

(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
2011年5月5日(05.05.2011)

(10) 国際公開番号
WO 2011/052056 A1

- (51) 国際特許分類:
H04L 9/32 (2006.01)
- (21) 国際出願番号: PCT/JP2009/068584
- (22) 国際出願日: 2009年10月29日(29.10.2009)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (71) 出願人(米国を除く全ての指定国について): 三菱電機株式会社(Mitsubishi Electric Corporation) [JP/JP]; 〒1008310 東京都千代田区丸の内二丁目7番3号 Tokyo (JP).
- (72) 発明者; および
- (75) 発明者/出願人(米国についてのみ): 服部 充洋(HATTORI, Mitsuhiro) [—/JP]; 〒1008310 東京都千代田区丸の内二丁目7番3号 三菱電機株式会社内 Tokyo (JP). 柴田 陽一(SHIBATA, Yoichi) [—/JP]; 〒1008310 東京都千代田区丸の内二丁目7番3号 三菱電機株式会社内 Tokyo (JP). 伊藤 隆(ITO, Takashi) [—/JP]; 〒1008310 東京都千代田区丸の内二丁目7番3号 三菱電機株式会社内 Tokyo (JP). 松田 規(MATSUDA, Nori) [—/JP]; 〒1008310 東京都千代田区丸の内二丁目7番3号 三菱電機株式会社内 Tokyo (JP).

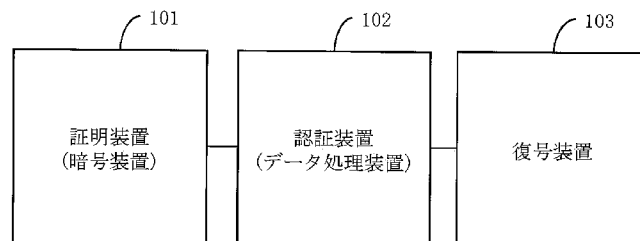
番3号 三菱電機株式会社内 Tokyo (JP). 高島克幸(TAKASHIMA, Katsuyuki) [—/JP]; 〒1008310 東京都千代田区丸の内二丁目7番3号 三菱電機株式会社内 Tokyo (JP). 米田 健(YONEDA, Takeshi) [—/JP]; 〒1008310 東京都千代田区丸の内二丁目7番3号 三菱電機株式会社内 Tokyo (JP).

- (74) 代理人: 溝井 章司, 外(MIZOI, Shoji et al.); 〒2470056 神奈川県鎌倉市大船二丁目17番10号 N T A大船ビル3階 溝井国際特許事務所 Kanagawa (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, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

[続葉有]

- (54) Title: DATA PROCESSING DEVICE
- (54) 発明の名称: データ処理装置

[図1]



101 Verification Device (Encryption Device)

102 Authentication Device (Data Processing Device)

103 Decryption Device

(57) Abstract: A verification device (101) encrypts a feature vector for registration using a public key associated with a secret key in a decryption device (103) and random numbers, and registers the encrypted feature vector for registration in an authentication device (102). During authentication, the verification device encrypts a feature vector for authentication using the aforementioned public key and random numbers, and while the two encrypted feature vectors are in a state of encryption, the authentication device generates encryption similarity information from which the degree of similarity between the two feature vectors can be derived in the decryption device by means of decryption processing using the aforementioned secret key. The decryption device (103) decrypts the encryption similarity information and derives the degree of similarity of the plaintext, and in the authentication device (102), the source is authenticated if the degree of similarity is at or above a threshold value. Thus, the degree of similarity can be derived without using the feature vector of the plaintext, enabling safe authentication with a low possibility of plaintext theft.

(57) 要約:

[続葉有]



WO 2011/052056 A1



(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, LS, MW, MZ, NA, 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 (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, SE, SI, SK, 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))

証明装置 101 が、復号装置 103 にて秘密鍵と対応付けられている公開鍵と、乱数を用いて登録用の特徴ベクトルを暗号化し、登録用の暗号化特徴ベクトルを認証装置 102 に登録し、認証時には、証明装置が認証用の特徴ベクトルを前記公開鍵と乱数を用いて暗号化し、認証装置が、2つの暗号化特徴ベクトルが暗号化された状態のままで、復号装置において前記秘密鍵を用いた復号処理により2つの特徴ベクトル間の類似度を導出可能な暗号化類似度情報を生成し、復号装置 103 が暗号化類似度情報を復号して平文の類似度を導出し、認証装置 102 では、類似度がしきい値以上であれば本人と判定し、平文の特徴ベクトルを用いることなく類似度を導出でき、平文の窃取の可能性の低い安全な本人認証を実現する。

明 細 書

発明の名称： データ処理装置

技術分野

[0001] 本発明は、生体情報等を用いて本人認証を行う認証技術に関する。

背景技術

[0002] 指紋認証や静脈認証などの生体認証は、指紋の紋様や静脈の形が個人ごとに異なることを利用して個人識別を行う仕組みのことである。

近年はビルの入退室管理やパーソナルコンピュータのログイン管理、銀行ATM（Automated Teller Machine）での本人認証などのアクセス管理に用いられている。

[0003] 生体認証においては、ユーザ（被認証者あるいは証明者）と認証装置（認証者）の間で以下のようにして認証を行うのが一般的である。

[0004] あらかじめ登録段階において、ユーザが自分の生体情報を認証装置に登録しておく。

そして認証時には、ユーザが認証装置に生体情報を提示する。

認証装置は、登録されている生体情報と提示された生体情報とを照合し、その類似度がある条件を満たしていればユーザ本人であると判断し、条件を満たしていなければ他人であると判断する。

[0005] このような生体認証において、生体情報は個人を特徴付けるプライバシー情報であるため保護されることが望ましい。

そこで、登録時に生体情報を暗号化して登録し、認証時にも生体情報を暗号化して照合を行うことで、生体情報そのものを露わにすることなく生体認証を行う方法が提案されている（例えば特許文献1）。

また、生体情報の暗号化に利用可能な暗号アルゴリズムとして、例えば、非特許文献1－4に開示の暗号アルゴリズムが考えられる。

先行技術文献

特許文献

[0006] 特許文献1：特表2008-521025号公報

非特許文献

[0007] 非特許文献1：T. Okamoto、K. Takashima、“Homomorphic encryption and signatures from vector decomposition”、Pairing 2008、Lecture Notes in Computer Science、Vol. 5209、pp. 57-74、2008.

非特許文献2：D. Boneh、E. -J. Goh、K. Nissim、“Evaluating 2-DNF formulas on ciphertexts”、Theory Of Cryptography Conference、Lecture Notes in Computer Science、Vol. 3378、pp. 325-341、2005.

非特許文献3：C. Gentry、“Fully homomorphic encryption using ideal lattices”、ACM Symposium on Theory Of Computing、pp. 169-178、2009.

非特許文献4：D. Freeman、M. Scott、E. Teske、“A taxonomy of pairing-friendly elliptic curves”、Journal Of Cryptology、2009年6月.

発明の概要

発明が解決しようとする課題

[0008] 特許文献1では、公開鍵暗号技術を用いた暗号化により生体情報の保護を図っているが、生体情報を暗号化する際、暗号アルゴリズムとしてPaillier暗号やElGamal暗号などの通常の準同型暗号を用いている。

ここで通常の準同型暗号とは、例えばT個の暗号文 $E(x_1)$ 、 $E(x_2)$ 、 $\dots$ 、 $E(x_T)$ を用いて暗号文 $E(x_1 + x_2 + \dots + x_T)$ が計算で

きるというように、複数の暗号文から元の平文の和の暗号文が計算できるような暗号である。

ここで $E(x_1)$ はある公開鍵を用いて生成した x_1 の暗号文を表す。

なお、上記では加算を例に挙げたが、正確に定義すると、ここでいう通常の準同型暗号とは、複数の暗号文から元の平文に対してある 1 種類の演算を施した暗号文が計算できるような暗号である。

演算の種類としては、有限体における加法や乗法などの種類があるが、いずれにしても 1 種類のみ演算が可能な暗号である。

[0009] しかし、このような通常の準同型暗号を用いた場合、認証時の計算過程において、暗号化した生体情報だけですべての処理を完結させることはできず、平文の生体情報を必要とする箇所が存在していた。

[0010] 例えば、特許文献 1 に記載の認証方法の場合、類似度判定の指標として、生体情報から生成された特徴ベクトルのハミング距離（すなわち、ベクトルを構成するビット列同士のハミング距離）を利用し、以下のような手順で秘匿照合処理を行っていた。

なお、ここでは、ユーザは認証装置に直接アクセスするのではなく、証明装置にアクセスし、証明装置が認証装置との間で通信を行って、生体情報の登録処理および認証処理を行うものとする。

つまり、生体情報を用いたりモートログインをも含めたより一般的な生体認証方式を想定する。

また、暗号化時には、システム共通の公開鍵を用いて暗号化を行うものとする。

[0011] 登録時、証明装置はユーザから生体情報を抽出し、抽出した生体情報からユーザの特徴を表す特徴ベクトルを構成する。

この特徴ベクトルをビット列 $X = (x_1, x_2, \dots, x_T)$ とする。

証明装置は、抽出した特徴ベクトルを、Paillier 暗号を用いてビットごとに暗号化して暗号化ビット列 $E(X) = (E(x_1), E(x_2), \dots, E(x_T))$ を計算し、認証装置に送付して登録する。

認証時、証明装置は登録時と同様にユーザから生体情報ビット列 $Y = (y_1, y_2, \dots, y_T)$ を抽出する。

その上で、登録しておいた暗号化ビット列 $E(X) = (E(x_1), E(x_2), \dots, E(x_T))$ を認証装置から受け取る。

ここで証明装置は、ビット列 X と Y のハミング距離 $d_H(X, Y)$ の暗号文を算出するに際して、準同型暗号の以下の性質（数 1）を利用する。

[0012] [数1]

$$E(d_H(X, Y)) = \prod_{i=1}^T E(x_i^2 - 2x_i y_i + y_i^2) = \prod_{i=1}^T E(x_i - 2x_i y_i + y_i) = \prod_{i=1}^T E(x_i) E(y_i) E(x_i)^{-2y_i}$$

[0013] ここで、第 2 式から第 3 式への移行は、 x_1, y_1 が 0、1 の二値しかとらないことによる。

また、第 3 式から第 4 式への移行は、Paillier 暗号が通常の準同型暗号であり、暗号文同士の積により元の平文の和の暗号文が得られるという性質による。

[0014] この性質を利用して、証明装置は、認証装置から受け取った暗号化ビット列 $E(X) = (E(x_1), E(x_2), \dots, E(x_T))$ と、生体情報ビット列 $Y = (y_1, y_2, \dots, y_T)$ を用いて以下の値を計算し（数 2）、認証装置に送付する。

[0015] [数2]

$$\prod_{i=1}^T E(y_i) E(x_i)^{-2y_i}$$

[0016] 認証装置では、受け取った値に以下の値（数 3）を掛け合わせ、暗号化ハミング距離 $E(d_H(X, Y))$ を計算する。

そして、セキュアプロトコルを用いてハミング距離を復号し、類似度判定を行う。

[0017]

[数3]

$$\prod_{i=1}^T E(x_i)$$

[0018] このように、Paillier暗号などの通常の準同型暗号を用いた場合には、 $-2x_i y_i$ の暗号文を計算する際に $E(x_i)^{-2y_i}$ と計算するため、指数部分に平文 y_i が必要である。

つまり、準同型暗号の本質上、すべてを暗号文で処理することはできない。

そのため、一旦認証装置から証明装置に暗号化生体情報 $E(X) = (E(x_1), E(x_2), \dots, E(x_T))$ を送付し、証明装置が平文 y_i を用いた計算を行う必要がある。

[0019] この暗号化生体情報の送付に際しては、認証の対象となるユーザが別途ID情報などによって特定されているいわゆる1:1認証の場合には1人分の送付でよいが、認証の対象となるユーザが特定されておらず、データベースに格納された多くのユーザとの照合を必要とするいわゆる1:N認証の場合には、ユーザ数に比例した送付が必要となる。

そのため、ユーザ数に比例して認証装置と証明装置との間の通信量が増大するという課題がある。

[0020] また、証明装置から平文の生体情報をできるだけ早く消去することがセキュリティの観点から望ましい。

しかし、上記のように認証に平文の生体情報が必要なため、特に1:N認証においては認証が完了するまで端末上の生体情報を消去できず、窃取の危険により長くさらされてしまうという課題がある。

[0021] 本発明は、上記のような課題を解決することを主な目的の一つとし、認証処理の過程において必要であった平文を不要とし、平文の窃取の機会を減少させ、それによってより安全性の高い秘匿照合方法を提供することを主な目的とする。

また、認証装置と証明装置との間の通信量を低減させることも目的とする。

課題を解決するための手段

- [0022] 本発明に係るデータ処理装置は、
- 二重準同型暗号アルゴリズムに基づいて復号装置において生成され、前記復号装置から配布された公開鍵を記憶する公開鍵記憶部と、
- 前記復号装置から配布された前記公開鍵を保有する暗号装置が保有する前記公開鍵を用いて暗号化した第1データを暗号化第1データとして記憶する暗号化データ記憶部と、
- 前記暗号化第1データが前記暗号化データ記憶部に記憶された後に前記暗号装置が保有する前記公開鍵を用いて暗号化した第2データを暗号化第2データとして入力する暗号化データ入力部と、
- 前記公開鍵の少なくとも一部を用いて、乱数を生成する乱数生成部と、
- 前記暗号化第1データと前記暗号化第2データに対して前記公開鍵記憶部に記憶されている前記公開鍵と前記乱数生成部により生成された乱数を用いた演算を行って、前記暗号化第1データと前記暗号化第2データがそれぞれ暗号化された状態のままで、前記公開鍵に対応付けられて生成された秘密鍵を用いた復号処理により前記第1データと前記第2データとの間の類似度を導出可能な暗号化された情報を暗号化類似度情報として生成する暗号化類似度生成部とを有することを特徴とする。

発明の効果

- [0023] 本発明によれば、暗号化第1データと暗号化第2データがそれぞれ暗号化された状態のままで、公開鍵に対応付けられて生成された秘密鍵を用いた復号処理により第1データと第2データとの間の類似度を導出可能な暗号化類似度情報を生成するので、平文である第1データと第2データを用いることなく第1データと第2データの類似度を導出することができ、平文の窃取の可能性の低い安全な本人認証を実現することができる。

図面の簡単な説明

[0024] [図1]実施の形態 1 に係る生体認証システムの構成例を示す図。

[図2]実施の形態 1 に係る証明装置の構成例を示す図。

[図3]実施の形態 1 に係る認証装置の構成例を示す図。

[図4]実施の形態 1 に係る復号装置の構成例を示す図。

[図5]実施の形態 1 に係るセットアップ処理の例を示すフローチャート図。

[図6]実施の形態 1 に係る生体情報の登録処理の例を示すフローチャート図。

[図7]実施の形態 1 に係る認証処理の例を示すフローチャート図。

[図8]実施の形態 1 に係る認証処理の例を示すフローチャート図。

[図9]実施の形態 1 に係る認証処理の例を示すフローチャート図。

[図10]実施の形態 2 に係る生体情報の登録処理の例を示すフローチャート図

。

[図11]実施の形態 2 に係る認証処理の例を示すフローチャート図。

[図12]実施の形態 2 に係る認証処理の例を示すフローチャート図。

[図13]実施の形態 3 に係るセットアップ処理の例を示すフローチャート図。

[図14]実施の形態 3 に係る生体情報の登録処理の例を示すフローチャート図

。

[図15]実施の形態 3 に係る認証処理の例を示すフローチャート図。

[図16]実施の形態 3 に係る認証処理の例を示すフローチャート図。

[図17]実施の形態 3 に係る認証処理の例を示すフローチャート図。

[図18]実施の形態 4 に係る認証処理の例を示すフローチャート図。

[図19]実施の形態 4 に係る認証処理の例を示すフローチャート図。

[図20]実施の形態 4 に係る認証処理の例を示すフローチャート図。

[図21]実施の形態 1 に係るセットアップ処理の概要を示すフローチャート図

。

[図22]実施の形態 1 に係る生体情報の登録処理の概要を示すフローチャート図。

[図23]実施の形態 1 に係る認証処理の概要を示すフローチャート図。

[図24]実施の形態 1 に係る認証処理の概要を示すフローチャート図。

[図25]実施の形態1に係る証明装置、認証装置、復号装置のハードウェア構成例を示す図。

発明を実施するための形態

[0025] 以下に示す実施の形態では、生体情報を保護するための暗号方式として、通常の準同型暗号ではなく、二重準同型暗号 (Doubly Homomorphic Encryption) と呼ばれる暗号を用いる。

ここで二重準同型暗号とは、通常の準同型暗号とは異なり、例えば $2T$ 個の暗号文 $E(x_1), E(x_2), \dots, E(x_T), E(y_1), E(y_2), \dots, E(y_T)$ を用いて暗号文 $E(x_1 * y_1 + x_2 * y_2 + \dots + x_T * y_T)$ が計算できるというように、複数の暗号文から元の平文の有限体上の和と積を組み合わせた暗号文を計算できる暗号である。

つまり、以下に示す実施の形態では、登録用の生体情報は T (T は2以上の整数) 個の部分データから構成され、認証用の生体情報は T (T は2以上の整数) 個の部分データから構成される。

そして、登録されている T 個の部分データと、認証用として入力された T 個の部分データにおいて値が一致する部分データの数やハミング距離等を類似度として導出して、類似度が所定レベル以上であれば本人であると認証する。

[0026] 二重準同型暗号の具体的なアルゴリズムとしては、例えば非特許文献1から非特許文献3に開示のアルゴリズムがある。

生体認証においてこれらの二重準同型暗号を利用するには、生体情報から特徴ベクトルを生成する方法と、特徴ベクトルに対する二重準同型暗号の適用方法とにそれぞれ工夫を加える必要がある。

[0027] 生体認証では、本人判定をするための指標に様々な種類があり、それに応じて特徴ベクトルの生成方法にも様々な種類がある。

しかし、二重準同型暗号の特性を生かして平文の特徴ベクトルを認証処理時に不要とするためには、本人判定の指標をそのまま用いてもよいというわけではない。

以下の実施の形態では、特徴点の有無を 1, 0 のビット列で表現し、1 のビットが一致した箇所の数の多さを指標とすることにより本人判定をする方法、ビット列同士のハミング距離を指標とすることにより本人判定をする方法、数値列同士のユークリッド二乗距離を指標とすることにより本人判定をする方法、を開示する。

[0028] また、本人判定の方法に合わせて各文献の暗号の適用方法を工夫する必要がある。

本発明では、実施の形態 1 および実施の形態 2 において非特許文献 1 の適用方法を開示し、実施の形態 3 および実施の形態 4 において非特許文献 2 の適用方法を開示する。

[0029] ここで、非特許文献 1 の岡本一高島暗号のアルゴリズムを、実施の形態 1 および実施の形態 2 の説明に必要となる範囲に限って説明する。

[0030] 岡本一高島暗号は、楕円曲線を用いて定義される双対ペアリングベクトル空間を用いた暗号である。

この双対ペアリングベクトル空間を構成する方法は複数考えられるが、ここでは楕円曲線の直積により構成する方法に基づいて説明する。

なお、楕円曲線上の群の演算は一般に加法群の演算として記述されることが多いが、ここでは有限体上の演算も含めすべて乗法群として記述する。

また、非対称ペアリングを用いたより一般的な方式に従って記述する。

[0031] G 、 $G^\wedge$ 、 G_T をそれぞれ素数位数 q の群とする。

$F_q = \{0, 1, \dots, q-1\}$ とする。

$e : G \times G^\wedge \rightarrow G_T$ を、双線型性（任意の $u \in G$, $v^\wedge \in G^\wedge$, $a, b \in F_q$ に対して $e(u^a, v^{\wedge b}) = e(u, v^\wedge)^{ab}$ となる性質）および非退化性（ $e(g, g^\wedge) \neq 1$ であるような $g \in G$, $g^\wedge \in G^\wedge$ が存在する性質）を満たすペアリングとする。

N 個の群 G の直積集合を $V = G \times G \times \dots \times G$ 、同じく N 個の群 $G^\wedge$ の直積集合を $V^\wedge = G^\wedge \times G^\wedge \times \dots \times G^\wedge$ とする。

このとき、数 4 に示す関係が成り立つ。

[0032] [数4]

$$\mathbf{x} = (g^{x_1}, g^{x_2}, \dots, g^{x_N}) \in V, \mathbf{y} = (g^{y_1}, g^{y_2}, \dots, g^{y_N}) \in V, \alpha \in F_q \text{ に対して、}$$

$$\mathbf{x} + \mathbf{y} = (g^{x_1+y_1}, g^{x_2+y_2}, \dots, g^{x_N+y_N})$$

$$\alpha \mathbf{x} = (g^{\alpha x_1}, g^{\alpha x_2}, \dots, g^{\alpha x_N})$$

と定義すると、 V はベクトル空間を構成する。

同様に、

$$\hat{\mathbf{x}} = (\hat{g}^{x_1}, \hat{g}^{x_2}, \dots, \hat{g}^{x_N}) \in \hat{V}, \hat{\mathbf{y}} = (\hat{g}^{y_1}, \hat{g}^{y_2}, \dots, \hat{g}^{y_N}) \in \hat{V}, \alpha \in F_q \text{ に対して、}$$

$$\hat{\mathbf{x}} + \hat{\mathbf{y}} = (\hat{g}^{x_1+y_1}, \hat{g}^{x_2+y_2}, \dots, \hat{g}^{x_N+y_N})$$

$$\alpha \hat{\mathbf{x}} = (\hat{g}^{\alpha x_1}, \hat{g}^{\alpha x_2}, \dots, \hat{g}^{\alpha x_N})$$

と定義すると、 $\hat{V}$ はベクトル空間を構成する。

なお、本明細書では $\hat{G}, \hat{g}, \hat{v}$ 等の「 $\hat{}$ 」が文字の上に付された記号と $G^{\wedge}, g^{\wedge}, v^{\wedge}$ 等の「 $\wedge$ 」が文字の横に付された記号は同じものとする。後述の $A^{\wedge}, C^{\wedge}, a^{\wedge}, c^{\wedge}, d^{\wedge}, w^{\wedge}$ 等についても同様である。

[0033] 2つのベクトル空間 $V, \hat{V}$ のペアリングとして、

$$u = (u_1, u_2, \dots, u_N) \in V, \hat{v} = (\hat{v}_1, \hat{v}_2, \dots, \hat{v}_N) \in \hat{V} \text{ に対するペアリングを、数5のように定義する。}$$

[0034] [数5]

$$e(\mathbf{u}, \hat{\mathbf{v}}) = \prod_{i=1}^N e(u_i, \hat{v}_i)$$

[0035] ベクトル空間 $V, \hat{V}$ において、数6に示す関係が成り立つ。

[0036]

[数6]

$$\mathbf{a}_1 = (g, 1, 1, \dots, 1), \mathbf{a}_2 = (1, g, 1, \dots, 1), \dots, \mathbf{a}_N = (1, 1, 1, \dots, g)$$

$$\hat{\mathbf{a}}_1 = (\hat{g}, 1, 1, \dots, 1), \hat{\mathbf{a}}_2 = (1, \hat{g}, 1, \dots, 1), \dots, \hat{\mathbf{a}}_N = (1, 1, 1, \dots, \hat{g})$$

とすると、 $\mathbf{A} = (\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_N)$, $\hat{\mathbf{A}} = (\hat{\mathbf{a}}_1, \hat{\mathbf{a}}_2, \dots, \hat{\mathbf{a}}_N)$ はそれぞれベクトル空間 $V, \hat{V}$ の基底となる。また、 $\mathbf{A}, \hat{\mathbf{A}}$ は、 $e(\mathbf{a}_i, \hat{\mathbf{a}}_j) = e(g, \hat{g})^{\delta_{i,j}}$ を満たす。

ここで $\delta_{i,j}$ はクロネッカーのデルタである。この基底 $\mathbf{A}, \hat{\mathbf{A}}$ を標準基底と呼ぶ。

[0037] $\mathbf{x} = x_1 \mathbf{a}_1 + x_2 \mathbf{a}_2 + \dots + x_N \mathbf{a}_N \in V$ とする。

ベクトル空間 V におけるディストーション写像 $\phi_{i,j} : V \rightarrow V$ を、 $\phi_{i,j}(x) = x_j \mathbf{a}_i$ と定義する。

同様に、 $\hat{\mathbf{x}} = x_1 \hat{\mathbf{a}}_1 + x_2 \hat{\mathbf{a}}_2 + \dots + x_N \hat{\mathbf{a}}_N \in \hat{V}$ に対し、 $\hat{\phi}_{i,j} : \hat{V} \rightarrow \hat{V}$ を、 $\hat{\phi}_{i,j}(\hat{\mathbf{x}}) = x_j \hat{\mathbf{a}}_i$ と定義する。

このようなディストーション写像は容易に計算可能である。

[0038] このように、標準基底があり、空間同士のペアリングが定義され、計算可能なディストーション写像が定義された2つのベクトル空間を双対ペアリングベクトル空間という。

[0039] $X = (X_{i,j})$, $\hat{X} = (\hat{X}_{i,j})$ を、各要素が F_q から一様ランダムに選ばれた値で構成される N 行 N 列の正方行列とする。

このように構成した X , $\hat{X}$ はきわめて高い確率で正則行列となる。

このような正則行列を用いて、数7に示すように定義すると、 $W = (w_1, w_2, \dots, w_N)$, $\hat{W} = (\hat{w}_1, \hat{w}_2, \dots, \hat{w}_N)$ もまた基底となる。この基底をランダム基底と呼ぶ。

[0040] [数7]

$$\mathbf{w}_i = \sum_{j=1}^N \chi_{i,j} \mathbf{a}_j, \hat{\mathbf{w}}_i = \sum_{j=1}^N \hat{\chi}_{i,j} \hat{\mathbf{a}}_j$$

[0041] 非特許文献1によれば、ベクトル空間 V , $\hat{V}$ におけるランダム基底 $W =$

$(w_1, w_2, \dots, w_N)$, $\hat{W} = (\hat{w}_1, \hat{w}_2, \dots, \hat{w}_N)$ に関して、以下の性質が成り立つ。

[0042] F^{N_q} の要素 $(x_1, x_2, \dots, x_N)$ が与えられたとき、 $x = x_1 w_1 + x_2 w_2 + \dots + x_N w_N$, $\hat{x} = x_1 \hat{w}_1 + x_2 \hat{w}_2 + \dots + x_N \hat{w}_N$ を得ることは容易である。

しかし、 $x = x_1 w_1 + x_2 w_2 + \dots + x_L w_L$, $\hat{x} = x_1 \hat{w}_1 + x_2 \hat{w}_2 + \dots + x_L \hat{w}_L$ ($1 < L \leq N$) が与えられたときに、 $X = (X_{i,j})$, $\hat{X} = (\hat{X}_{i,j})$ を用いずしてベクトル $y = x_1 w_1 + x_2 w_2 + \dots + x_L w_L$, $\hat{y} = x_1 \hat{w}_1 + x_2 \hat{w}_2 + \dots + x_L \hat{w}_L$ ($1 \leq l < L$) を得ることは、一般化された Diffie-Hellman 計算問題と同程度に難しいことが知られている。

一方で、 $X = (X_{i,j})$, $\hat{X} = (\hat{X}_{i,j})$ を用いるならば、以下のアルゴリズム Deco (数 8) により上記のようなベクトル分解が容易に計算可能である。なお、数 8 中の k は整数である。

[0043]

[数8]

$$\text{Deco}(\mathbf{x}, \langle \mathbf{w}_1, \dots, \mathbf{w}_l \rangle, X) :$$

$$(t_{i,j}) \leftarrow X^{-1}$$

$$\mathbf{y} \leftarrow \sum_{i=1}^L \sum_{j=1}^l \sum_{k=1}^L t_{i,j} x_{j,k} \phi_{k,i}(\mathbf{x})$$

$$\text{Deco}(\hat{\mathbf{x}}, \langle \hat{\mathbf{w}}_1, \dots, \hat{\mathbf{w}}_l \rangle, \hat{X}) :$$

$$(\hat{t}_{i,j}) \leftarrow \hat{X}^{-1}$$

$$\hat{\mathbf{y}} \leftarrow \sum_{i=1}^L \sum_{j=1}^l \sum_{k=1}^L \hat{t}_{i,j} \hat{x}_{j,k} \hat{\phi}_{k,i}(\hat{\mathbf{x}})$$

[0044] この性質から、正則行列を秘密鍵とすることによりトラップドア関数を実現できる。

[0045] 以下、双対ペアリングベクトル空間を用いて、生体情報を暗号化したまま生体認証を行う方法の例を説明する。

[0046] 実施の形態 1 .

本実施の形態では、生体認証で用いる特徴ベクトルとして、特徴点の配列を用意し、ユーザがその特徴点を保有する場合に 1、特徴点を保有しない場合に 0 を配列に格納して、配列を特徴ベクトルとし、認証時には 1 が一致している箇所数を類似度の指標とするような認証方式を例に説明する。

[0047] より詳しく言うと、例えば指紋認証の場合、指紋画像を小領域に分割しその領域内で隆線の流れる方向を調べると、個人ごとに各領域における流れの方向に特徴が出る。

そこで、例えば各領域について 4 つの流れの方向（0 度、45 度、90 度

、１３５度など）を定義しておき、検出した流れの方向を１、それ以外を０として、N個すべての領域について各４個の配列を用意し、検出値にしたがって配列値を定めることで特徴ベクトルとするような認証方式を考える。

[0048] このような認証方式においては、同一人物の特徴ベクトルでは１の位置がほぼ同じであるため、登録した特徴ベクトルと認証対象の特徴ベクトルの内積値が大きくなることが期待される。

一方、別人物の特徴ベクトルでは１の位置が本人のときよりも異なることが多いため、２つの特徴ベクトルの内積値が小さくなることが期待される。

[0049] 図１は、実施の形態１－４に係る生体認証システムの構成例を示す図である。

[0050] 図１において、証明装置１０１はユーザから生体情報を測定し、測定した生体情報を用いて秘匿照合処理を行う装置である。

認証装置１０２は、ユーザの生体情報を暗号化して格納しておくとともに、格納した暗号化された生体情報を用いて認証を行う装置である。

復号装置１０３は、暗号化データを復号する装置である。

なお、証明装置１０１は暗号装置の例であり、認証装置はデータ処理装置の例である。

[0051] 図２は、証明装置１０１の内部構成の構成例を示す図である。

[0052] 図２において、生体情報抽出部２０１は、光学カメラ、赤外線カメラなどの各種センサを用いて、個人識別を行うのに必要となる生体情報をユーザから抽出する。

特徴ベクトル形成部２０２は、生体情報抽出部２０１で抽出された生体情報から、個人の特徴を表す特徴ベクトルを形成する。

乱数生成部２０３は、公開鍵の一部を用いて乱数を生成する。

暗号化部２０４は、乱数生成部２０３が生成した乱数を用いて特徴ベクトルを暗号化する。

記憶部２０５は、公開鍵などの各種データを格納する。記憶部２０５が記憶する公開鍵は、復号装置１０３で生成され、復号装置１０３から配布され

た公開鍵である。

通信部 206 は、データベースなど他の装置との間でデータの送受信を行う。

[0053] 図 3 は、認証装置 102 の内部構成の構成例を示す図である。

[0054] 図 3 において、記憶部 301 は、暗号化された特徴ベクトル（以下、暗号化特徴ベクトルともいう）や公開鍵などの各種データを格納する。記憶部 301 は、公開鍵記憶部及び暗号化データ記憶部の例である。

なお、記憶部 301 が記憶する暗号化特徴ベクトルは、証明装置 101 により暗号化された登録用の特徴ベクトルである。暗号化前の登録用の特徴ベクトルが第 1 データの例に相当し、暗号化特徴ベクトルが暗号化第 1 データの例に相当する。

また、記憶部 301 が記憶する公開鍵は、復号装置 103 で生成され、復号装置 103 から配布された公開鍵である。

[0055] 暗号化類似度生成部 302 は、登録されている暗号化特徴ベクトルと、認証用の暗号化特徴ベクトルから、暗号化類似度情報を算出する。

認証用の暗号化特徴ベクトルは、証明装置 101 により暗号化された認証用の特徴ベクトルである。暗号化前の認証用の特徴ベクトルが第 2 データの例に相当し、暗号化特徴ベクトルが暗号化第 2 データの例に相当する。

また、暗号化類似度情報は、公開鍵に対応付けられて生成された秘密鍵を用いた復号処理により登録用の特徴ベクトル（第 1 データ）と認証用の特徴ベクトル（第 2 データ）との間の類似度を復号装置 103 において導出可能な暗号化された情報である。

[0056] 判定部 303 は、復号された類似度から個人識別を行い、本人か否かを判定する。

つまり、判定部 303 は、類似度を解析して、認証用の特徴ベクトルの発生源が正当であるか否かを判定する。

[0057] 通信部 304 は、証明装置 101 や復号装置 103 との間でデータの送受信を行う。

より具体的には、通信部 304 は、登録用の暗号化特徴ベクトルが記憶部 301 に格納された後に証明装置 101 から認証用の暗号化特徴ベクトルを受信する。

また、通信部 304 は、暗号化類似度生成部 302 により生成された暗号化類似度情報を復号装置 103 に送信する。

また、通信部 304 は、復号装置 103 において暗号化類似度情報に対して秘密鍵を用いた復号処理が行われて導出された登録用の特徴ベクトルと認証用の特徴ベクトルとの間の類似度（平文）を受信する。

通信部 304 は、暗号化データ入力部、暗号化類似度出力部及び類似度入力部の例である。

[0058] 乱数生成部 305 は、公開鍵の一部を用いて乱数を生成する。

[0059] 図 4 は復号装置 103 の内部構成の構成例を示す図である。

[0060] 図 4 において、パラメータ生成部 401 は、公開鍵や秘密鍵など、暗号化と復号に必要なパラメータを生成する。

復号部 402 は、暗号化類似度情報を復号し、平文の類似度を取り出す。

記憶部 403 は、公開鍵や秘密鍵などの各種データを格納する。

通信部 404 は、データベースなど他の装置との間でデータの送受信を行う。

[0061] 次に、本実施の形態に係るデータ処理方法を説明する。

[0062] まず、動作の全体像を説明する。

動作は、セットアップ処理、登録処理、認証処理の 3 つに分かれる。

セットアップ処理では、復号装置 103 が、暗号化と復号に必要なパラメータを生成する。

登録処理では、証明装置 101 がユーザの生体情報を暗号化して認証装置 102 に送付し、認証装置 102 が記憶部 301 に格納する。

認証処理では、まず証明装置 101 がユーザの生体情報を暗号化して認証装置 102 に送付する。次に、認証装置 102 が、記憶部 301 の暗号化生体情報と受領した暗号化生体情報を用いて暗号化類似度情報を生成し復号装

置 103 に送付する。次に、復号装置 103 が類似度を復号し、認証装置 102 に復号された類似度を送付する。最後に認証装置 102 が類似度とすべき値とを比較し、認証をする。

[0063] 以下、図 21－図 24 を用いて、各処理の概要を説明する。

図 21 がセットアップ処理の概要を示し、図 22 が登録処理の概要を示し、図 23 及び図 24 が認証処理の概要を示す。

[0064] まず、図 21 を参照して、セットアップ処理の概要を説明する。

最初に、復号装置 103 のパラメータ生成部 401 が、岡本－高島暗号アルゴリズムに基づき、秘密鍵 s_k と公開鍵 p_k を生成する (S2101)。

次に、復号装置 103 の記憶部 403 が秘密鍵 s_k を記憶し、通信部 404 が公開鍵 p_k を証明装置 101 及び認証装置 102 に送信する (S2102)。

次に、証明装置 101 では、通信部 206 が公開鍵 p_k を受信し、記憶部 205 が公開鍵 p_k を記憶し、認証装置 102 では、通信部 304 が公開鍵 p_k を受信し、記憶部 301 が公開鍵 p_k を記憶する (S2102)。

なお、ここでは、公開鍵 p_k を送受信する例を説明しているが、証明装置 101 及び認証装置 102 に公開鍵 p_k を配布する方法は他の方法でもよい。

例えば、復号装置 103 が公開鍵 p_k を記録媒体に格納し、証明装置 101 及び認証装置 102 において当該記録媒体から公開鍵 p_k を読み出して格納するようにしてもよい。

[0065] 次に、図 22 を参照して、登録処理の概要を説明する。

最初に、証明装置 101 において、生体情報抽出部 201 が、ユーザの生体情報を抽出する (S2201)。

次に、証明装置 101 の特徴ベクトル形成部 202 が、S2201 で抽出された生体情報の特徴ベクトル b を生成する (S2202)。

次に、証明装置 101 の乱数生成部 203 が公開鍵 p_k の一部を用いて乱数を生成し、また、暗号化部 204 が記憶部 205 から公開鍵 p_k を読み出

し、暗号化部204が公開鍵 p_k と乱数を用いて特徴ベクトル b を暗号化する(S2203)。

次に、証明装置101の通信部206が、暗号化された特徴ベクトル C を認証装置102に送信する(S2204)。

次に、認証装置102の通信部304が、暗号化された特徴ベクトル C を受信し、記憶部205が暗号化された特徴ベクトル C を記憶する(S2205)。

[0066] 次に、図23及び図24を参照して、認証処理の概要を説明する。

最初に、証明装置101において、生体情報抽出部201が、ユーザの生体情報を抽出する(S2301)。

次に、証明装置101の特徴ベクトル形成部202が、S2301で抽出された生体情報の特徴ベクトル b' を生成する(S2302)。

次に、証明装置101の乱数生成部203が公開鍵 p_k の一部を用いて乱数を生成し、また、暗号化部204が記憶部205から公開鍵 p_k を読み出し、暗号化部204が公開鍵 p_k と乱数を用いて特徴ベクトル b' を暗号化する(S2303)。

次に、証明装置101の通信部206が、暗号化された特徴ベクトル $C^{\wedge}$ を認証装置102に送信する(S2304)。

次に、認証装置102の通信部304が、暗号化された特徴ベクトル $C^{\wedge}$ を受信する(S2305)。

[0067] 次に、認証装置102の暗号化類似度生成部302が、記憶部301の暗号化特徴ベクトル C を読み出す(S2401)。

次に、認証装置102の乱数生成部305が公開鍵 p_k の一部を用いて乱数を生成し、また、暗号化類似度生成部302が記憶部301から公開鍵 p_k を読み出し、暗号化類似度生成部302が記憶部301から読み出した暗号化特徴ベクトル C と証明装置101から受信した暗号化特徴ベクトル $C^{\wedge}$ に対して、公開鍵 p_k と乱数を用いて暗号化類似度情報を生成する(S2402)。

認証装置 102 は、公開鍵 p_k に対応付けられている秘密鍵 s_k を知らないで、暗号化特徴ベクトル C 及び暗号化特徴ベクトル $C^{\wedge}$ を復号することはできない。このため、暗号化特徴ベクトル C 及び暗号化特徴ベクトル $C^{\wedge}$ が暗号化された状態のままで、暗号化類似度情報が生成される。

[0068] 次に、認証装置 102 の通信部 304 が、暗号化類似度情報を復号装置 103 に送信する (S2403)。

次に、復号装置 103 の通信部 404 が、暗号化類似度情報を受信する (S2404)。

次に、復号装置 103 の復号部 402 が、パラメータ生成部 401 から秘密鍵 s_k を読み出し、暗号化類似度情報に秘密鍵 s_k を用いて復号処理を行い、平文の類似度を導出する (S2405)。

次に、復号装置 103 の通信部 404 が、平文の類似度を認証装置 102 に送信する (S2406)。なお、類似度は、登録用の特徴ベクトル b と認証用の特徴ベクトル b' がどの程度類似しているかを示す情報であり、類似度からは特徴ベクトル、生体情報を計算することはできない。

次に、認証装置 102 の通信部 304 が、平文の類似度を受信する (S2407)。

次に、認証装置 102 の判定部 303 が、平文の類似度が所定のしきい値以上であるか否かを判定し、しきい値以上であれば本人であると判定し、しきい値を下回っている場合は、本人ではないと判定する (S2408)。

[0069] 以下、図 5－図 9 を参照して、各処理の動作をより詳しく説明する。

図 5 がセットアップ処理の詳細を示し、図 6 が登録処理の詳細を示し、図 7－図 9 が認証処理の詳細を示す。

[0070] まず、図 5 を用いてセットアップについて説明する。

セットアップでは、復号装置 103 が、公開鍵 p_k および秘密鍵 s_k を生成する。

この公開鍵 p_k および秘密鍵 s_k は、ユーザごとに異なる公開鍵および秘密鍵であってもよいし、システムに 1 つの公開鍵および秘密鍵であってもよ

い。

ここでは、説明を簡単にするために、システムに1つの公開鍵および秘密鍵を用いる場合について説明するが、これをユーザごとの公開鍵および秘密鍵の場合に拡張するのは容易である。

[0071] 図5は、パラメータ生成部401における公開鍵 p_k 及び秘密鍵 s_k の生成手順を示したフローチャートである。

[0072] はじめに、ステップS501にて、パラメータ生成部401は、群位数 q 、群 G 、 $G^\wedge$ 、 G_T 、生成元 $g \in G$ 、 $g^\wedge \in G^\wedge$ を定める。

この具体的な方法は例えば非特許文献4にあるので、ここでは省略する。

なお、群位数はセキュリティレベルに応じて定まるが、通常は200ビットや1024ビットなどの大きなサイズの素数とする。

[0073] 次に、ステップS502にて、パラメータ生成部401は、ベクトル空間を $V = G \times G \times G$ 、 $V^\wedge = G^\wedge \times G^\wedge \times G^\wedge$ とし、標準基底 $A = (a_1, a_2, a_3)$ 、 $A^\wedge = (a^\wedge_1, a^\wedge_2, a^\wedge_3)$ を定める。

この定め方はすでに述べたとおりである。

[0074] 次に、ステップS503にて、パラメータ生成部401は、0から $q-1$ までの整数から一様ランダムに値を9回取り出し、それらを用いて3行3列の行列 $X = (X_{i,j})$ を定める。

この行列は正則行列でなければならないが、この方法で行列を定めることによりきわめて高い確率で正則行列になる。なお、より正確性を期すのであれば、このように行列を定めた後に行列式を計算する方法により正則性を判定し、正則でなければ行列の要素を再度ランダムに選べばよい。

[0075] 次に、ステップS504にて、パラメータ生成部401は、0から $q-1$ までの整数から一様ランダムに値を9回取り出し、それらを用いて3行3列の行列 $X^\wedge = (X^\wedge_{i,j})$ を定める。

この行列はきわめて高い確率で正則行列になるが、正則行列にならなかった場合には再度ランダムに選べばよい。

[0076] 次に、ステップS505にて、パラメータ生成部401は、以下の数9お

よび数 10 によりランダム基底 $W = (w_1, w_2, w_3)$, $W^{\wedge} = (w^{\wedge}_1, w^{\wedge}_2, w^{\wedge}_3)$ を定める。

[0077] [数9]

$$w_i = \sum_{j=1}^3 \chi_{i,j} a_j$$

[0078] [数10]

$$\hat{w}_i = \sum_{j=1}^3 \hat{\chi}_{i,j} \hat{a}_j$$

[0079] 最後に、ステップ S506 にて、パラメータ生成部 401 は、公開鍵 $p_k = (q, V, V^{\wedge}, e, G_T, A, A^{\wedge}, W, W^{\wedge})$ を公開し、秘密鍵 $s_k = (X, X^{\wedge})$ を記憶部 403 に格納する。

[0080] 次に、図 6 を用いて、生体情報の登録方法を説明する。

[0081] なお、ここではユーザが証明装置 101 を経由して認証装置 102 に生体情報を登録する場合について説明するが、認証装置 102 上で直接生体情報を登録する場合や、登録用の専用装置を経由して登録する場合などにおいても同様の手順により実現できる。

[0082] 図 6 は、証明装置 101 において生体情報を登録する手順を示したフローチャートである。

[0083] はじめに、ステップ S601 にて、生体情報抽出部 201 が、ユーザの生体情報を抽出する。

これには様々な方法があるが、例えば指紋に光を当てて紋様をセンサで読み取るといったことにより抽出する。

[0084] 次に、ステップ S602 にて、特徴ベクトル形成部 202 が、生体情報から特徴ベクトル $b = (b_1, b_2, \dots, b_T)$ を形成する。

ここで T は特徴ベクトルを格納する配列の大きさであり、特徴ベクトルの

形成方法によって決まる値である。

本実施の形態の形成方法は、読み取った紋様を領域分割し、各領域で特徴点の有無を検出し、特徴点がある箇所配列に1、ない箇所配列に0を格納することにより特徴ベクトルを形成するという方法である。

[0085] 次に、ステップS603にて、乱数生成部203が、0から $q-1$ までの整数から一様ランダムに値を $2T$ 回取り出し、 $\{r_{2,i}, r_{3,i}\}_{i=1,2,\dots,T}$ とする。

なお、 $q-1$ の q は、公開鍵 p_k に含まれている q である。

[0086] 次に、ステップS604にて、暗号化部204が、 $c_i = b_i w_1 + r_{2,i} w_2 + r_{3,i} w_3$ により暗号化特徴ベクトル $C = (c_1, c_2, \dots, c_T)$ を計算する。

なお、 w_1, w_2, w_3 は、公開鍵の一部(W)として、復号装置103から配布されたものである。

[0087] 次に、ステップS605にて、通信部206が、暗号化特徴ベクトル $C = (c_1, c_2, \dots, c_T)$ を認証装置102に送信する。

その際、例えばSSL(Secure Sockets Layer)などの通信用改ざん検出技術を用いて通信の途中で改ざんが行われないようにすることが望ましい。

[0088] 最後に、ステップS606にて、認証装置102において、通信部304が暗号化特徴ベクトル $C = (c_1, c_2, \dots, c_T)$ を受信し、記憶部301に格納する。

[0089] 次に、図7ないし図9を用いて、認証方法を説明する。

なお、簡単のためここでは認証時に認証の対象となるユーザが別途ID情報などによって特定されているいわゆる1:1認証の場合について説明する。

[0090] 図7、図8、図9は、認証を行う手順を示したフローチャートである。

[0091] はじめに、ステップS701にて、証明装置101の生体情報抽出部201がユーザの生体情報を抽出する。

抽出方法は生体情報の登録時と同様である。

- [0092] 次に、ステップS702にて、証明装置101の特徴ベクトル形成部202が、生体情報から特徴ベクトル $b' = (b'_1, b'_2, \dots, b'_T)$ を形成する。

形成方法は、生体情報の登録時と同様である。

- [0093] 次に、ステップS703にて、証明装置101の乱数生成部203が、0から $q-1$ までの整数から一様ランダムに値を $2T$ 回取り出し、 $\{r'_{2,i}, r'_{3,i}\}_{i=1,2,\dots,T}$ とする。

- [0094] 次に、ステップS704にて、証明装置101の暗号化部204が、 $c^i = (b'_i w^1 + r'_{2,i} w^2 + r'_{3,i} w^3)$ により暗号化特徴ベクトル $C^i = (c^1, c^2, \dots, c^T)$ を計算する。

なお、 w^1, w^2, w^3 は、公開鍵の一部(W^i)として、復号装置103から配布されたものである。

- [0095] 次に、ステップS705にて、証明装置101の通信部206が、暗号化特徴ベクトル $C^i = (c^1, c^2, \dots, c^T)$ を認証装置102に送信する。

その際、例えばSSLなどの通信用改ざん検出技術を用いて通信の途中で改ざんが行われないようにすることが望ましい。

- [0096] 次に、ステップS706にて、認証装置102の通信部304が、暗号化特徴ベクトル $C^i = (c^1, c^2, \dots, c^T)$ を受信する。

- [0097] 次に、ステップS707にて、認証装置102において、暗号化類似度生成部302が、記憶部301から暗号化特徴ベクトル $C = (c_1, c_2, \dots, c_T)$ を取り出す。

このとき、一般に記憶部301には多数のユーザの暗号化生体情報が格納されているが、その中からどれを取り出すかについては、別途与えられるID情報を用いる。

- [0098] 次に、ステップS708にて、認証装置102の乱数生成部305が、0から $q-1$ までの整数から一様ランダムに値を $6T$ 回取り出し、 $\{s_{1,i}, s$

$\{s_{2,i}, s_{3,i}, \hat{s}_{1,i}, \hat{s}_{2,i}, \hat{s}_{3,i}\} \quad i=1, 2, \dots, T$ とする。

[0099] 次に、ステップS709にて、認証装置102の乱数生成部305が、0から $q-1$ までの整数から一様ランダムに値を4回取り出し、 $\{u_2, u_3, \hat{u}_2, \hat{u}_3\}$ とする。

[0100] 次に、ステップS710にて、認証装置102の暗号化類似度生成部302が、 $d_i = c_i + s_{1,i}w_1 + s_{2,i}w_2 + s_{3,i}w_3$ を計算する。

暗号化類似度生成部302は、これをすべての $i=1, 2, \dots, T$ について行う。

なお、 w_1, w_2, w_3 は、公開鍵の一部(W)として、復号装置103から配布されたものである。

[0101] 次に、ステップS711にて、認証装置102の暗号化類似度生成部302が、 $\hat{d}_i = \hat{c}_i + \hat{s}_{1,i}\hat{w}_1 + \hat{s}_{2,i}\hat{w}_2 + \hat{s}_{3,i}\hat{w}_3$ を計算する。

暗号化類似度生成部302は、これをすべての $i=1, 2, \dots, T$ について行う。

なお、 $\hat{w}_1, \hat{w}_2, \hat{w}_3$ は、公開鍵の一部($\hat{W}$)として、復号装置103から配布されたものである。

[0102] 次に、ステップS712にて、認証装置102の暗号化類似度生成部302が、数11に従って、 E を計算する。

[0103] [数11]

$$E = \sum_{i=1}^T (\hat{s}_{1,i}c_i + s_{1,i}\hat{s}_{1,i}w_1) + u_2w_2 + u_3w_3$$

[0104] 次に、ステップS713にて、認証装置102の暗号化類似度生成部302が、数12に従って、 $\hat{E}$ を計算する。

[0105]

[数12]

$$\hat{E} = \sum_{i=1}^T s_{1,i} \hat{\mathbf{c}}_i + \hat{u}_2 \hat{\mathbf{b}}_2 + \hat{u}_3 \hat{\mathbf{b}}_3$$

[0106] 次に、ステップS 7 1 4にて、認証装置1 0 2の通信部3 0 4が、 $(d_1, \dots, d_T, \hat{d}_1, \dots, \hat{d}_T, E, \hat{E})$ を復号装置1 0 3へ送信する。

その際、例えばSSLなどの通信用改ざん検出技術を用いて通信の途中で改ざんが行われないようにすることが望ましい。

なお、上記 $(d_1, \dots, d_T, \hat{d}_1, \dots, \hat{d}_T, E, \hat{E})$ が、一体となって暗号化類似度情報を構成する。

[0107] 次に、ステップS 7 1 5にて、復号装置1 0 3の通信部4 0 4が、 $(d_1, \dots, d_T, \hat{d}_1, \dots, \hat{d}_T, E, \hat{E})$ を受信する。

[0108] 次に、ステップS 7 1 6にて、復号装置1 0 3の復号部4 0 2が、記憶部4 0 3から秘密鍵 $s_k = (X, \hat{X})$ を取り出す。

[0109] 次に、ステップS 7 1 7にて、復号装置1 0 3の復号部4 0 2が、 X の逆行列 $X^{-1} = (t_{i,j})$ および $\hat{X}$ の逆行列 $\hat{X}^{-1} = (\hat{t}_{i,j})$ を計算する。

なお、この値は毎回計算するのではなく、あらかじめ計算した状態で記憶部4 0 3に格納しておき、それを取り出すものとしてもよい。

[0110] 次に、ステップS 7 1 8にて、復号装置1 0 3が、数1 3に従って Z_1 を計算する。

[0111] [数13]

$$Z_1 = \prod_{i=1}^T e(\text{Deco}(\mathbf{d}_i, \langle \mathbf{w}_1 \rangle, X), \text{Deco}(\hat{\mathbf{d}}_i, \langle \hat{\mathbf{w}}_1 \rangle, \hat{X}))$$

[0112] ここで、Decoアルゴリズムは以下の数1 4のように計算される。なお、数1 4中の k は整数である。

[0113]

[数14]

$$\text{Deco}(\mathbf{d}_i, \langle \mathbf{w}_1 \rangle, X) :$$

$$\mathbf{y} = \sum_{i=1}^3 \sum_{k=1}^3 t_{i,1} x_{1,k} \phi_{k,i}(\mathbf{d}_i)$$

$$\text{Deco}(\hat{\mathbf{d}}_i, \langle \hat{\mathbf{w}}_1 \rangle, \hat{X}) :$$

$$\hat{\mathbf{y}} = \sum_{i=1}^3 \sum_{k=1}^3 \hat{t}_{i,1} \hat{x}_{1,k} \phi_{k,i}(\hat{\mathbf{d}}_i)$$

[0114] 次に、ステップS719にて、復号装置103の復号部402が、 $Z_2 = e(\text{Deco}(E, \langle \mathbf{w}_1 \rangle, X), \mathbf{w}_1) \cdot e(\mathbf{w}_1, \text{Deco}(E, \langle \mathbf{w}_1 \rangle, X))$ を計算する。

このDecoアルゴリズムも上記と同様に計算される。

[0115] 次に、ステップS720にて、復号装置103の復号部402が $Z = Z_1 / Z_2$ を計算する。

[0116] 次に、ステップS721にて、復号装置103の復号部402が $e(g, g)$ を底とするZの離散対数dを計算する。

この離散対数dが、特徴点の一致数に対応しており、類似度を表す。

[0117] なお、離散対数を求める計算は現代の計算機能力では困難とされているが、dが小さい場合には効率的に計算することができる。

本実施の形態においてdは位数qに比べて十分小さいため、効率的に計算することができる。

[0118] 次に、ステップS722にて、復号装置103の通信部404が、類似度dを認証装置102へ送信する。

その際、例えばSSLなどの通信用改ざん検出技術を用いて通信の途中で

改ざんが行われないようにすることが望ましい。

[0119] 次に、ステップS 7 2 3にて、認証装置 1 0 2の通信部 3 0 4が、類似度 d を受信する。

[0120] 次に、ステップS 7 2 4にて、類似度 d がしきい値以上かを判定する。

しきい値は、利用する生体情報の種類や安全性要件などさまざまな要素を勘案してあらかじめシステムで決められた値である。

しきい値以上であれば、証明装置 1 0 1から送られてきた暗号化生体情報はIDで指定された本人のものであると判断する。

一方、しきい値未満であれば、証明装置 1 0 1から送られてきた暗号化生体情報はIDで指定された人物のものではなく、他人のものであると判断する。

[0121] 以上のステップにより、認証装置 1 0 2は証明装置 1 0 1との間で生体認証を行うことができる。

[0122] 以上の実施の形態によれば、認証装置 1 0 2には特徴ベクトルがそのまま保管されるのではなく、暗号化された状態で保管されるため、ユーザにとっては、プライバシー情報である特徴ベクトルが認証装置 1 0 2の管理者に盗み見られるというリスクを低減させることができるという効果がある。

[0123] また、認証装置 1 0 2にとっては、暗号化された特徴ベクトルが仮に漏洩したとしても、元の特徴ベクトル自体が漏洩することはないため、特徴ベクトルそのものを保管するのに比べてデータ管理の手間を削減できるという効果がある。

[0124] また、本実施の形態の手順に従えば、復号装置 1 0 3が復号できるのは類似度という指標値だけであり、特徴ベクトルを復号することはできない。

したがって、証明装置 1 0 1と復号装置 1 0 3が結託しない限り、認証の過程において特徴ベクトルが現れることはないため、生体情報を秘匿したままでの生体認証が可能であるという効果がある。

[0125] また、本実施の形態によれば、認証時に証明装置 1 0 1から認証装置 1 0 2へ暗号化特徴ベクトルを送付すれば、その後は認証装置 1 0 2と復号装置

103との間で認証処理を行うことができるため、特に1:N認証においては、証明装置101と認証装置102との間でユーザ数に比例した回数の通信を行う必要がなく、通信量を低減させることができるという効果がある。

[0126] また、本実施の形態によれば、認証時に証明装置101から認証装置102へ暗号化特徴ベクトルを送付すれば、その後は認証装置102と復号装置103との間で認証処理を行うことができるため、証明装置101上で取得した生体情報をただちに消去できる。

したがって、証明装置101における生体情報の窃取の機会を低減できるという効果がある。

[0127] また、本実施の形態では、特徴ベクトルの構成時に、特徴点がある箇所に1、特徴点がない箇所に0を格納し、1と0から構成されるベクトル同士で内積を取るという構成としたが、これに重要度の概念を導入し、重要な特徴点については重みをつける（たとえば1の代わりに5を格納する）という構成にすることもできる。

このような構成にすれば、単に内積をとる場合に比べて、より精度の高い生体認証を実現することができるという効果がある。

[0128] なお、本実施の形態では3次元の双対ペアリングベクトル空間を用いる方法を開示したが、3次元というのはあくまで例であって、必ずしも3次元である必要はない。

例えば2次元でも実施可能であるし、4次元以上でも実施可能である。

2次元の場合には、本実施の形態中に現れた w_3 、 w^*_3 のベクトルを取り除いて実施すればよい。

このようにすれば、生体情報の登録時や認証時の計算量を低減できるという効果がある。

また、4次元以上の場合には、増えた分のベクトルに w_2 、 w_3 、 w^*_2 、 w^*_3 と同様のはたらきをさせればよい。

すなわち、 c_i 、 c^*_i 、 d_i 、 d^*_i を計算する際、増えた分のベクトルに乱数係数をかけて、 w_2 、 w_3 、 w^*_2 、 w^*_3 に加え合わせればよい。

このようにすれば、より解読が困難な暗号文を作成することができ、安全性を向上させることができる。

[0129] また、本実施の形態では安全性向上のため、認証時にステップS709にて $\{u_2, u_3, u^{\wedge}_2, u^{\wedge}_3\}$ を選び、ステップS712およびステップS713にて使用する構成としていたが、これを省略することもできる。

そうすれば、認証の手順が省けるので、計算量を低減させることができる。

[0130] 実施の形態2.

以上の実施の形態1では、特徴点の一致数を評価指標として生体認証を行うという認証方法を開示したが、次に、特徴ベクトルのハミング距離またはユークリッド二乗距離により生体認証を行うという認証方法を述べる。

なお、本実施の形態に係る生体認証システムの構成例も図1に示した通りである。

また、本実施の形態に係る証明装置101、認証装置102、復号装置103の内部構成例も、図2～図4に示した通りである。

[0131] 本実施の形態では、実施の形態1と同様にT個の配列を用意し、それによって特徴ベクトルを構成するが、このとき類似度の指標として2つの特徴ベクトルのハミング距離またはユークリッド二乗距離を用いる。2つの特徴ベクトルを $b = (b_1, b_2, \dots, b_T)$ 、 $b' = (b'_1, b'_2, \dots, b'_T)$ とする。

このとき、2つの特徴ベクトルのハミング距離は、数15で与えられ（ただし $b_i, b'_i \in \{0, 1\}$ ）、また、2つの特徴ベクトルのユークリッド二乗距離は、数16で与えられる。

[0132] [数15]

$$d_H(b, b') = \sum_{i=1}^T (b_i \oplus b'_i) = \sum_{i=1}^T (b_i - b'_i)^2$$

[0133]

[数16]

$$d_{E2}(b, b') = \sum_{i=1}^T (b_i - b'_i)^2$$

[0134] 本実施の形態におけるパラメータ生成方法は、実施の形態1の図5と同様であるので説明を省略する。

[0135] 次に、図10を用いて、生体情報の登録方法を説明する。

[0136] なお、ここではユーザが証明装置101を経由して認証装置102に生体情報を登録する場合について説明するが、認証装置102上で直接生体情報を登録する場合や、登録用の専用装置を経由して登録する場合などにおいても同様の手順により実現できる。

[0137] 図10は、証明装置101において生体情報を登録する手順を示したフローチャートである。

[0138] ステップS1001とステップS1002は実施の形態1と同様である。

ただし、ここでハミング距離の場合は $b_i \in \{0, 1\}$ であり、ユークリッド二乗距離の場合は、 $b_i \in \{0, 1, \dots, q-1\}$ であることに注意する。

[0139] 次に、ステップS1003にて、乱数生成部203が、0から $q-1$ までの整数から一様ランダムに値を $4T$ 回取り出し、 $\{r_{2,i}, r_{3,i}, r_{2,i}^{\wedge}, r_{3,i}^{\wedge}\}_{i=1, 2, \dots, T}$ とする。

[0140] 次に、ステップS1004にて、暗号化部204が、 $c_i = b_i w_1 + r_{2,i} w_2 + r_{3,i} w_3$, $c_i^{\wedge} = b_i w_1^{\wedge} + r_{2,i}^{\wedge} w_2^{\wedge} + r_{3,i}^{\wedge} w_3^{\wedge}$ により暗号化特徴ベクトル $C = (c_1, c_2, \dots, c_T)$, 暗号化特徴ベクトル $C^{\wedge} = (c_1^{\wedge}, c_2^{\wedge}, \dots, c_T^{\wedge})$ を計算する。

なお、 w_1, w_2, w_3 と $w_1^{\wedge}, w_2^{\wedge}, w_3^{\wedge}$ は、公開鍵の一部(W 及び $W^{\wedge}$)として、復号装置103から配布されたものである。

[0141] 次に、ステップS1005にて、通信部206が、暗号化特徴ベクトル $C = (c_1, c_2, \dots, c_T)$, 暗号化特徴ベクトル $C^{\wedge} = (c_1^{\wedge}, c_2^{\wedge}, \dots, c_T^{\wedge})$ を認証装置102に送信する。

その際、例えばSSLなどの通信用改ざん検出技術を用いて通信の途中で改ざんが行われないようにすることが望ましい。

[0142] 最後に、ステップS1006にて、認証装置102が、暗号化特徴ベクトル $C = (c_1, c_2, \dots, c_T)$ 、暗号化特徴ベクトル $C^{\wedge} = (c^{\wedge}_1, c^{\wedge}_2, \dots, c^{\wedge}_T)$ を記憶部301に格納する。

[0143] 次に、図11、図12、図13を用いて、認証方法を説明する。

なお、簡単のためここでは認証時に認証の対象となるユーザが別途ID情報などによって特定されているいわゆる1:1認証の場合について説明する。

[0144] ステップS1101とステップS1102は実施の形態1と同様である。

ただし、ここでハミング距離の場合は $b'_i \in \{0, 1\}$ であり、ユークリッド二乗距離の場合は $b'_i \in \{0, 1, \dots, q-1\}$ であることに注意する。

[0145] 次に、ステップS1103にて、証明装置101の乱数生成部203が、0から $q-1$ までの整数から一様ランダムに値を $4T$ 回取り出し、 $\{r'_{2,i}, r'_{3,i}, r^{\wedge'}_{2,i}, r^{\wedge'}_{3,i}\}_{i=1,2,\dots,T}$ とする。

[0146] 次に、ステップS1104にて、証明装置101の暗号化部204が、 $c'_i = b'_i w_1 + r'_{2,i} w_2 + r'_{3,i} w_3$ 、 $c^{\wedge'}_i = b'_i w^{\wedge}_1 + r'_{2,i} w^{\wedge}_2 + r'_{3,i} w^{\wedge}_3$ により暗号化特徴ベクトル $C' = (c'_1, c'_2, \dots, c'_T)$ 、暗号化特徴ベクトル $C^{\wedge'} = (c^{\wedge'}_1, c^{\wedge'}_2, \dots, c^{\wedge'}_T)$ を計算する。

[0147] 次に、ステップS1105にて、証明装置101の通信部206が、暗号化特徴ベクトル $C' = (c'_1, c'_2, \dots, c'_T)$ 、暗号化特徴ベクトル $C^{\wedge'} = (c^{\wedge'}_1, c^{\wedge'}_2, \dots, c^{\wedge'}_T)$ を認証装置102に送信する。

その際、例えばSSLなどの通信用改ざん検出技術を用いて通信の途中で改ざんが行われないようにすることが望ましい。

[0148] 次に、ステップS1106にて、認証装置102の通信部206が、暗号化特徴ベクトル $C' = (c'_1, c'_2, \dots, c'_T)$ 、暗号化特徴ベクトル C

$\hat{c}' = (c'^1_1, c'^1_2, \dots, c'^1_T)$ を受信する。

- [0149] 次に、ステップS 1 1 0 7にて、認証装置 1 0 2の暗号化類似度生成部 3 0 2が、記憶部 3 0 1から暗号化特徴ベクトル $C = (c_1, c_2, \dots, c_T)$ 、暗号化特徴ベクトル $\hat{C} = (c^1_1, c^1_2, \dots, c^1_T)$ を取り出す。

このとき、一般に記憶部 3 0 1には多数のユーザの暗号化生体情報が格納されているが、その中からどれを取り出すかについては、別途与えられる ID 情報を用いる。

- [0150] 次に、ステップS 1 1 0 8にて、認証装置 1 0 2の乱数生成部 2 0 3が、0 から $q - 1$ までの整数から一様ランダムに値を $6 T$ 回取り出し、 $\{s_{1,i}, s_{2,i}, s_{3,i}, s^1_{1,i}, s^1_{2,i}, s^1_{3,i}\}_{i=1, 2, \dots, T}$ とする。

- [0151] 次に、ステップS 1 1 0 9にて、認証装置 1 0 2の乱数生成部 2 0 3が、0 から $q - 1$ までの整数から一様ランダムに値を 4 回取り出し、 $\{u_2, u_3, u^1_2, u^1_3\}$ とする。

- [0152] 次に、ステップS 1 1 1 0にて、認証装置 1 0 2の暗号化類似度生成部 3 0 2が、 $d_i = (c_i - c'^1_i) + s_{1,i}w_1 + s_{2,i}w_2 + s_{3,i}w_3$ を計算する。

なお、 w_1, w_2, w_3 は、公開鍵の一部 (W) として、復号装置 1 0 3 から配布されたものである。

- [0153] 次に、ステップS 1 1 1 1にて、認証装置 1 0 2の暗号化類似度生成部 3 0 2が、 $\hat{d}_i = (\hat{c}_i - \hat{c}'^1_i) + \hat{s}^1_{1,i}\hat{w}^1_1 + \hat{s}^1_{2,i}\hat{w}^1_2 + \hat{s}^1_{3,i}\hat{w}^1_3$ を計算する。

なお、 $\hat{w}^1_1, \hat{w}^1_2, \hat{w}^1_3$ は、公開鍵の一部 ($\hat{W}$) として、復号装置 1 0 3 から配布されたものである。

- [0154] 次に、ステップS 1 1 1 2にて、認証装置 1 0 2の暗号化類似度生成部 3 0 2が、数 1 7 に従って、 E を計算する。

- [0155]

[数17]

$$E = \sum_{i=1}^T (\hat{s}_{1,i}(\mathbf{c}_i - \mathbf{c}'_i) + s_{1,i}\hat{s}_{1,i}\mathbf{w}_1) + u_2\mathbf{w}_2 + u_3\mathbf{w}_3$$

[0156] 次に、ステップS 1 1 1 3にて、認証装置 1 0 2の暗号化類似度生成部 3 0 2が、数 1 8に従って、 $E^{\wedge}$ を計算する。

[0157] [数18]

$$\hat{E} = \sum_{i=1}^T s_{1,i}(\hat{\mathbf{c}}_i - \hat{\mathbf{c}}'_i) + \hat{u}_2\hat{\mathbf{w}}_2 + \hat{u}_3\hat{\mathbf{w}}_3$$

[0158] 次に、ステップS 1 1 1 4にて、認証装置 1 0 2の通信部 2 0 6が($d_1, \dots, d_T, d^{\wedge}_1, \dots, d^{\wedge}_T, \dots, E, E^{\wedge}$)を復号装置 1 0 3へ送信する。

その際、例えばSSLなどの通信用改ざん検出技術を用いて通信の途中で改ざんが行われないようにすることが望ましい。

本実施の形態では、($d_1, \dots, d_T, d^{\wedge}_1, \dots, d^{\wedge}_T, \dots, E, E^{\wedge}$)が暗号化類似度情報の例となる。

[0159] これ以降のステップは実施の形態 1と同様であるので説明を省略する。

[0160] 以上の実施の形態によれば、実施の形態 1と同様の効果を奏するのに加えて、類似度の指標としてハミング距離またはユークリッド二乗距離を用いることができるという効果がある。

[0161] 実施の形態 3.

以上、実施の形態 1および実施の形態 2にて、岡本－高島暗号を用いて生体認証を行う方法を開示したが、次に、非特許文献 2に示されたBGN(Boneh－Goh－Nissim)暗号を用いて生体認証を行う方法を開示する。

なお、本実施の形態に係る生体認証システムの構成例も図 1に示した通りである。

また、本実施の形態に係る証明装置 101、認証装置 102、復号装置 103 の内部構成例も、図 2－図 4 に示した通りである。

[0162] はじめに、BGN 暗号のアルゴリズムについて説明する。

BGN 暗号は、鍵生成、暗号化、復号の 3 つのアルゴリズムからなる。

[0163] 鍵生成アルゴリズムは以下のとおりである。

p 、 q をそれぞれ素数とする。

$N = pq$ として、 N を位数とする群 G 、 G_T を生成する。

$e : G \times G \rightarrow G_T$ を、双線型性および非退化性を満たすペアリングとする。

g 、 u を G から一様ランダムに選んだ要素とする。

$h = u^q$ により h を定める。

そして、公開鍵を $((G, G_T, N, e), g, h)$ 、秘密鍵を p とする。

[0164] 暗号化アルゴリズムは以下のとおりである。

なお、平文空間を $\{0, 1, \dots, L\}$ とする。 $\{0, 1, \dots, N-1\}$ から一様ランダムに r を選ぶ。

x に対する暗号文 $E(x)$ を $E(x) = g^x h^r$ とする。

[0165] 復号アルゴリズムは以下のとおりである。

暗号文を $E(x)$ とすると、まず、秘密鍵 p を用いて $E(x)^p$ を計算する。

定義より、 $E(x)^p = (g^x h^r)^p = (g^p)^x$ となる。

そして、この値について、 g^p を底とする離散対数を求め、元の平文 x を得る。

[0166] なお、離散対数を求める計算は現在の計算機能力では困難とされているが、平文空間の大きさ L が小さい場合には、Pollard のラムダ法を用いることにより $\sqrt{L}$ 程度の計算量で計算できることが知られている。

[0167] このような BGN 暗号を用いて、生体認証を行う方法を述べる。

本実施の形態では、実施の形態 1 と同様の特徴ベクトル構成法をとる場合について説明する。

すなわち、生体認証で用いる特徴ベクトルとして、特徴点の配列を用意し

、ユーザがその特徴点を保有する場合に1、特徴点を保有しない場合に0を配列に格納して、配列を特徴ベクトルとし、認証時には1が一致している箇所の数を類似度の指標とするような認証方式を例に説明する。

[0168] まず、図13を用いてセットアップについて説明する。

図13は、パラメータ生成部401における公開鍵及び秘密鍵の生成手順を示したフローチャートである。

[0169] はじめに、ステップS1301にて、パラメータ生成部401が、素数 p 、 q 、群 G 、 G_T を定める。

なお、素数はセキュリティレベルに応じて定まるが、素数 p と q の積を群位数とするため、通常は素因数分解ができないように素数を1024ビットや2048ビットなどの大きなサイズの素数とする。

[0170] 次に、ステップS1302にて、パラメータ生成部401が、 G から一様ランダムに g 、 u を選び、 $h = u^q$ を計算する。

[0171] 最後に、ステップS1303にて、パラメータ生成部401が、公開鍵 $p_k = ((G, G_T, N, e), g, h)$ を公開し、秘密鍵 $s_k = p$ を記憶部403に格納する。

[0172] 次に、図14を用いて、生体情報の登録方法を説明する。

なお、ここではユーザが証明装置101を経由して認証装置102に生体情報を登録する場合について説明するが、認証装置102上で直接生体情報を登録する場合や、登録用の専用装置を経由して登録する場合などにおいても同様の手順により実現できる。

[0173] 図14は、証明装置101において生体情報を登録する手順を示したフローチャートである。

[0174] はじめに、ステップS1401にて、生体情報抽出部201がユーザの生体情報を抽出する。これには様々な方法があるが、例えば指紋に光を当てて紋様をセンサで読み取るといったことにより抽出する。

[0175] 次に、ステップS1402にて、特徴ベクトル形成部202が、生体情報から特徴ベクトル $b = (b_1, b_2, \dots, b_T)$ を形成する。

[0176] 次に、ステップS 1 4 0 3にて、乱数生成部2 0 3が、0から $N-1$ までの整数から一様ランダムに値を T 回取り出し、 $\{r_i\}_{i=1, 2, \dots, T}$ とする。

[0177] 次に、ステップS 1 4 0 4にて、暗号化部2 0 4が、 $c_i = g^{b_i} h^{r_i}$ により暗号化特徴ベクトル $C = (c_1, c_2, \dots, c_T)$ を計算する。

なお、 g 、 h は公開鍵の一部として復号装置1 0 3から配布されたものである。

[0178] 次に、ステップS 1 4 0 5にて、通信部2 0 6が、暗号化特徴ベクトル $C = (c_1, c_2, \dots, c_T)$ を認証装置1 0 2に送信する。

[0179] 最後に、ステップS 1 4 0 6にて、認証装置1 0 2が、暗号化特徴ベクトル $C = (c_1, c_2, \dots, c_T)$ を記憶部3 0 1に格納する。

[0180] 次に、図1 5ないし図1 7を用いて、認証方法を説明する。

なお、簡単のためここでは認証時に認証の対象となるユーザが別途ID情報などによって特定されているいわゆる1 : 1認証の場合について説明する。

[0181] 図1 5、図1 6、図1 7は、認証を行う手順を示したフローチャートである。

[0182] はじめに、ステップS 1 5 0 1にて、証明装置1 0 1の生体情報抽出部2 0 1が、ユーザの生体情報を抽出する。

抽出方法は生体情報の登録時と同様である。

[0183] 次に、ステップS 1 5 0 2にて、証明装置1 0 1の特徴ベクトル形成部2 0 2が、生体情報から特徴ベクトル $b' = (b'_1, b'_2, \dots, b'_T)$ を形成する。

形成方法は、生体情報の登録時と同様である。

[0184] 次に、ステップS 1 5 0 3にて、証明装置1 0 1の乱数生成部2 0 3が、0から $N-1$ までの整数から一様ランダムに値を T 回取り出し、 $\{r'_i\}_{i=1, 2, \dots, T}$ とする。

[0185] 次に、ステップS 1 5 0 4にて、証明装置1 0 1の暗号化部2 0 4が、 $c'_i = g^{b'_i} h^{r'_i}$ により暗号化特徴ベクトル $C' = (c'_1, c'_2, \dots, c'_T)$

'_T) を計算する。

[0186] 次に、ステップS 1 5 0 5にて、証明装置 1 0 1の通信部 2 0 6が、暗号化特徴ベクトル $C' = (c'_1, c'_2, \dots, c'_T)$ を認証装置 1 0 2に送信する。

その際、例えばSSLなどの通信用改ざん検出技術を用いて通信の途中で改ざんが行われないようにすることが望ましい。

[0187] 次に、ステップS 1 5 0 6にて、認証装置 1 0 2の通信部 2 0 6が、暗号化特徴ベクトル $C' = (c'_1, c'_2, \dots, c'_T)$ を受信する。

[0188] 次に、ステップS 1 5 0 7にて、認証装置 1 0 2の暗号化類似度生成部 3 0 2が、記憶部 3 0 1から暗号化特徴ベクトル $C = (c_1, c_2, \dots, c_T)$ を取り出す。

[0189] 次に、ステップS 1 5 0 8にて、認証装置 1 0 2の乱数生成部 3 0 5が、0からN-1までの整数から一様ランダムに値を取り出し、sとする。

[0190] 次に、ステップS 1 5 0 9にて、認証装置 1 0 2の暗号化類似度生成部 3 0 2が、数19に従って、Eを計算する。

[0191] [数19]

$$E = \prod_{i=1}^T e(c_i, c'_i) \cdot e(g, h)^s$$

[0192] 次に、ステップS 1 5 1 0にて、認証装置 1 0 2の通信部 3 0 4が、Eを復号装置 1 0 3へ送信する。

その際、例えばSSLなどの通信用改ざん検出技術を用いて通信の途中で改ざんが行われないようにすることが望ましい。

本実施の形態では、Eが暗号化類似度情報となる。

[0193] 次に、ステップS 1 5 1 1にて、復号装置 1 0 3の通信部 4 0 4が、Eを受信する。

[0194] 次に、ステップS 1 5 1 2にて、復号装置 1 0 3の復号部 4 0 2が、記憶

部 4 0 3 から秘密鍵 p を取り出す。

[0195] 次に、ステップ S 1 5 1 3 にて、復号装置 1 0 3 の復号部 4 0 2 が、 $Z = E^p$ を計算する。

次に、ステップ S 1 5 1 4 にて、復号装置 1 0 3 の復号部 4 0 2 が、 $e(g, g)^p$ を底とする Z の離散対数 d を計算する。

本実施の形態でも、この離散対数 d が類似度に相当する。

[0196] 次に、ステップ S 1 5 1 5 にて、復号装置 1 0 3 の通信部 4 0 4 が d を認証装置 1 0 2 へ送信する。その際、例えば SSL などの通信用改ざん検出技術を用いて通信の途中で改ざんが行われないようにすることが望ましい。

[0197] 次に、ステップ S 1 5 1 6 にて、認証装置 1 0 2 の通信部 3 0 4 が、類似度 d を受信する。

[0198] 次に、ステップ S 1 5 1 7 にて、判定部 3 0 3 が、類似度 d がしきい値以上かを判定する。

このしきい値は、利用する生体情報の種類や安全性要件などさまざまな要素を勘案してあらかじめシステムで決められた値である。

しきい値以上であれば、証明装置 1 0 1 から送られてきた暗号化生体情報は ID で指定された本人のものであると判断する。

一方、しきい値未満であれば、証明装置 1 0 1 から送られてきた暗号化生体情報は ID で指定された人物のものではなく、他人のものであると判断する。

[0199] 以上のステップにより、認証装置 1 0 2 は証明装置 1 0 1 との間で生体認証を行うことができる。

[0200] 以上の実施の形態によれば、実施の形態 1 と同様の効果を奏するのに加えて、実施の形態 1 に比べて公開鍵、秘密鍵の数を低減できるという効果がある。

[0201] また、実施の形態 1 に比べて復号装置 1 0 3 に送付する暗号文の数を低減できるという効果がある。

[0202] 実施の形態 4.

以上の実施の形態 3 では、特徴ベクトルの内積を計算し、その値により生体認証を行うという認証方法を開示したが、次に、特徴ベクトルのハミング距離またはユークリッド二乗距離により生体認証を行うという認証方法を述べる。

なお、本実施の形態に係る生体認証システムの構成例も図 1 に示した通りである。

また、本実施の形態に係る証明装置 101、認証装置 102、復号装置 103 の内部構成例も、図 2－図 4 に示した通りである。

[0203] 本実施の形態におけるパラメータ生成方法と生体情報の登録方法は実施の形態 3 と同様であるので説明を省略する。

[0204] 次に、図 18、図 19、図 20 を用いて、認証方法を説明する。

なお、簡単のためここでは認証時に認証の対象となるユーザが別途 ID 情報などによって特定されているいわゆる 1 : 1 認証の場合について説明する。

[0205] ステップ S 1801 から S 1808 までは実施の形態 3 と同様であるので説明を省略する。

[0206] ステップ S 1809 にて、認証装置 102 の暗号化類似度生成部 302 が、数 20 に従って、E を計算する。

[0207] [数 20]

$$E = \prod_{i=1}^T e(c_i, g) \cdot e(c'_i, g) \cdot e(c_i, c'_i)^{-2} \cdot e(g, h)^s$$

[0208] これ以降のステップは実施の形態 3 と同様であるので説明を省略する。

[0209] 以上の実施の形態によれば、実施の形態 2 と同様の効果を奏する上に、実施の形態 3 と同様の効果を奏する。

[0210] 以上、実施の形態 1 から実施の形態 4 にわたって、二重準同型暗号を用いた生体認証方法を開示したが、これは生体認証に限らず、パターンマッチング分野に応用できることは明らかである。

すなわち、実施の形態 1－4 に示した認証方法によれば、データを暗号化したままでデータの類似度判定ができる。

したがって、データを暗号化したままでの画像検索、動画検索、音声検索などが可能となる。

[0211] 以上の実施の形態 1－4 では、生体認証と二重準同型暗号とを用いることで、生体情報を暗号化したままで生体認証を実現したことを説明した。

つまり、従来は、通常の準同型暗号を使っていたので、すべてを暗号化したままで認証処理を行うことができなかった。そのため認証処理においてユーザと認証装置との間の通信量が大きくなってしまうという課題がある。

二重準同型暗号を用いることで、すべてを暗号化したままで認証処理を行うことができるようになる。そのためユーザと認証装置との間の通信量を低減させることができるという効果が生まれる。

また、この生体認証と二重準同型暗号との組合せにより、安全でかつ通信量効率の高い生体認証が実現できるという効果が生まれる。

[0212] 最後に、実施の形態 1－4 に示した証明装置 101、認証装置 102、復号装置 103 のハードウェア構成例について説明する。

図 25 は、実施の形態 1－4 に示す証明装置 101、認証装置 102、復号装置 103 のハードウェア資源の一例を示す図である。

なお、図 25 の構成は、あくまでも証明装置 101、認証装置 102、復号装置 103 のハードウェア構成の一例を示すものであり、証明装置 101、認証装置 102、復号装置 103 のハードウェア構成は図 25 に記載の構成に限らず、他の構成であってもよい。

[0213] 図 25 において、証明装置 101、認証装置 102、復号装置 103 は、プログラムを実行する CPU 911 (Central Processing Unit、中央処理装置、処理装置、演算装置、マイクロプロセッサ、マイクロコンピュータ、プロセッサともいう) を備えている。

CPU 911 は、バス 912 を介して、例えば、ROM (Read Only Memory) 913、RAM (Random Access Me

memory) 914、通信ボード915、表示装置901、キーボード902、マウス903、磁気ディスク装置920と接続され、これらのハードウェアデバイスを制御する。

更に、CPU911は、FDD904 (Flexible Disk Drive)、コンパクトディスク装置905 (CDD)、プリンタ装置906と接続していてもよい。また、証明装置101は、生体情報を読み取るための読取り装置907と接続されている。また、磁気ディスク装置920の代わりに、光ディスク装置、メモリカード (登録商標) 読み書き装置などの記憶装置でもよい。

RAM914は、揮発性メモリの一例である。ROM913、FDD904、CDD905、磁気ディスク装置920の記憶媒体は、不揮発性メモリの一例である。これらは、記憶装置の一例である。

実施の形態1-4で説明した「記憶部」は、RAM914、磁気ディスク装置920等により実現される。

通信ボード915、キーボード902、マウス903、読取り装置907、FDD904などは、入力装置の一例である。

また、通信ボード915、表示装置901、プリンタ装置906などは、出力装置の一例である。

[0214] 通信ボード915は、他の装置と接続されている以外に、例えば、LAN (ローカルエリアネットワーク)、インターネット、WAN (ワイドエリアネットワーク)、SAN (ストレージエリアネットワーク) などに接続されていても構わない。

[0215] 磁気ディスク装置920には、オペレーティングシステム921 (OS)、ウィンドウシステム922、プログラム群923、ファイル群924が記憶されている。

プログラム群923のプログラムは、CPU911がオペレーティングシステム921、ウィンドウシステム922を利用しながら実行する。

[0216] また、RAM914には、CPU911に実行させるオペレーティングシ

ステム 9 2 1 のプログラムやアプリケーションプログラムの少なくとも一部が一時的に格納される。

また、RAM 9 1 4 には、CPU 9 1 1 による処理に必要な各種データが格納される。

[0217] また、ROM 9 1 3 には、BIOS (Basic Input Output System) プログラムが格納され、磁気ディスク装置 9 2 0 にはブートプログラムが格納されている。

証明装置 1 0 1、認証装置 1 0 2、復号装置 1 0 3 の起動時には、ROM 9 1 3 の BIOS プログラム及び磁気ディスク装置 9 2 0 のブートプログラムが実行され、BIOS プログラム及びブートプログラムによりオペレーティングシステム 9 2 1 が起動される。

[0218] 上記プログラム群 9 2 3 には、実施の形態 1 - 4 の説明において「～部」（「記憶部」以外、以下も同様）として説明している機能を実行するプログラムが記憶されている。プログラムは、CPU 9 1 1 により読み出され実行される。

[0219] ファイル群 9 2 4 には、実施の形態 1 - 4 の説明において、「～の判断」、「～の判定」、「～の計算」、「～の比較」、「～の導出」、「～の抽出」、「～の形成」、「～の更新」、「～の設定」、「～の登録」、「～の選択」等として説明している処理の結果を示す情報やデータや信号値や変数値やパラメータが、「～ファイル」や「～データベース」の各項目として記憶されている。

「～ファイル」や「～データベース」は、ディスクやメモリなどの記録媒体に記憶される。ディスクやメモリなどの記憶媒体に記憶された情報やデータや信号値や変数値やパラメータは、読み書き回路を介して CPU 9 1 1 によりメインメモリやキャッシュメモリに読み出され、抽出・検索・参照・比較・演算・計算・処理・編集・出力・印刷・表示などの CPU の動作に用いられる。

抽出・検索・参照・比較・演算・計算・処理・編集・出力・印刷・表示の

CPUの動作の間、情報やデータや信号値や変数値やパラメータは、メインメモリ、レジスタ、キャッシュメモリ、バッファメモリ等に一時的に記憶される。

また、実施の形態１－４で説明しているフローチャートの矢印の部分は主としてデータや信号の入出力を示し、データや信号値は、RAM 914のメモリ、FDD 904のフレキシブルディスク、CDD 905のコンパクトディスク、磁気ディスク装置 920の磁気ディスク、その他光ディスク、ミニディスク、DVD等の記録媒体に記録される。また、データや信号は、バス 912や信号線やケーブルその他の伝送媒体によりオンライン伝送される。

[0220] また、実施の形態１－４の説明において「～部」として説明しているものは、「～回路」、「～装置」、「～機器」であってもよく、また、「～ステップ」、「～手順」、「～処理」であってもよい。すなわち、「～部」として説明しているものは、ROM 913に記憶されたファームウェアで実現されていても構わない。或いは、ソフトウェアのみ、或いは、素子・デバイス・基板・配線などのハードウェアのみ、或いは、ソフトウェアとハードウェアとの組み合わせ、さらには、ファームウェアとの組み合わせで実施されても構わない。ファームウェアとソフトウェアは、プログラムとして、磁気ディスク、フレキシブルディスク、光ディスク、コンパクトディスク、ミニディスク、DVD等の記録媒体に記憶される。プログラムはCPU 911により読み出され、CPU 911により実行される。すなわち、プログラムは、実施の形態１－４の「～部」としてコンピュータを機能させるものである。あるいは、実施の形態１－４の「～部」の手順や方法をコンピュータに実行させるものである。

[0221] このように、実施の形態１－４に示す証明装置 101、認証装置 102、復号装置 103は、処理装置たるCPU、記憶装置たるメモリ、磁気ディスク等、入力装置たるキーボード、マウス、通信ボード等、出力装置たる表示装置、通信ボード等を備えるコンピュータであり、上記したように「～部」として示された機能をこれら処理装置、記憶装置、入力装置、出力装置を用

いて実現するものである。

符号の説明

[0222] 101 証明装置、102 認証装置、103 復号装置、201 生体
情報抽出部、202 特徴ベクトル形成部、203 乱数生成部、204
暗号化部、205 記憶部、206 通信部、301 記憶部、302 暗
号化類似度生成部、303 判定部、304 通信部、305 乱数生成部
、401 パラメータ生成部、402 復号部、403 記憶部、404
通信部。

請求の範囲

[請求項1]

二重準同型暗号アルゴリズムに基づいて復号装置において生成され、前記復号装置から配布された公開鍵を記憶する公開鍵記憶部と、

前記復号装置から配布された前記公開鍵を保有する暗号装置が保有する前記公開鍵を用いて暗号化した第1データを暗号化第1データとして記憶する暗号化データ記憶部と、

前記暗号化第1データが前記暗号化データ記憶部に記憶された後に前記暗号装置が保有する前記公開鍵を用いて暗号化した第2データを暗号化第2データとして入力する暗号化データ入力部と、

前記公開鍵の少なくとも一部を用いて、乱数を生成する乱数生成部と、

前記暗号化第1データと前記暗号化第2データに対して前記公開鍵記憶部に記憶されている前記公開鍵と前記乱数生成部により生成された乱数を用いた演算を行って、前記暗号化第1データと前記暗号化第2データがそれぞれ暗号化された状態のままで、前記公開鍵に対応付けられて生成された秘密鍵を用いた復号処理により前記第1データと前記第2データとの間の類似度を導出可能な暗号化された情報を暗号化類似度情報として生成する暗号化類似度生成部とを有することを特徴とするデータ処理装置。

[請求項2]

前記公開鍵記憶部は、

前記復号装置により前記二重準同型暗号アルゴリズムに基づいて秘密鍵と対応付けられて生成された公開鍵を記憶し、

前記データ処理装置は、更に、

前記暗号化類似度生成部により生成された暗号化類似度情報を前記復号装置に出力する暗号化類似度出力部と、

前記復号装置において前記暗号化類似度情報に対して前記秘密鍵を用いた復号処理が行われて導出された前記第1データと前記第2データとの間の類似度を入力する類似度入力部と、

前記類似度入力部により入力された前記類似度を解析して、前記第2データの発生源が正当であるか否かを判定する判定部とを有することを特徴とする請求項1に記載のデータ処理装置。

[請求項3]

前記暗号化データ記憶部は、

前記第1データを構成する T (T は2以上の整数)個の部分データが前記暗号装置により暗号化されて得られた T 個の暗号化された部分データで構成される暗号化第1データを記憶し、

前記暗号化データ入力部は、

前記第2データを構成する T (T は2以上の整数)個の部分データが前記暗号装置により暗号化されて得られた T 個の暗号化された部分データで構成される暗号化第2データを入力し、

前記暗号化類似度生成部は、

部分データごとに、前記暗号化第1データと前記暗号化第2データに対して前記公開鍵記憶部に記憶されている前記公開鍵と前記乱数生成部により生成された乱数を用いた演算を行って、前記第1データと前記第2データとの間の類似度として、前記第1データの T 個の部分データと前記第2データの T 個の部分データにおいて値が一致する部分データの数を導出可能な情報を生成することを特徴とする請求項1に記載のデータ処理装置。

[請求項4]

前記暗号化データ記憶部は、

前記第1データを構成する T (T は2以上の整数)個の部分データが前記暗号装置により暗号化されて得られた T 個の暗号化された部分データで構成される暗号化第1データを記憶し、

前記暗号化データ入力部は、

前記第2データを構成する T (T は2以上の整数)個の部分データが前記暗号装置により暗号化されて得られた T 個の暗号化された部分データで構成される暗号化第2データを入力し、

前記暗号化類似度生成部は、

部分データごとに、前記暗号化第 1 データと前記暗号化第 2 データに対して前記公開鍵記憶部に記憶されている前記公開鍵と前記乱数生成部により生成された乱数を用いた演算を行って、前記第 1 データと前記第 2 データとの間の類似度として、前記第 1 データの T 個の部分データと前記第 2 データの T 個の部分データにおけるハミング距離を導出可能な情報を生成することを特徴とする請求項 1 に記載のデータ処理装置。

[請求項 5]

前記暗号化データ記憶部は、

前記第 1 データを構成する T (T は 2 以上の整数) 個の部分データが前記暗号装置により暗号化されて得られた T 個の暗号化された部分データで構成される暗号化第 1 データを記憶し、

前記暗号化データ入力部は、

前記第 2 データを構成する T (T は 2 以上の整数) 個の部分データが前記暗号装置により暗号化されて得られた T 個の暗号化された部分データで構成される暗号化第 2 データを入力し、

前記暗号化類似度生成部は、

部分データごとに、前記暗号化第 1 データと前記暗号化第 2 データに対して前記公開鍵記憶部に記憶されている前記公開鍵と前記乱数生成部により生成された乱数を用いた演算を行って、前記第 1 データと前記第 2 データとの間の類似度として、前記第 1 データの T 個の部分データと前記第 2 データの T 個の部分データにおけるユークリッド二乗距離を導出可能な情報を生成することを特徴とする請求項 1 に記載のデータ処理装置。

[請求項 6]

前記公開鍵記憶部は、

前記二重準同型暗号アルゴリズムに基づいて生成された公開鍵として、岡本－高島暗号アルゴリズムに基づいて生成された公開鍵を記憶し、

前記暗号化データ記憶部は、

前記岡本－高島暗号アルゴリズムに基づいて生成された公開鍵による暗号化で得られた暗号化第1データを記憶し、

前記暗号化データ入力部は、

前記岡本－高島暗号アルゴリズムに基づいて生成された公開鍵による暗号化で得られた暗号化第2データを入力することを特徴とする請求項1に記載のデータ処理装置。

[請求項7]

前記公開鍵記憶部は、

正則行列である秘密鍵に対応付けられて生成されたランダム基底 w_1 、 w_2 、 w_3 、 $w^{\wedge}_1$ 、 $w^{\wedge}_2$ 、 $w^{\wedge}_3$ と所定の値 q を公開鍵として記憶し、

前記暗号化データ記憶部は、

前記第1データを構成する T (T は2以上の整数)個の部分データ b_i (添字 i は1から T)に前記ランダム基底 w_1 、 w_2 、 w_3 を保有する前記暗号装置により前記ランダム基底 w_1 、 w_2 、 w_3 を用いた暗号化が行われて得られた T 個の暗号化された部分データ c_i (添字 i は1から T)で構成される暗号化第1データを記憶し、

前記暗号化データ入力部は、

前記第2データを構成する T (T は2以上の整数)個の部分データ b'_i (添字 i は1から T)に前記ランダム基底 $w^{\wedge}_1$ 、 $w^{\wedge}_2$ 、 $w^{\wedge}_3$ を保有する前記暗号装置により前記ランダム基底 $w^{\wedge}_1$ 、 $w^{\wedge}_2$ 、 $w^{\wedge}_3$ を用いた暗号化が行われて得られた T 個の暗号化された部分データ $c^{\wedge}_i$ (添字 i は1から T)で構成される暗号化第2データを入力し、

前記乱数生成部は、

前記値 q に基づいて複数の乱数値 $s_{1,i}$ 、 $s_{2,i}$ 、 $s_{3,i}$ 、 $s^{\wedge}_{1,i}$ 、 $s^{\wedge}_{2,i}$ 、 $s^{\wedge}_{3,i}$ (添字 i は1から T)を生成し、前記値 q に基づいて複数の乱数値 u_2 、 u_3 、 $u^{\wedge}_2$ 、 $u^{\wedge}_3$ を生成し、

前記暗号化類似度生成部は、

$$d_i = c_i + (s_{1,i} \times w_1) + (s_{2,i} \times w_2) + (s_{3,i} \times w_3)$$

を添字 i について 1 から T までを計算し、

$$d^{\wedge}_i = c^{\wedge}_i + (s^{\wedge}_{1,i} \times w^{\wedge}_1) + (s^{\wedge}_{2,i} \times w^{\wedge}_2) + (s^{\wedge}_{3,i} \times w^{\wedge}_3)$$

を添字 i について 1 から T までを計算し、

$$E = \{ (s^{\wedge}_{1,i} \times c_i + s_{1,i} \times s^{\wedge}_{1,i} \times w_1) \text{ の添字 } i \text{ についての } 1 \text{ から } T \text{ までの総和} \} + (u_2 \times w_2) + (u_3 \times w_3)$$

、

$$E^{\wedge} = \{ (s_{1,i} \times c^{\wedge}_i) \text{ の添字 } i \text{ についての } 1 \text{ から } T \text{ までの総和} \} + (u^{\wedge}_2 \times w^{\wedge}_2) + (u^{\wedge}_3 \times w^{\wedge}_3)$$

計算した値 d_i 、 $d^{\wedge}_i$ 、 E 及び $E^{\wedge}$ を含む暗号化類似度情報を生成することを特徴とする請求項 6 に記載のデータ処理装置。

[請求項 8]

前記暗号化データ記憶部は、

T 個の部分データ b_i が前記暗号装置で生成された乱数値 $r_{2,i}$ と $r_{3,i}$ (添字 i は 1 から T) と前記ランダム基底 w_1 、 w_2 、 w_3 が用いられて $c_i = (b_i \times w_1) + (r_{2,i} \times w_2) + (r_{3,i} \times w_3)$ により暗号化された T 個の部分データ c_i で構成される暗号化第 1 データを記憶し、

前記暗号化データ入力部は、

T 個の部分データ b'_i が前記暗号装置で生成された乱数値 $r'_{2,i}$ と $r'_{3,i}$ (添字 i は 1 から T) と前記ランダム基底 $w^{\wedge}_1$ 、 $w^{\wedge}_2$ 、 $w^{\wedge}_3$ が用いられて $c^{\wedge}_i = (b'_i \times w^{\wedge}_1) + (r'_{2,i} \times w^{\wedge}_2) + (r'_{3,i} \times w^{\wedge}_3)$ により暗号化された T 個の部分データ $c^{\wedge}_i$ で構成される暗号化第 2 データを入力することを特徴とする請求項 7 に記載のデータ処理装置。

[請求項 9]

前記データ処理装置は、更に、

前記暗号化類似度生成部により生成された暗号化類似度情報を前記復号装置に出力する暗号化類似度出力部と、

前記復号装置において前記暗号化類似度情報に対して前記秘密鍵の

逆行列と双対ペアリングベクトル空間におけるディストーション写像とが用いられる復号処理が行われて導出された前記第1データと前記第2データとの間の類似度を入力する類似度入力部と、

前記類似度入力部により入力された前記類似度を解析して、前記第2データの発生源が正当であるか否かを判定する判定部とを有することを特徴とする請求項7に記載のデータ処理装置。

[請求項10]

前記公開鍵記憶部は、

正則行列である秘密鍵に対応付けて生成されたランダム基底 w_1 、 w_2 、 w_3 、 $w^{\wedge}_1$ 、 $w^{\wedge}_2$ 、 $w^{\wedge}_3$ と所定の値 q を公開鍵として記憶し、

前記暗号化データ記憶部は、

前記第1データを構成する T (T は2以上の整数)個の部分データ b_i (添字 i は1から T)に前記ランダム基底 w_1 、 w_2 、 w_3 を保有する前記暗号装置により前記ランダム基底 w_1 、 w_2 、 w_3 を用いた暗号化が行われて得られた T 個の暗号化された部分データ c_i (添字 i は1から T)と、前記第1データを構成する T 個の部分データ b_i に前記ランダム基底 $w^{\wedge}_1$ 、 $w^{\wedge}_2$ 、 $w^{\wedge}_3$ を保有する前記暗号装置により前記ランダム基底 $w^{\wedge}_1$ 、 $w^{\wedge}_2$ 、 $w^{\wedge}_3$ を用いた暗号化が行われて得られた T 個の暗号化された部分データ $c^{\wedge}_i$ (添字 i は1から T)で構成される暗号化第1データを記憶し、

前記暗号化データ入力部は、

前記第2データを構成する T (T は2以上の整数)個の部分データ b'_i (添字 i は1から T)に前記暗号装置により前記ランダム基底 w_1 、 w_2 、 w_3 を用いた暗号化が行われて得られた T 個の暗号化された部分データ c'_i (添字 i は1から T)と、前記第2データを構成する T 個の部分データ b'_i に前記暗号装置により前記ランダム基底 $w^{\wedge}_1$ 、 $w^{\wedge}_2$ 、 $w^{\wedge}_3$ を用いた暗号化が行われて得られた T 個の暗号化された部分データ $c'^{\wedge}_i$ (添字 i は1から T)で構成される暗号

化第2データを入力し、

前記乱数生成部は、

前記値 q に基づいて複数の乱数値 $s_{1,i}$ 、 $s_{2,i}$ 、 $s_{3,i}$ 、 $s^{^1}_{1,i}$ 、 $s^{^2}_{2,i}$ 、 $s^{^3}_{3,i}$ (添字 i は1から T) を生成し、前記値 q に基づいて複数の乱数値 u_2 、 u_3 、 $u^{^2}_2$ 、 $u^{^3}_3$ を生成し、

前記暗号化類似度生成部は、

$d_i = (c_i - c'_i) + (s_{1,i} \times w_1) + (s_{2,i} \times w_2) + (s_{3,i} \times w_3)$ を添字 i について1から T までを計算し、

$d^{^1}_i = (c^{^1}_i - c'^{^1}_i) + (s^{^1}_{1,i} \times w^{^1}_1) + (s^{^2}_{2,i} \times w^{^2}_2) + (s^{^3}_{3,i} \times w^{^3}_3)$ を添字 i について1から T までを計算し、

$E = \{ (s^{^1}_{1,i} \times (c_i - c'_i) + s_{1,i} \times s^{^1}_{1,i} \times w_1) \}$ の添字 i についての1から T までの総和 $\} + (u_2 \times w_2) + (u_3 \times w_3)$ を計算し、

$E^{^1} = [\{ s_{1,i} \times (c^{^1}_i - c'^{^1}_i) \} \}$ の添字 i についての1から T までの総和 $] + (u^{^2}_2 \times w^{^2}_2) + (u^{^3}_3 \times w^{^3}_3)$ を計算し、

計算した値 d_i 、 $d^{^1}_i$ 、 E 及び $E^{^1}$ を含む暗号化類似度情報を生成することを特徴とする請求項6に記載のデータ処理装置。

[請求項11]

前記暗号化データ記憶部は、

T 個の部分データ b_i が前記暗号装置で生成された乱数値 $r_{2,i}$ と $r_{3,i}$ (添字 i は1から T) と前記ランダム基底 w_1 、 w_2 、 w_3 が用いられて $c_i = (b_i \times w_1) + (r_{2,i} \times w_2) + (r_{3,i} \times w_3)$ により暗号化された T 個の部分データ c_i と、 T 個の部分データ b_i が前記暗号装置で生成された乱数値 $r^{^2}_{2,i}$ と $r^{^3}_{3,i}$ (添字 i は1から T) と前記ランダム基底 $w^{^1}_1$ 、 $w^{^2}_2$ 、 $w^{^3}_3$ が用いられて $c^{^1}_i = (b_i \times w^{^1}_1) + (r^{^2}_{2,i} \times w^{^2}_2) + (r^{^3}_{3,i} \times w^{^3}_3)$ により暗号化された T 個の部分データ $c^{^1}_i$ で構成される暗号化第1デー

タを記憶し、

前記暗号化データ入力部は、

T 個の部分データ b'_i が前記暗号装置で生成された乱数値 $r'_{2,i}$ と $r'_{3,i}$ (添字 i は 1 から T) と前記ランダム基底 w_1, w_2, w_3 が用いられて $c'_i = (b'_i \times w_1) + (r'_{2,i} \times w_2) + (r'_{3,i} \times w_3)$ により暗号化された T 個の部分データ c'_i と、 T 個の部分データ b'_i が前記暗号装置で生成された乱数値 $r'^{\wedge}_{2,i}$ と $r'^{\wedge}_{3,i}$ (添字 i は 1 から T) と前記ランダム基底 $w^{\wedge}_1, w^{\wedge}_2, w^{\wedge}_3$ が用いられて $c'^{\wedge}_i = (b'_i \times w^{\wedge}_1) + (r'^{\wedge}_{2,i} \times w^{\wedge}_2) + (r'^{\wedge}_{3,i} \times w^{\wedge}_3)$ により暗号化された T 個の部分データ $c'^{\wedge}_i$ で構成される暗号化第 2 データを入力することを特徴とする請求項 10 に記載のデータ処理装置。

[請求項 12]

前記データ処理装置は、更に、

前記暗号化類似度生成部により生成された暗号化類似度情報を前記復号装置に出力する暗号化類似度出力部と、

前記復号装置において前記暗号化類似度情報に対して前記秘密鍵の逆行列と双対ペアリングベクトル空間におけるディストーション写像とが用いられる復号処理が行われて導出された前記第 1 データと前記第 2 データとの間の類似度を入力する類似度入力部と、

前記類似度入力部により入力された前記類似度を解析して、前記第 2 データの発生源が正当であるか否かを判定する判定部とを有することを特徴とする請求項 10 に記載のデータ処理装置。

[請求項 13]

前記公開鍵記憶部は、

前記二重準同型暗号アルゴリズムに基づいて生成された公開鍵として、BGN (Boneh-Goh-Nissim) 暗号アルゴリズムに基づいて生成された公開鍵を記憶し、

前記 BGN 暗号アルゴリズムに基づいて生成された公開鍵による暗号化で得られた暗号化第 1 データを記憶し、

前記暗号化データ入力部は、

前記BGN暗号アルゴリズムに基づいて生成された公開鍵による暗号化で得られた暗号化第2データを入力することを特徴とする請求項1に記載のデータ処理装置。

[請求項14]

前記公開鍵記憶部は、

$N = p \times q$ (p 及び q は素数) を位数とする群 G からランダムに選択された値 g と値 u と、値 $h = u^q$ と、所定の値 N を公開鍵として記憶し、

前記暗号化データ記憶部は、

前記第1データを構成する T (T は2以上の整数) 個の部分データ b_i (添字 i は1から T) に値 g と値 h を保有する前記暗号装置により値 g と値 h を用いた暗号化が行われて得られた T 個の暗号化された部分データ c_i (添字 i は1から T) で構成される暗号化第1データを記憶し、

前記暗号化データ入力部は、

前記第2データを構成する T (T は2以上の整数) 個の部分データ b'_i (添字 i は1から T) に前記暗号装置により値 g と値 h を用いた暗号化が行われて得られた T 個の暗号化された部分データ c'_i (添字 i は1から T) で構成される暗号化第2データを入力し、

前記乱数生成部は、

前記値 N に基づいて乱数値 s を生成し、

前記暗号化類似度生成部は、

$E = e(c_i, c'_i) \times e(g, h)^s$ の添字 i について1から T までの総乗を計算し ($e: G \times G \rightarrow G$ は双線型性と非退化性を満たすペアリング)、計算した値 E を含む暗号化類似度情報を生成することを特徴とする請求項13に記載のデータ処理装置。

[請求項15]

前記公開鍵記憶部は、

$N = p \times q$ (p 及び q は素数) を位数とする群 G からランダムに選

択された値 g と値 u と、値 $h = u^q$ と、所定の値 N を公開鍵として記憶し、

前記暗号化データ記憶部は、

前記第 1 データを構成する T (T は 2 以上の整数) 個の部分データ b_i (添字 i は 1 から T) に値 g と値 h を保有する前記暗号装置により値 g と値 h を用いた暗号化が行われて得られた部分データ c_i (添字 i は 1 から T) で構成される暗号化第 1 データを記憶し、

前記暗号化データ入力部は、

前記第 2 データを構成する T (T は 2 以上の整数) 個の部分データ b'_i (添字 i は 1 から T) に前記暗号装置により値 g と値 h を用いた暗号化が行われて得られた T 個の暗号化された部分データ c'_i (添字 i は 1 から T) で構成される暗号化第 2 データを入力し、

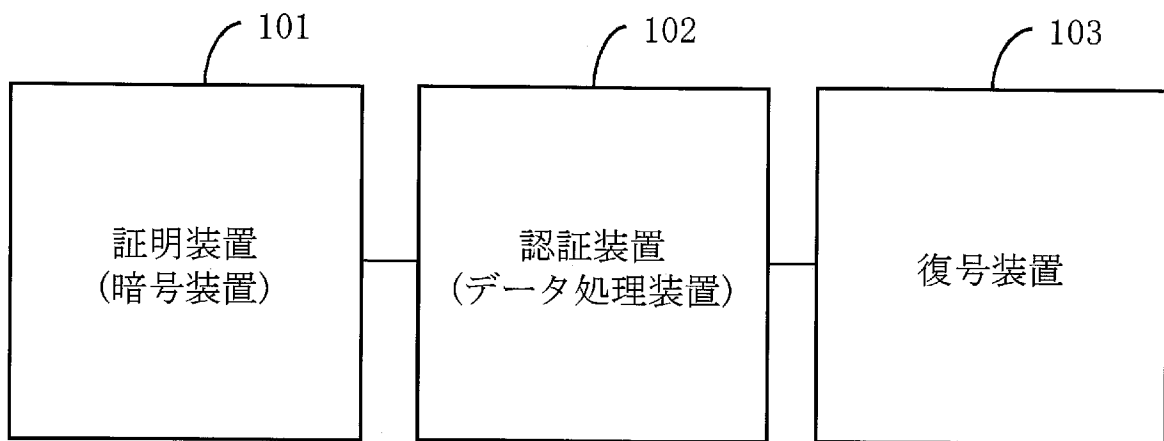
前記乱数生成部は、

前記値 N に基づいて乱数値 s を生成し、

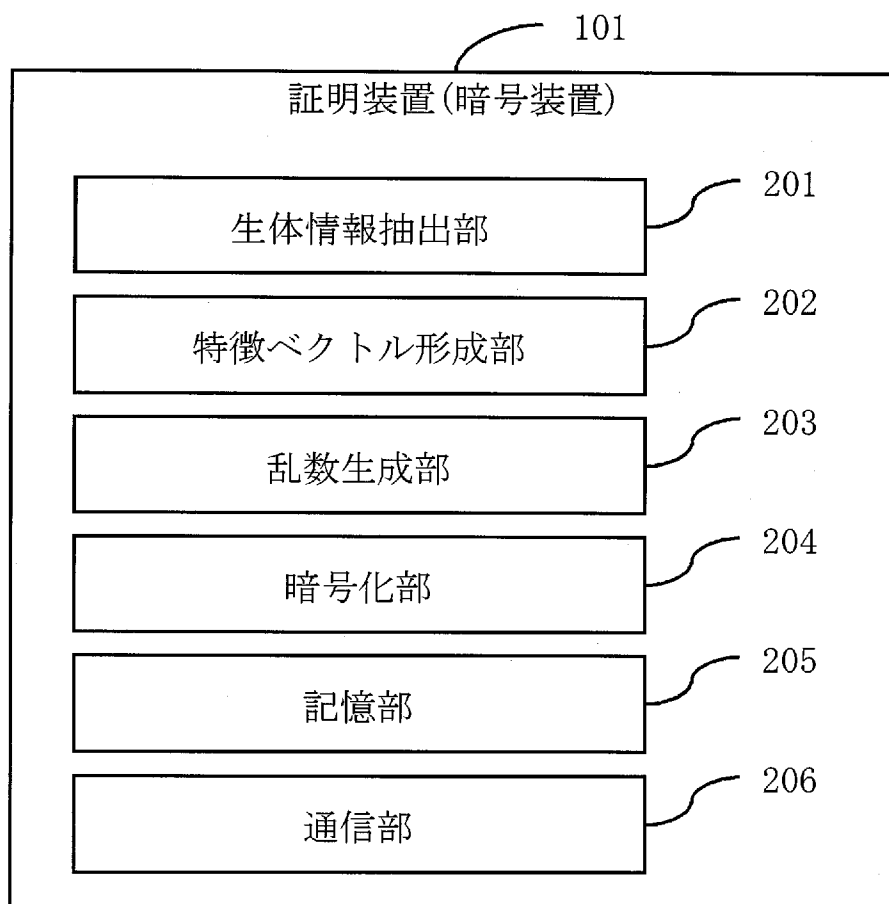
前記暗号化類似度生成部は、

$$E = e(c_i, g) \times e(c'_i, g) \times e(c_i \times c'_i)^{-2} \times e(g, h)^s$$
の添字 i について 1 から T までの総乗を計算し ($e: G \times G \rightarrow G$ は双線型性と非退化性を満たすペアリング)、計算した値 E を含む暗号化類似度情報を生成することを特徴とする請求項 13 に記載のデータ処理装置。

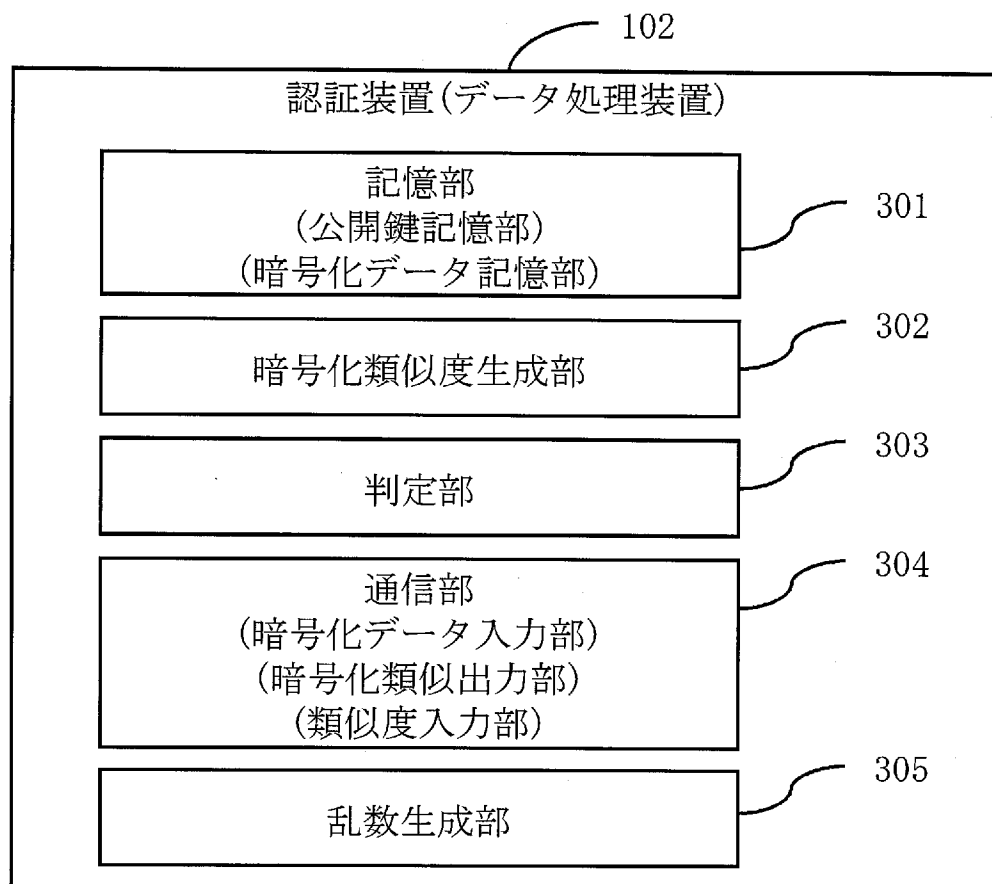
[図1]



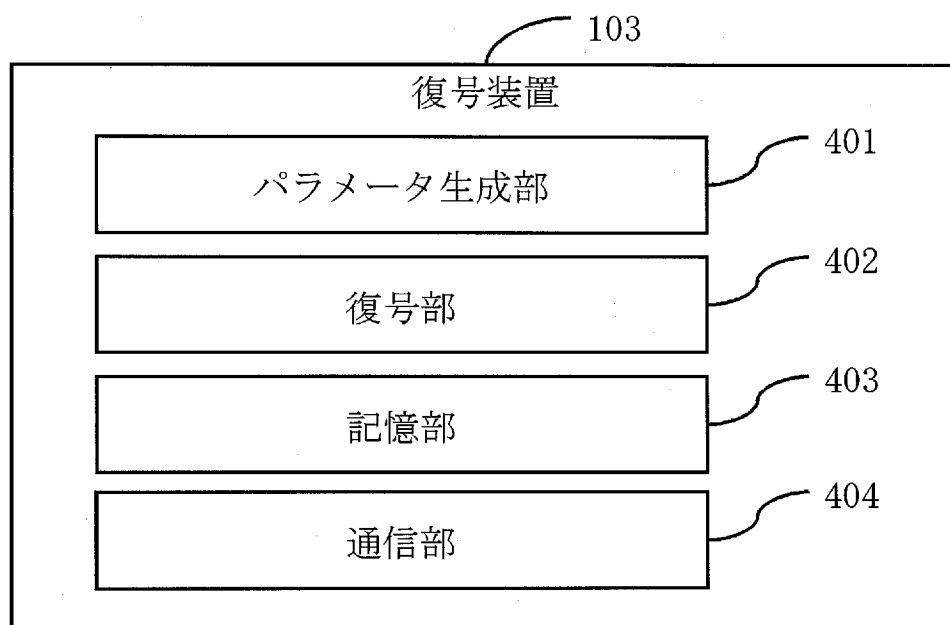
[図2]



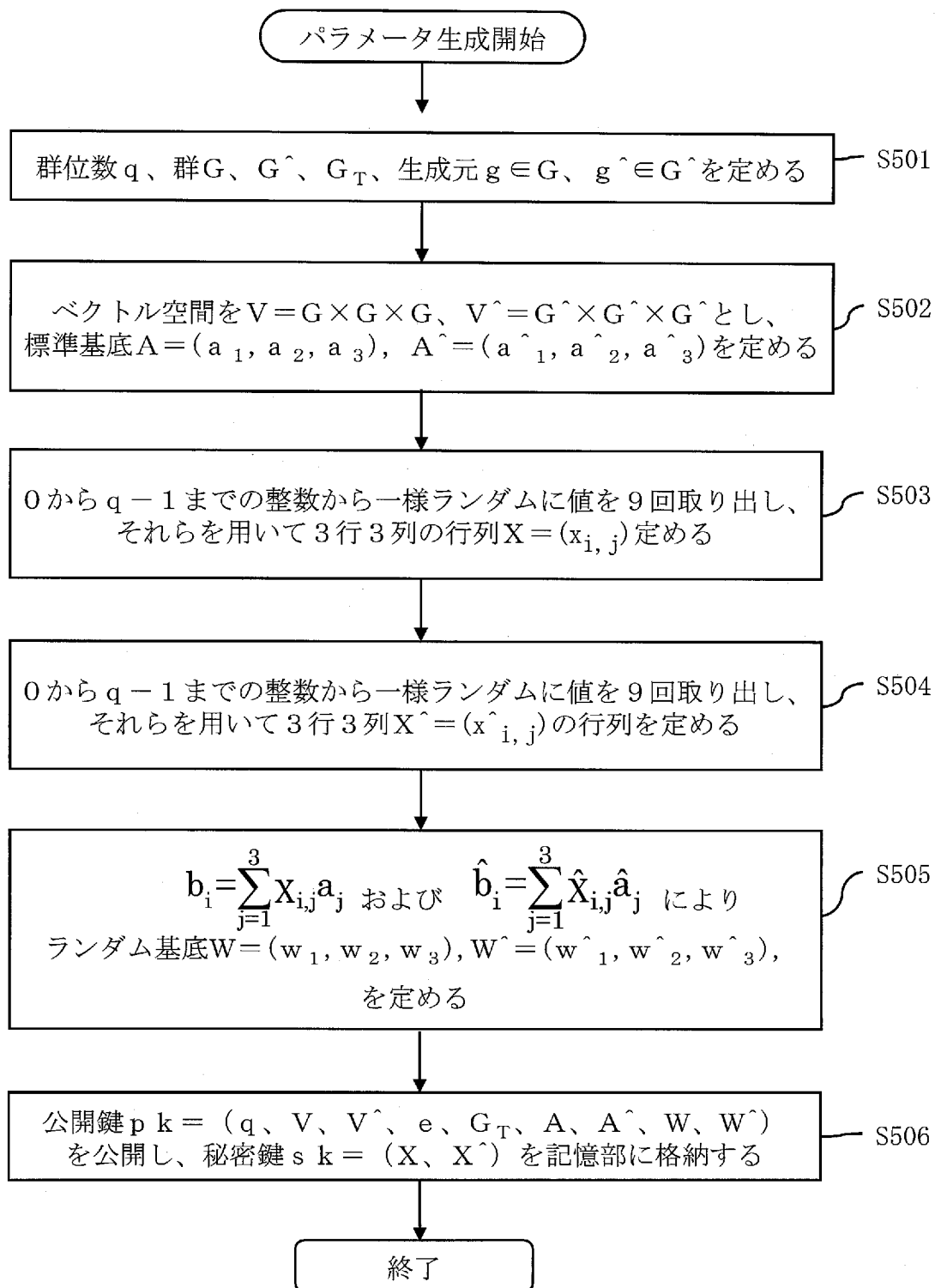
[図3]



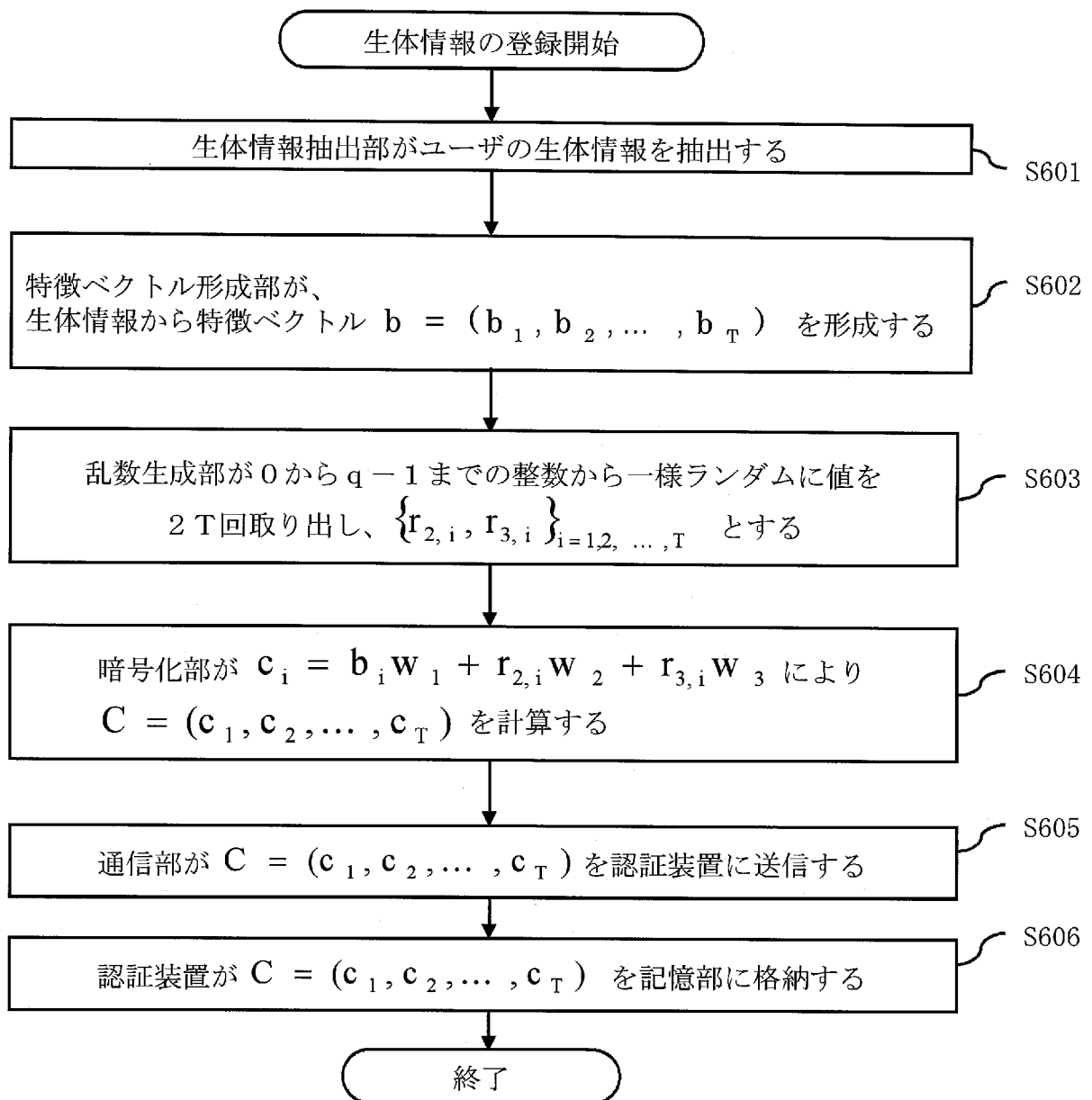
[図4]



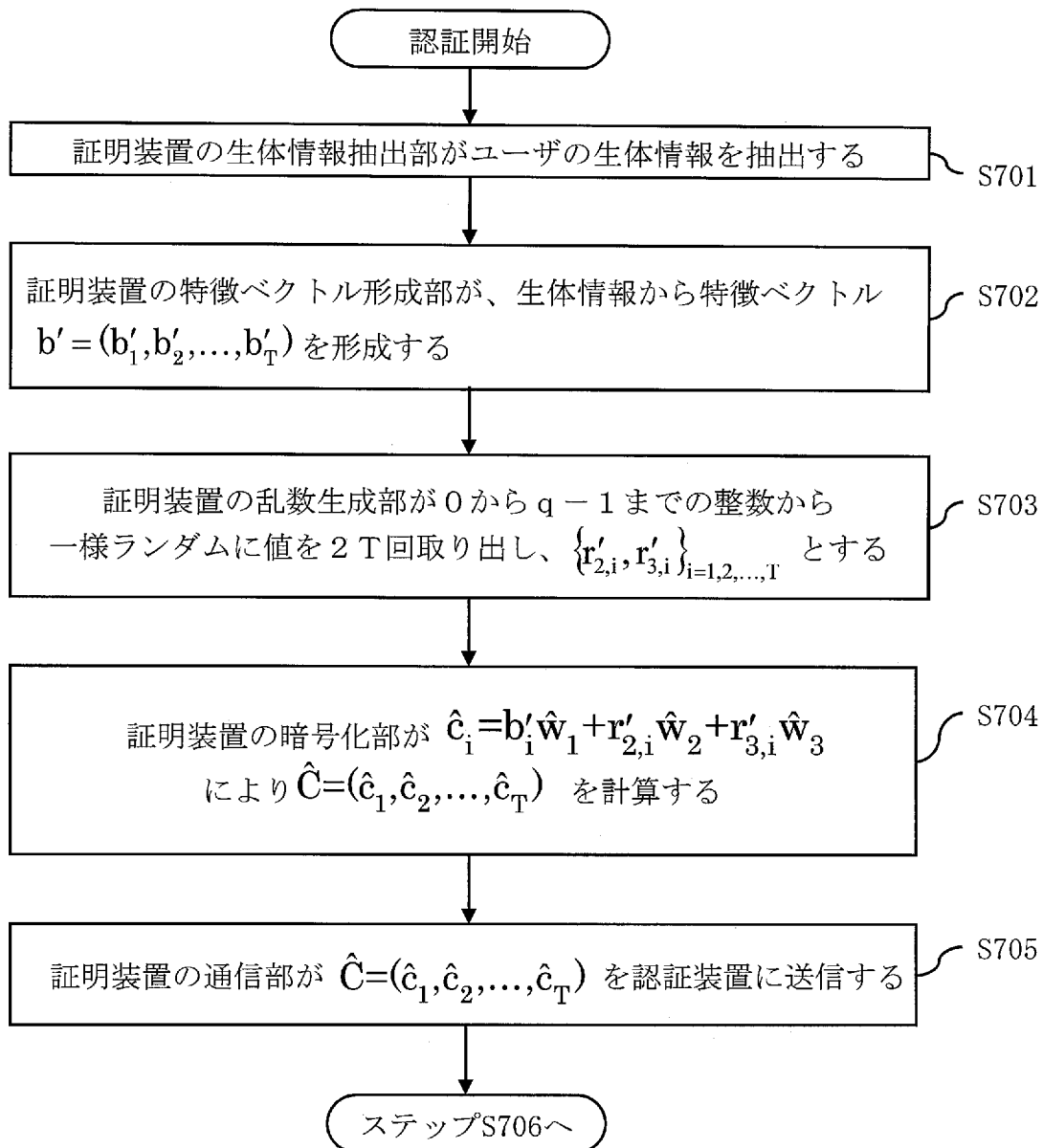
[図5]



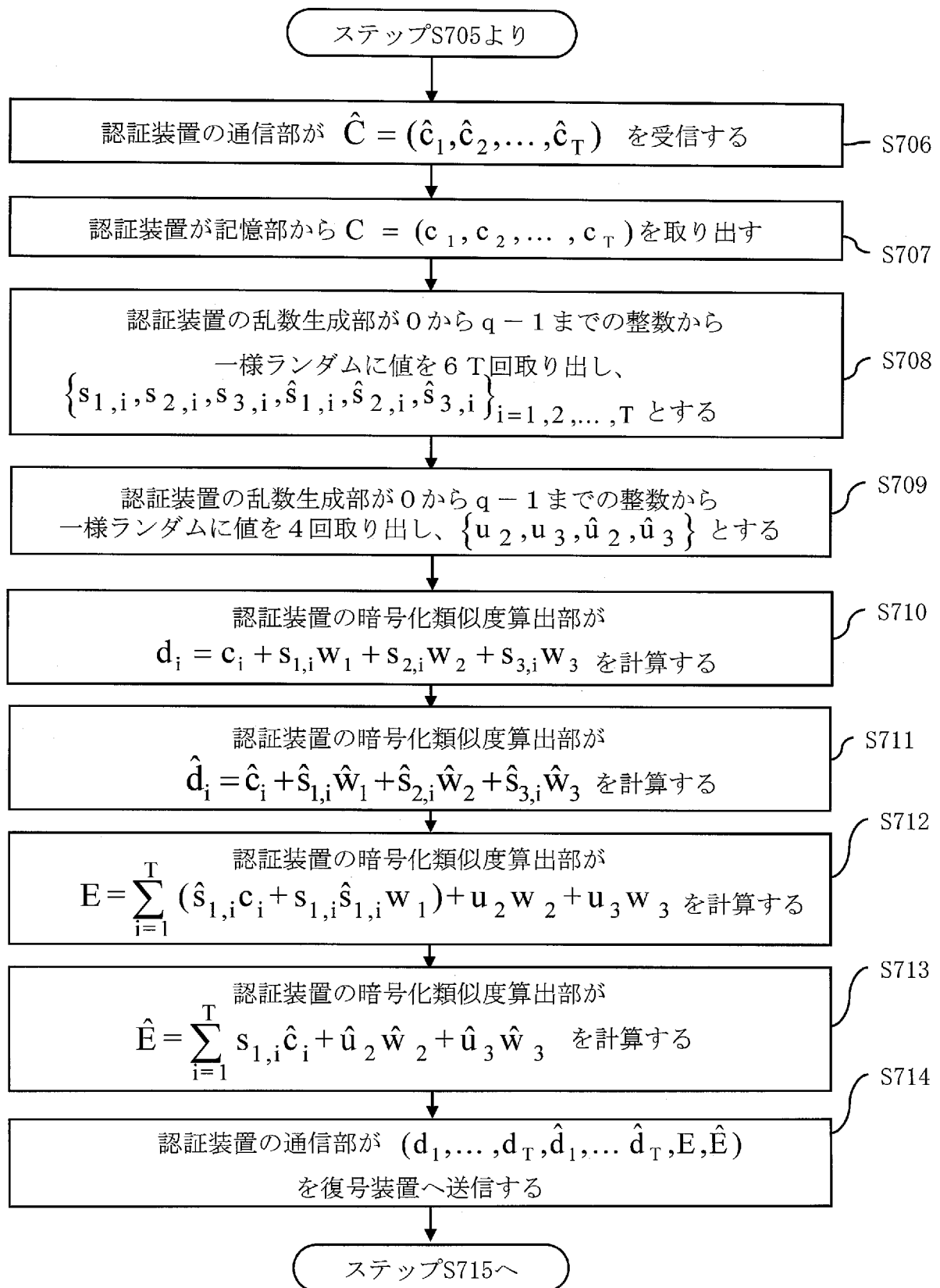
[図6]



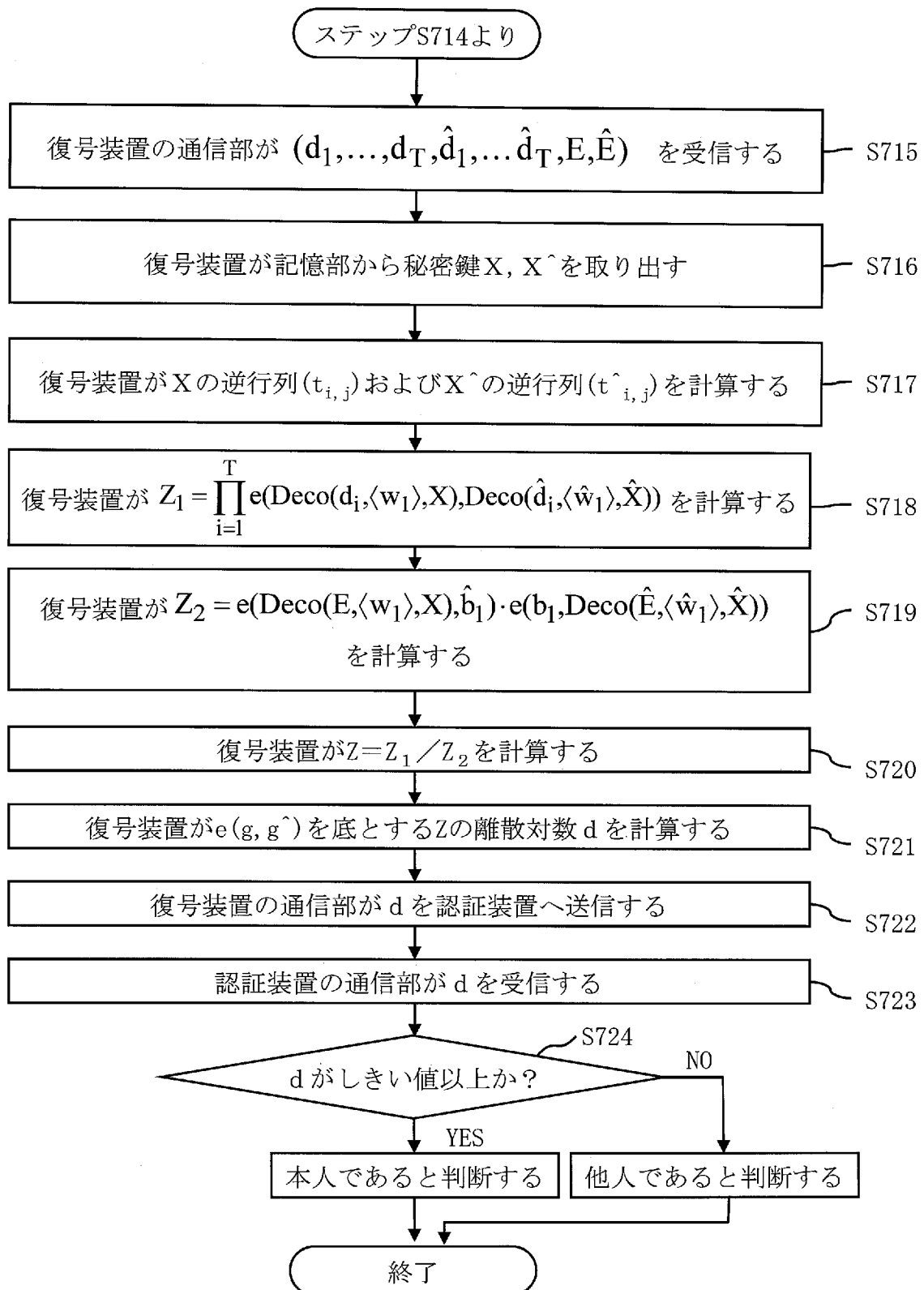
[図7]



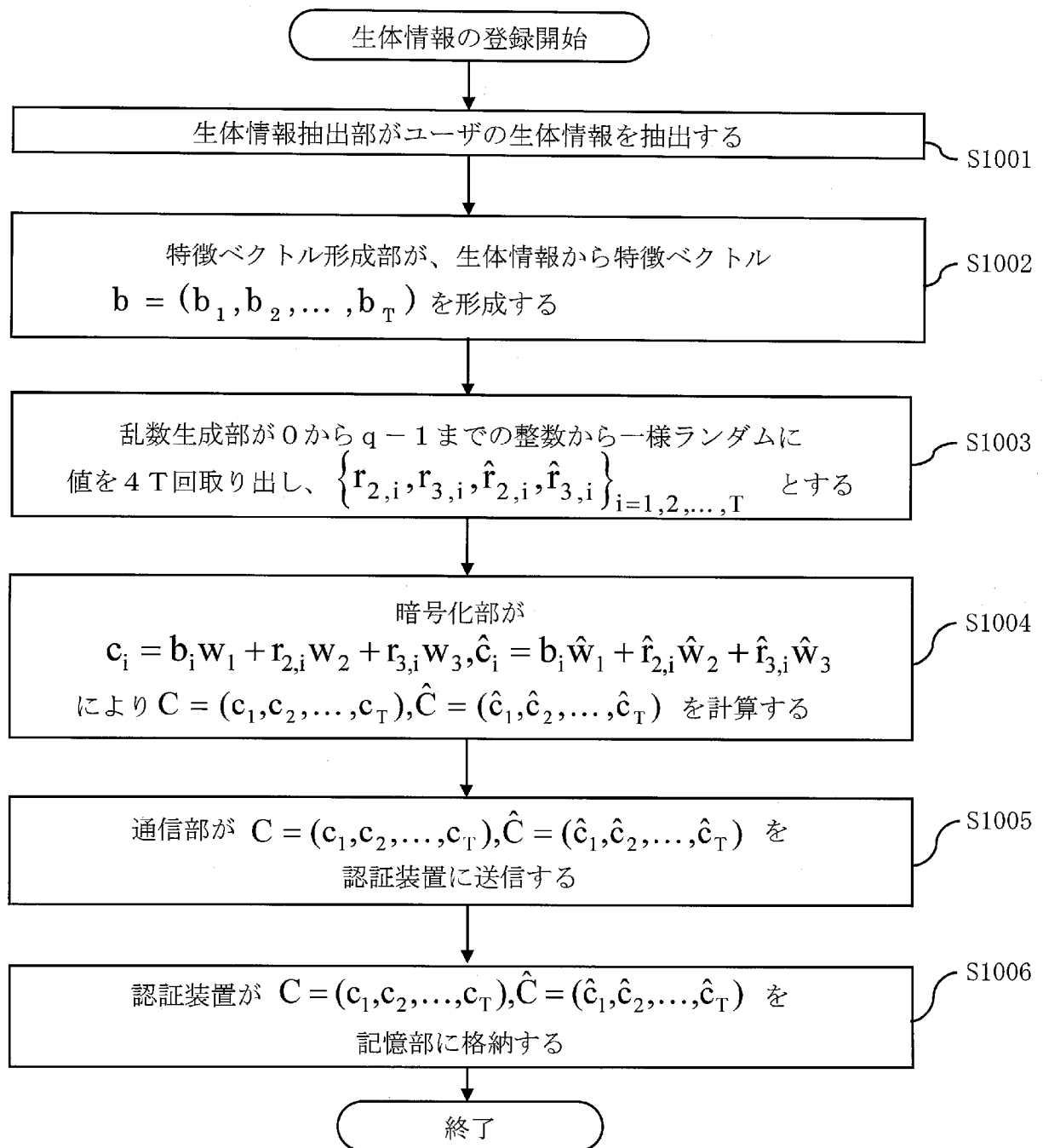
[図8]



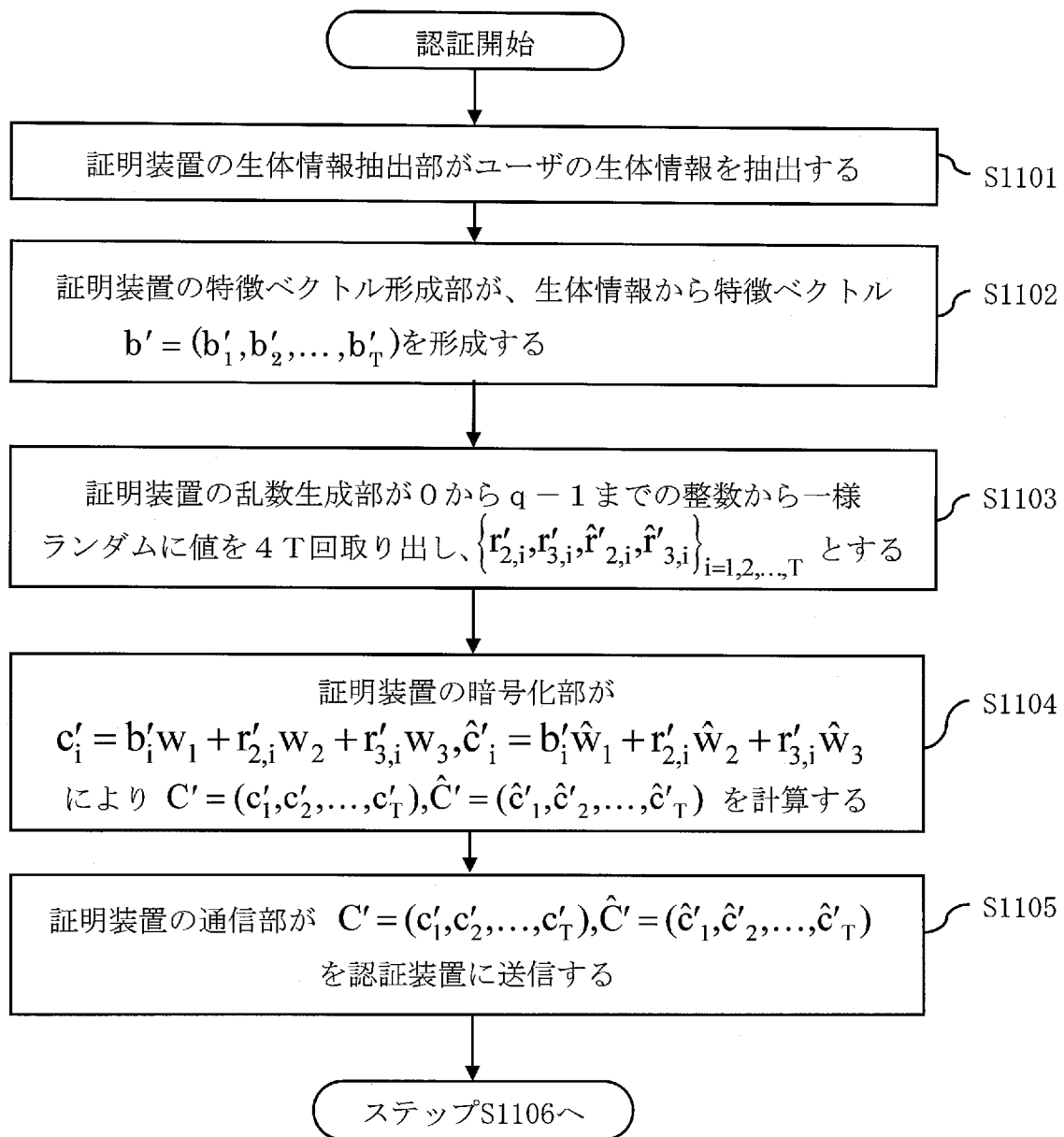
[図9]



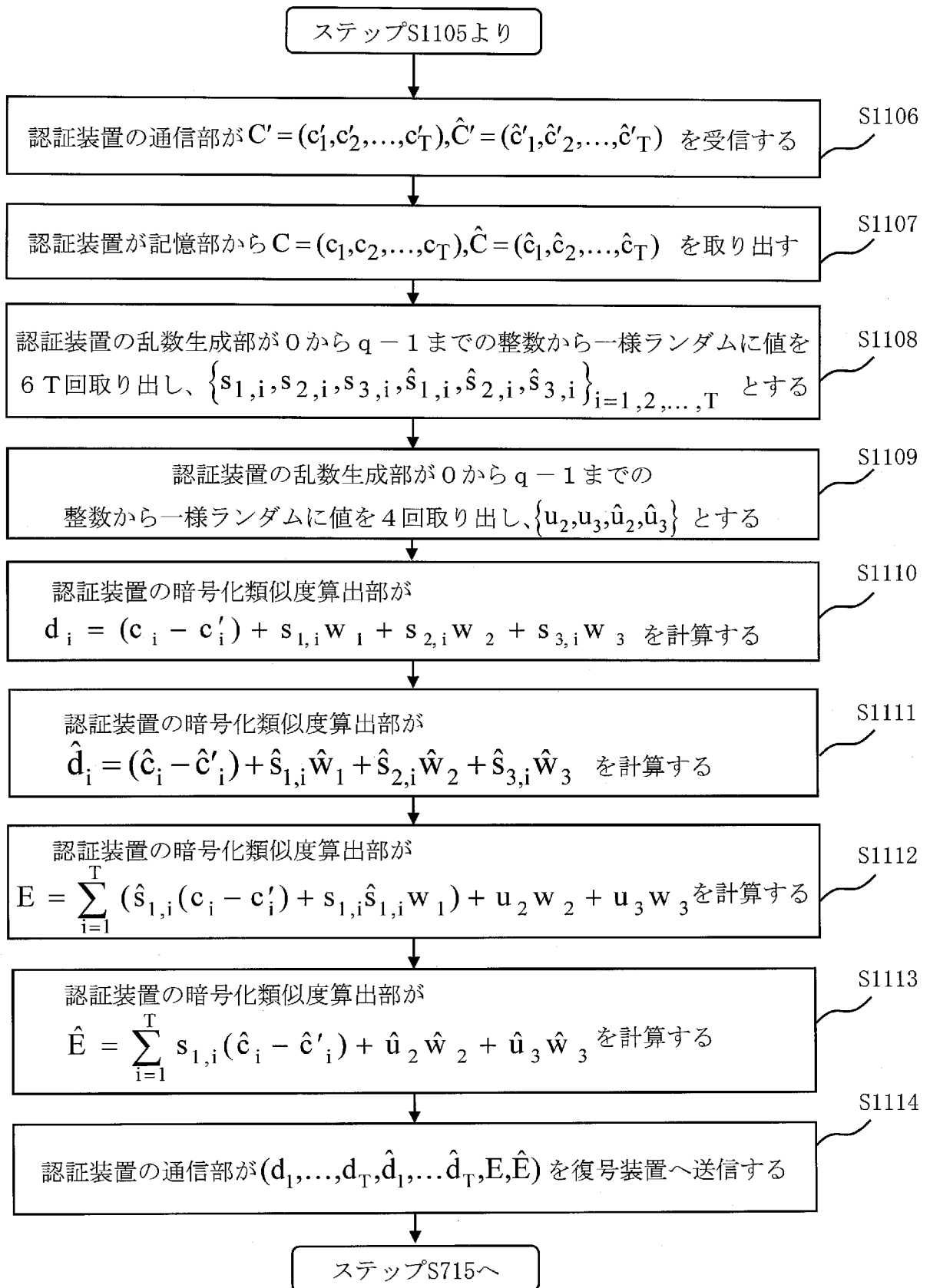
[図10]



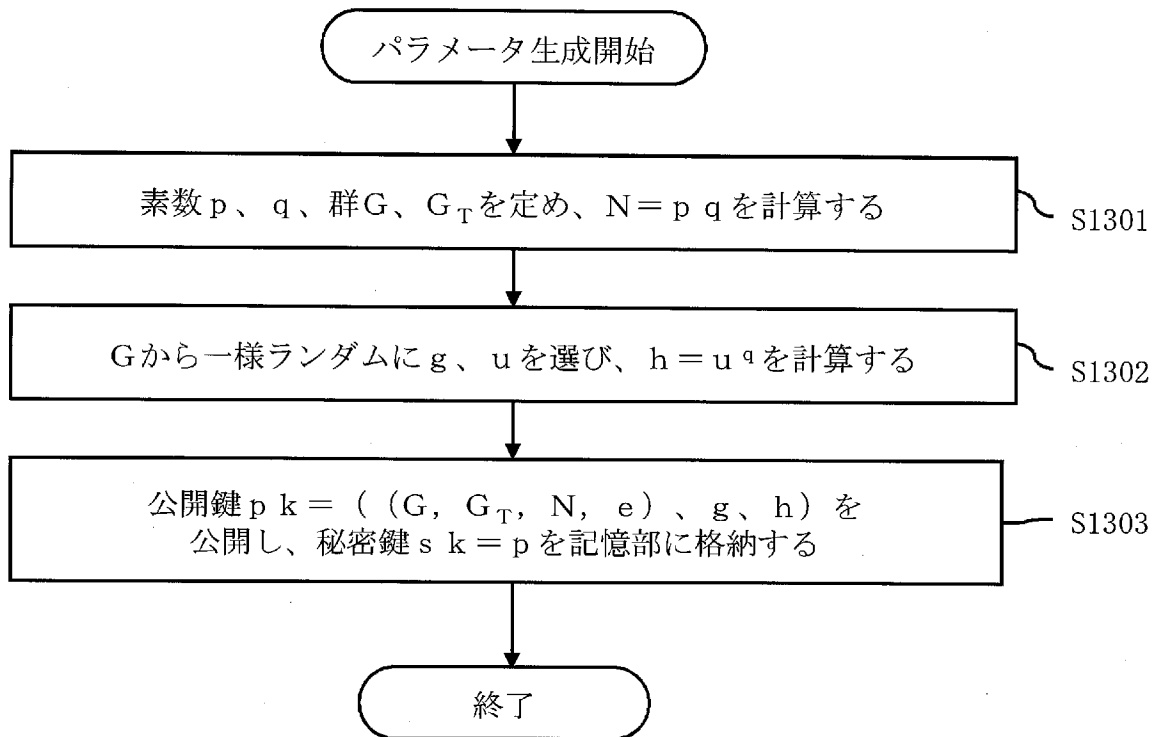
[図11]



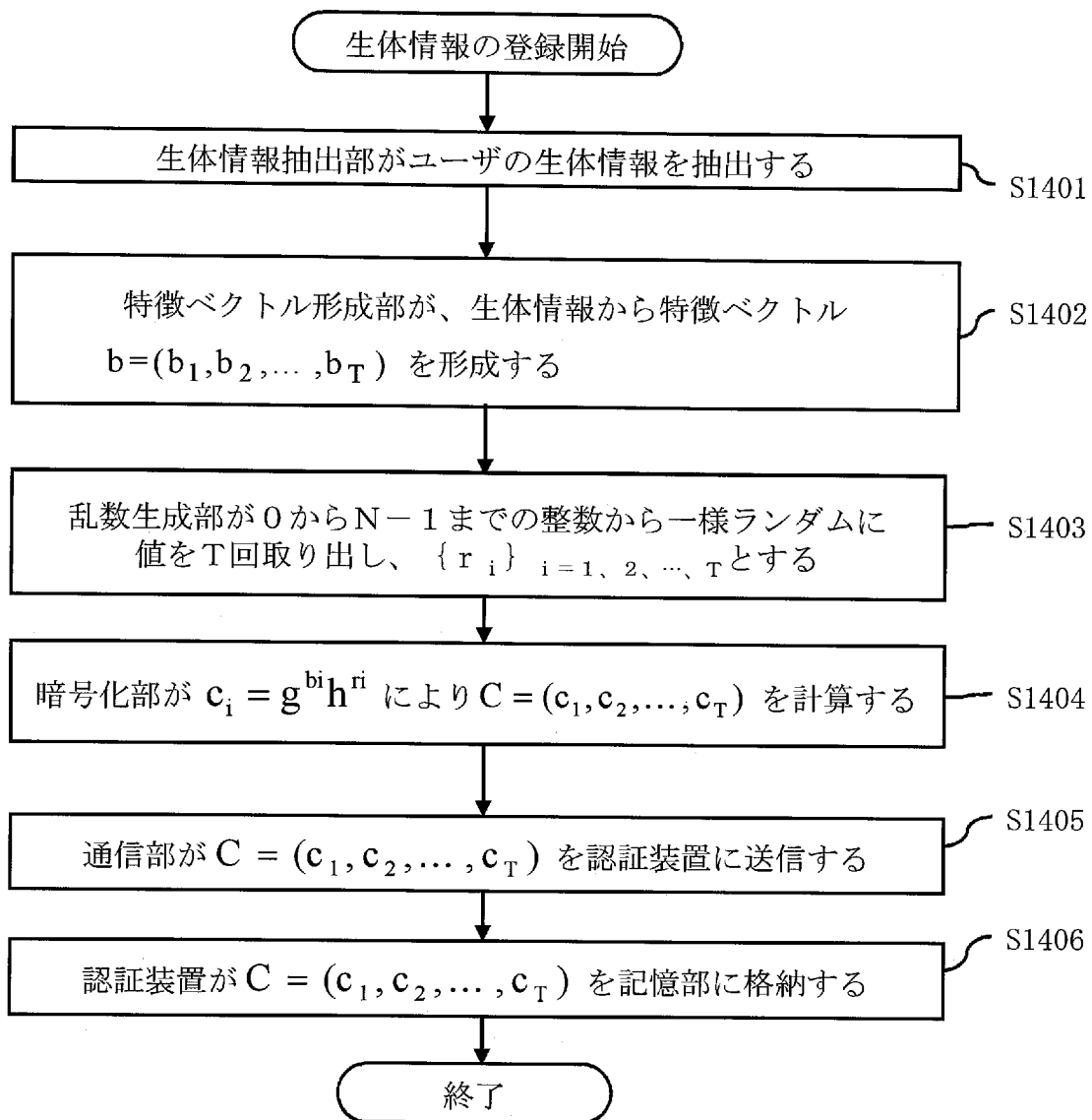
[図12]



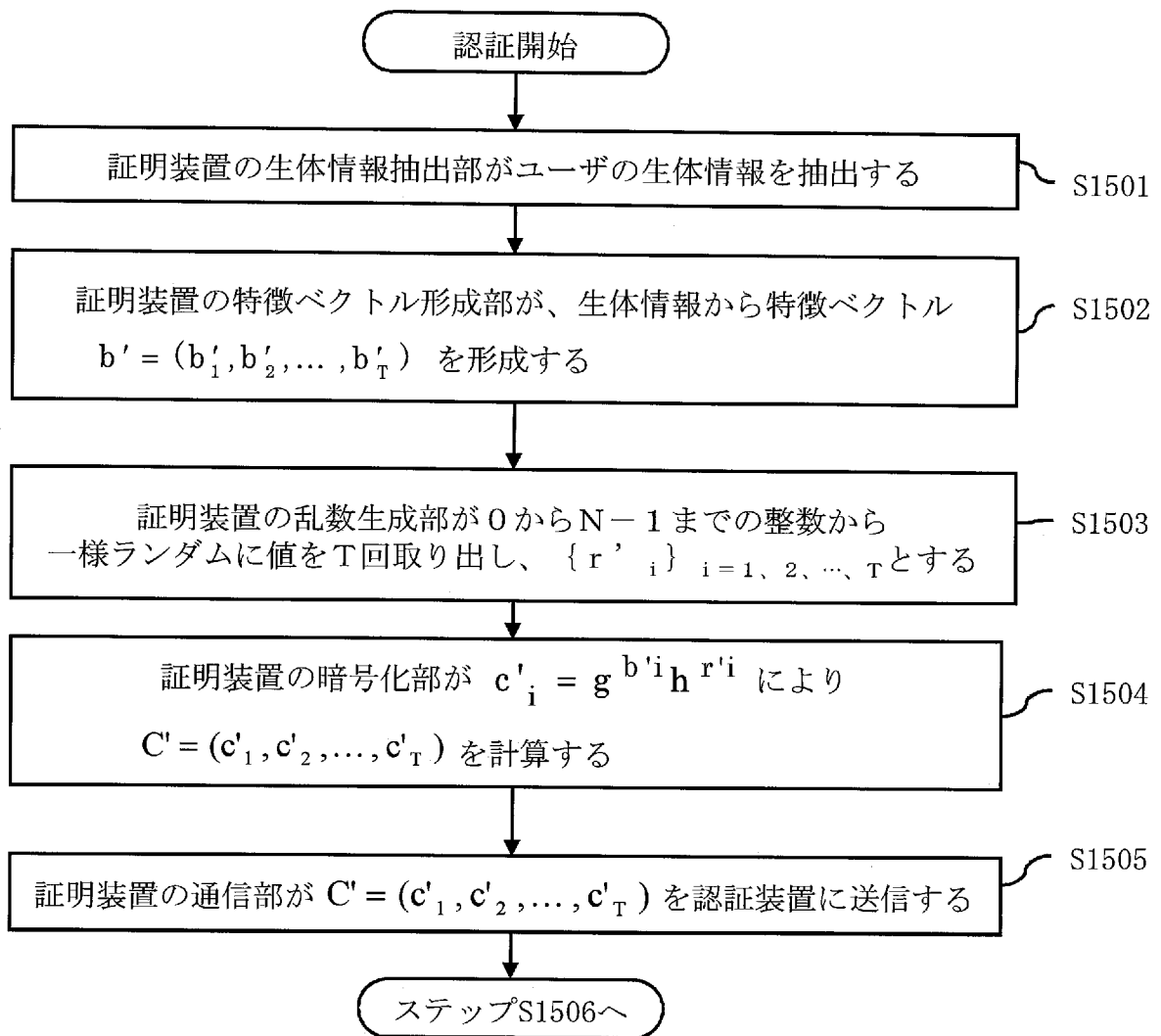
[図13]



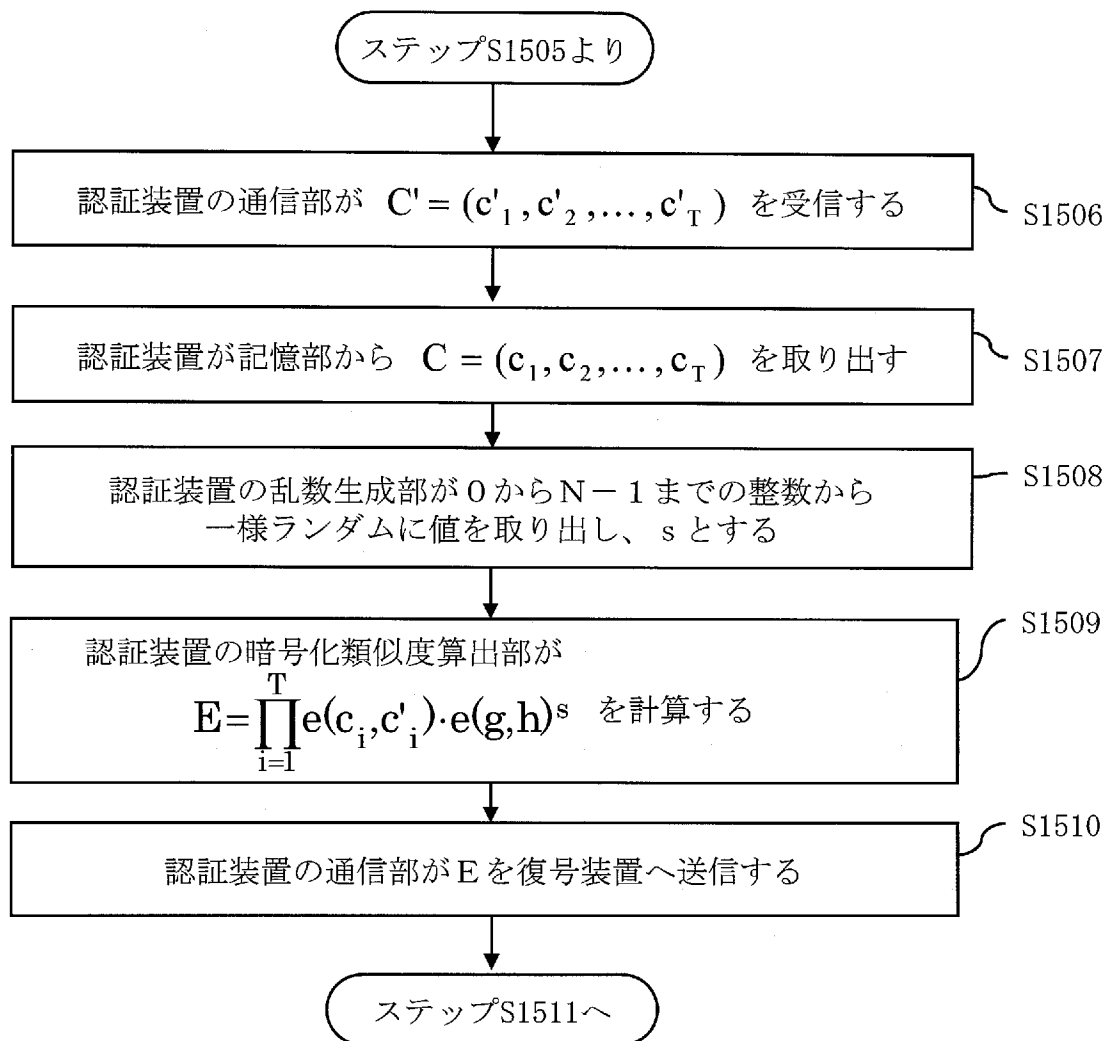
[図14]



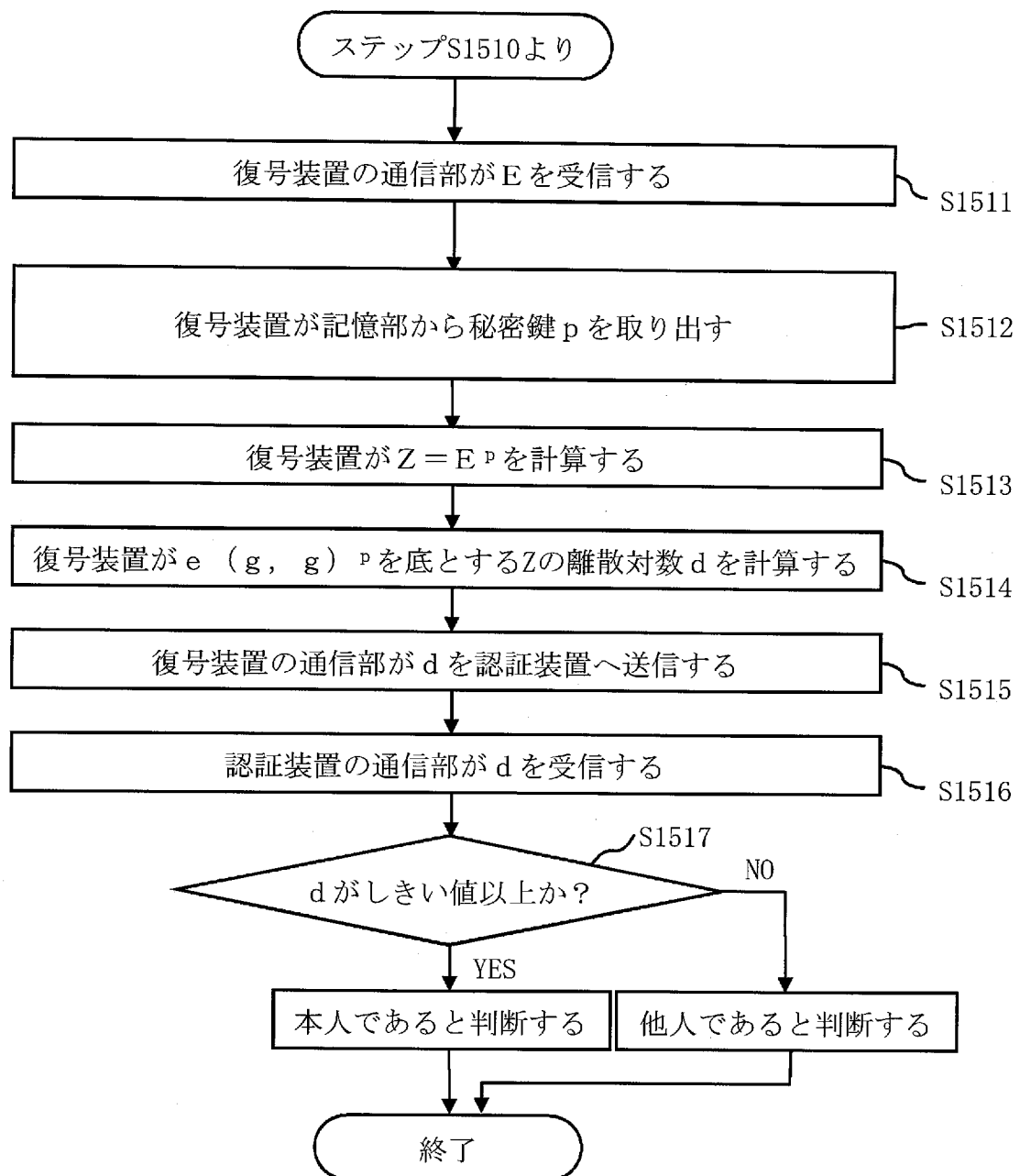
[図15]



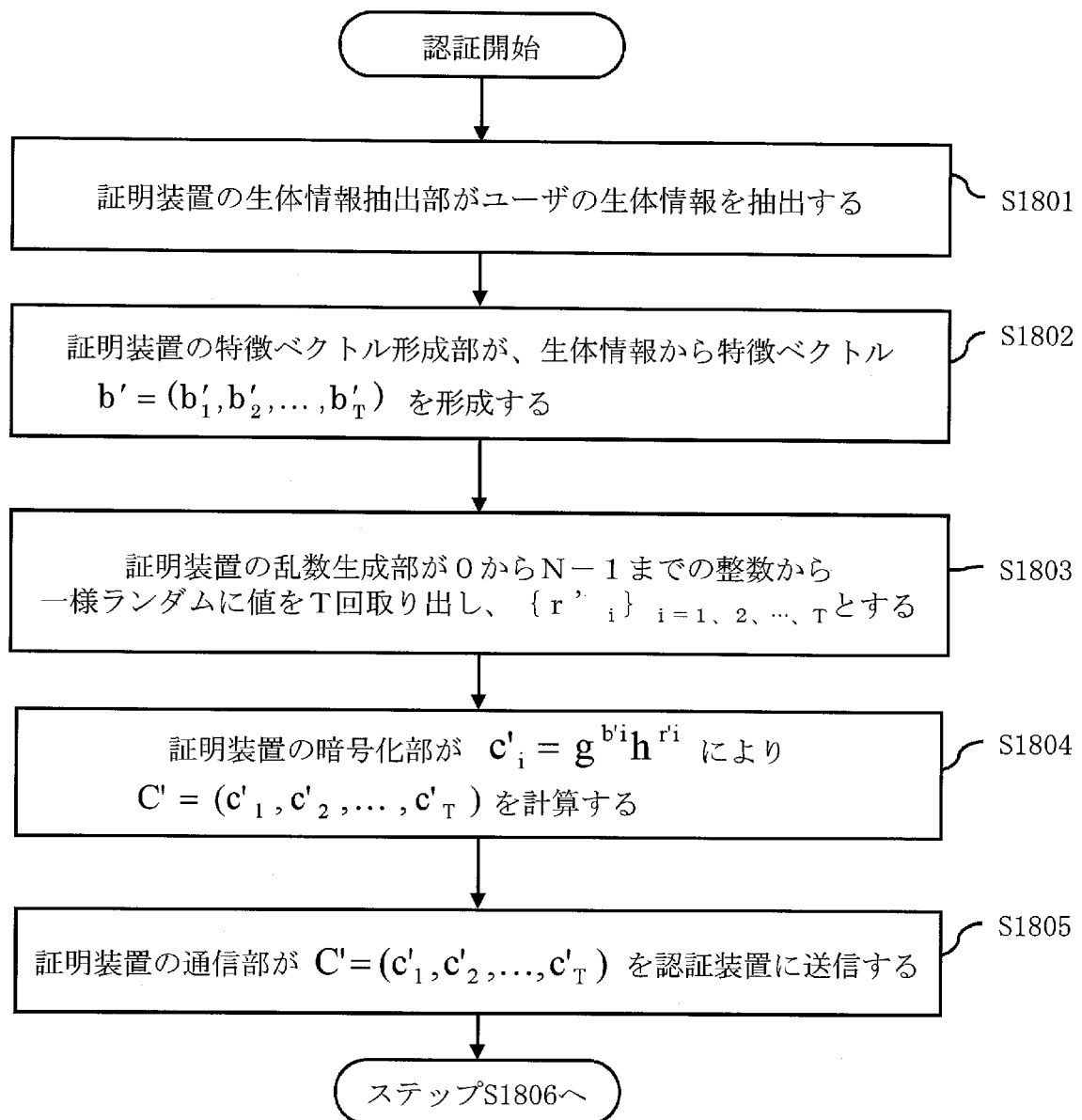
[図16]



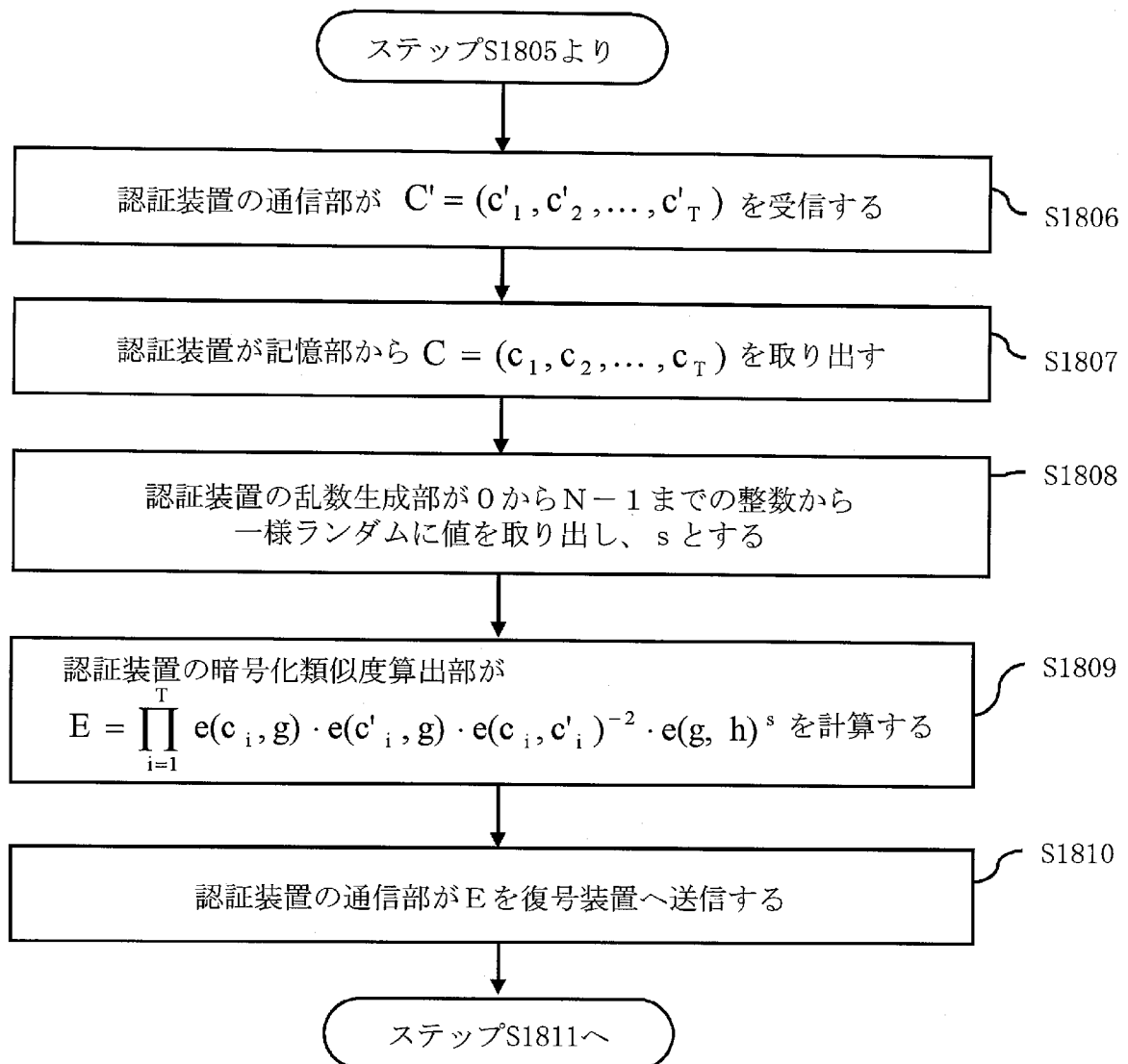
[図17]



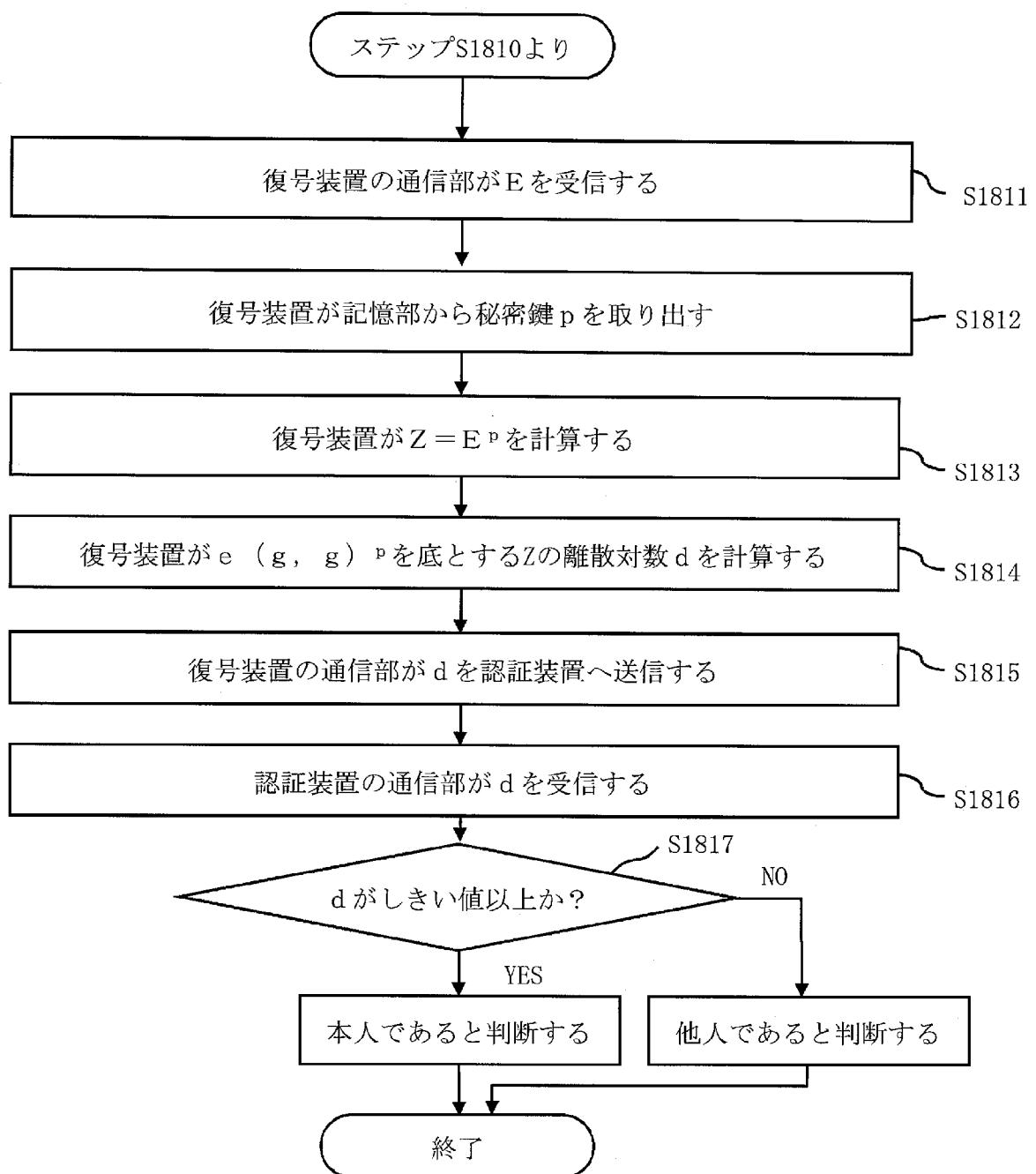
[図18]



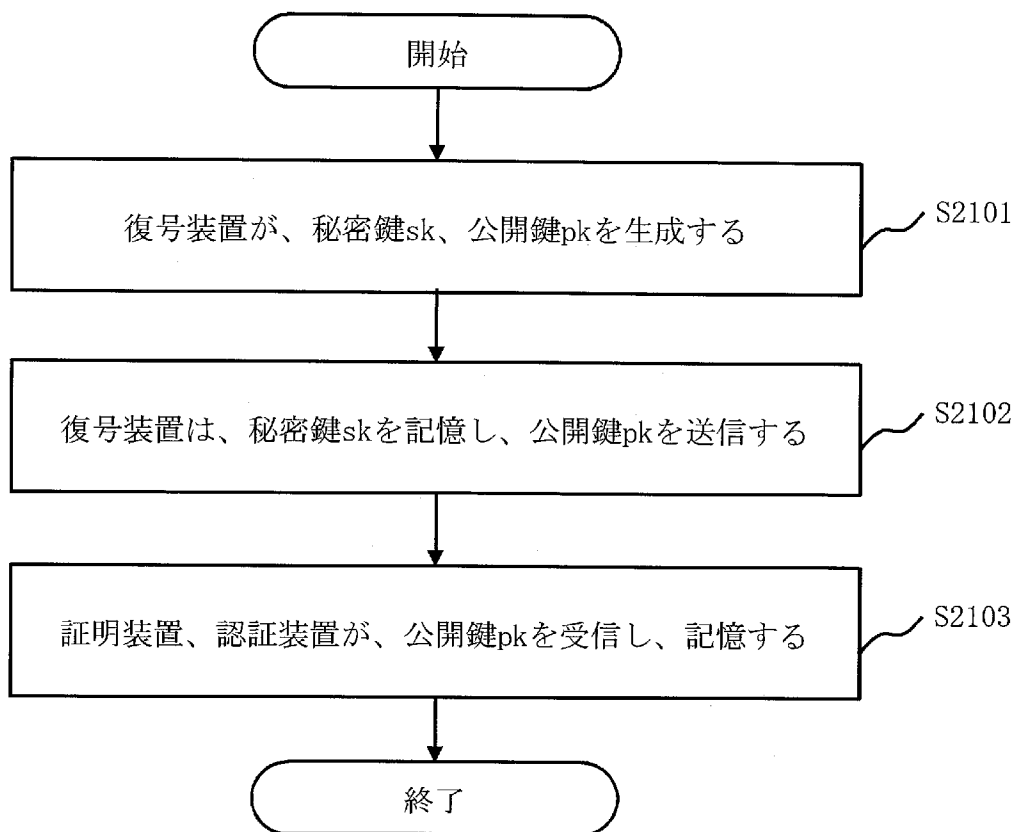
[図19]



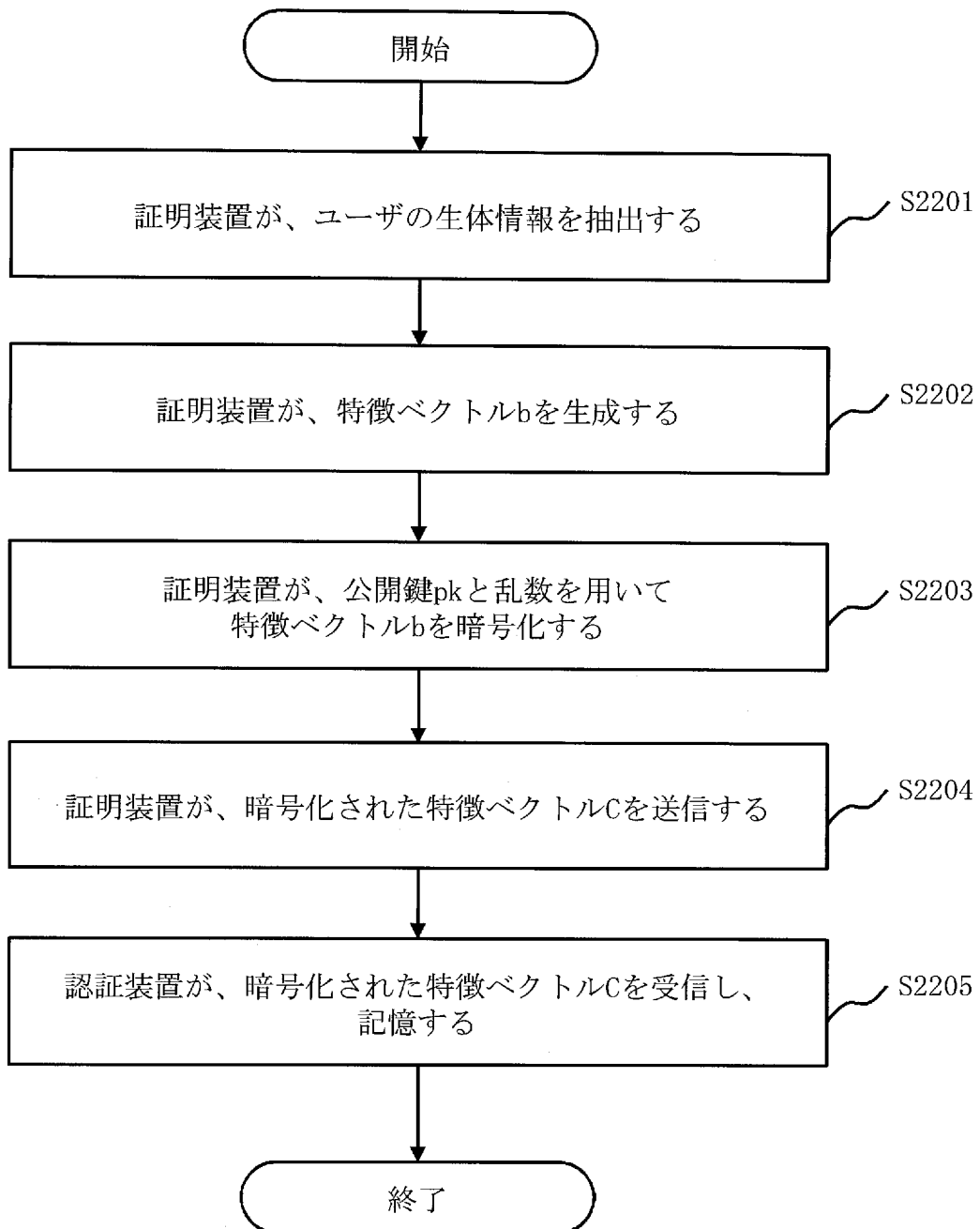
[図20]



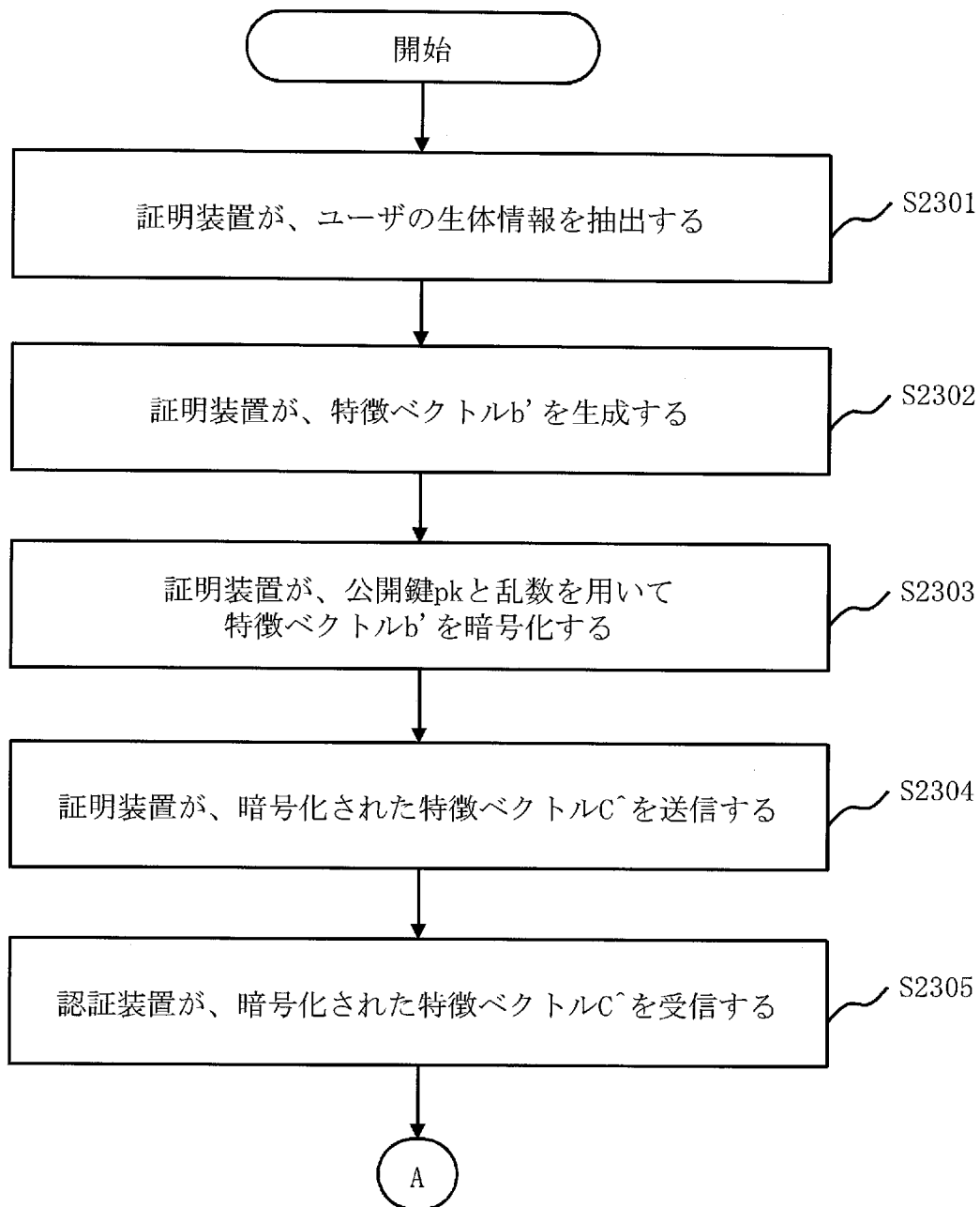
[図21]



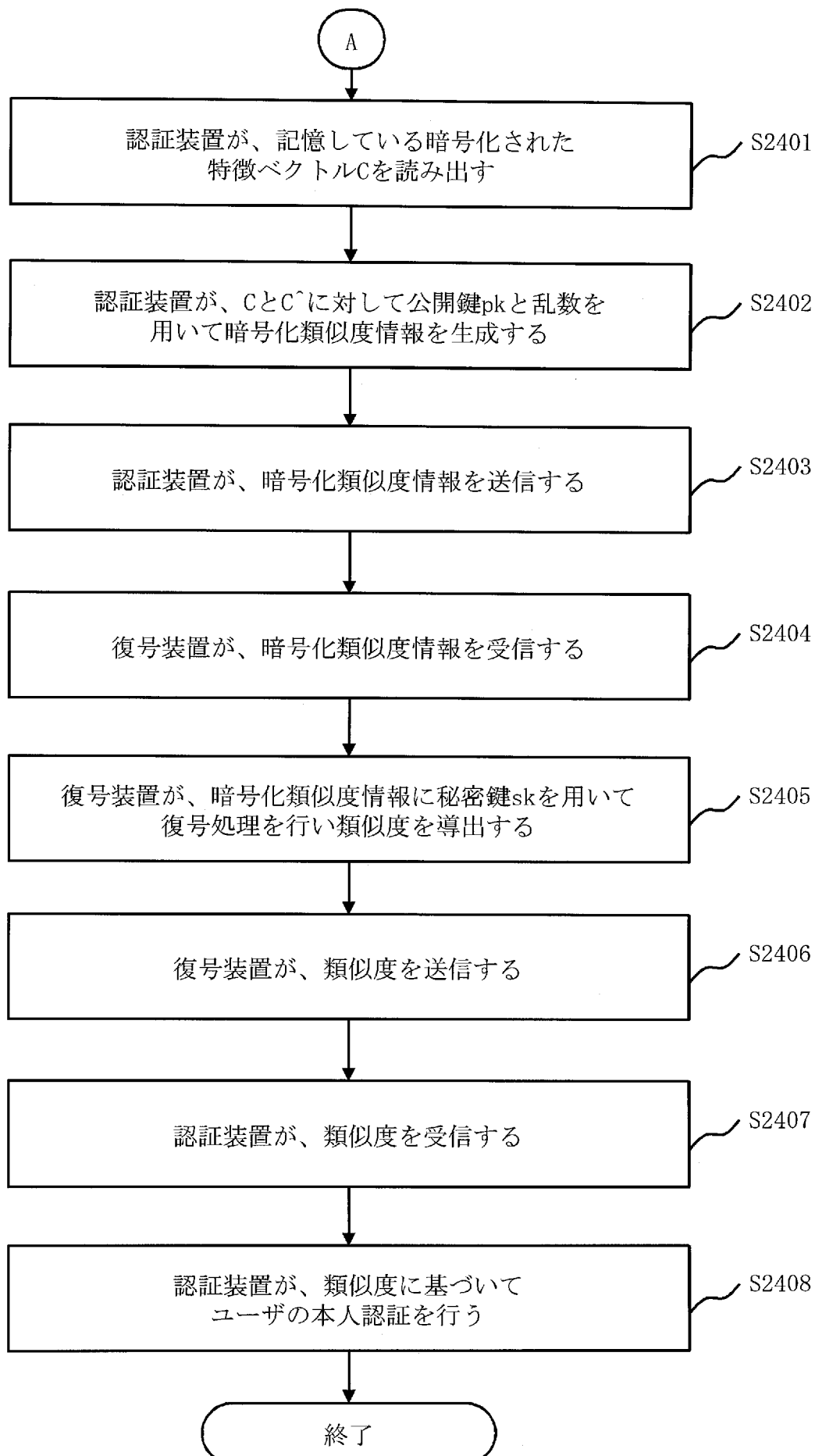
[図22]



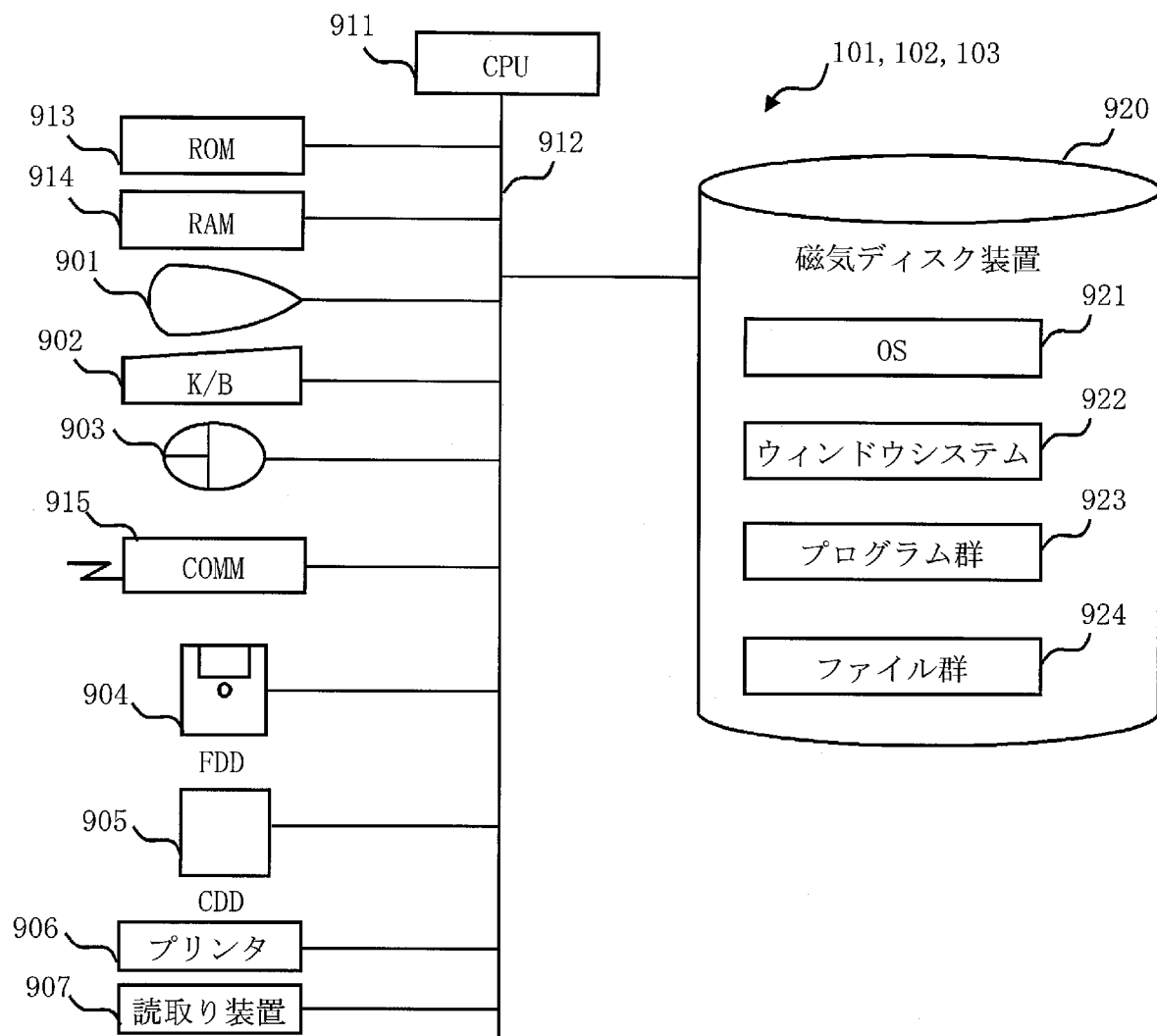
[図23]



[図24]



[図25]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2009/068584

A. CLASSIFICATION OF SUBJECT MATTER

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)

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	1996-2009
Kokai Jitsuyo Shinan Koho	1971-2009	Toroku Jitsuyo Shinan Koho	1994-2009

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	WO 2006/054208 A1 (KONINKLIJKE PHILIPS ELECTRONICS N.V.), 26 May 2006 (26.05.2006), page 8, line 24 to page 11, line 5 & US 2009/0006855 A1	1-15
A	Vladimir Kolesnikov et.al., How to Combine Homomorphic Encryption and Garbled Circuits, [online], Signal Processing in the EncryptEd Domain 2009, 2009.09, p.100-121, [retrieved on 2009-12-28], Retrieved from the Internet:<URL: http://www.speedproject.eu/dmdocuments/SPEED2009/papers/paper7.pdf>	1-15

☒ 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
28 December, 2009 (28.12.09)

Date of mailing of the international search report
12 January, 2010 (12.01.10)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2009/068584

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Mitsuhiro Hattori et.al., Public-key Encryption with Fuzzy Keyword Search, 2009 Nen Symposium on Cryptography and Information Security, 2009.01, p.1-6	1-15

A. 発明の属する分野の分類 (国際特許分類 (I P C))

Int.Cl. 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 (I P C))

Int.Cl. 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	1 9 2 2 - 1 9 9 6 年
日本国公開実用新案公報	1 9 7 1 - 2 0 0 9 年
日本国実用新案登録公報	1 9 9 6 - 2 0 0 9 年
日本国登録実用新案公報	1 9 9 4 - 2 0 0 9 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	WO 2006/054208 A1 (KONINKLIJKE PHILIPS ELECTRONICS N.V.) 2006.05.26, 第8頁第24行目～第11頁第5行目 & US 2009/0006855 A1	1-15
A	Vladimir Kolesnikov et.al., How to Combine Homomorphic Encryption and Garbled Circuits, [online], Signal Processing in the Encrypted Domain 2009, 2009.09, p.100-121, [retrieved on 2009-12-28], Retrieved from the Internet:<URL: http://www. speedproject.eu/dmdocuments/SPEED2009/papers/paper7.pdf>	1-15

☒ 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

2 8 . 1 2 . 2 0 0 9

国際調査報告の発送日

1 2 . 0 1 . 2 0 1 0

国際調査機関の名称及びあて先

日本国特許庁 (I S A / J P)

郵便番号 1 0 0 - 8 9 1 5

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)

鳥居 稔

5 S

3 8 5 7

電話番号 0 3 - 3 5 8 1 - 1 1 0 1 内線 3 5 4 6

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	Mitsuhiro Hattori et.al., Public-key Encryption with Fuzzy Keyword Search, 2 0 0 9 年暗号と情報セキュリティシンポジウム, 2009.01, p.1-6	1-15