

## Re: New ECC Paper (fast GF(p) point mul)

---

*Source:* <http://www.derkeiler.com/Newsgroups/sci.crypt/2006-06/msg01431.html>

---

- *From:* "Tom St Denis" <[tomstdenis@xxxxxxxxxx](mailto:tomstdenis@xxxxxxxxxx)>
  - *Date:* 29 Jun 2006 09:21:59 -0700
- 

Tom St Denis wrote:

Definitely nice to see advances in the GF(p) world. Unfortunately it doesn't [??] apply to NIST curves as the curve he uses is of the form

Scratch that. The author sent me more info ... hehehe.

Turns out you can map from the NIST style to Montgomery style if two things are true

1. There is at least one root to the equation  $x^3 - 3x + b$  in  $F_p$  [call it  $\alpha$ ]
2. The root plugged into  $3\alpha^2 + a$  is a QR in  $F_p$

Now I know how to find roots over  $Z$  and  $R$  [Newton comes in handy] but how do you do it over  $F_p$ ? Factoring it gives us

$$x(x^2 - 3) = -b$$

Any refreshers? hehehe

Tom

.