www.firstlight.cn

北京雷速科技有限公司

返回首页

Improved Collisions for Reduced ECHO-256

http://www.firstlight.cn 2010-11-18

In this work, we present a collision attack on 5/8 rounds of the ECHO-256 hash function with a complexity of 2^{112} in time and $2^{85.3}$ memory. In this work, we further show that the merge inbound phase can still be solved in the case of hash function attacks on ECHO. As correctly observed by Jean et al., the merge inbound phase of previous hash function attacks succeeds only with a probability of 2^{-128}. The main reason for this behavior is the low rank of the linear SuperMixColumns transformation. However, since there is enough freedom in ECHO we can solve the resulting linear equations with a complexity much lower than 2^{128}. On the other hand, also this low rank of the linear SuperMixColumns transformation allows us to extend the previous collision attacks by one more round.

存档文本