

## Re: LibTomMath vs MIRACL

**Source:** <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-07/2154.html>

---

**From:** Phil Carmody (*thefatphil\_demunge\_at\_yahoo.co.uk*)

**Date:** 07/30/03

Date: Wed, 30 Jul 2003 23:09:34 +0300

On Wed, 30 Jul 2003 14:54:15 +0000, Peter Gutmann wrote:

> *Paul Rubin* <[http://phr.cx@NOSPAM.invalid](mailto:phr.cx@NOSPAM.invalid)> writes:

>

>> *You might also take a look at GMP, which is under the Gnu LGPL, and*

>> *(like MIRACL) includes fast assembly code. There is also the bn*

>> *library which is part of OpenSSL. I believe bn is generally pretty*

>> *fast, but not quite as fast as GMP or MIRACL.*

>

> *The advantage of the OpenSSL bignum code is that it's targeted specifically at*

> *doing crypto, while GMP is a general-purpose numeric package. If your goal is*

> *just to implement the usual suspects { RSA, DH, DSA/Elgamal }, you need to do*

> *quite a bit more work with GMP than with OpenSSL bignum.*

The Lenstra ('maintained' by Paul Leyland now) LIP package has a few things that are aimed at PK crypto apps too. e.g. that thing where you do more than one expmod at a time (I forget what it's called, it's in HAC).

Phil