1026-11-101 **Edlyn E Teske*** (eteske@uwaterloo.ca), University of Waterloo, Dept. of Combinatorics and Optimization, Waterloo, Ontario N2L3G1, Canada. *Pairing-friendly elliptic curves for cryptography.*

Elliptic curves with small embedding degree and large prime-order subgroup are key ingredients for implementing pairing-based cryptographic systems. Such "pairing-friendly" curves are rare and thus require specific constructions. In this talk, we discuss a few aspects of these constructions. (Received February 19, 2007)