Report on

**Analysis of standard elliptic curves for the implementation of ECC Cipher in resource-constrained environments**

Submitted to Manipal University, Jaipur

Towards the partial fulfillment for the Award of the Degree of

**BACHELOR OF TECHNOLOGY**

In Computers Science and Engineering

2018-2022

By

Name - Jaidev Chaudhary  
Registration No- 189301036  
&  
Name - Saransh Sharma  
Registration No- 189301164



Under the guidance of

Dr. Umashankar Rawat



**Department of Computer Science and Engineering**

**School of Computing and Information Technology**

**Manipal University Jaipur**

**Jaipur, Rajasthan**

**1. Introduction:**

Nowadays, many publicly observable Internet protocols

offer cipher suites that contain elliptic curve based

cryptographic algorithms. Today, ECC is increasingly used

to implement public-key cryptography protocols, such as

digital signatures and key agreement protocols. Bitcoin,

secure shell (SSH), Transport Layer Security (TLS), and the

Austrian e-ID card is some of the application protocols

which make use of ECC in the real world [1]. Many E-

commerce applications also use elliptic curve cryptography,

due to its security features.

There are many international standards available for the

selection of elliptic curves. The choice of the curve is

dependent on the security requirement and the required

efficiency of the curve in terms of computation speed. In [2]

the first release of cryptographic standards specifying elliptic

curves for use in practice is given for the different key sizes.

The standards that recommend curves for various security

levels are defined over either prime or binary extension fields.

Currently, across the internet, the elliptic curves deployed are

mostly defined over prime fields [3]. In this paper, such

elliptic curves defined over prime fields are the subject of

analysis

Nowadays, many publicly observable Internet protocols

offer cipher suites that contain elliptic curve based

cryptographic algorithms. Today, ECC is increasingly used

to implement public-key cryptography protocols, such as

digital signatures and key agreement protocols. Bitcoin,

secure shell (SSH), Transport Layer Security (TLS), and the

Austrian e-ID card are some of the application protocols

which make use of ECC in the real world [1]. Many E-

commerce applications also use elliptic curve cryptography,

due to its security features.

There are many international standards available for the

selection of elliptic curves. The choice of the curve is

dependent on the security requirement and the required

efficiency of the curve in terms of computation speed. In [2]

the first release of cryptographic standards specifying elliptic

curves for use in practice is given for the different key sizes.

The standards that recommend curves for various security

levels are defined over either prime or binary extension fields.

Currently, across the internet, the elliptic curves deployed are

mostly defined over prime fields [3]. In this paper, such

elliptic curves defined over prime fields are the subject of

analysis

Nowadays, many publicly observable Internet protocols offer cipher suites that contain elliptic curve based cryptographic algorithms. Today, ECC is increasingly used to implement public-key cryptography protocols, such as digital signatures and key agreement protocols. Bitcoin, secure shell (SSH), Transport Layer Security (TLS), and the Austrian e-ID card are some of the application protocols which make use of ECC in the real world. Many E-commerce applications also use elliptic curve cryptography, due to its security features. There are many international standards available for the selection of elliptic curves. The choice of the curve is dependent on the security requirement and the required efficiency of the curve in terms of computation speed. In the first release of cryptographic standards specifying elliptic curves for use in practice is given for the different key sizes. The standards that recommend curves for various security levels are defined over either prime or binary extension fields. Currently, across the internet, the elliptic curves deployed are mostly defined over prime fields. In this paper, such elliptic curves defined over prime fields are the subject of analysis.

n elliptic curve systems, a sub exponential-time algorithm

is absent compared to systems based on the multiplicative

group of a finite field, so it is possible to maintain the same

level of security with an elliptic curve group that is smaller in

size [4]. The advantages of using smaller elliptic groups are

smaller key sizes, bandwidth savings, and faster

implementations which are useful for safety implementation

in resource-constrained applications. So, while implementing

ECC cryptosystem in the field of E-commerce it is important

to find a suitable curve that can work efficiently with

resource-constrained devices such as smart cards, personal

computer (PC) cards, and wireless devices, etc.

In elliptic curve systems, a sub exponential-time algorithm is absent compared to systems based on the multiplicative group of a finite field, so it is possible to maintain the same level of security with an elliptic curve group that is smaller in size. The advantages of using smaller elliptic groups are smaller key sizes, bandwidth savings, and faster implementations which are useful for safety implementation in resource-constrained applications. So, while implementing ECC cryptosystem in the field of E-commerce it is important to find a suitable curve that can work efficiently with resource-constrained devices such as smart cards, personal computer (PC) cards, and wireless devices, etc.

**1.1 Motivation:**

In the current digital world and public-key cryptography segment, the majority of deployments are fulfilled by the RSA based cryptosystems. Cryptosystems based on elliptic curves emerge as an alternative to the RSA cryptosystems. The security of the RSA cryptosystem is based on the integer factorization problem (IFP) whereas the security of ECC is based on the elliptic curve discrete logarithm problem (ECDLP). The significant attraction towards ECC is that the best-known algorithm for solving the ECDLP takes full exponential time while for solving IFP of RSA takes sub exponential time. ECC takes less memory than RSA and is better than RSA, especially on memory-constrained devices. Moreover, ECC provides same level of security as the RSA but with reduced key size.

**2. Literature:**

**Problem Statement**- Implementation of the Elliptic Curve Diffie-Hellman Algorithm and Elliptic Curve Digital Signature Algorithm

**Approach**- There are multiple standard Elliptical Curves that can be used with the ECC scheme

Each standard of curve strives to maintain the difficulty of the Elliptic Curve Discrete Logarithm Problem (ECDLP).

The main idea is to select a curve which is safe against the known attacks on ECDLP

The analysis is carried out using SageMath, which is a free open-source mathematics software system licensed under the GPL, using Python 3.

**3. Methodology and Framework:**

The analysis will be performed by considering each curve for the implementation of the Elliptic Curve Diffie-Hellman (ECDH) algorithm and the Elliptic Curve Digital Signature Algorithm (ECDSA). The analysis is carried out using SageMath, which is a free open-source mathematics software system licensed under the GPL, using Python 3.

* SOFTWARE
  + Windows 10
  + Python 3.x
* HARDWARE
  + HDD/SSD with sufficient storage capacity
  + Core i5 Processor
  + At least 4GB RAM

**4. Work Done:**

* Understood the mathematical foundations reqd.
* Understood the algorithmic concepts reqd.
* Created a web-app that plots the curves that are pre-defined
* Basic interface ready
* Back-end majorly completed
* Currently gives O/P for predefined parameters

The above bulletins have been implemented using following techniques:

Frontend: Html, CSS

Backend: python3, Flask, SQLAlchemy

**5. Future Plan:**

* We plan to learn sage math and implement in our code.
* Improve the UI of the app.
* Take user input so that the user can plot his/her curve.
* Fixing bugs on the backend.