(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第5274271号
(P5274271)

(45)発行日　平成25年8月28日(2013.8.28)　(24)登録日　平成25年5月24日(2013.5.24)

(51)Int.Cl.　　F I
G09C 1/00 (2006.01)　　G09C 1/00 660D
G06F 21/62 (2013.01)　　G06F 21/24 166A
　　G09C 1/00 650Z

請求項の数 12　(全 56 頁)

(21)出願番号　特願2009-7892(P2009-7892)
(22)出願日　平成21年1月16日(2009.1.16)
(65)公開番号　特開2010-164835(P2010-164835A)
(43)公開日　平成22年7月29日(2010.7.29)
審査請求日　平成23年10月24日(2011.10.24)

(73)特許権者　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目７番３号
(74)代理人　100099461
弁理士　溝井　章司
(72)発明者　服部　充洋
東京都千代田区丸の内二丁目７番３号　三菱電機株式会社内
(72)発明者　伊藤　隆
東京都千代田区丸の内二丁目７番３号　三菱電機株式会社内
(72)発明者　松田　規
東京都千代田区丸の内二丁目７番３号　三菱電機株式会社内

最終頁に続く

(54)【発明の名称】検索システム及び索引暗号化装置及び検索暗号化装置及び検索装置及びコンピュータプログラム及び検索方法

(57)【特許請求の範囲】
【請求項１】
索引暗号化装置と、検索暗号化装置と、検索装置とを有し、
上記索引暗号化装置は、データを記憶する記憶装置と、データを処理する処理装置と、索引記憶部と、索引暗号化部とを有し、
上記索引記憶部は、上記記憶装置を用いて、１以上ｎ以下のｎ個の整数（ｎは１以上の整数。）に対応するｎ個の索引データを記憶し、
上記索引暗号化部は、上記処理装置を用いて、１以上ｎ以下のｎ個の整数それぞれについて、上記索引記憶部が記憶した索引データを暗号化して、ｎ個の暗号化索引データとし、
上記検索暗号化装置は、データを記憶する記憶装置と、データを処理する処理装置と、検索記憶部と、多項式値算出部と、検索暗号化部とを有し、
上記検索記憶部は、上記記憶装置を用いて、１以上ｎ以下のｎ個の整数に対応するｎ個の検索データを記憶し、
上記多項式値算出部は、上記処理装置を用いて、１以上ｎ以下のｎ個の整数それぞれについて、（ｄ－１）次の一変数多項式（ｄは１以上ｎ以下の整数。）に上記整数を代入した値を算出して、ｎ個の多項式値とし、
上記検索暗号化部は、上記処理装置を用いて、１以上ｎ以下のｎ個の整数それぞれについて、上記検索記憶部が記憶した検索データと、上記多項式値算出部が算出した多項式値との組を暗号化して、ｎ個の暗号化検索データとし、

上記検索装置は、データを処理する処理装置と、データを記憶する記憶装置と、暗号化索引記憶部と、暗号化検索記憶部と、判定対象選択部と、補間係数値算出部と、写像算出部と、比較算出部と、判定部とを有し、
上記暗号化索引記憶部は、上記記憶装置を用いて、上記索引暗号化装置が暗号化したｎ個の暗号化索引データを記憶し、
上記暗号化検索記憶部は、上記記憶装置を用いて、上記検索暗号化装置が暗号化したｎ個の暗号化検索データを記憶し、
上記判定対象選択部は、上記処理装置を用いて、１以上ｎ以下のｎ個の整数のなかからｄ個の整数を選択して、ｄ個の判定対象整数とし、
上記補間係数値算出部は、上記処理装置を用いて、上記判定対象選択部が選択したｄ個の判定対象整数に基づいて、ラグランジュの補間係数の値を算出して、ｄ個の補間係数値とし、
上記写像算出部は、上記処理装置を用いて、上記判定対象選択部が選択したｄ個の判定対象整数それぞれについて、上記暗号化索引記憶部が記憶した暗号化索引データと、上記暗号化検索記憶部が記憶した暗号化検索データと、上記補間係数値算出部が算出した補間係数値との組を写像して、ｄ個の写像データとし、
上記比較算出部は、上記処理装置を用いて、上記写像算出部が写像したｄ個の写像データに基づいて、比較データを算出し、
上記判定部は、上記処理装置を用いて、上記比較算出部が算出した比較データに基づいて、上記判定対象選択部が選択したｄ個の判定対象整数について、上記索引データと、上記検索データとが一致するか否かを判定することを特徴とする検索システム。
【請求項２】
上記補間係数値算出部は、上記処理装置を用いて、上記判定対象選択部が選択したｄ個の判定対象整数のうちの一つを対象整数とし、上記判定対象選択部が選択したｄ個の判定対象整数のうち上記対象整数以外の（ｄ－１）個の判定対象整数を（ｄ－１）個の対象外整数とし、（ｄ－１）個の対象外整数それぞれについて、上記対象外整数から上記対象整数を差し引いた差で、上記対象外整数を割った商を算出し、算出した（ｄ－１）個の商の総積を算出して、上記対象整数についての補間係数値とすることを特徴とする請求項１に記載の検索システム。
【請求項３】
上記多項式値算出部は、上記処理装置を用いて、所定の秘密整数を上記一変数多項式の定数項として、上記多項式値を算出することを特徴とする請求項１または請求項２に記載の検索システム。
【請求項４】
上記検索システムは、更に、設定装置を有し、
上記設定装置は、秘密整数生成部と、公開元算出部とを有し、
上記秘密整数生成部は、上記処理装置を用いて、１以上ｐ未満の整数（ｐは素数。）をランダムに生成して、秘密整数とし、
上記公開元算出部は、上記処理装置を用いて、０以上ｐ未満の整数を位数ｐの群の元に単射する第一の写像により、上記秘密整数生成部が生成した秘密整数を写像した元を算出して、公開元とし、
上記索引暗号化装置は、公開元記憶部と、索引整数記憶部と、索引元算出部と、判定元算出部とを有し、
上記公開元記憶部は、上記記憶装置を用いて、上記設定装置が算出した公開元を記憶し、
上記索引整数記憶部は、上記記憶装置を用いて、ｎ個の１以上ｐ未満の整数を、１以上ｎ以下のｎ個の整数それぞれに対応する索引整数として記憶し、
上記索引元算出部は、上記処理装置を用いて、１以上ｎ以下のｎ個の整数それぞれについて、上記索引整数記憶部が記憶した索引整数に基づいて、０以上ｐ未満の整数を位数ｐの群の元に単射する第二の写像により、上記索引整数を写像した元を算出して、ｎ個の索

引元とし、
上記判定元算出部は、上記処理装置を用いて、上記公開元記憶部が記憶した公開元に基づいて、位数ｐの群の元を位数ｐの群の元に単射する第三の写像により、上記公開元を写像した元を算出して、判定元とし、
上記検索暗号化装置は、秘密整数記憶部と、検索整数記憶部と、多項式係数生成部と、検索元算出部とを有し、
上記秘密整数記憶部は、上記記憶装置を用いて、上記設定装置が生成した秘密整数を記憶し、
上記検索整数記憶部は、上記記憶装置を用いて、ｎ個の１以上ｐ未満の整数を、１以上ｎ以下のｎ個の整数それぞれに対応する検索整数として記憶し、
上記多項式係数生成部は、上記処理装置を用いて、（ｄ－１）個の０以上ｐ未満の整数をランダムに生成して、（ｄ－１）個の多項式係数とし、
上記多項式値算出部は、上記処理装置を用いて、上記秘密整数記憶部が記憶した秘密整数を、上記一変数多項式の定数項とし、上記多項式係数生成部が生成した（ｄ－１）個の多項式係数を、上記一変数多項式の１次から（ｄ－１）次までの各項の係数として、上記多項式値を算出し、
上記検索元算出部は、上記処理装置を用いて、１以上ｎ以下のｎ個の整数それぞれについて、上記検索整数記憶部が記憶した検索整数と、上記多項式値算出部が算出した多項式値とに基づいて、１以上ｐ未満の整数と０以上ｐ未満の整数との組を位数ｐの群の元に写像する第四の写像により、上記検索整数と上記多項式値との組を写像した元を算出して、ｎ個の検索元とし、
上記検索装置は、索引元記憶部と、判定元記憶部と、検索元記憶部と、写像元算出部と、比較元算出部とを有し、
上記索引元記憶部は、上記記憶装置を用いて、上記索引暗号化装置が算出したｎ個の索引元を記憶し、
上記判定元記憶部は、上記記憶装置を用いて、上記索引暗号化装置が算出した判定元を記憶し、
上記検索元記憶部は、上記記憶装置を用いて、上記検索暗号化装置が算出したｎ個の検索元を記憶し、
上記写像元算出部は、上記処理装置を用いて、上記判定対象選択部が選択したｄ個の判定対象整数それぞれについて、上記索引元記憶部が記憶した索引元と、上記検索元記憶部が記憶した検索元と、上記補間係数値算出部が算出した補間係数値とに基づいて、位数ｐの群の元と位数ｐの群の元と０以上ｐ未満の整数との組を位数ｐの群の元に写像する第五の写像により、上記索引元と上記検索元と上記補間係数値との組を写像した元を算出して、ｄ個の写像元とし、
上記比較元算出部は、上記処理装置を用いて、上記写像元算出部が算出したｄ個の写像元を群演算により結合した元を算出して、比較元とし、
上記判定部は、上記処理装置を用いて、上記比較元算出部が算出した比較元と、上記判定元記憶部が記憶した判定元とが等しい場合に、上記判定対象選択部が選択したｄ個の判定対象整数について、上記索引整数と、上記検索整数とが一致すると判定することを特徴とする請求項１乃至請求項３のいずれかに記載の検索システム。
【請求項５】
上記判定元算出部は、０以上ｐ未満の任意の整数について、上記任意の整数を上記第一の写像により写像した元を、上記第三の写像により写像した元が、上記任意の整数と等しい数の所定の元を、群演算により結合した元と等しくなる写像を、上記第三の写像として用い、
上記写像元算出部は、１以上ｐ未満の任意の第一の整数について、上記任意の第一の整数を上記第二の写像により写像した元と、上記任意の第一の整数と第二の整数との組を上記第四の写像により写像した元と、第三の整数との組を、上記第五の写像により写像した元が、上記第二の整数と上記第三の整数との積と等しい数の上記所定の元を、群演算によ

り結合した元と等しくなる写像を、上記第五の写像として用いることを特徴とする請求項４に記載の検索システム。

【請求項６】

上記設定装置は、更に、秘密乱数生成部と、公開乱数元算出部とを有し、

上記秘密乱数生成部は、上記処理装置を用いて、１以上ｎ以下のｎ個の整数それぞれについて、１以上ｐ未満の整数をランダムに生成して、ｎ個の秘密乱数とし、

上記公開元算出部は、上記処理装置を用いて、第一の群の元と第二の群の元との組を第三の群の元に写像する双線形ペアリング写像（上記第一の群及び上記第二の群及び上記第三の群の位数はｐ。）により、上記第一の群の生成元である第一生成元と、上記第二の群の生成元である第二生成元との組を写像した元である第三生成元と、上記秘密整数生成部が生成した秘密整数とに基づいて、上記秘密整数と等しい数の上記第三生成元を、上記第三の群の群演算により結合した元を算出して、公開元とし、

上記公開乱数元算出部は、上記処理装置を用いて、１以上ｎ以下のｎ個の整数それぞれについて、上記第一生成元と、上記秘密乱数生成部が生成した秘密乱数とに基づいて、上記秘密乱数と等しい数の上記第一生成元を、上記第一の群の群演算により結合した元を算出して、ｎ個の公開乱数元とし、

上記索引暗号化装置は、更に、公開乱数元記憶部と、索引乱数生成部とを有し、

上記公開乱数元記憶部は、上記記憶装置を用いて、上記設定装置が算出したｎ個の公開乱数元を記憶し、

上記索引乱数生成部は、上記処理装置を用いて、１以上ｐ未満の整数をランダムに生成して、索引乱数とし、

上記判定元算出部は、上記処理装置を用いて、上記公開元記憶部が記憶した公開元と、上記索引乱数生成部が生成した索引乱数とに基づいて、上記索引乱数と等しい数の上記公開元を、上記第三の群の群演算により結合した元を算出して、判定元とし、

上記索引元算出部は、上記処理装置を用いて、１以上ｎ以下のｎ個の整数それぞれについて、上記公開乱数元記憶部が記憶した公開乱数元と、上記索引整数記憶部が記憶した索引整数と、上記索引乱数生成部が生成した索引乱数とに基づいて、上記索引整数と上記索引乱数との積と等しい数の上記公開乱数元を、上記第一の群の群演算により結合した元を算出して、ｎ個の索引元とし、

上記検索暗号化装置は、更に、秘密乱数記憶部を有し、

上記秘密乱数記憶部は、上記記憶装置を用いて、上記設定装置が生成したｎ個の秘密乱数を記憶し、

上記検索元算出部は、上記処理装置を用いて、１以上ｎ以下のｎ個の整数それぞれについて、上記第二生成元と、上記秘密乱数記憶部が記憶した秘密乱数と、上記検索整数記憶部が記憶した検索整数と、上記多項式値算出部が算出した多項式値とに基づいて、上記秘密乱数と上記検索整数との積で上記多項式値を割った商と等しい数の上記第二生成元を、上記第二の群の群演算により結合した元を算出して、ｎ個の検索元とし、

上記検索装置において、

上記写像元算出部は、上記処理装置を用いて、上記判定対象選択部が選択したｄ個の判定対象整数それぞれについて、上記索引元記憶部が記憶した索引元と、上記検索元記憶部が記憶した検索元とに基づいて、上記双線形ペアリング写像により上記索引元と上記検索元との組を写像した上記第三の群の元を算出して、ｄ個のペアリング値とし、上記判定対象選択部が選択したｄ個の判定対象整数それぞれについて、算出した上記ペアリング値と、上記補間係数値算出部が算出した補間係数値とに基づいて、上記補間係数値と等しい数の上記ペアリング値を、上記第三の群の群演算により結合した元を算出して、ｄ個の写像元とし、

上記比較元算出部は、上記処理装置を用いて、上記写像元算出部が算出したｄ個の写像元を、上記第三の群の群演算により結合した元を算出して、比較元とすることを特徴とする請求項４または請求項５に記載の検索システム。

【請求項７】

上記設定装置は、更に、公開乱数元算出部を有し、
上記公開元算出部は、上記処理装置を用いて、第一の群の生成元である第一生成元（上記第一の群の位数はｐ。）と、上記秘密整数生成部が生成した秘密整数とに基づいて、上記秘密整数と等しい数の上記第一生成元を、上記第一の群の群演算により結合した元を算出して、公開元とし、
上記公開乱数元算出部は、上記処理装置を用いて、１以上ｎ以下のｎ個の整数それぞれについて、第二の群の生成元（上記第二の群の位数はｐ。）をランダムに生成して、ｎ個の公開乱数元とし、
上記索引暗号化装置は、更に、公開乱数元記憶部と、乱数元算出部と、索引乱数生成部とを有し、
上記公開乱数元記憶部は、上記記憶装置を用いて、上記設定装置が算出したｎ個の公開乱数元を記憶し、
上記索引乱数生成部は、上記処理装置を用いて、１以上ｐ未満の整数をランダムに生成して、索引乱数とし、
上記判定元算出部は、上記処理装置を用いて、上記第二の群の生成元である第二生成元と、上記公開元記憶部が記憶した公開元とに基づいて、上記第一の群の元と上記第二の群の元との組を第三の群の元（上記第三の群の位数はｐ。）に写像する双線形ペアリング写像により、上記公開元と上記第二生成元との組が写像される上記第三の群の元を算出し、算出した上記第三の群の元と、上記索引乱数生成部が生成した索引乱数とに基づいて、上記索引乱数と等しい数の上記第三の群の元を、上記第三の群の群演算により結合した元を算出して、判定元とし、
上記乱数元算出部は、上記処理装置を用いて、上記第一生成元と、上記索引乱数生成部が生成した索引乱数とに基づいて、上記索引乱数と等しい数の上記第一生成元を、上記第一の群の群演算により結合した元を算出して、乱数元とし、
上記索引元算出部は、上記処理装置を用いて、１以上ｎ以下のｎ個の整数それぞれについて、上記索引整数記憶部が記憶した索引整数と、上記公開乱数元記憶部が記憶した公開乱数元とに基づいて、０以上ｐ未満の整数と上記第二の群の元との組を上記第二の群の元に写像する写像関数により、上記索引整数と上記公開乱数元との組を写像した上記第二の群の元を算出して、ｎ個の索引関数値とし、１以上ｎ以下のｎ個の整数それぞれについて、算出した上記索引関数値と、上記索引乱数生成部が生成した索引乱数とに基づいて、上記索引乱数と等しい数の上記索引関数値を、上記第二の群の群演算により結合した元を算出して、ｎ個の索引元とし、
上記検索暗号化装置は、更に、公開乱数元記憶部と、検索乱数生成部と、検索乱数元算出部とを有し、
上記公開乱数元記憶部は、上記記憶装置を用いて、上記設定装置が算出したｎ個の公開乱数元を記憶し、
上記検索乱数生成部は、上記処理装置を用いて、１以上ｎ以下のｎ個の整数それぞれについて、１以上ｐ未満の整数をランダムに生成して、ｎ個の検索乱数とし、
上記検索元算出部は、上記処理装置を用いて、１以上ｎ以下のｎ個の整数それぞれについて、上記検索整数記憶部が記憶した検索整数と、上記公開乱数元記憶部が記憶した公開乱数元とに基づいて、上記写像関数により、上記検索整数と上記公開乱数元との組を写像して、上記第二の群の元を算出して、ｎ個の検索関数値とし、１以上ｎ以下のｎ個の整数それぞれについて、算出した上記検索関数値と、上記検索乱数生成部が生成した検索乱数とに基づいて、上記検索乱数と等しい数の上記検索関数値を、上記第二の群の群演算により結合した元を算出し、上記第二生成元と、上記多項式値算出部が算出した多項式値とに基づいて、上記多項式値と等しい数の上記第二生成元を、上記第二の群の群演算により結合した元を算出し、算出した上記第二の群の二つの元を上記第二の群の群演算により結合した元を算出して、ｎ個の検索元とし、
上記検索乱数元算出部は、上記処理装置を用いて、１以上ｎ以下のｎ個の整数それぞれについて、上記第一生成元と、上記検索乱数生成部が生成した検索乱数とに基づいて、上

記検索乱数と等しい数の上記第一生成元を、上記第一の群の群演算により結合した元を算出して、ｎ個の検索乱数元とし、
上記検索装置は、更に、乱数元記憶部と、検索乱数元記憶部とを有し、
上記乱数元記憶部は、上記記憶装置を用いて、上記索引暗号化装置が算出した乱数元を記憶し、
上記検索乱数元記憶部は、上記記憶装置を用いて、上記検索暗号化装置が算出したｎ個の検索乱数元を記憶し、
上記写像元算出部は、上記処理装置を用いて、上記判定対象選択部が選択したｄ個の判定対象整数それぞれについて、上記乱数元記憶部が記憶した乱数元と、上記検索元記憶部が記憶した検索元とに基づいて、上記双線形ペアリング写像により、上記乱数元と上記検索元との組を写像した上記第三の群の元を算出して、ｄ個の第一ペアリング値とし、上記判定対象選択部が選択したｄ個の判定対象整数それぞれについて、上記検索乱数元記憶部が記憶した検索乱数元と、上記索引元記憶部が記憶した索引元とに基づいて、上記双線形ペアリング写像により、上記検索乱数元と上記索引元との組を写像した上記第三の群の元を算出して、ｄ個の第二ペアリング値とし、上記判定対象選択部が選択したｄ個の判定対象整数それぞれについて、算出した上記第一ペアリング値と、算出した上記第二ペアリング値の逆元とを上記第三の群の群演算により結合した元を算出して、ｄ個の写像元とし、
上記比較元算出部は、上記処理装置を用いて、上記写像元算出部が算出したｄ個の写像元を、上記第三の群の群演算により結合した元を算出して、比較元とすることを特徴とする請求項４または請求項５に記載の検索システム。
【請求項８】
上記索引暗号化装置は、更に、索引変換部を有し、
上記索引変換部は、上記処理装置を用いて、１以上ｎ以下のｎ個の整数に対応するｎ個の索引文字列を入力し、１以上ｎ以下のｎ個の整数それぞれについて、任意の長さの文字列を１以上ｐ未満の整数に変換する変換写像により、入力した索引文字列を変換して、ｎ個の索引整数とし、
上記索引整数記憶部は、上記記憶装置を用いて、上記索引変換部が変換したｎ個の索引整数を記憶し、
上記検索暗号化装置は、更に、検索変換部を有し、
上記検索変換部は、上記処理装置を用いて、１以上ｎ以下のｎ個の整数に対応するｎ個の検索文字列を入力し、１以上ｎ以下のｎ個の整数それぞれについて、上記変換写像により、入力した検索文字列を変換して、ｎ個の検索整数とし、
上記検索整数記憶部は、上記記憶装置を用いて、上記検索変換部が変換したｎ個の検索整数を記憶することを特徴とする請求項４乃至請求項７のいずれかに記載の検索システム。
【請求項９】
データを記憶する記憶装置と、データを処理する処理装置と、検索記憶部と、多項式値算出部と、検索暗号化部とを有し、
上記検索記憶部は、上記記憶装置を用いて、１以上ｎ以下のｎ個の整数（ｎは１以上の整数。）に対応するｎ個の検索データを記憶し、
上記多項式値算出部は、上記処理装置を用いて、１以上ｎ以下のｎ個の整数それぞれについて、（ｄ－１）次の一変数多項式（ｄは１以上ｎ以下の整数。）に上記整数を代入した値を算出して、ｎ個の多項式値とし、
上記検索暗号化部は、上記処理装置を用いて、１以上ｎ以下のｎ個の整数それぞれについて、上記検索記憶部が記憶した検索データと、上記多項式値算出部が算出した多項式値との組を暗号化して、ｎ個の暗号化検索データとすることを特徴とする検索暗号化装置。
【請求項１０】
データを処理する処理装置と、データを記憶する記憶装置と、暗号化索引記憶部と、暗号化検索記憶部と、判定対象選択部と、補間係数値算出部と、写像算出部と、比較算出部と、判定部とを有し、

上記暗号化索引記憶部は、上記記憶装置を用いて、１以上ｎ以下のｎ個の整数（ｎは１以上の整数。）に対応するｎ個の索引データをそれぞれ暗号化したｎ個の暗号化索引データを記憶し、

上記暗号化検索記憶部は、上記記憶装置を用いて、１以上ｎ以下のｎ個の整数に対応するｎ個の検索データをそれぞれ暗号化したｎ個の暗号化検索データを記憶し、

上記判定対象選択部は、上記処理装置を用いて、１以上ｎ以下のｎ個の整数のなかからｄ個の整数（ｄは１以上ｎ以下の整数。）を選択して、ｄ個の判定対象整数とし、

上記補間係数値算出部は、上記処理装置を用いて、上記判定対象選択部が選択したｄ個の判定対象整数に基づいて、ラグランジュの補間係数の値を算出して、ｄ個の補間係数値とし、

上記写像算出部は、上記処理装置を用いて、上記判定対象選択部が選択したｄ個の判定対象整数それぞれについて、上記暗号化索引記憶部が記憶した暗号化索引データと、上記暗号化検索記憶部が記憶した暗号化検索データと、上記補間係数値算出部が算出した補間係数値との組を写像して、ｄ個の写像データとし、

上記比較算出部は、上記処理装置を用いて、上記写像算出部が写像したｄ個の写像データに基づいて、比較データを算出し、

上記判定部は、上記処理装置を用いて、上記比較算出部が算出した比較データに基づいて、上記判定対象選択部が選択したｄ個の判定対象整数について、上記索引データと、上記検索データとが一致するか否かを判定することを特徴とする検索装置。

【請求項１１】

データを記憶する記憶装置と、データを処理する処理装置とを有するコンピュータが実行することにより、上記コンピュータが請求項１０に記載の検索暗号化装置または請求項１１に記載の検索装置として機能することを特徴とするコンピュータプログラム。

【請求項１２】

索引暗号化装置が索引データを暗号化した暗号化索引データと、検索暗号化装置が検索データを暗号化した暗号化検索データとを用いて、検索装置が上記索引データと上記検索データとが一致するか否かを判定する検索方法において、

上記索引暗号化装置が、１以上ｎ以下のｎ個の整数（ｎは１以上の整数。）に対応するｎ個の索引データを記憶し、

上記索引暗号化装置が、１以上ｎ以下のｎ個の整数それぞれについて、記憶した索引データを暗号化して、ｎ個の暗号化索引データとし、

上記検索暗号化装置が、１以上ｎ以下のｎ個の整数に対応するｎ個の検索データを記憶し、

上記検索暗号化装置が、１以上ｎ以下のｎ個の整数それぞれについて、（ｄ－１）次の一変数多項式（ｄは１以上ｎ以下の整数。）に上記整数を代入した値を算出して、ｎ個の多項式値とし、

上記検索暗号化装置が、１以上ｎ以下のｎ個の整数それぞれについて、記憶した検索データと、算出した多項式値との組を暗号化して、ｎ個の暗号化検索データとし、

上記検索装置が、上記索引暗号化装置が暗号化したｎ個の暗号化索引データを記憶し、

上記検索装置が、上記検索暗号化装置が暗号化したｎ個の暗号化検索データを記憶し、

上記検索装置が、１以上ｎ以下のｎ個の整数のなかからｄ個の整数を選択して、ｄ個の判定対象整数とし、

上記検索装置が、選択したｄ個の判定対象整数に基づいて、ラグランジュの補間係数の値を算出して、ｄ個の補間係数値とし、

上記検索装置が、選択したｄ個の判定対象整数それぞれについて、記憶した暗号化索引データと、記憶した暗号化検索データと、算出した補間係数値との組を写像して、ｄ個の写像データとし、

上記検索装置が、写像したｄ個の写像データに基づいて、比較データを算出し、

上記検索装置が、算出した比較データに基づいて、選択したｄ個の判定対象整数について、上記索引データと、上記検索データとが一致するか否かを判定することを特徴とする

検索方法。
【発明の詳細な説明】
【技術分野】
【０００１】
この発明は、暗号化したままの状態で、暗号化した索引を暗号化した検索文により検索する秘匿検索に関する。
【背景技術】
【０００２】
秘匿検索とは、大量の暗号化されたデータのなかから欲しいデータを検索する場合において、暗号化されたデータを復号することなく、暗号化されたままの状態で検索をすることである。
秘匿検索には、検索に用いるキーワードをあらかじめ定めて索引キーワードとし、これを暗号化したものに対して、検索キーワードを指定して検索を行い、索引キーワードと検索キーワードとが一致するものを抽出する方式がある。
【０００３】
また、このような特殊な暗号方式を実現するための技術として、代数曲線上のペアリングなどの双線形ペアリング写像を利用する方式がある。
【先行技術文献】
【特許文献】
【０００４】
【特許文献１】特表２００５－５００７４０号公報
【特許文献２】特開２００７－１１４４９４号公報
【非特許文献】
【０００５】
【非特許文献１】Ｄａｎ Ｂｏｎｅｈ、Ｍａｔｔｈｅｗ Ｆｒａｎｋｌｉｎ著「Ｉｄｅｎｔｉｔｙ－Ｂａｓｅｄ Ｅｎｃｒｙｐｔｉｏｎ ｆｒｏｍ ｔｈｅ Ｗｅｉｌ Ｐａｉｒｉｎｇ」、Ｃｒｙｐｔｏ ２００１、ＬＮＣＳ第２１３９巻、２１３～２２９ページ、Ｓｐｒｉｎｇｅｒ－Ｖｅｒｌａｇ、２００１年。
【非特許文献２】Ｄａｎ Ｂｏｎｅｈ、Ｇｉｏｖａｎｎｉ Ｄｉ Ｃｒｅｓｃｅｎｚｏ、Ｒａｆａｉｌ Ｏｓｔｒｏｖｓｋｙ、Ｇｉｕｓｅｐｐｅ Ｐｅｒｓｉａｎｏ著「Ｐｕｂｌｉｃ Ｋｅｙ Ｅｎｃｒｙｐｔｉｏｎ ｗｉｔｈ ｋｅｙｗｏｒｄ Ｓｅａｒｃｈ」、Ｅｕｒｏｃｒｙｐｔ ２００４、ＬＮＣＳ第３０２７巻、５０６～５２２ページ、２００４年。
【非特許文献３】Ｊｏｎａｔｈａｎ Ｋａｔｚ、Ａｍｉｔ Ｓａｈａｉ、Ｂｒｅｎｔ Ｗａｔｅｒｓ著「Ｐｒｅｄｉｃａｔｅ Ｅｎｃｒｙｐｔｉｏｎ Ｓｕｐｐｏｒｔｉｎｇ Ｄｉｓｊｕｎｃｔｉｏｎｓ，Ｐｏｌｙｎｏｍｉａｌ Ｅｑｕａｔｉｏｎｓ，ａｎｄ Ｉｎｎｅｒ Ｐｒｏｄｕｃｔｓ」、Ｅｕｒｏｃｒｙｐｔ ２００８、ＬＮＣＳ第４９６５巻、１４６～１６２ページ、２００８年。
【発明の概要】
【発明が解決しようとする課題】
【０００６】
索引キーワードが複数種類あり、そのうちの一定数以上が、対応する検索キーワードと一致するものを抽出したい場合、索引キーワードが１つの場合における秘匿検索を応用し、抽出された集合に対して集合演算により抽出したいデータの集合を得る方式が考えられる。
しかし、この方式では、どのキーワードが一致したかすべてわかってしまうので、暗号方式としての安全性が低くなる可能性がある。
この発明は、例えば、上記のような課題を解決するためになされたものであり、検索実行時にどのキーワードが一致したかについての情報をできるだけ隠蔽することにより、暗号方式としての安全性を高めることを目的とする。

【課題を解決するための手段】
【０００７】
この発明にかかる検索システムは、
索引暗号化装置と、検索暗号化装置と、検索装置とを有し、
上記索引暗号化装置は、データを記憶する記憶装置と、データを処理する処理装置と、索引記憶部と、索引暗号化部とを有し、
上記索引記憶部は、上記記憶装置を用いて、１以上ｎ以下のｎ個の整数（ｎは１以上の整数。）に対応するｎ個の索引データを記憶し、
上記索引暗号化部は、上記処理装置を用いて、１以上ｎ以下のｎ個の整数それぞれについて、上記索引記憶部が記憶した索引データを暗号化して、ｎ個の暗号化索引データとし、
上記検索暗号化装置は、データを記憶する記憶装置と、データを処理する処理装置と、検索記憶部と、多項式値算出部と、検索暗号化部とを有し、
上記検索記憶部は、上記記憶装置を用いて、１以上ｎ以下のｎ個の整数に対応するｎ個の検索データを記憶し、
上記多項式値算出部は、上記処理装置を用いて、１以上ｎ以下のｎ個の整数それぞれについて、（ｄ－１）次の一変数多項式（ｄは１以上ｎ以下の整数。）に上記整数を代入した値を算出して、ｎ個の多項式値とし、
上記検索暗号化部は、上記処理装置を用いて、１以上ｎ以下のｎ個の整数それぞれについて、上記検索記憶部が記憶した検索データと、上記多項式値算出部が算出した多項式値との組を暗号化して、ｎ個の暗号化検索データとし、
上記検索装置は、データを処理する処理装置と、データを記憶する記憶装置と、暗号化索引記憶部と、暗号化検索記憶部と、判定対象選択部と、補間係数値算出部と、写像算出部と、比較算出部と、判定部とを有し、
上記暗号化索引記憶部は、上記記憶装置を用いて、上記索引暗号化装置が暗号化したｎ個の暗号化索引データを記憶し、
上記暗号化検索記憶部は、上記記憶装置を用いて、上記検索暗号化装置が暗号化したｎ個の暗号化検索データを記憶し、
上記判定対象選択部は、上記処理装置を用いて、１以上ｎ以下のｎ個の整数のなかからｄ個の整数を選択して、ｄ個の判定対象整数とし、
上記補間係数値算出部は、上記処理装置を用いて、上記判定対象選択部が選択したｄ個の判定対象整数に基づいて、ラグランジュの補間係数の値を算出して、ｄ個の補間係数値とし、
上記写像算出部は、上記処理装置を用いて、上記判定対象選択部が選択したｄ個の判定対象整数それぞれについて、上記暗号化索引記憶部が記憶した暗号化索引データと、上記暗号化検索記憶部が記憶した暗号化検索データと、上記補間係数値算出部が算出した補間係数値との組を写像して、ｄ個の写像データとし、
上記比較算出部は、上記処理装置を用いて、上記写像算出部が写像したｄ個の写像データに基づいて、比較データを算出し、
上記判定部は、上記処理装置を用いて、上記比較算出部が算出した比較データに基づいて、上記判定対象選択部が選択したｄ個の判定対象整数について、上記索引データと、上記検索データとが一致するか否かを判定することを特徴とする。
【発明の効果】
【０００８】
この発明にかかる検索システムによれば、（ｄ－１）次の一変数多項式の値を用いて、検索データを暗号化し、ラグランジュの補間係数の値を用いて、検索を実行するので、ｎ個のデータのうちｄ個以上が一致する場合に、一致することを検索装置が判定でき、ｄ個未満しか一致しない場合には、いずれのデータが一致したかを検索装置が知ることができない。これにより、索引データや検索データに関する情報の漏洩を防ぐことができる。
【図面の簡単な説明】

【０００９】
【図１】実施の形態１における検索システム８００の全体構成の一例を示すシステム構成図。
【図２】実施の形態１における復号装置８１０、暗号化装置８２０、サーバ装置８３０の外観の一例を示す斜視図。
【図３】実施の形態１における復号装置８１０、暗号化装置８２０、サーバ装置８３０のハードウェア資源の一例を示す図。
【図４】実施の形態１における設定装置１００の構成の一例を示すブロック構成図。
【図５】実施の形態１における検索暗号化装置３００の構成の一例を示すブロック構成図。
【図６】実施の形態１における索引暗号化装置２００の構成の一例を示すブロック構成図。
【図７】実施の形態１における検索装置４００の構成の一例を示すブロック構成図。
【図８】実施の形態１におけるデータ暗号化装置８４０、暗号化データ記憶装置８５０、データ復号装置８６０の構成の一例を示すブロック構成図。
【図９】実施の形態１における設定処理Ｓ６１０の流れの一例を示すフローチャート図。
【図１０】実施の形態１における索引暗号化処理Ｓ６３０の流れの一例を示すフローチャート図。
【図１１】実施の形態１における検索暗号化処理Ｓ６５０の流れの一例を示すフローチャート図。
【図１２】実施の形態１における検索実行処理Ｓ６７０の流れの一例を示すフローチャート図。
【図１３】実施の形態２における設定装置１００の構成の一例を示すブロック構成図。
【図１４】実施の形態２における検索暗号化装置３００の構成の一例を示すブロック構成図。
【図１５】実施の形態２における索引暗号化装置２００の構成の一例を示すブロック構成図。
【図１６】実施の形態２における検索装置４００の構成の一例を示すブロック構成図。
【図１７】実施の形態２における設定処理Ｓ６１０の流れの一例を示すフローチャート図。
【図１８】実施の形態２における索引暗号化処理Ｓ６３０の流れの一例を示すフローチャート図。
【図１９】実施の形態２における検索暗号化処理Ｓ６５０の流れの一例を示すフローチャート図。
【図２０】実施の形態２における検索実行処理Ｓ６７０の流れの一例を示すフローチャート図。
【発明を実施するための形態】
【００１０】
実施の形態１.
実施の形態１について、図１～図１２を用いて説明する。
【００１１】
図１は、この実施の形態における検索システム８００の全体構成の一例を示すシステム構成図である。
検索システム８００は、復号装置８１０、暗号化装置８２０、サーバ装置８３０を有する。
暗号化装置８２０は、データ本体（平文データ）とデータ本体をキーワード検索するための索引とを暗号化して、サーバ装置８３０に送る。サーバ装置８３０は、暗号化装置８２０から送られたデータ本体や索引を復号することができない。サーバ装置８３０は、暗号化されたデータ本体と索引とを、暗号化されたまま蓄積する。復号装置８１０は、キーワード検索を実行するための検索文を暗号化して、サーバ装置８３０に送る。サーバ装置

８３０は、復号装置８１０から送られた検索文を復号することができない。サーバ装置８３０は、暗号化されたままの検索文により、暗号化されたまま蓄積した索引を検索し、ヒットしたか否かを判定して、検索結果を返す。サーバ装置８３０は、復号装置８１０からの要求により、検索にヒットした索引に対応するデータ本体を復号装置８１０に送る。復号装置８１０は、サーバ装置８３０から送られたデータ本体を復号して、復号したデータ本体を取得する。

【００１２】

データ本体は、例えば、指紋・光彩・静脈などの生体情報を表わす画像データ、電子メール、その他のデータベースの各レコードなどである。

１つのデータ本体に対して、所定の数（以下「索引数ｎ」と呼ぶ。）の索引が付けられる。例えば、画像データに対しては、位置や大きさなどを正規化した上で各ピクセルの値を索引とする。電子メールに対しては、差出人や日付などを索引とする。データベースに対しては、各フィールドのデータを索引とする。

検索条件は、閾値ｄと、各索引に対応するデータとを指定する。各索引の内容と、その索引に対して指定したデータとが一致する数が閾値ｄ以上である場合に、ヒットしたと判定される。例えば、画像データであれば、閾値として指定した数以上のピクセルの値が一致するものがヒットするので、類似する画像を検索することができる。

なお、指定したデータが異なる位置の索引と一致しても、それは一致したものとは数えない。例えば、電子メールの差出人を検索するために指定したデータが、電子メールの送信先と一致しても、一致したとは数えない。

【００１３】

復号装置８１０は、設定装置１００、検索暗号化装置３００、データ復号装置８６０を有する。

設定装置１００は、索引や検索文を暗号化したり、検索したりするために必要なパラメータを設定する。設定装置１００は、設定したパラメータの一部（以下「公開パラメータ」と呼ぶ。）を、検索システム８００内で公開し、他の一部（以下「秘密パラメータ」と呼ぶ。）を、検索暗号化装置３００に対して秘密裡に通知する。

検索暗号化装置３００は、設定装置１００が設定した秘密パラメータ（秘密情報）を秘密裡に保持する。検索暗号化装置３００は、検索条件を入力し、秘密パラメータや公開パラメータ（公開情報）を用いて、検索文を暗号化する。暗号化された検索文（以下「暗号化検索データ」と呼ぶ。）は、サーバ装置８３０に対して通知される。

データ復号装置８６０は、サーバ装置８３０から通知されたデータ本体を復号する。

【００１４】

暗号化装置８２０は、索引暗号化装置２００、データ暗号化装置８４０を有する。

索引暗号化装置２００は、設定装置１００が設定した公開パラメータを用いて、索引を暗号化する。

データ暗号化装置８４０は、データ本体を暗号化する。なお、データ暗号化装置８４０がデータ本体を暗号化し、データ復号装置８６０が復号する暗号方式は、既存の公開鍵暗号方式や共通鍵暗号方式などであってもよい。

暗号化された索引（以下「暗号化索引データ」と呼ぶ。）と暗号化されたデータ本体とは組として、サーバ装置８３０に対して通知される。

【００１５】

サーバ装置８３０は、検索装置４００、暗号化データ記憶装置８５０を有する。

検索装置４００は、暗号化装置８２０から通知された暗号化索引データを蓄積し、復号装置８１０から通知された暗号化検索データにより、検索を実行する。

暗号化データ記憶装置８５０は、暗号化装置８２０から通知されたデータ本体を暗号化されたまま蓄積する。

【００１６】

なお、復号装置８１０・暗号化装置８２０・サーバ装置８３０の数は、１つに限らず、２つ以上であってもよい。復号装置８１０が複数ある場合、暗号化装置８２０は、各復号

装置８１０について設定されたパラメータを用いて、索引データを暗号化する。したがって、１つの索引データに対して、復号装置８１０の数と等しい数の暗号化索引データを生成する。また、サーバ装置８３０は、各復号装置８１０について暗号化装置８２０が生成した暗号化索引データを蓄積し、各復号装置８１０からの要求にしたがって、その復号装置８１０について蓄積した暗号化検索データにより、検索を実行する。

【００１７】

図２は、この実施の形態における復号装置８１０、暗号化装置８２０、サーバ装置８３０の外観の一例を示す斜視図である。

復号装置８１０、暗号化装置８２０、サーバ装置８３０は、システムユニット９１０、ＣＲＴ（Ｃａｔｈｏｄｅ・Ｒａｙ・Ｔｕｂｅ）やＬＣＤ（液晶）の表示画面を有する表示装置９０１、キーボード９０２（Ｋｅｙ・Ｂｏａｒｄ：Ｋ／Ｂ）、マウス９０３、ＦＤＤ９０４（Ｆｌｅｘｉｂｌｅ・Ｄｉｓｋ・Ｄｒｉｖｅ）、コンパクトディスク装置９０５（ＣＤＤ）、プリンタ装置９０６、スキャナ装置９０７などのハードウェア資源を備え、これらはケーブルや信号線で接続されている。

システムユニット９１０は、コンピュータであり、ファクシミリ機９３２、電話器９３１とケーブルで接続され、また、ローカルエリアネットワーク９４２（ＬＡＮ）、ゲートウェイ９４１を介してインターネット９４０に接続されている。

【００１８】

図３は、この実施の形態における復号装置８１０、暗号化装置８２０、サーバ装置８３０のハードウェア資源の一例を示す図である。

復号装置８１０、暗号化装置８２０、サーバ装置８３０は、プログラムを実行するＣＰＵ９１１（Ｃｅｎｔｒａｌ・Ｐｒｏｃｅｓｓｉｎｇ・Ｕｎｉｔ、中央処理装置、処理装置、演算装置、マイクロプロセッサ、マイクロコンピュータ、プロセッサともいう）を備えている。ＣＰＵ９１１は、バス９１２を介してＲＯＭ９１３、ＲＡＭ９１４、通信装置９１５、表示装置９０１、キーボード９０２、マウス９０３、ＦＤＤ９０４、ＣＤＤ９０５、プリンタ装置９０６、スキャナ装置９０７、磁気ディスク装置９２０と接続され、これらのハードウェアデバイスを制御する。磁気ディスク装置９２０の代わりに、光ディスク装置、メモリカード読み書き装置などの記憶装置でもよい。

ＲＡＭ９１４は、揮発性メモリの一例である。ＲＯＭ９１３、ＦＤＤ９０４、ＣＤＤ９０５、磁気ディスク装置９２０の記憶媒体は、不揮発性メモリの一例である。これらは、記憶装置あるいは記憶部の一例である。通信装置９１５、キーボード９０２、スキャナ装置９０７、ＦＤＤ９０４などは、入力部、入力装置の一例である。また、通信装置９１５、表示装置９０１、プリンタ装置９０６などは、出力部、出力装置の一例である。

【００１９】

通信装置９１５は、ファクシミリ機９３２、電話器９３１、ＬＡＮ９４２等に接続されている。通信装置９１５は、ＬＡＮ９４２に限らず、インターネット９４０、ＩＳＤＮ等のＷＡＮ（ワイドエリアネットワーク）などに接続されていても構わない。インターネット９４０或いはＩＳＤＮ等のＷＡＮに接続されている場合、ゲートウェイ９４１は不用となる。

磁気ディスク装置９２０には、オペレーティングシステム９２１（ＯＳ）、ウィンドウシステム９２２、プログラム群９２３、ファイル群９２４が記憶されている。プログラム群９２３のプログラムは、ＣＰＵ９１１、オペレーティングシステム９２１、ウィンドウシステム９２２により実行される。

【００２０】

上記プログラム群９２３には、以下に述べる実施の形態の説明において「～部」として説明する機能を実行するプログラムが記憶されている。プログラムは、ＣＰＵ９１１により読み出され実行される。

ファイル群９２４には、以下に述べる実施の形態の説明において、「～の判定結果」、「～の計算結果」、「～の処理結果」として説明する情報やデータや信号値や変数値やパラメータが、「～ファイル」や「～データベース」の各項目として記憶されている。「～

ファイル」や「～データベース」は、ディスクやメモリなどの記録媒体に記憶される。ディスクやメモリになどの記憶媒体に記憶された情報やデータや信号値や変数値やパラメータは、読み書き回路を介してＣＰＵ９１１によりメインメモリやキャッシュメモリに読み出され、抽出・検索・参照・比較・演算・計算・処理・出力・印刷・表示などのＣＰＵの動作に用いられる。抽出・検索・参照・比較・演算・計算・処理・出力・印刷・表示のＣＰＵの動作の間、情報やデータや信号値や変数値やパラメータは、メインメモリやキャッシュメモリやバッファメモリに一時的に記憶される。

また、以下に述べる実施の形態の説明において説明するフローチャートの矢印の部分は主としてデータや信号の入出力を示し、データや信号値は、ＲＡＭ９１４のメモリ、ＦＤＤ９０４のフレキシブルディスク、ＣＤＤ９０５のコンパクトディスク、磁気ディスク装置９２０の磁気ディスク、その他光ディスク、ミニディスク、ＤＶＤ（Ｄｉｇｉｔａｌ・Ｖｅｒｓａｔｉｌｅ・Ｄｉｓｋ）等の記録媒体に記録される。また、データや信号は、バス９１２や信号線やケーブルその他の伝送媒体によりオンライン伝送される。

【００２１】

また、以下に述べる実施の形態の説明において「～部」として説明するものは、「～回路」、「～装置」、「～機器」であってもよく、また、「～ステップ」、「～手順」、「～処理」であってもよい。すなわち、「～部」として説明するものは、ＲＯＭ９１３に記憶されたファームウェアで実現されていても構わない。或いは、ソフトウェアのみ、或いは、素子・デバイス・基板・配線などのハードウェアのみ、或いは、ソフトウェアとハードウェアとの組み合わせ、さらには、ファームウェアとの組み合わせで実施されても構わない。ファームウェアとソフトウェアは、プログラムとして、磁気ディスク、フレキシブルディスク、光ディスク、コンパクトディスク、ミニディスク、ＤＶＤ等の記録媒体に記憶される。プログラムはＣＰＵ９１１により読み出され、ＣＰＵ９１１により実行される。すなわち、プログラムは、以下に述べる「～部」としてコンピュータを機能させるものである。あるいは、以下に述べる「～部」の手順や方法をコンピュータに実行させるものである。

【００２２】

図４は、この実施の形態における設定装置１００の構成の一例を示すブロック構成図である。

【００２３】

設定装置１００は、設定記憶部１１０、ペアリング値算出部１２１、秘密生成部１３０、公開算出部１４０、公開出力部１５０を有する。

設定記憶部１１０は、磁気ディスク装置９２０を用いて、あらかじめ、検索システム８００の基本設定を表わすパラメータを記憶している。設定記憶部１１０が記憶するパラメータは、あらかじめ定められているものであってもよいし、設定装置１００が設定したものであってもよい。

【００２４】

検索システム８００は、群を用いて、暗号演算を行う。検索システム８００が暗号演算に用いる群は、ＣＰＵ９１１を用いて、群演算を計算可能な群であり、例えば、代数曲線上の点がなす群である。以下では、群演算を乗法的に記述する。例えば、群演算による元ａと元ｂとの結合を「積」と呼び「ａ・ｂ」あるいは「ａｂ」と記述する。また、元ａの逆元を「１／ａ」と記述し、元ａと元ｂの逆元１／ｂとの積を「商」と呼び「ａ／ｂ」と記述する。また、ｍ個の元ａの積を「累乗」と呼び「a^m」あるいは「ａ＾ｍ」と記述する。すなわち、「a^2＝ａ・ａ」「a^3＝ａ・ａ・ａ」「a^m＝ａ・ａ・…・ａ（ｍ個）」である。

検索システム８００では、三つの群G_1，G_2，G_3を暗号演算に用いる。三つの群G_1，G_2，G_3はいずれも、離散対数問題を解くことが困難な群である。なお、群G_1と群G_2とは、同一の群であってもよい。三つの群G_1，G_2，G_3の位数は、いずれも素数ｐである。群G_1の元と群G_2の元との組を群G_3の元へ写すペアリング写像ｅ：$G_1 \times G_2 \rightarrow G_3$が定義されていて、ＣＰＵ９１１を用いて、計算可能である。群G_1の元ｇ

と群G_2の元hとの組をペアリング写像eで写した群G_3の元を「e（g，h）」と記述する。ペアリング写像eは、双線形であり、非縮退である。すなわち、群G_1の任意の元g、群G_2の任意の元h、任意の整数a，bについて、次の式が成立する（双線形性）。

【数１１】

$$e(g^a, h^b) = e(g, h)^{a \cdot b}$$

また、元gが群G_1の単位元でなく、かつ、元hが群G_2の単位元でなければ、e（g，h）は、群G_3の単位元ではない（非縮退性）。

【００２５】

また、以下の説明において、整数の演算は、特に断わりのない限り、pを法とする剰余類からなる有限体Z_pにおける四則演算による。すなわち、加算・減算・乗算は、通常の整数の加算・減算・乗算の結果をpで割った余りを求めることにより演算し、除算は、除数の逆数（除数との乗算の結果が１になる整数）を乗ずることにより演算する。

【００２６】

設定装置１００は、あらかじめ定められた群G_1～G_3、ペアリング写像eなどを用いる構成であってもよいし、安全性の程度を定める指標であるセキュリティパラメータkを入力して、入力したセキュリティパラメータkに基づいて、暗号演算に用いる群G_1～G_3、ペアリング写像eなどを定義する構成であってもよい。その場合、設定装置１００は、定義した群G_1～G_3、ペアリング写像eなど公開パラメータの一部として公開する。

【００２７】

設定記憶部１１０は、第一生成元記憶部１１１、第二生成元記憶部１１２、第三生成元記憶部１１３、索引数記憶部１１５を有する。

第一生成元記憶部１１１は、磁気ディスク装置９２０を用いて、群G_1の生成元g_1を記憶する。第二生成元記憶部１１２は、磁気ディスク装置９２０を用いて、群G_2の生成元g_2を記憶する。第三生成元記憶部１１３は、磁気ディスク装置９２０を用いて、群G_3の生成元g_3を記憶する。索引数記憶部１１５は、磁気ディスク装置９２０を用いて、索引数nを記憶する。なお、索引数nは、１以上の整数である。

【００２８】

なお、設定装置１００は、索引数入力部を有する構成であってもよい。その場合、索引数入力部は索引数を入力し、索引数記憶部１１５は、索引数入力部が入力した索引数を記憶する。

【００２９】

ペアリング値算出部１２１は、ＣＰＵ９１１を用いて、第一生成元記憶部１１１が記憶した生成元g_1と、第二生成元記憶部１１２が記憶した生成元g_2とを入力する。ペアリング値算出部１２１は、ＣＰＵ９１１を用いて、生成元g_1と生成元g_2との組をペアリング写像eにより写像した元e（g_1，g_2）を算出する。ペアリング値算出部１２１は、ＣＰＵ９１１を用いて、算出した元を、群G_3の生成元g_3として出力する。第三生成元記憶部１１３は、ＣＰＵ９１１を用いて、ペアリング値算出部１２１が出力した群G_3の生成元g_3を入力し、磁気ディスク装置９２０を用いて、記憶する。

【００３０】

秘密生成部１３０は、ＣＰＵ９１１を用いて、秘密パラメータを生成する。秘密生成部１３０は、秘密整数生成部１３１、秘密乱数生成部１３２を有する。

秘密整数生成部１３１は、ＣＰＵ９１１を用いて、１以上p未満の整数をランダムに生成する。秘密整数生成部１３１は、ＣＰＵ９１１を用いて、生成した整数を秘密整数yとして出力する。

秘密乱数生成部１３２は、ＣＰＵ９１１を用いて、１以上n以下のn個の整数それぞれについて、１以上p未満の整数を１つずつランダムに生成する。秘密乱数生成部１３２は、ＣＰＵ９１１を用いて、生成したn個の整数を秘密乱数u_i（iは１以上n以下の整数。）として出力する。

【００３１】

公開算出部１４０は、ＣＰＵ９１１を用いて、公開パラメータを算出する。公開算出部１４０は、公開元算出部１４１、公開乱数元算出部１４２を有する。

公開元算出部１４１は、ＣＰＵ９１１を用いて、第三生成元記憶部１１３が記憶した群G_3の生成元g_3と、秘密整数生成部１３１が出力した秘密整数ｙとを入力する。公開元算出部１４１は、ＣＰＵ９１１を用いて、入力した生成元g_3と秘密整数ｙとに基づいて、元g_3のｙ乗である群G_3の元g_3^yを算出する。公開元算出部１４１は、ＣＰＵ９１１を用いて、算出した元を、公開元Ｙとして出力する。

公開乱数元算出部１４２は、ＣＰＵ９１１を用いて、第一生成元記憶部１１１が記憶した群G_1の生成元g_1と、秘密乱数生成部１３２が出力したｎ個の秘密乱数u_iとを入力する。公開乱数元算出部１４２は、ＣＰＵ９１１を用いて、１以上ｎ以下のｎ個の整数それぞれについて、生成元g_1と、対応する秘密乱数u_iとに基づいて、元g_1のu_i乗である群G_1の元［$g_1 \wedge u_i$］を算出する。公開乱数元算出部１４２は、ＣＰＵ９１１を用いて、算出したｎ個の元を公開乱数元U_i（ｉは１以上ｎ以下の整数。）として出力する。

【００３２】

公開出力部１５０は、公開算出部１４０が算出した公開パラメータを公開する。公開出力部１５０は、公開元出力部１５１、公開乱数元出力部１５２を有する。

公開元出力部１５１は、ＣＰＵ９１１を用いて、公開元算出部１４１が出力した公開元Ｙを入力する。公開元出力部１５１は、ＣＰＵ９１１を用いて、入力した公開元Ｙを外部に出力する。

公開乱数元出力部１５２は、ＣＰＵ９１１を用いて、公開乱数元算出部１４２が出力したｎ個の公開乱数元U_iを入力する。公開乱数元出力部１５２は、ＣＰＵ９１１を用いて、入力したｎ個の公開乱数元U_iを外部に出力する。

群G_1及び群G_3は、離散対数問題を解くことが困難な群であるから、公開元Ｙ及び公開乱数元U_iを公開しても、秘密整数ｙ及び秘密乱数u_iを第三者が知ることはできない。

【００３３】

図５は、この実施の形態における検索暗号化装置３００の構成の一例を示すブロック構成図である。

検索暗号化装置３００は、設定記憶部３１０、秘密記憶部３２０、検索条件入力部３３０、閾値記憶部３４１、多項式係数生成部３４２、多項式係数記憶部３４３、多項式値算出部３４４、検索変換部３５２、検索整数記憶部３５３、検索元算出部３６０、暗号化検索出力部３７０を有する。

【００３４】

設定記憶部３１０は、磁気ディスク装置９２０を用いて、検索システム８００の基本設定や設定装置１００が公開した公開パラメータなどを記憶する。設定記憶部３１０は、第二生成元記憶部３１２、索引数記憶部３１５を有する。

第二生成元記憶部３１２は、磁気ディスク装置９２０を用いて、群G_2の生成元g_2を記憶する。索引数記憶部３１５は、磁気ディスク装置９２０を用いて、索引数ｎを記憶する。

【００３５】

秘密記憶部３２０は、耐タンパ性のある記憶装置を用いて、設定装置１００が設定した秘密パラメータを記憶する。秘密記憶部３２０は、秘密整数記憶部３２１、秘密乱数記憶部３２３を有する。

秘密整数記憶部３２１は、耐タンパ性のある記憶装置を用いて、設定装置１００が生成した秘密整数ｙを記憶する。秘密乱数記憶部３２３は、耐タンパ性のある記憶装置を用いて、設定装置１００が生成したｎ個の秘密乱数u_iを記憶する。

【００３６】

検索条件入力部３３０は、キーボード９０２などの入力装置を用いて、検索条件を入力する。検索条件入力部３３０は、閾値入力部３３１、検索入力部３３２を有する。

閾値入力部３３１は、キーボード９０２などの入力装置を用いて、閾値ｄを入力する。閾値入力部３３１は、ＣＰＵ９１１を用いて、入力した閾値ｄを出力する。

検索入力部３３２は、キーボード９０２などの入力装置を用いて、１以上ｎ以下のｎ個の整数それぞれについて、任意の長さの文字列を入力する。検索入力部３３２は、ＣＰＵ９１１を用いて、入力したｎ個の文字列を検索文字列ω_i（ｉは１以上ｎ以下の整数。）として出力する。

【００３７】

検索入力部３３２が入力する検索文字列ω_iに対応する整数ｉは、一致判定をする索引の番号に対応している。例えば、１番目の索引が「氏名」、２番目の索引が「性別」、３番目の索引が「年齢」を表わす場合、検索入力部３３２は、１番目の検索文字列ω_1として利用者が検索したい「氏名」を入力し、２番目の検索文字列ω_2として利用者が検索したい「性別」を入力し、３番目の検索文字列ω_3として利用者が検索したい「年齢」を入力する。

なお、ある番号の索引を検索の対象としない場合には、検索入力部３３２は、その整数についての検索文字列ω_iを入力しない。上記の例において、「性別」を不問としたい場合には、検索入力部３３２は、２番目の検索文字列ω_2を入力しない。その場合、その番号の索引が検索文字列と一致することはないので、閾値入力部３３１は、閾値ｄとして１つ少ない閾値を入力する。

【００３８】

閾値記憶部３４１は、ＣＰＵ９１１を用いて、閾値入力部３３１が出力した閾値ｄを入力する。閾値記憶部３４１は、磁気ディスク装置９２０を用いて、入力した閾値ｄを記憶する。

【００３９】

多項式係数生成部３４２は、ＣＰＵ９１１を用いて、閾値記憶部３４１が記憶した閾値ｄに基づいて、１以上（ｄ－２）以下の（ｄ－２）個の整数それぞれについて、０以上ｐ未満の整数を１つずつランダムに生成する。多項式係数生成部３４２は、ＣＰＵ９１１を用いて、整数（ｄ－１）について、１以上ｐ未満の整数をランダムに生成する。多項式係数生成部３４２は、生成した（ｄ－１）個の整数を多項式係数a_j（ｊは１以上（ｄ－１）以下の整数。）として出力する。

【００４０】

多項式係数記憶部３４３は、ＣＰＵ９１１を用いて、多項式係数生成部３４２が出力した（ｄ－１）個の多項式係数a_jを入力する。多項式係数記憶部３４３は、ＲＡＭ９１４を用いて、入力した（ｄ－１）個の多項式係数a_jを記憶する。

【００４１】

多項式値算出部３４４は、ＣＰＵ９１１を用いて、多項式係数記憶部３４３が記憶した（ｄ－１）個の多項式係数a_jと、秘密整数記憶部３２１が記憶した秘密整数ｙとを入力する。多項式値算出部３４４は、ＣＰＵ９１１を用いて、入力した（ｄ－１）個の多項式係数a_jと、秘密整数ｙとに基づいて、多項式係数a_jをｊ次の項の係数とし、秘密整数ｙを定数項とする多項式$f(x)=\Sigma(a_j \cdot x^j)+y$について、ｘに１以上ｎ以下のｎ個の整数それぞれを代入した値を算出する。多項式値算出部３４４は、ＣＰＵ９１１を用いて、算出したｎ個の値を多項式値ｆ（ｉ）（ｉは１以上ｎ以下の整数。）として出力する。

具体的には、多項式値算出部３４４は、ＣＰＵ９１１を用いて、１以上ｄ－１以下の（ｄ－１）個の整数ｊそれぞれについて、整数ｉのｊ乗を算出し、算出した整数i^jと、多項式係数a_jとの積$(a_j \cdot i^j)$を算出する。多項式値算出部３４４は、ＣＰＵ９１１を用いて、算出した（ｄ－１）個の積$(a_j \cdot i^j)$と、秘密整数ｙとの総和$[\Sigma(a_j \cdot i^j)+y]$を算出して、多項式値ｆ（ｉ）とする。多項式値算出部３４４は、これを１以上ｎ以下のｎ個の整数ｉについて繰り返す。

【００４２】

検索変換部３５２は、ＣＰＵ９１１を用いて、検索入力部３３２が出力したｎ個の検索

文字列ω_iを入力する。検索変換部３５２は、ＣＰＵ９１１を用いて、入力したｎ個の検索文字列ω_iそれぞれについて、所定の写像Ｈにより、検索文字列ω_iを写像した整数を算出する。検索変換部３５２は、ＣＰＵ９１１を用いて、算出したｎ個の整数を検索整数η_i（ｉは１以上ｎ以下の整数。）として出力する。

写像Ｈは、任意の長さの文字列を１以上ｐ未満の整数に写す写像である。写像Ｈは、衝突耐性を有する。すなわち、任意の二つの文字列について、写像Ｈにより写した整数が等しくなる確率が極めて低い。例えば、検索変換部３５２は、写像Ｈとして、ハッシュ関数を用いる。あるいは、検索変換部３５２は、ハッシュ関数に、検索文字列ω_iの番号である整数ｉと検索文字列ω_iとを結合した文字列［ｉ‖ω_i］を入力する構成であってもよいし、ハッシュ関数の出力の逆数や、ハッシュ関数の出力の定数倍などを、写像Ｈにより写した整数とする構成であってもよい。

【００４３】

なお、検索入力部３３２が、ある整数についての検索文字列ω_iを入力しなかった場合、検索変換部３５２は、その整数について、１以上ｐ未満の整数をランダムに生成して、検索整数η_iとする。

【００４４】

検索整数記憶部３５３（検索記憶部）は、ＣＰＵ９１１を用いて、検索変換部３５２が出力したｎ個の検索整数η_iを入力する。検索整数記憶部３５３は、磁気ディスク装置９２０を用いて、入力したｎ個の検索整数η_i（検索データ）を記憶する。

【００４５】

検索元算出部３６０は、ＣＰＵ９１１を用いて、ｎ個の検索元T_i（ｉは１以上ｎ以下の整数。）を算出する。検索元T_iは、検索整数η_iを暗号化したものであり、暗号化検索データの一部である。検索元算出部３６０は、指数算出部３６１、累乗部３６６を有する。

指数算出部３６１は、ＣＰＵ９１１を用いて、秘密乱数記憶部３２３が記憶したｎ個の秘密乱数u_iと、多項式値算出部３４４が出力したｎ個の多項式値ｆ（ｉ）と、検索整数記憶部３５３が記憶したｎ個の検索整数η_iとを入力する。指数算出部３６１は、ＣＰＵ９１１を用いて、１以上ｎ以下のｎ個の整数それぞれについて、対応する秘密乱数u_iと、対応する多項式値ｆ（ｉ）と、対応する検索整数η_iとに基づいて、秘密乱数u_iと検索整数η_iとの積で、多項式値ｆ（ｉ）を割った商ｆ（ｉ）／（$u_i \cdot \eta_i$）（ｉは１以上ｎ以下の整数。）を算出する。指数算出部３６１は、ＣＰＵ９１１を用いて、算出したｎ個の商を出力する。

累乗部３６６は、ＣＰＵ９１１を用いて、第二生成元記憶部３１２が記憶した群G_2の生成元g_2と、指数算出部３６１が出力したｎ個の商ｆ（ｉ）／（$u_i \cdot \eta_i$）とを入力する。累乗部３６６は、ＣＰＵ９１１を用いて、１以上ｎ以下のｎ個の整数それぞれについて、生成元g_2と、対応する商ｆ（ｉ）／（$u_i \cdot \eta_i$）とに基づいて、元g_2のｆ（ｉ）／（$u_i \cdot \eta_i$）乗である群G_2の元を算出する。累乗部３６６は、ＣＰＵ９１１を用いて、算出したｎ個の元を検索元T_iとして出力する。

【００４６】

暗号化検索出力部３７０は、ＣＰＵ９１１を用いて、暗号化検索データを外部に出力する。暗号化検索出力部３７０は、閾値出力部３７１、検索元出力部３７２を有する。

閾値出力部３７１は、ＣＰＵ９１１を用いて、閾値記憶部３４１が記憶した閾値ｄを入力する。閾値出力部３７１は、ＣＰＵ９１１を用いて、入力した閾値ｄを外部に出力する。

検索元出力部３７２は、ＣＰＵ９１１を用いて、累乗部３６６が出力したｎ個の検索元T_iを入力する。検索元出力部３７２は、ＣＰＵ９１１を用いて、入力したｎ個の検索元T_iを外部に出力する。

【００４７】

なお、暗号化検索出力部３７０は、閾値出力部３７１が出力する閾値ｄを表わすデータと、検索元出力部３７２が出力するｎ個の検索元T_iを表わすデータとを１つに結合し、

暗号化検索データ（検索文）として出力する構成であってもよい。

【００４８】

図６は、この実施の形態における索引暗号化装置２００の構成の一例を示すブロック構成図である。

索引暗号化装置２００は、設定記憶部２１０、索引入力部２２１、索引変換部２２３、索引整数記憶部２２４、索引乱数生成部２３０、判定元算出部２４０、索引元算出部２５０、暗号化索引出力部２６０を有する。

【００４９】

設定記憶部２１０は、検索システム８００の基本設定や設定装置１００が公開した公開パラメータを記憶する。設定記憶部２１０は、索引数記憶部２１５、公開元記憶部２１６、公開乱数元記憶部２１７を有する。

索引数記憶部２１５は、磁気ディスク装置９２０を用いて、索引数ｎを記憶する。公開元記憶部２１６は、磁気ディスク装置９２０を用いて、設定装置１００が設定した公開元Ｙを記憶する。公開乱数元記憶部２１７は、磁気ディスク装置９２０を用いて、設定装置１００が設定したｎ個の公開乱数元U_iを記憶する。

【００５０】

索引入力部２２１は、キーボード９０２などの入力装置を用いて、１以上ｎ以下のｎ個の整数それぞれについて、任意の長さの文字列（キーワード）を入力する。索引入力部２２１は、ＣＰＵ９１１を用いて、入力したｎ個の文字列を索引文字列w_i（ｉは１以上ｎ以下の整数。）として出力する。

索引変換部２２３は、ＣＰＵ９１１を用いて、索引入力部２２１が記憶したｎ個の索引文字列w_iを入力する。索引変換部２２３は、ＣＰＵ９１１を用いて、入力したｎ個の索引文字列w_iそれぞれについて、写像Ｈにより、索引文字列w_iを写像した整数を算出する。索引変換部２２３は、ＣＰＵ９１１を用いて、算出したｎ個の整数を索引整数h_i（ｉは１以上ｎ以下の整数。）として出力する。

写像Ｈは、検索変換部３５２が用いる写像と同じ写像であり、衝突耐性を有する。したがって、索引文字列w_iと検索文字列ω_iとが一致する場合、索引整数h_iと検索整数η_iとは等しく、索引文字列w_iと検索文字列ω_iとが一致しない場合、索引整数h_iと検索整数η_iとは等しくない。

索引整数記憶部２２４（索引記憶部）は、ＣＰＵ９１１を用いて、索引変換部２２３が出力したｎ個の索引整数h_iを入力する。索引整数記憶部２２４は、磁気ディスク装置９２０を用いて、入力したｎ個の索引整数h_i（索引データ）を記憶する。

【００５１】

なお、一部あるいはすべてのデータ本体に対する索引として、ｎ個未満の索引文字列を指定することとしてもよい。その場合、索引入力部２２１は、索引文字列を指定しない整数についての索引文字列w_iを入力せず、索引変換部２２３が、０以上ｐ未満の整数をランダムに生成して索引整数h_iとし、索引整数記憶部２２４が記憶する。

【００５２】

索引乱数生成部２３０は、ＣＰＵ９１１を用いて、１以上ｐ未満の整数をランダムに生成する。索引乱数生成部２３０は、ＣＰＵ９１１を用いて、生成した整数を索引乱数ｓとして出力する。

【００５３】

判定元算出部２４０は、ＣＰＵ９１１を用いて、判定元Ｅ’を算出する。判定元Ｅ’は、索引乱数ｓを暗号化したものであり、暗号化索引データの一部である。判定元算出部２４０は、累乗部２４２を有する。

累乗部２４２は、ＣＰＵ９１１を用いて、公開元記憶部２１６が記憶した公開元Ｙと、索引乱数生成部２３０が出力した索引乱数ｓとを入力する。累乗部２４２は、ＣＰＵ９１１を用いて、入力した公開元Ｙと索引乱数ｓとに基づいて、元Ｙのｓ乗である群G_3の元Y^sを算出する。累乗部２４２は、ＣＰＵ９１１を用いて、算出した元Y^sを判定元Ｅ’として出力する。

ここで、公開元Ｙは、元g_3のｙ乗であるから、判定元Ｅ’は、元g_3の（ｓ・ｙ）乗である。

【００５４】

索引元算出部２５０は、ＣＰＵ９１１を用いて、ｎ個の索引元E_i（ｉは１以上ｎ以下の整数。）を算出する。索引元E_iは、索引整数h_iを暗号化したものであり、暗号化索引データの一部である。索引元算出部２５０は、指数算出部２５１、累乗部２５３を有する。

指数算出部２５１は、ＣＰＵ９１１を用いて、索引整数記憶部２２４が記憶したｎ個の索引整数h_iと、索引乱数生成部２３０が出力した索引乱数ｓとを入力する。指数算出部２５１は、ＣＰＵ９１１を用いて、１以上ｎ以下のｎ個の整数それぞれについて、索引乱数ｓと、対応する索引整数h_iとに基づいて、索引乱数ｓと索引整数h_iとの積$s \cdot h_i$を算出する。指数算出部２５１は、ＣＰＵ９１１を用いて、算出したｎ個の積$s \cdot h_i$を出力する。

累乗部２５３は、ＣＰＵ９１１を用いて、公開乱数元記憶部２１７が記憶したｎ個の公開乱数元U_iと、指数算出部２５１が出力したｎ個の積$s \cdot h_i$とを入力する。累乗部２５３は、ＣＰＵ９１１を用いて、１以上ｎ以下のｎ個の整数それぞれについて、対応する公開乱数元U_iと、対応する積$s \cdot h_i$とに基づいて、元U_iの（$s \cdot h_i$）乗である群G_2の元を算出する。累乗部２５３は、ＣＰＵ９１１を用いて、算出したｎ個の元を索引元E_iとして出力する。

ここで、公開乱数元U_iは、元g_1のu_i乗であるから、索引元E_iは、元g_1の（$s \cdot h_i \cdot u_i$）乗である。

【００５５】

暗号化索引出力部２６０は、ＣＰＵ９１１を用いて、暗号化索引データを外部に出力する。暗号化索引出力部２６０は、索引元出力部２６１、判定元出力部２６２を有する。

索引元出力部２６１は、ＣＰＵ９１１を用いて、累乗部２５３が出力したｎ個の索引元E_iを入力する。索引元出力部２６１は、ＣＰＵ９１１を用いて、入力したｎ個の索引元E_iを外部に出力する。

判定元出力部２６２は、ＣＰＵ９１１を用いて、累乗部２４２が出力した判定元Ｅ’を入力する。判定元出力部２６２は、ＣＰＵ９１１を用いて、入力した判定元Ｅ’を外部に出力する。

【００５６】

なお、暗号化索引出力部２６０は、索引元出力部２６１が出力するｎ個の索引元E_iを表わすデータと、判定元出力部２６２が出力する判定元Ｅ’を表わすデータとを１つに結合し、暗号化索引データ（キーワード暗号文）として出力する構成であってもよい。

【００５７】

図７は、この実施の形態における検索装置４００の構成の一例を示すブロック構成図である。

検索装置４００は、索引数記憶部４１５、暗号化索引記憶部４２０、暗号化検索記憶部４３０、判定対象選択部４４１、補間係数値算出部４４２、写像元算出部４５０、比較元算出部４６０、判定部４７０を有する。

【００５８】

索引数記憶部４１５は、磁気ディスク装置９２０を用いて、索引数ｎを記憶する。

【００５９】

暗号化索引記憶部４２０は、磁気ディスク装置９２０を用いて、索引暗号化装置２００が出力した暗号化索引データを記憶する。暗号化索引記憶部４２０は、１つのデータ本体に対して１つずつの暗号化索引データを記憶する。暗号化索引記憶部４２０は、索引元記憶部４２１、判定元記憶部４２２を有する。

索引元記憶部４２１は、磁気ディスク装置９２０を用いて、１つの暗号化索引データについてｎ個ずつの索引元E_iを記憶する。判定元記憶部４２２は、磁気ディスク装置９２０を用いて、１つの暗号化索引データについて１つずつの判定元Ｅ’を記憶する。

【００６０】
暗号化検索記憶部４３０は、磁気ディスク装置９２０を用いて、検索暗号化装置３００が出力した暗号化検索データを記憶する。暗号化検索記憶部４３０は、閾値記憶部４３１、検索元記憶部４３２を有する。
閾値記憶部４３１は、磁気ディスク装置９２０を用いて、閾値ｄを記憶する。検索元記憶部４３２は、磁気ディスク装置９２０を用いて、ｎ個の検索元T_iを記憶する。
【００６１】
判定対象選択部４４１は、ＣＰＵ９１１を用いて、１以上ｎ以下のｎ個の整数からなる集合の部分集合であり、ｄ個の整数からなる集合Ｓを選択する。
判定対象選択部４４１は、ＣＰＵ９１１を用いて、閾値記憶部４３１が記憶した閾値ｄを入力する。判定対象選択部４４１は、ＣＰＵ９１１を用いて、１以上ｎ以下のｎ個の整数のなかから、ｄ個の整数を選択する。判定対象選択部４４１は、ＣＰＵ９１１を用いて、選択したｄ個の整数（集合Ｓ）を出力する。
【００６２】
補間係数値算出部４４２は、ＣＰＵ９１１を用いて、ラグランジュの補間係数の値を算出する。ラグランジュの補間係数は、次の式により定義される。
【数１２】

$$\Delta_{i,\mathbf{S}}(x) \xleftarrow{\mathbf{def}} \prod_{j\in\mathbf{S},j\neq i} \frac{x-j}{i-j}$$

集合Ｓはｄ個の元からなるので、ラグランジュの補間係数は変数ｘについて（ｄ－１）次の多項式である。
補間係数値算出部４４２は、ラグランジュの補間係数の変数ｘに０を代入したときの値$\Delta_{i,S}(0)$を算出する。
補間係数値算出部４４２は、ＣＰＵ９１１を用いて、判定対象選択部４４１が出力したｄ個の整数を入力する。補間係数値算出部４４２は、ＣＰＵ９１１を用いて、入力したｄ個の整数それぞれについて、ラグランジュの補間係数の値を算出する。補間係数値算出部４４２は、ＣＰＵ９１１を用いて、算出したｄ個のラグランジュの補間係数の値を補間係数値$\Delta_{i,S}$として出力する。
具体的には、判定対象選択部４４１が選択したｄ個の整数のうち、補間係数値を求める対象である整数を対象整数ｉとし、対象整数ｉ以外の（ｄ－１）個の整数を対象外整数ｊとすると、補間係数値算出部４４２は、ＣＰＵ９１１を用いて、（ｄ－１）個の対象外整数ｊそれぞれについて、対象外整数ｊから対象整数ｉを差し引いた差（ｊ－ｉ）を算出し、算出した差（ｊ－ｉ）で対象外整数ｊを割った商［ｊ／（ｊ－ｉ）］を算出する。補間係数値算出部４４２は、ＣＰＵ９１１を用いて、算出した（ｄ－１）個の商［ｊ／（ｊ－ｉ）］すべての総積Π［ｊ／（ｊ－ｉ）］を算出して、補間係数値$\Delta_{i,S}$とする。
【００６３】
写像元算出部４５０（写像算出部）は、ＣＰＵ９１１を用いて、ｄ個の写像元e'_i（写像データ）を算出する。写像元算出部４５０は、ペアリング値算出部４５１、累乗部４５５を有する。
ペアリング値算出部４５１は、ＣＰＵ９１１を用いて、検索条件に合うか否かを判定する対象である索引について索引元記憶部４２１が記憶したｎ個の索引元E_iと、検索元記憶部４３２が記憶したｎ個の検索元T_iとを入力する。ペアリング値算出部４５１は、ＣＰＵ９１１を用いて、１以上ｎ以下のｎ個の整数それぞれについて、対応する索引元E_iと、対応する検索元T_iとに基づいて、索引元E_iと検索元T_iとの組をペアリング写像ｅにより写像した群G_3の元$e(E_i, T_i)$を算出する。ペアリング値算出部４５１は、ＣＰＵ９１１を用いて、算出したｎ個の元$e(E_i, T_i)$をペアリング値e_i（ｉは１以上ｎ以下の整数。）として出力する。

ここで、索引元E_iは、元g_1の（$s \cdot h_i \cdot u_i$）乗であり、検索元T_iは、元g_2の［$f(i) / (u_i \cdot \eta_i)$］乗であるから、ペアリング値$e_i$は、元$g_3$の［$f(i) \cdot s \cdot h_i / \eta_i$］乗である。

【００６４】

累乗部４５５は、ＣＰＵ９１１を用いて、補間係数値算出部４４２が出力したｄ個の補間係数値$\Delta_{i,S}$と、ペアリング値算出部４５１が出力したｎ個のペアリング値e_iのうちｄ個の補間係数値$\Delta_{i,S}$に対応する（すなわち、判定対象選択部４４１が選択したｄ個の整数に対応する）ｄ個のペアリング値e_iとを入力する。累乗部４５５は、判定対象選択部４４１が選択したｄ個の整数それぞれについて、対応する補間係数値$\Delta_{i,S}$と、対応するペアリング値e_iとに基づいて、ペアリング値e_iの$\Delta_{i,S}$乗である群G_3の元を算出する。累乗部４５５は、ＣＰＵ９１１を用いて、算出したｄ個の元を写像元e'_iとして出力する。

【００６５】

比較元算出部４６０（比較算出部）は、ＣＰＵ９１１を用いて、比較元Ｂ（比較データ）を算出する。比較元算出部４６０は、総積部４６１を有する。

総積部４６１は、ＣＰＵ９１１を用いて、累乗部４５５が出力したｄ個の写像元e'_iを入力する。総積部４６１は、ＣＰＵ９１１を用いて、入力したｄ個の元e'_iすべての総積Π［e'_i］を算出する。総積部４６１は、ＣＰＵ９１１を用いて、算出した総積Π［e'_i］を比較元Ｂとして出力する。

ここで、比較元Ｂは、

【数１３】

$$\begin{aligned} B &= \prod_{i \in S} e'_i = \prod_{i \in S} {e_i}^{\Delta_{i,S}} \\ &= \prod_{i \in S} \left[{g_3}^{f(i) \cdot \Delta_{i,S} \cdot s \cdot \frac{h_i}{\eta_i}} \right] \\ &= {g_3}^{s \cdot \sum_{i \in S} \left[f(i) \cdot \Delta_{i,S} \cdot \frac{h_i}{\eta_i} \right]} \end{aligned}$$

である。

【００６６】

判定部４７０は、ＣＰＵ９１１を用いて、検索条件に合うか否かを判定する対象である索引について判定元記憶部４２２が記憶した判定元Ｅ’と、総積部４６１が出力した比較元Ｂとを入力する。判定部４７０は、入力した判定元Ｅ’と比較元Ｂとを比較し、一致する場合に、その索引が検索条件に合うと判定する。判定部４７０は、ＣＰＵ９１１を用いて、判定した結果を検索結果として出力する。

【００６７】

ここで、

【数１４】

$$\phi(x) \xleftarrow{\text{def}} \sum_{i \in S} \left[f(i) \cdot \Delta_{i,S}(x) \right]$$

とおく。ラグランジュの補間係数$\Delta_{i,S}$（ｘ）は、定義より明らかに、ｘ＝ｉのとき１、ｘ∈Ｓかつｘ≠ｉのとき０である。したがって、ｘ∈Ｓのとき、φ（ｘ）＝ｆ（ｘ）である。φ（ｘ）及びｆ（ｘ）は、ｘについての（ｄ－１）次多項式であり、ｄ個のｘにつ

いてφ（ｘ）＝ｆ（ｘ）であるから、φ（ｘ）≡ｆ（ｘ）である。したがって、
【数１５】

$$\phi(0)= f(0)= y$$

である。
【００６８】
すべてのｉ∈Ｓについて、ｈ$_{i}$＝η$_{i}$である場合、比較元Ｂは、
【数１６】

$$\begin{aligned} B &= g_3^{\,s\cdot\sum_{i\in S}\left[f(i)\cdot\Delta_{i,S}\cdot\frac{h_i}{\eta_i}\right]} \\ &= g_3^{\,s\cdot\phi(0)}= g_3^{\,s\cdot y} \end{aligned}$$

であるから、比較元Ｂは、判定元Ｅ’と一致する。
【００６９】
一方、いずれかのｉ∈Ｓについて、ｈ$_{i}$≠η$_{i}$である場合、Ｂ＝Ｅ’となる確率は、極めて低い。例えば、ｉ∈Ｓ’（Ｓ’はＳの部分集合であり空集合でない。）について、ｈ$_{i}$≠η$_{i}$であり、それ以外のｉ∈Ｓについて、ｈ$_{i}$＝η$_{i}$だとすると、
【数１７】

$$\begin{aligned} B &= g_3^{\,s\cdot\sum_{i\in S}\left[f(i)\cdot\Delta_{i,S}\cdot\frac{h_i}{\eta_i}\right]} \\ &= g_3^{\,s\cdot y+s\cdot\sum_{i\in S'}\left[f(i)\cdot\Delta_{i,S}\cdot\left(\frac{h_i}{\eta_i}-1\right)\right]} \\ &= E'\cdot g_3^{\sum_{i\in S'}\left[f(i)\cdot\Delta_{i,S}\cdot\frac{h_i-\eta_i}{\eta_i}\right]} \end{aligned}$$

であるから、Ｂ＝Ｅ’となるのは、
【数１８】

$$\sum_{i\in S'}\left[f(i)\cdot\Delta_{i,S}\cdot(h_i-\eta_i)\right]= 0$$

の場合のみである。この値は、０以上ｐ未満のランダムな値をとるから、０になる確率は１／ｐである。ｐは通常大きな数であるから、この確率は、極めて低い。
【００７０】
図８は、この実施の形態におけるデータ暗号化装置８４０、暗号化データ記憶装置８５０、データ復号装置８６０の構成の一例を示すブロック構成図である。
【００７１】
データ暗号化装置８４０は、本体記憶部８４１、暗号化鍵記憶部８４２、本体暗号化部８４３を有する。

本体記憶部８４１は、磁気ディスク装置９２０を用いて、データ本体（平文データ）を記憶する。
暗号化鍵記憶部８４２は、磁気ディスク装置９２０を用いて、データ本体の暗号化に用いる暗号化鍵を記憶する。
本体暗号化部８４３は、ＣＰＵ９１１を用いて、本体記憶部８４１が記憶したデータ本体と、暗号化鍵記憶部８４２が記憶した暗号化鍵とを入力する。本体暗号化部８４３は、ＣＰＵ９１１を用いて、入力した暗号化鍵により、入力したデータ本体を暗号化する。本体暗号化部８４３は、ＣＰＵ９１１を用いて、暗号化したデータ本体を暗号化データ本体として出力する。
本体暗号化部８４３が用いる暗号方式は、例えばＲＳＡ暗号など一般的な公開鍵暗号方式であってもよいし、例えばＡＥＳ暗号など一般的な共通鍵暗号方式であってもよいし、ＩＤベース暗号などの暗号方式であってもよい。あるいは、本体暗号化部８４３は、ランダムに生成した共通鍵を用いて共通鍵暗号方式でデータ本体を暗号化した上で、暗号化鍵記憶部８４２が記憶した暗号化鍵を用いて公開鍵暗号方式などの暗号方式で共通鍵を暗号化し、暗号化したデータ本体と暗号化した共通鍵とを結合したものを暗号化データ本体とする構成としてもよい。
【００７２】
暗号化データ記憶装置８５０は、暗号化本体記憶部８５１、検索結果入力部８５２、検索本体出力部８５３を有する。
暗号化本体記憶部８５１は、磁気ディスク装置９２０を用いて、データ暗号化装置８４０が出力した暗号化データ本体を記憶する。
検索結果入力部８５２は、ＣＰＵ９１１を用いて、検索装置４００が出力した検索結果を入力する。
検索本体出力部８５３は、ＣＰＵ９１１を用いて、検索結果入力部８５２が入力した検索結果に基づいて、検索条件に合う索引に対応づけられた暗号化データ本体を、暗号化本体記憶部８５１が記憶した暗号化データ本体のなかから取得する。検索本体出力部８５３は、ＣＰＵ９１１を用いて、取得した暗号化データ本体を出力する。
【００７３】
なお、検索にヒットするか否かのみが問題となり、データ本体がない場合や、暗号化データ本体を暗号化索引データと結合した形式で検索装置４００が記憶する構成の場合には、暗号化データ記憶装置８５０がない構成であってもよい。
【００７４】
データ復号装置８６０は、復号鍵記憶部８６１、本体復号部８６２、復号本体出力部８６３を有する。
復号鍵記憶部８６１は、磁気ディスク装置９２０を用いて、データ暗号化装置８４０が記憶した暗号化鍵に対応する復号鍵を記憶する。
本体復号部８６２は、ＣＰＵ９１１を用いて、暗号化データ記憶装置８５０が出力した暗号化データ本体と、復号鍵記憶部８６１が記憶した復号鍵とを入力する。本体復号部８６２は、ＣＰＵ９１１を用いて、入力した復号鍵により、入力した暗号化データ本体を復号する。本体復号部８６２は、復号したデータ本体を復号データ本体として出力する。
復号本体出力部８６３は、ＣＰＵ９１１を用いて、本体復号部８６２が出力した復号データ本体を入力する。復号本体出力部８６３は、ＣＰＵ９１１を用いて、入力した復号データ本体を外部に出力する。
【００７５】
図９は、この実施の形態における設定処理Ｓ６１０の流れの一例を示すフローチャート図である。
設定処理Ｓ６１０において、設定装置１００は、検索システム８００で用いるパラメータを設定する。設定処理Ｓ６１０は、第三生成元算出工程Ｓ６１１、秘密整数生成工程Ｓ６１３、公開元算出工程Ｓ６１５、整数選択工程Ｓ６１６、秘密乱数生成工程Ｓ６１７、公開乱数元算出工程Ｓ６１９、整数繰り返し工程Ｓ６２０を有する。

【００７６】
第三生成元算出工程Ｓ６１１において、ペアリング値算出部１２１は、ＣＰＵ９１１を用いて、第一生成元記憶部１１１が記憶した群$Ｇ_{1}$の生成元$ｇ_{1}$と、第二生成元記憶部１１２が記憶した群$Ｇ_{2}$の生成元$ｇ_{2}$とに基づいて、元$ｇ_{1}$と元$ｇ_{2}$との組をペアリング写像ｅにより写像した群$Ｇ_{3}$の元ｅ（$ｇ_{1}$，$ｇ_{2}$）を算出して、元$ｇ_{3}$とする。
【００７７】
秘密整数生成工程Ｓ６１３において、秘密整数生成部１３１は、ＣＰＵ９１１を用いて、１以上ｐ未満の整数をランダムに生成して、秘密整数ｙとする。
【００７８】
公開元算出工程Ｓ６１５において、公開元算出部１４１は、ＣＰＵ９１１を用いて、第三生成元算出工程Ｓ６１１でペアリング値算出部１２１が算出した元$ｇ_{3}$と、秘密整数生成工程Ｓ６１３で秘密整数生成部１３１が生成した秘密整数ｙとに基づいて、元$ｇ_{3}$のｙ乗である群$Ｇ_{3}$の元$ｇ_{3}^{y}$を算出して、公開元Ｙとする。
【００７９】
整数選択工程Ｓ６１６において、秘密乱数生成部１３２は、ＣＰＵ９１１を用いて、１以上ｎ以下のｎ個の整数のなかから、整数を１つずつ順に選択して、整数ｉとする。
【００８０】
秘密乱数生成工程Ｓ６１７において、秘密乱数生成部１３２は、ＣＰＵ９１１を用いて、整数選択工程Ｓ６１６で選択した整数ｉについて、１以上ｐ未満の整数をランダムに生成して、秘密乱数$ｕ_{i}$とする。
【００８１】
公開乱数元算出工程Ｓ６１９において、公開乱数元算出部１４２は、ＣＰＵ９１１を用いて、整数選択工程Ｓ６１６で秘密乱数生成部１３２が選択した整数ｉについて、第一生成元記憶部１１１が記憶した群$Ｇ_{1}$の生成元$ｇ_{1}$と、第二秘密乱数生成工程Ｓ６１７で秘密乱数生成部１３２が生成した秘密乱数$ｕ_{i}$とに基づいて、元$ｇ_{1}$の$ｕ_{i}$乗である群$Ｇ_{1}$の元を算出して、公開乱数元$Ｕ_{i}$とする。
【００８２】
整数繰り返し工程Ｓ６２０において、秘密乱数生成部１３２は、１以上ｎ以下のすべての整数を、整数選択工程Ｓ６１６で選択したか否かを判定する。まだ選択していない整数があると判定した場合、秘密乱数生成部１３２は、整数選択工程Ｓ６１６に戻り、次の整数を選択する。すべての整数を選択したと判定した場合、設定装置１００は、設定処理Ｓ６１０を終了する。
【００８３】
図１０は、この実施の形態における索引暗号化処理Ｓ６３０の流れの一例を示すフローチャート図である。
索引暗号化処理Ｓ６３０において、索引暗号化装置２００は、暗号化した索引を生成する。索引暗号化処理Ｓ６３０は、索引乱数生成工程Ｓ６３１、判定元算出工程Ｓ６３３、整数選択工程Ｓ６３５、索引整数算出工程Ｓ６３６、索引元算出工程Ｓ６３７、整数繰り返し工程Ｓ６３８を有する。
【００８４】
索引乱数生成工程Ｓ６３１において、索引乱数生成部２３０は、ＣＰＵ９１１を用いて、１以上ｐ未満の整数をランダムに生成して、索引乱数ｓとする。
【００８５】
判定元算出工程Ｓ６３３において、累乗部２４２は、ＣＰＵ９１１を用いて、公開元記憶部２１６が記憶した公開元Ｙと、索引乱数生成工程Ｓ６３１で索引乱数生成部２３０が生成した索引乱数ｓとに基づいて、元Ｙのｓ乗である群$Ｇ_{3}$の元$Ｙ^{s}$を算出して、判定元Ｅ’とする。
【００８６】
整数選択工程Ｓ６３５において、索引変換部２２３は、ＣＰＵ９１１を用いて、１以上ｎ以下のｎ個の整数のなかから、整数を１つずつ順に選択して、整数ｉとする。

【００８７】
索引整数算出工程Ｓ６３６において、索引変換部２２３は、ＣＰＵ９１１を用いて、整数選択工程Ｓ６３５で選択した整数ｉについて、写像Ｈにより、索引入力部２２１が入力した索引文字列w_iを写像した整数を算出して、索引整数h_iとする。
【００８８】
索引元算出工程Ｓ６３７において、指数算出部２５１は、ＣＰＵ９１１を用いて、索引乱数生成工程Ｓ６３１で索引乱数生成部２３０が生成した索引乱数ｓと、索引整数算出工程Ｓ６３６で索引変換部２２３が算出した索引整数h_iとの積（$s \cdot h_i$）を算出する。
累乗部２５３は、ＣＰＵ９１１を用いて、整数選択工程Ｓ６３５で索引変換部２２３が選択した整数ｉについて、公開乱数元記憶部２１７が記憶した公開乱数元U_iと、指数算出部２５１が算出した積（$s \cdot h_i$）とに基づいて、元U_iの（$s \cdot h_i$）乗である群G_1の元を算出して、索引元E_iとする。
【００８９】
整数繰り返し工程Ｓ６３８において、索引変換部２２３は、ＣＰＵ９１１を用いて、１以上ｎ以下のすべての整数を、整数選択工程Ｓ６３５で選択したか否かを判定する。まだ選択していない整数があると判定した場合、索引変換部２２３は、整数選択工程Ｓ６３５に戻り、次の整数を選択する。すべての整数を選択したと判定した場合、索引暗号化装置２００は、索引暗号化処理Ｓ６３０を終了する。
【００９０】
図１１は、この実施の形態における検索暗号化処理Ｓ６５０の流れの一例を示すフローチャート図である。
検索暗号化処理Ｓ６５０において、検索暗号化装置３００は、暗号化した検索文を生成する。検索暗号化処理Ｓ６５０は、次数選択工程Ｓ６５１、多項式係数生成工程Ｓ６５２、次数繰り返し工程Ｓ６５３、最高次係数生成工程Ｓ６５４、整数選択工程Ｓ６５５、検索整数算出工程Ｓ６５６、多項式値算出工程Ｓ６５７、検索元算出工程Ｓ６５９、整数繰り返し工程Ｓ６６１を有する。
【００９１】
次数選択工程Ｓ６５１において、多項式係数生成部３４２は、ＣＰＵ９１１を用いて、１以上（ｄ－２）以下の（ｄ－２）個の整数のなかから、整数を１つずつ順に選択して、整数ｊとする。
【００９２】
多項式係数生成工程Ｓ６５２において、多項式係数生成部３４２は、ＣＰＵ９１１を用いて、次数選択工程Ｓ６５１で選択した整数ｊについて、０以上ｐ未満の整数をランダムに選択して、多項式係数a_jとする。
【００９３】
次数繰り返し工程Ｓ６５３において、多項式係数生成部３４２は、ＣＰＵ９１１を用いて、１以上（ｄ－２）以下のすべての整数を、次数選択工程Ｓ６５１で選択したか否かを判定する。まだ選択していない整数があると判定した場合、多項式係数生成部３４２は、次数選択工程Ｓ６５１に戻り、次の整数を選択する。すべての整数を選択したと判定した場合、検索暗号化装置３００は、最高次係数生成工程Ｓ６５４へ進む。
【００９４】
最高次係数生成工程Ｓ６５４において、多項式係数生成部３４２は、ＣＰＵ９１１を用いて、整数（ｄ－１）について、１以上ｐ未満の整数をランダムに選択し、多項式係数a_{d-1}とする。
【００９５】
整数選択工程Ｓ６５５において、検索変換部３５２は、ＣＰＵ９１１を用いて、１以上ｎ以下のｎ個の整数のなかから、整数を１つずつ順に選択して、整数ｉとする。
【００９６】
検索整数算出工程Ｓ６５６において、検索変換部３５２は、ＣＰＵ９１１を用いて、整数選択工程Ｓ６５５で選択した整数ｉについて、写像Ｈにより、検索入力部３３２が入力

した検索文字列ω_iを写像した整数を算出して、検索整数η_iとする。

【００９７】

多項式値算出工程Ｓ６５７において、多項式値算出部３４４は、ＣＰＵ９１１を用いて、秘密整数記憶部３２１が記憶した秘密整数ｙと、多項式係数生成工程Ｓ６５２で多項式係数生成部３４２が生成した（ｄ－２）個の多項式係数a_jと、最高次係数生成工程Ｓ６５４で多項式係数生成部３４２が生成した多項式係数a_{d-1}とに基づいて、多項式係数a_jをｊ次の項の係数とし、秘密整数ｙを定数項の係数とする一変数多項式ｆ（ｘ）に、整数選択工程Ｓ６５５で検索変換部３５２が選択した整数ｉを代入した値を算出して、多項式値ｆ（ｉ）とする。

【００９８】

検索元算出工程Ｓ６５９において、指数算出部３６１は、ＣＰＵ９１１を用いて、整数選択工程Ｓ６５５で検索変換部３５２が選択した整数ｉについて、秘密乱数記憶部３２３が記憶した秘密乱数u_iと、検索整数算出工程Ｓ６５６で検索変換部３５２が算出した検索整数η_iと、多項式値算出工程Ｓ６５７で多項式値算出部３４４が算出した多項式値ｆ（ｉ）とに基づいて、秘密乱数u_iと検索整数η_iとの積（$u_i \cdot \eta_i$）で、多項式値ｆ（ｉ）を割った商［ｆ（ｉ）／（$u_i \cdot \eta_i$）］を算出する。

累乗部３６６は、ＣＰＵ９１１を用いて、整数選択工程Ｓ６５５で検索変換部３５２が選択した整数ｉについて、第二生成元記憶部３１２が記憶した群G_2の生成元g_2と、指数算出部３６１が算出した商［ｆ（ｉ）／（$u_i \cdot \eta_i$）］とに基づいて、元g_2の［ｆ（ｉ）／（$u_i \cdot \eta_i$）］乗である群G_2の元を算出して、検索元T_iとする。

【００９９】

整数繰り返し工程Ｓ６６１において、検索変換部３５２は、ＣＰＵ９１１を用いて、１以上ｎ以下のすべての整数を、整数選択工程Ｓ６５５で選択したか否かを判定する。まだ選択していない整数があると判定した場合、検索変換部３５２は、整数選択工程Ｓ６５５に戻り、次の整数を選択する。すべての整数を選択したと判定した場合、検索暗号化装置３００は、検索暗号化処理Ｓ６５０を終了する。

【０１００】

図１２は、この実施の形態における検索実行処理Ｓ６７０の流れの一例を示すフローチャート図である。

検索実行処理Ｓ６７０において、検索装置４００は、検索を実行する。検索実行処理Ｓ６７０は、索引選択工程Ｓ６７１、整数選択工程Ｓ６７２、ペアリング値算出工程Ｓ６７３、整数繰り返し工程Ｓ６７４、判定選択工程Ｓ６７５、判定整数選択工程Ｓ６７６、補間係数値算出工程Ｓ６７７、累乗工程Ｓ６７８、判定整数繰り返し工程Ｓ６７９、総積工程Ｓ６８０、判定工程Ｓ６８１、判定繰り返し工程Ｓ６８２、索引繰り返し工程Ｓ６８３を有する。

【０１０１】

索引選択工程Ｓ６７１において、ペアリング値算出部４５１は、ＣＰＵ９１１を用いて、暗号化索引記憶部４２０が記憶した暗号化索引データのなかから、暗号化索引データを１つずつ順に選択する。

【０１０２】

整数選択工程Ｓ６７２において、ペアリング値算出部４５１は、ＣＰＵ９１１を用いて、１以上ｎ以下のｎ個の整数のなかから、整数を１つずつ順に選択して、整数ｉとする。

【０１０３】

ペアリング値算出工程Ｓ６７３において、ペアリング値算出部４５１は、ＣＰＵ９１１を用いて、索引選択工程Ｓ６７１で選択した暗号化索引データについて索引元記憶部４２１が記憶した索引元E_iと、整数選択工程Ｓ６７２で選択した整数ｉについて検索元記憶部４３２が記憶した検索元T_iとに基づいて、ペアリング写像ｅにより、索引元E_iと検索元T_iとの組を写像した群G_3の元を算出して、ペアリング値e_iとする。

【０１０４】

整数繰り返し工程Ｓ６７４において、ペアリング値算出部４５１は、ＣＰＵ９１１を用

いて、１以上ｎ以下のすべての整数を、整数選択工程Ｓ６７２で選択したか否かを判定する。まだ選択していない整数があると判定した場合、ペアリング値算出部４５１は、整数選択工程Ｓ６７２に戻り、次の整数を選択する。すべての整数を選択したと判定した場合、検索装置４００は、判定選択工程Ｓ６７５へ進む。

【０１０５】

判定選択工程Ｓ６７５において、判定対象選択部４４１は、ＣＰＵ９１１を用いて、閾値記憶部４３１が記憶した閾値ｄに基づいて、１以上ｎ以下のｎ個の整数のなかからｄ個の整数を選択する組み合わせのなかから、組み合わせを１つずつ順に選択して、集合Ｓとする。

【０１０６】

判定整数選択工程Ｓ６７６において、補間係数値算出部４４２は、ＣＰＵ９１１を用いて、判定選択工程Ｓ６７５で判定対象選択部４４１が選択した集合Ｓに含まれる整数のなかから、整数を１つずつ順に選択して、整数ｉとする。

【０１０７】

補間係数値算出工程Ｓ６７７において、補間係数値算出部４４２は、ＣＰＵ９１１を用いて、判定整数選択工程Ｓ６７６で選択した整数ｉについて、補間係数値$\Delta_{i,S}$を算出する。

【０１０８】

累乗工程Ｓ６７８において、累乗部４５５は、ＣＰＵ９１１を用いて、判定整数選択工程Ｓ６７６で補間係数値算出部４４２が選択した整数ｉについて、ペアリング値算出工程Ｓ６７３でペアリング値算出部４５１が算出したペアリング値e_iと、補間係数値算出工程Ｓ６７７で補間係数値算出部４４２が算出した補間係数値$\Delta_{i,S}$とに基づいて、ペアリング値e_iの$\Delta_{i,S}$乗である群G_3の元を算出して、写像元e'_iとする。

【０１０９】

判定整数繰り返し工程Ｓ６７９において、補間係数値算出部４４２は、ＣＰＵ９１１を用いて、集合Ｓに含まれるすべての整数を、判定整数選択工程Ｓ６７６で選択したか否かを判定する。まだ選択していない整数があると判定した場合、補間係数値算出部４４２は、判定整数選択工程Ｓ６７６に戻り、次の整数を選択する。すべての整数を選択したと判定した場合、検索装置４００は、総積工程Ｓ６８０へ進む。

【０１１０】

総積工程Ｓ６８０において、総積部４６１は、ＣＰＵ９１１を用いて、累乗工程Ｓ６７８で算出したｄ個の写像元e'_iの総積を算出して、比較元Ｂとする。

【０１１１】

判定工程Ｓ６８１において、判定部４７０は、ＣＰＵ９１１を用いて、索引選択工程Ｓ６７１でペアリング値算出部４５１が選択した索引について判定元記憶部４２２が記憶した判定元Ｅ’と、総積工程Ｓ６８０で総積部４６１が算出した比較元Ｂとを比較して、等しいか否かを判定する。等しいと判定した場合、判定部４７０は、ＣＰＵ９１１を用いて、索引選択工程Ｓ６７１でペアリング値算出部４５１が選択した索引が、検索条件に合致したと判定して、索引繰り返し工程Ｓ６８３へ進む。等しくないと判定した場合、検索装置４００は、判定繰り返し工程Ｓ６８２へ進む。

【０１１２】

判定繰り返し工程Ｓ６８２において、判定対象選択部４４１は、ＣＰＵ９１１を用いて、１以上ｎ以下のｎ個の整数のなかからｄ個の整数を選択するすべての組み合わせを、判定選択工程Ｓ６７５で選択したか否かを判定する。まだ選択していない組み合わせがあると判定した場合、判定対象選択部４４１は、判定選択工程Ｓ６７５に戻り、次の組み合わせを選択する。すべての組み合わせを選択したと判定した場合、判定部４７０は、索引選択工程Ｓ６７１でペアリング値算出部４５１が選択した索引が、検索条件に合致しないと判定して、索引繰り返し工程Ｓ６８３へ進む。

【０１１３】

索引繰り返し工程Ｓ６８３において、判定部４７０は、ＣＰＵ９１１を用いて、判定工

程Ｓ６８１あるいは判定繰り返し工程Ｓ６８２で判定した判定結果を出力する。ペアリング値算出部４５１は、ＣＰＵ９１１を用いて、暗号化索引記憶部４２０が記憶したすべての暗号化索引データを、索引選択工程Ｓ６７１で選択したか否かを判定する。まだ選択していない暗号化索引データがあると判定した場合、ペアリング値算出部４５１は、索引選択工程Ｓ６７１に戻り、次の暗号化索引データを選択する。すべての暗号化索引データを選択したと判定した場合、検索装置４００は、検索実行処理Ｓ６７０を終了する。

【０１１４】

上述したように、判定選択工程Ｓ６７５で判定対象選択部４４１が選択した集合Ｓに含まれるｄ個の整数すべてについて、索引整数h_iと検索整数η_iとが一致する場合のみ、比較元Ｂと判定元Ｅ’とが等しくなるので、その索引に含まれるｎ個の索引文字列w_iのうちｄ個以上の索引文字列w_iが、検索暗号化装置３００が指定した検索文字列ω_iと一致する場合に、判定部４７０は、検索条件に合致したと判定する。

このとき、検索装置４００は、索引文字列w_iと検索文字列ω_iとが一致するｄ個の整数ｉを知ることができる。上述した検索実行処理Ｓ６７０では、判定工程Ｓ６８１で比較元Ｂと判定元Ｅ’とが一致した場合、１以上ｎ以下のｎ個の整数のなかからｄ個の整数を選択するすべての組み合わせについて判定することをしないので、集合Ｓに含まれるｄ個の整数ｉ以外の（ｎ－ｄ）個の整数については、索引文字列w_iと検索文字列ω_iとが一致するか否かは明らかにならないが、判定工程Ｓ６８１で比較元Ｂと判定元Ｅ’とが一致した場合でも処理を続行し、１以上ｎ以下のｎ個の整数のなかからｄ個の整数を選択するすべての組み合わせについて比較元Ｂと判定元Ｅ’とが判定するか否かを判定する構成とすれば、検索装置４００は、１以上ｎ以下のｎ個の整数すべてについて、索引文字列w_iと検索文字列ω_iとが一致するか否かを知ることができる。すなわち、索引文字列w_iと検索文字列ω_iとがｄ個以上一致する場合には、どのデータが一致するかを知ることができる。

【０１１５】

しかし、暗号化索引記憶部４２０が記憶した索引元E_iや判定元Ｅ’、暗号化検索記憶部４３０が記憶した検索元T_iなどから、索引整数h_iや検索整数η_iを知ることはできないので、たとえ写像Ｈの逆写像H^{-1}を知っていたとしても、一致した索引文字列w_iや検索文字列ω_iを知ることはできない。

【０１１６】

また、１以上ｎ以下のｎ個の整数のうちｄ個未満の整数について、索引文字列w_iと検索文字列ω_iとが一致し、それ以外は一致しない場合、１以上ｎ以下のｎ個の整数のなかからｄ個の整数を選択するすべての組み合わせについて、比較元Ｂは、判定元Ｅ’と不一致となる。したがって、どのデータが一致するかを知ることはできない。

【０１１７】

索引元E_iには、索引文字列w_iによって定まる索引整数h_iの要素のほかに、索引ごとに異なるランダムな索引乱数ｓの要素が含まれている。したがって、ある索引の索引文字列w_iと別の索引の索引文字列w_iとが同じであったとしても、索引元E_iは索引ごとに異なり、索引文字列w_iが同じか否かについての情報を隠蔽している。

【０１１８】

ある索引文字列w_iが、ある検索条件における検索文字列ω_iと一致することがわかると、ある索引における索引文字列w_iと、他の索引における索引文字列w_iとが同じか否かを知ることができる。これは、索引文字列w_iを解読する手がかりになる可能性がある。様々な検索条件による検索を何回も繰り返すことにより手がかりが増えていくと、やがて、索引文字列w_i、ひいてはデータ本体を解読される可能性がある。

このため、ある索引文字列w_iが、ある検索条件における検索文字列ω_iと一致するか否かに関する情報は、できる限り知られないようにしたほうがよい。

【０１１９】

この実施の形態における検索システム８００は、１以上ｎ以下のｎ個の整数のうちｄ個未満の整数について、索引文字列w_iと検索文字列ω_iとが一致し、それ以外は一致しな

い場合、どの索引文字列w_iと検索文字列ω_iとが一致したかについての情報を秘匿できる。このため、索引文字列w_iを解読する手がかりの漏洩を最小限に抑えることができる。

【０１２０】

この実施の形態における検索システム８００は、索引暗号化装置２００と、検索暗号化装置３００と、検索装置４００とを有する。

上記索引暗号化装置２００は、データを記憶する記憶装置（磁気ディスク装置９２０）と、データを処理する処理装置（ＣＰＵ９１１）と、索引記憶部（索引整数記憶部２２４）と、索引暗号化部（索引元算出部２５０）とを有する。

上記索引記憶部は、上記記憶装置を用いて、１以上ｎ以下のｎ個の整数（ｎは１以上の整数。）に対応するｎ個の索引データ（索引整数h_i）を記憶する。

上記索引暗号化部は、上記処理装置を用いて、１以上ｎ以下のｎ個の整数それぞれについて、上記索引記憶部が記憶した索引データを暗号化して、ｎ個の暗号化索引データ（索引元E_i）とする。

上記検索暗号化装置３００は、データを記憶する記憶装置（磁気ディスク装置９２０）と、データを処理する処理装置（ＣＰＵ９１１）と、検索記憶部（検索整数記憶部３５３）と、多項式値算出部３４４と、検索暗号化部（検索元算出部３６０）とを有する。

上記検索記憶部は、上記記憶装置を用いて、１以上ｎ以下のｎ個の整数に対応するｎ個の検索データ（検索整数η_i）を記憶する。

上記多項式値算出部３４４は、上記処理装置を用いて、１以上ｎ以下のｎ個の整数それぞれについて、（ｄ－１）次の一変数多項式ｆ（ｘ）（ｄは１以上ｎ以下の整数。）に上記整数を代入した値を算出して、ｎ個の多項式値ｆ（ｉ）とする。

上記検索暗号化部は、上記処理装置を用いて、１以上ｎ以下のｎ個の整数それぞれについて、上記検索記憶部が記憶した検索データと、上記多項式値算出部３４４が算出した多項式値ｆ（ｉ）との組を暗号化して、ｎ個の暗号化検索データ（検索元T_i）とする。

上記検索装置４００は、データを処理する処理装置（ＣＰＵ９１１）と、データを記憶する記憶装置（磁気ディスク装置９２０）と、暗号化索引記憶部４２０と、暗号化検索記憶部４３０と、判定対象選択部４４１と、補間係数値算出部４４２と、写像算出部（写像元算出部４５０）と、比較算出部（比較元算出部４６０）と、判定部４７０とを有する。

上記暗号化索引記憶部４２０は、上記記憶装置を用いて、上記索引暗号化装置２００が暗号化したｎ個の暗号化索引データ（索引元E_i）を記憶する。

上記暗号化検索記憶部４３０は、上記記憶装置を用いて、上記検索暗号化装置３００が暗号化したｎ個の暗号化検索データ（検索元T_i）を記憶する。

上記判定対象選択部４４１は、上記処理装置を用いて、１以上ｎ以下のｎ個の整数のなかからｄ個の整数を選択して、ｄ個の判定対象整数とする。

上記補間係数値算出部４４２は、上記処理装置を用いて、上記判定対象選択部４４１が選択したｄ個の判定対象整数に基づいて、ラグランジュの補間係数の値を算出して、ｄ個の補間係数値$\Delta_{i,S}$とする。

上記写像算出部は、上記処理装置を用いて、上記判定対象選択部４４１が選択したｄ個の判定対象整数それぞれについて、上記暗号化索引記憶部４２０が記憶した暗号化索引データと、上記暗号化検索記憶部４３０が記憶した暗号化検索データと、上記補間係数値算出部４４２が算出した補間係数値との組を写像して、ｄ個の写像データ（写像元e'_i）とする。

上記比較算出部は、上記処理装置を用いて、上記写像算出部が写像したｄ個の写像データに基づいて、比較データ（比較元Ｂ）を算出する。

上記判定部４７０は、上記処理装置を用いて、上記比較算出部が算出した比較データに基づいて、上記判定対象選択部４４１が選択したｄ個の判定対象整数について、上記索引データと、上記検索データとが一致するか否かを判定する。

【０１２１】

この実施の形態における検索システム８００によれば、（ｄ－１）次の一変数多項式ｆ

（ｘ）の値ｆ（ｉ）を用いて、検索データを暗号化し、ラグランジュの補間係数の値$\Delta_{i,S}$を用いて、検索を実行するので、ｎ個のデータのうちｄ個以上が一致する場合に、一致することを検索装置４００が判定でき、ｄ個未満しか一致しない場合には、いずれのデータが一致したかを検索装置４００が知ることができない。これにより、索引データや検索データに関する情報の漏洩を防ぐことができる。

【０１２２】

この実施の形態における検索システム８００において、上記補間係数値算出部４４２は、上記処理装置（ＣＰＵ９１１）を用いて、上記判定対象選択部４４１が選択したｄ個の判定対象整数のうちの一つを対象整数ｉとし、上記判定対象選択部４４１が選択したｄ個の判定対象整数のうち上記対象整数以外の（ｄ－１）個の判定対象整数を（ｄ－１）個の対象外整数ｊとし、（ｄ－１）個の対象外整数ｊそれぞれについて、上記対象外整数ｊから上記対象整数ｉを差し引いた差（ｊ－ｉ）で、上記対象外整数ｊを割った商［ｊ／（ｊ－ｉ）］を算出し、算出した（ｄ－１）個の商の総積Π［ｊ／（ｊ－ｉ）］を算出して、上記対象整数ｉについての補間係数値$\Delta_{i,S}$とする。

【０１２３】

この実施の形態における検索システム８００によれば、未知の一変数関数について、判定対象選択部４４１が選択したｄ個の判定対象整数を代入したときの値が既知である場合におけるラグランジュの補間係数について、補間係数値算出部４４２が、ラグランジュの補間係数に０を代入したときの値を算出して補間係数値$\Delta_{i,S}$とするので、判定対象選択部４４１が選択したｄ個の判定対象整数について、索引データと検索データとが一致する場合に、比較元Ｂが、一変数多項式ｆ（ｘ）に０を代入したときの値ｆ（０）に対応する値となる。検索装置４００は、これを利用することにより、判定対象選択部４４１が選択したｄ個の判定対象整数について、索引データと検索データとが一致するか否かを判定する。

【０１２４】

この実施の形態における検索システム８００において、上記多項式値算出部３４４は、上記処理装置（ＣＰＵ９１１）を用いて、所定の秘密整数ｙを上記一変数多項式ｆ（ｘ）の定数項として、上記多項式値ｆ（ｉ）を算出する。

上記索引暗号化部（判定元算出部２４０）は、上記秘密整数ｙを暗号化したデータ（公開元Ｙ）に基づいて、上記索引データを暗号化する。

【０１２５】

この実施の形態における検索システム８００によれば、検索暗号化装置３００は、秘密変数ｙを（ｄ－１）次の一変数多項式ｆ（ｘ）の定数項とすることにより、秘密整数ｙについての情報をｎ個の多項式値ｆ（ｉ）に分散して埋め込む。このため、ｎ個の多項式値ｆ（ｉ）のうちｄ個以上を知ることができれば、秘密整数ｙを求めることができる。検索装置４００は、秘密整数ｙを直接求めることはしないが、判定対象選択部４４１が選択したｄ個の判定対象整数について、索引データと検索データとが一致する場合に、ｄ個の多項式値ｆ（ｉ）に対応する暗号化されたデータから、秘密整数ｙに対応する暗号化されたデータを求めることができる。検索装置４００は、これを利用することにより、判定対象選択部４４１が選択したｄ個の判定対象整数について、索引データと検索データとが一致するか否かを判定する。

【０１２６】

この実施の形態における検索システム８００は、更に、設定装置１００を有する。

上記設定装置１００は、秘密整数生成部１３１と、公開元算出部１４１とを有する。

上記秘密整数生成部１３１は、上記処理装置を用いて、１以上ｐ未満の整数（ｐは素数。）をランダムに生成して、秘密整数ｙとする。

上記公開元算出部１４１は、上記処理装置を用いて、０以上ｐ未満の整数を位数ｐの群の元に単射する第一の写像により、上記秘密整数生成部１３１が生成した秘密整数ｙを写像した元を算出して、公開元Ｙとする。

上記索引暗号化装置２００は、公開元記憶部２１６と、索引整数記憶部２２４と、索引

元算出部２５０と、判定元算出部２４０とを有する。
上記公開元記憶部２１６は、上記記憶装置を用いて、上記設定装置１００が算出した公開元Ｙを記憶する。
上記索引整数記憶部２２４は、上記記憶装置を用いて、ｎ個の１以上ｐ未満の整数を、１以上ｎ以下のｎ個の整数ｉそれぞれに対応する索引整数h_iとして記憶する。
上記索引元算出部２５０は、上記処理装置を用いて、１以上ｎ以下のｎ個の整数ｉそれぞれについて、上記索引整数記憶部２２４が記憶した索引整数h_iに基づいて、０以上ｐ未満の整数を位数ｐの群の元に単射する第二の写像により、上記索引整数h_iを写像した元を算出して、ｎ個の索引元E_iとする。
上記判定元算出部２４０は、上記処理装置を用いて、上記公開元記憶部２１６が記憶した公開元Ｙに基づいて、位数ｐの群の元を位数ｐの群の元に単射する第三の写像により、上記公開元Ｙを写像した元を算出して、判定元Ｅ’とする。
上記検索暗号化装置３００は、秘密整数記憶部３２１と、検索整数記憶部３５３と、多項式係数生成部３４２と、検索元算出部３６０とを有する。
上記秘密整数記憶部３２１は、上記記憶装置を用いて、上記設定装置１００が生成した秘密整数ｙを記憶する。
上記検索整数記憶部３５３は、上記記憶装置を用いて、ｎ個の１以上ｐ未満の整数を、１以上ｎ以下のｎ個の整数ｉそれぞれに対応する検索整数η_iとして記憶する。
上記多項式係数生成部３４２は、上記処理装置を用いて、（ｄ－１）個の０以上ｐ未満の整数をランダムに生成して、（ｄ－１）個の多項式係数a_jとする。
上記多項式値算出部３４４は、上記処理装置を用いて、上記秘密整数記憶部３２１が記憶した秘密整数ｙを、上記一変数多項式ｆ（ｘ）の定数項とし、上記多項式係数生成部３４２が生成した（ｄ－１）個の多項式係数a_jを、上記一変数多項式ｆ（ｘ）の１次から（ｄ－１）次までの各項の係数として、上記多項式値ｆ（ｉ）を算出する。
上記検索元算出部３６０は、上記処理装置を用いて、１以上ｎ以下のｎ個の整数ｉそれぞれについて、上記検索整数記憶部３５３が記憶した検索整数η_iと、上記多項式値算出部３４４が算出した多項式値ｆ（ｉ）とに基づいて、１以上ｐ未満の整数と０以上ｐ未満の整数との組を位数ｐの群の元に写像する第四の写像により、上記検索整数η_iと上記多項式値ｆ（ｉ）との組を写像した元を算出して、ｎ個の検索元T_iとする。
上記検索装置４００は、索引元記憶部４２１と、判定元記憶部４２２と、検索元記憶部４３２と、写像元算出部４５０と、比較元算出部４６０とを有する。
上記索引元記憶部４２１は、上記記憶装置を用いて、上記索引暗号化装置２００が算出したｎ個の索引元E_iを記憶する。
上記判定元記憶部４２２は、上記記憶装置を用いて、上記索引暗号化装置２００が算出した判定元Ｅ’を記憶する。
上記検索元記憶部４３２は、上記記憶装置を用いて、上記検索暗号化装置３００が算出したｎ個の検索元T_iを記憶する。
上記写像元算出部４５０は、上記処理装置を用いて、上記判定対象選択部４４１が選択したｄ個の判定対象整数ｉそれぞれについて、上記索引元記憶部４２１が記憶した索引元E_iと、上記検索元記憶部４３２が記憶した検索元T_iと、上記補間係数値算出部４４２が算出した補間係数値$\Delta_{i,S}$とに基づいて、位数ｐの群の元と位数ｐの群の元と０以上ｐ未満の整数との組を位数ｐの群の元に写像する第五の写像により、上記索引元E_iと上記検索元T_iと上記補間係数値$\Delta_{i,S}$との組を写像した元を算出して、ｄ個の写像元e'_iとする。
上記比較元算出部４６０は、上記処理装置を用いて、上記写像元算出部４５０が算出したｄ個の写像元e'_iを群演算により結合した元を算出して、比較元Ｂとする。
上記判定部４７０は、上記処理装置を用いて、上記比較元算出部４６０が算出した比較元Ｂと、上記判定元記憶部４２２が記憶した判定元Ｅ’とが等しい場合に、上記判定対象選択部４４１が選択したｄ個の判定対象整数ｉについて、上記索引整数h_iと、上記検索整数η_iとが一致すると判定する。

【０１２７】
この実施の形態における検索システム８００によれば、位数ｐが素数である群を用いて、暗号化処理をするので、用いることができる群や写像の種類が多く、安全性の高いシステムを構築することができる。
【０１２８】
ここでいうところの第一の写像をφ$_1$、第二の写像をφ$_2$、第三の写像をφ$_3$、第四の写像をφ$_4$、第五の写像をφ$_5$とすると、この実施の形態で用いる写像φ$_1$～φ$_5$は、次の式で定義される。
【数１９】

$$\phi_1 : \mathbb{Z}_p \to \mathbb{G}_3 \qquad \phi_1(x) = e(g_1, g_2)^x$$

$$\phi_2 : \mathbb{Z}_p \to \mathbb{G}_1 \qquad \phi_2(x) = (g_1{}^{u_i \cdot s})^x$$

$$\phi_3 : \mathbb{G}_3 \to \mathbb{G}_3 \qquad \phi_3(X) = X^s$$

$$\phi_4 : \mathbb{Z}_p^* \times \mathbb{Z}_p \to \mathbb{G}_2$$

$$\phi_4(x_1, x_2) = \left(g_2{}^{\frac{1}{u_i}} \right)^{\frac{x_2}{x_1}}$$

$$\phi_5 : \mathbb{G}_1 \times \mathbb{G}_2 \times \mathbb{Z}_p \to \mathbb{G}_3$$

$$\phi_5(X_1, X_2, x_3) = e(X_1, X_2)^{x_3}$$

【０１２９】
すなわち、第一の写像φ$_1$は、０以上ｐ未満の整数を位数ｐの群Ｇ$_3$の元へ写す写像であり、整数ｘを、元ｅ（ｇ$_1$，ｇ$_2$）のｘ乗へ写す。ｐは素数であり、元ｇ$_1$は群Ｇ$_1$の単位元でなく、元ｇ$_2$は群Ｇ$_2$の単位元でなく、ペアリング写像ｅは双線形かつ非縮退なので、元ｅ（ｇ$_1$，ｇ$_2$）は群Ｇ$_3$の単位元ではない。したがって、第一の写像φ$_1$は全単射であり、整数がｐを法とする加法についてなす群から群Ｇ$_3$への同型写像である。
第二の写像φ$_2$は、０以上ｐ未満の整数を位数ｐの群Ｇ$_1$の元へ写す写像であり、整数ｘを、元［ｇ$_1$の（ｕ$_i$・ｓ）乗］のｘ乗へ写す。生成元ｇ$_1$は群Ｇ$_1$の単位元でなく、秘密乱数ｕ$_i$及び索引乱数ｓは０でないので、元［ｇ$_1$の（ｕ$_i$・ｓ）乗］は群Ｇ$_1$の単位元ではない。したがって、第二の写像φ$_2$は全単射であり、整数がｐを法とする加法についてなす群から群Ｇ$_1$への同型写像である。
第三の写像φ$_3$は、位数ｐの群Ｇ$_3$の元を位数ｐの群Ｇ$_3$の元へ写す写像であり、元Ｘを、元Ｘのｓ乗へ写す。索引乱数ｓは０でない。したがって、第三の写像φ$_3$は全単射であり、群Ｇ$_3$の自己同型写像である。
第四の写像φ$_4$は、１以上ｐ未満の整数と０以上ｐ未満の整数との組を位数ｐの群Ｇ$_2$の元へ写す写像であり、整数ｘ$_1$と整数ｘ$_2$との組（ｘ$_1$，ｘ$_2$）を、元［ｇ$_2$の（１／ｕ$_i$）乗］の（ｘ$_2$／ｘ$_1$）乗へ写す。生成元ｇ$_2$は群Ｇ$_2$の単位元でないので、元［ｇ$_2$の（１／ｕ$_i$）乗］は群Ｇ$_2$の単位元ではない。したがって、整数ｘ$_1$を固定して考えると、第四の写像φ$_4$は全単射であり、整数がｐを法とする加法についてなす群から群Ｇ$_2$への同型写像である。また、整数ｘ$_2$を固定して考えると、第四の写像φ$_4$は単射であり、群Ｇ$_2$から単位元を除いた集合に対する全単射である。
第五の写像φ$_5$は、位数ｐの群Ｇ$_1$の元と位数ｐの群Ｇ$_2$の元と０以上ｐ未満の整数との組を位数ｐの群Ｇ$_3$の元へ写す写像であり、元Ｘ$_1$と元Ｘ$_2$と整数ｘ$_3$との組（Ｘ$_1$，Ｘ$_2$，ｘ$_3$）を、元ｅ（Ｘ$_1$，Ｘ$_2$）のｘ$_3$乗へ写す。ペアリング写像ｅは双線形かつ非

縮退である。したがって、X_2，x_3を固定して考えると、第五の写像ϕ_5は群G_1から群G_3への準同型写像であり、x_3が０でないとき全単射である。また、X_1，x_3を固定して考えると、第五の写像ϕ_5は群G_2から群G_3への準同型写像であり、x_3が０でないとき全単射である。更に、X_1，X_2を固定して考えると、第五の写像ϕ_5は全単射であり、整数がｐを法とする加法についてなす群から群G_3への同型写像である。

【０１３０】

上記判定元算出部２４０は、０以上ｐ未満の任意の整数ｘについて、上記任意の整数ｘを上記第一の写像ϕ_1により写像した元ϕ_1（ｘ）を、上記第三の写像ϕ_3により写像した元ϕ_3（ϕ_1（ｘ））が、上記任意の整数ｘと等しい数の所定の元Ｚを、群演算により結合した元［Z^x］と等しくなる写像を、上記第三の写像ϕ_3として用いる。

上記写像元算出部４５０は、１以上ｐ未満の任意の第一の整数x_1について、上記任意の第一の整数x_1を上記第二の写像ϕ_2により写像した元ϕ_2（x_1）と、上記任意の第一の整数x_1と第二の整数x_2との組を上記第四の写像ϕ_4により写像した元ϕ_4（x_1，x_2）と、第三の整数x_3との組を、上記第五の写像により写像した元ϕ_5（ϕ_2（x_1），ϕ_4（x_1，x_2），x_3）が、上記第二の整数x_2と上記第三の整数x_3との積と等しい数の上記所定の元Ｚを、群演算により結合した元［Ｚ＾（x_2・x_3）］と等しくなる写像を、上記第五の写像ϕ_5として用いる。

【０１３１】

この実施の形態における検索システム８００によれば、判定対象選択部４４１が選択したｄ個の判定対象整数について、索引整数h_iと検索整数η_iとが一致する場合に、比較元算出部４６０が算出する比較元Ｂと、判定元算出部２４０が算出する判定元Ｅ’とが一致する。検索装置４００は、これを利用することにより、判定対象選択部４４１が選択したｄ個の判定対象整数について、索引整数h_iと検索整数η_iとが一致するか否かを判定する。

【０１３２】

例えば、この実施の形態における写像ϕ_1～ϕ_5については、次の関係が成り立つ。

【数２０】

$$\phi_3(\phi_1(x)) = (e(g_1, g_2)^s)^x$$

$$\phi_5(\phi_2(x_1), \phi_4(x_1, x_2), x_3) = e\left(g_1^{u_i \cdot s \cdot x_1}, g_2^{\frac{x_2}{u_i \cdot x_1}}\right)^{x_3}$$

$$= (e(g_1, g_2)^s)^{x_2 \cdot x_3}$$

【０１３３】

上記５つの写像ϕ_1～ϕ_5は、この実施の形態における例に限らない。上述した関係が成り立つ組み合わせであれば、検索装置４００における検索が可能である。

【０１３４】

この実施の形態における検索システム８００において、上記設定装置１００は、更に、秘密乱数生成部１３２と、公開乱数元算出部１４２とを有する。

上記秘密乱数生成部１３２は、上記処理装置を用いて、１以上ｎ以下のｎ個の整数ｉそれぞれについて、１以上ｐ未満の整数をランダムに生成して、ｎ個の秘密乱数u_iとする。

上記公開元算出部１４１は、上記処理装置を用いて、第一の群G_1の元と第二の群G_2の元との組を第三の群G_3の元に写像する双線形ペアリング写像ｅ（上記第一の群G_1及び上記第二の群G_2及び上記第三の群G_3の位数はｐ。）により、上記第一の群G_1の生成元である第一生成元g_1と、上記第二の群G_2の生成元である第二生成元g_2との組を写像した元である第三生成元g_3と、上記秘密整数生成部１３１が生成した秘密整数ｙとに基づいて、上記秘密整数ｙと等しい数の上記第三生成元g_3を、上記第三の群G_3の群

演算により結合した元g_3^yを算出して、公開元Ｙとする。

上記公開乱数元算出部１４２は、上記処理装置を用いて、１以上ｎ以下のｎ個の整数ｉそれぞれについて、上記第一生成元g_1と、上記秘密乱数生成部１３２が生成した秘密乱数u_iとに基づいて、上記秘密乱数u_iと等しい数の上記第一生成元g_1を、上記第一の群G_1の群演算により結合した元［$g_1 \wedge u_i$］を算出して、ｎ個の公開乱数元U_iとする。

上記索引暗号化装置２００は、更に、公開乱数元記憶部２１７と、索引乱数生成部２３０とを有する。

上記公開乱数元記憶部２１７は、上記記憶装置を用いて、上記設定装置１００が算出したｎ個の公開乱数元U_iを記憶する。

上記索引乱数生成部２３０は、上記処理装置を用いて、１以上ｐ未満の整数をランダムに生成して、索引乱数ｓとする。

上記判定元算出部２４０は、上記処理装置を用いて、上記公開元記憶部２１６が記憶した公開元Ｙと、上記索引乱数生成部２３０が生成した索引乱数ｓとに基づいて、上記索引乱数ｓと等しい数の上記公開元Ｙを、上記第三の群G_3の群演算により結合した元Y^sを算出して、判定元Ｅ’とする。

上記索引元算出部２５０は、上記処理装置を用いて、１以上ｎ以下のｎ個の整数ｉそれぞれについて、上記公開乱数元記憶部２１７が記憶した公開乱数元U_iと、上記索引整数記憶部２２４が記憶した索引整数h_iと、上記索引乱数生成部２３０が生成した索引乱数ｓとに基づいて、上記索引整数h_iと上記索引乱数ｓとの積と等しい数の上記公開乱数元U_iを、上記第一の群G_1の群演算により結合した元［$U_i \wedge (s \cdot h_i)$］を算出して、ｎ個の索引元E_iとする。

上記検索暗号化装置３００は、更に、秘密乱数記憶部３２３を有する。

上記秘密乱数記憶部３２３は、上記記憶装置を用いて、上記設定装置１００が生成したｎ個の秘密乱数u_iを記憶する。

上記検索元算出部３６０は、上記処理装置を用いて、１以上ｎ以下のｎ個の整数ｉそれぞれについて、上記第二生成元g_2と、上記秘密乱数記憶部３２３が記憶した秘密乱数u_iと、上記検索整数記憶部３５３が記憶した検索整数η_iと、上記多項式値算出部３４４が算出した多項式値ｆ（ｉ）とに基づいて、上記秘密乱数u_iと上記検索整数η_iとの積で上記多項式値ｆ（ｉ）を割った商と等しい数の上記第二生成元g_2を、上記第二の群G_2の群演算により結合した元［$g_2 \wedge \{f(i) / (u_i \cdot \eta_i)\}$］を算出して、ｎ個の検索元$T_i$とする。

上記検索装置４００において、上記写像元算出部４５０は、上記処理装置を用いて、上記判定対象選択部４４１が選択したｄ個の判定対象整数ｉそれぞれについて、上記索引元記憶部４２１が記憶した索引元E_iと、上記検索元記憶部４３２が記憶した検索元T_iとに基づいて、上記双線形ペアリング写像ｅにより上記索引元E_iと上記検索元T_iとの組を写像した上記第三の群G_3の元ｅ（E_i，T_i）を算出して、ｄ個のペアリング値e_iとし、上記判定対象選択部４４１が選択したｄ個の判定対象整数ｉそれぞれについて、算出した上記ペアリング値e_iと、上記補間係数値算出部４４２が算出した補間係数値$\Delta_{i,S}$とに基づいて、上記補間係数値$\Delta_{i,S}$と等しい数の上記ペアリング値e_iを、上記第三の群G_3の群演算により結合した元［$e_i \wedge \Delta_{i,S}$］を算出して、ｄ個の写像元e'_iとする。

上記比較元算出部４６０は、上記処理装置を用いて、上記写像元算出部４５０が算出したｄ個の写像元e'_iを、上記第三の群G_3の群演算により結合した元$\Pi(e'_i)$を算出して、比較元Ｂとする。

【０１３５】

安全性の証明については省略するが、この実施の形態における検索システム８００によれば、索引整数や検索整数を解読しようとする第三者の攻撃に対して、安全性を有する。

【０１３６】

この実施の形態における検索システム８００において、上記索引暗号化装置２００は、

更に、索引変換部２２３を有する。
上記索引変換部２２３は、上記処理装置を用いて、１以上ｎ以下のｎ個の整数ｉに対応するｎ個の索引文字列w_iを入力し、１以上ｎ以下のｎ個の整数ｉそれぞれについて、任意の長さの文字列を１以上ｐ未満の整数に変換する変換写像Ｈにより、入力した索引文字列w_iを変換して、ｎ個の索引整数h_iとする。
上記索引整数記憶部２２４は、上記記憶装置を用いて、上記索引変換部２２３が変換したｎ個の索引整数h_iを記憶する。
上記検索暗号化装置３００は、更に、検索変換部３５２を有する。
上記検索変換部３５２は、上記処理装置を用いて、１以上ｎ以下のｎ個の整数ｉに対応するｎ個の検索文字列ω_iを入力し、１以上ｎ以下のｎ個の整数ｉそれぞれについて、上記変換写像Ｈにより、入力した検索文字列ω_iを変換して、ｎ個の検索整数η_iとする。
上記検索整数記憶部３５３は、上記記憶装置を用いて、上記検索変換部３５２が変換したｎ個の検索整数η_iを記憶する。
【０１３７】
この実施の形態における検索システム８００によれば、索引データ及び検索データとして、１以上ｐ未満の整数に限らず、任意の長さの文字列を用いることができるので、検索システム８００を応用できる範囲が広くなる。
【０１３８】
この実施の形態における索引暗号化装置２００によれば、算出した暗号化索引データを第三者に知られても、もとである索引データを知られることはなく、それでいて、暗号化索引データを用いて、ｎ個ある索引データのうちｄ個以上が検索データと一致するものを検索することを可能にする。また、ｎ個ある索引データのうち検索データと一致するものがｄ個未満の場合には、どの索引データが検索データと一致したかについても知られずに済むので、より高い安全性を実現できる。
【０１３９】
この実施の形態における検索暗号化装置３００によれば、算出した暗号化検索データを第三者に知られても、もとである検索データを知られることはなく、それでいて、暗号化検索データを用いて、ｎ個ある索引データのうちｄ個以上が検索データと一致するものを検索することを可能にする。また、ｎ個ある索引データのうち検索データと一致するものがｄ個未満の場合には、どの索引データが検索データと一致したかについても知られずに済むので、より高い安全性を実現できる。
【０１４０】
この実施の形態における検索装置４００によれば、暗号化索引データ及び暗号化検索データのいずれも復号することなく、ｎ個ある索引データのうちｄ個以上が検索データと一致するものを検索することができる。
【０１４１】
この実施の形態における索引暗号化装置２００・検索暗号化装置３００・検索装置４００は、いずれも、コンピュータを、索引暗号化装置２００または検索暗号化装置３００または検索装置４００として機能させるコンピュータプログラムを、コンピュータが実行することにより、実現することができる。
【０１４２】
この実施の形態における検索システム８００において、索引暗号化装置２００が索引データを暗号化した暗号化索引データと、検索暗号化装置３００が検索データを暗号化した暗号化検索データとを用いて、検索装置４００が上記索引データと上記検索データとが一致するか否かを判定する検索方法は、以下の工程を有する。
上記索引暗号化装置２００が、１以上ｎ以下のｎ個の整数ｉ（ｎは１以上の整数。）に対応するｎ個の索引データ（索引整数h_i）を記憶する。
上記索引暗号化装置２００が、１以上ｎ以下のｎ個の整数ｉそれぞれについて、記憶した索引データを暗号化して、ｎ個の暗号化索引データ（索引元E_i）とする。
上記検索暗号化装置３００が、１以上ｎ以下のｎ個の整数ｉに対応するｎ個の検索デー

タ（検索整数η_i）を記憶する。
上記検索暗号化装置３００が、１以上ｎ以下のｎ個の整数ｉそれぞれについて、（ｄ－１）次の一変数多項式ｆ（ｘ）（ｄは１以上ｎ以下の整数。）に上記整数ｉを代入した値を算出して、ｎ個の多項式値ｆ（ｉ）とする。
上記検索暗号化装置３００が、１以上ｎ以下のｎ個の整数ｉそれぞれについて、記憶した検索データと、算出した多項式値ｆ（ｉ）との組を暗号化して、ｎ個の暗号化検索データ（検索元T_i）とする。
上記検索装置４００が、上記索引暗号化装置２００が暗号化したｎ個の暗号化索引データを記憶する。
上記検索装置４００が、上記検索暗号化装置３００が暗号化したｎ個の暗号化検索データを記憶する。
上記検索装置４００が、１以上ｎ以下のｎ個の整数のなかからｄ個の整数を選択して、ｄ個の判定対象整数ｉとする。
上記検索装置４００が、選択したｄ個の判定対象整数ｉに基づいて、ラグランジュの補間係数の値を算出して、ｄ個の補間係数値$\Delta_{i,S}$とする。
上記検索装置４００が、選択したｄ個の判定対象整数ｉそれぞれについて、記憶した暗号化索引データと、記憶した暗号化検索データと、算出した補間係数値$\Delta_{i,S}$との組を写像して、ｄ個の写像データ（写像元e'_i）とする。
上記検索装置４００が、写像したｄ個の写像データに基づいて、比較データ（比較元Ｂ）を算出する。
上記検索装置４００が、算出した比較データに基づいて、選択したｄ個の判定対象整数ｉについて、上記索引データと、上記検索データとが一致するか否かを判定する。

【０１４３】
この実施の形態における検索方法によれば、検索暗号化装置３００が、（ｄ－１）次の一変数多項式ｆ（ｘ）の値ｆ（ｉ）を用いて、検索データを暗号化し、検索装置４００が、ラグランジュの補間係数の値$\Delta_{i,S}$を用いて、検索を実行するので、ｎ個のデータのうちｄ個以上が一致する場合に、一致することを検索装置４００が判定でき、ｄ個未満しか一致しない場合には、いずれのデータが一致したかを検索装置４００が知ることができない。これにより、索引データや検索データに関する情報の漏洩を防ぐことができる。

【０１４４】
以上説明した検索システム８００によれば、暗号化したままの状態でのキーワード検索が可能であり、複数のキーワードのうち、ある一定個以上が一致すれば検索にヒットする。検索にヒットしない場合には、どのキーワードが一致し、どのキーワードが一致しなかったかについての情報が漏れない。

【０１４５】
これに対し、単一のキーワードの検索方式を応用しても、複数のキーワードのうち、ある一定個以上が一致するか否かを判定することは可能である。すなわち、データ作成者（索引暗号化装置）が、キーワード数（索引数）に応じて複数の暗号化タグ（暗号化索引データ）を生成し、データ検索者（検索暗号化装置）も、検索キーワード数（索引数）に応じて複数の検索用トラップドア（検索暗号化データ）を生成して、データ保管サーバ（検索装置）が検索を実行して、それぞれのキーワードが一致するものを抽出すれば、複数のキーワードのうち一定個以上以上が一致するか否かを調べることができる。しかし、この方式の場合、データ保管サーバ（検索装置）は、キーワード自体を知ることはできないものの、どの暗号化タグとどの検索用トラップドアが何個一致したかが分かってしまう。したがって、この情報を利用して、データ保管サーバは、データ検索者がどのようなデータを検索しようとしているかについて推測をすることが可能になってしまう。

【０１４６】
以上説明した検索システム８００によれば、複数キーワードのうち一定個以上が一致するか否かが検索可能で、かつ、どの暗号化キーワードが何個一致したかに関する情報の漏洩を従来よりも低減させることができる。

【０１４７】
以上説明した検索システム８００は、素数位数の群におけるペアリングを利用している。これに対し、合成数位数の群におけるペアリングを利用する方式も考えられるが、その場合、利用できるペアリングの種類が限定されてしまう。以上説明した検索システム８００によれば、素数位数の群におけるペアリングを利用するので、利用できるペアリングの種類が限定されず、ペアリングの計算量を低減することができる。
【０１４８】
なお、以上の説明において、検索暗号化装置３００は、暗号化検索データとして閾値ｄを指定し、検索装置４００は、ｄ個以上の索引が一致するデータを検索する構成としているが、検索暗号化装置３００が、もっと細かく条件を指定する構成としてもよい。
例えば、検索暗号化装置３００は、必ず一致しなければならない索引の番号や、一致するか否かを問わない索引の番号を指定する構成としてもよい。一致するか否かを問わない索引の番号を指定する場合、その番号に対応する検索元T_iを暗号化検索データに含める必要はなく、暗号化検索データの量を少なくすることができる。
これを受けて、検索装置４００では、判定対象選択部４４１が、１以上ｎ以下のｎ個の整数のなかからｄ個の整数を選択する際、必ず一致しなければならない索引として指定された番号は、選択するｄ個の整数のなかに必ず含め、一致するか否かを問わない索引として指定された番号は、選択するｄ個の整数のなかに含めない。これにより、検索装置４００における計算量を減らすことができる。
【０１４９】
また、索引暗号化装置２００は、索引文字列を指定していない索引がある場合、その索引の番号を、暗号化索引データに含めて、検索装置４００に知らせる構成としてもよい。その場合、その番号に対応する索引元E_iを暗号化索引データに含める必要はなく、暗号化索引データの量を少なくすることができる。
これを受けて、検索装置４００では、その暗号化索引データに対して検索を実行する際、判定対象選択部４４１が、索引文字列を指定していないとされる索引の番号を、選択するｄ個の整数のなかに含めない。これにより、検索装置４００における計算量を減らすことができる。
【０１５０】
実施の形態２．
実施の形態２について、図１３～図２０を用いて説明する。
なお、実施の形態１と共通する部分については、同一の符号を付し、説明を省略する。
この実施の形態における検索システム８００の全体構成、復号装置８１０、暗号化装置８２０、サーバ装置８３０の外観及びハードウェア資源は、実施の形態１と同様である。
【０１５１】
図１３は、この実施の形態における設定装置１００の構成の一例を示すブロック構成図である。
設定装置１００は、設定記憶部１１０、秘密生成部１３０、公開算出部１４０、公開出力部１５０を有する。
【０１５２】
設定記憶部１１０は、第一生成元記憶部１１１、索引数記憶部１１５を有する。第一生成元記憶部１１１は、磁気ディスク装置９２０を用いて、群G_1の生成元g_1を記憶する。索引数記憶部１１５は、磁気ディスク装置９２０を用いて、索引数ｎを記憶する。
【０１５３】
秘密生成部１３０は、秘密整数生成部１３１を有する。秘密整数生成部１３１は、ＣＰＵ９１１を用いて、１以上ｐ以下の整数をランダムに生成し、秘密整数ｙとして出力する。
【０１５４】
公開算出部１４０は、公開元算出部１４１、公開乱数元算出部１４２、第二生成元算出部１４７を有する。

公開元算出部１４１は、ＣＰＵ９１１を用いて、第一生成元記憶部１１１が記憶した群$Ｇ_{1}$の生成元$ｇ_{1}$と、秘密整数生成部１３１が出力した秘密整数ｙとを入力する。公開元算出部１４１は、ＣＰＵ９１１を用いて、入力した生成元$ｇ_{1}$と秘密整数ｙとに基づいて、元$ｇ_{1}$のｙ乗である群$Ｇ_{1}$の元$ｇ_{1}^{y}$を算出する。公開元算出部１４１は、ＣＰＵ９１１を用いて、算出した元を公開元$ｇ_{1}$’として出力する。

公開乱数元算出部１４２は、ＣＰＵ９１１を用いて、索引数記憶部１１５が記憶した索引数ｎを入力する。公開乱数元算出部１４２は、ＣＰＵ９１１を用いて、１以上ｎ以下のｎ個の整数それぞれについて、群$Ｇ_{2}$の単位元以外の元をランダムに生成する。公開乱数元算出部１４２は、ＣＰＵ９１１を用いて、生成したｎ個の元を公開乱数元$ｕ_{i}$（ｉは１以上ｎ以下の整数。）として出力する。

第二生成元算出部１４７は、ＣＰＵ９１１を用いて、群$Ｇ_{2}$の単位元以外の元をランダムに生成する。第二生成元算出部１４７は、ＣＰＵ９１１を用いて、生成した元を生成元$ｇ_{2}$として出力する。

【０１５５】

公開出力部１５０は、公開元出力部１５１、公開乱数元出力部１５２、第一生成元出力部１５６、第二生成元出力部１５７を有する。公開元出力部１５１は、ＣＰＵ９１１を用いて、公開元算出部１４１が出力した公開元$ｇ_{1}$’を入力して、外部に出力する。公開乱数元出力部１５２は、ＣＰＵ９１１を用いて、公開乱数元算出部１４２が出力したｎ個の公開乱数元$ｕ_{i}$を入力して、外部に出力する。第一生成元出力部１５６は、ＣＰＵ９１１を用いて、第一生成元記憶部１１１が記憶した群$Ｇ_{1}$の生成元$ｇ_{1}$を入力して、外部に出力する。第二生成元出力部１５７は、第二生成元算出部１４７が出力した群$Ｇ_{2}$の生成元$ｇ_{2}$を入力して、外部に出力する。

【０１５６】

図１４は、この実施の形態における検索暗号化装置３００の構成の一例を示すブロック構成図である。

検索暗号化装置３００は、設定記憶部３１０、秘密記憶部３２０、検索条件入力部３３０、閾値記憶部３４１、多項式係数生成部３４２、多項式係数記憶部３４３、多項式値算出部３４４、検索変換部３５２、検索整数記憶部３５３、検索乱数生成部３８０、検索乱数元算出部３９０、検索元算出部３６０、暗号化検索出力部３７０を有する。

【０１５７】

設定記憶部３１０は、第一生成元記憶部３１１、第二生成元記憶部３１２、索引数記憶部３１５、公開乱数元記憶部３１７を有する。第一生成元記憶部３１１は、磁気ディスク装置９２０を用いて、群$Ｇ_{1}$の生成元$ｇ_{1}$を記憶する。第二生成元記憶部３１２は、磁気ディスク装置９２０を用いて、群$Ｇ_{2}$の生成元$ｇ_{2}$を記憶する。索引数記憶部３１５は、磁気ディスク装置９２０を用いて、索引数ｎを記憶する。公開乱数元記憶部３１７は、磁気ディスク装置９２０を用いて、設定装置１００が公開したｎ個の公開乱数元$ｕ_{i}$を記憶する。

【０１５８】

検索乱数生成部３８０は、ＣＰＵ９１１を用いて、１以上ｎ以下のｎ個の整数それぞれについて、１以上ｐ未満の整数をランダムに生成する。検索乱数生成部３８０は、ＣＰＵ９１１を用いて、生成したｎ個の整数を検索乱数$ｒ_{i}$（ｉは１以上ｎ以下の整数。）として出力する。

【０１５９】

検索乱数元算出部３９０は、ＣＰＵ９１１を用いて、ｎ個の検索乱数元$ｔ_{i}$（ｉは１以上ｎ以下の整数。）を算出する。検索乱数元$ｔ_{i}$は、検索乱数を暗号化したものであり、暗号化検索データの一部である。検索乱数元算出部３９０は、累乗部３９１を有する。

累乗部３９１は、ＣＰＵ９１１を用いて、第一生成元記憶部３１１が記憶した群$Ｇ_{1}$の生成元$ｇ_{1}$と、検索乱数生成部３８０が出力したｎ個の検索乱数$ｒ_{i}$とを入力する。累乗部３９１は、ＣＰＵ９１１を用いて、１以上ｎ以下のｎ個の整数それぞれについて、生成元$ｇ_{1}$と、対応する検索乱数$ｒ_{i}$とに基づいて、元$ｇ_{1}$の$ｒ_{i}$乗である群$Ｇ_{1}$の元［$ｇ_{1}$

＾ｒ$_i$］を算出する。累乗部３９１は、ＣＰＵ９１１を用いて、算出したｎ個の元を検索乱数元ｔ$_i$（ｉは１以上ｎ以下の整数。）として出力する。

【０１６０】

検索元算出部３６０は、関数値算出部３６２、二つの累乗部３６５，３６６、積算出部３６７を有する。

関数値算出部３６２は、ＣＰＵ９１１を用いて、公開乱数元記憶部３１７が記憶したｎ個の公開乱数元ｕ$_i$と、検索整数記憶部３５３が記憶したｎ個の検索整数η$_i$とを入力する。関数値算出部３６２は、ＣＰＵ９１１を用いて、１以上ｎ以下のｎ個の整数それぞれについて、対応する公開乱数元ｕ$_i$と、対応する検索整数η$_i$とに基づいて、検索整数η$_i$と公開乱数元ｕ$_i$との組を関数Ｕに代入した値を算出する。関数値算出部３６２は、ＣＰＵ９１１を用いて、算出したｎ個の値を関数値Ｕ（η$_i$，ｕ$_i$）（ｉは１以上ｎ以下の整数。）として出力する。

関数Ｕは、０以上ｐ未満の整数と群Ｇ$_2$の元との組を引数とし、値として、群Ｇ$_2$の元をとる。関数Ｕは、例えば、次の式により定義される。

【数２１】

$$U(x,u_i)\xleftarrow{\mathrm{def}}{g_2}^{x}\cdot u_i$$

この例において、関数値算出部３６２は、ＣＰＵ９１１を用いて、１以上ｎ以下の整数ｉについて、第二生成元記憶部３１２が記憶した群Ｇ$_2$の生成元ｇ$_2$と、検索変換部３５２が出力した検索整数η$_i$とに基づいて、元ｇ$_2$のη$_i$乗である群Ｇ$_2$の元［ｇ$_2$＾η$_i$］を算出する。関数値算出部３６２は、ＣＰＵ９１１を用いて、算出した元［ｇ$_2$＾η$_i$］と、公開乱数元記憶部３１７が記憶した公開乱数元ｕ$_i$との積を算出して、関数値Ｕ（η$_i$，ｕ$_i$）とする。

【０１６１】

累乗部３６５は、ＣＰＵ９１１を用いて、関数値算出部３６２が出力したｎ個の関数値Ｕ（η$_i$，ｕ$_i$）と、検索乱数生成部３８０が出力したｎ個の検索乱数ｒ$_i$とを入力する。累乗部３６５は、１以上ｎ以下のｎ個の整数それぞれについて、対応する関数値Ｕ（η$_i$，ｕ$_i$）と、対応する検索乱数ｒ$_i$とに基づいて、関数値Ｕ（η$_i$，ｕ$_i$）のｒ$_i$乗である群Ｇ$_2$の元［Ｕ（η$_i$，ｕ$_i$）＾ｒ$_i$］を算出する。累乗部３６５は、ＣＰＵ９１１を用いて、算出したｎ個の元［Ｕ（η$_i$，ｕ$_i$）＾ｒ$_i$］（ｉは１以上ｎ以下の整数。）を出力する。

【０１６２】

累乗部３６６は、ＣＰＵ９１１を用いて、第二生成元記憶部３１２が記憶した群Ｇ$_2$の生成元ｇ$_2$と、多項式値算出部３４４が出力したｎ個の多項式値ｆ（ｉ）とを入力する。累乗部３６６は、ＣＰＵ９１１を用いて、１以上ｎ以下のｎ個の整数それぞれについて、生成元ｇ$_2$と、対応する多項式値ｆ（ｉ）とに基づいて、元ｇ$_2$のｆ（ｉ）乗である群Ｇ$_2$の元［ｇ$_2$＾ｆ（ｉ）］を算出する。累乗部３６６は、ＣＰＵ９１１を用いて、算出したｎ個の元［ｇ$_2$＾ｆ（ｉ）］（ｉは１以上ｎ以下の整数。）を出力する。

【０１６３】

積算出部３６７は、ＣＰＵ９１１を用いて、累乗部３６５が出力したｎ個の関数値Ｕ（η$_i$，ｕ$_i$）と、累乗部３６６が出力したｎ個の元［ｇ$_2$＾ｆ（ｉ）］とを入力する。積算出部３６７は、ＣＰＵ９１１を用いて、１以上ｎ以下のｎ個の整数それぞれについて、対応する関数値Ｕ（η$_i$，ｕ$_i$）と、対応する元［ｇ$_2$＾ｆ（ｉ）］との積を算出する。積算出部３６７は、ＣＰＵ９１１を用いて、算出したｎ個の積を検索元Ｔ$_i$（ｉは１以上ｎ以下の整数。）として出力する。

【０１６４】

暗号化検索出力部３７０は、閾値出力部３７１、検索元出力部３７２、検索乱数元出力部３７３を有する。閾値出力部３７１は、ＣＰＵ９１１を用いて、閾値記憶部３４１が記憶した閾値ｄを入力して、外部に出力する。検索元出力部３７２は、ＣＰＵ９１１を用い

て、積算出部３６７が出力したｎ個の検索元T_iを入力して、外部に出力する。検索乱数元出力部３７３は、ＣＰＵ９１１を用いて、累乗部３９１が出力したｎ個の検索乱数元t_iを入力して、外部に出力する。

【０１６５】

図１５は、この実施の形態における索引暗号化装置２００の構成の一例を示すブロック構成図である。

索引暗号化装置２００は、設定記憶部２１０、索引入力部２２１、索引変換部２２３、索引整数記憶部２２４、索引乱数生成部２３０、判定元算出部２４０、乱数元算出部２７０、索引元算出部２５０、暗号化索引出力部２６０を有する。

【０１６６】

設定記憶部２１０は、第一生成元記憶部２１１、第二生成元記憶部２１２、索引数記憶部２１５、公開元記憶部２１６、公開乱数元記憶部２１７を有する。第一生成元記憶部２１１は、磁気ディスク装置９２０を用いて、群G_1の生成元g_1を記憶する。第二生成元記憶部２１２は、磁気ディスク装置９２０を用いて、群G_2の生成元g_2を記憶する。索引数記憶部２１５は、磁気ディスク装置９２０を用いて、索引数ｎを記憶する。公開元記憶部２１６は、磁気ディスク装置９２０を用いて、設定装置１００が公開した公開元g_1’を記憶する。公開乱数元記憶部２１７は、磁気ディスク装置９２０を用いて、設定装置１００が公開したｎ個の公開乱数元u_iを記憶する。

【０１６７】

判定元算出部２４０は、ペアリング値算出部２４１、累乗部２４２を有する。

ペアリング値算出部２４１は、ＣＰＵ９１１を用いて、公開元記憶部２１６が記憶した公開元g_1’と、第二生成元記憶部２１２が記憶した群G_2の生成元g_2とを入力する。ペアリング値算出部２４１は、ＣＰＵ９１１を用いて、ペアリング写像ｅにより、元g_1’と元g_2との組を写像した群G_3の元ｅ（g_1’，g_2）を算出する。ペアリング値算出部２４１は、ＣＰＵ９１１を用いて、算出した元ｅ（g_1’，g_2）を出力する。

累乗部２４２は、ＣＰＵ９１１を用いて、ペアリング値算出部２４１が出力した元ｅ（g_1’，g_2）と、索引乱数生成部２３０が出力した索引乱数ｓとを入力する。累乗部２４２は、ＣＰＵ９１１を用いて、元ｅ（g_1’，g_2）のｓ乗である群G_3の元［ｅ（g_1’，g_2）^{s}］を算出する。累乗部２４２は、ＣＰＵ９１１を用いて、算出した元を判定元Ｅ’として出力する。

ここで、公開元g_1’は、群G_1の生成元g_1のｙ乗であるから、判定元Ｅ’は、群G_3の元ｅ（g_1，g_2）の（ｓ・ｙ）乗である。

【０１６８】

乱数元算出部２７０は、ＣＰＵ９１１を用いて、乱数元Ｅ”を算出する。乱数元Ｅ”は、索引乱数を暗号化したものであり、暗号化索引データの一部である。乱数元算出部２７０は、累乗部２７１を有する。

累乗部２７１は、ＣＰＵ９１１を用いて、第一生成元記憶部２１１が記憶した群G_1の生成元g_1と、索引乱数生成部２３０が出力した索引乱数ｓとを入力する。累乗部２７１は、ＣＰＵ９１１を用いて、元g_1のｓ乗である群G_1の元（g_1^s）を算出する。累乗部２７１は、ＣＰＵ９１１を用いて、算出した元（g_1^s）を乱数元Ｅ”として出力する。

【０１６９】

索引元算出部２５０は、関数値算出部２５２、累乗部２５３を有する。

関数値算出部２５２は、ＣＰＵ９１１を用いて、公開乱数元記憶部２１７が記憶したｎ個の公開乱数元u_iと、索引整数記憶部２２４が記憶したｎ個の索引整数h_iとを入力する。関数値算出部２５２は、ＣＰＵ９１１を用いて、１以上ｎ以下のｎ個の整数それぞれについて、対応する公開乱数元u_iと、対応する索引整数h_iとに基づいて、索引整数h_iと公開乱数元u_iとの組を関数Ｕに代入した値を算出する。関数値算出部２５２は、ＣＰＵ９１１を用いて、算出したｎ個の値を関数値Ｕ（h_i，u_i）として出力する。

関数Ｕは、関数値算出部３６２が用いる関数と同じ関数である。したがって、索引整数

h_iと検索整数η_iとが等しければ、関数値算出部２５２が算出する関数値Ｕ（h_i，u_i）と関数値算出部３６２が算出する関数値Ｕ（η_i，u_i）とは等しい。

【０１７０】

累乗部２５３は、ＣＰＵ９１１を用いて、関数値算出部２５２が出力したｎ個の関数値Ｕ（h_i，u_i）と、索引乱数生成部２３０が出力した索引乱数ｓとを入力する。累乗部２５３は、ＣＰＵ９１１を用いて、１以上ｎ以下のｎ個の整数それぞれについて、関数値Ｕ（h_i，u_i）のｓ乗である群G_2の元［Ｕ（h_i，u_i）^{s}］を算出する。累乗部２５３は、ＣＰＵ９１１を用いて、算出したｎ個の元［Ｕ（h_i，u_i）^{s}］を索引元E_iとして出力する。

【０１７１】

暗号化索引出力部２６０は、索引元出力部２６１、判定元出力部２６３、乱数元出力部２６４を有する。索引元出力部２６１は、ＣＰＵ９１１を用いて、累乗部２５３が出力したｎ個の索引元E_iを入力して、外部に出力する。判定元出力部２６３は、ＣＰＵ９１１を用いて、累乗部２４２が出力した判定元Ｅ’を入力して、外部に出力する。乱数元出力部２６４は、ＣＰＵ９１１を用いて、累乗部２７１が出力した乱数元Ｅ”を入力して、外部に出力する。

【０１７２】

図１６は、この実施の形態における検索装置４００の構成の一例を示すブロック構成図である。

検索装置４００は、索引数記憶部４１５、暗号化索引記憶部４２０、暗号化検索記憶部４３０、判定対象選択部４４１、補間係数値算出部４４２、写像元算出部４５０、比較元算出部４６０、判定部４７０を有する。

【０１７３】

暗号化索引記憶部４２０は、索引元記憶部４２１、判定元記憶部４２２、乱数元記憶部４２４を有する。索引元記憶部４２１は、磁気ディスク装置９２０を用いて、１つの暗号化索引データについてｎ個ずつ索引元E_iを記憶する。判定元記憶部４２２は、磁気ディスク装置９２０を用いて、１つの暗号化索引データについて１つずつの判定元Ｅ’を記憶する。乱数元記憶部４２４は、磁気ディスク装置９２０を用いて、１つの暗号化索引データについて１つずつの乱数元Ｅ”を記憶する。

【０１７４】

暗号化検索記憶部４３０は、閾値記憶部４３１、検索元記憶部４３２、検索乱数元記憶部４３３を有する。閾値記憶部４３１は、磁気ディスク装置９２０を用いて、閾値ｄを記憶する。検索元記憶部４３２は、磁気ディスク装置９２０を用いて、ｎ個の検索元T_iを記憶する。検索乱数元記憶部４３３は、磁気ディスク装置９２０を用いて、ｎ個の検索乱数元t_iを記憶する。

【０１７５】

写像元算出部４５０は、二つのペアリング値算出部４５１，４５３、除算部４５４、累乗部４５５を有する。

ペアリング値算出部４５１は、ＣＰＵ９１１を用いて、乱数元記憶部４２４が記憶した乱数元Ｅ”と、検索元記憶部４３２が記憶したｎ個の検索元T_iとを入力する。ペアリング値算出部４５１は、ＣＰＵ９１１を用いて、１以上ｎ以下のｎ個の整数それぞれについて、乱数元Ｅ”と、対応する検索元T_iとに基づいて、ペアリング写像ｅにより、乱数元Ｅ”と検索元T_iとの組を写像した群G_3の元ｅ（Ｅ”，T_i）を算出する。ペアリング値算出部４５１は、ＣＰＵ９１１を用いて、算出したｎ個の元ｅ（Ｅ”，T_i）（ｉは１以上ｎ以下の整数。）を出力する。

ペアリング値算出部４５３は、ＣＰＵ９１１を用いて、索引元記憶部４２１が記憶したｎ個の索引元E_iと、検索乱数元記憶部４３３が記憶したｎ個の検索乱数元t_iとを入力する。ペアリング値算出部４５３は、ＣＰＵ９１１を用いて、１以上ｎ以下のｎ個の整数それぞれについて、対応する索引元E_iと、対応する検索乱数元t_iとに基づいて、ペアリング写像ｅにより、検索乱数元t_iと索引元E_iとの組を写像した群G_3の元ｅ（t_i

，Ｅ$_{i}$）を算出する。ペアリング値算出部４５３は、ＣＰＵ９１１を用いて、算出したｎ個の元ｅ（ｔ$_{i}$，Ｅ$_{i}$）（ｉは１以上ｎ以下の整数。）を出力する。

除算部４５４は、ＣＰＵ９１１を用いて、ペアリング値算出部４５１が出力したｎ個の元ｅ（Ｅ”，Ｔ$_{i}$）と、ペアリング値算出部４５３が出力したｎ個の元ｅ（ｔ$_{i}$，Ｅ$_{i}$）とを入力する。除算部４５４は、ＣＰＵ９１１を用いて、１以上ｎ以下のｎ個の整数それぞれについて、対応する元ｅ（Ｅ”，Ｔ$_{i}$）と、対応する元ｅ（ｔ$_{i}$，Ｅ$_{i}$）とに基づいて、元ｅ（Ｅ”，Ｔ$_{i}$）を元ｅ（ｔ$_{i}$，Ｅ$_{i}$）で割った商［ｅ（Ｅ”，Ｔ$_{i}$）／ｅ（ｔ$_{i}$，Ｅ$_{i}$）］を算出する。除算部４５４は、ＣＰＵ９１１を用いて、算出したｎ個の商をペアリング値ｅ$_{i}$（ｉは１以上ｎ以下の整数。）として出力する。

ここで、乱数元Ｅ”は、群Ｇ$_{1}$の生成元ｇ$_{1}$のｓ乗であり、検索元Ｔ$_{i}$は、群Ｇ$_{2}$の生成元ｇ$_{2}$のｆ（ｉ）乗と関数値Ｕ（η$_{i}$，ｕ$_{i}$）との積であり、検索乱数元ｔ$_{i}$は、群Ｇ$_{1}$の生成元ｇ$_{1}$のｔ$_{i}$乗であり、索引元Ｅ$_{i}$は、関数値Ｕ（ｈ$_{i}$，ｕ$_{i}$）のｓ乗であるから、ペアリング値ｅ$_{i}$は、

【数２２】

$$e_i = \frac{e(E'', T_i)}{e(t_i, E_i)} = \frac{e(g_1, g_2)^{s \cdot f(i)} \cdot e(g_1, U(\eta_i, u_i))^{s \cdot r_i}}{e(g_1, U(h_i, u_i))^{s \cdot r_i}}$$

【０１７６】

である。

【０１７７】

累乗部４５５は、ＣＰＵ９１１を用いて、補間係数値算出部４４２が出力したｄ個の補間係数値Δ$_{i，S}$と、ペアリング値算出部４５１が出力したｎ個のペアリング値ｅ$_{i}$のうち判定対象選択部４４１が選択したｄ個の整数に対応するｄ個のペアリング値ｅ$_{i}$とを入力する。累乗部４５５は、判定対象選択部４４１が選択したｄ個の整数それぞれについて、対応する補間係数値Δ$_{i，S}$と、対応するペアリング値ｅ$_{i}$とに基づいて、ペアリング値ｅ$_{i}$のΔ$_{i，S}$乗である群Ｇ$_{3}$の元を算出する。累乗部４５５は、ＣＰＵ９１１を用いて、算出したｄ個の元を写像元ｅ’$_{i}$として出力する。

【０１７８】

比較元算出部４６０は、総積部４６１を有する。

総積部４６１は、ＣＰＵ９１１を用いて、累乗部４５５が出力したｄ個の写像元ｅ’$_{i}$を入力する。総積部４６１は、ＣＰＵ９１１を用いて、入力したｄ個の写像元ｅ’$_{i}$すべての総積Π［ｅ’$_{i}$］を算出する。総積部４６１は、ＣＰＵ９１１を用いて、算出した総積Π［ｅ’$_{i}$］を比較元Ｂとして出力する。

ここで、比較元Ｂは、

【数２３】

$$B = \prod_{i\in S}\left[\frac{e(g_1,g_2)^{s\cdot f(i)}\cdot e(g_1,U(\eta_i,u_i))^{s\cdot r_i}}{e(g_1,U(h_i,u_i))^{s\cdot r_i}}\right]^{\Delta_{i,S}}$$

$$= \prod_{i\in S} e(g_1,g_2)^{s\cdot f(i)\cdot\Delta_{i,S}}\cdot\prod_{i\in S}\left[\frac{e(g_1,U(\eta_i,u_i))}{e(g_1,U(h_i,u_i))}\right]^{s\cdot r_i\cdot\Delta_{i,S}}$$

$$= e(g_1,g_2)^{s\cdot y}\cdot\prod_{i\in S}\left[\frac{e(g_1,U(\eta_i,u_i))}{e(g_1,U(h_i,u_i))}\right]^{s\cdot r_i\cdot\Delta_{i,S}}$$

である。

【０１７９】

判定部４７０は、ＣＰＵ９１１を用いて、検索条件に合うか否かを判定する対象である索引について判定元記憶部４２２が記憶した判定元Ｅ’と、総積部４６１が出力した比較元Ｂとを入力する。判定部４７０は、入力した判定元Ｅ’と比較元Ｂとを比較し、一致する場合に、その索引が検索条件に合うと判定する。判定部４７０は、ＣＰＵ９１１を用いて、判定した結果を出力する。

【０１８０】

すべてのｉ∈Ｓについて、$h_i=\eta_i$である場合、Ｕ（h_i，u_i）＝Ｕ（η_i，u_i）であるから、比較元Ｂは、

【数２４】

$$B = e(g_1,g_2)^{s\cdot y}$$

となり、比較元Ｂは、判定元Ｅ’と一致する。

【０１８１】

一方、いずれかのｉ∈Ｓについて、$h_i\neq\eta_i$である場合、Ｂ＝Ｅ’となる確率は、極めて低い。例えば、ｉ∈Ｓ’（Ｓ’はＳの部分集合であり空集合でない。）について、$h_i\neq\eta_i$であり、それ以外のｉ∈Ｓについて、$h_i=\eta_i$だとすると、

【数２５】

$$B = e(g_1,g_2)^{s\cdot y}\cdot\prod_{i\in S'}\left[\frac{e(g_1,U(\eta_i,u_i))}{e(g_1,U(h_i,u_i))}\right]^{s\cdot r_i\cdot\Delta_{i,S}}$$

である。例えば、関数Ｕが数２１で定義される関数である場合、

【数２６】

$$\prod_{i\in S'}\left[\frac{e(g_1,U(\eta_i,u_i))}{e(g_1,U(h_i,u_i))}\right]^{s\cdot r_i\cdot\Delta_{i,S}} = \prod_{i\in S'} e(g_1,g_2)^{s\cdot r_i\cdot\Delta_{i,S}\cdot(\eta_i-h_i)}$$

$$= e(g_1,g_2)^{s\cdot\sum_{i\in S'}[r_i\cdot\Delta_{i,S}\cdot(\eta_i-h_i)]}$$

であるから、Ｂ＝Ｅ’となるのは、

【数２７】

$$\sum_{i\in S'}[r_i\cdot\Delta_{i,S}\cdot(\eta_i-h_i)]=0$$

の場合のみである。この値は、０以上ｐ未満のランダムな値をとるから、０になる確率は１／ｐである。ｐは通常大きな数であるから、この確率は、極めて低い。

【０１８２】

図１７は、この実施の形態における設定処理Ｓ６１０の流れの一例を示すフローチャート図である。

設定処理Ｓ６１０は、第二生成元生成工程Ｓ６１２、秘密整数生成工程Ｓ６１４、公開元算出工程Ｓ６１５、整数選択工程Ｓ６１６、公開乱数元生成工程Ｓ６１８、整数繰り返し工程Ｓ６２０を有する。

【０１８３】

第二生成元生成工程Ｓ６１２において、第二生成元算出部１４７は、ＣＰＵ９１１を用いて、群$Ｇ_2$の元であって単位元でない元をランダムに生成して、生成元$ｇ_2$とする。

秘密整数生成工程Ｓ６１４において、秘密整数生成部１３１は、ＣＰＵ９１１を用いて、１以上ｐ未満の整数をランダムに生成して、秘密整数ｙとする。

公開元算出工程Ｓ６１５において、公開元算出部１４１は、ＣＰＵ９１１を用いて、第一生成元記憶部１１１が記憶した群$Ｇ_1$の生成元$ｇ_1$と、秘密整数生成工程Ｓ６１４で秘密整数生成部１３１が生成した秘密整数ｙとに基づいて、元$ｇ_1$のｙ乗である群$Ｇ_1$の元を算出して、公開元$ｇ_1$’とする。

【０１８４】

整数選択工程Ｓ６１６において、公開乱数元算出部１４２は、ＣＰＵ９１１を用いて、１以上ｎ以下のｎ個の整数のなかから、整数を１つずつ順に選択して、整数ｉとする。

公開乱数元生成工程Ｓ６１８において、公開乱数元算出部１４２は、ＣＰＵ９１１を用いて、整数選択工程Ｓ６１６で選択した整数iについて、群$Ｇ_2$の元であって単位元でない元をランダムに生成して、公開乱数元$ｕ_i$とする。

整数繰り返し工程Ｓ６２０において、公開乱数元算出部１４２は、ＣＰＵ９１１を用いて、１以上ｎ以下のすべての整数を、整数選択工程Ｓ６１６で選択したか否かを判定する。まだ選択していない整数があると判定した場合、公開乱数元算出部１４２は、ＣＰＵ９１１を用いて、整数選択工程Ｓ６１６に戻り、次の整数を選択する。すべての整数を選択したと判定した場合、設定装置１００は、設定処理Ｓ６１０を終了する。

【０１８５】

図１８は、この実施の形態における索引暗号化処理Ｓ６３０の流れの一例を示すフローチャート図である。

索引暗号化処理Ｓ６３０は、索引乱数生成工程Ｓ６３１、判定元算出工程Ｓ６３２、乱数元算出工程Ｓ６３４、整数選択工程Ｓ６３５、索引整数算出工程Ｓ６３６、索引元算出工程Ｓ６３７、整数繰り返し工程Ｓ６３８を有する。

【０１８６】

索引乱数生成工程Ｓ６３１において、索引乱数生成部２３０は、ＣＰＵ９１１を用いて、１以上ｐ未満の整数をランダムに生成して、索引乱数ｓとする。

判定元算出工程Ｓ６３２において、ペアリング値算出部２４１は、ＣＰＵ９１１を用いて、ペアリング写像ｅにより、公開元記憶部２１６が記憶した公開元$ｇ_1$’と、第二生成元記憶部２１２が記憶した群$Ｇ_2$の生成元$ｇ_2$との組を写像した群$Ｇ_3$の元ｅ（$ｇ_1$’，$ｇ_2$）を算出する。累乗部２４２は、ＣＰＵ９１１を用いて、ペアリング値算出部２４１が算出した元ｅ（$ｇ_1$’，$ｇ_2$）と、索引乱数生成工程Ｓ６３１で索引乱数生成部２３０が生成した索引乱数ｓとに基づいて、元ｅ（$ｇ_1$’，$ｇ_2$）のｓ乗である群$Ｇ_3$の元を算出して、判定元Ｅ’とする。

乱数元算出工程Ｓ６３４において、累乗部２７１は、ＣＰＵ９１１を用いて、第一生成

元記憶部２１１が記憶した群G_1の生成元g_1と、索引乱数生成工程Ｓ６３１で索引乱数生成部２３０が生成した索引乱数ｓとに基づいて、元g_1のｓ乗である群G_1の元を算出して、乱数元Ｅ”とする。

【０１８７】

整数選択工程Ｓ６３５において、索引変換部２２３は、ＣＰＵ９１１を用いて、１以上ｎ以下のｎ個の整数のなかから、整数を１つずつ順に選択して、整数ｉとする。

索引整数算出工程Ｓ６３６において、索引変換部２２３は、ＣＰＵ９１１を用いて、整数選択工程Ｓ６３５で選択した整数ｉについて、写像Ｈにより、索引入力部２２１が入力した索引文字列w_iを写像した整数を算出して、索引整数h_iとする。

索引元算出工程Ｓ６３７において、関数値算出部２５２は、ＣＰＵ９１１を用いて、整数選択工程Ｓ６３５で索引変換部２２３が選択した整数ｉについて、索引整数算出工程Ｓ６３６で索引変換部２２３が算出した索引整数h_iと、公開乱数元u_iとの組を、関数Ｕに代入した値である群G_2の元を算出して、関数値Ｕ（h_i，u_i）とする。累乗部２５３は、ＣＰＵ９１１を用いて、関数値算出部２５２が算出した関数値Ｕ（h_i，u_i）と、索引乱数生成工程Ｓ６３１で索引乱数生成部２３０が生成した索引乱数ｓとに基づいて、関数値Ｕ（h_i，u_i）のｓ乗である群G_2の元を算出して、索引元E_iとする。

整数繰り返し工程Ｓ６３８において、索引変換部２２３は、ＣＰＵ９１１を用いて、１以上ｎ以下のすべての整数を、整数選択工程Ｓ６３５で選択したか否かを判定する。まだ選択していない整数があると判定した場合、索引変換部２２３は、ＣＰＵ９１１を用いて、整数選択工程Ｓ６３５に戻り、次の整数を選択する。すべての整数を選択したと判定した場合、索引暗号化装置２００は、索引暗号化処理Ｓ６３０を終了する。

【０１８８】

図１９は、この実施の形態における検索暗号化処理Ｓ６５０の流れの一例を示すフローチャート図である。

検索暗号化処理Ｓ６５０は、次数選択工程Ｓ６５１、多項式係数生成工程Ｓ６５２、次数繰り返し工程Ｓ６５３、最高次係数生成工程Ｓ６５４、整数選択工程Ｓ６５５、検索整数算出工程Ｓ６５６、多項式値算出工程Ｓ６５７、検索乱数生成工程Ｓ６５８、検索元算出工程Ｓ６５９、検索乱数元算出工程Ｓ６６０、整数繰り返し工程Ｓ６６１を有する。

【０１８９】

検索乱数生成工程Ｓ６５８において、検索乱数生成部３８０は、ＣＰＵ９１１を用いて、整数選択工程Ｓ６５５で検索変換部３５２が選択した整数ｉについて、１以上ｐ未満の整数をランダムに生成して、検索乱数r_iとする。

検索元算出工程Ｓ６５９において、関数値算出部３６２は、ＣＰＵ９１１を用いて、整数選択工程Ｓ６５５で検索変換部３５２が選択した整数ｉについて、検索整数算出工程Ｓ６５６で検索変換部３５２が算出した検索整数η_iと、公開乱数元u_iとの組を、関数Ｕに代入した値である群G_2の元を算出して、関数値Ｕ（η_i，u_i）とする。累乗部３６５は、ＣＰＵ９１１を用いて、関数値算出部３６２が算出した関数値Ｕ（η_i，u_i）と、検索乱数生成工程Ｓ６５８で検索乱数生成部３８０が生成した検索乱数r_iとに基づいて、関数値Ｕ（η_i，u_i）のr_i乗である群G_2の元［Ｕ（η_i，u_i）＾r_i］を算出する。累乗部３６６は、ＣＰＵ９１１を用いて、第二生成元記憶部３１２が記憶した群G_2の生成元g_2と、多項式値算出工程Ｓ６５７で多項式値算出部３４４が算出した多項式値ｆ（ｉ）とに基づいて、元g_2のｆ（ｉ）乗である群G_2の元［g_2＾ｆ（ｉ）］を算出する。積算出部３６７は、ＣＰＵ９１１を用いて、累乗部３６６が算出した元［g_2＾ｆ（ｉ）］と、累乗部３６５が算出した元［Ｕ（η_i，u_i）＾r_i］との積である群G_2の元を算出して、検索元T_iとする。

検索乱数元算出工程Ｓ６６０において、累乗部３９１は、ＣＰＵ９１１を用いて、第一生成元記憶部３１１が記憶した群G_1の生成元g_1と、検索乱数生成工程Ｓ６５８で検索乱数生成部３８０が生成した検索乱数r_iとに基づいて、元g_1のr_i乗である群G_1の元を算出して、検索乱数元t_iとする。

【０１９０】

図２０は、この実施の形態における検索実行処理Ｓ６７０の流れの一例を示すフローチャート図である。

検索実行処理Ｓ６７０は、索引選択工程Ｓ６７１、整数選択工程Ｓ６７２、ペアリング値算出工程Ｓ６７３、整数繰り返し工程Ｓ６７４、判定選択工程Ｓ６７５、判定整数選択工程Ｓ６７６、補間係数値算出工程Ｓ６７７、累乗工程Ｓ６７８、判定整数繰り返し工程Ｓ６７９、総積工程Ｓ６８０、判定工程Ｓ６８１、判定繰り返し工程Ｓ６８２、索引繰り返し工程Ｓ６８３を有する。

【０１９１】

ペアリング値算出工程Ｓ６７３において、ペアリング値算出部４５１は、ＣＰＵ９１１を用いて、索引選択工程Ｓ６７１で選択した暗号化索引データについて乱数元記憶部４２４が記憶した乱数元Ｅ”と、整数選択工程Ｓ６７２で選択した整数ｉについて検索元記憶部４３２が記憶した検索元$Ｔ_{i}$とに基づいて、ペアリング写像ｅにより、乱数元Ｅ”と検索元$Ｔ_{i}$との組を写像した群$Ｇ_{3}$の元ｅ（Ｅ”，$Ｔ_{i}$）を算出して、第一ペアリング値とする。ペアリング値算出部４５３は、ＣＰＵ９１１を用いて、整数選択工程Ｓ６７２で選択した整数ｉについて、索引元記憶部４２１が記憶した索引元$Ｅ_{i}$と、検索乱数元記憶部４３３が記憶した検索乱数元$ｔ_{i}$とに基づいて、ペアリング写像ｅにより、検索乱数元$ｔ_{i}$と索引元$Ｅ_{i}$との組を写像した群$Ｇ_{3}$の元ｅ（$ｔ_{i}$，$Ｅ_{i}$）を算出して第二ペアリング値とする。除算部４５４は、ＣＰＵ９１１を用いて、ペアリング値算出部４５１が算出した第一ペアリング値ｅ（Ｅ”，$Ｔ_{i}$）と、ペアリング値算出部４５３が算出した第二ペアリング値ｅ（$ｔ_{i}$，$Ｅ_{i}$）とに基づいて、第一ペアリング値ｅ（Ｅ”，$Ｔ_{i}$）を第二ペアリング値ｅ（$ｔ_{i}$，$Ｅ_{i}$）で割った商である群$Ｇ_{3}$の元を算出して、ペアリング値$ｅ_{i}$とする。

【０１９２】

この実施の形態における検索システム８００は、実施の形態１と同様の効果を奏する。

更に、検索暗号化装置３００が耐タンパ性のある記憶装置などを用いて秘密裡に保持すべき秘密整数の数が、索引数ｎにかかわらず１つなので、耐タンパ性のある記憶装置の記憶容量によって、索引数ｎが制限されることがない。

【０１９３】

この実施の形態で用いる写像$φ_{1}$～$φ_{5}$は、次の式で定義される。

【数２８】

$$\phi_1 : \mathbb{Z}_p \to \mathbb{G}_1 \qquad \phi_1(x) = {g_1}^x$$

$$\phi_2 : \mathbb{Z}_p \to \mathbb{G}_2 \qquad \phi_2(x) = U(x, u_i)^s$$

$$\phi_3 : \mathbb{G}_1 \to \mathbb{G}_3 \qquad \phi_3(X) = e(X, g_2)^s$$

$$\phi_4 : \mathbb{Z}_p^* \times \mathbb{Z}_p \to \mathbb{G}_2$$

$$\phi_4(x_1, x_2) = {g_2}^{x_2} \cdot U(x_1, u_i)^{r_i}$$

$$\phi_5 : \mathbb{G}_2 \times \mathbb{G}_2 \times \mathbb{Z}_p \to \mathbb{G}_3$$

$$\phi_5(X_1, X_2, x_3) = \left[\frac{e({g_1}^s, X_2)}{e({g_1}^{r_i}, X_1)}\right]^{x_3}$$

【０１９４】

すなわち、第一の写像$φ_{1}$は、０以上ｐ未満の整数を位数ｐの群$Ｇ_{1}$の元へ写す写像であり、整数ｘを、元$ｇ_{1}$のｘ乗へ写す。元$ｇ_{1}$は群$Ｇ_{1}$の単位元でない。したがって、第一の写像$φ_{1}$は全単射であり、整数がｐを法とする加法についてなす群から群$Ｇ_{1}$への同型写像である。

第二の写像φ$_2$は、０以上ｐ未満の整数を位数ｐの群Ｇ$_2$の元へ写す写像であり、整数ｘを、関数値Ｕ（ｘ，ｕ$_i$）のｓ乗へ写す。索引整数ｓは０でない。したがって、関数Ｕがｘについて全単射であれば、第二の写像φ$_2$も全単射である。

第三の写像φ$_3$は、位数ｐの群Ｇ$_1$の元を位数ｐの群Ｇ$_3$へ写す写像であり、元Ｘを、元ｅ（Ｘ，ｇ$_2$）のｓ乗へ写す。生成元ｇ$_2$は群Ｇ$_2$の単位元でなく、ペアリング写像ｅは双線形かつ非縮退であり、索引乱数ｓは０でない。したがって、第三の写像φ$_3$は全単射であり、同型写像である。

第四の写像φ$_4$は、０以上ｐ未満の整数と０以上ｐ未満の整数との組を位数ｐの群Ｇ$_2$の元へ写す写像であり、整数ｘ$_1$と整数ｘ$_2$との組（ｘ$_1$，ｘ$_2$）を、元ｇ$_2$のｘ$_2$乗と関数値Ｕ（ｘ$_1$，ｕ$_i$）のｒ$_i$乗との積へ写す。生成元ｇ$_2$は群Ｇ$_2$の単位元でなく、検索乱数ｒ$_i$は０でない。したがって、ｘ$_2$を固定して考えると、ｘ$_2$が０でなく、関数Ｕが全単射であれば、第四の写像φ$_4$は、全単射である。また、ｘ$_1$を固定して考えると、第四の写像φ$_4$は全単射であり、整数がｐを法とする加法についてなす群から群Ｇ$_2$への同型写像である。

第五の写像φ$_5$は、位数ｐの群Ｇ$_2$の元と位数ｐの群Ｇ$_2$の元と０以上ｐ未満の整数との組を位数ｐの群Ｇ$_3$の元に写す写像であり、元Ｘ$_1$と元Ｘ$_2$と整数ｘ$_3$との組（Ｘ$_1$，Ｘ$_2$，ｘ$_3$）を、元ｅ（ｇ$_1$^{s}，Ｘ$_2$）を元ｅ（ｇ$_1$＾ｒ$_i$，Ｘ$_1$）で割った商のｘ$_3$乗へ写す。生成元ｇ$_1$は群Ｇ$_1$の単位元でなく、索引乱数ｓ及び検索乱数ｒ$_i$は０でなく、ペアリング写像ｅは双線形かつ非縮退である。したがって、Ｘ$_2$，ｘ$_3$を固定して考えると、第五の写像φ$_5$は、ｘ$_3$が０でないとき全単射である。また、Ｘ$_1$，ｘ$_3$を固定して考えると、第五の写像φ$_5$は、ｘ$_3$が０でないとき全単射であり、群Ｇ$_2$から群Ｇ$_3$への同型写像である。更に、Ｘ$_1$，Ｘ$_2$を固定して考えると、第五の写像φ$_5$は全単射であり、整数がｐを法とする加法についてなす群から群Ｇ$_3$への同型写像である。

【０１９５】

また、この実施の形態における写像φ$_1$～φ$_5$については、次の関係が成り立つ。

【数２９】

$$\phi_3(\phi_1(x)) = (e(g_1, g_2)^s)^x$$

$$\phi_5(\phi_2(x_1), \phi_4(x_1, x_2), x_3)$$

$$= \left[\frac{e({g_1}^s, {g_2}^{x_2} \cdot U(x_1, u_i)^{r_i})}{e({g_1}^{r_i}, U(x_1, u_i)^s)}\right]^{x_3}$$

$$= (e(g_1, g_2)^s)^{x_2 \cdot x_3}$$

【０１９６】

この実施の形態における検索システム８００において、上記設定装置１００は、更に、公開乱数元算出部１４２を有する。

上記公開元算出部１４１は、上記処理装置を用いて、第一の群Ｇ$_1$の生成元である第一生成元ｇ$_1$（上記第一の群Ｇ$_1$の位数はｐ。）と、上記秘密整数生成部１３１が生成した秘密整数ｙとに基づいて、上記秘密整数ｙと等しい数の上記第一生成元ｇ$_1$を、上記第一の群Ｇ$_1$の群演算により結合した元ｇ$_1$^{y}を算出して、公開元ｇ$_1$’とする。

上記公開乱数元算出部１４２は、上記処理装置を用いて、１以上ｎ以下のｎ個の整数ｉそれぞれについて、第二の群Ｇ$_2$の生成元（上記第二の群の位数はｐ。）をランダムに生成して、ｎ個の公開乱数元ｕ$_i$とする。

上記索引暗号化装置２００は、更に、公開乱数元記憶部２１７と、乱数元算出部２７０とを有する。

上記公開乱数元記憶部２１７は、上記記憶装置を用いて、上記設定装置１００が算出したｎ個の公開乱数元ｕ$_i$を記憶する。

上記索引乱数生成部２３０は、上記処理装置を用いて、１以上ｐ未満の整数をランダム

に生成して、索引乱数ｓとする。

上記判定元算出部２４０は、上記処理装置を用いて、上記第二の群G_2の生成元である第二生成元g_2と、上記公開元記憶部２１６が記憶した公開元g_1’とに基づいて、上記第一の群G_1の元と上記第二の群G_2の元との組を第三の群G_3の元（上記第三の群の位数はｐ。）に写像する双線形ペアリング写像ｅにより、上記公開元g_1’と上記第二生成元g_2との組が写像される上記第三の群G_3の元ｅ（g_1’，g_2）を算出し、算出した上記第三の群G_3の元ｅ（g_1’，g_2）と、上記索引乱数生成部２３０が生成した索引乱数ｓとに基づいて、上記索引乱数ｓと等しい数の上記第三の群G_3の元ｅ（g_1’，g_2）を、上記第三の群G_3の群演算により結合した元ｅ（g_1’，g_2）^{s}を算出して、判定元Ｅ’とする。

上記乱数元算出部２７０は、上記処理装置を用いて、上記第一生成元g_1と、上記索引乱数生成部２３０が生成した索引乱数ｓとに基づいて、上記索引乱数ｓと等しい数の上記第一生成元g_1を、上記第一の群G_1の群演算により結合した元g_1^sを算出して、乱数元Ｅ”とする。

上記索引元算出部２５０は、上記処理装置を用いて、１以上ｎ以下のｎ個の整数ｉそれぞれについて、上記索引整数記憶部２２４が記憶した索引整数h_iと、上記公開乱数元記憶部２１７が記憶した公開乱数元u_iとに基づいて、０以上ｐ未満の整数と上記第二の群G_2の元との組を上記第二の群G_2の元に写像する写像関数Ｕにより、上記索引整数h_iと上記公開乱数元u_iとの組を写像した上記第二の群G_2の元を算出して、ｎ個の索引関数値Ｕ（h_i，u_i）とし、１以上ｎ以下のｎ個の整数ｉそれぞれについて、算出した上記索引関数値Ｕ（h_i，u_i）と、上記索引乱数生成部２３０が生成した索引乱数ｓとに基づいて、上記索引乱数ｓと等しい数の上記索引関数値Ｕ（h_i，u_i）を、上記第二の群G_2の群演算により結合した元Ｕ（h_i，u_i）^{s}を算出して、ｎ個の索引元E_iとする。

上記検索暗号化装置３００は、更に、公開乱数元記憶部３１７と、検索乱数生成部３８０と、検索乱数元算出部３９０とを有する。

上記公開乱数元記憶部３１７は、上記記憶装置を用いて、上記設定装置１００が算出したｎ個の公開乱数元u_iを記憶する。

上記検索乱数生成部３８０は、上記処理装置を用いて、１以上ｎ以下のｎ個の整数ｉそれぞれについて、１以上ｐ未満の整数をランダムに生成して、ｎ個の検索乱数r_iとする。

上記検索元算出部３６０は、上記処理装置を用いて、１以上ｎ以下のｎ個の整数ｉそれぞれについて、上記検索整数記憶部３５３が記憶した検索整数η_iと、上記公開乱数元記憶部３１７が記憶した公開乱数元u_iとに基づいて、上記写像関数Ｕにより、上記検索整数η_iと上記公開乱数元u_iとの組を写像して、上記第二の群G_2の元を算出して、ｎ個の検索関数値Ｕ（η_i，u_i）とし、１以上ｎ以下のｎ個の整数ｉそれぞれについて、算出した上記検索関数値Ｕ（η_i，u_i）と、上記検索乱数生成部３８０が生成した検索乱数r_iとに基づいて、上記検索乱数r_iと等しい数の上記検索関数値Ｕ（η_i，u_i）を、上記第二の群G_2の群演算により結合した元［Ｕ（η_i，u_i）＾r_i］を算出し、上記第二生成元g_2と、上記多項式値算出部３４４が算出した多項式値ｆ（ｉ）とに基づいて、上記多項式値ｆ（ｉ）と等しい数の上記第二生成元g_2を、上記第二の群G_2の群演算により結合した元［g_2＾ｆ（ｉ）］を算出し、算出した上記第二の群の二つの元［Ｕ（η_i，u_i）＾r_i］，［g_2＾ｆ（ｉ）］を上記第二の群G_2の群演算により結合した元を算出して、ｎ個の検索元T_iとする。

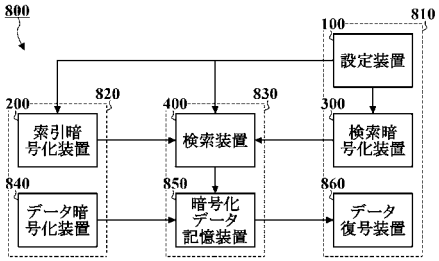
上記検索乱数元算出部３９０は、上記処理装置を用いて、１以上ｎ以下のｎ個の整数ｉそれぞれについて、上記第一生成元g_1と、上記検索乱数生成部３８０が生成した検索乱数r_iとに基づいて、上記検索乱数r_iと等しい数の上記第一生成元g_1を、上記第一の群G_1の群演算により結合した元［g_1＾r_i］を算出して、ｎ個の検索乱数元t_iとする。

上記検索装置４００は、更に、乱数元記憶部４２４と、検索乱数元記憶部４３３とを有

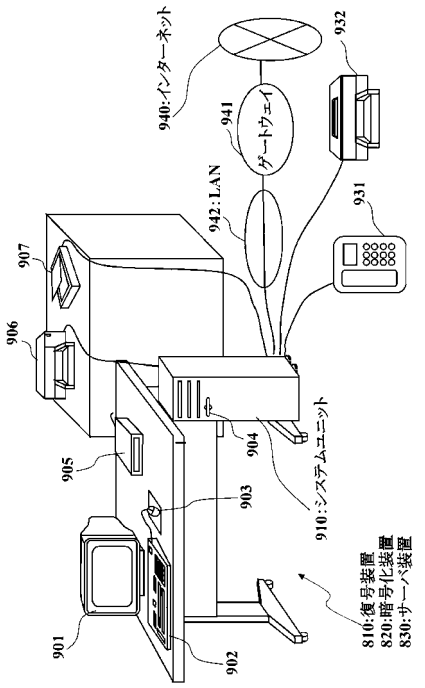
する。
上記乱数元記憶部４２４は、上記記憶装置を用いて、上記索引暗号化装置２００が算出した乱数元Ｅ”を記憶する。
上記検索乱数元記憶部４３３は、上記記憶装置を用いて、上記検索暗号化装置３００が算出したｎ個の検索乱数元t_iを記憶する。
上記写像元算出部４５０は、上記処理装置を用いて、上記判定対象選択部４４１が選択したｄ個の判定対象整数それぞれについて、上記乱数元記憶部４２４が記憶した乱数元Ｅ”と、上記検索元記憶部４３２が記憶した検索元T_iとに基づいて、上記双線形ペアリング写像ｅにより、上記乱数元Ｅ”と上記検索元T_iとの組を写像した上記第三の群の元を算出して、ｄ個の第一ペアリング値ｅ（Ｅ”，T_i）とし、上記判定対象選択部４４１が選択したｄ個の判定対象整数それぞれについて、上記検索乱数元記憶部４３３が記憶した検索乱数元t_iと、上記索引元記憶部４２１が記憶した索引元E_iとに基づいて、上記双線形ペアリング写像ｅにより、上記検索乱数元t_iと上記索引元E_iとの組を写像した上記第三の群G_3の元を算出して、ｄ個の第二ペアリング値ｅ（t_i，E_i）とし、上記判定対象選択部４４１が選択したｄ個の判定対象整数それぞれについて、算出した上記第一ペアリング値ｅ（Ｅ”，T_i）と、算出した上記第二ペアリング値ｅ（t_i，E_i）の逆元とを上記第三の群G_3の群演算により結合した元［ｅ（Ｅ”，T_i）／ｅ（t_i，E_i）を算出して、ｄ個の写像元e'_iとする。
上記比較元算出部４６０は、上記処理装置を用いて、上記写像元算出部４５０が算出したｄ個の写像元e'_iを、上記第三の群G_3の群演算により結合した元Π［e'_i］を算出して、比較元Ｂとする。
【０１９７】
安全性の証明については省略するが、この実施の形態における検索システム８００によれば、索引整数や検索整数を解読しようとする第三者の攻撃に対して、安全性を有する。
更に、検索暗号化装置３００が秘密裡に保持すべき秘密データの量が少なく、索引数ｎにかかわらず一定なので、耐タンパ性を有する記憶装置の記憶容量が少なくて済み、また、耐タンパ性を有する記憶装置の記憶容量により、索引数ｎが制限されることがない。
【０１９８】
なお、実施の形態１のなかで説明した各種の変形は、この実施の形態における検索システム８００に対しても適用することができる。
【０１９９】
以上説明した検索システム８００を、例えば、個人の年齢・住所・職業・嗜好などの属性情報を保存したデータベースに適用すれば、ある属性に近い人物のみを抽出する秘匿データマッチングを実現できる。あるいは、画像データをピクセルごとに保存したデータベースに適用すれば、ある画像に近い画像のみを抽出する秘匿画像マッチングを実現できる。あるいは、指紋情報・光彩情報・静脈情報などの生体情報を保存したデータベースに適用すれば、個人識別時に生体情報を用いて検索を行うことにより、生体情報の安全性を保ちつつ個人識別や個人認証を行う生体認証を実現できる。
【符号の説明】
【０２００】
１００　設定装置、１１０，２１０，３１０　設定記憶部、１１１，２１１，３１１　第一生成元記憶部、１１２，２１２，３１２　第二生成元記憶部、１１３　第三生成元記憶部、１１５，２１５，３１５，４１５　索引数記憶部、１２１　ペアリング値算出部、１３０　秘密生成部、１３１　秘密整数生成部、１３２　秘密乱数生成部、１４０　公開算出部、１４１　公開元算出部、１４２　公開乱数元算出部、１４７　第二生成元算出部、１５０　公開出力部、１５１　公開元出力部、１５２　公開乱数元出力部、１５６　第一生成元出力部、１５７　第二生成元出力部、２００　索引暗号化装置、２１６　公開元記憶部、２１７，３１７　公開乱数元記憶部、２２１　索引入力部、２２３　索引変換部、２２４　索引整数記憶部、２３０　索引乱数生成部、２４０　判定元算出部、２４１　ペアリング値算出部、２４２　累乗部、２５０　索引元算出部、２５１　指数算出部、２

５２　関数値算出部、２５３　累乗部、２６０　暗号化索引出力部、２６１　索引元出力部、２６２　判定元出力部、２６３　判定元出力部、２６４　乱数元出力部、２７０　乱数元算出部、２７１　累乗部、３００　検索暗号化装置、３２０　秘密記憶部、３２１　秘密整数記憶部、３２３　秘密乱数記憶部、３３０　検索条件入力部、３３１　閾値入力部、３３２　検索入力部、３４１　閾値記憶部、３４２　多項式係数生成部、３４３　多項式係数記憶部、３４４　多項式値算出部、３５２　検索変換部、３５３　検索整数記憶部、３６０　検索元算出部、３６１　指数算出部、３６２　関数値算出部、３６５，３６６　累乗部、３６７　積算出部、３７０　暗号化検索出力部、３７１　閾値出力部、３７２　検索元出力部、３７３　検索乱数元出力部、３８０　検索乱数生成部、３９０　検索乱数元算出部、３９１　累乗部、４００　検索装置、４２０　暗号化索引記憶部、４２１　索引元記憶部、４２２　判定元記憶部、４２４　乱数元記憶部、４３０　暗号化検索記憶部、４３１　閾値記憶部、４３２　検索元記憶部、４３３　検索乱数元記憶部、４４１　判定対象選択部、４４２　補間係数値算出部、４５０　写像元算出部、４５１，４５３　ペアリング値算出部、４５４　除算部、４５５　累乗部、４６０　比較元算出部、４６１　総積部、４７０　判定部、８００　検索システム、８１０　復号装置、８２０　暗号化装置、８３０　サーバ装置、８４０　データ暗号化装置、８４１　本体記憶部、８４２　暗号化鍵記憶部、８４３　本体暗号化部、８５０　暗号化データ記憶装置、８５１　暗号化本体記憶部、８５２　検索結果入力部、８５３　検索本体出力部、８６０　データ復号装置、８６１　復号鍵記憶部、８６２　本体復号部、８６３　復号本体出力部、９０１　表示装置、９０２　キーボード、９０３　マウス、９０４　ＦＤＤ、９０５　ＣＤＤ、９０６　プリンタ装置、９０７　スキャナ装置、９１０　システムユニット、９１１　ＣＰＵ、９１２　バス、９１３　ＲＯＭ、９１４　ＲＡＭ、９１５　通信装置、９２０　磁気ディスク装置、９２１　ＯＳ、９２２　ウィンドウシステム、９２３　プログラム群、９２４　ファイル群、９３１　電話器、９３２　ファクシミリ機、９４０　インターネット、９４１　ゲートウェイ、９４２　ＬＡＮ。

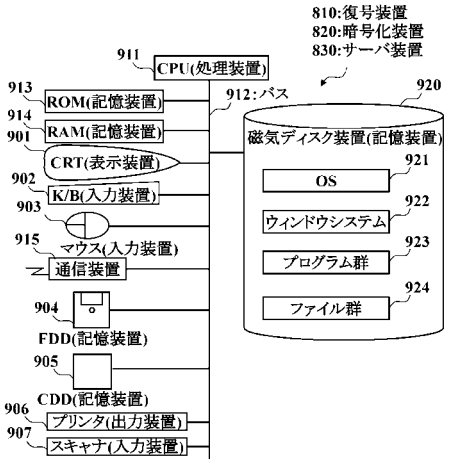
【図１】



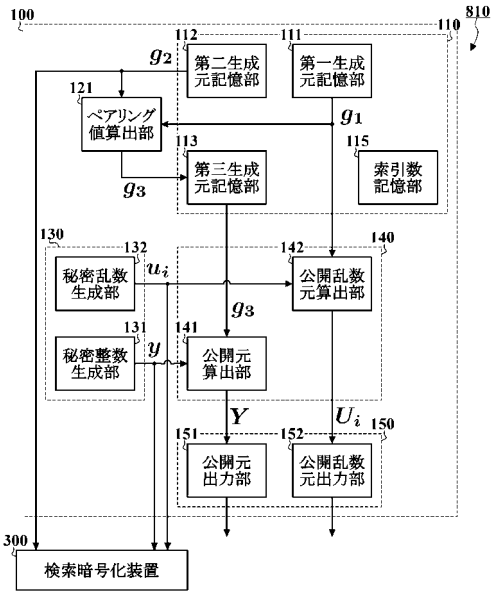
【図２】



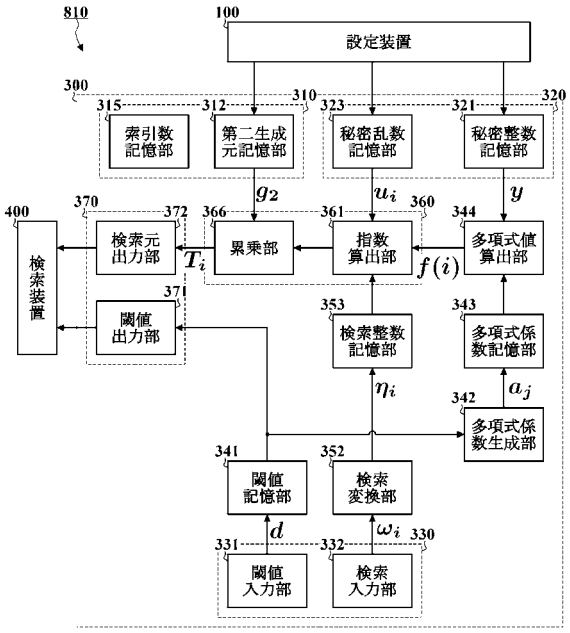
【図３】


810:復号装置
820:暗号化装置
830:サーバ装置
911
CPU(処理装置)
912:バス
913
ROM(記憶装置)
914
RAM(記憶装置)
901
CRT(表示装置)
902
K/B(入力装置)
903
915
マウス(入力装置)
通信装置
904
FDD(記憶装置)
905
CDD(記憶装置)
906
プリンタ(出力装置)
907
スキャナ(入力装置)
920
磁気ディスク装置(記憶装置)
921
OS
922
ウィンドウシステム
923
プログラム群
924
ファイル群

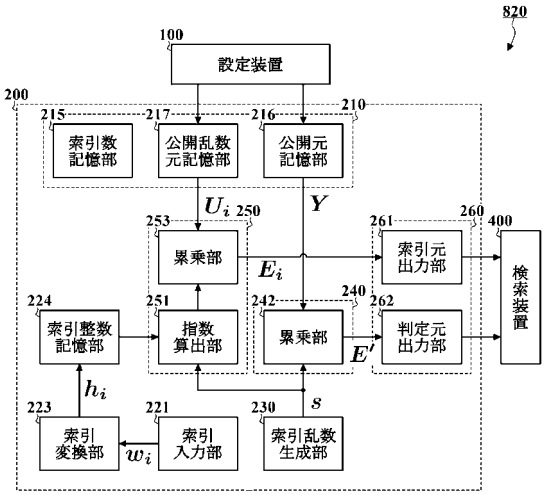
【図４】


100
810
110
112
111
g_2
第二生成元記憶部
第一生成元記憶部
121
ペアリング値算出部
g_1
113
第三生成元記憶部
115
索引数記憶部
g_3
130
132
秘密乱数生成部
u_i
142
公開乱数元算出部
140
g_3
131
秘密整数生成部
y
141
公開元算出部
Y
U_i
150
151
公開元出力部
152
公開乱数元出力部
300
検索暗号化装置

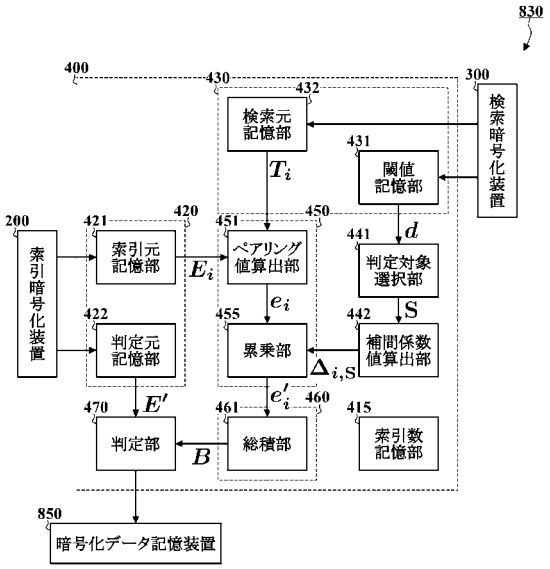
【図５】


810
100
設定装置
300
315
索引数記憶部
312
第二生成元記憶部
310
323
秘密乱数記憶部
321
秘密整数記憶部
320
g_2
u_i
y
400
検索装置
370
372
検索元出力部
T_i
366
累乗部
361
指数算出部
360
$f(i)$
344
多項式値算出部
371
閾値出力部
353
検索整数記憶部
343
多項式係数記憶部
η_i
a_j
342
多項式係数生成部
341
閾値記憶部
352
検索変換部
d
ω_i
330
331
閾値入力部
332
検索入力部

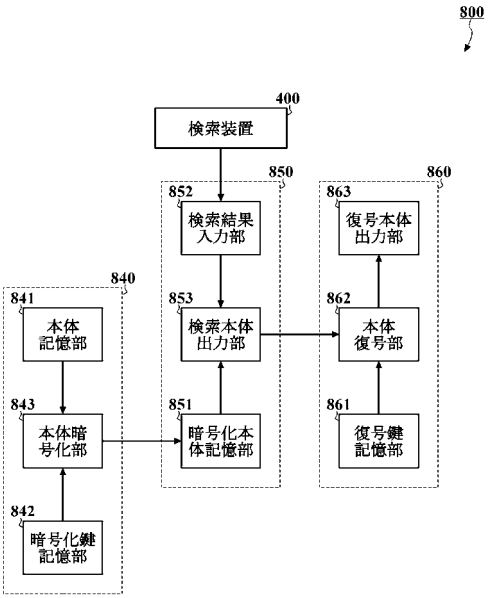
【図６】


820
100
設定装置
200
215
索引数記憶部
217
公開乱数元記憶部
216
公開元記憶部
210
U_i
Y
253
累乗部
250
E_i
261
索引元出力部
260
400
検索装置
224
索引整数記憶部
251
指数算出部
242
累乗部
240
E'
262
判定元出力部
h_i
s
223
索引変換部
w_i
221
索引入力部
230
索引乱数生成部

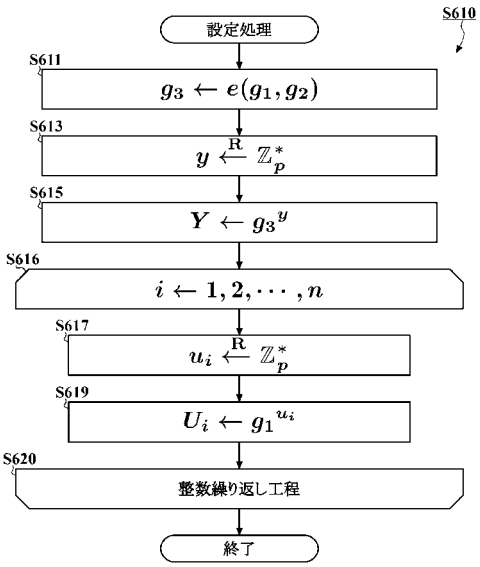
【図７】


830
400
430
432
300
検索暗号化装置
検索元記憶部
T_i
431
閾値記憶部
200
索引暗号化装置
421
索引元記憶部
420
451
ペアリング値算出部
450
441
判定対象選択部
d
E_i
e_i
S
422
判定元記憶部
455
累乗部
442
補間係数算出部
$\Delta_{i,S}$
e'_i
460
E'
470
461
415
判定部
総積部
索引数記憶部
B
850
暗号化データ記憶装置

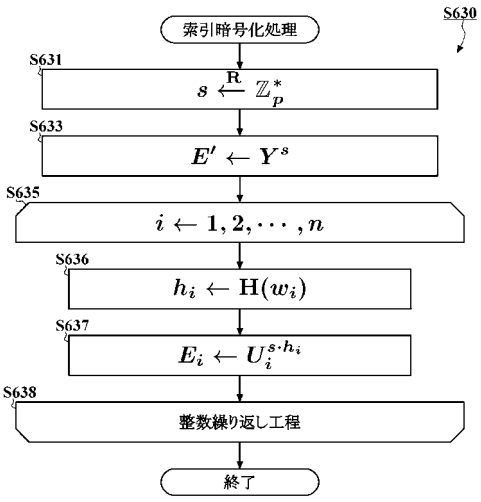
【図８】


800
400
検索装置
850
852
検索結果入力部
860
863
復号本体出力部
840
841
本体記憶部
853
検索本体出力部
862
本体復号部
843
本体暗号化部
851
暗号化本体記憶部
861
復号鍵記憶部
842
暗号化鍵記憶部

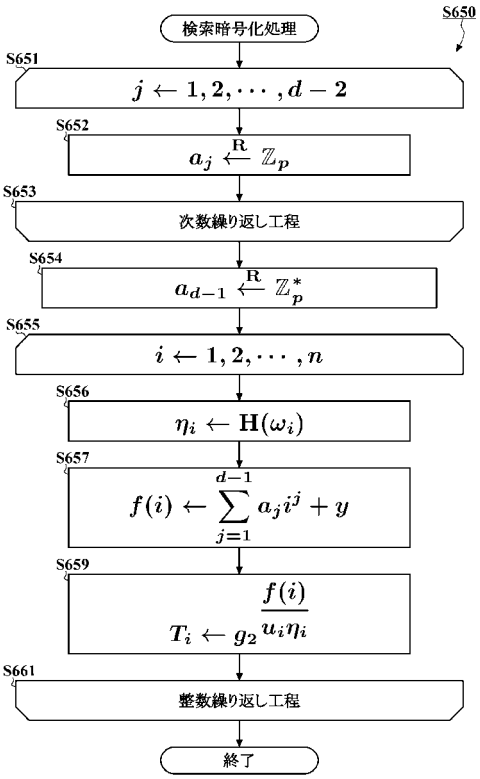
【図９】


S610
設定処理
S611
$g_3 \leftarrow e(g_1, g_2)$
S613
$y \xleftarrow{R} \mathbb{Z}_p^*$
S615
$Y \leftarrow {g_3}^y$
S616
$i \leftarrow 1, 2, \cdots, n$
S617
$u_i \xleftarrow{R} \mathbb{Z}_p^*$
S619
$U_i \leftarrow {g_1}^{u_i}$
S620
整数繰り返し工程
終了

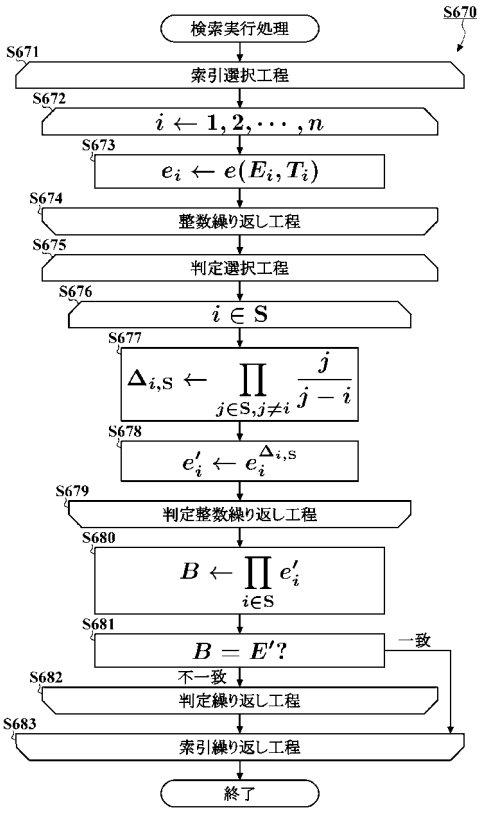
【図１０】


S630
索引暗号化処理
S631
$s \xleftarrow{R} \mathbb{Z}_p^*$
S633
$E' \leftarrow Y^s$
S635
$i \leftarrow 1, 2, \cdots, n$
S636
$h_i \leftarrow \mathrm{H}(w_i)$
S637
$E_i \leftarrow U_i^{s \cdot h_i}$
S638
整数繰り返し工程
終了

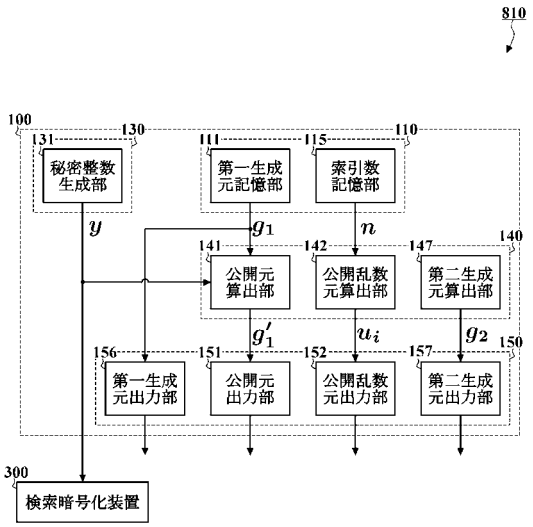
【図１１】



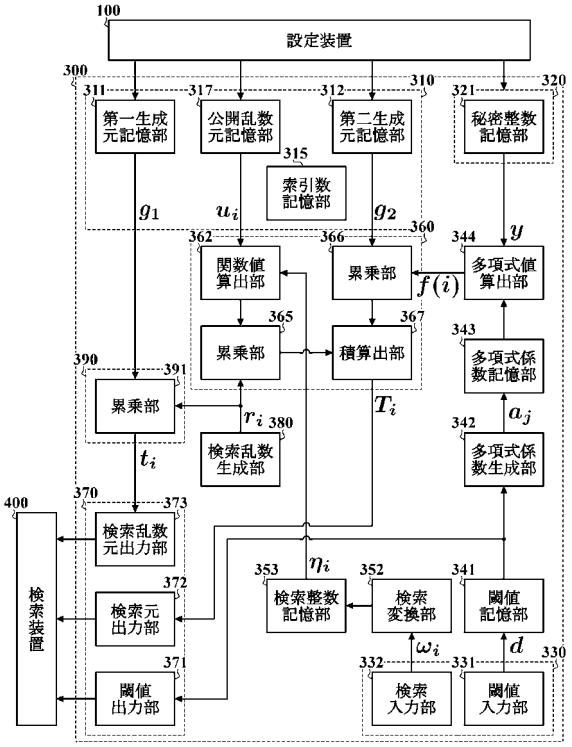
【図１２】



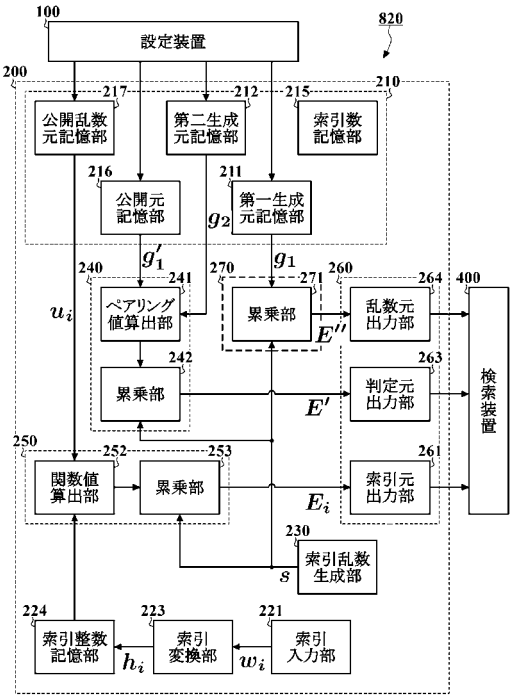
【図１３】



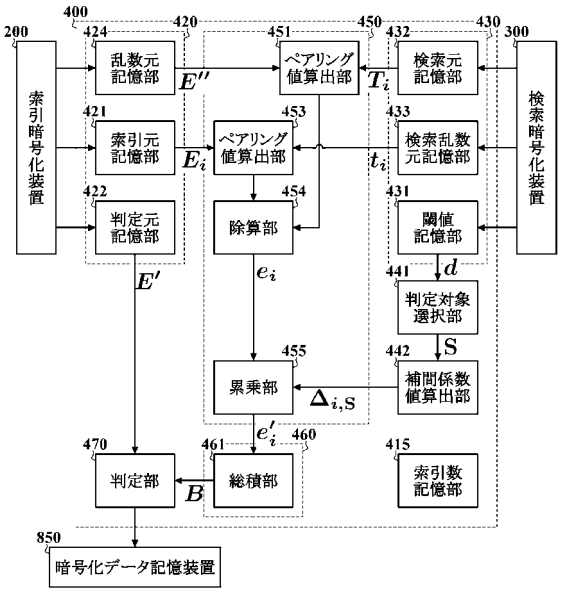
【図１４】



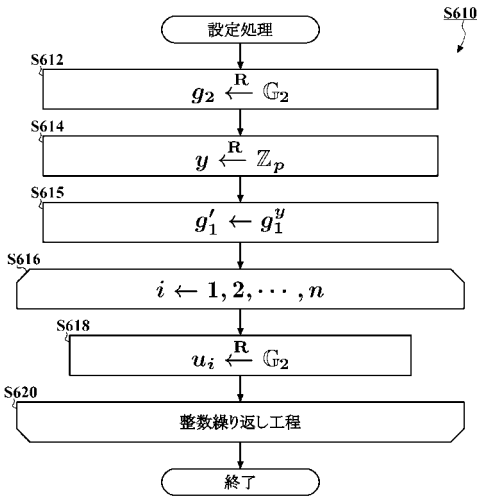
【図１５】



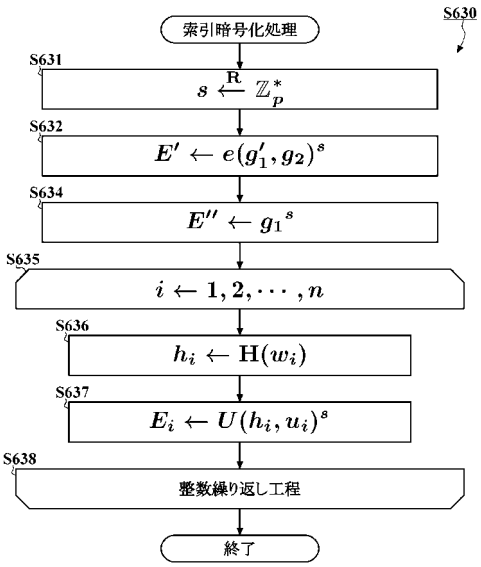
【図１６】



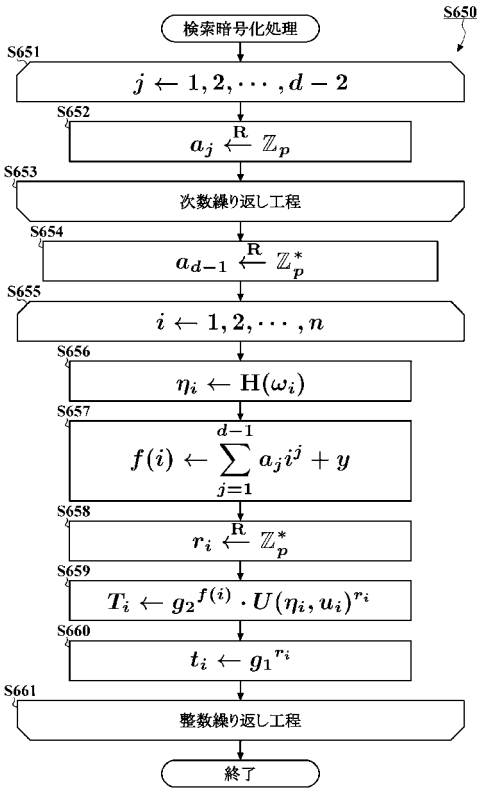
【図１７】



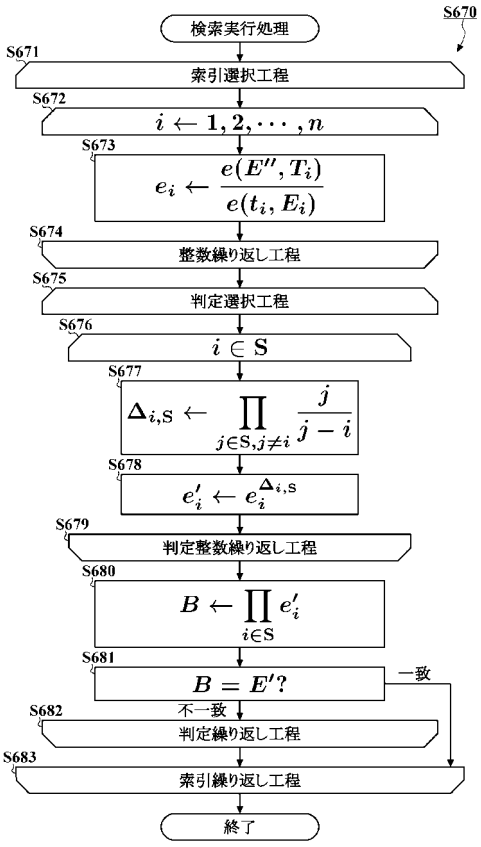
【図１８】



【図１９】


S650
検索暗号化処理
S651
$j \leftarrow 1, 2, \cdots, d-2$
S652
$a_j \xleftarrow{R} \mathbb{Z}_p$
S653
次数繰り返し工程
S654
$a_{d-1} \xleftarrow{R} \mathbb{Z}_p^*$
S655
$i \leftarrow 1, 2, \cdots, n$
S656
$\eta_i \leftarrow \mathrm{H}(\omega_i)$
S657
$f(i) \leftarrow \sum_{j=1}^{d-1} a_j i^j + y$
S658
$r_i \xleftarrow{R} \mathbb{Z}_p^*$
S659
$T_i \leftarrow {g_2}^{f(i)} \cdot U(\eta_i, u_i)^{r_i}$
S660
$t_i \leftarrow {g_1}^{r_i}$
S661
整数繰り返し工程
終了

【図２０】


S670
検索実行処理
S671
索引選択工程
S672
$i \leftarrow 1, 2, \cdots, n$
S673
$e_i \leftarrow \frac{e(E'', T_i)}{e(t_i, E_i)}$
S674
整数繰り返し工程
S675
判定選択工程
S676
$i \in \mathbf{S}$
S677
$\Delta_{i,\mathrm{S}} \leftarrow \prod_{j \in \mathrm{S}, j \neq i} \frac{j}{j-i}$
S678
$e_i' \leftarrow e_i^{\Delta_{i,\mathrm{S}}}$
S679
判定整数繰り返し工程
S680
$B \leftarrow \prod_{i \in \mathrm{S}} e_i'$
S681
$B = E'$?
一致
不一致
S682
判定繰り返し工程
S683
索引繰り返し工程
終了

フロントページの続き

(72)発明者　米田　健
東京都千代田区丸の内二丁目７番３号　三菱電機株式会社内
(72)発明者　辻　宏郷
東京都千代田区丸の内二丁目７番３号　三菱電機株式会社内
(72)発明者　太田　英憲
東京都千代田区丸の内二丁目７番３号　三菱電機株式会社内
(72)発明者　柴田　陽一
東京都千代田区丸の内二丁目７番３号　三菱電機株式会社内

審査官　金木　陽一

(56)参考文献　特開２００４－０２１６５４（ＪＰ，Ａ）
特開２０１０－０６１１０３（ＪＰ，Ａ）
Boneh, D., et al., Public Key Encryption with keyword Search, Advances in Cryptology - EUROCRYPT 2004, [online], ２００４年, pp. 506-522, [retrieved on 2012-11-20.] Retrieved from the Internet, ＵＲＬ, http://www.iacr.org/cryptodb/archive/2004/EUROCRYPT/1954/1954.pdf
Baek, J., et al., Public Key Encryption with Keyword Search Revisited, Cryptology ePrint Archive, [online], ２００５年, Report 2005/191, [retrieved on 2011-11-20]. Retrieved from the Internet, ＵＲＬ, http://eprint.iacr.org/2005/191
Hattori, M., et al., Public-key Encryption with Fuzzy Keyword Search, 2009年 暗号と情報セキュリティシンポジウム (SCIS2009) 予稿集CD-ROM, ２００９年　1月２０日, 3C1-4

(58)調査した分野(Int.Cl., ＤＢ名)
Ｇ０９Ｃ　　１／００
Ｇ０６Ｆ　２１／６２