1E-02

ブロック暗号KASUMIに対するBit-based Division Propertyの適用に向けた解析(II)

An analysis on the block cipher KASUMI by appling Bit-based Division Property (II)

杉尾 信行† 五十嵐 保隆‡ 本郷 節之†
北海道科学大学† 東京理科大学‡

1 はじめに

KASUMIは2000年に3GPP（3rd Generation Partnership Project）にてW-DCMA方式の国際標準暗号として採用された共通鍵暗号アルゴリズムである[1].

共通鍵暗号に対する汎用的，且つ強力な攻撃手法として，Knudsenと Wagnerらによる積分攻撃が知られている[3]．積分攻撃は平文集合を複数段暗号化した途中段出力集合のXOR総和が鍵に依存せず常に0となる性質を用いた攻撃である．

藤堂らは積分攻撃において代数次数を含めた解析が可能なDivision Property（DP）[4, 5]を提案した．また，藤堂らはbit単位でDivision Propertyの解析が可能なBit-based Division Property（BDP）を提案し，共通鍵ブロック暗号SIMONに適用した[6]．必要な計算量とメモリ量の観点から，ブロックサイズが32-bitを超える暗号に対するBDPを用いた解析は困難であった．

上記の課題を解決する為，Xiangらは軽量ブロック暗号に対し，混合整数線形計画問題（Mixed Integer Linear Programming, MILP）を用いてBDPによる積分特性探索を行う手法を提案した[7].

本稿では，Xiangらの手法に倣い，共通鍵ブロック暗号KASUMIに対して，MILPを用いてBDPによる積分特性探索を行う手法の適用に向けた解析結果について報告する．

1.1 関連研究

杉尾らはKASUMIに対してDPを用いた積分特性探索を行い，5段特性を発見した．この5段特性を用いて7段KASUMIが攻撃可能である事を示している[8].

また，杉尾らはKASUMIのS-boxに対するBDPの伝搬を解析している[9].

1.2 本研究の貢献

MILPを用いてBDPによる積分特性探索を行う手法の適用に向け，S-box（S7，S9）のBDP伝搬に関する制約式の導出を試みた．本研究の貢献は以下の通りである．

- S7の制約式は文献[2]を参考にEspressoアルゴリズムを用いて導出した．
- S9の制約式は計算量の観点からEspressoアルゴリズムで導出したSOP（Sum of Product）表現をPOS（Product of Sum）表現に変換する事が困難であり，導出する事が出来なかった．

2 Bit-based Division Property

藤堂らは積分攻撃で用いる積分特性の探索において，代数次数を含めた解析が可能なDivision Property（DP）を提案した[4, 5]．また，Bit-based Division Property（BDP）を提案し，bit単位でDivision Propertyの解析が可能となった[6]．本稿では，BDPについて概説する．詳細は文献[4, 5, 6]を参照のこと．

2.1 ビット積関数

任意のn bit変数aに対し，aのi番目の要素を$a[i]$と示すものとする．π_uを任意のn bit変数uを用いて1 bitを出力する関数とする．関数の入力をn bit変数xとした時，ビット積関数$\pi_u(x)$は以下の式で定義される．

$$\pi_u(x) := \prod_{i=1}^{n} x[i]^{u[i]} \tag{1}$$

$\pi_{\boldsymbol{u}}$を任意のm次元ベクトル$\boldsymbol{u} = (u_m, u_{m-1}, \cdots, u_1)$, $u_i \in \{0,1\}^n$を用いて1 bitを出力する関数とする．関数の入力をm次元ベクトル$\boldsymbol{x} = (x_m, x_{m-1}, \cdots, x_1)$, $x_i \in \{0,1\}^n$とした時，ビット積関数$\pi_{\boldsymbol{u}}(\boldsymbol{x})$は以下の式で定義される．

$$\pi_{\boldsymbol{u}}(\boldsymbol{x}) := \prod_{i=1}^{m} \pi_{u_i}(x_i) \tag{2}$$

ただし，本稿ではBit-based Division Propertyを扱う為，式(1)，(2)において$n = 1$である．

2.2 BDPの定義

m次元ベクトル$\boldsymbol{x}$の集合を$\mathbb{X}$とする．また，m次元ベクトル$\boldsymbol{k}$の集合を$\mathbb{K}$とする．集合$\mathbb{X}$がBDP $\mathcal{D}_{\mathbb{K}}^{1^m}$を持つ時，以下の条件を満たす．

$$\bigoplus_{\boldsymbol{x}\in\mathbb{X}} \pi_{\boldsymbol{u}}(\boldsymbol{x}) = \begin{cases} \text{unknown} & \text{if there are } \boldsymbol{k} \in \mathbb{K} \text{ s.t. } W(\boldsymbol{u}) \succeq \boldsymbol{k}, \\ 0 & \text{otherwise} \end{cases} \tag{3}$$

† Nobuyuki Sugio and Sadayuki Hongo, Hokkaido University of Science
‡ Yasutaka Igarashi, Tokyo University of Science

ここで，$W(\boldsymbol{u})$ は m 次元ベクトル $\boldsymbol{u}$ のハミング重みを示す．また，異なるベクトル $\boldsymbol{k}$ と $\boldsymbol{k'}$ に対し，全ての要素で $k_i \geq k'_i$ を満たす時，$\boldsymbol{k} \succeq \boldsymbol{k'}$ と記す．

3 MILP-aided Bit-based Division Property

計算量とメモリ量の観点から，ブロックサイズが 32-bit を超える暗号に対して BDP の適用は困難であることが指摘されている [6].

この課題に対し，Xiang らは混合整数線形計画問題（Mixed Integer Linear Programming, MILP）を用いて BDP による積分特性探索を行う手法を提案した [7]. この手法では，BDP の伝搬に関する制約式と目的関数を適切に設定する事で混合整数線形計画問題に変換し，`gurobi`[1]等のソルバーを利用する事で，BDP による積分特性探索を実現している．

4 共通鍵ブロック暗号 KASUMI

KASUMI はブロック単位で暗号化，復号化を行う共通鍵ブロック暗号アルゴリズムである [1]．入出力長は 64-bit，秘密鍵長は 128-bit であり，8 段の Feistel 構造を有している．KASUMI は W-CDMA 方式の国際標準暗号であり，第二世代（GSM 方式）と第三世代（W-CDMA 方式）の移動体通信システムで利用されている．

5 S-box の制約式

文献 [7] では，Xiang らは SageMath の inequality generator 関数を用いて S-box の BDP 伝搬に関する制約式を導出している．この手法は S-box のサイズが 4-bit であれば制約式の導出が可能であるが，S-box のサイズが大きい（8-bit，又はそれ以上）場合は計算量の観点で制約式の導出が不可能となる．KASUMI の S-box のサイズは S7 が 7-bit，S9 が 9-bit である為，SageMath の inequality generator 関数を用いて制約式を導出する事は出来ない．

上記の課題を解決する為，Abdelkhalek らは Quine-McCluskey アルゴリズムや Espresso アルゴリズムを用いて入出力サイズが大きい S-box の差分特性伝搬に関する制約式を導出する新たな手法を提案した [2].

本稿では，Abdelkhalek らの手法を応用し，Espresso アルゴリズムを用いて S-box の BDP 伝搬の制約式導出を試みた．解析結果を表 1 に示す．

S-box の制約式は POS 表現から導出可能であり，S7 の制約式は 648 本である事が判明した．紙面の都合上，全ての制約式を記載することが出来ない為，詳細は以下の URL にて公開する[2].

表 1: S-box の解析結果

S-box	BDP 伝搬数	SOP 表現	POS 表現
S7	1779	2481	648
S9	27623	11870	-

SOP：Sum of Product，POS：Product of Sum

また，S9 の制約式は計算量の観点から Espresso アルゴリズムで導出した SOP 表現を POS 表現に変換する事が困難であり，導出する事が出来なかった．

6 まとめと今後の課題

本稿では，共通鍵ブロック暗号 KASUMI に対して，MILP を用いて BDP による積分特性探索を行う手法の適用に向け，S-box の BDP 伝搬の制約式を解析した．S7 の制約式は導出する事が出来たが，計算量の観点から S9 の制約式を導出する事が出来なかった．

今後の課題は SOP 表現から制約式を導出する手法の検討や，その他の手法を検討する予定である．

謝辞

本研究は JSPS 科研費 JP21K21292 の助成を受けたものです．

参考文献

[1] 3GPP. “Specification of the 3GPP confidentiality and integrity algorithms; Document 2: Kasumi specification”, `http://www.3gpp.org`

[2] A. Abdelkhalek, Y. Sasaki, Y. Todo, M. Tolba and A. M. Youssef. “MILP Modeling for (Large) S-boxes to Optimize Probability of Differential Characteristics”, IACR Transactions on Symmetric Cryptology, Vol. 2017, No. 4, pp. 99-129, 2017.

[3] L. R. Knudsen and D. Wagner. “Integral cryptanalysis”. Proceedings of FSE 2002, LNCS 2365, pp.112-127, 2002.

[4] Y. Todo. “Structural Evaluation by Generalized Integral Property”, Proceedings of EUROCRYPT 2015, LNCS 9056, part1, pp. 287-314, 2015.

[5] Y. Todo. “Integral Cryptanalysis on Full MISTY1”, Proceedings of CRYPTO 2015, LNCS 9215 Part1, pp. 413-432, 2015.

[6] Y. Todo, M. Morii “Bit-Based Division Property and Application to Simon Family”, Proceedings of FSE 2016, pp. 357-377, 2016.

[7] Z. Xiang, W. Zhang, Z. Bao and D. Lin “Applying MILP Method to Searching Integral Distinguishers Based on Division Property for 6 Lightweight Block Ciphers”, Proceedings of ASIACRYPT 2016, pp.648-678, 2016.

[8] 杉尾信行，五十嵐保隆，金子敏信． “共通鍵ブロック暗号アルゴリズム KASUMI の積分攻撃 ”, SCIS2017, 2B1-4, 2017.

[9] 杉尾信行，本郷節之，五十嵐保隆．“ブロック暗号 KASUMI に対する Bit-Based Division Property の適用に向けた解析 ”，令和 3 年度 電気・情報関係学会 北海道支部連合大会, pp.116-117, 2021.

[1] `https://www.gurobi.com/`

[2] `https://github.com/NobuyukiSUGIO/KASUMI-Constrains-Sbox`