

## Re: Blowfish Sign Extension implementation risk

**Source:** <http://www.derkeiler.com/Newsgroups/sci.crypt/2004-04/2638.html>

---

**From:** Joe Peschel (jpeschel\_at\_no.spam.org)

**Date:** 04/29/04

Date: Thu, 29 Apr 2004 11:14:34 -0000

Tom St Denis <tom@seurescience.net> wrote in  
news:1d4kc.316703\$2oI1.158163@twister01.bloor.is.net.cable.rogers.com:

> *William Wallace wrote:*

>> *Tom St Denis <tom@seurescience.net> wrote in message*

>> *news:<IEGjc.303741\$2oI1.167578@twister01.bloor.is.net.cable.rogers.com*

>> *>...*

>>

>>> *So far you don't have a track record here or anywhere else for all I*

>>> *know [and think about it, the rest of the group knows as much about*

>>> *you as I do].*

>>

>>

>> *The idea I brought up stands on its own, as all ideas do. I don't*

>> *even claim to have invented the idea (designing an algorithm robust*

>> *to implementation errors). If others on sci.crypt only wish to*

>> *consider ideas from people they have heard of, that is there*

>> *business. But I have the feeling that not everybody on sci.crypt*

>> *thinks like you.*

>

> *The concept of a "robust" design is not new. The Twofish design for*

> *example is very thorough. Similarly other algorithms such as RC5 and*

> *RC6 are very elegantly described and trivial to get right.*

>

> *This is why I don't get why you think your idea is new or so important*

> *such that people should change the Blowfish specification to bend to*

> *your whim. Using XOR is not a good idea. It's not what was intended.*

> *Case closed.*

>

>>> *So you come here, proclaim a non-fix to a problem as "the only way*

>>> *to solve the problem" and then get all hostile when people tell*

>>> *you otherwise.*

>>

>>

>> *Good lord. Now why did you put quotes there? I didn't write that,*

>> *or anything like that. You challenge my credibility (when I am not*

>> *asking you or anybody to believe anything--this all started with a*

>> *thought for discussion)--then you lie by putting quotes around that*

>> *sentence.*

>

> *I didn't say you said that. I put that in quotes to capture the*

> *essence of the thread.*

No. When you put that phrase within quotation marks it looks as if you are quoting William, especially in the way you introduce the quoted material.

J

--

---

When will Bush come to his senses?

Joe Peschel

D.O.E. SysWorks

<http://members.aol.com/jpeschel/index.htm>

---