(19)日本国特許庁(JP)　(12)特　許　公　報(B1)　(11)特許番号
特許第6187624号
(P6187624)
(45)発行日　平成29年8月30日(2017.8.30)　(24)登録日　平成29年8月10日(2017.8.10)

(51)Int.Cl.　　F I
G09C 1/00 (2006.01)　G09C 1/00 610A
G06F 21/60 (2013.01)　G06F 21/60 320

請求項の数 8　(全 19 頁)

(21)出願番号　特願2016-53737(P2016-53737)
(22)出願日　平成28年3月17日(2016.3.17)
審査請求日　平成29年1月10日(2017.1.10)

早期審査対象出願

(73)特許権者　000005234
富士電機株式会社
神奈川県川崎市川崎区田辺新田１番１号
(74)代理人　100107766
弁理士　伊東　忠重
(74)代理人　100070150
弁理士　伊東　忠彦
(72)発明者　高務　健二
神奈川県川崎市川崎区田辺新田１番１号
富士電機株式会社内

審査官　青木　重徳

最終頁に続く

(54)【発明の名称】情報処理装置、情報処理方法及びプログラム

(57)【特許請求の範囲】
【請求項１】
入力データをＡＥＳ方式で暗号化又は復号化する情報処理装置であって、
第１ラウンドの処理対象となる前記入力データのうち、４バイトのサブラウンドデータを選択する選択部と、
前記サブラウンドデータを１バイトのデータごとに、前記第１ラウンドの次のラウンドである第２ラウンドで用いられる鍵データの成分を含むテーブルに基づいて変換して、それぞれ、４バイトの変換データを生成する変換部と、
それぞれの前記変換データの排他的論理和を計算する排他的論理和計算部と
を含む情報処理装置。
【請求項２】
前記第１ラウンドで用いられる前記テーブルには、乱数成分が含まれ、
前記第２ラウンドで用いられるテーブルには、前記乱数成分を打ち消す打消成分が含まれる請求項１に記載の情報処理装置。
【請求項３】
前記変換部は、乱数成分を含む前記変換データと、前記乱数成分を打ち消す打消成分を含む前記変換データとを生成する請求項１又は２に記載の情報処理装置。
【請求項４】
前記情報処理装置は、組み込みシステムである請求項１に記載の情報処理装置。
【請求項５】

前記選択が行われると、ＳｈｉｆｔＲｏｗｓ関数を実行した処理結果と同様の処理結果が得られる請求項１に記載の情報処理装置。
【請求項６】
前記テーブルに基づく変換及び前記排他的論理和の計算が行われると、ＡｄｄＲｏｕｎｄＫｅｙ関数、ＳｕｂＢｙｔｅｓ関数及びＭｉｘＣｏｌｕｍｎｓ関数をそれぞれ実行した処理結果と同様の処理結果が含まれる請求項１に記載の情報処理装置。
【請求項７】
入力データをＡＥＳ方式で暗号化又は復号化し、演算装置及び記憶装置を有する情報処理装置が行う情報処理方法であって、
前記演算装置が、第１ラウンドの処理対象となり、前記記憶装置が記憶する前記入力データのうち、４バイトのサブラウンドデータを選択する選択手順と、
前記演算装置が、前記サブラウンドデータを１バイトのデータごとに、前記第１ラウンドの次のラウンドである第２ラウンドで用いられる鍵データの成分を含むテーブルに基づいて変換して、それぞれ、４バイトの変換データを生成する変換手順と、
前記演算装置が、それぞれの前記変換データの排他的論理和を計算する排他的論理和計算手順と
を含む情報処理方法。
【請求項８】
入力データをＡＥＳ方式で暗号化又は復号化し、演算装置及び記憶装置を有するコンピュータに情報処理方法を実行させるためのプログラムであって、
前記演算装置が、第１ラウンドの処理対象となり、前記記憶装置が記憶する前記入力データのうち、４バイトのサブラウンドデータを選択する選択手順と、
前記演算装置が、前記サブラウンドデータを１バイトのデータごとに、前記第１ラウンドの次のラウンドである第２ラウンドで用いられる鍵データの成分を含むテーブルに基づいて変換して、それぞれ、４バイトの変換データを生成する変換手順と、
前記演算装置が、それぞれの前記変換データの排他的論理和を計算する排他的論理和計算手順と
を実行させるためのプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、情報処理装置、情報処理方法及びプログラムに関する。
【背景技術】
【０００２】
従来、データの暗号化及び復号化の方式として、ＦＩＰＳ（Ｆｅｄｅｒａｌ　Ｉｎｒｍａｔｉｏｎ　Ｐｒｏｃｅｓｓｉｎｇ　Ｓｔａｎｄａｒｄ）１９７（アメリカ国立標準技術研究所、２００１年公表）で定められているＡＥＳ（Ａｄｖａｎｃｅｄ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）方式が知られている。
【０００３】
また、ＡＥＳ方式において、セキュリティを向上させるための方法として、ホワイトボックスクリプトグラフィ（Ｗｈｉｔｅ－Ｂｏｘ　Ｃｒｙｐｔｏｇｒａｐｈｙ）が知られている（例えば、非特許文献１及び非特許文献２等）。
【０００４】
さらに、入力に依存する符号化を行うホワイトボックスクリプトグラフィが知られている。具体的には、まず、システムが、暗号化に用いられる鍵を示す複数の基本ブロックから構成するネットワークを備える。そして、基本ブロックが、入力データを出力データにマッピングする。さらに、ネットワークが、複数の基本ブロックのうちの第１基本ブロックからの出力データを選択された符号化方式に従って符号化する。また、符号化方式の選択は、入力メッセージに依存するようにする。その上、符号化の影響を補償するため、システムが、複数の再復号化方式のうちから選択される再復号化方式に従って中間データを

再符号化する補償器を有する。このようにして、リバースエンジニアリングに対して、複雑化させる方法が知られている（例えば、特許文献１等）。

【先行技術文献】

【非特許文献】

【０００５】

【非特許文献１】"Ｗｈｉｔｅ－Ｂｏｘ Ｃｒｙｐｔｏｇｒａｐｈｙ ａｎｄ ａｎ ＡＥＳ Ｉｍｐｌｅｍｅｎｔａｔｉｏｎ."Ｓ．Ｃｈｏｗ，Ｐ．Ｅｉｓｅｎ，Ｈ．Ｊｏｈｎｓｏｎ，Ｐ．Ｃ．ｖａｎ Ｏｏｒｓｃｈｏｔ．Ｉｎ ９ｔｈ Ａｎｎｕａｌ Ｗｏｒｋｓｈｏｐ ｏｎ Ｓｅｌｅｃｔｅｄ Ａｒｅａｓ ｉｎ Ｃｒｙｐｔｏｇｒａｐｈｙ（ＳＡＣ ２００２），Ａｕｇ．１５－１６ ２００２．

【非特許文献２】"Ａ Ｔｕｔｏｒｉａｌ ｏｎ Ｗｈｉｔｅ－ｂｏｘ ＡＥＳ."Ｊａｍｅｓ Ａ．Ｍｕｉｒ．Ａｄｖｎｃｅｓ ｉｎ Ｎｅｔｗｏｒｋ Ａｎａｌｙｓｉｓ ａｎｄ ｉｔｓ Ａｐｐｌｉｃａｔｉｏｎｓ，Ｍａｔｈｅｍａｔｉｃｓ ｉｎ Ｉｎｄｕｓｔｒｙ １８（２０１３），２０９－２２９．

【特許文献】

【０００６】

【特許文献１】特表２０１２－５２０５８９号公報

【発明の概要】

【発明が解決しようとする課題】

【０００７】

しかしながら、従来の方法では、ＡＥＳ方式において、入力と出力の関係から解析を行う方法等が用いられると、データが解読される場合があり、データの難読化ができていない場合がある。

【０００８】

本発明の１つの側面は、ＡＥＳ方式において、データを難読化することを目的とする。

【課題を解決するための手段】

【０００９】

一態様における、入力データをＡＥＳ方式で暗号化又は復号化する情報処理装置は、

第１ラウンドの処理対象となる前記入力データのうち、４バイトのサブラウンドデータを選択する選択部と、

前記サブラウンドデータを１バイトのデータごとに、前記第１ラウンドの次のラウンドである第２ラウンドで用いられる鍵データの成分を含むテーブルに基づいて変換して、それぞれ、４バイトの変換データを生成する変換部と、

それぞれの前記変換データの排他的論理和を計算する排他的論理和計算部と

を含む。

【発明の効果】

【００１０】

ＡＥＳ方式において、データを難読化することができる。

【図面の簡単な説明】

【００１１】

【図１】本発明の一実施形態に係る組み込みシステムのハードウェア構成の一例を説明するブロック図である。

【図２】本発明の一実施形態に係る暗号化の１ラウンド当たりの処理の一例を説明するフローチャートである。

【図３】本発明の一実施形態に係る最初のラウンドの処理の一例を説明する模式図である。

【図４】本発明の一実施形態に係るテーブルに含まれる鍵データの一例を説明する模式図である。

【図５】本発明の一実施形態に係るテーブルに含まれる乱数成分の一例を説明する模式図である。

【図６】本発明の一実施形態に係る中間のラウンドの処理の一例を説明する模式図（その１）である。
【図７】本発明の一実施形態に係る中間のラウンドの処理の一例を説明する模式図（その２）である。
【図８】本発明の一実施形態に係る最終のラウンドの処理の一例を説明する模式図である。
【図９】ホワイトボックスクリプトグラフィの一例の原理を示す概念図である。
【図１０】ホワイトボックスクリプトグラフィにおけるラウンド処理の一例を示す模式図である。
【図１１】比較例に係る暗号化の１ラウンド当たりの処理の一例を説明する模式図（その１）である。
【図１２】比較例に係る暗号化の１ラウンド当たりの処理の一例を説明する模式図（その２）である。
【図１３】比較例に係るＬＵＴのデータ容量の一例を示す表である。
【図１４】本発明の一実施形態に係る組み込みシステムの機能構成の一例を示す機能ブロック図である。
【発明を実施するための形態】
【００１２】
情報処理装置は、例えば、組み込みシステム（Ｅｍｂｅｄｄｅｄ　ｓｙｓｔｅｍ）である。組み込みシステムは、産業機器又は家電製品等に内蔵され、特定の機能を実現するためのシステムである。なお、情報処理装置は、ＰＣ（Ｐｅｒｓｏｎａｌ　Ｃｏｍｐｕｔｅｒ）等でもよい。以下、本発明の実施形態を図面に基づいて、情報処理装置が組み込みシステムである例で説明する。
【００１３】
１．組み込みシステムのハードウェア構成例
２．組み込みシステムによる全体処理例
３．組み込みシステムの機能構成例
＜＜１．組み込みシステムのハードウェア構成例＞＞
図１は、本発明の一実施形態に係る組み込みシステムのハードウェア構成の一例を説明するブロック図である。図示するように、組み込みシステム１は、演算装置ＨＷ１と、記憶装置ＨＷ２と、Ｉ／Ｆ（ｉｎｔｅｒｆａｃｅ）ＨＷ３とを有する。
【００１４】
演算装置ＨＷ１は、ＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）又はＭＰＵ（Ｍｉｃｒｏ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）等である。また、演算装置ＨＷ１は、組み込みシステム１が行う処理の全部又は一部を実現するための演算と、データの加工とを行う演算装置並びに組み込みシステム１が有するハードウェアを制御する制御装置である。さらに、演算装置ＨＷ１は、例えば、図示するように、ＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）ＨＷ１０及びＲＯＭ（Ｒｅａｄ－Ｏｎｌｙ　Ｍｅｍｏｒｙ）ＨＷ１１等の記憶装置を内蔵し、これらの記憶装置によって記憶領域を実現する。
【００１５】
ＲＡＭＨＷ１０は、演算装置ＨＷ１等が用いるプログラム、設定値又はデータ等を展開及び記憶するために用いられる記憶装置である。
【００１６】
ＲＯＭＨＷ１１は、演算装置ＨＷ１等が用いるプログラム、設定値又はデータ等を記憶する記憶装置である。
【００１７】
記憶装置ＨＷ２は、いわゆるメモリ（ｍｅｍｏｒｙ）等である。また、記憶装置ＨＷ２は、組み込みシステム１が用いるプログラム、設定値又はデータ等を記憶する主記憶装置である。なお、記憶装置ＨＷ２は、補助記憶装置等を有してもよい。
【００１８】

Ｉ／ＦＨＷ３は、組み込みシステム１にデータ等を入出力するインタフェースである。Ｉ／ＦＨＷ３は、バス、コネクタ、ケーブル及びドライバ等で実現される。

【００１９】

なお、組み込みシステム１のハードウェア構成は、図示する構成に限られない。例えば組み込みシステム１は、記憶装置ＨＷ２を有さなくともよい。また、組み込みシステム１は、更に演算装置等の補助装置を外部又は内部に有してもよい。

【００２０】

＜＜２．組み込みシステムによる全体処理例＞＞

本発明の実施形態に係る組み込みシステムは、データを暗号化又は復号化する。以下、組み込みシステムがデータを暗号化する場合を例に説明する。

【００２１】

図２は、本発明の一実施形態に係る暗号化の１ラウンド当たりの処理の一例を説明するフローチャートである。以下、ＡＥＳ方式において、処理の単位となる１６バイト（ｂｙｔｅ）の入力データに対する処理単位（以下「１ラウンド（ｒｏｕｎｄ）」という。）について説明する。なお、１ラウンド当たりの処理は、ＡＥＳ方式に用いられる鍵のビット（ｂｉｔ）長等に合わせて、繰り返し行われる。

【００２２】

また、以下の説明では、１ラウンド当たりの処理は、１６バイトのうち、選択される４バイトのデータを処理単位（以下「１サブラウンド（ｓｕｂ－ｒｏｕｎｄ）」という。）にする１サブラウンド当たりの処理が繰り返し行われる。つまり、１ラウンド当たりの処理では、４サブラウンドの処理が繰り返し行われる（４バイト（１サブラウンド）×４サブラウンド＝１６バイト、１ラウンド）。そして、１ラウンド当たりの処理は、図示する処理又は図示する処理と等価の処理である。

【００２３】

＜＜サブラウンドデータの選択例（ステップＳ０１０１）＞＞

ステップＳ０１０１では、組み込みシステムは、サブラウンドデータを選択する。すなわち、ステップＳ０１０１によって、入力される１６バイトの入力データのうち、４バイトのデータ（以下「サブラウンドデータ」という。）が選択される。なお、ステップＳ０１０１は、いわゆる「ＳｈｉｆｔＲｏｗｓ」に相当する処理である。以下、ステップＳ０１０１で選択される４バイトのデータのうち、１バイトのデータごとに行われる処理を説明する。すなわち、それぞれの１バイトのデータに対して、４回同様の処理が行われると、１サブラウンド当たりの処理となる。

【００２４】

＜＜テーブルに基づく変換例（ステップＳ０１０２）＞＞

ステップＳ０１０２では、組み込みシステムは、テーブルに基づいて変換を行う。なお、テーブルは、いわゆるＬＵＴ（Ｌｏｏｋ　Ｕｐ　Ｔａｂｌｅ）等である。テーブルについての詳細は、後述する。以下、ステップＳ０１０２による変換によって、生成されるデータを「変換データ」という。なお、変換データは、１バイトの入力に対して、１バイトを４つ、すなわち、４バイトとなる。

【００２５】

＜＜排他的論理和（ＸＯＲ、ｅｘｃｌｕｓｉｖｅ　ｏｒ）の計算例（ステップＳ０１０３）＞＞

ステップＳ０１０３では、組み込みシステムは、変換データの排他的論理和を計算する。なお、ステップＳ０１０２及びステップＳ０１０３は、いわゆる「ＡｄｄＲｏｕｎｄＫｅｙ」、「ＳｕｂＢｙｔｅｓ」及び「ＭｉｘＣｏｌｕｍｎｓ」に相当する処理である。

【００２６】

例えば、組み込みシステムは、図２に示す処理を以下のようなテーブルを用いて行う。

【００２７】

なお、以下の説明では、ラウンド数を「ｒ」で示し、「ｒ＝１」（初期値）から順に「ｒ＝Ｒ」まで、１ラウンド当たりの処理が繰り返し行われる例を説明する。すなわち、最

初に行われるラウンド（以下「最初のラウンド」という。）は、「ｒ＝１」とする。そして、最後に行われるラウンド（以下「最後のラウンド」という。）は、「ｒ＝Ｒ」とする。さらに、最初のラウンド及び最後のラウンド以外のラウンド（以下「中間のラウンド」という。）は、「ｒ＝２」乃至「ｒ＝Ｒ－１」とする。なお、鍵長によって、中間のラウンドの数が変化する。

【００２８】

最初のラウンドは、前に行われるラウンドがないラウンドである。一方で、最後のラウンドは、次に行われるラウンドがないラウンドである。これに対して、中間のラウンドは、前後に行われるラウンドがあるラウンドである。これらの点に対応するため、最初のラウンド、中間のラウンド及び最後のラウンドで行われるそれぞれの処理は、処理内容が異なる。そのため、以下の説明では、最初のラウンドと、中間のラウンドと、最後のラウンドとで行われるそれぞれの処理を分けて模式図を用いて説明する。

【００２９】

＜＜最初のラウンドの処理例＞＞

図３は、本発明の一実施形態に係る最初のラウンドの処理の一例を説明する模式図である。図示する処理では、最初のラウンドにおいて、まず、１ラウンド当たりの処理対象となる１６バイトのデータ（以下「入力データＤ＿ＩＮ」という。）から、組み込みシステムは、４つの１バイトのデータを選択する。そして、図は、組み込みシステムが、サブラウンドデータが有する１バイトのデータにそれぞれ行う処理の例を示す。具体的には、図示する例では、「０」乃至「１５」の１バイトのデータから構成される入力データＤ＿ＩＮから、第０番目データＤ＿１Ｂ０、第５番目データＤ＿１Ｂ５、第１０番目データＤ＿１Ｂ１０及び第１５番目データＤ＿１Ｂ１５の１バイトのデータが、それぞれ選択される例である。以下の説明では、サブラウンドデータのうち、第０番目データＤ＿１Ｂ０の１バイトのデータに対する処理を例に説明する。

【００３０】

なお、入力データＤ＿ＩＮから４つの１バイトのデータを選択する処理は、「ＳｈｉｆｔＲｏｗｓ」の処理に相当し、図２に示すステップＳ０１０１の処理に相当する。

【００３１】

次に、組み込みシステムは、第０番目データＤ＿１Ｂ０を、あらかじめ記憶されるテーブルＴＢに基づいて、変換する。そして、テーブルＴＢによる変換によって、１バイトの変換データが、４つ生成される。次に、組み込みシステムは、第０番目データＤ＿１Ｂ０、第５番目データＤ＿１Ｂ５、第１０番目データＤ＿１Ｂ１０及び第１５番目データＤ＿１Ｂ１５のそれぞれの変換データの１バイトずつの排他的論理和ＰＸを計算する。このように計算すると、組み込みシステムは、出力データＤ＿ＯＵＴのうち、第０番目出力データＤＯＵＴ０を出力できる。

【００３２】

同様に、図示するように、第０番目データＤ＿１Ｂ０、第５番目データＤ＿１Ｂ５、第１０番目データＤ＿１Ｂ１０及び第１５番目データＤ＿１Ｂ１５のそれぞれの変換データの１バイトずつの排他的論理和ＰＸを計算すると、組み込みシステムは、出力データＤ＿ＯＵＴのうち、第１番目出力データＤＯＵＴ１、第２番目出力データＤＯＵＴ２及び第３番目出力データＤＯＵＴ３をそれぞれ出力できる。

【００３３】

図３では、「Ｓ」は、Ｓ－ＢＯＸによる変換、すなわち、「ＳｕｂＢｙｔｅｓ」関数の実行と同様の成分を示す。また、「・０３」、「・０２」及び「・０１」は、ＡＥＳ既約多項式に基づくかけ算を示す。すなわち、例えば、「・０３」は、ＡＥＳ既約多項式に基づくかけ算で「３倍」を示す。さらに、「ｐ」は、次のラウンドで用いられる鍵データの一部又は全部を含む鍵データを示す。また、「ｋ」及び「ｉ」については、後述の中間のラウンド（図６参照）で説明する。以下、同様に記載する。

【００３４】

なお、テーブルＴＢによる変換は、図２に示すステップＳ０１０２に相当する。また、

排他的論理和ＰＸによる計算は、図２に示すステップＳ０１０３に相当する。さらに、テーブルＴＢには、最初のラウンドとは異なるラウンドで用いられる鍵データＤ＿Ｋが含まれる。例えば、第１ラウンドを「ｒ＝１」のラウンドとすると、第２ラウンドは、第１ラウンドの次に行われるラウンドであり、「ｒ＝２」のラウンド等である。これを図示すると、以下のように示せる。

【００３５】

図４は、本発明の一実施形態に係るテーブルに含まれる鍵データの一例を説明する模式図である。図は、第１ラウンドと、第２ラウンドとで行われるそれぞれの１サブラウンド当たりの処理において行われるテーブルＴＢによる変換の処理例を示す。なお、第１ラウンドは、例えば、図３に示すような最初のラウンド等である。一方で、第２ラウンドは、「ｒ＝２」等のラウンドである。

【００３６】

図示するように、第１ラウンドで用いられるテーブルＴＢには、第２ラウンドで用いられる鍵データが含まれる。例えば、第１ラウンドで用いられるテーブルＴＢには、あらかじめ、第２ラウンドで用いられる鍵データが含まれるように、生成される。このように、異なるラウンドの鍵データの全部又は一部をテーブルＴＢに含ませると、組み込みシステムは、第１ラウンドにおいて、第１ラウンド用のテーブルＴＢを解析しても、第１ラウンド用の鍵データを推定するのを難しくできる。すなわち、鍵データは、他のラウンドから入ってくる部分があると、組み込みシステムは、鍵データを推定するために行われる鍵データが有する１バイト当たりのデータを探索する処理量を多くすることができる。

【００３７】

図示する例では、第２ラウンドで用いられる４つの鍵データは、第０番目データに係る処理で用いられるテーブルＴＢにすべて入力される。例えば、このように、他のラウンドの鍵データＤ＿Ｋが含まれた鍵データが使用された場合と同様となるように、テーブルＴＢは、あらかじめ生成される。

【００３８】

ただし、本発明に係る実施形態は、これに限られない。例えば、組み込みシステムは、他のラウンドの鍵データをビット単位で、テーブルＴＢに分散させて入力させてもよい。このようにすると、鍵データを推定する場合において、他のラウンドから、鍵データの行き先は、「入力しない」と、４つ（１バイト×４通り）のテーブルとを合わせた５通りとされる。そして、他のラウンドの鍵データがビット単位で分散されて含まれるので、８ビットの場合には、他のラウンドの鍵データの行き先は、「5^{8}」の組み合わせとなる。これが１ラウンド当たりの処理では、組み込みシステムは、４つの１バイトのデータにそれぞれ当てはまるので、「$5^{8\times4}=5^{32}$」の組み合わせとすることができる。

【００３９】

このようにすると、暗号化処理における入力と出力の関係を解析し、データ等を解読しようとする方法に対して、組み込みシステムは、データを難読化させることができる。例えば、入力と、出力との関係から解析し、データを解読しようとする方法は、いわゆるＢＧＥアタック（「入出力対応攻撃」等という場合もある。）等である。より具体的には、ＢＧＥアタックは、例えば、「"Ｃｒｙｐｔａｎａｌｙｓｉｓ ｏｆ ａ Ｗｈｉｔｅ Ｂｏｘ ＡＥＳ Ｉｍｐｌｅｍｅｎｔａｔｉｏｎ." Ｏｌｉｖｉｅｒ Ｂｉｌｌｅｔ, Ｈｅｎｒｉ Ｇｉｌｂｅｒｔ, Ｃｈａｒａｆ Ｅｃｈ－Ｃｈａｔｂｉ, Ｓｅｌｅｃｔｅｄ Ａｒｅａｓ ｉｎ Ｃｒｙｐｔｏｇｒａｐｈｙ：１１ｔｈ Ｉｎｔｅｒｎａｔｉｏｎａｌ Ｗｏｒｋｓｈｏｐ, ＳＡＣ ２００４.」に記載されている方法等である。

【００４０】

図３に示す例では、ＢＧＥアタックがされると、入力の例である第０番目データＤ＿１Ｂ０と、出力の例である１バイトの出力データＤＯＵＴ０との関係から、入力と出力の間でどのような処理が行われているか等が解析される。すなわち、入力と出力の間で行われる処理を入力されたデータがどのような出力となるかに基づいて、鍵データ又は行われる処理内容を推測する方法がある。

【００４１】
これに対して、本発明に係る実施形態では、図４に示すように、組み込みシステムは、第１ラウンドに係る処理に、第２ラウンドで用いられる鍵データを含むテーブルＴＢを用いて、変換する処理を行う。すなわち、組み込みシステムは、あらかじめ生成されるテーブルＴＢに基づいて、変換を行う。そのため、ＢＧＥアタック等によって、テーブルＴＢ等が解析されても、組み込みシステムは、第１ラウンド用の鍵データが推測されるのを難しくできる。すなわち、図４に示すように、第１ラウンドに係る処理に、第２ラウンドで用いられる鍵データを含ませて処理を行うと、組み込みシステムは、ＢＧＥアタック等に対しても、鍵データを難読化することができる。このようにして、組み込みシステムは、ＡＥＳ方式において、データを難読化することができる。なお、乱数成分ＲＰは、例えば、乱数を生成する関数等を実行して生成される。
【００４２】
さらに、図２に示すように、ステップＳ０１０１及びステップＳ０１０３以外の処理は、１回のテーブルに基づく変換で行うようにすると、組み込みシステムは、行う処理の数を少なくできる。すなわち、１テーブル当たりに含まれる処理が多いと、セキュリティを破る目的等で、鍵データ又は行われている処理の解析の難易度を向上させることができる。このようにして、組み込みシステムは、セキュリティを向上させることができる。また、処理の数は、少ない方が処理負荷が軽くできる場合が多い。
【００４３】
なお、図４及び図５では、「Ｐ」は、前のラウンド（当ラウンドが最初のラウンドでないとする。）で行われた出力の際の変換（図３の例では、出力結果を出力データＤ＿ＯＵＴにおいて第０番目、第１番目、第２番目及び第３番目とする処理）（後述する図１２に示す比較例では、「Ｑ」に相当する処理）に対応する、当ラウンドで行う逆変換を示す。すなわち、前のラウンドで行われた「出力の際の変換」を「変換」とすると、「Ｐ」は、前のラウンドで「出力の際の変換」の「逆変換」を示す。
【００４４】
また、「ｆ」は、図３に示す「ｉ」及び「ｈ」を合わせた成分に相当する。なお、図４に示すように、「ｆ」、すなわち、「ｉ」及び「ｈ」は、１バイトを分割して、４ビットごとに変換されてもよい。
【００４５】
さらにまた、図３に示すように、テーブルＴＢには、乱数成分ＲＰが含まれるのが望ましい。このように、乱数成分ＲＰが含まれると、組み込みシステムは、ＡＥＳ方式において、データをより難読化することができる。これを図示すると、以下のように示せる。
【００４６】
図５は、本発明の一実施形態に係るテーブルに含まれる乱数成分の一例を説明する模式図である。図は、図４と同様に、第１ラウンドと、第２ラウンドとで行われるそれぞれの１サブラウンド当たりの処理において用いられるテーブルＴＢの例を示す。図示するように、第１ラウンドでは、組み込みシステムは、テーブルＴＢに乱数成分ＲＰが含まれるようにする。例えば、テーブルＴＢは、あらかじめ、乱数成分ＲＰを含むように、生成される。すなわち、例えば、乱数成分ＲＰを含むテーブルＴＢを生成するには、テーブルＴＢを示すデータを生成する際に、まず、乱数を発生させるランダム関数等を情報処理装置が実行して、乱数を発生させる。次に、情報処理装置は、発生した乱数が打ち消されるような成分（以下「打消成分ＣＰ」という。）を生成する。なお、図５では、「Ｒ」は、打消成分ＣＰを示す。
【００４７】
そして、図示するように、第１ラウンド用のテーブルＴＢに、乱数成分ＲＰが含まれるように、情報処理装置は、第１ラウンド用のテーブルＴＢを生成する。そのため、第１ラウンドで、乱数成分ＲＰが含まれるテーブルによる変換が行われた場合には、第１ラウンドで生成される変換データは、乱数成分ＲＰを有する。そこで、情報処理装置は、第１ラウンド用のテーブルＴＢに含まれた乱数成分ＲＰを打ち消す打消成分ＣＰが含まれるよう

に、第２ラウンド用のテーブルを生成する。このようにすると、第１ラウンドの変換で含まれた乱数成分ＲＰは、第２ラウンドの変換が行われると、打ち消される。

【００４８】

また、このように、乱数成分ＲＰが含まれるようにすると、データを解析するのに乱数成分ＲＰを解析する処理が必要となるため、組み込みシステムは、ＡＥＳ方式において、データをより難読化することができる。なお、図示する例では、乱数成分ＲＰは、「$2^{8\times 4}=2^{32}$」の組み合わせがある成分である。

【００４９】

なお、打消成分ＣＰは、第２ラウンド用のテーブルに入力されるに限られない。例えば、１ラウンド中に、サブラウンドデータに対して行われる４つの１バイトに対する変換のうち、３つの変換で、乱数成分ＲＰが含まれるテーブルが用いられ、残りの１つの処理で用いられるテーブルに打消成分ＣＰが含まれてもよい。このようにしても、組み込みシステムは、テーブルに乱数成分ＲＰが含まれるようにすることができ、ＡＥＳ方式において、データをより難読化することができる。

【００５０】

次に、図３に示すように、組み込みシステムは、各変換データのうち、それぞれの１バイトデータを１つずつ集め、計４つの１バイトデータに対して、排他的論理和ＰＸを計算して、出力データＤＯＵＴのうち、１バイトを生成する。図示するように、組み込みシステムが、１つのサブラウンドデータに対して、排他的論理和ＰＸまで行うと、組み込みシステムは、「ＤＯＵＴ０」、「ＤＯＵＴ１」、「ＤＯＵＴ２」及び「ＤＯＵＴ３」の１バイトデータを４つ生成することができる。

【００５１】

なお、テーブルＴＢに基づく変換及び排他的論理和ＰＸの計算は、「ＡｄｄＲｏｕｎｄＫｅｙ」、「ＳｕｂＢｙｔｅｓ」及び「ＭｉｘＣｏｌｕｍｎｓ」の処理に相当する。また、テーブルＴＢに基づく変換は、図２に示すステップＳ０１０２の処理に相当する。さらに、各変換データの排他的論理和ＰＸを計算する処理は、図２に示すステップＳ０１０３の処理に相当する。

【００５２】

なお、最初のラウンドの処理における鍵１バイトに対するテーブルの組み合わせは、図示するように、約「$2^{167.50}$」通りとなる。

【００５３】

＜＜中間のラウンドの処理例＞＞

図６は、本発明の一実施形態に係る中間のラウンドの処理の一例を説明する模式図（その１）である。なお、図示する処理は、図３に示す処理の次のラウンドである例とする。以下、図３に示す処理と異なる点を中心に説明する。

【００５４】

図示する処理は、図３に示す処理と比較すると、入力の際に、「$h_{r,0}^{-1}$」、「$h_{r,5}^{-1}$」、「$h_{r,10}^{-1}$」及び「$h_{r,15}^{-1}$」が含まれる点が異なる。この「$h_{r,0}^{-1}$」、「$h_{r,5}^{-1}$」、「$h_{r,10}^{-1}$」及び「$h_{r,15}^{-1}$」は、図３に示すテーブルＴＢによる変換による「ｈ」の逆変換となる成分の例である。なお、図では、「ｈ」は、ビットの並び替えを示し、排他的論理和に影響のない成分を示す。具体的には、「ｈ」によるビットの並び替えがされると、データ内のビットが並び替えられる。なお、８ビットの場合には、「ｈ」による並び替えは、「８！（階乗）」通りの組み合わせがある。これに対して、「h^{-1}」は、「ｈ」による並び替えを元に戻す並び替え（「ｈ」によって並び替えられる前に戻す）をすることを示す。そのため、「ｈ」及び「h^{-1}」の両方の成分があると、「ｈ」による並び替えがない場合と、同様の結果が得られる。

【００５５】

また、図示する処理は、図３に示す処理と比較すると、入力の際に、「$i_{r,0}$」、「$i_{r,5}$」、「$i_{r,10}$」及び「$i_{r,15}$」が含まれる点が異なる。この「$i_{r,0}$

」、「$i_{r,5}$」、「$i_{r,10}$」及び「$i_{r,15}$」は、図５に示すように、第１ラウンドでテーブルＴＢ（図５）に含まれる乱数成分ＲＰを打ち消す打消成分ＣＰの例である。例えば、「ｉ」は、乱数の排他的論理和による加算を示す。

【００５６】

また、図６では、「ｑ」は、当ラウンドの鍵データの成分を示す。詳しくは、鍵データの成分のうち、一部の成分は、前のラウンドに入力される場合がある。その場合において、「ｑ」は、前のラウンドに入力されず、残った成分を示す。なお、前のラウンドに、当ラウンドの鍵データの成分を入力しない場合には、当ラウンドの鍵データの全成分が残ることになる。一方で、図３、すなわち、最初のラウンドでは、前のラウンドがないため、「ｋ」で示す。さらに、「h^{-1}」、「ｉ」及び「ｑ」は、添え字で対応するラウンド及び入力データを示す。具体的には、「$h_{r,0}^{-1}$」の場合には、「ｒ」は、第１ラウンド、すなわち、前のラウンドを示し、「ｒ＋１」は、第２ラウンド、すなわち、当ラウンドを示す。「０」は、図示するように、入力データの０番目に対応することを示す。

【００５７】

さらに、図示する処理は、最初のラウンドの処理（図３参照）と同様に、「$p_{r+1,0,0}$」等のように、異なるラウンドで用いられる鍵データがテーブルに含まれる。第２ラウンドの場合には、異なるラウンドは、例えば、第３ラウンドのことである。このようにして、組み込みシステムは、異なるラウンドで用いられる鍵データを含ませて処理を行うと、最初のラウンドの処理と同様に、ＢＧＥアタック等に対してもデータを難読化することができる。

【００５８】

なお、中間のラウンドの処理における鍵１バイトに対するテーブルの組み合わせは、図示するように、約「$2^{209.37}$」通りとなる。

【００５９】

また、図６の次のサブラウンドでは、例えば、以下のように処理が行われる。

【００６０】

図７は、本発明の一実施形態に係る中間のラウンドの処理の一例を説明する模式図（その２）である。図７に示す処理は、図６と同様のラウンドにおいて、図６に示す処理の次のサブラウンドで行われる処理の例である。図示する例は、図６と比較すると、入力データから選択されるサブラウンドデータが異なる。図６と同様に、各サブラウンドデータが処理されるため、組み込みシステムは、最初のラウンドの処理及び図６に示す中間のラウンドの処理と同様に、ＢＧＥアタック等に対してもデータを難読化することができる。

【００６１】

＜＜最後のラウンドの処理例＞＞

図８は、本発明の一実施形態に係る最終のラウンドの処理の一例を説明する模式図である。なお、図示する処理は、図６及び図７に示す処理と比較すると、テーブルによる、「ＭｉｘＣｏｌｕｍｎｓ」に相当する処理がない点が異なる。また、図示する処理では、「ＡｄｄＲｏｕｎｄＫｅｙ」に相当する処理が２回行われる点が異なる。

【００６２】

最後のラウンドは、次のラウンドがないラウンドである。そのため、最後のラウンドの処理では、図３、図６及び図７に示す処理のように、後段のラウンドから鍵データが入力されない。ゆえに、最後のラウンドの処理は、前のラウンド（中間のラウンド等）に鍵データを入力し、一方で、後段のラウンドからの鍵データをテーブルに含ませて行う「ＭｉｘＣｏｌｕｍｎｓ」に相当する処理を行わない。

【００６３】

図９は、ホワイトボックスクリプトグラフィの一例の原理を示す概念図である。図示するように、暗号化処理は、入力データ（平文の状態のデータである。）に対して、「拡大鍵」等の鍵データを用いて暗号化し、出力データ（暗号文の状態のデータである。）を生成する処理である。そして、暗号化処理において、まず、鍵に対してアクセスを難しくするためのブラックボックス（Ｂｌａｃｋ－Ｂｏｘ）的アプローチがある。一方で、暗号化

処理において、鍵に対してアクセスされても、鍵と認識されるのを難しくするためのホワイトボックス（Ｗｈｉｔｅ－Ｂｏｘ）的アプローチがある。ホワイトボックスクリプトグラフィは、ホワイトボックス的アプローチの方法である。

【００６４】

図示するように、ホワイトボックスクリプトグラフィでは、暗号化における各処理と鍵データ（拡大鍵）とを合成して、演算をＬＵＴによる変換とする。特に、本発明に係る実施形態のように、複数の演算を１つのＬＵＴで行うと、複数の演算を行う場合よりも、処理負荷が小さくできる。そのため、ＬＵＴ等のテーブルによる変換を用いるのは、より組み込みシステム等には望ましい。そして、ホワイトボックスクリプトグラフィでは、図示するように、各処理の間（図では「処理Ａ」と「処理Ｂ」の間）に変換と、逆変換が挿入される。このように、ホワイトボックスクリプトグラフィは、変換と逆変換をＬＵＴに追加合成することにより、データを難読化する方法である。すなわち、図示する例では、テーブルは、「変換」と、「逆変換」と、「処理」とを１回の変換で行うように生成される。これを模式図で示すと、例えば、以下のように示せる。

【００６５】

図１０は、ホワイトボックスクリプトグラフィにおけるラウンド処理の一例を示す模式図である。図示するようなラウンド処理が、鍵長に合わせて繰り返し行われる。図示するように、１ラウンド当たりの処理では、サブラウンドデータに対して、「ＳｈｉｆｔＲｏｗｓ」、「ＡｄｄＲｏｕｎｄＫｅｙ」、「ＳｕｂＢｙｔｅｓ」及び「ＭｉｘＣｏｌｕｍｎｓ」の処理が行われる。図２に示す全体処理が行われると、図示する処理が行われた場合と、等価の処理結果となる。

【００６６】

＜＜比較例＞＞

図１１は、比較例に係る暗号化の１ラウンド当たりの処理の一例を説明する模式図（その１）である。図１１は、入力データＤ＿ＩＮのうち、４つの１バイトのデータに対して処理が行われ、出力データＤ＿ＯＵＴのうち、４つの１バイトのデータが生成される１サブラウンド当たりの処理の一例を示す。また、図１１に示す処理、すなわち、１ラウンド当たりの処理では、４サブラウンドの処理が繰り返し行われる。以下、１サブラウンド当たりの処理を中心に説明する。

【００６７】

ステップＳ０２０１では、４つの１バイトのデータが選ばれる。また、ＦＩＰＳ１９７で定められている「ＳｈｉｆｔＲｏｗｓ」関数を実行した処理結果と、ステップＳ０２０１を行った処理結果とは、同様の結果となる。

【００６８】

ステップＳ０２０２では、ステップＳ０２０１で選ばれる１バイトのデータが、いわゆるＴ－Ｂｏｘ等によって変換され、変換されたデータが出力される。

【００６９】

ステップＳ０２０３では、ステップＳ０２０２で出力されるデータに対して、いわゆるＸＯＲ－Ｔａｂｌｅｓ等のテーブルによって変換が行われ、図示するように、排他的論理和の計算が行われた場合と同様の処理結果が出力される。

【００７０】

図示するように、ＦＩＰＳ１９７で定められている「ＡｄｄＲｏｕｎｄＫｅｙ」関数、「ＳｕｂＢｙｔｅｓ」関数及び「ＭｉｘＣｏｌｕｍｎｓ」関数をそれぞれ実行した処理結果と、ステップＳ０２０２及びステップＳ０２０３をそれぞれ行った処理結果とは、同様の結果となる。

【００７１】

図示するように、１サブラウンド当たりの処理が行われると、ステップＳ０２０３の出力である４つの１バイトのデータが、出力データＤ＿ＯＵＴのうちの「０」乃至「３」のデータとして、生成される。

【００７２】

また、比較例の処理は、以下のように示せる。

【００７３】

図１２は、比較例に係る暗号化の１ラウンド当たりの処理の一例を説明する模式図（その２）である。サブラウンド処理におけるＬＵＴの入力及び出力の関係は、図示するように示せる。また、この比較例に用いるＬＵＴのデータ容量は、以下のようになる。

【００７４】

図１３は、比較例に係るＬＵＴのデータ容量の一例を示す表である。図示するように、データ容量は、鍵長、すなわち、行われるラウンド数に応じて異なる。

【００７５】

この比較例のように、１つのラウンドにおける処理に用いられるデータが、他のラウンドのデータを用いないと、入力と出力の関係を解析されると、１ラウンド中で複雑な処理をしても、データが解読される場合がある。

【００７６】

＜＜３．組み込みシステムの機能構成例＞＞

図１４は、本発明の一実施形態に係る組み込みシステムの機能構成の一例を示す機能ブロック図である。図示するように、組み込みシステム１は、選択部ＦＮ１と、変換部ＦＮ２と、排他的論理和計算部ＦＮ３とを含む。

【００７７】

選択部ＦＮ１は、入力データＤ＿ＩＮのうち、４バイトのサブラウンドデータＤ＿ＳＲを選択する。なお、入力データＤ＿ＩＮは、図３に示すように、１６バイトの１ラウンドデータである。また、選択部ＦＮ１によって、サブラウンドデータＤ＿ＳＲが選択されると、ＦＩＰＳ１９７で定められている「ＳｈｉｆｔＲｏｗｓ」関数を実行した処理結果と同様の処理結果が得られる。さらに、選択部ＦＮ１は、例えば、演算装置ＨＷ１（図１）等によって実現される。

【００７８】

変換部ＦＮ２は、サブラウンドデータＤ＿ＳＲを１バイトのデータごとに、異なるラウンドで用いられる鍵データの成分を含むテーブルに基づいて変換して、それぞれ、４バイトの変換データを生成する。なお、テーブルを示すテーブルデータＤＴは、十分な記憶領域が確保できる情報処理装置によって、あらかじめ生成されるのが望ましい。テーブルデータＤＴの生成には、ＲＡＭ又はスタックメモリといった記憶領域等が多く必要となる場合が多い。そこで、組み込みシステム１等の装置より、十分な記憶領域が確保できるＰＣ等によって、テーブルデータＤＴは、あらかじめ生成されるのが望ましい。すなわち、テーブルデータＤＴは、生成されるラウンドとは、他のラウンドの鍵データＤ＿Ｋを用いてあらかじめ生成され、組み込みシステム１にあらかじめ入力される。なお、変換部ＦＮ２は、例えば、演算装置ＨＷ１等によって実現される。

【００７９】

排他的論理和計算部ＦＮ３は、それぞれの変換データＤ＿ＣＨの排他的論理和を計算する。なお、排他的論理和計算部ＦＮ３は、例えば、演算装置ＨＷ１等によって実現される。

【００８０】

変換部ＦＮ２によるテーブルに基づく変換及び排他的論理和計算部ＦＮ３による排他的論理和の計算がそれぞれ行われると、出力は、ＦＩＰＳ１９７で定められている「ＡｄｄＲｏｕｎｄＫｅｙ」、「ＳｕｂＢｙｔｅｓ」及び「ＭｉｘＣｏｌｕｍｎｓ」の関数を実行した処理結果と同様の処理結果となる。

【００８１】

また、あるラウンドの処理（第１ラウンド）で用いられるテーブルには、他のラウンド（第２ラウンド）の鍵データＤ＿Ｋが含まれる。そのため、ＢＧＥアタック等によって、第１ラウンド当たりの入出力の関係が解析されても、テーブル及び鍵データを解析するのが難しくなるため、暗号化されたデータを解読するのが難しくなり、組み込みシステムは、データを難読化することができる。

【００８２】
また、本発明に係る実施形態では、１２８ビットの鍵長の場合には、組み込みシステムは、最初のラウンド及び中間のラウンドで、１ラウンドにつき、１６キロバイトのＬＵＴを用いる。また、組み込みシステムは、最後のラウンドで、４キロバイトのＬＵＴを用いる。したがって、組み込みシステムは、「１６×９ラウンド＋４＝１４８キロバイト」のデータ容量でＡＥＳ方式によって暗号化を行うことができる。なお、１９２ビットの鍵長の場合には、１１ラウンド行われるので、組み込みシステムは、「１６×１１ラウンド＋４＝１８０キロバイト」のデータ容量でＡＥＳ方式によって暗号化を行うことができる。さらに、２５６ビットの鍵長の場合には、１３ラウンド行われるので、組み込みシステムは、「１６×１３ラウンド＋４＝２１２キロバイト」のデータ容量でＡＥＳ方式によって暗号化を行うことができる。このようにして、組み込みシステムは、少ないデータ容量でＡＥＳ方式によって暗号化を行うことができる。
【００８３】
また、本発明は、使用できる記憶容量等に係る制約が多い組み込みシステムに適用される形態が望ましい。さらに、組み込みシステムは、プログラム及びデータの解読を難しくするため、図１に示すように、演算装置にメモリが内蔵されるハードウェア構成であるのが望ましい。
【００８４】
組み込みシステムは、例えば、いわゆるスマートメータ（Ｓｍａｒｔ　Ｍｅｔｅｒ）等に用いられる。そして、スマートメータ等は、外部装置等とデータを送受信する場合が多い。この場合には、スマートメータ等は、組み込みシステムによって、ＡＥＳ方式で暗号化してデータを送受信できる。これによって、送受信されるデータは、暗号化されているため、スマートメータは、データの送受信においてセキュリティを向上させることができる。
【００８５】
＜＜変形例＞＞
組み込みシステムは、ＡＥＳ方式によって、暗号化を行うに限られない。例えば、組み込みシステムは、各処理の逆関数に相当する処理を用いて、復号化を行ってもよい。なお、例えば、「ＳｈｉｆｔＲｏｗｓ」関数の逆関数は、「ＩｎｖＳｈｉｆｔＲｏｗｓ」関数等である。他にも、「ＳｕｂＢｙｔｅｓ」関数の逆関数は、「ＩｎｖＳｕｂＢｙｔｅｓ」関数であり、「ＭｉｘＣｏｌｕｍｎｓ」関数の逆関数は、「ＩｎｖＭｉｘＣｏｌｕｍｎｓ」関数である。
【００８６】
組み込みシステムは、スマートメータに限られない。例えば、組み込みシステムは、組込機器全般、クラウド等によって他の装置と通信を行う装置、ＩｏＴ（Ｉｎｔｅｒｎｅｔ　ｏｆ　Ｔｈｉｎｇｓ）に用いられる各装置又はこれらを組み合わせた１以上の情報処理装置を有する情報処理システム等であってもよい。
【００８７】
また、組み込みシステムは、１つの情報処理装置によって実現される構成に限られない。即ち、組み込みシステムは、２つ以上の情報処理装置を有する情報処理システムによって実現されてもよい。なお、情報処理システムでは、各処理の一部又は全部が分散、冗長、並列又はこれらを組み合わせるように、処理が行われてもよい。
【００８８】
さらに、本発明に係る実施形態は、情報処理装置又は情報処理システム等のコンピュータに情報処理方法を実行させるためのプログラムによって実現されてもよい。すなわち、プログラムは、本発明に係る情報処理方法をコンピュータに実行させるためのプログラムであって、プログラミング言語等によって記述されるコンピュータプログラムである。
【００８９】
また、プログラムは、ＤＶＤ若しくはブルーレイ（登録商標）等の光ディスク、フラッシュメモリ、磁気ディスク又は光磁気ディスク等の記録媒体に記憶され、頒布されてもよ

い。さらに、プログラムは、電気通信回線等を介して、頒布されてもよい。

【００９０】

以上、本発明の好ましい実施例について詳述したが、本発明は、係る特定の実施形態に限定されるものではない。すなわち、特許請求の範囲に記載された本発明の要旨の範囲内において、種々の変形又は変更が可能である。

【符号の説明】

【００９１】

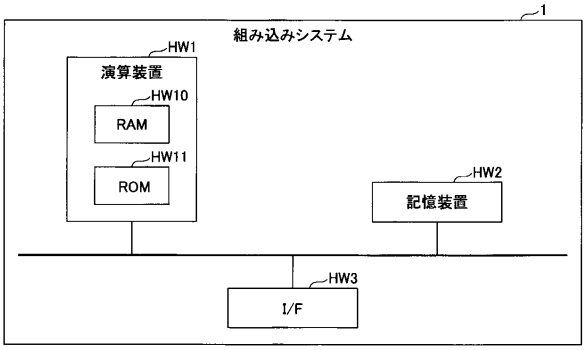
１　組み込みシステム
Ｄ＿ＩＮ　入力データ
Ｄ＿ＯＵＴ　出力データ
ＴＢ　テーブル
Ｄ＿Ｋ　鍵データ
ＲＰ　乱数成分
ＣＰ　打消成分
ＦＮ１　選択部
ＦＮ２　変換部
ＦＮ３　排他的論理和計算部

【要約】

【課題】ＡＥＳ方式において、データを難読化することを目的とする。
【解決手段】入力データをＡＥＳ方式で暗号化又は復号化する情報処理装置が、第１ラウンドの処理対象となる前記入力データのうち、４バイトのサブラウンドデータを選択し、前記サブラウンドデータを１バイトのデータごとに、前記第１ラウンドの次のラウンドである第２ラウンドで用いられる鍵データの成分を含むテーブルに基づいて変換して、それぞれ、４バイトの変換データを生成し、それぞれの前記変換データの排他的論理和を計算することで上記課題を解決する。
【選択図】図１４

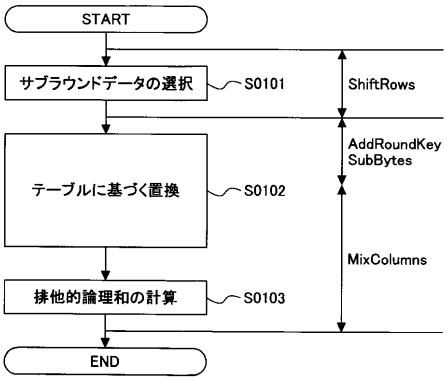
【図１】

本発明の一実施形態に係る
組み込みシステムのハードウェア構成の一例を説明するブロック図



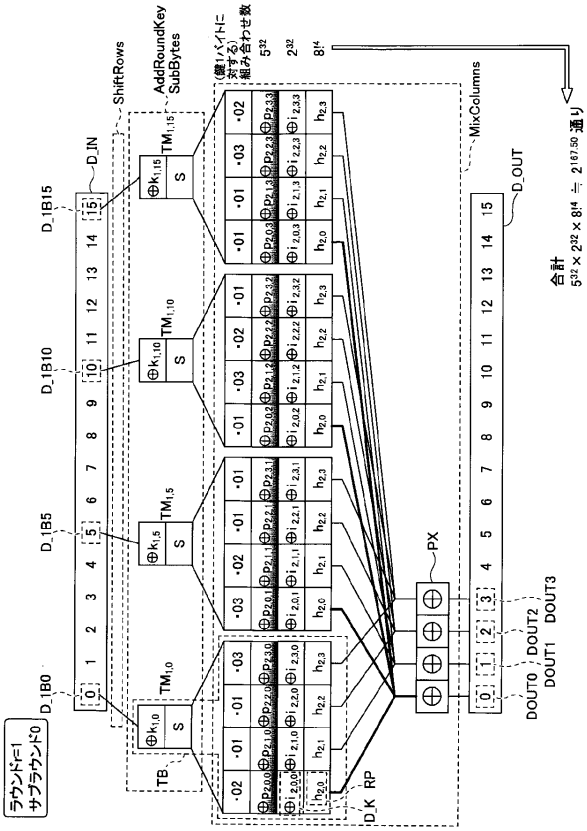
【図２】

本発明の一実施形態に係る
暗号化の1ラウンド当たりの処理の一例を説明するフローチャート



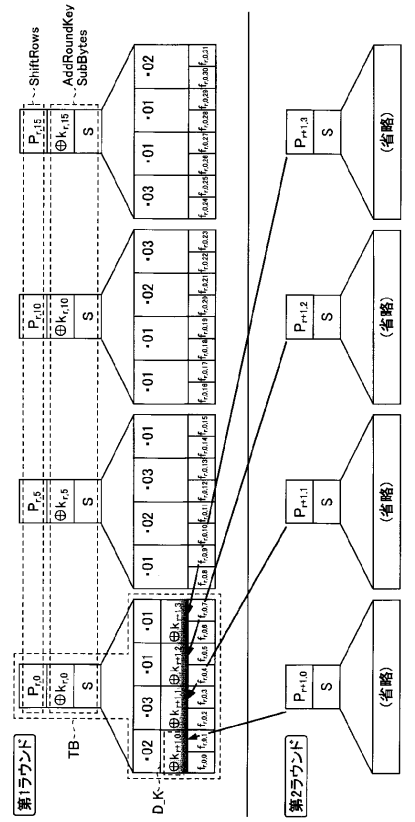
【図３】

本発明の一実施形態に係る最初のラウンドの処理の一例を説明する模式図

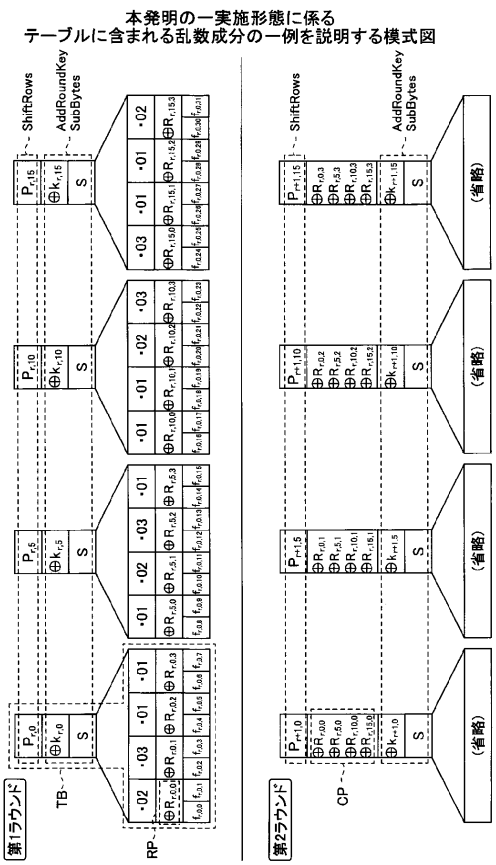


【図４】

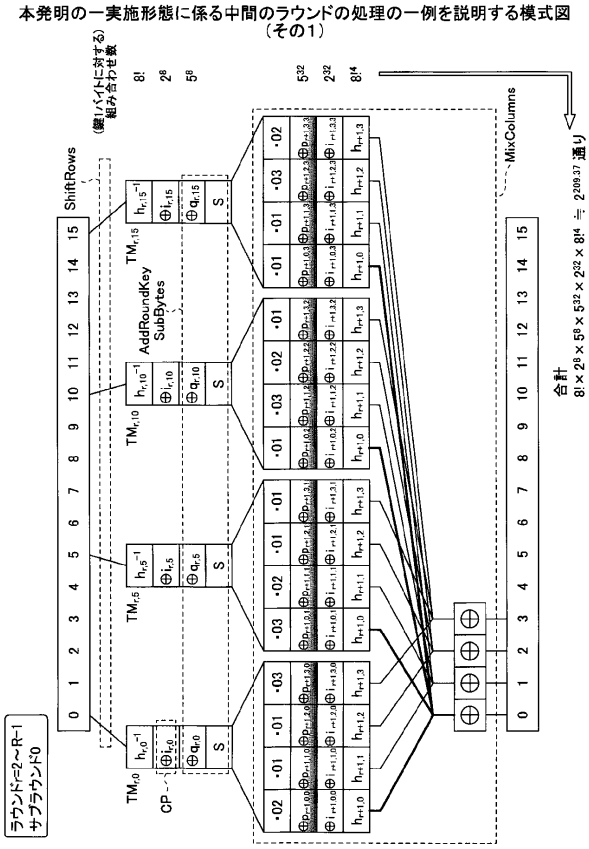
本発明の一実施形態に係る
テーブルに含まれる鍵データの一例を説明する模式図



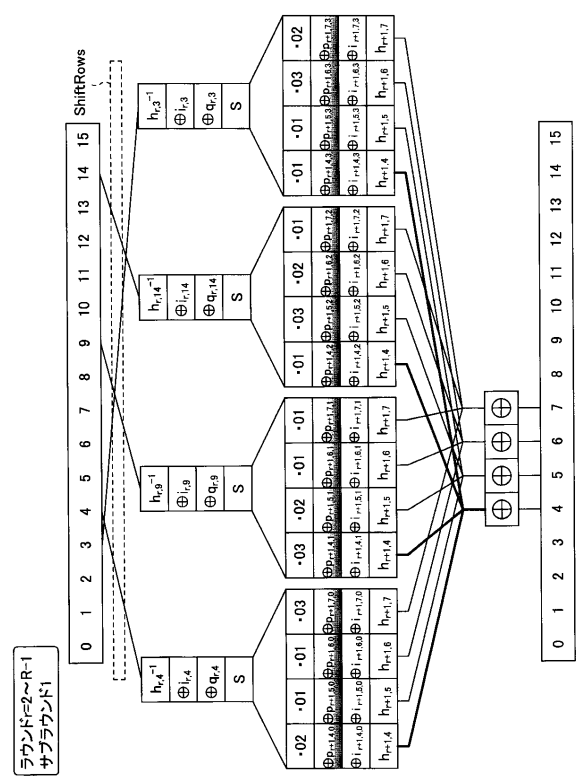
【図５】


本発明の一実施形態に係る
テーブルに含まれる乱数成分の一例を説明する模式図
ShiftRows
AddRoundKey
SubBytes
第1ラウンド
TB
RP
第2ラウンド
CP
(省略)

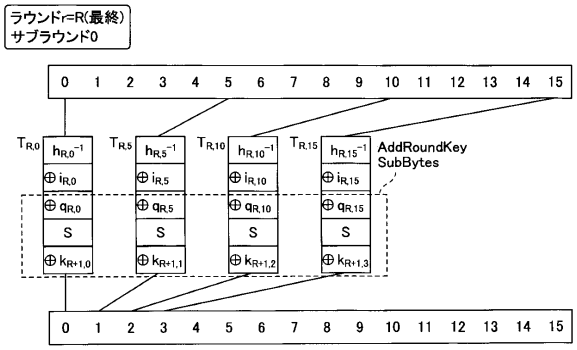
【図６】


本発明の一実施形態に係る中間のラウンドの処理の一例を説明する模式図
(その1)
ShiftRows
AddRoundKey
SubBytes
MixColumns
ラウンドr=2～R-1
サブラウンド0
合計

【図７】

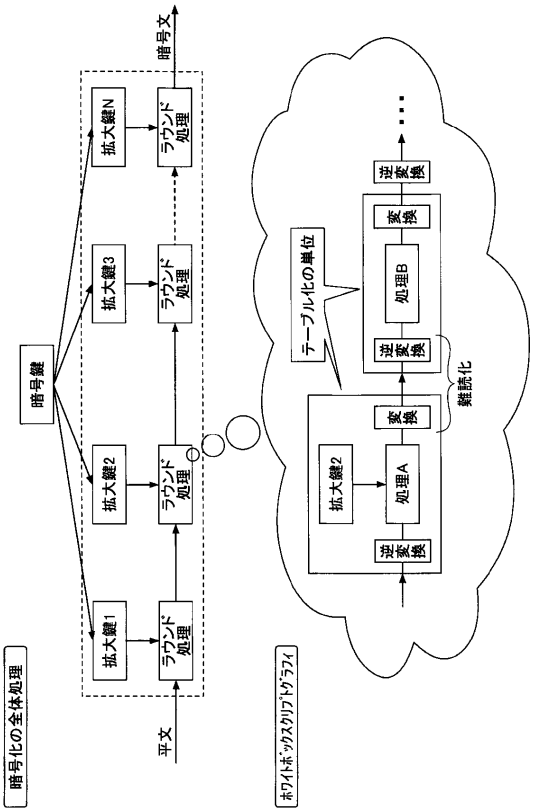

本発明の一実施形態に係る中間のラウンドの処理の一例を説明する模式図
(その2)
ShiftRows
ラウンドr=2～R-1
サブラウンド1

【図８】


本発明の一実施形態に係る最終のラウンドの処理の一例を説明する模式図
ラウンドr=R(最終)
サブラウンド0
AddRoundKey
SubBytes

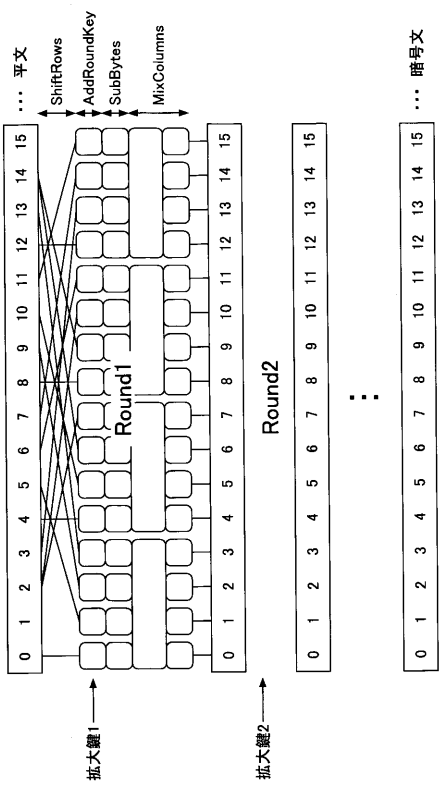
【図９】

ホワイトボックスクリプトグラフィの一例の原理を示す概念図



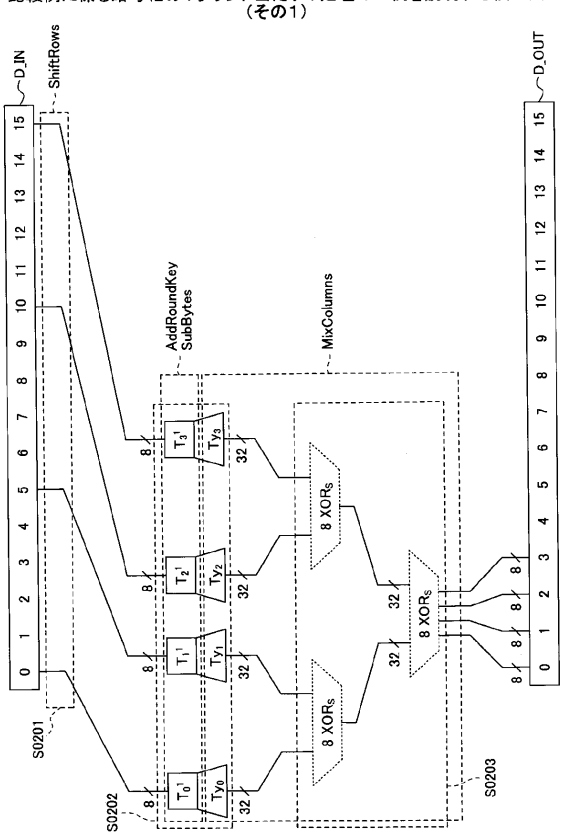
【図１０】

ホワイトボックスクリプトグラフィにおけるラウンド処理の一例を示す模式図



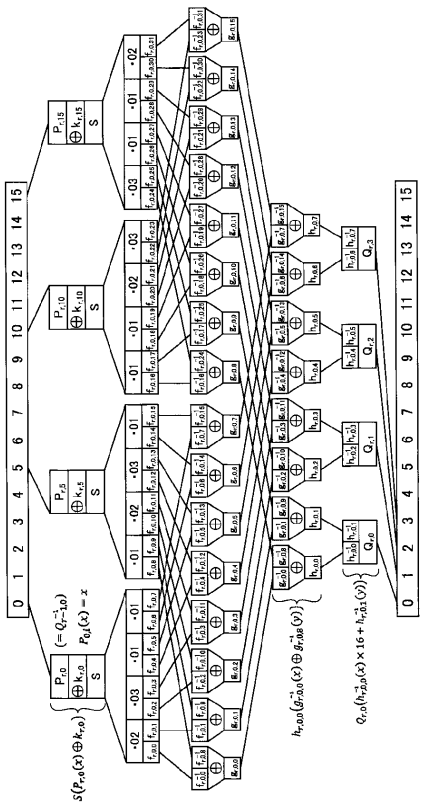
【図１１】

比較例に係る暗号化の1ラウンド当たりの処理の一例を説明する模式図（その1）



【図１２】

比較例に係る暗号化の1ラウンド当たりの処理の一例を説明する模式図（その2）



【図１３】

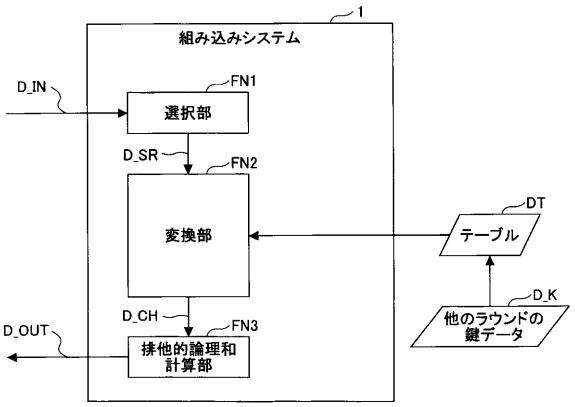
比較例に係るLUTのデータ容量の一例を示す表

	1ラウンドあたり	128bit	192bit	256bit
1段目	16	144	176	208
2, 3段目	12	108	132	156
4段目	4	36	44	52
(最終ラウンド)		4	4	4
Total		292	356	420

単位:(kByte)

【図１４】

本発明の一実施形態に係る
組み込みシステムの機能構成の一例を示す機能ブロック図



フロントページの続き

(56)参考文献 特開２００３－１９５７４９（ＪＰ，Ａ）
特開２００８－０１７４８９（ＪＰ，Ａ）
特許第５４８５６９４（ＪＰ，Ｂ２）
特表２００５－５１３５４１（ＪＰ，Ａ）
米国特許出願公開第２０１０／００５４４６１（ＵＳ，Ａ１）
米国特許出願公開第２０１３／００１０９６３（ＵＳ，Ａ１）
米国特許第０８４２２６６８（ＵＳ，Ｂ１）
Yoni De Mulder, et al., Cryptanalysis of a Perturbated White-Box AES Implementation, LNCS, Progress in Cryptology - INDOCRYPT 2010, Springer, ２０１０年１２月, Vol.6498, pp.292-310
Chung Hun Baek, et al., Analytic Toolbox for White-Box Implementations: Limitation and Perspective, Cryptology ePrint Archive: Report 2014/688, ［オンライン］, ２０１４年９月 ４日, Version: 20140904:060921, ［検索日 平成２９年１月２１日］、インターネット, ＵＲＬ, <https://eprint.iacr.org/eprint-bin/getfile.pl?ently=2014/688&version=20140904:0609218&file=688.pdf>

(58)調査した分野(Int.Cl., ＤＢ名)
Ｇ０９Ｃ １／００
Ｇ０６Ｆ ２１／６０