

Re: ECC template library

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2006-04/msg00501.html>

- *From:* "Ben Livengood" <ben.livengood@xxxxxxxx>
 - *Date:* 17 Apr 2006 14:37:35 -0700
-

tomstdenis@xxxxxxxx wrote:

gregofiesh@xxxxxxxx wrote:

The Hanalei Company is proud to present an Elliptic Curve Cryptography library written in C++ for free download to the general public.

<http://www.hanaleicompany.com/main.aspx?pageid=security>

Additionally, The Hanalei Company presents an essay on the current US law regarding exports of encryption software that is freely available.

<http://www.hanaleicompany.com/main.aspx?pageid=security.thelaw>

It actually looks like nice C++.

... you're using affine point algorithms though. And that's just a sin.

:~)

Still for once I can say "Kudos on the simple yet functional code" about something in C++. And as my many "fans" in this group knows that doesn't happen often.

Tom

Speaking of ECC over $GF(2^n)$, any chance you can get AMD to provide a bit flag or prefix for turning off the carry propagation circuitry in the MUL and DIV instructions? My guess is that $GF(2^n)$ is quite a bit faster than $GF(p)$ when done in hardware, not to mention unencumbered by patents...