology, Kharagpur is comparable to that of any recognised University/Institute of higher learning in any country.

DESCRIPTION OF THE 7-POINT GRADE SYSTEM

Description	Letter Grade	Grade Point Per Credit	Percentage of Numerical Marks
Excellent	Ex	10	90% and above
Very Good	A	09	80% or above but less than 90%
Good	B	08	70% or above but less than 80%
Fair	C	07	60% or above but less than 70%
Average	D	06	50% or above but less than 60%
Pass	P	05	35% or above but less than 50%
Fail	F	02	Below 35%

Report on: A Study of Hyperelliptic-Curve Cryptography
Submitted by: Anindya Ganguly

This is an excellent thesis on a difficult subject. Chapter 2 gives a comprehensive treatment of mathematics required for the problem under consideration. Chapter 3 is on Jacobian order computation. This chapter contains descriptions of several known algorithms. This is strong point of the thesis.

Chapter 4 contains a detailed analysis of the cryptographic primitive that the authors construct using their hyperelliptic curve. Apart from the research contributions, this thesis will help the reader gain good exposure to the elliptic curve cryptography.

This is a well written thesis. I recommend it for acceptance as an MS Thesis without hesitation.

(CS7555-16CS72P01)
INDIAN INSTITUTE OF TECHNOLOGY KHARAGPUR
KHARAGPUR 721302

RECOMMENDATION ON MS THESIS

Name of the Student: **Anindya Ganguly**
Title of the Thesis: **A Study of Hyperelliptic-Curve Cryptography**

Please send detailed report on the thesis on separate sheet, and specify recommendation by ticking any one of the following **

* the thesis be accepted for award of MS degree

OR

* the thesis is acceptable subject to clarification of certain points at the time of viva-voce
(Please enclose list of the points).

OR

* the thesis is acceptable subject to modification/clarification/revision
(Please enclose your suggestions for the modification etc. desired)
After modification the thesis should not be referred back to me.

OR


* the thesis is acceptable subject to modification/clarification/revision
(Please enclose your suggestions for the modification etc. desired)
After modification the thesis should be referred back to me for final Assessment.

OR

* the thesis be rejected (please enclose your comments)

LETTER GRADE AWARDED (Please see table below) A

Place Kharagpur

Signature of the Examiner: 

Date 21-03-2021

Name of the Examiner:

Strengths of the Thesis (of 16CS72P01).

The author propose a new family of hyperelliptic curves. He then proposes an algorithm for computing the order of Jacobians for subfield curves.
In Chapter 2 discusses the mathematical preliminaries of hyperelliptic curves, where the divisors, divisor classes, and the Jacobians are introduced.
Chapter 3 shows the complexities of computing the orders of Jacobians specially it shows how using point counting algorithms over large prime fields are complicated and inefficient for hyperelliptic curves compared to elliptic curves. Finally, it proposes how point counting algorithm can be used for subfield curves. Chapter 4 gives the security analyses of the proposed technique.

I find the contents of the thesis worthy of an MS work and recommend for award of MS degree.

Weakness of the Thesis (of 16CS72P01).

No weakness as such. Just a few observations:
In Section 1.4, Chapter 4 is missing. This may be corrected.
A concluding remark, even at the end of chapter 2 will help in continuation of the thesis.
In the Concluding chapter the Limitations of the proposed technique is missing.

Questions to be asked during Thesis Defence (of 16CS72P01).

- 1 What is the gain in computational complexity of using point counting algorithm over the proposed subfield hyperelliptic curves with respect to using it over hyperelliptic curves.
- 2 Explicitly mention the limitations in terms of performance of the proposed technique.

Place: Kharagpur

Signature of the Examiner

Date: 21.03.2021

Name of the Examiner

** It may be mentioned that the standard of an MS thesis at Indian Institute of Technology, Kharagpur is comparable to that of any recognised University/Institute of higher learning in any country.

DESCRIPTION OF THE 7-POINT GRADE SYSTEM

Description	Letter Grade	Grade Point Per Credit	Percentage of Numerical Marks
Excellent	Ex	10	90% and above
Very Good	A	09	80% or above but less than 90%
Good	B	08	70% or above but less than 80%
Fair	C	07	60% or above but less than 70%
Average	D	06	50% or above but less than 60%
Pass	P	05	35% or above but less than 50%
Fail	F	02	Below 35%