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

特許第4598269号
(P4598269)

(45)発行日　平成22年12月15日(2010.12.15)　(24)登録日　平成22年10月1日(2010.10.1)

(51)Int.Cl.			F I		
G09C	1/00	(2006.01)	G09C	1/00	650Z
H04L	9/32	(2006.01)	G09C	1/00	620A
G06F	7/72	(2006.01)	G09C	1/00	620Z
			H04L	9/00	675B
			G06F	7/72	

請求項の数 18　(全 20 頁)

(21)出願番号　特願2000-538291 (P2000-538291)
(86)(22)出願日　平成11年3月25日 (1999.3.25)
(65)公表番号　特表2002-508523 (P2002-508523A)
(43)公表日　平成14年3月19日 (2002.3.19)
(86)国際出願番号　PCT/CA1999/000254
(87)国際公開番号　WO1999/049386
(87)国際公開日　平成11年9月30日 (1999.9.30)
審査請求日　平成18年3月24日 (2006.3.24)
(31)優先権主張番号　09/047,518
(32)優先日　平成10年3月25日 (1998.3.25)
(33)優先権主張国　米国(US)

(73)特許権者　397071791
サーティコム　コーポレーション
カナダ国　オンタリオ　エル４ダブリュー　５エル１，ミシソーガ，エクスプローラー・ドライブ　５５２０，フォース・フロア
(74)代理人　100107489
弁理士　大塩　竹志
(74)代理人　100113701
弁理士　木島　隆一
(74)代理人　100115026
弁理士　圓谷　徹
(74)代理人　100116241
弁理士　金子　一郎

最終頁に続く

(54)【発明の名称】楕円曲線上の高速有限体演算

(57)【特許請求の範囲】

【請求項１】

楕円曲線暗号システムの暗号モジュールを動作させることにより、公開鍵を生成する方法であって、該モジュールは、メモリと、楕円曲線の計算を実行するプロセッサとを含み、該メモリは、該楕円曲線暗号システムによって用いられる楕円曲線のパラメータを格納し、該楕円曲線上にある座標（x_1，y_1）を有する点Ｐを格納し、

該方法は、

ａ）該プロセッサを用いて点Ｐの射影Ｘ座標および射影Ｚ座標を計算するステップと、

ｂ）該プロセッサにおいて、Ｐの射影Ｘ座標および射影Ｚ座標を利用することにより、

ｉ）ｋＰの射影Ｘ座標X_2および射影Ｚ座標Z_2の値と、

ｉｉ）（ｋ＋１）Ｐの射影Ｘ座標X_3および射影Ｚ座標Z_3の値と

を取得するステップと、

ｃ）X_2およびZ_2の値を組み合わせることにより、ｋＰのｘアフィン座標x_2を導出するステップと、

ｄ）該点Ｐの座標と該導出されたx_2の値と（ｋ＋１）Ｐの射影座標X_3、Z_3とを組み合わせることにより、該点ｋＰのアフィンｙ座標y_2の値を取得するステップと、

ｅ）該暗号モジュールによって実行される暗号動作において、ｋＰの座標（x_2、y_2）を利用するステップと

を含む、方法。

【請求項２】

前記楕円曲線暗号システムは、標数が２の体にわたって定義されている、請求項１に記載の方法。

【請求項３】

ｋＰのアフィンｙ座標の決定は、$x_1 Z_3$の逆数を用いて実行される、請求項２に記載の方法。

【請求項４】

ｋＰのアフィンｙ座標の決定は、以下の式

【数１】

$$y_2 = (x_1 + x_2)\left(\frac{1}{x_1 Z_3}(X_3(x_1 + x_2) + Z_3 y_1) + x_2\right) + y_1$$

に従って実行される、請求項３に記載の方法。

【請求項５】

前記楕円曲線暗号システムは、標数が奇数の体にわたって定義されている、請求項１に記載の方法。

【請求項６】

ｋＰのアフィンｙ座標の決定は、Z_3の逆数を用いて実行される、請求項５に記載の方法。

【請求項７】

前記楕円曲線は、一対のパラメータａ、ｂに関連付けられており、ｋＰのアフィンｙ座標の決定は、以下の式

【数２】

$$y_2 = \frac{1}{2y_1}\left((x_1 + x_2)(a + x_1 x_2) + 2b - x_3(x_2 - x_1)^2\right).$$

に従って実行される、請求項６に記載の方法。

【請求項８】

ｋＰのアフィンｙ座標の決定は、$y_1 Z_3$の逆数を用いて実行される、請求項５に記載の方法。

【請求項９】

前記楕円曲線は、一対のパラメータａ、ｂに関連付けられており、ｋＰのアフィンｙ座標の決定は、以下の式

【数３】

$$y_2 = \frac{1}{2y_1 Z_3}\left(Z_3((x_1 + x_2)(a + x_1 x_2) + 2b) - X_3(x_2 - x_1)^2\right).$$

に従って実行される、請求項８に記載の方法。

【請求項１０】

暗号動作において用いられる公開鍵ｋＰを計算する暗号システムであって、該システムは、該暗号システムにおいて用いられる楕円曲線を定義するパラメータおよび点Ｐ＝（x_1，y_1）が格納されているメモリと、楕円曲線の計算を実行し、該メモリと通信する算術論理部とを含み、該算術演算部は、Ｐの射影Ｘ座標および射影Ｚ座標を取得するように構成されており、

該算術演算部は、

ａ）Ｐの射影Ｘ座標および射影Ｚ座標を利用することにより、

ｉ）ｋＰの射影Ｘ座標X_2および射影Ｚ座標Z_2の値と、

ｉｉ）（ｋ＋１）Ｐの射影Ｘ座標X_3および射影Ｚ座標Z_3との値と

を取得することと、

ｂ）X_2およびZ_2の値を組み合わせることにより、ｋＰのアフィン座標x_2を導出することと、

ｃ）該点Ｐの座標と該導出されたx_2の値と（ｋ＋１）Ｐの射影座標X_3、Z_3とを組み合わせることにより、該点ｋＰのアフィンｙ座標y_2の値を取得することと

によって、該公開鍵ｋＰを計算する、暗号システム。

【請求項１１】

前記楕円曲線は、標数が２の体にわたって定義されている、請求項１０に記載の暗号システム。

【請求項１２】

ｋＰのアフィンｙ座標の決定は、x_1 Z_3の逆数を用いて実行される、請求項１１に記載の暗号システム。

【請求項１３】

ｋＰのアフィンｙ座標の決定は、以下の式

【数４】

$$y_2 = (x_1 + x_2)\left(\frac{1}{x_1 Z_3}(X_3(x_1 + x_2) + Z_3 y_1) + x_2\right) + y_1$$

に従って実行される、請求項１２に記載の暗号システム。

【請求項１４】

前記楕円曲線暗号システムは、標数が奇数の体にわたって定義されている、請求項１０に記載の暗号システム。

【請求項１５】

ｋＰのアフィンｙ座標の決定は、前記Z_3の逆数を用いて実行される、請求項１４に記載の暗号システム。

【請求項１６】

前記楕円曲線は、一対のパラメータａ、ｂに関連付けられており、ｋＰのアフィンｙ座標の決定は、以下の式

【数５】

$$y_2 = \frac{1}{2y_1}\left((x_1 + x_2)(a + x_1 x_2) + 2b - x_3(x_2 - x_1)^2\right).$$

に従って実行される、請求項１２に記載の暗号システム。

【請求項１７】

ｋＰのアフィンｙ座標の決定は、y_1 Z_3の逆数を用いて実行される、請求項１４に記載の暗号システム。

【請求項１８】

前記楕円曲線は、一対のパラメータａ、ｂに関連付けられており、ｋＰのアフィンｙ座標の決定は、以下の式

【数６】

$$y_2 = \frac{1}{2y_1 Z_3}\left(Z_3((x_1 + x_2)(a + x_1 x_2) + 2b) - X_3(x_2 - x_1)^2\right)$$

に従って実行される、請求項１７に記載の暗号システム。

【発明の詳細な説明】

本発明は、有限体（finite field）上で演算を高速に行う方法に関連し、特に、暗号システムで使われる体（field ）$F_2{}^m$上で行われる演算に関連するものである。

【０００１】

〔発明の背景〕

ここでは、$F_2{}^m$ において標数が２の有限体を扱う。この有限体を用いれば楕円曲線に関する代数計算を効率よく実行できる。体$F_2{}^m$は、F_2上でのｍ次元ベクトル空間として見ることができる。F_2上における$F_2{}^m$の基底が一旦選択されると、$F_2{}^m$の元が、０と１との成分からなる長さｍのベクトルとして上手く表現できる。ハードウェアでは、長さｍのシフトレジスターに体の元が記録されている。体の元の加算は、ベクトル表現についてビットを用いてＸＯＲ演算（Θで表す）を実行することによって行う。この演算の所要時間は、クロック周期１つ分である。

【０００２】

ある所からメッセージが送信されたことと、その内容が通信中に改竄されていないこととを確認するためには、デジタル署名が使用される。

【０００３】

広く使用されている署名プロトコールセットの中には、送信者の個人キーを使ってメッセージに署名する、ＥＬＧａｍａｌ公開キー署名方式を使用するものがある。この方式では、受信者は、送信者の公開キーを使ってその署名を認証することができる。

【０００４】

こういった方式を実行するプロトコールには色々あって、広く使われているものがいくつか存在する。ただし、いずれの場合であっても、受信者側で計算を実行して署名を認証しなければならない点については同じである。受信者側に十分な計算能力があれば、計算の必要性は取りたてて問題にはならない。しかし「スマート・カード」を利用した機器のように、受信者側の計算能力に限界のある場合には、計算をしなければならないがために認証に時間がかかってしまうことがある。

【０００５】

公開キー方式は、対応しきれない程の離散的なログ問題のあるように見えるいくつかの群の１つを使って実行できるが、有限体において、楕円曲線上にある複数の点の特徴を使って実行すれば、特に目立った効果が得られる。つまり、こうすることで、例えば$Z_p{}^*$で実行することに比べ、比較的低い次数の体で必要な安全性を得られるといった効果が生まれる。したがって、署名をやり取りするための通信帯域を、小さくできる。

【０００６】

実行の際、一般に、署名部分ｓは、以下の式で表される。

ｓ＝ａｅ＋ｋ（ｍｏｄ　ｎ）

ここで、Ｐは、曲線上の点であり、前もって定義されたシステムのパラメタである。ｋは、短期個人キーあるいはセッションキーとして選択されたランダムな整数で、対応する短期公開キーＲ＝ｋＰを有している。ａは、送信者の長期個人キーで、相当する公開キーａＰ＝Ｑを有している。ｅは、メッセージｍと短期公開キーＲとの、ＳＨＡハッシュ関数などの安全なハッシュ（secure hash ）である。ｎは、曲線の次数である。

【０００７】

送信者は、受信者に対してｍ、ｓ、およびＲを含んだメッセージを送る。そして、その署名を、Ｒ’＝（ｓＰ－ｅＱ）の値を求めることによって認証する。この値Ｒ’は、Ｒに対応しているはずであり、計算で求めたＲ’がＲに等しければ、署名を本物であると認定できる。

【０００８】

この認証を行うためには、ｓＰとｅＱとを求めるために点について乗算を何度か行う必要があるが、どちらも計算は複雑である。

【０００９】

F_qが有限体であると仮定すれば、F_q上の楕円曲線はスーパーシンギュラー曲線と非スーパーシンギュラー曲線との２つの類に分けられる。また、F_qの標数を２、つまり$q=2^M$と仮定すれば、上記の類は以下のように定義される。

（１）方程式$y^2+ay=x^3+bx^2+c$（ただし、ａ，ｂ，$c\in F_q$、$a\neq 0$）の全ての解と、無限遠点と呼ばれる特別な点Ｏとで、F_q上でスーパーシンギュラー曲線を形成する。

（２）方程式$y^2 + xy = x^3 + ax^2 + b$（ただし、a，b∈$F_q$、b≠０）の全ての解と、無限遠点と呼ばれる特別な点Ｏとで、F_q上で非スーパーシンギュラー曲線を形成する。

【００１０】

これらの点について適当な加算を定義すれば、加算に関するアーベル群を得られる。$y^2 + ay = x^3 + bx^2 + c$で表されるスーパーシンギュラー楕円曲線Ｅについて、点Ｐ（x_1，y_1）と点Ｑ（x_1，y_1）との２点の加算は以下のようになる。

Ｐ（x_1，y_1）∈Ｅのとき、全てのＰ∈Ｅについて、－Ｐを、－Ｐ＝（x_1，$y_1 + a$），Ｐ＋Ｏ＝Ｏ＋Ｐ＝Ｐと定義する。

また、Ｑ＝（x_2，y_2）∈Ｅ　かつ　Ｑ≠－Ｐのとき、ＰとＱとの和を表す点を（x_3、y_3）と表記する。ここで、x_3は、

【００１１】

【数２】

$$x_3 = \begin{cases} \left(\dfrac{y_1 \Theta y_2}{x_1 \Theta x_2}\right)^2 \Theta x_1 \Theta x_2 & (P \neq Q) \end{cases}$$

あるいは、

$$x_3 = \begin{cases} \dfrac{x_1^4 \Theta b^2}{a^2} & (P = Q) \end{cases}$$

である。

また、y_3は、

$$y_3 = \begin{cases} \left(\dfrac{y_1 \Theta y_2}{x_1 \Theta x_2}\right) \Theta (x_1 \Theta x_3) \Theta y_1 \Theta a & (P \neq Q) \end{cases}$$

あるいは、

$$y_3 = \begin{cases} \left(\dfrac{x_1^2 \Theta b}{a}\right) \Theta (x_1 \Theta x_3) \Theta y_1 \Theta a & (P = Q) \end{cases}$$

である。

【００１２】

非スーパーシンギュラー楕円曲線である$y^2 + xy = x^3 + ax^2 + b$について、点Ｐ（$x_1$，$y_1$）と点Ｑ（$x_1$，$y_1$）との２点の加算は、以下のようになる。

【００１３】

Ｐ（x_1，y_1）∈Ｅのとき、全てのＰ∈Ｅ，Ｏ＋Ｐ＝Ｐ＋Ｏ＝Ｐについて、－Ｐを－Ｐ＝（x_1，$y_1 + x_1$）と定義する。

【００１４】

また、Ｑ＝（x_2，y_2）∈Ｅ　かつ　Ｑ≠－Ｐのとき、Ｐ＋Ｑは点（x_3、y_3）である。ここで、x_3は、

【００１５】

【数３】

$$x_3 = \begin{cases} \left(\dfrac{y_1 \Theta y_2}{x_1 \Theta x_2}\right)^2 \Theta \dfrac{y_1 \Theta y_2}{x_1 \Theta x_2} \Theta x_1 \Theta x_2 \Theta a & (P \neq Q) \end{cases}$$

あるいは、

$$x_3 = \begin{cases} x_1^2 \Theta \dfrac{b}{x_1^2} & (P = Q) \end{cases}$$

である。

また、ｙ３は、

$$y_3 = \begin{cases} \left(\dfrac{y_1 \Theta y_2}{x_1 \Theta x_2}\right) \Theta (x_1 \Theta x_3) \Theta x_3 \Theta y_1 & (P \neq Q) \end{cases}$$

あるいは、

$$y_3 = \begin{cases} x_1^2 \Theta \left(x_1 \Theta \dfrac{y_1}{x_1}\right) \Theta x_3 \Theta x_3 & (P = Q) \end{cases}$$

である。

【００１６】

ここでは、この２種類の楕円曲線のうち、スーパーシンギュラー曲線の方が、ＭＯＶアタックに対して強いため好ましい。Ｅ上の２点の和を計算するには、この２点が存在する下層の体（underlying field）F_{2^m} において乗算、加算、逆演算を行う必要のあることがわかる。さらに、これらの演算を実行するには、それぞれ基本的なビット演算を何度か実行する必要がある。

【００１７】

ＥｌＧａｍａｌあるいはＤｉｆｆｉｅ－Ｈｅｌｌｍａｎ方式で暗号演算を実行する際、あるいは、一般的に楕円曲線を用いて暗号演算を実行する際には、ｋＰ＝Ｐ＋Ｐ＋…＋Ｐ（ＰをｋＰ回加える。ただしｋは正の整数で、Ｐ∈Ｅ）を計算する必要があるが、そのためには（x_3、y_3）をｋ－１回計算しなければならない。暗号に応用するには一般にｋが大きな値を取ることが必要であるが、大きな値のｋをデータ通信に用いるのは実用的でないと今までは考えられてきた。ｋが大きな値、例えば１０２４ビットを取ると、ｋＰを計算するにはＰを2^{1024}回加えなければならない。

【００１８】

しかも、乗算に関する群では、乗算および逆演算の計算量が非常に大きくなり、体における乗算よりも、体における逆演算の方がコスト高となる。２点を加える際に射影座標を採用すれば、逆演算は不用になるが、加算を実行するために必要な乗算の回数は、擬似座標を用いるときに比べ多くなる。

【００１９】

バンストーンその他は、雑誌「暗号学」に掲載された論文、「楕円曲線を用いた暗号システムとその実行」（"Ellpitic Curve Cryptosystems and Their Implementation" by Van stone et al., published in The Journal of Cryptology）中で、射影座標に変換することによって逆演算を不要にして、２つの点を加える方法について記している。この方法では、逆演算をしないですむので全体の演算速度は上昇しているが、これは、装置のコンパクト性の犠牲の上に成り立っている。つまり、ＰとＱとを記録し、さらに加算を実行する際の中間結果を記録するために余分なレジスタが必要になるのである。しかも、この方法では計算中にｙ座標を使わなければならない。

【００２０】
〔発明の要旨〕
本発明は、上記のことを踏まえてなされ、以上で述べた欠点を克服、あるいは軽減する方法と装置とを提供することを目的の１つとしている。
【００２１】
また、本発明は、スマートカード等、演算能力の限られたプロセッサでも比較的に効率よく実行することの可能な、有限体の元について乗算を実行する方法を提供することも目的としている。
【００２２】
さらに本発明は、楕円曲線に基づいた暗号化方式において、署名の認証を高速化する方法と装置とを提供することも目的としている。
【００２３】
本発明では、体F_{2^m}上で定義される楕円曲線上の点Ｐの倍数を決定する方法を提供し、この方法は、数値ｋを、２値数k_iからなるベクトルとして表すステップと、差がＰを越えない１対の点である点P_1および点P_2を作るステップと、k_iをそれぞれ順に選択し、さらに、それぞれのk_iについて、k_iが１のときには、上記点P_1および点P_2の対を加えて新しい点P_1を形成し、点Ｐを点P_1に加えて新しい点P_2を形成して、これらの新しい２点で点P_1および点P_2の対を置き換え、また、k_iが０のときには、上記点P_1を２倍して新しい点P_1を形成し、上記点Ｐを加えて新しい点P_2を形成して、これらの新しい２点で点P_1および点P_2の対を置き換え、Ｍ－１回（ただし、Ｍはｋの桁数）の繰り返しで上記点P_1から積ｋＰを求めるステップを含んでいる。
【００２４】
さらに、本発明者は、計算中に点Ｐのｙ座標を用いないで積ｋＰの計算を実行できる方法に基づいて、実際に計算を行った。
【００２５】
以下の記述では、実施例を用いて本発明を説明する。ただし、本発明はこれらの実施例に限られるものではなく、実施例はあくまでも例にすぎない。
【００２６】
〔好ましい実施の形態の詳細な説明〕
図１を参照すると、データ通信システム２は、通信路１４を介して接続された送信側１０と受信側１２とからなる一対の通信部を有している。各通信部１０・１２は、それぞれに関連付けられた暗号化／解読部１６を有しており、暗号化／解読部１６は、以下に説明するように、デジタル情報を処理でき、通信路１４を介して送信されるように、デジタル情報を生成するものである。暗号化／解読部は、キー交換プロトコル、および暗号化／解読アルゴリズム等を実行するものである。
【００２７】
モジュール１６は、図２に概略的に示されており、キー交換およびキー生成などの演算を行うために、算術論理部２０を含んでいる。個人キーレジスタ２２は、ランダム数生成部２４から、例えば、１５５ビットのデータ列で生成される個人キーｄを含んでおり、公開キーレジスタ２６に記憶される公開キーを生成するために使用される。基準点レジスタ２８は、各座標（ｘ，ｙ）で選択された楕円曲線上に位置する、基準点Ｐの座標を含んでおり、（ｘ，ｙ）は、１５５ビットのデータ列で表される。各データ列は２値数のベクトルであり、２値数のそれぞれは、座標の正規基底表現における、有限体の元の係数である。
【００２８】
選択された楕円曲線は、$y^2 + xy = x^3 + ax^2 + b$の一般式で表され、該曲線のパラメタ、すなわち、係数ａおよびｂは、パラメタレジスタ３０に記憶される。レジスタ２２，２４，２６，２８，３０の内容は、必要に応じて、ＣＰＵ３２の制御下において算術部２０に転送されてもよい。
【００２９】
公開キーレジスタ２６の内容も、適切な要請を受信することにより、通信路１４に供する

ことができる。最も簡単な実行では、共通の安全な領域（secure zone ）にある各暗号化モジュール１６は、同一の曲線および基準点で動作するため、レジスタ２８および３０の内容はアクセス可能である必要はない。さらなる高度性が必要であれば、各モジュール１６は、独自の曲線および基準点を選択してもよく、その場合、レジスタ２８および３０の内容は、通信路１４にアクセス可能である必要がある。

【００３０】

モジュール１６は、暗号化およびキー交換で使用される上記生成部２４から、セッションシードである整数ｋを受信する整数レジスタ３４をさらに備えている。また、モジュール１６は、演算中に必要に応じて一時記憶部として使用されるランダムアクセスメモリ（ＲＡＭ）３６を有している。

【００３１】

一般的な実施の形態では、送信側は、送信側の公開キーＱ、メッセージｍ、送信側の短期公開キーＲ、および送信側の署名部分ｓなどからなるデータ列を形成する。データ列は、形成後、通信路１４を介して所望の受信者１２に送信される。

【００３２】

簡略化のため、送信側１２の署名部分ｓは、上記したように、ｓ＝ａｅ＋ｋ　（ｍｏｄｎ）の式で表されるものとするが、無論、他の署名プロトコルも使用可能である。認証のためには、署名ｓＰ－ｅＱを演算すると共に、Ｒと比較する必要がある。

【００３３】

したがって、受信者の最初の工程は、データ列からＱの値を検索することである。ハッシュ値ｅも、メッセージｍ、および点Ｒの座標から演算されてもよい。これにより、受信者は、ｓＰおよびｅＱの演算により認証を行える。

【００３４】

ｓＰおよびｅＱの計算を高速化するために、受信者は、新しい点ｓＰの座標を以下のように計算することができ、下層の体（underlying field）F_{2^m} における乗算、加算、および逆演算（inverses）が数回行われることを防止する。すなわち、受信者は、図３に示す、「２倍加算」方法の手段によりｓＰを計算できる。

【００３５】

図３を参照すると、本発明の一実施形態により説明される、点ｋＰを得るために値ｋで楕円曲線Ｅ上の点Ｐを乗算する「２倍加算」方法では、最初に、ｋを２値の状態で表すことにより実行される。次に、連続する点の対（ｍＰ，（ｍ＋１）Ｐ）が設定される。ｋの連続する桁のそれぞれが順に考慮され、ｋの２値表現における０値が出現すると、点の対のうち、最初の点が２倍され、次の点に１が加算される。すなわち、（ｍＰ，（ｍ＋１）Ｐ）から（２ｍＰ，（２ｍ＋１）Ｐ）が演算される。また、ｋの２値表現における１値が出現すると、点の対のうち、最初の点は、前回の点の対を加算することによって得られ、次の点は、最初の点に１を加算することによって得られる。すなわち、（ｍＰ，（ｍ＋１）Ｐ）から（（２ｍ＋１）Ｐ，（２ｍ＋２）Ｐ）が演算される。

【００３６】

これは、ｋ＝２３である場合の、以下の簡単な例により説明される。ｋの値が、２値の対（１１０１１）で表されるとすると、上記の規定を１対の点（Ｐ，２Ｐ）に適用することにより、（２Ｐ，３Ｐ）；（５Ｐ，６Ｐ）；（１１Ｐ，１２Ｐ）の、連続する点の数列が得られ、最終的に（２３Ｐ，２４Ｐ）が得られる。したがって、点の対のうち、最初の点が必要とされる点である。

【００３７】

このように、ある点の対の各点が、Ｐだけ異なっている体で、点の対に対し上記の「２倍加算」演算を連続的に行うことにより、最終の結果である２３Ｐが得られる。さらに、「２倍加算」演算の回数は、最大で、ｋのビット数より１だけ少ない回数に等しく、（ｍ－１）回である。「２倍加算」方法は、大きな値を持つｋに対して、プロセッサによる演算の回数を削減するにの優れた利点を有するものである。これは、発明の背景で説明した、単一の点Ｐに対してｋの２倍乗算および加算を行う場合と対象的である。

【００３８】
ｓＰおよびｅＱの計算の説明に戻ると、受信者は、上記の実施の形態を適用し、$F_2{}^m$で定義された、非スーパーシンギュラー楕円曲線Ｅ，$y^2+xy=x^3+ax^2+b$に対してｓＰを計算することができる。
【００３９】
$P_1=(x_1, y_1)$であり、$P_2=(x_2, y_2)$である場合、$P_1 \neq \pm P_2$は、曲線Ｅ上の点であるため、$P_1+P_2=(x_3, y_3)$のように定義することができ、式中、
$x_3=\lambda^2+\lambda+x_1+x_2+a$　　（１）
であり、曲線の傾きは、
$\lambda=(y_2+y_1)/(x_2+x_1)$
で表すことができる。
【００４０】
同様に、$-P_2=(x_2, y_2+x_2)$であり、$P_1-P_2=(x_4, y_4)$である場合、
$x_4=(\lambda!)^2+(\lambda!)+x_1+x_2+a=\lambda^2+x/(x_1+x_2)^2+\lambda+x_2/(x_1+x_2)+x_1+x_2+a$　　（２）
であり、式中、
$(\lambda!)=(y_2+x_2+y_1)/(x_2+x_1)=x_2/(x_2+x_1)+\lambda$であり、$x_3$および$x_4$を加算すると、
$x_3+x_4=x/(x_1+x_2)^2+x_2/(x_1+x_2)=x_1x_2/(x_1+x_2)^2$　（３）
が得られる。
（P_1+P_2）のｘ座標x_3を演算するには、P_1、P_2、および（P_1-P_2）のｘ座標のみが必要ではあるが、この演算は、逆演算を必要とするため、最適に効率がよいものではない。また、これらの計算はｙ座標を必要としない。
【００４１】
再び図２を参照すると、値ｋＰは、「２倍加算」方法を用いて計算することができる。新しい点の対を演算する場合は、常時、上記の数式（３）の加算公式が使用され、演算はｍ回行われる。
【００４２】
したがって、x_1、x_2、およびx_4を伴うx_3を得るための公式が得られたことになる。しかしながら、この公式は逆演算を含むものであり、コストが高くなってしまう。この公式は、以下のように変更することができ、x_1、x_2、およびx_3の値が、x_1/z_1，x_2/z_2，x_3/z_3で表されるとすると仮定し、x_1，x_2，x_3，z_1，z_2，z_3が、「２倍追加」アルゴリズムで保持された値だとする。そして、これらの新しい表記を数式（３）に置換すると、以下のようになる。
【００４３】
【数４】

$$\frac{x_3}{z_3}=x_4+\frac{\dfrac{x_1x_2}{z_1z_2}}{\left(\dfrac{x_1}{z_1}+\dfrac{x_2}{z_2}\right)^2}=x_4+\frac{x_1x_2z_1z_2}{(x_1z_2+x_2z_1)^2}=\frac{x_4(x_1z_2+x_2z_1)^2+x_1x_2z_1z_2}{(x_1z_2+x_2z_1)^2}$$

【００４４】
したがって、$x_3=x_4(x_1z_2+x_2z_1)^2+x_1x_2z_1z_2$，とし、$z_3=(x_1z_2+x_2z_1)^2$とすれば、図３に示す「２倍追加」アルゴリズムを、（新しい表記を用いて）実行することができ、このアルゴリズムのほとんどにおいて逆演算を避けることができる。
【００４５】

x_3 およびz_3 の上記式から、x_3 は、最大で、４回の乗算演算を行うことによって計算できることが分かる。

【００４６】

点P_1 およびP_2 の合計は、x_3 に関して表現され、z_3 は、比較的高コストな逆演算をｘ座標に対して行うことなく得られ、最大で４回の乗算および２回の２乗により演算できる。残余の加算および２乗の演算は、演算能力に関して比較的低コストで行われる。$(x_1 z_2 + x_2 z_1)^2$ の項の演算は、括弧内の値の正規基底表現の循環シフトにより得られ、これは、汎用プロセッサにより比較的簡単に行うことができる。アルゴリズムの終了時点で、必要に応じて、元の表記に転換することができる。

【００４７】

再び図３を参照すると、点Ｐ(x_1, y_1)を２倍するために、$2(x_1, y_1) = (x_3, y_3)$とし、上記と同様に、楕円曲線Ｅの式が、$F_2{}^m$ 上で$y^2 + xy = x^3 + ax^2 + b$として得られる場合、点２Ｐのｘ座標は、

$x_3 = x_1{}^2 + (b / x_1{}^2)$

として表される。

【００４８】

前回と同様に、座標を射影座標として表すと、

$x_3 = x_1{}^4 + b z_1{}^4$

$z_3 = (x_1 z_1)^2$

あるいは

$x_3 = (x_1 + \sqrt{(\sqrt{b})} z_1)$

が得られる。

【００４９】

ｂを比較的小さくすることにより、演算的に高コストである演算処理を、z_3 項に対して、略１回の乗算演算に省略することができる。最後の式にしたがって、$\sqrt{(\sqrt{b})}$を事前に演算することにより、x_3 を計算することができ、必要とされる２乗は２回分少なくなる。また、正規基底表現で述べたように、$x_1{}^4$および$z_1{}^4$の演算は、それぞれの値の表現の２回の循環シフトによって得られ、$(x_1 z_1)^2$ は、積の１回の循環シフトにより得られる。

【００５０】

上述した、図３に示す「２倍追加」方法を適用すると、ｍビットのスカラーに対して、$F_2{}^m$ 上で定義されたｋＰの計算は、最大で、（ｍ－１）回の「２倍加算」演算が必要となることが分かる。上記の説明から、楕円曲線上の点に対する２倍演算は、最大で２回の乗算演算を行うことによってなされ、加算演算は、最大で４回の乗算演算を行うことによってなされる。したがって、本発明の方法を用いてｋＰの座標を演算するには、最大で、６回の（ｍ－１）の乗算演算が必要となる。

【００５１】

ｘの値を計算すれば、上記したように、ｙ座標の値も求めることができる。しかしながら、各ｘ座標には、最大で、２つのｙ座標が存在することになる。例えば、点２４Ｐを得るための最後の工程では、２４Ｐは２３Ｐ＋Ｐ＝２４Ｐで表すことができるため、２３ＰおよびＰの両点が分かることになる。点Ａ＝２３Ｐのｘ座標x_{23}が上記のように得られたと仮定すると、楕円曲線式Ｅにx_{23}を置換し、得られる二次方程式を解くことにより、点Ａ＝$(x_{23}, y_{23}{}^{(1)})$、およびＢ＝$(x_{23}, y_{23}{}^{(2)})$に対応する２つのｙの値が得られる。次に、２４Ｐ＝２３Ｐ＋Ｐを計算することにより得られたｘ座標x_{24}を、楕円曲線式に置換することにより、$(x_{24}, y_{24}{}^{(1)})$および$(x_{24}, y_{24}{}^{(2)})$の２点が得られる。このようにして得られた２点は記憶される。点Ａ＋Ｂには、一般的な点加算により、点Ｐが加算され、それぞれ対応する、Ａ＋Ｐ＝(x_a, y_a)、およびＢ＋Ｐ＝(x_b, y_b)が得られる。これらの点が全て一致しない場合は、(x_b, y_b)が正しい点となり、そうでなければ、点(x_b, y_b)が正しい点となる。したがって、点Ｐの倍数は、ｙ座標を知ることなしに簡単に計算することができ、さらに、必要ならば、ｙ座標は計算の

終了時に得ることができる。

【００５２】

したがって、例えば、再び楕円曲線に対するＥｌＧａｍａｌ方式を参照すると、ｒ＝ｋＰ＝（ｘ，ｙ）を演算する必要がある。この場合、ｙ座標は省略でき、メッセージｍのハッシュを得て、ｘ座標であるｅ＝ｈ（ｍ／／ｘ）を得ることができる。そして、送信側は、受信者に対して、署名ｓおよびハッシュｅを含んだメッセージを送信する。署名ｓは、ｓ＝（ｄｅ＋ｋ）ｍｏｄ　ｎの形式を有しており、ｄは、送信側の個人キーであり、ｋは、送信側により生成されたランダム数である。そして、受信者は、ｓＰ－ｅＱ＝ｒを計算することにより署名を認証する。ｓＰおよびｅＱは共に、本発明の「２倍加算」方法により計算することができる。ｓＰおよびｅＱのｘの値が楕円曲線式Ｅに再び置換されることにより、各値から、ｙの２つの可能値である（x_1，$y_1^{(1)}$），（x_1，$y_1^{(2)}$）、および（x_2，$y_2^{(1)}$），（x_2，$y_2^{(2)}$）が得られる。これらの点の順列（パーミュテーション）間で点減法が行われた場合、正しいｙにより、適切なマッチングｒが得られる。これらの置換のいずれによってもマッチングｒが得られない場合は、署名は認証されない。

【００５３】

図４は、図３を参照して説明した方法により得られたｋＰのｙ座標を求めるさらなる方法の概略図であり、ある点Ｐ＝（ｘ，ｙ）、（ｋ－１）Ｐであるｘ座標x_{k-1}、およびｋＰであるｘ’を番号５０で示している。図３でｋＰのｘ座標を演算することから示唆されるように、（ｋ－１）Ｐのｘ座標も計算される。

【００５４】

したがって、最初に、楕円曲線式に置換することにより、点（ｘ’，ｙ’）が該曲線上に位置するようにｙ’の値を得る。次に、工程５４において、点Ｑを、（ｘ’，ｙ’）に指定する。そして、点Ｑ－Ｐ＝（ｘ"，ｙ"）を、単一点減算（singlepoint subtraction）により完成する。得られたｘ座標ｘ"を、（ｋ－１）のｘ座標x_{k-1}と工程５６で比較し、ｘ"＝x_{k-1}であれば、ｙ’が、ｋＰのｙ座標となり、そうでなければ、ｙ’が、－ｋＰのｙ座標となる。なお、この方法は、０＜ｋ＜点Ｐの次数、であれば実行可能なものである。

【００５５】

ｋＰを演算する本発明の方法を使用することにより、ｋｐおよび（ｋ＋１）Ｐ上にｘ座標が得られるように、（ｋ＋１）Ｐを演算することができる。この場合、ｙ座標は、Ｑ＋Ｐ＝（ｘ"，ｙ"）を演算し、座標ｘ"を、（ｋ＋１）Ｐのｘ座標と比較することによって求めることができる。

【００５６】

図５を参照し、楕円曲線署名の認証のための、本発明の実施形態のさらなる適用を番号７０により示す。上記にように、第１の通信部１０は、個人キーランダム整数ｄ、および点Ｑ＝ｄＰを演算することによって得られた、対応公開キーＱを含むものとする。メッセージｍに署名するために、ハッシュ関数Ｈを用いて、ハッシュ値ｅがメッセージｍから演算される。次に、ランダム整数ｋが、個人セッションキーとして選択される。対応公開キーｋＰは、ランダム整数ｋから計算される。そして、第１の通信部は、点ｋＰのｘ座標を整数ｚとして表現し、第１の署名部分ｒ＝ｚ　ｍｏｄ　ｎを計算する。

【００５７】

その後、第２の署名部分$s=k^{-1}(e+dr)$　ｍｏｄ　ｎも計算される。そして、署名部分ｓおよびｒ、そしてメッセージＭが、第２の通信部１２に送信される。第２の通信部１２により署名（ｒ，ｓ）をメッセージＭに対して認証するためには、第２の通信部１２は、第１の通信部１０の公開キーＱを参照する。メッセージＭのハッシュｅ’は、ハッシュ関数Ｈを用いて計算され、ｅ’＝Ｈ（Ｍ）となる。$c=s^{-1}$ ｍｏｄ　ｎの値も計算される。次に、整数値u_1とu_2とが計算され、u_1＝ｅ’ｃ　ｍｏｄ　ｎ、およびu_2＝　ｒｃ　ｍｏｄ　ｎとなる。署名を認証するためには、u_1Ｐ＋u_2Ｑの値を計算する必要がある。Ｐは知られており、システムワイドパラメタであるため、u_1Ｐの値は、予め

計算されたＰの乗数を用いて素早く演算することができる。例えば、これらの値は、２Ｐ、４Ｐ、８Ｐなどの、Ｐの倍数を予め記憶したテーブルから組み合わせて求めることができる。これに対し、点Ｑは流動的であり、ユーザによって変化するものであるため、u_2Ｑの値の演算は時間を要するものであり、一般的に、予め演算しておくことはできない。

【００５８】

しかしながら、本発明に開示の方法による手段により、署名の認証を大幅に高速化することができる。通常、Ｒ＝u_1 Ｐ＋u_2 Ｑが演算される。点Ｒ＝（ｘ，ｙ）の体の元ｘが、整数ｚに転換され、ｖ＝ｚ　ｍｏｄ　ｎ　の値が演算される。ｖ＝ｒであれば、署名は認証されたことになる。

【００５９】

また、u_2 Ｑを演算するために、「２倍加算」の利点を使用する方法がある。u_2 のモジュラー逆演算（modular inverse）が、$u_2^* = u_2^{-1}$ ｍｏｄ　ｎと計算された場合、Ｒは、u_2（$u_1 u_2^*$ Ｐ＋Ｑ）として表すことができ、すなわち、$u_2 u_2^* = 1$の恒等式（identity）が使用される。$u_1 u_2^*$ の値は整数であるため、簡単に計算できる。したがって、点$u_1 u_2^*$ Ｐは、予め記憶された、Ｐの倍数の値から簡単に計算、もしくは形成できる。その後、点Ｑは、点$u_1 u_2^*$ Ｐに、１回の加算により加算され、新しい点Ｒ’が得られる。

【００６０】

したがって、署名を認証するためには、受信者は、u_2 Ｒ’の値のｘ座標を求めるだけでよいことになる。この計算は、図３を参照して説明した「２倍加算」方法を用いて行うことができる。計算結果がｒと等しければ、署名は認証されたことになる。得られる値は、点u_1 Ｐ＋u_2 Ｑのｘ座標である。ｖ＝ｘ　ｍｏｄ　ｎの値は演算され、ｒに対する認証が行われる。なお、この方式では、署名生成および認証のためにｙ座標は使用されていないため、演算は必要とはなっていない。しかしながら、これらの場合、ｘおよびｙ座標に対して別の方式を使用することができ、ｙ座標は、上述した方法で得られるか、あるｘ座標に対応する２つのｙ座標を計算し、それぞれを、署名の証明する目的のために使用することができる。これらのいずれにおいても比較が満たされない場合は、署名は認証されないことになる。つまり、認証は、点Ｒ＝U_1 Ｐ＋U_2 Ｑの演算を必要とするためである。これは、以下のように行われる。Ｑのｘ座標のみを送信し、図３の「２倍加算」を使用するか、もしくは、Ｅ（F_p）に対してU_2 Ｑのｘ座標を演算する。このｘ座標に対応する両点に対して、いずれにより認証されるかを調べる。

【００６１】

再び図１を参照すると、ｋＰで表される通信部間でキーが伝達される場合、通信帯域幅を低減する場合、送信側は、ｋＰの座標の内の１つのみを送信し、他方の座標を受信側で演算することができる。例えば、体の元がF_2^{155}に対して１５５ビットである場合、例えば、他方の座標の正しい値である単一のビットとしての識別子を送信してもよい。これにより、第２の座標が、受信側により演算され、正しいものを識別子から識別することが可能となる。

【００６２】

したがって、図１を参照すると、送信部１０は、最初に、受信側１２の公開キーｄＰとして、座標x_0 を表すビット列、および、座標y_0 の単一のビットを受信する。

【００６３】

送信側１０は、レジスタ３０に曲線のパラメタを有しているため、座標x_0 および曲線のパラメタを使用することにより、算術部２０から、他方の座標y_0 の可能値を得ることができる。

【００６４】

$y^2 + xy = x^3 + ax^2 + b$の式および座標$x_0$ を有する曲線については、y_0 の可能値y_1 およびy_2 は、$y^2 + x_0 y = x_0^3 + a x_0^2 + b$のルートとなる。

【００６５】

ｙの解を得ることにより、演算部２０において、２つの可能ルートが得られ、送信された

情報ビットとの比較により、どちらの値がｙの値として適当かが示される。

【００６６】

第２の座標（y_0）の２つの可能値は、x_0だけ異なっており、すなわち、$y_1 = y_2 + x_0$である。y_0の２つの値はy_0により異なっているため、y_1とy_2は、x_0の表現に「１」が現れるときには常時異なることになる。したがって、送信される追加ビットは、これらの位置のいずれかから選択され、y_0の値の対応ビットを調べることにより、２つのルートのいずれが適切な値かが示される。

【００６７】

したがって、受信側１０は、１５６ビットのみが検索されるにも関わらず、公開キーｋＰの座標を生成することができる。

【００６８】

セッションキーｋＰの受信側１２への送信も、送信側１０は、x_0およびy_0の選択された識別ビットである、１つの座標のみを送信すればよいので、同様に効率的に行うことができる。その後、受信側１２は、y_0の可能値を再形成し、適切なほうを選択することができる。

【００６９】

体$F_2{}^m$では、２ａ＝０とした二次方程式の解の公式を用いてｙの解を求めることができない。したがって、その他の方法を使用する必要があり、これを効率的に行うために、特に、算術部２０が適用される。

【００７０】

一般的に、x_0が０でなければ、$y = x_0 z$である場合、$x_0{}^2 z^2 + x_0{}^2 z = x^3{}_0 + a x_0{}^2 + b$となる。これは、$z^2 + z = x_0 + a + (b / x_0{}^2)$　$1 = c$のように書くことができる。すなわち、

$z^2 + z = c$

である。

【００７１】

y_0の２つの可能値を得るためには、ｍが奇数であれば、

$z = c + c^4 + c^{16} + \cdots + c^{2m-1}$

あるいは、$z = 1 + c + \cdots + c^{2m-1}$が用いられる。

【００７２】

ｍが偶数である場合も、c^w（ただし、$w = 2^g$）の形態を有する項を用いた同様の解法が存在する。

【００７３】

これは、$F_2{}^m$の正規基底表現に特に好適に使用される。

【００７４】

上述したように、$F_2{}^m$の体の元を、ｇ乗するためには、体の元が正規基底で表される、ｇ回循環シフト（g fold cyclic shift）により行える。

【００７５】

したがって、ｚの各値は、得られたy_0の値をシフト、および加算することにより演算することができる。正しい値は、送信された追加ビットにより求めることができる。

【００７６】

したがって、$F_2{}^m$の正規基底表現を使用することにより、y_0の座標を回復するために使用されるプロトコルを簡略化することができる。

【００７７】

Ｐ＝（x_0 y_0）が、体$F_2{}^m$で定義された楕円曲線Ｅである、$y^2 + xy = x^3 + a x^2 + b$上の点である場合、$y_0$は、$x_0 = 0$である場合は０であり、$x_0 \neq 0$である場合は、体の元$y_0 \cdot x_0{}^{-1}$の最小有効ビットと定義される。

【００７８】

Ｐのｘ座標x_0、およびビットy_0は、送信側１０および受信側１２間で送受信される。ｙ座標は、以下のように回復される。

【００７９】
（１）x_0 ＝０であれば、y_0 は、パラメタレジスタ３０に記憶された体の元ｂのベクトル表現を、左側へ１段循環シフトすることにより得ることができる。すなわち、$b = b_{m-1}\ b_{m-2} \cdots b_1\ b_0$ であれば、$y = b_{m-2} \cdots b_1\ b_0\ b_{m-1}$ である。
【００８０】
（２）$x_0 \neq 0$であれば、以下が行われる。
（２．１）$F_2{}^m$ で体の元$c = x_0 + a + b x_0{}^{-2}$を演算する。
（２．２）ｃのベクトル表現を、$c = c_{m-1} c_{m-2} \cdots c_1\ c_0$ とする。
（２．３）
$z_0 = y_0$,
$z_1 = c_0 \Theta z_0$,
$z_2 = c_1 \Theta z_1$,
:
$z_{m-2} = c_{m-3} \Theta z_{m-3}$,
$z_{m-1} = c_{m-2} \Theta z_{m-2}$
と設定し、体の元$z = z_{m-1}\ z_{m-2} \cdots z_1\ z_0$ を形成する。
（２．４）最後に、$y_0 = x_0 \cdot z$を演算する。
【００８１】
なお、$x_0{}^{-2}$の演算は、上記のように、算術部２０で簡単に演算することができ、y_0 の演算は、乗法部４８により得ることができる。
【００８２】
上記の例では、y_0 の適切な値の識別は、単一のビットの送信、および得られたルートの値を比較することにより得られていた。しかしながら、他の識別子を使用することによっても、値の適切な一方を識別することができ、演算は、ＧＦ（2^m）の体の楕円曲線による暗号化に限定されない。例えば、体が、Z_p ｐ＝３（ｍｏｄ　４）として選択される場合、適切な値と関連付けられたルジャンドルの記号を、適切な値として指定するために送信することができる。また、Ｚｐの元の集合は、$y \neq 0$であるとすれば、ｙが１つの部分集合であるとき、－ｙが他方となるような性質で、部分集合の対にさらに分割することができる。そして、任意の値をそれぞれの部分集合に割り当て、座標x_0 と共に送信し、y_0 の適切な値はどの部分集合に位置するかが示される。したがって、y_0 の適切な値を求めることができる。簡略的に、y_0 の適切な値の識別を促進するために、部分集合が区間配置される、適切な表現をとることができる。なお、上記した方法の１つを用いて座標を求めることもできる。
【００８３】
これらの方法は、楕円曲線を用いた暗号化に特に好適なものであるが、代数曲線に対しても使用できるものであり、曲線上の点の座標を転送する必要のある誤り訂正エンコーディングなどの、他の分野への適用も可能なものである。
【００８４】
したがって、有限体$GF_2{}^m$ 内に位置する楕円曲線を使用すると共に、正規基底表現を使用することにより、楕円曲線を用いた暗号化に必要な演算を効率的に行うことができる。このような演算は、ソフトウェアやハードウェアのいずれによっても実現することができ、演算の構成により、ハードウェアにより実現された有限体乗数の使用が特に効率的になる。
【００８５】
F_p およびF_{2m}上の楕円曲線点のスカラー倍数の演算効率を向上させるための、本発明のさらなる実施の形態を以下に示す。F_{2m}で定義される、一般化した楕円曲線式Ｅである、Ｅ：$y^2 + xy = x^3 + ax^2 + b$, $b \neq 0$を考慮する。
【００８６】
Ｐ＝（x_1, y_1）が生成元である場合、図３および投影曲線に対して説明した方法を用いて、ｋＰ,（ｋ＋１）Ｐが得られ、ｋはスカラーであり、ｋＰ＝（X_2, Z_2）,（ｋ＋１

）Ｐ＝（Ｘ$_3$,Ｚ$_3$）．
である。
【００８７】
ここでの目的は、ｋＰ＝（ｘ$_2$,ｙ$_2$）のアフィン座標（affine coordinates）を得ることであり、ｘ$_2$＝（Ｘ$_2$／Ｚ$_2$）であることは明らかになっている。
【００８８】
（ｋ＋１）Ｐ＝（ｘ$_3$,ｙ$_3$）のアフィン座標を考慮すると、
【００８９】
【数５】

$$x_3 = \lambda^2 + \lambda + x_1 + x_2 + a, \lambda = \frac{y_1 + y_2}{x_1 + x_2}$$

$$\lambda^2 + \lambda + (x_1 + x_2) + a = \frac{y_1^2 + y_2^2 + (x_1 + x_2)(y_1 + y_2) + (x_1 + x_2)^3 + a(x_1 + x_2)^2}{(x_1 + x_2)^2}$$

$$= \{y_2^2 + x_1 y_2 + x_2 y_1 + x_2 y_2 + x_1^2 x_2 + x_1 x_2^2 + x_2^3 + a x_2^2\} \frac{1}{(x_1 + x_2)^2}$$

$$= \frac{\{b + b + x_1 y_2 + x_2 y_1 + x_1^2 x_2 + x_1 x_2^2\}}{(x_1 + x_2)^2}$$

$$= \frac{x_1 y_2 + x_2 y_1 + x_2^2 x_1 + x_1^2 x_2}{(x_1 + x_2)^2}$$

$$= \frac{x_1 y_2 + x_2 y_1 + x_1 x_2 (x_1 + x_2)}{(x_1 + x_2)^2}$$

【００９０】
であり、
ｙ$_2$の解を求めると、
【００９１】
【数６】

$$y_2 = \frac{1}{x_1}\{x_3 (x_1 + x_2)^2 + x_2 y_1 + x_1 x_2 (x_1 + x_2)\} \qquad (*)$$

【００９２】
が得られ、
ｘ$_1$およびｙ$_1$は分かっているが、
ｘ$_2$＝（Ｘ$_2$／Ｚ$_2$）とｘ$_3$＝（Ｘ$_3$／Ｚ$_3$）とを演算する必要がある。これらは、２回の逆演算（inversions）と、２回の乗算とを必要とする。式を書き換えると、
【００９３】
【数７】

$$y_2 = (x_1 + x_2)\left\{\frac{1}{x_1}[X_3(x_1 + x_2) + y_1] + x_2\right\} + y_1$$

$$= (x_1 + x_2)\left\{\frac{1}{x_1 Z_3}[X_3(x_1 + x_2) + Z_3 y_1] + x_2\right\} + y_1$$

【００９４】

となり、これらの数量を演算するには、x_1 Z_3_およびZ_2 を逆演算し、４回の乗算が必要となる。x_1 Z_3 は１回の乗算を必要とするので、合計は２回の逆演算および５回の乗算である。

特異な標数の場合、

【００９５】

【数８】

$$E : y^2 = x^3 + ax + b$$

$$x_3 = \lambda^2 - x_1 - x_2 \qquad \lambda = \frac{y_2 - y_1}{x_2 - x_1}$$

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right) - x_1 - x_2$$

$$= \frac{y_2^2 - 2y_1y_2 + y_1^2 - (x_1 + x_2)(x_2 - x_1)^2}{(x_2 - x_1)^2}$$

$$= y_2^2 - 2y_1y_2 + y_1^2 - (x_1 + x_2)(x_2^2 - 2x_1x_2 + x_1^2)$$

$$= y_2^2 - 2y_1y_2 - x_1x_2^2 + 2x_1^2x_2 - x_2^3 + 2x_1x_2^2 - x_2x_1^2$$

$$= \frac{ax_2 + b + ax_1 + b - 2y_1y_2 - x_1x_2^2 + x_1^2x_2 + 2x_1x_2^2}{(x_2 - x_1)}$$

【００９６】

であり、

y_2 の解を求めると、

【００９７】

【数９】

$$2y_1y_2 = -x_3(x_2 - x_1)^2 + ax_2 + 2b + ax_1 + x_1x_2^2 + x_1^2x_2$$

もしくは

$$y_2 = \frac{1}{2y_1}\left\{-x_3(x_2 - x_1)^2 + a(x_2 + x_1) + 2b + x_1x_2(x_1 + x_2)\right\}$$

$$= \frac{1}{2y_1}\left\{(x_1 + x_2) + (a + x_1x_2) - x_3(x_2 - x_1)^2\right\}$$

【００９８】

となり、x_3 を置換すると、

【００９９】

【数１０】

$$x_2 = \frac{X_2}{Z_2}$$

$$y_2 = \frac{1}{2y_1 Z_3}\left\{Z_3(x_1+x_2)(a+x_1x_2) - X_2(x_2-x_1)^2\right\}$$

【０１００】

が得られる。

同様に、体Ｆｐでは、

【０１０１】

【数１１】

$$y^2 = x^3 + ax + b$$

$$x_3 = \lambda^2 - x_1 - x_2$$

$$y_3 = \lambda\ (x_1 - x_3) - y_1$$

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \qquad (P2 \neq P3)$$

$$x_3 = \frac{y_2^2 - 2y_1y_2 + y_1^2 - (x_2-x_1)^2(x_2+x_1)}{(x_2-x_1)^2}$$

$$= \frac{y_2^2 - 2y_1y_2 + y_1^2 - x_2^3 + x_1^2x_2 + x_1x_2^2 - x_1^3}{(x_2-x_1)^2}$$

$$= \frac{ax_2 + b + ax_1 + b - 2y_1y_2 + x_1x_2(x_1+x_2)}{(x_2-x_1)^2}$$

$$y_2 = \frac{1}{2y_1}\left[(x_1+x_2)\bullet(a+x_1x_2) + 2b - x_3(x_2-x_1)^2\right]$$

$$x_2 = X_2\frac{1}{Z_2}, x_3 = X_3\frac{1}{Z_3}$$

【０１０２】

であり、逆演算と７個の倍数を意味し、または、同等に、１回の逆演算と１３個の倍数を意味する。

３ｉ＋７ｍ＝１ｉ＋１３ｍ

x_3 を置換すると、

【０１０３】

【数１２】

$$x_2 = X_2 \frac{1}{Z_2}$$

$$y_2 = \frac{1}{2y_1 Z_3} \bullet \left\{ Z_3 \bullet \left[(x_1 + x_2), (a + x_1 x_2) + 2b \right] - X_3 (x_2 - x_1)^2 \right\}$$

【０１０４】
が得られる。
この場合、２回の逆演算と８個の倍数、または、同等に、１回の逆演算と１１個の倍数が得られる。
【０１０５】
したがって、本発明は、一般的に、暗号化方法およびそのシステムに関するものであり、特に、有限体の元が、プロセッサに対して効率的に乗算される、楕円曲線暗号化方法およびそのシステムに関するものである。上記暗号化方法およびそのシステムは、適当にプログラムされ汎用コンピュータなどの、適応する全てのプロセッサユニットとして実現できるものである。
【０１０６】
本発明は、ある特定の実施の形態を参照して説明されたものではあるが、添付の特許請求の範囲に記載する発明の範囲を越えることなく、当業者によって様々に変更可能なものである。
【図面の簡単な説明】
【図１】　データ通信システムの概略を示す図である。
【図２】　暗号化／暗号解読ユニットの概略を示すブロック図である。
【図３】　点の倍数を計算するためのフローチャートである。
【図４】　ｙ座標を取り出すためのフローチャートである。

【図１】

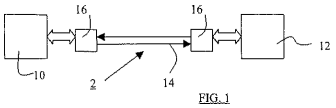
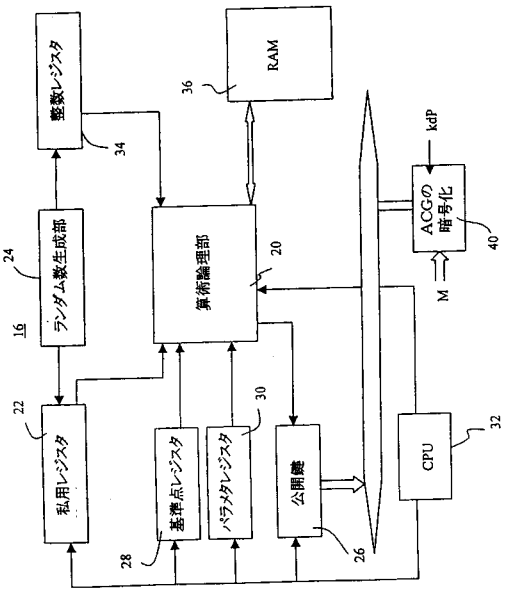
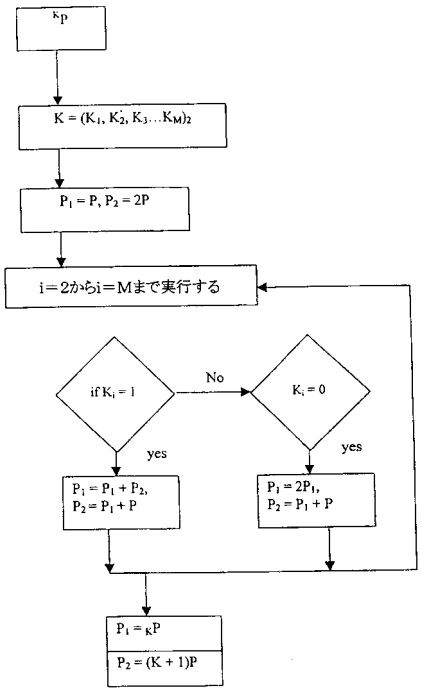


FIG. 1

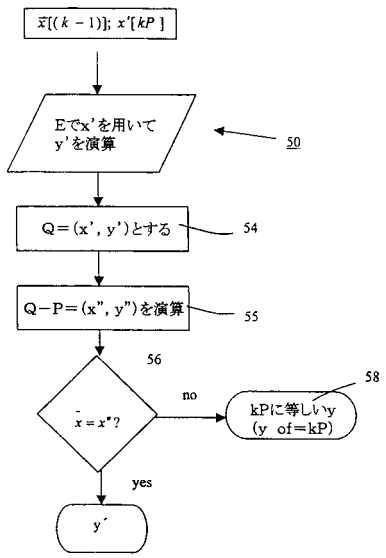
【図２】



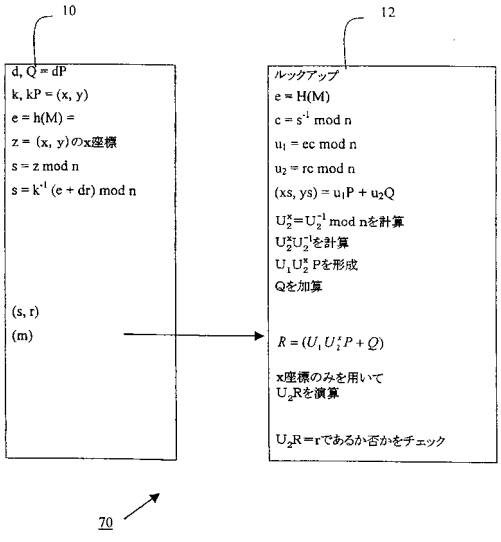
【図３】



【図４】



【図５】



フロントページの続き

(72)発明者 ヴァンストーン，スコット，エー.
カナダ，オンタリオ州 エヌ２ティー ２エイチ４，ワーテルロー，サンドブルック コート ５３９
(72)発明者 ミューリン，ロナルド，シー.
カナダ，オンタリオ州 エヌ２エル ４アール９，ワーテルロー，ツイン オークス クレセント ５３３
(72)発明者 アンティパ，エイドリアン
カナダ，オンタリオ州 エル４ゼット ３アール３，ミシソーガ，コーティナ クレセント ５６２３
(72)発明者 ギャラント，ロバート
カナダ，オンタリオ州 エル５エム ５エヌ１，ミシソーガ，ローズブッシュ ロード ４７８８

審査官 新田 亮

(56)参考文献 国際公開第９６／００４６０２（WO，Ａ１）
欧州特許出願公開第０８７４３０７（ＥＰ，Ａ１）
G.B.Agnew, An Implementation of Elliptic Curve Cryptosystems Over F2^155, [online], IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, １９９３年 ６月, VOL.11,NO.5, p.804-813, [retrieved on 2009-07-15], Retrieved from the Internet, ＵＲＬ, http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=00223883

(58)調査した分野(Int.Cl.，ＤＢ名)
G09C 1/00
G06F 7/72
H04L 9/32