Practical Near-Collisions and Collisions on Round-Reduced ECHO-256 Compression Function

http://www.firstlight.cn 2010-11-08

In this paper, we present new results on the second-round SHA-3 candidate ECHO. We describe a method to construct a collision in t he compression function of ECHO-256 reduced to four rounds in 2^52 operations on AES-columns without significant memory requirement s. Our attack uses the most recent analyses on ECHO, in particular the SuperSBox and SuperMixColumns layers to utilize efficiently the avail able freedom degrees. We also show why some of these results are flawed and we propose a solution to fix them. Our work improve the tim e and memory complexity of previous known techniques by using available freedom degrees more precisely. Finally, we validate our work b y an implementation leading to near-collisions in 2^36 operations.

存档文本