北海道科学大学研究紀要
第51号（2023年）
論文

Bulletin of Hokkaido University
of Science, No.51(2023)
Papers

共通鍵ブロック暗号 SLIM に対する中間一致攻撃を用いた安全性の評価

Security evaluation for the symmetric block cipher SLIM based on Meet-in-the-Middle Attack.

杉尾　信行 *

Nobuyuki Sugio

2023 年 9 月 13 日

概要

The symmetric block cipher SLIM proposed by Aboushosha is one of the Lightweight cryptographies. SLIM is designed for the Radio frequency identifcation (RFID) systems. SLIM is a 32-bit block cipher based on the Feistel structure with a 80-bit secret key. In this paper, we present a Meet-in-the-Middle attack on reduced-round SLIM. We show that 11-round SLIM is attackable with 20 pairs of known plaintext-ciphertext, $2^{73.4}$ times of encryption and $2^{70.4}$ bytes of memory.

1　序論

共通鍵ブロック暗号 SLIM は Aboushosha らによって RFID システム向けに設計された軽量暗号アルゴリズムである [1]．SLIM の入出力ブロック長は 32-bit，秘密鍵長は 80-bit，標準段数は 32 段で構成されている．

共通鍵ブロック暗号の安全性評価は，計算量理論的安全性[*1]に基づいて評価が行われている．計算量理論的安全性は，アルゴリズムの計算量に着目した安全性の尺度である．秘密鍵 K bit の総当たりを行う全数探索法（Brute Force Method）を用いた場合，2^K 回の暗号化計算量が必要となる．全数探索法は暗号の内部構造に依らず，秘密鍵のサイズに応じて解読に必要な計算量を見積もる事ができる．暗号アルゴリズムが既知の場合，攻撃者は暗号アルゴリズムの内部構造を利用して全数探索法よりも効率的な攻撃を目指す手法をショートカット法（Short Cut Method）と呼ぶ．

近年，共通鍵ブロック暗号に対する代表的なショートカット法として差分攻撃（Differential Cryptanalysis）[2] と線形攻撃（Linear Cryptanalysis）[3] が知られている．SLIM の提案書では，差分攻撃と線形攻撃に関する評価はなされているが，中間一致攻撃（Meet-in-the-Middle Attack）への耐性評価はなされていない．

中間一致攻撃 [4] は Diffie と Hellman が提案した拡大鍵生成部の脆弱性を利用して攻撃する手法である．中間一致攻撃は共通鍵暗号に対して差分攻撃や線形攻撃と同様に汎用的かつ強力な攻撃手法の一つである [5]–[11]．本論文では，SLIM に対する中間一致攻撃を行い，第三者の観点から SLIM の安全性を評価する事を目的とする．

本論文の貢献を以下に示す．

- 縮小版 SLIM に対し，発見的手法を用いて中間一致攻撃が可能な拡大鍵の探索を調査した．調査の結果，11 段の縮小版 SLIM に対して秘密

* 北海道科学大学 工学部 情報工学科

[*1] その他の安全性は「統計的安全性」や「情報理論的安全性」等の指標がある．[21]

表 1　結果一覧

Round	Data [pairs]	Encryption [times]	Memory [bytes]	Method
11	20 KP	$2^{73.4}$	$2^{70.4}$	Meet-in-the-Middle Attack (**本稿**)
12	2^{31} CP	$2^{77.1}$	-	Higher-order Differential Attack[13]
14	2^{32} CP	2^{32}	$2^{12.58}$	Differential Cryptanalysis[14]

KP（Known Plaintext）：既知平文・暗号文組（攻撃者は既知の平文と対応する暗号文を入手可能）
CP（Chosen Plaintext）：選択平文・暗号文組（攻撃者は任意の平文と対応する暗号文を入手可能）

鍵の全数探索法よりも効率的な中間一致特性が存在する事を明らかにした．

- 発見した特性を用いて，11 段の縮小版 SLIM に対する鍵回復攻撃を示す．鍵回復攻撃に必要な既知平文・暗号文組数は 20，暗号化計算量は $2^{73.4}$ 回である．また，必要なメモリ量は $2^{70.4}$ bytes である．結果を表 1 に示す．

最後に本論文の構成を以下に示す．第 2 章で SLIM の関連研究を示す．第 3 章で中間一致攻撃の概要を述べる．第 4 章で共通鍵ブロック暗号 SLIM の内部構造について説明する．第 5 章で SLIM に対する中間一致攻撃が可能な特性を示し，第 6 章で SLIM に対する中間一致攻撃を行う．第 7 章にて考察を述べた後，第 8 章で結論と今後の課題を示す．

2　関連研究

曽山らは共通鍵ブロック暗号 SLIM に対して計算機実験により高階差分特性 [12] を網羅的に調査し，9 段の 31 階差分特性が存在する事を発見した [13]．また，9 段の特性を用いて 12 段の SLIM に対する鍵回復攻撃を示した．攻撃に必要な選択平文・暗号文組数は 2^{31}，暗号化計算量は $2^{77.1}$ 回である．

また，Chan らは SLIM に対する差分特性を調査し，14 段の SLIM に対する鍵回復攻撃を示した [14]．攻撃に必要な選択平文・暗号文組数は 2^{32}，暗号化計算量は 2^{32} 回である．また，必要なメモリ量は $2^{12.58}$ bytes である．尚，Chan らの差分攻撃は平文空間 2^{32} の全てを用いるフル・コードブック攻撃である事に注意が必要である．

3　中間一致攻撃

中間一致攻撃（Meet-in-the-Middle Attack）は Diffie と Hellman らによって提案された共通鍵ブロック暗号に対する攻撃手法である [4]．以下に攻撃の概要と攻撃に必要な平文数，メモリ量と暗号化計算量を示す．

3.1　攻撃の概要

$E(X;K)$ を入力 $X \in GF(2)^n$，鍵 $K \in GF(2)^s$ から $Y \in GF(2)^m$ を出力する暗号化関数とする．暗号化関数 $E(\cdot)$ を 2 段繰り返す暗号を考える．

$$C = E(E(P;K_1);K_2) \tag{1}$$

P は既知平文，C は既知平文 P に対応する暗号文を表し，K_1 と K_2 は各暗号化関数で使用される拡大鍵を示す．尚，秘密鍵 $K = K_1||K_2$ とし，秘密鍵長は $2s$ ビットとする．記号 $||$ は結合を表す．

中間一致攻撃は，既知平文 P を拡大鍵 K_1 で暗号化して得られる中間値と，暗号文 C を拡大鍵 K_2 で復号して得られる中間値が確率的に一致する事を利用して，拡大鍵 K_1 と K_2 を導出する手法である．

3.2　攻撃に必要な平文数，メモリ量と暗号化計算量

攻撃者は異なる 2 組の既知平文・暗号文組（$P1, C1$）と（$P2, C2$）を予め入手したとする．

まず始めに既知平文 $P1$ を拡大鍵 K_1 の全ての候補で暗号化して得られる中間値を Z_{K_1} とし，その集合を $\{Z_{K_1}\}$ とする．

$$Z_{K_1} = E(P1;K_1) \tag{2}$$

続いて，暗号文 $C1$ を拡大鍵 K_2 の全ての候補で復号して得られる中間値を Z_{K_2} とし，その集合を

$\{Z_{K_2}\}$ とする．

$$Z_{K_2} = E^{-1}(C; K_2) \tag{3}$$

ここで $E^{-1}(\cdot)$ は暗号化関数 E の逆関数を示し，$Z_{K_2} \in GF(2)^m$ とする．

集合 $\{Z_{K_1}\}$ と集合 $\{Z_{K_2}\}$ には，値が一致する要素（即ち $Z_{K_1} = Z_{K_2}$）が少なくとも 1 つ存在する．この時の拡大鍵 K_1 と K_2 の候補 (K_1', K_2') に対し，別の既知平文・暗号文組 $(P2, C2)$ を用いて以下の計算が成立するか検証する．

$$C2 = E(E(P2; K_1'); K_2') \tag{4}$$

式 (4) が成立すれば，推定した鍵候補 (K_1', K_2') は正しい拡大鍵とする．成立しなければ，新たな候補 (K_1', K_2') に対して式 (4) を検証する．

中間一致攻撃に必要な暗号化計算量は式 (2) と (3) を別々に計算する為，$T = 2 \times 2^s$ 回である．また，メモリ量は $M = 2 \times 2^s/8$ bytes である．

4 共通鍵ブロック暗号 SLIM

4.1 表記法

- P：平文 32-bit.
- C：平文 P に対応する暗号文 32-bit．上位 16-bit（左 16-bit）を C_L，下位 16-bit（右 16-bit）を C_R と表す．
- L_i：i 段目出力（$i = 1, 2, \cdots, 32$）上位 16-bit データ．平文 P の上位 16-bit は L_0 と表す．
- R_i：i 段目出力（$i = 1, 2, \cdots, 32$）下位 16-bit データ．平文 P の下位 16-bit は R_0 と表す．
- $Z[j]$：中間値 Z の j（$j = 0, 1, \cdots, 15$） ビット目の値を示す．上位（左）から順に $j = 0, 1, 2, \cdots, 15$ とする．複数ビットを同時に示す場合は $Z[j-k]$ の様に記す．
- $\ll$：左巡回シフト．例えば中間値 Z を 2 bit 左巡回シフトする場合，$Z \ll_2$ と示す．

4.2 内部構造

共通鍵ブロック暗号 SLIM は Aboushosha らが提案した RFID 向け軽量暗号アルゴリズムである [1]．入出力ブロック長は 32-bit，秘密鍵長は 80-bit であり，標準段数は 32 段の Feistel 型構造である．SLIM の段関数を図 1 に示す．SLIM の段関数は，4-bit 入出力の非線形関数 S-box を 4 つ並列にした構造と線形関数 Q にて構成される．S-box の入出力テーブルを表 2 に示す．また，線形関数 Q は 16-bit 入出力を持つ関数であり，内部構造を図 2 に示す．線形関数 Q は表 3 に従って 1-bit 毎に並べ替える処理を行う．

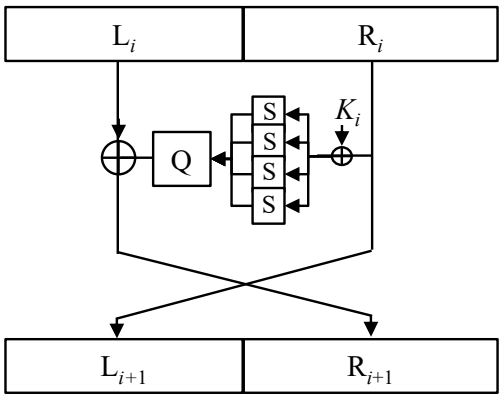

図 1　段関数

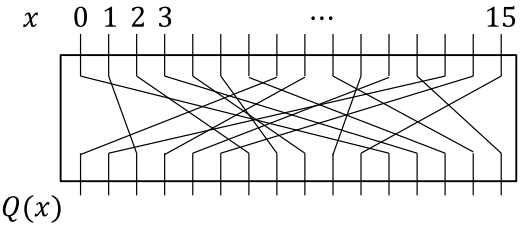

図 2　線形関数 Q

4.3 拡大鍵生成部

共通鍵ブロック暗号 SLIM は 80-bit の秘密鍵から，各段で使用する 16-bit の拡大鍵 K_i（$i = 1, 2, \cdots, 32$）を生成する．拡大鍵 K_i は SLIM の全体構造とは独立した拡大鍵生成部にて生成される．拡大鍵生成部の内部構造を図 3 に示す．

拡大鍵 K_i の生成は以下の手順で行われる．

- 拡大鍵 K_1，K_2，$\cdots$，K_5 は秘密鍵 80-bit から直接生成される．K_1 は秘密鍵 80-bit の最下位 16-bit であり，K_2 は次の 16-bit，以下同様に

表 2　S-box

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S(x)$	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2

表 3　線形関数 Q

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$Q(x)$	7	13	1	8	11	14	2	5	4	10	15	0	3	6	9	12

表 4　拡大鍵生成部で用いられる S-box

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S(x)$	0	8	6	D	5	F	7	C	4	E	2	3	9	1	B	A

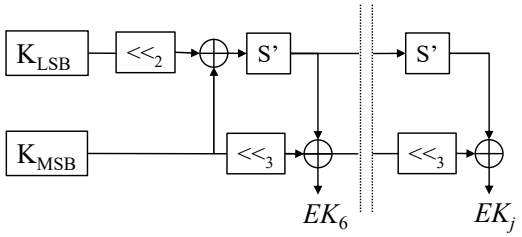

図 3　拡大鍵生成部

して K_5 までの拡大鍵を導出する．

- 秘密鍵 80-bit を上位 40-bit（K_{MSB}）と下位 40-bit（K_{LSB}）に分割する．S' は表 4 に示す 4-bit 入出力の S-box を 10 個並列にした関数である．2bit 又は 3bit の左巡回シフトは 4bit 単位で処理される．拡大鍵生成部の各出力 EK_j は 40 bit である．拡大鍵 K_6 は EK_6 の下位 16 bit，K_7 は EK_6 の次の 16bit である．K_8 は EK_6 の上位 8bit と EK_7 の下位 8 ビットを連結したものである．以下同様にして拡大鍵 K_i ($i = 6, 7, \cdots, 32$) が生成される．

5　SLIM の特性解析

本章では，中間一致攻撃に用いる事が可能な SLIM の特性について記す．本稿では便宜上，4 つ並列に並んだ S-box の上位から順に S_1，S_2，S_3，S_4 とする．各 S-box に入力される拡大鍵の少なくとも 1-bit が未知の場合，未知の拡大鍵の影響がどの様に広がるのか特性を解析した．表 5 から表 12 に得られた特性を示す．

記号 0 は未知の拡大鍵の影響を受けないビット位置を示し，記号？は拡大鍵の影響により値が未知となるビット位置を示す．解析の結果，拡大鍵の少なくとも 1-bit が未知の場合，暗号化の時は 3 段目出力 32-bit が全て未知になる事が判明し，復号の時は 1 段目出力 32-bit が全て未知になる事が判明した．

表 5　拡大鍵の影響伝搬特性 (暗号化，S_1 の場合)

段数	(L_i, R_i)
1	(0000000000000000, 00?000?0000??000)
2	(00?000?0000??000, ????????????????)
3	(????????????????, ????????????????)

表 6　拡大鍵の影響伝搬特性 (暗号化，S_2 の場合)

段数	(L_i, R_i)
1	(0000000000000000, ?000000??0000?00)
2	(?000000??0000?00, ????????????????)
3	(????????????????, ????????????????)

表 7　拡大鍵の影響伝搬特性 (暗号化，S_3 の場合)

段数	$(L_i,\ R_i)$
1	$(0000000000000000, 000??0000?0000?0)$
2	$(000??0000?0000?0, ????????????????)$
3	$(????????????????, ????????????????)$

表 8　拡大鍵の影響伝搬特性 (暗号化，S_4 の場合)

段数	$(L_i,\ R_i)$
1	$(0000000000000000, 0?000?0000?0000?)$
2	$(0?000?0000?0000?, ????????????????)$
3	$(????????????????, ????????????????)$

表 9　拡大鍵の影響伝搬特性 (復号，S_1 の場合)

段数	$(L_i,\ R_i)$
1	$(????????????????, ????????????????)$
2	$(????????????????, 00?000?0000??000)$
3	$(00?000?0000??000, 0000000000000000)$

表 10　拡大鍵の影響伝搬特性 (復号，S_2 の場合)

段数	$(L_i,\ R_i)$
1	$(????????????????, ????????????????)$
2	$(????????????????, ?000000??0000?00)$
3	$(?000000??0000?00, 0000000000000000)$

表 11　拡大鍵の影響伝搬特性 (復号，S_3 の場合)

段数	$(L_i,\ R_i)$
1	$(????????????????, ????????????????)$
2	$(????????????????, 000??0000?0000?0)$
3	$(000??0000?0000?0, 0000000000000000)$

表 12　拡大鍵の影響伝搬特性 (復号，S_4 の場合)

段数	$(L_i,\ R_i)$
1	$(????????????????, ????????????????)$
2	$(????????????????, 0?000?0000?0000?)$
3	$(0?000?0000?0000?, 0000000000000000)$

6　SLIM に対する中間一致攻撃

本章では，5 章で得られた特性を用いて 11 段に縮小した SLIM の鍵回復攻撃を示す．

6.1　攻撃者の条件

攻撃者の条件は「既知平文攻撃（攻撃者は既知の平文と，平文に対応した暗号文のペアが入手できる条件)」にて攻撃を行うものとし，拡大鍵生成部を含めた解析を行う事とする．

6.2　11 段 SLIM への鍵回復攻撃

本節にて 11 段 SLIM への鍵回復攻撃を行う．図 1 より，1 段毎に 16-bit の拡大鍵が存在する．1 段目から 4 段目の拡大鍵 K_i $(i = 1, 2, \cdots, 4)$ 64 bit と 5 段目の拡大鍵の上位 4 bit $K_5[0-3]$ の合計 68 bit を全数探索法にて推定した場合，6 段目出力の $L_6[j]$ $(j = 2, 6, 11, 12)$ 4 bit が平文から導出可能である．詳細は図 4 を参照のこと．尚，6 段目出力の白い部分は拡大鍵の推定によって平文から導出可能な部分であり，赤い部分は推定しない拡大鍵の影響で未知となる部分である．

同様に暗号文側から 11 段目から 8 段目の拡大鍵 K_i $(i = 11, 10, \cdots, 8)$ 64 bit と 7 段目の拡大鍵の上位 4 bit $K_7[0-3]$ の合計 68 bit を全数探索法にて推定した場合，6 段目出力 $L_6[j]$ $(j = 2, 6, 11, 12)$ 4 bit が暗号文から導出可能である．尚, 6 段目出力の白い部分は拡大鍵の推定によって暗号文から導出可能な部分であり，青い部分は推定しない拡大鍵の影響で未知となる部分である．$L_6[j]$ $(j = 2, 6, 11, 12)$ 4 bit の値を突き合わせる事により，11 段 SLIM の中間一致攻撃が可能である．

ここで，$L_6[j]$ $(j = 2, 6, 11, 12)$ は 4 bit である為，拡大鍵の推定が正しい場合は確率 1 で，推定が誤りの場合は確率 $(2^{-1})^4 = 1/16$ で $L_6[j]$ $(j = 2, 6, 11, 12)$ の値が一致する．その為，一組の既知平文・暗号文のペアから，拡大鍵の候補数を平均

1/16 個ずつ絞り込むことが出来る．従って，$2^{68} \cdot (2^{-4})^{\alpha} \ll 1$ を満たす異なる α 組の既知平文・暗号文ペアを用意する事で，推定した拡大鍵を一意に特定することが出来る．ここでは，$\alpha = 20$ とする．

以上から，11 段 SLIM の鍵回復攻撃に必要な既知平文・暗号文組数は $D = 20$ であり，拡大鍵の回復に必要な暗号化計算量は $T_1 = 2 \times 20 \times 2^{68} \approx 2^{73.4}$ 回である．また，メモリ量は $M = 2 \times 20 \times 2^{68}/8 \approx 2^{70.4}$ bytes である．

4 章に示す拡大鍵生成部を用いる事で，秘密鍵 80 bit の導出を行う．1 段目から 5 段目の拡大鍵は秘密鍵から直接導出される．従って，秘密鍵 80 bit 中 68 bit は上記の鍵回復攻撃にて導出済みである．残りの秘密鍵 12 bit は全数探索法を用いて導出を行う．SLIM の入出力長は 32 bit である為，1 組の平文・暗号文組を用いて 12 bit の秘密鍵に全数探索法を適用する場合，偽鍵が生き残る確率は $2^{12} \times 2^{-32} = 2^{-24}$ である．その為，偽鍵をふるいにかける為に必要な平文・暗号文組は 1 組で十分であり，この際に用いる平文・暗号文ペアは前述の既知平文・暗号文ペアを流用可能である．その為，残りの秘密鍵 12 bit の回復に必要な暗号化計算量は $T_2 = 2^{12}$ 回である．

以上から，秘密鍵 80 bit の導出に必要な暗号化計算量は以下の式で見積もられる．

$$T = T_1 + T_2 \approx 2^{73.4} \tag{5}$$

7 考察

本論文で用いた中間一致攻撃では，11 段の縮小版 SLIM に対して鍵回復攻撃を行った．中間一致攻撃を行う場合，攻撃者の前提条件は「既知平文・暗号文攻撃（既知の平文と，平文に対応した暗号文のペアが入手できる条件）」である．実際の攻撃を想定した場合，一般に，攻撃者の前提条件は以下の順で緩和される（即ち，攻撃者に有利な条件となる）．

1. 暗号文単独攻撃：攻撃者は暗号文のみを入手できる条件
2. 既知平文・暗号文攻撃：既知の平文と，平文に対応した暗号文のペアが入手できる条件
3. 選択平文・暗号文攻撃（又は，選択暗号文・平文攻撃）：攻撃者は任意の平文と対応する暗号文のペア（又は，任意の暗号文と対応する平文のペア）が入手できる条件

また，中間一致攻撃では，暗号化又は復号した値をメモリに保持する必要がある為，実際の鍵回復攻撃を行う際には既知平文・暗号文組数，暗号化計算量に加えてメモリ量も考慮する必要がある．本論文で示した中間一致攻撃で必要なメモリ量は $2^{70.4}$ bytes であり，現実的に用意する事は困難である為，理論的な結果として理解が必要である．

次に，本論文の研究成果が社会・産業界にどの様な有益性をもたらすのか以下で論じる．

未来社会の姿として Society 5.0 が提唱されている．これは『サイバー空間（仮想空間）とフィジカル空間（現実空間）を高度に融合させたシステムにより，経済発展と社会的課題の解決を両立する，人間中心の社会（Society）』として内閣府が公表したものである[*2]．SLIM はフィジカル空間（現実空間）に存在する何百万もの IoT デバイスで動作する RFID システム向けに設計された軽量暗号であり，本論文の研究成果によって「攻撃者が既知平文・暗号文組を入手できる条件において，SLIM を採用している RFID システムは中間一致攻撃に対して安全である」という事が初めて明らかになった．この事により，SLIM を採用した IoT デバイスを社会で安心して利用する事が出来る．

また，IoT デバイスを製造する産業界では，提案者以外の第三者評価によって安全性が示された暗号の一つとして SLIM を採用する事が可能となる．

8 結論

本論文では，共通鍵ブロック暗号 SLIM の中間一致攻撃に対する安全性を評価した．評価の結果，11 段縮小版 SLIM に対し，既知平文・暗号文組数が 20，暗号化計算量は $2^{73.4}$ 回，メモリ量は $2^{70.4}$ bytes で鍵回復攻撃できる事を示した．SLIM の標

[*2] https://www8.cao.go.jp/cstp/society5_0/

準仕様段数は 32 段である為，本論文で示した中間一致攻撃に対して SLIM は安全である．

今後の課題は，中間一致攻撃の改良手法（Splice-and-cut 技法 [5],[9] や 3-Subset 技法 [6]）を用いた評価である．また，積分攻撃 [15]–[18] に加え，近年提案されているや混合整数計画法（MILP）を用いた暗号解析手法 [19],[20] を適用し，様々な観点から共通鍵ブロック暗号 SLIM の安全性を評価する事である．

参考文献

(1) B. Aboushosha, R. A. Ramadan, A. D. Dwivedi, A. El-Sayed, M. M. Dessouky: SLIM A Lightweight Block Cipher for Internet of Health Things, IEEE Access, 8, pp. 203747 - 203757.

(2) E. Biham, A. Shamir: Differential Cryptanalysis of the Data Encryption Standard, Springer-Verlag, New York, pp.79-88, 1993.

(3) M. Matsui: Linear Cryptanalysis Method for DES Cipher, Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques, EUROCRYPT '93, LNCS, vol. 765, pp.386-397, 1993.

(4) W. Diffie and M. E. Hellman: Exhaustive Cryptanalysis of the NBS Data Encryption Standard, Journals of the Computer vol. 10, pp. 74-84, 1977.

(5) K. Aoki, Y. Sasaki: Meet-in-the-Middle Attack against Reduced SHA-0 and SHA-1, Proceeding of the 29th International Cryptology Conference, CRYPTO 2009, LNCS, vol. 5677, pp. 70-89, 2009.

(6) A. Bogdanov, C. Rechberger: A 3-Subset Meet-in-the-Middle Attack: Cryptanalysis of the Lightweight Block Cipher KTANTAN, Proceedings of the 17th International Workshop, SAC 2010, LNCS, vol. 6544, pp. 229-240, 2010.

(7) A. Canteaut, M. Naya-Plasencia, B. Vayssiere: Sieve-in-the-Middle: Improved MITM Attacks, Proceedings of the 33rd Annual International Cryptology Conference, CRYPTO 2013, LNCS, vol. 8042, pp. 222–240, 2013.

(8) X. Dong, J. Hua, S. Sun, Z. Li, X. Wang, L. Hu: Meet-in-the-Middle Attacks Revisited: Key-Recovery, Collision, and Preimage Attacks, Proceedings of the 41st Annual International Cryptology Conference, CRYPTO 2021, LNCS, vol. 12827, pp. 278–308, 2021.

(9) Y. Igarashi, R. Sueyoshi, T. Kaneko, T. Fuchida: Meet-in-the-middle Attack with Splice-and-Cut Technique on the 19-round Variant of Block Cipher HIGHT, Proceedings of the Information Science and Applications, LNEE, vol. 339, pp. 423–429, 2015.

(10) Y. Sasaki, L. Wang: Meet-in-the-Middle Technique for Integral Attacks against Feistel ciphers, Proceedings of the 19th International Conference, Selected Areas in Cryptography, SAC 2013, LNCS, vol. 7707, pp. 234-251, 2013.

(11) Y. Wei, J. Lu, Y. Hu: Meet-in-the-Middle Attack on 8 Rounds of the AES Block Cipher under 192 Key Bits, Proceedings of the International Conference on Information Security Practice and Experience, ISPEC 2011, LNCS, vol. 6672, pp. 222–232, 2011.

(12) X. Lai: Higher Order Derivatives and Differential Cryptanalysis, Proceedings of the Communications and Cryptography, pp.227-233, 1994.

(13) T. Soyama, K. Tabata, and N. Sugio: Higher-order differential attack on the symmetric-key block cipher SLIM, Proceedings of the 2023 Symposium on Cryptgraphy and Information Security, 2023.

(14) Y. Y. Chan, C. Khor, J. S. Teh, W. J. Teng, N. Jamil: Differential Cryptanalysis of Lightweight Block Ciphers SLIM and LCB, Proceeding of the International Symposium on Emerging Information Security and Applications, EISA 2022, Emerging Information Security and Applications, pp. 55–67, 2023.

(15) L. R. Knudsen and D. Wagner: Integral cryptanalysis, Proceedings of Fast Software Encryption, FSE 2002, LNCS, vol. 2365, pp.112-127, 2002.

(16) N. Sugio, Y. Igarashi, and S. Hongo: Integral Cryptanalysis of Reduced-round KASUMI, Transactions of the IEICE on Fundamentals of Electronics, Communications and Computer Sciences, vol.E105-A, no.9, pp. 1309-1316, 2022.

(17) Y. Todo: Structural Evaluation by Generalized Integral Property, Proceedings of the 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT 2015, LNCS, vol. 9056, part1, pp. 287-314, 2015.

(18) Y. Todo, M. Morii: Bit-Based Division Property and Application to Simon Family, Proceedings of the 23rd International Conference on Fast Software Encryption, FSE 2016, LNCS, vol. 9783, pp. 357-377, 2016.

(19) N. Mouha, Q. Wang, D. Gu, B. Preneel: Differential and Linear Cryptanalysis Using Mixed-Integer Linear Programming, Proceedings of the 7th International Conference, Inscrypt 2011, LNCS, vol. 7537, pp. 57–76, 2011.

(20) Z. Xiang, W. Zhang, Z. Bao, and D. Lin: Applying MILP Method to Searching Integral Distinguishers Based on Division Property for 6 Lightweight Block Ciphers, Proceedings of the 22nd International Conference on the Theory and Application of Cryptology and Information Security, ASIACRYPT2016, LNCS, vol. 10031, pp. 648-678, 2016.

(21) 電子情報通信学会，情報セキュリティハンドブック，オーム社，2004.

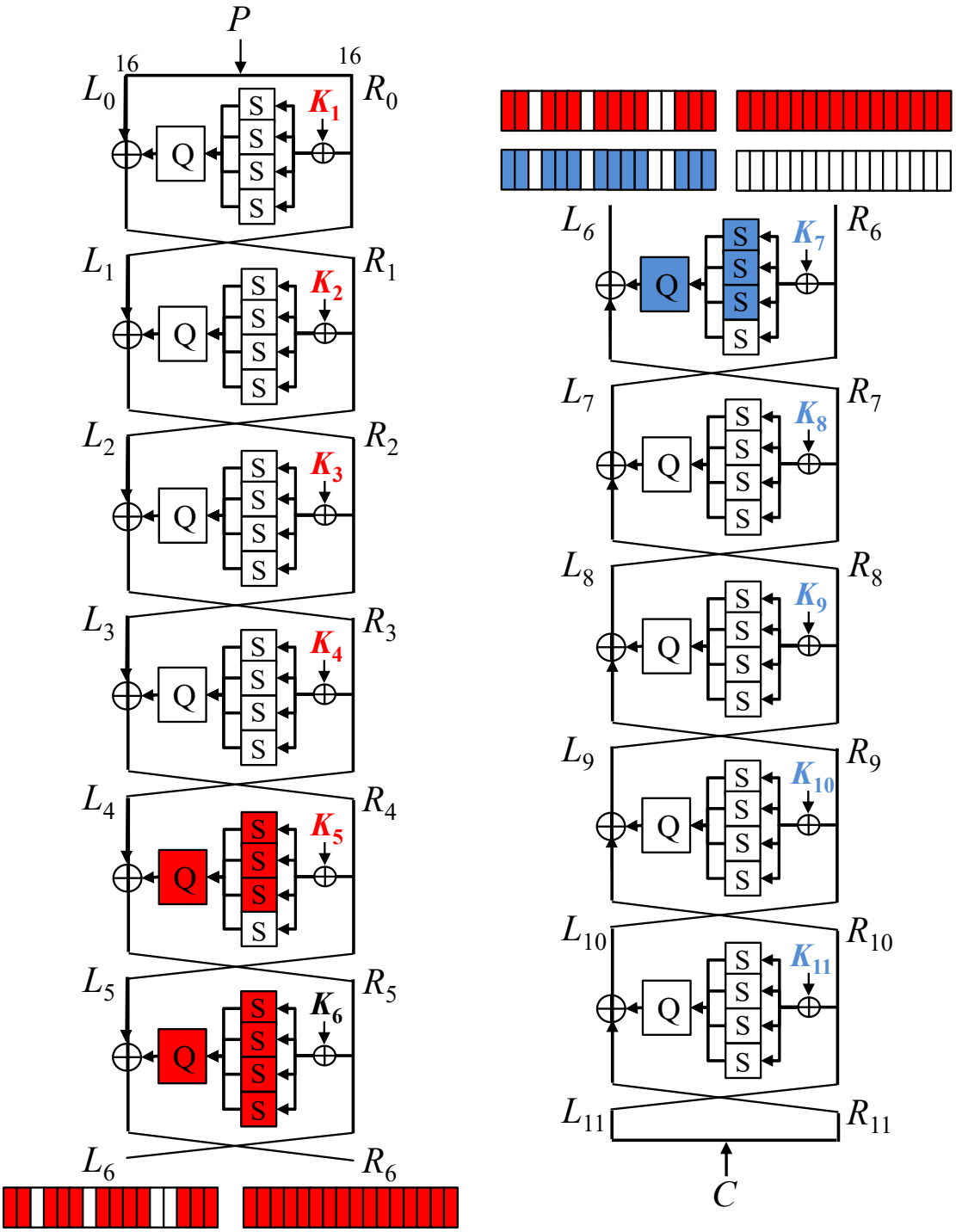

図 4　11 段 SLIM に対する中間一致攻撃