1026-11-153

Tanja Lange*, Codingtheory and Cryptology; Dept Math & CS, Technische Universiteit Eindhoven, PO Box 513, 5600 MB Eindhoven, Netherlands. *Unified addition formulae for elliptic curves.*

Several coordinate systems and addition formulas were suggested to implement elliptic curve scalar multiplication. If the system is implemented on a smart card additional care needs to be taken not to leak the secret through side channels such as time or power consumption. Countermeasures often lead to less efficient systems and/or can be applied to a smaller class of curves.

In this talk we treat elliptic curves over finite fields of characteristic larger than 3. After reviewing the existing coordinate systems we present new formulae and compare the costs. (Received February 25, 2007)