

Re: Hash function, Birthday paradox and probabilities.

Source: <http://sci.tech-archive.net/Archive/sci.math/2006-03/msg02816.html>

- *From:* James Waldby <j-waldby@xxxxxxxx>
 - *Date:* Thu, 16 Mar 2006 00:57:44 -0700
-

fabrice.gautier@xxxxxxxx wrote:

....

Lets have:

- a hash function $H()$ that take as input a bit string of length L and return an hash of length N bits (ie an integer in the range $[0, 2^N[)$
- a iterator function F , that takes as input a bit string of length L and return another bit string of length L ,
- $S[0], S[1], \dots, S[n]$, bit strings of length L , so that $S[i+1]=F(S[i])$,
- $h[0], \dots, h[n]$, so that $h[i]=H(S[i])$
- M a fixed hash

Given all that lets define m , the smallest positive integer so that $h[m]=M$.

....

Now the question is what is the best function $a()$ to minimize m (in average), and how to minimize the "spread" of m around its average. (There must be a better word than "spread" but I dont remember)

[Variance]

I was thinking that, wether I use random or increments, the average of m should be 2^N , and my experiences seem to agree with that.

....

If the hash function does a really good job of scattering its L -bit inputs randomly and uniformly across an N -bit range, and if the $S[i]$ ordering is basically random, then m should average no more than $n/2$ [with $n = 2^N$] to a first collision, but around n between collisions as you go on. If you lack intimate knowledge of hash function H , you probably cannot make the average smaller by changing the presentation order of the $S[i]$, unless H is a bad hash function. (Note, Bruce Schneier writes, "Honestly,

Re: Hash function, Birthday paradox and probabilities.

we in the cryptography community know very little about hash functions", 1/4 of the way along in http://www.schneier.com/blog/archives/2005/03/more_hash_funct.html but perhaps he's exaggerating.)

Have you studied the "multicollision attack" work of Joux and of Wang et al? Eg, see refs at end of Dan Kaminsky's paper "MD5 To Be Considered Harmful Someday", at eg http://www.doxpara.com/md5_someday.pdf .

-jiw

.