講演番号：113

軽量ブロック暗号 GIFT に対する高階差分特性調査

D－19　　Basic study on saturation property of GIFT block cipher

伊藤　亮†　五十嵐　保隆†
Ryo ITO†　Yasutaka IGARASHI†
† 東京理科大学理工学専攻電気工学科
† Faculty of Engineering, Tokyo University of Science

1. はじめに

GIFT は 2017 年に Subhadeep Banik, Sumit Kumar Pandey らによって提案された軽量ブロック暗号である[1]。飽和特性は高階差分特性をさらに細分化したものであり、その特性を利用した高階差分攻撃は Lai が提案した暗号攻撃手法である。暗号化関数のブール多項式の代数次数に着目した攻撃法であり、 共通鍵暗号アルゴリズム全般に広く適用できる攻撃法である。PRIDE には飽和攻撃の識別子となる飽和特性の調査は実施されていなかった。本稿では GIFT に対し提案者評価を上回れるかどうか飽和特性の調査を行った。

2. GIFT のデータ撹拌部

GIFT のブロック長は 64bit、鍵長は 128 bit、段数は 28 段である。R 関数は SBox を用いて非線形変換を行う S 層と、1bit 毎のデータの入れ換えを行う P 層で構成される。P は平文、C は暗号文、R_i は i 段目の段関数、RK^i は i 段での暗号化鍵を表す。段関数の構造を図 2 に示す。

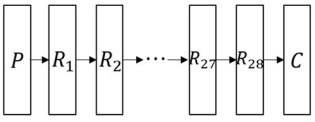

図 1 GIFT の全体構造

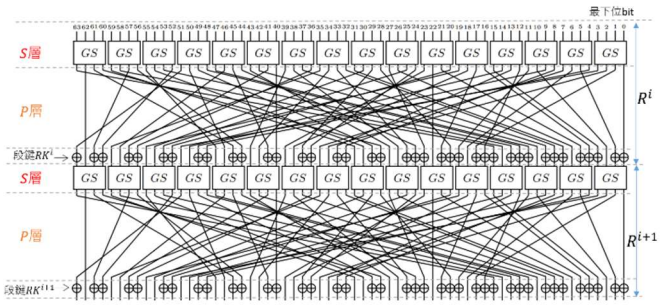

図 2 段関数

3. 高階差分

3.1 定義

入力$X \in \mathrm{GF}(2)^n$と鍵$K \in \mathrm{GF}(2)^r$から$Y \in \mathrm{GF}(2)^m$を出力する暗号化関数を$Y = E(X;K)$と表す。このとき$\mathrm{E}(X;K)$のXに対するi階差分を以下の式で定義する。

$$\Delta^{(i)}_{V^{(i)}} E(X;K) = \sum_{\alpha \in V^{(i)}} E^{\oplus}(X \oplus \alpha;K) \quad (1)$$

但し、$V^{(i)}$ は$\mathrm{GF}(2)^n$の i次元部分空間であり、αは入力差分である。

3.2 性質

関数$E(X;K)$の X に関するブール代数次数が N ならば Xと Kに依存せず、次式が成立

$$deg_x\{E(X;K)\} = N \Rightarrow \begin{cases} \Delta^{(N)} E(X;K) = const \\ \Delta^{(N+1)} E(X;K) = 0 \end{cases} \quad (2)$$

また、高階差分は⊕演算に関し、線形性を持つ。

$$\begin{aligned} &\Delta^{(N)}\{E(X;K_1) \oplus F(X;K_2)\} \\ &= \Delta^{(N)} E(X;K_1) \oplus \Delta^{(N)} F(X;K_2) \end{aligned} \quad (3)$$

3.3 飽和特性

Nビットデータ Xの集合$\{X_j | X_j \in \{0,1\}^N, 0 \le j < 2^N\}$の性質として以下の5通りを定義する。ただし、$Y_i$は$X = i$の出現度数である。

Constant(C)　：$\forall_{i,k}\ ;\ X_i = X_k$
All(A)　：$\forall_{i,k}\ ; i \neq k \rightarrow X_i \neq X_k$
Even(E)　：$\forall_i\ ;\ Y_i \equiv 0 \pmod 2$
Balance(B)　：$\sum_i^{\oplus} X_i = 0$
Unknown(U)　：不定値

U 以外は識別子として利用可能である。

4 高階差分特性の調査

計算機実験により、24 階差分を与えると、8 段目出力の高階差分値が 0 になることを発見した。

5 結び

GIFT に対する飽和特性を報告した。24 階差分を用いて 8 段特性が得られることを示した。

6 今後の研究予定

より少ない計算量での攻撃が可能となる高階差分特性の発見。

参考文献

[1] Subhadeep Banik, Sumit Kumar Pandey “GIFT A Small Present Towards Reaching the Limit of Lightweight Encryption”
[2] Baoyu Zhu“MILP-based Differential Attack on Round-reduced GIFT”
[3] L.R. Knudsen, “Truncated and Higher Order Differentials,” 2nd Fast Software Encryption(1994), LNCS 1008, pp.196-211, Springer-Verlag, 1995.
[4] 金子敏信 “共通鍵暗号の安全性評価” https://www.jstage.jst.go.jp/article/essfr/7/1/7_14/_pdf