

# Re: Making a weak Hash stronger until a fix comes along -- concatenation of hash functions... .2: Concatenation

**Source:** <http://www.derkeiler.com/Newsgroups/sci.crypt/2005-09/1204.html>

---

**From:** David Wagner ([daw\\_at\\_taverner.cs.berkeley.edu](mailto:daw_at_taverner.cs.berkeley.edu))

**Date:** 09/27/05

Date: Mon, 26 Sep 2005 23:13:26 +0000 (UTC)

Max Power wrote:

>*My use of concatenation was not totally clear.*

>*I would never consider adding the strings of the 2 hashes together.*

We understood that. As I and another poster have both pointed out, there are attacks on concatenation (see Joux's multi-collision work) which show that concatenation adds a lot less security than you might think.

Taking the hash and feeding it into another hash function doesn't help. If you use  $g(f(x))$  as your hash function, and if  $f(\cdot)$  has collisions, then so will  $g(f(\cdot))$ . Think about it.

Salts don't help, either.

>*True, it is not a perfect solution -- but merely an adequate one.*

Unfortunately, the proposals you presented are neither adequate nor a solution, I'm sorry to say.