

Re: Knapsack/Subset–Sum based cryptoschemes

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2006-08/msg01664.html>

- *From:* "Tom St Denis" <tomstdenis@xxxxxxxxx>
 - *Date:* 30 Aug 2006 07:40:29 -0700
-

Eduard Toews wrote:

Hi,

I am writing my diploma thesis on knapsack based cryptoschemes. Does anybody know if up-to-date there are Knapsack/Subset–Sum based cryptoschemes being subject of current research? If the answer is yes, which are the most important?

Thanks in advance, any help would be appreciated

I suppose actually looking would be too much to ask?

There are no crypto standards that I know that are knapsack based. Primarily because they mostly all been broken and are not as clean cut as say RSA or ECC.

I don't think all of them are broken, at least not to the point of making a solution trivial. But you'd be hardpressed to find one with comparable security as say ECC P-256 with the same level of efficiency.

Tom

.