

998-94-23

Edlyn E Teske* (eteske@uwaterloo.ca), Department of Combinatorics and Optimization,
Waterloo, Ontario N2L3G1, Canada. *Key escrow with elliptic curves.*

We present an elliptic curve trapdoor system which is of interest in key escrow applications. In this system, a pair (E_s, E_{pb}) of elliptic curves over $\mathbb{F}_{2^{161}}$ is constructed with the following properties: (i) the Gaudry-Hess-Smart Weil descent attack reduces the elliptic curve discrete logarithm problem (ECDLP) in $E_s(\mathbb{F}_{2^{161}})$ to a hyperelliptic curve DLP in the Jacobian of a curve of genus 7 or 8, which is computationally feasible, but by far not trivial; (ii) E_{pb} is isogenous to E_s ; (iii) the best attack on the ECDLP in $E_{pb}(\mathbb{F}_{2^{161}})$ is the parallelized Pollard rho method.

The curve E_{pb} is used just as usual in elliptic curve cryptosystems. The curve E_s is submitted to a trusted authority for the purpose of key escrow. The crucial difference from other key escrow scenarios is that the trusted authority has to invest a considerable amount of computation to compromise a user's private key, which makes applications such as widespread wire-tapping impossible. (Received December 25, 2003)