

Re: BSD license compatible hash algorithm?

Re: BSD license compatible hash algorithm?

Source: <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/hackers/2007-12/msg00278.html>

- *From:* "Aryeh M. Friedman" <aryeh.friedman@xxxxxxxx>
 - *Date:* Sun, 30 Dec 2007 18:27:08 -0500
-

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

Hash: SHA1

Dag-Erling Smørgrav wrote:

"Aryeh M. Friedman" <aryeh.friedman@xxxxxxxx> writes:

All hashes have issues with pooling.... see
<http://www.burtleburtle.net/bob/hash/index.html>... btw it is a
old wives tale that the number of buckets should be prime (mostly
based on the very weak implementation Knuth offered)

Not an "old wives' tale", but rather an easy way to implement a
hash algorithm that is good enough for most simple uses: metric
modulo table size, where metric is a number derived from the item
in such a manner as to give a good spread.

Sorry for taking a while to reply.... but the above only applies if
your using a very primitive hash like Knuth's multiplication one....
every modern hash I know of should have 2^k buckets actually for some
 $k < 2^{32}$ [in almost all cases $< 2^{16}$ except for algorithms like the one I
mentioned I am working on which sets $k=n$ where n =the bit count of the
key].

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>

iD8DBQFHeCIMzIOMjAek4JIRA1A+AKCVC0oObIPhF7QZARtkfUmdGX4hVACfcyPd
qhtFfOt2lOaxcmCDt6/wXsE=
=jztY

-----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"