(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5228803号
(P5228803)
(45)発行日　平成25年7月3日(2013.7.3)　(24)登録日　平成25年3月29日(2013.3.29)

(51)Int.Cl.　　F I
G09C 1/00 (2006.01)　　G09C 1/00 610B
H04L 9/10 (2006.01)　　H04L 9/00 621Z

請求項の数 6　(全 33 頁)

(21)出願番号　特願2008-279028(P2008-279028)
(22)出願日　平成20年10月30日(2008.10.30)
(65)公開番号　特開2010-109639(P2010-109639A)
(43)公開日　平成22年5月13日(2010.5.13)
審査請求日　平成23年7月4日(2011.7.4)

(73)特許権者　308014341
富士通セミコンダクター株式会社
神奈川県横浜市港北区新横浜二丁目１０番２３
(74)代理人　100094525
弁理士　土井　健二
(74)代理人　100094514
弁理士　林　恒徳
(72)発明者　岡田　壮一
東京都新宿区西新宿二丁目７番１号　富士通マイクロエレクトロニクス株式会社内
(72)発明者　磯部　正義
東京都新宿区西新宿二丁目７番１号　富士通マイクロエレクトロニクス株式会社内

最終頁に続く

(54)【発明の名称】共通鍵ブロック暗号におけるスワップ回路及び、それを有する暗号化・復号化回路

(57)【特許請求の範囲】
【請求項１】
複数の動作モードに対応して、暗号化及び復号化を行う暗号化・復号化回路において、
入力端子から入力されるテキストデータとイニシャルベクタデータ(以下イニシャルベクタをIVと称する)とを前記動作モードに応じて第1または第2の出力端子に出力するスワップ回路と、
前記第1の出力端子から前記テキストデータまたはIVデータのいずれか一方を入力し、暗号処理及び復号処理を行う暗号・復号処理ユニットと、
前記第2の出力端子から前記IVデータまたはテキストデータのいずれか他方を入力し、排他的論理和演算を行う排他的論理和処理ユニットとを有し、
前記スワップ回路は、
テキストデータ書き込みイネーブル信号またはIVデータ書き込みイネーブル信号に応答して、前記テキストデータまたはIVデータをそれぞれ格納し、前記第1、第2の出力端子にそれぞれ出力する第1、第2のレジスタと、
動作モード信号に応答して、前記テキストデータ書き込みイネーブル信号またはIVデータ書き込みイネーブル信号のいずれか一方を選択して前記第1のレジスタに供給する第1のセレクタと、いずれか他方を選択して前記第2のレジスタに供給する第2のセレクタとを有し、
さらに、前記暗号・復号処理ユニットの出力と、前記排他的論理和処理ユニットの出力と、前記第1または第2のレジスタに格納されたテキストデータと、前記第1または第2のレ

ジスタに格納されたIVデータとに応じて、更新されたIVデータを前記第1または第2のレジスタに出力するIV更新ユニットを有することを特徴とする暗号化・復号化回路。
【請求項２】
前記複数の動作モードは、少なくとも、CBCモードと、CFBモードと、OFBモードとを有し、
前記CBCモードのときは、前記第1のセレクタは前記テキストデータ書き込みイネーブル信号を選択し、前記第2のセレクタは前記IVデータ書き込みイネーブル信号を選択し、暗号化時に、前記排他的論理和処理ユニットは前記テキストデータとIVデータの排他的論理和演算を行い前記暗号・復号処理ユニットは前記排他的論理和演算されたデータを暗号処理し、前記IV更新ユニットは当該暗号処理されたデータを前記更新されたIVデータとして前記第2のレジスタに出力することを特徴とする請求項1に記載の暗号化・復号化回路。
【請求項３】
前記複数の動作モードは、少なくとも、CBCモードと、CFBモードと、OFBモードとを有し、
前記CFBモードのときは、前記第1のセレクタは前記IVデータ書き込みイネーブル信号を選択し、前記第2のセレクタは前記テキストデータ書き込みイネーブル信号を選択し、暗号化時に、前記暗号・復号処理ユニットは前記IVデータを暗号処理し、前記排他的論理和処理ユニットは当該暗号処理されたIVデータと前記テキストデータの排他的論理和演算を行い、前記IV更新ユニットは当該排他的論理和演算されたデータと前記IVデータをビット演算処理し、当該ビット演算処理されたデータを前記更新されたIVデータとして前記第1のレジスタに出力することを特徴とする請求項1に記載の暗号化・復号化回路。
【請求項４】
前記複数の動作モードは、少なくとも、CBCモードと、CFBモードと、OFBモードとを有し、
前記OFBモードのときは、前記第1のセレクタは前記IVデータ書き込みイネーブル信号を選択し、前記第2のセレクタは前記テキストデータ書き込みイネーブル信号を選択し、暗号化および復号化時に、前記暗号・復号処理ユニットは前記IVデータを暗号処理し、前記排他的論理和処理ユニットは当該暗号処理されたIVデータと前記テキストデータの排他的論理和演算を行い、前記IV更新ユニットは前記暗号処理されたIVデータを前記更新されたIVデータとして前記第1のレジスタに出力することを特徴とする請求項1に記載の暗号化・復号化回路。
【請求項５】
前記排他的論理和処理ユニットが前記第1と第2の両方の出力端子から前記テキストデータとIVデータの両方を入力する請求項1に記載の暗号化・復号化回路。
【請求項６】
さらに、前記第1と第2のセレクタの両方が前記IVデータ書き込みイネーブル信号を選択し、前記第1と第2のレジスタに供給した後、動作モード信号に応答して、前記第1と第2のセレクタのいずれか一方が前記テキストデータ書き込みイネーブル信号を選択する請求項1に記載の暗号化・復号化回路。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、スワップ回路及び、それを有する暗号化・復号化回路に関し、特に共通鍵ブロック暗号におけるTEXTデータとIVデータをスワップするスワップ回路及び、それを有する暗号化・復号化回路に関する。
【背景技術】
【０００２】
近年、情報化社会において重要な情報の漏洩や改ざんや不正コピー等に対処するために、様々な分野で所定の規則に従った情報の暗号化および復号化が行われている。そして、スマートカード等の小型携帯用情報記憶媒体の分野においても情報の暗号化および復号化

が行われており、その実現のために当該カード等は暗号化・復号化回路を搭載している。

【０００３】

暗号化方式の一つに共通鍵暗号方式がある。そして、その暗号化回路においては、米国標準の代表的な規格であるDES(Data Encryption Standard)方式や、AES方式(Advanced Encryption Standard)が採用されている。DES方式とAES方式ではブロック暗号化を行い、平文と称される暗号化するためのデータはブロック単位で暗号文に暗号化され、同様に、暗号文はブロック単位で平文に復号化される。また、その暗号化および復号化のブロック単位は、DES方式では64-bit長であり、AES方式では128-bit長である。また、各暗号化方式には複数の動作モードが規定されており、それらの動作モードに応じて、具体的な暗号化および復号化処理が行われる。そして、これらの動作モードは、DES方式においてはECB(Electronic Codebook)モードとCBC(Cipher Block Chaining)モードとCFB(Cipher Feedback)モードとOFB(Output Feedback)モードの4つが規定されており、AES方式においては、DES方式の4つのモードに加えて、さらにCTR(Counter)モードが規定されている。

【０００４】

以下に、図1～4を用いてDES方式において規定された各動作モードの態様を示す。各図は、動作モード別の暗号化・復号化の概念図であり、左半分は暗号化の概念図、右半分は復号化の概念図を表す。そして、各図は、平文Piが入力されて暗号化が行われ、暗号文Ciとして出力され、暗号文Ciが入力されて復号化が行われ、平文Piとして出力される態様を示している。ここで、平文Piと暗号文Ciは、前述したように暗号化・復号化のブロック単位であり、添字iは、暗号化が行われるブロック化された平文、若しくは復号化が行われるブロック化された暗号文の一連のブロック番号を表す。また、平文Piの暗号化と暗号文Ciの復号化には、レジスタIVにセットされたイニシャルベクタViと称される暗号化パラメータが、適宜、更新されながら用いられる。途中データDiは、暗号化、復号化の処理の途中で生成されるデータを表す。また、入力データに対し、暗号処理ユニットEncは暗号処理を行い、復号処理ユニットDecは復号処理を行う。なお、図中に明記していないが、暗号・復号処理には共通鍵がパラメータとして使用される。

【０００５】

[ECBモード]

図1は、ECBモードの概念図である。暗号化において、入力される平文Piは、暗号処理ユニットEncにより暗号化され、暗号文Ciとして出力される。

【０００６】

また、復号化において、入力される暗号文Ciは、復号処理ユニットDecにより復号化され、平文Piとして出力される。

【０００７】

以下に、ECBモードの処理を表す式を示す。

暗号化：Ci=Enc(Pi)　(i=1,2,3,・・・)

復号化：Pi=Dec(Ci)　(i=1,2,3,・・・)

[CBCモード]

図2は、CBCモードの概念図である。暗号化において、64bit長にブロック分割された平文のはじめのブロックである平文P_1の暗号化のために、イニシャルベクタViの初期値がレジスタIVにセットされ、イニシャルベクタV_1として使用される。次に、平文P_1とイニシャルベクタV_1の排他的論理和演算が行われ、途中データD_1が出力される。そして、途中データD_1は暗号処理ユニットEncにより暗号処理され、暗号文C_1として出力される。そして、次のブロックである平文P_2の暗号化のために、暗号文C_1がレジスタIVにセットされ、イニシャルベクタV_2として使用される。そして、以下同様にレジスタIVの値が更新され、ブロック単位で平文Piの暗号化が行われる。

【０００８】

また、復号化において、64bit長にブロック分割された暗号文の、はじめのブロックである暗号文C_1の復号化のために、イニシャルベクタViの初期値がレジスタIVにセットされ、イニシャルベクタV_1として使用される。次に、暗号文C_1が復号処理ユニットDecにより

復号処理され、途中データD_1として出力される。そして、途中データD_1とイニシャルベクタV_1の排他的論理和演算が行われ、平文P_1が出力される。そして、次のブロックである暗号文C_2の復号化のために、暗号文C_1がレジスタIVにセットされ、イニシャルベクタV_2として使用される。そして、以下同様にレジスタIVの値が更新され、ブロック単位で暗号文Ciの復号化が行われる。

【０００９】

以下に、CBCモードの処理を表す式を示す。なお、XORは排他的論理和を示す。

暗号化：V_1=[初期値] (i=1)

$Vi=C_{i-1}$ (i=2,3,・・・)

Ci=Enc(Pi XOR Vi) (i=1,2,3,・・・)

復号化：V_1=[初期値] (i=1)

$Vi=C_{i-1}$ (i=2,3,・・・)

Pi=Dec(Ci) XOR Vi (i=1,2,3,・・・)

[CFBモード]

図3は、CFBモードの概念図である。前述したとおり、DES方式において、平文データは64bit毎にブロック化されてブロック単位に暗号化・復号化が行われる。しかし、CFBモードにおいては、ブロック化された64bit長の平文は、さらに細かくk-bit長にブロック化され、その細分されたブロック単位に暗号化・復号化が行われる。そして、CFBモードでは、それらの処理を行うために、ビットシフト等のビット演算処理が行われる。なお、レジスタIVにセットされるイニシャルベクタViは、常に64bit長であるが、前述した平文データには、k-bit長として一般的に1bit長、8bit長、64bit長等が用いられる。そこで、以下、図3のCFBモードの概念図において示されるnを64、kを8として具体的に説明する。

【００１０】

暗号化において、8bit長にブロック分割された平文の、はじめのブロックである平文P_1の暗号化のために、イニシャルベクタViの初期値がレジスタIVにセットされ、イニシャルベクタV_1として使用される。次に、イニシャルベクタV_1は暗号処理ユニットEncにより暗号処理され、途中データD_1として出力される。次に、途中データD_1の上位8bitが取り出され、8bit長に分割された平文P_1と排他的論理和演算が行われ、8bit長の暗号文C_1が出力される。次に前述した64bit長のイニシャルベクタV_1の下位56bitと前記暗号文C_1を連結した値がレジスタIVにセットされ、次の平文P_2の暗号化のために、イニシャルベクタV_2として使用される。そして、以下同様にレジスタIVが更新され、ブロック単位で平文Piの暗号化が行われる。

【００１１】

また、復号化において、8bit長にブロック分割された暗号文の、はじめのブロックである暗号文C_1の復号化のために、イニシャルベクタViの初期値がレジスタIVにセットされ、イニシャルベクタV_1として使用される。次に、イニシャルベクタV_1は暗号処理ユニットEncにより暗号処理され、途中データD_1として出力される。次に、途中データD_1の上位8bitが取り出され、8bit長に分割された暗号文C_1と排他的論理和演算が行われ、8bit長の平文P_1が出力される。次に前述した64bit長のイニシャルベクタV_1の下位56bitと前記暗号文C_1を連結した値がレジスタIVにセットされ、次の暗号文C_2の復号化のために、イニシャルベクタV_2として使用される。そして、以下同様にレジスタIVが更新され、ブロック単位で暗号文Ciの復号化が行われる。

【００１２】

以下に、CFBモードの処理を表す式を示す。

暗号化：V_1=[初期値] (i=1)

$Vi=LSB_{n-k}(V_{i-1})|C_{i-1}$ (i=2,3,・・・)

$Di=MSB_k(Enc(Vi))$ (i=1,2,3,・・・)

Ci=Pi XOR Di (i=1,2,3,・・・)

復号化：V_1=[初期値] (i=1)

$Vi=LSB_{n-k}(V_{i-1})|C_{i-1}$ (i=2,3,・・・)

$Di=MSB_k(Enc(Vi))$ (i=1,2,3,・・・)
Pi=Ci XOR Di (i=1,2,3,・・・)

[OFBモード]

図4は、OFBモードの概念図である。暗号化において、ブロック分割された平文の、はじめのブロックである平文P_1の暗号化のために、イニシャルベクタViの初期値がレジスタIVにセットされ、イニシャルベクタV_1として使用される。次にイニシャルベクタV_1は暗号処理ユニットEncにより暗号処理され、途中データD_1として出力される。次に途中データD_1と平文P_1の排他的論理和演算が行われ、C_1が出力される。そして、次のブロックである平文P_2の暗号化のために、前述した途中データD_1がレジスタIVにセットされ、イニシャルベクタV_2として使用される。そして、以下同様にレジスタIVが更新され、ブロック単位で平文Piの暗号化が行われる。

【００１３】

また、復号化において、ブロック分割された暗号文の、はじめのブロックである暗号文C_1の復号化のために、イニシャルベクタViの初期値がレジスタIVにセットされ、イニシャルベクタV_1として使用される。次にイニシャルベクタV_1は暗号処理ユニットEncにより暗号処理され、途中データD_1として出力される。次に途中データD_1と暗号文C_1の排他的論理和演算が行われ、P_1が出力される。そして、次のブロックである暗号文C_2の復号化のために、前述した途中データD_1がレジスタIVにセットされ、イニシャルベクタV_2として使用される。そして、以下同様にレジスタIVが更新され、ブロック単位で暗号文Ciの復号化が行われる。

【００１４】

以下に、OFBモードの処理を表す式を示す。

暗号化：V_1=[初期値] (i=1)
$Vi=D_{i-1}$ (i=2,3,・・・)
Di=Enc(Vi) (i=1,2,3,・・・)
Ci=Pi XOR Di (i=1,2,3,・・・)
復号化：V_1=[初期値] (i=1)
$Vi=D_{i-1}$ (i=2,3,・・・)
Di=Enc(Vi) (i=1,2,3,・・・)
Pi=Ci XOR Di (i=1,2,3,・・・)

以上のように、DES方式には異なる態様で暗号化および復号化を行う4つの動作モードが存在する。そして、スマートカード等の小型携帯用情報記憶媒体に使用される当該暗号化・復号化回路には、これら全ての動作モードに対応でき、さらに小型であることが要求されている。

【００１５】

特許文献１では、特殊な回路構成により、DES方式のCBCモードとCFBモードの両方を実行できる暗号化回路ついて記載している。

【００１６】

また、特許文献２では、暗号化処理をホストコンピュータと切り離し、独立させることにより、アクセス処理も含めてホストコンピュータの処理を軽減する旨が記載されている。

【００１７】

また、特許文献３では、ブロック化された平文データの複数ブロックを一度に読み込み可能なバッファを設け、当該バッファに読み込み可能なブロック数よりも少ないブロック数を読み込むことで、暗号化チェーンの切れ目による特殊な処理による平文データの上書きを解消する旨が記載されている。

【特許文献１】特開2000-75785号公報
【特許文献２】特開2004-126323号公報
【特許文献３】特開2006-330126号公報

【発明の開示】

【発明が解決しようとする課題】
【００１８】
しかしながら、従来は、前述したとおり、平文とイニシャルベクタに対して行われる暗号・復号処理と排他的論理和演算は、動作モードに応じて、その順序と組み合わせが異なるため、暗号化・復号化回路は、動作モード別の回路を全て搭載させるなど、小型化が困難であった。
【００１９】
そこで、本発明の目的は、DES方式やAES方式で規定された各動作モードに対応できる小型の暗号化・復号化回路を提供することにある。
【課題を解決するための手段】
【００２０】
１つの態様によれば、複数動作モードに対応して、暗号化及び復号化を行う暗号化・復号化回路において、入力端子から入力されるテキストデータとイニシャルベクタデータ(以下イニシャルベクタをIVと称する)とを前記動作モードに応じて第1または第2の出力端子に出力するスワップ回路と、前記第1の出力端子から前記テキストデータまたはIVデータのいずれか一方を入力し、暗号処理及び復号処理を行う暗号・復号処理ユニットと、前記第2の出力端子から前記IVデータまたはテキストデータのいずれか他方を入力し、排他的論理和演算を行う排他的論理和処理ユニットとを有し、前記スワップ回路は、前記テキストデータを格納する第1のレジスタと、前記IVデータを格納する第2のレジスタと、動作モード信号に応答して、前記第1または第2のレジスタの出力のいずれか一方を選択して前記第1の出力端子に出力する第1のセレクタと、動作モード信号に応答して、前記第1または第2のレジスタの出力のいずれか他方を選択して前記第2の出力端子に出力する第2のセレクタとを有し、さらに、前記暗号・復号処理ユニットの出力と、前記排他的論理和処理ユニットの出力と、前記第1のレジスタに格納されたテキストデータと、前記第2のレジスタに格納されたIVデータとに応じて、更新されたIVデータを前記第2のレジスタに出力するIV更新ユニットを有することを特徴とする。
【００２１】
別の態様によれば、複数動作モードに対応して、暗号化及び復号化を行う暗号化・復号化回路において、入力端子から入力されるテキストデータとイニシャルベクタデータ(以下イニシャルベクタをIVと称する)とを前記動作モードに応じて第1または第2の出力端子に出力するスワップ回路と、前記第1の出力端子から前記テキストデータまたはIVデータのいずれか一方を入力し、暗号処理及び復号処理を行う暗号・復号処理ユニットと、前記第2の出力端子から前記IVデータまたはテキストデータのいずれか他方を入力し、排他的論理和演算を行う排他的論理和処理ユニットとを有し、前記スワップ回路は、テキストデータ書き込みイネーブル信号またはIVデータ書き込みイネーブル信号に応答して、前記テキストデータまたはIVデータをそれぞれ格納し、前記第1、第2の出力端子にそれぞれ出力する第1、第2のレジスタと、動作モード信号に応答して、前記テキストデータ書き込みイネーブル信号またはIVデータ書き込みイネーブル信号のいずれか一方を選択して前記第1のレジスタに供給する第1のセレクタと、いずれか他方を選択して前記第2のレジスタに供給する第2のセレクタとを有し、さらに、前記暗号・復号処理ユニットの出力と、前記排他的論理和処理ユニットの出力と、前記第1または第2のレジスタに格納されたテキストデータと、前記第1または第2のレジスタに格納されたIVデータとに応じて、更新されたIVデータを前記第1または第2のレジスタに出力するIV更新ユニットを有することを特徴とする。
【発明の効果】
【００２２】
上記発明によれば、小型の暗号化・復号化回路を提供することができる。
【発明を実施するための最良の形態】
【００２３】
以下，図面にしたがって本発明の実施の形態について説明する。但し，本発明の技術的

範囲はこれらの実施の形態に限定されず，特許請求の範囲に記載された事項とその均等物まで及ぶものである。

【００２４】

以下、本実施の形態に関して、DES方式の暗号化・復号化回路を例に説明するが、AES方式に関しても同様の実施の形態が可能である。

【００２５】

前述したとおり、DES方式において、平文とイニシャルベクタに対して暗号・復号処理と排他的論理和演算が行われる。そして、各動作モードに応じて、その順序と組み合わせが異なる。そのため、全ての動作モードに対応可能な暗号化・復号化回路は、暗号・復号処理ユニットと排他的論理和処理ユニットとを有し、平文とイニシャルベクタは、各動作モードの規定に応じて暗号・復号処理ユニットと排他的論理和処理ユニットに入力される。また、以降、本実施の形態における暗号化・復号化回路に入力される、暗号化のためにブロック化された平文、若しくは復号化のためにブロック化された暗号文をTEXTデータと称し、イニシャルベクタをIVデータと称する。また、暗号化もしくは復号化されて出力されるデータを、それぞれ暗号化データ及び復号化データと称する。

【００２６】

はじめに、前述した各動作モードの説明を参照し、TEXTデータとIVデータのいずれの入力データが、直接的に暗号・復号処理されるかを示す。ECBモードでは、IVデータは使用せず、TEXTデータが暗号・復号処理される。また、CBCモードでは、暗号化において、直接的に暗号処理される入力データはないが、復号化において、TEXTデータが復号処理される。そして、CFBモードとOFBモードでは、IVデータが暗号・復号処理される。

【００２７】

以上の動作を実現するために、本実施の形態における暗号化・復号化回路は、動作モードに応じてデータの入れ替えを行うスワップ回路を有する。これより、ECBモードとCBCモードのときは、TEXTデータが暗号・復号処理ユニットに入力され、CFBモードとOFBモードのときは、IVデータが暗号・復号処理ユニットに入力される。

【００２８】

図5は、本実施の形態における暗号化・復号化を行うシステムの構成例である。暗号化・復号化マクロ100とメモリ104と鍵レジスタ106は、バス105を介してCPU103により制御され、暗号化および復号化は暗号化・復号化マクロ100により行われる。また、暗号化・復号化マクロ100は、スワップ回路90a、暗号化・復号化演算ユニット101、モード設定ユニット102とを有する。また、スワップ回路90aは、メモリ104から入力データI_DTとして入力されるTEXTデータとIVデータのいずれかがセットされるレジスタreg41とレジスタreg42を有する。そして、暗号化・復号化演算ユニット101は、前述した暗号・復号処理ユニット1と排他的論理和処理ユニット2とを有し、さらに、一連の暗号化において、2回目以降のブロック暗号化を行うために、IVデータの更新を行うIV更新ユニット50を有する。また、モード設定ユニット102は、各動作モードに対応した動作モード信号ecb、cbc、cfb、ofbをスワップ回路90aと暗号化・復号化演算ユニット101に送信する。そして、それら動作モード信号に応じて、スワップ回路90aが有するレジスタから、暗号化・復号化ユニット演算101が有する暗号・復号処理ユニット1と排他的論理和処理ユニット2に、各動作モードに規定されたデータが入力される。なお、暗号化・復号化には、パラメータである鍵が用いられ、暗号・復号処理ユニット1は、この鍵を用いて暗号演算もしくは復号演算を行う。

【００２９】

次に、図5における暗号化・復号化システムの動作を、図6に示すフローチャートを用いて説明する。図6は、CBCモード、CFBモード、OFBモードの暗号化・復号化処理の流れを示すフローチャートである。

【００３０】

図5において、スワップ回路90aと暗号化・復号化演算ユニット101に、モード設定ユニット102から、設定に応じた動作モード信号がアサートされている。

【００３１】
初回のTEXTデータ暗号化・復号化のために、メモリ104から入力データI_DTとしてIVデータの初期値が入力され、レジスタreg41にセットされる(ステップT1)。次に、メモリ104から入力データI_DTとしてTEXTデータが入力され、レジスタreg42にセットされる(ステップT2)。
【００３２】
暗号化・復号化マクロ100は、ステップT1、T2によりレジスタにセットされたデータは、スワップ回路90aの機能により、各動作モードの規定に応じた処理ユニット1、2に入力され、暗号化・復号化が行われる(ステップT3)。
【００３３】
そして、暗号化・復号化されたデータが、出力データO_DTとして出力され、バス105を介してメモリ104に格納される(ステップT4)。
【００３４】
そして、次のTEXTデータ暗号化・復号化のために、IV更新ユニット50は各動作モードの規定に応じてIVデータを更新する。そして、その更新されたIVデータは、ステップT1でIVデータがセットされたレジスタと同じレジスタreg41にセットされる(ステップT5)。
【００３５】
そして、暗号化・復号化される後続のTEXTデータがある場合は処理をステップT2に移し、後続のTEXTデータがない場合は終了する(ステップT6)。
【００３６】
なお、本実施の形態においては、以上のとおり暗号化・復号化が行われるが、実際の構成と処理の流れはこれに限ったものではない。
【００３７】
[第1の実施の形態]
図7は、第1の実施の形態における暗号化・復号化回路に用いられる、スワップ回路の構成図である。スワップ回路90は、TEXTレジスタ3とIVレジスタ4とセレクタSEL11とセレクタSEL12とを有する。また、符号w1～w8は経路若しくはその経路に送信されるデータを表す。
【００３８】
はじめに、本第1の実施の形態の概要を説明する。スワップ回路90は、入力データI_DTであるTEXTデータとIVデータがセットされる専用のレジスタとして、TEXTレジスタ3とIVレジスタ4を有する。そして、スワップ回路90は、各々のレジスタにセットされたデータを、動作モードの規定に応じて、セレクタSEL11、SEL12を用いてスワップさせ、暗号・復号処理ユニット1もしくは排他的論理和処理ユニット2のいずれかに入力させる。すなわち、スワップ回路90では、TEXTデータとIVデータのセットされるレジスタは決められており、動作モードに応じてレジスタにセットされたデータの出力先を切り替える。
【００３９】
次に、スワップ回路90が有する構成要素の動作を説明する。TEXTレジスタ3とIVレジスタ4は、入力データI_DTであるTEXTデータとIVデータがそれぞれセットされる専用のレジスタである。また、各々の入力データI_DTは同一の経路から入力される。そして、TEXTレジスタ3には、TEXTデータ書き込みイネーブル信号TEXT_WRのアサートに対応して、経路w1を介してTEXTデータがセットされる。また、同様にIVレジスタ4には、IVデータ書き込みイネーブル信号IV_WRのアサートに応答して、経路w2を介してIVデータがセットされる。
【００４０】
セレクタSEL11、SEL12は、レジスタ3、4と同じビット長を有し、TEXTレジスタ3にセットされたTEXTデータとIVレジスタ4にセットされたIVデータとのいずれかを選択して、各処理ユニットに出力する。また、セレクタSEL11は、CFBモード信号cfbとOFBモード信号ofbを制御入力とし、両信号の論理和演算(OR)を行う。以下、演算式”｜”は、論理和(OR)を示す。そして、セレクタSEL11は、演算値(cfb|ofb)=0の場合、TEXTレジスタ3を選択し、TEXTデータが経路w3、w7を介して暗号・復号処理ユニット1に入力される。また、セレ

クタSEL11は、演算値(cfb|ofb)=1の場合、IVレジスタ4を選択し、IVデータが経路w6、w7を介して暗号・復号処理ユニット1に入力される。つまり、動作モード信号cfb、ofbのいずれかが有効「1」になったとき、IVレジスタ4内のIVデータが暗号・復号処理ユニット1に入力される。同様に、セレクタSEL12は、演算値(cfb|ofb)=0の場合、IVレジスタ4を選択し、IVデータが経路w4、w8を介して排他的論理和処理ユニット2に入力さる。また、セレクタSEL12は、演算値(cfb|ofb)=1の場合、TEXTレジスタ3を選択し、TEXTデータが経路w5、w8を介して排他的論理和処理ユニット2に入力される。

【００４１】

暗号・復号処理ユニット1は、入力データw7に対し暗号処理もしくは復号処理を行い、排他的論理和処理ユニット2は、入力データw8に対し排他的論理和処理を行う。

【００４２】

次に、スワップ回路90の動作モード別の具体的な動作を説明する。まず、IVレジスタ4へのIVデータ書き込みイネーブル信号IV_WR のアサートに応答して、入力データI_DTとしてIVデータが経路w2を介してIVレジスタ4にセットされる。そして、TEXTレジスタ3へのTEXTデータ書き込みイネーブル信号TEXT_WRのアサートに応答して、入力データI_DTとしてTEXTデータが経路w1を介してTEXTレジスタ3にセットされる。

【００４３】

それから、CBCモードの場合は、演算値(cfb|ofb)=0であり、セレクタSEL11はTEXTレジスタ3を選択し、セレクタSEL12はIVレジスタ4を選択しているため、TEXTデータは経路w3、w7を介して暗号・復号処理ユニット1に入力され、IVデータは経路w4、w8を介して排他的論理和処理ユニット2に入力される。

【００４４】

また、CFBモードもしくはOFBモードの場合は、演算値(cfb|ofb)=1であり、セレクタSEL11はIVレジスタ4を選択し、セレクタSEL12はTEXTレジスタ3を選択しているため、IVデータは経路w6、w7を介して暗号・復号処理ユニット1に入力され、TEXTデータは経路w5、w8を介して排他的論理和処理ユニット2に入力される。

【００４５】

次に、DES方式の全ての動作モードに対応可能な、スワップ回路90を用いた暗号化回路の構成について説明する。

【００４６】

図8は、スワップ回路90で構成した暗号化回路の模式図であり、DES方式における4つの動作モード全てに対応できる構成である。また、符号w1、w2、・・・は、経路若しくはその経路に送信されるデータを表す。

【００４７】

前述した暗号・復号処理ユニット1もしくは排他的論理和処理ユニット2に入力されたデータは、各動作モードの規定に対応して経路w50、w60を介して各ユニット間で受け渡され、暗号化もしくは復号化が行われ、データO_DTとして出力される。

【００４８】

IV更新ユニット50は、各動作モードの規定に応じてIVデータを更新し、経路w70を介して、更新されたIVデータをIVレジスタ4にセットする。つまりCBCモードとCFBモードとOFBモードの2回目以降のTEXTデータの暗号化・復号化においては、前回の暗号化・復号化の演算結果等によりIVデータが更新されるが、本実施の形態における暗号化回路において、IV更新ユニット50が、このIVデータの更新処理を行う。そして、IV更新ユニット50は、データw10～w15を入力とし、各動作モードに応じてIV更新処理を行うCFBフィードバック部CFB_FBとOFBフィードバック部OFB_FBとCBCフィードバック部CBC_FBとを有する。

【００４９】

IVレジスタ4には、経路w2と経路w70のデータ入力経路がある。つまり前述したように、初回の暗号化において使用されるIVデータは、経路w2を介してIVレジスタ4にセットされ、2回目以降に使用されるIVデータは、IV更新ユニット50により更新され、経路w70を介してIVレジスタ4にセットされる。例えばCBCモードの暗号化においては、図2のブロック図

に示すように、暗号処理ユニットEncにより暗号処理された暗号文CiがレジスタIVにセットされるが、同様に、図8において、暗号・復号処理ユニット1により暗号化された暗号文Ciに相当するデータが、経路w50、w14を介してIV更新ユニット50のCBCフィードバック部CBC_FBに入力され、経路w70を介してIVレジスタ4にセットされる。同様に、CBCモードの復号化においては、図2のブロック図に示すように、暗号文CiがレジスタIVにセットされるが、図8において、復号化される暗号文Ciに相当するTEXTデータが、経路w3、w7、w9、w15を介してIV更新ユニット50のCBCフィードバック部CBC_FBに入力され、経路w70を介してIVレジスタ4にセットされる。

【００５０】

図9は、図8の模式図の具体的な回路構成例である。図9中の点線で示される部分は、図8のCFBフィードバック部CFB_FBとOFBフィードバック部OFB_FBとCBCフィードバック部CBC_FBに相当し、各々のフィードバック部が、次の暗号化で使用する更新されたIVデータw71～w73をセレクタSEL38に出力する。そして、セレクタSEL38は、CBCモード信号cbcとCFBモード信号cfbとOFBモード信号ofbとを制御入力とし、これら動作モード信号に応じて更新IVデータw71～w73のいずれかをデータw70aとして出力する。なお、各フィードバック部CFB_FB、OFB_FB、CBC_FBの動作についての詳細は後述する。

【００５１】

セレクタSEL39は、busy信号を制御入力とし、busy=0のときは入力データw2をデータw80として出力し、busy=1のときは入力データw70aをデータw80として出力する。これより、IVデータは、初回の暗号化においては、busy=0とすることで経路w2を介してIVレジスタ4にセットされ、暗号化演算がはじまってからは常にbusy=1とすることで、経路w70aを介してIVレジスタ4にセットされる。

【００５２】

以下、図8を用いて図10～図15により、各動作モードの動作説明をする。各図において、動作時にデータ送信に使用される経路とアサートされる動作モード信号と動作する構成要素のみ実線で示し、他は点線とした。また、IV更新ユニット50の動作に関しては、図9の具体例も併用して説明する。

【００５３】

[ECBモード]

図10は第1の実施の形態における暗号化・復号化回路の、ECBモードの暗号化・復号化時の動作図である。

【００５４】

暗号化において、TEXTレジスタ3には、TEXTデータ書き込みイネーブル信号TEXT_WRのアサートに応答して、経路w1を介してTEXTデータがセットされる。また、ECB暗号化モードでは、動作モード信号の演算値(cfb|ofb)=0であり、セレクタSEL11は、経路w3を選択する。それより、TEXTデータが暗号・復号処理ユニット1に経路w3、w7を介して入力され、暗号化されて暗号化データO_DTとして出力される。以下同様に、TEXTデータがTEXTレジスタ3にセットされ、暗号・復号処理ユニット1により暗号化されて暗号化データO_DTとして出力される。

【００５５】

一方、復号化において、TEXTレジスタ3には、TEXTデータ書き込みイネーブル信号TEXT_WRのアサートに応答して、経路w1を介して暗号文であるTEXTデータがセットされる。また、ECB復号化モードでは、動作モード信号の演算値(cfb|ofb)=0であり、セレクタSEL11は、経路w3を選択する。それより、TEXTデータが暗号・復号処理ユニット1に経路w3、w7を介して入力され、復号化されて復号化データO_DTとして出力される。以下同様に、TEXTデータがTEXTレジスタ3にセットされ、暗号・復号処理ユニット1により復号化されて復号化データO_DTとして出力される。

【００５６】

以上の動作は、図1で説明したECBモードの態様と一致している。なお、ECBモードでは、IVデータは使用されず、IV更新ユニット50は動作しない。

【００５７】
[CBCモード]
図11は第1の実施の形態における暗号化・復号化回路の、CBCモードの暗号化時の動作図である。
【００５８】
暗号化において、初回のTEXTデータ暗号化のために、IVレジスタ4には、IVデータ書き込みイネーブル信号IV_WRのアサートに応答して、経路w2を介してIVデータの初期値がセットされる。次に、TEXTレジスタ3には、TEXTデータ書き込みイネーブル信号TEXT_WRのアサートに応答して、経路w1を介してTEXTデータがセットされる。また、CBC暗号化モードでは、動作モード信号の演算値(cfb|ofb)=0であり、セレクタSEL11は、経路w3を選択し、セレクタSEL12は、経路w4を選択する。
【００５９】
そして、経路w3、w7、w9を介してTEXTデータが、また、経路w4、w8を介してIVデータが排他的論理和処理ユニット2に入力され、排他的論理和演算が行われる。そして、その結果である図2の途中データDiに相当するデータw60が暗号・復号処理ユニット1に入力され、暗号処理され、暗号化データO_DTとして出力される。
【００６０】
そして、次のTEXTデータ暗号化のために、前述した暗号化データO_DTは、経路w50、w14を介してIV更新ユニット50のCBCフィードバック部CBC_FBに入力され、IVデータ書き込みイネーブル信号IV_WRのアサートに応答して、経路w70を介してIVレジスタ4にセットされる。次に、TEXTレジスタ3には、TEXTデータ書き込みイネーブル信号TEXT_WRのアサートに応答して、経路w1を介してTEXTデータがセットされる。そして、以下同様に暗号化が繰り返される。
【００６１】
図12は第1の実施の形態における暗号化・復号化回路の、CBCモードの復号化時の動作図である。
【００６２】
復号化において、初回のTEXTデータ復号化のために、IVレジスタ4には、IVデータ書き込みイネーブル信号IV_WRのアサートに応答して、経路w2を介してIVデータの初期値がセットされる。次に、TEXTレジスタ3には、TEXTデータ書き込みイネーブル信号TEXT_WRのアサートに応答して、経路w1を介して暗号文であるTEXTデータがセットされる。また、CBC復号化モードでは、動作モード信号の演算値(cfb|ofb)=0であり、セレクタSEL11は、経路w3を選択し、セレクタSEL12は、経路w4を選択する。
【００６３】
そして、TEXTデータは、経路w3、w7を介して暗号・復号処理ユニット1に入力され、復号処理され、図2の途中データDiに相当するデータw50が排他的論理和処理ユニット2に入力される。また、経路w4、w8を介してIVデータが排他的論理和処理ユニット2に入力され、復号処理されたTEXTデータと排他的論理和演算される。そして、その結果である復号化データが経路w60を介して暗号・復号処理ユニット1に送信され、復号化データO_DTとして出力される。
【００６４】
そして、次のTEXTデータ復号化のために、TEXTレジスタ3内のTEXTデータは、経路w3、w7、w9、w15を介してIV更新ユニット50 のCBCフィードバック部CBC_FBに入力され、IVデータ書き込みイネーブル信号IV_WRのアサートに応答して、経路w70を介してIVレジスタ4にセットされる。次に、TEXTレジスタ3には、TEXTデータ書き込みイネーブル信号TEXT_WRのアサートに応答して、経路w1を介してTEXTデータがセットされる。そして、以下同様に復号化が繰り返される。
【００６５】
ここで、図8と図9において、ともに対応するCBCフィードバック部CBC_FBに関して説明する。図9において、セレクタSEL37は、動作モード信号cbc、decを制御入力とし、暗号化

時の暗号化データw14と復号化時のTEXTデータw15を切り替える。すなわち、CBC暗号化時はCBCモード信号cbcのアサートに応答して、入力データw14をデータw73として出力し、CBC復号化時はCBCモード信号cbcとDEC信号decのアサートに応答して、入力データw15をデータw73として出力する。

【００６６】

以上の動作は、図2で説明したCBCモードの態様と一致している。

【００６７】

[CFBモード]

図13は第1の実施の形態における暗号化・復号化回路の、CFBモードの暗号化時の動作図である。図3で説明したようにCFBモードにおいては、64bit長のTEXTデータは、さらにk-bitに分割され、k-bit単位で暗号化が行われる。そのため、以下に示す本実施の形態における暗号化・復号化回路の、CFBモードの動作では、各々の処理は64bit長で行われるが、データの上位k-bitのみを暗号化データの有効値とする。すなわち、有効なTEXTデータは、TEXTレジスタの上位k-bitにセットされ、残りの下位ビットには例えば0値がセットされて、64bit長の暗号化が行われる。そして、64bit長の暗号化データの上位k-bitのみを有効値とする。また、上位k-bitを有効なTEXTデータとし、残りの下位ビットは0値とした64bit長のTEXTデータを入力前に作成し、その64bit長のデータを入力してTEXTレジスタにセットしてもよい。

【００６８】

暗号化において、初回のTEXTデータ暗号化のために、IVレジスタ4には、IVデータ書き込みイネーブル信号IV_WRのアサートに応答して、経路w2を介して64bit長のIVデータの初期値がセットされる。次に、TEXTレジスタ3の上位k-bitには、TEXTデータ書き込みイネーブル信号TEXT_WRのアサートに応答して、経路w1を介してk-bit長のTEXTデータがセットされ、残りの下位ビットには0値がセットされる。また、CFB暗号化モードでは、動作モード信号の演算値(cfb|ofb)=1であり、セレクタSEL11は、経路w6を選択し、セレクタSEL12は、経路w5を選択する。

【００６９】

そして、IVデータは、経路w6、w7を介して暗号・復号処理ユニット1に入力され、暗号処理され、図3の途中データDiに相当するデータw50が排他的論理和処理ユニット2に入力される。また、経路w5、w8を介してTEXTデータが排他的論理和処理ユニット2に入力され、暗号処理されたIVデータw50と排他的論理和演算される。そして、その結果である暗号化データが経路w60を介して暗号・復号処理ユニット1に送信され、有効値である上位k-bitが暗号化データO_DTとして出力される。

【００７０】

そして、次のTEXTデータ暗号化のために、IVレジスタ4内のIVデータが経路w6、w7、w9、w10を介して、また、前述の暗号化データが経路w60、w11を介して、IV更新ユニット50のCFBフィードバック部CFB_FBに入力され、ビット処理され、IVデータ書き込みイネーブル信号IV_WRのアサートに応答して、経路w70を介してIVレジスタ4にセットされる。なお、CFBフィードバック部CFB_FBにおけるビット処理は後述する。次に、TEXTレジスタ3の上位k-bitには、TEXTデータ書き込みイネーブル信号TEXT_WRのアサートに応答して、経路w1を介して、後続するk-bitのTEXTデータがセットされ、残りの下位ビットには0値がセットされる。そして、以下同様に暗号化が繰り返される。

【００７１】

図14は第1の実施の形態における暗号化・復号化回路の、CFBモードの復号化時の動作図である。

【００７２】

復号化において、初回のTEXTデータ復号化のために、IVレジスタ4には、IVデータ書き込みイネーブル信号IV_WRのアサートに応答して、経路w2を介して64bit長のIVデータの初期値がセットされる。次に、TEXTレジスタ3の上位k-bitには、TEXTデータ書き込みイネーブル信号TEXT_WRのアサートに応答して、経路w1を介して暗号文であるk-bit長のTEXTデー

タがセットされ、残りの下位ビットには0値がセットされる。また、CFB復号化モードでは、動作モード信号の演算値(cfb|ofb)=1であり、セレクタSEL11は、経路w6を選択し、セレクタSEL12は、経路w5を選択する。

【００７３】

そして、IVデータは、経路w6、w7を介して暗号・復号処理ユニット1に入力され、暗号処理され、図3の途中データDiに相当するデータw50が排他的論理和処理ユニット2に入力される。また、経路w5、w8を介してTEXTデータが排他的論理和処理ユニット2に入力され、暗号処理されたIVデータw50と排他的論理和演算される。そして、その結果である復号化データが経路w60を介して暗号・復号処理ユニット1に送信され、有効値である上位k-bitが復号化データO_DTとして出力される。

【００７４】

そして、次のTEXTデータ復号化のために、IVレジスタ4内のIVデータが経路w6、w7、w9、w10を介して、また、TEXTレジスタ3内のTEXTデータが経路w5、w8、w12を介して、IV更新ユニット50のCFBフィードバック部CFB_FBに入力され、ビット処理され、IVデータ書き込みイネーブル信号IV_WRのアサートに応答して、経路w70を介してIVレジスタ4にセットされる。次に、TEXTレジスタ3の上位k-bitには、TEXTデータ書き込みイネーブル信号TEXT_WRのアサートに応答して、経路w1を介して後続するk-bitのTEXTデータがセットされ、残りの下位ビットには0値がセットされる。そして、以下同様に復号化が繰り返される。

【００７５】

ここで、図8と図9において、ともに対応するCFBフィードバック部CFB_FBに関して説明する。図9において、第1のビット処理部61は暗号化・復号化時のIVデータw10をk-bit左シフトし、データw91として出力する。また、セレクタSEL34は、動作モード信号cfb、decを制御入力とし、暗号化時の暗号化データw11と復号化時のTEXTデータw12を切り替える。すなわち、CFB暗号化時はCFBモード信号cfbのアサートに応答して、暗号化データw11をデータw93として出力し、CFB復号化時はCFBモード信号cfbとDEC信号decのアサートに応答して、TEXTデータw12をデータw93として出力する。また、第2のビット処理部63は入力データw93の上位k-bitをデータw92として出力する。そして、最終的にCFBフィードバック部CFB_FBは、第1のビット処理部によりk-bit左シフトされたデータw91の下位k-bitにk-bitのデータw92を加えて、新規のIVデータw71として出力する。

【００７６】

以上の動作は、図3で説明したCFBモードの態様と一致している。

【００７７】

[OFBモード]

図15は第1の実施の形態における暗号化・復号化回路の、OFBモードの暗号化・復号化時の動作図である。

【００７８】

暗号化において、初回のTEXTデータ暗号化のために、IVレジスタ4には、IVデータ書き込みイネーブル信号IV_WRのアサートに応答して、経路w2を介してIVデータの初期値がセットされる。次に、TEXTレジスタ3には、TEXTデータ書き込みイネーブル信号TEXT_WRのアサートに応答して、経路w1を介してTEXTデータがセットされる。また、OFB暗号化モードでは、動作モード信号の演算値(cfb|ofb)=1であり、セレクタSEL11は、経路w6を選択し、セレクタSEL12は、経路w5を選択する。

【００７９】

そして、IVデータは、経路w6、w7を介して暗号・復号処理ユニット1に入力され、暗号処理され、図4の途中データDiに相当するデータw50が排他的論理和処理ユニット2に入力される。また、経路w5、w8を介してTEXTデータが排他的論理和処理ユニット2に入力され、暗号処理されたIVデータw50と排他的論理和演算される。そして、その結果である暗号化データが経路w60を介して暗号・復号処理ユニット1に送信され、暗号化データO_DTとして出力される。

【００８０】

そして、次のTEXTデータ暗号化のために、前述した途中データDiが、経路w50、w13を介してIV更新ユニット50のOFBフィードバック部OFB_FBに入力され、IVデータ書き込みイネーブル信号IV_WRのアサートに応答して、経路w70を介してIVレジスタ4にセットされる。なお、OFBフィードバック部OFB_FBは、図9に示すとおり単なるフィードバック経路である。次に、TEXTレジスタ3には、TEXTデータ書き込みイネーブル信号TEXT_WRのアサートに応答して、経路w1を介してTEXTデータがセットされる。そして、以下同様に暗号化が繰り返される。

【００８１】

一方、復号化において、初回のTEXTデータ復号化のために、IVレジスタ4には、IVデータ書き込みイネーブル信号IV_WRのアサートに応答して、経路w2を介してIVデータの初期値がセットされる。次に、TEXTレジスタ3には、TEXTデータ書き込みイネーブル信号TEXT_WRのアサートに応答して、経路w1を介して暗号文であるTEXTデータがセットされる。また、OFB復号化モードでは、動作モード信号の演算値(cfb|ofb)=1であり、セレクタSEL11は、経路w6を選択し、セレクタSEL12は、経路w5を選択する。

【００８２】

そして、IVデータは、経路w6、w7を介して暗号・復号処理ユニット1に入力され、暗号処理され、図4の途中データDiに相当するデータw50が排他的論理和処理ユニット2に入力される。また、経路w5、w8を介してTEXTデータが排他的論理和処理ユニット2に入力され、暗号処理されたIVデータw50と排他的論理和演算される。そして、その結果である復号化データが経路w60を介して暗号・復号処理ユニット1に送信され、復号化データO_DTとして出力される。

【００８３】

そして、次のTEXTデータ復号化のために、前述した途中データDiが、経路w50、w13を介してIV更新ユニット50のOFBフィードバック部OFB_FBに入力され、IVデータ書き込みイネーブル信号IV_WRのアサートに応答して、経路w70を介してIVレジスタ4にセットされる。次に、TEXTレジスタ3には、TEXTデータ書き込みイネーブル信号TEXT_WRのアサートに応答して、経路w1を介してTEXTデータがセットされる。以下同様に復号化が繰り返される。

【００８４】

以上の動作は、図4で説明したOFBモードの態様と一致している。

【００８５】

[第2の実施の形態]

図16は、第2の実施の形態における暗号化・復号化回路に用いられる、スワップ回路の構成図である。スワップ回路95は、レジスタreg31とレジスタreg32とセレクタSEL21とセレクタSEL22とを有する。また、符号w1、w2、w7、w8は経路若しくはその経路に送信されるデータを表す。

【００８６】

はじめに本第2の実施の形態の概要を説明する。スワップ回路95は、入力データI_DTであるTEXTデータもしくはIVデータのいずれかがセットされる共用のレジスタreg31、reg32を有する。そして、レジスタreg31、reg32には、セレクタSEL21、SEL22から、動作モードの規定に応じてTEXTデータ書き込みイネーブル信号TEXT_WRもしくはIVデータ書き込みイネーブル信号IV_WRを示す書き込みイネーブル信号reg1_wr、reg2_wrがアサートされる。これより、レジスタreg31、reg32には、TEXTデータ若しくはIVデータのいずれかがセットされる。そして、レジスタreg31にセットされたデータは、経路w7を介して暗号・復号処理ユニット1に入力され、レジスタreg32にセットされたデータは、経路w8を介して排他的論理和処理ユニット2に入力される。すなわち、スワップ回路95では、各々のレジスタにセットされたデータに対して行われる処理は決まっており、動作モードに応じて各々のレジスタにTEXTデータまたはIVデータがセットされる。

【００８７】

また、第1の実施の形態におけるスワップ回路90では、TEXTレジスタとIVレジスタを切り替えるために、レジスタ長と同じビット長のセレクタSEL11、SEL12を必要とする。一方

で、本第2の実施の形態におけるスワップ回路95では、動作モードに応じた書き込みイネーブル信号reg1_wr、reg2_wrをレジスタreg31、reg32にアサートするために、1bit長のセレクタSEL21、SEL22を用い、いずれかの書き込みイネーブル信号を選択する。すなわち、例えばDES方式における各々の動作モードに対応するために、第1の実施の形態におけるスワップ回路90では、2つの64bit長のセレクタが必要であるのに対し、第2の実施の形態におけるスワップ回路95においては、2つの1bit長のセレクタを用いればよい。これより、本第2の実施の形態によれば、セレクタのbit長を減少させることができ、配線数も減少させることができ、回路規模の小型化と省電力化が可能である。

【００８８】

なお、本第2の実施の形態のセレクタを使用することにより、簡単な構成でデータの分割入力を行うことができる。例えばDES方式の64bit長のレジスタに32bitづつ2回の入力を行う場合、32bit毎のレジスタそれぞれに1bitのセレクタを用いて前述と同様の入力処理を行えばよい。すなわち、データの分割入力を行う場合に、その分割数に応じた数ビットのセレクタで対応できる。

【００８９】

次に、スワップ回路95が有する構成要素の動作を説明する。レジスタreg31、reg32は、入力データI_DTであるTEXTデータもしくはIVデータのいずれかがセットされる共用のレジスタであり、各々の入力データI_DTは同一の経路から入力される。

【００９０】

セレクタSEL21は、動作モード信号cfb、ofbを制御入力とし、TEXTデータ書き込みイネーブル信号TEXT_WRとIVデータ書き込みイネーブル信号IV_WRを入力とし、レジスタreg31に書き込みイネーブル信号reg1_wrを出力する。つまり、セレクタSEL21は、動作モード信号cfb、ofbに応じて、TEXTデータ書き込みイネーブル信号TEXT_WR若しくはIVデータ書き込みイネーブル信号IV_WRのいずれかを選択し、書き込みイネーブル信号reg1_wrとしてレジスタreg31に出力する。

【００９１】

ECBモードとCBCモードの時は、演算値(cfb|ofb)=0であり、レジスタreg31には書き込みイネーブル信号reg1_wrとしてTEXT_WRがアサートされる。また、CFBモードとOFBモードの時は、演算値(cfb|ofb)=1であり、レジスタreg31には書き込みイネーブル信号reg1_wrとしてIV_WRがアサートされる。そして、書き込みイネーブル信号reg1_wrがTEXT_WRのときは、レジスタreg31にTEXTデータがセットされ、書き込みイネーブル信号reg1_wrがIV_WRのときは、レジスタreg31にIVデータがセットされる。

【００９２】

セレクタSEL22も同様の動作を行うが、動作モード信号cfb、ofbに対応して選択されるイネーブル信号が、セレクタSEL21と逆になる。つまり、ECBモードとCBCモードの時は、演算値(cfb|ofb)=0であり、レジスタreg32には書き込みイネーブル信号reg2_wrとしてIV_WRがアサートされる。また、CFBモードとOFBモードの時は、演算値(cfb|ofb)=1となりレジスタreg32には書き込みイネーブル信号reg2_wrとしてTEXT_WRがアサートされる。

【００９３】

また、レジスタreg31にセットされたデータは経路w7を介して、暗号・復号処理ユニット1に入力され、暗号処理もしくは復号処理される。そして、レジスタreg32にセットされたデータは経路w8を介して排他的論理和処理ユニット2に入力され、排他的論理和処理される。

【００９４】

図17は、本第2の実施の形態におけるスワップ回路が有するセレクタ回路の一例である。図16、図17を用いてTEXTデータとIVデータを各々の動作モードに応じて具体的にレジスタにセットする手順を以下に示す。

【００９５】

ECBモード又はCBCモードのときは、ORゲートp1の出力は(cfb|ofb)=0である。そして、はじめにIVデータのセットを行うためTEXTデータ書き込みイネーブル信号TEXT_WR=0、IV

データ書き込みイネーブル信号IV_WR=1となる。これより、図17に示すセレクタ回路は、IVデータ書き込みイネーブル信号IV_WR=1を、ORゲートp5からは書き込みイネーブル信号reg1_wr=1として、ORゲートp4からは書き込みイネーブル信号reg2_wr=1として出力する。そして、レジスタreg31とレジスタreg32にはそれぞれの書き込みイネーブル信号reg1_wr、reg2_wrがアサートされ、それぞれのレジスタに入力データI_DTであるIVデータがセットされる。次に、TEXTデータのセットを行うためTEXTデータ書き込みイネーブル信号TEXT_WR=1、IVデータ書き込みイネーブル信号IV_WR=0となる。これより、図17に示すセレクタ回路は、TEXTデータ書き込みイネーブル信号TEXT_WR=1をORゲートp5からはイネーブル信号reg1_wr=1として出力し、ORゲートp4からはreg2_wr=0として出力する。そして、レジスタreg31には書き込みイネーブル信号reg1_wrがアサートされ、入力データI_DTであるTEXTデータがセットされる。また、レジスタreg32は書き込みイネーブル信号reg2_wr=0より、そのまま前述したIVデータを保持する。以上より、ECBモードとCBCモードのときは、レジスタreg31にTEXTデータがセットされ、レジスタreg32にIVデータがセットされる。

【００９６】

同様に、CFBモード又はOFBモードのときは、ORゲートp1の出力は(cfb|ofb)=1である。そして、はじめにIVデータのセットを行うためTEXTデータ書き込みイネーブル信号TEXT_WR=0、IVデータ書き込みイネーブル信号IV_WR=1となる。これより、図17に示すセレクタ回路は、ORゲートp4、p5から書き込みイネーブル信号reg1_wr=1、reg2_wr=1を出力する。そして、レジスタreg31とレジスタreg32には、それぞれの書き込みイネーブル信号reg1_wr、reg2_wrがアサートされ、それぞれのレジスタに入力データI_DTであるIVデータがセットされる。次に、TEXTデータのセットを行うためTEXTデータ書き込みイネーブル信号TEXT_WR=1、IVデータ書き込みイネーブル信号IV_WR=0となる。これより、図17に示すセレクタ回路は、ORゲートp4、p5からイネーブル信号reg1_wr=0、reg2_wr=1を出力する。そして、レジスタreg32には書き込みイネーブル信号reg2_wrがアサートされ、入力データI_DTであるTEXTデータがセットされる。また、レジスタreg31は書き込みイネーブル信号reg1_wr=0により、そのまま前述したIVデータを保持する。以上より、CFBモードとOFBモードのときは、ECBモードとCBCモードのときとは逆に、レジスタreg31にIVデータが格納され、レジスタreg32にTEXTデータが格納される。

【００９７】

以上のように図17に示すセレクタ回路は、動作モード信号cfb、ofbの演算値(cfb|ofb)の如何に関わらず、IVデータを両方のレジスタreg31、reg32にセットし、その後、どちらか一方のレジスタにTEXTデータを上書きしてセットする。そして、TEXTデータをセットする際に、動作モード信号cfb、ofbの演算値(cfb|ofb)に応じて、TEXTデータが上書きされるレジスタが決まる。すなわち、IVデータ入力後に動作モードの設定を行うことも可能であり、本セレクタ回路には、設定順序の自由度を広げる効果もある。

【００９８】

次に、スワップ回路95の動作モード別の具体的な動作を説明する。この別の具体例によれば、IVデータをレジスタにセットするときには、動作モード信号が確定している必要がある。すなわち、CBCモードの場合は、動作モード信号cfb、ofbはセレクタSEL21、SEL22にアサートされず、演算値(cfb|ofb)=0である。従って、書き込みイネーブル信号reg2_wrとして選択されたIV_WR のアサートに応答して、入力データI_DTであるIVデータが経路w2を介してレジスタreg32にセットされる。また、書き込みイネーブル信号reg1_wrとして選択されたTEXT_WR のアサートに応答して、入力データI_DTであるTEXTデータが経路w1を介してレジスタreg31にセットされる。これより、レジスタreg31にセットされたTEXTデータは経路w7を介して、暗号・復号処理ユニット1に入力されれ、レジスタreg32にセットされたIVデータは経路w8を介して排他的論理和処理ユニット2に入力される。

【００９９】

さらに、CFBモードの場合は、CFBモード信号cfbがセレクタSEL21、SEL22にアサート(cfb=1)されるため、演算値(cfb|ofb)=1である。従って、書き込みイネーブル信号reg1_wrとして選択されたIV_WR のアサートに応答して、入力データI_DTであるIVデータが経路w1を

介してレジスタreg31にセットされる。また、書き込みイネーブル信号reg2_wrとして選択されたTEXT_WR のアサートに応答して、入力データI_DTであるTEXTデータが経路w2を介してレジスタreg32にセットされる。これより、レジスタreg31にセットされたIVデータは経路w7を介して、暗号・復号処理ユニット1に入力され、レジスタreg32にセットされたTEXTデータは経路w8を介して排他的論理和処理ユニット2に入力される。

【０１００】

OFBモードの場合は、OFBモード信号ofbが、セレクタSEL21、SEL22にアサート(ofb=1)されるため、演算値(cfb|ofb)=1であり、CFBモードと同様のデータ入力処理が行われる。

【０１０１】

次に、DES方式の全ての動作モードに対応可能な、スワップ回路95を用いた暗号化回路の構成について説明する。

【０１０２】

図18は、スワップ回路95で構成した暗号化回路の模式図であり、DES方式における4つの動作モード全てに対応できる構成である。この暗号化回路は、スワップ回路の部分を除いて第1の実施の形態と同じ構成であるため、以下に相違する部分を説明する。

【０１０３】

IV更新ユニット50は、各動作モードの規定に応じてIVデータを更新し、経路w75若しくは経路w76を介して、更新されたIVデータをレジスタreg31若しくはレジスタreg32にセットする。

【０１０４】

また、レジスタreg31には、経路w1と経路w75のデータ入力経路がある。そして、CFBモードとOFBモードの場合は、前述したとおり、初回の暗号化において使用されるIVデータは経路w1を介してレジスタreg31にセットされる。また、2回目以降の暗号化に使用されるIVデータは、IV更新ユニット50により更新され、経路w75を介してレジスタreg31にセットされる。同様に、レジスタreg32には、経路w2と経路w76のデータ入力経路がある。そして、CBCモードの場合は、初回の暗号化において使用されるIVデータは経路w2を介してレジスタreg32にセットされる。また、2回目以降の暗号化に使用されるIVデータは、IV更新ユニット50により更新され、経路w76を介してレジスタreg32にセットされる。

【０１０５】

また、図19は、図18の模式図の具体的な回路構成例である。図9に示した第1の実施の形態における回路構成例と比較すると、出力データw71、w72、w73がレジスタにセットされるまでの経路が異なる。

【０１０６】

セレクタSEL35は、動作モード信号cfb、ofbに応じて、データw71、w72のいずれかをデータw70bとして出力する。また、セレクタSEL33は、busy=0のときは入力データw1をデータw81として出力し、busy=1のときは入力データw70bをデータw81として出力する。また、セレクタSEL36は、busy=0のときは入力データw2をデータw82として出力し、busy=1のときは入力データw73をデータw82として出力する。

【０１０７】

例えばCBCモードにおいて、1回目の暗号化におけるTEXTデータとIVデータの入力の際はbusy=0となり、レジスタreg32には経路w2を介してIVデータがセットされ、レジスタreg31には経路w1を介してTEXTデータがセットされる。そして、busy=1となり、暗号化演算が行われる。1回目の暗号化が行われた後、busy=1であるため、経路w73、w82を介して更新されたIVデータがレジスタreg32にセットされる。次に、busy=0となり、経路w1と経路w2からTEXTデータが入力される。その際、前述したとおり、CBCモードの設定によりレジスタreg31の書き込みイネーブル信号reg1_wr=1であり、レジスタreg31にはTEXTデータがセットされる。一方、レジスタreg32の書き込みイネーブル信号reg2_wr=0であり、レジスタreg32は、更新されたIVデータを保持する。そして、busy=1となり、以下同様に演算が行われる。

【０１０８】

以下、図18を用いて図20～図25により、各動作モードの動作説明をする。各図において、動作時にデータ送信に使用される経路とアサートされる動作モード信号と動作する構成要素のみ実線で示し、他は点線とした。

【０１０９】

[ECBモード]

図20は第2の実施の形態における暗号化・復号化回路の、ECBモードの暗号化・復号化時の動作図である。

【０１１０】

ECB暗号化モードでは、動作モード信号の演算値(cfb|ofb)=0であり、レジスタreg31には、書き込みイネーブル信号reg1_wrとして選択されたTEXT_WRのアサートに応答して、経路w1を介してTEXTデータがセットされる。それより、TEXTデータが暗号・復号処理ユニット1に経路w7を介して入力され、暗号化されて出力される。以下同様に、TEXTデータがレジスタreg31に経路w1を介してセットされ、暗号・復号処理ユニット1により暗号化されて暗号化データO_DTとして出力される。

【０１１１】

一方、ECB復号化モードでは、動作モード信号の演算値(cfb|ofb)=0であり、レジスタreg31には、書き込みイネーブル信号reg1_wrとして選択されたTEXT_WRのアサートに応答して、暗号文であるTEXTデータがレジスタreg31に経路w1を介してセットされる。それより、TEXTデータが暗号・復号処理ユニット1に経路w7を介して入力され、復号化されて出力される。以下同様に、TEXTデータがレジスタreg31に経路w1を介してセットされ、暗号・復号処理ユニット1により復号化されて復号化データO_DTとして出力される。

【０１１２】

以上の動作は、図1で説明したECBモードの態様と一致している。なお、ECBモードでは、IVデータは使用されず、IV更新ユニット50は動作しない。

【０１１３】

[CBCモード]

図21は第2の実施の形態における暗号化・復号化回路の、CBCモードの暗号化時の動作図である。

【０１１４】

CBC暗号化モードでは、動作モード信号の演算値(cfb|ofb)=0により、書き込みイネーブル信号reg2_wrとして選択されたIV_WRのアサートに応答して、IVデータの初期値がレジスタreg32にセットされる。このとき、図17のセレクタの場合は、IVデータの初期値はレジスタreg31にもセットされる。その後、レジスタreg31には、書き込みイネーブル信号reg1_wrとして選択されたTEXT_WRのアサートに応答して、TEXTデータがセットされる。

【０１１５】

そして、経路w7、w9を介してTEXTデータが、また、経路w8を介してIVデータが排他的論理和処理ユニット2に入力され、排他的論理和演算が行われる。そして、その結果である図2の途中データDiに相当するデータw60が暗号・復号処理ユニット1に入力され、暗号処理され、暗号化データO_DTとして出力される。

【０１１６】

そして、次のTEXTデータ暗号化のために、前述した暗号化データO_DTは、経路w50、w14を介してIV更新ユニット50のCBCフィードバック部CBC_FBに入力され、IVデータ書き込みイネーブル信号IV_WRのアサートに応答して、経路w76を介してレジスタreg32にセットされる。次に、レジスタreg31には、書き込みイネーブル信号reg1_wrとして選択されたTEXT_WRのアサートに応答して、経路w1を介してTEXTデータがセットされる。そして、以下同様に暗号化が繰り返される。

【０１１７】

図22は第2の実施の形態における暗号化・復号化回路の、CBCモードの復号化時の動作図である。

【０１１８】

CBC復号化モードでは、動作モード信号の演算値(cfb|ofb)=0により、書き込みイネーブル信号reg2_wrとして選択されたIV_WRのアサートに応答して、IVデータの初期値がレジスタreg32にセットされる。同様にして、レジスタreg31には、書き込みイネーブル信号reg1_wrとして選択されたTEXT_WRのアサートに応答して、TEXTデータがセットされる。

【０１１９】

そして、TEXTデータは、経路w7を介して暗号・復号処理ユニット1に入力され、復号処理され、図2の途中データDiに相当するデータw50が排他的論理和処理ユニット2に入力される。また、経路w8を介してIVデータが排他的論理和処理ユニット2に入力され、復号処理されたTEXTデータw50と排他的論理和演算される。そして、その結果である復号化データが経路w60を介して暗号・復号処理ユニット1に送信され、復号化データO_DTとして出力される。

【０１２０】

そして、次のTEXTデータ復号化のために、レジスタreg31内のTEXTデータが経路w7、w9、w15を介してIV更新ユニット50 のCBCフィードバック部CBC_FBに入力され、書き込みイネーブル信号reg2_wrとして選択されたIV_WRのアサートに応答して、経路w76を介してレジスタreg32にセットされる。次に、レジスタreg31には、書き込みイネーブル信号reg1_wrとして選択されたTEXT_WRのアサートに応答して、経路w1を介してTEXTデータがセットされる。以下同様に復号化が繰り返される。

【０１２１】

以上の動作は、図2で説明したCBCモードの態様と一致している。

【０１２２】

[CFBモード]

図23は第2の実施の形態における暗号化・復号化回路の、CFBモードの暗号化時の動作図である。なお、第1の実施の形態と同様に、以下に示すCFBモードにおける暗号化・復号化は、データの上位k-bitを有効値とする。

【０１２３】

CFB暗号化モードでは、動作モード信号の演算値(cfb|ofb)=1により、書き込みイネーブル信号reg1_wrとして選択されたIV_WRのアサートに応答して、64bit長のIVデータの初期値がレジスタreg31にセットされる。同様にして、レジスタreg32の上位k-bitには、書き込みイネーブル信号reg2_wrとして選択されたTEXT_WRのアサートに応答して、k-bit長のTEXTデータがセットされ、残りの下位ビットには0値がセットされる。

【０１２４】

そして、IVデータは、経路w7を介して暗号・復号処理ユニット1に入力され、暗号処理され、図3の途中データDiに相当するデータw50が排他的論理和処理ユニット2に入力される。また、経路w8を介してTEXTデータが排他的論理和処理ユニット2に入力され、暗号処理されたIVデータw50と排他的論理和演算される。そして、その結果である暗号化データが経路w60を介して暗号・復号処理ユニット1に送信され、有効値である上位k-bitが暗号化データO_DTとして出力される。

【０１２５】

そして、次のTEXTデータ暗号化のために、レジスタreg31内のIVデータが経路w7、w9、w10を介して、また、前述の暗号化データが経路w60、w11を介して、IV更新ユニット50のCFBフィードバック部CFB_FBに入力され、前述したビット処理され、書き込みイネーブル信号reg1_wrとして選択されたIV_WRのアサートに応答して、経路w75を介してレジスタreg31にセットされる。次に、レジスタreg32の上位k-bitには、書き込みイネーブル信号reg2_wrとして選択されたTEXT_WRのアサートに応答して、経路w2を介して後続するk-bitのTEXTデータがセットされ、残りの下位k-bitには0値がセットされる。そして、以下同様に暗号化が繰り返される。

【０１２６】

図24は第2の実施の形態における暗号化・復号化回路の、CFBモードの復号化時の動作図である。

【０１２７】
CFB復号化モードでは、動作モード信号の演算値(cfb|ofb)=1により、書き込みイネーブル信号reg1_wrとして選択されたIV_WRのアサートに応答して、64bit長のIVデータの初期値がレジスタreg31にセットされる。同様にして、レジスタreg32の上位k-bitには、書き込みイネーブル信号reg2_wrとして選択されたTEXT_WRのアサートに応答して、k-bit長のTEXTデータがセットされ、残りの下位ビットには0値がセットされる。
【０１２８】
そして、IVデータは、経路w7を介して暗号・復号処理ユニット1に入力され、暗号処理され、図3の途中データDiに相当するデータw50が排他的論理和処理ユニット2に入力される。また、経路w8を介してTEXTデータが排他的論理和処理ユニット2に入力され、暗号処理されたIVデータw50と排他的論理和演算される。そして、その結果である復号化データが経路w60を介して暗号・復号処理ユニット1に送信され、有効値である上位k-bitが復号化データO_DTとして出力される。
【０１２９】
そして、次のTEXTデータ復号化のために、レジスタreg31内のIVデータが経路w7、w9、w10を介して、また、レジスタreg32内のTEXTデータが経路w8、w12を介して、IV更新ユニット50のCFBフィードバック部CFB_FBに入力され、前述したビット処理が行われ、書き込みイネーブル信号reg1_wrとして選択されたIV_WRのアサートに応答して、経路w75を介してレジスタreg31にセットされる。次に、レジスタreg32の上位k-bitには、書き込みイネーブル信号reg2_wrとして選択されたTEXT_WRのアサートに応答して、経路w2を介して後続するk-bitのTEXTデータがセットされ、残りの下位k-bitには0値がセットされる。そして、以下同様に復号化が繰り返される。
【０１３０】
以上の動作は、図3で説明したCFBモードの態様と一致している。
【０１３１】
[OFBモード]
図25は第2の実施の形態における暗号化・復号化回路の、OFBモードの暗号化・復号化時の動作図である。
【０１３２】
OFB暗号化モードでは、動作モード信号の演算値(cfb|ofb)=1により、書き込みイネーブル信号reg1_wrとして選択されたIV_WRのアサートに応答して、IVデータの初期値がレジスタreg31にセットされる。同様にして、レジスタreg32には、書き込みイネーブル信号reg2_wrとして選択されたTEXT_WRのアサートに応答して、TEXTデータがセットされる。
【０１３３】
そして、IVデータは、経路w7を介して暗号・復号処理ユニット1に入力され、暗号処理され、図4の途中データDiに相当するデータw50が排他的論理和処理ユニット2に入力される。また、経路w8を介してTEXTデータが排他的論理和処理ユニット2に入力され、暗号処理されたIVデータw50と排他的論理和演算される。そして、その結果である暗号化データが経路w60を介して暗号・復号処理ユニット1に送信され、暗号化データO_DTとして出力される。
【０１３４】
そして、次のTEXTデータ暗号化のために、前述した途中データDiが、経路w50、w13を介してIV更新ユニット50のOFBフィードバック部OFB_FBに入力され、書き込みイネーブル信号reg1_wrとして選択されたIV_WRのアサートに応答して、経路w75を介してレジスタreg31にセットされる。次に、レジスタreg32には、書き込みイネーブル信号reg2_wrとして選択されたTEXT_WRのアサートに応答して、経路w2を介してTEXTデータがセットされる。そして、以下同様に暗号化が繰り返される。
【０１３５】
一方、OFB復号化モードでは、動作モード信号の演算値(cfb|ofb)=1により、書き込みイネーブル信号reg1_wrとして選択されたIV_WRのアサートに応答して、IVデータの初期値が

レジスタreg31にセットされる。同様にして、レジスタreg32には、書き込みイネーブル信号reg2_wrとして選択されたTEXT_WRのアサートに応答して、TEXTデータがセットされる。

【０１３６】

そして、IVデータは、経路w7を介して暗号・復号処理ユニット1に入力され、暗号処理され、図4の途中データDiに相当するデータw50が排他的論理和処理ユニット2に入力される。また、経路w8を介してTEXTデータが排他的論理和処理ユニット2に入力され、暗号処理されたIVデータw50と排他的論理和演算される。そして、その結果である復号化データが経路w60を介して暗号・復号処理ユニット1に送信され、復号化データO_DTとして出力される。

【０１３７】

そして、次のTEXTデータ復号化のために、前述した途中データDiが、経路w50、w13を介してIV更新ユニット50のOFBフィードバック部OFB_FBに入力され、書き込みイネーブル信号reg1_wrとして選択されたIV_WRのアサートに応答して、経路w75を介してレジスタreg31にセットされる。次に、レジスタreg32には、書き込みイネーブル信号reg2_wrとして選択されたTEXT_WRのアサートに応答して、経路w2を介してTEXTデータがセットされる。そして、以下同様に復号化が繰り返される。

【０１３８】

以上の動作は、図4で説明したOFBモードの態様と一致している。

【０１３９】

以上の実施の形態をまとめると，次の付記のとおりである。

【０１４０】

(付記１)

複数動作モードに対応して、暗号化及び復号化を行う暗号化・復号化回路において、

入力端子から入力されるテキストデータとイニシャルベクタデータ(以下イニシャルベクタをIVと称する)とを前記動作モードに応じて第1または第2の出力端子に出力するスワップ回路と、

前記第1の出力端子から前記テキストデータまたはIVデータのいずれか一方を入力し、暗号処理及び復号処理を行う暗号・復号処理ユニットと、

前記第2の出力端子から前記IVデータまたはテキストデータのいずれか他方を入力し、排他的論理和演算を行う排他的論理和処理ユニットとを有し、

前記スワップ回路は、

前記テキストデータを格納する第1のレジスタと、

前記IVデータを格納する第2のレジスタと、

動作モード信号に応答して、前記第1または第2のレジスタの出力のいずれか一方を選択して前記第1の出力端子に出力する第1のセレクタと、

動作モード信号に応答して、前記第1または第2のレジスタの出力のいずれか他方を選択して前記第2の出力端子に出力する第2のセレクタとを有し、

さらに、前記暗号・復号処理ユニットの出力と、前記排他的論理和処理ユニットの出力と、前記第1のレジスタに格納されたテキストデータと、前記第2のレジスタに格納されたIVデータとに応じて、更新されたIVデータを前記第2のレジスタに出力するIV更新ユニットを有することを特徴とする暗号化・復号化回路。

【０１４１】

(付記２)

前記複数の動作モードは、少なくとも、CBCモードと、CFBモードと、OFBモードとを有し、

前記CBCモードのときは、前記第1のセレクタは前記第1のレジスタの出力を選択し、前記第2のセレクタは前記第2のレジスタの出力を選択し、暗号化時に、前記排他的論理和処理ユニットは前記テキストデータとIVデータの排他的論理和演算を行い前記暗号・復号処理ユニットは前記排他的論理和演算されたデータを暗号処理し、前記IV更新ユニットは当該暗号処理されたデータを前記更新されたIVデータとして前記第2のレジスタに出力する

ことを特徴とする付記1に記載の暗号化・復号化回路。

【０１４２】

(付記３)

前記複数の動作モードは、少なくとも、CBCモードと、CFBモードと、OFBモードとを有し、

前記CBCモードのときは、前記第1のセレクタは前記第1のレジスタの出力を選択し、前記第2のセレクタは前記第2のレジスタの出力を選択し、復号化時に、前記暗号・復号処理ユニットは前記テキストデータを復号処理し、前記排他的論理和処理ユニットは当該復号処理されたテキストデータと前記IVデータの排他的論理和演算を行い、前記IV更新ユニットは前記テキストデータを前記更新されたIVデータとして前記第2のレジスタに出力することを特徴とする付記1に記載の暗号化・復号化回路。

【０１４３】

(付記４)

前記複数の動作モードは、少なくとも、CBCモードと、CFBモードと、OFBモードとを有し、

前記CFBモードのときは、前記第1のセレクタは前記第2のレジスタの出力を選択し、前記第2のセレクタは前記第1のレジスタの出力を選択し、暗号化時に、前記暗号・復号処理ユニットは前記IVデータを暗号処理し、前記排他的論理和処理ユニットは当該暗号処理されたIVデータと前記テキストデータの排他的論理和演算を行い、前記IV更新ユニットは当該排他的論理和演算されたデータと前記IVデータをビット演算処理し、当該ビット演算処理されたデータを前記更新されたIVデータとして前記第2のレジスタに出力することを特徴とする付記1に記載の暗号化・復号化回路。

【０１４４】

(付記５)

前記複数の動作モードは、少なくとも、CBCモードと、CFBモードと、OFBモードとを有し、

前記CFBモードのときは、前記第1のセレクタは前記第2のレジスタの出力を選択し、前記第2のセレクタは前記第1のレジスタの出力を選択し、復号化時に、前記暗号・復号処理ユニットは前記IVデータを暗号処理し、前記排他的論理和処理ユニットは当該暗号処理されたIVデータと前記テキストデータの排他的論理和演算を行い、前記IV更新ユニットは前記IVデータと前記テキストデータをビット演算処理し、当該ビット演算処理されたデータを前記更新されたIVデータとして前記第2のレジスタに出力することを特徴とする付記1に記載の暗号化・復号化回路。

【０１４５】

(付記６)

前記複数の動作モードは、少なくとも、CBCモードと、CFBモードと、OFBモードとを有し、

前記OFBモードのときは、前記第1のセレクタは前記第2のレジスタの出力を選択し、前記第2のセレクタは前記第1のレジスタの出力を選択し、暗号化および復号化時に、前記暗号・復号処理ユニットは前記IVデータを暗号処理し、前記排他的論理和処理ユニットは当該暗号処理されたIVデータと前記テキストデータの排他的論理和演算を行い、前記IV更新ユニットは前記暗号処理されたIVデータを前記更新されたIVデータとして前記第2のレジスタに出力することを特徴とする付記1に記載の暗号化・復号化回路。

【０１４６】

(付記７)

複数動作モードに対応して、暗号化及び復号化を行う暗号化・復号化回路において、

入力端子から入力されるテキストデータとイニシャルベクタデータ(以下イニシャルベクタをIVと称する)とを前記動作モードに応じて第1または第2の出力端子に出力するスワップ回路と、

前記第1の出力端子から前記テキストデータまたはIVデータのいずれか一方を入力し、

暗号処理及び復号処理を行う暗号・復号処理ユニットと、
前記第2の出力端子から前記IVデータまたはテキストデータのいずれか他方を入力し、排他的論理和演算を行う排他的論理和処理ユニットとを有し、
前記スワップ回路は、
テキストデータ書き込みイネーブル信号またはIVデータ書き込みイネーブル信号に応答して、前記テキストデータまたはIVデータをそれぞれ格納し、前記第1、第2の出力端子にそれぞれ出力する第1、第2のレジスタと、
動作モード信号に応答して、前記テキストデータ書き込みイネーブル信号またはIVデータ書き込みイネーブル信号のいずれか一方を選択して前記第1のレジスタに供給する第1のセレクタと、いずれか他方を選択して前記第2のレジスタに供給する第2のセレクタとを有し、
さらに、前記暗号・復号処理ユニットの出力と、前記排他的論理和処理ユニットの出力と、前記第1または第2のレジスタに格納されたテキストデータと、前記第1または第2のレジスタに格納されたIVデータとに応じて、更新されたIVデータを前記第1または第2のレジスタに出力するIV更新ユニットを有することを特徴とする暗号化・復号化回路。

【０１４７】

(付記８)
前記複数の動作モードは、少なくとも、CBCモードと、CFBモードと、OFBモードとを有し、
前記CBCモードのときは、前記第1のセレクタは前記テキストデータ書き込みイネーブル信号を選択し、前記第2のセレクタは前記IVデータ書き込みイネーブル信号を選択し、暗号化時に、前記排他的論理和処理ユニットは前記テキストデータとIVデータの排他的論理和演算を行い前記暗号・復号処理ユニットは前記排他的論理和演算されたデータを暗号処理し、前記IV更新ユニットは当該暗号処理されたデータを前記更新されたIVデータとして前記第2のレジスタに出力することを特徴とする付記7に記載の暗号化・復号化回路。

【０１４８】

(付記９)
前記複数の動作モードは、少なくとも、CBCモードと、CFBモードと、OFBモードとを有し、
前記CBCモードのときは、前記第1のセレクタは前記テキストデータ書き込みイネーブル信号を選択し、前記第2のセレクタは前記IVデータ書き込みイネーブル信号を選択し、復号化時に、前記暗号・復号処理ユニットは前記テキストデータを復号処理し、前記排他的論理和処理ユニットは当該復号処理されたテキストデータと前記IVデータの排他的論理和演算を行い、前記IV更新ユニットは前記テキストデータを前記更新されたIVデータとして前記第2のレジスタに出力することを特徴とする付記7に記載の暗号化・復号化回路。

【０１４９】

(付記１０)
前記複数の動作モードは、少なくとも、CBCモードと、CFBモードと、OFBモードとを有し、
前記CFBモードのときは、前記第1のセレクタは前記IVデータ書き込みイネーブル信号を選択し、前記第2のセレクタは前記テキストデータ書き込みイネーブル信号を選択し、暗号化時に、前記暗号・復号処理ユニットは前記IVデータを暗号処理し、前記排他的論理和処理ユニットは当該暗号処理されたIVデータと前記テキストデータの排他的論理和演算を行い、前記IV更新ユニットは当該排他的論理和演算されたデータと前記IVデータをビット演算処理し、当該ビット演算処理されたデータを前記更新されたIVデータとして前記第1のレジスタに出力することを特徴とする付記7に記載の暗号化・復号化回路。

【０１５０】

(付記１１)
前記複数の動作モードは、少なくとも、CBCモードと、CFBモードと、OFBモードとを有し、

前記CFBモードのときは、前記第1のセレクタは前記IVデータ書き込みイネーブル信号を選択し、前記第2のセレクタは前記テキストデータ書き込みイネーブル信号を選択し、復号化時に、前記暗号・復号処理ユニットは前記IVデータを暗号処理し、前記排他的論理和処理ユニットは当該暗号処理されたIVデータと前記テキストデータの排他的論理和演算を行い、前記IV更新ユニットは前記テキストデータと前記IVデータをビット演算処理し、当該ビット演算処理されたデータを前記更新されたIVデータとして前記第1のレジスタに出力することを特徴とする付記7に記載の暗号化・復号化回路。

【０１５１】

(付記１２)

前記複数の動作モードは、少なくとも、CBCモードと、CFBモードと、OFBモードとを有し、

前記OFBモードのときは、前記第1のセレクタは前記IVデータ書き込みイネーブル信号を選択し、前記第2のセレクタは前記テキストデータ書き込みイネーブル信号を選択し、暗号化および復号化時に、前記暗号・復号処理ユニットは前記IVデータを暗号処理し、前記排他的論理和処理ユニットは当該暗号処理されたIVデータと前記テキストデータの排他的論理和演算を行い、前記IV更新ユニットは前記暗号処理されたIVデータを前記更新されたIVデータとして前記第1のレジスタに出力することを特徴とする付記7に記載の暗号化・復号化回路。

【０１５２】

(付記１３)

前記排他的論理和処理ユニットが前記第1と第2の両方の出力端子から前記テキストデータとIVデータの両方を入力する付記1および7に記載の暗号化・復号化回路。

【０１５３】

(付記１４)

さらに、前記第1と第2のセレクタの両方が前記IVデータ書き込みイネーブル信号を選択し、前記第1と第2のレジスタに供給した後、動作モード信号に応答して、前記第1と第2のセレクタのいずれか一方が前記テキストデータ書き込みイネーブル信号を選択する付記7に記載の暗号化・復号化回路。

【０１５４】

(付記１５)

前記入力端子から入力される前記テキストデータと前記IVデータの複数回の分割入力に伴い、前記第1、第2のレジスタは複数に分割され、当該分割された第1、第2のレジスタ毎に前記第1、第2のセレクタを有する付記7に記載の暗号化・復号化回路。

【図面の簡単な説明】

【０１５５】

【図１】図1は、ECBモードの概念図である。

【図２】図2は、CBCモードの概念図である。

【図３】図3は、CFBモードの概念図である。

【図４】図4は、OFBモードの概念図である。

【図５】図5は、暗号化・復号化を行うシステムの構成図の一例である。

【図６】図6は、CBCモード、CFBモード、OFBモードの暗号化処理の流れを示すフローチャートである。

【図７】図7は、第1の実施の形態における、暗号化回路で使用されるスワップ回路の構成図である。

【図８】図8は、スワップ回路90を用いて構成した暗号化・復号化回路の模式図である。

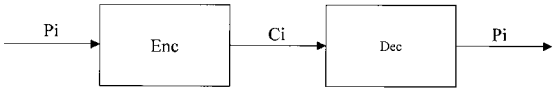
【図９】図9は、図8に示される模式図の具体的な回路構成例である。

【図１０】図10は、第1の実施の形態における暗号化・復号化回路の、ECBモードの暗号化・復号化時の動作図である。

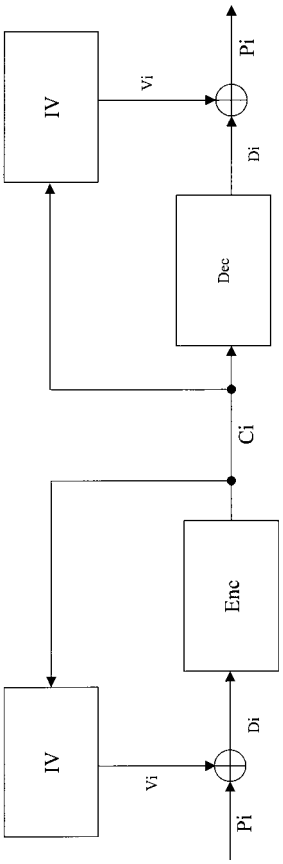
【図１１】図11は、第1の実施の形態における暗号化・復号化回路の、CBCモードの暗号化時の動作図である。

【図１２】図12は、第1の実施の形態における暗号化・復号化回路の、CBCモードの復号化時の動作図である。
【図１３】図13は、第1の実施の形態における暗号化・復号化回路の、CFBモードの暗号化時の動作図である。
【図１４】図14は、第1の実施の形態における暗号化・復号化回路の、CFBモードの復号化時の動作図である。
【図１５】図15は、第1の実施の形態における暗号化・復号化回路の、OFBモードの暗号化・復号化時の動作図である。
【図１６】図16は、第2の実施の形態における、暗号化回路で使用されるスワップ回路の構成図である。
【図１７】図17は、本第2の実施の形態におけるスワップ回路を構成するセレクタ回路の一例である。
【図１８】図18は、スワップ回路95を用いて構成した暗号化・復号化回路の模式図である。
【図１９】図19は、図18に示される模式図の具体的な回路構成例である。
【図２０】図20は、第2の実施の形態における暗号化・復号化回路の、ECBモードの暗号化・復号化時の動作図である。
【図２１】図21は、第2の実施の形態における暗号化・復号化回路の、CBCモードの暗号化時の動作図である。
【図２２】図22は、第2の実施の形態における暗号化・復号化回路の、CBCモードの復号化時の動作図である。
【図２３】図23は、第2の実施の形態における暗号化・復号化回路の、CFBモードの暗号化時の動作図である。
【図２４】図24は、第2の実施の形態における暗号化・復号化回路の、CFBモードの復号化時の動作図である。
【図２５】図25は、第2の実施の形態における暗号化・復号化回路の、OFBモードの暗号化・復号化時の動作図である。
【符号の説明】
【０１５６】
1 暗号・復号処理ユニット
2 排他的論理和処理ユニット
3 TEXTレジスタ
4 IVレジスタ
50 IV更新ユニット
90a、90、95 スワップ回路

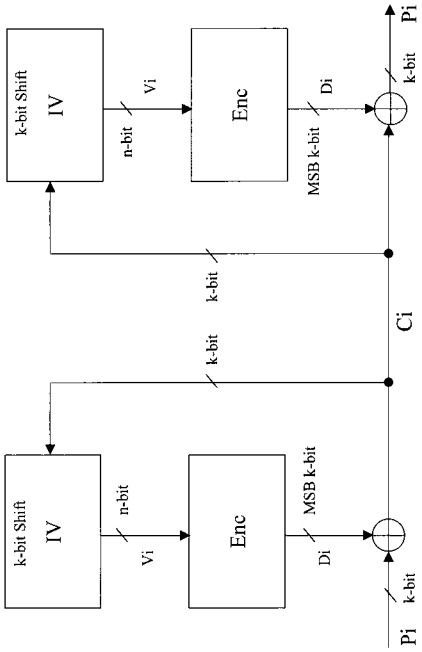
【図１】


Pi
Enc
Ci
Dec
Pi

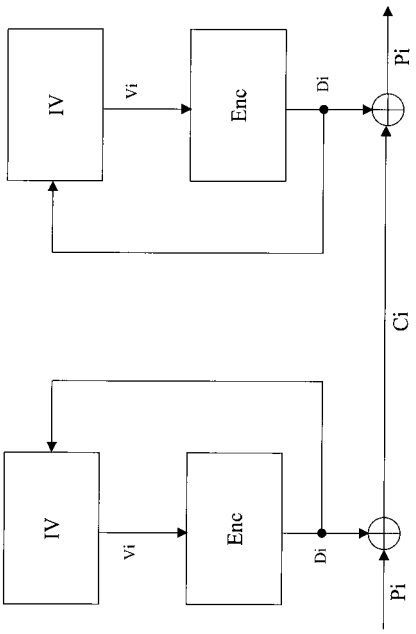
【図２】


IV
Vi
Pi
Di
Dec
Ci
Enc
IV
Vi
Di
Pi

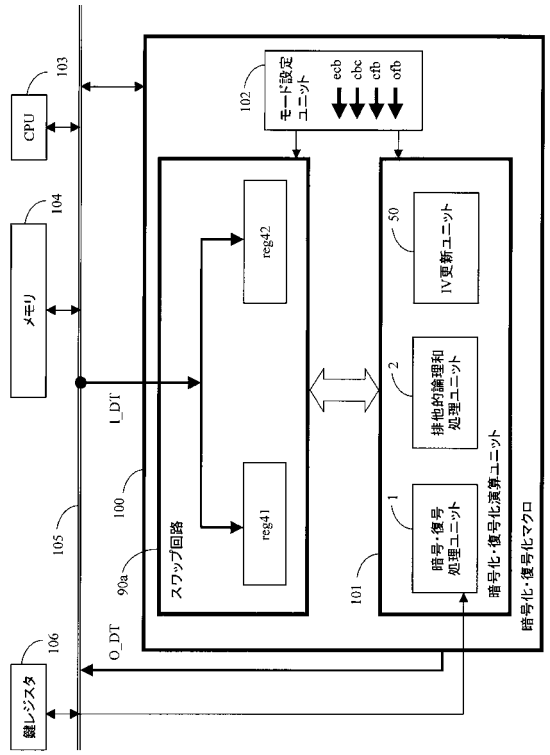
【図３】


k-bit Shift
IV
n-bit
Vi
Enc
Di
MSB k-bit
k-bit
Pi
k-bit
Ci
k-bit
k-bit Shift
IV
n-bit
Vi
Enc
MSB k-bit
Di
k-bit
Pi

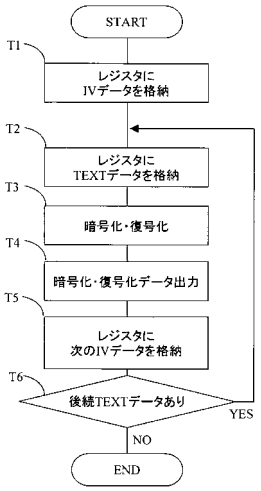
【図４】


IV
Vi
Enc
Di
Pi
Ci
IV
Vi
Enc
Di
Pi

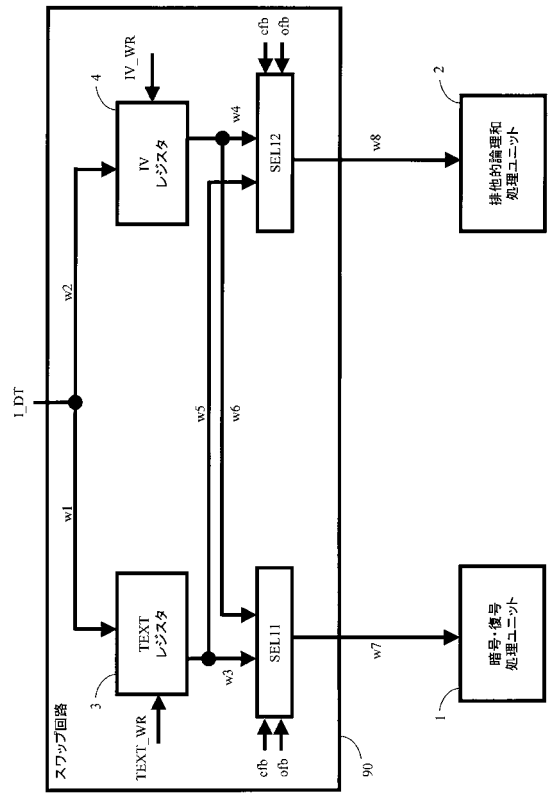
【図５】


CPU
103
メモリ
104
鍵レジスタ
106
I_DT
O_DT
100
105
90a
101
102
モード設定ユニット
ecb
cbc
cfb
ofb
スワップ回路
reg42
reg41
50
IV更新ユニット
2
排他的論理和処理ユニット
1
暗号・復号処理ユニット
暗号化・復号化演算ユニット
暗号化・復号化マクロ

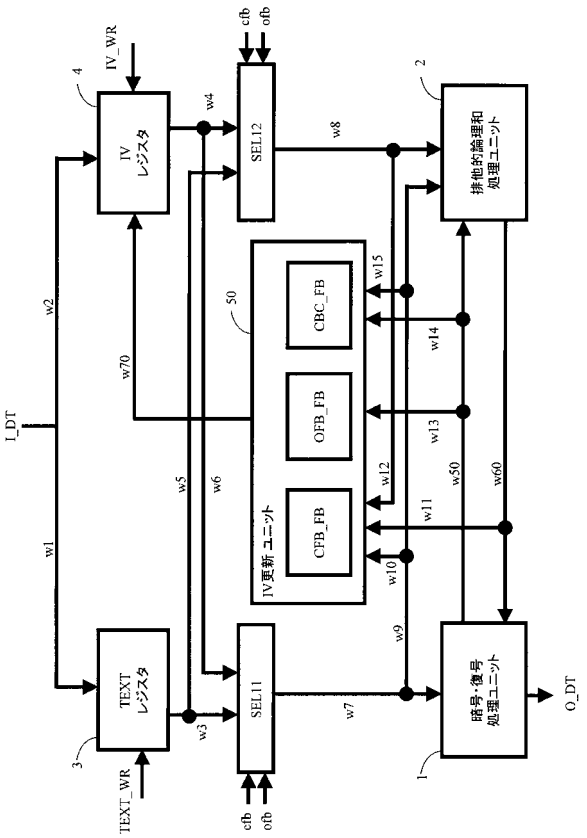
【図６】


START
T1
レジスタに
IVデータを格納
T2
レジスタに
TEXTデータを格納
T3
暗号化・復号化
T4
暗号化・復号化データ出力
T5
レジスタに
次のIVデータを格納
T6
後続TEXTデータあり
YES
NO
END

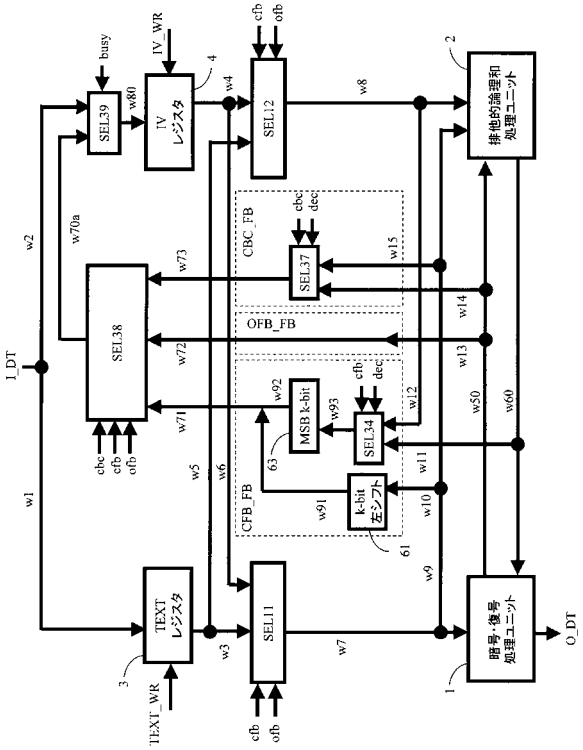
【図７】


I_DT
IV_WR
4
IV
レジスタ
TEXT
レジスタ
3
TEXT_WR
cfb
ofb
SEL12
SEL11
w1
w2
w3
w4
w5
w6
w7
w8
2
排他的論理和
処理ユニット
1
暗号・復号
処理ユニット
スワップ回路
90

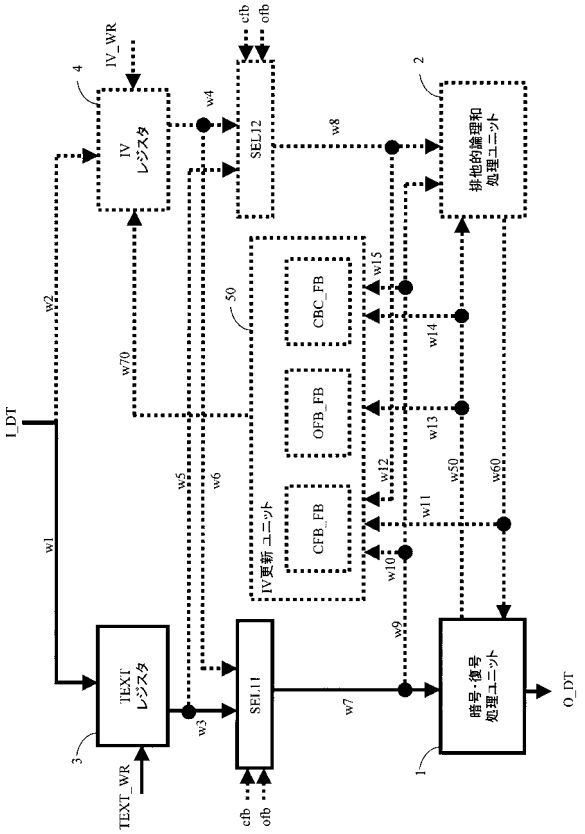
【図８】


I_DT
IV_WR
4
IV
レジスタ
TEXT
レジスタ
3
TEXT_WR
cfb
ofb
SEL12
SEL11
w1
w2
w3
w4
w5
w6
w7
w8
w9
w10
w11
w12
w13
w14
w15
w50
w60
w70
50
IV更新ユニット
CBC_FB
OFB_FB
CFB_FB
2
排他的論理和
処理ユニット
1
暗号・復号
処理ユニット
O_DT

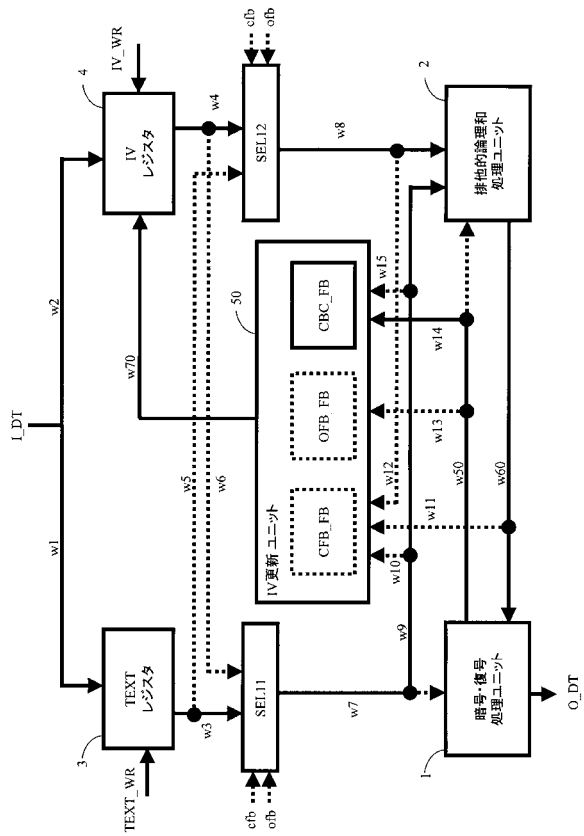
【図９】



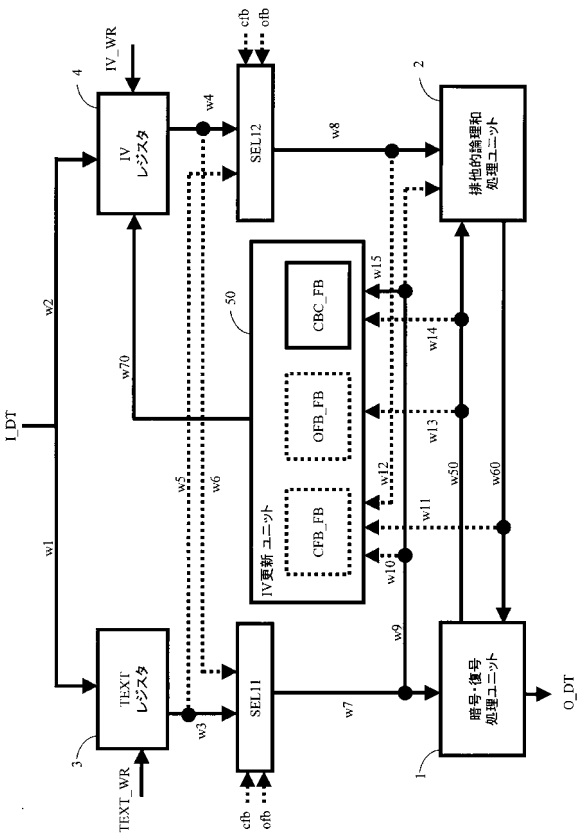
【図１０】



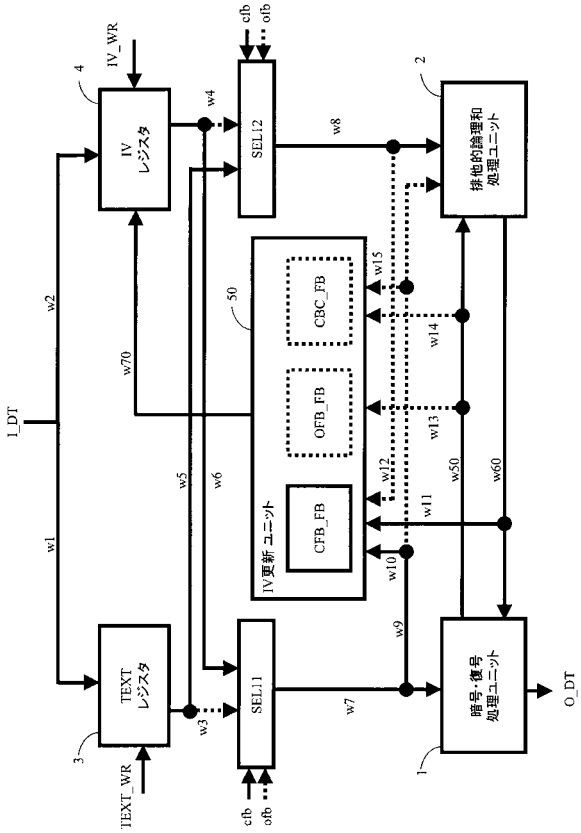
【図１１】



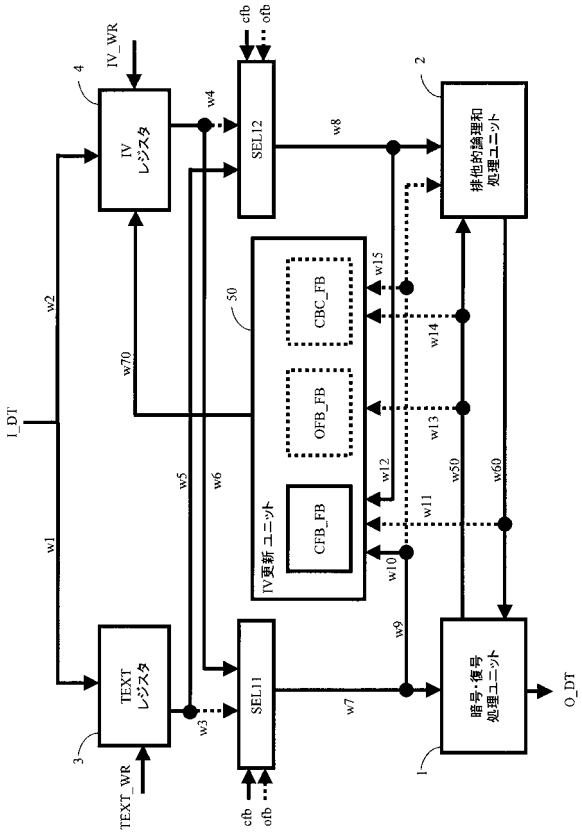
【図１２】



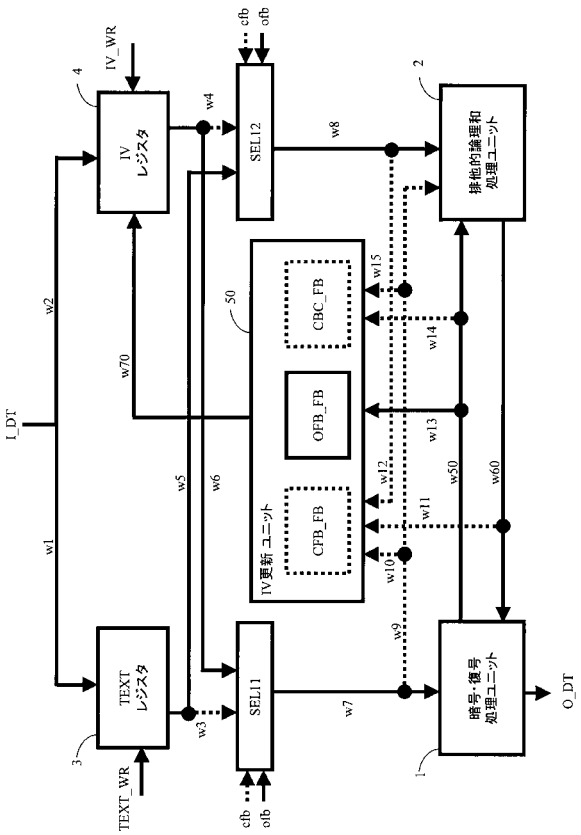
【図１３】



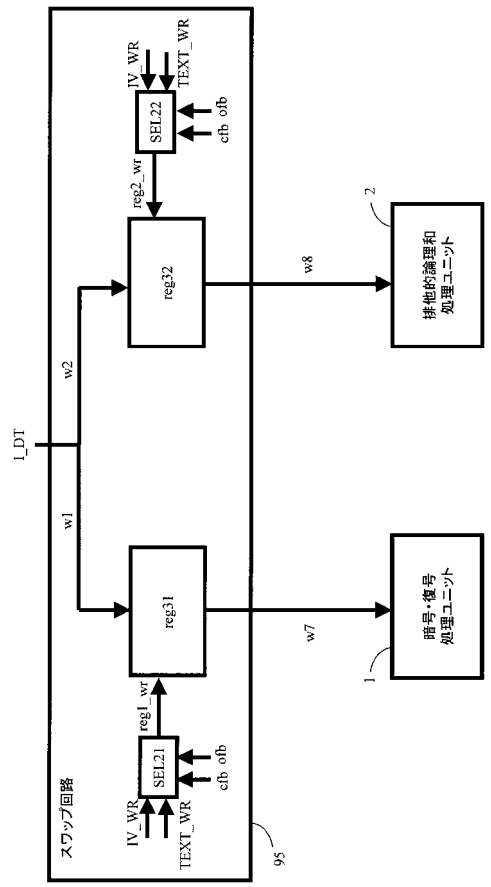
【図１４】



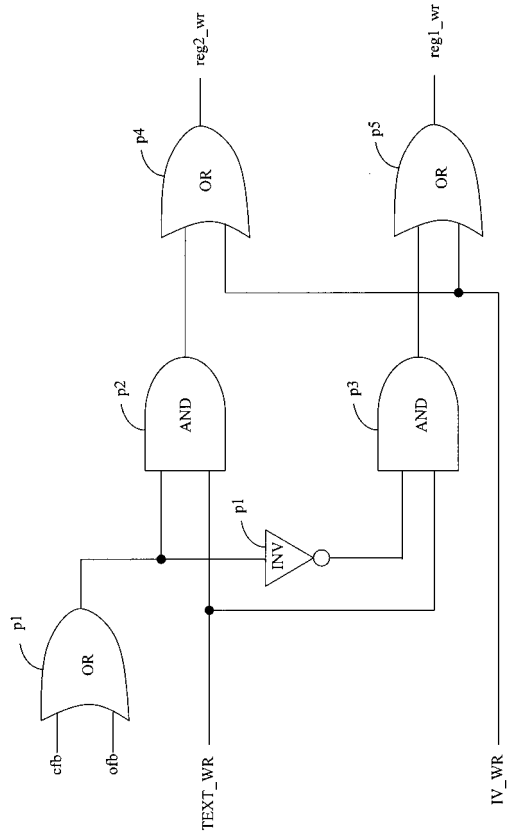
【図１５】



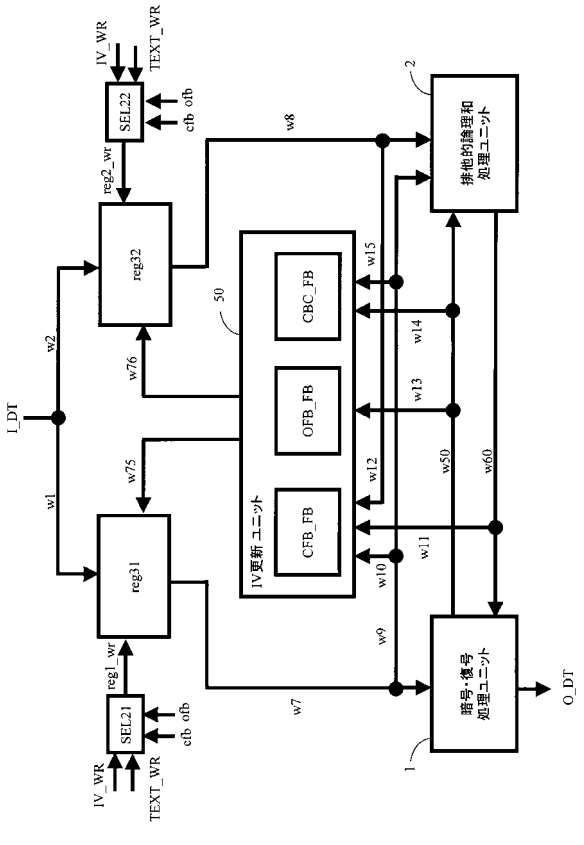
【図１６】



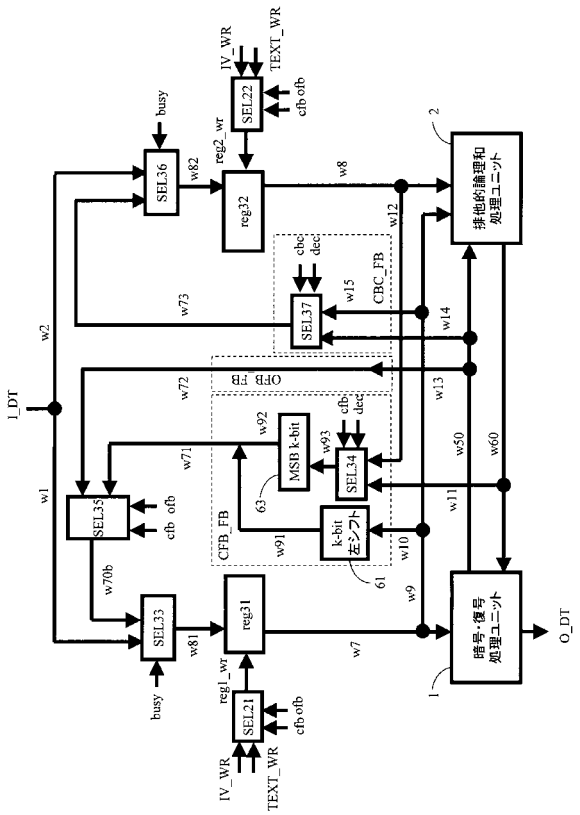
【図１７】



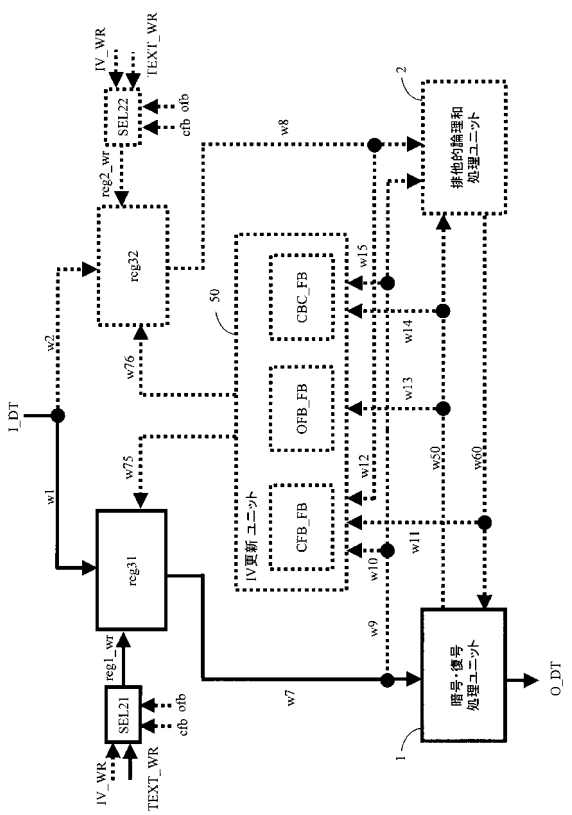
【図１８】



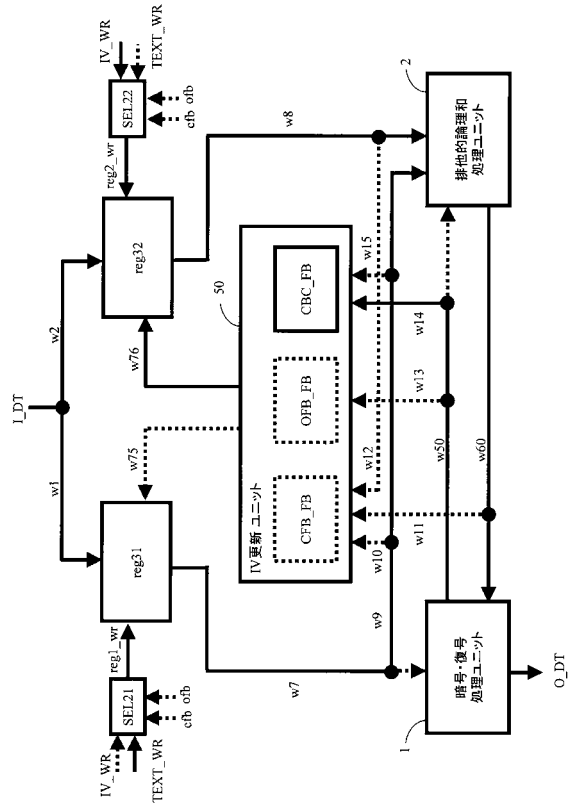
【図１９】



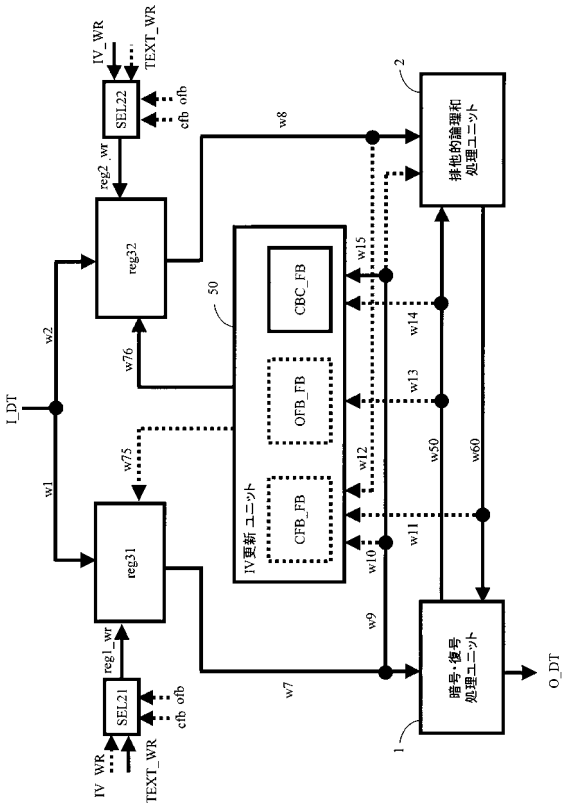
【図２０】



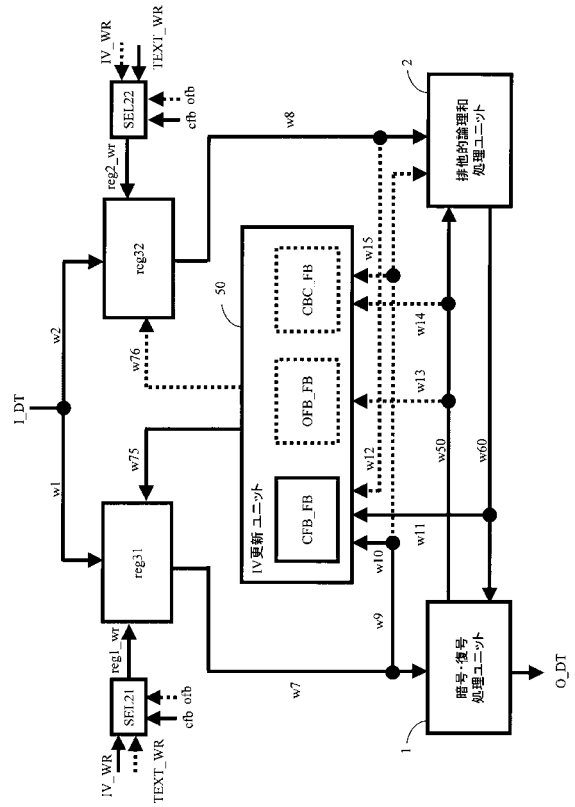
【図２１】



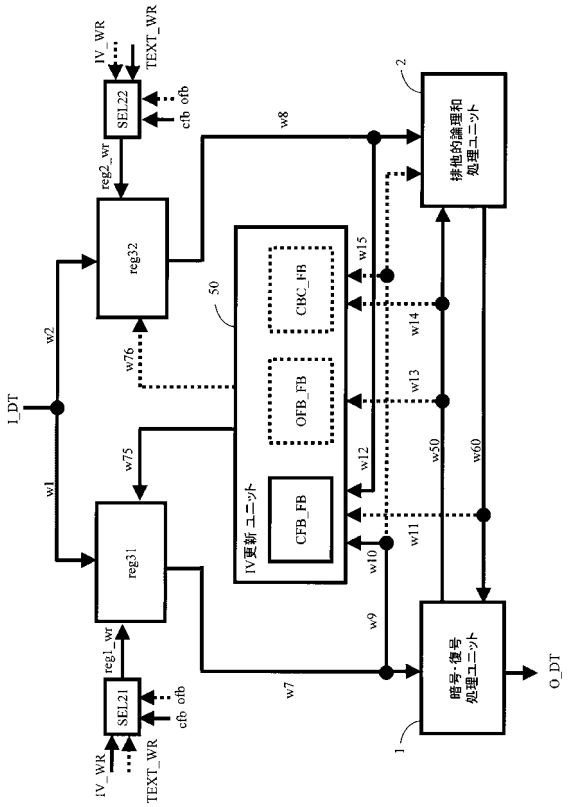
【図２２】



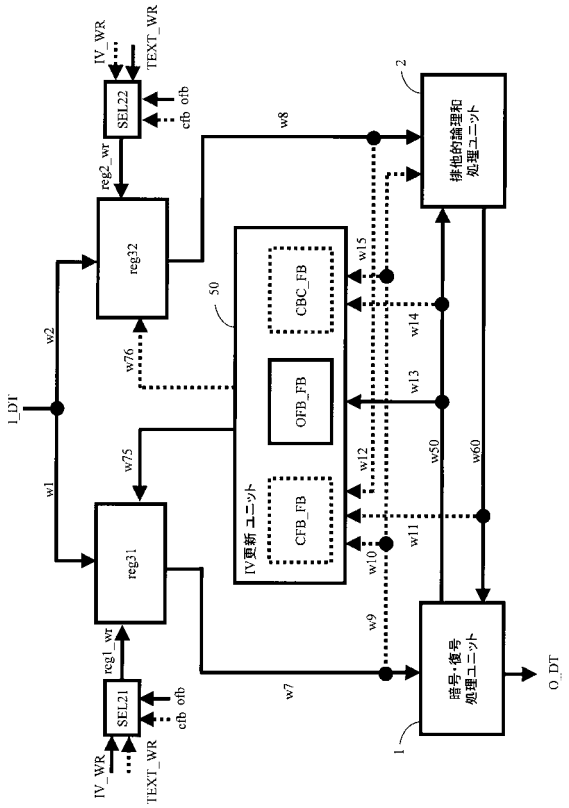
【図２３】



【図２４】



【図２５】


IV_WR
TEXT_WR
SEL22
cfb ofb
reg2_wr
reg32
w8
2
排他的論理和
処理ユニット
w15
w14
w13
w12
w11
w10
w9
w7
w76
w75
w2
w1
I_DT
50
CBC_FB
OFB_FB
CFB_FB
IV更新ユニット
reg31
reg1_wr
SEL21
暗号/復号
処理ユニット
w50
w60
O_DT
1

フロントページの続き

審査官　石田　信行

(56)参考文献　特開平７－２６１６６２（ＪＰ，Ａ）
特開２０００－７５７８５（ＪＰ，Ａ）
特開２００２－２９７０３０（ＪＰ，Ａ）
特開２００４－２２６９６６（ＪＰ，Ａ）
米国特許第０５６３１９６０（ＵＳ，Ａ）
国際公開第２００４／０１５９１６（WO，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０９Ｃ　　１／００
Ｈ０４Ｌ　　９／１０