Cryptography from the Tropical Hessian Pencil

Jean-Marie Chauvet

MassiveRand, Inc.

Abstract

The Hessian Pencil displays rich algebraic and geometric structures which recently new applications to computational problems in elliptic curves and in theoretical physics. Most of these properties transfer naturally to the *Tropical Hessian Pencil*, the result of replacing the field underlying the Hessian Pencil by the tropical semiring $(\mathbb{R} \cup \{-\infty\}, max, +)$. The use of Hessian curves in cryptography is well documented, and unified complete formulas for addition on generalized Hessian curves over finite fields are well-known. This paper presents addition and doubling formulas for the Tropical Hessian Pencil which are also extremely fast as big integer multiplications are not used.

Keywords:
2000 MSC: 14G50 11T71

1. Introduction

2. The Tropical Hessian Pencil

3. Doubling and Addition

4. Conclusions

[1]