
Subject: Re: New hash folding function...

Posted by [gprentice](#) on Tue, 22 Jan 2008 07:55:43 GMT

[View Forum Message](#) <> [Reply to Message](#)

Your new hash-fold function seems similar to the last step of that hash function on Wikipedia

```
hash += (hash << 3);  
hash ^= (hash >> 11);  
hash += (hash << 15);
```

Is this a standard type of thing to do after the byte-by-byte bit even when you're not saving the pre-masked result. Is there a mathematical basis for this "extra" bit (like CRC) or was it just found by trial and error?

Why do you call it "hash-fold" if it doesn't actually reduce the range of values

- or if

```
return (h >> 23) - (h >> 9) - (h >> 15) - h;
```

does reduce the range of values, how does it do that, since it's unsigned arithmetic?

Graeme
