

## Re: SHA-512 and 128-bit integers

**Source:** <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-04/1695.html>

---

**From:** Tom St Denis ([tomstdenis\\_at\\_yahoo.com](mailto:tomstdenis_at_yahoo.com))

**Date:** 04/29/03

Date: 29 Apr 2003 14:23:33 -0700

Shill <devnull@example.com> wrote in message news:<b8mekm\$u01\$1@biggoron.nerim.net>...

> > *SHA doesn't require 128-bit data types.*

>

> *For the love of christ, don't be so peremptory.*

>

> *In SHA-384 and SHA-512, the message length in bits is a 128-bit integer.*

Yeah, whoa. Seems I did know about that [judging by the code] but its been so darn long.

I think by the LTC code base my intentions were quite clear. That people are not likely to hash  $2^{61}$  bytes of data and using two 64-bit counters for the length would waste time.

Sorry for flying off the handle there. Just kinda tired of people poking erroneous bugs at me its a shock when there are real concerns :-)

Tom