

Re: Public Key, Set-(bi)partition

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2004-04/1923.html>

From: Peter Fairbrother (zenadsl6186_at_zen.co.uk)

Date: 04/24/04

Date: Sat, 24 Apr 2004 03:19:31 +0100

Kiuhnm wrote:

[snipped, I'm having trouble with the notation]

Didn't Diffie try that a long time ago, in his (heroic) search for a working PK system?

Was it was mentioned in the original SciAm RSA article, or something around then? I'm a bit hazy on the details, but wasn't it broken like knapsacks?

Could be completely wrong here.

--

Peter Fairbrother