Smart's Attack Over Non Prime Field

Pierre Chrétien

June 2025

1 Introduction

We present Smart's attack over non prime field $\mathbb{F}_q$. We construct an anomalous curve over a non prime finite field and implement Smart's attack in SageMath.

2 Smart's attack

[1]

References

[1] Franck Leprévost, Jean Monnerat, Sébastien Varrette, and Serge Vaudenay. Generating anomalous elliptic curves. *Information Processing Letters*, 93(5):225–230, 2005.