(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2020-4199
(P2020-4199A)
(43)公開日　令和2年1月9日(2020.1.9)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 16/00	(2019.01)	G06F	17/30	412	5J104
G09C 1/00	(2006.01)	G09C	1/00	660D	
		G06F	17/30	120A	

審査請求 未請求　請求項の数 18　ＯＬ　（全 26 頁）

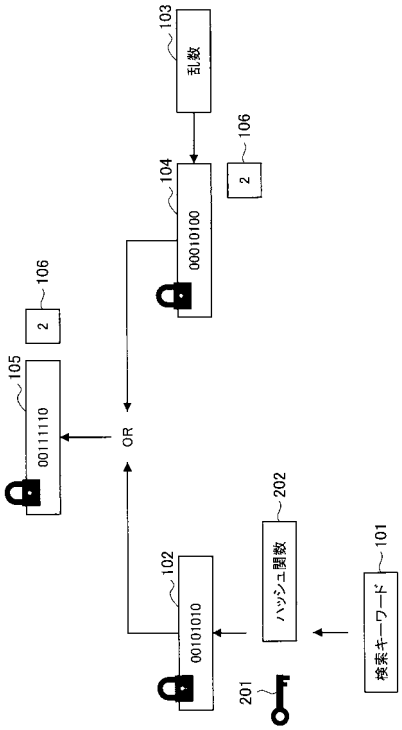
(21)出願番号　特願2018-124466 (P2018-124466)
(22)出願日　平成30年6月29日 (2018.6.29)

(71)出願人　000002185
ソニー株式会社
東京都港区港南１丁目７番１号
(74)代理人　100095957
弁理士　亀谷　美明
(74)代理人　100096389
弁理士　金本　哲男
(74)代理人　100101557
弁理士　萩原　康司
(74)代理人　100128587
弁理士　松本　一騎
(72)発明者　内田　篤史
東京都港区港南１丁目７番１号　ソニー株式会社内

最終頁に続く

(54)【発明の名称】情報処理装置および情報処理方法

(57)【要約】
【課題】検索性能とセキュリティ性を両立する情報検索が可能となる。
【解決手段】情報検索に係るキーワードから鍵付ハッシングを用いて算出したハッシュ値を所定長のビット列にマッピングした暗号化ビット列を生成し、動的に生成された乱数に基づいて、前記暗号化ビット列から所定の数のビットを選択し、選択した前記所定の数のビットを反転し、前記暗号化ビット列、および前記ビット反転部が反転したビットの数を示す反転ビット数情報を外部装置に送信する情報処理装置が提供される。
【選択図】図５



【特許請求の範囲】
【請求項１】
情報検索に係るキーワードから鍵付ハッシングを用いて算出したハッシュ値を所定長のビット列にマッピングした暗号化ビット列を生成する暗号化部と、
動的に生成された乱数に基づいて、前記暗号化ビット列から所定の数のビットを選択し、選択した前記所定の数のビットを反転するビット反転部と、
前記暗号化ビット列、および前記ビット反転部が反転したビットの数を示す反転ビット数情報を外部装置に送信する通信部と、
を備える、
情報処理装置。
【請求項２】
前記情報検索に係るキーワードは、検索キーワードであり、
前記暗号化部は、前記検索キーワードおよび鍵付ハッシングを用いて算出したハッシュ値を所定長のビット列にマッピングした暗号化キーワードを生成し、
前記ビット反転部は、前記動的に生成された乱数に基づいて、前記暗号化キーワードから所定の数のビットを選択し、選択した前記所定の数のビットを反転し、
前記通信部は、前記暗号化キーワード、および前記暗号化キーワードに係る反転ビット数情報を外部装置に送信し、前記暗号化キーワードに対応する暗号検索結果を受信し、
前記暗号検索結果は、検索可能暗号を用いた情報検索の結果である、
請求項１に記載の情報処理装置。
【請求項３】
前記暗号化ビット列は、ブルームフィルタである、
請求項１に記載の情報処理装置。
【請求項４】
前記暗号化部は、複数の前記暗号化ビット列の論理和の計算結果である集合暗号化ビット列を生成し、
前記ビット反転部は、前記動的に生成された乱数に基づいて、前記集合暗号化ビット列から、所定の数のビットを選択し、選択した前記所定の数のビットを反転し
前記通信部は前記反転されたビットの数に係る反転ビット数情報および前記集合暗号化ビット列を送信する、
請求項１に記載の情報処理装置。
【請求項５】
前記通信部は、複数の前記暗号化ビット列、前記ビット反転部が反転したビットの数に係る複数の反転ビット数情報、および論理条件をさらに送信する、
請求項２に記載の情報処理装置。
【請求項６】
前記論理条件は、論理和条件または論理積条件であり、
送信した前記暗号化ビット列に対する暗号検索結果は、少なくとも２つ以上の前記暗号化ビット列との論理和条件または論理積条件に基づく暗号検索結果である、
請求項５に記載の情報処理装置。
【請求項７】
前記ビット反転部は、前記動的に生成された乱数に基づいて、前記暗号化ビット列から、所定の数の０値ビットを選択し、前記選択した記所定の数の０値ビットを１値ビットに反転する、
請求項１に記載の情報処理装置。
【請求項８】
前記情報検索に係るキーワードは、検索インデックスであり、
前記暗号化部は、前記検索インデックスおよび鍵付ハッシングを用いて算出したハッシュ値を所定長のビット列にマッピングした暗号化インデックスを生成し、
前記ビット反転部は、前記動的に生成された乱数に基づいて、前記暗号化インデックス

から所定の数のビットを選択し、選択した前記所定の数のビットを反転する、
請求項１に記載の情報処理装置。
【請求項９】
前記通信部は、送信した暗号化キーワードに対応する、前記所定の数のビットが反転された前記暗号化インデックスに対応する暗号化された前記反転ビット数情報を、検索結果としてさらに受信し、
前記暗号化された反転ビット数情報に基づいて、暗号化される前の前記反転ビット数情報を生成する復号部をさらに備え、
前記復号部は、前記暗号化キーワードと前記暗号化される前の反転ビット数情報の論理積を計算し、前記計算の結果に基づいて、前記検索結果が誤判定であるか否かを判定する、
請求項８に記載の情報処理装置。
【請求項１０】
前記暗号化部は、ＨＭＡＣアルゴリズムを用いて、前記暗号化ビット列を生成する、
請求項１に記載の情報処理装置。
【請求項１１】
クライアント端末から、暗号化キーワード、および前記暗号化キーワードの反転ビット数を示す反転ビット数情報を受信する通信制御部と、
前記暗号化キーワードと保存する暗号化インデックスの排他的論理和を計算したビット計算結果と、前記ビット計算結果に対するビットカウント結果とを取得するビット計算部と、
前記暗号化キーワードの反転ビット数および前記暗号化インデックスの反転ビット数の合計と、前記ビットカウント結果との大小関係の比較に基づいて、前記暗号化キーワードが前記暗号化インデックスに含まれているか否かを判定するビット一致判定部と、
を備え、
前記暗号化キーワードおよび前記暗号化インデックスは、鍵付ハッシングを用いて算出されたハッシュ値を所定長のビット列にマッピングした後、動的に生成された乱数に基づいて所定の数のビットが反転された暗号化ビット列であり、
前記通信制御部は、前記暗号化キーワードが前記暗号化インデックスに含まれていると、前記ビット一致判定部が判定した場合、前記暗号化キーワードに対応する検索結果を前記クライアント端末に送信する、
情報処理装置。
【請求項１２】
前記検索結果は、暗号化データまたは前記暗号化データに係るリストのうち少なくともいずれかを含む、
請求項１１に記載の情報処理装置。
【請求項１３】
前記ビット一致判定部は、前記ビットカウント結果が、前記暗号化キーワードと前記暗号化インデックスの双方の反転されたビット数の合計以下である場合、前記暗号化キーワードが前記暗号化インデックスに含まれていると判定する、
請求項１１に記載の情報処理装置。
【請求項１４】
前記通信制御部は、複数の前記暗号化キーワード、複数の前記暗号化キーワードに係る複数の反転ビット数情報、および論理条件を受信し、
前記ビット計算部は、複数の前記暗号化キーワードのそれぞれに関し、前記暗号化インデックスとの排他的論理和を計算して前記ビット計算結果および前記ビットカウント結果を取得し、
前記ビット一致判定部は、前記複数の暗号化キーワードと前記暗号化インデックスの双方の反転されたビット数の合計と、前記ビット計算結果との大小関係に基づいて、前記暗号化キーワードが前記暗号化インデックスに含まれているか否かをそれぞれ判定し、

前記通信制御部は、前記複数の暗号化キーワードに対応する判定が論理条件を満たしている場合、検索結果を送信する、
請求項１１に記載の情報処理装置。
【請求項１５】
前記論理条件は、論理和条件を含み、
前記通信制御部は、論理和条件に基づいて、前記ビット一致判定部が前記複数の暗号化キーワードのうち、少なくとも１つの前記暗号化キーワードが前記暗号化インデックスに含まれていると判定した場合、前記複数の暗号化キーワードに対応する検索結果を送信する、
請求項１４に記載の情報処理装置。
【請求項１６】
前記論理条件は、論理積条件を含み、
前記通信制御部は、論理積条件に基づいて、前記ビット一致判定部が前記複数の暗号化キーワードのすべてが前記暗号化インデックスに含まれていると判定した場合、前記複数の暗号化キーワードに対応する検索結果を送信する、
請求項１４に記載の情報処理装置。
【請求項１７】
プロセッサが、
情報検索に係るキーワードから鍵付ハッシングを用いて算出したハッシュ値を所定長のビット列にマッピングした暗号化ビット列を生成することと、
動的に生成された乱数に基づいて、前記暗号化ビット列から所定の数のビットを選択し、選択した前記所定の数のビットを反転することと、
反転したビットの数に係る反転ビット数情報および前記暗号化ビット列を外部装置に送信することと、
を含む、情報処理方法。
【請求項１８】
プロセッサが、
クライアント端末から、暗号化キーワード、および前記暗号化キーワードの反転ビット数を示す反転ビット数情報を受信することと、
前記暗号化キーワードと保存する暗号化インデックスの排他的論理和を計算したビット計算結果と、前記ビット計算結果に対するビットカウント結果とを取得することと、
前記暗号化キーワードの反転ビット数および前記暗号化インデックスの反転ビット数の合計と、前記ビットカウント結果との大小関係の比較に基づいて、前記暗号化キーワードが前記暗号化インデックスに含まれているか否かを判定することと、
を含み、
前記暗号化キーワードおよび前記暗号化インデックスは、鍵付ハッシングを用いて算出されたハッシュ値を所定長のビット列にマッピングした後、動的に生成された乱数に基づいて所定の数のビットが反転された暗号化ビット列であり、
前記暗号化キーワードが前記暗号化インデックスに含まれていると判定した場合、前記暗号化キーワードに対応する検索結果を前記クライアント端末に送信する、
情報処理方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本開示は、情報処理装置および情報処理方法に関する。
【背景技術】
【０００２】
近年、クラウドサービスの普及に伴って、データを外部の情報処理サーバに預ける機会が増えている。上記のような情報処理サーバでは、セキュリティ性確保のためにデータの暗号化などを行うのが一般的である。また、近年では、セキュリティ性をより向上させる

方策の一つとして、データを暗号化したまま外部サーバに送信し、情報検索を実行することが可能な検索可能暗号技術が開発されている。例えば、特許文献１では、ノイズを加えた測定値と検索対象データとの差分を計算することで、データを暗号化したまま検索の実行を可能にする技術が開示されている。

【先行技術文献】

【特許文献】

【０００３】

【特許文献１】特表２０１５－５１０３４３号公報

【発明の概要】

【発明が解決しようとする課題】

【０００４】

しかし、特許文献１に開示される装置では、同一内容のデータを暗号化する場合、同一のノイズが加えられてしまうため、暗号化データの出現頻度などから、暗号化前のデータが推測される可能性がある。

【０００５】

そこで、本開示では、検索性能とセキュリティ性を両立する情報検索が可能な情報処理装置、方法を提案する。

【課題を解決するための手段】

【０００６】

本開示によれば、情報検索に係るキーワードから鍵付ハッシングを用いて算出したハッシュ値を所定長のビット列にマッピングした暗号化ビット列を生成する暗号化部と、動的に生成された乱数に基づいて、前記暗号化ビット列から所定の数のビットを選択し、選択した前記所定の数のビットを反転するビット反転部と、前記暗号化ビット列、および前記ビット反転部が反転したビットの数を示す反転ビット数情報を外部装置に送信する通信部と、を備える情報処理装置が提供される。

【０００７】

本開示によれば、クライアント端末から、暗号化キーワード、および前記暗号化キーワードの反転ビット数を示す反転ビット数情報を受信する通信制御部と、前記暗号化キーワードと保存する暗号化インデックスの排他的論理和を計算したビット計算結果と、前記ビット計算結果に対するビットカウント結果とを取得するビット計算部と、前記暗号化キーワードの反転ビット数および前記暗号化インデックスの反転ビット数の合計と、前記ビットカウント結果との大小関係の比較に基づいて、前記暗号化キーワードが前記暗号化インデックスに含まれているか否かを判定するビット一致判定部と、を備え、前記暗号化キーワードおよび前記暗号化インデックスは、鍵付ハッシングを用いて算出されたハッシュ値を所定長のビット列にマッピングした後、動的に生成された乱数に基づいて所定の数のビットが反転された暗号化ビット列であり、前記通信制御部は、前記暗号化キーワードが前記暗号化インデックスに含まれていると前記ビット一致判定部が判定した場合、前記暗号化キーワードに対応する検索結果を前記クライアント端末に送信する情報処理装置が提供される。

【０００８】

本開示によれば、プロセッサが、情報検索に係るキーワードから、鍵付ハッシングを用いて算出したハッシュ値を所定長のビット列にマッピングした暗号化ビット列を生成することと、動的に生成された乱数に基づいて、前記暗号化ビット列から所定の数のビットを選択し、選択した前記所定の数のビットを反転することと、反転したビットの数に係る反転ビット数情報および前記暗号化ビット列を外部装置に送信することと、を含む情報処理方法が提供される。

【０００９】

本開示によれば、プロセッサが、クライアント端末から、暗号化キーワード、および前記暗号化キーワードの反転ビット数を示す反転ビット数情報を受信することと、前記暗号化キーワードと保存する暗号化インデックスの排他的論理和を計算したビット計算結果と

、前記ビット計算結果に対するビットカウント結果とを取得することと、前記暗号化キーワードの反転ビット数および前記暗号化インデックスの反転ビット数の合計と、前記ビットカウント結果との大小関係の比較に基づいて、前記暗号化キーワードが前記暗号化インデックスに含まれているか否かを判定することと、を含み、前記暗号化キーワードおよび前記暗号化インデックスは、鍵付ハッシングを用いて算出されたハッシュ値を所定長のビット列にマッピングした後、動的に生成された乱数に基づいて所定の数のビットが反転された暗号化ビット列であり、前記暗号化キーワードが前記暗号化インデックスに含まれていると前記ビット一致判定部が判定した場合、前記暗号化キーワードに対応する検索結果を前記クライアント端末に送信する情報処理方法が提供される。

【発明の効果】

【００１０】

以上説明したように本開示によれば、検索性能とセキュリティ性を両立する情報検索が可能である。

【００１１】

なお、上記の効果は必ずしも限定的なものではなく、上記の効果とともに、または上記の効果に代えて、本明細書に示されたいずれかの効果、または本明細書から把握され得る他の効果が奏されてもよい。

【図面の簡単な説明】

【００１２】

【図１】検索可能暗号技術の概要を説明するための図である。

【図２】本実施形態に係る情報処理システムの構成例を示すブロック図である。

【図３】同実施形態に係る情報処理端末１０の機能構成例を示すブロック図である。

【図４】同実施形態に係る情報処理サーバ２０の機能構成例を示すブロック図である。

【図５】同実施形態に係る情報処理端末１０による暗号化ビット列の生成について説明するための図である。

【図６】同実施形態に係る情報処理サーバ２０による検索処理について説明するための図である。

【図７】同実施形態に係る情報処理サーバ２０による検索処理について説明するための図である。

【図８】同実施形態に係る検索処理の誤判定の検出動作を説明するための図である。

【図９】同実施形態に係る複数の暗号化ビット列、反転したビットの数に係る複数の反転ビット数情報、および論理条件を含む情報検索に係る動作を説明するための図である。

【図１０】同実施形態に係る暗号化インデックスを情報処理サーバ２０に登録する動作の流れの一例を示す図である。

【図１１】同実施形態に係る暗号化キーワードを含む暗号化インデックスを検索する動作の流れの一例を示す図である。

【図１２】本開示の一実施形態に係る情報処理端末１０および情報処理サーバ２０のハードウェア構成例を示すブロック図である。

【発明を実施するための形態】

【００１３】

以下に添付図面を参照しながら、本開示の好適な実施の形態について詳細に説明する。なお、本明細書及び図面において、実質的に同一の機能構成を有する構成要素については、同一の符号を付することにより重複説明を省略する。

【００１４】

なお、説明は以下の順序で行うものとする。

１．概要
２．システム構成例
３．情報処理端末１０の機能構成例
４．情報処理サーバ２０の機能構成例
５．動作例

６．動作の流れ
７．ハードウェア構成例
８．まとめ

【００１５】

＜１．概要＞

まず、本開示の一実施形態の概要について説明する。近年、クラウドサービスの普及に伴って、データを外部の情報処理サーバに預ける機会が増えている。それに伴い重要なデータがインターネットを通じて利用されることになるため、クラウドサービスの利用に関して、データ漏洩などに関する不安の声が挙がっている。対策として、暗号化通信を利用することで、一定のセキュリティ性を確保することは可能である。しかしながら、ローカルに設置されるクライアント端末から、クラウドに設置されるサーバへ情報検索を行う場合は、少なくとも１回は復号処理を実行する必要がある。だが近年、検索データおよび検索キーワードを暗号化したまま検索を実行することが可能な検索可能暗号技術が開発されている。

【００１６】

ここで、検索可能暗号技術について説明する。図１は、検索可能暗号技術の概要を説明するための図である。図１の左側には、検索対象データの登録処理の様子が示されている。図１左側において、ユーザＵは、まず、ローカルに設置されたクライアント端末を用いて、平文データＤと平文データから抽出されたキーワードリストを、ユーザ鍵ＵＫを用いて暗号化している。次に、ユーザＵは、クラウド側に設置されるサーバに、平文データＤが暗号化された暗号化データＥＤ、およびキーワードリストが暗号化された暗号化インデックスＥＩを送信している。

【００１７】

また、図１右側には、検索処理の様子が示されている。ユーザＵは、ローカル側で検索キーワードを、ユーザ鍵ＵＫを用いて暗号化し、暗号化キーワードＥＫＷをクラウド側に送信している。クラウド側では、受信した暗号化キーワードＥＫＷと、保管する暗号化インデックスＥＩの比較を行い、暗号化キーワードＥＫＷが、保管する暗号化インデックスＥＩに含まれるか否かの判定を行っている。暗号化キーワードＥＫＷを含む暗号化インデックスＥＩが存在する場合、当該暗号化インデックスＥＩに対応する暗号化データＥＤが、ローカル側へと送信される。最終的に、ユーザＵは、暗号化データＥＤがローカル側で復号されることで、検索対象である平文データＤを入手する。

【００１８】

このように、上述の検索可能暗号技術によれば、ユーザＵは、クラウド側に保存されている暗号化データＥＤを復号することなく、暗号化キーワードＥＫＷおよびを用いて暗号化データＥＤを取得することが可能となる。しかしながら、上述の検索可能暗号技術の場合、同じキーワードの検索インデックスから、常に同じ暗号化インデックスが生成されるため、暗号化インデックスの頻出具合に基づいて、暗号化前の検索インデックスが推定される可能性がある。それに対して、確率暗号を用いて暗号化を実行することで、毎回異なる暗号文を生成することが可能となる。しかし一方で、検索性能は低くなってしまう。

【００１９】

本開示の一実施形態に係る技術思想は、上記の点に着目して発想されたものであり、検索性能とセキュリティ性を両立した情報検索が可能である。このために、本開示の一実施形態に係る情報処理装置は、情報検索に係るキーワードから、鍵付ハッシングを用いて算出したハッシュ値を所定のビット列にマッピングした暗号化ビット列を生成することを特徴の一つとする。また、本実施形態に係る情報処理装置は、動的に生成された乱数に基づいて、暗号化ビット列から所定の数のビットを選択し、選択した所定の数のビットを反転することを特徴の一つとする。また、本実施形態に係る情報処理装置は、ビット反転部が反転したビットの数に係る反転ビット数情報および暗号化ビット列を外部装置に送信することを特徴の一つとする。

【００２０】

ここで、情報検索に係るキーワードとは、例えば検索キーワードや検索インデックスをいう。またここで、検索インデックスとは、平文データの内容を検索するための索引をいう。また、反転ビット数情報とは、暗号化ビット列のビットを構成するビットのうち、暗号化後に値が反転したビットの数である反転ビット数に関する情報、をいう。

【００２１】

また、本開示の一実施形態に係る情報処理装置は、クライアント端末から、暗号化キーワード、および暗号化キーワードの反転ビット数を示す反転ビット数情報を受信することを特徴の一つとする。また、本開示の一実施形態に係る情報処理装置は、暗号化キーワードと保存する暗号化インデックスの排他的論理和を計算したビット計算結果と、ビット計算結果に対するビットカウント結果とを取得することを特徴の一つとする。暗号化キーワードの反転ビット数および暗号化インデックスの反転ビット数の合計と、ビットカウント結果との大小関係の比較に基づいて、暗号化キーワードが暗号化インデックスに含まれているか否かを判定することを特徴の一つとする。ここで、ビットカウントとは、ビット列に含まれる１値ビットの数を数えることである。

【００２２】

係る情報処理端末１０および情報処理サーバ２０の特徴によれば、例えば十分な検索スピードを保ったまま、情報漏えいの可能性がより少ない情報検索が可能となる。

【００２３】

＜２．システム構成例＞

次に、本開示の一実施形態に係る情報処理システムの構成例について説明する。図２は、本実施形態に係る情報処理システムの構成例を示すブロック図である。当該情報処理システムは、情報処理端末１０、情報処理サーバ２０を備える。また、上記の各構成は、互いに情報通信が行えるように、ネットワーク３０を介して接続される。

【００２４】

なお、本開示では、情報処理端末１０を、クライアントと称する場合がある。また、本開示では、情報処理端末１０による処理を、ローカル側の処理、と称する場合がある。また、本開示では、情報処理サーバ２０を、単に、サーバと称する場合がある。また、本開示では、情報処理サーバ２０による処理を、クラウド側の処理、と称する場合がある。

【００２５】

（情報処理端末１０）

本実施形態に係る情報処理端末１０は、ユーザの入力操作に基づいて、データを暗号化データの登録や検索可能暗号を用いた情報検索するための情報処理装置である。また、本実施形態に係る情報処理端末１０は、情報検索に係るキーワードから、鍵付ハッシングを用いて算出したハッシュ値を所定のビット列にマッピングした暗号化ビット列を生成する情報処理装置である。

【００２６】

ユーザは、情報処理端末１０により検索性能とセキュリティ性を両立する情報検索を行うことが可能である。本実施形態に係る情報処理端末１０は、例えば、携帯電話、スマートフォン、タブレット端末、ウェアラブル装置、ＰＣ（Ｐｅｒｓｏｎａｌ Ｃｏｍｐｕｔｅｒ）などであり得る。しかし、本実施形態に係る情報処理端末１０は係る例に限定されず、上記の処理の実行が可能な種々の装置であり得る。

【００２７】

（情報処理サーバ２０）

本実施形態に係る情報処理サーバ２０は、情報処理端末１０から送信された暗号化データを保存する情報処理装置である。

【００２８】

また、本実施形態に係る情報処理サーバ２０は、情報処理端末１０から送信された暗号化キーワードに対応する検索結果を情報処理端末１０へ送信する情報処理装置である。またここで、検索結果とは、例えば暗号化データや、暗号化データに係るリストを含む。

【００２９】

（ネットワーク３０）
ネットワーク３０は、情報処理端末１０と情報処理サーバ２０とを接続する機能を有する。ネットワーク３０は、インターネット、電話回線網、衛星通信網などの公衆回線網や、Ｅｔｈｅｒｎｅｔ（登録商標）を含む各種のＬＡＮ（Ｌｏｃａｌ Ａｒｅａ Ｎｅｔｗｏｒｋ）、ＷＡＮ（Ｗｉｄｅ Ａｒｅａ Ｎｅｔｗｏｒｋ）などを含んでもよい。また、ネットワーク３０は、ＩＰ－ＶＰＮ（Ｉｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌ－Ｖｉｒｔｕａｌ Ｐｒｉｖａｔｅ Ｎｅｔｗｏｒｋ）などの専用回線網を含んでもよい。また、ネットワーク３０は、Ｗｉ－Ｆｉ（登録商標）、Ｂｌｕｅｔｏｏｔｈ（登録商標）など無線通信網を含んでもよい。

【００３０】
以上、本実施形態に係る情報処理システムの構成例について説明した。なお、図２を用いて説明したシステム構成はあくまで一例であり、本実施形態に係る情報処理システムの構成は、仕様や運用に応じて柔軟に変形可能である。

【００３１】
＜３．情報処理端末１０の機能構成例＞
次に、本実施形態に係る情報処理端末１０の機能構成例について説明する。図３は、本実施形態に係る情報処理端末１０の機能構成例を示すブロック図である。図３を参照すると、本実施形態に係る情報処理端末１０は、入力部１１、抽出部１２、暗号化部１３、鍵管理部１４、ビット反転部１５、乱数生成部１６、通信部１７、出力部１８および復号部１９を備える。

【００３２】
（入力部１１）
本実施形態に係る入力部１１は、ユーザによる入力操作を受け付け、平文データや検索キーワードを、後述する抽出部１２または暗号化部１３に出力する機能を有する。

【００３３】
（抽出部１２）
本実施形態に係る抽出部１２は、入力部１１がユーザから受け付けた平文データから、単語もしく単語の組み合わせを抽出することで、検索インデックスを生成する機能を有する。抽出部１２は、形態素解析やｎ－ｇｒａｍを用いて当該データから所定のキーワードを抽出することで、検索インデックスを生成してもよい。

【００３４】
（暗号化部１３）
本実施形態に係る暗号化部１３は、入力部１１により入力された平文データまたは検索キーワード、並びに抽出部１２に抽出されたキーワードリストを、鍵付ハッシングを用いて算出したハッシュ値を所定長のビット列にマッピングする、ハッシュ方式を用いることで暗号化ビット列を生成する機能を有する。なお、ハッシュ方式は、検索キーワード数に依存しない固定長ビット列を用いるため、公開鍵暗号方式や共通鍵方式と比べて、種々の処理が高速である点が長所である。またここで、本実施形態に係る暗号化部１３は，当該暗号化ビット列として、ブルームフィルタ、カウンティングフィルタのようなＡＭＱ(Ａｐｐｒｉｘｉｍａｔｅ Ｍｅｍｂｅｒｓｈｉｐ Ｑｕｅｒｙ)形式にエンコードしたものなどを利用してよい。

【００３５】
また、平文データを暗号化し、暗号化データを生成してよい。また、暗号化部１３は、ＨＭＡＣアルゴリズムを用いて、暗号化ビット列を生成してよい。また、複数の暗号化ビット列の論理和を計算することで集合暗号化ビット列を生成し、当該集合暗号化ビット列を暗号化インデックスまたは暗号化キーワードとみなしてもよい。

【００３６】
（鍵管理部１４）
本実施形態に係る鍵管理部１４は、平文データ、検索インデックスおよび検索キーワードを暗号化するために用いられる鍵を管理する機能を有する。鍵管理部１４は、暗号化部

１３の要求に基づいて、鍵を暗号化部１３に送信する。なお、暗号化部１３へ送信された鍵は、暗号化部１３によりハッシュ関数に代入される。また、本実施形態に係る鍵管理部１４は、復号部１９が暗号化データ、暗号化インデックスおよび暗号化キーワードを復号するために用いられる鍵を管理する機能を有する。

【００３７】

（ビット反転部１５）

本実施形態に係るビット反転部１５は、動的に生成された乱数に基づいて、暗号化ビット列から所定の数のビットを選択し、選択した所定の数のビットを反転する機能を有する。本実施形態に係るビット反転部１５が有する上記の機能によれば、情報処理端末１０と情報処理サーバ２０との間で送受信される所定の数のビットが反転された暗号化ビット列を、毎回異なるビット列とすることが可能となる。

【００３８】

また、ビット反転部１５は、動的に生成された乱数に基づいて、暗号化ビット列から、所定の数の０値ビットを選択し、選択した所定の数の０値ビットを１値ビットに反転してよい。

【００３９】

（乱数生成部１６）

本実施形態に係る乱数生成部１６は、乱数を生成する機能を有する。本実施形態に係る乱数生成部１６は、生成した乱数をビット反転部１５に送信する機能を有する。なお、乱数生成部１６が生成した乱数は、ビット反転部１５による暗号化ビット列のビットの反転処理に用いられる。

【００４０】

（通信部１７）

本実施形態に係る通信部１７は、暗号化ビット列およびビット反転部１５が反転したビットの数を示す反転ビット数情報を情報処理サーバ２０などの外部装置に送信する機能を有する。また、本実施形態に係る通信部１７は、暗号化キーワードおよびビット反転部１５が反転したビットの数に係る反転ビット数情報を情報処理サーバ２０に送信し、送信した暗号化キーワードに対する暗号検索結果を受信してよい。ここで、暗号検索結果は、検索可能暗号に係る技術を用いて実行する情報検索の結果をいう。またここで、暗号化キーワードに対する検索結果とは、例えば当該暗号化キーワードを含む暗号化インデックスや、当該暗号化インデックスに対応する暗号化データ、を含む。

【００４１】

また、本実施形態に係る通信部１７は、複数の暗号化ビット列、ビット反転部が反転したビットの数に係る複数の反転ビット数情報および論理条件をさらに送信してもよい。ここで、論理条件とは、例えば論理和条件や論理積条件をいう。また、本実施形態に係る通信部１７は、送信した暗号化キーワードに対応する所定の数のビットが反転された暗号化インデックスおよび、暗号化インデックスに対応する反転ビット数情報を受信してよい。

【００４２】

（出力部１８）

本実施形態に係る出力部１８は、情報処理サーバ２０から通信部１７が受信した暗号検索結果をユーザに対し出力する機能を有する。本実施形態に係る出力部１８は、視覚情報を提示する表示デバイスなどを備える。上記の表示デバイスには、例えば、液晶ディスプレイ（ＬＣＤ：Ｌｉｑｕｉｄ　Ｃｒｙｓｔａｌ　Ｄｉｓｐｌａｙ）装置、ＯＬＥＤ（Ｏｒｇａｎｉｃ　Ｌｉｇｈｔ　Ｅｍｉｔｔｉｎｇ　Ｄｉｏｄｅ）ディスプレイ装置、などが挙げられる。

【００４３】

（復号部１９）

本実施形態に係る復号部１９は、暗号化された情報を復号する機能を有する。また、本実施形態に係る復号部１９は、情報処理サーバ２０から受信された暗号化インデックスおよび、暗号化インデックスに対応する反転ビット数情報を用いて、ビットが反転される前

の暗号化インデックスを生成してよい。復号部１９は、復号した情報を出力部１８へ送信してもよい。なお、復号対象の情報としては、暗号化データ、暗号化インデックス、暗号化キーワード、暗号化された反転ビット数情報、などが挙げられる。

【００４４】

以上、本実施形態に係る情報処理端末１０の機能構成例について説明した。なお、図３を用いて説明した上記の構成はあくまで一例であり、本実施形態に係る情報処理端末１０の機能構成は係る例に限定されない。本実施形態に係る情報処理端末１０の機能構成は、仕様や運用に応じて柔軟に変形可能である。

【００４５】

＜４．情報処理サーバ２０の機能構成例＞

次に、本実施形態に係る情報処理サーバ２０の機能構成例について説明する。図４は、本実施形態に係る情報処理サーバ２０の機能構成例を示すブロック図である。図４を参照すると、本実施形態に係る情報処理サーバ２０は、通信制御部２１、検索部２２、記憶部２３、ビット計算部２４およびビット一致判定部２５を備える。

【００４６】

（通信制御部２１）

本実施形態に係る通信制御部２１は、情報処理端末１０から、暗号化キーワード、および暗号化キーワードの反転ビット数を示す反転ビット数情報を受信する機能を有する。

【００４７】

また、本実施形態に係る通信制御部２１は、ビット一致判定部２５が、暗号化キーワードが暗号化インデックスに含まれていると判定した場合、暗号化キーワードに対応する検索結果を情報処理端末１０に送信してもよい。

【００４８】

（検索部２２）

本実施形態に係る検索部２２は、後述するビット計算部２４およびビット一致判定部２５を備え、通信制御部２１を介して受信した暗号化キーワードが、暗号化インデックスに含まれているか否かを判定する機能を有する。また、本実施形態に係る検索部２２は、記憶部２３から暗号化インデックスを取り出す機能を有する。

【００４９】

（記憶部２３）

本実施形態に係る記憶部２３は、各種情報を一時的または恒常的に記憶するための記憶領域である。例えば、記憶部２３には、情報検索に係る各種情報が記憶されてもよい。具体的な一例として、本実施形態に係る記憶部２３は、暗号化データ、暗号化インデックス、またはビット反転部１５が反転したビットの数に係る反転ビット数情報を記憶する。もちろん、上記はあくまで一例であり、記憶部２３に記憶される情報の種別は特に限定されない。

【００５０】

（ビット計算部２４）

本実施形態に係るビット計算部２４は、暗号化キーワードと保存する暗号化インデックスの排他的論理和を計算したビット計算結果と、ビット計算結果に対するビットカウント結果とを取得する機能を有する。また、本実施形態に係るビット計算部２４は、複数の暗号化キーワードのそれぞれに関し、暗号化インデックスとの排他的論理和を計算してビット計算結果、およびビットカウントを実行してビットカウント結果を取得してよい。ここで、ビットカウントとは、対象のビット列中の１値ビットがいくつ存在するか数えることをいう。

【００５１】

（ビット一致判定部２５）

本実施形態に係るビット一致判定部２５は、暗号化キーワードの反転ビット数および暗号化インデックスの反転ビット数の合計と、ビットカウント結果との大小関係の比較に基づいて、暗号化キーワードが暗号化インデックスに含まれているか否かを判定する機能を

有する。本実施形態に係るビット一致判定部２５は、ビット計算結果が、暗号化キーワードと暗号化インデックスの双方の反転されたビット数の合計以下である場合、検索キーワードが検索インデックスに含まれていると判定してよい。

【００５２】

以上、本実施形態に係る情報処理サーバ２０の機能構成例について説明した。なお、図３を用いて説明した上記の構成はあくまで一例であり、本実施形態に係る情報処理端末１０の機能構成は係る例に限定されない。本実施形態に係る情報処理サーバ２０の機能構成は、仕様や運用に応じて柔軟に変形可能である。

【００５３】

＜５．動作例＞

次に、本実施形態に係る情報処理端末１０および情報処理サーバ２０の情報検索に係る動作の流れについて説明する。図５は、本実施形態に係る情報処理端末１０による暗号化ビット列の生成について説明するための図である。図５には、情報検索に係るキーワードから鍵付ハッシュ関数を用いて暗号化ビット列が生成され、動的に生成された乱数に基づいて、当該暗号化ビット列のうち所定の数のビットが反転される流れが示されている。

【００５４】

ここで、暗号化ビット列は、検索キーワードが暗号化された暗号化キーワード、または検索インデックスが暗号化された暗号化インデックスである。情報処理端末１０が、検索キーワードまたは検索インデックスを暗号化して、所定の数のビットを反転する動作の流れは同一であるため、以下まとめて説明する。

【００５５】

図５において、まず本実施形態に係るビット反転部１５は、情報検索に係るキーワード１０１から、ユーザ鍵２０１およびハッシュ関数２０２を用いて暗号化ビット列１０２を生成する。ここで、暗号化部１３は、ＨＭＡＣアルゴリズムを用いて、暗号化ビット列１０２を生成してもよい。

【００５６】

より具体的には、まず本実施形態に係る暗号化部１３は、情報検索に係るキーワード１０１から、ユーザ鍵２０１および２０２ハッシュ関数を用いてハッシュ値を算出する。図５の一例において、情報検索に係るキーワード１０１は、検索キーワードであるが、検索インデックスであってもよい。暗号化部１３は、算出したハッシュ値を所定長のビット列にマッピングすることで、値が「００１０１０１０」である暗号化ビット列１０２を生成する。

【００５７】

一方、乱数生成部１６は、乱数１０３を動的に生成する。次に、ビット反転部１５は、乱数生成部１６が生成した乱数１０３を用いて、暗号化ビット列１０２と同じ長さの乱数ビット列１０４を生成する。図５に示す一例の場合、ビット反転部１５は、値が「０００１０１００」である乱数ビット列１０４を生成している。また、ビット反転部１５は、乱数ビット列１０４に対して、ビットカウントを行い、値が「２」であるビットカウント結果１０６を生成している。

【００５８】

さらに、本実施形態に係るビット反転部１５は、暗号化ビット列１０２と乱数ビット列１０４の論理和を計算し、所定の数のビットが反転された、値が「００１１１１１０」である暗号化ビット列１０５を生成する。

【００５９】

図５において、情報検索に係るキーワード１０１が検索インデックスである場合、上記の処理の後、暗号化ビット列１０５である暗号化インデックスは、情報処理サーバ２０へ送信され、記憶部２３に格納される。なお、以下では、上記のように生成された暗号化ビット列１０５が暗号化キーワードであり、情報処理サーバ２０が当該暗号化キーワードを用いて検索処理を行う場合の動作の流れについて説明する。

【００６０】

図６および図７は、本実施形態に係る情報処理サーバ２０による検索処理について説明するための図である。図６には、暗号化キーワードと暗号化インデックスの排他的論理和を計算し、計算結果から、反転したビットの数を取得する流れが示されている。

【００６１】

具体的に説明する。図６に示す一例において、本実施形態に係るビット計算部２４は、まず、情報処理端末１０から受信した、値が「００１１１１１０」である暗号化キーワード１０５と、値が「００１０１１１１」である暗号化インデックス１０７の排他的論理和を計算し、値が「０００１０００１」であるビット計算結果１０８を取得する。次に、本実施形態に係るビット計算部２４は、ビット計算結果１０８にビットカウントを行い、１値ビットの数「２」のビットカウント結果１０９を生成する。

【００６２】

図７は、暗号化キーワードが暗号化インデックスに含まれているか否かを判定する流れを示す図である。図７において、本実施形態に係るビット一致判定部２５は、暗号化キーワード１０５の反転された反転ビット数１０６と暗号化インデックス１０７の反転された反転ビット数１１０の合計の、値が「３」である反転合計１１１を算出する。次に、本実施形態に係るビット一致判定部２５は、ビット計算部２４が算出した、ビット計算結果１０８のビットカウント結果１０９と反転合計１１１との大小関係を判定する。

【００６３】

ここで、ビット一致判定部２５は、ビットカウント結果１０９が、反転合計１１１以下である場合、暗号化キーワード１０５が暗号化インデックス１０７に含まれていると判定してよい。当該判定の理由を以下に説明する。暗号化キーワード１０５が暗号化インデックス１０７に含まれている場合、排他的論理和を計算することにより、ビットが反転される前の暗号化ビット列部分が相殺される。そのため、最終的に当該排他的論理和の計算結果として残るのは、暗号化キーワード１０５と暗号化インデックス１０７の乱数ビット列のみである。つまり、ビットカウント結果１０９は、暗号化キーワード１０５が暗号化インデックス１０７に含まれている場合、反転合計１１１以下の値となる。

【００６４】

図７に示す一例では、値が「２」である暗号化キーワード１０５の反転ビット数１０６と、値が「１」である暗号化インデックス１０７の反転された反転ビット数１１０が示されている。本実施形態に係るビット一致判定部２５は、値が「３」である反転ビット数１０６と、反転ビット数１１０の合計「３」である反転合計１１１を算出する。次に、本実施形態に係るビット一致判定部２５は、値が「３」である反転合計１１１と値が「２」であるビットカウント結果１０９との大小関係を判定している。

【００６５】

次に、本実施形態に係るビット一致判定部２５は、大小関係の判定の結果、ビットカウント結果１０９が反転合計１１１以下であることから、暗号化キーワード１０５が暗号化インデックス１０７に含まれていると判定している。言い換えれば、本実施形態に係るビット一致判定部２５は、当該暗号化ビット列１０５に対応する検索キーワードが当該暗号化インデックス１０７に対応する検索インデックスに含まれていると判定している。

【００６６】

このように、本実施形態に係る情報処理端末１０および情報処理サーバ２０は、暗号化キーワードおよび暗号化インデックスに乱数ビット列を加えた情報検索を実行することを特徴の一つとする。係る特徴によれば、確率暗号を用いておらず、また乱数ビット列が判明しなければ元の暗号化キーワードが分からないため、検索性能とセキュリティ性を両立させた情報検索が可能となる。

【００６７】

以上、本実施形態に係る情報検索の基本的な動作ついて説明した。一方、ブルームフィルタのようなあるビット列が他のビット列の集合に含まれているか否かを確率的に検索するために用いられるフィルタを暗号化ビット列として用いる場合、検索対象の検索キーワードに対応する暗号化キーワードが、当該暗号化キーワードと一致しない暗号化インデッ

クスに対して、一致すると誤判定されてしまう場合もある。そこで、本実施形態では、情報処理端末１０は、当該誤判定を検出することが可能である。以下、一例として、動的に生成された乱数に基づいて選択された、所定の数の０値ビットが１値ビットに反転された暗号化インデックスに係る検出動作の場合について説明する。図８は、本実施形態に係る検索処理の誤判定の検出動作を説明するための図である。

【００６８】

図８に示す一例では、ビット一致判定部２５により暗号化ビット列１０２が含まれていると判定された暗号化インデックス１０７および暗号化インデックス１１４が情報処理サーバ２０に保存されている。また、情報処理サーバ２０には、暗号化インデックス１０７に対応する乱数ビット列１１２が暗号化された暗号化乱数ビット列１１８、暗号化インデックス１１４に対応する乱数ビット列１１６が暗号化された暗号化乱数ビット列１１５も併せて保存されている。

【００６９】

以下、ビット一致判定部２５による判定が、誤判定であるか否かを判定する動作の流れについて説明する。まず、情報処理サーバ２０の通信制御部２１は、値が「００１０１１１１」である暗号化インデックス１０７、および暗号化乱数ビット列１１８を情報処理端末１０へ送信する。次に、情報処理端末１０の復号部１９は、受信された暗号化乱数ビット列１１８を復号し、値が「０００００１０１」である乱数ビット列１１２を生成する。復号部１９は、乱数ビット列１１２と暗号化キーワードである暗号化ビット列１０２の論理積を計算し、値が「０００００００」である判定結果ビット列１１３を生成する。ここで、暗号化インデックス１０７が暗号化キーワードである暗号化ビット列１０２と一致する場合、図８に示す一例のように、判定結果ビット列１１３は、０値ビットのみのビット列になる。

【００７０】

また同様に、情報処理サーバ２０の通信制御部２１は、値が「００１０１１１１」である暗号化インデックス１１４、および暗号化乱数ビット列１１５を情報処理端末１０へ送信する。情報処理端末１０の復号部１９は、受信された暗号化乱数ビット列１１５を復号し、値が「０００００００１０」である乱数ビット列１１６を生成する。復号部１９は、乱数ビット列１１６と暗号化キーワードである暗号化ビット列１０２の論理積を計算し、値が「０００００００１０」である判定結果ビット列１１７を生成する。ここで、暗号化インデックス１１４が、暗号化キーワードである暗号化ビット列１０２と一致しない場合、図８に示す一例のように、判定結果ビット列１１７は、１値ビットが存在するビット列になる。

【００７１】

このように、情報処理端末１０は、ビット一致判定部２５による判定が誤判定であるか否かを判定することが可能である。係る機能によれば、検索精度の向上を実現することが可能である。

【００７２】

なお、上記では、単一の暗号化キーワードを検索する場合の例について説明してきた。一方、情報処理端末１０が情報処理サーバ２０へ送信する検索条件は、検索対象とする暗号化キーワードは複数含んでいてもよい。また、当該検索条件は、論理条件をさらに含んでよい。図９は、本実施形態に係る複数の暗号化ビット列、反転したビットの数に係る複数の反転ビット数情報、および論理条件を含む情報検索に係る動作の流れについて説明するための図である。図９には、複数の暗号化キーワードと論理条件が示されている。

【００７３】

図９を参照すると、情報処理端末１０の通信部１７は、値が「００１０１０１０」である第１の暗号化キーワード１１９および値が「００１０１０１１」である第２の暗号化キーワード１２１、値が「２」である反転ビット数情報１２０および値が「１」である反転ビット数情報１２２、論理条件２０３を情報処理サーバ２０へ送信している。ここで、論理条件は、例えば論理和条件や論理積条件、をいう。すなわち、論理条件は、例えばＡＮ

Ｄ条件やＯＲ条件、をいう。ここで、情報処理サーバ２０のビット一致判定部２５は、通信制御部２１が受信した複数の検索キーワードと論理条件を用いて、当該複数の検索キーワードの検索結果が、当該論理条件を満たしているか否かを判定することができる。ビット計算部２４は、複数の暗号化キーワードと、暗号化インデックスの排他的論理和を計算し、それぞれビット計算結果を取得する。また、ビット一致判定部２５は、複数の暗号化キーワードと暗号化インデックスの双方の反転されたビット数の合計と、ビット計算結果との大小関係に基づいて、暗号化キーワードが暗号化インデックスに含まれているか否かをそれぞれ判定する。通信制御部２１は、受信された論理条件に関する判定をさらに実行する。

【００７４】

情報処理サーバ２０は、情報処理端末１０が送信した上記情報に対する検索結果を情報処理端末１０へ送信する。論理条件が論理和条件の場合、複数の暗号化キーワードのうち、少なくとも１の暗号化キーワードが暗号化インデックスに含まれているとビット一致判定部２５が判定した場合、複数の暗号化キーワードに対応する検索結果を送信する。図９の一例の場合、値が「００１０１０１０」である第１の暗号化キーワード１１９と、値が「００１０１０１１」である第２の暗号化キーワード１２１のいずれかが暗号化インデックスに含まれているとビット一致判定部２５が判定した場合、暗号化インデックスに含まれていると判定された暗号化キーワードに対する検索結果を情報処理端末１０へ送信する。

【００７５】

なお、上記では、論理条件が論理和条件である例について説明したが、論理条件が論理積条件でもよい。本実施形態に係る情報処理端末１０は、ビット反転部１５が反転したビットの数に係る複数の反転ビット数情報、論理積条件および複数の暗号化キーワードをさらに送信してよい。本実施形態に係る情報処理サーバ２０は、複数の暗号化キーワードのすべてが暗号化インデックスに含まれていると前記ビット一致判定部が判定した場合、前記複数の暗号化キーワードに対応する検索結果を送信してよい。

【００７６】

係る機能によれば、利便性とセキュリティ性を両立し、また柔軟な情報検索が可能となる。

【００７７】

以上説明したように、本実施形態に係る情報処理端末１０および情報処理サーバ２０によれば、暗号化データおよび暗号化インデックスの生成や、暗号化キーワードを用いた検索を実現することが可能である。また、情報処理端末１０おとび情報処理サーバ２０は、暗号化データおよび暗号化インデックスの更新または削除の処理の実行も可能である。

【００７８】

情報処理端末１０は、更新対象または削除対象となる暗号化データに対応する暗号化インデックスおよび反転ビット数情報を情報処理サーバ２０から取得する。次に、情報処理端末１０は、受信された暗号化インデックスを復号することで、検索インデックスを生成し、復号された検索インデックスが検索キーワードと一致するか否かを判定する。復号された検索インデックスが検索キーワードと一致すると判定された場合、情報処理端末１０は、当該検索インデックスに対応する平文データの更新処理または削除処理の実行を情報処理サーバ２０に依頼する。

【００７９】

このように、情報処理端末１０および情報処理サーバ２０が有する機能によれば、検索性能とセキュリティ性を両立しながら、コンピュータソフトウェアの基本処理を実行することが可能となる。

【００８０】

＜６．動作の流れ＞

次に本実施形態に係る情報処理端末１０と情報処理サーバ２０の暗号化インデックスを登録する動作の流れについて説明する。図１０は、本実施形態に係る暗号化インデックス

を情報処理サーバ２０に登録する動作の流れの一例を示す図である。

【００８１】

図１０を参照すると、まず、情報処理端末１０の入力部１１がユーザによる入力操作を受け付け、平文データを受信する（Ｓ１１０１）。次に、抽出部１２は、ステップＳ１１０１で受信された平文データに基づいて、検索インデックスを生成する（Ｓ１１０２）。次に、暗号化部１３は、ステップＳ１１０２で生成された検索インデックスから、鍵付ハッシングを用いて算出したハッシュ値を所定のビット列にマッピングし、暗号化インデックスを生成する（Ｓ１１０３）。

【００８２】

一方、乱数生成部１６は乱数を生成し、ビット反転部１５は、乱数生成部１６が生成した乱数に基づいて、暗号化ビット列と同じ長さである乱数ビット列を生成する（Ｓ１１０４）。次に、ビット反転部１５は、ステップＳ１１０４で生成された乱数ビット列と暗号化ビット列との排他的論理和を計算する（Ｓ１１０５）。次に、通信部１７は、暗号化データ、暗号化インデックスおよび反転ビット数情報を情報処理サーバ２０へ送信する（Ｓ１１０６）。

【００８３】

情報処理サーバ２０の通信制御部２１は、ステップＳ１１０６で送信された暗号化データ、暗号化インデックスおよび反転ビット数情報を受信し、記憶部２３へ送信する。記憶部２３は、受信した暗号化データ、暗号化インデックスおよび反転ビット数情報を記憶領域へ格納する（Ｓ１１０７）。

【００８４】

次に、所定の検索キーワードを含む平文データを検索する動作の流れについて説明する。図１１は、本実施形態に係る暗号化キーワードを含む暗号化インデックスを検索する動作の流れの一例を示す図である。図１１を参照すると、まず、情報処理端末１０の入力部１１がユーザによる入力操作を受け付け、検索キーワードを受信する（Ｓ１２０１）。次に、暗号化部１３は、ステップＳ１２０１で受信された検索キーワードから、鍵付ハッシングを用いて算出したハッシュ値を所定のビット列にマッピングした暗号化キーワードを生成する（Ｓ１２０２）。

【００８５】

一方、乱数生成部１６は乱数を生成し、ビット反転部１５は、乱数生成部１６が生成した乱数に基づいて、暗号化ビット列と同じ長さである乱数ビット列を生成する（Ｓ１２０３）。次に、ビット反転部１５は、ステップＳ１２０３で生成された乱数ビット列に基づいて、暗号化キーワードから所定の数のビットを選択し、選択した所定の数のビットを反転する（Ｓ１２０４）。次に、通信部１７は、ステップＳ１２０４で生成された暗号化ビット列および反転ビット数情報を情報処理サーバ２０へ送信する（Ｓ１２０５）。

【００８６】

情報処理サーバ２０の通信制御部２１は、ステップＳ１２０５で送信された暗号化キーワードおよび反転ビット数情報を受信する（Ｓ１２０５）。次に、検索部２２は、記憶部２３に格納された暗号化インデックスを取り出し、ビット計算部２４へ送信する（Ｓ１２０６）。次に、ビット計算部２４は、ステップＳ１２０６で取り出された暗号化キーワードと、ステップＳ１２０５で受信した暗号化インデックスの排他的論理和を計算する（Ｓ１２０７）。次に、ビット一致判定部２５は、ステップＳ１２０６で計算されたビット計算結果に対しビットカウントを行い、ビットカウント結果を生成する（Ｓ１２０８）。次に、暗号化キーワードの反転ビット数および暗号化インデックスの反転ビット数の合計と、ステップＳ１２０８で生成されたビットカウント結果との大小関係の比較に基づいて、暗号化キーワードが暗号化インデックスに含まれているか否かを判定する（Ｓ１２０９）。ビット一致判定部２５が暗号化インデックスに暗号化キーワードが含まれていると判定した場合、通信制御部２１は、暗号化キーワードに対応する検索結果を情報処理端末１０へ送信する（Ｓ１２１０）。

【００８７】

＜７．ハードウェア構成例＞
次に、本開示の一実施形態に係る情報処理端末１０および情報処理サーバ２０のハードウェア構成例について説明する。図１２は、本開示の一実施形態に係る情報処理端末１０および情報処理サーバ２０のハードウェア構成例を示すブロック図である。図１２を参照すると、情報処理端末１０および情報処理サーバ２０は、例えば、プロセッサ８７１と、ＲＯＭ８７２と、ＲＡＭ８７３と、ホストバス８７４と、ブリッジ８７５と、外部バス８７６と、インターフェース８７７と、入力装置８７８と、出力装置８７９と、ストレージ８８０と、ドライブ８８１と、接続ポート８８２と、通信装置８８３と、を有する。なお、ここで示すハードウェア構成は一例であり、構成要素の一部が省略されてもよい。また、ここで示される構成要素以外の構成要素をさらに含んでもよい。

【００８８】
（プロセッサ８７１）
プロセッサ８７１は、例えば、演算処理装置又は制御装置として機能し、ＲＯＭ８７２、ＲＡＭ８７３、ストレージ８８０、又はリムーバブル記録媒体９０１に記録された各種プログラムに基づいて各構成要素の動作全般又はその一部を制御する。

【００８９】
（ＲＯＭ８７２、ＲＡＭ８７３）
ＲＯＭ８７２は、プロセッサ８７１に読み込まれるプログラムや演算に用いるデータ等を格納する手段である。ＲＡＭ８７３には、例えば、プロセッサ８７１に読み込まれるプログラムや、そのプログラムを実行する際に適宜変化する各種パラメータ等が一時的又は永続的に格納される。

【００９０】
（ホストバス８７４、ブリッジ８７５、外部バス８７６、インターフェース８７７）
プロセッサ８７１、ＲＯＭ８７２、ＲＡＭ８７３は、例えば、高速なデータ伝送が可能なホストバス８７４を介して相互に接続される。一方、ホストバス８７４は、例えば、ブリッジ８７５を介して比較的データ伝送速度が低速な外部バス８７６に接続される。また、外部バス８７６は、インターフェース８７７を介して種々の構成要素と接続される。

【００９１】
（入力装置８７８）
入力装置８７８には、例えば、マウス、キーボード、タッチパネル、ボタン、スイッチ、及びレバー等が用いられる。さらに、入力装置８７８としては、赤外線やその他の電波を利用して制御信号を送信することが可能なリモートコントローラ（以下、リモコン）が用いられることもある。また、入力装置８７８には、マイクロフォンなどの音声入力装置が含まれる。

【００９２】
（出力装置８７９）
出力装置８７９は、例えば、ＣＲＴ（Ｃａｔｈｏｄｅ　Ｒａｙ　Ｔｕｂｅ）、ＬＣＤ、又は有機ＥＬ等のディスプレイ装置、スピーカ、ヘッドホン等のオーディオ出力装置、プリンタ、携帯電話、又はファクシミリ等、取得した情報を利用者に対して視覚的又は聴覚的に通知することが可能な装置である。また、本開示に係る出力装置８７９は、触覚刺激を出力することが可能な種々の振動デバイスを含む。

【００９３】
（ストレージ８８０）
ストレージ８８０は、各種のデータを格納するための装置である。ストレージ８８０としては、例えば、ハードディスクドライブ（ＨＤＤ）等の磁気記憶デバイス、半導体記憶デバイス、光記憶デバイス、又は光磁気記憶デバイス等が用いられる。

【００９４】
（ドライブ８８１）
ドライブ８８１は、例えば、磁気ディスク、光ディスク、光磁気ディスク、又は半導体メモリ等のリムーバブル記録媒体９０１に記録された情報を読み出し、又はリムーバブル

記録媒体９０１に情報を書き込む装置である。
【００９５】
（リムーバブル記録媒体９０１）
リムーバブル記録媒体９０１は、例えば、ＤＶＤメディア、Ｂｌｕ－ｒａｙ（登録商標）メディア、ＨＤ　ＤＶＤメディア、各種の半導体記憶メディア等である。もちろん、リムーバブル記録媒体９０１は、例えば、非接触型ＩＣチップを搭載したＩＣカード、又は電子機器等であってもよい。
【００９６】
（接続ポート８８２）
接続ポート８８２は、例えば、ＵＳＢ（Ｕｎｉｖｅｒｓａｌ　Ｓｅｒｉａｌ　Ｂｕｓ）ポート、ＩＥＥＥ１３９４ポート、ＳＣＳＩ（Ｓｍａｌｌ　Ｃｏｍｐｕｔｅｒ　Ｓｙｓｔｅｍ　Ｉｎｔｅｒｆａｃｅ）、ＲＳ－２３２Ｃポート、又は光オーディオ端子等のような外部接続機器９０２を接続するためのポートである。
【００９７】
（外部接続機器９０２）
外部接続機器９０２は、例えば、プリンタ、携帯音楽プレーヤ、デジタルカメラ、デジタルビデオカメラ、又はＩＣレコーダ等である。
【００９８】
（通信装置８８３）
通信装置８８３は、ネットワークに接続するための通信デバイスであり、例えば、有線又は無線ＬＡＮ、Ｂｌｕｅｔｏｏｔｈ（登録商標）、又はＷＵＳＢ（Ｗｉｒｅｌｅｓｓ　ＵＳＢ）用の通信カード、光通信用のルータ、ＡＤＳＬ（Ａｓｙｍｍｅｔｒｉｃ　Ｄｉｇｉｔａｌ　Ｓｕｂｓｃｒｉｂｅｒ　Ｌｉｎｅ）用のルータ、又は各種通信用のモデム等である。
【００９９】
＜８．まとめ＞
以上説明したように、本開示の一実施形態に係る情報処理端末１０および情報処理サーバ２０は、乱数に基づいて、暗号化キーワードおよび暗号化インデックスから選択された所定のビットを反転して、情報検索を行うことが可能となる。係る機能によれば、検索性能とセキュリティ性を両立する通信により情報検索を実行することができる。
【０１００】
以上、添付図面を参照しながら本開示の好適な実施形態について詳細に説明したが、本開示の技術的範囲はかかる例に限定されない。本開示の技術分野における通常の知識を有する者であれば、特許請求の範囲に記載された技術的思想の範疇内において、各種の変更例または修正例に想到し得ることは明らかであり、これらについても、当然に本開示の技術的範囲に属するものと了解される。
【０１０１】
また、本明細書に記載された効果は、あくまで説明的または例示的なものであって限定的ではない。つまり、本開示に係る技術は、上記の効果とともに、または上記の効果に代えて、本明細書の記載から当業者には明らかな他の効果を奏しうる。
【０１０２】
また、本明細書の情報処理端末１０および情報処理サーバ２０の処理に係る各ステップは、必ずしもシーケンス図に記載された順序に沿って時系列に処理される必要はない。例えば、情報処理端末１０および情報処理サーバ２０の処理に係る各ステップは、フローチャートに記載された順序と異なる順序で処理されても、並列的に処理されてもよい。
【０１０３】
なお、以下のような構成も本開示の技術的範囲に属する。
（１）
情報検索に係るキーワードから鍵付ハッシングを用いて算出したハッシュ値を所定長のビット列にマッピングした暗号化ビット列を生成する暗号化部と、

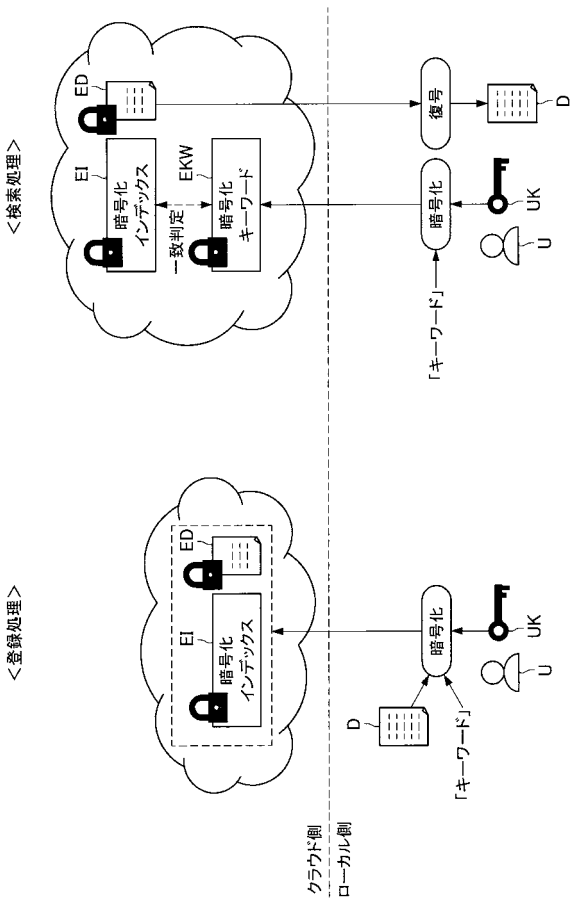
動的に生成された乱数に基づいて、前記暗号化ビット列から所定の数のビットを選択し、選択した前記所定の数のビットを反転するビット反転部と、
前記暗号化ビット列、および前記ビット反転部が反転したビットの数を示す反転ビット数情報を外部装置に送信する通信部と、
を備える、
情報処理装置。
（２）
前記情報検索に係るキーワードは、検索キーワードであり、
前記暗号化部は、前記検索キーワードおよび鍵付ハッシングを用いて算出したハッシュ値を所定長のビット列にマッピングした暗号化キーワードを生成し、
前記ビット反転部は、前記動的に生成された乱数に基づいて、前記暗号化キーワードから所定の数のビットを選択し、選択した前記所定の数のビットを反転し、
前記通信部は、前記暗号化キーワード、および前記暗号化キーワードに係る反転ビット数情報を外部装置に送信し、前記暗号化キーワードに対応する暗号検索結果を受信し、
前記暗号検索結果は、検索可能暗号に係る技術を用いて実行する情報検索の結果である、
前記（１）に記載の情報処理装置。
（３）
前記暗号化ビット列は、ブルームフィルタである、
前記（１）または（２）に記載の情報処理装置。
（４）
前記暗号化部は、複数の前記暗号化ビット列の論理和の計算結果である集合暗号化ビット列を生成し、
前記ビット反転部は、前記動的に生成された乱数に基づいて、前記集合暗号化ビット列から、所定の数のビットを選択し、選択した前記所定の数のビットを反転し、
前記通信部は前記反転されたビットの数に係る反転ビット数情報および前記集合暗号化ビット列を送信する、
前記（１）～（３）のいずれかに記載の情報処理装置。
（５）
前記通信部は、前記ビット反転部が反転したビットの数に係る複数の反転ビット数情報、論理条件および複数の前記暗号化ビット列をさらに送信する、
前記（１）～（４）のいずれかに記載の情報処理装置。
（６）
前記論理条件は、論理和条件または論理積条件であり、
送信した前記暗号化ビット列に対する暗号検索結果は、少なくとも２つ以上の前記暗号化ビット列との論理和条件または論理積条件に基づく暗号検索結果である、
前記（５）に記載の情報処理装置。
（７）
前記ビット反転部は、前記動的に生成された乱数に基づいて、前記暗号化ビット列から、所定の数の０値ビットを選択し、前記選択した記所定の数の０値ビットを１値ビットに反転する、
前記（１）～（６）のいずれかに記載の情報処理装置。
（８）
前記情報検索に係るキーワードは、検索インデックスであり、
前記暗号化部は、前記検索インデックスおよび鍵付ハッシングを用いて算出したハッシュ値を所定長のビット列にマッピングした暗号化インデックスを生成し、
前記ビット反転部は、前記動的に生成された乱数に基づいて、前記暗号化インデックスから所定の数のビットを選択し、選択した前記所定の数のビットを反転する、
前記（１）、３～（７）のいずれかに記載の情報処理装置。
（９）

前記通信部は、送信した暗号化キーワードに対応する、前記所定の数のビットが反転された前記暗号化インデックスに対応する暗号化された前記反転ビット数情報を、検索結果としてさらに受信し、
前記暗号化された反転ビット数情報に基づいて、暗号化される前の前記反転ビット数情報を生成する復号部をさらに備え、
前記復号部は、前記暗号化キーワードと前記暗号化される前の反転ビット数情報の論理積を計算し、前記計算の結果に基づいて、前記検索結果が誤判定であるか否かを判定する、
前記（８）に記載の情報処理装置。
（１０）
前記暗号化部は、ＨＭＡＣアルゴリズムを用いて、前記暗号化ビット列を生成する、
前記（１）～（９）のいずれかに記載の情報処理装置。
（１１）
クライアント端末から、暗号化キーワード、および前記暗号化キーワードの反転ビット数を示す反転ビット数情報を受信する通信制御部と、
前記暗号化キーワードと保存する暗号化インデックスの排他的論理和を計算したビット計算結果と、前記ビット計算結果に対するビットカウント結果とを取得するビット計算部と、
前記暗号化キーワードの反転ビット数および前記暗号化インデックスの反転ビット数の合計と、前記ビットカウント結果との大小関係の比較に基づいて、前記暗号化キーワードが前記暗号化インデックスに含まれているか否かを判定するビット一致判定部と、
を備え、
前記暗号化キーワードおよび前記暗号化インデックスは、鍵付ハッシングを用いて算出されたハッシュ値を所定長のビット列にマッピングした後、動的に生成された乱数に基づいて所定の数のビットが反転された暗号化ビット列であり、
前記通信制御部は、前記暗号化キーワードが前記暗号化インデックスに含まれていると、前記ビット一致判定部が判定した場合、前記暗号化キーワードに対応する検索結果を前記クライアント端末に送信する、
情報処理装置。
（１２）
前記検索結果は、暗号化データまたは、前記暗号化データに係るリストを含む、
前記（１１）に記載の情報処理装置。
（１３）
前記ビット一致判定部は、前記ビットカウント結果が、前記暗号化キーワードと前記暗号化インデックスの双方の反転されたビット数の合計以下である場合、前記暗号化キーワードが前記暗号化インデックスに含まれていると判定する、
前記（１１）または（１２）に記載の情報処理装置。
（１４）
前記通信制御部は、複数の前記暗号化キーワード、複数の前記暗号化キーワードに係る複数の反転ビット数情報、および論理条件を受信し、
前記ビット計算部は、複数の前記暗号化キーワードのそれぞれに関し、前記暗号化インデックスとの排他的論理和を計算して前記ビット計算結果および前記ビットカウント結果を取得し、
前記ビット一致判定部は、前記複数の暗号化キーワードと前記暗号化インデックスの双方の反転されたビット数の合計と、前記ビット計算結果との大小関係に基づいて、前記検索キーワードが前記検索インデックスに含まれているか否かをそれぞれ判定し、
前記通信制御部は、前記複数の暗号化キーワードに対応する判定が論理条件満たしている場合、検索結果を送信する、
前記（１１）に記載の情報処理装置。
（１５）

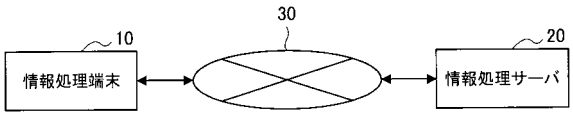
前記論理条件は、論理和条件であり、
前記通信制御部は、論理和条件に基づいて、前記複数の暗号化キーワードのうち、少なくとも１つの前記の暗号化キーワードが前記暗号化インデックスに含まれていると前記ビット一致判定部が判定した場合、前記複数の暗号化キーワードに対応する検索結果を送信する、
前記（１４）に記載の情報処理装置。
（１６）
前記論理条件は、論理積条件であり、
前記通信制御部は、論理積条件に基づいて、前記複数の暗号化キーワードのうち、全部の前記暗号化キーワードが前記暗号化インデックスに含まれていると前記ビット一致判定部が判定した場合、前記複数の暗号化キーワードに対応する検索結果を送信する、
前記（１４）に記載の情報処理装置。
（１７）
プロセッサが、
情報検索に係るキーワードから、鍵付ハッシングを用いて算出したハッシュ値を所定長のビット列にマッピングした暗号化ビット列を生成することと、
動的に生成された乱数に基づいて、前記暗号化ビット列から所定の数のビットを選択し、選択した前記所定の数のビットを反転することと、
反転したビットの数に係る反転ビット数情報および前記暗号化ビット列を外部装置に送信することと、
を含む、情報処理方法。
（１８）
プロセッサが、
クライアント端末から、暗号化キーワード、および前記暗号化キーワードの反転ビット数を示す反転ビット数情報を受信することと、
前記暗号化キーワードと保存する暗号化インデックスの排他的論理和を計算したビット計算結果と、前記ビット計算結果に対するビットカウント結果とを取得することと、
前記暗号化キーワードの反転ビット数および前記暗号化インデックスの反転ビット数の合計と、前記ビットカウント結果との大小関係の比較に基づいて、前記暗号化キーワードが前記暗号化インデックスに含まれているか否かを判定することと、
を含み、
前記暗号化キーワードおよび前記暗号化インデックスは、鍵付ハッシングを用いて算出されたハッシュ値を所定長のビット列にマッピングした後、動的に生成された乱数に基づいて所定の数のビットが反転された暗号化ビット列であり、
前記暗号化キーワードが前記暗号化インデックスに含まれていると判定した場合、前記暗号化キーワードに対応する検索結果を前記クライアント端末に送信する、
情報処理方法。
【符号の説明】
【０１０４】
１０　情報処理端末
１１　入力部
１２　抽出部
１３　暗号化部
１４　鍵管理部
１５　ビット反転部
１６　乱数生成部
１７　通信部
１８　出力部
１９　復号部
２０　情報処理サーバ

２１　　通信制御部
２２　　検索部
２３　　記憶部
２４　　ビット計算部
２５　　ビット一致判定部
３０　　ネットワーク

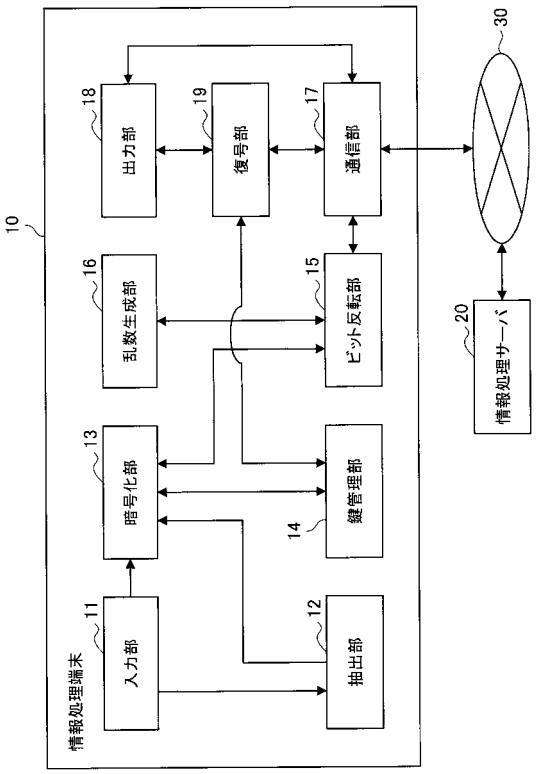
【図１】



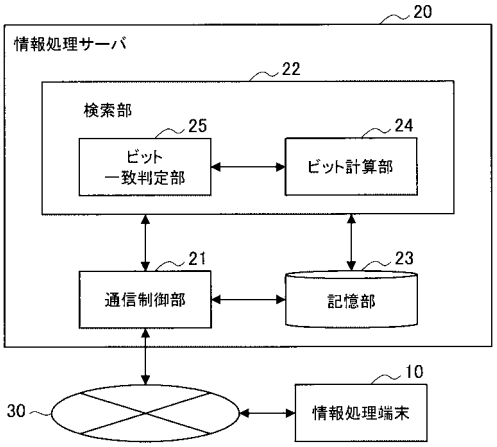
【図２】



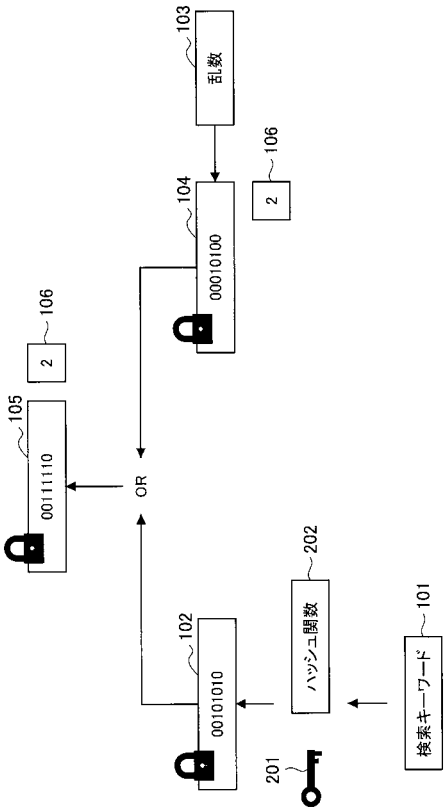
【図３】


10
情報処理端末
入力部
11
出力部
18
暗号化部
13
乱数生成部
16
復号部
19
鍵管理部
14
ビット反転部
15
抽出部
12
通信部
17
30
情報処理サーバ
20

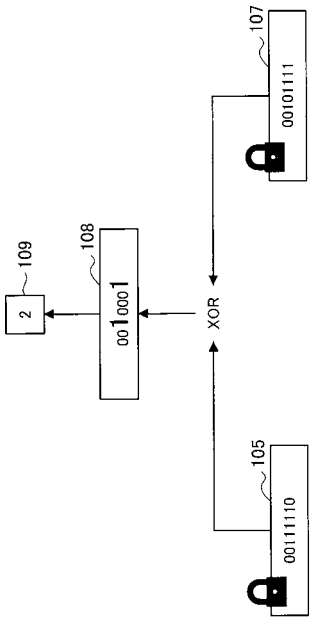
【図４】


20
情報処理サーバ
22
検索部
25
ビット
一致判定部
24
ビット計算部
21
通信制御部
23
記憶部
30
10
情報処理端末

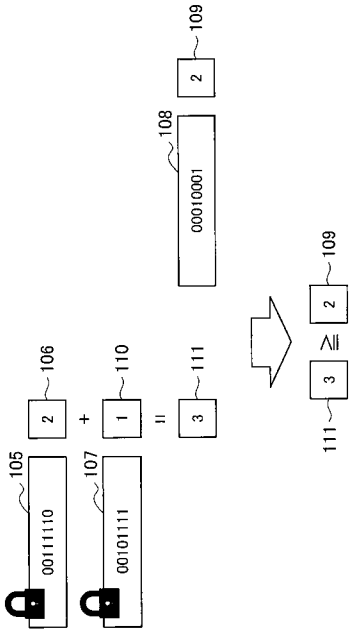
【図５】


103
乱数
106
2
104
00010100
106
2
105
00111110
OR
202
ハッシュ関数
101
検索キーワード
102
00101010
201

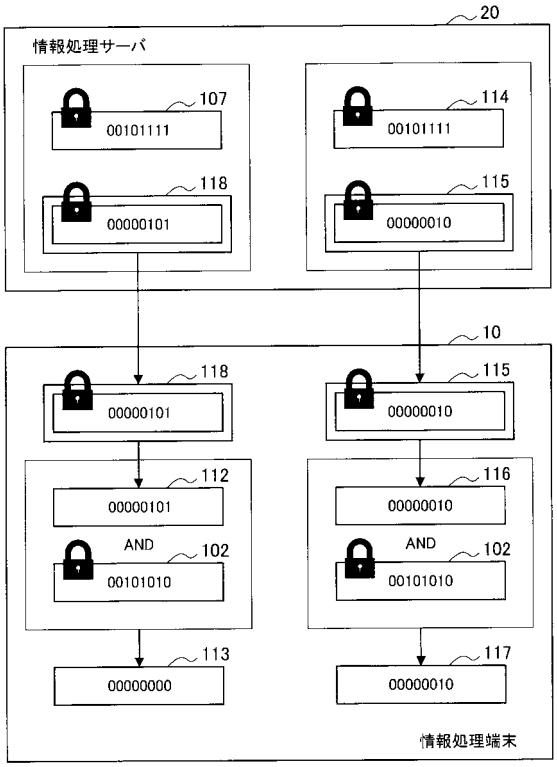
【図６】


107
00101111
109
2
108
001000 1
XOR
105
00111110

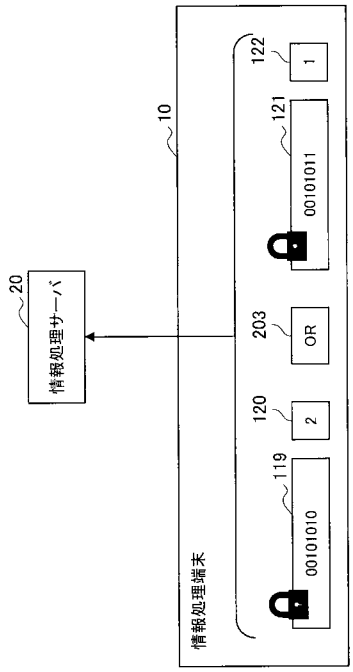
【図７】


109
2
108
00010001
106
2
+
110
1
=
111
3
105
00111110
107
00101111
≧
109
2
111
3

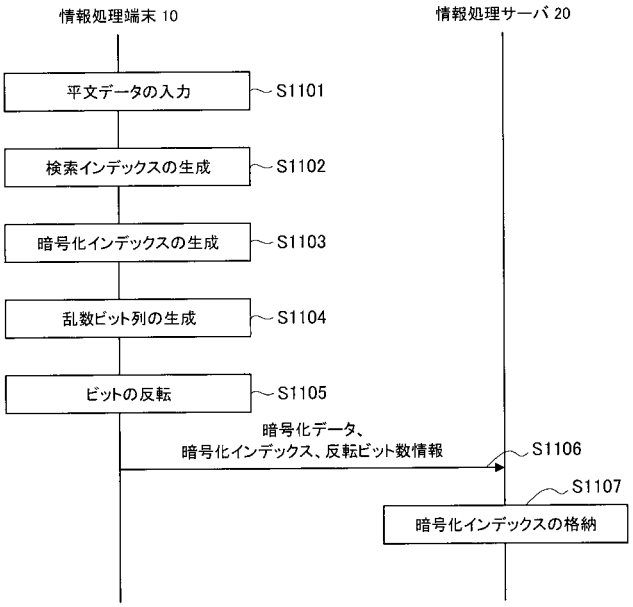
【図８】


20
情報処理サーバ
107
00101111
118
00000101
114
00101111
115
00000010
10
118
00000101
115
00000010
112
00000101
AND
102
00101010
116
00000010
AND
102
00101010
113
00000000
117
00000010
情報処理端末

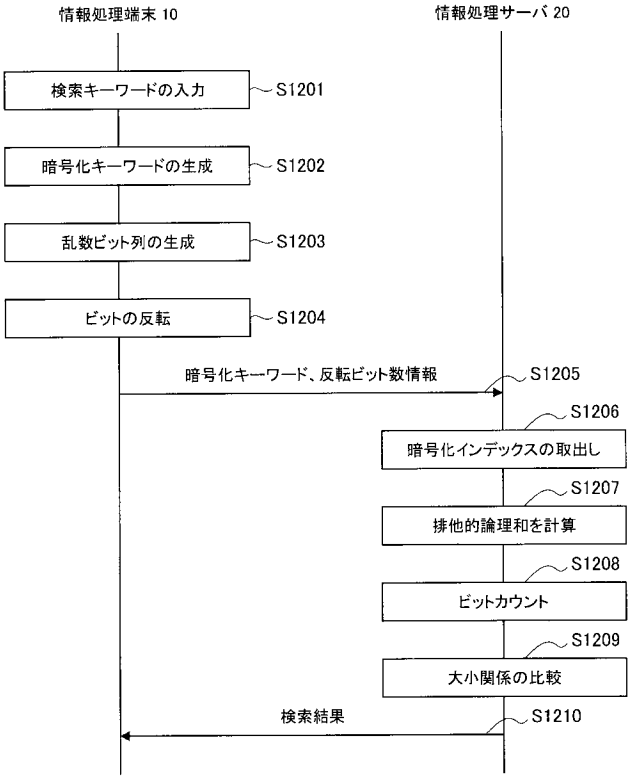
【図９】


20
情報処理サーバ
10
122
1
121
00101011
203
OR
120
2
119
00101010
情報処理端末

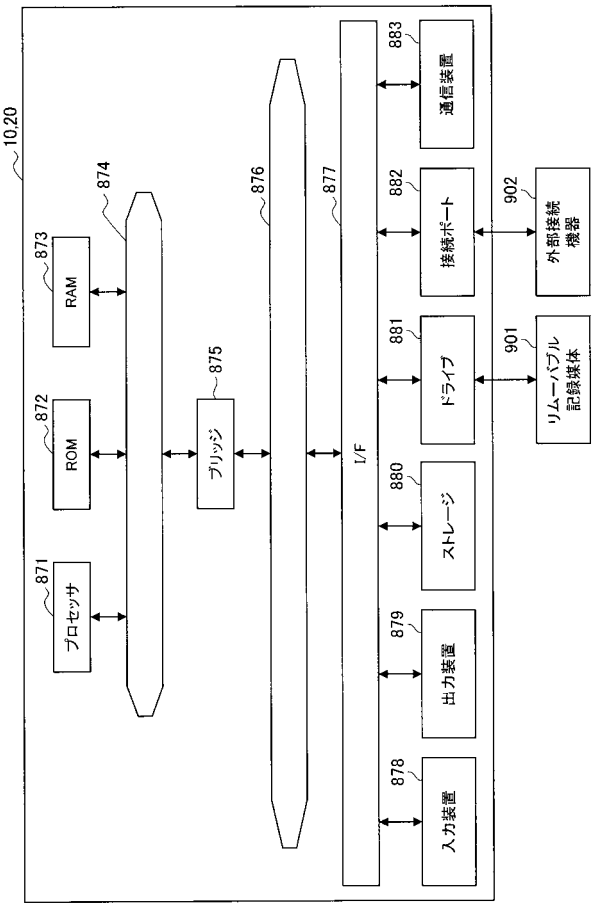
【図１０】


情報処理端末 10
情報処理サーバ 20
平文データの入力
S1101
検索インデックスの生成
S1102
暗号化インデックスの生成
S1103
乱数ビット列の生成
S1104
ビットの反転
S1105
暗号化データ、
暗号化インデックス、反転ビット数情報
S1106
S1107
暗号化インデックスの格納

【図１１】


情報処理端末 10
情報処理サーバ 20
検索キーワードの入力
S1201
暗号化キーワードの生成
S1202
乱数ビット列の生成
S1203
ビットの反転
S1204
暗号化キーワード、反転ビット数情報
S1205
S1206
暗号化インデックスの取出し
S1207
排他的論理和を計算
S1208
ビットカウント
S1209
大小関係の比較
検索結果
S1210

【図１２】


10,20
871
プロセッサ
872
ROM
873
RAM
874
875
ブリッジ
876
877
I/F
878
入力装置
879
出力装置
880
ストレージ
881
ドライブ
882
接続ポート
883
通信装置
901
リムーバブル記録媒体
902
外部接続機器

フロントページの続き

(72)発明者　丸山　信也
東京都港区港南１丁目７番１号　ソニー株式会社内
Ｆターム(参考) 5J104 AA16　EA18　JA03　NA02　NA12　PA14