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.