MARS の最大差分 / 線形特性確率について

盛合 志帆

日本電信電話株式会社

2001 年 1 月 12 日

概要

本報告書は CRYPTREC にて公募された共通鍵ブロック暗号 MARS の安全性の詳細評価報告であり、(1) ブロック暗号の検証評価 — (a) 最大線形 / 差分確率もしくは最大線形 / 差分特性確率について報告するものである。本評価の結果、最大差分特性確率については、 keyed transformation (16 段の cryptographic core) の最大差分特性確率として、自己評価書に記述されている 2^{-156} という値を妥当と判断する。最大線形特性確率については、 keyed transformation の最大線形特性確率として、提案者により NIST に public comment として提出されている文献に記述されている 2^{-120} という値を妥当と判断する。しかし、 MARS の最大差分／線形特性確率のより妥当な評価結果を得るには、さらに詳細な評価が必要で、多くの時間を要すると考える。