(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5710460号
(P5710460)
(45)発行日　平成27年4月30日(2015.4.30)　(24)登録日　平成27年3月13日(2015.3.13)

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

請求項の数 4　(全 30 頁)

(21)出願番号　特願2011-275637(P2011-275637)
(22)出願日　平成23年12月16日(2011.12.16)
(65)公開番号　特開2013-126221(P2013-126221A)
(43)公開日　平成25年6月24日(2013.6.24)
審査請求日　平成26年1月29日(2014.1.29)

(73)特許権者　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(74)代理人　100089118
弁理士　酒井　宏明
(74)代理人　100112656
弁理士　宮田　英毅
(72)発明者　駒野　雄一
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　太田　和夫
東京都調布市調布ヶ丘１－５－１　国立大学法人　電気通信大学内

最終頁に続く

(54)【発明の名称】暗号化鍵生成装置およびプログラム

(57)【特許請求の範囲】
【請求項１】
物理的複製困難関数により入力情報を変換して出力情報を出力する変換部と、
前記出力情報の中で複数のインデックス情報がそれぞれ指し示す位置の複数の情報を複数のパターン情報として記憶部に記憶させる記憶制御部と、
複数の前記インデックス情報に基づいて暗号化鍵を生成する生成部と、
前記出力情報と複数の前記パターン情報とをそれぞれ比較して、前記出力情報の中で複数の前記パターン情報と類似する情報が出現する複数の位置を検出する比較部と、
複数の前記パターン情報をマスク処理するマスク処理部と、を備え、
前記記憶制御部は、マスク処理された複数の前記パターン情報を前記記憶部に記憶させ、
前記比較部は、マスク処理された複数の前記パターン情報をマスク処理された前記出力情報と比較する、または、マスク処理された複数の前記パターン情報をマスク処理前の複数の前記パターン情報に復元して前記出力情報と比較することで、前記出力情報の中で複数の前記パターン情報と類似する複数の情報が出現する複数の位置を検出し、
前記生成部は、前記比較部が検出した複数の位置を複数の前記インデックス情報として再現し、再現した複数の前記インデックス情報に基づいて前記暗号化鍵を再現することを特徴とする暗号化鍵生成装置。
【請求項２】
物理的複製困難関数により入力情報を変換して出力情報を出力する変換部と、

前記出力情報を、秘密情報が示す量だけ巡回シフトした情報をパターン情報として記憶部に記憶させる記憶制御部と、
前記秘密情報に基づいて暗号化鍵を生成する生成部と、
前記出力情報を巡回シフトしながら前記パターン情報と比較して、前記出力情報が前記パターン情報と類似するときの巡回シフト量を検出する比較部と、を備え、
前記生成部は、前記比較部が検出した巡回シフト量を前記秘密情報として再現し、再現した前記秘密情報に基づいて前記暗号化鍵を再現することを特徴とする暗号化鍵生成装置。

【請求項３】
コンピュータに、
物理的複製困難関数により入力情報を変換して出力情報を出力する機能と、
前記出力情報の中で複数のインデックス情報がそれぞれ指し示す位置の複数の情報を複数のパターン情報として、各パターン情報をマスク処理する機能と、
マスク処理された複数の前記パターン情報を記憶部に記憶させる機能と、
複数の前記インデックス情報に基づいて暗号化鍵を生成する機能と、
マスク処理された複数の前記パターン情報をマスク処理された前記出力情報と比較する、または、マスク処理された複数の前記パターン情報をマスク処理前の複数の前記パターン情報に復元して前記出力情報と比較することで、前記出力情報の中で複数の前記パターン情報と類似する複数の情報が出現する複数の位置を検出する機能と、
検出した複数の位置を複数の前記インデックス情報として再現し、再現した複数の前記インデックス情報に基づいて前記暗号化鍵を再現する機能と、を実現させることを特徴とするプログラム。

【請求項４】
コンピュータに、
物理的複製困難関数により入力情報を変換して出力情報を出力する機能と、
前記出力情報を、秘密情報が示す量だけ巡回シフトした情報をパターン情報として記憶部に記憶させる機能と、
前記秘密情報に基づいて暗号化鍵を生成する機能と、
前記出力情報を巡回シフトしながら前記パターン情報と比較して、前記出力情報が前記パターン情報と類似するときの巡回シフト量を検出する機能と、
検出した巡回シフト量を前記秘密情報として再現し、再現した前記秘密情報に基づいて前記暗号化鍵を再現する機能と、を実現させることを特徴とするプログラム。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明の実施の形態は、暗号化鍵生成装置およびプログラムに関する。
【背景技術】
【０００２】
暗号プロトコルは、暗号化鍵や認証鍵（以下では、これらを暗号化鍵と総称する。）を利用して、守秘や認証などの機能を実現する。暗号プロトコルは、秘密裏に生成された暗号化鍵を利用する必要がある。暗号化鍵の秘匿性を高める方法として、物理的複製困難関数（ＰＵＦ：Physically Unclonable Function）を利用して暗号化鍵を生成する方法が知られている。
【０００３】
物理的複製困難関数は、同一の入力からデバイス固有の値を出力する関数である。物理的困難関数を利用して生成された暗号化鍵は、外部のデバイスで複製することが困難になるため、鍵生成や認証における要素技術として注目を集めている。物理的複製困難関数を用いて暗号化鍵を生成する場合でも、効率良く暗号化鍵を生成できるようにすることが求められる。
【先行技術文献】

【非特許文献】
【０００４】
【非特許文献１】Zdenek (Sid) Paral and Srinivas Devadas, “Reliable and Efficient PUF-Based Key Generation Using Pattern Matching”, 2011 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST 2011)
【発明の概要】
【発明が解決しようとする課題】
【０００５】
本発明が解決しようとする課題は、物理的複製困難関数を用いて効率良く暗号化鍵を生成することができる暗号化鍵生成装置およびプログラムを提供することである。
【課題を解決するための手段】
【０００６】
実施形態の暗号化鍵生成装置は、変換部と、記憶制御部と、生成部と、比較部と、マスク処理部と、を備える。前記変換部は、物理的複製困難関数により入力情報を変換して出力情報を出力する。前記記憶制御部は、前記出力情報の中で複数のインデックス情報がそれぞれ指し示す位置の複数の情報を複数のパターン情報として記憶部に記憶させる。前記生成部は、複数の前記インデックス情報に基づいて暗号化鍵を生成する。前記比較部は、前記出力情報と複数の前記パターン情報とをそれぞれ比較して、前記出力情報の中で複数の前記パターン情報と類似する情報が出現する複数の位置を検出する。前記マスク処理部は、複数の前記パターン情報をマスク処理する。また、前記記憶制御部は、マスク処理された複数の前記パターン情報を前記記憶部に記憶させ、前記比較部は、マスク処理された複数の前記パターン情報をマスク処理された前記出力情報と比較する、または、マスク処理された複数の前記パターン情報をマスク処理前の複数の前記パターン情報に復元して前記出力情報と比較することで、前記出力情報の中で複数の前記パターン情報と類似する複数の情報が出現する複数の位置を検出し、前記生成部は、前記比較部が検出した複数の位置を複数の前記インデックス情報として再現し、再現した複数の前記インデックス情報に基づいて前記暗号化鍵を再現する。
【図面の簡単な説明】
【０００７】
【図１】第１実施形態の暗号化鍵生成装置の機能ブロック図。
【図２】第１実施形態の暗号化鍵設定の処理の流れを示すフローチャート。
【図３】第１実施形態の暗号化鍵再現の処理の流れを示すフローチャート。
【図４】第１実施例の暗号化鍵生成装置のブロック図。
【図５】第１実施例の暗号化鍵設定の処理の流れを示すフローチャート。
【図６】第１実施例の暗号化鍵再現の処理の流れを示すフローチャート。
【図７】第２実施形態の暗号化鍵生成装置の機能ブロック図。
【図８】第２実施形態の暗号化鍵設定の処理の流れを示すフローチャート。
【図９】第２実施形態の暗号化鍵再現の処理の流れを示すフローチャート。
【図１０】第２実施例の暗号化鍵生成装置のブロック図。
【図１１】第２実施例の暗号化鍵設定の処理の流れを示すフローチャート。
【図１２】第２実施例の暗号化鍵再現の処理の流れを示すフローチャート。
【発明を実施するための形態】
【０００８】
実施形態の暗号化鍵生成装置は、暗号化鍵設定と、暗号化鍵再現の２つの処理を実行する機能を持つ。暗号化鍵設定は、暗号化鍵を最初に生成する処理であり、暗号化鍵再現は、暗号化鍵が必要となるときに、暗号化鍵設定において生成した暗号化鍵を再現する処理である。つまり、オリジナルの暗号化鍵を生成することが暗号化鍵設定であり、オリジナルの暗号化鍵と同じ暗号化鍵を生成することが暗号化鍵再現である。暗号化鍵生成は、暗号化鍵設定と暗号化鍵再現の双方を含む概念である。

【０００９】
（第１実施形態）
＜概要＞
まず、第１実施形態の暗号化鍵生成装置の概要を説明する。第１実施形態の暗号化鍵生成装置は、暗号化鍵設定において、情報の位置を示すインデックス情報を用いて暗号化鍵を生成し、暗号化鍵に用いたインデックス情報が示す位置のＰＵＦの出力をパターン情報として記憶する。また、第１実施形態の暗号化鍵生成装置は、暗号化鍵再現において、記憶したパターン情報と類似するＰＵＦの出力の位置を探索（パターン照合）することで、暗号化鍵設定で暗号化鍵の生成に用いたインデックス情報を再現し、暗号化鍵を再現する。
【００１０】
暗号化鍵の生成に用いるインデックス情報は情報量が小さいため、多くのインデックス情報を組み合わせて一つの暗号化鍵を生成する必要がある。そこで、第１実施形態の暗号化鍵生成装置は、ラウンド処理の繰り返しにより一つの暗号化鍵を生成する。このとき、第１実施形態の暗号化鍵生成装置は、ＰＵＦの出力を効率よく利用してラウンド処理の回数を少なくできるようにするために、一つのラウンドで複数のインデックス情報を扱う。
【００１１】
また、一つのラウンドにおけるＰＵＦの出力の中で複数のインデックス情報が示す位置の複数のパターン情報をそのまま記憶すると、情報に重なりが生じてインデックス情報の相互関係が推測される虞がある。そこで、第１実施形態の暗号化鍵生成装置では、マスク生成関数（ＭＧＦ：Mask Generation Function）を利用して、記憶するパターン情報ごとに異なるデータ（マスク情報）を加算することで、暗号化鍵の生成に用いたインデックス情報の秘匿性を高める。
【００１２】
＜構成＞
次に、図１を参照して、第１実施形態の暗号化鍵生成装置の概略構成を説明する。図１は、第１実施形態の暗号化鍵生成装置１００の機能的な構成を示す機能ブロック図である。
【００１３】
図１に示すように、本実施形態の暗号化鍵生成装置１００は、通信部１０１、記憶部１０２、ＰＵＦ入力生成部１０３、ＰＵＦ１０４、ＰＵＦ出力一時記憶部１０５、インデックス情報生成部１０６、ＭＧＦ１０７、マスク処理部１０８、比較部１０９、および鍵生成部１１０を備える。
【００１４】
通信部１０１は、暗号化鍵生成装置１００と外部システムとの間の通信を行うインターフェースである。
【００１５】
記憶部１０２は、暗号化鍵設定において、マスク処理部１０８が生成する後述の変形パターン情報を記憶するメモリである。記憶部１０２は、例えば、ＲＡＭ、ＥＥＰＲＯＭ（登録商標）などで構成される。なお、記憶部１０２は、暗号化鍵生成装置１００の外部にあってもよい。記憶部１０２が暗号化鍵生成装置１００の外部にある場合、暗号化鍵生成装置１００の各部は、記憶部１０２に対するデータの書き込みや読み出しを、通信部１０１を介して行う。
【００１６】
ＰＵＦ入力生成部１０３は、予め定められた初期値Ｉ＿｛０，１｝あるいはインデックス情報生成部１０６が出力するインデックス情報Ｉ＿｛ｒ，ｊ｝に基づき、ＰＵＦ１０４へ入力するＰＵＦ入力情報を生成する。例えば、ＰＵＦ入力生成部１０３は、ＰＵＦ入力情報が所定の長さとなるように、初期値Ｉ＿｛０，１｝あるいはインデックス情報Ｉ＿｛ｒ，ｊ｝に対して予め定められたデータを連結して、ＰＵＦ入力情報を生成する。また、ＰＵＦ入力生成部１０３は、初期値Ｉ＿｛０，１｝あるいはインデックス情報Ｉ＿｛ｒ，

ｊ｝をハッシュ関数などに入力して、ＰＵＦ入力情報を生成するようにしてもよい。また、ＰＵＦ入力生成部１０３に入力される情報が複数ある場合には、ＰＵＦ入力生成部１０３は、それら入力情報を連結したり、ビット演算あるいは算術演算することで、ＰＵＦ入力情報を生成するようにしてもよい。ＰＵＦ入力生成部１０３は、初期値Ｉ＿｛０，１｝あるいはインデックス情報Ｉ＿｛ｒ，ｊ｝に加えて、後述するラウンド番号ｒ、ＰＵＦ１０４が出力するビットの番号ｃｎ、あるいは回路動作時のクロックサイクル番号（記載は省略する。）などを入力してもよい。

【００１７】

ＰＵＦ１０４は、物理的複製困難関数である。物理的複製困難関数は、あるデバイスに搭載されると、同一の入力からそのデバイス固有の値を出力する関数である。非特許文献１において開示される暗号化鍵生成装置は、複数のＰＵＦの出力を排他的論理和演算して得られる値を利用する。以降の説明では、ＰＵＦ１０４は、このような複数のＰＵＦとそれらの出力を排他的論理和演算して値を出力する回路や、複数のＰＵＦとそれら出力をビット演算あるいは算術演算して値を出力する回路を用いてもよい。ＰＵＦ１０４は、各ラウンドにおいて、ＰＵＦ入力生成部１０３が生成したＰＵＦ入力情報を入力し、Ｌ＋Ｗ－１ビットのＰＵＦ出力情報を出力する。

【００１８】

ＰＵＦ出力一時記憶部１０５は、各ラウンドにおいてＰＵＦ１０４が出力するＰＵＦ出力情報を一時的に記憶する。本実施形態の暗号化鍵生成装置１００は、各ラウンドにおいて、Ｌ＋Ｗ－１ビットのＰＵＦ出力情報のうちＷビットのデータをパターン情報として利用する。本実施形態においては、ＰＵＦ出力一時記憶部１０５は、例えば、Ｌ＋Ｗ－１ビットのレジスタで構成される。このとき、ＰＵＦ出力一時記憶部１０５は、当該ラウンドでＰＵＦ１０４が出力するＬ＋Ｗ－１ビットのＰＵＦ出力情報を保持し、後述するマスク処理部１０８は、ＰＵＦ出力一時記憶部１０５が記憶するＬ＋Ｗ－１ビットのＰＵＦ出力情報のうち、Ｗビットのデータを利用する。あるいは、後述する第１実施例のように、ＰＵＦ出力一時記憶部１０５は、Ｗビットのシフトレジスタで構成され、ＰＵＦ１０４が１ビット出力するごとに、記憶する中で最も古い１ビットを破棄する構成であってもよい。

【００１９】

インデックス情報生成部１０６は、各ラウンドにおいて、１からＬの間で、Ｎ＿ｒ個（１≦Ｎ＿ｒ、ｒはラウンド番号）のインデックス情報Ｉ＿｛ｒ，１｝，．．．，Ｉ＿｛ｒ，Ｎ＿ｒ｝を生成する。各インデックス情報Ｉ＿｛ｒ，ｊ｝（１≦ｊ≦Ｎ＿ｒ）は、１からＬの間でランダムに選ばれてもよいし、任意のｊとｋについて、インデックス情報Ｉ＿｛ｒ，ｊ｝とインデックス情報Ｉ＿｛ｒ，ｋ｝とがＷ以上離れるように選ばれてもよい。また、各インデックス情報Ｉ＿｛ｒ，ｊ｝は、通信部１０１により暗号化鍵生成装置１００の外部から受け付けるなどして、予め定められた値を用いてもよい。各インデックス情報Ｉ＿｛ｒ，ｊ｝を外部から受け付ける場合には、暗号化鍵生成装置１００はインデックス情報生成部１０６を備えていなくてもよい。インデックス情報Ｉ＿｛ｒ，ｊ｝は、ＰＵＦ出力情報の中のパターン情報の位置を指し示す情報である。本実施形態では、インデックス情報Ｉ＿｛ｒ，ｊ｝がＰＵＦ出力情報の中のパターン情報の先頭位置を指し示すものとして説明するが、パターン情報の先頭位置に限らず、予め定めた所定の位置を指し示すものであってもよい。

【００２０】

ＭＧＦ１０７は、予め定められた初期値Ｉ＿｛０，１｝あるいはインデックス情報生成部１０６が出力するインデックス情報Ｉ＿｛ｒ，ｊ｝に基づき、パターン情報に対して加算するマスク情報を生成するマスク生成関数（Mask Generation Function）である。本実施形態にかかる暗号化鍵生成装置１００は、各ラウンドにおいて、Ｎ＿ｒ個のマスク情報Ｍ＿｛ｒ，１｝，．．．，Ｍ＿｛ｒ，Ｎ＿ｒ｝を利用する。ハードウェア実装において複数のマスク情報を並行して生成するためには、暗号化鍵生成装置１００の中に複数のＭＧＦ１０７が存在してもよい（図１では一つのＭＦＧ１０７のみを図示している。）。あるいは、一つのＭＧＦ１０７をＮ＿ｒ回利用して、Ｎ＿ｒ個のマスク情報Ｍ＿｛ｒ，１｝

，．．．，Ｍ＿｛ｒ，Ｎ＿ｒ｝を生成してもよい。また、ＭＧＦ１０７は、ＰＵＦ入力生成部１０３と一部あるいはすべて同一の処理を行うものであってもよい。ＭＧＦ１０７がＰＵＦ入力生成部１０３と同一の処理を行う場合、ＰＵＦ入力生成部１０３とＭＧＦ１０７は、同一の処理を行う部分について、単一の装置を用いた構成であってもよい（すべて同一の処理である場合には、ＰＵＦ入力生成部１０３とＭＧＦ１０７を単一の装置で構成できる。）。ＭＧＦ１０７は、初期値Ｉ＿｛０，１｝あるいはインデックス情報Ｉ＿｛ｒ，ｊ｝に加えて、ラウンド番号ｒや１からＮ＿ｒの間の番号などを入力してもよい。

【００２１】

マスク処理部１０８は、ＰＵＦ出力一時記憶部１０５が記憶するＬ＋Ｗ－１ビットのＰＵＦ出力情報の出力のうち、インデックス情報Ｉ＿｛ｒ，ｊ｝で示される位置からＷビットのデータであるパターン情報Ｙ＿｛ｒ，ｊ｝に対して、ＭＧＦ１０７が生成するマスク情報Ｍ＿｛ｒ，ｊ｝を加算して、変形パターン情報Ｚ＿｛ｒ，ｊ｝を生成する。例えば、マスク情報Ｍ＿｛ｒ，ｊ｝がＷビットの場合には、マスク処理部１０８は、パターン情報Ｙ＿｛ｒ，ｊ｝とマスク情報Ｍ＿｛ｒ，ｊ｝との排他的論理和により、変形パターン情報Ｚ＿｛ｒ，ｊ｝を生成することができる。また、マスク処理部１０８は、パターン情報Ｙ＿｛ｒ，ｊ｝とマスク情報Ｍ＿｛ｒ，ｊ｝とから、予め定められた規則に従って変形パターン情報Ｚ＿｛ｒ，ｊ｝を生成するようにしてもよい。ハードウェア実装において複数のマスク処理を並行して実行するためには、暗号化鍵生成装置１００の中に複数のマスク処理部１０８が存在してもよい（図１では一つのマスク処理部１０８のみを図示している。）。あるいは、一つのマスク処理部１０８をＮ＿ｒ回利用して、Ｎ＿ｒ個の変形パターン情報Ｚ＿｛ｒ，１｝，．．．，Ｚ＿｛ｒ，Ｎ＿ｒ｝を生成してもよい。

【００２２】

比較部１０９は、暗号化鍵再現において、ＰＵＦ出力一時記憶部１０５が記憶するＰＵＦ出力情報のうちのＷビットのデータに対してＭＧＦ１０７が生成するマスク情報Ｍ＿｛ｒ，ｊ｝を加算したデータ（以下、参照情報という。）と、記憶部１０２が記憶する変形パターン情報Ｚ＿｛ｒ，ｊ｝とが、類似のデータであるか否かを判定する。類似のデータであるか否かの判定は、例えば、比較対象となる二つのデータのハミング距離（異なるビットの数）が予め定められた閾値Ｔ以下であるか否かで判定する。あるいは、二つのデータが所定の長さの同一の部分系列を含むか否かで判定するなど、別の方法で判定してもよい。ハードウェア実装において複数の判定処理を並行して実行するためには、暗号化鍵生成装置１００の中に複数の比較部１０９が存在してもよい（図１では一つの比較部１０９のみを図示している。）。あるいは、一つの比較部１０９をＮ＿ｒ回利用して、それぞれの判定処理を行ってもよい。

【００２３】

鍵生成部１１０は、Ｎ＿１＋．．．＋Ｎ＿Ｒ個のインデックス情報の集合｛Ｉ＿｛ｒ，ｊ｝｝＿｛ｒ，ｊ｝を用いて、暗号化鍵を生成する。例えば、鍵生成部１１０は、集合｛Ｉ＿｛ｒ，ｊ｝｝＿｛ｒ，ｊ｝に含まれるインデックス情報Ｉ＿｛ｒ，ｊ｝をすべて連結して暗号化鍵を生成するようにしてもよいし、集合｛Ｉ＿｛ｒ，ｊ｝｝＿｛ｒ，ｊ｝に含まれるインデックス情報Ｉ＿｛ｒ，ｊ｝をビット演算あるいは算術演算して暗号化鍵を生成するようにしてもよい。

【００２４】

ここで、本実施形態で用いる定数を表す記号について説明する。Ｌは、インデックス情報生成部１０６が生成するインデックス情報Ｉ＿｛ｒ，ｊ｝の最大値を表す。Ｗは、ＰＵＦ１０４が出力するＰＵＦ出力情報のうち、パターン情報Ｙ＿｛ｒ，ｊ｝として利用するデータのビット長を表す。Ｎ＿ｒは、第ｒラウンドにおいて、インデックス情報生成部１０６が生成するインデックス情報Ｉ＿｛ｒ，ｊ｝の個数を表す。Ｎ＿ｒはラウンドごとに異なっていてもよいし、同一でもよい。Ｒは、暗号化鍵生成および暗号化鍵再現において実行されるラウンドの総数を表す。Ｉ＿｛０，１｝は、ＰＵＦ入力生成部１０３に入力するデータの初期値を表す。

【００２５】

本実施形態の暗号化鍵生成装置１００は、例えば、ＣＰＵなどの演算装置、ＲＯＭやＲＡＭなどの記憶装置、ＨＤＤ、ＣＤドライブ装置などの外部記憶装置、通信装置などを備えた、通常のコンピュータを利用したハードウェア構成を採用することができる。そして、コンピュータによって実行されるプログラムにより、上記のハードウェア資源を利用して、通信部１０１、記憶部１０２、ＰＵＦ入力生成部１０３、ＰＵＦ１０４、ＰＵＦ出力一時記憶部１０５、インデックス情報生成部１０６、ＭＧＦ１０７、マスク処理部１０８、比較部１０９、および鍵生成部１１０の各機能構成を実現することができる。

【００２６】

＜暗号化鍵設定＞

次に、図２を参照して、第１実施形態の暗号化鍵生成装置１００が実行する暗号化鍵設定の処理について説明する。図２は、暗号化鍵生成装置１００による暗号化鍵設定の一連の処理の流れを示すフローチャートである。

【００２７】

図２のフローチャートで示す暗号化鍵設定の処理は、暗号化鍵生成装置１００が暗号化鍵設定開始の命令を受け付けることで開始される。暗号化鍵生成装置１００は、暗号化鍵設定開始の命令を受け付けると、ラウンド番号ｒを１で初期化し、ｒ＝１，．．．，Ｒに対して、以下の処理をそれぞれ実行する。

【００２８】

インデックス情報生成部１０６は、Ｎ＿ｒ個のインデックス情報Ｉ＿｛ｒ，１｝，．．．，Ｉ＿｛ｒ，Ｎ＿ｒ｝を生成する（ステップＳ１０１）。ステップＳ１０１の処理は、後述するステップＳ１０４において、ＰＵＦ出力一時記憶部１０５が、ＰＵＦ１０４が出力する第ｒラウンドにおけるＰＵＦ出力情報のＷ－１ビット目を記憶するまでに行われていればよく、例えば、第ｒラウンドの処理が開始される前に行われていてもよい。

【００２９】

ＰＵＦ入力生成部１０３は、予め定められた初期値あるいはステップＳ１０１でインデックス情報生成部１０６が生成したインデックス情報｛Ｉ＿｛ｉ，ｊ｝｝＿｛０≦ｉ＜ｒ，１≦ｊ≦Ｎ＿ｒ｝を入力として、ＰＵＦ１０４が第ｒラウンドのｃｎビット目を出力するためのＰＵＦ入力情報Ｘ＿｛ｒ，ｃｎ｝を生成する（ステップＳ１０２）。ステップＳ１０２の処理は、後述するステップＳ１０４において、ＰＵＦ入力情報Ｘ＿｛ｒ，ｃｎ｝がＰＵＦ１０４に入力されるまでに行われていればよく、例えば、第ｒラウンドの処理が開始される前に行われていてもよい。

【００３０】

ＭＧＦ１０７は、ｊ＝１，．．．，Ｎ＿ｒについて、予め定められた初期値あるいはステップＳ１０１でインデックス情報生成部１０６が生成したインデックス情報｛Ｉ＿｛ｉ，ｊ｝｝＿｛０≦ｉ≦ｒ，１≦ｊ≦Ｎ＿ｒ｝とｒとｊを入力として、マスク情報Ｍ＿｛ｒ，ｊ｝を生成する（ステップＳ１０３）。ステップＳ１０３の処理は、後述するステップＳ１０５において、マスク処理部１０８が変形パターン情報を生成するまでに行われていればよく、例えば、第ｒラウンドの処理が開始される前に行われていてもよい。

【００３１】

ＰＵＦ出力一時記憶部１０５は、ステップＳ１０２でＰＵＦ入力生成部１０３が生成したＰＵＦ入力情報Ｘ＿｛ｒ，ｃｎ｝を入力としてＰＵＦ１０４が出力するＬ＋Ｗ－１ビットのＰＵＦ出力情報を記憶する（ステップＳ１０４）。

【００３２】

ＰＵＦ出力一時記憶部１０５がＰＵＦ出力情報を記憶すると、暗号化鍵生成装置１００は、ｊ＝１，．．．，Ｎ＿ｒについて、ＰＵＦ出力一時記憶部１０５が記憶する第ｒラウンドにおけるＰＵＦ出力情報の第Ｉ＿｛ｒ，ｊ｝ビット目から第Ｉ＿｛ｒ，ｊ｝＋Ｗ－１ビット目に対して、以下のステップＳ１０５～ステップＳ１０７の処理を繰り返し実行する。

【００３３】

ＰＵＦ出力一時記憶部１０５が第ｒラウンドにおけるＰＵＦ出力情報の第Ｉ＿｛ｒ，ｊ

}ビット目から第Ｉ＿{ｒ，ｊ}＋Ｗ－１ビット目を記憶していると仮定する（ｊとは異なるｊ’でＩ＿{ｒ，ｊ}＝Ｉ＿{ｒ，ｊ’}となることがあってもよい）。マスク処理部１０８は、例えば、ステップＳ１０４でＰＵＦ出力一時記憶部１０５が記憶したＰＵＦ出力情報のうちのＷビットのデータと、ステップＳ１０３でＭＧＦ１０７が生成したマスク情報Ｍ＿{ｒ，ｊ}との排他的論理和により、変形パターン情報Ｚ＿{ｒ，ｊ}を生成する（ステップＳ１０５）。

【００３４】

記憶部１０２は、ステップＳ１０５でマスク処理部１０８が生成した変形パターン情報Ｚ＿{ｒ，ｊ}を記憶する（ステップＳ１０６）。

【００３５】

記憶部１０２に変形パターン情報Ｚ＿{ｒ，ｊ}が記憶されると、暗号化鍵生成装置１００は、ｊ＜Ｎ＿ｒであるか否かを判定する（ステップＳ１０７）。ここで、ｊ＜Ｎ＿ｒであるならば（ステップＳ１０７：Ｙｅｓ）、暗号化鍵生成装置１００は、ｊをｊ＋１に置き換えて、ステップＳ１０５に戻って以降の処理を繰り返す。一方、ｊ＝Ｎ＿ｒであるならば（ステップＳ１０７：Ｎｏ）、暗号化鍵生成装置１００は、ｒ＜Ｒであるか否かを判定する（ステップＳ１０８）。ここで、ｒ＜Ｒであるならば（ステップＳ１０８：Ｙｅｓ）、暗号化鍵生成装置１００は、ｒをｒ＋１に置き換えて、ステップＳ１０１に戻って以降の処理を繰り返す。一方、ｒ＝Ｒであるならば（ステップＳ１０８：Ｎｏ）、ステップＳ１０９に進む。

【００３６】

鍵生成部１１０は、例えば、各ラウンドにおいてインデックス情報生成部１０６が生成したＮ＿１＋．．．＋Ｎ＿Ｒ個のインデックス情報からなる集合{Ｉ＿{ｉ，ｊ}}＿{０≦ｉ≦Ｒ，１≦ｊ≦Ｎ＿ｉ}に含まれる各インデックス情報Ｉ＿{ｉ，ｊ}を連結して、暗号化鍵を生成する（ステップＳ１０９）。

【００３７】

＜暗号化鍵再現＞

次に、図３を参照して、第１実施形態の暗号化鍵生成装置１００が実行する暗号化鍵再現の処理について説明する。暗号化鍵再現の処理は、上述の暗号化鍵設定の処理が終わった後、暗号プロトコルが暗号化鍵を必要とするときに実行される。図３は、暗号化鍵生成装置１００による暗号化鍵再現の一連の処理の流れを示すフローチャートである。

【００３８】

図３のフローチャートで示す暗号化鍵再現の処理は、暗号化鍵生成装置１００が暗号化鍵再現開始の命令を受け付けることで開始される。暗号化鍵生成装置１００は、暗号化鍵再現開始の命令を受け付けると、ラウンド番号ｒを１で初期化し、ｒ＝１，．．．，Ｒに対して、以下の処理をそれぞれ実行する。

【００３９】

ＰＵＦ入力生成部１０３は、予め定められた初期値あるいは前回のラウンド処理で再現されたインデックス情報{Ｉ＿{ｉ，ｊ}}＿{０≦ｉ＜ｒ，１≦ｊ≦Ｎ＿ｒ}を入力として、ＰＵＦ１０４が第ｒラウンドのｃｎビット目を出力するためのＰＵＦ入力情報Ｘ＿{ｒ，ｃｎ}を生成する（ステップＳ２０１）。ステップＳ２０１の処理は、後述するステップＳ２０３において、ＰＵＦ入力情報Ｘ＿{ｒ，ｃｎ}がＰＵＦ１０４に入力されるまでに行われていればよく、例えば、第ｒラウンドの処理が開始される前に行われていてもよい。

【００４０】

ＭＧＦ１０７は、ｊ＝１，．．．，Ｎ＿ｒについて、予め定められた初期値あるいは前回のラウンド処理で再現されたインデックス情報{Ｉ＿{ｉ，ｊ}}＿{０≦ｉ≦ｒ，１≦ｊ≦Ｎ＿ｒ}とｒとｊを入力として、マスク情報Ｍ＿{ｒ，ｊ}を生成する（ステップＳ２０２）。ステップＳ２０２の処理は、後述するステップＳ２０４において、マスク処理部１０８がパターン照合の対象となる参照情報を生成するまでに行われていればよく、例えば、第ｒラウンドの処理が開始される前に行われていてもよい。

【００４１】
ＰＵＦ出力一時記憶部１０５は、ステップＳ２０１でＰＵＦ入力生成部１０３が生成したＰＵＦ入力情報Ｘ＿｛ｒ，ｃｎ｝を入力としてＰＵＦ１０４が出力するＰＵＦ出力情報を記憶する（ステップＳ２０３）。
【００４２】
ＰＵＦ出力一時記憶部１０５がＰＵＦ出力情報を記憶すると、暗号化鍵生成装置１００は、ｋ＝１，．．．，Ｌについて、ＰＵＦ出力一時記憶部１０５が記憶する第ｋビット目から第ｋ＋Ｗ－１ビット目に対して、以下のステップＳ２０４～ステップＳ２０８の処理を繰り返し実行する。また、暗号化鍵生成装置１００は、ｊ＝１，．．．，Ｎ＿ｒについて、以下のステップＳ２０４～ステップＳ２０７の処理を繰り返し実行する。
【００４３】
マスク処理部１０８は、例えば、ＰＵＦ出力一時記憶部１０５が記憶する第ｒラウンドにおけるＰＵＦ出力情報の第ｋビット目から第ｋ＋Ｗ－１ビット目までのＷビットのデータと、ステップＳ２０２でＭＧＦ１０７が生成したマスク情報Ｍ＿｛ｒ，ｊ｝との排他的論理和により、参照情報を生成する（ステップＳ２０４）。
【００４４】
比較部１０９は、ステップＳ２０４でマスク処理部１０８が生成した参照情報と、記憶部１０２が記憶する変形パターン情報Ｚ＿｛ｒ，ｊ｝とが類似データであるか否かを判定する（ステップＳ２０５）。なお、ここでは、ＰＵＦ出力情報のＷビットのデータにマスク情報を加算した参照情報と、記憶部１０２が記憶する変形パターン情報とを比較して、これら二つのデータが類似データであるか否かを判定しているが、記憶部１０２が記憶する変形パターン情報にマスク情報を加算してパターン情報を再現し、マスク情報を加算しないＰＵＦ出力情報のＷビットのデータと、再現したパターン情報とを比較して、これら二つのデータが類似のデータであるか否かを判定するようにしてもよい。
【００４５】
比較部１０９が二つのデータを類似データであると判定した場合（ステップＳ２０５：Ｙｅｓ）、暗号化鍵生成装置１００は、Ｉ＿｛ｒ，ｊ｝＝ｋとしてインデックス情報Ｉ＿｛ｒ，ｊ｝を再現する（ステップＳ２０６）。つまり、記憶部１０２が記憶する変形パターン情報Ｚ＿｛ｒ，ｊ｝に類似すると判定された参照情報のＰＵＦ出力情報における開始位置ｋを、インデックス情報Ｉ＿｛ｒ，ｊ｝として再現する。なお、同一のｋにおいて、複数のｊ，ｊ’について、Ｉ＿｛ｒ，ｊ｝＝Ｉ＿｛ｒ，ｊ’｝＝ｋとして、複数のインデックス情報が再現されるようにしてもよい。比較部１０９が二つのデータを類似データではない判定した場合には（ステップＳ２０５：Ｎｏ）、ステップＳ２０６の処理はスキップする。
【００４６】
その後、暗号化鍵生成装置１００は、ｊ＜Ｎ＿ｒであるか否かを判定する（ステップＳ２０７）。ここで、ｊ＜Ｎ＿ｒであるならば（ステップＳ２０７：Ｙｅｓ）、暗号化鍵生成装置１００は、ｊをｊ＋１に置き換えて、ステップＳ２０４に戻って以降の処理を繰り返す。一方、ｊ＝Ｎ＿ｒであるならば（ステップＳ２０７：Ｎｏ）、暗号化鍵生成装置１００は、ｋ＜Ｌであるか否かを判定する（ステップＳ２０８）。ここで、ｋ＜Ｌであるならば（ステップＳ２０８：Ｙｅｓ）、ｋをｋ＋１に置き換えて、ステップＳ２０４に戻って以降の処理を繰り返す。なお、ｋ＝１，．．．，Ｌについて、ステップＳ２０４～ステップＳ２０８の処理を繰り返しても再現できないインデックス情報Ｉ＿｛ｒ，ｊ｝が存在する場合には、暗号化鍵生成装置１００は、処理を停止するようにしてもよいし、再現できないインデックス情報Ｉ＿｛ｒ，ｊ｝に予め定められた値あるいはランダムな値を設定してもよい。
【００４７】
ステップＳ２０８の判定の結果がｋ＝Ｌであるならば（ステップＳ２０８：Ｎｏ）、暗号化鍵生成装置１００は、ｒ＜Ｒであるか否かを判定する（ステップＳ２０９）。ここで、ｒ＜Ｒであるならば（ステップＳ２０９：Ｙｅｓ）、暗号化鍵生成装置１００は、ｒを

ｒ＋１に置き換えて、ステップＳ２０１に戻って以降の処理を繰り返す。一方、ｒ＝Ｒであるならば（ステップＳ２０９：Ｎｏ）、ステップＳ２１０に進む。

【００４８】

鍵生成部１１０は、例えば、各ラウンドにおいて再現したＮ＿１＋．．．＋Ｎ＿Ｒ個のインデックス情報｛Ｉ＿｛ｉ，ｊ｝｝＿｛０≦ｉ≦Ｒ，１≦ｊ≦Ｎ＿ｉ｝を連結して、暗号化鍵を生成する（ステップＳ２１０）。なお、鍵生成部１１０は、インデックス情報｛Ｉ＿｛ｉ，ｊ｝｝＿｛０≦ｉ≦Ｒ，１≦ｊ≦Ｎ＿ｉ｝の代わりに、ＰＵＦ入力情報｛Ｘ＿｛ｒ，ｃｎ｝｝＿｛１≦ｒ≦Ｒ｝を連結して暗号化鍵を生成してもよい。あるいは、鍵生成部１１０は、インデックス情報｛Ｉ＿｛ｉ，ｊ｝｝＿｛０≦ｉ≦Ｒ，１≦ｊ≦Ｎ＿ｉ｝に加えて、ＰＵＦ入力情報｛Ｘ＿｛ｒ，ｃｎ｝｝＿｛１≦ｒ≦Ｒ｝を連結して暗号化鍵を生成してもよい。また、鍵生成部１１０は、連結した値を暗号化鍵として用いてもよいし、連結した値をハッシュ関数などに入力し、得られた値を暗号化鍵として用いてもよい。

【００４９】

なお、本実施形態の暗号化鍵生成装置１００は、暗号化鍵の生成に用いたインデックス情報の秘匿性を高めるために、ＰＵＦ出力情報のうちのインデックス情報が指し示す位置からＷ－１ビットのデータであるパターン情報に対してマスク情報を加算して変形パターン情報を生成し、この変形パターン情報を記憶部１０２に記憶するようにしている。しかし、処理の高速化を優先する場合には、暗号化鍵生成装置１００は、パターン情報そのものを記憶部１０２に記憶するようにしてもよい。この場合、暗号化鍵生成装置１００は、ＭＧＦ１０７およびマスク処理部１０８を備えない構成となる。また、暗号化鍵設定の処理では、図２に示したフローチャートのステップＳ１０３およびステップＳ１０５の処理を実施せず、ステップＳ１０６において、ＰＵＦ出力一時記憶部１０５が記憶している第ｒラウンドにおけるＰＵＦ出力情報の第Ｉ＿｛ｒ，ｊ｝ビット目から第Ｉ＿｛ｒ，ｊ｝＋Ｗ－１ビット目までのＷビットのデータを、パターン情報として記憶部１０２に記憶する。そして、暗号化鍵再現の処理では、図３に示したフローチャートのステップＳ２０２およびステップＳ２０４の処理を実施せず、ステップＳ２０５において、比較部１０９が、ＰＵＦ出力一時記憶部１０５が記憶している第ｒラウンドにおけるＰＵＦ出力情報の第ｋビット目から第ｋ＋Ｗ－１ビット目までのＷビットのデータと、記憶部１０２が記憶するパターン情報とが類似データであるか否かを判定する。

【００５０】

また、本実施形態の暗号化鍵生成装置１００では、ＰＵＦ入力生成部１０３が、インデックス情報Ｉ＿｛ｒ，ｊ｝に基づいて、ＰＵＦ１０４に入力するＰＵＦ入力情報Ｘ＿｛ｒ，ｃｎ｝を生成するようにしている。しかし、ＰＵＦ入力生成部１０３は、例えばＰＵＦ１０４への起動信号など、インデックス情報Ｉ＿｛ｒ，ｊ｝に依存しない固定値を、ＰＵＦ入力情報として生成するようにしてもよい。

【００５１】

また、本実施形態の暗号化鍵生成装置１００では、ＰＵＦ１０４が、各ラウンドにおいてＬ＋Ｗ－１ビットのＰＵＦ出力情報を出力するようにしている。しかし、ＰＵＦ１０４がＬ＋Ｗ－１ビットを超えるＰＵＦ出力情報を出力し、各ラウンドでそのＰＵＦ出力情報の一部を利用する構成であってもよい。例えば、ＰＵＦ１０４に対して固定値のＰＵＦ入力情報が入力され、ＰＵＦ１０４がＲ×（Ｌ＋Ｗ－１）ビットのＰＵＦ出力情報を出力するようにしてもよい。この場合には、第ｉラウンドでは、ＰＵＦ出力一時記憶部１０５がＰＵＦ出力情報のうち（ｉ－１）×（Ｌ＋Ｗ）ビット目からＬ＋Ｗ－１ビットのデータを記憶し、以降の処理を実施する構成とすることができる。

【００５２】

＜実施形態の効果＞

第１実施形態の効果を説明するにあたり、まず、非特許文献１が開示する暗号化鍵の生成方法を概説する。非特許文献１が開示する暗号化鍵の生成方法では、一つのラウンドにおいて一つのインデックス情報のみを扱う。すなわち、非特許文献１が開示する暗号化鍵の生成方法では、暗号化鍵設定において、第ｉラウンドで一つのインデックス情報Ｉ＿ｉ

を選び、第ｉラウンドにおけるＰＵＦ出力情報のうち、第Ｉ＿ｉビットからＷビットのデータを記憶部に記憶する。また、非特許文献１が開示する暗号化鍵の生成方法では、暗号化鍵再現において、第ｉラウンドにおけるＰＵＦ出力情報のうち、記憶部が記憶するＷビットのデータと類似の箇所を探索して、インデックス情報Ｉ＿ｉを再現する。

【００５３】

このように、非特許文献１が開示する暗号化鍵の生成方法では、一つのラウンドにおいて一つのインデックス情報のみを扱うため、所定の長さの暗号化鍵を生成するために必要なインデックス情報Ｉ＿ｉの数と同じ回数だけラウンド処理を繰り返す必要があり、暗号化鍵に十分な情報量を持たせるために必要となるラウンド処理の回数が多くなるという問題があった。例えば、非特許文献１が開示する暗号化鍵の生成方法では、１２８ビットの暗号化鍵を生成するために、各ラウンドで１０ビットのインデックス情報Ｉ＿ｉを利用し、ラウンド処理を１６回繰り返す必要があった。

【００５４】

これに対して、第１実施形態の暗号化鍵生成装置１００によれば、一つのラウンドで複数のインデックス情報Ｉ＿｛ｉ，ｊ｝を生成あるいは再現できるため、所定の長さの暗号化鍵を生成するために必要なラウンド処理の回数が、非特許文献１が開示する暗号化鍵の生成方法よりも少なくなる。例えば、本実施形態の暗号化鍵生成装置１００では、１２８ビットの暗号化鍵を生成するにあたり、各ラウンドで１０ビットのインデックス情報Ｉ＿｛ｉ，ｊ｝を４つずつ利用すれば、４回のラウンド処理の繰り返しのみで、非特許文献１が開示する暗号化鍵の生成方法と同じ情報量をもつ暗号化鍵を生成することができる。このように、本実施形態の暗号化鍵生成装置１００は、非特許文献１が開示する暗号化鍵の生成方法と比べてラウンド処理の繰り返し回数を削減することができ、効率的に暗号化鍵を生成できる。

【００５５】

＜第１実施例の構成＞

次に、第１実施形態の暗号化鍵生成装置１００をより具体化した第１実施例について説明する。図４は、第１実施例の暗号化鍵生成装置１０００のブロック図である。

【００５６】

図４に示すように、第１実施例の暗号化鍵生成装置１０００は、４種類のレジスタ１００１，１００２，１００３，１０１５、外部メモリ１００４、カウンタ１００５、ＰＵＦ演算回路１００６、ＰＵＦ入力生成回路１００７、マスク生成回路１００８、排他的論理和演算回路１００９、インデックス情報生成回路１０１０、インデックス情報再現回路１０１１、比較回路１０１２、選択回路１０１３、および鍵生成回路１０１４を備える。

【００５７】

レジスタＩ１００１は、複数のインデックス情報を保持するレジスタである。レジスタＩ１００１は、各ラウンドｒごとに複数のインデックス情報を保持してもよく、複数のラウンドｉ＝１，．．．，ｒに関するインデックス情報をまとめて保持してもよい。

【００５８】

レジスタＰ１００２は、ＰＵＦ演算回路１００６に入力するＰＵＦ入力情報を保持するレジスタである。なお、後述するＰＵＦ入力生成回路１００７の出力が、そのままＰＵＦ演算回路１００６に入力される場合には、暗号化鍵生成装置１０００はレジスタＰ１００２を備えなくともよい。

【００５９】

レジスタＳ１００３は、ＰＵＦ演算回路１００６が出力するＰＵＦ出力情報を保持するシフトレジスタである。レジスタＳ１００３は、ＰＵＦ演算回路１００６が出力するＰＵＦ出力情報のうちのＷビットのデータを保持する。レジスタＳ１００３は、上述した第１実施形態の暗号化鍵生成装置１００におけるＰＵＦ出力一時記憶部１０５に相当する。

【００６０】

外部メモリ１００４は、排他的論理和演算回路１００９が出力する変形パターン情報を記憶するメモリである。外部メモリ１００４は、上述した第１実施形態の暗号化鍵生成装

置１００における記憶部１０２に相当する。
【００６１】
カウンタ１００５は、各ラウンドにおいて、ＰＵＦ演算回路１００６の出力ビット数をカウントし、カウンタ値ｃｎを記憶する。
【００６２】
ＰＵＦ演算回路１００６は、上述した第１実施形態の暗号化鍵生成装置１００におけるＰＵＦ１０４を実装した演算回路であり、ＰＵＦ入力情報を入力としてＰＵＦ出力情報を出力する。
【００６３】
ＰＵＦ入力生成回路１００７は、レジスタＩ１００１が保持するインデックス情報に基づいて、ＰＵＦ演算回路１００６に入力するＰＵＦ入力情報を生成する。ＰＵＦ入力生成回路１００７は、上述した第１実施形態の暗号化鍵生成装置１００におけるＰＵＦ入力生成部１０３に相当する。
【００６４】
マスク生成回路１００８は、上述した第１実施形態の暗号化鍵生成装置１００におけるＭＧＦ１０７を実装した演算回路であり、レジスタＩ１００１が保持するインデックス情報に基づき、マスク情報を生成して出力する。
【００６５】
排他的論理和演算回路１００９は、レジスタＳ１００３が保持するＰＵＦ出力情報とマスク生成回路１００８が出力するマスク情報とを排他的論理和演算する回路である。排他的論理和演算回路１００９は、上述した第１実施形態の暗号化鍵生成装置１００におけるマスク処理部１０８に相当する。
【００６６】
インデックス情報生成回路１０１０は、暗号化鍵設定の各ラウンドｒにおいて、１からＬまでのＮ＿ｒ個のインデックス情報を発生させる回路である。インデックス情報再現回路１０１１は、暗号化鍵再現において、後述する比較回路１０１２の出力に基づき、カウンタ１００５の値をインデックス情報として再現する。インデックス情報生成回路１０１０およびインデックス情報再現回路１０１１は、上述した第１実施形態の暗号化鍵生成装置１００におけるインデックス情報生成部１０６に相当する。
【００６７】
比較回路１０１２は、暗号化鍵再現において、外部メモリ１００４が記憶する変形パターン情報と排他的論理和演算回路１００９の出力とを比較する回路であり、比較する変形パターン情報と排他的論理和演算回路１００９の出力とが類似のデータであると判断する場合には１を出力し、そうでない場合には０を出力する。
【００６８】
選択回路１０１３は、暗号化鍵設定の処理を実行しているときにはインデックス情報生成回路１０１０の出力を選択してレジスタＩ１００１に出力し、暗号化鍵再現の処理を実行しているときにはインデックス情報再現回路１０１１の出力を選択してレジスタＩ１００１に出力する。
【００６９】
鍵生成回路１０１４は、レジスタＩ１００１が保持するインデックス情報に基づき、暗号化鍵を生成する回路である。鍵生成回路１０１４は、上述した第１実施形態の暗号化鍵生成装置１００における鍵生成部１１０に相当する。
【００７０】
レジスタＫ１０１５は、鍵生成回路１０１４が出力する暗号化鍵を保持するレジスタである。
【００７１】
なお、図４では、第１実施例の暗号化鍵生成装置１０００を構成する各回路と回路間を結ぶ線を一つのみ図示しているが、各ラウンドで複数のインデックス情報を生成あるいは再現させるために、複数のマスク生成回路１００８や排他的論理和演算回路１００９、イ

ンデックス情報生成回路１０１０、インデックス情報再現回路１０１１、比較回路１０１２、選択回路１０１３を並列に実装することが望ましい。ただし、第１実施例の暗号化鍵再現装置１０００は、これらの回路を一つずつ実装し、時分割で利用して複数のインデックス情報を生成あるいは再現してもよい。

【００７２】

＜第１実施例の暗号化鍵設定＞

次に、図５を参照して、第１実施例の暗号化鍵生成装置１０００が実行する暗号化鍵設定の処理について説明する。図５は、第１実施例の暗号化鍵生成装置１０００による暗号化鍵設定の一連の処理の流れを示すフローチャートである。

【００７３】

図５のフローチャートで示す暗号化鍵設定の処理は、第１実施例の暗号化鍵生成装置１０００が暗号化鍵設定開始の命令を受け付けることで開始される。第１実施例の暗号化鍵生成装置１０００は、暗号化鍵設定開始の命令を受け付けると、ラウンド番号ｒを１で初期化し、ｒ＝１，．．．，Ｒに対して、以下の処理をそれぞれ実行する。

【００７４】

カウンタ１００５は、カウンタ値ｃｎを１に初期化する（ステップＳ３０１）。

【００７５】

インデックス情報生成回路１０１１は、Ｎ＿ｒ個のインデックス情報Ｉ＿｛ｒ，１｝，．．．，Ｉ＿｛ｒ，Ｎ＿ｒ｝を生成し、レジスタＩ１００１に格納する（ステップＳ３０２）。ステップＳ３０２の処理は、後述するステップＳ３０６において、レジスタＳ１００３が、ＰＵＦ演算回路１００６が出力する第ｒラウンドにおけるＰＵＦ出力情報のＷ－１ビット目を記憶するまでに行われていればよく、例えば、第ｒラウンドの処理が開始される前に行われていてもよい。

【００７６】

レジスタＩ１００１にインデックス情報が格納されると、第１実施例の暗号化鍵再現装置１０００は、ｃｎ＝１，２，．．．，Ｌ＋Ｗ－１について、以下の処理を繰り返す。

【００７７】

ＰＵＦ入力生成回路１００７は、予め定められた初期値あるいはステップＳ３０２でインデックス情報生成回路１０１１が生成したインデックス情報｛Ｉ＿｛ｉ，ｊ｝｝＿｛０≦ｉ＜ｒ，１≦ｊ≦Ｎ＿ｒ｝を入力として、ＰＵＦ演算回路１００６が第ｒラウンドのｃｎビット目を出力するためのＰＵＦ入力情報Ｘ＿｛ｒ，ｃｎ｝を生成する（ステップＳ３０３）。

【００７８】

レジスタＰ１００２は、ＰＵＦ入力生成回路１００７が生成したＰＵＦ入力情報Ｘ＿｛ｒ，ｃｎ｝を格納する（ステップＳ３０４）。ステップＳ３０４の処理は、後述するステップＳ３０６において、ＰＵＦ入力情報Ｘ＿｛ｒ，ｃｎ｝がＰＵＦ演算回路１００６に入力されるまでに行われていればよく、例えば、第ｒラウンドの処理が開始される前に行われていてもよい。

【００７９】

マスク生成回路１００８は、ｊ＝１，．．．，Ｎ＿ｒについて、予め定められた初期値あるいはインデックス情報生成回路１０１０により生成され、レジスタＩ１００１に格納されたインデックス情報｛Ｉ＿｛ｉ，ｊ｝｝＿｛０≦ｉ≦ｒ，１≦ｊ≦Ｎ＿ｒ｝とｒとｊを入力として、マスク情報Ｍ＿｛ｒ，ｊ｝を生成する（ステップＳ３０５）。ステップＳ３０５の処理は、後述するステップＳ３０８において、排他的論理和演算回路１００９が排他的論理和の演算を行うまでに行われていればよく、例えば、第ｒラウンドの処理が開始される前に行われていてもよい。

【００８０】

レジスタＳ１００３は、ステップＳ３０４でレジスタＰ１００２に格納されたＰＵＦ入力情報Ｘ＿｛ｒ，ｃｎ｝を入力としてＰＵＦ演算回路１００６が出力するＰＵＦ出力情報を記憶する（ステップＳ３０６）。ここで、第１実施例の暗号化鍵生成装置１０００では

、各ｃｎについて、ＰＵＦ演算回路１００６が１ビットのデータを出力することとし、レジスタＳ１００３は、それまでに記憶していたデータを１ビットだけシフトして記憶するとともに、新たにＰＵＦ演算回路１００６が出力する１ビットのデータを記憶する。

【００８１】

排他的論理和演算回路１００９は、レジスタＳ１００３が記憶するＷビットのデータと、マスク生成回路１００８が出力するマスク情報Ｍ＿｛ｒ，ｊ｝との排他的論理和Ｚ＿｛ｒ，ｊ｝を計算する（ステップＳ３０７）。

【００８２】

第１実施例の暗号化鍵生成装置１０００は、カウンタ１００５のカウンタ値ｃｎがＩ＿｛ｒ，ｊ｝＋Ｗ－１と一致するか否かを判定し（ステップＳ３０８）、カウンタ値ｃｎがＩ＿｛ｒ，ｊ｝＋Ｗ－１と一致するときに（ステップＳ３０８：Ｙｅｓ）、排他的論理和演算回路１００９の出力Ｚ＿｛ｒ，ｊ｝を変形パターン情報として外部メモリ１００４に記憶する（ステップＳ３０９）。ただし、ｊは１からＮ＿ｒの間の数である。なお、カウンタ値ｃｎがＩ＿｛ｒ，ｊ｝＋Ｗ－１と一致しないときは（ステップＳ３０８：Ｎｏ）、ステップＳ３０９の処理はスキップする。

【００８３】

その後、第１実施例の暗号化鍵生成装置１０００は、カウンタ１００５のカウンタ値ｃｎ＜Ｌ＋Ｗ－１か否かを判定する（ステップＳ３１０）。ここで、ｃｎ＜Ｌ＋Ｗ－１であるならば（ステップＳ３１０：Ｙｅｓ）、暗号化鍵生成装置１０００は、ｃｎをｃｎ＋１に置き換えて、ステップＳ３０３に戻って以降の処理を繰り返す。一方、ｃｎ＝Ｌ＋Ｗ－１であるならば（ステップＳ３１０：Ｎｏ）、暗号化鍵生成装置１０００は、ｒ＜Ｒであるか否かを判定する（ステップＳ３１１）。ここで、ｒ＜Ｒであるならば（ステップＳ３１１：Ｙｅｓ）、暗号化鍵生成装置１０００は、ｒをｒ＋１に置き換えて、ステップＳ３０１に戻って以降の処理を繰り返す。一方、ｒ＝Ｒであるならば（ステップＳ３１１：Ｎｏ）、ステップＳ３１２に進む。

【００８４】

鍵生成回路１０１４は、例えば、各ラウンドにおいてレジスタＩ１００１に格納されたインデックス情報の集合｛Ｉ＿｛ｉ，ｊ｝｝＿｛０≦ｉ≦Ｒ，１≦ｊ≦Ｎ＿ｉ｝に含まれる各インデックス情報Ｉ＿｛ｉ，ｊ｝を連結して暗号化鍵を生成し、レジスタＫ１０１５に格納する（ステップＳ３１２）。

【００８５】

＜第１実施例の暗号化鍵再現＞

次に、図６を参照して、第１実施例の暗号化鍵生成装置１０００が実行する暗号化鍵再現の処理について説明する。図６は、第１実施例の暗号化鍵生成装置１０００による暗号化鍵再現の一連の処理の流れを説明するフローチャートである。

【００８６】

図６のフローチャートで示す暗号化鍵再現の処理は、第１実施例の暗号化鍵生成装置１０００が暗号化鍵再現開始の命令を受け付けることで開始される。第１実施例の暗号化鍵生成装置１０００は、暗号化鍵再現開始の命令を受け付けると、ラウンド番号ｒを１で初期化し、ｒ＝１，．．．，Ｒに対して、以下の処理をそれぞれ実行する。

【００８７】

カウンタ１００５は、カウンタ値ｃｎを１に初期化する（ステップＳ４０１）。

【００８８】

第１実施例の暗号化鍵再現装置１０００は、ｃｎ＝１，２，．．．，Ｌ＋Ｗ－１について、以下の処理を繰り返す。

【００８９】

ＰＵＦ入力生成回路１００７は、予め定められた初期値あるいは前回のラウンド処理でインデックス情報再現回路１０１１が再現したインデックス情報｛Ｉ＿｛ｉ，ｊ｝｝＿｛０≦ｉ≦ｒ，１≦ｊ≦Ｎ＿ｒ｝を入力として、ＰＵＦ演算回路１００６が第ｒラウンドのｃｎビット目を出力するためのＰＵＦ入力情報Ｘ＿｛ｒ，ｃｎ｝を生成する（ステップＳ

４０２）。
【００９０】
レジスタＰ１００２は、ＰＵＦ入力生成回路１００７が生成したＰＵＦ入力情報Ｘ＿｛ｒ，ｃｎ｝を格納する（ステップＳ４０３）。ステップＳ４０３の処理は、後述するステップＳ４０５において、ＰＵＦ入力情報Ｘ＿｛ｒ，ｃｎ｝がＰＵＦ演算回路１００６に入力されるまでに行われていればよく、例えば、第ｒラウンドの処理が開始される前に行われていてもよい。
【００９１】
マスク生成回路１００８は、ｊ＝１，．．．，Ｎ＿ｒについて、予め定められた初期値あるいは前回のラウンド処理で再現されたインデックス情報｛Ｉ＿｛ｉ，ｊ｝｝＿｛０≦ｉ≦ｒ，１≦ｊ≦Ｎ＿ｒ｝とｒとｊを入力として、マスク情報Ｍ＿｛ｒ，ｊ｝を生成する（ステップＳ４０４）。ステップＳ４０４の処理は、後述するステップＳ４０６において、排他的論理和演算回路１００９が比較回路１０１２の入力となる排他的論理和を計算するまでに行われていればよく、例えば、第ｒラウンドの処理が開始される前に行われていてもよい。
【００９２】
レジスタＳ１００３は、ステップＳ４０３でレジスタＰ１００２に格納されたＰＵＦ入力情報Ｘ＿｛ｒ，ｃｎ｝を入力としてＰＵＦ演算回路１００６が出力するＰＵＦ出力情報を記憶する（ステップＳ４０５）。ここで、第１実施例の暗号化鍵生成装置１０００では、各ｃｎについて、ＰＵＦ演算回路１００６が１ビットのデータを出力することとし、レジスタＳ１００３は、それまでに記憶していたデータを１ビットだけシフトして記憶するとともに、新たにＰＵＦ演算回路１００６が出力する１ビットのデータを記憶する。
【００９３】
排他的論理和演算回路１００９は、レジスタＳ１００３が記憶するＷビットのデータと、マスク生成回路１００８が出力するマスク情報Ｍ＿｛ｒ，ｊ｝との排他的論理和により、変形パターン情報Ｚ＿｛ｒ，ｊ｝との比較対象となる参照情報を生成する（ステップＳ４０６）。
【００９４】
比較回路１０１２は、ステップＳ４０６で生成された参照情報と、外部メモリ１００４が記憶する変形パターン情報Ｚ＿｛ｒ，ｊ｝とを比較して、これらが類似データであるか否かを判定する（ステップＳ４０７）。
【００９５】
比較回路１０１２が二つのデータを類似データであると判定した場合（ステップＳ４０７：Ｙｅｓ）、インデックス情報再現回路１０１１は、カウンタ１００５が記憶するカウンタ値ｃｎについて、Ｉ＿｛ｒ，ｊ｝＝ｃｎ－Ｗ＋１としてインデックス情報Ｉ＿｛ｒ，ｊ｝を再現する（ステップＳ４０８）。つまり、変形パターン情報Ｚ＿｛ｒ，ｊ｝に類似すると判定された参照情報は、カウンタ１００５のカウンタ値ｃｎからＷビット分遡った位置を開始位置とするＷビットのＰＵＦ出力情報とマスク情報Ｍ＿｛ｒ，ｊ｝との排他的論理和であるので、カウンタ１００５のカウンタ値ｃｎからＷビット分遡った位置を、インデックス情報Ｉ＿｛ｒ，ｊ｝として再現する。比較回路１０１２が二つのデータを類似データではないと判定した場合には（ステップＳ４０７：Ｎｏ）、ステップＳ４０８の処理はスキップする。
【００９６】
その後、第１実施例の暗号化鍵生成装置１０００は、カウンタ１００５のカウンタ値ｃｎ＜Ｌ＋Ｗ－１か否かを判定する（ステップＳ４０９）。ここで、ｃｎ＜Ｌ＋Ｗ－１であるならば（ステップＳ４０９：Ｙｅｓ）、暗号化鍵生成装置１０００は、ｃｎをｃｎ＋１に置き換えて、ステップＳ４０２に戻って以降の処理を繰り返す。一方、ｃｎ＝Ｌ＋Ｗ－１であるならば（ステップＳ４０９：Ｎｏ）、暗号化鍵生成装置１０００は、ｒ＜Ｒであるか否かを判定する（ステップＳ４１０）。ここで、ｒ＜Ｒであるならば（ステップＳ４１０：Ｙｅｓ）、暗号化鍵生成装置１０００は、ｒをｒ＋１に置き換えて、ステップＳ４

０１に戻って以降の処理を繰り返す。一方、ｒ＝Ｒであるならば（ステップＳ４１０：Ｎｏ）、ステップＳ４１１に進む。

【００９７】

鍵生成回路１０１４は、例えば、各ラウンドにおいてインデックス情報再現回路１０１１により再現され、レジスタＩ１００１に格納されたインデックス情報の集合｛Ｉ＿｛ｉ，ｊ｝｝＿｛０≦ｉ≦Ｒ，１≦ｊ≦Ｎ＿ｉ｝に含まれる各インデックス情報Ｉ＿｛ｉ，ｊ｝を連結して暗号化鍵を生成し、レジスタＫ１０１５に格納する（ステップＳ４１１）。なお、鍵生成回路１０１４は、インデックス情報｛Ｉ＿｛ｉ，ｊ｝｝＿｛０≦ｉ≦Ｒ，１≦ｊ≦Ｎ＿ｉ｝の代わりに、ＰＵＦ入力情報｛Ｘ＿｛ｒ，ｃｎ｝｝＿｛１≦ｒ≦Ｒ｝を連結して暗号化鍵を生成してもよい。あるいは、鍵生成回路１０１４は、インデックス情報｛Ｉ＿｛ｉ，ｊ｝｝＿｛０≦ｉ≦Ｒ，１≦ｊ≦Ｎ＿ｉ｝に加えて、ＰＵＦ入力情報｛Ｘ＿｛ｒ，ｃｎ｝｝＿｛１≦ｒ≦Ｒ｝を連結して暗号化鍵を生成してもよい。また、鍵生成回路１０１４は、連結した値を暗号化鍵として用いてもよいし、連結した値をハッシュ関数などに入力し、得られた値を暗号化鍵として用いてもよい。

【００９８】

（第２実施形態）

＜概要＞

まず、第２実施形態の暗号化鍵生成装置の概要を説明する。第２実施形態の暗号化鍵生成装置は、暗号化鍵設定において、秘密情報を用いて暗号化鍵を生成し、ＰＵＦの出力を秘密情報が示すシフト量だけ巡回シフトした情報をパターン情報として記憶する。また、第２実施形態の暗号化鍵生成装置は、暗号化鍵再現において、ＰＵＦの出力を１ビットずつ巡回シフトしながら記憶したパターン情報と比較し（パターン照合）、ＰＵＦの出力がパターン情報と類似するときのＰＵＦの出力の巡回シフト量を検出することで、暗号化鍵設定で暗号化鍵の生成に用いた秘密情報を再現し、暗号化鍵を再現する。

【００９９】

＜構成＞

次に、図７を参照して、第２実施形態の暗号化鍵生成装置の概略構成を説明する。図７は、第２実施形態の暗号化鍵生成装置２００の機能的な構成を示す機能ブロック図である。

【０１００】

図７に示すように、本実施形態の暗号化鍵生成装置２００は、通信部２０１、記憶部２０２、ＰＵＦ入力生成部２０３、ＰＵＦ２０４、ＰＵＦ出力一時記憶部２０５、秘密情報生成部２０６、出力シフト部２０７、比較部２０８、および鍵生成部２０９を備える。

【０１０１】

通信部２０１は、暗号化鍵生成装置２００と外部システムとの間の通信を行うインターフェースである。

【０１０２】

記憶部２０２は、暗号化鍵設定において、ＰＵＦ２０４が出力するＰＵＦ出力情報を出力シフト部２０７で巡回シフトすることで得られるパターン情報Ｚ＿ｒを記憶するメモリである。記憶部２０２は、例えば、ＲＡＭ、ＥＥＰＲＯＭ（登録商標）などで構成される。なお、記憶部２０２は、暗号化鍵生成装置２００の外部にあってもよい。記憶部２０２が暗号化鍵生成装置２００の外部にある場合、暗号化鍵生成装置２００の各部は、記憶部２０２に対するデータの書き込みや読み出しを、通信部２０１を介して行う。

【０１０３】

ＰＵＦ入力生成部２０３は、予め定められた初期値Ｉ＿０あるいは秘密情報生成部２０６が出力する秘密情報Ｉ＿ｒに基づき、ＰＵＦ２０４へ入力するＰＵＦ入力情報を生成する。例えば、ＰＵＦ入力生成部２０３は、ＰＵＦ入力情報が所定の長さとなるように、初期値Ｉ＿０あるいは秘密情報Ｉ＿ｒに対して予め定められたデータを連結して、ＰＵＦ入力情報を生成する。また、ＰＵＦ入力生成部２０３は、初期値Ｉ＿０あるいは秘密情報Ｉ＿ｒをハッシュ関数などに入力して、ＰＵＦ入力情報を生成するようにしてもよい。また

、ＰＵＦ入力生成部２０３に入力される情報が複数ある場合には、ＰＵＦ入力生成部２０３は、それら入力情報を連結したり、ビット演算あるいは算術演算することで、ＰＵＦ入力情報を生成するようにしてもよい。

【０１０４】

ＰＵＦ２０４は、物理的複製困難関数である。物理的複製困難関数は、あるデバイスに搭載されると、同一の入力からそのデバイス固有の値を出力する関数である。非特許文献１において開示される暗号化鍵生成装置は、複数のＰＵＦの出力を排他的論理和演算して得られる値を利用する。以降の説明では、ＰＵＦ２０４は、このような複数のＰＵＦとそれらの出力を排他的論理和演算して値を出力する回路や、複数のＰＵＦとそれら出力をビット演算あるいは算術演算して値を出力する回路を用いてもよい。ＰＵＦ２０４は、各ラウンドにおいて、ＰＵＦ入力生成部２０３が生成したＰＵＦ入力情報を入力し、ＷビットのＰＵＦ出力情報を出力する。

【０１０５】

ＰＵＦ出力一時記憶部２０５は、各ラウンドにおいてＰＵＦ２０４が出力するＰＵＦ出力情報を一時的に記憶する。本実施形態のＰＵＦ出力一時記憶部２０５は、例えば、Ｗビットのレジスタで構成される。

【０１０６】

秘密情報生成部２０６は、各ラウンドにおいて１つの秘密情報Ｉ＿ｒを生成する。各ラウンドにおいて秘密情報生成部２０６が生成する秘密情報Ｉ＿ｒは、後述の出力シフト部２０７においてＰＵＦ出力情報を巡回シフトさせる量を示す情報である。なお、秘密情報Ｉ＿ｒは、通信部２０１により暗号化鍵生成装置２００の外部から受け付けるなどして、予め定められた値を用いてもよい。この場合には、暗号化鍵生成装置２００は秘密情報生成部２０６を備えていなくてもよい。

【０１０７】

出力シフト部２０７は、第ｒラウンドにおけるＰＵＦ出力情報Ｙ＿ｒを、秘密情報Ｉ＿ｒに基づき巡回シフトする。例えば、出力シフト部２０７は、ＰＵＦ出力情報Ｙ＿ｒをを Ｉ＿ｒビット左巡回シフトしてもよいし、予め定められた規則に基づき、秘密情報Ｉ＿ｒに応じたシフト量だけ巡回シフトしてもよい。

【０１０８】

比較部２０８は、暗号化鍵再現において、ＰＵＦ出力一時記憶部２０５が記憶するＰＵＦ出力情報を巡回シフトしながら記憶部２０２が記憶するパターン情報Ｚ＿ｒと比較して、ＰＵＦ出力情報がパターン情報Ｚ＿ｒと類似するときの巡回シフト量を検出する。例えば、比較部２０８は、ＰＵＦ出力一時記憶部２０５が記憶するＰＵＦ出力情報を１ビットずつ巡回シフトすることで順次得られる参照情報Ｚ’＿ｒと、記憶部２０２が記憶するパターン情報Ｚ＿ｒとが類似のデータであるか否かを判定する。類似のデータであるか否かの判定は第１実施形態と同様であるため、ここでは説明を省略する。

【０１０９】

鍵生成部２０９は、ラウンドごとに生成されるＲ個の秘密情報の集合を用いて、暗号化鍵を生成する。例えば、鍵生成部２０９は、Ｒ個の秘密情報Ｉ＿ｒをすべて連結して暗号化鍵を生成するようにしてもよいし、Ｒ個の秘密情報Ｉ＿ｒをビット演算あるいは算術演算して暗号化鍵を生成するようにしてもよい。

【０１１０】

ここで、本実施形態で用いる定数を表す記号について説明する。Ｗは、ＰＵＦ２０４が出力するＰＵＦ出力情報のビット長を表し、各ラウンドにおいて、秘密情報生成部２０６が生成する秘密情報Ｉ＿ｒの最大値を表す。Ｒは、暗号化鍵生成および暗号化鍵再現において実行されるラウンドの総数を表す。Ｉ＿０は、ＰＵＦ入力生成部２０３に入力するデータの初期値を表す。

【０１１１】

本実施形態の暗号化鍵生成装置２００は、例えば、ＣＰＵなどの演算装置、ＲＯＭやＲＡＭなどの記憶装置、ＨＤＤ、ＣＤドライブ装置などの外部記憶装置、通信装置などを備

えた、通常のコンピュータを利用したハードウェア構成を採用することができる。そして、コンピュータによって実行されるプログラムにより、上記のハードウェア資源を利用して、通信部２０１、記憶部２０２、ＰＵＦ入力生成部２０３、ＰＵＦ２０４、ＰＵＦ出力一時記憶部２０５、秘密情報生成部２０６、出力シフト部２０７、比較部２０８、および鍵生成部２０９の各機能構成を実現することができる。

【０１１２】

＜暗号化鍵設定＞

次に、図８を参照して、第２実施形態の暗号化鍵生成装置２００が実行する暗号化鍵設定の処理について説明する。図８は、暗号化鍵生成装置２００による暗号化鍵設定の一連の処理の流れを示すフローチャートである。

【０１１３】

図８のフローチャートで示す暗号化鍵設定の処理は、暗号化鍵生成装置２００が暗号化鍵設定開始の命令を受け付けることで開始される。暗号化鍵生成装置２００は、暗号化鍵設定開始の命令を受け付けると、ラウンド番号ｒを１で初期化し、ｒ＝１，．．．，Ｒに対して、以下の処理をそれぞれ実行する。

【０１１４】

秘密情報生成部２０６は、秘密情報Ｉ＿ｒを生成する（ステップＳ５０１）。ステップＳ５０１の処理は、第ｒラウンドの処理が開始される前に行われていてもよい。

【０１１５】

ＰＵＦ入力生成部２０３は、予め定められた初期値あるいはステップＳ５０１で秘密情報生成部２０６が生成した秘密情報｛Ｉ＿ｉ｝＿｛０≦ｉ＜ｒ｝を入力として、ＰＵＦ２０４が第ｒラウンドのＰＵＦ出力情報を出力するためのＰＵＦ入力情報Ｘ＿ｒを生成する（ステップＳ５０２）。ステップＳ５０２の処理は、後述するステップＳ５０３において、ＰＵＦ入力情報Ｘ＿ｒがＰＵＦ２０４に入力されるまでに行われていればよく、例えば、第ｒラウンドの処理が開始される前に行われていてもよい。

【０１１６】

ＰＵＦ出力一時記憶部２０５は、ステップＳ５０２でＰＵＦ入力生成部２０３が生成したＰＵＦ入力情報Ｘ＿ｒを入力としてＰＵＦ２０４が出力するＷビットのＰＵＦ出力情報を記憶する（ステップＳ５０３）。

【０１１７】

出力シフト部２０７は、例えば、ステップＳ５０３でＰＵＦ出力一時記憶部２０５が記憶したＰＵＦ出力情報を、ステップＳ５０１で秘密情報生成部２０６が生成した秘密情報Ｉ＿ｒで示されるシフト量だけ左巡回シフトして、パターン情報Ｚ＿ｒを生成する（ステップＳ５０４）。

【０１１８】

記憶部２０２は、ステップＳ５０４で出力シフト部２０７が生成したパターン情報Ｚ＿ｒを記憶する（ステップＳ５０５）。

【０１１９】

記憶部２０２にパターン情報Ｚ＿ｒが記憶されると、暗号化鍵生成装置２００は、ｒ＜Ｒであるか否かを判定する（ステップＳ５０６）。ここで、ｒ＜Ｒであるならば（ステップＳ５０６：Ｙｅｓ）、暗号化鍵生成装置２００は、ｒをｒ＋１に置き換えて、ステップＳ５０１に戻って以降の処理を繰り返す。一方、ｒ＝Ｒであるならば（ステップＳ５０６：Ｎｏ）、ステップＳ５０７に進む。

【０１２０】

鍵生成部２０９は、例えば、各ラウンドにおいて秘密情報生成部２０６が生成したＲ個の秘密情報Ｉ＿ｒを連結して、暗号化鍵を生成する（ステップＳ５０９）。

【０１２１】

＜暗号化鍵再現＞

次に、図９を参照して、第２実施形態の暗号化鍵生成処理２００が実行する暗号化鍵再現の処理について説明する。暗号化鍵再現の処理は、上述の暗号化鍵設定の処理が終わっ

た後、暗号プロトコルが暗号化鍵を必要とするときに実行される。図９は、暗号化鍵生成装置２００による暗号化鍵再現の一連の処理の流れを示すフローチャートである。

【０１２２】

図９のフローチャートで示す暗号化鍵再現の処理は、暗号化鍵生成装置２００が暗号化鍵再現開始の命令を受け付けることで開始される。暗号化鍵生成装置２００は、暗号化鍵再現開始の命令を受け付けると、ラウンド番号ｒを１で初期化し、ｒ＝１，．．．，Ｒに対して、以下の処理をそれぞれ実行する。

【０１２３】

ＰＵＦ入力生成部２０３は、予め定められた初期値あるいは前回のラウンド処理で再現された秘密情報｛Ｉ＿ｉ｝＿｛０≦ｉ＜ｒ｝を入力として、ＰＵＦ２０４が第ｒラウンドのＰＵＦ出力情報を出力するためのＰＵＦ入力情報Ｘ＿ｒを生成する（ステップＳ６０１）。ステップＳ６０１の処理は、後述するステップＳ６０３において、ＰＵＦ入力情報Ｘ＿ｒがＰＵＦ２０４に入力されるまでに行われていればよく、例えば、第ｒラウンドの処理が開始される前に行われていてもよい。

【０１２４】

ＰＵＦ出力一時記憶部２０５は、ステップＳ６０１でＰＵＦ入力生成部２０３が生成したＰＵＦ入力情報Ｘ＿ｒを入力としてＰＵＦ２０４が出力するＷビットのＰＵＦ出力情報を記憶する（ステップＳ６０２）。

【０１２５】

ＰＵＦ出力一時記憶部２０５がＰＵＦ出力情報を記憶すると、暗号化鍵生成装置２００は、ｋ＝１，．．．，Ｗについて、ＰＵＦ出力一時記憶部２０５が記憶するＰＵＦ出力情報に対して、以下のステップＳ６０３～ステップＳ６０６の処理を繰り返し実行する。

【０１２６】

出力シフト部２０７は、例えば、ＰＵＦ出力一時記憶部２０５がＰＵＦ出力情報をｋビット左巡回シフトさせて、参照情報Ｚ’＿ｒを生成する（ステップＳ６０３）。

【０１２７】

比較部２０８は、ステップＳ６０３で出力シフト部２０７が生成した参照情報Ｚ’＿ｒと、記憶部２０２が記憶するパターン情報Ｚ＿ｒとが類似データであるか否かを判定する（ステップＳ６０４）。なお、比較部２０８は、記憶部２０２が記憶するパターン情報Ｚ＿ｒに対して、出力シフト部２０７が参照情報Ｚ’＿ｒを生成する際に行うシフトの方向とは逆方向のシフトを行って得られるデータと、ＰＵＦ出力一時記憶部２０５がＰＵＦ出力情報とを比較して、これらが類似データであるか否かを判定するようにしてもよい。

【０１２８】

比較部２０８が二つのデータを類似データであると判定した場合（ステップＳ６０４：Ｙｅｓ）、暗号化鍵生成装置２００は、Ｉ＿ｒ＝ｋとして秘密情報Ｉ＿ｒを再現する（ステップＳ６０５）。つまり、記憶部２０２が記憶するパターン情報Ｚ＿ｒに類似すると判定された参照情報Ｚ’＿ｒが出現するまでのＰＵＦ出力情報の巡回シフト量ｋを、秘密情報Ｉ＿ｒとして再現する。比較部２０８が二つのデータを類似データではないと判定した場合には（ステップＳ６０４：Ｎｏ）、ステップＳ６０５の処理はスキップする。

【０１２９】

その後、暗号化鍵生成装置２００は、ｋ＜Ｗであるか否かを判定する（ステップＳ６０６）。ここで、ｋ＜Ｗであるならば（ステップＳ６０６：Ｙｅｓ）、ｋをｋ＋１に置き換えて、ステップＳ６０３に戻って以降の処理を繰り返す。なお、ｋ＝１，．．．，Ｗについて、ステップＳ６０３～ステップＳ６０６の処理を繰り返しても再現できない秘密情報Ｉ＿ｒが存在する場合には、暗号化鍵生成装置２００は、処理を停止するようにしてもよいし、再現できない秘密情報Ｉ＿ｒに予め定められた値あるいはランダムな値を設定してもよい。

【０１３０】

ステップＳ６０６の判定の結果がｋ＝Ｗであるならば（ステップＳ６０６：Ｎｏ）、暗号化鍵生成装置２００は、ｒ＜Ｒであるか否かを判定する（ステップＳ６０７）。ここで

、ｒ＜Ｒであるならば（ステップＳ６０７：Ｙｅｓ）、暗号化鍵生成装置２００は、ｒをｒ＋１に置き換えて、ステップＳ６０１に戻って以降の処理を繰り返す。一方、ｒ＝Ｒであるならば（ステップＳ６０７：Ｎｏ）、ステップＳ６０８に進む。

【０１３１】

鍵生成部２０９は、例えば、各ラウンドにおいて再現したＲ個の秘密情報Ｉ＿ｒを連結して、暗号化鍵を生成する（ステップＳ６０８）。なお、鍵生成部２０９は、秘密情報Ｉ＿ｒの代わりに、ＰＵＦ入力情報｛Ｘ＿ｒ｝＿｛１≦ｒ≦Ｒ｝を連結して暗号化鍵を生成してもよい。あるいは、鍵生成部２０９は、秘密情報Ｉ＿ｒに加えて、ＰＵＦ入力情報｛Ｘ＿ｒ｝＿｛１≦ｒ≦Ｒ｝を連結して暗号化鍵を生成してもよい。また、鍵生成部２０９は、連結した値を暗号化鍵として用いてもよいし、連結した値をハッシュ関数などに入力し、得られた値を暗号化鍵として用いてもよい。

【０１３２】

なお、本実施形態の暗号化鍵生成装置２００では、ＰＵＦ入力生成部２０３が、秘密情報Ｉ＿ｒに基づいて、ＰＵＦ２０４に入力するＰＵＦ入力情報Ｘ＿ｒを生成するようにしている。しかし、ＰＵＦ入力生成部２０３は、例えばＰＵＦ２０４への起動信号など、秘密情報Ｉ＿ｒに依存しない固定値を、ＰＵＦ入力情報Ｘ＿ｒとして生成するようにしてもよい。

【０１３３】

また、本実施形態の暗号化鍵生成装置２００では、ＰＵＦ２０４が、各ラウンドにおいてＷビットのＰＵＦ出力情報を出力するようにしている。しかし、ＰＵＦ２０４がＷビットを超えるＰＵＦ出力情報を出力し、各ラウンドでそのＰＵＦ出力情報の一部を利用する構成であってもよい。例えば、図８のステップＳ５０５において、ＰＵＦ出力情報を巡回シフトして得られるデータの前半Ｖビット（Ｖ＜Ｗ）をパターン情報Ｚ＿ｒとして利用してもよい。あるいは、ＰＵＦ２０４がＷビットを超えるＰＵＦ出力情報を出力するとき、ＰＵＦ出力一時記憶部２０５が、ＰＵＦ出力情報のうちの前半Ｖビット（Ｖ＜Ｗ）と後半Ｗ－Ｖビットを連結して記憶し、以降の処理を実施する構成とすることができる。また、例えば、ＰＵＦ２０４に対して固定値のＰＵＦ入力情報Ｘ＿ｒが入力され、ＰＵＦ２０４がＲ×ＷビットのＰＵＦ出力情報を出力する場合には、第ｉラウンドでは、ＰＵＦ出力一時記憶部２０５がＰＵＦ出力情報のうち（ｉ－１）×Ｗビット目からＷビットのデータを記憶し、以降の処理を実施する構成とすることができる。

【０１３４】

なお、本実施形態の暗号化鍵生成装置２００では、ＰＵＦ入力生成部２０３がＰＵＦ２０４への起動信号などの秘密情報Ｉ＿ｒに依存しない固定値をＰＵＦ入力情報Ｘ＿ｒとして生成する場合に、以下に示すように、各ラウンドにおける暗号化鍵の更新が可能になる。すなわち、暗号化鍵設定の処理では、出力シフト部２０７がＰＵＦ出力情報を巡回シフトしてパターン情報Ｚ＿ｒを生成するため、記憶部２０２には、パターン情報Ｚ＿１，・・・，Ｚ＿Ｒが記憶される。ここで、暗号化鍵を更新する場合は、記憶部２０２が記憶するパターン情報Ｚ＿ｒを、Ｚ＿ｒをΔ＿ｒだけ巡回シフトして得られるＺ＿ｒ’に置き換える。Ｚ＿ｒ’は、ＰＵＦ出力情報をＩ＿ｒ＋Δ＿ｒだけ巡回シフトして得られる値であるため、暗号化鍵再現の処理では、｛Ｉ＿ｒ＋Δ＿ｒ｝＿｛１≦ｒ≦Ｒ｝に基づいて暗号化鍵が生成される。つまり、｛Ｉ＿ｒ｝＿｛１≦ｒ≦Ｒ｝に基づく暗号化鍵を、｛Ｉ＿ｒ＋Δ＿ｒ｝＿｛１≦ｒ≦Ｒ｝に基づく暗号化鍵に更新することができる。

【０１３５】

＜実施形態の効果＞

非特許文献１が開示する暗号化鍵の生成方法では、ＰＵＦの出力の長さを十分に長く設定し、その一部のみを記憶部に記憶して暗号化鍵の生成および再現に利用している。例えば、非特許文献１が開示する暗号化鍵の生成方法では、Ｌは１０２４ビット、Ｗは２５６ビットとされ、各ラウンドでＰＵＦは１３７９ビット出力しなければならなかった。

【０１３６】

このように、非特許文献１が開示する暗号化鍵の生成方法では、各ラウンドごとに２５

６ビットの情報を記憶部に記憶させるために、ＰＵＦは１３７９ビット出力しなければならず、ＰＵＦの利用効率が悪いという問題があった。

【０１３７】

これに対して、第２実施形態の暗号化鍵生成装置２００によれば、一つのラウンドでＰＵＦ２０４が出力するＰＵＦ出力情報はWビットであり、このWビットのＰＵＦ出力情報を巡回シフトして得られるパターン情報を記憶部２０２に記憶する構成であるため、非特許文献１が開示する暗号化鍵の生成方法と比べて、各ラウンドで生成するＰＵＦ出力情報は短くてよい。例えば、Ｗ＝２５６とする場合に、非特許文献１が開示する暗号化鍵の生成方法では１３７９ビットのＰＵＦ出力情報が必要であったのに対して、第２実施形態の暗号化鍵生成装置２００では２５６ビットでよく、各ラウンドにおけるＰＵＦ２０４の出力ビット数は１／５程度になる。このように、本実施形態の暗号化鍵生成装置２００は、非特許文献１が開示する暗号化鍵の生成方法と比べてＰＵＦの出力を少なくし、効率的に暗号化鍵を生成できる。

【０１３８】

＜第２実施例の構成＞

次に、第２実施形態の暗号化鍵生成装置２００をより具体化した第２実施例について説明する。図１０は、第２実施例の暗号化鍵生成装置２０００のブロック図である。

【０１３９】

図１０に示すように、第２実施例の暗号化鍵生成装置２０００は、４種類のレジスタ２００１，２００２，２００３，２０１４、外部メモリ２００４、カウンタ２００５、ＰＵＦ演算回路２００６、ＰＵＦ入力生成回路２００７、巡回シフト回路２００８、秘密情報生成回路２００９、秘密情報再現回路２０１０、比較回路２０１１、選択回路２０１２、および鍵生成回路２０１３を備える。

【０１４０】

レジスタＩ２００１は、秘密情報を保持するレジスタである。レジスタＩ２００１は、各ラウンドｒごとに１つの秘密情報を保持してもよく、複数のラウンドｉ＝１，．．．，ｒに関する秘密情報をまとめて保持してもよい。

【０１４１】

レジスタＰ２００２は、ＰＵＦ演算回路２００６に入力するＰＵＦ入力情報を保持するレジスタである。なお、後述するＰＵＦ入力生成回路２００７の出力が、そのままＰＵＦ演算回路２００６に入力される場合には、鍵生成装置２０００はレジスタＰ２００２を備えなくともよい。

【０１４２】

レジスタＲ２００３は、ＰＵＦ演算回路２００６が出力するＰＵＦ出力情報を保持するレジスタである。レジスタＲ２００３は、ＰＵＦ演算回路２００６が出力するWビットのＰＵＦ出力情報を保持する。レジスタＲ２００３は、上述した第２実施形態の暗号化鍵生成装置２００におけるＰＵＦ出力一時記憶部２０５に相当する。

【０１４３】

外部メモリ２００４は、巡回シフト回路２００８が出力するパターン情報を記憶するメモリである。外部メモリ２００４は、上述した第２実施形態の暗号化鍵生成装置２００における記憶部２０２に相当する。

【０１４４】

カウンタ２００５は、各ラウンドにおいて、巡回シフト回路２００８によるＰＵＦ出力情報の巡回シフト量をカウントし、カウンタ値ｃｎを記憶する。

【０１４５】

ＰＵＦ演算回路２００６は、上述した第２実施形態の暗号化鍵生成装置２００におけるＰＵＦ２０４を実装した演算回路であり、ＰＵＦ入力情報を入力としてＰＵＦ出力情報を生成し出力する。

【０１４６】

ＰＵＦ入力生成回路２００７は、レジスタＩ２００１が保持する秘密情報に基づいて、

ＰＵＦ演算回路２００６に入力するＰＵＦ入力情報を生成する。ＰＵＦ入力生成回路２００７は、上述した第２実施形態の暗号化鍵生成装置２００におけるＰＵＦ入力生成部２０３に相当する。

【０１４７】

巡回シフト回路２００８は、レジスタＲ２００３が記憶するＷビットのＰＵＦ出力情報を、レジスタＩ２００１に格納されている秘密情報で示される値だけ巡回シフトして、外部メモリ２００４に記憶するパターン情報を生成する。巡回シフト回路２００８は、上述した第２実施形態の暗号化鍵生成装置２００における出力シフト部２０７に相当する。なお、レジスタＲ２００３と巡回シフト回路２００８とを併せて実装し、レジスタＲ２００３内でＰＵＦ出力情報の巡回シフトを行うようにしてもよい。あるいは、ＰＵＦ演算装置２００６が１ビット出力するごとに、レジスタＲ２００３内で、レジスタＩ２００１に格納されている秘密情報で示される値の番地にＰＵＦ出力情報を巡回シフトしながら書き込んでもよい。

【０１４８】

秘密情報生成回路２００９は、暗号化鍵設定の各ラウンドｒにおいて、一つの秘密情報を発生させる回路である。秘密情報再現回路２０１０は、暗号化鍵再現において、後述する比較回路２０１１の出力に基づき、カウンタ２００５の値を秘密情報として再現する。秘密情報生成回路２００９および秘密情報再現回路２０１０は、上述した第２実施形態の暗号化鍵生成装置２００における秘密情報生成部２０６に相当する。

【０１４９】

比較回路２０１１は、暗号化鍵再現において、外部メモリ２００４が記憶するパターン情報と巡回シフト回路２００８が出力する参照情報とを比較する回路であり、比較するパターン情報と参照情報とが類似のデータであると判断する場合には１を出力し、そうでない場合には０を出力する。

【０１５０】

選択回路２０１２は、暗号化鍵設定の処理を実行しているときには秘密情報生成回路２００９の出力を選択してレジスタＩ２００１に出力し、暗号化鍵再現の処理を実行しているときには秘密情報再現回路２０１０の出力を選択してレジスタＩ２００１に出力する。

【０１５１】

鍵生成回路２０１３は、レジスタＩ２００１が保持する秘密情報に基づき、暗号化鍵を生成する回路である。鍵生成回路２０１３は、上述した第２実施形態の暗号化鍵生成装置２００における鍵生成部２０９に相当する。

【０１５２】

レジスタＫ２０１４は、鍵生成回路２０１３が出力する暗号化鍵を保持するレジスタである。

【０１５３】

＜第２実施例の暗号化鍵設定＞

次に、図１１を参照して、第２実施例の暗号化鍵生成装置２０００が実行する暗号化鍵設定の処理について説明する。図１１は、第２実施例の暗号化鍵生成装置２０００による暗号化鍵設定の一連の処理の流れを示すフローチャートである。

【０１５４】

図１１のフローチャートで示す暗号化鍵設定の処理は、第２実施例の暗号化鍵生成装置２０００が暗号化鍵設定開始の命令を受け付けることで開始される。第２実施例の暗号化鍵生成装置２０００は、暗号化鍵設定開始の命令を受け付けると、ラウンド番号ｒを１で初期化し、ｒ＝１，．．．，Ｒに対して、以下の処理をそれぞれ実行する。

【０１５５】

カウンタ２００５は、カウンタ値ｃｎを１に初期化する（ステップＳ７０１）。

【０１５６】

秘密情報生成回路２００９は、秘密情報Ｉ＿ｒを生成し、レジスタＩ２００１に格納する（ステップＳ７０２）。ステップＳ７０２の処理は、例えば、第ｒラウンドの処理が開

始される前に行われていてもよい。

【０１５７】

ＰＵＦ入力生成回路２００７は、予め定められた初期値あるいはステップＳ７０１で秘密情報生成回路２００９が生成した秘密情報Ｉ＿ｒを入力としてＰＵＦ入力情報Ｘ＿ｒを生成し、レジスタＰ２００２に格納する（ステップＳ７０３）。ステップＳ７０３の処理は、例えば、第ｒラウンドの処理が開始される前に行われていてもよい。

【０１５８】

レジスタＲ２００３は、ステップＳ７０３でレジスタＰ２００２に格納されたＰＵＦ入力情報Ｘ＿ｒを入力としてＰＵＦ演算回路２００６が出力するＷビットのＰＵＦ出力情報を記憶する（ステップＳ７０４）。

【０１５９】

ＷビットのＰＵＦ出力情報がレジスタＲ２００３に記憶されると、第２実施例の暗号化鍵再現装置２０００は、ｃｎ＝１，２，．．．，Ｗについて、以下のステップＳ７０５～ステップＳ７０８の処理を繰り返す。

【０１６０】

巡回シフト回路２００８は、レジスタＲ２００３が記憶するＰＵＦ出力情報を１ビットずつ左巡回シフトする（ステップＳ７０５）。このステップＳ７０５の処理によりＰＵＦ出力情報が１ビット左巡回シフトされるたびに、カウンタ２００５のカウンタ値ｃｎがインクリメントされる。

【０１６１】

第２実施例の暗号化鍵生成装置２０００は、カウンタ２００５のカウンタ値ｃｎがＩ＿ｒと一致するか否か、つまり、秘密情報Ｉ＿ｒが示すシフト量だけＰＵＦ出力情報が巡回シフトされたか否かを判定し（ステップＳ７０６）、カウンタ値ｃｎがＩ＿ｒと一致するときに（ステップＳ７０６：Ｙｅｓ）、巡回シフト回路２００８の出力をパターン情報として外部メモリ２００４に記憶する（ステップＳ７０７）。なお、カウンタ値ｃｎがＩ＿ｒと一致しないときは（ステップＳ７０６：Ｎｏ）、ステップＳ７０７の処理はスキップする。

【０１６２】

その後、第２実施例の暗号化鍵生成装置２０００は、カウンタ２００５のカウンタ値ｃｎ＜Ｗか否かを判定する（ステップＳ７０８）。ここで、ｃｎ＜Ｗであるならば（ステップＳ７０８：Ｙｅｓ）、暗号化鍵生成装置２０００は、ステップＳ７０５に戻って以降の処理を繰り返す。一方、ｃｎ＝Ｗであるならば（ステップＳ７０８：Ｎｏ）、暗号化鍵生成装置２０００は、ｒ＜Ｒであるか否かを判定する（ステップＳ７０９）。ここで、ｒ＜Ｒであるならば（ステップＳ７０９：Ｙｅｓ）、暗号化鍵生成装置２０００は、ｒをｒ＋１に置き換えて、ステップＳ７０１に戻って以降の処理を繰り返す。一方、ｒ＝Ｒであるならば（ステップＳ７０９：Ｎｏ）、ステップＳ７１０に進む。

【０１６３】

鍵生成回路２０１３は、例えば、各ラウンドにおいてレジスタＩ２００１に格納された秘密情報の集合｛Ｉ＿ｉ｝＿｛０≦ｉ≦Ｒ｝に含まれる各秘密情報Ｉ＿ｒを連結して暗号化鍵を生成し、レジスタＫ２０１４に格納する（ステップＳ７１０）。

【０１６４】

＜第２実施例の暗号化鍵再現＞

次に、図１２を参照して、第２実施例の暗号化鍵生成装置２０００が実行する暗号化鍵再現の処理について説明する。図１２は、第２実施例の暗号化鍵生成装置２０００による暗号化鍵再現の一連の処理の流れを説明するフローチャートである。

【０１６５】

図１２のフローチャートで示す暗号化鍵再現の処理は、第２実施例の暗号化鍵生成装置２０００が暗号化鍵再現開始の命令を受け付けることで開始される。第２実施例の暗号化鍵生成装置２０００は、暗号化鍵再現開始の命令を受け付けると、ラウンド番号ｒを１で初期化し、ｒ＝１，．．．，Ｒに対して、以下の処理をそれぞれ実行する。

【０１６６】
カウンタ２００５は、カウンタ値ｃｎを１に初期化する（ステップＳ８０１）。
【０１６７】
ＰＵＦ入力生成回路２００７は、予め定められた初期値あるいは前回のラウンド処理で秘密情報再現回路２０１０が再現した秘密情報｛Ｉ＿ｉ｝＿｛０≦ｉ＜ｒ｝を入力としてＰＵＦ入力情報Ｘ＿ｒを生成し、レジスタＰ２００２に格納する（ステップＳ８０２）。ステップＳ８０２の処理は、例えば、第ｒラウンドの処理が開始される前に行われていてもよい。
【０１６８】
レジスタＲ２００３は、ステップＳ８０２でレジスタＰ２００２に格納されたＰＵＦ入力情報Ｘ＿ｒを入力としてＰＵＦ演算回路２００６が出力するＷビットのＰＵＦ出力情報を記憶する（ステップＳ８０３）。
【０１６９】
ＷビットのＰＵＦ出力情報がレジスタＲ２００３に記憶されると、第２実施例の暗号化鍵再現装置２０００は、ｃｎ＝１，２，．．．，Ｗについて、以下のステップＳ８０４～ステップＳ８０７の処理を繰り返す。
【０１７０】
巡回シフト回路２００８は、レジスタＲ２００３が記憶するＰＵＦ出力情報を１ビットずつ左巡回シフトして、パターン情報の比較対象となる参照情報Ｚ＿ｒを生成する（ステップＳ８０４）。このステップＳ８０４の処理によりＰＵＦ出力情報が１ビットずつ左巡回シフトされて新たな参照情報が生成されるたびに、カウンタ２００５のカウンタ値ｃｎがインクリメントされる。
【０１７１】
比較回路２０１１は、ステップＳ８０４で生成された参照情報Ｚ’＿ｒと、外部メモリ２００４が記憶するパターン情報Ｚ＿ｒとを比較して、これらが類似データであるか否かを判定する（ステップＳ８０５）。
【０１７２】
比較回路２０１１が二つのデータを類似データであると判定した場合（ステップＳ８０５：Ｙｅｓ）、秘密情報再現回路２０１０は、カウンタ２００５が記憶するカウンタ値ｃｎを秘密情報Ｉ＿ｒとして再現する（ステップＳ８０６）。つまり、パターン情報Ｚ＿ｒに類似すると判定された参照情報Ｚ’＿ｒは、カウンタ２００５のカウンタ値ｃｎで示される巡回シフト量だけＰＵＦ出力情報を左巡回シフトした情報であるので、カウンタ２００５のカウンタ値ｃｎが示す巡回シフト量を、秘密情報Ｉ＿ｒとして再現する。比較回路２０１１が二つのデータを類似データではない判定した場合には（ステップＳ８０５：Ｎｏ）、ステップＳ８０６の処理はスキップする。
【０１７３】
その後、第２実施例の暗号化鍵生成装置２０００は、カウンタ２００５のカウンタ値ｃｎ＜Ｗか否かを判定する（ステップＳ８０７）。ここで、ｃｎ＜Ｗであるならば（ステップＳ８０７：Ｙｅｓ）、暗号化鍵生成装置２０００は、ステップＳ８０４に戻って以降の処理を繰り返す。一方、ｃｎ＝Ｗであるならば（ステップＳ８０７：Ｎｏ）、暗号化鍵生成装置２０００は、ｒ＜Ｒであるか否かを判定する（ステップＳ８０８）。ここで、ｒ＜Ｒであるならば（ステップＳ８０８：Ｙｅｓ）、暗号化鍵生成装置２０００は、ｒをｒ＋１に置き換えて、ステップＳ８０１に戻って以降の処理を繰り返す。一方、ｒ＝Ｒであるならば（ステップＳ８０８：Ｎｏ）、ステップＳ８０９に進む。
【０１７４】
鍵生成回路２０１３は、例えば、各ラウンドにおいて秘密情報再現回路２０１０により再現され、レジスタＩ２００１に格納された秘密情報の集合｛Ｉ＿ｉ｝＿｛０≦ｉ≦Ｒ｝に含まれる各秘密情報Ｉ＿ｒを連結して暗号化鍵を生成し、レジスタＫ２０１４に格納する（ステップＳ８０９）。なお、鍵生成回路２０１３は、秘密情報｛Ｉ＿ｉ｝＿｛０≦ｉ≦Ｒ｝の代わりに、ＰＵＦ入力情報｛Ｘ＿ｒ｝＿｛１≦ｒ≦Ｒ｝を連結して暗号化鍵を生

成してもよい。あるいは、鍵生成回路２０１３は、秘密情報｛Ｉ＿ｉ｝＿｛０≦ｉ≦Ｒ｝に加えて、ＰＵＦ入力情報｛Ｘ＿ｒ｝＿｛１≦ｒ≦Ｒ｝を連結して暗号化鍵を生成してもよい。また、鍵生成回路２０１３は、連結した値を暗号化鍵として用いてもよいし、連結した値をハッシュ関数などに入力し、得られた値を暗号化鍵として用いてもよい。

【０１７５】

以上、第１実施形態および第２実施形態とそれらの具体的な実施例について説明したが、これら実施形態の暗号化鍵生成装置は、通常のコンピュータを利用したハードウェア構成を採用し、コンピュータによって実行されるプログラムにより、上述した各機能構成を実現する構成とすることができる。

【０１７６】

上述した暗号化鍵生成装置の各機能構成を実現するプログラムは、例えば、インストール可能な形式又は実行可能な形式のファイルでＣＤ－ＲＯＭ、フレキシブルディスク（ＦＤ）、ＣＤ－Ｒ、ＤＶＤ（Ｄｉｇｉｔａｌ　Ｖｅｒｓａｔｉｌｅ　Ｄｉｓｋ）などのコンピュータで読み取り可能な記録媒体に記録されて提供される。

【０１７７】

また、上述した暗号化鍵生成装置の各機能構成を実現するプログラムを、インターネットなどのネットワークに接続されたコンピュータ上に格納し、ネットワーク経由でダウンロードさせることにより提供するように構成してもよい。また、上述した暗号化鍵生成装置の各機能構成を実現するプログラムを、インターネットなどのネットワーク経由で提供または配布するように構成してもよい。さらに、上述した暗号化鍵生成装置の各機能構成を実現するプログラムを、ＲＯＭなどに予め組み込んで提供するように構成してもよい。

【０１７８】

上述した暗号化鍵生成装置の各機能構成を実現するプログラムは、各機能構成に対応するコンポーネントを含むモジュール構成となっており、実際のハードウェアとしてはＣＰＵ（プロセッサ）が上記記憶媒体からプログラムを読み出して実行することにより上記各コンポーネントが主記憶装置上にロードされ、暗号化鍵生成装置の各機能構成が主記憶装置上に生成されるようになっている。

【０１７９】

以上、具体的な例を挙げながら詳細に説明したように、実施形態の暗号化鍵生成装置によれば、物理的複製困難関数を用いて効率良く暗号化鍵を生成することができる。

【０１８０】

なお、第１実施形態および第２実施形態とそれらの具体的な実施例は、その構成要素を適宜組み合わせることで、種々の発明を形成することができる。例えば、第２実施形態の暗号化鍵生成装置２００がＭＧＦ１０７およびマスク処理部１０８を備え、巡回シフトしたＰＵＦ出力情報をマスク処理して記憶部１０２に記憶する構成とすることもできる。また、第２実施形態の暗号化鍵生成装置２００が、各ラウンドにおいて、複数の秘密情報を生成あるいは再現するようにしてもよい。

【０１８１】

また、以上説明した実施形態は、例として提示したものであり、発明の範囲を限定することは意図していない。上記の新規な実施形態は、その他の様々な形態で実施されることが可能であり、発明の要旨を逸脱しない範囲で、種々の省略、置き換え、変更を行うことができる。上記の実施形態やその変形は、発明の範囲や要旨に含まれるとともに、請求の範囲に記載された発明とその均等の範囲に含まれる。

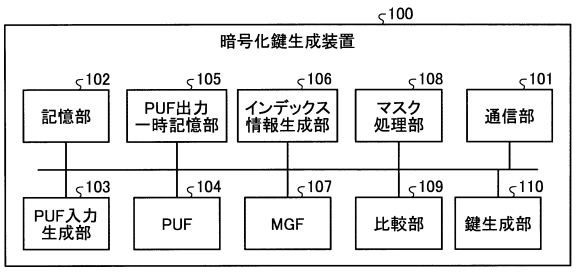
【符号の説明】

【０１８２】

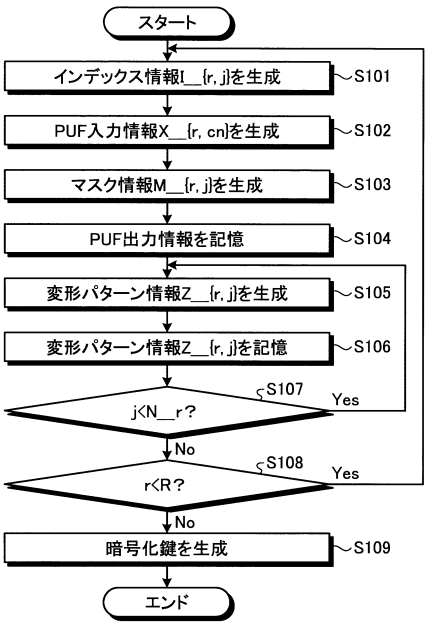
１００　暗号化鍵生成装置
１０２　記憶部
１０４　ＰＵＦ
１０７　ＭＧＦ
１０８　マスク処理部

１０９　比較部
１１０　鍵生成部
２００　暗号化鍵生成装置
２０２　記憶部
２０４　ＰＵＦ
２０７　出力シフト部
２０８　比較部
２０９　鍵生成部
１０００　暗号化鍵生成装置
１００４　外部メモリ
１００６　ＰＵＦ演算回路
１００８　マスク生成回路
１００９　排他的論理和演算回路
１０１２　比較回路
１０１４　鍵生成回路
２０００　暗号化鍵生成装置
２００４　外部メモリ
２００６　ＰＵＦ演算回路
２００８　巡回シフト回路
２０１１　比較回路
２０１３　鍵生成回路

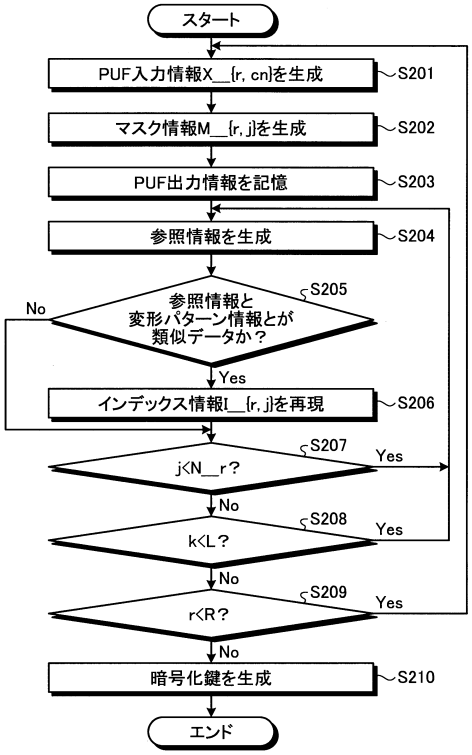
【図１】



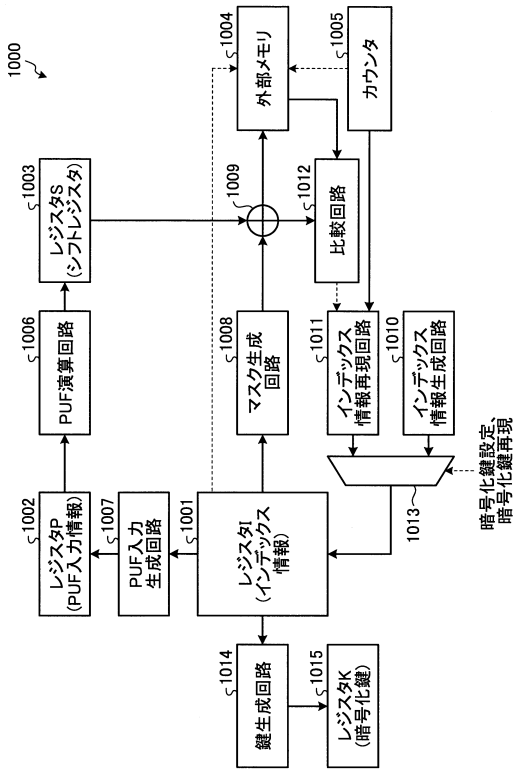
【図２】



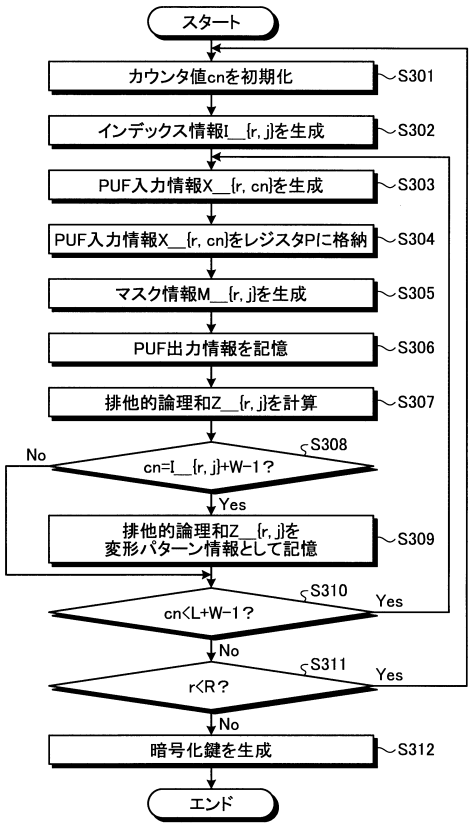
【図３】


スタート
PUF入力情報X__{r, cn}を生成
S201
マスク情報M__{r, j}を生成
S202
PUF出力情報を記憶
S203
参照情報を生成
S204
参照情報と
変形パターン情報とが
類似データか？
S205
No
Yes
インデックス情報I__{r, j}を再現
S206
j<N__r？
S207
Yes
No
k<L？
S208
Yes
No
r<R？
S209
Yes
No
暗号化鍵を生成
S210
エンド

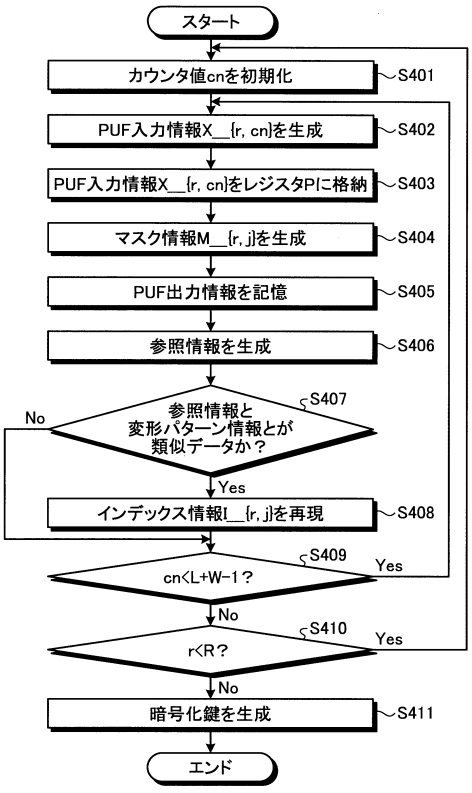
【図４】


1000
外部メモリ
1004
カウンタ
1005
レジスタS
(シフトレジスタ)
1003
比較回路
1012
1009
PUF演算回路
1006
マスク生成
回路
1008
インデックス
情報再現回路
1011
インデックス
情報生成回路
1010
暗号化鍵設定、
暗号化鍵再現
レジスタP
(PUF入力情報)
1002
PUF入力
生成回路
1007
レジスタI
(インデックス
情報)
1001
1013
鍵生成回路
1014
レジスタK
(暗号化鍵)
1015

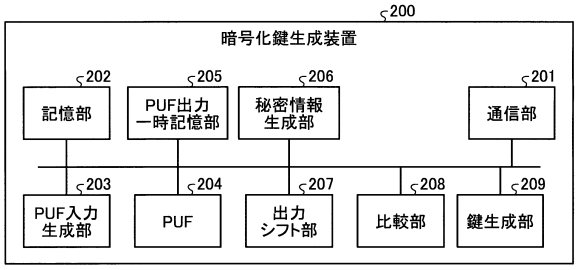
【図５】


スタート
カウンタ値cnを初期化
S301
インデックス情報I__{r, j}を生成
S302
PUF入力情報X__{r, cn}を生成
S303
PUF入力情報X__{r, cn}をレジスタPに格納
S304
マスク情報M__{r, j}を生成
S305
PUF出力情報を記憶
S306
排他的論理和Z__{r, j}を計算
S307
No
cn=I__{r, j}+W-1？
S308
Yes
排他的論理和Z__{r, j}を
変形パターン情報として記憶
S309
cn<L+W-1？
S310
Yes
No
r<R？
S311
Yes
No
暗号化鍵を生成
S312
エンド

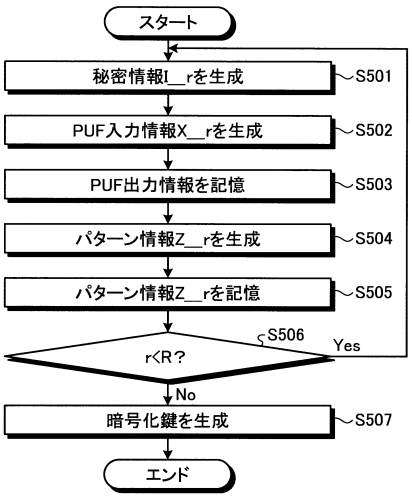
【図６】


スタート
カウンタ値cnを初期化
S401
PUF入力情報X__{r, cn}を生成
S402
PUF入力情報X__{r, cn}をレジスタPに格納
S403
マスク情報M__{r, j}を生成
S404
PUF出力情報を記憶
S405
参照情報を生成
S406
No
参照情報と
変形パターン情報とが
類似データか？
S407
Yes
インデックス情報I__{r, j}を再現
S408
cn<L+W-1？
S409
Yes
No
r<R？
S410
Yes
No
暗号化鍵を生成
S411
エンド

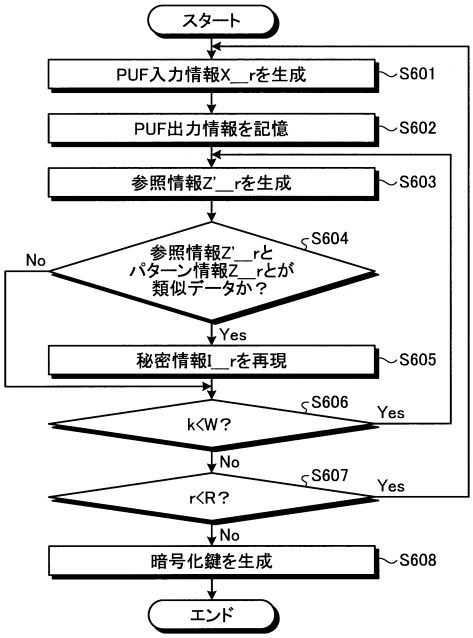
【図７】


200
暗号化鍵生成装置
202
記憶部
205
PUF出力一時記憶部
206
秘密情報生成部
201
通信部
203
PUF入力生成部
204
PUF
207
出力シフト部
208
比較部
209
鍵生成部

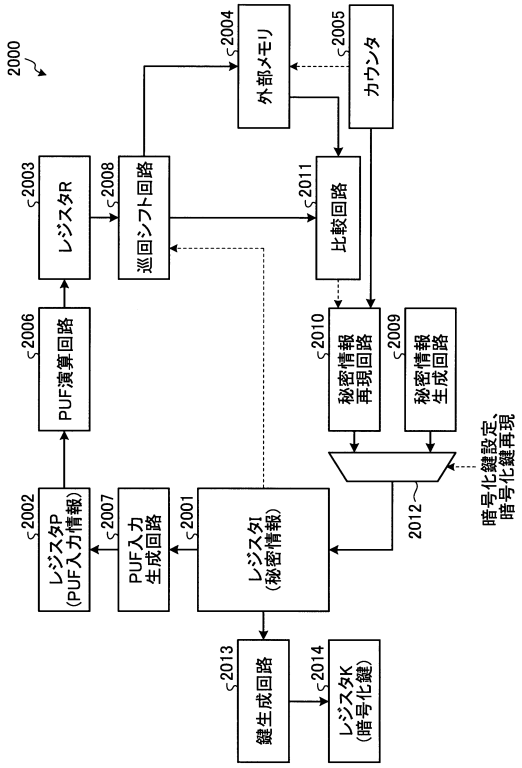
【図８】


スタート
秘密情報I__rを生成
S501
PUF入力情報X__rを生成
S502
PUF出力情報を記憶
S503
パターン情報Z__rを生成
S504
パターン情報Z__rを記憶
S505
S506
r<R?
Yes
No
暗号化鍵を生成
S507
エンド

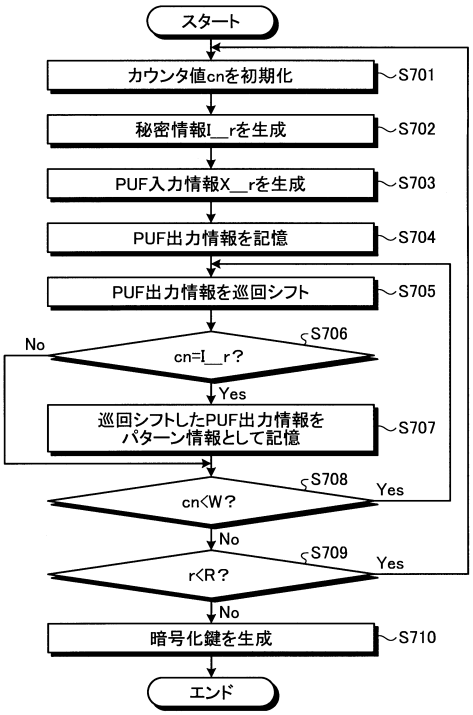
【図９】


スタート
PUF入力情報X__rを生成
S601
PUF出力情報を記憶
S602
参照情報Z'__rを生成
S603
S604
参照情報Z'__rとパターン情報Z__rとが類似データか？
No
Yes
秘密情報I__rを再現
S605
S606
k<W?
Yes
No
S607
r<R?
Yes
No
暗号化鍵を生成
S608
エンド

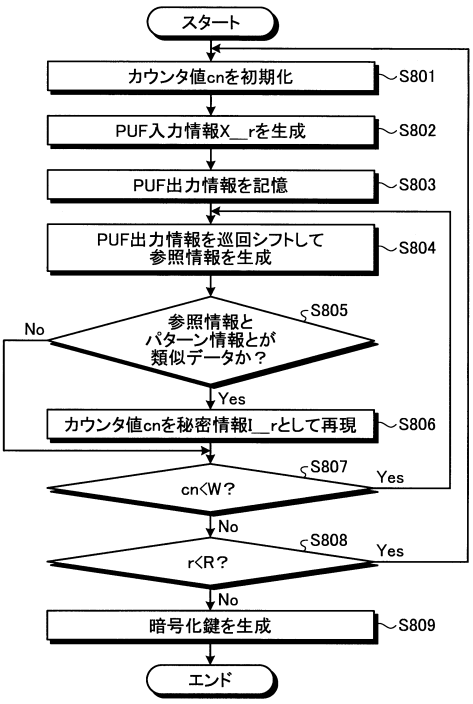
【図１０】


2000
2004
外部メモリ
2005
カウンタ
2003
レジスタR
2008
巡回シフト回路
2011
比較回路
2006
PUF演算回路
2010
秘密情報再現回路
2009
秘密情報生成回路
暗号化鍵設定、暗号化鍵再現
2012
2002
レジスタP(PUF入力情報)
2007
PUF入力生成回路
2001
レジスタI(秘密情報)
2013
鍵生成回路
2014
レジスタK(暗号化鍵)

【図１１】


スタート
カウンタ値cnを初期化
S701
秘密情報I__rを生成
S702
PUF入力情報X__rを生成
S703
PUF出力情報を記憶
S704
PUF出力情報を巡回シフト
S705
cn=I__r？
S706
No
Yes
巡回シフトしたPUF出力情報を
パターン情報として記憶
S707
cn<W？
S708
Yes
No
r<R？
S709
Yes
No
暗号化鍵を生成
S710
エンド

【図１２】


スタート
カウンタ値cnを初期化
S801
PUF入力情報X__rを生成
S802
PUF出力情報を記憶
S803
PUF出力情報を巡回シフトして
参照情報を生成
S804
参照情報と
パターン情報とが
類似データか？
S805
No
Yes
カウンタ値cnを秘密情報I__rとして再現
S806
cn<W？
S807
Yes
No
r<R？
S808
Yes
No
暗号化鍵を生成
S809
エンド

フロントページの続き

(72)発明者 ▲崎▼山 一男
東京都調布市調布ヶ丘１－５－１ 国立大学法人 電気通信大学内

審査官 打出 義尚

(56)参考文献 Zdenek Sid PARAL, Srinivas DEVADAS, Reliableand efficient puf-based key generation using pattern matching, In 2011 IEEE International Symposiumon Hardware-Oriented Security and Trust(HOST2011), IEEE, ２０１１年, pages 128-133, ＵＲＬ, http://people.csail.mit.edu/devadas/pubs/host2011.pdf

(58)調査した分野(Int.Cl., ＤＢ名)
Ｈ０４Ｌ ９／１０