TripleDES 拡張暗号アルゴリズム

2G－5

佐野文彦† 川村信一‡ 才所敏明†

†（株）東芝 ＳＩ技術開発センター ‡（株）東芝 研究開発センター

1 はじめに

本稿では我々が設計した暗号アルゴリズム Triplo を提案する。Triplo は 256 ビットの暗号化鍵をもつ 64 ビットブロック暗号であり、特定のパターンを持った鍵を与えることにより、DES,DES-SS,2key-TripleDES の三種類の暗号アルゴリズムと同一の暗号化処理を指定することが可能な暗号アルゴリズムである。

2 アルゴリズムの概要

Triplo は 3 種類の暗復号化関数ブロックの組み合わせで構成され、それぞれ基本関数 Ea、Eb および Qa と呼ぶ。以下に暗号化モードでの各基本ブロックの構成を述べる。

2.1.1 基本関数 Ea

基本関数 Ea は DES-SS[2]の段関数を 16 段繰り返す構造を持つ暗復号化ブロックである。

2.1.2 基本関数 Eb

基本関数 Eb は DES[1]の段関数を 16 段繰り返す構造を持つ暗復号化ブロックである。

2.1.3 基本関数 Qa

基本関数 Qa は図 1 に示す構造を持つ変換関数である。入力の右 32 ビットは 32 ビットの鍵 QK_1 と XOR される。QK_2 はそれぞれ 1 ビットの鍵であり、S9 は S_9(K,B)とする。ここで S_9 (0,B)=B であり、S_9 (1,B)には表 1 の非線型置換テーブルを用いる。

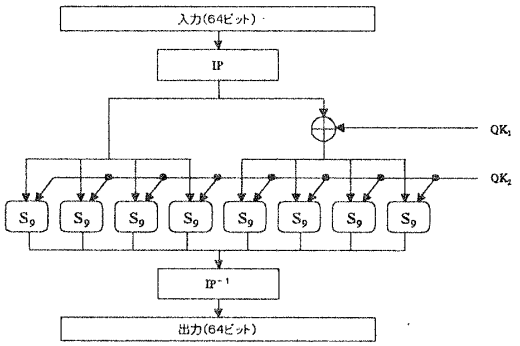

図 1： 基本関数 Qa の構造

2.2 基本関数の構成

データ暗号化の処理は図 2 の構造により、64 ビットの入力ブロックに対して基本関数 Ea →Qa→Eb→Qa→Ea の順序で鍵に依存した攪拌が行われ、最終的な出力である 64 ビットの暗号文が得られる。

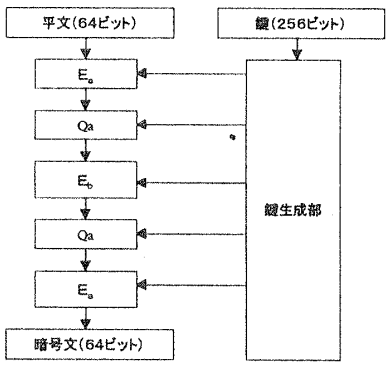

図 2： データ暗号化部の構成

2.3 鍵スケジュール

256 ビットの鍵から拡大鍵を生成する鍵スケジュール部の構成は図 3 であらわされる。鍵は 56 ビットずつのブロックに分割され、それぞれ所定の操作により、各基本関数ブロックの拡大鍵が生成される。

"Block Encryption Algorithm Triplo"

†Fumihiko Sano, ‡Shinichi Kawamura,
†Toshiaki Saisho.
†System Integration Technology Center,
‡R&D Center,
TOSHIBA CORPORATION

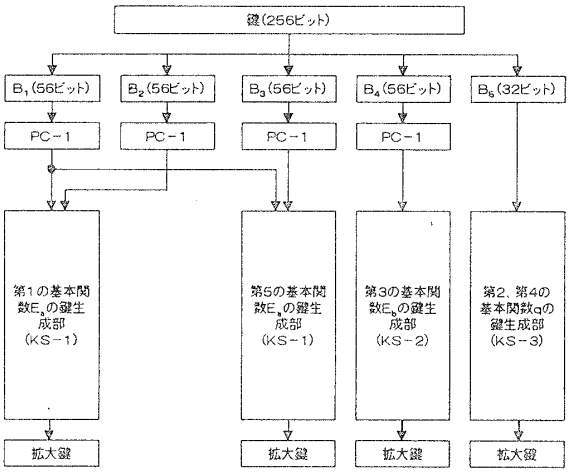

図３：　鍵スケジュール部

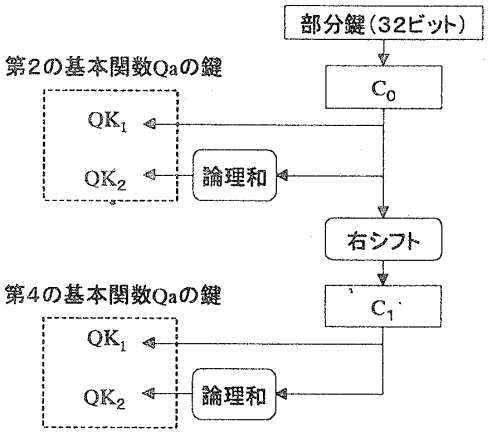

図４：鍵生成部 KS-3

PC-１は、入力を７ビットずつのブロックに分割し各ブロックに１ビットのパリティを加える拡大転置であり、56 ビットの入力に対して 64 ビットを出力する。

暗号化モードの鍵生成では、KS-1 は 128 ビットの入力に対して、DES-SS 暗号化モードの拡大鍵を生成し、KS-2 は 64 ビットの入力に対して、DES 復号モードの拡大鍵を生成する。KS-3 は以下の通り。

3 おわりに

本稿では 256 ビットの暗号化鍵を用いた 64 ビットブロック暗号を提案した。本アルゴリズムは、特定のパターンの鍵を入力することにより、DES、DES-SS、TripleDES との互換性を有する。

参考文献

[1] FIPS PUB 46-3, “DATA ENCRYPTION STANDARD”, 1999.

[2]佐野，櫻井．“DES-SS:DES 互換な 128 ビット鍵長ブロック暗号”，SITA96,1996.

表１：転置テーブル　$S_9(1,B)$

124	79	197	90	4	126	227	226	200	118	225	43	155	110	119	29
134	228	125	20	6	160	39	2	47	177	217	234	145	249	128	92
149	179	24	26	144	238	240	104	85	12	10	95	73	129	167	251
213	123	222	187	82	132	235	168	46	86	162	27	250	0	140	215
220	157	67	254	158	91	3	55	194	21	25	37	210	41	182	30
252	116	84	38	59	201	253	231	170	96	22	218	137	89	63	180
60	169	255	62	209	190	223	32	127	207	8	51	7	44	150	45
57	9	141	208	151	153	239	143	211	97	58	108	148	69	161	121
76	71	64	244	171	14	33	204	49	78	15	175	75	99	113	54
135	102	28	87	114	199	212	142	191	181	186	219	93	216	241	103
188	174	224	183	16	221	165	133	31	56	106	232	80	88	105	242
11	52	202	40	109	236	35	163	138	23	146	117	237	17	192	147
156	154	122	203	205	50	1	112	206	189	193	246	61	176	42	233
13	18	5	214	166	111	131	152	185	247	164	19	173	195	72	172
130	100	74	70	120	107	34	136	65	115	178	248	245	81	229	66
83	94	198	139	243	53	68	101	48	77	196	36	230	159	98	184