

【公報種別】特許法第 17 条の 2 の規定による補正の掲載  
 【部門区分】第 6 部門第 2 区分  
 【発行日】平成23年8月4日(2011.8.4)

【公表番号】特表2010-530990(P2010-530990A)  
 【公表日】平成22年9月16日(2010.9.16)  
 【年通号数】公開・登録公報2010-037  
 【出願番号】特願2010-512742(P2010-512742)  
 【国際特許分類】

G 0 9 C 1/00 (2006.01)

【F I】

G 0 9 C 1/00 6 2 0 Z

G 0 9 C 1/00 6 5 0 Z

【手続補正書】

【提出日】平成23年6月15日(2011.6.15)

【手続補正 1】

【補正対象書類名】明細書

【補正対象項目名】全文

【補正方法】変更

【補正の内容】

【発明の詳細な説明】

【発明の名称】公開行列に基づき、誤り訂正符号の復号を用いて認証を行う方法

【技術分野】

【0001】

本発明は、公開行列 ( p u b l i c m a t r i x ) に基づき、誤り訂正符号の復号を用いて暗号化・認証を行う方法に関する。

【0002】

本発明はまた、暗号化装置の動作によって上記のような認証の方法を実行するように構成される処理手段を備える暗号化装置に関する。

【背景技術】

【0003】

暗号化・認証を行う方法は広く知られている。

【0004】

最も広く知られている暗号化・認証を行う方法は、現在のところ、リベスト ( R i v e s t )、シャミア ( S h a m i r ) およびエーデルマン ( A d l e m a n ) により開発された R S A アルゴリズムに基づいている。この R S A アルゴリズムのセキュリティ ( s e c u r i t y ) は、大きな整数を因数分解することに関する数学的な難しさにある。

【0005】

しかしながら、このような暗号化・認証を行う方法は、幾つかの欠点を有している。これらの欠点の中で特に注目すべき点は、上記の R S A アルゴリズムが、非常に大きな整数を使用した計算能力を必要とし、とりわけ、離散的な指数関数計算を必要とする点である。この種の計算は、特に、スマートカードまたは無線タグ ( R F タグ ) のような、限られた処理能力を有する低価格の暗号化装置上で実行される際に計算の速度が遅くなる傾向にある。このため、前述のような暗号化・認証を行う方法は、現在のところ、これらの暗号化装置には利用できない。

【0006】

R S A アルゴリズムに基づいて暗号化・認証を行う方法の代替方法の中で、公開行列を利用し、誤り訂正符号の復号を用いて暗号化・認証を行う方法が広く知られている。

【0007】

より詳しくいえば、本発明は、このような誤り訂正符号の復号を用いて暗号化・認証を行う方法に関するものである。

【0008】

このような暗号化・認証を行う方法は、NP (non-deterministic polynomial) 完全性を有する数学的な問題のソースであって、それゆえに、解くことが非常に難しい数学的な問題のソースであるという利点を有している。この結果、このような暗号化・認証を行う方法は、高度にセキュリティに富んでいる。その上、誤り訂正符号を復号するための計算の速度は、RSAアルゴリズムに基づいた計算の速度よりも速い。

【0009】

暗号化において誤り訂正符号を用いることは、1980年代より公知である。

【0010】

欧州特許出願公開第0661846号公報（後述の特許文献1に対応する）においては、公開行列に基づき、誤り訂正符号の復号を用いて暗号化・認証を行う方法が記述されている。

【0011】

さらに、この欧州特許出願公開第0661846号公報においては、当該欧州特許出願の出願人による先行技術文献である「シンドローム・デコーディングに基づいた新しい識別スキーム (A new identification scheme based on syndrome decoding)」(ジェイ・スターン (J. Stern) 著、1993年発行) (後述の非特許文献1に対応する) と同様に、代表的に100キロビット (kbit) ~ 1000キロビット (kbit) のオーダーの非常に大きなランダム公開行列を用いたスターン・シンドローム・プロトコル (Stern syndrome protocol) と呼ばれる認証プロトコルが記述されている。

【0012】

同様に、他の先行技術文献である「誤り訂正符号に基づいて改良された識別スキーム (Improved identification scheme based on error-correcting codes)」(ベロン (Veron) 著、工学、通信分野およびコンピュータ関連分野に適用可能な代数学、1997年発行 (Applicable Algebra in Engineering, Communication and Computing, 1997)) (後述の非特許文献2に対応する) においても、公開行列に基づき、誤り訂正符号の復号を用いて暗号化・認証を行う方法との関連において、シンドローム・プロトコルの変化の様子が記述されている。このようなプロトコルは、ベロン・プロトコル (Veron protocol) と呼ばれている。

【0013】

これらの認証プロトコルにおいては、大抵の場合、公開行列はランダムである。それゆえに、上記プロトコルを実行するための暗号化装置のメモリ内に公開行列の全ての係数を記憶することが必要である。

【0014】

しかしながら、低価格の暗号化装置における記憶上の制限によって、上記のようなプロトコルを実行することが不可能になる。このような事態は、特に、スマートカードまたは無線タグを使用する場合に発生し得る。

【0015】

前述の先行技術文献である「シンドローム・デコーディングに基づいた新しい識別スキーム (A new identification scheme based on syndrome decoding)」(ジェイ・スターン (J. Stern) 著、1993年発行) において、この著者は、さらに、初期値および擬似乱数生成器 (pseudo-random generator) に基づいて擬似乱数を使用することにより公開行列を生成することを提案している。しかしながら、擬似乱数生成器の仕様は、今日まで未解決のままになっている問題である。さらに、このような擬似乱数生成器を動作させ

ることは、低価格の暗号化装置における限られた容量と両立しない。

【0016】

2007年6月24日に開始されたISIT 2007コンファレンスにおいて、他の先行技術文献である「SYND：セキュリティの減少を伴う非常に高速のコードに基づいた暗号ストリーム（SYND：a very fast Code-Based Cipher Stream with a security reduction）」（ガボリ他（Gaborit et al.）著）（後述の非特許文献3に対応する）が提示されている。ただし、この先行技術文献は、この日まで公衆によるアクセスが不可能であった。

【先行技術文献】

【特許文献】

【0017】

【特許文献1】欧州特許出願公開第0661846号公報

【非特許文献】

【0018】

【非特許文献1】「シンドローム・デコーディングに基づいた新しい識別スキーム（A new identification scheme based on syndrome decoding）」（ジェイ・スターン（J. Stern）著、1993年発行）

【非特許文献2】「誤り訂正符号に基づいて改良された識別スキーム（Improved identification scheme based on error-correcting codes）」（ベロン（Veron）著、工学、通信分野およびコンピュータ関連分野に適用可能な代数学、1997年発行（Applicable Algebra in Engineering, Communication and Computing, 1997））

【非特許文献3】「SYND：セキュリティの減少を伴う非常に高速のコードに基づいた暗号ストリーム（SYND：a very fast Code-Based Cipher Stream with a security reduction）」（ガボリ他（Gaborit et al.）著、2007年6月24日に開始されたISIT 2007コンファレンスにて提示された資料）

【発明の概要】

【発明が解決しようとする課題】

【0019】

したがって、本発明の1つの目的は、特に、限られた処理能力および/または記憶容量を有する暗号化装置といったような、低価格の暗号化装置にて実行することができるような、公開行列に基づき、誤り訂正符号の復号を用いて暗号化・認証を行う方法を提供することにある。

【0020】

より特定のにいえば、本発明の1つの目的は、公開行列に基づき、誤り訂正符号の復号を用いて暗号化・認証を行う方法において記憶されるべき公開データの量を減少させることにある。

【0021】

さらに、前述の先行技術文献にて使用されている複数のランダム行列は、暗号化装置における高速の計算にはそれほど適していない。

【0022】

本発明の他の目的は、高速の計算を可能にするような、公開行列に基づき、誤り訂正符号の復号を用いて暗号化・認証を行う方法を提供することにある。

【課題を解決するための手段】

【0023】

上記目的を達成するために、本発明との関連において、新しいタイプの公開行列が提示

されている。

【0024】

特に、上記目的は、公開行列が擬似巡回行列 (quasi-cyclic matrix) であるという事実によって、本発明に従って達成される。

【0025】

擬似巡回行列は、複数の巡回ブロックの並置 (juxtaposition) を有する行列として知られている。この巡回ブロックの並置においては、1つの行から次の行へのシフトが、巡回的置換 (circular permutation) によって行われる。

【0026】

この結果、公開行列における全ての情報を記憶する際に、各々の巡回ブロック内の1つの基本の行を記憶するのみで十分であり、各々の巡回ブロックの他の行は、置き換えによって基本の行から推定されることになる。これによって、上記のような暗号化・認証を行う方法にて記憶されるべきデータの量が大幅に減少する。

【0027】

さらに、巡回ブロックの性質のおかげで、ベクトルと擬似巡回行列との乗算が高速に行われる。さらにまた、誤り訂正符号の復号を用いて暗号化・認証を行う方法は、このような乗算を実行する。このことは、本発明に従って暗号化・認証を行う方法が、暗号化計算の速度を向上させるのを可能にすること意味する。

【0028】

それゆえに、本発明に従って暗号化・認証を行う方法は、暗号化装置が、限られた記憶容量および処理能力を有している場合であっても、この暗号化装置にて容易に実行される。

【0029】

本発明に従って暗号化・認証を行う方法は、前述の先行技術文献にて記述されているプロトコル (すなわち、スターン・シンδροームを用いたデコーディングのためのプロトコル、および、ベロンにより記述されているようなスターン・シンδροームを用いたデコーディングのためのデュアル・プロトコル) に対して互換性を有する公開行列を提供するといったような付加的な利点を有する。

【0030】

本発明の第1の実施態様において、擬似巡回行列は、 $k$ 行および $2k$ 列を有し、且つ、 $k \times k$ のサイズの単位行列ブロック (identity block) と $k \times k$ のサイズの巡回ブロック (circulant block) との並置を有する。

【0031】

この場合、認証を行う方法にて使用される秘密鍵 (private key) は、 $2k$ のサイズのワード $x$ である。また一方で、公開鍵 (public key) は、 $k$ のサイズのシンδροーム $s$ と、擬似巡回行列の第1の行の半分の量とを有する。それゆえに、シンδροーム・デコーディング・プロトコルは、 $4k$ ビットから実行され得る。

【0032】

好ましくは、本発明の第1の実施態様において、巡回ブロックは、 $k$ のサイズのランダムベクトル (random vector) により規定 (定義) されることが可能である。

【0033】

この第1の実施態様における公開行列は、スターン・プロトコルまたはベロン・プロトコルにおける公開行列として使用されることが可能である。

【0034】

本発明の第2の実施態様において、公開行列は、 $k$ 行および $2k$ 列を有する擬似巡回形の間行列に基づいて構築され、この間行列は、 $k$ のサイズの第1の巡回形正方形ブロックからなるブロックAと $k$ のサイズの第2の巡回形正方形ブロックからなるブロックBとの並置により構成される。この場合に、間行列は、下記の式

## 【数 1】

$$G' = [A \mid B]$$

により表される形態を有しており、公開行列は、中間行列に左からブロック A の逆行列を乗算することによって構築され、これによって、公開行列は、下記の式

## 【数 2】

$$G = [I \mid A^{-1} \cdot B]$$

により表される形態を有するようになる。ここで、行列  $A^{-1}$  は、ブロック A の逆行列である。

## 【0035】

好ましくは、本発明の第 2 の実施態様において、第 1 の巡回ブロックおよび第 2 の巡回ブロックは、それぞれ、第 1 のベクトルおよび第 2 のベクトルにより規定され、第 1 のベクトルおよび第 2 のベクトルにより形成されるベクトルは、低次 (low order) のベクトルである。

## 【0036】

この場合、第 1 のベクトルおよび前記第 2 のベクトルは、このような次数の制限がある状態でランダムである。

## 【0037】

本発明の第 2 の実施態様において、公開行列は、特に、ベロン・プロトコルにおける公開行列として使用されることが可能である。

## 【0038】

この場合、他の特定の実施態様において、ベロン・プロトコルの秘密 (secret) は、第 1 のベクトルおよび第 2 のベクトルにより構築されるような、行ベクトルから転置された列ベクトルからなる。

## 【0039】

このようなベクトルは、 $2k$  のサイズの秘密鍵に対応している。また一方で、公開鍵は、 $k$  のサイズ分の秘密鍵により誘導される巡回ブロックに基づいて決定され得る。それゆえに、デコーディング・プロトコルは、 $3k$  ビットから実行され得る。

## 【0040】

本発明はまた、コンピュータ・プログラムの動作によって前述のような認証の方法を実行するように取り決められた複数の命令を有するコンピュータ・プログラムに関するものである。

## 【0041】

本発明はまた、前述のような認証の方法を実行するよう構成される処理手段を有する暗号化装置に関するものである。

## 【0042】

本発明はまた、このような暗号化装置を具備するスマートカードに関するものである。

## 【0043】

以下、非限定的な例に基づいて、添付の図面を参照しながら本発明の様々な実施形態 (実施例) を説明する。

## 【図面の簡単な説明】

【 0 0 4 4 】

【図 1】擬似巡回行列の一般的な表示を示す図である。

【図 2】本発明の第 1 の実施例に従って認証を行う方法において使用されるべき公開行列を示す図である。

【図 3】図 2 に示されている行列を構成する行列ブロックの一例を示す図である。

【図 4】本発明の第 2 の実施例に従って認証を行う方法において使用されるべき公開行列を構築するために用いられるような低次のワードからなる中間行列を示す図である。

【図 5】図 4 に示されている中間行列を形成する行列ブロックの一例を示す図である。

【発明を実施するための形態】

【 0 0 4 5 】

本発明に従って、公開行列に基づき、誤り訂正符号の復号を用いて暗号化・認証を行う方法は、スターン・シンドローム・デコーディング・プロトコルの助けを借りて実行され得る。

【 0 0 4 6 】

このようなプロトコルは、前述の特許文献 1 の欧州特許出願公開第 0 6 6 1 8 4 6 号公報、および、前述の非特許文献 1 の「シンドローム・デコーディングに基づいた新しい識別スキーム (A new identification scheme based on syndrome decoding)」(ジェイ・スターン (J. Stern) 著、1993 年発行) にて申し分なく記述されている。さらに、上記のようなプロトコルは、誤り訂正符号を用いた暗号学の分野における当業者によく知られている。

【 0 0 4 7 】

これらの先行技術文献は、上記のようなプロトコルを実行する際に参考にされるであろう。

【 0 0 4 8 】

スターン・プロトコルの主要なステップに関する注意事項を以下に示す。スターン・シンドローム・デコーディング・プロトコルにおいて、2 つのエンティティ (entities) は、バイナリ・コードにより構成される公開行列  $H$  を含む。さらに、秘密コードは、低次のワードであり、公開鍵は、上記公開行列と上記ワードとの積である。

【 0 0 4 9 】

スターン・プロトコルを用いて認証を実行するに際して、本出願人は、ベリファイア (verifier)  $V$  によってそれ自身を認証することを必要とするエンティティ  $P$ 、すなわち、プローバ (prover) を考慮に入れる。一連の回転 (turn) が実行される場合、各々の回転を正しく実行することによって、プローバ  $P$  が真 (true) であるというアイデンティティ (identity) の可能性が増加していく。各々の回転は、プローバ  $P$  がベリファイア  $V$  にエンゲイジメント (engagement) を送るという第 1 のステップからなる。次に、第 2 のステップにおいて、ベリファイア  $V$  は、プローバ  $P$  にチャレンジ (challenge) を返送する。さらに、第 3 のステップにおいて、プローバ  $P$  は、ベリファイア  $V$  に応答を送る。ここで、ベリファイア  $V$  は、プローバ  $P$  の応答が、そのプローバ  $P$  の公開鍵に一致していることを検証する。

【 0 0 5 0 】

プローバ  $P$  の公開鍵とプローバ  $P$  の秘密鍵との間のリンクは、シンドローム・デコーディングの問題に基づいている。前述のスターン・プロトコルの動作に関する処理の詳細は、当業者によく知られている。この当業者は、必要に応じて前述の先行技術文献を参考にすることもできる。

【 0 0 5 1 】

同様に、当業者は、ベロン・プロトコルもよく知っており、このベロン・プロトコルを実行する際に、必要に応じて、前述の先行技術文献 (非特許文献 2) の「誤り訂正符号に基づいて改良された識別スキーム (Improved identification scheme based on error-correcting codes)」(ベロン (Veron) 著、工学、通信分野およびコンピュータ関連分野に適用可能な代

数学、1997年発行 (Applicable Algebra in Engineering, Communication and Computing, 1997)) を参照するかもしれない。

【0052】

ペロン・プロトコルの主要なステップは以下のように要約される。

【0053】

ペロン・プロトコルを用いた認証を実行するに際して、このペロン・プロトコルの大部分のステップは、前述のスターン・プロトコルの場合と同じである。各々のステップにおいて実行される計算に違いが見られるが、この違いは、ほんのわずかである。より特定のにいえば、公開鍵と秘密鍵との間のリンクは、ある特定の行列または誤り訂正符号に関連している低次のワードを見つけ出すことに基づいている。

【0054】

前述の先行技術文献においては、公開鍵が記述されている。本発明によれば、前述の先行技術文献と同様にプロトコルが実行される。ただし、本発明では、前述の先行技術文献にて記述されている公開行列を、以下に述べるような複数の公開行列に置き換えている。前述のようなプロトコルの各々にて使用可能であるタイプの公開行列を以下に述べる。

【0055】

本発明の第1の実施例にて以下に述べるような公開行列Hは、スターン・プロトコルまたはペロン・プロトコルにおける公開行列として同等に使用されることが可能である。さらに、本発明の第2の実施例にて以下に述べるような公開行列Gは、ペロン・プロトコルにて使用されることが可能である。

【0056】

本発明によれば、公開行列は擬似巡回行列であり、この擬似巡回行列は、複数の巡回ブロックの並置を有することを意味するものである。図1は、このような擬似巡回行列（公開行列H）の一般的な表示を含む。このような擬似巡回行列は、複数の巡回形正方形ブロック  $A_1, A_2, \dots, A_n$  により構成される。これらの巡回形正方形ブロックの1つは、基本のベクトルに基づいて置換により規定される。

【0057】

図2に示すように、本発明の第1の実施例によれば、公開行列Hは、図1に関連して既述された行列と同じタイプであり、 $k$  行および  $2k$  列を有する。この公開行列Hは、 $k$  のサイズの正方形の単位行列（単位行列ブロック）I、および、 $k$  のサイズの正方形の巡回行列（巡回ブロック）Cからなる。この正方形の巡回行列Cは、複数の“0”および複数の“1”により構成される。それゆえに、公開行列Hは、下記の式

【数3】

$$H = [I \mid C].$$

により表される形態を有する。

【0058】

ここで、図3を参照しながら、巡回行列Cをより詳細に説明する。この巡回行列Cは、ランダムベクトル  $[c_1, c_2, \dots, c_{k-1}, c_k]$  からなる第1の行を有する。ここで、 $c_i$  は、“0”または“1”である。次に続く複数の行は、第1の行の連続的な置き換えによって決定される。これによって、巡回行列Cは、全体が第1の行によって決定されることになる。

【0059】

上記の公開行列Hは、前述のスターン・プロトコルおよびペロン・プロトコルにて使用されることが可能である。

## 【 0 0 6 0 】

本発明の第 2 の実施例において、 $k$  行および  $2k$  列を有する擬似巡回形の間中ブロック  $G$  が規定される。この中間ブロック  $G$  は、 $k$  のサイズの第 1 の巡回形正方形ブロックからなるブロック  $A$ 、および、 $k$  のサイズの第 2 の巡回形正方形ブロックからなるブロック  $B$  により構成される。この中間ブロック  $G$  は、図 4 に図示されている。この中間ブロック  $G$  は、下記の式

## 【 数 4 】

$$G' = [A \mid B]$$

により表される形態を有する。

そして、公開行列  $G$  は、下記の式

## 【 数 5 】

$$G = [I \mid A^{-1} \cdot B]$$

により表される形態を有しており、第 1 の単位行列ブロックおよび第 2 のブロックにより構成することによって構築される。この第 2 のブロックは、行列  $B$  に  $A$  の逆行列  $A^{-1}$  を左から乗算することによって構成される。以後、積  $A^{-1} \cdot B$  の結果として生成される行列は、 $D$  と表わされる。

## 【 0 0 6 1 】

上記のような公開行列  $G$  は、ベロン・プロトコルにおける公開行列として使用されることが可能である。

## 【 0 0 6 2 】

複数の行列（ブロック） $A$ 、 $B$  が、図 5 に図示されている。これらの行列  $A$ 、 $B$  は、それぞれの第 1 の行  $a = [a_1, a_2, \dots, a_{k-1}, a_k]$ 、 $b = [b_1, b_2, \dots, b_{k-1}, b_k]$  に基づいて規定される。ここで、 $a_i$  および  $b_i$  は、“0” または “1” の値を有する。これらの 2 つの第 1 の行はランダムベクトルであり、ベクトル  $[a, b]$  が、ベロン・プロトコルにおける次数の条件を満たすように選択される。

## 【 0 0 6 3 】

この場合、ベロン・プロトコルにおける秘密データは、 $2k$  のサイズのベクトル<sup>t</sup>  $[a, b]$ 、すなわち、行ベクトル  $[a, b]$  から転置された列ベクトルである。また一方で、公開データは、 $k$  のサイズの行列  $D$  を記述するベクトル、すなわち、行列  $D$  の第 1 の行である。

## 【 0 0 6 4 】

本発明の第 2 の実施例の利点は、低次の秘密データ（ベクトル）<sup>t</sup>  $[a, b]$  が、公開行列において直接的に記述されているという点である。

## 【 0 0 6 5 】

本発明によれば、本発明の第 1 の実施例に関してベロン・プロトコルまたはスターン・プロトコルにて既述された複数の行列の使用、特に、本発明の第 2 の実施例に関してベロン・プロトコルにて既述された複数の行列の使用は、暗号化プロトコルに課せられたセキュリティの制約を維持することを可能にする。

## 【 0 0 6 6 】

特に、コードのパラメータがギルバート・バルシャモフ限界（Gilbert - Varshamov limit）より低い値を有する場合に、通常の攻撃に対してコードが保護されることは広く知られている。

## 【 0 0 6 7 】

本発明の第 1 の実施例において、次数  $w$  の秘密  $X$  に関していえば、次数  $w$  が、ギルバート・バルシャモフ限界よりもちょっと低い値になるように選択されている場合には、パラメータ  $[2k, k]$  のコード内に次数  $w$  のワード（秘密） $X$  を見つけ出すために必要なコストが少なくとも  $2^{80}$  になるように、 $k$  が選択される。

## 【 0 0 6 8 】

本発明の第 1 の実施例に関して上記のような条件を満たすパラメータの一例は、 $k = 317$ 、および、 $w = 69$  である。これらのパラメータの値によって、シンδροーム  $s$  に対応する  $634$  のサイズの公開データが提供されると共に、 $2k$  のサイズの秘密および行列  $C$  の第 1 の行に対応する  $951$  のサイズの秘密データが付与される。この場合、公開行列  $H$  は、 $HX = s$  によって決定される。ここで、 $s$  はシンδροーム、 $X$  は秘密鍵（secret key）、そして、 $H$  は公開行列である。

## 【 0 0 6 9 】

本発明の第 2 の実施例においては、例えば、 $k = 347$ 、 $w = 76$  といったように、ギルバート・バルシャモフ限界よりも低い次数  $w$  を有するベクトル  $x$  ( $x = [a, b]$ ) が選択される。これによって、下記の式

## 【数 6】

$${}^t x = {}^t [a, b]$$

により表されるような  $694$  ビットのサイズの秘密データが提供される。また一方で、行列  $D$  の第 1 の行により規定されるような  $347$  ビットのサイズの公開データが提供される。

## 【 0 0 7 0 】

かくして、本発明に従って複数の擬似巡回行列を使用することは、スターン・プロトコルまたはベロン・プロトコルにて通常使用されるサイズに比べて、複数の行列のサイズを減少させることを可能にする。代表的には、複数の行列のサイズを数  $100$  キロビットから約  $300$  ビットに減少させることが可能になる。

## 【 0 0 7 1 】

本発明に従って、公開行列に基づき、誤り訂正符号の復号を用いて暗号化・認証を行う方法は、スターン・プロトコルまたはベロン・プロトコルを使用することにより、暗号化装置にて容易に実行され得る。

## 【 0 0 7 2 】

特に、本発明の第 1 の実施例で記述されている公開行列  $H$  は、スターン・プロトコルまたはベロン・プロトコルにて同等に使用されることが可能であり、本発明の第 2 の実施例で記述されている公開行列  $G$  は、ベロン・プロトコルにて使用されることが可能である。

## 【 0 0 7 3 】

本発明に従って暗号化・認証を行う方法を実行するために、プロセッサは、前述のような単一または複数の擬似巡回行列を用いて上記のプロトコルを実行するようにプログラミングされる。暗号化装置はまた、暗号化計算の期間中にデータを記憶するためのメモリを備えている。

## 【 0 0 7 4 】

本発明に従って暗号化・認証を行う方法が、誤り訂正符号の復号を行う際に使用される複数の行列のサイズを減少させることを可能にするという事実によって、上記の暗号化装置は、例えば、スマートカードのチップにより構成され得る。

## 【 手続補正 2 】

【補正対象書類名】特許請求の範囲

【補正対象項目名】全文

【補正方法】変更

【補正の内容】

【特許請求の範囲】

【請求項 1】

公開行列に基づき、誤り訂正符号の復号を用いて暗号化・認証を行う方法であって、前記公開行列は擬似巡回行列であることを特徴とする、暗号化・認証を行う方法。

【請求項 2】

前記公開行列（H）は、k 行および 2 k 列を有し、且つ、 $k \times k$  のサイズの単位行列ブロックと  $k \times k$  のサイズの巡回ブロックとの並置を有する請求項 1 記載の方法。

【請求項 3】

前記公開行列（H）は、下記の式

【数 1】

$$H = [I \mid C]$$

により表されるタイプの公開行列であり、ここで、I は、 $k \times k$  のサイズの単位行列ブロックであり、C は、 $k \times k$  のサイズの巡回ブロックである請求項 1 記載の方法。

【請求項 4】

前記巡回ブロックは、k のサイズのランダムベクトルにより規定される請求項 2 または 3 記載の方法。

【請求項 5】

前記巡回ブロックは、バイナリ・データにより構成される請求項 2 から 4 のいずれか一項に記載の方法。

【請求項 6】

サイズを表す k の数は、3 1 7 に等しい請求項 2 から 5 のいずれか一項に記載の方法。

【請求項 7】

前記擬似巡回行列は、スターン・プロトコルまたはペロン・プロトコルにて使用される請求項 2 から 5 のいずれか一項に記載の方法。

【請求項 8】

前記公開行列は、k 行および 2 k 列を有する擬似巡回形の間行列（G）に基づいて構築され、前記中間行列（G）は、k のサイズの第 1 の巡回形正方形ブロックからなるブロック A と k のサイズの第 2 の巡回形正方形ブロックからなるブロック B との並置により構成され、この場合に、前記中間行列（G）は、下記の式

【数 2】

$$G' = [A \mid B]$$

により表される形態を有しており、

前記公開行列は、前記中間行列に左から前記ブロック A の逆行列を乗算することによって構築され、これによって、前記公開行列は、下記の式

## 【数 3】

$$G = [I \mid A^{-1} \cdot B]$$

により表される形態を有するようになり、ここで、行列  $A^{-1}$  は、前記ブロック A の逆行列である請求項 1 記載の方法。

## 【請求項 9】

前記第 1 の巡回ブロックおよび前記第 2 の巡回ブロックは、それぞれ、第 1 のベクトルおよび第 2 のベクトルにより規定され、前記第 1 のベクトルおよび前記第 2 のベクトルにより形成されるベクトルは、低次のベクトルである請求項 8 記載の方法。

## 【請求項 10】

前記第 1 のベクトルおよび前記第 2 のベクトルがランダムである請求項 9 記載の方法。

## 【請求項 11】

前記公開行列は、ペロン・プロトコルにおける公開行列として使用される請求項 8 から 10 のいずれか一項に記載の方法。

## 【請求項 12】

前記ペロン・プロトコルの秘密は、前記第 1 のベクトルおよび前記第 2 のベクトルにより構築されるような、行ベクトルから転置された列ベクトルからなる請求項 11 記載の方法。

## 【請求項 13】

コンピュータ・プログラムの動作によって請求項 11 記載の方法を実行するための複数の命令を有することを特徴とするコンピュータ・プログラム。

## 【請求項 14】

請求項 1 から 12 のいずれか一項に記載の方法を実行するように構成される処理手段を備えることを特徴とする暗号化装置。

## 【請求項 15】

請求項 14 に記載の暗号化装置を具備することを特徴とするスマートカード。