

## Re: Elliptic curves over finite fields of characteristic 3

**Source:** <http://www.derkeiler.com/Newsgroups/sci.crypt/2005-07/1588.html>

---

**From:** Colin Andrew Percival ([cperciva\\_at\\_sfu.ca](mailto:cperciva_at_sfu.ca))

**Date:** 07/28/05

Date: Wed, 27 Jul 2005 22:31:58 +0000 (UTC)

Peter Schwabe <[peter\\_schwabe@web.de](mailto:peter_schwabe@web.de)> wrote:

- > *does anyone know, where to find detailed information about how to*
- > *implement elliptic curves over finite fields of characteristic 3. Detailed*
- > *means: Which projective coordinates should be used, how does the group law*
- > *look like etc.*

As Paul said, I don't think anyone has looked at ECC over  $GF(3^k)$  --- probably because if you're going to use a prime power then  $GF(2^k)$  is rather easier to implement.

Colin Percival