(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2012 年 4 月 12 日(12.04.2012)

PCT

(10) 国際公開番号
WO 2012/046805 A1

(51) 国際特許分類:
G09C 1/00 (2006.01) *H04L 9/32* (2006.01)

(21) 国際出願番号: PCT/JP2011/073098

(22) 国際出願日: 2011 年 10 月 6 日(06.10.2011)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願 2010-228250 2010 年 10 月 8 日(08.10.2010) JP

(71) 出願人 (米国を除く全ての指定国について): 国立大学法人岡山大学 (NATIONAL UNIVERSITY CORPORATION OKAYAMA UNIVERSITY) [JP/JP]; 〒7008530 岡山県岡山市北区津島中一丁目１番１号 Okayama (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 野上保之 (NOGAMI Yasuyuki) [JP/JP]; 〒7008530 岡山県岡山市北区津島中三丁目１番１号　国立大学法人岡山大学大学院自然科学研究科内 Okayama (JP). 森川良孝 (MORIKAWA Yoshitaka) [JP/JP]; 〒7008530 岡山県岡山市北区津島中三丁目１番１号　国立大学法人岡山大学大学院自然科学研究科内 Okayama (JP). 出田哲也 (IZUTA Tetsuya) [JP/JP]; 〒7008530 岡山県岡山市北区津島中三丁目１番１号　国立大学法人岡山大学工学部内 Okayama (JP).

(74) 代理人: 松尾憲一郎 (MATSUO Kenichiro); 〒8100042 福岡県福岡市中央区赤坂１丁目１０番１７号　しんくみ赤坂ビル７階 Fukuoka (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

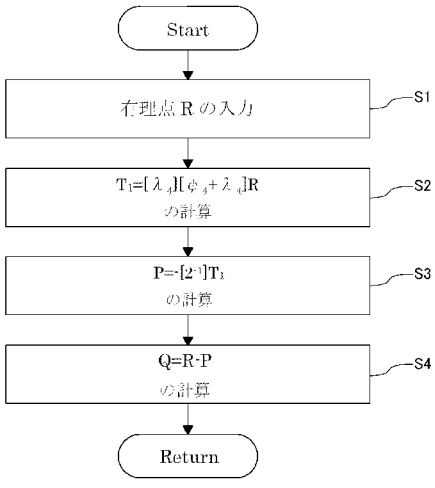
(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK,

[続葉有]

(54) **Title**: RATIONAL POINT INFORMATION COMPRESSION DEVICE, RATIONAL POINT INFORMATION COMPRESSION METHOD, AND RATIONAL POINT INFORMATION COMPRESSION PROGRAM

(54) 発明の名称 : 有理点情報圧縮装置、有理点情報圧縮方法及び有理点情報圧縮プログラム

[図6]



S1 INPUT RATIONAL POINT R
S2 CALCULATE $T_1 = [\lambda_4][\Phi_4 + \lambda_4] R$
S3 CALCULATE $P = [2^{-1}] T_1$
S4 CALCULATE $Q = R - P$

(57) **Abstract**: Provided are a rational point information compression device, a rational point information compression method, and a rational point information compression program which compress and restore rational point information for a rational point group with an embedded degree of 1. With an additive group formed of rational points on an elliptical curve defined over a finite field F_p of a characteristic P designated $E(F_p)$, and sets of rational points having a composite number order r, i.e., subgroups of the additive group, designated $G_1 = E(F_p)[r]$ and $G_2 = E(F_p)[r]$, rational points $P \in G_1$ and $Q \in G_2$ are compressed into the rational point R by the formula $R = P + Q$ when being transmitted, and the rational point R is factored and restored into the rational points P and Q at the receiving end, thus shortening the data length involved in transmission and reception.

(57) 要約: 有理点群の埋め込み次数を１とした場合において、有理点情報を圧縮・復元する有理点情報圧縮装置、有理点情報圧縮方法、及び有理点情報圧縮プログラムを提供する。標数 P の有限体 F_p 上で定義された楕円曲線上の有理点のなす加法群を $E(F_p)$とし、合成数位数 r を持つ有理点の集合すなわち加法群の部分群を $G_1=E(F_p)[r]$, $G_2=E(F_p)[r]$として、有理点 $P \in G_1$, $Q \in G_2$ を送信する際に $R=P+Q$ として有理点 R に圧縮し、受信先で、有理点 R から有理点 P,Q を分解・復元することにより、送受信に伴うデータ長を短縮する。

WO 2012/046805 A1

SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:

— 国際調査報告（条約第 21 条(3)）

明　細　書

発明の名称 ：

有理点情報圧縮装置、有理点情報圧縮方法及び有理点情報圧縮プログラム

技術分野

[0001] 本発明は、楕円曲線暗号、ペアリング暗号における有理点情報圧縮装置、有理点情報圧縮方法及び有理点情報圧縮プログラムに関する。特に有理点群の埋め込み次数を１とした場合の、楕円曲線暗号、ペアリング暗号における有理点情報圧縮装置、有理点情報圧縮方法及び有理点情報圧縮プログラムに関する。

背景技術

[0002] 昨今、インターネットなどの電気通信回線を利用した情報ネットワーク技術が高度に発展し、インターネットによって様々な情報を取得するだけでなく、インターネットバンキングや行政機関への電子申請などのような各種のサービスが提供されてきている。

[0003] このようなサービスを利用する場合には、サービスの利用者が成りすましや架空の人間などではなく、適正な利用者であることを確認するための認証処理が必要であり、信頼性の高い認証方法として、公開鍵と秘密鍵を用いる公開鍵暗号をベースとした電子認証技術がよく利用されている。

[0004] しかしながら、公開鍵暗号方式の電子認証では、公開鍵及び秘密鍵が漏洩した場合には直ちに公開鍵と秘密鍵を変更する必要がある。このため、公開鍵及び秘密鍵の管理を慎重に行わなければならず、また、必要に応じて新たな公開鍵と秘密鍵の設定登録作業が生じるという煩雑さがある。このため、最近では、利用者の氏名やメールアドレスのように利用者特有のIDを用いて電子認証を行うIDベース暗号が用いられることが多くなっている。

[0005] また、電子認証を行う認証装置によって利用者の個人認証を行った場合には、認証装置に利用者ごとの履歴が蓄積されることとなる。この履歴情報自体が利用者の個人情報であるため、最近では、この履歴情報が漏洩すること

による個人情報の漏洩のおそれが指摘されている。

[0006] そこで、認証装置では利用者の個人情報を利用して認証を行うのではなく、複数の利用者をひとまとまりのグループとして、このグループに所属していることを示すグループ署名を用いることにより、利用者を特定することなく認証を行うことによって、認証装置に個人情報が蓄積されることなく認証を可能としたグループ署名技術が提案されている。

[0007] 国家UNS戦略プログラムにおいても、プライバシを保護しつつユーザ認証を行うことのできる匿名認証技術の重要性、必要性が取り上げられている。UNS:Universal Communications、New Generation Networks、Security and safety

[0008] このようなIDベース暗号やグループ署名等を簡便に実現するための数学的な土台としてペアリング暗号がある。ペアリングとは、楕円曲線上で定義される２入力１出力の関数であり、入力は楕円曲線上の２つの有理点、出力は有限体の元が用いられている。このペアリングは２入力に対して双線形性を持つ。例えば、Pを素体F_p上で定義される楕円曲線上の有理点、Qをk次拡大体F_{p^k}上で定義される楕円曲線上の有理点として、PとQを入力して拡大体$F^*_{p^k}$の元ｚが出力されるとき、a倍のPとｂ倍のQを入力するとｚのab乗が出力される。ペアリング暗号では、この双線形性を利用して暗号システムを構築する。なお、ここで「ｋ」を埋め込み次数と呼び「$F^*_{p^k}$」は、位数がp^kである有限体（拡大体）から単位元０を除いた乗法群を表わす。

[0009] 楕円曲線上の有理点とは、楕円曲線$y^2 = x^3+ax+b$を満たす有限体F_qの元の座標（x,y）の組をいう。この集合に無限遠点Oを加えたものは加法群を成し、E(Fq)と表わす。すなわち、楕円曲線上の2つの有理点P、Qを通る直線が楕円曲線と交わる点のｘ軸を対称とした点をRとすれば、P+Q=Rが成立する。この演算を楕円加算と呼ぶ。PとQが同一点の場合はPを通る接線が楕円曲線と交わる点のｘ軸を対称とした点をRとすれば、P＋P=2P=Rが成立する。この演算を楕円２乗算と呼ぶ。ペアリング暗号及び楕円暗号の安全性の根拠は楕円曲線上の離散対数問題の求解困難性に基づいている。素因数分解の困難性を

安全性の根拠とするRSA暗号等と比べ、はるかに短い鍵長で同等の暗号強度（安全性強度）を実現できる。

[0010] ディジタルグループ署名では、グループに所属する個人ユーザのアクセス権の認証処理を行う際に、アクセス権が失効している個人ユーザを除外するためのペアリング演算を行った後に所定の個人ユーザのペアリング演算を行って認証処理を行うことにより、個人ユーザごとのアクセス権の発行または失効の属性変更に柔軟に対応可能としている。

[0011] したがって、例えば、10,000人の個人ユーザで構成されるグループのディジタルグループ署名の場合、アクセス権が失効している個人ユーザが100人いれば、100回のペアリング演算が必要となっており、現時点での一般的な電子計算機による1回のペアリング演算に約0.1秒を要していることから、100回のペアリング演算には約10秒を要することとなってしまうため、実用上、個人ユーザの数が制限されることとなって、広く利用されるものとはなっていなかった。

[0012] そこで、ペアリング演算の演算速度を向上させることによりディジタルグループ署名の実用性を向上させるために、例えば、ペアリング演算として楕円曲線上で定義されるTateペアリング演算法を用い、演算負荷を低減させて高速化を図る技術が提案されている。

[0013] このように、これまでペアリングを用いた暗号方式（IDベース暗号、グループ署名等）は数多く提案されているが、その多くは、160ビット以上の素数位数を持つペアリング曲線（ペアリングに効率のよい楕円曲線）を用いるものである。本発明者らはこれまで、土台の数学的構造から、拡大体における計算、楕円曲線暗号の計算、ペアリング計算について出願を行なってきた。そのいずれもが、素数位数のペアリング暗号を効率化するものである。

[0014] 一方、近年、有理点群の埋め込み次数が１で2000ビットを超える合成数位数を持つペアリング曲線を用いるものが提案されており、また新たなアプリケーションも提案されている（例えば、非特許文献１参照。）。

[0015] 素数位数のペアリング暗号を効率化するこれまでの手法は、本発明がター

ゲットとする大きな合成数位数のペアリングに対して即座に適用できるものではない。言い換えれば、合成数位数のペアリング曲線は埋め込み次数が１となるなど特殊な状況におかれるため、これを考慮した新たな高速化手法を提案する必要性がでてきた。埋め込み次数を１とする理由は、ペアリング暗号の暗号強度を必要十分に確保するための強度と効率のバランスを図るのに最も適しているのが埋め込み次数１だからである。埋め込み次数を大きくした場合は暗号強度が十分すぎ、また実現する上での効率が悪くなる。

[0016] このようなペアリング暗号または楕円曲線暗号のプロトコルでは、複数の有理点の情報をネットワークで送受信することとなる。例えば、有理点Pと有理点Qを送信するなどである。これらの有理点を個別に送れば、合成数位数が2000ビットとすると、標数は4000ビットとなり、有理点P,Qのｘ座標、y座標を考えると、４倍の16000ビットを送信することとなる。

[0017] 電子認証システムでは、大量のユーザリストが送受信され、ペアリング計算時間とともに、これら多数の有理点情報を含むユーザリストのネットワーク上での送受信時間が問題となっている。

[0018] これに対し、上記の例で、もし有理点P及びQのペアに対し、R=P+Qという楕円加算して圧縮した有理点Rを送信し、受信先で元の有理点P及びQを復元できれば、その送信する情報量はこのペア当たり半分の8000ビットで済むことになる。

[0019] 有理点の圧縮方法については、例えば、非特許文献２、特許文献１などが知られている。特許文献１では、有限体F_q及び拡大体F_q^k上の有理点2点を楕円加算して圧縮し、受信先で射影により元の有理点を復元する方法等が開示されている。

先行技術文献

特許文献

[0020] 特許文献1：特開2008-178035号公報

非特許文献

[0021] 非特許文献1：D. Boneh, K. Rubin and A. Silverberg, “Finding Composit

e Order Ordinary Elliptic Curves Using the Cock-Pinch method”

非特許文献2：Ian F.Blake et al, “Advances in Elliptic Curve Cryptography”

発明の概要

発明が解決しようとする課題

[0022] しかしながら、本発明が対象とする有理点群の埋め込み次数が１の場合、有理点P及びQを圧縮して有理点Rを送信し、受信先でこれを分解・復元する方法は、これまで知られていなかった。

[0023] 本発明者らは、このような現状に鑑み、有理点の情報圧縮を効率的に行うべく研究開発を行って、本発明を成すに至ったものである。

課題を解決するための手段

[0024] 本発明の有理点情報圧縮装置では、

標数ｐの有限体F_p上で定義された楕円曲線上の有理点の成す加法群を$E(F_p)$とし、合成数位数ｒを持つ有理点の集合すなわち前記加法群の部分群を$G_1=E(F_p)[r]$、$G_2=E(F_p)[r]$として、

有理点$P\in G_1$及び有理点$Q\in G_2$の情報を送受信するCPU及び記憶手段を備えた有理点情報圧縮装置において、

前記加法群$E(F_p)$は、埋め込み次数を１とし、

前記電子計算機のCPUは、

有理点P’を入力して前記記憶手段に記憶する入力手段と、

前記電子計算機のCPUを有理点部分群特定手段として機能させて、前記記憶手段から前記有理点P’を読み出し、自己準同型写像ϕにより、

$\lambda_1 P=\phi(P)$、$\lambda_2 Q=\phi(Q)$ （$\lambda_1\neq\lambda_2$は整数）を満足する前記有理点P及びQの集合である前記部分群G_1及びG_2を特定する有理点部分群特定手段と、

前記記憶手段から前記有理点PまたはQを読み出し、前記自己準同型写像$\phi(P)$または$\phi(Q)$を演算しその結果の有理点を前記記憶手段に記憶する自己準同型写像演算手段と、

前記有理点P及び前記有理点Qから有理点R＝P+Qを演算する第1演算手段と、

前記有理点Rから有理点P及び有理点Qを演算する第2演算手段と、

を有することとした。

[0025] さらに本発明の有理点情報圧縮装置では、

前記楕円曲線は、 $E: y^2 = x^3 + ax$, $a \in F_p$, $4 | (p-1)$ であり、

前記合成数位数 r は、$r | \#E(F_p)$, $4 | (r-1)$ を満たし、

前記整数λ_1、λ_2は、$\lambda_1^2+1 \equiv 0 \pmod r$、$\lambda_2^2+1 \equiv 0 \pmod r$を満たし、

前記自己準同型写像は、$\phi : E(F_p)[r] \rightarrow E(F_p)[r]$、

$(x,y) \rightarrow (-x, \zeta y)$, $\zeta^4=1$, $\zeta, \zeta^2 (\neq 1) \in F_p$ であり、

前記第2演算手段は、前記有理点P, 前記有理点Qの演算を、それぞれ

$[\lambda_1][\phi+\lambda_1]R=[-2]P$, $Q=R-P$ を用いて行うことにも特徴を有するものである。

[0026] 本発明の有理点情報圧縮装置では、

前記楕円曲線は、 $E: y^2 = x^3 + b$, $b \in F_p$, $3 | (p-1)$ であり、

前記合成数位数 r は、$r | \#E(F_p)$, $3 | (r-1)$ を満たし、

前記整数λ_1、λ_2は、$\lambda_1^2+\lambda_1+1 \equiv 0 \pmod r$、$\lambda_2^2+\lambda_2+1 \equiv 0 \pmod r$を満たし、

前記自己準同型写像は、$\phi : E(F_p)[r] \rightarrow E(F_p)[r]$、

$(x,y) \rightarrow (\varepsilon x, y)$, $\varepsilon^3=1$, $\varepsilon (\neq 1) \in F_p$ であり、

前記第2演算手段は、前記有理点P, 前記有理点Qの演算を、それぞれ

$[2\lambda_1+1][\phi+\lambda_1+1]R=[-3]P$, $Q=R-P$ を用いて行うことにも特徴を有するものである。

[0027] さらに本発明の有理点情報圧縮装置では、

前記楕円曲線は、 $E: y^2 = x^3 + b$, $b \in F_p$, $6 | (p-1)$ であり、

前記合成数位数 r は、$r | \#E(F_p)$, $3 | (r-1)$ を満たし、

前記整数λ_1、λ_2は、$\lambda_1^2-\lambda_1+1 \equiv 0 \pmod r$、$\lambda_2^2-\lambda_2+1 \equiv 0 \pmod r$を満たし、

前記自己準同型写像は、$\phi : E(F_p)[r] \rightarrow E(F_p)[r]$、

$(x,y) \rightarrow (\varepsilon x, -y)$, $\varepsilon^3=1$, $\varepsilon (\neq 1) \in F_p$ であり、

前記第2演算手段は、前記有理点P, 前記有理点Qの演算を、それぞれ

$[2\lambda_1-1][\phi+\lambda_1-1]R=[-3]P$, $Q=R-P$ を用いて行うことにも特徴を有するも

のである。

[0028] 本発明の有理点情報圧縮方法では、

標数ｐの有限体F_p上で定義された楕円曲線上の有理点の成す加法群を$E(F_p)$とし、合成数位数ｒを持つ有理点の集合すなわち前記加法群の部分群を$G_1=E(F_p)[r]$、$G_2=E(F_p)[r]$として、

有理点$P\in G_1$及び有理点$Q\in G_2$の情報を送受信する場合に、CPU及び記憶手段を備えた電子計算機で行う情報圧縮方法において、

前記加法群$E(F_p)$は、埋め込み次数を１とし、

前記電子計算機のCPUを入力手段として機能させて、有理点P’を入力して前記記憶手段に記憶する入力ステップと、

前記電子計算機のCPUを有理点部分群特定手段として機能させて、前記記憶手段から前記有理点P’を読み出し、自己準同型写像ϕにより、

$\lambda_1 P=\phi(P)$、$\lambda_2 Q=\phi(Q)$ （$\lambda_1\neq\lambda_2$は整数）を満足する前記有理点P及びQの集合である前記部分群G_1及びG_2を特定するステップと、

前記電子計算機のCPUを自己準同型写像演算手段として機能させて、前記記憶手段から前記有理点PまたはQを読み出し、前記自己準同型写像$\phi(P)$または$\phi(Q)$を演算しその結果の有理点を前記記憶手段に記憶する自己準同型写像演算ステップと、

前記電子計算機のCPUを第1演算手段として機能させて、前記有理点P及び前記有理点Qから有理点R=P+Qを演算する第1演算ステップと、

前記電子計算機のCPUを第2演算手段として機能させて、前記有理点Rから有理点P及び有理点Qを演算する第2演算ステップと、

を有することとした。

[0029] さらに本発明の有理点情報圧縮方法では、

前記楕円曲線は、 $E: y^2 = x^3 + ax$, $a\in F_p$, $4|(p-1)$ であり、

前記合成数位数ｒは、$r|\#E(F_p)$, $4|(r-1)$ を満たし、

前記整数λ_1、λ_2は、$\lambda_1^2+1\equiv 0 \pmod r$、$\lambda_2^2+1\equiv 0 \pmod r$を満たし、

前記自己準同型写像は、$\phi: E(F_p)[r] \rightarrow E(F_p)[r]$、

$(x,y) \rightarrow (-x,\zeta y)$, $\zeta^4=1$, $\zeta, \zeta^2(\neq 1)\in F_p$ であり、

前記第２演算ステップは、前記有理点P，前記有理点Qの演算を、それぞれ

$[\lambda_1][\phi+\lambda_1]R=[-2]P$, $Q=R-P$ を用いて行うことにも特徴を有するものである。

[0030] さらに本発明の有理点情報圧縮方法では、

前記楕円曲線は、 $E:y^2 = x^3+b$, $b\in F_p$, $3|(p-1)$ であり、

前記合成数位数ｒは、$r|\#E(F_p)$, $3|(r-1)$ を満たし、

前記整数λ_1、λ_2は、$\lambda_1^2+\lambda_1+1\equiv 0(\mathrm{mod}\ r)$、$\lambda_2^2+\lambda_2+1\equiv 0(\mathrm{mod}\ r)$を満たし、

前記自己準同型写像は、$\phi:E(F_p)[r] \rightarrow E(F_p)[r]$、

$(x,y) \rightarrow (\varepsilon x,y)$, $\varepsilon^3=1$, $\varepsilon(\neq 1)\in F_p$ であり、

前記第2演算ステップは、前記有理点P，前記有理点Qの演算を、それぞれ

$[2\lambda_1+1][\phi+\lambda_1+1]R=[-3]P$, $Q=R-P$ を用いて行うことにも特徴を有するものである。

[0031] さらに本発明の有理点情報圧縮方法では、

前記楕円曲線は、 $E:y^2 = x^3+b$, $b\in F_p$, $6|(p-1)$ であり、

前記合成数位数ｒは、$r|\#E(F_p)$, $3|(r-1)$ を満たし、

前記整数λ_1、λ_2は、$\lambda_1^2+\lambda_1+1\equiv 0(\mathrm{mod}\ r)$、$\lambda_2^2+\lambda_2+1\equiv 0(\mathrm{mod}\ r)$を満たし、

前記自己準同型写像は、$\phi:E(F_p)[r] \rightarrow E(F_p)[r]$、

$(x,y) \rightarrow (\varepsilon x,-y)$, $\varepsilon^3=1$, $\varepsilon(\neq 1)\in F_p$ であり、

前記第2演算ステップは、前記有理点P，前記有理点Qの演算を、それぞれ

$[2\lambda_1-1][\phi+\lambda_1-1]R=[-3]P$, $Q=R-P$ を用いて行うことにも特徴を有するものである。

[0032] 本発明の有理点情報圧縮プログラムでは、

標数ｐの有限体F_p上で定義された楕円曲線上の有理点の成す加法群を$E(F_p)$とし、合成数位数ｒを持つ有理点の集合すなわち前記加法群の部分群を$G_1=E(F_p)[r]$、$G_2=E(F_p)[r]$として、

有理点$P\in G_1$及び有理点$Q\in G_2$の情報を送受信する場合に、CPU及び記憶手段を備えた電子計算機に行わせる有理点情報圧縮プログラムにおいて、

前記加法群$E(F_p)$は、埋め込み次数を１とし、

前記電子計算機のCPUを

有理点P’を入力して前記記憶手段に記憶する入力手段、

前記記憶手段から前記有理点P’を読み出し、自己準同型写像ϕにより、

$\lambda_1 P=\phi(P)$、$\lambda_2 Q=\phi(Q)$　（$\lambda_1 \neq \lambda_2$は整数）を満足する前記有理点P及びQの集合である前記部分群G_1及びG_2を特定する有理点部分群特定手段、

前記記憶手段から前記有理点PまたはQを読み出し、前記自己準同型写像$\phi(P)$または$\phi(Q)$を演算しその結果の有理点を前記記憶手段に記憶する自己準同型写像演算手段、

前記有理点P及び前記有理点Qから有理点R=P+Qを演算する第1演算手段、

前記有理点Rから有理点P及び有理点Qを演算する第2演算手段、

として機能させることとした。

[0033]　さらに本発明の有理点情報圧縮プログラムでは、

前記楕円曲線は、$E: y^2 = x^3 + ax$, $a \in F_p$, $4|(p-1)$ であり、

前記合成数位数ｒは、$r|\#E(F_p)$, $4|(r-1)$ を満たし、

前記整数λ_1、λ_2は、$\lambda_1^2+1 \equiv 0 \pmod r$、$\lambda_2^2+1 \equiv 0 \pmod r$を満たし、

前記自己準同型写像は、$\phi: E(F_p)[r] \rightarrow E(F_p)[r]$、

$(x,y) \rightarrow (-x, \zeta y)$, $\zeta^4=1$, $\zeta, \zeta^2(\neq 1) \in F_p$　であり、

前記第2演算手段は、前記有理点P，前記有理点Qの演算を、それぞれ

$[\lambda_1][\phi+\lambda_1]R=[-2]P$, $Q=R-P$　を用いて行うことにも特徴を有するものである。

[0034]　さらに本発明の有理点情報圧縮プログラムでは、

前記楕円曲線は、$E: y^2 = x^3 + b$, $b \in F_p$, $3|(p-1)$ であり、

前記合成数位数ｒは、$r|\#E(F_p)$, $3|(r-1)$ を満たし、

前記整数λ_1、λ_2は、$\lambda_1^2+\lambda_1+1 \equiv 0 \pmod r$、$\lambda_2^2+\lambda_2+1 \equiv 0 \pmod r$を満たし、

前記自己準同型写像は、$\phi: E(F_p)[r] \rightarrow E(F_p)[r]$、

$(x,y) \rightarrow (\varepsilon x, y)$, $\varepsilon^3=1$, $\varepsilon(\neq 1) \in F_p$　であり、

前記第2演算手段は、前記有理点P，前記有理点Qの演算を、それぞれ

$[2\lambda_1+1][\phi+\lambda_1+1]R=[-3]P$, $Q=R-P$ を用いて行うことにも特徴を有するものである。

[0035] さらに本発明の有理点情報圧縮プログラムでは、

前記楕円曲線は、 $E:y^2=x^3+b$, $b\in F_p$, $6|(p-1)$ であり、

前記合成数位数 r は、$r|\#E(F_p)$, $3|(r-1)$ を満たし、

前記整数λ_1、 λ_2は、 $\lambda_1^2+\lambda_1+1\equiv 0 \pmod r$、 $\lambda_2^2+\lambda_2+1\equiv 0 \pmod r$を満たし、

前記自己準同型写像は、 $\phi:E(F_p)[r] \rightarrow E(F_p)[r]$、

$(x,y) \rightarrow (\varepsilon x,-y)$, $\varepsilon^3=1$, $\varepsilon(\neq 1)\in F_p$ であり、

前記第2演算手段は、前記有理点P, 前記有理点Qの演算を、それぞれ

$[2\lambda_1-1][\phi+\lambda_1-1]R=[-3]P$, $Q=R-P$ を用いて行うことにも特徴を有するものである。

発明の効果

[0036] 本発明によれば、有理点P,Qの情報を送信する時に有理点Pと有理点Qの楕円加算を行い求めた有理点Rの情報を送信し、受信先で有理点Rの情報を分解し有理点P,Qの情報を復元することとなり、送受信する有理点の情報量を半分に圧縮することができる。この分解復元に要する計算は、有理点のペアあたり、おおよそスカラー倍算1回分である。このことにより、インターネット等のネットワークを介して有理点情報を送受信する際の効率化を図ることができる。

図面の簡単な説明

[0037] [図1]本発明の実施形態にかかる情報圧縮装置の概略模式図である。

[図2]本発明の実施形態にかかるクライアント装置上の情報圧縮装置の全体構成を例示したブロック図である。

[図3]本発明の実施形態にかかる認証サーバ上の情報圧縮装置の全体構成を例示したブロック図である。

[図4]本発明の実施形態にかかる有理点部分群特定部の機能構成を例示した図である。

[図5]本発明の実施形態にかかる有理点情報復元部の機能構成を例示した図で

ある。

[図6]本発明の実施形態にかかる有理点情報復元プログラムのフローチャートである。

[図7]本発明の実施形態にかかる有理点部分群特定部プログラムのフローチャートである。

発明を実施するための形態

[0038] 本発明の成果を適用できるようなペアリング曲線は、以下のような条件を満たす必要がある。まず、標数ｐの有限体F_p上で定義される楕円曲線を、

E/F_p: $y^2 = x^3 + ax + b$, $a \in F_p$ $b \in F_p$とし、

$E(F_p)$:標数ｐの有限体F_p上で定義される楕円曲線の有理点が成す加法群、

ｒ：$E(F_p)$の位数$\#E(F_p)$を割り切る合成数、

E[r]：位数が合成数ｒである有理点の集合、

ϕ:有理点に対する自己準同型写像、

ｔ：フロベニウス写像のトレース、

[j]：有理点をｊ倍する写像、

G：$G=E[r] \cap \mathrm{Ker}(\phi - \lambda)$、（$\lambda$は整数）を満たす有理点の集合、と定義する。

また、ｘ｜ｙは、ｘがｙを割り切ることを表わすものとする。

[0039] 楕円曲線の生成にはCM（Complex Multiplication）法が知られている。標数ｐ、フロベニウス自己準同型写像のトレースｔ、判別式Dによる次式のようなCM方程式において、判別式D=1,3の場合を考える。

$4p = t^2 - Ds^2$ (1)

この時、ペアリング曲線の式はそれぞれ以下のように与えられる。

E_a: $y^2 = x^3 + ax$, $a \in F_p$ (D=1) (2a)

E_b: $y^2 = x^3 + b$, $b \in F_p$ (D=3) (2b)

本発明者らは、大きな合成数位数に対してこのようなペアリング曲線を生成する簡便な生成法を提案済みである。上記のペアリング曲線上の有理点が、簡単な自己準同型写像ϕ（即ち有理点をP、整数をλとして、$\phi(P) = \lambda P$）を持つためには、パラメータの条件がある。これには、以下に示すように、自

己準同型写像の周期３，４，６に対応して3次、4次、6次の3つの場合がある。この自己準同型写像はスカラー倍算、ペアリングに用いる他、本発明では、この自己準同型写像を有理点情報の圧縮・復元に用いる。以下に、パラメータの条件及びその写像を示す。

[0040] ＜3次の場合＞

楕円曲線のパラメータが、$3|(p-1)$, $E: y^2=x^3+b$, $b\in F_p$, D=3の場合、$r|\#E(F_p)$, $3|(r-1)$ を満たす合成数ｒに対して、次式を満足するある整数λ_3が存在する。

$\lambda_3^2+\lambda_3+1\equiv 0 \pmod r$ (3)

また、以下に示す周期３の自己準同型写像ψ_3が与えられる。

[数1]

$$\psi_3: E(F_p)[r] \to E(F_p)[r], \tag{4a}$$

$$(x,y) \longmapsto (\varepsilon x, y),\ \varepsilon^3=1,\ \varepsilon(\neq 1)\in F_p. \tag{4b}$$

このような合成数ｒを位数として持つ有理点を$P\in E(F_p)[r]$とすれば、3次の場合、$[\lambda_3]P=\psi_3(P)$の関係を用いることで後述の有理点情報圧縮の効率化を図っている。

[0041] しかしながら、有理点群の埋め込み次数が１の場合、一般の有理点$P'\in E(F_p)[r]$に対しては、$[\lambda_3]P'=\psi_3(P')$は成り立たない。上述したように、これを満たすような有理点の割合は$1/r=1/2^{2000}$ であり、簡便にそのような有理点及び有理点部分群を準備できる必要がある。

[0042] 本発明では、本発明者らが発見した以下の性質を用いる。

まず、任意の有理点$P'\in E(F_p)[r]$は次式を満たす。

$[(\psi_3-\lambda_3)(\psi_3+\lambda_3+1)]P'=0$ (5)

ここで、0は、無限遠点を示す。以下の記述においても同様である。

すなわち、ランダムに生成した有理点$P'\in E(F_p)[r]$を$(\psi_3+\lambda_3+1)$倍し、

$P=[\psi_3+\lambda_3+1]P'$ (6)

とすることにより、その有理点Pは$[\lambda_3]P=\psi_3(P)$を満たすこととなる。そし

て、そのようなPが生成する有理点部分群をG_1 とする。また逆に、

$Q=[\phi_3 - \lambda_3]P'$ (7)

とすれば、$[\lambda_3 +1]Q= -\phi_3(Q)$を満たす有理点Qとなる。そして、そのようなQが生成する有理点部分群をG_2 とする。これらG_1 及びG_2 を用いて後述の有理点情報の圧縮・復元を実現することができる。

[0043] ＜関係式の導出法の説明＞

3次の場合の式(5)の導出について以下に説明する。

まず、任意の有理点$P' \in E(F_p)[r]$は、$E(F_p)$のフロベニウス写像のトレースt及びフロベニウス写像ϕを用いて、次式を満たすことが知られている。

$\phi:(x,y)\rightarrow(x^p,y^p)$

$(\phi^2 - t\phi+[p])P' = 0$ (8)

同様に、P’をE(F_p)と同型な群を内包する拡大体上ツイスト曲線E’(F_{p^3})に写像した有理点P~を考えれば、E’(F_p)のフロベニウス写像のトレースをt’として次式を満たす。

$(\phi^2 - t'\phi+[p])P^{\sim}= 0$ (9)

ここで、ツイスト曲線は、$E': y^2 = x^3+bv^{-2}, b\in F_p$で与えられ、vは$F_p$の３乗非剰余な元であり、P~は、P’=(x,y)として以下で与えられる。

$P^{\sim} = (xv^{2/3}, yv)$ (10)

ここで、上式を写像ϕ: $P' \in E(F_p)\rightarrow P^{\sim}\in E'(F_{p^3})$とすれば、式(9)は次式のように変形できる。

$\{(\phi^{-1}\phi^2\phi) - t'(\phi^{-1}\phi\phi) +[p]\}P' = 0$ (11)

そしてこの場合、$\phi^{-1}\phi\phi=\phi_3$が成り立つので次式を得る。

$(\phi_3^2 - t'\phi_3+[p])P' = 0$ (12)

上式に対して、有理点群の埋め込み次数が１であることから$p\equiv 1 \pmod r$であり、加えてこれに用いる楕円曲線を$t' \equiv -1$(3次)、0(4次)、1(6次) (mod r) となるように生成していることから、$P' \in E(F_p)[r]$ （位数ｒの有理点）とすれば、３次のときには次式を得る。

$(\phi_3^2 + \phi_3+[1])P' = 0$ (13)

一方で3次の場合には、式(3)を満たすような整数λ_3も存在し、すなわち$\phi_3^2+\phi_3+1\equiv 0 \pmod r$を、$\phi_3$を変数とするような方程式と考えれば、その解の1つがϕ_3となる。したがって、式(5)のような因数分解された関係式が得られる。

[0044] ＜4次の場合＞

同様に、楕円曲線のパラメータが、$4|(p-1)$, $E: y^2=x^3+ax$, $a\in F_p$, $D=1$の場合、

$r|\#E(F_p)$, $4|(r-1)$ を満たす合成数rに対して、次式を満足するある整数λ_4が存在する。

$\lambda_4^2+1\equiv 0 \pmod r$ (14)

また、以下に示す周期4の自己準同型写像ϕ_4が与えられる。

[数2]

$$\psi_4: E(F_p)[r] \to E(F_p)[r], \tag{15a}$$

$$(x,y) \mapsto (-x,\zeta y),\ \zeta^4=1,\ \zeta(\neq 1)\in F_p. \tag{15b}$$

このような合成数rを位数として持つ有理点を$P\in E(F_p)[r]$とすれば、4次の場合、$[\lambda_4]P=\phi_4(P)$の関係を用いることで後述の有理点情報圧縮の効率化を図っている。

[0045] 本発明では、本発明者らが発見した以下の性質を用いる。

まず、任意の有理点$P'\in E(F_p)[r]$は次式を満たす。

$[(\phi_4-\lambda_4)(\phi_4+\lambda_4)]P'=0$ (16)

すなわち、ランダムに生成した有理点$P'\in E(F_p)[r]$を$(\phi_4+\lambda_4)$倍し、

$P=[\phi_4+\lambda_4]P'$ (17)

とすることにより、その有理点Pは$[\lambda_4]P=\phi_4(P)$を満たすこととなる。そして、そのようなPが生成する有理点部分群をG_1とする。また逆に、

$Q=[\phi_4-\lambda_4]P'$ (18)

とすれば、$[\lambda_4]Q=-\phi_4(Q)$を満たす有理点Qとなる。そして、そのようなQが生成する有理点部分群をG_2とする。これらG_1及びG_2を用いて後述の有理点情報の圧縮・復元を実現することができる。

[0046] 4次の場合の式(16)の導出については、3次の場合と同様であるので説明は省略する。

[0047] ＜６次の場合＞

さらに同様に、楕円曲線のパラメータが、6|(p-1), E: $y^2=x^3+b$, $b\in F_p$, D=3の場合、

r|#E(F_p), 3|(r-1) を満たす合成数ｒに対して、次式を満足するλ_6が存在する。

$\lambda_6^2-\lambda_6+1\equiv 0 \pmod r$ (19)

また、以下に示す周期６の自己準同型写像ϕ_6が与えられる。

[数3]

$$\psi_6: E(F_p)[r] \to E(F_p)[r], \qquad (20a)$$

$$(x,y) \longmapsto (\varepsilon x, -y),\ \varepsilon^3=1,\ \varepsilon(\neq 1)\in F_p. \qquad (20b)$$

このような位数ｒを持つ有理点をP∈E(F_p)[r]とし、6次の場合、$[\lambda_6]P=\phi_6(P)$の関係を用いることで後述の有理点情報圧縮の効率化を図っている。

[0048] 本発明では、本発明者らが発見した以下の性質を用いる。

まず、任意の有理点P’∈E(F_p)[r]は次式を満たす。

$[(\phi_6-\lambda_6)(\phi_6+\lambda_6-1)]P'=0$ (22)

すなわち、ランダムに生成した有理点P’∈E(F_p)[r]を$(\phi_6+\lambda_6-1)$倍し、

$P=[\phi_6+\lambda_6-1]P'$ (23)

とすることにより、その有理点Pは$[\lambda_6]P=\phi_6(P)$を満たすこととなる。そして、そのようなPが生成する有理点部分群をG_1 とする。また逆に、

$Q=[\phi_6-\lambda_6]P'$ (24)

とすれば、$[\lambda_6-1]Q=-\phi_6(Q)$を満たす有理点Qとなる。そして、そのようなQが生成する有理点部分群をG_2 とする。これらG_1 及びG_2 を用いて後述の有理点情報の圧縮・復元を実現することができる。

[0049] 6次の場合の式(22)の導出についても、3次の場合と同様であるので説明は省略する。

[0050] 本発明の有理点情報の圧縮装置、圧縮方法及び圧縮プログラムでは、有理

点群の埋め込み次数が１の場合において、有理点部分群G_1、G_2を特定し、2つの有理点$P \in G_1$、$Q \in G_2$ を送信する際に有理点P,Qを楕円加算して圧縮した有理点Rを送信している。受信先での元の有理点情報P,Qへの分解・復元は、上述のG_1、 G_2の特性を利用して行う。以下に4次、3次、及び6次の場合について説明する。いずれもスカラー倍算1回程度の計算で、有理点情報を分解・復元できる。

[0051] ＜4次の場合＞

まず、有理点P, Qは次式を満たす。

$[\lambda_4]P=\phi_4(P)$, $[\lambda_4]Q=-\phi_4(Q)$ (25)

すなわち、言い換えればそれぞれ次式を満たす。

$[\phi_4-\lambda_4]P=0$, $[\phi_4+\lambda_4]Q=0$ (26)

したがって、受信データR=P+Qに対して、例えば、$[\phi_4+\lambda_4]$倍算を施せば、

$[\phi_4+\lambda_4]R=[\phi_4+\lambda_4](P+Q)$

$=[\phi_4+\lambda_4]P+[\phi_4+\lambda_4]Q$

$=[\phi_4+\lambda_4]P+ 0$

$=\phi_4(P)+[\lambda_4]P$

$=[\lambda_4]P+[\lambda_4]P$

$=2[\lambda_4]P$

となり、両辺にλ_4 を乗じて、$r=\lambda_4^2+1\equiv 0$を適用すれば次式を得る。

$[\lambda_4][\phi_4+\lambda_4]R=2[\lambda_4^2]P=[-2]P$

これに$[-2^{-1} \bmod r]$倍算を施せばPを得ることができる。Qは、Q=R-Pにより求めることができる。このようにスカラー倍算1回くらいの計算量で分解・復元ができるため、情報圧縮してデータを送信することの効率化を図ることができる。

[0052] ＜3次の場合＞

まず、有理点P, Qは次式を満たす。

$[\lambda_3]P=\phi_3(P)$, $[\lambda_3+1]Q=-\phi_3(Q)$ (27)

すなわち、言い換えればそれぞれ次式を満たす。

$[\phi_3-\lambda_3]P=0,\ [\phi_3+\lambda_3+1]Q=0$ (28)

したがって、受信データR=P+Qに対して、例えば$[\phi_3+\lambda_3+1]$倍算を施せば、

$[\phi_3+\lambda_3+1]R=[\phi_3+\lambda_3+1](P+Q)$

$=[\phi_3+\lambda_3+1]P+[\phi_3+\lambda_3+1]Q$

$=[\phi_3+\lambda_3+1]P+0$

$=\phi_3(P)+[\lambda_3]P+P$

$=[2\lambda_3+1]P$

となり、両辺に$[2\lambda_3+1]$ を乗じて、$r=\lambda_3^2+\lambda_3+1\equiv 0$ を適用すれば次式を得る。

$[2\lambda_3+1][\phi_3+\lambda_3+1]R=[2\lambda_3+1]^2P$

$=[4\lambda_3^2+4\lambda_3+1]P$

$=[-3]P$ (29)

これに$[-3^{-1}\bmod r]$倍算を施せばPを得ることができる。Qは、Q=R-P により求めることができる。このようにスカラー倍算1回くらいの計算量で分解・復元ができるため、情報圧縮してデータを送信することの効率化を図ることができる。

[0053] <6次の場合>

まず、有理点P, Qは 次式を満たす。

$[\lambda_6]P=\phi_6(P),\ [\lambda_6-1]Q=-\phi_6(Q)$ (30)

すなわち、言い換えればそれぞれ次式を満たす。

$[\phi_6-\lambda_6]P=0,\ [\phi_6+\lambda_6-1]Q=0$ (31)

したがって、受信データR=P+Qに対して、例えば$[\phi_6+\lambda_6-1]$倍算を施せば、

$[\phi_6+\lambda_6-1]R=[\phi_6+\lambda_6-1](P+Q)$

$=[\phi_6+\lambda_6-1]P+[\phi_6+\lambda_6-1]Q$

$=[\phi_6+\lambda_6-1]P+0$

$=\phi_6(P)+[\lambda_6]P-P$

$=[2\lambda_6-1]P$ (32)

となり、両辺に$[2\lambda_6-1]$ を乗じて、$r=\lambda_6^2-\lambda_6+1\equiv 0$ を適用すれば次式を得る

。

$[2\lambda_6-1][\psi_6+\lambda_6-1]R=[2\lambda_6-1]^2P$

$=[4\lambda_6^2-4\lambda_6+1]P$

$=[-3]P$ (33)

これに$[-3^{-1}\mathrm{mod}\ r]$倍算を施せばPを得ることができる。Qは、Q=R-P により求めることができる。このようにスカラー倍算1回くらいの計算量で分解・復元ができるため、情報圧縮してデータを送信することの効率化を図ることができる。

[0054] 上述したように、4次の場合には、2^{-1} 倍算が、3次及び6次の場合は、3^{-1}倍算が必要となる。これらのスカラー倍算は通常のスカラー倍算よりも効率よく求めることができる。

[0055] ＜2^{-1} 倍算＞

まず、$r=\lambda_4^2+1$ に注意すれば、$2^{-1}\mathrm{mod}\ r$ は、次式で求めることができる。ここで、λ_4 が偶整数であることに注意する。

$2^{-1}=(r+1)/2$

$=(\lambda_4^2+2)/2$

$=\lambda_4\cdot(\lambda_4/2)+1$

すなわち、有理点Tに対する2^{-1} 倍算は、以下のようになる。

$[2^{-1}]T=[\lambda_4\cdot(\lambda_4/2)+1]T$

$=\psi_4([\lambda_4/2]T)+T$

すなわち、実質的には、$\lambda_4/2$ 程度の計算量で求められ、これはrのビットサイズの約半分なので計算コストは通常のスカラー倍算の半分になる。

[0056] ＜3^{-1} 倍算＞

3次の場合の3^{-1} 倍算は、$r=\lambda_3^2+\lambda_3+1$ に注意すれば以下のように求まる。

$3^{-1}=(2r+1)/3$

$=(2\lambda_3^2+2\lambda_3+3)/3$

$=(2\lambda_3(\lambda_3+1)+3)/3$

$=\lambda_3\cdot 2(\lambda_3+1)/3+1$

ただしこの場合、λ_3+1 は、３の倍数であることが条件である。

すなわち、有理点Tに対する3^{-1} 倍算は、以下のようになる。

$[3^{-1}]T=[\lambda_3\cdot 2(\lambda_3+1)/3+1]T$

$=\phi_3([2(\lambda_3+1)/3]T)+T$

すなわち、実質的には、$\lambda_3\cdot 2/3$ 程度の計算量で求められ、これはrのビットサイズの約半分なので計算コストは通常のスカラー倍算の半分になる。

[0057] 6次の場合の3^{-1}倍算は、$r=\lambda_6^2-\lambda_6+1$ に注意すれば以下のように求まる。

$3^{-1}=(2r+1)/3$

$=(2\lambda_6^2-2\lambda_6+3)/3$

$=(2\lambda_6(\lambda_6-1)+3)/3$

$=\lambda_6\cdot 2(\lambda_6-1)/3+1$

ただしこの場合、λ_6-1 は、３の倍数であることが条件である。

すなわち、有理点Tに対する3^{-1} 倍算は、以下のようになる。

$[3^{-1}]T=[\lambda_6\cdot 2(\lambda_6-1)/3+1]T$

$=\phi_6([2(\lambda_6-1)/3]T)+T$

すなわち、実質的には、$\lambda_6\cdot 2/3$ 程度の計算量で求められ、これはrのビットサイズの約半分なので計算コストは通常のスカラー倍算の半分になる。

[0058] 以下において、本発明の実施形態について、図を用いて説明する。

図１は、本発明の実施形態にかかる有理点情報圧縮装置の概略模式図である。

図２は、本発明の実施形態にかかるクライアント装置上の有理点情報圧縮装置100の全体構成を例示したブロック図である。

図3は、本発明の実施形態にかかる認証サーバ上の有理点情報圧縮装置200の全体構成を例示したブロック図である。

まず、図1、図2、及び図3を用いてこの形態の全体について説明し、次にその詳細について説明する。

なお、本実施形態では、所要の電子計算機で構成された認証サーバ及びクライアント装置によってディジタルグループ署名の認証処理を行う際に、与

えられたペアリング曲線から上述した有理点部分群を特定するプログラム、及び有理点情報を復元するプログラム部分についてのみ説明する。なお、有理点部分群の特定及び有理点情報復元の演算は、認証サーバまたは、クライアント装置で実行される場合に限定されるものではなく、少なくともCPUなどの演算手段及び記憶手段を備えた装置であれば、どのような装置であってもよい。

[0059] 図１に示すように、認証サーバまたはクライアント装置を構成する電子計算機10は、演算処理を実行するCPU11と有理点部分群特定プログラム、有理点情報復元プログラム、ペアリング演算プログラムなどの各種プログラム、及びこれらのプログラムで使用するデータなどを記憶したハードディスクなどの記憶装置12と、これらのプログラムを展開して実行可能とするとともに、これらプログラムの実行にともなって生成されたデータを一時的に記憶するRAMなどで構成されたメモリ装置13を備えている。図１中、14はバスである。

[0060] また、認証サーバを構成する電子計算機10は、インターネットなどの電気通信回線20に接続され、この電気通信回線20に接続されたクライアント装置30から送信されたディジタルグループ署名の署名データを受信可能としている。図１中、15は電子計算機10の入出力部である。

[0061] 図２に、クライアント装置上の有理点情報圧縮装置100を示す。図２に示すように、有理点情報圧縮装置100は、有理点部分群特定部110と、認証データ生成部120と、有理点情報圧縮部130と、入出力部140とを有する。

まず、ディジタルグループ署名データ（認証データ）を生成するクライアント装置では、与えられたペアリング曲線から有理点部分群G_1、G_2を特定する（有理点部分群特定部110）。次に、署名データを生成し（認証データ生成部120）、署名データを構成する有理点$P \in G_1$及び$Q \in G_2$のペアを楕円加算して有理点Rに圧縮する（有理点情報圧縮部130）。全てのペアについて圧縮した後、署名データを入出力部140より、認証サーバに向け送信する。

[0062] 図３に、認証サーバ上の有理点情報圧縮装置200を示す。図３に示すように、有理点情報圧縮装置200は、入出力部210と、有理点情報復元部220と、認証

処理部230と、認証結果データ生成部240と、有理点情報圧縮部250と、入出力部260とを有する。

認証サーバを構成する電子計算機10では、クライアント装置30からディジタルグループ署名の署名データが送信されると、入出力部210を経由して署名データを受信し、受信した署名データをメモリ装置13に一旦記憶し、有理点情報復元プログラムを起動して元の有理点のペアの情報を復元した後（有理点情報復元部220）、ペアリング演算プログラムを起動して、ペアリング演算を実行している(認証処理部230)。

その後、認証結果のデータを生成し（認証結果データ生成部240）、有理点のペアの情報を圧縮し（有理点情報圧縮部250）、入出力部260を経由してクライアント装置に向け送信している。

[0063] 次に、本実施形態の詳細について図を用いて説明する。

＜有理点部分群の特定＞

[0064] 図４は図１で示した装置で所定のプログラムを実行させることにより実現される有理点部分群特定部110の機能構成を例示した図である。

図７は有理点部分群特定部の処理を行う有理点部分群特定プログラムのフローチャートである。

電子計算機10では、起動した有理点部分群特定プログラムによって、図７に示すフローチャートに基づいて効率的な自己準同型写像を可能とする有理点部分群を特定している。すなわち、入力された、有理点群が埋め込み次数１の一般の有理点を特定の有理点部分群内の有理点に変換している。この場合電子計算機10は有理点部分群特定手段として機能する。以下では、3次の場合について説明する。

[0065] ステップ T1（有理点入力部111）では、外部から与えられ入力手段により記憶手段に記憶された一般の有理点P’を読み出している。

ステップ T2（定数演算部112）では、あらかじめレジスタ119に記憶された有限体の標数ｐ及び合成数位数ｒとを用いて、式（３）で示した$\lambda^2+\lambda+1\equiv 0 \pmod r$となるλ及び、式（４ｂ）で示した$\varepsilon^3\equiv 1 \pmod p$となるε(

≠1)を演算し設定している。

ステップ T3（自己準同型写像演算部113）では、式（４ｂ）の$\phi(P')$:(x,y)→(εx,y)として、P’のｘ座標値ｘをε倍し、$\phi(P')$を求めている。

ステップ T4（有理点演算部114）では、式（６）のP=$\phi(P')$+(λ+1)P’を計算している。

ステップ T5（判定部115）では、P=0 （無限遠点） かどうかを判定している。

P=0 の場合は、2つの部分群を特定できないのでエラー・リターンしている（発生確率は、$1/2^{2000}$程度である。）。

ステップ T6（有理点演算部114)では、式（７）のQ=$\phi(P')$+(-λ)P’を計算している。

ステップ T7(判定部115)では、Q=0 （無限遠点）かどうかを判定している。

Q=0 の場合は2つの部分群を特定できないのでエラー・リターンしている（発生確率は、$1/2^{2000}$程度である。）。

ステップ T8では、P、Qを記憶手段に記憶している。Pの集合が有理点部分群G_1となり、Qの集合が有理点部分群G_2となる。

[0066] 本実施形態では、3次の場合について説明したが、4次,及び6次の場合も、λ、$\phi(P')$、εまたはζ、P、Qがそれぞれ

4次では、式(14)：$\lambda^2+1\equiv 0 \pmod r$、

式(15b)：$\phi(P')$:(x,y)→(-x,ζy)，($\zeta^4=1$, ζ, $\zeta^2(\neq 1)\in F_p$)、

式(17) ：P=$\phi(P')$ +λP’、

式(18)：Q=$\phi(P')$ +(-λ)P’

となり、

6次では、式(19)：$\lambda^2-\lambda+1\equiv 0 \pmod r$、

式(20b)：$\phi(P')$:(x,y)→(εx,-y)，($\varepsilon^3=1$, $\varepsilon(\neq 1)\in F_p$)、

式(23)：P=$\phi(P')$ +(λ-1)P’、

式(24)：Q=$\phi(P')$ +(-λ)P’

となるだけであり、同様に有理点部分群を特定することができる（説明は省略する。）。

[0067] ＜有理点情報の圧縮＞

有理点$P \in G_1$, $Q \in G_2$の圧縮はこれらの有理点を楕円加算して有理点Rとすることにより行う。これにより、有理点のデータ長は半分となる。

[0068] ＜有理点情報の復元＞

図５は図１で示した装置で所定のプログラムを実行させることにより実現される有理点情報復元部220の機能構成を例示した図である。

図６は有理点情報復元部の処理を行う有理点復元プログラムのフローチャートである（4次の場合）。

電子計算機10では、起動した有理点復元プログラムによって、図６に示すフローチャートに基づいて有理点Rから有理点P, Qを求めている。この場合電子計算機10は第2演算手段として機能する。以下では、４次の場合について説明する。

[0069] まず、有理点Rを入力し、メモリ手段13に記憶する。（ステップ S1、パラメータ入力部221）

次に、

$T_1=[\lambda_4][\phi_4+\lambda_4]R$

を計算する。（ステップ S2、レジスタ229、定数演算部222、自己準同型写像演算部224）

次に、

$P=-[2^{-1}]T_1$

を計算する。（ステップS3、2^{-1}演算部223、有理点演算部225）

次に、

$Q=R-P$

を計算する。（ステップS4、有理点演算部225）

[0070] 2^{-1}倍算は、具体的には、以下のアルゴリズムを実行している。

［表１］4次の場合の2^{-1}倍算アルゴリズム

入力：λ_4、$T_1 \in G_1$

出力：$[2^{-1}]T_1$

1. $T \leftarrow [\lambda_4/2]T_1$

2. $T \leftarrow \phi_4(T)+T_1$

3. Return T

すなわち、ステップ１では、有理点T_1の$[\lambda_4/2]$倍算を実行し、Tに代入している。ステップ２では、ステップ１で求めたTの自己準同型写像ϕ_4を実行し、有理点T_1を加算してTに代入している。ステップ３では戻り値をTとしてリターンしている。

[0071] 4次の場合の有理点の復元は、具体的には、以下のアルゴリズムを実行している。

［表２］4次の場合有理点復元アルゴリズム

入力：λ_4、$R=P+Q$, $P \in G_1$, $Q \in G_2$

出力：P, Q

1. $T_1 \leftarrow \phi_4(R)$

2. $T_1 \leftarrow [\lambda_4]T_1-R$

3. $P \leftarrow -[2^{-1}]T_1$

4. $Q \leftarrow R-P$

5. Return P, Q

すなわち、ステップ1では、有理点Rの自己準同型写像ϕ_4を実行し、T_1に代入している。ステップ２では、有理点T_1の$[\lambda_4]$倍算を実行し、次に-Rを楕円加算してT_1に代入している。ステップ３では、［表１］のアルゴリズムを実行し、符号をマイナスにしてPを求めている。ステップ４では、Rと-Pを楕円加算してQを求めている。ステップ5では、P, Qを戻り値としてリターンしている。

[0072] 次に3次の場合について説明する。

3次の場合の3^{-1}倍算は、具体的には、以下のアルゴリズムを実行している。

［表３］３次の場合の3^{-1}倍算アルゴリズム

入力：λ_3、$T_1 \in G_1$

出力：$[3^{-1}]T_1$

1. $T \leftarrow [2(\lambda_3+1)/3]T_1$

2. $T \leftarrow \phi_3(T)+T_1$

3. Return T

すなわち、ステップ１では、有理点T_1の$[2(\lambda_3+1)/3]$倍算を実行し、Tに代入している。ステップ２では、ステップ１で求めたTの自己準同型写像ϕ_3を実行し、有理点T_1を加算してTに代入している。ステップ３では戻り値をTとしてリターンしている。

[0073] 3次の場合の有理点の復元は、具体的には、以下のアルゴリズムを実行している。

［表４］3次の場合有理点復元アルゴリズム

入力：λ_3、$R=P+Q$, $P \in G_1$, $Q \in G_2$

出力：P, Q

1. $T_1 \leftarrow \phi_3(R)$

2. $T_2 \leftarrow 2T_1+R$

3. $T_2 \leftarrow [\lambda_3]T_2$

4. $T_1 \leftarrow T_2+T_1-R$

5. $P \leftarrow -[3^{-1}]T_1$

6. $Q \leftarrow R-P$

7. Return P, Q

すなわち、ステップ1では、有理点Rの自己準同型写像ϕ_3を行い、T_1に代入している。ステップ２では、有理点T_1の2倍算を実行し、次にRを楕円加算してT_2に代入している。ステップ３では、有理点T_2の$[\lambda_3]$倍算を行いT_2に代入している。ステップ4では、T_2, T_1, -Rを楕円加算してT_1に代入している。ステップ5では、［表３］のアルゴリズムを実行し、符号をマイナスにしてPを求めている。ステップ６では、Rと-Pを楕円加算してQを求めている。ステップ7では、P, Qを戻り値としてリターンしている。

[0074] 次に６次の場合について説明する。

6次の場合の3^{-1}倍算は、具体的には、以下のアルゴリズムを実行している。

［表５］６次の場合の3^{-1}倍算アルゴリズム

入力：λ_6、$T_1 \in G_1$

出力：$[3^{-1}]T_1$

1. $T \leftarrow [2(\lambda_6-1)/3]T_1$
2. $T \leftarrow \phi_6(T)+T_1$
3. Return T

すなわち、ステップ１では、有理点T_1の$[2(\lambda_6-1)/3]$倍算を実行し、Tに代入している。ステップ２では、ステップ１で求めたTの自己準同型写像ϕ_6を実行し、有理点T_1を加算してTに代入している。ステップ３では戻り値をTとしてリターンしている。

[0075] 6次の場合の有理点の復元は、具体的には、以下のアルゴリズムを実行している。

［表6］6次の場合の有理点復元アルゴリズム

入力：λ_6、$R=P+Q$, $P \in G_1$, $Q \in G_2$

出力：P, Q

1. $T_1 \leftarrow \phi_6(R)$
2. $T_2 \leftarrow 2T_1-R$
3. $T_2 \leftarrow [\lambda_6]T_2$
4. $T_1 \leftarrow T_2-T_1-R$
5. $P \leftarrow -[3^{-1}]T_1$
6. $Q \leftarrow R-P$
7. Return P, Q

すなわち、ステップ1では、有理点Rの自己準同型写像ϕ_6を実行し、T_1に代入している。ステップ２では、有理点T_1の2倍算を実行し、次に-Rを楕円加算してT_2に代入している。ステップ３では、有理点T_2の$[\lambda_6]$倍算を行いT_2に代入している。ステップ4では、T_2, $-T_1$, -Rを楕円加算してT_1に代入している。ス

テップ5では、［表５］のアルゴリズムを実行し、符号をマイナスにしてPを求めている。ステップ６では、Rと-Pを楕円加算してQを求めている。ステップ7では、P，Qを戻り値としてリターンしている。

符号の説明

[0076] 10 電子計算機

11 CPU

12 記憶装置

13 メモリ装置

14 バス

15 入出力部

20 電気通信回線

30 クライアント装置

100 有理点情報圧縮装置

110 有理点部分群特定部

111 有理点入力部

112 定数演算部

113 自己準同型写像演算部

114 有理点演算部

115 判定部

119 レジスタ

120 認証データ生成部

130 有理点情報圧縮部

140 入出力部

200 有理点情報圧縮装置

210 入出力部

220 有理点情報復元部

221 パラメータ入力部

222 定数演算部

223 2^{-1}演算部

224 自己準同型写像演算部

225 有理点演算部

229 レジスタ

230 認証処理部

240 認証結果データ生成部

250 有理点情報圧縮部

260 入出力部

請求の範囲

[請求項1] 標数ｐの有限体F_p上で定義された楕円曲線上の有理点の成す加法群を$E(F_p)$とし、合成数位数ｒを持つ有理点の集合すなわち前記加法群の部分群を$G_1=E(F_p)[r]$、$G_2=E(F_p)[r]$として、

有理点$P\in G_1$及び有理点$Q\in G_2$の情報を送受信するCPU及び記憶手段を備えた有理点情報圧縮装置において、

前記加法群$E(F_p)$は、埋め込み次数を１とし、

前記電子計算機のCPUは、

有理点P’を入力して前記記憶手段に記憶する入力手段と、

前記電子計算機のCPUを有理点部分群特定手段として機能させて、前記記憶手段から前記有理点P’を読み出し、自己準同型写像ϕにより、

$\lambda_1 P=\phi(P)$、$\lambda_2 Q=\phi(Q)$ （$\lambda_1\neq\lambda_2$は整数）を満足する前記有理点P及びQの集合である前記部分群G_1及びG_2を特定する有理点部分群特定手段と、

前記記憶手段から前記有理点PまたはQを読み出し、前記自己準同型写像$\phi(P)$ または$\phi(Q)$を演算しその結果の有理点を前記記憶手段に記憶する自己準同型写像演算手段と、

前記有理点P及び前記有理点Qから有理点R＝P+Qを演算する第1演算手段と、

前記有理点Rから有理点P及び有理点Qを演算する第2演算手段と、

を有する有理点情報圧縮装置。

[請求項2] 前記楕円曲線は、 $E: y^2 = x^3 + ax$, $a\in F_p$, $4|(p-1)$ であり、

前記合成数位数ｒは、$r|\#E(F_p)$, $4|(r-1)$ を満たし、

前記整数λ_1、λ_2は、$\lambda_1^2+1\equiv 0 \pmod r$、$\lambda_2^2+1\equiv 0 \pmod r$を満たし、

前記自己準同型写像は、$\phi: E(F_p)[r] \rightarrow E(F_p)[r]$、

$(x,y) \rightarrow (-x, \zeta y)$, $\zeta^4=1$, $\zeta, \zeta^2(\neq 1)\in F_p$ であり、

前記第2演算手段は、前記有理点P, 前記有理点Qの演算を、それぞれ

$[\lambda_1][\phi+\lambda_1]R=[-2]P$, $Q=R-P$ を用いて行う請求項１に記載の有理点情報圧縮装置。

[請求項3] 前記楕円曲線は、 $E:y^2 = x^3+b$, $b\in F_p$, $3|(p-1)$ であり、

前記合成数位数ｒは、$r|\#E(F_p)$, $3|(r-1)$ を満たし、

前記整数λ_1、λ_2は、$\lambda_1^2+\lambda_1+1\equiv 0 \pmod r$、$\lambda_2^2+\lambda_2+1\equiv 0 \pmod r$を満たし、

前記自己準同型写像は、$\phi:E(F_p)[r] \rightarrow E(F_p)[r]$、

$(x,y) \rightarrow (\varepsilon x, y)$, $\varepsilon^3=1$, $\varepsilon(\neq 1)\in F_p$ であり、

前記第2演算手段は、前記有理点P, 前記有理点Qの演算を、それぞれ $[2\lambda_1+1][\phi+\lambda_1+1]R=[-3]P$, $Q=R-P$ を用いて行う請求項１に記載の有理点情報圧縮装置。

[請求項4] 前記楕円曲線は、 $E:y^2 = x^3+b$, $b\in F_p$, $6|(p-1)$ であり、

前記合成数位数ｒは、$r|\#E(F_p)$, $3|(r-1)$ を満たし、

前記整数λ_1、λ_2は、$\lambda_1^2-\lambda_1+1\equiv 0 \pmod r$、$\lambda_2^2-\lambda_2+1\equiv 0 \pmod r$を満たし、

前記自己準同型写像は、$\phi:E(F_p)[r] \rightarrow E(F_p)[r]$、

$(x,y) \rightarrow (\varepsilon x, -y)$, $\varepsilon^3=1$, $\varepsilon(\neq 1)\in F_p$ であり、

前記第2演算手段は、前記有理点P, 前記有理点Qの演算を、それぞれ $[2\lambda_1-1][\phi+\lambda_1-1]R=[-3]P$, $Q=R-P$ を用いて行う請求項１に記載の有理点情報圧縮装置。

[請求項5] 標数ｐの有限体F_p上で定義された楕円曲線上の有理点の成す加法群を$E(F_p)$とし、合成数位数ｒを持つ有理点の集合すなわち前記加法群の部分群を$G_1=E(F_p)[r]$、$G_2=E(F_p)[r]$として、

有理点$P\in G_1$及び有理点$Q\in G_2$の情報を送受信する場合に、CPU及び記憶手段を備えた電子計算機で行う情報圧縮方法において、

前記加法群$E(F_p)$は、埋め込み次数を１とし、

前記電子計算機のCPUを入力手段として機能させて、有理点P’を入力して前記記憶手段に記憶する入力ステップと、

前記電子計算機のCPUを有理点部分群特定手段として機能させて、前記記憶手段から前記有理点P’を読み出し、自己準同型写像ϕにより、

$\lambda_1 P=\phi(P)$、$\lambda_2 Q=\phi(Q)$ （$\lambda_1 \neq \lambda_2$は整数）を満足する前記有理点P及びQの集合である前記部分群G_1及びG_2を特定するステップと、

前記電子計算機のCPUを自己準同型写像演算手段として機能させて、前記記憶手段から前記有理点PまたはQを読み出し、前記自己準同型写像$\phi(P)$ または$\phi(Q)$を演算しその結果の有理点を前記記憶手段に記憶する自己準同型写像演算ステップと、

前記電子計算機のCPUを第1演算手段として機能させて、前記有理点P及び前記有理点Qから有理点R=P+Qを演算する第1演算ステップと、

前記電子計算機のCPUを第2演算手段として機能させて、前記有理点Rから有理点P及び有理点Qを演算する第2演算ステップと、

を有する有理点情報圧縮方法。

[請求項6] 前記楕円曲線は、 $E: y^2 = x^3 + ax$, $a \in F_p$, $4 | (p-1)$ であり、

前記合成数位数 r は、$r | \#E(F_p)$, $4 | (r-1)$ を満たし、

前記整数λ_1、λ_2は、$\lambda_1^2+1 \equiv 0 \pmod r$、$\lambda_2^2+1 \equiv 0 \pmod r$を満たし、

前記自己準同型写像は、$\phi: E(F_p)[r] \rightarrow E(F_p)[r]$、

$(x,y) \rightarrow (-x, \zeta y)$, $\zeta^4=1$, $\zeta, \zeta^2 (\neq 1) \in F_p$ であり、

前記第２演算ステップは、前記有理点P, 前記有理点Qの演算を、それぞれ

$[\lambda_1][\phi+\lambda_1]R=[-2]P$, $Q=R-P$ を用いて行う請求項５に記載の有理点情報圧縮方法。

[請求項7] 前記楕円曲線は、 $E: y^2 = x^3 + b$, $b \in F_p$, $3 | (p-1)$ であり、

前記合成数位数 r は、$r | \#E(F_p)$, $3 | (r-1)$ を満たし、

前記整数λ_1、λ_2は、$\lambda_1^2+\lambda_1+1 \equiv 0 \pmod r$、$\lambda_2^2+\lambda_2+1 \equiv 0 \pmod r$を満たし、

前記自己準同型写像は、$\phi: E(F_p)[r] \rightarrow E(F_p)[r]$、

$(x,y) \rightarrow (\varepsilon x, y)$, $\varepsilon^3=1$, $\varepsilon(\neq 1)\in F_p$ であり、

前記第2演算ステップは、前記有理点P，前記有理点Qの演算を、それぞれ

$[2\lambda_1+1][\phi+\lambda_1+1]R=[-3]P$, $Q=R-P$ を用いて行う請求項５に記載の有理点情報圧縮方法。

[請求項8] 前記楕円曲線は、 $E: y^2 = x^3+b$, $b\in F_p$, $6|(p-1)$ であり、

前記合成数位数ｒは、$r|\#E(F_p)$, $3|(r-1)$ を満たし、

前記整数λ_1、λ_2は、$\lambda_1^2+\lambda_1+1\equiv 0 \pmod r$、$\lambda_2^2+\lambda_2+1\equiv 0 \pmod r$を満たし、

前記自己準同型写像は、$\phi: E(F_p)[r] \rightarrow E(F_p)[r]$、

$(x,y) \rightarrow (\varepsilon x, -y)$, $\varepsilon^3=1$, $\varepsilon(\neq 1)\in F_p$ であり、

前記第2演算ステップは、前記有理点P，前記有理点Qの演算を、それぞれ

$[2\lambda_1-1][\phi+\lambda_1-1]R=[-3]P$, $Q=R-P$ を用いて行う請求項５に記載の有理点情報圧縮方法。

[請求項9] 標数ｐの有限体F_p上で定義された楕円曲線上の有理点の成す加法群を$E(F_p)$とし、合成数位数ｒを持つ有理点の集合すなわち前記加法群の部分群を$G_1=E(F_p)[r]$、$G_2=E(F_p)[r]$として、

有理点$P\in G_1$及び有理点$Q\in G_2$の情報を送受信する場合に、CPU及び記憶手段を備えた電子計算機に行わせる有理点情報圧縮プログラムにおいて、

前記加法群$E(F_p)$は、埋め込み次数を１とし、

前記電子計算機のCPUを

有理点P’を入力して前記記憶手段に記憶する入力手段、

前記記憶手段から前記有理点P’を読み出し、自己準同型写像ϕにより、

$\lambda_1P=\phi(P)$、$\lambda_2Q=\phi(Q)$ （$\lambda_1\neq\lambda_2$は整数）を満足する前記有理点P及びQの集合である前記部分群G_1及びG_2を特定する有理点部分群特定

手段、

前記記憶手段から前記有理点PまたはQを読み出し、前記自己準同型写像$\phi(P)$または$\phi(Q)$を演算しその結果の有理点を前記記憶手段に記憶する自己準同型写像演算手段、

前記有理点P及び前記有理点Qから有理点R=P+Qを演算する第1演算手段、

前記有理点Rから有理点P及び有理点Qを演算する第2演算手段、

として機能させる有理点情報圧縮プログラム。

[請求項10] 前記楕円曲線は、 $E:y^2 = x^3 +ax$, $a\in F_p$, $4|(p-1)$ であり、

前記合成数位数 r は、$r|\#E(F_p)$, $4|(r-1)$ を満たし、

前記整数λ_1、λ_2は、$\lambda_1^2+1\equiv 0(\mathrm{mod}\ r)$、$\lambda_2^2+1\equiv 0(\mathrm{mod}\ r)$ を満たし、

前記自己準同型写像は、$\phi:E(F_p)[r] \rightarrow E(F_p)[r]$、

$(x,y) \rightarrow (-x,\zeta y)$, $\zeta^4=1$, $\zeta, \zeta^2(\neq 1)\in F_p$ であり、

前記第2演算手段は、前記有理点P, 前記有理点Qの演算を、それぞれ$[\lambda_1][\phi+\lambda_1]R=[-2]P$, $Q=R-P$ を用いて行う請求項９に記載の有理点情報圧縮プログラム。

[請求項11] 前記楕円曲線は、 $E:y^2 = x^3 +b$, $b\in F_p$, $3|(p-1)$ であり、

前記合成数位数 r は、$r|\#E(F_p)$, $3|(r-1)$ を満たし、

前記整数λ_1、λ_2は、$\lambda_1^2+\lambda_1+1\equiv 0(\mathrm{mod}\ r)$、$\lambda_2^2+\lambda_2+1\equiv 0(\mathrm{mod}\ r)$を満たし、

前記自己準同型写像は、$\phi:E(F_p)[r] \rightarrow E(F_p)[r]$、

$(x,y) \rightarrow (\varepsilon x,y)$, $\varepsilon^3=1$, $\varepsilon(\neq 1)\in F_p$ であり、

前記第2演算手段は、前記有理点P, 前記有理点Qの演算を、それぞれ$[2\lambda_1+1][\phi+\lambda_1+1]R=[-3]P$, $Q=R-P$ を用いて行う請求項９に記載の有理点情報圧縮プログラム。

[請求項12] 前記楕円曲線は、 $E:y^2 = x^3 +b$, $b\in F_p$, $6|(p-1)$ であり、

前記合成数位数 r は、$r|\#E(F_p)$, $3|(r-1)$ を満たし、

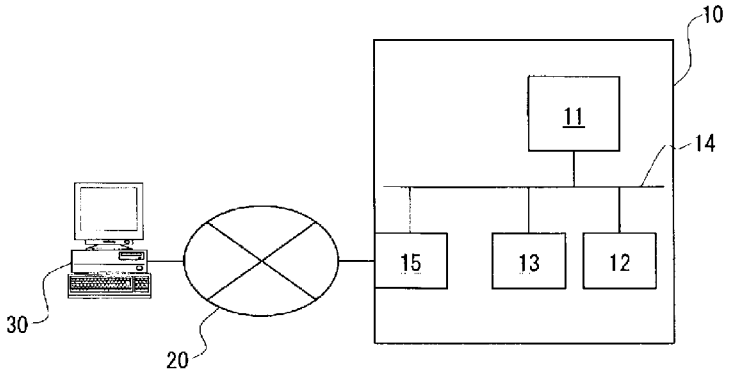
前記整数λ_1、λ_2は、$\lambda_1^2+\lambda_1+1\equiv 0 \pmod r$、$\lambda_2^2+\lambda_2+1\equiv 0 \pmod r$を満たし、

前記自己準同型写像は、$\phi : E(F_p)[r] \rightarrow E(F_p)[r]$、

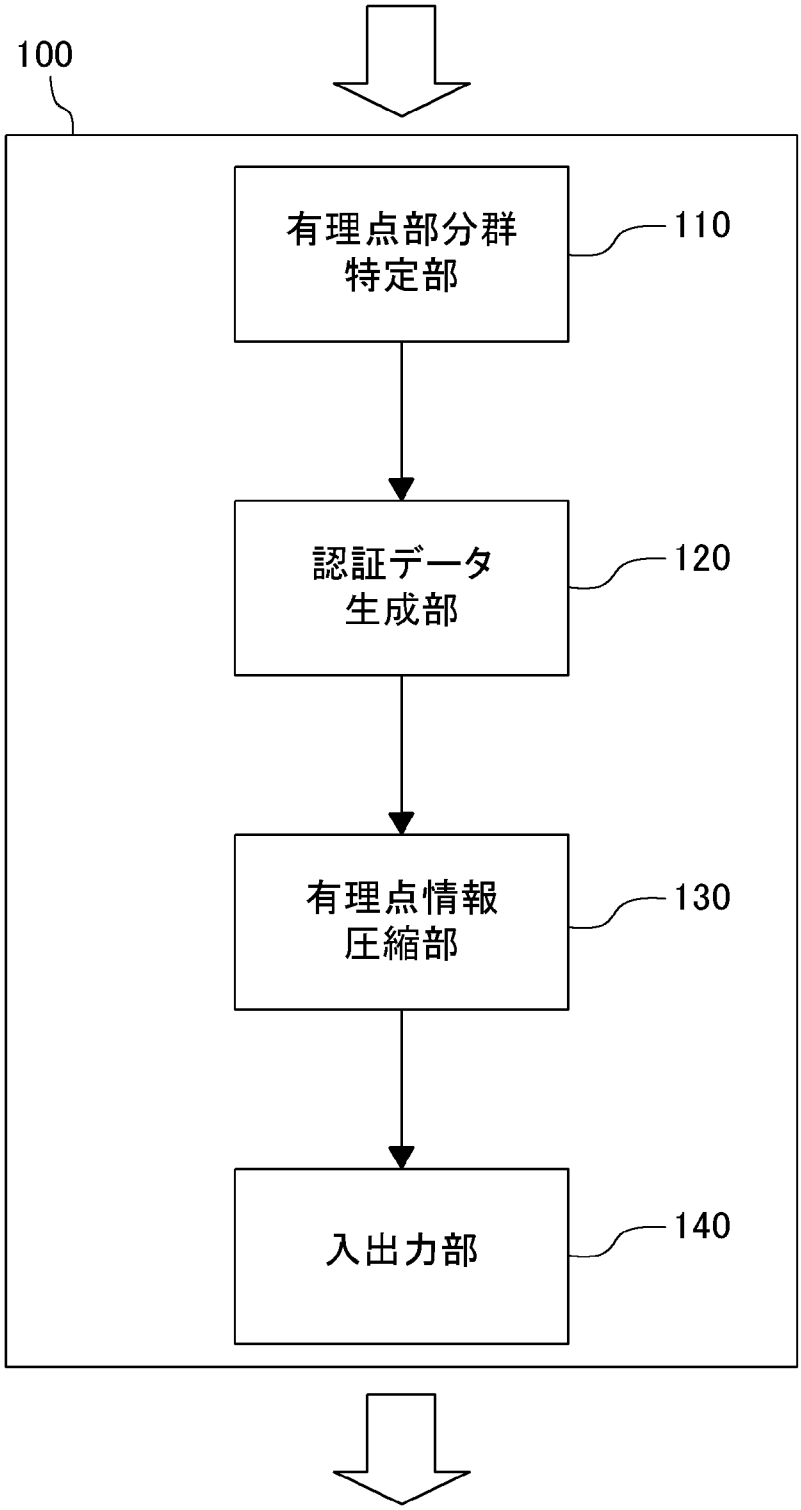
$(x, y) \rightarrow (\varepsilon x, -y)$, $\varepsilon^3=1$, $\varepsilon(\neq 1)\in F_p$ であり、

前記第2演算手段は、前記有理点P，前記有理点Qの演算を、それぞれ$[2\lambda_1-1][\phi+\lambda_1-1]R=[-3]P$, $Q=R-P$ を用いて行う請求項９に記載の有理点情報圧縮プログラム。

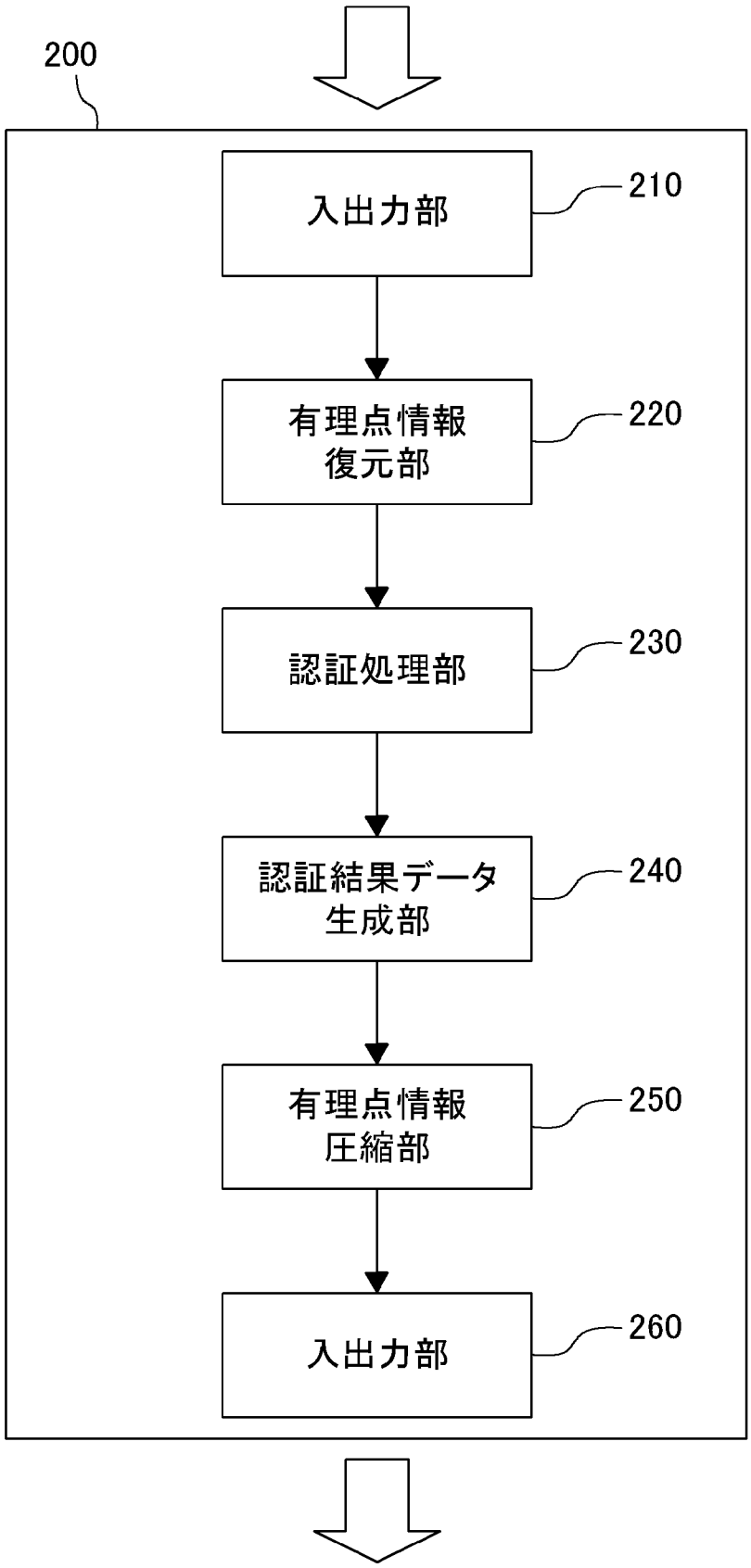
[図1]



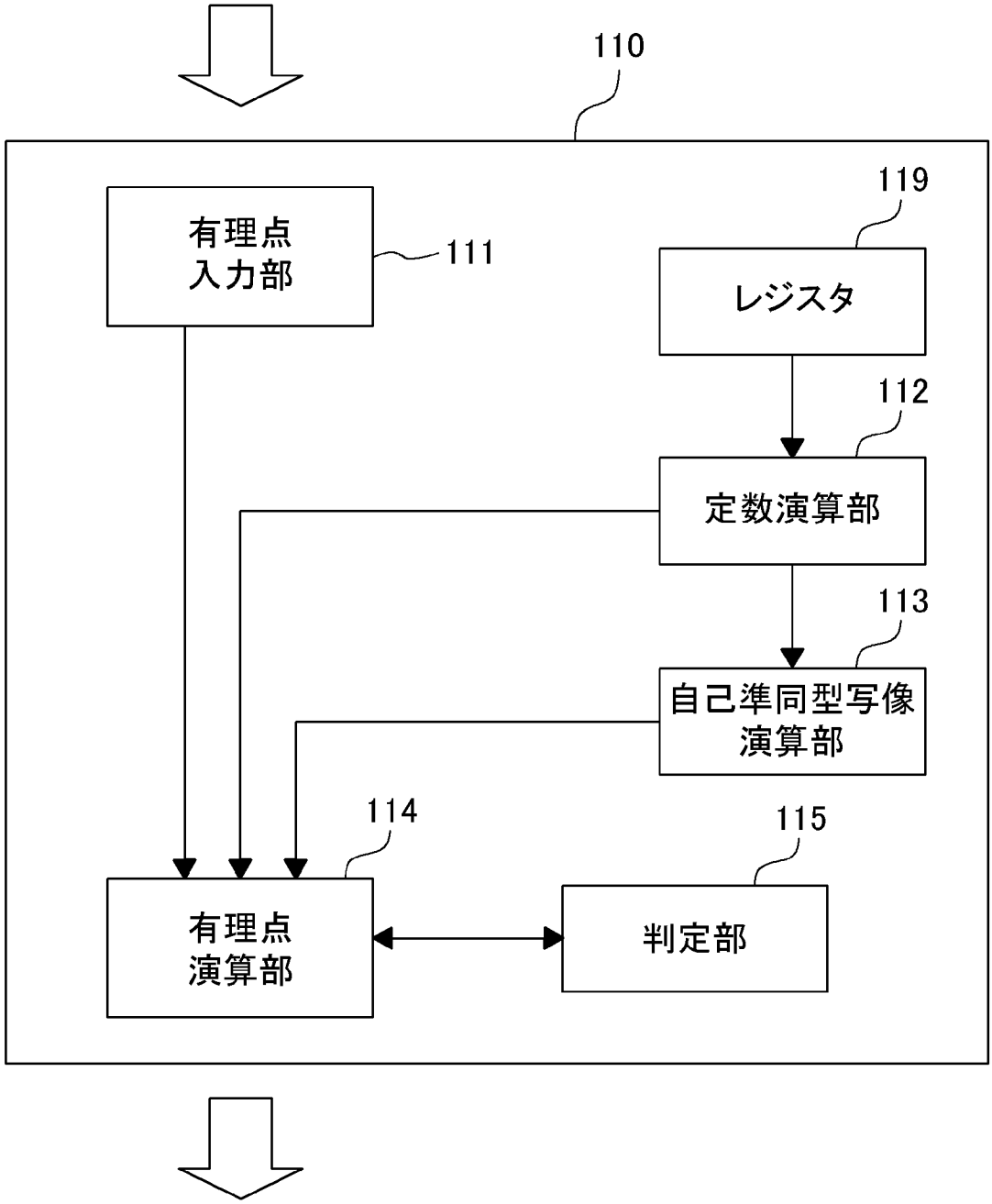
[図2]



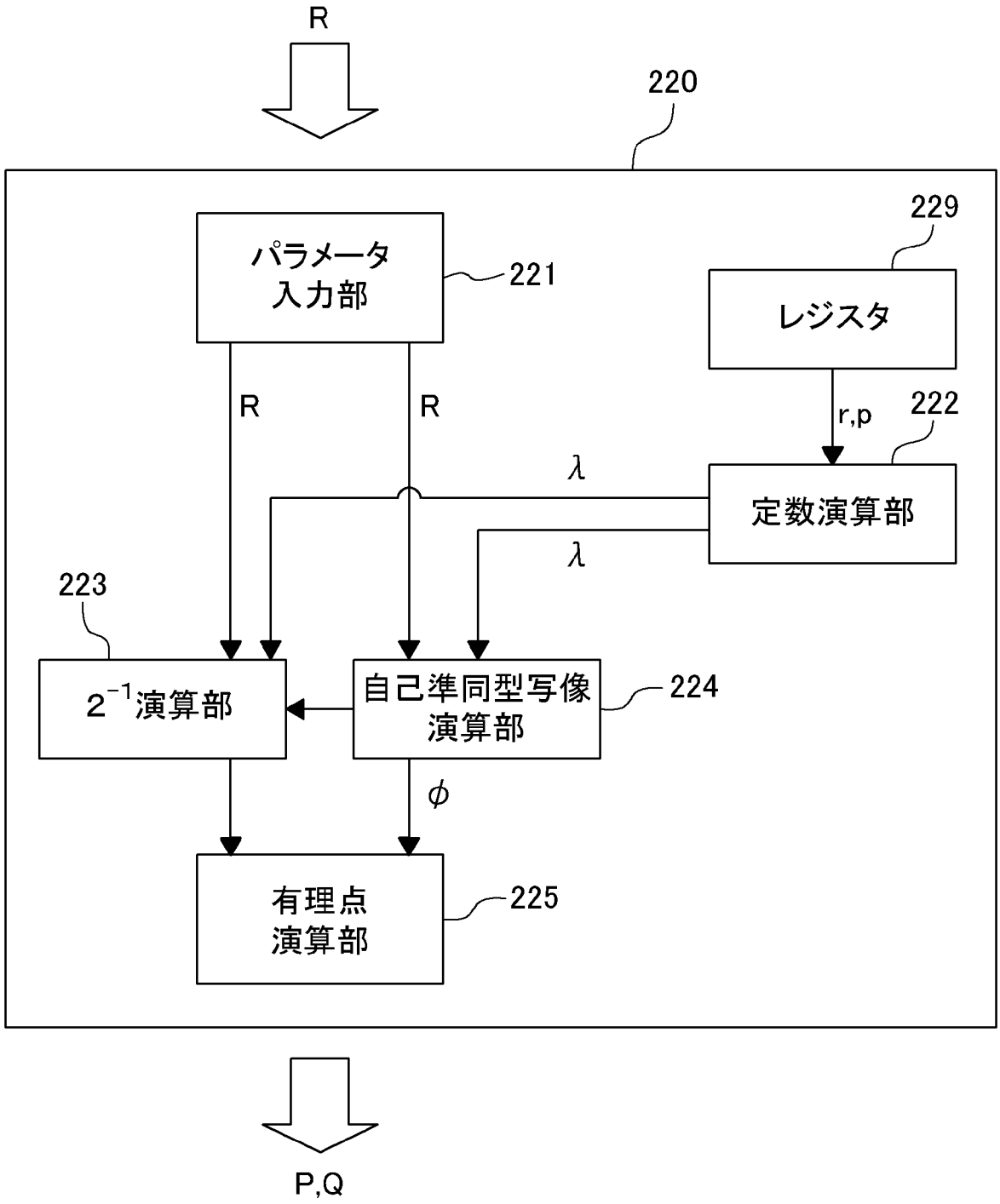
[図3]


200
入出力部
210
有理点情報
復元部
220
認証処理部
230
認証結果データ
生成部
240
有理点情報
圧縮部
250
入出力部
260

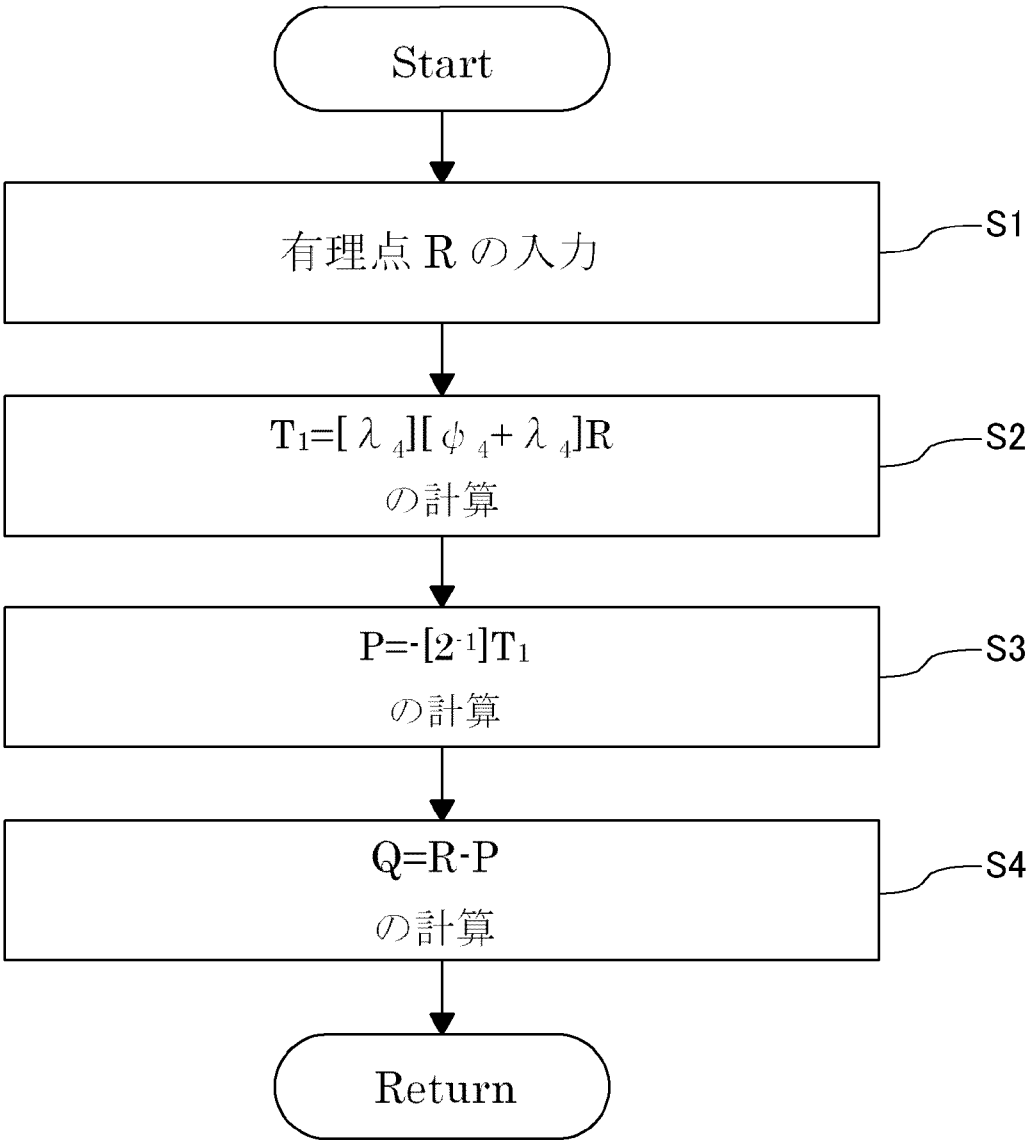
[図4]


110
有理点
入力部
111
119
レジスタ
112
定数演算部
113
自己準同型写像
演算部
114
有理点
演算部
115
判定部

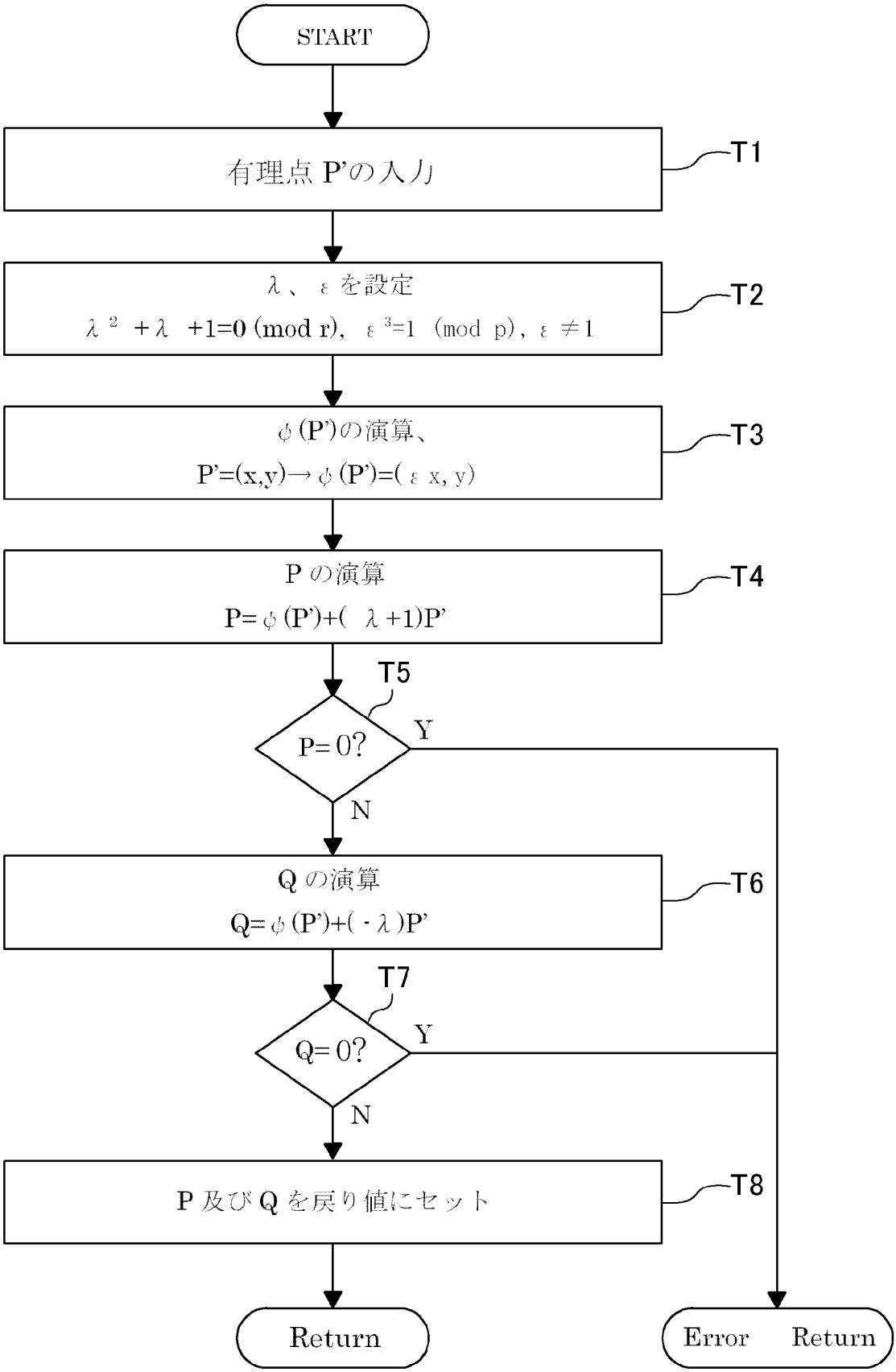
[図5]


R
220
229
パラメータ
入力部
221
レジスタ
R
R
r,p
222
λ
定数演算部
λ
223
2^{-1}演算部
自己準同型写像
演算部
224
φ
有理点
演算部
225
P,Q

[図6]


Start
有理点Rの入力
S1
$T_1=[\lambda_4][\phi_4+\lambda_4]R$
の計算
S2
$P=-[2^{-1}]T_1$
の計算
S3
Q=R-P
の計算
S4
Return

[図7]


START
有理点 P'の入力
T1
λ、εを設定
λ²+λ+1=0 (mod r), ε³=1 (mod p), ε≠1
T2
φ(P')の演算、
P'=(x,y)→φ(P')=(εx, y)
T3
P の演算
P=φ(P')+(λ+1)P'
T4
T5
P=0?
Y
N
Q の演算
Q=φ(P')+(-λ)P'
T6
T7
Q=0?
Y
N
P 及び Q を戻り値にセット
T8
Return
Error Return

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2011/073098

A. CLASSIFICATION OF SUBJECT MATTER
G09C1/00(2006.01)i, *H04L9/32*(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G09C1/00, H04L9/32

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2011
Kokai Jitsuyo Shinan Koho	1971-2011	Toroku Jitsuyo Shinan Koho	1994-2011

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2008-178035 A (Toshiba Corp.), 31 July 2008 (31.07.2008), entire text (Family: none)	1-12
A	JP 2009-109772 A (Okayama University), 21 May 2009 (21.05.2009), entire text & US 2010/0260333 A1 & EP 2216767 A1 & WO 2009/057656 A1 & CN 101842824 A & KR 10-2010-0094487 A	1-12
A	WO 2010/024401 A1 (Okayama University), 04 March 2010 (04.03.2010), entire text (Family: none)	1-12

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
22 November, 2011 (22.11.11)	06 December, 2011 (06.12.11)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2011/073098

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2010/061951 A1 (Okayama University), 03 June 2010 (03.06.2010), entire text (Family: none)	1-12

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１１／０７３０９８

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　G09C1/00(2006.01)i, H04L9/32(2006.01)i

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.　G09C1/00, H04L9/32

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２０１１年
日本国実用新案登録公報	１９９６－２０１１年
日本国登録実用新案公報	１９９４－２０１１年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
A	JP 2008-178035 A (株式会社東芝) 2008.07.31, 全文 (ファミリーなし)	1-12
A	JP 2009-109772 A (国立大学法人 岡山大学) 2009.05.21, 全文 & US 2010/0260333 A1 & EP 2216767 A1 & WO 2009/057656 A1 & CN 101842824 A & KR 10-2010-0094487 A	1-12
A	WO 2010/024401 A1 (国立大学法人 岡山大学) 2010.03.04, 全文 (ファミリーなし)	1-12

☑　Ｃ欄の続きにも文献が列挙されている。

☐　パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー

「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの

「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「Ｏ」口頭による開示、使用、展示等に言及する文献

「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献

「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「＆」同一パテントファミリー文献

国際調査を完了した日 ２２．１１．２０１１	国際調査報告の発送日 ０６．１２．２０１１
国際調査機関の名称及びあて先 日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員）　５Ｓ　９４６９ 石田　信行 電話番号　０３－３５８１－１１０１　内線　３５４６

C（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
A	WO 2010/061951 A1 (国立大学法人 岡山大学) 2010.06.03, 全文 (ファミリーなし)	1-12