ブロック暗号の大域構造と局所構造とに関する設計と解析

— 192 ビット鍵 128 ビットブロック暗号 Qcode[1] の提案 —

櫻井 幸一

九州大学 大学院 システム情報科学研究科 情報工学専攻

〒 812-81 福岡市東区箱崎 6-10-1

Phone.092-642-4050 Fax.092-632-5204

sakurai@csce.kyushu-u.ac.jp

あらまし: 本稿では，ブロック暗号の解析として，インボルーション型に代表される大域構造と (DES 暗号で使用される) S 箱に代表される局所構造とに注目し，従来提案されているブロック暗号の強度の評価を行う．さらに，得られた解析結果をふまえて，128 ビットを処理単位とする 192 ビット鍵長ブロック暗号 Qcode を提案し，その設計基準を述べる．

キーワード: DES 型暗号, ブロック暗号, S-box, 差分解読法，線形解読法

On the design and analysis of block-ciphering algorithms with remarking their global and local structures

— Qcode[2] : a 128-bit block ciphering algorithm with 192-bit key —

Kouichi SAKURAI

Graduate School of Information Science and Electrical Engineering

Kyushu University

6-10-1 Hakozaki, Higashi-ku, Fukuoka 812-81, Japan

Phone.+81-92-642-4050 Fax.+81-92-632-5204

sakurai@csce.kyushu-u.ac.jp

Abstract: The global and local strucutures in block ciphering algorithms are investigated. Especially, based on the observed designing criteria, a new ciphering algorithm named **Qcode** is proposed, which is a 128-bit block cipher with 192-bit key length. The designing principle of Qcode is described.

keywords: DES-like cipher, S-box, differential cryptanalysis, linear cryptanalysis

[1] **Qcode** は 佐野文彦（九州大学大学院システム情報科学研究科） と 櫻井幸一との研究 [SS96a,SS96b,SS96c] によるものである．

[2] The algorithm Qcode is developed in the series of the joint work with Fumihiko SANO of Kyushu Univ [SS96a,SS96b,SS96c].

1 はじめに

ブロック暗号の解読方法として，差分解読法 [BS90] や線形解読法 [M93] が提案されている．これらの解読法に対して耐性を持つブロック暗号を設計するためには，少なくとも，差分特性確率および線形特性確率が十分に小さいことを示さなければならない．また，より厳密には差分解読法に対する強度は，入出力の差分値を固定した場合でのあらゆる差分特性確率の和である差分確率により評価する必要がある．線形解読法に対してもどうように，入出力のマスク値を固定した場合でのあらゆる線形特性確率の和である線形確率により評価する必要がある．

ブロック暗号として，最も有名なものは対合 (involution) 構造を持った DES[FIPS77] である．対合型暗号は，使用される F 関数の構造によらず，暗号化復号化可能であるという利点がある．しかし，その一方で，暗号処理の各段でデータブロックの半分しか処理されない問題点がある．

我々は，各段の下位ブロックに全単射置換の関数を挿入する (図 4) ことにより，従来の対合構造を用いた場合よりも，少ない段数で差分特性確率および線形特性確率を小さくすることが可能であることを示す．

提案する暗号アルゴリズム Qcode は，128 ビットを処理単位とするブロック暗号であり，図 4に表される構造を用いる．また，Qcode に使用する各関数には，文献 [SS96a] で提案した有限体上の巾乗演算を用いることにより，高次多項式を用いながら，十分に小さい最大差分特性確率および最大線形特性確率を持つ．

従来の暗号が一般に同一の構造を繰り返すことにより構成されているのに対し，本稿で提案する Qcode は，平文暗号文側の解読に弱い部分に，今回提案する図 4の構造を用い，中間段は速度の低下を抑えるために従来の対合型構造を用いる．

2 対合 (involution) 型暗号

有名なブロック暗号の DES は対合型暗号の典型である．ここで，対合的暗号とは，以下の式で表される対合構造を利用した暗号化処理方式を呼ぶ．

$$\begin{aligned}(L_1, R_1) &= P \\ L_i &= R_{i-1} \\ R_i &= L_{i-1} \oplus F(R_{i-1}, K_i) \\ C &= (L_n, R_n)\end{aligned}$$

この方式の利点は，F 関数の構造によらず復号化可能であるという点にある．その一方で，暗号化処理の各段でデータブロックの半分は処理されないという問題点がある．例えば，最上段と最下段の F 関数への入力は，それぞれ平文および暗号文から直接導出できてしまう．線形解読法では，直接 F 関数の入力となるデータを用い，上下一段の F 関数に鍵を加えた状態の線形近似式を用いて解読を行う (n-2) 段攻撃により導出される鍵ビットが増加する．また，基本構造を繰り返す対合型暗号では，暗号

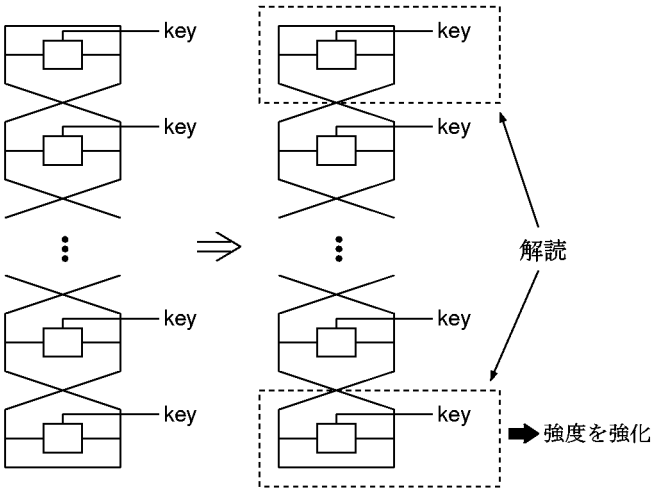

図 1: 対合型暗号の解読

全体の差分解読法や線形解読法に対する強度の増加は，段数に対して必ずしも定比例しない [K96].

このような等分割の対合型暗号の他にも，不等分割を用いた構造も提案されている [SB95]．端的な例としては，SHARK[RDPBW] などで用いられているように，データブロック全体を処理する方式もある．

$$Y = F(X, K)$$

こういった方式では，入出力のデータの一部がそのまま F 関数の入力となるといった問題点は解消される．しかし，一度に処理しなければならないデータブロックのサイズが増加するといった問題もある．

本稿では，差分解読法および線形解読法に対する強度評価には，それぞれ特性差分確率 [NK92](DCP)，特性線形確率 [N93] を用いる．対合型暗号に組み込まれる関数 F の最大差分特性確率および最大線形特性確率をそれぞれ，DCP^F_{max}，LCP^F_{max} とすると，$2n$ 段の暗号アルゴリズム全体の DCP,LCP の上界は $(DCP^F_{max})^n$，$(LCP^F_{max})^n$ で与えられる．これはあくまで最悪例であるが，鍵ビットを増加させた場合，十分に小さい最大特性確率を得るためには鍵ビット数に比例した段数が必要なことを示唆する．

3 提案する構造

我々が提案するQcodeの基本構造は，対合型構造の平文側および暗号文側から近いs段部分において，各段の下位ブロック(F関数の入力側)に全単射置換関数を組み込んだ構造を持つ．このQcodeの新構造はこの部分単独での解析において，192ビット鍵の全数探索基準に考えて十分に小さい差分特性確率および線形特性確率を持つよう設計する．

Qcodeは図5に示される，図4の構造と一般的な対合構造を組み合わせた暗号アルゴリズムである．図4の関数Jは全単射置換の関数である必要があるため，SHARK[RDPBW]を改良した暗号アルゴリズムJawsを用いる．また，関数Rには，LOKI91[BKPS]に用いられているS-boxをより高い巾指数に改良した関数Rockを用いる．

この構造は，一般的な対合構造よりも差分特性確率/線形特性確率を小さくすることが可能な反面，一段あたりの処理量がJawsの分だけ増加し速度が低下するという欠点を抱えている．この欠点を補うために，図4の構造を単純に繰り返さずに，暗号の上下3段は図4の構造を採用し，それらを連結する中間の段では，Rockを用いた単純な対合型構造を用いることにより処理効率の低下を抑え設計を採用した．したがって，Qcodeは図4の構造をそれぞれs段，Jawsの段数をt段，単純な対合構造のu段の三つのパラメータ$s-t-u$を持った設計の暗号である．

3.1 Jawsの構造

JawsはSHARK[RDPBW]のS-boxを変更した暗号である．SHARKのS-boxには$1/x$が使用されていたのに対して，JawsではSHARKの改良としてS-boxに，より高い次数の巾乗演算を用いる．

図5の上下各s段に挿入されたJaws-Blockは，Jawsをt段重ねた構造である．ただし，SHARKでは存在した最終段の鍵挿入層および逆拡乱層は構成上省略される．Jawsは入出力がそれぞれmビットの全単射置換S-boxがn個用いられている．鍵挿入層は，入力と拡大鍵との排他的論理和である．拡乱層は3.2節に述べる演算により隣接する2段で$n+1$個のS-boxが差分特性および線形表現に用いられる．

Jaws部分のS-boxには，最良と予想されている差分/線形特性確率を持つ高次巾乗関数または，[SS96a]で提案した準最良の線形特性確率を持つ以下の演算を使用する．

$$S(x) = (x^{119} \bmod 263) \bmod 256$$

上記関数は，x^3やx^{-1}といった差分確率および線形確率がおそらく最小となる有限体上の巾乗演算とは若干異なった関数である．S-boxは差分特性確率2^{-6}，線形特性確率$(1.25 \times 2^{-3})^2$の特性を持つ．この関数を用いた場合線形解読法に対して若干弱くなるが，最良の差分/線形特性確率を持つ関数とは代数的に性質の異なることが期待される．また代数的な攻撃の可能性を考慮して，高次数の関数を選択している．

ただし，既知の問題点としてこの関数は位数が14と短いという問題がある．たが，S-boxの出力がそのまま次のS-boxの入力となっているわけではない．拡乱層による線形変換や，鍵ビットの挿入などの操作が行われるため，位数に着目した代数的表現によって容易に解読できるわけではない．しかし，位数が短いことが問題となる攻撃が存在した場合を考慮して，最良の特性確率を持つ高次巾関数の採用も併せて考える．

3.2 拡乱(diffusion)層

拡乱層[RDPBW]は，なだれ効果によりビットを分散させ，差分解読および線形解読において近似に用いられるS-boxの数を増加させる構造である．逆変換可能な線形変換θにおいて，拡乱層の効果は分岐数Bにより評価される．

$\mathrm{w}_h(\mathrm{a})$をaのハミング重みとして次式で定義する．ハミング重みは，aの非零のブロック数である．

$$B(\theta) = \min_{a \neq 0}(w_h(a) + w_h(\theta(a)))$$

Bは拡乱層の最悪例での拡乱性能を表す．すなわち，Bは隣接する2段において，差分特性/線形表現に用いられるS-boxの数の下限を与える．SHARKでは，$B = n + 1$となる最適な線形変換としてReed-Soloman符号[MS77]が用いられている．Qcodeで使用する拡乱層も同様の最適な分岐数を持った線形変換を用いる．

3.3 Rockの構造

各段に組み込まれるF関数をRockと呼ぶ．RockはLOKI91 [BKPS]に用いられているF関数の演算を参考に，より高い巾指数を持った巾乗関数を組み込んだS-boxから構成される．設計方針として，F関数の実装にはテーブル参照を前提とし，演算の複雑さはあまり考慮しないことにした．テーブル参照を用いる場合，速度はメモリーのアクセス速度に依存してしまうが，複雑な演算を伴うF関数の処理はしばしば速度の低下を招くため，テーブル参照を用いた方が速度的に有利なことも多い．

Rockに用いるS-boxは12ビット入力8ビット出力である．したがって，S-boxひとつあたりのサイズは4Kバイトである．8個あるS-boxを別々に構成した場合，S-boxのテーブルのサイズは合計で32Kバイトになる．

メモリーの利用を軽減するため，8 個の S-box は同一のものを使用する．

Rock に用いられる S-box は以下の演算で表される．Y_i は S_i への入力である．

$$
\begin{aligned}
shift &= \{2,4,5,0,2,7,3,1,6,5,1,6,0,3,4,7\} \\
row &= Y_i\{11,10,1,0\} \\
col &= Y_i\{9,8,\cdots,3,2\} \\
t &= col^3 + 7 \times col^2 \\
&+ 7 \times (col \oplus (col >> shift_{row}/2) + 7 \\
S_i(Y_i) &= (LROT(t, shift_{row})^{491} \bmod 379) \bmod 256 \\
shift_{row} &\in \{2,4,5,0,2,7,3,1,6,5,1,6,0,3,4,7\}
\end{aligned}
$$

LROT(a,b) はデータ b に a ビット左巡回シフト演算を行う．shift_{row} は入力に依存した巡回シフトのシフト数のテーブルである．

Rock の最大差分特性確率および最大線形特性確率は以下の通りである．

$$DCP_{max} = 2^{-3.8} \qquad LCP_{max} = 2^{-7.0}$$

Rock は拡大転置したあと拡大鍵を挿入した結果を S-box で変換し，さらに拡乱層で線形変換を行う構造となっている．拡大転置 E には，以下の変換行列を用いる．各要素の表記は最上位から数えたビット位置である．

表 1: Rock の拡大転置 E

4	3	2	1	64	$\cdots$	57
60	59	58	57	56	$\cdots$	49
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
20	19	18	17	16	$\cdots$	9
12	11	10	9	8	$\cdots$	1

使用メモリー量を軽減するために，Jaws の拡乱層と Rock の拡乱層は同一のものを用いる．ただし，実装上は Jaws の拡乱層は S-box と組み合わされた演算結果が参照テーブルの内容となる．このテーブルを共有するために，Rock の各 S-box は実装上は Rock の S-box に Jaws の全単射置換 S-box の逆変換を組み合わせたものを使用する．

3.4 Rock 組み込みの設計

Qcode は，全単射置換の Jaws を用いた処理部と，非全単射な Rock を用いた処理部の二つの異なる関数を用いた処理を行う．Jaws ブロックは拡乱層の効果により Jaws の段数に比例して差分特性確率 / 線形特性確率が小さくなる．

Rock には Jaws で用いたものと同一の拡乱層が組み込まれている．そのため，図 2のように Rock を多段化することにより差分特性確率と線形特性確率を向上させることが可能であると考えられるが，Rock の非全単射性と拡大転置の存在存在により拡乱層の効果が若干異なる．

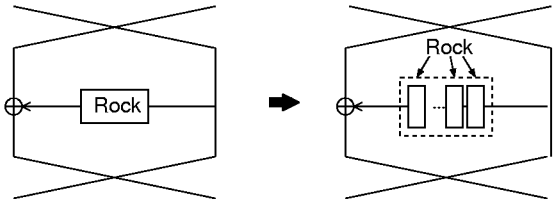

図 2: Rock の重複化

Jaws では，拡乱層の効果により段数が増加すれば特性確率が小さくなるのに対して，Rock のみを多段化した場合，差分解読法および線形解読法に対する強度は向上しない差分値やマスク値の入力が存在することに注意が必要である．そのような例を以下に示す．

非全単射関数を多段化した場合への差分解読法の適用を考える．Rock の出力差分 $\Delta Y = 0$ かつ入力差分 $\Delta X \neq 0$ の場合，Rock の出力側の差分値が 0 であるため，それ以後の Rock の入出力差分は確率 1 で 0 となる．したがって，Rock の最大特性差分を n 段組み合わせた場合，多段化された Rock 部の最大特性差分 $\text{DCP}^R_{max} \leq DCP^{Rock}_{max}$ である．線形解読法に対しても同様のことが示される．

対合構造に対する差分値 (マスク値) の波及の最悪例としては，2n 段インボルーション部の差分特性 / 線形表現に n 段の F 関数が用いられ，かつ F 関数中で S-box が一つしか用いられない場合が仮定される．この場合，大量の段数を必要としてしまう．

F 関数を強化するためには Rock の多段化が考えられるが，先に述べた理由により効果が小さい場合が存在する．そこで，Rock と Jaws を組み合わせた図 3の構造を提案する．差分解読法に対して考えみると，Rock を多段化した場合，出力の差分値が 0 となった Rock 以降の段は差分解読法に対して効果が期待できない．図 3の構造では，Rock の差分特性および入力側の Jaws の差分特性の双方が F 関数に用いられる．線形解読法に対しても同様である．

3.5 鍵生成部

対合型暗号では，各段で鍵を挿入するため，大量の鍵が必要である．一般に，この拡大鍵は入力鍵から各段で

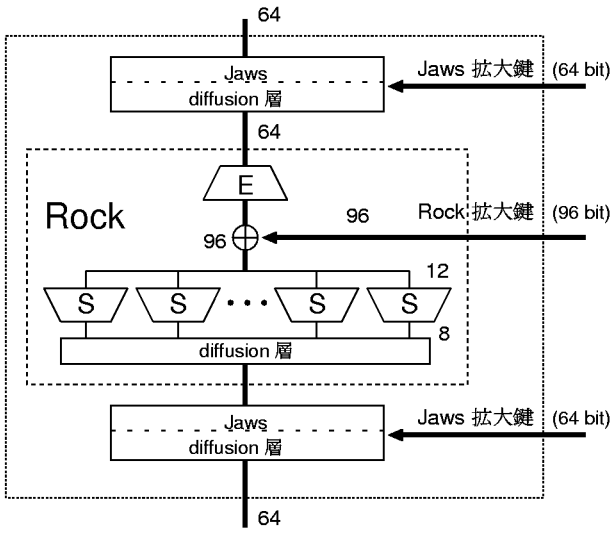

図 3: Rock ブロックの構造

用いられる拡大鍵を生成する鍵生成部により生成される．

鍵生成部の構成方法としては，暗号の速度を向上させるために，できるだけ構造を簡素にするアプローチと，鍵生成部に暗号化処理部分と同程度の複雑さを導入する二つのアプローチが存在する．鍵生成部を簡素に構成した場合，速度的に有利である一方で，鍵生成部に着目した攻撃が可能となる可能性がある．

また，鍵生成部に複雑な構造を用いる場合，極端な例としてはF 関数に用いるハッシュ関数を組み込み，データ暗号部と同等の強度与えることにより鍵に着目した攻撃を困難にすることが可能である．しかし，この方式では鍵生成部による処理の低下が無視できない．

提案する暗号では，後者のアプローチに近い若干複雑な鍵生成部を用いることにした．鍵生成にはデータの巡回シフトだけでなく一部のデータの変換にはJaws を用いた変換を行う構造を採用した．

鍵のビット長は 192 ビットである．鍵生成部は，この 192 ビットの鍵から各段の Rock および Jaws に用いられる拡大鍵を生成する． Jaws は一ブロックで t 段の構成を持つものを上下それぞれ s 段に組み込むので，合計 2st 段分必要である． Rock ブロックには全体で (2s+u) 段必要である． Qcode の鍵生成部は図 6で表される．鍵はまず 64 ビットずつの 3 ブロックに分割され，それぞれ巡回シフトや Jaws による変換を繰り返し，ビット選択で必要なだけの拡大鍵が取り出される．

4 強度評価

まず， Qcode の一部である図 4の構造を持つ暗号の評価を行う． Qcode は 192 ビット鍵ブロック暗号であるため，最大差分特性確率および最大線形特性確率はそれぞれ 2^{-192} 程度で抑えられることが期待される．

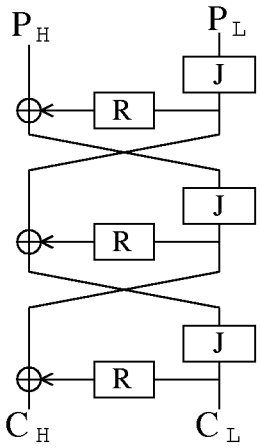

図 4:

図 4の構造の Jaws ブロック (J) の最大差分特性確率を $\mathrm{DCP}_m^J ax$， Rock ブロック (R) の最大差分特性確率を $\mathrm{DCP}_m^R ax$ とすると，図 4の構造 (3 段以上) の DCP_{max}およびLCP_{max} の上界は次式で与えられる．

$$\begin{aligned} DCP_{max} &\leq DCP^J_{max} \times DCP^R_{max} \\ LCP_{max} &\leq LCP^J_{max} \times LCP^R_{max} \end{aligned}$$

差分特性に関しては， $\Delta P_H \neq 0, \Delta P_L = 0, \Delta C_H \neq 0, \Delta C_L = 0$ の場合に上記の最大特性差分確率が求まる．

Rock ブロックは Jaws と Rock を組み合わせた図 3の構造を持つ． Jaws ブロックに組み込む S-box と段数 t を変化させた場合での DCP_{max},LCP_{max} の値は表 4で表される．

表 2: 図 3 の最大差分特性確率と最大線形特性確率

	最良関数を使用		準最良関数を使用	
t	DCP_{max}	LCP_{max}	DCP_{max}	LCP_{max}
2	$2^{-111.8}$	$2^{-115.0}$	$2^{-111.8}$	$2^{-111.7}$
4	$2^{-169.6}$	$2^{-183.0}$	$2^{-169.6}$	$2^{-181.7}$
6	$2^{-227.4}$	$2^{-234.0}$	$2^{-227.4}$	$2^{-231.7}$

次に Qcode の対合構造部の強度評価を行う．対合構造の F 関数位置には Jaws-Rock-Jaws 段数が 1-1-1 の

Rock ブロック (R) を組み込む．この場合 Rock ブロックの $\mathrm{DCP}^R_{max}(\mathrm{LCP}^R_{max})$ は次式で与えられる．

$$DCP^R_{max} \leq (DCP^{Jaws}_{max})^2 \times DCP^{rock}_{max}$$

対合構造部の段数が 2u の場合，全体の DCP_{max} および LCP_{max} の上界は次式で与えられる．

$$\begin{aligned} DCP_{max} &\leq 2^{-111.8u} \\ LCP_{max} &\leq \begin{cases} 2^{-103.4u} & \text{(準最良の場合)} \\ 2^{-115u} & \text{(最良の場合)} \end{cases} \end{aligned}$$

したがって，Jaws ブロックに組み込む S-box と対合部の段数 u を変化させた場合での DCP_{max},LCP_{max} の値は表 4で表される．

表 3: 対合部の最大差分特性確 率と最大線形特性確率

	最良関数を使用		準最良関数を使用	
u	DCP_{max}	LCP_{max}	DCP_{max}	LCP_{max}
2	$2^{-57.8}$	$2^{-61.0}$	$2^{-57.8}$	$2^{-58.7}$
4	$2^{-115.6}$	$2^{-128.0}$	$2^{-115.6}$	$2^{-119.4}$
6	$2^{-173.4}$	$2^{-183.0}$	$2^{-173.4}$	$2^{-178.1}$
8	$2^{-231.2}$	$2^{-244.0}$	$2^{-231.2}$	$2^{-234.8}$

5 Qcode の速度

図 5の各パラメータ (s-t-u) を変更した場合でのデータ処理部のスループットを計測した．

表 4: Qcode の速度

	u (単位: Mbits/sec)			
s-t	6	8	10	12
3-4	1.61	1.45	1.34	1.28
3-6	1.11	1.06	0.93	0.92
4-4	1.21	1.14	1.07	0.99
4-6	0.82	0.79	0.76	0.72
0-0	12.00	8.90	6.95	6.12

(実験環境)

OS: Linux CPU: Pentium 120MHz

コンパイラ: gcc-2.7.2 -O2

6 まとめ

本稿では，128 ビットを処理単位とする 192 ビット鍵ブロック暗号 Qcode の提案を行った． Qcode は従来の対合構造を元に，新しい関数を挿入した構造である．この構造は従来の対合構造を用いた場合よりも，差分 / 線形特性確率を小さくすることが可能である．

今後の課題としては，

1. 最大平均差分 / 線形確率を用いた証明可能安全性の評価
2. 速度と暗号の強度とのバランスを考慮した各部構造の段数の決定
3. 使用メモリー量の削減

が挙げられる．

参考文献

[AO96] 青木和麻呂, 太田和夫. “最大平均差分確率および最大平均線形確率のより厳密な評価.” 暗号と情報セキュリティシンポジウム, SCIS96-4A(1996).

[BD93] T.Beth, C.Ding. “On Almost Perfect Nonlinear Permutation.” Advances in Cryptology – Eurocrypt’93, Springer-Verlag(1993)

[BKPS] L.Brown, M.Kwan. J.Pieprzyk, J. Seberry. “Improving Resistance to Differential Cryptalaysis and the Redesign of LOKI.” Advances in Cryptology – ASIACRYPT’91, Springer-Verlag(1991)

[Ba96] S.Vaudenay, “An experiment on DES statistical cryptanalysis” Proc. of 3rd ACM CCCS(1996).

[BS90] E.Biham and A.Shamir. “Differential Cryptanalysis of DES-like Cryptosystems.” Journal of CRYPTOLOGY,Vol.4,Number 1,1991(The extended abstract appeared at CRTPTO’90)

[CV94] F.Chabaud, S.Vaudenay. Links Between Differential and Linear Cryptanalysis. Preproceedings of Eurocrypt’94 (1994).

[FIPS77] “Data Encryption Standard.” Federal Information Processing Standards Publicatoin 46, National Bureau of Standards,U.S.Department of Commerce (1977)

[JK96] T.Jakobsen, L.Knudsen. “Breaking Ciphers of Low Nonlinear Order.” in Short talk, Fast Software Encryption Third International Workshop, Springer(1996).

[LMM91] X. Lai, J.L.Massey, S. Murphy. Markov Ciphers and Differential Cryptanalysis. Advances in Cryptology — EUROCRYPT’94, Lecture Notes in Computer Science 547), Springer-Verlag(1991).

[K96] 金子 泰祥.“DES 型暗号の段数に依存する証明可能安全性評価.” 信学技報, ISEC96-8 (1996)

[Knu94] L. Knudses. Truncated and Higher Order Differentials. Fast Software Encryption, Springer-Verlag(1994).

[Lai94] X. Lai. Higher Order Derivatives and Differential Cryptanalysis. Communications and Cryptography, Kluwer Academic Publishers(1994).

[M93] 松井 充. “DES 暗号の線形解読 (I).” 暗号と情報セキュリティシンポジウム,SCIS93-3C(1993)

[M95A] M.Matsui. Recent Topics on Block Ciphers — Open Problems To Be Solved —. JAPAN-KOREA JW-ISC'95 PROCEEDINGS(1995)

[M95B] 松井充. ブロック暗号の差分解読法と線形解読法に対する証明可能安全性について. 第 18 回 情報理論とその応用シンポジウム (SITA95) 予稿集, C-2-C (1995).

[M96] 松井充. ブロック暗号アルゴリズム MISTY, 信学技報, ISEC96-11(1996).

[MISTY96] 松井充, 市川哲也, 反町亨, 時田俊雄, 山岸篤弘. 差分解読法と線形解読法に対する証明可能安全性をもつ実用ブロック暗号. 暗号と情報セキュリティシンポジウム, SCIS96-4C(1996).

[MS77] F. MacWilliams, N.Sloane, “The Tehory of Error-Correcting Codes,” North-Holland, Amsterdam (1997).

[N93] K. Nyberg. Differentially uniform mappings for cryptography. Advances in Cryptology – Eurocrypt'93, Springer-Verlag(1993).

[N94] K.Nyberg. Linear Approximation of Block Ciphers. Advances in Cryptology - Eurocrypt'94,Lecture Notes in Computer Science 950, Springer-Verlag(1994).

[NK92] K.Nyberg, L.Knudsen. Provable Security Against Differential Cryptanalysis. Advances in Cryptology — CRYPTO'92, Lecure Notes in Computer Science 740, Springer-Verlag(1993).

[NK95] K.Nyberg, L.Knudsen. Provable Security Against Differential Attack. Journal of Cryptology, Vol.8, no.1(1995).

[RDPBW] V.Rijmen, J.Daemen, B.Preneel, A.Bosselaers, E.Win. “The Cipher SHARK.” Fast Software Encryption Third International Workshop, Springer(1996)

[SB95] B. Schneier, M. Blaze, “MacGuffin: an unbalanced Feistel network block cipher.” Fast Software Encryption, Springer-Verlag(1994)

[SS96a] 佐野 文彦, 櫻井 幸一.“多項式が生成する S-box の暗号論的性質について” 電子情報通信学会 信学技報, ISEC96-39 (1996)

[SS96b] 佐野 文彦, 櫻井 幸一.“ブロック暗号の基本構造に関する一考察” 電子情報通信学会 信学技報, ISEC96 (Nov. 1996)

[SS96c] 佐野 文彦, 櫻井 幸一.“Qcode: インターネット向け 192 ビット鍵 128 ビットブロック暗号アルゴリズム”Working Draft (Nov. 1996)

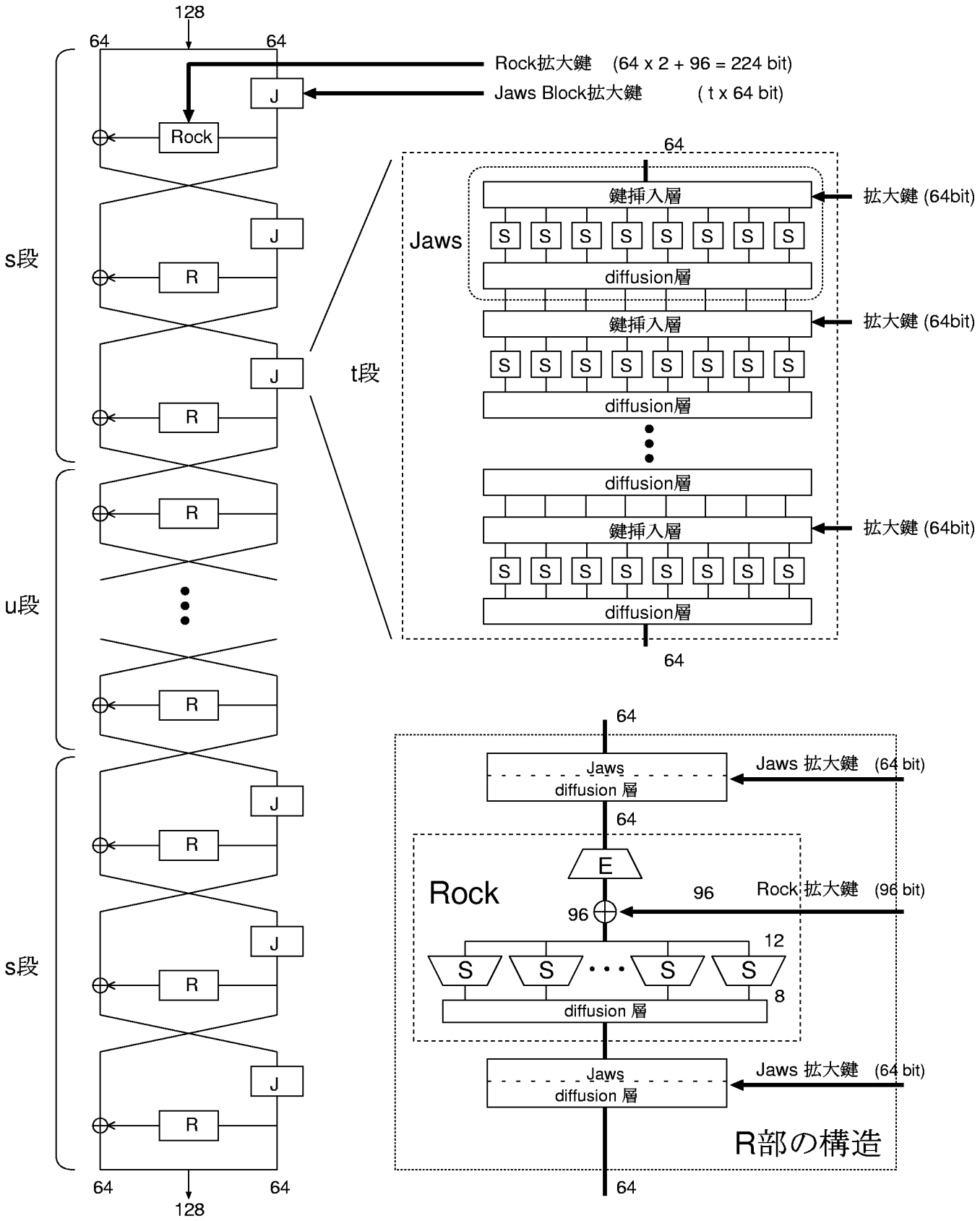

図 5: Qcode の全体構造

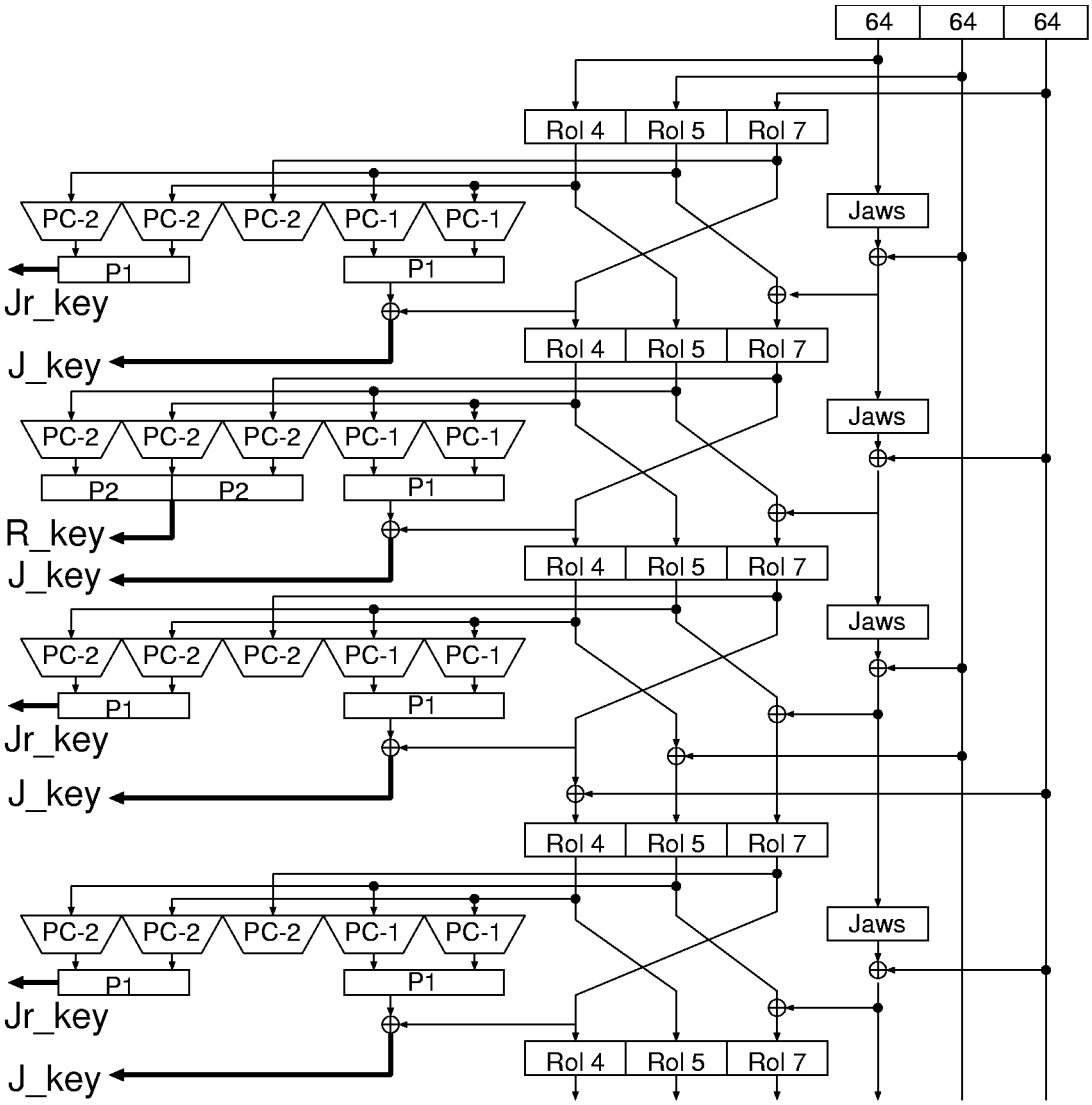

図 6: 鍵生成部の構造

PC-1,PC-2:	64 ビットから 32 ビットを選択
P1,P2:	ビット転置
Rol 4:	64 ビットブロックを 4 ビット左巡回シフト
Rol 5:	64 ビットブロックを 5 ビット左巡回シフト
Rol 7:	64 ビットブロックを 7 ビット左巡回シフト
R_key:	Rock への拡大鍵 96 ビット
Jr_key:	Rock 構造部中の Jaws への拡大鍵 64 ビット
J_key:	Jaws への拡大鍵 64 ビット