

軽量ブロック暗号 DoT に対する MILP を用いた線形攻撃 Linear attack on lightweight block cipher DoT using MILP

青柳 光祐 *
Kosuke Aoyagi

五十嵐 保隆 †
Yasutaka Igarashi

キーワード 軽量ブロック暗号, DoT, 線形攻撃, MILP

あらまし

DoT は、2019 年に Patil らによって提案された SPN 構造を持つ軽量ブロック暗号である。ブロック長は 64 ビット、鍵長は 128 ビット、段数は 31 段である。DoT の線形特性は提案者による簡単な見積もりしかなく、第三者による評価はなされていない。本稿では、DoT の線形特性を MILP (Mixed Integer Linear Programming) を利用して探索した。得られた特性を用いて、DoT 全段に対しての鍵回復に必要な平文数、計算量を算出した。

ブロック暗号 DoT

DoT は、巡回シフト (図 1 の " $\lll$ ", " $\ggg$ ")、4 bits S-box (図 1 の "S")、ビットの入れ替え (図 1 の "8-P") で構成されている。1 段分の構造を以下の図 1 に示す。

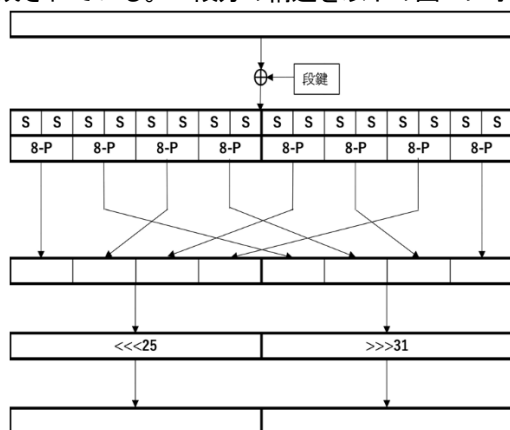


図 1 : DoT 1 段分の構造

MILP を用いた線形解析

目的関数および制約条件は線形であり、変数の全てまたは一部が整数に制限される数理最適化問題を混合整数

線形計画法 (Mixed Integer Linear Programming) と呼ぶ。目的関数を線形特性確率、制約条件を暗号化関数の線形マスクの伝搬規則から線形不等式とし解析を行った。解析の結果、30 段で最大線形特性確率 2^{-60} 、31 段で最大線形特性確率 2^{-62} を与える線形パスを発見した。

線形特性を利用した鍵回復

30 段のショートカット部に 1 段の鍵回復部をつけた DoT に対し、鍵回復に必要な計算量・平文数を算出した。MILP による解析の結果得られた 30 段で 2^{-60} を与える線形パスの中から、16 組の線形パスを利用した。

表 1 : 鍵回復に必要な計算量・平文数

暗号化計算量	必要な平文数
$2^{59.05}$	2^{60}

参考文献

- [1] Jagdish Patil et al, "DoT: A New Ultra-lightweight SP Network Encryption Design for Resource-Constrained Environment" Springer Nature Singapore Pte Ltd. 2019, Part of the Advances in Intelligent Systems and Computing book series (AISC, volume 828)
- [2] Nicky Mouha, "Differential and Linear Cryptanalysis using Mixed-Integer Linear Programming" In Information Security and Cryptology – 7th International Conference, Inscrypt 2011, Beijing, China. Revised Selected Papers. Pp.55-76

* 東京理科大学理工学研究科電気工学専攻, 〒278-8510 千葉県野田市山崎 2641, 7321501@ed.tus.ac.jp

† 東京理科大学理工学研究科電気工学専攻, 〒278-8510 千葉県野田市山崎 2641