Hierocrypt-3 の最大線形 / 差分確率 および最大線形 / 差分特性確率について

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 Hierocrypt-3 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。

Hierocrypt-3 では入れ子型 SPN 構造を採用しており、その拡散層 (diffusion layer) として最大距離分離符号 (Maximum Distance Separable Code) に用いられる行列を利用している。このような暗号の active S-box 数の下限は 容易に評価できることが知られており、自己評価書ではこの方法により最大差分／線形特性確率の上限を評価している。 Hierocrypt-3 においてこの評価方法は妥当であり、提案者が示している数値も正しいと判断できる。よって、 Hierocrypt-3 は 2 段以上で 2^{-150} の最大差分／線形特性確率を超えないことが保証できる。

最大差分／線形確率については、 Hong らの示した結果を利用して、 Hierocrypt-3 の部分構造についての最大差分／線形確率を評価することができる。自己評価書では、これを利用して Hierocrypt-3 全体の最大差分／線形確率を評価している。この評価には一部、厳密ではないところがあったため、再評価を行なった。再評価の結果、鍵スケジュールに問題がなく、その結果各段に与えられる鍵が一様でランダムに分布していると仮定した場合、 Hierocrypt-3 は 2 段, 3 段で最大差分／線形確率はそれぞれ 2^{-96} を超えないことが保証でき、 4 段で 2^{-168} を超えないことが示された。