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

特許第4819269号
(P4819269)

(45)発行日　平成23年11月24日(2011.11.24)　(24)登録日　平成23年9月9日(2011.9.9)

(51)Int.Cl.		F I		
H04L 9/32	(2006.01)	H04L	9/00	675A
G06F 21/20	(2006.01)	H04L	9/00	673D
H04L 9/30	(2006.01)	G06F	15/00	330F
		H04L	9/00	663Z

請求項の数 26　(全 18 頁)

(21)出願番号	特願2001-518980 (P2001-518980)
(86)(22)出願日	平成12年8月4日(2000.8.4)
(65)公表番号	特表2003-507964 (P2003-507964A)
(43)公表日	平成15年2月25日(2003.2.25)
(86)国際出願番号	PCT/EP2000/007597
(87)国際公開番号	WO2001/015378
(87)国際公開日	平成13年3月1日(2001.3.1)
審査請求日	平成19年8月3日(2007.8.3)
(31)優先権主張番号	199 40 341.4
(32)優先日	平成11年8月25日(1999.8.25)
(33)優先権主張国	ドイツ(DE)

(73)特許権者　596007511
ギーゼッケ　ウント　デブリエント　ゲーエムベーハー
Ｇｉｅｓｅｃｋｅ　＆　Ｄｅｖｒｉｅｎｔ　ＧｍｂＨ
ドイツ連邦共和国　Ｄ－８１６７７　ミュンヘン　プリンツレーゲンテンシュトラッセ　１５９
(74)代理人　100073184
弁理士　柳田　征史
(74)代理人　100090468
弁理士　佐久間　剛

最終頁に続く

(54)【発明の名称】データを保護するための方法

(57)【特許請求の範囲】
【請求項１】
データの保護方法を実行するための装置であって、
（ａ）デジタル化生物測定学的特徴データを作成するために生物測定学的特徴をデジタル化するための手段と、
（ｂ）秘密データを提供するための手段と、
を備え、
（ｃ）前記秘密データをフォールトトレラントであるように符号化と復号化を行うための手段と、
（ｄ）デジタル化生物測定学的特徴データを手掛かりに、前記フォールトトレラントに符号化された秘密データの暗号化と暗号解除を行うための手段と、
を有することを特徴とする装置。
【請求項２】
コードワードを作成するための手段を更に有することを特徴とする請求項１記載の装置。
【請求項３】
初期訂正データを作成するための手段を更に有することを特徴とする請求項１記載の装置。
【請求項４】
ハッシュ値を生成するための手段を更に有することを特徴とする請求項１から３のいず

れか1項記載の装置。
【請求項５】
前記生物測定学的特徴を公開部分と秘密部分に分解するための手段を更に有することを特徴とする請求項１から４のいずれか１項記載の装置。
【請求項６】
前記分解するための手段は、統計的照会を手掛かりに前記生物測定学的特徴を公開部分と秘密部分とに分解することを特徴とする請求項５記載の装置。
【請求項７】
手書き署名を生物測定学的特徴として取得するための手段を更に有することを特徴とする請求項１から６のいずれか１項記載の装置。
【請求項８】
データを保護するための装置を動作させる方法であって、
（ａ）正当な利用者が生物測定学的特徴を提供するステップと、
（ｂ）デジタル化するための手段が、前記生物測定学的特徴をデジタル化して、デジタル化生物測定学的認証特徴データを作成するステップと、
（ｃ）暗号化と暗号解除を行うための手段が、前記デジタル化生物測定学的認証特徴データに基づいて暗号化コードワードを暗号解除するステップと、
（ｄ）秘密データを復元するための手段が、前記暗号解除された暗号化コードワードから、自由に選択できる訂正容量を有する符号理論法に基づいて、秘密データを復元するステップと、
を含む認証段階を有することを特徴とする方法。
【請求項９】
（ａ）前記正当な利用者が生物測定学的特徴を提供するステップと、
（ｂ） デジタル化するための手段が、前記生物測定学的特徴をデジタル化して、デジタル化生物測定学的特徴データを作成するステップと、
（ｃ） 秘密データを提供するための手段が秘密データを提供するステップと、
（ｄ） 暗号化と暗号解除を行うための手段が、前記デジタル化生物測定学的特徴データに基づいて前記秘密データを暗号化し、符号化と復号化を行うための手段が、前記秘密データをフォールトトレラントであるように符号化するステップと、
を含む初期設定段階を有することを特徴とする請求項８記載の方法。
【請求項１０】
連続したステップとして、
（ａ）符号化と復号化を行うための手段が、前記秘密データをフォールトトレラントであるように符号化してコードワードを作成するステップと、
（ｂ）暗号化と暗号解除を行うための手段が、前記デジタル化生物測定学的特徴データに基づいて前記コードワードを暗号化して暗号化コードワードを作成するステップと、
を有することを特徴とする請求項９記載の方法。
【請求項１１】
コードワードを作成するための手段が、前記コードワードを生成行列から作成することを特徴とする請求項１０記載の方法。
【請求項１２】
初期訂正データを作成するための手段が、許容コードワードの領域を記述する初期訂正データを作成するステップを有することを特徴とする請求項９記載の方法。
【請求項１３】
初期訂正データを作成するための手段が、前記デジタル化生物測定学的特徴データに基づいて初期訂正データを作成するステップを有することを特徴とする請求項９記載の方法。
【請求項１４】
（ａ）認証訂正データを作成するための手段が、前記デジタル化生物測定学的認証特徴データに基づいて認証訂正データを作成するステップと、

（ｂ）生物測定学的特徴データを復元するための手段が、前記認証および初期訂正データに基づいて前記デジタル化生物測定学的特徴データを復元するステップと、
（ｃ）暗号化と暗号解除を行うための手段が、前記復元されたデジタル化生物測定学的特徴データに基づいて暗号化秘密データを暗号解除するステップと、
を有することを特徴とする請求項１２または１３記載の方法。
【請求項１５】
前記初期訂正データがｎを法とするデジタル化生物測定学的特徴データの計算によって作成されることを特徴とする請求項１３記載の方法。
【請求項１６】
前記認証訂正データがｎを法とする前記認証特徴データの計算によって作成されることを特徴とする請求項１４記載の方法。
【請求項１７】
利用者固有の初期訂正データ符号化ステップおよび／または利用者固有のフォールトトレラント符号化ステップを有することを特徴とする請求項１２から１６のいずれか１項記載の方法。
【請求項１８】
データを分解するための手段が、公開部分と秘密部分を、前記生物測定学的特徴から割り出しまたは予測することを特徴とする請求項９から１７のいずれか1項記載の方法。
【請求項１９】
データを分解するための手段が、前記生物測定学的特徴の公開部分と秘密部分への分離を、経験的照会を手掛かりに実行することを特徴とする請求項１８記載の方法。
【請求項２０】
ハッシュ値を生成するための手段が、ハッシュ関数を利用してデジタル化生物測定学的特徴データからハッシュ値を作成することを特徴とする請求項９から１８のいずれか１項記載の方法。
【請求項２１】
ハッシュ値を生成するための手段が、ハッシュ関数を利用して前記デジタル化生物測定学的認証特徴データからハッシュ値を作成することを特徴とする請求項８から２０のいずれか１項記載の方法。
【請求項２２】
前記生物測定学的特徴が行動バイオメトリックであることを特徴とする請求項８から２１のいずれか１項記載の方法。
【請求項２３】
前記生物測定学的特徴が手書き署名から成ることを特徴とする請求項８から２２のいずれか1項記載の方法。
【請求項２４】
データを分解するための手段が、手書き署名を公開部分と秘密部分とに分解し、前記秘密部分が前記署名の動的情報の正規のサブセットであることを特徴とする請求項２３記載の方法。
【請求項２５】
前記生物測定学的特徴の提供および／またはデジタル化が複数回実行されることを特徴とする請求項８から２４のいずれか1項記載の方法。
【請求項２６】
秘密データを提供するための手段が、前記秘密データを公開鍵方法で生成することを特徴とする請求項８から２５のいずれか1項記載の方法。
【発明の詳細な説明】
【０００１】
本発明はデータの保護に関し、特に生物測定学的特徴に基づいたデジタルデータの真正性と完全性を保証するための方法に関する。
【０００２】

経済のほぼ全分野においてグローバリゼーションが一層の進展をみせるなか、特に新しい情報技術の重要性はますます高まってきている。これは、主に、電子通信網の利用の進展に適用される。その最もよく知られた形態はおそらくインターネットであろう。製品とサービスの国際的な交易の増加によって、情報の安全な発信が絶対的に必要なものとなった。現在、金融取引額は製品交易額の何倍にもなっている。このデータトラフィックは現在、電子通信網上で一定の形態で取り扱われる（例えば、ｅコマースなどの電子取引）。この形態の通信は、非電子領域と同様に、当該取引の当事者が取引時に内容と相手方の本人性に関する陳述書（特に意思表明書）を信用できるようにする必要を伴う。しかし、このような電子取引（オンライン取引）は通常、当事者同士の直接的な連絡を伴わず、電子的な形態のデータが存在するだけであるため、それ以外の場合に通常行われるような直接の対話によって実現できない。不正操作に対抗した取引データの認証と保護が可能でなければ、実現は望めないのである。データ保全性の確実なチェックも、電子保存個人データの保護に関して大きな重要性を有する。デジタル署名は、データの真正性と完全性を確保するひとつの方法である。認証を受けた人、グループ、または装置だけがデータに変更を加えることができる。また、署名が本物であるかどうか誰もが確認することができる。

【０００３】

公知の署名方法では、いわゆる非対称暗号化方式を使用する。このような方法の基本的な過程は、以下に略述する。

【０００４】

この署名システムの各参加者について、秘密鍵と公開鍵など、互いに一定の数学的関係を有するキーペアが生成される。デジタル署名を生成するには、送信者が自分の秘密鍵を通常は特殊署名特徴として使用する。署名対象の文書はまず、いわゆるハッシュ方法によって圧縮され、その結果得られるダイジェストが所定のアルゴリズムに従って秘密鍵とリンクされ、その結果が転送対象文書にデジタル署名として追加される。受信者は同様にここでその文書を圧縮して、このダイジェストを、その署名を送信者の公開鍵で暗号解除することで得られるデジタル署名に含まれるダイジェストと比較する。一致の場合は、送信テキストと受信テキストが同じであること、つまり不正操作も転送エラーも発生していないことが確実である。また、秘密鍵を所有する送信者が当該署名を生成できたことも確実である。何故なら、そうでないと、公開鍵は「合う」ことはないのであり、原ダイジェストへの変換が発生することがありえないのである。

【０００５】

今日の署名方法のセキュリティは、平文、署名文、および関連公開署名鍵をハッカーが入手した場合でも、現行の知識レベルでは個人署名鍵を割り出せないという事実に基づいている。非対称暗号化方式の１つの例がＲＳＡである。このＲＳＡ法は、１９７７年（”On Digital Signatures and Public Key Cryptosystems（デジタル署名と公開鍵暗号システムについて）”, MIT Laboratory for Computer Science Technical Memorandum 82, １９７７年4月）と１９７８年（”A Method for Obtaining Digital Signatures and Public−Key Cryptosystems（デジタル署名を取得する方法と公開鍵暗号システム）”, Communications of the ACM 2／１９７８）にこの方法を提示した開発者のRonald L. Rivest、Adi Shamir、およびLeonard Adlemanにちなんで命名された。ＲＳＡは整数論的考察に基づくもので、大きな数字が因数分解しにくい、つまり素因数に分解しにくいことを前提としている。これは、いわゆる因数分解の問題である。これに要する計算量が膨大であるため、この暗号化はたとえ鍵が適切に選択された場合でもブルートフォース攻撃で破ることは事実上不可能である。暗号解読攻撃で公表されているものはない。

【０００６】

このため、このような非対象暗号化方法は、署名文書と署名鍵との一意の関連付けが可能にする。署名文書と人または組織との関連付けにはまだ問題点がある。しかし、それが成

功するためには、次の条件が保証される必要がある。第一に、権利を有する所有者だけが自分の個人署名鍵にアクセスできること、第二に、各公開鍵がそれに一意に関連付けられた関連秘密鍵の正当な所有者を有することである。

【０００７】

第一の条件を満たすため、その署名鍵の正当な所有者を生物測定学的特徴によって識別する可能性が存在する。

【０００８】

第二の条件を満たすため、多くのシステムは、いわゆる信頼できる第三者機関、つまり、取引に直接関与せずその信用性が確かであると考えられる第三者を含む。相互の信頼とチェックのシステムは、トラストモデルと呼ばれることが多い。

【０００９】

認証とデータ完全性チェックへの署名方法の利用の例としては、インターネットやその他のデータネットワーク上で電子的に締結される契約、電子取引（ｅコマース）、資源への条件付きアクセス（データ接続または外部記憶装置など）、エクスポートされ生産プラントに読み込まれるプロセス制御データ、個人データ管理（患者データ管理または政府関連機関内）などである。

【００１０】

すべてのセキュリティシステムと同様に、今日公知となっている署名方法は、攻撃を受ける可能性が数多く存在する。これらが、図６の表に示されている。

【００１１】

公知の署名システムにはは、たとえばいわゆるスマートカードシステムなどがある。スマートカードを利用した多くのシステムは、鍵自体に対する攻撃（暗号解読攻撃）、ブルートフォース攻撃（ＢＦＡ）、そして鍵を保存するハードウェアに対する攻撃からの良好な保護を提供する。しかし、リプレイおよびフェイクターミナル攻撃（ＲＡ）、および利用者に対する攻撃は比較的有望であり、従ってスマートカードシステムはかかる攻撃に関してはセキュリティリスクとなる。

【００１２】

システムによっては、署名鍵の盗用から利用者を保護しようとするものもある。個人識別番号（ＰＩＮ）と生物測定方法の両方が使用される。トラストモデルへの攻撃（ＴＭＡ）については、大半の提供業者は認証システムを検討さえしていない。

【００１３】

以下において、デジタル署名と生物測定学的特徴の測定を組み合わせた従来のシステムについて記述する。顧客の秘密署名鍵と、測定した生物測定学的特徴のデジタル表現のサンプルまたはプロトタイプ（いわゆるテンプレート）は、いずれも保存された形態で存在している。次の特定の認証手順が取られる。ＰＩＮを入力するかまたは生物測定学的特徴を読み取らせるなどして、利用者が本人性を確認する。この生物測定データは、テンプレートとの比較によって検証される。測定された特徴のプロトタイプからの距離が閾値よりも小さい場合は、その取引は有効になる。この比較は、読取装置または中央クリアランスハウスの中で実行される。後者のケースでは、（暗号化されたまたは平文の）生物測定データは、ネットワーク上を転送される。秘密署名鍵が公開される。利用者が文書にデジタル署名することにより本人性を確認する。ＲＳＡ方式または他の非対称暗号化方式が通常実装される。これは、スマートカードまたはその他の不正操作不能なハードウェアに実装されることが多い。署名入りハードウェア。署名された文書はネットワーク上を転送される。暗号操作は、利用者の公開署名鍵によって検証される。

【００１４】

上記の各方式のセキュリティは、スマートカードから離れることのない秘密署名鍵に基づいている。このため、スマートカードが正当な所有者の手にあるかぎり、秘密の署名鍵自体への「マン・イン・ザ・ミドル」攻撃（ＭＭＡ）は不可能である。

【００１５】

顧客の個人署名鍵と、測定された生物測定学的特徴のデジタル表現のプロトタイプとの両

方が保存形態で存在する方式の一例が、国際特許出願公開第９９／１２１４４　Ａ１号に記載されている。

【００１６】

国際特許出願公開第９９／１２１４４　Ａ１号で提案された方式は、テンプレートが中央クリアリングハウス内に保存形式で存在することを規定する。後者は、測定された生物測定学的特徴のプロトタイプからの距離が閾値より小さい場合には、利用者の名前をデジタル署名する。

【００１７】

しかし、国際特許出願公開第９９／１２１４４　Ａ１号で提案される方式は、本質的に一定のセキュリティ問題を伴うという欠点を有する。第一に、利用者は、生物測定学的特徴の読み込みを行う読取装置、クリアリングハウス、および公衆網を信頼しなければならない。従って、フェイクターミナル攻撃が発生する可能性がある。次に、生物測定学的特徴のデジタル表現が読取装置に読み込まれることがある（いわゆるリプレイ攻撃（ＲＡ））。第二に、読取装置またはテンプレートを保存するエンティティに対する攻撃（ＳＫＴ）も起こり得る。このような攻撃は、測定された生物測定学的特徴のデジタル表現のテンプレートを読み取ることを目的としている。こうした攻撃はまたオンラインでも実行される可能性がある（ＭＭＡ）。第三に、測定された生物測定学的特徴のデジタル表現のテンプレートに関連付けられたデータが交換される可能性がある（ＳＴＸ）。

【００１８】

国際特許出願公開第９８／５０８７５号は、デジタル署名方法と生物測定を使用したいわゆる生物測定識別方式について記述している。この方式は、測定した生物測定学的特徴のデジタル表現のテンプレートがいわゆる生物測定証明書内への保存によって交換されることを防止する。テンプレート、そしてそれに関連付けられた利用者データは、認証局（ＣＡ）によって検証されデジタル署名される。これにより、そのテンプレートに関連付けられた利用者データは交換できなくなる。ただし、この欠点は、リプレイ攻撃の可能性を排除できないことである。

【００１９】

国際特許出願公開第９８／５２３１７号も同様にデジタル署名方法について記述している。国際特許出願公開第９８／５２３１７号に基づく方法は、生物測定学的特徴（ＢＭ）のデジタル表現（テンプレート）の保存をなしにすることによってＳＴＴおよびＳＴＸ攻撃を阻止しようとする。初期設定段階でＢＭを使用して、ＢＭをソリューションとする問題のいわゆるインスタンス、つまりクラスの代表的または特定の例を作成する。このため、デジタル表現は明示的に保存されず、その問題のインスタンスの中に隠される。国際特許出願公開第９８／５２３１７号は、このデジタル表現が類似データの塊（カモフラージュ）の中に隠されるようこの問題を設計することを提案している。

【００２０】

更なるコンピュータ援用処理を行うための生物測定学的特徴の捕捉では、分解能が非常に正確ではあるが常に有限であるためにデジタル化測定値の丸め誤差を出すことの多いアナログ・デジタル変換を前提としている。更に、生物測定学的特徴の捕捉時に測定センサーシステムに対して利用者がまったく同じ姿勢を取ると想定することは非現実的である。行動生物測定学的特徴の測定は、利用者に自分の行動を２度正確に複製することを期待できないという別の問題を伴う。しかし、生物測定学的特徴を利用するポイントは、人との絶対的に唯一の関連性である（例： 指紋、網膜）。従って、必要なフォールトトレランスに関する情報、あるいは様々な測定値がどのようにして唯一の関連を生むかに関する情報が絶対必要である。国際特許出願公開第９８／５２３１７号は、この方法のフォールトトレランスがどれくらいかについて情報を全く提供していない。また、この問題のソリューションが読み取られないためにどれくらいの量のカモフラージュ情報が必要であるかについても不明である。この方法のセキュリティを定量化または単にそれを評価するだけの場合でも、これは必要な条件である。

【００２１】

ドイツ国公開特許第４２４３９０８　Ａ１号は、秘密署名鍵の保存を行うことをやめ、また生物測定学的特徴のデジタル表現の保存をせずに、ＰＫＴ、ＴＡ、ＳＴＴ、およびＳＴＸを防止しようとする。これは、次のようにして行われる。生物測定学的特徴ＡＢＭが測定される。生物測定学的特徴ＡＢＭがデジタル化される。この生物測定学的特徴のデジタル表現から、いわゆる固定長個別値ＩＷが計算される。個別値ＩＷから、送信者の秘密署名鍵ＳＫ（Ａ）が計算される。このメッセージは、上記キーＳＫ（Ａ）によって暗号化される。

【００２２】

しかし、ＩＷの計算が、一定のフォールトトレランスを有する関数ｆによって行われるのは、不利である。その理由は、極めて大きな重要性をもつこのフォールトトレランスがそのような関数についてどのように決定されるかが不明であるからである。この用途では、単に、それが「システムのセキュリティに適合する低い蓋然性を以ってのみ」２人のユーザに同じ個別値を割り当てることが要求される。どの関数またはどのクラスの関数がその用途で必要とされる特性を有するかが不明であることが、同様に不利である。その代わりに、この用途の記述は、関数ｆに無衝突性が必要であるが、言い換えれば、同一の関数値に２つの入力値をみつけることは不可能でなくてはならないが、にもかかわらずこれは一定のフォールトトレランスを有することになる。これらの１８０°正反対の条件を有するこのような関数は定義上存在できない。この結果は、同一の生物測定学的特徴の新測定値からの同じ秘密鍵の常に複製可能な生成が間違いなく不可能であること、つまり署名された文書またはデータは公知の公開鍵では識別も認証もできないことである。

【００２３】

米国特許第５８３２０９１号は、指紋から一意の値を取得するための方法について記述している。この方法は以下のように機能する。第一のステップで、指紋はフーリエ変換される。次に、フーリエ係数が、その指紋のテンプレートおよび測定装置の解像度に依存する画像化に付される。逆変換から一意の値が取得され、そこから署名鍵が決定できる。しかし、この方法は次の欠点を有する。この方法は指紋についてのみ機能すること。この方法はフーリエ変換を必要とすること。テンプレートに依存する画像化ではテンプレートについてこの方法がどれくらいの量の情報を明らかにするのか割り出せないことである。そのため、ブルートフォース攻撃に対するセキュリティレベルを定量化することはできず、この方法は、測定装置の分解能に起因するエラーを訂正するだけである。指先のホコリや小さな傷に起因するエラーが訂正されるかどうかも不明である。

【００２４】

このため、上述の方法はすべて、ブルートフォース攻撃の計算量およびその結果として暗号解除からの保護に関する量的な表現ができないという欠点を共有している。そのため、これらは、生物測定による保護の定量化には利用できない。

【００２５】

対照的に、本発明は、先行技術の各方式に比べてセキュリティレベルの高いデータ保護方法をどう提供するかという課題に基づいている。

【００２６】

さらに、生物測定学的特徴によって署名鍵の安全な暗号化を可能にする方法を提供することは、本発明の課題である。

【００２７】

本発明の更なる課題は、かかる方法において生物測定による暗号の保護を定量化する可能性を提供することである。

【００２８】

これらの各課題は、請求項１と８に述べた特徴によって解決される。

【００２９】

本用途では、本発明は、秘密鍵（署名鍵）が署名鍵所有者の生物測定学的特徴から取得したデータとともに暗号化される署名方法を利用する。この暗号化は、自分のデジタル署名を署名鍵を使って与えた人が実は正当な所有者であるとの保証を実現する。

【００３０】
第一のステップでは、署名鍵の所有者の生物測定学的特徴、できればその所有者の手書き署名が認証段階（検証）で提供される。この生物測定学的特徴から測定データが取得される。
【００３１】
第二のステップでは、この生物測定学的特徴の測定データが収集および更なる処理のためにデジタル化される。
【００３２】
第三のステップでは、その署名鍵が復元される。署名鍵はまず認証段階で測定された生物測定学的特徴に基づいて暗号解除され、次に符号理論方式に基づいて復元される。あるいは、初期設定段階で測定された生物測定学的特徴は、認証段階で測定された生物測定学的特徴から符号理論に基づいて最初に復元することができる。これはその後に署名鍵を暗号解除する。誤り訂正方法の訂正容量は自由に選択できる。つまり、元のフォールトトレラントの符号化された値は、このエラー訂正方法の入力が逸脱しすぎない場合にのみ復元される。
【００３３】
この用途による方法では、秘密データ、つまり署名鍵とデジタル化した特徴データあるいはその秘密の部分のいかなる点においても保存がなく、その結果、生物測定学的特徴のプロトタイプを交換または盗用することはできない。従って、本用途による本方法は、以下の攻撃の可能性に対処する。
【００３４】
●非対称暗号化方法によりＫＡに対処。
【００３５】
●ＰＫＴ攻撃は署名鍵が保存されないため不可能。
【００３６】
●ＳＴＴおよびＳＴＸ攻撃は生物測定学的特徴のデジタル表現、あるいはその関連秘密部分が保存されないことから同様に防止される。
【００３７】
●ＭＭＡ攻撃は生物測定学的特徴がデータネットワーク上を転送されないことから防止される。
【００３８】
●有利な実施態様では、生物測定学的特徴が外部読取装置に読み込まれないことによってＲＡ攻撃が防止される。外部読取装置を想定した他の有利な実施態様では、ＲＡ攻撃は、特に請求項７に記載の方法が生物測定学的特徴の２つのまったく同一のデジタル表現を拒絶することから先行技術に比較されて、妨げられる。
【００３９】
請求項９は、本用途に基づく方法の初期設定段階（登録）から認証段階の有利な実施態様である。１つのステップでは関連する生物測定学的特徴がそれに応じてデジタル化される。他のステップでは秘密のデータが提供される。公開鍵の場合、非対称署名方法に必要な鍵生成、つまり署名鍵の生成が実行される。他のステップでは、秘密データが、符号理論方式を基にしてフォールトトレラントであるように符号化され、生物測定学的特徴に基づいて暗号化される。
【００４０】
請求項１０は、初期設定段階の有利な実施態様である。秘密データがまず最初にフォールトトレラントであるように符号化される。結果として得られるコードワードは原メッセージよりも長い。この冗長情報はいくつかのビットが反転したメッセージを復号する役割を果たす。このコードワードは次に生物測定学的特徴に基づいて暗号化される。
【００４１】
請求項１１は、請求項１０に記載した方法の有利な実施態様である。このコードワードは、秘密データを生成行列に掛けることにより生成される。これは、例えば許可されたコー

ドワードの領域を表現するための効率的な方法です。

【００４２】

請求項１２は、初期設定段階の変形例である。秘密データ（メッセージ）は、符号化によって変更されない。その代わりに、別の訂正データ（初期訂正データ）が生成される。上記データは、許可されたコードワードの領域を記述する。

【００４４】

請求項１３は、初期設定段階の他の変形例である。別の訂正データが生物測定学的特徴に依存して作成される。

【００４５】

請求項１４は、認証段階の変形例である。認証段階では、別の訂正データ（認証訂正データ）がまず生物測定学的特徴に依存して作成される。他のステップで、初期設定段階で測定されたこの生物測定学的特徴が復元される。これは、上記の訂正データ、つまり初期設定段階で作成された訂正データと認証段階で測定された生物測定学的特徴に基づいて行われる。他のステップでは、復元された生物測定学的特徴データを基にして秘密データが復号される。

【００４６】

請求項１５は、請求項１４に記載された方法の変形例である。訂正データは、ｎを法とする生物測定学的特徴から取得された各パラメータの計算によって作成される。上記データに基づいて、真の値からのずれがｎ以下の値が真の値の上にマッピングされ、ずれがｎより大きい値がランダム値の上にマッピングされる。

【００４７】

請求項１６は、請求項１４に記載の方法の変形例である。認証訂正データは、請求項１５、ｎを法とする生物測定学的認証特徴から得たパラメータの計算、に記載の方法にあるとおり、作成される。この生物測定学的特徴データは、各剰余の差を決定することにより復元される。これはまさに、ずれがｎより小さいときの各値の差である。

【００４８】

請求項１７は、訂正方法が利用者固有の実施態様である。これを使用すると、訂正能力を利用者内の生物測定学的特徴の差異にあわせて構成できる。

【００４９】

請求項１８によれば、デジタル化された特徴はさらに、ブルートフォース攻撃の労力を定量化する可能性と、また、システムが適切に設計されている場合には、生物測定による保護に対するシステムの一般的定量化を提供するための第二のステップの中で、公開部分と非公開または秘密部分に分解される。生物測定学的特徴の非公開部分だけが署名鍵を符号化するために利用されるため、ブルートフォース攻撃の労力は依然として定量化可能である。

【００５０】

請求項１９によれば、デジタル化した生物測定学的特徴データの分解には、経験的照会が現在最も簡単に実行されることから、経験的照会を利用するのが好ましい。

【００５１】

請求項２０によれば、ハッシュ値は、デジタル化した生物測定学的特徴データまたは秘密鍵または署名鍵を符号化するためのその非公開部分からハッシュ機能を用いて作成されるのが好ましい。これは、特徴データを固定長ビットストリングにする利点、そしてその結果、関連署名鍵の符号化を簡素化して、ＸＯＲ演算などで簡単に実行できるようにする利点を有する。

【００５２】

請求項２１によれば、ハッシュ値はまだ、認証段階で作成されたデジタル化生物測定学的特徴データから、ハッシュ機能を用いて作成され、既に保存されている前の認証のハッシュ値と比較されるのが好ましい。このハッシュ機能はいわゆるワンウェイ機能の特殊な形態であるため、無衝突性という特性を有する。無衝突性という用語は、暗号法では、類似しているが同一でないテキストが完全に異なるチェックサムを発生することを意味すると

理解されている。テキストの各ビットは、このチェックサムに影響を与えなければならない。これは、簡単な言葉では、この機能が同一入力値の場合には、固定ビット長の正確に１つの同一出力値を常に発生することを意味する。この特性は、同じ生物測定学的特徴が上記のように繰り返して捕捉されるとき、正確に２つの同一測定データレコードを取得することが事実上不可能であるため、この用途に基づく方法により活用される。したがって、現行ハッシュ値と保存ハッシュ値との比較が肯定的な結果をもたらす場合、これは、リプレイ攻撃が関与している可能性を強く指示している。セキュリティは、従って、認証を中止することによって保証できる。

【００５３】

請求項２２と２３によれば、本方法に使用する生物測定学的特徴が行動バイオメトリクスであるのが好ましい。これらは偽造が困難であるという利点を有する。各パターンまたは特徴の単純なコピーは事実上排除される。

【００５４】

請求項２４によれば、本用途に基づく方法は、手書き署名が動的および静的部分に簡単に分解でき、これが生物測定学的特徴を秘密部分と公開部分に分解する役割を果たすことから、手書き署名を行動バイオメトリックとして使用する。

【００５５】

請求項２５によれば、この手書き署名は、署名の秘密部分が動的情報の適切なサブセットとなり、それによって定量化を可能にしあるいは定量化を可能な状態に保持するよう、公開部分と秘密部分とに分解されることが好ましい。

【００５７】

請求項２６によれば、一般普及率と信頼性の高さにより、従来の公開鍵方式が鍵生成に提案されるのが好ましい。

【００５８】

請求項１から７によれば、上記した手法を採用するデータ保護方法を簡単に実行するための装置が提案される。

【００５９】

本用途に基づく方法は、このように、先行技術に比べて大きな度合いのデータ保護を可能にする。さらに、本発明に基づく方法は、秘密データの保存によって署名方法への攻撃に弱い点を新たに作ることなく、署名鍵の符号化または暗号化を可能にする。本用途に基づく方法と装置は更に、個人またはグループの安全な認証を可能にする。本発明に基づく方法は更に、生物測定学的特徴から、ＰＩＮまたはＲＳＡなどの暗号方式への入力として使用できる再生可能な値の決定を可能にする。また、この方法と装置は、生物測定による保護の定量化、つまりブルートフォース攻撃の労力の予測に基本的に利用しやすい。本発明に基づく方法とは異なり、既存の各方法は、ＳＳＴまたはＳＴＸなどの他の攻撃を排除できない。つまりブルートフォースが最善の攻撃方法となるようにはできないのである。生物測定プロトタイプなどの盗用などとは異なり、ブルートフォースは、少しでも定量化可能な唯一の攻撃である。生物測定学的特徴の秘密部分が少なくとも署名鍵自体と同じ長さであれば、生物測定学的特徴の秘密部分は少なくとも署名鍵へのブルートフォース攻撃と同じ労力を要する。これは、少なくともブルートフォース攻撃で署名鍵を推定するのに必要な労力に関する数値表現を許可する。そのため、生物測定による署名鍵の追加暗号化とともに署名方式を使用してデータを保護する本用途に基づく方法のセキュリティレベルがどれくらいかを定量化することは可能である。

【００６０】

本発明の他の特徴と利点は、下位の請求項と、図面を参照した例の以下の説明の中に記載した。

【００６１】

電子商取引では、その取引当事者の本人性と取引データの完全性が明確に確認できることが何よりも重要である。取引の当事者の本人性を認証するための様々な方法がある。

【００６２】

知識による識別では、識別は、実際には通常パスワード、パスフレーズ、あるいはＰＩＮなどの共有秘密によって行われる。所有物による識別では、識別は、署名鍵や個人識別カードなどによって行われる。生物測定による識別では、指紋、瞳孔パターンによって行われる。

【００６３】

同様に、上記の各方法の色々な組合せが可能である。このため、ｅｃカードで取引を行う者は所有物（カード）と知識（ＰＩＮ）により本人性を確認することになる。

【００６４】

高いセキュリティ要件を満たせない認証方法もある。このため、知識による識別は常に、利用者がパスフレーズまたはＰＩＮを書き留める危険を伴う。更に、パスフレーズまたはＰＩＮは、保存データから暗号解読により判別できる。このような危険に対抗するため、多くの新しい認証方法ではデジタル署名を利用している。デジタル署名は別の利点も有する。これらは、署名データの完全性を同時に確保する。つまり、署名とデータは不可分に織り合わされているのである。

【００６５】

スマートカードまたはその他の携帯可能な媒体に保存されたデジタル書名は、「知識による識別」の特殊なケースにすぎない。従って、これらは、ＰＩＮまたは生物測定によりさらに保護されることが多い。

【００６６】

図２は、デジタル署名を利用した従来の取引である。この取引は以下の各ステップを含む。認証局が証明書を発行し、正当な所有者を各デジタル署名に割り当てたディレクトリを保管する。署名者が契約書に署名する。受取人が署名者の公開鍵に基づいてその署名を確認する。受取人は、認証局が保管するディレクトリを調べる。

【００６７】

この形態の取引はいくつかの欠点を有する。受取人は署名者の公開鍵を知っていることに依存している。究極的には、当該支払いと秘密署名鍵との関連付けだけがある。つまり、当該鍵の正当な所有者が実際にその契約に署名した人なのかどうかが第一に不明である。そして顧客と受取人はフォーマットについて合意しなければならない。

【００６８】

顧客が本人性を確認した後でなければ契約に署名できない方法もある。この方法は次に、図１と３に示す通り行われる。図１では、一時的にのみ存在するデータが点線で囲まれており、それより長い時間存在するデータは実線で囲まれている。図３は、デジタル署名と認証を伴う従来の取引である。認証は、生物測定学的特徴を測定することによって実行できる。受取人は、署名者の公開鍵とその特徴のサンプルを知っていることに依存している。測定された生物測定学的特徴のデジタル表現がデータネットワーク上を転送されることに注意する必要がある。次に、商店主側は、保存サンプル（テンプレート）により、測定された生物測定学的特徴を比較する。この関連で、ＭＭＡ、ＲＡ、ＳＴＴ、ＳＴＸなどの攻撃が発生する可能性がある。

【００６９】

図５は、本用途に基づく署名方法の概略フローチャートである。初期設定および認証段階の２つの独立した方法が一緒に示されている。これは、以下の各ステップを含む。第一に、初期設定段階では利用者の生物測定学的特徴が測定されデジタル化される。これは、その特徴のプロトタイプＰと呼ばれる。この生物測定学的特徴は数回測定される場合がある。この場合、プロトタイプＰは複数の測定値から決定され、装置の初期化のための利用される。プロトタイプＰは次に公開および秘密部分に分解されるのが理想である。完全な生物測定学的特徴、特徴の各秘密部分、あるいはそのプロトタイプが保存されていることは決してない。第二に、第二の初期設定ステップでは、プロトタイプＰから訂正データが計算されて、測定された生物測定学的特徴が自由に選択可能な許容差以内である場合にそれらの再構築を可能にする。第三に、第三の初期設定ステップでは、暗号方法の実行に必要なデータが計算される。第四に、第四の初期設定ステップでは、暗号方法の秘密データが

プロトタイプＰまたはＰの部分と適切な形でリンクされる。第五に、認証段階において、利用者の生物測定学的特徴が再度測定されデジタル化される。好適な実施態様では、生物測定学的特徴が利用者の署名であり、その署名の動的な特徴も捕捉される。利用者は自分の署名を当該装置の表示部に書くことができる。その利用者が「外部」装置に自分の生物測定学的特徴を残すよう要求されないことに注意する必要がある。これは、生物測定学的特徴の盗用を妨げる。第六に、この生物測定学的特徴は、任意の判断で、「分類部分」と「検証部分」に分解してもよい。「分類部分」は、公にアクセス可能な情報のみを含む。この「分類部分」の情報に基づいた生物測定学的特徴と利用者との予備的な関連付けが失敗すると、その利用者は拒絶される。「検証部分」は、公にアクセス不能な情報のみを含む。好適な実施態様では、これは、その署名の動的特徴である場合がある。第七に、「検証部分」または秘密鍵の正当な所有者だけがアクセスできるその他の情報から、プロトタイプＰまたはそれから計算した値が再構築され、一意の形でその利用者に関連付けられる。異なる利用者に対するこの関連付けルールの無衝突性が必要とされる。第八に、この値―また他のファイル―から、固定長の値が、逆関数の計算が困難な無衝突関数によって生成される。このような関数の例は、メッセージダイジェスト５（ＭＤ５）である。この値は、秘密署名鍵を決定するための開始値となる。あるいは、秘密署名鍵は値Ｐから直接決定される。第九に、その装置は請求書または請求書の一部に署名する。署名鍵は次に即時削除される。

【００７０】

以下に、認証段階での値Ｐの再構築についてさらに正確に記述する。値Ｐ上へのマッピングには、次の特性を有するアルゴリズムが利用される。ａ）これは、デジタル化した生物測定学的特徴などの正当な入力値を確実に値Ｗ上にマッピングする。この場合、これはプロトタイプＰである。ｂ）これは、不当な入力値を値Ｗ上にマッピングしない。ｃ）これは正当な値の許容変動についてスケーラブルである。ｄ）マッピング機能は、正当な入力値のある区間の外では不連続である。つまり、これは傾斜法が適用できないことを意味する。ｅ）これは正当な入力値の特性に関する結論を許す。

【００７１】

特性ａ）、ｂ）、およびｃ）は、この方法の信頼性を説明している。特性ｄ）とｃ）は、値Ｗの計算方法の分析は、攻撃者にいかなる利点も提供しないことを説明している。つまり、これはシステムへの攻撃の労力は、ブルートフォース攻撃の労力と等しいことを意味する。ただし、これは、入力値―生物測定データの部分など―が公開でない場合に成り立つ。

【００７２】

上記の各要件は、共通のエラー訂正方法の復号段階によって満たされる。上記の方法の適用は、マッピング対象の値Ｗが開始値で重複して符号化されることを前提とする。

【００７３】

図７は、誤った生物測定学的特徴の訂正への符号理論の符号化・復号段階の転送を示す。上側の線は、初期設定段階を示す。下側の線は認証段階を示す。初期設定段階で、秘密データ（公開鍵法における秘密鍵など）が、生成行列（または生成多項式）によって正規のコードワード上に最初にマッピングされる。デジタル化された生物測定学的特徴（初期設定ＢＭ）は、ビット単位ＸＯＲ演算によってこのコードワードを暗号化する。

【００７４】

認証段階（下側の線）では、この暗号化されたコードワードが、後に測定される生物測定学的特徴によって暗号解除される（認証ＢＭ）。この生物測定学的認証特徴は初期設定段階で測定された生物測定学的特徴と正確に一致しないことから、誤ったコードワードが発生する。これは、符号理論法の復号段階によって再構築できる。

【００７５】

以下には、原則として上記の本用途に基づく署名方法が好適な例に関して詳細に記述される。

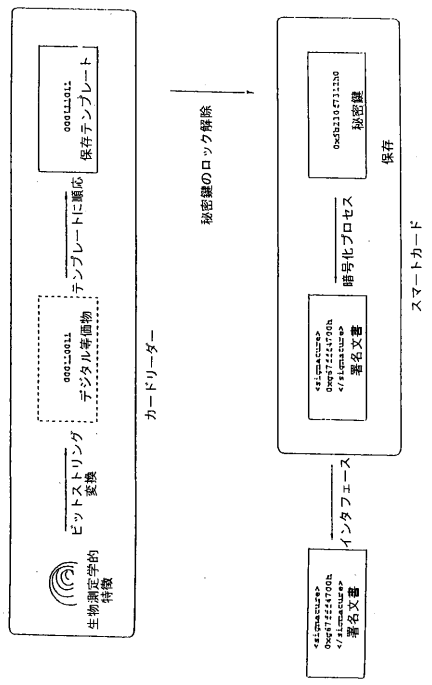
【００７６】

１．　初期設定段階
（ａ）初期設定段階では、正当な利用者が装置の表示部に複数回署名する。
【００７７】
（ｂ）その署名がデジタル化される。静的および動的情報が検出される。
【００７８】
（ｃ）その署名のサンプルまたはプロトタイプＰが計算される。
【００７９】
（ｄ）デジタル化した各署名間の差異が割り出される。
【００８０】
（ｅ）その署名の静的情報が分類目的で保存される。
【００８１】
（ｆ）その署名の動的情報が総人口の署名に関する静的および心理的情報と比較される。各署名の統計的特性に関する知識で取得することができず、またその署名者に特徴的である動的情報が「秘密」として分類される。
【００８２】
（ｇ）この特徴のバイナリ表現が、図４に示すように、エッジ長ｎの升目の中に配置される。値ｎは、この方法を検討する上で何の役割も果たさない。ｎが大きければ大きいほど、この方法によって訂正される誤り率は低くなる。値ｎは、その方法が所望のエラー数を訂正できるように選択される。これは、利用者の測定済み生物測定学的特徴の中で予期される誤り率を是正するために、おそらくステップ１（ｄ）で測定される差異、統計的、心理的、あるいはその他の知識に基づいて選択される。部分的特徴が違えば誤り率も違うと想定できる。この特徴の長さは秘密ではない。最後の升目が完全に埋められない場合、長方形が使用できる。欠落しているビットはゼロで埋められる。
【００８３】
（ｈ）パリティは各行および各列から示される。つまり、２ｎ－１の独立値である。
【００８４】
（ｉ）パリティは本用途に基づいた装置などに保存される。これらは原則として同様に保護できるが、これらは次の中では公開情報とみなされる。これにより、升目当たりの秘密ビット数は（ｎ－１）２となる。
【００８５】
（ｊ）最後の升目では、複数の列のパリティが一定の列長さに属するように組み合わされる。
【００８６】
（ｋ）すべての署名が削除される。
【００８７】
（ｌ）適切な公開鍵方法では、キーペアが生成される。
【００８８】
（ｍ）秘密鍵は、秘密鍵のビット単位ＸＯＲを生物測定学的特徴（またはそのハッシュ値）とともに保存して秘密鍵を削除することなどにより、特徴のバイナリ表現を使って保護される。
【００８９】
（ｎ）一般にアクセス可能とみなされる全人口に関する統計データを使用して、推測することもできずまたエラー訂正用に利用されることもないことから秘密とみなされる、生物測定学的特徴のビット数を表わす数値Ｎが決定される。このエラー訂正情報により、１回の攻撃の中で推測されるビット数は、攻撃者が訂正方法を知っていることから、升目当たり２ｎ－１減らすことができる。その結果得られる数値がこの方法のセキュリティの尺度である。
【００９０】
（ｏ）この署名のプロトタイプのすべての秘密部分が削除される。
【００９１】

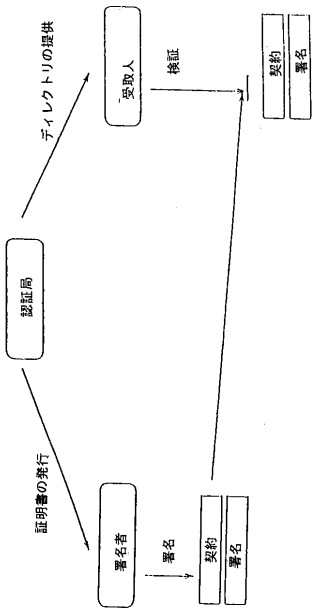
（ｐ）公開鍵と秘密鍵を含むキーペアが生成される。
【００９２】
（ｑ）値Ｐと秘密署名鍵が削除される。
【００９３】
２．　認証段階
（ａ）認証段階で、正当な利用者が装置の表示部に署名する。
【００９４】
（ｂ）その署名が適切な入力装置でデジタル化される。静的および動的情報が検出される。これは、初期設定段階と特に同じ装置であっても構わない。
【００９５】
（ｃ）デジタル化された署名のハッシュ値が計算される。これは、次の認証段階で新規署名のハッシュ値と比較できる。直前に書かれた書名と正確に一致するデジタル化した署名は拒絶される。これはリプレイ攻撃を妨げる。
【００９６】
（ｄ）複数の利用者について装置が初期化された場合、署名の公開情報が分類目的に使用される。
【００９７】
（ｅ）生物測定学的特徴のバイナリ表現が初期設定段階の各升目の中に入力される。
【００９８】
（ｆ）各行および各列のパリティが計算される。
【００９９】
（ｇ）１ビットエラーはすべて保存パリティとの比較によって局在化され訂正される（図４を参照）。
【０１００】
（ｈ）１つの升目に複数のエラーがあると訂正は失敗する。これは、特に不十分な偽造が入力された場合である。
【０１０１】
（ｉ）訂正された特徴は公開鍵方法の秘密鍵を復元するために利用される。１（ｍ）からの例示方法では、この特徴のビット単位ＸＯＲ（またはハッシュ値）が１（ｍ）の結果によって計算される。この値が秘密鍵である。
【０１０２】
（ｊ）署名する文書は新たに生成された秘密鍵によって署名される。
【０１０３】
（ｋ）秘密署名鍵が削除される。
【０１０４】
（ｌ）署名文書が転送される。
【０１０５】
（ｍ）エラー訂正機能は、デジタル化された生物測定学的特徴が訂正間隔の境界からどれくらい離れているかに関する結論を許可しない。従って、傾斜法は適切な攻撃可能性ではない。
【図面の簡単な説明】
【図１】　デジタル署名による認証方法を使用した従来型スマートカードシステムの取引過程である
【図２】　デジタル署名を使用した従来の取引の過程である
【図３】　デジタル署名と他の認証ステップを使用した従来の取引の過程である
【図４】　本用途に基づく初期設定および認証段階の訂正データの比較の概略図
【図５】　本用途に基づく初期設定および認証段階のフローチャートである
【図６】　攻撃の可能性と、さらに生物測定を利用したデジタル署名方法への対策をまとめた表である
【図７】　誤った生物測定学的特徴の訂正への符号理論方式の符号化・復号段階の転送で

ある

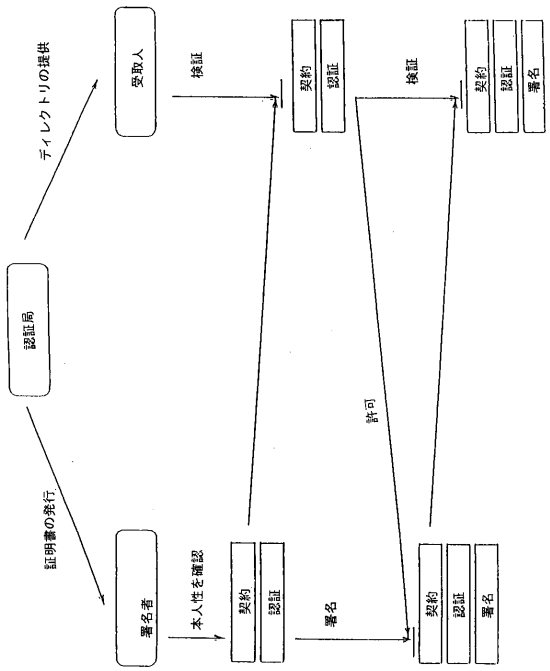
【図１】


カードリーダー
生物測定学的特徴
ビットストリング変換
デジタル等価物
テンプレートに順応
保存テンプレート
秘密鍵のロック解除
インタフェース
署名文書
暗号化プロセス
秘密鍵
保存
スマートカード

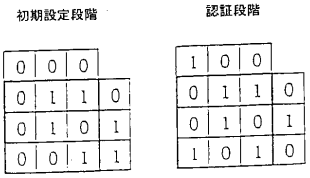
【図２】


認証局
ディレクトリの提供
受取人
検証
契約
署名
証明書の発行
署名者
署名
契約
署名

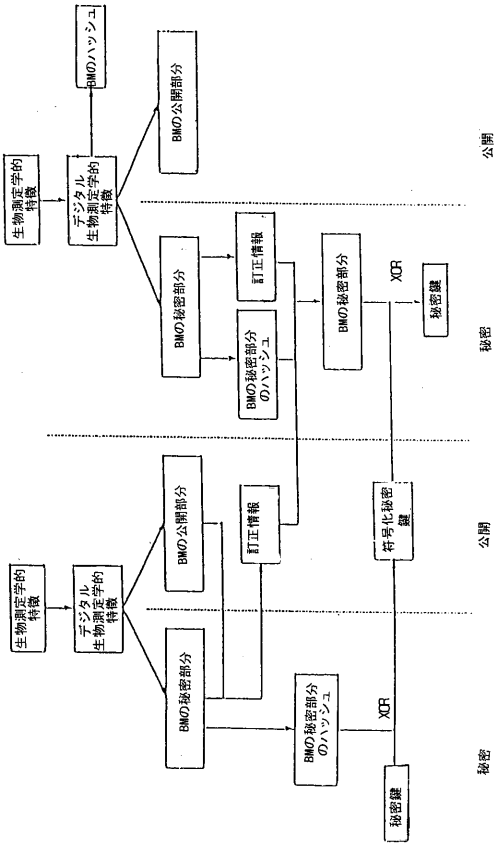
【図３】



【図４】



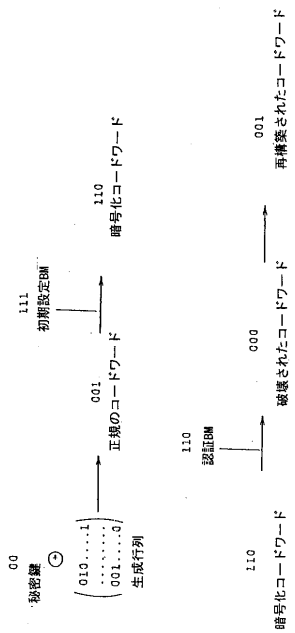
【図５】



【図６】

攻撃の可能性	対策
暗号解読攻撃（ＫＡ）	非対称暗号化技術
ブルートフォース攻撃（ＢＦＡ）	適切な鍵長の選択
タンパー攻撃（ＴＡ）	タンパー防止または耐タンパー性のあるハードウェア
破損トラストモデル（ＴＭＡ）	透明なトラストモデルの選択
破損利用者（ＵＡ）	透明性
マン・イン・ザ・ミドル攻撃（ＭＭＡ）	ネットワーク上でのセキュリティクリティカルなデータの転送を行わない
リプレイ攻撃、フェイクターミナル攻撃（ＲＡ）	ネットワーク上でのセキュリティクリティカルなデータの転送を行わない （パスワード、ＰＩＮ、またはバイオメトリによる）鍵の保護
秘密署名鍵の盗用（ＰＫＴ）	
保存されている生物測定学的特徴のプロトタイプの盗用（ＳＴＩ）	プロトタイプを保存しない
保存されている生物測定学的特徴のプロトタイプの交換（ＳＴＸ）	プロトタイプの保護、プロトタイプを保存しない
保存されているＰＩＮへの暗号解読攻撃（ＫＡＰ）	適切な暗号化方法の選択

【図７】


00
秘密鍵
生成行列
001
正規のコードワード
110
暗号化コードワード
111
初期設定BM
110
暗号化コードワード
110
認証BM
000
破壊されたコードワード
001
再構築されたコードワード

フロントページの続き

(72)発明者 フォーゲル，コルヤ
ドイツ連邦共和国 Ｄ－３３６０４ ビーレフェルト アンドレーアスーラマイーシュトラーセ １５
(72)発明者 バインリッヒ，シュテファン
ドイツ連邦共和国 Ｄ－８０６３９ ミュンヘン ニーベルンゲンーシュトラーセ １２
(72)発明者 マルティーニ，ウルリッヒ
ドイツ連邦共和国 Ｄ－８１５４１ ミュンヘン ツェッペリーンシュトラーセ １２

審査官 松平 英

(56)参考文献 特開平０１－１６１９３８（ＪＰ，Ａ）
特開平０３－０７３６３３（ＪＰ，Ａ）
特開平１１－０７３１０３（ＪＰ，Ａ）
特開平１１－１４９４５３（ＪＰ，Ａ）
特開平１１－１８７００７（ＪＰ，Ａ）
特開平１１－２６１５５０（ＪＰ，Ａ）
特開平１１－３１６８１８（ＪＰ，Ａ）
特開２００１－００７８０２（ＪＰ，Ａ）
特表平１０－５０３６０９（ＪＰ，Ａ）
特表２００１－５１２６５４（ＪＰ，Ａ）
特表２００１－５２３９１９（ＪＰ，Ａ）
特表２００１－５２５９６０（ＪＰ，Ａ）
特表２００２－５３８５０４（ＪＰ，Ａ）
特表２００２－５３８５３０（ＪＰ，Ａ）
特開平０３－１０４３３８（ＪＰ，Ａ）
特開平０９－１４７０７２（ＪＰ，Ａ）
特開平０２－０２８７７５（ＪＰ，Ａ）
特開平１０－２６２９５１（ＪＰ，Ａ）
国際公開第９９／０３３２１９（WO，Ａ１）
George I. Davida et al, On Enabling Secure Applications Through Off-line Biometric Identification, Proceedings of the IEEE Symposium on Security and Privacy, １９９８年 ５月, p. 148-157
中川 純一，ＰＧＰと電子メールのセキュリティ，目からウロコのＯｕｔｌｏｏｋ Ｅｘｐｒｅｓｓ，日本，エーアイ出版株式会社 AI Publishing，１９９９年 2月２７日，初版，ｐ．８５～１００

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L 9/00
G09C 1/00
G06F 21/20
G06F 21/24