【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】平成17年8月11日(2005.8.11)

【公開番号】特開2005-86747(P2005-86747A)
【公開日】平成17年3月31日(2005.3.31)
【年通号数】公開・登録公報2005-013
【出願番号】特願2003-319590(P2003-319590)
【国際特許分類第７版】
　Ｈ０４Ｌ　9/08
【ＦＩ】
　Ｈ０４Ｌ　9/00　６０１Ｂ
　Ｈ０４Ｌ　9/00　６０１Ｅ

【手続補正書】
【提出日】平成17年3月16日(2005.3.16)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
　暗号文生成処理を実行する情報処理装置であり、
　多分木構成の最下位ノードであるリーフに対応する複数の情報処理装置から暗号文提供対象として抽出した選択情報処理装置にのみ格納された鍵に基づく復号処理によって取得可能な暗号文からなる暗号文ブロック、および該暗号文ブロックを構成する暗号文に適用した暗号鍵情報としての鍵指定コードを、情報処理装置に対する提供情報として生成する処理を実行する構成を有し、
　前記鍵指定コードは、前記選択情報処理装置をリーフとした鍵指定木の構成ノード毎の鍵指定情報を含み、該鍵指定情報は、前記鍵指定木の構成ノードにおいて特定リーフの集合として定義される分割可能なサブセットを複数に分割した分割サブセットに対応するサブセットキーを適用した暗号文を前記暗号文ブロック中に含むか否かのサブセット分割識別情報を含む構成であることを特徴とする情報処理装置。
【請求項２】
　前記鍵指定情報は、
　前記鍵指定木の構成ノードがリーフに対応するか否かを示すリーフビット、
　前記ノードに定義されるサブセットに対応するサブセットキーを適用した暗号文を前記暗号文ブロック中に含むか否かを示す鍵指定ビットと、
　前記ノードにおいて定義される分割可能なサブセットを複数に分割した分割サブセットに対応するサブセットキーを適用した暗号文を前記暗号文ブロック中に含むか否かのサブセット分割識別情報としてのパーティションビットとを含む構成であることを特徴とする請求項１に記載の情報処理装置。
【請求項３】
　前記多分木は３分木構成であり、
　前記サブセット分割識別情報は、
　前記鍵指定木の構成ノードに対応して設定される１ビット情報であり、
　前記サブセット分割識別ビット情報０または１によって、前記暗号文ブロック中に、前記ノードに定義された分割可能なサブセットを複数に分割した分割サブセットに対応するサブセットキーを適用した暗号文を含むか、分割可能なサブセットに対応する１つのサブ

セットキーを適用した暗号文を持つかを示す構成であることを特徴とする請求項１に記載の情報処理装置。
【請求項４】
前記鍵指定情報は、さらに、
前記分割サブセットの分割態様を示す分割法指定情報を含む構成であることを特徴とする請求項１に記載の情報処理装置。
【請求項５】
前記鍵指定情報は、
ａ．前記鍵指定木の構成ノードに定義されるサブセットに対応するサブセットキーを適用した暗号文を前記暗号文ブロック中に含むか否かを示す鍵指定ビット、
ｂ．該構成ノードにおいて定義される分割可能なサブセットを複数に分割した分割サブセットに対応するサブセットキーを適用した暗号文を前記暗号文ブロック中に含むか否かのサブセット分割識別情報としてのパーティションビット、
ｃ．前記分割サブセットの分割態様を示す分割法指定情報ビット、
上記、ａ．鍵指定ビット、ｂ．パーティションビット、ｃ．分割法指定情報ビットの組み合わせを識別可能な符号化データとして構成した情報であることを特徴とする請求項１に記載の情報処理装置。
【請求項６】
前記情報処理装置は、
前記暗号文ブロックと、前記鍵指定コードと、さらに、
前記鍵指定コードに含まれる鍵指定情報のエンコード方法を識別可能とした鍵指定情報エンコード方法識別情報を情報処理装置に対する提供情報として生成する処理を実行する構成であることを特徴とする請求項１に記載の情報処理装置。
【請求項７】
暗号文復号処理を実行する情報処理装置であり、
多分木構成の最下位ノードであるリーフに対応する複数の情報処理装置から暗号文提供対象として抽出した選択情報処理装置にのみ格納された鍵に基づく復号処理によって取得可能な暗号文からなる暗号文ブロック、および該暗号文ブロックを構成する暗号文に適用した暗号鍵情報としての鍵指定コードを入力し、
前記鍵指定コードから前記選択情報処理装置をリーフとした鍵指定木の構成ノード毎の鍵指定情報を取得し、前記鍵指定情報から、特定リーフの集合として定義される分割可能なサブセットを複数に分割した分割サブセットに対応するサブセットキーを適用した暗号文が前記暗号文ブロックに含まれるか否かのサブセット分割識別情報を取得し、
該取得情報に基づいて、前記暗号文ブロックに含まれる暗号文から復号処理対象の暗号文選択処理を実行する構成を有することを特徴とする情報処理装置。
【請求項８】
前記鍵指定情報は、
前記鍵指定木の構成ノードがリーフに対応するか否かを示すリーフビット、
前記ノードに定義されるサブセットに対応するサブセットキーを適用した暗号文を前記暗号文ブロック中に含むか否かを示す鍵指定ビットと、
前記ノードにおいて定義される分割可能なサブセットを複数に分割した分割サブセットに対応するサブセットキーを適用した暗号文が前記暗号文ブロック中に含まれるか否かのサブセット分割識別情報としてのパーティションビットとを含み、
前記リーフビット、前記鍵指定ビット、および前記パーティションビットに基づいて、前記暗号文ブロックに含まれる暗号文から復号処理対象の暗号文選択処理を実行する構成を有することを特徴とする請求項７に記載の情報処理装置。
【請求項９】
前記多分木は３分木構成であり、
前記サブセット分割識別情報は、
前記鍵指定木の構成ノードに対応して設定される１ビット情報であり、

前記情報処理装置は、
前記サブセット分割識別ビット情報が０であるか１であるかによって、前記暗号文ブロック中に、前記ノードに定義された分割可能なサブセットを複数に分割した分割サブセットに対応するサブセットキーを適用した暗号文を含むか、分割可能なサブセットに対応する１つのサブセットキーを適用した暗号文を持つかを判定する構成であることを特徴とする請求項７に記載の情報処理装置。
【請求項１０】
前記情報処理装置は、
前記鍵指定情報の情報態様と各態様に対応する暗号文態様とを対応付けたテーブルを有し、該テーブルおよび前記取得情報に基づいて、前記暗号文ブロックに含まれる暗号文から復号処理対象の暗号文選択処理を実行する構成を有することを特徴とする請求項７に記載の情報処理装置。
【請求項１１】
前記鍵指定情報は、さらに、
前記分割サブセットの分割態様を示す分割法指定情報を含み、
前記情報処理装置は、
前記分割法指定情報に基づいて、分割サブセットの分割態様を判別し、該判別情報に基づいて、前記暗号文ブロックに含まれる暗号文から復号処理対象の暗号文選択処理を実行する構成を有することを特徴とする請求項７に記載の情報処理装置
【請求項１２】
前記鍵指定情報は、
ａ．前記鍵指定木の構成ノードに定義されるサブセットに対応するサブセットキーを適用した暗号文を前記暗号文ブロック中に含むか否かを示す鍵指定ビット、
ｂ．該構成ノードにおいて定義される分割可能なサブセットを複数に分割した分割サブセットに対応するサブセットキーを適用した暗号文を前記暗号文ブロック中に含むか否かのサブセット分割識別情報としてのパーティションビット、
ｃ．前記分割サブセットの分割態様を示す分割法指定情報ビット、
上記、ａ．鍵指定ビット、ｂ．パーティションビット、ｃ．分割法指定情報ビットの組み合わせを識別可能な符号化データとして構成した情報であり、
前記情報処理装置は、
前記符号化データに基づいて、前記暗号文ブロックに含まれる暗号文から復号処理対象の暗号文選択処理を実行する構成を有することを特徴とする請求項７に記載の情報処理装置。
【請求項１３】
前記情報処理装置は、
前記暗号文ブロックと、前記鍵指定コードと、さらに、
前記鍵指定コードに含まれる鍵指定情報のエンコード方法を識別可能とした鍵指定情報エンコード方法識別情報を入力し、
前記鍵指定情報エンコード方法識別情報に基づいて、前記鍵指定コードのエンコード方法を識別し、該識別結果に基づく鍵指定コードの解析により、前記暗号文ブロックに含まれる暗号文から復号処理対象としての暗号文の選択処理を実行する構成を有することを特徴とする請求項７に記載の情報処理装置。
【請求項１４】
情報記録媒体であり、
多分木構成の最下位ノードであるリーフに対応する複数の情報処理装置から暗号文提供対象として抽出した選択情報処理装置にのみ格納された鍵に基づく復号処理によって取得可能な暗号文からなる暗号文ブロックと、
前記暗号文ブロックを構成する暗号文に適用した暗号鍵情報としての鍵指定コードと、
を格納し、
前記鍵指定コードは、前記選択情報処理装置をリーフとした鍵指定木の構成ノード毎の

鍵指定情報を含み、該鍵指定情報は、前記鍵指定木の構成ノードにおいて特定リーフの集合として定義される分割可能なサブセットを複数に分割した分割サブセットに対応するサブセットキーを適用した暗号文を前記暗号文ブロック中に含むか否かのサブセット分割識別情報を含む構成であることを特徴とする情報記録媒体。

【請求項１５】

暗号文生成処理を実行する情報処理方法であり、

多分木構成の最下位ノードであるリーフに対応する複数の情報処理装置から暗号文提供対象として抽出した選択情報処理装置にのみ格納された鍵に基づく復号処理によって取得可能な暗号文からなる暗号文ブロックの生成ステップと、

前記暗号文ブロックを構成する暗号文に適用した暗号鍵情報としての鍵指定コードを生成する鍵指定コード生成ステップとを有し、

前記鍵指定コード生成ステップは、

前記選択情報処理装置をリーフとした鍵指定木の構成ノード毎の鍵指定情報として、前記鍵指定木の構成ノードにおいて特定リーフの集合として定義される分割可能なサブセットを複数に分割した分割サブセットに対応するサブセットキーを適用した暗号文を前記暗号文ブロック中に含むか否かのサブセット分割識別情報を設定するサブセット分割識別情報設定ステップを含むことを特徴とする情報処理方法。

【請求項１６】

前記鍵指定コード生成ステップは、

前記鍵指定情報として、

前記鍵指定木の構成ノードがリーフに対応するか否かを示すリーフビット、

前記ノードに定義されるサブセットに対応するサブセットキーを適用した暗号文を前記暗号文ブロック中に含むか否かを示す鍵指定ビットと、

前記ノードにおいて定義される分割可能なサブセットを複数に分割した分割サブセットに対応するサブセットキーを適用した暗号文を前記暗号文ブロック中に含むか否かのサブセット分割識別情報としてのパーティションビットとを設定するステップを含むことを特徴とする請求項１５に記載の情報処理方法。

【請求項１７】

前記多分木は３分木構成であり、

前記鍵指定コード生成ステップは、

前記鍵指定情報に設定する前記サブセット分割識別情報を、

前記鍵指定木の構成ノードに対応して設定される１ビット情報として設定し、

前記サブセット分割識別ビット情報０または１によって、前記暗号文ブロック中に、前記ノードに定義された分割可能なサブセットを複数に分割した分割サブセットに対応するサブセットキーを適用した暗号文を含むか、分割可能なサブセットに対応する１つのサブセットキーを適用した暗号文を持つかを示す情報ビットとして設定することを特徴とする請求項１５に記載の情報処理方法。

【請求項１８】

前記鍵指定コード生成ステップは、

前記鍵指定情報として、さらに、

前記分割サブセットの分割態様を示す分割法指定情報を設定するステップを含むことを特徴とする請求項１５に記載の情報処理方法。

【請求項１９】

前記鍵指定コード生成ステップは、

ａ．前記鍵指定木の構成ノードに定義されるサブセットに対応するサブセットキーを適用した暗号文を前記暗号文ブロック中に含むか否かを示す鍵指定ビット、

ｂ．該構成ノードにおいて定義される分割可能なサブセットを複数に分割した分割サブセットに対応するサブセットキーを適用した暗号文を前記暗号文ブロック中に含むか否かのサブセット分割識別情報としてのパーティションビット、

ｃ．前記分割サブセットの分割態様を示す分割法指定情報ビット、

上記、ａ．鍵指定ビット、ｂ．パーティションビット、ｃ．分割法指定情報ビットの組み合わせを識別可能な符号化データを前記鍵指定情報として生成する処理を含むことを特徴とする請求項１５に記載の情報処理方法。

【請求項２０】

前記情報処理方法は、

前記暗号文ブロックと、前記鍵指定コードと、さらに、

前記鍵指定コードに含まれる鍵指定情報のエンコード方法を識別可能とした鍵指定情報エンコード方法識別情報を情報処理装置に対する提供情報として生成するステップを有することを特徴とする請求項１５に記載の情報処理方法。

【請求項２１】

暗号文復号処理を実行する情報処理方法であり、

多分木構成の最下位ノードであるリーフに対応する複数の情報処理装置から暗号文提供対象として抽出した選択情報処理装置にのみ格納された鍵に基づく復号処理によって取得可能な暗号文からなる暗号文ブロック、および該暗号文ブロックを構成する暗号文に適用した暗号鍵情報としての鍵指定コードを入力するステップと、

前記鍵指定コードから前記選択情報処理装置をリーフとした鍵指定木の構成ノード毎の鍵指定情報を取得し、前記鍵指定情報から、特定リーフの集合として定義される分割可能なサブセットを複数に分割した分割サブセットに対応するサブセットキーを適用した暗号文が前記暗号文ブロックに含まれるか否かのサブセット分割識別情報を取得する鍵指定コード解析ステップと、

前記鍵指定コード解析ステップにおいて取得した取得情報に基づいて、前記暗号文ブロックに含まれる暗号文から復号処理対象の暗号文選択処理を実行するステップと、

を有することを特徴とする情報処理方法。

【請求項２２】

前記鍵指定情報は、

前記鍵指定木の構成ノードがリーフに対応するか否かを示すリーフビット、

前記ノードに定義されるサブセットに対応するサブセットキーを適用した暗号文を前記暗号文ブロック中に含むか否かを示す鍵指定ビットと、

前記ノードにおいて定義される分割可能なサブセットを複数に分割した分割サブセットに対応するサブセットキーを適用した暗号文が前記暗号文ブロック中に含まれるか否かのサブセット分割識別情報としてのパーティションビットとを含み、

前記鍵指定コード解析ステップは、

前記リーフビット、前記鍵指定ビット、および前記パーティションビットに基づいて、前記暗号文ブロックに含まれる暗号文から復号処理対象の暗号文選択に必要な情報の取得処理を実行するステップであることを特徴とする請求項２１に記載の情報処理方法。

【請求項２３】

前記多分木は３分木構成であり、

前記サブセット分割識別情報は、

前記鍵指定木の構成ノードに対応して設定される１ビット情報であり、

前記鍵指定コード解析ステップは、

前記サブセット分割識別ビット情報が０であるか１であるかによって、前記暗号文ブロック中に、前記ノードに定義された分割可能なサブセットを複数に分割した分割サブセットに対応するサブセットキーを適用した暗号文を含むか、分割可能なサブセットに対応する１つのサブセットキーを適用した暗号文を持つかを判定するステップを含むことを特徴とする請求項２１に記載の情報処理方法。

【請求項２４】

前記鍵指定コード解析ステップは、

前記鍵指定情報の情報態様と各態様に対応する暗号文態様とを対応付けたテーブルに基づいて、前記暗号文ブロックに含まれる暗号文から復号処理対象の暗号文選択に必要な情報を取得する処理を実行するステップを含むことを特徴とする請求項２１に記載の情報処

理方法。
【請求項２５】
前記鍵指定情報は、さらに、
前記分割サブセットの分割態様を示す分割法指定情報を含み、
前記鍵指定コード解析ステップは、
前記分割法指定情報に基づいて、分割サブセットの分割態様を判別し、該判別情報に基づいて、前記暗号文ブロックに含まれる暗号文から復号処理対象の暗号文選択に必要な情報を取得する処理を実行するステップを含むことを特徴とする請求項２１に記載の情報処理方法。
【請求項２６】
前記鍵指定情報は、
ａ．前記鍵指定木の構成ノードに定義されるサブセットに対応するサブセットキーを適用した暗号文を前記暗号文ブロック中に含むか否かを示す鍵指定ビット、
ｂ．該構成ノードにおいて定義される分割可能なサブセットを複数に分割した分割サブセットに対応するサブセットキーを適用した暗号文を前記暗号文ブロック中に含むか否かのサブセット分割識別情報としてのパーティションビット、
ｃ．前記分割サブセットの分割態様を示す分割法指定情報ビット、
上記、ａ．鍵指定ビット、ｂ．パーティションビット、ｃ．分割法指定情報ビットの組み合わせを識別可能な符号化データとして構成した情報であり、
前記鍵指定コード解析ステップは、
前記符号化データに基づいて、前記暗号文ブロックに含まれる暗号文から復号処理対象の暗号文選択に必要な情報を取得する処理を実行するステップを含むことを特徴とする請求項２１に記載の情報処理方法。
【請求項２７】
暗号文生成処理を実行するコンピュータ・プログラムであり、
多分木構成の最下位ノードであるリーフに対応する複数の情報処理装置から暗号文提供対象として抽出した選択情報処理装置にのみ格納された鍵に基づく復号処理によって取得可能な暗号文からなる暗号文ブロックの生成ステップと、
前記暗号文ブロックを構成する暗号文に適用した暗号鍵情報としての鍵指定コードを生成する鍵指定コード生成ステップとを有し、
前記鍵指定コード生成ステップは、
前記選択情報処理装置をリーフとした鍵指定木の構成ノード毎の鍵指定情報として、前記鍵指定木の構成ノードにおいて特定リーフの集合として定義される分割可能なサブセットを複数に分割した分割サブセットに対応するサブセットキーを適用した暗号文を前記暗号文ブロック中に含むか否かのサブセット分割識別情報を設定するサブセット分割識別情報設定ステップを含むことを特徴とするコンピュータ・プログラム。
【請求項２８】
暗号文復号処理を実行するコンピュータ・プログラムであり、
多分木構成の最下位ノードであるリーフに対応する複数の情報処理装置から暗号文提供対象として抽出した選択情報処理装置にのみ格納された鍵に基づく復号処理によって取得可能な暗号文からなる暗号文ブロック、および該暗号文ブロックを構成する暗号文に適用した暗号鍵情報としての鍵指定コードを入力するステップと、
前記鍵指定コードから前記選択情報処理装置をリーフとした鍵指定木の構成ノード毎の鍵指定情報を取得し、前記鍵指定情報から、特定リーフの集合として定義される分割可能なサブセットを複数に分割した分割サブセットに対応するサブセットキーを適用した暗号文が前記暗号文ブロックに含まれるか否かのサブセット分割識別情報を取得する鍵指定コード解析ステップと、
前記鍵指定コード解析ステップにおいて取得した取得情報に基づいて、前記暗号文ブロックに含まれる暗号文から復号処理対象の暗号文選択処理を実行するステップと、
を有することを特徴とするコンピュータ・プログラム。