

Re: [Khufu] Pre-Computing the S-Boxes and obtaining aux. keys

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2004-11/0016.html>

From: Matt (matt_crypto_at_yahoo.co.uk)

Date: 11/01/04

Date: 1 Nov 2004 04:52:14 -0800

Nikola Skoric <nick-news@net4u.hr> wrote:

>
> *So, the point is this guy was in the same position as I am. He has the*
> *algorithm, but he did some quick hacks to get around the fact he hasn't*
> *any clue how to generate auxiliary keys and S-Boxes. The algorithm*
> *itself is well explained in the Merkle's paper and to be honest I didn't*
> *even bother to understand the C code in that file except to ensure that*
> *the function initialize() (which builds the aux key material and the*
> *boxes) is just an ugly hack.*
>
> *Now, I might be missing something obvious... in that case, I BEG you to*
> *point me in the right direction because I'm facing a solid brick wall*
> *here...*

Try the following address:

<http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PALL&p=1&u=/netahtml/srchnum.htm&>

Then click on "Images", and browse the document (it's a series of TIFF images, you might need special graphics software to view them). Eventually you get to C source code, including some which generates the S-box from the RAND numbers. And, moreover, some test vectors, which are quite useful for testing your own implementation. Hope that helps somewhat. If you manage to get a working Khufu implementation, I'd encourage you to release the source code on the Internet,

— Matt