

# Re: Revert MD4

---

*Source:* <http://sci.tech-archive.net/Archive/sci.math/2007-10/msg05637.html>

---

- *From:* galathaea <[galathaea@xxxxxxxxxx](mailto:galathaea@xxxxxxxxxx)>
  - *Date:* 29 Oct 2007 23:54:35 -0700
- 

On Oct 29, 2:52 pm, Federico Bertola <[federico.bertola...@xxxxxxxxxx](mailto:federico.bertola...@xxxxxxxxxx)> wrote:

2<sup>128</sup> (you write this right?) are teorically possibles COLLISIONS that means that a file has the same hash value as the original but with a infinite range of length.  
For example a file of 3 Mb may have a collision in a 300 Kb file as in a 2 Tb file!!!  
If I close the range of possibilities fixing the length I can find (at leas one if the length is the same as the original) very fewer collisions!  
I mean a MD4 in a not-so-hostile environment where you have some information about the original file.

there are just under 200,000 3MB files with the same hash

there an infinite number of files of any size

it is impossible to revert a hash  
in the way you mentioned

the cryptographic attacks on md4 are different  
they find different messages  
with the same hash

being able to do this  
means the hash is not safe for validation purposes  
as man-in-the-middle interception  
can replace messages that still authorise

-----  
galathaea: prankster, fablist, magician, liar

.