CIPHERUNICORN-Aの差分/線形解読に対する安全性について

暗号技術評価ワークショップ
ランプセッション
2002.1.28
日本電気株式会社

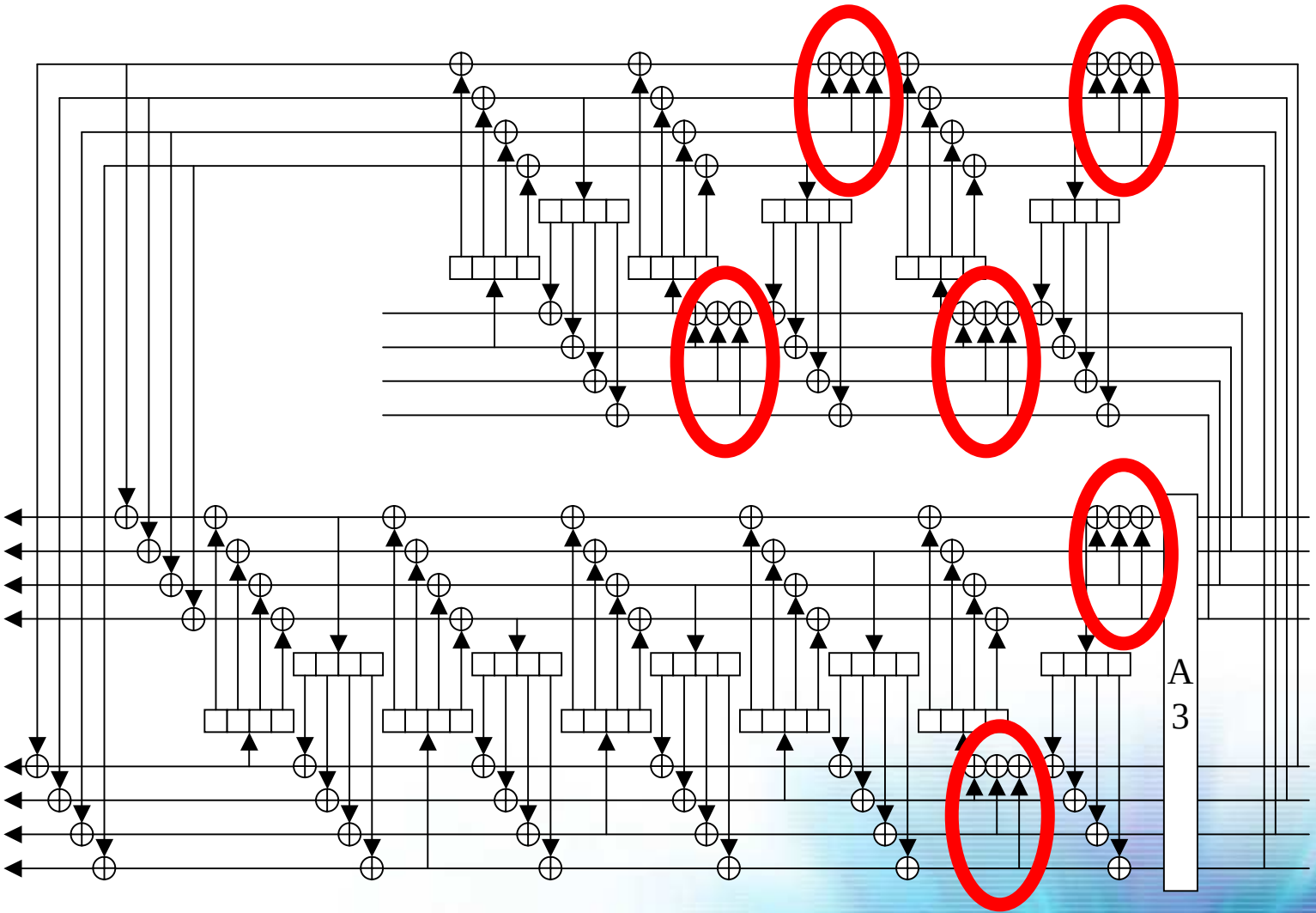
目次

- 評価概要
- 評価方法
- 評価結果
- まとめ

評価概要

- 差分特性確率・線形特性確率を調査
- 従来(自己評価書)より詳細で網羅的な評価
- 差分特性確率、線形特性確率ともに2^{-128}を下回ることを確認

従来の近似(mF関数)



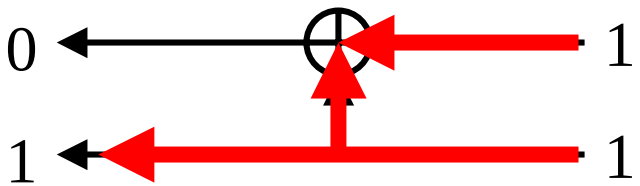
従来からの変更点

- 従来の評価
  - 探索範囲の限定
    - 差分(マスク)の合流地点では「消える」場合のみに限定
  - 乗算を排他的論理和で近似

- 今回の評価
  - 起こり得る全ての場合を探索
    - 差分(マスク)の合流地点で「消える」「消えない」場合を網羅
  - 乗算は排他的論理和で近似せず、(ﾊﾞｲﾄｵﾘｴﾝﾃｯﾄﾞで)起こり得る全ての場合を探索
  - 乗算で発生する確率を一部考慮

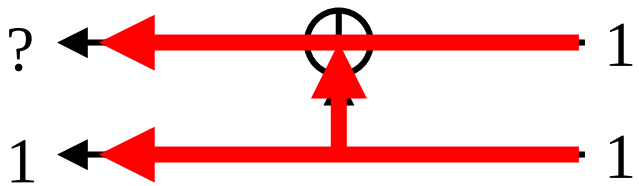
合流地点の扱い(差分通過の例)

従来の評価



01 ← 11のみ

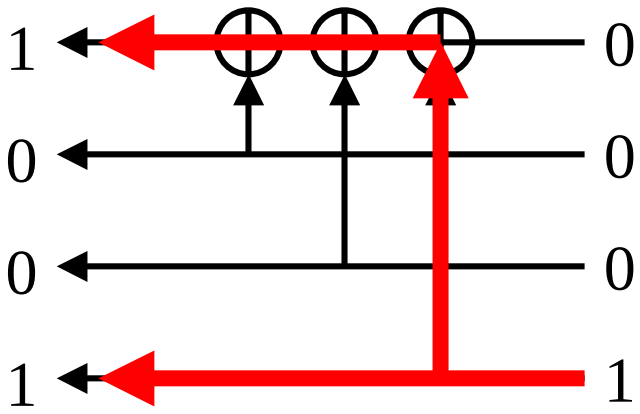
今回の評価



01 ← 11
11 ← 11

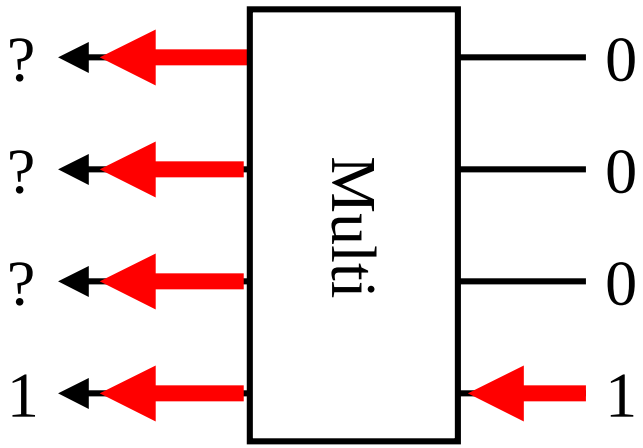
乗算の扱い(差分通過の例)

従来の評価



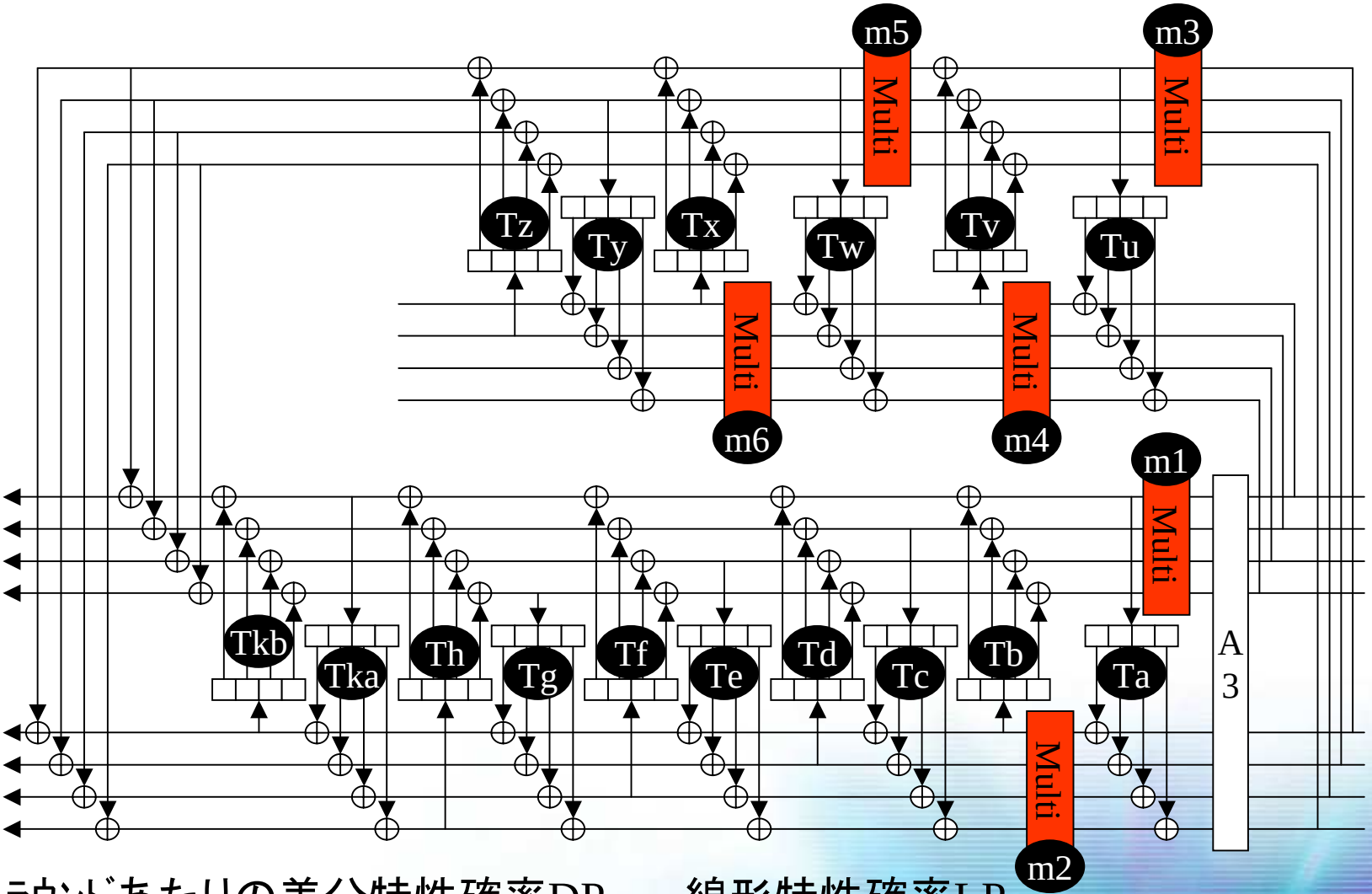
1001 ← 0001のみ

今回の評価



1001 ← 0001
0001 ← 0001
0011 ← 0001
⋮

今回の近似(mF'関数)



ﾗｳﾝﾄﾞあたりの差分特性確率$DP_{mF'}$、線形特性確率$LP_{mF'}$

15段目出力の差分特性確率DCP、線形特性確率LCP

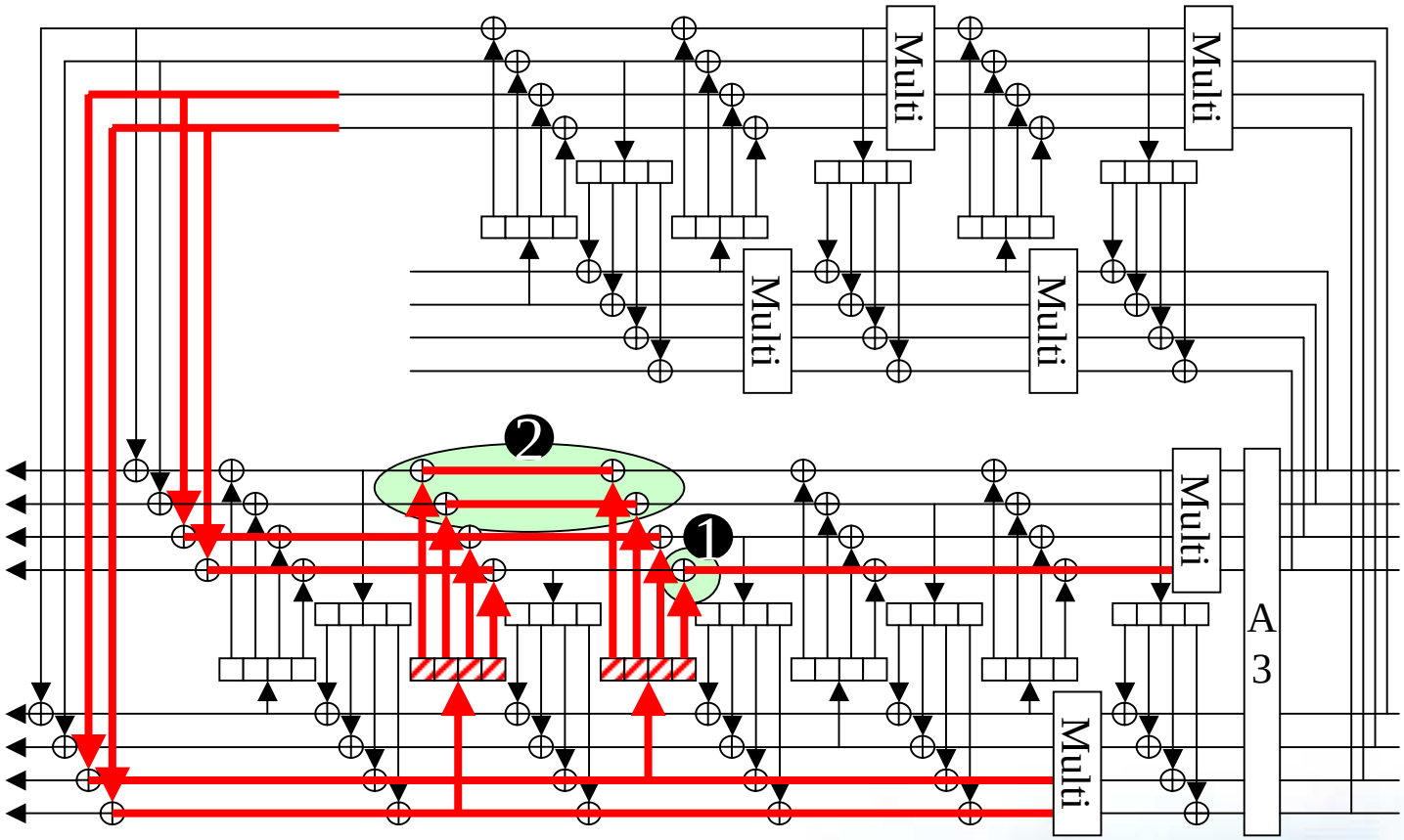
評価方法

- バイトオリエンテッドで経路を全数探索
  - （方法は従来と同じ、ただし探索範囲を拡大）
- アクティブなS-box数から確率を計算
  - （従来と同じ）
- 乗算における確率も一部考慮
  - （今回、追加）

評価結果(差分解読)

- 出力差分=0となる場合
  - 15段目出力で2^{-133}以下であることを確認
- 出力差分≠0となる場合
  - 15段目出力で2^{-130}以下であることを確認

差分経路例(出力差分=0)



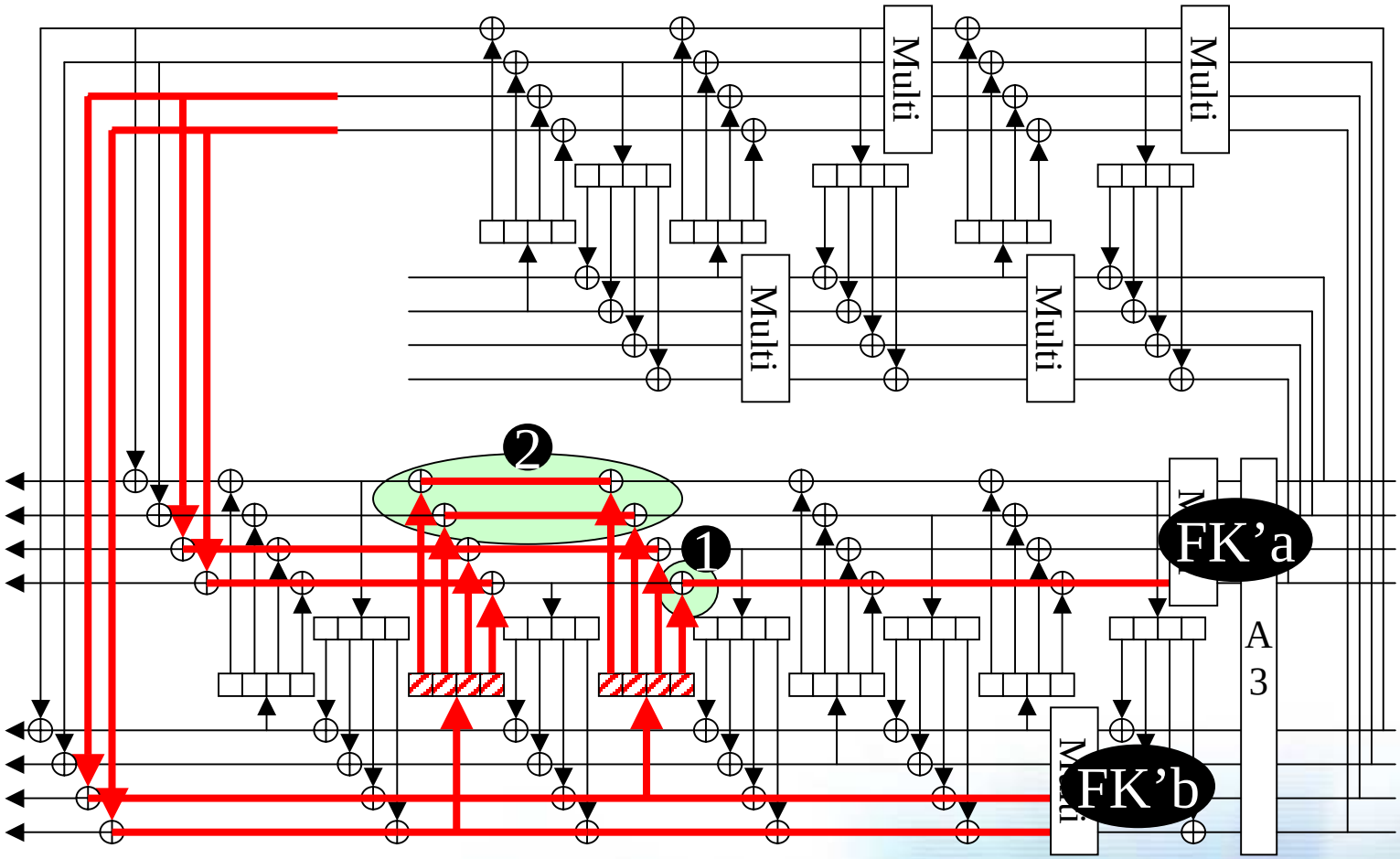
❶ m1の出力差分とTfの出力差分が消しあう確率 … $2^{-6.000} \times 2^{-6.000} = 2^{-12.000}$

❷ TfとThの出力差分の上位2バイトが消しあう確率 … $2^{-7.000}$

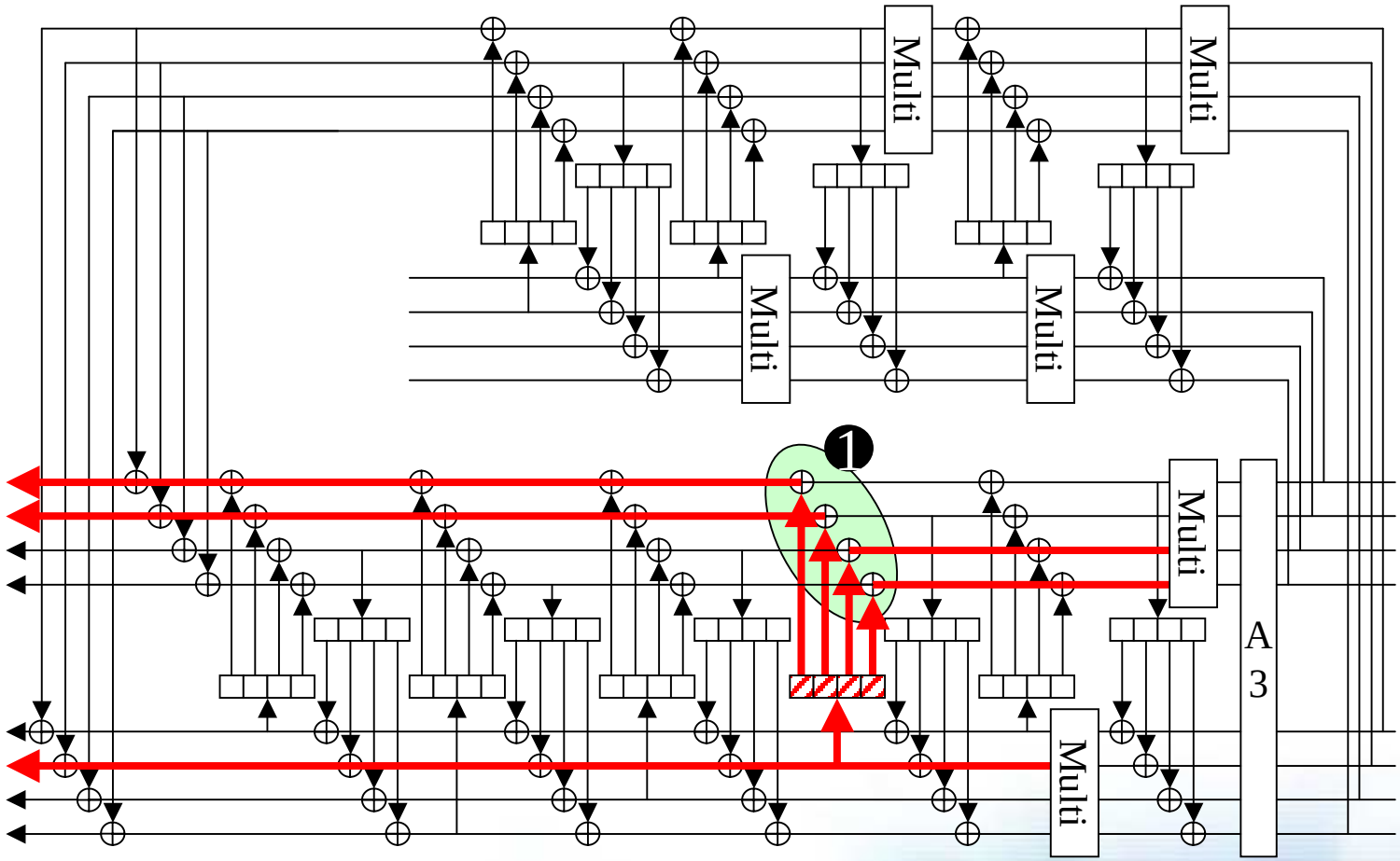
$$DP_{mF'} \leqq ❶(2^{-6.000} \times 2^{-6.000}) \times ❷(2^{-7.000}) = 2^{-19.000}$$

$$DCP \leqq (2^{-19.000})^{15 \times 1/2} = 2^{-133.000}$$

独立性の確認差分経路例(出力差分=0)



差分経路例(出力差分≠0)

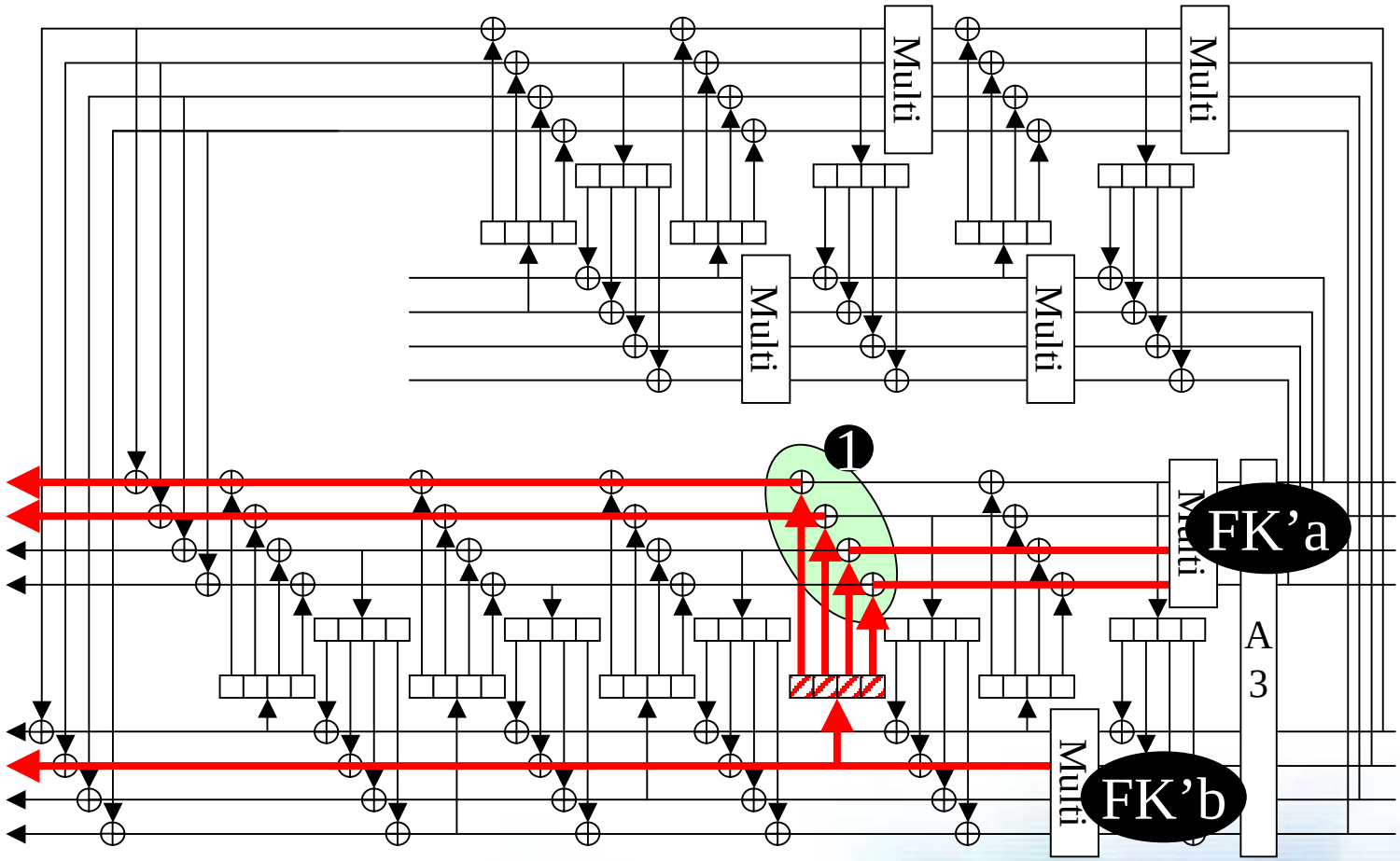


❶ Tdの出力差分とm1の出力差分が消しあう確率 … $2^{-7.000} \times 2^{-6.000} = 2^{-13.000}$

$$DP_{mF'} \leqq \text{❶}(2^{-7.000} \times 2^{-6.000}) = 2^{-13.000}$$

$$DCP \leqq (2^{-13.000})^{15 \times 2/3} = 2^{-130.000}$$

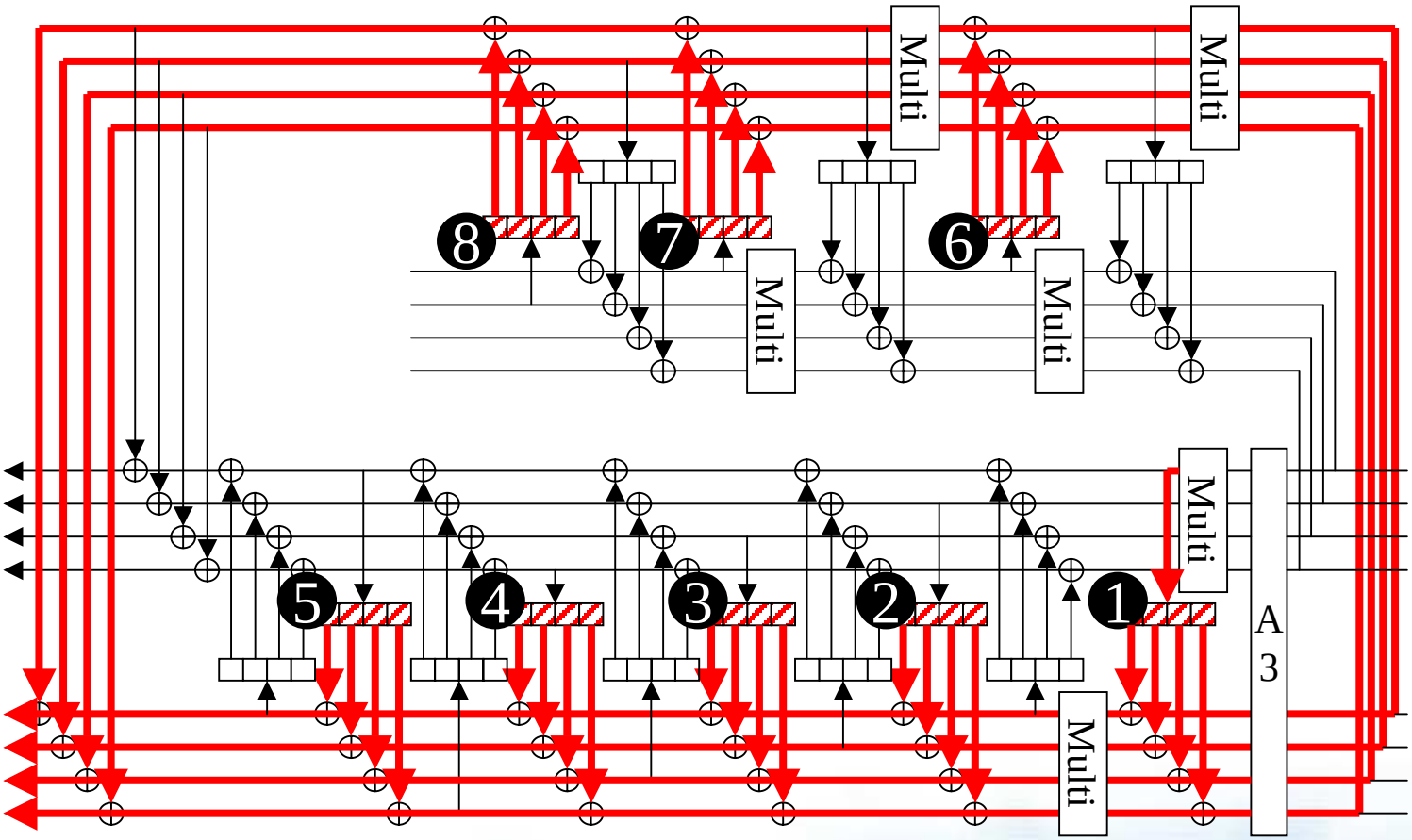
独立性の確認差分経路例(出力差分≠0)



評価結果(線形解読)

- 入力マスク値=0となる場合
  - 15段目出力で2^{-149}より小さいことを確認
- 入力マスク値≠0となる場合
  - 15段目出力で2^{-210}より小さいことを確認

線形経路例(入力マスク=0)



❶
❷❸❹❺❻❼❽

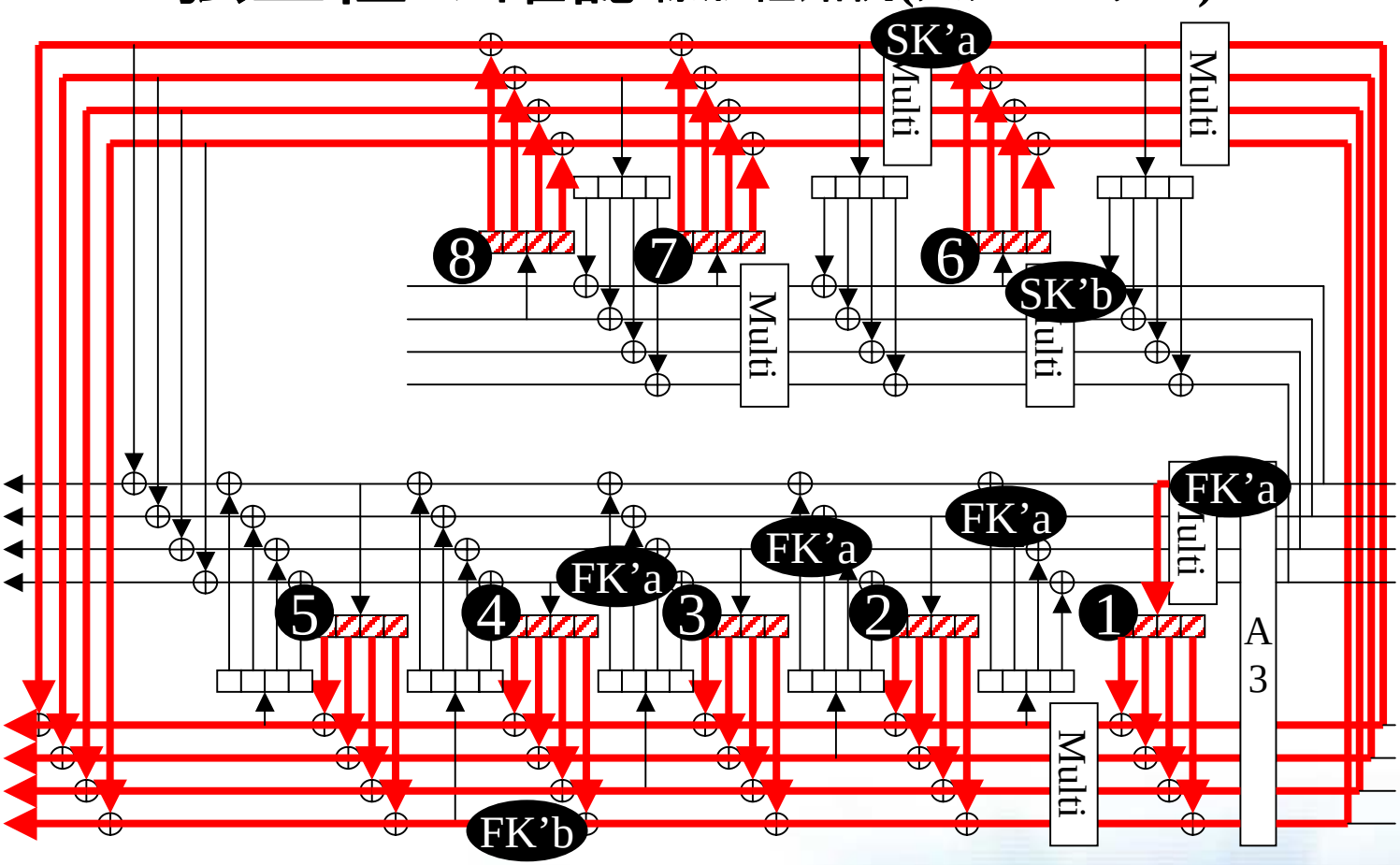
{(S_0 ‖ S_1 ‖ S_2 ‖ S_3)で入力マスク≠0} $=2^{-2.385}$

{(S_0 ‖ S_1 ‖ S_2 ‖ S_3)で入力マスク=0}$^7=(2^{-2.712})^7$

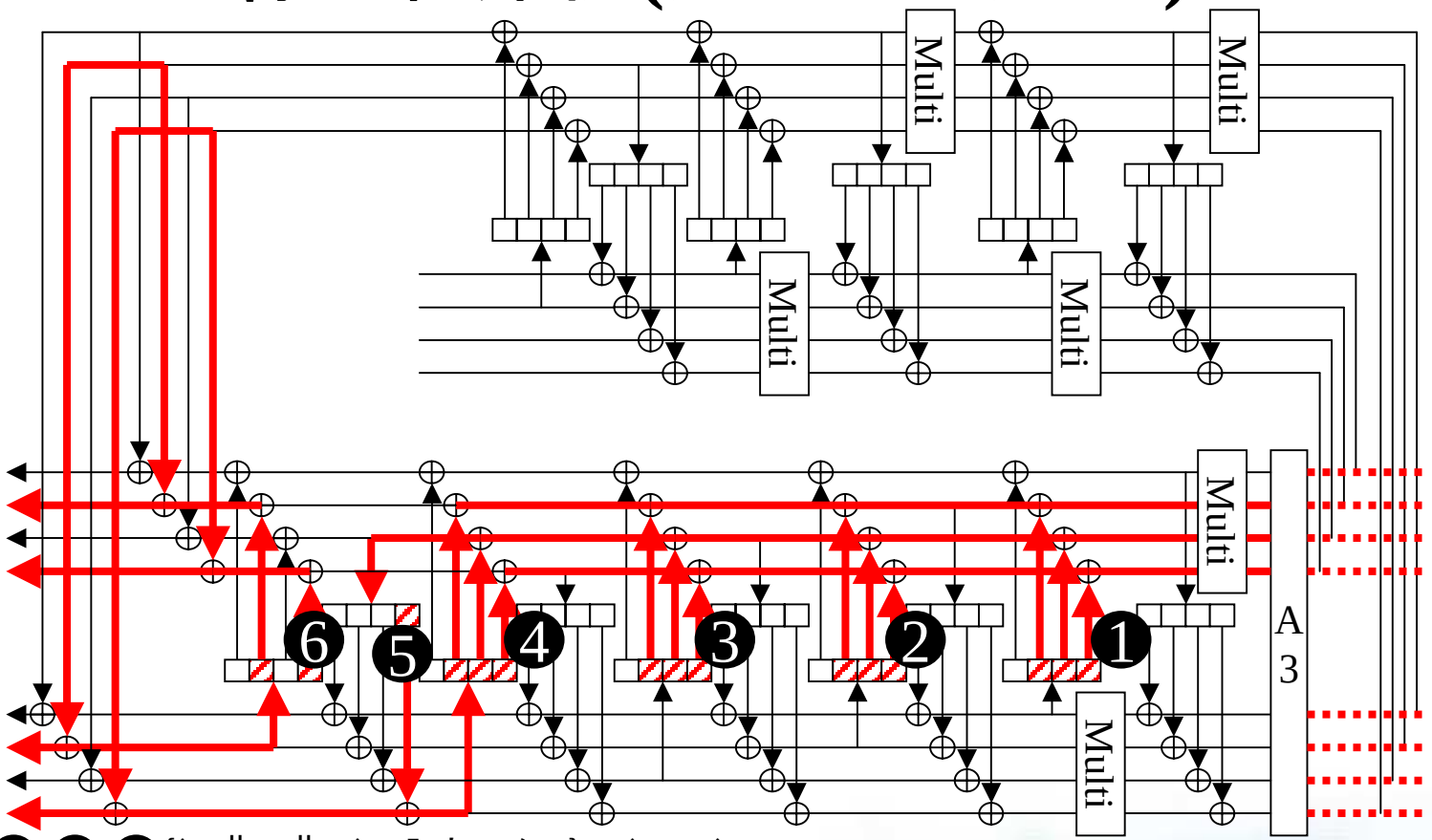
$$LP_{mF'} \leqq ❶(2^{-2.385}) \times ❷❸❹❺❻❼❽(2^{-2.712})^7 = 2^{-21.369}$$

$$LCP \leqq (2^{-21.369})^{15\times 1/2} = 2^{-149.583}$$

独立性の確認線形経路例(入力マスク=0)



線形経路例(入力マスク≠0)



❶❷❸ {(S_1 ‖ S_2 ‖ S_3)で入力マスク=0}^{3} = $(2^{-3.081})^3$

❹ {(S_1 ‖ S_2 ‖ S_3)で入力マスク≠0} = $2^{-2.712}$

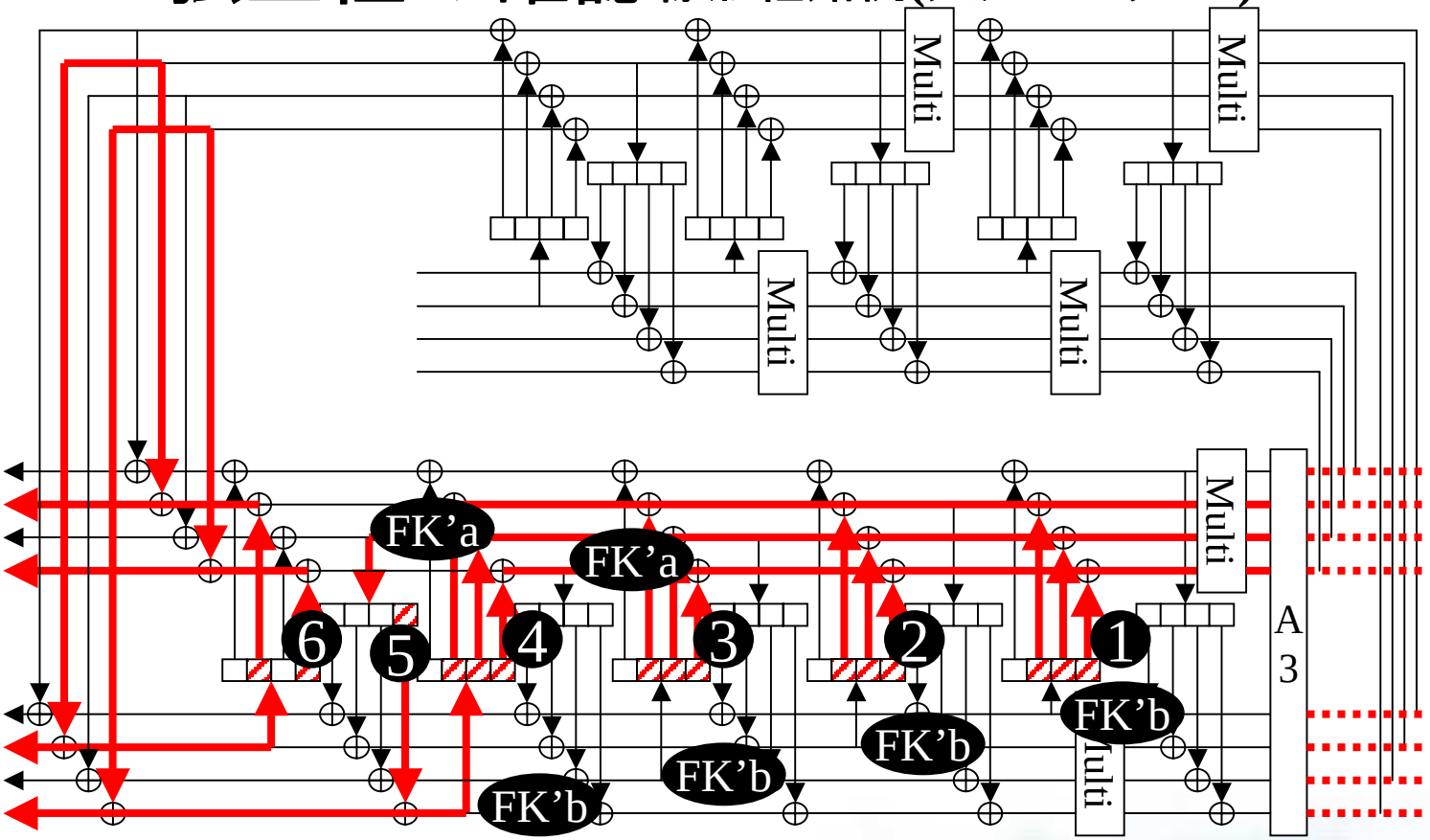
❺ {S_3} = $2^{-6.000}$

❻ {(S_1 ‖ S_3)で入力マスク≠0} = $2^{-3.081}$

$$LP_{mF'} \leqq ❶❷❸ (2^{-3.081})^3 \times ❹ (2^{-2.712}) \times ❺ (2^{-6.000}) \times ❻ (2^{-3.081}) = 2^{-21.036}$$

$$LCP \leqq (2^{-21.036})^{15 \times 2/3} = 2^{-210.360}$$

独立性の確認線形経路例(入力マスク≠0)



まとめ

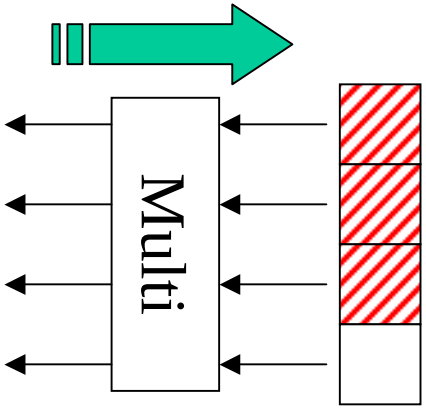
- 従来よりも全数探索の範囲を広げて調査
- 従来の評価に加え乗算の確率も一部考慮
- 差分特性確率、線形特性確率ともに2^{-128}より小さいことを確認
  - 従来評価において2^{-128}より確率が大きくなる場合全てについて確認

参考1(T_n関数の差分・線形確率)

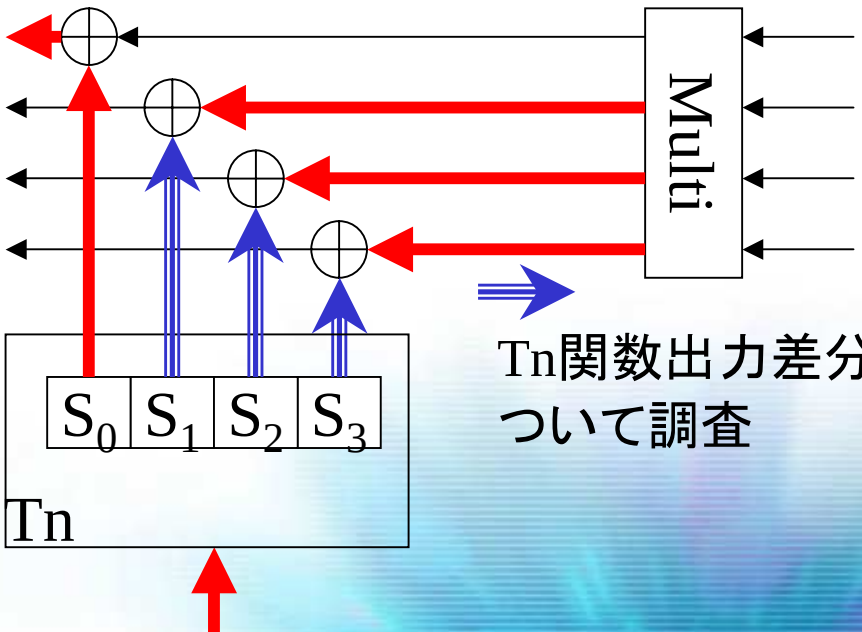
換字ﾃｰﾌﾞﾙの組合せ	最大差分確率	最大線形確率	
		入力ﾏｽｸ＝0	入力ﾏｽｸ≠0
S_0	$2^{-6.000}$	—	$2^{-6.000}$
S_1	$2^{-6.000}$	—	$2^{-6.000}$
S_2	$2^{-6.000}$	—	$2^{-6.000}$
S_3	$2^{-6.000}$	—	$2^{-6.000}$
$S_0 \parallel S_1$	$2^{-7.000}$	$2^{-3.825}$	$2^{-3.081}$
$S_0 \parallel S_2$	$2^{-7.000}$	$2^{-3.660}$	$2^{-3.081}$
$S_0 \parallel S_3$	$2^{-7.000}$	$2^{-3.504}$	$2^{-3.081}$
$S_1 \parallel S_2$	$2^{-7.000}$	$2^{-3.504}$	$2^{-3.081}$
$S_1 \parallel S_3$	$2^{-7.000}$	$2^{-3.825}$	$2^{-3.081}$
$S_2 \parallel S_3$	$2^{-7.000}$	$2^{-3.660}$	$2^{-3.215}$
$S_0 \parallel S_1 \parallel S_2$	$2^{-7.000}$	$2^{-3.215}$	$2^{-2.599}$
$S_0 \parallel S_1 \parallel S_3$	$2^{-7.000}$	$2^{-3.215}$	$2^{-2.599}$
$S_0 \parallel S_2 \parallel S_3$	$2^{-7.000}$	$2^{-3.215}$	$2^{-2.712}$
$S_1 \parallel S_2 \parallel S_3$	$2^{-7.000}$	$2^{-3.081}$	$2^{-2.712}$
$S_0 \parallel S_1 \parallel S_2 \parallel S_3$	$2^{-7.000}$	$2^{-2.712}$	$2^{-2.385}$

参考2(乗算の差分確率の求め方)

逆元を用いて逆方向に調査



上位24ビットの差分
に注目



Tn関数出力差分値に
ついて調査

参考3(乗算の差分・線形確率)

乗算の出力 丸め差分	最大差分確率	
	定数 (0x7e167289)	定数 (0xfe21464b)
0001	$2^{-6.000}$	$2^{-6.245}$
0010	$2^{-4.994}$	$2^{-5.999}$
0011	$2^{-6.000}$	$2^{-6.069}$
0100	$2^{-2.999}$	$2^{-3.999}$
0101	ー	ー
0110	ー	ー
0111	$2^{-7.181}$	$2^{-7.167}$
1000～1111	ー	ー

ーは未調査

※今回の線形特性確率調査では確率1とみなした