Cryptology ePrint Archive: Report 2011/656

Use Data-depend Function Build Message Expansion Function

ZiJie Xu and Ke Xu

Abstract: We had found functions can be used to fix bits [2] by given differences. We use these functions build a message expansion function. In the message expansion function, there are some bits include message bits and incremental bits produced from message bits, these bits will be used as parameter of date-depend function. This message expansion function will fixed at lease n × 5.5 bits with given differences, and any message modification will affect at least 8 data-depend function parameter.

Category / Keywords: Message expansion function, Data-depend function, message modification

Date: received 4 Dec 2011

Contact author: xuzijiewz at gmail com

Available formats: PDF | BibTeX Citation

Version: 20111209:205201 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]