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

The so called *Invalid curve attack* is a real threat for cryptographic protocols based on elliptic curves. The attack has first been presented in citeBMM00 and the use of twists described in [3]. OpenPGP.js prior to 4.2.0 was found to be vulnerable[1]. Bluetooth has been proven to be vulnerable to a "Fixed Coordinate" variant [2]. The SafeCurves website and the associated paper [1] point out as

> An ECC implementor can stop an invalid-curve attack by checking whether the input point Q satisfies the correct curve equation; [...] But this creates a conflict between simplicity and security. An implementation that does not include this check is simpler and more likely to be produced, and will pass typical functionality tests.

It is also at heart of many Capture The Flag and cryptographic challenges on dedicated platforms.
The rest of the paper is organized as follows. Section 2 recalls the basics mathematical concepts used in the sequel, we recall basics facts about discrete logarithm problem (DLP) and twists of elliptic curves. Section 3 presents the general setting of the attack and ways to exploit poor implementation and weak curves.

This paper has primarily an expository role.

2 Background Material

Notations : We will denote by $\mathbb{F}_q$ the finite field with $q = p^n$ elements where $p \geq 5$ and $n \in \mathbb{N} - \{0\}$. We will denote by $E/\mathbb{F}_q$ an elliptic curve defined over $\mathbb{F}_q$. The reader is assumed to be familiar with basic theory of elliptic curves.

The characteristic p being different from 2 and 3, every elliptic curve $E/\mathbb{F}_q$ may be written as

$$E : y^2 = x^3 + ax + b, \quad a, b \in \mathbb{F}_q.$$

This is a so called *short Weierstrass form* of E.

Remarks :

- The characteristic p being greater than 5 is not a restriction in our context since p will usually be a large prime number.
- The short Weierstrass form is not unique.

```
k = GF(11**2)
u = k(2)
E = EllipticCurve(k,[1,1])
E_ = EllipticCurve(k,[u**(-4),u**(-6)])
E.is_isomorphic(E_)
E.isomorphism_to(E_)
```

2.1 Twists of Elliptic Curves

- Automorphismes d'une courbe elliptique.
- Cas particulier de l'équation short p ¿ 3.
- Description des twists, expliquer pourquoi j différent de 0 et 1728 n'est pas un problème, donc seulement le twist quadratique à considérer en général, écriture des morphismes
- exemples

[1] https://www.cve.org/CVERecord?id=CVE-2019-9155

2.2 Discrete Logarithm Problem

Definition 1. Let G be a group in multiplicative notation. The **Discrete Logarithm Problem** (DLP) is : given $g, h \in G$ find $a \in \mathbb{Z}$ such that $h = g^a$.

Remarks :

1. Let $\mathbb{L}/\mathbb{F}_q$ be a field extension and $E/\mathbb{F}_q$ an elliptic curve. The group of $\mathbb{L}$-rationnal points of E denoted $E(\mathbb{L})$ (that is the solutions $(x, y) \in \mathbb{L}^2$ of the Weierstrass equation defining E) is usually written with an additive law. So the DLP for elliptic curves may be rephrased : given $P, G \in E(\mathbb{L})$ find $a \in \mathbb{Z}$ such that $P = aG$.

Solving the DLP

- Polhig Helman, BSGS, Rho.
- Sage Discretelog vs Q.log(P)

3 Invalid Curve Attack

3.1 General Setting

Position du problème : les algo de multiplication d*P n'utilisent que le coeff a de E, on peut passer (x,y) n'étant pas sur E.

- DLP peut etre trop dur sur E à cause de d'un ordre pas assez smooth.
- Si on peut faire calculer k*T pour T sur une autre courbe E' on peut trouver T modulo les premiers de l'ordre de E'.
- si le twist a un ordre avec d'autres facteurs premier que E alors on connait k modulo de nouveaux premiers.
- cela peut suffire à retrouver k (CRT)

3.2 Exploiting Ladders and twists

- L'importance des ladders cf Safe Curves
- L'importance des multiplications où on ne passe que le x.

References

[1] Daniel J. Bernstein and Tanja Lange. Safe curves for elliptic-curve cryptography. Cryptology ePrint Archive, Paper 2024/1265, 2024.

[2] Eli Biham and Lior Neumann. Breaking the bluetooth pairing – the fixed coordinate invalid curve attack. Cryptology ePrint Archive, Paper 2019/1043, 2019.

[3] P.-A. Fouque, R. Lercier, D. Réal, and F. Valette. Fault Attack on Elliptic Curve with Montgomery Ladder Implementation. In *FDTC '08. 5th Workshop on Fault Diagnosis and Tolerance in Cryptography*, pages 92–98. IEEE-CS Press, August 2008.