

Re: 16-bit ECC on prime fields

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2005-05/1182.html>

From: Bryan Olson (*fakeaddress_at_nowhere.org*)

Date: 05/29/05

Date: Sun, 29 May 2005 10:09:26 GMT

DeepHalo wrote:

- > *Implement an 16-bit ECC cryptosystem on prime fields.*
- >
- > *I have a term-project and I want to implement this using Java. In order*
- > *to write code I have to understand its theory but I couldn't find any*
- > *RFC style explanation. Can you please help?*

Try the "SEC 1" doc, available at:

http://www.secg.org/?action=secg.docs_secg

--

--Bryan

[Full disclosure: I'm a former Certicom employee and still own stock.]