

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2006-215281
(P2006-215281A)

(43) 公開日 平成18年8月17日(2006.8.17)

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

審査請求 未請求 請求項の数 3 O L (全 18 頁)

(21) 出願番号	特願2005-28116 (P2005-28116)	(71) 出願人	000001889 三洋電機株式会社 大阪府守口市京阪本通2丁目5番5号
(22) 出願日	平成17年2月3日(2005.2.3)	(74) 代理人	110000176 一色国際特許業務法人
		(72) 発明者	石村 静 大阪府守口市京阪本通2丁目5番5号 三洋電機株式会社内
		(72) 発明者	池谷 昭 大阪府守口市京阪本通2丁目5番5号 三洋電機株式会社内
		(72) 発明者	千明 一雅 大阪府守口市京阪本通2丁目5番5号 三洋電機株式会社内
		Fターム(参考)	5J104 AA18 AA32 JA13 NA10 NA22 NA25

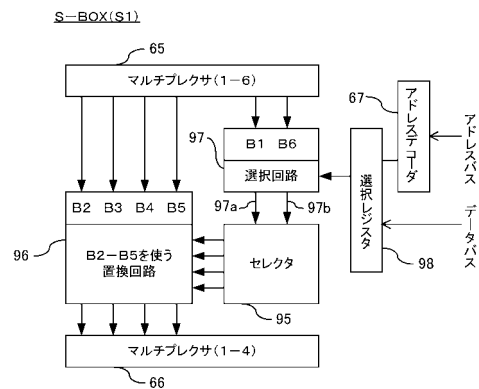
(54) 【発明の名称】 暗号処理回路

(57) 【要約】

【課題】 共通鍵ブロック暗号方式の換字処理を行う暗号処理回路において、ハードウェアを修正せずに換字処理における入力データと出力データとの対応規則を変更可能とすることにより、安全性を高める。

【解決手段】 複数ビットの入力データを変換して出力する共通鍵ブロック暗号方式の換字処理を行う暗号処理回路であって、前記入力データと、前記入力データの並べ替えを指示する選択データと、を受信し、前記入力データを前記選択データに基づいて並べ替えたデータを所定の対応規則に基づいて変換して出力する論理回路であることとする。

【選択図】 図16



【特許請求の範囲】

【請求項 1】

複数ビットの入力データを変換して出力する共通鍵ブロック暗号方式の換字処理を行う暗号処理回路であって、

前記入力データと、前記入力データの並べ替えを指示する選択データと、を受信し、前記入力データを前記選択データに基づいて並べ替えたデータを所定の対応規則に基づいて変換して出力する論理回路であることを特徴とする暗号処理回路。

【請求項 2】

請求項 1 に記載の暗号処理回路であって、

前記共通鍵ブロック暗号方式が DES であり、

前記所定の対応規則が、DES の S - B O X に入力されるデータと前記 S - B O X から出力されるデータとの対応規則であることを特徴とする暗号処理回路。

10

【請求項 3】

請求項 2 に記載の暗号処理回路であって、

前記論理回路は、

前記 S - B O X に入力される前記複数ビットの入力データの最上位ビット及び最下位ビットを前記選択データに基づいて並べ替えて出力する選択回路と、

前記選択回路から出力される前記複数ビットの入力データの最上位ビット及び最下位ビットと、前記複数ビットの入力データの最上位ビット及び最下位ビット以外のビットと、を前記所定の対応規則に基づいて変換して出力する換字回路と、

20

を備えることを特徴とする暗号処理回路。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、共通鍵ブロック暗号方式に用いられる暗号処理回路に関する。

【背景技術】

【0002】

近年、キーレスエントリーシステムのように、無線等の通信手段によりデータを送受信することが広く行われている。キーレスエントリーシステムの場合、第三者にデータが不正に解読されることのないよう、データは暗号化された上で送受信される。

30

【0003】

データの暗号化方式は多種多様であるが、DES (Data Encryption Standard) や AES (Advanced Encryption Standard) 等の標準規格を用いることが望ましい。これらの標準規格の暗号化方式の場合、不正に解読されるリスクの算出が容易であり、不正に解読された場合の保険料をこのリスクに基づいて算定することができるからである。逆に、標準規格以外の独自規格等の暗号化方式を用いる場合、不正に解読されるリスクの算出が難しく、概して、保険料が高くなることが多い。

【0004】

このような DES や AES 等の共通鍵ブロック暗号化方式では、データをいくつかのブロックに分割し、そのブロックごとに換字処理が行われる。この換字処理は、入力データと出力データとの対応を示す対応表をメモリに記憶しておき、与えられた入力データに対応する出力データを対応表に基づいて求めるといったソフトウェアによる処理により実現することもできる。

40

【0005】

しかし、換字処理をソフトウェアで実現する場合、メモリに記憶された対応表の参照等を繰り返し行うため、処理負荷が高く、消費電力が大きい。そのため、キーレスエントリーシステムに、換字処理がソフトウェアで実現された共通鍵ブロック暗号方式を採用すると、利用者が施錠・解錠の操作を行う子機の電池消耗が早くなり、また、施錠・解錠に対するレスポンスが低下してしまうという問題があった。そこで、共通鍵ブロック暗号方式

50

における換字処理等をハードウェアにより実現する方法が提案されている（例えば、特許文献１）。

【特許文献１】特開２００４－１７８５０７号公報

【発明の開示】

【発明が解決しようとする課題】

【０００６】

しかしながら、換字処理をハードウェアにより実現した場合、入力データと出力データとの対応規則が固定化されてしまう。そのため、差分攻撃法や線形攻撃法等によってその対応規則が解析されたような場合等に、ハードウェアを修正しないと換字処理における対応規則を変更することができず、安全性が十分ではなかった。

10

【０００７】

本発明は上記課題を鑑みてなされたものであり、共通鍵ブロック暗号方式の換字処理を行う暗号処理回路において、ハードウェアを修正せずに換字処理における入力データと出力データとの対応規則を変更可能とすることにより、安全性を高めることを目的とする。

【課題を解決するための手段】

【０００８】

上記目的を達成するため、本発明の暗号処理回路は、複数ビットの入力データを変換して出力する共通鍵ブロック暗号方式の換字処理を行う暗号処理回路であって、前記入力データと、前記入力データの並べ替えを指示する選択データと、を受信し、前記入力データを前記選択データに基づいて並べ替えたデータを所定の対応規則に基づいて変換して出力する論理回路であることとする。

20

【０００９】

また、前記共通鍵ブロック暗号方式がDESであり、前記所定の対応規則が、DESのS-BOXに入力されるデータと前記S-BOXから出力されるデータとの対応規則であることとすることができる。

【００１０】

さらに、前記論理回路は、前記S-BOXに入力される前記複数ビット（例えば６ビット）の入力データの最上位ビット及び最下位ビットを前記選択データに基づいて並べ替えて出力する選択回路と、前記選択回路から出力される前記複数ビットの入力データの最上位ビット及び最下位ビットと、前記複数ビットの入力データの最上位ビット及び最下位ビット以外のビットと、を前記所定の対応規則に基づいて変換して出力する換字回路と、を備えることとすることができる。

30

【発明の効果】

【００１１】

共通鍵ブロック暗号方式の換字処理を行う暗号処理回路において、ハードウェアを修正せずに換字処理における入力データと出力データとの対応規則を変更可能とすることにより、安全性を高めることができる。

【発明を実施するための最良の形態】

【００１２】

＝ 全体構成 ＝

図１は、本発明の暗号処理回路を用いる一実施形態である自動車の錠の施錠・解錠を行うキーレスエントリーシステム１の全体構成を示す図である。キーレスエントリーシステム１は、携帯型の子機２と自動車等に搭載される親機３とを含んで構成されている。子機２は、例えば、自動車のドアロックやステアリングロックの鍵穴に差し込むキーのハンドル部等に設けられている。また、親機３は、自動車側に設けられている。

40

【００１３】

子機２は、電池１１、操作スイッチ１２、データ処理回路１３、及び送受信回路１４を備えている。電池１１は、子機２の各部の動作に必要な電力を供給するためのものである。操作スイッチ１２は、利用者からの施錠・解錠の指示を受け付けるスイッチである。デ

50

ータ処理回路 1 3 は、施錠・解錠の際に必要な認証用のデータの生成等を行う。送受信回路 1 4 は、データ処理回路 1 3 から出力されるデジタルデータをアナログデータに変換し、これを増幅して電磁波として送出する回路である。また、送受信回路 1 4 は、親機 3 から送出された電磁波を受信し、これをデジタルデータに変換してデータ処理回路 1 3 に入力することもできる。なお、電磁波としては、電波や赤外線が用いられる。

【 0 0 1 4 】

親機 3 は、データ処理回路 2 1、送受信回路 2 2、及び駆動回路 2 3 を備えている。データ処理回路 2 1 は、子機 2 から受信する認証用のデータに基づいた認証処理等を行う。送受信回路 2 2 は、子機 2 から送出された電磁波を受信し、これをデジタルデータに変換してデータ処理回路 2 2 に入力する回路である。また、送受信回路 2 2 は、データ処理回路 2 1 から出力されるデジタルデータをアナログデータに変換し、これを増幅して電磁波として送出することもできる。駆動回路 2 3 は、自動車の錠を施錠・解錠するロック機構を作動させるアクチュエータ 2 4 に駆動信号を送信する回路である。なお、親機 2 の各部 2 1 ~ 2 3 には、自動車のバッテリー 2 5 から電力が供給されている。

10

【 0 0 1 5 】

== データ処理回路の構成 ==

図 2 は、データ処理回路 1 3 の構成を示す図である。データ処理回路 1 3 は、CPU 5 1 A、RAM (Random Access Memory) 5 2 A、EEPROM (Electrically Erasable Programmable Read-Only Memory) 5 3 A、乱数生成回路 5 4 A、暗号処理回路 5 5 A、及び入出力ポート 5 6 A を備えている。そして、各部 5 1 A ~ 5 6 A はバス 5 7 A により互いに通信可能に接続されている。

20

【 0 0 1 6 】

CPU 5 1 A は、データ処理回路 1 3 の全体を制御するものである。RAM 5 2 A には、CPU 5 1 A が使用する作業用データ等が記憶される。EEPROM 5 3 A は書き換え可能な不揮発性メモリであり、プログラムや保存用のデータ等が記憶されている。乱数生成回路 5 4 A は、暗号化の処理において用いられる疑似乱数又は物理乱数を生成する回路である。暗号処理回路 5 5 A は、共通鍵ブロック暗号方式における転置又は換字の処理を行う回路である。入出力ポート 5 6 A は、データ処理回路 1 3 の外部にある操作スイッチ 1 2 や送受信回路 1 4 等とデータの送受信を行うためのインタフェースである。

【 0 0 1 7 】

なお、本実施形態では、共通鍵ブロック暗号方式として DES (Data Encryption Standard) を用いることとする。このようなデータ処理回路 1 3 では、プログラムの実行や暗号処理回路 5 5 A の制御等により、DES の暗号化又は復号の処理が行われる。なお、データ処理回路 2 1 も同様の構成であり、CPU 5 1 B、RAM 5 2 B、EEPROM 5 3 B、乱数生成回路 5 4 B、暗号処理回路 5 5 B、入出力ポート 5 6 B、及び各部 5 1 B ~ 5 6 B を互いに通信可能に接続するバス 5 7 B を備えている。

30

【 0 0 1 8 】

== 通信手順 ==

図 3 は、キーレスエントリーシステム 1 の子機 2 と親機 3 との間における通信手順を示すフローチャートである。まず、子機 2 の操作スイッチ 1 2 の操作等により送信処理が起動される (S 3 0 1)。子機 2 のデータ処理回路 1 3 は、EEPROM 5 3 A に記憶されている車番 (車体番号) を親機 3 に送信する (S 3 0 2)。親機 3 のデータ処理回路 2 1 は、子機 2 から車番が送信されてくるのを待機しており (S 3 0 3)、子機 2 から送信されてくる車番を受信すると、当該車番を EEPROM 5 3 B に記憶されている車番と比較する (S 3 0 4)。

40

【 0 0 1 9 】

車番が一致しない場合 (S 3 0 4 : N G)、親機 3 のデータ処理回路 2 1 は、別の自動車の車番が送信されてきたと判断し、受信待機処理に戻る (S 3 0 3)。車番が一致すると (S 3 0 4 : O K)、データ処理回路 2 1 は、乱数生成回路 5 4 B を用いて 6 4 ビットの一時鍵 R 0 を生成する (S 3 0 5)。そして、データ処理回路 2 1 は、この一時鍵 R 0

50

を、EEPROM 53Bに記憶されている共通鍵Kを用いてDESで暗号化して子機2に送信する(S306)。

【0020】

子機2のデータ処理回路13は、親機3から送信されてくる暗号化された一時鍵R0を受信すると、EEPROM 53Aに記憶されている共通鍵Kを用いて一時鍵R0を復号する(S307)。続いて、データ処理回路13は、乱数生成回路54Aを用いて64ビットの一時鍵R1を生成する(S308)。そして、データ処理回路13は、この一時鍵R1を親機3から受信した一時鍵R0を用いてDESで暗号化して親機3に送信する(S309)。親機3のデータ処理回路21は、子機2から送信されてくる暗号化された一時鍵R1を受信すると、一時鍵R0を用いて一時鍵R1を復号する(S310)。

10

【0021】

その後、子機2のデータ処理回路13は、施錠・解錠指示等の情報データを、一時鍵R1を用いてDESで暗号化して親機3に送信する(S311)。親機3のデータ処理回路21は、子機2から送信されてくる暗号化された情報データを受信すると、一時鍵R1を用いて情報データを復号する(S312)。そして、データ処理回路21は、情報データに基づいて、例えば、駆動回路23を介してアクチュエータ24に施錠・解錠指示信号を送信する。

【0022】

このように、キーレスエントリーシステム1においては、子機2及び親機3において乱数生成回路54A, 54Bを用いて一時鍵を生成し、DESによる暗号化及び復号の処理を繰り返し行うことにより、セキュリティ強度を高めている。

20

【0023】

== DESの暗号化・復号の処理 ==

図4は、DESの暗号化の処理の流れを示すフローチャートである。DESの暗号化処理は、第1段から第16段までの処理で構成されている。まず、暗号化の対象となる64ビットの平文を初期転置(Initial Permutation)により並べ替え、第1段の入力データとなる左側の32ビット(L₀)及び右側の32ビット(R₀)を生成する(S401)。そして、第2段の入力データとなるL₁及びR₁は次式(1, 2)により求められる。

【数1】

$$L_1 = R_0 \quad \dots (1)$$

$$R_1 = L_0 \oplus F(R_0, K_1) \quad \dots (2)$$

30

【0024】

ここで、K₁は64ビットの共通鍵から生成された鍵である。まず、64ビットの共通鍵を縮約型転置(Permuted Choice 1:以後「PC1転置」と称する)により56ビットに変換し、左側の28ビット(C₀)及び右側の28ビット(D₀)を生成する(S402)。さらに、C₀及びD₀を左ローテートシフトして、C₁及びD₁を生成する(S403, S404)。そして、C₁及びD₁を縮約型転置(Permuted Choice 2:以後「PC2転置」と称する)により48ビットに変換することにより、K₁が得られる(S405)。また、C₁及びD₁をさらに左ローテートシフトし、PC2転置を行うことにより、第2段以降で用いられる鍵K₂~K₁₆を生成することができる。

40

【0025】

このようにして求められたL₁及びR₁が第2段の入力データとなり、第16段まで繰り返し処理が実行される。つまり、L_n及びR_nは、次式(3, 4)により求められる。

【数 2】

$$L_n = R_{n-1} \quad \dots (3)$$

$$R_n = L_{n-1} \oplus F(R_{n-1}, K_{n-1}) \quad \dots (4)$$

【0026】

そして、第16段の出力データである L_{16} 及び R_{16} に対して最終転置 (Inverse Initial Permutation) を行うことにより、平文を暗号化した暗号文を得ることができる (S406)。

10

【0027】

図5は、F関数 ($F(R, K)$) の処理の流れを示す図である。まず、32ビットのデータ R を拡大型転置により48ビットに変換し、 R' を生成する (S501)。次に、 R' と48ビットの鍵 K とをビット毎に排他的論理和することにより得られる48ビットのデータを6ビットずつに分割し、 $S1 \sim S8$ の S -BOXに入力する。そして、各 S -BOXから出力される4ビットを合わせて構成される32ビットのデータを転置 (以後「P転置」と称する) により並べ替えたデータがF関数の出力データとなる (S502)。

【0028】

図6は、DESの復号の処理の流れを示すフローチャートである。DESの復号処理は、暗号化処理と同様に第1段から第16のまでの処理で構成されている。まず、復号の対象となる64ビットの暗号文を初期転置により並べ替え、第1段の入力データとなる左側の32ビット (R_{16}) 及び右側の32ビット (L_{16}) を生成する (S601)。そして、第2段の入力データとなる R_{15} 及び L_{15} は次式 (5) 及び (6) により求められる。

20

【数 3】

$$R_{15} = L_{16} \quad \dots (5)$$

$$L_{15} = R_{16} \oplus F(L_{16}, K_{16}) \quad \dots (6)$$

30

【0029】

ここで、 K_{16} は、64ビットの共通鍵から生成された鍵である。まず、64ビットの共通鍵をPC1転置により56ビットに変換し、左側の28ビット (C_{16}) 及び右側の28ビット (D_{16}) を生成する (S602)。そして、 C_{16} 及び D_{16} をPC2転置により48ビットに変換することにより、 K_{16} が得られる (S603)。また、 C_{16} 及び D_{16} を右ローテートシフトし、PC2転置を行うことにより、第2段以降で用いられる鍵 $K_{15} \sim K_1$ を生成することができる。

【0030】

このようにして求められた R_{15} 及び L_{15} が第2段の入力データとなり、第16段まで繰り返し処理が実行される。つまり、 R_n および L_n は、次式 (7) 及び (8) により求められることとなる。

40

【数 4】

$$R_{n-1} = L_n \quad \dots (7)$$

$$L_{n-1} = R_n \oplus F(L_n, K_n) \quad \dots (8)$$

【0031】

50

そして、第16段の出力データである R_0 及び L_0 に対して最終転置を行うことにより、暗号文を復号した平文を得ることができる(5604)。なお、復号処理における L_n 、 R_n 、 C_n 、 D_n 、 K_n は、暗号化処理における L_n 、 R_n 、 C_n 、 D_n 、 K_n と同一のものである。また、 $C_0 = C_{16}$ 、 $D_0 = D_{16}$ である。

【0032】

== 暗号処理回路の構成 ==

本実施形態では、図4～図6で説明した暗号化及び復号の処理における転置・換字処理が暗号処理回路55A、55Bを用いて実現されている。暗号処理回路55A及び暗号処理回路55Bは同様の構成であるため、以後、暗号処理回路55Aについて説明する。図7は、暗号処理回路55Aの構成を示す図である。暗号処理回路55Aは、入力レジスタ(データ入力部)61、転置・換字部62、出力バッファ(データ出力部)63、選択レジスタ64、マルチプレクサ65、66、及びアドレスデコーダ67を備えている。

10

【0033】

入力レジスタ61は、複数のD型フリップフロップ(以後「D-FF」と称する)を用いて構成された64ビットのレジスタであり、D-FFの入力端子Dがバス57Aのデータバスに接続され、D-FFの出力端子Q(出力ポート)がマルチプレクサ65を介して転置・換字部62に接続されている。また、入力レジスタ61を構成するD-FFのクロック入力端子には、書き込み信号(WRITE)が入力される。なお、例えば、データバスが8ビットである場合には、入力レジスタ61は、8ビットのレジスタを8つ用いた構成とすることができる。

20

【0034】

転置・換字部62は、初期転置部71、最終転置部72、拡大型転置部73、S-BOX部74、P転置部75、PC1転置部76、ローテートシフト部77、及びPC2転置部78の8つのモジュールを備えている。転置・換字部62の各モジュール71～78は、入力レジスタ61から入力されるデータに対して転置又は換字処理を行い、マルチプレクサ66を介して出力バッファ63に出力する。

【0035】

なお、S-BOX部74が本発明の換字部に該当し、その他の各部71、72、73、75、76、77、78が本発明の転置部に該当する。また、選択レジスタ64、マルチプレクサ65、及びマルチプレクサ66が本発明の選択部に該当する。

30

【0036】

出力バッファ63は、64ビットのトライステートバッファであり、その64ビットの入力端子(入力ポート)にマルチプレクサ66を介して転置・換字部62が接続されており、出力端子がバス57Aのデータバスに接続されている。なお、例えば、データバスが8ビットである場合には、出力バッファ63は、8ビットのトライステートバッファを8つ用いた構成とすることができる。

【0037】

選択レジスタ64は、複数のD-FFを用いて構成された、例えば8ビットのレジスタであり、D-FFの入力端子Dがバス57Aのデータバスに接続され、D-FFの出力端子Qがマルチプレクサ65、66に接続されている。また、選択レジスタ64を構成するD-FFのクロック入力端子には、書き込み信号(WRITE)が入力される。選択レジスタ64には、転置・換字部62のうちの何れのモジュールを選択するかを示す選択データが書き込まれる。マルチプレクサ65は、選択レジスタ64から出力される選択データに基づいて、入力レジスタ61から出力されるデータを該当のモジュールに出力する。また、マルチプレクサ66は、選択レジスタ64から出力される選択データに基づいて、該当のモジュールから出力されるデータを出力バッファ63に出力する。

40

【0038】

アドレスデコーダ67は、バス57Aのアドレスバスに接続されており、アドレスバスで指定されたアドレスに該当する回路を選択する。なお、本実施形態においては、入力レジスタ61への書き込みアドレスと、出力バッファ63からの読み出しアドレスは同一で

50

あることとする。

【0039】

データ処理回路13において、暗号処理回路55Aを用いて転置又は換字処理を行う流れについて説明する。まず、CPU51Aは、アドレスバスに選択レジスタ64のアドレスを出力し、データバスに転置・換字部62の所望のモジュールを示す選択データを出力し、書き込み信号(WRITE)を出力することにより、選択レジスタに選択データを書き込む。続いて、CPU51Aは、アドレスバスに入力レジスタ61のアドレスを出力し、データバスに転置又は換字処理の入力データを出力し、書き込み信号(WRITE)を出力することにより、入力レジスタ61に当該入力データを書き込む。これにより、入力レジスタ61に入力されたデータがマルチプレクサ65を介して所望のモジュールに入力され、転置又は換字処理の結果がマルチプレクサ66を介して出力バッファ63に出力される。

10

【0040】

その後、CPU51Aは、入力レジスタ61と同一のアドレスである出力バッファ63のアドレスをアドレスバスに出力し、出力バッファ63に読み出し信号(READ)を入力する。これにより、入力データに対して転置又は換字処理を行ったデータが出力バッファ63からデータバスに出力される。このように、CPU51Aは、入力レジスタ61にデータを書き込み、出力バッファ63からデータを読み出すだけで、転置又は換字処理を行うことができる。

【0041】

== 転置・換字部の構成 ==

次に、転置・換字部62の各モジュール71~78の構成について説明する。

20

【0042】

(1) 初期転置

図8は、初期転置におけるビット毎の対応規則91を示す図である。この対応規則91は、例えば、初期転置部71に入力される64ビットの入力データの58ビット目が出力データの1ビット目となり、入力データの50ビット目が出力データの2ビット目となるというような、64ビットの入力データと64ビットの出力データとのビット毎の対応を示すものである。

【0043】

図9は、初期転置部71の構成を示す図である。図に示すように、初期転置部71の入力側と出力側とが、対応規則91に基づいて結線されている。例えば、入力側の58ビット目が出力側の1ビット目となるように結線され、入力側の50ビット目が出力側の2ビット目となるように結線されている。つまり、初期転置部71は、マルチプレクサ65, 66を介して、入力レジスタ61の出力端子Qと出力バッファ63の入力端子とを対応規則91に基づいて接続していることとなる。

30

【0044】

(2) 最終転置

図10は、最終転置におけるビット毎の対応規則92を示す図である。この対応規則92は、例えば、最終転置部72に入力される64ビットの入力データの40ビット目が出力データの1ビット目となり、入力データの8ビット目が出力データの2ビット目となるというような、64ビットの入力データと64ビットの出力データとのビット毎の対応を示すものである。

40

【0045】

図11は、最終転置部72の構成を示す図である。図に示すように、最終転置部72の入力側と出力側とが、対応規則92に基づいて結線されている。例えば、入力側の40ビット目が出力側の1ビット目となるように結線され、入力側の8ビット目が出力側の2ビット目となるように結線されている。つまり、最終転置部72は、マルチプレクサ65, 66を介して、入力レジスタ61の出力端子Qと出力バッファ63の入力端子とを対応規則92に基づいて接続していることとなる。

50

【 0 0 4 6 】

(3) 拡大型転置

図 1 2 は、拡大型転置におけるビット毎の対応規則 9 3 を示す図である。この対応規則 9 3 は、例えば、拡大型転置部 7 3 に入力される 3 2 ビットの入力データの 3 2 ビット目が出力データの 1 ビット目となり、入力データの 1 ビット目が出力データの 2 ビット目となるというような、3 2 ビットの入力データと 4 8 ビットの出力データとのビット毎の対応を示すものである。なお、拡大型転置においては、3 2 ビットの入力データを 4 8 ビットの出力データに拡大するため、入力データのうちの 1 6 ビットは、出力データの 2 ビット目と出力される。例えば、入力データの 1 ビット目は、出力データの 2 ビット目及び 4 8 ビット目の 2 ビット目と出力される。

10

【 0 0 4 7 】

図 1 3 は、拡大型転置部 7 3 の構成を示す図である。図に示すように、拡大型転置部 7 3 の入力側と出力側とが、対応規則 9 3 に基づいて結線されている。例えば、入力側の 3 2 ビット目が出力側の 1 ビット目となるように結線され、入力側の 1 ビット目が出力側の 2 ビット目となるように結線されている。つまり、拡大型転置部 7 3 は、マルチプレクサ 6 5 , 6 6 を介して、入力レジスタ 6 1 の出力端子 Q と出力バッファ 6 3 の入力端子とを対応規則 9 3 に基づいて接続していることとなる。

【 0 0 4 8 】

(4) S - B O X

図 1 4 は、S - B O X 部 7 4 の構成を示す図である。図に示すように、S - B O X 部 7 4 は、S 1 ~ S 8 で構成されており、4 8 ビットの入力データの先頭から 6 ビットごとに分割したデータが S 1 ~ S 8 に入力される。そして、例えば、S 1 においては、6 ビットの入力データが対応規則に基づいて 4 ビットに変換されて出力される。同様に、S 2 ~ S 8 においても、6 ビットの入力データが夫々の対応規則に基づいて 4 ビットに変換されて出力される。

20

【 0 0 4 9 】

図 1 5 は、S - B O X (S 1) の対応規則 9 4 を示す図である。この対応規則 9 4 では、S 1 に入力される 6 ビットの入力データの 1 ビット目と 6 ビット目 (B 1 ・ B 6) が行となり、入力データの 2 ビット目から 5 ビット目 (B 2 ~ B 5) が列となり、その交差する箇所にあるデータが出力データとなる。例えば、入力データ “ 1 1 0 0 0 0 ” が S 1 に入力されたとする。この場合、B 1 ・ B 6 は “ 1 0 ” となり、3 行目が選択される。そして、B 2 ~ B 5 は “ 1 0 0 0 ” となり、これを 1 0 進で表した 8 列目が選択される。これにより、3 行目の 8 列目にある 1 0 進の “ 1 5 ” を 2 進で表した “ 1 1 1 1 ” が出力される。同様に、S 2 ~ S 8 に対しても対応規則が定められている。

30

【 0 0 5 0 】

図 1 6 は、S - B O X 部 7 4 の S 1 の構成を示す図である。図に示すように、S 1 は、セレクタ 9 5、置換回路 9 6、及び選択回路 9 7 を備えている。また、S 1 ~ S 8 共通で用いられる選択レジスタ 9 8 が設けられている。なお、セレクタ 9 5 及び置換回路 9 6 が本発明の換字回路に該当する。

【 0 0 5 1 】

セレクタ 9 5 には、選択回路 9 7 を介して B 1 及び B 6 が入力され、その入力に従い、対応規則 9 4 のどの行が選択されるかを示す信号を置換回路 9 6 に出力する。置換回路 9 6 には、B 2 ~ B 5 を対応規則 9 4 の各行の値に変換する論理回路が構成されており、B 2 ~ B 5 を、セレクタ 9 5 からの信号に基づいて変換して出力する。

40

【 0 0 5 2 】

選択レジスタ 9 8 は、複数の D - F F を用いて構成された、例えば 8 ビットのレジスタであり、D - F F の入力端子 D がバス 5 7 A のデータバスに接続され、D - F F の出力端子 Q が選択回路 9 7 に接続されている。そして、選択回路 9 7 は、選択レジスタ 9 8 から出力される選択データに従って、セレクタ 9 5 に出力する B 1 と B 6 とを並べ替えることができる。例えば、選択レジスタ 9 8 から選択データ “ 0 ” が出力されている場合、選択

50

回路 97 は、1 ビット目 97 a から B 1 を出力し、2 ビット目 97 b から B 6 を出力する。また、選択レジスタ 98 から選択データ “ 1 ” が出力されている場合、選択回路 97 は、1 ビット目 97 a から B 6 を出力し、2 ビット目 97 b から B 1 を出力する。

【 0 0 5 3 】

つまり、前述した入力データ “ 1 1 0 0 0 0 ” の場合、選択レジスタ 98 から選択データ “ 1 ” が出力されている場合、選択回路 97 からセレクタ 95 に入力されるデータは “ 0 1 ” となり 2 行目が選択され、2 行目の 8 列目にある 10 進の “ 1 0 ” を 2 進で表した “ 1 0 1 0 ” が出力される。このように、選択レジスタ 98 に書き込まれる選択データを変化させることにより、S 1 の対応規則 94 を変化させることができる。

【 0 0 5 4 】

また、S 2 ~ S 8 についても、S 1 と同様に構成されている。つまり、S 1 ~ S 8 で構成される S - B O X 部 74 は、マルチプレクサ 65 , 66 を介して、入力レジスタ 61 の出力端子 Q から並列出力される入力データを S 1 ~ S 8 の対応規則に基づいて変換して出力バッファ 63 の入力端子に出力する論理回路であると言える。

【 0 0 5 5 】

なお、本実施形態においては、最上位と最下位の 2 ビットを選択回路 97 で並べ替えてセレクタ 95 に入力し、残りの 4 ビットを置換回路 96 に入力する構成としたが、S - B O X 部 74 の構成はこれに限られず、入力される 6 ビット (B 1 ~ B 6) を選択データに基づいて並べ替えたデータを、対応規則に基づいて 4 ビットに変換する論理回路であればよい。

【 0 0 5 6 】

(5) P 転置

図 17 は、P 転置におけるビット毎の対応規則 101 を示す図である。この対応規則 101 は、例えば、最終転置部 75 に入力される 32 ビットの入力データの 16 ビット目が出力データの 1 ビット目となり、入力データの 7 ビット目が出力データの 2 ビット目となるというような、32 ビットの入力データと 32 ビットの出力データとのビット毎の対応を示すものである。

【 0 0 5 7 】

図 18 は、P 転置部 75 の構成を示す図である。図に示すように、P 転置部 75 の入力側と出力側とが、対応規則 101 に基づいて結線されている。例えば、入力側の 16 ビット目が出力側の 1 ビット目となるように結線され、入力側の 7 ビット目が出力側の 2 ビット目となるように結線されている。つまり、P 転置部 75 は、マルチプレクサ 65 , 66 を介して、入力レジスタ 61 の出力端子 Q と出力バッファ 63 の入力端子とを対応規則 101 に基づいて接続していることとなる。

【 0 0 5 8 】

(6) P C 1 転置

図 19 は、P C 1 転置におけるビット毎の対応規則 102 を示す図である。この対応規則 102 は、例えば、P C 1 転置部 76 に入力される 64 ビットの入力データの 57 ビット目が出力データの 1 ビット目となり、入力データの 49 ビット目が出力データの 2 ビット目となるというような、64 ビットの入力データと 56 ビットの出力データとのビット毎の対応を示すものである。なお、P C 1 転置においては、64 ビットの入力データを 56 ビットの出力データに縮約するため、入力データのうちの 8 ビットは出力データに出力されない。

【 0 0 5 9 】

図 20 は、P C 1 転置部 76 の構成を示す図である。図に示すように、P C 1 転置部 76 の入力側と出力側とが、対応規則 102 に基づいて結線されている。例えば、入力側の 57 ビット目が出力側の 1 ビット目となるように結線され、入力側の 49 ビット目が出力側の 2 ビット目となるように結線されている。つまり、P C 1 転置部 76 は、マルチプレクサ 65 , 66 を介して、入力レジスタ 61 の出力端子 Q と出力バッファ 63 の入力端子とを対応規則 102 に基づいて接続していることとなる。

10

20

30

40

50

【0060】

(7) ローテートシフト

図21は、ローテートシフトにおける入力データと出力データとの対応規則103を示す図である。つまり、対応規則103は、28ビットの C_1 及び28ビットの D_1 は、28ビットの C_0 及び28ビットの D_0 を1ビット左ローテートシフトすることにより得られ、 C_2 及び D_2 は、 C_1 及び D_1 を1ビット左ローテートシフトすることにより得られ、 C_3 及び D_3 は、 C_2 及び D_2 を2ビット左ローテートシフトすることにより得られることを示している。このように、対応規則103においては、 $C_1 \sim C_{16}$ 及び $D_1 \sim D_{16}$ までのローテート数が示されている。なお、左ローテートシフトの処理は入力データの各ビットと出力データの各ビットとが1対1で対応したものであり、他の転置処理と同様にビット毎の対応規則であると言える。

10

【0061】

図22は、ローテートシフト部77の構成を示す図である。図は、ローテートシフト部77のうち、 C_0 及び D_0 から C_1 及び D_1 を生成する部分を示すものであり、入力側の C_0 及び D_0 を夫々1ビット左ローテートシフトして出力側に C_1 及び D_1 として出力されるように結線されている。また、 C_0 及び D_0 から $C_2 \sim C_{16}$ 及び $D_2 \sim D_{16}$ を生成する部分についても、同様に構成されている。つまり、ローテートシフト部77は、マルチプレクサ65, 66を介して、入力レジスタ61の出力端子Qと出力バッファ63の入力端子とを対応規則103に基づいて接続していることとなる。

【0062】

なお、 $C_1 \sim C_{16}$ 及び $D_1 \sim D_{16}$ を生成するローテートシフト部77を、例えば、 C_1 及び D_1 を生成する回路、 C_2 及び D_2 を生成する回路、というように夫々別々に構成することも可能であるが、これらをまとめて構成することも可能である。つまり、ローテートシフト部77は、入力レジスタ61から出力される C_0 及び D_0 から、 $C_1 \sim C_{16}$ 及び $D_1 \sim D_{16}$ を一度に生成し、出力バッファ63に出力するようにすることも可能である。この場合、出力バッファ63は56ビット(7バイト)を16倍した112バイト以上の容量が必要である。このように、 $C_1 \sim C_{16}$ 及び $D_1 \sim D_{16}$ を一度に生成するようにすることで、鍵 $K_1 \sim K_{16}$ を生成するためのローテートシフトを一度の処理で行うことができるため、暗号化及び復号の処理の処理速度を向上させることができる。

20

【0063】

(8) PC2 転置

図23は、PC2転置におけるビット毎の対応規則104を示す図である。この対応規則104は、例えば、PC2転置部78に入力される56ビットの入力データの14ビット目が出力データの1ビット目となり、入力データの17ビット目が出力データの2ビット目となるというような、56ビットの入力データと48ビットの出力データとのビット毎の対応を示すものである。なお、PC2転置においては、56ビットの入力データを48ビットの出力データに縮約するため、入力データのうちの8ビットは出力データに出力されない。

30

【0064】

図24は、PC2転置部78の構成を示す図である。図に示すように、PC2転置部78の入力側と出力側とが、対応規則104に基づいて結線されている。例えば、入力側の14ビット目が出力側の1ビット目となるように結線され、入力側の17ビット目が出力側の2ビット目となるように結線されている。つまり、PC2転置部78は、マルチプレクサ65, 66を介して、入力レジスタ61の出力端子Qと出力バッファ63の入力端子とを対応規則104に基づいて接続していることとなる。

40

【0065】

以上、本発明の一実施形態である暗号処理回路55A, 55Bを適用したキーレスエントリーシステム1について説明した。前述したように、暗号処理回路55A, 55BのS-BOX部74は、S1~S8の各S-BOXに入力される6ビットのデータを選択レジスタ98から出力される選択データに基づいて並べ替えたデータを所定の対応規則に基づ

50

いて変換して出力する。つまり、選択レジスタに記憶されている選択データを書き換えることにより、ハードウェアを修正せずにS - B O Xにおける入力データと出力データとの対応規則を変更可能とし、安全性を高めることができる。とくに、本実施形態の暗号処理回路55A, 55BのS - B O X部74においては、6ビットの入力データの最上位ビット及び最下位ビットを選択データに基づいて並べ替えることにより、例えばS1における対応規則94において選択される行を、ハードウェアを修正せずに変更可能とすることにより、安全性を高めている。

【0066】

なお、本実施形態においては、本発明の暗号処理回路を共通鍵ブロック暗号方式の一つであるDESに適用した例を説明したが、共通鍵ブロック暗号方式はDESに限られず、トリプルDESやAES (Advanced Encryption Standard) 等の共通鍵ブロック暗号方式においても、同様の構成によりハードウェアを修正せずに換字処理における入力データと出力データとの対応規則を変更可能とし、安全性を高めることができる。

10

【0067】

また、本実施形態においては、暗号処理回路55A, 55Bの適用例としてキーレスエントリーシステム1をあげたが、キーレスエントリーシステム1に限らず、例えばICカードを用いた自動改札システムや入退室管理システム等、データの暗号化が必要な様々なシステムに適用することが可能である。

【0068】

以上、本発明の実施形態について説明したが、上記実施形態は本発明の理解を容易にするためのものであり、本発明を限定して解釈するためのものではない。本発明は、その趣旨を逸脱することなく、変更、改良され得ると共に、本発明にはその等価物も含まれる。

20

【図面の簡単な説明】

【0069】

【図1】本発明の暗号処理回路を用いる一実施形態である自動車の錠の施錠・解錠を行うキーレスエントリーシステムの全体構成を示す図である。

【図2】データ処理回路の構成を示す図である。

【図3】キーレスエントリーシステムの子機と親機との間における通信手順を示すフローチャートである。

【図4】DESの暗号化の処理の流れを示すフローチャートである。

30

【図5】F関数(F(R, K))の処理の流れを示す図である。

【図6】DESの復号の処理の流れを示すフローチャートである。

【図7】暗号処理回路の構成を示す図である。

【図8】初期転置におけるビット毎の対応規則を示す図である。

【図9】初期転置部の構成を示す図である。

【図10】最終転置におけるビット毎の対応規則を示す図である。

【図11】最終転置部の構成を示す図である。

【図12】拡大型転置におけるビット毎の対応規則を示す図である。

【図13】拡大型転置部の構成を示す図である。

【図14】S - B O X部の構成を示す図である。

40

【図15】S - B O X (S1)における対応規則を示す図である。

【図16】S - B O X部のS1の構成を示す図である。

【図17】P転置におけるビット毎の対応規則を示す図である。

【図18】P転置部の構成を示す図である。

【図19】PC1転置におけるビット毎の対応規則を示す図である。

【図20】PC1転置部の構成を示す図である。

【図21】ローテートシフトにおけるローテート数を示す図である。

【図22】ローテートシフト部の構成を示す図である。

【図23】PC2転置におけるビット毎の対応規則を示す図である。

【図24】PC2転置部の構成を示す図である。

50

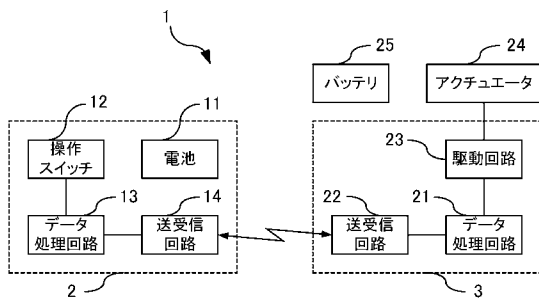
【符号の説明】

【0070】

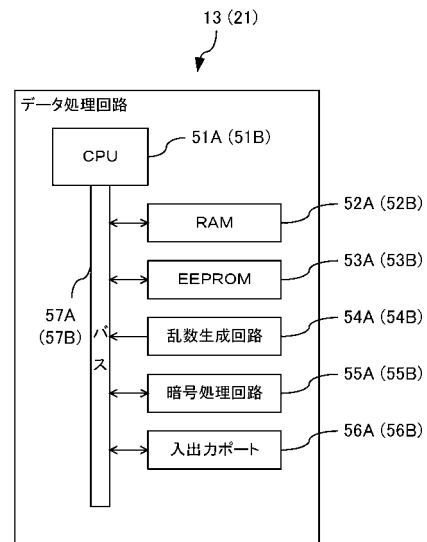
- 1 キーレスエントリーシステム
- 3 親機
- 12 操作スイッチ
- 14, 22 送受信回路
- 24 アクチュエータ
- 51A, 51B CPU
- 53A, 53B EEPROM
- 55A, 55B 暗号処理回路
- 61 入力レジスタ
- 63 出力バッファ
- 65, 66 マルチプレクサ
- 71 初期転置部
- 73 拡大型転置部
- 75 P転置部
- 77 ロータートシフト部
- 95 セレクタ
- 97 選択回路

- 2 子機
- 11 電池
- 13, 21 データ処理回路
- 23 駆動回路
- 25 バッテリ
- 52A, 52B RAM
- 54A, 54B 乱数生成回路
- 56A, 56B 入出力ポート
- 62 転置・換字部
- 64 選択レジスタ
- 67 アドレスデコーダ
- 72 最終転置部
- 74 S-BOX部
- 76 PC1転置部
- 78 PC2転置部
- 96 置換回路
- 98 選択レジスタ

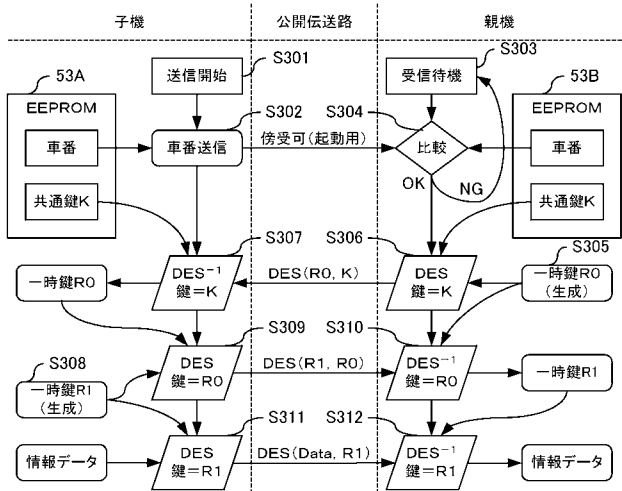
【図1】



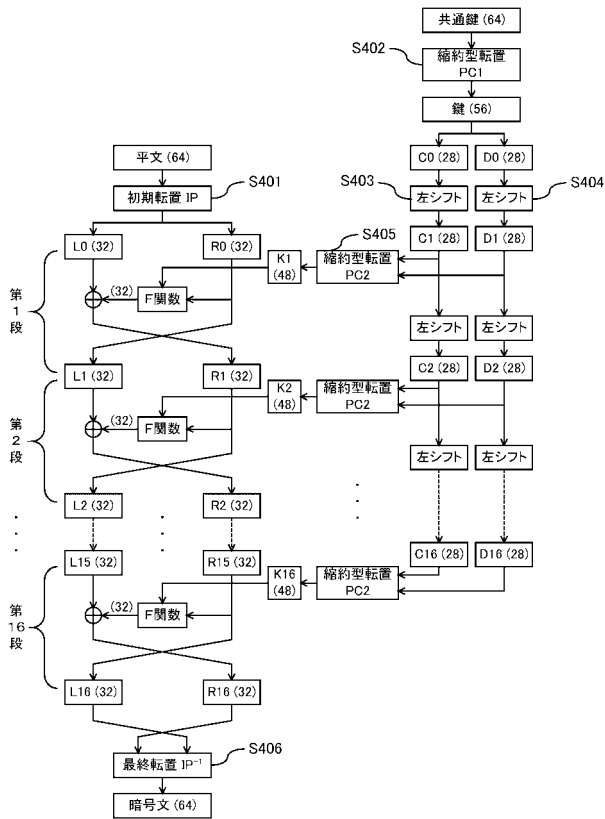
【図2】



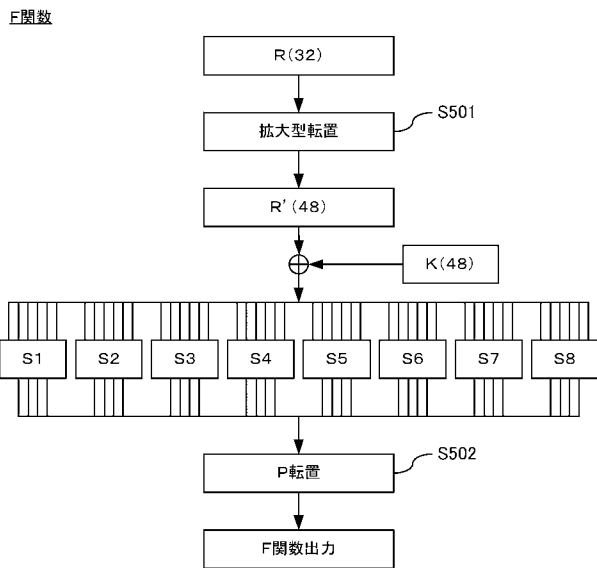
【 図 3 】



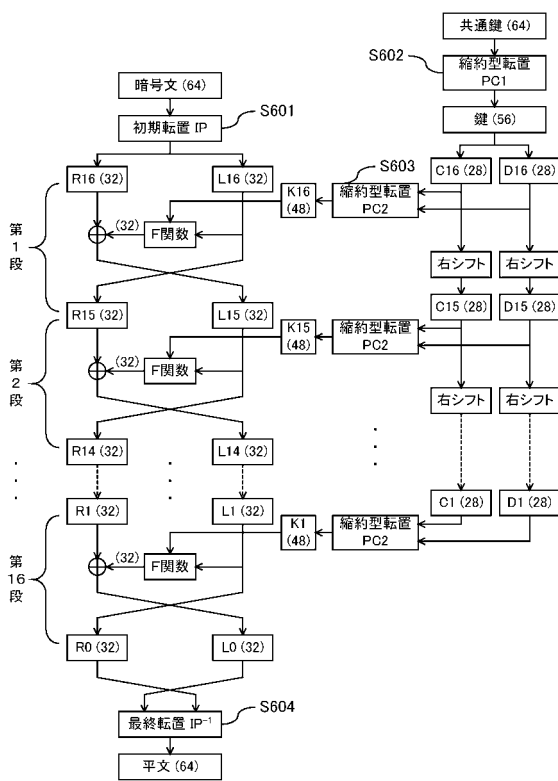
【 図 4 】



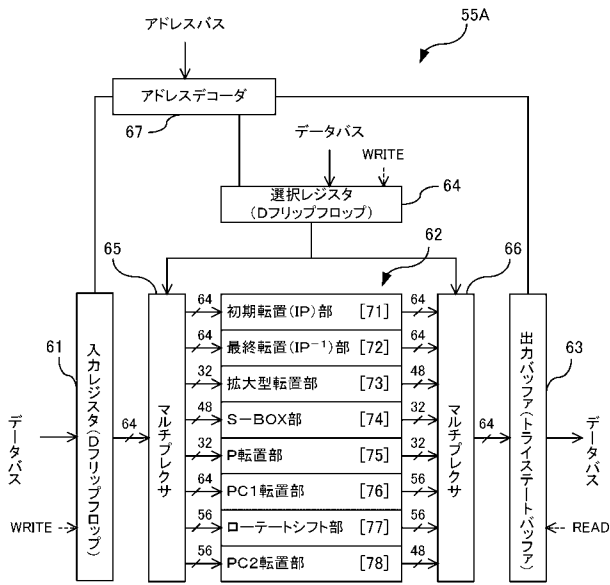
【 図 5 】



【 図 6 】



【 図 7 】



【 図 8 】

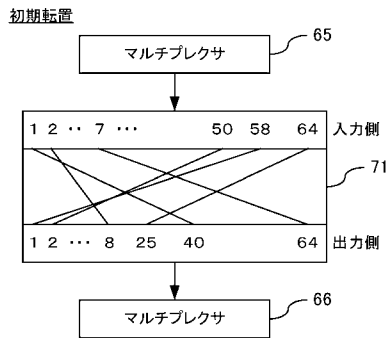
初期転置

	1	2	3	4	5	6	7	8
1	58	50	42	34	26	18	10	2
9	60	52	44	36	28	20	12	4
17	62	54	46	38	30	22	14	6
25	64	56	48	40	32	24	16	8

33	57	49	41	33	25	17	9	1
41	59	51	43	35	27	19	11	3
48	61	53	45	37	29	21	13	5
56	63	55	47	39	31	23	15	7

図8は初期転置のデータテーブルを示している。L(32)とR(32)のグループ分けが示されている。

【 図 9 】



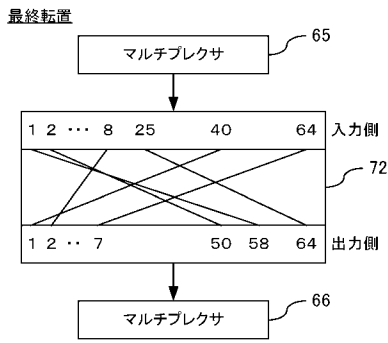
【 図 10 】

最終転置

	1	2	3	4	5	6	7	8
1	40	8	48	16	56	24	64	32
9	39	7	47	15	55	23	63	31
17	38	6	46	14	54	22	62	30
25	37	5	45	13	53	21	61	29
33	36	4	44	12	52	20	60	28
41	35	3	43	11	51	19	59	27
48	34	2	42	10	50	18	58	26
56	33	1	41	9	49	17	57	25

図10は最終転置のデータテーブルを示している。

【図 1 1】

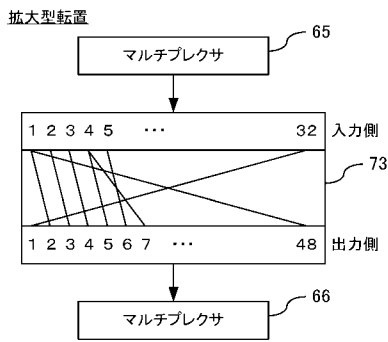


【図 1 2】

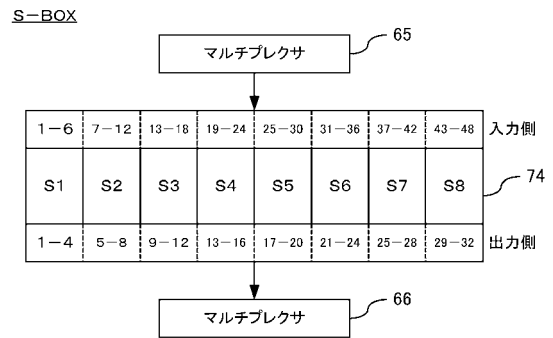
拡大型転置

	1	2	3	4	5	6	
1	32	1	2	3	4	5	→S1(6)
7	4	5	6	7	8	9	→S2(6)
13	8	9	10	11	12	13	→S3(6)
19	12	13	14	15	16	17	→S4(6)
25	16	17	18	19	20	21	→S5(6)
31	20	21	22	23	24	25	→S6(6)
37	24	25	26	27	28	29	→S7(6)
43	28	29	30	31	32	1	→S8(6)

【図 1 3】



【図 1 4】



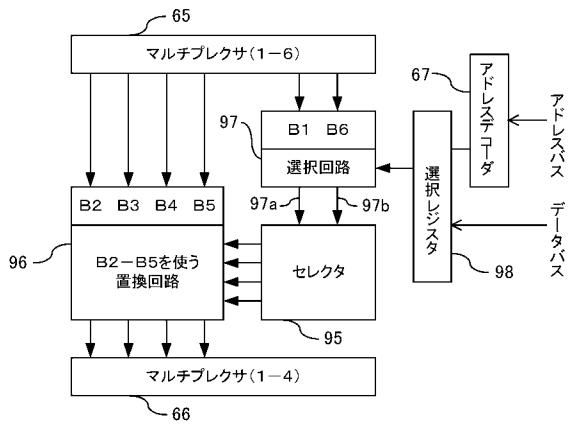
【図 1 5】

S-BOX(S1)

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
00	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
B1 01	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
B6 10	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
11	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

【図16】

S-BOX(S1)

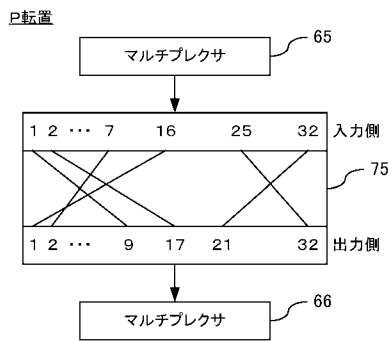


【図17】

P転置

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

【図18】



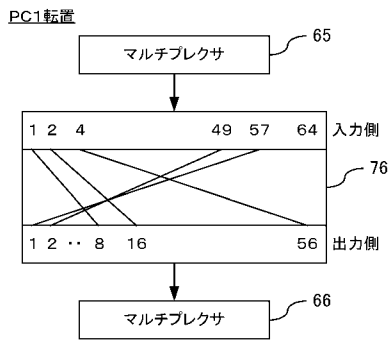
【図19】

PC1転置

	1	2	3	4	5	6	7
1	57	49	41	33	25	17	9
8	1	58	50	42	34	26	18
15	10	2	59	51	43	35	27
22	19	11	3	60	52	44	36
29	63	55	47	39	31	23	15
36	7	62	54	46	38	30	22
43	14	6	61	53	45	37	29
50	21	13	5	28	20	12	4

C(28) and D(28) groupings are indicated on the right side of the table.

【図 20】

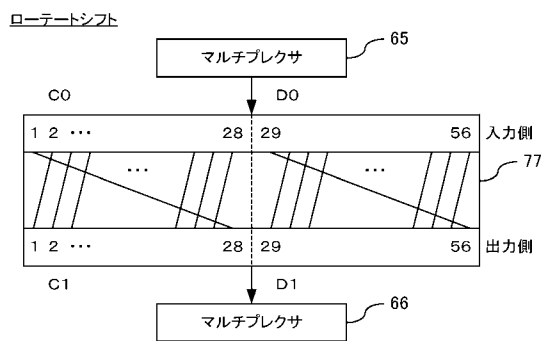


【図 21】

ローテートシフト

	ローテート数
C1, D1	1
C2, D2	1
C3, D3	2
C4, D4	2
C5, D5	2
C6, D6	2
C7, D7	2
C8, D8	2
C9, D9	1
C10, D10	2
C11, D11	2
C12, D12	2
C13, D13	2
C14, D14	2
C15, D15	2
C16, D16	1

【図 22】



【図 23】

PC2 転置

	1	2	3	4	5	6
1	14	17	11	24	1	5
7	3	28	15	6	21	10
13	23	19	12	4	26	8
19	16	7	27	20	13	2
25	41	52	31	37	47	55
31	30	40	51	45	33	48
37	44	49	39	56	34	53
43	46	42	50	36	29	32

【図 24】

