

Re: portable countermeasures against AES timing attacks

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2006-07/msg00610.html>

- *From:* "TC" <gg.20.keen4some@xxxxxxxxxxxxxxxxx>
 - *Date:* 17 Jul 2006 08:20:51 -0700
-

Wei Dai wrote:

c) How to detect the cache line size?

Can't you do that via the CPUID op?

HTH,
TC (MVP MSAccess)
<http://tc2.atspace.com>
(Atspace currently unreliable. Please be patient or try again later.)

.