

Re: BSD license compatible hash algorithm?

Re: BSD license compatible hash algorithm?

Source: <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/hackers/2007-12/msg00226.html>

- *From:* "Aryeh M. Friedman" <aryeh.friedman@xxxxxxxxx>
 - *Date:* Fri, 28 Dec 2007 08:12:49 -0500
-

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

Ivan Voras wrote:

On 28/12/2007, Aryeh M. Friedman <aryeh.friedman@xxxxxxxxx> wrote:

Matter of fact this weakness is the main avenue of attack on cryptographic hashes see <http://eprint.iacr.org/2004/199.pdf> A slightly off topic side note NIST is having a contest to attempt to mitigate these issues in "SHA-3" see: <http://csrc.nist.gov/groups/ST/hash/sha-3/index.html>. Currently there only 4 teams that have expressed interest in entering perhaps this will get more interest.

All of this is true but it's not very useful for hash tables (crypto-strength hash functions are generally too slow for the purpose) :)

Depends on the size of the table... I work with a algothem that regularly has tables between 2^{32} and 2^{64} buckets (even though the we use a slightly different terminology)

Aryeh M. Friedman

FloSoft Systems

<http://www.flosoft-systems.com>

Developer, not business, friendly

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v2.0.4 (FreeBSD)

Comment: Using GnuPG with Mozilla - <http://enigmail.mozdev.org>

iD8DBQFHdPZRzIOMjAek4JIRAnB+AJ0Z838CziWAYdKURNpTM6/XMMbYvgCfSpQI
QDhOMxfzc+Y9vd+KKwphezs=
=g+cW

-----END PGP SIGNATURE-----

Re: BSD license compatible hash algorithm?

Re: BSD license compatible hash algorithm?

freebsd-hackers@xxxxxxxxxxx mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-hackers>

To unsubscribe, send any mail to "freebsd-hackers-unsubscribe@xxxxxxxxxxx"