

Re: BSD license compatible hash algorithm?

Re: BSD license compatible hash algorithm?

Source: <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/hackers/2007-12/msg00223.html>

- *From:* "Aryeh M. Friedman" <aryeh.friedman@xxxxxxxxx>
 - *Date:* Fri, 28 Dec 2007 08:03:40 -0500
-

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

Hash: SHA1

Ivan Voras wrote:

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

All hashes have issues with pooling.... see
<http://www.burtleburtle.net/bob/hash/index.html>...

Here's a more direct link:
<http://www.burtleburtle.net/bob/hash/doobs.html>

This one is much better according to
http://en.wikipedia.org/wiki/Hash_table#Choosing_a_good_hash_function

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.

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>

iD8DBQFHdPQrzIOMjAek4JIRAgd2AJ43fYJ6SkceoLP8kD1wso5mpN1uGwCfaYoC
Vgkl6P2riL9JIEK+MKCnd4k=

Re: BSD license compatible hash algorithm?

Re: BSD license compatible hash algorithm?

=o/Eb

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

freebsd-hackers@xxxxxxxxxxx mailing list

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

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