

Re: ECC Result Verification

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2004-11/0048.html>

From: Tom St Denis (tomstdenis_at_gmail.com)

Date: 11/02/04

Date: Mon, 01 Nov 2004 21:51:40 -0500

flip wrote:

> *Hi All,*

>

> *can someone please verify these results?*

>

> *E: $y^2 = x^3 + 1x + 1 \pmod{23}$*

>

> *The set of points that satisfy E are given by:*

While not "general purpose" LibTomCrypt has ECC "mulmod", "addmod" and "dblmod" functions you can use. Just plug in your own curve into the system and add some hackage [e.g. rip the ECC code from LTC].

Tom