(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3600454号
(P3600454)
(45)発行日　平成16年12月15日(2004.12.15)　(24)登録日　平成16年9月24日(2004.9.24)

(51)Int.Cl.[7]　F I
G09C 1/00　G09C 1/00 610B
H04L 9/06　H04L 9/00 611A

請求項の数 30　(全 22 頁)

(21)出願番号　特願平10-233921
(22)出願日　平成10年8月20日(1998.8.20)
(65)公開番号　特開2000-66585(P2000-66585A)
(43)公開日　平成12年3月3日(2000.3.3)
審査請求日　平成13年2月6日(2001.2.6)

(73)特許権者　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(74)代理人　100058479
弁理士　鈴江　武彦
(74)代理人　100084618
弁理士　村松　貞男
(74)代理人　100068814
弁理士　坪井　淳
(74)代理人　100092196
弁理士　橋本　良郎
(74)代理人　100091351
弁理士　河野　哲
(74)代理人　100088683
弁理士　中村　誠

最終頁に続く

(54)【発明の名称】暗号化・復号装置、暗号化・復号方法、およびそのプログラム記憶媒体

(57)【特許請求の範囲】
【請求項１】
平文ブロックを与えられた鍵情報に依存して暗号文ブロックに変換する暗号化装置であって、
あらかじめ定められたひとつまたは複数のマスクパターンとそのビット反転のマスクパターンの各ペア（a_i, a_i^-）（ｉは１以上の正の整数）の中から一方を、暗号化を行う毎にランダムに選択する手段と、
装置内部の平文に依存したビットを、前記選択手段により選択されたマスクパターンによってマスクする手段と、
暗号文を出力する前に、暗号文から前記マスクａの影響を除去する手段とを具備したことを特徴とする暗号化装置。
【請求項２】
平文ブロックを与えられた鍵情報に依存して暗号文ブロックに変換する暗号化装置であって、
あらかじめ定められたひとつまたは複数のマスクパターンとそのビット反転のマスクパターンの各ペア（a_i, a_i^-）（ｉは１以上の正の整数）の中から一方を、暗号化を行う毎にランダムに選択する手段と、
装置内部の中間的なビットデータを、前記選択手段により選択されたマスクパターンによってマスクする手段と、
前記マスク手段によりマスクされた中間的なビットデータから前記マスクａの影響を除去

する手段とを具備したことを特徴とする暗号化装置。
【請求項３】
平文ブロックを与えられた鍵情報に依存して暗号文ブロックに変換する暗号化装置であって、
装置内部の中間的なデータにデータ変換を行うデータ変換手段と、
あらかじめ定められたひとつまたは複数のマスクパターンとそのビット反転のマスクパターンの各ペア（a_i, a_i^-）（ｉは１以上の正の整数）の中から一方を、暗号化を行う毎にランダムに選択する手段と、
前記データ変換手段の入力を、前記選択手段により選択されたマスクパターンによってマスクする手段と、
前記マスク手段によりマスクされた、前記データ変換手段の出力から前記マスクａの影響を除去する手段とを具備したことを特徴とする暗号化装置。
【請求項４】
前記装置内部の平文に依存したビットを選択されたマスクパターンによってマスクする手段、および前記暗号文から該マスクａの影響を除去する手段が、排他的論理和、定数ｗを法とする加算または減算、および定数ｗを法とする乗算または除算のいずれかで構成されることを特徴とする請求項１記載の暗号化装置。
【請求項５】
前記装置内部の中間的なビットデータを選択されたマスクパターンによってマスクする手段、およびマスクされた中間的なビットデータから該マスクａの影響を除去する手段は、排他的論理和、定数ｗを法とする加算または減算、および定数ｗを法とする乗算または除算のいずれかで構成されることを特徴とする請求項２記載の暗号化装置。
【請求項６】
前記データ変換手段、前記データ変換手段の入力を前記選択されたマスクパターンによってマスクする手段、および前記マスクされたデータの変換手段の出力から該マスクａの影響を除去する手段は、排他的論理和、定数ｗを法とする加算または減算、および定数ｗを法とする乗算または除算のいずれかで構成されることを特徴とする請求項３記載の暗号化装置。
【請求項７】
前記データ変換手段は、ビット入れ替え手段またはビット換字手段のいずれかで構成されることを特徴とする請求項３の暗号化装置。
【請求項８】
前記あらかじめ定められたひとつ又は複数のマスクパターンとそのビット反転のマスクパターンの各ペア（a_i, a_i^-）（ｉは１以上の正の整数）の中から一方を、暗号化を行う毎にランダムに選択する手段と、前記データ変換手段の入力を、前記マスクパターンa_iによってマスクする手段と、および前記マスクされた、前記データ変換手段の出力から前記マスクa_iの影響を除去する手段と、
をテーブル形式で記憶する第1の記憶手段と、
前記データ変換手段の入力をマスクパターンa_i^-によってマスクする手段と、
前記マスクされた前記データ変換手段の出力から前記マスクa_i^-の影響を除去する手段と、
をテーブル形式で記憶する第２の記憶手段と、
前記第1の記憶手段と第2の記憶手段の一方を、暗号化を行う毎にランダムに選択し、マスクされたデータに対して前記データ変換手段の処理を行う、マスクされたデータの変換手段とをさらに有することを特徴とする請求項３記載の暗号化装置。
【請求項９】
前記マスクパターンとそのビット反転のマスクパターンのペア（ａ，a^-）が、あらかじめ定められた固定のマスクパターンとそのビット反転のマスクパターンのペア（ａ，a^-）で構成されることを特徴とする請求項１記載の暗号化装置。
【請求項１０】

前記マスクパターンとそのビット反転のマスクパターンのペア（ａ，ａ¯）が、必ずしも秘密でないことを特徴とする請求項１記載の暗号化装置。

【請求項１１】

ｎビット長のビット列ｘの１のビットの数を示すハミング重みをＨ（ｘ）と定義し、前記ｎビット長のビット列ｘが前記マスクａのとき、前記マスクａのハミング重みＨ（ａ）が０＜Ｈ（ａ）＜ｎを満足することを特徴とする請求項１記載の暗号化装置。

【請求項１２】

ｎビット長のビット列ｘの１のビットの数を示すハミング重みをＨ（ｘ）と定義し、前記ｎビット長のビット列ｘが前記マスクａのとき、前記マスクａのハミング重みＨ（ａ）と、前記マスクａのビット反転ａ¯のハミング重みＨ（ａ¯）の差の絶対値が、ｎ／２未満であることを特徴とする請求項１記載の暗号化装置。

【請求項１３】

暗号ブロックを与えられた鍵情報に依存して平文ブロックに変換する復号装置であって、

あらかじめ定められたひとつまたは複数のマスクパターンとそのビット反転のマスクパターンの各ペア（a_i，a_i^-）（ｉは１以上の正の整数）の中から一方を、復号を行う毎にランダムに選択する手段と、

装置内部の暗号文に依存したビットを、前記選択手段により選択されたマスクパターンによってマスクする手段と、

平文を出力する前に、前記平文から前記マスクａの影響を除去する手段とを具備したことを特徴とする復号装置。

【請求項１４】

暗号ブロックを与えられた鍵情報に依存して平文ブロックに変換する復号装置であって、

あらかじめ定められたひとつまたは複数のマスクパターンとそのビット反転のマスクパターンの各ペア（a_i，a_i^-）（ｉは１以上の正の整数）の中から一方を、復号を行う毎にランダムに選択する手段と、

装置内部の中間的なビットデータを、前記選択手段により選択されたマスクパターンによってマスクする手段と、

前記マスク手段によりマスクされた中間的なビットデータから前記マスクａの影響を除去する手段とを具備したことを特徴とする復号装置。

【請求項１５】

装置内部の中間的なデータに対してデータ変換を行なうデータ変換手段を備え、暗号ブロックを与えられた鍵情報に依存して前記データ変換手段により平文ブロックに変換する復号装置であって、

あらかじめ定められたひとつまたは複数のマスクパターンとそのビット反転のマスクパターンの各ペア（a_i，a_i^-）（ｉは１以上の正の整数）の中から一方を、復号を行う毎にランダムに選択する手段と、

前記データ変換手段の入力を、前記選択手段により選択されたマスクパターンによってマスクする手段と、

前記マスク手段によりマスクされた、前記データ変換手段の出力から前記マスクａの影響を除去する手段とを具備したことを特徴とする復号装置。

【請求項１６】

前記装置内部の暗号文に依存したビットを選択されたマスクパターンによってマスクする手段と、該暗号文から該マスクａの影響を除去する手段とが、排他的論理和、定数ｗを法とする加算または減算、および定数ｗを法とする乗算または除算のいずれかで構成されることを特徴とする請求項１３記載の復号装置。

【請求項１７】

前記装置内部の中間的なビットデータを選択されたマスクパターンによってマスクする手段と、マスクされた中間的なビットデータから該マスクａの影響を除去する手段とが、排他的論理和、定数ｗを法とする加算または減算、および定数ｗを法とする乗算または除算のいずれかで構成されることを特徴とする請求項１４記載の復号装置。

【請求項１８】
前記データ変換手段と、前記選択されたマスクパターンを用いて、前記第1のデータ変換手段の入力を選択されたマスクパターンによってマスクする手段と、前記マスクされた第1のデータ変換手段の出力から該マスクａの影響を除去する手段とが、排他的論理和、定数ｗを法とする加算または減算、および定数ｗを法とする乗算または除算のいずれかで構成されることを特徴とする請求項１５記載の復号装置。
【請求項１９】
前記データ変換手段は、ビット入れ替え変換手段またはビット換字手段のいずれかで構成されることを特徴とする請求項１５の暗号化装置。
【請求項２０】
あらかじめ定められたひとつまたは複数のマスクパターンとそのビット反転のマスクパターンの各ペア（a_i ,a_i^-）（ｉ＝１以上の正の整数）の中から一方を、復号を行う毎にランダムに選択する手段と、
前記データ変換手段の入力をマスクパターンa_iによってマスクする手段と、
前記マスクされた該データ変換手段の出力から前記マスクa_iの影響を除去する手段、
をテーブル形式で記憶する第1の記憶手段と、
前記データ変換手段の入力をマスクパターンa_i^-によってマスクする手段と、
前記マスクされた該データ変換手段の出力から前記マスクa_i^-の影響を除去する手段と、
をテーブル形式で記憶する第２の記憶手段と、
前記第1の記憶手段と第2の記憶手段の一方を、暗号化を行う毎にランダムに選択し、マスクされたデータに対して前記データ変換手段の処理を行うマスクされたデータの変換手段とをさらに有することを特徴とする請求項１５記載の復号装置。
【請求項２１】
前記マスクパターンとそのビット反転のマスクパターンのペア（a_i ,a_i^-）が、あらかじめ定められた固定のマスクパターンとそのビット反転のマスクパターンのペア（a_i ,a_i^-）であることを特徴とする請求項１３記載の復号装置。
【請求項２２】
前記マスクパターンとそのビット反転のマスクパターンのペア（a_i ,a_i^-）が、必ずしも秘密でないことを特徴とする請求項１３記載の復号装置。
【請求項２３】
ｎビット長のビット列ｘの１のビットの数を示すハミング重みをＨ（ｘ）と定義し、前記ｎビット長のビット列ｘが前記マスクａのとき、前記マスクａのハミング重みＨ（ａ）が、０＜Ｈ（ａ）＜ｎを満足することを特徴とする請求項１３記載の復号装置。
【請求項２４】
ｎビット長のビット列ｘの１のビットの数を示すハミング重みをＨ（ｘ）と定義し、前記ｎビット長のビット列ｘが前記マスクａのとき、前記マスクａのハミング重みＨ（ａ）と、前記マスクａのビット反転a^-のハミング重みＨ（a^-）の差の絶対値が、ｎ／２未満であることを特徴とする請求項１３記載の復号装置。
【請求項２５】
平文ブロックを与えられた鍵情報に依存して暗号文ブロックに変換させるための、コンピュータ読み出し可能なプログラムコード手段が記憶されたコンピュータ使用可能なプログラム記憶媒体であって、
コンピュータに、あらかじめ定められたひとつまたは複数のマスクパターンとそのビット反転のマスクパターンの各ペア（a_i ,a_i^-）（ｉは１以上の正の整数）の中から一方を、暗号化を行う毎にランダムに選択させるためのコンピュータ読み出し可能なプログラムコード手段と、
コンピュータに、前記選択されたマスクパターンを用いて、方法内部の平文に依存したビットを選択されたマスクパターンによってマスクさせるためのコンピュータ読み出し可能なプログラムコード手段と、

コンピュータに、暗号文を出力する前に、暗号文から前記マスクａの影響を除去させるためのコンピュータ読み出し可能なプログラムコード手段とを具備したことを特徴とするプログラム記憶媒体。

【請求項２６】

平文ブロックを与えられた鍵情報に依存して暗号文ブロックに変換する暗号化装置であって、

あらかじめ定められたひとつ又は複数のマスクパターンとそのビット反転のマスクパターンの各ペア（a_i，a_i^-）（ｉは１以上お正の整数）の中から一方を、暗号化を行なう毎にランダムに選択する手段と、

装置内部の鍵に依存したビットを、前記選択手段により選択されたマスクパターンによってマスクする手段と、

装置内部の中間的なデータに対して鍵によってデータ変換を行なうデータ変換手段と、

前記データ変換手段の出力から前記マスクａの影響を除去する手段とを具備したことを特徴とする暗号化装置。

【請求項２７】

前記マスクパターンとそのビット反転のマスクパターンのペア（ａ，a^-）が、あらかじめ定められた固定のマスクパターンとそのビット反転のマスクパターンのペア（ａ、a^-）で構成されることを特徴とする請求項２６記載の暗号化装置。

【請求項２８】

前記マスクパターンとそのビット反転のマスクパターンのペア（ａ、a^-）が、必ずしも秘密でないことを特徴とする請求項２６記載の暗号化装置。

【請求項２９】

ｎビット長のビット列ｘの１のビットの数を示すハミング重みをＨ（ｘ）と定義し、前記ｎビット長のビット列ｘが前記マスクａのとき、前記マスクａのハミング重みＨ（ａ）が０＜Ｈ（ａ）＜ｎを満足することを特徴とする請求項２６記載の暗号化装置。

【請求項３０】

ｎビット長のビット列ｘの１のビットの数を示すハミング重みをＨ（ｘ）と定義し、前記ｎビット長のビット列ｘが前記マスクａのとき、前記マスクａのハミング重みＨ（ａ）と、前記マスクａのビット反転a^-のハミング重みＨ（ａ）の差の絶対値が、ｎ／２未満であることを特徴とする請求項２６記載の暗号化装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は暗号化装置、復号装置、暗号化手法、および復号手法に関し、特に、秘密鍵ブロック暗号を用いた暗号化装置、復号装置、暗号化手法、復号手法、およびそのプログラム記憶媒体に関する。

【０００２】

【従来の技術】

ＤＥＳ（Ｄａｔａ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ）は、現在、最も広範に用いられている秘密鍵ブロック暗号であり、特開昭５１－１０８７０１号広報に詳細に記載されている。

【０００３】

ＤＥＳ に関してはさまざまな観点からの評価が行われており、差分解読法や線形解読法といった鍵の全数探索よりも効率的な解読法が提案された。

【０００４】

なお、差分解読法については、文献、Ｅ．Ｂｉｈａｍ ａｎｄ Ａ．Ｓｈａｍｉｒ，Ｄｉｆｆｅｒｅｎｔｉａｌ Ｃｒｙｐｔａｎａｌｙｓｉｓ ｏｆ ＤＥＳ－ｌｉｋｅ Ｃｒｙｐｔｏｓｙｓｔｅｍｓ，Ｊｏｕｒｎａｌ ｏｆ ＣＲＹＰＴＯＬＯＧＹ，Ｖｏｌ．４，Ｎｕｍｂｅｒ １，１９９１ に、線形解読法については、文献、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に記載されている。
【０００５】
新たな解読方法としてＤＰＡ（Ｄｉｆｆｅｒｅｎｔｉａｌ　Ｐｏｗｅｒ　Ａｎａｌｙｓｉｓ　）が提案されている。ＤＰＡ　はデータのあるビットに着目して消費電力の差異（ビット０のときの消費電力とビット１のときの消費電力）を計測し、ビットを推測する。例えば、ＤＥＳ　の場合、既知の暗号文出力と鍵の推測により、Ｓ　箱の入力およびそれに対応する出力を推測する。上記Ｓ　箱出力で推測した、ある１ビットが０あるいは１である場合の消費電力の差異を計測し、推測の正当性の検証、すなわち鍵の推測の正当性の検証を行う手法がＤＰＡ　である。
【０００６】
【発明が解決しようとする課題】
このため、上述したＤＰＡによりＤＥＳが解読される恐れがあり、さらなるセキュリティが求められていた。
【０００７】
本発明の目的は、従来の暗号化装置、復号装置、暗号化手法、および復号手法のデータ暗号化処理結果を変更することなく、ＤＰＡによる解読を困難にする暗号化・復号装置、およびそのプログラム記憶媒体を提供することである。
【０００８】
【課題を解決するための手段】
上述の課題を解決するため、本発明は、平文ブロックを与えられた鍵情報に依存して暗号文ブロックに変換する暗号化装置において、あらかじめ定められたひとつまたは複数のマスクパターンとそのビット反転のマスクパターンの各ペア（a_i，　a_i^-）（ｉは１以上の正の整数）の中から一方を、暗号化を行う毎にランダムに選択する手段と、装置内部の平文に依存したビットを、前記選択手段により選択されたマスクパターンによってマスクする手段と、暗号文を出力する前に、暗号文から前記マスクａの影響を除去する手段とを具備したことを特徴とする。
【０００９】
また、本発明は、暗号ブロックを与えられた鍵情報に依存して平文ブロックに変換する復号装置において、あらかじめ定められたひとつまたは複数のマスクパターンとそのビット反転のマスクパターンの各ペア（a_i，　a_i^-）（ｉは１以上の正の整数）の中から一方を、復号を行う毎にランダムに選択する手段と、装置内部の暗号文に依存したビットを、前記選択手段により選択されたマスクパターンによってマスクする手段と、平文を出力する前に、前記平文から前記マスクａの影響を除去する手段とを具備したことを特徴とする。
【００１２】
また、本発明は、平文ブロックを与えられた鍵情報に依存して暗号文ブロックに変換させるための、コンピュータ読み出し可能なプログラムコード手段が記憶されたコンピュータ使用可能なプログラム記憶媒体において、コンピュータに、あらかじめ定められたひとつまたは複数のマスクパターンとそのビット反転のマスクパターンの各ペア（a_i，　a_i^-）（ｉは１以上の正の整数）の中から一方を、暗号化を行う毎にランダムに選択させるためのコンピュータ読み出し可能なプログラムコード手段と、コンピュータに、前記選択されたマスクパターンを用いて、方法内部の平文に依存したビットを選択されたマスクパターンによってマスクさせるためのコンピュータ読み出し可能なプログラムコード手段と、コンピュータに、暗号文を出力する前に、暗号文から前記マスクａの影響を除去させるためのコンピュータ読み出し可能なプログラムコード手段とを具備したことを特徴とする。
【００１３】
この発明によれば、本来のデータをマスクし、各Ｓ箱に入力する直前でそのマスクを解除する。しかし、このマスクを解除したときに、ＤＰＡにより解読される恐れがある。このため、この発明によれば、Ｓ箱への入力直前におけるマスク解除、マスク解除後の本来の

データによるＳ箱への入力、およびＳ箱からの出力のマスク操作を、事前に計算し、テーブルとして記憶し、テーブルを参照することにより計算結果を求める。このため、暗号化および復号の処理中に、マスク解除のための排他的論理和の計算や、マスクをかけるための排他的論理和の計算が行われることはないので、ＤＰＡによる解読は不可能となる。

【００１４】

【発明の実施形態】

以下、図面を参照して本発明の実施形態を説明する。

【００１５】

図１は本発明が適用される、暗号化アルゴリズムＤＥＳ　の構成を示す図であり、平文（６４ビット）３を外部から入力された鍵８に依存して攪拌し、対応する暗号文を出力する第１段～第１６段から構成されるデータ攪拌部１と、鍵情報ｋを前記データ攪拌部に供給される中間鍵に展開する鍵スケジュール部２からなる。

【００１６】

図１において、平文（６４ビット）３は初期転置ＩＰ　　４が施された後、２つに等分される。等分された結果の左側３２ビットのデータと右側３２ビットのデータはそれぞれ、段関数５の入力となる。段関数の構造は後述する。段関数の出力の左側３２ビットのデータと右側３２ビットのデータは入れ替えられて次段の段関数の入力となる。

【００１７】

上記段関数を１６段繰り返した後、最終転置ＩＰ$^{-1}$６　により暗号文７が出力される。

【００１８】

図２は図１に示す段関数５の詳細ブロック図である。段関数１７は転置Ｅ１１、排他的論理和１３、Ｓ箱１４、転置Ｐ１５および排他的論理和１６とで構成される。

【００１９】

右側３２ビットのデータを拡大転置Ｅ　１１により４８ビットに拡大し、その結果を排他的論理和１３に出力する。排他的論理和１３は、転置Ｅ　１１の出力と、拡大鍵１２の排他的論理和を出力する。排他的論理和１３の出力４８ビットは６ビットのデータに等分され、各Ｓ　箱１４の入力となる。この実施形態では、各Ｓ箱はテーブルで構成され、６４エントリの６ビット入力に対してそれぞれ４ビットデータを出力する。例えばＤＥＳのＳ１は、６ビット入力の左端を第１ビット、右端を第６ビットとすると、第１ビットと第６ビットを２進数とみなした数字で図３に示すＳ箱の表の行を指定する。なお、図３に示すＳ箱の表の行番号は上から０、１、２、３行と数える。次に残りの４ビットを２進数とみなした数字で列の番号を指定する。列番号も左端から０、１、２、３、…１５列と数える。例えば、Ｓ１の入力を０１１０１１とすると、行番号は０１すなわち、図３において、上から２番目の行となる。次に、列番号は０１１０１すなわち１３（左から１４番目の列）なので表の値は５となる。従ってＳ１の出力はこの２進表現である０１０１となる。なお、図３では、Ｓ箱の出力を行と列で示したが、一般には、０から６３までの入力に対応した表として構成される。各Ｓ　箱の出力を結合した３２ビットのデータは、転置Ｐ　１５によりビット転置操作が行われ、その結果が排他的論理和１６に出力される。排他的論理和１６は左側３２ビットのデータと転置Ｐ　１５の出力との排他的論理和を出力する。

【００２０】

図４は図１に示す段関数５および図２に示す段関数１７の詳細回路図であり、図５ａは第１段の段関数への入力の構成を示す図であり、図５ｂは第１６段の段関数の出力の構成を示す図である。

【００２１】

以下、図４、図５ａ、および図５ｂを参照して本発明の実施形態を詳細に説明する。

【００２２】

図４において、ａおよびｂはそれぞれ３２ビットのマスクを表し、$\bar{a}$はａの全ビット反転を表す。図４に示す段関数３５において、排他的論理和２５は、右側３２ビットのデータを、スイッチＳＷ２３の出力と排他的論理和を行い拡大転置Ｅ２６に出力する。拡大転置Ｅ２６の出力は、排他的論理和２７において拡大鍵Ｋｉと排他的論理和が行われ、スイ

ッチＳＷ１２に出力する。スイッチＳＷ１２は、後述の乱数列Ｒｉｊによりデータの分岐を行う。例えば、Ｒｉｊ　が０の場合には、スイッチＳＷ１２は、データを０側に分岐し、Ｒｉｊ　が１の場合には、データを１側に分岐する。

【００２３】

図４において、スイッチＳＷ１２の分岐以降は、各Ｓ箱についての構成を示す図であり、すなわちＳ箱２９はＤＥＳ　のＳ１～Ｓ８に対応する。

【００２４】

スイッチＳＷ１２が、データを０側に分岐した場合、破線３４ａで示す処理を行う。すなわち、排他的論理和３２ａは、排他的論理和２７の出力と、マスクａに拡大転置Ｅ　を行った結果のＳ　箱の入力に対応する６ビット（Ｅ（ａ））との排他的論理和を行い、その結果をＳ箱２９に出力する。Ｓ箱２９においては、対応するＳ箱のテーブル参照が行われた結果が、排他的論理和３３ａに出力される。

【００２５】

排他的論理和３３ａにおいては、マスクａに転置Ｐ３０の逆転置$Ｐ^{-1}$を行った結果である$Ｐ^{-1}$（　ａ）　のビットと、Ｓ箱２９の出力との排他的論理和が行われ、その結果がスイッチＳＷ１１に出力される。

【００２６】

一方、スイッチＳＷ１２が、データを１側に分岐した場合、破線３４ｂで示す処理を行う。すなわち、排他的論理和３２ｂは、排他的論理和２７の出力と、マスク$ａ^{-}$に拡大転置Ｅ　を行った結果のＳ　箱の入力に対応するビットとの排他的論理和を行い、その結果をＳ箱２９に出力する。Ｓ箱２９は、対応するＳ箱のテーブルを参照し、その結果を排他的論理和３３ｂに出力する。

【００２７】

排他的論理和３３ｂは、マスク$ａ^{-}$に転置Ｐ（３０）の逆転置$Ｐ^{-1}$を行った結果である$Ｐ^{-1}$（$ａ^{-}$）のＳ箱の出力に対応する４ビットと、Ｓ箱２９の出力との排他的論理和を行い、その結果をスイッチＳＷ１１に出力する。

【００２８】

ただし、上記破線３４ａおよび３４ｂで示す各処理は、暗号化および復号の処理中に行ってはならない。なぜならば、上記マスクによるデータの秘匿を行っていても、Ｓ箱２９の入出力は秘匿されていないため、Ｓ箱の処理の消費電力の差異を用いた解読が試みられる可能性があるからである。

【００２９】

本発明の実施形態では、破線３４ａおよび３４ｂで示す各処理結果は、暗号化および復号を行う前に事前計算により処理結果を作成し、暗号化および復号処理を行う。例えば、各Ｓ箱について、Ｓ箱の入力のインデックスと出力を書き換えたテーブルを用意し、暗号化および復号の処理に用いる。このとき、マスクａに対応したＳ箱のテーブルとマスク$ａ^{-}$に対応したＳ箱のテーブルを用意する。例えば、マスクａを使って、図４の処理ブロック３４ａを計算した結果は以下の通りである。今、マスクａを（０１１０　１１１１　１１００　１０１０　０１１０　１１００　１１００　００１１）とする。拡大転置Ｅは図６に示す表で表される。図６の表において、各行は上からＳ１、Ｓ２、…Ｓ８への入力に対応する。また、各列は左端の第１ビットがＳ箱の入力の第１ビットに対応する。表の数字は拡大転置Ｅへの入力の第Ｘビットを表す。すなわち、Ｓ１の入力は、Ｅへの入力の第３２、１、２、３、４、、５ビットになる。従って、マスクａが上記の例の場合、Ｓ１の入力に対応するビットマスク（ａ）は（１０１１０１）となる。転置Ｐの表は図７に示される。図７において、左から順番にＰの出力の第１ビットから第３２ビットまでに対応する。（１行目と２行目は連続している）。各項目は入力の第Ｘビットを表す。すなわち、転置Ｐの出力の第１ビットは入力の第１６ビットになる。Ｓ１に対応するビットは転置Ｐの入力の第１、２、３、４ビットなので、それぞれＰの出力の第９、１７、２３、３１ビットに対応する。Ｓ１の出力に対応するマスクは$Ｐ^{-1}$（ａ）すなわち、Ｐの出力がａになる値なので、マスクａの第９、１７、２３、３１ビットが$Ｐ^{-1}$（ａ）となる。従って、

Ｓ１の出力に対応するマスクは（１００１）となる。従って、マスクａが上記の場合、Ｓ１の入力に対応するビットマスクＥ（ａ）は（１０１１０１）、Ｓ１の出力に対応するビットマスクＰ$^{-1}$（ａ）は（１００１）となる。実際に作成するマスクａに対応したテーブルは、入力をビットマスクＥ（ａ）と排他的論理和した結果をＳ１の入力としてＳ１の出力を計算して、そのＳ１の出力にビットマスクＰ$^{-1}$（ａ）を排他的論理和で加えたものがテーブルの出力になる。上記マスクａの場合、入力が（０００００、０００００１、…１１１１１）に対応する隠蔽されたＳ１の出力（０から６３までの入力に対する出力）を列挙すると、それぞれの出力を列挙すると、図８に示すような結果となる。また、マスクａ$^{-}$（ａのビット反転）のテーブルは、図９に示すような結果となる。

【００３０】

破線３４ａおよび３４ｂで示す各処理ブロックの出力は、転置Ｐ３０において、転置が行われ排他的論理和３１に出力される。排他的論理和３１は、左側３２ビットのデータと、転置Ｐ３０の出力との排他的論理和を行う。排他的論理和２４は右側３２ビットのデータと、スイッチＳＷ１３の出力との排他的論理和を取り、新たな右側３２ビットのデータとする。

【００３１】

図５ａにおいて、平文（６４ビット）を初期転置ＩＰ４１ａにより転置を行った結果は、等分され、右側３２ビットと左側３２ビットとなる。排他的論理和４４ａは、左側３２ビットのデータと、スイッチＳＷ２１の出力との排他的論理和を取る。この排他的論理和４４ａの出力は、第１　段の段関数の入力の左側３２ビットとなる。排他的論理和４２ａは右側３２ビットのデータと、スイッチＳＷ１４の出力との排他的論理和を取る。排他的論理和４３ａは、排他的論理和４２ａの出力と、スイッチＳＷ２２の出力との排他的論理和を取る。

【００３２】

この排他的論理和４３ａの出力は、第１段の段関数の入力の右側３２ビットとなる。なお、図５ａにおいて、排他的論理和の性質により４２ａと４３ａの順序は入れ替えても良い。

【００３３】

図５ｂにおいて、平文（６４ビット）を初期転置ＩＰ４１ａにより転置を行った結果は、等分され、右側３２ビットと左側３２ビットとなる。排他的論理和４４ｂは、左側３２ビットのデータと、スイッチＳＷ２１の出力との排他的論理和を取る。これにより、図５ａの排他的論理和４３ａにおいて加えたマスクの影響を除去する。排他的論理和４４ｂの出力は、最終転置ＩＰ$^{-1}$　　４１ｂに入力される。排他的論理和４２ｂは、右側３２ビットのデータと、スイッチＳＷ１４の出力との排他的論理和を取る。排他的論理和４３ｂは、排他的論理和４２ｂの出力と、スイッチＳＷ２２の出力との排他的論理和を取る。これにより、図５ａの排他的論理和４４ａにおいて加えたマスクの影響を除去する。排他的論理和４３ｂの出力は、最終転置ＩＰ$^{-1}$　　４１ｂに入力される。なお、図５ｂにおいて、排他的論理和の性質により４２ｂと４３ｂの順序は入れ替えても良い。

【００３４】

図４、図５ａ　および図５ｂで示した構成の特徴を以下に述べる。

【００３５】

排他的論理和４４ａ、４２ａ、および４３ａは、マスクａおよびｂなどのマスクにより、データを秘匿する。これにより、データ攪拌部において、左側３２ビットのデータおよび右側３２ビットのデータを外界から観測することが困難となる。しかし、上記マスクによるデータの秘匿を行った場合、図２の各Ｓ　箱１４への入力が本来の平文データのものと異なる結果となる。したがって、各Ｓ　箱１４の出力も異なる結果、出力される暗号文が本来の平文データに対応したもので無くなる。

【００３６】

上記問題点を解消するために、各段の段関数においては、図４の排他的論理和２５において、マスクｂあるいはマスクｂ$^{-}$と排他的論理和を行う。これにより、図５ａ　において

加えたマスクｂまたはｂ¯による秘匿の影響を除去する。
【００３７】
さらに、スイッチＳＷ１２で０側の分岐の場合、排他的論理和３２ａ　において、図５ａ　で加えたマスクａ　による秘匿の影響を除去する。すなわち、Ｓ　２９の入力は、本来の平文入力の場合と同じ入力となる。Ｓ　２９の出力は、排他的論理和３３ａ　において、マスクａ　により再び秘匿される。ここで、処理ブロック３４ａ　は事前計算によりテーブル参照で行われるので、外界から、Ｓ　２９の直接の入出力に関係した電力消費のデータの有意な変異を観測することはできない。
【００３８】
図４の排他的論理和２４により、右側３２ビットのデータに加えたマスクａ　あるいはマスクａ¯の影響を一旦除去する。しかし、右側３２ビットのデータは依然、マスクｂあるいはマスクｂ¯により秘匿されているので安全である。右側３２ビットのデータは次段の左側３２ビットのデータになり、排他的論理和３１において転置Ｐ　３０の出力と排他的論理和を行うことにより、再び、マスクａ　（あるいはマスクａ¯）およびマスクｂ（あるいはマスクｂ¯）によって秘匿され、その次の段の右側入力となる。したがって、上述の通り、各段の各Ｓ　箱における変換のＤＥＳ　との同一性は保たれる。
【００３９】
また、最終段の出力においては、図５ａ　において加えた各マスクの秘匿の影響を除去するため、図５ｂに示した、各マスクによる排他的論理和を行う。
【００４０】
スイッチＳＷ１１、ＳＷ１２、ＳＷ１３、およびＳＷ１４は、乱数列｛Ｒ　１ｉ｝によって制御する。スイッチＳＷ２１、ＳＷ２２、およびＳＷ２３は、乱数列｛Ｒ２ｉ｝によって制御する。例えば、各スイッチは、Ｒｊｉ＝０のとき０側の分岐を、Ｒｊｉ　＝１のとき１側の分岐を選ぶ。スイッチの制御を行う乱数列｛Ｒ　１ｉ｝および｛Ｒ　２ｉ｝は、各ブロックの暗号化および復号の処理ごとに変化させることを特徴とする。例えば、ある暗号化の処理では各段のスイッチＳＷ１１、ＳＷ１２、ＳＷ１３、およびＳＷ１４はすべて０側で処理を行い、別の暗号化では、各段のスイッチＳＷ１１、ＳＷ１２、ＳＷ１３、およびＳＷ１４はすべて１側で処理を行う。
【００４１】
乱数列｛Ｒ　１ｉ｝と乱数列｛Ｒ２ｉ｝に明白な依存関係があった場合、攻撃者にマスクａ　とマスクｂを推測する手がかりを与えることになるので、乱数列｛Ｒ　１ｉ｝と乱数列｛Ｒ２ｉ｝には明らかな依存関係を持たない乱数列を用いる。
【００４２】
理想的には、統計的に独立な２つの乱数列を用いることが推奨される。
【００４３】
ただし、実際には、統計的依存関係が存在しても、その影響が充分小さければ、ＤＰＡ対策として有効である。本発明を実装する手段として２つのｍ系列生成器を用意して、第１のｍ系列生成器の出力を｛Ｒ１ｊ｝、第２のｍ系列生成器の出力を｛Ｒ２ｊ｝とすることが考えられる。ｍ系列の周期が充分長く２つのｍ系列生成器の系列長、対応する規約多項式式、初期値の一部または全部が異なるようにすれば上記条件を充分満たすと考えられる。連数列の別な実現手段として、１つのｍ系列生成器を用意し、それを１回の暗号化または復号の処理毎に２ビットを生成させ、その第１ビットを｛Ｒ　１ｊ｝、第２ビットを｛Ｒ　２ｊ｝として用いることが考えられる。
【００４４】
ここではｍ系列生成器を具体例として挙げたが、実用上安全と考えられる乱数列生成器なら何を用いても良い。なお、この乱数列が外部からは推測されない様に実装する必要がある。あるいは別な実現手段として、乱数列をあらかじめ記憶装置に蓄えておき、それを順次参照することも可能である。なお、この乱数列が外部からは推測されない様に実装する必要がある。
【００４５】

図４、図５ａ、および図５ｂにおいて、ビット列の１の数、すなわちハミング重みをＨ（ａ）で定義する。ＤＰＡ　では、データ暗号化処理に伴う消費電力の差異を観測して暗号化鍵に関する情報を収集する。上記マスクを用いたデータの隠蔽により、外界からの消費電力の計測と処理されるデータの対応をとることが困難となる。しかし、マスクのハミング重みに差異がある場合、複数の暗号化処理データの計測と統計情報により、マスクａとｂのみを用いているデータのみを抽出することができる可能性がある。そして、そのようなデータのみの抽出が可能ならば、ＤＰＡの手法を用いることにより、従来の場合同様に鍵の抽出が可能となる。このように使用されているマスクがａ　なのかａ¯なのかの区別ができて充分な対策にならない。例えば、マスクａ　とａ¯あるいはマスクｂとｂ¯のハミング重みが同じとすれば、外界からの計測でマスクを判別することは困難となり安全であるが、逆に、マスクのビット重みに偏りがあるならば、安全性は著しく劣化する。

【００４６】

したがって、図４、図５ａ、および図５ｂにおいて、Ｈ（ａ）＝Ｈ（ａ¯）＝Ｈ（ｂ）＝Ｈ（ｂ¯）＝ｎ／２＝１６の条件を満たすマスクの選択（以下、マスクのハミング重みが等しい）ならば安全性は高い。ここでマスクａおよびｂのビット数ｎは３２であるので、マスクａ、マスクｂ、およびそれらのビット反転のビット重みがそれぞれ１６であるマスク値を使用することが推奨される。ただし、理想的には上記のようにマスクのハミング重みがマスクのビット長の丁度半分であるマスクを使用することが推奨されるが、ハミング重みがほぼ等しい２つのマスクを用い同様の効果が得られる。

【００４７】

すなわち、各マスクのハミング重みが極端に偏っていなければ、外界からの計測でマスクを判別することは容易でなく、ＤＰＡ対策としての効果が得られる。

【００４８】

さらに、図４のＤＥＳ　の拡大転置２６の特性に着目する。上記ハミング重みに着目したマスク値の選択と同様の理由から、排他的論理和３２ａ　および３２ｂにおいて加えられる、Ｅ　（ａ　）とＥ　（ａ¯）のハミング重みが等しくなるマスクを選択する。すなわち、Ｈ　（Ｅ（ａ））＝Ｈ　（Ｅ（ａ¯））を満足するマスクを選択する。

【００４９】

上記マスクの条件をＤＥＳ　の実装に当てはめると、例えばマスクａ　に対しては、マスクａ　を４ビットづつ区切ったときの各ブロックの“第１ビット”（左端のビット）の１の数＝マスクａ　を４ビットづつ区切ったときの各ブロックの“第４ビット”（右端のビット）の１の数＝４の条件を満たすことを要求する。すなわち、上記条件を満たすマスクａ　およびマスクｂの選択を特徴とする。上記条件を満たすマスク値の例として、（１００００１１１１０１１０１１１１００１０１００１００００１）$_2$　　や（１１０１１０１００１１００１０１００１１０１０１１００００１０１０）$_2$　　などが使用できる。

【００５０】

ただし、理想的には上記条件を満たすマスク値を使用することが推奨されるが、「マスクａ　を４ビットづつ区切ったときの各ブロックの“第１ビット”の１の数」と「マスクａ　を４ビットづつ区切ったときの各ブロックの“第４ビット”の１の数」が、極端に偏っていなければ同様の効果が得られる。

【００５１】

なお、上記条件を満たすマスク値を使用する場合において、スイッチを制御する乱数列｛Ｒ　１ｊ｝と｛Ｒ　２ｊ｝が自明な相関を持たないならば、マスクａ　とマスクｂが同一のマスク値であっても、ＤＰＡ　対策として有効である。

【００５２】

図１に示したＤＥＳ　の構成は最も広く知られているものであるが、処理の高速化をねらい、様々な等価変形を施したＤＥＳ　の構成法が知られている。

【００５３】

以下、本発明をＤＥＳ　に適用した場合における変形例について説明する。

【００５４】
図１０はＤＥＳ　の等価変形の例である。図１０に示すＤＥＳ　の実装においては、処理の効率化のために、拡大転置Ｅ　１１と転置Ｐ　１５を一つの転置にまとめＥＰ５３として処理している。入力された平文５８を初期転置ＩＰ５７において転置を行った出力は、二つに等分され、右側３２ビットは拡大転置Ｅ　５１ａ　に入力され、左側３２ビットは拡大転置Ｅ　５１ｂに入力される。拡大転置Ｅ５１ａの出力４８ビットは第一段の入力の右側４８ビットである。拡大転置Ｅ５１ｂの出力４８ビットは第一段の入力の左側４８ビットである。入力の右側４８ビットは排他的論理和５５において、拡大鍵Ｋ１と排他的論理和が行われ、Ｓ箱５４に出力される。Ｓ箱５４はテーブル参照により対応する出力をＥＰ５３に出力する。ＥＰ５３において、入力は転置が行われ、排他的論理和５６に出力される。排他的論理和５６において、拡大転置Ｅ５１ｂの出力である左側４８ビットと、ＥＰ５３の出力の排他的論理和が行われ、次段の入力の右側４８ビットになる。上記第１段の処理を第１６段まで繰り返す。第１６段の出力において、右側４８ビットは縮約転置Ｅ$^{-1}$５２ａに入力され、左側４８ビットは縮約転置Ｅ$^{-1}$５２ｂに入力され、それぞれの出力３２ビットは最終転置ＩＰ$^{-1}$５９に入力され、６４ビットの暗号文６０が出力される。
【００５５】
このような変形版ＤＥＳ　に本発明を適用し、ＤＰＡ　を防止する手法を以下に示す。
【００５６】
図１１は図１０で示したＤＥＳの実装に対する、本発明の一実施形態である。図１１において、Ｅ（ａ）／Ｅ（ａ$^{-}$）は図３に示した、排他的論理和によるスイッチＳＷ２３のマスクの加え方を表す。すなわち、Ｅ（ａ）／Ｅ（ａ$^{-}$）はＥ（ａ）もしくはＥ（ａ$^{-}$）によるマスクを表す。
【００５７】
図１１は、図１０で示したＤＥＳの実装に対しても、図４、図５ａ、および図５ｂで示した本発明の適用が可能であることを示す一実施形態である。
【００５８】
入力された平文に初期転置を行った出力は、二つに等分され、右側３２ビットは拡大転置Ｅ　６１ａに入力され、左側３２ビットは拡大転置Ｅ　６１ｂに入力される。拡大転置Ｅ６１ａの出力４８ビットは排他的論理和６４において、マスクＥ（ａ）／Ｅ（ａ$^{-}$）と排他的論理和が行われ、排他的論理和６５に出力される。排他的論理和６５において、排他的論理和６４の出力はマスクＥ（ｂ）／Ｅ（ｂ$^{-}$）と排他的論理和が行われ、第１段の入力の右側４８ビットになる。なお、排他的論理和の性質により、排他的論理和６４と６５の順序を入れ替えても良い。
【００５９】
拡大転置Ｅ６１ｂの出力４８ビットは排他的論理和６９において、マスクＥ（ｂ）／Ｅ（ｂ$^{-}$）と排他的論理和が行われ、第１段の入力の左側４８ビットになる。
【００６０】
入力の右側４８ビットは、排他的論理和６６において、マスクＥ（ａ）／Ｅ（ａ$^{-}$）と排他的論理和が行われ、次段の入力の左側４８ビットになる。入力の右側４８ビットは、排他的論理和６７において、マスクＥ（ｂ）／Ｅ（ｂ$^{-}$）と排他的論理和が行われ、排他的論理和６８に出力される。排他的論理和６７の出力は、排他的論理和６８において、拡大鍵Ｋ１と排他的論理和が行われ、Ｓ＾６２に出力される。Ｓ＾６２の構造については後述する。ＳＳ＾６２の出力はＥＰ６３により転置が行われ、排他的論理和７０に出力される。
【００６１】
排他的論理和７０において、入力データの左側４８ビットと、ＥＰ６３の出力は排他的論理和が行われ、次段の入力の右側４８ビットになる。上記第１段の処理を第１６段まで繰り返す。最終段の出力においては、第１段への入力で述べた処理の逆を行う。すなわち、右側４８ビットには排他的論理和６５、排他的論理和６４および縮約転置Ｅ$^{-1}$を行い、

左側４８ビットには排他的論理和６５および縮約転置Ｅ$^{-1}$を行い、それぞれの出力３２ビットづつを最終転置に出力する。

【００６２】

図１２は図１１に示したＳ＾６２の構造を示す図である。

【００６３】

図１２において、α＝Ｅ（ａ）、α^{-}＝　Ｅ（ａ$^{-}$）と表す。Ｓ＾６２の入力は、排他的論理和７１において、マスクαあるいはマスクα^{-}と排他的論理和が行われ、Ｓ箱７２に入力される。Ｓ箱７２の出力は、排他的論理和７３において、マスクＰ$^{-1}$Ｅ$^{-1}$（α）あるいはマスクＰ$^{-1}$Ｅ$^{-1}$（α^{-}）と排他的論理和が行われ、Ｓ＾６２の出力となる。

【００６４】

すなわち、図１２の７４は、本発明においては図４に示したスイッチＳＷ１２およびスイッチＳＷ１１を含む、処理ブロック３４ａと３４ｂに対応する。ただし、７４の処理は、暗号化および復号の処理中に行ってはならない。なぜならば、上記マスクによるデータの秘匿を行っていても、Ｓ箱７２の入出力は秘匿されていないため、Ｓ箱の処理による消費電力の差異を用いた解読が試みられる可能性があるからである。

【００６５】

本発明の実施形態においては、暗号化および復号を行う前に、事前計算により７４の処理結果を作成し、暗号化および復号処理で使用することを特徴とする。例えば、各Ｓ箱について、Ｓ箱の入力のインデックスと出力を書き換えたテーブルを用意し、Ｓ＾として暗号化および復号の処理に用いる。このとき、マスクαに対応したＳ＾のテーブルとマスクα^{-}に対応したＳ＾のテーブルがＳ箱に用意される。

【００６６】

図１３はＤＥＳ　の等価変形の別の例である。

【００６７】

図１３に示すＤＥＳ　の実装においては、処理の効率化のために、拡大転置Ｅ　１１と転置Ｐ　１５を一つの転置にまとめＥＰ８３として処理している。入力された平文８８を初期転置ＩＰ８７において転置を行った出力は、二つに等分され、右側３２ビットは転置Ｐ$^{-1}$８１ａ　に入力され、左側３２ビットは転置Ｐ$^{-1}$８１ｂに入力される。転置Ｐ$^{-1}$８１ａの出力３２ビットは第一段の入力の右側３２ビットである。転置Ｐ$^{-1}$８１ｂの出力３２ビットは第一段の入力の左側３２ビットである。入力の右側３２ビットはＥＰ８３に入力され、拡大転置を行われた結果が排他的論理和８５に出力される。排他的論理和８５において、拡大鍵Ｋ１と排他的論理和が行われ、Ｓ箱８４に出力される。Ｓ箱８４はテーブル参照により対応する出力を排他的論理和８６に出力する。排他的論理和８６において、拡大転置Ｅ８１ｂの出力である左側３２ビットと、Ｓ箱８４の出力の排他的論理和が行われ、次段の入力の右側３２ビットになる。上記第１段の処理を第１６段まで繰り返す。

【００６８】

第１６段の出力において、右側３２ビットは転置Ｐ８２ａに入力され、左側３２ビットは転置Ｐ８２ｂに入力され、それぞれの出力３２ビットは最終転置ＩＰ$^{-1}$８９に入力され、６４ビットの暗号文９０が出力される。このような変形版ＤＥＳ　に本発明を適用し、ＤＰＡ　を防止する手法を以下に示す。

【００６９】

図１４は図１３で示したＤＥＳの等価変形の例に対する、本発明の一実施形態である。

【００７０】

図１４において、Ｐ$^{-1}$（ａ）／Ｐ$^{-1}$（ａ$^{-}$）は図３に示した、排他的論理和によるスイッチＳＷ２３のマスクの加え方を表す。すなわち、Ｐ$^{-1}$（ａ）／Ｐ$^{-1}$（ａ$^{-}$）はＰ$^{-1}$（ａ）もしくはＰ$^{-1}$（ａ$^{-}$）によるマスクを表す。

【００７１】

図１４は、図１３で示したＤＥＳの実装に対しても、図４、図５ａ、および図５ｂで示し

た本発明の適用が可能であることを示す一実施形態である。

【００７２】

入力された平文に初期転置を行った出力は、二つに等分され、右側３２ビットは転置Ｐ$^{-1}$９１ａ に入力され、左側３２ビットは転置Ｐ$^{-1}$９１ｂに入力される。転置Ｐ$^{-1}$９１ａの出力３２ビットは排他的論理和９４において、Ｐ$^{-1}$（ａ）／Ｐ$^{-1}$（ａ$^{-}$）と排他的論理和が行われ、排他的論理和９５に出力される。排他的論理和９５において、排他的論理和９４の出力はマスクＰ$^{-1}$（ｂ）／Ｐ$^{-1}$（ｂ$^{-}$）と排他的論理和が行われ、第１段の入力の右側３２ビットになる。転置Ｐ$^{-1}$９１ａの出力３２ビットは排他的論理和９４において、マスクＰ$^{-1}$（ｂ）／Ｐ$^{-1}$（ｂ$^{-}$）と排他的論理和が行われ、第１段の入力の左側３２ビットになる。なお、排他的論理和の性質により、排他的論理和９４と９５の順序を入れ替えても良い。

【００７３】

入力の右側３２ビットは、排他的論理和９６において、マスクＰ$^{-1}$（ａ）／Ｐ$^{-1}$（ａ$^{-}$）と排他的論理和が行われ、次段の入力の左側３２ビットになる。入力の右側３２ビットは、排他的論理和９７において、マスクＰ$^{-1}$（ｂ）／Ｐ$^{-1}$（ｂ$^{-}$）と排他的論理和が行われ、ＥＰ９３に出力される。ＥＰ９３において拡大転置を行った結果の４８ビット出力は、排他的論理和９８に出力され、拡大鍵Ｋ１と排他的論理和が行われ、Ｓ＾９２に出力される。Ｓ＾９２の構造については後述する。Ｓ＾９２の出力は、排他的論理和１００に出力され、入力データの左側３２ビットと、排他的論理和が行われ、次段の入力の右側３２ビットになる。上記第１段の処理を第１６段まで繰り返す。

【００７４】

最終段の出力においては、第１段への入力で述べた処理の逆を行う。すなわち、右側３２ビットには排他的論理和９５、排他的論理和９４および転置Ｐを行い、左側３２ビットには排他的論理和９５および転置Ｐを行い、それぞれの出力３２ビットづつを最終転置に出力する。

【００７５】

図１５は図１４に示したＳ＾９２の構造を示す図である。

【００７６】

図１５において、α＝Ｐ$^{-1}$（ａ）、α^{-}＝Ｐ$^{-1}$（ａ$^{-}$）と表す。

【００７７】

Ｓ＾９２の入力は、排他的論理和１０１において、マスクαあるいはマスクα^{-}と排他的論理和が行われ、Ｓ箱１０２に入力される。

【００７８】

Ｓ箱１０２の出力は、排他的論理和１０３において、マスクＰ$^{-1}$Ｅ$^{-1}$（α）あるいはマスクＰ$^{-1}$Ｅ$^{-1}$（α^{-}）と排他的論理和が行われ、Ｓ＾９２の出力となる。すなわち、図１５の１０４は、本発明においては図４に示したスイッチＳＷ１２およびスイッチＳＷ１１を含む、３４ａと３４ｂに対応する。ただし、１０４の処理は、暗号化および復号の処理中に行ってはならない。なぜならば、上記マスクによるデータの秘匿を行っていても、Ｓ箱１０２の入出力は秘匿されていないため、Ｓ箱の処理による消費電力の差異を用いた解読が試みられる可能性があるからである。すなわち、本発明の実施形態においては、暗号化および復号を行う前に、事前計算により１０４の処理結果を作成し、暗号化および復号処理で使用することを特徴とする。例えば、各Ｓ箱について、Ｓ箱の入力のインデックスと出力を書き換えたテーブルを用意し、Ｓ＾として暗号化および復号の処理に用いる。

【００７９】

このとき、マスクαに対応したＳ＾のテーブルとマスクα^{-}に対応したＳ＾のテーブルがＳ箱に用意される。

【００８０】

次に、図１６、図１７、および図１８を用いて本発明を鍵スケジュール部に適用した一実施形態を説明する。

【００８１】
真の鍵のビットパターンＫをマスクするマスクパターンｃとそのビット反転パターンｃ－を用意し、Ｋを指定された２項演算を用いてｃによって変換した値をＫｃとし、また同じ２項演算を用いてＫをｃ－によって変換した値をＫｃ－とし、ＫｃとＫｃ－をあらかじめ記憶装置に記憶しておき、暗号化または復号を実施する度にランダムにＫｃとＫｃ－の一方を選択し、それを真の鍵と同様の処理によって処理し、平文に対して前記２項演算によって作用させると共に、その２項演算の出力からｃまたはｃ－の対応するパターンの影響を前記２項演算の逆変換により除去する。２項演算として排他的論理和を用いる暗号方式の例としてＤＥＳ　方式に本発明を適用した場合の例を示す。まず、鍵ＫｃとＫｃ－の２つのマスクされた鍵を用意する。

【００８２】
Ｋｃ　＝　Ｋ　（＋）　ｃ
Ｋｃ－＝　Ｋ　（＋）　ｃ－
但し、記号（＋）　はビット毎の排他的論理和を表す。

【００８３】
暗号化または復号に先立ってまずＫｃ，Ｋｃ－のいずれか一方をランダムに選択し、ＤＥＳ　の鍵スケジュール処理を行い、順次１６通りの拡大鍵を生成する。Ｋｃから拡大された１６個の鍵は記号Ｋｃｉ（ｉ＝１、…１６）で表し、Ｋｃ－から拡大された鍵はＫｃ－ｉ　（ｉ＝１、…１６）であらわす。Ｋｃから拡大された拡大鍵はマスクｃの影響を、またＫｃ－から拡大された拡大鍵はマスクｃ－の影響をそれぞれ受けている。その影響はＤＥＳ　の鍵スケジュール処理により定まるが、ここでは、マスクを掛けていない真の鍵Ｋを鍵スケジュールで拡大した鍵をＫｉ（ｉ＝１、…１６）と表し、ＫｉとＫｃｉの排他的論理和をｃｉとし、ＫｉとＫｃ－ｉの排他的論理和をｃ－ｉ　とする。すなわちｃｉ＝　Ｋｉ　（＋）Ｋｃｉ
ｃ－ｉ　＝　Ｋｉ　（＋）　Ｋｃ－ｉ
ＤＥＳ　において各拡大鍵Ｋｉは拡大転置Ｅの直後にビット毎の排他的論理和演算によってメッセージに作用させられる。本発明においては、Ｋｉの代わりにＫｃｉまたはＫｃ－ｉを作用させる。Ｋｃｉを作用させた場合にはＫ　ｃｉを作用させた後に、ｃｉを排他的論理和によって作用させてその影響を取り除き、Ｋｃ－ｉを作用させた場合にはｃｉ－を作用させた後に、排他的論理和演算で作用させその影響を取り除く。ｃｉ、ｃｉ－はそれぞれｃおよびｃ－をＤＥＳ　の鍵スケジュールで拡大鍵同様に拡大することによって得られる。ｃｉやｃｉ－は暗号化または復号の度に選択されたマスクｃまたはｃ－から作成してもよい。但し、外部からの観測に対して最も漏洩する情報が少ない方法は、あらかじめｃｉとｃ－ｉをすべて計算しておくことである。その場合、４８ビットのマスク１６通りを２セット、合計１５３６ビットあらかじめ用意することになる。このマスクは例えばＩＣカードに本発明を適用した場合、少なくともカード毎固定で良いので、ｃｉ，ｃ－ｉはＲＯＭに書き込んでおくことができる。このことはメモリ量の制約が強いＩＣカードにおいては特に重要である。一般に同じビット数を記憶する場合、ＲＡＭ　やＥＥＰＲＯＭに比べＲＯＭ　の面積は小さい。従って１５３６ビットのマスクをＲＯＭ　に記憶させることはＲＡＭ　やＥＥＰＲＯＭに記憶させるのに比べＬＳＩチップ面積の使用効率が高くなる。

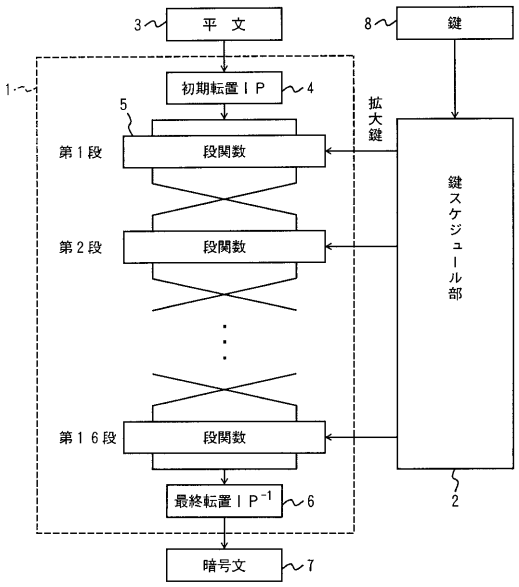
【００８４】
図１６にＤＥＳ　の鍵スケジュールを示す。

【００８５】
図中（ＰＣ－１）１１１と（ＰＣ－２）１１３はビットの選択と転置を組み合わせた関数であり、記号ＲＯＴ１１２は巡回シフト演算を表す。外部から入力された６４ビットの鍵Ｋ１１５は（ＰＣ－１）１１１により、その内８ビットが捨てられ、２８ビットの２つのビット列が巡回シフト１１２に渡される。巡回シフトされた合計５６ビットのデータはＰＣ－２変換１１３に入力され、拡大鍵４８ビットが出力される。図では１段分の拡大鍵のみ出力しているが、巡回シフトとＰＣ－２を繰り返すことによって２、３、．．．、１６

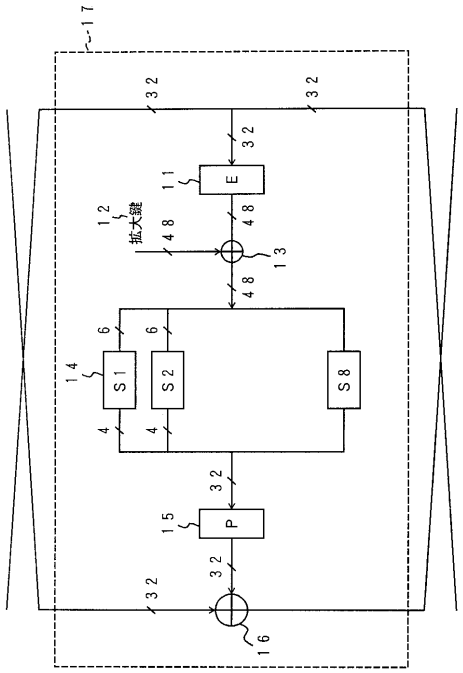
段の拡大鍵を生成する。
【００８６】
図１７は鍵スケジュール部に本発明を適用した場合の処理の流れを表している。
【００８７】
鍵スケジュールの鍵入力段ではスイッチＳＷ３１により、ＫｃとＫｃ－からランダムにほぼ１　／２　の確率で選択し、鍵スケジュール部１２２に入力される。以下の鍵スケジュール部内での処理は通常のＤＥＳ　の鍵スケジュール処理と同じである。出力される拡大鍵１２３は入力された鍵がＫｃであれば、Ｋｃｉ、Ｋｃ－の時にはＫｃ－ｉとなる。
【００８８】
図１８はマスクの影響を受けた拡大鍵を各ラウンド関数においてメッセージに作用させる様子を示している。
【００８９】
ＫｃｉまたはＫｃ－ｉの一方をメッセージに作用させる方法は、通常の場合Ｋｉを作用させるのとまったく同じであり、拡大転置Ｅ１３１の出力４８ビットに、排他的論理和１３２において拡大鍵ＫｃｉまたはＫｃ－ｉをビット毎の排他的論理和演算によって作用させる。こうして作用させた結果はマスクｃまたはｃ－の影響を受けているのでこのままＳ箱に入力させると正しい暗号変換ができなくなる。従ってＳ箱に入力する前にマスクｃまたはｃ－の影響を取り除く処理が必要である。具体的にはマスクの影響がｃｉの場合、ｃｉを排他的論理和１３３によってＳ箱１３４の入力前に作用させる。排他的論理和の逆変換は排他的論理和であるので、これによってｃｉの影響が除去できる。マスクの影響がｃ－ｉの場合も同様である。
【００９０】
本実施形態においてマスクｃ－はマスクｃのビット反転に選べば、拡大鍵の各ビットは１と０の値をほぼ均等に採る。これによって、暗号装置外部からの種々の観測に対して鍵に関する情報の漏洩を無くすことができる。漏洩する情報をできる限り少なくするには、さらにｃｉとｃ－ｉのハミング重みが近い値をとることが望ましい。但しｃｉはｃを鍵スケジュールに通した結果であり全ての段のｃｉのハミング重みを完全にコントロールすることは困難である。そこで、例えば元のマスクｃのハミング重みがビットサイズの１／２であるように選ぶ方法が考えられる。
【００９１】
上述した実施形態においては、ＤＥＳ　方式への適用について詳しく述べたが、本発明はこれに限らず、排他的論理和の様な２項演算、ビット入れ替えに相当する転置、Ｓ　箱に相当する換字の３種の一部または全部を使用して構成される様な暗号方式全般に適用可能である。
【００９２】
【発明の効果】
本発明によれば、与えられた暗号化および復号処理の同一性を保証しつつ、ＤＰＡ　による解読を困難にすることにより、ＤＰＡ　に対する安全性を増大することができる。
【図面の簡単な説明】
【図１】ＤＥＳ　アルゴリズムの全体構成を示す図。
【図２】ＤＥＳ　の段関数の構成を示す図。
【図３】ＤＥＳの規格表に従うＳ箱の内容の一例を示す図。
【図４】本発明による段関数にマスクを加えた構成を示す図。
【図５】本発明による入力段及び最終段でマスクを加えた構成を示す図。
【図６】拡大転置Ｅの表を示す図。
【図７】転置Ｐの表を示す図。
【図８】マスクａの場合の、入力が（０００００００、０００００１、…１１１１１１）に対応する隠蔽されたＳ１の出力を示す図。
【図９】マスクａ－（ａのビット反転）のテーブルを示す図。
【図１０】ＤＥＳ　アルゴリズムの一実装例の構成を示す図。

【図１１】図１０の構成において、本発明による段関数にマスクを加えた構成を示す図。
【図１２】図１１のＳ＾の構成を示す図。
【図１３】ＤＥＳ　アルゴリズムの別の一実装例の構成を示す図。
【図１４】図１３の構成において、本発明による段関数にマスクを加えた構成を示す図。
【図１５】図１４のＳ＾の構成を示す図。
【図１６】ＤＥＳ　アルゴリズムの鍵スケジュール部の構成を示す図。
【図１７】本発明による鍵スケジュール部にマスクを加える構成を示す図。
【図１８】本発明による段関数に鍵スケジュール部で加えたマスクを加える構成を示す図
。
【符号の説明】
１…データ攪拌部
２…鍵スケジュール部
３…平文
４…初期転置ＩＰ
５…段関数
６…最終転置ＩＰ$^{-1}$
７…暗号文
８…鍵
１１…拡大転置Ｅ
１２…拡大鍵
１３…排他的論理和
１４…Ｓ箱
１５…転置Ｐ
１６…排他的論理和
１７…段関数
２４、２５、２７、３１、３２ａ、３２ｂ、３３ａ、３３ｂ…排他的論理和
２６…拡大転置Ｅ
２９…Ｓ箱
ＳＷ１１，ＳＷ１２、ＳＷ１３、ＳＷ２１、ＳＷ２２、ＳＷ２３…スイッチ
３４ａ、３４ｂ…処理
４２ａ、４３ａ、４４ａ、４２ｂ、４３ｂ、４４ｂ…排他的論理和
４１ａ…初期転置ＩＰ
４１ｂ…最終転置ＩＰ$^{-1}$

【図１】



【図２】

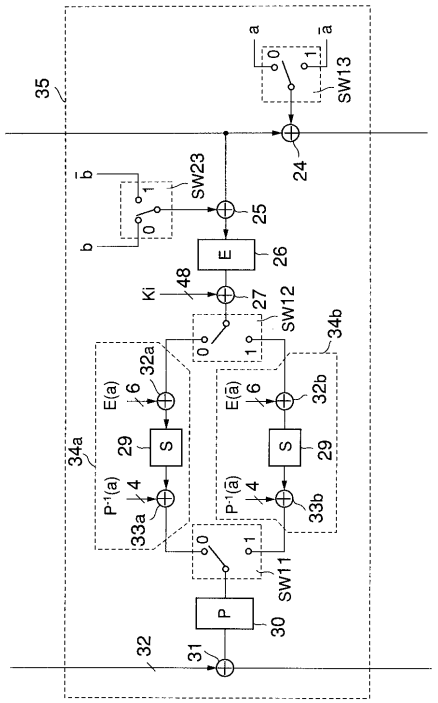


【図３】

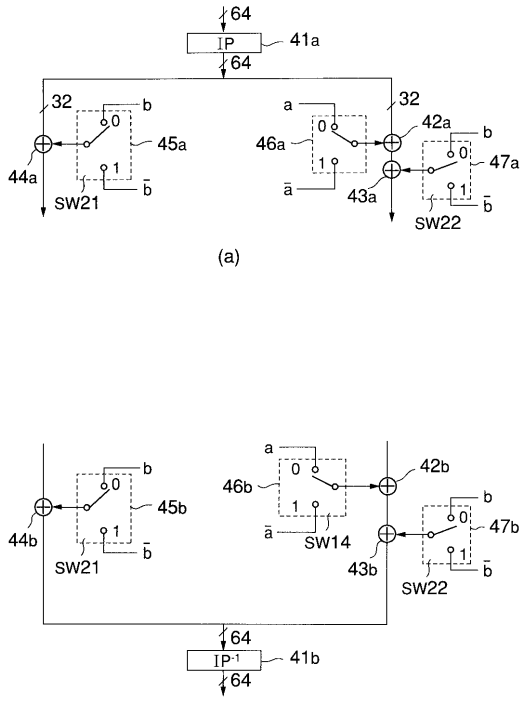
S１の表

14, 4, 13, 1, 2, 15, 11, 8, 3, 10, 6, 12, 5, 9, 0, 7,
0, 15, 7, 4, 14, 2, 13, 1, 10, 6, 12, 11, 9, 5, 3, 8,
4, 1, 14, 8, 13, 6, 2, 11, 15, 12, 9, 7, 3, 10, 5, 0,
15, 12, 8, 2, 4, 9, 1, 7, 5, 11, 3, 14, 10, 0, 6, 13,

【図４】



【図５】



【図６】

拡大転置Ｅの表

32, 1, 2, 3, 4, 5
4, 5, 6, 7, 8, 9
8, 9, 10, 11, 12, 13
12, 13, 14, 15, 16, 17
16, 17, 18, 19, 20, 21
20, 21, 22, 23, 24, 25
24, 25, 26, 27, 28, 29
28, 29, 30, 31, 32, 1

【図７】

転置Ｐの表

16, 7, 20, 21, 29, 12, 28, 17, 1, 15, 23, 26, 5, 18, 31, 10,
2, 8, 24, 14, 32, 27, 3, 9, 19, 13, 30, 6, 22, 11, 4, 25

【図８】

マスクａの場合の、入力が（000000, 000001, …, 111111）に
対応する隠蔽されたＳ１の出力

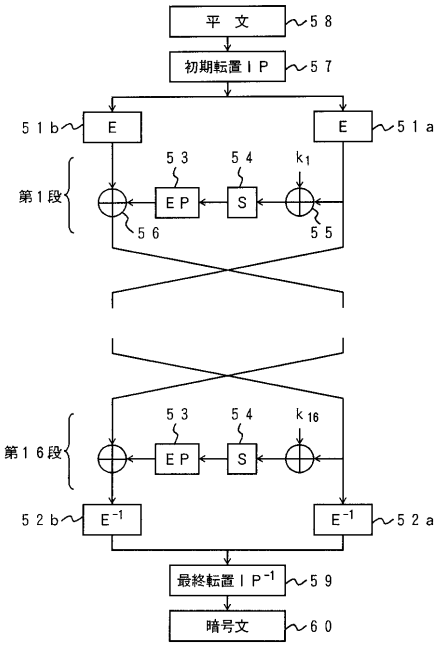
8 11 14 2 13 4 0 15 1 7 11 1 6 13 5 8 15 12 4 9 3 10 9
3 10 0 7 14 12 6 2 5 4 2 8 1 7 11 11 6 14 4 13 8 9 7 6
13 10 9 1 14 0 12 12 0 5 15 2 5 3 10 15 3

【図９】

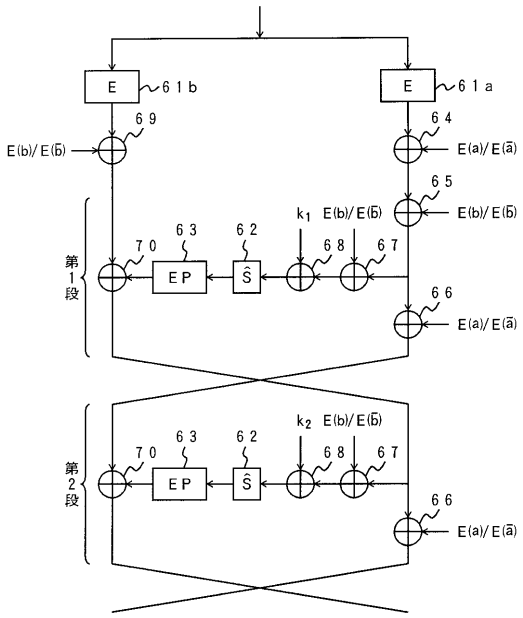
マスク$\bar{a}$（ａのビット反転）のテーブル

12 0 5 12 10 13 0 10 15 3 3 15 1 14 6 5 2 9 8 6 7 2 11 1 9 4 4 8 14 7 13 11 10 1
3 9 3 1 8 15 5 12 6 5 12 6 11 3 0 7 10 2 9 14 4 8 14 0 15 11 2 13 1 4 7

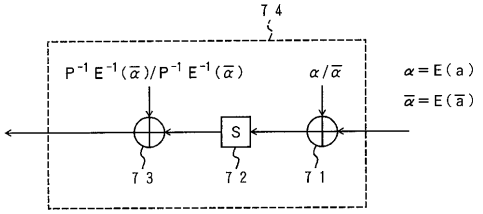
【図１０】



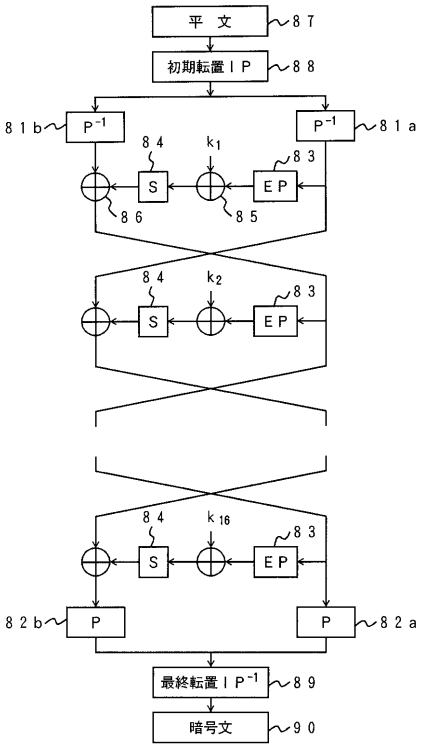
【図１１】



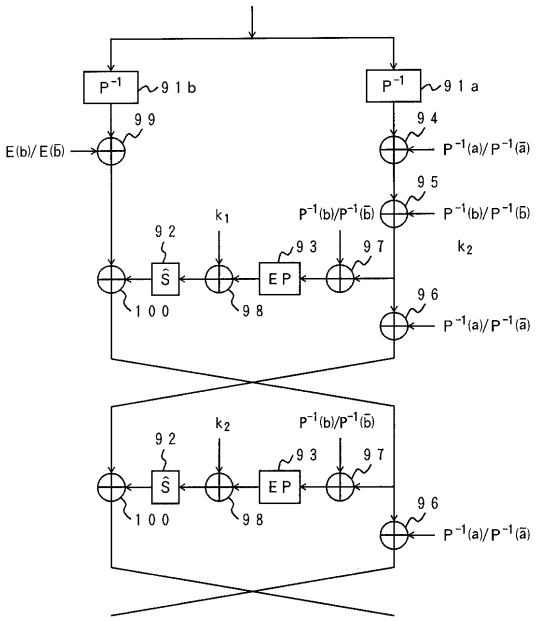
【図１２】



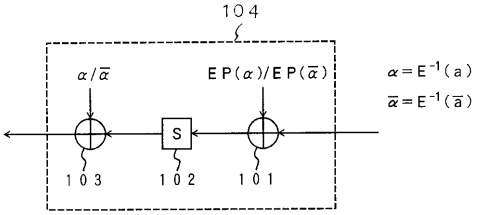
【図１３】



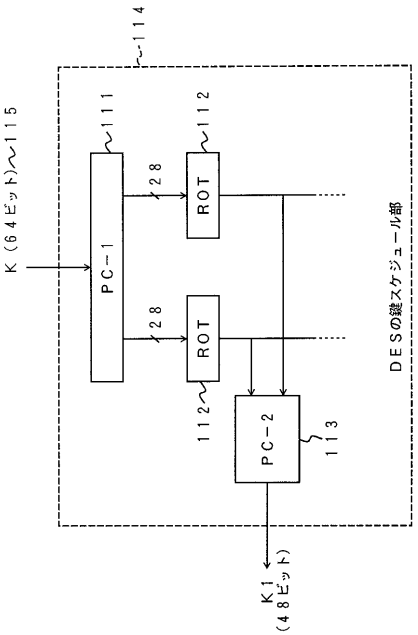
【図１４】



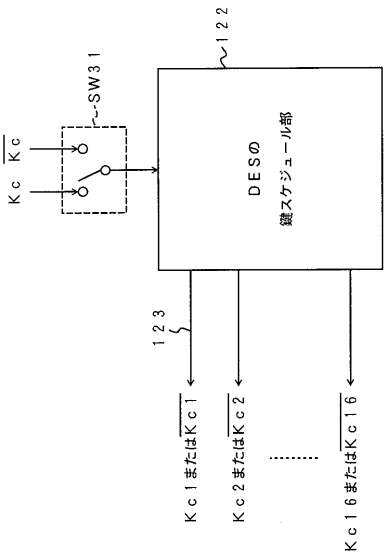
【図１５】



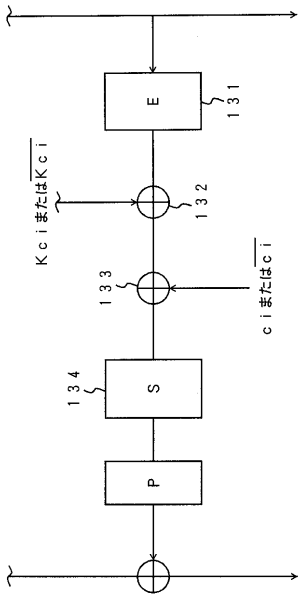
【図１６】



【図１７】



【図１８】



フロントページの続き

(74)代理人　100070437
　　弁理士　河井　将次
(72)発明者　川村　信一
　　東京都府中市東芝町１番地　株式会社東芝府中工場内
(72)発明者　佐野　文彦
　　東京都府中市東芝町１番地　株式会社東芝府中工場内

審査官　石田　信行

(56)参考文献　特開平１０－１５４９７６（ＪＰ，Ａ）
　　特開平０６－１６１３５３（ＪＰ，Ａ）
　　特開平０４－３６５２４０（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.^{7}，ＤＢ名)
　　G09C　1/00　610
　　H04L　9/06