Cryptology ePrint Archive: Report 2013/170

Fast Collision Attack on MD5

Tao Xie and Fanbao Liu and Dengguo Feng

Abstract: We presented the first single block collision attack on MD5 with complexity of 2^{47} MD5 compressions and posted the challenge for another completely new one in 2010. Last year, Stevens presented a single block collision attack to our challenge, with complexity of 2^{50} MD5 compressions. We really appreciate Stevens's hard work. However, it is a pity that he had not found even a better solution than our original one, let alone a completely new one and the very optimal solution that we preserved and have been hoping that someone can find it, whose collision complexity is about 2^{41} MD5 compressions. In this paper, we propose a method how to choose the optimal input difference for generating MD5 collision pairs. First, we divide the sufficient conditions into two classes: strong conditions and weak conditions, by the degree of difficulty for condition satisfaction. Second, we prove that there exist strong conditions in only 24 steps (one and a half rounds) under specific conditions, by utilizing the weaknesses of compression functions of MD5, which are difference inheriting and message expanding. Third, there should be no difference scaling after state word q_{25} so that it can result in the least number of strong conditions in each differential path, in such a way we deduce the distribution of strong conditions for each input difference pattern. Finally, we choose the input difference with the least number of strong conditions and the most number of free message words. We implement the most efficient 2-block MD5 collision attack, which needs only about 2^{18} MD5 compressions to find a collision pair, and show a single-block collision attack with complexity 2^{41}.

Category / Keywords: Hash Function; MD5 Differential Cryptanalysis; Collision Attack; Single-Block Collision

Date: received 25 Mar 2013

Contact author: liufanbao at gmail com