(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
2014 年 11 月 20 日(20.11.2014)

WIPO | PCT

(10) 国際公開番号
WO 2014/185447 A1

(51) 国際特許分類:
H04L 9/32 (2006.01) *G06F 21/31* (2013.01)

(21) 国際出願番号: PCT/JP2014/062815

(22) 国際出願日: 2014 年 5 月 14 日(14.05.2014)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願 2013-102956 2013 年 5 月 15 日(15.05.2013) JP

(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: 加藤　朝道(KATO, Asamichi); 〒2220033 神奈川県横浜市港北区新横浜３丁目２０番１２号加藤内外特許事務所内 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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, 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, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

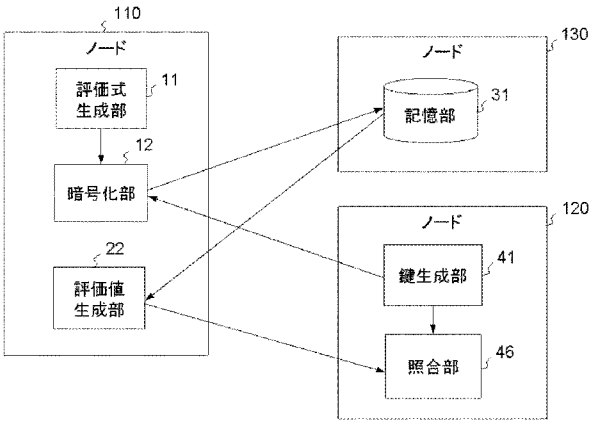
(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, 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:
— 国際調査報告（条約第 21 条(3)）

WO 2014/185447 A1

(54) **Title**: VERIFICATION SYSTEM, NODE, VERIFICATION METHOD, AND PROGRAM

(54) 発明の名称 : 照合システム、ノード、照合方法およびプログラム



11	Evaluation-expression generation unit
12	Encryption unit
22	Evaluation-value generation unit
31	Storage unit
41	Key generation unit
46	Verification unit
110, 120, 130	Node

(57) **Abstract**: A first node generates an evaluation expression for evaluating the distance with respect to authentication data, encrypts coefficients of the evaluation expression using a public key received from a second node for generating a public key/secret key pair, and transmits the encrypted coefficients to a third node. When data to be authenticated that is to be verified against the authentication data is received, the first node acquires the encrypted coefficients from the third node, generates, on the basis of the data to be authenticated and the encrypted coefficients, an evaluation value for verifying, against the authentication data, the data to be authenticated, and transmits the evaluation value to the second node. As a result, the processing load of the authentication-side node during verification of encrypted text is reduced.

(57) 要約: 第１のノードは、認証データとの距離を評価する評価式を生成し、公開鍵と秘密鍵の対を生成する第２のノードから受信した公開鍵により、評価式の係数を暗号化して第３のノードに送信し、認証データと照合される被認証データを受信すると、暗号化された係数を第３のノードから取得して、被認証データおよび暗号化された係数に基づいて、被認証データを認証データと照合するための評価値を生成し、評価値を第２のノードに送信する。暗号文の照合における認証側ノードの処理負荷を軽減する。

明　細　書

発明の名称 ： 照合システム、ノード、照合方法およびプログラム

技術分野

[0001] ［関連出願についての記載］

本発明は、日本国特許出願：特願２０１３－１０２９５６号（２０１３年５月１５日出願）に基づくものであり、同出願の全記載内容は引用をもって本書に組み込み記載されているものとする。

本発明は、照合システム、ノード、照合方法およびプログラムに関し、特に、照合されるデータの曖昧さを許容する照合システム、ノード、照合方法およびプログラムに関する。

背景技術

[0002] 近年、クラウドの普及に伴い、ネットワークに接続された計算機資源に利用者のデータを蓄積し、蓄積されたデータを用いて提供されるサービスが急速に広がってきている。このようなサービスでは、利用者の機微なデータを扱う機会も増大してきている。したがって、利用者のデータが安全に管理されていることを保証することが重要になってきている。

[0003] このような状況の下、オープンなネットワーク環境でデータを暗号化したまま管理し、データを復号することなく、検索、統計処理などを行う技術の研究開発が活発に行われている。

[0004] また、近年、パスワードや磁気カードを用いた個人認証の脆弱性をついた犯罪が頻発しており、指紋、静脈などの生体的な特徴に基づくより安全性の高い生体認証技術が注目を集めている。

[0005] 生体認証においては、認証情報の検証を行うために、生体情報に関するテンプレートをデータベースに保管する必要がある。指紋、静脈などの生体情報は基本的に生涯不変のデータであり、情報が漏洩すると甚大な被害がもたらされるため、高い機密性が要求される。

[0006] このため、テンプレートが漏洩しても「なりすまし」を行えないように、

テンプレート情報を秘匿したまま認証を行うテンプレート保護型の生体認証技術が重要となってきている。

[0007] 例えば、指紋データを多項式上の点として表現し、その点にランダムな点を付加して指紋データを秘匿したデータをテンプレートとして生体認証を行う方式が、特許文献１に記載されている。

[0008] また、準同型性を有する公開鍵暗号を利用することにより、認証を求めているクライアントの生体情報を保護する方式が、非特許文献１に記載されている。

先行技術文献

特許文献

[0009] 特許文献1：特開２００６－１５８８５１号公報

非特許文献

[0010] 非特許文献1：Siamak F. Shahandashti, Reihaneh Safavi-Naini, and Philip Ogunbona, "Private Fingerprint Matching," ACISP2012.

発明の概要

発明が解決しようとする課題

[0011] 上記の特許文献および非特許文献の全開示内容は、本書に引用をもって繰り込み記載されているものとする。以下の分析は、本発明者によってなされたものである。

[0012] 特許文献１の方式は、生体認証を何度も繰り返したとき、十分な強度で生体情報が保護されていないおそれがあることが知られている。

[0013] 一方、非特許文献１は、準同型性を有する公開鍵暗号を利用することにより、認証を求めているクライアントの生体情報を保護する方式を提案している。

[0014] 生体情報を保護しない生体認証方式では、生体情報（例えば、指紋など）からマニューシャと呼ばれる特徴点を抽出し、マニューシャを認証用テンプレートとしてサーバに登録する。一般に、マニューシャは、タイプ、座標(x,

y)、角度という３つの成分から成る。タイプは特徴点のタイプを表し、例えば、端点、分岐点などがある。座標は特徴点の座標を表し、角度は特徴点における接線の傾きを表す。

[0015] サーバは、認証時において、クライアントの生体情報から抽出されたマニューシャと、認証用テンプレートとして登録されたマニューシャが一致することを確認する。（１）特徴点のタイプが一致し、（２）特徴点間の距離が閾値以内であり、（３）特徴点における接線の傾きの差が閾値以内である、という３条件が満たされたとき、マニューシャが一致したとみなされる。

[0016] 具体的には、認証時に抽出されたマニューシャを(type1,(x1,y1),θ1)とし、登録されたマニューシャを(type2,(x2,y2),θ2)としたとき、

（１）type1=type2

（２）0≦((x1-x2)^2+(y1-y2)^2)≦δd

（３）0≦(θ1-θ2)^2≦δt

の３条件が満たされたとき、２つのマニューシャが一致したとみなされる。

[0017] ここで、δd、δtはシステムによって決められるパラメータである。また、（２）で評価される距離は、２次元ユークリッド距離、または、L2ノルムと呼ばれる。同様に、（３）で評価される距離は１次元ユークリッド距離と呼ばれる。以下では、これらをまとめてユークリッド距離と呼び、DとD’のユークリッド距離をd(D,D’)と表す。

[0018] 非特許文献１には、認証要求をしているクライアントの生体情報を秘匿できる生体認証方式が記載されている。具体的には、Aided ComputationおよびSet Intersectionと呼ばれる暗号プロトコルを利用することにより、認証時に抽出されたマニューシャ(type1,(x1,y1),θ1)をサーバに明かさずに、サーバに登録されたマニューシャ(type2,(x2,y2),θ2)とマニューシャ(type1,(x1,y1),θ1)とが一致するかどうかを確認することができる。

[0019] 以下では、クライアントからサーバに対して事前に登録されるデータを「認証データ」という。また、認証時に抽出され認証データとの照合が行われるデータを「被認証データ」という。上記の例では、マニューシャ(type2,(x

2,y2),θ2)は認証データに相当し、マニューシャ(type1,(x1,y1),θ1)は被認証データに相当する。

[0020] これらの暗号プロトコルを説明する準備として、公開鍵暗号について説明する。公開鍵暗号は、鍵生成、暗号化、復号の３つのアルゴリズムからなる。鍵生成はセキュリティパラメータを入力として受け取り、公開鍵pkと秘密鍵skを出力する確率的アルゴリズムである。暗号化は、公開鍵pkとメッセージMを入力として受け取り、暗号文Cを出力する確率的アルゴリズムである。復号は、秘密鍵skと暗号文Cを入力として受け取り、復号結果Mを出力する決定的アルゴリズムである。

[0021] 以下、鍵生成、暗号化、復号の各アルゴリズムを次のように記載する。

鍵生成：KeyGen(1^k)→(pk,sk)

暗号化：Enc(pk,M)→C

復号：Dec(sk,C)→M

[0022] 公開鍵暗号方式が準同型性を有するとは、ある演算(*)、(+)に対して、以下の式が成立する場合をいう。

Enc(pk,M1(+)M2)=Enc(pk,M1)(*)Enc(pk,M2)

[0023] 例えば、Paillier暗号は、(*)を乗算、(+)を加算とした準同型性を有する公開鍵暗号であることが知られている。次に、Paillier暗号について説明する。

[0024] 鍵生成：セキュリティパラメータ1^kを受け取る。

kビットの素数p,qをランダムに選び、n=pqとする。

次に、g=1+n mod n^2とする。

公開鍵pk=(n,g)、秘密鍵sk=(p,q)を出力する。

[0025] 暗号化：pk=(n,g)、メッセージmを入力として受け取る。

Z*_{n^2}からランダムにrを選ぶ。

C=(1+mn)・r^n mod n^2を計算する。

暗号文Cを出力する。

[0026] 復号：sk=(p,q)、暗号文Cを入力として受け取る。

λ=(p-1)(q-1)を計算する。

m=(c^{λ} mod n^2 -1)/(g^{λ} mod n^2 -1) mod nを計算する。

平文mを出力する。

[0027] C1=Enc(pk,m1)=(1+m1 n)・r1^n mod n^2、C2=Enc(pk,m2)=(1+m2 n)・r2^n mod n^2とすると、C1×C2=(1+(m1+m2)n+m1・m2・n^2)・(r1r2)^n mod n^2=(1+(m1+m2)n)・(r1r2)^n mod n^2 =Enc(pk,m1+m2)となり、Paillier暗号は準同型性を有する。このように、暗号化したまま平文の加算を行うことができる公開鍵暗号を、加法準同型公開鍵暗号と呼ぶ。

[0028] Set Intersectionとは、２人のエンティティであるアリス（Alice）とボブ（Bob）の間で行われる暗号プロトコルである。アリスはあるデータaを持ち、ボブはデータの集合Bを持つものと仮定する。このとき、Set Intersectionはアリスの持つデータaをボブに秘匿したまま、データaが集合Bに含まれるかどうかを確認するプロトコルである。

[0029] 簡単のため、集合B={b1,b2,b3}としてSet Intersectionを説明する。また、ボブは加法準同型公開鍵暗号の公開鍵pkを公開し、対応する秘密鍵skを保持しているものとする。

[0030] １．ボブはx=b1,b2,b3のとき、値が0となり、それ以外のとき、値が0以外となる多項式F(x)を生成する。例えば、F(x)=(x-b1)(x-b2)(x-b3)とすればよい。このような多項式は、ラグランジェ補間を利用して容易に生成することができる。ここで、F(x)の係数をα[0]、α[1]、…、α[n]とする。すなわち、F(x)=α[n]x^n+α[n-1]x^{n-1}+…+α[1]x+α[0]である。

２．ボブは、公開鍵pkを使用してα[0]、α[1]、…、α[n]をそれぞれ暗号化する。また、ボブは、暗号文C[0]、C[1]、…、C[n]をアリスに送付する。

３．アリスは、a^{n}、a^{n-1}、…、a^{0}を計算する。さらに、アリスは、C[n]^{a^{n}}、C[n-1]^{a^{n-1}}、…、C[0]^{a^{0}}を計算する。

４．アリスは、C=C[n]^{a^{n}}・C[n-1]^{a^{n-1}}・…・C[0]^{a^{0}}を計算する。準同型性により、C=Enc(pk、F(a))である。また、アリスは、ランダムにrを選択し、C’=C^{r}とする。さらに、アリスは、C’をボブに送付する

。

５．ボブは、受け取ったC’を復号する。ボブは、復号結果が0の場合、アリスは集合Bに含まれるデータを有すると判断し、復号結果が0以外の場合、アリスは集合Bに含まれるデータを持たないと判断する。

[0031] 簡単のため、入力aを持つアリスと、集合Bおよび秘密鍵skを持つボブによるSet Intersectionのプロトコルを Set Intersection[アリス(a),ボブ(B,sk)](pk)と表記する。ここで、pkはアリスとボブの共通入力である公開鍵pkを表す。

[0032] 次に、Aided Computationを説明する。Aided Computationも、２人のエンティティであるアリスとボブの間で行われる暗号プロトコルである。アリスはあるデータaの暗号文Enc(pk,a)を持ち、ボブはデータの集合Bおよび公開鍵pkに対応する秘密鍵skを持つものと仮定する。ボブの暗号は、加法準同型公開鍵暗号である。このとき、Aided Computationはアリスの持つデータaをボブに秘匿したまま、データaが集合Bに含まれるかどうかを確認するプロトコルである。Aided Computationでは、Set Intersectionとは異なり、アリスはデータaの平文を知らない。

[0033] 簡単のため、B={b1,b2,b3}としてAided Computationを説明する。また、x=b1,b2,b3のときに0となり、それ以外のときに0以外となる多項式F(x)が公開されているものとする。すなわち、F(x)=α[n]x^n+α[n-1]x^{n-1}+…+α[1]x+α[0]であり、α[0]～α[n]が公開されているとする。

[0034] １．アリスはランダムにrを選び、Enc(pk,ra)={Enc(pk,a)}^{r}を計算し、ボブに送付する。

２．ボブはEnc(pk,ra)を復号し、raを得る。

３．ボブは(ra)^{α[1]}、(ra)^{α[2]}、…、(ra)^{α[n]}を計算し、それぞれ公開鍵pkを用いて暗号化する。すなわち、C[i]=Enc(pk,(ra)^{α[i]})をi=1～nに対して行い、C[1]～C[n]をアリスに送付する。

４．アリスは、i=1～nに対してC’[i]=(C[i])^{1/(r^{i})}を計算する。

５．アリスはC=C’[1]・C’[2]・…・C’[n]・Enc(pk,α[0])を計算し、ボブ

に送付する。準同型性より、C=Enc(pk,F(a))である。

６．ボブは、Cを復号する。ボブは、復号結果が0の場合、アリスは集合Bに含まれるデータの暗号文を有すると判断し、復号結果が0以外の場合、アリスは集合Bに含まれるデータの暗号文を持たないと判断する。

[0035] 簡単のため、入力Enc(pk,a)を持つアリスと、集合Bおよび秘密鍵skを持つボブによる関数F(x)に対するAided Computationのプロトコルを Aided Computation[アリス(Enc(pk,a)),ボブ(B,sk)](pk,F(x))と表す。ここで、pkはアリスとボブへの共通入力である公開鍵pkを表す。

[0036] 非特許文献１では、クライアントのマニューシャ(type1,(x1,y1),θ1)（被認証データ）と、サーバに保管されている認証用テンプレート(type2,(x2,y2),θ2)（認証データ）が一致することを確認するために、Set Intersectionと Aided Computationを利用する。具体的には、以下の処理を行う。

[0037] （１）タイプの一致：Set Intersection[クライアント(type1),サーバ(type2,sk)](pk)を行う。

[0038] （２）距離の一致：まず暗号化したまま(x1,y1)および(x2,y2)間のユークリッド距離を計算する。

（ア）サーバはB={0,1,…,δd}として、F(x)を生成する。

（イ）サーバはEnc(pk,x2^2),Enc(pk,x2),Enc(pk,y2^2),Enc(pk,y2)をそれぞれ計算し、クライアントに送付する。

（ウ）クライアントはEnc(pk,x1^2),Enc(pk,y1^2)を計算する。

（エ）クライアントはEnc(pk,x1^2)・{Enc(pk,x2)}^{-2x1}・Enc(pk,x2^2)・Enc(pk,y1^2)・{Enc(pk,y2)}^{-2y1}・Enc(pk,y2^2)=Enc(pk,(x1-x2)^2+(y1-y2)^2)を計算する。

（オ）Aided Computation[クライアント(Enc(pk,(x1-x2)^2+(y1-y2)^2)),サーバ({0,1,…,δd},sk)](pk,F(x))を実行する。

[0039] （３）角度の一致：距離の一致と同様に、Enc(pk,(θ1-θ2)^2)を計算し、B’={0,1,…,δt}に対応したG(x)に対するAided Computation[クライアント(Enc(pk,(θ1-θ2)^2),サーバ(B’,sk)](pk,G(x))を実行する。

[0040] しかしながら、非特許文献１に記載された技術によると、照合ごとにサーバ（認証側ノード）がクライアント（被認証側ノード）から送られてくるデータの復号および復号結果の再暗号化を行う必要があり、照合時におけるサーバ（認証側ノード）の負荷が大きいという問題がある。

[0041] そこで、暗号文の照合時における認証側ノードの処理負荷を軽減することが要望される。本発明の目的は、かかる要望に寄与する照合システム、ノード、照合方法およびプログラムを提供することにある。

課題を解決するための手段

[0042] 本発明の第１の視点に係る照合システムは、

第１のノード、第２のノードおよび第３のノードを備え、

前記第１のノードは、認証データとの距離を評価する評価式を生成する評価式生成部と、

公開鍵により前記評価式の係数を暗号化して前記第３のノードに送信する暗号化部と、

前記認証データと照合される被認証データを受信すると、暗号化された前記係数を前記第３のノードから取得して、前記被認証データおよび暗号化された前記係数に基づいて、前記被認証データを前記認証データと照合するための評価値を生成して前記第２のノードに送信する評価値生成部と、を有し、

前記第２のノードは、前記公開鍵と秘密鍵の対を生成し、前記公開鍵を第１のノードに送信する鍵生成部と、

前記秘密鍵を用いて前記評価値を復号することにより、前記被認証データを前記認証データと照合する照合部と、を有し、

前記第３のノードは、暗号化された前記係数を保持する記憶部を有する。

[0043] 本発明の第２の視点に係るノードは、

認証データとの距離を評価する評価式を生成する評価式生成部と、

公開鍵と秘密鍵の対を生成する第２のノードから受信した前記公開鍵により、前記評価式の係数を暗号化して第３のノードに送信する暗号化部と、

前記認証データと照合される被認証データを受信すると、暗号化された前記係数を前記第３のノードから取得して、前記被認証データおよび暗号化された前記係数に基づいて、前記被認証データを前記認証データと照合するための評価値を生成して前記第２のノードに送信する評価値生成部と、を備える。

[0044] 本発明の第３の視点に係る照合方法は、

第１のノードが、認証データとの距離を評価する評価式を生成する工程と、

公開鍵と秘密鍵の対を生成する第２のノードから受信した前記公開鍵により、前記評価式の係数を暗号化して第３のノードに送信する工程と、

前記認証データと照合される被認証データを受信すると、暗号化された前記係数を前記第３のノードから取得して、前記被認証データおよび暗号化された前記係数に基づいて、前記被認証データを前記認証データと照合するための評価値を生成する工程と、

前記評価値を前記第２のノードに送信する工程と、を含む。

[0045] 本発明の第４の視点に係るプログラムは、

認証データとの距離を評価する評価式を生成する処理と、

公開鍵と秘密鍵の対を生成する第２のノードから受信した前記公開鍵により、前記評価式の係数を暗号化して第３のノードに送信する処理と、

前記認証データと照合される被認証データを受信すると、暗号化された前記係数を前記第３のノードから取得して、前記被認証データおよび暗号化された前記係数に基づいて、前記被認証データを前記認証データと照合するための評価値を生成する処理と、

前記価値を前記第２のノードに送信する処理と、を第１のノードに設けられたコンピュータに実行させる。

なお、プログラムは、非一時的なコンピュータ可読記録媒体（non-transitory computer-readable storage medium）に記録されたプログラム製品として提供することができる。

発明の効果

[0046] 本発明に係る照合システム、ノード、照合方法およびプログラムによると、暗号文の照合における認証側ノードの処理負荷を軽減することが可能となる。

図面の簡単な説明

[0047] [図1]一実施形態に係る照合システムの構成を一例として示すブロック図である。

[図2]第１の実施形態に係る照合システムの構成を一例として示すブロック図である。

[図3]第１の実施形態に係る照合システムのデータ登録動作を一例として示すシーケンス図である。

[図4]第１の実施形態に係る照合システムの暗号文照合動作を一例として示すシーケンス図である。

[図5]第３の実施形態に係る照合システムの構成を一例として示すブロック図である。

[図6]第３の実施形態に係る照合システムのデータ登録動作を一例として示すシーケンス図である。

[図7]第３の実施形態に係る照合システムの暗号文照合動作を一例として示すシーケンス図である。

発明を実施するための形態

[0048] はじめに、一実施形態の概要について説明する。なお、この概要に付記する図面参照符号は、専ら理解を助けるための例示であり、本発明を図示の態様に限定することを意図するものではない。

[0049] 図１は、一実施形態に係る照合システムの構成を一例として示すブロック図である。図１を参照すると、照合システムは、被認証側ノードとして第１のノード１１０を備え、認証側ノードとして第２のノード１２０と第３のノード１３０を備えている。第１のノード１１０は、評価式生成部１１、暗号化部１２、および、評価値生成部２２を有する。一方、第２のノード１２０

は、鍵生成部４１および照合部４６を有する。また、第３のノード１３０は記憶部３１を有する。

[0050] 第１のノード１１０の評価式生成部１１は、認証データとの距離を評価する評価式を生成する。第２のノード１２０の鍵生成部４１は、公開鍵と秘密鍵の対を生成し、公開鍵を第１のノード１１０に送信する。第１のノード１１０の暗号化部１２は、公開鍵により評価式の係数を暗号化して第３のノード１３０に送信する。第３のノード１３０の記憶部３１は、暗号化された係数を保持する。

[0051] 第１のノード１１０の評価値生成部２２は、認証データと照合される被認証データを受信すると、暗号化された係数を第３のノード１３０から取得して、被認証データおよび暗号化された係数に基づいて、被認証データを認証データと照合するための評価値を生成して第２のノード１２０に送信する。第２のノード１２０の照合部４６は、秘密鍵を用いて評価値を復号することにより、被認証データを前記認証データと照合する。

[0052] ここで、暗号化部１２は、加法準同型性を有する暗号化方式に基づいて暗号化を行うことが好ましい。一例として、暗号化部１２は、Paillier暗号に基づいて暗号化を行ってもよい。

[0053] 評価式生成部１１は、認証データとの距離が所定の距離以内であるときにゼロとなる多項式を評価式として生成してもよい。暗号化部１２は、当該多項式がi次の項の係数をα[i]（i=0,1,…,N）とするN次の多項式である場合、公開鍵により係数α[i]を暗号化し、暗号化された係数C[i]を求めて第３のノード１３０に送信してもよい。このとき、評価値生成部２２は、被認証データD'を受信すると、暗号化された係数C[i]を第３のノード１３０から取得して、C[N]^{D'^N}・C[N-1]^{D'^{N-1}}・…・C[1]^D'・C[0]を、上記の評価値として生成することが好ましい。

[0054] また、照合部４６は、秘密鍵を用いて評価値を復号した値がゼロか否かに基づいて、被認証データを認証データと照合してもよい。

[0055] さらに、認証データおよび被認証データは、n次元の要素を含んでいてもよ

い。このとき、評価式生成部１１は、被認証データと認証データとのn次元ユークリッド距離が所定の距離以内であるときにゼロとなる多項式を、上記の評価式として生成してもよい。

[0056] また、認証データおよび被認証データは、複数の要素を含んでいてもよい。このとき、評価式生成部１１は、複数の要素のそれぞれについて被認証データと認証データとの距離が所定の距離以内であるときゼロとなる多項式を求め、複数の要素に対して求めた多項式の和を、上記の評価式として生成することが好ましい。

[0057] 非特許文献１に記載された技術によると、照合ごとにサーバがクライアントから送られてくるデータの復号および復号結果の再暗号化を行う必要があり、照合におけるサーバ（認証側ノード）の負荷が大きいという問題がある。

[0058] 上記一実施形態に係る照合システムによると、データ登録時に、データあるいはデータの暗号文ではなく、照合に必要な評価式に関する情報を第１のノード１１０（被認証側ノード）が生成し、（認証側ノードに含まれる）第３のノード１３０に登録することで、かかる問題が解消される。また、用いる暗号化方式に準同型性という特殊な性質を持たせることで、暗号化したままデータのユークリッド距離を計算することを可能とし、暗号データを復号することなく照合可能であることを保証している。

[0059] かかる照合システムによると、認証側ノードに含まれる第２のノード１２０および第３のノード１３０が行う処理量が少ないため、照合処理の高速化が実現される。また、かかる照合システムによると、処理の並列化を行うことが容易となり、多くの照合要求に同時に対応することができる。その理由は、データ登録時に、第１のノード１１０（被認証側ノード）によって、照合に必要な情報が生成され、第３のノード１３０に登録されているからである。

[0060] ＜実施形態１＞

次に、第１の実施形態に係る照合システムについて、図面を参照して詳細

に説明する。

[0061] 図２は、本実施形態に係る照合システムの構成を一例として示すブロック図である。図２を参照すると、照合システムは、登録データ生成装置１０、照合要求装置２０、記憶装置３０、および、データ照合装置４０を備えている。

[0062] なお、図２は照合システムが４つのノードによって構成される場合を例示するが、本発明の照合システムは図示の態様に限定されない。一例として、登録データ生成装置１０と照合要求装置２０をまとめて第１のノードとし、データ照合装置４０を第２のノードとし、記憶装置３０を第３のノードとしてもよい。

[0063] 登録データ生成装置１０は、評価式生成部１１および暗号化部１２を備えている。

[0064] 評価式生成部１１は、秘匿の対象となる認証データと、パラメータとを入力とし、評価式を生成する。暗号化部１２は、認証データと、評価式と、データ照合装置４０が公開している暗号化鍵とを入力とし、暗号データを出力する。

[0065] 記憶装置３０は、記憶部３１および識別子管理部３２を備えている。記憶部３１は、登録データ生成装置１０から送付された暗号データとともに、識別子管理部３２によって付与された固有の識別子を記憶する。

[0066] 照合要求装置２０は、照合要求部２１、評価値生成部２２、および、照合用データ生成部２３を備えている。

[0067] 照合要求部２１は、認証データと照合すべき被認証データを受け取り、データ照合装置４０へ照合要求を送付する。評価値生成部２２は、被認証データと、データ照合装置４０から受信した照合用情報を入力として、暗号化評価値を生成する。照合用データ生成部２３は暗号化評価値を入力として、照合用データを生成する。

[0068] データ照合装置４０は、鍵生成部４１、照合用情報送付部４２、結果生成部４３、および、判定部４４を備えている。

[0069] 鍵生成部４１は、公開鍵暗号の公開鍵および秘密鍵を生成し、公開鍵を公開、秘密鍵を保持する。照合用情報送付部４２は、照合要求装置２０から送付された照合要求を入力として受け取り、照合用情報を送付する。結果生成部４３は、照合要求装置２０から送付された照合用データと秘密鍵を入力とし、結果データを出力する。判定部４４は、結果データを入力として受け取り、照合結果を生成し、出力する。

[0070] 次に、本実施形態に係る照合システムの動作を、図面を参照して詳細に説明する。

[0071] 照合システムの動作は、データ登録フェーズと暗号文照合フェーズの２つのフェーズに大別される。ここで、データ登録フェーズでは、登録データ生成装置１０に認証データを入力し、認証データを暗号化し、記憶装置３０に登録する。一方、暗号文照合フェーズでは、照合要求装置２０に入力された被認証データを秘匿しながら、被認証データが、記憶装置３０に記憶されている暗号データの平文と近い（すなわち、ユークリッド距離の小さい）ものであるか否かを判定する。

[0072] 以下、各フェーズにおける動作に関して詳細に説明する。

[0073] [データ登録フェーズ]

図３は、本実施形態に係る照合システムのデータ登録フェーズにおける動作を一例として示すシーケンス図である。

[0074] 図３を参照すると、データ照合装置４０の鍵生成部４１は、加法準同型暗号の公開鍵および秘密鍵を生成し、公開鍵を公開する（ステップＡ１）。

[0075] 次に、登録データ生成装置１０は、秘匿対象となる認証データと、公開鍵と、パラメータを受け付ける（ステップＡ２）。

[0076] 次に、登録データ生成装置１０の評価式生成部１１は、入力された認証データとパラメータから評価式を生成する(ステップＡ３)。

[0077] 次に、登録データ生成装置１０の暗号化部１２は、評価式と公開鍵から暗号データを生成し、記憶装置３０に送付する（ステップＡ４）。

[0078] 記憶装置３０の識別子管理部３２は、暗号データを受信すると、暗号デー

タに対して固有の識別子を付与する（ステップＡ５）。また、識別子管理部３２は、暗号データと識別子の組を記憶部３１に記録する（ステップＡ６）。

[0079] [暗号文照合フェーズ]

図４は、本実施形態に係る照合システムのデータ登録フェーズにおける動作を一例として示すシーケンス図である。

[0080] 図４を参照すると、照合要求装置２０の照合要求部２１は、被認証データが受け付け、照合要求を出力する（ステップＢ１）。

[0081] 次に、データ照合装置４０の照合用情報送付部４２は、識別子と照合要求を受信すると、識別子に対応した暗号データを記憶装置３０から受信し（ステップＢ２）、照合用情報を出力する（ステップＢ３）。

[0082] 照合要求装置２０の評価値生成部２２は、照合用情報を受信すると、評価式を計算し、暗号化評価値を出力する（ステップＢ４）。

[0083] 照合用データ生成部２３は、暗号化評価値と照合用情報を受け付けると、照合用データを生成し、データ照合装置４０に出力する（ステップＢ５）。

[0084] データ照合装置４０の結果生成部４３は、照合用データと秘密鍵を受信すると、結果データを生成する（ステップＢ６）。

[0085] 判定部４４は、結果データを受信すると、判定結果を生成して出力する（ステップＢ７）。

[0086] 本実施形態に係る照合システムでは、データ登録時に、データまたはデータの暗号文ではなく、照合に必要な評価式に関する情報を登録データ生成装置１０が生成して記憶装置３０に登録する。かかる照合システムによると、認証側ノードを構成するデータ照合装置４０の処理負荷を、非特許文献１に記載されたサーバの処理負荷と比較して、削減することが可能となる。

[0087] ＜実施形態２＞

次に、第２の実施形態に係る照合システムついて、図面を参照して詳細に説明する。

[0088] 本実施形態では、第１の実施形態に係る照合システムにおいて、距離とし

て１次元ユークリッド距離を用いる。すなわち、認証データDと被認証データD’の距離d(D,D’)=(D-D’)^{2}が閾値d以下である場合、認証データDと被認証データD’はマッチしたと判定する。一方、距離閾値d(D,D’)=(D-D’)^{2}が閾値dよりも大きい場合、認証データDと被認証データD’マッチしないと判定する。また、本実形態では、加法準同型暗号（例えば、Paillier暗号など）を利用する。以下、各フェーズにおける動作に関して、図３および図４を用いて詳細に説明する。

[0089] [データ登録フェーズ]

図３を参照すると、データ照合装置４０の鍵生成部４１は、加法準同型暗号の公開鍵pkと秘密鍵skを生成し、公開鍵pkを公開する（ステップＡ１）。

[0090] 次に、登録データ生成装置１０は、秘匿対象となる認証データDと、鍵生成部４１により生成された公開鍵pkを受け付ける（ステップＡ２）。

[0091] 次に、登録データ生成装置１０の評価式生成部１１は、入力された認証データDとパラメータdから、(D-x)^2=0,1,…,dのときF(x)=0となり、それ以外のときF(x)が0以外となる多項式F(x)をランダムに生成する（ステップＡ３）。

[0092] 例えば、F(x)=(D-x)^2・((D-x)^2-1)・((D-x)^2-2)・…・((D-x)^2-d)は2d+2次元の多項式であり、(D-x)^2=0,1,…,dのときにF(x)=0となり、それ以外のときにF(x)が0以外となる。簡単のため、F(x)=α[N]x^{N}+α[N-1]x^{N-1}+…+α[0]とする。前述の例では、F(x)は2d+2次元であるため、N=2d+1である。

[0093] 次に、暗号化部１２は、公開鍵pkと多項式F(x)の係数を入力として、暗号データC={Enc(pk,α[0]),Enc(pk,α[1]),…,Enc(pk,α[N])}を生成し、記憶装置３０に送付する（ステップＡ４）。

[0094] 記憶装置３０の識別子管理部３２は、暗号データを受信すると、暗号データに対して固有の識別子IDを付与する（ステップＡ５）。また、識別子管理部３２は、暗号データと識別子の組(C,ID)を記憶部３１に記録する（ステップＡ６）。

[0095] [暗号文照合フェーズ]

図４を参照すると、データ照合装置４０は、記憶部３１に記憶された暗号データと、暗号データに対応する識別子の組(C,ID)を受け付ける（ステップＢ２）。

[0096] 照合要求装置２０の照合要求部２１は、被認証データD’と公開鍵pkを受け付けると、照合要求reqを生成して、データ照合装置４０に出力する（ステップＢ１）。照合要求reqは、照合を要求するメッセージである。

[0097] ここでは、データ照合装置４０は、暗号と識別子の組を受け付けるものとした（ステップＢ２）。ただし、照合要求reqは識別子IDを含み、データ照合装置４０は識別子IDに対応する暗号文Cを記憶装置３０から受信するようにしてもよい。

[0098] データ照合装置４０の照合用情報送付部４２は、照合要求を受信すると、照合要求装置２０に照合用情報Cを出力する（ステップＢ３）。本実施形態では、照合用情報は登録されている暗号データCとする。ただし、照合用情報は、暗号データC以外にも必要な情報（例えば、セッションIDなど）を含んでいてもよい。

[0099] 照合要求装置２０の評価値生成部２２は、照合用情報Cを受信すると、次のように暗号化評価値を計算する（ステップＢ４）。

１．V=Enc(pk,α[N])^{D’^{N}}・Enc(pk,α[N-1])^{D’^{N-1}}・…・Enc(pk,α[0])とする。

２．乱数rを選び，res=V^{r}とする。

[0100] 照合用データ生成部２３は、暗号化評価値resと照合用情報を受け付けると、照合用データresを生成し、データ照合装置４０に出力する（ステップＢ５）。

[0101] ここで、照合用データは、ステップＢ４で計算された暗号化評価値resとした。ただし、照合用データは、暗号化評価値res以外にも必要な情報（セッションＩＤなど）を含んでいてもよい。

[0102] また、ステップＢ４の２は、d(D,D’)＜dの場合の出力をランダムにするた

めに行われる。出力をランダムにする必要がない場合、ステップＢ４の２を省略してもよい。

[0103] データ照合装置４０の結果生成部４３は、照合用データresと秘密鍵skを受信すると、照合用データresを復号し、復号結果として結果データRESULTを得る（ステップＢ６）。

[0104] 判定部４４は、結果データRESULTを受け付けると、RESULT=0の場合、d(D,D’)≦dと判定し、それ以外の場合、d(D,D’)>dと判定する（ステップＢ７）。

[0105] 本実施形態では、記憶装置３０に登録されている認証データは暗号データである。また、照合フェーズにおいて照合要求装置２０から送付されるデータはいずれも暗号文である。したがって、記憶装置３０に対して、登録されたデータ認証Dおよび被認証データD’に関する情報は一切洩れない。

[0106] また、本実施形態では、１次元のユークリッド距離の例を挙げたが、多項式F(x)を変更することにより、容易に２次元以上のユークリッド距離にも適用することができる。

[0107] さらに、認証データDが複数の要素からなる場合にも容易に適用可能である。例えば、D=(Dx,Dy)であり、d(Dx,Dx’)≦dxかつd(Dy,Dy’)≦dyか否かを判定したい場合、多項式f(x)をxがd(Dx,x)≦dxのときに0、それ以外のときに0以外となるように設定するとともに、多項式g(y)をyがd(Dy,y)≦dyのときに0、それ以外のときに0以外となるように設定し、F(x,y)=f(x)+g(y)とすればよい。

[0108] 本実施形態に係る照合システムでは、データ登録時に、データまたはデータの暗号文を登録する代わりに、登録データ生成装置１０が照合に必要な評価式に関する情報を生成して記憶装置３０に登録する。かかる照合システムによると、認証側ノードを構成するデータ照合装置４０の処理負荷を、非特許文献１に記載されたサーバの処理負荷と比較して、削減することが可能となる。

[0109] ＜実施形態３＞

次に、第３の実施形態に係る照合システムついて、図面を参照して詳細に説明する。

[0110] 図５は、本実施形態に係る照合システムの構成を一例として示すブロック図である。図５を参照すると、照合システムは、登録データ生成装置１００、照合要求装置２００、記憶装置３００、データ照合装置４００、および、照合補助装置５００を備えている。

[0111] なお、図５は照合システムが５つのノードによって構成される場合を例示するが、本発明の照合システムは図示の態様に限定されない。一例として、登録データ生成装置１００と照合要求装置２００をまとめて第１のノードとし、照合補助装置５００を第２のノードとし、記憶装置３００とデータ照合装置４００をまとめて第３のノードとしてもよい。

[0112] 登録データ生成装置１００は、評価式生成部１０１および暗号化部１０２を備えている。評価式生成部１０１は、秘匿の対象となる認証データとパラメータを入力とし、評価式を生成する。暗号化部１０２は、認証データと、評価式と、照合補助装置５００が公開している暗号化鍵とを入力とし、暗号データを出力する。

[0113] 記憶装置３００は、記憶部３０１および識別子管理部３０２を備えている。記憶部３０１は、登録データ生成装置１００から送付された暗号データとともに、識別子管理部３０２によって付与された固有の識別子を記憶する。

[0114] 照合要求装置２００は、照合要求部２０１、評価値生成部２０２、および、照合用データ生成部２０３を備えている。照合要求部２０１は、認証データと照合すべき被認証データを入力として受け取り、データ照合装置４００へ照合要求を送付する。評価値生成部２０２は、被認証データと、データ照合装置４００から受信した照合用情報を入力として、暗号化評価値を生成する。照合用データ生成部２０３は、暗号化評価値を入力として、照合用データを生成する。

[0115] データ照合装置４００は、照合用情報送付部４０１、照合補助要求部４０２、および、判定部４０３を備えている。照合用情報送付部４０１は、照合

要求装置２００から送付された照合要求を入力として受け取り、照合用情報を送付する。照合補助要求部４０２は、照合要求装置２００から送付された照合用データを入力とし、照合補助装置５００に対して照合補助要求を出力する。判定部４０３は、照合補助要求に対して照合補助装置５００が出力した結果データを入力として受け取り、照合結果を生成して出力する。

[0116] 照合補助装置５００は、鍵生成部５０１および照合補助部５０２を備えている。鍵生成部５０１は、加法準同型暗号の公開鍵および秘密鍵を生成し、公開鍵を公開し、秘密鍵を記憶する。照合補助部５０２は、データ照合装置４００が出力した照合補助要求と、秘密鍵とを入力とし、結果データを出力する。

[0117] 次に、本実施形態に係る照合システムの動作について、図面を参照して詳細に説明する。

[0118] 照合システムの動作は、データ登録フェーズと、暗号文照合フェーズの２つのフェーズに大別される。ここで、データ登録フェーズでは、登録データ生成装置１００に認証データを入力し、認証データを暗号化し、記憶装置３００に登録する。一方、暗号文照合フェーズでは、照合要求装置２００に入力された被認証データを秘匿しながら、被認証データが記憶装置３００に記憶されている暗号データの平文と近い（すなわち、ユークリッド距離の小さい）ものであるか否かを判定する。

[0119] 以下、各フェーズにおける動作に関して詳細に説明する。

[0120] [データ登録フェーズ]

図６は、本実施形態に係る照合システムのデータ登録フェーズにおける動作を一例として示すシーケンス図である。

[0121] 図６を参照すると、照合補助装置５００の鍵生成部５０１は、加法準同型暗号の公開鍵および秘密鍵を生成し、公開鍵を公開する（ステップＣ１）。

[0122] 次に、登録データ生成装置１００は、秘匿対象となる認証データと、鍵生成部５０１により生成された公開鍵と、パラメータとを受け付ける（ステップＣ２）。

[0123] 次に、登録データ生成装置１００の評価式生成部１０１は、入力された認証データとパラメータから、評価式を生成する（ステップＣ３）。次に、登録データ生成装置１００の暗号化部１０２は、評価式と公開鍵から、暗号データを生成し、記憶装置３００に送付する（ステップＣ４）。

[0124] 記憶装置３００の識別子管理部３０２は、暗号データを受信すると、暗号データに対して固有の識別子を付与する（ステップＣ５）。また、識別子管理部３０２は、暗号データと識別子の組を記憶部３０１に記録する（ステップＣ６）。

[0125] [暗号文照合フェーズ]

図７は、本実施形態に係る照合システムの暗号文照合フェーズにおける動作を一例として示すシーケンス図である。

[0126] 図７を参照すると、照合要求装置２００の照合要求部２０１は、被認証データを受け付け、照合要求を出力する（ステップＤ１）。

[0127] データ照合装置４００の照合用情報送付部４０１は、識別子と照合要求を受信すると、識別子に対応した暗号データを記憶装置３００から受信し（ステップＤ２）、照合用情報を出力する（ステップＤ３）。

[0128] 照合要求装置２００の評価値生成部２０２は、照合用情報を受信すると、評価式を計算し、暗号化評価値を出力する（ステップＤ４）。

[0129] 照合用データ生成部２０３は、暗号化評価値と照合用情報を入力とし、照合用データを生成し、データ照合装置４００に出力する（ステップＤ５）。

[0130] データ照合装置４００の照合補助要求部４０２は、照合用データを受信すると、照合補助要求を生成し、照合補助装置５００に出力する（ステップＤ６）。

[0131] 照合補助装置５００の照合補助部５０２は、照合補助要求と秘密鍵を入力とし、結果データを生成し、データ照合装置４００に出力する（ステップＤ７）。

[0132] データ照合装置４００の判定部４０３は、結果データを受信すると、判定結果を生成して出力する（ステップＤ８）。

[0133] 本実施形態に係る照合システムでは、データ登録時に、データまたはデータの暗号文を登録する代わりに、登録データ生成装置１００が照合に必要な評価式に関する情報を生成して記憶装置３００に登録する。かかる照合システムによると、認証側ノードを構成するデータ照合装置４００および照合補助装置５００の処理負荷を、非特許文献１に記載されたサーバの処理負荷と比較して、削減することが可能となる。

[0134] ＜実施形態４＞

次に、第４の実施形態に係る照合システムについて、図面を参照して詳細に説明する。

[0135] 本実施形態では、第３の実施形態に係る照合システムにおいて、距離として１次元ユークリッド距離を用いる。すなわち、認証データDと被認証データD’との距離d(D,D’)=(D-D’)^{2}が閾値d以下である場合、認証データDと被認証データD’はマッチしたと判定する。一方、距離d(D,D’)=(D-D’)^{2}が閾値dよりも大きい場合、認証データDと被認証データD’マッチしないと判定する。また、本実施形態では、加法準同型暗号（例えば、Paillier暗号など）を利用する。以下、各フェーズにおける動作に関して、図６および図７を参照して詳細に説明する。

[0136] [データ登録フェーズ]

図６を参照すると、照合補助装置５００の鍵生成部５０１は、加法準同型暗号の公開鍵pkおよび秘密鍵skを生成し、公開鍵pkを公開する（ステップＣ１）。

[0137] 次に、登録データ生成装置１００は、秘匿対象となる認証データDと、鍵生成部５０１により生成された公開鍵pkとを受け付ける（ステップＣ２）。

[0138] 次に、登録データ生成装置１００の評価式生成部１０１は、入力された認証データDとパラメータdから、(D-x)^2=0,1,…,dのときにF(x)=0となり、それ以外のときにF(x)が0以外となる多項式F(x)をランダムに生成する（ステップＣ３）。

[0139] 例えば、F(x)=(D-x)^2・((D-x)^2-1)・((D-x)^2-2)・…・((D-x)^2-d)は2d

+2次元の多項式であり、(D-x)^2=0,1,…,dのときにF(x)=0となり、それ以外のときにF(x)が0以外となる。簡単のため、F(x)=α[N]x^{N}+α[N-1]x^{N-1}+…+α[0]とする。上記の例ではF(x)は2d+2次元であるため、N=2d+1である。

[0140] 次に、暗号化部１０２は、公開鍵pkと多項式F(x)の係数を入力として、暗号データC={Enc(pk,α[0]),Enc(pk,α[1])、…、Enc(pk,α[N])}を生成し、記憶装置３００に送付する（ステップＣ４）。

[0141] 記憶装置３００の識別子管理部３０２は、暗号データを受信すると、暗号データに対して固有の識別子IDを付与する（ステップＣ５）。また、識別子管理部３０２は、暗号データと識別子の組(C,ID)を記憶部３０１に記憶する（ステップＣ６）。

[0142] [暗号文照合フェーズ]

図７を参照すると、データ照合装置４００は、記憶部３０１に記憶された暗号データと暗号データに対応する識別子の組(C,ID)を受け付ける（ステップＤ２）。

[0143] 次に、照合要求装置２００の照合要求部２０１は、被認証データD’と公開鍵pkを受け付ける（ステップＤ１）。

[0144] 次に、照合要求装置２００の照合要求部２０１は、被認証データD’と公開鍵pkを受け付けると、照合要求reqを生成し、データ照合装置４００に出力する（ステップＤ１）。照合要求reqは、照合を要求するメッセージである。

[0145] ここでは、データ照合装置４００は、暗号と識別子の組を受け付けるものとした（ステップＤ２）。ただし、照合要求reqが識別子IDを含み、データ照合装置４００が識別子IDに対応する暗号文Cを記憶装置３００から受信するようにしてもよい。

[0146] データ照合装置４００の照合用情報送付部４０１は、照合要求を受信すると、照合要求装置２００に照合用情報Cを出力する（ステップＤ３）。本実施形態では、照合用情報は、登録されている暗号データCとする。ただし、照合用情報は、暗号データC以外にも必要な情報（例えば、セッションＩＤなど）を含んでいてもよい。

[0147] 照合要求装置２００の評価値生成部２０２は、照合用情報Cを受信すると、次のように暗号化評価値を計算する（ステップＤ４）。

[0148] １．V=Enc(pk,α[N])^{D'^{N}}・Enc(pk,α[N-1])^{D'^{N-1}}・…・Enc(pk,α[0])とする。

２．乱数rを選び，res=V^{r}とする。

[0149] 照合用データ生成部２０３は、暗号化評価値resと照合用情報を入力とし、照合用データresを生成し、データ照合装置４００に出力する（ステップＤ５）。

[0150] ここでは、照合用データはステップＤ４で計算された暗号化評価値resとした。ただし、照合用データは、暗号化評価値res以外にも必要な情報（セッションＩＤなど）を含んでいてもよい。

[0151] また、ステップＤ４の２は、d(D,D')＜dの場合の出力をランダムにするために行われる。出力をランダムにする必要がない場合、ステップＤ４の２を省略してもよい。

[0152] データ照合装置４００の照合補助要求部４０２は、照合用データresと秘密鍵skを受信すると、照合補助要求resを照合補助装置５００に出力する（ステップＤ６）。

[0153] ここでは、照合補助要求を暗号化評価値resとした。ただし、照合補助要求は、暗号化評価値res以外にも必要な情報（例えば、セッションIDや要求日時など）を含んでいてもよい。

[0154] 照合補助装置５００の照合補助部５０２は、照合補助要求resと秘密鍵skを入力とし、resを復号し、復号結果を結果データRESULTとしてデータ照合装置４００に出力する（ステップＤ７）。

[0155] 判定部４４は、結果データRESULTを入力とし、RESULT=0の場合、d(D,D')≦dであると判定し、それ以外の場合、d(D,D')>dと判定する（ステップＤ８）。

[0156] 本実施形態では、記憶装置３００に登録されているデータは暗号データである。また、照合フェーズにおいて照合要求装置２００から送付されるデー

タはいずれも暗号文である。したがって、記憶装置３００およびデータ照合装置４００に対して、登録された認証データDおよび被認証データD’に関する情報は一切洩れない。

[0157] また、本実施形態では、１次元のユークリッド距離の例を挙げたが、多項式F(x)を変更することにより、容易に２次元以上のユークリッド距離にも適用することができる。

[0158] さらに、認証データDが複数の要素からなる場合にも容易に適用可能である。例えば、D=(Dx,Dy)であり、d(Dx,Dx’)≦dxかつd(Dy,Dy’)≦dyかどうかを判定したい場合、多項式f(x)をxがd(Dx,x)≦dxのときに0となり、それ以外のときに0以外となるように設定するとともに、多項式g(y)をyがd(Dy,y)≦dyのときに0となり、それ以外は0以外となるように設定し、F(x,y)=f(x)+g(y)とすればよい。

[0159] 本実施形態に係る照合システムでは、データ登録時に、データまたはデータの暗号文ではなく、（被認証側のノードに含まれる）登録データ生成装置１００が照合に必要な評価式に関する情報を生成して、（認証側ノードに含まれる）記憶装置３００に登録する。かかる照合システムによると、（認証側ノードに含まれる）データ照合装置４００および照合補助装置５００の処理負荷を、非特許文献１に記載されたサーバの処理負荷と比較して、削減することが可能となる。

[0160] 上記実施形態に係る認証システムは、一例として、タイプと２次元座標と角度を要素とするマニューシャを用いた生体認証に対して適用することができる。具体的には、データ登録フェーズにおける入力データと、暗号文照合フェーズにおける入力データを、指紋や静脈などから取得した生体情報（マニューシャ）とする。これにより、生体情報を秘匿したまま、記憶装置に格納された暗号化された生体データと、照合要求装置から創出された暗号化された生体データが同一人物から採取されたものであるか否かを、２つの入力データのユークリッド距離が一定数以下となるかどうかにより判定することが可能となる。特に、生体情報は、常に安定して同一のデータが取得できる

わけではないことが知られている。一方、同一人物から取得されるデータは類似している（各要素のユークリッド距離が小さいデータが取得できる）と仮定することができる。したがって、本発明に係る照合システムは、生体認証に対して好適に適用し得る。

[0161] なお、上記の特許文献および非特許文献の全開示内容は、本書に引用をもって繰り込み記載されているものとする。本発明の全開示（請求の範囲を含む）の枠内において、さらにその基本的技術思想に基づいて、実施形態の変更・調整が可能である。また、本発明の全開示の枠内において種々の開示要素（各請求項の各要素、各実施形態の各要素、各図面の各要素などを含む）の多様な組み合わせ、ないし、選択が可能である。すなわち、本発明は、請求の範囲を含む全開示、技術的思想にしたがって当業者であればなし得るであろう各種変形、修正を含むことは勿論である。特に、本書に記載した数値範囲については、当該範囲内に含まれる任意の数値ないし小範囲が、別段の記載のない場合でも具体的に記載されているものと解釈されるべきである。

[0162] なお、本発明において、下記の形態が可能である。

［形態１］

上記第１の視点に係る照合システムのとおりである。

［形態２］

前記暗号化部は、加法準同型性を有する暗号化方式に基づいて暗号化を行う、形態１に記載の照合システム。

［形態３］

前記暗号化部は、Paillier暗号に基づいて暗号化を行う、形態２に記載の照合システム。

［形態４］

前記評価式生成部は、認証データとの距離が所定の距離以内であるときにゼロとなる多項式を前記評価式として生成する、形態１ないし３のいずれか一に記載の照合システム。

［形態５］

前記暗号化部は、前記多項式がi次の項の係数を$\alpha[i]$（i=0,1,…,N）とするN次の多項式である場合、公開鍵により前記係数$\alpha[i]$を暗号化し、暗号化された係数C[i]を求めて前記第３のノードに送信し、

前記評価値生成部は、前記被認証データD'を受信すると、暗号化された前記係数C[i]を前記第３のノードから取得して、C[N]^{D'^N}・C[N-1]^{D'^{N-1}}・…・C[1]^D'・C[0]を前記評価値として生成する、形態４に記載の照合システム。

［形態６］

前記照合部は、前記秘密鍵を用いて前記評価値を復号した値がゼロか否かに基づいて、前記被認証データを前記認証データと照合する、形態４または５に記載の照合システム。

［形態７］

前記認証データおよび前記被認証データは、n次元の要素を含み、

前記評価式生成部は、前記被認証データと前記認証データとのn次元ユークリッド距離が所定の距離以内であるときにゼロとなる多項式を前記評価式として生成する、形態４ないし６のいずれか一に記載の照合システム。

［形態８］

前記認証データおよび前記被認証データは、複数の要素を含み、

前記距評価式生成部は、前記複数の要素のそれぞれについて前記被認証データと前記認証データとの距離が所定の距離以内であるときゼロとなる多項式を求め、前記複数の要素に対して求めた多項式の和を、前記評価式として生成する、形態１ないし７のいずれか一に記載の照合システム。

［形態９］

上記第２の視点に係るノードのとおりである。

［形態１０］

前記暗号化部は、加法準同型性を有する暗号化方式に基づいて暗号化を行う、形態９に記載のノード。

［形態１１］

前記暗号化部は、Paillier暗号に基づいて暗号化を行う、形態１０に記載のノード。

［形態１２］

前記評価式生成部は、認証データとの距離が所定の距離以内であるときにゼロとなる多項式を前記評価式として生成する、形態９ないし１１のいずれか一に記載のノード。

［形態１３］

前記暗号化部は、前記多項式がi次の項の係数を$\alpha[i]$（i=0,1,…,N）とするN次の多項式である場合、公開鍵により前記係数$\alpha[i]$を暗号化し、暗号化された係数C[i]を求めて前記第３のノードに送信し、

前記評価値生成部は、前記被認証データD'を受信すると、暗号化された前記係数C[i]を前記第３のノードから取得して、C[N]^{D'^N}・C[N-1]^{D'^{N-1}}・…・C[1]^D'・C[0]を前記評価値として生成する、形態１２に記載のノード。

［形態１４］

前記認証データおよび前記被認証データは、n次元の要素を含み、

前記評価式生成部は、前記被認証データと前記認証データとのn次元ユークリッド距離が所定の距離以内であるときにゼロとなる多項式を前記評価式として生成する、形態１２または１３に記載のノード。

［形態１５］

前記認証データおよび前記被認証データは、複数の要素を含み、

前記距評価式生成部は、前記複数の要素のそれぞれについて前記被認証データと前記認証データとの距離が所定の距離以内であるときゼロとなる多項式を求め、前記複数の要素に対して求めた多項式の和を、前記評価式として生成する、形態９ないし１４のいずれか一に記載のノード。

［形態１６］

第１のノード、第２のノードおよび第３のノードを備えた照合システムにおける照合方法であって、

前記第２のノードが、公開鍵と秘密鍵の対を生成し、前記公開鍵を第１のノードに送信する工程と、

前記第１のノードが、認証データとの距離を評価する評価式を生成する工程と、

前記第１のノードが、前記公開鍵により前記評価式の係数を暗号化して前記第３のノードに送信する工程と、

前記第３のノードが、暗号化された前記係数を保持する工程と、

前記第１のノードが、前記認証データと照合される被認証データを受信すると、暗号化された前記係数を前記第３のノードから取得して、前記被認証データおよび暗号化された前記係数に基づいて、前記被認証データを前記認証データと照合するための評価値を生成して前記第２のノードに送信する工程と、

前記第２のノードが、前記秘密鍵を用いて前記評価値を復号することにより、前記被認証データを前記認証データと照合する工程と、を含む、照合方法。

［形態１７］

上記第３の視点に係る照合方法のとおりである。

［形態１８］

前記第１のノードは、加法準同型性を有する暗号化方式に基づいて暗号化を行う、形態１７に記載の照合方法。

［形態１９］

前記第１のノードは、Paillier暗号に基づいて暗号化を行う、形態１８に記載の照合方法。

［形態２０］

前記第１のノードは、認証データとの距離が所定の距離以内であるときにゼロとなる多項式を前記評価式として生成する、形態１７ないし１９のいずれか一に記載の照合方法。

［形態２１］

前記第１のノードは、前記多項式がi次の項の係数をα[i]（i=0,1,…,N）とするN次の多項式である場合、公開鍵により前記係数α[i]を暗号化し、暗号化された係数C[i]を求めて前記第３のノードに送信し、

前記被認証データD'を受信すると、暗号化された前記係数C[i]を前記第３のノードから取得して、C[N]^{D'^N}・C[N-1]^{D'^{N-1}}・…・C[1]^D'・C[0]を前記評価値として生成する、形態２０に記載の照合方法。

［形態２２］

前記認証データおよび前記被認証データは、n次元の要素を含み、

前記第１のノードは、前記被認証データと前記認証データとのn次元ユークリッド距離が所定の距離以内であるときにゼロとなる多項式を前記評価式として生成する、形態２０または２１に記載の照合方法。

［形態２３］

前記認証データおよび前記被認証データは、複数の要素を含み、

前記第１のノードは、前記複数の要素のそれぞれについて前記被認証データと前記認証データとの距離が所定の距離以内であるときゼロとなる多項式を求め、前記複数の要素に対して求めた多項式の和を、前記評価式として生成する、形態１７ないし２２のいずれか一に記載の照合方法。

［形態２４］

上記第４の視点に係るプログラムのとおりである。

［形態２５］

加法準同型性を有する暗号化方式に基づいて暗号化する処理を、前記コンピュータに実行させる、形態２４に記載のプログラム。

［形態２６］

Paillier暗号に基づいて暗号化する処理を、前記コンピュータに実行させる、形態２５に記載のプログラム。

［形態２７］

認証データとの距離が所定の距離以内であるときにゼロとなる多項式を前記評価式として生成する処理を、前記コンピュータに実行させる、形態２４

ないし２６のいずれか一に記載のプログラム。

［形態２８］

前記多項式がi次の項の係数をα[i]（i=0,1,…,N）とするN次の多項式である場合、公開鍵により前記係数α[i]を暗号化し、暗号化された係数C[i]を求めて前記第３のノードに送信する処理と、

前記被認証データD'を受信すると、暗号化された前記係数C[i]を前記第３のノードから取得して、C[N]^{D'^N}・C[N-1]^{D'^{N-1}}・…・C[1]^D'・C[0]を前記評価値として生成する処理と、を前記コンピュータに実行させる、形態２７に記載のプログラム。

［形態２９］

前記認証データおよび前記被認証データは、n次元の要素を含み、

前記被認証データと前記認証データとのn次元ユークリッド距離が所定の距離以内であるときにゼロとなる多項式を前記評価式として生成する処理を、前記コンピュータに実行させる、形態２７または２８に記載のプログラム。

［形態３０］

前記認証データおよび前記被認証データは、複数の要素を含み、

前記複数の要素のそれぞれについて前記被認証データと前記認証データとの距離が所定の距離以内であるときゼロとなる多項式を求め、前記複数の要素に対して求めた多項式の和を、前記評価式として生成する処理を、前記コンピュータに実行させる、形態２４ないし２９のいずれか一に記載のプログラム。

符号の説明

[0163] １０、１００　登録データ生成装置

１１、１０１　評価式生成部

１２、１０２　暗号化部

２０、２００　照合要求装置

２１、２０１　照合要求部

２２、２０２　評価値生成部

２３、２０３　　照合用データ生成部

３０、３００　　記憶装置

３１、３０１　　記憶部

３２、３０２　　識別子管理部

４０、４００　　データ照合装置

４１　　鍵生成部

４２、４０１　　照合用情報送付部

４３　　結果生成部

４４、４０３　　判定部

４６　　照合部

１１０、１２０、１３０　ノード

４０２　　照合補助要求部

５００　　照合補助装置

５０１　　鍵生成部

５０２　　照合補助部

請求の範囲

[請求項1] 第１のノード、第２のノードおよび第３のノードを備え、

前記第１のノードは、認証データとの距離を評価する評価式を生成する評価式生成部と、

公開鍵により前記評価式の係数を暗号化して前記第３のノードに送信する暗号化部と、

前記認証データと照合される被認証データを受信すると、暗号化された前記係数を前記第３のノードから取得して、前記被認証データおよび暗号化された前記係数に基づいて、前記被認証データを前記認証データと照合するための評価値を生成して前記第２のノードに送信する評価値生成部と、を有し、

前記第２のノードは、前記公開鍵と秘密鍵の対を生成し、前記公開鍵を第１のノードに送信する鍵生成部と、

前記秘密鍵を用いて前記評価値を復号することにより、前記被認証データを前記認証データと照合する照合部と、を有し、

前記第３のノードは、暗号化された前記係数を保持する記憶部を有する、照合システム。

[請求項2] 前記暗号化部は、加法準同型性を有する暗号化方式に基づいて暗号化を行う、請求項１に記載の照合システム。

[請求項3] 前記評価式生成部は、認証データとの距離が所定の距離以内であるときにゼロとなる多項式を前記評価式として生成する、請求項１または２に記載の照合システム。

[請求項4] 前記暗号化部は、前記多項式がi次の項の係数を$\alpha[i]$（i=0,1,…,N）とするN次の多項式である場合、公開鍵により前記係数$\alpha[i]$を暗号化し、暗号化された係数C[i]を求めて前記第３のノードに送信し、

前記評価値生成部は、前記被認証データD'を受信すると、暗号化された前記係数C[i]を前記第３のノードから取得して、C[N]^{D'^N}・C[N-1]^{D'^{N-1}}・…・C[1]^D'・C[0]を前記評価値として生成する

、請求項３に記載の照合システム。

[請求項5] 前記照合部は、前記秘密鍵を用いて前記評価値を復号した値がゼロか否かに基づいて、前記被認証データを前記認証データと照合する、請求項３または４に記載の照合システム。

[請求項6] 前記認証データおよび前記被認証データは、n次元の要素を含み、

前記評価式生成部は、前記被認証データと前記認証データとのn次元ユークリッド距離が所定の距離以内であるときにゼロとなる多項式を前記評価式として生成する、請求項３ないし５のいずれか１項に記載の照合システム。

[請求項7] 前記認証データおよび前記被認証データは、複数の要素を含み、

前記距評価式生成部は、前記複数の要素のそれぞれについて前記被認証データと前記認証データとの距離が所定の距離以内であるときゼロとなる多項式を求め、前記複数の要素に対して求めた多項式の和を、前記評価式として生成する、請求項１ないし６のいずれか１項に記載の照合システム。

[請求項8] 認証データとの距離を評価する評価式を生成する評価式生成部と、

公開鍵と秘密鍵の対を生成する第２のノードから受信した前記公開鍵により、前記評価式の係数を暗号化して第３のノードに送信する暗号化部と、

前記認証データと照合される被認証データを受信すると、暗号化された前記係数を前記第３のノードから取得して、前記被認証データおよび暗号化された前記係数に基づいて、前記被認証データを前記認証データと照合するための評価値を生成して前記第２のノードに送信する評価値生成部と、を備える、ノード。

[請求項9] 第１のノードが、認証データとの距離を評価する評価式を生成する工程と、

公開鍵と秘密鍵の対を生成する第２のノードから受信した前記公開鍵により、前記評価式の係数を暗号化して第３のノードに送信する工

程と、

前記認証データと照合される被認証データを受信すると、暗号化された前記係数を前記第３のノードから取得して、前記被認証データおよび暗号化された前記係数に基づいて、前記被認証データを前記認証データと照合するための評価値を生成する工程と、

前記評価値を前記第２のノードに送信する工程と、を含む、照合方法。

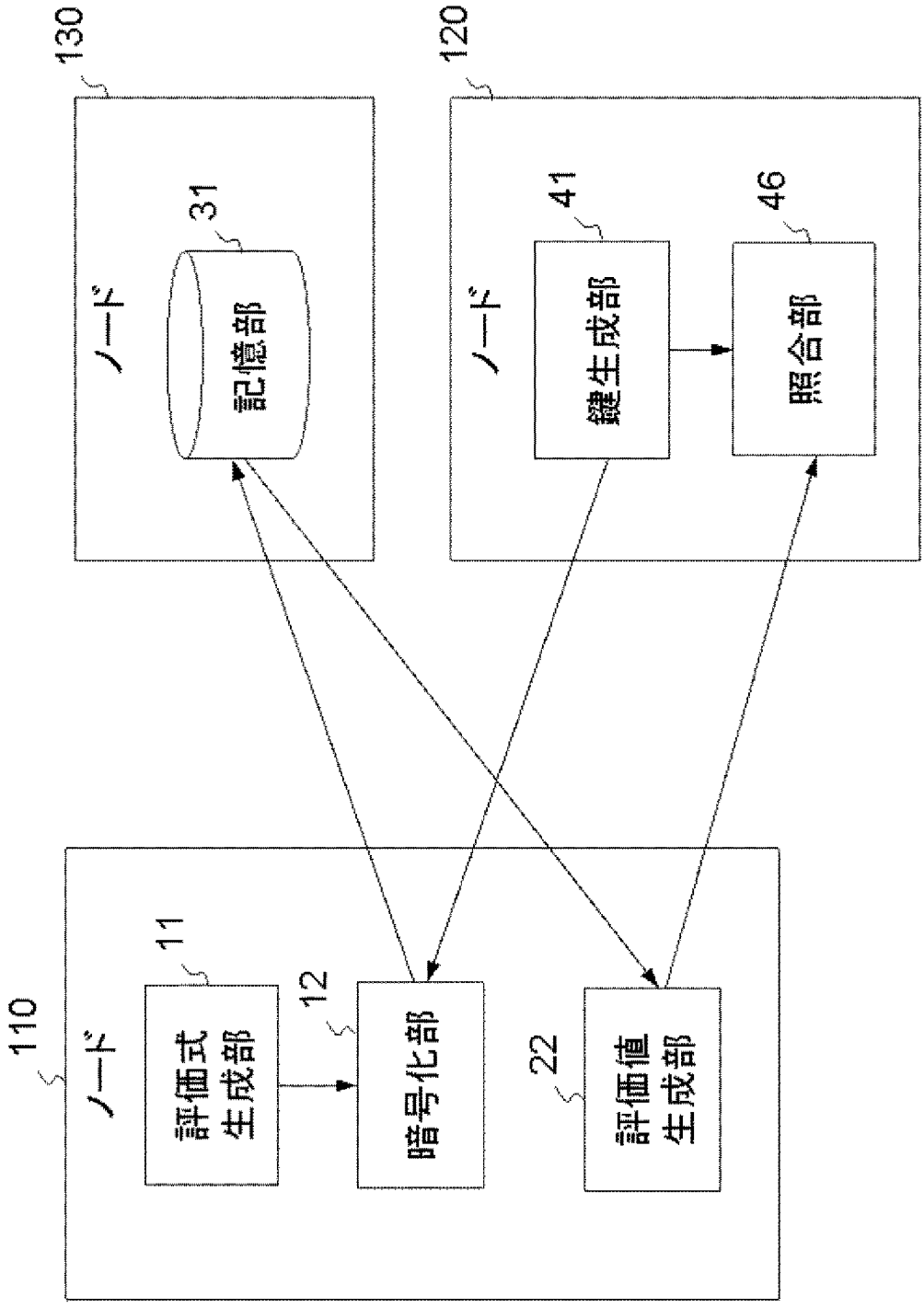
[請求項10] 認証データとの距離を評価する評価式を生成する処理と、

公開鍵と秘密鍵の対を生成する第２のノードから受信した前記公開鍵により、前記評価式の係数を暗号化して第３のノードに送信する処理と、

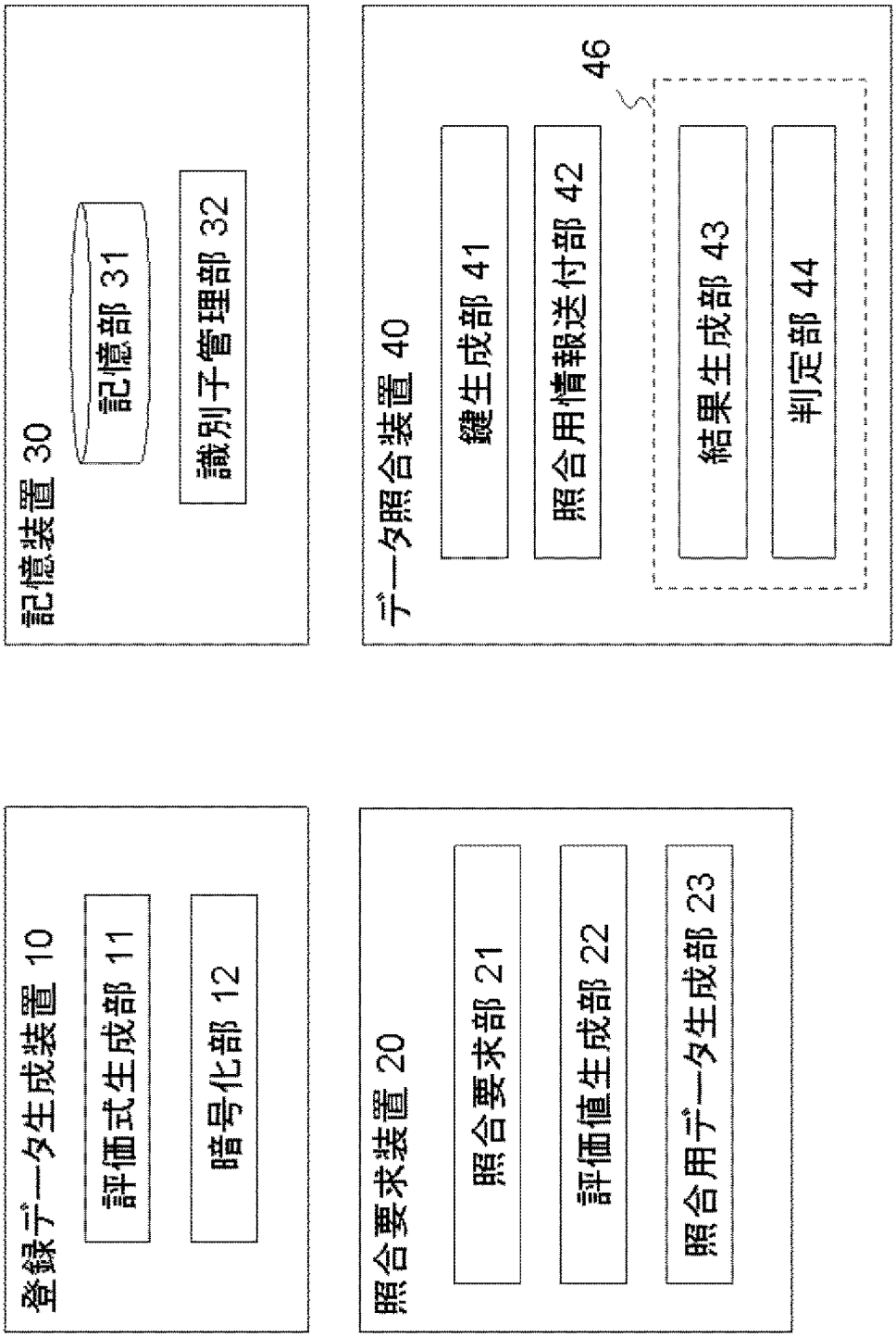
前記認証データと照合される被認証データを受信すると、暗号化された前記係数を前記第３のノードから取得して、前記被認証データおよび暗号化された前記係数に基づいて、前記被認証データを前記認証データと照合するための評価値を生成する処理と、

前記価値を前記第２のノードに送信する処理と、を第１のノードに設けられたコンピュータに実行させる、プログラム。

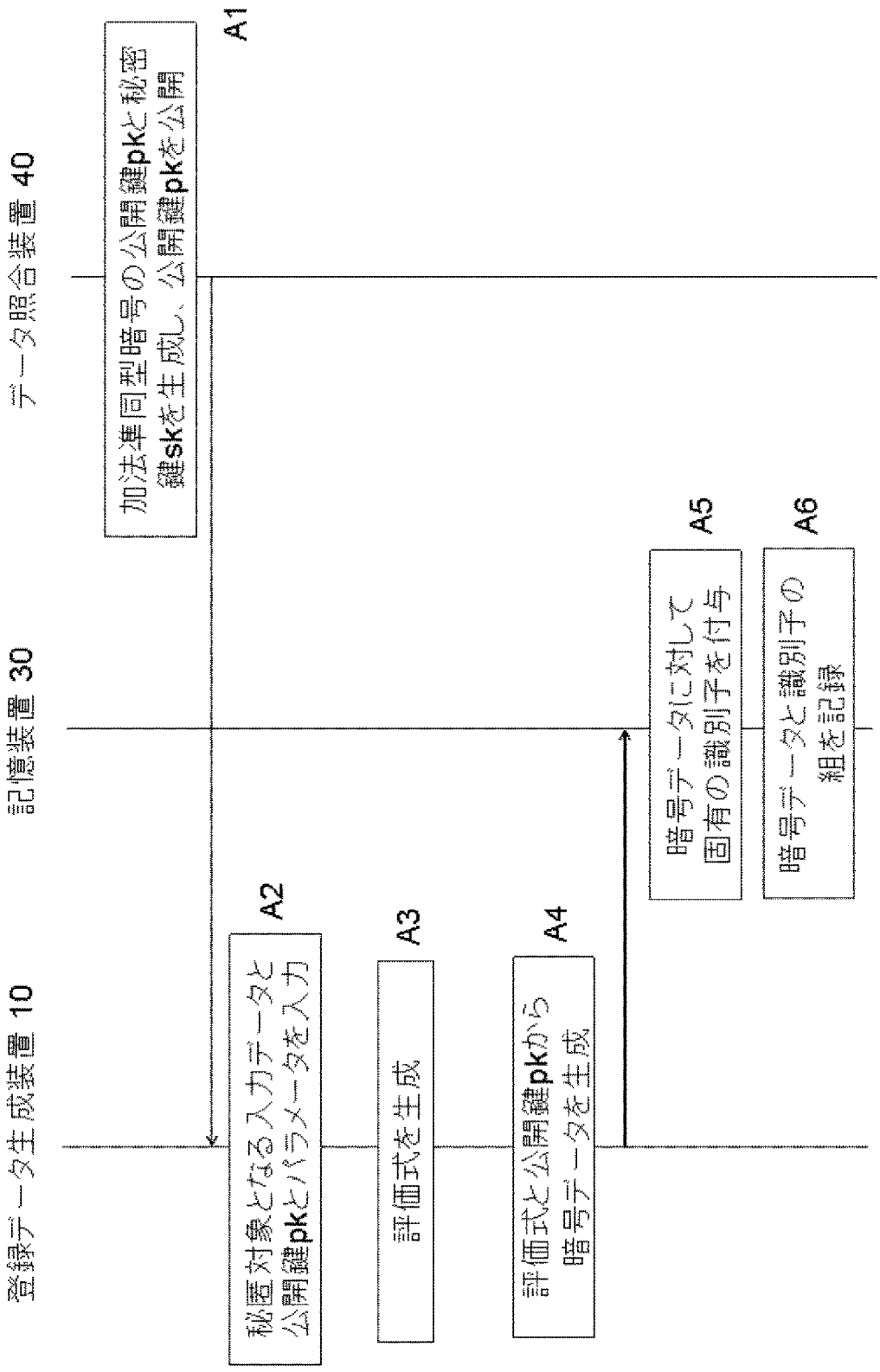
[図1]


130
120
110
ノード
記憶部
31
ノード
鍵生成部
41
照合部
46
ノード
評価式
生成部
11
暗号化部
12
評価値
生成部
22

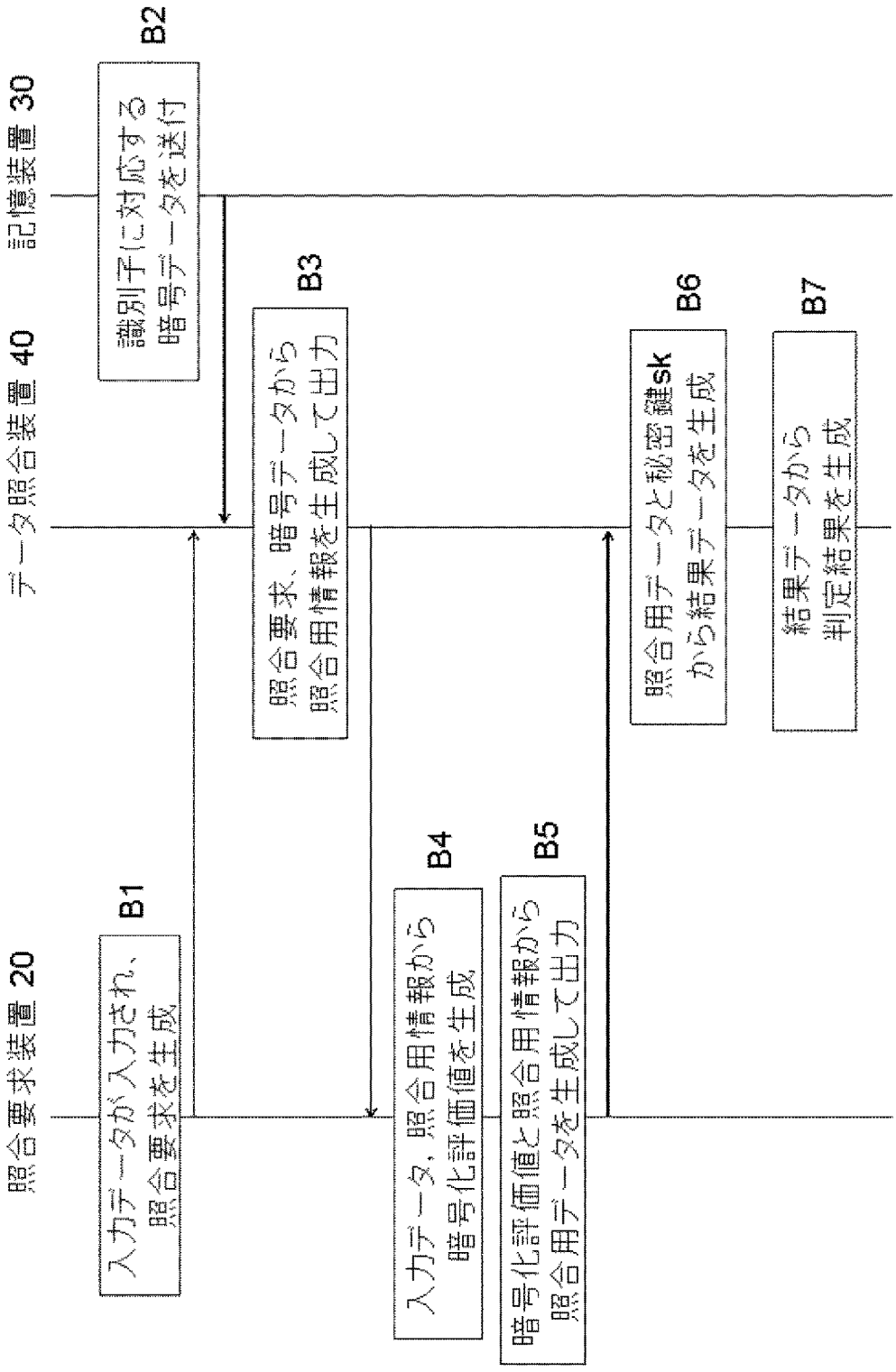
[図2]


登録データ生成装置 10
評価式生成部 11
暗号化部 12
記憶装置 30
記憶部 31
識別子管理部 32
照合要求装置 20
照合要求部 21
評価値生成部 22
照合用データ生成部 23
データ照合装置 40
鍵生成部 41
照合用情報送付部 42
結果生成部 43
判定部 44
46

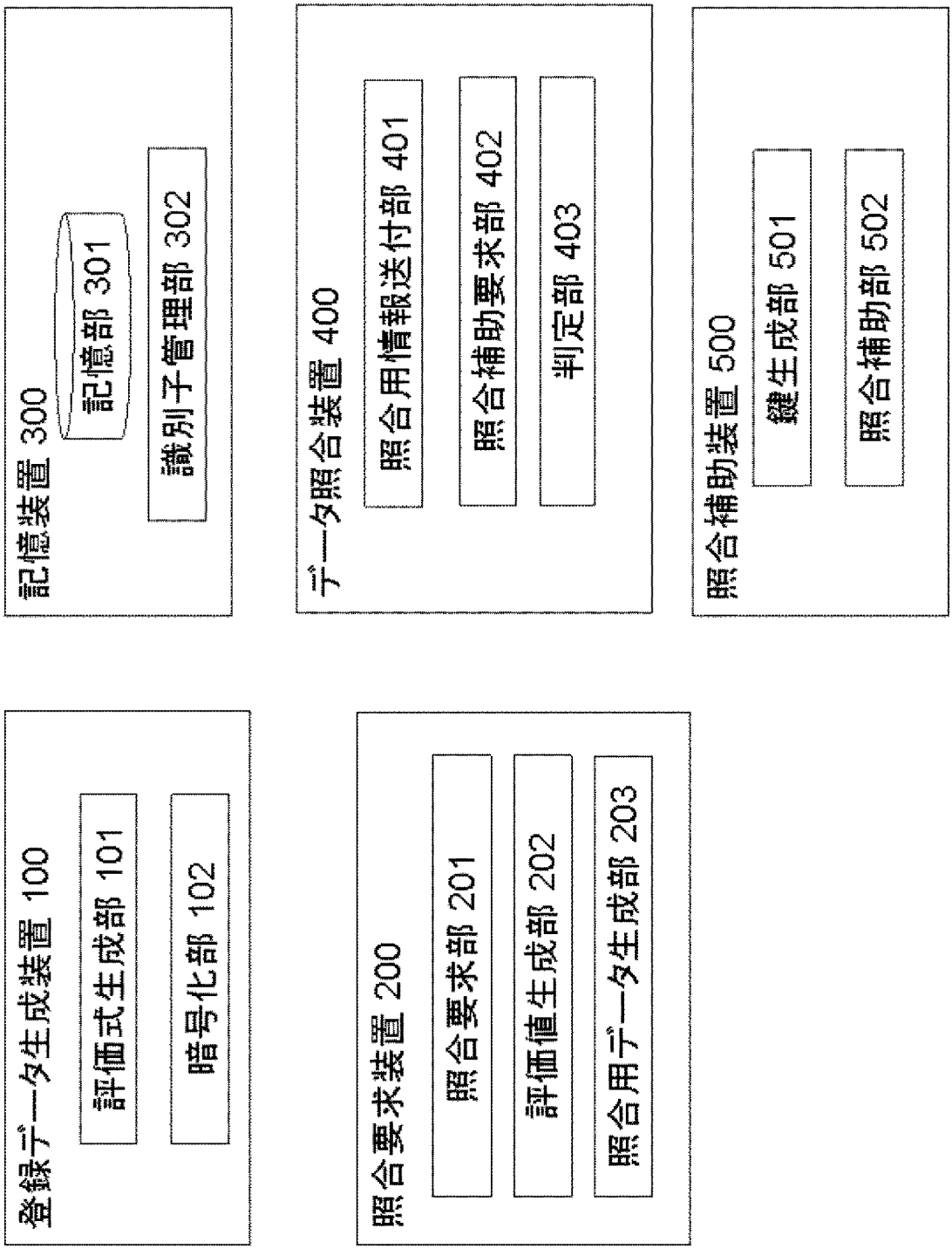
[図3]


データ照合装置 40
記憶装置 30
登録データ生成装置 10
A1
加法準同型暗号の公開鍵pkと秘密鍵skを生成し、公開鍵pkを公開
A2
秘匿対象となる入力データと公開鍵pkとパラメータを入力
A3
評価式を生成
A4
評価式と公開鍵pkから暗号データを生成
A5
暗号データに対して固有の識別子を付与
A6
暗号データと識別子の組を記録

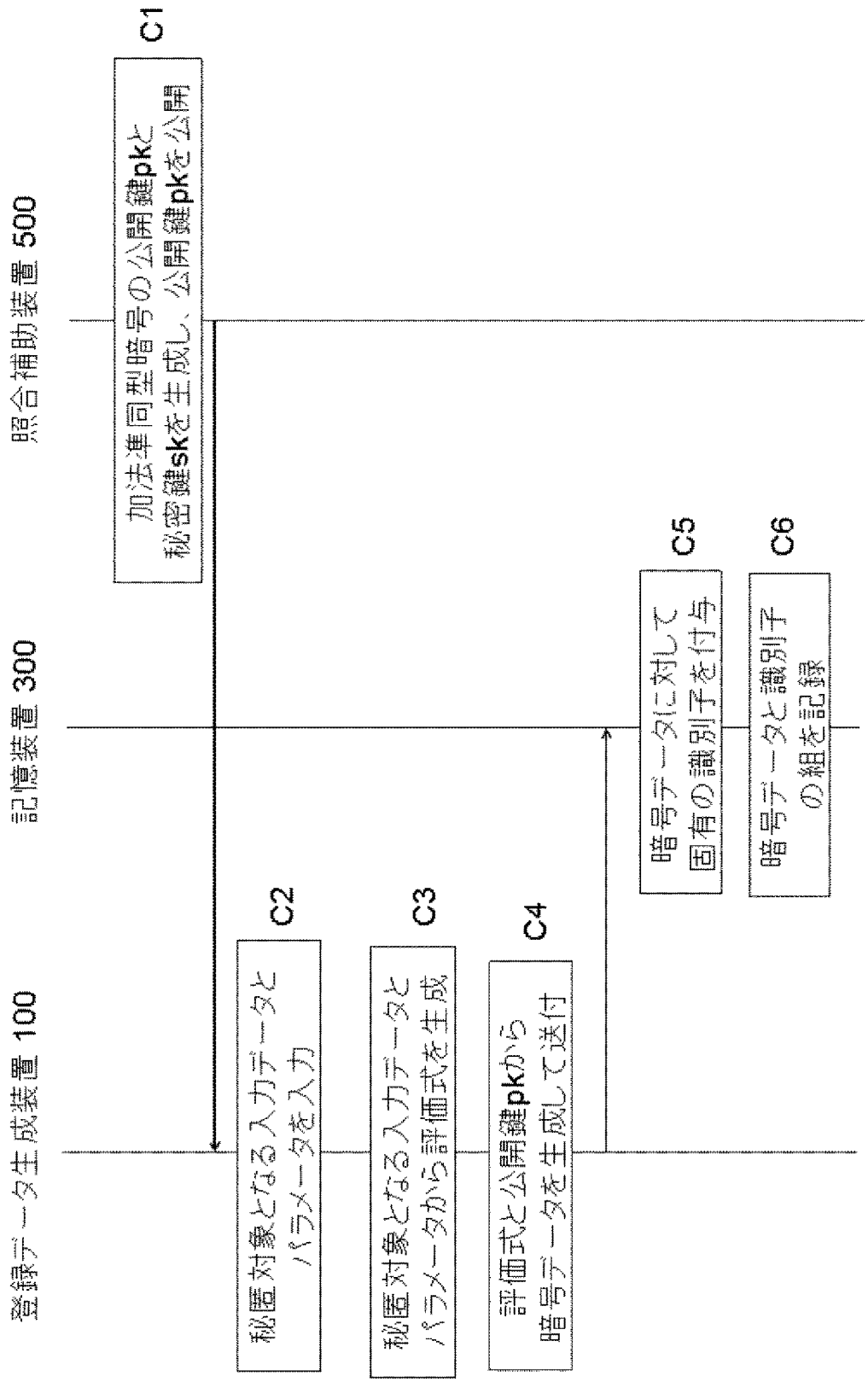
[図4]


照合要求装置 20
データ照合装置 40
記憶装置 30
B1
入力データが入力され、照合要求を生成
B2
識別子に対応する暗号データを送付
B3
照合要求、暗号データから照合用情報を生成して出力
B4
入力データ、照合用情報から暗号化評価値を生成
B5
暗号化評価値と照合用情報から照合用データを生成して出力
B6
照合用データと秘密鍵skから結果データを生成
B7
結果データから判定結果を生成

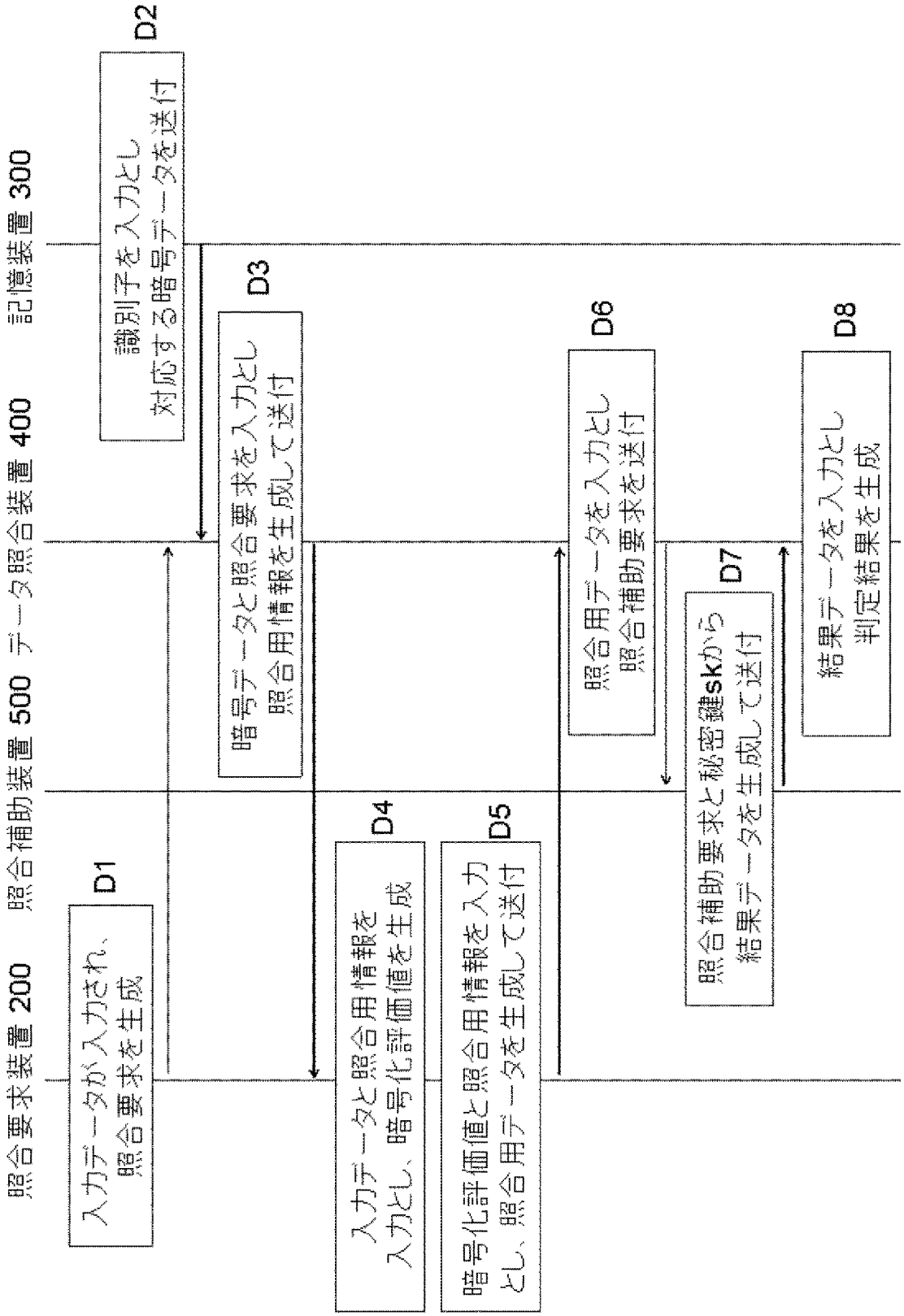
[図5]


記憶装置 300
記憶部 301
識別子管理部 302
データ照合装置 400
照合用情報送付部 401
照合補助要求部 402
判定部 403
照合補助装置 500
鍵生成部 501
照合補助部 502
登録データ生成装置 100
評価式生成部 101
暗号化部 102
照合要求装置 200
照合要求部 201
評価値生成部 202
照合用データ生成部 203

[図6]


照合補助装置 500
記憶装置 300
登録データ生成装置 100
C1
加法準同型暗号の公開鍵pkと
秘密鍵skを生成し、公開鍵pkを公開
C2
秘匿対象となる入力データと
パラメータを入力
C3
秘匿対象となる入力データと
パラメータから評価式を生成
C4
評価式と公開鍵pkから
暗号データを生成して送付
C5
暗号データに対して
固有の識別子を付与
C6
暗号データと識別子
の組を記録

[図7]


照合要求装置 200
照合補助装置 500
データ照合装置 400
記憶装置 300
入力データが入力され、照合要求を生成
D1
識別子を入力とし対応する暗号データを送付
D2
暗号データと照合要求を入力とし照合用情報を生成して送付
D3
入力データと照合用情報を入力とし、暗号化評価値を生成
D4
暗号化評価値と照合用情報を入力とし、照合用データを生成して送付
D5
照合用データを入力とし照合補助要求を送付
D6
照合補助要求と秘密鍵skから結果データを生成して送付
D7
結果データを入力とし判定結果を生成
D8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2014/062815

A. CLASSIFICATION OF SUBJECT MATTER
H04L9/32(2006.01)i, *G06F21/31*(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)
H04L9/32, G06F21/31

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	1996-2014
Kokai Jitsuyo Shinan Koho	1971-2014	Toroku Jitsuyo Shinan Koho	1994-2014

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2012/056582 A1 (Hitachi, Ltd.), 03 May 2012 (03.05.2012), paragraphs [0029] to [0094]; fig. 3, 4 & US 2013/0212645 A1 & EP 2634955 A1 & CN 103155479 A	1-10
A	WO 2011/052056 A1 (Mitsubishi Electric Corp.), 05 May 2011 (05.05.2011), paragraphs [0025] to [0160] & US 2012/0207299 A1 & EP 2495908 A1 & CN 102598576 A	1-10

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

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

Date of the actual completion of the international search	Date of mailing of the international search report
30 July, 2014 (30.07.14)	12 August, 2014 (12.08.14)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2014/062815

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2008-521025 A (Koninklijke Philips Electronics N.V.), 19 June 2008 (19.06.2008), paragraphs [0008] to [0046] & JP 4938678 B & US 2009/0006855 A1 & EP 1815637 A1 & WO 2006/054208 A1 & CN 101057448 A	1-10
A	US 2009/0310779 A1 (PRIVYLINK PTE LTD.), 17 December 2009 (17.12.2009), paragraphs [0090] to [0137] & WO 2008/010773 A1 & SG 139580 A & AU 2007275938 A	1-10

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１４／０６２８１５

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, G06F21/31(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, G06F21/31

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	１９７１－２０１４年
日本国実用新案登録公報	１９９６－２０１４年
日本国登録実用新案公報	１９９４－２０１４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）

IEEE Xplore

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 2012/056582 A1 (株式会社日立製作所) 2012.05.03, 段落 0029-0094, 図 3,4 & US 2013/0212645 A1 & EP 2634955 A1 & CN 103155479 A	1-10
A	WO 2011/052056 A1 (三菱電機株式会社) 2011.05.05, 段落 0025-0160 & US 2012/0207299 A1 & EP 2495908 A1 & CN 102598576 A	1-10

☑　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	国際調査報告の発送日
３０．０７．２０１４	１２．０８．２０１４

国際調査機関の名称及びあて先
日本国特許庁（ＩＳＡ／ＪＰ）
郵便番号１００－８９１５
東京都千代田区霞が関三丁目４番３号

特許庁審査官（権限のある職員）　５Ｓ　４５３８
金沢　史明
電話番号　０３－３５８１－１１０１　内線　３５４６

C（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
A	JP 2008-521025 A（コーニンクレッカ フィリップス エレクトロニクス エヌ ヴィ）2008.06.19, 段落 0008-0046 & JP 4938678 B & US 2009/0006855 A1 & EP 1815637 A1 & WO 2006/054208 A1 & CN 101057448 A	1-10
A	US 2009/0310779 A1 (PRIVYLINK PTE LTD) 2009.12.17, 段落 0090-0137 & WO 2008/010773 A1 & SG 139580 A & AU 2007275938 A	1-10