

# Factoring paper is wrong

**Source:** <http://sci.tech-archive.net/Archive/sci.math/2004-06/2708.html>

---

**From:** James Harris ([jstevh\\_at\\_msn.com](mailto:jstevh_at_msn.com))

**Date:** 06/13/04

Date: 13 Jun 2004 16:40:22 -0700

My apologies but the paper that I thought solved the factoring problem had a dumb mistake in it, as in a key place while I properly had  $h_1$   $h_2 = T^4$ , in my derivation I was actually using  $h_1 h_2 = T$ , which is how I got what looked to me like a spectacular result.

The error is non-fixable in terms of that approach.

The factoring method itself does work, but so far I haven't gotten it to work well for decent bitlengths as so far at best it works for bitlengths of 40 and under, so it's useless at this point for even approaching RSA.

The problem is determining  $s$ , so at this point, my approach of using surrogate factoring is just a curiosity.

James Harris