(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4659149号
(P4659149)
(45)発行日　平成23年3月30日(2011.3.30)　(24)登録日　平成23年1月7日(2011.1.7)

(51)Int.Cl.　F I
H04L 9/32 (2006.01)　H04L 9/00 675B

請求項の数 33　(全 22 頁)

(21)出願番号　特願2004-17044(P2004-17044)
(22)出願日　平成16年1月26日(2004.1.26)
(65)公開番号　特開2004-229308(P2004-229308A)
(43)公開日　平成16年8月12日(2004.8.12)
審査請求日　平成18年12月27日(2006.12.27)
(31)優先権主張番号　0301108
(32)優先日　平成15年1月24日(2003.1.24)
(33)優先権主張国　フランス(FR)

(73)特許権者　591034154
フランス・テレコム
フランス、７５５０５　パリ、セデックス・１５、プラス・ダルレ、６
(74)代理人　100080447
弁理士　太田　恵一
(72)発明者　マルク　ジロル
フランス共和国，１４０００　カーン，リュ　ヴィヴィアンヌ　４

審査官　石田　信行

最終頁に続く

(54)【発明の名称】電子チップの不正行為に対する保護の非対称暗号通信法

(57)【特許請求の範囲】
【請求項１】
アプリケーションと電子チップの間のトランザクションにおいて、入力パラメータから認証値Ｖを電子チップ内で計算することからなる、ワイヤードロジックチップのための、電子チップの不正行為に対する保護の非対称暗号通信法であり、前記方法が、
・チップ内に含まれるシリアル擬似乱数生成器を用いて、トランザクションに固有の確率変数ｒと呼ばれる擬似乱数をチップによって発生させることと、
・数学的関係式によって確率変数ｒに結びつけられ、また、チップのデータメモリ内に保存された、トランザクションに先立ってチップの擬似乱数生成器と同一のものであるアプリケーションの擬似乱数生成器を用いてアプリケーションによって計算されるパラメータｘを、チップからアプリケーションに伝達することと、
・入力パラメータとして、トランザクションに固有の確率変数ｒと、一対の非対称キー（ｓ、ｐ）に属するプライベートキーｓとを有するシリアル関数を用いて、認証値Ｖの全体または一部を構成するパラメータｙを、チップによって計算することと、
・チップ内に備えられた出力手段によってｙから得られた認証値Ｖを、チップからアプリケーションに伝達することと、
・入力パラメータが、少なくとも公開キーｐを含む公開パラメータのみによって構成される確認関数を用いて、前記認証値Ｖをアプリケーションによって確認することとからなる段階を含むことを特徴とする方法。
【請求項２】

トランザクションに固有の確率変数ｒの発生が、
・混合関数を用いて混合関数の入力パラメータの全てまたは一部を混合し、一連のビットを混合関数の出力に提供することと、
・旧状態と一連のビットの一つの値に依存する関数によって、旧状態から新状態に移行させることで有限状態オートマトンの状態変化を実行することと、
・オートマトンの一つの状態を入力引数として有する出力関数を用いて、確率変数ｒの全体または一部を形成するために、一連の乱数ビットを決定することとからなることを特徴とする、請求項１に記載の方法。

【請求項３】
混合関数の入力パラメータの一つが秘密キーＫで構成され、該秘密キーが、チップとアプリケーションの間で共有され、チップの保護された記憶領域内に保存されることを特徴とする、請求項２に記載の方法。

【請求項４】
数学的関係式が、特性として結合的である演算を備えている要素ｇの集合Ｇ内の関数g^rで構成されることを特徴とする、請求項１または請求項２に記載の方法。

【請求項５】
集合Ｇが、ｎが任意の正の整数であるとき、ｎより小さく、ｎに対して素である正またはゼロである整数の群Z_n^*であることを特徴とする、請求項４に記載の方法。

【請求項６】
集合Ｇが、任意の有限体に作られた楕円曲線であることを特徴とする、請求項４に記載の方法。

【請求項７】
シリアル関数が、演算のリストから取られた演算を実行する算術関数であり、該リストが、リストの項目として、加算、減算および左または右へのシフトを含んでいることを特徴とする、請求項１または請求項２に記載の方法。

【請求項８】
算術関数が、加算のみを実行することを特徴とする、請求項７に記載の方法。

【請求項９】
算術関数が、減算のみを実行することを特徴とする、請求項７に記載の方法。

【請求項１０】
算術関数が、さらに入力引数として入力パラメータを有し、アプリケーションによってシリアル関数の入力パラメータｔに割り当てられた値に応じて、次の演算：ｙ＝ｒおよびｙ＝ｒ＋ｓの一つを実行することからなることを特徴とする、請求項７に記載の方法。

【請求項１１】
数学的関係式が、特性として結合的である演算を備えている要素ｇの集合Ｇ内の関数g^rで構成され、確認関数が、該関数を認証値Ｖに適用して得られた結果すなわちg^Vを、パラメータｔの値に応じて、次の値：値ｘ、値ｘとその秘密キーｓに対応するチップの公開キーｐとの積（ｘｐ）、の一つと比較し、このことが、パラメータｔの値に応じて、ｙが認証値Ｖに等しく、ｐが関数$p=g^s$によって定義され、秘密キーｓに対応するチップの公開キーである、次の方程式：$g^y=x$と$g^y=xp$、の一方をテストすることに等しくなることを特徴とする、請求項１０に記載の方法。

【請求項１２】
算術関数が、さらに入力引数として入力パラメータを有し、アプリケーションによってシリアル関数の入力パラメータｔに割り当てられた値に応じて、次の演算：ｙ＝ｒおよびｙ＝ｒ－ｓ、の一つを実行することからなることを特徴とする、請求項７に記載の方法。

【請求項１３】
数学的方程式が、特性として結合的である演算を備えている要素ｇの集合Ｇ内の関数g^rで構成され、確認関数が、パラメータｔの値に応じて、該関数を認証値Ｖに適用して得られた結果すなわちg^V、または該結果g^Vと秘密キーｓに対応するチップの公開キーｐとの積$g^V.p$を、値ｘと比較し、このことが、パラメータｔの値に応じて、ｙが認証値Ｖ

に等しく、ｐが方程式ｐ＝ｇ^{s}によって定義され、秘密キーｓに対応するチップの公開キーである、次の方程式：ｇ^{y}＝ｘとｇ^{y}．ｐ＝ｘ、の一方をテストすることに等しくなることを特徴とする、請求項１２に記載の方法。

【請求項１４】

算術関数が、さらに入力引数として入力パラメータを有し、アプリケーションによってシリアル関数の入力パラメータｔに割り当てられた値に応じて、次の演算：ｙ＝ｒ＋２^{i}ｓを実行することからなり、このパラメータｔが、ｍビット（ｔ$_{m-1}$、・・・、ｔ$_{0}$）のチェーンで構成され、そのビットの一つだけ、ビットｔ$_{i}$が１に等しく、ｍが自然数であることを特徴とする、請求項７に記載の方法。

【請求項１５】

数学的関係式が、特性として結合的である演算を備えている要素ｇの集合Ｇ内の関数ｇ^{r}で構成され、確認関数が、パラメータｔの値に応じて、ｙが認証値Ｖに等しく、ｐが関数ｐ＝ｇ^{s}によって定義され、秘密キーｓに対応するチップの公開キーである、方程式ｇ^{y}＝ｘｐ＾（２＾ｉ）をテストすることからなることを特徴とする、請求項１４に記載の方法。

【請求項１６】

算術関数が、さらに入力引数として入力パラメータを有し、アプリケーションによってシリアル関数の入力パラメータｔに割り当てられた値に応じて、次の演算：ｙ＝ｒ＋２^{t}ｓを実行することからなることを特徴とする、請求項７に記載の方法。

【請求項１７】

数学的関係式が、特性として結合的である演算を備えている要素ｇの集合Ｇ内の関数ｇ^{r}で構成され、確認関数が、ｙが認証値Ｖに等しく、ｐが関数ｐ＝ｇ^{s}によって定義され、秘密キーｓに対応するチップの公開キーである、次の方程式ｇ^{y}＝ｘｐ＾（２＾ｔ）をテストすることからなることを特徴とする、請求項１６に記載の方法。

【請求項１８】

算術関数が、さらに入力引数として入力パラメータを有し、アプリケーションによってシリアル関数の入力パラメータｔに割り当てられた値に応じて、ｔが整数である次の演算：ｙ＝ｒ＋ｔｓを実行することからなることを特徴とする、請求項７に記載の方法。

【請求項１９】

数学的関係式が、特性として結合的である演算を備えている要素ｇの集合Ｇ内の関数ｇ^{r}で構成され、確認関数が、該関数を認証値Ｖに適用して得られた結果すなわちｇ^{V}を、値ｘと秘密キーｓに対応するチップの公開キーｐのｔ乗との積（ｘｐ^{t}）と比較し、このことが、パラメータｔの値に応じて、ｙが認証値Ｖに等しく、ｐが関数ｐ＝ｇ^{s}によって定義され、秘密キーｓに対応するチップの公開キーである、次の方程式：ｇ^{y}＝ｘｐ^{t}をテストすることに等しくなることを特徴とする、請求項１８に記載の方法。

【請求項２０】

チップからアプリケーションに伝達されたパラメータｘが、数学的関数によって確率変数ｒに接続された一つの要素と、アプリケーションに結びつけられたデータを含むオプションフィールドＤとに適用されたハッシュ関数の結果であることを特徴とする、請求項１または請求項２に記載の方法。

【請求項２１】

シリアル関数は、演算のリストから取られた演算を実行する算術関数であり、

該リストは、リストの項目として、加算、減算および左または右へのシフトを含んでおり、

算術関数が、さらに入力引数として入力パラメータを有し、アプリケーションによってシリアル関数の入力パラメータｔに割り当てられた値に応じて、次の演算：ｙ＝ｒ＋２^{i}ｓを実行することからなり、このパラメータｔが、ｍビット（ｔ$_{m-1}$、・・・、ｔ$_{0}$）のチェーンで構成され、そのビットの一つだけ、ビットｔ$_{i}$が１に等しく、ｍが自然数であることを特徴とする、請求項２０に記載の方法。

【請求項２２】

数学的関係式が、特性として結合的である演算を備えている要素ｇの集合Ｇ内の関数ｇ^{r}で構成され、確認関数が、パラメータｔの値に応じて、ｙが認証値Ｖに等しく、ｐが関数ｐ＝ｇ^{s}によって定義され、秘密キーｓに対応するチップの公開キーである、次の方程式：ｈ（ｇ^{y}／ｐ＾（２＾ｉ），Ｄ）＝ｘをテストすることからなることを特徴とする、請求項２１に記載の方法。

【請求項２３】

数学的関係式が、特性として結合的である演算を備えている要素ｇの集合Ｇ内の関数ｇ^{r}であり、確認関数が、ｙが認証値Ｖに等しく、ｐが関数ｐ＝ｇ$^{-s}$によって定義され、秘密キーｓに対応するチップの公開キーである、次の方程式：ｈ（ｇ^{y}・ｐ＾（２＾ｉ），Ｄ）＝ｘをテストすることからなることを特徴とする、請求項２１に記載の方法。

【請求項２４】

シリアル関数は、演算のリストから取られた演算を実行する算術関数であり、

該リストは、リストの項目として、加算、減算および左または右へのシフトを含んでおり、

算術関数が、さらに入力引数として入力パラメータを有し、アプリケーションによってシリアル関数の入力パラメータｔに割り当てられた値に応じて、次の演算：ｙ＝ｒ－２^{i}ｓを実行することからなり、このパラメータｔが、ｍビット（t_{m-1}、・・・、t_{0}）のチェーンで構成され、そのビットの一つだけ、ビットt_{i}が１に等しく、ｍが自然数であることを特徴とする、請求項２０に記載の方法。

【請求項２５】

数学的関係式が、特性として結合的である演算を備えている要素ｇの集合Ｇ内の関数ｇ^{r}で構成され、確認関数が、ｙが認証値Ｖに等しく、ｐが関数ｐ＝ｇ^{s}によって定義され、秘密キーｓに対応するチップの公開キーである、次の方程式：ｈ（ｇ^{y}・ｐ＾（２＾ｉ），Ｄ）＝ｘをテストすることからなることを特徴とする、請求項２４に記載の方法。

【請求項２６】

数学的関数が、特性として結合的である演算を備えている要素ｇの集合Ｇ内の関数ｇ^{r}で構成され、チップからアプリケーションに伝達されたパラメータｘが、Ｄがアプリケーションに結びつけられたデータを含むオプションフィールドを示し、ｈがハッシュ関数である、ｘ＝ｈ（ｇ^{r}、Ｄ）型の関係式の結果であることを特徴とする、請求項２０に記載の方法。

【請求項２７】

シリアル関数が、入力引数として入力パラメータを有し、アプリケーションによってシリアル関数の入力パラメータｔに割り当てられた値に応じて、次の演算：ｙ＝ｒとｙ＝ｒ＋ｓ、の一つを実行することからなり、確認関数が、パラメータｔの値に応じて、ｙが認証値Ｖに等しく、ｐが方程式ｐ＝ｇ^{s}によって定義され、秘密キーｓに対応するチップの公開キーである、次の方程式：ｈ（ｇ^{y}、Ｄ）＝ｘとｈ（ｇ^{y}／ｐ、Ｄ）＝ｘ、の一方をテストすることを特徴とする、請求項２６に記載の方法。

【請求項２８】

シリアル関数が、入力引数として入力パラメータを有し、アプリケーションによってシリアル関数の入力パラメータｔに割り当てられた値に応じて、次の演算：ｙ＝ｒとｙ＝ｒ＋ｓ、の一つを実行することからなり、確認関数が、パラメータｔの値に応じて、ｙが認証値Ｖに等しく、ｐが方程式ｐ＝ｇ$^{-s}$によって定義され、秘密キーｓに対応するチップの公開キーである、次の方程式：ｈ（ｇ^{y}、Ｄ）＝ｘとｈ（ｇ^{y}．ｐ、Ｄ）＝ｘ、の一方をテストすることを特徴とする、請求項２６に記載の方法。

【請求項２９】

シリアル関数が、入力引数として入力パラメータを有し、アプリケーションによってシリアル関数の入力パラメータｔに割り当てられた値に応じて、次の演算：ｙ＝ｒとｙ＝ｒ－ｓ、の一つを実行することからなり、確認関数が、パラメータｔの値に応じて、ｙが認証値Ｖに等しく、ｐが方程式ｐ＝ｇ^{s}によって定義され、秘密キーｓに対応するチップの公開キーである、次の方程式：ｈ（ｇ^{y}、Ｄ）＝ｘとｈ（ｇ^{y}．ｐ、Ｄ）＝ｘ、の一方をテ

ストすることを特徴とする、請求項２６に記載の方法。
【請求項３０】
集合Ｇは、ｎが任意の正の整数であるとき、ｎより小さく、ｎに対して素である正またはゼロの整数の群Z_n^*であることを特徴とする、請求項７から請求項２９のいずれか一つに記載の方法。
【請求項３１】
集合Ｇは、任意の有限体に作られた楕円曲線であることを特徴とする、請求項７から請求項２９のいずれか一つに記載の方法。
【請求項３２】
アプリケーションと電子チップの間のトランザクションにおいて、入力パラメータから認証値Ｖを電子チップによって計算することからなる、請求項１から請求項３１のいずれか一つに記載の電子チップの不正行為に対する保護の非対称暗号通信法を使用することを可能にする、電子チップ付装置であり、前記装置が、
・トランザクションに固有の確率変数ｒを発生させるシリアル擬似乱数生成器と、
・一つのｘの値が保存された第１の記憶手段であって、ここで、パラメータｘの値は、トランザクションに先立ってチップ内に含まれる擬似乱数生成器と同一のものであるアプリケーションの擬似乱数生成器を用いてアプリケーションによって計算され、数学的関係式によって確率変数ｒの値に結びつけられているものである、第１の記憶手段と、
・トランザクションに固有の確率変数ｒに結びつけられたパラメータｘを、電子チップからアプリケーションに伝達する手段と、
・入力パラメータとして、トランザクションに固有の確率変数ｒと、一対の非対称キー（ｓ、ｐ）に属するプライベートキーｓとを有し、パラメータｙを出力に提供するシリアル関数の実行手段と、
・パラメータｙから認証値Ｖを構成するための出力手段とを備えていることを特徴とする電子チップ付装置。
【請求項３３】
アプリケーションと電子チップの間のトランザクションにおいて、もっぱら公開であるパラメータから、電子チップによって計算された認証値Ｖを確認することからなる、請求項１から請求項３１のいずれか一つに記載の電子チップの不正行為に対する保護の非対称暗号通信法を実行するための確認装置であり、
前記装置が、認証値Ｖと公開キーｐを入力に取る確認関数の実行手段を備えていることを特徴とする確認装置。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は暗号通信法の分野に関するものである。
特に、本発明はアプリケーションとチップの間のトランザクションにおける、電子チップの不正行為に対する保護の非対称暗号通信法に関するものである。
【０００２】
本発明は、ワイヤードロジック集積回路式あるいはマイクロプロセッサ式のチップ、特に電話通信の成立、自動販売機における物品の支払い、パーキングメーターによる駐車場の賃貸、公共交通機関のような、あるいはインフラストラクチャ（通行料、美術館、図書館）の利用のようなサービスの支払いなど、さまざまな取引において用いられるプリペイドカードに備えられたチップの不正行為に対する保護を可能にする点で、きわめて有利な応用が見いだされる。
【背景技術】
【０００３】
現在、プリペイドカードは各種の不正行為を受けやすい。
第１のタイプの不正行為はカードを無許可で複製することからなり、この操作を特徴づ

けるためにクローニングという用語がよく用いられる。
第２のタイプの不正行為は、カードに与えられたデータ、特にカードに書き込まれたクレジットの金額を変更することからなる。
これらの不正行為と闘うために暗号通信法が使われており、これは一方では、認証手段を用いてカード認証を保証し、および／またはデジタル認証手段によるデータ認証を保証するためであり、また他方では、必要ならば暗号化手段によってデータの機密性を保持するためである。
暗号通信法は、認証の場合の認証者と認証対象という二つの実体に作用するものであって、該通信法は対称または非対称とすることができる。
通信法が対称（あるいは「秘密キー式」、二つの用語は同義）の場合、二つの実体は正確に同一の情報、特に秘密キーを共有する。
通信法が非対称（あるいは「公開キー式」、二つの用語は同義語である）の場合、２つの実体の一方が一対のキーを有し、該キーの一つが秘密で、他方が公開であり、したがって共有される秘密キーはない。
多くのシステムにおいて、特にチップが「ワイヤードロジック」タイプの場合、非対称暗号通信法は低速で高価であるため、対称暗号通信法だけがプリペイドカードに用いられる。
対称暗号通信法において開発された最初のいくつかの認証メカニズムは、それぞれのカードについて異なる認証値を一度だけ計算し、該認証値をカードの記憶装置の中に保存し、トランザクションごとにそれを読み取り、割り当て済みの認証値が保存されるか再計算されるトランザクションを支えているネットワークのアプリケーションに質問して、認証値を確認するものである。
これらのメカニズムの保護は不十分である。
なぜなら、認証値はあるカードについて常に同一なので、不正に盗み取り、複製し、再利用できるので、このカードのクローンを製作できるからである。
クローン撲滅のために、カードの受動認証メカニズムは、さらにデータの完全性を保証することができる能動認証メカニズムに取って代わられた。
【０００４】
対称能動認証メカニズムの一般原理は次の通りである。
認証の際、電子チップとアプリケーションが、認証ごとに所定の引数リストに適用された関数の結果である認証値を計算する。
引数リストは、乱数を含むことができ、乱数は、認証ごとにアプリケーションによって決定されるデータ、電子チップに含まれるデータ、電子チップとアプリケーションによって認識されている秘密キーである。
電子チップによって計算された認証値が、アプリケーションによって計算された認証値と同値であるとき、電子チップは真正と判定され、電子チップとアプリケーションの間のトランザクションが許可される。
【０００５】
このようなメカニズムは広く知られているが、その大半は少なくとも、マイクロプロセッサが利用する容量に等しい計算容量を必要とする。
したがって、これらのメカニズムはマイクロプロセッサを用いるカードには適しているが、はるかに基本的な計算手段を備えているワイヤードロジックチップにはあまり適していない。
【０００６】
対称認証能動メカニズムをワイヤードロジックチップに組み込むことができたとき、最初の一歩が踏み出された。
例えば、仏国特許出願公開第２８２６５３１号の番号で２００２年１２月２７日に公開されたフランス特許出願は、このようなメカニズムを特定できる方法を記載している。
なお、これらのメカニズムによって発生させられた認証値も、上述のフランス特許出願

の教示のように、擬似乱数的ビット列と解釈され、入力パラメータの少なくとも一つを変動させることで、認証値の計算方法は、このとき、擬似乱数的ビットの生成法になる。
【特許文献１】仏国特許出願公開第２８２６５３１号明細書
【発明の開示】
【発明が解決しようとする課題】
【０００７】
しかしながら、秘密キー式メカニズムは、公衆電話、電子支払い端末、あるいはさらに公共交通機関の改札などの中にあるもののような、チップの認証を担当する確認装置が、前記チップに保有されている秘密キーを認識することを要求する。
その結果、大きな不便が生じる。
すなわち、前記装置がアプリケーションとの関係において発行されたどのようなチップでも認証しようとすると、全てのチップの秘密キーを保存しなければならない、あるいはどのようなチップの秘密キーをも再び見つけることを可能にする、マザーキーまたはマスターキーとも呼ばれる、ベースキーを保存しなければならないということである。
いずれの場合にも、これらの装置のそれぞれは、発行された全てのチップの秘密キーを再び見つけるための情報を十分に保存しており、したがって、それらの中のどのチップであってもクローンを製造するに足る情報を保存している。
その結果、確認装置のどれかへの侵入が成功すれば、アプリケーションの安全性がその全体において喪失されることになる。
【０００８】
したがって、ワイヤードロジックチップ内に、特に多数のチップを展開しているアプリケーションの中に、公開キー式認証能動メカニズムを組み込めることが絶対に必要であり、このことは一般的に、チップはきわめて安価なので、ワイヤードロジックチップを使用するアプリケーションには当てはまる。
しかしながら、現時点ではこのようなメカニズムは存在していない。
その理由は、公開キー式メカニズムは一般的に、大きな数を対象とする多数の操作を必要とし、そのためシリコンの表面積がきわめて小さく、計算論理がきわめて基本的な演算配線に還元される、ワイヤードロジックチップ内への組み込みに適していないということである。
これらの基本的演算は一般的にシリアルで実行されるが、それはオペランドがビットごとに連続的に導入され、この導入が内部レジスタの状態を次第に変化させ、該レジスタの最終値が、関数の結果の計算の基礎に使われるという意味である。
【課題を解決するための手段】
【０００９】
本発明は、ワイヤードロジックカード内で使用することができる、公開キー式認証能動メカニズムに関するものである。
【００１０】
より正確には、本発明はアプリケーションと電子チップの間のトランザクションにおける、電子チップの不正行為に対する保護の非対称暗号通信法に関するものであり、特にワイヤードロジックチップに適し、特に認証メカニズムを設置することを目的とするものであり、該メカニズムは上述の対称暗号通信法の欠陥がないもので、アプリケーションのセキュリティをその全体において強化し、特にクローン作製をより困難にするためのものである。
【００１１】
このために、本発明はアプリケーションと電子チップの間のトランザクションにおいて、入力パラメータから認証値Ｖを電子チップ内で計算することからなる、電子チップの不正行為に対する保護の非対称暗号通信法を目的とする。
本方法は以下のことから構成される過程を含む。
【００１２】
・チップ内に含まれるシリアル擬似乱数生成器を用いて、トランザクションに固有の確率

変数ｒと呼ばれる擬似乱数をチップによって発生させる過程と、
・トランザクションに先立って、アプリケーションによって計算されたパラメータｘをチップからアプリケーションに伝達する過程で、該パラメータが数学的関係式によって確率変数ｒに結びつけられ、チップのデータメモリ内に保存されている過程と、
・シリアル関数を用いて、チップによってパラメータｙを計算する過程で、該関数が入力パラメータとして少なくともトランザクションに固有の確率変数ｒと、一対の非対称キー（ｓ、ｐ）に属するプライベートキーｓとを有しており、パラメータｙが認証値Ｖの全体または一部を構成している過程と、
・認証値Ｖをチップからアプリケーションに伝達する過程と、
・確認関数を用いて、前記認証値Ｖをアプリケーションによって確認する過程で、入力パラメータが少なくとも一つの公開キーｐを含む、公開パラメータのみで構成されている過程。

【００１３】

本発明はさらに、アプリケーションと電子チップの間のトランザクションにおいて、入力パラメータから認証値Ｖを電子チップによって計算することからなる、前述の目的による電子チップの不正行為に対する保護の非対称暗号通信法の使用を可能にする、電子チップ付装置を目的とする。

該装置は、
・トランザクションに固有の確率変数ｒを発生させるシリアル擬似乱数生成器と、
・ｘの少なくとも一つの値が保存された第１の記憶手段で、パラメータｘの値がトランザクションに先立ってアプリケーションによって計算され、数学的関係式によって確率変数ｒに結びつけられたものと、
・トランザクションに固有の確率変数ｒに結びつけられたパラメータｘを、電子チップからアプリケーションに伝達する手段と、
・入力パラメータとして、少なくともトランザクションに固有の確率変数ｒと、一対の非対称キー（ｓ、ｐ）に属するプライベートキーｓとを有し、パラメータｙを出力に提供する、シリアル関数の実行手段と、
・少なくともパラメータｙから認証値Ｖを構成するための出力手段とを備えている。

【００１４】

本発明はさらに、アプリケーションと電子チップの間のトランザクションにおいて、電子チップの不正行為に対する保護の非対称暗号通信法を実行するための確認装置を目的とし、該装置は、もっぱら公開であるパラメータから、電子チップによって計算された認証値Ｖを確認することからなる、本発明の目的にそっている。

該装置は確認関数の実行手段を備えており、該関数は少なくとも一つの認証値Ｖと公開キーｐを入力に取る。

【００１５】

本発明による方法は、公開パラメータのみを用いて確認可能な認証値Ｖの発生を可能にする利点があり、該値はシリアル関数、すなわち入力を構成するパラメータのビットを連続的に処理する関数のみによって発生させられる。

【００１６】

暗号通信法と装置の入力パラメータは、シリアル関数内で処理され、後者は、入力パラメータに全て、または部分的に依存するデータを出力に提供する。

【００１７】

方法と装置の入力パラメータはあるリストに属し、該リストは、認証メカニズムの実行の場合、少なくとも一つの識別子Ｉと、秘密のプライベートキーｓと、プライベートキーｓに対応する公開キーｐと、この公開キーの証明書と、確認装置によって提供された第２の確率変数ｔとを備えている。

【００１８】

確率変数ｒの計算を可能にするシリアル擬似乱数生成器は、上述の仏国特許出願公開第２８２６５３１号の番号で２００２年１２月２７日に公開されたフランス特許出願に記載

されたタイプの対称認証法に有利に基づくことができる。
したがって、このような方法の計算関数をｆ（Ｋ、Ｍ）で表すと、Ｋが対称秘密キーを表し、Ｍが関数ｆの他のオペランド全体を表すが、このとき確率変数ｒは、Ｋの同じ値を保ちながら、Ｍの異なる値に関数ｆを反復適用することで発生させられる。
例として、ｆの出力値ｚのサイズがｋビットに等しく、確率変数ｒのサイズが１６ｋビットに等しいとき、チップの最初の認証の際に使用される第１の確率変数ｒは、１６の出力値ｆ（Ｋ、$Ｍ_{1}$）、ｆ（Ｋ、$Ｍ_{2}$）、・・・、ｆ（Ｋ、$Ｍ_{16}$）の連結に等しく選択することができる。
第２の確率変数は、１６の出力値ｆ（Ｋ、$Ｍ_{17}$）、ｆ（Ｋ、$Ｍ_{18}$）、・・・、ｆ（Ｋ、$Ｍ_{32}$）などの連結に等しく選択することが可能など、すべての値$Ｍ_{i}$は、互いに判別される（典型的には、$Ｍ_{i+1}$の値は$Ｍ_{i}$の値の増加によって得られる）。
擬似乱数生成器を目的とする、認証法を用いる他の多くの方法も可能である。

【００１９】

シリアル関数は、加算、減算と左または右へのシフトを含んでいる。
実際、これらの演算は連続的に、非常に容易に実現することができる。

【００２０】

すなわち、本発明の課題を解決するための手段は、つぎの通りである。

【００２１】

第１に、
アプリケーションと電子チップの間のトランザクションにおいて、入力パラメータから認証値Ｖを電子チップ内で計算することからなる、ワイヤードロジックチップのための、電子チップの不正行為に対する保護の非対称暗号通信法であり、前記方法が、
・チップ内に含まれるシリアル擬似乱数生成器を用いて、トランザクションに固有の確率変数ｒと呼ばれる擬似乱数をチップによって発生させること（１）と、
・数学的関係式によって確率変数ｒに結びつけられ、チップのデータメモリ内に保存された、トランザクションに先立ってアプリケーションによって計算されるパラメータｘを、チップからアプリケーションに伝達すること（２）と、
・入力パラメータとして、少なくともトランザクションに固有の確率変数ｒと、一対の非対称キー（ｓ、ｐ）に属するプライベートキーｓとを有するシリアル関数を用いて、認証値Ｖの全体または一部を構成するパラメータｙを、チップによって計算すること（３）と、
・認証値Ｖをチップからアプリケーションに伝達すること（４）と、
・入力パラメータが、少なくとも一つの公開キーｐを含む、公開パラメータで排他的に構成される認証関数を用いて、前記認証値Ｖをアプリケーションによって確認すること（５）とからなる段階を含むことを特徴とする方法。
第２に、
トランザクションに固有の確率変数ｒの発生が、
・混合関数（１２）を用いて入力パラメータの全てまたは一部を混合し、一連のビットを混合関数の出力に提供することと、
・少なくとも旧状態と一連のビットの一つの値に依存する関数によって、旧状態から新状態に移行させることで有限状態オートマトン（１３）の状態変化を実行することと、
・オートマトンの少なくとも一つの状態を入力引数として有する出力関数（１４）を用いて、確率変数ｒの全体または一部を形成するために、一連の乱数ビットを決定することとからなることを特徴とする、上記第１に記載の方法。
第３に、
入力パラメータの一つが秘密キーＫで構成され、該秘密キーが、チップとアプリケーションの間で共有され、チップの保護された記憶領域内に保存されることを特徴とする、上記第２に記載の方法。
第４に、
数学的関係式が、特性として少なくとも結合的である演算を備えている要素ｇの集合Ｇ

内の関数g^rで構成されることを特徴とする、上記第１または上記第２に記載の方法。
第５に、
集合Ｇが、ｎより小さく、ｎに対して素である正またはゼロである整数の群Z_n^*であることを特徴とする、上記第４に記載の方法。
第６に、
集合Ｇが、任意のあらゆる有限体に作られたあらゆる楕円曲線であることを特徴とする、上記第４に記載の方法。
第７に、
シリアル関数が、あるリストから取られた演算を実行する算術関数であり、該リストが、加算、減算および左または右へのシフトを含んでいることを特徴とする、上記第１または上記第２に記載の方法。
第８に、
算術関数が、加算のみを実行することを特徴とする、上記第７に記載の方法。
第９に、
算術関数が、減算のみを実行することを特徴とする、上記第７に記載の方法。
第１０に、
算術関数が、さらに入力引数として入力パラメータを有し、アプリケーションによってシリアル関数の入力パラメータｔに割り当てられた値に応じて、次の演算：ｙ＝ｒおよびｙ＝ｒ＋ｓの一つを実行することからなることを特徴とする、上記第７に記載の方法。
第１１に、
数学的関係式が、特性として少なくとも結合的である演算を備えている要素ｇの集合Ｇ内の関数g^rで構成され、確認関数が、認証値Ｖに適用された関数によって提供される結果を、パラメータｔの値に応じて、次の値：値ｘ、値ｘとその秘密キーｓに対応するチップの公開キーｐとの積（ｘｐ）、の一つと比較し、このことが、パラメータｔの値に応じて、ｙが認証値Ｖに等しく、ｐが関数$p=g^s$によって定義され、秘密キーｓに対応するチップの公開キーである、次の方程式：$g^y=x$と$g^y=xp$、の一方をテストすることに等しくなることを特徴とする、上記第１０に記載の方法。
第１２に、
算術関数が、さらに入力引数として入力パラメータを有し、アプリケーションによってシリアル関数の入力パラメータｔに割り当てられた値に応じて、次の演算：ｙ＝ｒおよびｙ＝ｒ－ｓ、の一つを実行することからなることを特徴とする、上記第７に記載の方法。
第１３に、
数学的方程式が、特性として少なくとも結合的である演算を備えている要素ｇの集合Ｇ内の関数g^rで構成され、確認関数が、認証値Ｖに適用された数学的方程式によって提供された結果を、パラメータｔの値に応じて、次の値：値ｘ、値ｘと秘密キーｓに対応するチップの公開キーｐとの積（ｘｐ）、の一つと比較し、このことが、パラメータｔの値に応じて、ｙが認証値Ｖに等しく、ｐが方程式$p=g^s$によって定義され、秘密キーｓに対応するチップの公開キーである、次の方程式：$g^y=x$と$g^y.\ p=x$、の一方をテストすることに等しくなることを特徴とする、上記第１２に記載の方法。
第１４に、
算術関数が、さらに入力引数として入力パラメータを有し、アプリケーションによってシリアル関数の入力パラメータｔに割り当てられた値に応じて、次の演算：$y=r+2^i s$を実行することからなり、このパラメータｔが、ｍビット（t_{m-1}、・・・、t_0）のチェーンで構成され、そのビットの一つだけ、ビットt_iが１に等しく、ｍが自然数であることを特徴とする、上記第７に記載の方法。
第１５に、
数学的関係式が、特性として少なくとも結合的である演算を備えている要素ｇの集合Ｇ内の関数g^rで構成され、確認関数が、パラメータｔの値に応じて、ｙが認証値Ｖに等しく、ｐが関数$p=g^s$によって定義され、秘密キーｓに対応するチップの公開キーである、方程式$g^y=xp\wedge(2\wedge i)$をテストすることからなることを特徴とする、上記第１

４に記載の方法。

第１６に、

算術関数が、さらに入力引数として入力パラメータを有し、アプリケーションによってシリアル関数の入力パラメータｔに割り当てられた値に応じて、次の演算：ｙ＝ｒ＋２^{t}ｓを実行することからなることを特徴とする、上記第７に記載の方法。

第１７に、

数学的関係式が、特性として少なくとも結合的である演算を備えている要素ｇの集合Ｇ内の関数ｇ^{r}で構成され、確認関数が、ｙが認証値Ｖに等しく、ｐが関数ｐ＝ｇ^{s}によって定義され、秘密キーｓに対応するチップの公開キーである、次の方程式ｇ^{y}＝ｘｐ＾（２＾ｔ）をテストすることからなることを特徴とする、上記第１６に記載の方法。

第１８に、

算術関数が、さらに入力引数として入力パラメータを有し、アプリケーションによってシリアル関数の入力パラメータｔに割り当てられた値に応じて、ｔが整数である次の演算：ｙ＝ｒ＋ｔｓを実行することからなることを特徴とする、上記第７に記載の方法。

第１９に、

数学的関係式が、特性として少なくとも結合的である演算を備えている要素ｇの集合Ｇ内の関数ｇ^{r}で構成され、確認関数が、認証値Ｖに適用された関数によって提供される結果を、パラメータｔの値に応じて、次の値：値ｘ、値ｘと秘密キーｓに対応するチップの公開キーｐとの積（ｘｐ）、の一つと比較し、このことが、パラメータｔの値に応じて、ｙが認証値Ｖに等しく、ｐが関数ｐ＝ｇ^{s}によって定義され、秘密キーｓに対応するチップの公開キーである、次の方程式：ｇ^{y}＝ｘｐ^{t}をテストすることに等しくなることを特徴とする、上記第１８に記載の方法。

第２０に、

チップからアプリケーションに伝達されたパラメータｘが、数学的関数によって確率変数ｒに接続された少なくとも一つの要素と、アプリケーションに結びつけられたデータを含むオプションフィールドＤとに適用されたハッシュ関数の結果であることを特徴とする、上記第１または上記第２に記載の方法。

第２１に、

算術関数が、さらに入力引数として入力パラメータを有し、アプリケーションによってシリアル関数の入力パラメータｔに割り当てられた値に応じて、次の演算：ｙ＝ｒ＋２^{i}ｓを実行することからなり、このパラメータｔが、ｍビット（ｔ$_{m-1}$、・・・、ｔ$_{0}$）のチェーンで構成され、そのビットの一つだけ、ビットｔ$_{i}$が１に等しく、ｍが自然数であることを特徴とする、上記第２０に記載の方法。

第２２に、

数学的関係式が、特性として少なくとも結合的である演算を備えている要素ｇの集合Ｇ内の関数ｇ^{r}で構成され、確認関数が、パラメータｔの値に応じて、ｙが認証値Ｖに等しく、ｐが関数ｐ＝ｇ^{s}によって定義され、秘密キーｓに対応するチップの公開キーである、次の方程式：ｈ（ｇ^{y}／ｐ＾（２＾ｉ），Ｄ）＝ｘをテストすることからなることを特徴とする、上記第２１に記載の方法。

第２３に、

数学的関係式が、特性として少なくとも結合的である演算を備えている要素ｇの集合Ｇ内の関数ｇ^{r}であり、確認関数が、ｙが認証値Ｖに等しく、ｐが関数ｐ＝ｇ$^{-s}$によって定義され、秘密キーｓに対応するチップの公開キーである、次の方程式：ｈ（ｇ^{y}・ｐ＾（２＾ｉ），Ｄ）＝ｘをテストすることからなることを特徴とする、上記第２１に記載の方法。

第２４に、

算術関数が、さらに入力引数として入力パラメータを有し、アプリケーションによってシリアル関数の入力パラメータｔに割り当てられた値に応じて、次の演算：ｙ＝ｒ－２^{i}ｓを実行することからなり、このパラメータｔが、ｍビット（ｔ$_{m-1}$、・・・、ｔ$_{0}$）のチェーンで構成され、そのビットの一つだけ、ビットｔ$_{i}$が１に等しく、ｍが自然数で

あることを特徴とする、上記第２０に記載の方法。
第２５に、
数学的関係式が、特性として少なくとも結合的である演算を備えている要素ｇの集合Ｇ内の関数g^rで構成され、確認関数が、ｙが認証値Ｖに等しく、ｐが関数$p=g^s$によって定義され、秘密キーｓに対応するチップの公開キーである、次の方程式：ｈ（$g^y \cdot p^{(2^i)}$，Ｄ）＝ｘをテストすることからなることを特徴とする、上記第２４に記載の方法。
第２６に、
数学的関数が、特性として少なくとも結合的である演算を備えている要素ｇの集合Ｇ内の関数g^rで構成され、チップからアプリケーションに伝達されたパラメータｘが、Ｄがアプリケーションに結びつけられたデータを含むオプションフィールドを示し、ｈがハッシュ関数である、ｘ＝ｈ（g^r、Ｄ）型の関係式の結果であることを特徴とする、上記第２０に記載の方法。
第２７に、
シリアル関数が、入力引数として入力パラメータを有し、アプリケーションによってシリアル関数の入力パラメータｔに割り当てられた値に応じて、次の演算：ｙ＝ｒとｙ＝ｒ＋ｓ、の一つを実行することからなり、確認関数が、値ｘを、パラメータｔの値に応じて、ｙが認証値Ｖに等しく、ｐが方程式$p=g^s$によって定義され、秘密キーｓに対応するチップの公開キーである、次の値：ｈ（g^y、Ｄ）、ｈ（g^y／ｐ、Ｄ）、の一つと比較することを特徴とする、上記第２６に記載の方法。
第２８に、
シリアル関数が、入力引数として入力パラメータを有し、アプリケーションによってシリアル関数の入力パラメータｔに割り当てられた値に応じて、次の演算：ｙ＝ｒとｙ＝ｒ＋ｓ、の一つを実行することからなり、確認関数が、値ｘをパラメータｔの値に応じて、ｙが認証値Ｖに等しく、ｐが方程式$p=g^{-s}$によって定義され、秘密キーｓに対応するチップの公開キーである、次の値：ｈ（g^y、Ｄ）、ｈ（g^y．ｐ、Ｄ）の一つと比較することを特徴とする、上記第２６に記載の方法。
第２９に、
シリアル関数が、入力引数として入力パラメータを有し、アプリケーションによってシリアル関数の入力パラメータｔに割り当てられた値に応じて、次の演算：ｙ＝ｒとｙ＝ｒ－ｓ、の一つを実行することからなり、確認関数が、値ｘをパラメータｔの値に応じて、ｙが認証値Ｖに等しく、ｐが方程式$p=g^s$によって定義され、秘密キーｓに対応するチップの公開キーである、次の値：ｈ（g^y、Ｄ）、ｈ（g^y．ｐ、Ｄ）の一つと比較することを特徴とする、上記第２６に記載の方法。
第３０に、
集合Ｇは、ｎより小さく、ｎに対して素である正またはゼロの整数の群Z_n^*であることを特徴とする、上記第７から上記第２９のいずれか一つに記載の方法。
第３１に、
集合Ｇは、任意のあらゆる有限体に作られたあらゆる楕円曲線であることを特徴とする、上記第７から上記第２９のいずれか一つに記載の方法。
第３２に、
アプリケーションと電子チップの間のトランザクションにおいて、入力パラメータから認証値Ｖを電子チップによって計算することからなる、上記第１から上記第３１のいずれか一つに記載の電子チップの不正行為に対する保護の非対称暗号通信法を使用することを可能にする、電子チップ付装置（６）であり、前記装置が、
・トランザクションに固有の確率変数ｒを発生させるシリアル擬似乱数生成器（７）と、
・少なくとも一つのｘの値が保存された第１の記憶手段（８）で、パラメータｘの値が、トランザクションに先立ってアプリケーションによって計算され、数学的関係式によって確率変数ｒの値に結びつけられているものと、
・トランザクションに固有の確率変数ｒに結びつけられたパラメータｘを、電子チップか

らアプリケーションに伝達する手段（９）と、
・入力パラメータとして、少なくともトランザクションに固有の確率変数ｒと、一対の非対称キー（ｓ、ｐ）に属するプライベートキーｓとを有し、パラメータｙを出力に提供するシリアル関数の実行手段（１０）と、
・少なくともパラメータｙから認証値Ｖを構成するための出力手段（９）とを備えていることを特徴とする電子チップ付装置。
第３３に、
アプリケーションと電子チップの間のトランザクションにおいて、もっぱら公開であるパラメータから、電子チップによって計算された認証値Ｖを確認することからなる、上記第１から上記第３１のいずれか一つに記載の電子チップの不正行為に対する保護の非対称暗号通信法を実行するための確認装置であり、
前記装置が、少なくとも認証値Ｖと公開キーｐを入力に取る確認関数の実行手段を備えていることを特徴とする確認装置。
【発明の効果】
【００２２】
本発明によると、ワイヤードロジックチップ内に、特に多数のチップを展開しているアプリケーションの中に、公開キー式認証能動メカニズムを組み込めることが可能になる。
【発明を実施するための最良の形態】
【００２３】
本発明のその他の特徴と利点は、付属の図面を参照して、非制限的な例として挙げられた、本発明の特定の実施態様の下記の説明を読むことによって明らかになるだろう。
【００２４】
図１は、本発明による方法のフローチャートである。
図２は、本発明による電子チップ付装置の概略図である。
図３は、本発明による電子チップ付装置における擬似乱数生成器の実施例の概略図である。
図４は、本発明による電子チップ付装置におけるシリアル関数の実行手段の実施例の概略図である。
【００２５】
図１は、アプリケーションと電子チップの間のトランザクションにおける、本発明による電子チップの不正行為に対する保護の非対称暗号通信法のフローチャートを示している。
【００２６】
本方法は、入力パラメータから認証値を電子チップ内で計算することからなる。
【００２７】
図１の番号１に示すように、第１の過程において、本方法はチップ内に含まれたシリアル擬似乱数生成器を用いて、確率変数と呼ばれる擬似乱数ｒをチップによって発生させることからなる。
擬似乱数ｒである確率変数は、トランザクションに固有である。
【００２８】
図１の番号２に示すように、第２の過程において、本方法はパラメータｘをチップからアプリケーションに伝達することからなる。
このパラメータｘは、トランザクションに先立ってアプリケーションによって計算され、チップのデータメモリ内に保存される。
このパラメータｘは、数学的関係式によって確率変数ｒに結びつけられる。
アプリケーションは、少なくとも一つのパラメータｘを計算し、有利にはいくつかを計算する。
実施のある場合によれば、これらのパラメータｘは、あるチップに対するある集合において、連続的に取られた値に適用される数学的関数の結果である。
この集合は、チップによって生成した確率変数ｒのさまざまな値が、集合内に含まれる

ようになっている。

【００２９】

したがって、確率変数ｒとパラメータｘを結びつける数学的関数は、典型的にはある演算を備えた集合Ｇの中の指数関数で構成され、該演算は、少なくとも、特性として結合的であって、乗算の形で記される。

すなわち、関数は$x = g^r$であり、ここでｒは整数、ｇはアプリケーションによってあらかじめ選択された前記集合Ｇの要素を示す。

【００３０】

ｒは擬似乱数であり、チップごとに、また認証ごとに異なっている。

それは２回計算され、最初はアプリケーションによって、２回目はチップ自体によって計算される。

ｒを計算した後、アプリケーションは対応するｘを計算する。

アプリケーションは、次に、チップのカスタマイズの際に少なくとも一つのｘの値をチップ内に保存する。

有利には、アプリケーションはいくつかのｘの値を保存する。

アプリケーションとチップは、ｒの同じ値を発生させなければならないので、アプリケーションの擬似乱数生成器とチップの擬似乱数生成器は、厳密に同一でなければならない。

【００３１】

ｇは、有利にはアプリケーションに接続された全ての電子チップについて同一とすることが、またはチップに固有とすることができる。

後者の場合、ｇは、電子チップの公開キーのｐの不可欠な部分となる。

集合Ｇの典型的な例は、ｎが任意の正の整数であるとき、ｎ以下でありｎに対して素である正またはゼロの整数の群Z_n^*、あるいはまた、あらゆる有限体に作られたあらゆる楕円曲線である。

【００３２】

図１の番号３に示すように、第３の過程において、本方法はシリアル関数を用いて、パラメータｙをチップによって計算することからなり、該関数は入力パラメータとして、少なくともトランザクションに固有の確率変数ｒと、一対の非対称キー（ｓ、ｐ）に属する秘密のプライベートキーｓとをに有しており、このパラメータｙは、認証値Ｖの全体または一部を構成する。

ここで、シリアル関数は、算術関数で構成される。

【００３３】

図１の番号４に示すように、第４の過程において、該方法は認証値Ｖをチップからアプリケーションに伝達することからなる。

【００３４】

図１の番号５に示すように、第５の過程において、本方法は確認関数を用いて、前記認証値Ｖをアプリケーションによって確認することからなり、該確認関数の入力パラメータは、少なくとも公開キーｐを含む、公開パラメータのみによって構成される。

【００３５】

図２は、本発明による電子チップ付装置を概略的に示している。

電子チップ付装置は、アプリケーションと電子チップの間のトランザクションにおける、本発明による電子チップの不正行為に対する保護の非対称暗号通信法の使用を可能にするもので、入力パラメータから認証値Ｖを電子チップによって計算することからなる。

【００３６】

電子チップ付装置６は、

・トランザクションに固有の確率変数ｒを発生させるシリアル擬似乱数生成器７と、

・トランザクションに先立ってアプリケーションによって計算される、一つまたは複数のパラメータｘが保存された第１の記憶手段である記憶装置８で、それぞれのパラメータｘが数学的関係式によって確率変数ｒの値に結びつけられ、該値がシリアル擬似乱数生成器

によって発生させることができる値の集合に含まれるものと、
・トランザクションに固有の確率変数ｒに結びつけられたパラメータｘの第１の出力手段９と、
・シリアル関数１０の実行手段で、入力パラメータとして、少なくともトランザクションに固有の確率変数ｒと、一対の非対称キー（ｓ、ｐ）に属するプライベートキーｓとを有し、このパラメータｙが認証値Ｖの全体または一部を構成するものと、
・少なくともパラメータｙから認証値Ｖを構成した後の、この値の第２の出力手段９とを備えている。

【００３７】

シリアル擬似乱数生成器７は、図２に照らし合わせて採用され、記載された実施例の場合、上述の仏国特許出願公開第２８２６５３１号の番号で２００２年１２月２７日に公開されたフランス特許出願に記載のタイプの対称暗号通信法に基づいている。

したがって、ｆ（Ｋ、Ｍ）でこのような方法の計算関数を表すと、Ｋは対称秘密キーを表し、Ｍは関数ｆの他のオペランドの集合を表すが、このとき確率変数ｒは、Ｋの同じ値を保ちながら、関数ｆをＭの異なる値に反復適用することで発生させられる。

例として、ｆの出力値ｚのサイズがｋビットに等しく、確率変数ｒのサイズが１６ｋビットに等しいとき、チップの最初の認証の際に使用される第１の確率変数ｒは、ｆ（Ｋ、M_1）、ｆ（Ｋ、M_2）、・・・、ｆ（Ｋ、M_{16}）といった１６個の出力値の連結に等しく選択することができ、第２の確率変数は、ｆ（Ｋ、M_{17}）、ｆ（Ｋ、M_{18}）、・・・、ｆ（Ｋ、M_{32}）などの１６個の出力値の連結に等しく選択することが可能で、すべての値M_iは互いに区別される。

【００３８】

図３は、このようなシリアル擬似乱数生成器７を示している。

この発生器は、混合の結果であるデータＥ’＝（e'_1、e'_2、・・・e'_n、・・・、e'_N）を出力に提供するための、入力パラメータの全体または一部の混合手段１２、少なくとも旧状態と一連のビット（e'_1、e'_2、・・・e'_n、・・・、e'_N）の値に依存する関数によって、旧状態から新状態に移行する有限状態オートマトン１３、オートマトンの少なくとも一つの状態を含む入力引数から値ｚを計算し、ついで連続する１６個の出力値ｆ（Ｋ、M_1）、ｆ（Ｋ、M_2）、・・・、ｆ（Ｋ、M_{16}）の連結を実施して、選択される確率変数ｒの値を決定するための出力手段１４とを備える。

混合手段１２の入力パラメータは、非網羅的リスト内で取ることができる。

該リストは、秘密キーＫ、チップの内部データＤ、データＤのメモリアドレス、チップの外部データＤ’、アプリケーションによって提供される確率変数Ｒ’を含む。

【００３９】

混合手段１２は、入力データの線形または非線形関数とすることができる混合関数ＭＩＸを実行する。

【００４０】

線形関数の第１の例は、入力データ間のスカラー積を実施することからなる。

【００４１】

線形関数の別の実行例によれば、混合手段は、線形フィードバックシフトレジスタを含んでおり、該レジスタにおいて、入力パラメータのビットは連続して入力され、レジスタの初期状態および／またはフィードバックビットの値に影響を与える。

【００４２】

非線形関数の実施例によれば、混合手段は、非線形フィードバックシフトレジスタを含んでおり、該レジスタにおいて入力パラメータのビットは連続して入力される。

出力Ｓ’の値は、このレジスタの内容から抽出される一つまたは複数のビットで構成することができる。

【００４３】

オートマトン１３ＡＵＴの第１の実施例は、ブール回路を用いることからなる。

すなわち、例えば、ｋ＋１ビットのベクトル（A_1、A_2、・・・A_{k+1}）にｋビッ

トのベクトル（Ａ’$_1$、Ａ’$_2$、・・・Ａ’$_k$）を組み合わせる。
ここで、それぞれのビットＡ’$_i$は、排他的ＯＲ、ＯＲ（内包的）、ＡＮＤ、ＮＯＴなどの基本演算を用いることで、ビット（Ａ$_1$、Ａ$_2$、・・・Ａ$_k$）から得られる。
この際、（Ａ$_1$、Ａ$_2$、・・・Ａ$_k$）は、オートマトンの旧状態を表している。
オートマトンは、ｋビットの内部状態（Ａ$_1$、Ａ$_2$、・・・Ａ$_k$）を有し、新ベクトル（Ａ$_1$、Ａ$_2$、・・・Ａ$_k$、Ｓ’ｅ’）がブール回路の入力に存在するたびに、新状態（Ａ’$_1$、Ａ’$_2$、・・・Ａ’$_k$）を出力に提供する。
新ベクトルは、内部状態と混合関数ＭＩＸの出力で構成される。

【００４４】

オートマトン１３の第２の実施例は、数の表によって定義されるビット変換を用いることからなる。
ｋ＝８のとき、例えば、８ビットバイト（Ａ$_1$、Ａ$_2$、・・・Ａ$_8$）を２つの４ビットバイト（Ａ$_1$、Ａ$_2$、Ａ$_3$，Ａ$_4$）と（Ａ$_5$、Ａ$_6$、Ａ$_7$，Ａ$_8$）に分割する。
そして、混合関数の出力ビットＥ’ｅ’がゼロに等しいときは変換Ｔを、あるいはＥ’ｅ’が１に等しいときは変換Ｕを、それぞれの４ビットバイトに適用することができる。
変換Ｔは、４ビットバイトのそれぞれの値（ａ、ｂ、ｃ、ｄ）に４ビットバイトの値（ａ’、ｂ’、ｃ’、ｄ’）を組み合わせる表によって定義される。
Ｕについても同様である。

【００４５】

全ての入力値を計算に入れたとき、オートマトン１３は、ある最終状態にある（Ｆ$_1$、Ｆ$_2$、・・・Ｆ$_k$）。

【００４６】

シリアル擬似乱数生成器の出力手段１４は、典型的にはオートマトンの最終状態に適用された恒等関数である出力関数と連結演算を実行する。
この手段は、例えば、サイズが１６ｋビットである、確率変数ｒのサイズに等しい記憶領域である。

【００４７】

一つまたは複数のパラメータｘが保存されている第１の記憶手段である記憶装置８は、典型的には、非揮発性メモリで構成され、該メモリは必要ならば書換可能である。
パラメータｘは、電子チップの市販の前にメモリ内に書き込まれる。
パラメータｘの計算に介在する確率変数ｒの値は、チップが忠実にこの値を再計算できるように選択される。
図２に照らし合わせて記載したシリアル擬似乱数生成器の例において、この条件は、秘密キーＫがチップとアプリケーションによって共有されることを要求する。
したがって、チップを流通させる前に、アプリケーションは計算関数が上述のｆで示された認証方法の反復適用によって、ｘのいくつかの値を計算し、チップのデータメモリ内に、これらの値を保存する。
認証のたびに、チップは、確率変数ｒを再計算し、それに対応するパラメータｘの値をデータメモリ内で読み取る。
図２に照らし合わせて記載したシリアル擬似乱数生成器の例において、ｒとｘの間の対応は、Ｍ$_1$の値として、ｒのこの値に対応するｘの値のアドレス決定を可能にする情報を選択することで確立され、０以上もしくは０に等しいｉについてのＭ$_i$＋１の値は、Ｍ$_i$の値を増加させることで得られる。

【００４８】

メモリ内の場所を節約するために、パラメータｘは、有利には要素自体ｇ^{r}ではなく、この要素のハッシュ関数ｈによる画像（また場合によっては、アプリケーションのデータなどの他の要素）に等しく選択される。
すなわち、ｘ＝ｈ（ｇ^r、Ｄ）となる。
ここで、Ｄは、例えば、アプリケーションに結びつけられたデータを含むオプションフィールドを示す。

例えば、Ｄはアプリケーションによって決定されたユーロの金額を示す。
この場合、それぞれのクーポンは電子貨幣を表し、それぞれの認証は、かかる貨幣の消費を表す。
【００４９】
トランザクションに固有の確率変数ｒに結びつけられたパラメータｘの第１の出力手段９は、典型的には出入力バッファである。
【００５０】
シリアル関数を実行する手段１０の一つの例は、図４に照らし合わせて記載されている。
シリアル関数は、入力パラメータとして確率変数ｒと、一対の非対称キー（ｓ、ｐ）に属する秘密のプライベートキーｓとを有している。
ｐは、公開キーである。
【００５１】
シリアル関数を実行する手段１０は、計算と繰り上がりを考慮に入れたビット加算器で構成される。
【００５２】
ｒのカレントビットr_iの値は、第１のレジスタ１５に取り込まれ、カレントビットs_iの値は、第２のレジスタ１６に取り込まれる。
第３のレジスタ１７は、先行ビットの加算の結果である繰り上がりc_iを取り込む。
最後に、第４のレジスタ１８は、先行する加算の際に得られた繰り上がりとともに、カレントビットr_iとs_iの値の合算の後に得られたビットy_iを取り込み、この繰り上がりは、第３のレジスタ１７の内容に対応している。
繰り上がりc_iは、ＡＮＤ素子１９の出力であり、その入力が最初の２つのレジスタ１５，１６の出力である、先行ビットの加算の際に発生した繰り上がりと、ＡＮＤ素子２０の出力でありその入力がカレントビットｒｉとｓｉの値である、カレントビットの加算の際に発生した繰り上がりを考慮した結果である。
中間ＡＮＤ素子２１は、先行ビットの加算の際に発生した繰り上がりがある時には、カレントビットの一つだけが１であるとき、繰り上がりを発生させる。
繰り上がりは、入力がカレントビットの値である排他的ＯＲ素子２２の出力である。
【００５３】
したがって、繰り上がりc_iは、中間ＡＮＤ素子２１とＡＮＤ素子２０の出力の間のＯＲ２３である。
該素子２０の入力は、カレントビットr_iとs_iである。
この繰り上がりc_iは、r_iとs_iの後続ビットの加算の際に考慮に入れるために、第３のレジスタ１７に取り込まれる。
【００５４】
ビットy_iは、繰り上がりの値とともにカレントビットr_iとs_iの値の加算の結果として生じる。
該加算値は、入力がカレントビットr_iとs_iの値である排他的ＯＲ素子２２の出力である。
繰り上がりの値は、入力が先行する排他的ＯＲ素子２２の出力と第３のレジスタ１７の出力である、排他的ＯＲ素子２４の出力である。
【００５５】
レジスタ１５，１６，１７、１８の値は、０に初期化される。
【００５６】
これによって、最終的に、$y_i = r_i + s_i + c_i \pmod 2$と$c_{i+1} = r_i + s_i + c_i \ (\mathrm{div}\ 2)$が与えられる。
ここで、c_0は、０に等しく選択される。
【００５７】
特定の応用によれば、シリアル関数は、さらに、入力パラメータとしてアプリケーショ

ンによって提供された確率変数ｔを有する。

【００５８】

図２に照らし合わせて記載された方法によると、チップが確率変数ｒを発生させる。

ついで、（例えば、関数ｘ＝ｇ^{r}を介して）データメモリ内の前記確率変数に対応するパラメータｘの値を読み取る。

その後、チップは、ｘの値をアプリケーションに送る。

その後、アプリケーションは、サイズが１ビットに減らされた確率変数ｔをチップに送る。

【００５９】

このとき、２つの場合が生じる。

ｔの値が０に等しいとき、チップはｙ＝ｒを選択する。

ｔの値が１に等しいとき、チップはｙ＝ｒ＋ｓを選択する。

この選択の導入は、当業者には周知であり、したがって詳細には述べない。

【００６０】

認証値Ｖは、ｙに等しく取り、アプリケーションに送られる。

【００６１】

確認は方程式のテストからなり、ｔが０に等しいときはｇ^{y}＝ｘ、あるいはｔが１に等しいときはｇ^{y}＝ｘｐである。

ここで、ｐは関数ｐ＝ｇ^{s}によって定義され、秘密キーｓに対応するチップの公開キーである。

これらのパラメータが十分に大きく選択されたとき、今日広く認められている仮説である離散対数仮説によれば、ｇとｐからｓを再び見つけることは実現不可能である。

【００６２】

特定の応用によれば、ハッシュ関数ｈは、ｘの計算に使用できる。

この場合、確認方程式は、ｔが０に等しいときはｈ（ｇ^{y}、Ｄ）＝ｘ、あるいはｔが１に等しいときはｈ（ｇ^{y}／ｐ、Ｄ）＝ｘとなる。

確認方程式内のいっさいの除算を避けるため、ｙ＝ｒ＋ｓの代わりにｙ＝ｒ－ｓを選択することもできる。

その場合、第２の確認方程式は、ｈ（ｇ^{y}・ｐ、Ｄ）＝ｘとなる。

もう一つの可能性は、ｐ＝ｇ^{s}の代わりにｐ＝ｇ$^{-s}$を選択することである。

その場合は、ｈ（ｇ^{y}、Ｄ）＝ｘとｈ（ｇ^{y}・ｐ、Ｄ）＝ｘという確認方程式に至る。

【００６３】

前述の実施において、秘密キーｓを認識しているもの以外のすべてのチップは、最大２分の１の確率でアプリケーションによって有効と認識されうる認証値を提供する。

このことによって、すでに真正なチップとクローンの間の判別が確立できるが、この判別は、実際に適用する大半の場合において不十分である。

【００６４】

クローンが成功する確率を大幅に減らすための一つの解決法は、確率変数ｔのビット数ｍを増加させることにある。

例えば、確率変数ｔは、６４ビットのチェーン（ｔ$_{63}$、ｔ$_{62}$、・・・、ｔ$_{0}$）に等しく選択され、そのビットの一つだけが１に等しい。

ｉが、ｔ$_{i}$が１に等しくなるような唯一の指数であるとき、その場合、ｙの値はｙ＝ｒ＋２^{i}ｓに等しく選択される。

この値は、連続的に計算することが非常に容易であるが、それはｒとｉビットのｓを左に（左に行くほど重いとき）にシフトさせることで得られた整数の加算を実施することに帰するからである。

このとき、確認方程式は、ｇｙ＝ｘｐ＾（２＾ｉ）である。

この条件において、秘密キーｓを知っているもの以外のすべてのチップは、最大６４分の１の確率でアプリケーションによって有効と認識されうる認証値を提供する。

【００６５】

特定の応用によれば、ハッシュ関数ｈは、ｘの計算に使用できる。
この場合、確認方程式は、ｈ（ｇ^{y}／ｐ＾（２＾ｉ）、Ｄ）＝ｘとなる。
確認方程式内のいっさいの除算を避けるため、ｙ＝ｒ＋２^{i}ｓの代わりにｙ＝ｒ－２^{i}ｓを選択することもできる。
その場合、第２の確認方程式は、ｈ（ｇ^{y}・ｐ＾（２＾ｉ）、Ｄ）＝ｘとなる。
もう一つの可能性は、ｐ＝ｇ^{s}の代わりにｐ＝ｇ$^{-s}$を選択することである。
その場合は、ｈ（ｇ^{y}・ｐ＾（２＾ｉ）、Ｄ）＝ｘという確認方程式に至る。

【００６６】

記載したこの解決法の場合、先に定義したようなチェーンｔの代わりに、０とｍ－１の間に含まれる整数をｔの値に選ぶことは、セキュリティの観点から同じことになる。
このとき、ｙは、ｙ＝ｒ＋２^{t}ｓに等しく取られ、確認方程式はｇ^{y}＝ｘｐ＾（２＾ｔ）になる。

【００６７】

特定の応用によれば、ハッシュ関数ｈは、ｘの計算に使用できる。
この場合、確認方程式はｈ（ｇ^{y}／ｐ＾（２＾ｔ）、Ｄ）＝ｘとなる。
確認方程式内のいっさいの除算を避けるため、ｙ＝ｒ＋２^{t}ｓの代わりにｙ＝ｒ－２^{t}ｓを選択することもできる。
その場合、第２の確認方程式は、ｈ（ｇ^{y}・ｐ＾（２＾ｔ）、Ｄ）＝ｘとなる。
もう一つの可能性は、ｐ＝ｇ^{s}の代わりにｐ＝ｇ$^{-s}$を選択することである。
その場合は、ｈ（ｇ^{y}・ｐ＾（２＾ｔ）、Ｄ）＝ｘという確認方程式に至る。

【００６８】

先に定義したようなチェーンｔの代わりに、０とｍ－１の間に含まれる整数をｔの値に選ぶことは、セキュリティの観点からまたしても同じことになる。
このとき、ｙは、ｙ＝ｒ＋ｔｓに等しく取られ、確認方程式はｇ^{y}＝ｘｐ^{t}である。

【００６９】

特定の応用によれば、ハッシュ関数ｈは、ｘの計算に使用できる。
この場合、確認方程式はｈ（ｇ^{y}／ｐ^{t}、Ｄ）＝ｘとなる。
確認方程式内のいっさいの除算を避けるため、ｙ＝ｒ＋ｔｓの代わりにｙ＝ｒ－ｔｓを選択することもできる。
その場合、第２の確認方程式は、ｈ（ｇ^{y}・ｐ^{t}、Ｄ）＝ｘとなる。
もう一つの可能性は、ｐ＝ｇ^{s}の代わりにｐ＝ｇ$^{-s}$を選択することである。
その場合は、ｈ（ｇ^{y}・ｐ^{t}、Ｄ）＝ｘという確認方程式に至る。

【００７０】

確率変数ｔは、もちろん他の値を取ることができる。

【００７１】

認証値Ｖの第２の出力手段は、典型的には出力関数を用い、該関数はパラメータｙに適用された恒等関数である。
この出力手段９は、例えば、サイズがパラメータｙのサイズに等しい記録領域である。

【００７２】

アプリケーションと電子チップの間のトランザクションの際に、アプリケーションと電子チップは、本発明による電子チップの不正行為に対する保護の非対称暗号通信法を実行する。
この実行の際に、アプリケーションはチップの認証のために、本発明による認証装置を利用する。
本装置は、本発明による方法の認証関数を実行する手段を備えている。
この手段は、もっぱら公開であるパラメータを用いることで、電子チップによって計算された認証値Ｖを確認する。
該パラメータは、少なくともチップの秘密キーｓに結びつけられた公開キーｐを備えている。

【００７３】

本発明による方法の前述の実施態様の一つによれば、確認装置は認証値Ｖに適用された算術関数によって提供された結果（ｇ^{y}）を、パラメータｔの値に応じて、次の値：値ｘ、値ｘと秘密キーｓに対応するチップの公開キーｐとの積（ｘｐ）、の一つと比較する。

このとき、ｙは認証値Ｖに等しく、ｐは関数ｐ＝ｇ^{s}によって定義され、秘密キーｓに対応するチップの公開キーである。

【００７４】

この手段は、典型的には計算機である。

【図面の簡単な説明】

【００７５】

【図１】本発明による方法のフローチャートである。

【図２】本発明による電子チップ付装置の概略図である。

【図３】本発明による電子チップ付装置における擬似乱数生成器の実施例の概略図である。

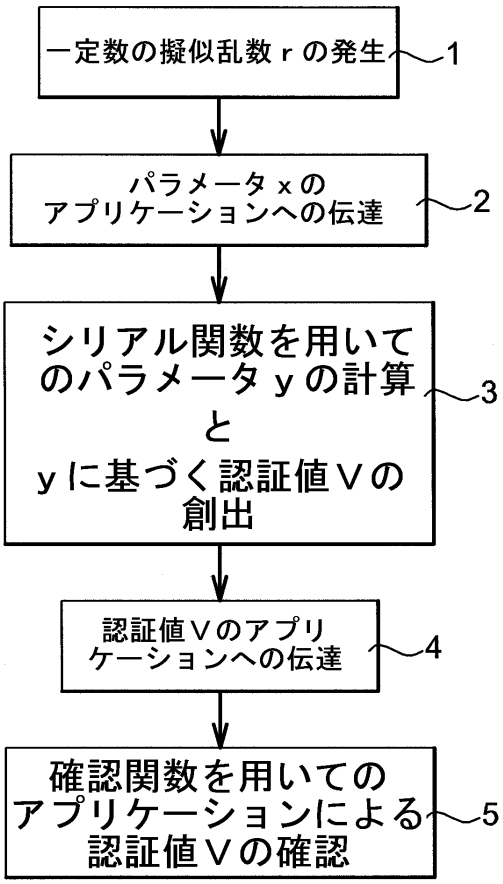
【図４】本発明による電子チップ付装置におけるシリアル関数の実行手段の実施例の概略図である。

【符号の説明】

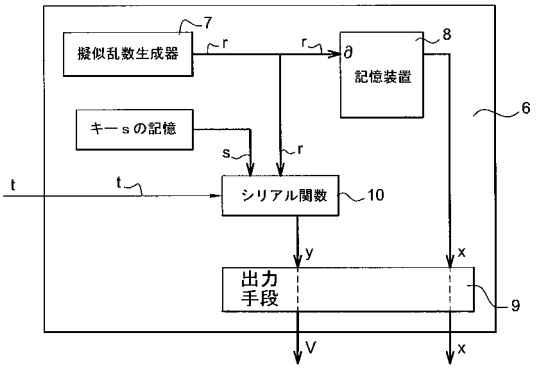
【００７６】

６　電子チップ付装置
７　擬似乱数生成器
８　記憶装置
９　出力手段
１０　シリアル関数
１２　混合手段
１３　オートマン
１４　出力手段

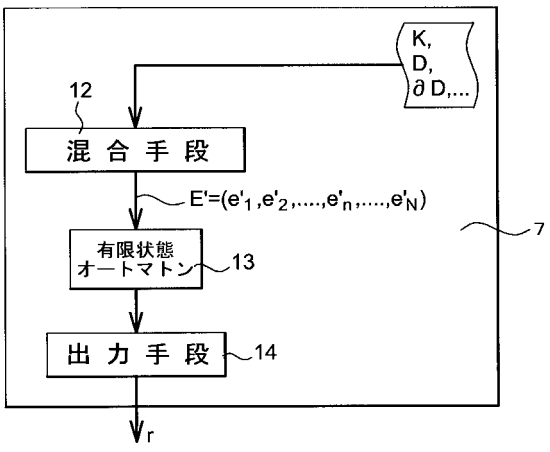
【図１】



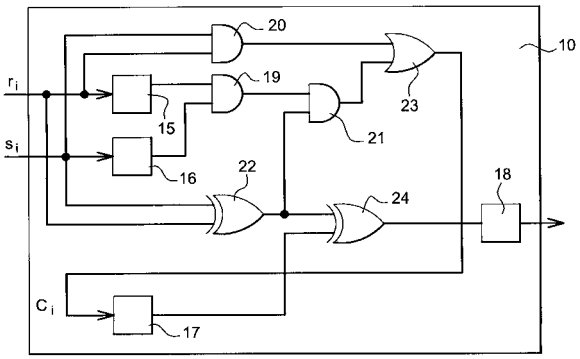
【図２】



【図３】



【図４】



フロントページの続き

(56)参考文献 特表２００５－５０３０５９（ＪＰ，Ａ）
特開平０５－３２３８７４（ＪＰ，Ａ）

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