

(19) 日本国特許庁(JP)

(12) 公表特許公報(A)

(11) 特許出願公表番号

特表2008-514975

(P2008-514975A)

(43) 公表日 平成20年5月8日(2008.5.8)

(51) Int.Cl.
G09C 1/00 (2006.01)F I
G09C 1/00 610Bテーマコード (参考)
5J104

審査請求 未請求 予備審査請求 未請求 (全 26 頁)

(21) 出願番号 特願2007-532996 (P2007-532996)
 (86) (22) 出願日 平成17年9月20日 (2005.9.20)
 (85) 翻訳文提出日 平成19年5月16日 (2007.5.16)
 (86) 国際出願番号 PCT/IB2005/003104
 (87) 国際公開番号 W02006/033013
 (87) 国際公開日 平成18年3月30日 (2006.3.30)
 (31) 優先権主張番号 2004905507
 (32) 優先日 平成16年9月24日 (2004.9.24)
 (33) 優先権主張国 オーストラリア (AU)
 (31) 優先権主張番号 2004906543
 (32) 優先日 平成16年11月16日 (2004.11.16)
 (33) 優先権主張国 オーストラリア (AU)
 (31) 優先権主張番号 2004907361
 (32) 優先日 平成16年12月30日 (2004.12.30)
 (33) 優先権主張国 オーストラリア (AU)

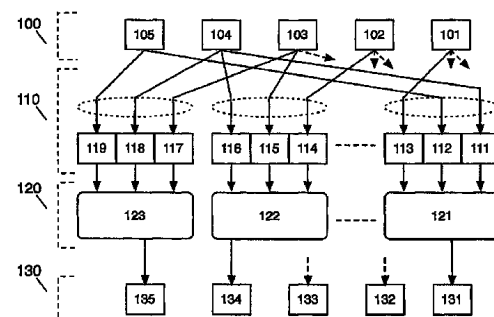
(71) 出願人 507092126
 シナプティック ラボラトリーズ リミテ
 ッド
 イギリス領バージン諸島 トルトーラ ロ
 ードタウン ビーオーボックス 146
 トライデント チャンバーズ
 (74) 代理人 100096024
 弁理士 柏原 三枝子
 (72) 発明者 オニール, ショーン
 オーストラリア クイーンズランド 40
 06 フォーティチュードヴァリー, ブラ
 ンスウィックストリート 255/421
 Fターム(参考) 5J104 AA18 JA05 JA09 JA13 NA39
 PA07

最終頁に続く

(54) 【発明の名称】 sボックス

(57) 【要約】

多入力多出力のsボックスであって、a個の隣接番号の入力ビット(101, 102, 103, 104, 105) I_1 、 I_2 乃至 I_a を受信し、ここでaは少なくとも4であり、b個の連続番号の出力ビット(131, 132, 133, 134, 135) O_1 、 O_2 乃至 O_b を出力する。このsボックスは、c個の一次sボックス(121, 122, 123) s_{b1} 、 s_{b2} 乃至 s_{bc} を含む。各一次sボックス(121, 122, 123)は多入力単一出力のブール関数 f_1 、 f_2 乃至 f_c を具え、これらが多入力と単一出力の関係を規定する。各一次sボックス(121, 122, 123)はそれぞれ入力ビット s_1 、 s_2 乃至 s_c のセットを受信し、これらのセットがそれぞれ前記sボックスへのa個の入力ビット(101, 102, 103, 104, 105)から選択され、それぞれ s_{l1} 、 s_{l2} 乃至 s_{lc} ビットを含む。前記 s_{l1} 、 s_{l2} 乃至 s_{lc} の数は3乃至(a-1)の範囲内にあり、前記 s_{l1} 、 s_{l2} 乃至 s_{lc} の数の合計がaより大きい。前記sボックスのb個の出力ビット(131, 132, 133, 134, 135)が、前記



【特許請求の範囲】

【請求項 1】

多入力多出力の s ボックスであって：

a 個の隣接番号の (contiguously numbered) 入力ビット I_1 、 I_2 乃至 I_a を受信し、ここで a は少なくとも 4 であり、

b 個の連続番号の出力ビット O_1 、 O_2 乃至 O_b を出力するよう構成され、

この s ボックスが：

c 個の一次 s ボックス $s b_1$ 、 $s b_2$ 乃至 $s b_c$ を含み、それぞれ：

多入力単一出力のブール関数 f_1 、 f_2 乃至 f_c を含み、これらが多入力と単一出力の関係の規定しており、

入力ビット s_1 、 s_2 乃至 s_c のセットをそれぞれ受信するよう構成され、これらのセットがそれぞれ前記 s ボックスへの a 個の入力ビットから選択され、それぞれ $s l_1$ 、 $s l_2$ 乃至 $s l_c$ ビットを含み、これにより：

前記 $s l_1$ 、 $s l_2$ 乃至 $s l_c$ の数が 3 乃至 $(a-1)$ の範囲内にあり；

前記 $s l_1$ 、 $s l_2$ 乃至 $s l_c$ の数の合計が a より大きく、

前記 s ボックスの b 個の出力ビットが、前記 c 個のブール関数の出力を含むことを特徴とする s ボックス。

【請求項 2】

請求項 1 の多入力多出力 s ボックスにおいて、前記 s ボックスの b 個の出力ビットが前記 c 個の一次 s ボックスの出力であることを特徴とする s ボックス。

【請求項 3】

請求項 1 または 2 の多入力多出力 s ボックスにおいて、a が 16 以上であることを特徴とする s ボックス。

【請求項 4】

請求項 1 乃至 3 のいずれか 1 項の多入力多出力 s ボックスにおいて、b が 16 以上であることを特徴とする s ボックス。

【請求項 5】

請求項 1 乃至 4 のいずれか 1 項の多入力多出力 s ボックスにおいて、c が 12 以上 b 以下であることを特徴とする s ボックス。

【請求項 6】

請求項 1 乃至 5 のいずれか 1 項の多入力多出力 s ボックスにおいて、それぞれ 1 から a の i と j について、 s_i と s_j の各セットが $\min(s l_i, s l_j) - 1$ ビット以下を共有することを特徴とする s ボックス。

【請求項 7】

請求項 1 乃至 6 のいずれか 1 項の多入力多出力 s ボックスにおいて、前記数 $s l_1$ 、 $s l_2$ 乃至 $s l_c$ の合計が a の 1.5 倍より大または等しいことを特徴とする s ボックス。

【請求項 8】

請求項 1 乃至 7 のいずれか 1 項の多入力多出力 s ボックスにおいて、a、b、c の少なくとも 1 つが素数であることを特徴とする s ボックス。

【請求項 9】

請求項 1 乃至 8 のいずれか 1 項の多入力多出力 s ボックスにおいて、前記数 a と b が 1 より大きな公約数を持たないことを特徴とする s ボックス。

【請求項 10】

請求項 1 乃至 9 のいずれか 1 項の多入力多出力 s ボックスにおいて、前記数 $s l_1$ 、 $s l_2$ 乃至 $s l_c$ の少なくとも 2 つが同じであることを特徴とする s ボックス。

【請求項 11】

請求項 10 の多入力多出力 s ボックスにおいて、前記数 $s l_1$ 、 $s l_2$ 乃至 $s l_c$ の全部が同じであることを特徴とする s ボックス。

【請求項 12】

請求項 1 乃至 11 のいずれか 1 項の多入力多出力 s ボックスにおいて、入力ビットセッ

ト s_1 、 s_2 乃至 s_c がそれぞれ、確率的プロセス (provabilistic) を用いて選択されることを特徴とする s ボックス。

【請求項 13】

請求項 1 乃至 12 のいずれか 1 項の多入力多出力 s ボックスにおいて、前記入力ビットセット s_1 、 s_2 乃至 s_c の少なくとも 1 つを選択するのに用いられるプロセスがキード (keyed) されていることを特徴とする s ボックス。

【請求項 14】

請求項 12 または 13 の多入力多出力 s ボックスにおいて、前記入力ビットセット s_1 、 s_2 乃至 s_c の選択は、少なくとも 1 の基準 (criterion) を満たすよう実践的に改良 (heuristically refined) されていることを特徴とする s ボックス。

10

【請求項 15】

請求項 1 乃至 14 のいずれか 1 項の多入力多出力 s ボックスにおいて、前記ブール関数 f_1 、 f_2 乃至 f_c は確率的プロセス (provabilistic) を用いて生成されることを特徴とする s ボックス。

【請求項 16】

請求項 1 乃至 15 のいずれか 1 項の多入力多出力 s ボックスにおいて、前記ブール関数 f_1 、 f_2 乃至 f_c の少なくとも 1 つを生成するのに用いられるプロセスがキード (keyed) されていることを特徴とする s ボックス。

【請求項 17】

請求項 15 または 16 の多入力多出力 s ボックスにおいて、前記少なくとも 1 のブール関数 f_1 、 f_2 乃至 f_c の選択は、少なくとも 1 の基準 (criterion) を満たすよう実践的に改良 (heuristically refined) されていることを特徴とする s ボックス。

20

【請求項 18】

請求項 1 乃至 17 のいずれか 1 項の多入力多出力 s ボックスにおいて、前記ブール関数 f_1 、 f_2 乃至 f_c の少なくとも 1 つは平衡したブール関数 (ballanced Boolean function) であることを特徴とする s ボックス。

【請求項 19】

請求項 18 の多入力多出力 s ボックスにおいて、前記ブール関数 f_1 、 f_2 乃至 f_c がそれぞれ平衡したブール関数 (ballanced Boolean function) であることを特徴とする s ボックス。

30

【請求項 20】

請求項 1 乃至 19 のいずれか 1 項の多入力多出力 s ボックスにおいて、前記ブール関数 f_1 、 f_2 乃至 f_c の少なくとも 1 つが、2 対 1 マルチプレクサ関数 (two-to-one multiplexer function) を具えることを特徴とする s ボックス。

【請求項 21】

請求項 20 の多入力多出力 s ボックスにおいて、前記ブール関数 f_1 、 f_2 乃至 f_c がそれぞれ 2 対 1 マルチプレクサ関数 (two-to-one multiplexer function) を具えることを特徴とする s ボックス。

【請求項 22】

請求項 1 乃至 21 のいずれか 1 項の多入力多出力 s ボックスにおいて、前記ブール関数 f_1 、 f_2 乃至 f_c の少なくとも 1 つがユニークなブール関数であることを特徴とする s ボックス。

40

【請求項 23】

請求項 22 の多入力多出力 s ボックスにおいて、前記ブール関数 f_1 、 f_2 乃至 f_c がそれぞれユニークなブール関数であることを特徴とする s ボックス。

【請求項 24】

請求項 22 または 23 の多入力多出力 s ボックスにおいて、前記関数 f_1 、 f_2 乃至 f_c 間の差 (difference) がアフィン (affine) であることを特徴とする s ボックス。

【請求項 25】

請求項 1 乃至 24 のいずれか 1 項の多入力多出力 s ボックスにおいて、実行時に再構成

50

される (reconfigured) ことを特徴とする s ボックス。

【請求項 26】

請求項 1 乃至 25 のいずれか 1 項の多入力多出力 s ボックスにおいて、前記入力ビットセット s_1 乃至 s_c の少なくとも 1 つが実行時に変更されることを特徴とする s ボックス。

【請求項 27】

請求項 1 乃至 26 のいずれか 1 項の多入力多出力 s ボックスにおいて、前記関数 f_1 、 f_2 乃至 f_c の少なくとも 1 つが実行時に再構成されることを特徴とする s ボックス。

【請求項 28】

請求項 1 乃至 27 のいずれか 1 項の多入力多出力 s ボックスにおいて、 $(c - a)$ 乃至 a のすべての i について： 10

各一次 s ボックス s_{b_i} への s_{l_i} の入力ビットのセットが、入力ビット I_1 乃至 I_i から選択され；

入力ビット I_i と出力ビットの関係が線形であることを特徴とする s ボックス。

【請求項 29】

請求項 28 の多入力多出力 s ボックスにおいて、 I_1 乃至 I_a の a 個のビットセットの $T = (a - c)$ ビットのサブセットが、ビット I_1 乃至 I_T の $T \times T$ の全単射 (bijective mapping) の入力であることを特徴とする s ボックス。

【請求項 30】

請求項 1 乃至 29 のいずれか 1 項の多入力多出力 s ボックスにおいて、 W が一定である $(W + 1)$ 乃至 a のすべての i について： 20

前記一次 s ボックス s_{b_i} への s_{l_i} の入力ビットのセットが、入力ビット $I_{(i - w)}$ 乃至 I_i から選択され；

入力ビット I_i と前記 s ボックス s_{b_i} の出力ビットの関係が線形であることを特徴とする s ボックス。

【請求項 31】

請求項 30 の多入力多出力 s ボックスにおいて、 W が 2 乃至 $(a - 1)$ の範囲にあることを特徴とする s ボックス。

【請求項 32】

請求項 30 または 31 の多入力多出力 s ボックスにおいて、 I_1 乃至 I_w の W ビットが、 $W \times W$ の全単射の入力であることを特徴とする s ボックス。 30

【請求項 33】

請求項 1 乃至 27 のいずれか 1 項の多入力多出力 s ボックスにおいて、入力ビット s_1 、 s_2 乃至 s_c のセットの入力ビットの s_{l_1} 、 s_{l_2} 乃至 s_{l_c} の選択は：

隣接番号の (contiguously numbered) 入力ビット I_1 、 I_2 乃至 I_a では、ビット I_a がビット $I_{(a - 1)}$ と同様にビット I_1 と隣接 (contiguous) するよう扱われ、これにより入力ビット I_1 、 I_2 乃至 I_a がビットの巡回収集 (circular collection) とみなされ；

前記隣接番号の入力ビット I_1 、 I_2 乃至 I_a のセットは、ビット w_1 乃至 w_d の領域 (windows) のセットを含むとみなされ、ここで d は 3 乃至 $(c / 3)$ の範囲にあり： 40

各領域 (window) が最初と最後の領域境界を有し、各領域境界が、一次 s ボックス s_{b_i} と $s_{b_{i+1}}$ 間の同じ方向に 1 ビット位置ずつ増大し；

隣接番号の (contiguously numbered) 出力ビット O_1 、 O_2 乃至 O_b のセットでは、前記ビット O_b がビット O_{b-1} と同様にビット O_1 と隣接するよう扱われ、これにより出力ビット O_1 、 O_2 乃至 O_b がビットの巡回収集とみなされ；

セット s_{b_1} 乃至 s_{b_c} 内の各一次 s ボックス s_{b_k} について：

一次 s ボックス s_{b_k} への入力ビットが、領域 w_k 以外の入力ビットの少なくとも 2 つの領域からの少なくとも 1 のビットを含むことを特徴とする s ボックス。

【請求項 34】

請求項 33 の多入力多出力 s ボックスにおいて、各一次ボックス s_{b_i} について、領域 50

w_1 乃至 w_d の少なくとも 2 つのサイズが異なることを特徴とする s ボックス。

【請求項 35】

請求項 1 乃至 27 のいずれか 1 項の多入力多出力 s ボックスにおいて、入力ビット s_1 、 s_2 乃至 s_c のセットの入力ビットの s_{l_1} 、 s_{l_2} 乃至 s_{l_c} の選択はそれぞれ：

隣接番号の (contiguously numbered) 入力ビット I_1 、 I_2 乃至 I_a では、ビット I_a がビット I_{a-1} と同様にビット I_1 と隣接 (contiguous) するよう扱われ、これにより入力ビット I_1 、 I_2 乃至 I_a がビットの巡回収集 (circular collection) とみなされ；

前記隣接番号の入力ビット I_1 、 I_2 乃至 I_a のセットは、入力ビット w_1 乃至 w_d の隣接領域 (windows) のセットを含むとみなされ、ここで d は 2 乃至 $(a/3)$ の範囲にあり；

隣接番号の (contiguously numbered) 出力ビット O_1 、 O_2 乃至 O_b のセットでは、前記ビット O_b がビット $O_{(b-1)}$ と同様にビット O_1 と隣接するよう扱われ、これにより出力ビット O_1 、 O_2 乃至 O_b がビットの巡回収集とみなされ；

セット s_{b_1} 乃至 s_{b_c} 内の各一次 s ボックス s_{b_k} について：

一次 s ボックス s_{b_k} への入力ビットが、領域 w_k 以外の入力ビットの少なくとも 2 つの領域からの少なくとも 1 のビットを含むことを特徴とする s ボックス。

隣接番号の (contiguously numbered) 出力ビット O_1 、 O_2 乃至 O_b のセットが、出力ビット w_1 乃至 w_d の隣接領域のセットを含むとみなされ；セット s_{b_1} 乃至 s_{b_c} 内の各一次 s ボックス s_{b_k} について；

出力ビット w_k の領域が、前記一次 s ボックス s_{b_k} の出力ビットを含み、前記一次 s ボックス s_{b_k} への入力ビットが、領域 w_k 以外の入力ビットの少なくとも 2 つの領域からの少なくとも 1 のビットを含むことを特徴とする s ボックス。

【請求項 36】

請求項 1 乃至 35 の多入力多出力 s ボックスを少なくとも 2 つ含む構造であって、前記多入力多出力 s ボックスのいずれの対もその入力を共有しないことを特徴とする構造。

【請求項 37】

請求項 1 乃至 41 の多入力多出力 s ボックスを少なくとも 2 つ含む構造であって、少なくとも 1 対の前記多入力多出力 s ボックスが少なくとも 1 の入力を共有することを特徴とする構造。

【請求項 38】

請求項 36 または 37 の構造において、前記多入力多出力 s ボックスの少なくとも 2 つが接続 (pipelined) されていることを特徴とする構造。

【請求項 39】

請求項 36 乃至 38 のいずれか 1 項の構造において、少なくとも 1 の前記多入力多出力 s ボックスへの入力が、別の前記多入力多出力 s ボックスの b 個の出力より少ないか等しいサブセットを含むことを特徴とする構造。

【請求項 40】

請求項 36 乃至 39 のいずれか 1 項の構造において、前記多入力多出力 s ボックスの b 個の出力より少ないか等しいサブセットが、さらに別の前記多入力多出力 s ボックスの入力に用いられる前に処理 (manipulated) されていることを特徴とする構造。

【請求項 41】

請求項 36 乃至 40 のいずれか 1 項の構造において、少なくとも 2 つの前記多入力多出力 s ボックスについて：

一方の s ボックスの入力ビット数他方の s ボックスの入力ビット数と異なるか；

一方の s ボックスの出力ビット数他方の s ボックスの出力ビット数と異なるか、のいずれか 1 以上であることを特徴とする構造。

【請求項 42】

請求項 41 の構造において、前記少なくとも 2 つの多入力多出力 s ボックスの各々の入力ビット数が、1 以外の公約数を持たないことを特徴とする構造。

【請求項 4 3】

請求項 4 1 または 4 2 の構造において、前記少なくとも 2 つの多入力多出力 s ボックスの各々の出力ビット数が、1 以外の公約数を持たないことを特徴とする構造。

【請求項 4 4】

請求項 4 1 乃至 4 3 のいずれか 1 項の構造において、前記少なくとも 2 つの多入力多出力 s ボックスのうちの 1 つの入力ビット数が、前記少なくとも 2 つの多入力多出力 s ボックスのうちの別の入力ビット数より少なくとも 50 % 多いことを特徴とする構造。

【請求項 4 5】

請求項 4 1 乃至 4 3 のいずれか 1 項の構造において、前記少なくとも 2 つの多入力多出力 s ボックスのうちの 1 つからの出力ビット数が、前記少なくとも 2 つの多入力多出力 s ボックスのうちの別の出力ビット数より少なくとも 50 % 多いことを特徴とする構造。

10

【請求項 4 6】

請求項 3 6 乃至 4 5 のいずれか 1 項の構造において、前記少なくとも 2 つの多入力多出力 s ボックスのうちの 1 つの前記一次 s ボックス $s b_1$ 、 $s b_2$ 乃至 $s b_c$ の少なくとも 1 つが、前記少なくとも 2 つの多入力多出力 s ボックスのうちの別の一次 s ボックス $s b_1$ 、 $s b_2$ 乃至 $s b_c$ と異なることを特徴とする構造。

【請求項 4 7】

請求項 1 乃至 4 6 のいずれか 1 項の発明において、少なくとも 1 つの多入力多出力 s ボックスの b 個の出力と同じかこれより少ないサブセットが、別のプロセスへの入力に用いられることを特徴とする発明。

20

【請求項 4 8】

請求項 4 7 の多入力多出力 s ボックスにおいて、少なくとも 1 つの多入力多出力 s ボックスの b 個の出力より少ないか等しいサブセットがさらに、別のプロセスへの入力に用いられる前に処理 (manipulated) されることを特徴とする s ボックス。

【請求項 4 9】

請求項 1 乃至 4 8 のいずれか 1 項の多入力多出力 s ボックスにおいて、前記 c 個の一次 s ボックス $s b_1$ 、 $s b_2$ 乃至 $s b_c$ への入力ビット s_1 、 s_2 乃至 s_c のセットが：

a 個のビットから導出 (drawn) される c 個の添字位置 (index positions) の順序セット (ordered sets) P_1 乃至 P_c を確率的 (probabilistically) に選択するステップであって、各セット P_1 乃至 P_c はそれぞれ要素 s_{1_1} 、 s_{1_2} 乃至 s_{1_c} を有するステップと；

30

各添字位置の順序セット P_1 乃至 P_c について、これらのセットのいずれか 2 つが同じ位置に同じ要素を含む場合に、これら要素の 1 つをセット P_1 乃至 P_c の別のものから確率的に選択された添字位置に交換 (swapping) するステップと；

添字位置の c 個のセット P_1 乃至 P_c のそれぞれについて反復的に：

前記セットが添字位置の別の P_1 乃至 P_c の各セットと共有する要素の数を決定するステップと；

共通の数の任意数 t を持つ添字位置の c 個のセット P_1 乃至 P_c のうちの 2 つの要素 P_i と P_k の各々について、 P_i の $(t+1)/2$ の数を：

c 個のセット P_1 乃至 P_c の残りの $(c-2)$ のセットを、 P_i と共有する要素の数の順番で分類 (sorting) し；

40

前記 $(c-2)$ のセットから、 P_i と共有する要素の数が最も少ない 1 のセット P_m を選択し；

前記セット P_i と P_k に共通の 1 の要素を選択し；

前記選択した要素を前記セット P_m のうちの 1 つと交換 (swapping) することにより、

配置転換するステップと；

を具える実践的プロセス (heuristic process) により選択されることを特徴とする s ボックス。

【請求項 5 0】

50

請求項 1 乃至 49 のいずれか 1 項の発明をシミュレートすることを特徴とするプロセス。

【請求項 51】

請求項 51 のプロセスにおいて、ワードベースの一般目的のプロセッサに実装されることを特徴とするプロセス。

【請求項 52】

請求項 49 乃至 51 のいずれか 1 項のプロセスにおいて、静的ビット置換処理、キー従属ビット置換処理、データ従属ビット置換処理のいずれか 1 以上を含むビット置換処理を実行するバイナリマスキング (binary masking) を用いることを特徴とするプロセス。

【請求項 53】

請求項 52 のプロセスにおいて、ビット置換処理を実行するバイナリマスキングを用い、これらのビット置換処理が：

前記セット s_1 、 s_2 乃至 s_c の要素を選択するステップと；

前記 c 個のブール関数の出力を置換するステップとのいずれか 1 以上を実現し；

前記バイナリマスキングが；

静的ビット置換処理と；キー従属置換処理と；データ従属置換処理とのいずれか 1 以上を実行すべく用いられることを特徴とするプロセス。

【請求項 54】

請求項 53 のプロセスにおいて、前記ビット置換処理がハードウェアに補助されることを特徴とするプロセス。

【請求項 55】

請求項 54 のプロセスにおいて、前記ハードウェアに補助されたビット置換処理が、グループオペレーション (GRP)、その逆、オメガフリップネットワーク (OMFLIP)、PPERM、CROSS、BFLY 処理からなる群から選択されることを特徴とするプロセス。

【請求項 56】

請求項 50 乃至 53 のいずれか 1 項のプロセスにおいて、ハードウェア補助ビットローテーション処理 (hardware-assisted bitwise rotation operations) を用いて、前記ビット置換処理を実行することを特徴とするプロセス。

【請求項 57】

請求項 50 乃至 53 のいずれか 1 項のプロセスにおいて、ハードウェア補助ビットシフティング処理 (hardware-assisted bitwise shifting operations) を用いて、前記ビット置換処理を実行することを特徴とするプロセス。

【請求項 58】

請求項 50 乃至 53 のいずれか 1 項のプロセスにおいて、ハードウェア補助バイトスワッピング処理 (hardware-assisted byte swapping operations) を用いて、前記ビット置換処理を実行することを特徴とするプロセス。

【請求項 59】

請求項 50 乃至 58 のいずれか 1 項のプロセスにおいて、ルックアップテーブルを用いて換字 (substitution) およびビット置換処理の少なくとも 1 を実行することを特徴とするプロセス。

【請求項 60】

請求項 50 乃至 59 のいずれか 1 項のプロセスにおいて、少なくとも 1 のワードベースの基本ブール関数 (word-based primitive Boolean function) を用いて換字処理 (substitution operation) を実行することを特徴とするプロセス。

【請求項 61】

ブロック暗号、ストリーム暗号、疑似乱数生成器、またはハッシュ関数のラウンド関数を具える回路であって、この暗号回路が、請求項 1 乃至 49 のいずれか 1 項の多入力多出力 s ボックスのうちの少なくとも 1 つを具え、前記回路には、前記 1 以上の他入力多出力 s ボックスの入出力間でゼロ乃至 6 以下の範囲の繰り越し操作の破られていない演算繰り

10

20

30

40

50

越し理論チェーン (unbroken arithmetic carry-logic chain) があることを特徴とする回路。

【請求項 62】

暗号プロセスであって、

a 個の隣接番号の (contiguously numbered) 入力ビット I_1 、 I_2 乃至 I_a を受信し、ここで a は少なくとも 4 であり、

b 個の連続番号の出力ビット O_1 、 O_2 乃至 O_b を出力し、

前記方法が：

c 個の一次 s ボックス操作 (primitive s-box operations) s_{b_1} 、 s_{b_2} 乃至 s_{b_c} を含み、その各々が：

多入力単一出力のブール関数 f_1 、 f_2 乃至 f_c を含み、これらが多入力と単一出力の関係を規定しており、

入力ビット s_1 、 s_2 乃至 s_c のセットをそれぞれ受信し、これらのセットがそれぞれ暗号化関数 (the cryptographic function) への a 個の入力ビットから選択され、それぞれ s_{l_1} 、 s_{l_2} 乃至 s_{l_c} ビットを含み、これにより：

前記 s_{l_1} 、 s_{l_2} 乃至 s_{l_c} の数が 3 乃至 $(a-1)$ の範囲内にあり；

前記 s_{l_1} 、 s_{l_2} 乃至 s_{l_c} の数の合計が a より大きく、

前記暗号化関数の b 個の出力ビットが、前記 c 個のブール関数の出力を含むことを特徴とするプロセス。

【請求項 63】

請求項 62 の暗号プロセスにおいて、前記 s ボックスの b 個の出力ビットが前記 c 個の一次 s ボックス処理の出力であることを特徴とするプロセス。

【請求項 64】

請求項 62 または 63 の暗号プロセスにおいて、a が 16 以上であることを特徴とするプロセス。

【請求項 65】

請求項 62 乃至 64 のいずれか 1 項の暗号プロセスにおいて、b が 16 以上であることを特徴とするプロセス。

【請求項 66】

請求項 62 乃至 65 のいずれか 1 項の暗号プロセスにおいて、c が 12 以上 b 以下であることを特徴とするプロセス。

【請求項 67】

請求項 62 乃至 66 のいずれか 1 項の暗号プロセスにおいて、それぞれ 1 から a の i と j について、 s_i と s_j の各セットが $\min(s_{l_i}, s_{l_j}) - 1$ ビット以下を共有することを特徴とするプロセス。

【請求項 68】

請求項 62 乃至 67 のいずれか 1 項の暗号プロセスにおいて、前記数 s_{l_1} 、 s_{l_2} 乃至 s_{l_c} の合計が a の 1.5 倍より大きいあるいは等しいことを特徴とするプロセス。

【請求項 69】

請求項 62 乃至 68 のいずれか 1 項の暗号プロセスにおいて、a、b、c の少なくとも 1 つが素数であることを特徴とするプロセス。

【請求項 70】

請求項 62 乃至 69 のいずれか 1 項の暗号プロセスにおいて、前記数 a と b が 1 より大きな公約数を持たないことを特徴とするプロセス。

【請求項 71】

請求項 62 乃至 70 のいずれか 1 項の暗号プロセスにおいて、前記数 s_{l_1} 、 s_{l_2} 乃至 s_{l_c} の少なくとも 2 つが同じであることを特徴とするプロセス。

【請求項 72】

請求項 71 の暗号プロセスにおいて、前記数 s_{l_1} 、 s_{l_2} 乃至 s_{l_c} の全部が同じであることを特徴とするプロセス。

【請求項 7 3】

請求項 6 2 乃至 7 2 のいずれか 1 項の暗号プロセスにおいて、入力ビットセット s_1 、 s_2 乃至 s_c がそれぞれ、確率的プロセス (provabilistic) を用いて選択されることを特徴とするプロセス。

【請求項 7 4】

請求項 6 2 乃至 7 3 のいずれか 1 項の暗号プロセスにおいて、前記入力ビットセット s_1 、 s_2 乃至 s_c の少なくとも 1 つを選択するのに用いられるプロセスがキード (keyed) されていることを特徴とするプロセス。

【請求項 7 5】

請求項 7 3 または 7 4 の暗号プロセスにおいて、前記入力ビットセット s_1 、 s_2 乃至 s_c の選択は、少なくとも 1 の基準 (criterion) を満たすよう実践的に改良 (heuristically refined) されていることを特徴とするプロセス。 10

【請求項 7 6】

請求項 6 2 乃至 7 5 のいずれか 1 項の暗号プロセスにおいて、前記ブール関数 f_1 、 f_2 乃至 f_c は確率的プロセス (provabilistic) を用いて生成されることを特徴とするプロセス。

【請求項 7 7】

請求項 6 2 乃至 7 6 のいずれか 1 項の暗号プロセスにおいて、前記ブール関数 f_1 、 f_2 乃至 f_c の少なくとも 1 つを生成するのに用いられるプロセスがキード (keyed) されていることを特徴とするプロセス。 20

【請求項 7 8】

請求項 7 6 または 7 7 の暗号プロセスにおいて、前記少なくとも 1 のブール関数 f_1 、 f_2 乃至 f_c の選択は、少なくとも 1 の基準 (criterion) を満たすよう実践的に改良 (heuristically refined) されていることを特徴とするプロセス。

【請求項 7 9】

請求項 6 2 乃至 7 8 のいずれか 1 項の暗号プロセスにおいて、前記ブール関数 f_1 、 f_2 乃至 f_c の少なくとも 1 つは平衡したブール関数 (ballanced Boolean function) であることを特徴とするプロセス。

【請求項 8 0】

請求項 7 9 の暗号プロセスにおいて、前記ブール関数 f_1 、 f_2 乃至 f_c がそれぞれ平衡したブール関数 (ballanced Boolean function) であることを特徴とするプロセス。 30

【請求項 8 1】

請求項 6 2 乃至 8 0 のいずれか 1 項の暗号プロセスにおいて、前記関数 f_1 、 f_2 乃至 f_c の少なくとも 1 つが、2 対 1 マルチプレクサ関数 (two-to-one multiplexer function) を具えることを特徴とするプロセス。

【請求項 8 2】

請求項 8 1 の暗号プロセスにおいて、前記関数 f_1 、 f_2 乃至 f_c がそれぞれ 2 対 1 マルチプレクサ関数 (two-to-one multiplexer function) を具えることを特徴とするプロセス。

【請求項 8 3】

請求項 6 2 乃至 8 2 のいずれか 1 項の暗号プロセスにおいて、前記関数 f_1 、 f_2 乃至 f_c の少なくとも 1 つがユニークなブール関数であることを特徴とするプロセス。 40

【請求項 8 4】

請求項 8 3 の暗号プロセスにおいて、前記関数 f_1 、 f_2 乃至 f_c がそれぞれユニークなブール関数であることを特徴とするプロセス。

【請求項 8 5】

請求項 8 3 または 8 4 の暗号プロセスにおいて、前記関数 f_1 、 f_2 乃至 f_c 間の差 (difference) がアフィン (affine) であることを特徴とするプロセス。

【請求項 8 6】

請求項 6 2 乃至 8 5 のいずれか 1 項の暗号プロセスにおいて、実行時に再構成される (50

reconfigured) ことを特徴とするプロセス。

【請求項 87】

請求項 62 乃至 86 のいずれか 1 項の暗号プロセスにおいて、前記入力ビットセット s_1 乃至 s_c の少なくとも 1 つが実行時に変更されることを特徴とするプロセス。

【請求項 88】

請求項 62 乃至 87 のいずれか 1 項の暗号プロセスにおいて、前記関数 f_1 、 f_2 乃至 f_c の少なくとも 1 つが実行時に再構成されることを特徴とするプロセス。

【請求項 89】

請求項 62 乃至 88 のいずれか 1 項の暗号プロセスにおいて、 $(c - a)$ 乃至 a のすべての i について：

10

各一次 s ボックス処理 $s b_i$ への $s l_i$ の入力ビットのセットが、入力ビット I_1 乃至 I_i から選択され；

入力ビット I_i と出力ビットの関係が線形であることを特徴とするプロセス。

【請求項 90】

請求項 89 の暗号プロセスにおいて、 I_1 乃至 I_a の a 個のビットセットの $T = (a - c)$ ビットのサブセットが、ビット I_1 乃至 I_T の $T \times T$ の全単射 (bijective mapping) の入力であることを特徴とするプロセス。

【請求項 91】

請求項 62 乃至 90 のいずれか 1 項の暗号プロセスにおいて、 W が一定である場合の $(W + 1)$ 乃至 a のすべての i について：

20

前記一次 s ボックス処理 $s b_i$ への $s l_i$ の入力ビットのセットが、入力ビット $I_{(i - w)}$ 乃至 I_i から選択され；

入力ビット I_i と前記 s ボックス $s b_i$ の出力ビットの関係が線形であることを特徴とするプロセス。

【請求項 92】

請求項 91 のいずれか 1 項の暗号プロセスにおいて、 W が 2 乃至 $(a - 1)$ の範囲にあることを特徴とするプロセス。

【請求項 93】

請求項 91 または 92 の暗号プロセスにおいて、 I_1 乃至 I_w の W ビットが、 $W \times W$ の全単射の入力であることを特徴とするプロセス。

30

【請求項 94】

請求項 62 乃至 88 のいずれか 1 項の暗号プロセスにおいて、入力ビット s_1 、 s_2 乃至 s_c のセットの入力ビットの $s l_1$ 、 $s l_2$ 乃至 $s l_c$ の選択はそれぞれ：

隣接番号の (contiguously numbered) 入力ビット I_1 、 I_2 乃至 I_a では、ビット I_a がビット $I_{(a - 1)}$ と同様にビット I_1 と隣接 (contiguous) するよう扱われ、これにより入力ビット I_1 、 I_2 乃至 I_a がビットの巡回収集 (circular collection) とみなされ；

前記隣接番号の入力ビット I_1 、 I_2 乃至 I_a のセットは、ビット w_1 乃至 w_d の領域 (windows) のセットを含むとみなされ、ここで d は 3 乃至 $(c / 3)$ の範囲にあり：

各領域 (window) が最初と最後の領域境界を有し、各領域境界が、一次 s ボックス $s b_i$ と $s b_{i + 1}$ 間の同じ方向に 1 ビット位置ずつ増大し；

40

隣接番号の (contiguously numbered) 出力ビット O_1 、 O_2 乃至 O_b のセットでは、前記ビット O_b がビット $O_{b - 1}$ と同様にビット O_1 と隣接するよう扱われ、これにより出力ビット O_1 、 O_2 乃至 O_b がビットの巡回収集とみなされ；

セット $s b_1$ 乃至 $s b_c$ 内の各一次 s ボックス $s b_k$ について：

一次 s ボックス $s b_k$ への入力ビットが、領域 w_k 以外の入力ビットの少なくとも 2 つの領域からの少なくとも 1 のビットを含むことを特徴とするプロセス。

【請求項 95】

請求項 94 の暗号プロセスにおいて、各一次ボックス $s b_i$ について、領域 w_1 乃至 w_d の少なくとも 2 つのサイズが異なることを特徴とするプロセス。

50

【請求項 96】

請求項 62 乃至 88 のいずれか 1 項の暗号プロセスにおいて、入力ビット s_1 、 s_2 乃至 s_c のセットの入力ビットの s_{l_1} 、 s_{l_2} 乃至 s_{l_c} の選択はそれぞれ：

隣接番号の (contiguously numbered) 入力ビット I_1 、 I_2 乃至 I_a では、ビット I_a がビット I_{a-1} と同様にビット I_1 と隣接 (contiguous) するよう扱われ、これにより入力ビット I_1 、 I_2 乃至 I_a がビットの巡回収集 (circular collection) とみなされ；

前記隣接番号の入力ビット I_1 、 I_2 乃至 I_a のセットは、入力ビット w_1 乃至 w_d の隣接領域 (windows) のセットを含むとみなされ、ここで d は 2 乃至 $(a/3)$ の範囲にあり；

隣接番号の (contiguously numbered) 出力ビット O_1 、 O_2 乃至 O_b のセットでは、前記ビット O_b がビット $O_{(b-1)}$ と同様にビット O_1 と隣接するよう扱われ、これにより出力ビット O_1 、 O_2 乃至 O_b がビットの巡回収集とみなされ；

セット s_{b_1} 乃至 s_{b_c} 内の各一次 s ボックス s_{b_k} について：

一次 s ボックス s_{b_k} への入力ビットが、領域 w_k 以外の入力ビットの少なくとも 2 つの領域からの少なくとも 1 のビットを含むことを特徴とする s ボックス。

隣接番号の (contiguously numbered) 出力ビット O_1 、 O_2 乃至 O_b のセットが、出力ビット w_1 乃至 w_d の隣接領域のセットを含むとみなされ；セット s_{b_1} 乃至 s_{b_c} 内の各一次 s ボックス s_{b_k} について：

出力ビット w_k の領域が、前記一次 s ボックス s_{b_k} の出力ビットを含み、前記一次 s ボックス s_{b_k} への入力ビットが、領域 w_k 以外の入力ビットの少なくとも 2 つの領域からの少なくとも 1 のビットを含むことを特徴とするプロセス。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、換字ボックス (substitution box) の構成に関し、ある実施例はハードウェアとして有効であり、ある実施例はソフトウェアとして有効である。

【背景技術】

【0002】

本出願は、2004 年 9 月 24 日出願のオーストラリア暫定特許出願 2004905507、2004 年 11 月 16 日出願の 2004906543、2004 年 12 月 30 日出願の 2004907361、2004 年 12 月 31 日出願の 2004907374、2005 年 4 月 29 日出願の 2005902136 の優先権を主張するものであり、これらの内容は参照としてここに組み込まれている。

【0003】

本明細書において、クレームも含み、「具える」または「具えている」の語は明確に規定された特徴、整数、ステップ、構成要素の存在を特定するのに用いるものであり、他の 1 以上の特徴、整数、ステップ、構成要素の存在または追加を排除するものではなく；またビット i の「添字位置 (index position)」 P_i は、隣接入力ビットセット a 内のビット i の位置を示すのに用いる。

【0004】

本明細書において、「確率的プロセス」の語は、「乱数」および「疑似乱数」プロセスの双方に用い、これには疑似乱数プロセスが定数またはキー要素で「キード (kyed)」または「シード (seeded)」されている場合や、ランダム性のソースや疑似乱数アルゴリズムが取得可能 (available) な場合を含む。様々な公知の疑似乱数生成器やストリーム暗号をこの目的に利用することができる。

【0005】

本明細書において、公開された文献への参照は、その文献の内容が本明細書の熟練した読者に共有の一般知識の部分となすと容認するものではない。

【0006】

10

20

30

40

50

我々の創作的な特徴をより容易に認識可能とすべく、我々はこの技術に関連するこれまでに公開されたいくつかの文献の概要を以下に明らかにする。

【0007】

錯乱 (confusion) と拡散 (diffusion) の定義は、1949年にC. E. Shannonにより彼の文献「Communication Theory of Secrecy Systems」で初めて公に紹介された。

【0008】

sボックス (substitution box: 換字ボックス) はデジタル符号化された入力を受け、この入力を異なるデジタル符号化された出力に変換し、すなわち錯乱を生じさせる。pボックス (permutation box: 置換ボックス) はデジタル符号化された入力を受け、同じビットを出力として返し、これらの値を変更しないがその順番を変え、すなわち拡散を生じさせる。

10

【0009】

「雪崩効果」は、最も単純な形では、入力の単一ビット順列 (single bit change) にラウンド関数 (round function) で少なくとも2ビット順列の出力とする暗号特性である。これはsボックスに必要な特性として、Horst Feistelにより、1973年5月のScientific American, Vol. 228, Number 5において公開された彼の暗号特性を記載した「Cryptography and Computer Privacy」にて紹介された。この刊行物は、完全な任意対任意の換字 (any-to-any substitution) は 128×128 といった大きなsボックスでは技術の限界により達成できないことを記している。結果として、非常に小さく実用的なサイズ (4×4) の非線形sボックスが部分的な錯乱と部分的な拡散を実行すべく選択され、大きなpボックスがsボックスの出力に接続されShannonが規定するようにさらなる拡散を実行すべく選択される。

20

【0010】

最初のデジタルブロック暗号は広くHorst Feistelにより達成された。このブロック暗号は、1974年3月19日に発行された米国特許3,798,359 (Feistel) にあるように、小さな 4×4 のsボックスと、64または128ビットに行われる置換処理を組み合わせている。この 4×4 のsボックスは、組み合わせ理論 (combinatorial logic) を用いるよう設計されている。

【0011】

sボックスとpボックスは、殆どのフェイステル型またはフェイステルネットワーク暗号および他の暗号原理 (cryptographic primitive) の要素として利用されている。これらは1976年5月18日に公開された米国特許3,958,081 (Ehrsam, et al.) に開示された公開データ暗号化標準 (DES) にも利用されている。このDES暗号は、1977年に米国連邦規格となった。ここで注目すべきは、その時点で公に知られていない重要な暗号基準を保護しつつ、組み合わせ理論を用いたハードウェア実装を確たる有効なものにすべく、 6×4 のsボックスが慎重に選択されていることである。

30

【0012】

sボックスの換字処理は、概して演算的ではない。例えば、限定しないが加算、乗算、累乗といった演算処理は、しばしば非演算的sボックス (non-arithmetic s-box) の代わりに、またはこれとともに利用される。このような演算処理と非演算的sボックスの組合せに基づく換字-置換ネットワーク (substitution-permutation networks) は、ワードベースの処理構造に有効である。この種の構造の一例が、1981年3月10日に公開された米国特許4,255,811 (Adler) に記載されており、 2^n を法とする加算または減算、nビット幅XOR、静的nビット置換 (static n-bit permutations)、nビットキー従属ローテーション操作 (n-bit key-dependent rotation operations) を用いる暗号が開示されている。同種のさらなる構成が、1991年1月1日に公開された米国特許4,982,429 (Takaragi, et al.)、1992年4月7日に公開された5,103,479 (Takaragi, et al.) に開示されている。ワードベースの非線形演算処理が、例えばRon Rivestによる1992年4月のRecommendation for Comment 1321に記載されたMD5暗号ハッシュ関数といった暗号ハッシュ関数に用いられている。

40

50

【0013】

pボックス（置換ボックス）についての意味深い研究はなく、これは設計者の判断に委ねられ、多くの場合は完全に線形または無作為に選択される。

【0014】

フェイステルネットワーク暗号はまた、その構造内で殆どの場合に線形で、拡散（diffusion）に寄与する関数の組合せを含む。線形コンバイナ（XOR）を拡散率の高い非線形演算処理に置き換える一例に、ソヴィエト国家基準局；情報処理システム；暗号保護；暗号アルゴリズム推奨のGOSTと呼ばれるものがある。1989年GOST 28147-89。このGOST暗号は、ワードベースのローテーション操作（rotation operation）を用いてsボックス間でビットの拡散を実現させた暗号の例でもある。

10

【0015】

「完成基準」（completeness criterion）は、最初に文献「Structured Design of Substitution-Permutation Encryption Networks」、IEEE Transactions of Computers、Vol. 28, No. 10, 747、1979年、John B. KamとGeorge I. Davida、により明確に規定された。暗号変換は、各暗号文ビットが平文ビットに従属する場合に「完成」する。この完成基準を満たす暗号が、1981年6月23日公開の米国特許4,275,265（Davida, et al.）に見られる。この完成基準は、例えばNインスタンスのM入力対単一出力のブール関数がそれぞれM入力ビットの完全なセットを入力とする $M \times N$ のsボックスを必要とする。

【0016】

20

1982年の文献「Are Big S-Boxes Best」において、J. Gordon とH. Retkinは、コンテンツがすべての考え得る出力のセットの無作為の置換として選択される場合にsボックスの暗号特性を探索している。この文献は、最初の役割が、エントリ数が十分に多い場合にはこのように無作為に選択したsボックスで様々な望ましい暗号特性が発見されることを示すことを含んでいる。例えば、 $1/2^{64}$ の無作為に生成される可逆の 6×6 sボックスは、活用可能な線形性を有する。

【0017】

1982年のF. Ayoubによる文献「Probabilistic completeness of substitution-permutation encryption networks」、IEEE Proceedings, 129(5):195-199には、その時点で最新の研究が、特定の状況下において、計画的なトラップドアからの開放の証明として、ランダム選択により換字関数（substitution function）を設計しうることを示している。この文献はまた、置換もまた例えばユーザキーで無作為に選択しうることを開示しており、得られるネットワークは、非常に高い確立で、完成された特性を有する。

30

【0018】

我々の $M \times 1$ のsボックスへのブール関数のランダム選択を許可する場合に、上記2文献を参照する。

【0019】

カナダ、オンタリオ、キングストン、クイーンズ大学電気工学部のA. F. Webster とS. E. Tavaresの修士論文「On the Design of S-Boxes」、LNCS no. 219, pp523-534 (1986)において、筆者は「厳格な雪崩基準（strict avalanche criterion: SAC）」を明示的に規定している。このSACは、各暗号文出力ビットが、単一の入力ビットが補足された場合にも正確に $1/2$ の確立で変換されるべきであることを述べている。

40

【0020】

この論文は、この実践的なプロセスが、SACとさらなる「雪崩変動独立（avalanche variable independence）」特性とを満足する 4×4 のsボックスの選択に用いられることを記載している。このプロセスは、SACを満たす潜在的に可逆のすべての 4×1 関数を選択し、一度にこれらを4つ組み合わせて 4×4 の換字ボックスを生成することで開始する。この論文にはさらなる実践的な技術が記載されており、前のステップで作成された「完全な」sボックスの有限数の集合（families）から 4×1 のブール関数を選択することによりサーチプロセスを最適化する。

50

【0021】

この論文は、米国特許 4, 275, 265 (DAVIDA, et al.) 記載の暗号がいかにか S A C に合致しないかを強調し、他の研究者にそれまで認識された D E S の潜在的な弱点を確認している。また、S A C を満足しない構成を、数ラウンドにわたり構築を繰り返すことにより、S A C を満足する構成に変換しうることを強調している。これは、構築が換字置換ネットワークである場合であって置換の電送 (wiring) が無作為である場合に実現するようである。

【0022】

s ボックスの完全な非線形の基準は、1989年に文献「Nonlinearity Criteria for Cryptographic Functions」、Advances in Cryptology-- EUROCRYPT '89、549-562、筆者 Meier とStaffelbachで初めて記載された。この筆者は、完全な非線形基準は拡散に作用し、事実上 S A C の要求よりも厳しい。

【0023】

1992年の文献「On immunity against Biham and Shamir's Differential Cryptanalysis」、Information Processing Letters、vol. 41、1992年2月14日、pp77-80、Carlisle M. Adamsには、差分暗号解読を免除した実用的なサイズの s ボックスの作成方法が記載されている。

【0024】

1998年8月18日に公開された米国特許 5, 796, 837 (Kim, et al.) は、線形および差分暗号解読を免除した実用的なサイズの $M \times N$ の s ボックスの作成方法を開示している。2000年2月29日に公開された米国特許 6, 031, 911 (Adams, et al.) は、S A C および他の基準を増分プロセス (incremental process) で迅速に満たす $M \times N$ の s ボックスを生成する発見的な技術を開示している (上述した A. F. Webster と S. E. Tavares の論文「On the Design of S-Boxes」と同様の技術である)。

【0025】

公開された案件の前述の分析から、非演算的な s ボックスの研究および非演算的 s ボックスの作成の一般的な方向性は3つの学派に分かれており、すなわち、適度に大きな s ボックスを選択しすべての可能な出力を無作為に置換するもの、強固として知られる s ボックスからキー従属 s ボックス (key-dependent s-boxes) を作成するもの、所望の暗号特性を固定の s ボックスに保証する新規で厳格な発見的基準を見つけ出すものである。いずれの場合にも、これらの非演算的な s ボックスを作成する3つの学派は、s ボックスが最低限完成した基準を高い確率で保証すべきことに同意している。

【0026】

以下が非演算的な s ボックスに関する特性である：

- s ボックス構築用の均衡のとれたブール関数を実用無作為に選択可能である；
- 無作為に均衡のとれたブール関数から $M \times N$ の s ボックスを構築可能であり、発見的 (heuristic) で改良されており S A C を充足する；
- $M \times N$ の s ボックスを、固定的な初期の置換 (fixed initial permutation) により選択可能である；
- 暗号換字置換 (S P) ネットワークの単一ラウンドを、この S P ネットワーク自体は S A C を満足しなくても、各々独立して S A C を満足する1以上のユニークな $M \times N$ の s ボックスから構築可能である；
- 上述の暗号 S P ネットワークの単一ラウンドが S A C を満たさないが、完全な S P ネットワークが2またはそれ以上の繰り返しラウンドの後に S A C を満たす；

【0027】

いずれの場合にも、例えば得られる最高の非線形、得られる最高の代数的階級 (algebraic degree)、得られる最速の雪崩といった理想の特性を有する小さく実用的なサイズの s ボックスを選択して、換字—置換ネットワークを技術的に不可能な大きく強固な s ボックスに近似させる。

【0028】

ソフトウェアまたはワードベースのプロセッサ構造において、基本のブール理論作用（AND、MOV—move/copy、NAND、NOR、NOT、OR、XNOR、XOR等）は、厳密に構成されたパラレルNビット幅の入力に対して実行される単一命令多重データ（single-instruction-multiple-data：SIMD）操作の形式である。例えば、IBMのPowerPCまたはIntel×86構造といった通常目的の32ビットプロセッサを考えると、ブールのAND命令は32の個別のビット毎にAND操作を、32ビット幅のレジスタブロックに供給される64ビットの入力に対して行い、32ビットの出力を出す。

【0029】

M×NのsボックスとM×1のブール関数を、ルックアップテーブルとして、または適切な基本SIMD操作の選択および構成を通じて、ソフトウェアに実装する。2対1マルチプレクサに有効な32協働ソフトウェア（32 concurrent software）の暗号実装を用いるSIMD操作の一例が、暗号ハッシュ機能MD5にみられる。

【0030】

SIMD命令の最も明瞭な特徴は、その完全な平行性にある：各入力レジスタの各ビットは出力の同じ位置のビットにのみ作用し—各入力レジスタの最小桁のビットは出力の最小桁のビットにのみ作用し、各入力レジスタの最上位のビットは出力の最上位のビットにのみ作用する等である。このような作用は、固定または可変のローテーション（fixed or variable rotation）を用いずに繰り返しまたは互いにグループ化する場合に、バイトのスワッピングまたは他の（固定または可変の）置換、換字または演算操作は、各出力ビットがNビット幅の各入力レジスタの1より多いビットに作用するのを許可しない。このため、暗号化アプリケーションに必須の各入力レジスタの異なるビット間で拡散を生じるには、固定または可変のローテーション、バイトのスワッピングまたは他の（固定または可変の）ビットの置換、ビットの換字、または演算操作が必要である。

【0031】

以下の技術が、ビットの拡散を導くのに必要なビット毎の置換操作を実行するワードベース構造に使用されている：

- 通常ルックアップテーブルとして実装されsボックスに組み合わせられる、pボックス；
- 1989年公開のGOST基準28147—89にみられる固定のビットローテーション操作；
- 上記米国特許4, 255, 811（Adler）に記載のキー従属ビットローテーション操作；
- 1979年公開の米国特許4, 157, 454に記載のデータ従属ローテーション操作；
- 1989年12月19日公開の米国特許4, 888, 798（Earnest）に記載された、ビットローテーション操作と組み合わせた、および例えばOR、XOR、ADD操作と組み合わせた、ビット毎のマスキングAND操作；
- 「On permutation operations in cipher design」、Ruby B. Lee, Z. J. Shi, Y. L. Yin, Ronald L. Rivest, M. J. B. Robshaw、で提唱されているグループ操作や、例えば文献「Efficient permutation instructions for fast software cryptography」、IEEE Micro, 21(6): 56-69、2001年12月、R. B. Lee et al. に記載されたPPERMやCROSS操作、または「Arbitrary bit permutations in one or two cycles」、Proceedings of the 15th International Conference on Application Specific Systems, Architectures and Processors, 237-247頁、2003年7月、Z. Shi et al.、にあるような置換命令；
- 1989年公開のGOST基準28147—89にみられるワードベースの演算操作（ADD、SUB、MUL、DIV）；
- あまり一般的でないバイトスワッピング、ワードスワッピング、ビット順序反転操作；

【0032】

10

20

30

40

50

上記特許に開示されている静的なビット毎の置換と展開操作 (expansion operations) は、その提案または目的に拘わらず、ソフトウェアの実装さらなる論理回路を用いることなく、直接ハードウェアに実装されている。動的なビット毎の置換操作は s ボックスと、演算操作と、データ従属およびキー従属ローテーション (任意選択キーとして) とを含み、置換はハードウェア内でブール関数を使用したりルックアップテーブルとして実装される。

【0033】

Eli Biham により 1997 年に公開された文献 A Fast New DES Implementation in Software に記載されたビットのスライシングは、基本的な AND、OR、XOR、NOT ブール理論関数と移動演算のみを用いて並行に実行される複合暗号インスタンスが得られる。上記にみられるように、ビットのスライシングは 32 または 64 の異なる暗号インスタンス間での相互関係を生成するものではない。ビットスライシングは、単一のプロセッサレジスタ内のビット置換の代わりに、異なる N ビット幅レジスタを直接参照して迅速な平行化されたソフトウェア実装を実現する。ビットスライシングにより単一の暗号を実行する連続的な実行待ち時間が増大するが、実行量が低減する。

【0034】

実践的なアルゴリズム (ときに近時アルゴリズムと呼ばれる) は、さもなくば多項式アルゴリズムが与えられない問題 (intractable problem) の良好な解答を迅速に導く確率的アルゴリズム (probabilistic algorithms) である。このような解答は最適であったりなかったりするが、良好な解答を見つれたり与えられた回答を導いたりすることが事実上コンピュータで実行不能な、多項式アルゴリズムが与えられない問題に許容しうると考えられる。以下のいずれかの実践的なアルゴリズムを、乱数または疑似乱数的に選択された電送置換 (wiring permutations) を改善するために、また品質基準として用いられる暗号基準により判断される本発明の好適な実施例で用いられるブール関数に適用可能である：遺伝的アルゴリズム、グリーディアルゴリズム (Greedy algorithms)、ランダムサーチ、タブーサーチ (Tabu search)、ヒルクライミング、アントコロニー最適化 (Ant Colony Optimization)、疑似アニーリング (Simulated Annealing)、またはこれらの混成および並列の変異体 (parallel variant)。適切なアルゴリズムが以下に記載されている：

Approximation Algorithms、Vijay V. Vazirani、Springer-Verlag、ハイデルベルグ、2001 年、ISBN: 3-540-65367-8 30

Approximation Algorithms for NP-hard Problems、D. S. Hochbaum、PWS 出版社、ボストン、1996 年、ISBN: 0-534-94968-1

Automated Cryptanalysis of Substitution Ciphers、W. S. Forsyth と R. Safavi-Naini、Cryptologia vol XVII, No. 4 にて公開、1993 年、407-418 頁

Automated Cryptanalysis of Transposition Ciphers、J. P. Giddy と R. Safavi-Naini、The Computer Journal vol XVII, No. 4、1994 年

Two-Stage Optimisation in the Design of Boolean Functions、John Andrew Clark と Jeremy Jacob、Lecture Notes in Computer Science 1841 春号、2000 年、ISBN: 3-540-67742-9、242-254 頁 40

【発明の開示】

【課題を解決するための手段】

【0035】

これに対し、本発明の一態様は、多入力多出力の s ボックスであって、
a 個の隣接番号の (contiguously numbered) 入力ビット I_1 、 I_2 乃至 I_a を受信し、
ここで a は少なくとも 4 であり、
b 個の連続番号の出力ビット O_1 、 O_2 乃至 O_b を出力するよう構成され、
この s ボックスが：
c 個の一次 s ボックス s_{b_1} 、 s_{b_2} 乃至 s_{b_c} を含み、それぞれ：
多入力単一出力のブール関数 f_1 、 f_2 乃至 f_c を含み、これらが多入力と単一出力の

関係を規定しており、

入力ビットセット s_1 、 s_2 乃至 s_c をそれぞれ受信するよう構成され、これらのセットがそれぞれ前記 s ボックスへの a 個の入力ビットから選択され、それぞれ s_{l_1} 、 s_{l_2} 乃至 s_{l_c} ビットを含み、これにより：

前記 s_{l_1} 、 s_{l_2} 乃至 s_{l_c} の数が 3 乃至 $(a-1)$ の範囲内にあり；

前記 s_{l_1} 、 s_{l_2} 乃至 s_{l_c} の数の合計が a より大きく、

前記 s ボックスの b 個の出力ビットが、前記 c 個のブール関数の出力を含むことを特徴とする。

【0036】

別の態様によると、本発明は以下の暗号方法を提供する：

a 個の隣接番号の (contiguously numbered) 入力ビット I_1 、 I_2 乃至 I_a を受信し、ここで a は少なくとも 4 であり、

b 個の連続番号の出力ビット O_1 、 O_2 乃至 O_b を出力し、

前記方法が：

c 個の一次 s ボックス操作 (primitive s-box operations) s_{b_1} 、 s_{b_2} 乃至 s_{b_c} を含み、それぞれ：

多入力単一出力のブール関数 f_1 、 f_2 乃至 f_c を含み、これらが多入力と単一出力の関係を規定しており、

入力ビットセット s_1 、 s_2 乃至 s_c をそれぞれ受信し、これらのセットがそれぞれ暗号化関数 (the cryptographic function) への a 個の入力ビットから選択され、それぞれ s_{l_1} 、 s_{l_2} 乃至 s_{l_c} ビットを含み、これにより：

前記 s_{l_1} 、 s_{l_2} 乃至 s_{l_c} の数が 3 乃至 $(a-1)$ の範囲内にあり；

前記 s_{l_1} 、 s_{l_2} 乃至 s_{l_c} の数の合計が a より大きく、

前記暗号関数の b 個の出力ビットが、前記 c 個のブール関数の出力を含むことを特徴とする。

【発明を実施するための最良の形態】

【0037】

図 1 は、本発明の好適な実施例にかかあるキー・データ従属置換ネットワーク暗号 (key-and-data-dependent substitution-permutation network cipher) の一部を図示するものである。図 1 は、直接的に回路としてハードウェア的に実現してもよいし、以下に示すようにワードベース構造にシミュレートしてもよい。

【0038】

図 1 に示す実施例の入力 100 は、5 つのビット 101、102、103、104、105 からなる。関数 (function) 110 が、入力ビットを置換する役割も果たす 3 つの要素により、入力 100 の静的な展開 (static expansion) を示している。ファンクション 120 は、 3×1 の s ボックスのインスタンスを具え、図 1 にはこれらの 3 つ (121、122、123) のみを示す。出力 130 は、5 つのビット 131、132、133、134、135 からなる。 3×1 の s ボックス 123 は、入力 100 から 3 つの入力のユニークなセット、すなわちビット 105 とサイクリックな次の 2 ビット 104 と 103 とを取り、単一の出力ビット 135 を生成する。 3×1 の s ボックス 122 は、入力 100 から 3 つの入力のユニークなセット、すなわちビット 104 とサイクリック名次の 2 ビット 103 と 102 とを取り、単一の出力ビット 134 を生成する。 3×1 の s ボックス 121 は、入力 100 から 3 つの入力のユニークなセット、すなわちビット 103 とサイクリックな次の 2 ビット 105 と 104 とを取り、単一の出力ビット 131 を生成する。各出力ビット 130 は 3×1 の s ボックスにより生成され、各 s ボックスは入力 100 からの 3 つの入力ビットのセットを受け、ここで 3 つの入力ビットの 5 つのセットはそれぞれ、他の 3 つの入力ビットの 5 つのセットと 2 ビットより多くを共有しない。

【0039】

それぞれ別個に、符号 120 で示されている複数の s ボックス関数は、非線形 3 入力 1 出力ブール関数からなる。図 1 に示す好適な実施例では、符号 120 で示される複数の s

ボックス関数はそれぞれ、ユニークな 3 入力 1 出力の平衡な (balanced) 非線形ブール関数を実行する。

【0040】

図 1 に示す本発明の好適な実施例は、従来の $M \times N$ の s ボックスと比較して電送 (wiring) の冗長さが低減されている：符号 120 で示す領域の L 対 1 (L -to-1) のブール関数は、領域 120 における他の L から 1 のブール関数と L 以下の入力を共有する。これに対し、従来の $M \times N$ の s ボックスはすべて、完成基準 (completeness criterion) を満足するために、完全な電送の冗長性を有する必要がある：すべての出力ビットの完全な M 対 1 ブール関数 (M -to-1 Boolean function) は、その M 個の入力すべてを s ボックス内の他の M 対 1 ブール関数と共有する必要がある。

10

【0041】

図示の目的のため、 s ボックス 123、122、121 は、ビット 119、116、113 がそれぞれビットセット {118, 117}、{115, 114}、{112, 111} をデータ入力とする各マルチプレクサのセクタ入力となる 2 対 1 マルチプレクサ関数 (two-to-one multiplexer functions) となるよう選択される。 s ボックス 120 の選択とデータ入力はともに入力 100 から導出され、 s ボックス 120 はデータ従属置換 (data-dependent permutation) の形である。

【0042】

この方法では、図 1 に示す本発明の実施例は、複数の入力ビットの展開—置換 (expansion-permutation) と、マルチプレクサ関数と、出力ビット置換 (output bit permutation) とを具える。これにより、入力 100 の所定の 1 対 L (1 -to- L) 展開と、展開された中間状態 110 の所定のビット置換と、展開された中間状態 110 を L 対 1 圧縮 (L -to-1 compression) して状態 130 を出力とするキー・データ従属換字 (key-and-data-dependent substitution) とが得られる。

20

【0043】

出力 130 が入力 100 にフィードバックされる場合、このような構成を「並列フィードバックの有数非線形シフトレジスタ」または「並列フィードバック型 NLFSR」と呼ぶことができる。本発明の好適な実施例では、130 の出力が入力 100 としてフィードバックされる。2 つのサイクリックビットが右へ流れる出力 130 の各ビットの従属性により、ビット作用はサイクリックに左に流れる。本例では、要求される拡散の完成を得るには最低 2 ラウンドを要する。

30

【0044】

このプロセスを実現する回路において、出力 130 の各ビットのクリティカルパス電送待ち時間はおおよそ均一となることが予想される。これに対し本発明では、演算操作に基づいた回路に実装される s ボックスは常に、繰り越し操作 (carry operations) のチェーンの最上位のビットに従属して、強固で非一様なクリティカルパス電送待ち時間を示す。

【0045】

図 2 は、本発明の別の好適な実施例にかかるキー・データ従属換字置換ネットワーク暗号プロセスの全単射異形 (bijective variant) の一部である。領域 200 は、25 ビットの入力を示している。領域 201 は、入力 252 の左の 24 ビットを示す。領域 210 は、25 ビットの出力を示す。領域 211 は、領域 240 として示す 25 対 1 s ボックス (twenty five-to-one s -boxes) に従属する 20 ビットの出力を示す (図にはこれらの 20 の s ボックスの 1 つのみを符号 241 で示している)。領域 221 は、5 ビットの入力を示す。領域 223 は、5 つの入力ビット 221 の全単射 (可逆の) 5×5 換字—置換 222 に従属する 5 ビットの出力を示す。

40

【0046】

領域 240 の多入力単一出力ブール関数 241 はそれぞれ、例えば領域 201 の符号 231、232、233、234、235 といった 5 ビットの予め定められたセット 230 を入力とし、出力として、ビット 253 を出力として生成する 250 内の線形コンバイナ (XOR/XNOR) 251 に第 1 の入力ビットを生成する。入力ビット 252 は 251

50

への2つの入力のうちの2つ目である。領域250の各線形コンバイナ251用に、領域240の対応するブール関数がこの第2の入力ビットの左の領域のみから入力をコンバイナに受け取り、この領域が201として示されている。

【0047】

図2に示す本発明の好適な実施例では、領域240で図示されたステップに用いられる基本の5対1sボックス241は、領域230に図示するステップで用いられる5つの入力221から235と、単一の出力と、前記入力ビットと出力ビット感の関係を規定する5対1ブール関数とからなり、各平衡非線形ブール関数241は無作為に選択される。

【0048】

図3は、本発明の好適な実施例にかかるワードベースのキー・データ従属換字ー置換ネットワークの一部を示す図である。このデータステート (data state) 310は15ビット幅で3ワード (あるいは最も便利な表記により、ブロック、サブブロック、レジスタ) に仕切られている。ワード311は、5つのビット321、322、323、324、325からなり；ワード312は、5つのビット331、332、333、334、335からなり；ワード313は5つのビット341、342、343、344、345からなる。

【0049】

領域350は、このデータステートの3つのファクタによる静的展開置換 (static expansion permutation) を示す。領域360は、 3×1 の非線形換字ボックス関数 (図にはこれらの1つのみ示す) を示す。

【0050】

データステート365は、15ビットで、3ワードに仕切られている。ワード366は5つのビット371、372、373、374、375からなり；ワード367は5つのビット381、382、383、384、385からなり；ワード368は5つのビット391、392、393、394、395からなる。

【0051】

図示する 3×1 の換字置換関数361は、受信される3つの入力のユニークなセットを取得し、これはワード313のビット344から派生するビット352と、ワード312のビット332から派生するビット353と、ワード311のビット325から派生するビット351とからなる。図示するsボックス361は、ワード367に単一ビットの出力385を生成する。

【0052】

ステート365の15ビットすべてにおいて、360の各 3×1 sボックスは、上記テンプレートに従い、4入力のユニークなセットを出力する。

【0053】

図3に示す本発明の好適な実施例にかかるワードベースのキー・データ従属換字ー置換ネットワーク暗号は、暗号ソフトウェアのパフォーマンスを改善する直接的なメカニズムを提供する。

【0054】

図4は、本発明の好適な実施例にかかる図1に示す暗号を実装するソフトウェアの一例を示す図である。図4に示すプロセスは、ワード長が5ビットのプロセッサで実行される。ワード400は、5つのビット401、402、403、404、405からなり；ワード410は、5つのビット411、412、413、414、415からなり；ワード430は5つのビット431、432、433、434、435からなり、ワード470は5つのビット471、472、473、474、475からなる。ワード400は、ワード410および430への複製 (duplication) を通して、3つのワードに展開される。

【0055】

ワード410は、サイクリックなローテーション419を用いて、1ビットから最上位のビットに向かって静的 (static) に置換される。これにより、ビット411、412、

10

20

30

40

50

4 1 3、4 1 4、4 1 5は、それぞれ出力4 2 2、4 2 3、4 2 4、4 2 5、4 2 1として置換される。出力ビット4 2 1から4 2 5は、4 5 0の単一のワード入力として用いられる。

【0 0 5 6】

ワード4 3 0は、サイクリックなローテーション4 3 9を用いて、2ビットから最上位のビットに向かって静的（static）に置換される。これにより、ビット4 3 1、4 3 2、4 3 3、4 3 4、4 3 5は、それぞれ出力4 4 3、4 4 4、4 4 5、4 4 1、4 4 2として置換される。出力ビット4 4 1から4 4 5は、4 5 0の単一のワード入力として用いられる。

【0 0 5 7】

領域4 5 0は、3つの入力ワードをとる関数を規定し、図1に図示するマルチプレクサ作用を実現するワードベースの基本のブール関数でなるワードベースの命令4 6 0のシーケンスを実行する。仮にワード4 0 0をA、ワード4 2 0をB、ワード4 4 0をC、ワード4 7 0をDとすると、5つのビット幅2対1マルチプレクサを表すことができ、A h a選択入力でなり、BとCは以下のデータ入力でなる：

$$D = (A \text{ AND } B) \text{ OR } ((\text{NOT } A) \text{ AND } C)$$

【0 0 5 8】

領域4 8 1は、どのようにビット4 7 1が入力4 0 1、4 2 1、4 4 1にのみ従属するのかを視覚的に示している。領域4 8 2から4 8 5は、それぞれビット4 7 2から4 7 5の従属性を示している。

【0 0 5 9】

5ビット変数（five-bit variables）の語で完全な5ビット幅のプロセスの実装を説明すると、以下のようになる：

$$D = (A \text{ AND } (A \text{ ROT } 1)) \text{ OR } ((\text{NOT } A) \text{ AND } (A \text{ ROT } 2))$$

【0 0 6 0】

一般目的の5ビットレジスタRAが入力であるアセンブラ擬似コード（assembler pseudo code）では、RBとRCは一次レジスタでありRDが出力であり、これと同じアルゴリズムが以下の6操作で自明的（trivially）に実現される：

RB=RA rotate left 1

RC=RA and RB

RA=not RA

RB=RB rotate left 1

RD=RA and RB

RD=RD or RC

【0 0 6 1】

上記プロセスは、普遍性を失わずに、どのように置換操作がカスケード（cascade）されるかと、移動／複製操作が最適化されるかを示している。例えばバイトスワッピング（byte-swapping）、ルックアップテーブル、バイナリマスキング操作（binary masking operations）といった他の操作をがソフトウェアプロセッサで実現可能であり、これにより技術者が、プロセッサ命令の短いシーケンスで表現される幅広い電送置換（wiring permutations）を実現することができ、したがってハードウェア性能を落とすことなく要求されたソフトウェア性能を得ることができる。

【0 0 6 2】

図1、2、3に示す本発明の好適な実施例では、すべての入力ビット1 0 0、2 0 1、3 1 0をそれぞれ展開された入力ビット1 1 0、2 4 0、3 5 0への割り当てること（assignments）を含む内部電送置換（internal wiring permutations）は、1 2 0、2 4 0、3 6 0内の複数の基本のL対1 sボックスからそれぞれ1 3 0、2 1 0、3 6 5内のすべての出力ビットへの出力ビットのすべての割り当てとともに、無作為に選択される。

【0 0 6 3】

本発明の別の好適な実施例では：

- ー内部電送置換 (internal wiring permutation) がキー従属疑似ランダムプロセスで選択される；
- ー内部電送置換が数式により選択される；
- ー内部電送置換が、入力と出力ビット間の単一ラウンドまたは複数ラウンドの多項式の関係における冗長性を低減するよう帰納的に細分され (heuristically refined) ；
- ー内部電送置換が、ハードウェア回路最適化の最大電送待ち時間により制限される；
- ー1 2 1、1 2 2、1 2 3、2 4 1、3 6 1への入力が、それぞれ出力1 3 1、1 3 4、1 3 5、2 5、3 8 5からの間隔に制限される；
- ー領域1 2 0、2 4 0、3 6 0の各基本のL対1 sボックスが、それぞれ領域1 3 0、2 1 0、3 6 5の各出力ビットに関し、領域1 0 0、2 0 1、3 1 0、の入力ビットの同じ関連位置から選択される； 10
- ー領域1 2 0、2 4 0、3 6 0内の基本のL対1 sボックスのいくつかが、1または複数のキービットを入力として受信するよう構成されている；
- ー異なる電送置換が暗号処理の各ラウンドで選択される；
- ー出力1 3 0、2 1 0、3 6 5の幅が、それぞれ入力1 0 0、2 0 0、3 1 0と異なる；
- ー内部電送置換が、3 2ビットまたは1 2 8ビットの一般目的のプロセッサ命令の短いシーケンスとして実装しうる置換に限定される；
- ー内部電送置換が、2 0 0 4年1 0月1 3日に提出された継続中のオーストラリア暫定特許出願2 0 0 4 9 0 5 8 9 7、「Process of and Apparatus for Encoding a digital signal」にみられるバイトスワッピングとローテーションシーケンシングの組合せに適合する； 20
- ー領域1 2 0、2 4 0、3 6 0のすべての基本のL対1 sボックスに単一のブール関数が用いられる；
- ー領域1 2 0、2 4 0、3 6 0の基本のL対1 sボックスに複数のブール関数が用いられる；
- ー領域1 2 0、2 4 0、3 6 0の基本のL対1 sボックスに用いられるすべてのブール関数が異なる；
- ー領域1 2 0、2 4 0、3 6 0の基本のL対1 sボックスに用いられるブール関数のいくつかが、キー従属疑似ランダムプロセスを用いて選択される；
- ー領域1 2 0、2 4 0、3 6 0の基本のL対1 sボックスに用いられるブール関数の選択が、入力と出力ビット間の単一ラウンドまたは複数ラウンドの多項式の関係における冗長性を低減するよう帰納的に細分される (heuristically refined) ； 30
- ー元の入力変数 (またはプロセッサレジスタ) のみが後続の処理で用いられる；
- ー少なくとも1または複数の中間変数 (またはプロセッサレジスタ) が後続の処理で用いられる；
- ー中間変数 (またはプロセッサレジスタ) のみが後続の処理で用いられる；
- ーsボックスを設ける方法が、以下の継続中の特許出願にみられる双方向ブロック連鎖方式にも適合する；
- 2 0 0 4年1 1月5日出願のオーストラリア暫定出願2 0 0 4 9 0 6 3 6 4と2 0 0 5年1月1 0日出願の2 0 0 5 9 0 0 0 8 7、ともに名称がA method of Endoding a Signal； 40
- 2 0 0 5年5月1 0日出願の国際特許出願P C T / I B 2 0 0 5 / 0 0 1 4 9 9、名称Method of Encoding and Decoding Data；
- 2 0 0 5年5月1 0日出願の国際特許出願P C T / I B 2 0 0 5 / 0 0 1 4 8 7、名称Process of and Apparatus for Encoding a Signal；
- 2 0 0 5年5月1 0日出願の国際特許出願P C T / I B 2 0 0 5 / 0 0 1 4 7 5、名称A Method of and Apparatus for Encoding a Signal in a Hashing Primitive；
- 各文献の内容は本願に参照として組み込まれる。

【0 0 6 4】

本発明の好適な実施例で用いられる電送置換および/またはブール関数は、「ファミリ 50

ー」キーと呼ばれるキー要素に従属し、このような暗号のハードウェア（RFID、ASIC等）の実装は、固定の基本プール理論を伴う固定的な電送として実装された場合にまだ有効である。

【0065】

重要なことは、252の左のビットのみへの基本のL対1sボックス201への入力ビットの選択の唯一の制限は、入力ビット252と出力ビット253間の線形関係と組み合わせ、図2のように操作され、ブール関数または内部電送置換の選択に拘わらず、全単射（可逆の）操作を確実にする。

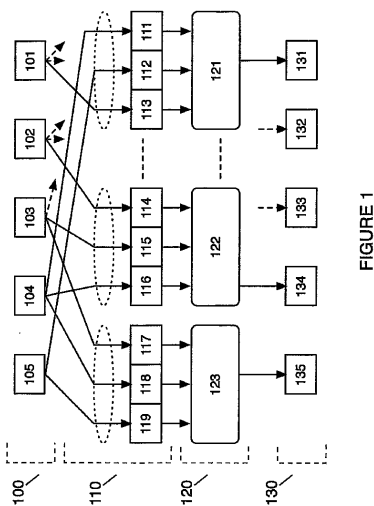
【図面の簡単な説明】

【0066】

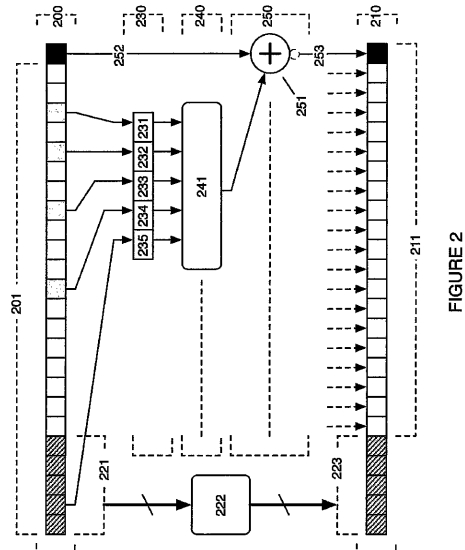
本発明をより理解し易くすべく、その好適な実施例が図面を参照しながら説明され、ここで図1、2、3、4は本発明の好適な実施例にかかる方法を図示するものである。

10

【図1】



【図2】



【図 3】

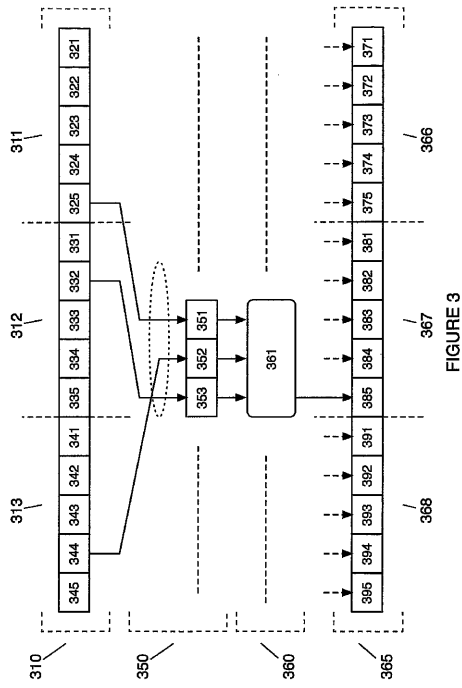


FIGURE 3

【図 4】

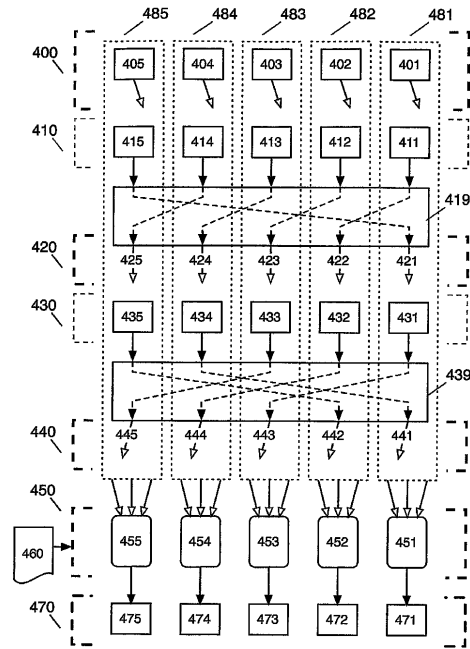


FIGURE 4

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2005/003104

A. CLASSIFICATION OF SUBJECT MATTER INV. H04L9/06		
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) H04L		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the international search (name of data base and, where practical, search terms used) EPO-Internal, WPI Data, INSPEC		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 745 577 A (LEECH ET AL) 28 April 1998 (1998-04-28) column 4, line 29 - column 7, line 6	1-96
A	US 2002/003876 A1 (LIM YOUNG-WON) 10 January 2002 (2002-01-10) the whole document	1-96
A	US 2002/027987 A1 (ROELSE PETRUS LAMBERTUS ADRIAANUS) 7 March 2002 (2002-03-07) the whole document	1-96
☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.		
* Special categories of cited documents : "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier document but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art. "&" document member of the same patent family		
Date of the actual completion of the international search 20 April 2006		Date of mailing of the international search report 03/05/2006
Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016		Authorized officer Apostolescu, R

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/IB2005/003104

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
US 5745577	A	28-04-1998	NONE	
US 2002003876	A1	10-01-2002	JP 2002049309 A	15-02-2002
US 2002027987	A1	07-03-2002	AU 6908601 A	14-01-2002
			CN 1383648 A	04-12-2002
			WO 0203605 A1	10-01-2002
			JP 2004502965 T	29-01-2004
			TW 527811 B	11-04-2003

フロントページの続き

(31)優先権主張番号 2004907374
(32)優先日 平成16年12月31日(2004.12.31)
(33)優先権主張国 オーストラリア(AU)
(31)優先権主張番号 2005902136
(32)優先日 平成17年4月29日(2005.4.29)
(33)優先権主張国 オーストラリア(AU)

(81)指定国 AP(BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), EA(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), EP(AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OA(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG), AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW

【要約の続き】

c 個のブール関数の出力を含む。

【選択図】 図 1