(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2015-79228
(P2015-79228A)
(43)公開日　平成27年4月23日(2015.4.23)

| (51)Int.Cl. | | | F I | | | テーマコード（参考） |
|---|---|---|---|---|---|---|
| G09C | 1/00 | (2006.01) | G09C | 1/00 | 660D | 5J104 |
| H04L | 9/08 | (2006.01) | H04L | 9/00 | 601F | |

審査請求 未請求　請求項の数 19　ＯＬ　（全 26 頁）

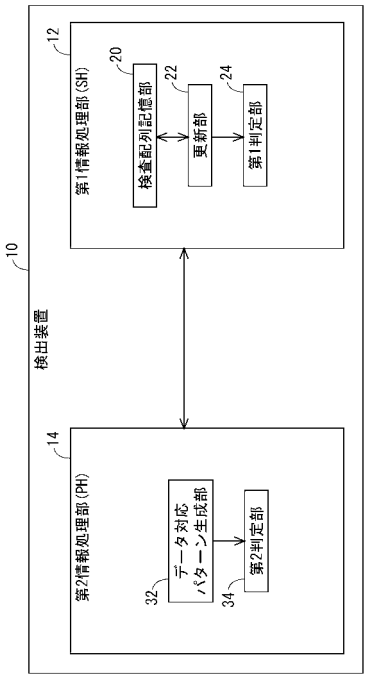
(21)出願番号　特願2013-217903 (P2013-217903)
(22)出願日　平成25年10月18日 (2013.10.18)

(71)出願人　504171134
国立大学法人　筑波大学
茨城県つくば市天王台一丁目１番１
(71)出願人　504173471
国立大学法人北海道大学
北海道札幌市北区北８条西５丁目
(74)代理人　110000877
龍華国際特許業務法人
(72)発明者　原田　弘毅
茨城県つくば市天王台一丁目１番１　国立大学法人筑波大学内
(72)発明者　佐久間　淳
茨城県つくば市天王台一丁目１番１　国立大学法人筑波大学内

最終頁に続く

(54)【発明の名称】検出装置、検出方法、コンピュータ、及び、プログラム

(57)【要約】
【課題】非決定性有限オートマトンを直接使用することができなかった。
【解決手段】検出装置は、入力データ列に予め定められた検出対象パターンが含まれるか否かを検出する検出装置であって、前記検出対象パターンの各データ位置に対応して、前記入力データ列において前記検出対象パターンにおける当該データ位置までのパターン部分を検出中か否かを示す検査配列を記憶する検査配列記憶部と、データの種類毎に、前記検出対象パターンの各データ位置が当該種類のデータか否かを示すデータ対応パターンを生成するデータ対応パターン生成部と、次の入力データに対応する前記データ対応パターンに基づいて、前記検査配列を更新する更新部と、前記検出対象パターンの末尾のデータ位置に対応する前記検査配列の要素に基づいて、前記入力データ列中に前記検出対象パターンが含まれたか否かを判定する判定部と、を備える。
【選択図】図１



【特許請求の範囲】
【請求項１】
入力データ列に予め定められた検出対象パターンが含まれるか否かを検出する検出装置であって、
前記検出対象パターンの各データ位置に対応して、前記入力データ列において前記検出対象パターンにおける当該データ位置までのパターン部分を検出中か否かを示す検査配列を記憶する検査配列記憶部と、
データの種類毎に、前記検出対象パターンの各データ位置が当該種類のデータか否かを示すデータ対応パターンを生成するデータ対応パターン生成部と、
次の入力データに対応する前記データ対応パターンに基づいて、前記検査配列を更新する更新部と、
前記検出対象パターンの末尾のデータ位置に対応する前記検査配列の要素に基づいて、前記入力データ列中に前記検出対象パターンが含まれたか否かを判定する判定部と、
を備える検出装置。
【請求項２】
前記更新部は、前記検査配列の各データ位置に対応する要素の値と、次の入力データに対応する前記データ対応パターンにおける次のデータ位置に対応する要素の値とに基づいて、前記検査配列の次のデータ位置に対応する要素の値を算出する請求項１に記載の検出装置。
【請求項３】
前記検査配列記憶部は、前記検出対象パターンの各データ位置に対応して、当該データ位置までのパターン部分を検出中である場合に０となる要素を有する前記検査配列を記憶し、
前記データ対応パターン生成部は、データの種類毎に、前記検出対象パターンの各データ位置が当該種類のデータである場合に０となる要素を有する前記データ対応パターンを生成し、
前記更新部は、前記検査配列の各データ位置に対応する要素の値、および、次の入力データに対応するデータ対応パターンにおける次のデータ位置に対応する要素の値が共に０であることに応じて、前記検査配列の次のデータ位置に対応する要素を０とする請求項２に記載の検出装置。
【請求項４】
前記更新部は、前記検査配列の各データ位置に対応する要素の値と、次の入力データに対応するデータ対応パターンにおける次のデータ位置に対応する要素の値とを加算して、前記検査配列の次のデータ位置に対応する要素の値とする請求項３に記載の検出装置。
【請求項５】
予め定められたデータ位置における値を複数回繰り返すことを許容する前記検出対象パターンについて、前記更新部は、前記検査配列の各データ位置に対応する要素の値と、前記検査配列の次のデータ位置に対応する要素の値と、次の入力データに対応するデータ対応パターンにおける次のデータ位置に対応する要素の値とに基づいて、前記検査配列の次のデータ位置に対応する要素の値を算出する請求項２から４のいずれか一項に記載の検出装置。
【請求項６】
前記検査配列記憶部および前記更新部を有し、前記入力データ列を管理する第１情報処理部と、
前記データ対応パターン生成部を有し、前記検出対象パターンを管理する第２情報処理部と、
を備え、
前記データ対応パターン生成部は、データの種類毎のデータ対応パターンを暗号化した暗号化データ対応パターンを前記第２情報処理部へと送信し、
前記検査配列記憶部は、前記検査配列を暗号化した暗号化検査配列を記憶し、

前記更新部は、次の入力データに対応する前記暗号化データ対応パターンに基づいて、前記暗号化検査配列を更新し、
前記判定部は、暗号化された前記検出対象パターンの末尾のデータ位置に対応する前記暗号化検査配列の要素に基づいて、前記入力データ列中に前記検出対象パターンが含まれたか否かを判定する
請求項１から５のいずれか一項に記載の検出装置。
【請求項７】
前記データ対応パターン生成部は、前記第２情報処理部の公開鍵である第２公開鍵を用いて加法準同型性暗号により前記データ対応パターンを暗号化し、
前記更新部は、前記第２公開鍵を用いて加法準同型性暗号により前記検査配列を暗号化して、前記暗号化検査配列の各データ位置に対応する要素の値、および、次の入力データに対応する前記暗号化データ対応パターンにおける次のデータ位置に対応する要素の値の、加法準同型性暗号における加法に基づき暗号化された前記検査配列を更新する
請求項６に記載の検出装置。
【請求項８】
前記第２情報処理部は、前記判定部を更に有し、
前記第１情報処理部は、前記検出対象パターンの末尾のデータ位置に対応する前記暗号化検査配列の要素を第１乱数によりべき乗した値に基づく検査用データを前記第２情報処理部へと送信し、
前記第２情報処理部の前記判定部は、前記検査用データを前記第２情報処理部の秘密鍵である第２秘密鍵により復号化して前記検査配列の要素を乱数によりべき乗した値を求め、当該値が０か否かに基づいて前記入力データ列中に前記検出対象パターンを検出したか否かを判定する請求項７に記載の検出装置。
【請求項９】
前記第１情報処理部は、前記判定部を更に有し、
前記第１情報処理部は、前記検出対象パターンの末尾のデータ位置に対応する前記暗号化検査配列の要素を第１乱数によりべき乗した値に基づく検査用データを前記第２情報処理部へと送信し、
前記第２情報処理部は、前記検査用データを前記第２情報処理部の秘密鍵である第２秘密鍵により復号化したデータに基づく値を前記第１情報処理部の公開鍵である第１公開鍵により暗号化したデータを第２乱数によりべき乗した値を求め、検査用応答データとして前記第１情報処理部へと返信し、
前記第１情報処理部の判定部は、前記検査用応答データを復号化したデータの値が０か否かに基づいて前記入力データ列に前記検出対象パターンを検出したか否かを判定する
請求項７に記載の検出装置。
【請求項１０】
前記第１情報処理部は、前記検出対象パターンの末尾のデータ位置に対応する前記暗号化検査配列の要素を前記第１乱数によりべき乗した値と第３乱数を前記第２公開鍵により暗号化した値とを加法準同型性暗号における加法により加えた前記検査用データと、前記第３乱数を前記第１公開鍵により暗号化した乱数交換データとを前記第２情報処理部へと送信し、
前記第２情報処理部は、前記検査用データを前記第２秘密鍵により復号化し前記第１公開鍵により暗号化した値に前記乱数交換データを加えたデータを前記第２乱数によりべき乗して前記検査用応答データとして返信する
請求項９に記載の検出装置。
【請求項１１】
前記検査配列記憶部は、前記検出対象パターンの各データ位置に対応して、前記検出対象パターンにおける当該データ位置までのパターン部分を検出中である場合に０となる要素を有する前記検査配列を暗号化した前記暗号化検査配列を記憶し、
前記検出対象パターンは、予め定められたデータ位置における値を複数回繰り返すこと

を許容するものであり、
前記更新部は、次の入力データに対応する前記暗号化データ対応パターン及び前記暗号化検査配列に基づいて、パターン部分の一致を各データ位置から次のデータ位置へと伝搬させるための暗号化伝搬配列を生成して、前記暗号化伝搬配列に基づく第１配列および前記暗号化検査配列に基づく第２配列を前記第２情報処理部に送信し、
前記第２情報処理部は、前記第１配列および前記第２配列に基づいて、前記予め定められたデータ位置以外のデータ位置においては前記暗号化伝搬配列の対応する要素を前記更新部に取得させ、前記予め定められたデータ位置においては前記暗号化検査配列および前記暗号化伝搬配列の対応する要素の積を前記更新部に取得させるための返信用配列を生成して前記第１情報処理部へと返信する更新補助部を更に備え、
前記更新部は、前記返信用配列に基づいて前記検査配列を更新する
請求項７から１０のいずれか一項に記載の検出装置。
【請求項１２】
前記第１情報処理部の前記更新部は、
前記暗号化伝搬配列の各データおよび第４乱数を前記第２公開鍵により暗号化した値同士を加法準同型性暗号の加法により加えた各要素を有する前記第１配列と、
前記暗号化検査配列の各データおよび第５乱数を前記第２公開鍵により暗号化した値同士を加法準同型性暗号の加法により加えた各要素を有する前記第２配列と、
前記暗号化検査配列の各データを前記第４乱数によりべき乗した値と、前記第４乱数および前記第５乱数の積を前記第２公開鍵により暗号化した値と、前記暗号化伝搬配列を前記第５乱数および第６乱数の積によりべき乗した値と、第７乱数を前記第２公開鍵により暗号化した値とを、加法準同型性暗号の加法により加えた各要素を有する第３配列と、
を前記第２情報処理部に送信し、
前記第２情報処理部の前記更新補助部は、
前記予め定められたデータ位置においては、前記第１配列の要素を復号化した値および前記第２配列の要素を復号化した値の積を前記第２公開鍵により暗号化した値を要素とし、前記予め定められたデータ位置以外のデータ位置においては前記第３配列の要素を前記第２公開鍵により暗号化し直した値を要素とする前記返信用配列と、
前記予め定められたデータ位置においては前記第２公開鍵により０を暗号化した値を要素とし、前記予め定められたデータ位置以外においては前記第２公開鍵により１を暗号化した値を要素とする第４配列と、
を前記第１情報処理部に返信する
請求項１１に記載の検出装置。
【請求項１３】
前記更新部は、前記返信用配列の各要素と、前記暗号化検査配列を前記第４乱数のマイナス値によりべき乗した値と、前記第４乱数および前記第５乱数を前記第２公開鍵により暗号化した値の逆元と、前記暗号化伝搬配列を前記第５乱数のマイナス値によりべき乗した値と、前記第４配列を前記第７乱数のマイナス値によりべき乗した値とを、加法準同型性暗号の加法により加えた各要素により前記検査配列を更新する
請求項１２に記載の検出装置。
【請求項１４】
当該検出装置は、前記入力データ列として商品の広告履歴データおよび商品の購買履歴データの少なくとも一方を含む履歴データ列を入力し、
前記履歴データ列中に前記検出対象パターンが検出されたことに応じて、広告を発行すべきことを示すトリガ情報を出力する出力部を更に備える
請求項１から１３のいずれか一項に記載の検出装置。
【請求項１５】
当該検出装置は、前記入力データ列として遺伝子配列を入力し、
前記遺伝子配列中に前記検出対象パターンが検出されたか否かを出力する出力部を更に備える

請求項１から１３のいずれか一項に記載の検出装置。
【請求項１６】
入力データ列に予め定められた検出対象パターンが含まれるか否かを検出する検出方法であって、
前記検出対象パターンの各データ位置に対応して、前記入力データ列において前記検出対象パターンにおける当該データ位置までのパターン部分を検出中か否かを示す検査配列を記憶する検査配列記憶段階と、
データの種類毎に、前記検出対象パターンの各データ位置が当該種類のデータか否かを示すデータ対応パターンを生成するデータ対応パターン生成段階と、
次の入力データに対応する前記データ対応パターンに基づいて、前記検査配列を更新する更新段階と、
前記検出対象パターンの末尾のデータ位置に対応する前記検査配列の要素に基づいて、前記入力データ列中に前記検出対象パターンが含まれたか否かを判定する判定段階と、
を備える検出方法。
【請求項１７】
入力データ列に予め定められた検出対象パターンが含まれるか否かを検出する検出装置としてコンピュータを機能させるプログラムであって、
前記検出対象パターンの各データ位置に対応して、前記入力データ列において前記検出対象パターンにおける当該データ位置までのパターン部分を検出中か否かを示す検査配列を記憶する検査配列記憶部と、
データの種類毎に、前記検出対象パターンの各データ位置が当該種類のデータか否かを示すデータ対応パターンを生成するデータ対応パターン生成部と、
次の入力データに対応する前記データ対応パターンに基づいて、前記検査配列を更新する更新部と、
前記検出対象パターンの末尾のデータ位置に対応する前記検査配列の要素に基づいて、前記入力データ列中に前記検出対象パターンが含まれたか否かを判定する判定部と、
して機能させるプログラム。
【請求項１８】
請求項６から１３のいずれか１項に記載の前記第１情報処理部または前記第２情報処理部として機能するコンピュータ。
【請求項１９】
請求項６から１３のいずれか１項に記載の前記第１情報処理部または前記第２情報処理部としてコンピュータを機能させるプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、検出装置、検出方法、コンピュータ、及び、プログラムに関する。
【背景技術】
【０００２】
近年の個人情報保護の必要性の高まりにより、保護が必要なデータを開示せずに入力データ列中に特定の検出対象パターンが含まれているか否かを検出する秘密パターン照合の重要性が高まっている（非特許文献１～３）。
［非特許文献１］ J. R. Troncoso-Pastoriza, S. Katzenbeisser, and M. Celik. Privacy preserving error resilient dna searching through oblivious automata. In Proc. Comput. Commun. Security (CCS'07), pages 519{528. ACM, 2007.
［非特許文献２］ K. B. Frikken. Practical private dna string searching and matching through efficient oblivious automata evaluation. In Data and Applications Security XXIII, pages 81-94. Springer, 2009.
［非特許文献３］ 渡邊裕治, 立石孝彰. 通信回数を低減した紛失オートマトン計算. In 暗号と情報セキュリティシンポジウム(SCIS2012) 予稿集, 2012 年.

【発明の概要】
【発明が解決しようとする課題】
【０００３】
上記非特許文献１～３においては、いずれも決定性有限オートマトン（ＤＦＡ：Ｄｅｔｅｒｍｉｎｉｓｔｉｃ　Ｆｉｎｉｔｅ　Ａｕｔｏｍａｔｏｎ）を想定しており、非決定性有限オートマトン（ＮＦＡ：Ｎｏｎ－ｄｅｔｅｒｍｉｎｉｓｔｉｃ　Ｆｉｎｉｔｅ　Ａｕｔｏｍａｔｏｎ）を直接使用することができなかった。
【課題を解決するための手段】
【０００４】
本発明の第１の態様においては、入力データ列に予め定められた検出対象パターンが含まれるか否かを検出する検出装置であって、前記検出対象パターンの各データ位置に対応して、前記入力データ列において前記検出対象パターンにおける当該データ位置までのパターン部分を検出中か否かを示す検査配列を記憶する検査配列記憶部と、データの種類毎に、前記検出対象パターンの各データ位置が当該種類のデータか否かを示すデータ対応パターンを生成するデータ対応パターン生成部と、次の入力データに対応する前記データ対応パターンに基づいて、前記検査配列を更新する更新部と、前記検出対象パターンの末尾のデータ位置に対応する前記検査配列の要素に基づいて、前記入力データ列中に前記検出対象パターンが含まれたか否かを判定する判定部と、を備える検出装置を提供する。
【０００５】
本発明の第２の態様においては、入力データ列に予め定められた検出対象パターンが含まれるか否かを検出する検出方法であって、前記検出対象パターンの各データ位置に対応して、前記入力データ列において前記検出対象パターンにおける当該データ位置までのパターン部分を検出中か否かを示す検査配列を記憶する検査配列記憶段階と、データの種類毎に、前記検出対象パターンの各データ位置が当該種類のデータか否かを示すデータ対応パターンを生成するデータ対応パターン生成段階と、次の入力データに対応する前記データ対応パターンに基づいて、前記検査配列を更新する更新段階と、前記検出対象パターンの末尾のデータ位置に対応する前記検査配列の要素に基づいて、前記入力データ列中に前記検出対象パターンが含まれたか否かを判定する判定段階と、を備える検出方法を提供する。
【０００６】
本発明の第３の態様においては、入力データ列に予め定められた検出対象パターンが含まれるか否かを検出する検出装置としてコンピュータを機能させるプログラムであって、前記検出対象パターンの各データ位置に対応して、前記入力データ列において前記検出対象パターンにおける当該データ位置までのパターン部分を検出中か否かを示す検査配列を記憶する検査配列記憶部と、データの種類毎に、前記検出対象パターンの各データ位置が当該種類のデータか否かを示すデータ対応パターンを生成するデータ対応パターン生成部と、次の入力データに対応する前記データ対応パターンに基づいて、前記検査配列を更新する更新部と、前記検出対象パターンの末尾のデータ位置に対応する前記検査配列の要素に基づいて、前記入力データ列中に前記検出対象パターンが含まれたか否かを判定する判定部と、して機能させるプログラムを提供する。
【０００７】
なお、上記の発明の概要は、本発明の特徴の全てを列挙したものではない。また、これらの特徴群のサブコンビネーションもまた、発明となりうる。
【図面の簡単な説明】
【０００８】
【図１】検出装置１０の全体構成図である。
【図２】検出方法の全体の流れを説明するフローチャートである。
【図３】図２に示す検出方法で生成されるデータ対応パターン$M_{T\,i}$を説明する図である。
【図４】ステップＳｓ２０８の状態配列$S_i$の更新処理のフローチャートである。

【図５】更新処理によって更新される状態配列Ｓ$_{i}$を説明する図及び表である。
【図６】ステップＳｐ１１０及びＳｓ２１０の照合結果の判定処理のフローチャートである。
【図７】ステップＳｐ１１０及びＳｓ２１０の照合結果の判定処理のフローチャートである。
【図８】状態配列の更新処理を変更した検出装置１０の全体構成図である。
【図９】セルフループの出力を説明する図である。
【図１０】変更した状態配列の更新処理のフローチャートである。
【図１１】上述した実施形態の効果を説明する表である。
【図１２】本実施形態に係るコンピュータ１９００のハードウェア構成の一例を示す。
【発明を実施するための形態】
【０００９】
以下、発明の実施の形態を通じて本発明を説明するが、以下の実施形態は特許請求の範囲にかかる発明を限定するものではない。また、実施形態の中で説明されている特徴の組み合わせの全てが発明の解決手段に必須であるとは限らない。
【００１０】
図１は、検出装置１０の全体構成図である。検出装置１０は、入力データ列Ｔ中に予め定められた検出対象パターンＰが含まれるか否かを検出する。本実施形態においては、検出装置１０は、入力データ列Ｔを取得・保持・管理する第１情報処理部１２（ＳＨ：Ｓｔｒｉｎｇ　Ｈｏｌｄｅｒとも示す。）と、検出対象パターンＰを保持・管理する第２情報処理部１４（ＰＨ：Ｐａｔｔｅｒｎ　Ｈｏｌｄｅｒとも示す。）とを備え、第１情報処理部１２および第２情報処理部１４の間で入力データ列Ｔおよび検査対象パターンＰを互いに秘匿しつつ、入力データ列Ｔ中に検出対象パターンＰを検出する秘密パターン照合を実現する。ここで、第１情報処理部１２および第２情報処理部１４は、一例としてプログラムを実行可能なコンピュータまたは情報処理装置であってよく、有線または無線ネットワークを介して互いに接続される。
【００１１】
尚、以下においては、第１情報処理部１２および第２情報処理部１４間で入力データ列Ｔおよび検出対象パターンＰを秘匿する秘密パターン照合を中心に示すが、第１情報処理部１２および第２情報処理部１４間で秘密を持たないパターン照合については以下における暗号処理を除くことで実現できる。
【００１２】
第１情報処理部１２は、複数のデータを含む入力データ列Ｔの一例として、複数の文字Ｔｉを含む文字列Ｔを管理する。ここで、第１情報処理部１２は、オフラインで文字列Ｔ全体を取得してパターン照合に供してもよく、オンラインで文字列Ｔの各文字を順次取得し、順次パターン照合に供してもよい。以下においては、第１情報処理部１２が、文字列Ｔとして、１文字目からｎ文字までの文字Ｔ１からＴｎを順次入力していくオンライン処理を中心に示す。第１情報処理部１２は、検査配列記憶部２０と、更新部２２と、第１判定部２４とを有する。
【００１３】
検査配列記憶部２０は、検出対象パターンＰの各データ位置（文字位置）に対応して、文字列Ｔにおいて検出対象パターンＰにおける当該データ位置までのパターン部分を検出中か否かを示す検査配列の一例である状態配列を記憶する。ここで本実施形態においては、検出対象パターンＰのパターン長をｍとする。検査配列記憶部２０は、ｉ－１番目の文字Ｔ$_{i-1}$（１≦ｉ≦ｎ）までの照合を終えた状態において、検出対象パターンＰの各データ位置ｊ（０≦ｊ≦ｍ）に対応して、当該データ位置ｊまでのパターン部分（すなわちＰ［１］～Ｐ［ｊ］の部分）を検出中である場合に検出中を示す値０となる配列要素Ｓ$_{i-1}$［ｊ］を有する状態配列Ｓ$_{i-1}$を記憶する。すなわち、状態配列Ｓ$_{i-1}$の配列要素Ｓ$_{i-1}$［ｊ］は、文字列Ｔのｉ－１文字目の文字Ｔ$_{i-1}$までを読み込んだ状態において、検出対象パターンＰのｊ番目のパターン要素までの一致を検出しているかどうかを

表す遷移状態を示す。本実施形態においては、$S_{i-1}[j]=0$ならばactive（すなわちｊ番目のパターン要素までの一致を検出していること）、$S_{i-1}[j]\neq 0$ならばinactive（すなわちｊ番目のパターン要素までの一致を検出していないこと）とする。

【００１４】

尚、検査配列記憶部２０は、秘密パターン照合を実現するために、第２情報処理部１４の第２公開鍵$pk^{PH}$により状態配列$S_i$を暗号化し、暗号化状態配列$S_{Ei}$として記憶する。

【００１５】

更新部２２は、後述する第２情報処理部１４のデータ対応パターン生成部３２が生成した、文字列Ｔの次の文字$T_i$に対応するデータ対応パターン$M_{Ti}$に基づいて、状態配列$S_{i-1}$を更新し、更新された状態配列$S_i$とする。例えば、更新部２２は、状態配列$S_{i-1}$の各データ位置ｊ－１に対応する要素の一例である配列要素$S_{i-1}[j-1]$の値と、文字列Ｔの次の文字Ｔｉに対応するデータ対応パターン$M_{Ti}$における次のデータ位置ｊに対応する要素の一例であるパターン要素$M_{Ti}[j]$とに基づいて、状態配列$S_i$の次のデータ位置ｊに対応する配列要素$S_i[j]$を算出する。これにより、更新部２２は、ｉ－１番目の文字$T_{i-1}$まで入力された状態で検出対象パターンＰのｊ－１番目のパターン部分までの一致を検出しており（$S_{i-1}[j-1]$が検出中を示す値であり）、かつ、ｉ番目の文字$T_i$に対応するデータ対応パターン$M_{Ti}$のｊ番目の要素$M_{Ti}[j]$が検査対象パターンＰのｊ番目のパターン要素に文字$T_i$が含まれることを示す場合に、状態配列Ｓｉ［ｊ］をｊ番目のパターン部分までの一致を検出していることを示す値に更新することができる。なお、本実施形態に係る更新部２２は、上記更新処理を暗号化された状態配列である暗号化状態配列$S_{Ei}$に対して行うが、この処理については後述する。

【００１６】

第１判定部２４は、第２情報処理部１４の第２判定部３４と協働して、検出対象パターンＰの末尾のデータ位置ｍに対応する状態配列$S_i[m]$に基づいて、文字列Ｔ中に検査対象パターンＰが含まれているか否かを判定する。本実施形態に係る第１判定部２４は、状態配列$S_i[m]$を暗号化した暗号化状態配列$S_{Ei}[m]$に基づく判定を行う。尚、ｍの一例は、検出対象パターンＰの文字数である。

【００１７】

第２情報処理部１４は、検出対象パターンＰを管理する。第２情報処理部１４は、データ対応パターン生成部３２と、第２判定部３４を有する。

【００１８】

データ対応パターン生成部３２は、データの種類の一例である文字Ｔｉの種類毎に、検出対象パターンＰの各データ位置ｊが当該種類のデータか否かを示すデータ対応パターン$M_{Ti}$を生成する。ここで、文字Ｔｉの種類は、文字列Ｔを構成する文字集合Σの要素であり、例えばａ、ｂ等のアルファベット、数字、日本語文字、および、データ要素の値等であってよい。例えば、データ対応パターン生成部３２は、データの文字Ｔｉの種類毎に、検出対象パターンＰの各データ位置ｊが当該種類の文字である場合に文字が検出対象パターンＰの対応するパターン要素に含まれることを示す値０となる要素$M_{Ti}[j]$を有するデータ対応パターン$M_{Ti}$を生成する。

【００１９】

データ対応パターン生成部３２は、文字Ｔｉの種類毎のデータ対応パターン$M_{Ti}$を、第２情報処理部１４の第２公開鍵$pk^{PH}$により暗号化して、暗号化データ対応パターン$M_{ETi}$を第１情報処理部１２へと送信する。

【００２０】

第２判定部３４は、第１情報処理部１２の第１判定部２４と協働して、検出対象パターンＰの末尾のデータ位置ｍに対応する状態配列$S_i$の配列要素$S_i[m]$に基づいて、文字列Ｔ中に検出対象パターンＰが含まれたか否かを判定する。本実施形態に係る第２判定部３４は、状態配列$S_i[m]$を暗号化した暗号化状態配列$S_{Ei}[m]$に基づく判定を

行う。

【００２１】

次に、検査方法について説明する。

【００２２】

各検査方法における暗号化は、加法準同型性公開鍵暗号による。加法準同型性公開鍵暗号の一例は、Paillier暗号である。Paillier暗号は、"P. Paillier. Public-key cryptosystems based on composite degree residuosity classes. In Advances in cryptology EUROCRYPT'99, pages 223-238. Springer, 1999."に記載されている。加法準同型性公開鍵暗号は、同一の公開鍵で暗号化された暗号文同士の積が対応する平文同士の和の暗号文となり、式（１）の関係を満たす。暗号については、Ｅｎｃを用いる。従って、例えば、平文ｔを暗号化して暗号ｃにする場合、ｃ＝Ｅｎｃ（ｔ）と表記する。白丸○は、暗号同士の積の演算子とする。ｔ１、ｔ２は平文である。ｒ１、ｒ２は、乱数である。ｒ１、ｒ２は、暗号の安全性を保つため暗号化毎に変更することが好ましい。尚、説明の簡略化のため乱数ｒ１、ｒ２は省略して表記する。また、復号については、Ｄｅｃを用いる。従って、例えば、暗号ｃを復号して平文ｔにする場合、ｔ＝Ｄｅｃ（ｃ）と表記する。

【数１】

$$\left.\begin{aligned} &Encpk(t1;r1)\circ Encpk(t2;r2)=Encpk(t1+t2;r1+r2)\\ &Encpk(t1;r1)^{t2}=Encpk(t1t2;r1t2)\end{aligned}\right\}(1)$$

【００２３】

また、次に示す式（２）により、同一の平文を持つ異なる暗号文を生成する再暗号化もできる。

【数２】

$$C=Encpk(t)\circ Encpk(0) \qquad (2)$$

【００２４】

図２は、検出方法の全体の流れを説明するフローチャートである。図２に示す検出方法は、第１情報処理部１２及び第２情報処理部１４がプログラムを読み込むことによって実行される。図２に示す検査方法は、入力された検査対象パターンＰからそれを受理する非決定性有限オートマトンを構築して文字列Ｔ上でその遷移を模倣することで照合を実行する。本実施形態では、更に、ビット並列パターン照合方法を準同型性暗号上の秘密計算へを実施可能とすべく、配列と加法のみを用いる。尚、Ｓｈｉｆｔ－ＯＲ法を配列上で実行するアルゴリズムを配列Ｓｈｉｆｔ－ＯＲ法とする。図３は、図２に示す検出方法で生成されるデータ対応パターン$Ｍ_{Ｔｉ}$を説明する図である。本実施形態では、文字列Ｔが第１情報処理部１２に入力されている。また、検出対象パターンＰが第２情報処理部１４に入力されている。実施形態では、検出対象パターンＰ=ａｂａｂｂとして、文字列Ｔ＝ａｂａｂａｂｂとする。

【００２５】

図２に示す検査方法では、第２情報処理部１４において、データ対応パターン生成部３２が、第２情報処理部１４の公開鍵及び秘密鍵として第２秘密鍵$ｓｋ^{ＰＨ}$及び第２公開鍵$ｐｋ^{ＰＨ}$を生成する（Ｓｐ１０２）。次に、データ対応パターン生成部３２は、公開鍵$ｐｋ^{ＰＨ}$を第１情報処理部１２へと送信する（Ｓｐ１０４）。データ対応パターン生成部３２は、式（３）によって、データ対応パターン$Ｍ_{Ｔｉ}$を生成する。データ対応パターン生

成部３２は、検出対象パターンＰ＝ａｂａｂｂの文字種"ａ"についてのデータ対応パターンＭａを生成する場合、式（３）に基づいて、検出対象パターンＰの１番目及び３番目はａなので、Ｍａ［１］＝Ｍａ［３］＝０となる。一方、検出対象パターンＰの２番目、４番目及び５番目はｂなので、Ｍａ［２］＝Ｍａ［４］＝Ｍａ［５］＝１となる。これにより、データ対応パターン生成部３２は、式（３）によって、図３に示す検出対象パターンＰ＝ａｂａｂｂのデータ対応パターン$M_{Ti}$を生成する。

【数３】

$$M_{\sigma}[j]=\begin{cases}0 & (P[j]=\sigma)\\ 1 & (otherwise)\end{cases} \qquad (3)$$

【００２６】

データ対応パターン生成部３２は、文字Ｔｉの種類毎にデータ対応パターン$M_{Ti}$の各パターン要素$M_{ETi}$［ｊ］を暗号化して、暗号化パターン要素$M_{ETi}$［ｊ］を生成する（Ｓｐ１０６）。例えば、データ対応パターン生成部３２は、生成した第２公開鍵$pk^{PH}$及び第２公開鍵$sk^{PH}$のうち、当該第２公開鍵$pk^{PH}$を用いて加法準同型性暗号によりデータ対応パターン$M_{Ti}$を暗号化してもよい。データ対応パターン生成部３２は、暗号化パターン要素$M_{ETi}$［ｊ］を含む暗号化データ対応パターン$M_{ETi}$を第１情報処理部１２へと送信する（Ｓｐ１０８）。

【００２７】

第１情報処理部１２では、検査配列記憶部２０が、第２情報処理部１４から送信された公開鍵$pk^{PH}$、及び、暗号化されたデータ対応パターン$M_{Ti}$を受信する（Ｓｓ２０２、Ｓｓ２０４）。

【００２８】

第１情報処理部１２では、更新部２２は、式（４）によって、状態配列$S_i$の初期値$S_0$が暗号化された暗号化状態配列$S_{E0}$を生成して、検査配列記憶部２０に記憶させる（Ｓｓ２０６）。

【数４】

$$\left.\begin{aligned}S_{E0}[0]&=Encpk^{PH}(0)\\ S_{E0}[j]&=Encpk^{PH}(1)\end{aligned}\right\} \quad (4)$$

$$j=1,2,\cdots,m$$

【００２９】

次に、更新部２２は、後述する暗号化状態配列$S_{Ei}$の更新処理によって、状態配列$S_i$が暗号化された暗号化状態配列$S_{Ei}$の各配列要素$S_{Ei}$［ｊ］を生成して、順次、暗号化状態配列$S_{Ei}$を更新する（Ｓｓ２０８）。第１判定部２４は、後述する照合結果の判定処理を実行する（Ｓｓ２１０）。この後、更新部２２及び第１判定部２４は、それぞれステップＳｓ２０８及びＳｓ２１０をそれぞれｎ回繰り返す。尚、ｎの一例は、文字列Ｔの文字数である。

【００３０】

第２情報処理部１４では、第２判定部３４が、第１判定部２４の照合結果の判定処理と連動して、後述する照合結果の判定処理（Ｓｐ１１０）をｎ回繰り返す。尚、第２判定部３４が、検査対象パターンＰが文字列Ｔを含むか否かを判定する場合、照合結果$\Gamma^{PH}$を

ｎ回出力して、当該判定を実行する。

【００３１】

図４は、ステップＳｓ２０８の状態配列$S_i$の更新処理のフローチャートである。更新処理のフローチャートに先立って、第１情報処理部１２に文字列Ｔ、暗号化データ対応パターン$M_{ETi}$、暗号化状態配列$S_{Ei-1}$が入力されている。図５は、更新処理によって更新される状態配列$S_i$を説明する図及び表である。図５の上図は、検出対象パターンＰ＝ａｂａｂｂを受け付けた非決定性有限オートマトンによる状態遷移の図である。図５の上図における各丸の中の数字は、データ位置ｊを示す。図５の下図において、最上位の行は、データ位置ｊを示す。各行は、文字列Ｔのｉ文字目の文字を読み込んだ場合に生成される状態配列$S_i$を示す。状態配列$S_i$の初期値である状態配列$S_0$の各要素は、$S_0[0]=0$と、及び、$S_0[j]=1$、$j\in\{1、2、・・・、m\}$、$S_i[0]=0$に初期設定されている。各セルは、配列要素$S_i[j]$を示す。配列要素$S_i[j]$は、値が０の場合、activeであって、値が０でない場合、inactiveである。尚、本実施形態では、更新された状態配列$S_i$が暗号化された状態配列$S_{Ei}$を生成する。

【００３２】

図４に示すように、状態配列$S_{Ei}$の更新処理では、更新部２２は、ｊ＝０の配列要素$S_i[0]$の値として予め定められた０を、第２公開鍵$pk^{PH}$を用いて加法準同型性暗号により暗号化して、暗号化状態配列$S_{Ei}$の暗号化配列要素$S_{Ei}[0]$を生成する（Ｓｓ２２０）。換言すれば、更新部２２は、ｊ＝０の配列要素$S_i[0]$の値を、ｉの値に関わらず０とし、文字Ｔｉが入力される度にデータ対応パターンＭの先頭からのマッチングを開始させる。

【００３３】

次に、更新部２２は、暗号化配列要素$S_{Ei}[j]$を更新する（Ｓｓ２２２）。ここで、更新部２２は、暗号化されていない状態で示すと、配列要素$S_i[j]$を式（５）によって算出する。具体的には、更新部２２は、状態配列$S_{i-1}$の各データ位置ｊ－１に対応する配列要素$S_{i-1}[j-1]$の値、および、文字列Ｔの次の文字Ｔｉに対応するデータ対応パターン$M_{Ti}$における次のデータ位置ｊに対応するパターン要素$M_{Ti}[j]$の値が共に０であることに応じて、状態配列$S_i$の次のデータ位置ｊに対応する配列要素$S_i[j]$を０とする。例えば、更新部２２は、状態配列$S_{i-1}$の各データ位置ｊ－１に対応する配列要素$S_{i-1}[j-1]$の値と、文字列Ｔの次の文字Ｔｉに対応するデータ対応パターン$M_{Ti}$における次のデータ位置ｊに対応するパターン要素$M_{Ti}[j]$の値とを加算して、状態配列$S_i$の次のデータ位置ｊに対応する配列要素$S_i[j]$とする。

【００３４】

例えば、ｉ＝６、ｊ＝１の配列要素$S_6[1]$の値は、配列要素$S_5[0]$の値が０であって、図３に示すように$M_{T6}[1]=Mb[1]$の値が１なので、それぞれを足して１となる。ｉ＝７、ｊ＝５の配列要素$S_7[5]$の値は、配列要素$S_6[4]$の値が０であって、$M_{T6}[5]=Mb[5]$の値が０なので、それぞれを足して０となる。

【数５】

$$S_i[j]=S_{i-1}[j-1]+M_{Ti}[j] \quad (5)$$

【００３５】

本実施形態において、更新部２２は、パターン要素$M_{Ti}[j]$ではなく、暗号化された暗号化パターン要素$M_{ETi}[j]$を第２情報処理部１４から受信している。従って、更新部２２は、次の文字列Ｔに対応する暗号化データ対応パターン$M_{ETi}$に基づいて、加法準同型性の性質より自明の下記の式（６）によって、暗号化状態配列$S_{Ei}$の配列要素$S_{Ei}[j]$を算出して更新する。具体的には、更新部２２は、１つ前の暗号化状態配列$S_{Ei-1}$の各データ位置ｊ－１に対応する配列要素$S_{Ei-1}[j-1]$の値、およ

び、次の文字列Ｔに対応する暗号化データ対応パターン$M_{ETi}$における次のデータ位置ｊに対応する暗号化パターン要素$M_{ETi}$［ｊ］の値との積、即ち、加法準同型性暗号における加法に基づき暗号化状態配列$S_{Ei}$を算出して更新する。

【数６】

$$S_{Ei}[j]=S_{Ei-1}[j-1]\circ M_{ETi}[j] \quad (6)$$

【００３６】

更新部２２は、ステップＳｓ２２２を、ｍ回繰り返すまで続ける。ここでいうｍは、検出対象パターンＰ＝ａｂａｂｂに含まれる文字数であって、本実施形態では５個である。上述した図２に示すように、更新部２２は、更新処理のステップＳｓ２０８をｎ回繰り返す。これにより、更新部２２は、図５に示すｎ個の状態配列$S_i$が暗号化された暗号化状態配列$S_{Ei}$を生成することになる。これにより、状態配列の更新処理が終了する。

【００３７】

図６は、ステップＳｐ１１０及びＳｓ２１０の照合結果の判定処理のフローチャートである。照合結果の判定処理のフローチャートに先立って、第１情報処理部１２に第２公開鍵$pk^{PH}$が入力され、第２情報処理部１４には第２秘密鍵$sk^{PH}$が入力されている。尚、図６に示す照合結果の判定処理は、第２情報処理部１４が照合結果を判定する場合である。尚、データ対応パターン$M_{Ti}$が暗号化されている場合、第２判定部３４は、暗号化検出対象パターン$P_E$の末尾のデータ位置ｍに対応する暗号化状態配列$S_{Ei}$の暗号化配列要素$S_{Ei}$［ｍ］に基づいて、文字列Ｔ中に検出対象パターンＰが含まれたか否かを判定する。以下、判定処理について詳細に説明する。

【００３８】

図６に示すように、照合結果の判定処理では、第１情報処理部１２の第１判定部２４が第１乱数Ｖ［ｉ］及び第３乱数Ｗ［ｉ］を生成する（Ｓｓ２３０）。尚、乱数は、ｉ毎、即ち、文字列Ｔの文字毎に生成される。第１判定部２４が、式（７）によって、第１乱数Ｖ［ｉ］によりべき乗した暗号化配列要素$S_{Ei}$［ｍ］が、公開鍵$pk^{PH}$によって暗号化された第３乱数Ｗ［ｉ］によって、ランダム化された検査用データ$Z_E$［ｉ］を算出する（Ｓｓ２３２）。尚、暗号化配列要素$S_{Ei}$［ｍ］は、検出対象パターンＰの末尾のデータ位置ｍに対応する暗号化状態配列$S_E$の要素である。

【数７】

$$Z_E[i]=S_{Ei}[m]^{V[i]}\circ Encpk^{PH}(W[i])^{-1} \quad (7)$$

【００３９】

第１判定部２４は、検査用データ$Z_E$［ｉ］を第２情報処理部１４へと送信する（Ｓｓ２３４）。

【００４０】

第２情報処理部１４では、第２判定部３４が、検査用データ$Z_E$［ｉ］を受信する（Ｓｐ１２０）。第２判定部３４は、受信した検査用データ$Z_E$［ｉ］を公開鍵$pk^{PH}$によって復号して、検査用データＺ［ｉ］を生成する（Ｓｐ１２２）。

【００４１】

第１判定部２４は、第３乱数Ｗ［ｉ］を第２情報処理部１４へと送信する。（Ｓｓ２３６）。

【００４２】

第２判定部３４は、第３乱数Ｗ［ｉ］を受信する（Ｓｐ１２４）。第２判定部３４は、検査用データ$Z_E$［ｉ］を第２情報処理部１４の秘密鍵である第２秘密鍵$sk^{PH}$により復号化する。第２判定部３４は、式（８）に基づいて、復号した検査用データＺ［ｉ］と

、受信した第３乱数Ｗ［ｉ］との和によって、末尾のデータ位置ｍの状態配列Ｓ$_{i}$の配列要素Ｓ$_{i}$［ｍ］を第１乱数Ｖ［ｉ］によりべき乗した値である照合結果Γ$^{PH}$［ｉ］として算出する（Ｓｐ１２６）。尚、第３乱数Ｗ［ｉ］は省略してもよい。

【数８】

$$\Gamma^{PH}[i]=Z[i]+W[i]=Si[m]^{V[i]} \quad (8)$$

【００４３】

第２判定部３４は、照合結果Γ$^{PH}$［ｉ］の値が０か否かに基づいて文字列Ｔ中に検出対象パターンＰを検出したか否かを判定する。（Ｓｐ１２８）。換言すれば、第２判定部３４は、暗号化検出対象パターンＰ$_{E}$の末尾のデータ位置ｍに対応する暗号化状態配列Ｓ$_{Ei}$の暗号化配列要素Ｓ$_{Ei}$［ｍ］に基づいて、文字列Ｔ中に検出対象パターンＰが含まれたか否かを判定する。具体的には、第２判定部３４は、照合結果Γ$^{PH}$［ｉ］が"０"の場合、検出対象パターンＰが文字列Ｔに含まれていると判定して、それ以外は検出対象パターンＰが文字列Ｔに含まれていないと判定する。例えば、第２判定部３４は、図５の例では、ｉ＝７において、Ｓｉ［５］＝０（active）を検出して、文字列Ｔの７文字目が、合致した検査対象パターンＰの末尾であると判定する。これにより、照合結果の判定処理が終了する。尚、第１判定部２４を有する第１情報処理部１２は、何らの結果も得ることはない。換言すれば、第２情報処理部１４は、第１情報処理部１２に何らの情報を与えることなく、検出対象パターンＰが文字列Ｔに含まれているか否かを検出できる。

【００４４】

図７は、ステップＳｐ１１０及びＳｓ２１０の照合結果の判定処理のフローチャートである。照合結果の判定処理のフローチャートに先立って、第１情報処理部１２に第２公開鍵ｐｋ$^{PH}$が入力され、第２情報処理部１４には第２秘密鍵ｓｋ$^{PH}$が入力されている。尚、図７に示す照合結果の判定処理は、第１情報処理部１２の第１判定部２４が照合結果を判定する場合である。図７の処理において、点線で囲まれたステップが図６と異なる。図６と同じ処理には、同じステップ番号を付与して説明を省略する。

【００４５】

本実施形態においては、第２判定部３４は、検出対象パターンＰの末尾のデータ位置ｍに対応する状態配列Ｓ$_{i}$の配列要素Ｓ$_{i}$［ｍ］に基づいて、文字列Ｔ中に検出対象パターンＰが含まれたか否かを判定する。

【００４６】

第１情報処理部１２の第１判定部２４は、検出対象パターンＰ］の末尾のデータ位置ｍに対応する暗号化状態配列Ｓ$_{Ei}$の配列要素Ｓ$_{Ei}$［ｍ］を第１乱数Ｖ［ｉ］によりべき乗した値に基づく検査用データＺ$_{E}$［ｉ］を第２情報処理部１４へと送信する。

【００４７】

例えば、第１判定部２４は、検出対象パターンＰの末尾のデータ位置ｍに対応する暗号化状態配列Ｓ$_{Ei}$の配列要素Ｓ$_{Ei}$［ｍ］を第１乱数Ｖ［ｉ］によりべき乗した値と第３乱数Ｗ［ｉ］を第２公開鍵ｐｋ$^{PH}$により暗号化した値とを加法準同型性暗号における加法により加えた検査用データＺ［ｉ］と、第３乱数Ｗ［ｉ］を第１公開鍵ｐｋ$^{SH}$により暗号化した乱数交換データＲＤとを第２情報処理部１４へと送信してもよい。

【００４８】

第１判定部２４は、後述する第２情報処理部１４から返信された検査用応答データＺ'$_{E}$［ｉ］を復号化したデータの値が０か否かに基づいて文字列Ｔに検出対象パターンＰを検出したか否かを判定する。

【００４９】

第２情報処理部１４の第２判定部３４は、検査用データＺ$_{E}$［ｉ］を第２情報処理部１４の秘密鍵である第２秘密鍵ｓｋ$^{PH}$により復号化したデータに基づく値を第１情報処理部１２の公開鍵である第１公開鍵ｐｋ$^{SH}$により暗号化したデータを第２乱数Ｗ'［ｉ］

によりべき乗した値を求め、検査用応答データ$Z'_E[i]$として第１情報処理部１２へと返信する。例えば、第１判定部２４は、検査用データＺ［ｉ］を第２秘密鍵$sk^{PH}$により復号化し第１公開鍵$pk^{SH}$により暗号化した値に乱数交換データＲＤを加えたデータを第２乱数Ｗ'［ｉ］によりべき乗して検査用応答データ$Z'_E[i]$として返信する。

【００５０】

図７に示すように、第１情報処理部１２では、第１判定部２４が、秘密鍵$sk^{SH}$、及び、公開鍵$pk^{SH}$を生成する（Ｓｓ２４０）。次に、第１判定部２４は、式（９）によって、第３乱数Ｗ［ｉ］を暗号化した第３乱数$W_E[i]$を算出する（Ｓｓ２４２）。

【数９】

$$W_E[i]=Encpk^{SH}(W[i]) \quad (9)$$

【００５１】

第１判定部２４は、第１公開鍵$pk^{SH}$、及び、第３乱数$W_E[i]$を第２情報処理部１４へ送信する（Ｓｓ２４４）。

【００５２】

第２情報処理部１４では、第２判定部３４が、第１公開鍵$pk^{SH}$、及び、第３乱数$W_E[i]$を受信する（Ｓｐ１３０）。第２判定部３４は、新たに第２乱数$W'_E[i]$を生成する（Ｓｐ１３２）。第２判定部３４は、式（１０）によって、照合結果を秘密にしつつシェアするために暗号化検査用データ$Z_E[i]$をランダム化した検査用応答データ$Z'_E[i]$を算出する（Ｓｐ１３４）。

【数１０】

$$Z'_E[i]=(Z_E[i]\circ W[i])^{W'[i]} \quad (10)$$

【００５３】

第２判定部３４は、第２乱数$W'_E[i]$及び検査用応答データ$Z'_E[i]$を第１情報処理部１２へと送信する（Ｓｐ１３６）。

【００５４】

第１判定部２４は、第２判定部３４が送信した第２乱数$W'_E[i]$及び検査用応答データ$Z'_E[i]$を受信する（Ｓｓ２４６）。次に、第１判定部２４は、式（１１）によって、照合結果$\Gamma^{SH}[i]$を算出する（Ｓｓ２４８）。

【数１１】

$$\Gamma^{SH}[i]=Decsk^{SH}(Z'_E[i])=Si[m]^{V[i]W'[i]} \quad (11)$$

【００５５】

第１判定部２４は、照合結果$\Gamma^{SH}[i]$の結果で、パターンＰが文字列Ｔに含まれているか否かを判定する。具体的には、第１判定部２４は、照合結果$\Gamma^{SH}[i]$が"０"の場合、検出対象パターンＰが文字列Ｔに含まれていると判定して、それ以外は検出対象パターンＰが文字列Ｔに含まれていないと判定する。これにより、照合結果の判定処理が終了する。尚、第２判定部３４を有する第２情報処理部１４は、何らの結果も得ることはない。換言すれば、第１情報処理部１２は、第２情報処理部１４に何らの情報を与えることなく、検出対象パターンＰが文字列Ｔに含まれているか否かを検出できる。

【００５６】

次に、上述した実施形態の状態配列の更新処理を変更した形態について説明する。図８

は、状態配列の更新処理を変更した検出装置１０の全体構成図である。図９は、セルフループの出力を説明する図である。本実施形態は、セルフループの遷移処理を含む場合に有効である。

【００５７】

図８に示す検査配列記憶部２０は、検出対象パターンＰの各データ位置に対応して、検出対象パターンＰにおける当該データ位置までのパターン部分を検出中である場合に０となる要素を有する状態配列$S_i$を暗号化した暗号化状態配列$S_{Ei}$を記憶する。

【００５８】

予め定められたデータ位置Ｌにおける値を複数回繰り返すセルフループを許容する検出対象パターンＰの場合、例えば、更新部２２は、状態配列$S_{i-1}$の各データ位置ｊに対応する配列要素$S_{i-1}[j]$と、状態配列$S_{i-1}$の次のデータ位置ｊに対応する配列要素$S_i[j]$と、次の文字列Ｔに対応するデータ対応パターン$M_{Ti}$における次のデータ位置ｊ＋１に対応するパターン要素$M_{Ti}[j]$とに基づいて、状態配列$S_i$の次のデータ位置ｊ＋１に対応する配列要素$S_i[j+1]$を算出する。尚、セルフループとは、現在の状態への遷移である。セルフループによって、パターンから生成される非決定性有限オートマトンでは無現ギャップが実現される。

【００５９】

セルフループによる遷移は、状態配列$S_i$を図９に示す関係に基づいて、更新する。尚、図９の出力は、上述の式（５）により文字の遷移を実行した後、次の式（１２）の処理によって得られる。尚、式（１２）は、ループのある状態については、文字の遷移以前の状態との積をとることでセルフループ遷移を実現して、ループのない状態に関しては何も実行しない。

【数１２】

$$S_i[j]=\begin{cases} S_i[j]\cdot S_{i-1}[j] & (j\in L) \\ S_i[j] & (\text{otherwise}) \end{cases} \qquad (12)$$

【００６０】

更新部２２は、式（５）及び文字列Ｔの次に入力される文字に対応する暗号化データ対応パターン$M_{Ei-1}$及び暗号化状態配列$S_{Ei-1}$に基づいて、パターン部分の一致を各データ位置ｊ－１から次のデータ位置ｊへと伝搬させるための暗号化伝搬配列$S_{Ei}$を生成して、暗号化伝搬配列$S_{Ei}$に基づく第１配列$S'_{Ei}$の要素$S'_{Ei}[j]$および暗号化状態配列$S_{Ei-1}$に基づく第２配列$S'_{Ei-1}$の要素$S'_{Ei-1}[j]$を第２情報処理部１４に送信する。

【００６１】

第２情報処理部１４は、更新補助部３６を更に備える。更新補助部３６は、第１配列$S'_{Ei}$および第２配列$S'_{Ei-1}$に基づいて、予め定められたセルフループのデータ位置Ｌ以外のデータ位置においては暗号化伝搬配列$S_{Ei}$の対応する要素$S_{Ei}[j]$を更新部２２に取得させ、予め定められたデータ位置Ｌにおいては暗号化状態配列$S_{Ei-1}$および暗号化伝搬配列$S_{Ei}$の対応する要素$S_{Ei}[j]$の積を更新部２２に取得させるための返信用配列$S^*_{Ei}$を生成して第１情報処理部１２へと返信する。

【００６２】

更新部２２は、返信用配列$S^*_{Ei}$に基づいて状態配列$S_{Ei}$を更新する。

【００６３】

第１情報処理部の更新部２２は、暗号化伝搬配列$S_{Ei}$の各データおよび第４乱数$R_i[j]$を第２公開鍵$pk^{PH}$により暗号化した値同士を加法準同型性暗号の加法により加えた各要素$S'_{Ei}[j]$を有する第１配列$S'_{Ei}$と、暗号化状態配列$S_{Ei}$の各デー

タおよび第５乱数$Q_i[j]$を第２公開鍵$pk^{PH}$により暗号化した値同士を加法準同型性暗号の加法により加えた各要素$S'_{Ei-1}[j]$を有する第２配列$S'_{Ei-1}$と、暗号化状態配列$S_{Ei}$の各データを第４乱数$R_i[j]$によりべき乗した値と、第４乱数$R_i[j]$および第５乱数$Q_i[j]$の積を第２公開鍵$pk^{PH}$により暗号化した値と、暗号化伝搬配列$S_{Ei}$を第５乱数$Q_i[j]$および第６乱数$K_i[j]$の積によりべき乗した値と、第７乱数$U_i[j]$を第２公開鍵$pk^{PH}$により暗号化した値とを、加法準同型性暗号の加法により加えた各要素を有する第３配列$\Delta_{Ei}$とを第２情報処理部１４に送信する。

【００６４】

第２情報処理部の更新補助部３６は、予め定められたデータ位置Ｌにおいては、第１配列$S'_{Ei}$の要素$S'_{Ei}[j]$を復号化した値および第２配列$S'_{Ei-1}$の要素$S'_{Ei-1}[j]$を復号化した値の積を第２公開鍵$pk^{PH}$により暗号化した値を要素とし、予め定められたデータ位置Ｌ以外のデータ位置においては第３配列$\Delta_{Ei}$の要素$\Delta_{Ei}[j]$を第２公開鍵$pk^{PH}$により暗号化し直した値を要素とする返信用配列$S^*_{Ei}$と、予め定められたデータ位置Ｌにおいては第２公開鍵$pk^{PH}$により０を暗号化した値の要素を暗号化零$E_{Ei}[j]$とし、予め定められたデータ位置Ｌ以外においては第２公開鍵$pk^{PH}$により１を暗号化した値を要素$E_{Ei}[j]$とする第４配列$E_{Ei}$とを第１情報処理部１２に返信する。

【００６５】

更新部２２は、返信用配列$S^*_{Ei}$の各要素$S^*_{Ei}[j]$と、暗号化状態配列$S_{Ei}$を第４乱数$R_i[j]$のマイナス値によりべき乗した値と、第４乱数$R_i[j]$および第５乱数$Q_i[j]$を第２公開鍵$pk^{PH}$により暗号化した値の逆元と、暗号化伝搬配列$S_{Ei}$を第５乱数$Q_i[j]$のマイナス値によりべき乗した値と、第４配列$E_{Ei}$を第７乱数$U_i[j]$のマイナス値によりべき乗した値とを、加法準同型性暗号の加法により加えた各要素により状態配列$S_i$を更新する。

【００６６】

図１０は、変更した状態配列の更新処理のフローチャートである。状態配列の更新処理の当該フローチャートでは、第１情報処理部１２に文字列Ｔ、暗号化データ対応パターン$M_{ETi}$、暗号化状態配列$S_{i-1}$、及び、第２公開鍵$pk^{PH}$が入力されている。第２情報処理部１４には、セルフループのデータ位置Ｌ、第２秘密鍵$sk^{PH}$、第２公開鍵$pk^{PH}$が入力されている。本フローチャートは、無限長ギャップを含むパターンへの拡張を行った拡張配列Ｓｈｉｆｔ－ＯＲ法である。尚、図１０に示す処理は、図４に示す処理の後に継続して実行される。また、Ｌはセルフループを行う予め定められた処理の番号であって、$L \subset \{1、\cdots、m\}$である。

【００６７】

図４に示すステップＳｓ２２０からＳｓ２２２が実行される。次に、更新部２２は、乱数$K_i[j]$、$R[j]$、$Q_i[j]$、$U_i[j]$を生成する（Ｓｓ２６０）。尚、更新部２２は、一例として、１からＮまでの整数から乱数$K_i[j]$、$R[j]$、$Q_i[j]$、$U_i[j]$を抽出する。更新部２２は、式（１３）及び生成した乱数から、第１配列$S'_{Ei}$の要素$S'_{Ei}[j]$、第２配列$S'_{Ei-1}$の要素$S'_{Ei-1}[j]$、及び、第３配列$\Delta_{Ei}$の要素$\Delta_{Ei}[j]$を算出する（Ｓｓ２６２）。

【数１３】

$$\left.\begin{aligned} S'_{Ei}[j]&=S_{Ei}[j]\circ Encpk^{PH}(R_i[j])\\ S'_{Ei-1}[j]&=S_{Ei-1}[j]\circ Encpk^{PH}(Q_i[j])\\ \Delta_{Ei}[j]&=S_{Ei-1}[j]^{Ri[j]}\circ Encpk^{PH}(Q_i[j]\cdot R_i[j])\\ &\quad\circ S_{Ei}[j]^{Ki[j]\cdot Qi[j]}\circ Encpk^{PH}(U_i[j]) \end{aligned}\right\} \quad (13)$$

【００６８】
更新部２２は、算出した第１配列Ｓ'$_{Ei}$、第２配列Ｓ'$_{Ei-1}$、及び、第３配列Δ$_{Ei}$を第２情報処理部１４へと送信する（Ｓｓ２６４）。更新部２２は、ステップＳｓ２６０からＳ２６４をｍ回繰り返す。
【００６９】
第２情報処理部１４では、更新補助部３６が、第１情報処理部１２から送信された第１配列Ｓ'$_{Ei}$、第２配列Ｓ'$_{Ei}$、及び、第３配列Δ$_{Ei}$を受信する（Ｓｐ１４０）。
【００７０】
次に、更新補助部３６は、今回の処理対象のデータ位置ｊがセルフループのデータ位置Ｌに含まれるか否かを判断する（Ｓｐ１４４）。更新補助部３６は、データ位置ｊがデータ位置Ｌに含まれると判断すると（Ｓｐ１４４：Ｙｅｓ）、式（１４）によって、返信用配列Ｓ＊$_{Ei}$の各要素Ｓ＊$_{Ei}$［ｊ］を算出するとともに、式（１５）によって、暗号化零Ｅ$_{Ei}$［ｊ］を算出する（Ｓｐ１４６）。
【数１４】

$$\begin{aligned} S^*_{Ei}[j]&=Encpk^{PH}(Decsk^{PH}(S'_{Ei}[j])\cdot Decsk^{PH}(S'_{Ei-1}[j]))\\ &=Encpk^{PH}((S_i[j]+R_i[j])\cdot(S_{i-1}[j]+Q_i[j]))\\ &=Encpk^{PH}((S_i[j]\cdot S_{i-1}[j]+Q_i[j]\cdot S_i[j]+\\ &\quad+R_i[j]\cdot S_{i-1}[j]+R_i[j]\cdot Q_i[j]) \end{aligned} \quad (14)$$

【数１５】

$$E_{Ei}[j]=Encpk^{PH}(0) \quad (15)$$

【００７１】
一方、更新補助部３６は、データ位置ｊがデータ位置Ｌに含まれないと判断すると（Ｓｐ１４４：Ｎｏ）、式（１６）によって、返信用配列Ｓ＊$_{Ei}$の各要素Ｓ＊$_{Ei}$［ｊ］を算出するとともに、式（１７）によって、暗号化零Ｅ$_{Ei}$［ｊ］を算出する（Ｓｐ１４８）。ここで、本実施形態では、第７乱数Ｕを用いることによって、Ｓ$_i$［ｊ］＝０の場合であっても、式（１６）の関係においても、式（１８）に示すように第７乱数Ｕ$_i$［ｊ］が残るので、Ｓ$_i$［ｊ］＝０であることが第２情報処理部１４にはわからない。

【数１６】

$$S^{*}_{Ei}[j]= \Delta_{Ei}[j] \circ Encpk^{PH}(0) \qquad (16)$$

【数１７】

$$E_{Ei}[j]= Encpk^{PH}(1) \qquad (17)$$

【数１８】

$$(S_{Ei-1}[j]+Q_i[j](K_i[j]-1))S_{Ei}[j]-U_i[j]= 0 \qquad (18)$$

【００７２】
更新補助部３６は、算出した返信用配列Ｓ＊Ｅｉの各要素Ｓ＊Ｅｉ［ｊ］、及び、暗号化零ＥＥｉ［ｊ］を第１情報処理部１２へ送信する（Ｓｐ１５０）。更新補助部３６は、ステップＳｐ１４４からＳｐ１５０をｍ回繰り返す。

【００７３】
更新部２２は、第２情報処理部１４から送信された返信用配列Ｓ＊Ｅｉ［ｊ］、及び、暗号化零ＥＥｉ［ｊ］を受信する（Ｓｓ２６６）。更新部２２は、式（１８）によって、状態配列ＳＥｉの各要素ＳＥｉ［ｊ］を算出して更新する（Ｓｓ２６８）。

【数１９】

$$S_{Ei}[j]= S^{*}_{Ei}[j] \circ S_{Ei-1}[j]^{-Ri[j]} \circ Encpk^{PH}(Q_i[j] \cdot R_i[j])^{-1} \circ S_{Ei}[j]^{-Qi[j]} \circ E_{Ei}[j]^{-Ui[j]} \qquad (19)$$

【００７４】
図１１は、上述した実施形態の効果を説明する表である。表中のＳＰＭ１の列は、図４に示す実施形態の性能を示す。表中のＳＰＭ２の列は、図１０に示す実施形態の性能を示す。

【００７５】
上述の非特許文献は、事前処理では文字列の文字数ｎに依存するとともに、更新処理では文字列が含みうる文字種（いわゆるアルファベット等）の数Σに依存する。これにより、各非特許文献は、それぞれの処理における計算量が増加する。一方、図１１に示すように、本実施形態は、事前処理では文字列の文字数ｎに依存せず、更新処理では文字列が含みうる文字種の数Σに依存しないので、それぞれの処理における計算量を低減できる。特に、本実施形態は、文字数ｎ及び文字種の数Σが大きくなる日本語テキスト及び購買ログ等において、より計算量の増加を各非特許文献に比べて、抑制することができる。

【００７６】
次に、上述した実施形態を具体的に適用する例を示す。

【００７７】
例えば、上述した実施形態は、購買履歴の検出に適用してもよい。この場合、検出装置１０は、入力データ列として商品の広告履歴データおよび商品の購買履歴データの少なくとも一方を含む履歴データ列が入力される。検出装置１０は、出力部を更に備えることが好ましい。出力部は、履歴データ列中に検出対象パターンＰが検出されたことに応じて、広告を発行すべきことを示すトリガ情報を出力する。

【００７８】
また、例えば、上述した実施形態は、遺伝子配列の検出に適用してもよい。この場合、検出装置１０は、入力データ列として遺伝子配列が入力される。検出装置１０は、出力部を更に備えることが好ましい。出力部は、遺伝子配列中に検出対象パターンが検出されたか否かを出力する。
【００７９】
上述したように、検出装置１０は、非決定性有限オートマトンを直接評価することにより、非決定性有限オートマトンを決定性有限オートマトンに変換した場合に、文字列Ｔの文字数及び検出対象パターンの文字数の増加に伴う状態数の増加を低減して、通信量及び計算量を低減できる。更に、検出装置１０は、文字列Ｔ及び検査対象パターンＰを、加法準同型性を満たす暗号により暗号化することによって、文字列Ｔ及び検査対象パターンＰを相手に知られることなく、上述の効果を実現できる。
【００８０】
上述した実施形態は、一例であって、各実施形態における構成、値、データの種類等は適宜変更してよい。また、各実施形態を適切に組み合わせてもよい。
【００８１】
例えば、検出対象パターンＰのｈ番目の要素Ｐ［ｈ］が複数の文字を含む集合である文字種Ａである場合、各文字σ∈Σに対して、マスク配列Ｍσ［ｈ］を式（１９）によって生成してもよい。
【数２０】

$$M_\sigma[h]=\begin{cases}0 & (P[h]=\sigma\in A)\\ 1 & (\text{otherwise})\end{cases} \qquad (20)$$

【００８２】
上述の実施形態では、入力データ列を文字列としたが、入力データ列は文字列以外のデータ列であってもよい。
【００８３】
以上、本発明を実施の形態を用いて説明したが、本発明の技術的範囲は上記実施の形態に記載の範囲には限定されない。上記実施の形態に、多様な変更または改良を加えることが可能であることが当業者に明らかである。その様な変更または改良を加えた形態も本発明の技術的範囲に含まれ得ることが、特許請求の範囲の記載から明らかである。
【００８４】
特許請求の範囲、明細書、および図面中において示した装置、システム、プログラム、および方法における動作、手順、ステップ、および段階等の各処理の実行順序は、特段「より前に」、「先立って」等と明示しておらず、また、前の処理の出力を後の処理で用いるのでない限り、任意の順序で実現しうることに留意すべきである。特許請求の範囲、明細書、および図面中の動作フローに関して、便宜上「まず、」、「次に、」等を用いて説明したとしても、この順で実施することが必須であることを意味するものではない。
【００８５】
図１２は、本実施形態に係るコンピュータ１９００のハードウェア構成の一例を示す。本実施形態に係るコンピュータ１９００は、第１情報処理部１２及び第２情報処理部１４の一例である。コンピュータ１９００は、ホスト・コントローラ２０８２により相互に接続されるＣＰＵ２０００、ＲＡＭ２０２０、グラフィック・コントローラ２０７５、及び表示部２０８０を有するＣＰＵ周辺部と、入出力コントローラ２０８４によりホスト・コントローラ２０８２に接続される通信インターフェイス２０３０、及び、ハードディスクドライブ２０４０を有する入出力部と、入出力コントローラ２０８４に接続されるＲＯＭ

２０１０、メモリドライブ２０５０及び入出力チップ２０７０を有するレガシー入出力部とを備える。

【００８６】

ホスト・コントローラ２０８２は、ＲＡＭ２０２０と、高い転送レートでＲＡＭ２０２０をアクセスするＣＰＵ２０００及びグラフィック・コントローラ２０７５とを接続する。ＣＰＵ２０００は、ＲＯＭ２０１０及びＲＡＭ２０２０に格納されたプログラムに基づいて動作し、各部の制御を行う。グラフィック・コントローラ２０７５は、ＣＰＵ２０００等がＲＡＭ２０２０内に設けたフレーム・バッファ上に生成する画像データを取得し、表示部２０８０上に表示させる。これに代えて、グラフィック・コントローラ２０７５は、ＣＰＵ２０００等が生成する画像データを格納するフレーム・バッファを、内部に含んでもよい。

【００８７】

入出力コントローラ２０８４は、ホスト・コントローラ２０８２と、比較的高速な入出力装置である通信インターフェイス２０３０、ハードディスクドライブ２０４０を接続する。通信インターフェイス２０３０は、ネットワークを介して他の装置と通信する。ハードディスクドライブ２０４０は、コンピュータ１９００内のＣＰＵ２０００が使用する表示プログラム等のプログラム及びデータを格納する。

【００８８】

また、入出力コントローラ２０８４には、ＲＯＭ２０１０と、メモリドライブ２０５０、及び入出力チップ２０７０の比較的低速な入出力装置とが接続される。ＲＯＭ２０１０は、コンピュータ１９００が起動時に実行するブート・プログラム、及び／又は、コンピュータ１９００のハードウェアに依存するプログラム等を格納する。メモリドライブ２０５０は、メモリカード２０９０から例えば表示プログラム等のプログラム又はデータを読み取り、ＲＡＭ２０２０を介してハードディスクドライブ２０４０に提供する。入出力チップ２０７０は、メモリドライブ２０５０を入出力コントローラ２０８４へと接続すると共に、例えばパラレル・ポート、シリアル・ポート、キーボード・ポート、マウス・ポート等を介して各種の入出力装置を入出力コントローラ２０８４へと接続する。

【００８９】

ＲＡＭ２０２０を介してハードディスクドライブ２０４０に提供されるプログラムは、メモリカード２０９０、又はＩＣカード等の記録媒体に格納されて利用者によって提供される。表示プログラム等のプログラムは、記録媒体から読み出され、ＲＡＭ２０２０を介してコンピュータ１９００内のハードディスクドライブ２０４０にインストールされ、ＣＰＵ２０００において実行される。

【００９０】

コンピュータ１９００にインストールされ、コンピュータ１９００を検出装置１０として機能させるプログラムは、検査配列記憶モジュール、データ対応パターン生成モジュール、更新モジュール、及び、判定モジュールとを備える。これらのプログラム又はモジュールは、ＣＰＵ２０００等に働きかけて、コンピュータ１９００を、検査配列記憶モジュール、データ対応パターン生成モジュール、更新モジュール、及び、判定モジュールとしてそれぞれ機能させる。

【００９１】

これらのプログラムに記述された情報処理は、コンピュータ１９００に読込まれることにより、ソフトウェアと上述した各種のハードウェア資源とが協働した具体的手段である検査配列記憶モジュール、データ対応パターン生成モジュール、更新モジュール、及び、判定モジュールとして機能する。そして、これらの具体的手段によって、本実施形態におけるコンピュータ１９００の使用目的に応じた情報の演算又は加工を実現することにより、使用目的に応じた特有の検出装置１０が構築される。

【００９２】

一例として、コンピュータ１９００と外部の装置等との間で通信を行う場合には、ＣＰＵ２０００は、ＲＡＭ２０２０上にロードされた通信プログラムを実行し、通信プログラ

ムに記述された処理内容に基づいて、通信インターフェイス２０３０に対して通信処理を指示する。通信インターフェイス２０３０は、ＣＰＵ２０００の制御を受けて、ＲＡＭ２０２０、ハードディスクドライブ２０４０、又はメモリカード２０９０等の記憶装置上に設けた送信バッファ領域等に記憶された送信データを読み出してネットワークへと送信し、もしくは、ネットワークから受信した受信データを記憶装置上に設けた受信バッファ領域等へと書き込む。このように、通信インターフェイス２０３０は、ＤＭＡ（ダイレクト・メモリ・アクセス）方式により記憶装置との間で送受信データを転送してもよく、これに代えて、ＣＰＵ２０００が転送元の記憶装置又は通信インターフェイス２０３０からデータを読み出し、転送先の通信インターフェイス２０３０又は記憶装置へとデータを書き込むことにより送受信データを転送してもよい。

【００９３】

また、ＣＰＵ２０００は、ハードディスクドライブ２０４０、メモリドライブ２０５０（メモリカード２０９０）等の外部記憶装置に格納されたファイルまたはデータベース等の中から、全部または必要な部分をＤＭＡ転送等によりＲＡＭ２０２０へと読み込ませ、ＲＡＭ２０２０上のデータに対して各種の処理を行う。そして、ＣＰＵ２０００は、処理を終えたデータを、ＤＭＡ転送等により外部記憶装置へと書き戻す。このような処理において、ＲＡＭ２０２０は、外部記憶装置の内容を一時的に保持するものとみなせるから、本実施形態においてはＲＡＭ２０２０および外部記憶装置等をメモリ、記憶部、または記憶装置等と総称する。本実施形態における各種のプログラム、データ、テーブル、データベース等の各種の情報は、このような記憶装置上に格納されて、情報処理の対象となる。なお、ＣＰＵ２０００は、ＲＡＭ２０２０の一部をキャッシュメモリに保持し、キャッシュメモリ上で読み書きを行うこともできる。このような形態においても、キャッシュメモリはＲＡＭ２０２０の機能の一部を担うから、本実施形態においては、区別して示す場合を除き、キャッシュメモリもＲＡＭ２０２０、メモリ、及び／又は記憶装置に含まれるものとする。

【００９４】

また、ＣＰＵ２０００は、ＲＡＭ２０２０から読み出したデータに対して、プログラムの命令列により指定された、本実施形態中に記載した各種の演算、情報の加工、条件判断、情報の検索・置換等を含む各種の処理を行い、ＲＡＭ２０２０へと書き戻す。例えば、ＣＰＵ２０００は、条件判断を行う場合においては、本実施形態において示した各種の変数が、他の変数または定数と比較して、大きい、小さい、以上、以下、等しい等の条件を満たすかどうかを判断し、条件が成立した場合（又は不成立であった場合）に、異なる命令列へと分岐し、またはサブルーチンを呼び出す。また、ＣＰＵ２０００は、記憶装置内のファイルまたはデータベース等に格納された情報を検索することができる。

【００９５】

以上に示したプログラム又はモジュールは、外部の記録媒体に格納されてもよい。記録媒体としては、メモリカード２０９０の他に、ＤＶＤ又はＣＤ等の光学記録媒体、ＭＯ等の光磁気記録媒体、テープ媒体、ＩＣカード等の半導体メモリ等を用いることができる。また、専用通信ネットワーク又はインターネットに接続されたサーバシステムに設けたハードディスク又はＲＡＭ等の記憶装置を記録媒体として使用し、ネットワークを介してプログラムをコンピュータ１９００に提供してもよい。

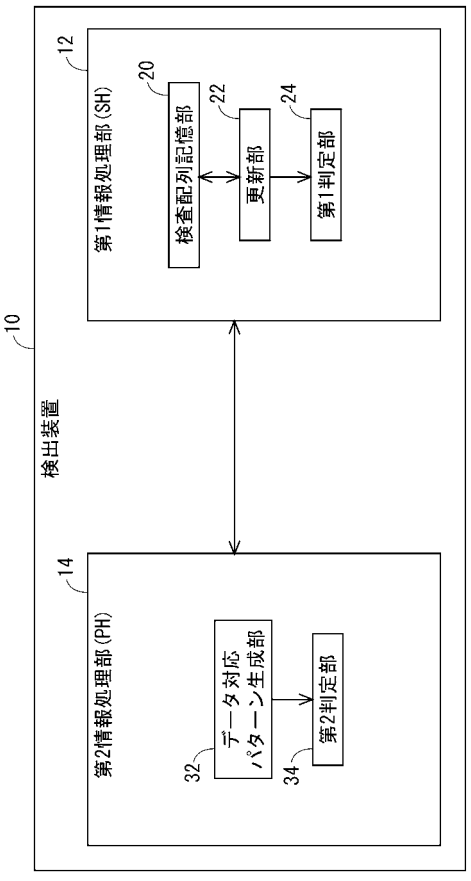
【符号の説明】

【００９６】

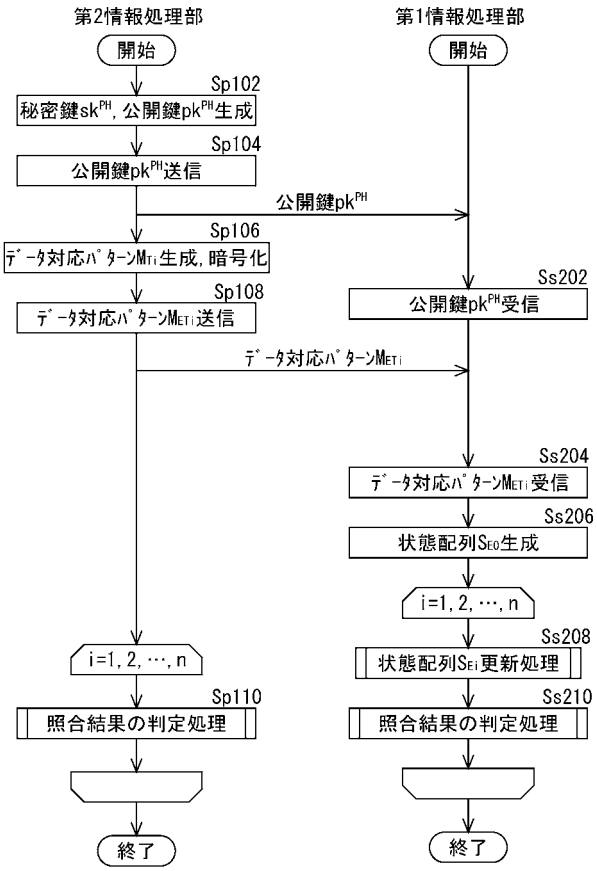
１０　検出装置
１２　第１情報処理部
１４　第２情報処理部
２０　検査配列記憶部
２２　更新部
２４　第１判定部
３２　データ対応パターン生成部

３４　第２判定部
３６　更新補助部
１９００　コンピュータ
２０００　ＣＰＵ
２０１０　ＲＯＭ
２０２０　ＲＡＭ
２０３０　通信インターフェイス
２０４０　ハードディスクドライブ
２０５０　メモリドライブ
２０７０　入出力チップ
２０７５　グラフィック・コントローラ
２０８０　表示部
２０８２　ホスト・コントローラ
２０８４　入出力コントローラ
２０９０　メモリカード

【図１】



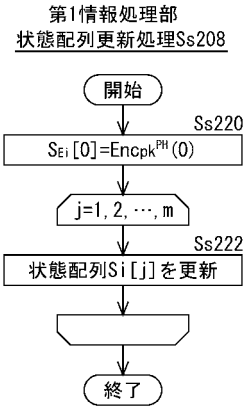

【図２】



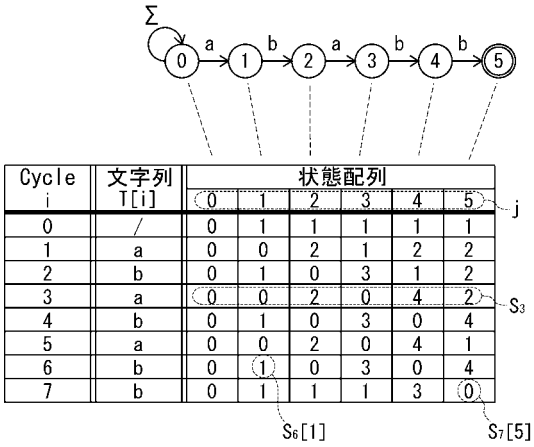
【図３】

| 状態番号[j] | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| Ma | 0 | 1 | 0 | 1 | 1 |
| Mb | 1 | 0 | 1 | 0 | 0 |

【図４】



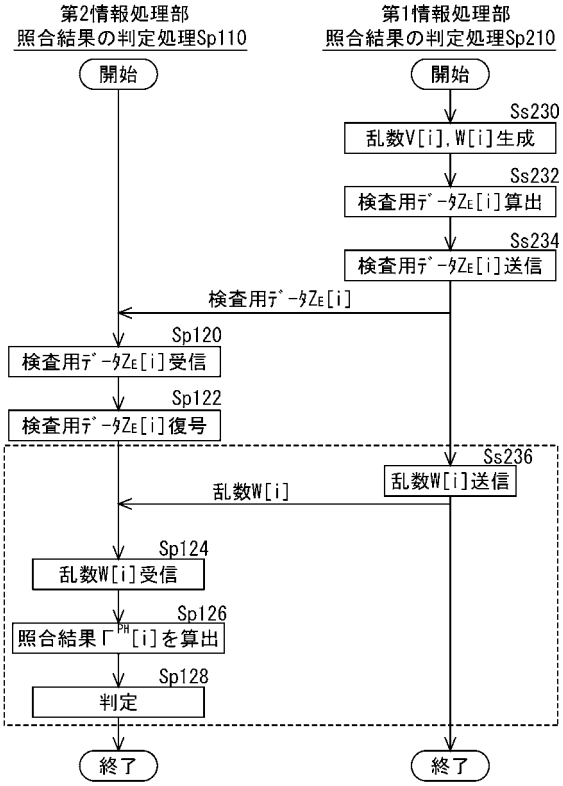

【図５】



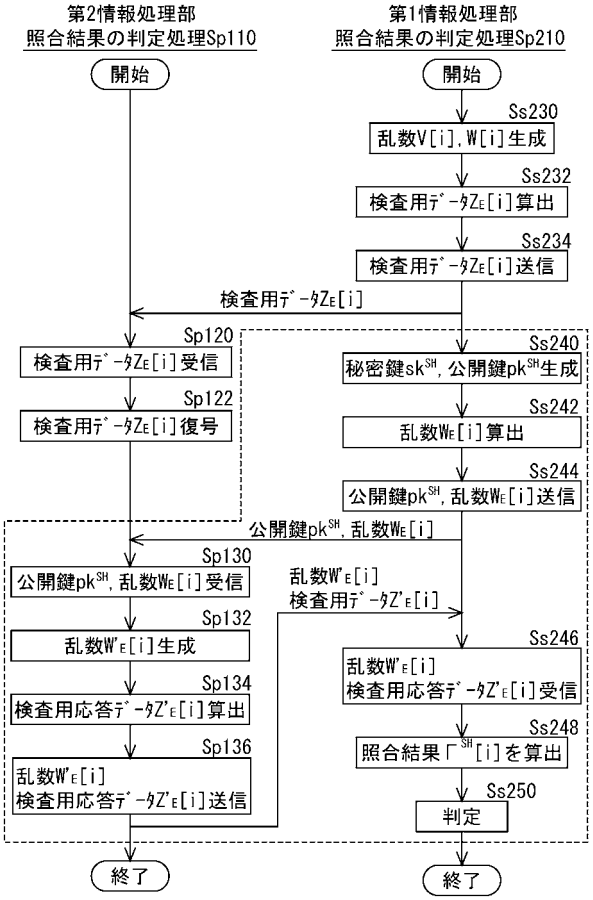

| Cycle i | 文字列 T[i] | 状態配列 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 0 | / | 0 | 1 | 1 | 1 | 1 | 1 |
| 1 | a | 0 | 0 | 2 | 1 | 2 | 2 |
| 2 | b | 0 | 1 | 0 | 3 | 1 | 2 |
| 3 | a | 0 | 0 | 2 | 0 | 4 | 2 |
| 4 | b | 0 | 1 | 0 | 3 | 0 | 4 |
| 5 | a | 0 | 0 | 2 | 0 | 4 | 1 |
| 6 | b | 0 | 1 | 0 | 3 | 0 | 4 |
| 7 | b | 0 | 1 | 1 | 1 | 3 | 0 |

j

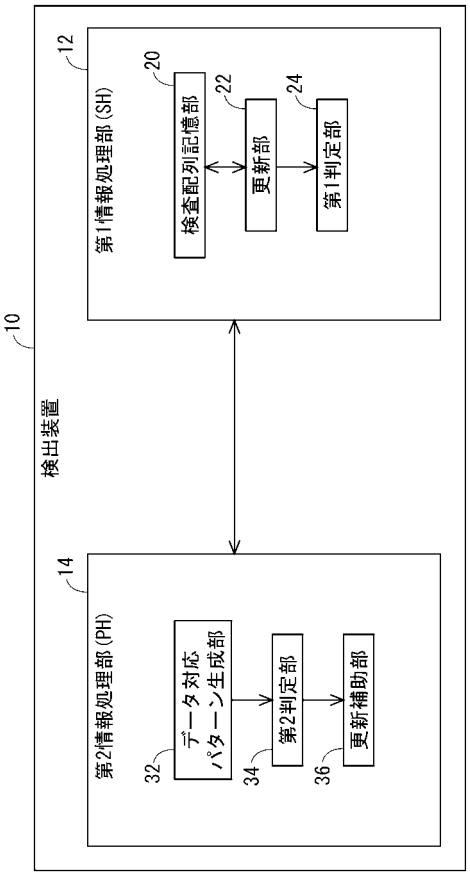
【図６】



【図７】



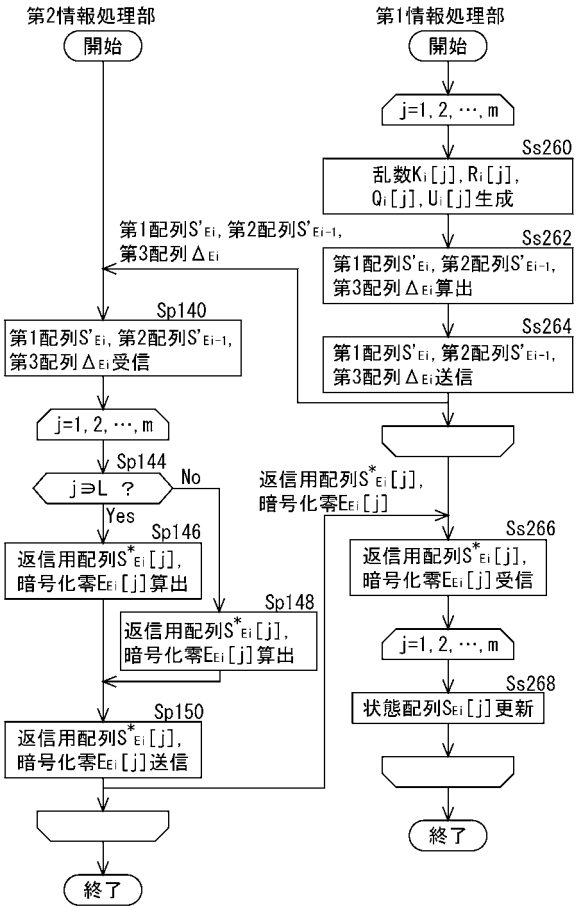

【図８】




【図９】

| | | $S_{i-1}[j]$ | |
|---|---|---|---|
| | | inactive | active |
| $S_i[j]$ | inactive | inactive | if $j \in L$ : active<br>if $j \notin L$ : inactive |
| | active | active | active |

【図１０】

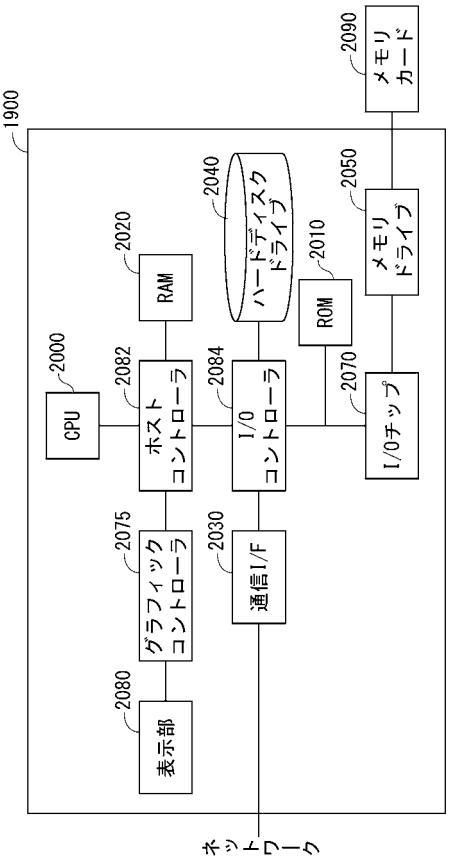


【図１１】

| | | SPM 1 | SPM 2 |
|---|---|---|---|
| 照合結果の取得者 | | SH or PH | SH or PH |
| 事前処理 | 時間計算量 | O (m \|Σ\|) | O (m \|Σ\|) |
| | 通信計算量 | O (m \|Σ\|) | O (m \|Σ\|) |
| 更新処理 | 時間計算量 | O (m) | O (m) |
| | 通信計算量 | O (1) | O (m) |
| ラウンド計算量 | | O (1) | O (n) |
| オンライン対応パターンクラス | | 対応 CM + CC | 対応 CM + CC + ILG |

SH:第1情報処理部　　CM:完全合致
PH:第2情報処理部　　CC:文字種
ILG:無限長ギャップ

【図１２】



フロントページの続き

(72)発明者　有村　博紀
北海道札幌市北区北８条西５丁目　国立大学法人北海道大学内
(72)発明者　笹川　裕人
北海道札幌市北区北８条西５丁目　国立大学法人北海道大学内
Ｆターム(参考) 5J104 AA16　EA08　EA19　JA21