(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第5426540号
(P5426540)

(45)発行日　平成26年2月26日(2014.2.26)　(24)登録日　平成25年12月6日(2013.12.6)

(51)Int.Cl.　F I
H04L 9/32 (2006.01)　H04L 9/00 675B
G09C 1/00 (2006.01)　G09C 1/00 620Z
G09C 1/00 650Z

請求項の数 15　(全 13 頁)

(21)出願番号　特願2010-512742 (P2010-512742)
(86)(22)出願日　平成20年6月20日 (2008.6.20)
(65)公表番号　特表2010-530990 (P2010-530990A)
(43)公表日　平成22年9月16日 (2010.9.16)
(86)国際出願番号　PCT/FR2008/000871
(87)国際公開番号　WO2009/016272
(87)国際公開日　平成21年2月5日 (2009.2.5)
審査請求日　平成23年6月15日 (2011.6.15)
(31)優先権主張番号　0704518
(32)優先日　平成19年6月22日 (2007.6.22)
(33)優先権主張国　フランス(FR)

(73)特許権者　501089863
サントル　ナシオナル　ドゥ　ラ　ルシェルシェサイアンティフィク（セエヌエールエス）
フランス国，エフ－７５０１６　パリ，リュ　ミッシェル　アンジュ３
(74)代理人　100099759
弁理士　青木　篤
(74)代理人　100092624
弁理士　鶴田　準一
(74)代理人　100122965
弁理士　水谷　好男
(74)代理人　100141162
弁理士　森　啓

最終頁に続く

(54)【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

(57)【特許請求の範囲】
【請求項１】
暗号装置が、公開行列に基づき、誤り訂正符号の復号を用いて暗号的に認証を行う方法であって、秘密鍵は低次のワードであり関連する公開鍵は前記公開行列と前記秘密鍵との積であり、前記公開行列は擬似巡回行列であり、
前記擬似巡回行列の要素の一部のみに関するデータが前記暗号装置のメモリに格納されゝ
前記暗号装置は前記データを用いて認証を行うことを特徴とする、暗号的に認証を行う方法。
【請求項２】
前記公開行列（Ｈ）は、ｋ行および２ｋ列を有し、且つ、ｋ*ｋのサイズの単位行列ブロックとｋ*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*ｋのサイズの単位行列ブロックであり、Ｃは、ｋ*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、３１７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・プロトコルまたはベロン・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２ｋ列を有する擬似巡回形の中間行列（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】

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

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、ベロン・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】

前記ベロン・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】

コンピュータに請求項１から１２のいずれか一項に記載の方法を実行させるための複数

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装置。
【請求項１５】
請求項１４に記載の暗号装置を具備することを特徴とするスマートカード。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、公開行列（ｐｕｂｌｉｃ　ｍａｔｒｉｘ）に基づき、誤り訂正符号の復号を用いて暗号的に認証を行う方法に関する。
【０００２】
本発明はまた、暗号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装置に関する。
【背景技術】
【０００３】
暗号的に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的に認証を行う方法は、現在のところ、リベスト（Ｒｉｖｅｓｔ）、シャミア（Ｓｈａｍｉｒ）およびエーデルマン（Ａｄｌｅｍａｎ）により開発されたＲＳＡアルゴリズムに基づいている。このＲＳＡアルゴリズムのセキュリティ（ｓｅｃｕｒｉｔｙ）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、このような暗号的に認証を行う方法は、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ＲＳＡ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（ＲＦタグ）のような、限られた処理能力を有する低価格の暗号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、前述のような暗号的に認証を行う方法は、現在のところ、これらの暗号装置には利用できない。
【０００６】
ＲＳＡアルゴリズムに基づいて暗号的に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的に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的に認証を行う方法に関するものである。
【０００８】
このような暗号的に認証を行う方法は、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、このような暗号的に認証を行う方法は、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】
暗号法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的に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，Ｃｍｍｕｎｉｃａｔｉｏｎ　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的に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，Ｃｍｍｕｎｉｃａｔｉｏｎ 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装置といったような、低価格の暗号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的に認証を行う方法を提供することにある。

【００２０】

より特定的にいえば、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的に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的に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、上記のような暗号的に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て

行われる。さらにまた、誤り訂正符号の復号を用いて暗号的に認証を行う方法は、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的に認証を行う方法が、暗号計算の速度を向上させるのを可能にすることを意味する。

【００２８】

それゆえに、本発明に従って暗号的に認証を行う方法は、暗号装置が、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、この暗号装置にて容易に実行される。

【００２９】

本発明に従って暗号的に認証を行う方法は、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・シンドロ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・シンドロ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、$k^{*}k$のサイズの単位行列ブロック（ｉｄｅｎｔｉｔｙ　ｂｌｏｃｋ）と$k^{*}k$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、公開データは、ｋのサイズのシンドローム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、シンドローム・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中間行列に基づいて構築され、この中間行列は、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、中間行列は、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】

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

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、公開データは、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に構成される処理手段を有する暗号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】

【００４４】

【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】

【００４５】

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的に認証を行う方法は、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。

【００４６】

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０６６１８４６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。

【００４７】

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。

【００４８】

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を保持している。さらに、秘密鍵は、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。

【００４９】

スターン・プロトコルを用いて認証を実行するに際して、ベリファイア（ｖｅｒｉｆｉｅｒ）Ｖに対してそれ自身を認証することを望むエンティティＰ、すなわち、プローバ（ｐｒｏｖｅｒ）を考える。複数回実行され、各回が正しく実行されれば、プローバＰである確率が増加していく。各回は、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にレスポンスを送る。ここで、ベリファイアＶは、プローバＰのレスポンスが、そのプローバＰの公開鍵と矛盾がないことを検証する。

【００５０】

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ができる。

【００５１】

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，Ｃｍｍｕｎｉｃａｔｉｏｎ ａｎｄ Ｃｏｍｐｕｔｉｎｇ，１９９７））を参照することができる。

【００５２】

ベロン・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】

ベロン・プロトコルを用いた認証を実行するに際して、このベロン・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。より特定的にいえば、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・プロトコルまたはベロン・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、ベロン・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，．．．，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，．．．，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・プロトコルおよびベロン・プロトコルにて使用されることが可能である。

【００６０】

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中間ブロック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】

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

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$A^{-1}.B$の結果として生成される行列は、Ｄと表わされる。

【００６１】

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。

【００６２】

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，．．．，a_{k-1}，a_k〕、ｂ＝〔b_1，b_2，．．．，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。

【００６３】

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^t〔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。

【００６４】

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）^{t}〔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。

【００６５】

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。

【００６６】

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－Ｖａｒｓｈａｎｏｖ　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。

【００６７】

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。

【００６８】

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、シンドローム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はシンドローム、Ｘは秘密鍵（ｓｅｃｒｅｔ　ｋｅｙ）、そして、Ｈは公開行列である。

【００６９】

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。

【００７０】

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。

【００７１】

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的に認証を行う方法は、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、暗号装置にて容易に実行され得る。

【００７２】

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。

【００７３】

本発明に従って暗号的に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。暗号装置はまた、暗号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。

【００７４】

本発明に従って暗号的に認証を行う方法が、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。

【図１】

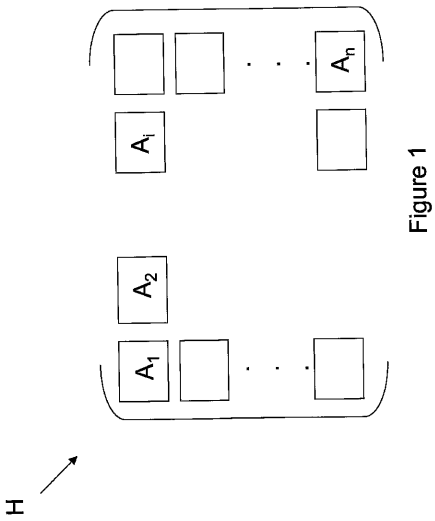

Figure 1

【図２】

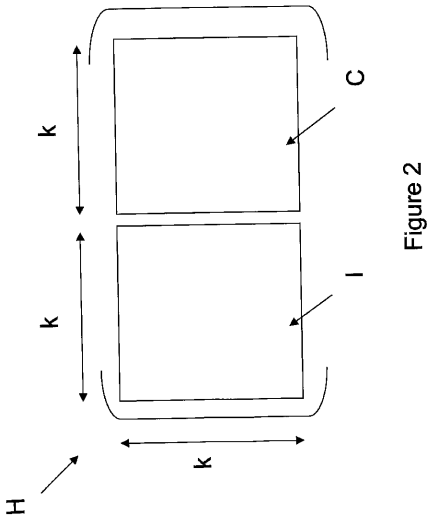

Figure 2

【図３】

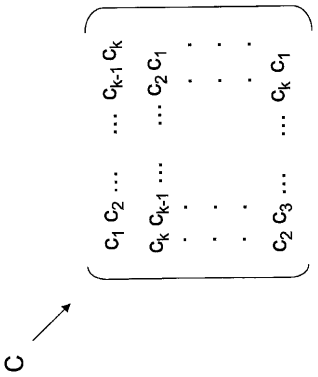

Figure 3

【図４】

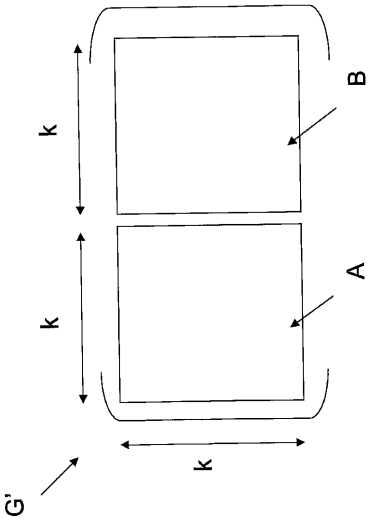

Figure 4

【図５】

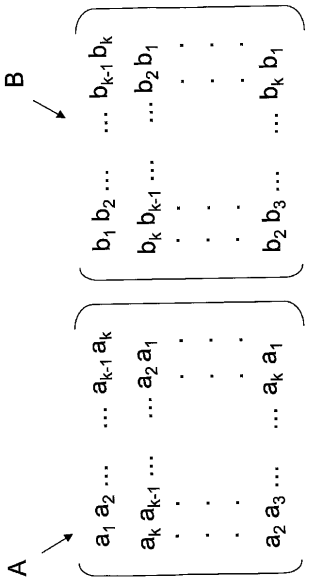

Figure 5

フロントページの続き

(72)発明者　ガボリ，フィリップ
フランス国，エフ－８７０００　リモージュ，リュ　グフィール　ドゥ　ラストゥール，１２

審査官　青木　重徳

(56)参考文献　特開２００６－１３３３８０（ＪＰ，Ａ）
特開平０７－２３５９２２（ＪＰ，Ａ）
特表２０００－５１６７３３（ＪＰ，Ａ）
畑雅恭，橋本和憲，武田成史，“高次元対称符号の形成とトポロジーに関する考察　－誤り訂正同時暗号符号化について－”，電子情報通信学会技術研究報告，日本，社団法人電子情報通信学会，１９９１年　9月19日，Ｖｏｌ．９１，Ｎｏ．２２５，ｐ．１－１１
笠原正雄，“代数的誤り訂正符号とランダム符号化に基づく拡大体上の公開鍵暗号”，電子情報通信学会技術研究報告，日本，社団法人電子情報通信学会［オンライン］，２００４年１１月１日，Ｖｏｌ．１０４，Ｎｏ．４２１，ｐ．２１－２６，［平成２５年　1月１７日検索］，インターネット，ＵＲＬ，<http://ci.nii.ac.jp/els/110003204397.pdf?id=ART0003631922&type=pdf&lang=jp&host=cinii&order_no=&ppv_type=0&lang_sw=&no=1358403236&cp=>
笠原正雄，“ランダム符号化に基づくK行列ＰＫＣ　－新しいＳＥ（ｇ）－ＰＫＣの提案と合わせて－”，電子情報通信学会技術研究報告，日本，社団法人電子情報通信学会［オンライン］，２００６年　3月１０日，Ｖｏｌ．１０５，Ｎｏ．６６４，ｐ．１１３－１１８，［平成２５年　1月１７日検索］，インターネット，ＵＲＬ，<http://ci.nii.ac.jp/els/110004680292.pdf?id=ART0007412096&type=pdf&lang=jp&host=cinii&order_no=&ppv_type=0&lang_sw=&no=1358403414&cp=>
山川　茂紀，崔　洋，萩原　学，古原　和邦，今井　秀樹，“ＬＤＰＣ符号を用いたＭｃＥｌｉｅｃｅ署名方式”，電子情報通信学会技術研究報告，日本，社団法人電子情報通信学会，２００９年　3月　2日，Ｖｏｌ．１０８，Ｎｏ．４７３，ｐ．５３７－５４３
Philippe Gaborit, Cedric Lauradoux, Nicolas Sendrier, “SYND: a Fast Code-Based Stream Ciper with a Security Reduction”, IEEE International Symposium on Information Theory (ISIT 2007), [online], ２００７年　6月２４日, p.186-190, [retrieved on 2013-01-17]. Retrieved from the Internet, ＵＲＬ, <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4557224>

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／３２
Ｇ０９Ｃ　　１／００