

Re: Conjectured pseudorandom functions

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2005-04/2113.html>

From: David Wagner (daw_at_taverner.cs.berkeley.edu)

Date: 04/30/05

Date: Sat, 30 Apr 2005 03:44:08 +0000 (UTC)

>What are the conjectured pseudorandom functions with arbitrary input
>length commonly used in practice?

SHA1-HMAC is a good example. AES-OMAC is another.

>Is it necessary to choose the key of
>a pseudorandom function uniformly from the key space in order to ensure
>its randomness?

For most of these PRFs, yes.

>Could we just feed the output of the pseudorandom
>function on an input x as the key to another pseudorandom function?

Assuming you mean $F(F(k,x), y)$, the answer is basically yes,
depending on what you want to do with it and what you want to
achieve with this construction. Do you want to elaborate?