(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3927419号
(P3927419)
(45)発行日　平成19年6月6日(2007.6.6)　(24)登録日　平成19年3月9日(2007.3.9)

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

請求項の数 4　(全 23 頁)

(21)出願番号　特願2002-32938(P2002-32938)
(22)出願日　平成14年2月8日(2002.2.8)
(65)公開番号　特開2003-234733(P2003-234733A)
(43)公開日　平成15年8月22日(2003.8.22)
審査請求日　平成16年10月12日(2004.10.12)

(73)特許権者　392026693
株式会社エヌ・ティ・ティ・ドコモ
東京都千代田区永田町二丁目１１番１号
(74)代理人　100088155
弁理士　長谷川　芳樹
(74)代理人　100092657
弁理士　寺崎　史朗
(74)代理人　100114270
弁理士　黒川　朋也
(74)代理人　100108213
弁理士　阿部　豊隆
(74)代理人　100113549
弁理士　鈴木　守

最終頁に続く

(54)【発明の名称】情報登録方法、端末装置、情報登録サーバ、情報登録システム

(57)【特許請求の範囲】
【請求項１】
端末装置から送信される情報を情報登録サーバに登録する情報登録方法において、
前記端末装置が、ＮＴＲＵ公開鍵暗号方式により、短い多項式φと公開鍵ｈと小さいモジュラス値ｐと大きいモジュラス値ｑとを用いて、短い多項式で表現された前記情報αの暗号文ｅ＝ｐ＊φ＊ｈ＋α（ｍｏｄ　ｑ）を生成する第１の暗号文生成ステップと、
前記端末装置が、前記第１の暗号文生成ステップにおいて生成された前記暗号文ｅを、前記情報登録サーバに対して送信する第１の暗号文送信ステップと、
前記端末装置が、ＮＴＲＵ公開鍵暗号方式により、短い多項式ψと前記公開鍵ｈと前記小さいモジュラス値ｐと前記大きいモジュラス値ｑとを用いて、短い多項式ξの暗号文ａ＝ｐ＊ψ＊ｈ＋ξ（ｍｏｄ　ｑ）を生成する第２の暗号文生成ステップと、
前記端末装置が、前記第２の暗号文生成ステップにおいて生成された前記暗号文ａを、前記情報登録サーバに対して送信する第２の暗号文送信ステップと、
前記情報登録サーバが、前記情報αと前記短い多項式ψとの双方と比較してさらに短い多項式ｃを前記端末装置に対して送信するチャレンジ送信ステップと、
前記端末装置が、前記情報αと前記短い多項式φと前記短い多項式ψと前記短い多項式ξと前記情報登録サーバから送信された前記さらに短い多項式ｃとを用いて、多項式ｘ＝ξ＋ｃ＊αと多項式ｒ＝ψ＋ｃ＊φとを生成するレスポンス生成ステップと、
前記端末装置が、前記レスポンス生成ステップにおいて生成された前記多項式ｘと前記多項式ｒとを、前記情報登録サーバに対して送信するレスポンス送信ステップと、

前記情報登録サーバが、前記端末装置から送信された前記多項式ｘと前記多項式ｒとがともに短い多項式であることを検証し、かつ、前記暗号文ｅと前記暗号文ａと前記公開鍵ｈと前記小さいモジュラス値ｐと前記大きいモジュラス値ｑと前記さらに短い多項式ｃと前記多項式ｘと前記多項式ｒとがａ＝ｐ＊ｒ＊ｈ＋ｘ－ｃ＊ｅ（ｍｏｄ　ｑ）の関係を満たすことを検証することにより、前記端末装置から送信される暗号文ｅに対応する情報αを前記端末装置の利用者が知っていることを検証する検証ステップと、
前記情報登録サーバが、前記検証ステップによって、前記端末装置から送信される暗号文ｅに対応する情報αを前記端末装置の利用者が知っていることが検証された場合に、前記情報αまたは前記情報αの暗号文ｅを登録する情報登録ステップと
を備えたことを特徴とする情報登録方法。

【請求項２】
端末装置から送信される情報を情報登録サーバに登録する情報登録方法に用いる前記端末装置において、
ＮＴＲＵ公開鍵暗号方式により、短い多項式φと公開鍵ｈと小さいモジュラス値ｐと大きいモジュラス値ｑとを用いて、短い多項式で表現された前記情報αの暗号文ｅ＝ｐ＊φ＊ｈ＋α（ｍｏｄ　ｑ）を生成する第１の暗号文生成手段と、
前記第１の暗号文生成手段において生成された前記暗号文ｅを、前記情報登録サーバに対して送信する第１の暗号文送信手段と、
ＮＴＲＵ公開鍵暗号方式により、短い多項式ψと前記公開鍵ｈと前記小さいモジュラス値ｐと前記大きいモジュラス値ｑとを用いて、短い多項式ξの暗号文ａ＝ｐ＊ψ＊ｈ＋ξ（ｍｏｄ　ｑ）を生成する第２の暗号文生成手段と、
前記第２の暗号文生成手段において生成された前記暗号文ａを、前記情報登録サーバに対して送信する第２の暗号文送信手段と、
前記情報登録サーバから送信される、前記情報αと前記短い多項式ψとの双方と比較してさらに短い多項式ｃを受信するチャレンジ受信手段と、
前記情報αと前記短い多項式φと前記短い多項式ψと前記短い多項式ξと前記チャレンジ受信手段によって受信した前記さらに短い多項式ｃとを用いて、多項式ｘ＝ξ＋ｃ＊αと多項式ｒ＝ψ＋ｃ＊φとを生成するレスポンス生成手段と、
前記レスポンス生成手段によって生成された前記多項式ｘと前記多項式ｒとを、前記情報登録サーバに対して送信するレスポンス送信手段と
を備えたことを特徴とする端末装置。

【請求項３】
端末装置から送信される情報を情報登録サーバに登録する情報登録方法に用いる前記情報登録サーバにおいて、
ＮＴＲＵ公開鍵暗号方式により、短い多項式φと公開鍵ｈと小さいモジュラス値ｐと大きいモジュラス値ｑとを用いて前記端末装置において生成され、前記端末装置から送信される、短い多項式で表現された前記情報αの暗号文ｅ＝ｐ＊φ＊ｈ＋α（ｍｏｄ　ｑ）を受信する第１の暗号文受信手段と、
ＮＴＲＵ公開鍵暗号方式により、短い多項式ψと前記公開鍵ｈと前記小さいモジュラス値ｐと前記大きいモジュラス値ｑとを用いて前記端末装置において生成され、前記端末装置から送信される、短い多項式ξの暗号文ａ＝ｐ＊ψ＊ｈ＋ξ（ｍｏｄ　ｑ）を受信する第２の暗号文受信手段と、
前記情報αと前記短い多項式ψとの双方と比較してさらに短い多項式ｃを前記端末装置に対して送信するチャレンジ送信手段と、
前記情報αと前記短い多項式φと前記短い多項式ψと前記短い多項式ξと前記さらに短い多項式ｃとを用いて前記端末装置において生成され、前記端末装置から送信される、多項式ｘ＝ξ＋ｃ＊αと多項式ｒ＝ψ＋ｃ＊φとを受信するレスポンス受信手段と、
前記レスポンス受信手段によって受信した前記多項式ｘと前記多項式ｒとがともに短い多項式であることを検証し、かつ、前記暗号文ｅと前記暗号文ａと前記公開鍵ｈと前記小さいモジュラス値ｐと前記大きいモジュラス値ｑと前記さらに短い多項式ｃと前記多項式ｘ

と前記多項式ｒとがａ＝ｐ＊ｒ＊ｈ＋ｘ－ｃ＊ｅ（ｍｏｄ　ｑ）の関係を満たすことを検証することにより、前記端末装置から送信される暗号文ｅに対応する情報αを前記端末装置の利用者が知っていることを検証する検証手段と、
前記検証手段によって、前記端末装置から送信される暗号文ｅに対応する情報αを前記端末装置の利用者が知っていることが検証された場合に、前記情報αまたは前記情報αの暗号文ｅを登録する情報登録手段と
を備えたことを特徴とする情報登録サーバ。
【請求項４】
端末装置と情報登録サーバとを備え、前記端末装置から送信される情報を前記情報登録サーバに登録する情報登録システムにおいて、
前記端末装置は、請求項２に記載の端末装置であり、
前記情報登録サーバは、請求項３に記載の情報登録サーバである
ことを特徴とする情報登録システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、情報登録方法、情報登録システム、及びこれに用いる端末装置、情報登録サーバに関するものである。
【０００２】
【従来の技術】
ネットワークを介したデータの送受信の活発化に伴い、セキュリティ上の問題が無視できなくなってきている。そこで、例えば鍵寄託などのように、秘密性の高い情報（例えば秘密鍵）を公正な登録センタ（情報登録サーバ）に登録しておき、一定の認証が行われた場合にのみ秘密情報を利用できるようにする技術が知られている。
【０００３】
しかし、第３者のなりすましなどにより、秘密情報が登録センタに不正に登録されることもありうる。この問題に対処するため、検証可暗号方法が用いられる。検証可暗号方法とは、暗号文の送信者が暗号文に対応する平文を知っていることを、暗号文の受信者が当該平文に関する情報を得ることなく検証する方法である。すなわち、登録センタは、検証可暗号方法により、登録すべき秘密情報の暗号文を送信してきた者が当該秘密情報を本当に知っていること（すなわち他人から暗号文のみを盗取した者ではないこと）を、秘密情報自体を知らなくとも、知ることができ、その結果、秘密情報の登録を安全に行うことができる。
【０００４】
このような検証可暗号方法としては、例えば、素因数分解型の暗号方式を用いる方法（例えばE. Fujisaki and T. Okamoto, A Practical and Provably Secure Scheme for Public Verifiable Secret Sharing and Its Application, In Proceedings of EUROCRYPT'98, LNCS 1403, Springer, pp.32-46(1998), F. Bao, An Efficient verifiable encryption scheme for encryption of discrete logarithm, In Proceeding of CARDIS'98, LNCS 1820, Springer, pp.213-220(2000)）、離散対数型の暗号方式を用いる方法（例えばM. Stadler, Publicly Verifiable Secret Sharing, In Proceedings of EUROCRYPT'96, LNCS 1070, Springer, pp.190-199(1996)）などが知られている。
【０００５】
【発明が解決しようとする課題】
しかし、上記従来の技術にかかる検証可暗号方法を用いた情報登録方法は、いずれも、計算量が非常に多くなってしまうという問題点があった。特に、携帯性を重視するがゆえに高速のＣＰＵや大容量のメモリを搭載することが困難である移動通信端末においては、上記従来の技術にかかる検証可暗号方法は、その計算量の多さから、いずれも、実用に向かない。
【０００６】

そこで、本発明は、上記問題点を解決し、計算量の少ない情報登録方法、情報登録システム、及びこれに用いる端末装置、情報登録サーバを提供することを課題とする。

【０００７】

【課題を解決するための手段】

上記課題を解決するために、本発明の情報登録方法は、端末装置から送信される情報を情報登録サーバに登録する情報登録方法であって、上記端末装置が、ＮＴＲＵ公開鍵暗号方式により、短い多項式φと公開鍵ｈと小さいモジュラス値ｐと大きいモジュラス値ｑとを用いて、短い多項式で表現された上記情報αの暗号文ｅ＝ｐ＊φ＊ｈ＋α（ｍｏｄ　ｑ）を生成する第１の暗号文生成ステップと、上記端末装置が、上記第１の暗号文生成ステップにおいて生成された上記暗号文ｅを、上記情報登録サーバに対して送信する第１の暗号文送信ステップと、上記端末装置が、ＮＴＲＵ公開鍵暗号方式により、短い多項式ψと上記公開鍵ｈと上記小さいモジュラス値ｐと上記大きいモジュラス値ｑとを用いて、短い多項式ξの暗号文ａ＝ｐ＊ψ＊ｈ＋ξ（ｍｏｄ　ｑ）を生成する第２の暗号文生成ステップと、上記端末装置が、上記第２の暗号文生成ステップにおいて生成された上記暗号文ａを、上記情報登録サーバに対して送信する第２の暗号文送信ステップと、上記情報登録サーバが、上記情報αと上記短い多項式ψとの双方と比較してさらに短い多項式ｃを上記端末装置に対して送信するチャレンジ送信ステップと、上記端末装置が、上記情報αと上記短い多項式φと上記短い多項式ψと上記短い多項式ξと上記情報登録サーバから送信された上記さらに短い多項式ｃとを用いて、多項式ｘ＝ξ＋ｃ＊αと多項式ｒ＝ψ＋ｃ＊φとを生成するレスポンス生成ステップと、上記端末装置が、上記レスポンス生成ステップにおいて生成された上記多項式ｘと上記多項式ｒとを、上記情報登録サーバに対して送信するレスポンス送信ステップと、上記情報登録サーバが、上記端末装置から送信された上記多項式ｘと上記多項式ｒとがともに短い多項式であることを検証し、かつ、上記暗号文ｅと上記暗号文ａと上記公開鍵ｈと上記小さいモジュラス値ｐと上記大きいモジュラス値ｑと上記さらに短い多項式ｃと上記多項式ｘと上記多項式ｒとがａ＝ｐ＊ｒ＊ｈ＋ｘ－ｃ＊ｅ（ｍｏｄ　ｑ）の関係を満たすことを検証することにより、上記端末装置から送信される暗号文ｅに対応する情報αを上記端末装置の利用者が知っていることを検証する検証ステップと、上記情報登録サーバが、上記検証ステップによって、上記端末装置から送信される暗号文ｅに対応する情報αを上記端末装置の利用者が知っていることが検証された場合に、上記情報αまたは上記情報αの暗号文ｅを登録する情報登録ステップとを備えたことを特徴としている。

【０００８】

また、本発明の端末装置は、端末装置から送信される情報を情報登録サーバに登録する情報登録方法に用いる上記端末装置であって、ＮＴＲＵ公開鍵暗号方式により、短い多項式φと公開鍵ｈと小さいモジュラス値ｐと大きいモジュラス値ｑとを用いて、短い多項式で表現された上記情報αの暗号文ｅ＝ｐ＊φ＊ｈ＋α（ｍｏｄ　ｑ）を生成する第１の暗号文生成手段と、上記第１の暗号文生成手段において生成された上記暗号文ｅを、上記情報登録サーバに対して送信する第１の暗号文送信手段と、ＮＴＲＵ公開鍵暗号方式により、短い多項式ψと上記公開鍵ｈと上記小さいモジュラス値ｐと上記大きいモジュラス値ｑとを用いて、短い多項式ξの暗号文ａ＝ｐ＊ψ＊ｈ＋ξ（ｍｏｄ　ｑ）を生成する第２の暗号文生成手段と、上記第２の暗号文生成手段において生成された上記暗号文ａを、上記情報登録サーバに対して送信する第２の暗号文送信手段と、上記情報登録サーバから送信される、上記情報αと上記短い多項式ψとの双方と比較してさらに短い多項式ｃを受信するチャレンジ受信手段と、上記情報αと上記短い多項式φと上記短い多項式ψと上記短い多項式ξと上記チャレンジ受信手段によって受信した上記さらに短い多項式ｃとを用いて、多項式ｘ＝ξ＋ｃ＊αと多項式ｒ＝ψ＋ｃ＊φとを生成するレスポンス生成手段と、上記レスポンス生成手段によって生成された上記多項式ｘと上記多項式ｒとを、上記情報登録サーバに対して送信するレスポンス送信手段とを備えたことを特徴としている。

【０００９】

また、本発明の情報登録サーバは、端末装置から送信される情報を情報登録サーバに登録

する情報登録方法に用いる上記情報登録サーバであって、ＮＴＲＵ公開鍵暗号方式により、短い多項式φと公開鍵ｈと小さいモジュラス値ｐと大きいモジュラス値ｑとを用いて上記端末装置において生成され、上記端末装置から送信される、短い多項式で表現された上記情報αの暗号文ｅ＝ｐ＊φ＊ｈ＋α（ｍｏｄ　ｑ）を受信する第１の暗号文受信手段と、ＮＴＲＵ公開鍵暗号方式により、短い多項式ψと上記公開鍵ｈと上記小さいモジュラス値ｐと上記大きいモジュラス値ｑとを用いて上記端末装置において生成され、上記端末装置から送信される、短い多項式ξの暗号文ａ＝ｐ＊ψ＊ｈ＋ξ（ｍｏｄ　ｑ）を受信する第２の暗号文受信手段と、上記情報αと上記短い多項式ψとの双方と比較してさらに短い多項式ｃを上記端末装置に対して送信するチャレンジ送信手段と、上記情報αと上記短い多項式φと上記短い多項式ψと上記短い多項式ξと上記さらに短い多項式ｃとを用いて上記端末装置において生成され、上記端末装置から送信される、多項式ｘ＝ξ＋ｃ＊αと多項式ｒ＝ψ＋ｃ＊φとを受信するレスポンス受信手段と、上記レスポンス受信手段によって受信した上記多項式ｘと上記多項式ｒとがともに短い多項式であることを検証し、かつ、上記暗号文ｅと上記暗号文ａと上記公開鍵ｈと上記小さいモジュラス値ｐと上記大きいモジュラス値ｑと上記さらに短い多項式ｃと上記多項式ｘと上記多項式ｒとがａ＝ｐ＊ｒ＊ｈ＋ｘ－ｃ＊ｅ（ｍｏｄ　ｑ）の関係を満たすことを検証することにより、上記端末装置から送信される暗号文ｅに対応する情報αを上記端末装置の利用者が知っていることを検証する検証手段と、上記検証手段によって、上記端末装置から送信される暗号文ｅに対応する情報αを上記端末装置の利用者が知っていることが検証された場合に、上記情報αまたは上記情報αの暗号文ｅを登録する情報登録手段とを備えたことを特徴としている。

【００１０】

さらに、本発明の情報登録システムは、上述の端末装置と上述の情報登録サーバとを備えたことを特徴としている。

【００１１】

ＮＴＲＵ公開鍵暗号方式を用いることにより、素因数分解型の暗号方式を用いる場合や離散対数型の暗号方式を用いる場合と比較して、計算量を少なくすることができる。また、情報登録サーバにおいて、多項式ｘと多項式ｒとがともに短い多項式であることを検証し、かつ、ａ＝ｐ＊ｒ＊ｈ＋ｘ－ｃ＊ｅ（ｍｏｄ　ｑ）の関係が満たされることを検証することにより、端末装置の利用者が暗号文ｅに対応する平文の情報αを知っていることを情報登録サーバにおいて検証できた場合にのみ情報登録を行うことで、不正な情報登録を排除することができる。その結果、情報登録サーバに情報を登録するに際し、情報登録の信頼性を損なうことなく、その計算量を削減することができる。

【００１２】

【発明の実施の形態】

本発明の実施形態にかかる情報登録システムを説明する前に、本実施形態において用いられるＮＴＲＵ公開鍵暗号方式について簡単に説明しておく。

【００１３】

［定義］

多項式環Ｒ（（１）式参照）に属する多項式ａ（ｘ）（（２）式参照）をベクトルａ（（３）式参照）とみなし、そのセンターノルム｜ａ｜を（４）式に示すように定義する。

【００１４】

【数１】

$$R = Z[x]/\left(x^N - 1\right) \qquad \cdots(1)$$

【００１５】

【数２】

$$a(x)=a_0+a_1x+\cdots a_{N-1}x^{N-1}=\sum_{i=0}^{N-1}a_ix^i\in R \qquad \cdots(2)$$

【００１６】
【数３】

$$a=(a_0,a_1,\cdots,a_{N-1})\in Z^N \qquad \cdots(3)$$

【００１７】
【数４】

$$|a|=\sqrt{\sum_{i=0}^{N-1}\left(a_1-\frac{1}{N}\sum_{i=0}^{N-1}a_i\right)^2}=\sqrt{\sum_{i=0}^{N-1}a_i{}^2-\frac{1}{N}\left(\sum_{i=0}^{N-1}a_i\right)^2} \qquad \cdots(4)$$

【００１８】
このとき、例えば（５）式を満たすような多項式ａ（ｘ）を短い多項式と呼ぶ。
【００１９】
【数５】

$$|a|=O\left(\sqrt{N}\right) \qquad \cdots(5)$$

【００２０】
すなわち、短い多項式とは、そのセンターノルムが、多項式の次数Ｎの増加に伴って増加するように（例えば、Ｎの平方根に比例するように）あらかじめ定められたしきい値よりも小さくなるような多項式である。
【００２１】
また、（２）式で表される多項式ａ（ｘ）と（６）式で表される多項式ｂ（ｘ）とを用いた演算式ａ（ｘ）・ｂ（ｘ）（ｍｏｄ　ｘ^{N}－１）をａ＊ｂで表す。
【００２２】
【数６】

$$b(x)=\sum_{i=0}^{N-1}b_ix^i\in R \qquad \cdots(6)$$

【００２３】
ここで、ｃ（ｘ）＝ａ＊ｂ（（７）式参照）をベクトルｃ（（８）式参照）とみなすと、ベクトルａ（（３）式参照）とベクトルｂ（（９）式参照）とベクトルｃ（（８）式参照）とは、（１０）式の関係を満たす。
【００２４】
【数７】

$$c(x)=\sum_{k=0}^{N-1}c_k x^k = a*b \in R \qquad \cdots(7)$$

$$\left(c_k = \sum_{i+j=k(\mathrm{mod}\,N)} a_i b_j \right)$$

【００２５】
【数８】

$$c=(c_0,c_1,\cdots,c_{N-1})\in Z^N \qquad \cdots(8)$$

【００２６】
【数９】

$$b=(b_0,b_1,\cdots,b_{N-1})\in Z^N \qquad \cdots(9)$$

【００２７】
【数１０】

$$|c|=|a*b|\approx|a|\cdot|b| \qquad \cdots(10)$$

【００２８】
［準備］
適当な自然数Ｎ（例えば１００～５００の値）に対して、大きなモジュラス値ｑ（例えばＮの半分程度の値）と小さなモジュラス値ｐ（例えば２，３などの値）とを、x^N-1，ｐ，ｑが互いに素であるように定める。また、R_p，R_qをそれぞれ、Z_p，Z_qの元を係数とするＮ－１次多項式の集合とする。
【００２９】
［鍵生成］
短い多項式ｆ，ｇを任意に定め、これらを秘密鍵とする。この多項式ｆに関し、（１１）式を満たすF_p、及び（１２）式を満たすF_qを計算した後、（１３）式により公開鍵ｈを計算する。
【００３０】
【数１１】

$$f*F_p=1(\mathrm{mod}\,p) \qquad \cdots(11)$$

【００３１】
【数１２】

$$f*F_q=1(\mathrm{mod}\,q) \qquad \cdots(12)$$

【００３２】

【数１３】

$$h = F_q * g(\mathrm{mod}\, q) \qquad \cdots(13)$$

【００３３】
［暗号化］
メッセージｍの属するメッセージ空間Ｌ$_m$を（１４）式のように定義する。ここで、メッセージｍに対してランダムな短い多項式ｒを定め、（１５）式を用いて暗号文ｅを生成する。

【００３４】
【数１４】

$$m \in L_m = \left\{ m \in R \middle| -\frac{1}{2}(p-1) \le m_i \le \frac{1}{2}(p-1) \right\} \qquad \cdots(14)$$

【００３５】
【数１５】

$$e = p * r * h + m(\mathrm{mod}\, q) \qquad \cdots(15)$$

【００３６】
［復号化］
秘密鍵ｆと暗号文ｅとから（１６）式を用いてａを計算し、さらに（１７）式を用いてｂを計算し、このｂと秘密鍵ｆのＲ$_p$での逆元Ｆ$_p$とから、（１８）式を用いてメッセージｍを復号することができる。

【００３７】
【数１６】

$$a = f * e(\mathrm{mod}\, q) \qquad \cdots(16)$$

【００３８】
【数１７】

$$b = a(\mathrm{mod}\, p) \qquad \cdots(17)$$

【００３９】
【数１８】

$$m = F_p * b(\mathrm{mod}\, p) \qquad \cdots(18)$$

【００４０】

［ＮＴＲＵ仮定］
ＮＴＲＵ公開鍵暗号方式は、R_qに属する多項式ｈが与えられたときに、（１９）式を満たす短い多項式ｆ，ｇを求めることは困難であるとの仮定に基づいている。
【００４１】
【数１９】

$$f * h = g(\mathrm{mod}\, q) \qquad \cdots(19)$$

【００４２】
これは、ｄｅｇ　ｈ＝Ｎ－１のとき、秘密鍵ｆ，ｇを求めるための最も効率的な方法は、２Ｎ次元ラティス上の短いベクトルを探す問題を解くことと考えられるからである。
【００４３】
続いて、本発明の実施形態にかかる情報登録システムの説明に用いる定義について説明しておく。まず、２つの集合S_1，S_2をそれぞれ（２０）式、（２１）式のように定義する。
【００４４】
【数２０】

$$S_1 = \left\{ f \in R \,\middle|\, |f| = O(1) \right\} \qquad \cdots(20)$$

【００４５】
【数２１】

$$S_2 = \left\{ f \in R \,\middle|\, |f| = O\left(\sqrt{N}\right) \right\} \qquad \cdots(21)$$

【００４６】
すなわち、集合S_2は短い多項式の集合であり、S_1はさらに短い多項式の集合である。ここで、さらに短い多項式とは、そのセンターノルムが、多項式の次数Ｎによらないあらかじめ定められたしきい値よりも小さくなるような多項式である。従って、多項式の次数Ｎが大きい（例えば１００～５００）場合、さらに短い多項式のセンターノルムは、短い多項式のセンターノルムと比較して十分小さい。
【００４７】
上記定義のもとで、集合Ｌα，Ｌφ，L_c，L_x，L_rはそれぞれ、（２２）式を満たすものとする。
【００４８】
【数２２】

$$L_\alpha, L_\phi \subseteq S_2,\ L_c \subseteq S_1,\ L_x, L_r \subseteq S_2 \qquad \cdots(22)$$

【００４９】
すなわち、集合Ｌα，Ｌφ，L_x，L_rそれぞれは、短い多項式の集合であり、集合L_cは、さらに短い多項式の集合である。
【００５０】
ここで、αが集合Ｌαの要素であり、φが集合Ｌφの要素であり、ｃが集合L_cの要素で

あり、ξが集合Ｌξの要素であり、ψが集合Ｌψの要素であるならば、（２３）式、（２４）式、（２５）式を満たすような集合Ｌξ，Ｌψを定める。

【００５１】

【数２３】

$$x = \xi + c * \alpha \in L_x \qquad \cdots(23)$$

【００５２】

【数２４】

$$r = \phi + c * \phi \in L_r \qquad \cdots(24)$$

【００５３】

【数２５】

$$L_\xi, L_\phi = S_2 \qquad \cdots(25)$$

【００５４】

例えば、集合Ｌα，Ｌφ，L_c，L_x，L_rがそれぞれ、（２６）～（３０）式で表される場合、集合Ｌξ，Ｌψはそれぞれ、（３１）式、（３２）式で定義できる。

【００５５】

【数２６】

$$L_\alpha = L_m \qquad \cdots(26)$$

【００５６】

【数２７】

$$L_\phi = \left\{ f \in R_p \,\middle|\, |f| = O\left(\sqrt{N}\right) \right\} \qquad \cdots(27)$$

【００５７】

【数２８】

$$L_c = \left\{ f \in R_q \,\middle|\, |f| = O(1) \right\} \qquad \cdots(28)$$

【００５８】

【数２９】

$$L_x = \left\{ f \in R_p \,\middle|\, |f| = O\left(\sqrt{N}\right) \right\} \qquad \cdots(29)$$

【００５９】
【数３０】

$$L_r = L_x \qquad \cdots(30)$$

【００６０】
【数３１】

$$L_\xi = L_\phi \qquad \cdots(31)$$

【００６１】
【数３２】

$$L_\phi = L_\phi \qquad \cdots(32)$$

【００６２】
以下では、集合Ｌα，Ｌφ，L_c，Ｌξ，Ｌψ，L_x，L_rのサンプル空間をそれぞれ、（３３）～（３９）式のように定義する。尚、集合L^*_{cf}は、（４０）式によって与えられる。

【００６３】
【数３３】

$$L_\alpha = R_2 \qquad \cdots(33)$$

【００６４】
【数３４】

$$L_\phi = L_\alpha \qquad \cdots(34)$$

【００６５】
【数３５】

$$L_c = \left\{ c = c_i x^i + c_j x^j + c_k x^k + c_l x^l \in R_5 \;\middle|\; i,j,k,l \in \{0,1,\cdots,N-1\}, c_i, c_j, c_k, c_l \in \{0,1\} \right\} \qquad \cdots(35)$$

【００６６】
【数３６】

$$L_\xi = R_5 \setminus L^*_{cf} \qquad \cdots(36)$$

【００６７】
【数３７】

$$L_\phi = L_\xi \qquad \cdots(37)$$

【００６８】

【数３８】

$$L_x = R_5 \qquad \cdots(38)$$

【００６９】
【数３９】

$$L_r = L_x \qquad \cdots(39)$$

【００７０】
【数４０】

$$L^*_{cf} = \left\{ g = c * f \in R_5 \,\middle|\, c \in L_c, f \in R_2 \right\} \qquad \cdots(40)$$

【００７１】
続いて、本発明の実施形態にかかる情報登録システムについて図面を参照して説明する。尚、本実施形態にかかる情報登録システムは、本発明の実施形態にかかる端末装置および情報登録サーバを含んでいる。
【００７２】
まず、本実施形態にかかる情報登録システムの構成について説明する。図１は、本実施形態にかかる情報登録システムの構成図である。本実施形態にかかる情報登録システム１０は、移動通信端末１２（端末装置）と情報登録サーバ１４とを備え、移動通信端末１２から送信される情報（例えば秘密情報）を情報登録サーバ１４に登録する情報登録システムである。
【００７３】
ここで、移動通信端末１２と情報登録サーバ１４は、移動体通信網などのネットワーク１６を介して接続されており、互いにデータの送受信ができるようになっている。また、移動通信端末１２と情報登録サーバ１４とのそれぞれは、ネットワーク１６を介して鍵生成サーバ１８に接続されており、鍵生成サーバ１８から送信される公開鍵などのデータを受信することができるようになっている。
【００７４】
移動通信端末１２は、物理的には、ＣＰＵ、メモリ、ディスプレイ、入力キー、データ送受信回路などを備えた携帯電話として構成される。移動通信端末１２は、機能的な構成要素として、第１暗号文生成部２０（第１の暗号文生成手段）と、第１暗号文送信部２２（第１の暗号文送信手段）と、第２暗号文生成部２４（第２の暗号文生成手段）と、第２暗号文送信部２６（第２の暗号文送信手段）と、チャレンジ受信部２８（チャレンジ受信手段）と、レスポンス生成部３０（レスポンス生成手段）と、レスポンス送信部３２（レスポンス送信手段）とを備えて構成される。
【００７５】
情報登録サーバ１４は、物理的には、ＣＰＵ、メモリ、ディスプレイ、磁気ディスク装置や光ディスク装置などの格納装置、キーボードやマウスなどの入力装置、モデムやデジタル通信ユニットなどのデータ送受信装置などを備えたコンピュータシステムとして構成される。情報登録サーバ１４は、機能的な構成要素として、第１暗号文受信部３６（第１の暗号文受信手段）と、第２暗号文受信部３８（第２の暗号文受信手段）と、チャレンジ送信部４０（チャレンジ送信手段）と、レスポンス受信部４２（レスポンス受信手段）と、検証部４４（検証手段）と、情報登録部４６（情報登録手段）とを備えて構成される。以下、各構成要素について詳細に説明する。
【００７６】

移動通信端末１２の第１暗号文生成部２０は、上述のＮＴＲＵ公開鍵暗号方式により、短い多項式φと公開鍵ｈと小さいモジュラス値ｐと大きいモジュラス値ｑとを用いて、（４１）式に従い、短い多項式で表現された平文α（移動通信端末１２の利用者が情報登録センタ１４に登録したい情報の平文）の暗号文ｅを生成する。

【００７７】

【数４１】

$$e = p * \phi * h + \alpha \pmod{q} \qquad \cdots(41)$$

【００７８】

ここで、公開鍵ｈと小さいモジュラス値ｐと大きいモジュラス値ｑとは、あらかじめ鍵生成サーバ１８によって生成され、鍵生成サーバ１８から移動通信端末１２に対して送信されている。平文αは、（３３）式に示す集合Ｌαの要素であり、移動通信端末１２のユーザによって入力される。また、短い多項式φは、（３４）式に示す集合Ｌφの要素であり、移動通信端末１２のユーザによって入力されても良いし、第１暗号文生成部２０によってランダムに生成されてもよい。

【００７９】

第１暗号文送信部２２は、第１暗号文生成部２０によって生成された暗号文ｅを、情報登録サーバ１４に対して送信する。

【００８０】

第２暗号文生成部２４は、上述のＮＴＲＵ公開鍵暗号方式により、短い多項式ψと上記公開鍵ｈと上記小さいモジュラス値ｐと上記大きいモジュラス値ｑとを用いて、（４２）式に従い、短い多項式ξの暗号文ａを生成する。

【００８１】

【数４２】

$$a = p * \phi * h + \xi \pmod{q} \qquad \cdots(42)$$

【００８２】

ここで、短い多項式ψは、（３７）式に示す集合Ｌψの要素であり、移動通信端末１２のユーザによって入力されても良いし、第２暗号文生成部２４によってランダムに生成されてもよい。また、短い多項式ξは、（３６）式に示す集合Ｌξの要素であり、移動通信端末１２のユーザによって入力されても良いし、第２暗号文生成部２４によってランダムに生成されてもよい。

【００８３】

第２暗号文送信部２６は、第２暗号文生成部２４によって生成された暗号文ａを、情報登録サーバ１４に対して送信する。

【００８４】

チャレンジ受信部２８は、情報登録サーバ１４から送信される、上記平文αと上記短い多項式ψとの双方と比較してさらに短い多項式ｃ（チャレンジ）を受信する。ここで、さらに短い多項式ｃは、（３５）式に示す集合$Ｌ_{c}$の要素である。

【００８５】

レスポンス生成部３０は、上記平文αと上記短い多項式φと上記短い多項式ψと上記短い多項式ξと上記チャレンジ受信部２８によって受信した上記さらに短い多項式ｃとを用いて、（４３）式、（４４）式に従い、多項式ｘと多項式ｒ（レスポンス）を生成する。

【００８６】

【数４３】

$$x = \xi + c * \alpha \qquad \cdots(43)$$

【００８７】
【数４４】

$$r = \phi + c * \phi \qquad \cdots(44)$$

【００８８】
レスポンス送信部３２は、レスポンス生成部３４によって生成された上記多項式ｘと上記多項式ｒ（レスポンス）を、情報登録サーバ１４に対して送信する。
【００８９】
情報登録サーバ１４の第１暗号文受信部３６は、移動通信端末１２から送信される上記暗号文ｅを受信する。また、第２暗号文受信部３８は、移動通信端末１２から送信される上記暗号文ａを受信する。
【００９０】
チャレンジ送信部４０は、上記平文αと上記短い多項式ψとの双方と比較してさらに短い多項式ｃ（チャレンジ）を移動通信端末１２に対して送信する。ここで、上記さらに短い多項式ｃは、情報登録サーバ１４のユーザによって入力されても良いし、チャレンジ送信部４０によって生成されてもよい。
【００９１】
レスポンス受信部４２は、移動通信端末１２から送信される多項式ｘと多項式ｒ（レスポンス）を受信する。
【００９２】
検証部４４は、▲１▼レスポンス受信部４２によって受信した上記多項式ｘと上記多項式ｒとがともに短い多項式であることを検証し（すなわち、多項式ｘが（３８）式に示す集合L_xの要素であり、かつ、多項式ｒが（３９）式に示す集合L_rの要素であることを検証し）、かつ、▲２▼上記暗号文ｅと上記暗号文ａと上記公開鍵ｈと上記小さいモジュラス値ｐと上記大きいモジュラス値ｑと上記さらに短い多項式ｃと上記多項式ｘと上記多項式ｒとが、（４５）式を満たすことを検証する。
【００９３】
【数４５】

$$a = p * r * h + x - c * e \pmod{q} \qquad \cdots(45)$$

【００９４】
ここで、公開鍵ｈと小さいモジュラス値ｐと大きいモジュラス値ｑとは、あらかじめ鍵生成サーバ１８によって生成され、鍵生成サーバ１８から移動通信端末１２に対して送信されている。
【００９５】
上記▲１▼と▲２▼との双方が検証された場合、検証部４４は、情報登録サーバ１４から送信された暗号文ｅに対応する平文αを当該移動通信端末１２の利用者が知っていることが検証されたものとする。一方、上記▲１▼と▲２▼との少なくとも一方が検証されなかった場合、検証部４４は、移動通信端末１２から送信された暗号文ｅに対応する平文αを当該移動通信端末１２の利用者が知っていることが検証されなかったものとする。
【００９６】
情報登録部４６は、移動通信端末１２から送信される暗号文ｅに対応する平文αを当該移動通信端末１２の利用者が知っていることが検証部４４によって検証された場合に、当該平文αの暗号文ｅを登録する。暗号文ｅの登録は、情報登録サーバ１４に備えられた格納装置の所定の領域に、移動通信端末１２を識別する情報と関連づけられて暗号文ｅが格納されることによって行われる。
【００９７】
ここで、上記多項式ｘ，ｒとがともに短い多項式である（すなわち、多項式ｘが（３８）

式に示す集合L_xの要素であり、かつ、多項式ｒが（３９）式に示す集合L_rの要素である）ことを検証し、（４５）式が満たされることを検証することによって検証可暗号方式が実現することを、以下の３つの補題を証明することによって証明する。

【００９８】

［補題１］証明者（移動通信端末１２）が正しければ、上記検証により、受理される。

【００９９】

ｘが（４６）式で表され、ｒが（４７）式で表されるとき、ξ，ψ，ｃ，α，φはそれぞれ（４８）式を満たすことから、ｘ，ｒは（４９）式を満たす。

【０１００】

【数４６】

$$x=\xi+c*\alpha \qquad \cdots(46)$$

【０１０１】

【数４７】

$$r=\phi+c*\phi \qquad \cdots(47)$$

【０１０２】

【数４８】

$$\xi,\phi\in L_x\setminus L^*_{cf},c\in L_c,\alpha\in L_\alpha,\phi\in L_\phi \qquad \cdots(48)$$

【０１０３】

【数４９】

$$x\in L_x,r\in L_r \qquad \cdots(49)$$

【０１０４】

また、上述の（４１）式は、Ｒの要素である任意の多項式Ｅを用いて、（５０）式のように表される。

【０１０５】

【数５０】

$$p*\phi*h+\alpha=e+q*E\quad(E\in R) \qquad \cdots(50)$$

【０１０６】

同様に、上述の（４２）式は、Ｒの要素である任意の多項式Ａを用いて、（５１）式のように表される。

【０１０７】

【数５１】

$$p*\phi*h+\xi=a+q*A\quad(A\in R) \qquad \cdots(51)$$

【０１０８】

ここで、（４６）式、（４７）式、（５０）式、（５１）式を用いると、（５２）式が導かれる。

【０１０９】

【数５２】

$$\begin{aligned} & p*r*h+x-c+e \\ &= p*(\phi+c*\phi)*h+(\xi+c*\alpha)-c*e \\ &= (p*\phi*h+\xi)+c*(p*\phi*h+\alpha)-c*e \\ &= a+q*A+c*(e+q*E)-c*e \\ &= a+q*(A+c*E) \end{aligned} \qquad \cdots(52)$$

（５２）式に対してｍｏｄ　ｑの演算を施すことで、（５３）式が導かれる。

【０１１０】

【数５３】

$$a = p*r*h+x-c*e(\mathrm{mod}\,q) \qquad \cdots(53)$$

（証明終）

【０１１１】

［補題２］証明者が誤っていれば、上記検証により、エラー率ε≧３／＃Ｌ$_c$で拒否される。

【０１１２】

エラー率ε≧３／＃Ｌ$_c$であるので、＃Ｌ$_c$通りの質問に対して、＃Ｌ$_c$ε≧３個のエラーが存在する。つまり、Ｌ$_c$の中から、検証式を満たす少なくとも３つの異なるｃ，ｃ’，ｃ”を選ぶことができる。

【０１１３】

ここで、フォーキング・レンマより、公開鍵ｈを入力して、（５４）式を満たすｅ，（ｘ，ｒ，ｃ），（ｘ’，ｒ’，ｃ’），（ｘ”，ｒ”，ｃ”）を出力する確率的多項式時間アルゴリズムが存在すると仮定する。

【０１１４】

【数５４】

$$\begin{aligned} a &= p*r*h+x-c*e \\ &= p*r'*h+x'-c'*e \\ &= p*r''*h+x''-c''*e(\mathrm{mod}\,q) \end{aligned} \qquad \cdots(54)$$

【０１１５】

このとき、Δｘ$_1$，Δｘ$_2$，Δｒ$_1$，Δｒ$_2$，Δｃ$_1$，Δｃ$_2$をそれぞれ（５５）～（６０）式のようにおくと、（５４）式から、（６１）式及び（６２）式が導かれる。

【０１１６】

【数５５】

$$\Delta x_1 = x - x' \qquad \cdots(55)$$

【０１１７】

【数５６】

$$\Delta x_2 = x - x'' \qquad \cdots(56)$$

【０１１８】

【数５７】

$$\Delta r_1 = r - r' \qquad \cdots(57)$$

【０１１９】
【数５８】

$$\Delta r_2 = r - r'' \qquad \cdots(58)$$

【０１２０】
【数５９】

$$\Delta c_1 = c - c' \qquad \cdots(59)$$

【０１２１】
【数６０】

$$\Delta c_2 = c - c'' \qquad \cdots(60)$$

【０１２２】
【数６１】

$$p * \Delta r_1 * h + \Delta x_1 = \Delta c_1 * e + q * A_1 \qquad \cdots(61)$$

【０１２３】
【数６２】

$$p * \Delta r_2 * h + \Delta x_2 = \Delta c_2 * e + q * A_2 \qquad \cdots(62)$$

【０１２４】
続いて、（６１）式、（６２）式のｑ＊Ａ$_1$，ｑ＊Ａ$_2$をそれぞれ移項し、両辺にそれぞれΔｃ$_2$，Δｃ$_1$を乗ずることにより、（６３）式が導かれる。
【０１２５】
【数６３】

$$\begin{aligned} &\Delta c_1 * \Delta c_2 * e \\ &= p * \Delta c_2 * \Delta r_1 * h + \Delta c_2 * \Delta x_1 - q * \Delta c_2 * A_1 \\ &= p * \Delta c_1 * \Delta r_2 * h + \Delta c_1 * \Delta x_2 - q * \Delta c_1 * A_2 \end{aligned} \qquad \cdots(63)$$

【０１２６】
ここで、ΔＸ，ΔＲをそれぞれ（６４）式、（６５）式のようにおくと、（６３）式から（６６）式が導かれ、その結果、（６７）式が満たされる。
【０１２７】
【数６４】

$$\Delta X = \Delta c_1 * \Delta x_2 - \Delta c_2 * \Delta x_1 \qquad \cdots(64)$$

【０１２８】
【数６５】

$$\Delta R = \Delta c_2 * \Delta r_1 - \Delta c_1 * \Delta r_2 \qquad \cdots(65)$$

【０１２９】
【数６６】

$$p * \Delta R * h = \Delta X + q * (\Delta c_2 * A_1 - \Delta c_1 * A_2) \qquad \cdots(66)$$

【０１３０】
【数６７】

$$p * \Delta R * h = \Delta X \pmod{q} \qquad \cdots(67)$$

【０１３１】
｜ΔＸ｜，｜ΔＲ｜は、それぞれ、（６８）式、（６９）式を満たすので、多項式時間でＮＴＲＵラティスを解くことができることを意味する。
【０１３２】
【数６８】

$$|\Delta X| = O\left(\sqrt{N}\right) \qquad \cdots(68)$$

【０１３３】
【数６９】

$$|\Delta R| = O\left(\sqrt{N}\right) \qquad \cdots(69)$$

【０１３４】
これは、ＮＴＲＵラティスを解くことが難しければ、証明者はうそをつけないことを意味する。
（証明終）
【０１３５】
［補題３］上記検証においては、検証者（情報登録サーバ１４）に対して、平文αに関する情報を与えない。
【０１３６】
次のようなシミュレータを作成する。すなわち、与えられたｅに対して、L_xの要素であるｘ’，L_rの要素であるｒ’，L_cの要素であるｃ’をランダムに選択する。そして、（ｈ，ｅ，ｐ＊ｒ’＊ｈ＋ｘ’－ｃ’＊ｅ（ｍｏｄ　ｑ））をランダムオラクルに質問する。既に同じ質問がされている確率はきわめて小さいので、ランダムオラクルは、この質問に対する回答をｃ’としてリストに入れる。このときシミュレータの出力によるプルーフ

は（ｘ’，ｒ’，ｃ’）となる。
【０１３７】
このとき、＃Ｌα，＃Ｌφ，＃$Ｌ_{c}$，＃$Ｌ_{x}$，＃$Ｌ_{r}$は、（７０）～（７３）式を満たし、極めて小さいので、上記検証可暗号方式で出現する（ｘ，ｒ，ｃ）の系列がシミュレータによって生成される（ｘ’，ｒ’，ｃ’）の系列と統計的識別不可能となる。
【０１３８】
【数７０】

$$\#L_{\alpha}=\#L_{\phi}=\#R_{2}=2^{N} \qquad \cdots(70)$$

【０１３９】
【数７１】

$$\#L_{c}={}_{N}C_{4}2^{4} \qquad \cdots(71)$$

【０１４０】
【数７２】

$$\#L_{x}=\#L_{r}=\#R_{5}=5^{N} \qquad \cdots(72)$$

【０１４１】
【数７３】

$$(\#L_{c})(\#L_{\alpha})(\#L_{\phi})/(\#L_{x})(\#L_{r})=\left({}_{N}C_{4}2^{2N+4}\right)/5^{2N} \qquad \cdots(73)$$

【０１４２】
上記シミュレータは、誰にでも作成できる。このことは、検証者が平文に関する情報を得ないことを意味する。
（証明終）
【０１４３】
続いて、本実施形態にかかる情報登録システムの動作について説明し、併せて、本発明の実施形態にかかる情報登録方法について説明する。
【０１４４】
図２は、本実施形態にかかる情報登録システム１０の動作を示すフローチャートである。情報登録システム１０を構成する移動通信端末１２と情報登録サーバ１４に対しては、鍵生成サーバ１８によって生成された公開鍵ｈと小さいモジュラス値ｐと大きいモジュラス値ｑとが、あらかじめ送信されている。
【０１４５】
移動通信端末１２から情報登録サーバ１４に対して情報の登録を行おうとする場合、まず、移動通信端末１２において、上述の（４１）式に基づき、移動通信端末１２の利用者が情報登録センタ１４に登録したい情報の平文αに対する暗号文ｅが生成され（Ｓ１２）、情報登録サーバ１４に対して送信される（Ｓ１４）。ここで、αは、（３３）式に示す集合Ｌαの要素であり、φ（図２参照）は、（３４）式に示す集合Ｌφの要素である。
【０１４６】
また、移動通信端末１２において、上述の（４２）式に基づき、多項式ξに対する暗号文ａが生成され（Ｓ１６）、情報登録サーバ１４に対して送信される（Ｓ１８）。ここで、ξは、（３６）式に示す集合Ｌξの要素であり、ψ（図２参照）は、（３７）式に示す集

合Ｌψの要素である。

【０１４７】

続いて、暗号文ｅ及び暗号文ａを受信した情報登録サーバ１４から、移動通信端末１２に対して、さらに短い多項式ｃ（チャレンジ）が送信される（Ｓ２０）。ここで、さらに短い多項式ｃは、（３５）式に示す集合$Ｌ_{c}$の要素である。

【０１４８】

情報登録サーバ１４から送信されたさらに短い多項式ｃ（チャレンジ）が移動通信端末１２によって受信されると、移動通信端末１２において、（４３）式及び（４４）式に従って、多項式ｘと多項式ｒ（レスポンス）が生成され（Ｓ２２）、生成された多項式ｘと多項式ｒ（レスポンス）が情報登録サーバ１４に対して送信される（Ｓ２４）。

【０１４９】

その後、情報登録サーバ１４において、移動通信端末１２から送信された多項式ｘと多項式ｒとがともに短い多項式であること（すなわち、多項式ｘが（３８）式に示す集合$Ｌ_{x}$の要素であり、かつ、多項式ｒが（３９）式に示す集合$Ｌ_{r}$の要素であること）が検証され（Ｓ２６）、上記暗号文ｅと上記暗号文ａと上記公開鍵ｈと上記小さいモジュラス値ｐと上記大きいモジュラス値ｑと上記さらに短い多項式ｃと上記多項式ｘと上記多項式ｒとが、（４５）式を満たすことが検証される（Ｓ２８）。

【０１５０】

ここで、移動通信端末１２から送信された多項式ｘと多項式ｒとの少なくとも一方が短い多項式ではない場合（すなわち、多項式ｘが（３８）式に示す集合$Ｌ_{x}$の要素ではないか、または、多項式ｒが（３９）式に示す集合$Ｌ_{r}$の要素ではない場合）、情報登録サーバ１４において、移動通信端末１２から送信される暗号文ｅに対応する平文αを当該移動通信端末１２の利用者が知らないものと判断され、情報登録サーバ１４への情報登録は行われない。また、上記暗号文ｅと上記暗号文ａと上記公開鍵ｈと上記小さいモジュラス値ｐと上記大きいモジュラス値ｑと上記さらに短い多項式ｃと上記多項式ｘと上記多項式ｒとが、（４５）式を満たさない場合も、情報登録サーバ１４において、移動通信端末１２から送信される暗号文ｅに対応する平文αを当該移動通信端末１２の利用者が知らないものと判断され、情報登録サーバ１４への情報登録は行われない。

【０１５１】

一方、移動通信端末１２から送信された多項式ｘと多項式ｒとがともに短い多項式であり（すなわち、多項式ｘが（３８）式に示す集合Ｌの要素であり、かつ、多項式ｒが（３９）式に示す集合Ｌの要素であり）、かつ、上記暗号文ｅと上記暗号文ａと上記公開鍵ｈと上記小さいモジュラス値ｐと上記大きいモジュラス値ｑと上記さらに短い多項式ｃと上記多項式ｘと上記多項式ｒとが、（４５）式を満たす場合、情報登録サーバ１４において、移動通信端末１２から送信される暗号文ｅに対応する平文αを当該移動通信端末１２の利用者が知っているものと判断され、情報登録サーバ１４への情報登録が行われる（Ｓ３０）。より具体的には、移動通信端末１２から送信された暗号文ｅが、情報登録サーバ１４に備えられた格納装置の所定の領域に、移動通信端末１２を識別する情報と関連づけられて格納される。この場合、情報登録サーバ１４が暗号文ｅに対応する平文αを移動通信端末１２からさらに受信し、当該平文αを情報登録サーバ１４に登録するようにしてもよい。

【０１５２】

また、図２を用いて説明した上記フローにおいて、移動通信端末１２から情報登録サーバ１４に対し、暗号文ａが送信されない場合、多項式ｘ，ｒ（レスポンス）が送信されない場合は、それぞれ、その後の処理が中止される。

【０１５３】

また、図２を用いて説明した上記フローを、移動通信端末１２及び情報登録サーバ１４以外の第３者に公開し、移動通信端末１２と情報登録サーバ１４との間の情報の送受信フローが正しいかどうかを外部から確認できるようにしてもよい。図２を用いて説明した上記フローを第３者に公開することで、当該第３者（例えば移動通信端末１２に対してサービ

スを提供するサービスプロバイダ）は、情報登録サーバ１４に対して何ら問い合わせを行うことなく、移動通信端末１２から情報登録サーバ１４に対して一定の情報の登録があったことを知ることができ、移動通信端末１２との迅速なデータの送受信（例えば迅速なサービスの提供）が可能となる。

【０１５４】

続いて、本実施形態にかかる情報登録システムの作用及び効果について説明する。本実施形態にかかる情報登録システム１０は、ＮＴＲＵ公開鍵暗号方式を用いることにより、素因数分解型の暗号方式を用いる場合や離散対数型の暗号方式を用いる場合と比較して、計算量を少なくすることができる。これは、従来技術にかかる暗号方式が指数演算を主とした暗号方式であったのに対し、ＮＴＲＵ公開鍵暗号方式は、積、和の演算を主とした暗号方式であるからである。また、本実施形態にかかる情報登録システム１０においては、情報登録サーバ１４において、多項式ｘと多項式ｒとがともに短い多項式であることを検証し、かつ、ａ＝ｐ＊ｒ＊ｈ＋ｘ－ｃ＊ｅ（ｍｏｄ　ｑ）の関係が満たされることを検証することにより、移動通信端末１２の利用者が暗号文ｅに対応する平文αを知っていることを情報登録サーバ１４において検証できた場合にのみ情報登録を行う。したがって、不正な情報登録を排除することができる。その結果、情報登録サーバ１４に情報を登録するに際し、情報登録の信頼性を損なうことなく、その計算量を削減することができる。

【０１５５】

また、本実施形態にかかる情報登録システム１０は、ＮＴＲＵ公開鍵暗号方式を用いることにより、素因数分解型の暗号方式や離散対数型の暗号方式を利用するための仮定が成立しなくなった場合であっても利用しうる。

【０１５６】

本実施形態にかかる情報登録システム１０は、例えばインターネットなどのネットワーク上における鍵寄託などに好適に利用可能である。また、その計算量の少なさゆえに、携帯電話やＩＣカードなどの携帯型端末に好適に適用可能である。

【０１５７】

【発明の効果】

本発明の情報登録方法及び情報登録システムは、ＮＴＲＵ公開鍵暗号方式を用いることにより、素因数分解型の暗号方式を用いる場合や離散対数型の暗号方式を用いる場合と比較して、計算量を少なくすることができる。また、情報登録サーバにおいて、多項式ｘと多項式ｒとがともに短い多項式であることを検証し、かつ、ａ＝ｐ＊ｒ＊ｈ＋ｘ－ｃ＊ｅ（ｍｏｄ　ｑ）の関係が満たされることを検証することにより、端末装置の利用者が暗号文ｅに対応する平文αを知っていることを情報登録サーバにおいて検証できた場合にのみ情報登録を行うことで、不正な情報登録を排除することができる。その結果、情報登録サーバに情報を登録するに際し、情報登録の信頼性を損なうことなく、その計算量を削減することができる。

【図面の簡単な説明】

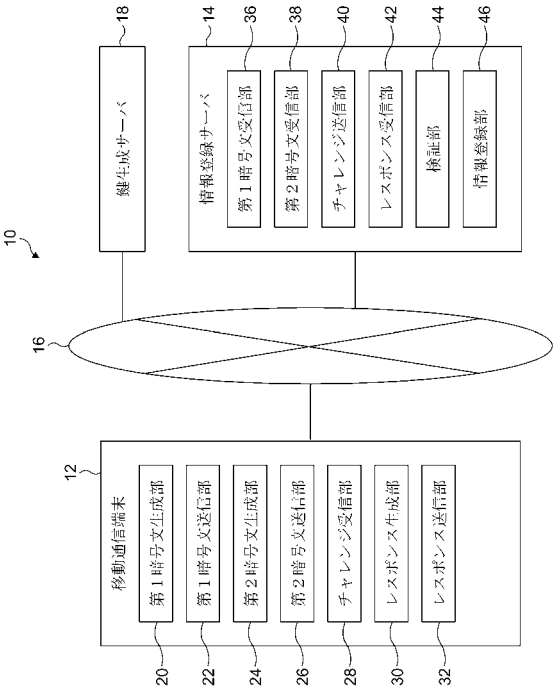
【図１】情報登録システムの構成図である。

【図２】情報登録システムの動作を示すフローチャートである。

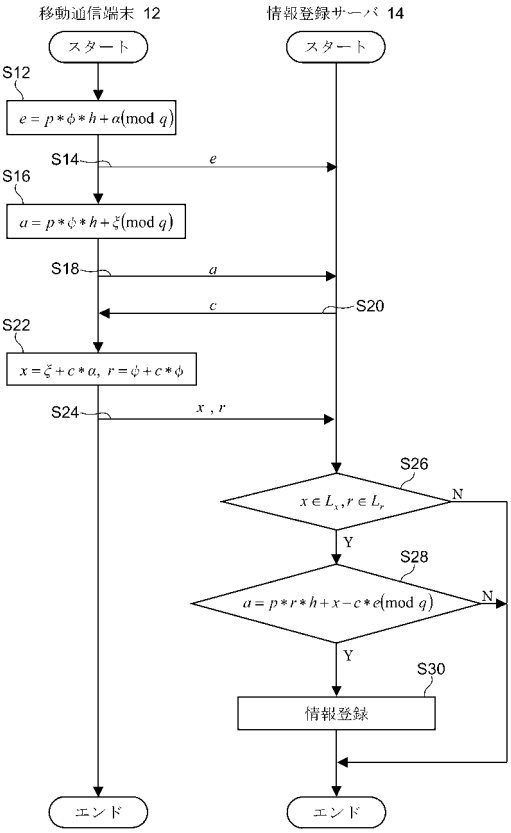
【符号の説明】

１０…情報登録システム、１２…移動通信端末，１４…情報登録サーバ、１６…ネットワーク、１８…鍵生成サーバ、２０…第１暗号文生成部、２２…第１暗号文送信部、２４…第２暗号文生成部、２６…第２暗号文送信部、２８…チャレンジ受信部、３０…レスポンス生成部、３２…レスポンス送信部、３６…第１暗号文受信部、３８…第２暗号文受信部、４０…チャレンジ送信部、４２…レスポンス受信部、４４…検証部、４６…情報登録部

【図１】


10
18
鍵生成サーバ
14
情報登録サーバ
36
第１暗号文受信部
38
第２暗号文受信部
40
チャレンジ送信部
42
レスポンス受信部
44
検証部
46
情報登録部
16
12
移動通信端末
第１暗号文生成部
第１暗号文送信部
第２暗号文生成部
第２暗号文送信部
チャレンジ受信部
レスポンス生成部
レスポンス送信部
20
22
24
26
28
30
32

【図２】


移動通信端末 12
情報登録サーバ 14
スタート
スタート
S12
$e = p*\phi*h+\alpha \pmod q$
S14
e
S16
$a = p*\phi*h+\xi \pmod q$
S18
a
c
S20
S22
$x = \xi + c*\alpha,\ r = \phi + c*\phi$
S24
x , r
S26
$x \in L_x, r \in L_r$
N
Y
S28
$a = p*r*h+x-c*e \pmod q$
N
Y
S30
情報登録
エンド
エンド

フロントページの続き

(72)発明者　小栗　伸幸
東京都千代田区永田町二丁目１１番１号　株式会社エヌ・ティ・ティ・ドコモ内

審査官　石田　信行

(56)参考文献　特表２００５－５１５６５９（ＪＰ，Ａ）
特表２００３－５３５４９９（ＪＰ，Ａ）
特表２０００－５１６７３３（ＪＰ，Ａ）

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