Fast Invalid Curve Attack using twists

Pierre Chrétien

February 2025

Abstract

Exploiting Invalid Curve Attack is a recurrent problem in CTF. We present the common structure of the attack and give some insight to speed up the attack. This paper has primarily an expository role.

1 Introduction

This paper has primarily an expository role.

2 Background Material

2.1 Twists of Elliptic Curves

2.2 Discrete Logarithm Problem

3 Invalid Curve Attack

3.1 General Setting

test [1]

3.2 Exploiting Ladders and twists

References

[1] Donald E. Knuth. *The TEX Book*. Addison-Wesley Professional, 2024.