

Re: Montgomery Reduction for GF(2)[x] ?

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-05/2411.html>

From: Colin Andrew Percival (*cperciva_at_sfu.ca*)

Date: 05/31/03

Date: 31 May 2003 01:51:40 GMT

Tom St Denis <tomstdenis@iahu.ca> wrote:

- > 1. for t from 1 to k do
- > 2. if the lsb of $p(x)$ is one then
- > 3. $p(x) = p(x) + v(x)$
- > 4. $p(x) = p(x) / x$

How is that better than:

1. for t from k to 1 do
2. if the msb of $p(x)$ is one then
3. $p(x) = p(x) + v(x) * x^{(t-1)}$

Colin Percival