

Re: C-equivalence aware hash function

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2005-11/1053.html>

From: Jean-Luc Cooke (jlcooke_at_engsoc.org)

Date: 11/29/05

Date: 29 Nov 2005 16:29:30 GMT

Polarity preservation is the easy step as I demonstrated earlier.

The row and column sorting wouldn't be a problem if you only had to do one of them, as Rose showed they aren't commutative. I'm still not sure how to solve FG's problem.

JLC

Mike Amling <nospam@icic.gov.ir> wrote:

> *To canonicalize, you also have to disambiguate the polarity reversal*
> *criteria for matrices with an even number of rows or an even number of*
> *columns. Both of the matrices*

> $1 \ -1$

> $1 \ -1$

> *and*

> $1 \ -1$

> $-1 \ 1$

> *are canonical under Dr. Wagner's specification in that they have sorted*
> *columns and rows, and do not invite polarity inversion. But they are*
> *C-equivalent.*

> --Mike Amling

--