(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5633563号
(P5633563)
(45)発行日　平成26年12月3日(2014.12.3)　(24)登録日　平成26年10月24日(2014.10.24)

(51)Int.Cl.　F I
G09C 1/00 (2006.01)　G09C 1/00 620Z
G09C 1/00 650Z

請求項の数 10　(全 18 頁)

(21)出願番号	特願2012-518114 (P2012-518114)
(86)(22)出願日	平成22年6月28日 (2010.6.28)
(65)公表番号	特表2012-531634 (P2012-531634A)
(43)公表日	平成24年12月10日 (2012.12.10)
(86)国際出願番号	PCT/FR2010/051339
(87)国際公開番号	WO2011/001093
(87)国際公開日	平成23年1月6日 (2011.1.6)
審査請求日	平成25年6月7日 (2013.6.7)
(31)優先権主張番号	0954473
(32)優先日	平成21年6月30日 (2009.6.30)
(33)優先権主張国	フランス(FR)

(73)特許権者　510171966
モルフォ
フランス国　パリ　エフ－７５０１５、リュ　ルブラン　２７
(74)代理人　100082108
弁理士　神崎　真一郎
(74)代理人　100156199
弁理士　神崎　真
(72)発明者　トマ　イカール
フランス国　パリ　Ｆ－７５０１５　リュ　ルブラン　２７　モルフォ内
(72)発明者　エルベ　シャバンヌ
フランス国　パリ　Ｆ－７５０１５　リュ　ルブラン　２７　モルフォ内

最終頁に続く

(54)【発明の名称】楕円曲線上のパラメータ化による暗号法

(57)【特許請求の範囲】
【請求項１】
装置（１０）もしくはコントローラ（１１）のいずれかとして定義される第１電子装置と、上記装置（１０）もしくは上記コントローラ（１１）のいずれか他方として定義される第２電子装置とを有し、パスワード（π）に基づく、コントローラ（１１）による装置（１０）の制御方法であって、次の：
／１／　上記第１電子装置が、
【数１】

$$E_{a,b}(x,y):x^3+ax+b=y^2$$

の有限体F_q（ｑは、整数である）において、乱数値r_1に基づき、楕円曲線の点P_1（Ｘ，Ｙ）を決定するステップと、
／２／　前記第１電子装置が、
【数４５】

$$P(X,Y)=F(k,k')$$

（式中、Ｆは、F_qにおける$F_q \times F_q$の全射関数である）であるような、第１及び第２パラメータk_1及びk_1'を求めるステップと、
／３／　前記第１電子装置が、前記第１及び第２パラメータk_1及びk_1'およびパスワード（π）を用いて、暗号化された第１、第２パラメータを求めるステップと、

／４／　前記第１電子装置が、暗号化された前記第１及び第２パラメータを前記第２電子装置へと伝送するステップとを含み、

対照的に、前記第２電子装置が、前記ステップ／１／と同様、乱数値r_2に基づいて楕円曲線の点P_2（Ｘ，Ｙ）を決定し、前記ステップ／２／と同様、第１及び第２パラメータk_2及びk_2’を求め、前記ステップ／３／と同様、暗号化された第１、第２パラメータを求め、前記ステップ／４／と同様、暗号化された前記第１及び第２パラメータを前記第１電子装置へと伝送するステップとを含み、

前記関数Ｆは、F_qの入力要素ｚ及びｚ’がいかなるものであれ、Ｆ（ｚ，ｚ’）が楕円曲線の点であり、前記入力要素が式（１）を満たさないようになっている制御方法。

【請求項２】

前記関数Ｆは：

【数８】

$$F(k, k') = f'(k') + f_{a,b}(k)$$

（式中、$f_{a,b}$は、入力パラメータを取り、かつ楕円曲線の点を提供する、楕円曲線の係数ａ及びｂに基づく逆関数であり、ｆ’は、パラメータに応じて楕円曲線の点を発生させる関数である）

と書き表され、前記ステップ／２／で、次の：

－　パラメータｋ’の値をランダムに発生させるステップと、

－　ｆ’（ｋ’）の値を計算するステップと、

－　次式：

【数９】

$$k = f_{a,b}^{-1}(P(X,Y) - f'(k'))$$

によりパラメータｋの値を決定するステップにより、パラメータｋ及びｋ’を求める請求項１に記載の制御方法。

【請求項３】

前記関数ｆ’は：

【数１０】

$$f'(k') = k'.G$$

（式中、Ｇは、楕円曲線の点の集合の生成元である）

と書き表され、パラメータｋの値は、次式：

【数１１】

$$k = f_{a,b}^{-1}(P(X,Y) - k'.G)$$

により決定される請求項２に記載の制御方法。

【請求項４】

前記関数ｆ’は：

【数１３】

$$f'(k') = f_{a,b}(k')$$

ように書き表され、

パラメータｋの値は、次式：

【数１４】

$$k = f_{a,b}^{-1}(P(X,Y) - f_{a,b}(k'))$$

により決定される請求項２に記載の制御方法。

【請求項５】

前記関数Ｆが、スカルバの等式：

【数２８】

$$f(X_1(k)).f(X_2(k)).f(X_3(k))=U(k)^2$$

（式中、ｆは、楕円曲線Ｅ$_{a,b}$を定義する多項式である）
を満たす多項式Ｘ$_1$（ｋ）、Ｘ$_2$（ｋ）、Ｘ$_3$（ｋ）、及びＵ（ｋ）を用いて得られた、少なくとも１つの逆関数ｆ$_{a,b}$を含む請求項１から４のいずれかに記載の制御方法。
【請求項６】
前記関数ｆ$_{a,b}$は：
【数２４】

$$x=(v^2-b-u^6/27)^{1/3}+u^2/3$$

かつ
【数２５】

$$y=u.x+v$$

（式中、
【数４１】

$$v=\frac{3a-u^4}{6u}$$

かつｆ$_{a,b}$（０）＝０）
であるように、Ｆ$_q$におけるパラメータｕに、Ｆ$_q{}^2$（式中、ｑは、２　ｍｏｄ　３に等しい）におけるパラメータ対（ｘ，ｙ）を対応させる請求項５に記載の制御方法。
【請求項７】
次の：
－　前記第１電子装置が、前記第２電子装置からの暗号化された第１及び第２パラメータからなるメッセージを受信するステップと、
－　前記第１電子装置が、前記メッセージから第１及び第２パラメータを復号し、パラメータｐ及びｐ’を求めるステップと、
－　前記第１電子装置が、次式：
【数３５】

$$K=r_1.F(p,p')$$

（式中、ｒ$_1$は、前記ステップ／１／で使用される乱数値である）
を用いて共通の秘密の値Ｋを計算するステップと、
対照的に、前記第２電子装置が、第１電子装置からのメッセージを受信するステップと、前記メッセージから第１及び第２パラメータを復号するステップと、前記共通の秘密の値Ｋを計算するステップとを、更に利用できる請求項１から６のいずれかに記載の制御方法。
【請求項８】
パスワードによる制御システムにおける装置（１０）、もしくは前記装置（１０）を制御するためのコントローラ（１１）として用いる電子装置であって、
上記電子装置は、
－　有限体Ｆ$_q$（ｑは、整数である）において、乱数値ｒ$_1$に基づき、楕円曲線の点Ｐ（Ｘ，Ｙ）を決定することに適しており、前記楕円曲線が、式：
【数１】

$$E_{a,b}(x,y):x^3+ax+b=y^2$$

である、決定装置（４１）と、

【数７】

$$P=F(k,k')$$

（式中、Ｆは、Ｆ$_q$におけるＦ$_q$×Ｆ$_q$の全射関数である）
であるような、第１及び第２パラメータｋ及びｋ’を求めることに適した取得装置（４２）と、
－　前記第１及び第２パラメータｋ及びｋ’およびパスワード（π）を用いて、暗号化された第１、第２パラメータを求めることに適した暗号化装置（４３）と、
暗号化された前記第１及び第２パラメータを、前記電子装置が装置（１０）である場合には上記前記コントローラ（１１）に、前記電子装置がコントローラ（１１）である場合には装置（１０）に、それぞれ伝送することに適したインタフェース装置（４４）とを含み、
前記関数Ｆは、Ｆ$_q$の入力要素ｚ及びｚ’がいかなるものであれ、Ｆ（ｚ，ｚ’）が楕円曲線の点であり、入力要素が（数１）を満たさないようになっている電子装置。
【請求項９】
請求項１から７のいずれかに記載の制御方法に記載した前記第１、第２電子装置として用いることを特徴とする請求項８に記載の電子装置。
【請求項１０】
コントローラとして請求項８又は９に記載の第１電子装置と、制御する装置として請求項８又は９に記載の第２電子装置とを少なくとも含む、パスワードによる制御システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、楕円曲線の点の使用、特にはＥＫＥ（英語で「Ｅｎｃｒｙｐｔｅｄ　Ｋｅｙ　Ｅｘｃｈａｎｇｅｄ（暗号化鍵交換）」）タイプのアルゴリズムの分野におけるこの使用に基づくメッセージの暗号法に関する。
【背景技術】
【０００２】
パスワードによる認証方法は、ＥＫＥタイプのアルゴリズムの使用に基づく。図１は、このタイプのアルゴリズムを示す。
【０００３】
装置Ｄ１０は、パスワードπに基づき、コントローラＣ１１に認証されることを望む。その構成要素の各々は、パスワードπを知っている。その上、楕円曲線Ｅ$_{a,b}$及び楕円曲線の点の集合の生成元Ｇを、パブリックパラメータとして考慮する。楕円曲線は、次式：
【数１】

$$E_{a,b}(x,y): x^3+ax+b=y^2$$

を満たす。
【０００４】
ステップ１２において、装置Ｄ１０は、乱数ｒ$_1$を発生させる。次に装置は、コントローラ１１にこの乱数を楕円曲線の点の形式で伝送する。そのために装置は：
【数２】

$$V=r_1.G$$

を満たす、伝送する値Ｖを決定する。
【０００５】
この結果は、次にパスワードによりＥ$_\pi$（ｒ$_1$．Ｇ）（Ｅ$_\pi$は、パスワードによる暗号化関数である）の形式で暗号化される。
【０００６】

次に装置は、値E_{π}（r_1．G）を示してコントローラ宛てにメッセージ１３を発信する。

【０００７】

メッセージ１３の受信後に、今度はコントローラ１１が、乱数値r_2をステップ１４で発生させる。次にコントローラは、この値を楕円曲線の点の形式で伝送し、結果：

【数３】

$$E_{\pi}(r_2.G)$$

を示して、メッセージ１５を装置１０に伝送する。

【０００８】

乱数値r_1及びr_2の暗号化形式でのこの交換に続き、装置１０は、ステップ１６で、パスワードD_{π}による復号関数を用いて、メッセージ１５に含まれる情報：

【数４】

$$r_2.G = D_{\pi}E_{\pi}(r_2.G)$$

を復号して、コントローラによって発生した乱数値r_2を回復し、
コントローラ１１は、ステップ１７で、メッセージ１３に含まれる情報：

【数５】

$$r_1.G = D_{\pi}E_{\pi}(r_1.G)$$

を復号して、装置１０によって発生した乱数値r_1を回復する。

【０００９】

このようにして、保護された交換に続き、各構成要素は、共通の鍵Ｋを計算できる：

【数６】

$$K = r_1.r_2.G$$

【００１０】

このタイプのアルゴリズムは、パスワード又はパスワードから派生した鍵により、値を暗号化形式で交換することを目的とする。しかしながら、有限対F_qに対して（数１）を満たす楕円曲線の古典的な表示によれば、図１に関して記載される交換により、潜在的な攻撃者が、パスワードπに関連して情報を推論できるようになることに注意すべきである。実際、２つのメッセージ１３及び１５を介して、上記のように乱数値を暗号化形式で交換することは、パスワードの秘密の侵入を許し得る情報冗長性を提供する。更に正確には、盗聴の度に、攻撃者は、メッセージ１３及び１５において交換された情報を復号するためのパスワードをテストできる。次に、２つのケースが攻撃者に対して現れる。第１のケースにおいて、復号された情報は、曲線の点に対応し、従ってパスワードは、正しい。第２のケースにおいて、復号された情報は、楕円曲線の点に対応せず、パスワードは、発見されない。盗聴及び別個のパスワードを繰り返すと、攻撃者にとり、要素の有限集合に属するパスワードを見出すことがこのようにして可能になる。

【発明の概要】

【発明が解決しようとする課題】

【００１１】

本発明は、状況を改善することを目的とする。

【課題を解決するための手段】

【００１２】

本発明の第１の態様は、装置（１０）もしくはコントローラ（１１）のいずれかとして定義される第１電子装置と、上記装置（１０）もしくは上記コントローラ（１１）のいずれか他方として定義される第２電子装置とを有し、パスワード（π）に基づく、コントローラ（１１）による装置（１０）の制御方法であって、次の：

／１／　上記第１電子装置が、

【数１】

$$E_{a,b}(x,y):x^3+ax+b=y^2$$

の有限体Ｆ$_{q}$（ｑは、整数である）において、乱数値ｒ$_{1}$に基づき、楕円曲線の点Ｐ$_{1}$（Ｘ，Ｙ）を決定するステップと、

／２／　前記第１電子装置が、

【数４５】

$$P(X,Y)=F(k,k')$$

（式中、Ｆは、Ｆ$_{q}$におけるＦ$_{q}$×Ｆ$_{q}$の全射関数である）であるような、第１及び第２パラメータｋ$_{1}$及びｋ$_{1}$’を求めるステップと、

／３／　前記第１電子装置が、前記第１及び第２パラメータｋ$_{1}$及びｋ$_{1}$’およびパスワード（π）を用いて、暗号化された第１、第２パラメータを求めるステップと、

／４／　前記第１電子装置が、暗号化された前記第１及び第２パラメータを前記第２電子装置へと伝送するステップとを含み、

対照的に、前記第２電子装置が、前記ステップ／１／と同様、乱数値ｒ$_{2}$に基づいて楕円曲線の点Ｐ$_{2}$（Ｘ，Ｙ）を決定し、前記ステップ／２／と同様、第１及び第２パラメータｋ$_{2}$及びｋ$_{2}$’を求め、前記ステップ／３／と同様、暗号化された第１、第２パラメータを求め、前記ステップ／４／と同様、暗号化された前記第１及び第２パラメータを前記第１電子装置へと伝送するステップとを含み、

前記関数Ｆは、Ｆ$_{q}$の入力要素ｚ及びｚ’がいかなるものであれ、Ｆ（ｚ，ｚ’）が楕円曲線の点であり、前記入力要素が式（１）を満たさないようになっている。

【００１３】

この措置のために、先行技術に対して、以上に記載したような攻撃を回避することが可能である。実際、これらの条件において、入力で供給されたパラメータが、いかなるものであれ、関数Ｆが、出力で楕円曲線の点を常に提供し、入力パラメータが、楕円曲線の古典的な式を満たさないので、求めた結果が、楕円曲線Ｅ$_{a,b}$の点（Ｘ，Ｙ）に対応するか決定して、パスワードをテストすることは、もはや可能でない。従って巧妙に、潜在的な攻撃者に、使用されるパスワードを推論できるようにし得るいかなる情報も提供しないように、この全射関数Ｆを使用して、楕円曲線の点を異なった方法で示すことが予想される。

【００１４】

（数１）と異なるパラメータ化による楕円曲線の点Ｐ（Ｘ，Ｙ）を示すことを可能にするかかる関数Ｆを決定するために、逆関数ｆ$_{a,b}^{-1}$が、入力パラメータから、（数１）を満たさない２つのパラメータにより曲線の点を回復することを可能にする、逆関数ｆ$_{a,b}$によることも可能である。

【００１５】

関数Ｆは：

【数８】

$$F(k,k')=f'(k')+f_{a,b}(k)$$

（式中、ｆ$_{a,b}$は、入力パラメータを取り、かつ楕円曲線の点を提供する、楕円曲線の係数ａ及びｂに基づく逆関数であり、ｆ’は、パラメータに応じて楕円曲線の点を発生させる関数である）

と書き表すことができ、ステップ／２／で、次の：

－　パラメータｋ’の値をランダムに発生させるステップと、

－　ｆ’（ｋ’）の値を計算するステップと、

－　次式：

【数９】

$$k = f_{a,b}^{-1}(P(X,Y) - f'(k'))$$

によりパラメータｋの値を決定するステップとにより、パラメータｋ及びｋ’を求める。

【００１６】

好適には、乱数値のパラメータｋ’に基づき、楕円曲線の点を発生させ得る関数ｆ’と、可逆的な、楕円曲線の係数ａ及びｂに基づく関数ｆ$_{a,b}$とを組み合わせると、記載した攻撃を回避しながら、曲線の点をパラメータ化できるようにする関数Ｆを求めることができる。

【００１７】

特に関数ｆ’は：

【数１０】

$$f'(k') = k'.G$$

（式中、Ｇは、楕円曲線の点の集合の生成元である）

と書き表すことができ、パラメータｋの値は、次式：

【数１１】

$$k = f_{a,b}^{-1}(P(X,Y) - k'.G)$$

により決定される。

【００１８】

これらの条件において、関数Ｆは、次の：

【数１２】

$$F(k,k') = f_{a,b}(k) + k'.G$$

ように書き表せる。

【００１９】

あるいは、関数ｆ’は：

【数１３】

$$f'(k') = f_{a,b}(k')$$

のように書き表せ、

パラメータｋの値は、次式：

【数１４】

$$k = f_{a,b}^{-1}(P(X,Y) - f_{a,b}(k'))$$

により決定される。

【００２０】

これらの条件において、関数Ｆは、次の：

【数１５】

$$F(k,k') = f_{a,b}(k) + f_{a,b}(k')$$

ように書き表せる。

【００２１】

このように、一般的に本発明による曲線の点Ｐ（Ｘ，Ｙ）をパラメータ化するために、第１ステップで、パラメータｋ’の値のための曲線の点を求めることが予想される。次に、表すべき点Ｐ（Ｘ，Ｙ）及び第１ステップで求めた点の減算に対応する曲線の点を決定する。そこで、楕円曲線の別の点を求める。次いで、この点に対して、ｆ$_{a,b}$の逆関数を適用し、パラメータｋの値を求める。点Ｐは、そこで（数１）を満たさないパラメータｋ及びｋ’の対の形式で示される。

【００２２】
本発明の実施態様において、関数Ｆは、
【数１６】

$$\forall P=(X,Y)\in E_{a,b},\left|f_{a,b}^{-1}(X,Y)\right|<L$$

（式中、Ｌは、楕円曲線（数１）の点の数に対して比較的小さい値を有する整数である）のような少なくとも１つの逆関数ｆ$_{a,b}$を含む。
【００２３】
関数Ｆが、関数ｆ$_{a,b}$を含むこととは、関数Ｆを第１及び第２パラメータに適用することが、この関数ｆ$_{a,b}$を第１及び第２パラメータの少なくとも１つに適用することに対応することを意味する。このようにして一方で、第１パラメータに基づき曲線の点を発生させること、及び他方で第２パラメータを求めるために、ｆ$_{a,b}$の逆関数を適用することを予想できる。このように実行しながら、これら２つのパラメータにより楕円曲線の点を示すことができる。
【００２４】
このようにして、関数Ｆを第１及び第２パラメータに適用することは、
【数１７】

$$\forall P(X,Y)\in E_{a,b},\left|f_{a,b}^{-1}(X,Y)\right|<L$$

（式中、Ｌは、楕円曲線（数１）の点の数に対して比較的小さい値を有する整数である）のような関数ｆ$_{a,b}$の２つのパラメータの少なくとも１つに適用することに対応し得る。
【００２５】
換言すると、本明細書で考慮される関数ｆ$_{a,b}$は、楕円曲線の点の数に対して著しく小さい最大値によって抑えられる楕円曲線Ｅ$_{a,b}$の点Ｐの集合に対応する原像を有する。実際、これが当てはまらない場合、単純に、ある数をランダムに引き出して、関数ｆ$_{a,b}$を逆にすることが可能である。この状況において、例えばＬが、曲線の点の数の１／2^{80}倍よりも小さいと考えることができる。
【００２６】
条件（数１７）を満たす逆関数を使用して、上記のように暗号化するために使用されるパスワードの攻撃を可能にしない、パラメータｋ及びｋ’を介して曲線上の点を示すことを可能にする関数Ｆを容易に求めることができる。
【００２７】
本発明の実施態様において、関数ｆ$_{a,b}$は、ｘが次式：
【数１８】

$$x^3+ax+b-(ux+Q(u,a,b))^2=0$$

の唯一の解であり、：
【数１９】

$$y=u.x+Q(u,a,b)$$

を満たすように、パラメータｕに、パラメータ対（ｘ，ｙ）を対応させる。
【００２８】
この（数１８）は、（数１）中のｙを項ｕｘ＋Ｑ（ｕ，ａ，ｂ）によって置換して求められる。項Ｑ（ｕ，ａ，ｂ）は、変数ｕ、ａ及びｂの有理分数を指す。
【００２９】
この（数１８）が、唯一の根しか認めないことは、パラメータｕがいかなるものであれ、次項の表された判別式Δ（ｕ，ａ，ｂ）が、２乗でないことを意味する：

【数２０】

$$x^3+ax+b-(ux+Q(u,a,b))^2$$

【００３０】

ｑ＝２　ｍｏｄ　３に関して：

【数２１】

$$\Delta(u,a,b)=-3R(u,a,b)^2$$

（式中、Ｒは、有理分数である）と書き表せる。

【００３１】

実際、ｐ＝２　ｍｏｄ　３に関して、－３は、２乗でなく、従って－３Ｒ（ｕ，ａ，ｂ）^{2}は、決して２乗の項ではない。

【００３２】

（数１８）が、唯一の根しか認めないので、次項は、１次の多項式である：

【数２２】

$$\gcd(x^3+ax+b-(ux+Q(u,a,b))^2, X^P-X)$$

（式中、ｇｃｄは、最大公約数である）。

【００３３】

X_Pと表されるこの多項式の根は、楕円曲線上の点の横座標である。最後に、横座標X_P及び縦座標ｕ．X_P＋Ｑ（ｕ，ａ，ｂ）の点は、曲線上の点である。

【００３４】

実施例において、次式：

【数２３】

$$Q(u,a,b)=\frac{236196u^2ab+405u^8a-20412u^6b-45927u^4a^2-u^{12}+19683a^3}{54u(-162au^4+2187a^2-u^8+2916bu^2)}$$

を満たす有理分数Ｑ（ｕ，ａ，ｂ）を考慮できる。

【００３５】

実施態様において、関数$f_{a,b}$は、好適にはF_q（ｑは、２　ｍｏｄ　３に等しい）において以下のように定義できる。関数$f_{a,b}$は：

【数２４】

$$x=(v^2-b-u^6/27)^{1/3}+u^2/3$$

かつ

【数２５】

$$y=u.x+v$$

（式中、

【数２６】

$$v=\frac{3a-u^4}{6u}=Q(u,a,b)$$

かつ$f_{a,b}(0)=0$）

であるように、パラメータｕに、パラメータ対（ｘ，ｙ）を対応させる。

【００３６】

かかる関数は、可逆である。実際、楕円曲線のＰ（Ｘ，Ｙ）とすると、関数$f_{a,b}$による点の原像は、次式：

【数２７】

$$u^4 - 6u^2x + 6uy - 3a = 0$$

の解である。

【００３７】

しかるに、かかる多項式は、容易に逆にできる。

【００３８】

更に、この関数$f_{a,b}$の原像の点Ｐの集合は、楕円曲線の点の数の前では小さいＬによって抑えられる。

【００３９】

このようにして、この関数は、以上に定義した特性を満たす。

【００４０】

関数Ｆの基礎を、スカルバ（Ｓｋａｌｂａ）の式を満たす多項式から定義される関数$f_{a,b}$の使用に置くことも予想できる。

【００４１】

スカルバの等式を満たす多項式が、２００７年６月１１日に出版されたＭａｃｉｅｊ Ｕｌａｓの文献「Ｒａｔｉｏｎａｌ ｐｏｉｎｔｓ ｏｎ ｃｅｒｔａｉｎ ｈｙｐｅｒｌｌｉｐｔｉｃ ｃｕｒｖｅｓ ｏｖｅｒ ｆｉｎｉｔｅ ｆｉｅｌｄｓ」において定義されることに注意すべきである。これらの関数は、可逆である。実際、多項式X_1（ｋ）、X_2（ｋ）、X_3（ｋ）、及びＵ（ｋ）がスカルバの等式を満たすので、すなわち：

【数２８】

$$f(X_1(k)).f(X_2(k)).f(X_3(k)) = U(k)^2$$

（式中、ｆは、楕円曲線$E_{a,b}$を定義する多項式である）

を満たすので。

【００４２】

更に正確には、ｆは、式：

【数２９】

$$f(x) = y^2$$

（式中、ｘ及びｙは、$F_q{}^2$の要素であり、対（ｘ，ｙ）は、$E_{a,b}$の点を示す）

を満たす。

【００４３】

$f_{a,b}$（ｋ）は、点Ｐ＝（X_i（ｋ），ｆ（X_i（ｋ））$^{1/2}$）（式中、ｉは、ｆ（X_i（ｋ））がF_qにおいて２乗であるようになっている）として定義される。従って、この関数$f_{a,b}$を逆にするために、点Ｐ＝（Ｘ，Ｙ）なので、３つの多項式：

【数３０】

$$X_1(k_s) - X = 0$$

$$X_2(k_s) - X = 0$$

$$X_3(k_s) - X = 0$$

の解k_sを計算する。

【００４４】

これらの解の各々は、$f_{a,b}$によるＰの原像である。

【００４５】

Ｆ（ｋ，ｋ’）が：

【数３１】

$$F(k,k') = f_{a,b}(k) + f_{a,b}(k')$$

と書き表される場合。

【００４６】

好適には、入力値の一様分布に関して、ｆ$_{a,b}$の出力値の点の一様分布を求められる。この場合に、入力値が、ランダムに決定されるならば、出力値は、ランダム分布を同様に示す。

【００４７】

このように実行しながら、情報を提供し得る、使用されるパラメータの値の統計的研究に基づく攻撃を回避できる。実際、楕円曲線の点Ｐ上のこの関数ｆ$_{a,b}$の逆数が、この逆関数の入力パラメータの複数の値に対応する場合、統計的法則によりこれらの値の幾つかが、他の値よりも頻繁に再び現れることが可能である。従って、攻撃者が、交換された情報に対してパスワードをテストして、この統計的法則を知っているならば、交換されたパラメータの値が、この法則に従っているか否かを決定できる。それにより攻撃者は、テストされたパスワードが、正しいか否かをこのように推論できる。

【００４８】

このタイプの攻撃を回避するために、以下に記載するようなアルゴリズムを利用することが好適であり得る。

【００４９】

Ｄ$_{i}$を、関数ｆ$_{a,b}$による原像数ｉを正確に有する楕円曲線Ｅ$_{a,b}$の点の集合と仮定する。以下に記載する実施例において、５つの集合Ｄ$_{1}$、Ｄ$_{2}$、Ｄ$_{3}$、Ｄ$_{4}$及びＤ$_{5}$を定義する。

【００５０】

楕円曲線の点をランダムに、一様分布させて発生させる関数のＧＥＮに注目する。

【数３２】

$$\text{Let } \delta_i = \frac{i}{L}$$

を、集合Ｄ$_{1}$に関連した確率とする。

【００５１】

ｔ＝０からＴ－１（式中、Ｔは、整数である）に関して、

－　関数ＧＥＮにより点Ｐ$_{t}$を発生させる、

－　Ｐ$_{t}$が、Ｄ０の要素ならば、最初に行く、

－　Ｐ$_{t}$が、Ｄｉの要素ならば、

○　０～１に含まれ、かつ

【数３３】

$$\Pr(b = 0) = \delta_i$$

を満たす値ｂをランダムに選択する、

○　ｂが１に等しいならば、ステップ（１）に行く、

○　そうでない場合、

－　集合

【数３４】

$$f_{a,b}^{-1}(P_t)$$

中で、要素ｕをランダムに選択する、

－　ｕ戻す。

【００５２】

成功確率１－１／２^{k}を求めるために、ｋで算定される１次の多項式に等しいＴ、換言

すればｋの倍数のＴを有すれば、十分であることに注目すべきである。
【００５３】
次の：
－　第１及び第２パラメータを暗号化形式で、パスワードによって示すメッセージを受信するステップと、
－　第１及び第２パラメータを復号し、パラメータｐ及びｐ’を求めるステップと、
－　次式：
【数３５】

$$K = r_1.F(p,p')$$

（式中、r_1は、ステップ／１／で使用される乱数値である）によりコントローラによって共通の秘密の値Ｋを計算するステップとを更に利用できる。
【００５４】
従って、装置及びコントローラは、パスワードの秘密を危険な状態に置く情報を交換せずに、最終的に共通鍵を持つことができる。
【００５５】
本発明の第２の態様は、本発明の第１の態様による制御方法を利用するために適した手段を含む電子装置を提案する。
【００５６】
本発明の第３の態様は、コントローラとして第２の態様による第１電子装置と、制御する装置として第２の態様による第２電子装置とを少なくとも含む、パスワードによる制御システムを提案する。
【００５７】
本発明の他の態様、目的及び利点は、実施態様の１つの記載を読めば、現れるであろう。
【００５８】
本発明は同様に、図を用いてより良く理解されるであろう。
【図面の簡単な説明】
【００５９】
【図１】すでに記載した、先行技術による制御方法の主要なステップを示す図である。
【図２】本発明の実施態様による制御方法の主要なステップを示す図である。
【図３】本発明の実施態様による装置と、コントローラとの間の制御方法の利用を示す図である。
【図４】本発明の実施態様による装置及びコントローラを示す図である。
【発明を実施するための形態】
【００６０】
図２は、本発明の実施態様による制御方法の主要なステップを示す。
【００６１】
ステップ２１で、有限体F_q（ｑは、整数である）において、乱数値r_1に基づき楕円曲線の点Ｐ＝（Ｘ，Ｙ）を決定する。次に、ステップ２２で、
【数７】

$$P=F(k,k')$$

（式中、Ｆは、F_qにおける$F_q \times F_q$のような全射関数である）
であるような第１及び第２パラメータｋ及びｋ’を求める。
【００６２】
このようにして求めたパラメータにより、装置と、コントローラとの間の交換中に、パスワードの秘密を保護するように、点Ｐを巧妙に示せるようになる。
【００６３】
ステップ２３で、パスワードπ　E_π（ｋ，ｋ’）に応じた暗号化による暗号化形式で

第１及び第２パラメータを求める。
【００６４】
この巧妙な形式で、秘密の共通鍵を発生させるように、乱数値r_1が、ステップ２４で、制御する装置からコントローラに、コントローラから制御する装置にそれぞれ好適には伝送できる。
【００６５】
関数Ｆは、F_qの要素ｚ及びｚ’がいかなるものであれ、Ｆ（ｚ，ｚ’）が楕円曲線の点であり、要素ｚ及びｚ’が（数１）を満たさないようになっている。
【００６６】
図３は、本発明の実施態様による制御する装置１０と、コントローラ１１との間のメッセージ交換を示す。
【００６７】
制御する装置Ｄ１０は、最初にステップ３１で、乱数値r_1を発生させる。楕円曲線の点の集合の次数が、整数Ｎである時、r_1は、値の集合：［０，Ｎ－１］によって任意に取ることができる。
【００６８】
次に、この乱数値から、生成元Ｇを使用して、楕円曲線$E_{a,b}$の点Ｐ＝（Ｘ，Ｙ）を発生させる。かかる生成元は、楕円曲線のいかなる点Ｐに関しても：
【数３６】

$$P=h.G$$

のような値ｈが存在するようになっている。
【００６９】
従って：
【数３７】

$$P_1=r_1.G$$

のような点P_1を求める。
【００７０】
次にステップ３３で、式（２）を満たす、そのＸ及びＹ座標と異なるパラメータにより点P_1を示すために、パラメータk_1及びk_1’の値を決定する。
【００７１】
これらのパラメータk_1及びk_1’を決定するために、最初にパラメータの乱数値k_1’を発生させることができる。次に曲線の点のｘ、ｙ座標のパラメータに対応させる関数$f_{a,b}$を適用するか、楕円曲線の点の生成元Ｇを使用して、この乱数値k_1’に、楕円曲線の点P_{k1}が対応する。
【００７２】
次に、$f_{a,b}$の逆適用を、楕円曲線の点の群における減算：Ｐ（Ｘ，Ｙ）－P_{k1}に対応する点に適用して、パラメータk_1の値を求める。
【００７３】
パラメータk_1及びk_1’は、点Ｐ（Ｘ，Ｙ）を示す。次に、パスワードπに基づく暗号化関数E_πによって、以上で求めた第１及び第２パラメータを暗号化し、メッセージ３４を介してコントローラに伝送する。
【００７４】
対称的に、コントローラは、ステップ３５で乱数値r_2を発生させる。次に、ステップ３６でこの値を楕円曲線の点P_2に変換する。次いで、以前にステップ３３で記載したように、コントローラは、ステップ３７で第１及び第２パラメータk_2及びk_2’のそれぞれの値を求める。次に、コントローラは、メッセージ３８を介してこれらの値を制御する装置１０に伝送する前に、これらの値を暗号化する。
【００７５】

従って、制御する装置１０は、乱数値r_1と、値k_2及びk_2’と、関数Ｆとを持つ。
【００７６】
従ってステップ３９で、装置は、点P_2：
【数３８】

$$P_2=F(k_2,k'_2)$$

を回復する。
【００７７】
従って、装置は、コントローラと共有される秘密鍵Ｋを求めるが、それにもかかわらず
【数６】

$$K = r_1.r_2.G$$

を満たすパスワードに関する何らかの情報を提供することはない。
【００７８】
コントローラは、対称的にステップ３０１で秘密鍵Ｋを回復する。
【００７９】
以上に定義したような関数Ｆは、異なる形式で書き表せる。以下の部分で、乱数値の暗号化された交換の際に、好適には情報冗長性を提供しないことを可能にする、この点Ｐの異なる表示を記載する。
【００８０】
関数Ｆは：
【数７】

$$P=F(k,k')$$

であるような、かつ（数１）がｋ及びｋ’によって満たされることなく、あらゆる値の対（ｋ，ｋ’）に関して、Ｐが楕円曲線の点であるような、F_qにおける$F_q \times F_q$の全射である。
【００８１】
かかる状況において、好適にはいかなる情報も、先行技術とは反対に、交換される乱数値の交換に基づいて、パスワードに関して推論され得ない。実際、値の対（ｋ，ｋ’）は、その場合装置と、コントローラとの間で暗号化されて交換される。しかし、この値の対を回復するために、攻撃者となり得る者によって試みられるパスワードがいかなるものであれ、（数１）がｋ及びｋ’によって満たされることなく、求められたあらゆる結果が楕円曲線上の点に対応するので、このパスワードが、正しいか否かを決定することは、不可能である。
【００８２】
かかる表示は、次の特性：
【数３９】

$$\forall P \in E_{a,b}, \left| f_{a,b}^{-1}(P) \right| < L$$

（式中、Ｌは、整数である）
を示す関数$f_{a,b}$（Ｕ）の好適な特性に基づくことができる。
【００８３】
換言すると、この関数の原像の集合の大きさは、楕円曲線の点の数の前では小さい数Ｌによって抑えられる。
【００８４】
次の関数$f_{a,b}$（Ｕ）を考慮すると、$f_{a,b}$（０）＝０と仮定して：

【数４０】

$$x=(v^2-b-u^6/27)^{1/3}+u^2/3$$

かつ

【数４１】

$$v=\frac{3a-u^4}{6u}$$

のように、$F_q{}^2$におけるパラメータ対（ｘ，ｕ．ｘ＋ｖ）をF_qにおけるパラメータｕに対応させる、本発明の実施態様による関数Ｆを好適には決定できる。

【００８５】

この場合、関数Ｆは：

【数４２】

$$F(k,k')=f_{a,b}(k)+f_{a,b}(k')$$

又は

【数４３】

$$F(k,k')=f_{a,b}(k)+k'.G$$

と書き表せる。

【００８６】

$f_{a,b}$が、スカルバの等式：

【数２８】

$$f(X_1(k)).f(X_2(k)).f(X_3(k))=U(k)^2$$

（式中、X_1（ｋ）、X_2（ｋ）、X_3（ｋ）、及びＵ（ｋ）は、例えば、２００７年６月１１日に出版されたＭａｃｉｅｊ　Ｕｌａｓの文献「Ｒａｔｉｏｎａｌ　ｐｏｉｎｔｓ　ｏｎ　ｃｅｒｔａｉｎ　ｈｙｐｅｒｌｌｉｐｔｉｃ　ｃｕｒｖｅｓ　ｏｖｅｒ　ｆｉｎｉｔｅ　ｆｉｅｌｄｓ」において定義されたようなスカルバの等式を満たす多項式である）

を満たす多項式から生じた関数であることも考慮できる。

ここで$f_{a,b}$（ｋ）は、（X_i（ｋ），ｆ（X_i（ｋ））$^{1/2}$）（式中、ｉは、ｆ（X_i（ｋ））がF_qにおいて２乗であるようになっている）として定義される。

【００８７】

図４は、本発明の実施態様による制御する装置と、コントローラとを含む制御システムを示す。

【００８８】

かかる制御システムは、制御する装置１０として電子装置と、本発明の実施態様による制御構成要素又はコントローラ１１とを少なくとも含む。かかる電子装置は、制御する装置として、又はコントローラとして使用されるとしても：

－　有限体F_q（ｑは、整数である）において、乱数値r_1に基づき、楕円曲線の点Ｐ（Ｘ，Ｙ）を決定することに適しており、楕円曲線が、

【数１】

$$E_{a,b}(x,y):x^3+ax+b=y^2$$

を満たす、決定装置４１と、

【数７】

$$P=F(k,k')$$

（式中、Ｆは、F_qにおける$F_q \times F_q$の全射関数である）
であるような、第１及び第２パラメータｋ及びｋ’を求めることに適した取得装置４２と、
－　パスワードに応じた暗号化による暗号化形式で第１及び第２パラメータを求めることに適した暗号化装置４３と、
－　暗号化された前記第１及び第２パラメータをコントローラに伝送することに適したインタフェース装置４４とを含むことができ、
関数Ｆは、F_qの入力要素ｚ及びｚ’がいかなるものであれ、Ｆ（ｚ，ｚ’）が楕円曲線の点であり、入力要素が（数１）を満たさないようになっている。

【００８９】

パスワードE_πによる暗号化関数は、異なる方法で定義できる。暗号化関数は、入力パラメータでビット列を取り、出力でビット列を戻す。それにもかかわらず、パスワードの機密性を保証するために、戻された値が、パスワードに関する情報を与えないことが必要である。従って、２つのケース：
－　パスワードが、古典的な暗号化関数の暗号化鍵として使用されるケースか、
－　パスワードが、データベースにおいて楕円曲線のパブリックパラメータの値を示す指数であるケースを区別できる。両方のケースにおいて、暗号化アルゴリズムは、以下のように展開でき、パラメータの値ｋ又はｋ’をビット列に変換するために、次の方法を適用できる：

【００９０】

乱数値ｒを選択する。次に：

【数４４】

$$v' = v + r.q'$$

（式中、ｑ’は、ｑか、Ｎに対応し、ｑは、基礎体F_qの要素数であり、Ｎは、楕円曲線の点の数である）
を計算して、パラメータの値ｖをビット列に変化する。次いでビット列によりｖ’を示すことができる。

パスワードπが指数である場合に、パブリックパラメータ（ｑ又はＮ）を知る唯一の人が、ｖの値を見出せるので、ｖ’は、パスワードの形式でｖの暗号化された値である。

【００９１】

パスワードが、古典的な暗号化関数の暗号化鍵として使用される場合、暗号化関数E_πを使用して、ｖ’を暗号化すれば十分である。

【００９２】

このように受信面では、第１のケースにおいて、ｖ’ ｍｏｄ ｑ’を計算してｖを回復できる。第２のケースにおいて、ｖ’を見出し、最後にｖ’ ｍｏｄ Ｎを計算してｖを計算し得るために、復号関数によって送信されたビット列を復号せねばならない。

【００９３】

本発明は、好適には楕円曲線を使用するあらゆるタイプの暗号計算において利用できる。特に本発明は、好適にはＰＡＣＥ（英語で「Ｐａｓｓｗｏｒｄ Ａｕｔｈｅｎｔｉｃａｔｅｄ Ｃｏｎｎｅｃｔｉｏｎ Ｅｓｔａｂｌｉｓｈｍｅｎｔ（パスワード認証された接続確立）」）のような、パスワードによる認証プロトコル中にあり得る。この場合に本発明は、暗号計算の実行時間に関連したいかなる攻撃も許さずに、計算性能の改善を可能にする。

【００９４】

本発明は、好適には、電子パスポートのような、電子識別文書の検査のために使用されるような、私生活を尊重するプロトコルの状況でも適用できる。実際、先行技術とは反対に、提示されたプロトコルを盗聴しても、使用される楕円曲線のパブリックパラメータを見出せない。

【図１】

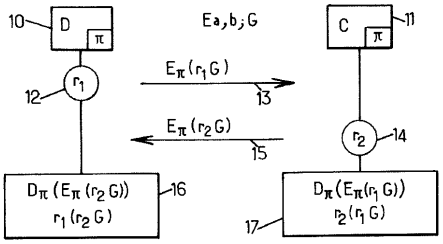


FIG.1.

【図２】

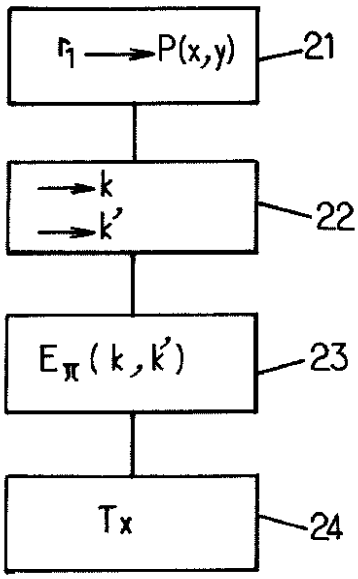


FIG.2.

【図３】

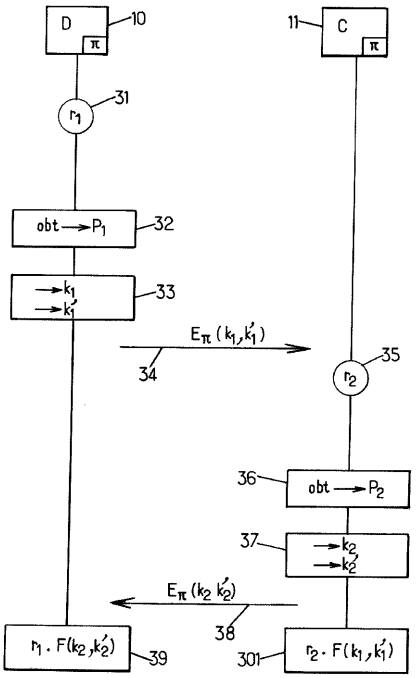
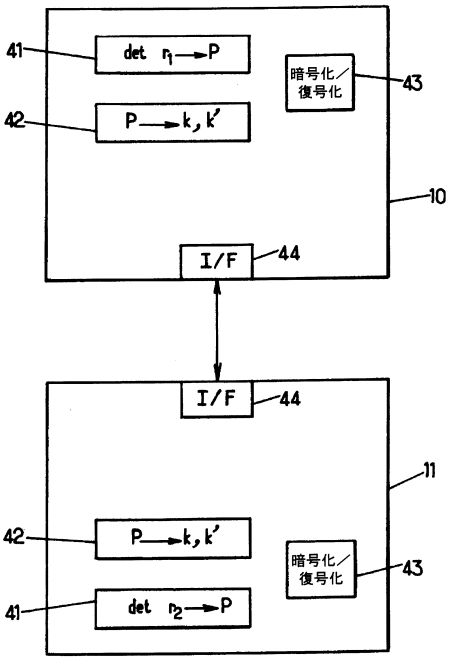


FIG.3.

【図４】



フロントページの続き

審査官　青木　重徳

(56)参考文献　特開２０１０－１６４７９６（ＪＰ，Ａ）
米国特許第０７０６２０４４（ＵＳ，Ｂ１）
米国特許第０６２１２２７９（ＵＳ，Ｂ１）
米国特許出願公開第２００３／０２３５３００（ＵＳ，Ａ１）
国際公開第２０１０／０８１９８０（WO，Ａ１）
Maciej Ulas, “Rational points on certain hyperelliptic curves over finite fields”, arXiv.org > math > arXiv:0706.1448, [online], ２００７年　６月１１日, arXiv:0706.1448v1, p.1-9, [retrieved on 2014-05-13]. Retrieved from the Internet, ＵＲＬ, <http://arxiv.org/pdf/0706.1448v1.pdf>
Eric Brier, Jean-Sebastien Coron, Thomas Icart, David Madore, Hugues Randriam, and Mehdi Tibouchi, “Efficient Indifferentiable Hashing into Ordinary Elliptic Curves”, Cryptology ePrint Archive: Report 2009/340, [online], ２００９年　７月１３日, Version: 20090713:020919, [retrieved on 2013-12-13]. Retrieved from the Internet, ＵＲＬ, <eprint.iacr.org/eprint-bin/getfile.pl?entry=2009/340&version=20090713:020919&file=340.pdf>
Thomas Icart, “How to Hash into Elliptic Curves”, Cryptology ePrint Archive: Report 2009/226, [online], ２００９年　５月３０日, Version: 20090530:041605, [retrieved on 2013-12-13]. Retrieved from the Internet, ＵＲＬ, <https://eprint.iacr.org/2009/226.pdf>

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０９Ｃ　　１／００