ABSTRACTION

This research presents comparation between two methods of MD5 differential attack. Differential attack of MD5 used for searching two block data pairs that each of two block data having same MD5 digest value. The methods are technic that have been proposed by Jun Yajima et. al. and the begining technic of differential attack for MD5 that have been proposed by XiaoYun Wang et. al.. Both technics give differential way to search two block pairs of data.

Collision data searched in exhaustive way and including condition variables for each MD5 iteration and difference result of each iteration proccess.

Comparation of two technics applied by searching of two block data pairs using first block data pairs as input. Test of Jun technic applied by passing first block data pairs of Wang to Jun's searching proccess of block 2 pairs. Wang's test applied in the same way. Second test is condition parameter testing. Two block pairs of valid collision data is passed through condition parameter checking of each technic in order to known which condition parameter that giving success or fail. Condition parameter of Jun's receives input 2 block pairs of valid data from searching result of Wang's technic. Condition parameter testing for Wang's applied in the same way.

Testing results shown that Jun's searching technic giving more results and faster than Wang's have. More global, can be said that Wang's searching technic is a subset of Jun's.

Keywords: *MD5, Collision, Cryptanalysis, Differential Attack*