

Re: Pseudorandom Hashing

Source: <http://sci.tech-archive.net/Archive/sci.electronics.design/2004-09/5994.html>

From: Tim Wescott (tim_at_wescottnospamdesign.com)

Date: 09/23/04

Date: Thu, 23 Sep 2004 15:26:18 -0700

Jim Thompson wrote:

> *On Thu, 23 Sep 2004 14:40:28 -0700, Tim Wescott*

> *<tim@wescottnospamdesign.com> wrote:*

>

>

>>*I am having trouble coming up with the right keywords to do a web*

>>*search, so help me out here:*

>>

>>*There is a technique where, to significantly reduce the probability of*

>>*getting a long string of zeros, a message is run through a CRC*

>>*generator, and the output bits are taken off. The transmitted message*

>>*is thoroughly hashed, yet it is a simple matter of a shift register and*

>>*some XOR gates to decode the message on the other end.*

>>

>>*I thought I knew how to do this, yet in trying to actually make it work*

>>*I find that over half of my brain cells appear to be attending a*

>>*management seminar.*

>

>

> *"attending a management seminar".... I like that ;-)*

>

>

>>*So, know where I can find out how to do this right? "pseudorandom" and*

>>*"hash" get me tons of cryptography, but not what I'm looking for.*

>>

>>*Thanks.*

>

>

> *My mind is slow today also, but isn't it the same in AND out...*

>

> *XMIT: 2-bit SR, XOR the two SR Q's together to get output*

>

> *RECV: SAME*

>

> *...Jim Thompson*

IIRC you XOR and feed back on the input, and just XOR on the output.

But IIRC then I wouldn't need to ask.

sci.electronics.design: Re: Pseudorandom Hashing

--

Tim Wescott

Wescott Design Services

<http://www.wescottdesign.com>