(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6763378号
(P6763378)
(45)発行日　令和2年9月30日(2020.9.30)　(24)登録日　令和2年9月14日(2020.9.14)

(51)Int.Cl.　　F I
G09C 1/00 (2006.01)　G09C 1/00 650Z
H04L 9/32 (2006.01)　H04L 9/00 673D

請求項の数 8　(全 36 頁)

(21)出願番号　特願2017-524611 (P2017-524611)
(86)(22)出願日　平成28年6月14日 (2016.6.14)
(86)国際出願番号　PCT/JP2016/002865
(87)国際公開番号　WO2016/203762
(87)国際公開日　平成28年12月22日 (2016.12.22)
審査請求日　令和1年5月15日 (2019.5.15)
(31)優先権主張番号　特願2015-122751 (P2015-122751)
(32)優先日　平成27年6月18日 (2015.6.18)
(33)優先権主張国・地域又は機関
日本国(JP)

(73)特許権者　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(74)代理人　100109313
弁理士　机　昌彦
(74)代理人　100124154
弁理士　下坂　直樹
(72)発明者　一色　寿幸
東京都港区芝五丁目７番１号
日本電気株式会社内
(72)発明者　肥後　春菜
東京都港区芝五丁目７番１号
日本電気株式会社内

審査官　行田　悦資

最終頁に続く

(54)【発明の名称】暗号情報作成装置、暗号情報作成方法、暗号情報作成プログラム、及び、照合システム

(57)【特許請求の範囲】
【請求項１】
閾値に基づく範囲に含まれている第１値を算出し、準同型性を有する暗号方式に従い、算出した前記第１値を暗号化することによって、前記第１値が暗号化された第１暗号文を作成する範囲暗号手段と、
類似している程度を表す第２値が、前記暗号方式に従い暗号化された第２暗号文と、前記第１暗号文とに、前記暗号方式に従った演算を適用することによって、前記第１値と前記第２値とが加算された値が暗号化された第３暗号文を作成し、第１乱数が暗号化された第４暗号文を作成し、前記第３暗号文の第２乱数乗を算出し、算出した値と、前記第４暗号文とを掛け算した値を算出することによって、第５暗号文を作成し、作成した前記第５暗号文と、前記第１乱数とが関連付けされた比較情報セットを作成する演算手段と
を備える暗号情報作成装置。
【請求項２】
複数の前記比較情報セットを含む暗号化情報において、前記比較情報セットの並び順を、ランダム、または、擬似的にランダムに並び替える並び替え手段
をさらに備える請求項１に記載の暗号情報作成装置。
【請求項３】
前記演算手段は、前記第１暗号文と、前記第２暗号文とが掛け算された値を算出することによって、前記第３暗号文を作成する
請求項１または請求項２に記載の暗号情報作成装置。

【請求項４】
第１情報に含まれる第１要素が２乗された２乗値の総和を算出し、前記第１要素、及び、前記総和を暗号化することによって、該第１要素及び前記総和が暗号化された第１要素暗号文を作成する暗号手段と、
前記第１要素暗号文と、第２情報に含まれる第２要素の値とを用いて、前記暗号方式に従い、前記第１情報と、前記第２情報との間の距離を表す前記第２値が暗号化された前記第２暗号文を作成する暗号化距離手段と
を備える請求項１乃至請求項３のいずれかに記載の暗号情報作成装置。
【請求項５】
前記暗号化距離手段は、前記第１要素暗号文に含まれる前記第１要素の（－２×前記第２要素）乗を算出することによって第６暗号文を作成し、前記第６暗号文、前記第２要素の２乗の第２総和が暗号化された暗号文、及び、前記第１要素暗号文に含まれる前記総和が暗号化された暗号文を積算することによって、前記第２暗号文を作成する
請求項４に記載の暗号情報作成装置。
【請求項６】
請求項４または請求項５に記載の暗号情報作成装置と、
前記第３暗号文を復号することによって、前記第１値と前記第２値とが加算された前記値を算出し、算出した前記値が特定の条件を満たすか否かに基づき、前記第２情報が受け入れ可能であるか否かを判定する照合手段と
を備える照合システム。
【請求項７】
情報処理装置によって、閾値に基づく範囲に含まれている第１値を算出し、準同型性を有する暗号方式に従い、算出した前記第１値を暗号化することによって、前記第１値が暗号化された第１暗号文を作成し、類似している程度を表す第２値が前記暗号方式に従い暗号化された第２暗号文と、前記第１暗号文とに、前記暗号方式に従った演算を適用することによって、前記第１値と前記第２値とが加算された値が暗号化された第３暗号文を作成し、第１乱数が暗号化された第４暗号文を作成し、前記第３暗号文の第２乱数乗を算出し、算出した値と、前記第４暗号文とを掛け算した値を算出することによって、第５暗号文を作成し、作成した前記第５暗号文と、前記第１乱数とが関連付けされた比較情報セットを作成する暗号情報作成方法。
【請求項８】
閾値に基づく範囲に含まれている第１値を算出し、準同型性を有する暗号方式に従い、算出した前記第１値を暗号化することによって、前記第１値が暗号化された第１暗号文を作成する範囲暗号機能と、
類似している程度を表す第２値が前記暗号方式に従い暗号化された第２暗号文と、前記第１暗号文とに、前記暗号方式に従った演算を適用することによって、前記第１値と前記第２値とが加算された値が暗号化された第３暗号文を作成し、第１乱数が暗号化された第４暗号文を作成し、前記第３暗号文の第２乱数乗を算出し、算出した値と、前記第４暗号文とを掛け算した値を算出することによって、第５暗号文を作成し、作成した前記第５暗号文と、前記第１乱数とが関連付けされた比較情報セットを作成する演算機能と
をコンピュータに実現させる暗号情報作成プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、たとえば、照合対象である情報を照合する場合に参照する情報を作成する暗号情報作成装置等に関する。
【背景技術】
【０００２】
クラウドコンピューティング（以降、「クラウド」と表す）が普及するにつれ、クラウドにおける通信ネットワーク（以降、「ネットワーク」と表す）に接続された計算資源に

利用者のデータを格納し、格納されたデータを利用するデータサービスは、広まっている。該データサービスは、機密性の高いデータを管理することも多い。該データサービスは、管理しているデータが安全であることを保証する必要がある。

【０００３】

利用者が自由に通信接続可能（オープン）な通信ネットワークにおいて、データを安全に管理することは肝要である。このため、暗号化されたデータを暗号化されたまま管理し、該暗号化されたデータを復号することなく、検索や、統計処理等の処理を実行する技術の研究開発が活発である。

【０００４】

また、パスワード、または、磁気カードを用いた個人認証における脆弱性を利用した犯罪が頻発している。この結果、指紋、または、静脈等の生体が有する特徴（生体情報）に基づく認証情報を用いて、より安全性の高い認証を実現する生体認証技術が注目を集めている。生体認証技術は、生体情報を識別可能なテンプレートをデータベースに格納し、格納したテンプレートに基づき、認証すべき対象である生体情報が受理可能か否かを検証する。

【０００５】

指紋、静脈等の生体情報は、基本的に個々人で不変なデータとされている。このため、生体情報がデータベースの外部に漏洩した場合、その被害は、甚大である。したがって、生体情報は、高い機密性が要求される情報の一つである。

【０００６】

生体認証技術においては、他の認証技術と同様に、生体情報を登録した生体に、該生体と異なる生体がなりすますこと（すなわち、「なりすまし」）を防ぐ必要がある。たとえば、テンプレート保護型の生体認証技術は、上述したテンプレートを秘匿したまま認証することにより、たとえ、テンプレートが漏洩したとしても、該テンプレートに基づく「なりすまし」を防ぐ。

【０００７】

以降、特許文献１乃至特許文献９、非特許文献１、及び、非特許文献２を参照しながら、生体認証技術に関連している技術について説明する。

【０００８】

特許文献１に開示された方式は、指紋の隆線の形状を表す座標値を含むにデータに、ランダムな座標値を付加することにより、該データが秘匿であるテンプレートを作成する。該方式は、該テンプレートに基づき、生体認証を実行する。

【０００９】

特許文献２に開示された照合システムは、信頼できる第三者による介入を導入することにより、該照合システムに関する機密情報が格納されたサーバーに登録されているデータを秘匿する。しかし、該照合システムによれば、照合処理における第三者の負荷が大きい。

【００１０】

特許文献３に開示された技術によれば、信頼できる第三者による介入を導入したシステムにおいて、照合処理における第三者の負荷は、特許文献２に開示された照合システムに比べて軽減される。しかし、特許文献３に開示された技術によれば、距離の指標としてユークリッド距離を利用する場合に、登録されるデータのサイズは、許容される曖昧さを表す指標の４乗に比例して増大する。

【００１１】

特許文献４に開示された方式は、データベースに格納される暗号データのサイズが、許容される曖昧さのパラメータに依存せず、かつ、第三者の負荷が軽い方式である。該方式によれば、該暗号データから平文データに復号する、及び、照合する対象データから平文データに復号することが可能である。該方式は、格納されている平文データと、照合する対象である平文データとの距離を算出し、算出した距離に基づき照合処理を実行する。

【００１２】

特許文献５に開示された暗号文照合システムは、記憶装置に登録された第１の暗号文と、照合対象である第２の暗号文とに対して、それぞれ、補助データを生成し、生成した補助データに対応する平文のハミング距離を算出する。該暗号文照合システムは、算出したハミング距離が所定値以下であるか否かに基づき、第２の暗号文に関する照合処理を実行する。

【００１３】

特許文献６に開示された個人認証システムは、パスワードと、該パスワードとは異なる語であるスクランブル要素とを記憶しており、認証時に、該パスワードと、スクランブル要素とを表示する。該個人認証システムは、利用者が、表示したスクランブル要素、または、パスワードのうち、パスワードのみを選択した場合に、該利用者を認証する。

【００１４】

特許文献７に開示された暗号処理装置は、複数の数値からなる第１ベクトルと、複数の数値からなる第２ベクトルとの暗号化秘匿距離を算出する。該暗号処理装置は、まず、該第１ベクトルに関する第１の重みと、該第２ベクトルに関する第２の重みとを算出する。該暗号処理装置は、算出した第１の重みと、第２の重みとを、準同型性を有する暗号方式に従い暗号化し、暗号化された第１の重み、及び、暗号化された第２の重みに基づき、該第１ベクトルと、該第２ベクトルとの暗号化秘匿距離を算出する。

【００１５】

特許文献８に開示された匿名化データ生成装置は、データブロックに含まれる複数の数値を含む数値属性値に関して、該数値属性値に含まれている各数値を加減することによって、該数値属性値から所定の距離以内である数値属性値の集合を表すデータブロックの集合を作成する。

【００１６】

特許文献８において、係るデータブロックは、機密属性値、及び、数値属性値を含む。該匿名化データ生成装置は、作成したデータブロックの集合に含まれる各データブロックと、該機密属性値との度数分布を算出し、算出した度数分布が所定の条件を満たしているか否かを判定する。該匿名化データ生成装置は、所定の条件を満たしているデータブロックに含まれる数値属性値を、該所定の距離以内の数値属性値にて置換する。

【００１７】

特許文献９に開示された情報授受伝達装置において、送り手は、問い合わせに応じて、該問い合わせに対する応答を、公開鍵を用いて暗号化し、暗号化された応答を受け手に送信する。受け手は、該応答を受信し、該応答を、秘密鍵を用いて復号する。

【００１８】

非特許文献１に開示された方式は、準同型性を有する公開鍵暗号を用いて、サーバーに格納されている生体情報の機密性を確保する。

【００１９】

非特許文献１は、認証要求しているクライアントの生体情報を秘匿可能な生体認証方式を開示する。該生体認証方式は、Ａｉｄｅｄ＿Ｃｏｍｐｕｔａｔｉｏｎなる暗号プロトコル、及びＳｅｔ＿Ｉｎｔｅｒｓｅｃｔｉｏｎなる暗号プロトコルに従い認証処理を実行する。

【００２０】

非特許文献２に開示された秘匿指紋認証方式によれば、準同型暗号の代わりにＳｏｍｅｗｈａｔ準同型暗号と呼ばれる公開鍵暗号を利用する。該秘匿指紋認証方式によれば、登録されるデータのサイズは、許容される曖昧さの指標に関する２乗のオーダである。

【先行技術文献】

【特許文献】

【００２１】

【特許文献１】特開２００６－１５８８５１号公報
【特許文献２】国際公開第２０１４／１８５４５０号
【特許文献３】国際公開第２０１４／１８５４４７号

【特許文献４】国際公開第２０１２／１１４４５２号
【特許文献５】国際公開第２０１４／１７５３３４号
【特許文献６】国際公開第２００７／０６６３８５号
【特許文献７】特開２０１４－１２６８６５号公報
【特許文献８】特開２０１４－１０９９３４号公報
【特許文献９】特開２００６－２１０９６４号公報
【非特許文献】
【００２２】
【非特許文献１】「Ｐｒｉｖａｔｅ Ｆｉｎｇｅｒｐｒｉｎｔ Ｍａｔｃｈｉｎｇ」，Ｓｉａｍａｋ Ｆ. Ｓｈａｈａｎｄａｓｈｔｉ，Ｒｅｉｈａｎｅｈ Ｓａｆａｖｉ－Ｎａｉｎｉ，ａｎｄ Ｐｈｉｌｉｐ Ｏｇｕｎｂｏｎａ，ＡＣＩＳＰ２０１２.、ｐｐ ４２６－４３３
【非特許文献２】「テンプレートサイズの小さい秘匿指紋認証方式」，肥後，一色，森，尾花，暗号と情報セキュリティシンポジウム（ＳＣＩＳ２０１５），２０１５.
【発明の概要】
【発明が解決しようとする課題】
【００２３】
しかし、特許文献１乃至特許文献９、非特許文献１、または、非特許文献２に開示された、いずれの技術を用いたとしても、また、これらの技術を如何様に組み合わせたとしても、機密性を担保する必要があるデータが漏洩してしまう可能性がある。たとえば、機密性を担保する必要があるデータは、テンプレートと、対象データとの距離である。この理由は、認証対象を表す対象データと、テンプレートとの距離を照合に際して復号する必要があるので、その復号により生じるデータが漏洩する可能性があるからである。
【００２４】
すなわち、上述したような技術を用いた場合には、たとえ、認証対象を表す対象データと、テンプレートとの距離が秘匿化されたまま算出されたとしても、該秘匿化された距離を復号し、その結果、算出される値が所定の条件を満たすか否かが、該対象データを受理するか否かを決定する。従って、該技術によれば、たとえば、復号された距離に基づき、ヒルクライミング攻撃を受ける可能性がある。
【００２５】
そこで、本発明の主たる目的は、照合対象である情報と、参照すべき情報との、より安全な照合処理が可能になる情報を作成することができる暗号情報作成装置等を提供することである。
【課題を解決するための手段】
【００２６】
前述の目的を達成するために、本発明の一態様において、暗号情報作成装置は、
閾値に基づく範囲に含まれている第１値を算出し、準同型性を有する暗号方式に従い、算出した前記第１値を暗号化することによって、前記第１値が暗号化された第１暗号文を作成する範囲暗号手段と、
類似している程度を表す第２値が前記暗号方式に従い暗号化された第２暗号文と、前記第１暗号文とに、前記暗号方式に従った演算を適用することによって、前記第１値と前記第２値とが加算された値が暗号化された第３暗号文を作成する演算手段と
を備える。
【００２７】
また、本発明の他の見地として、暗号情報作成方法は、
閾値に基づく範囲に含まれている第１値を算出し、準同型性を有する暗号方式に従い、算出した前記第１値を暗号化することによって、前記第１値が暗号化された第１暗号文を作成し、類似している程度を表す第２値が前記暗号方式に従い暗号化された第２暗号文と、前記第１暗号文とに、前記暗号方式に従った演算を適用することによって、前記第１値と前記第２値とが加算された値が暗号化された第３暗号文を作成する。

【００２８】
さらに、同目的は、係る暗号情報作成プログラム、及び、そのプログラムを記録するコンピュータが読み取り可能な記録媒体によっても実現される。
【発明の効果】
【００２９】
本発明に係る暗号情報作成装置等によれば、照合対象である情報と、参照すべき情報との、より安全な照合処理が可能になる情報を作成することができる。
【図面の簡単な説明】
【００３０】
【図１】本発明の第１の実施形態に係る照合システムが有する構成を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セットアップフェーズにおける処理の流れを示すフローチャートである。
【図３】第１の実施形態に係る照合システムのデータ登録フェーズにおける処理の流れを示すフローチャートである。
【図４】第１の実施形態に係る照合システムの暗号文照合フェーズにおける処理の流れを示すフローチャートである。
【図５】本発明の第２の実施形態に係る照合システムが有する構成を示すブロック図である。
【図６】第２の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処理の流れを示すフローチャートである。
【図７】本発明の第３の実施形態に係る照合システムが有する構成を示すブロック図である。
【図８】第３の実施形態に係る照合システムのセットアップフェーズにおける処理の流れを示すシーケンス図である。
【図９】第３の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処理の流れを示すシーケンス図である。
【図１０】第３の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処理の流れを示すシーケンス図である。
【図１１】第４の実施形態に係る照合システムが有する構成を示すブロック図である。
【図１２】第４の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処理の流れを示すシーケンス図である。
【図１３】本発明の第５の実施形態に係る暗号情報作成装置が有する構成を示すブロック図である。
【図１４】第５の実施形態に係る暗号情報作成装置における処理の流れを示すフローチャートである。
【図１５】本発明の各実施形態に係る暗号情報作成装置または照合システムを実現可能な計算処理装置のハードウェア構成例を概略的に示すブロック図である。
【発明を実施するための形態】
【００３１】
はじめに、本願の各実施形態にて使用する演算子について説明する。
【００３２】
以降に示す式番号に示される式において、等号演算子「＝」を用いられることがあるが、該等号演算子は、該等号演算子を用いて結合される式（値）が等価であることを表す。また、各式の途中に記載された「・・・」は、該途中に含まれる同様の演算が省略されていることを表す。たとえば、「１＋・・・＋Ｎ」は、１からＮまでの整数値の総和演算を表す。また、たとえば、「Ｘ（１）＋・・・＋Ｘ（Ｎ）」は、１からＮまでの整数Ｉに関して、Ｘ（Ｉ）を足し合わせる演算を表す。たとえば、「１、・・・、Ｎ」は、１からＮまでの整数を表す。また、以降に示す式において、べき乗演算子「＾」が用いられることがある。たとえば、Ｑ＾Ｒは、ＱのＲ乗を表す。

【００３３】
次に、本願発明を適用可能な一例である生体認証装置に関して説明し、その後、本願発明に関連している技術について説明する。
【００３４】
次に、生体認証装置の一例について説明する。
【００３５】
生体認証装置は、生体情報（たとえば、指紋等の画像）において指紋の隆線を抽出し、抽出した隆線を表す特徴点（マニューシャ）を作成する。該生体認証装置は、作成したマニューシャを、認証する対象を表す対象情報を認証する場合に参照するテンプレートとして、サーバー等の情報処理装置に登録する。たとえば、２次元座標空間Ｘ－Ｙにおいて、マニューシャは、隆線に含まれる座標値（ｘ，ｙ）、該座標値における隆線の特徴を表すタイプ、及び、該座標値における隆線の方向を表す角度θを含む。ただし、θ、ｘ、及び、ｙは、実数を表す。該タイプは、たとえば、該座標値における隆線が端点であるタイプ、または、該座標値における該隆線が分岐点であるタイプ等を含む。たとえば、隆線の方向は、該座標値において、隆線の接線方向の傾きである。
【００３６】
該生体認証装置は、クライアントを認証する場合に、該クライアントの生体情報に基づき作成したマニューシャと、受理すべき生体情報に基づき作成したマニューシャとが整合しているか否かを判定する。たとえば、ある２つのマニューシャが整合する条件は、
（条件１）２つのマニューシャにおいて、タイプが一致している、
（条件２）２つのマニューシャにおいて、座標値の距離が所定の範囲以内である、
（条件３）２つのマニューシャにおいて、角度の差が所定の範囲以内である、
なる３つの条件である。より具体的に、２つのマニューシャが、（$type_1$，（x_1，y_1），θ_1）、（$type_2$，（x_2，y_2），θ_2）である場合に、該３つの条件は、たとえば、以下の３つである。
【００３７】
（条件１）$type_1$と$type_2$とが等しい、
（条件２）$0 \leqq ((x_1-x_2)^2+(y_1-y_2)^2) \leqq \delta_d$、
（条件３）$0 \leqq (\theta_1-\theta_2)^2 \leqq \delta_t$、
ただし、δ_d、δ_tは、受理可能であるか否かを判定する基準を表す閾値ｔ等のパラメータを表す。尚、θ_1、θ_2、x_1、x_2、y_1、及び、y_2は実数を表す。
【００３８】
条件２に示された例において、距離は、たとえば、２次元ユークリッド距離、Ｌ２ノルムを用いて計測される。条件３に示された例において、距離は、たとえば、１次元ユークリッド距離を用いて計測される。以降、説明の便宜上、上述した狭義の距離等を含む広義の距離をまとめて「ユークリッド距離」と表す。ユークリッド距離ｄ（ＱＡ，ＱＢ）は、たとえば、ＱＡとＱＢとの間の距離を表す。
【００３９】
次に、本願発明に関連している技術ついて説明する。まず、暗号プロトコルに関連する公開鍵暗号について説明する。
【００４０】
公開鍵暗号は、鍵を生成するアルゴリズム（鍵生成アルゴリズム）、生成した鍵を用いて暗号化するアルゴリズム（暗号化アルゴリズム）、及び、復号鍵を用いて暗号化された暗号データを復号するアルゴリズム（復号アルゴリズム）を含む。鍵生成アルゴリズムは、復号鍵の長さを設定するパラメータ等のセキュリティパラメータに基づき、公開鍵と、秘密鍵とを算出する確率的アルゴリズムである。暗号化アルゴリズムは、公開鍵を用いて、メッセージが暗号化された暗号文を算出する確率的アルゴリズムである。復号アルゴリズムは、秘密鍵を用いて暗号文を復号することによって、該暗号文が復号された復号結果を算出する決定的アルゴリズムである。
【００４１】

公開鍵暗号に含まれているアルゴリズムは、以下の鍵生成アルゴリズム、暗号化アルゴリズム、及び、復号アルゴリズムに示す３つのアルゴリズムを含む。すなわち、

・鍵生成アルゴリズムＫｅｙＧｅｎ：（１^{k}）→（ｐｋ，ｓｋ）、

・暗号化アルゴリズムＥｎｃ：（ｐｋ，Ｍ）→Ｃ、

・復号アルゴリズムＤｅｃ：（ｓｋ，Ｃ）→Ｍ、

ただし、１^{k}（すなわち、１がｋビット並んだビット列）は、セキュリティパラメータを表す。ｐｋは、公開鍵を表す。ｓｋは、秘密鍵を表す。Ｍは、入力されたメッセージを表す。Ｃは、暗号文を表す。Ｅｎｃは、暗号化する処理を表す。Ｄｅｃは、復号する処理を表す。右向きの矢印によって示される演算子「→」の左側は、入力を表し、演算子「→」の右側は該入力の場合に算出される出力を表す。

【００４２】

公開鍵暗号のうち、式１に示す条件を満足する方式は、準同型性を有する公開鍵暗号と呼ばれる。すなわち、

$Enc(pk, M_1 \# M_2) = Enc(pk, M_1) @ Enc(pk, M_2)$・・・（式１）、

ただし、＃、及び、@は、それぞれ異なる、ある演算子を表す。また、$Ｍ_{1}$、及び、$Ｍ_{2}$は、それぞれ、メッセージを表す。

【００４３】

次に、暗号プロトコルのうち、準同型性を有する公開鍵暗号の一例であるＰａｉｌｌｉｅｒ暗号について説明する。

【００４４】

説明の便宜上、（Ｑ）ｍｏｄ（Ｒ）は、ＱをＲにて割り算した場合の剰余を算出する演算を表すとする。Ｑ、Ｒは、整数を表す。$Ｚ_{\{ｎ^{2}\}}$は、０からｎ^{2}－１までの整数のうち、ｎ^{2}と互いに素である（すなわち、最大公約数が１である）数の集合を表すとする。演算子「／」は、逆数を表すとする。たとえば、「１／Ｑ」は、Ｑの逆数を表す。また。たとえば、「Ｑ／Ｒ」は、Ｑに、Ｒの逆数を掛け算した値を表す。

【００４５】

たとえば、Ｐａｉｌｌｉｅｒ暗号は、式１における演算子「@」を乗算演算子、及び、式１における演算子「＃」を加算（加法）演算子とする公開鍵暗号の一例である。すなわち、Ｐａｉｌｌｉｅｒ暗号は、加法に関して準同型性を有する公開鍵暗号の一例である。

【００４６】

より具体的に、Ｐａｉｌｌｉｅｒ暗号は、以下の鍵生成アルゴリズム、暗号化アルゴリズム、及び、復号アルゴリズムを含む。

【００４７】

（鍵生成アルゴリズム）：セキュリティパラメータ１^{k}を入力として受信する。ｋビットの素数ｐ、及び、素数ｑをランダムに選び、ｐ×ｑ（＝ｎと表す）を算出する。算出したｎを用いて、（（１＋ｎ）ｍｏｄ（ｎ^{2}））（＝ｇとする）を算出する。（ｎ，ｇ）を公開鍵ｐｋとして算出する。（ｐ，ｑ）を秘密鍵ｓｋとして算出する。

【００４８】

（暗号化アルゴリズム）：公開鍵ｐｋ、及び、メッセージＭを入力として受信する。$Ｚ_{\{ｎ^{2}\}}$からランダムにｒを選ぶ。（（１＋ｍ×ｎ）×ｒ^{n}）ｍｏｄ（ｎ^{2}））を算出し、算出した値を暗号文Ｃとして設定する。

【００４９】

（復号アルゴリズム）：秘密鍵ｓｋ、及び、暗号文Ｃを入力として受信する。（ｐ－１）×（ｑ－１）（算出した値をλとする）を算出する。（（ｃ$^{\{\lambda\}}$）ｍｏｄ（ｎ^{2}－１））／（（（ｇ$^{\{\lambda\}}$）ｍｏｄ（ｎ^{2}－１））ｍｏｄ（ｎ））を算出し、算出した結果を平文ｍとして出力する。

【００５０】

次に、Ｐａｉｌｌｉｅｒ暗号が準同型性を有する理由について説明する。

【００５１】

ここでは、一例として、暗号文Ｃ１を式２に従い定義する。また、暗号文Ｃ２を式３に従い定義する。

【００５２】

$C1=Enc(pk, M_1)=((1+M_1\times n)\times r1^n) \bmod (n^2)$・・・（式２）、

$C2=Enc(pk, M_2)=((1+M_2\times n)\times r2^n) \bmod (n^2)$・・・（式３）。

【００５３】

この場合に、Ｃ１、及び、Ｃ２が掛け算された値を算出することによって、式４が成り立つ。すなわち、

$$C1\times C2=((1+(M_1+M_2)\times n+M_1\times M_2\times n^2)\times(r1\times r2)^n) \bmod (n^2)$$
$$=((1+(M_1+M_2)\times n)\times(r1\times r2)^n) \bmod (n^2)$$
$$=Enc(pk, M_1+M_2)$$・・・（式４）。

【００５４】

式４によって、「$Enc(pk, M_1)\times Enc(pk, M_2)=Enc(pk, M_1+M_2)$」が満たされるので、式１に異なる２種類の演算子（＃、@）を用いて示した準同型性の条件が満たされる。したがって、Ｐａｉｌｌｉｅｒ暗号は、準同型性を有する。換言すれば、本例において準同型性とは、メッセージM_1と、メッセージM_2との加算結果が暗号化された暗号文が、メッセージM_1が暗号化された暗号文、及び、メッセージM_2が暗号化された暗号文が掛け算された暗号文に等しいことを表す。すなわち、準同型性を利用すれば、暗号文を復号することなく秘匿したままの状態で、メッセージに関する処理を実行することができることを表す。

【００５５】

次に、本願発明に関連している技術の一例である暗号プロトコルのうち、Ｓｅｔ＿Ｉｎｔｅｒｓｅｃｔｉｏｎについて説明する。Ｓｅｔ＿Ｉｎｔｅｒｓｅｃｔｉｏｎは、エンティティＡｌｉｃｅと、エンティティＢｏｂとの間にて用いられる暗号プロトコルである。たとえば、Ａｌｉｃｅは、クライアントを表し、Ｂｏｂは、サーバーを表す。この暗号プロトコルに関して以下に説明する。

【００５６】

Ａｌｉｃｅは、あるデータａを有し、Ｂｏｂは、データの集合Ｂを有するとする。この場合に、Ｓｅｔ＿Ｉｎｔｅｒｓｅｃｔｉｏｎは、データａをＢｏｂに秘匿したまま、データａが集合Ｂに含まれているか否かを判定するプロトコルを表す。

【００５７】

説明の便宜上、集合Ｂを$\{b_1, b_2, b_3\}$とする場合を例として、Ｓｅｔ＿Ｉｎｔｅｒｓｅｃｔｉｏｎを説明する。Ｂｏｂは、加法に関して準同型性を有する公開鍵暗号に従った公開鍵ｐｋを公開し、その公開鍵ｐｋにて暗号化した暗号文を復号可能な秘密鍵ｓｋを保持しているとする。

【００５８】

Ｂｏｂは、ｘの値がb_1、b_2、または、b_3である場合に０であり、ｘが、その他の値である場合に、０以外の値である条件を満たす多項式Ｆ（ｘ）を作成する。Ｂｏｂは、多項式Ｆ（ｘ）として、たとえば、$(x-b_1)\times(x-b_2)\times(x-b_3)$を作成する。Ｂｏｂは、ラグランジェ補間に基づき、多項式Ｆ（ｘ）を作成することができる。ここでは、該ラグランジェ補間に関する説明自体は省略する。

【００５９】

一般にｎ次多項式Ｆ（ｘ）について、各次数の項の係数をα［ｉ］（ただし、$0\leqq i\leqq n$）とする。すなわち、この場合に、多項式は、式５として表される、

$F(x)=\alpha[n]\times x^n+\alpha[n-1]\times x^{\{n-1\}}+\cdots+\alpha[1]\times x+\alpha[0]$　・・・（式５）。

【００６０】

Ｂｏｂは、暗号鍵ｐｋに基づき、α［ｉ］（ただし、０≦ｉ≦ｎ）が暗号化された暗号文Ｃ［ｉ］を作成する。Ｂｏｂは、作成した暗号文Ｃ［ｉ］を、Ａｌｉｃｅに送信する。

【００６１】

Ａｌｉｃｅは、Ｂｏｂが送信した暗号文Ｃ［ｉ］を受信する。Ａｌｉｃｅは、データａがｉ乗（ただし、０≦ｉ≦ｎ）された値$a^{\{i\}}$を算出する。さらに、Ａｌｉｃｅは、受信した暗号文Ｃ［ｉ］の$a^{\{i\}}$乗を算出することにより、$C[i]^{\{a^{\{i\}}\}}$を算出する。

【００６２】

Ａｌｉｃｅは、式６に従い、算出した$C[i]^{\{a^{\{i\}}\}}$を用いて暗号文Ｃを算出する。すなわち、

$C=C[n]^{\{a^{\{n\}}\}}\times C[n-1]^{\{a^{\{n-1\}}\}}\times\cdots\times C[0]^{\{a^{\{0\}}\}}$・・・（式６）。

【００６３】

尚、式６は、以下に示す式変形によって、式７に示すＥｎｃ（ｐｋ，Ｆ（ａ））と等価であることがわかる。すなわち、

$C=Enc(pk,\alpha[n])^{\{a^{\{n\}}\}}\times\cdots\times Enc(pk,\alpha[0])^{\{a^{\{0\}}\}}$

$=Enc(pk,\alpha[n]\times a^{\{n\}})\times\cdots\times Enc(pk,\alpha[0]\times a^{\{0\}})$

$=Enc(pk,\alpha[n]\times a^{\{n\}}+\cdots+\alpha[0]\times a^{\{0\}})$

＝Ｅｎｃ（ｐｋ、Ｆ（ａ））・・・（式７）、

ただし、ｐｋは、ＡｌｉｃｅとＢｏｂとが参照可能な公開鍵ｐｋを表す。

【００６４】

Ａｌｉｃｅが算出した暗号文Ｃは、式７の通り、Ｅｎｃ（ｐｋ、Ｆ（ａ））である。さらに、Ａｌｉｃｅは、乱数ｒを算出し、算出した乱数ｒを用いて、暗号文Ｃが乱数ｒ乗した値$C^{\{r\}}$（以降、「ＣＰ」と表す）を算出する。この場合に、Ａｌｉｃｅは、たとえば、擬似乱数を算出する手順に従い、乱数ｒ（ただし、ｒは、０ではない実数）を算出する。Ａｌｉｃｅは、算出した値ＣＰを、Ｂｏｂに送信する。

【００６５】

Ｂｏｂは、該値ＣＰを受信し、受信した値ＣＰを、秘密鍵ｓｋを用いて復号することにより、該値ＣＰが復号された復号結果（すなわち、ｒ×Ｆ（ａ））を算出する。算出した復号結果が０である場合に、Ｆ（ａ）は０である。すなわち、ｘが、b_1、b_2、または、b_3である場合に多項式Ｆ（ｘ）が０であるので、ａは、b_1、b_2、または、b_3のいずれかに等しい。したがって、Ｂｏｂは、算出した復号結果が０である場合に、Ａｌｉｃｅが、Ｂに含まれるデータを有すると判定する。Ｂｏｂは、算出した復号結果が０以外である場合に、ＡｌｉｃｅがＢに含まれるデータを有していないと判定する。

【００６６】

説明の便宜上、上述したような、入力ａを有するＡｌｉｃｅと、集合Ｂ及び秘密鍵ｓｋを有するＢｏｂとを用いて実現されるＳｅｔ＿Ｉｎｔｅｒｓｅｃｔｉｏｎプロトコルを、ＳｅｔＩｎｔｅｒｓｅｃｔｉｏｎ［Ａｌｉｃｅ（ａ），Ｂｏｂ（Ｂ，ｓｋ）］（ｐｋ）と表す。上記のＳｅｔ＿Ｉｎｔｅｒｓｅｃｔｉｏｎプロトコルに関する表記法は、後述する説明において、該プロトコルを参照する場合に用いることとする。

【００６７】

次に、暗号プロトコルのうち、Ｓｅｔ＿Ｉｎｔｅｒｓｅｃｔｉｏｎプロトコルと、Ａｉｄｅｄ＿Ｃｏｍｐｕｔａｔｉｏｎプロトコルとに従い、認証処理を実行する認証方式の一例について説明する。尚、Ａｉｄｅｄ＿Ｃｏｍｐｕｔａｔｉｏｎプロトコル自体に関する説明を省略する。

【００６８】

該認証方式は、上記２つのプロトコルに従い、認証する対象であるクライアントに関するマニューシャ（$type_1$，（x_1，y_1），θ_1）と、テンプレート（$type_2$，

（x_2，y_2），θ_2）とを照合する方式である。該認証方式においては、たとえば、以下の処理Ｎ１乃至処理Ｎ３に示された処理に従い、認証処理が実行される。

【００６９】

・処理Ｎ１：２つのタイプ（すなわち、$type_1$、$type_2$）が一致するか否かを判定する。すなわち、Ｓｅｔ＿Ｉｎｔｅｒｓｅｃｔｉｏｎに関する説明にて、Ａｌｉｃｅがクライアントを表し、データａがタイプ$type_1$を表し、Ｂｏｂがサーバーを表し、集合Ｂがタイプ$type_2$を含む集合を表している、Ｓｅｔ＿Ｉｎｔｅｒｓｅｃｔｉｏｎプロトコルを実行する。すなわち、該プロトコルは、ＳｅｔＩｎｔｅｒｓｅｃｔｉｏｎ［クライアント（$type_1$）、サーバー（$type_2$，ｓｋ）］（ｐｋ）と表すことができる。

【００７０】

・処理Ｎ２：距離が受理されるか否かを算出する。すなわち、以下の処理（Ｎ２－１）乃至（Ｎ２－６）に従い処理に従い、距離が受理されるか否かを算出する。

【００７１】

処理（Ｎ２－１）：暗号化されたまま、座標値（x_1，y_1）及び座標値（x_2，y_2）と間のユークリッド距離を計算する。

【００７２】

処理（Ｎ２－２）：サーバーは、閾値δ_dに基づき、０からδ_dに至る値を含む集合Ｂを作成する。すなわち、サーバーは、Ｂ＝｛０，１，・・・，δ_d｝を作成する。次に、サーバーは、作成した集合Ｂに含まれる値にて０であり、該値以外の値にて０以外の値である多項式Ｆ（ｘ）を作成する。

【００７３】

処理（Ｎ２－３）：サーバーは、値x_2^2が暗号化された暗号文Ｅｎｃ（ｐｋ，x_2^2）、値x_2が暗号化された暗号文Ｅｎｃ（ｐｋ，x_2）、値y_2^2が暗号化された暗号文Ｅｎｃ（ｐｋ，y_2^2）、及び、値y_2が暗号化された暗号文Ｅｎｃ（ｐｋ，y_2）を算出する。サーバーは、算出した暗号文を、クライアントに送信する。

【００７４】

処理（Ｎ２－４）：クライアントは、該暗号文を受信する。クライアントは、値x_1^2が暗号化された暗号文Ｅｎｃ（ｐｋ，x_1^2），値y_1^2が暗号化された暗号文Ｅｎｃ（ｐｋ，y_1^2）を算出する。

【００７５】

処理（Ｎ２－５）：クライアントは、算出した暗号文、及び、受信した暗号文を用いて、該暗号文を掛け算した値Ｅｎｃ（ｐｋ，$(x_1-x_2)^2+(y_1-y_2)^2$）を、式１３に示すように、算出した値等を掛け算することによって算出する、

$$Enc(pk, x_1^2) \times \{Enc(pk, x_2)\}^{\{-2\times x_1\}} \times Enc(pk, x_2^2) \times Enc(pk, y_1^2) \times \{Enc(pk, y_2)\}^{\{-2\times y_1\}} \times Enc(pk, y_2^2) \cdots (式13)、$$

処理（Ｎ２－６）：Ａｌｉｃｅがクライアントを表し、データａが「$(x_1-x_2)^2+(y_1-y_2)^2$）」を表し、Ｂｏｂがサーバーを表し、集合Ｂが｛０，１，・・・，δ_d｝を表しているＡｉｄｅｄ＿Ｃｏｍｐｕｔａｔｉｏｎに従い処理が実行される。

【００７６】

・処理Ｎ３：サーバーは、角度（すなわち、θ_1、θ_2）が一致するか否かを、以下の処理（Ｎ３－１）乃至（Ｎ３－３）によって判定する。

【００７７】

処理（Ｎ３－１）：サーバーは、処理（Ｎ２－１）乃至処理（Ｎ２－６）に示された処理と同様の処理に従い、Ｅｎｃ（ｐｋ，$(\theta_1-\theta_2)^2$）を算出する、

処理（Ｎ３－２）：サーバーは、閾値δ_tに基づき、０からδ_tに至る値を含む集合ＢＰを作成する。すなわち、サーバーは、ＢＰ＝｛０，１，・・・，δ_t｝を作成する、

処理（Ｎ３－３）：サーバーは、作成した集合ＢＰに含まれる値にて０となる多項式Ｇ（ｘ）に関するＡｉｄｅｄ＿Ｃｏｍｐｕｔａｔｉｏｎに従い処理を実行する。

【００７８】

しかし、上述したＳｅｔ＿Ｉｎｔｅｒｓｅｃｔｉｏｎプロトコルと、Ａｉｄｅｄ＿Ｃｏｍｐｕｔａｔｉｏｎプロトコルとに従い認証処理を実行する認証方式によれば、照合におけるサーバーの負荷が大きいという課題がある。この理由は、サーバーがクライアントから送信されたデータの復号、及び、復号結果の再暗号化を行う必要があるからである。さらに、該認証方式によれば、サーバーに登録されているデータが平文であり、必ずしも、該データを秘匿することができないという課題、上述したステップにおいて算出した距離を秘匿できないという課題等ある。本発明の発明者は、上述したような課題を見出した。

【００７９】

次に、本願明細書の以下の説明において便宜上用いる用語である、登録データ、及び、対象データについて説明する。登録データは、秘匿する対象を表すデータであるとする。対象データは、登録データと照合する対象を表すとする。登録データは、たとえば、指紋照合におけるテンプレートを表す。対象データは、たとえば、クライアントを認証する場合に、該クライアントの生体情報に基づき作成されたマニューシャを表す。たとえば、指紋照合においては、クライアントから受信したマニューシャ（すなわち、対象データ）と、テンプレート（すなわち、登録データ）とが照合され、照合した結果に応じて、クライアントを受理（受け入れ）可能か否かが判定される。

【００８０】

以下の説明において、「受理」は、たとえば、登録データと、対象データとが類似している（または、一致している）場合に、該対象データを受け入れ可能であることを表す。

【００８１】

以下の説明では、便宜上、本願の各実施形態において、「距離」という言葉を用いて、処理を説明する。距離は、たとえば、対象データを構成する要素と、登録データを構成する要素とを用いて算出されるユークリッド距離を表す。ただし、距離なる文言でなくともよく、他の指標（対象データと、登録データとが類似している程度を表す類似度）であってもよい。

【００８２】

以降、上述したような課題を解決可能な、本発明を実施する実施形態について、図面を参照しながら、詳細に説明する。

【００８３】

＜第１の実施形態＞

図１を参照しながら、本発明の第１の実施形態に係る照合システム１０１が有する構成について詳細に説明する。図１は、本発明の第１の実施形態に係る照合システム１０１が有する構成を示すブロック図である。

【００８４】

第１の実施形態に係る照合システム１０１は、大別して、登録データ装置１０２と、照合要求装置１０３と、記憶装置１０４と、データ照合装置１０５と、照合補助装置１０６とを有する。

【００８５】

登録データ装置１０２は、暗号化部１０７を有する。

【００８６】

照合要求装置１０３は、照合要求部１１０と、暗号化距離部１１１と、距離集合部１１２と、シャッフル部１１３とを有する。

【００８７】

記憶装置１０４は、暗号文記憶部１０８と、識別子管理部１０９とを有する。

【００８８】

データ照合装置１０５は、照合情報送信部１１４と、照合補助依頼部１１５と、判定部１１６とを有する。

【００８９】
照合補助装置１０６は、鍵生成部１１７と、照合補助部１１８と、鍵記憶部１１９とを有する。尚、鍵記憶部１１９は、照合システム１０１において、照合補助装置１０６のみが参照することができるとする。
【００９０】
登録データ装置１０２と、照合要求装置１０３と、記憶装置１０４と、データ照合装置１０５と、照合補助装置１０６とは、たとえば、通信ネットワークを介して、相互に通信することが可能であるとする。
【００９１】
次に、上述したような構成を有する照合システム１０１における処理について詳細に説明する。本発明の各実施形態に係る照合システム１０１の動作は、セットアップフェーズと、データ登録フェーズと、暗号文照合フェーズとの３つのフェーズに大別される。まず、該３つのフェーズに含まれている処理に関して概略を説明する。
【００９２】
セットアップフェーズは、主として、前述した式１を参照して説明したような加法に関して準同型性を有する暗号方式に従い、入力されたセキュリティパラメータに基づき、暗号鍵と復号鍵とを作成するフェーズを表す。
【００９３】
データ登録フェーズは、主として、受信した登録データを暗号化する処理等によって作成された暗号化登録情報を、暗号文記憶部１０８に格納するフェーズを表す。
【００９４】
暗号文照合フェーズは、主として、登録データが秘匿されたままの状態において、対象データが、暗号文記憶部１０８に記憶されている暗号化登録情報に基づき、受理可能であるか否かを判定するフェーズである。
【００９５】
以上、上述した３つのフェーズにおける動作に関して、それぞれ、詳細に説明する。
【００９６】
まず、図２を参照しながら、第１の実施形態に係る照合システム１０１のセットアップフェーズにおける処理について説明する。図２は、第１の実施形態に係る照合システム１０１のセットアップフェーズにおける処理の流れを示すフローチャートである。
【００９７】
照合補助装置１０６における鍵生成部１１７は、たとえば、外部装置等から、作成する鍵の長さ等を指定する情報を含むセキュリティパラメータを受信する。鍵生成部１１７は、加法に関して準同型性を有する暗号に従い、受信したセキュリティパラメータに応じた暗号鍵と復号鍵とを作成する（ステップＡ１）。たとえば、鍵生成部１１７は、上述したＰａｉｌｌｉｅｒ暗号における鍵生成アルゴリズムに従い、暗号鍵と復号鍵とを作成する。鍵生成部１１７は、照合システム１０１において、作成した暗号鍵を公開する（ステップＡ２）。鍵生成部１１７は、作成した復号鍵を、照合補助装置１０６における鍵記憶部１１９に格納する（ステップＡ３）。
【００９８】
次に、図３を参照しながら、第１の実施形態に係る照合システム１０１のデータ登録フェーズにおける処理について説明する。図３は、第１の実施形態に係る照合システム１０１のデータ登録フェーズにおける処理の流れを示すフローチャートである。
【００９９】
登録データ装置１０２における暗号化部１０７は、たとえば、外部装置等から、秘匿する対象を表す登録データを受信する（ステップＢ１）。次に、暗号化部１０７は、照合補助装置１０６が作成した暗号鍵を用いて、登録データを暗号化する、さらに、暗号化部１０７は、登録データを構成している要素に基づいて登録データの大きさ（サイズ）を表す指標を算出し、算出した大きさを表す指標を暗号化する。たとえば、暗号化部１０７は、該大きさを表す指標として、該要素の２乗和を算出し、算出した和を暗号化する。暗号化

部１０７は、暗号化された登録データ、及び、暗号化された該指標を含む暗号情報を作成する（ステップＢ２）。暗号化部１０７は、作成した暗号情報を、記憶装置１０４における識別子管理部１０９に送信する。

【０１００】

記憶装置１０４における識別子管理部１０９は、暗号化部１０７が送信した暗号情報を受信し、受信した該暗号情報を識別可能な登録識別子を作成する（ステップＢ３）。識別子管理部１０９は、作成した登録識別子と、受信した暗号情報とが関連付けされた暗号化登録情報を作成し（ステップＢ４）、作成した暗号化登録情報を、記憶装置１０４における暗号文記憶部１０８に格納する。識別子管理部１０９は、登録識別子を、登録データ装置１０２に送信してもよい（ステップＢ５）。あるいは、識別子管理部１０９は、登録識別子を、ディスプレイ等のユーザインターフェース（ＵＩ）に表示してもよい。

【０１０１】

登録データ装置１０２は、識別子管理部１０９が送信した登録識別子を表示してもよい。

【０１０２】

次に、図４を参照しながら、第１の実施形態に係る照合システム１０１の暗号文照合フェーズにおける処理について説明する。図４は、第１の実施形態に係る照合システム１０１の暗号文照合フェーズにおける処理の流れを示すフローチャートである。

【０１０３】

照合要求装置１０３における照合要求部１１０は、たとえば、外部装置等から、登録識別子と、対象データとを受信する。照合要求部１１０は、暗号化登録情報において、受信した登録識別子に関連付けされた暗号情報を要求する照合要求を作成する（ステップＣ１）。照合要求部１１０は、作成した照合要求を、データ照合装置１０５における照合情報送信部１１４に送信する。受信した登録識別子を「ｉｎｄｅｘ」と表す場合に、照合要求部１１０が作成する照合要求は、たとえば、「ｒｅｑｕｅｓｔ＝（ｉｎｄｅｘ）」なる態様にて表すことができる。さらに、照合要求装置１０３における照合要求部１１０は、受信した対象データを、照合要求装置１０３における暗号化距離部１１１に出力する。

【０１０４】

データ照合装置１０５における照合情報送信部１１４は、照合要求部１１０が送信した照合要求を受信し、受信した該照合要求に含まれている登録識別子を読み取る。照合情報送信部１１４は、暗号化登録情報において、読み取った登録識別子に関連付けされている暗号情報を特定する（ステップＣ２）。照合情報送信部１１４は、特定した暗号情報を、照合要求装置１０３における暗号化距離部１１１に送信する（ステップＣ３）。

【０１０５】

照合要求装置１０３における暗号化距離部１１１は、照合要求装置１０３における照合要求部１１０が出力した対象データを入力し、さらに、照合情報送信部１１４が送信した暗号情報を受信する。暗号化距離部１１１は、式１を参照して前述したような、加法に関して準同型性を有する暗号方式に従う演算を、受信した対象データと、受信した暗号情報とに適用する。この処理によって、該暗号情報を復号することなく、該対象データと、該暗号情報の基を表す登録データとの距離が暗号化された暗号化距離を算出する（ステップＣ４）。

【０１０６】

たとえば、ステップＣ４において、暗号化距離部１１１は、受信した対象データの大きさを表す指標を算出し、算出した指標を暗号化する。次に、暗号化距離部１１１は、受信した暗号情報に含まれている暗号化された登録データに、該対象データに基づく所定の演算を適用することによって値を算出する。暗号化距離部１１１は、算出した値と、対象データに関して暗号化された大きさを表す指標と、受信した暗号情報に含まれている暗号化された大きさを表す指標とを積算することによって、該暗号化距離を算出する。

【０１０７】

暗号化距離部１１１は、算出した暗号化距離を、照合要求装置１０３における距離集合

部１１２に出力する。

【０１０８】

尚、説明の便宜上、暗号化距離部１１１は、対象データと、登録データとの距離を算出するとしたが、距離である必要はなく、他の指標（対象データと、登録データとが類似している程度を表す類似度）であってもよい。上述の各実施形態においても同様である。

【０１０９】

照合要求装置１０３における距離集合部１１２は、暗号化距離部１１１から暗号化距離を入力する。距離集合部１１２は、対象データを受理可能か否かを判定する基準を表す閾値ｔを読み取る。距離集合部１１２は、読み取った該閾値ｔに基づいて区画される範囲に含まれる値（説明の便宜上、「第１値」と表す）を算出し、算出した第１値の負数が暗号化された暗号文を、暗号鍵を用いて作成する。たとえば、距離集合部１１２は、（－閾値ｔ）乃至０に含まれている整数値を、該第１値として算出する。あるいは、距離集合部１１２は、たとえば、（－閾値ｔ）乃至「－１」に含まれている整数値を、該第１値として算出する。距離集合部１１２は、受信した暗号化距離と、該暗号文とが掛け算された値を算出する。この場合に、距離集合部１１２が算出した値は、対象データと、暗号情報の基である登録データとの距離に、第１値が引かれた値が暗号化された値（説明の便宜上、「第２値」と表す）である。すなわち、距離集合部１１２は、１つ以上の第２値を算出する。尚、第１値及び第２値は、後述する実施形態を説明する場合に参照する値である。

【０１１０】

距離集合部１１２は、算出した第２値に対して、たとえば、擬似乱数を算出する手順に従い、２つの乱数（説明の便宜上、「第１乱数」、「第２乱数」と表す）を作成する。距離集合部１１２は、第１乱数を、公開鍵を用いて暗号化することによって、該第１乱数が暗号化された暗号文を作成する。次に、距離集合部１１２は、作成した第２値が「第２乱数」乗された値を算出し、さらに、算出した値に、第１乱数が暗号化された暗号文を掛け算した暗号文（説明の便宜上、「第３値」と表す）を算出する。距離集合部１１２は、算出した第３値と、暗号化されていない乱数とが関連付けされた比較情報セットを作成する。距離集合部１１２は、作成した１つ以上の第２値に関する比較情報セットを含む暗号化距離情報（または、暗号化情報）を作成する（ステップＣ５）。距離集合部１１２は、作成した暗号化距離情報を、照合要求装置１０３におけるシャッフル部１１３に出力する。

【０１１１】

尚、距離集合部１１２は、算出した第２値に対して、必ずしも、２つの乱数を作成する必要はなく、１つの乱数であってもよい。この場合に、距離集合部１１２は、作成した第２値が「暗号化されていない乱数の値」乗した値を算出し、算出された値を含む暗号化距離情報を作成してもよい。すなわち、距離集合部１１２が作成する手順は、上述した処理手順に限定されない。

【０１１２】

照合要求装置１０３におけるシャッフル部１１３は、距離集合部１１２が出力した暗号化距離情報を入力する。シャッフル部１１３は、受信した暗号化距離情報において、該暗号化距離情報に含まれている比較情報セットの並び順をランダムに並び替えることによって、該暗号化距離情報に含まれている要素がランダムに並べられているランダム距離情報を作成する（ステップＣ６）。ここで、ランダムに並び替えるとは、たとえば、擬似的に生成される擬似乱数に従い並び順を変えることを表してもよい。シャッフル部１１３は、作成したランダム距離情報を、データ照合装置１０５における照合補助依頼部１１５に出力する。

【０１１３】

データ照合装置１０５における照合補助依頼部１１５は、シャッフル部１１３が出力したランダム距離情報を入力し、受信したランダム距離情報に関する照合処理を実行することを要求する照合補助要求を作成し、作成した照合補助要求を、照合補助装置１０６における照合補助部１１８に送信する（ステップＣ７）。たとえば、照合補助要求は、ランダム距離情報を含む情報として実現することができる。

【０１１４】
照合補助装置１０６における照合補助部１１８は、照合補助依頼部１１５が送信した照合補助要求を受信する。次に、照合補助部１１８は、鍵記憶部１１９から復号鍵を読み取る。照合補助部１１８は、照合補助要求に含まれているランダム距離情報を読み取り、読み取った復号鍵を用いて、該ランダム距離情報を復号することによって、受信した該照合補助要求が復号された照合情報を作成する。照合補助部１１８は、作成した照合情報を、データ照合装置１０５における判定部１１６に送信する（ステップＣ８）。
【０１１５】
データ照合装置１０５における判定部１１６は、照合補助部１１８が送信した照合情報を受信する。判定部１１６は、受信した照合情報に含まれている比較情報セットに関して、第３値と、乱数とを読み取る。判定部１１６は、読み取った第３値と、読み取った乱数とが一致する要素を、該照合情報が含んでいる場合に、一致であることを表す照合結果情報を作成する（ステップＣ９）。判定部１１６は、該第３値と、該乱数とが一致する要素を、該照合情報が含んでいない場合に、不一致であることを表す照合結果情報を作成する。判定部１１６は、作成した照合情報を出力してもよい。
【０１１６】
尚、データ照合装置１０５における判定部１１６は、受信した照合情報に含まれている比較情報セットが１つの値のみを含む場合に、該値と０とが一致するか否かに基づき、照合結果情報を作成してもよい。たとえば、判定部１１６は、読み取った値と、０とが一致する要素を、該照合情報が含んでいる場合に、一致であることを表す照合結果情報を作成する。判定部１１６は、読み取った値と、０とが一致する要素を、該照合情報が含んでいない場合に、不一致であることを表す照合結果情報を作成する。
【０１１７】
次に、第１の実施形態に係る照合システム１０１に関する効果について説明する。
【０１１８】
第１の実施形態に係る照合システム１０１によれば、照合対象である情報と、参照すべき情報との、より安全な照合処理が可能になる情報を作成することができる。この理由は、照合処理において、対象データを受理可能か否かを判定する基準を表す閾値ｔに基づき区画される範囲に含まれる第１値と、対象データ及び登録データ間の距離とが加算された値が暗号化された第２値を、距離を復号することなく求めることができるからである。この場合に、照合システム１０１は、該距離を復号することなく、第２値を含む照合情報を作成する。
【０１１９】
照合補助部１１８は、該照合情報を受信し、受信した復号情報を復号することによって、第１値及び距離が加算された値を算出し、該値が所定の条件を満たすか否かに応じて、対象データを受理するか否かを判定する。すなわち、照合要求装置１０３において、対象データと、登録データとの距離は復号されない。この結果、復号された距離に基づき、テンプレートを復元するヒルクライミング攻撃を受ける可能性はなくなる。
【０１２０】
さらに、本実施形態に係る照合システム１０１によれば、照合対象である情報と、参照すべき情報とを、より安全に照合することができる。この理由は、図３のステップＢ４等に関する説明に示したように、記憶装置１０４が、暗号化された登録データ、及び、暗号化された大きさを表す指標を記憶しているからである。したがって、たとえ、記憶装置１０４に格納されたデータが傍受されたとしても、該データが暗号化されているので、本実施形態に係る照合システム１０１によれば、登録データが漏洩してしまうリスクを低減することができる。
【０１２１】
さらに、図３のステップＣ４等に関する説明に示したように、照合要求装置１０３は、登録データ装置１０２にて算出された暗号情報に対して演算処理を実行することにより、対象データと、登録データとの間の暗号化距離を算出する。さらに、ステップＣ５等に関

する説明に示したように、照合要求装置１０３は、算出した暗号化距離を用いて乱数倍等の値を算出する。この処理の結果算出される暗号情報は、対象データと、登録データとの距離とは異なる値を含む情報である。この結果、たとえ、照合補助装置１０６が、該暗号情報に含まれる情報を復号したとしても、算出される値は、該対象データと、登録データとの距離とは異なる。したがって、実施形態に係る照合システム１０１によれば、登録データが漏洩してしまうリスクを低減することができる。

【０１２２】

第１の実施形態に係るシャッフル部１１３によれば、より一層、安全な照合処理が可能である。この理由は、シャッフル部１１３が、要素の順序を並び替えることによって、異なる照合情報を作成することができるからである。たとえば、シャッフル部１１３がランダムに要素の順序を並び替えることによって、照合システム１０１は、認証処理のたびに、異なる照合情報を作成する。この場合に、たとえ、照合情報が傍受されたとしても、第１の実施形態に係る照合システム１０１によれば、傍受された照合情報に基づきテンプレートを作成することはより困難である。

【０１２３】

さらに、第１の実施形態に係るシャッフル部１１３によれば、より一層、安全な照合処理が可能である。この理由は、距離集合部１１２が算出する第３値が、乱数乗された値であるので、対象データと、登録データとの距離を推定することができないからである。

【０１２４】

＜第２の実施形態＞

次に、上述した第１の実施形態を基本とする本発明の第２の実施形態について説明する。

【０１２５】

以降の説明においては、本実施形態に係る特徴的な部分を中心に説明すると共に、上述した第１の実施形態と同様な構成については、同一の参照番号を付すことにより、重複する説明を省略する。

【０１２６】

図５を参照しながら、本発明の第２の実施形態に係る照合システム２０１が有する構成について詳細に説明する。図５は、本発明の第２の実施形態に係る照合システム２０１が有する構成を示すブロック図である。

【０１２７】

第２の実施形態に係る照合システム２０１は、大別して、登録データ装置１０２と、照合要求装置２０２と、記憶装置１０４と、データ照合装置２０３と、照合補助装置１０６とを有する。

【０１２８】

照合要求装置２０２は、照合要求部１１０と、照合データ作成部２０４とを有する。

【０１２９】

データ照合装置２０３は、照合情報送信部２０５と、距離集合部１１２と、シャッフル部１１３と、照合補助依頼部１１５と、判定部１１６とを有する。

【０１３０】

登録データ装置１０２と、照合要求装置２０２と、記憶装置１０４と、データ照合装置２０３と、照合補助装置１０６とは、たとえば、通信ネットワークを介して、相互に通信することが可能であるとする。

【０１３１】

次に、本発明の第２の実施形態に係る照合システム２０１における処理について詳細に説明する。第２の実施形態に係る照合システム２０１の動作は、セットアップフェーズと、データ登録フェーズと、暗号文照合フェーズの３つのフェーズに大別される。以降においては、各フェーズにおける処理に関して詳細に説明する。

【０１３２】

第２の実施形態に係るセットアップフェーズにおける処理は、第１の実施形態に係るセ

ットアップフェーズにおける処理と同様である。このため、第２の実施形態に係るセットアップフェーズに関する説明を省略する。同様に、第２の実施形態に係るデータ登録フェーズにおける処理は、第１の実施形態に係るデータ登録フェーズにおける処理と同様である。このため、第２の実施形態に係るデータ登録フェーズに関する説明を省略する。

【０１３３】

図６を参照しながら、第２の実施形態に係る照合システム２０１の暗号文照合フェーズにおける処理について説明する。図６は、第２の実施形態に係る照合システム２０１の暗号文照合フェーズにおける処理の流れを示すフローチャートである。

【０１３４】

尚、ステップＤ１における処理は、ステップＣ１と同様の処理である。また、ステップＤ６乃至ステップＤ９における処理は、ステップＣ６乃至ステップＣ９と同様の処理である。このため、これらのステップにおける処理に関する説明を省略する。

【０１３５】

データ照合装置２０３における照合情報送信部２０５は、照合要求装置２０２における照合要求部１１０が送信した照合要求を受信し、受信した該照合要求に含まれている登録識別子を読み取る。照合情報送信部２０５は、暗号化登録情報において、読み取った登録識別子に関連付けされた暗号情報を特定する（ステップＤ２）。照合情報送信部２０５は、特定した暗号情報を、照合要求装置２０２における照合データ作成部２０４に送信する（ステップＤ３）。

【０１３６】

照合要求装置２０２における照合データ作成部２０４は、照合情報送信部２０５が送信した暗号情報を受信する。照合データ作成部２０４は、さらに、外部装置等から、対象データを受信する。照合データ作成部２０４は、加法に関して準同型性を有する暗号方式に従う演算を、受信した対象データと、受信した暗号情報とに適用することによって、該暗号情報を復号することなく、該対象データと、該暗号情報の基を表す登録データとの距離が暗号化された暗号化距離を算出する（ステップＤ４）。照合データ作成部２０４は、算出した暗号化距離を、データ照合装置２０３における距離集合部１１２に送信する。

【０１３７】

データ照合装置２０３における距離集合部１１２は、照合データ作成部２０４が送信した暗号化距離を受信する。距離集合部１１２は、受信した暗号化距離に関して、ステップＣ５に示された処理と同様の処理を実行する（ステップＤ５）。

【０１３８】

次に、第２の実施形態に係る照合システム２０１に関する効果について説明する。

【０１３９】

第２の実施形態に係る照合システム２０１によれば、照合対象である情報と、参照すべき情報との、より安全な照合処理が可能になる情報を作成することができる。この理由は、第２の実施形態に係る照合システム２０１が有する構成は、第１の実施形態に係る照合システム１０１が有する構成を含むからである。

【０１４０】

さらに、第２の実施形態に係る照合システム２０１によれば、照合対象である情報と、参照すべき情報とを、より効率的に、安全に照合することができる。たとえば、照合要求装置２０２が、比較的計算リソースの小さい携帯端末や、生体情報を取得する専用端末（たとえば、スキャナやカメラを含む装置）であっても、第２の実施形態に係る照合システム２０１によれば、短期間に安全な照合処理を可能にする。この理由は、ステップＤ４において、照合要求装置２０２がデータ照合装置２０３に送信するデータ量が、第１の実施形態に係る照合システム１０１と比較して少ないからである。第１の実施形態において、照合要求装置１０３がデータ照合装置１０５に送信するデータは、たとえば、ランダム距離情報である。ランダム距離情報は、比較情報セットの並び順を並び替えることによって作成される情報であり、対象データを受理可能か否かを判定する基準を表す閾値ｔに基づいて区画される範囲に含まれる値に応じたデータ量を含む。これに対して、第２の実施形

態において、照合要求装置２０２がデータ照合装置２０３に送信するデータは、暗号化距離である。したがって、該データは、暗号化距離に応じたデータ量を含む。

【０１４１】

暗号化距離のデータ量は、閾値ｔに基づいて区画される範囲に含まれる値のデータ量に比べて少ないので、照合要求装置２０２がデータ照合装置２０３に送信するデータ量は、第１の実施形態に係る照合システム１０１と比較して少ない。

【０１４２】

＜第３の実施形態＞

次に、上述した第１の実施形態を基本とする本発明の第３の実施形態について説明する。

【０１４３】

以降の説明においては、本実施形態に係る特徴的な部分を中心に説明すると共に、上述した第１の実施形態と同様な構成については、同一の参照番号を付すことにより、重複する説明を省略する。

【０１４４】

第３の実施形態においては、距離としてｎ次元ユークリッド距離が採用されている場合の例である。すなわち、２つのｎ（ただし、ｎは、自然数を表す）次元ベクトルＸ（式１４）、及び、ベクトルＹ（式１５）との間の距離ｄは、式１６に従い算出される。すなわち、

Ｘ＝（ｘ［１］，ｘ［２］，・・・，ｘ［ｎ］）・・・（式１４）、

Ｙ＝（ｙ［１］，ｙ［２］，・・・，ｙ［ｎ］）・・・（式１５）、

$d(X, Y) = (x[1] - y[1])^{\{2\}} + (x[2] - y[2])^{\{2\}} + \cdots + (x[n] - y[n])^{\{2\}}$ ・・・（式１６）、

ただし、ｘ［ｉ］、ｙ［ｉ］（$1 \leqq i \leqq n$）は実数を表す。

【０１４５】

距離が、対象データが受理可能であるか否かの基準を表す閾値ｔ以下である場合に、第３の実施形態に係る照合システム３０１は、ＸとＹとの距離が近いと判定する。すなわち、照合システム３０１は、対象データＹが、登録データＸによって受理可能であると判定する。または、照合システム３０１は、登録データＸが、対象データＹによって受理可能であると判定する。

【０１４６】

距離が該閾値ｔよりも大きい場合に、第３の実施形態に係る照合システム３０１は、登録データＸと対象データＹとの間の距離が遠いと判定する。すなわち、照合システム３０１は、対象データＹが、登録データＸによって受理不可能であると判定する。または、照合システム３０１は、登録データＸが、対象データＹによって受理不可能であると判定する。

【０１４７】

また、第３の実施形態において、照合システム３０１は、加法に関して準同型性を有する暗号（たとえば、Ｐａｉｌｌｉｅｒ暗号等）に基づき、暗号化または復号処理を実行すると仮定して、第３の実施形態に係る照合システム３０１における処置について説明する。しかし、第３の実施形態に係る照合システム３０１においては、加法Ｅｌｇａｍａｌ暗号、楕円Ｅｌｇａｍａｌ暗号等の加法に関して準同型性を有する暗号を採用してもよい。

【０１４８】

まず、Ｐａｉｌｌｉｅｒ暗号について説明する。Ｐａｉｌｌｉｅｒ暗号アルゴリズムは、鍵生成アルゴリズム、暗号化アルゴリズム、及び、復号アルゴリズムを含む。以降では、各アルゴリズムについて詳細に説明する。

【０１４９】

鍵生成アルゴリズムは、以下の鍵生成１乃至鍵生成６に示された処理を含む。すなわち、

・鍵生成１：セキュリティパラメータ1^{k}を受信する、

・鍵生成２：ｋビットの素数ｐ、及び、ｋビットの素数ｑをランダムに選ぶ、
・鍵生成３：ｐ×ｑ（＝ｎとする）を算出する、
・鍵生成４：（１＋ｎ）ｍｏｄ（ｎ^{2}）（＝ｇとする）を算出する、
・鍵生成５：算出したｎと算出したｇとの組（ｎ，ｇ）を暗号鍵ｐｋとして算出する、
・鍵生成６：算出した素数ｐと、算出した素数ｑとの組（ｐ，ｑ）を復号鍵ｓｋとして生成する、
ただし、ｍｏｄは、剰余を算出する演算子を表す。

【０１５０】
暗号化アルゴリズムは、以下の暗号化１乃至暗号化３に示された処理を含む。すなわち、
・暗号化１：暗号鍵ｐｋ（＝（ｎ，ｇ））と、メッセージＭとを受信する、
・暗号化２：$Z_{\{n\hat{}2\}}$から、ランダムにｒを選ぶ、
・暗号化３：（（１＋ｍ×ｎ）×ｒ^{n}）ｍｏｄ（ｎ^{2}）を算出し、算出した値を暗号文Ｃとして算出する。

【０１５１】
復号アルゴリズムは、以下の復号１乃至復号２に示された処理を含む。すなわち、
復号鍵ｓｋ（＝（ｐ，ｑ））と、暗号文Ｃとを入力とを受信する。

【０１５２】
・復号１：（ｐ－１）×（ｑ－１）（＝λとする）を計算する、
・復号２：（（ｃ$^{\{\lambda\}}$）ｍｏｄ（ｎ^{2}－１））／（（ｇ$^{\{\lambda\}}$）ｍｏｄ（ｎ^{2}－１））ｍｏｄ（ｎ）（＝ｍとする）を算出する。

【０１５３】
図７を参照しながら、本発明の第３の実施形態に係る照合システム３０１が有する構成について詳細に説明する。図７は、本発明の第３の実施形態に係る照合システム３０１が有する構成を示すブロック図である。

【０１５４】
第３の実施形態に係る照合システム３０１は、大別して、登録データ装置３０２と、照合要求装置３０８と、記憶装置３０３と、データ照合装置３０４と、照合補助装置３０５とを有する。

【０１５５】
登録データ装置３０２は、暗号化部３０６を有する。

【０１５６】
記憶装置３０３は、暗号文記憶部１０８と、識別子管理部３０７とを有する。

【０１５７】
照合要求装置３０８は、照合要求部３０９と、暗号化距離部３１０と、距離集合部３１１と、シャッフル部３１２とを有する。

【０１５８】
データ照合装置３０４は、照合情報送信部３１３と、照合補助依頼部１１５と、判定部１１６とを有する。

【０１５９】
照合補助装置３０５は、鍵生成部３１４と、照合補助部３１５と、鍵記憶部１１９とを有する。

【０１６０】
登録データ装置３０２と、照合要求装置３０８と、記憶装置３０３と、データ照合装置３０４と、照合補助装置３０５とは、たとえば、通信ネットワークを介して、相互に通信することが可能であるとする。

【０１６１】
次に、上述したセットアップフェーズ、データ登録フェーズ、及び、暗号文照合フェーズにおける処理について詳細に説明する。

【０１６２】

まず、セットアップフェーズにおける処理について説明する。

【０１６３】

図８を参照しながら、第３の実施形態に係る照合システム３０１のセットアップフェーズにおける処理について説明する。図８は、第３の実施形態に係る照合システム３０１のセットアップフェーズにおける処理の流れを示すシーケンス図（フローチャート）である。

【０１６４】

照合要求装置３０８における鍵生成部３１４は、たとえば、外部装置等から、復号鍵の長さを設定するセキュリティパラメータ1^{k}と、閾値ｔを含むパラメータとを受信する。鍵生成部３１４は、鍵生成１乃至鍵生成６に示した鍵生成アルゴリズムに従い、暗号鍵ｐｋと、復号鍵ｓｋとを生成する（ステップＡＡ１）。鍵生成部３１４は、生成した暗号鍵ｐｋを照合システム３０１に公開する（ステップＡＡ２）。鍵生成部３１４は、作成した復号鍵ｓｋを鍵記憶部１１９に格納する（ステップＡＡ３）。

【０１６５】

尚、ステップＡＡ１乃至ステップＡＡ３における処理は、ステップＡ１乃至ステップＡ３における処理の一例を表している。

【０１６６】

図９を参照しながら、第３の実施形態に係る照合システム３０１のデータ登録フェーズにおける処理について説明する。図９は、第３の実施形態に係る照合システム３０１のデータ登録フェーズにおける処理の流れを示すシーケンス図である。

【０１６７】

登録データ装置３０２における暗号化部３０６は、たとえば、外部装置等から、秘匿対象となる登録データＸと、閾値ｔ等を含むパラメータとを受信する。尚、登録データＸを、（ｘ［１］，ｘ［２］，・・・，ｘ［ｎ］）と表すとする。

【０１６８】

次に、暗号化部３０６は、受信した登録データＸに含まれる要素ｘ［ｉ］に関して、ｘ［ｉ］を２乗した値を算出することにより、$x[i]^{\{2\}}$（ｘｘ［ｉ］と表す）を算出する。ただし、ｉは、$1 \leqq i \leqq n$を満たす自然数を表す。次に、暗号化部３０６は、鍵生成部３１４が生成した暗号鍵ｐｋを用いて、たとえば、暗号化１乃至暗号化３に示された暗号化アルゴリズムに従い、要素ｘ［ｉ］を暗号化することにより、要素ｘ［ｉ］が暗号化された暗号化データｃ［ｉ］を作成する。暗号化部３０６は、暗号鍵ｐｋを用いて、たとえば、暗号化１乃至暗号化３に示された暗号化アルゴリズムに従い、ｘｘ［ｉ］を暗号化することにより、ｘｘ［ｉ］が暗号化された暗号化データＣＣ［ｉ］を作成する。

【０１６９】

すなわち、暗号化部３０６は、式１７に示された暗号化データＣ、及び、式１８に示された暗号化データを作成する。

【０１７０】

Ｃ：（ｃ［１］，ｃ［２］，・・・，ｃ［ｎ］）・・・（式１７）、
（ｃｃ［１］，ｃｃ［２］，・・・，ｃｃ［ｎ］）・・・（式１８）。

【０１７１】

登録データ装置３０２における暗号化部３０６は、式１８に従い作成されたｃｃ［ｉ］（ただし、$1 \leqq i \leqq n$）を掛け算することによって、暗号化データＣＣを作成する。暗号化部３０６は、作成した暗号化データＣと、作成した暗号化データＣＣとを含む暗号情報（Ｃ，ＣＣ）を作成し（ステップＢＢ１）、作成した暗号情報（Ｃ，ＣＣ）を、記憶装置３０３における識別子管理部３０７に送信する（ステップ（ＢＢ２－１））。

【０１７２】

次に、記憶装置３０３における識別子管理部３０７は、該暗号情報（Ｃ，ＣＣ）を受信し（ステップ（ＢＢ２－２））、受信した暗号情報に対して、該暗号情報（Ｃ，ＣＣ）を一意に識別可能な登録識別子ｉｎｄｅｘを作成する（ステップＢＢ３）。識別子管理部３０７は、暗号情報（Ｃ，ＣＣ）と、作成した登録識別子ｉｎｄｅｘとが関連付けされた暗

号化登録情報を作成し、作成した暗号化登録情報を暗号文記憶部１０８に格納する（ステップＢＢ４）。識別子管理部３０７は、作成した登録識別子ｉｎｄｅｘを、登録データ装置３０２に送信してもよい（ステップ（ＢＢ５－１））。

【０１７３】

登録データ装置３０２は、識別子管理部３０７が送信した登録識別子ｉｎｄｅｘを受信し（ステップ（ＢＢ５－２））、受信した登録識別子ｉｎｄｅｘを、表示部（不図示）に表示する（ステップＢＢ６）。

【０１７４】

尚、ステップＢＢ１乃至ステップＢＢ６における処理は、前述した図３に示すステップＢ１乃至ステップＢ５における処理の一例を表している。

【０１７５】

図１０を参照しながら、第３の実施形態に係る照合システム３０１のデータ暗号文照合フェーズにおける処理について説明する。図１０は、第３の実施形態に係る照合システム３０１の暗号文照合フェーズにおける処理の流れを示すシーケンス図である。

【０１７６】

照合要求装置３０８における照合要求部３０９は、照合する対象を表す対象データＹと、対象データＹに照合する暗号情報を表す登録識別子ｉｎｄｅｘとを、たとえば、外部装置等から受信する。照合要求部３０９は、さらに、対象データが受理可能であるか否かを判定する基準を表す閾値ｔを含むパラメータと、暗号鍵ｐｋとを読み取る。

【０１７７】

ここで、対象データＹを、（ｙ［１］，ｙ［２］，・・・，ｙ［ｎ］）と表すこととする。

【０１７８】

照合要求部３０９は、受信した登録識別子ｉｎｄｅｘに関連付けされた暗号情報を要求する照合要求を作成し（ステップＣＣ１）、作成した照合要求を、データ照合装置３０４における照合情報送信部３１３に送信する（ステップ（ＣＣ２－１））。たとえば、照合要求は、「ｒｅｑｕｅｓｔ＝（ｉｎｄｅｘ）」として表すことができる。照合要求は、さらに、登録識別子ｉｎｄｅｘとは異なる情報（たとえば、閾値ｔ、暗号鍵ｐｋ等）を含んでいてもよい。

【０１７９】

データ照合装置３０４における照合情報送信部３１３は、照合要求部３０９が送信した該照合要求を受信する（ステップ（ＣＣ２－２））。照合情報送信部３１３は、記憶装置３０３に格納されている暗号化登録情報において、受信した照合要求に含まれている登録識別子ｉｎｄｅｘに関連付けされた暗号情報Ｃを特定する（ステップＣＣ３）。照合情報送信部３１３は、特定した暗号情報Ｃを、照合要求装置３０８における暗号化距離部３１０に送信する（ステップ（ＣＣ４－１））。

【０１８０】

照合要求装置３０８における暗号化距離部３１０は、照合要求部３０９が送信した対象データＹと、照合情報送信部３１３が送信した暗号情報Ｃとを受信する（ステップ（ＣＣ４－２））。暗号化距離部３１０は、読み取った暗号情報Ｃと、読み取った対象データＹとを用いて、以下のステップ（Ｋ１－１）乃至ステップ（Ｋ１－３）に示された処理に従い、値ｄｄ［ｉ］を算出する。すなわち、

ステップ（Ｋ１－１）：１，２，・・・，ｎなるｉに関して、暗号情報Ｃに含まれている要素ｃ［ｉ］の｛－２×ｙ［ｉ］｝乗を算出する。この処理によって、$(c[i])^{\{-2\times y[i]\}}$が算出される。すなわち、$Enc(pk, x[i])^{\{-2\times y[i]\}}$（＝Ｅｎｃ（ｐｋ，－２×ｙ［ｉ］×ｘ［ｉ］））が算出される。

【０１８１】

ステップ（Ｋ１－２）：１，２，・・・，ｎなるｉに関して、対象データＹに含まれている要素ｙ［ｉ］を２乗した値を算出し、算出した値を、暗号鍵ｐｋを用いて暗号化する。すなわち、この処理によって、$Enc(pk, y[i]^{\{2\}})$が算出される。

【０１８２】
　ステップ（Ｋ１－３）：１，２，・・・，ｎなるｉに関して、ステップ（Ｋ１－１）に示された処理に従い算出された値（すなわち、（ｃ［ｉ］）$^{\{-2\times y[i]\}}$）と、ステップ（Ｋ１－２）に従い算出された値（すなわち、Ｅｎｃ（ｐｋ，ｙ［ｉ］$^{\{2\}}$））とが掛け算された値を算出することによって、値ｄｄ［ｉ］を算出する。
【０１８３】
　ステップ（Ｋ１－１）乃至ステップ（Ｋ１－３）に示す処理によって、（ｃ［ｉ］）$^{\{-2\times y[i]\}}$×Ｅｎｃ（ｐｋ，（ｙ［ｉ］）$^{\{2\}}$）（＝ｄｄ［ｉ］）が算出される。尚、ｄｄ［ｉ］は、式１９と等価である。
【０１８４】
　ｄｄ［ｉ］＝（ｃ［ｉ］）$^{\{-2\times y[i]\}}$×Ｅｎｃ（ｐｋ，（ｙ［ｉ］）$^{\{2\}}$）
　　＝Ｅｎｃ（ｐｋ，－２×ｙ［ｉ］×ｘ［ｉ］）×Ｅｎｃ（ｐｋ，（ｙ［ｉ］）$^{\{2\}}$）
　　＝Ｅｎｃ（ｐｋ，（ｘ［ｉ］）$^{\{2\}}$－２×ｘ［ｉ］×ｙ［ｉ］＋（ｙ［ｉ］）$^{\{2\}}$－（ｘ［ｉ］）$^{\{2\}}$）
　　＝Ｅｎｃ（ｐｋ，（ｘ［ｉ］－ｙ［ｉ］）$^{\{2\}}$－（ｘ［ｉ］）$^{\{2\}}$）・・・（式１９）。
【０１８５】
　したがって、ステップ（Ｋ１－１）乃至ステップ（Ｋ１－３）に示された処理によって、値ｄｄ［ｉ］が算出される。
【０１８６】
　照合要求装置３０８における暗号化距離部３１０は、算出した各ｄｄ［ｉ］と、暗号化データＣＣとが掛け算された値を算出することにより、登録データＸと、対象データＹとの間の距離が暗号化された暗号化距離を算出する（ステップＣＣ５）。すなわち、暗号化距離部３１０は、ｄｄ［１］×ｄｄ［２］×・・・×ｄｄ［ｎ］×ＣＣ（＝ｄとする）に従い演算を実行することにより、暗号化距離を算出する。
【０１８７】
　尚、算出される値ｄは、上述した式１９によれば、以下の通りである。
【０１８８】
　ｄ＝Ｅｎｃ（ｐｋ，（ｘ［１］－ｙ［１］）$^{\{2\}}$－（ｘ［１］）$^{\{2\}}$）×・・・×Ｅｎｃ（ｐｋ，（ｘ［ｎ］－ｙ［ｎ］）$^{\{2\}}$－（ｘ［ｎ］）$^{\{2\}}$）×ＣＣ
　　＝Ｅｎｃ（ｐｋ，（ｘ［１］－ｙ［１］）$^{\{2\}}$＋（ｘ［２］－ｙ［２］）$^{\{2\}}$＋・・・＋（ｘ［ｎ］－ｙ［ｎ］）$^{\{2\}}$））。
【０１８９】
　すなわち、これは、登録データＸと、対象データＹとの間を、ユークリッドノルムにて測定した場合の距離が暗号化された暗号化距離を表す。尚、説明の便宜上、値ｄを、ｄ［０］と表す。
【０１９０】
　暗号化距離部３１０は、算出した暗号化距離を、照合要求装置３０８における距離集合部３１１に出力する。
【０１９１】
　次に、照合要求装置３０８における距離集合部３１１は、暗号化距離部３１０が出力した暗号化距離を入力し、入力した暗号化距離から暗号化距離ｄを読み取る。次に、距離集合部３１１は、読み取った暗号化距離ｄと、閾値ｔとに基づいて、以下のステップ（Ｋ２－１）乃至ステップ（Ｋ２－５）に示す処理に従い、値を算出する。すなわち、
　・ステップ（Ｋ２－１）：０，・・・，ｔなるｉに対して、乱数ｒ［ｉ］（以降、「第１乱数」と表す）、乱数Ａ［ｉ］（以降、「第２乱数」と表す）を選ぶ、
　・ステップ（Ｋ２－２）：０，・・・，ｔなるｉに対して、乱数Ａ［ｉ］が、暗号鍵ｐｋを用いて暗号化された値Ｅｎｃ（ｐｋ，Ａ［ｉ］）を算出する、
　・ステップ（Ｋ２－３）：０，・・・，ｔなるｉに対して、ｉにマイナスを付した値が

、暗号鍵ｐｋを用いて暗号化された値Ｅｎｃ（ｐｋ，－ｉ）を算出する、
・ステップ（Ｋ２－４）：算出したＥｎｃ（ｐｋ，－ｉ）と、暗号化距離ｄとが掛け算された値を算出することによって、値ｒ［ｉ］を算出する、
・ステップ（Ｋ２－５）：ステップ（Ｋ２－４）にて算出した値と、ステップ（Ｋ２－２）にて算出した値とが掛け算された値を算出することによって、値（ｄ×Ｅｎｃ（ｐｋ，－ｉ））$^{\{r[i]\}}$×Ｅｎｃ（ｐｋ，Ａ［ｉ］）を算出する。

【０１９２】
すなわち、ステップ（Ｋ２－１）乃至ステップ（Ｋ２－５）によって、登録データＸと対象データＹとの距離から閾値ｔ以下の値を減じた値を乱数ｒ［ｉ］倍した値に、乱数Ａ［ｉ］を加えた値ｄｐ［ｉ］が算出される。

【０１９３】
距離集合部３１１は、算出したｄｐ［ｉ］と、乱数Ａ［ｉ］とが関連付けされた比較情報セットを作成し、作成された比較情報セットがｉの値の小さな順に並べられた暗号化距離情報Ｄを作成する（ステップＣＣ６）。この場合に、暗号化距離情報Ｄは、たとえば、（（ｄｐ［０］，Ａ［０］），（ｄｐ［１］，Ａ［１］），・・・，（ｄｐ［ｔ］，Ａ［ｔ］））と表すことができる。

【０１９４】
距離集合部３１１は、算出した暗号化距離情報Ｄを、照合要求装置３０８におけるシャッフル部３１２に出力する。

【０１９５】
次に、照合要求装置３０８におけるシャッフル部３１２は、距離集合部３１１が出力した暗号化距離情報Ｄを入力し、受信した暗号化距離情報Ｄにおける比較情報セットの順序が並び変えられたランダム距離情報ＤＰを作成する。たとえば、シャッフル部３１２は、（ステップＣＡ１）乃至（ステップＣＡ２）に示す処理に従い、ランダム距離情報ＤＰを作成する。

【０１９６】
・ステップＣＡ１：０からｔまでの整数（以降、［０，ｔ］とも表す）に関して順列πを作成する。すなわち、［０，ｔ］に含まれているｊ（ただし、０≦ｊ≦ｔ）に対してπ（ｊ）も［０，ｔ］に含まれており、かつ、ｊが異なる場合には、π（ｊ）が異なる（すなわち、π（ｊ）に重複がない）。尚、作成される順列πは、たとえば、ランダムに並び替えることが可能な順列である。

【０１９７】
・ステップＣＡ２：［０，ｔ］に関して、作成したπ（ｊ）が小さい順にｊを並び替えされたランダム距離情報ＤＰを作成する。

【０１９８】
すなわち、シャッフル部３１２は、暗号化距離情報Ｄに含まれている比較情報セットを、ランダムな順列πに従って並び替えることにより、ランダム距離情報ＤＰを作成する（ステップＣＣ７）。シャッフル部３１２は、作成したランダム距離情報ＤＰを、データ照合装置３０４における照合補助依頼部１１５に送信する（ステップ（ＣＣ８－１））。

【０１９９】
データ照合装置３０４における照合補助依頼部１１５は、シャッフル部３１２が送信したランダム距離情報ＤＰを受信し（ステップ（ＣＣ８－２））、受信したランダム距離情報ＤＰに関する照合処理を実行することを要求する照合補助要求を作成する（ステップＣＣ９）。照合補助依頼部１１５は、作成した照合補助要求を、照合補助装置３０５における照合補助部３１５に送信する（ステップ（ＣＣ１０－１））。たとえば、照合補助要求は、ランダム距離情報ＤＰを含む情報として実現することができる。照合補助要求は、ランダム距離情報ＤＰを含むとしたが、さらに、他のデータを含んでいてもよい。

【０２００】
照合補助装置３０５における照合補助部３１５は、照合補助依頼部１１５が送信した照合補助要求を受信する（ステップ（ＣＣ１０－２））。照合補助部３１５は、鍵記憶部１

１９から復号鍵ｓｋを読み取り、ランダム距離情報ＤＰに含まれている比較情報セットのうち要素ｄｐ［ｉ］（ただし、０≦ｉ≦ｔ）を、読み取った復号鍵ｓｋを用いて復号する。照合補助部３１５は、要素ｄｐ［ｉ］を復号することにより、該要素ｄｐ［ｉ］が復号された照合情報を作成する（ステップＣＣ１１）。この処理において、照合補助部３１５は、たとえば、復号鍵ｓｋを用いて、要素ｄｐ［ｉ］を復号する。すなわち、以下の式２０に示されたランダム距離情報ＤＰに関して、復号鍵ｓｋを用いて復号される。

【０２０１】

ＤＰ＝（（ｄｐ［０］，ＡＰ［０］），（ｄｐ［１］，ＡＰ［１］），・・・，（ｄｐ［ｔ］，ＡＰ［ｔ］））・・・（式２０）。

【０２０２】

照合補助部３１５は、作成した照合情報を、データ照合装置３０４における判定部１１６に送信する（ステップ（ＣＣ１２－１））。

【０２０３】

次に、データ照合装置３０４における判定部１１６は、照合補助部３１５が送信した照合情報を受信し（ステップ（ＣＣ１２－２））、受信した照合情報が一致していることを表す場合に、対象データＹが受理されたことを表す照合結果情報を作成する。判定部１１６は、受信した照合情報が不一致であることを表す場合に、対象データＹが受理されなかった（不受理である）ことを表す照合結果情報を作成する（ステップＣＣ１３）。

【０２０４】

たとえば、照合補助部３１５は、受信した照合情報において、あるｉ（０≦ｉ≦ｔ）に対して、ｄｐ［ｉ］が復号された復号結果がＡＰ［ｉ］に一致するｉがある場合に、一致であることを表す照合結果情報を作成する。照合補助部３１５は、受信した照合情報において、ｄｐ［ｉ］が復号された復号結果がＡＰ［ｉ］に一致するｉがない場合に、不一致であることを表す照合結果情報を作成する。

【０２０５】

ステップＣＣ１乃至ステップＣＣ１３における処理は、前述した図４に示すステップＣ１乃至ステップＣ９における処理の一例を表している。

【０２０６】

第３の実施形態において、記憶装置３０３に登録されている暗号情報は「登録データＸのおける要素数＋１」個の暗号化データである。また、ステップＣＣ６において作成される閾値（ｔ＋１）個の暗号文を復号した結果は、登録された登録データと、対象データの距離が閾値ｔ以下である場合に０を含み、それ以外は乱数である。（ｔ＋１）個の暗号文をシャッフルすることにより、照合補助装置３０５に対しても距離を秘匿できる。

【０２０７】

また、第３の実施形態では、ユークリッド距離の例を挙げたが、暗号文照合フェーズのステップＣＣ５を変更することにより他の距離（ハミング距離、マハラノビス距離等）にも容易に適用可能である。

【０２０８】

次に、第３の実施形態に係る照合システム３０１に関する効果について説明する。

【０２０９】

第３の実施形態に係る照合システム３０１によれば、照合対象である情報と、参照すべき情報との、より安全な照合処理が可能になる情報を作成することができる。この理由は、第３の実施形態に係る照合システム３０１が有する構成は、第１の実施形態に係る照合システム１０１が有する構成を含むからである。

【０２１０】

さらに、第３の実施形態に係る照合システム３０１によれば、照合対象である情報と、参照すべき情報とを、安全に照合することが可能である。この理由は、暗号化距離部３１０が、第１値と、第２値とに加え、さらに、第１乱数を加算することによって、たとえば、認証処理の度に、異なる照合情報を作成されるからである。この場合に、たとえ、照合情報が傍受されたとしても、第３の実施形態に係る照合システム３０１によれば、傍受さ

れた照合情報に基づきテンプレートを作成することはより困難である。

【０２１１】

さらに、第３の実施形態に係る照合システム３０１によれば、より一層、安全な照合処理が可能である。この理由は、暗号化距離部３１０が、第１値と、第２値とに、第１乱数と、第２乱数とを用いた演算を適用することによって、たとえば、認証処理のたびに、異なる照合情報を作成されるからである。この場合に、たとえ、照合情報が傍受されたとしても、本実施形態に係る照合システム３０１によれば、傍受された照合情報に基づきテンプレートを作成することはより困難である。

【０２１２】

＜第４の実施形態＞

【０２１３】

次に、上述した第２の実施形態を基本とする本発明の第４の実施形態について説明する。

【０２１４】

以降の説明においては、本実施形態に係る特徴的な部分を中心に説明すると共に、上述した第２の実施形態と同様な構成については、同一の参照番号を付すことにより、重複する説明を省略する。

【０２１５】

図１１を参照しながら、本発明の第４の実施形態に係る照合システム４０１が有する構成について詳細に説明する。図１１は、第４の実施形態に係る照合システム４０１が有する構成を示すブロック図である。

【０２１６】

第４の実施形態に係る照合システム４０１は、大別して、登録データ装置１０２と、照合要求装置４０２と、記憶装置１０４と、データ照合装置４０３と、照合補助装置１０６とを有する。

【０２１７】

照合要求装置４０２は、照合要求部１１０と、照合データ作成部４０４とを有する。

【０２１８】

データ照合装置４０３は、照合情報送信部２０５と、距離集合部４０５と、シャッフル部１１３と、照合補助依頼部１１５と、判定部１１６とを有する。

【０２１９】

登録データ装置１０２と、照合要求装置４０２と、記憶装置１０４と、データ照合装置４０３と、照合補助装置１０６とは、たとえば、通信ネットワークを介して、相互に通信することが可能であるとする。

【０２２０】

以下、各フェーズにおける動作に関して詳細に説明する。尚、セットアップフェーズ、及び、データ登録フェーズにおける動作は、上述した各実施形態にて説明した動作と同様である。このため、セットアップフェーズ、及び、データ登録フェーズにおける説明を省略する。以降では、暗号文照合フェーズについて詳細に説明する。

【０２２１】

図１２を参照しながら、第４の実施形態に係る照合システム４０１のデータ暗号文照合フェーズにおける処理について説明する。図１２は、第４の実施形態に係る照合システム４０１の暗号文照合フェーズにおける処理の流れを示すシーケンス図である。

【０２２２】

照合要求装置４０２における照合要求部１１０は、たとえば、外部装置等から、登録識別子と、対象データとを受信する。照合要求部１１０は、暗号化登録情報において、受信した登録識別子に関連付けされた暗号情報を要求する照合要求を作成する（ステップＤＤ１）。照合要求部１１０は、作成した照合要求を、データ照合装置４０３における照合情報送信部２０５に送信する（ステップ（ＤＤ２－１））。

【０２２３】

データ照合装置４０３における照合情報送信部２０５は、照合要求装置４０２における照合要求部１１０が送信した照合要求を受信し（ステップ（ＤＤ２－２））、受信した該照合要求に含まれている登録識別子を読み取る。照合情報送信部２０５は、暗号化登録情報において、読み取った登録識別子に関連付けされた暗号情報Ｃを特定する（ステップＤＤ３）。照合情報送信部２０５は、特定した暗号情報Ｃを、照合要求装置４０２における照合データ作成部４０４に送信する（ステップ（ＤＤ４－１））。

【０２２４】

照合要求装置４０２における照合データ作成部４０４は、照合情報送信部２０５が送信した暗号情報Ｃを受信する（ステップ（ＤＤ４－２））。照合データ作成部４０４は、受信した暗号情報Ｃと、読み取った対象データＹとを用いて、前述した図１０のステップＣＣ５に示された処理と同様の処理を実行することにより、暗号化距離を算出する（ステップＤＤ５）。照合データ作成部４０４は、算出した暗号化距離を、データ照合装置４０３における距離集合部４０５に送信する（ステップ（ＤＤ６－１））。

【０２２５】

データ照合装置４０３における距離集合部４０５は、照合データ作成部４０４が送信した暗号化距離を受信し（ステップ（ＤＤ６－２））、受信した暗号化距離に関して、距離集合部３１１が実行する処理と同様の処理を実行することにより、暗号化距離情報Ｄを作成する（ステップＤＤ７）。照合データ作成部４０４は、作成した暗号化距離情報Ｄを、データ照合装置４０３におけるシャッフル部１１３に送信する。

【０２２６】

データ照合装置４０３におけるシャッフル部１１３は、シャッフル部３１２における処理と同様の処理を実行することにより、ランダム距離情報ＤＰを作成する（ステップＤＤ８）。シャッフル部１１３は、作成したランダム距離情報ＤＰを、データ照合装置４０３における照合補助依頼部１１５に出力する。

【０２２７】

以降、前述した図１０のステップＣＣ９乃至ステップＣＣ１３に示した処理と同様の処理が、ステップＤＤ９乃至ステップＤＤ１３において実行される。

【０２２８】

次に、第４の実施形態に係る照合システム４０１に関する効果について説明する。

【０２２９】

第４の実施形態に係る照合システム４０１によれば、照合対象である情報と、参照すべき情報との、より安全な照合処理が可能になる情報を作成することができる。この理由は、第４の実施形態に係る照合システム４０１が有する構成は、第１の実施形態に係る照合システム１０１が有する構成を含むからである。

【０２３０】

さらに、第４の実施形態に係る照合システム４０１によれば、照合対象である情報と、参照すべき情報とを、効率的に、安全に照合することができる。たとえば、照合要求装置４０２が、比較的計算リソースの小さい携帯端末や、生体情報を取得する専用端末（たとえば、スキャナやカメラを含む装置）であっても、第４の実施形態に係る照合システム４０１によれば、短期間に安全な照合処理を可能にする。この理由は、ステップ（ＤＤ４－１）において、照合要求装置４０２がデータ照合装置４０３に送信するデータが、第３の実施形態に係る照合システム３０１に係ると比較して少ないからである。第３の実施形態において、該データは、たとえば、ランダム距離情報である。これに対して、第４の実施形態において、該データは、登録データと対象データとの間の距離が暗号化された暗号化距離である。暗号化距離のデータ量は、閾値ｔに基づいて区画される範囲に含まれる値のデータ量に比べて少ないので、照合要求装置４０２がデータ照合装置４０３に送信するデータ量は、第３の実施形態に係る照合システム３０１と比較して少ない。

【０２３１】

尚、上述した各実施形態において、ユークリッド距離の例を挙げたが、他の距離（ハミング距離、マハラノビス距離等）であってもよい。

【０２３２】
＜第５の実施形態＞
図１３、及び、図１４を参照しながら、本発明の第５の実施形態に係る暗号情報作成装置５０１が有する構成と、第５の実施形態に係る暗号情報作成装置５０１における処理とについて詳細に説明する。図１３は、本発明の第５の実施形態に係る暗号情報作成装置５０１が有する構成を示すブロック図である。図１４は、第５の実施形態に係る暗号情報作成装置５０１における処理の流れを示すフローチャートである。
【０２３３】
第５の実施形態に係る暗号情報作成装置５０１は、範囲暗号部５０２と、演算部５０３とを有する。
【０２３４】
範囲暗号部５０２は、閾値ｔに基づいて区画される範囲に含まれている第１値を算出する（ステップＳ５０１）。たとえば、範囲暗号部５０２は、閾値（－ｔ）から０に至る範囲に含まれている値を、該第１値として算出する。あるいは、範囲暗号部５０２は、たとえば、閾値（－ｔ）から（－１）に至る範囲に含まれている値を、該第１値として算出する。次に、範囲暗号部５０２は、準同型性を有する暗号方式に従い、算出した第１値を暗号化することによって、該第１値が暗号化された第１暗号文を作成する（ステップＳ５０２）。
【０２３５】
演算部５０３は、該暗号方式に従いある値（以降、「第２値」と表す）が暗号化された第２暗号文と、該第１暗号文とに、暗号方式に従った演算を適用することによって、該第１値と該第２値とが加算された値が暗号化された第３暗号文を作成する（ステップＳ５０３）。
【０２３６】
演算部５０３は、式１を参照して説明したような加法に関して準同型性を有する暗号方式に従い処理を実行する場合に、たとえば、第２暗号文と、第１暗号文と掛け算することによって、該第３暗号文を作成する。
【０２３７】
尚、閾値ｔは、たとえば、対象データを受理するか否かを判定する基準を表す閾値である。第２値は、たとえば、対象データと、登録データとの距離、または、対象データと、登録データとが類似している程度を表す類似度である。この場合に、第２暗号文は、たとえば、該距離が暗号化された値である。
【０２３８】
たとえば、範囲暗号部５０２、及び、演算部５０３は、上述した実施形態に示した距離集合部等が有する機能によって、実現することができる。
【０２３９】
次に、第５の実施形態に係る暗号情報作成装置５０１に関する効果について説明する。
【０２４０】
第５の実施形態に係る暗号情報作成装置５０１によれば、照合対象である情報と、参照すべき情報との、より安全な照合処理が可能になる情報を作成することができる。この理由は、照合処理において、受理するか否かを判定する基準を表す閾値ｔに基づいて区画される範囲に含まれる第１値と、ある値とが加算された値を、第２値が暗号化された第２暗号文を復号することなく求めることができるからである。この理由について詳細に説明する。
【０２４１】
暗号情報作成装置５０１における処理に関する説明にて例示したように、第２値は、たとえば、対象データと、登録データとの距離（または、類似度）を表す。この場合に、暗号情報作成装置５０１は、図１４に示した処理に従い、距離を復号することなく、該距離と、該閾値ｔに含まれている値とが加算された値が暗号化された第３暗号文（すなわち、上述した照合情報と同様の内容に関して暗号化された暗号文）を作成する。

【０２４２】
復号装置（たとえば、各実施形態に示した照合補助部）は、該第３暗号文を受信し、受信した復号情報を復号することによって、第１値、及び、第２値が加算された値を算出し、該値が所定の条件を満たすか否かに応じて、対象データを受理可能であるか否かを判定する。すなわち、復号装置（たとえば、各実施形態に示した照合補助装置）は、対象データと、登録データとの距離を復号することなく、対象データを受理可能であるか否かを判定することができる。この結果、本実施形態に係る暗号情報作成装置５０１によれば、たとえば、復号された距離に基づきテンプレートを復元するヒルクライミング攻撃を受ける可能性は低下する。
【０２４３】
これに対して、特許文献１乃至特許文献９、非特許文献１、及び、非特許文献２に開示された技術によれば、距離を暗号化したまま、該距離と閾値ｔとの大小を比較することはできない。すなわち、これらの技術は、暗号化された距離を復号することによって、該距離と、閾値ｔとの大小を比較する。したがって、これらの技術によれば、暗号化された距離を復号するので、該距離が外部に漏えいしてしまう可能性がある。
【０２４４】
したがって、第５の実施形態に係る暗号情報作成装置５０１によれば、照合対象である情報と、参照すべき情報との、より安全な照合処理が可能になる情報を作成することができる。
【０２４５】
（ハードウェア構成例）
上述した本発明の各実施形態における照合システム、または、暗号情報作成装置を、１つの計算処理装置（情報処理装置、コンピュータ）を用いて実現するハードウェア資源の構成例について説明する。但し、係る暗号情報作成装置（照合システム）は、物理的または機能的に少なくとも２つの計算処理装置を用いて実現してもよい。また、係る暗号情報作成装置（照合システム）は、専用の装置として実現してもよい。
【０２４６】
図１５は、第１の実施形態乃至第４の実施形態に係る照合システム、または、第５の実施形態に係る暗号情報作成装置を実現可能な計算処理装置のハードウェア構成例を概略的に示す図である。計算処理装置２０は、中央処理演算装置（Ｃｅｎｔｒａｌ＿Ｐｒｏｃｅｓｓｉｎｇ＿Ｕｎｉｔ、以降「ＣＰＵ」と表す）２１、メモリ２２、ディスク２３、及び、不揮発性記録媒体２４を有する。計算処理装置２０は、通信インターフェース（以降、「通信ＩＦ」と表す）２７を有する。計算処理装置２０は、さらに、入力装置２５、及び、出力装置２６を有してもよい。計算処理装置２０は、通信ＩＦ２７を介して、他の計算処理装置、及び、通信装置と情報を送受信することができる。
【０２４７】
不揮発性記録媒体２４は、コンピュータが読み取り可能な、たとえば、コンパクトディスク（Ｃｏｍｐａｃｔ＿Ｄｉｓｃ）、デジタルバーサタイルディスク（Ｄｉｇｉｔａｌ＿Ｖｅｒｓａｔｉｌｅ＿Ｄｉｓｃ）である。また、不揮発性記録媒体２４は、ユニバーサルシリアルバスメモリ（ＵＳＢメモリ）、ソリッドステートドライブ（Ｓｏｌｉｄ＿Ｓｔａｔｅ＿Ｄｒｉｖｅ）等であってもよい。不揮発性記録媒体２４は、電源を供給しなくても係るプログラムを保持し、持ち運びを可能にする。不揮発性記録媒体２４は、上述した媒体に限定されない。また、不揮発性記録媒体２４の代わりに、通信ＩＦ２７を介して、通信ネットワークを介して係るプログラムを持ち運びしてもよい。
【０２４８】
すなわち、ＣＰＵ２１は、ディスク２３に記憶されているソフトウェア・プログラム（コンピュータ・プログラム：以下、単に「プログラム」と称する）を、実行する際にメモリ２２にコピーし、演算処理を実行する。ＣＰＵ２１は、プログラム実行に必要なデータをメモリ２２から読み取る。外部への出力が必要な場合には、ＣＰＵ２１は、出力装置２６に出力結果を出力する。外部からプログラムを入力する場合、ＣＰＵ２１は、入力装置

２５からプログラムを読み取る。ＣＰＵ２１は、上述した図１、図５、図７、図１１、または、図１３に示す各部が表す機能（処理）に対応するところのメモリ２２にある照合プログラム（図２乃至図４、図６、図８乃至図１０、または、図１２）、または、暗号情報作成プログラム（図１４）を解釈し実行する。ＣＰＵ２１は、上述した本発明の各実施形態において説明した処理を順次実行する。

【０２４９】

すなわち、このような場合、本発明は、係る照合プログラム、または、係る暗号情報作成プログラムによっても成し得ると捉えることができる。さらに、係る照合プログラム、または、係る暗号情報作成プログラムが記録されたコンピュータが読み取り可能な不揮発性の記録媒体によっても、本発明は成し得ると捉えることができる。

【０２５０】

以上、上述した実施形態を模範的な例として本発明を説明した。しかし、本発明は、上述した実施形態には限定されない。すなわち、本発明は、本発明のスコープ内において、当業者が理解し得る様々な態様を適用することができる。

【０２５１】

この出願は、２０１５年６月１８日に出願された日本出願特願２０１５－１２２７５１を基礎とする優先権を主張し、その開示の全てをここに取り込む。

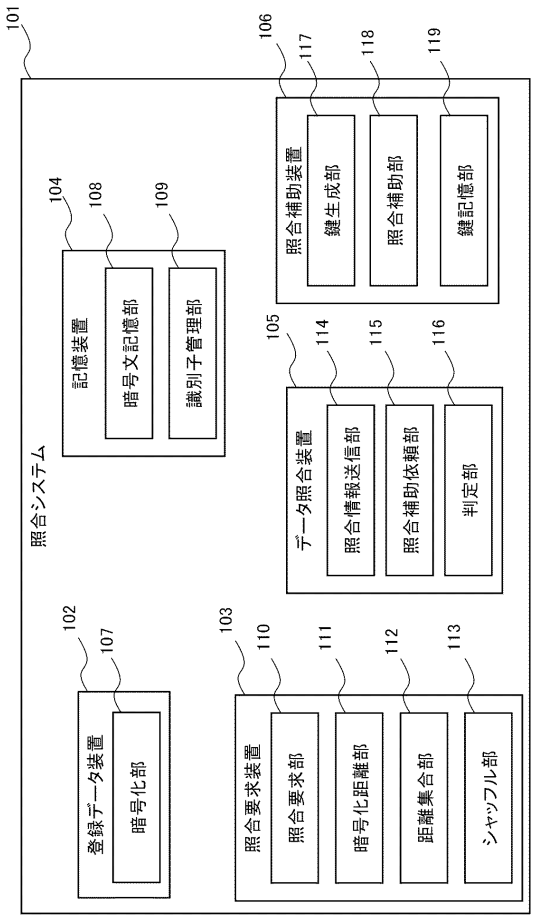
【符号の説明】

【０２５２】

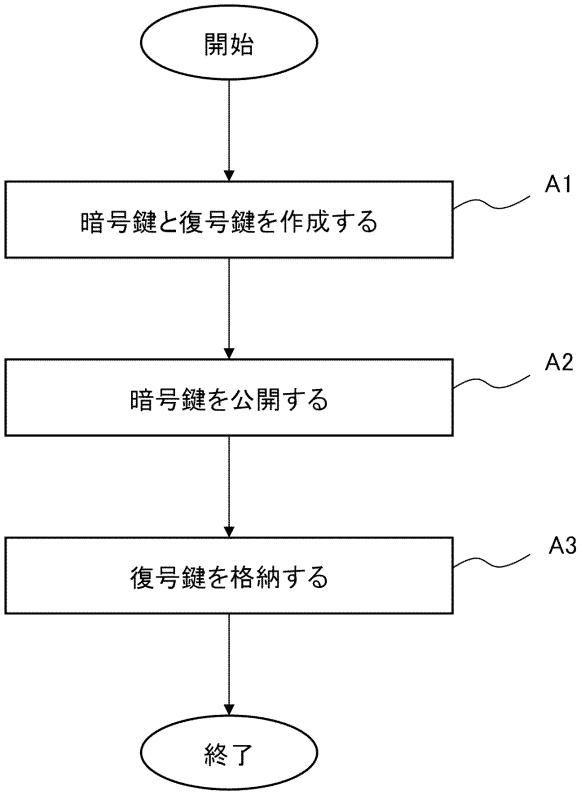
１０１　照合システム
１０２　登録データ装置
１０３　照合要求装置
１０４　記憶装置
１０５　データ照合装置
１０６　照合補助装置
１０７　暗号化部
１０８　暗号文記憶部
１０９　識別子管理部
１１０　照合要求部
１１１　暗号化距離部
１１２　距離集合部
１１３　シャッフル部
１１４　照合情報送信部
１１５　照合補助依頼部
１１６　判定部
１１７　鍵生成部
１１８　照合補助部
１１９　鍵記憶部
２０１　照合システム
２０２　照合要求装置
２０３　データ照合装置
２０４　照合データ作成部
２０５　照合情報送信部
３０１　照合システム
３０２　登録データ装置
３０３　記憶装置
３０４　データ照合装置
３０５　照合補助装置
３０６　暗号化部
３０７　識別子管理部

３０８　照合要求装置
３０９　照合要求部
３１０　暗号化距離部
３１１　距離集合部
３１２　シャッフル部
３１３　照合情報送信部
３１４　鍵生成部
３１５　照合補助部
４０１　照合システム
４０２　照合要求装置
４０３　データ照合装置
４０４　照合データ作成部
４０５　距離集合部
５０１　暗号情報作成装置
５０２　範囲暗号部
５０３　演算部
２０　計算処理装置
２１　ＣＰＵ
２２　メモリ
２３　ディスク
２４　不揮発性記録媒体
２５　入力装置
２６　出力装置
２７　通信ＩＦ

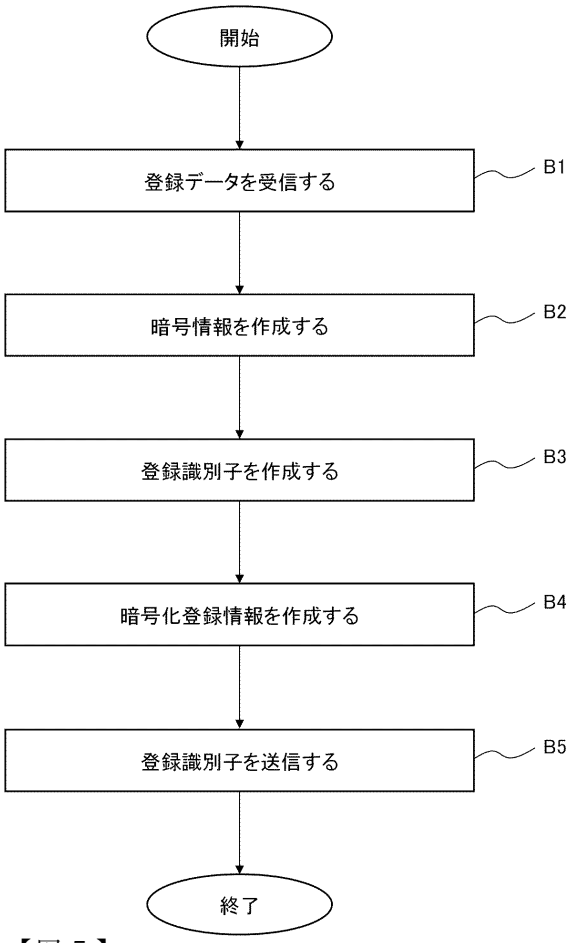
【図１】



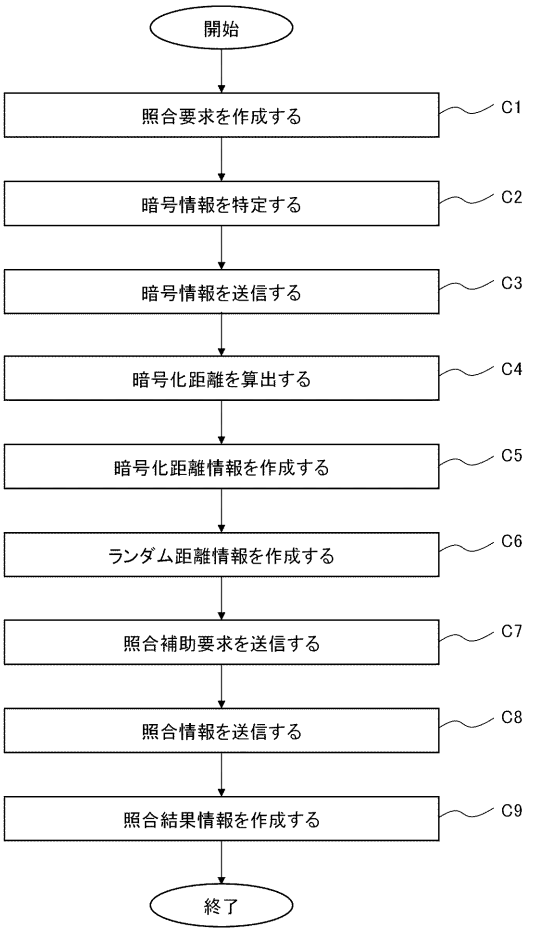
【図２】



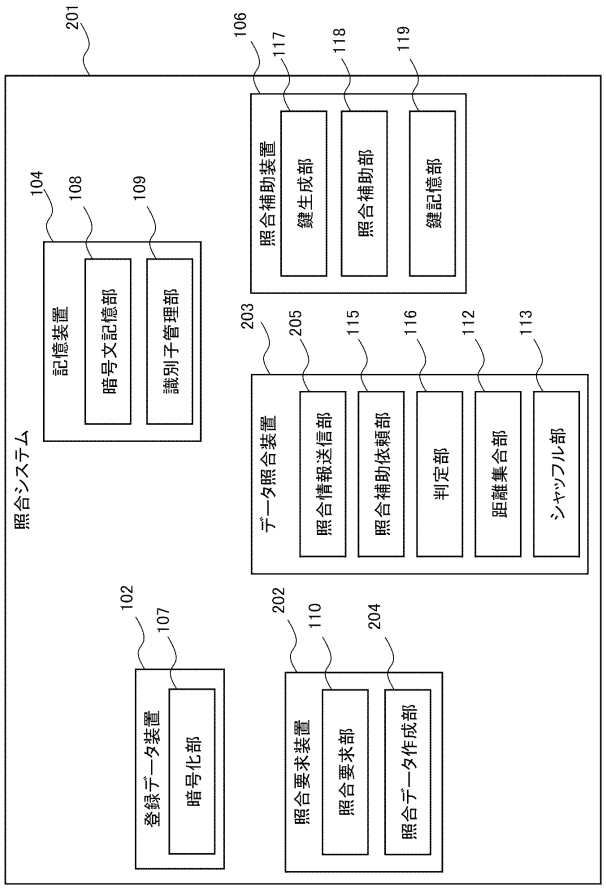
【図３】


開始
登録データを受信する
B1
暗号情報を作成する
B2
登録識別子を作成する
B3
暗号化登録情報を作成する
B4
登録識別子を送信する
B5
終了

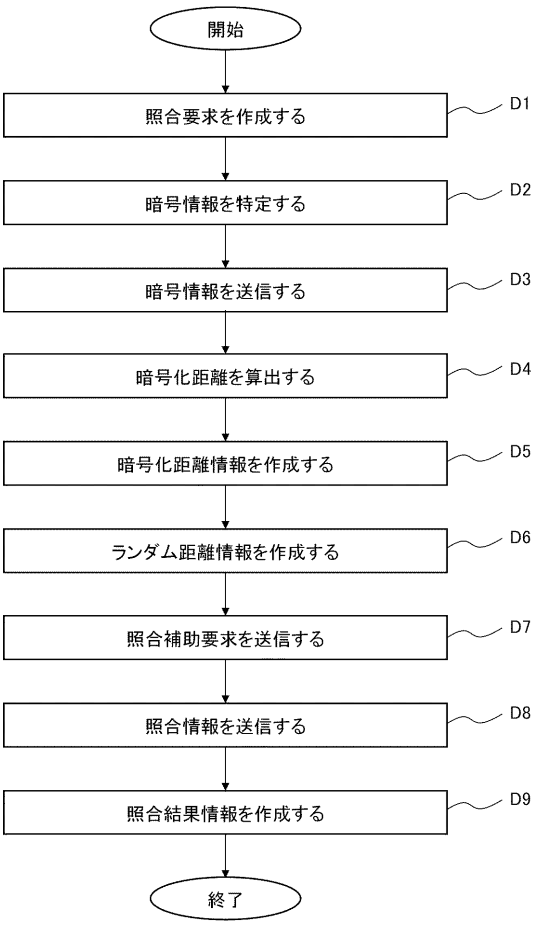
【図４】


開始
照合要求を作成する
C1
暗号情報を特定する
C2
暗号情報を送信する
C3
暗号化距離を算出する
C4
暗号化距離情報を作成する
C5
ランダム距離情報を作成する
C6
照合補助要求を送信する
C7
照合情報を送信する
C8
照合結果情報を作成する
C9
終了

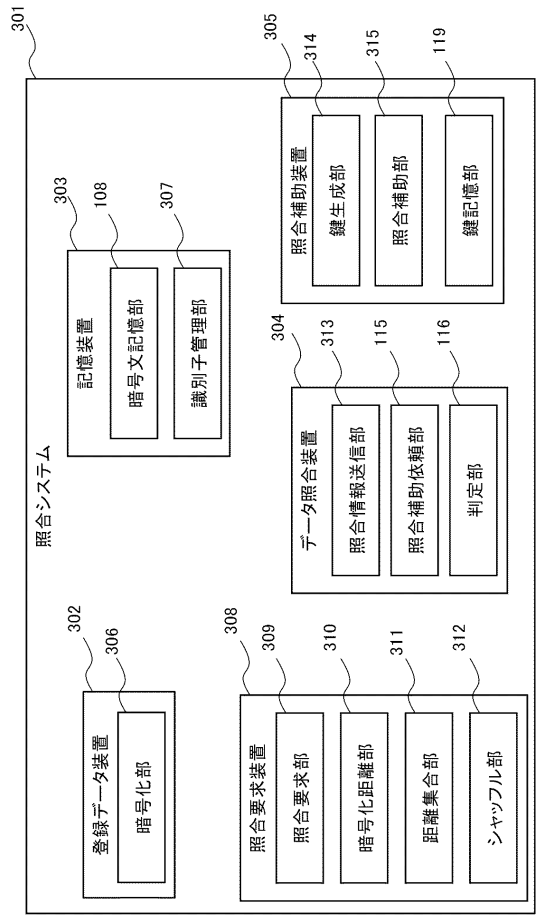
【図５】


201
照合システム
106
117
118
119
照合補助装置
鍵生成部
照合補助部
鍵記憶部
104
108
109
記憶装置
暗号文記憶部
識別子管理部
203
205
115
116
112
113
データ照合装置
照合情報送信部
照合補助依頼部
判定部
距離集合部
シャッフル部
102
107
登録データ装置
暗号化部
202
110
204
照合要求装置
照合要求部
照合データ作成部

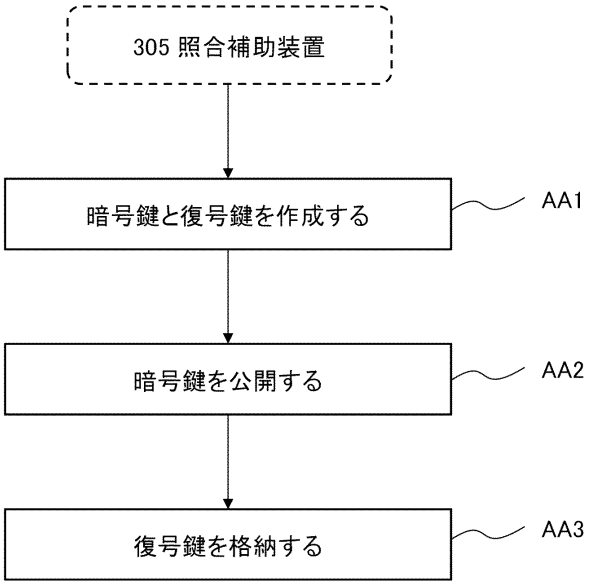
【図６】


開始
照合要求を作成する
D1
暗号情報を特定する
D2
暗号情報を送信する
D3
暗号化距離を算出する
D4
暗号化距離情報を作成する
D5
ランダム距離情報を作成する
D6
照合補助要求を送信する
D7
照合情報を送信する
D8
照合結果情報を作成する
D9
終了

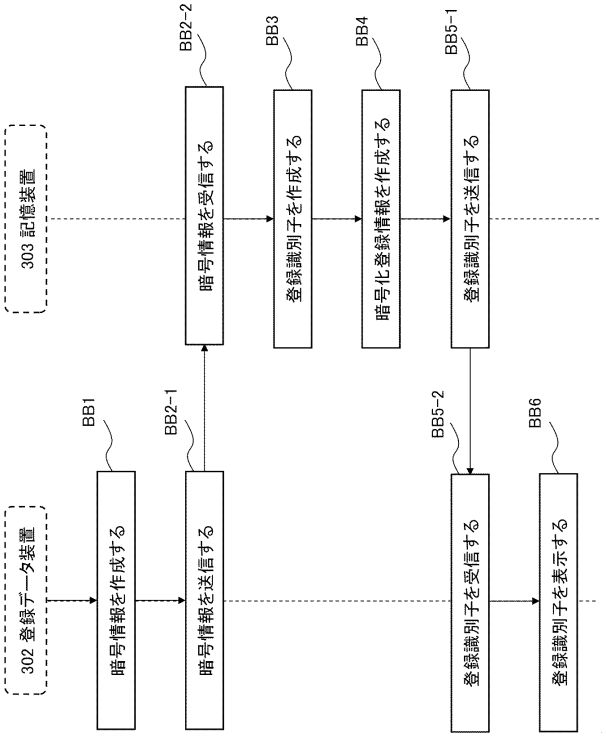
【図７】


301
照合システム
303
記憶装置
108
暗号文記憶部
307
識別子管理部
305
照合補助装置
314
鍵生成部
315
照合補助部
119
鍵記憶部
304
データ照合装置
313
照合情報送信部
115
照合補助依頼部
116
判定部
302
登録データ装置
306
暗号化部
308
照合要求装置
309
照合要求部
310
暗号化距離部
311
距離集合部
312
シャッフル部

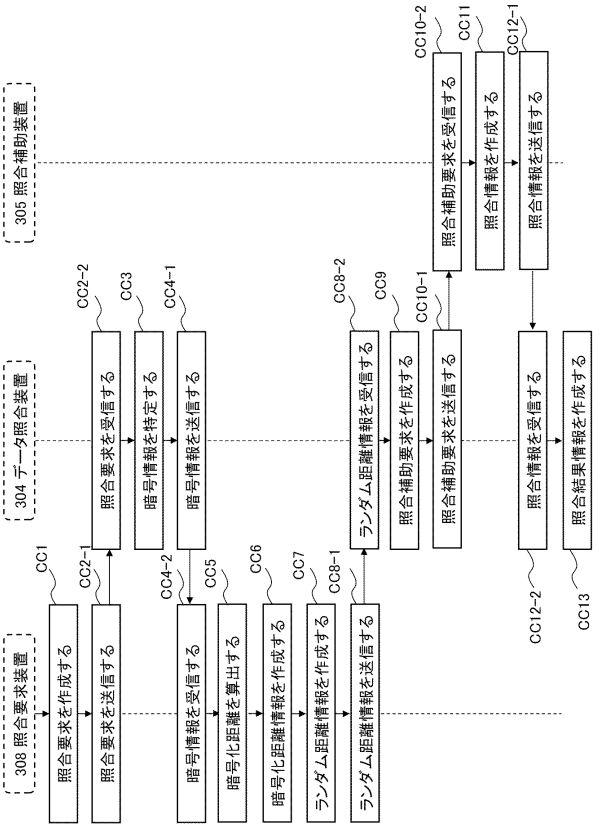
【図８】


305 照合補助装置
暗号鍵と復号鍵を作成する
AA1
暗号鍵を公開する
AA2
復号鍵を格納する
AA3

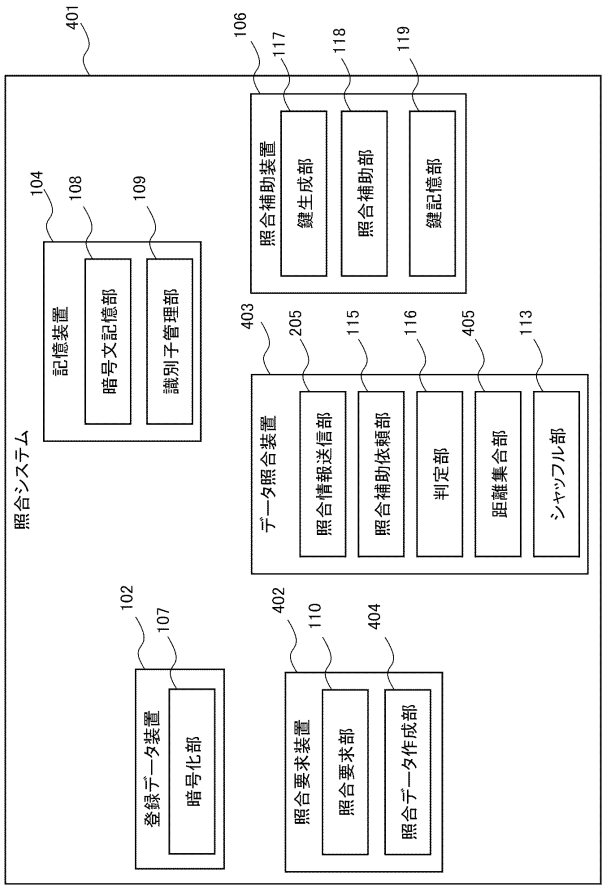
【図９】


303 記憶装置
302 登録データ装置
暗号情報を作成する
BB1
暗号情報を送信する
BB2-1
暗号情報を受信する
BB2-2
登録識別子を作成する
BB3
暗号化登録情報を作成する
BB4
登録識別子を送信する
BB5-1
登録識別子を受信する
BB5-2
登録識別子を表示する
BB6

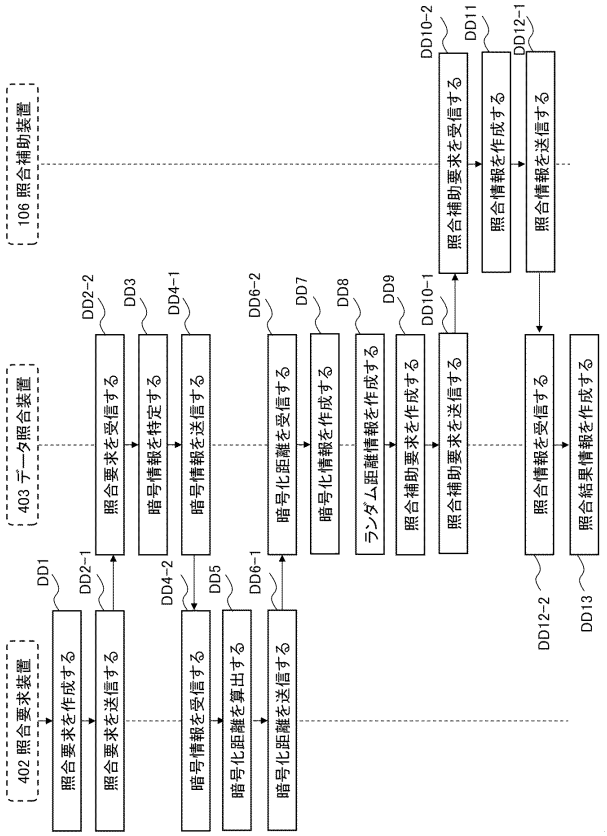
【図１０】


305 照合補助装置
304 データ照合装置
308 照合要求装置
照合要求を作成する
CC1
照合要求を送信する
CC2-1
照合要求を受信する
CC2-2
暗号情報を特定する
CC3
暗号情報を送信する
CC4-1
暗号情報を受信する
CC4-2
暗号化距離を算出する
CC5
暗号化距離情報を作成する
CC6
ランダム距離情報を作成する
CC7
ランダム距離情報を送信する
CC8-1
ランダム距離情報を受信する
CC8-2
照合補助要求を作成する
CC9
照合補助要求を送信する
CC10-1
照合補助要求を受信する
CC10-2
照合情報を作成する
CC11
照合情報を送信する
CC12-1
照合情報を受信する
CC12-2
照合結果情報を作成する
CC13

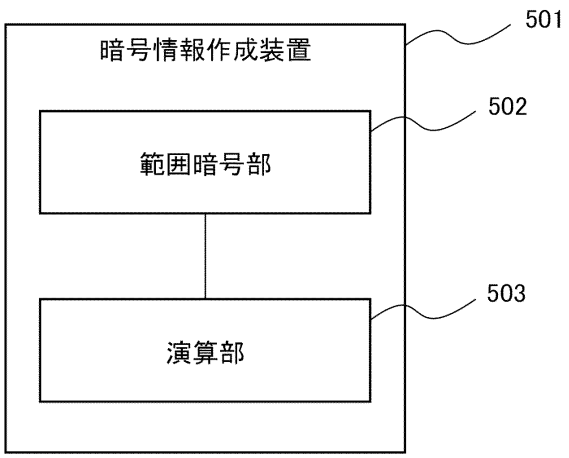
【図１１】



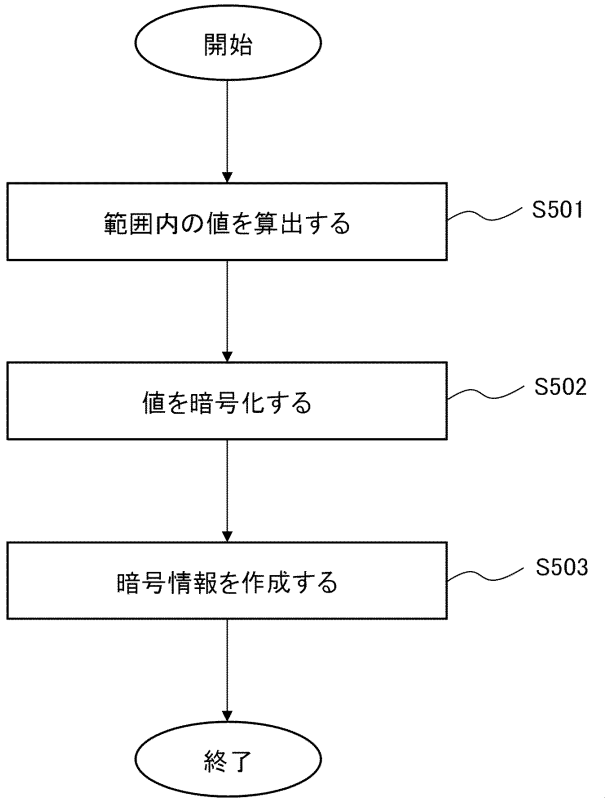
【図１２】



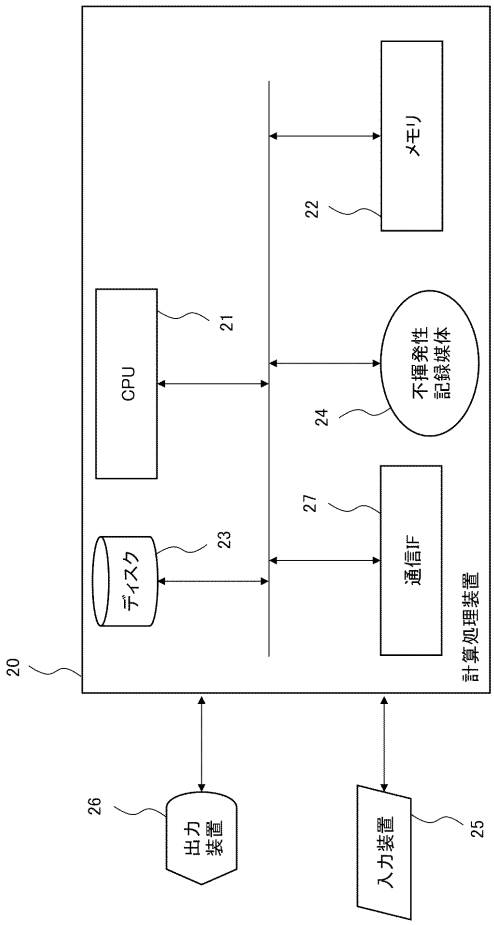
【図１３】



【図１４】



【図１５】


20
計算処理装置
CPU
21
メモリ
22
ディスク
23
不揮発性
記録媒体
24
通信IF
27
出力
装置
26
入力装置
25

フロントページの続き

(56)参考文献 特開２０１０－２３７６５３（ＪＰ，Ａ）
特開２００９－１２９２９２（ＪＰ，Ａ）
特表２００８－５２１０２５（ＪＰ，Ａ）
尾形わかは 他，リモートバイオメトリクス認証に有効な「近い」ことを示す零知識証明プロトコル，第２９回情報理論とその応用シンポジウム 予稿集，日本，情報理論とその応用学会，２００６年１１月２８日，pp.319-322
小暮 淳 他，準同型暗号を用いた秘匿生体認証，２０１４年 暗号と情報セキュリティシンポジウム概要集，日本，電子情報通信学会，２０１４年 1月２４日，pp.1-8

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