

Re: CRC reverse engineering

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2007-05/msg00029.html>

- *From:* daw@xxxxxxxxxxxxxxxxxxxxxxxxxxxx (David Wagner)
 - *Date:* Wed, 2 May 2007 17:16:06 +0000 (UTC)
-

mvrpfswe wrote:

There must be a more elegant way of figuring this out rather than a brute force,

One conceptually simple thing you can try is linear algebra.

Assume that each bit of the presumed-CRC-output can be written an (unknown) linear function data bits; write down a system of linear equations; and then use linear algebra (Gaussian elimination) to solve the system of linear equations and find the linear function (if there is one) that describes how to compute that output bit as a function of the input bits.

.