

New Paper

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2004-01/2098.html>

From: Tom St Denis (tomstdenis_at_iahu.ca)

Date: 01/31/04

Date: Sat, 31 Jan 2004 01:25:21 GMT

Title: The CSQUARE Transform

Abstract: In this paper we show how to combine the design concepts of the SQUARE and CS block ciphers to produce a pseudo-random permutation CSQUARE suitable for use in block cipher and hash design with a very high multi-round trail weight. The new design inherits the hardware efficiency of the SQUARE linear transform pattern as well as the efficiency of the fast pseudo-Hadamard transform over a finite field. We demonstrate the DMWT hash function which makes use of our new results.

URL: <http://libtomcrypt.org/dmwt.pdf>

Note: It's a draft and work in progress. I appreciate all comments, critiques, etc...

Thanks,
Tom