

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第4161859号
(P4161859)

(45) 発行日 平成20年10月8日 (2008. 10. 8)

(24) 登録日 平成20年8月1日 (2008. 8. 1)

(51) Int. Cl. F I
H04L 9/08 (2006.01)
H04L 9/00 G01B
H04L 9/00 G01E

請求項の数 27 (全 51 頁)

(21) 出願番号	特願2003-319590 (P2003-319590)	(73) 特許権者	000002185
(22) 出願日	平成15年9月11日 (2003. 9. 11)		ソニー株式会社
(65) 公開番号	特開2005-86747 (P2005-86747A)		東京都港区港南1丁目7番1号
(43) 公開日	平成17年3月31日 (2005. 3. 31)	(74) 代理人	100093241
審査請求日	平成17年3月16日 (2005. 3. 16)		弁理士 宮田 正昭
		(74) 代理人	100101801
			弁理士 山田 英治
		(74) 代理人	100086531
			弁理士 澤田 俊夫
		(72) 発明者	浅野 智之
			東京都品川区北品川6丁目7番35号 ソニー株式会社内
		審査官	速水 雄太

最終頁に続く

(54) 【発明の名称】 情報処理装置、情報記録媒体、および情報処理方法、並びにコンピュータ・プログラム

(57) 【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

10

20

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。

10

【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。

20

【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。

30

【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、

40

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

50

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

10

20

30

40

50

徴とする請求項 7 に記載の情報処理装置。

【請求項 14】

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。

10

【請求項 15】

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、

20

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 14 に記載の情報処理方法。

【請求項 16】

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 14 に記載の情報処理方法。

30

【請求項 17】

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 14 に記載の情報処理方法。

【請求項 18】

40

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 14 に記載の情報処理方法。

50

【請求項 19】

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 14 に記載の情報処理方法。

【請求項 20】

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 21】

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 20 に記載の情報処理方法。

【請求項 22】

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 20 に記載の情報処理方法。

【請求項 23】

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 20 に記載の情報処理方法。

【請求項 24】

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 20 に記載の情報処理方法。

【請求項 25】

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 20 に記載の情報処理方法。

【請求項 26】

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 27】

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。

【発明の詳細な説明】

【技術分野】

【0001】

10

20

30

40

50

本発明は、情報処理装置、情報記録媒体、および情報処理方法、並びにコンピュータ・プログラムに関する。さらに、詳細には、木構造を適用した情報配信構成において、様々なサブセット、すなわち、ユーザデバイスとしての情報処理装置の集合を規定した様々なタイプのサブセットを設定した情報配信を可能とするとともに、情報処理装置側で効率的に自己の複合可能な暗号文を選択することを可能とした情報処理装置、情報記録媒体、および情報処理方法、並びにコンピュータ・プログラムに関する。

【背景技術】

【0002】

昨今、音楽等のオーディオデータ、映画等の画像データ、ゲームプログラム、各種アプリケーションプログラム等、様々なソフトウェアデータ（以下、これらをコンテンツ（Content）と呼ぶ）が、インターネット等のネットワークを介して、あるいはC D (Compact Disc)、D V D (Digital Versatile Disk)、M D (Mini Disk)等の情報記録媒体（メディア）を介して流通している。これらの流通コンテンツは、ユーザの所有するP C (Personal Computer)、C D プレーヤ、D V D プレーヤ、M D プレーヤ等の再生装置、あるいはゲーム機器等の様々な情報処理装置において再生され利用される。

10

【0003】

音楽データ、画像データ等、多くのコンテンツは、一般的にその作成者あるいは販売者に頒布権等が保有されている。従って、これらのコンテンツの配布に際しては、一定の利用制限、すなわち、正規なユーザに対してのみ、コンテンツの利用を許諾し、許可のない複製等が行われないようにする構成をとるのが一般的となっている。

20

【0004】

特に、近年においては、情報をデジタル的に記録する記録装置や記憶媒体が普及しつつある。このようなデジタル記録装置および記憶媒体によれば、例えば画像や音声を劣化させることなく記録、再生を繰り返すことが可能であり、不正コピーコンテンツのインターネットを介した配信や、C D - R 等の記録媒体に対する不正コピーという問題が発生している。

【0005】

このようなコンテンツの不正利用を防止する1つの方式として、コンテンツあるいは暗号化コンテンツを復号するための鍵を暗号化して配布し、特定の正規ユーザまたは正規デバイスのみが、配布データの復号を可能としたシステムがある。例えばブロードキャストエンクリプション（Broadcast Encryption）方式の一態様である階層型木構造を適用した構成が知られている。

30

【0006】

階層型木構造を適用した暗号鍵等の暗号データ提供処理について、図を参照して説明する。

【0007】

図1に示す階層型木構造は2分木を用いており、その最下層が葉（リーフ）と呼ばれ、頂点、各分岐部およびリーフを含む部分をノードと称する。なお、頂点をルート、あるいはルートノードと呼ぶ。図1に示す2分木階層型木構造において、リーフは8～15、ノードは1～15、ルートは1である。

40

【0008】

この2分木階層型木構造におけるリーフ8～15にコンテンツの利用機器としての再生機、受信機等の情報処理装置を1つずつ割り当てる。

【0009】

また、木の各ノード（リーフを含む）1～15にそれぞれノードキーを1つずつ割り当てる。リーフ8～15に割り当てるノードキーはリーフキーと呼ばれる場合もある。

【0010】

リーフに対応する各情報処理装置には、対応するリーフからルートまでの経路にあるノードに割り当てられたノードキーが与えられる。図1の構成では、リーフ8から15までに割り当てられた8台の情報処理装置があり、ノード1から15までにそれぞれノードキ

50

ーが割り当てられており、リーフ 8 に対応する情報処理装置 101 には、ノード 1, 2, 4, 8 に割り当てられた 4 個のノードキーが与えられる。また、リーフ 12 に対応する情報処理装置 102 には、ノード 1, 3, 6, 12 に割り当てられた 4 個のノードキーが与えられる。各情報処理装置は、これらのノードキーを安全に保管する。

【0011】

このノードキーの配布処理を伴うセッティングを用いて、選択した情報処理装置のみが取得可能な情報を送信する方法を図 2 を参照して説明する。たとえば、特定の音楽、画像データ等のコンテンツを暗号化した暗号化コンテンツをブロードキャスト配信、あるいは DVD 等の記録媒体に格納して誰でも取得可能な状態で流通させ、その暗号化コンテンツを復号するための鍵（コンテンツキー Kc）を特定のユーザ、すなわち正規なコンテンツ利用権を持つユーザまたは情報処理装置にのみ提供する構成を想定する。

10

【0012】

図 2 に示すリーフ 14 に割り当てられた情報処理装置を不正な機器として、排除（リボーク）し、それ以外の情報処理装置が正規な情報処理装置であるとする。この場合、リーフ 14 に割り当てられた情報処理装置ではコンテンツキー Kc を取得できないが、他の情報処理装置ではコンテンツキー Kc を取得できる暗号文を生成して、その暗号文をネットワークを介してあるいは記録媒体に格納して配布する。

【0013】

この場合、リボーク（排除）される情報処理装置が持つノードキー（図 2 では×印で表現）以外のノードキーのうち、できるだけ多数の情報処理装置に共有されているもの、すなわち木の上部にあるものをいくつか用いて、コンテンツキーを暗号化して送信すればよい。

20

【0014】

図 2 に示す例では、ノード 2, 6, 15 のノードキーを用いて、コンテンツキー Kc を暗号化した暗号文のセットを生成して提供する。すなわち、

$$E(NK_2, Kc), E(NK_6, Kc), E(NK_{15}, Kc)$$

の暗号文を生成して、ネットワーク配信あるいは記録媒体に格納して提供する。なお、 $E(A, B)$ はデータ B を鍵 A で暗号化したデータを意味する。また NK_n は、図に示す第 n 番のノードキーを意味する。従って、上記式は、

コンテンツキー Kc をノードキー NK_2 で暗号化した暗号化データ $E(NK_2, Kc)$ と、コンテンツキー Kc をノードキー NK_6 で暗号化した暗号化データ $E(NK_6, Kc)$ と、コンテンツキー Kc をノードキー NK_{15} で暗号化した暗号化データ $E(NK_{15}, Kc)$ と、を含む 3 つの暗号文のセットであることを意味している。

30

【0015】

上記 3 つの暗号文を作り、例えば同報通信路を用いて全情報処理装置に送信すれば、リボーク対象でない情報処理装置（図 2 示すリーフ 8～13 および 15 に対応する情報処理装置）はいずれかの暗号文を自分が持つノードキーで復号することが可能であり、コンテンツキー Kc を得ることができる。しかし、リボーク（排除）されたリーフ 14 に対応する情報処理装置は、上記の 3 つの暗号文に適用された 3 つのノードキー NK_2 、 NK_6 、 NK_{15} のいずれも保有していないので、この暗号文を受領しても、復号処理を行うことができずコンテンツキー Kc を得ることはできない。

40

【0016】

ところで、上述した処理において、3 つの暗号文 $E(NK_2, Kc)$ 、 $E(NK_6, Kc)$ 、 $E(NK_{15}, Kc)$ が各情報処理装置に提供されることになるが、リボークされていない各情報処理装置は、自分がどの暗号文を復号できるのかを調べ、その復号可能な暗号文を選択して復号処理を行う得ることが必要となる。上述の例では 3 つの暗号文の設定であるが、実際には、情報処理装置の数は膨大な数となり、情報処理装置に提供される暗号文の数も大量となる。従って、暗号文の先頭から順次、復号処理を繰り返し実行してみるといった処理は負担が大きくなる。

【0017】

50

このため、暗号文の提供時に、各情報処理装置が選択すべき暗号文を知ることが可能な鍵指定コードを暗号文とともに各情報処理装置に提供する構成が提案されている。この構成については、例えば特許文献1に詳細が記述されている。

【0018】

鍵指定コードを暗号文とともに各情報処理装置に提供する構成について、図3を参照して説明する。図3に示すように、暗号化に用いられたノードキーを木構造を用いて表し、その構造をコード化して鍵指定コードを作り、これを暗号文ブロックとともに同報送信する。情報処理装置は鍵指定コードを受領し、受領した鍵指定コードを解析することで自分がどの暗号文をどのノードキーを用いて復号すればよいかを知り、効率的に復号処理を行うことが可能となる。

10

【0019】

鍵指定コードについて、説明する。図3は、先の図2と同様、リボーク（排除）機器をリーフ14に対応する情報処理装置として、3つの暗号文、

$E(NK_2, Kc)$, $E(NK_6, Kc)$, $E(NK_{15}, Kc)$

を送信する場合の例を示している。

【0020】

まず、図3において、太線で示した部分木は、暗号化に用いられたノードキーが割り当てられたすべてのノード121, 122, 123をリーフとし、もとの木構造のルート120をルートとする木であり、これを鍵指定木と呼ぶ。

【0021】

鍵指定木の構造をデータで示すため、各ノードから、左右に枝が出ているかどうかを表す情報を設定する。

20

【0022】

1つのノードにつき2ビットの情報（鍵指定情報）[00] [01] [10] [11]のいずれかを用いて表現する。すなわち、あるノードにつけられた鍵指定情報の最初（左側）のビットが[1]ならばそのノードから左に枝が出ている（鍵指定木に左側の子ノードが存在する）ことを示し、[0]ならばそのノードから左に枝は出していない（左側の子ノードは存在しない）ことを示す。鍵指定情報の最後（右側）は、同様に右側の枝の情報を表す。

【0023】

すなわち、あるノードの鍵指定情報ビットが[11]であればそのノードから両側に枝が出ていることを示し、[01]であれば左側のみに、[10]であれば右側のみに枝が出ていることを示す。また[00]は枝はいずれも出ておらず、そのノードが鍵指定木のリーフであることを示す。

30

【0024】

すなわち、各ノードにおいて、左右に鍵指定木の枝があるか否かを2ビットの情報で示し、枝がある場合を[1]ない場合を[0]として、

左右とも枝ありの場合：[11]

左にのみ枝ありの場合：[10]

右にのみ枝ありの場合：[01]

左右に枝なしの場合：[00]

として鍵指定情報ビットを設定する。

40

【0025】

この鍵指定情報ビットを鍵指定木の上位層から順に、かつ同層については左から順に並べて、鍵指定コードを設定する。図3に示す構成の場合、鍵指定木は、ノードNo. 1, 2, 3, 6, 7, 15によって構成されているので、これらの各ノードの鍵指定情報ビットを順に並べたデータ、すなわち、

[110011000100]

が、鍵指定コードとして設定される。

【0026】

50

上述した例は、2分木ツリー構成における例であるが、3分木等、任意の分木数（a）を持つa分木ツリーなどの多分木構成の場合についても、同様の鍵指定コードの設定が行われる。

【0027】

図4にa分木ツリーの構成例として3分木構成を示す。3分木のリーフに受信機、再生機、PCなどのコンテンツ利用機器としての情報処理装置を1つずつ割り当てる。図4に示す例は、分木数a=3、総情報処理装置数N=27の例である。

【0028】

各情報処理装置は、それが割り当てられたリーフ番号jを用いて、 u_j として表現する。ただしj=14, 15, ..., 40である。また、木の各内部ノード（リーフ以外のノード）kについて、以下の $2^a - 2$ 個のサブセットを定める。

【数1】

$$S_{k,b_1b_2\dots b_a}$$

$$\text{ただし、} b_i \in \{0,1\}, \sum_{i=1}^a b_i \neq 0, \sum_{i=1}^a b_i \neq a$$

10

20

以下、簡潔に説明するため、 $b_1 b_2 \dots b_a$ をBと表す。

【0029】

a=3の例では、 $2^a - 2 = 6$ であり、各内部ノードkについて、

$S_{k, 100}, S_{k, 010}, S_{k, 001}, S_{k, 110}, S_{k, 101}, S_{k, 011}$

の6個のサブセットを定める。

さらにルート（ノード1）についてのみ、サブセット $S_{1, 111}$ を定める。

30

【0030】

各サブセット

【数2】

$$S_{k,b_1b_2b_3}$$

40

は、ノードkの子ノードのうち左からi番目のものの子孫である情報処理装置を構成要素とする集合である。たとえば図4の例では、ノード1に規定される7つのサブセット $S_{1, 111}, S_{1, 100}, S_{1, 010}, S_{1, 001}, S_{1, 110}, S_{1, 101}, S_{1, 011}$ 中、の2つを例とすると、

$$S_{1, 111} = \{u_{14}, u_{15}, \dots, u_{40}\}$$

$$S_{1, 100} = \{u_{14}, u_{15}, \dots, u_{22}\}$$

50

である。

すなわち、 $S_{1, 111}$ は、すべてのリーフを含む集合である。

$S_{1, 100}$ は、ルートノードの左端の枝に属するリーフを含む集合である。

【0031】

また、ノード5に規定される6つのサブセット $S_{5, 100}$, $S_{5, 010}$, $S_{5, 001}$, $S_{5, 110}$, $S_{5, 101}$, $S_{5, 001}$ 中、の1つを例とすると、

$S_{5, 101} = \{u_{14}, u_{16}\}$

である。

すなわち、 $S_{5, 101}$ は、ノード5の左端および右端の枝に属するリーフを含む集合である。

10

【0032】

それぞれのサブセット $S_{k, B}$ に対して、サブセットキー $[SK_{k, B}]$ がひとつずつ割り当てられ、各情報処理装置は自分が所属するサブセットのサブセットキーを与えられ、秘密に保管する。

【0033】

たとえば、図4の例において、情報処理装置 u_{14} は、 $S_{1, 100}$, $S_{1, 110}$, $S_{1, 101}$, $S_{1, 111}$, $S_{2, 100}$, $S_{2, 110}$, $S_{2, 101}$, $S_{5, 100}$, $S_{5, 110}$, $S_{5, 101}$ の10個のサブセットに所属するので、それぞれのサブセットキーを与えられる。

【0034】

20

すなわち、10個のサブセット $S_{1, 100}$, $S_{1, 110}$, $S_{1, 101}$, $S_{1, 111}$, $S_{2, 100}$, $S_{2, 110}$, $S_{2, 101}$, $S_{5, 100}$, $S_{5, 110}$, $S_{5, 101}$ に対応する10個のサブセットキー $SK_{1, 100}$, $SK_{1, 110}$, $SK_{1, 101}$, $SK_{1, 111}$, $SK_{2, 100}$, $SK_{2, 110}$, $SK_{2, 101}$, $SK_{5, 100}$, $SK_{5, 110}$, $SK_{5, 101}$ を情報処理装置にセキュアに格納している。

【0035】

このサブセットキーの情報処理装置に対する配布を伴うセッティングの後、例えばコンテンツ管理者等が選択した情報処理装置のみが取得可能な情報、例えばコンテンツキーを提供する方法を図5を参照して説明する。

【0036】

30

いま、情報処理装置 $u_{14} \sim u_{40}$ の中から、 u_{27} , u_{28} , u_{33} , u_{36} , u_{37} , u_{38} , u_{39} , u_{40} (図5中の×印) をリボークし、それ以外の情報処理装置に情報(たとえば、コンテンツキー K_c)を送信するものとする。この場合、リボークされる情報処理装置が割り当てられたリーフからルートへの枝をすべて消すと、1つ以上の、それぞれ分離した部分木(図で太線で示す)が残る。それぞれの部分木には、その部分木のルートにおいて定義された1つのサブセットが対応しており、そのサブセットに対応するサブセットキーを用いてコンテンツキーを暗号化して暗号文ブロックを構成し同報送信する。

【0037】

図5の構成を持つ部分木は、図に示すように、部分木131, 132, 133, 134, 135の5つの部分木であり、これら5つの部分木のルートは、ノード(1, 3, 9, 11, 12)である。従って、図5の例では、コンテンツキーの提供者としての送信者は、これらの部分木のルートにおいて定義された各部分木に対応する1つのサブセットに対応するサブセットキーを適用して暗号文ブロックを生成する。

40

【0038】

すなわち、図5の例では、コンテンツキーの提供者としての送信者は、

$E(SK_{1, 100}, K_c)$, $E(SK_{3, 101}, K_c)$, $E(SK_{9, 100}, K_c)$, $E(SK_{11, 101}, K_c)$, $E(SK_{12, 100}, K_c)$

の5つの暗号文をノードの番号順に並べたものを暗号文ブロックとし、送信する。この5つの暗号文の暗号化に適用したサブセットキー、すなわち、

50

$SK_{1,100}$, $SK_{3,101}$, $SK_{9,100}$, $SK_{11,101}$, $SK_{12,100}$, のいずれかを保有する情報処理装置のみが、暗号文を復号してコンテンツキー K_c を取得できることになる。

【0039】

図5に示す例では、部分木131, 132, 133, 134, 135の5つの部分木に属する情報処理装置の各々は、サブセットキー $SK_{1,100}$, $SK_{3,101}$, $SK_{9,100}$, $SK_{11,101}$, $SK_{12,100}$, のいずれかを保持しており、コンテンツキー K_c を取得することができる。

【0040】

すなわち、

(1) 部分木131に属する $u_{14} \sim u_{22}$ は、サブセットキー $SK_{1,100}$ を有しており、暗号文 $E(SK_{1,100}, K_c)$ を復号してコンテンツキー K_c を取得できる。

(2) 部分木132に属する $u_{23} \sim u_{25}$ 、 $u_{29} \sim u_{31}$ はサブセットキー $SK_{3,101}$ を有しており、暗号文 $E(SK_{3,101}, K_c)$ を復号してコンテンツキー K_c を取得できる。

(3) 部分木133に属する u_{26} は、サブセットキー $SK_{9,100}$ を有しており、暗号文 $E(SK_{9,100}, K_c)$ を復号してコンテンツキー K_c を取得できる。

(4) 部分木134に属する u_{32} 、 u_{34} は、サブセットキー $SK_{11,101}$ を有しており、暗号文 $E(SK_{11,101}, K_c)$ を復号してコンテンツキー K_c を取得できる。

(5) 部分木135に属する u_{35} は、サブセットキー $SK_{12,100}$ を有しており、暗号文 $E(SK_{12,100}, K_c)$ を復号してコンテンツキー K_c を取得できる。

【0041】

一方、リボークされた情報処理装置 u_{27} , u_{28} , u_{33} , u_{36} , u_{37} , u_{38} , u_{39} , u_{40} (図5中の×印) は、サブセットキー $SK_{1,100}$, $SK_{3,101}$, $SK_{9,100}$, $SK_{11,101}$, $SK_{12,100}$, のいずれも保持しておらず、コンテンツキー K_c を取得できない。

【0042】

ところで、上述の処理においても、リボークされていない情報処理装置は、自分がどの暗号文を復号すべきかを知る必要があり、前述の2分木構成と同様の鍵指定コードを作り、これを暗号文ブロックとともに同報送信する。情報処理装置は鍵指定コードを受信し、それを解析することで自分がどの暗号文をどのノードキーを用いて復号すればよいかを知り、復号処理を行う。

【0043】

3分木構成における鍵指定コードについて、図6を参照して説明する。図6において、太線で示された木は、鍵指定木であり、暗号化に用いられたサブセットキーに対応するサブセットが定義されたすべてのノード(1, 3, 9, 11, 12)を接続し、もとの木構造のルート(1)をルートとして設定し、これが鍵指定木となる。

【0044】

鍵指定木の構造を、そのルートから、左から i 番目の子に対して枝が出ているかどうかを表す1つのノードにつき3ビットの情報(チャイルドビット: *Child bit*)と、そのノードで定義されたサブセットキーが暗号化に用いられている場合にその種類を示す3ビットの情報(鍵指定ビット: *Key Specify Bit*)から成る、合計6ビットの鍵指定情報を用いて表現する。

【0045】

あるノードにつけられた鍵指定情報の最初の3ビット(チャイルドビット)は、

[1] ならばそのノードからそのビットの位置に対応する子ノードに対して枝が出ている(鍵指定木に対応する子ノードが存在する)ことを示し、

[0] ならばそのノードから対応する子ノードに対して枝は出していない(対応する子ノ

10

20

30

40

50

ードは存在しない)ことを示す。

例えば、あるノードの情報が、

[1 1 1]であれば、すべての子ノードに対して枝が出ている。

[1 0 0]であれば、一番左側の子ノードにのみ枝が出ている。

[1 1 0]であれば、一番左と中央の子ノードに枝が出ている。

[0 0 0]であれば、枝はいずれも出ておらず、そのノードが鍵指定木のリーフ(葉)であることを示す。

【0 0 4 6】

また、鍵指定情報の最後の3ビット(鍵指定ビット)は、そのノードに定義されたどのサブセットに対応するサブセットキーが、上記の暗号文ブロック中の暗号文を作るために用いられているかを示す。

【0 0 4 7】

すなわち、あるノードkの鍵指定ビット情報が、

[1 0 0]であればサブセットキー $SK_{k, 1 0 0}$ が適用された暗号文が含まれている。

。

[1 1 0]であればサブセットキー $SK_{k, 1 1 0}$ が適用された暗号文が含まれている。

。

[0 0 0]であれば、そのノードに対して定義されたサブセットに対応するサブセットキーは使用されていないことを示す。

【0 0 4 8】

図6に示すように、鍵指定木の各ノードにつけられた6ビットの鍵指定情報を、ノードの番号順に並べたものが鍵指定コードとなる。

【0 0 4 9】

図6の構成では、鍵指定木は、ノードNo. 1, 3, 4, 9, 11, 12によって構成されているので、これらの各ノードの鍵指定情報ビットを順に並べたデータ、すなわち、

[0 1 1 1 0 0 0 1 0 1 0 1 1 1 0 0 0 0 0 0 0 1 0 0 0 0 0 1 0 1 0 0 0 1 0 0]

が、鍵指定コードとして設定される。

【0 0 5 0】

しかし、このような鍵指定コードは、構成ビットが長くなるという欠点を有する。上述の構成では、鍵指定木は、ノードNo. 1, 3, 4, 9, 11, 12の6ノードによって構成され、各ノード毎に6ビットの情報を持つので、鍵指定コードは $6 \times 6 = 36$ ビットとなる。鍵指定コードは、リーフ数の増加や、鍵指定木の構成の複雑化に伴い、さらに多くのビット数が必要になる。

【0 0 5 1】

そこで、鍵指定コードの情報量を削減する構成が提案された。図7を参照してその構成について説明する。図7に示す処理は、上述した6ビットの鍵指定コード中、前半の3ビットのチャイルドビットを1ビットのリーフビットcとして置き換えたものである。

【0 0 5 2】

図7に示す鍵指定木の各ノード(1, 3, 4, 9, 11, 12, 13)には、3ビットのチャイルドビットの代わりに1ビットのリーフビットcが設定される。

【0 0 5 3】

リーフビットは、

[1]であるとき、鍵指定木のリーフであることを示す。

[0]であるとき、リーフ以外のノードであることを示す。

【0 0 5 4】

図7に示す例において鍵指定木中のリーフノードはノード(9, 11, 12, 13)であり、これらのノードのリーフビットは、[1]に設定される。それ以外のノード(1, 3, 4)のノードのリーフビットは、[0]に設定される。

【0 0 5 5】

リーフビットc = 1の場合には、そのノードは、部分木のリーフであり、そのノードか

10

20

30

40

50

ら鍵指定木の枝は出ていない、また、リーフビット $c = 0$ の場合には、そのノードは、部分木のリーフではなく、そのノードから鍵指定木の枝が出ている。どの枝が出ているかは、後半3ビットの鍵指定ビット情報によって判定される。すなわち、鍵指定ビット情報 $[d, d, d]$ 中、 $d = 0$ として設定されたビットに対応する子ノードに枝がでてい

【0056】

リーフビット $= c$ 、鍵指定ビット $= d d d$ としたとき、例えばあるノード k の鍵指定情報が、

$c, d d d = 0, 0 0 1$ であれば、そのノード k から左と中央の子ノードに対して枝が出ており、また、サブセットキー $SK_{k, 0 0 1}$ が暗号化に適用されていることを示す。

$c, d d d = 0, 1 1 0$ であれば、そのノード k から右の子ノードに対して枝が出ており、また、サブセットキー $SK_{k, 1 1 0}$ が暗号化に適用されていることを示す。

リーフビット $c = 1$ の場合には、そのノード k から枝が出ていないことを示す。暗号化に適用されているサブセットキーについての意味は同様であり、サブセットキー $SK_{k, d d d}$ が暗号化に適用されていることを示す。

【0057】

図7に示す例、すなわち情報処理装置 $u_{14} \sim u_{40}$ の中から、 $u_{27}, u_{28}, u_{33}, u_{36}, u_{37}, u_{38}, u_{39}, u_{40}$ (図7中の×印) をリポーくし、それ以外の情報処理装置に情報 (たとえば、コンテンツキー K_c) を送信するものとする。

【0058】

この場合、図7に示すように、サブセットが定義されるノード、すなわち、ノード1, 3, 9, 11, 12, および、そのノードがルートとなる部分木に属する葉がすべてリポーくされているノードのうち、他の同様の部分木の間ノードになっていないノード、すなわち、ノード13を連結した鍵指定木が設定され、設定された鍵指定木を構成する各ノード (1, 3, 4, 9, 11, 12, 13) にリーフビット $= c$ 、鍵指定ビット $= d d d$ が以下のように設定される。

ノード1: (0, 100)

ノード3: (0, 101)

ノード4: (0, 000)

ノード9: (1, 100)

ノード11: (1, 101)

ノード12: (1, 100)

ノード13: (1, 000)

【0059】

この結果、鍵指定コードは、上記各ビットを順に並べた値、すなわち、

$[0100010100001100110111001000]$

となり、28ビット情報となる。

【0060】

このように、リーフビットを適用することにより、先に図6を参照して説明した3ビットのチャイルドビットを適用した例では36ビットの情報量となっていた鍵指定コードを28ビットまで削減することができる。

【0061】

なお、リポーくする情報処理装置がない場合、全情報処理装置が保有するサブセットキー $SK_{1, 1 1 1}$ が用いられた暗号文が提供されるが、これを表現するためにはルートの鍵指定情報を1, 111とすればよい。

【0062】

ところで、このブロードキャストエンクリプションシステムに対する攻撃を考えてみる。たとえば、攻撃者が、ある情報処理装置をリバースエンジニアリングして、その情報処理装置が持つサブセットキーを取り出し、また情報処理装置の複製を製造して、取り出したサブセットキーをその複製情報処理装置において使うという状況がある。複製情報処理装置は、当然ながら海賊版業者などが作ったライセンス対象外の情報処理装置であり、ラ

10

20

30

40

50

イセンス機器であれば行わない不正コピーや再生コンテンツのインターネットへの再配信などを行う可能性がある。そして、この複製情報処理装置がブラックマーケットで売買されるような状況を考える。また、そのサブセットキーを用いて攻撃者が受信ソフトウェアを作成し、インターネット上で配布するような状況も考えられる。

【0063】

複製情報処理装置を入手できた場合、リバースエンジニアリングか、または非特許文献1に記載の方法を用いて、その複製情報処理装置で用いられているサブセットキーを特定することができる。

【0064】

ここで、複製情報処理装置でリーフを1つだけ含むサブセットに対するサブセットキーが用いられていれば、そのサブセットキーを持つ正当な情報処理装置は1台しかないので、それ以降においてその情報処理装置をリボークすればよい。

【0065】

しかし、複製情報処理装置が、そのようなサブセットキーを持たず、複数のリーフ（葉）を構成要素とするサブセットに対応するサブセットキー（たとえば、木の上位のノードに対して定義されたサブセットのサブセットキー）のみを格納し、そのサブセットキーを適用した処理を行っているとする、そのサブセットキーは複数のリーフ（葉）に対応する複数の情報処理装置に共通に格納されているサブセットキーであるため、どの情報処理装置からサブセットキーが盗まれたかを特定することができない。

【0066】

たとえば、図7の例、すなわち、情報処理装置 $u_{14} \sim u_{40}$ の中から、 u_{27} , u_{28} , u_{33} , u_{36} , u_{37} , u_{38} , u_{39} , u_{40} （図7中の×印）がリボークされている状態において、現在はリボークされていない情報処理装置 u_{23} , u_{24} , u_{25} , u_{29} , u_{30} , u_{31} のいずれかが攻撃者によりリバースエンジニアリングされ、その情報処理装置が持つサブセットキーが露呈したが、攻撃者はそのうちのノード3において定義されたサブセット $S_{3,101}$ に対応するサブセットキー $SK_{3,101}$ のみを使って複製情報処理装置を製造したとする。

【0067】

この場合、ノード3において定義されたサブセット $S_{3,101}$ に対応するサブセットキー $SK_{3,101}$ は、情報処理装置 u_{23} , u_{24} , u_{25} , u_{29} , u_{30} , u_{31} のいずれにも共通に格納されたサブセットキーであるため、これらの情報処理装置中、どの情報処理装置が攻撃、すなわち不正に利用されたのか特定できないという問題が発生し、不正な情報処理装置を特定したりリボーク処理ができなくなるという問題がある。

【特許文献1】特開2001-352322号公報

【非特許文献1】D. Naor, M. Naor and J. Lotspiech 著, "Revocation and Tracing Schemes for Stateless Receivers," *Advances in Cryptology-Crypto 2001, Lecture Notes in Computer Science 2139*, Springer, pp. 41-62, 2001

【発明の開示】

【発明が解決しようとする課題】

【0068】

本発明は、このような状況に鑑みてなされたものであり、木構造を用いた情報配信方式を適用した暗号文送信構成において、攻撃者による様々な攻撃が行なわれた場合、効率的にリボーク対象としてのリーフに対応する情報処理装置の特定を可能とした情報処理装置、情報記録媒体、および情報処理方法、並びにコンピュータ・プログラムを提供することを目的とする。

【0069】

より、具体的には鍵指定コードの構成情報として新たな情報を付加することで、様々なサブセットを設定した暗号文の提供を可能とし、暗号文を受領するユーザデバイスとして

10

20

30

40

50

の情報処理装置において、本発明に従った鍵指定情報からなる鍵指定コードに基づいて、自己の保有するサブセットキーによって復号可能な暗号文を効率的に選択することを可能とした情報処理装置、情報記録媒体、および情報処理方法、並びにコンピュータ・プログラムを提供することを目的とする。

【課題を解決するための手段】

【0070】

本発明の第1の側面は、

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、

10

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にある。

【0071】

さらに、本発明の情報処理装置の一実施態様において、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。

20

【0072】

さらに、本発明の情報処理装置の一実施態様において、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。

30

【0073】

さらに、本発明の情報処理装置の一実施態様において、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。

【0075】

さらに、本発明の情報処理装置の一実施態様において、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。

40

【0080】

さらに、本発明の情報処理装置の一実施態様において、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

50

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。

【0081】

さらに、本発明の第2の側面は、

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にある。

【0082】

さらに、本発明の情報処理装置の一実施態様において、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。

【0083】

さらに、本発明の情報処理装置の一実施態様において、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。

【0084】

さらに、本発明の情報処理装置の一実施態様において、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。

【0085】

さらに、本発明の情報処理装置の一実施態様において、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。

【0087】

さらに、本発明の情報処理装置の一実施態様において、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

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。

【0090】

さらに、本発明の情報処理装置の一実施態様において、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。

10

【0102】

さらに、本発明の第4の側面は、

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、

20

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にある。

【0103】

さらに、本発明の情報処理方法の一実施態様において、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。

30

【0104】

さらに、本発明の情報処理方法の一実施態様において、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。

40

【0105】

さらに、本発明の情報処理方法の一実施態様において、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。

【0107】

さらに、本発明の情報処理方法の一実施態様において、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

50

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。

【0112】

さらに、本発明の情報処理方法の一実施態様において、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。

10

【0113】

さらに、本発明の第5の側面は、

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、

20

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にある。

【0114】

さらに、本発明の情報処理方法の一実施態様において、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。

30

【0115】

さらに、本発明の情報処理方法の一実施態様において、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。

40

【0116】

さらに、本発明の情報処理方法の一実施態様において、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。

【0117】

50

さらに、本発明の情報処理方法の一実施態様において、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。

【0119】

さらに、本発明の情報処理方法の一実施態様において、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。

10

【0123】

さらに、本発明の第6の側面は、

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、

20

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・プログラムにある。

30

【0124】

さらに、本発明の第7の側面は、

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、

40

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・プログラムにある。

【0125】

なお、本発明のコンピュータ・プログラムは、例えば、様々なプログラム・コードを実行可能なコンピュータ・システムに対して、コンピュータ可読な形式で提供する記憶媒体、通信媒体、例えば、CDやFD、MOなどの記録媒体、あるいは、ネットワークなどの

50

通信媒体によって提供可能なコンピュータ・プログラムである。このようなプログラムをコンピュータ可読な形式で提供することにより、コンピュータ・システム上でプログラムに応じた処理が実現される。

【0126】

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。なお、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

【発明の効果】

【0127】

本発明の構成によれば、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し、鍵指定コードの構成データである鍵指定木ノード毎の鍵指定情報中に、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（パーティションビット）を含める構成としたので、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生成して情報処理装置に送信することが可能となり、暗号文および鍵指定コードを受領した情報処理装置側においては、受領した暗号文が、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であるか否かを判別して、鍵指定コードに基づいて、自己の復号対象の暗号文を選択することが可能となる。

【0128】

本発明の構成によれば、木構造を用いた情報配信方式を適用した暗号文送信構成において、様々な分割サブセットを設定した暗号文の提供が可能となるので、攻撃者による様々な攻撃が行なわれた場合、効率的にリボーク対象としてのリーフに対応する情報処理装置の特定が可能となる。

【0129】

さらに、本発明の構成によれば、分割態様が複数あるサブセットにおいても、分割態様を示す分割法指定ビットを設定した構成としたので、例えば3分木構成において2つの枝と1つの枝の様々な組み合わせや3つの枝毎の分割サブセットの設定など任意の分割態様の設定が可能となる。暗号文ブロックからの暗号文選択および復号処理を行う情報処理装置では、鍵指定コードに含まれる鍵指定情報に含まれる分割法指定ビットを解析することにより、復号対象の暗号文を選択することができる。

【0130】

さらに、本発明の構成において、鍵指定ビット、パーティションビット、分割法指定ビットのビット情報を符号化した構成によれば、鍵指定コードの情報量を削減することが可能となる。

【発明を実施するための最良の形態】

【0131】

以下、図面を参照しながら本発明の情報処理装置、情報記録媒体、および情報処理方法、並びにコンピュータ・プログラムの詳細について説明する。

【実施例1】

【0132】

背景技術の欄において説明したように、多分木構成を用いて、特定の情報処理装置においてのみ取得可能な情報としての暗号文を設定し、かつ、各情報処理装置において、どの暗号文を選択すべきかを示す鍵指定コードを暗号文と併せて送付することにより、暗号文を受信した情報処理装置側では、鍵指定コードに基づいて、自装置において復号可能な暗号文を選択して、効率的に復号することが可能となる。

【0133】

前述したように、鍵指定コードは、鍵指定木の構成情報と、どのノードのキーが適用されているかを示す情報によって構成される。先に図7を参照して説明した多分木構成においては、リーフビットを適用することで、鍵指定コードの情報量を削減する構成としている。

【0134】

しかし、図7に示す構成において、情報処理装置 $u_{14} \sim u_{40}$ の中から、 u_{27} , u_{28} , u_{33} , u_{36} , u_{37} , u_{38} , u_{39} , u_{40} (図7中の×印) がリボークされている状態において、現在はリボークされていない情報処理装置 u_{23} , u_{24} , u_{25} , u_{29} , u_{30} , u_{31} のいずれかが攻撃者によりリバースエンジニアリングされ、その情報処理装置が持つサブセットキーが露呈し、攻撃者が情報処理装置 u_{23} , u_{24} , u_{25} , u_{29} , u_{30} , u_{31} に共通に格納されたサブセットキー、すなわち、ノード3において定義されたサブセット $S_{3, 101}$ に対応するサブセットキー $SK_{3, 101}$ を、多数の機器にコピーして、不正機器を大量に製造したと想定する。

10

【0135】

この様な場合、システム管理者が、不正機器を入手し、不正に利用されているサブセットキーが、サブセットキー $SK_{3, 101}$ であることを解明しても、サブセットキー $SK_{3, 101}$ は、情報処理装置 u_{23} , u_{24} , u_{25} , u_{29} , u_{30} , u_{31} の全てに共通に格納されたキーであり、情報処理装置 u_{23} , u_{24} , u_{25} , u_{29} , u_{30} , u_{31} のいずれが不正に利用されたかを特定することができない。

20

【0136】

その結果、情報処理装置 u_{23} , u_{24} , u_{25} , u_{29} , u_{30} , u_{31} のいずれかを選択的にリボーク（排除）することができないということになる。サブセットキー $SK_{3, 101}$ を使った暗号文の提供を停止すると、情報処理装置 u_{23} , u_{24} , u_{25} , u_{29} , u_{30} , u_{31} のすべてをまとめてリボーク（排除）することになってしまい、正当な機器も排除されてしまうという問題が発生する。

【0137】

このような場合、図8に示す部分木中のノード3, 201において定義されたサブセット $S_{3, 101}$ に対応するサブセットキー $SK_{3, 101}$ の適用をやめて、ノード3, 201において定義された他のサブセット $S_{3, 100}$ に対応するサブセットキー $SK_{3, 100}$ と、サブセット $S_{3, 001}$ に対応するサブセットキー $SK_{3, 001}$ とを用いるようにすれば、上記のような、サブセットキー $SK_{3, 101}$ のみを格納した不正機器では、暗号文の復号ができず、不正機器によるコンテンツ利用等を排除することができる。

30

【0138】

すなわち、図9に示すように、部分木を分割して複数の部分木として再設定する。図9(1)に示す部分木211はサブセット $S_{3, 101}$ によって定義される部分木であり、対応するサブセットキー $SK_{3, 101}$ を適用した暗号文とした場合、すなわち、

$E(SK_{3, 101}, Kc)$ を設定した場合、サブセット $S_{3, 101}$ に属する情報処理装置、 u_{23} , u_{24} , u_{25} , u_{29} , u_{30} , u_{31} の全てが共通に有するサブセットキー $SK_{3, 101}$ を適用して共通に復号可能な暗号文となる。

40

【0139】

これを図9(2)に示す部分木211Aと211Bに分割する。部分木211Aはサブセット $S_{3, 100}$ によって定義される部分木であり、部分木211Bはサブセット $S_{3, 001}$ によって定義される部分木であり、それぞれ対応するサブセットキー $SK_{3, 100}$ 、 $SK_{3, 001}$ を適用した暗号文を構成する。すなわち、

$E(SK_{3, 100}, Kc)$ と、

$E(SK_{3, 001}, Kc)$ と、

を設定する。サブセット $S_{3, 100}$ に属する情報処理装置 u_{23} , u_{24} , u_{25} は、暗号文 $E(SK_{3, 100}, Kc)$ を選択して復号しコンテンツキーを取得し、サブセット $S_{3, 001}$ に属する情報処理装置 u_{29} , u_{30} , u_{31} は、暗号文 $E(SK_{3, 001}, Kc)$ を選択して復号しコンテンツキーを取得し、

50

001, Kc) を選択して復号しコンテンツキーを取得することが必要となる。

【0140】

このように、情報処理装置に提供する暗号文ブロックを下記(1)から(2)に変更する。

(1) 暗号文ブロック = $E(SK_1, 100, Kc)$, $E(SK_3, 101, Kc)$, $E(SK_9, 100, Kc)$, $E(SK_{11}, 101, Kc)$, $E(SK_{12}, 100, Kc)$

(2) 暗号文ブロック = $E(SK_1, 100, Kc)$, $E(SK_3, 100, Kc)$, $E(SK_3, 001, Kc)$, $E(SK_9, 100, Kc)$, $E(SK_{11}, 101, Kc)$, $E(SK_{12}, 100, Kc)$

10

【0141】

このような処理により、サブセットキー $SK_3, 101$ のみを格納した不正機器では、暗号文の復号ができず、サブセットキー $SK_3, 101$ のみを格納した不正機器によるコンテンツの不正利用を排除することができる。

【0142】

攻撃者は、さらに、情報処理装置 u_{23} , u_{24} , u_{25} , u_{29} , u_{30} , u_{31} のいずれかから取得したサブセット $S_3, 100$ に対応するサブセットキー $SK_3, 100$ と、サブセット $S_3, 001$ に対応するサブセットキー $SK_3, 001$ とを格納した不正機器を製造することも可能であるが、その不正機器を入手し解析することにより、適用している新たなサブセットキーが判明する。この処理を繰り返すことにより最終的には攻撃された、すなわち不正な鍵情報取得処理の対象となった唯一の情報処理装置を特定することが可能となる。

20

【0143】

このように唯一の情報処理装置が特定されれば、その情報処理装置のみを対象としたリボーク処理が可能となり、鍵情報の漏洩していない他の情報処理装置に対する影響を及ぼすことなく、1つの情報処理装置のリボークのみで、全ての不正機器、すなわちリボークされた情報処理装置に格納された鍵情報のコピー情報を持つ不正機器による配信情報(コンテンツキー Kc など)の不正取得を排除できる。

【0144】

このような情報処理装置の特定処理を行う場合、例えば図8に示すノード3, 201に対して、複数の枝202, 203に対応するサブセット $S_3, 101$ が選択された場合に、

30

a. 許容サブセット(複数の枝に対応するサブセット)全体に対応するサブセットキーを用いて暗号文を作るか、すなわち、

$E(SK_3, 101, Kc)$

それとも、

b. 許容サブセット(複数の枝に対応するサブセット)を分割した複数のサブセットに対応する複数のサブセットキーを用いて複数の暗号文を作るか、すなわち、

$E(SK_3, 100, Kc)$, $E(SK_3, 001, Kc)$

とするか、

40

いずれをも選択的に実行できるようにすることが必要である。

【0145】

また、上記のような処理を行う場合、従来の鍵指定コード、すなわち、背景技術の欄で説明した1ビットのリーフビットと、3ビットの鍵指定ビット構成では、上記、a, bのいずれの態様を持つ暗号文が含まれているかを判別することはできない。

【0146】

以下、本実施例の構成として、特定のノードに対して、複数の枝に対応するサブセットが選択された場合に、

a. 許容サブセット(複数の枝に対応するサブセット)全体に対応するサブセットキーを用いた暗号文を有するか、

50

それとも、

b. 許容サブセット（複数の枝に対応するサブセット）を分割した複数のサブセットに対応する複数のサブセットキーを用いた複数の暗号文を有するか、

a、bいずれの情報を持つ暗号文であるかを識別するための情報ビット（パーティションビット）を、鍵指定コード中に付加した構成とした実施例を説明する。

【0147】

図10以下を参照して、本実施例に係る鍵指定コードの構成、処理例の詳細について説明する。

【0148】

図10には、情報処理装置 $u_{14} \sim u_{40}$ の中から、 u_{27} 、 u_{28} 、 u_{33} 、 u_{36} 、 u_{37} 、 u_{38} 、 u_{39} 、 u_{40} （図10中の×印）がリボークされている状態における鍵指定木301を太線で示している。

10

【0149】

図10に示すように、鍵指定木301を構成する各ノード（1, 3, 4, 9, 11, 12, 13）には鍵指定情報が設定される。鍵指定情報は、

リーフビットc：1ビット

鍵指定ビットd：3ビット

パーティションビットe：1ビット

のビット構成を持つ（c, d d d, e）の計5ビットの鍵指定情報として設定される。

【0150】

20

なお、リーフビットcは、

[1]であるとき、鍵指定木のリーフであることを示し、

[0]であるとき、リーフ以外のノードであることを示す。

【0151】

鍵指定ビット、3ビットd d dは、そのノードに定義されたどのサブセットに対応するサブセットキーが、上記の暗号文ブロック中の暗号文を作るために用いられているかを示す。すなわち、あるノードkの鍵指定ビット情報が、

[100]であればサブセットキー $SK_{k, 100}$ が適用された暗号文が含まれている。

[110]であればサブセットキー $SK_{k, 110}$ が適用された暗号文が含まれている、ただし、これは、後述するように、パーティションビット $e=0$ の場合であり、パーティションビット $e=1$ の場合には、サブセットキー $SK_{k, 100}$ が適用された暗号文と、サブセットキー $SK_{k, 010}$ が適用された暗号文の2つの分割された暗号文が含まれている。

30

[000]であれば、そのノードに対して定義されたサブセットに対応するサブセットキーは使用されていないことを示す。

【0152】

リーフビットc、鍵指定ビット3ビットd d dは、パーティションビット $e=0$ の場合は、従来のルールと同様であるが、パーティションビット $e=1$ として設定されている場合は、リーフビットcの意味は変化しないが、鍵指定ビット3ビットd d dはその意味が変化する場合がある。

40

【0153】

パーティションビットeは、鍵指定ビットd d dの重みが2以上、すなわちビットの（d d d）中、1であるビットの個数が2以上であるときにのみ有効である。鍵指定ビットd d dの重みとは、ビットd d dの3つのビット中の1の数を言う。パーティションビットeは、鍵指定ビットd d dの重みが2以上の場合にのみ有効となる。具体的には、鍵指定ビットd d d = (011)、(101)、(110)、(111)の場合にのみ有効である。

【0154】

それ以外の場合は $e=0$ でも $e=1$ でも構わないが、簡潔のためデフォルトを $e=0$ と

50

する。すなわち、パーティションビット $e = 0$ の場合は、パーティションビットが存在しない従来技術と同様、リーフビットと、鍵指定ビット情報のみからなる鍵指定コードとして解釈される。

【0155】

パーティションビット $e = 1$ の場合は、そのノード k に定義されたサブセットに対応する複数のサブセットキーが個別に適用された暗号文を持つことを意味する。

【0156】

ノード k に定義されるサブセットは、 $S_{k, 100}$, $S_{k, 010}$, $S_{k, 001}$, $S_{k, 110}$, $S_{k, 101}$, $S_{k, 001}$ の6個のサブセットである。ただし、ルート（ノード1）についてのみ、サブセット $S_{1, 111}$ が含まれる。これらの複数のサブセットに対応するサブセットキーは、 $SK_{k, 100}$, $SK_{k, 010}$, $SK_{k, 001}$, $SK_{k, 110}$, $SK_{k, 101}$, $SK_{k, 001}$ であり、ルート（ノード1）のみ、サブセットキー $SK_{1, 111}$ を含む。

10

【0157】

例えば、ノード k において、

鍵指定ビット $ddd = (110)$ であり、かつ、

パーティションビット $e = 1$ の場合には、

サブセットキー $SK_{k, 100}$ と、 $SK_{k, 010}$ を用いた2つの暗号文が存在していることを意味する。

パーティションビット $e = 0$ の場合には、

サブセットキー $SK_{k, 110}$ を用いた1つの暗号文が存在していることを意味する。

20

【0158】

また、ノード k において、

鍵指定ビット $ddd = (111)$ であり、かつ、

パーティションビット $e = 1$ の場合には、

サブセットキー $SK_{k, 100}$ と、 $SK_{k, 010}$ と、 $SK_{k, 001}$ を用いた3つの暗号文が存在していることを意味する。

パーティションビット $e = 0$ の場合には、

サブセットキー $SK_{k, 111}$ を用いた1つの暗号文が存在していることを意味する。

【0159】

リボークする受信機がない場合、サブセットキー $SK_{1, 111}$ を用いるのであればルートの鍵指定情報は、パーティションビット $e = 0$ として、

$(c, ddd, e) = (1, 111, 0)$

とすればよい。これは、従来のリーフビット c : 1ビット、鍵指定ビット d : 3ビットの鍵指定情報と同様の情報である。

30

【0160】

一方、サブセットキー $SK_{1, 111}$ を用いずに、個別に3つのサブセットキー $SK_{k, 100}$ と、 $SK_{k, 010}$ と、 $SK_{k, 001}$ を用いる場合には、ルートの鍵指定情報は、パーティションビット $e = 1$ として、

$(c, ddd, e) = (1, 111, 1)$

とすればよい。

40

【0161】

図10に示す例は、情報処理装置 $u_{14} \sim u_{40}$ の中から、 u_{27} , u_{28} , u_{33} , u_{36} , u_{37} , u_{38} , u_{39} , u_{40} (図10中の×印) がリボークされている状態における鍵指定木を太線で示した図である。情報処理装置 $u_{14} \sim u_{40}$ の中から、 u_{27} , u_{28} , u_{33} , u_{36} , u_{37} , u_{38} , u_{39} , u_{40} (図10中の×印) をリボークし、それ以外の情報処理装置に情報（たとえば、コンテンツキー K_c ）を送信するものとする。

【0162】

この場合、鍵指定木は、ノード $(1, 3, 4, 9, 11, 12, 13)$ を構成ノードと

50

して、リーフノードをノード（9，11，12，13）として設定される。この構成を持つ鍵指定木構成ノードにリーフビット＝c、鍵指定ビット＝ddd、パーティションビットeが、図に示すように、以下の如く設定される。

ノード1：（0，100，0）
 ノード3：（0，101，1）
 ノード4：（0，000，0）
 ノード9：（1，100，0）
 ノード11：（1，101，0）
 ノード12：（1，100，0）
 ノード13：（1，000，0）

10

【0163】

この結果、鍵指定コードは、上記各ビットを順に並べた値、すなわち、
 [01000010110000011000110101100010000]
 となる。

【0164】

上記設定において、ノード3の鍵指定情報が、

（c，ddd，e）＝（0，101，1）

であり、パーティションビットe＝1である。

鍵指定ビットは、ddd＝（101）であるので、これは、上述の鍵指定コードに対応して設定される暗号文ブロックには、

20

サブセットキーSK_{3, 100}と、SK_{3, 001}を用いた2つの暗号文が存在していることを意味する。すなわち、

暗号文ブロック＝・・・E（SK_{3, 100}，Kc），E（SK_{3, 001}，Kc）・・・

として構成されていることを意味する。

【0165】

もし、ノード3の鍵指定情報が、

（c，ddd，e）＝（0，101，0）

であり、パーティションビットe＝0の場合は、

サブセットキーSK_{3, 101}のみを用いた暗号文が存在していることを意味する。すなわち、

30

暗号文ブロック＝・・・E（SK_{3, 101}，Kc）・・・

として構成されていることを意味する。

【0166】

任意のノードiにおいて、鍵指定ビット（ddd）と、パーティションビット（e）の組み合わせ（ddd，e）が取りうる値と、そのときに暗号文ブロックに含まれる暗号文の対応を示した対応テーブルを図11に示す。

【0167】

この対応テーブルを用いて、各情報処理装置は、鍵指定コードから、暗号文ブロックにおいて暗号文が並ぶ順番を判別し、自分が何番目の暗号文を復号すればよいかを知ることができる。なお、暗号文ブロックにおいて暗号文が並べられる順番であるが、まずその暗号化に用いられたサブセットキーに対応するサブセットが定義されるノード番号の若い順が一番プライオリティが高く（すなわち、サブセットキーSK_{2, xxx}とSK_{3, yy}を用いた暗号文では必ず前者が先に置かれる）、ノード番号が同一のものの中では、SK_{k, zzz}のzzzを2進数で表された数として見たときに、大きい順で置かれる（すなわち、サブセットキーSK_{k, 101}とSK_{k, 010}を用いた暗号文では必ず前者が先に置かれる）、というようにルールを決めておけば、暗号文の順番は一意に定まり、暗号文および鍵指定コードを受領する情報処理装置はどの暗号文を復号すればよいかを求めることができる。

40

【0168】

50

暗号文ブロックと、鍵指定コードを受領する各情報処理装置は、図 1 1 に示す対応テーブルを記憶部に格納するか、あるいは、対応テーブルに対応する鍵指定コードの解釈アルゴリズムを実行するプログラムを記憶部に格納し、対応テーブルを参照して、あるいは、鍵指定コードの解釈アルゴリズムを実行するプログラムに従って、暗号文ブロックにおいて暗号文が並ぶ順番を判別し、自分が何番目の暗号文を復号すればよいかを判定する。なお、対応テーブル、または鍵指定コードの解釈アルゴリズムを実行するプログラムは、暗号文ブロックや鍵指定コードの提供時に各情報処理装置に提供する構成としてもよい。

【0169】

このように、本実施例において、鍵指定コードは、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、鍵指定情報は、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を含むコードとして設定される。

10

【0170】

暗号文ブロックと、鍵指定コードを受領したユーザデバスとしての情報処理装置は、鍵指定コードの解析を実行し、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が、暗号文ブロック中に含まれるか否かを判定して、その判定に基づいて、暗号文ブロックから、自装置に格納されたサブセットキーを適用して復号することが可能な暗号文を選択する。

20

【0171】

図 1 2 は、図 8 で示した例に加えて、さらに、サブセットキー $SK_{1, 100}$ をサブセットキー $SK_{2, 100}$ 、 $SK_{2, 010}$ 、 $SK_{2, 001}$ の 3 つに分割した部分木の構成を示している。

【0172】

前述したように、ルートノード（ノード No. 1）以外のノード k は、サブセット S_k 、 111 を有していない。すなわち、あるノードの子ノードを全指定するサブセットは、そのノードの上位ノードによって指定可能であるからである。従って、図 1 2 に示す情報処理装置 $u_{14} \sim u_{22}$ を指定するサブセットは、 $S_{2, 111}$ ではなく、 $S_{1, 100}$ によって指定される。

30

【0173】

この場合、サブセット $S_{1, 100}$ に対応するサブセットキー $SK_{1, 100}$ による暗号文は、

$E(SK_{1, 100}, Kc)$ となるが、これを、
 情報処理装置 $\{u_{14}, u_{15}, u_{16}\}$ を含むサブセット $S_{2, 100}$ と、
 情報処理装置 $\{u_{17}, u_{18}, u_{19}\}$ を含むサブセット $S_{2, 010}$ と、
 情報処理装置 $\{u_{20}, u_{21}, u_{22}\}$ を含むサブセット $S_{2, 001}$ と、
 の 3 つのサブセットに分割して、それぞれのサブセット毎に取得可能な暗号文を設定する場合、サブセットキー $SK_{1, 100}$ を、サブセットキー $SK_{2, 100}$ 、 $SK_{2, 010}$ 、 $SK_{2, 001}$ の 3 つに分割し、暗号文として、

40

$E(SK_{2, 100}, Kc)$

$E(SK_{2, 010}, Kc)$

$E(SK_{2, 001}, Kc)$

の 3 つを設定する。

【0174】

これは、すなわち、図 1 3 に示すように、部分木を分割して複数の部分木として再設定する処理である。図 1 3 (1) に示す部分木 311 はサブセット $S_{1, 100}$ によって定義される部分木であり、対応するサブセットキー $SK_{1, 100}$ を適用した暗号文とした場合、すなわち、

$E(SK_{1, 100}, Kc)$ を設定した場合、サブセット $S_{1, 100}$ に属する情報処

50

理装置、 u_{14} 、 $\sim u_{22}$ の全てが共通に有するサブセットキー $SK_{1,100}$ を適用して共通に復号可能な暗号文となる。

【0175】

これを図13(2)に示す部分木311Aと311Bと311Cに分割する。部分木311Aはサブセット $S_{2,100}$ によって定義される部分木、部分木311Bはサブセット $S_{2,010}$ によって定義される部分木、部分木311Cはサブセット $S_{2,001}$ によって定義される部分木となる。

【0176】

それぞれ対応するサブセットキー $SK_{2,100}$ 、 $S_{2,010}$ 、 $SK_{2,001}$ を適用した暗号文を構成する。すなわち、

$E(SK_{2,100}, KC)$

$E(SK_{2,010}, KC)$

$E(SK_{2,001}, KC)$

の3つを設定する。

サブセット $S_{2,100}$ に属する情報処理装置 u_{14} 、 u_{15} 、 u_{16} は、暗号文 $E(SK_{2,100}, KC)$ を選択して復号しコンテンツキーを取得し、サブセット $S_{2,010}$ に属する情報処理装置 u_{17} 、 u_{18} 、 u_{19} は、暗号文 $E(SK_{2,010}, KC)$ を選択して復号しコンテンツキーを取得し、サブセット $S_{2,001}$ に属する情報処理装置 u_{20} 、 u_{21} 、 u_{22} は、暗号文 $E(SK_{2,001}, KC)$ を選択して復号しコンテンツキーを取得することが必要となる。

【0177】

上記の設定とした場合の鍵指定木の各ノードにおける鍵指定情報(c, d d d, e)は図14に示すとおりとなる。

【0178】

図14は、情報処理装置 $u_{14} \sim u_{40}$ の中から、 u_{27} 、 u_{28} 、 u_{33} 、 u_{36} 、 u_{37} 、 u_{38} 、 u_{39} 、 u_{40} (図14中の×印)がリボークされている状態における鍵指定木321を太線で示した図である。情報処理装置 $u_{14} \sim u_{40}$ の中から、 u_{27} 、 u_{28} 、 u_{33} 、 u_{36} 、 u_{37} 、 u_{38} 、 u_{39} 、 u_{40} (図14中の×印)をリボークし、それ以外の情報処理装置に情報(たとえば、コンテンツキーKC)を送信するものとする。

【0179】

この場合、鍵指定木は、ノード(1, 2, 3, 4, 9, 11, 12, 13)を構成ノードとして、リーフノードをノード(2, 9, 11, 12, 13)として設定される。この構成を持つ鍵指定木構成ノードにリーフビット=c、鍵指定ビット=d d d、パーティションビットeが、例えば以下のように設定される。

ノード1: (0, 000, 0)

ノード2: (1, 111, 1)

ノード3: (0, 101, 1)

ノード4: (0, 000, 0)

ノード9: (1, 100, 0)

ノード11: (1, 101, 0)

ノード12: (1, 100, 0)

ノード13: (1, 000, 0)

【0180】

この結果、鍵指定コードは、上記各ビットを順に並べた値、すなわち、

[0000011111010110000011000110101100010000]

となる。

【0181】

上記設定において、ノード2の鍵指定情報が、

$(c, d d d, e) = (1, 1 1 1, 1)$

であり、パーティションビット $e = 1$ である。

鍵指定ビットは、 $d d d = (1 1 1)$ であるので、上述の鍵指定コードに対応して設定される暗号文ブロックには、

サブセットキー $SK_{2, 1 0 0}$ と、 $SK_{2, 0 1 0}$ と、 $SK_{2, 0 0 1}$ を用いた 3 つの暗号文が存在していることを意味する。すなわち、

暗号文ブロック = $\cdots E(SK_{2, 1 0 0}, Kc), E(SK_{2, 0 1 0}, Kc), E(SK_{3, 0 0 1}, Kc) \cdots$

として構成されていることを意味する。

【0182】

上述のように、本実施例によれば、任意のノードにおいて、1 つのサブセットで定義可能な集合を複数の分割サブセットに区別して、設定し、それぞれの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生成して情報処理装置に送信することができるとともに、パーティションビットを設定した鍵指定情報を設定した鍵指定コードを生成し提供する構成とした。

【0183】

従って、暗号文および鍵指定コードを受領した情報処理装置は、受領した暗号文が、分割サブセットを設定し、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である場合も、分割サブセットを用いない構成である場合も、鍵指定コードに基づいて、自己の復号対象の暗号文を選択することが可能となる。

【実施例 2】

【0184】

上述した実施例においては、例えば、サブセットキー $SK_{3, 1 0 1}$ を、

$SK_{3, 1 0 0}$ 、 $SK_{3, 0 0 1}$ に分割したり、あるいは、

サブセットキー $SK_{1, 1 0 0}$ を、

$SK_{2, 1 0 0}$ 、 $SK_{2, 0 1 0}$ 、 $SK_{2, 0 0 1}$ に分割する例を説明した。すなわち、あるサブセットキーを分割する場合には、必ずただひとつの方法で、サブセットキーを $SK_{x, y y y}$ と表したときの $y y y$ 部分の重み (1 であるビットの個数) が 1 になるように分割していた。

【0185】

しかし、分木数が 3 以上の場合には、分割態様は、様々な態様が可能となる。たとえば図 15 に示すように、ノード 1 に対応して設定されるサブセット $S_{1, 1 0 0}$ を、ノード 2 に対応して設定される 2 つのサブセット $S_{2, 1 0 1}$ と、 $S_{2, 0 1 0}$ の 2 つに分割し、2 つのサブセット $S_{2, 1 0 1}$ と、 $S_{2, 0 1 0}$ の対応サブセットキー $SK_{2, 1 0 1}$ と、 $SK_{2, 0 1 0}$ を適用した暗号文を送付したいという場合がある。

【0186】

各ノードに設定される鍵指定情報のうち、鍵指定ビット $d d d$ の重みが 2 ビット (1 の数が 2) のときは分割する方法は 1 通りであり、重みが 3 ビットの場合 ($d d d = 1 1 1$ のとき) は、4 通りの分割方法がある。すなわち、

(1) $(1 0 0)$ 、 $(0 1 0)$ 、 $(0 0 1)$

(2) $(1 0 0)$ 、 $(0 1 1)$

(3) $(0 1 0)$ 、 $(1 0 1)$

(4) $(0 0 1)$ 、 $(1 1 0)$

の 4 通りである。

【0187】

このような多種類の分割態様がある場合、これらの分割態様のどの態様で分割が実行されたかを判別する情報が必要となる。この情報を分割法指定ビット (Partition Specify Bit) と呼ぶ。

【0188】

この分割法指定ビットを鍵指定木の鍵指定情報の構成ビットとして 2 ビット ($f f$) を

10

20

30

40

50

新たに付加する。3分木構成の場合、分割態様は最大で、上記4通りであるので、鍵指定情報の構成ビットとして2ビット(f f)を新たに付加する。

【0189】

図16に、鍵指定木を構成するノードiに設定される鍵指定情報中の、鍵指定ビットddd、パーティションビットe、分割法指定ビットffのパターンについて示す。分割法指定ビットffは、鍵指定ビットddd、パーティションビットeが、(ddd, e) = (111, 1)のときのみ有効である。その他の場合は、分割法指定ビットff = 00として設定され、上述の実施例1に従った解釈がなされる。

【0190】

図16に示す4つのエントリのみが、鍵指定ビットddd、パーティションビットeが、(ddd, e) = (111, 1)であり、これらの場合、分割法指定ビットffに基づいて、暗号文の解釈が行われることになる。

【0191】

(1) (ddd, e, ff) = (111, 1, 00)の場合、

3つのサブセットキー: $SK_{i, 100}$ 、 $SK_{i, 010}$ 、 $SK_{i, 001}$ を適用して、

3つの暗号文: $E(SK_{i, 100}, Kc)$ 、 $E(SK_{i, 010}, Kc)$ 、 $E(SK_{i, 001}, Kc)$ を設定することを示す。

(2) (ddd, e, ff) = (111, 1, 01)の場合、

2つのサブセットキー: $SK_{i, 100}$ 、 $SK_{i, 011}$ を適用して、

2つの暗号文: $E(SK_{i, 100}, Kc)$ 、 $E(SK_{i, 011}, Kc)$ を設定することを示す。

(3) (ddd, e, ff) = (111, 1, 10)の場合、

2つのサブセットキー: $SK_{i, 101}$ 、 $SK_{i, 010}$ を適用して、

2つの暗号文: $E(SK_{i, 101}, Kc)$ 、 $E(SK_{i, 010}, Kc)$ を設定することを示す。

(4) (ddd, e, ff) = (111, 1, 11)の場合、

2つのサブセットキー: $SK_{i, 110}$ 、 $SK_{i, 001}$ を適用して、

2つの暗号文: $E(SK_{i, 110}, Kc)$ 、 $E(SK_{i, 001}, Kc)$ を設定することを示す。

【0192】

各情報処理装置は、図16に示す対応テーブルを用いて、鍵指定コードから、暗号文ブロックにおいて暗号文が並ぶ順番を判別し、自分が何番目の暗号文を復号すればよいかを知らることができる。

【0193】

暗号文ブロックと、鍵指定コードを受領する各情報処理装置は、図16に示す対応テーブルを記憶部に格納するか、あるいは、対応テーブルに対応する鍵指定コードの解釈アルゴリズムを実行するプログラムを記憶部に格納し、対応テーブルを参照して、あるいは、鍵指定コードの解釈アルゴリズムを実行するプログラムに従って、暗号文ブロックにおいて暗号文が並ぶ順番を判別し、自分が何番目の暗号文を復号すればよいかを判定する。なお、対応テーブル、あるいは、鍵指定コードの解釈アルゴリズムを実行するプログラムは、暗号文ブロックや鍵指定コードの提供時に各情報処理装置に提供する構成としてもよい。

【0194】

なお、暗号文ブロックにおいて暗号文が並べられる順番であるが、まずその暗号化に用いられたサブセットキーに対応するサブセットが定義されるノード番号の若い順が一番プライオリティが高く(すなわち、サブセットキー $SK_{2, xxx}$ と $SK_{3, yyy}$ を用いた暗号文では必ず前者が先に置かれる)、ノード番号が同一のものの間では、 $SK_{k, zzz}$ のzzzを2進数で表された数として見たときに、大きい順で置かれる(すなわち、サブセットキー $SK_{k, 101}$ と $SK_{k, 010}$ を用いた暗号文では必ず前者が先に置か

10

20

30

40

50

れる)、というようにルールを決めておけば、暗号文の順番は一意に定まり、暗号文および鍵指定コードを受領する情報処理装置はどの暗号文を復号すればよいかを求めることができる。

【0195】

分割法指定ビット $f f$ を含む鍵指定情報、すなわち、

リーフビット: c

鍵指定ビット: $d d d$

パーティションビット: e

分割法指定ビット: $f f$

からなる ($c, d d d, e, f f$) の計7ビット構成を持つ鍵指定情報を鍵指定木の各構成ノードに設定した例を図17に示す。 10

【0196】

図17は、情報処理装置 $u_{14} \sim u_{40}$ の中から、 $u_{27}, u_{28}, u_{33}, u_{36}, u_{37}, u_{38}, u_{39}, u_{40}$ (図17中の×印) がリボークされている状態における鍵指定木401を太線で示した図である。情報処理装置 $u_{14} \sim u_{40}$ の中から、 $u_{27}, u_{28}, u_{33}, u_{36}, u_{37}, u_{38}, u_{39}, u_{40}$ (図17中の×印) をリボークし、それ以外の情報処理装置に情報 (たとえば、コンテンツキー K_c) を送信するものとする。

【0197】

この場合、鍵指定木は、ノード (1, 2, 3, 4, 9, 11, 12, 13) を構成ノードとして、リーフノードをノード (2, 9, 11, 12, 13) として設定される。この構成を持つ鍵指定木構成ノードにリーフビット = c 、鍵指定ビット = $d d d$ 、パーティションビット e 、分割法指定ビット $f f$ が、例えば以下のように設定される。 20

ノード1: (0, 000, 0, 00)

ノード2: (1, 111, 1, 10)

ノード3: (0, 101, 0, 00)

ノード4: (0, 000, 0, 00)

ノード9: (1, 100, 0, 00)

ノード11: (1, 101, 0, 00)

ノード12: (1, 100, 0, 00)

ノード13: (1, 000, 0, 00)

30

【0198】

この結果、鍵指定コードは、上記各ビットを順に並べた値、すなわち、

[0000000111111001010000000000001100000011010000110000001000000]

となる。

【0199】

上記設定において、ノード2の鍵指定情報が、

($c, d d d, e, f f$) = (1, 111, 1, 10)

であり、鍵指定情報、パーティションビット ($d d d, e$) = (111, 1) である。 40

分割法指定ビット ($f f$) = (10) であるので、

これは、上述の鍵指定コードに対応して設定される暗号文ブロックには、

サブセットキー $SK_{2, 101}$ と、 $SK_{2, 010}$ とを用いた2つの暗号文が存在していることを意味する。すなわち、

暗号文ブロック = $\cdots E(SK_{2, 101}, K_c), E(SK_{2, 010}, K_c) \cdots$

として構成されていることを意味する。

【0200】

図17の例において、リボークする受信機がなく、全受信機を構成要素とするサブセット $S_{1, 111}$ に対応するサブセットキーで暗号化した暗号文1つだけを送信する場合に 50

は、ルートの鍵指定情報を $(c, d d d, e, f f) = (1, 1 1 1, 0, 0 0)$ として鍵指定コードを構成すればよい。この指定情報は、リーフビット c と鍵指定ビット $d d d$ のみの情報構成の場合と同様の解釈となる。

【0201】

上述のように、本実施例によれば、任意のノードにおいて、1つのサブセットで定義可能な集合を複数の分割サブセットに区別して、設定し、それぞれの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生成して情報処理装置に送信することができるとともに、パーティションビットを設定し、かつ分割法指定ビットを設定したことにより、様々な分割態様を区別した分割サブセットの設定が可能となり、様々な分割態様を区別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の生成が可能となる。

10

【0202】

暗号文および鍵指定コードを受領した情報処理装置は、受領した暗号文が、分割サブセットを設定し、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である場合、分割法指定ビットに基づいて、分割態様を判別することが可能となり、自己の復号対象の暗号文を選択することが可能となる。

【実施例3】

【0203】

先に、図16を参照して説明した鍵指定情報 $(d d d, e, f f)$ 、すなわち、
鍵指定ビット； $d d d$

パーティションビット： e

20

分割法指定ビット： $f f$

の $(d d d, e, f f)$ の5ビットからなる情報に対応して設定される暗号文ブロックに含まれる暗号文のパターンは、図16に示すように、「暗号文なし」も含めて全部で15通りである。

【0204】

実施例2では、 $(d d d, e, f f)$ の6ビットを用いてこの15通りのデータを表しているが、15通りのデータは4ビットで表現することが可能であるので、図18に示すように、 $(d d d, e, f f)$ の6ビットの値を符号化（エンコード）した4ビットの値 $(g g g g)$ または $(h h h h)$ を用いることにより、鍵指定情報に必要なビット数を減らすことが可能である。

30

【0205】

図18の $(g g g g)$ は、テーブルの上から12段目までの(1)～(12)のデータエントリは、 $(g g g g) = (d d d, e)$ とし、一番下の3段の(13)～(15)のエントリは、 $(d d d, e)$ の組み合わせに残りのビット構成を割り当てた構成となっている。

【0206】

このため、エンコードされた $(g g g g)$ とエンコード前の $(d d d, e)$ との対応を求めるのが容易になっている。

【0207】

$(d d d, e, f f)$ のかわりにエンコードビット $(g g g g)$ の4ビットを用いて、
鍵指定情報を、

40

リーフビット： c

エンコードビット： $g g g g$

の $(c, g g g g)$ 5ビット構成とした場合の鍵指定木と各ノードに設定される鍵指定情報、および鍵指定コードの構成を図19に示す。

【0208】

図19は、情報処理装置 $u_{14} \sim u_{40}$ の中から、 $u_{27}, u_{28}, u_{33}, u_{36}, u_{37}, u_{38}, u_{39}, u_{40}$ (図19中の×印) がリボークされている状態における鍵指定木421を太線で示した図である。情報処理装置 $u_{14} \sim u_{40}$ の中から、 $u_{27}, u_{28}, u_{33}, u_{36}, u_{37}, u_{38}, u_{39}, u_{40}$ (図19中の×印) をリボ

50

ークし、それ以外の情報処理装置に情報（たとえば、コンテンツキー K c）を送信するものとする。

【0209】

この場合、鍵指定木は、ノード（1, 2, 3, 4, 9, 11, 12, 13）を構成ノードとして、リーフノードをノード（2, 9, 11, 12, 13）として設定される。この構成を持つ鍵指定木構成ノードにリーフビット = c、鍵指定ビット = d d d、パーティションビット e、分割法指定ビット f f の設定と、リーフビット = c と、エンコードビット = g g g g の（c, g g g g）5ビットとした設定の対応を以下に示す。

ノード1：（0, 000, 0, 00）→（0, 0000）

ノード2：（1, 111, 1, 10）→（1, 0101）

ノード3：（0, 101, 0, 00）→（0, 1010）

ノード4：（0, 000, 0, 00）→（0, 0000）

ノード9：（1, 100, 0, 00）→（1, 1000）

ノード11：（1, 101, 0, 00）→（1, 1010）

ノード12：（1, 100, 0, 00）→（1, 1000）

ノード13：（1, 000, 0, 00）→（1, 0000）

【0210】

この結果、鍵指定コードは、上記各ビットを順に並べた値、すなわち、

[000001010101010000000110001101011000100000]

となる。

【0211】

リーフビット = c、鍵指定ビット = d d d、パーティションビット e、分割法指定ビット f f の設定の7ビットの鍵指定情報を各ノードに設定した場合、上述のように鍵指定木の構成ノードが8つの場合 $8 \times 7 = 56$ ビットとなるが、リーフビット = c と、エンコードビット = g g g g の（c, g g g g）5ビットとした場合、 $8 \times 5 = 40$ ビットとなり情報量が $5/7$ に削減される。

【0212】

なお、図19の例において、リポーくする受信機がなく、全受信機を構成要素とするサブセット $S_{1, 111}$ に対応するサブセットキーで暗号化した暗号文1つだけを送信する場合には、ルートの鍵指定情報を（c, g g g g）=（1, 1110）として鍵指定コードを構成すればよい。この指定情報は、リーフビット = c、鍵指定ビット = d d d、パーティションビット e、分割法指定ビット f f の設定の7ビットの鍵指定情報にデコードすると、

（c, d d d, e, f f）=（1, 111, 0, 00）

となり、リーフビット c と鍵指定ビット d d d のみの情報構成の場合と同様の解釈となる。

【0213】

図18に示すエンコードビット（h h h h）の4ビットは、（g g g g）の4ビットのうちの上位3ビットの重みが2（すなわち、110または101または011）であるものの最下位ビットをビット反転させたものとなっている。このコード化方法のメリットは、コード h h h h の重みを調べることにより、そのノードに対し何個の暗号文が暗号文ブロックに存在するかを調べるのが容易であるということである。

【0214】

すなわち、図18（B）に示すように、h h h h の重みが0であれば暗号文はなく、重みが1か3であれば暗号文は1つだけ存在し、重み2であれば2つの暗号文が、重み4であれば3つの暗号文が存在するようになっている。ある受信機は、自分が復号すべき暗号文に用いられたサブセットキーに対応するサブセットが定義されたノード以外のノードのサブセットキーを用いて作られた暗号文の並びの詳細を知る必要はなく、自分が復号すべき暗号文を得るためにはそれぞれのノードで何個の暗号文があり、自分が復号すべき暗号

10

20

30

40

50

文が全体で何番目に存在するかを知らねばよいので、エンコードビット (h h h h) の重みを調べることで暗号文ブロックに含まれる個数が簡単にわかることは、受信機の処理の負荷の軽減につながる。

【0215】

(d d d, e, f f) のかわりにエンコードビット (h h h h) の4ビットを用いて、鍵指定情報を、

リーフビット: c

エンコードビット: h h h h

の (c, h h h h) 5ビット構成とした場合の鍵指定木と各ノードに設定される鍵指定情報、および鍵指定コードの構成を図20に示す。

10

【0216】

図20は、情報処理装置 $u_{14} \sim u_{40}$ の中から、 u_{27} , u_{28} , u_{33} , u_{36} , u_{37} , u_{38} , u_{39} , u_{40} (図20中の×印) がリボークされている状態における鍵指定木431を太線で示した図である。情報処理装置 $u_{14} \sim u_{40}$ の中から、 u_{27} , u_{28} , u_{33} , u_{36} , u_{37} , u_{38} , u_{39} , u_{40} (図20中の×印) をリボークし、それ以外の情報処理装置に情報 (たとえば、コンテンツキー Kc) を送信するものとする。

【0217】

この場合、鍵指定木は、ノード (1, 2, 3, 4, 9, 11, 12, 13) を構成ノードとして、リーフノードをノード (2, 9, 11, 12, 13) として設定される。この構成を持つ鍵指定木構成ノードにリーフビット=c、鍵指定ビット=d d d、パーティションビットe、分割法指定ビットf fの設定と、リーフビット=cと、エンコードビット=h h h hの (c, h h h h) 5ビットとした設定の対応を以下に示す。

20

ノード1: (0, 000, 0, 00) → (0, 0000)

ノード2: (1, 111, 1, 10) → (1, 0101)

ノード3: (0, 101, 0, 00) → (0, 1011)

ノード4: (0, 000, 0, 00) → (0, 0000)

ノード9: (1, 100, 0, 00) → (1, 1000)

ノード11: (1, 101, 0, 00) → (1, 1011)

ノード12: (1, 100, 0, 00) → (1, 1000)

30

ノード13: (1, 000, 0, 00) → (1, 0000)

【0218】

この結果、鍵指定コードは、上記各ビットを順に並べた値、すなわち、

[000001010101011000000110001101111000100000]

となる。

【0219】

リーフビット=c、鍵指定ビット=d d d、パーティションビットe、分割法指定ビットf fの設定の7ビットの鍵指定情報を各ノードに設定した場合、上述のように鍵指定木の構成ノードが8つの場合 $8 \times 7 = 56$ ビットとなるが、リーフビット=cと、エンコードビット=h h h hの (c, h h h h) 5ビットとした場合、 $8 \times 5 = 40$ ビットとなり情報量が $5/7$ に削減される。

40

【0220】

なお、図20の例において、リボークする受信機がなく、全受信機を構成要素とするサブセット $S_{1, 111}$ に対応するサブセットキーで暗号化した暗号文1つだけを送信する場合には、ルートの鍵指定情報を (c, h h h h) = (1, 1110) として鍵指定コードを構成すればよい。この指定情報は、リーフビット=c、鍵指定ビット=d d d、パーティションビットe、分割法指定ビットf fの設定の7ビットの鍵指定情報にデコードすると、

(c, d d d, e, f f) = (1, 111, 0, 00)

50

となり、リーフビット c と鍵指定ビット d d d のみの情報構成の場合と同様の解釈となる。

【0221】

なお、各情報処理装置は、図18に示す対応テーブルを用いて、鍵指定コードから、暗号文ブロックにおいて暗号文が並ぶ順番を判別し、自分は何番目の暗号文を復号すればよいかを知ることができる。

【0222】

暗号文ブロックと、鍵指定コードを受領する各情報処理装置は、図18に示す対応テーブルを記憶部に格納するか、あるいは、対応テーブルに対応する鍵指定コードの解釈アルゴリズムを実行するプログラムを記憶部に格納し、対応テーブルを参照して、あるいは、
鍵指定コードの解釈アルゴリズムを実行するプログラムに従って、暗号文ブロックにおいて暗号文が並ぶ順番を判別し、自分は何番目の暗号文を復号すればよいかを判定する。なお、対応テーブル、あるいは、鍵指定コードの解釈アルゴリズムを実行するプログラムは、暗号文ブロックや鍵指定コードの提供時に各情報処理装置に提供する構成としてもよい。

10

【0223】

上述のように、本実施例によれば、情報量を大幅に削減した鍵指定コードの生成、提供が可能となる。ところで、図19および20で説明した実施例3では、鍵指定情報(c, d d d, e, f f)のうちc以外の6ビットを4ビットのg g g gまたはh h h hにエンコードする方法を示したが、cも含めた7ビットをエンコードして5ビットの鍵指定情報にする構成としてもよい。たとえば、cとg g g gあるいはcとh h h hを連結した5ビットを新たな鍵指定情報とすることも可能である。

20

【0224】

次に、上述した各実施例を実行する情報処理装置、すなわち暗号文、鍵指定コードを生成し提供する送信装置等の情報処理装置、暗号文、鍵指定コードを受領して、暗号文を選択し復号してコンテンツキー等の情報取得を行なう受信装置等の情報処理装置（本構造のリーフに設定される機器）の構成例について図21を参照して説明する。なお、本方式においてディスクなどの記録媒体に暗号文、鍵指定コードを格納して提供する場合は、送信装置はディスク書き込み装置もしくはディスク製造装置、受信機はディスク再生装置などの情報処理装置によって構成される。図21中、点線で囲った部分はオプションであり、必ずしも具備されない。たとえば通信路が記録媒体でない場合には、必ずしもメディアインタフェースは必要ではない。

30

【0225】

一例としての情報処理装置は、図21に示すように、コントローラ501、演算ユニット502、入出力インタフェース503、セキュア記憶部504、メイン記憶部505、ディスプレイ装置506、メディアインタフェース507を備える。

【0226】

コントローラ501は、例えばコンピュータ・プログラムに従ったデータ処理を実行する制御部としての機能を有するCPUによって構成される。演算ユニット502は、例えば暗号鍵の生成、乱数生成、及び暗号処理のための専用の演算機能を提供する。入出力インタフェース503は、キーボード、マウス等の入力手段からのデータ入力や、外部出力装置に対するデータ出力、ネットワークを介したデータ送受信処理に対応するインタフェースである。

40

【0227】

セキュア記憶部504は、例えば暗号鍵としてのノードキー、各種ID、前述した対応テーブルなど、安全にまたは秘密に保持すべきデータを保存する記憶部である。メイン記憶部505は、例えばコントローラ501において実行するデータ処理プログラム、その他、一時記憶処理パラメータ、プログラム実行のためのワーク領域等に使用されるメモリ領域である。セキュア記憶部504及びメイン記憶部505は、例えばRAM、ROM等によって構成されるメモリである。ディスプレイは復号コンテンツの出力等に利用され

50

る。メディアインタフェース507は、CD、DVD、MD等のメディアに対する読出／書込機能を提供する。

【0228】

図22に、DVD等の記録媒体に暗号化コンテンツを格納し、さらに、暗号化コンテンツの暗号鍵であるコンテンツキーKcを複数のサブセットキーで暗号化した暗号文ブロックと、鍵指定コードを格納した情報記録媒体の構成例を示す。

【0229】

情報記録媒体600には、コンテンツキーKcを用いて暗号化された暗号化コンテンツ620のほかに、正当なコンテンツ利用権を有するデバイス（リーフ設定情報処理装置）がコンテンツキーを取得するための暗号鍵ブロック情報としてのEKB（Enabling Key Block）610が記録されている。

10

【0230】

暗号鍵ブロック情報としてのEKB（Enabling Key Block）610には、前述のように鍵指定木の構成ノードにおいて設定される様々なサブセットキーによってコンテンツキーを暗号化した1つ以上の暗号文を含む暗号文ブロック612と鍵指定コード611から構成される。

【0231】

また、暗号鍵ブロック情報としてのEKB（Enabling Key Block）610には、一例として、そのEKBの新旧を表すバージョン番号や、EKBに含まれる情報が正当なエンティティにより作られ、改ざんされていないことを証明するためのデジタル署名等の認証コードなどを構成要素としてもよい。

20

【0232】

図23に、ユーザデバイスとしての情報処理装置に提供する暗号文ブロックと鍵指定コードから構成される暗号鍵ブロック情報としてのEKBを生成する情報処理装置におけるEKBを生成処理フローを示す。

【0233】

暗号文生成処理を実行する情報処理装置は、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。

30

【0234】

生成する鍵指定コードは、前述した実施例において説明したように、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むデータである。

【0235】

鍵指定情報は、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、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、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、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等を含む情報として設定される。

40

【0236】

なお、図23の処理フローにおいては、コンテンツキーで暗号化されたコンテンツが既に準備されているということを前提としている。まず、ステップS101において、リボーク対象となる受信機、再生機等、リーフに設定されるリボーク情報処理装置を決定する。

【0237】

このリボーク機器決定結果に基づいて、ステップS102では、先の実施例で説明した、部分木、鍵指定木が設定され、鍵指定木に従って暗号化に用いるサブセットキーを決定する。

50

【0238】

ステップS103では、どのタイプの鍵指定情報のエンコード処理を実行するかを判定する。すなわち、

(1) 従来技術として説明した鍵指定コード、すなわち、

リーフビット：c

鍵指定ビット：ddd

の(c, ddd)のビット構成とする方法。

(2) 実施例1で説明した鍵指定コード、すなわち、

リーフビット：c

鍵指定ビット：ddd

パーティションビット：e

の(c, ddd, e)のビット構成とする方法。

(3) 実施例2で説明した鍵指定コード、すなわち、

リーフビット：c

鍵指定ビット：ddd

パーティションビット：e

分割法指定ビット：ff

の(c, ddd, e, ff)のビット構成とする方法。

(4) 実施例3で説明した鍵指定コード、すなわち、

リーフビット：c

エンコードビット：gggg

の(c, gggg)のビット構成とする方法。

(5) 実施例3で説明した鍵指定コード、すなわち、

リーフビット：c

エンコードビット：hhhh

の(c, hhhh)のビット構成とする方法。

これらの各エンコード方法のどの方法を適用するかを決定する。

【0239】

エンコード処理方法が決定すると、ステップS104において鍵指定木の構成ノードの鍵指定情報を決定方法に従ってエンコードを実行する。なお、どのエンコード方法を適用するかは、設定した鍵指定木の構成に基づいて判断する、あるいは実際に各エンコードを実行して、ビット長を比較して、より短いビット長となるエンコードを行なうとするなどの判定を行なって決定してもよい。

【0240】

次に、ステップS105では、鍵指定情報を連結した鍵指定コードを生成する。

【0241】

次に、ステップS106において、暗号文ブロックを生成する。これは、ステップS102において決定したサブセットキーを適用して送信情報、例えばコンテンツキーKcを暗号化する処理である。なお、暗号文ブロックは、サブセットキーのノード番号順に並べ、かつ、同一ノードに対する複数の暗号文がある場合には前述のルール、すなわち、SK_k, zzzのZZZを2進数で表現した正数とみた場合に、大きい順に並べる。

【0242】

ステップS107では、ステップS105で生成した鍵指定コードと、ステップS106で生成した暗号文ブロックをパッケージとした暗号鍵ブロック(EKB)を生成する。

【0243】

ステップS108では、暗号鍵ブロック(EKB)とコンテンツキーKcで暗号化した暗号化コンテンツをネットワークを介して送信、あるいは情報記録媒体に格納する。なお、ステップS103で決定したエンコード方法についての識別情報も併せてネットワークを介して送信、あるいは情報記録媒体に格納する構成としてもよい。具体例については後述する。

10

20

30

40

50

【0244】

次に、図24を参照して、暗号文ブロックと鍵指定コードから構成される暗号鍵ブロック情報としてのEKBと暗号化コンテンツを受領し、コンテンツ再生処理を行うユーザデバイスとしての情報処理装置における処理手順について説明する。

【0245】

暗号文復号処理を実行する情報処理装置は、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て、鍵指定コードから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

10

を取得し、鍵指定情報から各種の情報取得を行い、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。また、エンコード方法についての識別情報も入力する構成としてもよい。

【0246】

鍵指定情報には、前述の実施例において説明したように、鍵指定木の構成ノードがリーフに対応する可否を示すリーフビット、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可否を示す鍵指定ビット、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暗号文ブロック中に含む可否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、分割サブセットの分割態様を示す分割法指定情報

20

ビット等を含んでおり、これらの鍵指定情報に基づいて、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。

【0247】

ステップS201において、エンコード方法識別情報を入力する。暗号鍵ブロックとしてのEKBには、図25に示すように、鍵指定コードのエンコード態様を示す情報が格納される。

【0248】

図25に示す例は、情報記録媒体700に暗号鍵ブロックとしてのEKB710を格納した例である。

【0249】

30

情報記録媒体700には、コンテンツキーKcを用いて暗号化された暗号化コンテンツのほかに、正当なコンテンツ利用権を有するデバイス（リーフ設定情報処理装置）がコンテンツキーを取得するための暗号鍵ブロック情報としてのEKB（Enabling Key Block）710が記録され、EKB（Enabling Key Block）710には、前述のように鍵指定木の構成ノードにおいて設定される様々なサブセットキーによってコンテンツキーを暗号化した1つ以上の暗号文を含む暗号文ブロック713と鍵指定コード712、さらに、鍵指定コードのエンコード態様を示す情報としての鍵指定情報エンコード方法識別値711が格納されている。鍵指定情報エンコード方法識別値711の具体例については後述する。

【0250】

40

なお、ネットワーク配信によりEKBを送信する場合にも同様の情報が送信される。

【0251】

図24に戻り、ユーザデバイスとしての情報処理装置における処理についての説明を続ける。ステップS202では、ステップS201で入力したエンコード方法識別情報に基づいてエンコード方法を判別する。

【0252】

ステップS203では、鍵指定コードを入力する。なお、エンコード方法識別情報、鍵指定コードは、ネットワークを介して受信する場合、情報記録媒体から読み取る場合がある。

【0253】

50

ステップS204において、エンコード情報に基づく鍵指定コード解釈を実行する。

【0254】

次に、ステップS205において、リボークされているか否かを判定する。これは、鍵指定コードに基づいて、自装置が復号可能な暗号文が選択できれば、リボークされていないことになり、選択できなければリボークされていると判定する。鍵指定コードを用いて鍵指定木の全部または一部を再構築して判定することができる。

【0255】

リボークされている場合は、暗号文ブロック中に含まれるどの暗号文も自装置に格納したサブセットキーを適用して復号できないので、コンテンツ復号、再生を実行することなく処理を終了する。

10

【0256】

リボークされていない場合は、ステップS206において、自己のサブセットキーで復号できる暗号文を暗号文ブロックから選択する。選択処理は、鍵指定コードに基づいて選択する。

【0257】

暗号文ブロックには、すべての鍵指定情報で指定された暗号文がノード番号順、さらに1つのノードに対し複数の暗号文が存在するときには前述の順に並んでいるので、復号すべき暗号文も一意に決定できる。たとえば図17の例で、情報処理装置 u_{17} は、リーフ17からルートへのパス上にあるノード2を見つけ、その鍵指定情報が、

$(c, ddd, e, ff) = (1, 111, 1, 10)$ なので、このノードにおいて定義されている、情報処理装置 u_{17} を構成要素とするサブセット $S_{2, 010}$ に対応するサブセットキー $SK_{2, 010}$ を用いた暗号文が暗号文ブロックに存在することがわかる。

20

【0258】

そして、この暗号文は、ノード2において定義されたサブセットのサブセットキーを用いて作られた暗号文の2つめに置かれていることもわかる。さらにそれ以外のノードの鍵指定情報も見ると、ノード2より番号が若いノードで対応するサブセットキーが用いられているものはないから、サブセットキー $SK_{2, 010}$ を用いた暗号文は暗号文ブロック全体の2番目の暗号文であることがわかるので、これを上記のサブセットキーを用いて復号すべきであることがわかる。

30

【0259】

いま、図17の例について説明したが、他の例でも同様に、リボークされていない受信機は復号すべき暗号文および復号に使用するサブセットキーを一意に特定できる。

【0260】

ステップS207では、選択した暗号文を入力し、自己の保有するサブセットキーを適用して復号処理を実行してコンテンツキー K_c を取得する。

【0261】

ステップS208において、取得したコンテンツキー K_c を適用して暗号化コンテンツを復号しコンテンツを取得し、再生処理を行なう。

【0262】

40

図25を参照して説明したように、暗号文と鍵指定コードを格納した暗号鍵ブロック(EKB)には鍵指定情報エンコード方法識別値711が識別情報として格納されている。

【0263】

鍵指定情報エンコード方法識別値711の具体例について説明する。上述した実施例1～3において説明したように鍵指定コードの設定態様は様々な態様があり、このどのコードを適用するかは鍵指定コードの生成側が決定できる。

【0264】

例えば、

(1) 従来技術として説明した鍵指定コード、すなわち、

リーフビット：c

50

鍵指定ビット：d d d

の(c, d d d)のビット構成とする方法。

(2) 実施例1で説明した鍵指定コード、すなわち、

リーフビット：c

鍵指定ビット：d d d

パーティションビット：e

の(c, d d d, e)のビット構成とする方法。

(3) 実施例2で説明した鍵指定コード、すなわち、

リーフビット：c

鍵指定ビット：d d d

パーティションビット：e

分割法指定ビット：f f

の(c, d d d, e, f f)のビット構成とする方法。

(4) 実施例3で説明した鍵指定コード、すなわち、

リーフビット：c

エンコードビット：g g g g

の(c, g g g g)のビット構成とする方法。

(5) 実施例3で説明した鍵指定コード、すなわち、

リーフビット：c

エンコードビット：h h h h

の(c, h h h h)のビット構成とする方法。

これらの各エンコード方法のどの方法が適用されたかを鍵指定情報エンコード方法7 1 1に識別情報として設定する。

【0 2 6 5】

例えば、

(1)の方法：0 0 0

(2)の方法：0 0 1

(3)の方法：0 1 0

(4)の方法：0 1 1

(5)の方法：1 0 0

などのように、予め情報コードを定め、コンテンツ再生を行なう情報処理装置は、これらの鍵指定情報エンコード方法識別値7 1 1に設定された識別情報に基づいて、鍵指定コードがどの種類のものであるかを判別する。

【0 2 6 6】

このように、鍵指定情報エンコード方法識別値を設けることで、複数の技術のうち効率のよい方法を選択して用いることが可能となる。用いられる可能性のある鍵指定情報のルール(エンコード方法)がこれ以上ある場合でも、同様の「鍵指定情報エンコード方法」の値により指定するようにすれば対応可能である。

【0 2 6 7】

さて、上記の実施例では、コンテンツの利用を行う情報処理装置、たとえば図17に示すリーフu_{1 4}に対応する情報処理装置は、ノード1において定義されたサブセットのうち、S_{1, 1 0 0}, S_{1, 1 1 0}, S_{1, 1 0 1}, S_{1, 1 1 1}の4つのサブセットに対応する4つのサブセットキーを持つことになる。他の情報処理装置でも、組み合わせは変わるが4つのサブセットキーを持つことは同様である。

【0 2 6 8】

ここで、システムで使用するサブセットキーS_{x, y y y}のうちy y yの部分の重み(1であるビットの個数)をたとえば、最大で2とし、それ以下のもののみ使用する、ということにすれば、情報処理装置は、サブセットキーS_{K_{1, 1 1 1}}を持たなくてよくなる。もしリポークする機器がなく、通常はS_{K_{1, 1 1 1}}を暗号化に用いたい場合には、上記のいずれかの手法によりこれを分割して、たとえばS_{K_{1, 1 0 0}}, S_{K_{1, 0 1 1}}の

10

20

30

40

50

2つのサブセットキーを用いた2つの暗号文を暗号化ブロックにて送信する。

【0269】

このようにすることにより、暗号文ブロックのサイズは増加する可能性があるが、コンテンツ利用側の情報処理装置の持つ鍵数を減らせるというメリットがある。

【0270】

これは、上記の3分木の例よりも、4分木、もしくはそれ以上の多分木を用いた場合に大きな効果が期待される。

【0271】

なお、上述した実施例においては、3分木を中心として説明してきたが、本発明の構成は、4分木、もしくはそれ以上の他分木においても適用できる技術である。

10

【0272】

以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【0273】

なお、明細書中において説明した一連の処理はハードウェア、またはソフトウェア、あるいは両者の複合構成によって実行することが可能である。ソフトウェアによる処理を実行する場合は、処理シーケンスを記録したプログラムを、専用のハードウェアに組み込まれたコンピュータ内のメモリにインストールして実行させるか、あるいは、各種処理が実行可能な汎用コンピュータにプログラムをインストールして実行させることが可能である。

20

【0274】

例えば、プログラムは記録媒体としてのハードディスクやROM (Read Only Memory) に予め記録しておくことができる。あるいは、プログラムはフレキシブルディスク、CD-R (Compact Disc Read Only Memory)、MO (Magneto optical) ディスク、DVD (Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体に、一時的あるいは永続的に格納（記録）しておくことができる。このようなリムーバブル記録媒体は、いわゆるパッケージソフトウェアとして提供することができる。

30

【0275】

なお、プログラムは、上述したようなリムーバブル記録媒体からコンピュータにインストールする他、ダウンロードサイトから、コンピュータに無線転送したり、LAN (Local Area Network)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを受信し、内蔵するハードディスク等の記録媒体にインストールすることができる。

【0276】

なお、明細書に記載された各種の処理は、記載に従って時系列に実行されるのみならず、処理を実行する装置の処理能力あるいは必要に応じて並列的にあるいは個別に実行されてもよい。また、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

40

【産業上の利用可能性】

【0277】

以上、説明したように、本発明の構成によれば、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し、鍵指定コードの構成データである鍵指定木ノード毎の鍵指定情報中に、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暗号文ブ

50

ロック中に含むか否かのサブセット分割識別情報（パーティションビット）を含める構成としたので、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生成して情報処理装置に送信することが可能となり、暗号文および鍵指定コードを受領した情報処理装置側においては、受領した暗号文が、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であるか否かを判別して、鍵指定コードに基づいて、自己の復号対象の暗号文を選択することが可能となり、本発明は、木構造を適用した暗号文の提供構成において利用可能である。具体的には、暗号文生成、提供、送信を実行する情報処理装置、暗号文の復号、再生を実行するユーザデバイスとしての情報処理装置、暗号化コンテンツ等を格納した情報記録媒体において適用可能である。

【0278】

10

本発明の構成によれば、木構造を用いた情報配信方式を適用した暗号文送信構成において、様々な分割サブセットを設定した暗号文の提供が可能となるので、攻撃者による様々な攻撃が行なわれた場合、効率的にリボーク対象としてのリーフに対応する情報処理装置の特定が可能となるので、リボーク対象の特定処理の必要な、木構造を適用した暗号文の提供構成において利用可能である。具体的には、暗号文生成、提供、送信を実行する情報処理装置、暗号文の復号、再生を実行するユーザデバイスとしての情報処理装置、暗号化コンテンツ等を格納した情報記録媒体において適用可能である。

【0279】

さらに、本発明の構成によれば、分割態様が複数あるサブセットにおいても、分割態様を示す分割法指定ビットを設定した構成としたので、例えば3分木構成において2つの枝と1つの枝の様々な組み合わせや3つの枝毎の分割サブセットの設定など任意の分割態様の設定が可能となる。暗号文ブロックからの暗号文選択および復号処理を行う情報処理装置では、鍵指定コードに含まれる鍵指定情報に含まれる分割法指定ビットを解析することにより、復号対象の暗号文を選択することができる。さらに、本発明の構成において、鍵指定ビット、パーティションビット、分割法指定ビットのビット情報を符号化した構成によれば、鍵指定コードの情報量を削減することが可能となる。従って、本発明は、木構造を適用した暗号文の提供構成において利用可能である。具体的には、暗号文生成、提供、送信を実行する情報処理装置、暗号文の復号、再生を実行するユーザデバイスとしての情報処理装置、暗号化コンテンツ等を格納した情報記録媒体において適用可能である。

20

【図面の簡単な説明】

30

【0280】

【図1】2分木階層型木構造について説明する図である。

【図2】2分木階層型木構造において、選択した情報処理装置のみが取得可能な情報を送信する方法を説明する図である。

【図3】鍵指定コードを暗号文とともに各情報処理装置に提供する構成について説明する図である。

【図4】a分木ツリーの構成例として3分木構成を示す図である。

【図5】3分木構成において、例えばコンテンツ管理者等が選択した情報処理装置のみが取得可能な情報、例えばコンテンツキーを提供する方法を説明する図である。

【図6】3分木構成における鍵指定コードについて説明する図である。

40

【図7】リーフビットにより鍵指定コードの情報量を削減した構成について説明する図である。

【図8】サブセットの分割構成について説明する図である。

【図9】サブセットの分割構成について説明する図である。

【図10】実施例1に係る鍵指定コードの構成、処理例の詳細について説明する鍵指定木を示した図である。

【図11】実施例1に係る構成において、任意のノードiにおいて、鍵指定ビット（dd）と、パーティションビット（e）の組み合わせ（ddd, e）が取りうる値と、そのときに暗号文ブロックに含まれる暗号文の対応を示した対応テーブルを示した図である。

【図12】図8で示した例に加えて、さらに、サブセットキーSK₁, 100をサブセッ

50

トキー $SK_{2, 100}$ 、 $SK_{2, 010}$ 、 $SK_{2, 001}$ の3つに分割した部分木の構成を示した図である。

【図13】部分木を分割して複数の部分木として再設定する処理を説明する図である。

【図14】実施例1における鍵指定木の各ノードにおける鍵指定情報(c, d d d, e)を示す図である。

【図15】分木数が3以上の場合の分割態様について説明する図である。

【図16】実施例2における鍵指定木を構成するノードiに設定される鍵指定情報中の、鍵指定ビットd d d、パーティションビットe、分割法指定ビットf fのパターンについて示す図である。

【図17】実施例2に係る鍵指定情報(c, d d d, e, f f)の計7ビット構成を持つ鍵指定情報を鍵指定木の各構成ノードに設定した例を示す図である。 10

【図18】(d d d, e, f f)の5ビットの値を符号化(エンコード)した4ビットの値(g g g g)または(h h h h)として設定した例を説明する図である。

【図19】(c, g g g g)5ビット構成とした場合の鍵指定木と各ノードに設定される鍵指定情報、および鍵指定コードの構成を示した図である。

【図20】(c, h h h h)5ビット構成とした場合の鍵指定木と各ノードに設定される鍵指定情報、および鍵指定コードの構成を示した図である。

【図21】暗号文、鍵指定コードを生成し提供する送信装置等の情報処理装置、暗号文、鍵指定コードを受領して、暗号文を選択し復号してコンテンツキー等の情報取得を行なう受信装置等の情報処理装置の構成例を示す図である。 20

【図22】DVD等の記録媒体に暗号化コンテンツを格納し、さらに、暗号化コンテンツの暗号鍵であるコンテンツキーK cを複数のサブセットキーで暗号化した暗号文ブロックと、鍵指定コードを格納した情報記録媒体の構成例を示す図である。

【図23】ユーザデバイスとしての情報処理装置に提供する暗号文ブロックと鍵指定コードから構成される暗号鍵ブロック情報としてのE K Bを生成する情報処理装置におけるE K Bを生成処理フローを示す図である。

【図24】暗号文ブロックと鍵指定コードから構成される暗号鍵ブロック情報としてのE K Bと暗号化コンテンツを受領し、コンテンツ再生処理を行うユーザデバイスとしての情報処理装置における処理手順について説明する図である。

【図25】鍵指定コードのエンコード態様を示す情報が格納した鍵情報ブロック(E K B)構成を説明する図である。 30

【符号の説明】

【0281】

101 情報処理装置

120 ルートノード

121, 122, 123 ノード

131, 132, 133, 134, 135 部分木

201 ノード

211 部分木

301 鍵指定木 40

311 部分木

321 鍵指定木

351, 352 部分木

401 鍵指定木

421 鍵指定木

431 鍵指定木

500 情報処理装置

501 コントローラ

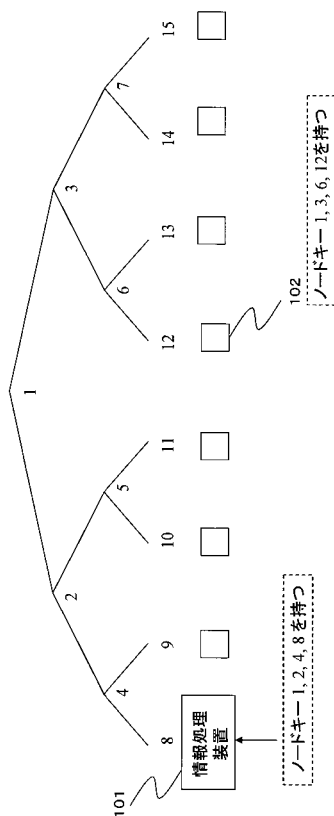
502 演算ユニット

503 入出力インタフェース 50

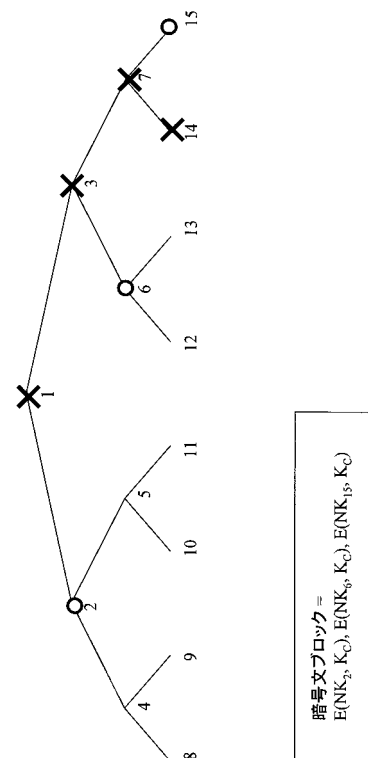
- 504 セキュア記憶部
- 505 メイン記憶部
- 506 ディスプレイ装置
- 507 メディアインタフェース
- 600 情報記録媒体
- 610 暗号鍵ブロック情報 (EKB)
- 611 鍵指定コード
- 612 暗号文ブロック
- 620 暗号化コンテンツ
- 700 情報記録媒体
- 710 暗号鍵ブロック情報 (EKB)
- 711 鍵指定情報エンコード方法識別値
- 712 鍵指定コード
- 713 暗号文ブロック

10

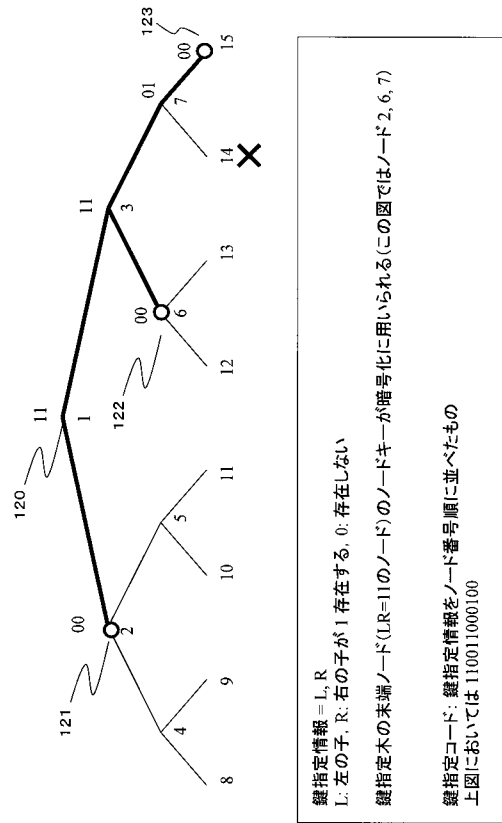
【図 1】



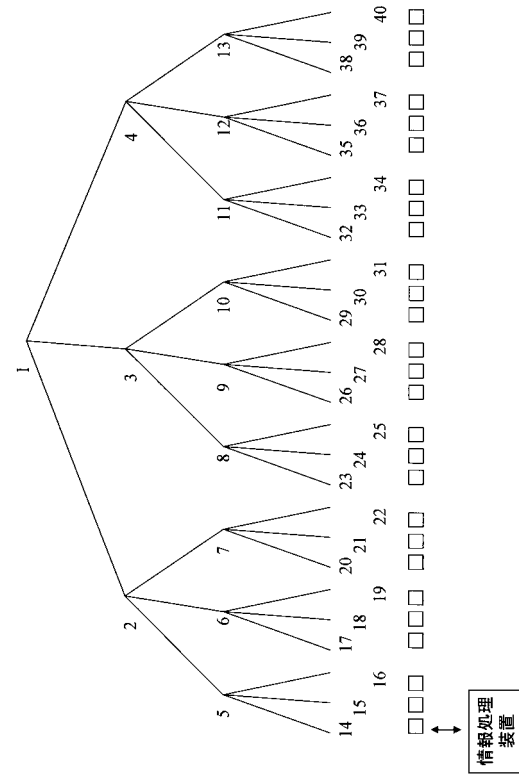
【図 2】



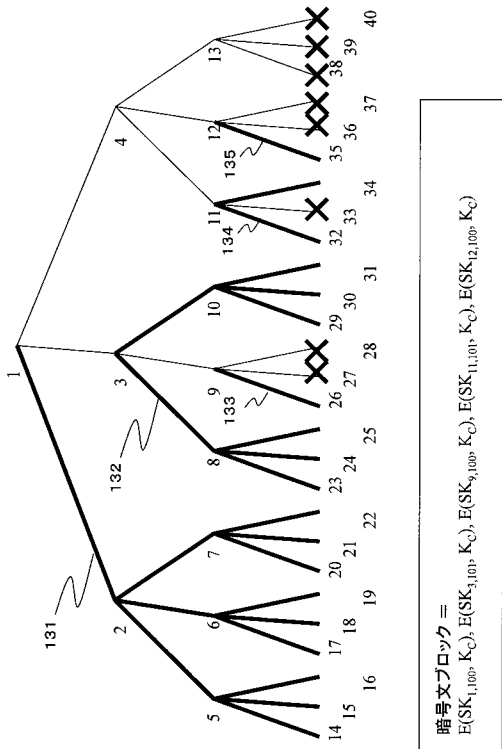
【図 3】



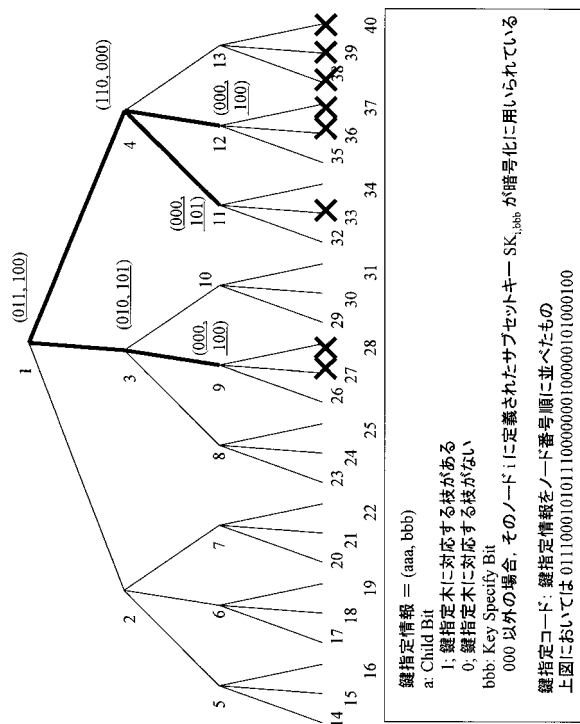
【図 4】



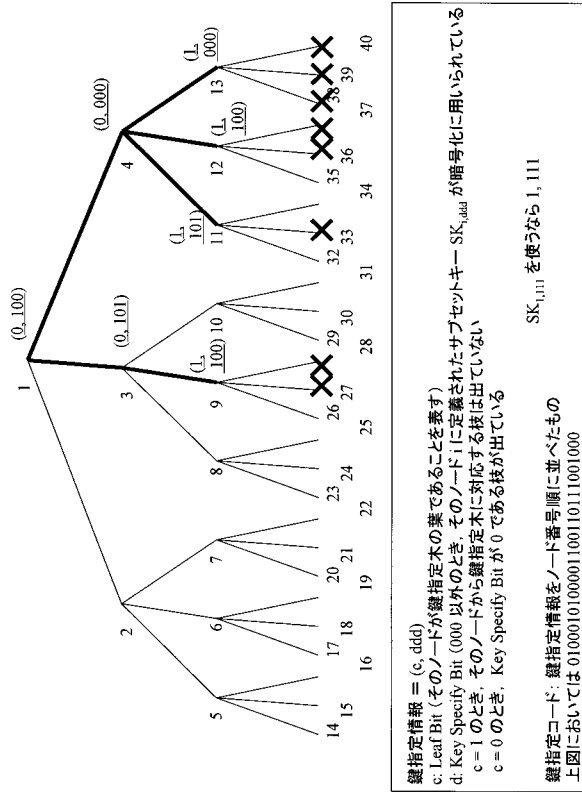
【図 5】



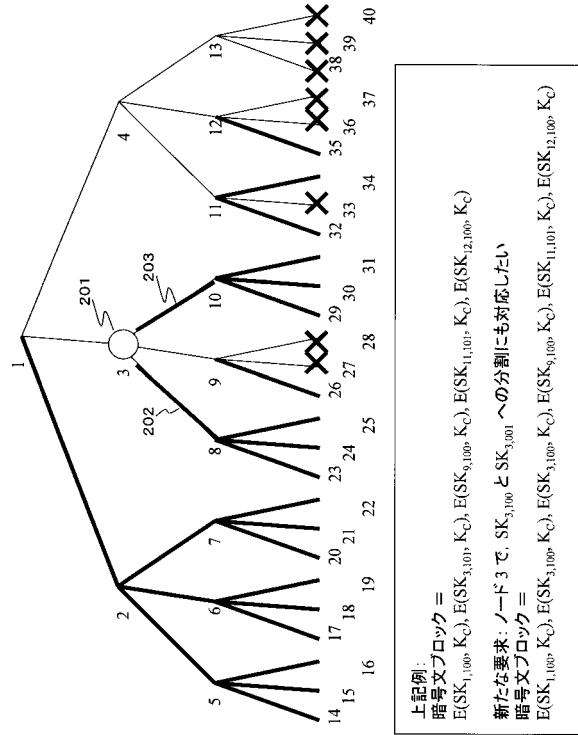
【図 6】



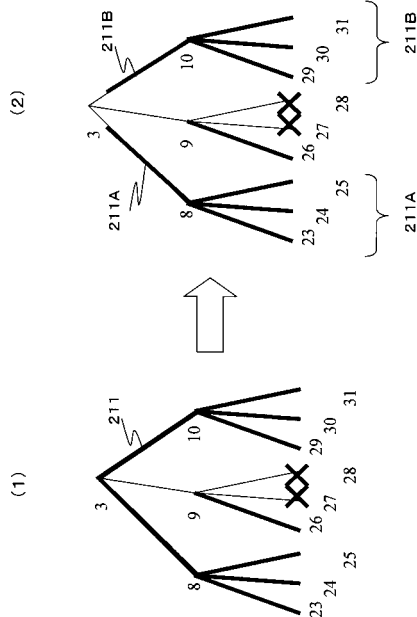
【図 7】



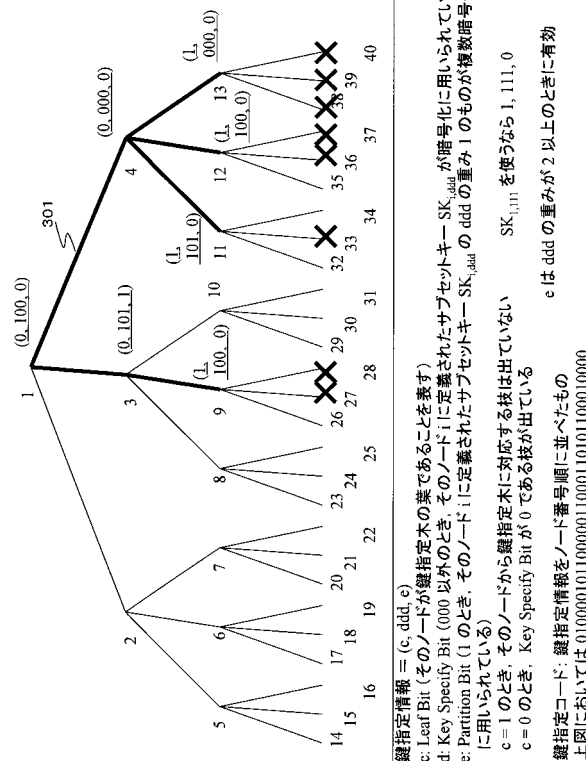
【図 8】



【図 9】



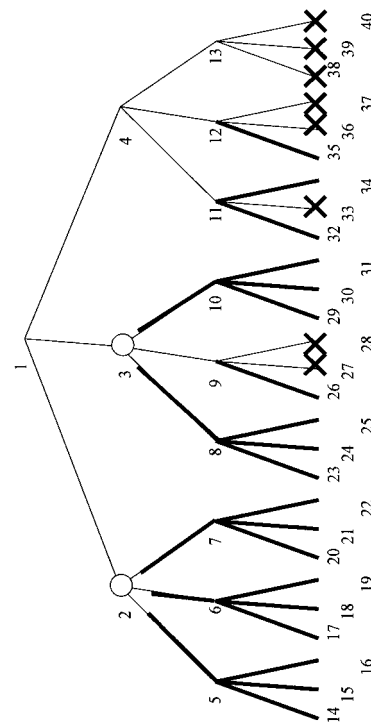
【図 10】



【図 1 1】

ノード i における ddd, e の値とその際に用いられる暗号文	
ddd, e	暗号文
000, 0	なし
100, 0	$E(SK_{1,100}, K_C)$
010, 0	$E(SK_{1,010}, K_C)$
001, 0	$E(SK_{1,001}, K_C)$
110, 0	$E(SK_{1,110}, K_C)$
110, 1	$E(SK_{1,100}, K_C), E(SK_{1,010}, K_C)$
101, 0	$E(SK_{1,100}, K_C), E(SK_{1,001}, K_C)$
101, 1	$E(SK_{1,100}, K_C), E(SK_{1,001}, K_C)$
011, 0	$E(SK_{1,010}, K_C), E(SK_{1,001}, K_C)$
011, 1	$E(SK_{1,010}, K_C), E(SK_{1,111}, K_C)$
111, 0	$E(SK_{1,100}, K_C), E(SK_{1,010}, K_C), E(SK_{1,001}, K_C)$
111, 1	$E(SK_{1,100}, K_C), E(SK_{1,010}, K_C), E(SK_{1,001}, K_C)$

【図 1 2】



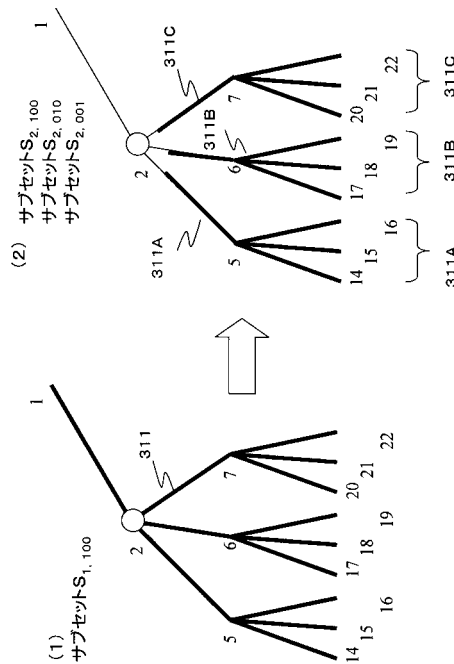
ノード 3 で、 $SK_{1,100}$ と $SK_{3,001}$ への分割にも対応した例

暗号文ブロック = $E(SK_{1,100}, K_C), E(SK_{1,001}, K_C), E(SK_{3,001}, K_C), E(SK_{9,100}, K_C), E(SK_{11,001}, K_C), E(SK_{12,100}, K_C)$
(ここまでは図 8 の例)

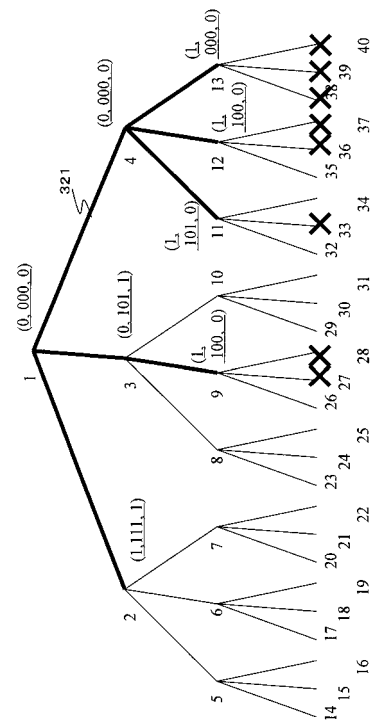
さらに、 $SK_{1,100}$ を $SK_{2,100}$ と $SK_{2,010}$ と $SK_{2,001}$ に分割したい

暗号文ブロック = $E(SK_{2,100}, K_C), E(SK_{2,010}, K_C), E(SK_{2,001}, K_C), E(SK_{3,001}, K_C), E(SK_{9,100}, K_C), E(SK_{11,001}, K_C), E(SK_{12,100}, K_C)$

【図 1 3】



【図 1 4】



鍵指定情報 = (c, ddd, e)

c: Leaf Bit (そのノードが鍵指定木の葉であることを表す)

d: Key Specify Bit (000 以外の場合、そのノード i に定義されたサブセットキー SK_{ddd} が暗号化に用いられている

e: Partition Bit (1 のとき、そのノード i に定義されたサブセットキー SK_{ddd} の ddd の重み 1 のものが複数暗号化に用いられている)

c = 1 のとき、そのノードから鍵指定木に対応する枝は出していない

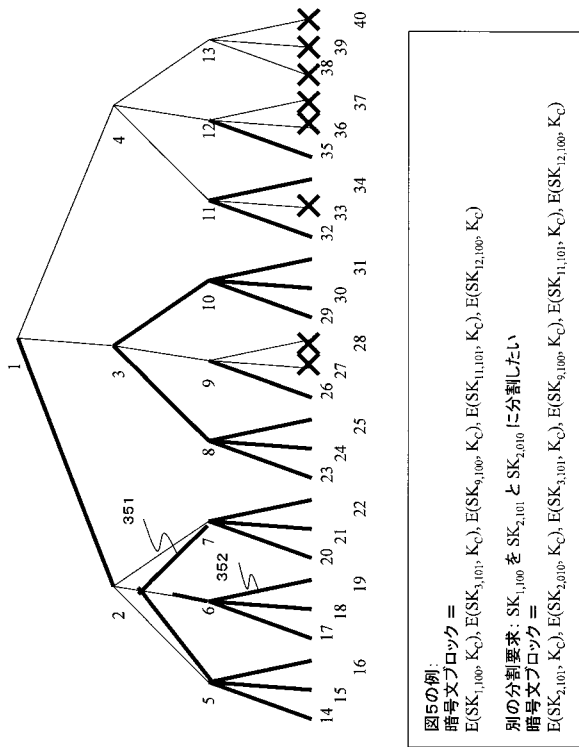
c = 0 のとき、Key Specify Bit が 0 である枝が出ている

鍵指定コード: 鍵指定情報をノード番号順に並べたもの

$SK_{1,111}$ を使うなら 1, 111, 0

上図においては 0000011111010110000011000110101100010000

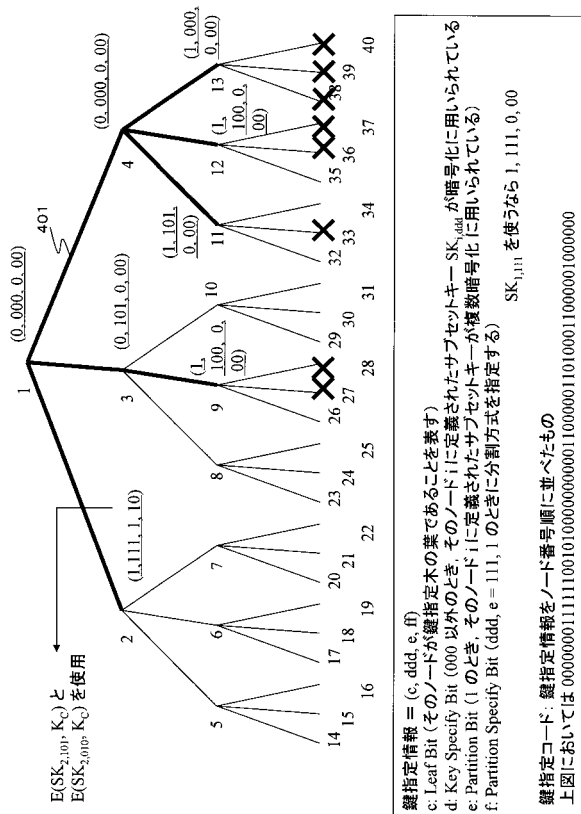
【図 15】



【図 16】

ノード i における ddd, e, ff の値とその際に用いられる暗号文	
ddd, e, ff	暗号文
(1) 000, 0, 00	なし
(2) 100, 0, 00	$E(SK_{1,100}, K_C)$
(3) 010, 0, 00	$E(SK_{3,101}, K_C)$
(4) 001, 0, 00	$E(SK_{9,100}, K_C)$
(5) 110, 0, 00	$E(SK_{1,101}, K_C)$
(6) 110, 1, 00	$E(SK_{1,100}, K_C), E(SK_{100}, K_C)$
(7) 101, 0, 00	$E(SK_{1,101}, K_C)$
(8) 101, 1, 00	$E(SK_{1,100}, K_C), E(SK_{100}, K_C)$
(9) 011, 0, 00	$E(SK_{3,101}, K_C)$
(10) 011, 1, 00	$E(SK_{3,101}, K_C), E(SK_{100}, K_C)$
(11) 111, 0, 00	$E(SK_{9,100}, K_C)$
(12) 111, 1, 00	$E(SK_{9,100}, K_C), E(SK_{100}, K_C)$
(13) 111, 1, 01	$E(SK_{1,100}, K_C), E(SK_{101}, K_C)$
(14) 111, 1, 10	$E(SK_{1,100}, K_C), E(SK_{101}, K_C)$
(15) 111, 1, 11	$E(SK_{1,100}, K_C), E(SK_{101}, K_C)$

【図 17】



【図 18】

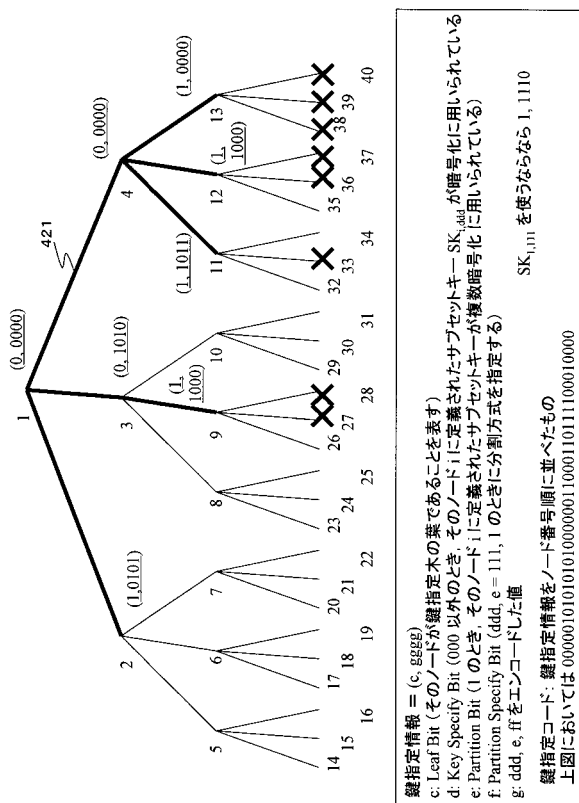
ノード i における ddd, e, ff の値とその際に用いられる暗号文	
ddd, e, ff	暗号文
(1) 000, 0, 00	なし
(2) 100, 0, 00	$E(SK_{1,100}, K_C)$
(3) 010, 0, 00	$E(SK_{3,101}, K_C)$
(4) 001, 0, 00	$E(SK_{9,100}, K_C)$
(5) 110, 0, 00	$E(SK_{1,101}, K_C)$
(6) 110, 1, 00	$E(SK_{1,100}, K_C), E(SK_{100}, K_C)$
(7) 101, 0, 00	$E(SK_{1,101}, K_C)$
(8) 101, 1, 00	$E(SK_{1,100}, K_C), E(SK_{100}, K_C)$
(9) 011, 0, 00	$E(SK_{3,101}, K_C)$
(10) 011, 1, 00	$E(SK_{3,101}, K_C), E(SK_{100}, K_C)$
(11) 111, 0, 00	$E(SK_{9,100}, K_C)$
(12) 111, 1, 00	$E(SK_{9,100}, K_C), E(SK_{100}, K_C)$
(13) 111, 1, 01	$E(SK_{1,100}, K_C), E(SK_{101}, K_C)$
(14) 111, 1, 10	$E(SK_{1,100}, K_C), E(SK_{101}, K_C)$
(15) 111, 1, 11	$E(SK_{1,100}, K_C), E(SK_{101}, K_C)$

(B)

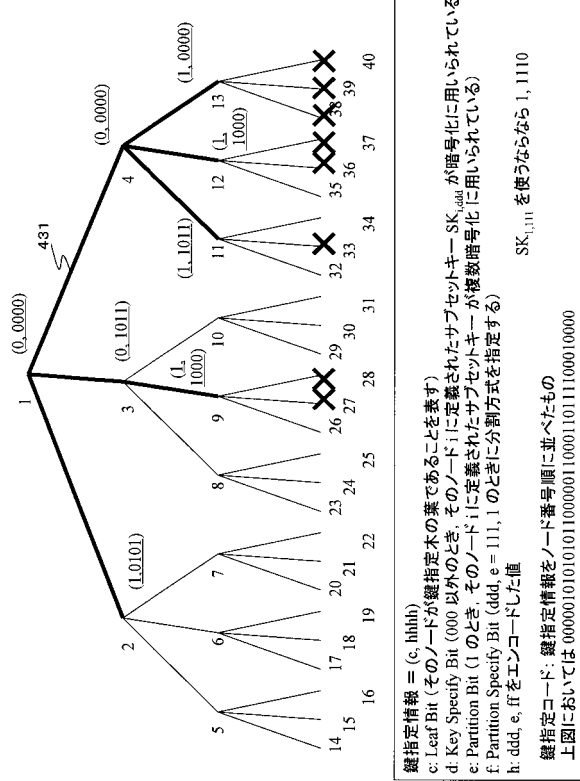
hhhh の重みと暗号文数	
重み	暗号文数
0	0
1	1
2	2
3	1
4	3

(A)

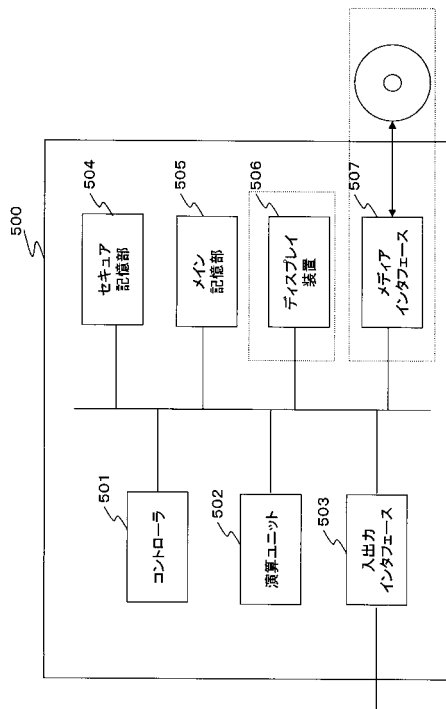
【図 19】



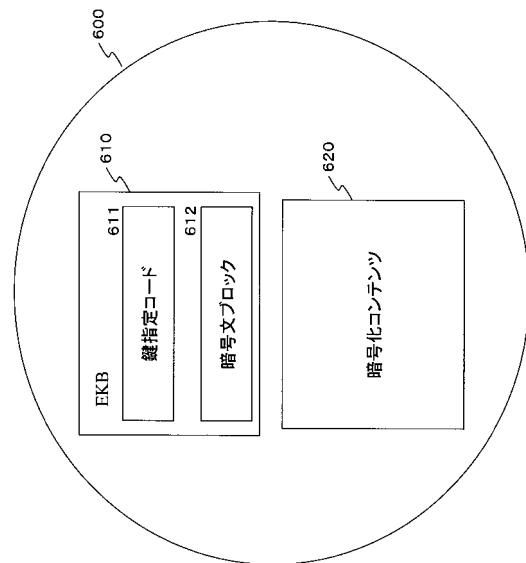
【図 20】



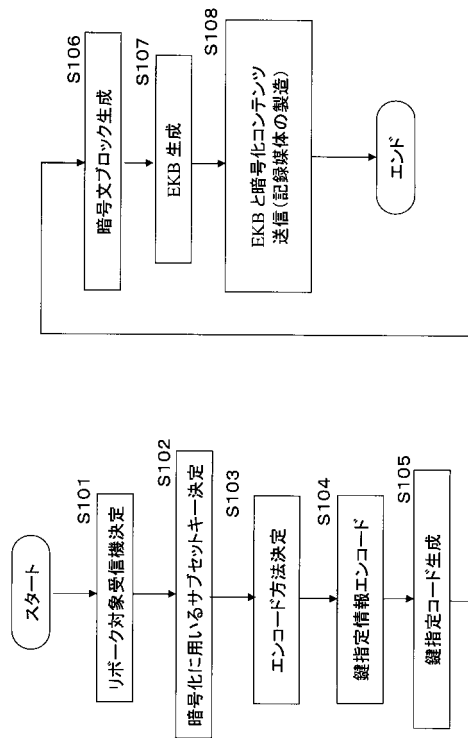
【図 2 1】



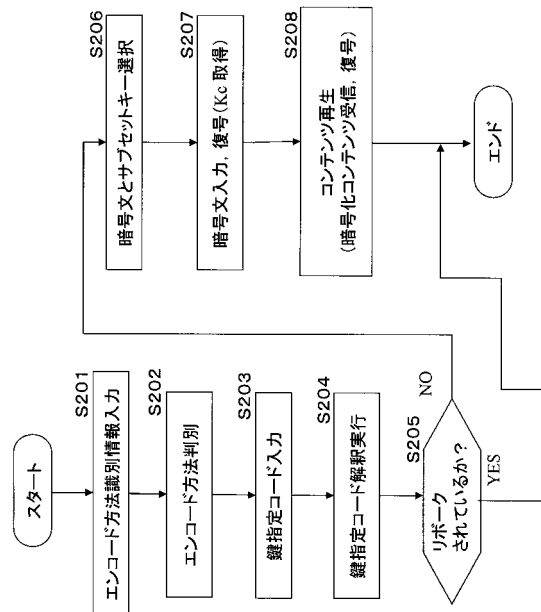
【图 2 2】



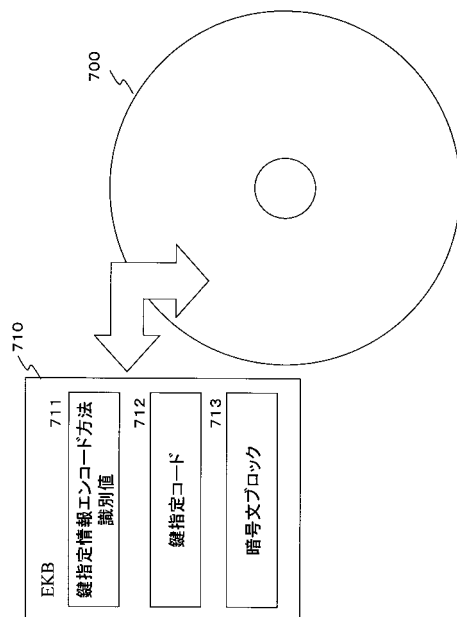
【図 2 3】



【図 2 4】



【図 2 5】



フロントページの続き

(56)参考文献 特開2003-169048 (JP, A)
国際公開第02/060118 (WO, A1)

(58)調査した分野(Int.Cl., DB名)
H04L 9/08