

(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
2021年3月25日(25.03.2021)



(10) 国際公開番号

WO 2021/053749 A1

- (51) 国際特許分類:
H04L 9/32 (2006.01) G06F 21/32 (2013.01)
- (21) 国際出願番号: PCT/JP2019/036523
- (22) 国際出願日: 2019年9月18日(18.09.2019)
- (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: 日本電気株式会社 (NEC CORPORATION) [JP/JP]; 〒1088001 東京都港区芝五丁目7番1号 Tokyo (JP).
- (72) 発明者: 一色 寿幸 (ISSHIKI, Toshiyuki); 〒1088001 東京都港区芝五丁目7番1号 日本電気株式会社内 Tokyo (JP).
- (74) 代理人: 梶田 邦之, 外 (KAJITA, Kuniyuki et al.); 〒2110005 神奈川県川崎市中区新丸子町915 武蔵小杉フコク生命ビル4階 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, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL,

(54) Title: INFORMATION CHECKING SYSTEM, CLIENT TERMINAL, SERVER, INFORMATION CHECKING METHOD, AND INFORMATION CHECKING PROGRAM

(54) 発明の名称: 情報照合システム、クライアント端末、サーバ、情報照合方法、及び情報照合プログラム

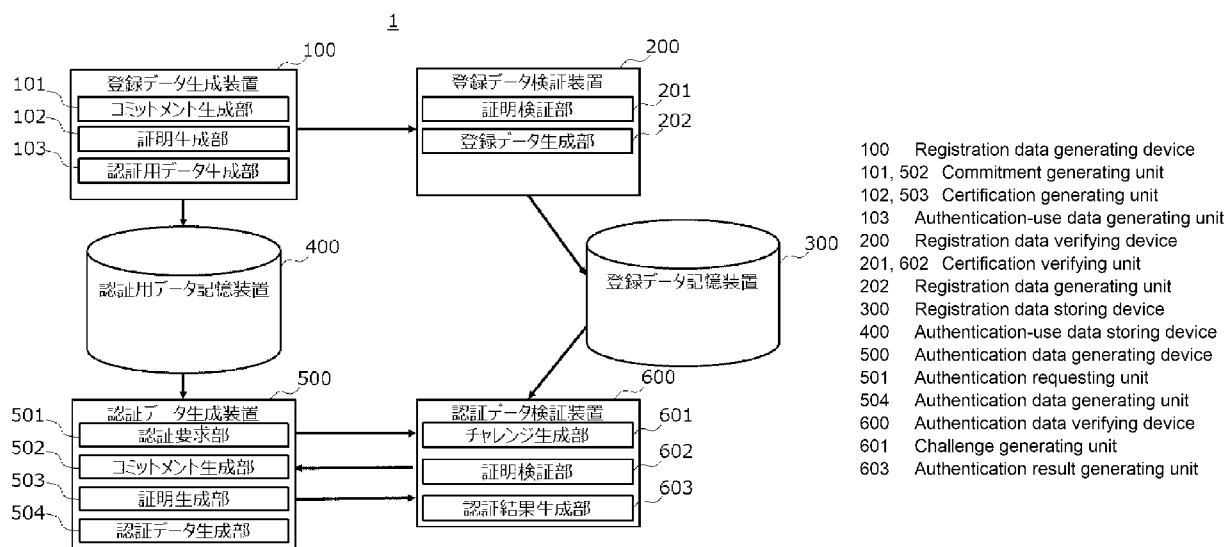


Fig. 1

(57) Abstract: Provided is a system or the like that is secure even against attacks in which the data space of one of data for registration and data for authentication is different from the data space of the other in checking of information. The present system comprises: a registration data generating device (100) that generates a first commitment of first input data for registration and also generates first certification data indicating that the first input data is included in a predetermined input data space; a registration data verifying device (200) that performs verification of the first commitment and the first certification data; an authentication data generating device (500) that generates a second commitment of second input data to be authenticated and also generates second certification data indicating that the second input data is included in the predetermined input data space and that a similarity between the second input data and registration data of a registration

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, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, 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, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類:

- 一 国際調査報告(条約第21条(3))

data storing device (300) is within a predetermined acceptance range; and an authentication data verifying device (600) that performs verification of the second commitment and the second certification data.

(57) 要約: 情報の照合において、登録及び認証のためのデータの一方のデータ空間と、他方のデータ空間が異なる攻撃に対しても安全なシステム等を提供する。本システムは、登録のための第1入力データの第1コミットメントと、第1入力データが予め定められた入力データ空間に含まれていることを示す第1証明データとを生成する登録データ生成装置(100)と、第1コミットメントと第1証明データの検証を行う登録データ検証装置(200)と、認証されるための第2入力データの第2コミットメントと、第2入力データが予め定められた入力データ空間に含まれていること及び第2入力データと登録データ記憶装置(300)の登録データの類似度が予め定められた受理範囲に含まれていることを示す第2証明データとを生成する認証データ生成装置(500)と、第2コミットメントと第2証明データの検証を行う認証データ検証装置(600)とを備える。

明 細 書

発明の名称：

情報照合システム、クライアント端末、サーバ、情報照合方法、及び情報照合プログラム

技術分野

[0001] 本発明は、情報照合システム、クライアント端末、サーバ、情報照合方法、及び情報照合プログラムに関する。

背景技術

[0002] 個人認証は、被登録者と被認証者の同一性を確認する手段である。事前に保存される被登録者に関する情報と、認証の都度取得される被認証者に関する情報を突き合わせることによって認証が実施される。

[0003] 個人認証の一手法である生体認証では顔や指紋や虹彩などの身体的特徴などを利用して認証を行う。より具体的には、生体から特徴量と呼ばれるデータを抽出して認証に用いる。生体から抽出される特徴量は抽出の都度少しずつ異なる。そのため、認証時には、被登録者から抽出された特徴量と、被認証者から抽出された特徴量とを比較し、それらが十分に類似していると認められれば認証成功となる。類似度の判定方法は特徴量抽出の手法に依存するが、一般的な手法では、特徴量はベクトルの形で表され、類似度は2つの特徴量の内積（正規化相関）、ユークリッド距離、ハミング距離等によって算出され、類似度が予め定められた範囲に含まれる場合に十分に類似していると判定する。

[0004] パスワード等の記憶による認証やICカード等の所持による認証と比べ、認証情報を入力するために記憶や所持などのユーザの能動的な準備が不要である利便性の高さや、認証情報を他人に使用されにくい安全性の高さなどが生体認証のメリットである。特徴量抽出法などの技術の進展や生体情報を採取できるセンサ機能（例えばカメラなど）を搭載した機器（例えばスマートフォン、タブレット端末など）の普及に伴い、近年、個人認証の手段として

、生体認証の利用が進んでいる。

[0005] また、生体認証技術においてゼロ知識証明を用いた例が知られている。例えば、特許文献1では、生体認証システム等において、認証サーバに対し、自分が正しい変換パラメータを知っていることを、変換パラメータに関する知識を与えずに証明する変換パラメータ証明機能が開示されている。また、特許文献1では、このような証明を、ゼロ知識証明などを用いて実現可能なことが開示されている（例えば、段落[0042]及び段落[0051]参照）。

先行技術文献

特許文献

[0006] 特許文献1：特開2008-092413号公報

非特許文献

[0007] 非特許文献1：Taher ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," IEEE transactions on information theory 31.4 (1985): 469-472.

発明の概要

発明が解決しようとする課題

[0008] 加法準同型公開鍵暗号方式などの暗号方式を利用した情報照合システムでは、入力データを暗号化により秘匿しているため、生体から生成されていないデータを用いた攻撃が想定される。このような生体から生成されていないデータから生成した登録データ又は認証データを用いた攻撃に対して安全な方式が要望される。

[0009] 例えば、生体から生成されていないデータを入力として、登録するためのデータを生成することや、認証を受けるためのデータを生成することも可能である。上述の加法準同型公開鍵暗号方式を利用した情報照合システム生体では、入力データを暗号化により秘匿してことから、上述の攻撃の例として、生体から生成されていないデータを用いて登録データを生成することによ

り、多くの生体特微量と一致して認証受理と判定されうる登録データを生成すること、及び、認証時に利用された生体特微量に関する情報を取得又は漏洩させるよう試みることなどの攻撃も想定される。また、生体から生成されていないデータを入力として認証を受けるデータを生成することにより、認証受理と判定され得るデータ（認証されるデータ）を生成することや、登録されている生体特微量に関する情報を取得又は漏洩させるよう試みる攻撃も想定される。

[0010] また、このような課題は、生体情報に限らず、予め定められたデータ空間とは別のデータ空間のデータから生成した登録データ又は認証データを用いた攻撃に対しても同様なことが言える。ここで、データ空間とは、例えば、生体情報など、登録するデータ又は認証されるデータを構成するデータ（値）がとり得る値の範囲、性質などをいう。

[0011] 本発明の目的は、情報の照合において、予め定められたデータ空間とは別のデータ空間のデータから生成した登録データ又は認証データを用いた攻撃に対しても安全な情報照合システム、クライアント端末、サーバ、情報照合方法、及び情報照合プログラムを提供することにある。一例として、本発明の目的のひとつは、生体情報を利用した情報の照合において、生体から生成されていないデータを用いた攻撃に対して安全な方式を提供することにある。

課題を解決するための手段

[0012] 本発明の情報照合システムは、登録のための第1入力データの第1コミットメントと、第1入力データが予め定められた入力データ空間に含まれていることを示す第1証明データとを生成する登録データ生成装置と、第1コミットメントと第1証明データの一部又は全部を記憶する認証用データ記憶装置と、第1コミットメントと第1証明データの検証を行う登録データ検証装置と、第1コミットメントと第1証明データの一部又は全部を登録データとして記憶する登録データ記憶装置と、認証されるための第2入力データの第2コミットメントと、第2入力データが上記予め定められた入力データ空間

に含まれていること及び第2入力データと上記登録データ記憶装置の登録データの類似度が予め定められた受理範囲に含まれていることを示す第2証明データとを生成する認証データ生成装置と、第2コミットメントと第2証明データの検証を行う認証データ検証装置と備える。

[0013] 本発明のクライアント端末は、登録のための第1入力データの第1コミットメントと、第1入力データが予め定められた入力データ空間に含まれていることを示す第1証明データとを含む登録データを生成する登録データ生成部と、第1コミットメントと第1証明データの一部又は全部を記憶する認証用データ記憶部と、認証されるための第2入力データの第2コミットメントと、第2入力データが予め定められた入力データ空間に含まれていること及び第2入力データと登録データの類似度が予め定められた受理範囲に含まれていることを示す第2証明データとを生成する認証データ生成部とを備える。

[0014] 本発明のサーバは、登録のための第1入力データの第1コミットメントと、第1入力データが予め定められた入力データ空間に含まれていることを示す第1証明データとを入力し、第1コミットメントと第1証明データの検証を行う登録データ検証部と、認証されるための第2入力データの第2コミットメントと、第2入力データが予め定められた入力データ空間に含まれていること及び第2入力データと登録データ記憶部の登録データの類似度が予め定められた受理範囲に含まれていることを示す第2証明データとを入力し、第2コミットメントと第2証明データの検証を行う認証データ検証部との少なくとも一方を備える。

[0015] 本発明の情報照合方法は、登録のための第1入力データの第1コミットメントと、第1入力データが予め定められた入力データ空間に含まれていることを示す第1証明データとを生成する登録データ生成処理と、第1コミットメントと第1証明データの一部又は全部を記憶する認証用データ記憶処理と、第1コミットメントと第1証明データの検証を行う登録データ検証処理と、第1コミットメントと第1証明データの一部又は全部を登録データとして

記憶する登録データ記憶処理と、認証されるための第2入力データの第2コミットメントと、第2入力データが上記予め定められた入力データ空間に含まれていること及び第2入力データと上記登録データ記憶部の登録データの類似度が予め定められた受理範囲に含まれていることを示す第2証明データとを生成する認証データ生成処理と、第2コミットメントと第2証明データの検証を行う認証データ検証処理とを含む。

[0016] 本発明の情報照合プログラムは、登録のための第1入力データの第1コミットメントと、第1入力データが予め定められた入力データ空間に含まれていることを示す第1証明データとを生成する登録データ生成処理と、第1コミットメントと第1証明データの一部又は全部を記憶する認証用データ記憶処理と、第1コミットメントと第1証明データの検証を行う登録データ検証処理と、第1コミットメントと第1証明データの一部又は全部を登録データとして記憶する登録データ記憶処理と、認証されるための第2入力データの第2コミットメントと、第2入力データが上記予め定められた入力データ空間に含まれていること及び第2入力データと上記登録データ記憶部の登録データの類似度が予め定められた受理範囲に含まれていることを示す第2証明データとを生成する認証データ生成処理と、第2コミットメントと第2証明データの検証を行う認証データ検証処理とをコンピュータに実行させる。

発明の効果

[0017] 本発明によると、情報の照合において、登録及び認証のためのデータの一方のデータ空間と、他方のデータ空間が異なる攻撃に対しても安全な情報照合システム、クライアント端末、サーバ、情報照合方法、及び情報照合プログラムを提供することができる。一例として、本発明によると、生体情報を利用した情報の照合において、生体から生成されていないデータを用いた攻撃に対して安全な方式を提供することが可能である。なお、本発明により、当該効果の代わりに、又は当該効果とともに、他の効果が奏されてもよい。

図面の簡単な説明

[0018] [図1]本発明の実施形態に係る情報照合システムの具体的な構成を示すブロッ

ク図である。

[図2]本実施形態における登録処理のフローチャートである。

[図3]本実施形態における照合処理のフローチャートである。

[図4]本実施形態における装置のハードウェア構成を示すブロック図である。

[図5]本実施形態における情報照合システムの一例を示すブロック図である。

[図6]本実施形態におけるクライアント端末の一例を示すブロック図である。

[図7]本実施形態におけるサーバの一例を示すブロック図である。

発明を実施するための形態

[0019] 以下、添付の図面を参照して本発明の実施形態を詳細に説明する。なお、本明細書及び図面において、同様に説明されることが可能な要素については、同一の符号を付することにより重複説明が省略され得る。

[0020] 説明は、以下の順序で行われる。

1. 関連技術
2. 本発明の実施形態の概要
3. 実施形態
 3. 1. システムの構成
 3. 2. 登録及び照合の動作
 3. 3. 実施例 1
 3. 4. 実施例 2
4. その他

[0021] <<1. 関連技術>>

個人認証は、被登録者と被認証者の同一性を確認する手段である。事前に保存される被登録者に関する情報と、認証の都度取得される被認証者に関する情報を突き合わせることによって認証が実施される。

[0022] 個人認証の一手法である生体認証では顔や指紋や虹彩などの身体的特徴などを利用して認証を行う。より具体的には、生体から特徴量と呼ばれるデータを抽出して認証に用いる。生体から抽出される特徴量は抽出の都度少しずつ異なる。そのため、認証時には、被登録者から抽出された特徴量と、被認

証者から抽出された特徴量とを比較し、それらが十分に類似していると認められれば認証成功となる。類似度の判定方法は特徴量抽出の手法に依存するが、一般的な手法では、特徴量はベクトルの形で表され、類似度は2つの特徴量の内積（正規化相関）、ユークリッド距離、ハミング距離等によって算出され、類似度が予め定められた範囲に含まれる場合に十分に類似していると判定する。

[0023] パスワード等の記憶による認証やICカード等の所持による認証と比べ、認証情報を入力するために記憶や所持などのユーザの能動的な準備が不要である利便性の高さや、認証情報を他人に使用されにくい安全性の高さなどが生体認証のメリットである。特徴量抽出法などの技術の進展や生体情報を採取できるセンサ機能（例えばカメラなど）を搭載した機器（例えばスマートフォン、タブレット端末など）の普及に伴い、近年、個人認証の手段として、生体認証の利用が進んでいる。

[0024] 一方で、生体認証には、生涯不変である生体情報はもし漏洩したとしても変更できないというデメリットもある。また、生体特徴量は、欧州の一般データ保護規則や日本の個人情報保護法において、個人情報に該当すると定められている。個人情報に該当するデータは、保管や外部提供等の取扱いに制限がある。また、法令等による制限だけでなく、社会的に受容されるための配慮も求められることが多い。一般に、個人情報保護の観点から、検証者（例えば認証サーバなど）側がユーザの生体情報に関する情報を保持しない生体認証方式が望ましい。その上で、ユーザが持つ端末（例えばスマートフォンなど）への攻撃も考慮し、ユーザの保持する端末がマルウェア等に乗っ取られた場合であっても生体情報が復元できない方式が望ましい。

[0025] そこで、生体情報を秘匿して保存し、秘匿したまま認証結果を判定できる生体認証手法が盛んに研究されている。秘匿したままの判定を実現する手段として、加法準同型性を有する公開鍵暗号方式を利用する手法が知られている。

[0026] 公開鍵暗号方式は、鍵生成アルゴリズム（Key Gen）、暗号化アルゴ

リズム（ E_{nc} ）、及び復号アルゴリズム（ D_{ec} ）の3つのアルゴリズムで構成される。鍵生成アルゴリズムは、セキュリティパラメータと呼ばれる鍵の強度を表すパラメータを用いて、暗号化鍵 e_k 及び復号鍵 d_k を生成する。この動作は、セキュリティパラメータを κ とすると、次式のように表すことができる。

$$KeyGen(\kappa) \rightarrow (e_k, d_k)$$

暗号化アルゴリズムは、暗号化鍵 e_k により平文のメッセージ m を暗号化した結果である暗号文 c を生成する。これは次式のように表すことができる。

$$Enc(e_k, m) \rightarrow c$$

復号アルゴリズムは、復号鍵 d_k により暗号文 c を復号した結果である m' を生成する。これは次式のように表すことができる。

$$Dec(d_k, c) \rightarrow m'$$

[0027] 公開鍵暗号方式は正しく暗号文を復号できる必要がある。すなわち、鍵生成アルゴリズムで生成された任意の暗号化鍵 e_k 及び復号鍵 d_k のペアに対し、任意のメッセージ m を暗号化鍵 e_k で暗号化した結果である暗号文 c を復号鍵 d_k によって復号した結果 m' は m と等しくなる必要がある。すなわち、 $KeyGen(\kappa) \rightarrow (e_k, d_k)$ に対し、任意の m について

$$Dec(d_k, Enc(e_k, m)) \rightarrow m$$

が成り立つ必要がある。

[0028] 公開鍵暗号方式では、暗号化鍵を持っていれば誰でも暗号化アルゴリズムを実行可能であるが、復号鍵なしでは復号アルゴリズムは実行できない。

[0029] 準同型性を有する公開鍵暗号方式（以下では、準同型公開鍵暗号と呼ぶ）は、公開鍵暗号の各アルゴリズムに加え、準同型演算アルゴリズム（ Hom ）を有する。

[0030] 準同型演算アルゴリズムは、暗号化鍵 e_k により、入力された複数の暗号文 c_1 、 c_2 に対応するメッセージの演算結果の暗号文を生成する。入力できるメッセージが2つである場合、次式のように表すことができる。

$$\text{Hom}(e_k, c_1, c_2) \rightarrow c$$

[0031] 例えば、加法準同型性を有する公開鍵暗号の場合、メッセージ m_1 の暗号化鍵 e_k による暗号文 c_1 と、メッセージ m_2 の暗号化鍵 e_k による暗号文 c_2 と、から生成される暗号文 c は $m_1 + m_2$ の暗号文である。すなわち、 $\text{KeyGen}(\kappa) \rightarrow (e_k, d_k)$ に対し、任意の m_1 と m_2 について、

$$\text{Enc}(e_k, m_1) \rightarrow c_1, \text{Enc}(e_k, m_2) \rightarrow c_2$$

とすると、

$$\text{Dec}(d_k, \text{Hom}(e_k, c_1, c_2)) \rightarrow m_1 + m_2$$

が成り立つ。

[0032] 加法準同型性を有する公開鍵暗号として、楕円曲線 E 上の暗号などが知られている。非特許文献1に開示されている楕円曲線 E 上の暗号の各アルゴリズムは次のように動作する。

[0033] 鍵生成アルゴリズムは、まず、セキュリティパラメータ κ を入力として受け取る。次に、 κ ビットの素数 q をランダムに選び、楕円曲線 E 上の位数が q である群の生成元 G を選ぶ。次に、1 以上 q 未満の整数 x を一様ランダムに選択し、 $H = [x]G$ とする。最後に、暗号化鍵 $e_k = (\kappa, q, E, G, H)$ 及び復号鍵 $d_k = (e_k, x)$ を出力する。

[0034] 暗号化アルゴリズムは、まず、暗号化鍵 $e_k = (\kappa, q, G, g, H)$ 及びメッセージ m を入力として受け取る。次に、1 以上 q 未満の整数 r を一様ランダムに選択し、 $C_a := [r]G$ 、 $C_b := [m]G + [r]H$ とする。最後に、暗号文 $c = (C_a, C_b)$ を出力する。

[0035] 復号アルゴリズムは、まず、復号鍵 $d_k = (e_k, x)$ 及び暗号文 $c = (C_a, C_b)$ を入力として受け取る。次に、 $M' = C_b - [x]C_a$ を計算する。最後に、復号結果 $m' = \text{Dlog}_G(M')$ を出力する。ただし、 Dlog_G は、 $\text{Dlog}_G([x]G) = x$ となる関数である。

[0036] メッセージ m の暗号文 $c = (C_a, C_b) = ([r]G, [m]G + [r]H)$ に対し、楕円 E 上の暗号の復号アルゴリズムにより、暗号文 c を m に正しく復号できることを、次式によって確認できる。

$$M' = C_b - [x] \cdot C_a = ([m] G + [r] H) - [x] \cdot ([r] G) \\ = [m] G + [r] ([x] \cdot G) - [x] \cdot ([r] G) = [m] G$$

[0037] 準同型演算アルゴリズムは、まず、暗号化鍵 $e_k = (\kappa, q, G, g, h)$ 及び第一の暗号文 $c_1 = (C_{1,a}, C_{1,b})$ 及び第二の暗号文 $c_2 = (C_{2,a}, C_{2,b})$ を入力として受け取る。次に、 $C_a = C_{1,a} + C_{2,a}$, $C_b = C_{1,b} + C_{2,b}$ を計算する。最後に、準同型演算結果 $c = (C_a, C_b)$ を出力する。

[0038] メッセージ m_1 の暗号文 ($C_{1,a} = [r] G$, $C_{1,b} = [m_1] G + [r] H$) 及びメッセージ m_2 の暗号文 ($C_{2,a} = [s] G$, $C_{2,b} = [m_2] G + [s] H$) に対し、次の2式が成り立つ。

$$C_a = [r + s] \cdot G$$

$$C_b = [m_1 + m_2] G + [r + s] H$$

したがって、 c は $m_1 + m_2$ の暗号文であり、楕円曲線 $E | \gamma |$ 暗号は加法準同型性を有する。

[0039] 加法準同型暗号を利用した情報照合システムの概要を以下に説明する。

[0040] 情報照合システムでは、入力データは n 次元自然数ベクトルとする (n は自然数)。つまり、入力データを $x = (x_1, x_2, \dots, x_n)$ とする。また、入力データ x と入力データ y の類似度を $\text{sim}(x, y)$ と表す。一般的に、 $\text{sim}(x, y)$ は、両データ x, y の二乗ユークリッド距離、ハミング距離、正規化相関などが用いられる。これらは加法準同型性を用いて、暗号化したまま計算できることが知られている。

[0041] (登録段階)

入力データ $x = (x_1, x_2, \dots, x_n)$ の各 x_i ($i = 1 \sim n$) を加法準同型暗号で暗号化する。すなわち、 $\{\text{Enc}(e_k, x_i)\}$ を生成し、記憶しておく。

[0042] (認証段階)

入力データ $y = (y_1, y_2, \dots, y_n)$ の各 y_i ($i = 1 \sim n$) と、準同型演算 Hom を用いて、 x と y の暗号化類似度 $\text{Enc}(e_k, \text{sim}(x, y))$ を計算する。

[0043] 暗号化類似度 $E_{nc}(e_k, sim(x, y))$ を復号し、類似度を得ることで、認証受理又は不受理の判定を行う。

[0044] ここで、入力データとして生体特徴量を想定すると、多くの生体認証方式では、入力データの空間が予め定められている。すなわち、各 x_i の値は、予め定められた a 以上 b 以下の自然数であり、 x は n 次元ベクトルであることが決められている。例えば、類似度をハミング距離とする生体認証方式では、各 x_i は 0 又は 1 であり、次元数 n は 1024、2048 などと決められている。

[0045] 一方で、加法準同型暗号の平文空間（暗号化できるメッセージの空間）は、セキュリティパラメータにより決められるものであって、入力データの空間と必ずしも一致しない。例えば、類似度をハミング距離とする情報照合システム（例えば生体認証など）では、各 x_i は 0 又は 1 であるが、用いる加法準同型暗号の平文空間は 2048 ビットの素数 q で割った余りの集合であることがしばしば考えられる。

[0046] 入力データの空間と、暗号方式の平文空間が一致しないことを利用した攻撃に対しても安全なシステムが要望されている。一般に、このような攻撃が行われていることを検知することは困難である。

[0047] 前述の例では、類似度としてハミング距離を用いた情報照合システムの場合で説明したが、他の類似度メトリック（例えば、二乗ユークリッド距離や正規化相関など）を用いた場合でも、同様の攻撃が可能であることが知られている。また、前述の例では、加法準同型暗号を用いた場合で説明したが、他の準同型暗号（乗法、Somewhat、完全）や線形マスクを用いた場合でも、同様の攻撃に対して安全であることが望ましい。

[0048] <<2. 本発明の実施形態の概要>>

まず、本発明の実施形態の概要を説明する。

[0049] （1）技術的課題

情報の照合において、登録及び認証のためのデータの一方のデータ空間と、他方のデータ空間が異なる攻撃に対しても安全なシステム等が望ましい。

[0050] (2) 技術的特徴

本発明の実施形態において、例えば、情報照合システムは、登録のための第1入力データの第1コミットメントと、第1入力データが予め定められた入力データ空間に含まれていることを示す第1証明データとを生成する登録データ生成装置と、第1コミットメントと第1証明データの一部又は全部を記憶する認証用データ記憶装置と、第1コミットメントと第1証明データの検証を行う登録データ検証装置と、第1コミットメントと第1証明データの一部又は全部を登録データとして記憶する登録データ記憶装置と、認証されるための第2入力データの第2コミットメントと、第2入力データが予め定められた入力データ空間に含まれていること及び第2入力データと登録データ記憶装置の登録データの類似度が予め定められた受理範囲に含まれていることを示す第2証明データとを生成する認証データ生成装置と、第2コミットメントと第2証明データの検証を行う認証データ検証装置とを備える。

[0051] これにより、情報の照合において、登録及び認証のためのデータの一方向データ空間と、他方のデータ空間が異なる攻撃に対しても安全なシステムが提供される。

[0052] なお、上述した技術的特徴は本発明の実施形態の具体的な一例であり、当然ながら、本発明の実施形態は上述した技術的特徴に限定されない。

[0053] 本発明を実施するための形態について図面を参照して詳細に説明する。尚、各図面及び明細書記載の各実施形態において、同様の構成要素には同一の符号を付与し、説明を適宜省略する。

[0054] <<3. 実施形態>>

<3. 1. システムの構成>

図5は、本実施形態に係る情報照合システム1の一例を示すブロック図である。また、図1は、本実施形態に係る情報照合システム1の具体的な構成を示すブロック図である。

[0055] 例えば、図5に示すように、情報照合システム1は、例えば、登録データ生成装置100と、登録データ検証装置200と、登録データ記憶装置30

０と、認証用データ記憶装置４００と、認証データ生成装置５００と、認証データ検証装置６００を有する。ただし、上記各装置は、別々の装置として実装することも可能であり、一部又は全てを同一の装置内に実装することも可能である。

[0056] また、例えば、登録データ生成装置１００と、認証用データ記憶装置４００と、認証データ生成装置５００は同一のクライアント端末内に実装し、登録データ検証装置２００と、登録データ記憶装置３００と、認証データ検証装置６００は各サーバに分けて実装することもでき、これにより、クライアント・サーバ型の認証システムを実現することが可能である。

[0057] 図６は、本実施形態におけるクライアント端末の一例を示すブロック図である。具体例として図６に示すように、クライアント端末２は、登録データ生成装置１００と、認証用データ記憶装置４００と、認証データ生成装置５００とを有する。

[0058] 図７は、本実施形態におけるサーバの一例を示すブロック図である。図７に示すように、サーバ３は、登録データ検証装置２００と認証データ検証装置６００のうち、いずれか一方又は両方の装置を有する。なお、サーバ３は、登録データ記憶装置３００を含んでもよいし、登録データ記憶装置３００と外部接続されていてもよい。

[0059] なお、情報照合システム１を構成する登録データ生成装置１００、登録データ検証装置２００、登録データ記憶装置３００、認証用データ記憶装置４００、認証データ生成装置５００、及び、認証データ検証装置６００は、それぞれ、登録データ生成部、登録データ検証部、登録データ記憶部、認証用データ記憶部、認証データ生成部、及び、認証データ検証部と称されてもよく、ひとつ又は複数のノード（装置）が、上述の各部のひとつ又は複数をもしてもよい。

[0060] 登録データ生成装置１００は、例えば、コミットメント生成部１０１と、証明生成部１０２と、認証用データ生成部１０３とを有する。コミットメント生成部１０１は、入力データ（第１入力データ）と、パラメータとを入力

し、入力データに基づくコミットメント（第1コミットメント）を生成する。ここで、入力データは、登録するためのデータ（登録データ）であり、例えば生体情報である。ここでの入力データは、本明細書において、第1入力データ又は入力データ $\times$ とも称される。パラメータは、例えばコミットメントを求める際に用いるパラメータである。入力されるパラメータの種類は予め定められることができる。証明生成部102は、入力データと、パラメータと、生成されたコミットメントとを入力し、入力データが予め定められた入力データ空間に含まれていることを示す証明データ（第1証明データ）を生成する。ここでのパラメータは、例えばゼロ知識証明により証明データを生成する際に用いるパラメータである。入力されるパラメータの種類は予め定められることができる。証明データは、例えば後述するゼロ知識証明による求めることができる。認証用データ生成部103は、生成されたコミットメントと、生成された証明データと、登録データ検証装置200の登録データ生成部から受信した、登録データの識別子（ID）とを入力し、認証用データを生成する。認証用データは、例えば、登録データの識別子（ID）と、上述の入力データ（第1入力データ）のコミットメント（第1コミットメント）を生成する際に用いた乱数等を含むことができる。

[0061] 登録データ検証装置200は、例えば、証明検証部201と、登録データ生成部202とを有する。証明検証部201は、パラメータと、登録データ生成装置100から受信したコミットメントと、証明データとを入力し、入力データが入力データ空間に含まれていることを検証する。ここで、パラメータは、例えば、入力データが入力データ空間に含まれていることを検証する際に用いるパラメータである。入力されるパラメータの種類は予め定められることができる。登録データ生成部202は、パラメータと、登録データ生成装置100から受信したコミットメントと、証明データと、検証の結果に基づいて、登録データに対する識別子（ID）と、登録データとを生成する。ここで、入力されるパラメータの種類は予め定められることができる。例えば、登録データとして登録するパラメータでもよい。ここで、登録デー

タは、上述の入力データ（第1入力データ）のコミットメント（第1コミットメント）と証明データ（第1証明データ）の一部又は全部を含むことができる。

[0062] 登録データ記憶装置300は、登録データの識別子（ID）と、登録データとを入力し、それらを対にして（関連づけて）、すなわち（ID、登録データ）を記憶する。

[0063] 認証用データ記憶装置400は、登録データ生成装置100の認証用データ生成部103が生成した認証用データを受信し、認証用データを記憶する。

[0064] 認証データ生成装置500は、例えば、認証要求部501と、コミットメント生成部502と、証明生成部503と、認証データ生成部504とを有する。認証要求部501は、認証用データ記憶装置400から受信（抽出）した認証用データに含まれる識別子（ID）を入力し、識別子（ID）を含む認証要求を生成する。コミットメント生成部502は、認証要求に対して認証データ検証装置600から受信したチャレンジと、パラメータと、認証用データと、入力データ（第2入力データ）とを入力し、コミットメント（第2コミットメント）を生成する。ここで、入力データは、認証を受けるデータであり、登録データと照合されるデータであり、例えば生体情報である。ここでの入力データは、本明細書において、第2入力データ又は入力データyとも称される。証明生成部503は、入力データと、パラメータと、コミットメントとを入力し、入力データが入力データ空間に含まれていること、及び、入力データと登録データとの類似度が予め定められた受理範囲に含まれることを示す証明データ（第2証明データ）を生成する。認証データ生成部504は、コミットメントと、証明データとを入力し、認証データを生成する。

[0065] 認証データ検証装置600は、例えば、チャレンジ生成部601と、証明検証部602と、認証結果生成部603と、を有する。チャレンジ生成部601は、認証データ生成装置500から受信した認証要求を入力する。また

、チャレンジ生成部 601 は、認証要求に含まれる登録データの識別子（ID）に対応した登録データを、登録データ記憶装置 300 から受信（抽出）し、所定のパラメータと、登録データからチャレンジを生成する。証明検証部 602 は、パラメータと、認証データ生成装置 500 から受信した認証データと、チャレンジとを入力する。また、証明検証部 602 は、認証データに含まれる証明データを検証し、検証結果を生成する。認証結果生成部 603 は、検証結果に基づき認証結果を生成する。

[0066] <3. 2. 登録及び照合の動作>

次に、図 2 及び図 3 を参照して、本実施形態における情報照合システム 1 の動作について説明する。図 2 は、入力データの登録の動作を表し、図 3 は、入力データと登録データの照合の動作を表す。なお、本実施形態において、データの送付（送信）及び受信は、各装置間で直接的に送受信されてもよいし、一方の装置が適宜の記憶部にデータを記憶し、他方の装置がデータを読み出すなど間接的な手法でデータを伝達してもよい。

[0067] 初めに、登録の動作を説明する。まず、登録データ生成装置 100 のコミットメント生成部 101 は、上述の入力データとパラメータを取得する（ステップ A1）。なお、パラメータは、セキュリティパラメータ、受理範囲、及び、入力データのとりうる範囲（空間）を含む公開情報であり、その生成手段は特に限定されない。例えば、登録データ検証装置 200 又は認証データ検証装置 600 がパラメータ生成機能を有していてもよいし、情報照合システム 1 の外部で生成してもよい。

[0068] コミットメント生成部 101 は、上述の入力データと、パラメータとを入力し、コミットメントを生成する（ステップ A2）。証明生成部 102 は、上述の入力データと、パラメータと、コミットメントを入力し、入力データが予め定められた入力データ空間に含まれていることを示す証明データを生成し、コミットメントと証明データを登録データ検証装置 200 に送付する（ステップ A3）。

[0069] 登録データ検証装置 200 の証明検証部 201 は、コミットメントと証明

データを登録データ生成装置から受信する（ステップA3）。証明検証部201は、証明データの検証を行う（ステップA4）。例えば、証明検証部201は、所定のパラメータと、コミットメントと、証明データを入力する。証明検証部201は、証明データの検証を行い、検証が失敗（不受理）の場合、処理を停止する。一方、証明検証部201は、検証が成功（受理）の場合、登録データの識別子（ID）を生成し、登録データ生成装置100に送付する。ここで、識別子（ID）は、登録データ固有の識別子であり、生成手段は限定されない。例えば、識別子（ID）の生成の度に増加するカウンタ値であってもよいし、乱数値であってもよい。

[0070] 登録データ生成部202は、コミットメント及び証明データを入力し、登録データを生成する（ステップA5）。登録データ生成部202は、識別子（ID）及び登録データを、登録データ記憶装置300に送付する（ステップA6）。識別子（ID）及び登録データを受信した登録データ記憶装置300は、（ID、登録データ）の対を記憶する（ステップA7）。

[0071] 登録データ生成装置100の認証用データ生成部103は、ステップA4において登録データ検証装置200から送信された識別子（ID）と、コミットメントと、証明データから、認証用データを生成する（ステップA8）。認証用データ生成部103は、認証用データを認証用データ記憶装置400に送付する（ステップA9）。認証用データを受信した認証用データ記憶装置400は、認証用データを記憶する（ステップA10）。

[0072] 次に、照合の動作を、図3を用いて説明する。まず、認証データ生成装置500の認証要求部501は、入力データyと、パラメータとを入力し、さらに認証用データ記憶装置400から認証用データを受信する（ステップB1）。認証要求部501は、入力データyと、パラメータと、認証用データから認証要求を生成し、生成された認証要求を認証データ検証装置600に送付する（ステップB2）。

[0073] 認証データ検証装置600のチャレンジ生成部601は、認証要求に含まれる識別子（ID）に対応した登録データを登録データ記憶装置300から

受信（抽出）し、さらに、パラメータを入力してチャレンジを生成し、チャレンジを認証データ生成装置 500 に送付する（ステップ B 3）。

[0074] 認証データ生成装置 500 のコミットメント生成部 502 は、チャレンジと、入力データ y と、パラメータと、認証用データを入力し、コミットメントを生成する（ステップ B 4）。証明生成部 503 は、コミットメントと、チャレンジと、入力データ y と、パラメータと、認証用データを入力し、入力データ y が予め定められた入力データの空間に含まれることと、及び、入力データ y と登録データ x の類似度が受理範囲に含まれることを示す証明データを生成する（ステップ B 5）。認証データ生成部 504 は、コミットメントと、証明データを入力し、認証データを生成し、認証データを認証データ検証装置 600 に送付する（ステップ B 6）。

[0075] 認証データ検証装置 600 の証明検証部 602 は、認証データと、登録データと、チャレンジと、パラメータを入力し、認証データに含まれる証明データの検証を行い、検証結果を生成する（ステップ B 7）。認証結果生成部 603 は、検証結果を入力し、認証結果を生成し、出力する（ステップ B 8）。

[0076] <3. 3. 実施例 1>

次に、本実施形態における情報照合システム 1 の動作の実施例 1 について説明する。本実施例では、類似度として正規化相関を用いる場合について説明する。入力データは以下の条件を満たすことを仮定する。

[0077] (1) 入力データは n 次元整数ベクトルである。すなわち、 $x = (x_1, x_2, \dots, x_n)$ であり、各 x_i は整数とする。

(2) 各 x_i は a 以上 b 以下の整数とする。すなわち、 $a \leq x_i \leq b$ を満たす。ここで、 a 、 b は予め定められた値であり、例えば整数でもよい。

(3) x は正規化されている。すなわち、すべての入力データ $x = (x_1, x_2, \dots, x_n)$ に対して、 $(x_1)^2 + (x_2)^2 + \dots + (x_n)^2 = A$ (A は 0 以上の定数) を満たす。

(4) 入力データ $x = (x_1, x_2, \dots, x_n)$ と入力データ $y = ($

$y_1, y_2, \dots, y_n$) が認証受理となるならば、 x と y の内積 $\langle x, y \rangle = x_1 y_1 + x_2 y_2 + \dots + x_n y_n$ が受理範囲 Θ に含まれる。

(5) 入力データ $x = (x_1, x_2, \dots, x_n)$ と入力データ $y = (y_1, y_2, \dots, y_n)$ が認証不受理となるならば、 x と y の内積 $\langle x, y \rangle = x_1 y_1 + x_2 y_2 + \dots + x_n y_n$ が受理範囲 Θ に含まれない。

[0078] さらに、本実施例では、Fujisaki-Okamotoコミットメントを利用する。コミットメント (Commit, Open) とは、コミットメントフェーズとオープンフェーズの2つからなるプロトコルである。コミットメントフェーズでは、送信者はある値 v と乱数 r を用いて、コミットメント $\text{Com}(v, r)$ を生成し、受信者に送付する。オープンフェーズでは、送信者は v 及び r を受信者に送ることにより、コミットメント $\text{Com}(v, r)$ をオープンする。ここで、コミットメントは秘匿性及び束縛性を満たすことが望ましい。秘匿性とは、コミットメント $\text{Com}(v, r)$ から v に関する情報が得られないという性質である。束縛性とは、 $\text{Com}(v, r)$ を、 $v' \neq v$ としてオープンすることができない、という性質である。Fujisaki-Okamotoコミットメントは、秘匿性及び束縛性を満たすコミットメント方式であることが知られている。

[0079] Fujisaki-Okamotoコミットメントを説明する。まず、セキュリティパラメータとして k, l, t, s が与えられる。現時点では安全性のために、 k は1024以上、 l は80以上、 t は160以上、 s は80以上の値が推奨されるが、これら以外の値でもよい。また、パラメータとして、 g, h, N が与えられている。ここで N は k ビットの素数 p, q の積である。 g, h はそれぞれ N で割った余りの集合 Z_N からランダムに選ばれた元であり、 $g = h^x \bmod N$ を満たす x や、 $h = g^y \bmod N$ を満たす y は公開されていないこととする。ここで、 g^x は g の x 乗を意味し、 $\bmod N$ は N の剰余を意味する。

[0080] (コミットメントフェーズ)

入力 v とし、 $\text{Com}(v, r) = g^v \cdot h^r \bmod N$ をコミットメン

トとする。

[0081] (オープンフェーズ)

v, r を送付する。

[0082] 次に、本実施例で用いるゼロ知識証明について説明する。まず、ゼロ知識証明とは、ある人（証明者）が他の人（検証者）に、ある命題が真であることを証明する際に、真であること以外の情報を漏らさずに証明する手法をいう。本実施例では、知識のゼロ知識証明、範囲のゼロ知識証明、及び、2乗のゼロ知識証明を用いる。

[0083] 例として、離散対数の知識のゼロ知識証明を説明する。ここで、証明者は $g^x \bmod N$ に対する離散対数 x を知っているものとし、 g^x を知る検証者に x の知識をゼロ知識証明するものとする。 H をハッシュ関数とする。

[0084] (証明段階)

- (1) ランダムに w を $[1, 2^{\{l+t+s\}} - 1]$ から選ぶ。
- (2) $c = H(g^w)$ を計算する。
- (3) $D = w + c \cdot s$ を計算する。
- (4) (c, D) を検証者に送る。

[0085] (検証段階)

- (1) $c = H(g^D \cdot (g^x)^{-c})$ が成り立つことを確認する。成り立っていたら受理、成り立っていなかったら不受理とする。

[0086] 次に、Fujisaki-Okamotoコミットメントを用いた2乗のゼロ知識証明及び範囲のゼロ知識証明を説明する。

[0087] まず、2乗のゼロ知識証明を説明する。証明者は、 $Com(x^2, r) = g^{\{x^2\}} \cdot h^r$ が x の2乗のコミットメントであることを、 $Com(x^2, r)$ を知る検証者にゼロ知識証明する。 H をハッシュ関数とする。

[0088] (証明段階)

- (1) 乱数 r_2 をランダムに $[-2^s \cdot N + 1, 2^s \cdot N - 1]$ から

選び、 $F = \text{Com}(x, r_2) = g^{\{x\}} \cdot h^{\{r_2\}} \bmod N$ を計算する。

(2) $r_3 = r - r_2 \cdot x$ を計算し、 $E = F^x \cdot h^{\{r_3\}} \bmod N$ を計算する。

(3) w を $[1, 2^{\{l+t\}} \cdot N - 1]$ から、 ηF を $[1, 2^{\{l+t+s\}} \cdot N - 1]$ から、 ηE を $[1, 2^{\{l+t+s\}} \cdot N - 1]$ からそれぞれランダムに選び、 $WF = g^{\{w\}} \cdot h^{\{\eta F\}} \bmod N$ 、 $WE = F^{\{w\}} \cdot h^{\{\eta E\}} \bmod N$ を計算する。さらに、 $c = H(WF || WE)$ を計算し、 $D = w + c \cdot x$ 、 $DF = \eta F + c \cdot r_2$ 、 $DE = \eta E + c \cdot r_3$ を計算する。

(4) (F, c, D, DF, DE) を検証者に送付する。

[0089] (検証段階)

(1) $c = H(g^D \cdot h^{\{DF\}} F^{-c} \bmod N || F^{\{D\}} \cdot h^{\{DE\}} \cdot E^{-c} \bmod N)$ を確認する。等号が成り立っていたら受理、成り立っていなかったら不受理とする。

[0090] 次に、範囲のゼロ知識証明を説明する。証明者は $E = \text{Com}(x, r) = g^x \cdot h^r \bmod N$ が $a \leq x \leq b$ のコミットメントであることを、 $\text{Com}(x, r)$ 及び a, b を知る検証者にゼロ知識証明する。なお、 H をハッシュ関数とする。 $\text{floor}(x)$ を x の小数点以下切り捨てを意味する関数とする。

[0091] (証明段階)

(1) x の知識のゼロ知識証明を行う。

(2) $E_1 = E / g^a \bmod N$ と $E_2 = g^b / E \bmod N$ を計算する。また、 $x_1 = x - a$ 、 $x_2 = b - x$ とする。

(3) $x_{11} = \text{floor}(\sqrt{x_1})$ 、 $x_{12} = x_1 - (x_{11})^2$ 、 $x_{21} = \text{floor}(\sqrt{x_2})$ 、 $x_{22} = x_2 - (x_{21})^2$ とする。

(4) r_{11} と r_{21} を $[-2^s \cdot N + 1, 2^s \cdot N - 1]$ から、そ

れぞれランダムに選ぶ。 $r_{12} = r - r_{11}$, $r_{22} = -r - r_{21}$ とする。

(5) $E_{11} = \text{Com}((x_{11})^2, r_{11})$ 、 $E_{12} = \text{Com}(x_{12}, r_{12})$ 、 $E_{21} = \text{Com}((x_{21})^2, r_{21})$ 、 $E_{22} = \text{Com}((x_{22})^2, r_{22})$ とする。

(6) E_{11} , E_{21} を検証者に送る。検証者は、 $E_{12} = E_1 / E_{11}$ 、 $E_{22} = E_2 / E_{21}$ を計算する。

(7) E_{11} と E_{21} がそれぞれ x_{11} , x_{21} の二乗であることを、二乗のゼロ知識証明を用いて証明する。

(8) w_1, w_2 を $[0, 2^{\{t+1\}} \cdot 2^{\sqrt{b-a}}]$ 、 η_1, η_2 を $[-2^{\{t+1+s\}N+1}, 2^{\{t+1+s\}N-1}]$ からランダムに選ぶ。 $W_1 = g^{\{w_1\}} \cdot h^{\{\eta_1\}} \bmod N$, $W_2 = g^{\{w_2\}} \cdot h^{\{\eta_2\}} \bmod N$ を計算する。

(9) $c = H(W_1, W_2)$ を計算する。

(10) $D_{11} = w_1 + x_{12} \cdot c$, $D_{12} = \eta_1 + r_{12} \cdot c$, $D_{21} = W_2 + x_{22} \cdot c$, $D_{22} = \eta_2 + r_{22} \cdot c$ を計算し、 $(c, D_{11}, D_{12}, D_{21}, D_{22})$ を検証者に送付する。

[0092] (検証段階)

(1) 証明のステップ1における知識のゼロ知識証明及びステップ7における二乗のゼロ知識証明をそれぞれ検証する。1つでも不受理があれば、検証の処理を停止する。

(2) $c = H(g^{\{D_{11}\}} \cdot h^{\{D_{12}\}} \cdot E_{12}^{\{-c\}}, g^{\{D_{21}\}} \cdot h^{\{D_{22}\}} \cdot E_{22}^{\{-c\}})$ が成立することを確認する。等号が成り立っていたら受理の検証結果、成り立っていなかったら不受理の検証結果を出力する。

[0093] 次に、本実施例の情報照合システム1の登録の動作について説明する。まず、登録データ生成装置100は、入力として、パラメータと入力データ $x = (x_1, x_2, \dots, x_n)$ を受け取る(ステップA1)。

[0094] コミットメント生成部101は、 $i = 1, \dots, n$ に対して、以下の処理を行う。

(1) $E_i = \text{Com}(x_i, r_i)$, $F_i = \text{Com}((x_i)^2, r'_i)$ を生成する(ステップA2)。すなわち、入力データに基づくコミットメントを生成する。ここで、 r_i は、ステップA1で入力されたパラメータに含まれてもよい。

[0095] 証明生成部102は、 $i = 1, \dots, n$ に対して、以下の処理を行う(ステップA3)。

(1) 次の4つのゼロ知識証明を行う。(1) E_i を用いて、 x_i の知識証明、(2) E_i を用いて、 $a \leq x_i \leq b$ であることのゼロ知識証明、(3) F_i を用いて、 x_i の二乗のゼロ知識証明。

(2) さらに、 $F_1, \dots, F_n$ を用いて、(4) $\sum (x_i)^2 = (x_1)^2 + (x_2)^2 + \dots + (x_n)^2 = A$ であることのゼロ知識証明を生成する。これは $F_1 \cdot F_2 \cdot \dots \cdot F_n = g^{\{\sum (x_i)^2\}} \cdot h^{\{\sum (r'_i)\}}$ であるため、 $F_1 \cdot F_2 \cdot \dots \cdot F_n / g^A = h^{\{\sum (r'_i)\}}$ となり、 $\sum (r'_i)$ の知識のゼロ知識証明を用いて実現できる。

[0096] 証明生成部102は、コミットメントと証明データを、登録データ検証装置200に送付する(ステップA3)。

[0097] コミットメントと証明データを受信した登録データ検証装置200の証明検証部201は、上述の(1)から(3)のゼロ知識証明の検証を行う。1つでも検証不受理であれば検証の処理を停止する。一方、すべて検証受理であれば、証明検証部201は、登録データの識別子(ID)を生成し、識別子(ID)を登録データ生成装置100に送付する(ステップA4)。

[0098] 登録データ生成部202は、コミットメント $\{E_i\}$ を登録データとする(ステップA5)。登録データ生成部202は、識別子(ID)と登録データの対(ID, 登録データ)を登録データ記憶装置300に送付する(ステップA6)。登録データ記憶装置300は、(ID, 登録データ)を記憶する(ステップA7)。

[0099] ステップA4において識別子（ID）を受信した登録データ生成装置100の認証用データ生成部103は、（ID， {r_i}）を認証用データとして生成する（ステップA8）。認証用データ生成部103は、（認証用データを認証用データ記憶装置400に送付する（ステップA9）。認証用データ記憶装置400は、認証用データを記憶する（ステップA10）。

[0100] 次に、本実施例の情報照合システム1の照合の動作について説明する。まず、認証データ生成装置500の認証要求部501は、入力データ $y = (y_1, y_2, \dots, y_n)$ と、パラメータとを入力として受け取り、認証用データ記憶装置400から認証用データ（ID， {r_i}）を受信（抽出）する（ステップB1）。一例として、入力データ y とともにログインID又はユーザの識別番号等を入力し、これらに関連づけられて記憶された認証用データを読み出してもよい。

[0101] 認証要求部501は、認証要求として、登録データの識別子（ID）を含むRequestを認証データ検証装置600に送付する（ステップB2）。

[0102] チャレンジ生成部601は、識別子（ID）に対応する登録データ（ID， {E_i}）を登録データ記憶装置300から受信（抽出）し、ランダムな値 c を用いて、{（E_i）^c， h^c }をチャレンジとし、チャレンジを認証データ生成装置500に送付する（ステップB3）。

[0103] 認証データ生成装置500のコミットメント生成部502は、各 $i = 1, 2, \dots, n$ に対して、以下の処理を行う。

(1) $Com(y_i, R_i) = g^{\{y_i\}} \cdot h^{\{R_i\}} \bmod N$ 、
 $Com((y_i)^2, R'_i) = g^{\{(y_i)^2\}} \cdot h^{\{R'_i\}} \bmod N$ 、
 $Com(x_i y_i, R''_i) = ((E_i)^c)^{\{y_i\}} \cdot h^{\{R''_i\}} \bmod N$ を計算する（ステップB4）

[0104] 証明生成部503は、各 $i = 1, 2, \dots, n$ に対して以下の処理を行う。

(1) (1) $Com(y_i, R_i)$ を用いて、 y_i の知識のゼロ知識証明、
 (2) $Com(y_i, R_i)$ を用いて、 $a \leq y_i \leq b$ の範囲のゼロ知識証

明, $(3) \text{Com}((y_i)^2, R'_i)$ を用いて、 y_i の二乗のゼロ知識証明。

(2) 次に、 $(4) \sum (y_i)^2 = (y_1)^2 + (y_2)^2 + \dots + (y_n)^2 = A$ であることのゼロ知識証明を生成する。これは登録の時と同様の方法で実現できる。

(3) 次に、 $\text{Com}(x_i y_i, R''_i)$ を用いて、 $(5) \langle x, y \rangle$ が受理範囲 Θ に含まれることのゼロ知識証明を生成する。これも登録の時と同様の方法で実現できる。すなわち、 $\text{Com}(x_1 y_1, R''_1) \cdot \text{Com}(x_2 y_2, R''_2) \cdot \dots \cdot \text{Com}(x_n y_n, R''_n) = g^{\{c \langle x, y \rangle\}} (h^{\{c\}})^{\{\sum (y_i \cdot r_i) + \sum (R''_i)\}}$ であるため、 h^c に対して、 $\sum (y_i \cdot r_i) + \sum (R''_i)$ の知識のゼロ知識証明を生成する (ステップ B5)。

[0105] 認証データ生成部 504 は、コミットメントと (1) から (5) の証明を証明データとして、認証データ検証装置 600 に送付する (ステップ B6)。

[0106] 証明検証部 602 は、(1) から (5) の証明を検証し、すべてが受理であれば検証結果を受理にし、そうでなければ検証結果を不受理にする (ステップ B7)。ここで、(4) の検証は、 $\text{Com}((y_1)^2, R'_1) \cdot \text{Com}((y_2)^2, R'_2) \cdot \dots \cdot \text{Com}((y_n)^2, R'_n) = g^{\{\sum (y_i)^2\}} \cdot h^{\{\sum (R'_i)\}} \bmod N$ であるため、 $\text{Com}((y_1)^2, R'_1) \cdot \text{Com}((y_2)^2, R'_2) \cdot \dots \cdot \text{Com}((y_n)^2, R'_n) / g^{\{A\}}$ として、ゼロ知識証明の検証を行うことにより実現できる。同様にして (5) の検証は、受理範囲 Θ に含まれる値 θ に対して、 $\text{Com}(x_1 y_1, R''_1) \cdot \text{Com}(x_2 y_2, R''_2) \cdot \dots \cdot \text{Com}(x_n y_n, R''_n) / g^{\{c \theta\}}$ として、ゼロ知識証明の検証を行うことにより実現できる。

[0107] 認証結果生成部 603 は、検証結果が受理であれば、認証結果を受理とし、そうでなければ認証結果を不受理とする (ステップ B8)。

[0108] なお、本実施例の説明では、 x 、 y のすべての次元に対して、 x_i （又は y_i ）が $a \leq x_i \leq b$ であることを証明しているが、その一部（例えば半分など）を証明するのでもよい。証明させる次元の選び方は限定されない。例えば、証明させる次元を登録データ検証装置200又は認証データ検証装置600がランダムに選んでもよい。

[0109] また、本実施例の説明では、各ゼロ知識証明を独立に行うように説明しているが、並列に実行する際によく知られた効率化を行ってもよい。例えば、各ゼロ知識証明の中でハッシュ関数の計算を行っているが、それを1度に合わせて計算してもよい。同様に、各ゼロ知識証明の中で x_i 又は y_i に関する知識の証明を行っているが、それを1度にまとめてしまっても構わない。

[0110] さらに、本実施例の説明では、登録データ生成装置100及び認証データ生成装置500がハッシュ関数を用いて c を計算しているが、それを登録データ検証装置200及び認証データ検証装置600が生成した乱数値 c と置き換えてもよい。このとき検証時に確認する式は、ハッシュ値の一致を確認するのではなく、 c に係する計算結果の一致を確認するものと変わる。

[0111] なお、本実施例の説明では、入力データが入力データの空間に含まれることや、入力データと登録データの類似度が受理範囲に含まれることを、それぞれゼロ知識証明を用いて証明しているが、すべてを秘匿する必要のない場合は、コミットメントのオープンを実行してもよい。例えば入力データの各次元の値の二乗和が定数 A であることは、コミットメントに用いられた乱数を明らかにすることでも容易に検証できる。

[0112] <3. 4. 実施例2>

次に、本実施形態における情報照合システム1の動作の実施例2について説明する。

[0113] 本実施例では、類似度として二乗ユークリッド距離を用いる場合について説明する。入力データは以下の条件を満たすことを仮定する。

(1) 入力データは n 次元整数ベクトルである。すなわち、 $x = (x_1, x_2, \dots, x_n)$ であり、各 x_i は整数とする。

(2) 各 x_i は a 以上 b 以下の整数とする。すなわち、 $a \leq x_i \leq b$ を満たす。

(3) 入力データ $x = (x_1, x_2, \dots, x_n)$ と入力データ $y = (y_1, y_2, \dots, y_n)$ が認証受理となるならば、 x と y のユークリッド距離の二乗 $d(x, y) = (x_1 - y_1)^2 + (x_2 - y_2)^2 + \dots + (x_n - y_n)^2$ が受理範囲 Θ に含まれる。

(4) 入力データ $x = (x_1, x_2, \dots, x_n)$ と入力データ $y = (y_1, y_2, \dots, y_n)$ が認証不受理となるならば、 x と y のユークリッド距離の二乗 $d(x, y) = (x_1 - y_1)^2 + (x_2 - y_2)^2 + \dots + (x_n - y_n)^2$ が受理範囲 Θ に含まれない。

[0114] 次に、本実施例の情報照合システム 1 の登録の動作について説明する。まず、登録データ生成装置 100 は、入力として、パラメータと入力データ $x = (x_1, x_2, \dots, x_n)$ を受け取る（ステップ A1）。

[0115] コミットメント生成部 101 は、 $i = 1, \dots, n$ に対して、以下の処理を行う。すなわち、 $E_i = \text{Com}(x_i, r_i)$ 、 $F_i = \text{Com}((x_i)^2, r'_i)$ を生成する（ステップ A2）。

[0116] 証明生成部 102 は、 $i = 1, \dots, n$ に対して、以下の処理を行う（ステップ A3）。すなわち、次の 3 つのゼロ知識証明を行う。（1） E_i を用いて、 x_i の知識証明、（2） E_i を用いて、 $a \leq x_i \leq b$ であることのゼロ知識証明、（3） F_i を用いて、 x_i の二乗のゼロ知識証明。

[0117] 証明生成部 102 は、コミットメントと証明データを登録データ検証装置 200 に送付する（ステップ A3）。

[0118] コミットメントと証明データを受信した登録データ検証装置 200 の証明検証部 201 は、上述の（1）から（3）のゼロ知識証明の検証を行う。証明検証部 201 は、1 つでも検証不受理であれば検証の処理を停止する。一方、すべて検証受理であれば、証明検証部 201 は、登録データの識別子（ID）を生成し、識別子（ID）を登録データ生成装置 100 に送付する（ステップ A4）。

[0119] 登録データ生成部202は、 $(\{E_i\}, F = F_1 \cdot F_2 \cdot \dots \cdot F_n)$ を登録データとする(ステップA5)。登録データ生成部202は、識別子(ID)と登録データの対(ID, 登録データ)を登録データ記憶装置300に送付する(ステップA6)。登録データ記憶装置300は、(ID, 登録データ)を記憶する(ステップA7)。

[0120] ステップA4において識別子(ID)を受信した登録データ生成装置100の認証用データ生成部103は、 $(ID, \{r_i\}, r' = \sum (r'_i))$ を認証用データとして生成する(ステップA8)。認証用データ生成部103は、認証用データを認証用データ記憶装置400に送付する(ステップA9)。認証用データ記憶装置400は、認証用データを記憶する(ステップA10)。

[0121] 次に、本実施例の情報照合システム1の照合の動作について説明する。まず、認証データ生成装置500の認証要求部501は、入力データ $y = (y_1, y_2, \dots, y_n)$ と、パラメータとを入力として受け取り、認証用データ記憶装置400から認証用データ(ID, $\{r_i\}, r')$ を受信(抽出)する(ステップB1)。一例として、入力データ y とともにログインID又はユーザの識別番号等を入力し、これらに関連づけられて記憶された認証用データを読み出してもよい。

[0122] 認証要求部501は、認証要求として、登録データの識別子(ID)を含むRequestを認証データ検証装置600に送付する(ステップB2)。

[0123] チャレンジ生成部601は、識別子(ID)に対応する登録データ(ID, $\{E_i\}, F)$ を登録データ記憶装置300から受信(抽出)し、ランダムな値 c を用いて、 $\{(E_i)^c\}, h^c$ をチャレンジとし、チャレンジを認証データ生成装置500に送付する(ステップB3)。

[0124] 認証データ生成装置500のコミットメント生成部502は、各 $i = 1, 2, \dots, n$ に対して、以下の処理を行う。

$$(1) \quad \text{Com}(y_i, R_i) = g^{\{y_i\}} \cdot h^{\{R_i\}} \bmod N,$$

$\text{Com}((y_i)^2, R'_i) = g^{\{(y_i)^2\}} \cdot h^{\{R'_i\}} \bmod N$ 、 $\text{Com}(x_i y_i, R''_i) = ((E_i)^c)^{\{y_i\}} \cdot h^{\{R''_i\}} \bmod N$ を計算する（ステップB4）。

(2) 次に、証明生成部503は、各 $i = 1, 2, \dots, n$ に対して以下の処理を行う。

(3) (1) $\text{Com}(y_i, R_i)$ を用いて、 y_i の知識のゼロ知識証明、(2) $\text{Com}(y_i, R_i)$ を用いて、 $a \leq y_i \leq b$ の範囲のゼロ知識証明、(3) $\text{Com}((y_i)^2, R'_i)$ を用いて、 y_i の二乗のゼロ知識証明。

(4) 次に、 $\text{Com}(x_i y_i, R''_i)$ と、 $\text{Com}((y_i)^2, R'_i)$ と、 $\{r_i\}$ と、 r' を用いて、(4) $d(x, y)$ が受理範囲 Θ に含まれることのゼロ知識証明を生成する。これは、 $\text{Com}(\sum((x_i)^2), r') \cdot \text{Com}((y_1)^2, R'_1) \cdot \dots \cdot \text{Com}((y_n)^2, R'_n) \cdot (\text{Com}(x_1 y_1, R''_1) \cdot \text{Com}(x_2 y_2, R''_2) \cdot \dots \cdot \text{Com}(x_n y_n, R''_n))^{\{-2/c\}} = g^{\{\sum(x_i)^2 + \sum(y_i)^2 - 2\langle x, y \rangle\}} (h)^{\{r' + \sum(R'_i) + \sum(y_i \cdot r_i) + \sum(R''_i)\}}$ であるため、 h に対して、 $r' + \sum(R'_i) + \sum(y_i \cdot r_i) + \sum(R''_i)$ の知識のゼロ知識証明を生成する（ステップB5）。

[0125] 認証データ生成部504は、コミットメントと(1)から(4)の証明を証明データとして、認証データ検証装置600に送付する（ステップB6）。

[0126] 証明検証部602は、(1)から(4)の証明を検証し、すべてが受理であれば検証結果を受理にし、そうでなければ検証結果を不受理にする（ステップB7）。

[0127] 認証結果生成部603は、検証結果が受理であれば、認証結果を受理とし、そうでなければ認証結果を不受理とする（ステップB8）。

[0128] 本実施例の説明では、 x 、 y のすべての次元に対して、 x_i (又は y_i)

が $a \leq x_i \leq b$ であることを証明しているが、その一部（例えば半分など）を証明するのでもよい。証明させる次元の選び方は問わない。例えば、証明させる次元を登録データ検証装置 200 又は認証データ検証装置 600 がランダムに選んでもよい。

[0129] また、本実施例の説明では、各ゼロ知識証明を独立に行うように説明しているが、並列に実行する際によく知られた効率化を行ってもよい。例えば、各ゼロ知識証明の中でハッシュ関数の計算を行っているが、それを 1 度に合わせて計算してもよい。同様に、各ゼロ知識証明の中で x_i 又は y_i に関する知識の証明を行っているが、それを 1 度にまとめてしまっても構わない。

[0130] さらに、本実施例の説明では、登録データ生成装置 100 及び認証データ生成装置 500 がハッシュ関数を用いて c を計算しているが、それを登録データ検証装置 200 及び認証データ検証装置 600 が生成した乱数値 c と置き換えてもよい。このとき検証時に確認する式は、ハッシュ値の一致を確認するのではなく、 c に関係する計算結果の一致を確認するものと変わる。

[0131] なお、本実施例の説明では、入力データが入力データの空間に含まれることや、入力データと登録データの類似度が受理範囲に含まれることを、それぞれゼロ知識証明を用いて証明しているが、すべてを秘匿する必要のない場合は、コミットメントのオープンを実行してもよい。

[0132] （効果）

上述した本実施形態における効果のひとつは、生体から生成されていないデータを入力データとして、登録データを生成することや、認証データを生成することを不可能にしていることである。また、これにより、より安全な情報照合システム 1 を実現することが可能になる。また、例えば、ステップ A2 及び A3 によって、入力データが予め定められた入力データの空間にあることをゼロ知識証明を用いて検証できる。

[0133] 上述した本実施形態では、登録データは $Fujisaki-Okamoto$ コミットメントのコミットメントと識別子 (ID) である。 $Fujisaki-Okamoto$ コミットメントは情報理論的な秘匿性を満たすことが

知られており、生体特徴量のコミットメントは乱数と見分けがつかないことが数学的に示されている。したがって、万が一コミットメントが漏洩したとしても、生体特徴量は漏洩しない。また、認証用データは、コミットメント生成時に使用した乱数と識別子IDである。明かに、認証用データから生体特徴量に関する情報は漏洩しない。

[0134] <<4. その他>>

図4は、装置のハードウェア構成を示すブロック図である。上述の各装置は、物理的に以下の構成を有することができる。装置10は、例えば、入力部11と、出力部12と、記憶部13と、処理部14とを有する。

[0135] 入力部11は、データ、情報、信号等を入力する。入力部11は、例えば、他の装置からデータ等を受信するインターフェース、ユーザからの入力を受け付ける操作部、生体情報を読み取る読取装置などでもよい。出力部12は、データ、情報、信号等を入力する。出力部12は、例えば、他の装置へデータ等を送信するインターフェース、画面を表示する表示部などでもよい。記憶部13は、装置10の動作のためのプログラム及びパラメータ、並びに様々なデータを、一時的に又は恒久的に記憶する。処理部14は、例えば、CPU (Central Processing Unit) などの1つ以上のプロセッサで構成される。処理部14は、例えば記憶部13に記憶されたプログラムを実行して、上述の各装置の動作を行ってもよい。プログラムは、上述の各装置の動作をプロセッサに実行させるためのプログラムであってもよい。

[0136] 上記実施形態の一部又は全部は、以下の付記のようにも記載され得るが、以下には限られない。

[0137] (付記1)

登録のための第1入力データの第1コミットメントと、第1入力データが予め定められた入力データ空間に含まれていることを示す第1証明データとを生成する登録データ生成装置と、

前記第1コミットメントと前記第1証明データの一部又は全部を記憶する

認証用データ記憶装置と、

前記第 1 コミットメントと前記第 1 証明データの検証を行う登録データ検証装置と、

前記第 1 コミットメントと前記第 1 証明データの一部又は全部を登録データとして記憶する登録データ記憶装置と、

認証されるための第 2 入力データの第 2 コミットメントと、前記第 2 入力データが前記予め定められた入力データ空間に含まれていること及び前記第 2 入力データと前記登録データ記憶装置の前記登録データの類似度が予め定められた受理範囲に含まれていることを示す第 2 証明データとを生成する認証データ生成装置と、

前記第 2 コミットメントと前記第 2 証明データの検証を行う認証データ検証装置と

を備えた情報照合システム。

[0138] (付記 2)

付記 1 に記載の情報照合システムであって、

前記登録データ生成装置が生成する第 1 証明データの一部又は全部が、ゼロ知識証明によるデータである

ことを特徴とする情報照合システム。

[0139] (付記 3)

付記 1 又は 2 に記載の情報照合システムであって、

前記認証データ生成装置が生成する前記第 2 証明データの一部又は全部が、ゼロ知識証明によるデータである

ことを特徴とする情報照合システム。

[0140] (付記 4)

付記 1 ～ 3 のいずれか 1 項に記載の情報照合システムであって、

前記登録データ記憶装置に記憶された前記登録データが、前記第 1 入力データの第 1 コミットメントを含む

ことを特徴とする情報照合システム。

[0141] (付記5)

付記1～4のいずれか1項に記載の情報照合システムであって、
前記認証用データ記憶装置に記憶された認証用データが、前記第1入力データの前記第1コミットメントを生成する際に用いた乱数を含む
ことを特徴とする情報照合システム。

[0142] (付記6)

付記1～5のいずれか1項に記載の情報照合システムであって、
前記登録データ生成装置が生成する前記第1コミットメントの一部又は全部が、パラメータ g 、 h 、 N 、前記第1入力データ x 、乱数 r に対して、 $g^x \cdot h^r \bmod N$ である
ことを特徴とする情報照合システム。

[0143] (付記7)

付記1～6のいずれか1項に記載の情報照合システムであって、
前記認証データ生成装置が生成する前記第2コミットメントの一部又は全部が、パラメータ g 、 h 、 N 、前記第2入力データ y 、乱数 r に対して、 $g^y \cdot h^r \bmod N$ である
ことを特徴とする情報照合システム。

[0144] (付記8) 登録のための第1入力データの第1コミットメントと、前記第1入力データが予め定められた入力データ空間に含まれていることを示す第1証明データとを含む登録データを生成する登録データ生成部と、

前記第1コミットメントと前記第1証明データの一部又は全部を記憶する
認証用データ記憶部と、

認証されるための第2入力データの第2コミットメントと、前記第2入力データが前記予め定められた入力データ空間に含まれていること及び前記第2入力データと前記登録データの類似度が予め定められた受理範囲に含まれていることを示す第2証明データとを生成する認証データ生成部と
を備えたクライアント端末。

[0145] (付記9)

登録のための第1入力データの第1コミットメントと、前記第1入力データが予め定められた入力データ空間に含まれていることを示す第1証明データとを入力し、前記第1コミットメントと前記第1証明データの検証を行う登録データ検証部と、

認証されるための第2入力データの第2コミットメントと、前記第2入力データが前記予め定められた入力データ空間に含まれていること及び前記第2入力データと登録データ記憶部の登録データの類似度が予め定められた受理範囲に含まれていることを示す第2証明データとを入力し、前記第2コミットメントと前記第2証明データの検証を行う認証データ検証部との少なくとも一方を備えたサーバ。

[0146] (付記10)

登録のための第1入力データの第1コミットメントと、第1入力データが予め定められた入力データ空間に含まれていることを示す第1証明データとを生成する登録データ生成処理と、

前記第1コミットメントと前記第1証明データの一部又は全部を記憶する認証用データ記憶処理と、

前記第1コミットメントと前記第1証明データの検証を行う登録データ検証処理と、

前記第1コミットメントと前記第1証明データの一部又は全部を登録データとして記憶する登録データ記憶処理と、

認証されるための第2入力データの第2コミットメントと、前記第2入力データが前記予め定められた入力データ空間に含まれていること及び前記第2入力データと登録データ記憶部の前記登録データの類似度が予め定められた受理範囲に含まれていることを示す第2証明データとを生成する認証データ生成処理と、

前記第2コミットメントと前記第2証明データの検証を行う認証データ検証処理と

を含む情報照合方法。

[0147] (付記 1 1)

登録のための第 1 入力データの第 1 コミットメントと、第 1 入力データが予め定められた入力データ空間に含まれていることを示す第 1 証明データとを生成する登録データ生成処理と、

前記第 1 コミットメントと前記第 1 証明データの一部又は全部を記憶する認証用データ記憶処理と、

前記第 1 コミットメントと前記第 1 証明データの検証を行う登録データ検証処理と、

前記第 1 コミットメントと前記第 1 証明データの一部又は全部を登録データとして記憶する登録データ記憶処理と、

認証されるための第 2 入力データの第 2 コミットメントと、前記第 2 入力データが前記予め定められた入力データ空間に含まれていること及び前記第 2 入力データと登録データ記憶部の前記登録データの類似度が予め定められた受理範囲に含まれていることを示す第 2 証明データとを生成する認証データ生成処理と、

前記第 2 コミットメントと前記第 2 証明データの検証を行う認証データ検証処理と

をコンピュータに実行させる情報照合プログラム。

産業上の利用可能性

[0148] 前述の通り、各実施形態の技術により、カメラ等のセンサで取得した生体情報と、データベースに保存されている一人又は複数人の生体情報とを、両者の持つ生体情報を互いに秘匿したまま、安全に照合することが可能である。センサの管理者（組織）と、データベースの管理者（組織）が異なる場合に、効果的である。

[0149] 各実施形態の技術は例えば、スマートフォン等を用いてリモートのサーバに対して生体認証を行う際に利用可能である。ユーザ自身が保持するスマートフォンに認証用データを、サーバに登録データをそれぞれ登録し、認証を行う際にスマートフォンで生体情報を採取し、記憶している認証用データを

用いて、認証データの生成を行い、サーバがユーザを認証することが可能となる。

[0150] スマートフォンを用いたりモート生体認証の利用例として、ネットショッピングや会員サービスの利用などが挙げられる。本技術を用いれば、サーバはユーザの生体情報に関して、同一生体であるか否か以外の情報を得ることなく、スマートフォンの生体認証機能を用いてユーザ認証を行うことが可能である。したがって、サーバからのユーザ情報の漏洩リスクを低減できる。

符号の説明

[0151]	1 0 0	登録データ生成装置（登録データ生成部）
	2 0 0	登録データ検証装置（登録データ検証部）
	3 0 0	登録データ記憶装置（登録データ記憶部）
	4 0 0	認証用データ記憶装置（認証用データ記憶部）
	5 0 0	認証データ生成装置（認証データ生成部）
	6 0 0	認証データ検証装置（認証データ検証部）

請求の範囲

- [請求項1] 登録のための第1入力データの第1コミットメントと、前記第1入力データが予め定められた入力データ空間に含まれていることを示す第1証明データとを生成する登録データ生成装置と、
- 前記第1コミットメントと前記第1証明データの一部又は全部を記憶する認証用データ記憶装置と、
- 前記第1コミットメントと前記第1証明データの検証を行う登録データ検証装置と、
- 前記第1コミットメントと前記第1証明データの一部又は全部を登録データとして記憶する登録データ記憶装置と、
- 認証されるための第2入力データの第2コミットメントと、前記第2入力データが前記予め定められた入力データ空間に含まれていること及び前記第2入力データと前記登録データ記憶装置の前記登録データの類似度が予め定められた受理範囲に含まれていることを示す第2証明データとを生成する認証データ生成装置と、
- 前記第2コミットメントと前記第2証明データの検証を行う認証データ検証装置と
- を備えた情報照合システム。
- [請求項2] 請求項1に記載の情報照合システムであって、
- 前記登録データ生成装置が生成する前記第1証明データの一部又は全部が、ゼロ知識証明によるデータである
- ことを特徴とする情報照合システム。
- [請求項3] 請求項1に記載の情報照合システムであって、
- 前記認証データ生成装置が生成する前記第2証明データの一部又は全部が、ゼロ知識証明によるデータである
- ことを特徴とする情報照合システム。
- [請求項4] 請求項1に記載の情報照合システムであって、
- 前記登録データ記憶装置に記憶された前記登録データが、前記第1

入力データの前記第1コミットメントを含む

ことを特徴とする情報照合システム。

[請求項5]

請求項1に記載の情報照合システムであって、

前記認証用データ記憶装置に記憶された認証用データが、前記第1入力データの前記第1コミットメントを生成する際に用いた乱数を含む

ことを特徴とする情報照合システム。

[請求項6]

請求項1に記載の情報照合システムであって、

前記登録データ生成装置が生成する前記第1コミットメントの一部又は全部が、パラメータ g 、 h 、 N 、前記第1入力データ x 、乱数 r に対して、 $g^x \cdot h^r \bmod N$ である

ことを特徴とする情報照合システム。

[請求項7]

請求項1に記載の情報照合システムであって、

前記認証データ生成装置が生成する前記第2コミットメントの一部又は全部が、パラメータ g 、 h 、 N 、前記第2入力データ y 、乱数 r に対して、 $g^y \cdot h^r \bmod N$ である

ことを特徴とする情報照合システム。

[請求項8]

登録のための第1入力データの第1コミットメントと、前記第1入力データが予め定められた入力データ空間に含まれていることを示す第1証明データとを含む登録データを生成する登録データ生成部と、

前記第1コミットメントと前記第1証明データの一部又は全部を記憶する認証用データ記憶部と、

認証されるための第2入力データの第2コミットメントと、前記第2入力データが前記予め定められた入力データ空間に含まれていること及び前記第2入力データと前記登録データの類似度が予め定められた受理範囲に含まれていることを示す第2証明データとを生成する認証データ生成部と

を備えたクライアント端末。

[請求項9] 登録のための第1入力データの第1コミットメントと、前記第1入力データが予め定められた入力データ空間に含まれていることを示す第1証明データとを入力し、前記第1コミットメントと前記第1証明データの検証を行う登録データ検証部と、

 認証されるための第2入力データの第2コミットメントと、前記第2入力データが前記予め定められた入力データ空間に含まれていること及び前記第2入力データと登録データ記憶部の登録データの類似度が予め定められた受理範囲に含まれていることを示す第2証明データとを入力し、前記第2コミットメントと前記第2証明データの検証を行う認証データ検証部と

の少なくとも一方を備えたサーバ。

[請求項10] 登録のための第1入力データの第1コミットメントと、前記第1入力データが予め定められた入力データ空間に含まれていることを示す第1証明データとを生成する登録データ生成処理と、

 前記第1コミットメントと前記第1証明データの一部又は全部を記憶する認証用データ記憶処理と、

 前記第1コミットメントと前記第1証明データの検証を行う登録データ検証処理と、

 前記第1コミットメントと前記第1証明データの一部又は全部を登録データとして記憶する登録データ記憶処理と、

 認証されるための第2入力データの第2コミットメントと、前記第2入力データが前記予め定められた入力データ空間に含まれていること及び前記第2入力データと登録データ記憶部の前記登録データの類似度が予め定められた受理範囲に含まれていることを示す第2証明データとを生成する認証データ生成処理と、

 前記第2コミットメントと前記第2証明データの検証を行う認証データ検証処理と

を含む情報照合方法。

[請求項11] 登録のための第1入力データの第1コミットメントと、前記第1入力データが予め定められた入力データ空間に含まれていることを示す第1証明データとを生成する登録データ生成処理と、

 前記第1コミットメントと前記第1証明データの一部又は全部を記憶する認証用データ記憶処理と、

 前記第1コミットメントと前記第1証明データの検証を行う登録データ検証処理と、

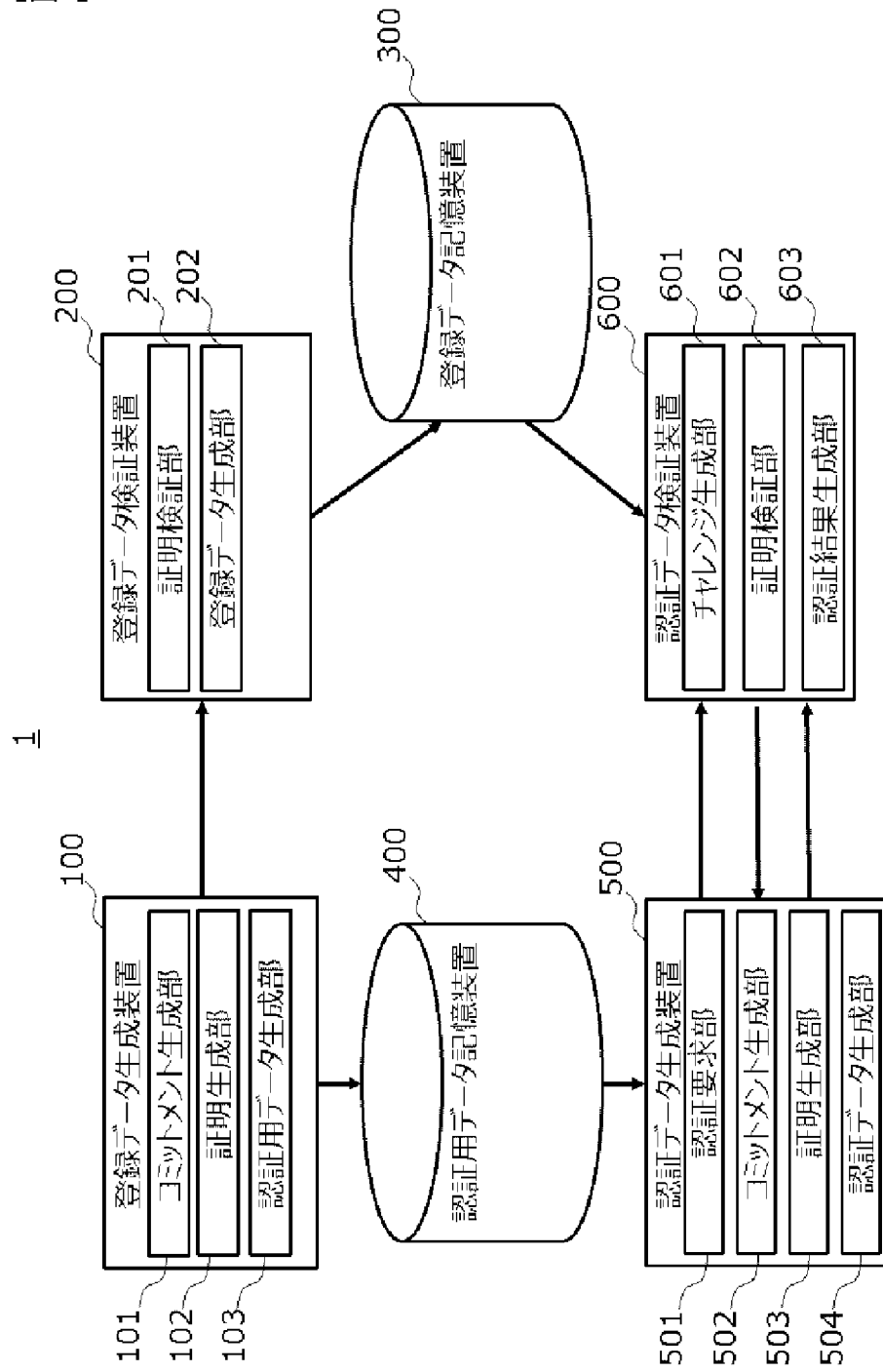
 前記第1コミットメントと前記第1証明データの一部又は全部を登録データとして記憶する登録データ記憶処理と、

 認証されるための第2入力データの第2コミットメントと、前記第2入力データが前記予め定められた入力データ空間に含まれていること及び前記第2入力データと登録データ記憶部の前記登録データの類似度が予め定められた受理範囲に含まれていることを示す第2証明データとを生成する認証データ生成処理と、

 前記第2コミットメントと前記第2証明データの検証を行う認証データ検証処理と

 をコンピュータに実行させる情報照合プログラム。

[図1]



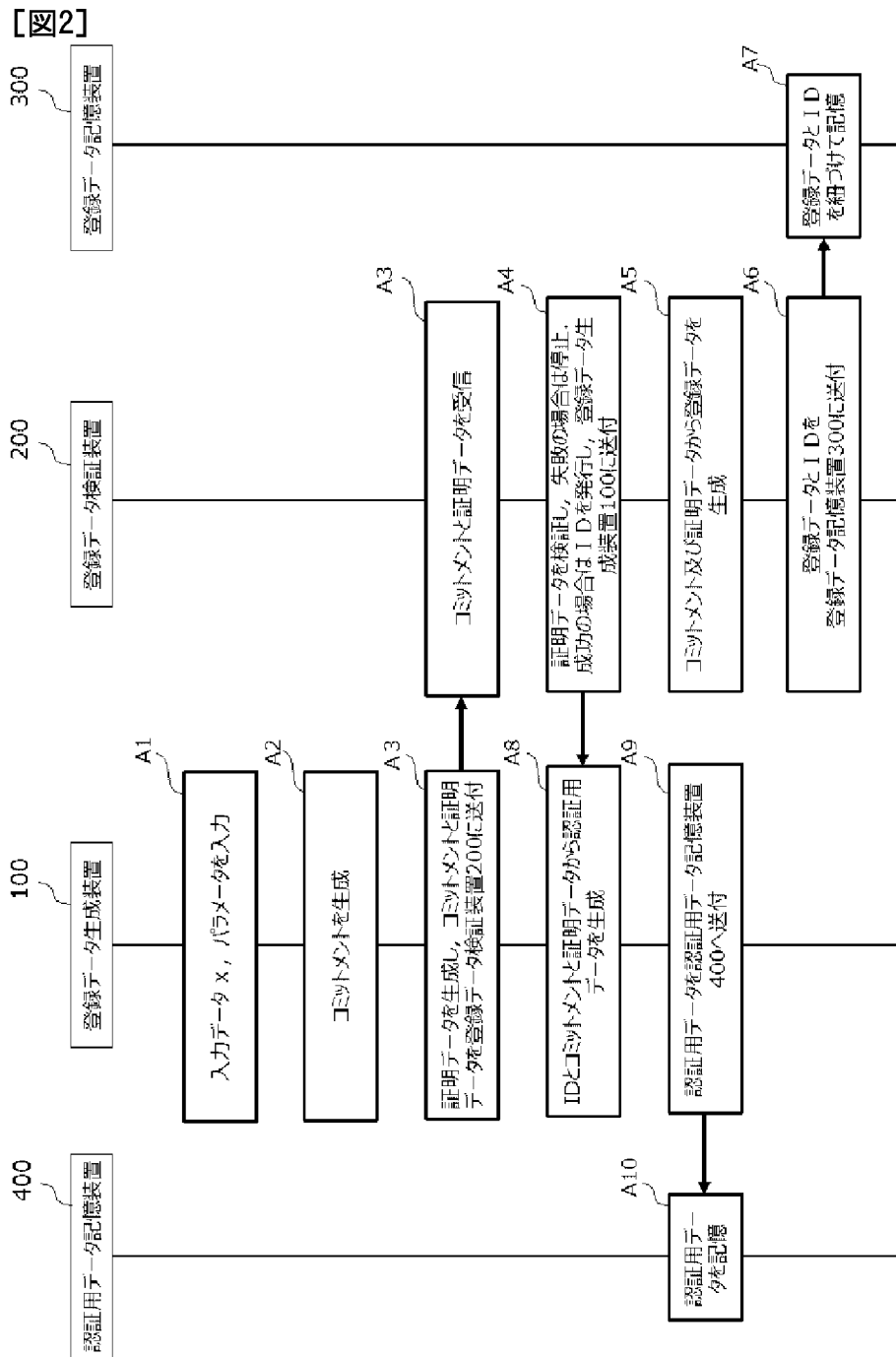


Fig. 2

[図3]

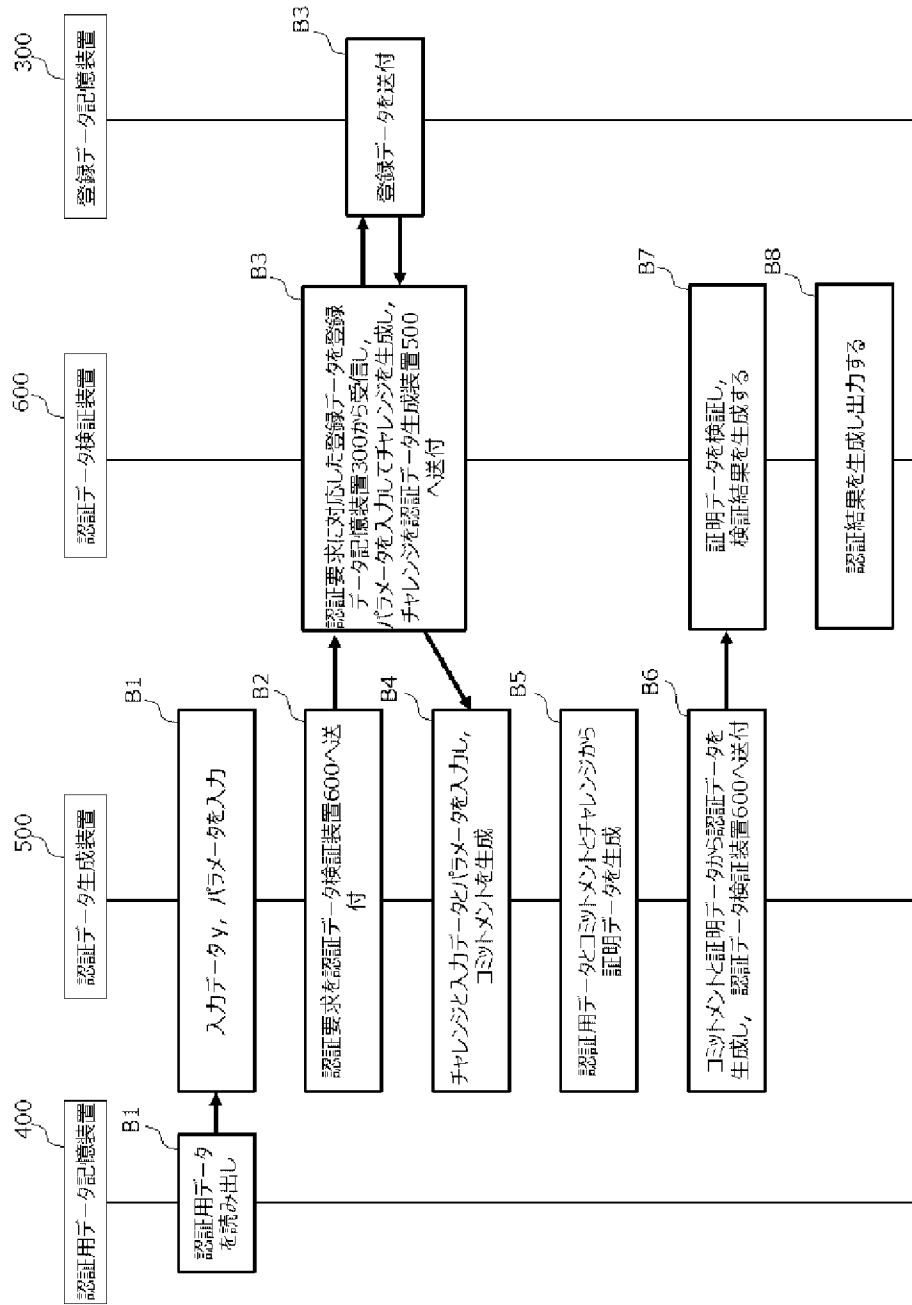


Fig. 3

[図4]

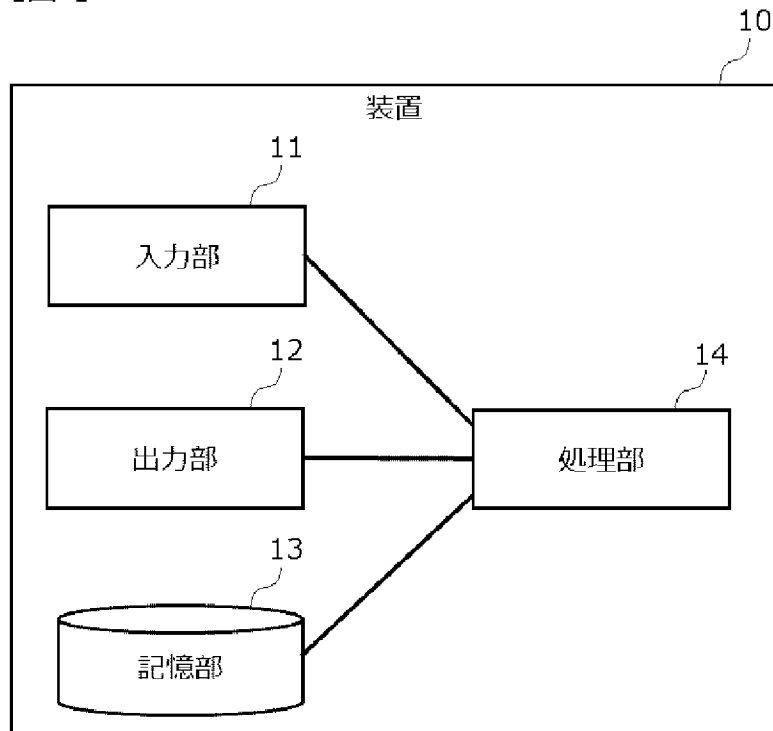


Fig. 4

[図5]

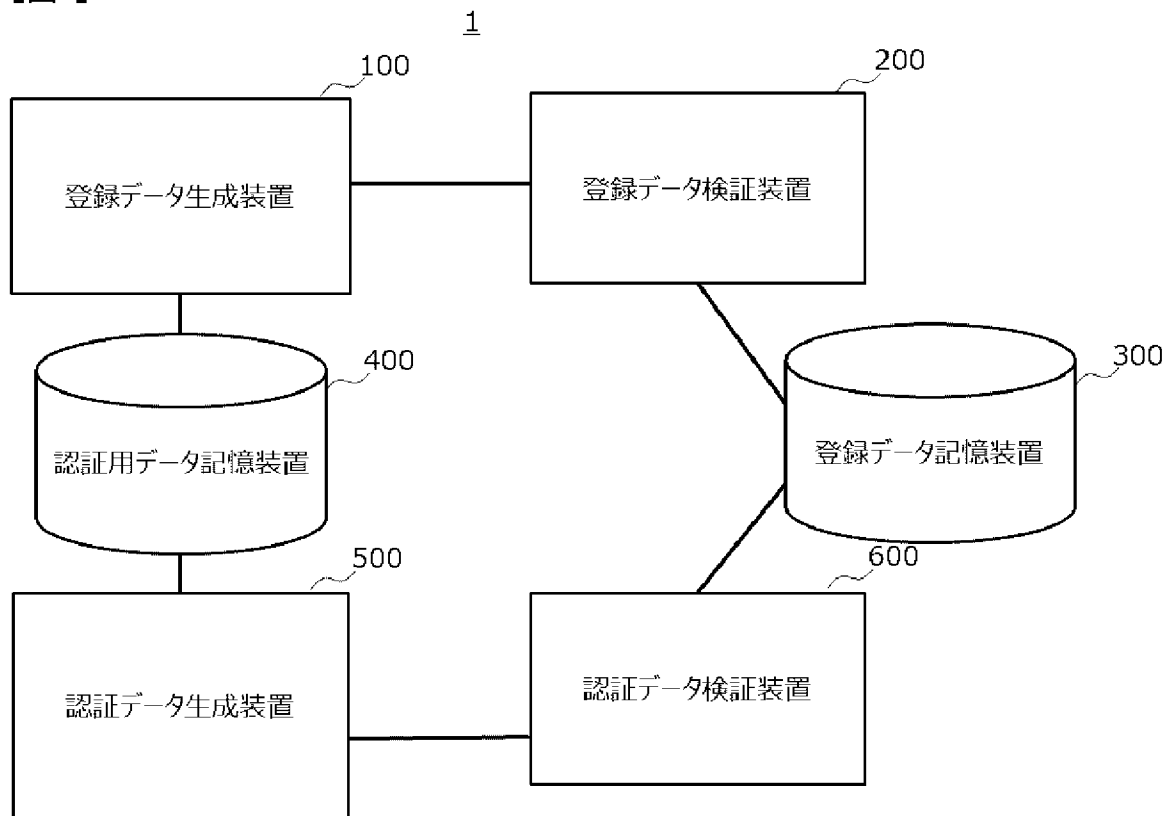


Fig. 5

[図6]

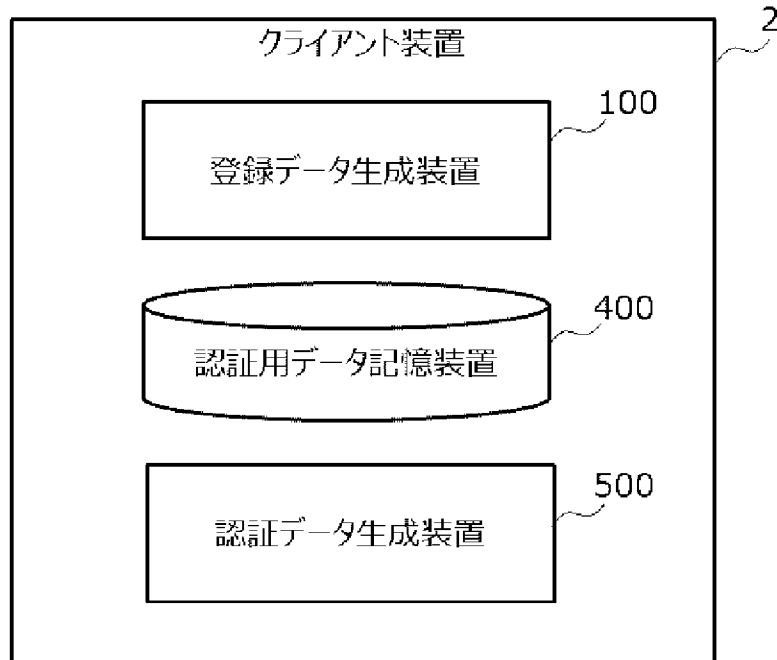


Fig. 6

[図7]

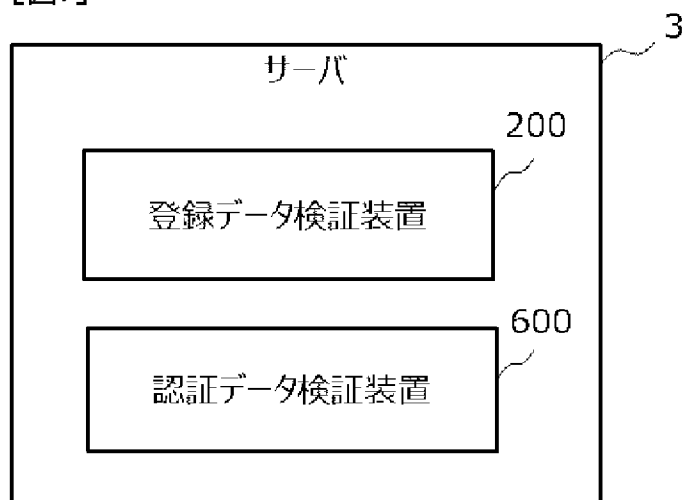


Fig. 7

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2019/036523

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl. H04L9/32 (2006.01) i, G06F21/32 (2013.01) 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)

Int.Cl. H04L9/32, G06F21/32

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

Published examined utility model applications of Japan	1922-1996
Published unexamined utility model applications of Japan	1971-2019
Registered utility model specifications of Japan	1996-2019
Published registered utility model applications of Japan	1994-2019

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 2011/148902 A1 (NEC CORPORATION) 01 December 2011 & US 2013/0073845 A1 & EP 2579501 A1	1-11
A	JP 2018-14622 A (HITACHI, LTD.) 25 January 2018 & US 2019/0238344 A1 & WO 2018/016160 A1	1-11
A	WO 2012/042775 A1 (PANASONIC CORPORATION) 05 April 2012 & US 2013/0174243 A1 & EP 2624160 A1	1-11
A	US 2019/0020482 A1 (PINDROP SECURITY, INC.) 17 January 2019 & WO 2019/014425 A1	1-11

☐ 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
22.11.2019

Date of mailing of the international search report
03.12.2019

Name and mailing address of the ISA/
Japan Patent Office
3-4-3, Kasumigaseki, Chiyoda-ku,
Tokyo 100-8915, Japan

Authorized officer

Telephone No.

A. 発明の属する分野の分類（国際特許分類（IPC））

Int.Cl. H04L9/32(2006.01)i, G06F21/32(2013.01)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. H04L9/32, G06F21/32

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	1971-2019年
日本国実用新案登録公報	1996-2019年
日本国登録実用新案公報	1994-2019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 2011/148902 A1（日本電気株式会社）2011.12.01, & US 2013/0073845 A1 & EP 2579501 A1	1-11
A	JP 2018-14622 A（株式会社日立製作所）2018.01.25, & US 2019/0238344 A1 & WO 2018/016160 A1	1-11
A	WO 2012/042775 A1（パナソニック株式会社）2012.04.05, & US 2013/0174243 A1 & EP 2624160 A1	1-11
A	US 2019/0020482 A1（PINDROP SECURITY, INC.）2019.01.17, & WO 2019/014425 A1	1-11

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	「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
「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	「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
「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）	「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
「O」 口頭による開示、使用、展示等に言及する文献	「&」 同一パテントファミリー文献
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願	

国際調査を完了した日

22.11.2019

国際調査報告の発送日

03.12.2019

国際調査機関の名称及びあて先

日本国特許庁（ISA/J P）

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）

金沢 史明

5 S

4538

電話番号 03-3581-1101 内線 3546