Integral攻撃の最新動向と MISTY1等への適用

NTTセキュアプラットフォーム研究所
藤堂　洋介

2016年2月

概 要

Integral 攻撃は文献 [KW02] で Knudsen らによって導入された解析手法である．この解析手法は強力な暗号解析手法の一つとして知られ以降多くの共通鍵暗号に適用されてきた．Eurocrypt2015 にて Integral 攻撃を改良する新手法が提案された [Tod15b]．新手法では Division Property と呼ばれる特性が新たに導入され，この特性の伝搬を評価することで Integral 攻撃の要となる Integral 特性が大幅に改良できることが示された．文献 [Tod15b] では Division Property の概念および基本的な関数に対する伝搬特性が示され，その応用として Feistel 構造と SPN 構造に対する汎用解析 (Generic Attack) が示された．より具体的な暗号方式への応用は CRYPTO2015 で示され [Tod15a]，CRYPTREC 推奨候補暗号リストである MISTY1 [Mat97] の初の暗号解読が示された．文献 [Tod15a] では Division Property を用いて MISTY1 の 6 段 Integral 特性を新たに発見した．これは従来の 4 段 Integral 特性から 2 段改良されている．結果として，新たに発見された Integral 特性を用いることで仕様段数である 8 段 MISTY1 の解読が可能となった．

本レポートの第一部では Division Property (基本編) と題して，Integral 攻撃の基本から Division Property の解説，Feistel 構造と SPN 構造に対する Generic Attack を解説する．具体的な暗号への応用は第二部の Division Property (応用編) で示す．第二部では Division Property を用いた解析を AES および MISTY1 に適用した結果を解説する．また文献 [ZW15] で示された LBlock [WZ11] および TWINE [SMMK12] への応用を解説する．最後に Division Property を CRYPTREC 推奨暗号リストに記載されている共通鍵暗号に適用した場合に関する考察を述べる．

目 次

第I部

Division Property (基本編)

第1章　はじめに

Integral 攻撃はブロック暗号 SQUARE に対する専用解析手法として提案され [DKR97]，その後 Knudsen らによって Integral 攻撃という名前で定式化された [KW02]．Integral 攻撃は強力な暗号解析手法の一つとして知られ提案以降多くの共通鍵暗号に適用されてきた．Integral 攻撃では，攻撃者は初めに Integral 特性を探索する必用がある．Integral 特性を探索する手法として 2 つの著名な手法が知られている．一つは Integral Property の伝搬特性を利用する方式であり，Integral 攻撃の提案論文でもある文献 [KW02] で導入された．もう一つは代数次数の上界を見積もる手法であり，しばしば高階差分攻撃 [Lai94, Knu94] という名前で提案される手法である．

Eurocrypt2015 で Integral 特性を探索する新手法が提案された [Tod15b]．文献 [Tod15b] では新たに Division Property と呼ばれる性質が定義され，Integral 特性はこの Division Property の伝搬特性を評価することで発見される．この手法で発見される Integral 特性は Integral Property の伝搬特性や代数次数の見積りによって得られる Integral 特性と比較して大幅に改良される場合が多い．文献 [Tod15b] では Division Property の概念および基本的な関数に対する伝搬特性が示され，その応用として Feistel 構造と SPN 構造に対する Generic Attack が示された．具体的な暗号方式への応用は文献 [Tod15a] で示され，CRYPTREC 推奨候補暗号リストに記載されている MISTY1 [Mat97] の初の暗号解読手法が提案された．文献 [Tod15a] では Division Property を用いて MISTY1 の 6 段 Integral 特性を新たに発見した．これは従来の 4 段 Integral 特性から 2 段改良されている．結果として，新たに発見された Integral 特性を用いることで仕様段数である 8 段 MISTY1 の解読が可能となった．

第一部では 2 章で Integral 攻撃の紹介および Integral 特性を探索する従来の手法を簡単に紹介する．その後，第 3 章では Division Property を解説する．Division Property を用いた解析の簡単な例として第 4 章で Feistel 暗号に対する Generic Attack，第 5 章で SPN 構造に対する Generic Attack をそれぞれ示す．より具体的な暗号方式への応用は，本レポートの第二部で示す．

第2章　基礎知識

本章では本レポートを理解する上で必要不可欠な基礎知識をまとめる．

2.1　表記法

本節では本レポートを通して共通する表記法を示す．標数 2 の拡大体 $\mathbb{F}_2^n$ 上と整数 $\mathbb{Z}$ 上の加算を区別するため，それぞれ加算記号として $\oplus$ と $+$ を利用する．任意の $a \in \mathbb{F}_2^n$ において，その i 番目のビットを $a[i]$ とし，ハミング重み $w(a)$ は $w(a) = \sum_{i=1}^{n} a[i]$ で計算される．$1^n \in \mathbb{F}_2^n$ は全てのビットが 1 である n ビット値，$0^n \in \mathbb{F}_2^n$ は全てのビットが 0 である n ビット値を表す．任意の集合 $\mathbb{K}$ に対して，$|\mathbb{K}|$ は集合の要素数を表し，ϕ は空集合を表す．

任意のベクトル $\vec{a} \in (\mathbb{F}_2^{n_1} \times \mathbb{F}_2^{n_2} \times \cdots \times \mathbb{F}_2^{n_m})$ に対して，ベクトル化ハミング重みは $W(\vec{a}) = [w(a_1), w(a_2), \ldots, w(a_m)] \in \mathbb{Z}^m$ で定義される．また任意の $\vec{k} \in \mathbb{Z}^m$ と $\vec{k'} \in \mathbb{Z}^m$ において，もし全ての i において $k_i \geq k'_i$ ならば $\vec{k} \succeq \vec{k'}$ と表記する．

2.1.1　Bit Product Function

本レポートではしばしば下記で定義する Bit Product Function が用いられる．

Definition 1 (Bit Product Function π_u)**.** Let $\pi_u : \mathbb{F}_2^n \to \mathbb{F}_2$ be a function for any $u \in \mathbb{F}_2^n$. Let $x \in \mathbb{F}_2^n$ be an input of π_u, and $\pi_u(x)$ is the AND of $x[i]$ satisfying $u[i] = 1$, i.e., it is defined as

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

またベクトルが入力されるとき下記で定義する Bit Product Function が用いられる．

Definition 2 (Bit Product Function $\pi_{\vec{u}}$)**.** Let $\pi_{\vec{u}} : (\mathbb{F}_2^{n_1} \times \mathbb{F}_2^{n_2} \times \cdots \times \mathbb{F}_2^{n_m}) \to \mathbb{F}_2$ be a function for any $\vec{u} \in (\mathbb{F}_2^{n_1} \times \mathbb{F}_2^{n_2} \times \cdots \times \mathbb{F}_2^{n_m})$. Let $\vec{x} \in (\mathbb{F}_2^{n_1} \times \mathbb{F}_2^{n_2} \times \cdots \times \mathbb{F}_2^{n_m})$ be an input of $\pi_{\vec{u}}$, i.e., $\pi_{\vec{u}}(\vec{x})$ is calculated as

$$\pi_{\vec{u}}(\vec{x}) := \prod_{i=1}^{m} \pi_{u_i}(x_i).$$

2.2 繰り返し暗号

現在利用される多くのブロック暗号は繰り返し暗号の構造を持つ．繰り返し暗号では平文 $p \in \mathbb{F}_2^n$ から暗号文 $c \in \mathbb{F}_2^n$ は

$$c = (F_r \circ F_{r-1} \circ \cdots \circ F_1)(p)$$

のように計算される．ここで F_i はラウンド関数と呼ばれ，上記の例のブロック暗号はブロック長が n である r 段繰り返し暗号と呼ばれる．ラウンド関数はブロック暗号全体と比較すると非常に脆弱な関数を用いる一方，非常に計算効率の良い構造を取る．さらにラウンド関数は入力 $x \in \mathbb{F}_2^n$ に対して

$$F_i(x) = F(k_i, x)$$

な構造を持つ．すなわちラウンド関数は 2 入力 1 出力関数であり，ここで k_i はラウンド鍵である．この構造によりブロック暗号全体で高い計算効率が達成可能となる．

繰り返し暗号では繰り返し回数 (ラウンド数) を増やせば増やすほど暗号としての安全性が強化され，一方で計算効率は低下する．設定したラウンド数が小さすぎたとき暗号としての安全性が損なわれる．一方で設定したラウンド数が大きすぎたとき暗号としての性能が損なわれる．したがって暗号設計者は自身が提案した暗号に対して自己解析を実行し，解析可能だった段数をもとに仕様段数を決定する．また提案された暗号が真に安全か否かは自己評価のみでは不十分であり，第三者による暗号解析も重要である．第三者解析でも同様に解析可能だった段数が報告され，仮に仕様段数全てに到達した場合，暗号は解読された状態となる．

現在では多くの暗号解析手法が知られている．2 大解析手法として知られるのは Biham が提案した差分解読法 [BS90] と松井氏が提案した線形解読法 [Mat93] である．この 2 つの解析手法は広く研究されており，証明可能安全を満たした暗号を設計することも可能である [NK95, Mat96, DR02, Vau03]．現在では上記解読法の他に不能差分攻撃 [BBS99]，高階差分攻撃 [Lai94]，Integral 攻撃 [KW02] といった多数の新しい解析手法が知られている．これらの解析手法は各特性の探索から始まる．例に不能差分攻撃を用いて解説する．不能差分攻撃では初め不能差分特性を探索する．不能差分特性とは “平文 p が特定の差分 Δp を持つとき暗号文 c が特定の差分 Δc を持つ確率は 0 である” という特性である．理想的ブロック暗号において Δp から Δc が生成される確率が大きい場合，攻撃者は不能差分特性を利用して不能差分識別子を構成できる．実際の暗号解析のシナリオでは仕様段数全てをカバーするような特性を発見する必要はない．仮に仕様段数から 1 段減らした暗号の特性を発見できたとする．このとき攻撃者は最終段で利用されるラウンド鍵を推測し暗号文から 1 段巻き戻した内部状態を計算する．正しいラウンド鍵を推測したとき攻撃者は正しい内部状態を得る．一方で誤ったラウンド鍵を推測し

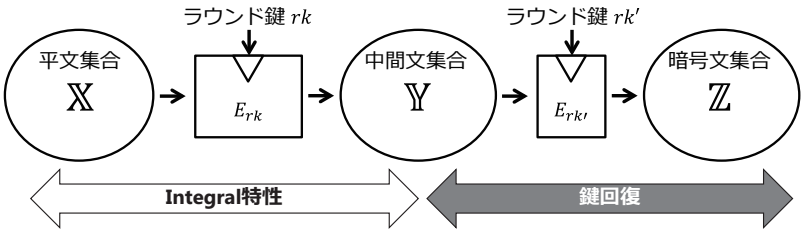


図 2.1: Outline of Integral Cryptanalysis

たとき計算される値はランダムに触れると仮定する．最終的に推測したラウンド鍵が正しいか否かを各特性を用いて判定する．このシナリオに関しては Integral 攻撃を例に次章で詳しく解説する．

2.3 Integral 攻撃

Integral 攻撃は初めブロック暗号 SQUARE に対する専用解析手法として提案され [DKR97] その後 Knudsen と Wagner によって定式化された [KW02]．図 2.1 は Integral 攻撃のアウトラインを示す．攻撃者は Integral 攻撃を実行する際，初めに Integral 特性の探索を行う．Integral 特性とは特定の平文集合に属する全ての平文を複数段暗号化した中間状態の和が全ての鍵に対して 0 になるような特性を指す．理想的なブロック暗号では中間状態の (一部の) 和が 0 になる確率は非常に小さいため攻撃者は Integral 特性を構築することで直ちに Integral 識別子を構成できる．また Integral 特性の段数が大きくなればなるほど Integral 攻撃は強力になると言える．実際の暗号解析のシナリオでは鍵回復を Integral 特性に付加することで Integral 攻撃を実行する．ブロック暗号が r 段 Integral 特性を持つと仮定する．このとき攻撃者は $r+s$ 段のブロック暗号の解析を試みる．攻撃者は最終 s 段で使われたラウンド鍵を推測し r 段中間状態の和を評価する．もし最終 s 段で推測されたラウンド鍵が正しい場合その和は必ず 0 となる．したがって和が非ゼロとなったとき推測したラウンド鍵は間違っていることが分かる．このような手順を繰り返すことで，攻撃者は最終 s 段で使われているラウンド鍵を正しく解読することができ，最終的にこれらの情報から秘密鍵を解読することができる．

2.3.1 Integral 特性

平文集合 $\mathbb{X}$ を r 段暗号化した中間文集合を $\mathbb{Y}$ とする．このとき最初の r 段で利用される全てのラウンド鍵で $\bigoplus_{y\in\mathbb{Y}} f(y) = 0$ となる平文集合を構成できるならば，この暗号は r 段 Integral 特性を持つと言う．ここで関数 f は攻撃者にとって既知の観測用関数である．課題はいかにして Integral 特性を発見するかである．以下に Integral 特性を発見する主要な 2 つの手法を紹介する．

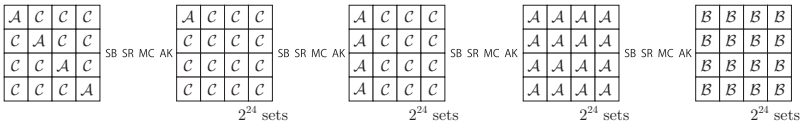


図 2.2: Integral distinguisher on 4-round AES

Integral Property

Integral Property の伝搬を評価する手法は Integral 特性を探索する上で最も頻用される手法であり，この手法を用いて構成された Integral 特性は多数存在する [KW02, LWZ11, WZ11, YPK02, ZRHD08]．この手法では以下に示す 4 つの Integral Property を利用する．

- ALL ($\mathcal{A}$)：Every value appears the same number in the multiset.
- BALANCE ($\mathcal{B}$)：The XOR of all texts in the multiset is 0.
- CONSTANT ($\mathcal{C}$)：The value is fixed to a constant for all texts in the multiset.
- UNKNOWN ($\mathcal{U}$)：The multiset is indistinguishable from one of n-bit random values.

Knudsen と Wagner は Integral Property の伝搬を用いて AES の 4 段 Integral 特性を示した [KW02]．図 2.2 はその Integral 特性を示す．初め攻撃者は対角成分を連結した 32 ビット値が $\mathcal{A}$ となるような 2^{32} 個の選択平文を用意する．1 段暗号化した中間状態は左上の 1 バイトが $\mathcal{A}$ となり残りが定数となる集合が 2^{24} セット作られる状態となる．2 段暗号化した中間状態は左 1 列の各バイトが $\mathcal{A}$ となり残りが定数となる集合が 2^{24} セット，3 段暗号化した中間状態は各バイトが $\mathcal{A}$ となる集合が 2^{24} セット作られる状態となる．結果として 4 段暗号化した中間状態の和は全バイト 0 となることが分かる．

しばしば Integral 攻撃は Square 攻撃や Saturation 攻撃 [Luc01] と呼ばれるが，これら 3 つの解析手法は同一の解析手法であることに注意されたい．

代数次数の見積り

Integral 特性を探索するもう一つの手法は代数次数の見積りである [Lai94, Knu94]．この手法はしばしば高階差分攻撃と呼ばれる．ブロック暗号の代数次数が高々 D だったとすると，$D+1$ 階差分を取った平文に対応する暗号文の和は必ず 0 になる．差分や和を標数 2 の拡大体上で演算するとき，高階差分を取ることは平文の $D+1$ ビットを active にした 2^{D+1} 平文集合を用いた Integral 攻撃と一致する．

この手法の課題は代数次数の上界を求めることが極めて難しいことにある．文献 [THK99] では数式処理システム REDUCE を用いて代数次数を見積り MISTY1 [Mat97] の 7 階差分特性を示した．この手法は非常に正確な代数次数を見積もれる一方で階数の高い高階差分を正確に導出することは計算量が膨大となるため困難である．効率的に繰返し暗号の代数次数の上界を導出する手法は文献 [CV02] で提案された．この手法は Boura らによって改良され Keccak [DBPA11] と *Luffa* [CSW08] の Integral 特性が示された [BCC11]．しかしながらこの手法によって導出される上界は，依然として非常に緩いものとなっている．

Integral 攻撃と高階差分攻撃は定義上では異なる解析手法である．しかしながら実際に暗号解析の応用を考える場合，Integral 攻撃と高階差分攻撃は同一の解析手法とみなせる場合が多い．本レポートでは Integral 攻撃と高階差分攻撃が異なってくる例を取り扱わないため，Integral 攻撃と高階差分攻撃は同一の解析手法として考えることとする．

2.4 ブール関数

ブール関数は $\mathbb{F}_2^n$ な入力から $\mathbb{F}_2$ な出力を得る関数である．暗号においてブール関数に関する知識は非常に重要である．暗号では平文 p から暗号文 c を生成するが，暗号文 c の各ビットは平文 p の全ビットに影響される．すなわち暗号とはブール関数の集合として考えることができる．

関数 $f : \mathbb{F}_2^n \to \mathbb{F}_2$ をブール関数とする．ブール関数を表現する手法として Algebraic Normal Form が頻用される．

Definition 3 (Algebraic Normal Form (ANF))**.** Any $f : \mathbb{F}_2^n \to \mathbb{F}_2$ can be represented as

$$f(x) = \bigoplus_{u \in \mathbb{F}_2^n} a_u^f \left(\prod_{i=1}^{n} x[i]^{u[i]} \right) = \bigoplus_{u \in \mathbb{F}_2^n} a_u^f \pi_u(x),$$

where $a_u^f \in \mathbb{F}_2$ is a constant value depending on f and u.

ブール関数の最も重要な性質の一つに代数次数があり，それは 1 つの項に現れる $x[i]$ の個数の最大値である．したがってブール関数の代数次数が d であるとき $w(u) > d$ となる全ての a_u^f が 0 となる．

第3章　Division Property

本章では文献 [Tod15b] で提案された Division Property を解説する．Division Property は代数次数を利用できるよう Integral Property [KW02] を一般化したものである．

3.1　モチベーション

Division Property の導入モチベーションを示す．代数次数の上界が d である全単射な S-box を考える．初めに Integral Property が $\mathcal{A}$ である入力集合を準備する．このとき出力集合もまた Integral Property $\mathcal{A}$ を持つ．次に Integral Property が $\mathcal{B}$ である入力集合を準備する．このとき出力集合は Integral Property $\mathcal{U}$ を持つ．さらに任意の $d+1$ ビットを active にすることで構成される 2^{d+1} 個の選択テキストを用いた入力集合を用意すると，その出力集合は S-box の代数次数が d であるため Integral Property $\mathcal{B}$ を持つ．Integral Property の伝搬特性はこの特性を利用することができない．

より具体的な暗号を例に考える．例として AES の S-box が代数次数 2 である S-box に置き換えられた modified-AES を考える．この modified-AES の仕様は S-box の仕様変更以外は全てオリジナルな AES と同一のものとする．初めに Integral Property の伝搬を考える．Integral Property は暗号の非線形部分ではなく線形部分を主に利用して Integral 特性を探索する．したがって代数次数の変更は非線形部分の仕様変更であり，Integral Property の伝搬には一切影響を与えない．したがって Integral Property の伝搬により発見される Integral 特性はオリジナルと同一の 4 段特性である．次に代数次数の上界を考える．ラウンド関数の代数次数は 2 のため r 回繰返し暗号の代数次数は高々2^r である．したがって 6 回繰り返し暗号の代数次数は高々$2^6 = 64 < 128$ であり，2^{65} 選択平文を用いることで 6 段 Integral 特性を導出できる．これは Integral Property を用いた場合の Integral 特性よりも 2 段改良されている．上記の考察は

- Integral Property は主に線形部分を利用し非線形部分を利用できない．
- 代数次数見積りは主に非線形部分を利用し線形部分を利用できない．

という直感を導く．

Division Property の導入モチベーションは線形部分と非線形部分の両方を利用できる性質の発見である．そのために初めに $\mathcal{A}$ と $\mathcal{B}$ の性質を同様の表記法で再定義し，非線形部分を利用できるよう $\mathcal{A}$ と $\mathcal{B}$ の間に隠れている有用な性質を導出する．次に線形部分を利用できるよう暗号構造全体に対する Division Property を考える．

3.1.1 Integral Property の再定義

$\mathbb{X}$ を各要素が n ビットである多重集合とする．初めに $\mathbb{X}$ は Integral Property $\mathcal{A}$ を満足すると仮定する．すなわち n ビットの各値がそれぞれ同一回出現すると仮定する．初めに n ビットから任意の 1 ビットを選択し $\mathbb{X}$ の全要素に対して選択したビットの排他的論理和を考える．このとき $\mathbb{X}$ は Integral Property $\mathcal{A}$ を満足するため排他的論理和は必ず 0 となる．また n ビットから任意の $n-1$ ビットを選択し $\mathbb{X}$ の全要素に対して選択されたビットの AND 値の排他的論理和を考える．このとき排他的論理和は同様に必ず 0 となる．最後に n ビット全ビットを選択し $\mathbb{X}$ の全要素に対して全ビットの AND 値の排他的論理和を考える．このとき排他的論理和が 0 になるか 1 になるかは不定となる [1]．上述の特徴は 2 章で導入した Bit Product Function π_u を用いて以下のように整理できる．多重集合の全要素 $x \in \mathbb{X}$ に対して $\pi_u(x)$ のパリティ，すなわち $\bigoplus_{x\in\mathbb{X}} \pi_u(x)$ は，$w(u) < n$ を満足する全ての u において even であり，$u = 1^n$ のときのみ不定となる．

次に $\mathbb{X}$ は Integral Property $\mathcal{B}$ を満足すると仮定する．初めに n ビットから任意の 1 ビットを選択し $\mathbb{X}$ の全要素に対して選択したビットの排他的論理和を考える．このとき $\mathbb{X}$ は Integral Property $\mathcal{B}$ を満足するため排他的論理和は必ず 0 となる．次に n ビットから任意の 2 ビットを選択し $\mathbb{X}$ の全要素に対して選択されたビットの AND 値の排他的論理和を考える．このとき $\mathbb{X}$ が Integral Property $\mathcal{B}$ を持つという条件のみでは排他的論理和が 0 になるか 1 になるかは不定となる．上述の特徴は Bit Product Function π_u を用いて以下のように整理できる．多重集合の全要素 $x \in \mathbb{X}$ に対して $\pi_u(x)$ のパリティ，すなわち $\bigoplus_{x\in\mathbb{X}} \pi_u(x)$ は，$w(u) < 2$ を満足する全ての u において even であり，$w(u) \geq 2$ を満足する全ての u において不定となる．

3.2 Division Property の定義

上述した $\mathcal{A}$ と $\mathcal{B}$ の再定義では同一の表記法が用いられている．具体的には多重集合の全要素 $x \in \mathbb{X}$ に対して $\pi_u(x)$ のパリティに注目し，u の集合を

[1] もし $\mathbb{X}$ の全ての値が同偶数回出現するならば排他的論理和は 0 になる．一方もし $\mathbb{X}$ の全ての値が同奇数回出現するならば排他的論理和は 1 になる．本レポートにおける Integral Property $\mathcal{A}$ の定義は，各値が同数回出現する多重集合であるため，$\mathbb{X}$ が Integral Property $\mathcal{A}$ を持つという条件のみでは排他的論理和が 0 になるか 1 になるかは不定となる．

even パリティになる部分集合と不定パリティになる部分集合に $w(u)$ に着目することで分割する．これらを一般化することで Division Property は以下のように定義される．

Definition 4 (Division Property)**.** Let $\mathbb{X}$ be a multiset whose elements take a value of $\mathbb{F}_2^n$, and k takes a value between 0 and n. When the multiset $\mathbb{X}$ has the division property $\mathcal{D}_k^n$, it fulfils the following conditions:

$$\bigoplus_{x\in\mathbb{X}} \pi_u(x) = \begin{cases} unknown & \text{if w(u)} \geq \text{k,} \\ 0 & \text{otherwise.} \end{cases}$$

要するに Division Property は，$\bigoplus_{x\in\mathbb{X}} \pi_u(x)$ が不定か 0 かに注目して u の集合を分割することで定義される．

Example 1. $\mathbb{X}$ は各値が $\mathbb{F}_2^4$ 上の値を持つ多重集合である．例として以下に示す $\mathbb{X}$ を考える．

$$\mathbb{X} := \{\texttt{0x0}, \texttt{0x3}, \texttt{0x3}, \texttt{0x3}, \texttt{0x5}, \texttt{0x6}, \texttt{0x8}, \texttt{0xB}, \texttt{0xD}, \texttt{0xE}\}.$$

$\pi_u(x)$ のパリティは以下の表で整理される．

	0x0	0x3	0x3	0x3	0x5	0x6	0x8	0xB	0xD	0xE	$\sum \pi_u(x)$
	0000	0011	0011	0011	0101	0110	1000	1011	1101	1110	$(\bigoplus \pi_u(x))$
$u = 0000$	1	1	1	1	1	1	1	1	1	1	10 (0)
$u = 0001$	0	1	1	1	1	0	0	1	1	0	6 (0)
$u = 0010$	0	1	1	1	0	1	0	1	0	1	6 (0)
$u = 0011$	0	1	1	1	0	0	0	1	0	0	4 (0)
$u = 0100$	0	0	0	0	1	1	0	0	1	1	4 (0)
$u = 0101$	0	0	0	0	1	0	0	0	1	0	2 (0)
$u = 0110$	0	0	0	0	0	1	0	0	0	1	2 (0)
$u = 0111$	0	0	0	0	0	0	0	0	0	0	0 (0)
$u = 1000$	0	0	0	0	0	0	1	1	1	1	4 (0)
$u = 1001$	0	0	0	0	0	0	0	1	1	0	2 (0)
$u = 1010$	0	0	0	0	0	0	0	1	0	1	2 (0)
$u = 1011$	0	0	0	0	0	0	0	1	0	0	1 (1)
$u = 1100$	0	0	0	0	0	0	0	0	1	1	2 (0)
$u = 1101$	0	0	0	0	0	0	0	0	1	0	1 (1)
$u = 1110$	0	0	0	0	0	0	0	0	0	1	1 (1)
$u = 1111$	0	0	0	0	0	0	0	0	0	0	0 (0)

$w(u) < 3$ を満足する全ての u で $\bigoplus_{x\in\mathbb{X}} \pi_u(x) = 0$ より，$\mathbb{X}$ は Division Property $\mathcal{D}_3^4$ を満足することがわかる．

Integral Property $\mathcal{B}$ の定義は Division Property $\mathcal{D}_2^n$ の定義と同一である．また Integral Property $\mathcal{U}$ の定義は Division Property $\mathcal{D}_1^n$ の定義と同一であ

る．一方で Integral Property $\mathcal{A}$ の定義は Division Property $\mathcal{D}_n^n$ の定義とわずかに異なる．実際 Integral Property $\mathcal{A}$ を満足する集合は $\mathcal{D}_n^n$ を満足するが逆は成立しない．例に各値をそれぞれ奇数回ずつ持つ多重集合を考える．この多重集合は明らかに Integral Property $\mathcal{A}$ を満足しないが Division Property $\mathcal{D}_n^n$ を満足する．

3.2.1 Division Property の伝搬特性

$s : \mathbb{F}_2^n \to \mathbb{F}_2^m$ を代数次数の上界が d である S-box とする．$\mathbb{X}$ は S-box の入力集合であり各要素は $\mathbb{F}_2^n$ の値をとる．$\mathbb{Y}$ は S-box の出力集合であり各要素は全ての $x \in \mathbb{X}$ に対して $s(x)$ で計算される．$\mathbb{X}$ が $\mathcal{D}_k^n$ を満足するときの $\mathbb{Y}$ の Division Property を考える．

Proposition 1 (Division Property の伝搬特性)**.** Let s be a function (S-box) from n bits to n' bits, and the degree is d. Assuming that an input multiset $\mathbb{X}$ has the division property $\mathcal{D}_k^n$, the output multiset $\mathbb{Y}$ has $\mathcal{D}_{\lceil \frac{k}{d} \rceil}^m$. In addition, assuming that $n = m$ and the S-box is a permutation, the output multiset $\mathbb{Y}$ has $\mathcal{D}_n^n$ when the input multiset has $\mathcal{D}_n^n$.

Proof. Division Property では $\bigoplus_{x\in\mathbb{X}} \pi_u(x)$ が不定か 0 かにしたがって $u \in \mathbb{F}_2^n$ を 2 つに分割する．したがって出力集合の Division Property を考えるとき，$\bigoplus_{s(x)\in\mathbb{Y}} \pi_v(s(x))$ が不定か 0 かにしたがって $v \in \mathbb{F}_2^m$ を 2 つに分割することを考える．$\bigoplus_{s(x)\in\mathbb{Y}} \pi_v(s(x)) = \bigoplus_{x\in\mathbb{X}} (\pi_v \circ s)(x)$ より $\bigoplus_{x\in\mathbb{X}} (\pi_v \circ s)(x)$ は ANF を用いて

$$\bigoplus_{x\in\mathbb{X}} (\pi_v \circ s)(x) = \bigoplus_{x\in\mathbb{X}} \left(\bigoplus_{u\in\mathbb{F}_2^n} a_u^{\pi_v \circ s} \pi_u(x) \right) = \bigoplus_{u\in\mathbb{F}_2^n} a_u^{\pi_v \circ s} \left(\bigoplus_{x\in\mathbb{X}} \pi_u(x) \right)$$

と表せる．もし全ての $u \in \mathbb{F}_2^n$ において $a_u^{\pi_v \circ s} \left(\bigoplus_{x\in\mathbb{X}} \pi_u(x) \right) = 0$ ならば，全ての $x \in \mathbb{X}$ に対する $(\pi_v \circ s)(x)$ のパリティは even である．u のハミング重みが k 以下のとき $\mathbb{X}$ は $\mathcal{D}_k^n$ を満足することから $\bigoplus_{x\in\mathbb{X}} \pi_u(x) = 0$ となる．したがって，もし $w(u) \geq k$ を満足する全ての $u \in \mathbb{F}_2^n$ において $a_u^{\pi_v \circ s} = 0$ ならばパリティは even である．言い換えればパリティが不定となる必要条件は $a_u^{\pi_v \circ s} = 1$ となる $u \in \mathbb{F}_2^n$ が $w(u) \geq k$ の範囲に存在することである．

d' は関数 $(\pi_v \circ s)$ の代数次数とする．このとき $a_u^{\pi_v \circ s} = 1$ となる u は $w(u) \leq d'$ の範囲にのみ存在する．さらに d' は高々$\min\{n, w(v) \times d\}$ である．したがってパリティが不定となる必要条件は

$$k \leq w(u) \leq d' \leq \min\{n, w(v) \times d\}$$

を満足する $u \in \mathbb{F}_2^n$ が存在することである．すなわちパリティが不定となる必要条件は $\lceil \frac{k}{d} \rceil \leq w(v)$ であり，出力集合 $\mathbb{Y}$ は $\mathcal{D}_{\lceil \frac{k}{d} \rceil}^m$ を持つ．

次に入力集合が $\mathcal{D}_n^n$ であり S-box が置換であると仮定する．このときパリティが不定となる必要条件は $a_u^{\pi_v \circ s} = 1$ となる $u = 1^n$ が存在することである．$w(v) < n$ を満足するとき，ブール関数 $(\pi_v \circ s)$ の代数次数は高々$n-1$ より $a_{1^n}^{\pi_v \circ s}$ は常に 0 である．したがってパリティが不定となる必要条件は $v = 1^n$ であり，出力集合 $\mathbb{Y}$ は $\mathcal{D}_n^n$ を持つ． □

Example 2. 下記の 4 ビット S-box を考える．

x	0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xA	0xB	0xC	0xD	0xE	0xF
$s(x)$	0x8	0xC	0x0	0xB	0x9	0xD	0xE	0x5	0xA	0x1	0x2	0x6	0x4	0xF	0x3	0x7

この S-box は全単射であり代数次数は 2 である．この S-box に対する入力多重集合 $\mathbb{X}$ として

$$\mathbb{X} := \{\texttt{0x0}, \texttt{0x3}, \texttt{0x3}, \texttt{0x3}, \texttt{0x5}, \texttt{0x6}, \texttt{0x8}, \texttt{0xB}, \texttt{0xD}, \texttt{0xE}\},$$

を用意する．この多重集合は例1 で示したものと同一であり，この Division Property は $\mathcal{D}_3^4$ である．このとき出力多重集合は

$$\mathbb{Y} := \{\texttt{0x8}, \texttt{0xB}, \texttt{0xB}, \texttt{0xB}, \texttt{0xD}, \texttt{0xE}, \texttt{0xA}, \texttt{0x6}, \texttt{0xF}, \texttt{0x3}\},$$

となる．下表は $\pi_v(y)$ の和を示す．

	0x8	0xB	0xB	0xB	0xD	0xE	0xA	0x6	0xF	0x3	$\sum \pi_v(y)$
	1000	1011	1011	1011	1101	1110	1010	0110	1111	0011	$(\bigoplus \pi_v(y))$
$v = 0000$	1	1	1	1	1	1	1	1	1	1	10 (0)
$v = 0001$	0	1	1	1	1	0	0	0	1	1	6 (0)
$v = 0010$	0	1	1	1	0	1	1	1	1	1	8 (0)
$v = 0011$	0	1	1	1	0	0	0	0	1	1	5 (1)
$v = 0100$	0	0	0	0	1	1	0	1	1	0	4 (0)
$v = 0101$	0	0	0	0	1	0	0	0	1	0	2 (0)
$v = 0110$	0	0	0	0	0	1	0	1	1	0	3 (1)
$v = 0111$	0	0	0	0	0	0	0	0	1	0	1 (1)
$v = 1000$	1	1	1	1	1	1	1	0	1	0	8 (0)
$v = 1001$	0	1	1	1	1	0	0	0	1	0	5 (1)
$v = 1010$	0	1	1	1	0	1	1	0	1	0	6 (0)
$v = 1011$	0	1	1	1	0	0	0	0	1	0	4 (0)
$v = 1100$	0	0	0	0	1	1	0	0	1	0	3 (1)
$v = 1101$	0	0	0	0	1	0	0	0	1	0	2 (0)
$v = 1110$	0	0	0	0	0	1	0	0	1	0	2 (0)
$v = 1111$	0	0	0	0	0	0	0	0	1	0	1 (1)

$w(v) < 2$ を満足する全ての $v \in \mathbb{F}_2^4$ において $\bigoplus_{y \in \mathbb{Y}} \pi_v(y) = 0$ となる．したがって多重集合 $\mathbb{Y}$ は Division Property $\mathcal{D}_2^4$ を満足する．

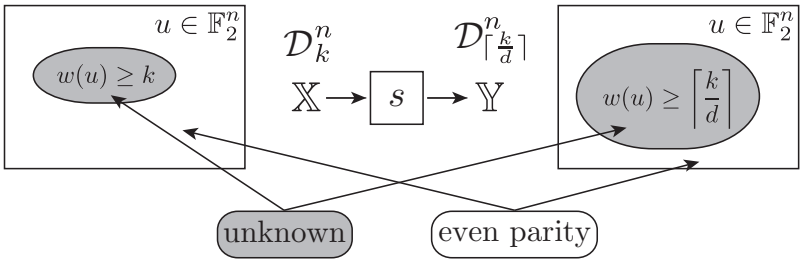


図 3.1: Propagation characteristic of division property

図 3.1 は Division Property の伝搬特性のイメージ図である．$\mathbb{X}$ および $\mathbb{Y}$ を入力多重集合と出力多重集合とする．初め $\bigoplus_{x\in\mathbb{X}} \pi_u(x)$ が不定となる u の要素数は少ない．しかしながら S-box を通過することで $\bigoplus_{x\in\mathbb{X}} \pi_u(s(x))$ が不定となる u の要素数は大きくなる．最終的に 0^n を除いた全ての u において $\bigoplus_{x\in\mathbb{X}} \pi_u(s(x))$ が不定となるとき，その集合は要素数が偶数個であるランダムな集合と識別不可能とみなす．

3.3 Vectorial Division Property

前節では要素が $\mathbb{F}_2^n$ の値をとる多重集合に注目し，その Division Property と伝搬特性を示した．このような多重集合は S-box や線形関数の入出力として用いられる．一方で実際の暗号はより複雑なデータ構造上で計算される．例に AES のラウンド関数の SubBytes を考える．SubBytes は 16 個の S-box が並列に並んでおり入出力は $(\mathbb{F}_2^8)^{16}$ の値をとる．本節では要素がベクトル化された多重集合の Division Property を定義し，複数の S-box を連結した非線形関数に対する伝搬特性を示す．

$\mathbb{X}$ は多重集合であり，各要素は $(\mathbb{F}_2^{n_1} \times \mathbb{F}_2^{n_2} \times \cdots \times \mathbb{F}_2^{n_m})$ 上の値をとるとする．Division Property が π_u を用いて多重集合を評価していたように，ベクトル化した Division Property は $\pi_{\vec{u}}$ を用いて多重集合を評価する．ここで $\vec{u}$ は $(\mathbb{F}_2^{n_1} \times \mathbb{F}_2^{n_2} \times \cdots \times \mathbb{F}_2^{n_m})$ 上の値をとる．

Definition 5 (Vectorial Division Property)**.** Let $\mathbb{X}$ be the multiset whose elements take a value of $(\mathbb{F}_2^{n_1} \times \mathbb{F}_2^{n_2} \times \cdots \mathbb{F}_2^{n_m})$, and $\vec{k}$ is an m-dimensional vector whose ith element takes a value between 0 and n_i. When the multiset $\mathbb{X}$ has the division property $\mathcal{D}^{n_1,n_2,\ldots,n_m}_{\vec{k}}$, the multiset fulfils the following conditions:

$$\bigoplus_{\vec{x}\in\mathbb{X}} \pi_{\vec{u}}(\vec{x}) = \begin{cases} unknown & \text{if } W(\vec{u}) \succeq \vec{k}, \\ 0 & \text{otherwise.} \end{cases}$$

本レポートでは要素が $(\mathbb{F}_2^n)^m$ である多重集合の Division Property を単純に

$\mathcal{D}_{\vec{k}}^{n^m}$ と表記する．図 3.2 に Division Property と Vectorial Division Property の違いを整理する．

3.3.1 Vectorial Division Property の伝搬特性

S-Layer を m 個の S-box が連結して構成される非線形関数とする．このとき i 番目の S-box のビット長を n_i とし代数次数を d_i とする．S-Layer の入力多重集合は Division Property $\mathcal{D}_{\vec{k}}^{n_1,n_2,\dots,n_m}$ を満足する仮定する．S-Layer の出力は $(x_1, x_2, \dots, x_m) \in \mathbb{X}$ に対して $S(\vec{x}) = (s_1(x_1), s_2(x_2), \dots, s_m(x_m))$ で計算され，その出力多重集合の Vectorial Division Property を考える．

Proposition 2 (Vectorial Division Property の伝搬特性)**.** Let S be a function that consists of m S-boxes, where the bit length and the algebraic degree of the ith S-box is n_i bits and d_i, respectively. The input and the output take a value of $(\mathbb{F}_2^{n_1} \times \mathbb{F}_2^{n_2} \times \cdots \times \mathbb{F}_2^{n_m})$, and $\mathbb{X}$ and $\mathbb{Y}$ denote the input multiset and the output multiset, respectively. Assuming that the multiset $\mathbb{X}$ has the division property $\mathcal{D}_{\vec{k}}^{n_1,n_2,\dots,n_m}$, the multiset $\mathbb{Y}$ has the division property $\mathcal{D}_{\vec{k}'}^{n_1,n_2,\dots,n_m}$, where $\vec{k}'$ is calculated as follows:

$$\vec{k}' = \left[\left\lceil \frac{k_1}{d_1} \right\rceil, \left\lceil \frac{k_2}{d_2} \right\rceil, \dots, \left\lceil \frac{k_m}{d_m} \right\rceil \right].$$

Here, when the ith S-box is bijective and $k_i = n_i$, k_i' is n_i not $\lceil n_i/d_i \rceil$.

Proof. 初めに 1 番目の S-box のみを適用し，要素が $[s_1(x_1), x_2, \dots, x_m]$ で表現される多重集合の Division Property を評価する．今，$\mathbb{X}$ は Division Property $\mathcal{D}_{\vec{k}}^{n_1,n_2,\dots,n_m}$ を満足すると仮定する．このとき，全ての $\vec{x} \in \mathbb{X}$ に対する $\pi_{\vec{v}}([s_1(x_1), x_2, \dots, x_m])$ のパリティは以下のように評価される．

$$\begin{aligned}
\bigoplus_{\vec{x}\in\mathbb{X}} \pi_{\vec{v}}([s_1(x_1), x_2, \dots, x_m]) &= \bigoplus_{\vec{x}\in\mathbb{X}} \left((\pi_{v_1} \circ s_1)(x_1) \times \prod_{i=2}^{m} \pi_{v_i}(x_i) \right) \\
&= \bigoplus_{\vec{x}\in\mathbb{X}} \left(\bigoplus_{u_1 \in \mathbb{F}_2^{n_1}} a_{u_1}^{(\pi_{v_1}\circ s_1)} \pi_{u_1}(x_1) \right) \left(\prod_{i=2}^{m} \pi_{v_i}(x_i) \right) \\
&= \bigoplus_{u_1 \in \mathbb{F}_2^{n_1}} \bigoplus_{\vec{x}\in\mathbb{X}} \left(a_{u_1}^{(\pi_{v_1}\circ s_1)} \pi_{u_1}(x_1) \times \prod_{i=2}^{m} \pi_{v_i}(x_i) \right) \\
&= \bigoplus_{u_1 \in \mathbb{F}_2^{n_1}} a_{u_1}^{(\pi_{v_1}\circ s_1)} \left(\bigoplus_{\vec{x}\in\mathbb{X}} \pi_{[u_1, v_2, v_3, \dots, v_m]}(\vec{x}) \right)
\end{aligned}$$

したがって全ての $u_1 \in \mathbb{F}_2^{n_1}$ に対して $a_{u_1}^{\pi_{v_1}\circ s_1} \left(\bigoplus_{x\in\mathbb{X}} \pi_{[u_1, v_2, v_3, \dots, v_m]}(x) \right)$ が 0 のとき，パリティは even になる．多重集合 $\mathbb{X}$ は Division Property $\mathcal{D}_{\vec{k}}^{n_1,n_2,\dots,n_m}$

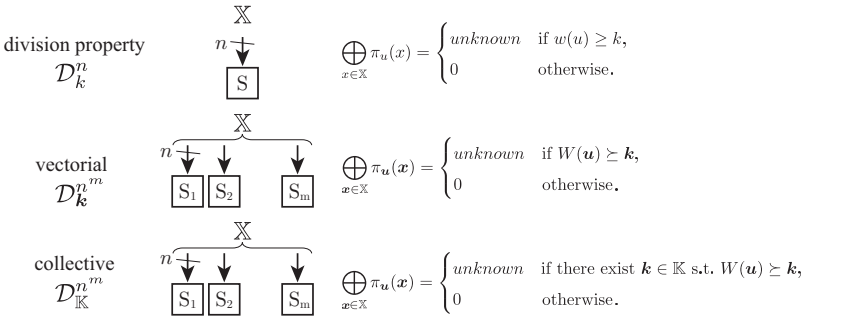


図 3.2: Division property, vectorial division property, and collective division property

を満足することから

$$\bigoplus_{\vec{x}\in\mathbb{X}} \pi_{\vec{u}}(\vec{x}) = \begin{cases} unknown & \text{if } W(\vec{u}) \succeq \vec{k} \\ 0 & \text{otherwise} \end{cases}$$

を満足する．したがって $W(\vec{u}) \succeq \vec{k}$ を満足する全ての $u_1 \in \mathbb{F}_2^{n_1}$ で $a_{u_1}^{\pi_{v_1} \circ s_1} = 0$ ならばパリティは even になる．言い換えると，パリティが不定となる必要条件は $a_{u_1}^{\pi_{v_1} \circ s_1} = 1$ となる $u_1 \in \mathbb{F}_2^{n_1}$ が $W(\vec{u}) \succeq \vec{k}$ の範囲に存在することである．Proposition 1 の証明と同様に，パリティが不定となる必要条件は $\lceil \frac{k_1}{d_1} \rceil < w(v_1)$ であり，出力多重集合 $\mathbb{Y}$ は $\mathcal{D}^{n_1,n_2,\ldots,n_m}_{[\lceil k_1/d_1 \rceil,k_2,k_3,\ldots,k_m}$ を満足する．

次に $\mathbb{X}$ が $\mathcal{D}^{n_1,n_2,\ldots,n_m}_{[n_1,k_2,k_3,\ldots,k_m]}$ を満足し S-box が全単射であると仮定する．Proposition 1 の証明と同様に，パリティが不定となる必要条件は $v = 1^{n_1}$ であり，出力多重集合 $\mathbb{Y}$ は $\mathcal{D}^{n_1,n_2,\ldots,n_m}_{[n_1,k_2,k_3,\ldots,k_m]}$ を満足する．

最終的に Proposition 2 は上記手順を全ての他の S-box に適用することで示される． □

3.4 Collective Division Property

Vectorial Division Property は要素が $(\mathbb{F}_2^{n_1} \times \mathbb{F}_2^{n_2} \times \cdots \mathbb{F}_2^{n_m})$ となる多重集合を評価できる．しかしながら Vectorial Division Property のみでは従来の Integral 攻撃と同等の解析を実現することは困難である．単純のため例として要素が $(\mathbb{F}_2^8)^2$ な値をとる集合 $\mathbb{X}$ を考える．ここで $\mathbb{X}$ の要素数は 256 であり，$\vec{x} \in \mathbb{X}$ の各要素は 0 から 255 まで独立に 1 回ずつとると仮定する．このような入力集合は Integral Property で言うところの $(\mathcal{A}, \mathcal{A})$ を満足し，この入力集合を S-Layer に適用して得られる出力集合も同様に $(\mathcal{A}, \mathcal{A})$ を満足する．今，このような集合の Division Property を考える．Division Property の本質は全ての $\vec{x} \in \mathbb{X}$ に対して $\pi_{\vec{u}}(\vec{x})$ のパリティが even になる $\vec{u}$ の部分集合と不定になる $\vec{u}$ の部分集合に分割することにあることから

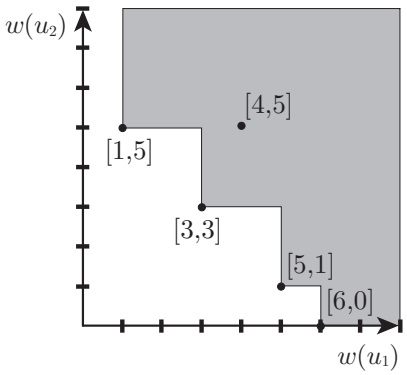


図 3.3: Division Property $\mathcal{D}^{8,8}_{\{[1,5],[3,3],[4,5],[5,1],[6,0]\}}$.

- $W(\vec{u}) \succeq [8,0]$ を満足する任意の $\vec{u}$ でパリティは不定.
- $W(\vec{u}) \succeq [0,8]$ を満足する任意の $\vec{u}$ でパリティは不定.
- $W(\vec{u}) \succeq [1,1]$ を満足する任意の $\vec{u}$ でパリティは不定.
- 上記以外の $\vec{u}$ でパリティは even.

と整理できる．すなわち，パリティが不定となる領域を単一のベクトルで表現することができない．Collective Division Property は複数のベクトルを収集することでパリティが不定となる領域を表現する．

Definition 6 (Collective Division Property)**.** Let $\mathbb{X}$ be the multiset whose elements take a value of $(\mathbb{F}_2^{n_1} \times \mathbb{F}_2^{n_2} \times \cdots \mathbb{F}_2^{n_m})$. Let $\mathbb{K}$ be a set whose elements take an m-dimensional vector whose ith element takes a value between 0 and n_i. When the multiset $\mathbb{X}$ has the division property $\mathcal{D}^{n_1,n_2,\ldots,n_m}_{\mathbb{K}}$, the multiset fulfils the following conditions:

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

$|\mathbb{K}| = 1$ である Collective Division Property は Vectorial Division Property と同一である．また Division Property $\mathcal{D}^{n_1,n_2,\ldots,n_m}_{\mathbb{K}}$ において $\vec{k} \succeq \vec{k}'$ を満足する $\vec{k} \in \mathbb{K}$ および $\vec{k}' \in \mathbb{K}$ が存在するとき，ベクトル $\vec{k}$ は冗長なため $\vec{k}$ を $\mathbb{K}$ から削除できる．入力多重集合 $\mathbb{X}$ が Division Property $\mathcal{D}^{n_1,n_2,\ldots,n_m}_{\mathbb{K}}$ を満足するとする．もし j 番目の要素が 1 で残りの全要素が 0 であるような $\vec{k}$ が $\mathbb{K}$ に含まれていないならば，$\bigoplus_{x\in\mathbb{X}} x_j$ は 0 になることが分かる．図 3.2 に Division Property，Vectorial Division Property，Collective Division Property の違いを整理する．

Example 3. $\mathbb{X}$ を要素が $(\mathbb{F}_2^8 \times \mathbb{F}_2^8)$ の値をとる多重集合とする．今 $\mathbb{X}$ が Division Property $\mathcal{D}^{8,8}_{\{[1,5],[3,3],[4,5],[5,1],[6,0]\}}$ を満足すると仮定する．図 3.3 はこの Division Property の概念図である．このとき，もし $[u_1, u_2]$ が図 3.3 の灰色部分から選択されるならば，$\bigoplus_{[x_1,x_2]\in\mathbb{X}} \pi_{[u_1,u_2]}([x_1, x_2])$ は不定となる．例に $\vec{u} = [\texttt{0x3F}, \texttt{0xFC}]$ を用いたとする．このとき $W(\vec{u}) = [6, 6]$ より $\bigoplus_{[x_1,x_2]\in\mathbb{X}} \pi_{[\texttt{0x3F},\texttt{0xFC}]}([x_1, x_2])$ は不定となる．一方で (u_1, u_2) が図 3.3 の白色部分から選択されるならば，$\bigoplus_{[x_1,x_2]\in\mathbb{X}} \pi_{[u_1,u_2]}([x_1, x_2])$ は 0 になる．このとき $\mathcal{D}^{8,8}_{\{[1,5],[3,3],[5,1],[6,0]\}}$ と $\mathcal{D}^{8,8}_{\{[1,5],[3,3],[4,5],[5,1],[6,0]\}}$ は不定領域が同一であることから，同一の Division Property と解釈できることに注意されたい．

3.4.1 Collective Division Property の伝搬特性

S-Layer の入力多重集合 $\mathbb{X}$ は Division Property $\mathcal{D}^{n_1,n_2,\ldots,n_m}_{\mathbb{K}}$ を満足する仮定する．入力 $(x_1, x_2, \ldots, x_m) \in \mathbb{X}$ に対する S-Layer の出力は $S(\vec{x}) = (s_1(x_1), s_2(x_2), \ldots, s_m(x_m))$ として計算される．このとき出力多重集合の Collective Division Property を考える．

Proposition 3 (Collective Division Property の伝搬特性)**.** Let S be a function that consists of m S-boxes, where the bit length and the algebraic degree of the ith S-box is n_i bits and d_i, respectively. The input and the output take a value of $(\mathbb{F}_2^{n_1} \times \mathbb{F}_2^{n_2} \times \cdots \times \mathbb{F}_2^{n_m})$, and $\mathbb{X}$ and $\mathbb{Y}$ denote the input multiset and the output multiset, respectively. Assuming that the multiset $\mathbb{X}$ has the division property $\mathcal{D}^{n_1,n_2,\ldots,n_m}_{\mathbb{K}}$, the multiset $\mathbb{Y}$ has the division property $\mathcal{D}^{n_1,n_2,\ldots,n_m}_{\mathbb{K}'}$, where $\mathbb{K}'$ is calculated as follows: First, $\mathbb{K}'$ is initialized to ϕ. Then, for all $\vec{k} \in \mathbb{K}$,

$$\mathbb{K}' = \mathbb{K}' \cup \left[\left\lceil \frac{k_1}{d_1} \right\rceil, \left\lceil \frac{k_2}{d_2} \right\rceil, \ldots, \left\lceil \frac{k_m}{d_m} \right\rceil \right],$$

is calculated. Here, when the ith S-box is bijective and $k_i = n_i$, k'_i is n_i not $\lceil n_i/d_i \rceil$.

Proof. 全ての $\vec{x} \in \mathbb{X}$ に対する $\pi_{\vec{v}}(S(\vec{x}))$ のパリティが不定となる $\vec{v}$ の部分集合を考える．このような部分集合は $\bigoplus_{\vec{x}\in\mathbb{X}} \pi_{\vec{u}}(\vec{x})$ が不定となる $\vec{u}$ からのみ得られることに注意されたい．したがって，全ての $\vec{k} \in \mathbb{K}$ に対して独立に Vectorial Division Property の伝搬を評価し，伝搬された全てのベクトルを収集することで，Collective Division Property の伝搬特性は得られる． □

3.5 単純な回路に対する伝搬特性

最後に暗号の線形関数部分に対する Division Property の伝搬特性を考える．本節では線形関数を構成する際に頻用される Copy，Split，Concatenation，

そして XOR に対する伝搬特性を示す.

3.5.1 Copy

入力 $x \in \mathbb{F}_2^n$ に対してコピー関数の出力は $[y_1, y_2] = [x, x]$ として計算される．$\mathbb{X}$ と $\mathbb{Y}$ をそれぞれ入出力多重集合とする．入力多重集合 $\mathbb{X}$ が Division Property $\mathcal{D}_k^n$ を満足するとき，出力多重集合 $\mathbb{Y}$ は Division Property $\mathcal{D}_{\mathbb{K}'}^{n,n}$ を満足し，ここで $\mathbb{K}'$ は以下のように計算される．初め $\mathbb{K}'$ は空集合 ϕ で初期化され，その後全ての i $(0 \le i \le k)$ に対して

$$\mathbb{K}' = \mathbb{K}' \cup [k-i, i],$$

が計算される.

Proof. $\mathbb{X}$ が Division Property $\mathcal{D}_k^n$ を満足すると仮定すると，$\bigoplus_{\vec{y}\in\mathbb{Y}} \pi_{\vec{v}}(\vec{y})$ は以下のように計算される.

$$\bigoplus_{\vec{y}\in\mathbb{Y}} \pi_{\vec{v}}(\vec{y}) = \bigoplus_{x\in\mathbb{X}} \pi_{[v_1,v_2]}([x,x]) = \bigoplus_{x\in\mathbb{X}} (\pi_{v_1}(x) \times \pi_{v_2}(x)) = \bigoplus_{x\in\mathbb{X}} (\pi_{v_1 \vee v_2}(x)) .$$

$\mathbb{X}$ は Division Property $\mathcal{D}_k^n$ を満足するため

$$\bigoplus_{x\in\mathbb{X}} \pi_u(x) = \begin{cases} unknown & w(u) \ge k \\ 0 & w(u) < k \end{cases}$$

を満足する．$w(v_1) + w(v_2) < k$ のとき $w(v_1 \vee v_2) \le w(v_1) + w(v_2) < k$ より $\bigoplus_{\vec{y}\in\mathbb{Y}} \pi_{\vec{v}}(\vec{y})$ は 0 になる．また $\bigoplus_{\vec{y}\in\mathbb{Y}} \pi_{\vec{v}}(\vec{y})$ が不定となる必要条件は $w(v_1) + w(v_2) \ge k$ である．したがって $\mathbb{Y}$ の Division Property は $\mathcal{D}_{\mathbb{K}'}^{n,n}$ であり，ここで $\mathbb{K}'$ の要素は下記ベクトルである.

$$[k-i, i] \quad \text{for } 0 \le i \le k.$$

□

3.5.2 Split

入力 $x \in \mathbb{F}_2^n$ に対して分割関数の出力は $y_1 \| y_2 = x$ として計算される．ここで $[y_1, y_2]$ は $(\mathbb{F}_2^{n_1} \times \mathbb{F}_2^{n-n_1})$ 上の値をとるとする．$\mathbb{X}$ と $\mathbb{Y}$ はそれぞれ入出力多重集合とする．入力多重集合 $\mathbb{X}$ が Division Property $\mathcal{D}_k^n$ を満足するとき，出力多重集合 $\mathbb{Y}$ は Division Property $\mathcal{D}_{\mathbb{K}'}^{n_1,n-n_1}$ を満足し，ここで $\mathbb{K}'$ は以下のように計算される．初め $\mathbb{K}'$ は空集合 ϕ で初期化され，その後全ての i $(0 \le i \le k)$ に対して

$$\mathbb{K}' = \mathbb{K}' \cup [k-i, i],$$

が計算される．ただし $(k-i) \le n_1$ かつ $i \le n - n_1$ となる.

Proof. $\mathbb{X}$ が Division Property $\mathcal{D}_k^n$ を満足すると仮定すると，$\bigoplus_{\vec{y}\in\mathbb{Y}} \pi_{\vec{v}}(\vec{y})$ は以下のように計算される．

$$\bigoplus_{\vec{y}\in\mathbb{Y}} \pi_{\vec{v}}(\vec{y}) = \bigoplus_{x\in\mathbb{X}} \pi_{[v_1\|v_2]}(x).$$

$\mathbb{X}$ は Division Property $\mathcal{D}_k^n$ を満足するため

$$\bigoplus_{x\in\mathbb{X}} \pi_u(x) = \begin{cases} unknown & w(u) \geq k \\ 0 & w(u) < k \end{cases}$$

を満足する．$w(v_1) + w(v_2) < k$ のとき $w(v_1\|v_2) = w(v_1) + w(v_2) < k$ より $\bigoplus_{\vec{y}\in\mathbb{Y}} \pi_{\vec{v}}(\vec{y})$ は 0 になる．また $\bigoplus_{\vec{y}\in\mathbb{Y}} \pi_{\vec{v}}(\vec{y})$ が不定となる必要条件は $w(v_1) + w(v_2) \geq k$ である．したがって $\mathbb{Y}$ の Division Property は $\mathcal{D}_{\mathbb{K}'}^{n_1,n-n_1}$ であり，ここで $\mathbb{K}'$ の要素は下記ベクトルである．

$$[k-i, i] \ \text{ for } 0 \leq i \leq k.$$

ここで y_1 は n_1 ビットより $k - i \leq n_1$，y_2 は $n - n_1$ ビットより $i \leq n - n_1$ となることに注意されたい． □

3.5.3 Concatenation

入力 $[x_1, x_2] \in (\mathbb{F}_2^{n_1} \times \mathbb{F}_2^{n_2})$ に対して連結関数の出力は $y = x_1\|x_2$ として計算される．$\mathbb{X}$ と $\mathbb{Y}$ をそれぞれ入出力多重集合とする．入力多重集合 $\mathbb{X}$ が Division Property $\mathcal{D}_{\mathbb{K}}^{n_1,n_2}$ を満足するとき，出力多重集合 $\mathbb{Y}$ は Division Property $\mathcal{D}_{k'}^{n_1+n_2}$ を満足し，ここで k' は

$$k' = \min_{[k_1,k_2]\in\mathbb{K}} \{k_1 + k_2\}$$

から計算される．

Proof. $\mathbb{X}$ が Division Property $\mathcal{D}_{\mathbb{K}}^{n_1,n_2}$ を満足すると仮定すると，$\bigoplus_{y\in\mathbb{Y}} \pi_v(y)$ は以下のように計算される．

$$\bigoplus_{y\in\mathbb{Y}} \pi_v(y) = \bigoplus_{[x_1,x_2]\in\mathbb{X}} \pi_{v_1\|v_2}(x_1\|x_2) = \bigoplus_{[x_1,x_2]\in\mathbb{X}} \pi_{[v_1,v_2]}([x_1, x_2]),$$

ここで $v = v_1\|v_2$ であり v_1 および v_2 はそれぞれ n_1 ビットと n_2 ビットである．入力多重集合 $\mathbb{X}$ は Division Property $\mathcal{D}_{\mathbb{K}}^{n_1,n_2}$ を満足することから

$$\bigoplus_{\vec{x}\in\mathbb{X}} \pi_{[u_1,u_2]}(\vec{x}) = \begin{cases} unknown & \text{if there exist } \vec{k} \in \mathbb{K} \text{ s.t. } W(\vec{u}) \succeq \vec{k} \\ 0 & \text{otherwise} \end{cases}$$

を満足する．$w(v) = w(v_1)+w(v_2) < \min_{\vec{k}\in\mathbb{K}}\{k_1+k_2\}$ なとき，$[w(v_1), w(v_2)] \succeq [k_1, k_2]$ を満足する $[k_1, k_2] \in \mathbb{K}$ は存在しない．したがって $\bigoplus_{y\in\mathbb{Y}} \pi_v(y)$ は 0 になる．また $\bigoplus_{y\in\mathbb{Y}} \pi_v(y)$ が不定となる必要条件は $w(v) \geq \min_{\vec{k}\in\mathbb{K}}\{k_1 + k_2\}$ である．したがって $\mathbb{Y}$ の Division Property は $\mathcal{D}^n_{k'}$ であり，ここで k' は $k' = \min_{\vec{k}\in\mathbb{K}}\{k_1 + k_2\}$ から計算される． □

3.5.4 XOR

入力 $[x_1, x_2] \in (\mathbb{F}_2^{n_1} \times \mathbb{F}_2^{n_2})$ に対して排他的論理和による圧縮関数の出力は $y = x_1 \oplus x_2$ として計算される．$\mathbb{X}$ と $\mathbb{Y}$ をそれぞれ入出力多重集合とする．入力多重集合 $\mathbb{X}$ が Division Property $\mathcal{D}^{n,n}_{\mathbb{K}}$ を満足するとき，出力多重集合 $\mathbb{Y}$ は Division Property $\mathcal{D}^n_{k'}$ を満足し，ここで k' は

$$k' = \min_{[k_1,k_2]\in\mathbb{K}}\{k_1 + k_2\}$$

から計算される．このとき k' が n より大きいとき，Division Property の伝搬は無効となる．すなわち全ての $v \in \mathbb{F}_2^n$ に対して $\oplus_{y\in\mathbb{Y}}\pi_v(y)$ は 0 となる．

Proof. Concatenation の伝搬特性と Proposition 1 を用いて証明する．今 F を $F(x_1\|x_2) = x_1 \oplus x_2$ として定義する．$\mathbb{X}$ が Division Property $\mathcal{D}^{n,n}_{\mathbb{K}}$ を満足すると仮定すると，要素が $(x_1\|x_2)$ である多重集合の Division Property は $\mathcal{D}^{2n}_{k'}$ であり，ここで k' は $k' = \min_{\vec{k}\in\mathbb{K}}\{k_1 + k_2\}$ から計算される．その後 F が適用されるが F の代数次数は 1 である．したがって $\mathbb{Y}$ の Division Property は $\mathcal{D}^n_{k'}$ である．ここで k' が n より大きいとき $\oplus_{y\in\mathbb{Y}}\pi_v(y)$ は全ての $v \in \mathbb{F}_2^n$ において 0 となることに注意されたい． □

第4章　Feistel構造に対するIntegral攻撃

本章では Division Property を用いて Feistel 構造の Integral 特性を探索する．

4.1　Feistel構造

Feistel 構造はブロック暗号を設計する際に頻用される暗号構造の一つである．n ビットブロック暗号が Feistel 構造を用いて設計されるとき，ラウンド関数の入出力は 2 つの $(n/2)$ ビット値で表現される．また $(n/2)$ ビット非線形関数 F がラウンド関数で使用され，本レポートではこの関数を F 関数と呼ぶ．ラウンド関数の入力を (w_1, w_2) とすると，出力 (z_1, z_2) は $(z_1, z_2) = (F(w_1) \oplus w_2, w_1)$ のように計算される．本レポートでは以下に定義する (ℓ, d)-Feistel に対する Integral 攻撃を考える．

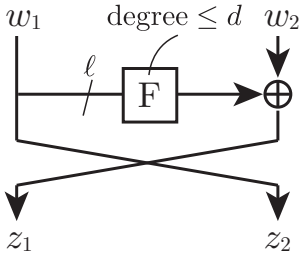


図 4.1: (ℓ, d)-Feistel

Definition 7 ((ℓ, d)-Feistel)．F 関数が代数次数 d 以下の ℓ ビット非線形関数のとき，この Feistel 構造を (ℓ, d)-Feistel と呼ぶ．

図 4.1 は (ℓ, d)-Feistel のラウンド関数を示す．Feistel 構造を採用している全てのブロック暗号は (ℓ, d)-Feistel と見なすことができ，例に DES [U.S77] は (32,5)-Feistel，Camellia [AIK+00] は (64,7)-Feistel，Simon $2n$ [BSS+13] は $(n, 2)$-Feistel と見なすことができる．

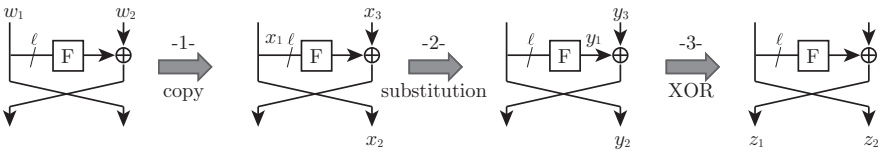


図 4.2: Propagation characteristic for (ℓ, d)-Feistel

4.2 (ℓ, d)-Feistel に対する伝搬特性

(ℓ, d)-Feistel に対する Division Property の伝搬特性を考える．図 4.2 に Feistel 構造の各操作を示す．初めに F 関数の入力が左半分のデータをコピーすることで作られる．次に F 関数が適用される．最後に F 関数の出力と右半分のデータが排他的論理和され，2 つのデータがスワップされ次のラウンドの入力となる．

- **copy** $(w_1, w_2) \in \mathbb{W}$ を入力として，ラウンド関数は初め $(x_1, x_2, x_3) = (w_1, w_1, w_2)$ を作成する．入力集合 $\mathbb{W}$ が Division Property $\mathcal{D}^{\ell^2}_{\mathbb{K}}$ を持つと仮定すると，出力集合 $\mathbb{X}$ は Division Property $\mathcal{D}^{\ell^3}_{\mathbb{K}'}$ を持ち，ここで $\mathbb{K}'$ は以下の手順で計算される．初め $\mathbb{K}'$ は空集合 ϕ で初期化され，次に全ての i $(i = 0, 1, \ldots, k_1)$ と 全ての $\vec{k} \in \mathbb{K}$ に対して，$\mathbb{K}' = \mathbb{K}' \cup [k_1 - i, i, k_2]$ が計算される．

- **substitution** x_1 に代数次数 d である F 関数が適用される．入力集合 $\mathbb{W}$ が Division Property $\mathcal{D}^{\ell^3}_{\mathbb{K}}$ を持つと仮定すると，出力集合 $\mathbb{X}$ は Division Property $\mathcal{D}^{\ell^3}_{\mathbb{K}'}$ を持ち，ここで $\mathbb{K}'$ の要素は全ての $\vec{k} \in \mathbb{K}$ に対して $(k'_1, k'_2, k'_3) = (\lceil k_1/d \rceil, k_2, k_3)$ で計算される．また F 関数が置換のとき，$k_1 = \ell$ とすると $k'_1 = \ell$ となることに注意されたい．

- **XOR** y_1 と y_3 を排他的論理和し，$(z_1, z_2) = (y_1 \oplus y_3, y_2)$ を作成する．入力集合 $\mathbb{Y}$ が Division Property $\mathcal{D}^{\ell^3}_{\mathbb{K}}$ を持つと仮定すると，出力集合 $\mathbb{Z}$ は Division Property $\mathcal{D}^{\ell^2}_{\mathbb{K}'}$ を持ち，ここで $\mathbb{K}'$ の要素は $k_1 + k_3 \leq \ell$ を満足する全ての $\vec{k} \in \mathbb{K}$ に対して $(k'_1, k'_2) = (k_1 + k_3, k_2)$ で計算される．

4.3 (ℓ, d)-Feistel の Integral 特性探索アルゴリズム

前節で示した伝搬特性をもとに (ℓ, d)-Feistel に対する Integral 特性探索アルゴリズムを考える．(ℓ, d)-Feistel の入力集合として，左半分の k_1 ビットと右半分の k_2 ビットを active にした $2^{k_1+k_2}$ 個の選択平文を用意する．この入力集合は Division Property $\mathcal{D}^{\ell^2}_{\{[k_1,k_2]\}}$ を満足する．Algorithm 1 は (k_1, k_2) を入力として (ℓ, d)-Feistel の Integral 特性の段数を導出する．Algorithm 1 は F 関数を置換に制限していない．ここで F 関数を置換に制限する．このとき

Algorithm 1 Path search for integral characteristics on (ℓ, d)-Feistel

1: **procedure** `FeistelFuncEval`(ℓ, d, k_1, k_2)
2: $\quad \mathbb{K} \Leftarrow \phi$
3: $\quad$ **for** $X = 0$ to k_1 **do**
4: $\quad\quad L \Leftarrow k_2 + \lceil X/d \rceil$
5: $\quad\quad$ **if** $L \leq \ell$ **then**
6: $\quad\quad\quad \mathbb{K} \Leftarrow \mathbb{K} \cup (L, k_1 - X)$
7: $\quad\quad$ **end if**
8: $\quad$ **end for**
9: $\quad$ **return** $\mathbb{K}$
10: **end procedure**

11: **procedure** `IntegralPathSearch`$(\ell, d, r = 0, k_1, k_2)$
12: $\quad \mathbb{K} \Leftarrow$ `FeistelFuncEval`(ℓ, d, k_1, k_2)
13: $\quad D \Leftarrow \max_{\vec{k} \in \mathbb{K}} \{k_1 + k_2\}$
14: $\quad$ **while** $1 < D$ **do**
15: $\quad\quad r \Leftarrow r + 1$
16: $\quad\quad \mathbb{K}' \Leftarrow \phi$
17: $\quad\quad$ **for all** $\vec{k} \in \mathbb{K}$ **do**
18: $\quad\quad\quad \mathbb{K}' \Leftarrow \mathbb{K}' \cup$ `FeistelFuncEval`(ℓ, d, k_1, k_2)
19: $\quad\quad$ **end for**
20: $\quad\quad \mathbb{K} \Leftarrow$ `SizeReduce`$(\mathbb{K}')$
21: $\quad\quad D \Leftarrow \max_{\vec{k} \in \mathbb{K}} \{k_1 + k_2\}$
22: $\quad$ **end while**
23: $\quad$ **return** r
24: **end procedure**

$X = \ell$ の場合 L は $k_2 + \ell$ になる (Algorithm 1 の 4 行目参照)．Algorithm 1 は `SizeReduce` を呼び出しているが，これは $W(\vec{k}) \succeq W(\vec{k}')$ を満足する $\vec{k} \in \mathbb{K}'$ と $\vec{k}' \in \mathbb{K}$ が存在するとき，$\vec{k}$ を $\mathbb{K}$ から削除する関数である．

4.3.1 比較検討

表 4.1 に $(32, 5)$-Feistel および $(64, 7)$-Feistel の r 段 Integral 特性を構成するのに必要な選択平文数を整理する．ここで非全単射 F 関数を用いた $(32, 5)$-Feistel は DES [U.S77] を，全単射 F 関数を用いた $(64, 7)$-Feistel は Camellia [AIK+00] をそれぞれ意識したパラメータである．2^D 選択平文を用いた (ℓ, d)-Feistel の Integral 特性を探索する際，入力の (k_1, k_2) として以下のパラ

表 4.1: The number of chosen plaintexts to construct r-round integral characteristics on $(32, 5)$- and $(64, 7)$-Feistel.

Target [Application]	F-function	$\log_2$(#texts)						Method
		$r = 4$	$r = 5$	$r = 6$	$r = 7$	$r = 8$	$r = 9$	
$(32, 5)$-Feistel [DES]	non-bijection	26	51	62	-	-	-	our
		26	-	-	-	-	-	degree
$(64, 7)$-Feistel [Camellia]	bijection	50	98	124	-	-	-	our
		50	-	-	-	-	-	degree
		64	-	-	-	-	-	integral

メータを用いた．

$$(k_1, k_2) = \begin{cases} (D - \ell, \ell) & \text{for } \ell \leq D, \\ (0, D) & \text{for } D < \ell. \end{cases}$$

Division Property を用いた手法と比較するために Integral Property の伝搬を用いた場合と代数次数の見積りを行う場合の 2 通りを考える．初めに Integral Property を用いる方法を考える．Integral Property は非線形関数の全単射性を利用するため F 関数が全単射でないとき有効な Integral 特性を導出しない．したがって Integral Property は F 関数が全単射なときのみ考慮する．次に代数次数の見積りを考える．SPN 構造では文献 [BCC11] のように代数次数の上界を理論的に抑える理論が存在するが，Feistel 構造に関しては改良された上界は知られていない．そこで以下に示す自然な上界を利用する．初めに平文の左半分を固定する．このとき r 段 (ℓ, d)-Feistel において，暗号文の右半分は平文の右半分に対して次数 d^{r-2} の非線形関数を通過したものとして表現できる．平文の右半分は ℓ ビットであるため，代数次数を利用する手法では $2^{d^{r-2}+1} < 2^{\ell}$ を満足する範囲で Integral 特性を構成できる．

結果として，調査した範囲では，全ての Integral 特性において Division Property は既存の手法よりも良い Integral 特性を発見した．一方で今回示す Integral 特性はあくまで (ℓ, d)-Feistel に対する汎用的なものであることに注意されたい．例に Camellia の Integral 特性に関しては，より効率の良い Integral 特性が既に知られており，これは Camellia の具体的な仕様を利用した Integral 特性である [YPK02]．$(64, 7)$-Feistel が 6 段 Integral 特性を持つとは，仮に Camellia の F 関数を代数次数 7 の任意の全単射非線形関数に置き換えたとしても，6 段 Integral 特性は必ず存在することを意味する．

4.3.2 Simon Family に対する Integral 特性

National Security Agency (NSA) が近年提案した軽量暗号に Simon がある [BSS+13]．本章で示した (ℓ, d)-Feistel に対する汎用解析を Simon に適用す

表 4.2: The number of chosen plaintexts to construct r-round integral characteristics on the SIMON family, where the F-function is not bijective.

Target	$\log_2$(#texts)								Method
[Application]	$r=6$	$r=7$	$r=8$	$r=9$	$r=10$	$r=11$	$r=12$	$r=13$	
$(16,2)$-Feistel	17	25	29	31	-	-	-	-	our
[SIMON 32]	-	-	-	-	-	-	-	-	degree
$(24,2)$-Feistel	17	29	39	44	46	47	-	-	our
[SIMON 48]	17	-	-	-	-	-	-	-	degree
$(32,2)$-Feistel	17	33	49	57	61	63	-	-	our
[SIMON 64]	17	-	-	-	-	-	-	-	degree
$(48,2)$-Feistel	17	33	57	77	87	92	94	95	our
[SIMON 96]	17	33	-	-	-	-	-	-	degree
$(64,2)$-Feistel	17	33	65	97	113	121	125	127	our
[SIMON 128]	17	33	-	-	-	-	-	-	degree

る．SIMON の F 関数は非常に軽量な構造を持つが，非全単射な関数であり従来の手法では Integral 特性を探索することは困難だった．Division Property は理論的に SIMON 32, 48, 64, 96, 128 が少なくとも 9, 11, 11, 13, 13 段 Integral 特性をそれぞれ持つことを示す．表 4.2 に Division Property による Integral 特性と自然な手法による代数次数見積りによる Integral 特性の比較を示す．

確かに Division Property は非自明な Integral 特性を示したが，Wang らは SIMON 32 が 15 段 Integral 特性をもつことを実験的に予測している [WLV+14]．SIMON 32 はラウンド鍵が F 関数後に適用されるため，Division Property による $(32,2)$-Feistel の 9 段 Integral 特性は 10 段 Integral 特性へ拡張可能である．しかしながら依然として 5 段の差が存在することが分かる．この 5 段の差は SIMON 32 の F 関数が任意の代数次数 2 の非線形関数ではなく，非常に軽量な非線形関数となっていることに起因するものと考えられる．

4.4 (ℓ, d)-Feistel に対する Integral 特性の整理

表 4.3 に (ℓ, d)-Feistel の Integral 特性を整理する．

表 4.3: The number of required chosen plaintexts to construct r-round integral distinguishers on (ℓ, d)-Feistel.

Target	F-function	$\log_2$(#texts)									Examples
		$r=6$	$r=7$	$r=8$	$r=9$	$r=10$	$r=11$	$r=12$	$r=13$	$r=14$	
$(16,2)$	non-bijection	17	25	29	31	-	-	-	-	-	SIMON 32 [BSS+13]
	bijection	16	23	28	30	31	-	-	-	-	
$(24,2)$	non-bijection	17	29	39	44	46	47	-	-	-	SIMON 48 [BSS+13]
	bijection	17	27	38	43	46	47	-	-	-	
$(32,2)$	non-bijection	17	33	49	57	61	63	-	-	-	SIMON 64 [BSS+13]
	bijection	17	32	47	56	60	62	63	-	-	
$(48,2)$	non-bijection	17	33	57	77	87	92	94	95	-	SIMON 96 [BSS+13]
	bijection	17	33	55	76	86	91	94	95	-	
$(64,2)$	non-bijection	17	33	65	97	113	121	125	127	-	SIMON 128 [BSS+13]
	bijection	17	33	64	95	112	120	124	126	127	

Target	F-function	$\log_2$(#texts)									Examples
		$r=3$	$r=4$	$r=5$	$r=6$	$r=7$	$r=8$	$r=9$	$r=10$	$r=11$	
$(32,5)$	non-bijection	6	26	51	62	-	-	-	-	-	DES [U.S77]
	bijection	6	26	46	61	-	-	-	-	-	
$(48,5)$	non-bijection	6	26	64	90	95	-	-	-	-	
	bijection	6	26	59	89	95	-	-	-	-	
$(64,5)$	non-bijection	6	26	77	118	126	-	-	-	-	
	bijection	6	26	72	117	126	-	-	-	-	

Target	F-function	$\log_2$(#texts)									Examples
		$r=3$	$r=4$	$r=5$	$r=6$	$r=7$	$r=8$	$r=9$	$r=10$	$r=11$	
$(32,7)$	non-bijection	8	35	60	-	-	-	-	-	-	
	bijection	8	32	59	-	-	-	-	-	-	
$(48,7)$	non-bijection	8	49	90	-	-	-	-	-	-	
	bijection	8	48	84	95	-	-	-	-	-	
$(64,7)$	non-bijection	8	50	104	125	-	-	-	-	-	
	bijection	8	50	98	124	-	-	-	-	-	Camellia [AIK+00]

Target	F-function	$\log_2$(#texts)									Examples
		$r=3$	$r=4$	$r=5$	$r=6$	$r=7$	$r=8$	$r=9$	$r=10$	$r=11$	
$(32,31)$	non-bijection	32	62	-	-	-	-	-	-	-	
	bijection	32	32	63	-	-	-	-	-	-	
$(48,47)$	non-bijection	48	94	-	-	-	-	-	-	-	
	bijection	48	48	95	-	-	-	-	-	-	
$(64,63)$	non-bijection	64	126	-	-	-	-	-	-	-	
	bijection	64	64	127	-	-	-	-	-	-	
$(32,32)$	non-bijection	33	-	-	-	-	-	-	-	-	
$(48,48)$	non-bijection	49	-	-	-	-	-	-	-	-	
$(64,64)$	non-bijection	65	-	-	-	-	-	-	-	-	

第5章　SPN構造に対するIntegral攻撃

本章ではDivision Propertyを用いてSPN構造のIntegral特性を探索する．

5.1　Substitute-Permutation Network

Substitute-Permutation Network (SPN構造) はFeistel構造と並んでブロック暗号を設計する際に頻用される暗号構造の一つである．SPN構造のラウンド関数はS-LayerとP-Layerで構成され，このラウンド関数を繰り返すことでブロック暗号が設計される．本レポートでは以下に定義する (ℓ, d, m)-SPNのIntegral特性を考える．

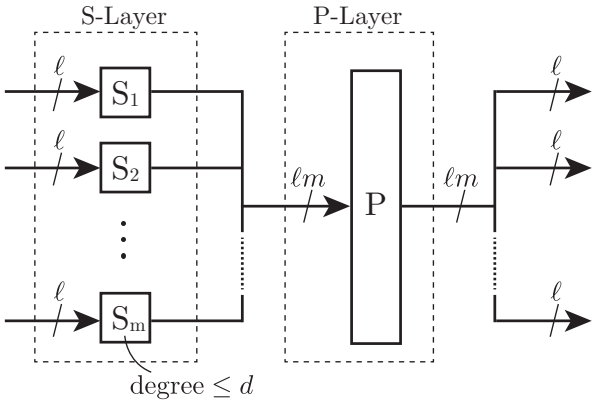


図 5.1: (ℓ, d, m)-SPN

Definition 8 ((ℓ, d, m)-SPN)．S-Layerは代数次数が d である ℓ ビット全単射S-boxが m 個並列に並ぶ構造を有する．P-Layerはこれらの S-box の出力を線形関数で撹拌する．このSPN構造を (ℓ, d, m)-SPNと呼ぶ．

図5.1は (ℓ, d, m)-SPNのラウンド関数を示す．(ℓ, d, m)-SPNを採用しているブロック暗号は多数存在し，有名な例としてAES [U.S01] は(8,7,16)-SPN，PRESENT [BKL+07] は(4,3,16)-SPN，Serpent [ABK98] は $(4, 3, 32)$-SPNを

それぞれ採用している．またハッシュ関数 Keccak [DBPA11] の内部で利用される Keccak-f [DBPA11] は $(5, 2, 320)$-SPN を採用している．

5.2 (ℓ, d, m)-SPN に対する伝搬特性

(ℓ, d, m)-SPN に対する Division Property の伝搬特性を考える．初め S-Layer に対する伝搬特性を評価する．次に P-Layer が適用されるが，S-Layer の出力は $(\mathbb{F}_2^\ell)^m$ の値を持つのに対し，P-Layer の入力は $\mathbb{F}_2^{\ell m}$ の値を持つ．したがって Concatenation の伝搬特性を利用して $\mathcal{D}_{\mathbb{K}}^{\ell^m}$ から $\mathcal{D}_{\mathbb{K}}^{\ell m}$ へ Division Property を変換し，その後 P-Layer を適用する．P-Layer 適用後，再び S-Layer が適用されるため，Split の伝搬特性を利用して $\mathcal{D}_{\mathbb{K}}^{\ell m}$ から $\mathcal{D}_{\mathbb{K}}^{\ell^m}$ へ Division Property を再変換する．

- **S-Layer** S-Layer の入力が Division Property $\mathcal{D}_{\mathbb{K}}^{\ell^m}$ を満足すると仮定する．S-Layer は m 個の代数次数 d である ℓ ビット S-box で構成されるため，Proposition 3 を用いて伝搬特性を評価できる．S-Layer の出力が Division Property $\mathcal{D}_{\mathbb{K}'}^{\ell^m}$ を持つと仮定すると，$\mathbb{K}'$ は以下の手順で計算される．初め $\mathbb{K}'$ は空集合 ϕ で初期化され，全ての $\vec{k} \in \mathbb{K}$ に対して $\mathbb{K}' = \mathbb{K}' \cup [k'_1, k'_2, \ldots, k'_m]$ が計算される．ここで $k_i < \ell$ なとき $k'_i = \lceil k_i/d \rceil$ となり，$k_i = \ell$ なとき $k'_i = \ell$ となる．

- **Conversion form S-Layer to P-Layer** S-Layer の出力集合 $\mathbb{X}$ の各要素は $(\mathbb{F}_2^\ell)^m$ 上の値をとり Division Property $\mathcal{D}_{\mathbb{K}}^{\ell^m}$ を満足すると仮定する．$\mathbb{Y}$ は P-Layer の入力集合であり，各要素は $\mathbb{F}_2^{\ell m}$ の値をとる．S-Layer の出力から P-Layer の入力への変換は単純なビット連結で実現され，すなわち $(x_1, x_2, \ldots, x_m) \in \mathbb{X}$ に対して $y \in \mathbb{Y}$ は $y = (x_1 \| x_2 \| \cdots \| x_m)$ で計算される．Concatenation の伝搬特性より，$\mathbb{Y}$ は Division Property $\mathcal{D}_{k'}^{\ell m}$ を満足し，ここで $k' = \min_{\vec{k} \in \mathbb{K}} \sum_{i=1}^m k_i$ となる．

- **P-Layer** P-Layer は (ℓm) ビット線形関数で実現される．線形関数の代数次数は 1 であるため，Division Property は変化しない．

- **Conversion form P-Layer to S-Layer** P-Layer の出力集合 $\mathbb{X}$ の各要素は $\mathbb{F}_2^{\ell m}$ の値をとり Division Property $\mathcal{D}_{\mathbb{K}}^{\ell m}$ を満足すると仮定する．$\mathbb{Y}$ は次ラウンドの S-Layer の入力集合であり，各要素は $(\mathbb{F}_2^\ell)^m$ の値をとる．P-Layer の出力から S-Layer の入力への変換はビット分割で実現され，すなわち $x \in \mathbb{X}$ に対して $(y_1, y_2, \ldots, y_m) \in \mathbb{Y}$ は $(y_1 \| y_2 \| \cdots \| y_m) = x$ で計算される．Split の伝搬特性より，$\mathbb{Y}$ は Division Property $\mathcal{D}_{\mathbb{K}'}^{\ell^m}$ を満足し，ここで $\mathbb{K}'$ は $\sum_{i=1}^m k'_i = k$ を満足する全ての $\vec{k'}$ の集合である．

P-Layer の出力集合が Division Property $\mathcal{D}_k^{\ell m}$ を満足するとき，次段の P-Layer の出力集合の Division Property $\mathcal{D}_{k'}^{\ell m}$ を考える．

初めに $k > (\ell-1)m$ のときを考える．このとき S-Layer の入力集合の Division Property を $\mathcal{D}_{\mathbb{K}}^{\ell^m}$ とすると，$\mathbb{K}$ には $(m-\ell m+k)$ 要素が ℓ であり $(\ell m-k)$ 要素が $\ell-1$ であるベクトルのみが含まれる．S-Layer を通過すると ℓ は ℓ に，$\ell-1$ は $\lceil\frac{\ell-1}{d}\rceil$ になることから，$k'=\lceil\frac{\ell-1}{d}\rceil(\ell m-k)+\ell(m-\ell m+k)$ となる．

次に $(\ell-1)m \geq k > \lfloor\frac{\ell-1}{d}\rfloor md$ のときを考える．(ℓ,d,m)-SPN の伝搬特性より S-Layer による Division Property の劣化が最大化されるときのみ考えればよい．このとき S-Layer の入力集合の Division Property を $\mathcal{D}_{\mathbb{K}}^{\ell^m}$ とすると，$\vec{k} \in \mathbb{K}$ の各要素が $\lfloor\frac{\ell-1}{d}\rfloor d$ を上回ると各 S-box あたりの Division Property の劣化が最大化できないことが分かる．したがって初めに各要素が $\lfloor\frac{\ell-1}{d}\rfloor d$ になるよう k を分配する．すると残りは $k-\lfloor\frac{\ell-1}{d}\rfloor dm$ となり，これを再び各要素に分配する．このとき各要素が ℓ になると S-box の全単射性より Division Property は一切劣化しない．したがって各要素あたり $\ell-1-\lfloor\frac{\ell-1}{d}\rfloor d$ を追加で割り当てるとき劣化が最大化される．便宜上 $\alpha = k-\lfloor\frac{\ell-1}{d}\rfloor dm$, $\beta=\ell-1-\lfloor\frac{\ell-1}{d}\rfloor d$ とすると，$k'=\lfloor\frac{\ell-1}{d}\rfloor m+\lceil\frac{\alpha}{\beta}\rceil$ となる．また k の値に関わらず $(\ell-1)=\lfloor\frac{\ell-1}{d}\rfloor d$ を満足する場合，この場合分けを考慮する必要はないことに注意されたい．

最後に $\lfloor\frac{\ell-1}{d}\rfloor md \geq k$ のときを考える．このとき (ℓ,d,m)-SPN のラウンド関数を単純に代数次数 d である一つの (ℓm) ビット S-box とみなして伝搬特性を評価する．したがって $k'=\lceil\frac{k}{d}\rceil$ となる．

結果として (ℓ,d,m)-SPN に対する Division Property の伝搬特性は以下のように表せる．

$$k' = \begin{cases} \lceil\frac{\ell-1}{d}\rceil(\ell m-k)+\ell(m-\ell m+k) & \text{if } k>(\ell-1)m \\ \lfloor\frac{\ell-1}{d}\rfloor m+\lceil\frac{\alpha}{\beta}\rceil & \text{if } (\ell-1)m\geq k>\lfloor\frac{\ell-1}{d}\rfloor md \\ \lceil\frac{k}{d}\rceil & \text{if } \lfloor\frac{\ell-1}{d}\rfloor md \geq k \end{cases}$$

5.3 (ℓ,d,m)-SPN の Integral 特性探索アルゴリズム

前節で示した伝搬特性をもとに (ℓ,d,m)-SPN に対する Integral 特性探索アルゴリズムを考える．(ℓ,d,m)-SPN の入力集合として，i 番目の S-box の入力 ℓ ビットのうち k_i ビットを active にした $2^{\sum_{i=1}^{m}k_i}$ 個の選択平文を用意する．この入力集合は Division Property $\mathcal{D}_{\vec{k}}^{\ell^m}$ を満足する．Algorithm 2 は $(k_1,k_2,\ldots,k_m)$ を入力として (ℓ,d,m)-SPN の Integral 特性の段数を導出する．

Algorithm 2 Path search for integral characteristics on (ℓ, d, m)-SPN

procedure `IntegralPathSearch`$(\ell, d, m, r = 0, k_1, k_2, \ldots, k_m)$
  if $k_i < \ell$ **then** $k_i \Leftarrow \lceil k_i/d \rceil$ ▷ 1-st round S-Layer
  end if
  $k \Leftarrow \sum_{i=1}^{m} k_i$ ▷ 1-st round P-Layer
  while $1 < k$ **do**
    $r \Leftarrow r + 1$
    if $k > (\ell - 1)m$ **then**
      $k \Leftarrow \lceil \frac{\ell-1}{d} \rceil (\ell m - k) + \ell(m - \ell m + k)$
    else if $k > \lfloor \frac{\ell-1}{d} \rfloor md$ **then**
      $\alpha \Leftarrow k - \lfloor \frac{\ell-1}{d} \rfloor dm$
      $\beta \Leftarrow \ell - 1 - \lfloor \frac{\ell-1}{d} \rfloor d$
      $k \Leftarrow \lfloor \frac{\ell-1}{d} \rfloor m + \lceil \frac{\alpha}{\beta} \rceil$
    else
      $k \Leftarrow \lceil k/d \rceil$
    end if
  end while
  return r
end procedure

表 5.1: The number of chosen plaintexts to construct r-round integral distinguishers on (ℓ, d, m)-SPN.

Target	$\log_2$(#texts)					Method
	$r = 3$	$r = 4$	$r = 5$	$r = 6$	$r = 7$	
$(4, 3, 16)$-SPN	12	28	52	60	-	our
[PRESENT]	28	52	60	63	-	degree
$(8, 7, 16)$-SPN	56	120	-	-	-	our
[AES]	117	127	-	-	-	degree

5.3.1 比較検討

表5.1 に $(4, 3, 16)$-SPN および $(8, 7, 16)$-SPN の r 段 Integral 特性を構成するのに必要な選択平文数を整理する．ここで $(4, 3, 16)$-SPN は PRESENT [BKL+07] を，$(8, 7, 16)$-SPN は AES [U.S01] をそれぞれ意識したパラメータである．2^D 選択平文を用いて (ℓ, d, m)-SPN の Integral 特性を探索する際，

表 5.2: The number of chosen plaintexts to construct r-round integral distinguishers on KECCAK-f and Serpent.

Target	$\log_2$(#texts)								Method
[Application]	$r=3$	$r=4$	$r=5$	$r=6$	$r=7$	$r=8$	$r=9$	$r=10$	
$(4,3,32)$-SPN	12	28	84	113	124	-	-	-	our
[Serpent]	28	82	113	123	127	-	-	-	degree

Target	$\log_2$(#texts)								Method
[Application]	$r=8$	$r=9$	$r=10$	$r=11$	$r=12$	$r=13$	$r=14$	$r=15$	
$(5,2,320)$-SPN	130	258	515	1025	1410	1538	1580	1595	our
[KECCAK-f]	257	513	1025	1409	1537	1579	1593	1598	degree

入力の $(k_1, k_2, \ldots, k_m)$ として以下のパラメータを用いた．

$$k_i = \begin{cases} \ell & \text{if } i\ell \leq D, \\ D-(i-1)\ell & \text{if } (i-1)\ell \leq D < i\ell, \\ 0 & \text{if } D < (i-1)\ell. \end{cases}$$

Division Property を用いた手法と比較するために Integral Property の伝搬を用いた場合と代数次数の見積りを行う場合を考える．初めに Integral Property を用いる方法を考える．(ℓ, d, m)-SPN の P-Layer は任意の線形関数を許容するため，Integral Property の伝搬は効果的な Integral 特性を導出しない．一方で代数次数を見積もる手法では，Boura らが提案した技術 [BCC11] を用いることで効果的な Integral 特性を発見できる．

結果として，調査した範囲では，全ての Integral 特性において Division Property は既存手法よりも良い Integral 特性を発見した．一方で今回示す Integral 特性はあくまで (ℓ, d, m)-SPN に対する汎用的なものであることに注意されたい．例に文献 [WW13] では PRESENT の 7 段 Integral 特性，文献 [KW02] では 4 段 Integral 特性が，各暗号の詳細な仕様を利用することで発見されている．今回の $(4, 3, 16)$-SPN や $(8, 7, 16)$-SPN の結果は，たとえ PRESENT や AES の P-Layer を任意の線形関数に置き換えたとしても，それぞれ 6 段 Integral 特性と 4 段 Integral 特性を持つことを示している．

5.3.2 Serpent と Keccak-f に対する Integral 特性

本章で示す Integral 特性は (ℓ, d, m)-SPN に対する汎用的なものである一方，Serpent [ABK98] と KECCAK-f [DBPA11] に対する Integral 特性では新規な Integral 特性を導く．Serpent は AES ファイナリストの一つであり $(4, 3, 32)$-SPN の構造を持つ．既存の Integral 特性は文献 [ZRHD08] で提案され，Serpent は 3.5 段 Integral 特性をもつことが示された．一方で Division Property の伝搬は $(4, 3, 32)$-SPN が 2^{124} 選択平文を用いて 7 段 Integral 特性を持つこ

とを示した．表 5.2 に Division Property による Integral 特性と代数次数の見積りによる Integral 特性の比較を示す．

KECCAK は SHA-3 に選ばれたハッシュ関数であり，そのコア関数 KECCAK-f は $(5, 2, 320)$-SPN の構造を持つ．文献 [BCC11] にて Boura らは KECCAK-f の代数次数を見積もり，KECCAK-f の zero-sum distinguisher を示した．表 5.2 に Division Property による Integral 特性と代数次数の見積りによる Integral 特性の比較を示す．結果，全ての段数において Division Property を用いた手法は文献 [BCC11] の手法より少ない選択平文数の Integral 特性を発見した．

5.4 (ℓ, d, m)-SPN に対する Integral 特性の整理

表 5.3 に (ℓ, d, m)-SPN の Integral 特性を整理する．

表 5.3: The number of required chosen plaintexts to construct r-round integral distinguishers on (ℓ, d, m)-SPN.

Target	Size	$\log_2$(#texts)							Examples
	(bits)	$r=4$	$r=5$	$r=6$	$r=7$	$r=8$	$r=9$	$r=10$	
$(4,3,16)$	64	28	52	60	-	-	-	-	PRESENT [BKL+07], LED [GPPR11]
$(4,3,24)$	96	28	76	89	-	-	-	-	
$(4,3,32)$	128	28	84	113	124	-	-	-	Serpent [ABK98], Noekeon [DPAR00]
$(4,3,40)$	160	28	84	136	152	-	-	-	
$(4,3,48)$	192	28	84	156	180	188	-	-	
$(4,3,56)$	224	28	84	177	209	220	-	-	
$(4,3,64)$	256	28	84	200	237	252	-	-	Minalpher [STA+14]
$(4,3,128)$	512	28	84	244	424	484	504	509	Prøst-256 [KLL+14]

Target	Size	$\log_2$(#texts)							Examples
	(bits)	$r=5$	$r=6$	$r=7$	$r=8$	$r=9$	$r=10$	$r=11$	
$(5,2,40)$	200	18	35	65	130	178	195	-	PRIMATE-80 [ABB+14]
$(5,2,56)$	280	18	35	65	130	230	265	275	PRIMATE-120 [ABB+14]
$(5,2,64)$	320	18	35	65	130	258	300	315	ASCON Permutation [DEMS14]

Target	Size	$\log_2$(#texts)							Examples
	(bits)	$r=9$	$r=10$	$r=11$	$r=12$	$r=13$	$r=14$	$r=15$	
$(5,2,160)$	800	258	515	705	770	790	798	-	Keccak-f[800] [DBPA11]
$(5,2,256)$	1280	258	515	1025	1195	1253	1271	1278	
$(5,2,320)$	1600	258	515	1025	1410	1538	1580	1595	Keccak-f[1600] [DBPA11]

Target	Size	$\log_2$(#texts)							Examples
	(bits)	$r=3$	$r=4$	$r=5$	$r=6$	$r=7$	$r=8$	$r=9$	
$(5,4,40)$	200	20	65	170	195	-	-	-	
$(5,4,56)$	280	20	65	230	270	-	-	-	
$(5,4,64)$	320	20	65	260	305	-	-	-	
$(5,4,160)$	800	20	65	260	665	770	795	-	
$(5,4,256)$	1280	20	65	260	1025	1220	1265	-	ICEPOLE Permutation [MGH+14]
$(5,4,320)$	1600	20	65	260	1025	1460	1565	1595	

Target	Size	$\log_2$(#texts)							Examples
	(bits)	$r=3$	$r=4$	$r=5$	$r=6$	$r=7$	$r=8$	$r=9$	
$(8,7,16)$	128	56	120	-	-	-	-	-	AES [U.S01]
$(8,7,24)$	192	56	176	-	-	-	-	-	Rijndael-192 [DR02]
$(8,7,32)$	256	56	232	-	-	-	-	-	Rijndael-256 [DR02]
$(8,7,64)$	512	56	344	488	-	-	-	-	Whirlpool primitive [BR03]

第II部

Division Property (応用編)

第6章　Division Propertyの応用

第二部では Division Property の応用に関して示す．Division Property では Split や Concatenation といった基本の伝搬特性を用いることで，評価したい関数に合わせて Division Property の定義を自由に変更して取り扱うことができる．従来の Integral Property や代数次数の見積りにおいても同様な評価は可能であったが，このような評価は非常に複雑であり，Division Property が実現するような統一的評価は困難だった．

Division Property の応用を検討する際に注意すべきこととして，どのような状態の Division Property が最適かを検討することは重要である．n ビットブロック暗号に対して Division Property を用いた解析を行う場合，$n = \sum_{i=1}^{m} \ell_i$ を満足するあらゆる $\mathcal{D}_{\mathbb{K}}^{\ell_1,\ell_2,\ldots,\ell_m}$ が利用可能である．例に F 関数が明らかにサブブロック単位に分割可能な Feistel 暗号の場合，これらの構造を利用可能な Division Property を利用することが推奨される．分割可能な構造を利用しない場合，第一部で示したような汎用解析手法以上の結果を得られない．一方で，あまりにも細かなサブブロックに分割した場合，コンピュータの支援を受けたとしても伝搬特性の評価は困難である．したがって最適なサブブロックを発見し Division Property を適用することが重要である．以降の章では AES [U.S01] のため $\mathcal{D}_{\mathbb{K}}^{8^{16}}$，MISTY1 [Mat97] のために $\mathcal{D}_{\mathbb{K}}^{7,2,7,7,2,7,7,2,7,7,2,7}$ を主に利用する．

第7章　AES型暗号に対するIntegral攻撃

本章では Division Property を用いて AES [U.S01] および AES 型暗号の Integral 特性を探索する．

7.1　AES型暗号

本章では AES 型暗号に対して Division Property を適用した結果を報告する．最も頻用されるブロック暗号として AES があり，AES は 128 ビットブロック暗号であり，安全性は 128 ビット，192 ビット，256 ビットから選択される．その内部状態は 4×4 の行列で表現され，行列の各要素は 8 ビットの値を取る．AES のラウンド関数は SubBytes，ShiftRows，MixColumns，AddRoundKey で構成され，それぞれの関数は以下のように定義される．

- SubBytes (SB)：行列の各要素を S-box を用いて別の値に置換する．
- ShiftRows (SR)：行列の i 番目の行の 4 バイトを $i-1$ バイト左にローテーションする．
- MixColumns (MC)：線形関数を用いて行列の各列の中身を撹拌する．
- AddRoundKey (AK)：ラウンド鍵を行列全体に排他的論理和する．

本章では AES 型暗号として以下の様な暗号構造を定義する．

Definition 9 ((ℓ, d, m)-AES)**.** 内部状態が $m \times m$ 行列で表現され，各要素が ℓ ビットの値を取るとする．すなわち (ℓ, d, m)-AES のブロック長は ℓm^2 ビットである．ラウンド関数の各構成関数は AES と同様に定義され，ただし S-box の代数次数は高々d とする．

今 $\vec{x} \in (\mathbb{F}_2^\ell)^{m^2}$ を (ℓ, d, m)-AES のラウンド関数の入力とすると，$\vec{x}$ は行列表現を用いて以下のように表せる．

$$\begin{bmatrix} x_1 & x_{m+1} & \cdots & x_{m^2-m+1} \\ x_2 & x_{m+2} & \cdots & x_{m^2-m+2} \\ \vdots & \vdots & \ddots & \vdots \\ x_m & x_{2m} & \cdots & x_{m^2} \end{bmatrix}.$$

$\vec{y} \in (\mathbb{F}_2^\ell)^{m^2}$ をラウンド関数の出力とすると，それは $\vec{y} = (\mathrm{AK} \circ \mathrm{MC} \circ \mathrm{SR} \circ \mathrm{SB})(\vec{x})$ より計算される．例に AES [U.S01] と `LED` [GPPR11] はそれぞれ $(8, 7, 4)$-AES と $(4, 3, 4)$-AES と見なすことができる．`PHOTON` [GPP11] の P_{256} はブロック暗号ではなく暗号学的置換であるが，$(4, 3, 8)$-AES と見なすことができる [1]．また (ℓ, d, m)-AES は (ℓ, d, m^2)-SPN のサブクラスとなっていることに注意されたい．

7.2 (ℓ, d, m)-AES に対するパス探索アルゴリズム

(ℓ, d, m)-SPN は線形関数として任意の関数を利用する．しかし多くの暗号はより特徴的な線形関数を利用しており，例に AES は ShiftRows と MixColumns の合成関数を線形関数として利用する．本章ではこの線形関数の特徴を利用した Division Property の伝搬特性探索アルゴリズムを考える．

Algorithm 3 に Division Property を用いた (ℓ, d, m)-AES に対する Integral 特性探索アルゴリズムを示す．Integral 特性探索は `IntegralPathSearch` を用いて評価され，それは `AesFuncEval` を呼び出す．`AesFuncEval` では AES 型暗号のラウンド関数の入力集合が Division Proeprty $\mathcal{D}_{\vec{k}}^{\ell^{mm}}$ を持つときの出力集合の Division Property が評価される．また `ShiftRows` は実際の ShifRows と同等の変化を Division Property の各値に適用する関数を表す．

実装効率を向上させるため，Algorithm 3 では `sort` を利用する，ここで `sort` は m 個の要素を辞書式順序に並べ替えることを意味する．これは (ℓ, d, m)-AES の各列から発生する伝搬はそれぞれ等価であることに起因する．例に入力集合が Division Property $\mathcal{D}_{\{\vec{k},\vec{k}'\}}^{(\ell m)^m}$ を満足したと仮定し，また $\vec{k}'$ は $\vec{k}$ の要素内を置換したものとする．このとき $\vec{k}$ から次のラウンド関数を評価後に得られる Division Property と $\vec{k}'$ から得られる Division Property は正確に一致する．したがって要素内を置換した結果一致するベクトルに関しては，そのどれか一つのみを評価すれば十分であり，これを `sort` を用いることで実現する (Algorithm 3 の 8 行目に対応)．

`IntegralPathSearch` は `Partition` 関数を呼び出すが，`Partition`$(\vec{k})$ では

$$\left(\sum_{r=1}^{m} k'_r, \sum_{r=1}^{m} k'_{m+r}, \ldots, \sum_{r=1}^{m} k'_{m(m-1)+r} \right) = (k_1, k_2, \ldots, k_m),$$

を満足する全てのとり得る $\vec{k}' \in \mathbb{Z}^{mm}$ が計算される．ここで，$\vec{k}'$ の各要素は 0 から ℓ までをとる．また `SizeReduce` では $\vec{k} \in \mathbb{K}$ と $\vec{k}' \in \mathbb{Z}$ において $\vec{k} \succeq \vec{k}'$ を満足するとき $\vec{k} \in \mathbb{Z}$ を削除する．

Algorithm 3 Path search for integral characteristics on (ℓ, d, m)-AES

procedure $\texttt{AesFuncEval}(\ell, d, m, \vec{k})$
  for $i = 1$ to m^2 **do**
    if $k_i < \ell$ **then** $k_i \Leftarrow \lceil k_i/d \rceil$ ▷ SubBytes
    end if
  end for
  $\vec{k} \Leftarrow \texttt{ShiftRows}(\vec{k})$ ▷ ShiftRows
  $k'_c \Leftarrow \sum_{r=1}^{m} k'_{m(c-1)+r}$ for all c ▷ MixColumns
  $\vec{k'} \Leftarrow \texttt{sort}(\vec{k'})$
  return $\vec{k'}$
end procedure

procedure $\texttt{IntegralPathSearch}(\ell, d, m, r = 0, \vec{k} \in \{0, 1, \ldots, \ell\}^{m^2})$
  $\mathbb{K} \Leftarrow \texttt{AesFuncEval}(\ell, d, m, \vec{k})$ ▷ 1-st round
  $D \Leftarrow \max_{\vec{k} \in \mathbb{K}}(\sum_{c=1}^{m} k_c)$
  while $1 < D$ **do**
    $r \Leftarrow r + 1$
    $\mathbb{K}' = \phi$
    for all $\vec{k} \in \mathbb{K}$ **do**
      $\mathbb{K}'' \Leftarrow \texttt{Partition}(\vec{k})$
      for all $\vec{k}'' \in \mathbb{K}''$ **do**
        $\mathbb{K}' \Leftarrow \mathbb{K}' \cup \texttt{AesFuncEval}(\ell, d, m, \vec{k}'')$
      end for
    end for
    $\mathbb{K} \Leftarrow \texttt{SizeReduce}(\mathbb{K}')$
    $D \Leftarrow \max_{\vec{k} \in \mathbb{K}}(\sum_{c=1}^{m} k_c)$
  end while
  return r
end procedure

7.2.1 $(4, 3, m)$-AES 型暗号への適用結果

表 7.1 に $(4, 3, m)$-AES の r 段 Integral 特性を構成するために必要な選択平文数を整理する．ここで 2^D 選択平文を用いて $(4, 3, m)$-AES の Integral 特性を探索する場合，1 ラウンド目のラウンド関数における Division Property の劣化が最小になるように $\vec{k}$ を選択する．

Division Property による改良 Integral 特性との比較のため，Integral Property の伝搬を用いた手法と代数次数の見積もりを用いた手法も同様に評価した．また $(4, 3, m)$-AES は $(4, 3, m^2)$-SPN と見なすことができるため，Algorithm 2

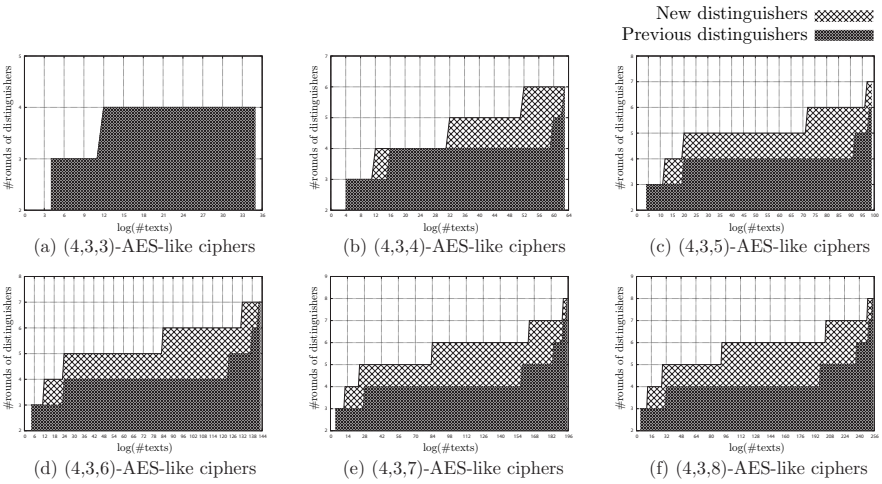
[1] PHOTON はハッシュ関数のため AddRoundKey の代わりに AddConstant が使われる

表 7.1: The number of chosen plaintexts to construct r-round integral distinguishers on $(4,3,m)$-AES.

Target [Application]	$\log_2$(#texts)						Method
	$r=3$	$r=4$	$r=5$	$r=6$	$r=7$	$r=8$	
$(4,3,3)$-AES	4	12	-	-	-	-	our (AES)
	12	28	-	-	-	-	our (SPN)
	28	34	-	-	-	-	degree
	4	12	-	-	-	-	integral
$(4,3,4)$-AES [LED]	4	12	32	52	-	-	our (AES)
	12	28	52	60	-	-	our (SPN)
	28	52	60	63	-	-	degree
	4	16	-	-	-	-	integral
$(4,3,5)$-AES [P_{100} in PHOTON]	4	12	20	72	97	-	our (AES)
	12	28	76	92	-	-	our (SPN)
	28	76	92	98	-	-	degree
	4	20	-	-	-	-	integral
$(4,3,6)$-AES [P_{144} in PHOTON]	4	12	24	84	132	-	our (AES)
	12	28	84	124	140	-	our (SPN)
	28	82	124	138	142	-	degree
	4	24	-	-	-	-	integral
$(4,3,7)$-AES [P_{196} in PHOTON]	4	12	24	84	164	192	our (AES)
	12	28	84	160	184	192	our (SPN)
	28	82	158	184	192	195	degree
	4	28	-	-	-	-	integral
$(4,3,8)$-AES [P_{256} in PHOTON]	4	12	28	92	204	249	our (AES)
	12	28	84	200	237	252	our (SPN)
	28	82	198	237	250	254	degree
	4	32	-	-	-	-	integral

を用いた場合も同様に評価した．

図 7.1 に $(4,3,m)$-AES 型暗号に対する既存の最良 Integral 特性 (代数次数見積りと Integral Property の伝搬特性の中で効率の良い方法) と，Division Property によって新たに発見した改良 Integral 特性の比較を示す．ここで横軸は利用する選択平文数を表し，縦軸は Integral 特性を構築できた段数を表す．図 7.1 より，我々が評価した範囲では Division Property による Integral 特性は常に従来手法を上回る結果となった．とりわけ，提案手法の利点は攻撃に要する選択平文数が少ない場合に大きくなる．例に $(4,3,8)$-AES (PHOTON P_{256} で利用) において，提案手法は 2^{92} 個の選択平文を用いて 6 段 Integral 特性を構築した．一方で $(4,3,8)$-AES を $(4,3,64)$-SPN と見なす場合は 2^{200}



(a) (4,3,3)-AES-like ciphers (b) (4,3,4)-AES-like ciphers (c) (4,3,5)-AES-like ciphers

(d) (4,3,6)-AES-like ciphers (e) (4,3,7)-AES-like ciphers (f) (4,3,8)-AES-like ciphers

図 7.1: Comparison between new and previous integral characteristics for $(4, 3, m)$-AES-like ciphers

個の選択平文，代数次数の見積りを利用する場合は 2^{237} 個の選択平文をそれぞれ要した．

7.2.2 $(4, 2, m)$-AES 型暗号への適用結果

S-box の代数次数が小さくなればなるほど，Division Property は従来手法よりも優れた Integral 特性を構築できると考えられる．したがって代数次数を 3 から 2 に引き下げた $(4, 2, m)$-AES 型暗号に対する Integral 特性を同様に評価する．表 7.2 に $(4, 2, m)$-AES の r 段 Integral 特性を構成するために必要な選択平文数を整理する．ここで 2^D 選択平文を用いて $(4, 2, m)$-AES の Integral 特性を探索する場合，1 ラウンド目のラウンド関数における Division Property の劣化が最小になるように $\vec{k}$ を選択する．Integral Property の伝搬特性は代数次数の減少に対して影響を与えないため常に 4 段 Integral 特性を構築するのみである．したがって代数次数の見積りを用いた手法とのみ比較する．

図 7.2 に $(4, 2, m)$-AES 型暗号に対する既存の最良 Integral 特性 (代数次数見積りと Integral Property の伝搬特性の中で効率の良い方法) と，Division Property によって新たに発見した改良 Integral 特性の比較を示す．ここで横軸は利用する選択平文数を表し，縦軸は Integral 特性を構築できた段数を表す．$(4, 3, m)$-AES 型暗号のときと同様に，我々が評価した範囲では Division Property による Integral 特性は常に従来手法を上回る結果となった．

表 7.2: The number of chosen plaintexts to construct r-round integral distinguishers on $(4, 2, m)$-AES.

Target	$\log_2$(#texts)							Method
	$r = 7$	$r = 8$	$r = 9$	$r = 10$	$r = 11$	$r = 12$	$r = 13$	
$(4, 2, 3)$-AES	34	35	-	-	-	-	-	degree
	25	35	-	-	-	-	-	our (AES)
$(4, 2, 4)$-AES	57	61	63	-	-	-	-	degree
	33	49	61	-	-	-	-	our (AES)
$(4, 2, 5)$-AES	83	92	96	98	99	-	-	degree
	37	60	80	96	99	-	-	our (AES)
$(4, 2, 6)$-AES	105	125	135	140	142	143	-	degree
	37	69	105	125	140	143	-	our (AES)
$(4, 2, 7)$-AES	129	163	180	188	192	194	195	degree
	36	69	116	163	184	192	195	our (AES)
$(4, 2, 8)$-AES	129	193	225	241	249	253	255	degree
	33	65	129	193	225	249	253	our (AES)

7.3 AES に対する伝搬特性評価

AES 型暗号の中で最も注目すべきパラメータは AES で採用されている $(8, 7, 4)$-AES である．本節では $(8, 7, 4)$-AES に対する Division Property の伝搬特性を考える．

7.3.1 4 段 Integral 特性の再発見

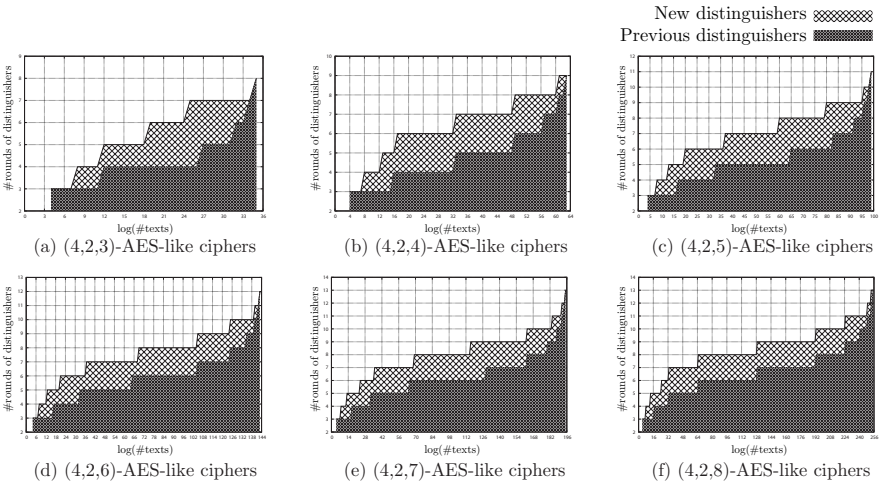
初めに Division Property の伝搬特性を用いて 4 段 Integral 特性の再発見を行う．Algorithm 3 の入力として

$$\vec{k} = \begin{bmatrix} 8 & 0 & 0 & 0 \\ 0 & 8 & 0 & 0 \\ 0 & 0 & 8 & 0 \\ 0 & 0 & 0 & 8 \end{bmatrix}$$

を利用したとき，Division Property は以下のように伝搬する．

$$\mathcal{D}_{\vec{k}}^{8^{16}} \xrightarrow{4R} \mathcal{D}_2^{128}$$

すなわち 2^{32} 個のテキストに対して 4 段後の 128 ビットの和は常に 0 となることが分かる．



(a) (4,2,3)-AES-like ciphers (b) (4,2,4)-AES-like ciphers (c) (4,2,5)-AES-like ciphers

(d) (4,2,6)-AES-like ciphers (e) (4,2,7)-AES-like ciphers (f) (4,2,8)-AES-like ciphers

図 7.2: Comparison between new and previous integral characteristics for $(4, 2, m)$-AES-like ciphers

7.3.2 新しい Integral 特性

より多くの選択平文を用いた場合の Division Property の伝搬を考える．初めに Algorithm 3 の入力として

$$\vec{k} = \begin{bmatrix} 8 & 8 & 0 & 0 \\ 0 & 8 & 8 & 0 \\ 0 & 0 & 8 & 8 \\ 8 & 0 & 0 & 8 \end{bmatrix}$$

を利用した．このとき Division Property は以下のように伝搬した．

$$\mathcal{D}_{\vec{k}}^{8^{16}} \xrightarrow{4R} \mathcal{D}_{3}^{128}$$

すなわち 4 段後，128 ビットから任意の 2 ビット以下を選択し，選択されたビットの AND 値の和を計算すると必ず 0 となることが分かる．さらに Algorithm 3 の入力として

$$\vec{k} = \begin{bmatrix} 8 & 8 & 8 & 0 \\ 0 & 8 & 8 & 8 \\ 8 & 0 & 8 & 8 \\ 8 & 8 & 0 & 8 \end{bmatrix}$$

を利用した．このとき Division Property は以下のように伝搬した．

$$\mathcal{D}_{\vec{k}}^{8^{16}} \xrightarrow{4R} \mathcal{D}_{4}^{128}$$

すなわち 4 段後，128 ビットから任意の 3 ビット以下を選択し，選択されたビットの AND 値の和を計算すると必ず 0 となることが分かる．

上述した Integral 特性は従来の評価からは得られない．しかしながら，このような特性を中間状態が持つとき，効率よく鍵回復を実行する方法は未解決問題である．したがって AES が上述の特徴を持っていたとしても，現段階では AES の安全性に影響を与えない．

第8章　MISTY1に対するIntegral攻撃

本章では Division Property を用いて MISTY1 [Mat97] の Integral 特性を探索する．また，この Integral 特性を用いて仕様段数の MISTY1 が 128 ビット未満の計算量で解読可能なことを示す．

8.1　MISTY1

MISTY1 は MISTY 構造を持つ F 関数を利用した Feistel 暗号であり，推奨パラメータは 8 段 FL5 層である．MISTY1 は様々な機関で標準化されており，例に CRYPTREC の推奨候補暗号リスト [CRY13]，ISO/IEC 18033-3 [ISO05]，NESSIE 推奨暗号 [NES04] に選ばれている．また RFC 2994 [OM00] でも MISTY1 が記述されている．

図 8.1 に MISTY1 の構造を示す．(X_i^L, X_i^R) は i 段目のラウンド関数の入力であり，また $X_i^L[j]$ および $X_i^R[j]$ は X_i^L および X_i^R の左から j 番目のビットを表す．MISTY1 は 128 ビット安全な 64 ビットブロック暗号であり，F 関数である FO_i は $FI_{i,1}$，$FI_{i,2}$，$FI_{i,3}$ を用いた 3 段 MISTY 構造で構成され，4 つの 16 ビット鍵 $KO_{i,1}$，$KO_{i,2}$，$KO_{i,3}$，$KO_{i,4}$ が使われる．また関数 $FI_{i,j}$ も MISTY 構造を持ち，9 ビット S-box S_9 と 7 ビット S-box S_7 が MISTY 構造の F 関数で利用され，1 つの 16 ビット鍵 $KI_{i,j}$ が使われる．付録 A に S_9 および S_7 の Algebraic Normal Form を示す．MISTY1 は FL 層付きの Feistel 暗号であり，FL_i 関数は 2 つの 16 ビット鍵 $KL_{i,1}$ と $KL_{i,2}$ を利用する．全てのラウンド鍵は 128 ビット秘密鍵 $(K_1, K_2, \ldots, K_8)$ から以下の手順で計算され，

Symbol	$KO_{i,1}$	$KO_{i,2}$	$KO_{i,3}$	$KO_{i,4}$	$KI_{i,1}$	$KI_{i,2}$	$KI_{i,3}$	$KL_{i,1}$	$KL_{i,2}$
Key	K_i	K_{i+2}	K_{i+7}	K_{i+4}	K'_{i+5}	K'_{i+1}	K'_{i+3}	$K_{\frac{i+1}{2}}$ (odd i) $K'_{\frac{i}{2}+2}$ (even i)	$K'_{\frac{i+1}{2}+6}$ (odd i) $K_{\frac{i}{2}+4}$ (even i)

ここで K_i および K'_i は i が 8 を超えた場合，K_{i-8} および K'_{i-8} と同一のものとする．また K'_i は入力として K_i，鍵として K_{i+1} を用いた $FI_{i,j}$ 関数の出力である．

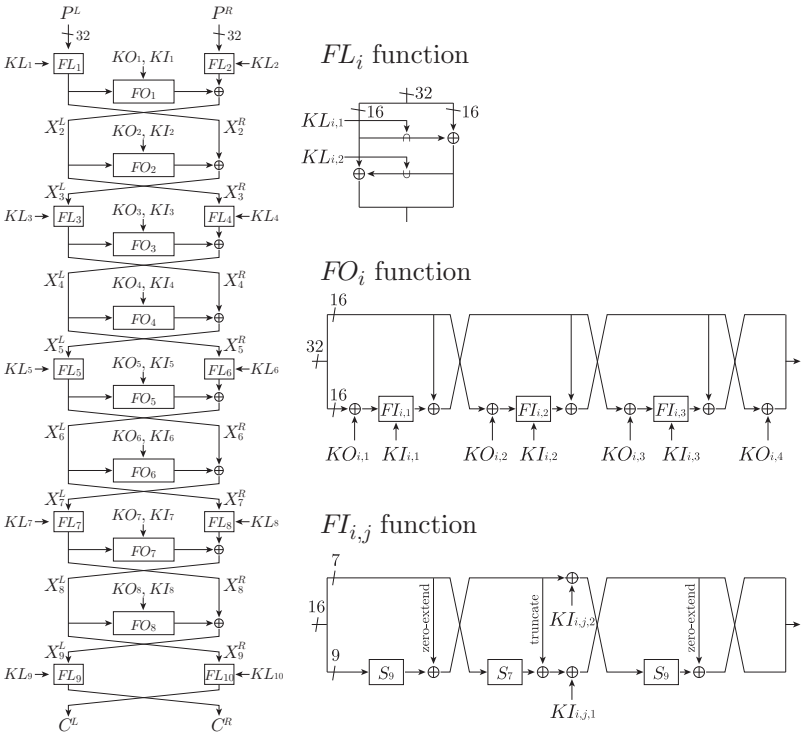


図 8.1: Specification of MISTY1

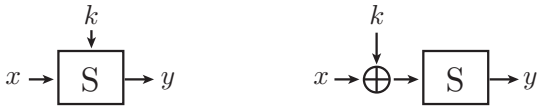


図 8.2: The left figure is an assumption used in [Tod15b]. The right one is a new assumption used in [Tod15a].

8.2 公開関数に対する Division Property の伝搬特性

Division Property を用いた MISTY1 の Integral 特性探索の前に，公開関数に対する Division Property の伝搬特性を考える．第一部では代数次数のみが攻撃者にとって既知な秘密関数に対する Division Property の伝搬特性が示された．しかしながら，実際の暗号では公開 S-box と秘密なラウンド鍵の加算を用いた構成，とりわけ加算として排他的論理和を用いた構成が頻用される．この場合，第一部で示した伝搬特性はさらに改良されうる．図 8.2 に第一部で示したものとの対象の違いを整理する．

図 8.2 の右図によって示された関数に対する Division Property の伝搬特性

を考える．初めに入力と秘密のラウンド鍵の排他的論理和が計算される．ここで固定値の排他的論理和は線形関数であることに注意されたい．したがって入力の Division Property とラウンド鍵の排他的論理和後の Division Property は正確に一致する．すなわち攻撃者はラウンド鍵の排他的論理和を取り除いて Division Property の伝搬特性を評価すればよい．次に公開 S-box が適用される．ここで S-box の仕様が公開されているため，攻撃者は S-box の ANF を正確に計算できる．S-box が n ビットから m ビットへの関数として，S-box の ANF は以下のように表せる．

$$\begin{aligned} y[1] &= f_1(x[1], x[2], \ldots, x[n]), \\ y[2] &= f_2(x[1], x[2], \ldots, x[n]), \\ &\vdots \\ y[m] &= f_m(x[1], x[2], \ldots, x[n]), \end{aligned}$$

ここで $x[i]\,(1 \leq i \leq n)$ は S-box の入力，$y[j]\,(1 \leq j \leq m)$ は S-box の出力，$f_j\,(1 \leq j \leq m)$ は S-box から計算されたブール関数である．Division Property は Bit Propduct Function π_u を用いて，u の全集合をパリティが 0 となる部分集合とパリティが不定となる部分集合に分割することにより評価される．したがって，出力の Division Property を評価することは次式のパリティを評価することと等しい．

$$\bigoplus_{x \in \mathbb{X}} F_u(x[1], x[2], \ldots, x[n]) = \bigoplus_{x \in \mathbb{X}} \prod_{i=1}^{m} f_i(x[1], x[2], \ldots, x[n])^{u[i]}.$$

攻撃対象が高々d な代数次数を持つ秘密関数のとき，F_u の代数次数が高々 $w(u) \times d$ である事実に基づき伝搬特性を評価した．一方で攻撃対象が公開関数であるとき，全ての u に対して F_u の代数次数を正確に計算できる．したがって同一の $w(u)$ を持つ全ての u において，F_u の代数次数が $w(u) \times d$ より小さいならば，Division Property の伝搬特性は改良可能である．

8.2.1 MISTY S-box への応用

S_7 の伝搬特性

MISTY は代数次数 3 である 7 ビット S-box S_7 を利用する．ここで S_7 の ANF は付録 A を参照されたい．S_7 に対する Division Property の伝搬特性を評価するため，全ての $v \in \mathbb{F}_2^7$ における $(\pi_v \circ S_7)$ の代数次数を評価する．$(\pi_v \circ S_7)$ の代数次数は v のハミング重みが増加するにつれて増加し，結果として以下の関係を持つことが分かる．

$w(v)$	0	1	2	3	4	5	6	7
degree	0	3	5	5	6	6	6	7

代数次数 3 である任意の 7 ビット S-box に対する Division Property の伝搬特性を評価すると，$w(v) \geq 2$ を満足する $(\pi_v \circ S_7)$ の代数次数は少なくとも 6 である．しかしながら S_7 の場合，$w(v) = 2$ または $w(v) = 3$ のときに $(\pi_v \circ S_7)$ の代数次数は高々5 である [1]．したがって S_7 に対する Division Property の伝搬特性は以下のように整理される．

$\mathcal{D}_k^7$ for input set $\mathbb{X}$	$\mathcal{D}_0^7$	$\mathcal{D}_1^7$	$\mathcal{D}_2^7$	$\mathcal{D}_3^7$	$\mathcal{D}_4^7$	$\mathcal{D}_5^7$	$\mathcal{D}_6^7$	$\mathcal{D}_7^7$
$\mathcal{D}_k^7$ for output set $\mathbb{Y}$	$\mathcal{D}_0^7$	$\mathcal{D}_1^7$	$\mathcal{D}_1^7$	$\mathcal{D}_1^7$	$\mathcal{D}_2^7$	$\mathcal{D}_2^7$	$\mathcal{D}_4^7$	$\mathcal{D}_7^7$

特筆すべきは，入力 Division Property $\mathcal{D}_6^7$ から出力 Division Property $\mathcal{D}_4^7$ が得られることである．代数次数 3 である 7 ビット S-box において，一般に $\mathcal{D}_6^7$ から $\mathcal{D}_2^7$ が得られる．Division Property では D_k^n において k が小さくなればなるほど Unknow な性質に近いとみなされるため，この結果は MISTY の S_7 は一般の代数次数 3 の 7 ビット S-box よりも Division Property の劣化が緩やかであることを意味する．

S_9 の伝搬特性

MISTY は S_7 の他に代数次数 2 である 9 ビット S-box S_9 を持つ．ここで S_9 の ANF は付録 A を参照されたい．S_7 のときと同様に，全ての v における $(\pi_v \circ S_9)$ の代数次数を評価する．$(\pi_v \circ S_9)$ の代数次数は v のハミング重みが増加するにつれて増加し，結果として以下の関係を持つことが分かる．

$w(v)$	0	1	2	3	4	5	6	7	8	9
degree	0	2	4	6	8	8	8	8	8	9

したがって S_9 に対する Division Property の伝搬特性は以下のように整理される．

$\mathcal{D}_k^9$ for input set $\mathbb{X}$	$\mathcal{D}_0^9$	$\mathcal{D}_1^9$	$\mathcal{D}_2^9$	$\mathcal{D}_3^9$	$\mathcal{D}_4^9$	$\mathcal{D}_5^9$	$\mathcal{D}_6^9$	$\mathcal{D}_7^9$	$\mathcal{D}_8^9$	$\mathcal{D}_9^9$
$\mathcal{D}_k^9$ for output set $\mathbb{Y}$	$\mathcal{D}_0^9$	$\mathcal{D}_1^9$	$\mathcal{D}_1^9$	$\mathcal{D}_2^9$	$\mathcal{D}_2^9$	$\mathcal{D}_3^9$	$\mathcal{D}_3^9$	$\mathcal{D}_4^9$	$\mathcal{D}_4^9$	$\mathcal{D}_9^9$

S_7 における Division Property の伝搬特性と異なり，S_9 における Division Property の伝搬特性は通常の代数次数 2 における 9 ビット S-box における伝搬特性から改善されない．

8.3 MISTY 1 の新しい Integral 特性

本節では MISTY1 に対する Division Property の伝搬特性の評価方法を示す．初めに MISTY1 の構成関数である FI 関数， FO 関数， FL 層に対する Division Property の伝搬特性をそれぞれ独立に評価する．その後， これらの評価結果をまとめ， MISTY1 全体に対する Division Property の伝搬特性評価アルゴリズムを構成する．

[1] 文献 [BC13] の Theorem 3.1 でも同様の評価が示されている．

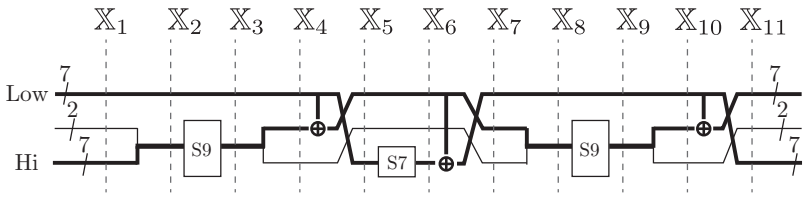


図 8.3: Structure of FI function

8.3.1 FI 関数に対する Division Property の伝搬特性

8.2.1 句で示した MISTY S-box の伝搬特性を用いて FI 関数に対する Division Property の伝搬特性を評価する．FI 関数は zero-extended XOR と truncated XOR の 2 種類の排他的論理和を用いる．MISTY 提案論文および既存解析論文では 9 ビット線と 7 ビット線を用いた FI 関数の表記が利用される．一方で，本稿では上記 2 種類の排他的論理和を考慮して，2 つの 7 ビット線と 1 つの 2 ビット線を用いた新しい FI 関数の表記を利用する．図 8.3 に新表記を用いた FI 関数を示す．ここで Division Property はラウンド鍵の排他的論理和に関して不定のため，鍵の排他的論理和を取り除いて表記していることに注意されたい．

初めに記号を定義する．$\mathbb{X}_1$ は FI 関数の入力多重集合である．同様に多重集合 $\mathbb{X}_2, \mathbb{X}_3, \ldots, \mathbb{X}_{11}$ を図 8.3 で示すように定義する．このとき多重集合 $\mathbb{X}_1, \mathbb{X}_5, \mathbb{X}_6, \mathbb{X}_{11}$ の要素は $(\mathbb{F}_2^7 \times \mathbb{F}_2^2 \times \mathbb{F}_2^7)$ の値を取る．また多重集合 $\mathbb{X}_2, \mathbb{X}_3, \mathbb{X}_8, \mathbb{X}_9$ の要素は $(\mathbb{F}_2^9 \times \mathbb{F}_2^7)$ の値，多重集合 $\mathbb{X}_4, \mathbb{X}_7, \mathbb{X}_{10}$ の要素は $(\mathbb{F}_2^2 \times \mathbb{F}_2^7 \times \mathbb{F}_2^7)$ の値をそれぞれ取る．多重集合 $\mathbb{X}_1$ と $\mathbb{X}_{11}$ は同様に $(\mathbb{F}_2^7 \times \mathbb{F}_2^2 \times \mathbb{F}_2^7)$ の値を取るため，FI 関数の伝搬は Division Property $\mathcal{D}_{\mathbb{K}}^{7,2,7}$ を用いて評価する．

Division Property の伝搬は以下のように評価される．

From $\mathbb{X}_1$ to $\mathbb{X}_2$: 最初の 7 ビット値と次の 2 ビット値をビット連結して 9 ビット値を生成する．$\mathbb{X}_2$ の Division Property は Concatenation の伝搬特性より導ける．

From $\mathbb{X}_2$ to $\mathbb{X}_3$: 最初の 9 ビット値を別の 9 ビット値に S_9 を用いて置換する．$\mathbb{X}_3$ の Division Property は 8.2.1 句で示した表をもとに導ける．

From $\mathbb{X}_3$ to $\mathbb{X}_4$: 最初の 9 ビット値が 2 ビット値と 7 ビット値に分割される．$\mathbb{X}_4$ の Division Property は Split の伝搬特性より導ける．

From $\mathbb{X}_4$ to $\mathbb{X}_5$: 中間の 7 ビット値に最後の 7 ビット値を排他的論理和し，全体をローテーションする．$\mathbb{X}_5$ の Division Property は Copy と XOR の伝搬特性より導ける．

From $\mathbb{X}_5$ to $\mathbb{X}_6$: 最初の 7 ビット値を別の 7 ビット値に S_7 を用いて置換する．$\mathbb{X}_6$ の Division Property は 8.2.1 句で示した表をもとに導ける．

Algorithm 4 Propagation for FI function

```
1: procedure FIEval(k_1, k_2, k_3)
2:     𝕂 ⇐ S9Eval(k⃗)                    ▷ 𝕏_1 → 𝕏_5
3:     𝕂' ⇐ S7Eval(𝕂)                   ▷ 𝕏_5 → 𝕏_7
4:     𝕂'' ⇐ S9Eval(𝕂')                 ▷ 𝕏_7 → 𝕏_11
5:     return 𝕂''
6: end procedure
```

```
1: procedure S9Eval(𝕂)
2:     𝕂' ⇐ φ
3:     for all k⃗ ∈ 𝕂 do
4:         [ℓ, c, r] ⇐ [k_1, k_2, k_3]
5:         k ⇐ ℓ + c
6:         if k < 9 then
7:             k ⇐ ⌈k/2⌉
8:         end if
9:         for c' ⇐ 0 to min(2, k) do
10:            for x ⇐ 0 to r do
11:                ℓ' ⇐ r − x
12:                r' ⇐ k − c' + x
13:                if r' ≤ 7 then
14:                    𝕂' ⇐ 𝕂' ∪ [ℓ', c', r']
15:                end if
16:            end for
17:        end for
18:    end for
19:    return SizeReduce(𝕂')
20: end procedure
```

```
21: procedure S7Eval(𝕂)
22:     𝕂' ⇐ φ
23:     for all k⃗ ∈ 𝕂 do
24:         [ℓ, c, r] ⇐ [k_1, k_2, k_3]
25:         k ⇐ ℓ
26:         if k = 6 then
27:             k ⇐ 4
28:         else if k < 6 then
29:             k ⇐ ⌈k/3⌉
30:         end if
31:         for x ⇐ 0 to r do
32:             ℓ' ⇐ c
33:             c' ⇐ r − x
34:             r' ⇐ k + x
35:             if r' ≤ 7 then
36:                 𝕂' ⇐ 𝕂' ∪ [ℓ', c', r']
37:             end if
38:         end for
39:     end for
40:     return SizeReduce(𝕂')
41: end procedure
```

From $\mathbb{X}_6$ to $\mathbb{X}_7$: 最初の 7 ビット値に最後の 7 ビット値を排他的論理和し，全体をローテーションする．$\mathbb{X}_7$ の Division Property は Copy と XOR の伝搬特性より導ける．

From $\mathbb{X}_7$ to $\mathbb{X}_8$: 最初の 7 ビット値と次の 2 ビット値をビット連結して 9 ビット値を生成する．$\mathbb{X}_8$ の Division Property は Concatenation の伝搬特性より導ける．

From $\mathbb{X}_8$ to $\mathbb{X}_{11}$: $\mathbb{X}_2$ から $\mathbb{X}_5$ までと同様にして，$\mathbb{X}_{11}$ の伝搬特性を評価する．

例として，付録 B に $\mathbb{X}_1$ が Division Property $\mathcal{D}^{7,2,7}_{\{[4,2,6]\}}$ を満足した場合の伝搬特性を示す．Algorithm 4 は FI 関数に対する伝搬特性表を生成するためのアルゴリズムである．AES 型暗号のときと同様に，Algorithm 4 は `SizeReduce` 関数を利用し，ここで $\vec{k} \in \mathbb{K}$ において $\vec{k} \succeq \vec{k}'$ を満足する $\vec{k}' \in \mathbb{K}$ が存在する場合，$\vec{k}$ は冗長であるため $\mathbb{K}$ から削除される．Algorithm 4 は入力 Division Property が $\mathcal{D}^{7,2,7}_{\{\vec{k}\}}$ であるときからの伝搬特性のみを評価する．任意の入力集合に対する伝搬特性を評価するためには，入力 Division Property が $\mathcal{D}^{7,2,7}_{\mathbb{K}}$ であるときからの伝搬特性を評価する必要がある．これは Vectorial Division

Property から Corrective Division Property への拡張を考えることと同様に単純に評価可能である．例に $\mathcal{D}^{7,2,7}_{\{\vec{k},\vec{k'}\}}$ からの伝搬特性を考える．初めに $\mathcal{D}^{7,2,7}_{\{\vec{k}\}}$ からの伝搬特性を評価して $\mathbb{K}_1$ を得る．次に $\mathcal{D}^{7,2,7}_{\{\vec{k'}\}}$ からの伝搬特性を評価して $\mathbb{K}_2$ を得る．最後に出力 Division Property $\mathcal{D}^{7,2,7}_{\mathbb{K}}$ の $\mathbb{K}$ は $\mathbb{K} = \mathbb{K}_1 \cup \mathbb{K}_2$ から計算される．

FI 関数に対する全 Division Property の伝搬評価は付録 C を参照されたい．最後に FI 関数に対する Division Property の伝搬特性を実験的に評価した結果を報告する．本実験では，任意の $\mathcal{D}^{7,2,7}_{\{[k_1,k_2,k_3]\}}$ において，この Division Property を満足する 100 個の入力多重集合をランダムに生成し出力多重集合の Division Property を評価した．結果として，実験により導かれた伝搬特性は付録 C で示した理論による伝搬特性と一致することを確認した．

8.3.2 FO 関数に対する Division Property の伝搬特性

Algorithm 5 Propagation for FO function

procedure FOEval$(k_1, k_2, k_3, k_4, k_5, k_6)$
  $\mathbb{K} \Leftarrow$ FORound$(\vec{k})$
  $\mathbb{K}' \Leftarrow$ FORound$(\mathbb{K})$
  $\mathbb{K}'' \Leftarrow$ FORound$(\mathbb{K}')$
  return $\mathbb{K}''$
end procedure

procedure FORound$(\mathbb{K})$
  $\mathbb{K}' \Leftarrow \phi$
  for all $\vec{k} \in \mathbb{K}$ **do**
    $\mathbb{Y} \Leftarrow$ FIEval(k_1, k_2, k_3)
    for all $\vec{y} \in \mathbb{Y}$ **do**
      for all $\vec{x}$ s.t. $(x_1 \leq k_4) \wedge (x_2 \leq k_5) \wedge (x_3 \leq k_6)$ **do**
        $\vec{k'} \Leftarrow [k_4 - x_1, k_5 - x_2, k_6 - x_3, y_1 + x_1, y_2 + x_2, y_3 + x_3]$
        if $(k'_4 \leq 7) \wedge (k'_5 \leq 2) \wedge (k'_6 \leq 7)$ **then**
          $\mathbb{K}' \Leftarrow \mathbb{K}' \cup \vec{k'}$
        end if
      end for
    end for
  end for
  return SizeReduce$(\mathbb{K}')$
end procedure

次に FI 関数に対する Division Property の伝搬特性表を基に，FO 関数に対する Division Property の伝搬特性を評価する．初めにラウンド鍵の排他的

論理和は Division Property に影響を与えないため取り除く．FO 関数の入出力は $(\mathbb{F}_2^7 \times \mathbb{F}_2^2 \times \mathbb{F}_2^7 \times \mathbb{F}_2^7 \times \mathbb{F}_2^2 \times \mathbb{F}_2^7)$ の値を取ることから，Division Property $\mathcal{D}_{\mathbb{K}}^{7,2,7,7,2,7}$ を用いて伝搬特性を考える．

表 8.1: 伝搬特性例

$\vec{k}$ of $\mathcal{D}_{\{\vec{k}\}}^{7,2,7,7,2,7}$	$\mathbb{K}$ of $\mathcal{D}_{\mathbb{K}}^{7,2,7,7,2,7}$
[1 1 2 3 1 5]	[0 0 0 0 0 4] [0 0 0 0 1 3] [0 0 0 0 2 2] [0 0 0 1 0 3] [0 0 0 1 1 2]
	[0 0 0 1 2 1] [0 0 0 2 0 2] [0 0 0 2 1 1] [0 0 0 2 2 0] [0 0 0 3 0 1]
	[0 0 0 3 1 0] [0 0 0 5 0 0] [0 0 1 0 0 3] [0 0 1 0 1 2] [0 0 1 0 2 1]
	[0 0 1 1 0 2] [0 0 1 1 1 1] [0 0 1 1 2 0] [0 0 1 2 0 1] [0 0 1 2 1 0]
	[0 0 1 3 0 0] [0 0 2 0 0 2] [0 0 2 0 1 1] [0 0 2 0 2 0] [0 0 2 1 0 1]
	[0 0 2 1 1 0] [0 0 2 2 0 0] [0 0 3 0 0 1] [0 0 3 0 1 0] [0 0 3 1 0 0]
	[0 0 5 0 0 0] [0 1 0 0 0 3] [0 1 0 0 1 2] [0 1 0 0 2 1] [0 1 0 1 0 2]
	[0 1 0 1 1 1] [0 1 0 1 2 0] [0 1 0 2 0 1] [0 1 0 2 1 0] [0 1 0 3 0 0]
	[0 1 1 0 0 2] [0 1 1 0 1 1] [0 1 1 0 2 0] [0 1 1 1 0 1] [0 1 1 1 1 0]
	[0 1 1 2 0 0] [0 1 2 0 0 1] [0 1 2 0 1 0] [0 1 2 1 0 0] [0 1 4 0 0 0]
	[0 2 0 0 0 2] [0 2 0 0 1 1] [0 2 0 0 2 0] [0 2 0 1 0 1] [0 2 0 1 1 0]
	[0 2 0 2 0 0] [0 2 1 0 0 1] [0 2 1 0 1 0] [0 2 1 1 0 0] [0 2 3 0 0 0]
	[1 0 0 0 0 3] [1 0 0 0 1 2] [1 0 0 0 2 1] [1 0 0 1 0 2] [1 0 0 1 1 1]
	[1 0 0 1 2 0] [1 0 0 2 0 1] [1 0 0 2 1 0] [1 0 0 4 0 0] [1 0 1 0 0 2]
	[1 0 1 0 1 1] [1 0 1 0 2 0] [1 0 1 1 0 1] [1 0 1 1 1 0] [1 0 1 2 0 0]
	[1 0 2 0 0 1] [1 0 2 0 1 0] [1 0 2 1 0 0] [1 0 4 0 0 0] [1 1 0 0 0 2]
	[1 1 0 0 1 1] [1 1 0 0 2 0] [1 1 0 1 0 1] [1 1 0 1 1 0] [1 1 0 2 0 0]
	[1 1 1 0 0 1] [1 1 1 0 1 0] [1 1 1 1 0 0] [1 1 3 0 0 0] [1 2 0 0 0 1]
	[1 2 0 0 1 0] [1 2 0 1 0 0] [1 2 2 0 0 0] [2 0 0 0 0 2] [2 0 0 0 1 1]
	[2 0 0 0 2 0] [2 0 0 1 0 1] [2 0 0 1 1 0] [2 0 0 3 0 0] [2 0 1 0 0 1]
	[2 0 1 0 1 0] [2 0 1 1 0 0] [2 0 3 0 0 0] [2 1 0 0 0 1] [2 1 0 0 1 0]
	[2 1 0 1 0 0] [2 1 2 0 0 0] [2 2 1 0 0 0] [3 0 0 0 0 1] [3 0 0 0 1 0]
	[3 0 0 2 0 0] [3 0 2 0 0 0] [3 1 1 0 0 0] [3 2 0 0 0 0] [4 0 0 1 0 0]
	[4 0 1 0 0 0] [4 1 0 0 0 0] [6 0 0 0 0 0]

FI 関数のときと同様に，FO 関数の入力 Division Property が Vectorial Division Property で表現できるときの伝搬特性表を Algorithm 5 により評価する．Collective Division Property の伝搬特性は各ベクトルから伝搬して得られた Division Property のユニオンとして計算されることに注意されたい．また例として，入力 Division Property が $\mathcal{D}_{\{[1,1,2,3,1,5]\}}^{7,2,7,7,2,7}$ で表現され場合の伝搬特性を表 8.1 に示す．

8.3.3 FL 層に対する Division Property の伝搬特性

MISTY1 は FL 層付きの Feistel 構造を持ち，2 段に 1 回 FL 層が存在し，各 FL 層では 2 つの FL 関数が左 32 ビットと右 32 ビットにそれぞれ適用される．FL 関数では初め，入力の左半分と鍵 $KL_{i,1}$ の AND が計算され，こ

Algorithm 6 Propagation for FL layer

procedure `FLLayerEval`($\mathbb{K}$)
  $\mathbb{K}' \Leftarrow \phi$
  for all $\vec{k} \in \mathbb{K}$ **do**
    $\mathbb{L} \Leftarrow$ `FlEval`$(k_1, k_2, \ldots, k_6)$
    $\mathbb{R} \Leftarrow$ `FlEval`$(k_7, k_8, \ldots, k_{12})$
    for all $\vec{\ell} \in \mathbb{L}$ **do**
      for all $\vec{r} \in \mathbb{R}$ **do**
        $\mathbb{K}' \Leftarrow \mathbb{K}' \cup [\ell_1, \ell_2, \ell_3, \ell_4, \ell_5, \ell_6, r_1, r_2, r_3, r_4, r_5, r_6]$
      end for
    end for
  end for
  return $\mathbb{K}'$
end procedure

procedure `FLEval`$(k_1, k_2, \ldots, k_6)$
  $\mathbb{K}' \Leftarrow \phi$
  $[\ell, c, r] \Leftarrow [k_1 + k_4, k_2 + k_5, k_3 + k_6]$
  for $k'_1 \Leftarrow 0$ to $\min(7, \ell)$ **do**
    for $k'_2 \Leftarrow 0$ to $\min(2, c)$ **do**
      for $k'_3 \Leftarrow 0$ to $\min(7, r)$ **do**
        $(k'_4, k'_5, k'_6) \Leftarrow (\ell - k'_1, c - k'_2, r - k'_3)$
        if $(k'_4 \leq 7) \wedge (k'_5 \leq 2) \wedge (k'_6 \leq 7)$ **then**
          $\mathbb{K}' \Leftarrow \mathbb{K}' \cup [k'_1, k'_2, k'_3, k'_4, k'_5, k'_6]$
        end if
      end for
    end for
  end for
  return `SizeReduce`$(\mathbb{K}')$
end procedure

の AND 値が入力の右半分に排他的論理和される．次に，入力の右半分と鍵 $KL_{i,2}$ の OR が計算され，この OR 値が入力の左半分に排他的論理和される．

FL 関数の入出力は $(\mathbb{F}_2^7 \times \mathbb{F}_2^2 \times \mathbb{F}_2^7 \times \mathbb{F}_2^7 \times \mathbb{F}_2^2 \times \mathbb{F}_2^7)$ の値を取ることから，Division Property $\mathcal{D}_{\mathbb{K}}^{7,2,7,7,2,7}$ を用いて伝搬特性を評価する．Algorithm 6 の `FLEval` は FL 関数に対する伝搬特性を評価する．FL 層は 2 つの FL 関数で構成されるため，Division Property $\mathcal{D}_{\mathbb{K}}^{7,2,7,7,2,7,7,2,7,7,2,7}$ を用いて伝搬特性を考える必要がある．Algorithm 6 の `FLLayerEval` は FL 層に対する伝搬特性を評価する．

Algorithm 7 Path search for r-round characteristics without first FL layer

procedure `Misty1Eval`$(k_1, k_2, \ldots, k_{12}, r)$
  $\mathbb{K} \Leftarrow$ `RoundFuncEval`$(\vec{k})$ ▷ 1st round
  for $i = 1$ to r **do**
    if i is even **then**
      $\mathbb{K} \Leftarrow$ `FlLayerEval`$(\mathbb{K})$ ▷ FL Layer
    end if
    $\mathbb{K} \Leftarrow$ `RoundFuncEval`$(\mathbb{K})$ ▷ (i+1)th round
  end for
  return $\mathbb{K}$
end procedure

procedure `RoundFuncEval`$(\mathbb{K})$
  $\mathbb{K}' \Leftarrow \phi$
  for all $\vec{k} \in \mathbb{K}$ **do**
    for all $\vec{x}$ s.t. $x_j \leq k_j$ for all $j = 1, 2, \ldots, 6$ **do**
      $[r_1, r_2, r_3] \Leftarrow [k_1 - x_1, k_2 - x_2, k_3 - x_3]$
      $[r_4, r_5, r_6] \Leftarrow [k_4 - x_4, k_5 - x_5, k_6 - x_6]$
      $\mathbb{Y} \Leftarrow$ `FOEval`$(x_1, x_2, x_3, x_4, x_5, x_6)$
      for all $\vec{y} \in \mathbb{Y}$ **do**
        $[\ell_1, \ell_2, \ell_3] \Leftarrow [k_7 + y_1, k_8 + y_2, k_9 + y_3]$
        $[\ell_4, \ell_5, \ell_6] \Leftarrow [k_{10} + y_4, k_{11} + y_5, k_{12} + y_6]$
        if $\ell_{j'} \leq 7$ for $j' \in \{1, 3, 4, 6\}$ and $\ell_{j'} \leq 2$ for $j' \in \{2, 5\}$ **then**
          $\mathbb{K}' \Leftarrow \mathbb{K}' \cup [\ell_1, \ell_2, \ell_3, \ell_4, \ell_5, \ell_6, r_1, r_2, r_3, r_4, r_5, r_6]$
        end if
      end for
    end for
  end for
  return `SizeReduce`$(\mathbb{K}')$
end procedure

8.3.4 MISTY1 の Integral 特性探索アルゴリズム

8.3.1 句にて FI 関数に対する Division Property の伝搬特性，8.3.2 句にて FO 関数に対する Division Property の伝搬特性，8.3.3 句にて FL 層に対する Division Property の伝搬特性をそれぞれ示した．これらの伝搬特性を組合せることで，MISTY1 の Integral 特性探索アルゴリズムを構築する．MISTY1 の入出力は 8 個の 7 ビット値と 4 個の 2 ビット値で構成されるため，Division Property $\mathcal{D}_{\mathbb{K}}^{7,2,7,7,2,7,7,2,7,7,2,7}$ を用いて伝搬特性を評価する．

実際に MISTY1 では FL 層が最初に適用されるが，これは Division Property を劣化させる．したがって初めに最初の FL 層を取り除いた MISTY1 に対する Integral 特性を探索する．取り除いた FL 層を通過する手法は次節の鍵回復技術のところで解説する．Algorithm 7 に最初の FL 層を取り除いた MISTY1 の Integral 特性探索アルゴリズムを示す．

結果として，Algorithm 7 を用いることで，最初と最後の FL 層を取り除いて 6 段を覆う Integral 特性を発見した．発見された Integral 特性は 2^{63} 個の選択平文を利用し，ここで先頭 7 ビット中の 1 ビットが定数であり，残りが全て active である選択平文が利用される．このとき，選択平文集合

表 8.2: Propagation from $\mathcal{D}^{7,2,7,7,2,7,7,2,7,7,2,7}_{\{[6,2,7,7,2,7,7,2,7,7,2,7]\}}$

#rounds	0	1	2	FL	3	4	FL	5	6
$\lvert\mathbb{K}\rvert$	1	1	9	16	2596	2617429	12268480	58962	131
$\max_w(\mathbb{K})$	63	63	63	63	62	55	47	27	8
$\min_w(\mathbb{K})$	63	63	61	61	43	19	19	4	1

は Division Proeprty $\mathcal{D}^{7,2,7,7,2,7,7,2,7,7,2,7}_{\{[6,2,7,7,2,7,7,2,7,7,2,7]\}}$ を満足する．したがって，$\vec{k} = [6,2,7,7,2,7,7,2,7,7,2,7]$ を Algorithm 7 の入力として利用する．

表 8.2 に $\mathbb{K}$ のサイズの変遷を整理する．ここで各段数の出力 Division Property において全ての冗長なベクトルを $\mathbb{K}$ から削除した．また $\min_w(\mathbb{K})$ および $\max_w(\mathbb{K})$ は以下の手順で計算される．

$$\min_w(\mathbb{K}) = \min_{\vec{k}\in\mathbb{K}} \left\{ \sum_{i=1}^{12} k_i \right\}, \quad \max_w(\mathbb{K}) = \max_{\vec{k}\in\mathbb{K}} \left\{ \sum_{i=1}^{12} k_i \right\}.$$

6 段計算後，131 個のベクトルが $\mathbb{K}$ に含まれ，詳細には付録 D を参照されたい．131 個のベクトルの中に $(1,0,0,0,0,0,0,0,0,0,0,0)$ が含まれていないことに注目し，これは先頭 7 ビットの和が常に 0 になることを意味する．図 8.4 に発見した 6 段 Integral 特性を示す，ここで和が 0 になるビットストリングを B で表記した．MISTY1 は FL 層があるため Integral 特性を 6 段と記しているが，FL 層がない場合，この 6 段 Integral 特性は 7 段 Integral 特性となり得ることに注意されたい．既存の 4 段 Integral 特性 [HTK04, TSSK08] と比較すると，Integral 特性が覆う段数は 2 段改良されている．

8.2 節で示したように MISTY1 の S_7 は脆弱な性質を持ち，$\mathcal{D}^7_6$ から $\mathcal{D}^7_4$ に伝搬する．興味深いことに，S_7 がこの脆弱な性質を持たないと仮定すると，すなわち `S7Eval` の 26 行目から 30 行目を変更すると，Algorithm 7 は 6 段 Integral 特性を発見できない．

高速実装技術

`SizeReduce` にて全ての冗長なベクトルを取り除く場合，その削除に $O(|\mathbb{K}|^2)$ の計算量を必要とするため Algorithm 7 の実行時間が増加する．したがって，より合理的な手法を考える．

$\mathcal{D}_{\mathbb{K}}$ を Division Property として，$\mathbb{K}$ は冗長なベクトルを持つとする．また冗長なベクトルを全て取り除いた要素を $\mathbb{K}'$ とする．このとき $\mathcal{D}_{\mathbb{K}}$ によって指し示されるパリティが不定となる u の部分集合と $\mathcal{D}_{\mathbb{K}'}$ によって指し示されるパリティが不定となる u の部分集合は一致する．すなわち，仮に `SizeReduce` を実行しなかったとしても伝搬特性に変化はなく，Algorithm 7 の結果は変化しない．したがって `SizeReduce` では大雑把だが高速に冗長なベクトルを削除していく．大雑把な `SizeReduce` では，初め $\mathbb{K}$ の中のベクトルを辞書式順

表 8.3: Propagation from $\mathcal{D}^{6,2,7,7,2,7,7,2,7,7,2,7}_{\{[0,0,0,0,0,0,0,0,7,0,0,7]\}}$

#rounds	0	1	2	FL	3	4	FL
$\lvert\mathbb{K}\rvert$	1	1	460	400	125	12	12
$\max_w(\mathbb{K})$	14	14	14	14	4	2	1
$\min_w(\mathbb{K})$	14	14	4	4	1	1	1

序でソートする．ここでソートされた $|\mathbb{K}|$ 個のベクトルを以下のように表す．

$$\vec{k}^{(1)}, \vec{k}^{(2)}, \ldots, \vec{k}^{(|\mathbb{K}|)}$$

このとき $i < j$ において $\vec{k}^{(i)} \succeq \vec{k}^{(j)}$ を満足する $(\vec{k}^{(i)}, \vec{k}^{(j)})$ は存在しない．そこで，2 つのインデックス $i = 1$ と $j = 2$ を用意し $\vec{k}^{(j)} \succeq \vec{k}^{(i)}$ を検査する．もし $\vec{k}^{(j)} \succeq \vec{k}^{(i)}$ ならば，$\vec{k}^{(j)}$ を取り除き j をインクリメントする．もし $\vec{k}^{(j)} \not\succeq \vec{k}^{(i)}$ ならば j をインクリメントする．さらに，もし “th” 回連続 $\vec{k}^{(j)}$ が取り除けなかった場合，i をインクリメントして $j = i + 1$ とする．このアルゴリズムでは th を自由に設定できる．$th = |\mathbb{K}|$ のとき，このアルゴリズムは完全に冗長なベクトルを削除する．調査した範囲では $th = 10$ や $th = 100$ が最適なパラメータと考えられる．

14 階差分特性の再発見

文献 [THK99] では MISTY1 の 14 階差分特性が示され，この差分特性の理論的な原理は文献 [BF00, CV02] らで議論されている．この 14 階差分では，14 ビット $P^R[10-16, 26-32]$ が active であり，残りが定数の入力集合を用意し，X_5^R の先頭 7 ビットの和が常に 0 になることを利用する．この高階差分特性を Algorithm 7 を用いて発見可能かを評価する．すなわち Algorithm 7 の入力として $\vec{k} = [0, 0, 0, 0, 0, 0, 0, 0, 7, 0, 0, 7]$ を用いて伝搬特性を調査する．表 8.3 に全ての冗長なベクトルを取り除いたうえでの $\mathbb{K}$ の伝搬を整理する．4 番目のラウンド関数の出力は Division Property $\mathcal{D}^{7,2,7,7,2,7,7,2,7,7,2,7}_{\mathbb{K}}$ を満足し，ここで $\mathbb{K}$ は以下の 12 個のベクトルを持つ．

[1,0,0, 0,0,0, 0,0,0, 0,0,0] [0,1,0, 0,0,0, 0,0,0, 0,0,0] [0,0,1, 0,0,0, 0,0,0, 0,0,0]
[0,0,0, 1,0,0, 0,0,0, 0,0,0] [0,0,0, 0,1,0, 0,0,0, 0,0,0] [0,0,0, 0,0,1, 0,0,0, 0,0,0]
[0,0,0, 0,0,0, 2,0,0, 0,0,0] [0,0,0, 0,0,0, 0,1,0, 0,0,0] [0,0,0, 0,0,0, 0,0,1, 0,0,0]
[0,0,0, 0,0,0, 0,0,0, 1,0,0] [0,0,0, 0,0,0, 0,0,0, 0,1,0] [0,0,0, 0,0,0, 0,0,0, 0,0,1]

この結果は X_5^R の先頭 7 ビットの和が常に 0 になること，すなわち文献 [THK99] で示された 14 階差分特性の存在を示している．

46 階差分特性

高階 Integral 特性を得る手法を用いることで 14 階差分特性は 46 階差分特性へと拡張できる．このとき 14 ビット $P^L[10-16, 26-32]$ と 32 ビット P^R

が active であり，残りが定数である選択平文を用意し，X_5^L の先頭 7 ビットの和が常に 0 になることを利用する．同様にして Division Property の伝搬特性を用いて 46 階差分特性を評価した．すなわち Algorithm 7 の入力として $\vec{k} = [0, 0, 7, 0, 0, 7, 7, 2, 7, 7, 2, 7]$ を用いて伝搬特性を調査する．結果として，X_5^L の先頭 16 ビットの和が常に 0 となることが判明した．文献 [HTK04] や文献 [TSSK08] で示された高階 Integral 特性を用いた手法では，和が 0 となるビットは先頭 7 ビットに限られる．一方で Division Proeprty を用いることで，和が 0 となる領域は 7 ビットではなく 16 ビットであることが新たに判明した．

8.4 Full MISTY1 に対する鍵回復攻撃

本節では 8.3 節で示した 6 段 Integral 特性を用いて仕様段数の MISTY1 の秘密鍵を解読する手法を示す．新しく発見された Integral 特性では X_7^L の先頭 7 ビットの和が 0 となる．また，Integral 特性は最初の FL 層を覆っていないため，初めに FL 層を通過する方法を示す．その後 2 つの FL 層および 1 つの FO 関数で用いられるラウンド鍵を推測し，和が 0 になっているか否かを評価して正しいラウンド鍵を推定する．

8.4.1 最初の FL 層を通過する方法

6 段 Integral 特性は最初の FL 層を通過しない．したがって，Integral 特性の入力となる選択テキストを用意するために，初めに $KL_{1,1}$ および $KL_{1,2}$ を推測して選択平文を構成する必用がある．ここで平文の右半分は全ての値を取るため $KL_{2,1}$ および $KL_{2,2}$ を推測する必要がないことに注意されたい．一般的に $KL_{1,1}$ および $KL_{1,2}$ を推測して選択平文を構築する場合，Full Code Book (全ての平文暗号文ペア) を用いた解析となる．しかしながら，推測する鍵ごとに適切に攻撃に利用する選択平文集合を選択することで，Full Code Book を避けた攻撃が可能になる．図 8.5，図 8.6，図 8.7 にそれぞれの場合の選択平文の取り方を示す．各図において，A_i は i ビットが active な入力集合を表す．例として先頭 1 ビットが定数であり，残り 63 ビットが active である選択平文を用いた Integral 特性を考える．右半分は全ての値を同数回取ることから，鍵の推測が必要な FL 層は左側のみである．初めに $KL_{1,2}[1] = 1$ と推測した場合，図 8.5 で示すように選択平文を用意する．次に $(KL_{1,1}[1], KL_{1,2}[1]) = (0, 0)$ と推測した場合，図 8.6 で示すように選択平文を用意する．最後に $(KL_{1,1}[1], KL_{1,2}[1]) = (1, 0)$ と推測した場合，図 8.7 で示すように選択平文を用意する．これらの選択平文は推測したラウンド鍵が正しいとき，それぞれ 6 段 Integral 特性を満足する．また $(1A_{15}\ 1A_{15}\ A_{16}\ A_{16})$

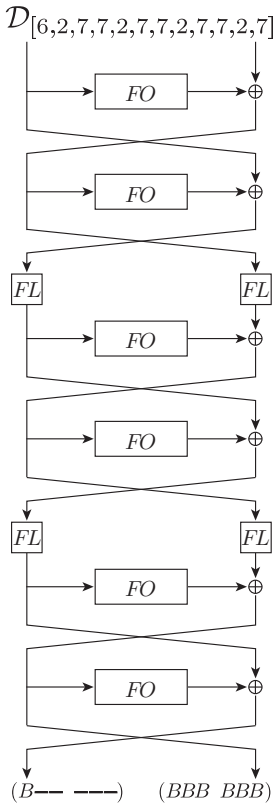


図 8.4: New 6-round integral characteristic

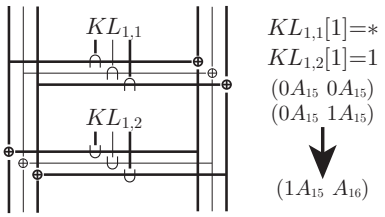


図 8.5: $KL_{1,2} = 1$

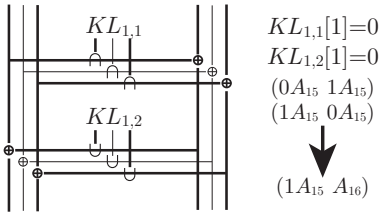


図 8.6: $KL_{1,1} = 0, KL_{1,2} = 0$

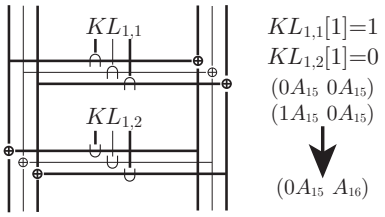


図 8.7: $KL_{1,1} = 1, KL_{1,2} = 0$

となるような 2^{62} 個の選択平文が用いられていないことに注意されたい．すなわち，Integral 特性は $2^{64} - 2^{62} \approx 2^{63.58}$ 個の選択平文を利用する．

8.4.2 Partial-Sum Technique を用いた鍵回復手順

図 8.8 に推測する必要のあるラウンド鍵を示す．初めに $KL_{1,1}[i](= K_1[i])$ および $KL_{1,2}[i](= K'_7[i])$ を推測し，Integral 特性を構築する選択平文を用意する．それぞれの Integral 特性において $X_7^L[1, \ldots, 7]$ の和が 0 になるか否かを評価する．正確には，任意の $j \in \{1, 2, \ldots, 7\}$ において $X_7^L[j]$ の和が 0 になるか否かを Partial-Sum Technique [FKL+00] を用いて評価する．

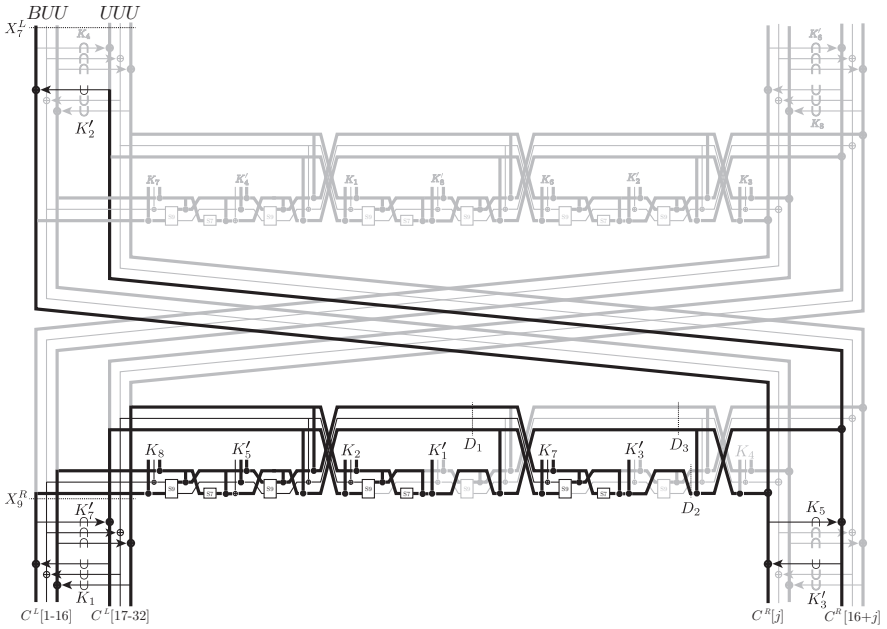


図 8.8: Key recovery step

表 8.4: Procedure of key recovery step

Step	Guessed key	#guessed total bits	New value	Discarded values	#texts	Values in set	Complexity
1		0			2^{34}	$C^L, C^R[j, 16+j]$	
2	K_1, K'_7	32	X_9^R	C^L	2^{34}	$X_9^R, C^R[j, 16+j]$	$2^{34+32} = 2^{66}$
3	K_8, K'_5	64	D_1	$X_9^R[1, \ldots, 16]$	2^{34}	$D_1, X_9^R[17, \ldots, 32], C^R[j, 16+j]$	$2^{34+64} = 2^{98}$
4	$K'_3[j], (K_7)$	65	$D_2[j]$	D_1 w/o $D_1[j]$	2^{20}	$D_1[j], D_2[j], X_9^R[17, \ldots, 32], C^R[j, 16+j]$	$2^{34+65} = 2^{99}$
5	$K_2, (K'_1[j])$	81	$D_3[j]$	$X_9^R[17, \ldots, 32], D_1[j]$	2^4	$D_2[j], D_3[j], C^R[j, 16+j]$	$2^{20+81} = 2^{101}$
6	$K_5[j], K'_2[j]$	83	$X_7^L[j]$	$D_2[j], D_3[j], C^R[j, 16+j]$	2^1	$X_7^L[j]$	$2^{4+83} = 2^{87}$

初めに任意の $j \in \{1, 2, \ldots, 7\}$ において 34 ビット値 $(C^L, C^R[j, 16+j])$ の出現頻度を保存する．その後，ラウンド鍵の一部を推測，出現頻度表のサイズ縮小を繰返し，$X_7^L[j]$ の和を計算する．表 8.4 に鍵回復手順を整理する，ここで各値は図 8.8 内で定義される．

Step 1 34 ビット値 $(C^L, C^R[j, 16+j])$ が出現する回数が偶数回か奇数回かを評価しメモリに保存する．

Step 2 32 ビット鍵 (K_1, K_7') を推測し，C^L から X_9^R を計算する．メモリから C^L を削除し，代わりに X_9^R を保存する．すなわち 34 ビット値 $(X_9^R, C^R[j, 16+j])$ をメモリに保存する．Step 2 の計算量は $2^{34} \times 2^{32} = 2^{66}$ となる．

Step 3 32 ビット鍵 (K_8, K_5') を推測し，X_9^R から D_1 を計算する．メモリから $X_9^R[1, \ldots, 16]$ を削除し，代わりに D_1 を保存する．すなわち 34 ビット値 $(D_1, X_9^R[17, \ldots, 32], C^R[j, 16+j])$ をメモリに保存する．Step 3 の計算量は $2^{34} \times 2^{64} = 2^{98}$ となる．

Step 4 1 ビット鍵 Guess 1-bit $K_3'[j]$ を推測し，Step 2 および Step 3 で推測した (K_7', K_8) から K_7 を計算し，D_1 から $D_2[j]$ を計算する．メモリから $D_1[j]$ を除いた D_1 を削除し，代わりに $D_2[j]$ を保存する．すなわち 20 ビット値 $(D_1[j], D_2[j], X_9^R[17, \ldots, 32], C^R[j, 16+j])$ をメモリに保存する．Step 4 の計算量は $2^{34} \times 2^{65} = 2^{99}$ となる．

Step 5 32 ビット鍵 K_2 を推測し，Step 2 および Step 5 で推測した (K_1, K_2) から $K_1'[j]$ を計算し，$(X_9^R[17, \ldots, 32], D_1[j])$ から $D_3[j]$ を計算する．メモリから $(X_9^R[17, \ldots, 32], D_1[j])$ を削除し，代わりに $D_3[j]$ を保存する．すなわち 4 ビット値 $(D_2[j], D_3[j], C^R[j, 16+j])$ をメモリに保存する．Step 5 の計算量は $2^{20} \times 2^{81} = 2^{101}$ となる．

Step 6 2 ビット鍵 $(K_5[j], K_2'[j])$ を推測し，Step 4 で推測した $K_3'[j]$ を用いて，$(D_2[j], D_3[j], C^R[j, 16+j])$ から $X_7^L[j]$ を計算する．Step 6 の計算量は $2^4 \times 2^{83} = 2^{87}$ となる．

上記手順より，$X_7^L[j]$ の和を評価するために必要な計算量は

$$2^{66} + 2^{98} + 2^{99} + 2^{101} + 2^{87} \approx 2^{101.5}$$

である．上記手順を任意の $j \in \{1, 2, \ldots, 7\}$ に対して繰り返すため，鍵回復手順の全体の計算量は $7 \times 2^{101.5} = 2^{104.3}$ となる．

鍵回復手順では以下に示す 124 ビット鍵

$$K_1, K_2, K_5[1, \ldots, 7], K_7, K_8,$$
$$K_1'[1, \ldots, 7], K_2'[1, \ldots, 7], K_3'[1, \ldots, 7], K_5', K_7'$$

を推測する必用がある．ここで K_7' および $K_1'[1,\ldots,7]$ は K_7, K_8 および K_1, K_2 を推測することでそれぞれ一意に決定できる．したがって推測される鍵ビットサイズは

$$K_1, K_2, K_5[1,\ldots,7], K_7, K_8,$$
$$K_2'[1,\ldots,7], K_3'[1,\ldots,7], K_5',$$

まで削減され，そのビットサイズは 101 ビットである．さらに，Integral 特性を構成するために既に 2 ビット鍵 $K_1[i]$ および $K_7'[i]$ を推測しているため，鍵回復手順で推測される鍵ビットサイズは 99 ビットである．誤った鍵において，$X_7^L[1,\ldots,7]$ の和が 0 となる確率は 2^{-7} である．したがって Integral 特性を用いることで，平均 $2^{99}\times 2^{-7} = 2^{92}$ 個のラウンド鍵候補が得られる．最後に以下に示す 27 ビット鍵

$$K_5[8,\ldots,16], K_2'[8,\ldots,16], K_3'[8,\ldots,16]$$

を推測する．K_3，K_4，K_6 は (K_2, K_2')，(K_3, K_3')，(K_5, K_5') をそれぞれ推測することで一意に求められる．したがって全体の計算量は $2^{92+27} = 2^{119}$ となる．2^{119} 個の秘密鍵候補から正しい秘密鍵を得るために 2 つの平文暗号文ペアを利用して，正しい鍵を探索する．これは $2^{119} + 2^{119-64} \approx 2^{119}$ の計算量で実行可能である．上記手順を $(K_1[i], K_7'[i]) \in \{(0,0),(0,1),(1,0),(1,1)\}$ に対して繰返し実行するため，Integral 攻撃全体に要する計算量は $4\times 2^{119} = 2^{121}$ となる．

8.4.3 Time and Data Complexity のトレードオフ

8.4.2 句では，$(2^{64} - 2^{62})$ 個の選択平文を用いて秘密鍵の解読を試みた．ここで誤った鍵が削除されない確率は 2^{-7} のため，最後の秘密鍵を力任せに探索するフェーズにて $2^{128-7} = 2^{121}$ の計算量が必要となる．そして，この計算量は Partial-Sum Technique による計算量を上回る．したがって，更に多くの選択平文数を用いて誤った鍵が削除される確率を大きくすることで，秘密鍵を解読するための全体の計算量を低下させることができる．

7 ビットの和が 0 であるような Integral 特性を構成するために，初めに acitve としない定数ビット位置を $i \in \{1,2,\ldots,7\}$ の 7 ビットから選択する．$i = 1$ なビットを定数ビットとして選択した場合，P^L が以下の値を満足する選択平文を利用する．

$$(00A_{14}\ \ 00A_{14}), (00A_{14}\ \ 01A_{14}), (01A_{14}\ \ 00A_{14}), (01A_{14}\ \ 01A_{14}),$$
$$(00A_{14}\ \ 10A_{14}), (00A_{14}\ \ 11A_{14}), (01A_{14}\ \ 10A_{14}), (01A_{14}\ \ 11A_{14}),$$
$$(10A_{14}\ \ 00A_{14}), (10A_{14}\ \ 01A_{14}), (11A_{14}\ \ 00A_{14}), (11A_{14}\ \ 01A_{14}),$$

表 8.5: Trade-off between time and data complexity

#characteristics	partial-sum part	brute-force part	Total
1	$1 \times 4 \times 2^{104.3}$	2^{121}	2^{121}
2	$2 \times 4 \times 2^{104.3}$	2^{114}	2^{114}
3	$3 \times 4 \times 2^{104.3}$	2^{107}	$2^{108.5}$
4	$4 \times 4 \times 2^{104.3}$	2^{100}	$2^{108.3}$
5	$5 \times 4 \times 2^{104.3}$	2^{93}	$2^{108.6}$

ここで A_{14} は他のビットと独立に全ての値を取る集合を意味する．また P^R は全ての値を取ることとする．したがって，例に $(00A_{14} \quad 00A_{14})$ は 2^{60} 個の選択平文を表す．さらに $i = 2$ なビットを定数ビットとして選択した場合，P^L が以下の値を満足する選択平文を利用する．

$$(00A_{14} \quad 00A_{14}), (00A_{14} \quad 10A_{14}), (10A_{14} \quad 00A_{14}), (10A_{14} \quad 10A_{14}),$$
$$(00A_{14} \quad 01A_{14}), (00A_{14} \quad 11A_{14}), (10A_{14} \quad 01A_{14}), (10A_{14} \quad 11A_{14}),$$
$$(01A_{14} \quad 00A_{14}), (01A_{14} \quad 10A_{14}), (11A_{14} \quad 00A_{14}), (11A_{14} \quad 10A_{14}).$$

両方の Integral 特性が使われるとき，P^L が $(11A_{14} \quad 11A_{14})$ となるような選択平文が利用されないことに注意されたい．したがって $(2^{64} - 2^{60})$ 個の選択平文を用いることで，誤った鍵が削除されない確率を 2^{-14} まで減少させることができる．同様に，3 つの Integral 特性を用いる，すなわち $(2^{64} - 2^{58})$ 個の選択平文を用いることで，誤った鍵が削除されない確率を 2^{-21} まで減少させることができる．

表 8.5 に攻撃に必要な計算量およびデータ量のトレードオフを整理する．各特性において，$(KL_{1,1}[1], KL_{1,2}[1]) \in \{(0,1), (1,1), (0,0), (1,0)\}$ を推測し，Partial-Sum Technique を用いて秘密鍵候補の削減を実行する．表 8.5 より 4 つの Integral 特性を利用するときが最適となる．すなわち $(2^{64} - 2^{56}) \approx 2^{63.994}$ 個の選択平文を用いたとき，秘密鍵を解読するために必要な計算量は最小化され，$2^{108.3}$ となる．

8.4.4 Bar-On の最適化

Cryptology ePrint Archive に，MISTY1 の鍵回復手順を最適化する手法が Bar-On によって示された [Bar15]．この手法では同様の 6 段 Integral 特性を用いるが，異なる鍵回復手順を利用する．初めに選択平文攻撃ではなく選択暗号文攻撃を利用する．これは最初 1 段のラウンド鍵を推測する手順が最後 1 段のラウンド鍵を推測する手順より効率的に実行可能なことに起因する．さらに Integral 攻撃の鍵回復手順を最適化する手法の一つである中間一致技術 [SW12] を利用する．結果として秘密鍵を解読するために必要な計算量は

劇的に減少し $2^{69.5}$ となる．一方で計算量を上述のものまで減らすためには Full Code Book を利用する必用がある．

8.5 今後の MISTY1 の安全性に関して

本レポートで報告した攻撃を実行するためには，少なくとも $2^{63.58}$ 個の選択平文暗号文ペアを収集する必用がある．また Bar-On の最適化により，MISTY1 の安全性は $2^{69.5}$ まで下回ったが，Bar-On の最適化は常に $2^{63.58}$ 個以上の選択平文を要求する．したがって現在知られている 2 つの解析手法は共に MISTY1 の現実的な利用における安全性を脅かすものではない．また上述した選択平文暗号文ペアが現実的に収集可能な未来では，64 ビットブロック暗号の利用そのものが控えられるべきである．一方で MISTY1 の今後の新規利用は控えるべきである．MISTY1 のセキュリティレベルが 70 ビット前後まで低下したことは事実であり，より優れた暗号方式の採用が推奨される．

上述した通り，本レポートで報告した攻撃手法は，今後改良されないという仮定において，MISTY1 の現実的な利用における安全性を脅かすものではない．したがって攻撃手法の改良可能性に関する議論は重要である．本レポートで報告した攻撃手法および Bar-On の最適化手法はともに共通の Integral 特性を利用し，この Integral 特性を構築するために $2^{63.58}$ 個の選択平文が求められることが，MISTY1 の利用が依然として現実的環境では危険ではないと判断する根拠である．したがって，より少ない選択平文数で同様の Integral 特性が発見された場合，MISTY1 の現実的な環境における安全性は大きく損なわれることとなる．MISTY1 の Integral 特性を改良できる可能性を示唆する一つの傍証として，12 階差分特性およびその拡張である 44 階差分特性の存在がある [TSKN12]．文献 [TSKN12] では 3 段 MISTY1 をブール関数で表現することにより 12 階差分特性の存在を示した．この 12 階差分特性は高階 Integral 特性を構築する手法を用いて 44 階差分特性に拡張可能である．Division Property の伝搬特性は 46 階差分特性 [HTK04, TSSK08] の存在証明および改良を示した．一方で 12 階差分特性および 44 階差分特性の存在は証明できていない．これは Division Property の伝搬特性は力任せな手法 (数式処理システム等を用いてブール関数を導出する手法) と比較すると誤差があることを意味する．Division Property は力任せな手法よりも高効率なため，より多くの active ビット数を持つ Integral 特性を現実的な時間で発見できる．しかし正確さでは力任せな手法より劣っている．

Division Property を用いた場合においても，さらに Integral 特性を改良できる可能性が残されている．本レポートで示した Integral 特性は実際の MISTY1 を含んだ特定の暗号群に対して有効である．例に Division Property の伝搬特性が共通な S_9 および S_7 を利用した場合，この MISTY1 ライクな暗号も同様の Integral 特性を持つ．MISTY1 の詳細な構造を利用した Integral

特性を Division Property を用いて探索したい場合，例に $\mathcal{D}_{\mathbb{K}}^{1^{64}}$ な Division Property を利用する．このとき MISTY1 の S-box の詳細な構造を利用した伝搬特性を探索でき，結果として Integral 特性を改良できる可能性がある．

第9章　各暗号方式への応用に向けて

本章では Division Property を用いた解析の応用に関して考察を述べる．初めに文献 [ZW15] で提案された一般化 Feistel 構造への応用および LBlock [WZ11], TWINE [SMMK12] に対する Integral 攻撃を示す．その後，CRYPTREC 暗号リストに記載されている暗号をはじめ，様々な暗号方式への応用に関する所感を述べる．

9.1　一般化 Feistel 構造への適用

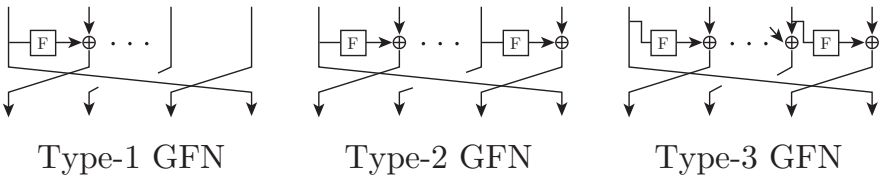


図 9.1: Three generalized Feistel networks

Feistel 構造はラウンド関数の入出力を 2 つに分割し，これらの 2 つのデータを F 関数を用いながら撹拌する．一般化 Feistel 構造はラウンド関数の入出力を m ($m > 2$) 個に分割して処理を行う [ZMI89]．文献 [ZMI89] では Type-1, Type-2，Type-3 な一般化 Feistel 構造が導入された．各方式において 1 ラウンド関数は，それぞれの F 関数を適用後に各ブランチの位置をローテーションする構造を持つ．図 9.1 に各 Type のラウンド関数を示す．

Zhang らは Type-1 一般化 Feistel 構造に対して Division Property の伝搬特性を調査した [ZW15].

Theorem 1. For Type-1 Generalized Feistel Network (GFN) whose number of branches is m ($m \leq 16$) and F-functions are bijective, there always exist integral distinguishers that covers $m^2 + m - 1$ rounds. Moreover, when F-functions are non-bijective, there always exist integral distinguishers that covers $m^2 + m - 2$ rounds.

表 9.1: Propagation of division property for Type-2 GFN

Round	Division property
0	[n-1,n,n,n]
1	[n,n,n,n-1]
2	[n,n,n-1,n], [n,1,n,n]
3	[n,n-1,n,n], [1,n,n,n], [2,n,n,1]
4	[n-1,n,n,n], [n,n,n,1], [n,n,1,2], [n,1,2,2]
5	[n,n,1,n], [n,1,2,n], [1,2,2,n], [2,2,2,1], [1,0,3,n], [2,0,3,1]
6	[2,2,1,2], [0,3,n,1], [3,2,1,0], [0,3,1,2], [1,3,1,0], [0,0,2,2], [1,0,2,0]
7	[2,1,0,3], [3,1,0,0], [0,2,2,0], [0,0,3,0], [0,2,0,1], [1,2,0,0], [0,0,1,1], [1,0,1,0]
8	[1,0,0,3], [2,0,0,0], [0,3,0,0], [0,0,1,0], [0,1,0,1] [1,1,0,0]
9	[0,0,0,2], [1,0,0,0], [0,1,0,0], [0,0,1,0]

同様に Type-2 一般化 Feistel 構造では以下の Theorem が成立する．

Theorem 2. For Type-2 Generalized Feistel Network (GFN) whose number of branches is m ($m \leq 16$) and F-functions are bijective, there always exist integral distinguishers that covers $2m+1$ rounds. Moreover, when F-functions are non-bijective, there always exist integral distinguishers that covers $2m$ rounds.

具体例として 4 ブランチ Type-2 GFN に対する Division Property の伝搬特性を表 9.1 に示す．

9.2 LBlock および TWINE への適用

文献 [SM10] にて一般化 Feistel 構造の改良が示された．Block Shuffle GFN (BSGFN) と呼ばれるこの改良手法では，F 関数を適用後に各ブランチの位置の移動をローテーションに限定せず，固定の任意の入替えによって移動する．結果として，ブランチの本数が 6 以上のとき，通常の GFN と比較してより少ない段数で Full Diffusion に到達できる入替えパターンが存在することが示された．この設計理論に基づく暗号方式として LBlock [WZ11] および TWINE [SMMK12] がある．両方式ともブランチの本数が 16 である Type-2 BSGFN 構造を有し，F 関数には全単射な 4 ビット S-box が用いられる．

LBlock および TWINE の Integral 特性を評価する．それぞれの提案者は Integral Property の伝搬特性を利用した解析を示しており，両方式とも 15 段 Integral 特性を有することが示されている [WZ11, SMMK12]．Zhang らは一般化 Feistel 構造と同様に，Division Property の伝搬特性を用いて両方式の Integral 特性を探索した [ZW15]．結果として，2^{63} 個の選択平文を利用することで，両方式ともに 16 段 Integral 特性が存在することが示された．

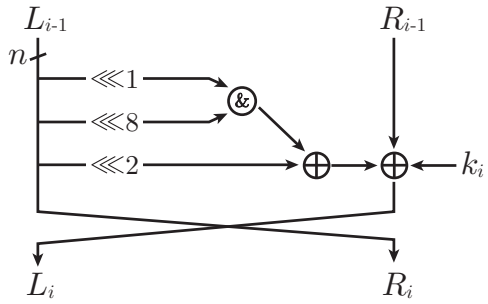


図 9.2: Round function of Simon $2n$

9.3 Simon への適用

Simon は NSA が 2013 年に提案した Feistel 構造を有する軽量ブロック暗号である [BSS+13]．Simon は異なるブロック長をサポートし，Simon $2n$ は $2n$ ビットのブロック長を持つ Simon を表す．ここで n は 16, 24, 32, 48, 64 からそれぞれ選ばれる．さらに mn ビット秘密鍵を用いる Simon $2n$ は Simon $2n/mn$ と表記される．

i 番目のラウンド関数の出力 (L_i, R_i) は以下の手順で計算される．

$$(L_i, R_i) = (L_{i-1}^{\lll 1} \wedge L_{i-1}^{\lll 8}) \oplus L_{i-1}^{\lll 2} \oplus R_{i-1} \oplus k_i, L_{i-1})$$

ここで $L^{\lll j}$ は L を左に j ビットローテーションした値を表し，k_i は i 番目のラウンド鍵を表す．また (L_0, R_0) は平文を表す．Simon のラウンド関数は `and`, `rotation`, `xor` で構成され，図 9.2 に Simon $2n$ のラウンド関数を示す．詳細には文献 [BSS+13] を参照されたい．

9.3.1 Simon の Integral 特性

Simon は S-box を利用しない暗号方式であり，このような暗号の Integral 特性を探索することは非常に困難である．文献 [WLV+14] にて，著者らは Simon 32 の Integral 特性を実験的に評価した．この実験ではランダムに選択された 2^{13} 個の秘密鍵に対して，左 1 ビットを定数にして残りを active とした 2^{31} 個の選択平文を利用した Integral 特性の調査が行われた．結果として 2^{13} 個の全ての鍵において Simon 32 は 15 段 Integral 特性を持つことが確認された．したがって著者らは少なくとも $1 - 1^{-13}$ の確率で Simon 32 の 15 段 Integral 特性が成立するとし，この Integral 特性を利用して 21 段 Simon 32 を攻撃した．

理論的に存在が確認された Integral 特性は Division Property を利用して文献 [Tod15b] で報告された．これは Simon $2n$ を $(n, 2)$-Feistel と近似して評価され，結果として Simon 32, 48, 64, 96, 128 が 9, 11, 11, 13, 13 段 Integral

特性をそれぞれ持つことが示された．Simon ではラウンド鍵が F 関数適用後に排他的論理和される．この構造を持つ場合，文献 [WLV+14] で示された手法を用いることで 1 段拡張した Integral 特性を鍵を推測することなく構成できる．したがって文献 [Tod15b] で存在を証明された Integral 特性は 10, 12, 12, 14, 14 段 Integral 特性となる．ここで Simon 32 の結果に注目する．実験的な手法では 15 段 Integral 特性が示されたのに対し，$(n, 2)$-Feistel への適用では 10 段 Integral 特性のみが示された．すなわち実験と証明の間には 5 段の隔たりがあることが分かる．

文献 [ZWW15] では Division Property とは異なる手法で Integral 特性の存在を証明する手法が提案された．この手法ではラウンド関数の $2n$ ビット出力の各ビットが平文の active ビットからどのような次数の ANF で記述できるかを評価する．したがって active ビット数が増えれば増えるほど莫大な計算量を必要とする．そこで文献 [ZWW15] では初め少ない active ビット数から Integral 特性を順方向に探索し，その後，文献 [ZSW+12] で提案された高階 Integral 特性を探索するアルゴリズムを適用する．結果として Simon 32, 48, 64, 96, 128 が 13, 14, 17, 21, 25 段 Integral 特性をそれぞれ持つことが示された．Simon 32 の結果に注目すると依然として実験と証明の間には 2 段の隔たりがあることが分かる．

文献 [TM16] では Division Property の派生として Bit-Based Division Property が提案された．文献 [Tod15b] において Division Property が十分な Simon の Integral 特性を示せなかった理由は，Simon $2n$ を $(n, 2)$-Feistel と近似していたことに起因する．すなわち $\mathcal{D}_{\mathbb{K}}^{n^2}$ を用いて伝搬特性を評価していた．文献 [TM16] では初め Conventional Bit-Based Division Property として $\mathcal{D}_{\mathbb{K}}^{1^n}$ を用いた伝搬特性が評価された．その結果 Simon 32 は 14 段 Integral 特性を持つことが示され，文献 [ZWW15] の結果から 1 段改良した．一方で実験と証明の間には 1 段の隔たりがあることが分かる．文献 [TM16] では，さらに Division Property の新しい派生型として Bit-Based Division Property using Three Subsets が提案された．通常の Division Property ではパリティが 0 か不定かに注目して u の集合を分割するのに対し，新しい派生型ではパリティが 0 か 1 か不定かに注目して u の集合を分割する．この新しい派生型を持って Simon 32 の Integral 特性を再度評価した結果，Simon 32 は 15 段 Integral 特性を持つこと (和が 0 となるビットの位置も含めて) が証明された．一方で Bit-Based Division Property では active ビット数が多い Integral 特性を探索することは実行不可能である．したがって Simon 32 以外の Simon に関しては文献 [ZSW+12] で示された高階 Integral 特性を探索するアルゴリズムとの併用が必要となる．高階 Integral 特性を探索するアルゴリズムを併用せずに妥当な Integral 特性を探索するアルゴリズムは未解決問題である．

9.4 電子政府推奨暗号リストへの適用に関する展望

AES 以外の CRYPTRECT 電子政府推奨暗号リストに対しては Division Property は適用されていない．本節では各暗号方式に対して Division Property を適用する場合の課題を整理する．

9.4.1 Camellia

Camellia [AIK+00] は代数次数 7 である 8 ビット S-box を用いた 128 ビット Feistel 型ブロック暗号である．Camellia を単純に $(64, 7)$-Feistel と近似し，$\mathcal{D}_{\mathbb{K}}^{64^2}$ とした場合の結果は既に表 4.3 に記載されている．しかしながら Camellia の構造を考慮すると $\mathcal{D}_{\mathbb{K}}^{8^{16}}$ を利用することが妥当と考えられる．また線形関数の P 関数が 2 進行列であることを利用した伝搬特性を評価することが推奨される．さらに Camellia は 6 段ごとに FL 層があり，この FL 層では 1 ビットのローテーションが計算される．したがって，このローテーションを考慮に入れた伝搬特性を評価する必用がある．

9.4.2 DES

電子政府推奨暗号リストに掲載されているのは 3-key Triple DES だが，Division Property の伝搬は各ラウンドごと独立に評価するため DES [U.S77] に対する伝搬特性と 3-key Triple DES に対する伝搬特性は一致する．Camellia と同様に DES を単純に $(32, 5)$-Feistel と近似し，$\mathcal{D}_{\mathbb{K}}^{32^2}$ とした場合の結果は既に表 4.3 に記載されている．DES は 6 ビット入力 4 ビット出力な S-box を利用するが，関数 E, 関数 P はビット置換である．ビット置換の脆弱性を十分に利用するために $\mathcal{D}_{\mathbb{K}}^{1^{64}}$ といった Bit-Based Division Property の利用が推奨される．しかしながら 64 ビットブロック暗号に対して Bit-Based Division Property の伝搬を評価することは非現実的である．したがってビット置換の構造を出来る限り利用しながら，$\mathcal{D}_{\mathbb{K}}^{4^{16}}$ を利用することが妥当と考えられる．

9.4.3 KCipher-2

KCipher-2 [KTS07] はストリーム暗号であるため，Integral 攻撃のフレームワークが正当に機能するかは議論の余地がある．しかしながらストリーム暗号に対しても選択 IV 攻撃を取ることで，内部状態の初期化ステップ解析には有効に利用可能と期待する．一方で KCipher-2 は内部関数に modular addition を持つ．modular addition はビットごとに次数に大きな偏りが生じる非線形関数である．この偏りを利用しないかぎりは有効な Integral 特性は発見できないと考えられる．偏りを利用する一つの手法として Bit-Based Division

Property があるが，やはり内部状態のビット長が非常に膨大であることから
非現実的である．

第10章　まとめ

本レポートでは Division Property の解説と共に，AES および MISTY1 への適用を解説した．

AES のように代数次数の大きな S-box を利用した暗号に対しては，Division Property により得られる恩恵は従来のものと比較して大きくはない．一方で AES に関しては Division Property を用いることで，従来の手法では発見できなかった特性を少なからず発見できている．これらの非自明な特性の有効活用法は今後の検討課題である．

MISTY1 のように S-box の入出力ビット長に対して代数次数が小さい場合，Division Property の恩恵は非常に大きい．従来手法では発見不可能な多くの Integral 特性を Division Property を用いることで発見できる．

一般的に n ビットブロック暗号において代数次数が $n-1$ に到達する段数を超えれば Integral 特性は発見できない．Division Property を利用した解析の結果，代数次数は初め効率よく上昇するがブロック長に近くなればなるほど上昇が鈍化することが分かった．すなわち，ほぼ Full Code Book を利用することで Integral 特性の覆う段数を以前知られていた以上に伸ばすことができるようになったと解釈できる．したがってセキュリティビット長よりもブロック長の方が大きな暗号方式に対しては，Division Property による解析が有効な解析になるとは期待できない．一方で，軽量暗号のように，ブロック長よりもセキュリティビット長が大きい暗号方式は，Division Property による解析が有効と考えられる．

関連図書

[ABB+14] Elena Andreeva, Begül Bilgin, Andrey Bogdanov, Atul Luykx, Florian Mendel, Bart Mennink, Nicky Mouha, Qingju Wang, and Kan Yasuda. PRIMATEs v1.02, 2014. Submission to CAESAR competition.

[ABK98] Ross Anderson, Eli Biham, and Lars Knudsen. Serpent: A proposal for the Advanced Encryption Standard, 1998. One of the five finalists of the AES contest.

[AIK+00] Kazumaro Aoki, Tetsuya Ichikawa, Masayuki Kanda, Mitsuru Matsui, Shiho Moriai, Junko Nakajima, and Toshio Tokita. Camellia: A 128-bit block cipher suitable for multiple platforms - design and analysis. In Douglas R. Stinson and Stafford E. Tavares, editors, *SAC*, volume 2012 of *LNCS*, pages 39–56. Springer, 2000.

[Bar15] Achiya Bar-On. A 2^{70} attack on the full MISTY1. *IACR Cryptology ePrint Archive*, 2015:746, 2015.

[BBS99] Eli Biham, Alex Biryukov, and Adi Shamir. Cryptanalysis of skipjack reduced to 31 rounds using impossible differentials. In Jacques Stern, editor, *EUROCRYPT*, volume 1592 of *LNCS*, pages 12–23. Springer, 1999.

[BC13] Christina Boura and Anne Canteaut. On the influence of the algebraic degree of f^{-1} on the algebraic degree of G $\circ$ F. *IEEE Transactions on Information Theory*, 59(1):691–702, 2013.

[BCC11] Christina Boura, Anne Canteaut, and Christophe De Cannière. Higher-order differential properties of Keccak and *Luffa*. In Antoine Joux, editor, *FSE*, volume 6733 of *LNCS*, pages 252–269. Springer, 2011.

[BF00] Steve Babbage and Laurent Frisch. On MISTY1 higher order differential cryptanalysis. In Dongho Won, editor, *ICISC*, volume 2015 of *LNCS*, pages 22–36. Springer, 2000.

[BKL+07] Andrey Bogdanov, Lars R. Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew J. B. Robshaw, Yannick Seurin, and C. Vikkelsoe. PRESENT: an ultra-lightweight block cipher. In Pascal Paillier and Ingrid Verbauwhede, editors, *CHES*, volume 4727 of *LNCS*, pages 450–466. Springer, 2007.

[BR03] Paulo S. L. M. Barreto and Vincent Rijmen. The Whirlpool hashing function, 2003. submitted to the NESSIE project, available at http://www.larc.usp.br/~pbarreto/WhirlpoolPage.html.

[BS90] Eli Biham and Adi Shamir. Differential cryptanalysis of DES-like cryptosystems. In Alfred Menezes and Scott A. Vanstone, editors, *CRYPTO*, volume 537 of *LNCS*, pages 2–21. Springer, 1990.

[BSS+13] Ray Beaulieu, Douglas Shors, Jason Smith, Stefan Treatman-Clark, Bryan Weeks, and Louis Wingers. The SIMON and SPECK families of lightweight block ciphers. *IACR Cryptology ePrint Archive*, 2013:404, 2013.

[CRY13] CRYPTREC. Specifications of e-government recommended ciphers. available at http://www.cryptrec.go.jp/english/method.html, 2013.

[CSW08] Christophe De Cannière, Hisayoshi Sato, and Dai Watanabe. Hash function *Luffa* - a SHA-3 candidate, 2008. Available at http://hitachi.com/rd/yrl/crypto/luffa/round1archive/Luffa_Specification.pdf.

[CV02] Anne Canteaut and Marion Videau. Degree of composition of highly nonlinear functions and applications to higher order differential cryptanalysis. In Lars R. Knudsen, editor, *EUROCRYPT*, volume 2332 of *LNCS*, pages 518–533. Springer, 2002.

[DBPA11] Joan Daemen, Guido Bertoni, Michaël Peeters, and Gilles Van Assche. The Keccak reference version 3.0, 2011.

[DEMS14] Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Martin Schläffer. Ascon v1, 2014. Submission to CAESAR competition.

[DKR97] Joan Daemen, Lars R. Knudsen, and Vincent Rijmen. The block cipher Square. In Eli Biham, editor, *FSE*, volume 1267 of *LNCS*, pages 149–165. Springer, 1997.

[DPAR00] Joan Daemen, Michaël Peeters, Gilles Van Assche, and Vincent Rijmen. The NOEKEON block cipher., 2000. submitted to the NESSIE project, available at http://gro.noekeon.org/.

[DR02] Joan Daemen and Vincent Rijmen. *The Design of Rijndael: AES - The Advanced Encryption Standard*. Information Security and Cryptography. Springer, 2002.

[FKL+00] Niels Ferguson, John Kelsey, Stefan Lucks, Bruce Schneier, Michael Stay, David Wagner, and Doug Whiting. Improved cryptanalysis of Rijndael. In Bruce Schneier, editor, *FSE*, volume 1978 of *LNCS*, pages 213–230. Springer, 2000.

[GPP11] Jian Guo, Thomas Peyrin, and Axel Poschmann. The PHOTON family of lightweight hash functions. In Phillip Rogaway, editor, *CRYPTO*, volume 6841 of *LNCS*, pages 222–239. Springer, 2011.

[GPPR11] Jian Guo, Thomas Peyrin, Axel Poschmann, and Matthew J. B. Robshaw. The LED block cipher. In Bart Preneel and Tsuyoshi Takagi, editors, *CHES*, volume 6917 of *LNCS*, pages 326–341. Springer, 2011.

[HTK04] Yasuo Hatano, Hidema Tanaka, and Toshinobu Kaneko. Optimization for the algebraic method and its application to an attack of MISTY1. *IEICE Transactions*, 87-A(1):18–27, 2004.

[ISO05] ISO/IEC. JTC1: ISO/IEC 18033: Security techniques – encryption algorithms – part 3: Block ciphers, 2005.

[KLL+14] Elif Bilge Kavun, Martin Mehl Lauridsen, Gregor Leander, Christian Rechberger, Peter Schwabe, and Tolga Yalçin. PRØST v1.1, 2014. Submission to CAESAR competition.

[Knu94] Lars R. Knudsen. Truncated and higher order differentials. In Bart Preneel, editor, *FSE*, volume 1008 of *LNCS*, pages 196–211. Springer, 1994.

[KTS07] Shinsaku Kiyomoto, Toshiaki Tanaka, and Kouichi Sakurai. K2: A stream cipher algorithm using dynamic feedback control. In Javier Hernando, Eduardo Fernández-Medina, and Manu Malek, editors, *SECRYPT*, pages 204–213. INSTICC Press, 2007.

[KW02] Lars R. Knudsen and David Wagner. Integral cryptanalysis. In Joan Daemen and Vincent Rijmen, editors, *FSE*, volume 2365 of *LNCS*, pages 112–127. Springer, 2002.

[Lai94] Xuejia Lai. Higher order derivatives and differential cryptanalysis. In *Communications and Cryptography*, volume 276 of *The Springer International Series in Engineering and Computer Science*, pages 227–233, 1994.

[Luc01] Stefan Lucks. The saturation attack - A bait for Twofish. In Mitsuru Matsui, editor, *FSE*, volume 2355 of *LNCS*, pages 1–15. Springer, 2001.

[LWZ11] Yanjun Li, Wenling Wu, and Lei Zhang. Improved integral attacks on reduced-round CLEFIA block cipher. In Souhwan Jung and Moti Yung, editors, *WISA*, volume 7115 of *LNCS*, pages 28–39. Springer, 2011.

[Mat93] Mitsuru Matsui. Linear cryptanalysis method for DES cipher. In Tor Helleseth, editor, *EUROCRYPT*, volume 765 of *LNCS*, pages 386–397. Springer, 1993.

[Mat96] Mitsuru Matsui. New structure of block ciphers with provable security against differential and linear cryptanalysis. In Dieter Gollmann, editor, *FSE*, volume 1039 of *LNCS*, pages 205–218. Springer, 1996.

[Mat97] Mitsuru Matsui. New block encryption algorithm MISTY. In Eli Biham, editor, *FSE*, volume 1267 of *LNCS*, pages 54–68. Springer, 1997.

[MGH+14] Pawe? Morawiecki, Kris Gaj, Ekawat Homsirikamol, Krystian Matusiewicz, Josef Pieprzyk, Marcin Rogawski, Marian Srebrny, and Marcin Wøjcik. ICEPOLE v1, 2014. Submission to CAESAR competition.

[NES04] NESSIE. New european schemes for signatures, integrity, and encryption. available at https://www.cosic.esat.kuleuven.be/nessie/, 2004.

[NK95] Kaisa Nyberg and Lars R. Knudsen. Provable security against a differential attack. *J. Cryptology*, 8(1):27–37, 1995.

[OM00] Hidenori Ohta and Mitsuru Matsui. A description of the MISTY1 encryption algorithm. available at https://tools.ietf.org/html/rfc2994, 2000.

[SM10] Tomoyasu Suzaki and Kazuhiko Minematsu. Improving the generalized Feistel. In *FSE*, volume 6147 of *LNCS*, pages 19–39, 2010.

[SMMK12] Tomoyasu Suzaki, Kazuhiko Minematsu, Sumio Morioka, and Eita Kobayashi. $\textnormal{\textsc{TWINE}}$: A lightweight block cipher for multiple platforms. In Lars R. Knudsen and Huapeng Wu, editors, *SAC*, volume 7707 of *LNCS*, pages 339–354. Springer, 2012.

[STA+14] Yu Sasaki, Yosuke Todo, Kazumaro Aoki, Yusuke Naito, Takeshi Sugawara, Yumiko Murakami, Mitsuru Matsui, and Shoichi Hirose. Minalpher v1, 2014. Submission to CAESAR competition.

[SW12] Yu Sasaki and Lei Wang. Meet-in-the-middle technique for integral attacks against Feistel ciphers. In Lars R. Knudsen and Huapeng Wu, editors, *SAC*, volume 7707 of *LNCS*, pages 234–251. Springer, 2012.

[THK99] Hidema Tanaka, Kazuyuki Hisamatsu, and Toshinobu Kaneko. Strenght of MISTY1 without FL function for higher order differential attack. In Marc P. C. Fossorier, Hideki Imai, Shu Lin, and Alain Poli, editors, *AAECC-13*, volume 1719 of *LNCS*, pages 221–230. Springer, 1999.

[TM16] Yosuke Todo and Masakatu Morii. Bit-based division property and application to Simon family. In *FSE*, 2016. (accepted).

[Tod15a] Yosuke Todo. Integral cryptanalysis on full MISTY1. In Rosario Gennaro and Matthew Robshaw, editors, *CRYPTO Part I*, volume 9215 of *LNCS*, pages 413–432. Springer, 2015.

[Tod15b] Yosuke Todo. Structural evaluation by generalized integral property. In Elisabeth Oswald and Marc Fischlin, editors, *EUROCRYPT Part I*, volume 9056 of *LNCS*, pages 287–314. Springer, 2015.

[TSKN12] Yukiyasu Tsunoo, Teruo Saito, Takeshi Kawabata, and Hirokatsu Nakagawa. Finding higher order differentials of MISTY1. *IEICE Transactions*, 95-A(6):1049–1055, 2012.

[TSSK08] Yukiyasu Tsunoo, Teruo Saito, Maki Shigeri, and Takeshi Kawabata. Higher order differential attacks on reduced-round MISTY1. In Pil Joong Lee and Jung Hee Cheon, editors, *ICISC*, volume 5461 of *LNCS*, pages 415–431. Springer, 2008.

[U.S77] U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology. *DATA ENCRYPTION STANDARD (DES)*, 1977. Federal Information Processing Standards Publication 46.

[U.S01] U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology. *Specification for the ADVANCED ENCRYPTION STANDARD (AES)*, 2001. Federal Information Processing Standards Publication 197.

[Vau03] Serge Vaudenay. Decorrelation: A theory for block cipher security. *J. Cryptology*, 16(4):249–286, 2003.

[WLV+14] Qingju Wang, Zhiqiang Liu, Kerem Varici, Yu Sasaki, Vincent Rijmen, and Yosuke Todo. Cryptanalysis of reduced-round SIMON32 and SIMON48. In Willi Meier and Debdeep Mukhopadhyay, editors, *INDOCRYPT*, volume 8885 of *LNCS*, pages 143–160. Springer, 2014.

[WW13] Shengbao Wu and Mingsheng Wang. Integral attacks on reduced-round PRESENT. In Sihan Qing and Jianying Zhou and Dongmei Liu, editor, *ICICS*, volume 8233 of *LNCS*, pages 331–345. Springer, 2013.

[WZ11] Wenling Wu and Lei Zhang. LBlock: A lightweight block cipher. In Javier Lopez and Gene Tsudik, editors, *ACNS*, volume 6715 of *LNCS*, pages 327–344. Springer, 2011.

[YPK02] Yongjin Yeom, Sangwoo Park, and Iljun Kim. On the security of CAMELLIA against the square attack. In Joan Daemen and Vincent Rijmen, editors, *FSE*, volume 2365 of *LNCS*, pages 89–99. Springer, 2002.

[ZMI89] Yuliang Zheng, Tsutomu Matsumoto, and Hideki Imai. On the construction of block ciphers provably secure and not relying on any unproved hypotheses. In *CRYPTO*, volume 435 of *LNCS*, pages 461–480, 1989.

[ZRHD08] Muhammad Reza Z'aba, Håvard Raddum, Matthew Henricksen, and Ed Dawson. Bit-pattern based integral attack. In Kaisa Nyberg, editor, *FSE*, volume 5086 of *LNCS*, pages 363–381. Springer, 2008.

[ZSW+12] Wentao Zhang, Bozhan Su, Wenling Wu, Dengguo Feng, and Chuankun Wu. Extending higher-order integral: An efficient unified algorithm of constructing integral distinguishers for block ciphers. In Feng Bao, Pierangela Samarati, and Jianying Zhou, editors, *ACNS*, volume 7341 of *LNCS*, pages 117–134. Springer, 2012.

[ZW15] Huiling Zhang and Wenling Wu. Structural evaluation for generalized feistel structures and applications to lblock and TWINE. In Alex Biryukov and Vipul Goyal, editors, *INDOCRYPT*, volume 9462 of *LNCS*, pages 218–237. Springer, 2015.

[ZWW15] Huiling Zhang, Wenling Wu, and Yanfeng Wang. Integral attack against bit-oriented block ciphers. In *ICISC*, 2015.

第III部

付録

付 録A　MISTY S-boxのANF

MISTY S-box S_7 の ANF は以下のように表せる.

$$
\begin{aligned}
y[0] &= x[0] \oplus x[1]x[3] \oplus x[0]x[3]x[4] \oplus x[1]x[5] \oplus x[0]x[2]x[5] \oplus x[4]x[5] \\
&\quad \oplus x[0]x[1]x[6] \oplus x[2]x[6] \oplus x[0]x[5]x[6] \oplus x[3]x[5]x[6] \oplus 1, \\
y[1] &= x[0]x[2] \oplus x[0]x[4] \oplus x[3]x[4] \oplus x[1]x[5] \oplus x[2]x[4]x[5] \oplus x[6] \oplus x[0]x[6] \\
&\quad \oplus x[3]x[6] \oplus x[2]x[3]x[6] \oplus x[1]x[4]x[6] \oplus x[0]x[5]x[6] \oplus 1, \\
y[2] &= x[1]x[2] \oplus x[0]x[2]x[3] \oplus x[4] \oplus x[1]x[4] \oplus x[0]x[1]x[4] \oplus x[0]x[5] \oplus x[0]x[4]x[5] \\
&\quad \oplus x[3]x[4]x[5] \oplus x[1]x[6] \oplus x[3]x[6] \oplus x[0]x[3]x[6] \oplus x[4]x[6] \oplus x[2]x[4]x[6], \\
y[3] &= x[0] \oplus x[1] \oplus x[0]x[1]x[2] \oplus x[0]x[3] \oplus x[2]x[4] \oplus x[1]x[4]x[5] \oplus x[2]x[6] \\
&\quad \oplus x[1]x[3]x[6] \oplus x[0]x[4]x[6] \oplus x[5]x[6] \oplus 1, \\
y[4] &= x[2]x[3] \oplus x[0]x[4] \oplus x[1]x[3]x[4] \oplus x[5] \oplus x[2]x[5] \oplus x[1]x[2]x[5] \oplus x[0]x[3]x[5] \\
&\quad \oplus x[1]x[6] \oplus x[1]x[5]x[6] \oplus x[4]x[5]x[6] \oplus 1, \\
y[5] &= x[0] \oplus x[1] \oplus x[2] \oplus x[0]x[1]x[2] \oplus x[0]x[3] \oplus x[1]x[2]x[3] \oplus x[1]x[4] \\
&\quad \oplus x[0]x[2]x[4] \oplus x[0]x[5] \oplus x[0]x[1]x[5] \oplus x[3]x[5] \oplus x[0]x[6] \oplus x[2]x[5]x[6], \\
y[6] &= x[0]x[1] \oplus x[3] \oplus x[0]x[3] \oplus x[2]x[3]x[4] \oplus x[0]x[5] \oplus x[2]x[5] \oplus x[3]x[5] \\
&\quad \oplus x[1]x[3]x[5] \oplus x[1]x[6] \oplus x[1]x[2]x[6] \oplus x[0]x[3]x[6] \oplus x[4]x[6] \oplus x[2]x[5]x[6].
\end{aligned}
$$

また MISTY S-box S_9 の ANF は以下のように表せる.

$$
\begin{aligned}
y[0] &= x[0]x[4] \oplus x[0]x[5] \oplus x[1]x[5] \oplus x[1]x[6] \oplus x[2]x[6] \oplus x[2]x[7] \oplus x[3]x[7] \oplus x[3]x[8] \\
&\quad \oplus x[4]x[8] \oplus 1, \\
y[1] &= x[0]x[2] \oplus x[3] \oplus x[1]x[3] \oplus x[2]x[3] \oplus x[3]x[4] \oplus x[4]x[5] \oplus x[0]x[6] \oplus x[2]x[6] \\
&\quad \oplus x[7] \oplus x[0]x[8] \oplus x[3]x[8] \oplus x[5]x[8] \oplus 1, \\
y[2] &= x[0]x[1] \oplus x[1]x[3] \oplus x[4] \oplus x[0]x[4] \oplus x[2]x[4] \oplus x[3]x[4] \oplus x[4]x[5] \oplus x[0]x[6] \\
&\quad \oplus x[5]x[6] \oplus x[1]x[7] \oplus x[3]x[7] \oplus x[8], \\
y[3] &= x[0] \oplus x[1]x[2] \oplus x[2]x[4] \oplus x[5] \oplus x[1]x[5] \oplus x[3]x[5] \oplus x[4]x[5] \oplus x[5]x[6] \\
&\quad \oplus x[1]x[7] \oplus x[6]x[7] \oplus x[2]x[8] \oplus x[4]x[8], \\
y[4] &= x[1] \oplus x[0]x[3] \oplus x[2]x[3] \oplus x[0]x[5] \oplus x[3]x[5] \oplus x[6] \oplus x[2]x[6] \oplus x[4]x[6] \\
&\quad \oplus x[5]x[6] \oplus x[6]x[7] \oplus x[2]x[8] \oplus x[7]x[8], \\
y[5] &= x[2] \oplus x[0]x[3] \oplus x[1]x[4] \oplus x[3]x[4] \oplus x[1]x[6] \oplus x[4]x[6] \oplus x[7] \oplus x[3]x[7] \\
&\quad \oplus x[5]x[7] \oplus x[6]x[7] \oplus x[0]x[8] \oplus x[7]x[8], \\
y[6] &= x[0]x[1] \oplus x[3] \oplus x[1]x[4] \oplus x[2]x[5] \oplus x[4]x[5] \oplus x[2]x[7] \oplus x[5]x[7] \oplus x[8] \\
&\quad \oplus x[0]x[8] \oplus x[4]x[8] \oplus x[6]x[8] \oplus x[7]x[8] \oplus 1, \\
y[7] &= x[1] \oplus x[0]x[1] \oplus x[1]x[2] \oplus x[2]x[3] \oplus x[0]x[4] \oplus x[5] \oplus x[1]x[6] \oplus x[3]x[6] \\
&\quad \oplus x[0]x[7] \oplus x[4]x[7] \oplus x[6]x[7] \oplus x[1]x[8] \oplus 1, \\
y[8] &= x[0] \oplus x[0]x[1] \oplus x[1]x[2] \oplus x[4] \oplus x[0]x[5] \oplus x[2]x[5] \oplus x[3]x[6] \oplus x[5]x[6] \\
&\quad \oplus x[0]x[7] \oplus x[0]x[8] \oplus x[3]x[8] \oplus x[6]x[8] \oplus 1.
\end{aligned}
$$

付 録B　FI関数に対する伝搬特性例

Division Property の伝搬特性を理解するために，FI 関数に対する伝搬特性を例に示す (図 8.3 参照．)．具体的には入力 Division Property が $\mathcal{D}^{7,2,7}_{\{[4,2,6]\}}$ の場合を例に伝搬特性を考える．

From $\mathbb{X}_1$ to $\mathbb{X}_2$: 先頭 7 ビット値と次の 2 ビット値をビット連結する．したがって Concatenation の伝搬ルールが適用され，入力多重集合 $\mathbb{X}_2$ は Division Property $\mathcal{D}^{9,7}_{\{[6,6]\}}$ を満足する．

From $\mathbb{X}_2$ to $\mathbb{X}_3$: 9 ビット S-box S_9 が適用される．したがって入力多重集合 $\mathbb{X}_3$ は Division Property $\mathcal{D}^{9,7}_{\{[3,6]\}}$ を満足する．

From $\mathbb{X}_3$ to $\mathbb{X}_4$: 先頭 9 ビット値が 2 ビット値と 7 ビット値に分割される．したがって Split の伝搬ルールが適用され，入力多重集合 $\mathbb{X}_4$ は Division Property $\mathcal{D}^{2,7,7}_{\{[0,3,6],[1,2,6],[2,1,6]\}}$ を満足する．

From $\mathbb{X}_4$ to $\mathbb{X}_5$: 後ろ 7 ビット値を中間 7 ビット値に排他的論理和する．したがって Copy と XOR の伝搬ルールが適用され，入力 Division Property の 3 個のベクトルからそれぞれ

$$
\begin{aligned}
&[0,3,6] \Rightarrow [0,3,6],[0,4,5],[0,5,4],[0,6,3],[0,7,2],\\
&[1,2,6] \Rightarrow [1,2,6],[1,3,5],[1,4,4],[1,5,3],[1,6,2],[1,7,1],\\
&[2,1,6] \Rightarrow [2,1,6],[2,2,5],[2,3,4],[2,4,3],[2,5,2],[2,6,1],[2,7,0],
\end{aligned}
$$

が伝搬される．その後ローテーションされ，$\mathbb{X}_5$ の Division Property は $\mathcal{D}^{7,2,7}_{\mathbb{K}}$ を満足し，ここで $\mathbb{K}$ は以下に示す 18 個のベクトルで構成される．

$$
\begin{aligned}
&[6,0,3],[5,0,4],[4,0,5],[3,0,6],[2,0,7],\\
&[6,1,2],[5,1,3],[4,1,4],[3,1,5],[2,1,6],[1,1,7],\\
&[6,2,1],[5,2,2],[4,2,3],[3,2,4],[2,2,5],[1,2,6],[0,2,7].
\end{aligned}
$$

From $\mathbb{X}_5$ to $\mathbb{X}_6$: 7 ビット S-box S_7 が適用される．18 個のそれぞれのベクトルに対して S_7 の伝搬特性を適用し，結果として以下に示す 18 個の

ベクトルを得る．

$$[4,0,3],[2,0,4],[2,0,5],[1,0,6],[1,0,7],$$
$$[4,1,2],[2,1,3],[2,1,4],[1,1,5],[1,1,6],[1,1,7],$$
$$[4,2,1],[2,2,2],[2,2,3],[1,2,4],[1,2,5],[1,2,6],[0,2,7].$$

上記のベクトル集合は冗長なベクトルを持つ．例に $[2,0,5]$ は $[2,0,5] \succ [2,0,4]$ となる $[2,0,4]$ を持つことから削除可能である．同様にして冗長なベクトルを削除する．結果として，入力多重集合 $\mathbb{X}_6$ は Division Property $\mathcal{D}_{\mathbb{K}}^{7,2,7}$ を満足し，ここで $\mathbb{K}$ は以下に示す 10 個のベクトルで構成される．

$$[0,2,7],[1,0,6],[1,1,5],[1,2,4],[2,0,4],$$
$$[2,1,3],[2,2,2],[4,0,3],[4,1,2],[4,2,1].$$

From $\mathbb{X}_6$ to $\mathbb{X}_7$: 後ろ 7 ビット値を先頭 7 ビット値に排他的論理和する．したがって Copy と XOR の伝搬ルールが適用され，入力 Division Property の 10 個のベクトルからそれぞれ

$[0,2,7] \Rightarrow [0,2,7],[1,2,6],[2,2,5],[3,2,4],[4,2,3],[5,2,2],[6,2,1],[7,2,0],$
$[1,0,6] \Rightarrow [1,0,6],[2,0,5],[3,0,4],[4,0,3],[5,0,2],[6,0,1],[7,0,0],$
$[1,1,5] \Rightarrow [1,1,5],[2,1,4],[3,1,3],[4,1,2],[5,1,1],[6,1,0],$
$[1,2,4] \Rightarrow [1,2,4],[2,2,3],[3,2,2],[4,2,1],[5,2,0],$
$[2,0,4] \Rightarrow [2,0,4],[3,0,3],[4,0,2],[5,0,1],[6,0,0],$
$[2,1,3] \Rightarrow [2,1,3],[3,1,2],[4,1,1],[5,1,0],$
$[2,2,2] \Rightarrow [2,2,2],[3,2,1],[4,2,0],$
$[4,0,3] \Rightarrow [4,0,3],[5,0,2],[6,0,1],[7,0,0],$
$[4,1,2] \Rightarrow [4,1,2],[5,1,1],[6,1,0],$
$[4,2,1] \Rightarrow [4,2,1],[5,2,0].$

が伝搬される．その後ローテーションされ，$\mathbb{X}_7$ の Division Property は $\mathcal{D}_{\mathbb{K}}^{7,2,7}$ を満足し，ここで $\mathbb{K}$ は以下に示す 16 個のベクトルで構成される．

$$[0,0,6],[0,1,5],[0,2,4],[0,3,3],[0,4,2],[0,6,1],[1,0,5],[1,1,4],$$
$$[1,2,3],[1,3,2],[1,5,1],[2,0,4],[2,1,3],[2,2,2],[2,4,1],[2,7,0].$$

From $\mathbb{X}_7$ to $\mathbb{X}_8$: 先頭 2 ビット値と次の 7 ビット値をビット連結する．したがって Concatenation の伝搬ルールが適用され，以下の 16 個のベクトルが得られる．

$$[0,6],[1,5],[2,4],[3,3],[4,2],[6,1],[1,5],[2,4],$$
$$[3,3],[4,2],[6,1],[2,4],[3,3],[4,2],[6,1],[9,0].$$

冗長なベクトルを取り除いた結果，入力多重集合 $\mathbb{X}_8$ は Division Property $\mathcal{D}_{\mathbb{K}}^{9,7}$ を満足し，ここで $\mathbb{K}$ は以下に示す 7 個のベクトルで構成される．

$$[0,6],[1,5],[2,4],[3,3],[4,2],[6,1],[9,0].$$

From $\mathbb{X}_8$ to $\mathbb{X}_9$: 9 ビット S-box S_9 が適用される．7 個のそれぞれのベクトルに対して S_9 の伝搬特性を適用し，結果として以下に示す 7 個のベクトルを得る．

$$[0,6],[1,5],[1,4],[2,3],[2,2],[3,1],[9,0].$$

冗長なベクトルを取り除いた結果，入力多重集合 $\mathbb{X}_9$ は Division Property $\mathcal{D}_{\mathbb{K}}^{9,7}$ を満足し，ここで $\mathbb{K}$ は以下に示す 5 個のベクトルで構成される．

$$[0,6],[1,4],[2,2],[3,1],[9,0].$$

From $\mathbb{X}_9$ to $\mathbb{X}_{10}$: 先頭 9 ビット値が 2 ビット値と 7 ビット値に分割される．したがって Split の伝搬ルールが適用され，入力多重集合 $\mathbb{X}_{10}$ は Division Property $\mathcal{D}_{\mathbb{K}}^{2,7,7}$ を満足し，ここで $\mathbb{K}$ は以下に示す 10 個のベクトルで構成される．

$$\begin{aligned}
&[0,6] \Rightarrow [0,0,6],\\
&[1,4] \Rightarrow [0,1,4],[1,0,4],\\
&[2,2] \Rightarrow [0,2,2],[1,1,2],[2,0,2],\\
&[3,1] \Rightarrow [0,3,1],[1,2,1],[2,1,1],\\
&[9,0] \Rightarrow [2,7,0].
\end{aligned}$$

From $\mathbb{X}_{10}$ to $\mathbb{X}_{11}$: 後ろ 7 ビット値を中間 7 ビット値に排他的論理和する．したがって Copy と XOR の伝搬ルールが適用され，入力 Division Property の 10 個のベクトルからそれぞれ

$$\begin{aligned}
&[0,0,6] \Rightarrow [0,0,6],[0,1,5],[0,2,4],[0,3,3],[0,4,2],[0,5,1],[0,6,0],\\
&[0,1,4] \Rightarrow [0,1,4],[0,2,3],[0,3,2],[0,4,1],[0,5,0],\\
&[1,0,4] \Rightarrow [1,0,4],[1,1,3],[1,2,2],[1,3,1],[1,4,0],\\
&[0,2,2] \Rightarrow [0,2,2],[0,3,1],[0,4,0],\\
&[1,1,2] \Rightarrow [1,1,2],[1,2,1],[1,3,0],\\
&[2,0,2] \Rightarrow [2,0,2],[2,1,1],[2,2,0],\\
&[0,3,1] \Rightarrow [0,3,1],[0,4,0],\\
&[1,2,1] \Rightarrow [1,2,1],[1,3,0],\\
&[2,1,1] \Rightarrow [2,1,1],[2,2,0],\\
&[2,7,0] \Rightarrow [2,7,0].
\end{aligned}$$

が伝搬される．その後ローテーションされ，$\mathbb{X}_{11}$ の Division Property は $\mathcal{D}_{\mathbb{K}}^{7,2,7}$ を満足し，ここで $\mathbb{K}$ は以下に示す 12 個のベクトルで構成される．

$$[0,0,4],[0,1,3],[0,2,2],[1,0,3],[1,1,2],[1,2,1],$$
$$[2,0,2],[2,1,1],[2,2,0],[4,0,1],[4,1,0],[6,0,0].$$

Algorithm 4 は任意の入力 Division Property $\mathcal{D}_{\{\vec{k}\}}^{7,2,7}$ からの伝搬特性を評価する．Algorithm 4 を実装することによって得られた伝搬特性表は付録 C を参照されたい．

付 録C　FI関数の伝搬特性表

表 C.1: Propagation from $\mathcal{D}^{7,2,7}_{\{[0,*,*]\}}$ to $\mathcal{D}^{7,2,7}_{\mathbb{K}}$

$\vec{k}$	$\mathbb{K}$
[0 0 0]	[0 0 0]
[0 0 1]	[0 0 1] [0 1 0] [1 0 0]
[0 0 2]	[0 0 1] [0 1 0] [1 0 0]
[0 0 3]	[0 0 1] [0 2 0] [1 0 0]
[0 0 4]	[0 0 2] [0 1 1] [0 2 0] [1 0 1] [1 1 0] [2 0 0]
[0 0 5]	[0 0 2] [0 1 1] [1 0 1] [1 1 0] [2 0 0]
[0 0 6]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [3 0 0]
[0 0 7]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [4 0 0]
[0 1 0]	[0 0 1] [0 1 0] [1 0 0]
[0 1 1]	[0 0 1] [0 1 0] [2 0 0]
[0 1 2]	[0 0 2] [0 1 1] [0 2 0] [1 0 1] [1 1 0] [2 0 0]
[0 1 3]	[0 0 2] [0 1 1] [0 2 0] [1 0 1] [1 1 0] [2 0 0]
[0 1 4]	[0 0 2] [0 1 1] [1 0 1] [1 1 0] [3 0 0]
[0 1 5]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [3 0 0]
[0 1 6]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [4 0 0]
[0 1 7]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [3 0 1] [3 1 0] [5 0 0]
[0 2 0]	[0 0 1] [0 1 0] [1 0 0]
[0 2 1]	[0 0 1] [0 1 0] [2 0 0]
[0 2 2]	[0 0 2] [0 1 1] [0 2 0] [1 0 1] [1 1 0] [2 0 0]
[0 2 3]	[0 0 2] [0 1 1] [0 2 0] [1 0 1] [1 1 0] [2 0 0]
[0 2 4]	[0 0 2] [0 1 1] [1 0 1] [1 1 0] [3 0 0]
[0 2 5]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [3 0 0]
[0 2 6]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [4 0 0]
[0 2 7]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [3 0 1] [3 1 0] [5 0 0]

表 C.2: Propagation from $\mathcal{D}^{7,2,7}_{\{[1,*,*]\}}$ to $\mathcal{D}^{7,2,7}_{\mathbb{K}}$

$\vec{k}$	$\mathbb{K}$
[1 0 0]	[0 0 1] [0 1 0] [1 0 0]
[1 0 1]	[0 0 1] [0 1 0] [2 0 0]
[1 0 2]	[0 0 2] [0 1 1] [0 2 0] [1 0 1] [1 1 0] [2 0 0]
[1 0 3]	[0 0 2] [0 1 1] [0 2 0] [1 0 1] [1 1 0] [2 0 0]
[1 0 4]	[0 0 2] [0 1 1] [1 0 1] [1 1 0] [3 0 0]
[1 0 5]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [3 0 0]
[1 0 6]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [4 0 0]
[1 0 7]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [3 0 1] [3 1 0] [5 0 0]
[1 1 0]	[0 0 1] [0 1 0] [1 0 0]
[1 1 1]	[0 0 1] [0 1 0] [2 0 0]
[1 1 2]	[0 0 2] [0 1 1] [0 2 0] [1 0 1] [1 1 0] [2 0 0]
[1 1 3]	[0 0 2] [0 1 1] [0 2 0] [1 0 1] [1 1 0] [2 0 0]
[1 1 4]	[0 0 2] [0 1 1] [1 0 1] [1 1 0] [3 0 0]
[1 1 5]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [3 0 0]
[1 1 6]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [4 0 0]
[1 1 7]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [3 0 1] [3 1 0] [5 0 0]
[1 2 0]	[0 0 1] [0 1 0] [2 0 0]
[1 2 1]	[0 0 2] [0 1 1] [0 2 0] [1 0 1] [1 1 0] [3 0 0]
[1 2 2]	[0 0 2] [0 1 1] [0 2 0] [1 0 1] [1 1 0] [3 0 0]
[1 2 3]	[0 0 2] [0 1 1] [1 0 1] [1 1 0] [3 0 0]
[1 2 4]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [4 0 0]
[1 2 5]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [4 0 0]
[1 2 6]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [3 0 1] [3 1 0] [5 0 0]
[1 2 7]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [4 0 1] [4 1 0] [6 0 0]

表 C.3: Propagation from $\mathcal{D}^{7,2,7}_{\{[2,*,*]\}}$ to $\mathcal{D}^{7,2,7}_{\mathbb{K}}$

$\vec{k}$	$\mathbb{K}$
[2 0 0]	[0 0 1] [0 1 0] [1 0 0]
[2 0 1]	[0 0 1] [0 1 0] [2 0 0]
[2 0 2]	[0 0 2] [0 1 1] [0 2 0] [1 0 1] [1 1 0] [2 0 0]
[2 0 3]	[0 0 2] [0 1 1] [0 2 0] [1 0 1] [1 1 0] [2 0 0]
[2 0 4]	[0 0 2] [0 1 1] [1 0 1] [1 1 0] [3 0 0]
[2 0 5]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [3 0 0]
[2 0 6]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [4 0 0]
[2 0 7]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [3 0 1] [3 1 0] [5 0 0]
[2 1 0]	[0 0 1] [0 1 0] [2 0 0]
[2 1 1]	[0 0 2] [0 1 1] [0 2 0] [1 0 1] [1 1 0] [3 0 0]
[2 1 2]	[0 0 2] [0 1 1] [0 2 0] [1 0 1] [1 1 0] [3 0 0]
[2 1 3]	[0 0 2] [0 1 1] [1 0 1] [1 1 0] [3 0 0]
[2 1 4]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [4 0 0]
[2 1 5]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [4 0 0]
[2 1 6]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [3 0 1] [3 1 0] [5 0 0]
[2 1 7]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [4 0 1] [4 1 0] [6 0 0]
[2 2 0]	[0 0 1] [0 1 0] [2 0 0]
[2 2 1]	[0 0 2] [0 1 1] [0 2 0] [1 0 1] [1 1 0] [3 0 0]
[2 2 2]	[0 0 2] [0 1 1] [0 2 0] [1 0 1] [1 1 0] [3 0 0]
[2 2 3]	[0 0 2] [0 1 1] [1 0 1] [1 1 0] [3 0 0]
[2 2 4]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [4 0 0]
[2 2 5]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [4 0 0]
[2 2 6]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [3 0 1] [3 1 0] [5 0 0]
[2 2 7]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [4 0 1] [4 1 0] [6 0 0]

表 C.4: Propagation from $\mathcal{D}^{7,2,7}_{\{[3,*,*]\}}$ to $\mathcal{D}^{7,2,7}_{\mathbb{K}}$

$\vec{k}$	$\mathbb{K}$
[3 0 0]	[0 0 1] [0 1 0] [2 0 0]
[3 0 1]	[0 0 2] [0 1 1] [0 2 0] [1 0 1] [1 1 0] [3 0 0]
[3 0 2]	[0 0 2] [0 1 1] [0 2 0] [1 0 1] [1 1 0] [3 0 0]
[3 0 3]	[0 0 2] [0 1 1] [1 0 1] [1 1 0] [3 0 0]
[3 0 4]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [4 0 0]
[3 0 5]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [4 0 0]
[3 0 6]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [3 0 1] [3 1 0] [5 0 0]
[3 0 7]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [4 0 1] [4 1 0] [6 0 0]
[3 1 0]	[0 0 1] [0 1 0] [2 0 0]
[3 1 1]	[0 0 2] [0 1 1] [0 2 0] [1 0 1] [1 1 0] [3 0 0]
[3 1 2]	[0 0 2] [0 1 1] [0 2 0] [1 0 1] [1 1 0] [3 0 0]
[3 1 3]	[0 0 2] [0 1 1] [1 0 1] [1 1 0] [3 0 0]
[3 1 4]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [4 0 0]
[3 1 5]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [4 0 0]
[3 1 6]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [3 0 1] [3 1 0] [5 0 0]
[3 1 7]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [4 0 1] [4 1 0] [6 0 0]
[3 2 0]	[0 0 2] [0 1 1] [0 2 0] [1 0 1] [1 1 0] [3 0 0]
[3 2 1]	[0 0 2] [0 1 1] [0 2 0] [2 0 1] [2 1 0] [4 0 0]
[3 2 2]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [4 0 0]
[3 2 3]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [4 0 0]
[3 2 4]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [3 0 1] [3 1 0] [5 0 0]
[3 2 5]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [3 0 1] [3 1 0] [5 0 0]
[3 2 6]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [4 0 1] [4 1 0] [6 0 0]
[3 2 7]	[0 0 5] [0 1 4] [0 2 3] [1 0 4] [1 1 3] [1 2 2] [2 0 3] [2 1 2] [2 2 1] [3 0 2] [3 1 1] [3 2 0] [5 0 1] [5 1 0] [7 0 0]

表 C.5: Propagation from $\mathcal{D}^{7,2,7}_{\{[4,*,*]\}}$ to $\mathcal{D}^{7,2,7}_{\mathbb{K}}$

$\vec{k}$	$\mathbb{K}$
[4 0 0]	[0 0 1] [0 1 0] [2 0 0]
[4 0 1]	[0 0 2] [0 1 1] [0 2 0] [1 0 1] [1 1 0] [3 0 0]
[4 0 2]	[0 0 2] [0 1 1] [0 2 0] [1 0 1] [1 1 0] [3 0 0]
[4 0 3]	[0 0 2] [0 1 1] [1 0 1] [1 1 0] [3 0 0]
[4 0 4]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [4 0 0]
[4 0 5]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [4 0 0]
[4 0 6]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [3 0 1] [3 1 0] [5 0 0]
[4 0 7]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [4 0 1] [4 1 0] [6 0 0]
[4 1 0]	[0 0 2] [0 1 1] [0 2 0] [1 0 1] [1 1 0] [3 0 0]
[4 1 1]	[0 0 2] [0 1 1] [0 2 0] [2 0 1] [2 1 0] [4 0 0]
[4 1 2]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [4 0 0]
[4 1 3]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [4 0 0]
[4 1 4]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [3 0 1] [3 1 0] [5 0 0]
[4 1 5]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [3 0 1] [3 1 0] [5 0 0]
[4 1 6]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [4 0 1] [4 1 0] [6 0 0]
[4 1 7]	[0 0 5] [0 1 4] [0 2 3] [1 0 4] [1 1 3] [1 2 2] [2 0 3] [2 1 2] [2 2 1] [3 0 2] [3 1 1] [3 2 0] [5 0 1] [5 1 0] [7 0 0]
[4 2 0]	[0 0 2] [0 1 1] [0 2 0] [1 0 1] [1 1 0] [3 0 0]
[4 2 1]	[0 0 2] [0 1 1] [0 2 0] [2 0 1] [2 1 0] [4 0 0]
[4 2 2]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [4 0 0]
[4 2 3]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [4 0 0]
[4 2 4]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [3 0 1] [3 1 0] [5 0 0]
[4 2 5]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [3 0 1] [3 1 0] [5 0 0]
[4 2 6]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [4 0 1] [4 1 0] [6 0 0]
[4 2 7]	[0 0 5] [0 1 4] [0 2 3] [1 0 4] [1 1 3] [1 2 2] [2 0 3] [2 1 2] [2 2 1] [3 0 2] [3 1 1] [3 2 0] [5 0 1] [5 1 0] [7 0 0]

表 C.6: Propagation from $\mathcal{D}^{7,2,7}_{\{[5,*,*]\}}$ to $\mathcal{D}^{7,2,7}_{\mathbb{K}}$

$\vec{k}$	$\mathbb{K}$
[5 0 0]	[0 0 2] [0 1 1] [0 2 0] [1 0 1] [1 1 0] [3 0 0]
[5 0 1]	[0 0 2] [0 1 1] [0 2 0] [2 0 1] [2 1 0] [4 0 0]
[5 0 2]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [4 0 0]
[5 0 3]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [4 0 0]
[5 0 4]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [3 0 1] [3 1 0] [5 0 0]
[5 0 5]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [3 0 1] [3 1 0] [5 0 0]
[5 0 6]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [4 0 1] [4 1 0] [6 0 0]
[5 0 7]	[0 0 5] [0 1 4] [0 2 3] [1 0 4] [1 1 3] [1 2 2] [2 0 3] [2 1 2] [2 2 1] [3 0 2] [3 1 1] [3 2 0] [5 0 1] [5 1 0] [7 0 0]
[5 1 0]	[0 0 2] [0 1 1] [0 2 0] [1 0 1] [1 1 0] [3 0 0]
[5 1 1]	[0 0 2] [0 1 1] [0 2 0] [2 0 1] [2 1 0] [4 0 0]
[5 1 2]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [4 0 0]
[5 1 3]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [4 0 0]
[5 1 4]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [3 0 1] [3 1 0] [5 0 0]
[5 1 5]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [3 0 1] [3 1 0] [5 0 0]
[5 1 6]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [4 0 1] [4 1 0] [6 0 0]
[5 1 7]	[0 0 5] [0 1 4] [0 2 3] [1 0 4] [1 1 3] [1 2 2] [2 0 3] [2 1 2] [2 2 1] [3 0 2] [3 1 1] [3 2 0] [5 0 1] [5 1 0] [7 0 0]
[5 2 0]	[0 0 2] [0 1 1] [0 2 0] [2 0 1] [2 1 0] [4 0 0]
[5 2 1]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [3 0 1] [3 1 0] [5 0 0]
[5 2 2]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [3 0 1] [3 1 0] [5 0 0]
[5 2 3]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [3 0 1] [3 1 0] [5 0 0]
[5 2 4]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [4 0 1] [4 1 0] [6 0 0]
[5 2 5]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [4 0 1] [4 1 0] [6 0 0]
[5 2 6]	[0 0 5] [0 1 4] [0 2 3] [1 0 4] [1 1 3] [1 2 2] [2 0 3] [2 1 2] [2 2 1] [3 0 2] [3 1 1] [3 2 0] [5 0 1] [5 1 0] [7 0 0]
[5 2 7]	[0 0 5] [0 1 4] [0 2 3] [1 0 4] [1 1 3] [1 2 2] [2 0 3] [2 1 2] [2 2 1] [4 0 2] [4 1 1] [4 2 0] [6 0 1] [6 1 0]

表 C.7: Propagation from $\mathcal{D}^{7,2,7}_{\{[6,*,*]\}}$ to $\mathcal{D}^{7,2,7}_{\mathbb{K}}$

$\vec{k}$	$\mathbb{K}$
[6 0 0]	[0 0 2] [0 1 1] [0 2 0] [1 0 1] [1 1 0] [3 0 0]
[6 0 1]	[0 0 2] [0 1 1] [0 2 0] [2 0 1] [2 1 0] [4 0 0]
[6 0 2]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [4 0 0]
[6 0 3]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [4 0 0]
[6 0 4]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [3 0 1] [3 1 0] [5 0 0]
[6 0 5]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [3 0 1] [3 1 0] [5 0 0]
[6 0 6]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [4 0 1] [4 1 0] [6 0 0]
[6 0 7]	[0 0 5] [0 1 4] [0 2 3] [1 0 4] [1 1 3] [1 2 2] [2 0 3] [2 1 2] [2 2 1] [3 0 2] [3 1 1] [3 2 0] [5 0 1] [5 1 0] [7 0 0]
[6 1 0]	[0 0 2] [0 1 1] [0 2 0] [2 0 1] [2 1 0] [4 0 0]
[6 1 1]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [3 0 1] [3 1 0] [5 0 0]
[6 1 2]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [3 0 1] [3 1 0] [5 0 0]
[6 1 3]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [3 0 1] [3 1 0] [5 0 0]
[6 1 4]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [4 0 1] [4 1 0] [6 0 0]
[6 1 5]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [4 0 1] [4 1 0] [6 0 0]
[6 1 6]	[0 0 5] [0 1 4] [0 2 3] [1 0 4] [1 1 3] [1 2 2] [2 0 3] [2 1 2] [2 2 1] [3 0 2] [3 1 1] [3 2 0] [5 0 1] [5 1 0] [7 0 0]
[6 1 7]	[0 0 5] [0 1 4] [0 2 3] [1 0 4] [1 1 3] [1 2 2] [2 0 3] [2 1 2] [2 2 1] [4 0 2] [4 1 1] [4 2 0] [6 0 1] [6 1 0]
[6 2 0]	[0 0 2] [0 1 1] [0 2 0] [2 0 1] [2 1 0] [4 0 0]
[6 2 1]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [3 0 1] [3 1 0] [5 0 0]
[6 2 2]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [3 0 1] [3 1 0] [5 0 0]
[6 2 3]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [3 0 1] [3 1 0] [5 0 0]
[6 2 4]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [4 0 1] [4 1 0] [6 0 0]
[6 2 5]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [4 0 1] [4 1 0] [6 0 0]
[6 2 6]	[0 0 5] [0 1 4] [0 2 3] [1 0 4] [1 1 3] [1 2 2] [2 0 3] [2 1 2] [2 2 1] [3 0 2] [3 1 1] [3 2 0] [5 0 1] [5 1 0] [7 0 0]
[6 2 7]	[0 0 5] [0 1 4] [0 2 3] [1 0 4] [1 1 3] [1 2 2] [2 0 3] [2 1 2] [2 2 1] [4 0 2] [4 1 1] [4 2 0] [6 0 1] [6 1 0]

表 C.8: Propagation from $\mathcal{D}^{7,2,7}_{\{[7,*,*]\}}$ to $\mathcal{D}^{7,2,7}_{\mathbb{K}}$

$\vec{k}$	$\mathbb{K}$
[7 0 0]	[0 0 2] [0 1 1] [0 2 0] [2 0 1] [2 1 0] [4 0 0]
[7 0 1]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [3 0 1] [3 1 0] [5 0 0]
[7 0 2]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [3 0 1] [3 1 0] [5 0 0]
[7 0 3]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [3 0 1] [3 1 0] [5 0 0]
[7 0 4]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [4 0 1] [4 1 0] [6 0 0]
[7 0 5]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [4 0 1] [4 1 0] [6 0 0]
[7 0 6]	[0 0 5] [0 1 4] [0 2 3] [1 0 4] [1 1 3] [1 2 2] [2 0 3] [2 1 2] [2 2 1] [3 0 2] [3 1 1] [3 2 0] [5 0 1] [5 1 0] [7 0 0]
[7 0 7]	[0 0 5] [0 1 4] [0 2 3] [1 0 4] [1 1 3] [1 2 2] [2 0 3] [2 1 2] [2 2 1] [4 0 2] [4 1 1] [4 2 0] [6 0 1] [6 1 0]
[7 1 0]	[0 0 2] [0 1 1] [0 2 0] [2 0 1] [2 1 0] [4 0 0]
[7 1 1]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [3 0 1] [3 1 0] [5 0 0]
[7 1 2]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [3 0 1] [3 1 0] [5 0 0]
[7 1 3]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [3 0 1] [3 1 0] [5 0 0]
[7 1 4]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [4 0 1] [4 1 0] [6 0 0]
[7 1 5]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [4 0 1] [4 1 0] [6 0 0]
[7 1 6]	[0 0 5] [0 1 4] [0 2 3] [1 0 4] [1 1 3] [1 2 2] [2 0 3] [2 1 2] [2 2 1] [3 0 2] [3 1 1] [3 2 0] [5 0 1] [5 1 0] [7 0 0]
[7 1 7]	[0 0 5] [0 1 4] [0 2 3] [1 0 4] [1 1 3] [1 2 2] [2 0 3] [2 1 2] [2 2 1] [4 0 2] [4 1 1] [4 2 0] [6 0 1] [6 1 0]
[7 2 0]	[0 0 5] [0 1 4] [0 2 3] [1 0 4] [1 1 3] [1 2 2] [3 0 3] [3 1 2] [3 2 1] [5 0 2] [5 1 1] [5 2 0] [7 0 1] [7 1 0]
[7 2 1]	[0 0 6] [0 1 5] [0 2 4] [1 0 5] [1 1 4] [1 2 3] [2 0 4] [2 1 3] [2 2 2] [4 0 3] [4 1 2] [4 2 1] [6 0 2] [6 1 1] [6 2 0]
[7 2 2]	[0 0 6] [0 1 5] [0 2 4] [1 0 5] [1 1 4] [1 2 3] [2 0 4] [2 1 3] [2 2 2] [4 0 3] [4 1 2] [4 2 1] [6 0 2] [6 1 1] [6 2 0]
[7 2 3]	[0 0 6] [0 1 5] [0 2 4] [1 0 5] [1 1 4] [1 2 3] [2 0 4] [2 1 3] [2 2 2] [4 0 3] [4 1 2] [4 2 1] [6 0 2] [6 1 1] [6 2 0]
[7 2 4]	[0 0 7] [0 1 6] [0 2 5] [1 0 6] [1 1 5] [1 2 4] [2 0 5] [2 1 4] [2 2 3] [3 0 4] [3 1 3] [3 2 2] [5 0 3] [5 1 2] [5 2 1] [7 0 2] [7 1 1] [7 2 0]
[7 2 5]	[0 0 7] [0 1 6] [0 2 5] [1 0 6] [1 1 5] [1 2 4] [2 0 5] [2 1 4] [2 2 3] [3 0 4] [3 1 3] [3 2 2] [5 0 3] [5 1 2] [5 2 1] [7 0 2] [7 1 1] [7 2 0]
[7 2 6]	[0 2 7] [1 1 7] [1 2 6] [2 0 7] [2 1 6] [2 2 5] [3 0 6] [3 1 5] [3 2 4] [4 0 5] [4 1 4] [4 2 3] [5 0 4] [5 1 3] [5 2 2] [7 0 3] [7 1 2] [7 2 1]
[7 2 7]	[7 2 7]

付 録D　MISTY1に対するDivision Propertyの伝搬特性

最初のFL層を取り除いたMISTY1に対して，$\mathcal{D}^{7,2,7,7,2,7,7,2,7,7,2,7}_{\{[6,2,7,7,2,7,7,2,7,7,2,7]\}}$ を満足する入力集合を用意した場合の伝搬結果を示す．以降簡単のために，$\vec{k}$ を $k_1k_2,\ldots,k_{12}$ と12桁の整数で表記する．また，Division Propertyを構成するベクトル数が膨大となったため，4段目，2回目のFL層，5段目の出力集合に対するDivision Propertyはベクトル数のみを表記する．

D.1　Plaintexts

627727727727

D.2　1st round

727727627727

D.3　2nd round

627727727727, 727727724727, 727727727724, 727727527727, 727727617727, 727727707727, 727727727527, 727727727617, 727727727707

D.4　1st FL Layer

627727727727, 727627727727, 727727724727, 727727725726, 727727726725, 727727727724, 727727527727, 727727617727, 727727627627, 727727627717, 727727707727, 727727717627, 727727717717, 727727727527, 727727727617, 727727727707

D.5　3rd round

724727727727, 725726727727, 726725727727, 727724727727, 725727012727, 725727102727, 726726012727, 726726102727, 727725012727, 727725102727, 725727014627, 725727104627, 725727121727, 725727211727, 725727301727, 726726014627, 726726104627, 726726121727, 726726211727, 726726301727, 727725014627, 727725104627, 727725121727, 727725211727, 727725301727, 725727123627, 725727213627, 725727303627, 725727320727, 725727410727, 725727500727, 726726123627, 726726213627, 726726303627, 726726320727, 726726410727,

726726500727, 727725123627, 727725213627, 727725303627, 727725320727, 727725410727,
727725500727, 725727017527, 725727107527, 725727124717, 725727214717, 725727304717,
725727322627, 725727322717, 725727412627, 725727412717, 725727502627, 725727502717,
726726017527, 726726107527, 726726124717, 726726214717, 726726304717, 726726322627,
726726322717, 726726412627, 726726412717, 726726502627, 726726502717, 727725017527,
727725107527, 727725124717, 727725214717, 727725304717, 727725322627, 727725322717,
727725412627, 727725412717, 727725502627, 727725502717, 725727017717, 725727017726,
725727107717, 725727107726, 725727126527, 725727216527, 725727306527, 725727324527,
725727324617, 725727414527, 725727414617, 725727504527, 725727504617, 725727521627,
725727521717, 725727611627, 725727611717, 725727701627, 725727701717, 726726017717,
726726017726, 726726107717, 726726107726, 726726126527, 726726216527, 726726306527,
726726324527, 726726324617, 726726414527, 726726414617, 726726504527, 726726504617,
726726521627, 726726521717, 726726611627, 726726611717, 726726701627, 726726701717,
727725017717, 727725017726, 727725107717, 727725107726, 727725126527, 727725216527,
727725306527, 727725324527, 727725324617, 727725414527, 727725414617, 727725504527,
727725504617, 727725521627, 727725521717, 727725611627, 727725611717, 727725701627,
727725701717, 725727126726, 725727127617, 725727216726, 725727217617, 725727306726,
725727307617, 725727324726, 725727414726, 725727504726, 725727523527, 725727523617,
725727613527, 725727613617, 725727703527, 725727703617, 725727720627, 725727720717,
726726126726, 726726127617, 726726216726, 726726217617, 726726306726, 726726307617,
726726324726, 726726414726, 726726504726, 726726523527, 726726523617, 726726613527,
726726613617, 726726703527, 726726703617, 726726720627, 726726720717, 727725126726,
727725127617, 727725216726, 727725217617, 727725306726, 727725307617, 727725324726,
727725414726, 727725504726, 727725523527, 727725523617, 727725613527, 727725613617,
727725703527, 727725703617, 727725720627, 727725720717, 725727327427, 725727327517,
725727417427, 725727417517, 725727507427, 725727507517, 725727523726, 725727524707,
725727613726, 725727614707, 725727703726, 725727704707, 725727722527, 725727722617,
725727722707, 726726327427, 726726327517, 726726417427, 726726417517, 726726507427,
726726507517, 726726523726, 726726524707, 726726613726, 726726614707, 726726703726,
726726704707, 726726722527, 726726722617, 726726722707, 727725327427, 727725327517,
727725417427, 727725417517, 727725507427, 727725507517, 727725523726, 727725524707,
727725613726, 727725614707, 727725703726, 727725704707, 727725722527, 727725722617,
727725722707, 725727327626, 725727327707, 725727327716, 725727327725, 725727417626,
725727417707, 725727417716, 725727417725, 725727507626, 725727507707, 725727507716,
725727507725, 725727526427, 725727526517, 725727616427, 725727616517, 725727706427,
725727706517, 725727722726, 725727724427, 725727724517, 725727724607, 726726327626,
726726327707, 726726327716, 726726327725, 726726417626, 726726417707, 726726417716,
726726417725, 726726507626, 726726507707, 726726507716, 726726507725, 726726526427,
726726526517, 726726616427, 726726616517, 726726706427, 726726706517, 726726722726,
726726724427, 726726724517, 726726724607, 727725327626, 727725327707, 727725327716,
727725327725, 727725417626, 727725417707, 727725417716, 727725417725, 727725507626,
727725507707, 727725507716, 727725507725, 727725526427, 727725526517, 727725616427,
727725616517, 727725706427, 727725706517, 727725722726, 727725724427, 727725724517,
727725724607, 725727526626, 725727526716, 725727526725, 725727527607, 725727616626,
725727616716, 725727616725, 725727617607, 725727706626, 725727706716, 725727706725,
725727707607, 725727724626, 725727724716, 725727724725, 726726526626, 726726526716,
726726526725, 726726527607, 726726616626, 726726616716, 726726616725, 726726617607,
726726706626, 726726706716, 726726706725, 726726707607, 726726724626, 726726724716,
726726724725, 727725526626, 727725526716, 727725526725, 727725527607, 727725616626,
727725616716, 727725616725, 727725617607, 727725706626, 727725706716, 727725706725,
727725707607, 727725724626, 727725724716, 727725724725, 725727727327, 725727727417,
725727727507, 726726727327, 726726727417, 726726727507, 727725727327, 727725727417,
727725727507, 725727727526, 725727727616, 725727727706, 725727727724, 726726727526,
726726727616, 726726727706, 726726727724, 727725727526, 727725727616, 727725727706,
727725727724, 527727727727, 617727727727, 627627727727, 627717727727, 707727727727,
717627727727, 717717727727, 727527727727, 727617727727, 727707727727, 726727010527,
726727010617, 726727010626, 726727010707, 726727010716, 726727010725, 726727011427,
726727012327, 726727012417, 726727012507, 726727100527, 726727100617, 726727100626,
726727100707, 726727100716, 726727100725, 726727101427, 726727102327, 726727102417,
726727102507, 727726010527, 727726010617, 727726010626, 727726010707, 727726010716,
727726010725, 727726011427, 727726012327, 727726012417, 727726012507, 727726100527,
727726100617, 727726100626, 727726100707, 727726100716, 727726100725, 727726101427,
727726102327, 727726102417, 727726102507, 726727012526, 726727012616, 726727012625,
726727012706, 726727012715, 726727012724, 726727014227, 726727014317, 726727014407,
726727102526, 726727102616, 726727102625, 726727102706, 726727102715, 726727102724,
726727104227, 726727104317, 726727104407, 726727120427, 726727121327, 726727121417,
726727121507, 726727210427, 726727211327, 726727211417, 726727211507, 726727300427,
726727301327, 726727301417, 726727301507, 727726012526, 727726012616, 727726012625,
727726012706, 727726012715, 727726012724, 727726014227, 727726014317, 727726014407,
727726102526, 727726102616, 727726102625, 727726102706, 727726102715, 727726102724,
727726104227, 727726104317, 727726104407, 727726120427, 727726121327, 727726121417,
727726121507, 727726210427, 727726211327, 727726211417, 727726211507, 727726300427,
727726301327, 727726301417, 727726301507, 726727014426, 726727014516, 726727014525,
726727014606, 726727014615, 726727014624, 726727104426, 726727104516, 726727104525,

726727104606, 726727104615, 726727104624, 726727121526, 726727121616, 726727121625,
726727121706, 726727121715, 726727121724, 726727123227, 726727123317, 726727123407,
726727211526, 726727211616, 726727211625, 726727211706, 726727211715, 726727211724,
726727213227, 726727213317, 726727213407, 726727301526, 726727301616, 726727301625,
726727301706, 726727301715, 726727301724, 726727303227, 726727303317, 726727303407,
726727320327, 726727320417, 726727320507, 726727410327, 726727410417, 726727410507,
726727500327, 726727500417, 726727500507, 727726014426, 727726014516, 727726014525,
727726014606, 727726014615, 727726014624, 727726104426, 727726104516, 727726104525,
727726104606, 727726104615, 727726104624, 727726121526, 727726121616, 727726121625,
727726121706, 727726121715, 727726121724, 727726123227, 727726123317, 727726123407,
727726211526, 727726211616, 727726211625, 727726211706, 727726211715, 727726211724,
727726213227, 727726213317, 727726213407, 727726301526, 727726301616, 727726301625,
727726301706, 727726301715, 727726301724, 727726303227, 727726303317, 727726303407,
727726320327, 727726320417, 727726320507, 727726410327, 727726410417, 727726410507,
727726500327, 727726500417, 727726500507, 726727002727, 726727017127, 726727017217,
726727017307, 726727107127, 726727107217, 726727107307, 726727123426, 726727123516,
726727123525, 726727123606, 726727123615, 726727123624, 726727213426, 726727213516,
726727213525, 726727213606, 726727213615, 726727213624, 726727303426, 726727303516,
726727303525, 726727303606, 726727303615, 726727303624, 726727320526, 726727320616,
726727320625, 726727320706, 726727320715, 726727320724, 726727322227, 726727322317,
726727322407, 726727410526, 726727410616, 726727410625, 726727410706, 726727410715,
726727410724, 726727412227, 726727412317, 726727412407, 726727500526, 726727500616,
726727500625, 726727500706, 726727500715, 726727500724, 726727502227, 726727502317,
726727502407, 727726002727, 727726017127, 727726017217, 727726017307, 727726107127,
727726107217, 727726107307, 727726123426, 727726123516, 727726123525, 727726123606,
727726123615, 727726123624, 727726213426, 727726213516, 727726213525, 727726213606,
727726213615, 727726213624, 727726303426, 727726303516, 727726303525, 727726303606,
727726303615, 727726303624, 727726320526, 727726320616, 727726320625, 727726320706,
727726320715, 727726320724, 727726322227, 727726322317, 727726322407, 727726410526,
727726410616, 727726410625, 727726410706, 727726410715, 727726410724, 727726412227,
727726412317, 727726412407, 727726500526, 727726500616, 727726500625, 727726500706,
727726500715, 727726500724, 727726502227, 727726502317, 727726502407, 627727012727,
627727102727, 717727012727, 717727102727, 726727004627, 726727004717, 726727004726,
726727017326, 726727017416, 726727017425, 726727017506, 726727017515, 726727017524,
726727107326, 726727107416, 726727107425, 726727107506, 726727107515, 726727107524,
726727124705, 726727124714, 726727126127, 726727126217, 726727126307, 726727214705,
726727214714, 726727216127, 726727216217, 726727216307, 726727304705, 726727304714,
726727306127, 726727306217, 726727306307, 726727322426, 726727322516, 726727322525,
726727322606, 726727322615, 726727322624, 726727322705, 726727322714, 726727324127,
726727324217, 726727324307, 726727412426, 726727412516, 726727412525, 726727412606,
726727412615, 726727412624, 726727412705, 726727412714, 726727414127, 726727414217,
726727414307, 726727502426, 726727502516, 726727502525, 726727502606, 726727502615,
726727502624, 726727502705, 726727502714, 726727504127, 726727504217, 726727504307,
726727521227, 726727521317, 726727521407, 726727611227, 726727611317, 726727611407,
726727701227, 726727701317, 726727701407, 727627012727, 727627102727, 727717012727,
727717102727, 727726004627, 727726004717, 727726004726, 727726017326, 727726017416,
727726017425, 727726017506, 727726017515, 727726017524, 727726107326, 727726107416,
727726107425, 727726107506, 727726107515, 727726107524, 727726124705, 727726124714,
727726126127, 727726126217, 727726126307, 727726214705, 727726214714, 727726216127,
727726216217, 727726216307, 727726304705, 727726304714, 727726306127, 727726306217,
727726306307, 727726322426, 727726322516, 727726322525, 727726322606, 727726322615,
727726322624, 727726322705, 727726322714, 727726324127, 727726324217, 727726324307,
727726412426, 727726412516, 727726412525, 727726412606, 727726412615, 727726412624,
727726412705, 727726412714, 727726414127, 727726414217, 727726414307, 727726502426,
727726502516, 727726502525, 727726502606, 727726502615, 727726502624, 727726502705,
727726502714, 727726504127, 727726504217, 727726504307, 727726521227, 727726521317,
727726521407, 727726611227, 727726611317, 727726611407, 727726701227, 727726701317,
727726701407, 627727014627, 627727104627, 627727121727, 627727211727, 627727301727,
717727014627, 717727104627, 717727121727, 717727211727, 717727301727, 726727017705,
726727017714, 726727017723, 726727107705, 726727107714, 726727107723, 726727126326,
726727126416, 726727126425, 726727126506, 726727126515, 726727126524, 726727216326,
726727216416, 726727216425, 726727216506, 726727216515, 726727216524, 726727306326,
726727306416, 726727306425, 726727306506, 726727306515, 726727306524, 726727324326,
726727324416, 726727324425, 726727324506, 726727324515, 726727324524, 726727324605,
726727324614, 726727414326, 726727414416, 726727414425, 726727414506, 726727414515,
726727414524, 726727414605, 726727414614, 726727504326, 726727504416, 726727504425,
726727504506, 726727504515, 726727504524, 726727504605, 726727504614, 726727521426,
726727521516, 726727521525, 726727521606, 726727521615, 726727521624, 726727521705,
726727521714, 726727523127, 726727523217, 726727523307, 726727611426, 726727611516,
726727611525, 726727611606, 726727611615, 726727611624, 726727611705, 726727611714,
726727613127, 726727613217, 726727613307, 726727701426, 726727701516, 726727701525,
726727701606, 726727701615, 726727701624, 726727701705, 726727701714, 726727703127,
726727703217, 726727703307, 726727720227, 726727720317, 726727720407, 727627014627,
727627104627, 727627121727, 727627211727, 727627301727, 727717014627, 727717104627,

727717121727, 727717211727, 727717301727, 727726017705, 727726017714, 727726017723,
727726107705, 727726107714, 727726107723, 727726126326, 727726126416, 727726126425,
727726126506, 727726126515, 727726126524, 727726216326, 727726216416, 727726216425,
727726216506, 727726216515, 727726216524, 727726306326, 727726306416, 727726306425,
727726306506, 727726306515, 727726306524, 727726324326, 727726324416, 727726324425,
727726324506, 727726324515, 727726324524, 727726324605, 727726324614, 727726414326,
727726414416, 727726414425, 727726414506, 727726414515, 727726414524, 727726414605,
727726414614, 727726504326, 727726504416, 727726504425, 727726504506, 727726504515,
727726504524, 727726504605, 727726504614, 727726521426, 727726521516, 727726521525,
727726521606, 727726521615, 727726521624, 727726521705, 727726521714, 727726523127,
727726523217, 727726523307, 727726611426, 727726611516, 727726611525, 727726611606,
727726611615, 727726611624, 727726611705, 727726611714, 727726613127, 727726613217,
727726613307, 727726701426, 727726701516, 727726701525, 727726701606, 727726701615,
727726701624, 727726701705, 727726701714, 727726703127, 727726703217, 727726703307,
727726720227, 727726720317, 727726720407, 627727123627, 627727213627, 627727303627,
627727320727, 627727410727, 627727500727, 717727123627, 717727213627, 717727303627,
717727320727, 717727410727, 717727500727, 726727007527, 726727007617, 726727007626,
726727126723, 726727127605, 726727127614, 726727216723, 726727217605, 726727217614,
726727306723, 726727307605, 726727307614, 726727324723, 726727327027, 726727327117,
726727327207, 726727414723, 726727417027, 726727417117, 726727417207, 726727504723,
726727507027, 726727507117, 726727507207, 726727523326, 726727523416, 726727523425,
726727523506, 726727523515, 726727523524, 726727523605, 726727523614, 726727613326,
726727613416, 726727613425, 726727613506, 726727613515, 726727613524, 726727613605,
726727613614, 726727703326, 726727703416, 726727703425, 726727703506, 726727703515,
726727703524, 726727703605, 726727703614, 726727720426, 726727720516, 726727720525,
726727720606, 726727720615, 726727720624, 726727720705, 726727720714, 726727722127,
726727722217, 726727722307, 727627123627, 727627213627, 727627303627, 727627320727,
727627410727, 727627500727, 727717123627, 727717213627, 727717303627, 727717320727,
727717410727, 727717500727, 727726007527, 727726007617, 727726007626, 727726126723,
727726127605, 727726127614, 727726216723, 727726217605, 727726217614, 727726306723,
727726307605, 727726307614, 727726324723, 727726327027, 727726327117, 727726327207,
727726414723, 727726417027, 727726417117, 727726417207, 727726504723, 727726507027,
727726507117, 727726507207, 727726523326, 727726523416, 727726523425, 727726523506,
727726523515, 727726523524, 727726523605, 727726523614, 727726613326, 727726613416,
727726613425, 727726613506, 727726613515, 727726613524, 727726613605, 727726613614,
727726703326, 727726703416, 727726703425, 727726703506, 727726703515, 727726703524,
727726703605, 727726703614, 727726720426, 727726720516, 727726720525, 727726720606,
727726720615, 727726720624, 727726720705, 727726720714, 727726722127, 727726722217,
727726722307, 627727017527, 627727107527, 627727124717, 627727214717, 627727304717,
627727322627, 627727322717, 627727412627, 627727412717, 627727502627, 627727502717,
717727017527, 717727107527, 717727124717, 717727214717, 717727304717, 717727322627,
717727322717, 717727412627, 717727412717, 717727502627, 717727502717, 726727327226,
726727327316, 726727327325, 726727327406, 726727327415, 726727327424, 726727327505,
726727327514, 726727417226, 726727417316, 726727417325, 726727417406, 726727417415,
726727417424, 726727417505, 726727417514, 726727507226, 726727507316, 726727507325,
726727507406, 726727507415, 726727507424, 726727507505, 726727507514, 726727523723,
726727524704, 726727526027, 726727526117, 726727526207, 726727613723, 726727614704,
726727616027, 726727616117, 726727616207, 726727703723, 726727704704, 726727706027,
726727706117, 726727706207, 726727722326, 726727722416, 726727722425, 726727722506,
726727722515, 726727722524, 726727722605, 726727722614, 726727722704, 726727724027,
726727724117, 726727724207, 727627017527, 727627107527, 727627124717, 727627214717,
727627304717, 727627322627, 727627322717, 727627412627, 727627412717, 727627502627,
727627502717, 727717017527, 727717107527, 727717124717, 727717214717, 727717304717,
727717322627, 727717322717, 727717412627, 727717412717, 727717502627, 727717502717,
727726327226, 727726327316, 727726327325, 727726327406, 727726327415, 727726327424,
727726327505, 727726327514, 727726417226, 727726417316, 727726417325, 727726417406,
727726417415, 727726417424, 727726417505, 727726417514, 727726507226, 727726507316,
727726507325, 727726507406, 727726507415, 727726507424, 727726507505, 727726507514,
727726523723, 727726524704, 727726526027, 727726526117, 727726526207, 727726613723,
727726614704, 727726616027, 727726616117, 727726616207, 727726703723, 727726704704,
727726706027, 727726706117, 727726706207, 727726722326, 727726722416, 727726722425,
727726722506, 727726722515, 727726722524, 727726722605, 727726722614, 727726722704,
727726724027, 727726724117, 727726724207, 627727017717, 627727017726, 627727107717,
627727107726, 627727126527, 627727216527, 627727306527, 627727324527, 627727324617,
627727414527, 627727414617, 627727504527, 627727504617, 627727521627, 627727521717,
627727611627, 627727611717, 627727701627, 627727701717, 717727017717, 717727017726,
717727107717, 717727107726, 717727126527, 717727216527, 717727306527, 717727324527,
717727324617, 717727414527, 717727414617, 717727504527, 717727504617, 717727521627,
717727521717, 717727611627, 717727611717, 717727701627, 717727701717, 726727327623,
726727327704, 726727327713, 726727327722, 726727417623, 726727417704, 726727417713,
726727417722, 726727507623, 726727507704, 726727507713, 726727507722, 726727526226,
726727526316, 726727526325, 726727526406, 726727526415, 726727526424, 726727526505,
726727526514, 726727616226, 726727616316, 726727616325, 726727616406, 726727616415,
726727616424, 726727616505, 726727616514, 726727706226, 726727706316, 726727706325,

726727706406, 726727706415, 726727706424, 726727706505, 726727706514, 726727722723,
726727724226, 726727724316, 726727724325, 726727724406, 726727724415, 726727724424,
726727724505, 726727724514, 726727724604, 727627017717, 727627017726, 727627107717,
727627107726, 727627126527, 727627216527, 727627306527, 727627324527, 727627324617,
727627414527, 727627414617, 727627504527, 727627504617, 727627521627, 727627521717,
727627611627, 727627611717, 727627701627, 727627701717, 727717017717, 727717017726,
727717107717, 727717107726, 727717126527, 727717216527, 727717306527, 727717324527,
727717324617, 727717414527, 727717414617, 727717504527, 727717504617, 727717521627,
727717521717, 727717611627, 727717611717, 727717701627, 727717701717, 727726327623,
727726327704, 727726327713, 727726327722, 727726417623, 727726417704, 727726417713,
727726417722, 727726507623, 727726507704, 727726507713, 727726507722, 727726526226,
727726526316, 727726526325, 727726526406, 727726526415, 727726526424, 727726526505,
727726526514, 727726616226, 727726616316, 727726616325, 727726616406, 727726616415,
727726616424, 727726616505, 727726616514, 727726706226, 727726706316, 727726706325,
727726706406, 727726706415, 727726706424, 727726706505, 727726706514, 727726722723,
727726724226, 727726724316, 727726724325, 727726724406, 727726724415, 727726724424,
727726724505, 727726724514, 727726724604, 627727126726, 627727127617, 627727216726,
627727217617, 627727306726, 627727307617, 627727324726, 627727414726, 627727504726,
627727523527, 627727523617, 627727613527, 627727613617, 627727703527, 627727703617,
627727720627, 627727720717, 717727126726, 717727127617, 717727216726, 717727217617,
717727306726, 717727307617, 717727324726, 717727414726, 717727504726, 717727523527,
717727523617, 717727613527, 717727613617, 717727703527, 717727703617, 717727720627,
717727720717, 726727526623, 726727526713, 726727526722, 726727527604, 726727616623,
726727616713, 726727616722, 726727617604, 726727706623, 726727706713, 726727706722,
726727707604, 726727724623, 726727724713, 726727724722, 726727727017, 726727727107,
727627126726, 727627127617, 727627216726, 727627217617, 727627306726, 727627307617,
727627324726, 727627414726, 727627504726, 727627523527, 727627523617, 727627613527,
727627613617, 727627703527, 727627703617, 727627720627, 727627720717, 727717126726,
727717127617, 727717216726, 727717217617, 727717306726, 727717307617, 727717324726,
727717414726, 727717504726, 727717523527, 727717523617, 727717613527, 727717613617,
727717703527, 727717703617, 727717720627, 727717720717, 727726526623, 727726526713,
727726526722, 727726527604, 727726616623, 727726616713, 727726616722, 727726617604,
727726706623, 727726706713, 727726706722, 727726707604, 727726724623, 727726724713,
727726724722, 727726727017, 727726727107, 627727327427, 627727327517, 627727417427,
627727417517, 627727507427, 627727507517, 627727523726, 627727524707, 627727613726,
627727614707, 627727703726, 627727704707, 627727722527, 627727722617, 627727722707,
717727327427, 717727327517, 717727417427, 717727417517, 717727507427, 717727507517,
717727523726, 717727524707, 717727613726, 717727614707, 717727703726, 717727704707,
717727722527, 717727722617, 717727722707, 726727727126, 726727727216, 726727727306,
726727727324, 726727727414, 726727727504, 727627327427, 727627327517, 727627417427,
727627417517, 727627507427, 727627507517, 727627523726, 727627524707, 727627613726,
727627614707, 727627703726, 727627704707, 727627722527, 727627722617, 727627722707,
727717327427, 727717327517, 727717417427, 727717417517, 727717507427, 727717507517,
727717523726, 727717524707, 727717613726, 727717614707, 727717703726, 727717704707,
727717722527, 727717722617, 727717722707, 727726727126, 727726727216, 727726727306,
727726727324, 727726727414, 727726727504, 627727327626, 627727327707, 627727327716,
627727327725, 627727417626, 627727417707, 627727417716, 627727417725, 627727507626,
627727507707, 627727507716, 627727507725, 627727526427, 627727526517, 627727616427,
627727616517, 627727706427, 627727706517, 627727722726, 627727724427, 627727724517,
627727724607, 717727327626, 717727327707, 717727327716, 717727327725, 717727417626,
717727417707, 717727417716, 717727417725, 717727507626, 717727507707, 717727507716,
717727507725, 717727526427, 717727526517, 717727616427, 717727616517, 717727706427,
717727706517, 717727722726, 717727724427, 717727724517, 717727724607, 726727727523,
726727727613, 726727727703, 726727727721, 727627327626, 727627327707, 727627327716,
727627327725, 727627417626, 727627417707, 727627417716, 727627417725, 727627507626,
727627507707, 727627507716, 727627507725, 727627526427, 727627526517, 727627616427,
727627616517, 727627706427, 727627706517, 727627722726, 727627724427, 727627724517,
727627724607, 727717327626, 727717327707, 727717327716, 727717327725, 727717417626,
727717417707, 727717417716, 727717417725, 727717507626, 727717507707, 727717507716,
727717507725, 727717526427, 727717526517, 727717616427, 727717616517, 727717706427,
727717706517, 727717722726, 727717724427, 727717724517, 727717724607, 727726727523,
727726727613, 727726727703, 727726727721, 627727526626, 627727526716, 627727526725,
627727527607, 627727616626, 627727616716, 627727616725, 627727617607, 627727706626,
627727706716, 627727706725, 627727707607, 627727724626, 627727724716, 627727724725,
717727526626, 717727526716, 717727526725, 717727527607, 717727616626, 717727616716,
717727616725, 717727617607, 717727706626, 717727706716, 717727706725, 717727707607,
717727724626, 717727724716, 717727724725, 727627526626, 727627526716, 727627526725,
727627527607, 727627616626, 727627616716, 727627616725, 727627617607, 727627706626,
727627706716, 727627706725, 727627707607, 727627724626, 727627724716, 727627724725,
727717526626, 727717526716, 727717526725, 727717527607, 727717616626, 727717616716,
727717616725, 727717617607, 727717706626, 727717706716, 727717706725, 727717707607,
727717724626, 727717724716, 727717724725, 627727727327, 627727727417, 627727727507,
717727727327, 717727727417, 717727727507, 727627727327, 727627727417, 727627727507,
727717727327, 727717727417, 727717727507, 627727727526, 627727727616, 627727727706,

627727727724, 717727727526, 717727727616, 717727727706, 717727727724, 727627727526,
727627727616, 727627727706, 727627727724, 727717727526, 727717727616, 727717727706,
727717727724, 727727010127, 727727010217, 727727010226, 727727010307, 727727010316,
727727010325, 727727010406, 727727010415, 727727010505, 727727011027, 727727011117,
727727011207, 727727012017, 727727012107, 727727100127, 727727100217, 727727100226,
727727100307, 727727100316, 727727100325, 727727100406, 727727100415, 727727100505,
727727101027, 727727101117, 727727101207, 727727102017, 727727102107, 727727010524,
727727010614, 727727010623, 727727010704, 727727010713, 727727010722, 727727011424,
727727012126, 727727012216, 727727012225, 727727012306, 727727012315, 727727012324,
727727012405, 727727012414, 727727012504, 727727014007, 727727100524, 727727100614,
727727100623, 727727100704, 727727100713, 727727100722, 727727101424, 727727102126,
727727102216, 727727102225, 727727102306, 727727102315, 727727102324, 727727102405,
727727102414, 727727102504, 727727104007, 727727120027, 727727120117, 727727120207,
727727121017, 727727121107, 727727210027, 727727210117, 727727210207, 727727211017,
727727211107, 727727300027, 727727300117, 727727300207, 727727301017, 727727301107,
727727012523, 727727012613, 727727012622, 727727012703, 727727012712, 727727012721,
727727014026, 727727014116, 727727014125, 727727014206, 727727014215, 727727014224,
727727014305, 727727014314, 727727014404, 727727102523, 727727102613, 727727102622,
727727102703, 727727102712, 727727102721, 727727104026, 727727104116, 727727104125,
727727104206, 727727104215, 727727104224, 727727104305, 727727104314, 727727104404,
727727120424, 727727121126, 727727121216, 727727121225, 727727121306, 727727121315,
727727121324, 727727121405, 727727121414, 727727121504, 727727123007, 727727210424,
727727211126, 727727211216, 727727211225, 727727211306, 727727211315, 727727211324,
727727211405, 727727211414, 727727211504, 727727213007, 727727300424, 727727301126,
727727301216, 727727301225, 727727301306, 727727301315, 727727301324, 727727301405,
727727301414, 727727301504, 727727303007, 727727320017, 727727320107, 727727410017,
727727410107, 727727500017, 727727500107, 727727002327, 727727002417, 727727002426,
727727002507, 727727014423, 727727014513, 727727014522, 727727014603, 727727014612,
727727014621, 727727104423, 727727104513, 727727104522, 727727104603, 727727104612,
727727104621, 727727121523, 727727121613, 727727121622, 727727121703, 727727121712,
727727121721, 727727123026, 727727123116, 727727123125, 727727123206, 727727123215,
727727123224, 727727123305, 727727123314, 727727123404, 727727211523, 727727211613,
727727211622, 727727211703, 727727211712, 727727211721, 727727213026, 727727213116,
727727213125, 727727213206, 727727213215, 727727213224, 727727213305, 727727213314,
727727213404, 727727301523, 727727301613, 727727301622, 727727301703, 727727301712,
727727301721, 727727303026, 727727303116, 727727303125, 727727303206, 727727303215,
727727303224, 727727303305, 727727303314, 727727303404, 727727320126, 727727320216,
727727320225, 727727320306, 727727320315, 727727320324, 727727320405, 727727320414,
727727320504, 727727322007, 727727410126, 727727410216, 727727410225, 727727410306,
727727410315, 727727410324, 727727410405, 727727410414, 727727410504, 727727412007,
727727500126, 727727500216, 727727500225, 727727500306, 727727500315, 727727500324,
727727500405, 727727500414, 727727500504, 727727502007, 727727001527, 727727001617,
727727001626, 727727002616, 727727002625, 727727002706, 727727002724, 727727004227,
727727004317, 727727004326, 727727004407, 727727004416, 727727004506, 727727017016,
727727017025, 727727017106, 727727017115, 727727017124, 727727017205, 727727017214,
727727017304, 727727107016, 727727107025, 727727107106, 727727107115, 727727107124,
727727107205, 727727107214, 727727107304, 727727123423, 727727123513, 727727123522,
727727123603, 727727123612, 727727123621, 727727213423, 727727213513, 727727213522,
727727213603, 727727213612, 727727213621, 727727303423, 727727303513, 727727303522,
727727303603, 727727303612, 727727303621, 727727320523, 727727320613, 727727320622,
727727320703, 727727320712, 727727320721, 727727322026, 727727322116, 727727322125,
727727322206, 727727322215, 727727322224, 727727322305, 727727322314, 727727322404,
727727410523, 727727410613, 727727410622, 727727410703, 727727410712, 727727410721,
727727412026, 727727412116, 727727412125, 727727412206, 727727412215, 727727412224,
727727412305, 727727412314, 727727412404, 727727500523, 727727500613, 727727500622,
727727500703, 727727500712, 727727500721, 727727502026, 727727502116, 727727502125,
727727502206, 727727502215, 727727502224, 727727502305, 727727502314, 727727502404,
727727521007, 727727611007, 727727701007, 727727004525, 727727004615, 727727004624,
727727004705, 727727004714, 727727004723, 727727017323, 727727017413, 727727017422,
727727017503, 727727017512, 727727017521, 727727107323, 727727107413, 727727107422,
727727107503, 727727107512, 727727107521, 727727124702, 727727124711, 727727126016,
727727126025, 727727126106, 727727126115, 727727126124, 727727126205, 727727126214,
727727126304, 727727214702, 727727214711, 727727216016, 727727216025, 727727216106,
727727216115, 727727216124, 727727216205, 727727216214, 727727216304, 727727304702,
727727304711, 727727306016, 727727306025, 727727306106, 727727306115, 727727306124,
727727306205, 727727306214, 727727306304, 727727322423, 727727322513, 727727322522,
727727322603, 727727322612, 727727322621, 727727322702, 727727322711, 727727324016,
727727324025, 727727324106, 727727324115, 727727324124, 727727324205, 727727324214,
727727324304, 727727412423, 727727412513, 727727412522, 727727412603, 727727412612,
727727412621, 727727412702, 727727412711, 727727414016, 727727414025, 727727414106,
727727414115, 727727414124, 727727414205, 727727414214, 727727414304, 727727502423,
727727502513, 727727502522, 727727502603, 727727502612, 727727502621, 727727502702,
727727502711, 727727504016, 727727504025, 727727504106, 727727504115, 727727504124,
727727504205, 727727504214, 727727504304, 727727521026, 727727521116, 727727521125,

727727521206, 727727521215, 727727521224, 727727521305, 727727521314, 727727521404, 727727611026, 727727611116, 727727611125, 727727611206, 727727611215, 727727611224, 727727611305, 727727611314, 727727611404, 727727701026, 727727701116, 727727701125, 727727701206, 727727701215, 727727701224, 727727701305, 727727701314, 727727701404, 727727720007, 727727007127, 727727007217, 727727007226, 727727007307, 727727007316, 727727007406, 727727017702, 727727017711, 727727017720, 727727107702, 727727107711, 727727107720, 727727126323, 727727126413, 727727126422, 727727126503, 727727126512, 727727126521, 727727216323, 727727216413, 727727216422, 727727216503, 727727216512, 727727216521, 727727306323, 727727306413, 727727306422, 727727306503, 727727306512, 727727306521, 727727324323, 727727324413, 727727324422, 727727324503, 727727324512, 727727324521, 727727324602, 727727324611, 727727414323, 727727414413, 727727414422, 727727414503, 727727414512, 727727414521, 727727414602, 727727414611, 727727504323, 727727504413, 727727504422, 727727504503, 727727504512, 727727504521, 727727504602, 727727504611, 727727521423, 727727521513, 727727521522, 727727521603, 727727521612, 727727521621, 727727521702, 727727521711, 727727523016, 727727523025, 727727523106, 727727523115, 727727523124, 727727523205, 727727523214, 727727523304, 727727611423, 727727611513, 727727611522, 727727611603, 727727611612, 727727611621, 727727611702, 727727611711, 727727613016, 727727613025, 727727613106, 727727613115, 727727613124, 727727613205, 727727613214, 727727613304, 727727701423, 727727701513, 727727701522, 727727701603, 727727701612, 727727701621, 727727701702, 727727701711, 727727703016, 727727703025, 727727703106, 727727703115, 727727703124, 727727703205, 727727703214, 727727703304, 727727720026, 727727720116, 727727720125, 727727720206, 727727720215, 727727720224, 727727720305, 727727720314, 727727720404, 727727007425, 727727007515, 727727007524, 727727007605, 727727007614, 727727007623, 727727126720, 727727127602, 727727127611, 727727216720, 727727217602, 727727217611, 727727306720, 727727307602, 727727307611, 727727324720, 727727327006, 727727327015, 727727327024, 727727327105, 727727327114, 727727327204, 727727414720, 727727417006, 727727417015, 727727417024, 727727417105, 727727417114, 727727417204, 727727504720, 727727507006, 727727507015, 727727507024, 727727507105, 727727507114, 727727507204, 727727523323, 727727523413, 727727523422, 727727523503, 727727523512, 727727523521, 727727523602, 727727523611, 727727613323, 727727613413, 727727613422, 727727613503, 727727613512, 727727613521, 727727613602, 727727613611, 727727703323, 727727703413, 727727703422, 727727703503, 727727703512, 727727703521, 727727703602, 727727703611, 727727720423, 727727720513, 727727720522, 727727720603, 727727720612, 727727720621, 727727720702, 727727720711, 727727722016, 727727722025, 727727722106, 727727722115, 727727722124, 727727722205, 727727722214, 727727722304, 727727327223, 727727327313, 727727327322, 727727327403, 727727327412, 727727327421, 727727327502, 727727327511, 727727417223, 727727417313, 727727417322, 727727417403, 727727417412, 727727417421, 727727417502, 727727417511, 727727507223, 727727507313, 727727507322, 727727507403, 727727507412, 727727507421, 727727507502, 727727507511, 727727523720, 727727524701, 727727526006, 727727526015, 727727526024, 727727526105, 727727526114, 727727526204, 727727613720, 727727614701, 727727616006, 727727616015, 727727616024, 727727616105, 727727616114, 727727616204, 727727703720, 727727704701, 727727706006, 727727706015, 727727706024, 727727706105, 727727706114, 727727706204, 727727722323, 727727722413, 727727722422, 727727722503, 727727722512, 727727722521, 727727722602, 727727722611, 727727722701, 727727724006, 727727724015, 727727724024, 727727724105, 727727724114, 727727724204, 727727327620, 727727327701, 727727327710, 727727417620, 727727417701, 727727417710, 727727507620, 727727507701, 727727507710, 727727526223, 727727526313, 727727526322, 727727526403, 727727526412, 727727526421, 727727526502, 727727526511, 727727616223, 727727616313, 727727616322, 727727616403, 727727616412, 727727616421, 727727616502, 727727616511, 727727706223, 727727706313, 727727706322, 727727706403, 727727706412, 727727706421, 727727706502, 727727706511, 727727722720, 727727724223, 727727724313, 727727724322, 727727724403, 727727724412, 727727724421, 727727724502, 727727724511, 727727724601, 727727526620, 727727526710, 727727527601, 727727616620, 727727616710, 727727617601, 727727706620, 727727706710, 727727707601, 727727724620, 727727724710, 727727727014, 727727727104, 727727727123, 727727727213, 727727727303, 727727727321, 727727727411, 727727727501, 727727727520, 727727727610, 727727727700

D.6 4th round

2617429 vectors

D.7 2nd FL layer

12268480 vectors

D.8 5th round

58962 vectors

D.9 6th round

000000000004, 000000000013, 000000000022, 000000000103, 000000000112, 000000000121, 000000000202, 000000000211, 000000000220, 000000000301, 000000000310, 000000000400, 000000001003, 000000001012, 000000001021, 000000001102, 000000001111, 000000001120, 000000001201, 000000001210, 000000001300, 000000002002, 000000002011, 000000002020, 000000002101, 000000002110, 000000002200, 000000003001, 000000003010, 000000004100, 000000007000, 000000010003, 000000010012, 000000010021, 000000010102, 000000010111, 000000010120, 000000010201, 000000010210, 000000010300, 000000011002, 000000011011, 000000011020, 000000011101, 000000011110, 000000011200, 000000012001, 000000012010, 000000012100, 000000015000, 000000020002, 000000020011, 000000020020, 000000020101, 000000020110, 000000020200, 000000021001, 000000021010, 000000021100, 000000024000, 000000100003, 000000100012, 000000100021, 000000100102, 000000100111, 000000100120, 000000100201, 000000100210, 000000100300, 000000101002, 000000101011, 000000101020, 000000101101, 000000101110, 000000101200, 000000102001, 000000102010, 000000102100, 000000105000, 000000110002, 000000110011, 000000110020, 000000110101, 000000110110, 000000110200, 000000111001, 000000111010, 000000111100, 000000114000, 000000120001, 000000120010, 000000120100, 000000123000, 000000200002, 000000200011, 000000200020, 000000200101, 000000200110, 000000200200, 000000201001, 000000201010, 000000201100, 000000204000, 000000210001, 000000210010, 000000210100, 000000213000, 000000222000, 000000300001, 000000300010, 000000303000, 000000312000, 000000321000, 000000400100, 000000502000, 000000511000, 000000520000, 000000701000, 000000710000, 000001000000, 000010000000, 000100000000, 001000000000, 010000000000, 100000000001, 100000000010, 100000000100, 100000001000, 100000010000, 100000100000, 200000000000

6 段と 2FL 層を評価したあとの出力 Division Property は上述のように 131 個のベクトルで表現できる．今 $e_i \in \mathbb{Z}^{12}$ を i 番目の要素が 1 であり，残りの全ての要素が 0 である単位ベクトルとする．Division Property が $\mathcal{D}_{\mathbb{K}}^{7,2,7,7,2,7,7,2,7,7,2,7}$ のとき，$\mathbb{K}$ が単位ベクトル e_i を含まない場合

$$\bigoplus_{\vec{x}\in\mathbb{K}} x_i = 0$$

となることが分かる．上述した 131 個のベクトルは 100000000000 を含まないことから，先頭 7 ビットの和は常に 0 となることが分かる．