軽量暗号 TWINE の小型回路実装方式の検討

森岡 澄夫◇　小林 栄太‡　峯松 一彦§　洲崎 智保†

◇ NEC 中央研究所
211-8666 神奈川県川崎市中原区下沼部 1753
s-morioka@ak.jp.nec.com

‡NEC グリーンプラットフォーム研究所
211-8666 神奈川県川崎市中原区下沼部 1753
e-kobayashi@fg.jp.nec.com

§ NEC 情報・ナレッジ研究所
211-8666 神奈川県川崎市中原区下沼部 1753
k-minematsu@ah.jp.nec.com

†NEC 情報・ナレッジ研究所
211-8666 神奈川県川崎市中原区下沼部 1753
t-suzaki@cb.jp.nec.com

あらまし　筆者らは従来より，データブロック長 64 ビットの軽量暗号 TWINE の提案・評価を行っている．その特徴は，改良型 Type-2 一般化 Feistel 構造を採用し，拡散層の実装がシンプルな事である．今回，SBox 回路を 1 個だけ用意して使いまわすシリアライズ手法により，小規模回路実装を試みた．一般にシリアライズでは，SBox やデータレジスタの入力を切り替えるため，セレクタを多数用いる．今回，拡散層実装をローテータによって行う工夫により，特殊な論理セル等を使うことなくセレクタ数を減らした．その結果，現時点で最小クラスの PRESENT シリアライズ実装と比べ，ゲート数はほぼ同じだが，配線領域まで含めた全面積はより小さくなった．

A compact H/W implementation of light-weight cipher TWINE

Sumio Morioka◇　Eita Kobayashi‡　Kazuhiko Minematsu§
Tomoyasu Suzaki†

◇ Central Research Laboratories,
NEC Corporation
1753 Shimonumabe, Nakahara-ku,
Kawasaki, Kanagawa 211-8666, JAPAN
s-morioka@ak.jp.nec.com

†Green Platform Research Laboratories,
NEC Corporation
1753 Shimonumabe, Nakahara-ku,
Kawasaki, Kanagawa 211-8666, JAPAN
e-kobayashi@fg.jp.nec.com

§ Knowledge Discovery Research Laboratories,
NEC Corporation
1753 Shimonumabe, Nakahara-ku,
Kawasaki, Kanagawa 211-8666, JAPAN
k-minematsu@ah.jp.nec.com

†Knowledge Discovery Research Laboratories,
NEC Corporation
1753 Shimonumabe, Nakahara-ku,
Kawasaki, Kanagawa 211-8666, JAPAN
t-suzaki@cb.jp.nec.com

Abstract　This paper presents a compact H/W implementation of a 64-bit lightweight block cipher TWINE which has an improved Type-2 generalized Feistel structure. In order to shrink circuit size, we have incorporated not only a standard serialize approach but also a new rotator-based block shuffling method. We don't use any backend design technique nor special cell such as gated clock and scan FF. The achieved gate count is almost the same with those of the other lightweight ciphers such as PRESENT. Yet the total chip area size, involving not only gate region but wiring region, becomes smaller because of elimination of multiplexers.

1 はじめに

近年，IC カード，RFID，センサモジュールなど小型電子デバイスの利用が進展している．それらのデバイスでは，使用可能電力（uW〜mW オーダ），プロセッサ処理能力（クロック周波数が数十 KHz〜十数 MHz），物理的サイズ等に強い制限がある．なおかつ，データ保持や通信における高セキュリティが要求される．

このため，十分なセキュリティ・レベルと低実装コストを両立した軽量暗号の研究が行われている [1–11]．AES の低コスト実装については従来多数の報告があるが [12, 13]，軽量暗号は AES のさらに数分の 1 の実装コストで済む．

筆者らは従来より，軽量暗号 TWINE を提案している [14,15]．その特徴は，(1) データ・ブロック長が 64 ビットと短いこと[1]，(2) Type-2 一般化 Feistel 構造（GFS）[16] を改良 [17] したうえで採用し，ソフト，回路いずれの実装でもリソース量あたりの処理性能が高いこと，(3) 各種攻撃に十分な耐性を持つこと等である．

本稿では，TWINE をさらに小規模な回路で実装する方法を検討した．多くの共通鍵暗号で，SBox 回路を一つだけ用意して使いまわすシリアライズ手法が試みられている [13]．本稿でもシリアライズを行うが，それに加え，セレクタ数も数分の一に減らすために次の工夫を施した：(A) 拡散層を複数のローテータの組み合わせで実装する，(B) 各ローテータを止めず，常に回し続ける，(C) SBox へ接続するレジスタ数が減るように演算をスケジューリングする．

なお，軽量暗号の回路実装報告には，セレクタを削減するために scan FF 等の特殊セルや gated clock を使った事例もある．しかし，本手法の特徴の一つとして，通常の LSI 設計フローで問題が生じないよう[2]，方式設計の工夫のみでセレクタを削減する．

上記工夫 (A)〜(C) を適用した結果，使用ゲート数を 1446GE に抑えることができた．この GE 値は他の軽量暗号のシリアライズ実装と同程度であるが，ゲート領域だけでなく配線領域まで含めた全面積は，現時点で最小クラスの PRESENT シリアライズ実装 [10] よりも小さくなった．

[1] 4 ビット× 16 語から成る．鍵長は 80 ないし 128 ビットである．

[2] Scan FF や gated clock は，本来，チップテストや低電力化のためにバックエンド工程で自動適用するものであり，フロントエンドで機能実現目的で論理設計に利用することは，未想定である．そのような利用の仕方は，デザイン・ルール違反になったり，バックエンド工程でタイミング・エラーや各種ツール適用時の問題などを引き起こす可能性があるので，好ましくない（実用 SoC/LSI 設計では，通常行わない）．

表 1: TWINE-80 暗号化アルゴリズム

$Function\ TWINE.Enc(PT_{(64)}, RK_{(32\times36)}, CT_{(64)})$

$X^1_{0(4)} \| X^1_{1(4)} \| \ldots \| X^1_{15(4)} \leftarrow PT$
$\mathrm{RK}^1_{(32)} \| \ldots \| \mathrm{RK}^{36}_{(32)} \leftarrow RK_{(32\times36)}$

for $i \leftarrow$ 1 **to** 35 **do begin**
  $\mathrm{RK}^i_{0(4)} \| \mathrm{RK}^i_{1(4)} \| \ldots \| \mathrm{RK}^i_{7(4)} \leftarrow \mathrm{RK}^i_{(32)}$
  for $j \leftarrow$ 0 **to** 7 **do**
    $X^i_{2j+1} \leftarrow F(X^i_{2j}, \mathrm{RK}^i_j) \oplus X^i_{2j+1}$
      $where\ F(a,b) \equiv S(a \oplus b)$

  for $h \leftarrow$ 0 **to** 15 **do**
    $X^{i+1}_{\pi[h]} \leftarrow X^i_h$ // Apply P-func
end

for $j \leftarrow$ 0 **to** 7 **do**
  $X^{36}_{2j+1} \leftarrow S(X^{36}_{2j} \oplus \mathrm{RK}^{36}_j) \oplus X^{36}_{2j+1}$
$CT \leftarrow X^{36}_0 \| X^{36}_1 \| \ldots \| X^{36}_{15}$

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

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

j	0	1	2	3	4	5	6	7
$\pi[j]$	5	0	1	4	7	12	3	8

j	8	9	10	11	12	13	14	15
$\pi[j]$	13	6	9	2	15	10	11	14

2 軽量暗号 TWINE のアルゴリズムの概要

TWINE の暗号化処理を表 1 に，ブロック図を図 1 上段に示す（詳細は文献 [14,15] を参照）．データ・ブロック長は 64 ビット（4 ビット× 16 語），鍵長は 80 ないし 128 ビットの Feistel 構造であり，ラウンド数は 36 である（最終ラウンドのみ P 関数適用を行わない）．F 関数は SBox（$S(x)$）を含み，P 関数（$\pi[j]$）はいわゆる拡散層である．一般的な共通鍵暗号と同じく秘密鍵からラウンド鍵を生成するが，その処理は図 1 下段のとおりである．

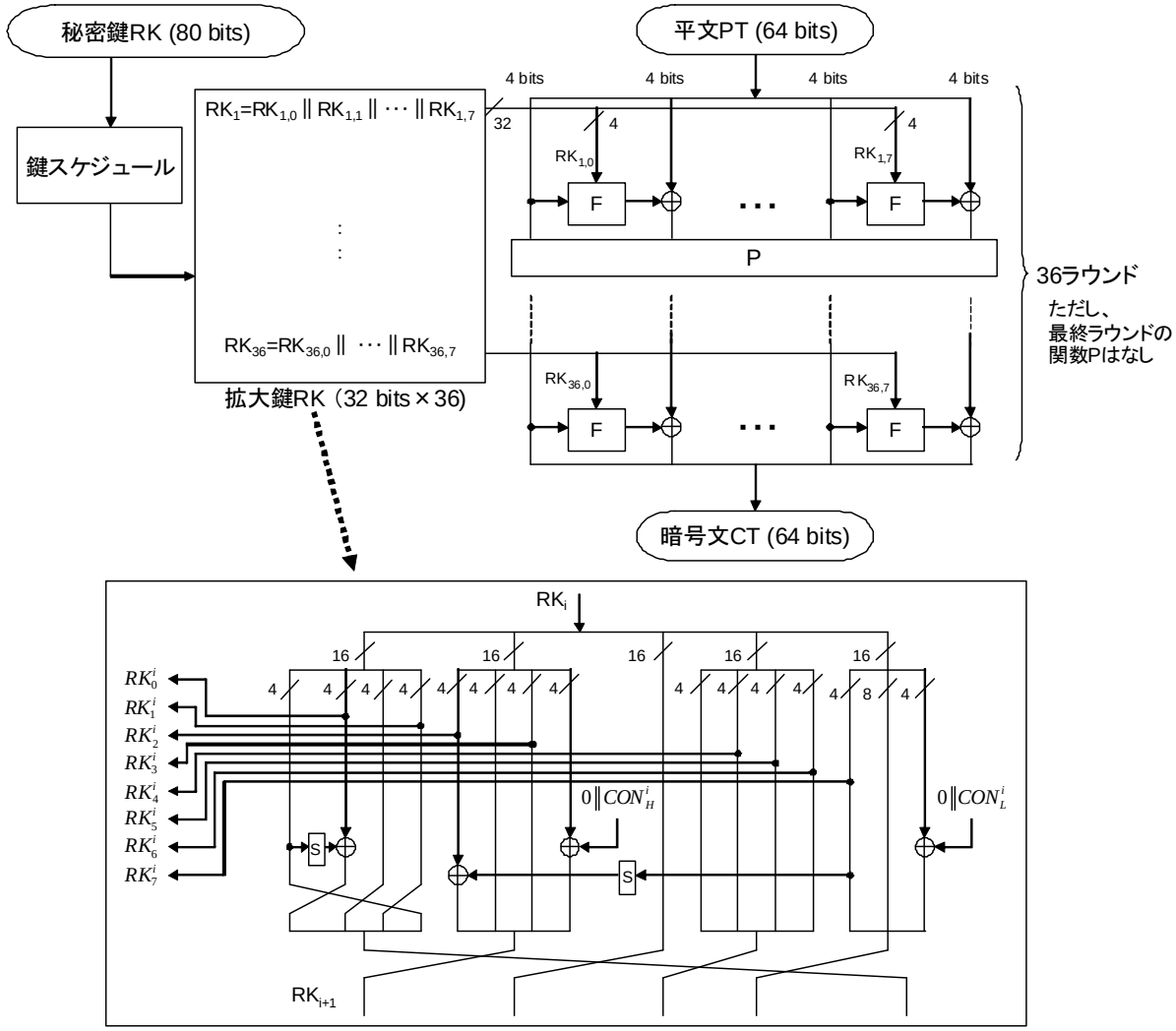


図 1: TWINE の処理ブロック図

データパスは Feistel 構造であるが，P 関数が 4 ビットを単位とする位置交換処理であることに注意されたい．他の共通鍵暗号では，拡散層でビット単位のこみ入った演算（パーミュテーションや線形変換など）をする場合が多いが，TWINE ではシンプルである．

3 小規模回路構成法と実装結果

3.1 通常のシリアライズで起きるセレクタ増加

TWINE 回路を標準的 1 ラウンド/クロック構成で実装すると，図 2(A) のようになる（鍵スケジューラ部は除く）．4 ビットのデータレジスタを 16 本持ち，1 ラウンド分の演算が組み合わせ回路となる．特に変わった点のない Feistel 型回路である．

これに対し，標準的なシリアライズを施した場合の回路構成を図 2(B) に示す．一つの F 関数回路だけを用意して使い回し，データ値を x1,x3,x5,⋯ と一つずつ順に更新する．F 関数適用が終了した後，P 関数を通して全データレジスタ x0〜x15 を一度にまとめて更新する．

この動作をするには，同図中に色付きで示したセレクタを，新たに設置しなければならない．つまり，(1) F 関数の入力を切り替える 8:1 セレクタ（各 4 ビット幅）2 本と，(2) 偶数位置レジスタ（x0,x2,⋯）の入力を切り替える 2:1 セレクタ（4 ビット幅）8 本と，(3) 奇数位置レジスタ（x1,x3,⋯）の入力を切り替える 3:1 セレクタ（4 ビット幅）8 本を追加する．

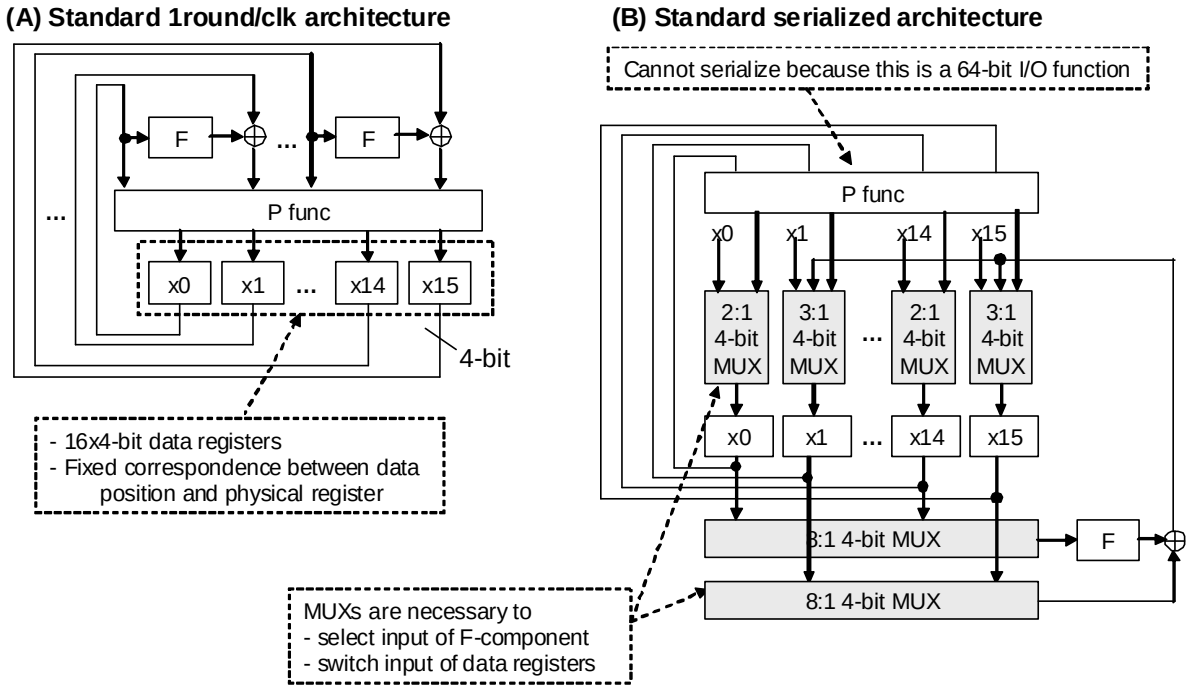


図 2: Feistel 構造の典型的な回路実装と，シリアライズによるセレクタ増加

よって TWINE 全体では，k:1 セレクタを 2:1 セレクタ $k-1$ 本と換算した時，2:1 セレクタを (7 × 4bit × 2 本)+(4bit × 8 本)+(2 × 4bit × 8 本)=152 本増やす事になる．2:1 セレクタの回路規模を 2〜3GE とすると，全体で 304〜456GE の増加になるが，これは 1000GE 前後の軽量暗号としては無視できない値である．

ここで，上記シリアライズ実施にあたり，注意を要する検討課題が二つある．

一つ目は，拡散層処理（P 関数）を置換処理（F 関数）と同様にシリアライズできるか否かである．たとえば AES では，MixColumns が 32 ビット，ShiftRows が 128 ビット入出力の関数であるため，これらを SubBytes と同じ 8 ビット単位に区切って処理する事や，SubBytes と同時並列に適用する事が難しい．他の暗号でも，拡散層がビット・パーミュテーションである場合などは同様である．つまり，置換が全部終わった後でなければ拡散ができないので，図 2(B) のうち，レジスタ入力部のセレクタ群がどうしても必要になる．PRESENT のシリアライズ実装 [10] でもこの問題が起きている．

二つ目は，追加したセレクタの規模が SBox の削減分よりも大きいと，シリアライズによる回路規模削減効果が無い事である．たとえば AES では，SBox の回路規模がセレクタと比べて大きい（1 個あたり 1000GE 前後 [12]）ので，問題にならない．しかし軽量暗号では，SBox の回路規模が数十 GE しかない事と [14]，SBox 数も少ないことから（Feistel 構造であるため），この問題が起きやすい．

3.2 提案するローテータ・ベース実装法

一般的な共通鍵暗号では，追加するセレクタ数を抑えることは難しい．しかし本稿では，TWINE の拡散層構成を活かし，セレクタ数を大幅に削減する手法を考案した．

提案する回路構成法を図 3 に示す．P 関数で行うデータ移動が 4 ビット単位の二つのローテートであることに着目し（図 3 下段），並列動作する二つのローテータ（各 4 ビット×8 語）と一つの F 関数で回路を構成することにした（図 3 上段）．この回路には次の三つの特徴がある：(**特徴** i) 二つのローテータを止めずに常時動作させ続ける．これにより，データレジスタの入力セレクタを排除する．F 関数適用と P 関数適用は同時並列に行われる．TWINE では $8n$ 回 ($n \geq 1$) のローテートでデータ位置が元に戻るため，$7+8(n-1)$ 回ローテートすれば P 関数

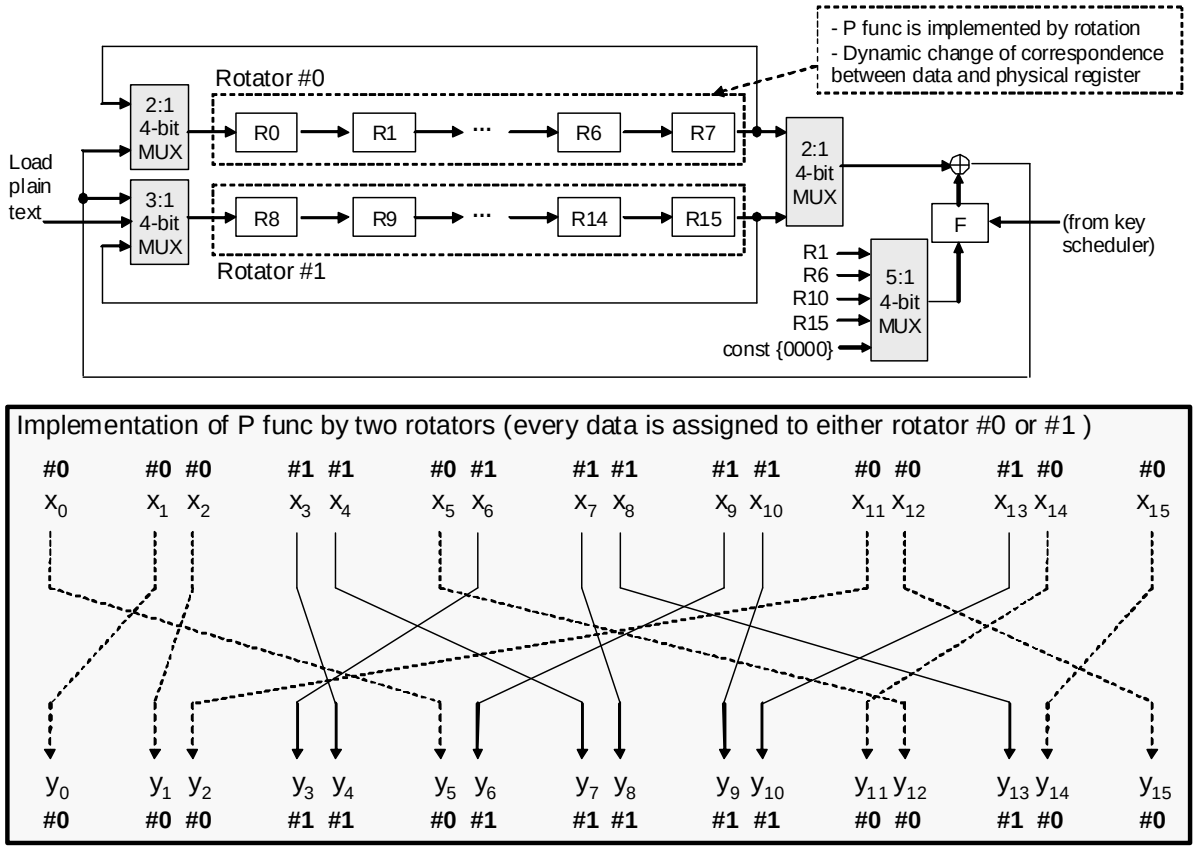


図 3: 提案するシフトレジスタ・ベースのシリアライズ実装

を 1 度適用した事になる．

(**特徴** ii) データのビット位置 x0〜x15 と物理レジスタ R0〜R15 の対応が固定ではなく，クロック毎に動的に変化する[3]．実際の様子を図 4 に示す．

(**特徴** iii) 上記 (ii) のもとで，F 関数につなぐレジスタ数を減らし，F 関数の入力セレクタ数を削減する．提案手法では，両ローテータの先頭レジスタ R7,R15 と別の 4 レジスタ（図 4 のうち太枠で囲った部分）を F 関数につなぐ．もし (ii) の工夫がなければ，全レジスタの出力を引き出さなければならず，セレクタを削減できない．

以上により，図 3 上段のとおりセレクタ追加量を 2:1 セレクタ 32 個相当にまで抑えることができる（提案手法を使わなければ，前述のとおり 152 個）．レジスタや F 関数はこれ以上削減できないので，データパス規模は理論上の下限に近いと考えられる．

以下，提案手法のもとでの回路の動きを再整理しておく．データは初め，図 4 の clock0 のようにレジスタ R0〜R15 に配置され，クロック毎に右ローテートする．最初の 8 クロックでは，ローテータ#0 中の奇数データ x5,x15,x11,x1 が順次 F 関数を通って変換される．他のデータは F 関数を通らずにそのまま各ローテータ末尾に戻る．次の 7 クロックでは，ローテータ#0 はそのままで，ローテータ#1 中の奇数データが順次 F 関数を通る．15 クロック経った時点で P 関数を 1 度適用したことになり，次のラウンドに入る．なお，鍵スケジューラも同様にローテータで構成するが（図 5），本稿では詳細な説明は割愛する．

3.3 回路実装の結果と評価

提案手法に基づく回路を Verilog HDL で実装し，Synopsys design compiler により論理合成

[3]一般的な回路実装では，たとえば物理レジスタ R0 にデータの x0 が，レジスタ R1 に x1 が入っており，その対応は変化せず常に固定である．しかし提案手法では，データのどのビットがどのレジスタに入るかが常時変わる．

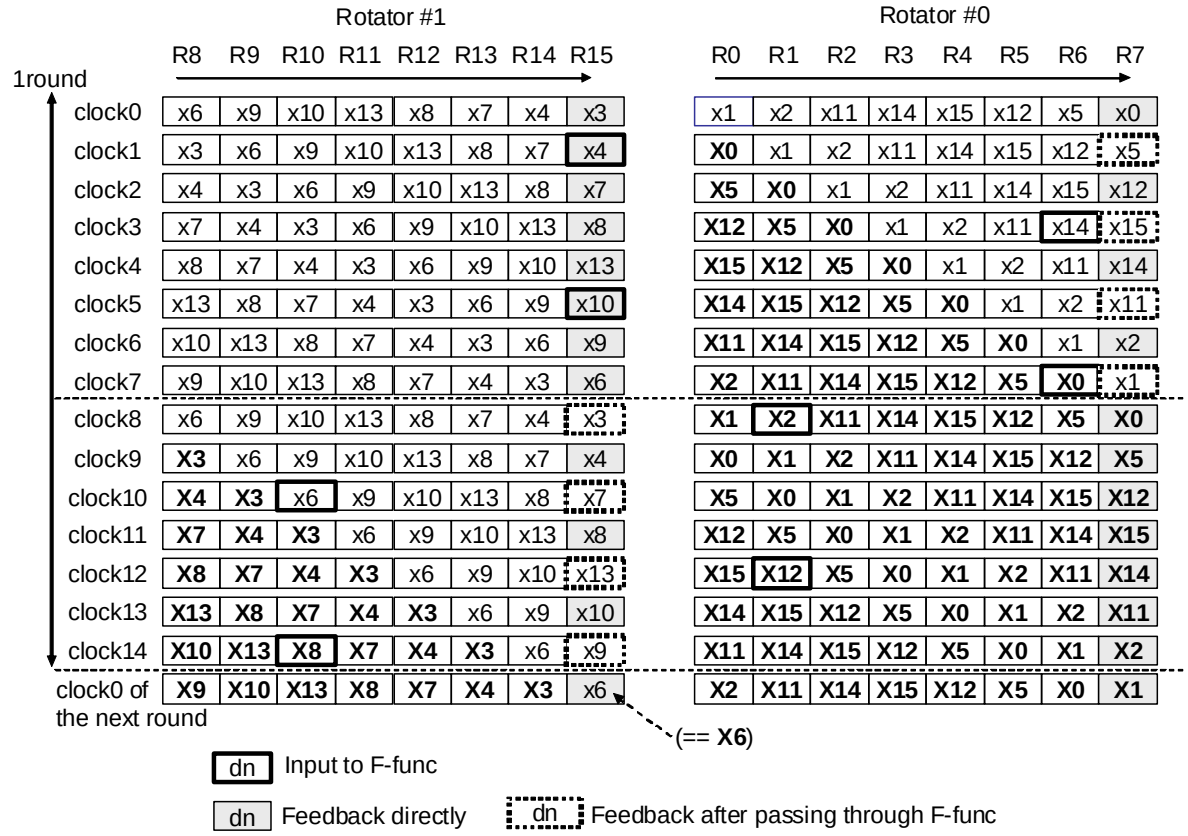


図 4: 提案するシリアライズ実装法のもとでのレジスタ値変化

した．各種軽量暗号との比較を表 3 に示す．また，現時点で最小クラスの PRESENT [10] との詳細比較を表 2 に示す．公平な比較のため，PRESENT と同じ UMC 0.18um スタンダードセル・ライブラリ UMCL18G212D3 を使用した．文献 [10] では scan FF や gated clock を使って GE 値を縮小し，配線面積も測定されていない．しかし今回は，**1.** で述べた理由により scan FF 等は未使用とし，配線面積と全面積も測定した．

表 2 のとおり，TWINE では 1 ラウンド/クロック構成（”round”）をシリアライズ構成（”serial”）にした時，GE 値は約 20%減少するのに対し，配線領域は約 45%減少する．ここで，ゲート領域よりも配線領域の方がずっと大きいので，ゲート数ではなく配線の減少率の方で全面積の大勢が決まる．2:1 セレクタ 1 個あたり配線が 3 本あるので，本手法のようにセレクタを減らすアプローチは効果的と言える．

結果として，シリアライズ版において，配線領域まで含めた全面積は PRESENT よりも TWINE の方が小さくなった．Scan FF や gated clock は使用していないが，仮に併用した場合，ゲート面積は約 1200GE 相当になる．

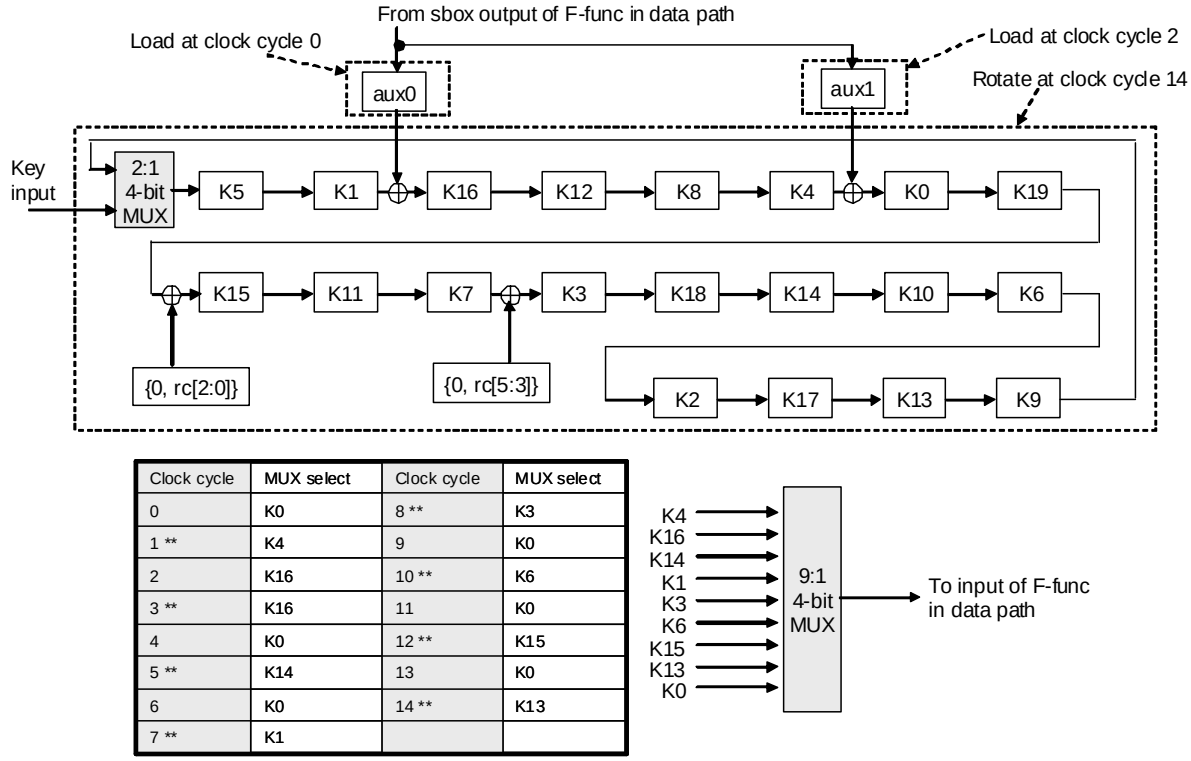
データパス系について見れば，80 ビットのデータ・レジスタ，1 個の SBox，および 2:1 セレクタ 32 個相当しか残っていないので，理論上の最小規模に近いものと考えられる．

4 おわりに

軽量暗号 TWINE の小規模回路実装方式について述べた．拡散層をローテータ実装し，シリアライズによる 2:1 セレクタ増加を 152 個から 32 個にまで抑制した．その結果，回路縮小目的の特殊セルなどを使用することなく方式設計のみで，配線領域まで含めた全面積を最小クラスに抑えることができた．

参考文献

[1] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M.J.B. Robshaw,



Clock cycle	MUX select	Clock cycle	MUX select
0	K0	8 **	K3
1 **	K4	9	K0
2	K16	10 **	K6
3 **	K16	11	K0
4	K0	12 **	K15
5 **	K14	13	K0
6	K0	14 **	K13
7 **	K1		

図 5: 今回用いた鍵スケジューラの回路構成

表 2: 提案手法による回路実装規模の詳細

	TWINE round◇	TWINE serial◇	PRESENT round◇	PRESENT serial◇	PRESENT round† [10]	PRESENT serial† [10]
UMC library 上 GE 値	1,809◇	1,446◇	2,238◇	1,435◇	1,650†	1,075†
セル領域面積 (um^2)	17,510◇	13,994◇	21,658◇	13,874◇	15,970†	10,403†
(うち，レジスタ全面積)	(8,136)	(10,661)	(8,572)	(9,357)	N/A	N/A
Scan FF 化可能レジスタ数	151	108	151	156	N/A (0)	N/A (0)
配線領域面積 (um^2)	82,227◇	45,220◇	111,487◇	50,914◇	N/A	N/A
全面積 (um^2)	99,737◇	59,214◇	133,145◇	64,788◇	N/A	N/A

[10] と同じ UMC0.18um スタセル使用，◇ は我々の HDL 実装を合成し ScanFF や Gated clock は未適用，† は適用した縮小後.

Y. Seurin and C. Vikkelsoe, “PRESENT: An Ultra-Lightweight Block Cipher”, CHES 2007, LNCS 4727, pp. 450-466, 2007.

[2] C. D. Canniere, O. Dunkelman and M. Knezevic. “KATAN and KTANTAN - A Family of Small and Efficient Hardware-Oriented Block Ciphers.” CHES ’09, pp. 272-288, 2009.

[3] J. Guo, T. Peyrin, A. Poschmann, M. J. B. Robshaw. “The LED Block Cipher.”, CHES’10, LNCS 6225, pp. 326-341.

[4] D. Hong, J. Sung, S. Hong, J. Lim, S. Lee, B. Koo, C. Lee, D. Chang, J. Lee, K. Jeong, H. Kim, J. Kim and S. Chee, “HIGHT: A New Block Cipher Suitable for Low-Resource Device.” CHES 2006, LNCS 4249, pp. 46-59, 2006.

[5] L. R. Knudsen, G. Leander, A. Poschmann and M. J. B. Robshaw. “PRINTcipher: A Block Cipher for IC-Printing.” CHES’10, LNCS 6225, pp. 16-32.

[6] Z. Gong, S. Nikova and Y.-W. Law. “KLEIN: A New Family of Lightweight Block Ciphers.” RFIDsec 2011.

[7] G. Leander, C. Paar, A. Poschmann, and K. Schramm. “New Lightweight DES Variants.” *Fast Software Encryption*-FSE’07, LNCS 4593, pp. 196-210, 2007.

[8] C. H. Lim and T. Korkishko. “mCrypton - A Lightweight Block Cipher for Security of Low-Cost RFID Tags and Sensors”. *Information Security Applications*-WISA’05, LNCS 3786, pp. 243-258, 2005.

表 3: 他の軽量暗号実装と本手法の比較

Algorithm	Function	Block (bit)	Key (bit)	Cycles/ block	Throughput (Kbps@100KHz)	Area (GE)	Gates / Memory bit	Type
TWINE **（提案手法）**	Enc	64	80	540	11.8	1446‡	6.75	serial
TWINE	Enc	64	80	36	178	1809‡	6.75	round
PRESENT [10]	Enc	64	80	547	11.4	1075‡	n/a	serial
PRESENT [1,10]	Enc	64	80	32	200	1650‡	6	round
AES [13]	Enc	128	128	226	57	2400	6	serial
mCRYPTON [8]	Enc	64	64	13	492.3	2420	5	round
SEA [9]	Enc+Dec	96	96	93	103	3758	n/a	round
HIGHT [4]	Enc+Dec	64	128	34	188.25	3048	n/a	round
KLEIN [6]	Enc	64	80	17	376.4	2629	n/a	round
KLEIN [6]	Enc	64	80	271	23.6	1478	n/a	serial
DES [7]	Enc	64	56	144	44.4	2309	12.19	serial
DESL [7]	Enc	64	56	144	44.4	1848	12.19	serial
KATAN [2]	Enc	64	80	254	25.1	1054	6.25	serial
Piccolo [11]	Enc	64	80	27	237	1496¶	6.25	round
Piccolo [11]	Enc+Dec	64	80	27	237	1634¶	6.25	round
Piccolo [11]	Enc	64	80	432	14.8	1043¶	6.25	serial
Piccolo [11]	Enc+Dec	64	80	432	14.8	1103¶	6.25	serial
LED [3]	Enc	64	80	1872	3.4	1040	6/4.67◇	serial
PRINTcipher [5]	Enc	48	80	48	12.5	503⋆	n/a	round

‡ 同一の UMC 0.18um ライブラリ使用．PRESENT は Gated clock, ScanFF 適用し縮小後．TWINE は未適用の縮小前．
¶ Includes a key register that costs 360 GEs; Piccolo can be implemented without a key register if key signal holds while encryption.
◇ Mixed usage of two memory units.
⋆ Hardwired key.

[9] F. Mace, F.-X. Standaert, and J.-J. Quisquater. “Implementations of the Block Cipher SEA for Constrained Applications.” Proceedings of the Third International Conference on RFID Security, RFIDSec 2007, pp.103-114.

[10] C. Rolfes, A. Poschmann, G. Leander, and C. Paar. “Ultra-Lightweight Implementations for Smart Devices - Security for 1000 Gate Equivalents.” Smart Card Research and Advanced Application Conference (CARDIS 2008), LNCS 5189, pp. 89-103, 2008.

[11] K. Shibutani, T. Isobe, H. Hiwatari, A. Mitsuda, T. Akishita, and T. Shirai. “Piccolo: An Ultra-Lightweight Blockcipher.” CHES 2011, LNCS 6917, pp. 342-357, 2011.

[12] Akashi Satoh, Sumio Morioka, Kohji Takano and Seiji Munetoh, ”A Compact Rijndael Hardware Architecture with S-Box Optimization.” ASIACRYPT2001, LNCS Vol.2248, pp.239-254, Dec 2001.

[13] A. Moradi, A. Poschmann, S. Ling, C. Paar, and H. Wang. “Pushing the Limits: A Very Compact and a Threshold Implementation of AES.” Eurocrypt 2011, LNCS 6632, pp. 69-88.

[14] T.Suzaki, K.Minematsu, S.Morioka and E.Kobayashi, ”TWINE: A Lightweight, Versatile Block Cipher,” ECRYPT Workshop on Lightweight Cryptography November 28-29, 2011.

[15] T.Suzaki, K.Minematsu, S.Morioka and E.Kobayashi, ”TWINE: A Lightweight Block Cipher for Multiple Platforms,” the conference on Selected Areas in Cryptography (SAC 2012).

[16] Y. Zheng, T. Matsumoto, and H. Imai. “On the Construction of Block Ciphers Provably Secure and Not Relying on Any Unproved Hypotheses.” *Advances in Cryptology* - CRYPTO ’89, LNCS 435, pp. 461-480, 1989.

[17] T. Suzaki and K. Minematsu. “Improving the Generalized Feistel.” *Fast Software Encryption*-FSE’10, LNCS 6147, pp.19-39, 2010.