

## Re: Problem with Montgomery product

**Source:** <http://www.derkeiler.com/Newsgroups/sci.crypt/2004-05/5512.html>

---

**From:** Giox (5218invalid\_at\_mynewsgate.net)

**Date:** 05/31/04

Date: Mon, 31 May 2004 14:54:37 GMT

Tom St Denis <tomstdenis@iahu.ca> ha scritto:

> *Giovanni Parodi wrote:*

> > *Hello everybody, I am an italian student and I have a problem with the*

> > *MonPro algorithm.*

> > *I read the paper "Analyzing and Comparing Montgomery Multiplication*

> > *Algorithms" because it's considered the better paper about this*

> > *argument freely available on the web (also in this NG it's often*

> > *referenced).*

> > *In this paper I found that it's possible to use the least significant*

> > *word of  $n'$  (indicated as  $n'0$ ), instead of  $n'$ . I don't understand why*

> > *it's possibile to do that. I tried to read the paper "A cryptographic*

> > *library for the Motorola DSP56000" (in which this trick has been*

> > *proposed), but I didn't understand the short explication given about*

> > *this argument.*

> > *I will appreciate your help. I think that the explanation is not very*

> > *difficult (because I didn't find a paper with an explicit explanation*

> > *of this topic), but I wasn't able to find it.*

> > *If possible can you give also a little example? Thanks a lot*

>

> *I have an implementation and explanation of how Montgomery reduction*

> *works in my LTM package [tommath.pdf in the archive]. It should help*

> *explain how the basic algorithm works from which you can figure out*

> *MontPro rather easily.*

>

> *Tom*

>

Hi Tom, thanks, I already read your document (before I send this post)

and in effect it's very clear, but I have problem understanding the use

of  $n'0$  instead of  $n'$ .

I will read your "book" another time, hoping this will help me, also if I

think I will need some more help :-(

However thanks a lot

--

La mia mail è  
giovanni.parodi79RIMUOVISPAM@lycos.it

Inviato da www.mynewsgate.net