(19)日本国特許庁(JP)

再公表特許(A1)

(11)国際公開番号
WO2011/036745

発行日　平成25年2月14日(2013.2.14)

(43)国際公開日　平成23年3月31日(2011.3.31)

(51)Int.Cl.			F I			テーマコード（参考）
H04L	9/10	(2006.01)	H04L	9/00	621A	5J104
H04L	9/08	(2006.01)	H04L	9/00	601E	
G09C	1/00	(2006.01)	G09C	1/00	610A	

審査請求 有　予備審査請求 未請求　（全 28 頁）

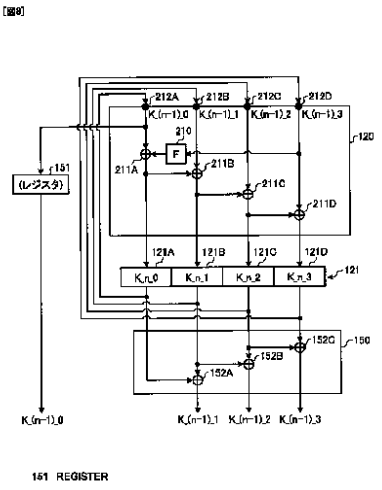
出願番号　特願2011-532824 (P2011-532824)
(21)国際出願番号　PCT/JP2009/066536
(22)国際出願日　平成21年9月24日(2009.9.24)
(81)指定国　AP(BW,GH,GM,KE,LS,MW,MZ,NA,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,MK,MT,NL,NO,PL,PT,RO,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,CZ,DE,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IS,JP,KE,KG,KM,KN,KP,KR,KZ,LA,LC,LK,LR,LS,LT,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PE,PG,PH,PL,PT,RO,RS,RU,SC,SD,SE,SG,SK,SL,SM,ST,SV,SY,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,ZA,ZM,ZW

(71)出願人　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　100089118
弁理士　酒井　宏明
(74)代理人　100112656
弁理士　宮田　英毅
(72)発明者　川端　健
東京都港区芝浦一丁目１番１号　株式会社東芝内
(72)発明者　藤崎　浩一
東京都港区芝浦一丁目１番１号　株式会社東芝内

最終頁に続く

(54)【発明の名称】鍵スケジュール装置および方法

(57)【要約】
検算を行う鍵を格納するレジスタの規模を小さくする。拡大鍵が分割されて拡大鍵生成回路に入力される。拡大鍵が分割された１の部分鍵に対して非線形変換が行われると共に、部分鍵のそれぞれに対して非線形変換の出力を用いて線形変換が行われ、変換された部分鍵が拡大鍵レジスタに格納される。拡大鍵レジスタに格納された部分鍵のうち、非線形変換の出力を直接的に用いて線形変換が行われる部分鍵が検算用拡大鍵レジスタに格納される。それ以外の部分鍵は、拡大鍵レジスタに接続される線形変換回路で、拡大鍵生成回路における線形変換とは逆の線形変換を施される。検算用拡大鍵レジスタに格納される部分鍵と、線形変換回路で拡大鍵生成回路における線形変換とは逆の線形変換を施された各部分鍵とを結合して、検算用拡大鍵が生成される。検算用拡大鍵レジスタは、１の部分鍵が格納可能な容量があればよい。



【特許請求の範囲】
【請求項１】
入力データに対して実行される演算に用いる第１の鍵を出力する鍵スケジュール装置であって、
拡大鍵を分割した各部分鍵のうち少なくとも１の部分鍵に対して非線形変換を施す非線形変換部と、
複数の線形変換回路を含み、該複数の線形変換回路の一部が前記非線形変換部の変換結果を直接用いて前記部分鍵の線形変換を行う第１の線形変換部と、
前記第１の線形変換部で前記線形変換を行われた前記部分鍵をそれぞれ格納する第１の格納部と、
前記第１の格納部に格納された前記部分鍵のうち前記非線形変換部の変換結果を直接用いて前記線形変換回路で線形変換が行われた部分鍵以外の部分鍵のそれぞれに対して、前記第１の線形変換部による変換に対して逆の線形変換を行う第２の線形変換部と、
前記複数の線形変換回路のうち前記非線形変換部の変換結果に対して直接的に前記線形変換を行う線形変換回路に対する入力のうち１を格納する第２の格納部と、
前記第２の線形変換部で前記逆の線形変換を施された部分鍵のそれぞれと、前記第２の格納部に格納された前記入力とを結合して、前記演算に対する検算を行う際に用いる第２の鍵として出力する出力部と
を備える
ことを特徴とする鍵スケジュール装置。
【請求項２】
前記第１の線形変換部および前記第２の線形変換部は、排他的論理和回路、ビットシフト回路、加算回路および減算回路のうち少なくとも１を用いて構成される
ことを特徴とする請求項１に記載の鍵スケジュール装置。
【請求項３】
前記第２の格納部は、前記入力部から前記非線形変換部の変換結果に対して直接的に線形変換を行う線形変換回路に入力される前記部分鍵を格納する
ことを特徴とする請求項２に記載の鍵スケジュール装置。
【請求項４】
前記第２の格納部は、前記非線形変換部の前記変換結果を格納し、
前記第２の線形変換部は、さらに、前記第２の格納部に格納される前記変換結果に対して逆の線形変換を行う
ことを特徴とする請求項２に記載の鍵スケジュール装置。
【請求項５】
入力データに対して実行される演算に用いる第１の鍵を出力する鍵スケジュール方法であって、
拡大鍵を分割した各部分鍵のうち少なくとも１の部分鍵に対して非線形変換を施す非線形変換ステップと、
複数の線形変換回路の一部が前記非線形変換ステップの変換結果を直接用いて前記部分鍵の線形変換を行う第１の線形変換ステップと、
前記第１の線形変換ステップで前記線形変換を行われた前記部分鍵をそれぞれ第１の格納部に格納する第１の格納ステップと、
前記第１の格納ステップに格納された前記部分鍵のうち前記非線形変換ステップの変換結果を直接用いて前記線形変換回路で線形変換が行われた部分鍵以外の部分鍵のそれぞれに対して、前記第１の線形変換ステップによる変換に対して逆の線形変換を行う第２の線形変換ステップと、
前記複数の線形変換回路のうち前記非線形変換ステップの変換結果に対して直接的に前記線形変換を行う線形変換回路に対する入力のうち１を第２の格納部に格納する第２の格納ステップと、
前記第２の線形変換ステップで前記逆の線形変換を施された部分鍵のそれぞれと、前記

第２の格納部に格納された前記入力とを結合して、前記演算に対する検算を行う際に用いる第２の鍵として出力する出力ステップと
を備える
ことを特徴とする鍵スケジュール方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、暗号化処理または復号処理の検算に用いる鍵の生成に関する。
【背景技術】
【０００２】
近年で一般的に用いられる暗号化方式の一つとして、ＡＥＳ(Advanced Encryption Standard)などのブロック暗号を用いたものがある。ブロック暗号は、鍵を入力として複数個の拡大鍵を出力する鍵スケジューラと、入力データの撹拌を行うスクランブラとで構成され、さらに、スクランブラが複数のラウンドぞれぞれで拡大鍵を用いて入力データの置換や転置などの演算処理を行う構成になっているものが多い。
【０００３】
このような複数のラウンド毎に演算処理を行う場合、ラウンド毎に検算を行うことでエラーを検出する方法が適用できる。ラウンド毎に検算を行う場合、検算用の回路を備えれば演算処理と検算処理とを並列化することが可能であり、１ラウンド分のオーバヘッドで演算結果が確定し、検算を含めた暗号化や復号処理を高速に行うことが可能である。非特許文献１には、ブロック暗号に適用するための様々なエラー検出方法が報告されている。
【先行技術文献】
【非特許文献】
【０００４】
【非特許文献１】“Concurrent Error Detection Schemes for Fault-based Side-Channel Cryptanalysis of Symmetric Block Cipher", IEEE Transactions on Computer-Added Design of Integrated circuit and Systems. VO.21 No.12, December 2002
【発明の概要】
【発明が解決しようとする課題】
【０００５】
暗号化装置や復号装置は、処理速度が高速であると共に、回路規模が小さいことが望ましい。暗号化や復号の演算中のエラーに対する対策である検算を行うには、検算結果に対する比較対象となる演算結果を保持または生成するためのレジスタが必要である。それと共に、検算に用いる拡大鍵を格納するため、拡大鍵格納用レジスタと同じ大きさのレジスタが必要となり、回路の小規模化を妨げていた。
【０００６】
本発明は、上記に鑑みてなされたものであって、検算を行う鍵を格納するレジスタの規模が小さい鍵スケジュール装置および方法を提供することを目的とする。
【課題を解決するための手段】
【０００７】
上述した課題を解決し、目的を達成するために、本発明は、入力データに対して実行される演算に用いる第１の鍵を出力する鍵スケジュール装置であって、拡大鍵を分割した各部分鍵のうち少なくとも１の部分鍵に対して非線形変換を施す非線形変換部と、複数の線形変換回路を含み、複数の線形変換回路の一部が非線形変換部の変換結果を直接用いて部分鍵の線形変換を行う第１の線形変換部と、第１の線形変換部で線形変換を行われた部分鍵をそれぞれ格納する第１の格納部と、第１の格納部に格納された部分鍵のうち非線形変換部の変換結果を直接用いて線形変換回路で線形変換が行われた部分鍵以外の部分鍵のそれぞれに対して、第１の線形変換部による変換に対して逆の線形変換を行う第２の線形変換部と、複数の線形変換回路のうち非線形変換部の変換結果に対して直接的に線形変換を

行う線形変換回路に対する入力のうち１を格納する第２の格納部と、第２の線形変換部で逆の線形変換を施された部分鍵のそれぞれと、第２の格納部に格納された入力とを結合して、演算に対する検算を行う際に用いる第２の鍵として出力する出力部とを備えることを特徴とする。

【発明の効果】

【０００８】

本発明によれば、検算を行う鍵を格納するレジスタの規模を小さくできるという効果を奏する。

【図面の簡単な説明】

【０００９】

【図１】検算を異種処理で行う場合の演算装置の基本的な構成の例を示す図。

【図２】拡大鍵生成回路を概略的に示す図。

【図３】拡大鍵生成回路の構成を示す図。

【図４】検算を異種処理で行う場合の処理を示すフローチャート。

【図５】検算を同種処理で行う場合の演算装置の基本的な構成を示す図。

【図６】検算を同種処理で行う場合の処理を示すフローチャート。

【図７】演算処理と検算処理との関係について説明するための図。

【図８】実施の形態による鍵スケジュール部の構成を示す図。

【図９】実施の形態による鍵スケジュール部を演算装置に適用させた例を示す図。

【図１０】実施の形態の第１の変形例による鍵スケジュール部の構成を示す図。

【図１１】実施の形態の第２の変形例による鍵スケジュール部の構成を示す図。

【発明を実施するための形態】

【００１０】

以下に添付図面を参照して、本発明に係る演算装置、方法およびプログラムの実施の形態を詳細に説明する。なお、本実施の形態では、暗号化および復号を、ＡＥＳ(Advanced Encryption Standard)に代表される、ブロック暗号を用いた暗号化方式で行う。また、本実施の形態に適用されるブロック暗号化方式では、暗号化装置および復号装置は、鍵を入力として複数個の拡大鍵を出力する鍵スケジューラ部と、入力データの撹拌を行うデータ撹拌部とで構成される。そして、データ撹拌部が複数のラウンドぞれぞれで拡大鍵を用いて入力データの置換や転置などの演算処理を行う。

【００１１】

＜暗号化および復号処理に対する検算の概略＞

先ず、本実施の形態に適用可能な、暗号化処理および復号処理で演算された演算データに対するエラー検出について、概略的に説明する。

【００１２】

暗号化装置および復号装置における演算データのエラーを検出する方法として、演算中のデータにパリティを付加してエラー検出を行う方法や、検算を行う方法がある。これらのうち、パリティを付加する方法は、入力ビット長が長くなるため、既存システムに対してパリティ付加によるエラー検出を行う暗号化装置や復号装置を適用する場合には、既存システムの変更が必要になる。

【００１３】

一方、検算によりエラー検出を行う方法は、入力ビット長の変更が無く、検算機能を付加した暗号化装置や復号装置を既存のシステムに適用することが比較的容易である。本実施の形態では、暗号化処理や復号処理で演算された演算データのエラー検出に、この検算方式を採用する。

【００１４】

検算方式では、さらに、暗号装置または復号装置において全体の演算処理が終わってから検算を行う方法と、ラウンド毎に検算を行う方法が考えられる。これらのうち、全体の演算処理が終わってから検算する方法は、１ブロックの入力に対して演算処理と検算処理とを行うため、演算結果が確定するまでの時間が検算を行わない場合に比べて２倍必要と

なる。そのため、高速な処理が要求されるシステムには適していない。

【００１５】

一方、ラウンド毎に検算処理を行う方法は、暗号化処理や復号処理を行う演算回路とは別個に検算用の回路を備えれば、データ演算処理と検算処理とを並列的に行うことができる。この場合、１ラウンド分のオーバヘッドで演算結果が確定し、検算を含めた暗号化処理または復号処理の高速化が可能である。

【００１６】

ところで、一般に、暗号化処理または復号処理の演算に対する検算は、演算と異なる処理により行う異種処理と、演算と同種の処理により行う同種処理とがある。

【００１７】

異種処理では、暗号化処理の演算に対する検算は、暗号化処理に対応する復号処理の演算により行う。同様に、復号処理の演算に対する検算は、暗号化処理の演算により行う。検算を異種処理により行う場合には、暗号化装置または復号装置は、暗号処理回路および復号処理回路の２種類の回路を備える。したがって、検算を異種処理により行う場合、１の装置で暗号化処理および復号処理の両方を実行可能に構成することができる。

【００１８】

これに対して、同種処理では、暗号化処理の演算に対する検算は、同じ暗号化処理の演算により行う。同様に、復号処理の演算に対する検算は、同じ復号処理の演算により行う。検算を同種処理により行う場合には、暗号化装置または復号装置は、暗号化処理回路または復号処理回路のうち装置の目的に即した１種類の回路を複数、備える。したがって、検算を同種処理により行う場合、検算を利用しない状態においてスループットを向上させるように構成できる。

【００１９】

先ず、検算を異種処理により行う場合について説明する。図１は、検算を異種処理により行う場合の、検算機能付き暗号化装置または復号装置の基本的な構成の例を示す。なお、暗号化装置と復号装置は、同一の構成で実現可能であるので、以下では、特に記載のない限り、暗号化装置および復号装置を纏めて演算装置と呼ぶ。

【００２０】

図１に例示される演算装置１００は、同じ演算処理を複数回繰り返し実行して、平文データの暗号化または暗号データの復号を行う。演算装置１００は、暗号化装置として機能する場合には、所定長の平文データと所定長の暗号鍵とが入力され、入力された平文データを暗号鍵を用いて暗号化して所定長の暗号文データを出力する。復号装置として機能する場合には、所定長の暗号文データと所定長の復号鍵とが入力され、入力された暗号文データを復号して所定長の平文データを出力する。また、演算装置１００は、暗号化または復号に対する検算機能を有する。

【００２１】

なお、演算装置１００に対して入力される平文または暗号データ、暗号鍵または復号鍵、ならびに、演算処理の繰り返し回数は、演算装置１００に適用される暗号化または復号方式によって定まるものとする。また、演算装置１００は、演算装置１００の各部に作用して全体の動作を制御するための制御部を備える（図示しない）。

【００２２】

演算装置１００は、鍵スケジュール部１０１とデータ撹拌部１０２とを有する。鍵スケジュール部１０１は、外部から入力された暗号鍵または復号鍵（以下では、特に記載のない限り、これらを纏めて「鍵」と呼ぶ）に基づき拡大鍵を生成する。また、鍵スケジュール部１０１は、自ら生成した拡大鍵に基づき、新たな拡大鍵を生成する。

【００２３】

データ撹拌部１０２は、外部から入力データとして入力された平文または暗号化データに対して、鍵スケジュール部１０１で生成された拡大鍵を用いて演算を行い、当該入力データを撹拌する（演算装置１００が暗号化装置の場合）。演算装置１００が復号装置の場合には、データ撹拌部１０２は、拡大鍵を用いて暗号化の際と逆の演算を行うことで、撹

拌されたデータを元に戻すことになる。また、データ撹拌部１０２は、拡大鍵を用いた演算を検算する機能を有する。

【００２４】

以降、特に記載のない限り、この暗号化の際のデータ撹拌と、復号の際の撹拌されたデータを元に戻す処理を、纏めてデータ撹拌と呼ぶ。

【００２５】

鍵スケジュール部１０１およびデータ撹拌部１０２は、互いに同期的に動作し、鍵スケジュール部１０１において新たな拡大鍵が生成される毎に、当該拡大鍵を用いてデータ撹拌部１０２において１回のデータ撹拌が行われる。この、鍵スケジュール部１０１において新たな拡大鍵が生成され、当該拡大鍵を用いてデータ撹拌部１０２がデータ撹拌を行う１回分の処理を、１ラウンドとする。演算装置１００におけるラウンド毎の動作は、例えば上述した制御部により制御される。

【００２６】

先ず、鍵スケジュール部１０１について説明する。鍵スケジュール部１０１は、この基本的な構成においては、拡大鍵生成回路１２０、拡大鍵レジスタ１２１および検算用拡大鍵レジスタ１２２を有する。

【００２７】

拡大鍵生成回路１２０は、例えば図２に概略的に示されるように、線形変換を行う線形変換部２１１と、非線形変換を行う非線形変換部２１０とを有し、入力された鍵または拡大鍵に対して線形変換および非線形変換を行い、新たな拡大鍵を生成する。

【００２８】

なお、線形は、本来は重ね合わせが可能なことをいい、ある関数ｆ(ｘ)を考えたときに、関数ｆ(ａｘ＋ｂｙ)＝ａｆ(ｘ)＋ｂｆ(ｙ)を満たす場合、その関数ｆ(ｘ)は、線形である。例えば、加減算による変換は、線形である。また例えば、排他的論理和による変換は、変換の順序を入れ替えても同じ出力値が得られるため上述の条件を満たし、線形である。一方、ランダムに値を割り当てたテーブルを、入力値をインデクスとして参照して出力値を得るような変換は、入力値と出力値との関係が一定ではなく、例えば変換の順序を入れ替えると異なる出力値が得られ、上述の条件を満たさないため、非線形である。

【００２９】

拡大鍵生成回路１２０は、外部から供給された鍵または拡大鍵レジスタ１２１に格納される拡大鍵に対して線形処理および非線形処理を施し、拡大鍵を生成する。拡大鍵生成回路１２０で生成された拡大鍵は、拡大鍵レジスタ１２１に格納され、拡大鍵レジスタ１２１が更新される。検算用拡大鍵レジスタ１２２は、拡大鍵レジスタ１２１と同一のビット長を格納可能とされ、拡大鍵レジスタ１２１から供給された拡大鍵が格納されることで更新される。

【００３０】

図３は、拡大鍵生成回路１２０の一例の構成を示すブロック図である。この図３に例示される拡大鍵生成回路１２０は、ＡＥＳによる拡大鍵生成を、拡大鍵生成回路と拡大鍵レジスタとで構成する場合の例である。拡大鍵生成回路１２０は、非線形変換を行う非線形変換回路２１０（図３の例では「Ｆ」と記述）と、線形変換を行う排他的論理和回路２１１Ａ、２１１Ｂ、２１１Ｃおよび２１１Ｄとを有する。なお、図３における排他的論理和回路２１１Ａ、２１１Ｂ、２１１Ｃおよび２１１Ｄが、図２で説明した線形変換部２１１に相当する。

【００３１】

ｎ－１ラウンド目の拡大鍵が４分割されて、拡大鍵生成回路１２０の入力端２１２Ａ、２１２Ｂ、２１２Ｃおよび２１２Ｄにそれぞれ入力される。ここで、初期状態の鍵（暗号鍵または復号鍵）を、０ラウンド目の拡大鍵（すなわちｎ＝１）であるものとする。この例では、ビット長が１２８ビットのｎ－１ラウンド目の拡大鍵が、ビット長が３２ビットの部分に４分割される。ここで、ｎ－１ラウンド目の拡大鍵の値を値K_(n-1)と表し、当該拡大鍵が４分割された各部分鍵の値を、それぞれ値K_(n-1)_0、値K_(n-1)_1、値K_(n-1

)_2および値K_(n-1)_3と表すものとする。

【００３２】

これら値K_(n-1)_0、値K_(n-1)_1、値K_(n-1)_2および値K_(n-1)_3が、拡大鍵生成回路１２０の入力端２１２Ａ、２１２Ｂ、２１２Ｃおよび２１２Ｄを介して排他的論理和回路２１１Ａ、２１１Ｂ、２１１Ｃおよび２１１Ｄそれぞれ一方の入力端に入力される。また、値K_(n-1)_3が非線形変換回路２１０に入力される。値K_(n-1)_3は、非線形変換回路２１０で非線形変換されて排他的論理和回路２１１の他方の入力端に入力される。

【００３３】

ここで、非線形変換回路２１０は、入力されたデータに対して非線形変換処理を施しデータを非線形に攪乱する。非線形変換回路２１０としては、例えば予め与えられたテーブルであるＳ－ＢＯＸ(Substitution Box)が用いられる。Ｓ－ＢＯＸは、典型的な例では、入力データのデータ長を１６ビットとしたとき、ＭＳＢ側の８ビットとＬＳＢ側の８ビットとでテーブルを参照し、入力データを、当該入力データとは異なる１６ビットの出力データに変換する。このＳ－ＢＯＸは、一般的には、演算装置１００の構成の大きな部分を占める大規模なものとなる。

【００３４】

排他的論理和回路２１１Ａは、一方の入力端に入力された値K_(n-1)_0と、他方の入力端に入力された、値K_(n-1)_3が非線形変換されたデータとの排他的論理和を取り、値K_n_0を出力する。この値K_n_0は、拡大鍵レジスタ１２１の領域１２１Ａに格納されると共に、排他的論理和回路２１１Ｂの他方の入力端に入力される。

【００３５】

排他的論理和回路２１１Ｂは、一方の入力端に入力された値K_(n-1)_1と、他方の入力端に入力された値K_n_0との排他的論理和を取り、値K_n_1を出力する。この値K_n_1は、拡大鍵レジスタ１２１の領域１２１Ｂに格納されると共に、排他的論理和回路２１１Ｃの他方の入力端に入力される。排他的論理和回路２１１Ｃは、一方の入力端に入力された値K_(n-1)_2と、他方の入力端に入力された値K_n_1との排他的論理和を取り、値K_n_2を出力する。この値K_n_2は、拡大鍵レジスタ１２１の領域１２１Ｃに格納されると共に、排他的論理和回路２１１Ｄの他方の入力端に入力される。排他的論理和回路２１１Ｄは、一方の入力端に入力された値K_(n-1)_3と、他方の入力端に入力された値K_n_2との排他的論理和を取り、値K_n_3を出力する。この値K_n_3は、拡大鍵レジスタ１２１の領域１２１Ｄに格納される。

【００３６】

このように、拡大鍵レジスタ１２１の各領域１２１Ａ、１２１Ｂ、１２１Ｃおよび１２１Ｄには、各排他的論理和回路２１１Ａ、２１１Ｂ、２１１Ｃおよび２１１Ｄそれぞれから出力された値K_n_0、値K_n_1、値K_n_2および値K_n_3が格納される。すなわち、ｎラウンド目の拡大鍵の値K_nは、値K_n＝{ K_n_0, K_n_1, K_n_2, K_n_3 }として、値K_n_0、値K_n_1、値K_n_2および値K_n_3のビット結合で表すことができる。換言すれば、ｎラウンド目の拡大鍵の値K_nは、値K_n_0、値K_n_1、値K_n_2および値K_n_3が結合されて生成される。

【００３７】

拡大鍵レジスタ１２１に格納される値K_n_0、値K_n_1、値K_n_2および値K_n_3は、入力端２１２Ａ、２１２Ｂ、２１２Ｃおよび２１２Ｄに対し、それぞれ値K_(n-1)_0、値K_(n-1)_1、値K_(n-1)_2および値K_(n-1)_3として入力され、次のラウンドの拡大鍵が生成される。

【００３８】

説明は図１に戻り、鍵スケジュール部１０１の動作について、概略的に説明する。最初に、鍵（暗号鍵または復号鍵）が拡大鍵生成回路１２０に供給される。拡大鍵生成回路１２０は、第１ラウンド目の処理として、供給された鍵に対して上述のようにして排他的論理和回路２１１Ａ～２１１Ｄによる線形変換と、非線形変換回路２１０による非線形変換を施し、拡大鍵の各値K_n_0、値K_n_1、値K_n_2および値K_n_3を生成する。生成された値

K_n_0、値K_n_1、値K_n_2および値K_n_3は、それぞれ拡大鍵レジスタ１２１の領域１２１Ａ～１２１Ｄに格納され、拡大鍵レジスタ１２１が更新される。

【００３９】

次のラウンドにおいて、拡大鍵レジスタ１２１に格納される拡大鍵（値K_n_0、値K_n_1、値K_n_2および値K_n_3）が、検算用の拡大鍵として検算用拡大鍵レジスタ１２２に格納され、検算用拡大鍵レジスタ１２２が更新される。その後、拡大鍵生成回路１２０は、拡大鍵レジスタ１２１に格納される拡大鍵に対して線形変換および非線形変換を施し、第２ラウンド目の拡大鍵を生成する。拡大鍵レジスタ１２１に格納される第１ラウンド目の拡大鍵により検算用拡大鍵レジスタ１２２が更新され、次いで、拡大鍵生成回路１２０により生成された第２ラウンド目の拡大鍵により拡大鍵レジスタ１２１が更新される。

【００４０】

以降、拡大鍵生成回路１２０による拡大鍵レジスタ１２１に格納された拡大鍵を用いた拡大鍵の生成、拡大鍵レジスタ１２１に格納される１ラウンド前の拡大鍵による検算用拡大鍵レジスタ１２２の更新、拡大鍵生成回路１２０により生成された現在のラウンドの拡大鍵による拡大鍵レジスタ１２１の更新が、所定のラウンド数だけ繰り返される。すなわち、検算用拡大鍵レジスタ１２２には、拡大鍵レジスタ１２１に格納される拡大鍵に対して１ラウンド前の拡大鍵が検算用の拡大鍵として格納される。

【００４１】

次に、データ撹拌部１０２について説明する。データ撹拌部１０２は、ラウンド演算回路１１０、ラウンド検算回路１１１、データレジスタ１１２、検算用データレジスタ１１３、比較回路１１４および信号選択部１１５を有する。

【００４２】

信号選択部１１５は、暗号化の対象となる平文データ、または、復号の対象となる暗号化データ（以下、纏めて処理対象データと呼ぶ）が入力されると共に、ラウンド演算回路１１０、データレジスタ１１２および検算用データレジスタ１１３の出力がそれぞれ入力される。信号選択部１１５は、比較回路１１４の出力信号に応じて、入力されたデータから、後述するデータレジスタ１１２および検算用データレジスタ１１３を更新するためのデータを選択する。

【００４３】

データレジスタ１１２および検算用データレジスタ１１３は、信号選択部１１５から出力されたデータにより更新される。詳細は後述するが、検算用データレジスタ１１３は、データレジスタ１１２に保持される１ラウンド前のデータにより更新される。データレジスタ１１２の更新は、検算用データレジスタ１１３の更新が行われた後に行われる。すなわち、検算用データレジスタ１１３は、データレジスタ１１２に格納されるデータに対して１ラウンド前のデータが格納される。

【００４４】

ラウンド演算回路１１０は、上述した鍵スケジュール部１０１の拡大鍵レジスタ１２１から拡大鍵を読み出して、データレジスタ１１２に保持されるデータに対して１ラウンドの所定の演算処理を行う。演算結果は、信号選択部１１５に供給される。

【００４５】

ここで、この演算装置１００が暗号化装置として機能する場合には、ラウンド演算回路１１０は、拡大鍵レジスタ１２１から読み出した拡大鍵を用いて、所定の暗号化方式に従い、データレジスタ１１２に格納されるデータに対する１ラウンドの暗号化処理を行う。

【００４６】

一方、この演算装置１００が復号装置として機能する場合には、ラウンド演算回路１１０は、拡大鍵レジスタ１２１から読み出した拡大鍵を用いて、所定の暗号化方式に従い、データレジスタ１１２に格納されるデータに対する１ラウンドの復号処理を行う。以下では、特に記載のない限り、ラウンド演算回路１１０で行われる暗号化処理および復号処理の演算を纏めて、演算処理と呼ぶ。

【００４７】

ラウンド検算回路１１１は、上述した鍵スケジュール部１０１の検算用拡大鍵レジスタ１２２から拡大鍵を読み出して、データレジスタ１１２に格納されるデータに対して１ラウンドの検算処理を行う。検算結果は、比較回路１１４に供給される。

【００４８】

ここで、ラウンド検算回路１１１の検算処理は、ラウンド演算回路１１０の逆の演算により行われる。すなわち、この演算装置１００が暗号化装置として機能する場合には、ラウンド検算回路１１１は、検算用拡大鍵レジスタ１２２から読み出した検算用拡大鍵を用いて、上述のラウンド演算回路１１０でなされる所定の暗号化方式に対応する演算により、データレジスタ１１２に格納されるデータに対する１ラウンドの復号処理の演算を行い、検算とする。

【００４９】

一方、この演算装置１００が復号装置として機能する場合には、ラウンド検算回路１１１は、検算処理として、上述のラウンド演算回路１１０でなされる復号処理が対応する所定の暗号化方式に従い、データレジスタ１１２に格納されるデータに対する１ラウンドの暗号化処理の演算を行う。以下では、特に記載のない限り、ラウンド検算回路１１１で行われる復号処理および暗号化処理の演算を纏めて、検算処理と呼ぶ。

【００５０】

このように、ラウンド検算回路１１１では、ラウンド演算回路１１０で行った演算処理結果を１ラウンド分戻す演算処理を行うことで、検算とする。

【００５１】

比較回路１１４は、ラウンド検算回路１１１の出力と検算用データレジスタ１１３に格納されるデータとを比較する。比較の結果、両者が一致すれば、比較回路１１４は、ラウンド演算回路１１０による演算処理が正しいと判断し、次のラウンドの演算を行うように信号選択部１１５を制御する。一方、比較の結果、両者が一致しなければ、比較回路１１４は、ラウンド演算回路１１０による演算処理にエラーが発生したと判断し、以降のラウンドの演算を停止するように信号選択部１１５を制御する。

【００５２】

図４は、検算を異種処理で行う場合の、データ撹拌部１０２による演算および検算処理を示す一例のフローチャートである。なお、図４に例示される処理は、暗号化方式または復号方式によって定められるラウンド回数がＲ回（Ｒ＞２）である場合の例である。現在のラウンド数は、例えばデータ撹拌部１０２が備える図示されないカウンタによりカウントされる。

【００５３】

最初のステップＳ４００で、処理対象データが演算装置１００に入力され、信号選択部１１５に供給される。また、図示しないが、鍵が演算装置１００に入力され、拡大鍵生成回路１２０に供給される。拡大鍵生成回路１２０は、入力された鍵に対して上述した線形変換および非線形変換を施して拡大鍵を生成する。この拡大鍵が拡大鍵レジスタ１２１に格納される。

【００５４】

次のステップＳ４０１で、信号選択部１１５は、処理対象データをデータレジスタ１１２および検算用データレジスタ１１３にそれぞれ格納する。そして、ラウンド演算回路１１０がデータレジスタ１１２に格納される処理対象データに対して、拡大鍵レジスタ１２１に格納される拡大鍵を用いて１ラウンド目の演算処理を施す。ラウンド演算回路１１０による演算結果が信号選択部１１５を介してデータレジスタ１１２に格納され、データレジスタ１１２が更新される。

【００５５】

鍵スケジュール部１０１において、拡大鍵レジスタ１２１に格納される拡大鍵が検算用拡大鍵レジスタ１２２に検算用拡大鍵として格納されると共に、拡大鍵生成回路１２０が拡大鍵レジスタ１２１に格納される拡大鍵を用いて新たな拡大鍵を生成する。生成された新たな拡大鍵は、拡大鍵レジスタ１２１に格納され、拡大鍵レジスタ１２１が更新される

。

【００５６】

次のステップＳ４０２で、ラウンド演算回路１１０は、データレジスタ１１２に格納されるデータを入力として、拡大鍵レジスタ１２１に格納される拡大鍵を用いて、２ラウンド目の演算処理を行う。それと共に、ステップＳ４０２で、ラウンド検算回路１１１は、データレジスタ１１２に格納されるデータを入力として、検算用拡大鍵レジスタ１２２に格納される拡大鍵を用いて検算処理を行う。

【００５７】

ラウンド検算回路１１１で行われる検算処理は、ラウンド演算回路１１０で行われる演算処理と逆の処理である。また、検算用拡大鍵レジスタ１２２に格納される拡大鍵は、拡大鍵レジスタ１２１に格納される拡大鍵に対して１ラウンド前の状態の拡大鍵である。したがって、ラウンド検算回路１１１での検算により、入力とされるデータレジスタ１１２に格納されるデータ１ラウンド前の状態に戻されることになる。ラウンド検算回路１１１による検算結果は、比較回路１１４に供給される。

【００５８】

次のステップＳ４０３で、比較回路１１４は、ラウンド検算回路１１１から供給された検算結果と、検算用データレジスタ１１３に格納されるデータとを比較して、両者が一致するか否かを判定する。若し、一致しないと判定されたら、演算処理にエラーがあったとされ、一連の処理が終了される。一方、両者が一致すると判定されたら、処理はステップＳ４０４に移行される。

【００５９】

ステップＳ４０４で、信号選択部１１５は、データレジスタ１１２のデータを検算用データレジスタ１１３に格納し、検算用データレジスタ１１３を更新すると共に、上述のステップＳ４０２で行われたラウンド演算回路１１０による演算結果をデータレジスタ１１２に格納し、データレジスタ１１２を更新する。

【００６０】

また、鍵スケジュール部１０１において、拡大鍵レジスタ１２１に格納される拡大鍵が検算用拡大鍵レジスタ１２２に検算用拡大鍵として格納される。また、拡大鍵生成回路１２０は、拡大鍵レジスタ１２１に格納される拡大鍵を用いて新たな拡大鍵を生成する。この新たな拡大鍵は、拡大鍵レジスタ１２１に格納され、拡大鍵レジスタ１２１が更新される。

【００６１】

次のステップＳ４０５で、例えば図示されないカウンタにより、ラウンド演算回路１１０における演算処理が所定回数（この例ではＲ－１回）を終了したか否かが判定される。若し、終了していないと判定されたら、処理がステップＳ４０２に戻され、次のラウンドの処理がなされる。

【００６２】

一方、ステップＳ４０５で、ラウンド演算回路１１０における演算処理が所定回数を終了したと判定されたら、処理はステップＳ４０６に移行される。ステップＳ４０６では、ラウンド検算回路１１１は、データレジスタ１１２に格納されるデータを入力として、検算用拡大鍵レジスタ１２２に格納される検算用拡大鍵を用いて検算処理を行う。検算処理の結果は、比較回路１１４に供給される。

【００６３】

次のステップＳ４０７で、比較回路１１４は、ラウンド検算回路１１１から供給された検算結果と、検算用データレジスタ１１３に格納されるデータとを比較して、両者が一致するか否かを判定する。若し、一致しないと判定されたら、演算処理にエラーがあったとされ、一連の処理が終了される。一方、両者が一致すると判定されたら、処理はステップＳ４０８に移行される。

【００６４】

ステップＳ４０８では、データレジスタ１１２に格納されるデータが出力データに決定

され、ステップＳ４０９で、当該出力データが演算装置１００から出力される。

【００６５】

なお、この図４のフローチャートによる処理は、演算装置１００が平文データの暗号化を行う暗号化装置あるいは暗号化データの復号を行う復号装置の何れであっても適用可能である。すなわち、ラウンド演算回路１１０が暗号化の演算を行い、ラウンド検算回路１１１が対応する復号の演算を行う場合であっても、ラウンド演算回路１１０が復号の演算を行い、ラウンド検算回路１１１が対応する暗号化の演算を行う場合であっても、図４のフローチャートによる処理を適用することができる。またこの場合、鍵スケジュール部１０１の動作は、演算装置１００が暗号化装置あるいは復号装置の何れの場合であっても同一である。

【００６６】

次に、検算を同種処理により行う場合について説明する。図５は、検算を同種処理により行う場合の、検算機能付き暗号化装置または復号装置の基本的な構成の例を示す。なお、検算を同種処理により行う場合でも、暗号化装置と復号装置は、同一の構成で実現可能であるので、以下では、特に記載のない限り、暗号化装置および復号装置を纏めて演算装置と呼ぶ。

【００６７】

図５に例示される演算装置１００’は、図１に例示した演算装置１００と同様に、同じ演算処理を複数回繰り返し実行して、平文データの暗号化または暗号データの復号を行う。演算装置１００’は、図１に例示した演算装置と同様に、暗号化または復号に対する検算機能を有する。なお、図５において、上述の図１と共通する部分には同一の符号を付し、詳細な説明を省略する。

【００６８】

演算装置１００’は、鍵スケジュール部１０１とデータ撹拌部１０２’とを有する。鍵スケジュール部１０１は、図１～図３を用いて説明した異種処理の場合の例と全く同じ構成および動作を適用できるので、ここでの説明を省略する。

【００６９】

データ撹拌部１０２’において、ラウンド検算回路１６０は、検算用拡大鍵レジスタ１２２から拡大鍵が供給されると共に、データレジスタ１１２に格納されるデータを入力として、ラウンド演算回路１１０と同一の演算を行う。すなわち、この演算装置１００’が暗号化装置として機能する場合には、ラウンド検算回路１６０は、検算用拡大鍵レジスタ１２２から供給される検算用拡大鍵を用いて、ラウンド演算回路１１０でなされる演算処理と同一の、所定の暗号化方式による演算を行う。

【００７０】

また、この演算装置１００’が復号装置として機能する場合にも、ラウンド検算回路１６０は、検算用拡大鍵レジスタ１２２から供給される検算用拡大鍵を用いて、ラウンド演算回路１１０でなされる演算処理と同一の、所定の暗号化方式による復号処理の演算を行う。

【００７１】

ラウンド検算回路１６０の検算結果は、比較回路１１４’に供給される。比較回路１１４’は、ラウンド検算回路１６０から供給された検算結果と、データレジスタ１１２に格納されるデータとを比較する。比較の結果、両者が一致すれば、比較回路１１４’は、ラウンド演算回路１１０による演算処理が正しいと判断し、次のラウンドの演算を行うように信号選択部１１５を制御する。一方、比較の結果、両者が一致しなければ、比較回路１１４’は、ラウンド演算回路１１０による演算処理にエラーが発生したと判断し、以降のラウンドの演算を停止するように信号選択部１１５を制御する。

【００７２】

図６は、検算を同種処理で行う場合の、データ撹拌部１０２’による演算および検算処理を示す一例のフローチャートである。なお、図５に例示される処理は、暗号化方式または復号方式によって定められるラウンド回数がＲ回（Ｒ＞２）である場合の例である。現

在のラウンド数は、例えばデータ撹拌部１０２’が備える図示されないカウンタによりカウントされる。

【００７３】

最初のステップＳ５００で、処理対象データが演算装置１００’に入力され、信号選択部１１５に供給される。また、図示しないが、鍵が演算装置１００’に入力され、拡大鍵生成回路１２０に供給される。拡大鍵生成回路１２０は、入力された鍵に対して上述した線形変換および非線形変換を施して拡大鍵を生成する。この拡大鍵が拡大鍵レジスタ１２１に格納される。

【００７４】

次のステップＳ５０１で、信号選択部１１５は、処理対象データをデータレジスタ１１２および検算用データレジスタ１１３にそれぞれ格納する。そして、ラウンド演算回路１１０がデータレジスタ１１２に格納される処理対象データに対して、拡大鍵レジスタ１２１に格納される拡大鍵を用いて１ラウンド目の演算処理を施す。ラウンド演算回路１１０による演算結果が信号選択部１１５を介してデータレジスタ１１２に格納され、データレジスタ１１２が更新される。

【００７５】

鍵スケジュール部１０１において、拡大鍵レジスタ１２１に格納される拡大鍵が、検算用拡大鍵レジスタ１２２に検算用拡大鍵として格納される。そして、拡大鍵生成回路１２０は、拡大鍵レジスタ１２１に格納される拡大鍵を用いて新たな拡大鍵を生成する。生成された新たな拡大鍵は、拡大鍵レジスタ１２１に格納され、拡大鍵レジスタ１２１が更新される。

【００７６】

次のステップＳ５０２で、ラウンド演算回路１１０は、データレジスタ１１２に格納されるデータを入力として、拡大鍵レジスタ１２１に格納される拡大鍵を用いて、２ラウンド目の演算処理を行う。それと共に、ステップＳ５０２で、ラウンド検算回路１６０は、検算用データレジスタ１１３に格納されるデータを入力として、検算用拡大鍵レジスタ１２２に格納される拡大鍵を用いて検算処理を行う。

【００７７】

ラウンド検算回路１６０で行われる検算処理は、ラウンド演算回路１１０で行われる演算処理と同一の処理である。一方、検算用拡大鍵レジスタ１２２に格納される検算用拡大鍵は、拡大鍵レジスタ１２１に格納される拡大鍵に対して１ラウンド前の状態の拡大鍵である。また、検算用データレジスタ１１３には、１ラウンド前のデータが格納されている。したがって、ラウンド検算回路１６０での検算により、ラウンド演算回路１１０で１ラウンド前に行われた演算と同一の演算が行われることになる。ラウンド検算回路１６０による検算結果は、比較回路１１４’に供給される。

【００７８】

次のステップＳ５０３で、比較回路１１４’は、ラウンド検算回路１６０から供給された検算結果と、データレジスタ１１２に格納されるデータとを比較して、両者が一致するか否かを判定する。この場合、データレジスタ１１２は、ステップＳ５０２によるラウンド演算回路１１０による演算結果による更新が行われていないので、１ラウンド目の演算結果が格納されていることになる。若し、一致しないと判定されたら、演算処理にエラーがあったとされ、一連の処理が終了される。一方、両者が一致すると判定されたら、処理はステップＳ５０４に移行される。

【００７９】

ステップＳ５０４で、信号選択部１１５は、データレジスタ１１２のデータを検算用データレジスタ１１３に格納し、検算用データレジスタ１１３を更新する。それと共に、ステップＳ５０４で、上述のステップＳ５０２で行われたラウンド演算回路１１０による演算結果が信号選択部１１５に供給される。信号選択部１１５は、供給された演算結果をデータレジスタ１１２に格納し、データレジスタ１１２を更新する。

【００８０】

また、鍵スケジュール部１０１において、拡大鍵レジスタ１２１に格納される拡大鍵が、検算用拡大鍵レジスタ１２２に検算用拡大鍵として格納される。また、拡大鍵生成回路１２０は、拡大鍵レジスタ１２１に格納される拡大鍵を用いた新たな拡大鍵を生成する。この新たな拡大鍵は、拡大鍵レジスタ１２１に格納され、拡大鍵レジスタ１２１が更新される。

【００８１】

次のステップＳ５０５で、例えば図示されないカウンタにより、ラウンド演算回路１１０における演算処理が所定回数（この例ではＲ－１回）を終了したか否かが判定される。若し、終了していないと判定されたら、処理がステップＳ５０２に戻され、次のラウンドの処理が行われる。

【００８２】

一方、ステップＳ５０５で、ラウンド演算回路１１０における演算処理が所定回数を終了したと判定されたら、処理はステップＳ５０６に移行される。ステップＳ５０６では、ラウンド検算回路１６０は、検算用データレジスタ１１３に格納されるデータを入力として、検算用拡大鍵レジスタ１２２に格納される検算用拡大鍵を用いて検算処理を行う。検算処理の結果は、比較回路１１４’に供給される。

【００８３】

次のステップＳ５０７で、比較回路１１４’は、ラウンド検算回路１６０から供給された検算結果と、データレジスタ１１２に格納されるデータとを比較して、両者が一致するか否かを判定する。若し、一致しないと判定されたら、演算処理にエラーがあったとされ、一連の処理が終了される。一方、両者が一致すると判定されたら、処理はステップＳ５０８に移行される。

【００８４】

ステップＳ５０８では、データレジスタ１１２に格納されるデータが出力データに決定され、ステップＳ５０９で、当該出力データが演算装置１００’から出力される。

【００８５】

なお、この図６のフローチャートによる処理は、演算装置１００’が平文データの暗号化を行う暗号化装置あるいは暗号化データの復号を行う復号装置の何れであっても適用可能である。すなわち、ラウンド演算回路１１０およびラウンド検算回路１６０が暗号化の演算を行う場合であっても、ラウンド演算回路１１０およびラウンド検算回路１６０が復号の演算を行う場合であっても、図６のフローチャートによる処理を適用することができる。またこの場合、鍵スケジュール部１０１の動作は、演算装置１００’が暗号化装置あるいは復号装置の何れの場合であっても同一である。

【００８６】

＜本実施の形態による検算機能付き演算装置＞

次に、本実施の形態による検算機能付き演算装置について説明する。上述した鍵スケジュール部１０１の動作と、図４および図６のフローチャートを用いて説明したデータ撹拌部１０２（またはデータ撹拌部１０２’）の動作から分かるように、ラウンド演算回路１１０における演算処理と、ラウンド検算回路１１１（またはラウンド検算回路１６０）における検算処理は、１ラウンド分ずれて実行される。そのため、演算装置１００（または演算装置１００’）は、２ラウンド分の拡大鍵をレジスタに保持する必要がある。

【００８７】

なお、図４および図６を用いて既に説明したように、検算を異種処理で行う演算装置１００と、同種処理で行う演算装置１００’とでは、演算処理と検算処理とが互いに対応するタイミングで行われる。そのため、煩雑さを避けるため、以下では、特に記載のない限り、演算装置１００および演算装置１００’について、演算装置１００で代表させて説明する。

【００８８】

図７を用いて、演算処理と検算処理との関係についてより具体的に説明する。先ず、１ラウンド目の処理では、ラウンド演算回路１１０において、１段目の拡大鍵を用いて１ラ

ウンド目の演算処理が行われる。次に、２ラウンド目の処理では、ラウンド演算回路１１０において、２段目の拡大鍵を用いて２ラウンド目の演算処理が行われると共に、ラウンド検算回路１１１において、１段目の拡大鍵を用いて１ラウンド目の演算処理結果に対して検算処理が行われる。すなわち、２ラウンド目の処理では、演算装置１００は、検算用の１段目の拡大鍵と、演算用の２段目の拡大鍵とを保持している必要がある。

【００８９】

３ラウンド目の処理では、ラウンド演算回路１１０において３段目の拡大鍵を用いて３ラウンド目の演算処理が行われると共に、ラウンド検算回路１１１において、２段目の拡大鍵を用いて２ラウンド目の演算結果に対して検算処理が行われる。すなわち、３ラウンド目の処理では、演算装置１００は、検算用の２段目の拡大鍵と、演算用の３段目の拡大鍵とを保持している必要がある。

【００９０】

以降、同様にして、ｎラウンド目の処理（図示しない）では、ラウンド演算回路１１０においてｎラウンド目の拡大鍵を用いてｎラウンド目の演算処理が行われると共に、ラウンド検算回路１１１において、検算用のｎ－１段目の拡大鍵を用いてｎ－１ラウンド目の検算処理が行われる。このように、ラウンド演算回路１１０およびラウンド検算回路１１１では、１ラウンド分ずれた拡大鍵を用いてそれぞれ演算および検算が行われる。

【００９１】

最終ラウンドのＮラウンド目の処理では、ラウンド演算回路１１０においてＮラウンド目の拡大鍵を用いてＮラウンド目の演算処理が行われると共に、ラウンド検算回路１１１において、Ｎ－１段目の拡大鍵を用いてＮ－１ラウンド目の検算処理が行われる。そして、最終的に、ラウンド検算回路１１１において、Ｎラウンド目の演算結果に対してＮ段目の拡大鍵を用いて検算処理を行い、検算結果が正しければ、Ｎラウンド目の演算結果が正しい暗号化データまたは平文データとして演算装置１００から出力される。

【００９２】

このように、演算装置１００は、１ラウンド目および最終ラウンドのＮラウンド目を除いて、各ラウンド毎に２の拡大鍵をレジスタに保持する必要がある。

【００９３】

本実施の形態では、図１または図５に例示される演算装置１００または演算装置１００’の鍵スケジュール部１０１に対して、拡大鍵生成回路１２０が有する線形変換部２００の逆の処理を行う線形変換回路を追加する。これにより、拡大鍵を保持するレジスタの容量を削減している。

【００９４】

図８は、本実施の形態による、線形変換回路が追加された鍵スケジュール部１４０の一例の構成を示す。この本実施の形態による鍵スケジュール部１４０は、拡大鍵生成回路１２０の構成、ならびに、拡大鍵生成回路１２０と拡大鍵レジスタ１２１との接続は、図３を用いて説明した構成をそのまま適用できる。なお、図８において、上述した図３を共通する部分には同一の符号を付し、詳細な説明を省略する。

【００９５】

ｎ－１ラウンド目の拡大鍵が４分割された各値K_(n-1)_0、値K_(n-1)_1、値K_(n-1)_2および値K_(n-1)_3が、拡大鍵生成回路１２０の入力端２１２Ａ、２１２Ｂ、２１２Ｃおよび２１２Ｄにそれぞれ入力され、拡大鍵の生成処理が行われる。処理の結果、新たな拡大鍵の各値K_n_0、値K_n_1、値K_n_2および値K_n_3が生成され、拡大鍵レジスタ１２１の領域１２１Ａ、１２１Ｂ、１２１Ｃおよび１２１Ｄにそれぞれ格納される。

【００９６】

図８において、拡大鍵レジスタ１２１から拡大鍵生成回路１２０の入力端２１２Ａ、２１２Ｂ、２１２Ｃおよび２１２Ｄに遡った演算を行うことができれば、ｎ－１ラウンド目の演算が可能となる。これにより、ｎラウンド目において、ｎ－１ラウンド目の拡大鍵の全てを保持していなくても、ｎ－１ラウンド目の拡大鍵を検算用拡大鍵として用いた検算処理を行うことができるようになる。

【００９７】
そこで、本実施の形態では、鍵スケジュール部１０１に対して、拡大鍵レジスタ１２１に格納される各値K_n_0、値K_n_1、値K_n_2および値K_n_3を前段の値に復元可能な回路を設ける。このとき、この回路として、回路規模の小さい可逆演算回路が選択される。
【００９８】
より具体的には、図８に例示されるように、排他的論理和回路１５２Ａ、１５２Ｂおよび１５２Ｃを有する線形変換回路１５０を設ける。そして、拡大鍵レジスタ１２１の領域１２１Ａ、１２１Ｂ、１２１Ｃおよび１２１Ｄに格納される各値K_n_0、値K_n_1、値K_n_2および値K_n_3を、排他的論理和回路１５２Ａ、１５２Ｂおよび１５２Ｃの各入力端にそれぞれ入力する。
【００９９】
より詳細には、排他的論理和回路１５２Ａの一方および他方の入力端に、拡大鍵レジスタ１２１の領域１２１Ａに格納される値K_n_0と、領域１２１Ｂに格納される値K_n_1とがそれぞれ入力される。また、排他的論理和回路１５２Ｂの一方および他方の入力端に、拡大鍵レジスタ１２１の領域１２１Ｂに格納される値K_n_1と、領域１２１Ｃに格納される値K_n_2とがそれぞれ入力される。さらに、排他的論理和回路１５２Ｃの一方および他方の入力端に、拡大鍵レジスタ１２１の領域１２１Ｃに格納される値K_n_2と、領域１２１Ｄに格納される値K_n_3とがそれぞれ入力される。
【０１００】
ここで、図８の構成から、領域１２１Ｂに格納される値K_n_1は、領域１２１Ａに格納される値K_n_0と入力端２１２Ｂに入力された値K_(n-1)_1との排他的論理和と見做すことができる。したがって、排他的論理和の性質から、値K_n_1と値K_n_0との排他的論理和を取ることで、入力端２１２Ｂに入力された値K_(n-1)_1を得ることができる。
【０１０１】
領域１２１Ｃに格納される値K_n_2および領域１２１Ｄに格納される値K_n_3についても同様である。領域１２１Ｃに格納される値K_n_2は、領域１２１Ｂに格納される値K_n_1と入力端２１２Ｃに入力された値K_(n-1)_2との排他的論理和と見做すことができ、値K_n_2と値K_n_1との排他的論理和を取ることで、入力端２１２Ｃに入力された値K_(n-1)_2を得ることができる。また、領域１２１Ｄに格納される値K_n_3は、領域１２１Ｃに格納される値K_n_2と入力端２１２Ｄに入力された値K_(n-1)_3との排他的論理和と見做すことができ、値K_n_3と値K_n_2との排他的論理和を取ることで、入力端２１２Ｄに入力された値K_(n-1)_3を得ることができる。
【０１０２】
このように、ｎ－１ラウンド目の拡大鍵を構成する値K_(n-1)_1、値K_(n-1)_2および値K_(n-1)_3については、拡大鍵レジスタ１２１の各領域１２１Ａ～１２１Ｄに格納されるｎラウンド目の拡大鍵の各値K_n_0、値K_n_1、値K_n_2および値K_n_3に対して排他的論理和を取ることで得ることができる。
【０１０３】
一方、入力端２１２Ａに入力された値K_(n-1)_0は、非線形回路２１０による非線形変換が含まれた演算が行われる。この場合、拡大鍵レジスタ１２１に格納される各値から値K_(n-1)_0を求めるためには、非線形回路２１０の逆変換を行うための回路を設ける必要がある。非線形回路２１０の逆変換を行う回路は、非線形回路２１０と同等の構成となり、回路規模も同等となるため、本実施の形態の主旨にそぐわない。
【０１０４】
そこで、本実施の形態では、検算用拡大鍵レジスタ１５１を設けて、非線形回路２１０の変換結果に対して直接的に線形変換を行う排他的論理和回路２１１Ａの入力のうち一方に、当該検算用拡大鍵レジスタ１５１を接続する。図８の例では、検算用拡大鍵レジスタ１５１を、排他的論理和回路２１１Ａの一方の入力端すなわち入力端２１２Ａに接続する。そして、ｎ－１ラウンド目に入力端２１２Ａに入力された値K_(n-1)_0を、この検算用拡大鍵レジスタ１５１に格納する。したがって、検算用拡大鍵レジスタ１５１は、値K_(n

-1)_0が格納可能なだけの容量を有すればよい。この例では、検算用拡大鍵レジスタ１５１は、拡大鍵レジスタ１２１の１／４の容量があればよいことになる。

【０１０５】

ｎラウンド目に、この検算用拡大鍵レジスタ１５１に格納される値K_(n-1)_0と、線形変換回路１５０の排他的論理和回路１５２Ａ～１５２Ｃそれぞれの出力である値K_(n-1)_1、値K_(n-1)_2および値K_(n-1)_3とをビット結合して、値K_(n-1)であるｎ－ラウンド目の拡大鍵すなわちｎラウンド目の検算用拡大鍵が生成される。

【０１０６】

なお、図８では、検算用拡大鍵レジスタ１５１が拡大鍵生成回路１２０の入力側に接続されるように説明したが、これは、検算用拡大鍵レジスタ１５１が拡大鍵レジスタ１２１における領域１２１Ａに対して接続されることと等価である。この場合、例えば、拡大鍵レジスタ１２１から拡大鍵が読み出されるタイミングで、拡大鍵レジスタ１２１の領域１２１Ａのデータが検算用拡大鍵レジスタ１５１に格納され、検算用拡大鍵レジスタ１５１が更新される。

【０１０７】

図９は、図８に例示した本実施の形態による鍵スケジュール部１４０を、上述した図１に例示される演算装置１００に対して鍵スケジュール部１０１に代えて適用させた例を示す。なお、図９において、上述した図１と共通する部分には同一の符号を付し、詳細な説明を省略する。

【０１０８】

図９に例示される演算装置１３０は、データ撹拌部１０２と鍵スケジュール部１４０とを有する。なお、鍵スケジュール部１４０において、線形変換回路１５０および検算用拡大鍵レジスタ１５１を纏めて鍵出力部１７０と呼ぶ。すなわち、鍵出力部１７０は、検算用拡大鍵レジスタ１５１に格納される値K_(n-1)_0と、線形変換回路１５０の出力である値K_(n-1)_1、値K_(n-1)_2および値K_(n-1)_3とをビット結合して、検算用拡大鍵として出力する。

【０１０９】

データ撹拌部１０２のラウンド演算回路１１０は、鍵スケジュール部１４０の拡大鍵レジスタ１２１からｎラウンド目の拡大鍵を読み出して１ラウンド分の演算処理を行う。また、ラウンド検算回路１１１は、検算用拡大鍵レジスタ１５１に格納される値K_(n-1)_0と、線形変換回路１５０の出力である値K_(n-1)_1、値K_(n-1)_2および値K_(n-1)_3とがビット結合された値K_(n-1)を、ｎラウンド目の検算用拡大鍵として用いて検算処理を行う。

【０１１０】

データ撹拌部１０２は、これら拡大鍵レジスタ１２１から読み出した拡大鍵と、検算用拡大鍵レジスタ１５１および線形変換回路１５０から供給される検算用拡大鍵とを用いて、図４のフローチャートを用いて説明した処理により、演算処理および検算処理を行う。

【０１１１】

上述では、演算装置１３０が、暗号化処理または復号処理の演算に対する検算を異種処理で行う例について説明したが、これはこの例に限定されるものではない。すなわち、本実施の形態は、暗号化処理また復号処理の演算に対する検算を同種処理で行う場合にも、同様に適用することができる。これは、検算を異種処理により行う図１の構成と、検算を同種処理により行う図５の構成とで鍵スケジュール部１０１の構成が共通していることから明らかである。

【０１１２】

このように、本実施の形態によれば、検算用拡大鍵レジスタ１５１は、拡大鍵の一部分を格納可能な容量を有すればよく、図１および図５を用いて説明したような、拡大鍵レジスタ１２１と同じ容量の検算用拡大鍵レジスタ１２２を持つ場合に比べて、遙かに回路規模を小さくすることができる。

【０１１３】

なお、本実施の形態によれば、線形変換回路１５０が新たに追加されているが、この線形変換回路１５０は高々３の排他的論理和回路１５２Ａ、１５２Ｂおよび１５２Ｃで構成されるものである。周知のように、排他的論理和回路は、非常に小規模な構成で実現され、検算用拡大鍵レジスタの容量が削減された効果を相殺するようなものではない。

【０１１４】

＜本実施の形態の第１の変形例＞

図１０は、本実施の形態の第１の変形例による鍵スケジュール部１４１の一例の構成を示す。なお、図１０において、上述した図８と共通する部分には同一の符号を付し、詳細な説明を省略する。本実施の形態の第１の変形例においては、検算用拡大鍵レジスタ１５１を、非線形回路２１０の変換結果に対して直接的に線形変換を行う排他的論理和回路２１１Ａの他方の入力端、すなわち、非線形変換回路２１０の出力に接続する。

【０１１５】

ここで、拡大鍵生成回路１２０では、非線形変換回路２１０の出力と入力端２１２Ａに入力されたｎ－１ラウンド目の拡大鍵における値K_(n-1)_0との排他的論理和を取ることで、拡大鍵における値K_n_0を生成している。したがって、検算用拡大鍵レジスタ１５１に格納されるデータを１ラウンド前の状態に戻すには、当該データに対して同等の処理を施す必要がある。

【０１１６】

そこで、本実施の形態の第１の変形例における線形変換回路１５０’は、上述の実施の形態による線形変換回路１５０に対して排他的論理和回路１５４をさらに設けた構成とする。そして、排他的論理和回路１５４により、検算用拡大鍵レジスタ１５１に保持されるデータと、拡大鍵レジスタ１２１の領域１２１Ａに格納される値K_n_0との排他的論理和を取る。これにより、拡大鍵生成回路１２０内の排他的論理和回路２１１Ａと同等の処理を行うことができ、排他的論理和回路１５４から、値K_n_0が1ラウンド分戻された値K_(n-1)_0が出力される。

【０１１７】

したがって、ｎラウンド目に、この検算用拡大鍵レジスタ１５１に格納される値K_(n-1)_0と、線形変換回路１５０の排他的論理和回路１５２Ａ～１５２Ｃそれぞれの出力である値K_(n-1)_1、値K_(n-1)_2および値K_(n-1)_3とをビット結合して、値K_(n-1)であるｎ－１ラウンド目の拡大鍵すなわちｎラウンド目の検算用拡大鍵が生成される。

【０１１８】

このように、本第１の実施の形態の第１の変形例においても、検算用拡大鍵レジスタ１５１は、非線形変換回路２１０の出力が格納可能なだけの容量を有すればよいことになる。この場合も、上述と同様に、検算用拡大鍵レジスタ１５１は、拡大鍵レジスタ１２１の１／４の容量があればよい。

【０１１９】

本実施の形態の第１の変形例によれば、検算用拡大鍵レジスタ１５１にデータが格納されるタイミングが、拡大鍵レジスタ１２１の各領域１２１Ａ、１２１Ｂ、１２１Ｃおよび１２１Ｄに値K_n_0、値K_n_1、値K_n_2および値K_n_3がそれぞれ格納されるタイミングと一致している。そのため、拡大鍵の各値K_n_0、値K_n_1、値K_n_2および値K_n_3が線形変換回路１５０’から出力されるタイミングの同時性の点で、上述の実施の形態による図８の構成に対して有利である。

【０１２０】

本実施の形態の第１の変形例による鍵スケジュール部１４１も、ｎラウンド目の拡大鍵とｎ－１ラウンド目の検算用拡大鍵とを同時に得ることができるため、上述した実施の形態による鍵スケジュール部１４０と同様に、図１に例示される演算装置１００における鍵スケジュール部１０１に代えて適用可能である。勿論、本実施の形態の第１の変形例による鍵スケジュール部１４１は、暗号化処理また復号処理の演算に対する検算を同種処理で行う場合にも、同様に適用することができる。

【０１２１】

＜本実施の形態の第２の変形例＞

次に、本実施の形態の第２の変形例について説明する。上述では、拡大鍵生成回路１２０における線形変換を、排他的論理和回路を用いて行っているが、これはこの例に限定されない。例えば、拡大鍵生成回路において、当該線形変換を他の構成で実現した場合であっても、本実施の形態を適用することができる。

【０１２２】

図１１は、本実施の形態の第２の変形例による鍵スケジュール部１４２の一例の構成を示す。この鍵スケジュール部１４２は、拡大鍵生成回路１２０”における線形変換を、加算回路とビットシフト回路とを用いて実現した例である。なお、図１１において、上述した図８と共通する部分には同一の符号を付し、詳細な説明を省略する。

【０１２３】

すなわち、拡大鍵生成回路１２０”に対し、ｎ－１ラウンド目の拡大鍵を４分割した各値K_(n-1)_0、値K_(n-1)_1、値K_(n-1)_2および値K_(n-1)_3が、入力端２１２Ａ、２１２Ｂ、２１２Ｃおよび２１２Ｄを介して排他的論理和回路２２０Ａ、加算回路２２１Ａ、排他的論理和回路２２０Ｂおよび加算回路２２１Ｂそれぞれの一方の入力端に入力される。また、値K_(n-1)_3が非線形変換回路２１０に入力される。値K_(n-1)_3は、非線形変換回路２１０で非線形変換されて排他的論理和回路２２０Ａの他方の入力端に入力される。

【０１２４】

排他的論理和回路２２０Ａは、一方の入力端に入力された値K_(n-1)_0と、他方の入力端に入力された、値K_(n-1)_3が非線形変換されたデータとの排他的論理和を取り、値K_n_0を出力する。この値K_n_0は、拡大鍵レジスタ１２１の領域１２１Ａに格納されると共に、加算回路２２１Ａの他方の入力端に入力される。

【０１２５】

加算回路２２１Ａは、一方の入力端に入力された値K_(n-1)_1と、他方の入力端に入力された値K_n_0とを加算し、値K_n_1を出力する。この値K_n_1は、拡大鍵レジスタ１２１の領域１２１Ｂに格納されると共に、ビットシフト回路２２２で左ビットシフトされて排他的論理和回路２２０Ｂの他方の入力端に入力される。排他的論理和回路２２０Ｂは、一方の入力端に入力された値K_(n-1)_2と、他方の入力端に入力された値K_n_1との排他的論理和を取り、値K_n_2を出力する。この値K_n_2は、拡大鍵レジスタ１２１の領域１２１Ｃに格納されると共に、加算回路２２１Ｂの他方の入力端に入力される。加算回路２２１Ｂは、一方の入力端に入力された値K_(n-1)_3と、他方の入力端に入力された値K_n_2とを加算し、値K_n_3を出力する。この値K_n_3は、拡大鍵レジスタ１２１の領域１２１Ｄに格納される。

【０１２６】

ここで、図１１の構成から、領域１２１Ｂに格納される値K_n_1は、領域１２１Ａに格納される値K_n_0と入力端２１２Ｂに入力された値K_(n-1)_1とを加算したものと見做すことができる。そのため、値K_n_1から値K_n_0を減ずることで、入力端２１２Ｂに入力された値K_(n-1)_1を得ることができる。

【０１２７】

領域１２１Ｃに格納される値K_n_2は、領域１２１Ｂに格納される値K_n_1と入力端２１２Ｃに入力された値K_(n-1)_2との排他的論理和と見做すことができる。そのため、値K_n_2と値K_n_1との排他的論理和を取ることで、入力端２１２Ｃに入力された値K_(n-1)_2を得ることができる。同様に、また、領域１２１Ｄに格納される値K_n_3は、領域１２１Ｃに格納される値K_n_2と入力端２１２Ｄに入力された値K_(n-1)_3とを加算したものと見做すことができる。そのため、値K_n_3から値K_n_2を減ずることで、入力端２１２Ｄに入力された値K_(n-1)_3を得ることができる。

【０１２８】

したがって、本実施の形態の第２の変形例では、拡大鍵レジスタ１２１に格納される拡大鍵を１ラウンド分戻すための線形変換回路１５０”を、減算回路１５５Ａ、右ビットシフトを行うビットシフト回路２３０、排他的論理和回路１５６および減算回路１５５Ｂを

順次接続して構成する。

【０１２９】

このような構成において、減算回路１５５Ａの減算入力端に拡大鍵レジスタ１２１の領域１２１Ａに格納される値K_n_0を入力し、領域１２１Ｂに格納される値K_n_1を減算回路１５５Ａの被減算入力端に入力する。減算回路１５５Ａで、値K_n_1から値K_n_0を減じてｎ－１ラウンド目の拡大鍵を構成する値K_(n-1)_1を得る。また、排他的論理和回路１５６の一方の入力端に、拡大鍵レジスタ１２１の領域１２１Ｂに格納される値K_n_1をビットシフト回路２３０で右ビットシフトさせて入力し、領域１２１Ｃに格納される値K_n_2を排他的論理和回路１５６の他方の入力端に入力する。排他的論理和回路１５６で、値K_n_1と値K_n_2との排他的論理和を取って、ｎ－１ラウンド目の拡大鍵を構成する値K_(n-1)_2を得る。さらに、減算回路１５５Ｂの減算入力端に拡大鍵レジスタ１２１の領域１２１Ｃに格納される値K_n_2を入力し、領域１２１Ｄに格納される値K_n_3を減算回路１５５Ｂの被減算入力端に入力する。減算回路１５５Ｂで、値K_n_1から値K_n_0を減じてｎ－１ラウンド目の拡大鍵を構成する値K_(n-1)_3を得る。

【０１３０】

このように、ｎ－１ラウンド目の拡大鍵を構成する値K_(n-1)_1、値K_(n-1)_2および値K_(n-1)_3については、拡大鍵レジスタ１２１の各領域１２１Ａ～１２１Ｄに格納されるｎラウンド目の拡大鍵の各値K_n_0、値K_n_1、値K_n_2および値K_n_3に対して減算処理および排他的論理和処理を行うことで得ることができる。

【０１３１】

一方、入力端２１２Ａに入力された値K_(n-1)_0は、非線形回路２１０による非線形変換が含まれた演算が行われる。そのため、上述した実施の形態と同様にして、ｎ－１ラウンド目に入力端２１２Ａに入力された値K_(n-1)_0を、この検算用拡大鍵レジスタ１５１に格納する。検算用拡大鍵レジスタ１５１は、値K_(n-1)_0が格納可能なだけの容量、すなわち拡大鍵レジスタ１２１の１／４の容量があればよい。

【０１３２】

ｎラウンド目に、この検算用拡大鍵レジスタ１５１に格納される値K_(n-1)_0と、線形変換回路１５０”の減算回路１５５Ａ、排他的論理和回路１５６および減算回路１５５Ｂそれぞれの出力である値K_(n-1)_1、値K_(n-1)_2および値K_(n-1)_3とをビット結合して、値K_(n-1)であるｎ－ラウンド目の拡大鍵すなわちｎラウンド目の検算用拡大鍵が生成される。

【０１３３】

このように、拡大鍵生成回路１２０”内で行われる線形変換を、排他的論理和以外の手段、例えば加算およびビットシフトを用いて行った場合でも、検算用拡大鍵レジスタの容量を削減することができる。

【０１３４】

なお、図１１の例では、検算用拡大鍵レジスタ１５１を拡大鍵生成回路１２０”の入力端２１２Ａに対して接続しているが、これはこの例に限定されない。例えば、図１０を用いて説明した実施の形態の第１の変形例の如く、非線形変換回路２１０の出力に対して検算用拡大鍵レジスタ１５１を接続する構成とすることも可能である。この場合には、図１０と同様に、検算用拡大鍵レジスタ１５１に格納されるデータと、領域１２１Ａに格納される値K_n_0との排他的論理和を取ることで、出力すべき値K_(n-1)_0を得る。

【０１３５】

本実施の形態の第２の変形例による鍵スケジュール部１４２も、ｎラウンド目の拡大鍵とｎ－１ラウンド目の検算用拡大鍵とを同時に得ることができるため、上述した実施の形態による鍵スケジュール部１４０と同様に、図１に例示される演算装置１００における鍵スケジュール部１０１に代えて適用可能である。勿論、本実施の形態の第２の変形例による鍵スケジュール部１４２は、暗号化処理また復号処理の演算に対する検算を同種処理で行う場合にも、同様に適用することができる。

【０１３６】

＜本実施の形態の第３の変形例＞

次に、本実施の形態の第３の変形例について説明する。上述の実施の形態では、拡大鍵生成回路１２０における線形変換を、排他的論理和回路を用いて行っているが、当該線形変換を、他の演算回路、例えば加算回路、減算回路、ビットシフト回路のうち１を用いて行うことも考えられる。

【０１３７】

線形変換を加算回路により行う場合、図８の拡大鍵生成回路１２０における排他的論理和回路２１１Ａ、２１１Ｂ、２１１Ｃおよび２１１Ｄを、それぞれ加算回路に置き換える。この場合には、線形変換回路１５０における排他的論理和回路１５２Ａ、１５２Ｂおよび１５２Ｃを、それぞれ減算回路に置き換えればよいことになる。

【０１３８】

線形変換を減算回路により行う場合、図８の拡大鍵生成回路１２０における排他的論理和回路２１１Ａ、２１１Ｂ、２１１Ｃおよび２１１Ｄを、それぞれ減算回路に置き換える。この場合には、線形変換回路１５０における排他的論理和回路１５２Ａ、１５２Ｂおよび１５２Ｃを、それぞれ加算回路に置き換えればよいことになる。

【０１３９】

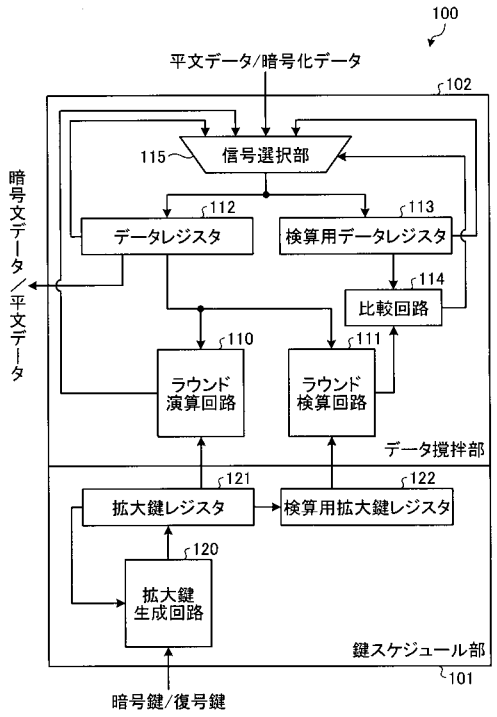
拡大鍵生成回路１２０における線形変換を、ビットシフト回路のみを用いて行うことも可能である。この場合には、線形変換回路１５０では、拡大鍵生成回路１２０で用いられたビットシフト回路と逆向きのビットシフトを行うビットシフト回路を、拡大鍵生成回路１２０のビットシフト回路と対応する位置に設ける。

【符号の説明】

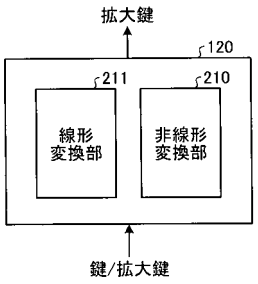
【０１４０】

１００，１００’　演算装置
１０１　鍵スケジュール部
１０２，１０２’　データ撹拌部
１１０　ラウンド演算回路
１１１，１６０　ラウンド検算回路
１１２　データレジスタ
１１３　検算用データレジスタ
１１４，１１４’　比較回路
１１５　信号選択部
１２０　拡大鍵生成回路
１２１　拡大鍵レジスタ
１２２　検算用拡大鍵レジスタ
１５０，１５０’，１５０”　線形変換回路
１５１　検算用拡大鍵レジスタ
１５２Ａ，１５２Ｂ，１５２Ｃ　排他的論理和回路
１７０　鍵出力部
２１０　非線形回路
２１１Ａ，２１１Ｂ，２１１Ｃ，２１１Ｄ　排他的論理和回路
２１２Ａ，２１２Ｂ，２１２Ｃ，２１２Ｄ　入力端

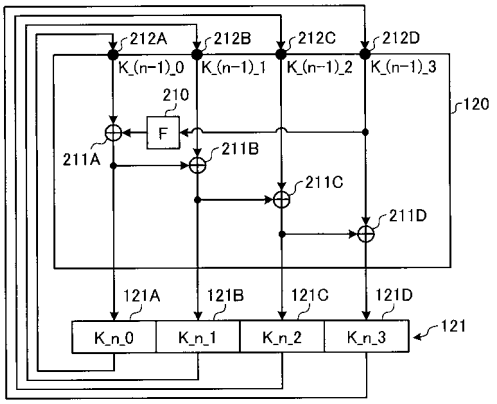
【図１】


100
平文データ/暗号化データ
102
115
信号選択部
112
データレジスタ
113
検算用データレジスタ
114
比較回路
110
ラウンド演算回路
111
ラウンド検算回路
データ撹拌部
121
拡大鍵レジスタ
122
検算用拡大鍵レジスタ
120
拡大鍵生成回路
鍵スケジュール部
101
暗号鍵/復号鍵
暗号文データ/平文データ

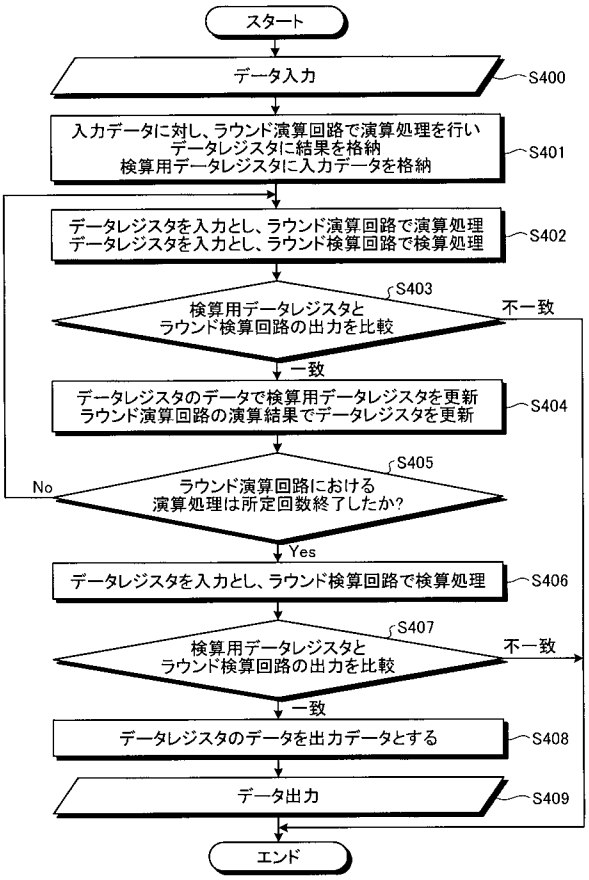
【図２】


拡大鍵
120
211
線形変換部
210
非線形変換部
鍵/拡大鍵

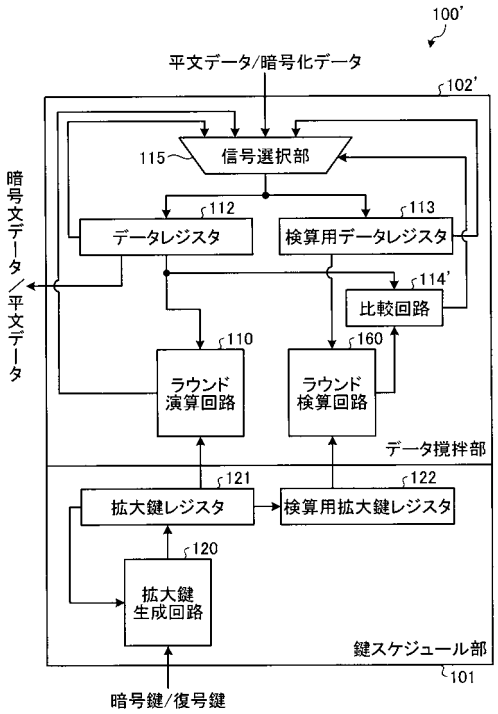
【図３】


212A
212B
212C
212D
K_(n-1)_0
K_(n-1)_1
K_(n-1)_2
K_(n-1)_3
210
F
120
211A
211B
211C
211D
121A
121B
121C
121D
K_n_0
K_n_1
K_n_2
K_n_3
121

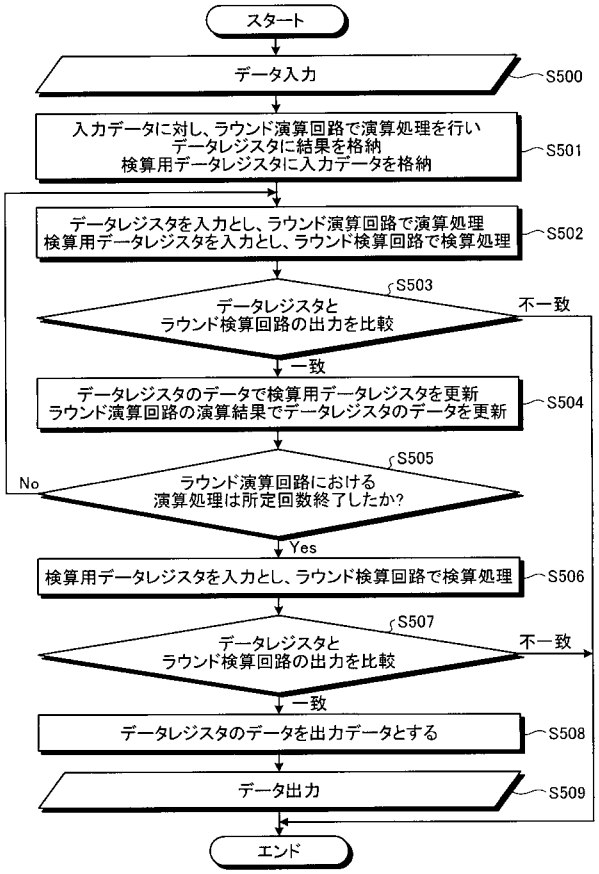
【図４】


スタート
データ入力
S400
入力データに対し、ラウンド演算回路で演算処理を行い
データレジスタに結果を格納
検算用データレジスタに入力データを格納
S401
データレジスタを入力とし、ラウンド演算回路で演算処理
データレジスタを入力とし、ラウンド検算回路で検算処理
S402
S403
検算用データレジスタと
ラウンド検算回路の出力を比較
不一致
一致
データレジスタのデータで検算用データレジスタを更新
ラウンド演算回路の演算結果でデータレジスタを更新
S404
S405
No
ラウンド演算回路における
演算処理は所定回数終了したか?
Yes
データレジスタを入力とし、ラウンド検算回路で検算処理
S406
S407
検算用データレジスタと
ラウンド検算回路の出力を比較
不一致
一致
データレジスタのデータを出力データとする
S408
データ出力
S409
エンド

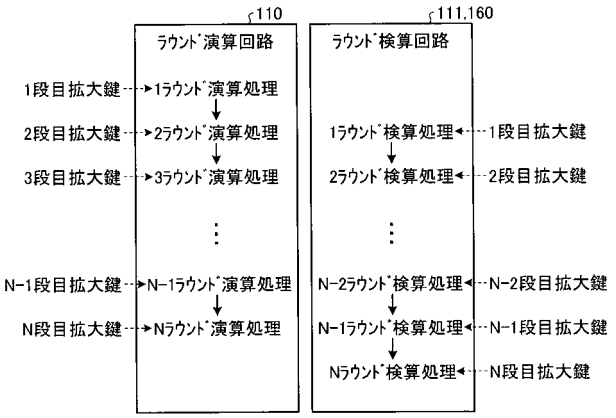
【図５】


100'
平文データ/暗号化データ
102'
115
信号選択部
112
データレジスタ
113
検算用データレジスタ
114'
比較回路
110
ラウンド演算回路
160
ラウンド検算回路
データ撹拌部
121
拡大鍵レジスタ
122
検算用拡大鍵レジスタ
120
拡大鍵生成回路
鍵スケジュール部
101
暗号鍵/復号鍵
暗号文データ/平文データ

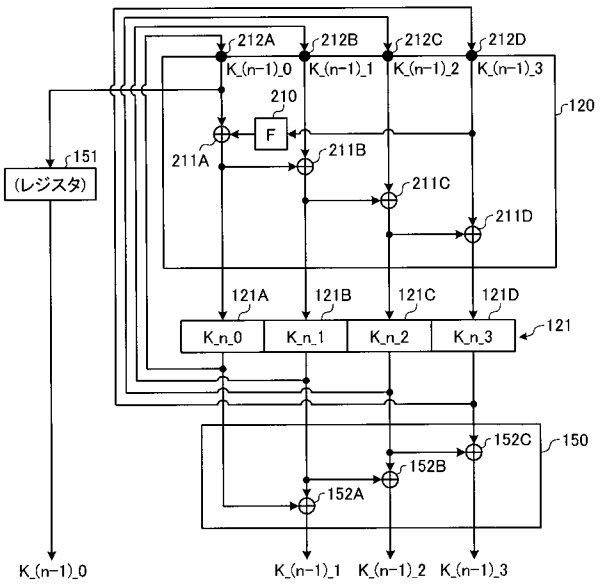
【図６】


スタート
データ入力
S500
入力データに対し、ラウンド演算回路で演算処理を行い
データレジスタに結果を格納
検算用データレジスタに入力データを格納
S501
データレジスタを入力とし、ラウンド演算回路で演算処理
検算用データレジスタを入力とし、ラウンド検算回路で検算処理
S502
S503
データレジスタと
ラウンド検算回路の出力を比較
不一致
一致
データレジスタのデータで検算用データレジスタを更新
ラウンド演算回路の演算結果でデータレジスタのデータを更新
S504
S505
No
ラウンド演算回路における
演算処理は所定回数終了したか?
Yes
検算用データレジスタを入力とし、ラウンド検算回路で検算処理
S506
S507
データレジスタと
ラウンド検算回路の出力を比較
不一致
一致
データレジスタのデータを出力データとする
S508
データ出力
S509
エンド

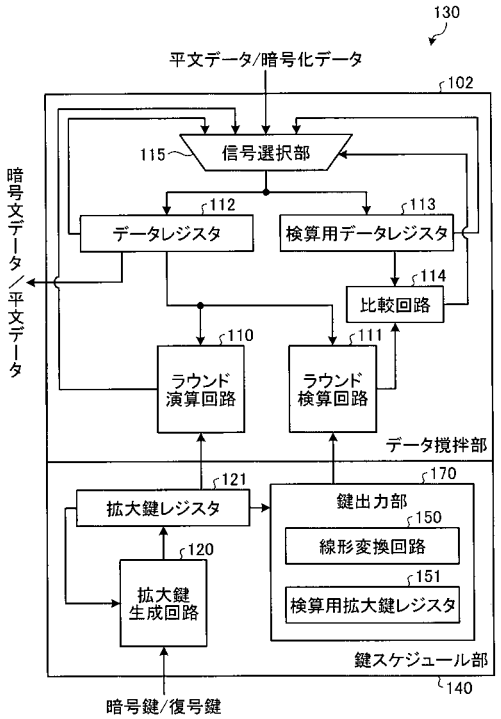
【図７】


110
ラウンド演算回路
111,160
ラウンド検算回路
1段目拡大鍵
1ラウンド演算処理
1ラウンド検算処理
1段目拡大鍵
2段目拡大鍵
2ラウンド演算処理
2ラウンド検算処理
2段目拡大鍵
3段目拡大鍵
3ラウンド演算処理
N-1段目拡大鍵
N-1ラウンド演算処理
N-2ラウンド検算処理
N-2段目拡大鍵
N段目拡大鍵
Nラウンド演算処理
N-1ラウンド検算処理
N-1段目拡大鍵
Nラウンド検算処理
N段目拡大鍵

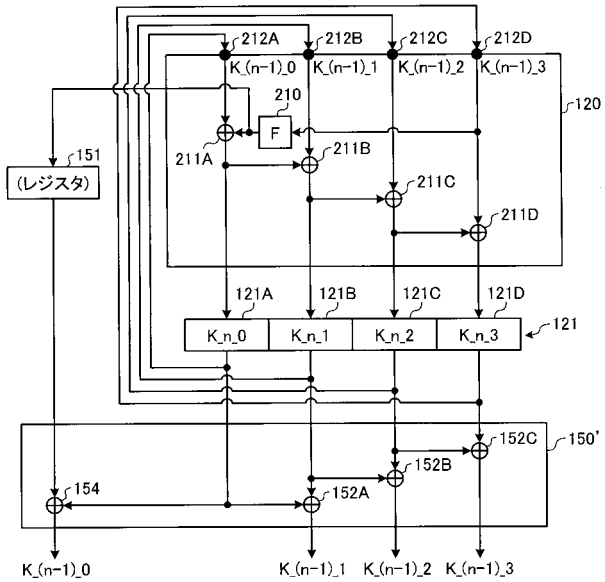
【図８】


212A
212B
212C
212D
K_(n-1)_0
K_(n-1)_1
K_(n-1)_2
K_(n-1)_3
210
F
120
151
(レジスタ)
211A
211B
211C
211D
121A
121B
121C
121D
K_n_0
K_n_1
K_n_2
K_n_3
121
152C
150
152B
152A
K_(n-1)_0
K_(n-1)_1
K_(n-1)_2
K_(n-1)_3

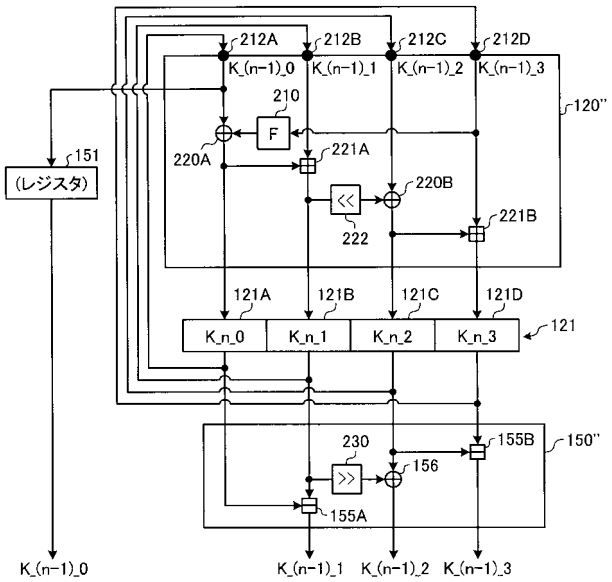
【図９】


130
平文データ/暗号化データ
102
115
信号選択部
112
データレジスタ
113
検算用データレジスタ
暗号文データ/平文データ
114
比較回路
110
ラウンド
演算回路
111
ラウンド
検算回路
データ撹拌部
121
拡大鍵レジスタ
170
鍵出力部
150
線形変換回路
120
拡大鍵
生成回路
151
検算用拡大鍵レジスタ
鍵スケジュール部
140
暗号鍵/復号鍵

【図１０】


212A
212B
212C
212D
K_(n-1)_0
K_(n-1)_1
K_(n-1)_2
K_(n-1)_3
210
F
120
151
(レジスタ)
211A
211B
211C
211D
121A
121B
121C
121D
K_n_0
K_n_1
K_n_2
K_n_3
121
152C
150'
152B
154
152A
K_(n-1)_0
K_(n-1)_1
K_(n-1)_2
K_(n-1)_3

【図１１】


212A
212B
212C
212D
K_(n-1)_0
K_(n-1)_1
K_(n-1)_2
K_(n-1)_3
210
F
120"
151
(レジスタ)
220A
221A
220B
222
221B
121A
121B
121C
121D
K_n_0
K_n_1
K_n_2
K_n_3
121
230
155B
150"
156
155A
K_(n-1)_0
K_(n-1)_1
K_(n-1)_2
K_(n-1)_3

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2009/066536

A. CLASSIFICATION OF SUBJECT MATTER
H04L9/06(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L9/06

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2009
Kokai Jitsuyo Shinan Koho 1971-2009 Toroku Jitsuyo Shinan Koho 1994-2009

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
JSTPlus/JMEDPlus/JST7580(JDreamII)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 8-30195 A (Nippon Telegraph And Telephone Corp.), 02 February 1996 (02.02.1996), paragraphs [0014] to [0018]; fig. 1 (Family: none)	1-5
A	JP 10-154976 A (Toshiba Corp.), 09 June 1998 (09.06.1998), paragraphs [0070] to [0085]; fig. 10 to 12 (Family: none)	1-5
A	JP 2005-503069 A (ST Microelectronics S.A.), 27 January 2005 (27.01.2005), paragraphs [0032] to [0047]; fig. 1, 2 & US 2005/0021990 A1 & EP 1423937 A & WO 2003/024017 A2	1-5

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26 October, 2009 (26.10.09)	02 November, 2009 (02.11.09)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (April 2007)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2009/066536

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2005-522912 A (Oberthur Card Systems S.A.), 28 July 2005 (28.07.2005), paragraphs [0009] to [0030]; fig. 1 to 3 & US 2006/0104438 A1 & EP 1493242 A & WO 2003/085881 A1	1-5

Form PCT/ISA/210 (continuation of second sheet) (April 2007)

国際調査報告	国際出願番号 ＰＣＴ／ＪＰ２００９／０６６５３６

A． 発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl. H04L9/06(2006.01)i

B． 調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl. H04L9/06

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２００９年
日本国実用新案登録公報	１９９６－２００９年
日本国登録実用新案公報	１９９４－２００９年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

JSTPlus/JMEDPlus/JST7580(JDreamII)

C． 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
A	JP 8-30195 A（日本電信電話株式会社）1996.02.02, 段落【００１４】－【００１８】,【図１】（ファミリーなし）	１－５
A	JP 10-154976 A（株式会社東芝）1998.06.09, 段落【００７０】－【００８５】,【図１０】－【図１２】（ファミリーなし）	１－５

☑ Ｃ欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
２６．１０．２００９	０２．１１．２００９

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）	５Ｓ	３１４６
日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	松平 英 電話番号 ０３－３５８１－１１０１ 内線 ３５４６		

様式ＰＣＴ／ＩＳＡ／２１０（第２ページ）（２００７年４月）

国際調査報告	国際出願番号 PCT／JP2009／066536

C（続き）． 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
A	JP 2005-503069 A (エステーミクロエレクトロニクス ソシエテ アノニム) 2005.01.27, 段落【００３２】－【００４７】,【図１】,【図２】 & US 2005/0021990 A1 & EP 1423937 A & WO 2003/024017 A2	１－５
A	JP 2005-522912 A (オベルトゥル カード システムズ ソシエテ アノニム) 2005.07.28, 段落【０００９】－【００３０】,【図１】－【図３】 & US 2006/0104438 A1 & EP 1493242 A & WO 2003/085881 A1	１－５

フロントページの続き

(72)発明者　新保　淳
東京都港区芝浦一丁目１番１号　株式会社東芝内
Ｆターム(参考) 5J104 AA16　AA18　AA32　EA04　JA03　NA37