Cryptology ePrint Archive: Report 2011/580

On a new generalization of Huff curves

Abdoul Aziz Ciss and Djiby Sow

Abstract: Recently two kinds of Huff curves were introduced as elliptic curves models and their arithmetic was studied. It was also shown that they are suitable for cryptographic use such as Montgomery curves or Koblitz curves (in Weierstrass form) and Edwards curves.

In this work, we introduce the new generalized Huff curves $ax(y^{2} -c) = by(x^{2}-d)$ with $abcd(a^{2}c-b^{2}d)\neq 0$, which contains the generalized Huff's model $ax(y^{2}- d) = by(x^{2}-d)$ with $abd(a^{2}-b^{2})\neq 0$ of Joye-Tibouchi-Vergnaud and the generalized Huff curves $x(ay^{2} -1) =y(bx^{2}-1)$ with $ab(a-b)\neq 0$ of Wu-Feng as a special case.

The addition law in projective coordinates is as fast as in the previous particular cases. More generally all good properties of the previous particular Huff curves, including completeness and independence of two of the four curve parameters, extend to the new generalized Huff curves. We verified that the method of Joye-Tibouchi-Vergnaud for computing of pairings can be generalized over the new curve.

Category / Keywords: public-key cryptography / Huff curves, pairing, divisor, Jacobian, Miller algorithm, elliptic curve models, Edwards curves, Koblitz Curves

Date: received 26 Oct 2011

Contact author: abdoul ciss at ucad edu sn